Barracuda Networks Technical Documentation

Barracuda **SSL VPN**

Administrator’s Guide

Version 2.2

RECLAIM YOUR NETWORK™

Copyright Notice

Trademarks

Contents

Chapter 1
Introduction

This chapter provides an overview of the Barracuda SSL VPN and includes the following topics:

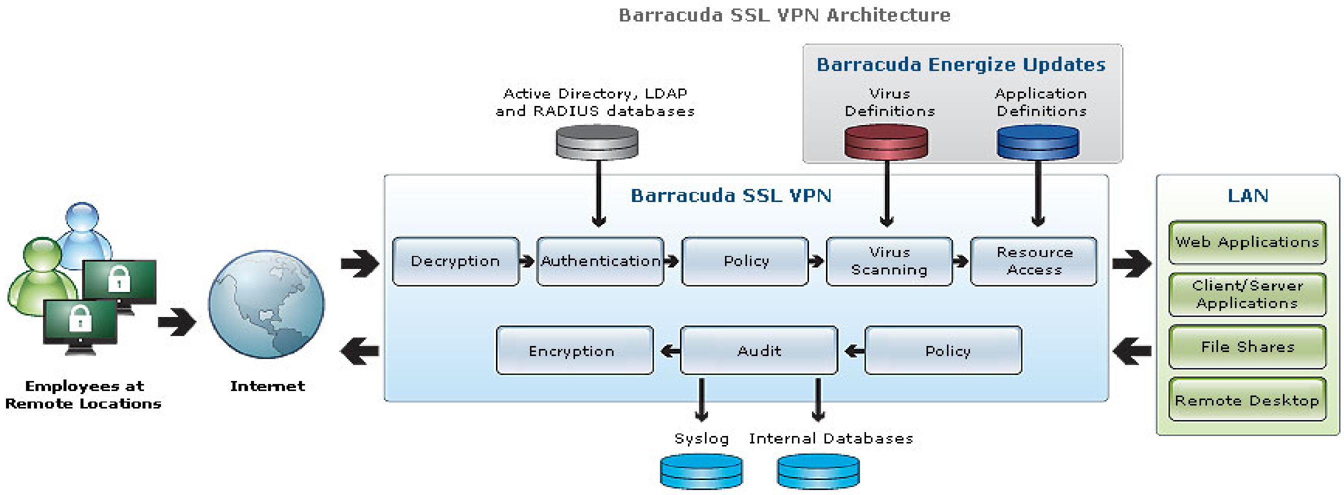
Overview

The Barracuda SSL VPN is an integrated hardware and software solution enabling secure, clientless remote access to internal network resources from any web browser.

Designed for remote employees and road warriors, the Barracuda SSL VPN provides comprehensive control over file systems and web-based applications requiring external access. The Barracuda SSL VPN integrates with third-party authentication mechanisms to control user access levels and provide single sign-on.

- Enables access to corporate intranets, file systems or other web-based applications
- Tracks resource access through auditing and reporting facilities
- Scans uploaded files for viruses and malware
- Leverages multi-factor, layered authentication mechanisms, including RSA SecurID tokens
- Integrates with existing Active Directory and LDAP directories
- Utilizes policies for granular access control framework
- •Supports any web browser on PC or Mac

Figure 1.1: Barracuda SSL VPN Architecture



Features of the Barracuda SSL VPN

Intranet Web Forwarding

The Barracuda SSL VPN acts as a web proxy for most intranet websites. There are a number of methods available to proxy intranet websites. The method is determined by the complexity of the website.

Windows Explorer Mapped Drives

When connecting using Windows 2000 or later, administrators configure the Barracuda SSL VPN Agent to automatically map network drives directly to file systems authorized for VPN access. These mapped drives are used like other network drives and are safely removed after the session ends. The Barracuda SSL VPN Agent transparently encrypts all files copied to and from mapped drives.

Application Launching

Using Application Launching, administrators can customize which applications are deployed to VPN users. The Barracuda SSL VPN includes a number of applications by default, such as SSH, SFTP, Telnet, and Remote Desktop clients. With the Remote Desktop application, users are able to access their desktops with ease.

Barracuda Network Connector

Designed for applications using UDP or for providing full network access to a client, the Barracuda Network Connector is a secure IP tunneling client installed on a user's workstation or laptop. When the Barracuda Network Connector is started, a full IP connection is created to the Barracuda SSL VPN appliance, enabling content to stream off the remote network and allowing the use of any TCP or UDP application, such as legacy client/server applications.

PPTP and L2TP/IPsec

The Barracuda SSL VPN can be configured to accept PPTP and L2TP/IPsec connections. This allows remote devices such as smartphones and Apple iPads to use their built-in network clients to establish a secure network connection, with no additional servers or special software required.

Remote Assistance

This helpdesk feature of the Barracuda SSL VPN enables system administrators to easily communicate with remote users that are in need of assistance. The built-in management system enables users to submit a request for help directly through the interface of the Barracuda SSL VPN, and also empowers authorized help personnel with direct access to and remotely control the system in trouble.

Single Sign-On

The Barracuda SSL VPN integrates with existing user databases via LDAP, Active Directory, and NIS. This ensures user account maintenance is centralized and eliminates the duplication of user data across the organization. Additionally, the Barracuda SSL VPN authenticates certain services using credentials, including:

- **Remote Desktop**. The Barracuda SSL VPN has the ability to pass the active users' Active Directory credentials through to the Remote Desktop session for true single sign-on.
- **Intranet Web Forwards**. When using the Reverse Proxy Web Forwarding feature, intranet websites can be launched passing through the active users' credentials to the web application allowing transparent authentication.

Hardware Token Authentication

The Barracuda SSL VPN supports RSA SecurID, VASCO, Secure Computing and CryptoCard authentication servers. The use of hardware token authentication allows for access using a One-Time Password (OTP) token.

Auditing and Reporting

All resource access through the Barracuda SSL VPN is audited. Reports are available in real time showing a comprehensive look at privilege usage, failed logins, file and intranet use. Additionally, the status page provides statistics showing system use and performance.

Multiple User Databases

User databases are used where multiple user repositories exist within an organization. By using user databases, the Barracuda SSL VPN can be configured to authenticate against multiple domain servers and other directories, such as Active Directory, LDAP, and NIS concurrently.

Energize Updates

Many security technologies are integrated into the Barracuda SSL VPN. In addition to the virus protection that is standard on all Barracuda Networks products, the Barracuda SSL VPN also delivers the latest in virus and application definitions through Energize Updates, which are updated at Barracuda Central.

Chapter 2

VPN Concepts

This chapter provides an overview of the Barracuda SSL VPN and includes the following topics:

Basic Terminology

The following is a list of some of the terms used by the Barracuda SSL VPN. Understanding these particular terms will aid in administering your Barracuda SSL VPN.

Table 2.1: Basic Terminology

Term	Description
Policy	A collection of user groups and/or individual user accounts that are to be granted the same access privileges to a network resource.
Access Rights	Permissions granted to specific policies for managing resource, System and Personal configurations.
Resource	A network location or application in your local network that is available to users connecting through the Barracuda SSL VPN.
Web Forwards	A type of resource for defining HTTP/HTTPS-based access.
Network Places	A type of resource for defining access to file systems.
Applications	A type of resource for defining access to client-server applications.
SSL Tunnels	A type of resource for defining access to non-Application ports on internal systems such as those that require direct logins.
Profiles	A type of resource for customizing an individual's access from a remote location.
Categories	A customizable method of grouping available resources for easy access.
Barracuda Network Connector	A utility that runs on a connecting system to provide it with full access to the internal network.
Barracuda SSL VPN Agent	A Java-based application that runs on the connecting system to create and manage secured connections with internal resources.
Barracuda Server Agent	A utility that runs on a system in one network, which allows the Barracuda SSL VPN to provide its resources to systems in other secured networks.

Barracuda SSL VPN Configurations

Barracuda SSL VPNs can be placed either outside your DMZ behind your organization's network firewall, or within the DMZ itself:

Table 2.2 shows when each deployment type is recommended.

Table 2.2: Deployment Type Details

Configuration	Advantages
BEHIND your corporate firewall (Typical Deployment)	Allows all authentication to be handled by the Barracuda SSL VPN. Only ONE firewall rule is needed to allow only secured traffic into your internal network.
BEFORE your corporate firewall (inside a DMZ)	Added layer of security, but will require additional firewall rules configured on both sets of corporate firewalls.

Note

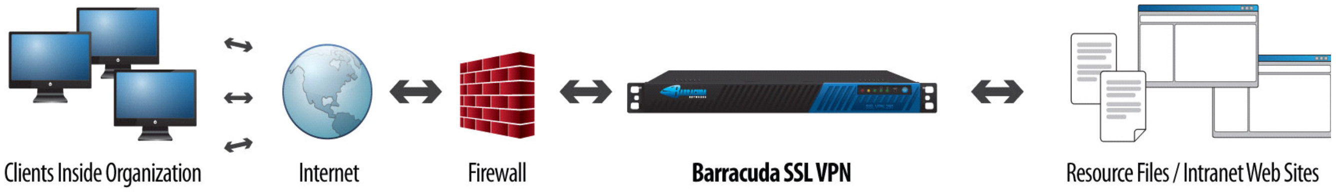
For specific information on the steps required to add new messages to the Barracuda SSL VPN, see *Basic Terminology* on page 14.

Typical Deployment

The Barracuda SSL VPN is typically placed behind your network firewall, with only specific ports (usually only 443, the standard SSL port) allowed through from the firewall to the Barracuda SSL VPN. Authorization happens on the Barracuda SSL VPN before any traffic is allowed into your internal network.

Placing the Barracuda SSL VPN inside your firewall gives you the flexibility to determine which of your internal network resources are available to your VPN users without requiring any additional re-configuring of your internal network. All you will need to configure are your access policies to the desired internal resources.

Figure 2.1: Sample layout for Typical Deployments


Clients Inside Organization
Internet
Firewall
Barracuda SSL VPN
Resource Files / Intranet Web Sites

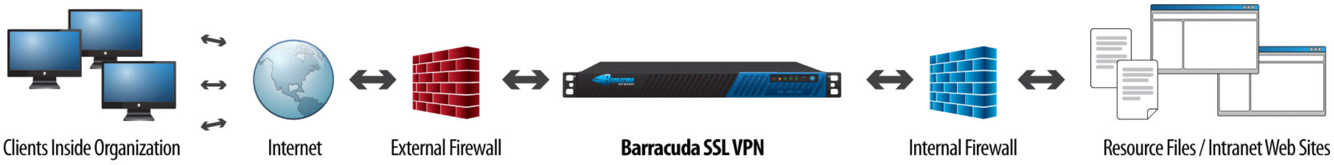
Clustered Deployment

If you have a pair of Barracuda SSL VPNs that you would like to load balance, you can deploy a load balancer between your firewall and the Barracuda SSL VPNs. Similarly, if you are using a proxy server, you deploy it between your firewall and Barracuda SSL VPN.

Other Deployments

If you have a DMZ in your network, then the Barracuda SSL VPN can be placed behind the external network firewall but in front of the internal one. This allows secure access through the external firewall to the Barracuda SSL VPN over port 443 but any access to resources on the trusted network will require another port to be opened on the internal firewall. This may provide an extra layer of isolation for your internal network, but will make it more difficult for you to manage individual resource access because of the additional rules that will be required both on your internal firewall as well as on the Barracuda SSL VPN.

Figure 2.2: Sample layout for DMZ Deployment


Clients Inside Organization
Internet
External Firewall
Barracuda SSL VPN
Internal Firewall
Resource Files / Intranet Web Sites

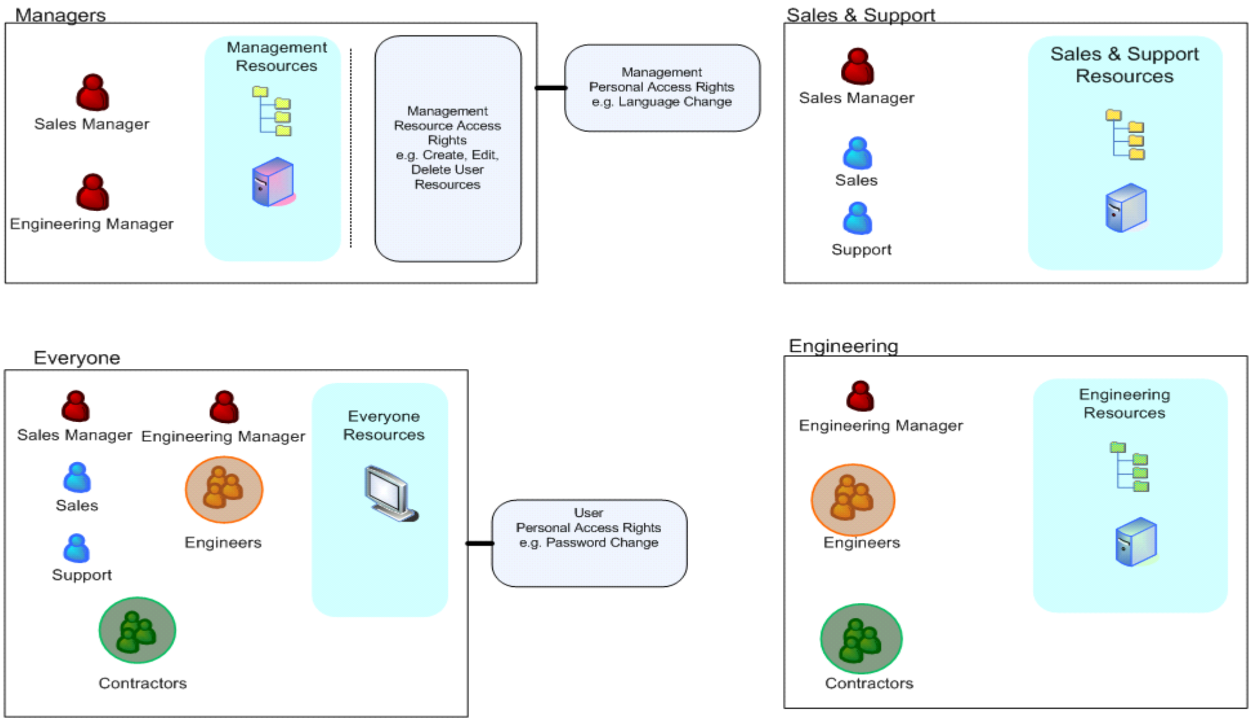
SSL VPN Concepts

Security Policy and Resource Management

The Barracuda SSL VPN provides granular access control to resources; for example, a company has a number of different departments, Engineering, Sales & Support, and each department has a manager. The company allows employees to work from home and as a result, each department requires secure access to relevant shared areas and resources on the company network. In addition, the managers have a level of responsibility which requires access to planning information and personal details for their department. Each manager is also required to act as an administrator for their own department. All employees have access to email and the company intranet.

To control use access levels to company resources such as web applications and files systems, you group employees differently. The following diagram shows how you can organize employees. Each of the following groups, *Managers, Sales & Support, Engineering, Everyone* are policies. A policy can consist of individual users or groups of users known as accounts and groups, respectively. The policy is a single entity and any conditions applicable to a policy apply equally to all accounts and groups within that policy. Accounts and groups are referred to as Principals. An account or group can be in more than one policy.

Each policy is attach to the required resources, granting policy members access to them. The *Everyone* Policy is a built-in, already available policy which has been created to allow an efficient way to allocate resources to all users; in this example, email and intranet access. All members of the *Engineering* Policy have access to specific engineering system resources; all members of the *Sales & Support* Policy have access to their own specific system resources.



The Engineering and Sales Managers are also members of the *Managers* policy and this allows them to access the planning and personal details information which is restricted to management personnel.

The configuration of resources and policies is flexible: it is possible for multiple resources to be assigned the same policy and also for multiple policies to be assigned to a single resource.

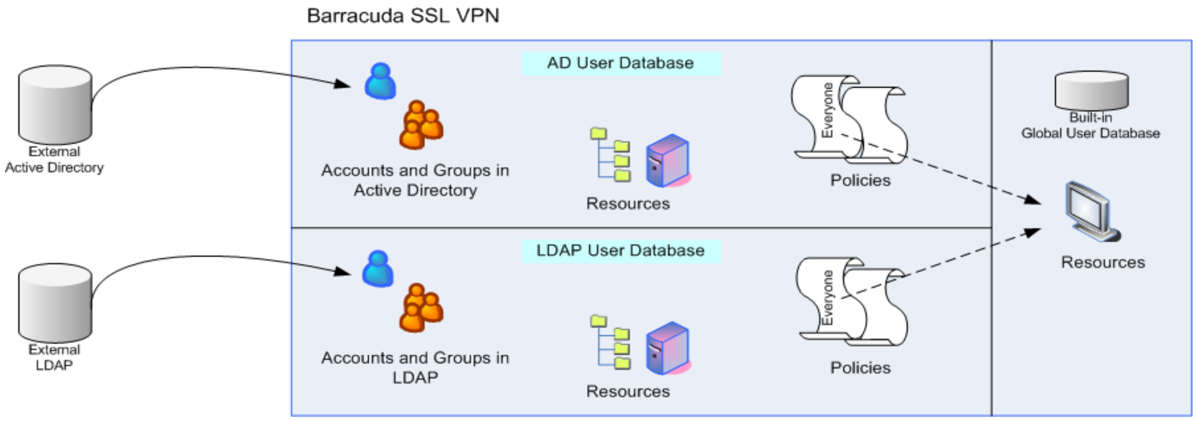
By default the *Everyone* Policy gives all users certain administrative controls such as the ability to change their password; this is achieved through the use of access rights. Access rights are attached to a policy and specify administration-type privileges. The *Managers* Policy has resource access rights attached which would allow managers to perform create, edit and delete actions, for example. This enables managers to perform administrative tasks by making certain resources available to their team. In the example, members of the *Sales & Support* and *Engineering* policies are able to use the resources made available to them but have no administrative control.

Organizational Control

The Barracuda SSL VPN has three internal preconfigured User Databases of type Built-in. These are Default, Super User and Global. The main system administrator is identified as the Super User who would delegate responsibility by creating administrative Accounts and Groups, with the necessary access rights, typically within the Default User Database.

In many cases it is likely that a repository of user information exists already, e.g. Active Directory or LDAP. Within the Barracuda SSL VPN you can create a user database to an existing repository and then use the Accounts and Groups defined within it when creating and assigning Resources and Policies. Resources and policies are only accessible to the Accounts and Groups within the same user database.

The Global User Database is the exception to this rule; policies across all user databases are visible to Global and so resources created in Global can have any policy assigned. This is an efficient way to make resources available to all users where a number of user databases exist; the diagram below shows how the *Everyone* policies from two user databases (AD and LDAP) are used to achieve this.



Chapter 3

Getting Started

The steps to installing your Barracuda SSL VPN into your network are as follows:

- The physical installation and accompanying network configurations that must be done to integrate the physical hardware into your corporate network.
- The configuration of the Barracuda SSL VPN itself, which is performed over two separate web interfaces: the **Administrative interface**, for system-related items, and the **Management interface**, for the Barracuda SSL VPN use and functionality.
- Fine tune both the Administrative and Management configurations, to customize both for your specific environment.

Initial Setup

These are the general steps to installing and integrating the Barracuda SSL VPN into your network. For more detailed instructions for each step, see the following reference pages.

Prepare for the Installation

Before installing your Barracuda SSL VPN, complete the following tasks:

1. Determine which type of deployment is most suitable to your network. For more information on the deployment options, see *Barracuda SSL VPN Configurations* on page 15.
2. Verify that you have the necessary equipment:
   - Barracuda SSL VPN (check that you have received the correct model)
   - AC power cord
   - Ethernet cables
   - VGA monitor (recommended)
   - PS2 keyboard (recommended)

Connect Barracuda SSL VPN to Network

1. Fasten the Barracuda SSL VPN to a standard 19-inch rack or other stable location.
2. Connect a CAT5 or a CAT6 Ethernet cable from your network switch to the ethernet port on the **back** of the Barracuda SSL VPN.
3. Connect the following to your Barracuda SSL VPN:
   - Power cord. AC input voltage range is 100-200 volts at 50/60 Hz.
   - VGA monitor
   - PS2 keyboard

   After you connect the AC power cord, you may hear the fan operate for a few seconds and then power off. This behavior is normal.
4. Press the **Power** button located on the front of the unit.

   The login prompt for the administrative console displays on the monitor, and the power light on the front of the Barracuda SSL VPN turns on. For a description of each indicator light, refer to *Understanding the Indicator Lights* on page 103.

Configure IP Address and Network Settings

The Barracuda SSL VPN is assigned a default IP address of **192.168.200.200**.

To set a new IP address from the administrative console:

1. Connect your keyboard and monitor directly to the Barracuda SSL VPN.
2. At the **barracuda login** prompt, enter **admin** for the login and **admin** for the password.

   The **User Confirmation Requested** window displays the current IP configuration of the Barracuda SSL VPN.
3. Using your **Tab** key, select **Change** and press **Enter** to change the IP configuration.
4. Enter the new IP address, netmask, and default gateway for your Barracuda SSL VPN. Select **Save** to enter your changes. (The Primary and Secondary DNS fields are optional at this time, but if not entered at this step then they must be entered in step 3b of *Configure Administrative Settings* on page 24). Select **Exit**.

