Barracuda Networks Technical Documentation

Barracuda **NG Network Access Client**

Administrator's Guide

Version SP4

RECLAIM YOUR NETWORK™

Copyright Notice

Trademarks

Barracuda NG Network Access Client

Chapter 1
Introduction

1.1 Endpoint Security and Network Access Control

With the advent of novel technologies, work habits have changed dramatically throughout the past decades. Notebooks and netbooks, smartphones and vast amounts of data easily portable on USB sticks and miniature storage cards, ubiquitous wireless network access, personal area networking, they all have attributed to the fact that endpoints in corporate networks have become an increasingly hard to control hazard.

Effective endpoint security today extends far beyond historical personal firewall and antivirus concepts. It still means protection of an endpoint against network threats using a host firewall and malware detection software, but extends the protection concept by a broader enforcement and validation of security policies that are specific to the identity of the device, the user and its current state. Powerful endpoint security concepts also necessitate full integration into an accompanying network access control framework.

Network Access Control (NAC) represents a novel technology aimed at guaranteeing that access to enterprise network resources is granted based upon authentication of the user and device as well as verification of the device's compliance with current security policies.

By default, a typical Network Access Control solution offers enhanced protection against malicious software and attackers, improved access control to the network for employees and guests, superior resource usage tracking, and a powerful policy adherence mechanism. As a consequence, the complexity of the network and the administration effort required is significantly reduced, a greater degree of integration among stand-alone security solutions is achieved, existing and potential security gaps are nicely closed, and a greater visibility of end-to-end security is provided.

1.2 Introduction to Barracuda NG Network Access Client

Barracuda NG Network Access Client denotes Barracuda Networks' endpoint security and network access control (NAC) framework. Administered endpoint integrity and endpoint access is what Barracuda NG Network Access Client provides. In order to achieve this, it consists of client software components[1], server side components, which the client software periodically communicates with to have the health state of its underlying operating system verified and its network access rights assessed. Barracuda NG Firewalls can interpret that information and subsequently allow or deny network access attempts by the respective client.

1. Available for Microsoft® Windows XP (32 Bit) and Vista (32 Bit and 64 Bit) Windows 7 (32 Bit and 64 Bit)operating systems

Before we have a closer look at the interplay of the various components and their roles let us briefly study what has inspired the design of the Barracuda NG Network Access Client endpoint security framework.

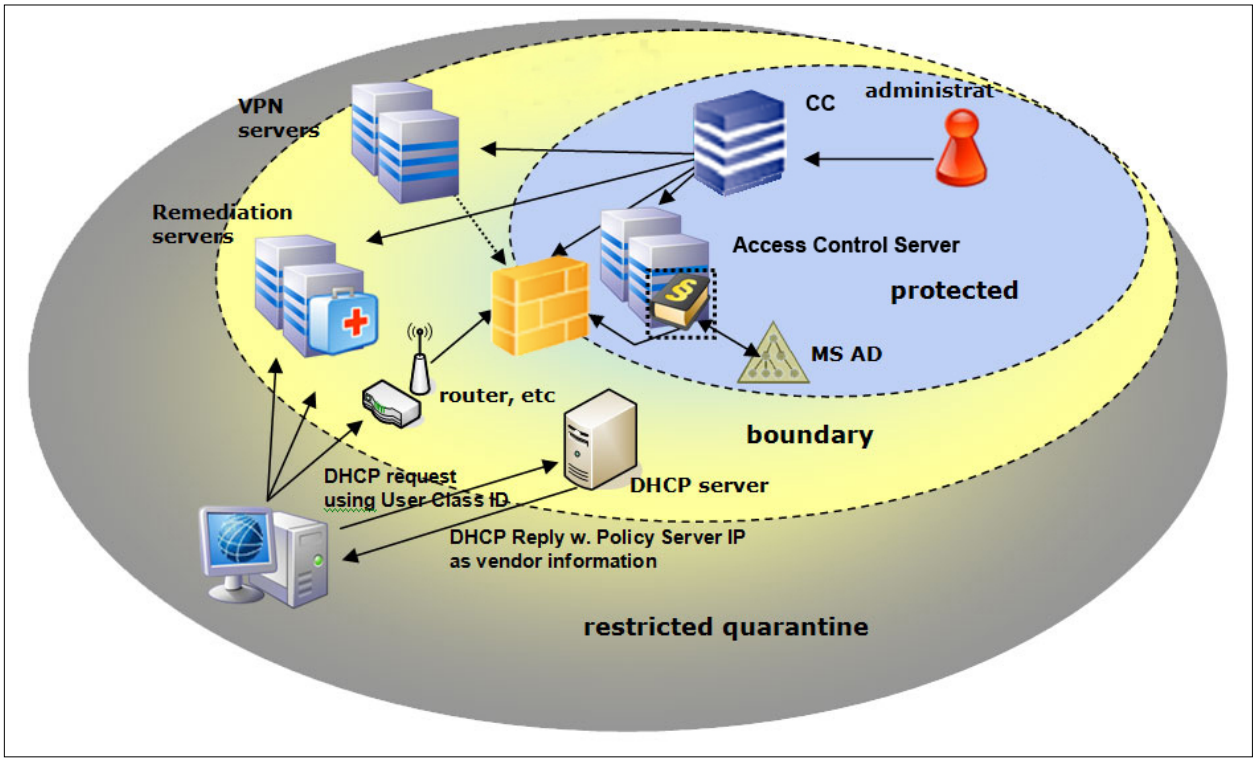
The originally very long list of requirements reads as follows in a slightly more condensed fashion:

- ***We want to create an endpoint security solution that is effective and yet still simple enough to be implemented and operated in a cost efficient manner.***
- ***We do not wish to require customers to completely change their infrastructures. This means that we do not require 802.1x aware switches and endpoints.***
- ***We support guest networking. There must be a simple way to distinguish between visitors and own users. We use a combination of client agent-based and DHCP-based address assignment. A combination of agent-based and DHCP enforcement will likely catch the most prevalent threats to network security.***
- ***We assess the client's health prior to its initial connecting to the network. Client system health assessments should also be carried out periodically afterwards to detect changes in the client health state.***
- ***Policies, such as applicable firewall rule set or access rights, must be selected according to both, identity and system health state. ID-based exceptions must be possible to cater for real world scenarios. A forced client update of several megabytes across a 2400 baud link is not meaningful when the link is required for important messaging.***
- ***Policies can be machine specific. A PC frequently going online with nobody actually being logged in, may already have been compromised. This routine situation must be easily accommodated within the policy framework. This also means we've got to find means to identify a machine in a unique fashion.***
- ***Policies may differ in different access contexts; this is the archetypal roaming laptop problem. A certain policy will apply to its user when connecting from within the corporate network. A different policy is required for accessing the nearest WLAN hotspot on the airport to build a secure VPN connection. Again, a different policy is required when operating the same equipment inside the user's private home network.***

The client software consists of the following subsystems:

- **Barracuda NG Personal Firewall**
  Being a centrally managed host firewall, this advanced firewall engine can handle up to four different firewall rule sets at once. Which rule sets are available to the firewall engine and which one of these is currently enforced depends on the policy applicable to user, machine, date, and time.
- **Barracuda NG Access Monitor**
  This software is responsible for sending the endpoint health status to the Access Control Service for baselining. Barracuda NG Access Monitors are dynamically downloaded and updated as required, supporting same full and delta updates. They are extremely light as they only occupy 340 KB in memory.
- **Barracuda NG VPN Client**
  Provides an integrated VPN client that secures mobile desktops connecting to the corporate LAN through the internet. The VPN client will establish a secure connection to a VPN Service. The Barracuda NG Access Monitor will then communicate through the VPN tunnel with the responsible so-called System Health Validator *(SHV). It is worth noticing that in this case the VPN server fully controls the virtual connection.*

Fig. 1–1 *Barracuda NG Network Access Client environment*



Note

Since the NG Network Access Clients are communicating with the Access Control Server in cyclic intervals, the Access Control Server should be placed as close as possible to the NG Network Access Clients. This helps reducing network traffic and getting better response times.

1.2.1 What can Barracuda NG Network Access Client be used for?

It can be used to implement an endpoint security policy on Windows based endpoints within a corporate network. In this context, Barracuda NG Network Access Client provides a managed personal firewall solution with periodic health assessments. Both, the outcome of the assessment as well as the identity of the machine and/or current user, will influence the policy applicable to the endpoint. Enforcement of the policy is provided by the software installed on the endpoint itself and with regard to enforcement outside the local collision domain by Barracuda NG Firewalls. The latter may interpret the access policy attribute assigned to the endpoint within their rule sets. This provides a way to enforce network access control concepts based on date and time, identity, and health state and type of network access. The latter is required to enforce different policies when access takes place through a VPN tunnel.

This setup requires the presence of at least one Access Monitor Service. This service entails two component services. The SHV is the policy matching engine that determines the applicable policy according to the connector's identity and current health state.

The SHV issues a digitally signed cookie to the connecting endpoint, which contains all the information pertinent to the identity and state of this client. That cookie serves as a passport of limited temporal validity with which the endpoint may identify itself to the remediation server.

The remediation server is the component from which policy attributes, such as firewall rule sets, welcome messages, and bitmaps as well as client software components required for updates can be obtained. It can be run on the same Barracuda NG Firewall system as the SHV or, for load balancing reasons, it can be spread out over several Barracuda NG Firewall systems.

Note

SHV and remediation server must always remain accessible to all endpoints regardless of the currently active firewall rule set.

How does the client know at which address the SHV service component may be reached? There are two options here. The first one is that the respective addresses are configured statically within the client configuration on the endpoint. This approach is mandatory if DHCP based address assignment is not used.

In the case of DHCP based address assignment the respective address or addresses are assigned to the client by way of the vendor ID DHCP option (43).

DHCP is also used to make a distinction between own endpoint systems with an installed NG client and the so called **guest systems**. As guest systems are not able to communicate with SHV they are not assigned any SHV addresses. By way of the DHCP user ID option sent by the client a DHCP server may assign an address from a pool on a separate subnet.

Note that while this approach may easily be circumvented by a skilled human attacker to gain network access, worm and other malware issued with limited intelligence located on visitor's notebooks are typically prevented from quickly spreading out into the principal network.

In this LAN scenario up to three firewall rule sets can be assigned to a secured and monitored endpoint. When the endpoint system goes online and connects to the SHV it will be assigned a "local machine" rule set and a "limited access" rule set. The limited access rule set is the one rule set that comes into effect when the endpoint is diagnosed as unhealthy by the SHV. Note that the quarantine state is not entered immediately as there is a configurable period of time during which the client is given a chance to recover from the current condition, for example by successfully starting a disabled anti-virus (AV) scanner service or updating an obsolete AV pattern file.

As soon as a user logs into the system a different policy may apply to the endpoint now, depending on the identity of the user and various other conditions. The assigned policy attributes may in due cause a different so-called "current user" rule set to be assigned. In contrast to the previous two this rule set is volatile. That means it is cleared when the user logs off or the system is rebooted.

Consequently a notebook that has been used in the office environment and is taken home in the evening will operate there with the most recently installed "local machine" firewall rule set.

Any endpoint whose system state is assessed as unhealthy will have the most recently installed "limited access" rule set activated by the NG client after a configurable grace period.

Barracuda NG Network Access Client can also be used to secure mobile desktops connecting to the corporate LAN through the internet. To this end, NG NAP provides an integrated VPN client. The VPN client will establish a secure connection to a Barracuda NG VPN Service. The NG Network Access Monitor will then communicate through the VPN tunnel with the responsible SHV. From this point on the overall procedure is quite analogous to the LAN scenario. The most notable difference is that the VPN server fully controls the virtual connection. That means that also traffic within the VPN network's collision domain is fully subject to the NG Network Access Control framework. This better control also necessitates that the remediation service component is also active on the very same Barracuda NG Firewall system, which is also hosting the VPN Service.

In the LAN context certain policy attributes together with a "current user" rule set are assigned. This setup supports a maximum of up to three different firewall rule sets. The rationale behind this

seemingly complex procedure is rather straightforward and easy to understand. As autonomous machine authentication is rather uncommon in the VPN context, the "limited access" and the "local machine" firewall rule sets and policies need to be provided together with the actual VPN rule set.

Note

The "local machine" rule set thus acts as a VPN-offline rule set that can be used to centrally control the network access rights of the mobile user even when they are not connected to the corporate LAN.

Table 1–1

	Policy		
VPN Assignment	**Healthy**	**Limited Access**	**VPN Offline**
	Firewall rule set	Firewall rule set	Firewall rule set (=local machine rule set)
	Message of the day	Message	
	Welcome picture		
	Network access policies		

1.2.2 Licensing Aspects

In order to operate an Access Control Service either as a SHV or a remediation server or both, a valid license needs to be present. On Barracuda NG Firewall systems, the Access Control Service is automatically licensed.

It is possible to equip all Barracuda NG Firewall branch office devices with a remediation server in order to reduce WAN traffic and optimize response times.

1.2.3 Policy Matching Procedure

Each Access Control Service belongs to a so called trustzone. All Access Control Services within the same trust zone share the same set of security policies. In addition, they share a signing key, so that a mutual trust relationship can be established.

Within each trustzone there are three policy rule sets. There is a "local machine" policy rule set that is used to determine a policy for a connecting machine. A connecting machine is an endpoint system that does not request user authentication.

As soon as user authentication is requested by the connecting client, the "current user" policy rule set is used for policy matching.

If the connection attempt is mediated by an intermittent VPN Service the VPN policy rule set is adopted.

1.3 What is a Policy Rule Set?

A policy rule set is an ordered list of policy rules that is processed from the top to the bottom in sequential order. If no identity match can be found a "no rule exception policy" is assigned. From now

on the client system is assumed untrusted and a configured "untrusted access" firewall rule set and client message applies.

Nevertheless, Barracuda Networks recommends to configure a catch-all rule at the end of the policy rule set. An explicit catch-all rule allows a better control of the required client health-state and gives more details to the end user. In addition more details in the server-side visualisation will be available.

Each policy rule consists of three parts:

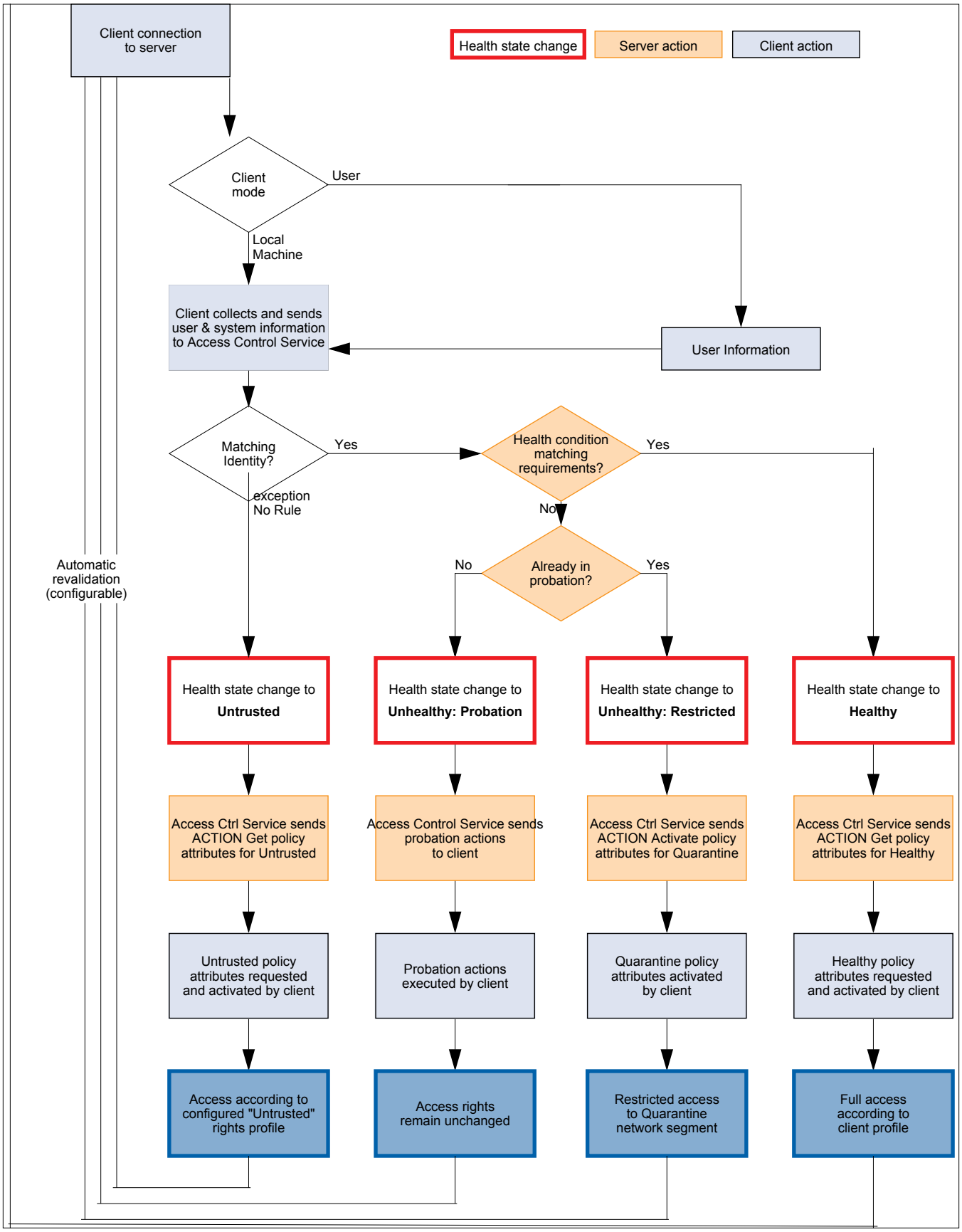
1. An identity related part that defines the applicable matching policy and criteria.

2. A health policy part is used to determine the health state by comparing the status information sent by the client with the specified required status. There are only three health states: healthy, probation, and unhealthy.

3. And finally, there is a third policy attribute part that contains firewall rule sets, messages, pictures, and network access policies that are assigned to a healthy client.

The matching procedure is graphically shown on the next page.

Fig. 1–2 *Client-Server actions during connection, health validation and assigning network access*



1.) Determine the applicable rule set

First of all, the NG Network Access Client determines in which context it is started and how it connects to the Access Control Service. The following three contexts are available:

- **Local Machine context**
  The local machine context is available in case no user has logged in. This applies during the startup of a Windows computer as well as after user logout.
  Since the Windows system behaves different between "Current User" and "Local Machine" context it is necessary to handle the local machine context separately. For example, no popups are allowed if no user is logged in. Certificate based authentication (see below) is available for both, Local Machine and Current User Authentication, but different Microsoft certificate stores are available to get the certificates from. Of course, a Local Machine certificate must not be password protected since dialogue boxes to request the password will not be available.
- **Current User context**
  As soon as a user has logged in successfully, the client switches to the current user context. Now additional information like the user name and the password (or kerberos ticket in case of NTLM authentication) can be used to perform identity matching.
  Since the user context allows to open client windows and popups, the client can notify the user about the current health state or request additional information (for example Basic Authentication: popup requests username and password).
- **VPN context**
  The VPN context is an extension of the current user context mentioned above. The client is able to determine if a Barracuda NG VPN connection was initiated as well as if the VPN server has Access Control Service capabilities. If the client mode is VPN all possibilities available in User mode are available as well. Additionally, an online and offline rule set can be assigned to the client.

2.) Client connects to Access Control Service

The next step for the client is to connect to the configured Access Control Service. The IP address of the Access Control Service is either configured manually (during installation) or is assigned by the DHCP server. The connection is based on TCP and uses port 44000 to communicate between client and server.

Note

The connection is always initiated by the client and never the other way round.

During the handshake, the Access Control Service notifies the client of it's capabilities (for example is NTLM authentication available).

As a response, the client collects all available system information and sends this information back to the Access Control Service together with authentication credentials.

This response contains details about the computer's network (for example IP address, MAC-Address), the computer's operating system (for example OS-Version, hostname, domain name, user and certificates) as well as details about installed health suite, Antivirus, or Antispyware products.

Further policy matching on the Access Control Service depends on the data collected and sent from the client.

3.) Determine Client identity

The Access Control Service has now all information to determine the client's identity. Depending on the client mode (Local Machine, Current User, VPN) the Access Control Server determines the applicable policy rule set, which is then used to perform identity matching.

The available identity information is sequentially matched from top to bottom with the identity conditions of the individual policies. Each policy can be configured to match if all configured identity criteria apply or if only one of the configured criteria applies.

Table 1–2

Matching Criteria	Local Machine	Current User	VPN
Client Connection Type	✓	✓	✓
Current Date/Time	✓	✓	✓
NetBios Domain	-	✓	✓
Group Patterns	-	✓	✓
User [Login Name]	-	✓	✓
Network	✓	✓	✓
OS Version	✓	✓	✓
Hostname	✓	✓	✓
MAC Address	✓	✓	✓
MS Machine SID	✓	✓	✓
x.509 Certificate Conditions	✓	✓	✓

If a match is found, the comparison of the health information sent by the client with the stated health requirements of the policy rule carries on.

Although the Access Control Service rule set bears analogy to a firewall rule set, one of the significant differences is that the handling in case no rule matches can be configured. Configuration of "no rule exception" notifying NG clients even if they can not be identified.

As this should really be treated as an exception, a better way to control clients is to manually apply a catch-all rule at the end of the policy rule set.

1.4 Health Matching

The most complex part of the policy rule matching is the matching of health conditions. This is due to the fact that not only matching of health requirements is done but actions on the client can be performed as well.

An overview of the health matching procedure is available in the flowchart above.

At the beginning of the communication between client and server the health state of the client is "uninitialized". If the quarantine rule set is already available on the client, then the client activates the available quarantine rule set but remains in the state **uninitialized**. This state triggers an immediate connection to the configured Access Control Service as described above.

As soon as the communication between the client and the Access Control service is established and policy matching is performed one of four different health states is assigned.

Usually both, Access Control service and NG VPN client, do have the same health state. The only exception is the state "uninitialized" mentioned above. In this case the Access Control Service is not aware of the existence of the NG client.

1.4.1 Health State "Untrusted"

As soon as the identity match is finished and the client's identity can not be validated, the health state changes to "Untrusted". Untrusted does not necessarily mean that the client may be a guest client but only that the Access Control Service can not determine the client's identity. Nevertheless the configuration parameter ***Access Control Service Trustzone*** > ***Settings*** > ***No Rule Exception*** allows to assign a set of client attributes.

1.4.2 Health State "Probation"

If the health match fails the client is said to be in probation. It still receives a cookie containing the unhealthy assessment as well as the detailed outcome of the health matching procedure. From here on the client software may take appropriate action and try to self-remedy the situation, for example by starting the AV scanner. In any case, the user will be informed of the current state of his or her system by an appropriate message.

After the client has performed the requested actions it reconnects to the Access Control Service again. Should the client be successful to self remedy the situation the Access Control service verifies the health conditions again and changes the client health state to "healthy" if the client complies to the assigned health policy from now on.

Should the client fail to self remedy the situation or does not reconnect in a reasonable amount of time, its status changes to unhealthy and the quarantine rules are enabled.

A client will never be in state "probation" for more than one connect cycle (see flowchart above). If the client does not respond within the configurable "Health Sate Probation time" (***Access Control Service Settings*** > ***System Health-Validator*** > ***General***) the Access Control Service automatically changes the client's health state to "Unhealthy".

1.4.3 Health State "Healthy"

Depending on the configuration the health policy could require an up-to-date Barracuda NG Personal Firewall installed and enabled or a running Antivirus software including up-to-date AV patterns. A list of available Health State requirements is available below.

Should all required criteria match, the client is deemed healthy and receives a signed cookie listing the applicable policy attributes. This signed cookie may be further used to authenticate against external trust zones.

1.4.4 Health State "Unhealthy"

Last but not least a client may not comply to the company's health policy. As described in the section Health State 'Probation' (see 1.4.2 Health State "Probation", page 13) the client will get the possibility to perform actions (either manual or automated) to to fulfil all health requirements before being put into quarantine.

If the client fails during a specific time it's state is changed to "Unhealthy". In other terms the client is put into quarantine. This means that the client enables it's latest quarantine rule set.

On the Barracuda NG Firewall the proper state is propagated to the firewall engine where limited access can therefore be enforced.

Note

Even the quarantine rule set must at least enable the client to connect to the Access Control Service, to the Microsoft active directory, and to the remediation servers. Depending on the company's infrastructure, more connections should be available to restore the client's health state to "Healthy" again.

1.4.5 Health State Requirements

The following list provides an overview of the available Health State requirements. Failing a health state requirement can either trigger automatic "self-remediation" or can require a manual action of the user.

The desired behavior is configurable since some versions of Antivirus- or Antispyware do not fully support auto-remediation. In case of manual action the user is informed about the required actions by the Barracuda NG Access Monitor.

A list of all supported AV and AS engines is available via ***Access Control Service Trustzone > Support Chart*** (see also 2.4.8 Support Chart, page 40).

Beside Barracuda Networks specific information, where health state requirements primarily depend on Antivirus or Antispyware settings, the following requirements can be verified:

- **Service Settings**
  - **Is the installed Barracuda NG Personal Firewall active?**
  - **Is the installed Virus Scanner active?**
  - **Is the installed Spyware Scanner active?**
- **Antivirus Settings**
  - **Which Virus Scanner vendors are allowed?**
  - **Enabled AV Real Time Protection?**
  - **When was the last AV Scan performed?**
  - **When was the AV Engine updated?**
  - **When were the AV Pattern Definitions updated?**
- **Antispyware Settings**
  - **Which Spyware Scanner vendors are allowed?**
  - **Enabled AS Real Time Protection?**
  - **When was the last AS Scan performed?**
  - **When was the AS Engine updated?**
  - **When were the AS Pattern Definitions updated?**
- **Advanced Health State**
  - **Which versions of the health suite are allowed?**
- **Miscellaneous**
  - **Are specific Registry keys set?**
  - **Which Microsoft hotfixes or service packs are present?**

To verify these requirements, each Access Control Service depends on up-to-date information of AV and AS products.

Barracuda Networks provides an online update service that helps Barracuda NG Network Access Client Clients to recognize and activate AV and AS products.

Furthermore the update service provides the information necessary to diagnose the up-to-dateness of the client's signature databases and engine versions..

Note

As a prerequisite, either the Access Control Service (standalone Barracuda NG Firewall) or the CC (for managed Barracuda NG Firewalls) must have access to the internet.

1.5 Endpoint Security Policy Introduction Practices (Analyse, Enforce, Monitor)

For implementing firewalls at formerly unrestricted network transitions like LAN-segments or endpoint firewalls for LAN endpoints, a smooth implementation tactics is widely used.

A widely used but not recommended way is to start with a pass all policy, analysing traffic instead of controlling it, and then introducing rules step-by-step reducing traffic using the pass-all policy, and at last replacing pass-all by block-all. This might be called the AEM-model:

1.) **Analyse**

2.) **Enforce**

3.) **Monitor**

When implementing a firewall at a clear network perimeter like an internal-internet transition it is not advisable to use this model. The rule set should be built according to SAEM:

1.) **Strictly Enforce**

2.) **Analyse**

3.) **Enforce**

4.) **Monitor**

While from a strict security point of view this is also recommended for formerly unrestricted network transitions, many administrators nevertheless use AEM for practical reasons. If, however, you have the chance to already know what should happen at the network point of concern, use as much of this know-how as possible and **do not start with pass-all only**. And if you use AEM, **do not finish with a pass-all rule**.

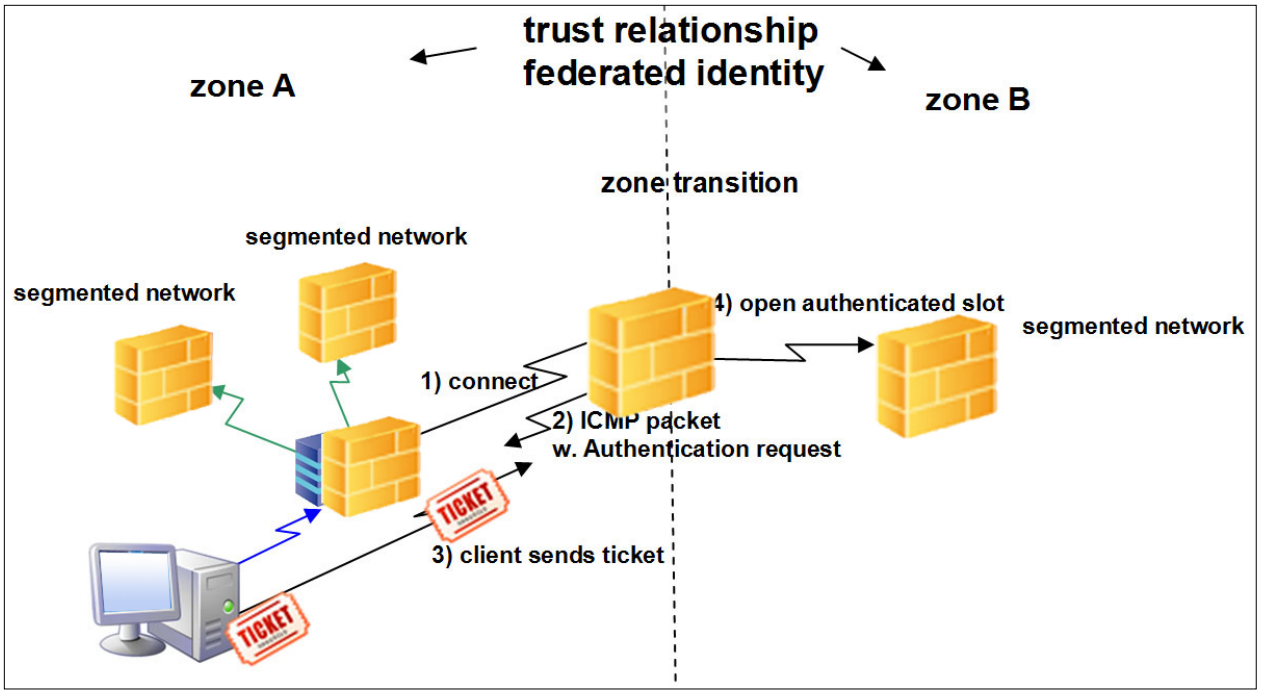
Keep in mind that your rule sets should always mirror your overall abstract security policy for the network point of concern. Using AEM or SAEM is not a matter of technical possibilities but of weighing risk and effort.

1.6 The Border Patrol

Clients often need to access remote trust zones for which restricted access rights and stronger security measures apply. Consequently, the means to assess the suitability of crossing clients to access target trust zones needs to be available. The building block responsible for evaluating trust zone transitions is called border patrol. In short, the border patrol validates the credentials of crossing clients, including authentication and health status data, so that the applicable security measures are correctly met.

An important aspect related to trust zone crossing is the synchronization of authentication data. Basically, trust zones need to have a consistent and up-to-date view of the clients' authentication information that is shared across the whole network. In this line the CC ensures that changes are replicated and synchronized across the various available servers and databases, so that identity federation is achieved.

Fig. 1–3 *Trust Relationships*



It is also relevant to notice that the authentication process is based on the use of ICMP packages. Succinctly, the client submits an access request to the border patrol. The border patrol responses by sending an authentication request through an ICMP package. Upon reception of the ICMP package the client replies with a ticket containing the cookie issued by the remediation service in the trust zone of origin and its corresponding access rights. If health status and permission match the minimum requirements of the target trust zone, the client is granted access. Otherwise, the border patrol denies the request.

Note

If the border patrol denies the request, then no remediation will be available. Access is either granted or fully denied.

Chapter 2
Server Config – Access Control Service

2.1 General

For proper operation, both components of the Barracuda NG Network Access Clients framework, Access Control Service and Baracuda NG Network Access Client that is, depend on up-to-date information regarding AV and AS products.

Barracuda Networks provides an online updating service that helps the Access Control Service verifying the up-to-dateness of the client's signature databases. In addition this information helps the client to recognize and activate AV and AS products.

Barracuda NG Firewall includes an automatic software downloader which periodically connects to the Barracuda Networks website. To reduce the need for permanent internet connection for Barracuda NG Firewalls the Barracuda Networks update service behaves differently on stand-alone-managed boxes and CC-administered boxes. Internet access using an HTTP/HTTPS proxy server is possible.

- ***Stand-alone-managed boxes running a Access Control Service require internet access. For configuration parameters see 2.2.6 General, page 21.***
- ***CC-administered boxes running an Access Control Service get the required files uploaded from the Barracuda NG Control Center. The CC itself requires internet access to secure.phion.com:443.***

2.2 Access Control Service Settings

This section defines the general parameters of the Access Control Service.

2.2.1 System Health Validator

List 2–1 *Access Control Server - Access Control Server Settings - System Health-Validator – section Trustzone (only available on CC)*

Parameter	Description
Name	On a Barracuda NG Control Center, this parameter allows referencing to global trustzone objects. An empty value indicates that the local trustzone configuration (for example, only this Access Control Service should use the configured trustzone) should be used (2.4 Access Control Service Trustzone, page 25).

List 2–2 *Access Control Server - Access Control Server Settings - System Health-Validator – section General*

Parameter	Description
Start System Health-Validator	Setting to **yes** starts the Access Control Server module before VPN health validation.
Health State Validity (min.)	This value restricts validity time of a health state. If the client does not re-evaluate its health state within that period, all assigned “network access rights” will be dropped.
Health State Probation (min.)	This value defines the probation interval of a health validation. If a client does not satisfy the health requirements in an initial health validation step, the client will be set into probation. It will get the special *network access right* “probation” additionally to the rights as it was healthy. If the client doesn’t become healthy within the probation time it will be set to health state “unhealthy” automatically after the probation time was elapsed.
External IPs	This option defines service IP addresses as *external* IP addresses. This information may be used in policy rules for health evaluation to distinguish between *external* and *internal* requests.

List 2–3 *Access Control Server - Access Control Settings - System Health-Validator – section User Authentication*

Parameter	Description
User Authentication Required	If this option is set to ***no*** the client will not re-evaluate its health state when a user logs on. For example, no "current user" health evaluation will take place.
PHIBS Authentication Scheme	The used phibs scheme for basic authentication.
Fallback PHIBS Auth. Scheme	This option is only available if Phibs Authentication Scheme was set to ***MSCHAP***. In this case this scheme is used for authentication if the MS-CHAP authentication fails. The client will display a pop-up requesting username and password.

List 2–4 *Access Control Server - Access Control Server Settings - System Health-Validator – section Local Machine Authentication*

Parameter	Description
Certificate Required	If set to ***yes***, a local machine authentication requires a certificate for a successful local machine authentication. **Caution:** do not forget to set a right Search String for Box Certificates since there is no "default" box certificate, which could be used for authentication. The client needs to know which certificate of the local certificate store should be used for health evaluation.
Search String Type	May be set to either ***Issuer*** or ***Subject***. This setting defines how the Search String for Box Certificates is interpreted.
Search String for Box Certificates	Either a X509 issuer string or a X509 subject string (for example **C=AT, O=Barracuda, OU=*,CN=***). Pattern matching is allowed.

List 2–5 *Access Control Server - Access Control Server Settings - System Health-Validator – section General Authentication*

Parameter	Description
Authentication Root Certificate	The root certificate is used to verify the validity of certificates provided by clients within a local computer health validation process.
Root Cert. Revocation Settings	This section provides configuration settings for certificate revocation. Certificate revocation can be done by using either CRL (LDAP) or OCSP.

List 2–6 *Access Control Server - Access Control Server Settings - System Health-Validator – section Referrals*

Parameter	Description
Remediation Server Location	This option defines where the remediation server can be reached. Select ***This***, if the remediation server is running on the same system as the Access Control Server. In this case ***Start Remediation Server*** must be set to ***yes***. Select ***Other***, if it is running on another system, and specify the remediation server IP addresses in the fields below.
Internal Remediation Server IPs	In this list, define the IP address(es) of the remediation servers that are accessible by clients within the Secure Network.
External Remediation Server IPs	In this list, define the IP address(es) of the remediation servers that are accessible by clients within the Restricted Network.

List 2–6 *Access Control Server - Access Control Server Settings - System Health-Validator – section Referrals*

Parameter	Description
VPN Remediation Service IPs	Define where the Access Control Service remediation service module is reachable for VPN clients. **Note:** This IP address must not be the same IP address as already used as an Internal or External Remediation Service IP address. Example: For the internal Clients the Access Control Service listening socket is on 10.0.8.108 and you want to have also a remediation service for clients which are connected with VPN. • ***Introduce an additional IP address, for example 10.0.8.150 on Virtual Server Layer and insert these two Bind IPs (10.0.8.108 and 10.0.8.150) in the Access Control Service Configuration.*** • ***Now open the Access Control service settings, scroll down to the VPN Remediation Service IPs and select the IP Address 10.0.8.150 from the pull-down menu.***
Sync authentication to Trustzone	Using a Barracuda NG Control Center multiple Access Control Services can reference to the same trustzone. Already validated clients can be propagated to all Access Control Services sharing the same trustzone configuration. This also affects gateway firewall authentication. This parameter is only available on a CC.

2.2.2 Remediation Service

List 2–7 *Access Control Server - Access Control Server Settings - Remediation Server – section General*

Parameter	Description
Start Remediation Service	Setting to ***yes*** starts the Access Control Server remediation service module.
TLS required	Set to ***yes*** will allow unencrypted downloads from the remediation server. This will increase download velocity, but decrease security since personal firewall rule sets are transmitted unencrypted over the network.

2.2.3 Trustzone-Border

List 2–8 *Access Control Server - Access Control Server Settings - Trustzone-Border – section General*

Parameter	Description
Start Border Health-Validator	Starts the Access Control Service module responsible for trustzone border health state evaluation.
Trustzone Border IP	IP address the health validator uses for listening for trustzone border health validations.
Foreign Health Passp. Verification	Add all foreign health passport verification keys whose health passports should be trusted for this border trustzone. The Health state of clients with a signed and trusted health passport is revalidated for this trustzone but their authentication credentials are accepted from the signed cookie.
Allowed Peer Networks	Only peers from listed networks are allowed to perform trustzone border health validations.

2.2.4 802.1X

List 2–9 *Access Control Server - Access Control Server Settings - 802.1X – section 802.1X*

Parameter	Description
Start 802.1X Radius Validator	To use 802.1X port authentication configure your 802.1X capable switch to use a RADIUS server with this servers server IP address. Then set this parameter to ***Yes***.
Log Authentications	Log every authentication request, for debugging purposes. (parameter is only visible in Advanced View mode)

List 2–9 *Access Control Server - Access Control Server Settings - 802.1X – section 802.1X*

Parameter	Description
Debug Log	Enable debugging log here. A service restart is required. (parameter is only visible in Advanced View mode)

List 2–10 *Access Control Server - Access Control Server Settings - 802.1X – section Radius Clients*

Parameter	Description
NAS identifiers	Network access servers (NAS alias switch) which are allowed to access the RADIUS server. Parameter description see list 2–11.

List 2–11 *NAS identifiers – section Radius Client Configuration*

Parameter	Description
IP Address	Client's IP address or subnet address.
Secret	RADIUS secret for the client.
Short Name	Client's short name.

List 2–12 *Access Control Server - Access Control Server Settings - 802.1X – section Radius Proxy*

Parameter	Description
Radius Proxy Dest. Servers	RADIUS destination servers where external requests should be proxied to. Parameter description see list 2–13.

List 2–13 *Radius Proxy Dest. Servers – section Radius Proxy Dest. Servers*

Parameter	Description
Realm	Leave empty for a default realm.
Dest. IP Address	Destination RADIUS server.
Dest. Port Auth.	Destination server's port for authentication.
Dest. Port Acct.	Destination server's port for accounting.
Dest. Secret	Destinations server's secret.

List 2–14 *Access Control Server - Access Control Server Settings - 802.1X – section Advanced*

Parameter	Description
Radius One Time Pwd Lifetime (s)	Cache the old password as one-time-password for <n> seconds. (only visible in Advanced View)

2.2.5 Advanced

List 2–15 *Access Control Server - Access Control Server Settings - Advanced – section General*

Parameter	Description
Log Level	This option defines the verbosity of log file output. Usually it should be set to 0 (that is "no debug output").
Number of used Threads	Number of used worker threads for health validation and remediation. The default value is 5. This should meet the requirements in most of the cases. Increasing this value leads to a more reactive server, but also increases the load on the system.
Keep Access Cache Entries (d)	Amount of days for wich access cache entries generated by activities traversing the Access Control Server should be deleted.

List 2–15 *Access Control Server - Access Control Server Settings - Advanced – section General*

Parameter	Description
Sync Access Cache to CC	By enabling this parameter, the access cache entries of this Access Control Service are synced to the Barracuda NG Control Center. Thus a consolidated health status of multiple Access Control Services will be available. Additionally the appropriate Barracuda NG Network Access Client service must be introduced on the CC. Use with care in case of limited bandwidth as the synchronisation consumes additional bandwidth. The parameter is only available in conjunction with a Barracuda NG Control Center.

List 2–16 *Access Control Server - Access Control Server Settings - Advanced – section TLS/SSL*

Parameter	Description
TLS/SSL Certificate	The X.509 certificate which is used with TLS.
TLS/SSL Private Key	Corresponding RSA private key which is used with TLS.

2.2.6 General

List 2–17 *Access Control Server - Access Control Server Settings - General – section Time Settings*

Parameter	Description
Download Interval	Specifies the download interval in minutes.

List 2–18 *Access Control Server - Access Control Server Settings - General – section Proxy Settings*

Parameter	Description
Use Proxy	Enables or disables usage of an HTTP/HTTPS proxy.
Proxy Host	IP address or hostname of the proxy server.
Proxy Server Port	Proxy server port.
Proxy User	If the HTTP proxy requires authentication, provide a valid username here.
Proxy Password	If the HTTP proxy requires authentication, provide a valid password here.

List 2–19 *Access Control Server - Access Control Server Settings - General – section Logging*

Parameter	Description
Log Level	Higher values provide more detailed log information.

2.3 Access Control Objects

Policy rule sets can reference to so-called **Access Control Objects**.

Access Control Objects are attributes which are assigned to the client according to the policies configured in the Access Control Service Trustzone.

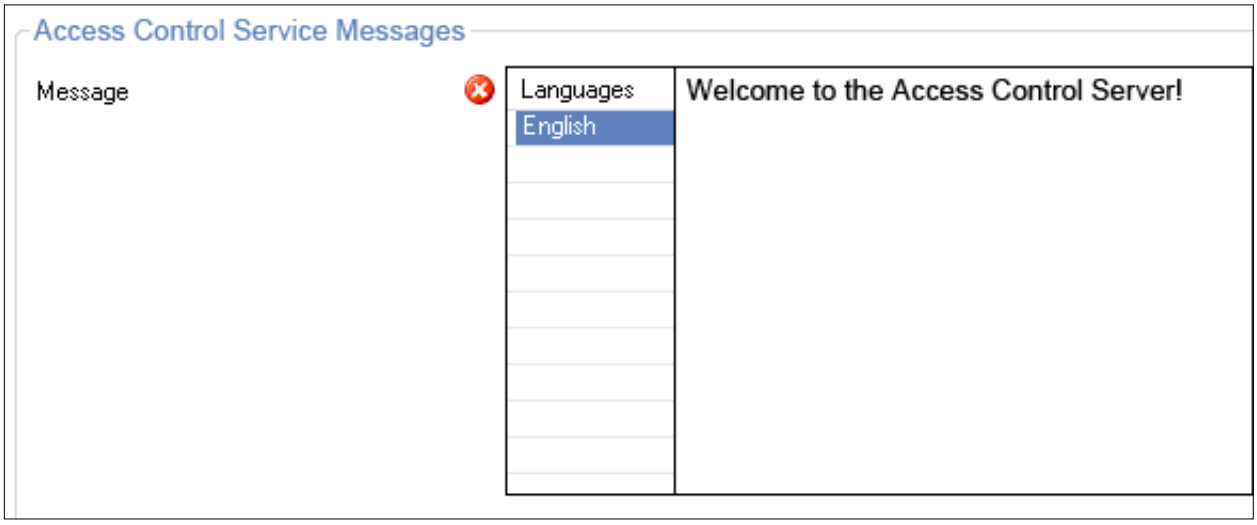
For those already familiar with Barracuda NG VPN, the Access Control Objects are similar to the objects available for Client to Site VPN.

Fig. 2–1 *Access Control Objects – Configuration tree - Access Control Objects*

- **Welcome Messages**

  can be used to display customized messages to welcome end-users to the corporate network, inform them about security policies, or display administrator contact details. For each policy rule may a different "welcome" message be displayed to individual groups of users. In addition, "welcome" messages may be used to display localized messages. Each message is assigned to a language. According to the client's language settings the localized message is displayed. The client will display the English language message as fallback.

Fig. 2–2 *Access Control Objects – Access Control Service Messages*

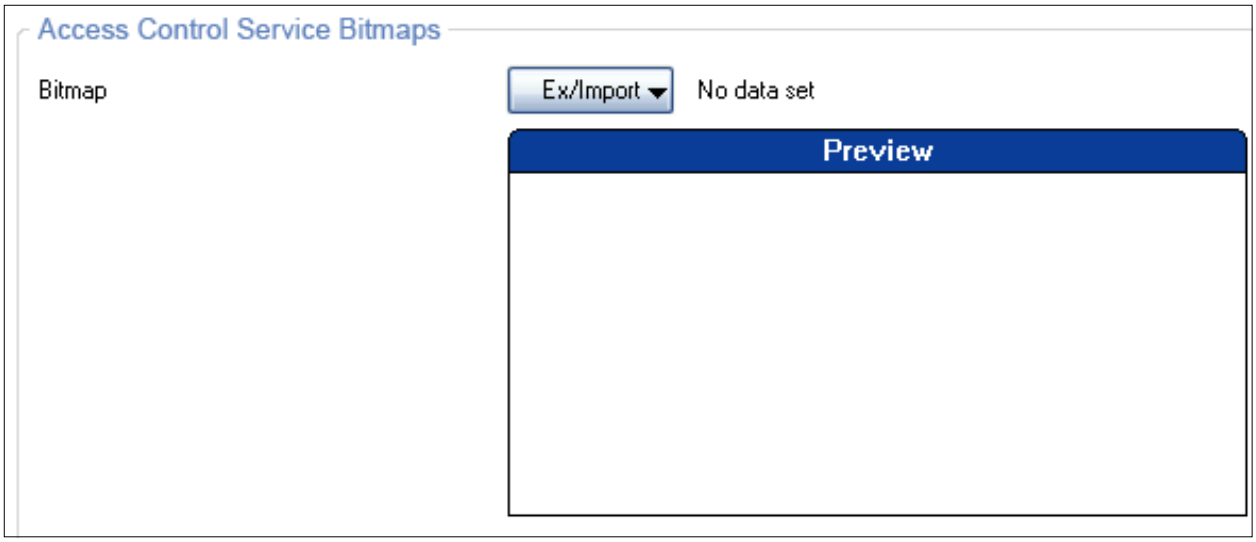


- **Pictures**

  assigned to clients are usually small bitmaps displaying the company's logo. Sometimes they are also used to notify the users about special events.

Assigned pictures are displayed in the client after successfully connecting to the Access Control Service.

Fig. 2–3 *Access Control Objects – Access Control Service Bitmaps*



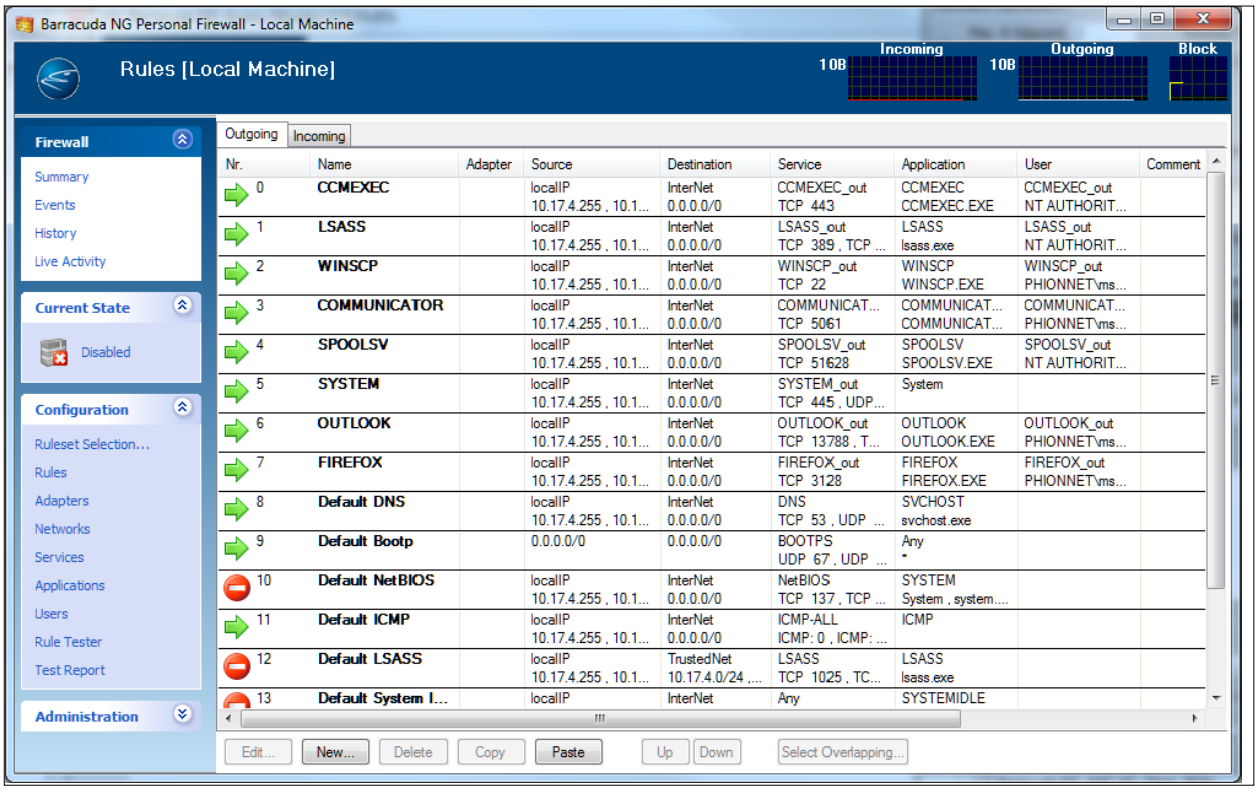
Note

Keep the size of your picture small since the picture will be transferred to all clients. Pictures larger than 167x90 pixels are scaled down on the Barracuda NG NAC anyway.

- **Personal Firewall Rules**

The details of a Barracuda NG Personal Firewall rule set is explained in Server Config – Personal Firewall Rules, page 41.

Fig. 2–4 *Access Control Objects – Firewall Rule Object*



- **Registry Check Objects**

  These objects allow an administrator to define registry checks to be performed on the client. This allows to validate registry keys and values just like taking action in case of failed validation. Available actions are "***Repair***", "***Notify***", or "***Fail***". In case of action type "***Fail***" the Access Control Service health validation will fail if the specified registry keys are not set appropriately.

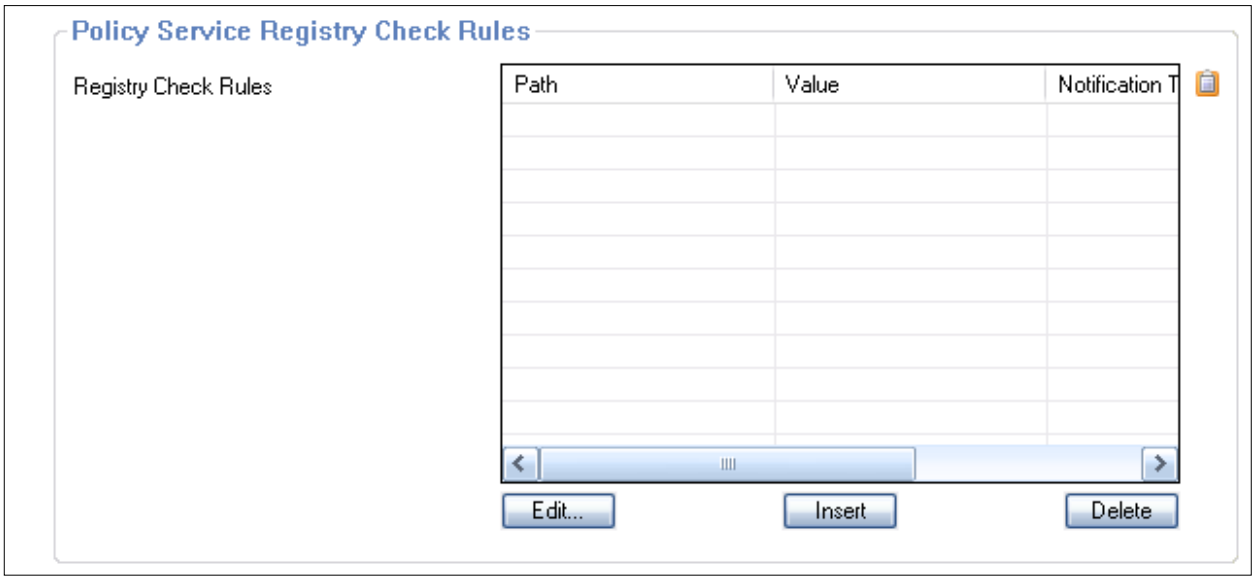
  "***Notify***" generates appropriate log messages on the Barracuda NG Firewall.

Note

Registry "key" changes (for example, introduction of a new registry key) are only done for local machine authentication. Thus, users needs to log off or reboot to activate these changes.

Registry values may also be verified and changed for user authentication.

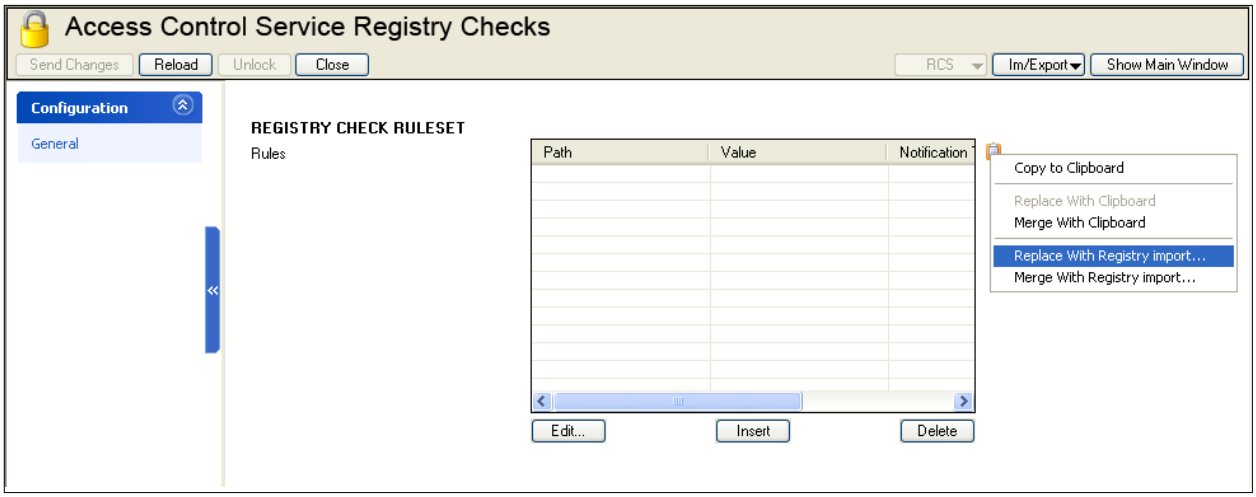
Fig. 2–5 *Access Control Objects – Access Control Service Registry Check Rules*



Import of a registry file:

Click (clipboard), import the adequate registry file.

Fig. 2–6 *Access Control Objects – Import registry file*



Note

Access Control Objects provide an hierarchical override mechanism. Objects on cluster level sharing the same name as global or range objects override the global definition(s). This mechanism works like the one using global firewall objects for the Barracuda NG Firewall.

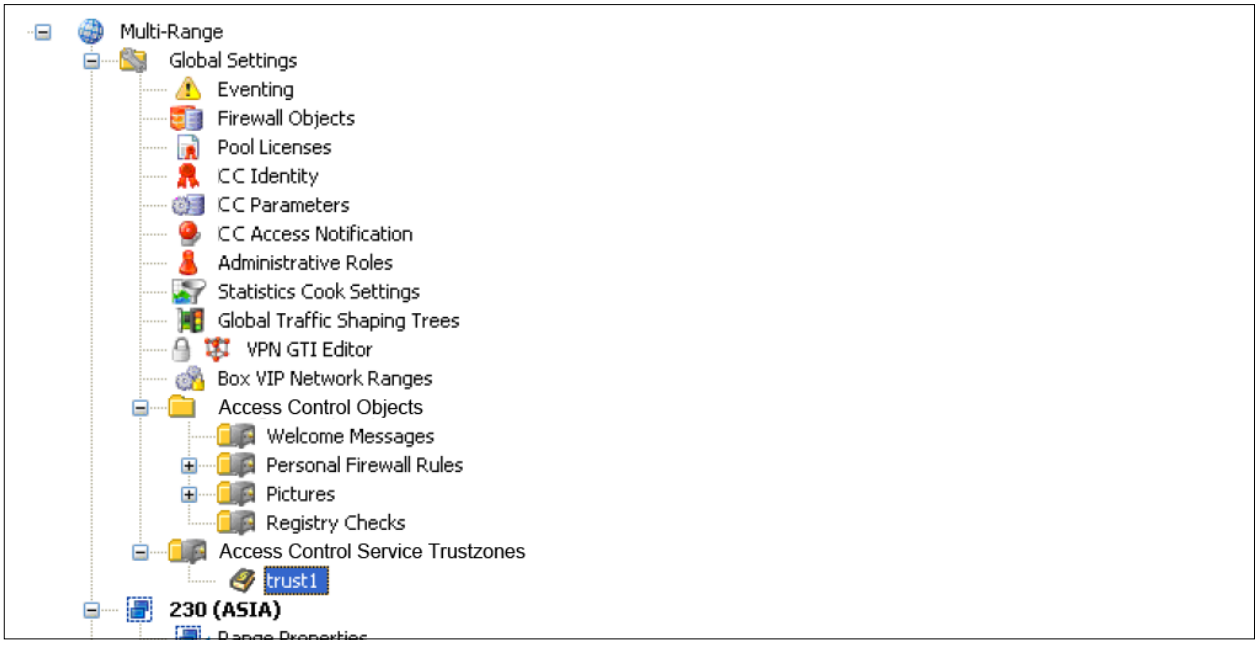
2.4 Access Control Service Trustzone

Each Access Control Service belongs to a so-called trustzone. To enable a company to enforce their security policies across multiple Barracuda NG Firewalls the Barracuda NG Control Center provides Access Control Service Trustzones as global objects. This advanced feature allows all Access Control Services within the same trust zone to share the same set of security policies. In addition they share a signing key, so that a mutual trust relationship can be established.

On stand-alone Barracuda NG Firewalls, configuration of the trustzone is located in the configuration node ***Virtual Servers*** > ***<servername>*** > ***Assigned Services*** > ***<servicename> (Access Control Service)*** > ***Access Control Service Trustzones***.

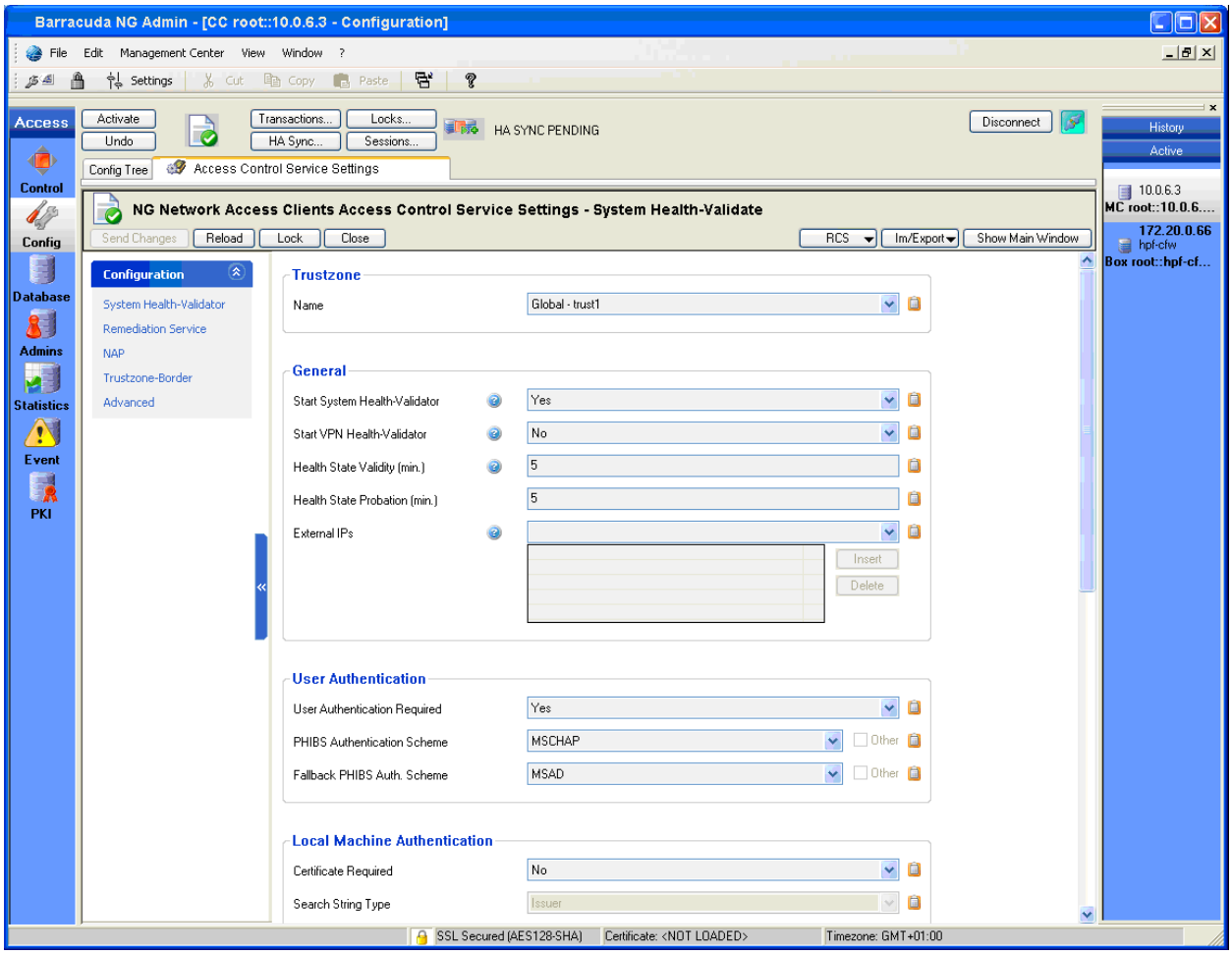
The Barracuda NG Control Center provides Access Control Service Trustzones either within the ***Global Settings*** directory or specifically as Range Settings or Cluster Settings. As usual these objects permit access only to administrators with appropriate administrative scope and appropriate permission.

Fig. 2–7 *Access Control Service Trustzone - Configuration tree*



The pre-defined **Access Control Service Trustzones** can be referenced within the configuration dialogue ***Virtual Servers*** > <*servername*> > ***Assigned Services*** > <*servicename*> ***(ACS)*** › ***Access Control Service Settings*** > ***System Health-Validator*** view > ***Trustzone*** section.

Fig. 2–8 *Access Control Service Trustzone - Configuration dialogue*



The Barracuda NG Control Center automatically links the Trustzone to the appropriate global / range / cluster object.

As mentioned in the introduction above, each trustzone contains three policy rule sets. There is a "local machine" policy rule set that is used to determine a policy for a connecting machine if no user is currently logged in. As soon as user authentication is requested by the connecting client, the "current user" policy rule set is used for policy matching.

Note

User authentication can be skipped by setting the the parameter "Access Control Service Settings" › User Authentication > User Authentication Required to "No". Furthermore, local machine rule sets allow to skip user authentication for a specific policy rule (***Policy Assignments > Exception > User Authentication Required***.

If the connection attempt is mediated by an intermittent VPN Service, then the VPN policy rule set is adopted. More details are available in the introduction above.

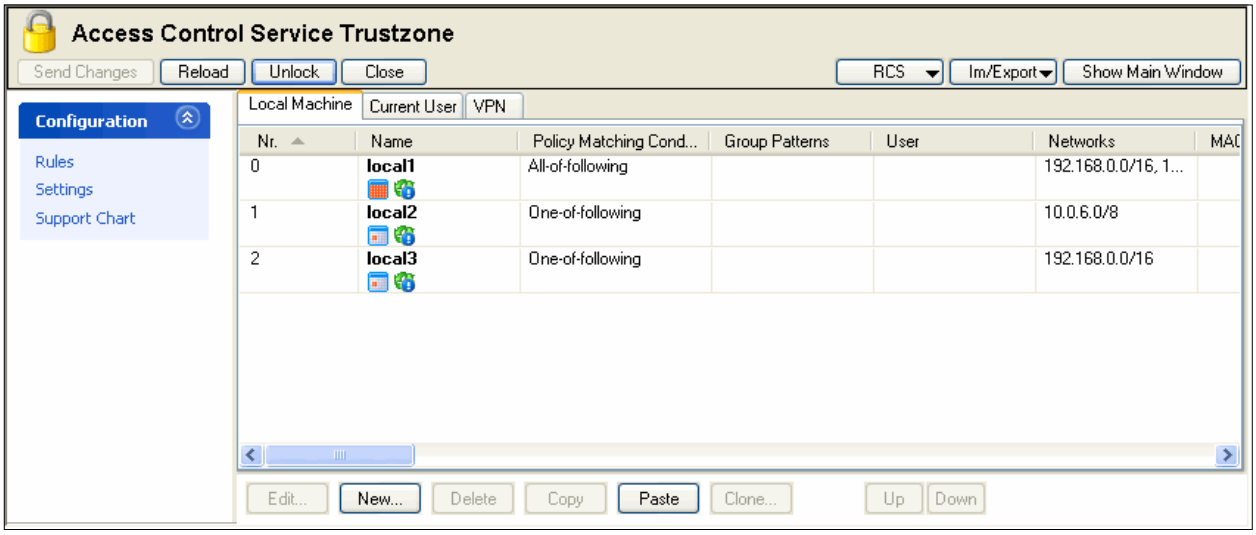
Create an Access Control Server service within ***Config*** > ***Box*** > ***Virtual Servers*** > <*servername*> > ***Assigned Services*** > <*servicename*> ***(ACS)***).

Click ***Access Control Service Trustzone*** to open the configuration dialogue.

2.4.1 Rules

The main window of a Access Control Service Trustzone is split up into a navigation bar on the left and three policy rule sets on the right (1.3 What is a Policy Rule Set?, page 8).

Fig. 2–9 *Access Control Service Trustzone - Rules*



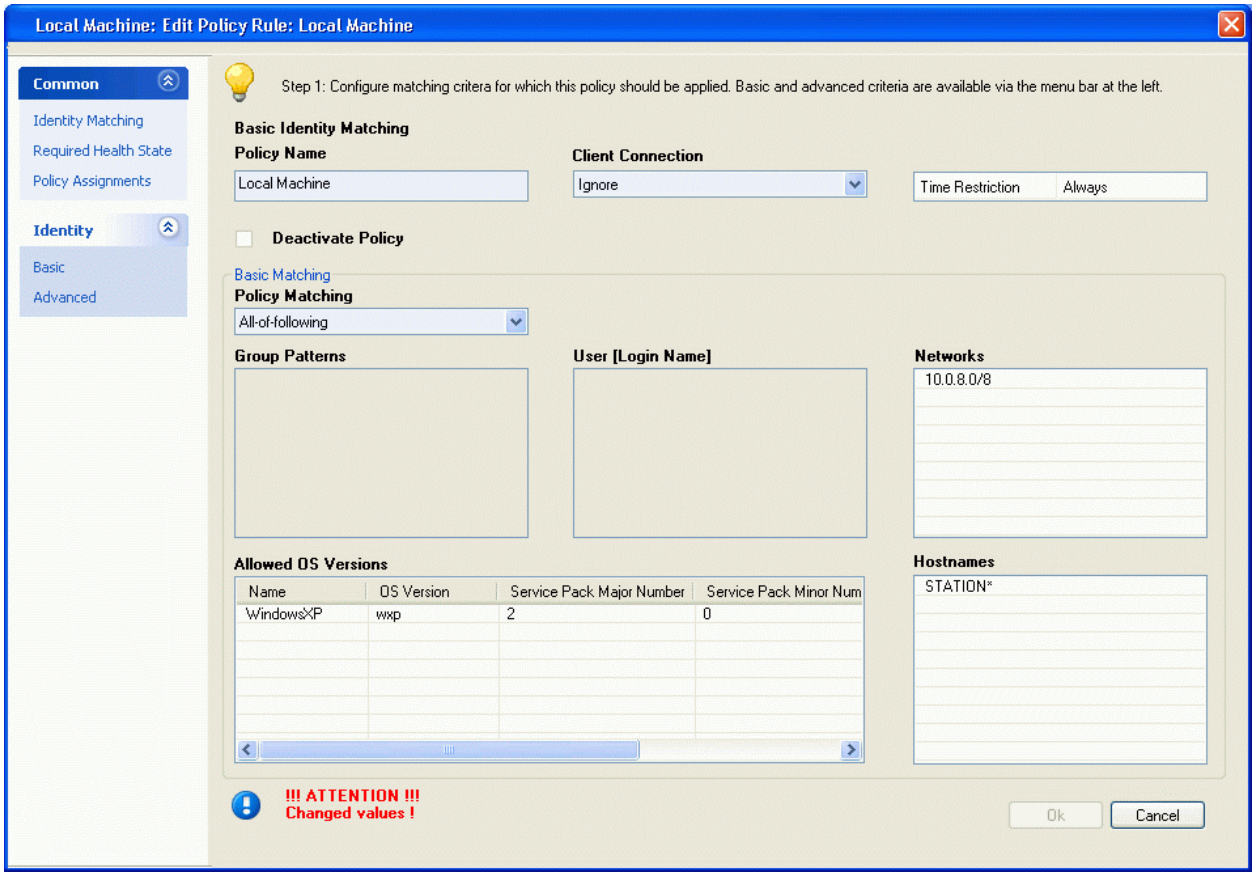
2.4.2 Identity Matching - Basic

The first step when processing a policy rule set (either local machine, current user, or VPN) is to determine the client's identity.

