

The Barracuda SSL VPN allows you to define and control the level of access that your external users have to specific resources inside your internal network. For users such as road warriors or network administrators that require general or more widespread network access, the Barracuda SSL VPN also provides full network connectivity via the **Barracuda Network Connector**.

Available for systems running Linux, Macintosh or Microsoft Windows, operation of the Barracuda Network Connector is transparent to the user since all configuration data is maintained on the server. Specific authorized users can be provided with complete TCP/UDP protocol access to the entire network in a manner similar to what is provided by IPsec, enabling the remote user to perform all standard functions, including mounting drives, accessing network shares and moving files, just as if they were physically inside the organization.

The Barracuda Network Connector consists of two components: a *server-side* component which just needs to be enabled to allow access by your designated users, and a *client-side* component that, when installed onto the remote system, connects to the server interfaces.

The remote and protected networks each continues to function independently within its own subnet. When a remote client connects to the Barracuda SSL VPN, a secondary IP address is assigned to it that is from the same (internal) range as that used by the Barracuda SSL VPN, and is what is used by the Barracuda Network Connector client when determining which routes to select in order to connect to various systems -- requests to the protected LAN will connect with the Network Connector IP address through the server into the protected network, while connection requests to the Internet will be left alone to continue connecting and functioning via the standard Internet IP address of the remote system, without going through the Barracuda SSL VPN at all.

System Requirements

The Barracuda Network Connector is available for use with the following operating systems:

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



Requires Administrative Account to Install

In order to install and run the Barracuda Network Connector service on a client machines, you will require the use of an account with administrative permissions in Windows.



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.

Configuring a New Network

Network creation and management is done from the **RESOURCES > Network Connector** page, by the *ssladmin* administrative user. Make sure that *ssladmin* is logged in on the **Manage System** (not *Manage Account*) mode, so that system-wide access can be configured.

1. From the users' access interface (typically located on port 80 or 443), log in as *ssladmin* and verify that you are in the **Manage System** mode (you should already be in this mode when you log in).
2. Navigate to the **RESOURCES > Network Connector** page. If you see *My Network Connector* instead of just *Network Connector*, or if you do not see the page at all, then you may need to switch into **Manage System** mode. Do so by clicking on the **Manage System** link in the upper right of the Web interface, just underneath the *ssladmin* username display.
3. Click on the **Configure Network** button to bring up the **Create Network Configuration** page. You will need to configure both the **Server Information** and **Policy Selection** sections:
4. In the **Server Information** section, configure the network information that will apply to your remote users:
 - a. The displayed **Network** and **IP Address** of the Barracuda SSL VPN are those already assigned to the Barracuda SSL VPN. The IP addresses distributed by the Barracuda Network Connector to remote systems must come from an IP address range that is accessible from the Network range displayed here.
 - b. In the **IP Address Range Start** and **End** fields, enter the first and last IP addresses of a DHCP range that can be assigned to remote systems. All Network Connector IP addresses will be assigned from a DHCP range that is derived from this information. To prevent IP conflicts, the specified range **cannot** be a part of any other existing DHCP range.
 - c. The default values for **Domain Name** and the **Primary DNS Server** are derived from the values already assigned to the Barracuda SSL VPN. The Domain Name configured here will be used whenever a requested system is identified only by its system name without the domain portion (i.e., not as an FQDN), and the Primary DNS Server will be used to resolve all supplied hostnames. If you want your remote users to default to using a different domain name and DNS server, enter your desired values here.
5. In the **Policies** section, select one or more Policies that contain the users who will be allowed access to this particular Network Connector configuration. From the **Available Policies** area, choose the Policies to add to the **Selected Policies** area. Select the **Show Personal Policies** checkbox to be able to choose from all user-defined Policies as well.
6. Click **Save** when you are done. This will create a LAN entry in the **Server Interfaces** section, and a corresponding LAN Client entry in the **Client Configurations** section.
7. Create (or copy) and configure Client settings as needed. In particular, if you have remote users on more than one type of platform (e.g., Windows, Linux, and/or MacOS), then you should definitely have one client configuration for each platform. See the **Configuring Clients** section below for more information.
8. Further changes to either the server or client configurations must be made by clicking the **Edit** action for that particular configuration.