   The new IP address and network settings are applied to your Barracuda SSL VPN.

Configure Your Corporate Firewall

If your Barracuda SSL VPN is located behind a corporate firewall, refer to *Table 3.1* for the ports that you need open on your corporate firewall to allow communication between the Barracuda SSL VPN, your email server, and the Internet. Port 25 is the default port used for SMTP traffic.

Table 3.1: Ports to Open on Your Corporate Firewall

Port	Direction	Protocol	Description
22	Out	TCP	Remote diagnostics and technical support services
25 (optional)	In/Out	TCP	Email notifications and alerts, including initial password notifications. See notes on the next page.
53	Out	TCP/UDP	DNS (Domain Name Server)
80	Out	TCP	Firmware and Energize Updates (unless configured to use a proxy)
123	Out	UDP	NTP (Network Time Protocol)
389	Out	TCP	Required only if Active Directory/LDAP read access is to be allowed.
443	In/Out	TCP	HTTPS/SSL port for SSL VPN access. See *Enabling SSL for Administrators and Users* on page 31
500	In/Out	UDP	Required only if L2TP/IPsec access is to be allowed.
636	Out	TCP	Required only if Active Directory/LDAP read/write access is to be allowed.
1723	In/Out	TCP	Required only if PPTP access is to be allowed. See note below.
4500	In/Out	UDP	Required only if L2TP/IPsec access is to be allowed.
8000	In/Out	TCP	Appliance administrator interface port (HTTP). See note below, and step 4c of *Controlling Access to the Administration Interface* on page 30.
8443	In/Out	TCP	Appliance administrator interface port (HTTPS). See note below, and step 4c of *Controlling Access to the Administration Interface* on page 30.

Note

The GRE (IP protocol 47) In/Out direction must be allowed for PPTP to function.

The Appliance Administrator interface ports on 8000/8443 should only be opened if you manage the appliance from the Internet.

Some organizations choose to have email notifications and alerts from the Barracuda SSL VPN sent to an external email address directly or by using an external Smart Host, without relaying through the corporate mail server. In these situations, the corporate firewall will have to be configured to allow outgoing emails from the Barracuda SSL VPN over the desired SMTP port.

The Barracuda SSL VPN should not usually be accepting incoming SMTP requests from systems outside of your organization's network. However, if your email server is located in a DMZ, you may need to configure your corporate firewall to allow incoming traffic over the designated SMTP port from your email server to the Barracuda SSL VPN.

The ports specified as the administration interface ports (8000/8443 or any other ports you choose) must be configured on your corporate firewall to allow traffic to the Barracuda SSL VPN only if you want to allow administration of the Barracuda SSL VPN from the Internet.

Configure Administrative Settings

After specifying the IP address of the Barracuda SSL VPN and opening the necessary ports on your corporate firewall, configure the Barracuda SSL VPN from the web administration interface. Make sure the system being used to access the web interface is connected to the same network as the Barracuda SSL VPN, and that the appropriate routing is in place to allow connection to the Barracuda SSL VPN's IP address via a web browser.

To configure administrative settings on the Barracuda SSL VPN:

1. From a web browser, enter **http://** followed by the IP address of the Barracuda SSL VPN, followed by the default web Interface HTTP port `:8000`.

   For example: `http://192.168.200.200:8000.`

2. Log into the administration interface, using **admin** for both the username and the password.
3. Navigate to the **BASIC > IP Configuration** page and perform the following steps:

   3a. In the TCP/IP Configuration section, verify the IP address, netmask, and default gateway for your Barracuda SSL VPN (entered in step 4 of *Configure IP Address and Network Settings* on page 21).

   3b. Enter the IP address of your primary and secondary DNS servers (if these have not yet been set up).

   3c. Enter the default hostname and default domain name of the Barracuda SSL VPN.

   3d. Click **Save Changes**.

Note

Whenever the IP address of your Barracuda SSL VPN on the **IP Configuration** page is changed, you are disconnected from the administration interface. Please log in again using the new IP address.

4. Navigate to the **BASIC > Administration** page and perform the following steps:

   4a. Assign a new administration password to the Barracuda SSL VPN. This is an optional step that is highly recommended for your own security and protection.

   4b. Make sure the local time zone is set correctly.

   Time on the Barracuda SSL VPN is automatically updated via NTP (Network Time Protocol). It requires that port 123 is opened for outbound UDP (User Datagram Protocol) traffic on your firewall (if the Barracuda SSL VPN is located behind one).

   The time zone must beset correctly because this information is used to determine the integrity of the message archive and in all logs and reports.

   4c. If desired, change the port number used to access the ***administration*** interface of the Barracuda SSL VPN. The default ports are 8000 (for HTTP) and 8443 (for HTTPS). Note that this is for the web interface that you are currently accessing, and *not* for the web interface and data ports that your users will use. For more information regarding the **admin** account, see *The admin user* on page 28.

   4d. If desired, change the port numbers that ***your users*** will use to access the Barracuda SSL VPN. The default ports are 80 for HTTP, and 443 for HTTPS. These are the ports for both accessing the web interface as well as transmitting all secured traffic. These will also be the ports over which the *ssladmin* account will log in for configuring SSL VPN user access and usage policies, on the SSL VPN Management Interface. For more information regarding the *ssladmin* account, see *The ssladmin user* on page 28.

   4e. Enter the amount of time for the session expiration length (in minutes) of your web administration interface session. At expiration, you are required to log back into the administration interface.

4f. Enter the email addresses for your Administrator to receive system alerts and notifications, and other urgent communications from Barracuda Networks.

4g. (Optional) Specify your local SMTP server in the Outbound SMTP Host/Smart Host field.

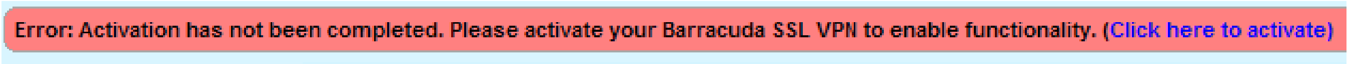
4h. Click **Save Changes**.

Activate Your Subscriptions

After installation, your Energize Updates and other optional subscriptions must be activated for the Barracuda SSL VPN to be fully enabled, and continue to receive the latest updates to all virus, policy, and document definitions from Barracuda Central. The Energize Updates service is responsible for downloading these updates to your Barracuda SSL VPN.

To activate your subscription status:

1. At the top of every page, you may see the following warning:



Error: Activation has not been completed. Please activate your Barracuda SSL VPN to enable functionality. (Click here to activate)

2. Click on the designated link to open up the **Product Activation** page in a new browser window.
3. On the **Product Activation** page, fill in the required fields and click **Activate**. A confirmation page opens to display the terms of your subscription.

   3a. If your Barracuda SSL VPN is not able to communicate directly to Barracuda Central servers, then an Activation Code will be displayed as well which you will need to enter in the next step.

4. Return to the Barracuda SSL VPN administration interface and navigate to the **BASIC > Status** page. In the **Subscription Status** section, verify that the word *Current* appears next to **Energize Updates**, **Instant Replacement Service** (if purchased), and **Premium Support** (if purchased).

   4a. If you had received an Activation Code above then there will also be an **Activation Code** area in this section, where you must first enter that **Code** and click **Save** to activate your Barracuda SSL VPN.

5. There may be a slight delay of a few minutes for the display to reflect your updated subscription status. If the status is still showing as unactivated, click **Refresh** in the **Subscription Status** section.

Note

If your subscription status does not change to *Current* within an hour, or if you have trouble filling out the **Product Activation** page, call your Barracuda Networks sales representative.

Update the Barracuda SSL VPN Firmware

To update the firmware on the Barracuda SSL VPN:

1. Navigate to the **ADVANCED > Firmware Update** page. Verify that the installed version matches the latest general release. The **Download Now** button next to the latest general release is disabled if the Barracuda SSL VPN is already up-to-date with the latest firmware.
2. *If the installed version does not match the latest general release*: read the release notes to learn about the latest features and fixes provided in the new firmware version, and click **Download Now** to begin the download. Updating the firmware may take several minutes. Do not turn off the unit during this process.

   You can view the download status by clicking the **Refresh** button next to the firmware download progress. A **Firmware downloaded** message displays once the download is complete, and the **Refresh** button will turn into **Apply Now**.
3. Click the **Apply Now** button when the download completes.
4. Click **OK** when prompted to reboot the Barracuda SSL VPN.

   A **Status** page displays the progress of the reboot. Once the reboot is complete, the login page appears.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Select **ADVANCED > Energize Updates**.
2. Select *On* for **Automatically Update**. The recommended setting is *On* for all available definitions.
3. Check to see if the current version is the same as the latest general release. If the rules are up-to-date, proceed to the next section. If the rules are not up-to-date, continue to the next step.
4. Click **Update** to download and install the latest available definitions onto the Barracuda SSL VPN.

Route Incoming Connections to the Barracuda SSL VPN

To use the features of the Barracuda SSL VPN, you must route HTTPS incoming connections on port 443 to the Barracuda. This is typically done by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN:

Note

The Appliance Administrator web interface ports on 8000/8443 will also need similar port forward configurations if you intend to manage the appliance from outside the corporate network.

Completing Configuration of the Barracuda SSL VPN

Once the Barracuda SSL VPN has been integrated into your corporate network, you will need to complete two sets of configurations, each done by a different administration account from a different web interface. The minimum required Administrative configurations would have already been done as a part of integrating the Barracuda SSL VPN into your network, but there are a few additional steps that are highly recommended. The SSL VPN Management configurations; however, will need to be done for any users to access your protected resources.

To complete the SSL VPN Management configurations:

1. Log in as the *ssladmin* user to the SSL VPN Management interface (port 80, or as otherwise specified in Step 4d of *Configure Administrative Settings* on page 24).
2. From the **ACCESS CONTROL > User Databases** page, configure one or more user databases from which all user and group information will be retrieved.
3. From the **ACCESS CONTROL > Policies** page, configure one or more Policies, to define which users and groups are to have the same access privileges. You can also choose to use the *Everyone* policy, which automatically includes all users with authorized access to the Barracuda SSL VPN.
4. From the **ACCESS CONTROL > Resources** page, configure one or more network resources that are to be made available to remote users.

Optional Administrative configurations:

1. Log in as the **admin** user to the Administrative interface (port 8000, or as otherwise specified in Step 4c of *Configure Administrative Settings* on page 24).
2. Install an SSL certificate.

The Barracuda SSL VPN Administrator Accounts

Once the Barracuda SSL VPN has been integrated into your corporate network, you will need to complete two sets of configurations, each done by a different administration account from a different web interface. The two administration accounts are:

- **admin:** For appliance administration and maintenance of the Barracuda SSL VPN. This account is what you would use to log into the Administration interface (typically at port 8000 or 8443), for performing actions like network configurations and firmware updates, and is what was used for everything in this chapter so far.

- **ssladmin:** For configuring usage and deployment of the Barracuda SSL VPN. This account is used to log into the usage and configuration (SSL VPN Management) interface (typically at port 80 or 443), for performing actions like managing access policies and user account maintenance.

The *admin* user

The **admin** account is the only one that is allowed to log into the Administration interface of the Barracuda SSL VPN, located by default at port 8000/8443. Also called the “appliance administrator”, this is the account that configures all settings related to the placement of the Barracuda SSL VPN hardware into your organization’s network, and which performs hardware maintenance tasks such as firmware updates, configuration backups and restores, and other troubleshooting. Access to this interface can be restricted to specific IP addresses by changing the **Administrator IP/Range** as described on Step 4c of *Configure Administrative Settings* on page 24. The password for this account can be changed on the **BASIC > Administration** page.

The *ssladmin* user

The *ssladmin* account is used to log in from the users’ web interface of the Barracuda SSL VPN, located by default at port 80/443. This “SSL VPN administrator” account manages all user access to the Barracuda SSL VPN, and defines all other usage parameters such as network and resource availability, user controls and IP address limitations.

There are two modes, or interfaces, available for *ssladmin*, one for managing VPN access (**Manage System** mode) and one for managing the account itself (**Manage Account** mode). The system management mode is what *ssladmin* will always be in when logging in. To switch between the two modes, click on the **Manage...** link in the upper right corner of the web interface. The link identifies the mode that you will switch into when clicked. Unless otherwise specified, the commands and directions listed must be done when in the **Manage System** mode, which means that the **Manage Account** link will be displayed.

To change the password for this account, click on the **Manage Account** link to get to the Account interface, and navigate to the **MY ACCOUNT > Change Password** page. If you have forgotten the password for this account and are not able to log in at all, the default password can be restored by the **admin** user from the appliance administration interface, on the **BASIC > Administration** page.

Chapter 4
Configuration Settings

This chapter outlines the various options available for configuration from both the Administrative and SSL VPN Management interfaces:

Administrative Settings

This section covers configuration of the administrative settings for your Barracuda SSL VPN, to customize it for your specific environment: All of the following are performed by the **admin** account from the Administration Interface as defined in Step 4c of *Configure Administrative Settings* on page 24.

Controlling Access to the Administration Interface

The **BASIC > Administration** page is where to perform the following tasks to accessing the web interface for the Barracuda SSL VPN:

- Change the password of the appliance administration account **admin**.
- Reset the password of the *ssladmin* account (used to configure VPN usage).
- Change the ports that the **admin** account will use to access the *administrative* web interface for the Barracuda SSL VPN over the web (default ports are 8000 and 8443).
- Change the port used by your users and the *ssladmin* account to access the Barracuda SSL VPN (default ports are 80 and 443).
- Change the length of time after which idle web interface connections will be terminated (the default is 20 minutes).
- Specify the IP addresses or netmask of the systems that can access the web administration interface. Attempts to log in as **admin** from other systems will be denied.
- Specify the IP addresses or netmask of the systems that can communicate with the Barracuda SSL VPN through SNMP (available on models 480 and higher).

Setting the Time Zone of the System

You set the time zone of your Barracuda SSL VPN from the **BASIC > Administration** page. The current time on the system is automatically updated via Network Time Protocol (NTP). When the Barracuda SSL VPN resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic.

It is important that the time zone is set correctly because this information is used in all logs and reports.

Note: The Barracuda SSL VPN automatically reboots when you change the time zone.

Customizing the Appearance of the Web Interface

The **ADVANCED > Appearance** page allows you to customize the default images used on the web interface. This tab is only displayed on the Barracuda SSL VPN 680 and above.

Enabling SSL for Administrators and Users

The **BASIC > Administration** page allows you to modify various settings related to SSL (HTTPS) access to the web interface for your Barracuda SSL VPN. SSL certificates are configured and uploaded from the **BASIC > SSL Certificate** page

SSL ensures that your passwords are encrypted and that all data is transmitted to and received from the administration interface is encrypted. All Barracuda SSL VPNs support SSL access without any additional configuring. However, some sites may wish to enforce using a secured connection to access the web interface, or prefer to use their own trusted certificates.

Note

The SSL configuration referred to here is related only for the web-based administrative interface. There is no need to explicitly configure SSL for traffic between the Barracuda SSL VPN and your email servers.

To Enforce SSL-only Access:

1. Navigate to the **BASIC > Administration** page. The **Appliance Web Interface** section should already have the web Interface HTTP Port and the web Interface HTTPS/SSL Port that you have configured in entered in step 4c of *Configure Administrative Settings* on page 24).
2. Set the **HTTPS/SSL Access Only** field to *Yes*. Setting this to *No* will still allow the Barracuda SSL VPN to accept non-SSL connections.
3. Click **Save Changes** to save and activate your changes.

If you want to change the certificate that is used, you must first create and upload it on the **BASIC > SSL Certificate** page, then change the *Certificate Type* in the **SSL Certificate Configuration** section. The Barracuda SSL VPN supports the following types of certificates:

- **Default (Barracuda Networks)** certificates are signed by Barracuda Networks. On some browsers, these may generate some benign warnings which can be safely ignored. No additional configuration is required to use these certificates, and are provided free of charge as the default type of certificate.
- **Private (self-signed)** certificates provide strong encryption without the cost of purchasing a certificate from a trusted Certificate Authority (CA). These certificates are created by providing the information requested in the **Certificate Generation** section of the **BASIC > SSL Certificate** page. You might also want to download the private root certificate and import it into your browser, to allow it to verify the authenticity of the certificate and prevent any warnings that may appear when accessing the web interface.
- **Trusted (signed by a trusted CA)** certificates are issued by trusted Certificate Authorities (CA), and must be purchased from them separately with a Certificate Signing Request (CSR). This can be downloaded after providing the information requested in the **Certificate Generation** section of the **BASIC > SSL Certificate** page. Once you have received the certificate and key from the CA, you must upload both items to the Barracuda SSL VPN from the **Trusted Certificate** section of that same page. The certificate will be in effect as soon as the upload is completed.

SSL VPN Settings

The SSL VPN Management Interface is the main point of interaction between the administrators of the system and the system itself. All of the following are managed by the *ssladmin* account while logged into the Administration interface as defined in Step 4d of *Configure Administrative Settings* on page 24.

User Databases

The **ACCESS CONTROL > User Databases** page identifies where all of your user account information is stored. You can choose to create local user accounts that are stored in a local database, or you can import and synchronize with your existing directory service. The Barracuda SSL VPN currently supports interactions with:

- Active Directory
- LDAP
- NIS
- OpenLDAP

The Barracuda SSL VPN also comes with a built-in user database into which you should place any manually-created user account.

User Accounts

For a user to use the Barracuda SSL VPN, they must either have an account in a user directory that has been imported onto the Barracuda SSL VPN, or have access to a resident account that was created explicitly for them on the Barracuda SSL VPN. Management of all user accounts are done by the *ssladmin* account from the Barracuda SSL VPN interface, on the **ACCESS CONTROL > User Databases** page.

Groups

There are two types of user groups on the Barracuda SSL VPN:

- **Imported Groups:** The groups as defined on your user authentication server, such as LDAP or NIS. These groups can be imported into the Barracuda SSL VPN by the *ssladmin* account from the Barracuda SSL VPN interface, on the **ACCESS CONTROL > User Databases** page.

- **Local Groups:** A custom group for use only on the Barracuda SSL VPN, consisting of local users, imported users or imported groups. These groups are defined by the *ssladmin* account from the Barracuda SSL VPN interface, on the **ACCESS CONTROL > User Databases** page, but once created they are treated just the same as any group that was imported from an external user authentication server. Local groups are used only when a *Built-In User Database* (page 64) is used.

Once these groups have been either imported or created on the Barracuda SSL VPN, they are treated identically. Authentication for each member in the group will be made according to the type of group they are in: locally for members of a local group and via communications with the appropriate authentication server for members of an imported group.

Policies

A policy is a combination of users and groups that all have the same access privileges to a specific collection of network resources. Policy membership is determined by the *ssladmin* account from the Barracuda SSL VPN interface, on the **ACCESS CONTROL > Policies** page, and are applied, or attached, to a specific resource from on the **RESOURCES** tab, on the page for that particular type of Resource.

A user or group can belong to multiple policies, each policy can be applied to more than one network resources, and each network resource can have multiple policies attached to it. However, only policies can be attached to a network resource. Any user that is to be granted access to any resource must be in a policy, even if that user is the only entity in that policy.

The built-in *Everyone* policy automatically includes all users who are allowed access to the Barracuda SSL VPN.

Resources

To make a resource available to your remote users, you must defined it on the Barracuda SSL VPN and have at least one policy attached to it to determine who is allowed to access the resource, and to what extent. For detailed information about each resource type, see *Resources* on page 46.

Resource Types

Resources that are on your network available can fall into one of the following categories, all of which are available from the **RESOURCES** tab:

- **Web Forwards** (*page 47*): Sites accessed through HTTP such as intranet wikis or a restricted-access mail server.
- **Network Places** (*page 51*): Locations reached by going to a specific (internal) IP address or system name, such as a Windows or UNIX file share, web folders or a networked printer.
- **Applications** (*page 53*): Programs or utilities that are require access by a client to a server, such as an RDP connection to a desktop system.
- **SSL Tunnels** (*page 54*): Systems that require connection to a port or application not defined as an Application, such as a Microsoft Terminal Server or a VMWare Server.
- **Profiles** (*page 56*): An individual user's identify on the network, containing configuration information related to the Barracuda SSL VPN Agent such as timeouts and local proxy settings.

If there are other resources that do not fall into any of the above, or if you wish to give a user unrestricted access to your internal network, you can choose to make the **Barracuda Network Connector** (*page 37*) available to them as well. This will allow the remote systems to act as if they are plugged directly into the internal network, and will have complete access to anything that the connecting user's individual authentication allows.

Policies and Resources

Once a resource has been defined, access to it must be granted by attaching a policy consisting of the authorized users and groups. More than one policy can be attached to any resource, and each Policy may be applied to many different resources. However, because only policies can be attached to resources, any user to whom you want to allow access **must** be in at least one of the attached Policies, or in a group that is a member of an attached policy.

Network Access Control

The **ACCESS CONTROL > NAC** page allows you to limit access to network resources based not just by users, but also on a variety of other factors such as the time of day, the connecting system's OS (operating system) and browser, and even whether or not any anti-virus software is running on the remote system. Exceptions to these limitations may be entered on the **ACCESS CONTROL > NAC Exceptions** page.