Depending on the value of the parameter Basic Matching > Policy Matching either all or one of the specified criteria must match to determine the client's identity.

If the identity match fails, the next rule is taken into account.

Fig. 2–10 *Access Control Service Trustzone - Rules - Identity Matching Basic*



List 2–20 *Access Control Service Trustzone - Rules - Identity Matching Basic – section Basic Identity Matching*

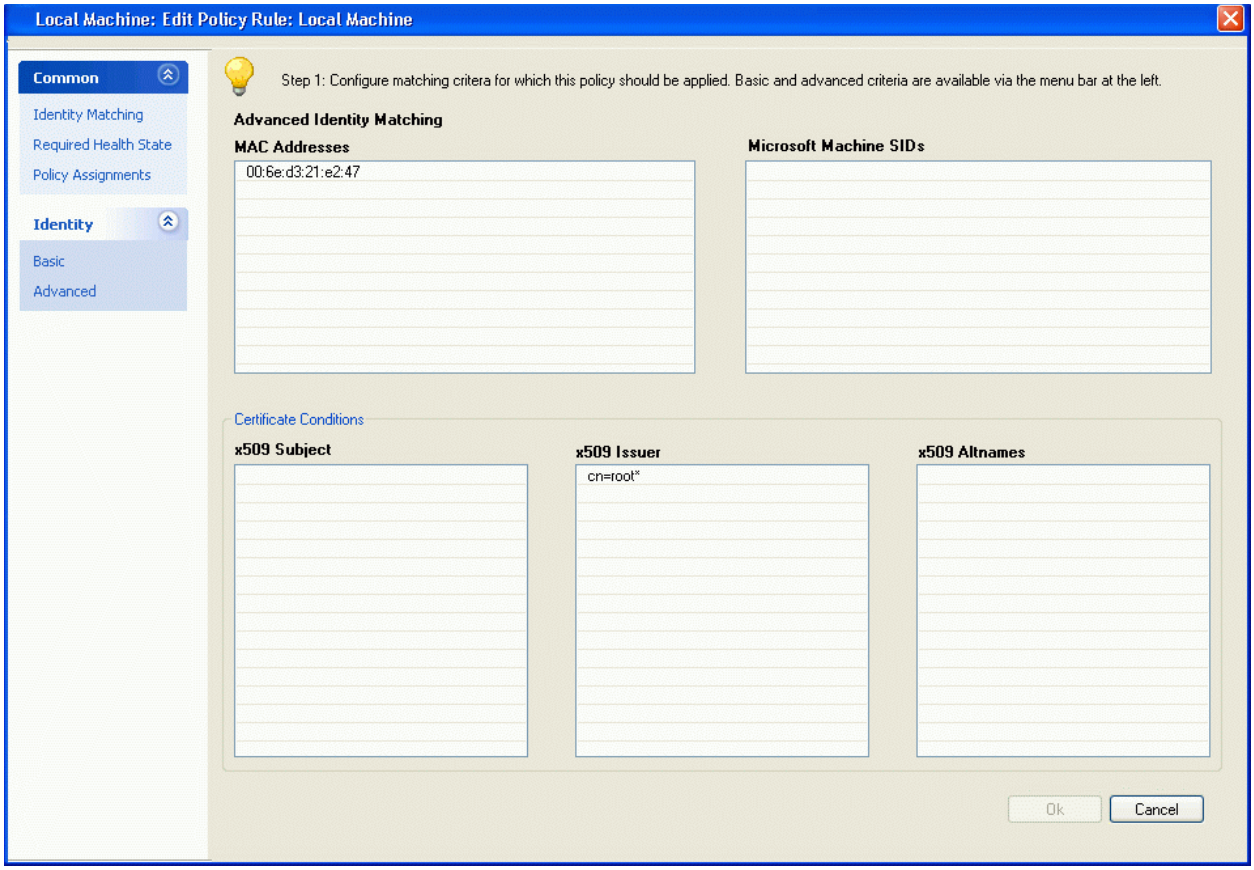
Parameter	Description
Policy Name	The name of the policy. This name is visible in the log file and in the access cache.
Deactivate Policy	Selecting the checkbox disables the configured policy.
Client Connection	• ***External*** • ***Ignore*** • ***Internal*** Set to ***External*** effects that this policy rule is ignored for internal connection (connections to an IP address which is not defined in External IPs, see above). Set to ***Internal*** effects that this policy rule is ignored for external connections (connection to an IP address which is defined in External IPs, see above). Set to ***Ignore*** means that the policy rule is neither ignored for internal nor external connections.
Time Restriction	Each policy rule can be assigned with a date and time restriction. The date restriction consists on a Start Date and an End Date. Out of that time period this policy rule will be ignored. The granularity of the time restriction is 1 hour on a weekly base. A rule is allowed at all times by default, that is all checkboxes in the ***Time Interval*** window are cleared. Selecting a checkbox denies a rule for the given time. Click to configure allowed and disallowed time intervals simultaneously. Click to clear selected checkboxes. Click to to configure disallowed time intervals. Select ***Continue if mismatch*** to proceed the health evaluation within the policy rule set with the next rule (default). Select ***Block if mismatch*** to stop the health evaluation process and set the client to "unhealthy" immediately.

List 2–21 *Access Control Service Trustzone - Rules - Identity Matching Basic – section Basic Matching*

Parameter	Description
Policy Matching	• ***All-of-following*** • ***One-of-following*** Set this option to ***All-of-following*** if all of the identity matching parameters (basic and advanced), except the empty ones, must match for a successful identity verification. If just one field does not match, the identity is not verified successfully within this policy rule and the health match process will proceed with the next policy rule in the policy rule set. Set this option to ***One-of-following*** effects that the identify verification succeeds if just one field matches. Fields left empty will be ignored in both cases. **Note:** All string comparison is done case insensitive. For all of the following identify matching fields applies that just one value of each field must match, for example if more than one group patterns are defined, it is necessary that at least one user group must match at least on defined group pattern.
Group Patterns	Enter group patterns here. At least one user group must match at least one of these patterns for successful identity verification. Be aware of using the right syntax for the group patterns: for example, MS Active Directory groups have be be entered as distinguished name (for example CN=group-*, OU=my-unit,CD=mycompany,DC=at).
Net Bios Domain	Enter the name of a NetBIOS Domain to match only users of a specific Domain. **Note:** Only available for "Current User" and "VPN" rule set
User [Login Name]	Enter user name patterns here. A user name is the login name (without leading "DOMAIN\").
Networks	Enter networks here. The users peer address must be part of at least one of these networks.
Allowed OS Versions	• ***Name*** • ***OS Versions*** • ***Service Pack Major Number*** • ***Service Pack Minor Number*** • ***Minimum Build Number*** • ***Policy on OS*** Define allowed or explicitly denied client OS version here. The ***OS Versions*** parameter needs to be one of the listed Microsoft Windows Versions. The ***Service Pack Major Number*** and the ***Service Pack Minor Number*** are the service pack numbers of the client OS. The ***Minimum Build Number*** needs to be the OS build number and is checked only, if Policy on OS was set to ***This-One-Or-Newer***. Possible values for Policy on OS field are • ***Exact-This-One*** the client OS must match OS Version, Service Pack Major Number, and Service Pack Minor Number. • ***Explicit-Deny*** If the clients OS matches OS Versions, Service Pack Major Number, and Service Pack Minor Number, then the current policy rule will be ignored for the current match, and health evaluation process proceeds with the next policy rule in the policy rule set. • ***This-One-Or-Newer*** In this case, the client OS must be identically equal to OS version. The client OS service pack major and minor number and its build number need to be equal or greater than those defined here.
Hostnames	Enter hostnames here. Patterns may be used.

2.4.3 Identity Matching - Advanced

Fig. 2–11 *Access Control Service Trustzone - Rules - Identity Matching Advanced*



List 2–22 *Access Control Service Trustzone - Rules - Identity Matching Advanced – section Advanced Identity Matching*

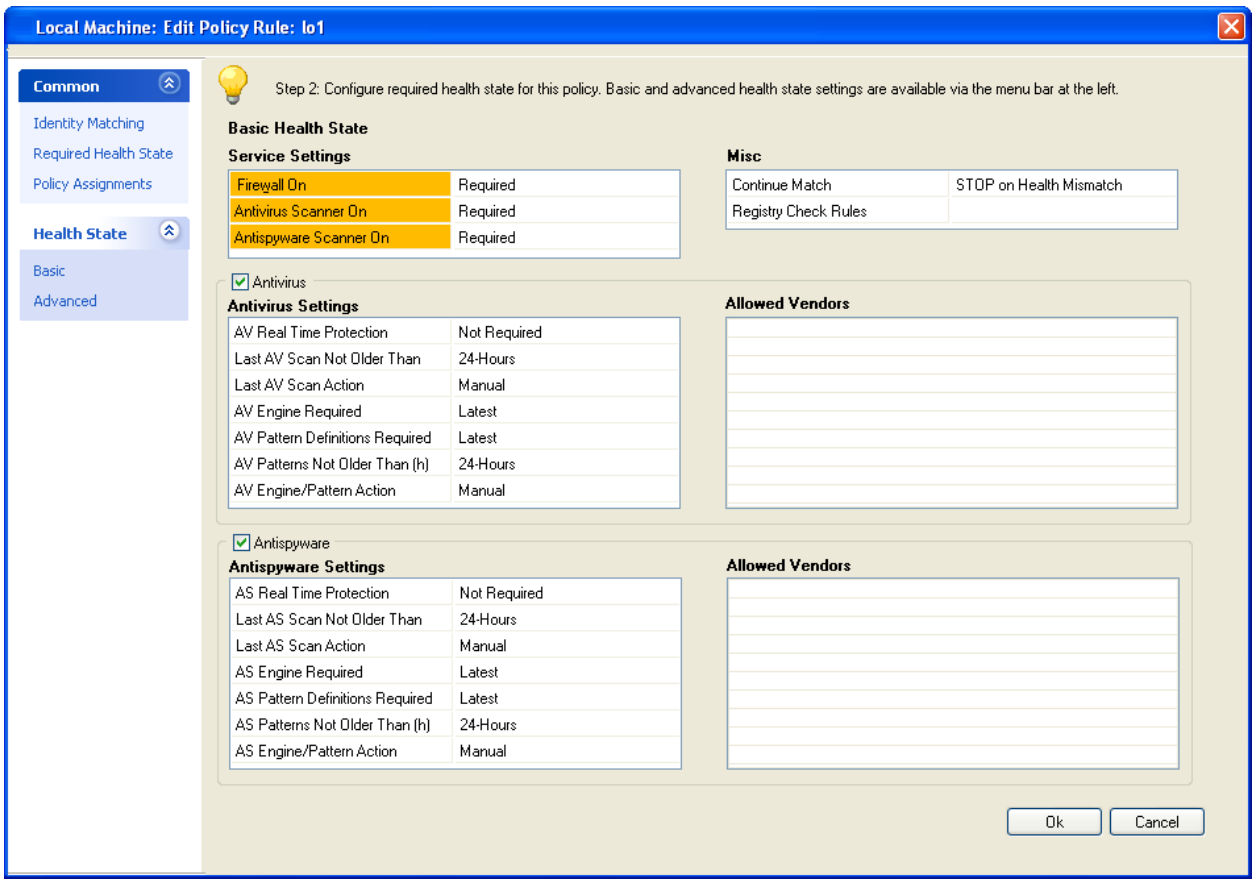
Parameter	Description
MAC Addresses	Enter MAC addresses here. Patterns may be used.
Microsoft Machine SIDs	Enter Microsoft Machine SIDs here. A SID is a - from the Microsoft OS generated - world wide unique machine identifier. The SID is visualized in the Access Control Server's access cache. Patterns may be used.

List 2–23 *Access Control Service Trustzone - Rules - Identity Matching Advanced – section Certificate Conditions*

Parameter	Description
x509 Subject	Enter X.509 subject name patterns here (for example, CN=name-*, O=my-company). The X.509 subject of the clients authentication certificate must match at least one of these patterns. **Note:** Certificate authentication is only possible in Local machine and basic user authentication.
x509 Issuer	Enter X.509 issuer name patterns here (e.g CN=name-*, O=my-company). The subject of the issuer of the clients certificate must match at least one of these patterns. **Note:** Certificate authentication is only possible in Local machine and basic user authentication.
x509 Altnames	Enter X.509 alternative name patterns here (IP:10.0.10.*). The subject alternative name of the clients authentication certificate must match at least one of these patterns. **Note:** Certificate authentication is only possible in Local machine and basic user authentication. The subject alternative name is prepended by its type (for example, "email:" or "IP:")

2.4.4 Required Health State - Basic

Fig. 2–12 *Access Control Service Trustzone - Rules - Required Health State Basic*



After successful verification of the client's identity, this configuration entity is used for determining the client's health state.

Some of the parameters provide the following options:

- ***Not required***

  The result of the health evaluation doesn't depend on this parameter.

- ***Required***

  If a ***Required*** parameter does not match, the user is notified and manual action is required. Furthermore the client's health state changes to "Probation".

- ***Required <Auto-Remediation>***

  Notifies the client too, but tries to automatically execute the necessary actions to fulfill the health requirements. During this period the client's health state changes to "Probation".

In case of third-party products (for example Virus scanner), Auto-Remediation may not work with all available engine versions. As fallback, the client always requests manual action.

List 2–24 *Access Control Service Trustzone - Rules - Required Health State Basic – section Service Settings*

Parameter	Description
NG Personal Firewall On	• ***Required*** • ***Required <Auto-Remediation>*** • ***Not Required (default)*** Set to ***Required*** if a client must have the personal firewall up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the firewall.
Antivirus Scanner On	• ***Required*** • ***Required <Auto-Remediation>*** • ***Not Required (default)*** Set to ***Required*** if a client must have the virus scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the virus scanner. **Note:** The option ***Required*** only takes effect when the checkbox ***Antivirus*** is selected (figure 2-12, page 31).
Antispyware Scanner On	• ***Required*** • ***Required <Auto-Remediation>*** • ***Not Required (default)*** Set to ***Required*** if a client must have the anti spyware scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the anti spyware scanner. **Note:** The option ***Required*** only takes effect when the checkbox ***Antispyware*** is selected (figure 2-12, page 31).

List 2–25 *Access Control Service Trustzone - Rules - Required Health State Basic – section Misc*

Parameter	Description
Continue Match	• ***STOP on Health Mismatch (default)*** • ***Continue on Health Mismatch*** Set this to ***Continue on Health Mismatch*** if the health validation should be continued with the next policy rule in the policy rule set, if the health-evaluation in the current rule gave the result that the client is not healthy. Set this to ***STOP on Health Mismatch*** if health validation should NOT continue with the next policy rule in the policy rule set if the client is not healthy. In this case the Policy Attributes of the current rule are assigned to the client, and the client is advised to heal itself.
Registry Check Rules	Here choose one of the ***Registry Check*** objects. The client's registry entries must match those of the selected registry check object to be healthy.

List 2–26 *Access Control Service Trustzone - Rules - Required Health State Basic*

Parameter	Description
Antivirus	Select this checkbox to enable the Antivirus settings parameters. Parameter description see list 2–27. (Default: not selected)
Antispyware	Select this checkbox to enable the Antispyware settings parameters. Parameter description see list 2–28. (Default: not selected)

List 2–27 *Access Control Service Trustzone - Rules - Required Health State Basic – section Antivirus*

Parameter	Description
AV Real Time Protection	• ***Required*** • ***Required <Auto-Remediation>*** • ***Not Required (default)*** Set to ***Required*** if a client must have enabled the real time protection of the anti virus scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real time protection of the virus scanner.
Last AV Scan Not Older Than	• ***Ignore*** • ***6-Hours > 1-Month*** • ***24-Hours (default)*** Set to a value unequal ***Ignore*** to ensure that the client's last full virus scan is not older than <value> to be healthy. If the client does not meet this requirement, it will be advised to perform a full anti virus scan.

List 2–27 *Access Control Service Trustzone - Rules - Required Health State Basic – section Antivirus*

Parameter	Description
Last AV Scan Action	• ***Manual*** • ***Auto Remediation*** Depending on this parameter either the user gets informed to manually perform a full AV system scan or that the client tries to execute a full system scan automatically.
AV Engine Required	• ***Ignore*** • ***Latest (default)*** • ***Previous*** • ***Last-2*** Set to ***Ignore*** if the clients' Virus Scanner version should not be checked. Set to ***Latest*** if the client must not have an older version of the Virus Scanner to be healthy. Set to ***Previous*** if the latest and the previous version of the Virus Scanner are allowed to be healthy. Set to ***Last-2*** if the latest, the previous and the second last Virus Scanner are allowed to be healthy. If the client does not meet the chosen requirement, it will be advised to perform a anti virus engine update.
AV Patterns Not Older Than (h)	• ***Ignore*** • ***6-Hours > 1-Month*** • ***24-Hours (default)*** Set this option to a value unequal ***Ignore*** to require anti virus patterns to be not older than <value> to be healthy. This option will be ignored if the latest anti virus pattern is older than <value>. For instance if this option is set to 6-Hours but the latest anti virus pattern was released 8 hours ago, the client will be set to state unhealthy due this option. Release cycles of anti virus patterns depend on the anti virus vendor.
AV Engine/Pattern Action	• ***Manual*** • ***Auto Remediation*** Depending on this parameter either the user gets informed to manually update the AV system or the client tries to trigger AV updates automatically.
Allowed Vendors	Chose one or more of the list of anti virus vendors to enforce a specific anti virus vendor product needs to be installed on the client. Anti virus products which are not listed here are ignored in the health validation process. This option is helpful especially to exclude some on the clients installed anti virus products from the health validation process. The list of available anti virus vendors is created dynamically.

List 2–28 *Access Control Service Trustzone - Rules - Required Health State Basic – section Antispyware*

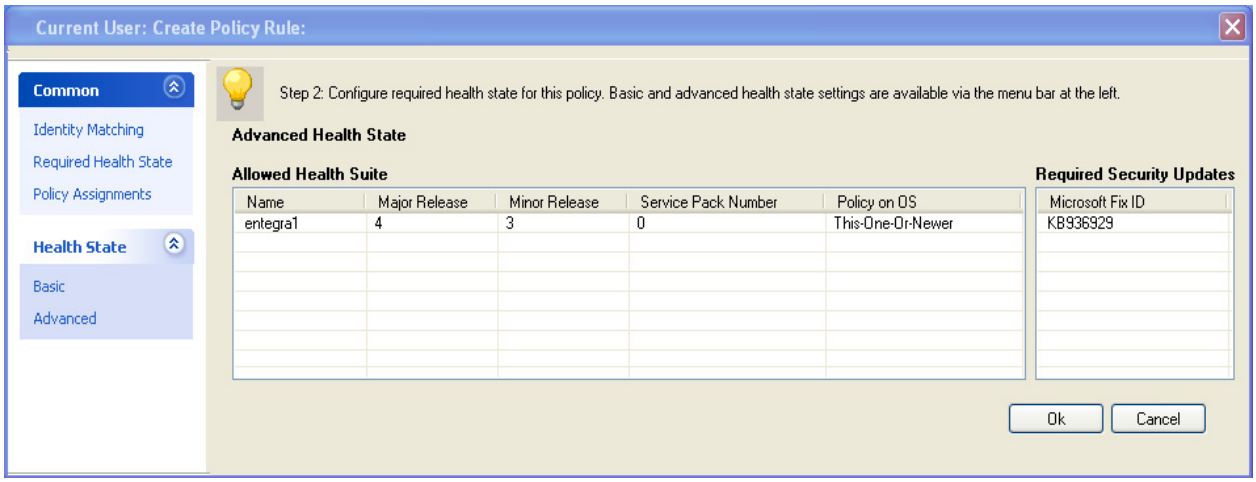
Parameter	Description
AS Real Time Protection	• ***Required*** • ***Required <Auto-Remediation>*** • ***Not Required (default)*** Set to ***Required*** if a client must have enabled the real time protection of the anti spyware scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real time protection of the anti spyware scanner.
Last AS Scan Action	• ***Manual*** • ***Auto Remediation*** Depending on this parameter either the user gets informed to manually perform a full AS scan or the client tries to execute a full system scan automatically.
Last AS Scan Not Older Than	• ***Ignore*** • ***6-Hours > 1-Month*** • ***24-Hours (default)*** Set to a value unequal ***Ignore*** to ensure that the clients last full anti spyware scan is not older than <value> to be healthy. If the client does not meet this requirement, it will be advised to perform a full anti spyware scan.
AS Engine Required	• ***Ignore*** • ***Latest (default)*** • ***Previous*** • ***Last-2*** Set to ***Ignore*** if the clients anti spyware engine version should not be checked. Set to ***Latest*** if the client must not have an older version of the anti spyware scanner engine to be healthy. Set to ***Previous*** if the latest and the previous version of the anti spyware scanner engine are allowed to be healthy. Set to ***Last-2*** if the latest, the previous and the second last anti spyware scanner engines are allowed to be healthy. If the client does not meet this requirement, it will be advised to perform an anti spyware engine update.

List 2–28 *Access Control Service Trustzone - Rules - Required Health State Basic – section Antispyware*

Parameter	Description
AS Pattern Definitions Required	• ***Ignore*** • ***Latest (default)*** • ***Previous*** • ***Last-2*** Set to ***Ignore*** if the clients anti spyware pattern definitions should not be checked. Be aware of the fact that in this case the client may be healthy without having any anti spyware patterns installed. Set to ***Latest*** if the client's anti spyware patterns must be up to date to be healthy. Set to ***Previous*** if the client's anti spyware patterns must either be up to date or of the previous version to be healthy. Set to ***Last-2*** if the client's anti spyware patterns must be up to date, the previous or the second last to be healthy. If the client does not meet this requirement, it will be advised to perform an anti spyware pattern definition update.
AS Patterns Not Older Than (h)	• ***Ignore*** • ***6-Hours > 1-Month*** • ***24-Hours (default)*** Set this option to a value unequal ***Ignore*** to require anti spyware patterns to be not older than <value> to be healthy. This option will be ignored if the latest anti spyware pattern is older than <value>. For instance if this option is set to 6-Hours but the latest anti spyware pattern was released 8 hours ago, the client will be set to state unhealthy due this option. Release cycles of anti spyware patterns depend on the anti spyware vendor.
AV Engine/Pattern Action	• ***Manual*** • ***Auto Remediation*** Depending on this parameter either the user gets informed to manually update the AS system or the client tries to trigger an AS update automatically.
Allowed Vendors	Chose one or more of the list of anti spyware vendors to enforce a specific anti spyware vendor product must be installed on the client. Anti spyware products which are not listed here are ignored in the health validation process. This option is helpful especially to exclude some on the clients installed anti spyware products from the health validation process. The list of available anti spyware vendors is created dynamically.

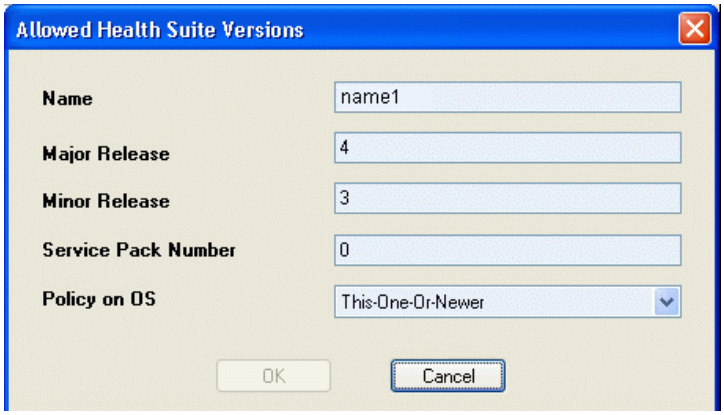
2.4.5 Required Health State - Advanced

Fig. 2–13 *Access Control Service Trustzone - Rules - Required Health State Advanced*



Select ***New*** (context menu) to create a new entry. The configuration dialog provides following entries:

Fig. 2–14 *Access Control Service Trustzone - Rules - Required Health State Advanced - Allowed Health Suite Versions*



List 2–29 *Access Control Service Trustzone - Rules - Required Health State Advanced - Allowed Health Suite Versions*

Parameter	Description
Name	Specify a name. Define allowed or explicitly denied client health suite version.
Major Release	The clients' health suite major number must match Major Release.
Minor Release	The clients' health suite minor number must match Minor Release.
Service Pack Number	The Service Pack Number must be the service pack number of the clients' health suite.
Policy on OS	• ***Exact-This-On*** The clients' health suite version must match all three number values. • ***Explicit-Deny*** If the clients' health suite version matches all three number values then the health state will be set unequal "health" and the clients will be advised to update the health suite. • ***This-One-Or-Newer*** In this case the clients' health suite major version must be identically equal to Major Version. The minor number and the service pack number needs to be equal or greater than those here defined.

Note

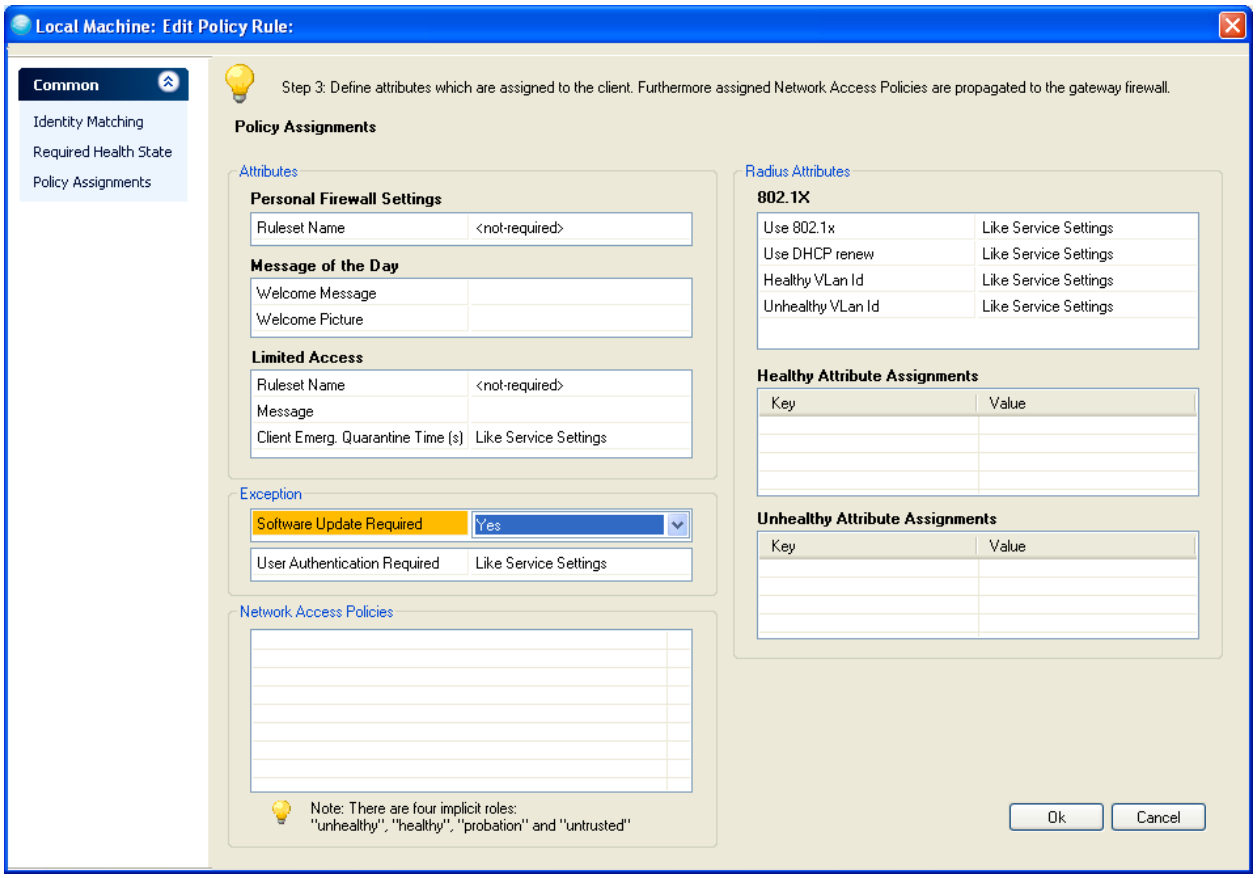
Health suite updates are always performed on an equal major number, for instance a client's health suite version 4.0.2 may be updated to 4.1.0 but not to 5.0.0.

It is also possible to include a check for the currently installed Microsoft hotfixes on the client computer.

- ***Right click into the Required Security Updates field***
- ***Click New... and enter the ID of the Microsoft hotfix.*** *For example:* `KB936929`

2.4.6 Policy Assignments

Fig. 2–15 *Access Control Service Trustzone - Rules - Policy Assignments*



List 2–30 *Access Control Service Trustzone - Rules - Policy Assignments – section Attributes*

Parameter	Description
Personal Firewall Settings	• ***Ruleset Name*** Choose one of the created Personal Firewall Rule objects here. If the client does not already have this rule set installed, the health state will be set to unequal "healthy" and the client will be advised to update the personal firewall rule set from the remediation server.
Message of the Day	Choose one of the created Welcome Message objects here. If the client does not already have this message, it will be advised to get the message from the remediation server.
Limit Access	• ***Ruleset Name*** • ***Message*** • ***Client Emerg. Quarantine Time (s)*** Define the quarantine rule set here. Assignment of "Limited Access" Rule Sets and Messages is only available for the "Local Machine" rule set. **Note:** The quarantine rule set ("Limited Access" rule set) is stored on the local machine. This means that the quarantine rule set can only be updated if the current user logs off or the client is rebooted. If a client changes it's state to "unhealthy" the local machine quarantine rule set is activated.

List 2–31 *Access Control Service Trustzone - Rules - Policy Assignments – section Exceptions*

Parameter	Description
Software Update Required	• ***Yes*** • ***No*** (default) • ***Yes-Even-Major*** Changing this value to ***Yes*** for as the client to automatically perform software updates if a new software version is available on the CC.

List 2–31 *Access Control Service Trustzone - Rules - Policy Assignments – section Exceptions*

Parameter	Description
User Authentication Required	• ***Yes*** • ***No*** • ***Like Service Settings (Default)*** Only available for local machine rule set. If set to "No", user authentication is not performed even if a user logs in.

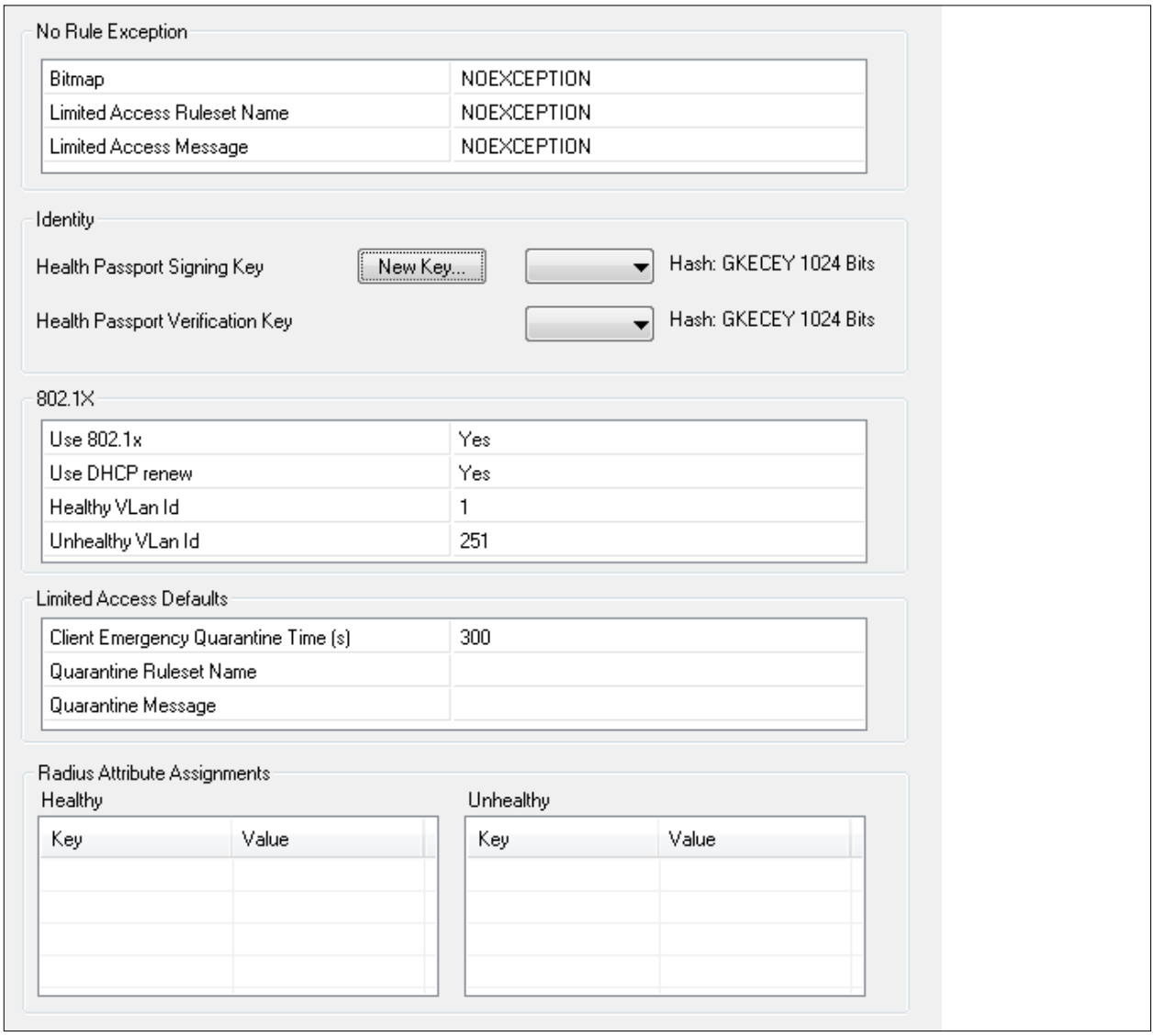
List 2–32 *Access Control Service Trustzone - Rules - Policy Assignments – section Radius Attributes*

Parameter	Description
802.1X	• ***Use 802.1x*** Enforces the usage of 802.1x port based authentication on the client computer. • ***Use DHCP renew*** Whenever the client is relocated into a different VLan this flag enforces the renewal of the client computers IP address. • ***Healthy Vlan Id*** Specifies the VLan, which will assigned to the client computers if they meet the configured health requirements. • ***Unhealthy VLan Id*** Specifies the VLan, which will assigned to the client computers if they do not meet the configured health requirements.
Healthy Attribute Assignments	RADIUS attribute assignments passed to RADIUS server as key value pairs, when the client meets the health requirements.
Unhealthy Attribute Assignments	RADIUS attribute assignments passed to RADIUS server as key value pairs, when the client does not meet the health requirements.

2.4.7 Settings

If no policy rule matched identity for a client or at least one matched, but the Continue Match parameter was set on that/those policy rules, the clients state will be untrusted and it be assigned the ***No Rule Exception*** attributes.

Fig. 2–16 *Access Control Service Trustzone - Settings*



List 2–33 *Access Control Service Trustzone - Settings – section No Rule Exception*

Parameter	Description
Bitmap	Here choose one of the ***Picture*** objects. The client will be advised to get the bitmap from the remediation server.
Limited Access Ruleset Name	Description see parameter ***Limit Access***, table 2–30, page 36.
Limited Access Message	

List 2–34 *Access Control Service Trustzone - Settings – section Identity*

Parameter	Description
Health Passport Signing Key	The Health Validator returns a digital passport to the client as result of the health validation. The passport contains all required information for the remediation server. To ensure authenticity the passport is digitally signed. **Note:** Since all Access Control Services of the same trustzone share the identify credentials, the remediation server instances can verify that a passport was issued by a health validator of the same trustzone. Here set the RSA key for digital passport signing.

List 2–34 *Access Control Service Trustzone - Settings – section Identity*

Parameter	Description
Health Passport Verification Key	Here set the RSA public key for verifying a digital passport signature. If one Access Control Server instance is a remediation server exclusively it is not necessary to set the ***Signing Key***, but only the ***Passport Verification Key***.

List 2–35 *Access Control Service Trustzone - Settings – section 802.1X*

Parameter	Description
802.1X	Description see parameter ***802.1X***, table 2–32, page 37

List 2–36 *Access Control Service Trustzone - Settings – section Limited Access Defaults*

Parameter	Description
Client Emergency Quarantine Time (s)	If the Access Control Server is not reachable anymore for the client, it switches automatically to the Quarantine or Unhealthy: Restricted State. Enter ***0*** to disable. For further information see parameter ***Limit Access***, table 2–30, page 36. **Note:** If no Access Control Server ip address is available this parameter doees not have any effect. See 11.3.2 Access Control Server IPs from Registry, page 160 and 11.3.3 Access Control Server IPs from DHCP, page 160
Quarantine Ruleset Name	Here choose one of the ***Personal Firewall Rules*** objects. The client will be advised to get the bitmap from the remediation server.
Quarantine Message	Here choose one of the ***Welcome Messages*** objects. The client will be advised to get the bitmap from the remediation server.
Health Validation Mode	• ***Moderate*** Health checks are executed after connection establishment. • ***Offensive*** Health checks are executed during connection establishment.

List 2–37 *Access Control Service Trustzone - Settings – section Radius Attribute Assignments*

Parameter	Description
	Generally with this feature it is possible to send additional attributes to the switch, depending on the health state of the client. VLAN Change attributes are already hardcoded.
Healthy	Description see parameter ***Healthy Attribute Assignments***, table 2–32, page 37
Unhealthy	Description see parameter ***Unhealthy Attribute Assignments***, table 2–32, page 37

2.4.8 Support Chart

This view provides information concerning Antivirus and Antispyware vendors and versions that are supported.

The Support Chart is automatically downloaded from the Barracuda Networks update service mentioned above and distributed to Barracuda NG Admin on connect. Thus, the Support Chart reflects the current capabilities of the Access Control Service.

Note

Restrictions on Microsoft® Windows Vista and Windows 7 64 Bit:

The supported features listed in the support chart may differ from the technically executed actions (e.g. automatic update of Windows Defender 1.x: the chart states **Implemented** though it may not work on the 64 Bit client. Reason: The released version of the 64 Bit client contains a 32 Bit compatible COM+ server for integrated OPSWAT-modules (health-check). Therefore this component is not yet implemented as native 64 Bit.

This leads to some restrictions regarding auto-remediation features of the health agent system:

- **Enabling/disabling of antivirus/antispyware can not be done automatically for some vendors (see support charts).**
- **Auto-remediation for antivirus/antispyware engine and pattern updates is disabled in the 64-bit client.**

Chapter 3
Server Config – Personal Firewall Rules

3.1 General

To configure the personal firewall rules browse to ***Client to Site*** and select the ***VPN FW*** tab. (***Config*** > ***Box*** > ***Virtual Servers*** > <servername> > ***Assigned Services*** > <servicename> ***(vpnserver)*** > ***Client to Site***).

Double-click the appropriate VPN Firewall Rule Set.

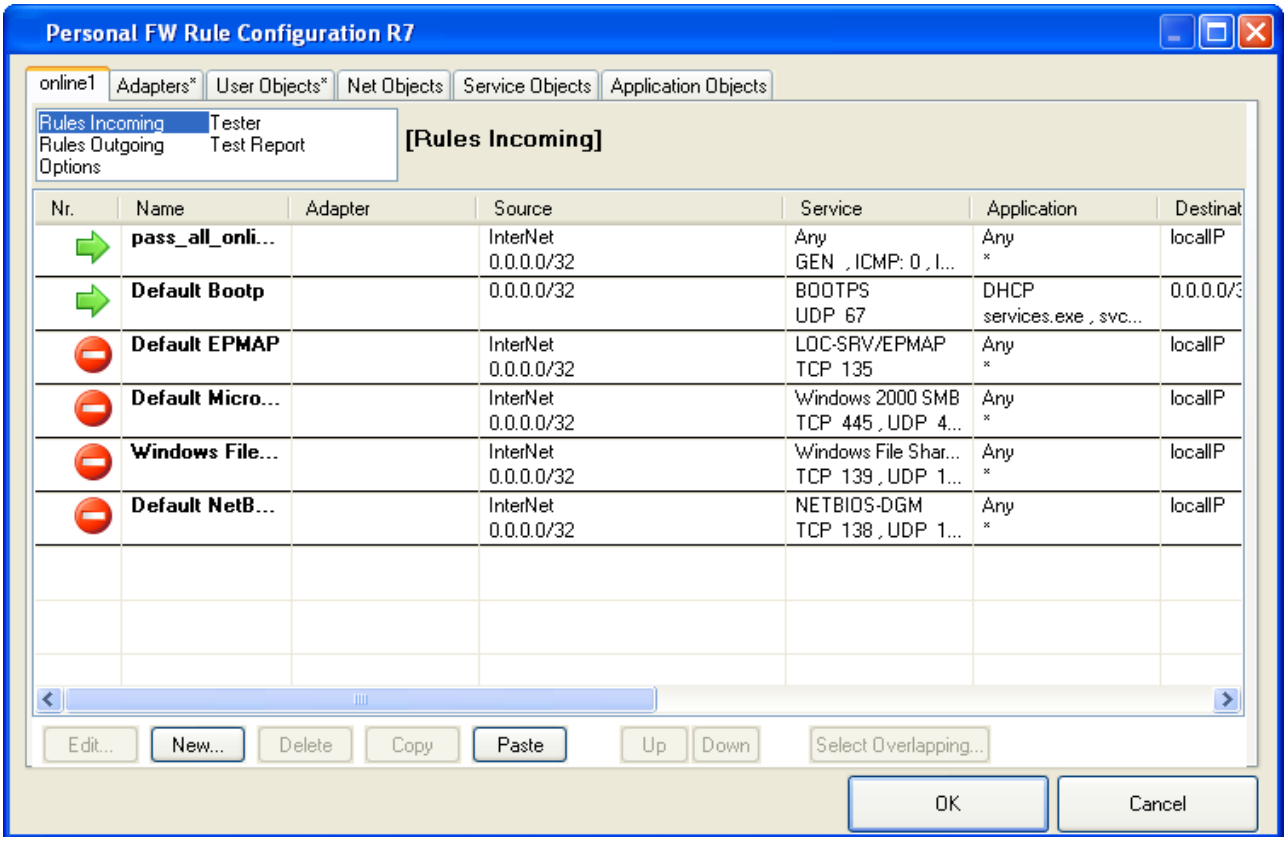
3.2 <Rule Set Name> Tab

This tab allows manual rule configuration, testing, and setting the options.

Note

Personal Firewall rule sets do not support Revision Control System (RCS).

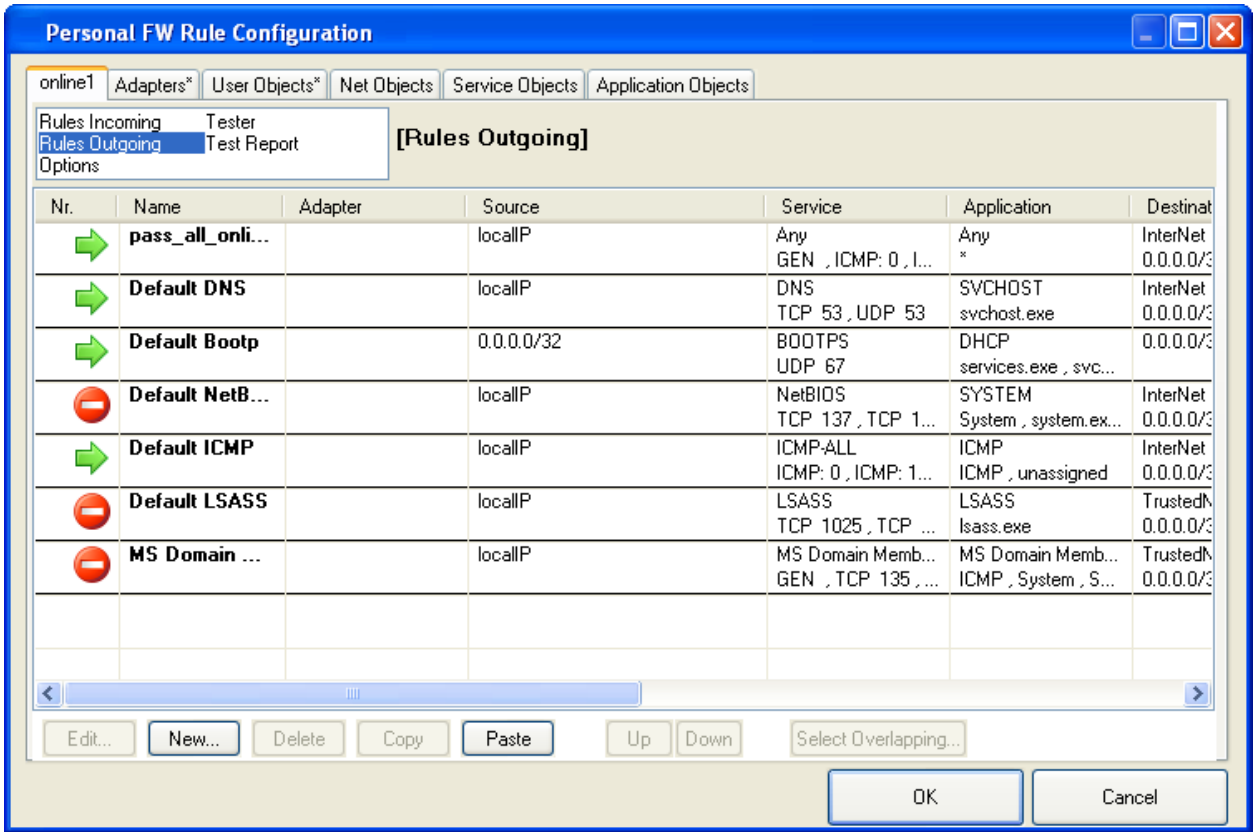
Fig. 3–1 *Rules Incoming*



3.2.1 Rules Incoming / Outgoing

Rules controlling incoming traffic are arranged in the ***Rules Incoming*** view, rules controlling outgoing traffic are arranged in the ***Rules Outgoing*** view (figure 3–1).

Fig. 3–2 *Rules Outgoing*



3.2.2 Context Menu

Select and right-click a list entry to display the following context menu:

Table 3–1 *Rule window - Context menu*

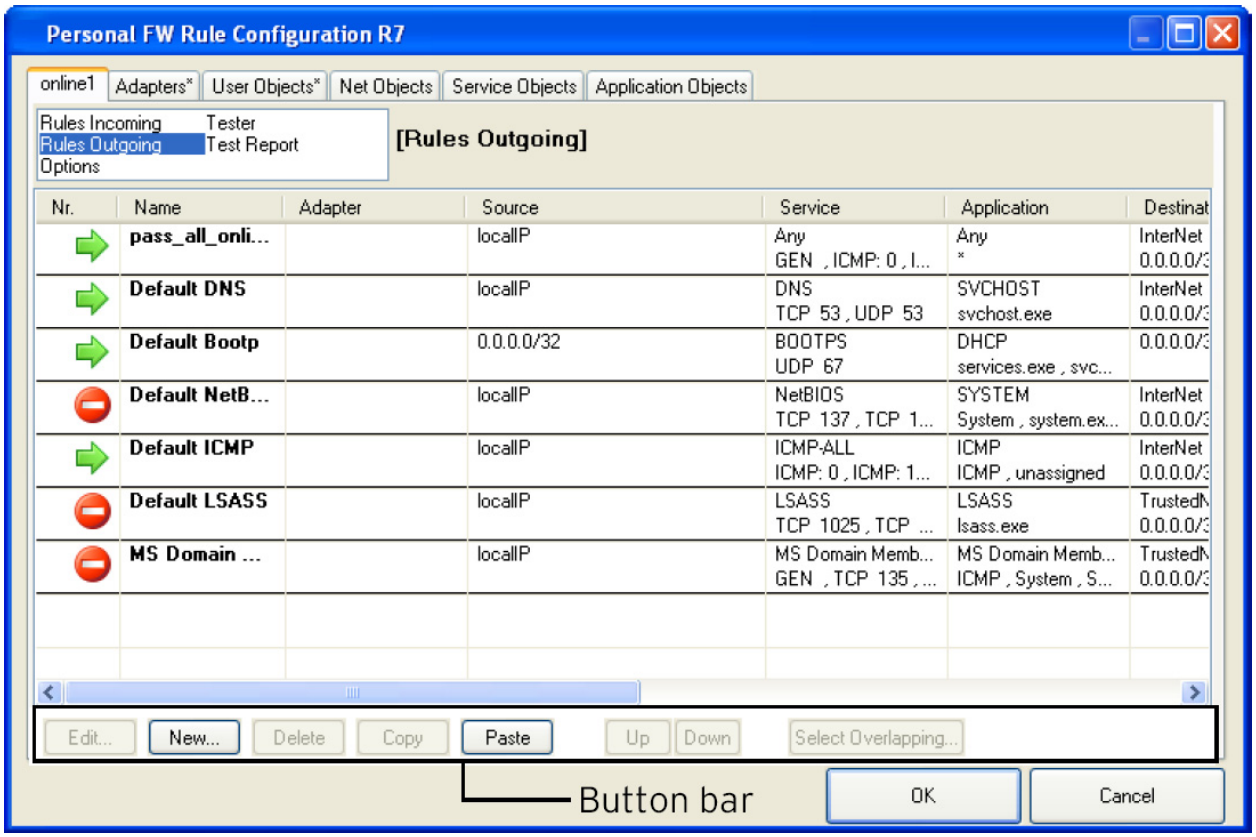
Item	Description
Show Source Addresses…	Opens a window displaying all source addresses affected by the selected rule.
Show Destination Addresses…	Opens a window displaying all destination addresses affected by the selected rule.
Show Services…	Opens a window displaying all services affected by the selected rule.
Show Applications…	Opens a window displaying all applications affected by the selected rule.
Show Adapters…	Opens a window displaying all adapters affected by the selected rule.
Show Users…	Opens a window displaying all users affected by the selected rule.
Select Overlapping…	As a connection request can match several conditions, the rules' succession within a rule set is very important. If incorrectly ordered, rules might interfere with one another. The function ***Select Overlapping*** is meant to help avoiding configuration mistakes. When applied to a selected rule, all rules possibly interfering with it are highlighted. In the majority of cases, the overlap is a harmless outcome of the use of very openly defined objects such as ***InterNet***.
Edit…	Opens the rule configuration dialog for the selected rule (3.2.4 Rule Configuration, page 45).

Table 3–1 *Rule window - Context menu*

Item	Description
New…	Opens the rule configuration dialog for a new rule (3.2.4 Rule Configuration, page 45).
Delete	Deletes the selected rule(s).
Copy	Copies the selected rule(s) to the clipboard.
Paste	Pastes the selected rule(s) from the clipboard.

3.2.3 Button Bar

Fig. 3–3 *Rules Outgoing – Button bar*



In the button bar, the ***Up*** and ***Down*** buttons complement options are available in the context menu.

Select a rule and click one of the buttons, to shift the rule further up or down within the rule set. Alternatively, you can use drag&drop.

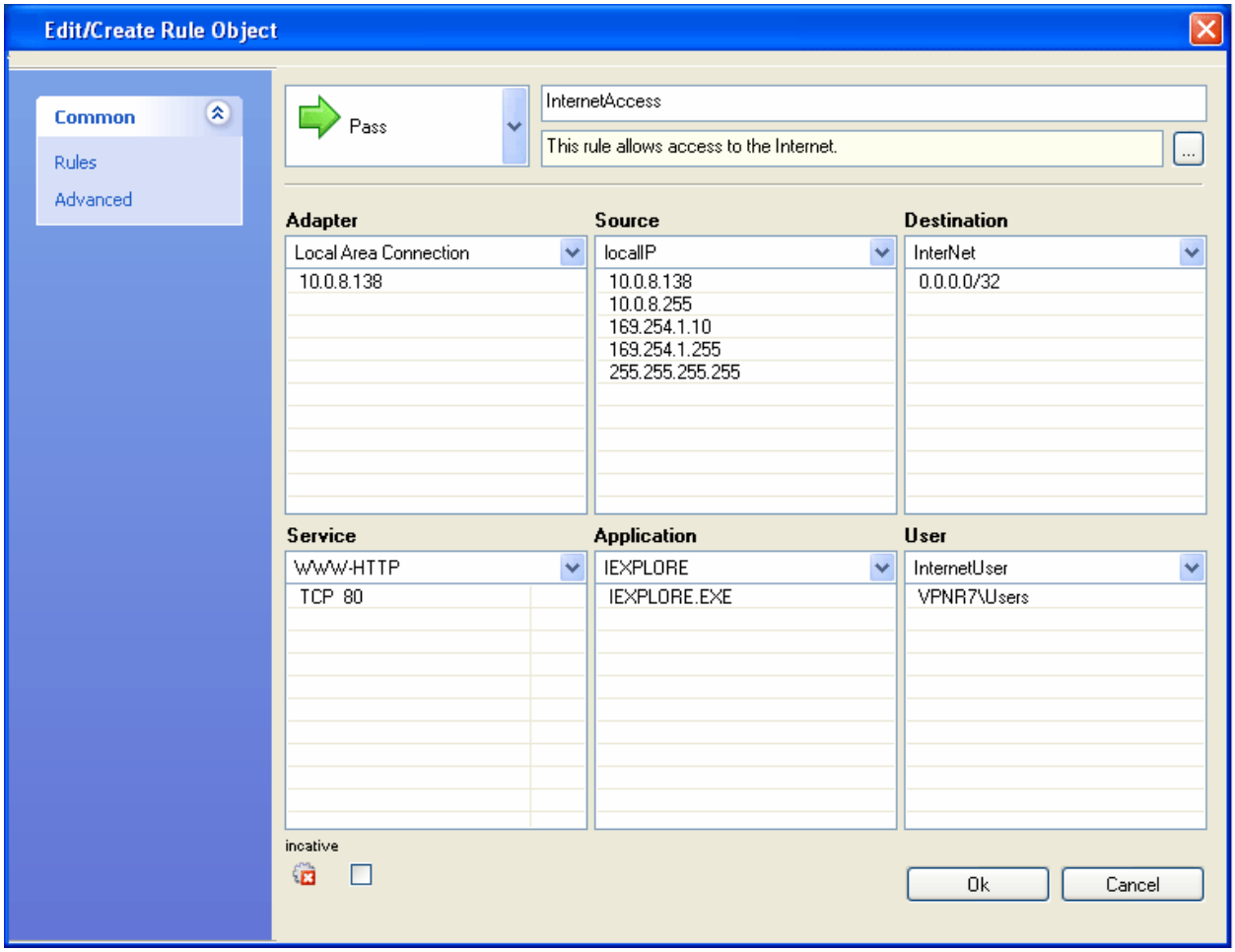
Note

According to a regular Barracuda NG Firewall rule set, the NG Firewall rule set is processed rule by rule until an applicable rule is available. Thus, to achieve correct rule processing, rules must be arranged in the correct order.

3.2.4 Rule Configuration

Select ***New…*** from the context menu to create a new rule.

Fig. 3–4 *Edit/Create Rule Object*



Configure the following connection details in the ***Rules*** view of the ***Rule Object*** window:

List 3–1 *Edit/Create Rule Object - Options in the Rules view*

Item / Parameter	Description
Action	Select ***Pass*** to enable a connection request, select ***Block*** to prevent it.
Name	Insert a rule name into this field. **Note:** The maximum length of this parameter is 50 characters.
Comment	For easier identification, insert a rule description (optional).
inactive	Select the ***inactive*** checkbox to disable a rule (default: unselected).

Note

A minimum specification of the following connection details is mandatory in the sections below:

- ***Source*** / ***Destination*** / ***Service*** **or**
- ***Adapter*** / ***Source*** / ***Service*** **or**
- ***Adapter*** / ***Destination*** / ***Service***

Caution

Modifying an object is a global action. For example, any other rule using the specific object will be affected by the modification.
This applies only for referenced objects, not for objects of type <explicit>.
Explicit objects are only available for the current rule.

Table 3–2 *Edit/Create Rule Object – Sections*

Section	Description
Adapter	Specify an adapter for the connection request. In the list all ***Adapter Objects*** that have been defined in the ***Adapter*** window are available (3.3 Adapters, page 51). Right-click the adapter window below the list and Select ***New…*** to create a new Adapter Object. Double-click an available entry to edit the assigned Adapter Object.
Source / Destination	Specify a source for the connection request. In the list all ***Network Objects*** that have been defined in the ***Networks*** window are available (3.5 Net Objects, page 55). Select ***<Explicit>*** to define a network object explicitly without adding it to the Network Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Network Object. Double-click an available entry to edit the assigned Network Object.
Service	Specify a service for the connection request. In the list all ***Service Objects*** that have been defined in the ***Services*** window are available (3.6 Service Objects, page 58). Select ***<Explicit>*** to define a network object explicitly without adding it to the Service Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Service Object. Double-click an available entry to edit the assigned Service Object.
Application (optional)	Specify an application for the connection request. In the list all ***Application Objects*** that have been defined in the ***Application*** window are available (3.7 Application Objects, page 59). Select ***<Explicit>*** to define an application object explicitly without adding it to the Application Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Application Object. Double-click an available entry to edit the assigned Application Object.
User (optional)	Specify an user for the connection request. In the list all ***User Objects*** that have been defined in the ***User*** window are available (3.4 User Objects, page 54). Select ***<Explicit>*** to define an user object explicitly without adding it to the User Objects listing. Right-click the source window below the list and Select ***New…*** to create a new User Object. Double-click an available entry to edit the assigned User Object.

Configure the following connection details in the ***Advanced*** view of the ***Rule Object*** window:

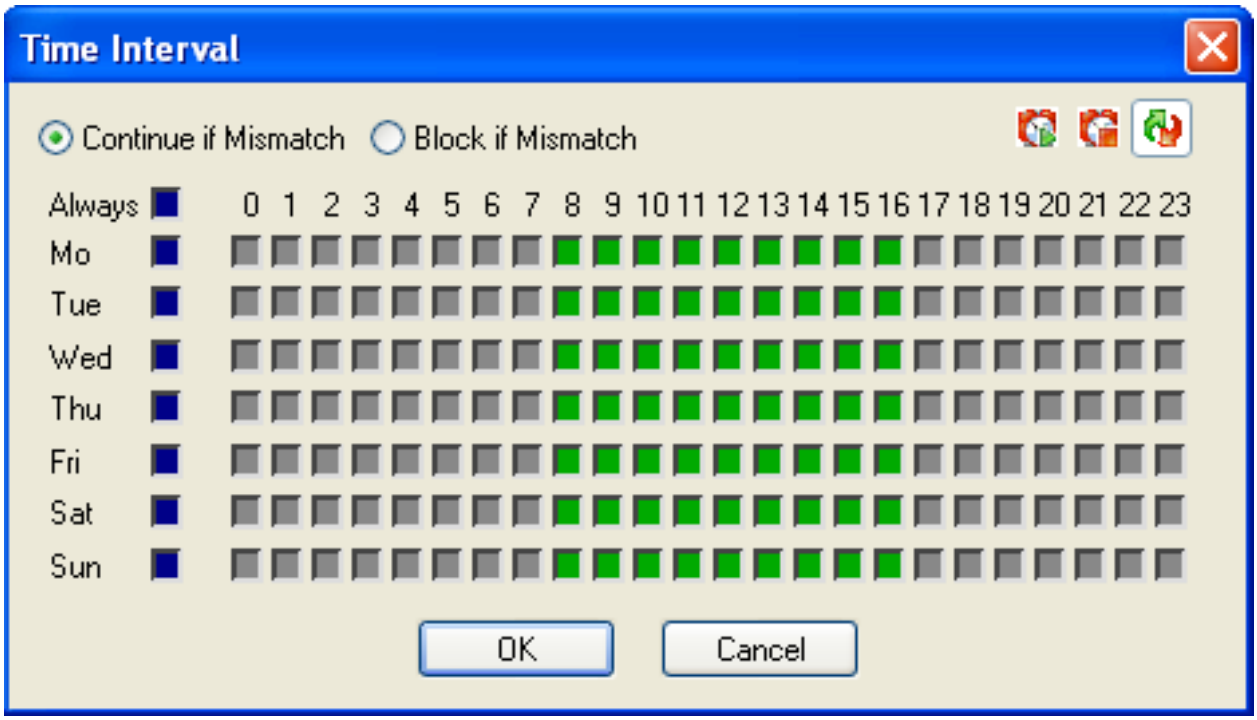
List 3–2 *Edit/Create Rule Object - Options in the Advanced view – section Rule Mismatch Policy*

Parameter	Description
Source / Service/ Destination / Application / User / Adapter	• ***Continue on Mismatch (default)*** Process the rule, even if the corresponding object does not match the configured setting. • ***BLOCK on Mismatch*** Do not process the rule if the corresponding object does not match the configured setting.

List 3–3 *Edit/Create Rule Object - Options in the Advanced view – section Miscellaneous*

Parameter	Description
Time Restriction	A time restriction can be assigned to each rule. The granularity is 1 hour on a weekly base. A rule is allowed at all times by default, for example, all checkboxes in the ***Time Interval*** window are cleared. Selecting a checkbox denies a rule for the given time. Select (set invert) from the list to configure allowed and disallowed time intervals simultaneously. Select (set allow) from the list to clear selected checkboxes. Select (set deny) from the list to to configure disallowed time intervals. Select ***Continue if mismatch*** to process the rule even if time restriction denies it. Select ***Block if mismatch*** to prevent rule processing if time restriction denies it (default). See figure 3–5: a time interval setting for a rule which has been set to disallowed on Monday and Thursday from 8 a.m. to 5 p.m.
Monitor Connections	• ***Yes*** • ***No***

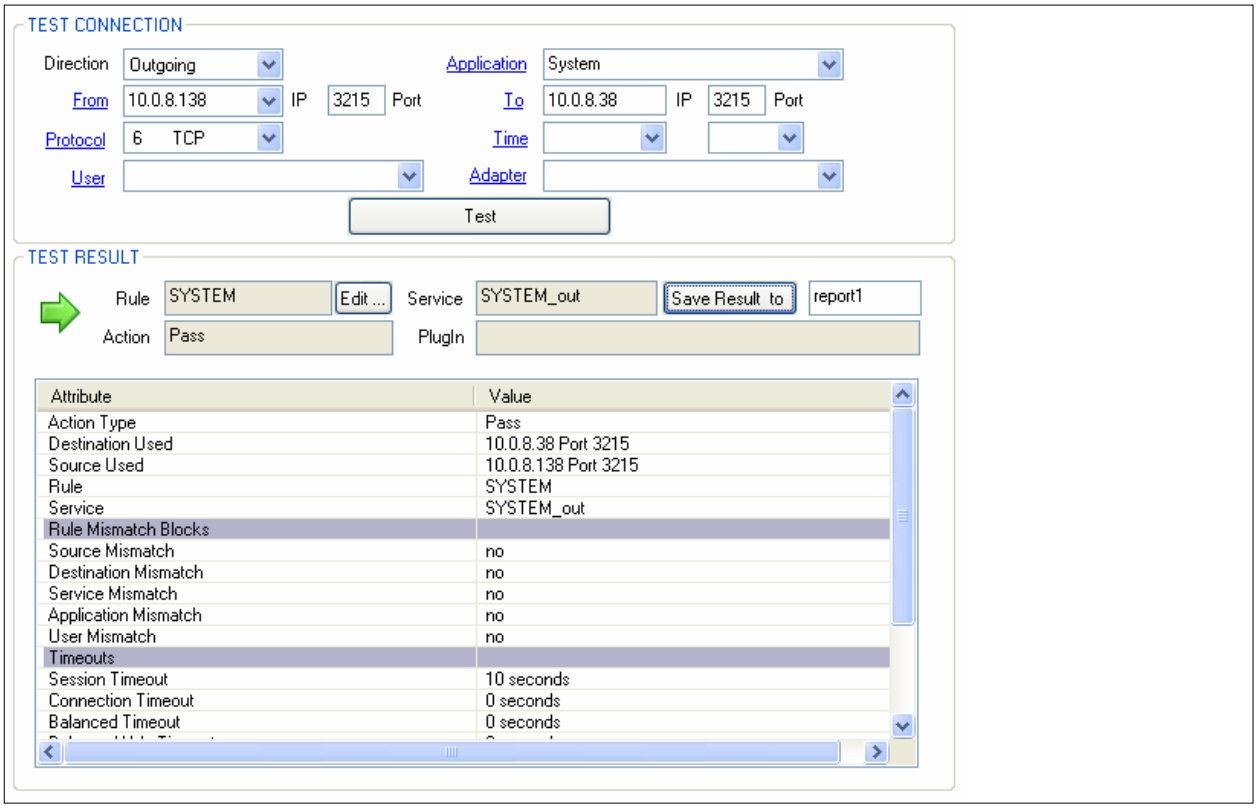
Fig. 3–5 *Time restriction dialog*



3.2.5 Tester

The ***Tester*** view allows testing rule sets for consistency.

Fig. 3–6 *Rule Tester*



The following entities are available for rule testing:

List 3–4 *Rule Tester parameters – section TEST CONNECTION*

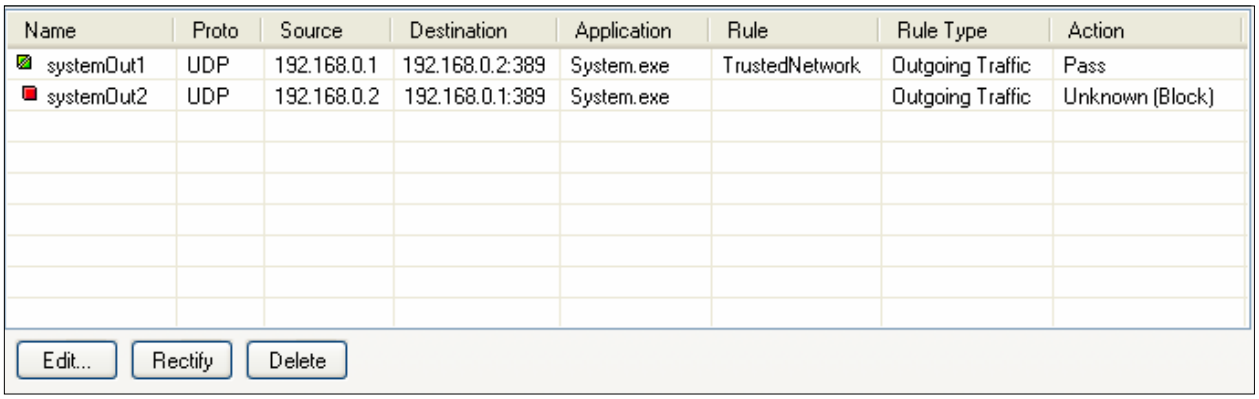
Parameter	Description
Direction	This is the direction of the traffic policy (***Incoming*** or ***Outgoing***).
Application	To query for an arbitrary application leave the asterisk (*), which is set as default value. Click the ***Application*** link and Select ***Update Applications*** to reset the field to the default value.
From: IP / Port	Insert Source IP and corresponding connection port. Click the ***From*** or ***To*** link to ***Swap IP*** and/or ***Port*** information.
Protocol	Specify which protocol to test. Click the ***Protocol*** link and select ***Show all Protocols*** to include other protocols than TCP/UDP and ICMP into the list.
Time (optional)	Insert day of the week and time (optionally). Click the ***Time*** link and select ***Insert current Time*** to insert current day and time.
User (optional)	Select an User from the list (Optionally). Click the ***User*** link and select ***Update Users*** to clear the field.
Adapter (optional)	Select an adapter from the list (Optionally). Click the ***Adapter*** link and select ***Update Adapters*** to clear the field.
Test	Click ***Test*** to test the connection and display the test result in the section below.

List 3–5 *Rule Tester parameters – section TEST RESULT*

Parameter	Description
Test Status Icon / Action	A connection attempt with the given values can either have failed or have been successful if a rule is applicable. A failed connection will be indicated by symbol and ***Action*** field ***Block*** ⛔. A successful connection attempt will be indicated by symbol and ***Action*** field ***Pass*** ➡.
Rule	The ***Rule*** field displays the applicable rule responsible for the rule test result. Click ***Edit…*** to open and modify the corresponding rule. If the connection attempt has been blocked because no rule has applied, the field will display the string ***<No Matching Rule Found>***.
Service	This field displays the applicable ***Service Object***.
PlugIn	If applicable, this field displays the name of the PlugIn that has been employed in the connection.
Save Result to	Insert the report name and click ***Save Result to*** to save the test result. The output of the connection test is written to the ***Test Report*** view (3.2.6 Test Report, page 48).
Attribute/Value listing	This listing displays attributes of the tested connection in detail.

3.2.6 Test Report

Fig. 3–7 *Test Report window*



Test reports are saved on a first come first served basis. Test results with ***Action Pass*** are indicated by a green icon (), test results with ***Action Blocked*** are indicated by a red icon ().

Changing any parameter in any configuration area that influences the result of a test report leads to a status icon change in the overview window. Green icons (✓) will become red (✗). To apply the new conditions to an already existing test report, select the data set in the overview window of the ***Test Reports*** window and click ***Rectify***.

Note

Subsequently to this action, the status icons will no longer indicate if an action has been successful or not, but instead if rectification has been applied. Rectified entries will be flagged with a green (✓) status icon, even if a tested connection attempt has failed.

Select a report and click ***Edit…*** to open the test result in the ***Rule Tester*** window. You may now use the report as template for further connection tests.

Select a report and click ***Delete*** to delete the report from the Test Report window.

3.2.7 Options

The ***Options*** view contains settings steering the overall behavior of the personal firewall if this rule set is active.