Configuring Clients

A default Client Configuration is automatically generated for every Server Interface that is created; however, you may need to edit this configuration to make suitable for the majority of your users. Additional Client Configurations may be required in some instances, such as for remote users on different platforms (e.g., Windows, Linux, and/or MacOS) that require different initialization commands. The easiest way to create additional Client Configurations is to create copies of the initial Client Configuration, and customize as needed.

1. From the **Client Configurations** section of the **RESOURCES > Network Connector** page, click on the **Edit** link associated with the LAN Client entry to bring up the **Edit Client Configuration** page.
2. In the **Details** section, enter how this configuration will be displayed to your users:
 - a. The **Name** identifies this particular Client Configuration. By default, the name will correspond to the name of the associated Server Interface.
 - b. If desired, enter a short **Description** for this configuration. This text will be visible to your users, and can help them determine which Client Configuration will be required for their particular situation.
 - c. The **Auto-Launch** setting determines whether a user logging into the Web interface of the Barracuda SSL VPN will simultaneously launch the Web version of the Barracuda Network Connector running with this configuration. This does not affect the ability of the stand-alone version of the Network Connector from also running with this particular Client Configuration.
3. The default values provided in the **Other** and **Routing** sections should not need to be changed for most sites.
 - a. The **Server Interface** identifies the network information that this Client Configuration is associated with. This should match the Server Interface that caused the creation of this Client Configuration.
 - b. The **IP Address** field should only be used when you expect *only one remote user to connect using this configuration*. If there is a value specified here, then the remote system that is connecting via the Barracuda Network Connector will always be assigned this IP address, regardless of any DHCP range that is set in the associated Server Interface.
 - c. If you wish to change the **Authentication Type** for the user of this Client Configuration, then select the desired method here.
 - d. In the **Routing** section, the **MTU** (Maximum Transmission Unit) setting should only be changed if your switch or firewall requires a non-standard setting; for example, ethernet jumbo frames may require larger values, whereas older equipment may need smaller values.
4. The **Commands** section is used to configure the initialization (**Up**) and sign-off (**Down**) commands for the remote system. There are Up and Down sections for each of the following three platforms: Microsoft Windows, Linux and Macintosh OS.
 - a. In the **Up Commands** area, enter the commands that you want the remote system to execute to prepare for *joining* the secured network. These can range from initializing environment variables, to adding network printers, to mapping of network drives.

Note: While you can still continue to add static routes with this method, starting with firmware version 2.0 you can now configure them automatically for all users in the **Published Networks** section of the Server Interface. See the section *Additional Server Configurations* below for more information.
 - b. In the **Down Commands** area, enter the commands that you want the remote system to execute when *leaving* the secured network. Typically, you will have a

corresponding Down Command for every Up Command that was configured, to reverse any actions that might have been taken.

5. The **Resource Categories** section is used to help group this Client Configuration with other Resources that your users frequently use. This Client Configuration will be available to your remote users on their *My Resources* page, under the Resource Category (or Categories) selected here. From the **Available Categories** area, select one or more (or all) Categories to add to the **Selected Categories** area. If you do not select any Resource Categories, then this Client Configuration will not be available from the users' *My Resource* page, only from their *My Network Connector* page.
6. In the **Policy Selection** section, select one or more Policies that contain the users who will be allowed access to this particular Network Connector configuration. From the **Available Policies** area, choose the Policies to add to the **Selected Policies** area. Select the **Show Personal Policies** checkbox to be able to choose from all user-defined Policies as well. If you wish to make this configuration available to all users, select and add the Everyone Policy.
7. Click **Save** when you are done. If you need to create another Client Configuration, you can do so in one of two ways:
 - a. Click on the **Copy** link to begin editing a copy of that configuration to save under a new Name.
 - b. Click on the **Create Client** button in the **Actions** section at the top of the page to start with a brand new configuration with all default settings.

Note: Exercise care when naming a Client Configuration, because once you have saved a Client Configuration, you *will NOT be able to change its Name*.
8. To install or download the Client Configuration, click on the **More ..** link in the Actions column for the configuration, and select the desired action.

Running the Service

Once created, the Barracuda Network Connector service is usually automatically activated on the server, so that all an authorized remote user needs to do to gain access to the protected network is to launch the Barracuda Network Connector client on their system. However, you can choose to manually disable the service if needed.