Access Rights

The *ssladmin* account can designate other users and groups to manage specific aspects of the Barracuda SSL VPN. To grant any policy the rights to manage a particular resource, system or their own personal configuration, navigate to the **ACCESS CONTROL > Access Rights** page and choose the specific rights to grant. See also the *Access Rights* section on page 63 for more details.

Additional Configuration Items

In addition to the configuration settings that are entered directly onto the Barracuda SSL VPN, there are a few additional steps that may wish to take, to allow easier access and maintenance:

Recommendations:

1. Register a hostname with your DNS server for the Barracuda SSL VPN; for example: `sslvpn.company.com`
2. Install an SSL certificate on the Barracuda SSL VPN for this hostname to ensure your users are able to determine that they are connecting to a genuine Barracuda SSL VPN that is registered to your organization.
3. Integrate the Barracuda SSL VPN with your existing user database. To cleanly integrate with your environment, the Barracuda can read in user accounts and authenticate against a number of different databases, including Microsoft Active Directory.
4. If your network uses a DMZ, you may wish to configure the Barracuda SSL VPN in this topology for greater security.

Chapter 5

Barracuda Network Connector

Resources are the key entities that a user of the system will interact with. The following topics are covered in this chapter:

Overview of Barracuda Network Connector

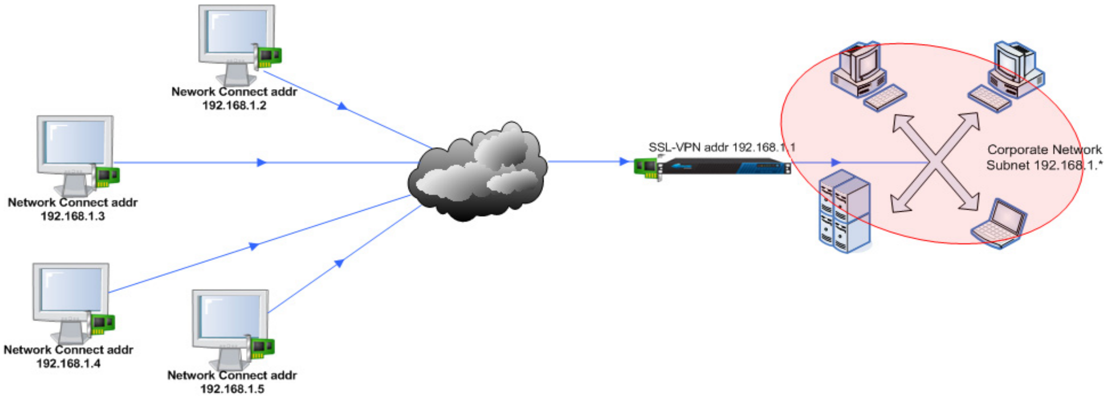
The Barracuda Network Connector provides users with full network connectivity allowing them to upload download files and mount drives as if they were on the local network. It works on Linux, Macintosh, and Microsoft Windows 2000, XP, 2003 and Vista operating systems.

This feature provides an OSI Layer 2 or 3 secure network extension, providing an easy-to-configure network interface with minimal maintenance overheads. With the Barracuda Network Connector installed, you can deploy full TCP/UDP protocol access to your SSL VPN users. It is designed to directly replace an IPsec VPN client and provides identical functionality without the associated firewall configuration issues of IPsec VPNs.

The Barracuda Network Connector provides full network connectivity to the connecting client. Users can access their organization's network and can remotely perform all of the standard functions such as adding new drives or moving files as if they were connected sitting in their office. Once installed, an administrator can configure any number of virtual network interfaces on the server and grant full network access to those users that require it.

The Barracuda Network Connector consists of two components: the server-side component which opens up server interfaces and the client-side component which connects to these interfaces. It is through these connections that data is transmitted and received between both parties.

The diagram below shows how the Barracuda Network Connector creates a tunnel between two endpoints.



Each separate network continues to function independently within its own subnet. Every connecting (remote) client has two network addresses: its standard Internet IP address, and a Network Connector IP address which will be from the same range as that used by the Barracuda SSL VPN server. In the above example, the `192.168.1.*` subnet. The Barracuda Network Connector client determines which network to use based on route settings that are published (sent) to the client from the Barracuda SSL VPN server. Requests to the corporate LAN connect with the Network Connector IP address through the server into the protected network, and connection requests to the Internet are left alone to continue connecting and functioning through the standard Internet IP address, without going through the Barracuda SSL VPN.

The Network Connector is not a clientless solution like the Barracuda SSL VPN Agent since it installs network virtual devices on each client's operating system. However all configuration data is maintained on the server so any changes to these are pushed down to client when it connects. Once installed, its operation is transparent to the user.

The Barracuda Network Connector is useful in the following types of situations, where you want to allow unrestricted access to the internal network.

- **Road Warrior**: One of the more common requirements of a VPN solution is to provide connectivity to employees out in the field. These users may want access to the organization's LAN to upload files, read email, and use client/server applications across the WAN.
- **Network Administrator**: Network administrators generally require unrestricted access to their corporate network as a nature of their job.

System Requirements

The Barracuda Network Connector can be installed on the following systems:

- Microsoft Windows 7, 2000, XP, Vista
- Linux 2.4 or higher with integrated TUN/TAP driver
- Macintosh 9.x, 10.x (Intel-based)

Note Requires Administrative Account to Install Service

In order to install and run the Barracuda Network Connector service on your client machines, you will require the use of an account with administrative permissions in Windows. Once the service is installed, a regular user can launch Network Connector configurations from Windows system tray.

Note If you are running Windows Vista

The Barracuda Network Connector client will request authorization using a UAC prompt. However, the dialog window may not always appear on top. If you do not see any new dialogs and the installation appears to have stalled, check the taskbar for the presence of a new dialog.

Network Connector Interface

The Barracuda Network Connector interface can be accessed from the **RESOURCES > Network Connector** page of the SSL VPN Management interface.

Connecting a Client to the Barracuda SSL VPN

The Barracuda Network Connector can be installed on the following systems:

- Microsoft Windows 7, 2000, XP, Vista
- Linux
- Macintosh

Client Configurations

To allow clients to connect successfully using the Barracuda Network Connector, create at least one client configuration so that some required initialization steps can be performed automatically upon connection.

To create a default Client Configuration:

1. Navigate to the **RESOURCES > Network Connector** page of the SSL VPN Management interface and click the **Configure Network** button.
2. In the **Create Client Configuration** that appears, enter the IP address range that should be used for remote systems.
3. From the **Available Policies** section, select the policy or policies that will be allowed remote access, and click **Add**.
4. Click **Save** to create the default configuration with the entered settings and return to the **Network Connector** page.

Up and Down Commands

You might also need to define some initialization commands that are run when a client connects to the Barracuda SSL VPN and closing commands when the client disconnects. These are called the Up Commands and the Down Commands, and must be added into the configuration. The commands you use are based on the operating system of the connecting system, so if you will have remote users running on more than one platform, you might want to create multiple configurations.

To add Up and Down Commands:

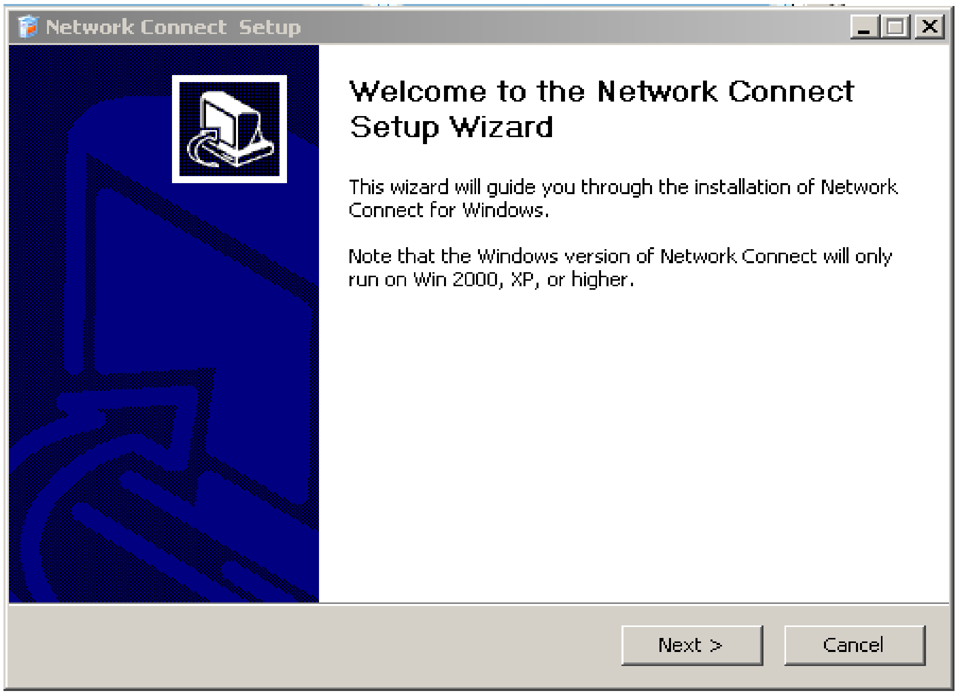
1. Navigate to the **RESOURCES > Network Connector** page of the SSL VPN Management interface and click on the **Edit** link for one of the configurations in the **Client Configurations** section at the bottom.
2. In the **Edit Client Configuration** window that appears, locate the **Commands** section.
3. In the **Up Commands** box, enter the initialization commands that should be executed on any client that is connecting to the Barracuda SSL VPN. An example of the types of commands that should be entered here are `route add` commands for Windows clients (so that the connecting system will know how to route to other systems in the network).
4. In the **Down Commands** box, enter the initialization commands that should be executed on a client before it completely disconnects to the Barracuda SSL VPN. For example. if you had added any routes in the **Up** command, then you will want to remove those in the **Down** Command.
5. Click **Save**.

Client Downloads and Installs

When a user has been authorized through a policy to use the Barracuda Network Connector, that user will see a **Network Connector** page on their **RESOURCES** page. From there, the client for the desired operating system can be downloaded.

Microsoft Windows

1. Navigate to the **RESOURCES > Network Connector** page and click the **Download Windows Client** button.
2. Once the installation package downloads, launch the installer. You'll be presented with a setup screen.

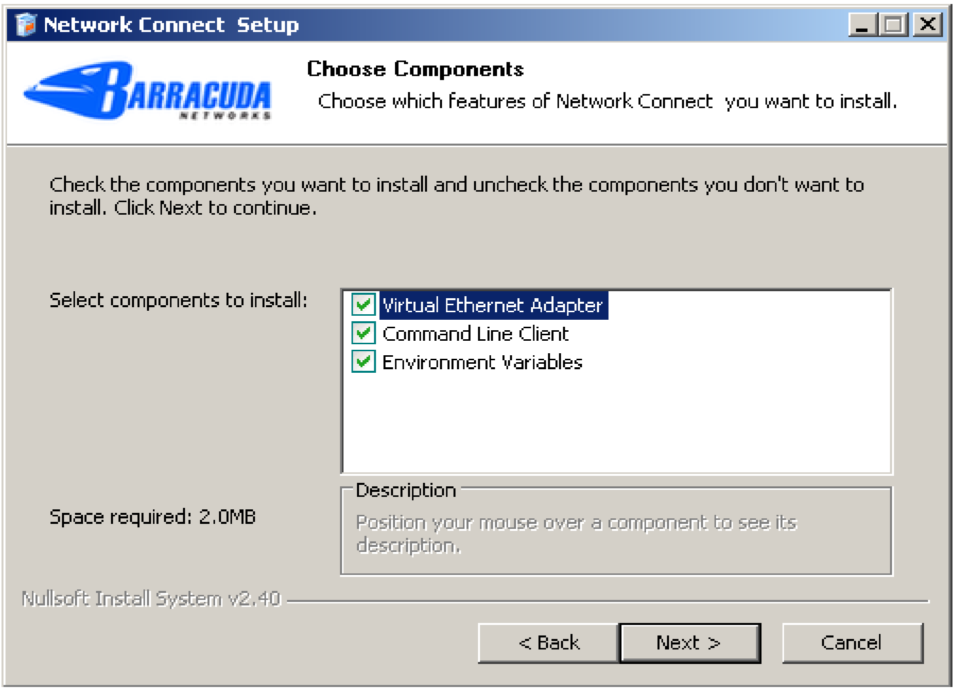


Welcome to the Network Connect Setup Wizard

This wizard will guide you through the installation of Network Connect for Windows.

Note that the Windows version of Network Connect will only run on Win 2000, XP, or higher.

3. Select the default settings as you continue through the installation.



Network Connect Setup

Choose Components

Choose which features of Network Connect you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Virtual Ethernet Adapter
- ☑ Command Line Client
- ☑ Environment Variables

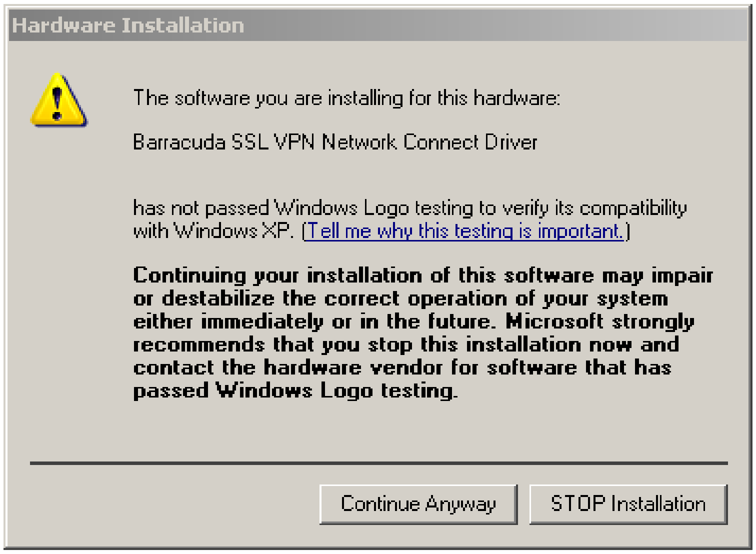
Space required: 2.0MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.40

4. On Windows XP and later, you may receive a compatibility warning which will be safe to ignore. If you get this dialog, click **Continue Anyway**.



Hardware Installation

The software you are installing for this hardware:

Barracuda SSL VPN Network Connect Driver

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

5. Once it is installed, return to the **RESOURCES > Network Connector** page of the SSL VPN Management interface. Click the **More…** link under **Actions**, and select **Launch Network Connect Client**.

6. This will start the client, and in the taskbar the TAP driver icon will appear.

When the Network Connector attempts to establish a connection the icon will flash briefly. Once a connection to the server has been established the icon will stop flashing indicating the connection has been established. The new Network Connector network will be available to use. From Windows Explorer you should now be able to access the drives of those machines on the Network Connector network.

Note **Routes are not immediately published on Microsoft Windows systems**

Due to restrictions imposed by Windows networking, the VPN routes are not immediately published when the Network Connector is launched. Expect to wait around 10-15 seconds after launching the client before the routes are published and the Network Connector client is fully usable.

Linux

1. Navigate to the **RESOURCES > Network Connector** page and click the **Download Linux Client** button.

   Unlike the Windows client, the Linux client package only contains a command line version of the Network Connector client. No virtual Ethernet adapter needs to be installed as a tap driver already exists on most Linux distributions.

   If launching Network Connector from the SSL VPN web-based interface only, there is no need to download the Linux client at all.
2. The Linux client must be run as root. So if launching from the command line either login as root, or 'su' from another account:

```
$ su root
Password: <root password>
#
```

3. Run the client:

```
# /path/to/nEXTclient [options ...]
```

4. Some Linux distributions use the `sudo` command, notably `Ubuntu`. So, if logged on as a normal user, run:

```
$ sudo /path/to/nEXTclient [options ...]
Password: <your password>
```

5. Launching the client from the web interface currently requires that the user is running the GNOME Desktop and has the `gksudo` command installed. Support for other desktops may be added.
6. After the client has been downloaded, the user will be presented with the password prompt: **Enter your password to perform administrative tasks**. After entering the password the client will start.
7. To stop the client, either logout of the web interface, or run the command:

```
$ killall nEXTclient
```

Macintosh

To get the Mac client working, configure the Up commands and Down commands, tailored to your network. You will need to know the IP address of the DNS server and the DNS search suffix.

1. Navigate to the **RESOURCES > Network Connector** page and click the **Download Mac Client** button.
2. Once installed, launch the program from the finder which will then run with a gray network icon at the top right of the screen. Click the icon, select **Preferences**, and enter the details for the SSL VPN server. For the **Client Configuration** field, enter the exact name of the Network Connector client that was created above.
3. To connect, simply click the icon and select connect. The icon should turn green when the connection is established.

Chapter 6

Resources

Resources are the key entities that a user of the system will interact with. The following topics are covered in this chapter:

Resources

All interactions with your secured network by a remote user fall into the following general types of access, called Resources on the Barracuda SSL VPN:

- **Web Forwards -** Using a web browser to interact with sites on the intranet
- **Network Places -** Accessing a network share or file system on the internal network
- **Applications -** Deploying and running applications which must be run locally, or "on site"
- **SSL Tunnels -** Creating a secured 1-to-1 connection to a specific system on the internal network, such as for remote management of local system
- **Network Connector** - Obtaining full TCP/IP access into the secured network.

Each access type is managed separately, and can be broken down even further to limit access by groups of users, or to individual users. The **RESOURCES** tab for each user will reflect the items to which they have been granted access by the system administrator.

Resources Rights

Access to a Resource is determined by the Resource Rights that are granted to a user. All users that are assigned to a Resource will also automatically be granted the associated Access Rights for launching that Resource. Additional Resource Rights, for creating personal Resources or editing existing ones, can also be granted to users via the Barracuda SSL VPN administrative user:

1. From the **ACCESS CONTROL > Access Rights** page, make sure that the appropriate Resource Rights are made available to the appropriate Policies
2. From the **RESOURCES** tab, navigate to the appropriate page for each Resource to define the parameters for a specific instance of that Resource type.

Resource Categorization

All Resources accessible by a particular user are listed on that user's **RESOURCES > My Resources** page. Each of these Resources can be assigned to a Resource Category, for display and grouping purposes on this page. By default, the following Categories are available:

- **All Categories** - No grouping are used, and all Resources are listed alphabetically.
- **Favorites -** All available Resources are listed in order of how frequently they were used.
- **Most Popular** - Only the most frequently used Resources are listed.
- **Most Recent -** Only the Resources recently used by the user are listed.

Global Resource Categories can be defined by the *ssladmin* administrator from the **RESOURCES > Resource Categories** page of the administrative interface. In addition, individual users can also be assigned the rights to create their own Resource Categories:

1. From the **ACCESS CONTROL > Access Rights** page, make sure that the appropriate Resource Rights are made available to the appropriate Policies.
2. Users with the appropriate Resource Rights can then go to their **RESOURCES > My Resource Categories** page to define their personal Resource Categories.

Web Forwards

Web Forwards are a secured method of making available internal-only websites and other web-based applications, to users who are remotely accessing their organization's protected network. Any website or application that has a Web Forward configured for it will be accessible to remote users with the proper credentials, avoiding any need to place potentially sensitive information outside of your organization's firewall. All communication is secured with SSL which is standard on all modern-day web browsers, so no additional routines or applications are needed for the site or by the remote user.

There are many different ways that a website or application can interact with a browser, but all will generally fall into one of the following types of Web Forwards:

- **Tunneled -** A direct connection is created from the remote system to the website host, using the Barracuda SSL VPN Agent. If the destination host is not directly accessible from the remote system via pre-existing routes, either a host file or a PAC (proxy auto-configuration) file with routing information can be downloaded onto the remote system with each session as needed.
- **Reverse Proxy** (Path-Based or Host-Based) - All web traffic is routed through the Barracuda SSL VPN between the remote system and the website host. The remote client accesses the desired website using the Barracuda SSL VPN as the hostname in the URL, with the path then being proxied, or translated, into the actual URL required by the website itself based on either the path in the requested URL (Path-Based), or the destination host itself (Host-Based).
- **Replacement Proxy -** All web traffic between the remote system and the website is processed by the Barracuda SSL VPN to replace any explicit mentions of the website host with the Barracuda SSL VPN. The contents of the web page are modified as it passes through the Barracuda SSL VPN, making it possible to create custom replacement values as needed for different remote users.
- **Direct URL -** An externally-accessible URL to a website that does not require any URL address translation. No web traffic goes through the Barracuda SSL VPN for this type of Web Forward.

Authentication

Web Forwards may only be launched by a member of a Policy with the appropriate Access rights. An additional authentication step can also be configured for Replacement and Reverse Proxy Web Forwards, for the additional security of the destination host:

- **Form-Based** - Users submit their authentication information into a JavaScript or HTML form which is then submitted (via POST or GET) to the destination site for verification.
- **HTTP -** The username and password for the connecting user is verified via one of three authentication methods (Basic, Digest or NTLM) before the connection to the destination is made.