List 3–6 *Barracuda NG Network Access Client*

Parameter	Description
Trusted Network	Network assignments and references in the network object that have been defined as trustworthy are updated dynamically, when network adapters are added to the system with trust assignment "trusted" or when IP address configuration of a trusted adapter changes (3.3 Adapters, page 51). By default, the ***Trusted Network*** option points to the preconfigured ***TrustedNet*** object (3.5 Net Objects, page 55). You may change the setting to another available network object. Be aware of possible implications. Set to ***No*** to disable this feature.
Domain Member	This option can only be set to ***yes*** when a network object has been configured as ***Trusted Network***. Setting to ***yes*** creates and activates default rules allowing applications required in Microsoft Windows domains.
Windows File Sharing	This option can only be set to ***yes*** when a network object has been configured as ***Trusted Network***. When set to ***yes*** incoming connections to local printer(s) and files are allowed.
Allow NetBIOS Incoming	Setting to ***yes*** (default: ***no***) allows incoming NetBIOS traffic.
Allow NetBIOS Outgoing	Setting to ***yes*** (default: ***no***) allows outgoing NetBIOS traffic.
Ask for unknown incoming connections	Set this value to ***yes*** to enforce manual confirmation for all incoming connection attempts. Confirmation for connection establishment grant is going to be requested by a notification pop-up.
Ask for unknown outgoing connections	Set this value to ***yes*** to enforce manual confirmation for all unknown outgoing connection attempts. Confirmation for connection establishment grant will be requested by a notification pop-up.
Ask for adapter update confirmation	Setting to ***yes*** (default) triggers a pop-up, when settings assigned to a network adapter change. See 9.9.1 Automatic Adapter Configuration, page 121 for details.

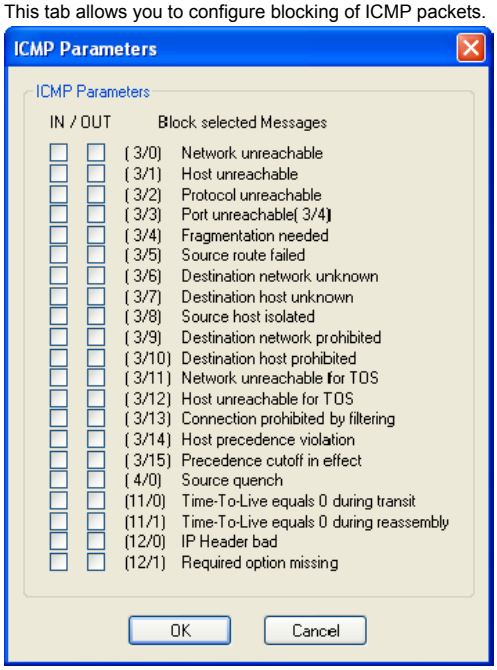
Parameter	Description
ICMP Parameters	This tab allows you to configure blocking of ICMP packets. 
Connect to the Internet with ADSL (PPTP)	Setting to yes creates a pass rule named ADSL in the Outgoing tab of the firewall configuration that is needed for Internet connections via ADSL. The service object used in this rule amongst others implements the services and protocols listed in table 3-3, page 50.

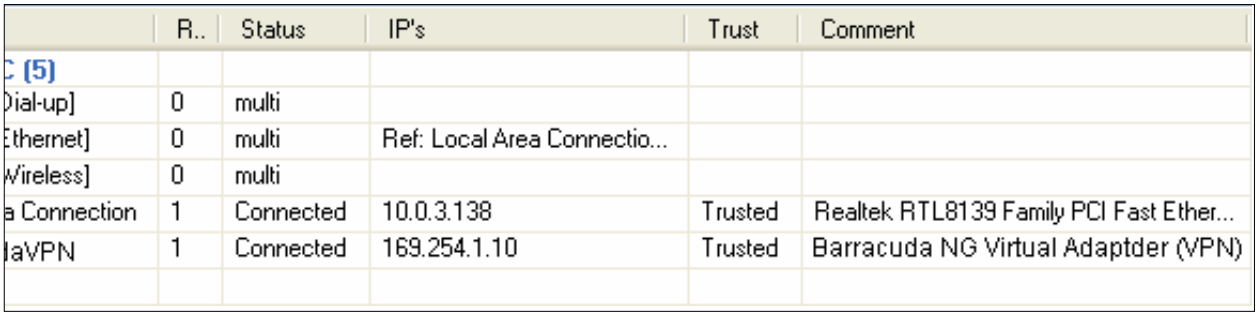
Table 3–3 *Services and protocols employed by the ADSL rule*

Port	Protocol	Service Name	Description
	GRE	pptp	Generic Routing Encapsulation; protocol which allows an arbitrary network protocol A to be transmitted over any other arbitrary network protocol B, by encapsulating the packets of A within GRE packets, which in turn are contained within packets of B
1723	TCP	NETBIOS-DGM	Point-to-Point tunnelling protocol; control port

3.3 Adapters

The Adapters tab allows you to view and configure network adapters available on the system. Adapters may be employed in firewall rules, in order to restrict rule processing to a specific adapter or a set of adapters only.

Fig. 3–8 *Adapter view*



	R..	Status	IP's	Trust	Comment
(5)					
Dial-up]	0	multi			
Ethernet]	0	multi	Ref: Local Area Connectio...		
Wireless]	0	multi			
a Connection	1	Connected	10.0.3.138	Trusted	Realtek RTL8139 Family PCI Fast Ether...
laVPN	1	Connected	169.254.1.10	Trusted	Barracuda NG Virtual Adaptder (VPN)

The listing is divided into the following columns:

Table 3–4 *Adapter view details*

Column	Description
Name	Name of the adapter object.
Referenced by	Number of references pointing to the adapter object
Status	Current connection status of the adapter object (***connected*** / ***disabled*** / ***multi***)
IP's	IP addresses and/or references assigned to the adapter object
Trust	Trust type assigned to the adapter object (***trusted*** / ***untrusted***)
Comment	Optional adapter object description

In the Adapter Objects view, several **dynamic** adapter objects (flagged with the icon) are preconfigured.

Note

Dynamic objects are updated at runtime when adapter configuration changes and cannot be edited manually. In order to work, Automatic Adapter Assignment must be selected in the Firewall Settings (9.4.1 Firewall Menu, page 91).

The following objects (assigned with status ***multi***) are available:

- ***Adapter [Dial-up]***

  This object summarizes all dial-up adapters available on the system (for example, UMTS, ISDN, and modem cards).

- ***Adapter [Ethernet]***

  This object summarizes all Ethernet adapters available on the system (for example, LAN devices).

- ***Adapter [Wireless]***

This object summarizes all wireless adapters available on the system (for example, WLAN cards).

Note

Adapters available on the system are automatically assigned to the appropriate adapter object with status type ***multi***. These objects may be used to construct abstract rule sets, for example, to configure a rule blocking access to all available dial-up or wireless adapters.

The following further adapter objects are available:

- ***[Network Connection name]*** (for example, ***Local Area Connection***)

  These are the LAN devices available on the system. The *Network Connection* name is retrieved from the Microsoft Windows Network Connections view (available through ***Start > Settings > Network Connections***).

Note

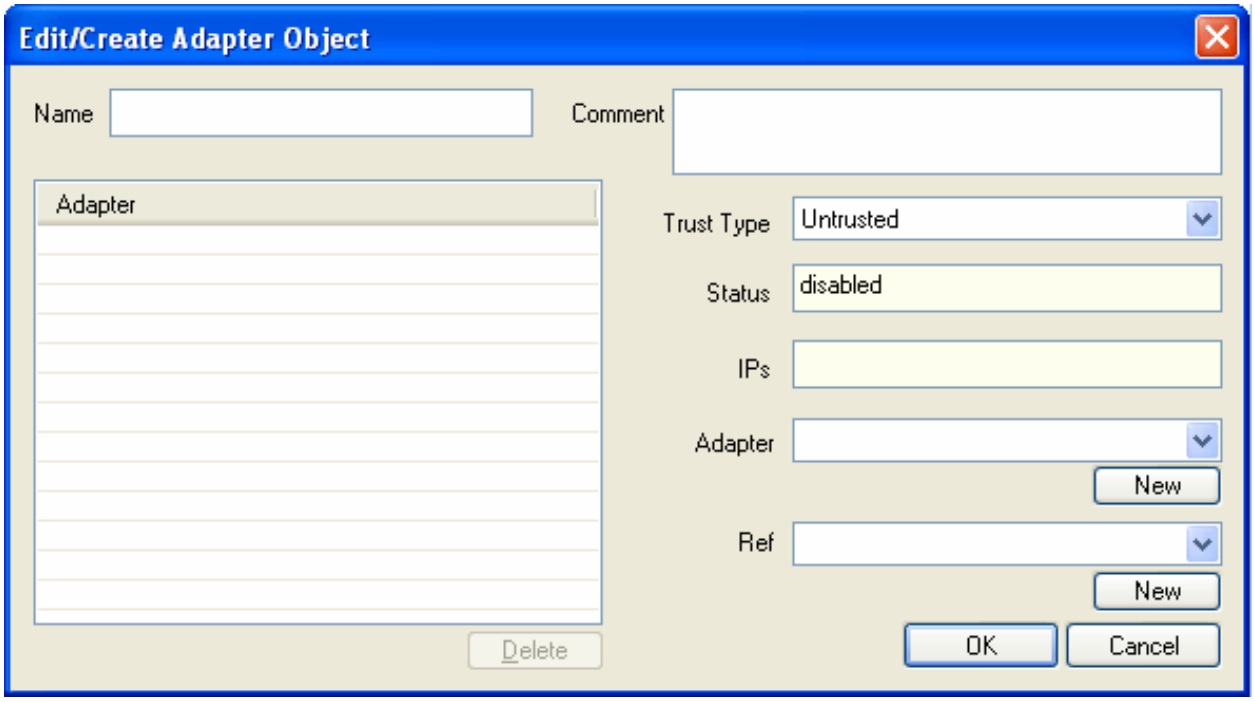
The "logical" Microsoft Windows name, dependent on the operating system's language version, and not the device name is applicable for object naming.

- ***Barracuda NG VPN***

  This is the virtual interface of the NG VPN client.

To create a new adapter object, click ***New…*** in the ***Adapter Objects*** window:

Fig. 3–9 *Edit/Create Adapter Object configuration dialog*



List 3–7 *Edit/Create Adapter Object options*

Parameter	Description
Name	Specify a name for the adapter object.

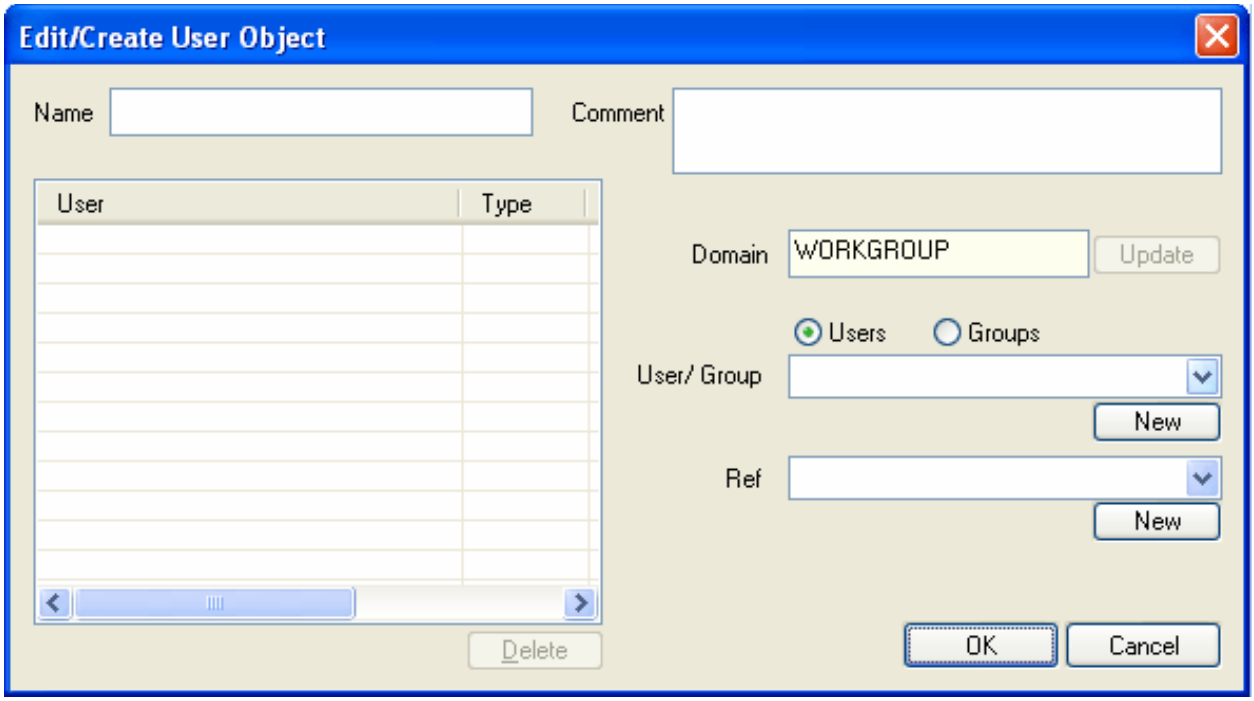
List 3–7 *Edit/Create Adapter Object options*

Parameter	Description
Comment	Optionally, insert an adapter description
Trust Type	Select ***Trusted*** to add a reference to the adapter object to the network object that has been defined as Trusted Network in the ***Administration*** > ***Firewall Settings*** (***Trusted Network***, page 120). If you do not want to create a reference, select ***Untrusted***. **Note:** When later changing the setting from ***Trusted*** to ***Untrusted***, the reference to the adapter object is automatically deleted from the ***Trusted Network*** object. References to ***Untrusted*** adapter objects may not be added to the ***Trusted Network*** object manually.
Status	This is a read-only field displaying the connection status of the adapter object.
IPs	This is a read only field, displaying the IPs assigned to the adapter object.
Adapter/Ref	Select network adapter and/or reference you wish to create the adapter object for. Click ***New*** to add your selection to the ***Adapter*** list.

3.4 User Objects

The ***User Objects*** tab allows you to create User and User Group objects, which may be employed in rule sets. Click ***New…*** to open the ***Edit/Create User Object*** dialog:

Fig. 3–10 *User Object dialog*



An user object is automatically created when a connection attempt is processed by the firewall. The object is then inserted into the corresponding rule.

In the ***User/Group*** list, the Microsoft Windows domain users and groups known to the Barracuda NG Firewall are available for selection. Local user/group information is displayed in the list first. If the Windows workstation is a member of a Microsoft Windows domain, domain user/group information may be retrieved from the Active Directory server by clicking ***Update***.

Note

Irrespective of the operating systems language version installed on the workstation, the following users will always be displayed in English:

- ***NT AUTHORITY\SYSTEM***
- ***NT AUTHORITY\LOCAL SERVICE***
- ***NT AUTHORITY\NETWORK SERVICE***
- ***NT AUTHORITY\NETWORK***

Warning

The internal firewall engine will transform these names to the appropriate language version. Do not insert them in another language manually.

3.5 Net Objects

The ***Net Objects*** tab facilitates IP address/network management. Use this tab for the following purposes:

- ***Assigning of names to single IP addresses***
- ***Combining multiple IPs/networks/references into networking objects***

Note

For a clearly arranged network management rather make use of referencing Network Objects than explicit IPs when configuring firewall rule sets.

Fig. 3–11 *Network Objects window*

Name	RefBy	Entries	Description
DYNAMIC (9)			
dhcpIP	0	255.255.255.255 , 0.0.0.0 , Ref...	Local IP with 0.0.0.0
InterNet	5	0.0.0.0/32	Unsecure Zone
localIP	13	169.254.1.10 , 10.0.8.138 , Ref...	All Local IPs
Net-Broadcast	1	169.254.1.255 , 10.0.8.255 , 25...	All Broadcasts
Net-Local Area Con...	1	10.0.8.0/8	Realtek RTL8139 Family PCI Fast Etherne...
Net-Multicast	1	239.255.0.0/16	Multicasting RFC 2365 and 3172
Net-netfenceVPN	1	169.254.1.0/8	phion Virtual Adapter (VPN)
TrustedNet	6	255.255.255.255 , Ref: Net-Mul...	Secure Zone
virtualIP	0	169.254.1.10	All Virtual Phion VPN IPs
LOCAL (1)			
ADSLNet	1	0.0.0.0/32	

In the ***Net Objects*** tab, a number of **dynamic** network objects (flagged with the icon) are preconfigured.

Note

Dynamic objects are updated at runtime when network configuration changes and cannot be edited manually. For dynamic update to work, Automatic Adapter Assignment must be selected in the Firewall Settings (9.4.1 Firewall Menu, page 91).

- ***localIP***

Contains all IPs that are configured on **trusted** adapters, and a reference to the Net-Broadcast object.

- ***virtualIP***

Contains the IP address assigned from the VPN server. The virtual IP is only available in case of established VPN connections.

- ***Net-[Network Connection name]***

These network objects contain the network addresses of each specific adapter available on the system. The *Network Connection* name is retrieved from the Microsoft Windows Network Connections view (available through ***Start > Control > Network Connections***).

Note

The "logical" Microsoft Windows name, which depends on the operating system's language version and not the device name, is applicable for object naming.

Net-[Network Connection name] objects may be used to set up abstract rule sets.

- ***InterNet***

The ***InterNet*** object may be used for outbound connections to the Internet (network 0.0.0.0/0).

- ***TrustedNet***

Use the ***TrustedNet*** object to refer to trustworthy networks. The content of this object is dependent on assignment of an adapter as trusted or untrusted (3.3 Adapters, page 51). When an adapter is specified as trusted the IP addresses living on it are added to the TrustedNet object. Vice versa they are deleted from it, when trust assignment changes to untrusted. The TrustedNet object is also updated when IP address configuration of a trusted adapter changes.

- ***Net-Barracuda NG VPN***

The Net-Barracuda NG VPN object contains the address of that network the ***virtualIP*** object is living in.

Note

Secured Routes are assigned to the ***Net-Barracuda NG VPN*** Object.

- ***Net-Broadcast***

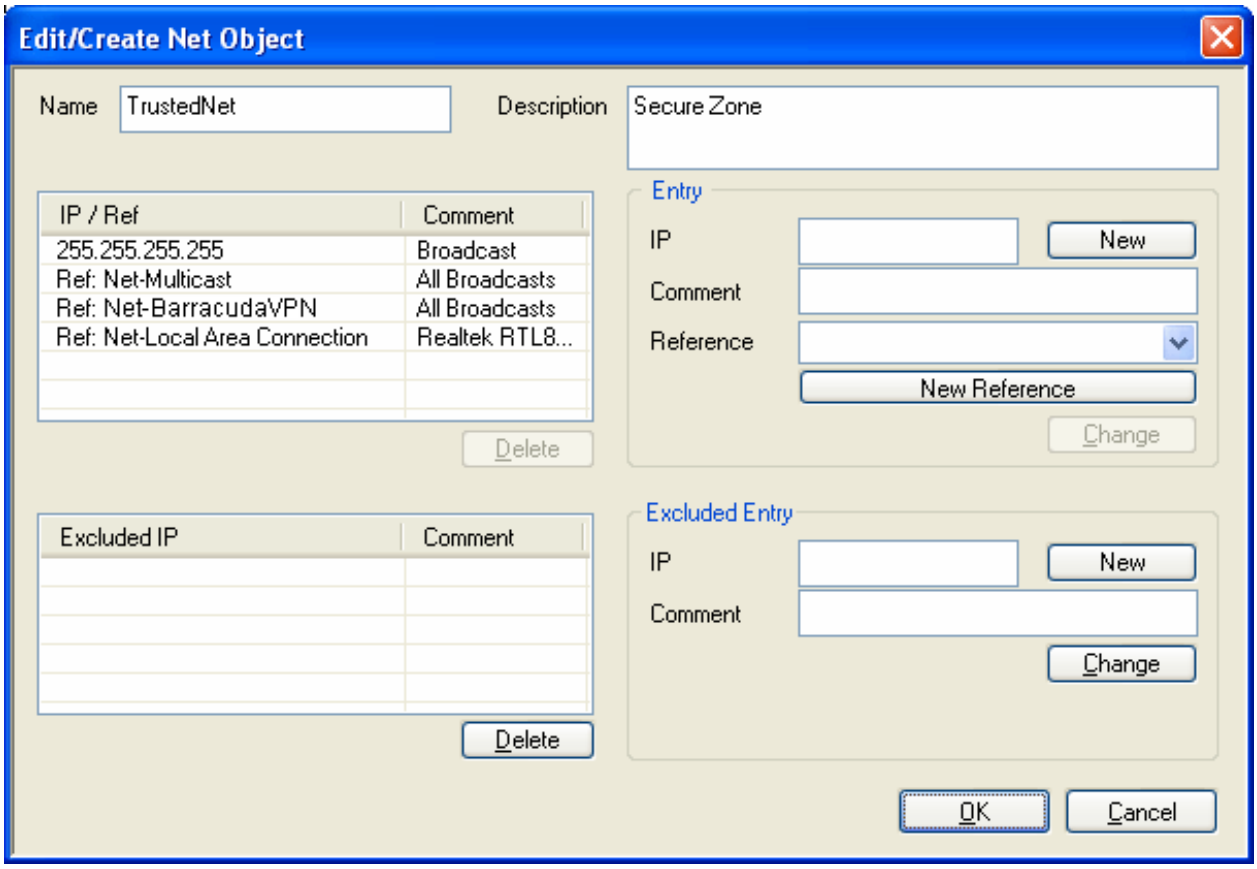
This object contains the broadcast addresses of IP addresses configured on **trusted** adapters. The broadcast addresses are calculated directly from the IPs.

- ***Net-Multicast***

This object includes the Multicast network 239.255.0.0/16.

Click ***New…*** to open the ***Net Object*** dialog.

Fig. 3–12 *Net Object dialog*



Insert ***Name*** and ***Description*** of the Net Object for easier identification.

In the ***Entry*** section insert IP/network address(es) of the new Net Object and/or specify a ***Reference*** to the Net Object, for example select an existing Net Object to refer to a new one.

The ***Excluded Entry*** section allows excluding specific networks from a network object.

Note

For transparency and consistency reasons, references are not available in this section.

3.6 Service Objects

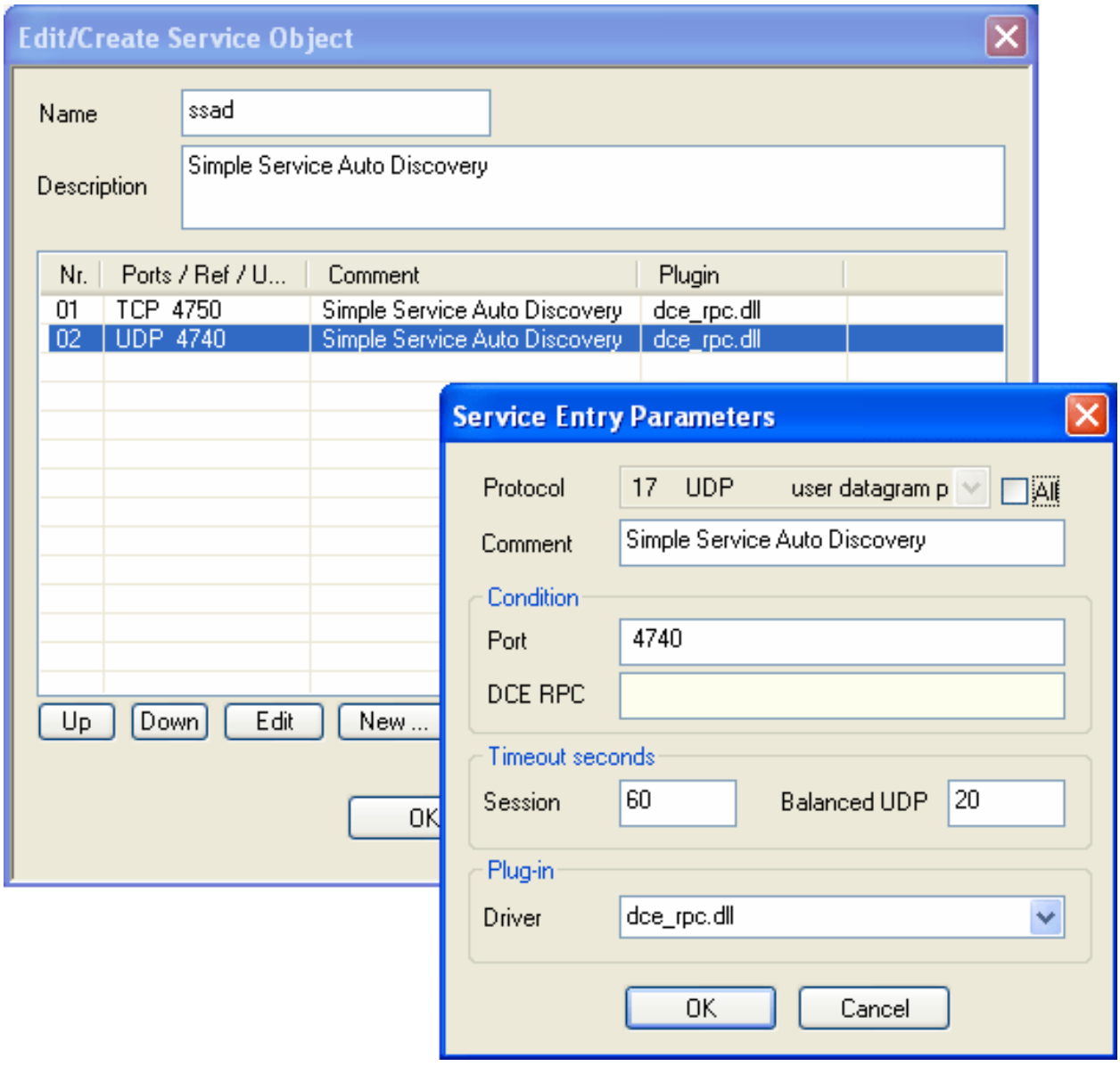
The ***Service Objects*** tab facilitates port and protocol management. Use the Services window to

- ***assign port and protocol to specific services***
- ***and merge multiple services to one service object using references.***

Note

Properties of Service Objects are described in detail in the Barracuda NG Firewall Administrator's Guide.

Fig. 3–13 *Service Object dialog*



The following services are available in the Barracuda NG Personal Firewall by default:

Table 3–5 *Service Objects available in the Personal Firewall*

Service Name	Port	Protocol	Connection	Description
		ICMP	**O / I**	Internet Control Message Protocol; ICMP messages, delivered in IP packets are used for out-of-band messages related to network operation, or misoperation.
DNS	53	TCP/UDP	**O**	Domain Name Service; method by which the Internet addresses in mnemonic form (for example barracuda.com) are converted into the equivalent numeric IP address (for example 134.220.4.1)
BOOTPS	67	UDP	**O**	Bootstrap protocol; also used for DHCP (Dynamic Host Configuration)
Kerberos	88	TCP/UDP	**O**	Protocol for authentication in Windows 2000 environment
NTP	123	UDP	**O**	Network Time Protocol; used to synchronize the time of a computer client or server to another server or reference time source
LOC-SRV/EPMAP	135	TCP	**O**	NETBIOS; very common protocol; it is supported on both, Ethernet and TokenRing. In NetBIOS, TCP and UDP communication is supported. It supports broadcasts and multi-casting and also three distinct services: Naming, Session, and Datagram.
NETBIOS-NS	137	UDP	**O / I**	
NETBIOS-DGM	138	UDP	**O / I**	
NETBIOS-SSN	139	TCP	**O / I**	
SNMP	161	UDP	**O**	Simple Network Protocol; Network management system contains two primary elements – Manager (console to perform network management functions) and Agents (entities that interface to the actual managed device). SNMP allows Managers and Agents to communicate.
LDAP	389	TCP/UDP	**O**	Lightweight Directory Access Protocol; set of protocols for accessing information directories.
CIFS	445	TCP	**O / I**	further development of the SMB protocol and serves as an addition and improvement to the standard protocols FTP and HTTP.
MSTASK	1026	TCP	**O**	Windows Task Scheduler; used to schedule tasks, such as backups or updates, to run at certain times or dates

3.7 Application Objects

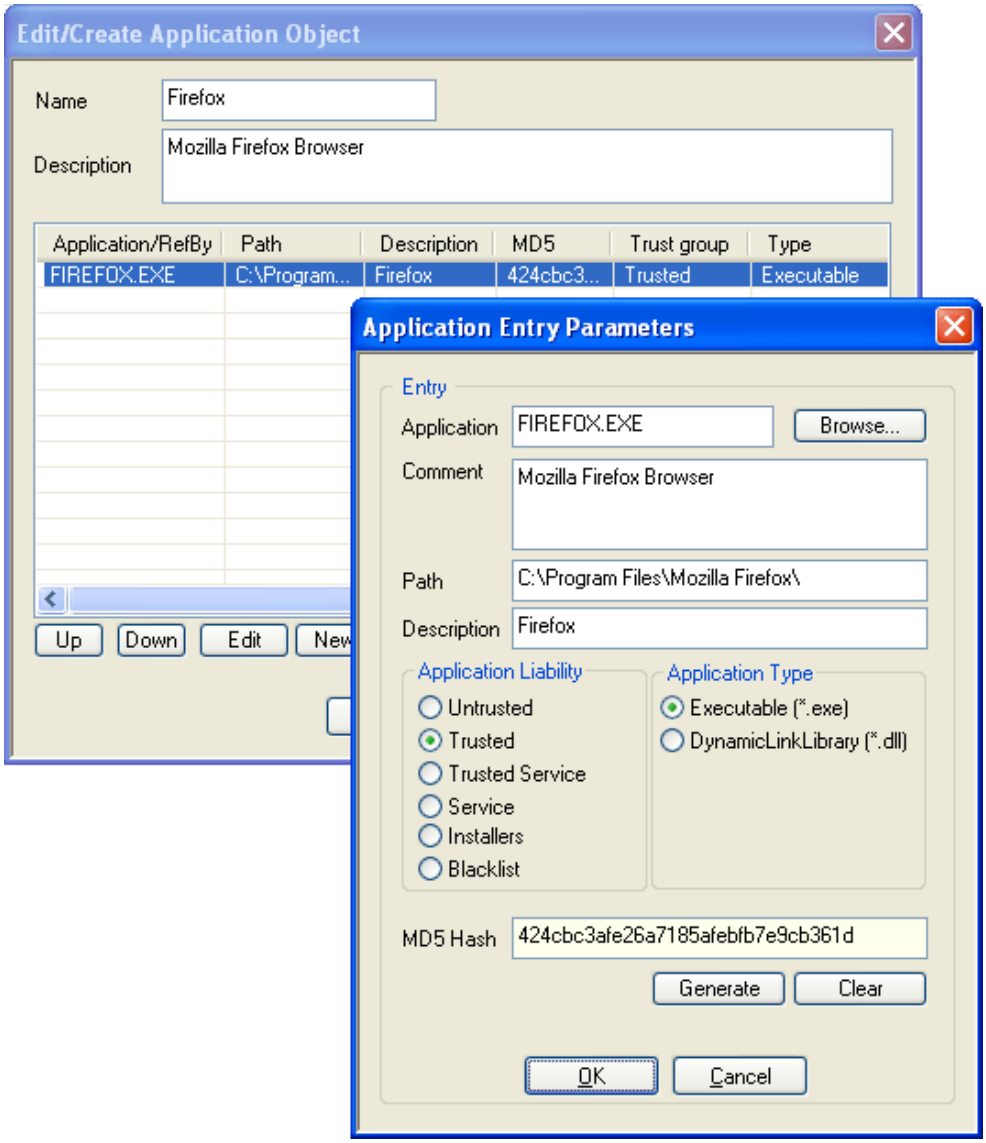
The ***Application Objects*** tab allows creating predefined applications, which may be employed in rule sets.

Click ***New…*** to open the ***Edit / Create Application Object*** window.

Note

Application Liability and ***Application Type*** classifications are purely informational.

Fig. 3–14 *Application Object dialog*



- ***Insert Name and Application Object Description for easier identification.***
- ***Again, click New… to specify an application. The Application Entry Parameters window opens.***
- ***Click Browse and select the file you want to create the object for. After selection, the path to the file and its inherent file description will be displayed in the Path and Description fields below.***
- ***Optionally, insert a file description into the Comment field.***
- ***Specify Application Liability and Application Type. Momentarily, the classification is purely informational.***
- ***Click Generate to create an MD5 Hash in order to clearly identify the selected file, when it is executed.***

Caution

MD5 Hash creation is recommended in order to avoid corrupt file and a vulnerable PC after an attack.

Note

Consider that when an application equipped with an MD5 Hash is used on multiple clients, file versions need to match exactly. Otherwise, the application object will not be applicable.
Click ***Clear*** to delete the hash.

Warning

In addition to the application, first level DLLs are taken into consideration. This provides additional security. However, DLLs used by first level DLLs are not monitored.

The following application objects, that are required in Microsoft Windows domains, are available within the Barracuda NG Personal Firewall by default:

Table 3–6 *Applications required in Microsoft Windows domains*

Application	Connection	Description
System	**O / I**	Services needed by the OS kernel
TCP/IP Ping Command	**O / I**	
lsass.exe	**O**	Local Security Authority Service; process responsible for management of local security authority domain authentication and Active Directory management.
services.exe	**O**	Upon startup, services.exe enumerates through all registry sub-keys located in ***HKEY_LOCAL_MACHINE\Services*** registry key.
spoolsv.exe	**O**	The Windows Printer Spooler stores printer jobs and forwards them to the printer when it is ready.
userinit.exe	**O**	By default, WinLogon executes this application that triggers logon scripts, re-establishes network connections,…
winlogon.exe	**O**	This application manages security-related user interactions in Windows NT. It handles logon and logoff requests, changing the password,…
svchost.exe	**O**	This is a generic host process name for services that are run from dynamic-link libraries (DLLs). There can be multiple instances of svchost.exe running at the same time.

Chapter 4
Operating & Monitoring Barracuda NG NAC

4.1 Box – Monitoring and Real-time Information

The Access Control Service provides extensive information about the currently available endpoints and their status. Both, real-time and historical information are displayed when logging into the status window.

The following tabs are available for operational purposes:

- ***Status* tab**
- ***Status VPN* tab**
- ***Access* tab**
- ***Quarantine* tab**

4.1.1 Available Columns

The lists in the real-time information GUI consist of the following columns:

- ***Time***

Displays date and time of the last client access

- ***Hostname***

Displays the client's hostname as reported by the client.

- ***IP Address***

Client's IP address as reported by the client.

- ***User***

Either "Local Machine" if no user information is available or the name of the logged in user (DOMAIN\username).

- ***Status***

Current status of the client. Possible values are "Machine logged in", "User logged in" or "User logged off". Additionally the status "Out of time" is displayed if the client did not reconnect to the Access Control Service within the configured time period ("Access Control Service Settings > System Health-Validator > Health State Validity"). This is often caused by powered off clients or by interrupted network connectivity.

- ***Information***

Summary of the client's health status or more details of a failed connection. Values could be "Client is healthy". If the client is unhealthy, the column "Information" contains details about the failed health checks. "No rule matched", another possible information, means that identity matching failed.

- ***Healthstate***

Last health state, which could be one of the four "Healthy", "Unhealthy", "Probation", or "Untrusted".

- ***IsolationState***

Possible values are Access", "Not Restricted", or "Probation".

- ***Auth. (PHIBS)***

Result of the last authentication, which could be either "OK" or "Not OK".

- ***Rule***

Name of the matching policy rule.

- ***Boxname***

Originating box where the Access Control Service runs on (only relevant in CC Barracuda NG Network Access Client GUI context).

- ***Type***

Displays the type "Health Evaluator", "Authenticator" or "Remediation", depending on the Access Control Service module which created the entry.

- ***MAC Address***

Client's MAC address as reported by the NG client.

- ***SID***

Client's local machine Secure Identifier (SID) as reported by the NG client.

4.1.2 Filtering

All available tabs provide filtering options at the top of the Barracuda NG Access Monitor GUI.

Note

To activate a filter and refresh the Status list it is necessary to press the button "Update List".
Filters are case sensitive. Some of the filters provide a list of available entries, other filter criteria can be entered manually. For manual input there are wildcards ('*', '?') available. For example, Filter `10.0.8.1?` filters for IP addresses 10.0.8.10 to 10.0.8.19, the filter `10.0.8.1*` also matches 10.0.8.100 to 10.0.8.199.

The filter categories are split into Basic Filters and Advanced Filters. Depending on the currently selected tab some filters are not available or set as preselection.

The Basic Filter provides the following filter criteria:

- ***From date/dime***

Restrict the time period for which entries should be listed.

- ***Health State***

This filter provides the different health states "Healthy", "Unhealthy", "Probation", and "Untrusted" to display only the selected entries

- ***Isolation***

  The categories "Not restricted", "Restricted", and "Probation" are available as filter criteria.

- ***IP***

  Filters the list for specific IP addresses.

- ***User***

  Filters the list for specific user entries.

- ***Type***

  Filters the list for entries of type "Health Evaluator", "Authenticator", or "Remediation", depending on the Access Control Service module which created the entry.

- ***Client***

  Filters the list for entries of type "Local Machine", "VPN", or "User".

The advanced filter provides the following criteria:

- ***MAC***

  MAC-address of the client (sent by NG client, so even in routed environments the original MAC address will be available).

- ***SID***

  Filter for microsoft machine SID.

- ***Box***

  Filter for originating box where the Access Control Service runs on (only relevant in CC Barracuda NG Network Access Client GUI context).

- ***Rule***

  Matching policy rule.

- ***Auth***

  Filter on authentication status.

- ***Host***

  Filter on hostname.

- ***Status***

  Filter on client status ("User logged in", "Machine logged in", "Logged out", "Out of time").

By activating the corresponding checkboxes. it is possible to combine multiple fields in order to achieve a more precise selection.

4.1.3 Context Menus

Right-click a list entry to activate the following context menus:

- ***The standard context menu accessible through the Tools item (see Barracuda NG Firewall Administration Guidance)***
- ***Follow this Computer…***

By selecting this context menu entry on a selected entry all entries with the selected client are displayed in a new tab. Criteria for identifying a computer is the computer's local machine secure identifier (SID).

- ***Visualize this Computer…***

This entry visualizes the health state of the selected client. The graphical status at the top of the main window displays the summarized health state per day. Selecting multiple entries displays statistics of clients in state "Unhealthy", "Probation", and "Healthy".

For single entries, the summary displays a red icon to indicate an unhealthy client if it was unhealthy only once per displayed time period (day/week). Grey icons mean that no data is available for this date. This might e.g. indicate a client that is powered off.

Fig. 4–1 *Box – Monitoring and Real-time Information – Visualizing 2 Computers*

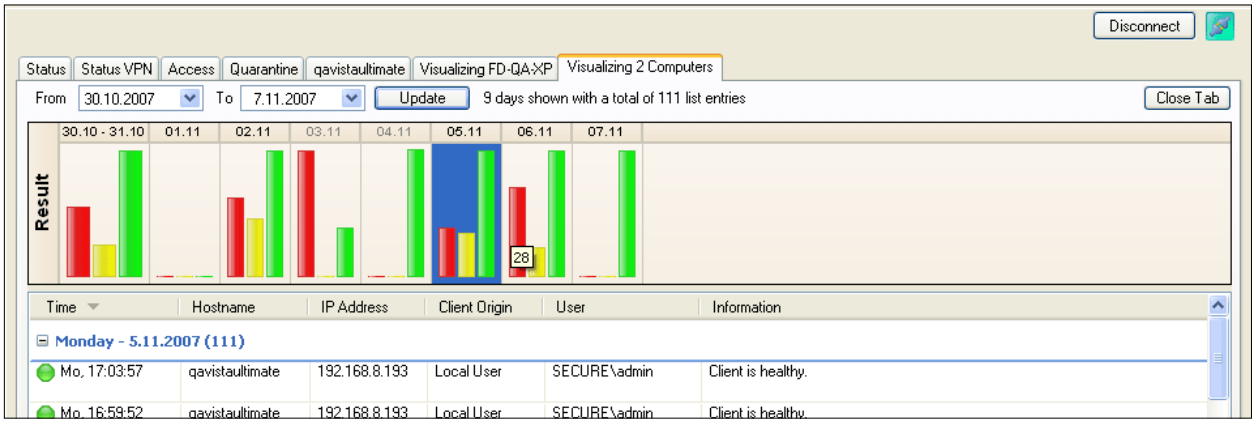
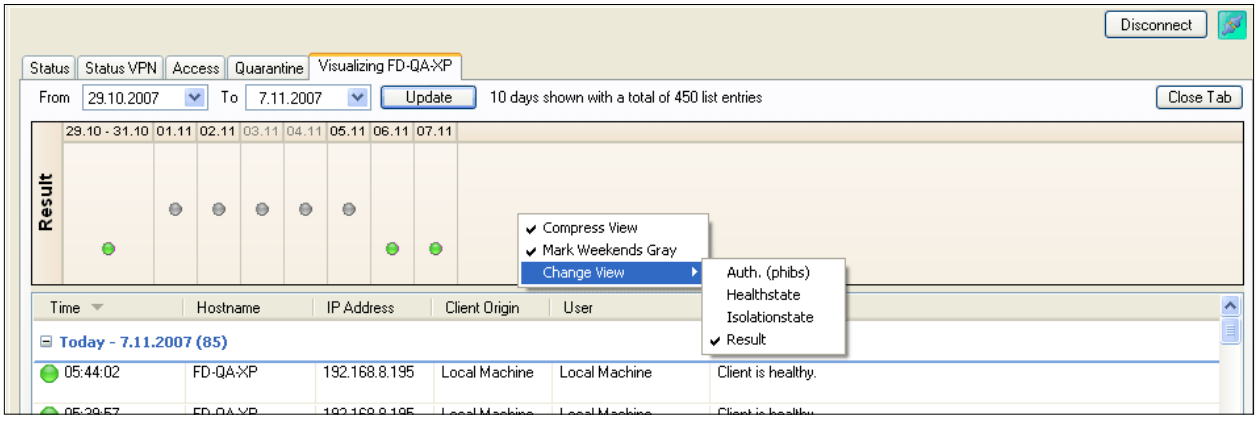


Fig. 4–2 *Box – Monitoring and Real-time Information – Visualizing FD-QA-XP*



- ***Show Log File…***

Displays the log entries relating to the selected client. Additionally, the access cache of the forwarding firewall can be displayed.

Note

Only log entries available on this Barracuda NG Firewall box will be displayed.

- ***Show Details…***

Displays detailed information about the selected client in a list view.

- ***Flush Cache >***

- ***Entry***
- ***This Computer***
- ***-ALL-***

Removes either the selected entry, or all entries belonging to the selected client, or all entries from the cache.

- ***Ungroup***

Displays all entries in a flat list instead of the default group view.

- ***Group by >***

For better lucidity, status entries may be grouped by their essential attributes such as time, IP address, or rule name. Entries are arranged in pop-up menus topped by a labelled title bar.

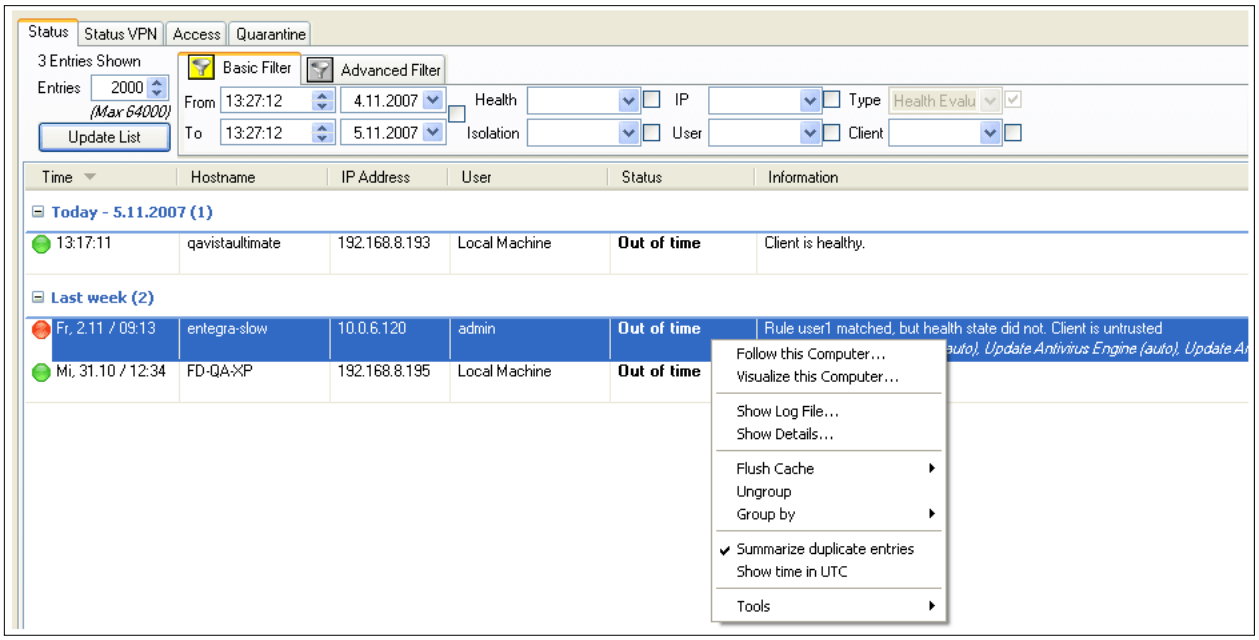
- ***Summarize duplicate entries***

Cumulate identical entries and in addition display the count (for example, how many entries are cumulated).

- ***Show time in UTC***

Show UTC time instead of Barracuda NG Firewall system timezone.

Fig. 4–3 *Box – Monitoring and Real-time Information – Show time in UTC*



4.1.4 Status Tab

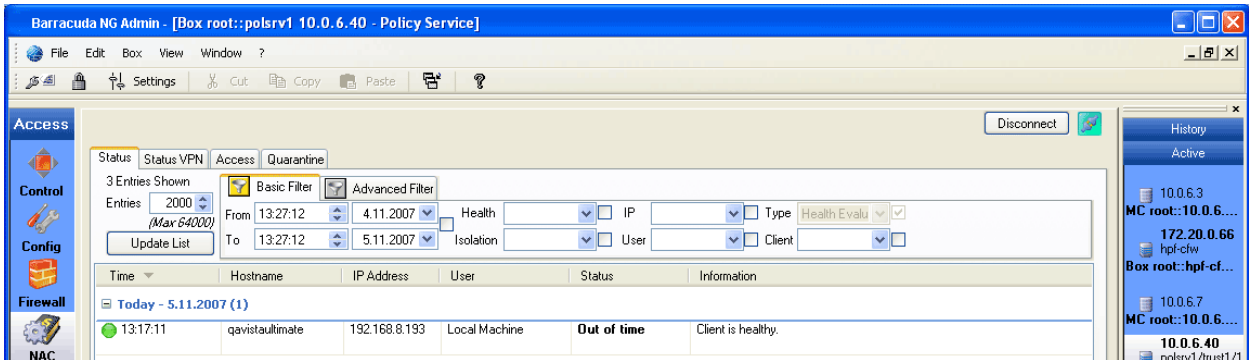
The Status tab summarizes the health information of all connected clients. The Barracuda NG Network Access Client framework does not depend on continuously established connections, but NG clients connect periodically to the Access Control Service. Thus the Status tab is able to display historical information of the clients, too. To update the list press ***Update List,*** since automatic updates are disabled.

As primary key, Barracuda NG Network Access Client uses the Microsoft Machine Secure Identifier (SID). The MS Machine SID is a unique value which could change only in case of severe hardware

modifications or re-installation of the operating system. This means that the Access Control Service can assign health states to the proper client even if the IP address changes or a user performs a logout.

The status tab displays only the last health status of a client. To get an overview of historical information, e.g. in order to display different states for a client but cumulate states if they were identical, change the view to the ***Access*** tab.

Fig. 4–4 *Box – Monitoring and Real-time Information – Status*



Note

Double-click an entry to open a new window where the Access Control Service logs corresponding to the appropriate entry are displayed. Optionally, the Firewall Access Cache may be displayed by pressing "Show Access Cache". Automatically an appropriate filter for the client's IP address is set. The cache selection includes forwarding and local-in and local-out traffic. This gives the administrators an easy way of trouble-shooting for their clients.

Alternatively, the full log entries are available via the ***Log Viewer*** module. The full Access Cache can be viewed in the Firewall GUI > Access Cache.

Both, log entries and firewall access cache, are only available if the the Access Control Service was active on the Barracuda NG Firewall box. Barracuda NG Firewalls do not sync their log files or the firewall access cache to the HA partner.

4.1.5 Status VPN Tab

This tab provides a subset of the information available in the Status tab. Only Barracuda NG Network Access Client Client connections established through VPN are enlisted. Manually applying filters in the Status tab results provides the same information.

4.1.6 Access Tab

The Access tab provides all information available for the Access Control Service. This includes health information (also displayed in the Status tab) and also data generated by the remediation module and the authenticator module.

4.1.7 Quarantine Tab

The Quarantine tab provides all information regarding clients which health state is unhealthy and which are therefore in quarantine.

Chapter 5
Client Installation

Installation files for VPN client installation are provided on the Barracuda NG Firewall Application CD-ROM. You may alternatively download the installation package from Barracuda Networks. An MSI file is additionally provided for software distribution systems.

Note

Copy the installation files onto the local hard disk before commencing installation.

Double-click `setup.exe` to start the installation routine.

Note

All Barracuda NG VPN client drivers are signed by Microsoft for Windows NT, Windows XP (32 Bit), Windows Vista (32 Bit and 64 Bit) and Windows 7 (32 Bit and 64 Bit) logo compliance.

Warning

Barracuda NG Network Access Client is not intended to work as complement to VPN clients and/or personal firewalls provided by other vendors. Thus, Barracuda Networks recommends to uninstall any other VPN client and/or personal firewalls prior to installation of Barracuda NG Network Access Client.
The only notable exception is the Microsoft Firewall which can be operated in conjunction with Barracuda NG Personal Firewall.

Caution

Installation requires administrator rights on the respective system.

Caution

For Microsoft Windows XP users it is highly recommended to have the official Service Pack 2 and recent hotfixes installed.

Warning

Take into consideration that the NG Personal Firewall is turned OFF by default and requires manual activation during the setup routine, or alternatively after successful installation.

The installation routine offers three basic ways of setup:

<Barracuda NG VPN client>, <Barracuda NG SSL VPN and NAC client>, <Custom>

- ***Barracuda NG VPN Client***
- ***Barracuda NG SSL VPN and NAC Client*** (complete installation)
- ***Custom***

A way to perform remote installation procedures is provided through customizable script files. Refer to the following chapters if you intend installing and configuring multiple clients remotely.

- ***Unattended Setup***

See 5.3 Unattended Setup, page 70

- ***Customer Setup***

See 5.4 Customer Setup, page 73

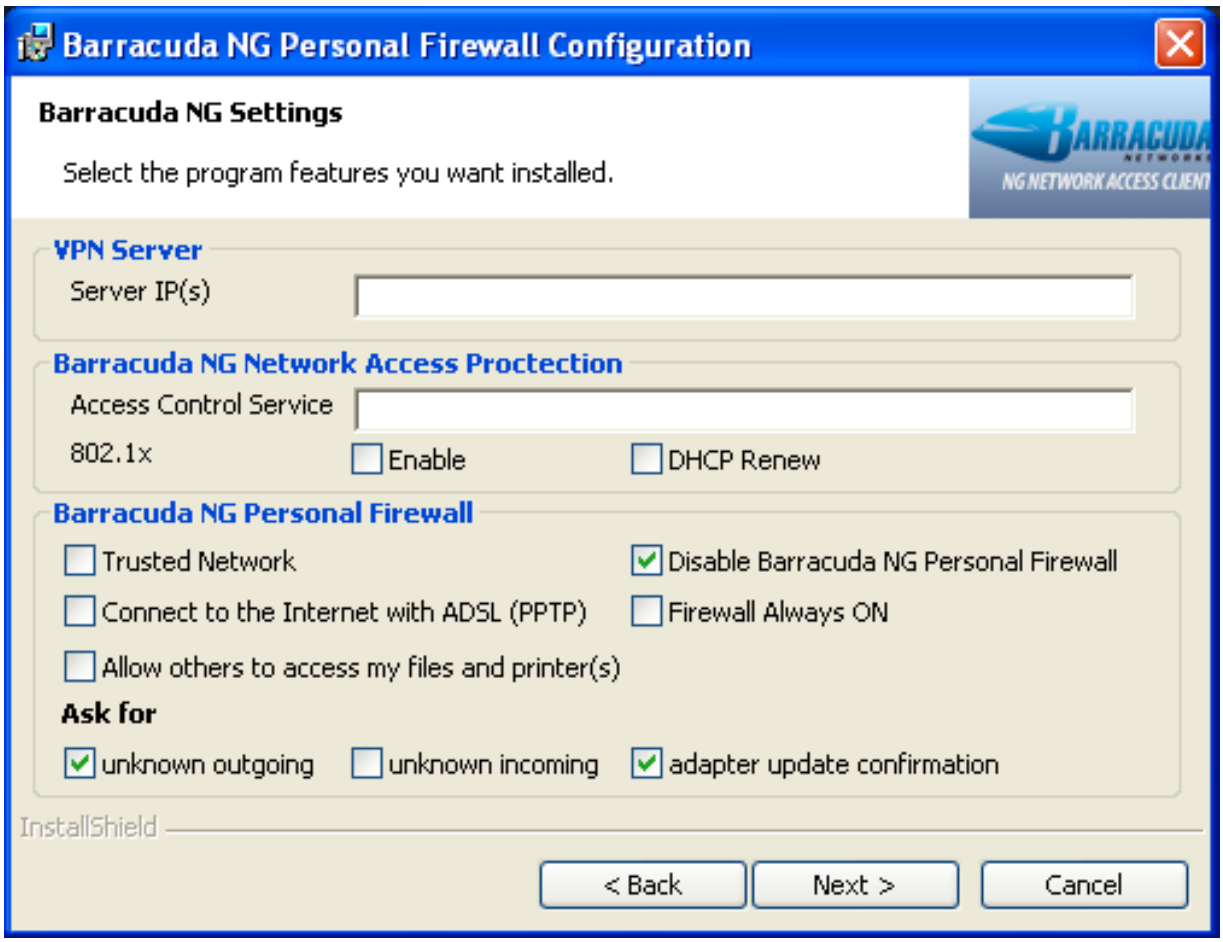
5.1 Complete Installation

The complete installation itself is a standard installation routine providing default settings (For example for connection behavior) for all product variants. Selecting this setup type does not require any deeper knowledge of the Barracuda NG Network Access Client. Simply follow the instructions on the screen.

Note

The following default settings apply when executing complete installation (details of these settings are described in 5.2 Custom Installation, page 70).

Fig. 5–1 *Complete Installation – default settings*



List 5–1 *Complete Installation — section Barracuda NG Access Monitor – default settings*

Parameter	Default
802.1x Enable	☐
DHCP Renew	☐

List 5–2 *Complete Installation — section NG Personal Firewall – default settings*

Parameter	Default
Trusted Network	☐
Connect to the Internet with ADSL (PPTP)	☐
Allow others to access my files and printer(s)	☐
Disable Barracuda NG Personal Firewall	☑
Firewall Always ON	☐

List 5–3 *Complete Installation — section Ask for – default settings*

Parameter	Default
unknown outgoing connections	☑
unknown incoming connections	☐
adapter update confirmation	☑

As soon as the installation procedure has completed, Barracuda NG Network Access Client is ready for use (for a feature list, see 8.2 Facts and Figures, page 83).

5.2 Custom Installation

This installation type is intended for experienced users. However, the basic settings defined during the installation routine require a deeper look, see table 5–1, page 71 and table 5–2, page 72.

5.3 Unattended Setup

Unattended installation procedure aims at concurrent remote installation and basic configuration of multiple clients and addresses the experienced system administrator.

Caution

Unattended setup requires administrator rights on the system where installation is executed.

Note

Msiexec (command-line options) apply for customisation of the installation procedure. For information on these options refer to
`http://technet2.microsoft.com/WindowsServer/en/library/9361d377-9011-4e21-8011-db371fa220ba1033.mspx?mfr=true`.

To specify non-default values for installation, Msiexec options may additionally be extended by

Barracuda NG Network Access Client specific properties. The available options for this purpose are listed in table 5–1 and table 5–2.

Save the following to a `.cmd` file and execute this file to trigger an unattended setup. Separate multiple specific properties with spaces:

Fig. 5–2 *Exemplary silent.cmd file for unattended setup*

```
@echo off
setup.exe /s /v"/qr CUSTOMER_INF=customer.inf PROGTYPE=R8 FW_NOTINSTALL=1"
```

Note

Specific properties must be inserted into one row.

Table 5–1 *Properties available for customisation of unattended setup*

Property	Value (*=default)	Corresponding Option in the Firewall Settings
DEFAULT_SHELL		Required when using another shell then explorer.exe (For example, Microsoft Embedded XP).
DHCPRENEW8021X	**0*** 1	Enable/disable 802.1X DHCP Renew
ENABLE8021X	**0*** 1	Enable/disable 802.1X
FW_ALWAYS_ON	**0*** 1	***Firewall Always ON***, page 72
FW_INSTALL_GINA	**0*** 1	Install Barracuda Networks GINA
FW_NOTINSTALL	**0*** 1	This option is for SMART-clients only, although SMART-clients still also work with installed firewall.
INSTALLDIR		Defines the installation path (`C:\Program Files\BarracudaNG`)
POLSRV_IP		Defines the IP address of the Access Control Server.
PROGTYPE		Installs selected product containing of: • ***NG Personal Firewall, VPN and system health validator*** • ***INSIDE - personal firewall and system health validator*** • ***R8 - personal firewall and VPN***
PROGTYPE	**VPN**	Chooses the VPN-only installation mode. Only the VPN client components will be installed.
PUB_CA_KEYCERT		Allows adding the name of the CA public certificate to the profile and requires adding the lines `copy certname.pem > nul` and `del certname.pem > nul` accordingly.
PWD	**[A secret password]**	Sets a password that will be requested prior to shutting down the client. It will not be possible for users to shut down the client without the correct password. Leaving the value blank removes the shutdown protection.

Note

The ***NG Personal Firewall*** settings can be edited after installation. For detailed information see 9.9 Administration - Firewall Settings Wizard, page 120.

- ***Trusted Network***

see description for parameter ***Trusted Network***, page 120

- ***Allow other to access my files and printer(s)***

see description for parameter ***Windows File Sharing***, page 120.

- ***Connect to the Internet with ADSL (PPTP)***

see description for parameter ***Connect to the Internet with ADSL (PPTP)***, page 120

- ***Ask for adapter update confirmation***

see description for parameter ***Ask for adapter update confirmation***, page 120

- ***Access Control Server Address***

This parameter defines the Access Control Server to be used.

- ***Ask for unknown outgoing/incoming connections***

Selecting these checkboxes causes a dialog to pop up for each unknown connection. Via this dialog the NG Personal Firewall rule set is modified automatically (9.9.2 Automatic Rule Configuration, page 122).

- ***Disable Barracuda Networks Secure Mode (Firewall off)***

Selecting this checkbox results in a "pass-all-behavior" of the NG Personal Firewall. Use this option for unattended setups.

- ***Firewall Always ON***

This option prevents deactivating the NG Personal Firewall.

Note

Any rule set which is assigned trough a policy- or VPN server will overwrite these options.

Table 5–2 *Properties available for customisation of unattended setup*

Property	Value (*=default)	Corresponding Option in the Firewall Settings
FW_TRUSTEDNETWORK	**0*** 1	***Trusted Network***, page 120
FW_SHARE	**0*** 1	***Windows File Sharing***, page 120
FW_ADSL	**0*** 1	***Connect to the Internet with ADSL (PPTP)***, page 120
FW_ASKOUT	0 **1***	***Ask for unknown outgoing connections***, page 120
FW_ASKIN	**0*** 1	***Ask for unknown incoming connections***, page 120
FW_ASKADAPTER	0 **1***	***Ask for adapter update confirmation***, page 120
FW_DISABLE	0 **1***	***Disable Barracuda Networks Secure Mode (Firewall off)***, page 72

5.4 Customer Setup

Note

The customer setup is only available for NG VPN Client

Customer setup is a comprehensive installation method, allowing you to fully preconfigure all NG Network Access Client settings on multiple installation systems remotely.

Customer setup addresses the experienced system administrator. In addition to pure installation and basic configuration, it allows you to:

- **Preconfigure an arbitrary number of connection profiles on the NG Network Access Client.**
- **Import license (.lic) files and X.509 certificates into the NG Network Access client.**
- **Import preconfigured rule sets into the NG Personal Firewall.**

Exemplary script files required for Customer Setup (`customer.inf`, `silent.cmd`) are available on the Application CD, allowing you to adapt the remote configuration procedure.

Caution

Customer setup requires administrator rights on the installation's target system.

Proceed as follows to prepare a completely customized setup:

1.) Edit the customer.inf file

See 5.4.1 customer.inf, page 73

2.) Edit the silent.cmd file

See 5.4.5 silent.cmd, page 78

3.) Copy the following files to the folder containing the setup.exe file:

- customer.inf
- silent.cmd
- active.i_fwrule (optional)
- [***LicenseName***].lic (optional)
- [***CertificateName***].pem (optional)

4.) Execute the silent.cmd file

5.4.1 customer.inf

Note

The syntax examples below are partly arranged in abstracts only. If needed as template, refer to the complete exemplary **customer.inf** file (15.1 customer.inf File Template, page 205).

The **customer.inf** file directs copying of required files and insertion of registry entries. It is divided into three sections of interest ("**Customer Areas**"):

- ***Customer Area [CustomerCopyFiles], page 74***
- ***Customer Area [CustomerReg], page 75***
- ***Customer Area [SourceDisksFiles], page 78***

Note

The content of the **customer.inf** file is treated case sensitive.

Warning

Do NOT rename the customer.inf file.

Caution

Remove nonessential parameters from the customer.inf file before applying it for Customer Setup.

Caution

The files customer.inf and silent.cmd are adapted to inclusion of a customer.lic file. If you are not importing a license (.lic) file during installation, delete the corresponding entries in both files. If you are using another name for the .lic file, do not forget to edit this file name within the installation files.

5.4.2 Section "1. Customer Area" / [PhionCustomerCopyFiles]

Fig. 5–3 *Example for section [CustomerCopyFiles]*

```
[PhionCustomerCopyFiles]

; destination-file-name[,source-file-name][,temporary-file-name][,flag]

customer.inf,,,2           ; important, do not remove
customer.lic,,,2           ; if importing a license file
active.i_fwrule,,,2        ; if importing a firewall rule set
```

Optionally, the following file-directives may be detailed:

Table 5–3 *File-directives applicable in the Customer Area" / [CustomerCopyFiles]*

Directive	Comment
destination-file-name	Specifies the name of the destination file. If no source-file-name is given, this specification is also the name of the source file.
source-file-name	Specifies the name of the source file. If the source and destination file names for the file copy operation are the same, source-file-name can be omitted.
temporary-file-name	Specifies the name of a temporary file to be created in the copy operation, if a file of the same name on the destination is open or currently in use. Only used on Windows 9x/Me platforms. The NT-based operating system automatically generates temporary file names when necessary and renames the copied source files the next time the operating system is started.
flag	These optional flags, expressed in hexadecimal notation or as a decimal value in a section entry, can be used to control how (or whether) a particular source file is copied to the destination. One or more (ORed) values for the following system-defined flags can be specified, but some of these flags are mutually exclusive:
0x00000400 (COPYFLG_REPLACEONLY)	Copy the source file to the destination directory only if the file is already present in the destination directory.

Table 5–3 *File-directives applicable in the Customer Area" / [CustomerCopyFiles]*

Directive	Comment
0x00000800 (COPYFLG_NODECOMP)	Copy the source file to the destination directory without decompressing the source file if it is compressed.
0x00000008 (COPYFLG_FORCE_FILE_IN_USE)	Force file-in-use behavior: do not copy over an existing file of the same name if it is currently open. Instead, copy the given source file with a temporary name so that it can be renamed and used when the next reboot occurs.
0x00000010 (COPYFLG_NO_OVERWRITE)	Do not replace an existing file in the destination directory with a source file of the same name. This flag cannot be combined with any other flags.
0x00001000 (COPYFLG_REPLACE_BOOT_FILE)	This file is required by the system loader. The system will prompt the user to reboot the system.
0x00002000 (COPYFLG_NOPRUNE)	Do not delete this operation to effectuate optimisation. For example, Setup might determine that the file copy operation is not necessary because the file already exists. However, the writer of the INF knows that the operation is required and directs Setup to override its optimisation and perform the file operation. (This flag can be used to ensure that files are copied if they are also specified in an INF DelFiles directive or an INF RenFiles directive.)
0x00000020 (COPYFLG_NO_VERSION_DIALOG)	Do not overwrite a file in the destination directory with the source file if the existing file is newer than the source file. This flag is irrelevant to digitally signed INF files. If a driver package is digitally signed, Setup installs the package as a whole and does not selectively omit files in the package based on other versions already present on the machine.
0x00000004 (COPYFLG_NOVERSIONCHECK)	Ignore file versions and overwrite existing files in the destination directory. This flag and the next two are mutually exclusive. This flag is irrelevant to digitally signed INF files.
0x00000040 (COPYFLG_OVERWRITE_OLDER_ ONLY)	Copy the source file to the destination directory only if the file on the destination will be superseded by a newer version. This flag is irrelevant to digitally signed INF files.
0x00000001 (COPYFLG_WARN_IF_SKIP)	Send a warning if the user selects to not copy a file. This flag and the next are mutually exclusive, and both are irrelevant to INF files that are digitally signed.
0x00000002 (COPYFLG_NOSKIP)	Do not allow the user to skip copying a file. This flag is implied if the driver package is signed.

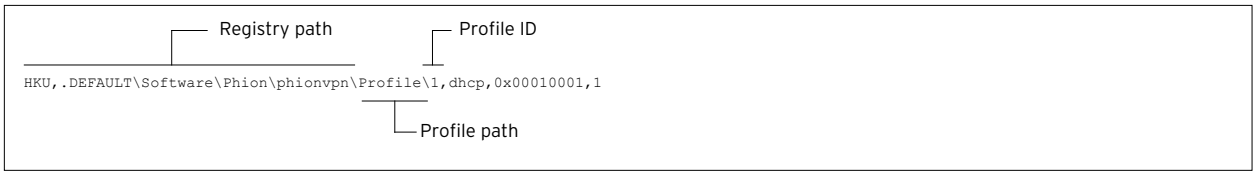
Note

Do not change the name of the firewall rule set entry (`active.i_fwrule`). If you do not intend installing the Barracuda Networks Firewall R8 with a predefined rule set meeting company policy, uncomment or delete this line.

5.4.3 Section "2. Customer Area" / [CustomerReg]

This section controls the configuration of profiles set up during installation. Profile settings are saved to `[HKEY_USERS\.DEFAULT\Software\Phion\phionvpn\Profile]`

Fig. 5–4 *Customer Setup – Profile settings*



For automated VPN profile creation, the following syntax is applicable in the **customer.inf** file:

```
reg-root, [subkey], [value-entry-name], [flags], [value]
```

This section is used for creating profiles and defining default values.

Table 5–4 *Directives applicable in the "Customer Area" / [CustomerReg]*

Directive	Comment
reg-root	Identifies the root of the registry tree for other values supplied in this entry. The value can be one of the following:
HKCR	Abbreviation for HKEY_CLASSES_ROOT
HKCU	Abbreviation for HKEY_CURRENT_USER
HKLM	Abbreviation for HKEY_LOCAL_MACHINE
HKU	Abbreviation for HKEY_USERS
subkey	This optional value, formed either as a %strkey% token defined in a Strings section of the INF or as a registry path under the given reg-root (key1\key2\key3…), specifies one of the following: A new subkey to be added to the registry at the end of the given registry path. An existing subkey in which the additional values specified in this entry will be written (possibly replacing the value of an existing named value entry of the given subkey). Both a new subkey to be added to the registry together with its initial value entry.
value-entry-name	This optional value either names an existing value entry in the given (existing) subkey or creates the name of a new value entry to be added in the specified subkey, whether it already exists or is a new key to be added to the registry. This value can be expressed either as "quoted string" or as a %strkey% token that is defined in the INFs Strings section. (If this is omitted for a string-type value, the value-entry-name is the default "unnamed" value entry for this key.) The operating system supports some system-defined special value-entry-name keywords. See the end of this Comments section for more information.
flags	This optional hexadecimal value, expressed as an ORed bitmask of system-defined low word and high word flag values, defines the data type for a value entry and/or controls the add-registry operation. Bitmask values for each of these flags are as follows:
0x00000001 (FLG_ADDREG_BINVALUETYPE)	The given value is "raw" data. (This value is identical to the FLG_ADDREG_TYPE_BINARY.)
0x00000002 (FLG_ADDREG_NOCLOBBER)	Prevent a given value from replacing the value of an existing value entry.
0x00000004 (FLG_ADDREG_DELVAL)	Delete the given subkey from the registry, or delete the specified value-entry-name from the specified registry subkey.
0x00000008 (FLG_ADDREG_APPEND)	Append a given value to that of an existing named value entry. This flag is valid only if FLG_ADDREG_TYPE_MULTI_SZ is also set. The specified string value is not appended if it already exists.
0x00000010 (FLG_ADDREG_KEYONLY)	Create the given subkey, but ignore any supplied value-entry-name and/or value.
0x00000020 (FLG_ADDREG_OVERWRITEONLY)	Reset to the supplied value only if the specified value-entry-name already exists in the given subkey.
0x00001000 (FLG_ADDREG_64BITKEY)	(Windows XP and later.) Make the specified change in the 64-bit registry. If not specified, the change is made to the native registry.
0x00002000 (FLG_ADDREG_KEYONLY_COMMON)	(Windows XP and later.) This is the same as FLG_ADDREG_KEYONLY but also works in a del-registry-section (see INF DelReg Directive).
0x00004000 (FLG_ADDREG_32BITKEY)	(Windows XP and later.) Make the specified change in the 32-bit registry. If not specified, the change is made to the native registry.
0x00000000 (FLG_ADDREG_TYPE_SZ)	The given value entry and/or value is of type REG_SZ. Note that this is the default type for a specified value entry, so the flags value can be omitted from any reg-root= line in an add-registry section that operates on a value entry of this type.
0x00010000 (FLG_ADDREG_TYPE_MULTI_SZ)	The given value entry and/or value is of the registry type REG_MULTI_SZ. This specification does not require any NULL terminator for a given string value.
0x00020000 (FLG_ADDREG_TYPE_EXPAND_SZ)	The given value entry and/or value is of the registry type REG_EXPAND_SZ.
0x00010001 (FLG_ADDREG_TYPE_DWORD)	The given value entry and/or value is of the registry type REG_DWORD.
0x00020001 (FLG_ADDREG_TYPE_NONE)	The given value entry and/or value is of the registry type REG_NONE.