Server Activation

Activation (and deactivation) of the Barracuda Network Connector server interface is done from the **RESOURCES > Network Connector** page, by the *ssladmin* administrative user. Make sure that *ssladmin* is logged in on the **Manage System** (not *Manage Account*) mode, so that system-wide access can be configured.

1. From the **Server Interfaces** section of the **RESOURCES > Network Connector** page, click on the **Edit** link for the Server Interface to bring up the **Edit Server Interface** page.
2. In the **Details** section, set the **Auto-Launch** setting to your desired value:
 - **Yes** will cause the Barracuda Network Connector to be activated the next time the Barracuda SSL VPN server is restarted.
 - **No** will disable the Barracuda Network Connector service upon the next restart of the Barracuda SSL VPN server.
3. Click **Save** when you are done. Make sure to restart the server in order for your new setting to take effect.

Connecting a Client to the Barracuda SSL VPN

The client portion can be launched by the remote user in one of two ways:

- Directly from the Web interface of the Barracuda SSL VPN
- A executable client on one of the following platforms:
 - Microsoft Windows 7, Vista, XP or 2000
 - Macintosh 9.x, 10.x (Intel-based)
 - Linux 2.4 or higher with integrated TUN/TAP driver

From the Web Interface *(for any platform)*

1. Log in as the remote user, and navigate to the **RESOURCES > My Network Connector** page.
2. From the **Network Connector** section, click on the icon for the version of the client you wish to launch. To view more details about each available client, leave the cursor over the icon to bring up a small window that displays additional information. If you are in *List* mode, click on the **Launch** link in the **Actions** column.
3. The **Launching Network Connector** page will be displayed, and a security window may appear asking for authorization to connect to the remote site. Click **Yes** to continue. You may also get a security warning regarding the *AgentLauncher* application. If you do, click **Run** to continue.
4. Once you are connected, the Network Connector status window will appear, containing a running display of your connection status. If you click the **Hide** button to close the window, you can re-display it at a later time by right-clicking on the Network Connector icon in the System Tray, and selecting **Show Status**.
5. A secure connection should now be available from the remote system to the protected network, providing access to all authorized systems within.
6. To disconnect the secure session, select **Disconnect** from either the Network Connector status window, or from the Network Connector icon in the System Tray.

Microsoft Windows

1. Navigate to the **RESOURCES > Network Connector** page and click the **Download Windows Client** button. You will be prompted to either Run or Save the installer.
2. Launch the installer once the installation package downloads, and select all default settings as you continue through the installation. **Note:** On Windows XP and later, if you get warned about any compatibility issues during the install, click **Continue Anyway**.




Requires Administrative Account to Install

In order to install and run the Barracuda Network Connector service on a client machines, you will require the use of an account with administrative permissions in Windows.

3. Once installed, the Barracuda Network Connector is ready for use by any user on the remote system who is logged in through the Web interface of the Barracuda SSL VPN. To be able to run this client in *stand-alone* mode, or without requiring an

explicit login through the Web interface, a configuration file for the client must be downloaded and installed onto the remote system.

4. A Client Configuration File for the Barracuda Network Connector is required only when using the Barracuda Network Connector in stand-alone mode. To *download* or *install* a configuration file for the client:
 - a. Log back into the Web interface of the Barracuda SSL VPN and return to the **RESOURCES > Network Connector** page.
 - b. Display the **Network Connector** section in **List** mode by clicking on the ListView icon () in the upper right of the section.
 - c. Click on the **More ..** link in the Actions column for the client, and select the desired action. **Note:** When installing the configuration file, you may be presented with various warnings depending on the security level that is configured on your system. Accept the warnings as they appear in order to continue with the installation.

5. To **launch** the Barracuda Network Connector client:
 - a. Go to your system's **Start** button and select **Programs > Barracuda > Network Connector > Network Connector GUI**. A red network icon will appear in your System Tray.
 - b. Right-click on that icon and select **Connect**.
 - c. Enter your username and password when prompted, and click **OK**.
 - d. The icon will flash while attempting to establish a connection, and will turn green when a secure connection to the protected network is in place and ready for use.