Allowed Hosts

In general, a Web Forward will only accept traffic that is destined for the system that houses the destination URL. However, Replacement and Reverse Proxy Web Forwards can also be configured with a list of **Allowed Hosts** whose traffic will also be accepted by that Web Forward. Doing so allows any links in the web content to an Allowed Host to function as expected, instead of being rejected as invalid.

Shared Web Hosts

For Web Forwards that direct traffic to a web server that acts as the host for multiple websites, extra information must be sent by the Barracuda SSL VPN to the destination server in order to identify the correct root directory for the desired website. This additional information is added to the headers for the web traffic when the **Multiple Services On Destination Host** option is enabled for the Web Forward.

Tunneled

A Tunneled Web Forward creates a secured direct connection, or tunnel, from the remote system to the system hosting the website through the Barracuda SSL VPN Agent so that no additional authentication becomes necessary, making this ideal for websites and applications that are hosted entirely on just the specified system. However, any attempts to follow a link to an external site may fail, since the established tunnel will not be authenticated for any other system.

All destination websites are presumed to be accessible by the remote system without any additional configuration changes. However, if special routing directions are necessary, such as for web hosts that have an IP address to which the remote system has no known route, one of two optional proxy types can be configured for Tunneled Web Forwards:

- **Host File Redirect -** Adds temporary entries to the remote system's hosts file to enable direct routing to the destination site. Upon launch of a Web Forward of this type, the Barracuda SSL VPN automatically uploads the additional information to the remote system. Because of this, the user then-currently logged in must have write permissions to the system's hosts file. Currently availably only for remote systems running the Microsoft Windows XP, Microsoft Vista and Microsoft 7 operating systems.
- **Proxy -** Creates and uses proxy settings in the web browser of the remote system to access the destination site. Upon launch, the Barracuda SSL VPN Agent downloads and installs a PAC file for the web browser, for use only when accessing the URL of the designated Web Forward.

Reverse Proxy

A Reverse Proxy Web Forward enables the Barracuda SSL VPN to act as the "substitute" destination host when remote systems need to access a website or application that is restricted to the internal network. All incoming web traffic is received from the external location by the Barracuda SSL VPN, then forwarded on to the appropriate internal website host. There are two types of Reverse Proxy Web Forwards that can be configured:

- **Path-Based Reverse Proxy -** Routes web traffic based on a specific path in the requested URL. This type is recommended for websites and applications containing links that all reside in distinct, named directories on the host system. Path-Based Reverse Proxies can be also used for items such as Citrix Web Interface that require secured, unrestricted access to the host system, by configuring the Web Forward to automatically launch the Barracuda SSL VPN Agent.
- **Host-Based Reverse Proxy -** Routes web traffic based on the hostname in the requested URL. This type is most useful for websites and applications that are not centralized under a single directory but instead uses relative paths in the web content, or require traversing the entire root of the web server.

Neither of these Reverse Proxy types will modify the actual content of the web traffic, nor do they require the Barracuda SSL VPN Agent or any hosts file alterations on the remote system.

Path-Based Reverse Proxy

The Path-Based Reverse Proxy, the most commonly used Web Forward type, acts as the front end to your web servers on the Internet or intranet. The Barracuda SSL VPN receives all the incoming web traffic from an external location and forwards it to the appropriate website host.

For a Path-Based Reverse Proxy to work, all possible destinations on the specified website or application for a particular Web Forward Resource must be within a directory on the web server; for example: for Microsoft Outlook Web Access (OWA), `/exchange` and `/exchweb`.

With a Path-Based Reverse Proxy, the Barracuda SSL VPN attempts to automatically detect all the paths that the target website uses, and add them to the Web Forward configuration when the Resource is launched.

For example, when you create a Web Forward for `http://sslvpn.example.com/blog` and this blog page also contains images from a path called /images from the root of the server, the Barracuda SSL VPN adds `/blog` and `/images` to the Web Forward configuration. This allows anything in the `/blog` or `/images` directory or subdirectories to work with this Web Forward.

The following example shows the paths that the Barracuda SSL VPN added to the Web Forward `http://sslvpn.example.com/blog` which the user can access:

```
https://sslvpn.example.com/blog/images/picture.jpg
```

The subdirectory of /images below /blog is added to this Web Forward.

```
https://sslvpn.example.com/blog/page2.htm
```

page.2.htm, a child of /blog, is added to this Web Forward.

When you try to access this Web Forward and the web content attempts to bring up an HTTP request that is not at one of those locations, such as:

```
http://sslvpn.example.local/news/index.html
```

the Barracuda SSL VPN automatically adds the path specified by that request; in this case:

```
/news
```

These paths do not work when they conflict with any paths that the Barracuda SSL VPN uses to display HTTP content, such as `/default/theme/js/fs`.

When parts of the web page are missing, the Barracuda SSL VPN might not have detected some of the paths. To resolve this issue, edit the Web Forward and manually add these extra paths.

Note: To use the Path-Based Reverse Proxy, make sure that you set the **Always Launch Agent** option.

Host-Based Reverse Proxy

The Host-Based Reverse Proxy allows the web content to be located anywhere on the destination web server, including its root. This is useful for websites and applications that specify a host header or use relative paths in the content.

The Host-Based Reverse Proxy creates a unique hostname and appends it to the subdomain of the Barracuda SSL VPN. In the following example, the Host-Based Reverse Proxy creates the unique hostname `12abd345` and appends it to the public URL. The subdomain is `sslvpn.company.com.`

```
http://12abd345.sslvpn.company.com/...
```

The Barracuda SSL VPN then uses this subdomain to determine the correct destination for the incoming web traffic. Because a unique subdomain is created for each Web Forward configured as a Host-Based Reverse Proxy, you must configure a DNS entry on your DNS server for each subdomain that is used to resolve to the Barracuda SSL VPN. You can identify every generated hostname and create an explicit entry for it on your DNS server, or create a wildcard entry so that all lookups resolve to the same IP address as the Barracuda SSL VPN.

As with the Path-Based Reverse Proxy, accessing links to a location that was not specified in the configuration fails unless you configure the destination hostname as an allowed host (with the **Allowed Host** option).

Replacement Proxy

A replacement proxy adjusts the links found in the source code of the actual web content that is returned from the web server, so that when pages are rendered on the remote system all links refer back to the Barracuda SSL VPN itself, as opposed to any absolute or relative paths that might have existed.

If you have absolute URL addressing, use the Replacement Proxy when the other Web Forwards do not work. The Replacement Proxy works most of the time, provided that the web page is not using a lot of JavaScript. However, using a Replacement Proxy is a little more resource intensive than the other proxies.

Because this method involves a literal replacement, the Barracuda SSL VPN actively searches for a very specific string of characters to replace with a different specific string of characters, carefully configure the actual string that you want to replace. In addition, because there are a number of ways in which links can be constructed (specified as relative or absolute paths, generated dynamically, written in ASCII characters or with HTML encoding, using English or non-English characters), this type of Web Forward might not recognize, and as a result, might not convert all instances of a particular URL.

Direct URL

A Direct URL creates a bookmark to access a URL without passing through the Barracuda SSL VPN. The Direct URL is different than the other Web Forward types because it is not proxied through the Barracuda SSL VPN.

Network Places

A Network Place is a resource that provides remote users with a secure web interface to the corporate network. A remote user can browse network shares, rename, delete, retrieve and upload files just as if he or she was connected in the office connected to the network.

Network Places enables remote users that have appropriate permissions to browse Microsoft Windows file shares, SAMBA file systems configured on UNIX, FTP and SFTP file systems. In addition, Network Places also provides support for Web Folders and the Windows Explorer Drive Mapping feature.

Web Folders

WebDAV (Web-based Distributed Authoring and Versioning) is a protocol that extends HTTP to define how basic file functions such as Copy, Move, Delete and Create Folder are performed over the Internet.

Web Folders is Microsoft's built-in support for WebDAV that is included with Internet Explorer 5. It enables the management of files on a WebDAV server by using a familiar Windows Explorer interface.

Using a WebDAV client as Web Folders, a remote user can access the organization’s network through the standard Windows Explorer interface without actually needing to log into the Barracuda SSL VPN.

When using Windows XP or later along with Internet Explorer, you can take advantage of Microsoft Web Folders to access your file resources. Web Folders are a great tool for remote working and once set up, accessing a share is simply a matter of clicking an icon and entering a Windows username and password when prompted.

Configured Web Folders must go through the Barracuda SSL VPN server so that the share be seen by the client operating system.

For security the Barracuda SSL VPN only allows Web Folders to be mapped to existing Network Places. If a network file system has not been configured through Network Places, then the Web Folder cannot be mapped to the desired location. This enforces policy restrictions; if a user does not have a policy which allows them to access a given network place then they will also be unable to map a Web Folder to it.

Windows Explorer Drive Mapping

The Windows Explorer Drive Mapping feature allows you to create a Network Place and assign it a drive letter when using Microsoft Windows 2000 or later.

When the Barracuda SSL VPN Agent is running, the drive becomes available under the user's Windows Explorer and like any other drive listed in Windows Explorer this drive can be accessed and any content accessible for the lifetime of the Agent.

Differences with WebDAV

WebDAV is limited to what file types it can support; certain files require specific WebDAV support added to them to be accessed while others are not accessible at all. With the Drive Mapping feature, any file can be accessed, modified and saved as long as it supports random access, can be accessed and is fully modifiable.

Another difference is that WebDAV supports only local buffering. For any file that you need to edit, WebDAV downloads a local copy that you can edit. When you are finished editing the copy, WebDAV uploads it back to the server. With the drive mapping feature any file can be edited in the traditional local buffered mode or also via streaming mode where the file is edited directly from the source.

Applications

Remote users may need to use client/server applications within the secure network so will need to use an application shortcut to facilitate this (a client/server application is something that uses software running on the client machine to connect to a server running elsewhere on the network e.g. an RDP connection to the desktop of their office PC). The applications resource allows the administrator to customize which applications are available by publishing a shortcut to each application required. The benefits of being able to distribute applications via the Barracuda SSL VPN are mainly due to the reduced software distribution costs, as the need to install specific application software on each client is removed in most cases.

The application resource consists of a shortcut and an application extension. When the application resource is invoked the SSL VPN Agent opens a tunnel to the destination machine and then launches the application specified by the shortcut; for example, the application extension. This application uses the tunnel for secure communication with the destination machine.

An Application requires:

- Shortcut identity; for example, Name
- Valid extension; for example, Application Type
- Hostname of the remote machine

For example, an application shortcut can be created to allow users access to their office PC desktop from home.

To use Microsoft's Remote Desktop, an application shortcut called **My Computer** is created with the **RDP – Microsoft RDP Client** as the extension to use (Application Type). When the user selects the **My Computer** application shortcut from their home PC, the RDP Client extension launches a remote desktop session to his or her office PC. The desktop of the remote PC will be displayed and the user will be able to work as though they were sitting in front of the PC in the office.

An application shortcut called **My Computer** can be created with the **UltraVNC** extension. This gives the user the same access to their office PC but by using a different application.

The extension is the method of connection used to gain access to the application and must be installed on the appliance before a shortcut can be created. A number of extensions are preinstalled on the Barracuda SSL VPN: a pull-down menu of all available extensions (Application Type) are located in the **Manage Account > Resources > Applications** page in the **Create Application Shortcut** section.

Each application type has potentially different requirements for operating information and this information can be specified by selecting the **Edit** action next to the Application on the **Manage Account > Resources > Applications** page.

SSL Tunnels

SSL Tunnels allow for connections to be made between networked computers. An SSL Tunnel is simply a connection between two TCP enabled components where all of the data transmitted over a tunnel is encrypted using the SSL protocol.

For example, a user may want to establish a secure tunnel to a Microsoft terminal server. To do this, the administrator configures an SSL Tunnel that uses 63389 as its source port and `example.company.com:3389` as the destination. The user activates this tunnel and then runs a locally installed RDP application, specify localhost as the hostname and 63389 as the port and all traffic will then be secured.

The same technique can be used for a number of different applications and protocols. A common use of tunnels is to secure the SMTP / POP protocols used for email access. Anything that uses TCP/IP client / server architecture will usually be able to be secured in this manner.

There are two types of tunnel:

- **Local**: A local (outgoing) tunnel protects TCP connections that your local computer forwards from a specified local port to a specified port on the SSL VPN that you are connected to. To use the tunnel, the application to be tunneled is set to connect to the local listener port. The connection beyond the SSL VPN is not secure. Other computers will not be able to use the tunnel if localhost is specified as the source port. If the source port has been set to your network IP address then other computers on the local network will be able to access the tunnel.
- **Remote**: A remote (incoming) tunnel protects TCP connections that are forwarded from the SSL VPN to a specified port on your computer. If the connection is forwarded beyond your computer that part of the connection is not secure.

Remote Assistance

Remote Assistance is a helpdesk feature of the Barracuda SSL VPN that enables remotely-connected users to easily communicate with and receive help from their IT department. Requests for assistance are submitted directly by the remote user from the web interface of the Barracuda SSL VPN, and can also be scheduled for a specific time.

The built-in Request management system, accessed by system administrators and other helpdesk personnel from their personal web interface to the Barracuda SSL VPN, allows them to track and respond to all open Remote Assistance Requests, including establishing secured, direct connections to the remote system if necessary.

Requirements

Remote Assistance is available on standalone Barracuda SSL VPN 380 and above, and requires the Barracuda SSL VPN Agent and a Java Virtual Machine (JVM) to be installed on both the remote and the helpdesk systems. A specialized VNC server and client is used to access and control the remote system, and is downloaded as needed from the Barracuda SSL VPN.

User Configuration

Remote Assistance users fall into one of two categories:

- the standard user, who requests assistance
- the helpdesk or system administrator, who responds to requests for assistance

The access rights granted to an account by the *ssladmin* administrative user (from the **ACCESS CONTROL > Access Rights** page) determine which category a particular account falls into. Only the accounts granted Remote Assistance Rights will have a **My Remote Assistance** page on their **RESOURCES** tab, from which Remote Assistance Requests are both made and responded to.

Remote Assistance Requests

When a user submits a remote assistance request, an entry is made in the **My Remote Assistance** pages for the user and all administrators from which this request is managed and responded to. The user and administrator can initiate a secured connection to the Barracuda SSL VPN. When both the requestor and the responder of a request have initiated connections, the Barracuda SSL VPN will connect the two so that secured, direct end-to-end communications is possible allowing:

- direct control by the administrator of the remote system’s desktop
- two-way instant messaging sessions
- secured file transfers

Profiles

Profiles contain the parameters for the general working environment for a user. There are two main areas of control: the Session and Barracuda SSL VPN Agent properties. A profile allows an administrator or user to alter the general working environment of the system. Modification is encapsulated into two distinct areas: those that affect a session and those that affect the Barracuda SSL VPN Agent.

The Barracuda SSL VPN Agent is an applet that tunnels data from insecure applications. The Agent intercepts the data and encrypts transmission. The SSL VPN Agent is mainly used by Resources such as SSL tunnels and Web Forwards. The session parameters affect how the active session behaves and includes such things as session inactivity timeout which defines how long a user can sit idle before being automatically logged out.

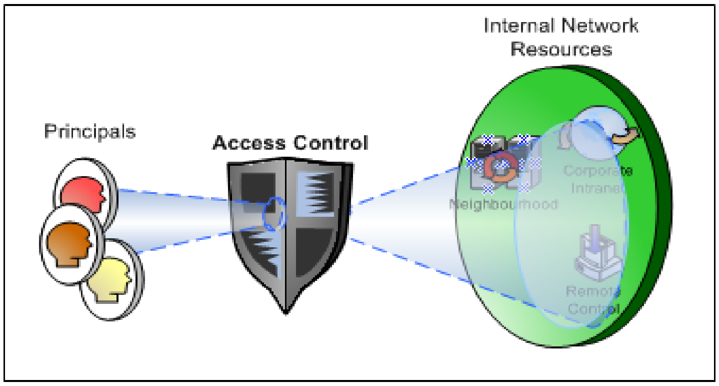
Profiles can be accessed and configured by both the administrator and the user, however only the administrator can configure the system default profile. Users who are granted the appropriate permissions can create and manage their own profiles. Profiles are a way for users to configure an environment based upon where they are accessing the system. For example, a user might configure a **home** profile which is configured for use when working from home and another called **On-site** which could be used for when the user is on a customer site.

Chapter 7
Access Control

This chapter describes how the Barracuda SSL VPN is able to achieve control of users and resources and the relationships between them. The following topics are covered in this chapter:

Overview

Access control manages all users from their initial log-on, until they exit the system. It secures user access to different areas of the internal network.



Access control is the key component in verifying a user accessing the system and determining the actions that they can perform. Every action performed within the Barracuda SSL VPN is monitored by the access control engine in real-time and, as the diagram depicts, it acts as the guardian of the system.

System of Trust

The concept of trust is a fundamental part of any secure system. It is crucial for the security policy to cater for and control how that trust is granted, used and revoked.

With trust playing such a significant part of remote access, the Barracuda SSL VPN allows for either coarsely grained or finely grained access control. This approach allows the product to mirror more closely the actual trust relationships present in the real world. In conjunction with multi-tiered authentication schemes, our security model is much more advanced than those offered by conventional VPN solutions.

Levels of Trust

Trust is administered in measures - the more trust a user has the more privileges they are granted. Again the opposite is said for someone who has a lesser degree of trust and consequently is given a lesser level of ownership and access.

The Barracuda SSL VPN follows this well established pattern. With the access control framework, administrators are seen as the most trusted users, seeing as they are ultimately in control of the appliance. Trusted users can be given a lesser measure of control. Finally, the standard user has a lesser degree of trust and therefore potentially the least level of access and responsibility.

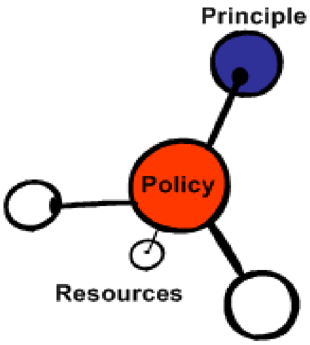
Access Control Architecture

The access control framework has been designed to tackle the following main issues.

- **Users and Groups**: Each organization's view on users and groups is almost always different. They do though share common behavior, i.e. 'Add User/Group' or 'Delete User/Group'. It is also likely that the organization's user/group directory already existed prior to the introduction of this appliance, for example an existing Active Directory domain or LDAP directory. The variety offered by such choice invariably gives rise to a number of different approaches and implementations.
- **Resource Access**: The intended outcome when implementing an SSL VPN solution is to allow remote access to network-based resources. The number of different types of network resource is relatively varied and new methods are likely to appear.
- **Resource Distribution**: A resource created within the system must be easily made accessible to those users that require it. Assigning resources on a per-user basis should be avoided wherever possible.
- **Resource Permissions**: Resources can have a range of permissions to limit how they may be assigned. When a resource is assigned to a user the user must be restricted to the access rights given. For example, a super user may create a resource to administer creation and assignment of application shortcuts only. This resource is assigned to a user who then attempts to delete an existing application shortcut; this operation will be declined.

In order to resolve the aforementioned issues the access control architecture relies on three key entities:

- **Principal**: The intended consumer of the resources, i.e. a user or a group.
- **Resource**: The networked resource, internal function or property item that the principal wishes to utilize, i.e. a Web Forward or the right to manage accounts.
- **Policy**: The relationship defined between the principal and resource. It is the component that ensures that only the right people can perform the right action.



Utilizing this methodology, the Barracuda SSL VPN is able to maintain robust, secure, and flexible access control architecture.

Principals

The principal simply refers to a user or group of users. The principal entity sits at one end of the access control chain. The process flow begins with this entity and ends with the resource entity.

Principals define users in two forms: the singular being represented by an Account and the plural being a collection of accounts known as a Group.

Accounts

An Account is simply a user that will access the system. This can be in the form of a standard remote user accessing the system to carry out their work or an administrator who maintains the system and creates users and organizes access control etc.

The only default user embedded within the Barracuda SSL VPN is the Administrator Account, *ssladmin*. All other users with administrative rights are created by this user and their administrative rights defined by their attached policies.

A policy structure should be considered before creating any accounts. Categorizing accounts into policies as *Administrators* or *Guest* will encourage a more structured and organized system. This is often imperative as the user base grows.

The administrator however is not categorized as a standard user, in fact the administrator is classified as the administrator of the system only and not as a typical user. The administrator's purpose is to perform configurations of the appliance and from then on the super user should delegate its responsibilities out to other users of the system through access rights (**Manage System > Access Control >Access Rights**).