Table 5–4 *Directives applicable in the "Customer Area" / [CustomerReg]*

Directive	Comment
value	This optionally specifies a new value for the specified value-entry-name to be added to the given registry key. Such a value can be a "replacement" value for an existing named value entry in an existing key, a value to be appended (flag value 0x00010008) to an existing named REG_MULTI_SZ-type value entry in an existing key, a new value entry to be written into an existing key, or the initial value entry for a new subkey to be added to the registry. The expression of such a value depends on the registry type specified for the flag as follows: • A registry string-type value can be expressed either as a "quoted string" or as a %strkey% token defined in a Strings section of the INF file. Such an INF-specified value need not include a NULL terminator at the end of each string. • A registry numerical-type value can be expressed as a hexadecimal (using 0x notation) or decimal number.

Note

The following describes only the minimum required information. You may add any other Barracuda Networks registry entry.

1.) Edit default entry

```
HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, Default, 0x00010001, 1
```

Value "1" sets a profile to the default profile of the Barracuda NG VPN Client. All other profiles take the value "0".

2.) Edit DHCP entry

```
HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, dhcp,        0x00010001, 1
```

Editing the value changes the value of the parameter ***Virtual Adapter Configuration***:

- ***Assign IP address manually***
- ***Use internal DHCP assignment (default)***
- ***Direct assignment***

3.) Edit profile name

```
HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, description, 0x00000000,
"profile name"
```

4.) Name the license (customer.lic)

```
HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, license,     0x00000000,
"%65600%\customer.lic"
```

Note

%65600% is used as placeholder for the installation directory.

5.) Enter IP address of the VPN server

```
HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, server,      0x00000000,
"192.168.0.1"
```

5.4.4 Section "3. Customer Area" / [SourceDisksFiles]

Fig. 5–5 *Example for section [SourceDisksFiles]*

```
 [SourceDisksFiles]
; Files for disk Customer Files #1
; filename = diskid[,[ subdir][, size]]

customer.inf,,,1
customer.lic,,,1           ; if a license file is imported
active.i_fwrule,,,1        ; if a firewall rule set is imported
```

A `SourceDisksFiles` section names the source files used during installation, identifies the installation disks that contain these files, and provides the path to the subdirectories, if any, on the distribution disks containing individual files.

The following directives are applicable:

`filename = diskid[,[ subdir][, size]]`

Table 5–5 *Directives applicable in the Customer Area" / [SourceDisksFiles]*

Directive	Comment
filename	Specifies the name of the file on the source disk.
diskid	Specifies the integer identifying the source disk that contains the file. This value and the initial path to the subdir(ectory), if any, containing the named file must be defined in a SourceDisksNames section of the same INF.
subdir	This optional value specifies the subdirectory (relative to the SourceDisksNames path specification, if any) on the source disk where the named file resides. If this value is omitted from an entry, the named source file is assumed to be in the path directory that was specified in the SourceDisksNames section for the given disk or, if no path directory was specified, in the installation root.
size	This optional value specifies the uncompressed size, in bytes, of the given file.

Note

Do not change the name of the firewall rule set entry (`active.i_fwrule`). If you do not intend installing the NG Personal Firewall with a predefined rule set meeting company policy, incomment or delete this line.

5.4.5 silent.cmd

Save the following to a `.cmd` file and execute this file to trigger an unattended customer setup. Separate multiple properties with spaces:

Fig. 5–6 *Exemplary silent.cmd file for unattended setup*

```
@echo off
setup.exe /s /v"/qr CUSTOMER_INF=customer.inf PROGTYPE=R8 FW_NOTINSTALL=1"
```

Note

Specific properties must be inserted into one row.

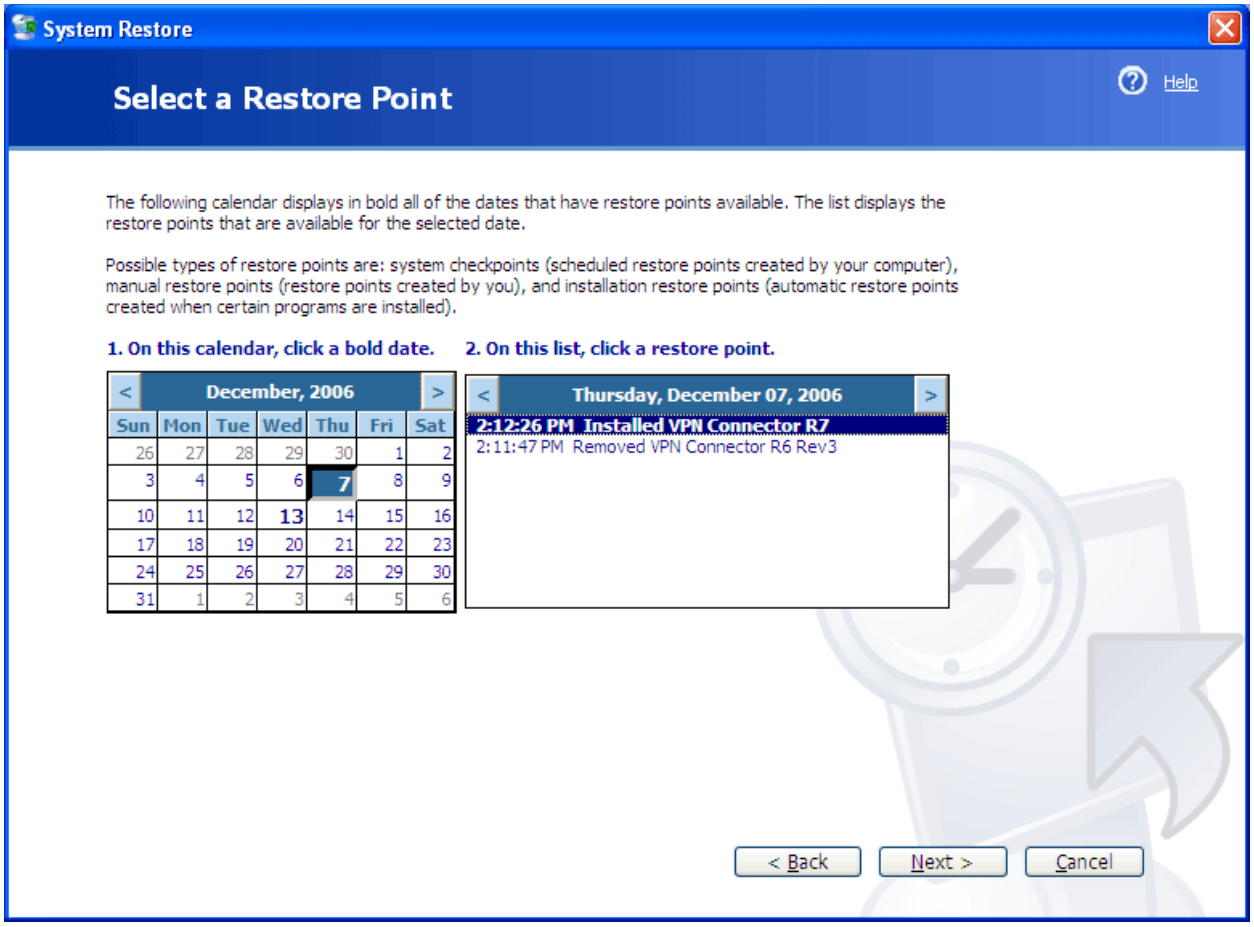
Note

For an overview of specific properties see table 5–1, page 71.

5.5 System Restore

Barracuda NG Network Access Clients installation and removal processes create **restore points** in the Windows **System Restore** area that you may use to restore your system to a previous state.

Fig. 5–7 *System Restore*



Refer to the OS help for details.

Chapter 6
Update or Migration

6.1 General

In case you are updating from predecessor versions, simply execute the setup executable and follow the on-screen instructions.

If you have particular questions regarding the migration process, then please contact the Barracuda Networks support.

Caution

For migration, it is mandatory to have the setup file locally on your system. A network installation is NOT possible. If the Personal Firewall is installed, make sure to disable the Internet connection prior to migration.

Note

After an update, the system needs to be restarted. Close all applications including the Barracuda NG VPN Client before rebooting the system.

Chapter 7
Uninstall

7.1 General

Note

Close all applications including the VPN client before uninstalling. You will be prompted to restart the system after uninstallation has completed.

7.2 Procedure

To uninstall the client, browse to ***Start > Control Panel > Add or Remove Programs > Barracuda NG Network Access Client*** and click ***Remove***.

Chapter 8
VPN Configuration

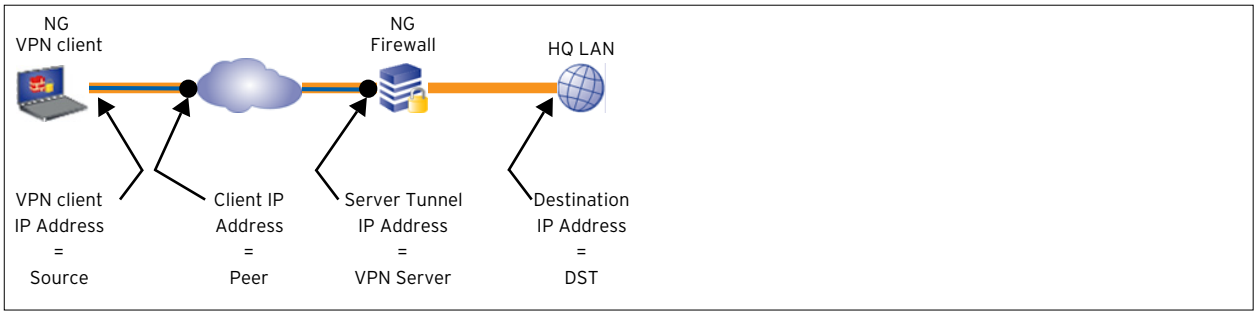
8.1 Overview

Virtual **P**rivate **N**etworks are an efficient and cost-saving way to use the internet as a transport alternative to dedicated lines or dial-up RAS overcoming the security risks of internet communications.

There are two well-established technologies for data encryption: IPSec and SSL (**S**ecure **S**ocket **L**ayer).

Most VPN implementations rely solely on IPSec, which has several disadvantages in modern network topologies. Barracuda NG VPN has incorporated both technology standards and hence improves the VPN connectivity substantially.

Fig. 8–1 *Structure of a VPN tunnel*



Barracuda Networks provides two types of VPN client licenses:

- ***Barracuda NG VPN Client***
- ***Barracuda NG SSL VPN and NAC***

Note

For detailed information concerning the different features of the two licenses, have a look at 8.2 Facts and Figures, page 83.

8.2 Facts and Figures

- ***VPN Licensing***

The ***Barracuda NG VPN Client*** license is included with every appliance. On box appliances, it allows for unlimited users, while on virtual appliances it is limited to the virtual appliance's capacity.

Optionally, the ***Barracuda NG SSL VPN and NAC*** subscription license is availabe. It enables SSL VPN functionality and includes Barracuda NG Network Access Client with the full client including the centrally managed Barracuda NG Personal Firewall.

- ***Authentication support***

Table 8–1 Authentication support

Function	Supported
Active Directory	✓
LDAP	✓
RADIUS	✓
MSNT	✓
RSAACE	✓
X509 certificates	✓
RSA tokens	✓
Smart cards	✓

- ***Personal firewall capabilities***

Table 8–2 Personal firewall capabilities

Function	Supported
Dynamic adapter object handling	✓
Dynamic user object handling	✓
RPC handling	✓
Multiple rule sets support	✓
Client side policy enforcement	✓

- ***Policy matching capabilities***

Table 8–3 Policy matching capabilities

Function	Comment
ID-based policies	✓
Support for ID-based Exemptions	✓, health condition and/or software update
Date and time conditions	✓
Access type	Support for internal and external category
Separate machine policies	✓
Separate policies	✓
Separate quarantine policies	✓
Machine properties	Microsoft operating system time, Microsoft SID, x.509 certificate (LocalMachine Account) with subject, issues, altname conditions, Hostname, MAC Address, network ACL, Netbios name
User properties	All of the above and login name and work group affiliation
Required client version	✓
Personal firewall active	✓

Table 8–3 Policy matching capabilities

Function	Comment
Antivirus (AV) product installed	✓
AV active	✓
AV realtime protection active	✓
Last AV scan time	✓
Enforce overdue AV scan	✓
AV engine version	✓
AV pattern version	✓
AV pattern max age	✓
Enforce overdue AV engine/pattern update	✓
AntiSpyware (AS) product installed	✓
AS active	✓
AS realtime protection active	✓
Last AS scan time	✓
Enforce overdue AS scan	✓
AS engine version	✓
AS pattern version	✓
AS pattern max age	✓
Enforce overdue AS engine/pattern update	✓
Personal firewall rule set	✓ [a]
Registry entries	✓ [a]
Welcome message	✓
Welcome picture	✓
C-ID support	✓
ID-based exemption from enforced client updates	✓
Gateway network access roles	✓

a. Not available for Barracuda NG VPN Client

- ***Usage Scenario***

Table 8–4 Usage Scenario

Function	Barracuda NG VPN Client	Barracuda NG SSL VPN and NAC
LAN protection	✓	✓
VPN remote access	✓	✓

- ***Architecture***

Table 8–5 Architecture

Function	Barracuda NG VPN Client	Barracuda NG SSL VPN and NAC
Integrated health agent	–	✓
Integrated VPN client	✓	✓
Integrated personal firewall	–	managed
Full entegra policy support		✓

- ***OS requirements***

Table 8–6 OS Requirements

Function	Barracuda NG VPN Client	Barracuda NG SSL VPN and NAC
Operation systems	Windows XP (32-Bit), Windows Vista (32-bit/64-bit), Windows 7 (32bit/64bit)	
Disk space	30 MB	
RAM	512 MB / 1024 MB (Vista)	
Processor	Intel 1.3 GHz	

Chapter 9
Barracuda NG Personal Firewall

9.1 Overview

The Barracuda NG Personal Firewall is a lighter version of the Barracuda NG Firewall especially designed for client usage. Nevertheless, most configuration options of the Barracuda NG Firewall are available. When connected to an Access Control Service or via VPN, the Barracuda NG Personal Firewall can accept rule sets sent from the Barracuda NG Firewall (depending on the used client license).

Open the configuration mode of the Barracuda NG Personal Firewall by right-clicking (VPN status) in the system tray and selecting **NG Personal Firewall** from the context menu or by browsing to **Start > All Programs > Barracuda NG Network Access Client > NG Firewall**.

Selection between the following functional firewall modes is available in the context menu of the system tray icon:

- ***Block All***
- ***Barracuda Networks Secure Mode***
- ***Disable Firewall (Allow all Traffic)***

The active operational mode is selected. To change the mode, click another item in the menu.

Warning

DO NOT directly switch from ***Disable Firewall (Allow all Traffic)*** to ***Block All***. Always select ***Barracuda Networks Secure Mode*** as intermediate step.

Each rule in a Barracuda NG Personal Firewall rule set is constructed from a variety of configuration entities (***Adapters***, ***Networks***, ***Services***, ***Applications***, ***Users***), which can be created and maintained independently from the rule set itself. They are then pieced together building a logical formation. Each configuration entity may be accessed from the ***Configuration*** sub-menu in the left navigation bar.

The ***Configuration*** section of the Barracuda NG Personal Firewall complements the automatic configuration mechanisms made available by the Firewall Settings Wizard in the ***Administration*** section (**9.9 Administration - Firewall Settings Wizard, page 120**). It allows you to:

- **Create rules from scratch in the *Rules* view (9.8.2 Rules, page 104).**
- **Modify objects and rules that have been created automatically determined through settings in the *Administration* view (9.9 Administration - Firewall Settings Wizard, page 120).**

- **Modify objects and rules that have been created in the *History* view by selecting *Add Pass/Block - Traffic Policy…* from the context menu (9.6.3 History, page 97)**

Note

Firewall administration experience is recommendable before manipulating the Barracuda NG Personal Firewall manually.

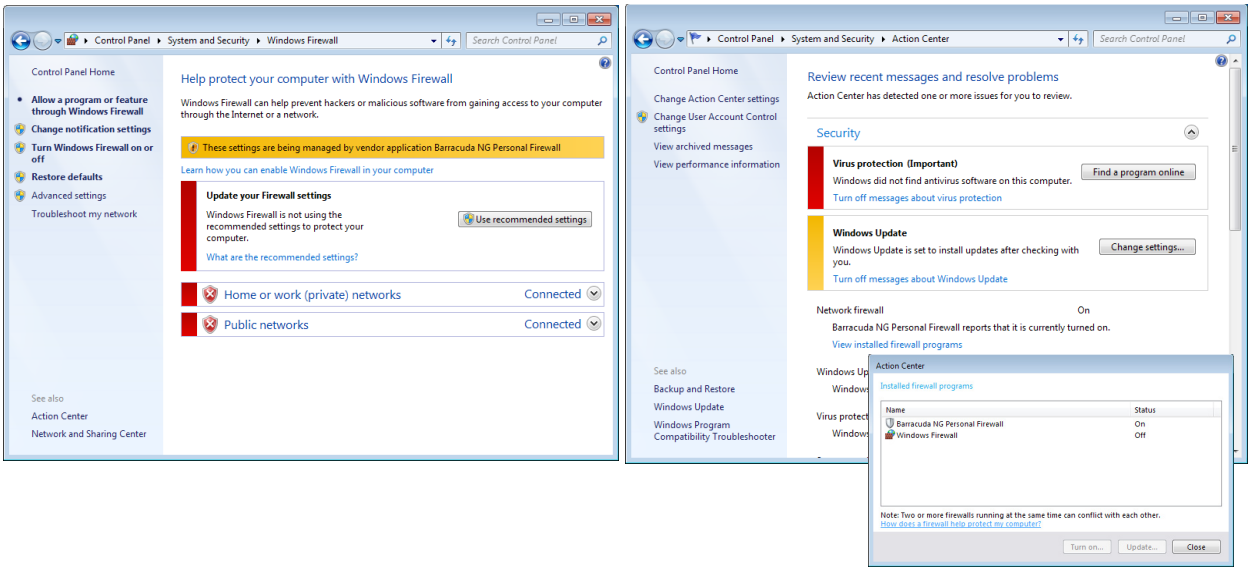
9.1.1 Integration within Windows 7

The Barracuda NG Personal Firewall integrates with Windows 7's intrusion control system. If configured to do so in ***Firewall Settings > Firewall Settings > Disable Windows Firewall***, it will properly replace the built-in Windows Firewall as long as it is enabled.

Disabling the Barracuda NG Personal Firewall will automatically re-enable the Windows Firewall.

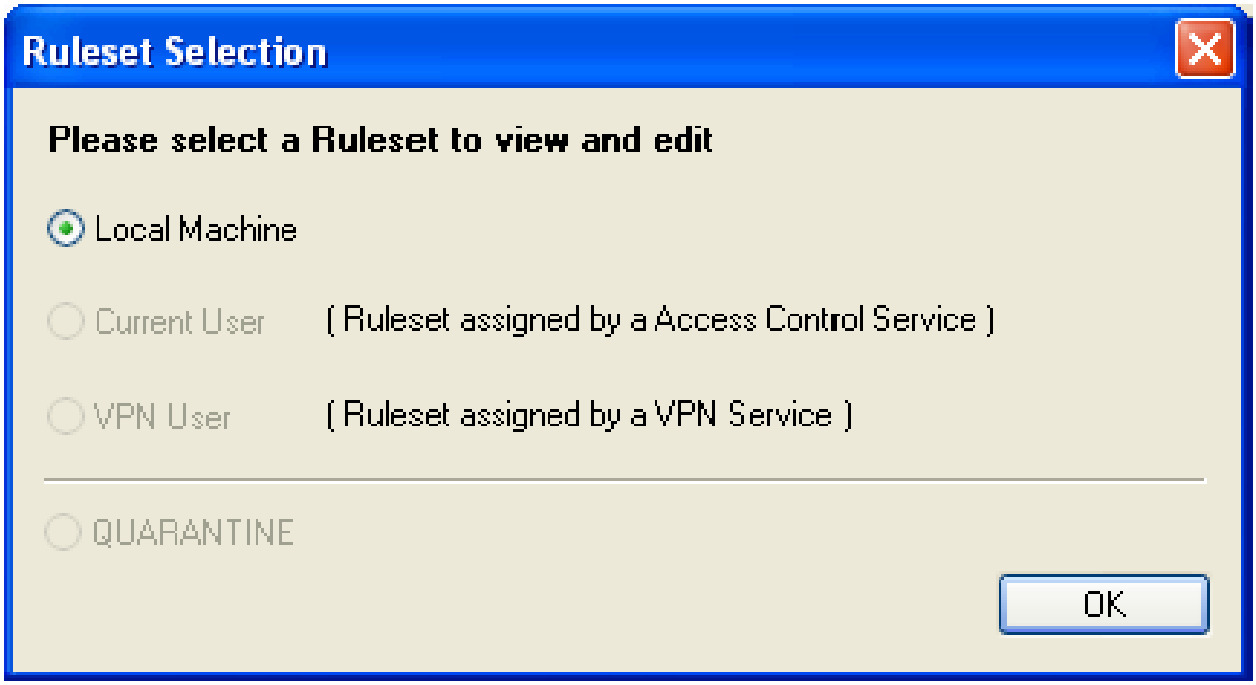
You can view the current protection status in your Windows 7 system within ***Control Panel > System and Security > Windows Firewall*** and within ***Control Panel > System and Security > Action Center***:

Fig. 9–1 *Windows 7 Windows Firewall and Action Center screens*



9.2 Rule Set Selection

Fig. 9–2 *Rule set selection*

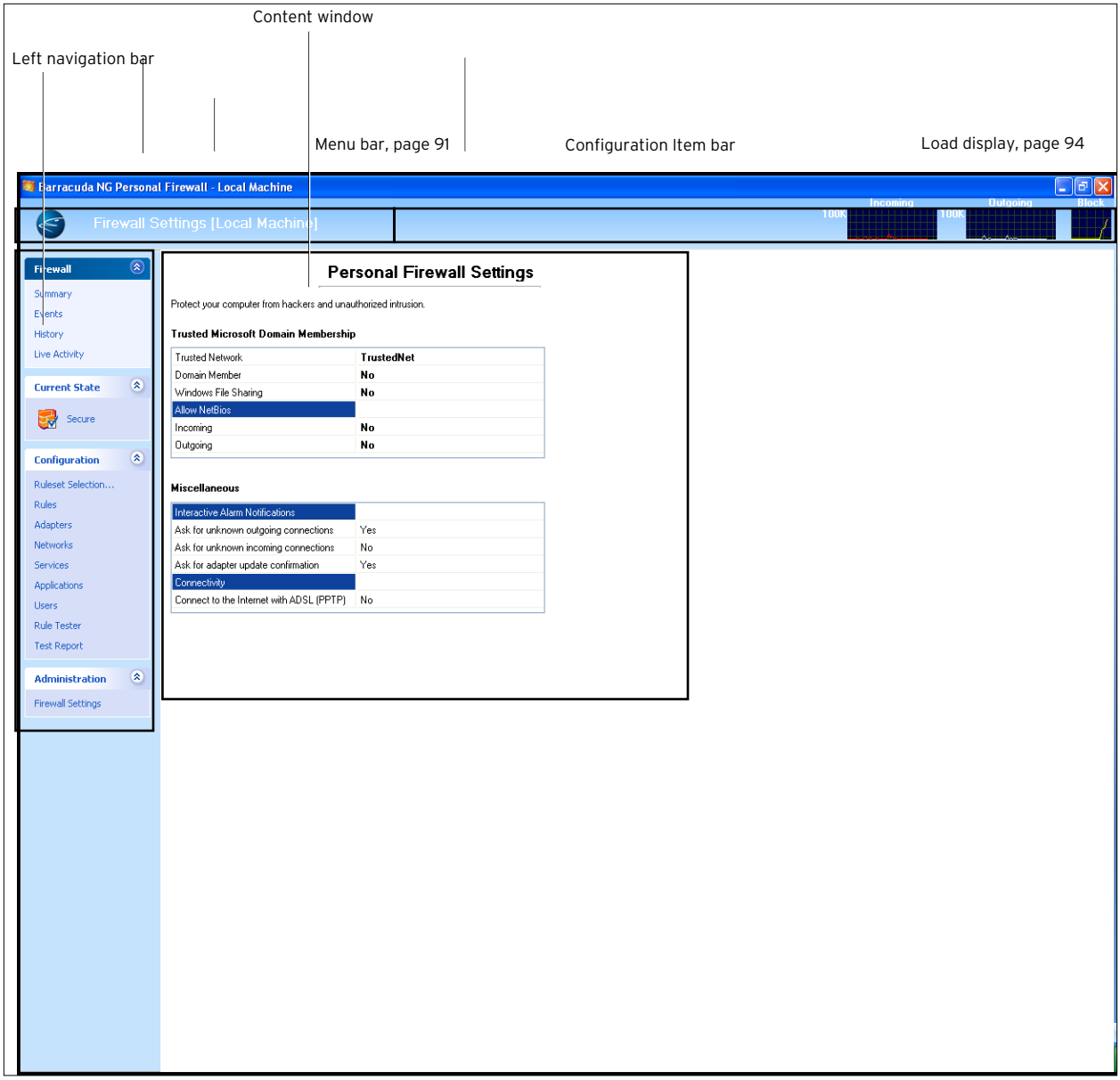


Click ***Rule Set Selection…*** to select one of the available rule sets for viewing. The Local Rule Set is selected by default. Only the Local Rule Set may be edited in the Barracuda NG Personal Firewall.

9.3 User Interface

The graphical user interface of the Barracuda NG Personal Firewall is built up of the following items:

Fig. 9–3 *Graphical Interface of the Barracuda NG Personal Firewall*



9.4 General Firewall Settings and Tasks (Menu Bar)

The following configuration items of the Barracuda NG Personal Firewall are accessible through the Menu Bar (use the ALT key to open/close the menu bar):

- ***Firewall***

see 9.4.1 Firewall Menu, page 91

- ***View***

see 9.4.2 View Menu, page 93

- ***Security Mode***

see 9.4.3 Security Mode Menu, page 94

9.4.1 Firewall Menu

- ***Save Configuration***

Select this item to save configuration changes immediately.

Note

Click the ***Save Configuration*** link within the ***Configuration*** Item bar to save configuration changes after prior confirmation inquiry.

- ***Settings…***

Select this item to adjust general behavior of the Barracuda Barracuda NG Personal Firewall. The following parameters are available for configuration.

Firewall Settings Tab:

List 9–1 Firewall Settings › Protocol Option

Parameter	Description
Log dropped packets/Log successful connections	Select these checkboxes to activate logging for dropped packets and/or successful connections. Log line structure is depicted in figure 9–5.

List 9–2 Firewall Settings › Protocol File

Parameter	Description
File name	This field defines path and name of the NG VPN client log file. By default, the file is saved to `C:\Program Files\BarracudaNG\phlog.txt`
Size limit	This field defines a maximum size for the log file (default: ***4096*** KByte).

List 9–3 Firewall Settings › Network Objects

Parameter	Description
IP Monitor	Selecting this checkbox (default: selected) activates dynamic update of ***Network Objects*** (9.8.7 Networks, page 110).

List 9–3 Firewall Settings › Network Objects

Parameter	Description
Automatic Adapter Assignment	Selecting this checkbox (default: selected) activates dynamic update of network interface adapters. When active, network adapters are automatically added to the ***Adapter Objects*** configuration area, when they are used the first time (9.8.6 Adapters, page 108).

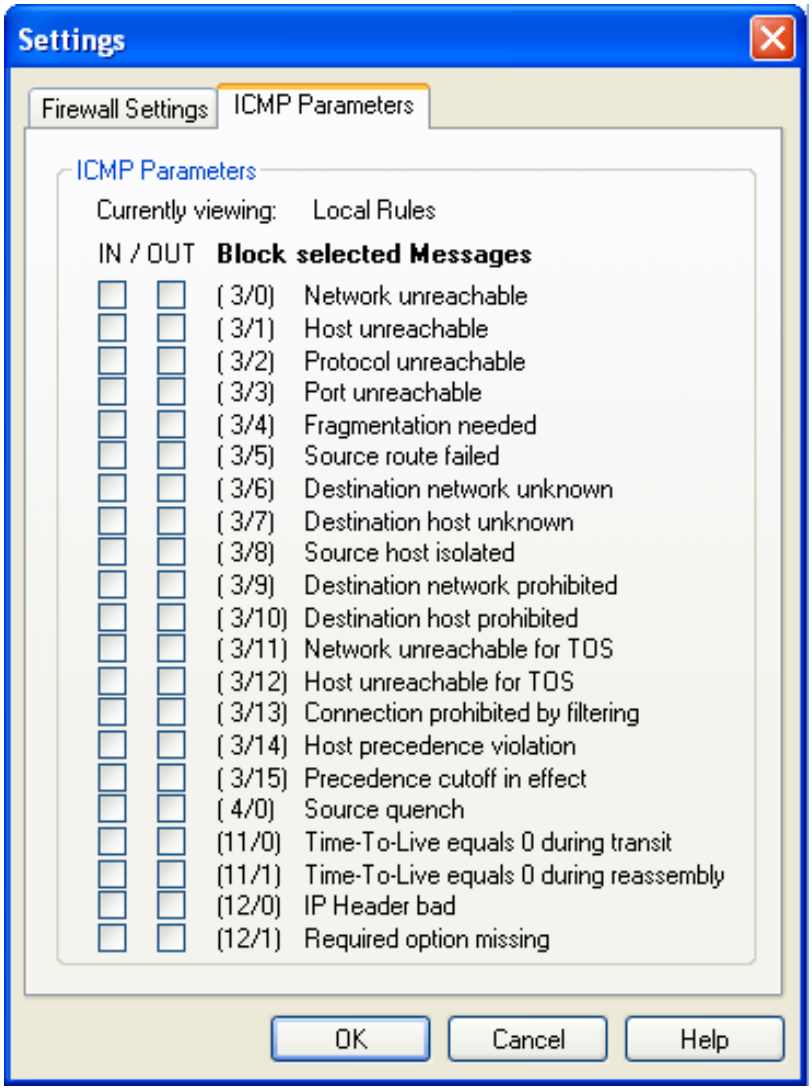
List 9–4 Firewall Settings › Firewall Settings

Parameter	Description
Disable Windows Firewall	Selecting this checkbox disables the Windows Firewall if it is installed (default: selected).
Block all IP Fragments	By default, IP fragments may generally pass the firewall notwithstanding the configured rule set. Select this checkbox to block IP fragments.
Passthru all IPv6 Packets	By default, IPv6 packets may generally pass the firewall notwithstanding the configured rule set. Select this checkbox to block IPv6 packets.

ICMP Parameters Tab:

This tab allows you to configure blocking of ICMP packets.

Fig. 9–4 *ICMP Parameters*



- ***Export Firewall Rule Set…***

This item allows you to export the rule set from the Barracuda NG Personal Firewall to a text file.

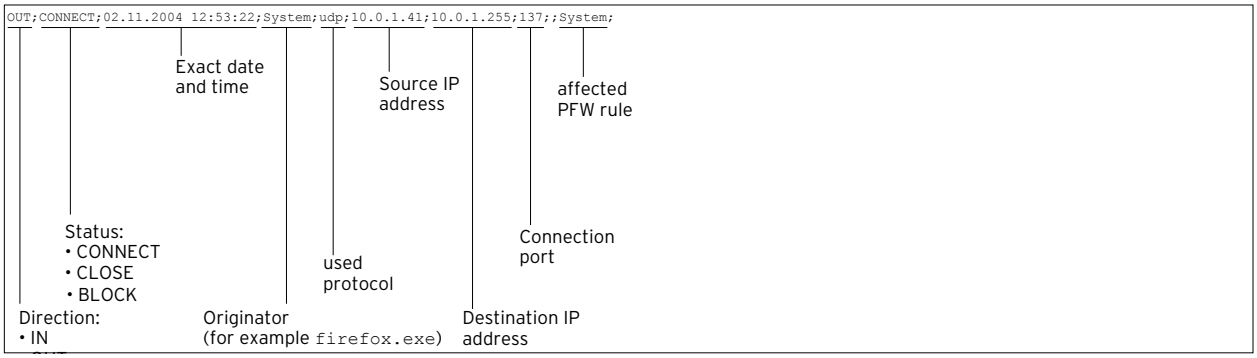
- ***Import Firewall Rule Set…***

This item allows you to import a rule set into the NG VPN client. The rule set may either originate from another Barracuda NG Personal Firewall or from a firewall configured on a Barracuda NG Firewall.

- ***Close Firewall Window***

Selecting this item closes the Barracuda NG Personal Firewall configuration window.

Fig. 9–5 *Logging syntax of the phlog.txt file*

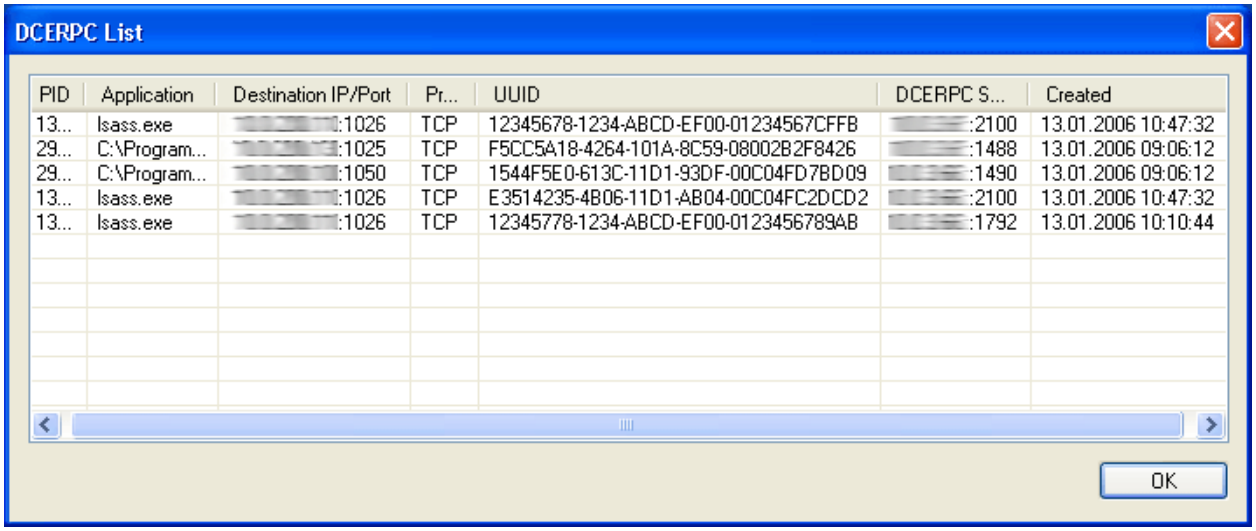


9.4.2 View Menu

- ***DCERPC List***

This dialog displays the status of each DCERPC communication slot (for detailed information concerning DCERPC, please consult the Barracuda NG Firewall Administrator's Guide).

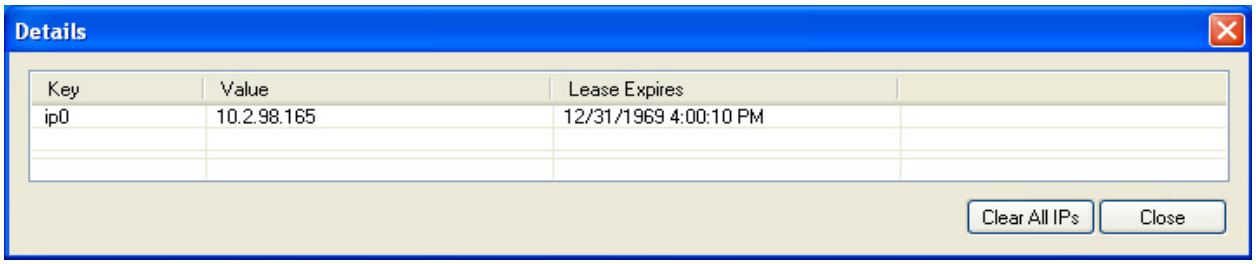
Fig. 9–6 *DCERPC List*



- ***Access Control Server IPs…***

Displays every Access Control Server the client knows of.

Fig. 9–7 *Access Control Server IPs*



9.4.3 Security Mode Menu

The items in the Security Mode menu allow you to adjust the security level of the Barracuda NG Firewall.

- ***Block All***

Prohibit all traffic.

- ***Disable Firewall (Allow All Traffic)***

Turn the firewall off and allow all traffic.

- ***Barracuda Networks Secure Mode***

Activate customized firewall rule sets.

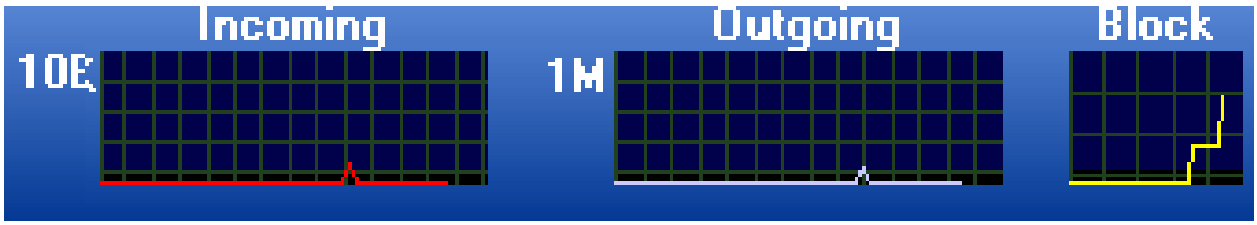
- ***Process Monitor***

Generate an entry in the event monitor for every process initiation (9.6.2 Events, page 96).

9.5 Load Display

The load display is a graphical view of current ***Incoming*** and ***Outgoing*** connections. The dimensions of the graphs depend on the current peak load. The last graph (***Block***) depicts the amount of blocked connections.

Fig. 9–8 *Load display*



9.6 NG Control Center - Monitoring Firewall Activities

Items arranged in the NG Control Center give a review of application activities in the Barracuda NG Personal Firewall. The NG Control Center is divided into the following sub-items:

- ***Summary***

see 9.6.1 Summary, page 95

- ***Events***

see 9.6.2 Events, page 96

- ***History***

see 9.6.3 History, page 97

- ***Live Activity***

see 9.6.7 Live Activity, page 100

9.6.1 Summary

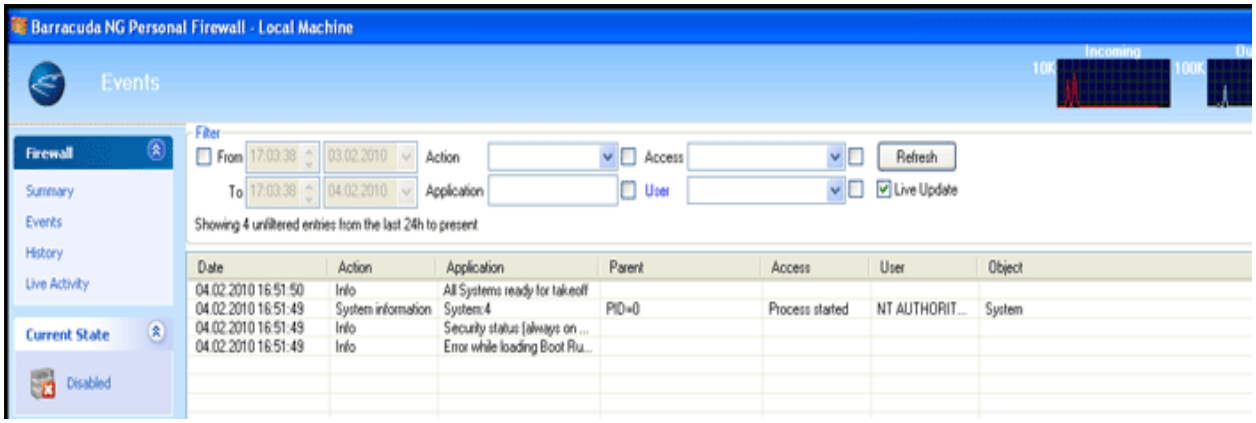
This view gives a quick comparison overview of the 5 most-used ***ports***, ***active internet,*** and ***blocked applications***.

Fig. 9–9 *NG Control Center: Summary window*

9.6.2 Events

The ***Events*** view details all applications that are currently or have been executed on the machine, irrespective, if they have requested passing the firewall. Double-click a list entry to view event details. Select ***Reload Logs*** from the context menu to reload the display of logged entries.

Fig. 9–10 *NG Control Center: Events window*



The listing is divided into the following columns:

Table 9–1 *Event view details*

Column	Description
Date	Date and time the connection has been initiated.
Action	Type of the recorded action: ***System Information***, ***Monitored*** connection, or ***Info***rmational message.
Application	The application that has initiated the connection and assigned port over which the connection is processed.
Parent	Parent process required that has initiated the application.
Access	Status and direction assigned to the connection. An application can be either in status ***Process started*** or ***ended***, and the connection direction can either be ***Outbound*** or ***Inbound***.
User	The ***User Object*** assigned to the connection (9.8.10 Users, page 117).
Object	Complete path to the application that is responsible for the connection.

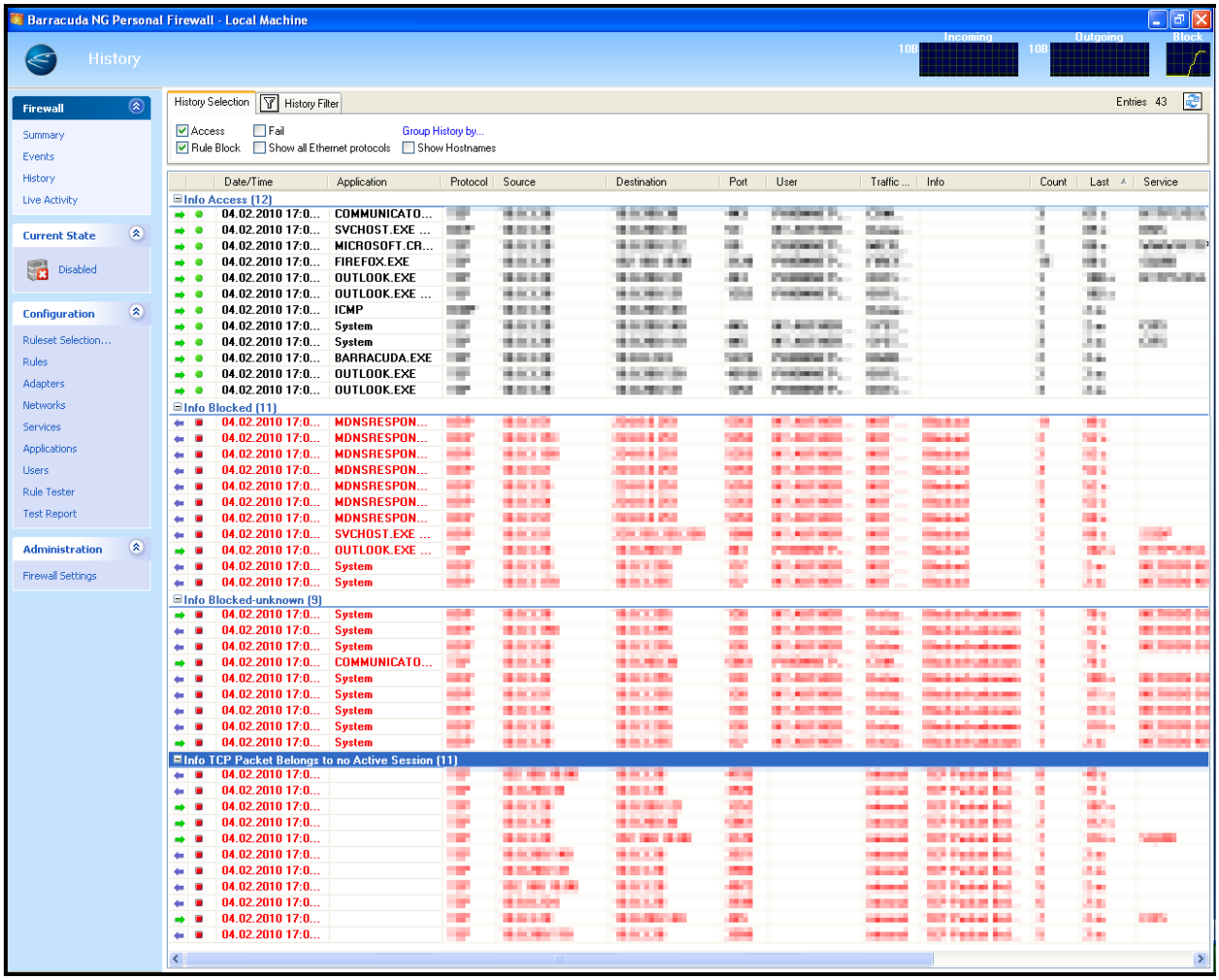
Filter Section*:*

The Filter section allows you to define filters in order to narrow down the view in the event listing. Select the checkbox assigned to an item to activate filter effectiveness and select or insert the desired filter value. Click ***Refresh*** to apply filter settings.

9.6.3 History

The ***History*** view details the entire network traffic (established connections and connection attempts) since the last system boot.

Fig. 9–11 *NG Control Center: History window*



9.6.4 Listing and Context Menu

The listing is divided into the following columns:

Table 9–2 *History window details*

Column	Description
Direction	Flags the connection direction (outgoing connections; incoming connections).
Connection State	Flags the connection state (granted connections; blocked connection attempts; failed connection attempts).
Date/Time	Date and time of traffic initiation.
Application	Name of the application.
Protocol	Protocol assigned to the application.
Source	Source IP of the connection.

Table 9–2 *History window details*

Column	Description
Destination	Destination IP of the connection.
Port	Connection port.
User	Name of the user who has initiated the connection attempt.
Traffic Policy	Name of the effective firewall rule.
Info	Connection status (passed, blocked, failed).
Count	Total number of connections processed over this slot.
Last	Expired time since last traffic over this slot.
Service	Affected service object or UUID (**U**niversal **U**nique **ID**entifier).
Adapter	NIC that was used for connection.
AID	Unique **A**ccess **ID** of the connection.

Select and then right-click a list entry to display the following context menu:

Table 9–3 *History window - Context menu*

Item	Description
Show Details	Select Show Details or double-click a list entry to view a summary of connection details.
Resolve Source/Destination IP	Tries to resolve the source/destination IP and summarizes the results (port, IP address, hostname and description) in a separate window.
Send to Rule Tester	Inserts the connection details into the rule tester and opens the rule tester window.
Add Pass Rule	Inserts the connection details into a new rule with default action ***Pass*** and opens the rule object window for editing.
Add Block Rule	Inserts the connection details into a new rule with default action ***Block*** and opens the rule object window for editing.
Flush History	Clears all entries from the history listing.
Ungroup	Undoes the group view and sorts connection entries into a successive listing.
Group by	Groups listing entries by the selected item.

9.6.5 History Selection Tab

In the ***History Selection*** tab, the following checkboxes are available for fast and easy filtering.

- ***Access***

  Only displays connections that have been granted (marked with).

- ***Rule Block***

  Only displays connection attempts that have been blocked (marked with).

- ***Fail***

  Only displays connection attempts that have failed (marked with).

- ***Show all Ethernet protocols***

  Additionally displays connection attempts over protocols other than TCP, UDP and ICMP.

- ***Show Hostnames***

Translates IP addresses into hostnames, if possible.

After each selection change, click to refresh the view. Click the ***Group History by*** link to sort listing entries by topic.

9.6.6 History Filter Tab

In the ***History Filter*** tab, filter conditions can be set to confine the view to the minimum wanted amount of entries. If filters apply, the ***History Filter*** tab is highlighted in yellow ().

Select the checkbox on the right side of an available filter to activate it and insert the condition to apply.

- ***Policy***

filters the connection's Traffic Policy

- ***Source***

filters the source IP address of the connection

- ***Application***

filters the application which has attempted to connect

- ***In/Out***

filters incoming or outgoing connections

- ***Protocol***

filters a connection protocol

- ***Destination***

filters the destination IP address of the connection

- ***Port***

filters a connection port

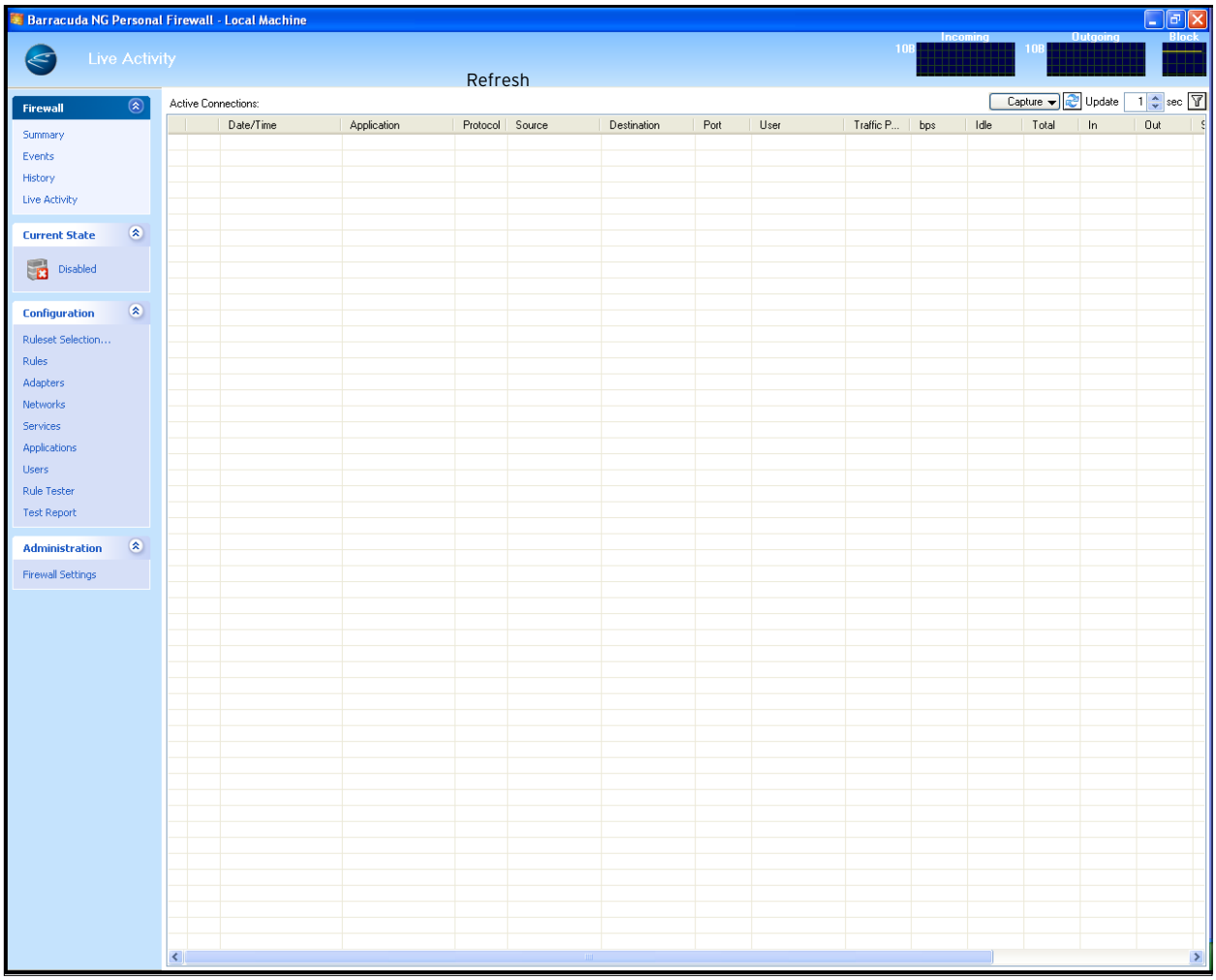
- ***Show matching entries/Hide matching entries***

select between displaying and hiding the matching entries

9.6.7 Live Activity

The ***Live Activity*** view details all currently active connections.

Fig. 9–12 *NG Control Center: Live Activity window*



9.6.8 Listing and Context Menu

The listing is divided into the following columns:

Table 9–4 *Live Activity window details*

Column	Description
Direction	Flags the connection direction (outgoing connections; incoming connections).
Load	Displays the current connection load (to).
Date/Time	Date and time of traffic initiation.
Application	Application name and its PID (**P**rocess **ID**).
Protocol	Protocol assigned to the application.
Source	Source IP of the connection.
Destination	Destination IP of the connection.
Port	Connection port.
User	Name of the user who has initiated the connection attempt.
Traffic Policy	Name of the effective firewall rule.
bps	Connection load in bits per second.
Idle	Idle time of the connection.
Total	Total amount of data transfer, that is sum of incoming (column ***In***) and outgoing (column ***Out***) traffic.
Start	Expired time span since connection initiation.
Service	Affected service object or UUID (**U**niversal **U**nique **ID**entifier).
ID	Internal slot ID.
Session Timeout	Effective connection state or current session timeout value.

Select and right-click a list entry to display the following context menu:

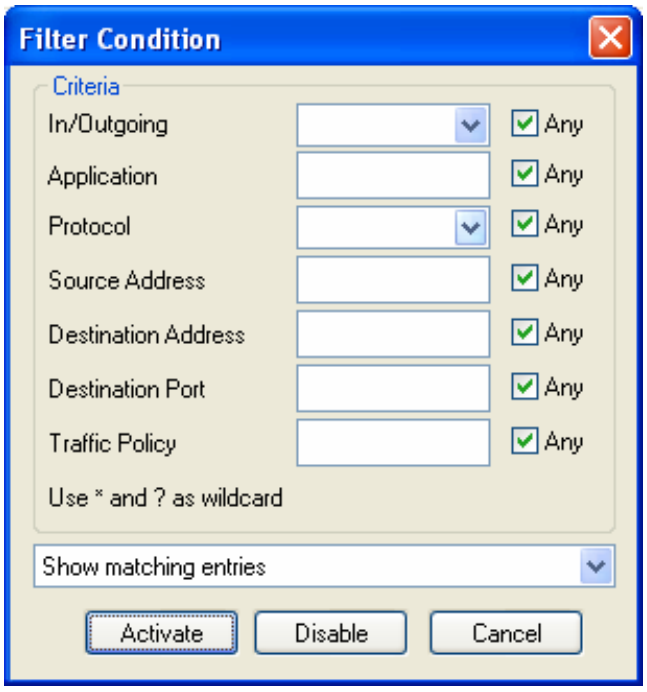
Table 9–5 *Live Activity window - Context menu*

Item	Description
Show Details	Select Show Details or double-click a list entry to view a summary of connection details.
Disconnect	Terminates the selected connection.
Resolve Source/Destination IP	Tries to resolve the source/destination IP and summarizes the results (port, IP address, hostname and description) in a separate window. **Note:** Entries displayed in italic indicate closed connections waiting for RST-ACK (**re**s**e**t **ack**nowledgement). The RST-ACK must be awaited in order to avoid its blocking by the firewall.

9.6.9 Filter Conditions

Click the filter button ( ) to open the ***Filter Condition*** window. This allows you to specify filter conditions in order to confine the view to the minimum wanted amount of entries.

Fig. 9–13 *Filter condition*



Click ***Activate*** to activate the filter settings. Click ***Disable*** to deactivate the filter settings.

After having specified a filter, click to refresh the view.

Click ***Capture*** to record traffic processed over the network interface.

Note

Administrator rights are required to use the ***Capture*** option.

Fig. 9–14 *Capture options*

The data acquired is saved as a CAP file in the local folder of the VPN client (`C:\Program Files\BarracudaNG`).

Note

A special viewer is needed (for example `wireshark; www.wireshark.org`, for viewing network traffic recorded in .cap files.

9.7 Current State - Setting the Security Mode

Clicking the link below this navigation item changes the effective state of the Barracuda NG Personal Firewall. The current state is depicted by one of the following icons and links respectively:

- ***Disabled***

  By default (after fresh installation) the firewall is in disabled state. Click the link to enable secure mode.

- ***Secure***

  This icon depicts secure firewall mode. Click the link to deactivate effectiveness of the configured rule set.

9.8 Configuration

Note

Usually the configuration of the firewall is directly made at the server (**Server Config – Personal Firewall Rules**, page 41).

9.8.1 General

Note

Windows Vista: If ***Increase permissions*** (figure 9–15) appears in the ***Configuration*** sub-menu you have no access to the configuration. For editing contact your system administrator.

Fig. 9–15 *Windows Vista – Configuration – Increase permissions*

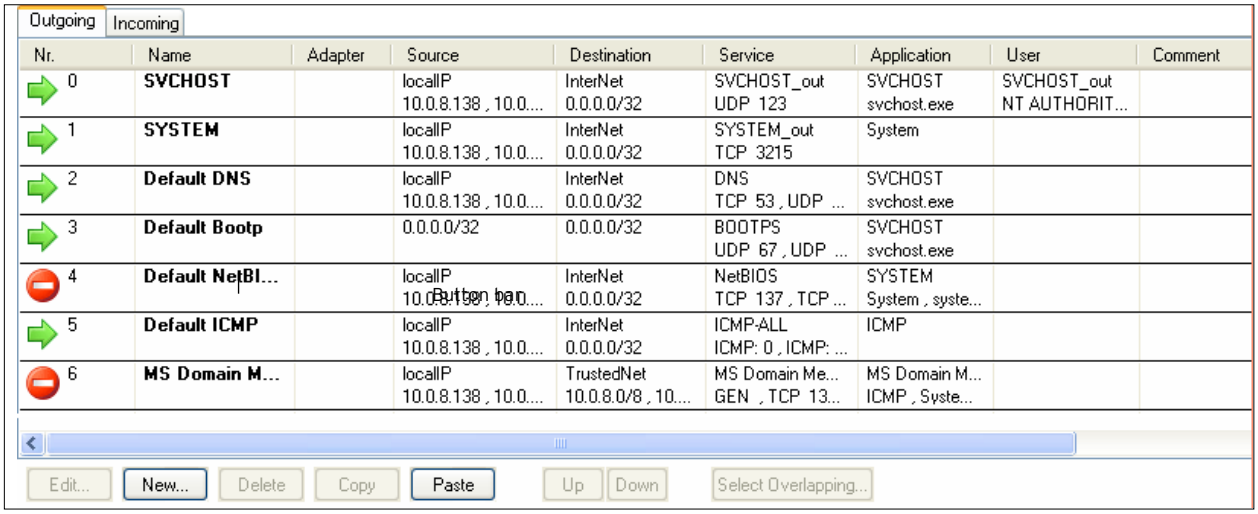
9.8.2 Rules

The Rules view allows manual rule configuration. Rules controlling incoming traffic are arranged in the ***Incoming*** tab, rules controlling Outgoing traffic are arranged in the ***Outgoing*** tab (figure 9–16).

Note

Personal Firewall rule sets are not capable of RCS.

Fig. 9–16 *Rules window*



9.8.3 Context Menu

Select and right-click a list entry to display the following context menu:

Table 9–6 *Rule window - Context menu*

Item	Description
Show Source Addresses…	Opens a window displaying all source addresses affected by the selected rule.
Show Destination Addresses…	Opens a window displaying all destination addresses affected by the selected rule.
Show Services…	Opens a window displaying all services affected by the selected rule.
Show Applications…	Opens a window displaying all applications affected by the selected rule.
Show Adapters	Opens a window displaying all adapters affected by the selected rule.
Show Users	Opens a window displaying all users affected by the selected rule.
Select Overlapping	As a connection request can match several conditions, the rules' succession within a rule set is very important. If incorrectly ordered, rules might interfere with one another. The function ***Select Overlapping*** is meant to help avoiding configuration mistakes. When applied to a selected rule, all rules possibly interfering with it are highlighted. In the majority of cases, the overlap is a harmless outcome of the use of very openly defined objects such as ***InterNet***.
Edit…	Opens the rule configuration dialog for the selected rule (9.8.5 Rule Configuration, page 105).
New…	Opens the rule configuration dialog for a new rule (9.8.5 Rule Configuration, page 105).
Delete	Deletes the selected rule(s).
Copy	Copies the selected rule(s) to the clipboard.

Table 9–6 *Rule window - Context menu*

Item	Description
Paste	Pastes the selected rule(s) from the clipboard.

9.8.4 Button Bar

In the button bar, the ***Up*** and ***Down*** buttons complement options are available in the context menu (see above).

Select a rule and click one of the buttons, to shift the rule further up or down within the rule set. Alternatively, you can use drag&drop.

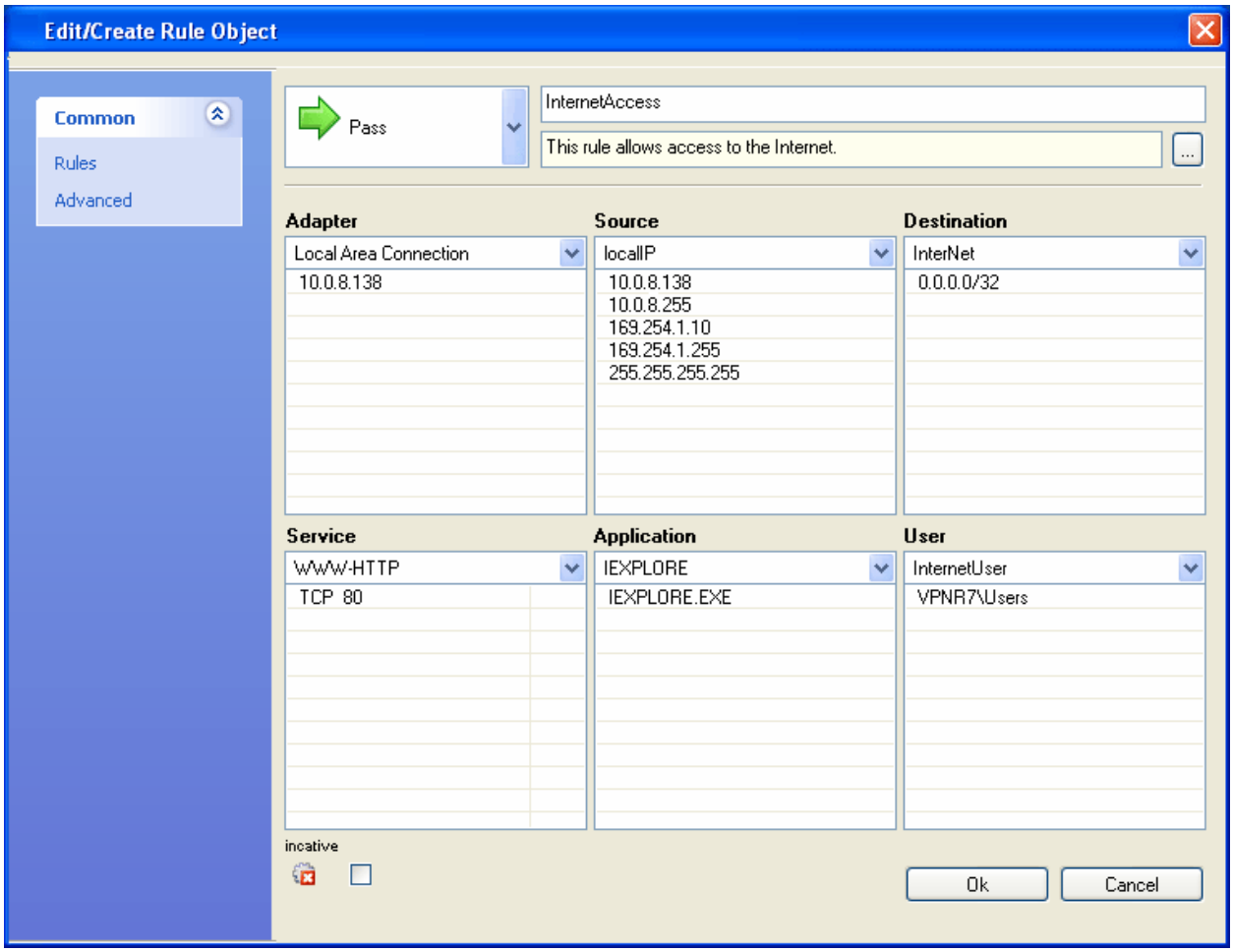
Note

According to a regular Barracuda NG Firewall rule set, the Barracuda NG Personal Firewall rule set is processed rule by rule until an applicable rule is available. Thus, to achieve correct rule processing, rules need to be arranged in the correct order.

9.8.5 Rule Configuration

Select ***New…*** from the context menu to create a new rule.

Fig. 9–17 *Rule configuration dialog*



Configure the following connection details in the ***Rules*** view of the ***Rule Object*** window:

List 9–5 *Rule Object - Options in the Rules view*

Item / Parameter	Description
Action	Select ***Pass*** to enable a connection request, select ***Block*** to prevent it.
Name	Insert a rule name into this field.
Comment	For easier identification, insert a rule description (optional).
inactive checkbox	Select the ***inactive*** checkbox to disable a rule (default: unselected).

Note

A minimum specification of the following connection details is mandatory in the sections below:

- ***Source*** / ***Destination*** / ***Service*** ***or***
- ***Adapter*** / ***Source*** / ***Service*** ***or***
- ***Adapter*** / ***Destination*** / ***Service***

Caution

Modifying an object is a global action. For example, any other rule using the specific object will be affected by the modification.
This applies only for referenced objects, not for objects of type <explicit>.
Explicit objects are only available for the current rule.

Table 9–7 *Rule Object - Options in the Rules view – sections*

Section	Description
Adapter	Specify an adapter for the connection request. In the list all ***Adapter Objects*** that have been defined in the ***Adapter*** window are available (9.8.6 Adapters, page 108). Right-click the adapter window below the list and Select ***New…*** to create a new Adapter Object. Double-click an available entry to edit the assigned Adapter Object.
Source / Destination	Specify a source for the connection request. In the list all ***Network Objects*** that have been defined in the ***Networks*** window are available (9.8.7 Networks, page 110). Select ***<Explicit>*** to define a network object explicitly without adding it to the Network Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Network Object. Double-click an available entry to edit the assigned Network Object.
Service	Specify a service for the connection request. In the list all ***Service Objects*** that have been defined in the ***Services*** window are available (9.8.8 Services, page 112). Select ***<Explicit>*** to define a network object explicitly without adding it to the Service Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Service Object. Double-click an available entry to edit the assigned Service Object.
Application (optional)	Specify an application for the connection request. In the list all ***Application Objects*** that have been defined in the ***Application*** window are available (9.8.9 Applications, page 114). Select ***<Explicit>*** to define an application object explicitly without adding it to the Application Objects listing. Right-click the source window below the list and Select ***New…*** to create a new Application Object. Double-click an available entry to edit the assigned Application Object.
User (optional)	Specify an user for the connection request. In the list all ***User Objects*** that have been defined in the ***User*** window are available (9.8.10 Users, page 117). Select ***<Explicit>*** to define an user object explicitly without adding it to the User Objects listing. Right-click the source window below the list and Select ***New…*** to create a new User Object. Double-click an available entry to edit the assigned User Object.

Configure the following connection details in the ***Advanced*** view of the ***Rule Object*** window:

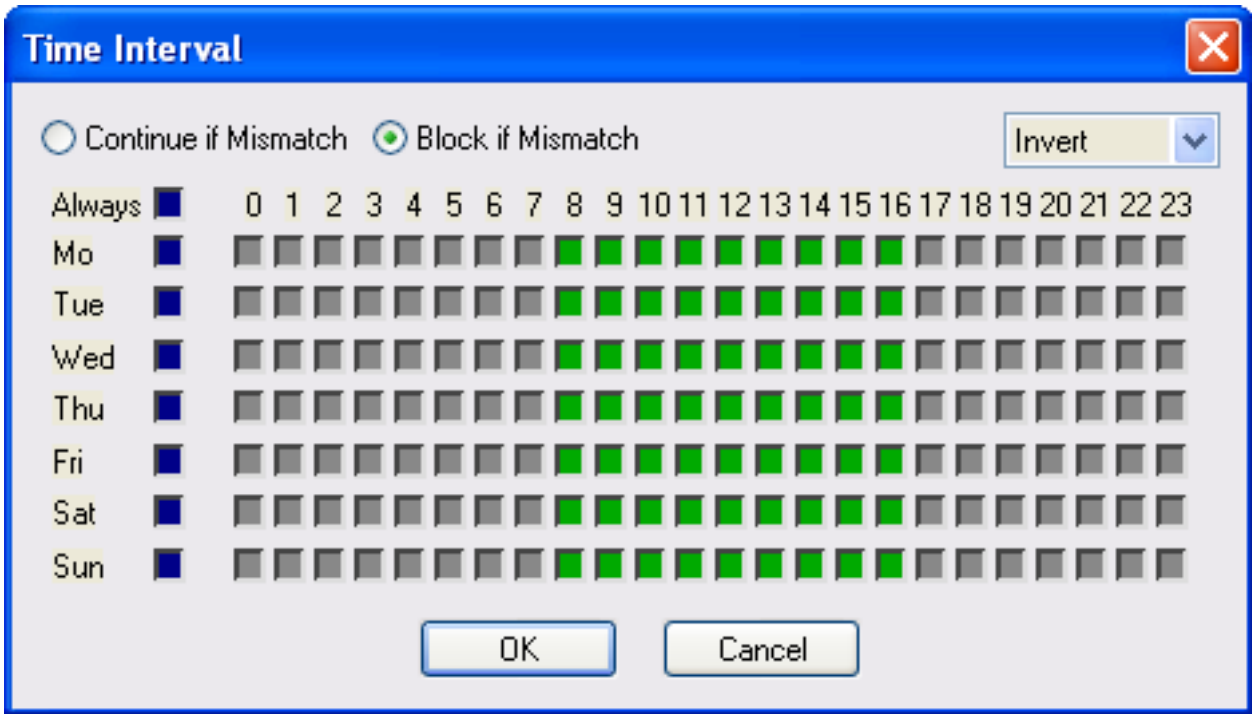
List 9–6 *Edit/Create Rule Object - Options in the Advanced view – section Rule Mismatch Policy*

Parameter	Description
Source / Service/ Destination / Application / User / Adapter	• ***Continue on Mismatch (default)*** Process the rule, even if the corresponding object does not match the configured setting. • ***BLOCK on Mismatch*** Do not process the rule if the corresponding object does not match the configured setting.

List 9–7 *Edit/Create Rule Object - Options in the Advanced view – section Miscellaneous*

Parameter	Description
Time Restriction	A time restriction can be assigned to each rule. The granularity is 1 hour on a weekly base. A rule is allowed at all times by default, for example, all checkboxes in the ***Time Interval*** window are cleared. Selecting a checkbox denies a rule for the given time. Select (set invert) from the list to configure allowed and disallowed time intervals simultaneously. Select (set allow) from the list to clear selected checkboxes. Select (set deny) from the list to to configure disallowed time intervals. Select ***Continue if mismatch*** to process the rule even if time restriction denies it. Select ***Block if mismatch*** to prevent rule processing if time restriction denies it (default). See figure 9–18: a time interval setting for a rule which has been set to disallowed on Monday and Thursday from 8 a.m. to 5 p.m.
Monitor Connections	• ***Yes*** • ***No***

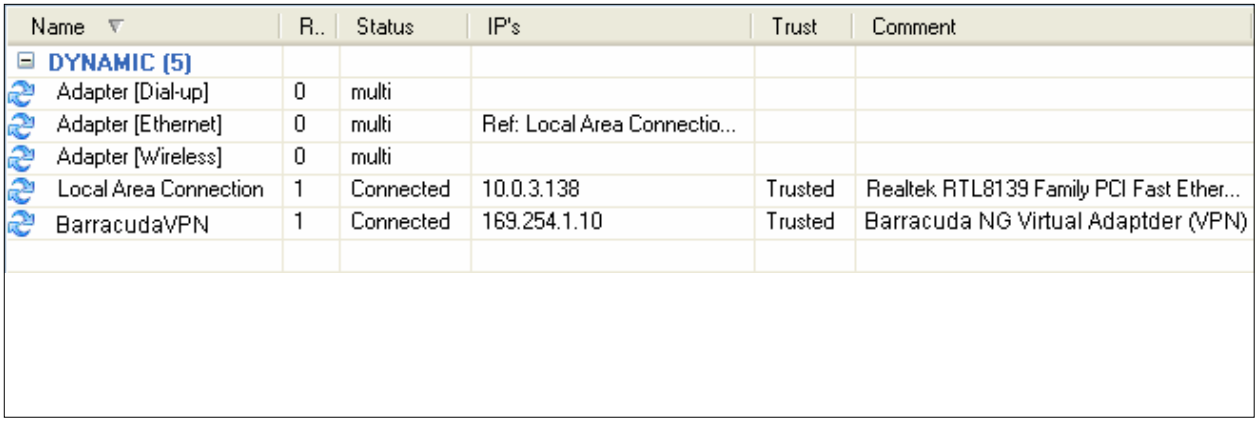
Fig. 9–18 *Time restriction dialog*



9.8.6 Adapters

The ***Adapters*** view allows you to view and configure network adapters available on the system. Adapters may be employed in firewall rules, in order to restrict rule processing to a specific adapter or a set of adapters only.

Fig. 9–19 *Adapter objects window*



The listing is divided into the following columns:

Table 9–8 *Adapter Object view details*

Column	Description
Name	Name of the adapter object.
Referenced by	Number of references pointing to the adapter object
Status	Current connection status of the adapter object (***connected*** / ***disabled*** / ***multi***)
IP's	IP addresses and / or references assigned to the adapter object
Trust	Trust type assigned to the adapter object (***trusted*** / ***untrusted***)
Comment	Optional adapter object description

In the ***Adapter Objects*** view, several **dynamic** adapter objects (flagged with the icon) are preconfigured.

Note

Dynamic objects are updated at runtime when adapter configuration changes and cannot be edited manually. In order to work, Automatic Adapter Assignment must be selected in the Firewall Settings (9.4.1 Firewall Menu, page 91).

The following objects (assigned with status ***multi***) are available:

- ***Adapter [Dial-up]***

  This object summarizes all dial-up adapters available on the system (for example, UMTS, ISDN, and modem cards).

- ***Adapter [Ethernet]***

  This object summarizes all Ethernet adapters available on the system (for example, LAN devices).

- ***Adapter [Wireless]***

This object summarizes all wireless adapters available on the system (for example, WLAN cards).

Note

Adapters available on the system are automatically assigned to the appropriate adapter object with status type ***multi***. These objects may be used to construct abstract rule sets, for example, to configure a rule blocking access to all available dial-up or wireless adapters.

The following further adapter objects are available:

- ***[Network Connection name]*** (for example, ***Local Area Connection***)

  These are the LAN devices available on the system. The *Network Connection* name is retrieved from the Microsoft Windows Network Connections view (available through **Start** > **Control** > **Network Connections**).

Note

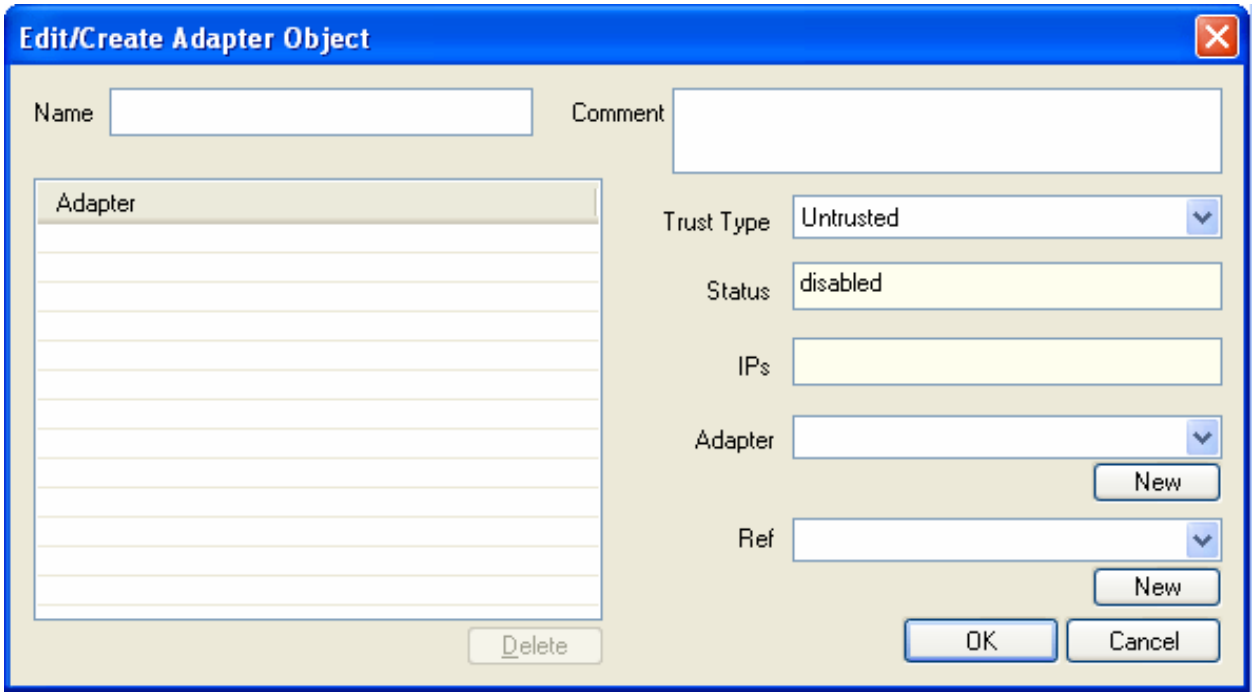
The "logical" Microsoft Windows name, which is dependent on the operating system's language version, and not the device name is applicable for object naming.

- ***NG VPN***

  This is the virtual interface of the Barracuda NG VPN Connector.

To create a new adapter object, click ***New…*** in the ***Adapter Objects*** window:

Fig. 9–20 *Edit/Create Adapter Object configuration dialog*



The following options are available:

List 9–8 *Edit/Create Adapter Object options*

Parameter	Description
Name	Specify a name for the adapter object.
Comment	Optionally, insert an adapter description
Trust Type	Select ***Trusted*** to add a reference to the adapter object to the network object that has been defined as Trusted Network in the ***Administration*** > ***Firewall Settings*** (***Trusted Network***, page 120). If you do not want to create a reference, select ***Untrusted***. **Note:** When later changing the setting from ***Trusted*** to ***Untrusted***, the reference to the adapter object is automatically deleted from the ***Trusted Network*** object. References to ***Untrusted*** adapter objects may not be added to the ***Trusted Network*** object manually.
Status	This is a read-only field displaying the connection status of the adapter object.
IPs	This is a read only field, displaying the IPs assigned to the adapter object.
Adapter	Select network adapter you wish to create the adapter object for. Click ***New*** to add your selection to the ***Adapter*** list.
Ref	Select network reference you wish to create the adapter object for. Click ***New*** to add your selection to the ***Adapter*** list.

9.8.7 Networks

The Networks view facilitates IP address/network management. Use the Networks window to

- ***assign names to single IP addresses***
- ***combine multiple IPs/networks/References into networking objects***

Note

For a clearly arranged network management rather make use of referencing Network Objects than explicit IPs when configuring firewall rule sets.

Fig. 9–21 *Network Objects window*

Name	RefBy	Entries	Description
DYNAMIC (9)			
dhcpIP	0	255.255.255.255 , 0.0.0.0 , Ref...	Local IP with 0.0.0.0
InterNet	5	0.0.0.0/32	Unsecure Zone
localIP	13	169.254.1.10 , 10.0.8.138 , Ref...	All Local IPs
Net-Broadcast	1	169.254.1.255 , 10.0.8.255 , 25...	All Broadcasts
Net-Local Area Con...	1	10.0.8.0/8	Realtek RTL8139 Family PCI Fast Etherne...
Net-Multicast	1	239.255.0.0/16	Multicasting RFC 2365 and 3172
Net-netfenceVPN	1	169.254.1.0/8	phion Virtual Adapter (VPN)
TrustedNet	6	255.255.255.255 , Ref: Net-Mul...	Secure Zone
virtualIP	0	169.254.1.10	All Virtual Phion VPN IPs
LOCAL (1)			
ADSLNet	1	0.0.0.0/32	

In the ***Network Objects*** window, a number of **dynamic** network objects (flagged with the icon) are preconfigured.

Note

Dynamic objects are updated at runtime when network configuration changes and cannot be edited manually. For dynamic update to work, Automatic Adapter Assignment must be selected in the Firewall Settings (9.4.1 Firewall Menu, page 91).

- ***localIP***

The localIP object contains all IPs that are configured on **trusted** adapters, and a reference to the Net-Broadcast object.

- ***virtualIP***

The virtualIP object contains the IP address assigned from the VPN server. The virtual IP is only available in case of established VPN connections.

- ***Net-[Network Connection name]***

These objects contain the network addresses of each specific adapter available on the system. The *Network Connection* name is retrieved from the Microsoft Windows Network Connections view (available through ***Start > Control > Network Connections***).

Note

The "logical" Microsoft Windows name, which dependents on the operating system's language version and not the device name, is applicable for object naming.

Net-[Network Connection name] objects may be used for setup of abstract rule sets.

- ***InterNet***

The ***InterNet*** object may be used for outbound connections to the Internet (network 0.0.0.0/0).

- ***TrustedNet***

Use the ***TrustedNet*** object to refer to trustworthy networks. The content of this object is dependent on assignment of an adapter as trusted or untrusted (9.8.6 Adapters, page 108). When an adapter is specified as trusted the IP addresses living on it are added to the TrustedNet object. Vice versa they are deleted from it, when trust assignment changes to untrusted. The TrustedNet object is also updated when IP address configuration of a trusted adapter changes.

- ***Net-NGVPN***

The Net-NGVPN object contains the address of that network the ***virtualIP*** object is living in.

Note

Secured Routes are assigned to the ***Net-NGVPN*** Object.

- ***Net-Broadcast***

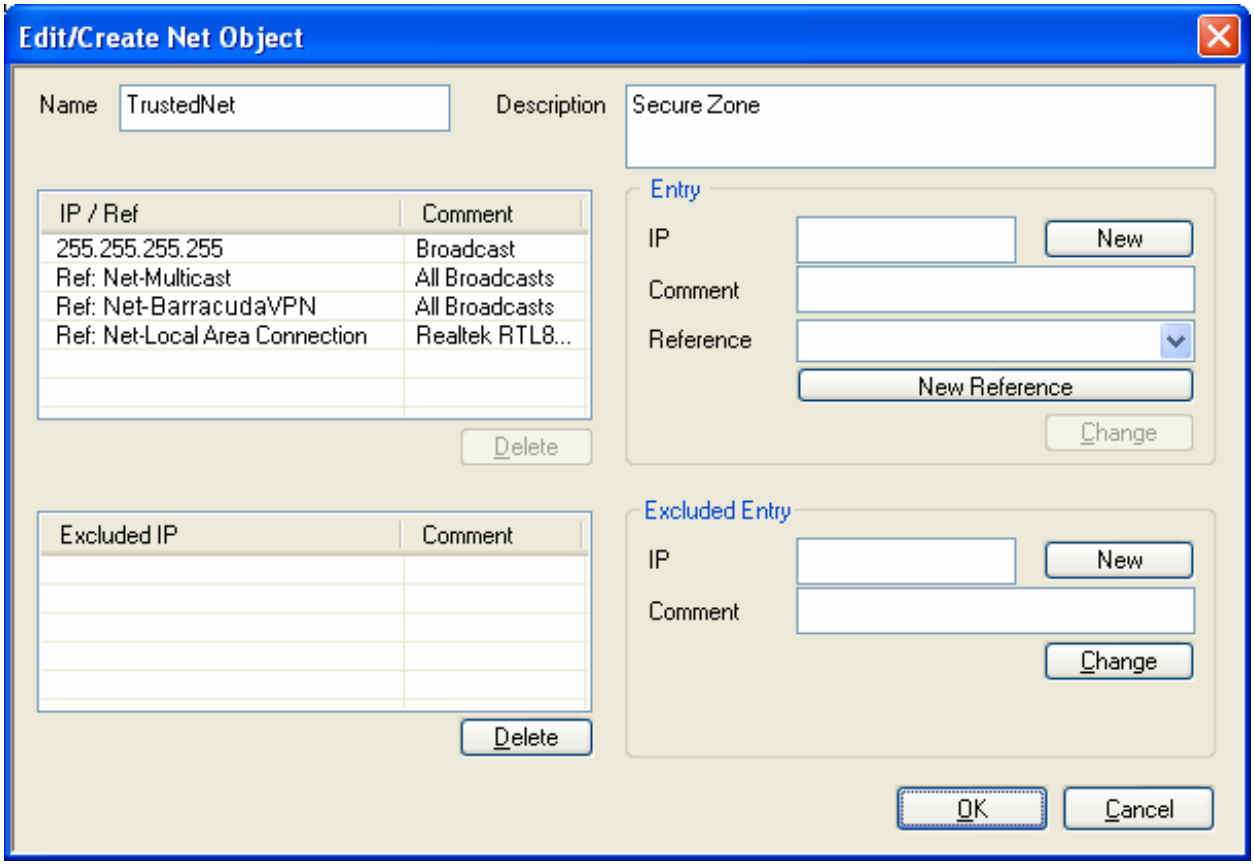
This object contains the broadcast addresses of IP addresses configured on **trusted** adapters. The broadcast addresses are calculated directly from the IPs.

- ***Net-Multicast***

This object includes the Multicast network 239.255.0.0/16.

Click ***New…*** to open the ***Net Object*** dialog.

Fig. 9–22 *Net Object dialog*



Insert ***Name*** and ***Description*** of the Net Object for easier identification.

In the ***Entry*** section insert IP/network address(es) of the new Net Object and/or specify a ***Reference*** to the Net Object, for example select an existing Net Object to refer to a new one.

The ***Excluded Entry*** section allows excluding specific networks from a network object.

Note

For transparency and consistency reasons, there are no references available in this section.

9.8.8 Services

The Services window facilitates port and protocol management. Use the Services window for the following purposes:

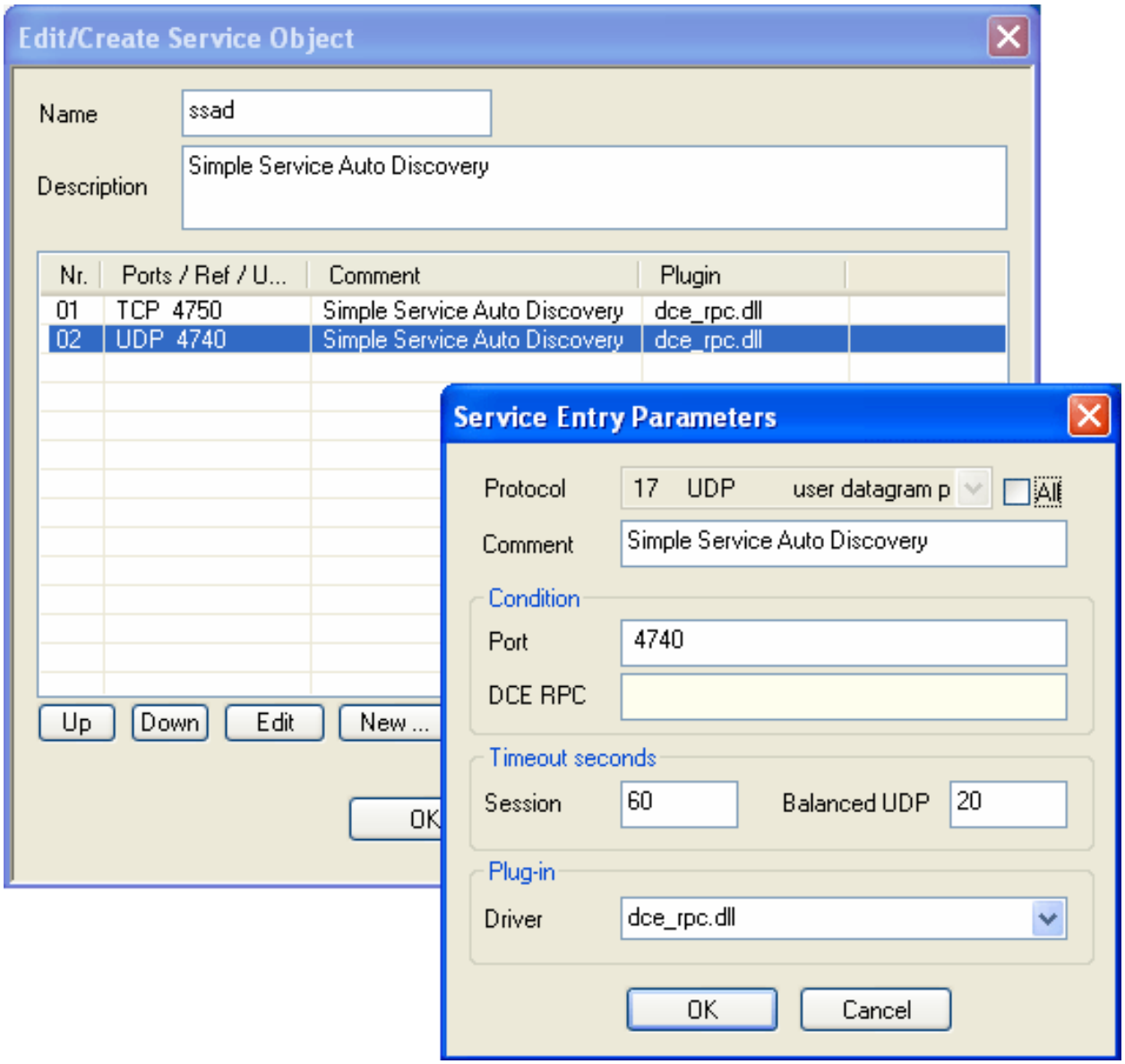
- ***Assigning ports and protocols to specific services.***

- ***Merging multiple services to one service object using references.***

Note

Properties of Service Objects are described in detail in the Barracuda NG Firewall Administrator's Guide.

Fig. 9–23 *Service Object dialog*



The following services are available in the Barracuda NG Personal Firewall by default:

Table 9–9 *Service Objects available in the Personal Firewall*

Service Name	Port	Protocol	Connection	Description
		ICMP	**O / I**	Internet Control Message Protocol; ICMP messages, delivered in IP packets are used for out-of-band messages related to network operation, or misoperation.
DNS	53	TCP/UDP	**O**	Domain Name Service; method by which the Internet addresses in mnemonic form (for example phion.com) are converted into the equivalent numeric IP address (for example 134.220.4.1)

Table 9–9 *Service Objects available in the Personal Firewall*

Service Name	Port	Protocol	Connection	Description
BOOTPS	67	UDP	**O**	Bootstrap protocol; also used for DHCP (Dynamic Host Configuration)
Kerberos	88	TCP/UDP	**O**	Protocol for authentication in Windows 2000 environment
NTP	123	UDP	**O**	Network Time Protocol; used to synchronize the time of a computer client or server to another server or reference time source
LOC-SRV/EPMAP	135	TCP	**O**	NETBIOS; very common protocol; it is supported on both, Ethernet and TokenRing. In NetBIOS, TCP and UDP communication is supported. It supports broadcasts and multi-casting plus three distinct services: Naming, Session, and Datagram.
NETBIOS-NS	137	UDP	**O / I**	
NETBIOS-DGM	138	UDP	**O / I**	
NETBIOS-SSN	139	TCP	**O / I**	
SNMP	161	UDP	**O**	Simple Network Protocol; Network management system contains two primary elements – Manager (console to perform network management functions) and Agents (entities that interface to the actual managed device). SNMP allows Managers and Agents to communicate.
LDAP	389	TCP/UDP	**O**	Lightweight Directory Access Protocol; set of protocols for accessing information directories.
CIFS	445	TCP	**O / I**	further development of the SMB protocol and serves as an addition and improvement to the standard protocols FTP and HTTP.
MSTASK	1026	TCP	**O**	Windows Task Scheduler; used to schedule tasks, such as backups or updates, to run at certain times or dates

9.8.9 Applications

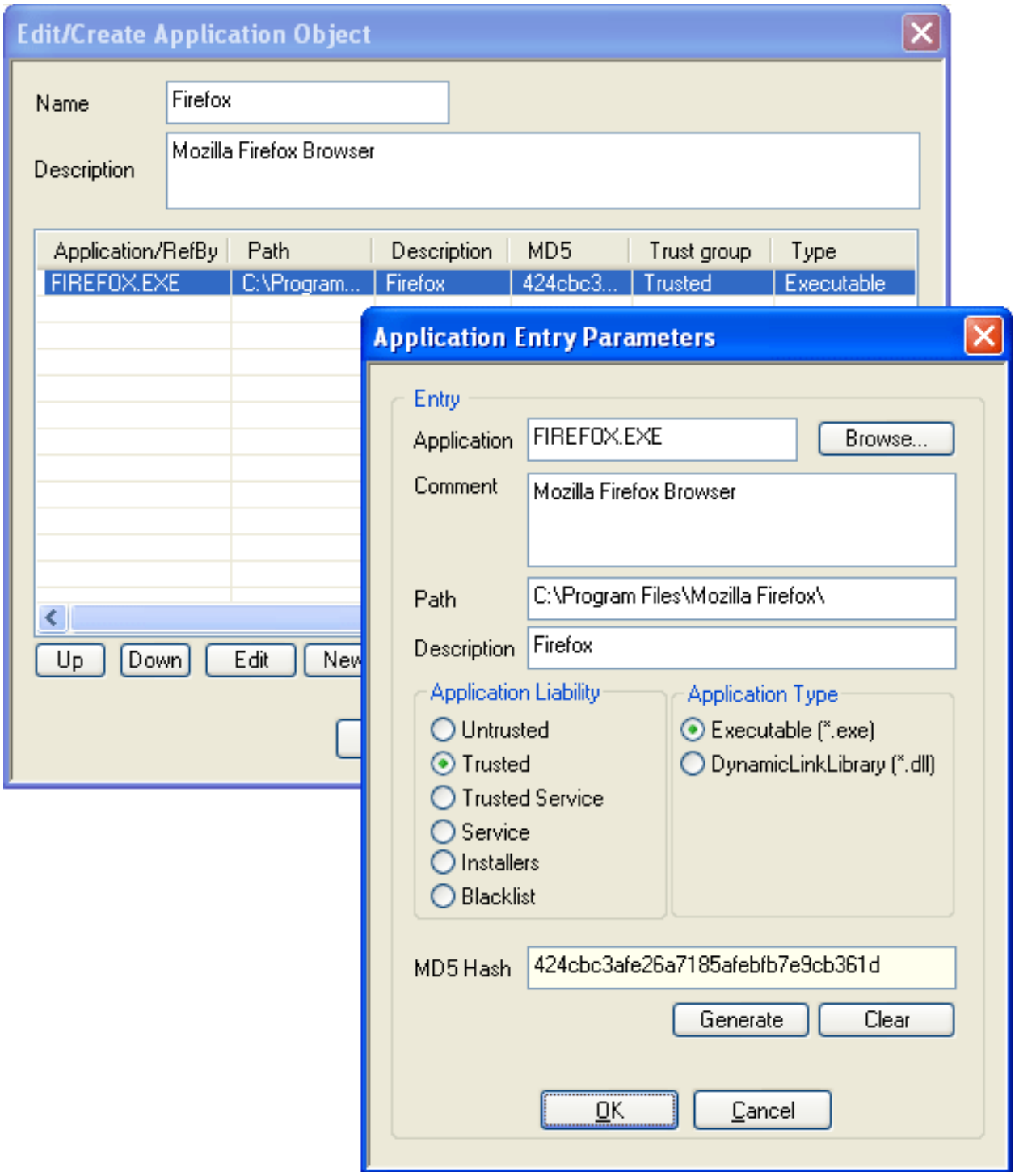
The Application Objects window allows creating predefined applications, which may be employed in rule sets.

Click ***New…*** to open the ***Application Object*** window.

Note

Application Liability and ***Application Type*** classification is purely informational.

Fig. 9–24 *Application Object dialog*



- ***Insert Name and Application Object Description for easier identification.***
- ***Again, click New… to specify an application. The Application Entry Parameters window opens.***
- ***Click Browse and select the file you want to create the object for. After selection, the path to the file and its inherent file description will be displayed in the Path and Description fields below.***
- ***Optionally, insert a file description into the Comment field.***
- ***Specify Application Liability and Application Type. Momentarily, the classification is purely informational.***

- ***Click Generate to create an MD5 Hash in order to clearly identify the selected file as soon as it is executed.***

Warning

MD5 Hash creation is recommended in order to avoid corrupt file and a vulnerable PC after an attack.

Note

Consider that when an application equipped with an MD5 Hash is used on multiple clients, file versions must match exactly. The application object will otherwise not be applicable.
To delete the hash, click ***Clear***.

Caution

In addition to the application, first level DLLs are taken into consideration. This provides additional security. However, DLLs that are used by first level DLLs are not monitored.

The following application objects, which are required in Microsoft Windows domains, are available in the Barracuda NG Personal Firewall by default:

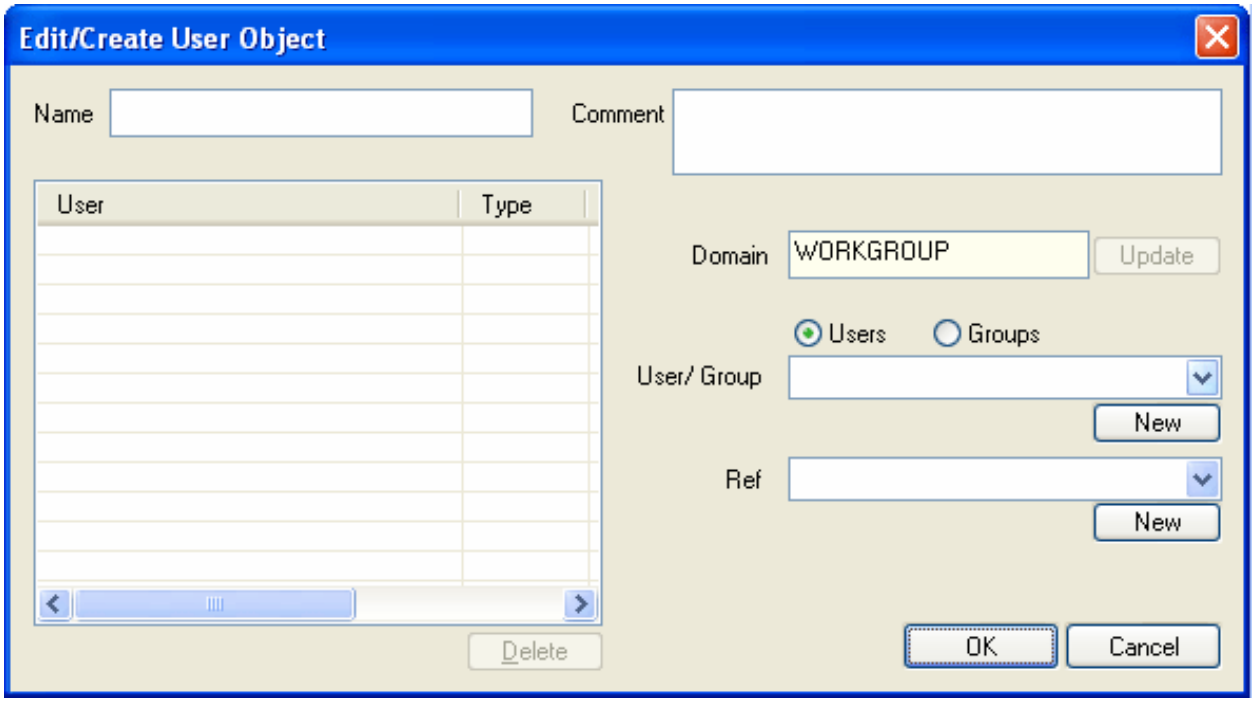
Table 9–10 *Applications required in Microsoft Windows domains*

Application	Connection	Description
System	**O** / **I**	Services needed by the OS kernel
TCP/IP Ping Command	**O** / **I**	
lsass.exe	**O**	Local Security Authority Service; process responsible for management of local security authority domain authentication and Active Directory management.
services.exe	**O**	Upon startup, services.exe enumerates through all registry sub-keys located in ***HKEY_LOCAL_MACHINE\Services*** registry key.
spoolsv.exe	**O**	The Windows Printer Spooler stores printer jobs and forwards them to the printer when it is ready.
userinit.exe	**O**	By default, WinLogon executes this application that triggers logon scripts, re-establishes network connections,…
winlogon.exe	**O**	This application manages security-related user interactions in Windows NT. It handles logon and logoff requests, changing the password,…
svchost.exe	**O**	This is a generic host process name for services that are run from dynamic-link libraries (DLLs). There can be multiple instances of svchost.exe running at the same time.

9.8.10 Users

The Users view allows you to create User and User Group objects, which may be employed in rule sets. Click ***New…*** to open the ***User Object*** window:

Fig. 9–25 *User Object dialog*



An user object is automatically created when a connection attempt is processed by the firewall. The object is then inserted into the corresponding rule.

In the ***User/Group*** list, the Microsoft Windows domain users and groups known to the Barracuda NG Firewall are available for selection. Local user/group information is displayed in the list first. If the Windows workstation is a member of a Microsoft Windows domain, domain user/group information may be retrieved from the Active Directory server by clicking ***Update***.

Note

Irrespective of the operating systems language version installed on the workstation, these users will always be displayed in English:

- ***NT AUTHORITY\SYSTEM***
- ***NT AUTHORITY\LOCAL SERVICE***
- ***NT AUTHORITY\NETWORK SERVICE***
- ***NT AUTHORITY\NETWORK***

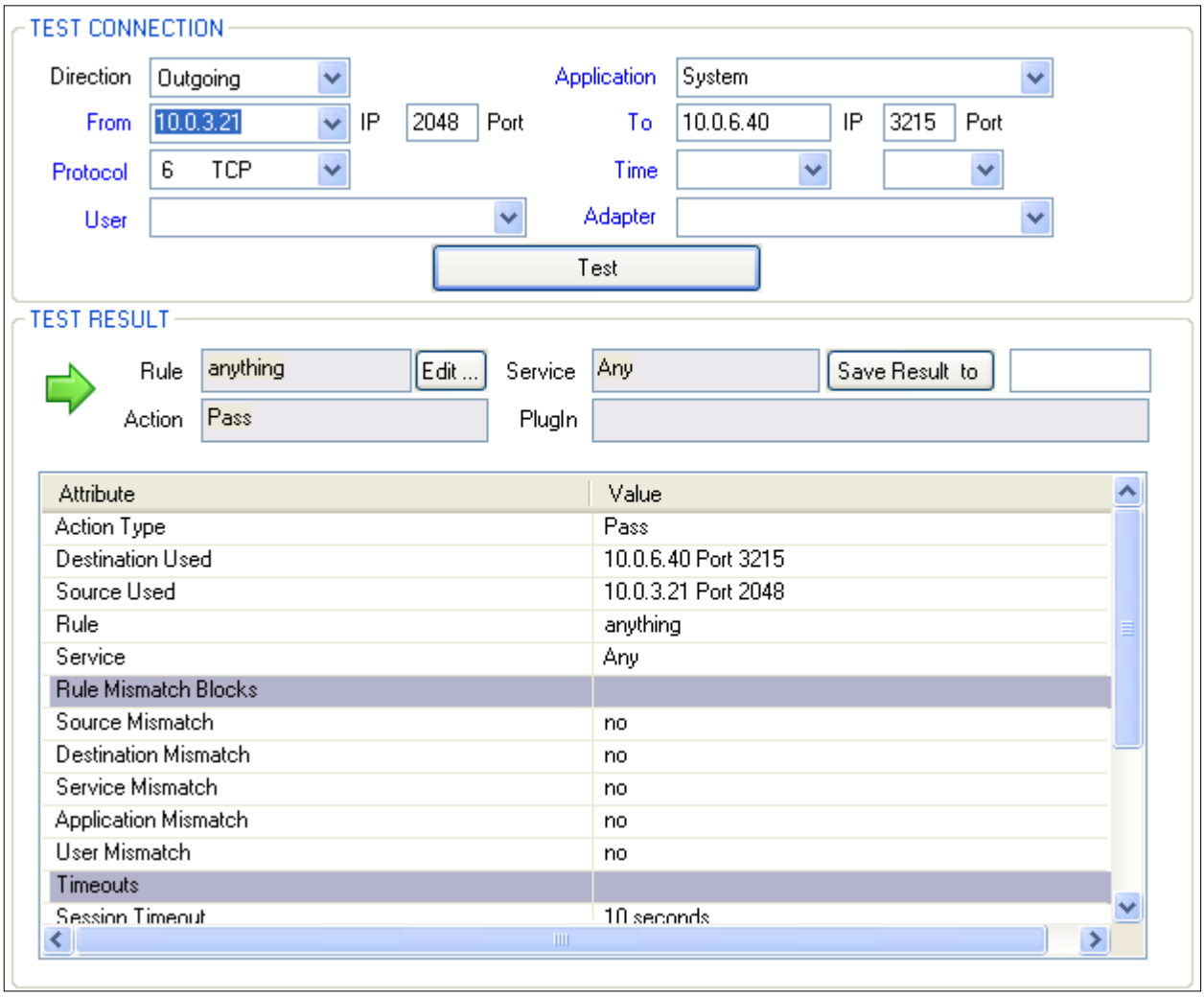
Warning

The internal firewall engine will transform these names to the appropriate language version. Do not insert them in another language manually.

9.8.11 Rule Tester

The ***Rule Tester*** view allows testing rule sets for consistency.

Fig. 9–26 *Rule Tester*



The following entities are available for rule testing:

List 9–9 *Rule Tester parameters – section TEST CONNECTION*

Parameter	Description
Direction	This is the direction of the traffic policy (***Incoming*** or ***Outgoing***).
Application	To query for an arbitrary application leave the asterisk (*), which is set as default value. Click the ***Application*** link and Select ***Update Applications*** to reset the field to the default value.
From: IP / Port	Insert Source IP and corresponding connection port. Click the ***From*** or ***To*** link to ***Swap IP*** and/or ***Port*** information.
Protocol	Specify which protocol to test. Click the ***Protocol*** link and select ***Show all Protocols*** to include other protocols than TCP/UDP and ICMP into the list.
Time (optional)	Insert day of the week and time (optionally). Click the ***Time*** link and select ***Insert current Time*** to insert current day and time.
User (optional)	Select an User from the list (Optionally). Click the ***User*** link and select ***Update Users*** to clear the field.
Adapter (optional)	Select an adapter from the list (Optionally). Click the ***Adapter*** link and select ***Update Adapters*** to clear the field.

List 9–9 *Rule Tester parameters – section TEST CONNECTION*

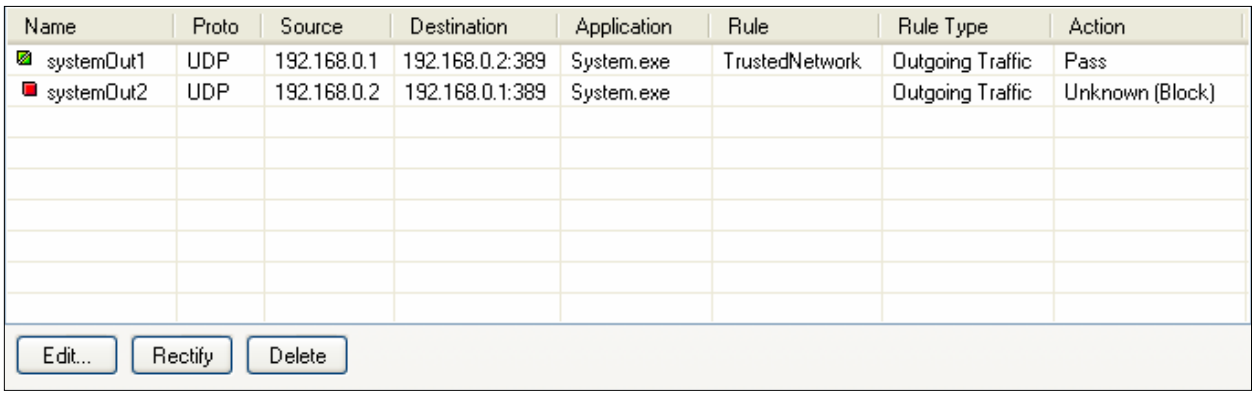
Parameter	Description
Test	Click ***Test*** to test the connection and display the test result in the section below.

List 9–10 *Rule Tester parameters – section TEST RESULT*

Parameter	Description
Test Status Icon / Action	A connection attempt with the given values can either have failed or have been successful if a rule is applicable. A failed connection will be indicated by symbol and ***Action*** field ***Block***. A successful connection attempt will be indicated by symbol and ***Action*** field ***Pass***.
Rule	The ***Rule*** field displays the applicable rule responsible for the rule test result. Click ***Edit…*** to open and modify the corresponding rule. If the connection attempt has been blocked because no rule has applied, the field will display the string ***<No Matching Rule Found>***.
Service	This field displays the applicable ***Service Object***.
PlugIn	If applicable, this field displays the name of the PlugIn that has been employed in the connection.
Save Result to	Insert the report name and click ***Save Result to*** to save the test result. The output of the connection test is written to the ***Test Report*** view (9.8.12 Test Reports, page 119).
Attribute/Value listing	This listing displays attributes of the tested connection in detail.

9.8.12 Test Reports

Fig. 9–27 *Test Report window*



Test reports are saved on a first come first served basis. Test results with ***Action Pass*** are indicated by a green icon (), test results with ***Action Blocked*** are indicated by a red icon ().

Changing any parameter in any configuration area that influences the result of a test report leads to a status icon change in the overview window. Green icons () will become red (). To apply the new conditions to an already existing test report, select the data set in the overview window of the ***Test Reports*** window and click ***Rectify***.

Note

Subsequently to this action, the status icons will no longer indicate if an action has been successful or not, but instead if rectification has been applied. Rectified entries will be flagged with a green () status icon, even if a tested connection attempt has failed.

Select a report and click ***Edit…*** to open the test result in the ***Rule Tester*** window. You may now use the report as template for further connection tests.

Select a report and click ***Delete*** to delete the report from the Test Report window.

9.9 Administration - Firewall Settings Wizard

Options available in the Firewall Settings view allow you to adjust the preconfigured local rule set of the Barracuda NG Personal Firewall. Setting changes triggers either rule creation, deletion or traffic policy change. Use this configuration area to customize the preconfigured rule set easily.

Note

The settings defined in this window by default are triggered by the specifications defined during installation (5.2 Custom Installation, page 70).

The following options are available for customisation:

List 9–11 *Firewall Settings parameters > Trusted Domain Membership*

Parameter	Description
Trusted Network	Network assignments and references in the network object that has been defined as trustworthy are updated dynamically when network adapters are added to the system with trust assignment "trusted" or when IP address configuration of a trusted adapter changes (9.8.6 Adapters, page 108). By default, the ***Trusted Network*** option points to the preconfigured ***TrustedNet*** object (9.8.7 Networks, page 110). You may change the setting to another available network object. Be aware of possible implications. Set to ***No*** to disable this feature.
Domain Member	This option can only be set to ***yes*** when a network object has been configured as ***Trusted Network***. Setting to ***yes*** creates and activates default rules allowing applications required in Microsoft Windows domains.
Windows File Sharing	This option can only be set to ***yes*** when a network object has been configured as ***Trusted Network***. When set to ***yes*** incoming connections to local printer(s) and files are allowed.
Allow NetBIOS	
Incoming	Setting to ***yes*** (default: ***no***) allows NetBIOS traffic.
Outgoing	Setting to ***yes*** (default: ***no***) allows NetBIOS traffic.

List 9–12 *Firewall Settings parameters > Miscellaneous*

Parameter	Description
Interactive Alarm Notifications	
Ask for unknown incoming connections	Set this value to ***yes*** to enforce manual confirmation for all incoming connection attempts. Confirmation for connection establishment grant is going to be requested by a notification pop-up. For information details on design of this notification window see 9.9.2 Automatic Rule Configuration, page 122.
Ask for unknown outgoing connections	Set this value to ***yes*** to enforce manual confirmation for all unknown outgoing connection attempts. Confirmation for connection establishment grant will be requested by a notification pop-up. For information details on design of this notification window see 9.9.2 Automatic Rule Configuration, page 122.
Ask for adapter update confirmation	Setting to ***yes*** (default) triggers a pop-up, when settings assigned to a network adapter change (9.9.1 Automatic Adapter Configuration, page 121).
Connectivity	
Connect to the Internet with ADSL (PPTP)	Setting to ***yes*** creates a pass rule named ADSL in the Outgoing tab of the firewall configuration that is needed for Internet connections via ADSL. The service object used in this rule amongst others implements the services and protocols listed in table 9-11.

Table 9–11 *Services and protocols employed by the ADSL rule*

Port	Protocol	Service Name	Description
	GRE	pptp	Generic Routing Encapsulation; protocol which allows an arbitrary network protocol A to be transmitted over any other arbitrary network protocol B, by encapsulating the packets of A within GRE packets, which in turn are contained within packets of B
1723	TCP	NETBIOS-DGM	Point-to-point tunnelling protocol; control port

9.9.1 Automatic Adapter Configuration

Set option ***Ask for adapter update confirmation*** in the Firewall Settings view (page 120) to ***yes*** (default), if you would like to be notified, when adapter configurations change. A security alert window will then pop-up, asking for configuration change confirmation.

Click ***Untrust*** to add the adapter to the ***Adapter Objects*** list and assign it as ***Untrusted*** adapter. This will create an incoming adapter block rule in the Incoming tab of the firewall rule set configuration area (9.8.2 Rules, page 104).

Click ***Trust*** to add the adapter to the ***Adapter Objects*** list and assign it as ***Trusted*** adapter. This will add a reference to the trusted adapter in the ***TrustedNet*** object and delete a possibly existing incoming adapter block rule in the Incoming tab of the firewall rule set configuration area (9.8.2 Rules, page 104).

Generally, the security alert window will pop up if:

- ***... an adapter is used for the first time, for example if it is added to the system.***
- ***... the IP configuration of an adapter changes, for example if an IP address is added or deleted.***

However, it will not pop up if:

- ***... an IP address is reintroduced (for example, DHCP renew).***
- ***... an adapter's IP configuration is reset to 0.0.0.0.***

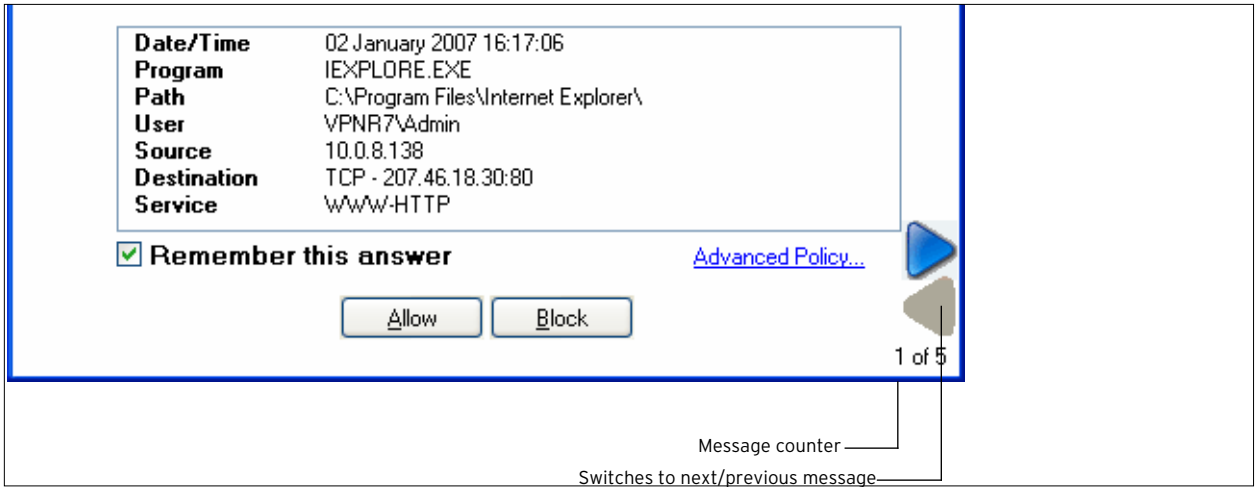
Note

For a detailed description of adapter configuration options see 9.8.6 Adapters, page 108.

9.9.2 Automatic Rule Configuration

If ***Ask for unknown outgoing/incoming connections*** has been activated in the ***Firewall Settings*** view (9.9 Administration - Firewall Settings Wizard, page 120), an unknown application/service requesting network connection will trigger a ***Security Alert*** pop-up window requesting authorisation.

Fig. 9–28 *Security Alert windows*



Note

Windows Vista: If you don't have access to the dialog (figure 9–28), then please contact your system administrator.

The following information is included in the Security Alert window:

Table 9–12 *Connection request details summarized in the Security Alert window*

Column	Description
Date/Time	Time of the connection request.
Local Server/Program	Application requesting the connection.
Path	Complete path to the application requesting the connection.
User	User responsible for the connection request.
Source/Destination	Connection source and target destination/port.
Service	Service requesting the connection.
Message Counter	Number of security alerts that are to be considered. Click the ◀▶ arrows to scroll through the alert windows.
More Info	Click this link to open the Barracuda NG Firewall online help file.

- ***Select the Remember this answer checkbox (default: selected) to allow or deny a connection request permanently. Selecting the checkbox automatically creates a corresponding rule in the Configuration area of the Barracuda NG Personal Firewall, including required Network, Service, Application and User Objects (9.8 Configuration, page 103). If cleared, the connection request is granted temporarily for this one specific connection request only.***

Selecting the checkbox also makes the ***Advanced Policy...*** link available. Click the link to customize further connection details:

Fig. 9–29 *Security Alert - Advanced Policy*

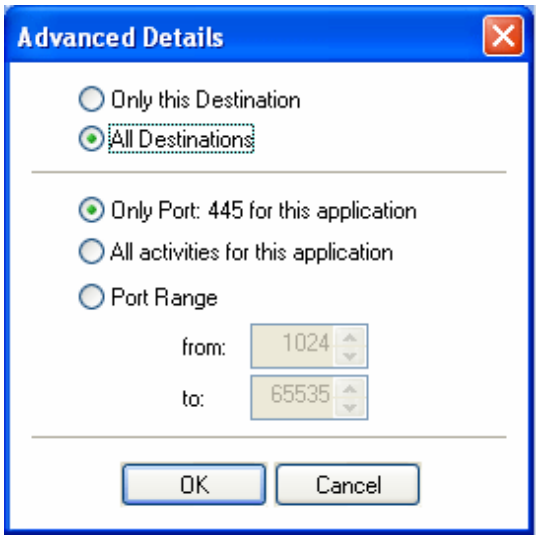


Table 9–13 Security Alert - Advanced Policy options

Column	Description
Only this Destination/Source	This option binds the outgoing/incoming connection to a specific IP address.
All Destinations/Sources	Select this option to detach connection binding from a specific IP address (default).
Only Port	This option binds the outgoing/incoming connection to a specific port. This option is selected by default to allow a restrictive rule set only.
All activities for this application	Select this option to allow connection initiation on arbitrary ports.
Port Range	Select this option and insert a port range to allow connection initiation on the specified ports only.

- ***Click Allow to grant the connection request in consideration of the conditions defined above.***
- ***Click Block to deny the connection request in consideration of the conditions defined above.***

Note

CTRL + left mouse button confirms all connection notifications present with ***Allow/Block***. The number of messages is shown in the message counter.
ESC confirms the current connection notification with ***Block***.

Note

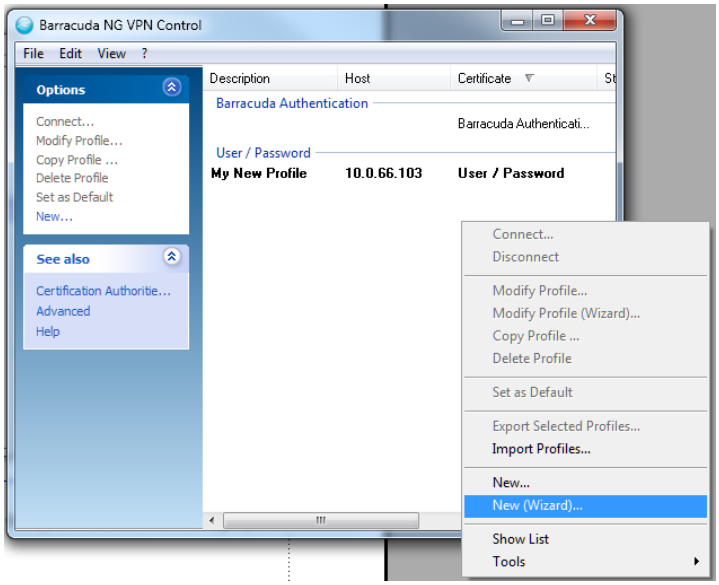
A connection request related to browsing the Internet with Microsoft Internet Explorer or another browser should be treated differently than other more specific connection requests. For connections initiated by the browser, select ***All Destinations***. With ***All Destinations*** selected, the rule set will be created referencing the global ***Net Object InterNet***. With ***Only this Destination*** selected the rule set generated will be created referencing only the specific web server's address.

Chapter 10
VPN Component Configuration

10.1 Create a New Profile Using the Profile Wizard

For your convenience, you may use the Profile Wizard to easily create and configure a new VPN profile.

Fig. 10–1 *VPN Profile Wizard Context Menu Item*



To start the wizard, right-click anywhere within the empty white space in the Barracuda NG VPN Control window, followed by choosing ***New (Wizard)...*** from the context menu.

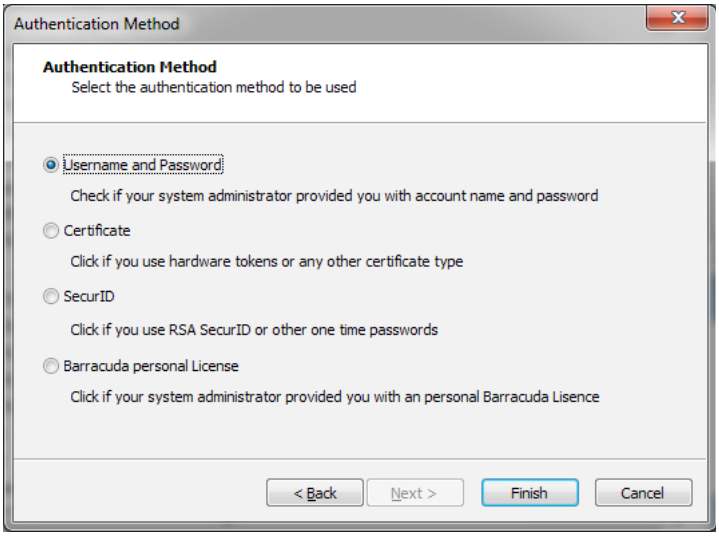
In the appearing ***Profile Wizard*** window, type the VPN server's address into the upper field and, optionally, a name to display into the lower field.

Fig. 10–2 *VPN Profile Wizard > Profile Wizard*

The next window is titled ***Authentication Method***. You can later change a different method for authentication in case you have chosen the wrong one.

Choosing ***Username and Password*** or ***SecurID*** will enable the ***Finish*** button, allowing you to complete the configuration process at this point.

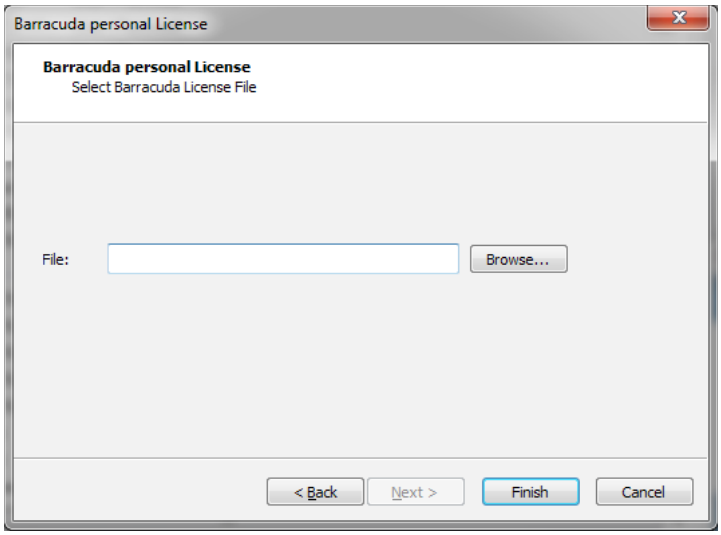
Fig. 10–3 *VPN Profile Wizard > Authentication Method*



However, if you selected one of the two remaining options, ***Certificate*** or ***Barracuda personal License***, you will be taken to another configuration step.

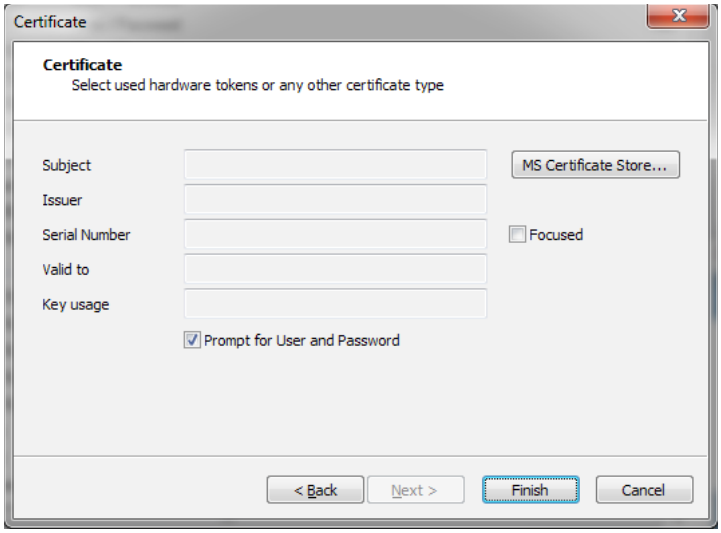
If you have chosen ***Barracuda personal License***, you will see the following window of the same title. To finish the configuration wizard, browse for the license file, then click ***Finish***.

Fig. 10–4 *VPN Profile Wizard > Enter personal License*



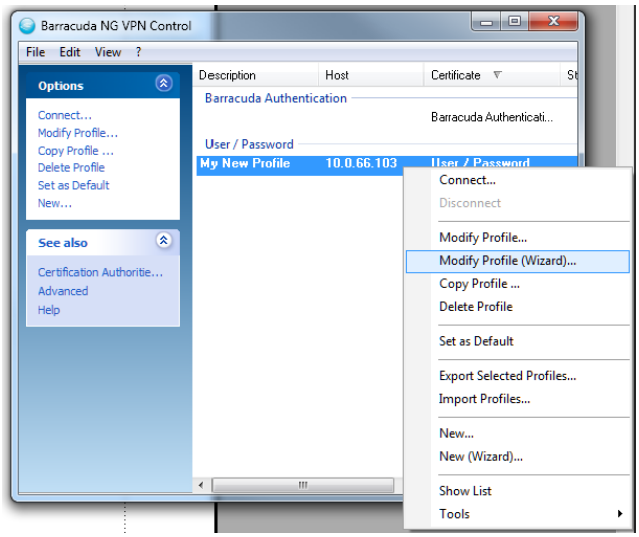
If you have chosen ***Certificate***, you will be taken to this dialog of the same title. Enter your certificate data and click ***Finish*** to complete the wizard.

Fig. 10–5 *VPN Profile Wizard > Certificate*



You can later call the wizard again by right-clicking ***Modify Profile (Wizard) ...*** at the respective VPN profile entry.

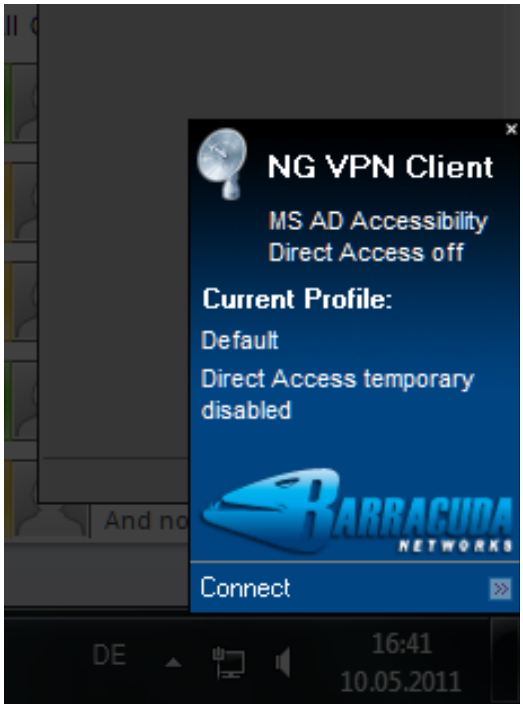
Fig. 10–6 *VPN Profile Wizard - Modify Existing Profile Using the Wizard*



10.2 Configure a New Profile Manually

Double-click the ***Barracuda NG Network Access Client*** icon (🖳) in the system tray to open the VPN component. This will bring up the client's status window which is attached to the tray.

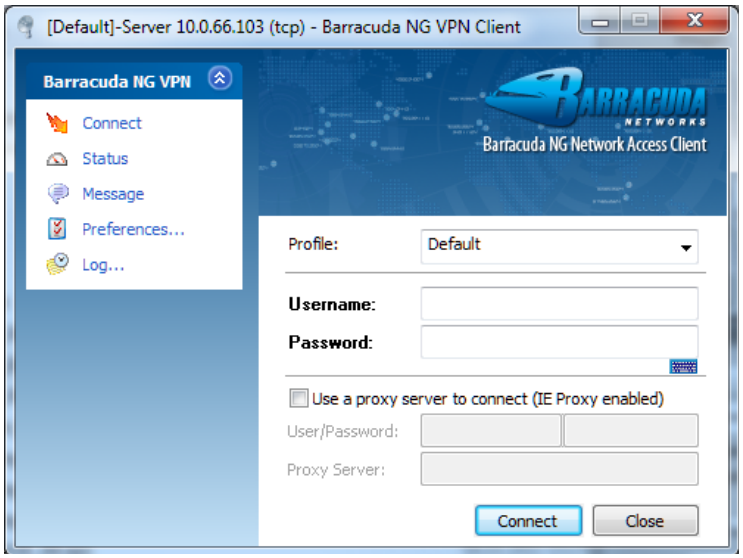
Fig. 10–7 *VPN client – tray status window*



Clicking ***Connect*** (altered by ***Disconnect***, if already connected) will open the client's configuration window.

On the first start or If no working VPN profile for automated connecting has been defined before, the client will show up with the ***Default*** profile's ***Connect*** dialog als shown below:

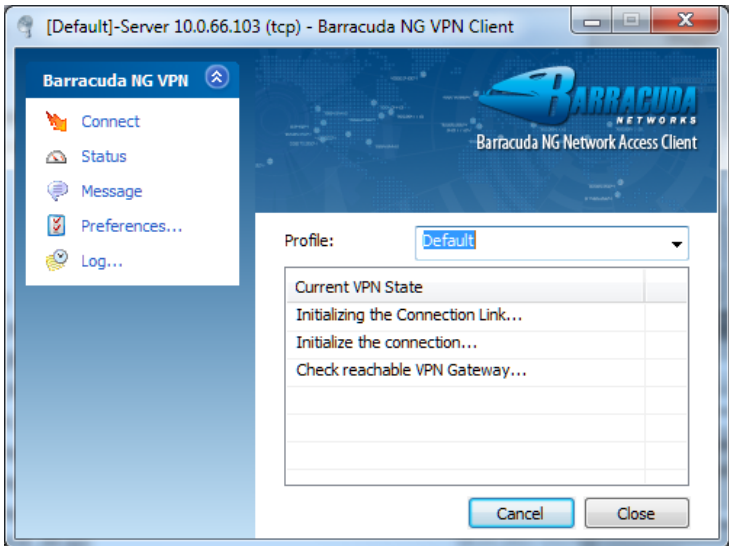
Fig. 10–8 *NG VPN client – Connect dialog*



The VPN profile can be chosen using the ***Profile*** dropdown.

Clicking ***Connect*** either left-hand or at the bottom would then initiate a connection using the chosen profile:

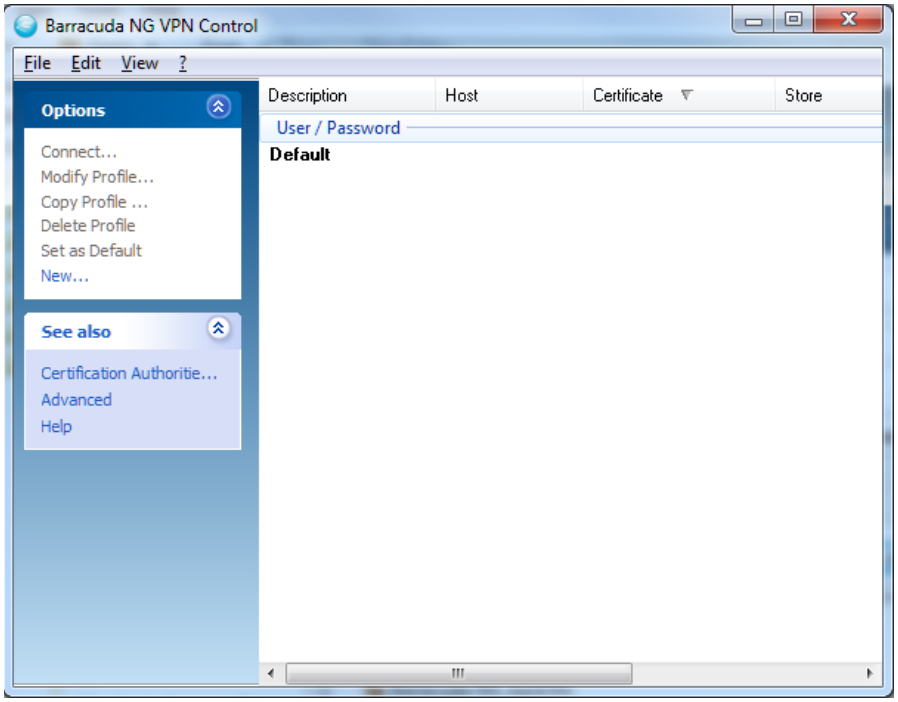
Fig. 10–9 *NG VPN client – Connect dialog*



However, before connecting for the first time you will of course need at least one working VPN profile.

Clicking ***Preferences...*** will bring up the Barracuda NG VPN Control dialog wherein the necessary configurations can be made:

Fig. 10–10 *NG VPN client – Connect dialog*



The space on the right side of this screen is reserved for a list of VPN profiles. It will be empty on the first start. You may now create a new VPN profile by clicking ***New...*** which will bring up another window for configuring the profile.

Insert a name for the connection entry into the ***Description*** field at the top. In the ***Certificate*** list, select and configure an authentication method, then insert the address of the remote server into the ***Remote Server*** field. Save the connection entries.

Best Practice

Configure a VPN profile for every known VPN server you might want to access. This way you can use the client's Direct Access functionality, enabling you to keep your VPN connection automatically up in the background via different VPN gateways. See ***Direct Access***, page 140.

The newly created profile can now be chosen as preconfigured profile from the VPN client dialog. Instead of creating a new profile, the default profile can of course be edited.

Advanced configuration options found in die ***Advanced Settings*** tab are described in-depth in ***Barracuda Networks Control / Preferences Dialog***, page 137.

Note

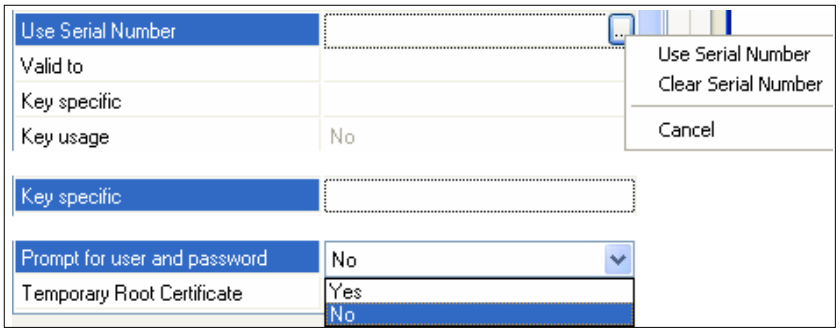
It is possible to create multiple profiles for several users with individual certificates.

In the following, several configuration fields will be encountered, which are to be edited by clicking into the either empty or already pre-filled field. One of three possible editing options will then be offered:

- ***a field where characters need to be inserted***

- ***a browse button including a context menu***
- ***a dropdown list (figure 10–11)***

Fig. 10–11 *Editing options of the VPN client dialog*



10.2.1 Functional Elements of the Barracuda NG Network Access Client's System Tray Icon

Installing Barracuda NG Network Access Clients adds a new icon to the system tray providing quick access to the main elements of VPN client and Barracuda NG Firewall R8. Double-click the icon to open the VPN client Connection dialog (10.3 Connection Dialog, page 132). Right-click the icon to make the following menu items available:

Fig. 10–12 *Context menu of the NG VPN Client system tray icon*

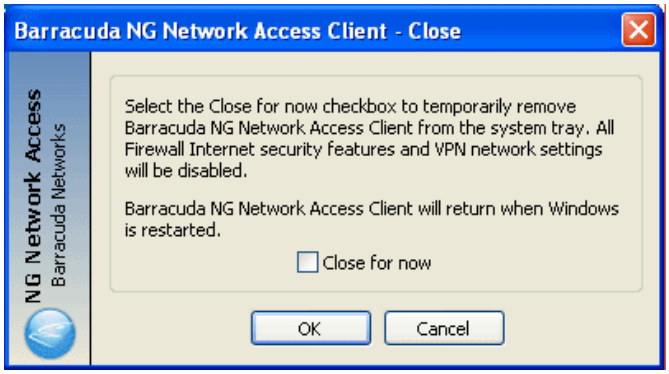
- ***About NG Network Access Client…***

Shows the version information.

- ***Shutdown NG Network Access Client…***

Shuts down the VPN for the current Windows session. The Barracuda NG Network Access Client will be available again after a system restart. Select the ***Close for now*** checkbox to proceed.

Fig. 10–13 *Close NG VPN Client informational window*



Caution

Shutting down the client will also disable the personal firewall, Take that into account especially if this is the only local firewall you're using.

Note

The whole Windows system needs to be restarted in order to restart the services.

- ***NG Access Monitor…***

Opens the Barracuda NG Access Monitor which provides information concerning the health state of the system.

- ***Secure Mode***
- ***Disable Firewall (Allow all Traffic)***

Allows you to change the operational modes of the Barracuda NG Personal Firewall. ***Secure Mode*** enables it, while ***Disable Firewall*** disables it. After installation, the firewall is disabled by default (Barracuda NG Personal Firewall, page 87).

- ***NG Personal Firewall…***

Opens the user interface of the Barracuda NG Personal Firewall (Barracuda NG Personal Firewall, page 87).

- ***NG VPN Client…***

Opens the Status dialog of the Barracuda NG VPN Client (10.4 Status Dialog, page 134).