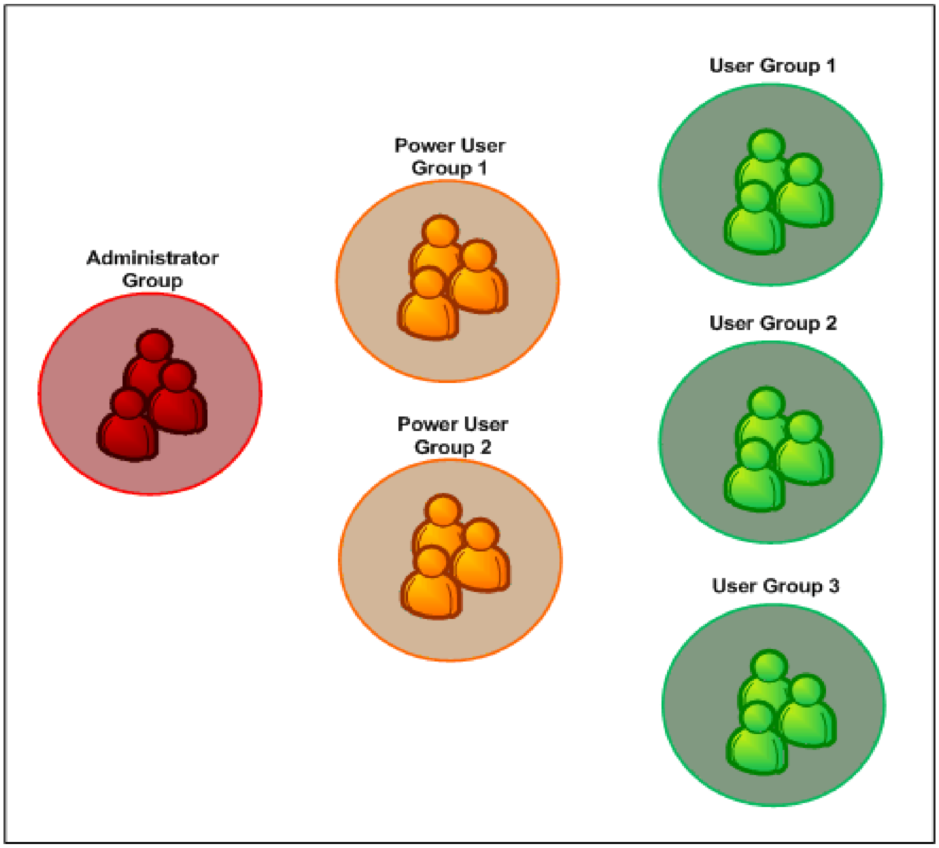
Note **Unsupported Database**

Actions such as ‘Create’, ‘Edit’, ‘Delete’ will not be accessible if the chosen user database does not support external modification by the Barracuda SSL VPN. To make such amendments the administrator must access the user database directly.

Groups

Groups represent the alternative type of principal. Groups offer a more convenient type for larger enterprises with a greater user base.

Groups allow for a more structured approach to account management; allowing an administrative user to categorize types of accounts under one heading as the diagram below shows.



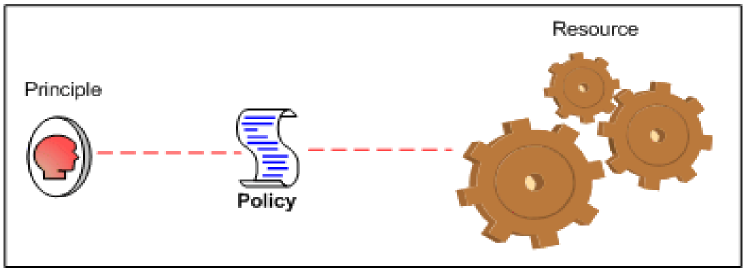
Groups can be manipulated within the system as single entities but remember that all operations on the Group will affect all accounts within the Group. For example, an SSL tunnel resource can be linked to a single Group and instantly every user within that Group will be granted access to the attached resource.

Resources

A Resource is defined as an application or data source. It sits at the other end of the access control chain. Think of it as the endpoint, or objective that a user wishes to achieve. This could be something as simple as a user accessing their email client to read their mail. In this case, the Resource would be the email. Similarly, an intranet website would also be classed as a Resource – just as a network share would be. All accessible stores of 'informational value' are deemed to be Resources under this concept.

Policies

A Policy is the glue by which all Principals and Resources can cohesively work together. As the diagram below shows, the means by which a Principal entity has access to a Resource entity is through the Policy and the means by which a Resource entity becomes accessible is again through the Policy.



Policies represent a form of trust. A high level of trust equates to a Policy of greater flexibility and responsibility; whereas a user with minimal trust may be assigned Policies that grant them fewer privileges.

A user of the system who has the need to manage a particular user database, for instance, must have a higher degree of trust and consequently is granted a Policy that covers a much greater scope of responsibility. The opposite can be said for a standard user whose Policy may only grant the bare essentials required to allow them to perform their duties.

Access Rights

Access Rights are essential in creating a well organized system. As mentioned earlier, the Super User should only be used to perform configuration of the system. From then on the Super User should create Management Users who are responsible for the daily uptake of the management and running of the system.

An Access Right allows the Super User to delegate an area of responsibilities to a Policy. Nearly all areas of the system can be delegated to different Policies.

All areas that can be managed are divided into their respective areas:

- **Resource Rights**: Items that can be managed in this area are all Resources such as Web Forwards, Profiles and Network Places can all have their create, edit and delete actions delegated out to a Policy.
- **System Rights**: Items that can be managed in this area that can be delegated are all system resources such as Policies, SSL certificates, Authentication Schemes, Accounts and Reporting.
- **Personal Rights**: Items that can be managed from the Manage Account interface are all personal resources such as Profiles, passwords, personal details, Favorites and Attributes.

The Access Rights interface summarizes the currently available permissions. The main page provides information on the resource permissions currently available.

Configuring User Databases

All user data used and managed by the appliance must be stored somewhere. The Barracuda SSL VPN allows the configuration of a number of databases to store this information. The User Database configuration page (**Manage System > Access Control > User Databases**) lists the available databases. A **Test** button is provided to check whether the server details are entered correctly

Built-In User Database

Configuring the built-in database is very simple; just select the **Built-in** option on the **User Database Type** page. The appliance does all configuration of the database itself internally.

As this is a new database, once the appliance is up and running it is necessary to create all Accounts and Groups from the **Manage System** interface. With the built-in database you will also be able to edit and remove users and roles directly.

Active Directory

Active Directory authentication allows for integration with a Microsoft Windows Domain Controller. Using this method of authentication you can read users and groups directly from the domain controller and authenticate your users against your Windows domain.

Once you have entered the relevant properties in the configuration page, a connection is made to the domain controller and when the service account has been authenticated, the Active Directory User Database is ready to be used.

The **Connection** area configures how to connect to the Microsoft Windows Active Directory service.

Active Directory database uses simple authentication for the service account. Simple authentication allows the use of non-standard character sets. With this type of authentication the account credentials need to be fully qualified.

LDAP

LDAP configuration allows you to authenticate against a standard LDAP User Database. Similarly to Active Directory authentication, a service account will need to be created in the LDAP schema in order for the Barracuda SSL VPN to authenticate users in this manner.

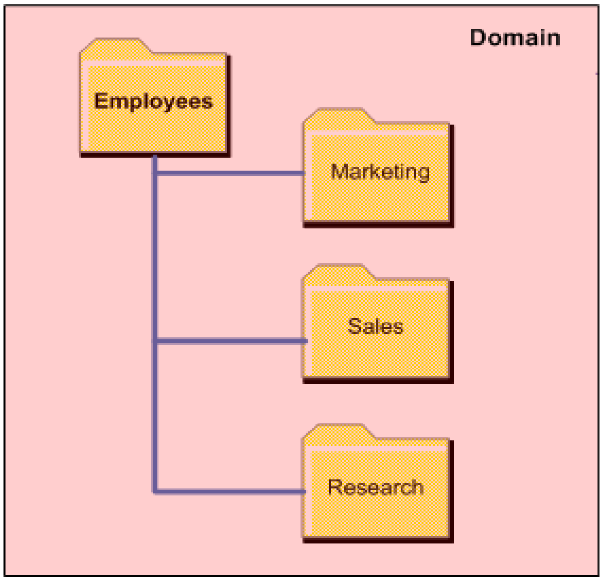
LDAP Class Objects

The Barracuda SSL VPN needs to understand which User and Role classes are in use by the given LDAP installation. Since each installation can use a different type of schema this information makes the appliance compatible with a larger number of LDAP installations.

Organizational Units (OUs)

In Active Directory and LDAP, ‘Organizational Units’ (OUs) are the key structure for organizing users, computers, and other object information into a more easily understandable layout.

As the diagram below shows the organization structure has a root OU with three nested OUs below.



This nesting enables the organization to distribute users across multiple logical structures for easier administration of network resources.

Organizational Unit Filter

The Include Organizational Unit Filter makes adding OUs easier.

Entries in the filter must be of the form `OU=<Organizational Unit name>`. For example, `OU=Research`.

If an OU is held below another OU then the entire hierarchy up to the parent OU must be listed. If an OU called ‘Marketing’ was stored under the ‘Employees’ OU; to add ‘Marketing’ the correct syntax would be `OU=Marketing`, `OU=Employees` with the separating comma being used to separate each element in the hierarchy.

To add all OUs in the domain simply leave the **Filters** list box empty. When the list box is empty, all OUs will be queried. If problems are encountered with Active Directory, try clearing the list box.

To remove an OU from the search add the OU into the Exclude Organizational Unit Filter section.

Troubleshooting

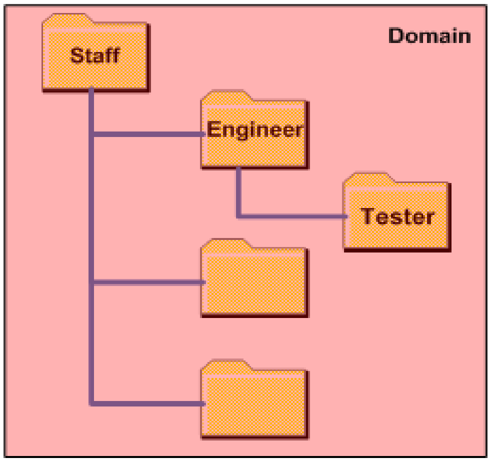
If your users are unable to connect via Active Directory, check that:

Double check that the AD settings are correct, ensure that the domain has been entered as the fully qualified domain name.

If the *username* does not work for the service account name, try *username@domain* instead.

If OUs have not been loaded successfully:

Any organizational units held within a tree structure need to be added with the entire parental structure.



In the above diagram to include `Tester` into the filters list the syntax should be `OU=Tester,OU=Engineer,OU=Staff`. The syntax begins with the lowest branch first.

- If any of the Windows OUs such as `Users` are needed then these are referred to as `CN=User` rather than `OU=User`.
- Check syntax of each filter. Every Organizational Unit must begin with `OU=`. If a hierarchy structure is being included, make sure you separate each element with a comma. Avoid using unnecessary spacing.
- Clear the organizational unit filter to ensure that the entire Active Directory tree is searched.

NIS User Database

The Barracuda SSL VPN can be configured to authenticate against a Network Information Service (NIS), also known as Yellow Pages. NIS is a Unix-based user database that was originally developed by Sun Microsystems.

Configuration of NIS is relatively simple, involving little more than entering the NIS server hostname and the NIS domain name

Chapter 8

Advanced Configuration

This chapter details advanced configuration options and attributes. The following topics are covered in this chapter.

Attributes

As with any large user management system, functionality that allows for simpler administration is always welcome. User attributes are a simple concept that allow for drastically reduced administration overhead.

User attributes are simply attributes that perform a similar function to ‘environment variables’, and can be created by a user and used throughout the system. The appliance comes with a set of default attributes that cannot be removed; these are used by the Personal Details Authentication module.

Security Questions

One of the default user attributes is **placeOfBirth**; all users have this attribute stored under the Security Questions section under **Manage Account > My Account > Attributes**. Each user can populate this attribute with their respective answer and when the Personal Details authentication module is used at log-on and asks a user for their place of birth, the module merely looks to the value stored under this attribute for each user logging into the system. If the attribute keyed in value matches that of the stored **placeOfBirth** value, authentication is successful.

For each user logging in, the respective attribute is compared allowing for a single attribute to be used by all users.

Applications

Attributes can be used with application shortcuts. For example, an attribute can be created which defines a hostname to use with a VNC Server application shortcut.

The attribute is created within the **Manage System > Advanced > Attributes** page under the Create Attribute section and given a name; for example, **vncServer** and a label **VNC Server**. Selecting the **Edit** action for this attribute allows the default hostname of the VNC server to be configured.

Each user is now able to define this attribute, specifying which server they wish to connect to when using a VNC application shortcut. The new **VNC Server** attribute will appear in the **Edit Attributes** section under **My Account > Attributes**.

The VNC application shortcut can be configured to use this new attribute. Browse to **Manage Account > Resources > Applications** and enter the relevant details in the Create Personal

Application Shortcut section:

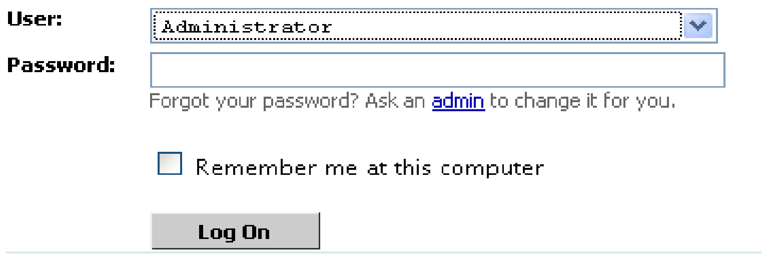
- Application Name: select **UltraVNC** from the pull-down menu
- Name: enter a name for this application shortcut
- Hostname: click the **${}** button at the side of the **Hostname** field and select *userAttributes:vncServer* from the list.

Whenever the application shortcut is executed, the system takes the current user’s **vncServer** attribute and uses the value as the hostname to connect to.

Each user can define their own **vncServer** attribute to point to whichever server they wish to connect to. Thus for every user the application shortcut works differently, connecting to a different server without any further modification.

Web Forwards

The flexibility of user attributes also means they can be used in Web Forwards. An example being a support case tracking application which requires a form to authenticate users.



User: Administrator

Password:

Forgot your password? Ask an admin to change it for you.

A standard username attribute cannot be used as the FORM has an **User** pull-down menu.

A user attribute is defined that specifies the associated user’s ID. Two new attributes are defined which are confidential to the user only and specify the username ID (e.g. **supportID***)* for the user and their password (e.g. **supportPassword**).

When the Web Forward is configured, the attributes are added to the authentication parameters. Navigate to the **Manage System > Resources > Web Forwards** page and select the **Edit** action for the Web Forward. In the **Authentication** section click the **${}** button next to the **Form Parameters** field and select *userAttributes:supportID* and *userAttributes:supportPassword* from the pull-down menu; add them to the **Form Parameters** section.

When the Web Forward is executed the **supportId** and **supportPassword** attributes are submitted during authentication into the website. The FORM object takes the **supportId** and identifies the username then takes the **supportPassword** as the associated password.

Instantly any user is able to access the support website using their credentials and this single Web Forward.

Types of Attributes

The above examples show the use of the user attribute where the attribute is assigned through the `${attr:attributeName}`command. There is also another attribute type called Policy Attribute. This attribute assigned to a policy and is referenced by the `${policyAttributes:examplevncHostname}` variable.

Policy attributes, once set, are set for all users under the assigned policy. The resource can be executed under a different policy and have a different value for each policy.

How to use Attributes

Once a user attribute has been created it can be used throughout the system. Wherever dynamic information can be loaded, user attributes can be used.

A user attribute is referenced via the `attr` command; a policy attribute is referenced by the `policyAttr` command. The following example shows how to set up a Network Place using user attributes.

1. The attribute is created within the **Manage System > Advanced > Attributes** page under the **Create Attribute** section and given a name, for example, **myNetHome** and a label **My Network Home**. Selecting the **Edit** action for this attribute allows the Category to be set to **Network Places**.
2. The Network Place is then created. Enter the required path and then click the **${}** button next to the **Path** field and select *userAttributes:myNetHome* from the list; giving e.g. `smb://examplepath.com/users/${attr:myNetHome}`
3. When this is executed the system replaces the `${attr:myNetHome}` with the user attribute value.
4. Each user is now able to define this attribute, specifying the value to use when creating their Network Place e.g. **RobertsP**. The new **My Network Home** attribute will appear in the Network Places section under **My Account > Attributes**.

Each time the Network Place is launched, the system dynamically takes the value of **My Network Home** from the logged in user and replaces the `${attr:myNetHome}` parameter in the path. Each user loads their home share. In this case, `smb://examplepath.com/users/RobertsP`

Session Variable

Another way to use dynamic parameters in the system is by using the session variable.

The session variable is used mainly when creating extensions, and it allows session information to be used and not user attributes. With the above example we could also have used 'session' as opposed to the `attr` variable.

For example, the session variable refers to the values available during the course of the session, for example `{$session:username}`. So as above the system would replace this with the username being used in this current session. This means that if the user's home share on the network is named the same as the username used to log into the appliance (as might be the case in an Active Directory environment) then this Network Place will work and the home share of RobertsP would still be loaded.

The session variable can also be used to reference the user's password; so in an example of an application shortcut which requires both username and password we could use `session:username` and `session:password`.

Barracuda Networks recommends that the **Automatically Update** setting be set to *On* so that the Barracuda SSL VPN receives the latest rules as soon as they are made available by Barracuda Central.

Microsoft Exchange 2003 RPC/HTTPS

Outlook with RPC/ HTTPS mode enabled allows you to connect to your Exchange server from an Outlook 2003 client in native mode using the Barracuda SSL VPN as a pass through proxy. Unlike POP/SMTP, this means that all mail is held centrally rather than being downloaded to each client.

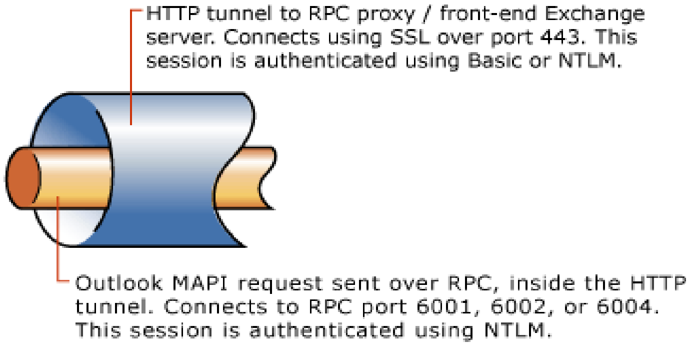
This feature provides a pass-thru proxy for Outlook RPC over HTTPS traffic. It is in no way a replacement for a front-end HTTPS server in a normal Exchange HTTPS topology, but is instead a facility to allow the Barracuda SSL VPN to become the Internet facing proxy for your Outlook users. This allows your Outlook clients and Exchange server to communicate over a single open port on the organization firewall.

Being part of the security framework provided by the Barracuda SSL VPN, your Exchange users benefit from the policy based security provided and access to this service is provided by way of authorized policies.

RPC/HTTPS

RPC over HTTP allows Microsoft Outlook clients to access Microsoft Exchange server over the internet. The MAPI protocol usually uses RPC to make calls to the Exchange server using TCP, but here we are able to tunnel Outlook RPC requests inside an HTTP session.

The RPC over HTTP Proxy networking component extracts the RPC requests from the HTTP request and forwards the RPC requests to the appropriate server. The advantage of this approach is that only the RPC proxy server has to allow access from the Internet. Back-end Exchange servers do not have to allow access from the Internet.


HTTP tunnel to RPC proxy / front-end Exchange server. Connects using SSL over port 443. This session is authenticated using Basic or NTLM.
Outlook MAPI request sent over RPC, inside the HTTP tunnel. Connects to RPC port 6001, 6002, or 6004. This session is authenticated using NTLM.

Configuration

Configuration consists of two parts: the server and the client. This document assumes that the Exchange administrator has already configured the Exchange server to accept RPC calls over HTTP. For further information on how to configure this please refer to the Microsoft website.

This chapter however does detail how to configure a new mail account to use your appliance as a proxy to communicate with the configured RPC/HTTPS Exchange server.

Prerequisites

The following is required:

- **Trusted Certificate**: You must have a trusted certificate installed or alternatively each client must trust the certificate by adding it to the Internet Explorer trusted certificate authorities' store.
- **HTTPS Proxy hostname**: The HTTPS proxy configured within Outlook must match that of the certificate used by the Barracuda SSL VPN. If the appliance is set up with a trusted certificate for the host `vpn.example.com` then this must be entered exactly into Outlook configuration for HTTPS otherwise Outlook will not connect to the appliance.
- **NTLM Authentication**: The RPC proxy will only work with Outlook clients that authenticate over NTLM.

Configuring the Barracuda SSL VPN as a RPC Proxy

Browse to the Outlook configuration settings under **Manage System > Advanced > Configuration**.

From here the Exchange server can be specified, along with the associated port and the protocol to use to communicate with Exchange. In addition all policies that have access to this feature can be added. To add a policy, simply select the available policies from the **Authorized Policies** list.