10.2.2 The Barracuda NG VPN Client's Menu Bar

The following items are available in the Barracuda NG VPN Client's menu bar:

- ***File Download (Update)…***

This item is only available when a connection to a VPN Server has been established. Use it to download updates from the VPN server and install them on the client.

- ***Close***

Closes the NG VPN Client window.

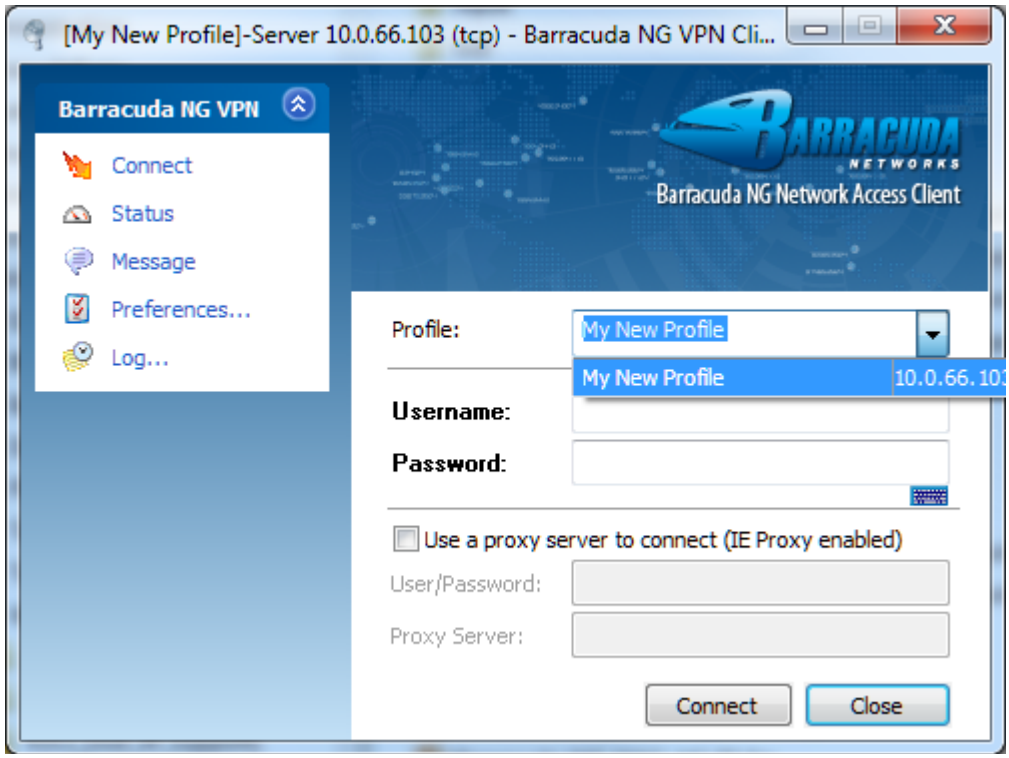
10.3 Connection Dialog

The NG VPN Client can be started in the following ways:

- ***Click Connect after left-clicking the icon in the system tray.***
- ***Use Start > All Programs > Barracuda NG Network Access Client > VPN Connector.***
- ***Use the Pre-Connector (12.2 VPN Connector, page 167). For using the Pre-Connector, a profile must already be configured.***
- ***Execute* rvpn.exe *(12.3 Remote VPN (rvpn), page 169). Before using Remote VPN, a profile must be configured.***

The following values are required for a successful login to the VPN server:

Fig. 10–14 *Profile selection in the Connect Dialog*



- ***Profile list***

Select a preconfigured profile for login here. The creation of new profiles is described in 10.6 Barracuda Networks Control / Preferences Dialog, page 137.

- ***Username and Password fields***

Depending on the chosen authentication method, username and/or password must be inserted here. With some authentication methods (Barracuda Networks authentication, X509 certificate), only a password might be required. If this is the case, then the username field is disabled.

- ***Use a proxy server to connect* checkbox**

  When use of a proxy server has been defined at profile creation time (10.6 Barracuda Networks Control / Preferences Dialog, page 137), then this checkbox will be selected by default, ***User/Password*** and ***Proxy Server*** will be displayed in the fields below at the same time. If the proxy server requires a password, you need to insert it into the respective field.

Note

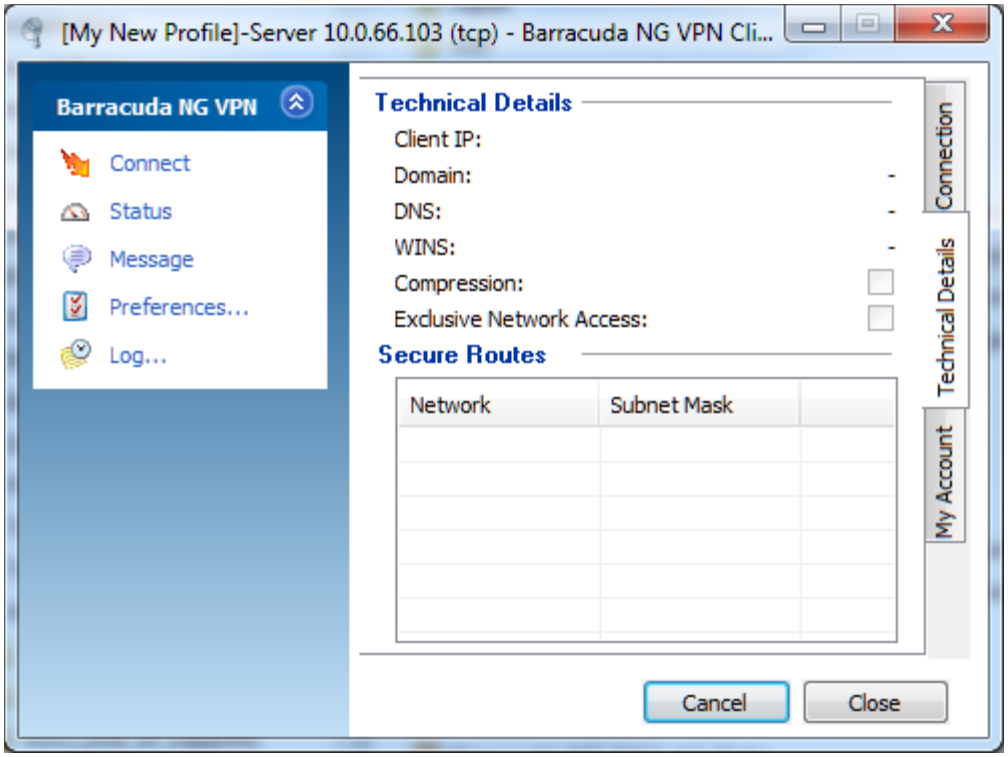
You can make use of the proxy server checkbox to override settings that have been defined at creation time of the profile. In certain cases you might want to define use of a proxy server though the profile settings do not require this (or vice versa), or you might need to use another proxy server than the configured one. The overriding option is especially useful if a user does not have administrator rights is therefore not able to change profile settings in general.

Click ***Connect*** to establish a connection to the VPN server.

10.4 Status Dialog

Use the Status dialog window to view properties of an established connection. Click ***Connect*** to establish a connection through the Status dialog. A profile for the connection needs to be chosen in the Connection dialog (10.3 Connection Dialog, page 132), though.

Fig. 10–15 *Status Dialog*



Technical Details tab:

Technical Details section:

- ***Client IP***

The assigned VPN client IP address (Source) and gateway IP address.

- ***Domain***

The assigned domain.

- ***DNS***

The assigned DNS IP address for the VPN connection

- ***WINS***

The assigned WINS address.

- ***Compression checkbox***

Selected if traffic between VPN server and client is compressed (***Compression***, page 144).

- ***Exclusive Network Access checkbox***

If Exclusive Network Access (ENA) has been activated on the VPN Server, then this checkbox is displayed selected.

Secure Routes section:

If secured routes have been assigned to the client by the VPN server, then their values will be displayed in the fields ***Network*** and ***Subnet Mask***.

Connection tab:

Connection section:

- ***Status***

Status information on the current connection, may it be active, initiating or shutting down.

- ***Duration***

The uptime for the current connection.

- ***VPN Server***

The VPN server to which the client currently is connected.

- ***VPN Server Time***

Local time on the VPN server.

- ***Compression checkbox***

Enable or disable compression.

- ***Exclusive Network Access checkbox***

If this is enabled, then only network resources available through the VPN can be accessed.

- ***Client IP***

The client's IP address within the VPN.

Activity section:

- ***Bytes Sent, Bytes Received***

Amount of traffic transferred so far during the current session.

- ***Bandwidth***

Graphical representation of the currently used bandwidth.

My Account tab:

Authentication section:

- ***Authentication scheme***

The currently method for authentication used for the currently established connection. Shows a respective status message if the VPN connection is not active.

In the same section below the authentication scheme entry, a set of properties for the currently active auth scheme will be displayed, such as user name or certificate information.

Data integrity and encryption section:

- ***Authentication Algorithm***

The currently used auth algorithm.

- ***Encryption Algorithm***

The currently used encryption algorithm.

- ***Tunnel Mode***

  The currently used transport mode for the VPN tunnel. Can display a value of TCP, UDP or Hybrid.

Cancel button:

Use this button to terminate a connection. Only shown if a connection is currently active.

Connect button:

Click this button to initiate a connection.

Close button:

Click this button to close the VPN client window. The VPN control window will remain open.

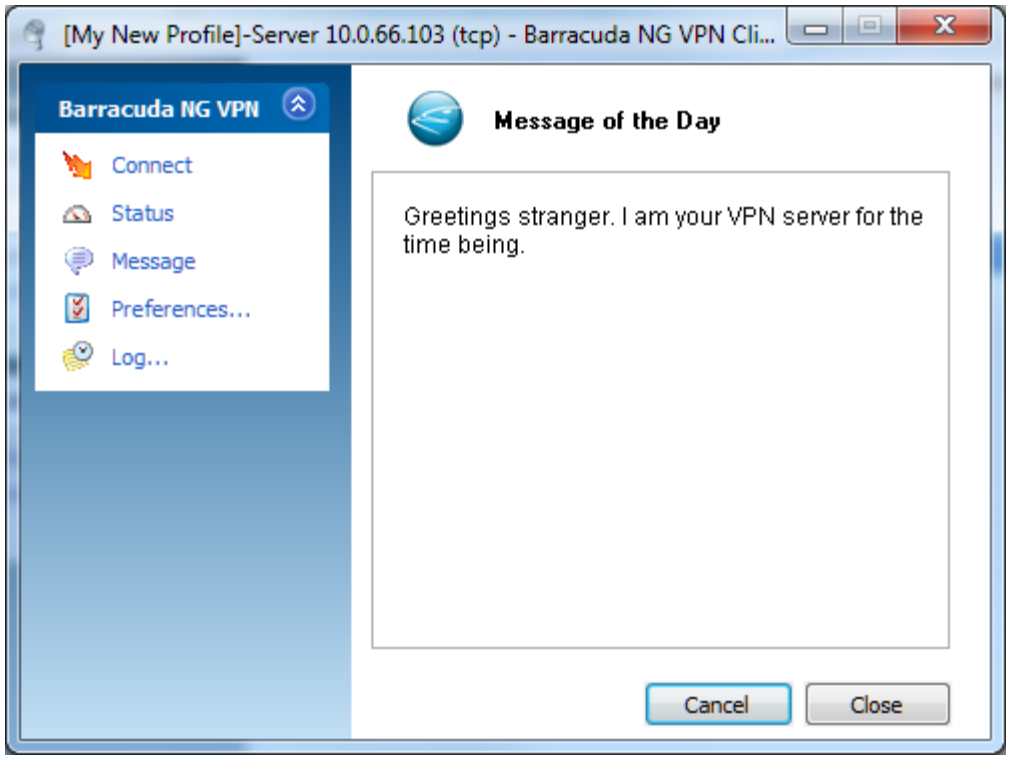
Change Server Password… link:

This link is only available as long as an active connection to the VPN server is established (***Barracuda Networks authentication*** only). It enables you to change your password on the server. Open the configuration dialog, insert a new password, confirm it and attest authenticity by inserting the current server password.

10.5 Message Dialog

This window displays the initial welcome message configured on the VPN server.

Fig. 10–16 *Message dialog window*



10.6 Barracuda Networks Control / Preferences Dialog

Click ***Preferences*** to open the ***Barracuda Networks Control*** panel.

Barracuda Networks Control is the user interface for configuration of profiles and Barracuda NG VPN adapter settings and the management of certificates.

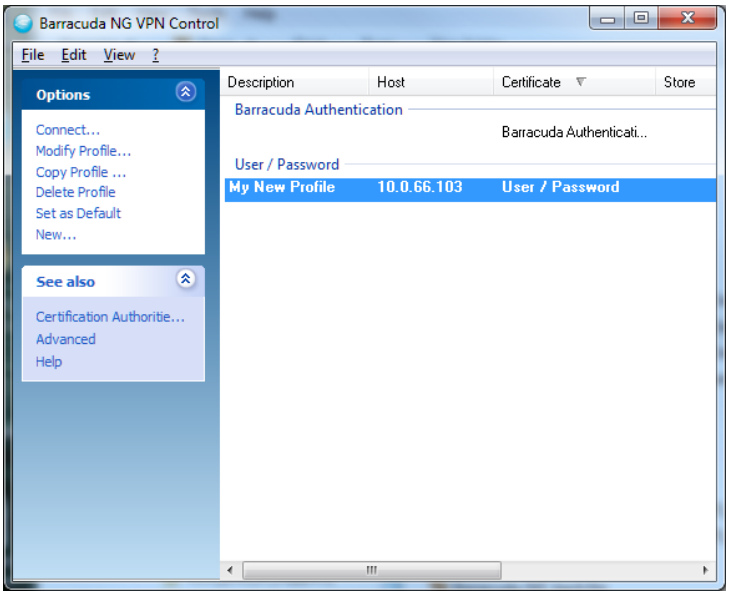
Barracuda Networks Control is also accessible via the Windows Control panel. Shortcut icons reside within the **Network and Internet Connections** and the **Security Center**.

The Barracuda Networks Control window is divided into a menu (***Options***) on the left and a configuration area on the right side.

At start-up, Barracuda NG VPN Control opens with the ***VPN Profiles*** configuration area. Further available for configuration are ***Certification Authorities...*** (10.6.2 Certification Authorities Configuration Window, page 138) and ***Advanced*** settings (10.6.3 Advanced, page 139).

10.6.1 VPN Profiles Configuration Window

Fig. 10–17 *Barracuda NG VPN Control*



All available profiles are listed in the overview window ordered by the connection type they were configured with. The connections are listed with the following attributes:

- ***Description***

The name of the profile.

- ***Host***

The configured VPN server to connect to.

- ***Certificate***

The certificate and authentication type used to connect (***Barracuda Networks authentication***, ***User / Password*** or ***X509 authentication***).

- ***Store***

The store into which the certificate was saved.

- ***Status***

The connection status. If you are not connected, you may click ***Connect…*** in the context menu in order to establish a connection. On the other hand, if you are connected, then you can click ***Disconnect*** in the context menu to terminate a connection.

- ***ID***

This is the profile ID.

Options menu:

- ***Connect...***

Select a VPN profile and click ***Connect*** to connect to a VPN server.

- ***Modify Profile…***
- ***Copy Profile...***
- ***Delete Profile...***

Modify, copy or delete an existing profile.

- ***Set as Default***

Defines the currently marked profile as new default profile. The default profile is displayed with bold letters in the overview window.

- ***New…***

Click ***New…*** to create a new VPN profile.

The profile configuration itself is done through the ***Connection Entries*** and ***Advanced Settings*** tabs (see 10.6.4 Connection Entries Tab, page 141 and 10.6.8 Advanced Settings Tab, page 143).

Context menu

Right-click into configuration area to open the ***Barracuda Networks Control*** context menu. The following additional items are available here:

- ***Disconnect***

Use this menu item to terminate a connection.

- ***Show List / Show Groups***

Arranges the profiles either in List or in Group view (default).

10.6.2 Certification Authorities Configuration Window

Manage certificates in the ***Certification Authorities*** configuration area. The following actions are possible:

Options section:

- ***View…***

Opens a window with detailed certificate information.

- ***Remove…***

Deletes the selected certificate from the certificate store.

- ***Import…***

Imports the certificate to the certificate store. Supported certificate types are: **DER encoded binary x.509**, **PKCS #12 certificates**, **PEM encoded binary x.509**

Export Certificate To section:

- ***File…***
- ***Clipboard***

Exports the certificate to a text file or to the clipboard for further use in another place.

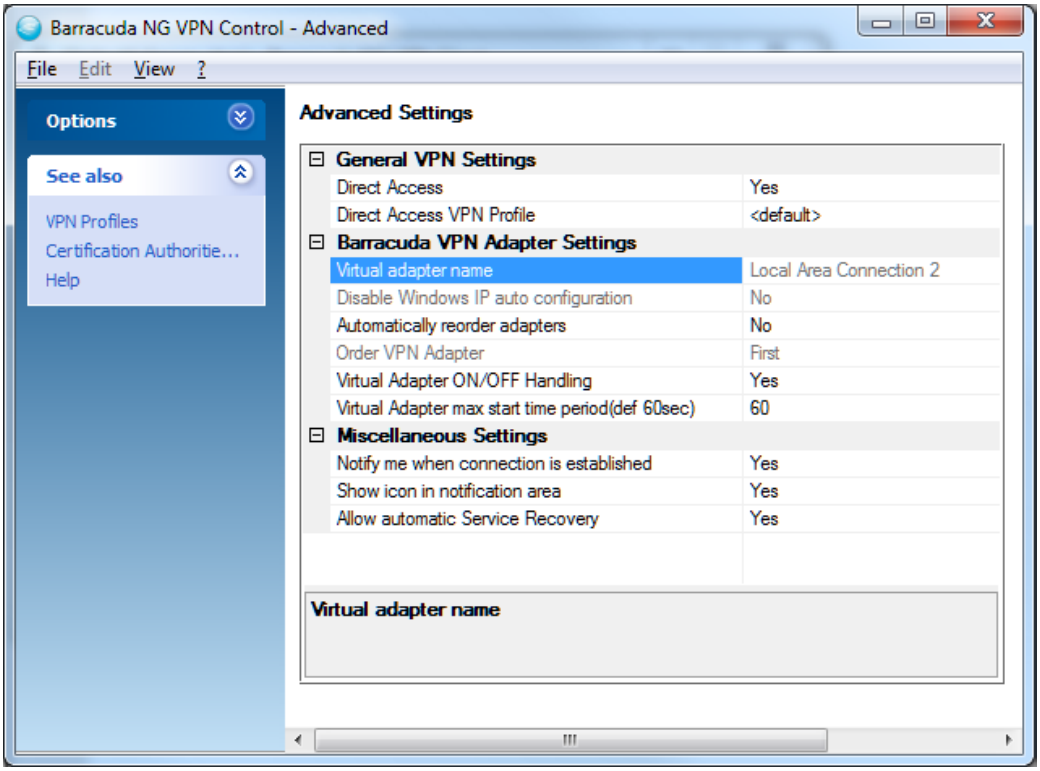
Note

For successful authentication, both certificates, client **AND** root certificate that is, must be available. If your certificate does not yet include the root certificate, add it here.

10.6.3 Advanced

Configure specific Barracuda NG VPN adapter settings here.

Fig. 10–18 *VPN Adapter Settings*



General VPN Settings section:

- ***Direct Access***

The VPN client can be configured so that it automatically reconnects to different gateways, if available. Upon an unwanted disconnection, reconnecting to the same gateway will be tried for three times. If this fails, a so-called "path finder connection" will be initiated, trying a variety of pre-defined gateways and finding the fastest one. This gives mobile users seamless access to corporate networks wherever they have Internet access. The reconnection process can be configured to happen in the background without any user interaction. The advanced reconnection mode can be activated by setting this to ***Yes***.

- ***Direct Access VPN Profile***

The name of the VPN profile that is used for establishing Direct Access connections.

Barracuda NG VPN Adapter Settings section:

- ***Disable Windows IP Auto Configuration***

Disable Windows XP's built-in automatic IP address configuration of the adapter.

- ***Automatically reorder adapters***

Place the VPN client's virtual adapter within the Windows adapter bindings right at the position that is configurable through ***Order VPN Adapter***.

- ***Order VPN Adapter***

The position of the VPN client's virtual adapter within the Windows adapter bindings. The sequence affects e.g. the DNS resolution of short DNS names or the function of Windows Remote Assistance.

- ***Virtual Adapter ON/OFF Handling***

Disables the virtual adapter as long as there is no active VPN connection. The adapter will be re-enabled as soon as a VPN connection is established.

- ***Virtual Adapter max start time period (def 60sec)***

Waiting period in seconds for an enabled adapter. You may increase this value on slow systems. Default and recommended value is ***60***.

Miscallenous Settings section:

- ***Notify me when connection is established***

Display a notifying popup as soon as a VPN connection has successfully been established.

- ***Show icon in notification area***

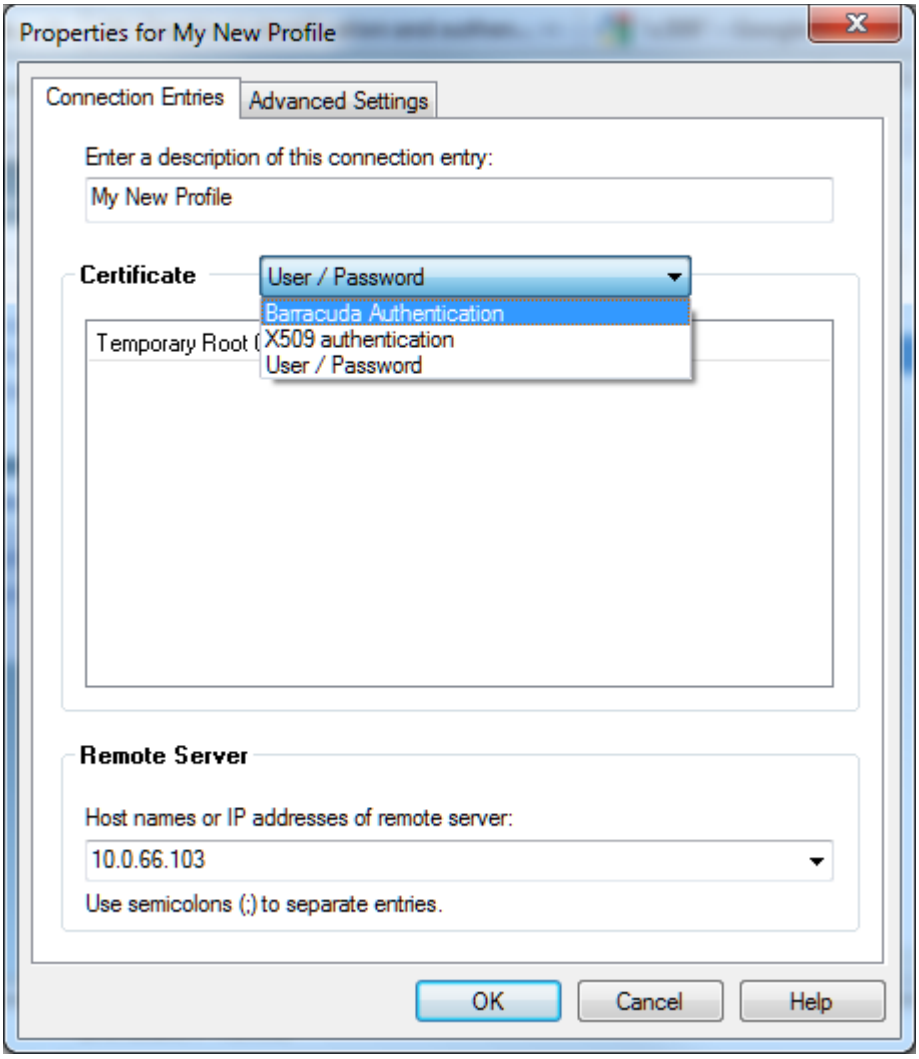
Display a status icon for the connection within the notification area of the task bar.

- ***Allow automatic Service Recovery***

Restart the service automatically in case of service termination.

10.6.4 Connection Entries Tab

Fig. 10–19 *Connection Entries tab*



- ***Enter a description of this connection entry* field**

Insert a profile name into this field. The name entered will be displayed as profile name in the Connection dialog window.

Certificate section:

Choose the authentication method required by the VPN server. The chosen authentication type appoints further configuration parameters.

Remote Server section:

- ***Host names or IP addresses of remote server:***

The VPN server's address. If entering a host name, make sure that this host name is DNS-resolvable. Separate multiple entries using semicolons (";").

10.6.5 Barracuda Authentication

Caution

Barracuda Authentication requires a valid certificate file (*.lic). The .lic file must be saved locally on the client system using it.

The following parameters are available for Barracuda Authentication:

List 10–1 *Parameters used with Barracuda NG authentication*

Parameter	Description
File	Select the certificate (*.lic) file needed for authentication at the VPN server.
Hash	**READ-ONLY** After a certificate has been loaded, its hash is displayed in this field.
Certificate File Password	**Only editable if a certificate file has been loaded.** The password for certificate usage can be changed here. Enter the new password and confirm it.

Note

The creation of a Barracuda Authentication related profile can be rudimentary adapted by including an .ini file into the creation process. If you want to make use of this option, then have a look at 10.6.8 Advanced Settings Tab, page 143 first. Subsequently, refer to 10.6.9 Adaptation of Profile Creation using an .ini file (Barracuda NG Authentication only), page 146 for further details.

10.6.6 X509 Authentication

The following parameters are available for X509 authentication:

Caution

Selecting this method requires a valid X.509 certificate (*.).

List 10–2 *Parameters available for use with X509 authentication*

Description	Description
Subject	After the X.509 certificate has been selected, its subject is displayed here.
Issuer	Displays the issuer of the selected X.509 certificate.
Use serial number	Defines if the certificate's serial number gets used in the authentication process.
Valid to	Displays date and time when the X.509 certificate looses validity.
Key specific	Hash value of the certificate file.
Key usage	Value of the KeyUsage keyCertSign bit. Possible values are Exchange (public key exchange) or Signing (digital signature).
Private Encrypt	Switches encryption procedure (private key for encryption, public for decryption) depending on whether crypto API is supported or not.
Prompt for user and password	Set to yes to request both, certificate and user/password validation.
Temporary Root Certificate	As soon as a temporary root certificate has been provided by the server, it can be viewed with the menu item ***Show…*** or deleted with the menu item ***Clear***.
Show external X509 Certificate	If an external X.509 certificate has been loaded, its properties can be viewed here.

List 10–2 *Parameters available for use with X509 authentication*

Description	Description
External File	Path to the external X.509 certificate.

10.6.7 User / Password

The following parameter is available for User / Password authentication:

List 10–3 *Parameters used with User/Password authentication*

Parameter	Description
Temporary Root Certificate	This field is set to the the value ***Not Available*** as long as a connection to the VPN server has never been established or if the certificate file has been deleted. As soon as a certificate is available, it can be viewed with the menu item ***Show…*** or deleted with the menu item ***Clear***.

10.6.8 Advanced Settings Tab

Individual profile settings related to connection details can be configured from within the ***Advanced Settings*** tab of the respective profile

Configure the following section when connecting to the VPN server over a proxy.

List 10–4 *Advanced Settings tab – Proxy Settings section*

Parameter	Description
via Proxy [Default: No Proxy]	Whether a proxy should be used and if, of which type it is.
Proxy[:Port] [-]	IP address and port for the proxy. If ***HTTP Proxy*** is selected, the system's proxy server is automatically set as default.
Proxy user [-]	**Note:** Only editable if ***HTTP Proxy*** is selected. The username required for authentication at the proxy server, if needed.
Domain [-]	**Note:** Only editable if ***HTTP Proxy*** is selected. The proxy server's domain.
Simulate SSL [No]	**Note:** Only editable if ***HTTP Proxy*** is selected. Set to ***Yes*** when using a proxy server requiring an SSL handshake.

Data integrity and encryption Section:

Note

Manipulations in the following fields should only be made by experts. Please take into consideration that the VPN server must support the settings configured here.

List 10–5 *Advanced Settings tab – Data integrity and encryption (ESP) section*

Parameter	Description
Authentication algorithm [Default: MD5]	The algorithm to be used for authenticating to the VPN server.

List 10–5 *Advanced Settings tab – Data integrity and encryption (ESP) section*

Parameter	Description
Encryption algorithm [AES]	The algorithm to be used for encryption.
Tunnel Mode [Response (UDP)]	The protocol to be used for tunnel traffic. The available options depend on the chosen proxy type: ***- Response (UDP)*** for Socks 5 ***- Reliability (TCP)*** for HTTP Proxy and Socks 4 - Selecting ***No Proxy*** gives access to both protocol types and offers an additional one called ***Optimized (Hybrid)*** indicating a combination of Response (UDP) and Reliability (TCP).

Tunnel Settings section:

List 10–6 *Advanced Settings tab – Tunnel Settings section*

Parameter	Description
Virtual Adapter Configuration [Default: Direct assignment]	The method to be used for gathering IP addresses. ***- Direct assignment*** - uses WMI (Windows Management Instrumentation) for assigning the IP address; recommended if DHCP is not available due to security aspects. ***- Use internal DHCP assignment*** - uses the integrated DHCP (Dynamic Host Configuration Protocol) for assigning the IP address ***- Assign IP address manually*** - IP address is entered manually in NIC properties
Compression [Yes]	***Yes*** triggers the Barracuda NG VPN Client to request compressed traffic. The server may or may not accept the request depending on both its configuration and the license type assigned to the VPN client. Client compression is only available to those clients that have assigned a secure connector license. **Note:** The gateway hosting the VPN server must hold a valid BOB license to use this feature. Refer to the respective product guide for licensing details. **Note:** To activate compression operability, the VPN Service needs to be restarted after BOB license installation.
Use Access Control Service	Validate the client's status through the Access Control Service before a VPN connection is established.
NAC intercept VPN connection [Default: Yes]	Configure here whether the Health Agent should intercept the VPN connection phase or wait until a VPN connection is established. Recommended value: ***No***.
Access Control Timeout [Default: 30]	Timeout value in seconds for the VPN Service to wait for the Health Agent. Recommended value: ***30***.
WLAN Roaming [Default: Yes]	Different IP addresses from the same profile are tried if a connection breaks. Recommended value: ***Yes***.
Fast Reconnect [Default: Yes]	Choose here whether to be prompted for user name and password on every connection attempt or not, enabling seamless automatic reconnecting. This is also important in conjunction with one-time passwords. Recommended value: ***Yes***.
Reconnect immidiately	Reconnect immidiately upon a connection break if set to ***Yes***.
One Time Password [No]	The behavior for reconnecting. If set to ***Yes***, then the password is queried anew when reconnecting. If set to ***no***, then reconnection is automatically performed without a password query.
Allow ENA Connection [Yes]	Allows/blocks ENA (Exclusive Network Access) connections. **Note:** For successful VPN connection establishment between a server forcing ENA and a client, this value must be set to ***Yes***. Otherwise, no connection is possible.
Allow Sending Offline Rule Set [Yes]	Enable the client to receive and use offline firewall rulesets from the VPN server. Offline firewall rulesets are effective as long as no VPN connection is active.
Silent Mode (No Keep Alive) [No]	Break all non-relevant communication over the VPN tunnel (for example for dial-up connections).
Keep alive (seconds) [10]	The time value in seconds to keep an idle VPN tunnel alive.
Soft Hearbeat [Default: No]	IKeep a VPN tunnel up by interpreting normal VPN traffic as keepalive traffic. Useful if the special keepalive packets are dropped somewhere between client and server.
Enable VPN Tunnel Probing [Default: Yes]	Probe a VPN tunnel prior to establishing a VPN connection. If this is set to ***Yes***, the reachability of configured IP addresses will be tested prior to establishing a tunnel. Recommended value: ***Yes***.
Check Round Trip Time (RTT) [Default: Yes]	Setting this to ***Yes*** will activate automatic selecting of the fastest VPN server by measuring the roundtrip times of all available servers prior to connecting if more than one server IP address has been configured in the profile. Recommended value: ***Yes***.

List 10–6 *Advanced Settings tab – Tunnel Settings section*

Parameter	Description
Terminate Countdown (sec.) [2]	Period in seconds to wait until a VPN connection is terminated.
After reconnect adapter reset	Reset the virtual adapter after reconnecting. This may help resolving connectivity issues.
Connect retry time (sec) [Default: 60]	A timeout period in seconds which will be used for reconnection attempts to the given profile. The lower this value is, the faster the connection to the fallback profile will be established, if defined. Recommended value: ***60***.
Fallback Profile	Fallback profiles can be defined here. These will be tried next if a connection to the respective profile cannot be established.

Always Connect section:

List 10–7 *Advanced Settings tab – Always Connect section*

Parameter	Description
Disable Active Directory Scan [Default: No]	Direct Access can be disabled if an Active Directory is found within the currently active connection. This ensures in office environments that the local WiFi is used by preventing a search for different gateways upon disconnecting. Recommended value: ***No***.

User Interface Settings section:

List 10–8 *Advanced Settings tab – User Interface Settings section*

Parameter	Description
Remember logon user name	The VPN connection GUI remembers the last entered user name. For security reasons, this parameter is disabled by default.
Show Popup [Yes]	Specifies whether pop up messages are displayed for incoming and outgoing connections.
Close after Connection [No]	Causes the VPN client dialog to close as soon as a VPN connection has successfully been established.
Save new Certificate Unattended [No]	Locally save new certificates without any user interaction.

OS Settings section:

List 10–9 *Advanced Settings tab – OS Settings section*

Parameter	Description
Start Script [-]	Define scripts to be started automatically on connecting (e.g. to automatically modify Internet Explorer settings).
Stop Script [-]	
Disconnect when user logs off [Yes]	The behavior expected when logging off from Windows (***Start > Log Off***): When set to ***Yes***, then the VPN connection is terminated on performing a system logout. If set to ***No***, then the VPN connection remains active.
Enable MS Logon [No]	Causes the user/password credentials entered during the log-in procedure on the Windows system to be sent automatically to the Barracuda NG Firewall Smart/Secure Connector. **Note:** On establishing a VPN connection, these credentials are automatically used for authentication. Using other credentials than these is not possible.
Certificate Store Flag	Assign the certificate location within Microsoft Windows' Certificate Management store.
Certificate Store [MY]	Assigns the certificate location within Microsoft Windows' Certificate Management store.

10.6.9 Adaptation of Profile Creation using an .ini file (Barracuda NG Authentication only)

Some parameters configurable in the ***Connection Entries*** and ***Advanced Settings*** (10.6.3 Advanced, page 139) tabs can be passed to the NG VPN Client through an `.ini` file. When a profile with ***Barracuda NG authentication*** is created the Barracuda NG Firewall Connector looks for an `.ini` file in the same directory as the .lic file is retrieved from. The `.ini` file is expected to be named equally to the `.lic` file (for example `C:\licenses\barracuda_user.lic` requires `C:\licenses\barracuda_user.ini`). If the `.ini` file is available, the values defined there will be used for the VPN profile.

The following parameters can be defined through the .ini file:

Fig. 10–20 *Example for an .ini file*

```
[Settings]
Description=Profile Name
Server=192.168.10.10
Proxy=proxy.sample.com:3128
ProxyType=HTTP
ProxyUser=testUser
ProxyDomain=SAMPLE
Dhcp=1
connectmode=tcp
;[tcp, udp, hybrid]
```

Caution

Remove unnecessary options from the .ini file.

- ***Description***

Name of the profile.

- ***Server***

IP address of the VPN server.

Note

The proxy related parameters must be removed from the .ini file, if connection establishment is not handled via a proxy server.

- ***Proxy***

URL or IP address of the proxy server.

- ***ProxyType***

Proxy server type. Possible options are: ***HTTP***, ***Socks4*** and ***Socks5***

- ***ProxyUser***

User name possibly needed for proxy authentication.

- ***ProxyDomain***

Windows domain within which the user is able to authenticate.

- ***Dhcp*** ***[corresponds to Virtual Adapter Configuration dropdown list in the Advanced Settings tab]***

Behavior of a DHCP client.
Possible options are:
2 IP address is assigned directly (using **W**indows **M**anagement **I**nstrumentation)
1 IP address is assigned dynamically (DCHP)
0 IP address is configured statically

- ***connectmode* [corresponds to Tunnel Mode dropdown list in the Advanced Settings tab]**

This parameter specifies the used connection mode. By default, this parameter is set to ***tcp***. The alternatively available modes are shown in brackets (*[]*). Please remove the bracket and its entries in order the get a working setup file.

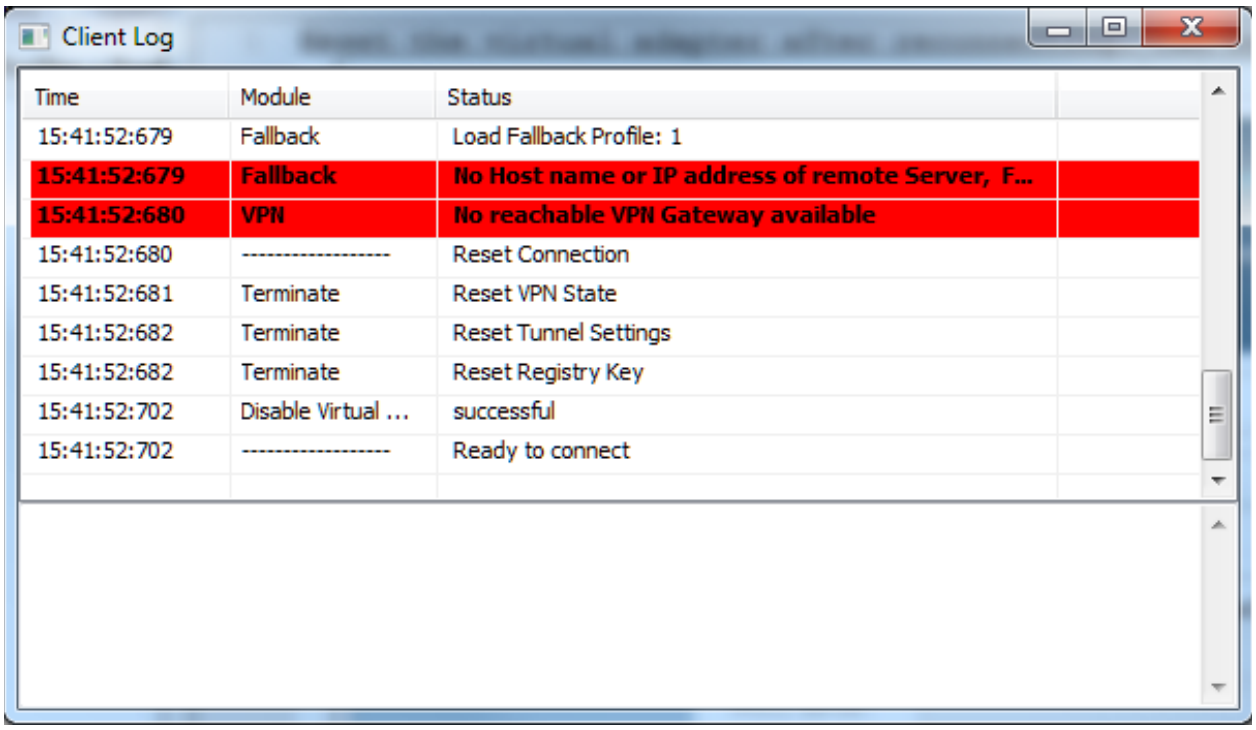
Note

When changing the protocol to ***udp***, be sure to delete all parameters related to the proxy.

10.7 Log Window

The log information screen displays information collected from the initiation of a connection attempt until disconnecting. Purely informational messages are logged conjointly with messages related to connection errors or other errors.

Fig. 10–21 *Log window*



- ***Time* row**

The log entry's time stamp.

- ***Module* row**

The module the respective log entry refers to.

- ***Status* row**

The status of several actions such as ***Internal loop***, ***Add Routes*** (added routes), ***Refresh IP*** (client IP), etc.

Chapter 11
Barracuda NG Access Monitor

11.1 Overview

11.1.1 Access Monitor

The **Access Monitor** is the key component of Barracuda NG Network Access Client. Its responsibilities include:

- ***Collecting information from the client computer necessary for health evaluation, including***
  - **Workstation identity information**
  - **Operating system information and patch level**
  - **Antivirus and Antispyware information**
- ***Communication with the Access Control Server***
- ***Taking security measurements dependent on the health evaluation result returned by the Access Control Server. This includes***
  - **Downloading and installing necessary updates**
  - **Restricting network access**
  - **Executing Antivirus / Antispyware updates and starting scans or updates**

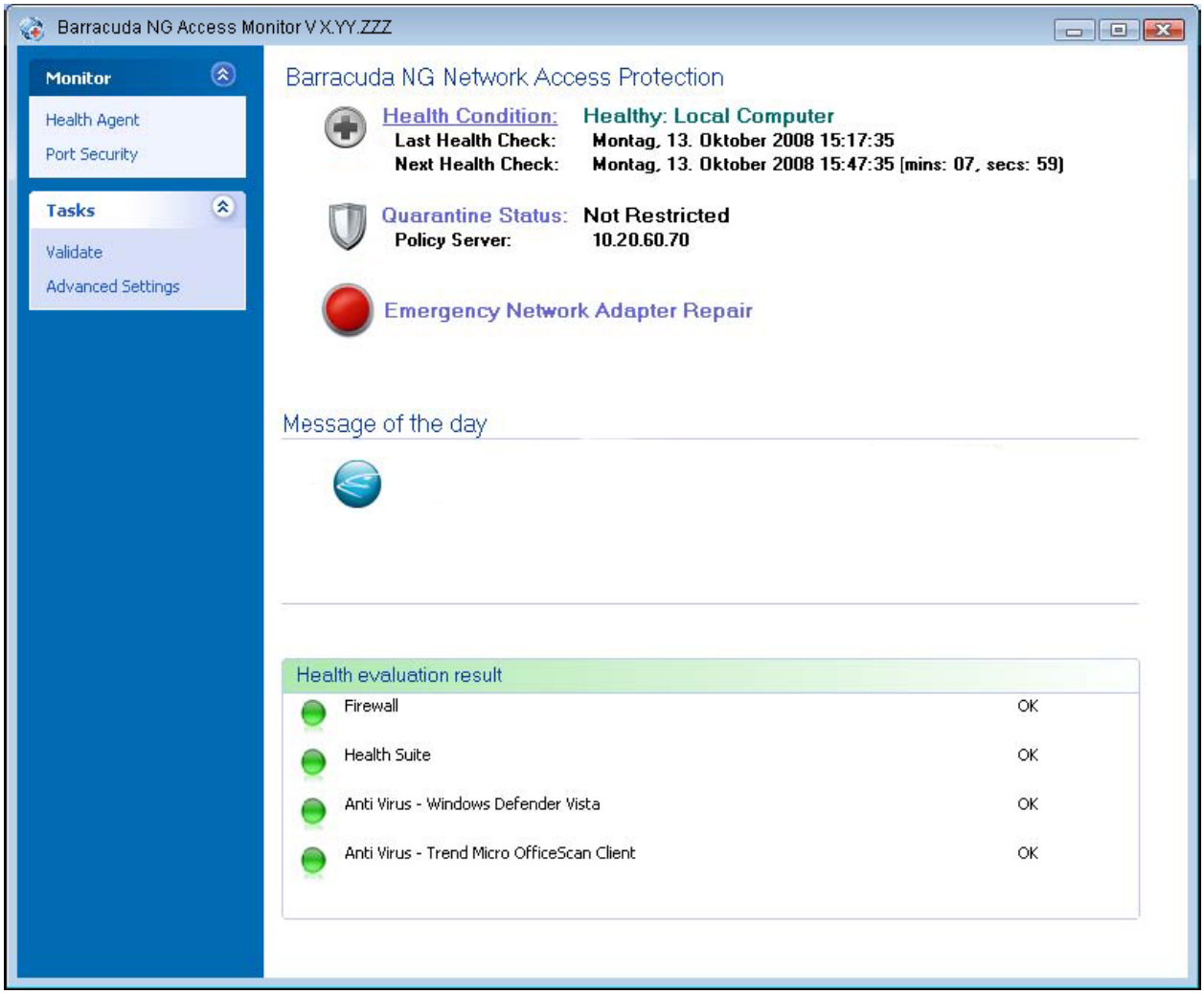
11.1.2 Port Security

The Barracuda NG Network Access Client implements the IEEE 802.1X standard. The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The credentials for authentication are obtained by the client computer from the Access Control Server, based on the client computer's health evaluation result, restricting or granting network access to the client computer.

11.2 Monitoring

11.2.1 Health Agent

Fig. 11–1 *Barracuda NG Access Monitor*



The **Barracuda NG Access Monitor** provides all necessary information regarding the client computers health state and network restriction.

Table 11–1 *Barracuda NG Access Monitor*

Property	Description
Health Condition	There are 3 different health states: • ***Healthy*** The client computer complies with the policy configured on the Access Control Server • ***Unhealthy*** The client computer does not comply with the policy; actions need to be taken to meet the health requirements. • ***Untrusted*** There is no rule defined for the client computer, thus he has only restricted network access.

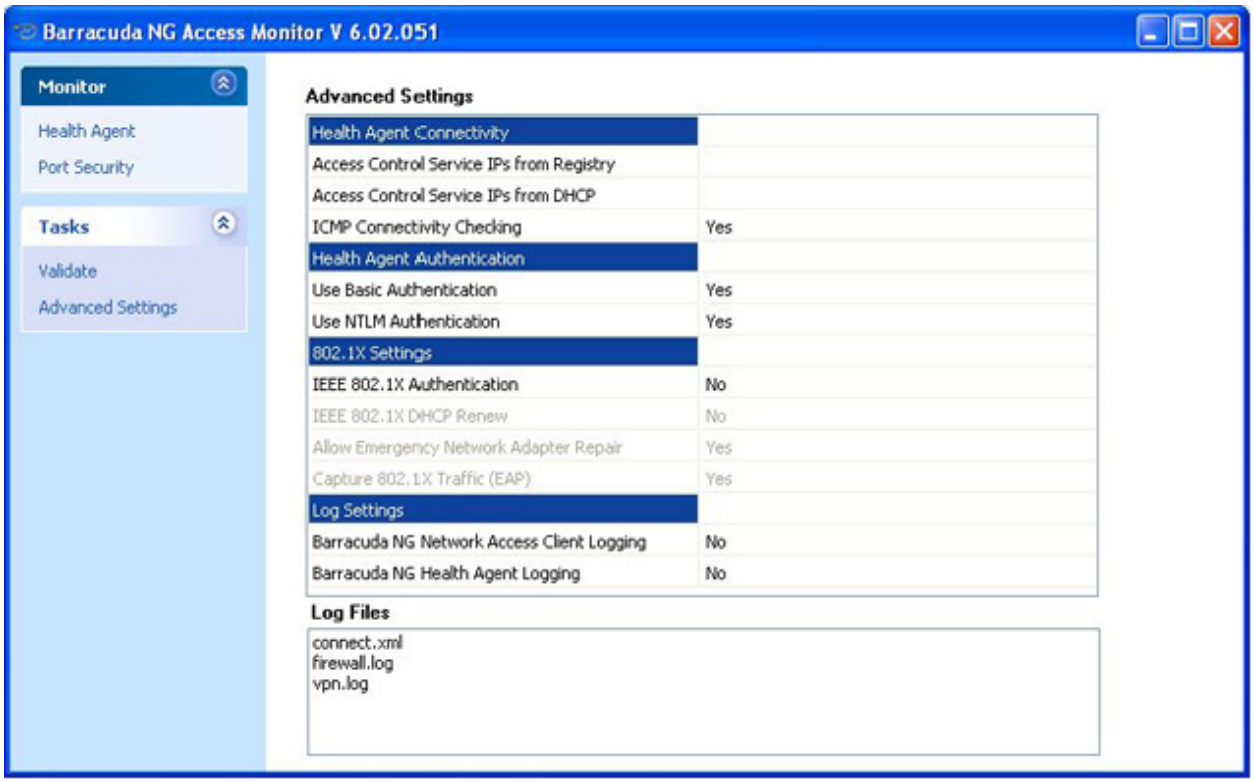
Table 11–1 *Barracuda NG Access Monitor*

Property	Description
Client Origin	• ***Local Computer*** Health evaluation for the client computer is mandatory; if the health evaluation for the client computer is not successful, evaluation based on user credentials is not possible. • ***Current User*** When multiple users use the same computer it is possible to start health evaluation based on user credentials, matching each user with its own policy depending on his role in the network. • ***VPN*** When connected to the Access Control Server using a VPN connection
Last Health Check	Date and time when the last health evaluation was performed.
Next Health Check	Date and time the next health evaluation will be performed.
Quarantine Status	The quarantine status depends on the health condition of the client computer. Three states are provided for policy based network access, these include: • ***Not Restricted*** Full network access is granted when the health evaluation result returns the health state ***Healthy***. • ***Probation*** When the client computer does not meet the configured health requirements, it will enter probation state. In this state he is not restricted in order to contact network resources necessary to meet all health requirements. If the following health evaluation does not return a ***Healthy*** state he will enter restricted network access mode. • ***Restricted*** If restricted network access is active, the Client will activate the quarantine rule set assigned by the Access Control Server. **Note:** It is possible to configure two quarantine rule sets, one for when the client computer does not meet the health requirements and is unhealthy. The other for when the client computer is untrusted because no rule is defined for it.
Access Control Server	IP or hostname of the Access Control Server that is being contacted for health evaluation. See 11.3.2 Access Control Server IPs from Registry, page 160 and 11.3.3 Access Control Server IPs from DHCP, page 160.
Emergency Network Adapter Repair	If enabled this allows you to reset the network adapters managed by the Port Security wpa_supplicant. To enable or disable see 11.3.12 Allow Emergency Network Adapter Repair, page 163.
Image of the day	Custom welcome image configurable on the Access Control Server, for following states: • ***Local Computer - healthy, limited access*** • ***Current User - healthy*** • ***VPN - healthy***
Message of the day	Custom welcome message supporting Unicode configurable on the Access Control Server for following states: • ***Local Computer - healthy, limited access*** • ***Current User - healthy*** • ***VPN - healthy, limited access***
Health evaluation result	This shows the actual health evaluation result. It holds an entry for every health criteria and if it complies with the policy configured. If a criterion does not meet the requirements, a description of necessary actions in order to comply with the policy is shown.

11.2.2 Advanced Status information

If more information is required, the Barracuda NG Access Monitor provides additional information through the Barracuda NG Access Monitor Advanced dialog. This can be opened by either clicking the ***Health Condition*** link (see: ***Health Condition***, table 11–1, page 150) or the Quarantine Status link (see: ***Quarantine Status***, same table) in the Health Agent view.

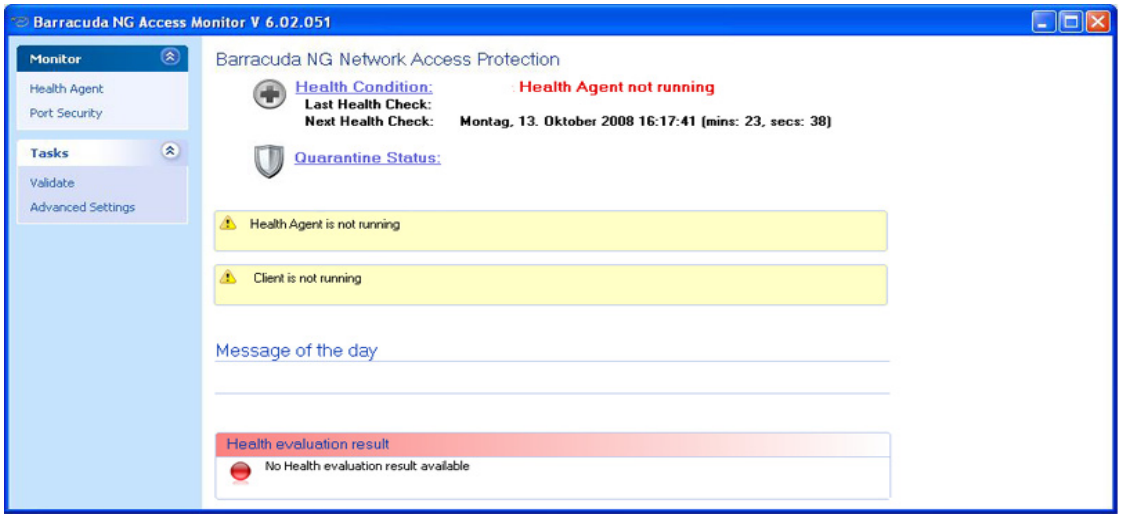
Fig. 11–2 *Barracuda NG Access Monitor Advanced*



11.2.3 Service Status

If either the Client service or the Barracuda NG Access Monitor Agent service, both vital for normal operation, is not running, a message will be shown for either of them (figure 11–3). No message indicates that both services are operating normally as intended.

Fig. 11–3 *Neither Client nor Barracuda NG Access Monitor service is running*



11.2.4 Communication Status

Whenever the Barracuda NG Access Monitor is working, a status message is displayed below the message of the day group (figure 11–4). While the Barracuda NG Access Monitor is communicating it is not possible to start a health evaluation. There are following communication states for the Barracuda NG Access Monitor:

Table 11–2 *Health Agent states*

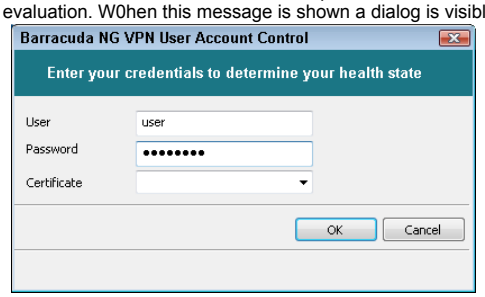
State	Description
Initializing	The Barracuda NG Access Monitor is initializing before entering operational state.
Termination	The Barracuda NG Access Monitor service is shutting down and freeing all resources.
Pending communication, validating	A health evaluation has been started, waiting for the result from the Access Control Server.
Pending communication, downloading	Files such as rule sets, patches and other, necessary to comply with the policy the client matched with are being downloaded.
Waiting for user input	The Barracuda NG Access Monitor requires user credentials for user specific authentication and health evaluation. W0hen this message is shown a dialog is visible to enter the user credentials. 

Fig. 11–4 *Barracuda NG Access Monitor communicating with the Access Control Server*

11.2.5 Connection Errors

If, for any reason, the Access Control Server can not be reached at the configured IP addresses for health evaluation, a connection error will be shown as in figure 11–5. See 11.3.4 ICMP Connectivity Checking, page 161 later on for more details on this specific connection error.

The connection error as in figure 11–6 occurs when the Barracuda NG Access Monitor has no Access Control Server IP addresses configured.

There are some options to resolve this:

- ***Configure a valid Access Control Server IP address locally (see 11.3.2 Access Control Server IPs from Registry, page 160)***

Use these instead if the Access Control Server IP addresses are distributed by DHCP:

- ***By using the Emergency Network Adapter Repair function/button (see 11.3.12 Allow Emergency Network Adapter Repair, page 163)***
- ***By using the operating system's built in ipconfig tool to obtain a new IP address for the client computer which will include a Access Control Server IP address to connect to***

In order to verify if an Access Control Server IP address was received through DHCP, look up the ***Barracuda NG Access Monitor Access Control Server IPs*** dialog. (see 11.3.3 Access Control Server IPs from DHCP, page 160).

Fig. 11–5 *Connection error using ICMP connectivity checking (see 3.1.3)*

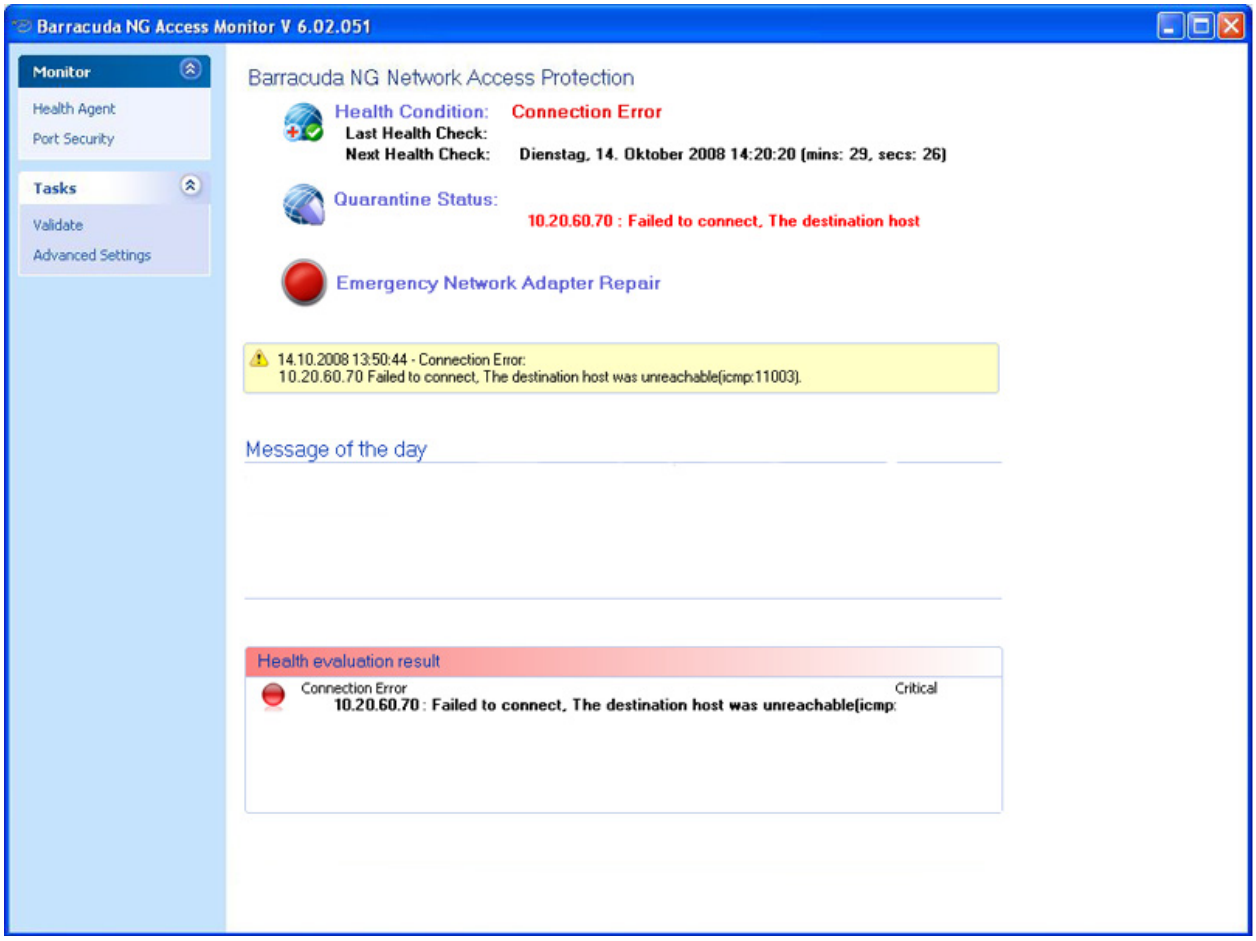
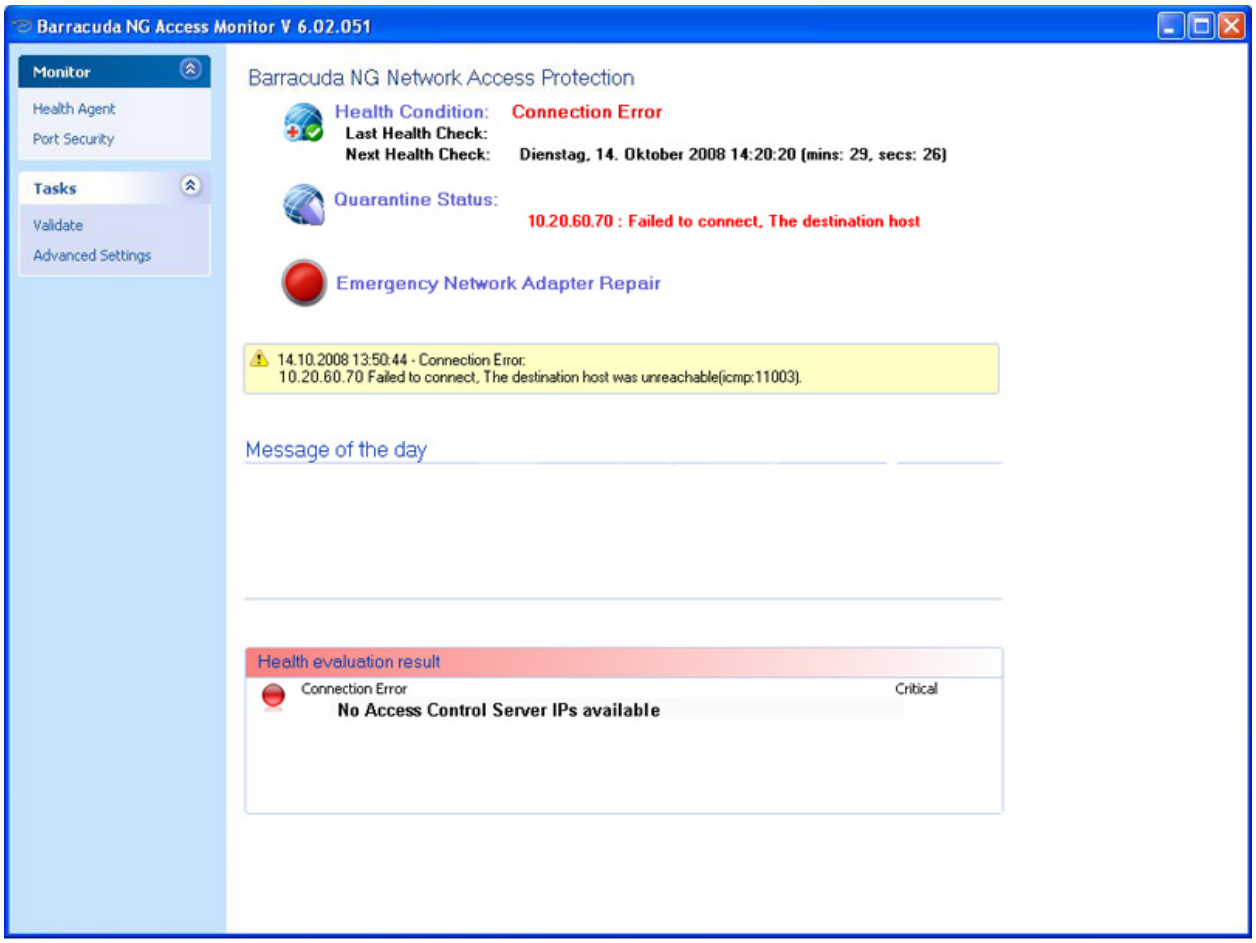


Fig. 11–6 *Connection error because no Access Control Server IP addresses are configured*



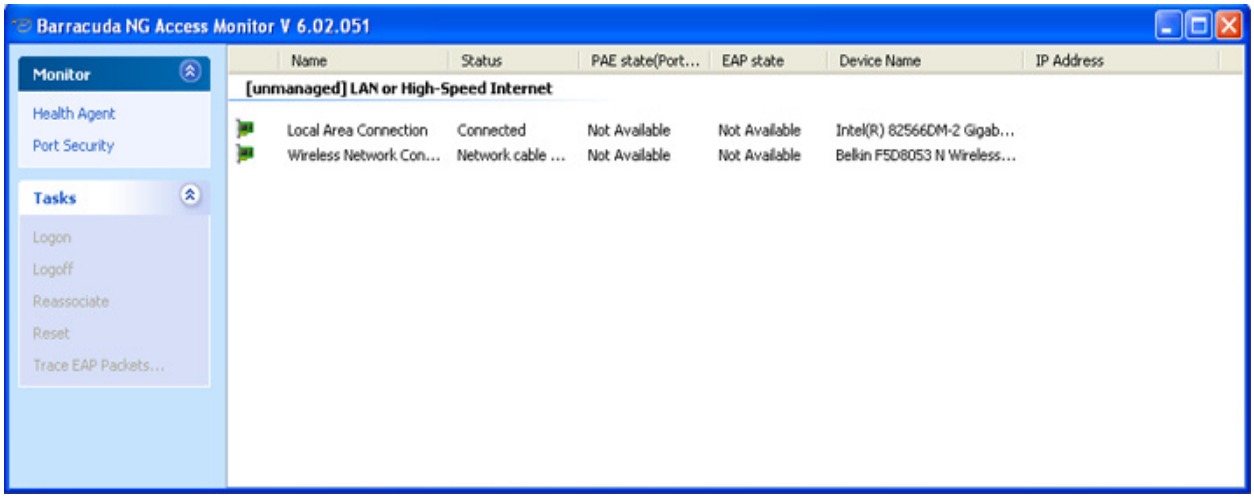
11.2.6 802.1X Authentication - Port Security

11.2.7 Network Interfaces

As seen in figure 11–7, the ***Port Security*** view lists all network interfaces available for 802.1X authentication in two groups:

- ***Managed***
- ***Unmanaged***

Fig. 11–7 *Port Security*



Managed network interfaces have been activated for the use of 802.1X authentication. The Barracuda NG Access Monitor provides several actions for all managed network interfaces when a wpa_supplicant is running for the network interface.

Table 11–3 *Barracuda NG Access Monitor actions for managed network interfaces*

Task	Description
Logon	Starts the 802.1X authentication scheme, by requesting network access through the switch, which enables the line protocol if successful, allowing all network traffic.
Logoff	Tells the switch, the client computer does not need network access any more. The switch will disable the line protocol and block all network traffic except for EAP, CDP and STP protocols.
Reassociate	Restart the authentication process if already authenticated.
Reset	This will reset the session password used for authentication against the RADIUS server. Hence the authentication process will start from beginning and client computer will receive a new session password.
Trace EAP Packets…	Opens the EAP Packet tracer with packet data for the selected network interface.

Unmanaged network interfaces have not been enabled yet to use the 802.1X authentication scheme. It is not possible to perform any actions on unmanaged interfaces through the Barracuda NG Access Monitor.

If available, the list shows the following information:

Table 11–4 *Barracuda NG Access Monitor information for unmanaged network interfaces*

Column	Description
Name	Friendly name of the network device

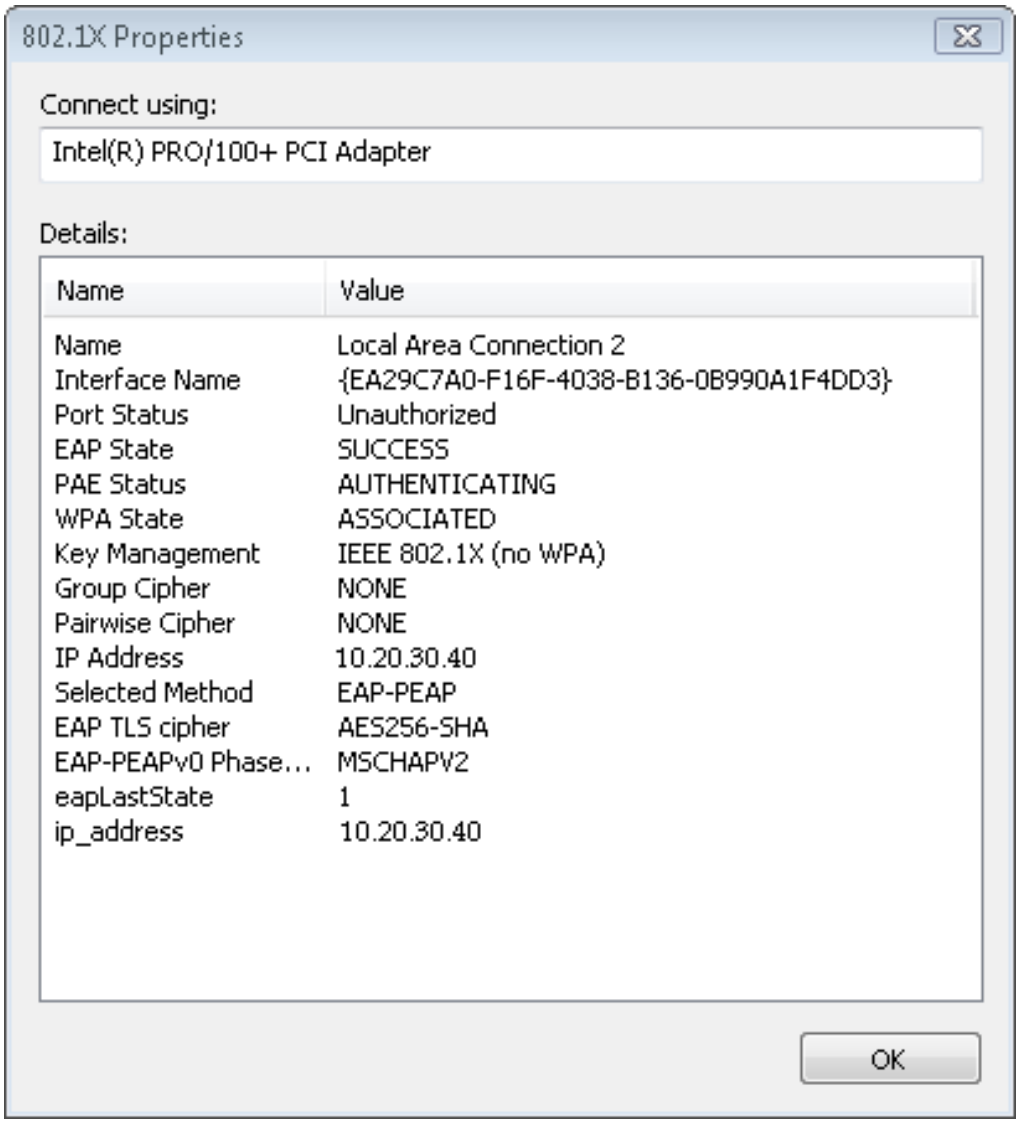
Table 11–4 *Barracuda NG Access Monitor information for unmanaged network interfaces*

Column	Description
Status	Shows the device status of the network interface, these include: • ***Network cable unplugged*** • ***Not connected*** • ***Disconnected*** • ***Connecting*** • ***Connected***
PAE state	Port Access Entity status
EAP state	Extensible Authentication Protocol status
Device Name	The name of the device made up by the manufacturer.
IP Address	IP Address the network interface is using.

11.2.8 Advanced Status Information

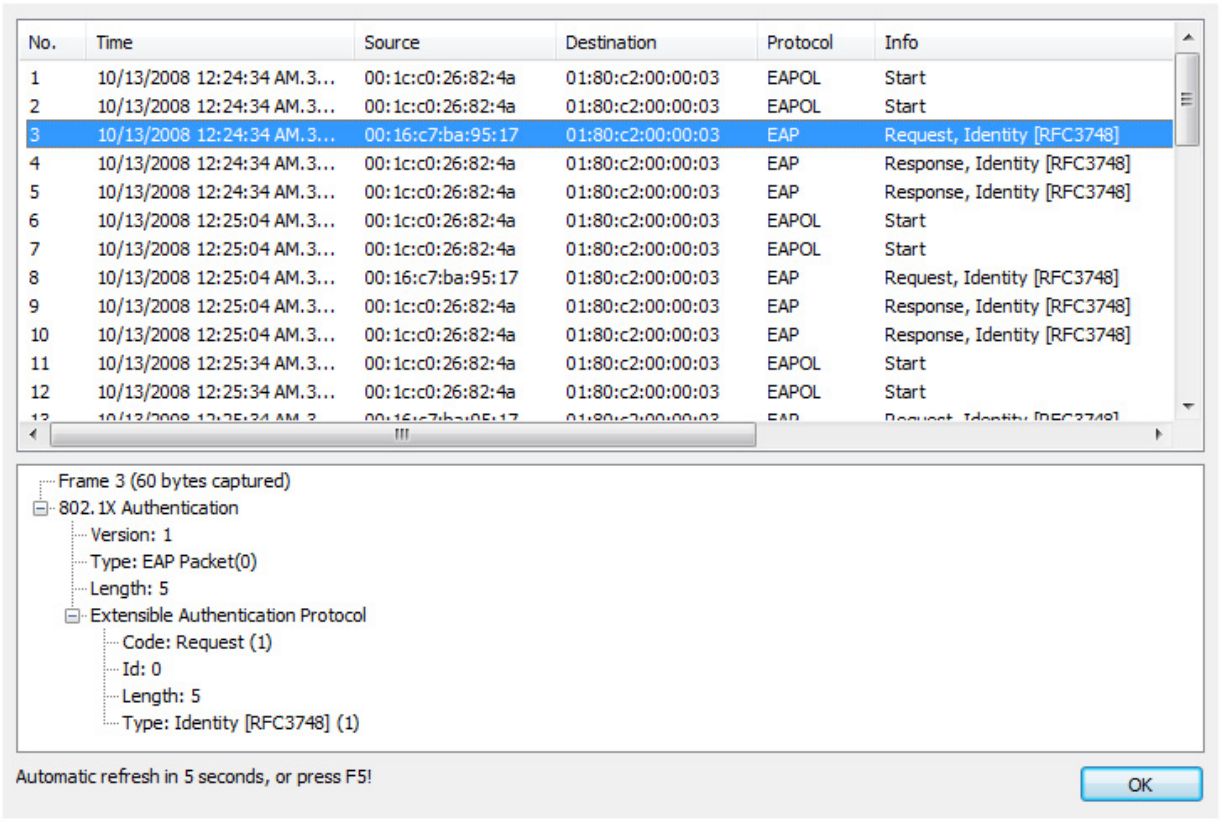
For more detailed information about a network interface, double-click it to open the ***802.1X Properties*** dialog, or right-click the desired network interface and choose ***Details...*** from the context menu.

Fig. 11–8 *Advanced network interface information*



11.2.9 EAP Tracer

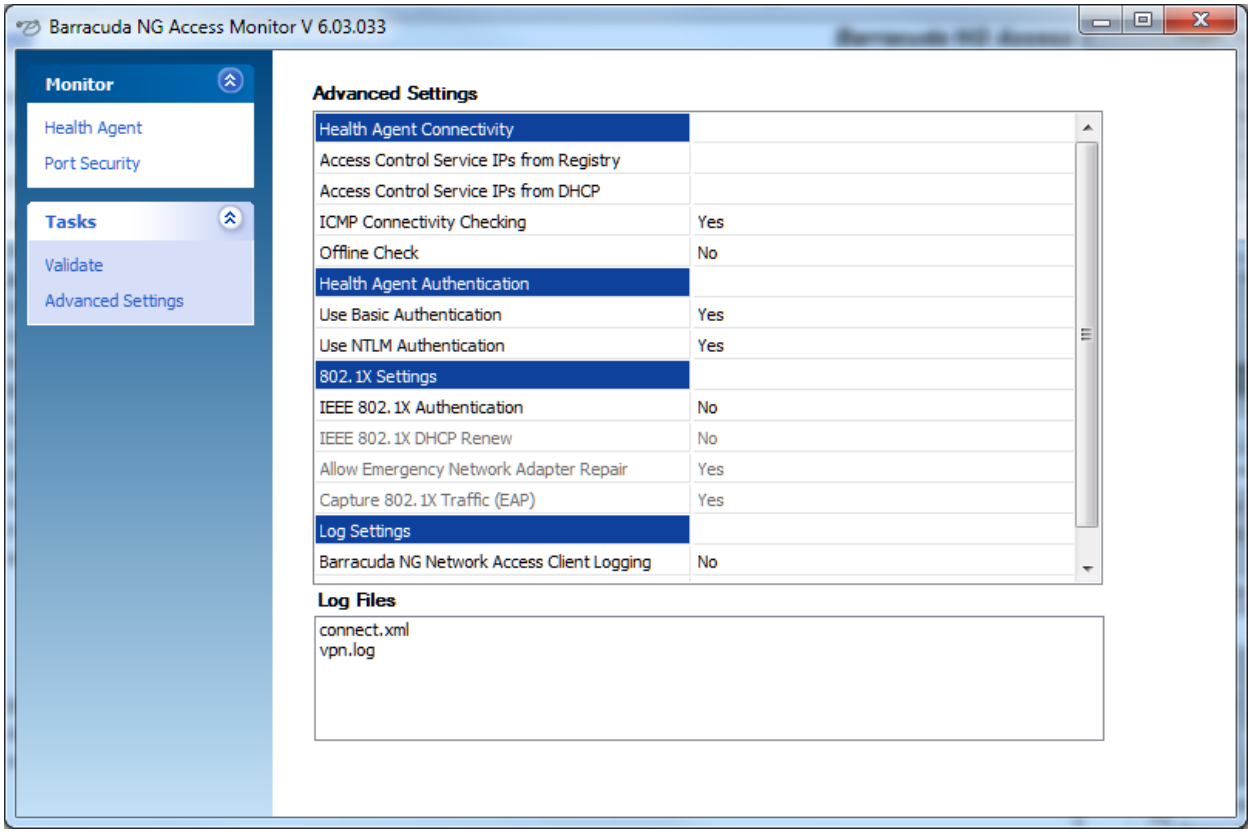
Fig. 11–9 *EAP Tracer*



The EAP Tracer allows you to view EAP and EAPOL packets captured by the Barracuda NG Access Monitor for every network interface which has the option Trace EAP Packets enabled (see 11.3.13 Capture 802.1X Traffic (EAP), page 164).

11.3 Configuration

Fig. 11–10 *Barracuda NG Access Monitor Advanced Settings*



List 11–1 *Configuration – Advanced Settings*

Parameter	Description
Access Control Server IPs from Registry	See 11.3.2 Access Control Server IPs from Registry, page 160
Access Control Server IPs from DHCP	See 11.3.3 Access Control Server IPs from DHCP, page 160
ICMP Connectivity Checking	See 11.3.4 ICMP Connectivity Checking, page 161
Offline Checkl	See 11.3.5 Offline Check, page 161
Use Basic Authentication	See 11.3.7 Use Basic Authentication, page 162
Use NTML Authentication	See 11.3.8 Use NTLM Authentication, page 162
IEEE 802.1X Authentication	See 11.3.10 IEEE 802.1X Authentication, page 163
IEEE 802.1X DHCP Renew	See 11.3.11 IEEE 802.1X DHCP Renew, page 163
Allow Emergency Network Adapter Repair	See 11.3.12 Allow Emergency Network Adapter Repair, page 163
Capture 802.1X Traffic (EAP)	See 11.3.13 Capture 802.1X Traffic (EAP), page 164
Barracuda NG Network Access Client Logging	See 11.3.16 Barracuda NG Network Access Client Logging, page 165
Barracuda NG Health Agent Logging	See 11.3.15 Barracuda NG Health Agent Logging, page 165

11.3.1 Health Agent Connectivity

This section holds all configuration section regarding the connectivity of the Barracuda NG Access Monitor.

11.3.2 Access Control Server IPs from Registry

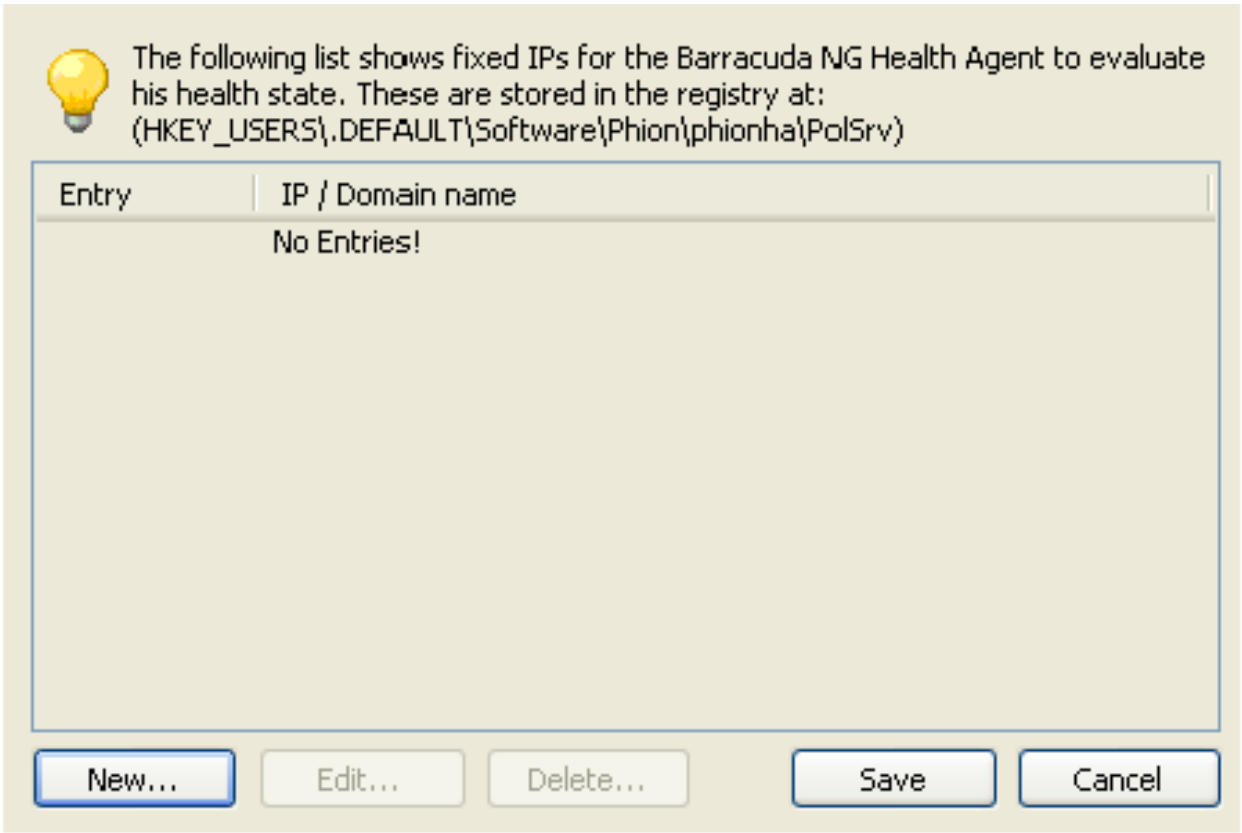
As shown in figure 11–11, the dialog allows creating, editing and deleting of Access Control Server IP addresses, which are stored in the registry. It is possible to configure as many Access Control Server IP addresses as required to ensure to ensure continuous connectivity.

As shown in figure 11–11, these IPs can be configured locally using the dialog, and then they are stored in the registry. These can be found as follows:

Table 11–5 *Registry entry for Access Control Server IPs*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\PolSrv`
Key	N (enumeration)
Value	IP or Hostname of a Access Control Server

Fig. 11–11 *Edit Access Control Server IPs in registry.*

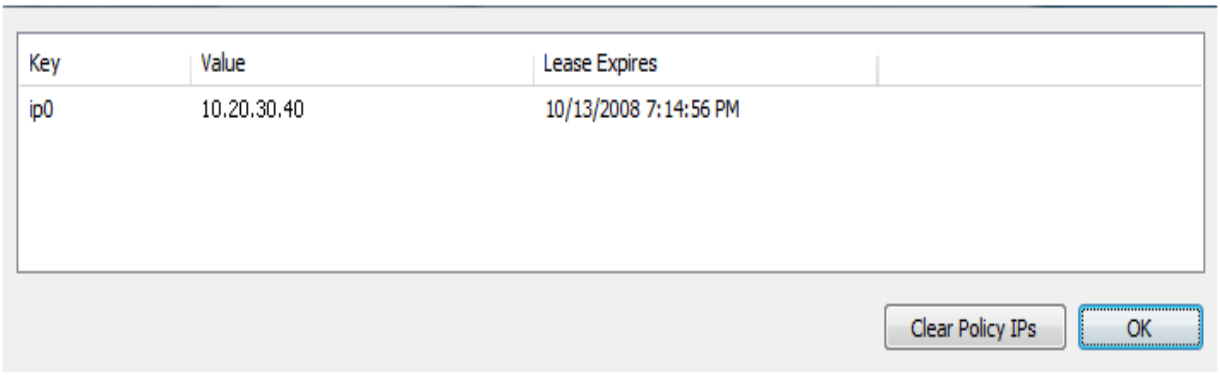


11.3.3 Access Control Server IPs from DHCP

When the Barracuda Networks DHCP server is configured to distribute the Access Control Server IPs using DHCP, these are listed in an advanced dialog, see figure 11–12. To open the dialog click the

Edit... button. If required, clear the Access Control Server IP addresses, which are received through DHCP, with the button ***Clear Policy IPs***.

Fig. 11–12 *Access Control Server IP addresses, received by DHCP.*



11.3.4 ICMP Connectivity Checking

As an advanced feature, the Barracuda NG Access Monitor is able to determine the connectivity to the Access Control Server using ICMP packets. If this option is enabled the Barracuda NG Access Monitor will send an ICMP packet to the Access Control Server, before connecting and starting health evaluation. If the ICMP packet sent, returns successfully the Barracuda NG Access Monitor will connect to the Access Control Server and start health evaluation. When this option is disabled, the Barracuda NG Access Monitor will start immediately connecting to the Access Control Server, instead of checking for connectivity first.

It is highly recommended to enable this feature when connecting to the Access Control Server through a VPN connection; otherwise connectivity may not be as satisfying as expected.

Note

When ICMP Connectivity checking is enabled, the NG Firewall must be configured to pass through ICMP packets, otherwise the Barracuda NG Access Monitor will not connect to the Access Control Server.

To edit this option manually, modify the following registry key:

Table 11–6 *Registry entry for ICMP connectivity*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\settings`
Key	ICMPProbing
Value	(Default=1) 0 - disabled 1 - enabled

11.3.5 Offline Check

Allows to disable the Health Agent if no network connection is active. This prevents the local firewall from unwantedly entering quarantine mode. The default and recommended value is ***Yes***.

To edit this option manually, modify the following registry key:

Table 11–7 *Registry entry for ICMP connectivity*

Item	Description
Path	`.DEFAULT\Software\Phion\phionha\settings\`
Key	UseConnectionState
Value	(Default=1) 0 - disabled 1 - enabled

11.3.6 Health Agent Authentication

11.3.7 Use Basic Authentication

This option specifies if basic user-password or certificate authentication should be used, in case the NTLM authentication fails.

To edit this option manually, modify the following registry key:

Table 11–8 *Registry entry for basic authentication*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\settings`
Key	UseBasicAuthFallback
Value	(Default=1) 0 - disabled 1 - enabled

11.3.8 Use NTLM Authentication

By enabling this option, the Barracuda NG Access Monitor will use windows user credentials provided by NTLM for authentication.

To edit this option manually, modify the following registry key:

Table 11–9 *Registry entry for NTML authentication*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\settings`
Key	UseNTLM
Value	(Default=1) 0 - disabled 1 - enabled

11.3.9 802.1X Settings

11.3.10 IEEE 802.1X Authentication

This option enables or disables the use of 802.1X authentication. When enabled, the Client will automatically start a wpa_supplicant for all network interfaces configured to use 802.1X authentication.

To edit this option manually, modify the following registry key:

Table 11–10 *Registry entry for 802.1X authentication*

Item	Description
Path	HKEY_USERS\.Default\Software\phion\phionvpn\settings
Key	8021XMonitor
Value	(Default=1) 0 - disabled 1 - enabled

11.3.11 IEEE 802.1X DHCP Renew

When 802.1X DHCP Renew is enabled, a DHCP request packet will be sent to obtain a new IP address, whenever a VLAN is assigned to the client computer by the switch.

To edit this option manually, modify the following registry key:

Table 11–11 *Registry entry for 802.1X DHCP Renew*

Item	Description
Path	HKEY_USERS\.Default\Software\phion\phionvpn\settings
Key	8021XEnableDHCPRenew
Value	(Default=1) 0 - disabled 1 - enabled

11.3.12 Allow Emergency Network Adapter Repair

This option enables the button for ***Emergency Network Adapter Repair*** in the Barracuda NG Access Monitor - ***Health Agent*** view. By clicking the button all network interfaces enabled to use 802.1X are being reset and will receive a new IP if the network interface is configured to use DHCP.

Note

Option IEEE 802.1X DHCP Renew must be enabled in order to allow emergency network adapter repair.

To edit this option manually, modify the following registry key:

Table 11–12 *Registry entry for emergency network adapter repair*

Item	Description
Path	HKEY_USERS\.Default\Software\phion\phionvpn\settings

Table 11–12 *Registry entry for emergency network adapter repair*

Item	Description
Key	AllowEmergencyRepair
Value	(Default=1) 0 - disabled 1 - enabled

11.3.13 Capture 802.1X Traffic (EAP)

If enabled, the Barracuda NG Access Monitor will capture all EAP (Extensible Authentication Protocol) and EAPOL (Extensible Authentication Protocol) packets and save them in the log directory located in the Barracuda NG Network Access Client installation directory. These files can be viewed using the EAP Tracer.

To edit this option manually, modify the following registry key:

Table 11–13 *Registry entry to capture 802.1X Traffic (EAP)*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	8021xTraceEAP
Value	(Default=1) 0 - disabled 1 - enabled

11.3.14 Log Settings

For proper analysis verbose output is essential, thus it is possible to enable logging for both the Health Agent service and the Barracuda NG Access Monitor service to receive detailed information, see 11.4 Log Files, page 165 for more information.

11.3.15 Barracuda NG Health Agent Logging

To edit this option manually, modify the following registry key:

Table 11–14 *Registry entry to log clients*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	Logging
Value	(Default=1) 0 - disabled 1 - enabled

11.3.16 Barracuda NG Network Access Client Logging

To edit this option manually, modify the following registry key:

Table 11–15 *Registry entry to log Barracuda NG Access Monitor*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\settings`
Key	Logging
Value	(Default=1) 0 - disabled 1 - enabled

11.4 Log Files

Information for analysis, serialized by the NG Network Access Client, is stored on the local hard drive if verbosity is enabled. These files can be found in the **log** directory located in the Barracuda NG Network Access Client installation directory. These files can be opened either using the Barracuda NG Access Monitor, by double clicking the desired log file in the "Advanced Settings" section or with the desired text editor.

Following log files are available, depending on the level of verbosity configured:

Table 11–16 *Log Files*

File	Description
phions.log	Log information by the Client Service, depending on option (see 11.3.15, Page 165)
phionha.log	Log information by the Barracuda NG Access Monitor, depending on option (see 11.3.16 Barracuda NG Network Access Client Logging, page 165)
wpa_supplicant_{UUID}.log	Log information by the wpa_supplicant for each network interface, depending on option (11.3.15 Barracuda NG Health Agent Logging, page 165)

Table 11–16 *Log Files*

File	Description
client.xml	Xml file containing the information sent to the Access Control Server containing information about the client computer when perform user based health evaluation.
connect.xml	Information about connectivity and connection errors.
download.xml	Contains data from the last download such as rule set, message of the day, …
downloadLocal.xml	Contains data received when a local computer based health evaluation succeeded.
downloadUser.xml	Contains data received when a user based health evaluation succeeded.
health.xml	Last health evaluation result returned by the Access Control Server.
healthLocal.xml	Last health evaluation result for local computer based health evaluation.
healthUser.xml	Last health evaluation result for user based health evaluation.

Chapter 12
Pre-Connector and Remote VPN

12.1 General

Pre-connectors and Remote VPN are tools that are meant to simplify/automate logon procedure. Optionally, combined with a prior dial-up connection, they may also be used to log on to a domain remotely.

12.2 VPN Connector

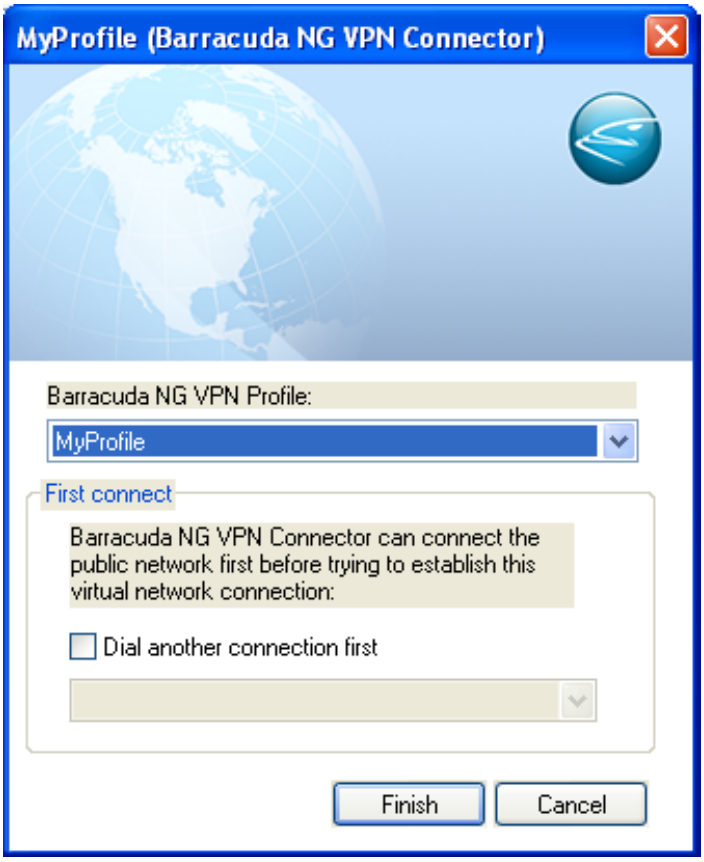
Create a connector to achieve following:

- ***Enable a user to gain quick access to a preconfigured profile or multiple profiles. Place shortcuts to the connectors on the client's desktop.***
- ***Connect to a VPN server directly from the Microsoft Windows login screen without prior login to the Windows system.***
- ***Connect to a VPN server with prior dial-up connection to a remote domain. Dial-up connection and remote domain login may also be called directly from the Windows login screen.***

12.2.1 Creating a Connector

Prior to creating a Barracuda NG VPN connector, the connection profile must be configured (10.6.8 Advanced Settings Tab, page 143). The connector may then be created using one of two possible methods.

Fig. 12–1 *Creating a Connector*



- ***Start the VPN client and enter the configuration mode for the required profile (Preferences > Select profile to change > Options > Modify Profile… > Advanced Settings tab > Pre Domain Logon > Create Connector…; see Advanced Settings Tab, page 143).***
- ***Browse to* Start > Control Panel > Network Connections*. A default Barracuda NG VPN Connector is available in the* Virtual Private Network *section. Modify or copy and thereafter rename the default profile.***

The checkbox ***Dial Another Connection First*** enables activation of a dial-up connection prior to tunnel establishment. Dialling is started automatically after start of the VPN connector.

Click ***Finish*** to create the connector or to save the settings that have been made respectively.

To create a shortcut for quick access, select a connector and drag it to the desktop.

12.2.2 Connecting And Disconnecting using the Barracuda NG VPN Client

To connect using the Barracuda NG VPN Client, double-click the corresponding shortcut (if available) or select the connector in ***Start*** > ***Control Panel*** > ***Network Connections***. Enter the necessary information and click ***OK*** to start the VPN tunnel.

To disconnect, double-click the corresponding shortcut (if available) or select the connector in ***Start*** > ***Control Panel*** > ***Network Connections*** and click ***Disconnect***.

12.2.3 Remote Domain Logon (Pre-Logon)

As soon as a Barracuda NG VPN connector has been created, Remote Domain Logon from the Windows login screen becomes possible with prior dial-up connection.

Select the checkbox ***Log on using dial-up connection*** when logging on to your PC and select the desired VPN connector connection profile from the list. Dial-up connection and tunnel are going to be established successively during logon process to your PC, enabling access to an otherwise inaccessible domain.

12.3 Remote VPN (rvpn)

Remote VPN allows connecting/disconnecting automatically via script. `rvpn.exe` is downloadable from Barracuda Networks.

1.) Create a VPN Profile

First, you must configure the required profile as described in the previous chapter (VPN Component Configuration, page 124).

2.) Allocate the Profile in the Windows Registry

Open the registry (`regedit`) and change into the folder ***HKEY_USERS*** > ***.DEFAULT*** > ***Software*** > ***Barracuda Networks*** > ***Barracuda NG VPN*** > ***Profile***.

3.) This directory contains an explicit directory for each VPN profile.

Warning

The sequence in the registry (1, 2, 3,…) does NOT match with the sequence in the NG VPN Client User Interface.

Have a look at the Description entry in the registry in order to find out which profile number matches the required VPN profile.

4.) Create an rvpn Profile

An rvpn profile contains several parameters that determine the actions to be taken when a profile is executed:

List 12–1 *Parameters contained in an rvpn profile*

Parameter	Description
`-c [X]`	Connect [number of retries - default 1]

List 12–1 *Parameters contained in an rvpn profile*

Parameter	Description
`-a [X, *]`	Local password [Certificate Password] (if any)
`-aa`	Pop-up for local password
`-cs [X]`	Client shutdown password protection. Prompts for the password definied in [X] whenever a user tries to shut down the VPN client. Leaving the password value blank deactivates this feature.
`-d`	Disconnect
`-f "X+X"`	Process to kill [0, KILL]
`-g [X]`	IP address of VPN server; **Note:** overrules the server IP set in the profile
`-h`	Hide console
`-n`	Profile name
`-o`	Proxy password
`-p`	VPN server password
`-pp`	Pop-up for VPN client password
`-preconnector [X]`	If VPN connection is terminated this preconnection is also terminated (for example for terminating modem connection)
`-r [X]`	Profile (registry ID)
`-u [X]`	User
`-v [X]`	Verbose
`-x [X]`	Command (showvpn, shofw)

- ***Examples:***

```
rvpn.exe -c -r 3 -a vpntest -p a12b34c56
```

This profile connects (`-c`) with client profile "3" (`-r 3`) using certificate password "vpntest" (`-a vpntest`) and server password "a12b34c56" (`-p a12b34c56`).

```
rvpn.exe -c 10 -r 3 -a vpntest -p a12b34c56
```

The same example with 10 retries for connecting (`-c 10`):

```
rvpn.exe -c -r 3 -aa -p a12b34c56
```

This profile starts a query for a local certificate password (`-aa`) via pop-up. Thus, the script does not run completely automatic. It requires manual input.

```
rvpn.exe -c -r 3 -a * -p a12b34c56
```

This profile starts a query for a certificate password (`-aa`) via DOS window. Thus, the script does not run completely automatic. It requires manual input.

12.4 Connection Procedure

After successful authentication against the VPN server, the client requests the configuration from it. As soon as the configuration is received, the VPN Service transmits this configuration to the Barracuda Networks Secure Personal Access Client (SPAC). This enables the SPAC to answer DHCP requests.

The following steps are carried out when a connection is to be established:

1.) Client opens a socket on the server, starts authentication and requests configuration

2.) Client receives configuration (IP, subnet mask, WINS, DNS,…)

3.) Client sends received information to the SPAC

4.) Client triggers ipconfig/renew for the Barracuda NG VPN Virtual Adapter

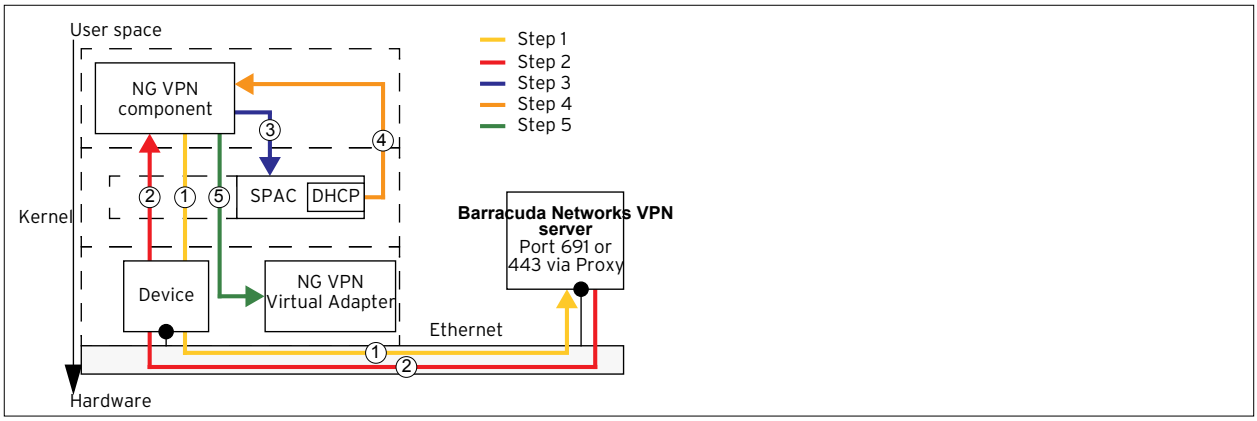
5.) SPAC answers DHCP requests for the Adapter with the configuration data

6.) Operating system reconfigures the Virtual Adapter

7.) VPN Service introduces additional routes

8.) The corresponding rule set for the Barracuda NG Personal Firewall is implemented.

Fig. 12–2 *Connection procedure*



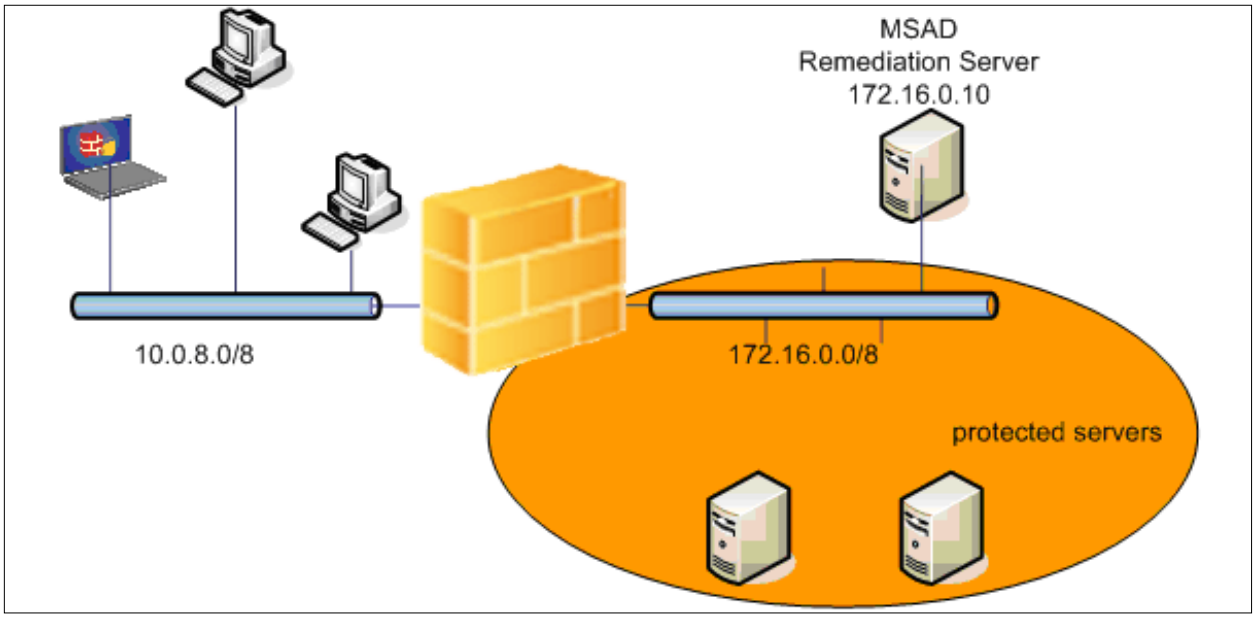
Chapter 13
Example Configuration

Introducing an up-and-running Barracuda NG Network Access Client environment involves several components, like global objects, trustzone settings, Access Control Service and gateway firewall configuration.

This section presents an overview how simple an environment can be set up. For further details of individual parameters please refer to the appropriate sections.

Beginning to use Barracuda NG Network Access Client does not necessarily require complex policy rule sets. Although rule sets will become more elaborated due to required exceptions, the sample includes only one policy within the rule set **Local Machine**.

Fig. 13–1 *Example configuration – environment*



The client LAN has the IP-range 10.0.8.0/24, the protected servers are located in the network 172.16.0.0/24. Additionally to the protected servers, one server acts as Microsoft Domain Controller and as remediation server for updating the antivirus patterns. This server has the IP address 172.16.0.10 - you need to grant access to this computer even for unknown or unhealthy clients.

The other servers located within the server segment should be protected - for example access to these servers should only be available for clients conforming to the corporate health policy.

The health policy requires to have a client installed and the personal firewall to be enabled. In addition, the company uses Trend Micro antivirus products, so it is required to have the AV engine enabled and to receive regular anti-virus ipattern updates.

13.1 Introduce Access Control Objects

As a first step it is recommended to prepare the Access Control Objects. These objects should be ready for referencing during trustzone configuration.

At the beginning, setting up an Barracuda NG Network Access Client infrastructure usually starts with two different Welcome messages, two different Personal Firewall rule sets, and one Picture.

To give users customized details about their health state we recommend to define different Welcome messages for unrestricted access ("healthy") and quarantine ("unhealthy"). In case of quarantine contact details of the company's IT support will be useful for the end user.

Like welcome messages, customized pictures are not really necessary for a Barracuda NG Network Access Client infrastructure. Nevertheless, companies usually want to display their own logo instead of the Barracuda Networks logo.

The most important part which is also required for proper operation is to set up Personal Firewall Rules.

13.2 Personal Firewall Rule Set

It is difficult to give guidelines for personal firewall rule sets. The required applications may strongly differ between companies.

Nevertheless, remember for all your Barracuda NG Personal Firewall rule sets:

All your clients, regardless of their health state, require network access. They need to contact the Access Control Service (TCP 44000, the rule is included in the default rule set) and the Microsoft Domain Controller. Otherwise no user login will be possible. Additionally, depending on the antivirus or antispyware product, access to HTTP servers may be necessary. Backup software, remote support and automatic software distribution often trigger connections from server to client, so it may be necessary to modify the incoming rule set of your personal firewall to allow incoming connections.

For the setup used in this example only small modifications to the default rule set are required. First create the quarantine rule set:

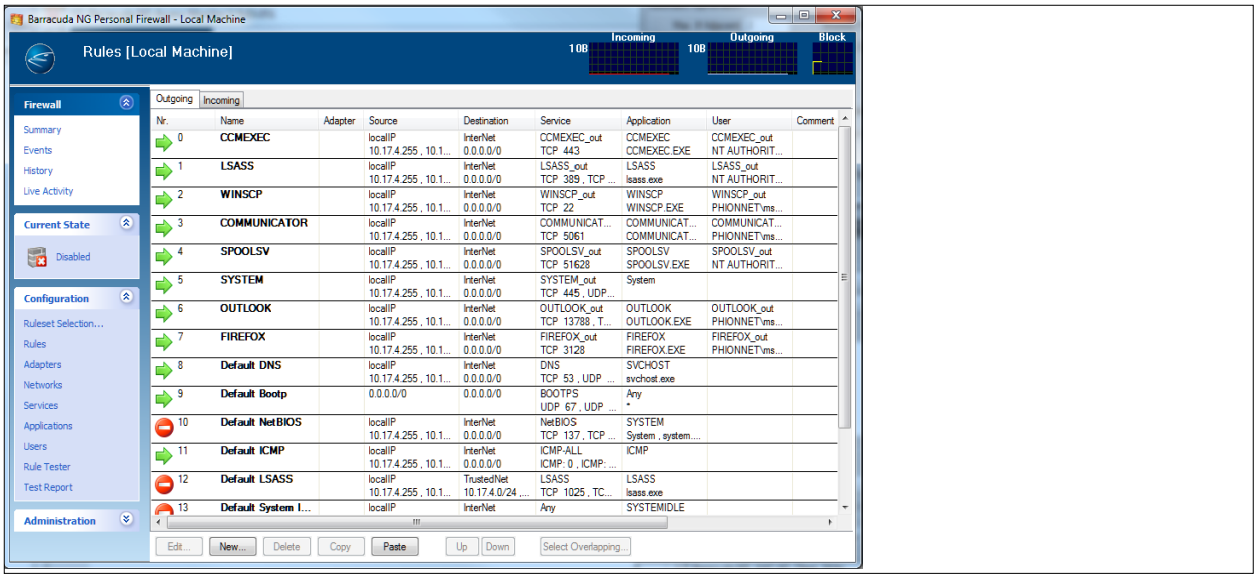
- ***In the configuration directory** Access Control Objects **>** Personal Firewall Rules **choose** New Access Control Firewall Rule Set… **in the context menu.***
- ***The object name of the rule set is* restrictedAccess.**
- ***Open the rule set* restrictedAccess.**

For the restrictedAccess rule set, the following new rules are added:

- ***Explicitly block Skype application.***
- ***Allow connections to the remediation-servers (172.16.0.10).***

- ***Allow HTTP/HTTPS connections to the internet. Some antivirus products use HTTP/HTTPS to download up-to-date engines and patterns.***

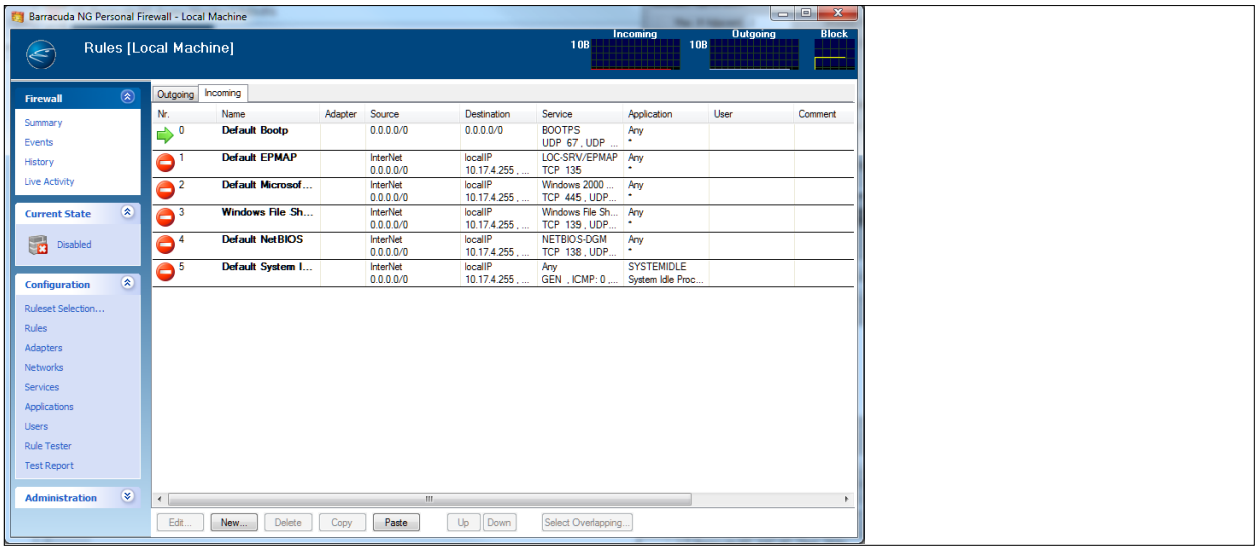
Fig. 13–2 *Example configuration – Personal Firewall rule set – Access Control Service - Rules – Outgoing tab example view*



Next create and edit the unrestricted rule set:

- ***For the unrestricted rule set, the Outgoing rules allow connections to the whole internal network. Add a pass rule using "LocalIPs" as source and "10.0.0.0/8" plus "172.16.0.0/24" as destination.***
- ***Additional remote desktop connections are allowed in the "Incoming" rule set.***

Fig. 13–3 *Example configuration – Personal Firewall rule set – Incoming tab example view*



13.3 Introduce an Access Control Service Trustzone

As mentioned above, the hierarchical structure of a Barracuda NG Control Center allows introduction of Access Control Service Trustzones at different levels (Global, Range, and Cluster). Thus, a decision about the proper place for a company's trustzone is required.

Administrators of stand-alone Barracuda NG Firewalls can avoid making this decision - you simply configure your trustzone within the ***Access Control Service > Trustzone*** node.

As a guideline for a simple setup using a CC, we recommend to use global trustzones or alternatively switch to range trustzones.

Note

For range or cluster based Access Control Services note that they can only reference trustzones within the same administrative scope (not from another range/cluster).

13.4 Configure an Access Control Service Trustzone

The main window of a Access Control Service Trustzone is split up into a navigation bar on the left and the three policy rule sets on the right.

To guarantee that our policy trustzone has a public/private key pair to properly authenticate clients to all participating Access Control Services, we initially need to create a Health Passport Signing Key (Settings > Identity > Health Passport Signing Key). The Health Passport is used for authenticating against other Access Control Service instances (for example Remediation Service and Border Patrol). Therefore, generation of a Heath Passport Signing key is required.

Click ***New Key…*** to create a new Health Passport Signing key. In this setup with local created public/private keys use the previously created key and export the public part into the clipboard. This public key is imported again as Health Passport Verification Key.

To keep our setup as simple as possible we will start with local machine policies. We recommend to extend your setup by applying user specific or VPN policies as a next step. At the beginning even setting up a restricted local machine rule set and configuring the gateway firewall rule set requires quite some time.

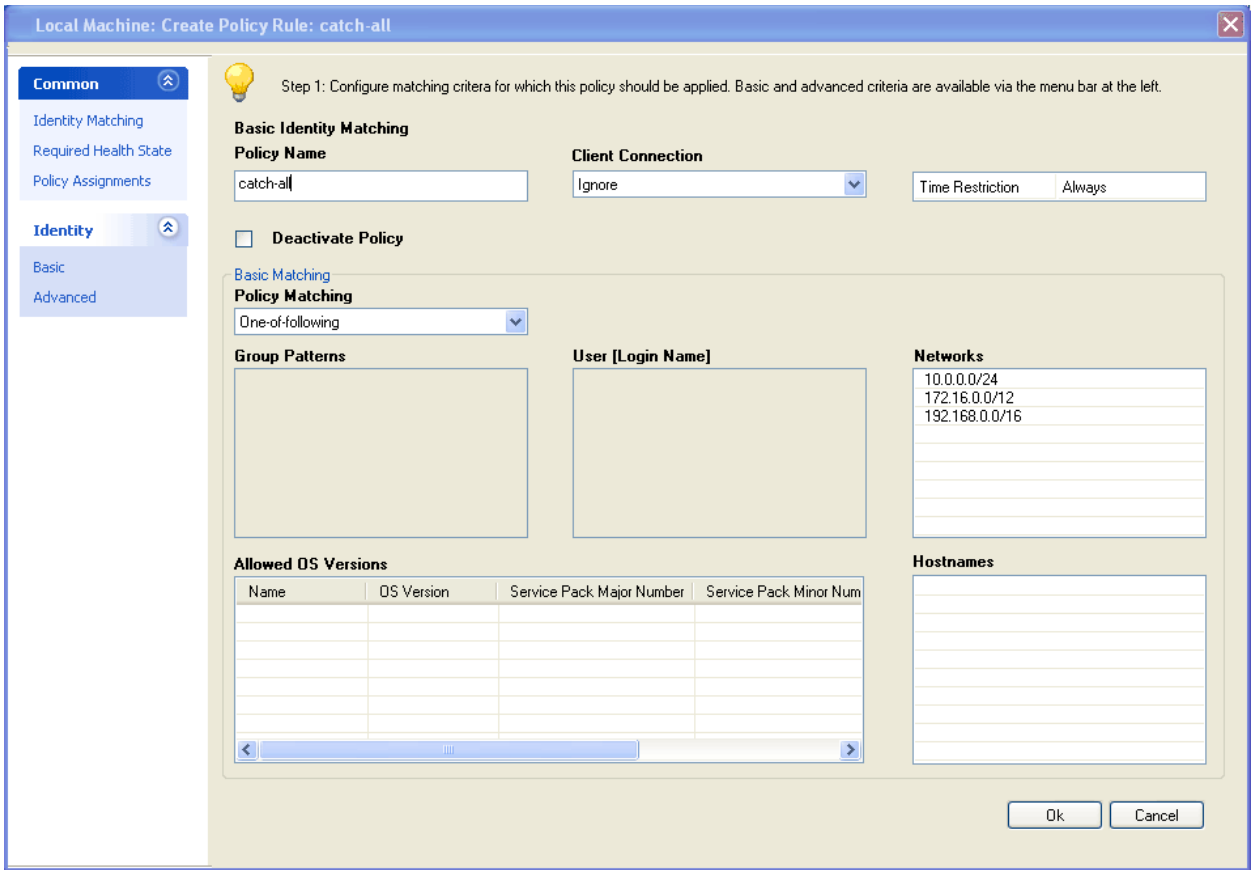
So as a next step create at least one rule within the "Local Machine" policy rule set. The first and for the moment the only available rule is our catch-all rule which usually should be at the end of your policy rule set. Click ***New…*** at the bottom of the policy rule set or via the context-menu to create a policy rule. When using more than one rule, remember that policy rule sets are processed from top to bottom.

The Policy Rule dialog is split up into these views:

- ***Identity Matching***
- ***Required Health State***
- ***Policy Assignments***

For the ***Identity Matching*** and ***Required Health State*** views, ***Basic*** and ***Advanced*** configuration dialogs exist.

Fig. 13–4 *Example configuration – Configure an Access Control Service Trustzone – Local Machine: Create Policy Rule: catch-all*



First start with defining the criteria for **Identity Matching**:

Since the Access Control Service in this sample setup is only reachable using private IP addresses we can restrict the ***Networks*** section to the private address ranges.

Note

The option ***Policy Matching*** (section Basic Matching) is set to One-of-following. Therefore you don't need to specify further matching criteria.

As a next step define the required health conditions. For the catch-all rule you can define the same policies you require for known clients, as security policies usually further restrict unknown clients instead of granting them lower health requirements.

To comply to the above mentioned security requirements set the following parameters:

List 13–1 *Example configuration – Configure a Access Control Service Trustzone – Local Machine: Edit Policy Rule – Parameters*

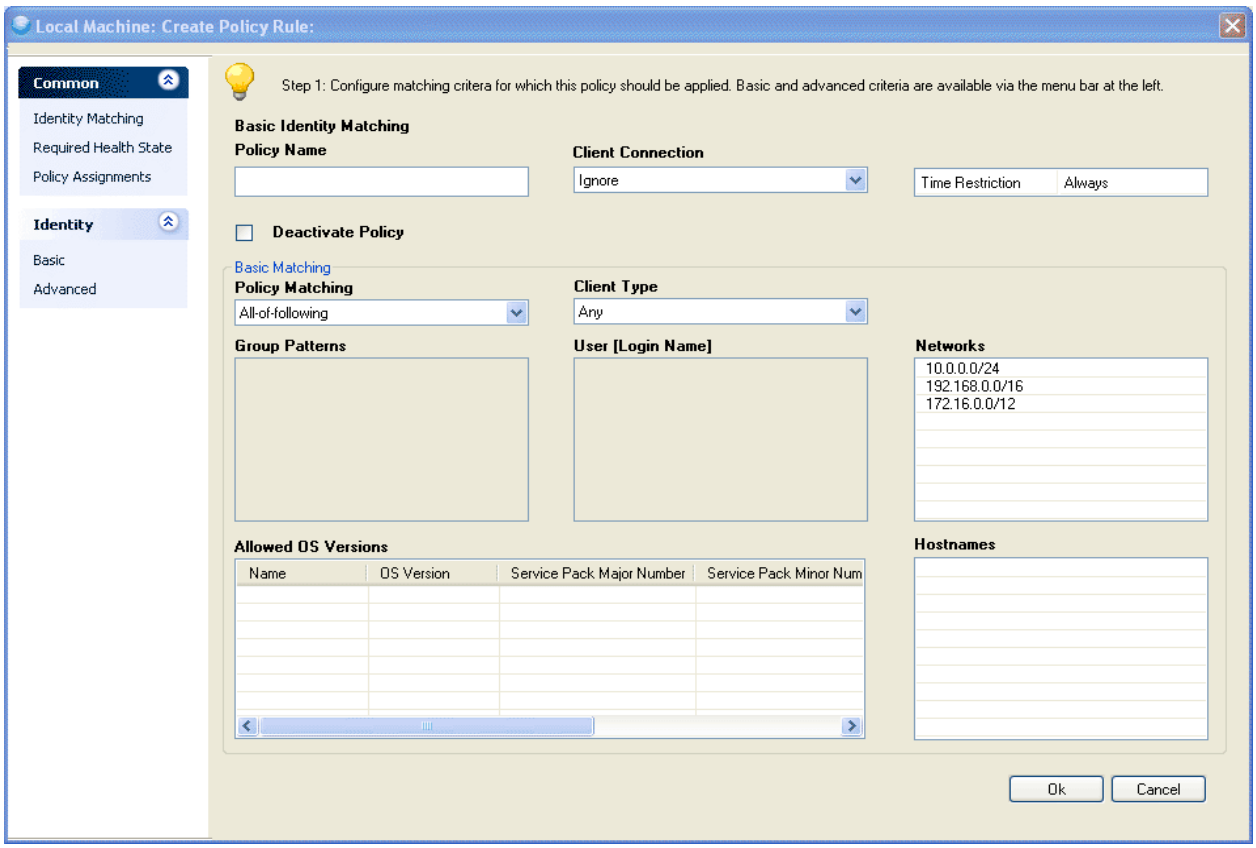
Parameter	Value
NG Personal Firewall On	Required <Auto-remediation>
Antivirus Scanner On	Required <Auto-remediation>
Last AV Scan Not Older Than	Ignore
AV Engine Required	Last-2
AV Pattern Definitions Required	Last-2
AV Engine/Pattern Action	Manual
Allowed Vendors	Trend Micro, Inc
Antispyware	disabled

The value ***Required <Auto-remediation>*** automatically enables the Barracuda NG Personal Firewall and the Antivirus Scanner if they are deactivated.

To set the parameter ***Last AV Scan Not Older Than*** to ***Ignore*** is due to the reason that performing a regular full-scan of the client computer takes quite some time. To enforce users to perform a full-scan during working hours is not always welcome if their computer is slowed down.

For the AV engine and for the AV patterns the settings above accept the current version and also two versions before. Usually companies already have mechanisms to perform regular updates of their AV engines and patterns - in the sample you can thus leave the setting ***AV Engine/Pattern Action*** to ***Manual***.

Fig. 13–5 *Example configuration – Configure a Access Control Service Trustzone – Local Machine: Edit Policy Rule: catch-all*



Note

Checking engine and pattern versions of Antivirus- or Antispyware products requires up-to-date information on server-side.

Instead continue with the view ***Policy Assignments*** and assign the following attributes:

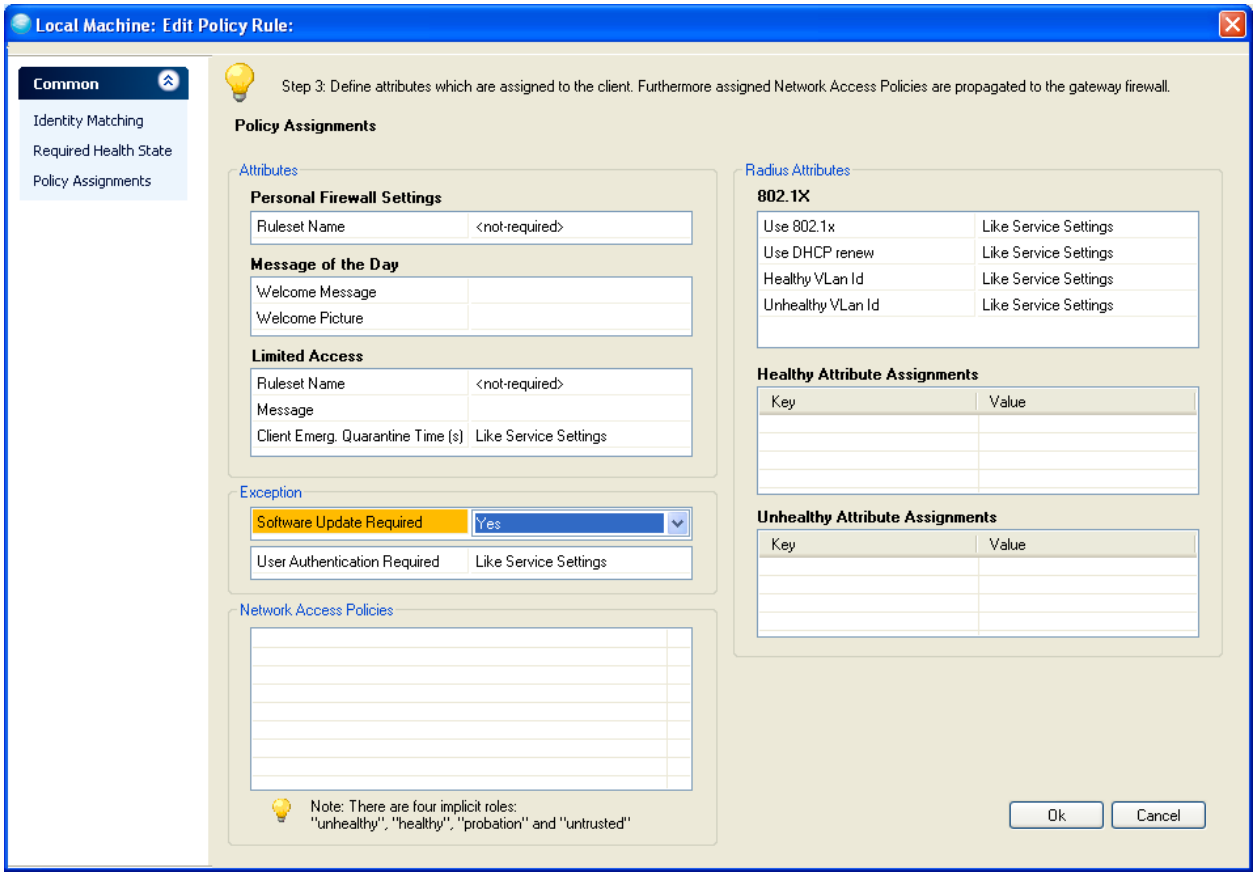
- ***Assign the Firewall Object unrestrictedAccess as Barracuda NG Network Access Client***
- ***Assign the Welcome Message NG Network Accesss Protection Welcome as Message of the Day. Since the local machine context of Microsoft Windows does not allow GUI dialogs before login, the GUI components Message of the day and Welcome picture are displayed as soon as a user has logged in.***
- ***Assign the Welcome Picture Barracuda NG Network Access Client Logo.***
- ***For Limited Access assign the appropriate Rule Set and Message***
- ***For the catch-all rule which matches all clients in the LAN, no automatic client update is required, thus the parameter Software Update Required is set to No.***

Note

Before deploying new client versions to large-scale environments, the client software will usually be tested on a limited number of clients. Thus it is recommended to create a separate policy rule which matches only a limited number of clients. In this policy rule enable automatic software update. After updating a smaller number of clients, one can enable automatic software update for the rest of the company's clients.

In the sample you are not required to manually add "Network Access Policies". Instead you can set up your firewall rules of the gateway firewall using the implicit roles **unhealthy**, **healthy**, **probation** and **untrusted**.

Fig. 13–6 *Example configuration – Configure a Access Control Service Trustzone – Local Machine: Edit Policy Rule – catch-all*



13.5 Configure Forwarding Firewall Rule Set

Enforcement of the security policy is provided by the Barracuda NG Network Access Client software installed on the endpoint itself. Whenever leaving the local collision domain, Barracuda NG Firewalls can provide additional protection. To enforce the health policy, Barracuda NG Firewalls may interpret the access policy attribute assigned to the endpoint within their rule sets. This provides a way to enforce network access control concepts based on date and time, identity and health state and type of network access.

To allow communication to protected servers only for clients conforming to the health policy, modify the gateway firewall rule set as follows:

- ***Open the forwarding firewall rule set and change to section** **User Groups.***
- ***Select** **New… in the context menu to create a new** **User Object.***
- ***After setting a name for the user object add a new User Condition***
  - **Within the *Policy Roles Patterns* section, change the logic operation to *One Pattern must match (OR).***
  - **Add two new Policy Roles Patterns: *healthy* and *probation.***
  - **Close the User condition dialog.**
- ***Create or edit the firewall rule** **Healthy-Access-to-protected-Servers.***
  - **Add a reference to the new user object *healthy-clients* within the *Authenticated user* dialog box.**

Fig. 13–7 *Example configuration – Configure forwarding firewall rule set – Edit/Create User Object > User Condition*

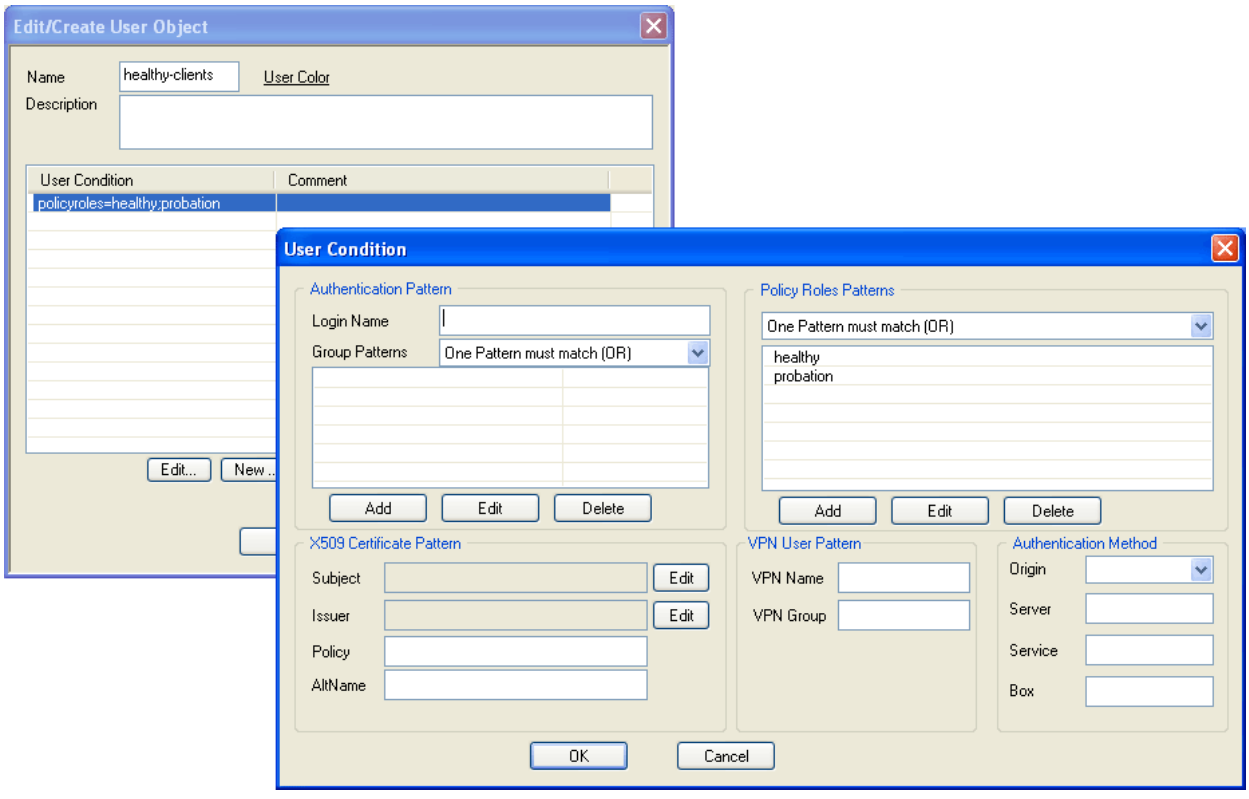


Fig. 13–8 *Example configuration – Configure forwarding firewall rule set – Edit Rule: Healthy-Access-to-protected-Servers[Rule]*

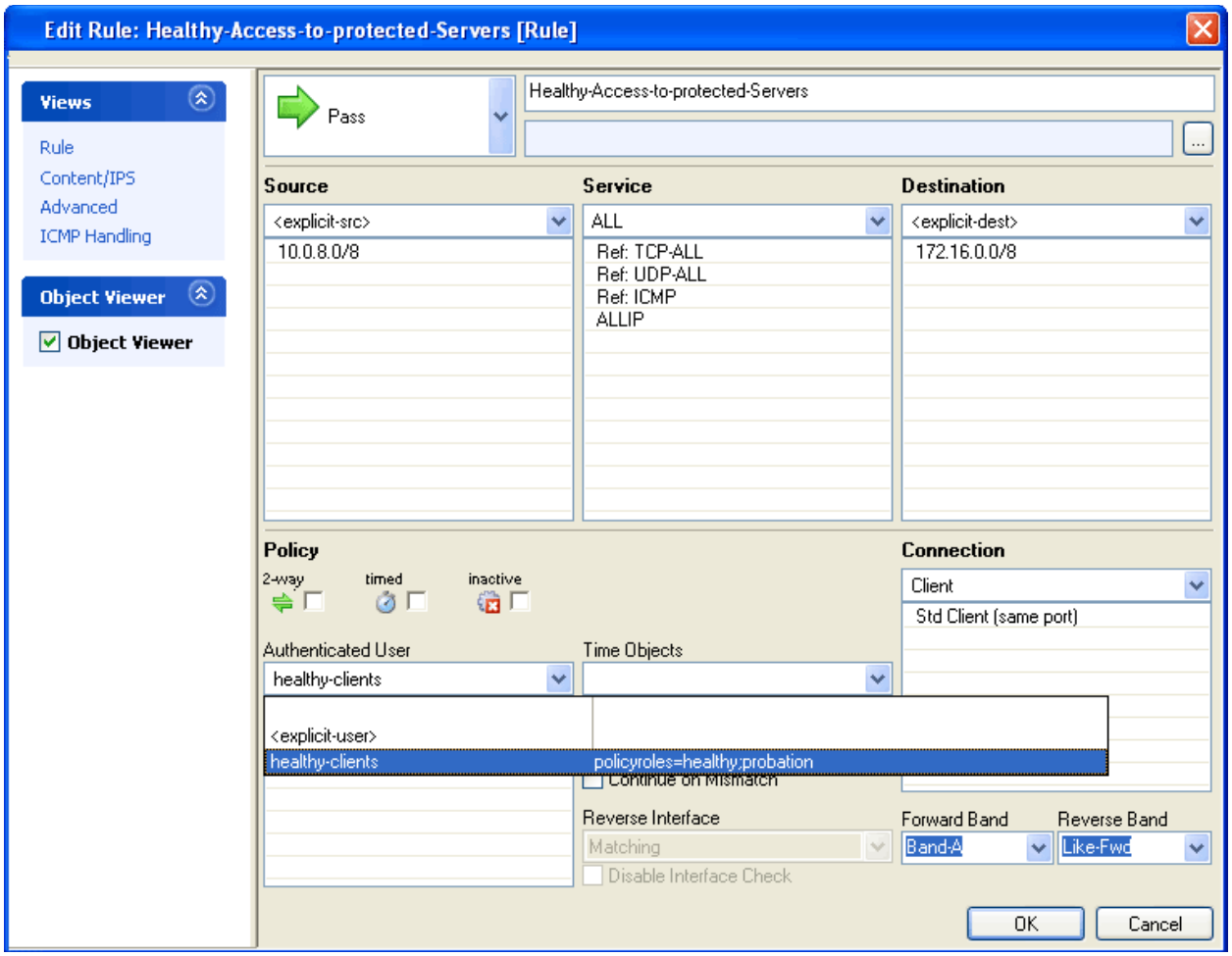
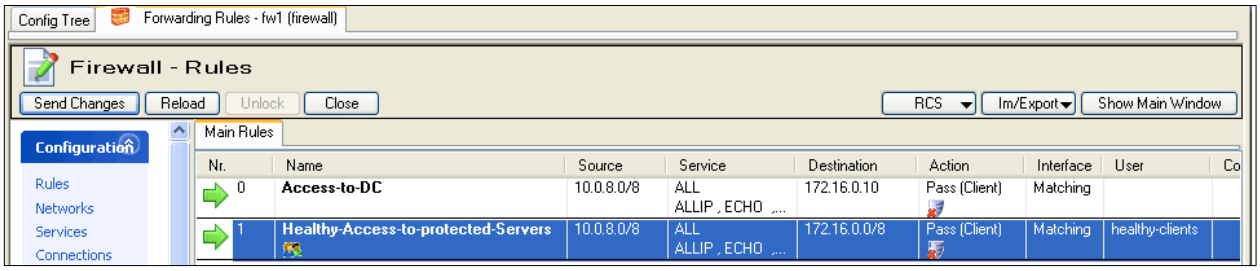


Fig. 13–9 *Example configuration – Configure forwarding firewall rule set – Firewall - Rules*



If the user authentication is assigned to the firewall rule, only clients either fully conforming to the policy ("healthy") or clients being in "probation" state are allowed to access the protected network.

Warning

Barracuda Networks allows access even for clients in "probation" since we do not want to block new connections or even terminate existing connections only because the antivirus patterns are not up-to-date for a few minutes. Remember that the client is in "probation" while it tries to execute the (auto)remediation actions. If the remediation fails, then it will become "unhealthy".

Chapter 14
802.1X – Technical Guideline

14.1 Overview

Barracuda NG Network Access Client features the IEEE 802.1X standard for port-based network access control. The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. Every client connected to a switch port must be authenticated by the authentication server before having access to any services provided by the switch or LAN. Until the client is authenticated, the only traffic allowed through the port the client is connected to, is the Extensible Authentication Protocol over LAN (EAPOL), the Cisco Discovery Protocol (CDP) and the Spanning Tree Protocol (STP).

Other than common implementations of the 802.1X standard, the client computer's health state is the criterion for access control. The health state of a client computer is evaluated by the Barracuda NG Access Control Server, accessible from within the initial assigned guest VLAN after the first authentication using default credentials succeeded. Once the client computer evaluated its health state, it will start the authentication using a unique identifier as username and a session id as password, received by the Access Control Server based on his health evaluation result. The authentication server will assign the client computer the VLAN configured for the result of the client computer's health evaluation result.

When the user logs off or shuts down the operating system, the Client service will notify the wpa-supplicant to send the logoff command so the switch disabling the line protocol on the port the client computer is connected to. The logoff, along with the logon and reassociate command can also be executed by the user manually using the Barracuda NG Access Monitor or the command-line interface.

The four key entities in the network environment using port security are:

- **Client computer**

  with an installed Barracuda NG SSL VPN and NAC Client utilizing the wpa-supplicant, which will request access to the LAN and will respond to identity requests by the switch. The wpa-supplicant will be started and controlled by the Client Service for 802.1X authentication, where as the Barracuda NG Access Monitor service is responsible for the evaluation of the client computer's health state.

- **Switch**

  Is responsible for controlling the physical access to the LAN based on the authentication status of the client. The switch acts as proxy between the client computer and the authentication server.

- **Authentication Server**

Necessary for authentication, validates the client computer's identity information forwarded by the switch and notifies the switch which VLAN the client computer is assigned to. Due to the switch's functionality as proxy the authentication service is transparent to the client.

- **Access Control Server**

The Access Control Server is required to determine the health state of the client computer based on the information provided by the Barracuda NG Access Monitor service. It also handles the configuration of the VLANs assigned to the client computers for healthy and unhealthy states.

14.2 Status Monitoring

Multiple sources of information are available in order to monitor the status of the components handling the 802.1X authentication process:

- ***EAP Packet Tracer***
- ***Barracuda NG Access Monitor***
- ***Log files on the client computer***
- ***Access Control Server logs***
- ***Switch web interface***
- ***Switch console interface***

14.2.1 EAP Packet Tracer

The EAP Packet tracer displays all EAP and EAPOL packets captured by phionuio driver. To enable the capturing of EAP Packets to be processed by the EAP Packet Tracer modify the following option.

Table 14–1 *Key 8021XTraceEAP*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	8021XTraceEAP
Value	Enables or disables verbose output to be written (Default=1). • ***0 - disabled*** • ***1 - enabled***

Note

Changing this value takes effect immediately.
This value may also be changed through the ***Advanced Settings*** of the Barracuda NG Access Monitor

For every network interface, the driver will generate a separate dump file named `wpa_{adapter_uid}.cap` which is located in the install directory's `log` folder.

14.2.2 Using the Barracuda NG Access Monitor for Analysis

The Barracuda NG Access Monitor provides within its port security section a listing of all network interfaces capable of 802.1X, displaying the current status.