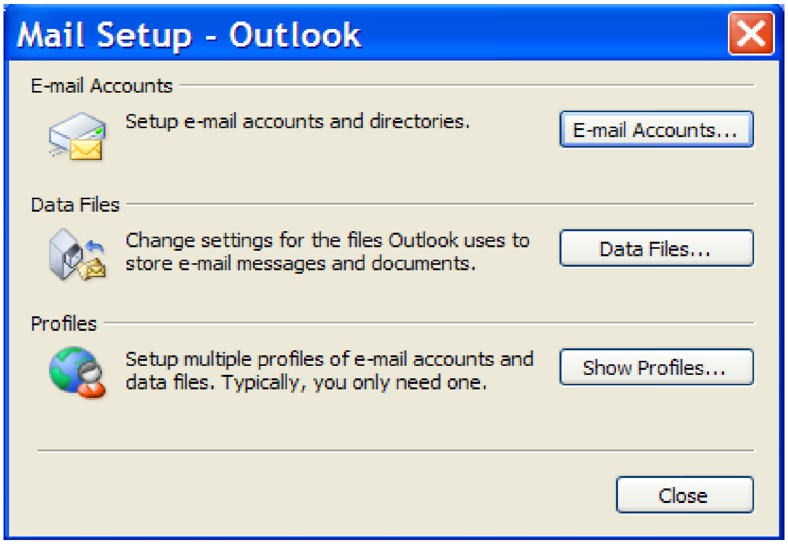
Users of any policies not part of the **Selected Policies** window will not have the ability to use Outlook over HTTPS.

Client Configuration

The final step in the configuration is that of the email client Outlook. Each user can either add a new profile to an existing account or as the following details; a new email account is created. Either way, the main steps are the same and relevant to both.

1. From the **Windows Control Panel**, access the Mail setup by selecting the **Mail** icon.

2. From the **Mail Setup-Outlook** window, click **E-mail Accounts. . .**



Mail Setup - Outlook

E-mail Accounts

Setup e-mail accounts and directories.

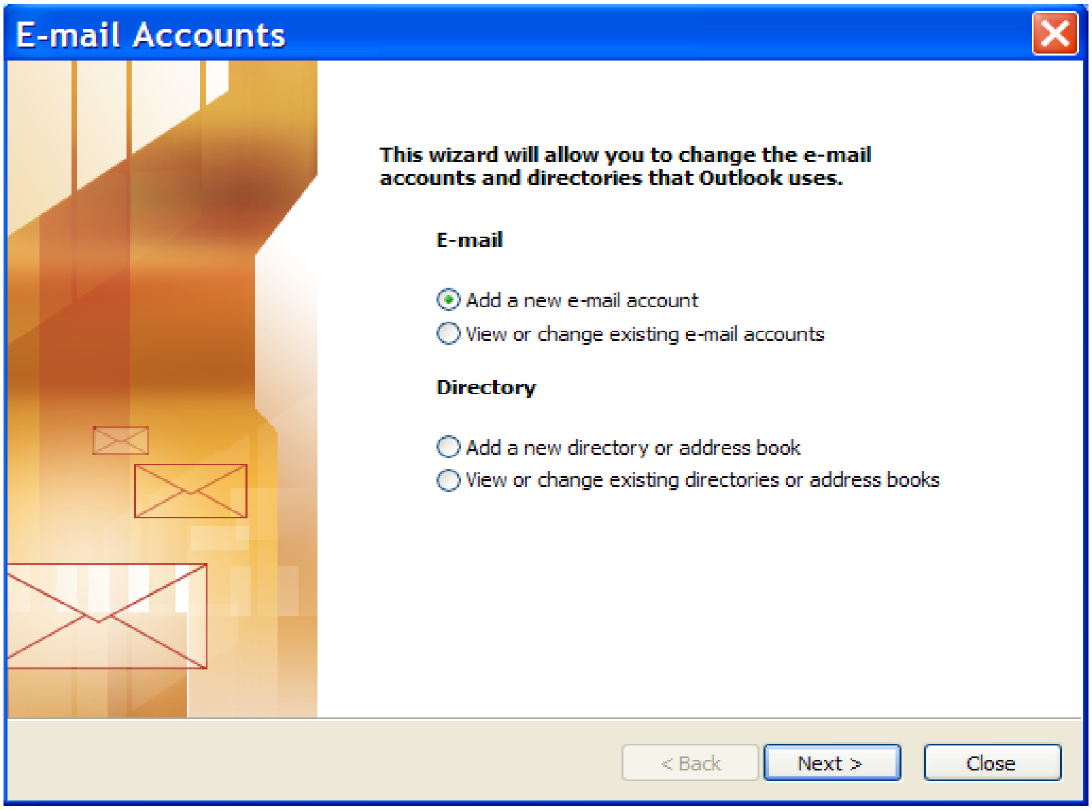
Data Files

Change settings for the files Outlook uses to store e-mail messages and documents.

Profiles

Setup multiple profiles of e-mail accounts and data files. Typically, you only need one.

3. In **E-mail**, select **Add a new email account**.



E-mail Accounts

This wizard will allow you to change the e-mail accounts and directories that Outlook uses.

E-mail

● Add a new e-mail account

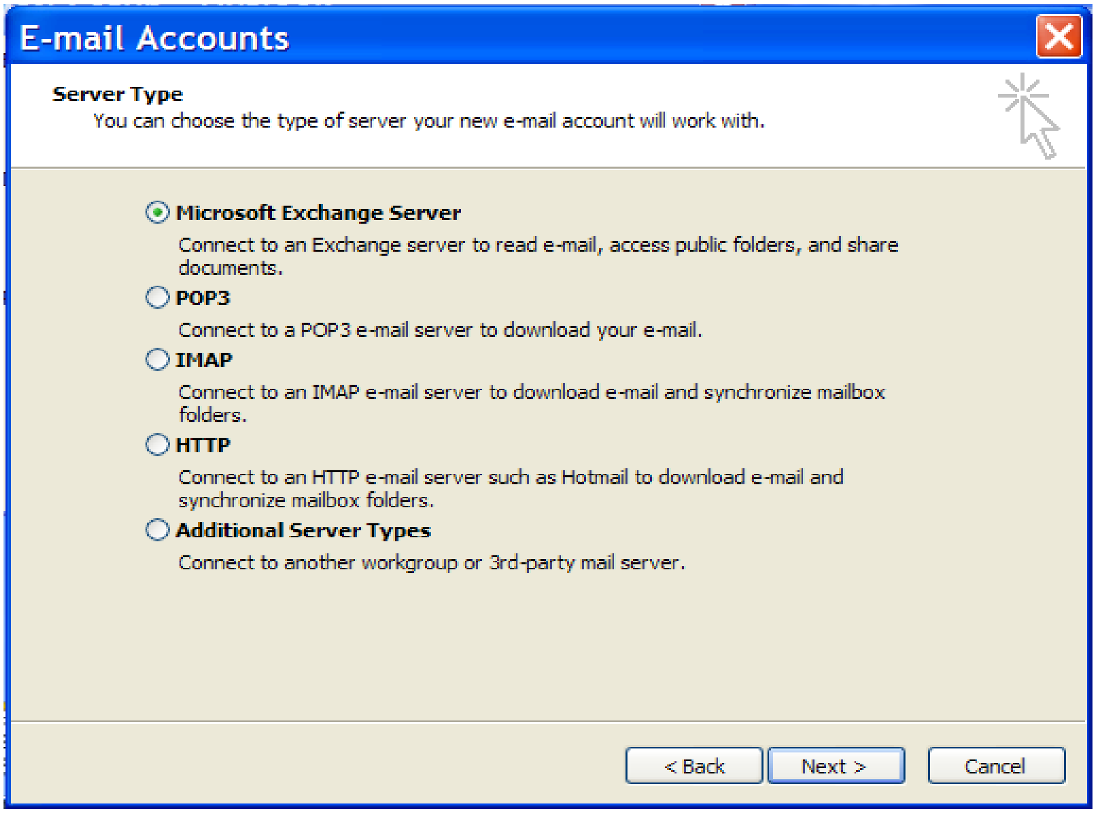
○ View or change existing e-mail accounts

Directory

○ Add a new directory or address book

○ View or change existing directories or address books

4. Under server type select **Microsoft Exchange Server** option.



Server Type

You can choose the type of server your new e-mail account will work with.

● **Microsoft Exchange Server**

Connect to an Exchange server to read e-mail, access public folders, and share documents.

○ **POP3**

Connect to a POP3 e-mail server to download your e-mail.

○ **IMAP**

Connect to an IMAP e-mail server to download e-mail and synchronize mailbox folders.

○ **HTTP**

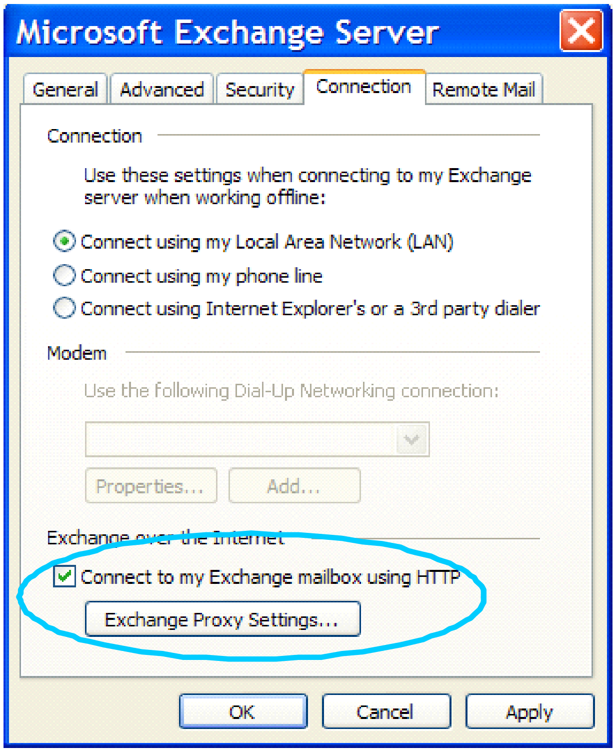
Connect to an HTTP e-mail server such as Hotmail to download e-mail and synchronize mailbox folders.

○ **Additional Server Types**

Connect to another workgroup or 3rd-party mail server.

5. Under the **Exchange server** settings, select the newly configured Exchange server and the name of your new mailbox.

6. From the same window select **More** settings. From the first window under the **Connection** tab, check the **Connect to my Exchange mailbox using HTTP**.



Connection

Use these settings when connecting to my Exchange server when working offline:

● Connect using my Local Area Network (LAN)
○ Connect using my phone line
○ Connect using Internet Explorer's or a 3rd party dialer

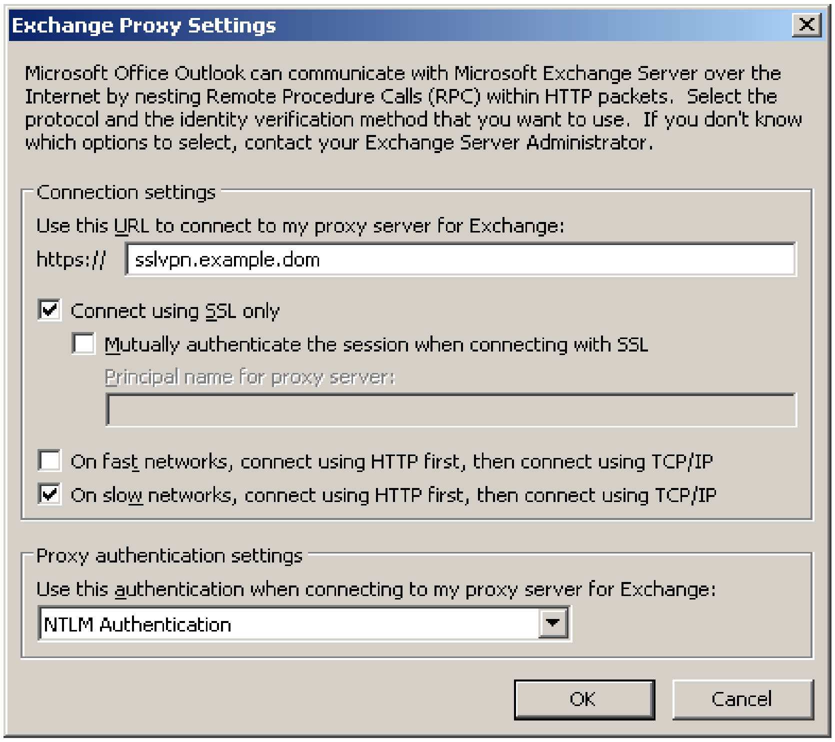
Modem

Use the following Dial-Up Networking connection:

Exchange over the Internet

☑ Connect to my Exchange mailbox using HTTP

7. Selecting the **Exchange Proxy Settings** button opens a final window in which the FQDN of the Barracuda SSL VPN should be entered into the **Use this URL to connect to my proxy server for Exchange** parameter. In the **Proxy authentication settings** select *NTLM Authentication*.



Microsoft Office Outlook can communicate with Microsoft Exchange Server over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Server Administrator.

Connection settings

Use this URL to connect to my proxy server for Exchange:

https:// sslvpn.example.dom

☑ Connect using SSL only

☐ Mutually authenticate the session when connecting with SSL

Principal name for proxy server:

☐ On fast networks, connect using HTTP first, then connect using TCP/IP

☑ On slow networks, connect using HTTP first, then connect using TCP/IP

Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange:

NTLM Authentication

The client is now configured.

Once Outlook is started, if your Barracuda SSL VPN has not been configured to use the same Windows account as the one the user is currently logged on with, the system will prompt for the Barracuda SSL VPN authentication credentials. After which if the user is recognized as a valid user of the RPC/ HTTPS resource, your appliance will enable communication between Outlook and the mail server over HTTPS.

Outlook Mobile Access

Exchange 2003 provides a feature called Outlook Mobile Access (OMA). OMA allows users to access Exchange data by using mobile devices. This browser based application is similar to Outlook Web Access but much more lightweight and intended for use on cell phones and PDAs.

Configuring the SSL VPN as a OMA Proxy

Configure the Exchange properties as per RPC Client Configuration. All clients that have access to Outlook using RPC/HTTPS will also have access to the lightweight OMA interface.

Test the connection from a mobile device by simply connecting your cell phone's web browser to the following address:

```
https://servername/oma
```

Outlook Web Access and Mail Check

This mail check feature presents to the user an instant view of his or her email account status directly through the Manage Account view without having to start their email client to check for new email. This feature can be used to check for email (and launch your web mail client) on any mail server that supports the POP3/IMAP protocols, including Microsoft Exchange.

The mailbox icon is visible from the Manage Account view and shows the status of new or any unread messages.

Clicking the refresh button also instantly checks the mail account and provides an instant update of its status. Clicking the mailbox itself will open a new window to the mail account.

Configuration of this relies on a Web Forward. The following provides basic steps on how to configure the mail check feature.

1. Create a Web Forward that connects to the mail server and check that it works correctly. No username or password has been specified in the configuration. When this Web Forward is launched we will be prompted for authentication.
2. Configure the mail check configuration parameters from **Manage System > Advanced > Configuration > Mail Checking**. The mail check feature requires the OWA server's details to access the mail server. Also the mail protocol has been specified and the hostname of the mail server.
3. The final step involves the configuration of personal details for each user from the **Manage Account** view. For each user the mail check tab becomes accessible from **Manage Account > My Account > Attributes**.

The Mail Check feature will automatically try and log onto the mail server with the currently logged on users credentials. When using Active Directory authentication along with a Microsoft Exchange mail server these are usually identical. If these are different, then each user needs to provide their mail authentication details on this screen. In addition the default mail folder (i.e. inbox) can be specified if needed.

If the system has been configured to use Active Directory and the mail accounts also uses the same Active Directory authentication credentials, the mail check extension will automatically use the user's Active Directory credentials to authenticate the user's mail account. There is then no need for users to provide authentication details in the mail check tab under personal details.

The mail check feature uses the Web Forward and the details defined in the mail check configuration page to connect to the mail server. It is from here it takes the individual user's authentication details to connect to their account and retrieve mail details.

4. Once all the user details have been provided the user should log back into the system. The mailbox icon will be visible in the top left of the main window.

Clicking on the mailbox will open a window to the mail account of the user without the need for authentication.

PPTP

You can configure the Barracuda SSL VPN to allow PPTP connections from remote devices using PPTP clients that support the Challenge-Handshake Authentication Protocol (CHAP), preferably MSCHAPv2.

The following operating systems have a built-in PPTP client:

- Microsoft Windows XP or higher
- Microsoft Windows Mobile 2003 (Ozone) or higher
- Mac OS X 10.2 (Jaguar) or higher
- SuSE Linux 10 (or equivalent), or higher

PPTP clients are also standard on most smartphones, including:

- Apple iPhones and iPads
- smartphones running Android 1.6 or higher
- tablets running Android 3.0 or higher

To Accept Connections Over PPTP:

1. On your organization's firewall, make sure to allow PPTP authentication traffic to and from the Barracuda SSL VPN. At a minimum, TCP over port 1723 and GRE (IP protocol 47) must be allowed to reach the Barracuda SSL VPN.
2. On the Barracuda SSL VPN, enable the built-in PPTP server to allow your remote users to authenticate and connect to the protected network. To configure PPTP settings, log in to the Barracuda SSL VPN with the *ssladmin* account in **Manage Mode** and navigate to the **RESOURCES > PPTP Server** page.
3. Instruct your remote users to log in at least once into the web interface of the Barracuda SSL VPN.
   Note: If the password for the remote user has changed since the last login, the user must log in again through the web interface for the new password to be registered appropriately.
4. On the remote device, create a PPTP connection to the Barracuda SSL VPN, making sure that the CHAP authentication method is selected.

For more information on configuring PPTP, see the technical document titled *Using PPTP with the Barracuda SSL VPN* on the support documentation page at http://www.barracuda.com/documentation.

L2TP/IPsec

You can configure the Barracuda SSL VPN to allow L2TP/IPsec connections from remote devices using an L2TP/IPsec client that supports using a pre-shared key (PSK) as an authentication protocol.

The following operating systems have a built-in L2TP/IPsec client:

- Microsoft Windows 2000 or higher
- Microsoft Windows Mobile 2003 (Ozone) Premium Edition, or higher
- Mac OS X 10.3 (Panther) or higher
- Linux 2.0 (or equivalent) or higher, with Openswan (implementation of IPsec)

L2TP/IPsec clients are also standard on most smartphones, including:

- Apple iPhones and iPads
- smartphones running Android 1.6 or higher
- tablets running Android 3.0 or higher

To Accept Connections Over L2TP/IPsec:

1. On your organization's firewall, allow authentication traffic to and from the Barracuda SSL VPN. UDP over ports 500 and 4500 must be allowed to reach the Barracuda SSL VPN for L2TP/IPsec connections to function.
2. On the Barracuda SSL VPN, enable the built-in IPsec server to allow your remote users to authenticate and connect to the protected network. To configure IPsec settings, log in to the Barracuda SSL VPN with the *ssladmin* account in **Manage Mode** and navigate to the **RESOURCES > IPsec Server** page.
   Note: Due to the nature of IPsec, the remote system must not use an IP address that falls into a range that is used inside the protected network.
3. On the remote device, create an L2TP/IPsec connection to the Barracuda SSL VPN.

For more information on configuring L2TP/IPsec, see the technical document titled *Using L2TP/IPsec with the Barracuda SSL VPN* on the support documentation page at http://www.barracuda.com/documentation.

Chapter 9

Agents of the Barracuda SSL VPN

This chapter explains the roles of various agents of the Barracuda SSL VPN Agent:

The Barracuda SSL VPN Agent

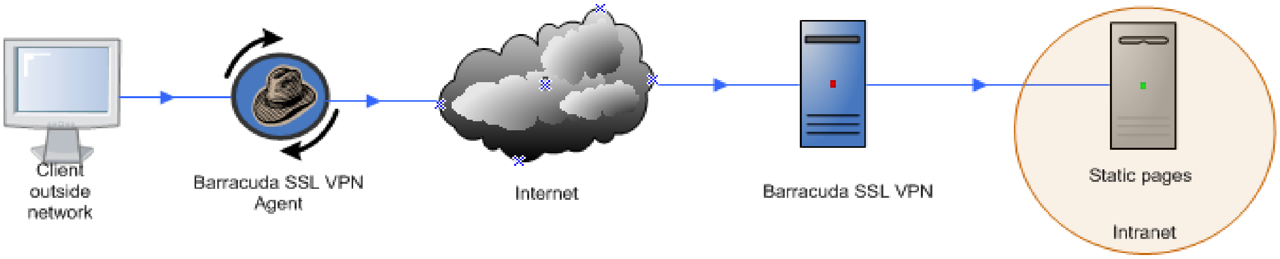
Many commonly used applications typically operate using unsecured protocols to facilitate the exchange of data. To the casual home user this is usually not a worry, though to the corporate user this is a critical vulnerability and one that leaves a business open to all manner of threats from password sniffing to industrial espionage.

With modern encryption protocols like SSL, data from these applications can be "tunneled" inside SSL packets. In the Barracuda SSL VPN appliance this is achieved through the use of the SSL VPN Agent – a small program that can intercept data transmitted by the insecure application, encrypting said data and transmitting the secure form over the wire. At the receiving end the appliance decrypts this data and forwards it to the appropriate destination within the trusted network.

With the Barracuda SSL VPN appliance comes a small SSL VPN Agent. This is a Java application that works in conjunction with your user session to provide SSL tunneling and application launching facilities provided by the appliance.

The Barracuda SSL VPN Agent is launched by a small Java applet placed on all pages that require access to the SSL VPN client. You only need to launch the client once per user session.

The Barracuda SSL VPN Agent is an essential tool for providing a secure tunnel for some of the resources detailed later in this document. When required, the resources automatically start the Agent.



Communication with Browser

The Barracuda SSL VPN Agent listens on a number of ports in the 65500+ range. This is normal behavior. The Agent is actually also a HTTP server and uses these ports to communicate with your web browser. All outbound network communications are sent through the HTTPS port 443

Precautions

It is important to remember that the SSL VPN Agent will provide a secure tunnel into your network until it is closed or times out due to inactivity. Your users must make sure that they log-off from their SSL VPN sessions. It is not wise to allow such a session to remain open and unattended even for a short period of time. The SSL VPN Agent will time out any tunnel that is inactive for a configurable period of time.

Executing Resources from the Barracuda SSL VPN Agent

Once the Barracuda SSL VPN agent is started you can execute any resource assigned to you directly from the taskbar icon. Clicking the right mouse button over the **Agent** icon will present a list of resources that can be executed directly from the Agent.

By opening the Tunnel Monitor it is possible to view any tunnels that are created through the life of the Barracuda SSL VPN agent. From here you can also kill any active tunnels.

The Barracuda Server Agent

The Barracuda server agent is a small client that is installed on a machine. Once installed the server agent registers itself with the appliance and then sits idle. It is only when the appliance requires its assistance does the client wake and begin performing its tasks.

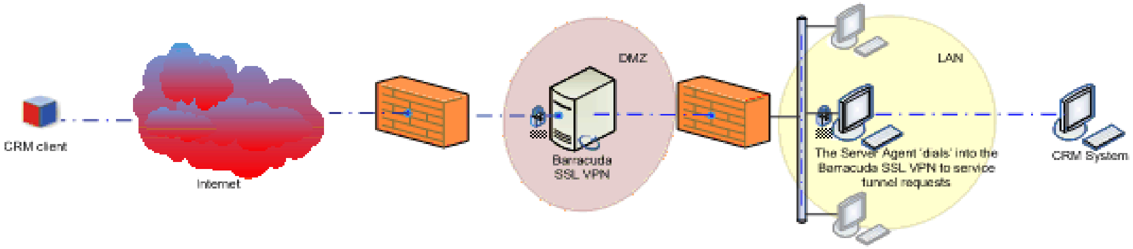
Purpose

The Barracuda server agent's purpose is simply to redirect traffic securely to a target host. As the diagram below shows, the server agent acts as a proxy directing traffic from the appliance to the remote system.

The administrator is thus able to configure an environment where there is no direct connection to the end host. For example, a server agent can be installed on a remote network and connect back to the appliance using the standard HTTPS port. With the configuration of routes an administrator can then set up resources that access services on the remote network without the need to open up a single port on the firewall protecting the remote network.

This same process can be used to access resources inside the LAN from a Barracuda SSL VPN residing in a DMZ.

In the diagram below, the appliance sits in the DMZ with other Internet facing servers. The DMZ is secured from the Internet with a firewall which only has port 443 open so that the appliance is accessible. The link from LAN to DMZ is also secured by a firewall. The administrator creates a Resource, for example a Web Forward to a CRM system; this requires a connection to the CRM service on the LAN. Instead of opening another port on the firewall between the DMZ and LAN, the administrator can position a server agent on the LAN side with a single port open which the server agent can receive data on.


CRM client
Internet
DMZ
Barracuda SSL VPN
LAN
The Server Agent 'dials' into the Barracuda SSL VPN to service tunnel requests
CRM System

Routes

A route defines an endpoint host that is associated with a single server agent. A server agent can be associated with a number of routes all of which define what endpoints a particular server agent can connect to. When a connection takes place the system determines which server agent is associated with the client's desired route and contacts that server agent passing it all the traffic.

Visibility

The Barracuda server agent is not something a user will actually see or select to use; it is actually a background process that takes over whenever a connection needs to go out from the appliance to a remote system.

If the administrator has routes configured and a server agent installed the system will take advantage of this and proxy the traffic through the server agent. A user will be unaware that a server agent is proxying his or her traffic. When no server agent is installed, the Barracuda SSL VPN will continue to make direct connections to its target host.

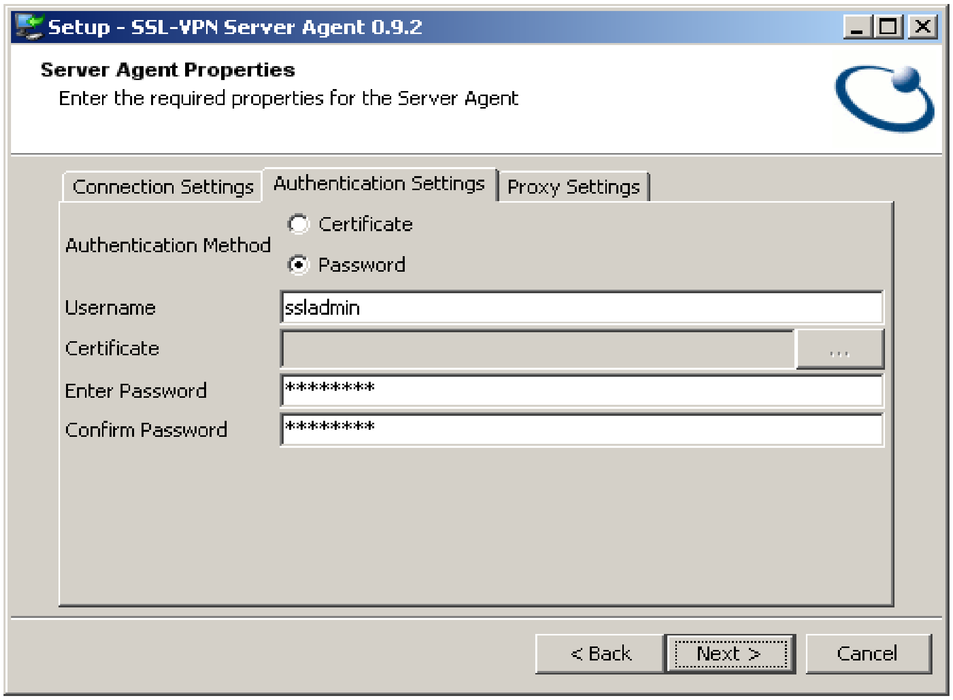
The server agent is strictly an administrator feature to help reassurance of security; its activation affects all resources.

Installing the Server Agent Client

Before any routing can begin the server agent client needs to be installed on a machine. This machine should be sufficiently placed so that the destined routes can be reached. As the diagram above shows, the client is on a machine which is inside the secured LAN this allows the server agent to access any resource inside the organization's network.

1. Select the appropriate **Download Client** action from the **Server Agent** page (**Manage System > Advanced > Server Agents**), this example uses the Windows client:
2. The client file will need to be saved to an appropriate place. Once done the extracted file should be executed.
3. Once the wizard has started and the license agreed a destination folder needs to be specified.

4. The next step is defining the **Server Agent** properties:



Setup - SSL-VPN Server Agent 0.9.2

Server Agent Properties

Enter the required properties for the Server Agent

Authentication Method ○ Certificate ● Password

Username ssladmin

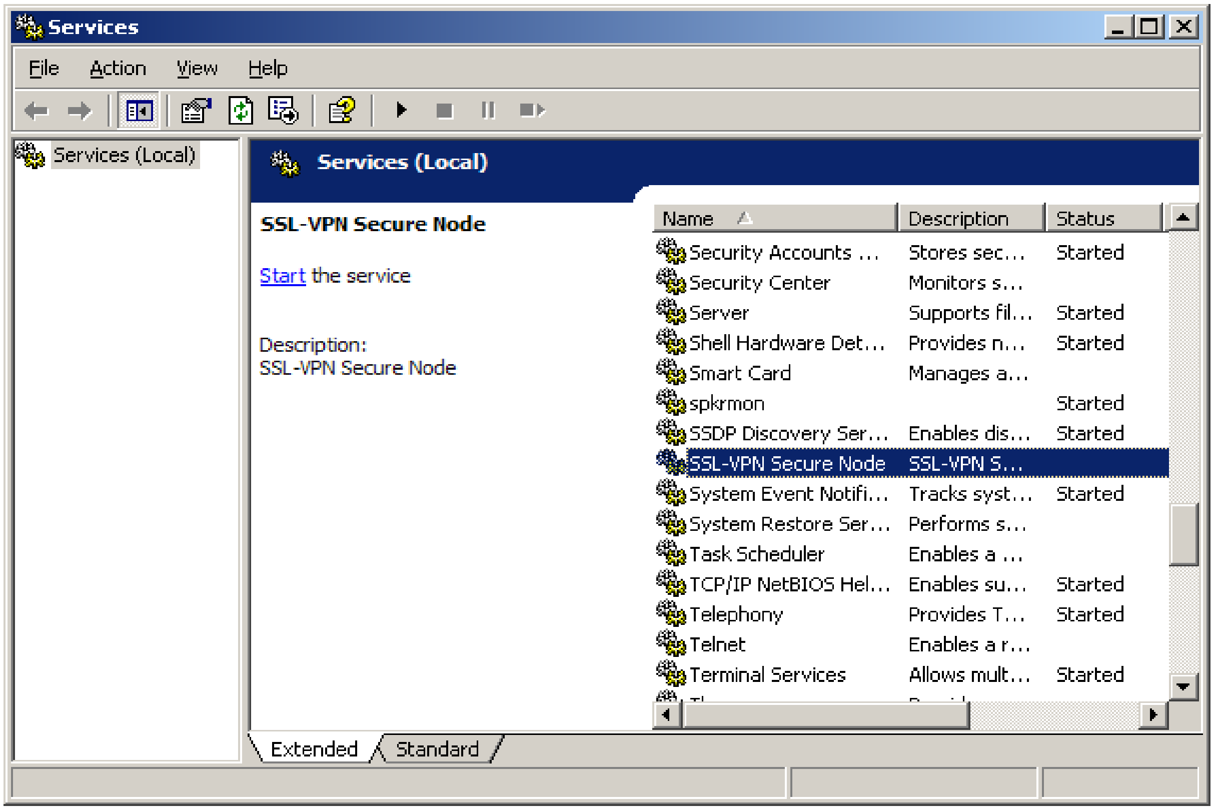
Certificate

Enter Password *********

Confirm Password *********

- Host: The hostname of the Barracuda SSL VPN to maintain communication with
- Port: The listening port of the Barracuda SSL VPN
- Authentication Method: Certificate or Password.
- Username: Username of a user that can access the server agent
- Certificate: If certificate has been chosen as the authentication method then this will be accessible. Browse to the appropriate certificate
- Password: If Password has been chosen as the authentication method then this will be accessible. Key in the password associated with the user. For a higher level of security a certificate can be used instead of a simple password.
- Confirm Password: Confirmation of above password

5. Once installed the client needs to be started. This is run as a process and so for Windows you need to start the Barracuda server agent service (**Control Panel > Administrative Tools > Services**).



SSL-VPN Secure Node

Start the service

Description:
SSL-VPN Secure Node

Name	Description	Status
Security Accounts ...	Stores sec...	Started
Security Center	Monitors s...	
Server	Supports fil...	Started
Shell Hardware Det...	Provides n...	Started
Smart Card	Manages a...	
spkrmon		Started
SSDP Discovery Ser...	Enables dis...	Started
SSL-VPN Secure Node	SSL-VPN S...	
System Event Notifi...	Tracks syst...	Started
System Restore Ser...	Performs s...	
Task Scheduler	Enables a ...	
TCP/IP NetBIOS Hel...	Enables su...	Started
Telephony	Provides T...	Started
Telnet	Enables a r...	
Terminal Services	Allows mult...	Started

The server agent service will now be running. If successfully configured the client should successfully register with the appliance and appear in the Server Agents page.

Server Agent Interface

The main **Server Agent** page (**Manage System > Advanced > Server Agents**) provides information on all successfully registered clients.

Chapter 10

Authentication Schemes

Authentication is the means of verifying a user's identity; this can be in the form of a password or a key/code. To allow for greater security the Barracuda SSL VPN uses authentication schemes to provide a multiple staged authentication process.

Authentication Schemes

An authentication scheme is simply a container for any number of authentication modules, such as One-Time Password (OTP), passwords, and certificates. This approach means that multi-tiered authentication can easily be implemented and even linked to existing authentication systems. The authentication scheme is then used as the basis of the login policy. The Barracuda SSL VPN allows for more than one of these schemes to be created and used.

All authentication schemes defined are visible from **Manage System > Access Control > Authentication Schemes**, and are listed in order of priority.

The following types of authentication can be used to control the level of access to a module:

Authentication	Type	For More Information:
Client Certificate	Primary/Secondary	*page 91*
IP Address	Primary/Secondary	*page 92*
Password	Primary/Secondary	*page 92*
PIN	Primary/Secondary	*page 93*
Public Key	Primary/Secondary	*page 93*
RADIUS	Primary/Secondary	*page 95*
OTP (One-Time Password)	Secondary	*page 96*
Personal Questions	Secondary	*page 97*

The above table also shows where an authentication module can be placed in relation to other modules. Any module marked above with primary means that it can be positioned first in an authentication scheme, while any module defined as secondary cannot be first in a scheme. Most of the Authentication Modules can be positioned anywhere first or second. Within the application itself, only those that cannot be first are marked.

The authentication scheme system enforces this by disallowing a secondary scheme to be positioned at the top of the chain.

When a user starts the authentication process they first have to enter a username. Once the username is submitted, checks are made to determine the correct authentication method to be used. This approach allows for different authentication methods to be used for different groups of users. For example, users attached to a *Sales* policy may only have to enter a username and password, whereas Sales Management may be attached to a policy that uses a password and PIN authentication scheme.

Note: If only one authentication scheme is configured on the system and only one user database is configured, then users will be prompted for their username and password on the same screen. If more than one authentication scheme is configured they will be prompted for username (and user database if more than one is in use). Once accepted another page will prompt for the password.

The built in authentication schemes allow those wanting to build a single, double or even a triple factored process to do so with ease. If only the default authentication scheme has been defined, the **Login** page presented to the user will have:

- Language selection
- Username entry

- Password entry

Where more than one authentication scheme has been defined, the first Login page will have:

- Language selection
- Username entry

Once the **Login** button is selected a second page is presented to the user where it is possible to choose an Authentication Scheme by clicking the **here** link. This action will load the schemes page where any defined scheme is selectable. When selected with the **OK** button the user is returned back to the **Login** page with the selected Authentication Scheme activated.

SSL Client Certificate Authentication

SSL client certificate authentication can be seen as the next progression in the authentication modules. It is more secure than the previous modules but requires a little more configuration. To some degree, client certificate authentication is an automatic authentication process requiring minimal interaction from the user. All the user is required to do is to install the certificate into the browser the first time that it is installed and then just select that certificate when prompted on future log on attempts. Everything else is performed by the browser and server.

A certificate is generated and validated before being imported into the client's browser. When this browser connects to the appliance the two begin instantly exchanging secure information to try and identify one another. The browser uses this certificate as a means of authenticating itself to the server. The server, aware of the provided certificate, is able to verify the client and automatically grant authentication.

Since a unique certificate can be assigned to each user, client certificates can provide a very secure means of access. Unlike the previous authentication methods, client certificates requires a bit more configuring but this only has to be done once. The general process is highlighted below.

- Enable authentication
- Create a CA
- Create client certificate (s)
- Import certificate (s) into browser

The certificate is tied into the browser which means that anyone using this machine can log into the system if they are using the same user account on the local machine. A primary authentication module should be used in conjunction with client certificate authentication such as password authentication to tighten access.

Before all these however, an authentication module should be available, which has client certificates included. Once these are all done, using certificates is a simple process.

1. All the administrator needs to do is enable the authentication scheme. A user selecting this scheme will force the browser to begin using the certificate to authenticate itself.
2. Once the authentication process begins the **Choose a digital certificate dialog** will appear. Select the appropriate certificate you wish to use then *OK* or *Cancel* if you do wish to use any.
3. If successful a message is displayed showing that the SSL client certificate is valid and the client will now be able to access the system.

IP Address Authentication

IP authentication relies on the physical address of a client machine and is able to determine the validity of a user even before the login page is displayed. This type of authentication ties the user to a specific IP address.

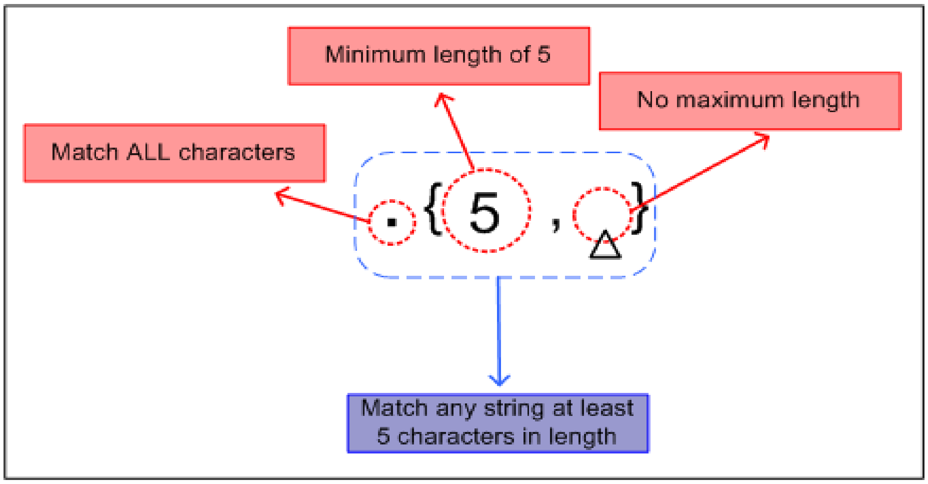
The authorized IP address is set in the **Manage System > Access Control > Accounts** page. It is this IP address that will be looked at when the user logs in. If the user's machine and authorized IP do not match, the user will be unable to log into the system. The default authorized IP is (*) which allows a user to log in from any machine.

Password Authentication

Password authentication is the most commonly used authentication scheme and it is the simplest and easiest to configure.

The length, format and expiration of passwords are all configurable, however initially these parameters are defaulted and whenever the administrator creates an account a password must be attached.

The structure of an account password is based on regular expressions and is defaulted to, **.{5,}**, which defines a password with a minimum size of 5 characters. This expression is detailed in the diagram below:



The security function password structure is built around regular expression syntax. Any valid regular expression can be used to parse the password. Some examples are given below:.

Expression	Meaning
X(n)	X exactly n number of times
X(n,m)	X between n and m times
.[^\s]{n,m}	Any character except whitespaces, with a length of between n and m number of characters
\w[n,m]	Word character [a-z, A-Z,_,0-9] between n and m

For more information, see *Regular Expressions* on page 113.

PIN Authentication

PIN Authentication is something all users with a bank account will already be familiar with. Again this is a standard Authentication Module and, much like a password, a user is expected to authenticate themselves with their private number.

The PIN itself can be as long or as short as the administrator defines and alerts to change this value periodically can also be configured. The administrator can also allow the user to set their own PIN when they first login. When combined with an Active Directory user database, PIN Authentication can prevent the locking of user accounts by dictionary attacks.

Public Key Authentication

Public key authentication is one of the most secure of authentication methods; not so much because of its secure authenticating process, but rather the authenticating identity used in the process can be stored on a removable USB key device.

Having a hardware medium which maintains the identity file adds a dimension of security that standard authentication processes do not have. No longer do passwords have to be juggled in someone's head or written down on a piece of paper but can be carried around and taken away with the user.

When the user accesses the system to login with public key authentication a random ticket is generated by the system. It is this ticket or token that is used to authenticate the user. The client side private key is used to sign the ticket. This ticket is then sent to the server. On receipt the server uses the corresponding public key to validate the signature against the token. If the signature is valid the user is then successfully authenticated.

This process can only take place if the user has their authentication key available and if that key is stored on a removable USB key then only the person with that USB key can actually log into the system. Unwarranted attempts are futile as the identity file is unique to each user.

Configuration

Configuring public key authentication is a simple two step process. All that is needed is an authentication scheme with public key authentication and then providing each user with their identity file, this step is detailed in the next section **Identity Creation**. From here all a user needs to do is log into the system.

1. The authentication key scheme should be selected at login.
2. The public key authentication method automatically begins to search for identity files across all the external drives including `C:\`*`HOME`* where *HOME* represents the user's home drive. Any files found are collated together. Using the **Use a known authentication key** option the user can then proceed to select the appropriate key file he or she wishes to use. The corresponding passphrase must also be supplied.

If however the key file is stored anywhere else the system will be unable to locate this file. The user will have to use the **Use an authentication key** option and manually locate the file.

If successful the user will be logged into the system.

An authentication key is the entity which uniquely identifies the user it is associated with. The key is used to sign the ticket the system produces at log on. To secure the key even further it is highly recommended that once a key is generated it is stored on the user's USB key.

A key can be created both by the administrator, from the **Manage System**, and the user from the **Manage Account**. In this section we detail both processes.

Creation from System

The administrator can initialize the key for a user and can continue to reset the key.