Additionally, the Barracuda NG Access Monitor allows opening a command-line interface for the selected device.

Supplicant console interface

If more detailed status information or control is required, the Barracuda NG Access Monitor provides the option to open a console interface for all instances of wpa-supplicants. This console interface allows monitoring and direct control of the wpa-supplicant.

Table 14–2 *Commands for wpa-supplicant*

Command	Description
`status verbose`	Lists all status information available from the wpa-supplicant
`logon`	Starts a new authentication sequence by sending an EAPOL start packet to the switch
`logoff`	Log off the client computer, disabling the line protocol on the port the client is connected to
`reassociate`	Will force a re-association

Note

Using the console interface requires Administrative privileges.

14.2.3 Log Files on the Client Computer

If verbose output is enabled log files are created for the following components:

Table 14–3 *Components - log files*

Component	Log Files
Client service	`phions.log`
Barracuda NG Access Monitor	`phionha.log`
For every instance of a running wpa-supplicant	`wpa_supplicant_{adapter_uid}.log`

The log files can be found in the folder `\log` located in the installation directory, which by default is `C:\Program Files\BarracudaNG\`. Also the Barracuda NG Access Monitor provides a view in the ***Advanced Settings*** section, listing all available log files and providing the functionality to open them in the default editor.

To enable or disable verbose the below registry needs to be set:

Table 14–4 *Key Logging*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	Logging
Value	Enables or disables verbose output to be written (Default=0). • ***0 - disabled*** • ***1 - enabled***

Note

Changing this value takes effect immediately.
This value may also be changed through the ***Advanced Settings*** of the Barracuda NG Access Monitor.

14.2.4 Switch Web Interface

The web interface provides various outputs for monitoring and configuration. These can be viewed in any web browser. The web interface additionally provides a simple command-line allowing configuring or showing any settings.

Following sample output shows the 802.1X configuration for the port used in this document.

- ***Command base-URL:***

```
/level/15/exec/-
```

- ***Complete URL:***

```
/level/15/exec/-/show/dot1x/interface/fa0\/3/CR
```

- ***Command:***

```
show dot1x interface fa0/3
```

Fig. 14–1 *802.1X configuration for the used ports*

```
Supplicant MAC 00a0.c992.0000
AuthSM State           = AUTHENTICATED(AUTH-FAIL-VLAN)
BendSM State           = IDLE
Posture                = N/A
   ReAuthPeriod       = 3600 Seconds (Locally Configured)
   ReAuthAction       = Reauthenticate
   TimeToNextReauth   = 3224 Seconds
PortStatus             = AUTHORIZED(AUTH-FAIL-VLAN)
MaxReq                 = 2
MaxAuthReq             = 2
HostMode               = Single
PortControl            = Auto
ControlDirection       = Both
QuietPeriod            = 1 Seconds
Re-authentication      = Enabled
ReAuthPeriod           = 3600 Seconds
ServerTimeout          = 30 Seconds
SuppTimeout            = 30 Seconds
TxPeriod               = 30 Seconds
Guest-Vlan             = 251
AuthFail-Vlan          = 252
AuthFail-Max-Attempts = 3
Critical Port          = Disabled
```

These values are described in more details on:

- ***ReAuthPeriod***

see 14.3.9 Periodic client re-authentication by the switch, page 193

- ***Guest-Vlan***

see 14.3.11 Authentication Message Exchange, page 194

- ***AuthFail-Vlan***

see 14.3.11 Authentication Message Exchange, page 194

- ***AuthFail-Max-Attempts***

see 14.3.11 Authentication Message Exchange, page 194

- ***QuietPeriod***

see 14.3.12 VLAN Assignment, page 195

The output following is the status of a network interface on the switch a client computer is connected to. The first line (underlined) shows the probably most important information about whether a client computer is connected to the port: `FastEthernet0/3 is down/up`. (up when a client is connected, and down if otherwise). The second part indicates if the line protocol is enabled (up) or disabled (down) restricting or allowing network traffic.

- ***Command base-URL:***

```
/level/15/exec/-
```

- ***Complete URL:***

```
/level/15/exec/-/show/dot1x/interface/fa0\/3/CR
```

- ***Command:***

```
show interface fa0/3
```

Fig. 14–2 *Status of a network interface on the switch*

```
FastEthernet0/3 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0016.c7ba.9505 (bia 0016.c7ba.9505)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:07:31, output 00:07:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7496 packets input, 1124053 bytes, 0 no buffer
     Received 7335 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 5949 multicast, 0 pause input
     0 input packets with dribble condition detected
     36644 packets output, 3008285 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

14.2.5 Switch Console Interface

For either administrative or informative purposes it is possible to connect to the switch using a telnet session. By default the console interface shows only little output. To enable higher verbosity it is recommended to enable debug information, as seen in the example, for various topics. To enable or disable debug logs it is required to enter the privileged exec mode.

To enter privileged exec mode, enter after initially authenticating following line:

- `enable`

Example enabling debug output:

- `debug aaa authentication`
- `debug aaa authorization`
- `debug aaa accounting`
- `debug dot1x all`
- `debug eap all`

Sample debug information for EAP should look something like this:

Fig. 14–3 *Sample debug information for EAP*

```
*Mar  2 23:13:32.140:     eap_authen : during state eap_auth_method_response, got event 11(eapMethodEnd)
*Mar  2 23:13:32.140: @@@ eap_authen : eap_auth_method_response -> eap_auth_select_action
*Mar  2 23:13:32.140:     eap_authen : during state eap_auth_select_action, got event 16(eapDecisionPass)
*Mar  2 23:13:32.140: @@@ eap_authen : eap_auth_select_action -> eap_auth_passthru_init
*Mar  2 23:13:32.140:     eap_authen : during state eap_auth_passthru_init, got event 18(eapPthruIdentity)
*Mar  2 23:13:32.140: @@@ eap_authen : eap_auth_passthru_init -> eap_auth_aaa_req
*Mar  2 23:13:32.140: AAA/AUTHEN/8021X (00000020): Pick method list 'default'
```

Note

The Cisco command line interface supports auto-competition for almost any command.

14.3 Authentication

14.3.1 Notes

- ***For convenience reading throughout this document, certain terms will be referred to by following aliases:***
  - **{install_directory}: The directory on the client computer, the Barracuda NG Access Monitor is installed to.**
  - **{adapter_uid}: The unique identifier for any network interface, this GUID can be viewed in the detail view of any network adapter in the port security window of the Barracuda NG Access Monitor**
- ***The 802.1X authentication mechanism is only supported on following types of network interfaces:***
  - **Ethernet**

- **Token Ring**
- **FDDI**
- **Point-to-Point**

14.3.2 Operational Sequence

14.3.3 Startup

1.) NG NAC services start

2.) Disabling Microsoft Windows 802.1X compliant software

3.) Starting the WPA supplicant

4.) WPA supplicant configuration

5.) WPA supplicant running

14.3.4 Runtime

1.) Re-authentication by the Client Service

2.) Re-authentication by the switch

3.) Re-authentication by the user using the command line

4.) Authentication Message Exchange

5.) VLAN Assignment

14.3.5 Shutdown

1.) Operating system shutdown by the user

2.) Operating system logoff by the user

3.) Manual Logoff command by the user

14.3.6 Start up

1.) Barracuda NG Network Access Client start

The Barracuda NG Network Access Client Secure Client 2.0 consists of two services, the main "Client" service and the "Barracuda NG Access Monitor" service which is dependent on the "Client" service. If verbose output is enabled, a log file for the Barracuda NG Client service, named "phions.log", and the Barracuda NG Access Monitor's "phionha.log", both within the log file directory (see Status Monitoring), will be created.

2.) Disabling Microsoft Windows 802.1X compliant software

Since Microsoft Windows ships with its own 802.1X compliant client software, the Client service needs to disable it before starting the WPA supplicant. The Microsoft 802.1X compliant client software consists of:

Table 14–5 *Microsoft 802.1X compliant client software*

Service Friendly Name	Service Name
Wired AutoConfig	• ***WZO (prior to Windows Vista)*** • ***dot3svc (Windows Vista)***
WLAN AutoConfig	Wlansvc
ndisuio	User Mode Input Output Driver

Once those services have been stopped by the client, the client will start the driver service that is necessary for handling requests from the switch.

After all supplicants have been terminated, they will be (re-) enabled. To verify for a successful disabling process, verbose output is available:

Fig. 14–4 *phions.log*

```
[009002007000] -->checking for WZO & Ndisuio and stopping them
[009002008000] ==> CheckAndStopService(dot3svc, true)
[009002008000] ==> CheckAndStopService(Wlansvc, true)
[009002008000] ==> CheckAndStopService(Ndisuio, true)
[009002006000] ==> togglephionuio
[009002006008] phionuio already running / phionuio started
[009002006000] <== togglephionuio
[009002007010] <-- finished WZO & Ndisuio service check
```

3.) Starting the wpa-supplicant

The " Client" service will start a WPA supplicant, named "wpa_supplicant.exe", for all supported network interfaces given following circumstances:

- ***"1.1.A is set to enabled***
- ***"1.1.B is set to enabled for the network interface to use 802.1X is set to enabled***

Table 14–6 *Key 8021XMonitor*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	8021XMonitor
Value	Enables or disables 8021X authentication on the client computer (Default=1) • ***0 - disabled*** • ***1 - enabled***

Note

Changes of this value take effect immediately.

Note

This value can also be changed within the ***Advanced Settings*** of the Barracuda NG Access Monitor, ***IEEE 802.1X Authentication*** parameter.

Table 14–7 *Key {adapter_uid}*

Item	Description
Path	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\phionuio\Parameters\Adapters\`
Key	{adapter_uid}
Value	Enables or disables 8021X authentication for the adapter with the specified adapter_uid (Default=0) • ***0 - disabled*** • ***1 - enabled***

Note

Changes of this value take effect immediately.

Note

This option may also be changed on the property page of the ***Barracuda Networks Personal Access Client*** within the network interface's properties dialog by changing the ***802.1X Authentication*** option.

Note

If an existing instance of a WPA supplicant is already running for the desired network interface while the service start is executed on the client, then the supplicant will be terminated followed by starting a new instance.

Alternatively the value in 1.1.A can be set by the Access Control Server, enforcing 802.1X authentication. To enable the enforced use of 802.1X by the Access Control Server, following option can be set:

- ***Enter the Access Control Server trust-zone configuration using the Barracuda NG Admin administration tool***
- ***Open the rule to enable the use of 802.1X authentication and select the view Policy Assignments***
- ***Set the option Use 802.1X Authentication to Yes or No as desired***

4.) wpa-supplicant configuration

In order for the "Client" service to run the wpa-supplicant, the wpa-supplicant requires a valid configuration file for every network interface a supplicant will operate on. These configuration files are located in the folder `{install_directory}\wpa` and generated by the Client service from a template configuration automatically.

If the configuration file for the network interface used is corrupted, following behavior will occur:

- ***The wpa-supplicant exe will terminate almost immediately and will not appear in the Process Explorer or Task Manager***
- ***If verbose output is enabled:***
  wpa_supplicant_{adapter_uid}.log:
  `Line X: Invalid configuration file …`

To resolve this problem proceed following steps:

- ***Delete the corrupted configuration file***

You will require elevated privileges to perform this step.

- ***Kill the process wpa_supplicant.exe***

You will require elevated privileges to perform this step.

Note

The Client service will generate the configuration file based on the template.

5.) wpa-supplicant running

A successful start of the wpa-supplicant can be verified by:

- ***The Process Explorer or Task Manager will show for every network interface using 802.1X, a wpa-supplicant, named "wpa_supplicant.exe" as child process of "phions.exe" appearing in the Process Explorer or Task Manager***
- ***If verbose output is enabled following verbose output needs to be present in the log files:***

Table 14–8 *wpa-supplicant running – phions.log*

Item	Output	Description
802.1X	`[009001000001]`	stating that 802.1X monitoring is enabled
	`[009004000002]`	stating the authentication method (machine, user, user with certificate)
	`[009002000009]`	802.1x monitor created
	`[009001000002]`	reloading adapter list for wpa_supplicant
Non-ethernet adapters	`[009001000003]`	`adapter found to be non-ethernet …`
Virtual adapters	`[009001000003]`	`found virtual adapter …`
Disabled adapters	`[009001000003]`	`found disabled adapter …`
Active adapters	`[009001000004]`	`802.1x disabled for adapter …`

Table 14–9 *wpa-supplicant running – wpa_supplicant_{adapter_uid}.log*

Output

`CTRL: Open pipe`
`CTRL: ConnectNamedPipe: connection in progress`
`Initializing interface '{adapter_uid}' …`

14.3.7 Runtime

During runtime the wpa-supplicant will re-authenticate periodically. This can be triggered either by the Client service or the switch.

14.3.8 Re-authentication by the client service

The client service is able to enforce a re-authentication, given the configured interval (see 2.0.A), independent of the switch's configuration. After the configured amount of seconds elapsed the Client service will start the authentication sequence. By sending a EAPOL Start packet (see: 2.3.I) and waiting for the identity request starting the authentication sequence (see: 2.3.II).

Table 14–10 *Registry entry for 802.1X authentication*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	8021XReAuthPeriod
Value	Desired number of seconds the "Client" service must wait until re-authentication (Default 3600 seconds) • ***0 - 4294967295***

Note

Changes of this value will take effect with the next health evaluation by the Barracuda NG Access Monitor service.

14.3.9 Periodic client re-authentication by the switch

You can enable periodic 802.1X client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600 (1 hour). This option must be changed either through a command line interface on the switch or the web interface.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts.

Commands:

- ***configure terminal***

  Enter global configuration mode

- ***interface <interface-id>***

  Specify the port to be configured, and enter interface configuration mode

- ***dot1x re-authentication***

  Enable periodic re-authentication of the client, which is disabled by default.

- ***dot1x timeout reauth-period*** <seconds>

  Set the number of seconds between re-authentication attempts.

  The range is 1 to 65535; the default is 3600 seconds.

  This command affects the behavior of the switch only if the periodic re-authentication is enabled.

- ***end***

  Return to privileged EXEC mode.

- ***show dot1x interface***

  Verify your entries

To disable periodic re-authentication, use the `no dot1x re-authentication interface` configuration command. To return to the default number seconds between re-authentication attempts, use the no dot1x timeout reauth-period interface configuration command.

Fig. 14–5 *Example*

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x reauth-period 4000
```

The re-authentication started by the switch is illustrated in 2.3.II.

14.3.10 Manually re-authenticating using the command line

You can manually re-authenticate the client connected to a specific port at any time by entering the `dot1x re-authenticate interface` <interface-id> privileged EXEC command in a remote telnet session on the switch or the web interface.

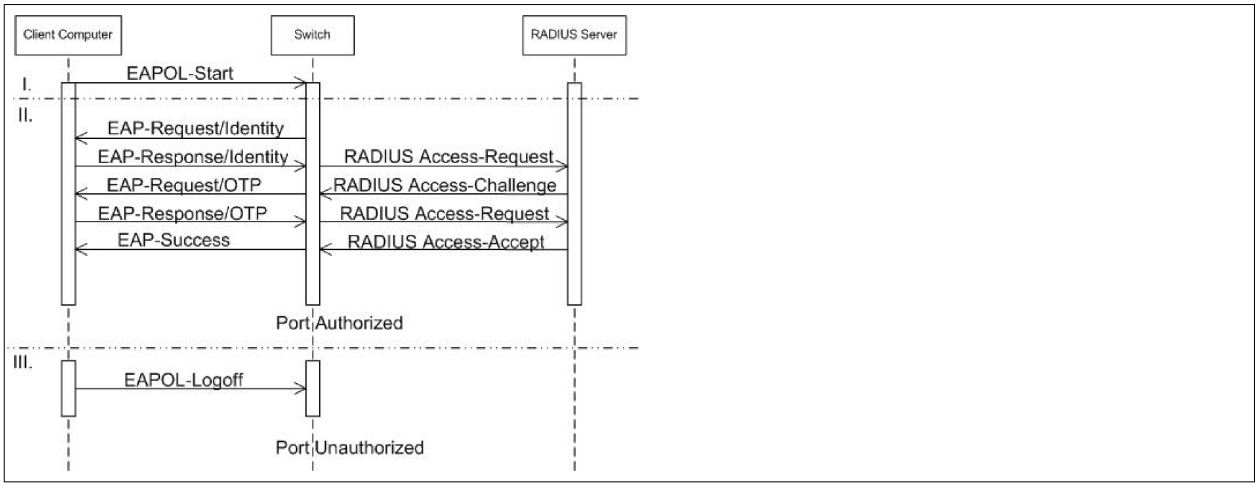
Fig. 14–6 *Example*

```
switch# dot1x re-authenticate interface fa0/3
```

14.3.11 Authentication Message Exchange

The following image illustrates the authentication message exchange between the client computer, the switch and the RADIUS authentication server:

Fig. 14–7 *Authentication Message Exchange Process*



Shown in the first section (I) is the initial EAPOL start packet sent by the wpa_supplicant from the client computer, starting the 802.1X authentication scheme. This occurs on following circumstances:

- ***An instance of the wpa-supplicant started and running beginning authentication.***
- ***The configured re-authentication period elapsed and the wpa-supplicant starts re-authentication.***

Section II illustrates the message exchange of the authentication. This occurs when:

- ***The client computer starts (re)-authentication; see section I above.***
- ***The configured re-auth period configured on the switch elapsed.***

- ***A re-authentication is triggered manually on the switch by a user through the command-line interface.***

Finally, section III shows the way the logoff command is sent to the switch in order to disable the line protocol on the port. There are several possibilities for the log-out process:

- ***The user shuts down the operating system on the client computer.***
- ***The user logged off the operating system on the client computer.***
- ***The user executed the logoff command manually using the Barracuda NG Access Monitor or the command-line interface.***

See for the EAPOL packet frames.

14.3.12 VLAN Assignment

Network access control is enforced by assigning the client different VLANs, each for a different state:

Table 14–11

VLAN	Condition	Description
Guest VLAN		Default VLAN which is initially assigned to the client computer
Authentication Fail	The authentication against the RADIUS server failed	The client computer will be assigned this VLAN if he fails to authenticate successfully before the maximum number of authentication failures is reached. The maximum number failures can be configured on the switch by setting the option AuthFail-Max-Attempts in the dot1x configuration on the desired port
Healthy	The client computer met all health requirements	This is the VLAN the client computer is indented to be assigned to.
Unhealthy	The client computer did not meet health requirements	In the Unhealthy-VLAN the client computer must be able to evaluate his health state and access resources vital for restoring a healthy state.

It is possible that to the client computer is a different VLAN addigned by the RADIUS server due to a failed authentication resulting of either:

- ***A change of the clients health state. This is the most common reason.***
- ***A change of the configuration on the Access Control Server.***
- ***A not matching session password.***

If this happens, then the switch will enter the Quiet Period, meanwhile disabling the line protocol and not responding to any packets received on the port the client computer is connected to.

Note

In the given engineering environment, the switch always enters the quiet period on the port the client computer is connected to, whenever a different one than the currently assigned VLAN is assigned to the client computer.

For faster response time it is recommended to set this value to 1 second. To change the quiet period, follow the steps below in privileged EXEC mode using a command-line interface on the switch.

Command:

- ***`configure terminal`***

  Enter the global configuration mode

- ***interface <interface-id>***

Specify the port to be configured, and enter the interface configuration mode

- ***dot1x timeout quiet-period <seconds>***

Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

The range is from 1 to 65535 seconds, the default is 60.

- ***end***

Return to the privileged EXEC mode.

- ***show dot1x interface***

Verify your entries.

To restore the default quiet time, use the `no dot1x timeout quiet-period` interface configuration command.

Fig. 14–8 *Example*

```
Switch(config-if)# dot1x timeout quiet-period 30
```

14.3.13 DHCP

It is possible instead of configuring the Access Control Server IPs locally on the client computer to distribute them via DHCP.

The Access Control Server IPs the client computer received via DHCP are visible in the Advanced Settings section of the Barracuda NG Access Monitor or the Barracuda NG Personal Firewall. Both provide the functionality to delete the Access Control Server IPs, if necessary.

DHCP Renew

If the client computers in the network are configured to obtain their IP address using DHCP, there is the possibility to trigger a DHCP renew whenever the client computer is assigned a different VLAN. This can be configured either on the Access Control Server forcing it on the clients, or on the client computer itself.

Table 14–12 *Key 8021xEnableDHCPRenew*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionvpn\settings`
Key	8021xEnableDHCPRenew
Value	Enables or disables DHCP request when the assigned VLAN changes. (Default=0) • ***0 - disabled*** • ***1 - enabled***

Note

Changes of this value take effect immidiately.

Note

This value may also be changed by using the ***Advanced Settings*** screen within the Barracuda NG Access Monitor.

To enable "DHCP Renew" on the Access Control Server enforcing it on all clients matching the rule it is configured, follow these steps:

- ***Enter the Access Control Server trustzone configuration using the Barracuda NG Admin administration tool***
- ***Open the rule to enable DHCP Renew and select the view Policy Assignments***
- ***Set the option Use DHCP Renew to Yes or No as desired***

Note

The value configured on the Access Control Server overwrites the value configured on the client computer.

14.3.14 ICMP Connectivity Checking

The Barracuda NG Access Monitor supports the usage of ICMP to check if the configured Access Control Server is available. The use of this option highly recommended because it avoids long timeouts, thus is enabled by default.

Table 14–13 *Key ICMPProbing*

Item	Description
Path	`HKEY_USERS\.Default\Software\phion\phionha\settings`
Key	ICMPProbing
Value	Enables or disables the use of ICMP packets to check if the Access Control Server is available. (Default=1) • ***0 - disabled*** • ***1 - enabled***

Note

This value may also be changed using the ***Advanced Settings*** within the Barracuda NG Access Monitor through the ***ICMP Connectivity Check*** parameter.

14.3.15 Resetting the 802.1X Authentication process

If, for which reason whatsoever, it is required to restart the 802.1X authentication process, the Barracuda NG Access Monitor provides the necessary functionality. In order to perform this you should follow these steps:

- ***Enter the Port Security section in the Barracuda NG Access Monitor***
- ***Selected the network interface to reset***
- ***Choose "Reset" from the tasks menu on the left or through the context menu of the network interface***

Once done, the session password will be reset and the 802.1X authentication process starts over.

14.3.16 Shutdown

14.3.17 Operating System Shutdown

When the client computer is been shut down, the Barracuda NG Access Monitor will send a logoff command to switch, causing the line protocol being disabled by the switch.

14.3.18 Operating System Logoff

When a user logs off his account from the operating system, the Barracuda NG Access Monitor follows the same procedure as above.

14.3.19 Manual Logoff

It is possible, if required, to logoff manually using the Barracuda NG Access Monitor. To do so take following steps:

- ***Enter the Barracuda NG Access Monitor Port Security section***
- ***Select the network interface to log off***
- ***Choose "Logoff" from the tasks menu on the left or through the context menu of the network interface***

To verify the logoff command was sent and executed properly, verbose output is required and needs to show the following:

Table 14–14 *phions.log*

Output
`[009003002002] sent command LOGOFF with answer [009003002003] about success`

Table 14–15 *phions.log*

	Output
	`[009002009001] monitor destroying`

For every supplicant	`[009003002002] sent command LOGOFF with answer [009003002003] about success`
	`[009003002002] sent command TERMINATE with answer [009003002003] about success`
	`[009003009003] thread for adapter … ended`

	`[009002009009] monitor destroyed`

14.4 Addendum

14.4.1 Packets

The table shows an EAPOL packet frame:

Table 14–16 *EAPOL packet frame*

Field Name	Size	Purpose
Version	1 Byte	Protocol version
Type	1 Byte	1 Start 2 Logoff
Length	2 Bytes	Length of the EAP packet
Data (EAP)	N Bytes	EAP packet

The table below shows the fields of the EAP request-response frame:

Table 14–17 *Fields of the EAP request-response frame*

Field Name	Size	Purpose
Code	1 Byte	1 Request 2 Response 3 Success 4 Failure
Identifier	1 Byte	To match request-response
Length	2 Byte	Length of total packet includes
Type	1 Byte	1 Identify 25 PEAP request Protected EAP communication
Data	N Byte	

14.4.2 WPA Supplicant Log File Identifiers

Table 14–18 *WPA Supplicant Log File Identifiers*

009	000	000	000	wpa_supplicant control
009	001	000	001	802.1x monitoring state (enabled/disabled)
			002	reloading adapter list
			004	stating adapter type and if it's added to list
			006	802.1x disabled for this adapter
			005	invalid values in adapter list
			008	excluding non-ethernet adapter

Table 14–18 *WPA Supplicant Log File Identifiers*

009	001	001	000	starting to reset 802.1x registry setting
			002	stating session live time
			010	finished resetting 802.1x registry settings
009	002			class C8021X Monitor
		000		constructor
			000	starting constructor
			010	leaving constructor
009	002	003		reloading adapters
			002	adding adapter to list to start supplicants
			004	removing adapter from list to start supplicants
			099	thread-id's of 802.1x threads
009	002	004		user logon/logoff
			002	reassociating user (logon value %d)
			004	sending events to threads
009	002	005		restart services (WZO & ndisuio)
			000	starting RestartServices
			003	error opening service manager
			004	REASSOCIATE event send to thread %d (thread id)
			004	EMERGENCYREPAIR event send to thread %d (thread id)
			005	error opening service %s
			006	service %s restarted successfully
			007	error starting service %s
			008	service started
			009	error in status query for service ndisuio
			010	leaving RestartServices
			044	set user event sent to thread %d (thread id)
009	002	006	000	starting TogglePhionUIO
			003	error opening service manager
			005	error opening service phionuio
			006	service phionuio started/stopped
			007	error starting/stopping service phionuio
			008	service phionuio already running/stopped
			010	leaving TogglePhionUIO
009	002	007	000	starting CheckServices
			010	leaving CheckServices

Table 14–18 *WPA Supplicant Log File Identifiers*

009	002	008	000	starting CheckAndStopService
			001	error opening service manager
			002	service %s not running
			003	error opening service %s
			004	service status for service %s
			005	error in status query for service %s
			006	stopped service %s
			007	error stopping service %s
			008	finished waiting for service to stop
			009	error in status query for service %s while waiting to stop
			010	leaving CheckAndStopService
009	002	009		shutdown / deletion
			000	starting to destroy 802.1x monitor
			003	thread did not shut down, terminating
			005	kill all pending supplicants
			010	finished destroying 802.1x monitor
009	003			class C8021XThread
		000		creation / startup
			001	thread starting/restarting for adapter %s (adapter uid)
			002	supplicant file information (conf, log, dump)
			003	no config found for supplicant on adapter xxx, create from template
			004	802.1x identity
			004	supplicant started for adapter %s (adapter uid)
			005	configuration template missing, prevent supplicant restart
			007	error creating config file, preventing restart
			008	starting supplicant with parameters …
			009	error starting supplicant …
			010	wpa_supplicant's process id
009	003	001		control pipe creation
			000	waiting for named pipe
			001	error opening control pipe
			002	control pipe status
009	003	002		sending / receiving commands over pipe
			001	success sending command over pipe
			002	failed sending command over pipe
			003	received response on command
			004	failed to read response on command

Table 14–18 *WPA Supplicant Log File Identifiers*

009	003	003		user authentication
			001	logging in as user username
			002	reassociation loop
			002	VLAN changed/unchanged, reassociate
			004	switched 802.1x authentication successfully
			004	waiting %d ms to retry new authentication
			101	logging in as user username (set user event)
			102	logging in as user username (reassociate event)
			133	received killed event
009	003	004	000	starting ip renew helper
			001	error allocating memory for GetAdaptersInfo
			003	GetAdaptersInfo failed
			005	error allocating memory for GetInterfaceInfo
			006	calling release ip
			008	calling renew ip
			010	leaving ip renew helper
009	003	005	…	FindStatus
			001	empty findState string
			003	empty expectedState string
			004	found findString with state expected
			005	expectedState not found
009	003	007	002	port state changed on adapter %s (adapter uid)
			002	eap failure %d from %d (do nothing) (count and max error)
			002	eap failure on adapter %s, reset user/pwd (adapter uid)
			022	eap failure on adapter %s (adapter uid)
			099	no running wpa_supplicant.exe found
			992	set user
009	003	008		closing / destroying pipe
			001	pipe closed
009	003	009		stopping / destroying thread
			003	thread ended on adapter xxx
			006	waiting for supplicant to enter LOGOFF state
			007	supplicant did not shutdown after terminate, kill process
009	004			class 8021XAuthData
		000	002	802.1x authentication method (local machine, current user)
			003	authentication type changed

Table 14–18 *WPA Supplicant Log File Identifiers*

009	004	004	002	GetTokenInformation failed in loadAuthData()
			003	lookup of account SID failed in loadAuthData()
			005	reading of machine SID failed in loadAuthData()
			006	using Barracuda NG Network Access Client label
			020	no user token found
			021	Get current logged in user token
			022	no active session, switch to local machine authentication
			023	no basic authentication user but active session, retrieve user
			023	8021xUser='%s' (user information)
			023	8021xDomain=%s (domain information)
			024	GetHostName Error=%s (error information)
			024	no user name found, switch to local computer authentication

14.4.3 Engineering Environment

This technical guideline is based on an engineering environment using following components:

Table 14–19 *Technical Guideline – Engineering Environment*

Switch	Cisco Catalyst 3560 - WS-C3560-48TS
Access Control Server	Barracuda NG Firewall 4.2
Barracuda Networks Secure Client	secure Client 2.0
Radius Server	FreeRADIUS

Additionally following tools have been used for analysis:

Table 14–20 *Technical Guideline – Tools*

Wireshark	Network monitoring and capturing tool
Process Explorer	Advanced process view by SysInternals
Regedit	Microsoft Windows Registry editor
Text editor	A text editor to view log files

14.4.4 Known Issues using Cisco Catalyst 3750-E Switch

Table 14–21 *Known Issues using Cisco Catalyst 3750-E Switch*

Firmware	C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc2) C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(46)SE, RELEASE SOFTWARE (fc2)
System image file	c3750e-universalk9-mz.122-44.SE.bin c3750e-universalk9-mz.122-46.SE.bin

In order for the RADIUS authentication to succeed with the above mentioned switch and software, "Authentication, Authorization and Accounting" need to be disabled. This can be done by following procedure:

Command:

- ***configure terminal***

  Enter global configuration mode

- ***no aaa accounting dot1x default group*** **<radius>**

  Disable accounting for 802.1X. The parameter `<radius>` sets the default group holding the attributes for RADIUS authentication. The group <radius> is configured and available by default. For any specific needs create your own group.

Otherwise, the RADIUS server receives an accounting request containing an empty user name. This request is not treated as an authentication failure; therefore the switch will not disable the port, allowing all network traffic. Given these circumstances client computers can perform health evaluations, but will be assigned a VLAN, remaining in the configured guest VLAN.

Furthermore, the legacy mode must be enabled on the switch to obtain a successful authentication. This is only possible by entering following command in the switch's command interface via telnet or the web interface.

- ***Switch# test aaa group radius server $Server$ $User$ Pwd port $Port$ legacy***

  Where the following must be replaced according to your configuration:

Table 14–22 *Command for Legacy Mode – Pptions*

$Server$	IP or host name of the RADIUS server
$User$	User name
Pwd	Password
$Port$	Tthe RADIUS server’s listening port

Chapter 15
Appendix

15.1 customer.inf File Template

Table 15–23 *customer.inf File Template*

Customer Install Files

Template code ready for copy-and-paste is listed below this table.

```
; ------------------------------------------------------------------------------------------
; customer.INF
;
; phion Customer Install Files
;
; Copyright 2008 phion AG
;
; For detailed information please consider the netfence entegra Guidance
; ------------------------------------------------------------------------------------------

[version]
signature  = "$Windows NT$"
provider   = %ph%

[Manufacturer]
%Phion%   = Phion

[DefaultInstall]
CopyFiles=PhionCustomerCopyFiles
AddReg = PhionCustomerReg

[DefaultUninstall]
DelFiles=PhionCustomerCopyFiles
DelReg = PhionCustomerReg

; ------------------------------------------------------------------------
; 1, Customer Area
; ------------------------------------------------------------------------
[PhionCustomerCopyFiles]

; destination-file-name[,source-file-name][,temporary-file-name][,flag]

customer.inf,,,2                                          ; important, do not remove
customer.lic,,,2                                           ; if importing a phion license file
active.i_fwrule,,,2                                      ; if importing a firewall rule set

; ------------------------------------------------------------------------
; 2, Customer Area
; REG_SZ    = 0x00000000
; REG_DWORD = 0x00010001
;
; Description:
;
; Certificate: AuthType (0x00010001)
;              0 -> phion authentication
```

```
;              1 -> X509 authentication
;              2 -> User / Password
;
; File: license (0x00000000)
; Subject: license (0x00000000)
;
; Microsoft Certificate Store Lookup: CertSearchOrder (0x00010001)
;              0 -> Lookup with Subject
;              1 -> Lookup with Issuer
;
; Use Serial Number: certserialnumber (0x00000000)
; Private Encrypt: PrivateEncrypt (0x00010001)
; Probe Encryption: ProbeEncryption (0x00010001)
; Prompt for user and password: AuthUser (0x00010001)
;
; Remote Server: server (0x00000000)
;
; Proxy Type Configuration: proxyType (0x00010001)
;              0 -> No Proxy
;              1 -> HTTP Proxy
;              2 -> Socks4
;              3 -> Socks5
;
; Proxy [:Port]: proxy (0x00000000)
; Proxy user: proxyuser (0x00000000)
; Domain: proxydomain  (0x00000000)
; Simulate SSL: simulateSSL (0x00010001)
;
; Authentication algorithm: hash (0x00010001)
;              1 -> MD5
;              2 -> SHA1
;
; Encryption Algorithm: encryption (0x00010001)
;              1 -> None
;              2 -> 3DES
;              4 -> AES
;              8 -> Cast
;              16 -> Blowfish
;              32 -> DES
;              64 -> AES256
;
; Tunnel Mode: mode (0x00010001)
;              1 -> Reliability (TCP)
;              2 -> Response (UDP)
;              3 -> Optimized (Hybrid)
;
; Virtual Adapter Configuration: dhcp (0x00010001)
;              0 -> Assign IP address manually
;              1 -> Use internal DHCP assignment (default)
;              2 -> Direct assignment
;
; Compression: streamCompression (0x00010001)
; Use Policy Server: usePolSrv,     0x00010001
; Disconnect when user logs off: terminateIfUserLogout (0x00010001)
; One Time Password: oneTimePassword (0x00010001)
; Allow ENA Connection: allowENA (0x00010001)
; Allow Sending Offline Ruleset: allowFWRule (0x00010001)
; Save new Certificate Unattended: unattended (0x00010001)
; Silent Mode (No Keep Alive): silent (0x00010001)
; Keep Alive (seconds): timeoutAlive (0x00010001)
; Start Script: startScript (0x00000000)
; Stop Script: stopScript (0x00000000)
; Enable MS Logon: enableMSLogon (0x00010001)
;
; Certificate Store Flag: StoreFlags (0x00010001)
;              ffffffff -> <Default>
;              10000 -> Current User
;              70000 -> Current User Group Policy
;              20000 -> Local Machine
;              90000 -> Local Machine Enterprise
;              80000 -> Local Machine Group Policy
;              50000 -> Phion VPN Service
;
; Certificate Store: store (0x00000000)
;              MY -> MY
;              Root -> Root
```

```
;              Trust -> Trust
;              CA -> CA
;
; Terminate Countdown (sec.): TerminateCountdown (0x00010001)
; Show Popup: ShowPopup (0x00010001)
; Close after Connect: CloseOnConnect (0x00010001)
; ------------------------------------------------------------------------------
[PhionCustomerReg]

; reg-root, [subkey], [value-entry-name], [flags], [value]

HKU, .DEFAULT\Software\Phion\phionvpn,      CustomerINF, 0x00000000, "%65600%\customer.inf"
; important, do not remove

; Profile 1 Example with phion.lic (Default selected)
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, Default,     0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, dhcp,        0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, AuthType,    0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, Description, 0x00000000, "phionLIC (Default)"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, license,     0x00000000, "%65600%\customer.lic"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\1, server,      0x00000000, "192.168.0.1"

; Profile 2 Example with extern linked X509 PKCS#12 File
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, Default, 0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, dhcp, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, AuthType, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, AuthUser, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, description, 0x00000000, "Extern PKCS#12"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, license, 0x00000000,
"%65600%\X509-Certificate.p12"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, server, 0x00000000, "192.168.0.1"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, mode, 0x00010001, 2
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, hash, 0x00010001, 2
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, PrivateEncrypt, 0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\2, store, 0x00000000, " "

; Profile 3 Example with Microsoft Certificate Store Linked x509 Certificate
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, Default, 0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, dhcp, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, AuthType, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, AuthUser, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, description, 0x00000000, "MY-Store Linked x509"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, license, 0x00000000, " "
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, server, 0x00000000, "192.168.0.1"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, mode, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, hash, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, PrivateEncrypt, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\3, store, 0x00000000, "MY"

; Profile 4 Example with phion.lic and Proxy Connection
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, Default,     0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, dhcp,        0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, Description, 0x00000000, "PhionLIC with Proxy"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, license,     0x00000000, "%65600%\customer.lic"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, server,      0x00000000, "192.168.0.1"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, Default, 0x00010001, 0
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, proxy, 0x00000000, "www.proxy.ip:3128"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, proxyType, 0x00010001, 1
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, proxyuser, 0x00000000, "testUser"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, proxydomain, 0x00000000, "PHION"
; HKU, .DEFAULT\Software\Phion\phionvpn\Profile\4, mode, 0x00000000, 1

; ------------------------------------------------------------------------------
; 3, Customer Area
; ------------------------------------------------------------------------------
[SourceDisksFiles]
; Files for disk phion AG Customer Files #1
; filename = diskid[,[ subdir][, size]]

customer.inf,,,1
customer.lic,,,1                                        ; if a phion license file is imported
active.i_fwrule,,,1                                      ; if a firewall rule set is imported

;------------------------------------------------------------------------------
; Do not change any attribute beyond this line!
;
```

```
[DestinationDirs]
PhionCustomerCopyFiles  = 65600

[SourceDisksNames]
1 = %DiskId1%,,,""

;-----------------------------------------------------------------------------
; Localizable Strings
;
[Strings]
ph                       = "Phion"
DisplayClassName         = "Phion Customer Files"
Phion                    = "Phion AG"
*Phiond.DeviceDesc       = "Phion Customer Files"
Phion.DeviceDesc         = "Phion Customer Files"
*Phion.DeviceDesc        = "Phion Customer Files"
phionvpn.Service.DispName = "Phion Customer Files"
DiskId1                  = "Phion Customer Files Disk #1"
```

15.2 VPN Profile Registry Keys

Table 15–24 *VPN Profile Registry Keys*

VPN Profile Registry Keys

```
"; 2, Customer Area"

"; REG_SZ    = 0x00000000"

"; REG_DWORD = 0x00010001"


"; Certificate: AuthType (0x00010001)"

";       0 -> Barracuda authentication"

";       1 -> X509 authentication"

";       2 -> User / Password"

";"

"; File: license (0x00000000)"

"; Subject: license (0x00000000)"

";"

"; Microsoft Certificate Store Lookup: CertSearchOrder (0x00010001)"

";       0 -> Lookup with Subject"

";       1 -> Lookup with Issuer"

";"

"; Use Serial Number: certserialnumber (0x00000000)"

"; Private Encrypt: PrivateEncrypt (0x00010001)"

"; Probe Encryption: ProbeEncryption (0x00010001)"

"; Prompt for user and password: AuthUser (0x00010001)"

";"

"; Remote Server: server (0x00000000)"

";"

"; Proxy Type Configuration: proxyType (0x00010001)"

";       0 -> No Proxy"

";       1 -> HTTP Proxy"

";       2 -> Socks4"

";       3 -> Socks5"

";"

"; Proxy [:Port]: proxy (0x00000000)"

"; Proxy user: proxyuser (0x00000000)"

"; Domain: proxydomain  (0x00000000)"

"; Simulate SSL: simulateSSL (0x00010001)"

";"

"; Authentication algorithm: hash (0x00010001)"

";       1 -> MD5"

";       2 -> SHA1"

";"
```

Table 15–24 *VPN Profile Registry Keys*

VPN Profile Registry Keys

```
"; Encryption Algorithm: encryption (0x00010001)"

";       1 -> None"

";       2 -> 3DES"

";       4 -> AES"

";       8 -> Cast"

";       16 -> Blowfish"

";       32 -> DES"

";       64 -> AES256"

";"

"; Tunnel Mode: mode (0x00010001)"

";       1 -> Reliability (TCP)"

";       2 -> Response (UDP)"

";       3 -> Optimized (Hybrid)"

";"

"; Virtual Adapter Configuration: dhcp (0x00010001)"

";       0 -> Assign IP address manually"

";       1 -> Use internal DHCP assignment (default)"

";       2 -> Direct assignment"

";"

"; Compression: streamCompression (0x00010001)"

"; Use Access Control Server: usePolSrv,     0x00010001"

"; Disconnect when user logs off: terminateIfUserLogout (0x00010001)"

"; One Time Password: oneTimePassword (0x00010001)"

"; Allow ENA Connection: allowENA (0x00010001)"

"; Allow Sending Offline Ruleset: allowFWRule (0x00010001)"

"; Save new Certificate Unattended: unattended (0x00010001)"

"; Silent Mode (No Keep Alive): silent (0x00010001)"

"; Keep Alive (seconds): timeoutAlive (0x00010001)"

"; Start Script: startScript (0x00000000)"

"; Stop Script: stopScript (0x00000000)"

"; Enable MS Logon: enableMSLogon (0x00010001)"

";"

"; Certificate Store Flag: StoreFlags (0x00010001)"

";       ffffffff -> <Default>"

";       10000 -> Current User"

";       70000 -> Current User Group Policy"

";       20000 -> Local Machine"

";       90000 -> Local Machine Enterprise"

";       80000 -> Local Machine Group Policy"

";       50000 -> Barracuda NG VPN Service"
```

Table 15–24 *VPN Profile Registry Keys*

VPN Profile Registry Keys

```
";"
"; Certificate Store: store (0x00000000)"
";       MY -> MY"
";       Root -> Root"
";       Trust -> Trust"
";       CA -> CA"
";"
"; Terminate Countdown (sec.): TerminateCountdown (0x00010001)"
"; Show Popup: ShowPopup (0x00010001)"
"; Close after Connect: CloseOnConnect (0x00010001)"
```

15.3 Profile Registry Keys

```
"Hardcoded Access Control Server IPs"

[HKEY_USERS\.DEFAULT\Software\Phion\phionha\PolSrv]
"1"="172.22.1.162"


[HKEY_USERS\.DEFAULT\Software\Phion\phionha\settings]
"Logging"=dword:00000001
"QuarantineCountDown"=dword:00004e20
"UseNTLM"=dword:00000001
"UseBasicAuthFallback"=dword:00000001
```

15.4 FAQs

- ***Connection to the VPN Server breaks immediately after it has been established***

A firewall rule set may have been damaged during transfer from the VPN server to the client. Disconnect all applications and connect again to solve the issue.

This behavior may also occur with slow connections. Increase the ***Keep alive (seconds)*** parameter (10.6.8 Advanced Settings Tab, page 143) if you encounter any problems.

- ***Connection breaks when IP address assignment over DHCP is used***

A connection problem occurs when the firewall slot is closed too early. Create a local Firewall rule set to solve the issue:

Action > Pass

Service > BOOTPS (rule out: UDP 67; rule in: UDP 68)

- ***The message*** `VPN Gateway not reachable via VPN tunnel` ***is logged to the events window***

Open the Expert tab (10.6.8 Advanced Settings Tab, page 143) and change from ***Virtual Adapter Configuration*** to ***Direct assignment*** or the other way around.

- ***The message*** `Session PHS: signature check failed (bad decrypt)` ***is logged to the events window.***

Deactivate ***Private Encrypt*** (10.3 Connection Dialog, page 132, Parameters available for use with X509 authentication, page 142).

15.5 Configuration Parameters

15.6 Parameter Lists

Chapter 1 Introduction

Chapter 2 Server Config – Access Control Service

Chapter 3 Server Config – Personal Firewall Rules

Chapter 4 Operating & Monitoring Barracuda NG NAC

Chapter 5 Client Installation

Chapter 6 Update or Migration

Chapter 7 Uninstall

Chapter 8 VPN Configuration

Chapter 9 Barracuda NG Personal Firewall

Chapter 10 VPN Component Configuration

Chapter 11 Barracuda NG Access Monitor

Chapter 12 Pre-Connector and Remote VPN

Chapter 13 Example Configuration

Chapter 14 802.1X – Technical Guideline

Chapter 15 Appendix

15.7 Figures

Chapter 1 Introduction

Chapter 2 Server Config – Access Control Service

Chapter 3 Server Config – Personal Firewall Rules

Chapter 4 Operating & Monitoring Barracuda NG NAC

Chapter 5 Client Installation

Chapter 6 Update or Migration

Chapter 7 Uninstall

Chapter 8 VPN Configuration

Chapter 9 Barracuda NG Personal Firewall

Chapter 10 VPN Component Configuration

Chapter 11 Barracuda NG Access Monitor

Chapter 12 Pre-Connector and Remote VPN

Chapter 13 Example Configuration

Chapter 14 802.1X – Technical Guideline

Chapter 15 Appendix

Barracuda Networks
Warranty and Software License Agreement

0.1 Barracuda Networks Limited Hardware Warranty

1. Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

2. Exclusive Remedy. Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks' option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks' discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

3. Exclusions and Restrictions. This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS' PRODUCTS AND THE SOFTWARE ARE PROVIDED "AS-IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

0.2 Barracuda Networks Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA NETWORKS SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU ARE A CORPORATION, PARTNERSHIP OR SIMILAR ENTITY, THEN THE SOFTWARE LICENSE GRANTED UNDER THIS AGREEMENT IS EXPRESSLY CONDITIONED UPON ACCEPTANCE BY A PERSON WHO IS AUTHORIZED TO SIGN

FOR AND BIND THE ENTITY. IF YOU ARE NOT AUTHORIZED TO SIGN FOR AND BIND THE ENTITY OR DO NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software and documentation, whether on disk, in flash memory, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this Agreement, and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Software is recorded but Barracuda retains ownership of the Software itself. If you have not completed a purchase of the Software and made payment for the purchase, the Software may only be used for evaluation purposes and may not be used in any production capacity. Furthermore the Software, when used for evaluation, may not be secure and may use publicly available passwords.

2. Permitted License Uses and Restrictions. If you have purchased a Barracuda Networks hardware product, this Agreement allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software. You may not make a backup copy of the Software. If you have purchased a Barracuda Networks Virtual Machine you may use the software only in the licensed number of instances of the licensed sizes and you may not exceed the licensed capacities. You may make a reasonable number of backup copies of the Software. If you have purchased client software you may install the software only on the number of licensed clients. You may make a reasonable number of backup copies of the Software. For all purchases you may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. You may not make the Software available over a network where it could be utilized by multiple devices or copied. Unless otherwise expressly provided in the documentation, your use of the Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as you may have paid Barracuda Networks the required license fee; and your use of the Software shall also be limited, as applicable and set forth in your purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to install Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Your use of the Software shall also be limited by any other restrictions set forth in your purchase order or in Barracuda Networks' product catalog, user documentation or Web site for the Software. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE. YOU EXPRESSLY AGREE NOT TO USE IT IN ANY OF THESE OPERATIONS.

3. You may not transfer, rent, lease, lend, or sublicense the Software or allow a third party to do so. YOU MAY NOT OTHERWISE TRANSFER THE SOFTWARE OR ANY OF YOUR RIGHTS AND OBLIGATIONS UNDER THIS AGREEMENT. You agree that you will have no right and will not, nor will it assist others to: (i) make unauthorized copies of all or any portion of the Software; (ii) sell, sublicense, distribute, rent or lease the Software; (iii) use the Software on a service bureau, time sharing basis or other remote access system whereby third parties other than you can use or benefit from the use of the Software; (iv) disassemble, reverse engineer, modify, translate, alter, decompile or otherwise attempt to discern the source code of all or any portion of the Software; (v) utilize or run the Software on more computers than you have purchased license to; (vi) operate the Software in a fashion that exceeds the capacity or capabilities that were purchased by you.

4. THIS AGREEMENT SHALL BE EFFECTIVE UPON INSTALLATION OF THE SOFTWARE OR PRODUCT AND SHALL TERMINATE UPON THE EARLIER OF: (A) YOUR FAILURE TO COMPLY WITH ANY TERM OF THIS AGREEMENT OR (B) RETURN, DESTRUCTION OR DELETION OF ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION. Rights of Barracuda Networks and your obligations shall survive any termination of this Agreement. Upon termination of this Agreement by Barracuda Networks, You shall certify in writing to Barracuda Networks that all copies of the Software have been destroyed or deleted from any of your computer libraries, storage devices, or any other location.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTIBILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, THAT CURRENT OR FUTURE VERSIONS OF ANY OPERATING SYSTEM WILL BE SUPPORTED, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. FURTHERMORE BARRACUDA NETWORKS SHALL ASSUME NO WARRANTY FOR ERRORS/BUGS, FAILURES OR DAMAGE WHICH WERE CAUSED BY IMPROPER OPERATION, USE OF UNSUITABLE

RESOURCES, ABNORMAL OPERATING CONDITIONS (IN PARTICULAR DEVIATIONS FROM THE INSTALLATION CONDITIONS) AS WELL AS BY TRANSPORTATION DAMAGE. IN ADDITION, DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING NETWORKS, BARRACUDA NETWORKS DOES NOT WARRANT THAT THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH THE SOFTWARE IS USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED PERPETUAL ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS WHICH YOU EITHER OWN OR CONTROL THAT ARE UTILIZED IN ANY BARRACUDA PRODUCT.

6. Termination and Fair Use Policy. BARRACUDA SHALL HAVE THE ABSOLUTE AND UNILATERAL RIGHT AT ITS SOLE DISCRETION TO DENY USE OF, OR ACCESS TO BARRACUDA SOFTWARE, IF YOU ARE DEEMED BY BARRACUDA TO BE USING THE SOFTWARE IN A MANNER NOT REASONABLY INTENDED BY BARRACUDA OR IN VIOLATION OF ANY LAW.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Content Restrictions. YOU MAY NOT (AND MAY NOT ALLOW A THIRD PARTY TO) COPY, REPRODUCE, CAPTURE, STORE, RETRANSMIT, DISTRIBUTE, OR BURN TO CD (OR ANY OTHER MEDIUM) ANY COPYRIGHTED CONTENT THAT YOU ACCESS OR RECEIVE THROUGH USE OF THE PRODUCT CONTAINING THE SOFTWARE. YOU ASSUME ALL RISK AND LIABILITY FOR ANY SUCH PROHIBITED USE OF COPYRIGHTED CONTENT. You agree not to publish any benchmarks, measurements, or reports on the product without Barracuda Networks' written express approval.

9. Third Party Software. Some Software which supports Bare Metal Disaster Recovery of Microsoft Windows Vista and Microsoft Windows 2008 Operating Systems (DR6) contains and uses components of the Microsoft Windows Pre-Installation Environment (WINPE) with the following restrictions: (i) the WINPE components in the DR6 product are licensed and not sold and may only be used with the DR6 product; (ii) DR6 is provided "as is"; (iii) Barracuda and its suppliers reserve all rights not expressly granted; (iv) license to use DR6 and the WINPE components is limited to use of the product as a recovery utility program only and not for use as a general purpose operating system; (v) Reverse engineering, decompiling or disassembly of the WINPE components, except to the extent expressly permitted by applicable law, is prohibited; (vi) DR6 contains a security feature from Microsoft that will automatically reboot the system without warning after 24 hours of continuous use; (vii) Barracuda alone will provide support for customer issues with DR6 and Microsoft and its Affiliates are released of all liability related to its use and operation; and, (viii) DR6 is subject to U.S. export jurisdiction.

10. Trademarks. Certain portions of the product and names used in this Agreement, the Software and the documentation may constitute trademarks of Barracuda Networks. You are not authorized to use any such trademarks for any purpose.

11. Export Restrictions. You may not export or re-export the Software without: (a) the prior written consent of Barracuda Networks, (b) complying with applicable export control laws, including, but not limited to, restrictions and regulations of the Department of Commerce or other United States agency or authority and the applicable EU directives, and (c) obtaining any necessary permits and licenses. In any event, you may not transfer or authorize the transfer of the Software to a prohibited territory or country or otherwise in violation of any applicable restrictions or regulations. If you are a United States Government agency the Software and documentation qualify as "commercial items", as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this Agreement may be incorporated, Government end user will acquire the Software and documentation with only those rights set forth in this Agreement. Use of either the Software or documentation or both constitutes agreement by the Government that the Software and documentation are "commercial computer software" and "commercial computer software documentation", and constitutes acceptance of the rights and restrictions herein.

12. General. THIS AGREEMENT IS GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA WITH JURISDICTION OF SANTA CLARA COUNTY, CALIFORNIA, UNLESS YOUR HEADQUARTERS IS LOCATED IN SWITZERLAND, THE EU, OR JAPAN. IF YOUR HEADQUARTERS IS LOCATED IN SWITZERLAND THE SWISS MATERIAL LAW SHALL BE USED AND THE JURISDICTION SHALL BE ZURICH. IF YOUR HEADQUARTERS IS LOCATED IN THE EU, AUSTRIAN LAW SHALL BE USED AND JURISDICTION SHALL BE INNSBRUCK. IF YOUR HEADQUARTERS IS LOCATED IN JAPAN, JAPANESE LAW SHALL BE USED AND JURISDICTION SHALL BE TOKYO. THIS AGREEMENT WILL NOT BE SUBJECT TO ANY CONFLICT-OF-LAWS PRINCIPLES IN ANY JURISDICTION. THIS AGREEMENT WILL NOT BE GOVERNED BY THE U.N. CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALES OF GOODS. This Agreement is the entire agreement between You and Barracuda Networks regarding the subject matter herein and supersedes any other communications with respect to the Software. If any provision of this Agreement is held invalid or unenforceable, the remainder of this Agreement will continue in full force and effect. Failure to prosecute a party's rights with respect to a default hereunder will not constitute a waiver of the right to enforce rights with respect to the same or any other breach.

13. Assignability. You may not assign any rights or obligations hereunder without prior written consent from Barracuda Networks.

14. Billing Issues. You must notify Barracuda of any billing problems or discrepancies within sixty (60) days after they first appear on the statement you receive from your bank, Credit Card Company, other billing company or Barracuda Networks. If you do not bring such problems or discrepancies to Barracuda Networks attention within the sixty (60) day period, you agree that you waive the right to dispute such problems or discrepancies.

15. Collection of Data. You agree to allow Barracuda Networks to collect information ("Statistics") from the Software in order to fight spam, virus, and other threats as well as optimize and monitor the Software. Information will be collected electronically and automatically. Statistics include, but are not limited to, the number of messages processed, the number of messages that are categorized as spam, the number of virus and types, IP addresses of the largest spam senders, the number of emails classified for Bayesian analysis, capacity and usage, websites not categorized, fingerprints of emails, and other statistics. Your data will be kept private and will only be reported in aggregate by Barracuda Networks.

16. Subscriptions. Software updates and subscription information provided by Barracuda Energize Updates or other services may be necessary for the continued operation of the Software. You acknowledge that such a subscription may be necessary. Furthermore some functionality may only be available with additional subscription purchases. Obtaining Software updates on systems where no valid subscription has been purchased or obtaining functionality where subscription has not been purchased is strictly forbidden and in violation of this Agreement. All initial subscriptions commence at the time of activation and all renewals commence at the expiration of the previous valid subscription. Unless otherwise expressly provided in the documentation, you shall use the Energize Updates Service and other subscriptions solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by you. All subscriptions are non-transferrable. Barracuda Networks makes no warranty that subscriptions will continue un-interrupted. Subscription may be terminated without notice by Barracuda Networks for lack of full payment.

17. Auto Renewals. If your Software purchase is a time based license, includes software maintenance, or includes a subscription, you hereby agree to automatically renew this purchase when it expires unless you notify Barracuda 15 days before the renewal date. Barracuda Networks will automatically bill you or charge you unless notified 15 days before the renewal date.

18. Time Base License. If your Software purchase is a time based license you expressly acknowledge that the Software will stop functioning at the time the license expires. You expressly indemnify and hold harmless Barracuda Networks for any and all damages that may occur because of this.

19. Support. Telephone, email and other forms of support will be provided to you if you have purchased a product that includes support. The hours of support vary based on country and the type of support purchased. Barracuda Networks Energize Updates typically include Basic support.

20. Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Software or Subscription and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Software or Subscriptions.

21. Open Source Licensing. Barracuda Networks products may include programs that are covered by the GNU General Public License (GPL) or other Open Source license agreements, in particular the Linux operating system. It is expressly put on record that the Software does not constitute an edited version or further development of the operating system. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks. Further details may be provided in an appendix to this agreement where the licenses are re-printed. Barracuda Networks makes available the source code used to build Barracuda products available at source.barracuda.com. This directory includes all the open source programs that are distributed on the Barracuda products. Obviously not all of these programs are utilized, but since they are distributed on the Barracuda product we are required to make the source code available.

0.3 Barracuda Networks Software License Agreement Appendix

The following license agreements may apply to the software provided by Barracuda Networks.

The GNU General Public License (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF GNU TERMS AND CONDITIONS

Barracuda Networks products may include programs that are covered by the GNU General Public License. The GNU General Public License is re-printed below for you reference.

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things. To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

* a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

* b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

* c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

* d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or

legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

* a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

* b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

* c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

* d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

* e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the

Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

* a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

* b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

* c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

* d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

* e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

* f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction,

each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of

the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF GNU TERMS AND CONDITIONS

Barracuda Networks Products may contain programs and software that are covered by the Lesser General Public License The Lesser General Public License is re-printed below for you reference

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first

think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

Terms and Conditions for Copying, Distribution and Modification

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under

copyright law that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU

FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Barracuda Networks Products may contain programs and software that are covered by the Artistic License The Artistic license is re-printed below for you reference.

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions

• "Package" efers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

• "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

• "Copyright Holder" is whoever is named in the copyright or copyrights for the package.

• "You" is you, if you're thinking about copying or distributing this Package.

• "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

• "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

Conditions

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in

aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these sub-routines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

Barracuda Networks Products may contain programs and software that are covered by the MIT-License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the names of the author(s) nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission. Disclaimer THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. (Note: The above license is copied from the BSD license at: www.opensource.org/licenses/bsd-license.html, substituting the appropriate references in the template.) (end)

Barracuda Networks Software may include programs that are covered by the Mozilla Public License Version 1.1

1. Definitions.

1.0.1 "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1 "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2 "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3 "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4 "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5 "Executable" means Covered Code in any form other than Source Code.

1.6 "Initial Developer'' means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7 "Larger Work'' means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8 "License'' means this document.

1.9 "Modifications'' means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

- A. Any addition to or deletion from the contents of a file
- containing Original Code or previous Modifications.
- B. Any new file that contains any part of the Original Code or
- previous Modifications.

1.10. "Original Code'' means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

- "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50 %) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1 The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2 Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1 Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2 Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3 Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4 Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5 Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A, and to related Covered Code.

6. Versions of the License.

6.1 New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2 Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3 Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1 This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3 If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4 In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

Barracuda Networks Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License: "Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Networks Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ''AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Networks Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau, All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395, tech-transfer@andrew.cmu.edu . Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, AND IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda Networks Products may contain programs and software that are copyright (c) 2000, 2001, 2002, 2003, 2004 John Lim All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this

list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of the John Lim nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. DISCLAIMER:THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JOHN LIM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are copyright protected by: AMCC 215 Moffet Park Drive, Sunnyvale California, CA-94089, USAwww.amcc.com. AMCC grants to you a non-exclusive, non-transferable, non-sublicensable license to use the Product.

LIMITS

You may not copy, modify, rent, sell, distribute, or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software; (2) you may not reverse engineer, decompile, or disassemble the Software; and (3) you many not sublicense the Software.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS

Title to all copies of the Software will remain with AMCC or its suppliers. The Software is copyrighted and protected by United States and Austrian copyright laws and international treaty provisions. You may not remove any copyright, patent, or other proprietary notices from the Software. AMCC and Barracuda Networks or its suppliers may make changes to the Software, or to items referenced therein, at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, AMCC grants no express or implied right under AMCC patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITATION OF LIABILITY

IN NO EVENT SHALL AMCC AND BARRACUDA NETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF AMCC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION

This agreement will be terminated at any time if you violate its terms. Upon termination, you will immediately destroy the software.

RESTRICTED RIGHTS LEGEND

The AMCC Software Products are "Restricted Computer Software." If the Software Products are licensed for use by the United States or for use in the performance of a United States government prime contract or subcontract, Customer agrees that the Software Products are delivered as: (i) "commercial computer software" as defined in DFARS 252.227-7013, Rights in Technical Data – Noncommercial Items; DFARS 252.227-7014, Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation; and DFARS 252.227-7015, Technical Data Commercial Items; (ii) as a "commercial item" as defined in FAR 2.101; or (iii) as "restricted commercial software" as defined in FAR 52.227-19, Commercial Computer Software – Restricted Rights; whichever is applicable. The use, duplication, and disclosure of the Software Products by the Department of Defense shall be subject to the terms and conditions set forth in the accompanying license agreement as provided in DFARS 227.7202. All other use, duplication and disclosure of the Software Products and Documentation by the United States shall be subject to the terms and conditions set forth in the accompanying license agreement and the restrictions contained in subsection (c) of FAR 52.227-19, Commercial Computer Software – Restricted Rights, or FAR 52.227-14, Rights in Data. Contractor/licensor is AMCC, 6290 Sequence Drive, San Diego, CA 92121.

Barracuda Networks Software may include programs that are covered by the Apache License. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the

NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Barracuda Networks Products may contain programs and software that are copyright (c) 1990, 1993, 1994, 1995;The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1996

The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are copyright (C) 2004 Internet Systems Consortium, Inc. ("ISC") Copyright (C) 1996-2003 Internet Software Consortium. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. $Id: COPYRIGHT,v 1.6.2.2.8.2 2004/03/08 04:04:12 marka Exp $ Portions Copyright (C) 1996-2001 Nominum, Inc. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda Networks Products may contain programs and software that are copyright Broadcom Corporation. THE SOFTWARE IS OFFERED "AS IS", AND BROADCOM GRANTS AND LICENSEE RECEIVES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, BY STATUTE, COMMUNICATION OR CONDUCT WITH LICENSEE, OR OTHERWISE. BROADCOM SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE OR NONINFRINGEMENT CONCERNING THE SOFTWARE OR ANY UPGRADES TO OR DOCUMENTATION FOR THE SOFTWARE. WITHOUT LIMITATION OF THE ABOVE, BROADCOM GRANTS NO WARRANTY THAT THE SOFTWARE IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION, AND GRANTS NO WARRANTY REGARDING USE OR THE RESULTS THEREFROM INCLUDING, WITHOUT LIMITATION, ITS CORRECTNESS, ACCURACY OR RELIABILITY.

Barracuda Networks Software may include programs that are covered by the The Code Project Open License. The The Code Project Open License is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs

The Code Project Open License (CPOL) 1.02

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

* Source Code and Executable Files can be used in commercial applications;

* Source Code and Executable Files can be redistributed; and

* Source Code can be modified to create derivative works.

* No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

* The Article accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

1. Definitions.

a. "Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

b. "Author" means the individual or entity that offers the Work under the terms of this License.

c. "Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

d. "Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

e. "Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

f. "Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

g. "Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

h. "Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

i. "You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

2. Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. You may use the standard version of the Source Code or Executable Files in Your own applications.

b. You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

c. You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

d. You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

e. The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

4. Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

5. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

b. You agree not to advertise or in any way imply that this Work is a product of Your own.

c. The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

d. You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

e. You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

f. You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

6. Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

7. Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

8. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9. Termination.

a. This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9,

10 and 11 will survive any termination of this License.

b. If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

c. Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

10. Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

11. Miscellaneous

a. This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

b. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d. This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Barracuda Networks Products may contain programs and software that are Copyright (c) 1999-2001, Angelos D. Keromytis. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may include programs that are covered by the OpenLDAP Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain copyright statements and notices, Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and Redistributions must contain a verbatim copy of this document.The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders. OpenLDAP is a registered trademark of the OpenLDAP Foundation. Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.(eay@cryptsoft.com).The implementation was written so as to conform with Netscapes SSL.This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following onditions are met:Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIALDAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Barracuda Networks Products may contain programs and software that are Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).Original SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)." The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Barracuda Networks Products may contain programs and software that are Copyright (c) 1999 - 2002 The PHP Group. All rights reserved. Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The

name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo". 4. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License. 5. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP, freely available from <http://www.php.net/>". THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of voluntary contributions made by many individuals on behalf of the PHP Group. The PHP Group can be contacted via Email at group@php.net. For more information on the PHP Group and the PHP project, please see <http://www.php.net>. This product includes the Zend Engine, freely available at <http://www.zend.com>.

Barracuda Networks Products may contain programs and software that are Copyright (c) 1996-2005, The PostgreSQL Global Development Group Portions Copyright (c) 1994, The Regents of the University of California Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies. IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Barracuda Networks Products may contain programs and software that are Copyright (c) 1997-2000 Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry.Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Barracuda Networks Products may contain programs and software that are Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson

(tjh@cryptsoft.com)". THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Barracuda Networks Products may contain programs and software that are Copyright 2000 Aaron D. Gifford. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A ARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain SNMP programs and software that are covered in part by the license below:

Various copyrights apply to this package, listed in 3 separate parts below. Please make sure to take note of all parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. ----

Part 1: CMU/UCD copyright notice: (BSD like) ----- Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001, Networks Associates Technology, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: •Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. •Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

•Neither the name of the NAI Labs nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY

OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: •Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. •Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. •The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are covered by the License below.

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

• "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

• "Copyright Holder" is whoever is named in the copyright or copyrights for the package.

• "You" is you, if you're thinking about copying or distributing this Package.

• "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

• "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding Standard Version executables, giving the nonstandard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.

8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Barracuda Networks Products may contain programs and software that are covered by the License below.

A part of this software uses the tun/tap driver for Mac OS X provided byMattias Nissler. This driver comes along with following terms of license:tun/tap driver for Mac OS X Copyright (c) 2004, 2005 Mattias Nissler <mattias.nissler@gmx.de>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ''AS IS'' AND ANYEXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR APARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THEAUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOTLIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSSOF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVERCAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IFADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are copyright (C) 2007 Advanced Software Production Line, S.L. All rights reserved. the software includes source code from the following projects, which are covered by their own licenses: Vortex Library, fully available at http://www.aspl.es/vortex AXL, fully available at: http://www.aspl.es/axl

DISCLAIMER: THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JOHN LIM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy). Copyright (c) 2005 - 2008 CACE Technologies, Davis (California). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: . Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT

HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors. This product includes software developed by the Kungliga Tekniska Högskolan and its contributors. This product includes software developed by Yen Yen Lim and North Dakota State University.

Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors." 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors." 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features

or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University" 4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1993 by Digital Equipment Corporation. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission. THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution. The name of Juniper Networks may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright 1989 by Carnegie Mellon. Permission to use, copy, modify, and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Carnegie Mellon not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Carnegie Mellon and Stanford University. Carnegie Mellon makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Barracuda Networks Products may contain programs and software that are copyright (c) 2003-2008, Jouni Malinen <j@w1.fi> and contributors All Rights Reserved. This program is dual-licensed under both the GPL version 2 and BSD license. Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may include programs that are covered by the BSD License:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ''AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Networks Products may contain programs and software that are Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Barracuda Networks Products may contain programs and software that are covered by the VIM License below.

I) There are no restrictions on distributing unmodified copies of Vim except that they must include this license text. You can also distribute unmodified parts of Vim, likewise unrestricted except that they must include this license text. You are also allowed to include executables that you made from the unmodified Vim sources, plus your own usage examples and Vim scripts.

II) It is allowed to distribute a modified (or extended) version of Vim, including executables and/or source code, when the following four conditions are met:

1) This license text must be included unmodified.

2) The modified Vim must be distributed in one of the following five ways:

a) If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.

b) If you have received a modified Vim that was distributed as mentioned under a) you are allowed to further distribute it unmodified, as mentioned at I). If you make additional changes the text under a) applies to those changes.

c) Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.

d) When you have a modified Vim which includes changes as mentioned under c), you can distribute it without the source code for the changes if the following three conditions are met:

- The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.

- You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.

- You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.

e) When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.

3) A message must be added, at least in the output of the ":version" command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2)e) adding the message is only required for as far as this does not conflict with the license used for the changes.

4) The contact information as required under 2)a) and 2)d) must not be removed or changed, except that the person himself can make corrections.

III) If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code. The preferred way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g., a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is <maintainer@vim.org>

IV) It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

Barracuda Networks Products may contain programs and software that are covered by PSF LICENSE AGREEMENT FOR PYTHON 2.4

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.4 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.4 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004 Python Software Foundation; All Rights Reserved" are retained in Python 2.4 alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.4 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.4.

4. PSF is making Python 2.4 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES,

EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.4 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.4 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.4, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python 2.4, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Barracuda Networks Products may contain programs and software that are Copyright (C) 1994-2004 The XFree86®Project, Inc. All rights reserved.Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution, and in the same place and form as other copyright, license and disclaimer information. 3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by The XFree86 Project, Inc (http://www.xfree86.org/) and its contributors", in the same place and form as other third-party acknowledgments. Alternately, this acknowledgment may appear in the software itself, in the same form and location as other such third-party acknowledgments. 4. Except as contained in this notice, the name of The XFree86 Project, Inc shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from The XFree86 Project, Inc. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE XFREE86 PROJECT, INC OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs and software that are Copyright (c) 2010, Intel Corporation, All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Issue Date: Aug 6, 2010

Barracuda Networks makes available the source code used to build Barracuda products available at source.barracuda.com. This directory includes all the programs that are distributed on the Barracuda products. Obviously not all of these programs are utilized, but since they are distributed on the Barracuda product we are required to make the source code available.

(v2.5)

Barracuda Networks Technical Documentation

RECLAIM YOUR NETWORK™