1. From the Accounts page (**Manage System > Access Control > Accounts**) click the **More…** button against the user. Select the *Generate Authentication Key* action from the list.
2. The system asks for a passphrase to encrypt the identity. When a passphrase has been supplied pressing the **Generate** button will create a key encrypted by the passphrase
3. The system provides the key in a zip file. This should be stored on to a secure location and the identity files extracted and given to the appropriate user. Barracuda Networks recommends that the user store the key file onto a USB key for greater security.

It is this key that will be used to authenticate the user during public key authentication.

Creation from Account

The user can also configure their identity. In fact the Super User, by using **Reset Authentication Key** can force users to create their own identities.

1. Select the **Update Authentication Key** action.
2. This takes us to the **Update Identity** window. From here the user's identity can be updated. As a security measure the user must also provide their account password. The system requires the new passphrase associated with this new identity. Once satisfied clicking the **Generate** button will create the new identity file.
3. As before the key is stored within a zip file. This should be stored, the key file extracted and stored on a USB key. When the user logs into the system, it is this identity the authentication module will ask for.

Resetting the Key

The administrator can force each user to define their own key when they first login to the Barracuda SSL VPN using public key authentication. Selecting this when a new account is created is a great way to encourage users to configure and manage their identities and other security passwords.

For reset to work correctly, the public key authentication must be in a scheme with at least *two* authentication modules, with the public key NOT positioned as the primary module.

These actions must be performed by the administrator.

1. From the Accounts page (**Manage System > Access Control > Accounts**) press the **More…** button against the user you wish to reset an authentication key for. From the **Action** list select the **Reset Authentication Key** action.
2. The system displays a warning message clarifying the action about to be performed. Selecting *Yes* will continue with the reset.
3. Now when the user next logs into the system they will be presented with the first authentication method and if successful, the second authentication method (authentication key) will not ask for a key but rather force the user to generate a new one

Much like before the identity will need to be safely stored on a secure medium such as a USB key. The user will be logged into the system and will now posses a new identity which will need to be presented the next time they log in.

Configuring Public Key

The Public Key configuration page can be accessed from **Manage System > Advanced > Configuration > Key Authentication**.

- **Allow User to Create Initial Authentication Key**: The administrator has the option of creating keys for the entire user base from the **Edit Accounts** page; this option however alleviates this need by forcing the users themselves to create their own key files at login time. If the user chooses key authentication the system will force the creation of a key.
- **Enforce Password Security Policy**: Enforce that passphrase conforms to the password policy under (**Manage System > Advanced > Configuration > Password Options**).

Import Authentication Key

This function allows for an already existing public key to be imported into the Barracuda SSL VPN as a user Authentication Key. This action can be performed by any users who have account editing privileges.

When the appliance scans a device such as a USB key, it tries to find the authentication key. This key should be in the root directory of the device in a sub-folder called **.sslvpn-ids**. For the external device to operate as required, the public key file must always be in this folder; for example, `E:\.sslvpn-ids\myPublicKey.pub.`

1. From the Accounts page (**Manage System > Access Control > Accounts**) click the **More…** button against the user you wish to reset an identity for. From the **Action** list select the *Import Authentication Key* action.
2. Simply locate the `*.pub` file that you wish to import using the file system **Browse** button.
3. Once the file is chosen simply use the **Upload** button to import the authentication key.

RADIUS Authentication

The RADIUS Authentication method (Remote Authentication Dial In User Service) is an AAA (authentication, authorization and accounting) protocol. It allows for a RADIUS server to be queried by the appliance to validate a user's login request.

As the RADIUS server is outside of the control of the appliance, certain actions will not be available such as create or edit. This also has an effect on how this module is used in an authentication scheme. As a username and password are supplied it can be used as either a primary or secondary form of authentication. It can also be combined with other modules, but of course care should be taken to ensure that the selected modules within an authentication scheme are compatible.

The prerequisite for this authentication method is an operating RADIUS server

The server must be available and be populated with all users that will be used for authentication; the appliance is merely interfacing with the results of the server and plays no part in the management of the server content.

Once the scheme is activated all that is required is the configuration of the appliance to locate the server. Once everything has been configured properly the user will be able to select **RADIUS** as the authentication scheme to use. When the user's authentication details are supplied, the appliance forwards these onto the RADIUS server. The authentication result returned determines whether the user is authenticated into the system.

Configuring RADIUS

The configuration parameters are vital to the success of the scheme. If any of these parameters are incorrect, the appliance will be unable to communicate with the RADIUS server. Make sure that you configure these parameters correctly. The parameters are accessible from (**Manage System > Advanced > Configuration > RADIUS**).

OTP Authentication

One-Time-Password (OTP) authentication can be seen as an extension to password authentication. With password authentication the configured password is used numerous times until a defined expiration date is hit and the password needs to be changed. The expiration tends to be around a month or so but with OTP Authentication, the password can only be used once and once only - not only that, the expiration of the password is measured in minutes and not days so even the OTP's existence is short lived.

Any email-enabled device can receive OTPs, meaning that your passwords may be sent by email to your inbox. Alternatively, if support for SMS through email is available in the country where the Barracuda SSL VPN resides, you can configure the OTP feature to send the password through email to an SMS gateway which will relay the message on to the user's cell phone.

SMS over Email

By using a third party service known as an SMTP/SMS gateway, the Barracuda SSL VPN can be configured to relay OTPs to your users' cell phones.

To Relay OTPs to Your Users' Cell Phone:

1. Pick a third party SMS gateway provider in your country and sign up for their Email to SMS service.
2. Configure your SMTP settings in (**Manage System > Advanced > Configuration > SMTP**) and ensure that the Barracuda SSL VPN can talk to your corporate mail server.
3. Navigate to the **One-Time Password** section and set the method of password delivery to.
4. Navigate to the **SMS** section and enter the email address associated with the provider of your choice in the **SMS Gateway Address** field.

The user will need to enter their cell phone number as a user attribute under (**Manage Account > My Account > Attributes**) to receive messages through SMS.

Personal Questions Authentication

This is another commonly used authentication module. Its simplicity and ease of use make this a favorite choice amongst multi-factored schemes.

Personal authentication relies on predefined personal information about the user. A set number of questions are managed by the system and when utilized the system takes a question and presents this to the user. A comparison is made between the current answer and the preset answer; if a match is made the user is authenticated.

This authentication method is a secondary option only and must work in conjunction with a more secure primary module.

The system uses in-built user attributes to define and store a set of five questions. These cannot be amended nor can a user add additional questions to these.

Hardware Token Authentication

Two-factor or multi-factor authentication is considered to be strong authentication today and this methodology combines the principle of ‘something you know’ with ‘something you have’. In terms of usage within the Barracuda SSL VPN, your users know their username/password, and will also have a hardware authentication key fob.

This is considered strong authentication because in order to compromise the system, an attacker must get access to the user’s password along with the physical authentication device that the user carries. Given that most intrusion attempts are conducted from remote locations, this makes the job of an intruder much more difficult.

We do not recommend the use of weak authentication methods such as password-only. The authentication methods are designed in such a way that you can layer them as you see fit.

Specific implementation details regarding each of the following methods are available from the main Barracuda Networks documentation page at *http://www.barracuda.com/documentation*.

SafeNet iKEY 2032 Configuration

This product takes the form of a small USB key device that is small enough to be carried as part of a bunch of keys on a chain. It uses SSL client certificate authentication to present a certificate to the appliance, making textbook use of the *something you know, something you have security* methodology by combining a secret passphrase with the certificate on the device.

The SafeNet iKey 2032 requires a special utility (CIP Utilities) installing on the client PC and this software deals with certificate management as well as performing tasks such as requesting passphrase when connecting to secure websites. When the device is inserted into the USB slot, the client software loads the certificate into the Windows certificate store where it may be accessed by the client’s browser and presented to the appliance.

Aladdin eToken PRO Configuration

Similarly to the SafeNet iKey, the Aladdin eToken PRO makes use of SSL client certificate authentication to present a digital certificate to the Barracuda SSL VPN server. The only real difference from the perspective of the administrator is that the eToken software itself that requires installing manually on the client PCs.

RSA SecurID Authentication Manager

The Barracuda SSL VPN is able to make use of SecurID authentication using the RADIUS feature to provide communication between the RSA server and the appliance.

When combined with the Active Directory user database this method is especially powerful as account management may be centrally managed with both the appliance and RSA Authentication Manager reading accounts from your Active Directory domain.

VASCO Digipass Token Configuration

The Barracuda SSL VPN can be configured to authenticate to a VASCO server using the RADIUS feature of the product. Note that VASCO do not currently include a RADIUS server with their product; therefore you will need to use an external RADIUS server (i.e. FreeRADIUS) to provide the RADIUS component of this solution

Secure Computing SafeWord

The Barracuda SSL VPN appliance can be configured to authenticate to a SafeWord server using the RADIUS feature of the product. Note that SafeWord requires an Active Directory database and Internet Authentication Server (IAS) installed on the Domain Controller.

Chapter 11

Monitoring the Barracuda SSL VPN

This chapter describes the monitoring tasks you can perform from the web interface.

Note

For more detailed information about a specific page in the web interface, view the online help by clicking the question mark icon on the right side of the interface.

Monitoring Tasks

This section describes the monitoring tasks you can perform from the web administration interface and from the front panel of the Barracuda SSL VPN, and contains the following topics:

Viewing Performance Statistics

The **BASIC > Status** page provides an overview of the health and performance of your Barracuda SSL VPN, including:

- Traffic and policy statistics, such as the amount of overall email traffic and how many messages have triggered a particular policy category.
- The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values will fluctuate based on the amount of traffic that is being handled, but if any setting remains consistently in the red for a long period of time, please contact Technical Support.

Setting Up SNMP Alerts

The Barracuda SSL VPN 450 and higher offers the ability to monitor various settings through SNMP, including:

- Traffic and policy statistics, such as:
    - the amount of overall traffic
    - number of messages that triggered a particular policy category
    - number of messages currently in the indexing queue.
- The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load.

Setting Up Emailed System Alerts

The **BASIC > Administration** page allows you to configure the Barracuda SSL VPN to automatically email notifications to the addresses you specify. To enter multiple addresses, separate each address with a comma.

System alerts notify you when:

- Your Energize Update subscription is about to expire
- New firmware updates are available
- Your system is low on disk space

Viewing System Tasks

The **ADVANCED > Task Manager** page provides a list of tasks that are in the process of being performed, and displays any errors encountered when performing these tasks.

Some of the tasks that the Barracuda SSL VPN tracks include:

- Imports of historical emails
- Exports of archived messages
- Configuration restoration

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy.

The **Task Errors** section will list an error until you manually remove it from the list. The errors are not phased out over time.

Understanding the Indicator Lights

The Barracuda SSL VPN has five indicator lights on the front panel that blink when the system processes any message.

Figure 11.1 displays the location of each of the lights.

Figure 11.1: Indicator Lights

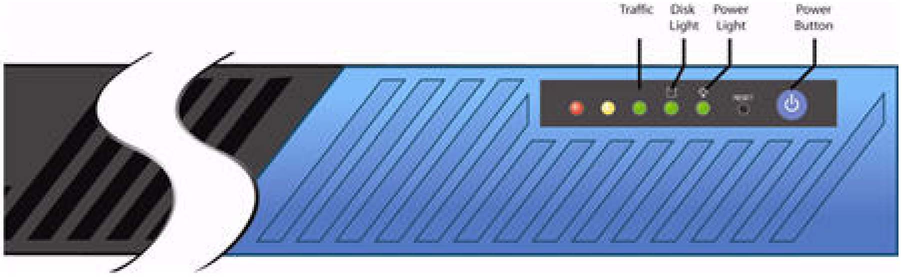


Table 11.1 describes each indicator light.

Table 11.1: Description of the Indicator Lights

Light	Color	Description
	Red	*Reserved for future use*
	Yellow	*Reserved for future use*
Traffic	Green	Blinks when the Barracuda SSL VPN processes traffic.
Data I/O	Green	Blinks during data transfer.
Power	Green	Displays a solid green light when the system is powered on.

Chapter 12
Maintenance

This chapter provides general instructions for general maintenance of the Barracuda SSL VPN.

Maintenance Functions

This section describes how to manage and maintain your Barracuda SSL VPN using the web administration interface, and contains the following topics:

Backing up and Restoring Your System Configuration

The **ADVANCED > Backup** page lets you back up and restore the configuration of your Barracuda SSL VPN. You should back up your system on a regular basis in case you need to restore this information on a replacement Barracuda SSL VPN or in the event your current system data becomes corrupt.

If you are restoring a backup file on a new Barracuda SSL VPN that is not configured, you need to assign your new system an IP address and DNS information on the **BASIC > IP Configuration** page.

Note the following about the backup file:

- Do not edit backup files. Any configuration changes you want to make need to be done through the web interface. The configuration backup file contains a checksum that prevents the file from being uploaded to the system if any changes are made.
- You can safely view a backup file in Windows WordPad or Microsoft Word. You should avoid viewing backup files in Windows Notepad because the file can become corrupted if you save the file from this application.
- The following information is not included in the backup file:
    - System password
    - System IP information
    - DNS information

Updating the Firmware of Your Barracuda SSL VPN

The **ADVANCED** > **Firmware Update** page allows you to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version.

If you have the latest firmware version already installed, the **Download Now** button will be disabled.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours.

Updating the Definitions from Energize Updates

The **ADVANCED > Energize Updates** page allows you to manually update the virus, application and security definitions used on your Barracuda SSL VPN, as well as change the interval at which the Barracuda SSL VPN checks for updates.

We recommend that the **Automatically Update** setting be set to *On* so your Barracuda SSL VPN receives the latest rules as soon as they are made available by Barracuda Central.

Replacing a Failed System

Before you replace your Barracuda SSL VPN, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem.

In the event that a Barracuda SSL VPN fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call Barracuda Networks Technical Support and arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old Barracuda SSL VPN back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks Technical Support can provide details on the best way to return the unit.

Barracuda Networks
3175 S. Winchester Blvd
Campbell, CA 95008

attn: RMA # <*your RMA number*>

Note To set up the new Barracuda SSL VPN so it has the same configuration as your old failed system, first manually configure the new system's IP information on the **BASIC > IP Configuration** page, and then restore the backup file from the old system onto the new system. For information on restoring data, refer to *Backing up and Restoring Your System Configuration* on page 106.

Reloading, Restarting, and Shutting Down the System

The **System Reload/Shutdown** section on the **BASIC > Administration** page allows you to shutdown, restart, and reload system configuration on the Barracuda SSL VPN.

Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can also perform a hard reset of the Barracuda SSL VPN by pressing the **RESET** button on the front panel of the system. Caution should be used when pressing the **reset** button, however, since doing so while the Barracuda SSL VPN is in a configuration update or other task can corrupt the system.

Using the Built-in Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides various tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda SSL VPN.

For example, you can test your Barracuda SSL VPN's connection to the Barracuda Networks update servers to make sure that it can successfully download the latest Energize Update definitions. You can also ping other devices from the Barracuda SSL VPN, perform a traceroute from the Barracuda SSL VPN to any another system, and execute various other troubleshooting commands.

Rebooting the System in Recovery Mode

If your Barracuda SSL VPN has a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available at the reboot menu to return your system to an operational state.

Before you use the diagnostic and recovery tools, do the following:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your Barracuda SSL VPN and run a memory test or perform a complete system recovery, as described below.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda SSL VPN.
2. Reboot the system by doing one of the following:
   - Click **Restart** on the **BASIC > Administration** page.
   - Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn back on the system.

   The Barracuda splash screen displays with the following three boot options:

   ```
   Barracuda
   Recovery
   Hardware_Test
   ```
3. Use your keyboard to select the desired boot option, and press **Enter**.

   You must select the boot option within three seconds of the splash screen appearing. If you do not select an option within three seconds, the Barracuda SSL VPN defaults to starting up in the normal mode (first option).

   For a description of each boot option, refer to *Reboot Options* on page 109.

Note

To stop a hardware test, reboot your Barracuda SSL VPN by pressing Ctrl-Alt-Del.

Reboot Options

Table 12.1 describes the options available at the reboot menu.

Table 12.1: Reboot Options

Reboot Options	Description
Barracuda	Starts the Barracuda SSL VPN in the normal (default) mode. This option is automatically selected if no other option is specified within the first three (3) seconds of the splash screen appearing.
Recovery	Displays the Recovery Console where you can select the following options: • **Perform filesystem repair**—Repairs the file system on the Barracuda SSL VPN. • **Perform full system re-image**—Restores the factory settings on your Barracuda SSL VPN and clears out all configuration information. • **Enable remote administration**—Initiates a connection to Barracuda Central that allows Barracuda Networks Technical Support to access the system. Another method for enabling this troubleshooting connection is to click **Establish Connection to Barracuda Networks** on the **ADVANCED >Troubleshooting** page. • **Run diagnostic memory test**—Runs a diagnostic memory test from the operating system. If problems are reported when running this option, we recommend running the Hardware_Test option next.
Hardware_Test	Performs a thorough memory test that shows most memory related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. Reboot your Barracuda SSL VPN to stop the hardware test.

Appendix A
About the Hardware

This appendix provides hardware information for the Barracuda SSL VPN. The following topics are covered:

Hardware Compliance

This section contains compliance information for the Barracuda SSL VPN hardware.

Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user in encouraged to try one or more of the following measures:
   - Reorient or relocate the receiving antenna.
   - Increase the separation between the equipment and the receiver.
   - Plug the equipment into an outlet on a circuit different from that of the receiver.
   - Consult the dealer on an experienced radio/ television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.

Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Appendix B

Regular Expressions

The Barracuda SSL VPN allows you to use regular expressions when creating Content Filtering policies. Regular Expressions allow you to flexibly describe text so that a wide range of possibilities can be matched.

When using regular expressions:

- Be careful when using special characters such as |, *****, '**.**' in your text. For more information, refer to *Using Special Characters in Expressions* on page 114.
- All matches are not case sensitive.

Table B.1 describes the most common regular expressions supported by the Barracuda SSL VPN.

Table B.1: Common Regular Expressions

Expression	**Matches...**
Operators	
*	Zero or more occurrences of the character immediately preceding
+	One or more occurrences of the character immediately preceding
?	Zero or one occurrence of the character immediately preceding
|	Either of the characters on each side of the pipe
( )	Characters between the parenthesis as a group
Character Classes	
.	Any character except new line
[ac]	Letter 'a' or letter 'c'
[^ac]	Anything but letter 'a' or letter 'c'
[a-z]	Letters 'a' through 'z'
[a-z.]	Letters 'a' through 'z' or 'A' through 'Z' or a dot
[a-z\-]	Letters 'a' through 'z' or 'A' through 'Z' or a dash
\d	Digit, shortcut for **[0-9]**
[^\d]	Non-digit
\a	Digit, shortcut for **[0-9]**
\w	Part of word: shortcut for **[A-Za-z0-9_]**
[^\w]	Non-word character

Table B.1: Common Regular Expressions

Expression	Matches...
\s	Space character: shortcut for **[\n\r\t]**
[^\s]	Non-space character
Miscellaneous	
^	Beginning of line
$	End of line
\b	Word boundary
\t	Tab character

Using Special Characters in Expressions

The following characters have a special meaning in regular expressions and should be prepended by a backward slash (\ ) when you want them interpreted literally:

Table B.2: Special Characters

.	$
[	(
]	)
\	|
*	^
?	@

Examples

Table B.3 provides some examples to help you understand how regular expressions can be used.

Table B.3: Regular Expressions

Example	Matches...
viagra	viagra, VIAGRA or vIaGRa
d+	One or more digits: 0, 42, 007
(bad|good)	letters 'bad' or matches the letters 'good'
^free	letters 'free' at the beginning of a line
v[i1]agra	viagra or v1agra
v(ia|1a)gra	viagra or v1agra
v\\|agra	v|agra
v(i|1|\\|)?agra	vagra, viagra, v1agra or v|agra

Table B.3: Regular Expressions

Example	Matches...
FREE	*FREE*
FREE V.*GRA	*FREE* VIAGRA, *FREE* VEHICLEGRA, etc

Appendix C

Limited Warranty and License

Limited Warranty

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.

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 the 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.

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 IS 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.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE 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, documentation, whether on disk, 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 License 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 Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.

2. Permitted License Uses and Restrictions. This License 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 and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.

3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.

4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

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, 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.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

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. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B)

YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively "Barracuda Networks"), grants to the end-user ("Customer") a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the "Energize Update Software"). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software 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 Customer; Customer's use of the Energize Update 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 Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's 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 the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;
ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, "Energize Update Software" shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customers expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph "(c)" of the "Commercial Computer Software - Restricted Rights" clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the "Technical Data-Commercial Items" clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update 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 Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other "open source" license agreements. The GNU 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.

GNU GENERAL PUBLIC LICENSE, (GPL) Version 2, June 1991

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, whethergratis 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.

GNU GENERAL PUBLIC LICENSE 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 TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda 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 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 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 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, 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 products may include programs that are covered by the Apache License or other Open Source license agreements. 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.

Apache License
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.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (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.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Source Code Availability

Per the GPL and other "open source" license agreements the complete machine readable source code for programs covered by the GPL or other "open source" license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of $100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We will mail the packaged source code for any program covered under the GPL or other "open source" license.

Index

Barracuda Networks Technical Documentation

RECLAIM YOUR NETWORK™