Routes are not immediately published on Microsoft Windows systems

Due to restrictions imposed by Windows networking, the VPN routes are not instantly 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.

Macintosh OS

1. Navigate to the **RESOURCES > Network Connector** page and click the **Download Mac Client** button. You will be prompted to either Run or Save the installer (.dmg file).
2. Launch the installer once the installation package downloads, and select all default settings as you continue through the installation.
3. Once installed, the Barracuda Network Connector is ready for use by any user on the remote system who is logged in through the Web interface of the Barracuda SSL VPN. To be able to run this client in *stand-alone* mode, or without requiring an explicit login through the Web interface, a configuration file for the client must be installed on the remote system.
4. A Client Configuration File for the Barracuda Network Connector is required only when using the Barracuda Network Connector in stand-alone mode. To *download* or *install* a configuration file for the client:


- a. Log back into the Web interface of the Barracuda SSL VPN and return to the **RESOURCES > Network Connector** page.
 - b. Display the **Network Connector** section in **List** mode by clicking on the ListView icon () in the upper right of the section.
 - c. Click on the **More ..** link in the Actions column for the client, and select the desired action. **Note:** When installing the configuration file, you may be presented with various warnings depending on the security level that is configured on your system. Accept the warnings as they appear in order to continue with the installation.
5. To **launch** the Barracuda Network Connector client:
- a. Select **Finder > Applications > Network Connector**. A gray network icon will appear in the top right of your screen.
 - b. Click the network icon and choose **Connect LAN1 Client** (where *LAN1* may be a different network name, depending on how it was configured by *ssladmin*).
 - c. Enter your username and password when prompted, and click **OK**.
 - d. The icon will turn green once a secure connection to the protected network has been established.

Linux

No separate client software is needed to connect from Linux systems to the Barracuda Network Connector service, since most modern Linux distros already contain the required support in the **OpenVPN NetworkManager-openvpn** application. However, a configuration file must be installed in order for the system to connect to the Barracuda SSL VPN.

1. Install OpenVPN NetworkManager if it is not already installed on your system. Depending on your Linux distribution, you may need to do this via one of the following methods:
 - a. Using `sudo`:

```
$ sudo apt-get install network-manager-openvpn
```
 - b. While logged in as `root`:

```
# yum install NetworkManager-openvpnt
```
 - c. Alternate steps as required by your particular Linux distribution.
2. Download and save the Client Configuration File for the Barracuda Network Connector:
 - a. Log into the Web interface of the Barracuda SSL VPN and go to the **RESOURCES > Network Connector** page.
 - b. Display the **Network Connector** section in **List** mode by clicking on the ListView icon () in the upper right of the section.
 - c. Click on the **More ..** link in the Actions column for the client, and select the *Download client configuration file*.
 - d. Save and extract the downloaded file into a permanent location, such as `$HOME/Documents/OpenVPN`.
3. Configure the Network Manager applet on your Linux system. Exact steps may vary based on your particular Linux distribution, but the resulting settings should be equivalent.
 - a. Left-click on the Network Manager entry on your Linux system panel and select **VPN Connections > Configure VPN**.

- b. Click **Add**, and select **OpenVPN** as the connection type.
 - c. Supply the requested server information as appropriate:
 - Gateway – Hostname or IP address of your Barracuda SSL VPN
 - Type – Always select “Password with Certificates”
 - User name – Your username on the Barracuda SSL VPN
 - Password – Password for the specified username
 - User Certificate – Select and browse for your client.certificate
 - Certificate – Select and browse for your ca.crt
 - Private Key – Select and browse for the client.key
 - d. Click **Advanced**, and select the following options:
 - Use custom gateway port – If your server is accessed on a different port.
 - Use custom renegotiation interval – Should be selected and set to 0 to prevent reconnection attempts.
 - Use a TCP connection.
 - Use a TAP device.
 - If you do **not** want all Internet traffic from this system to be routed through the Barracuda SSL VPN:
 1. On the IPv4 Settings tab, select **Routes**
 2. Select **Use this connection only for resources on its network**
 3. Click **Ok**
 - Click **Apply** to save the configuration settings.
4. Initiate a secured connection through the Barracuda SSL VPN:
 - a. Left-click on the Network Manager entry on your Linux system panel and select **VPN Connections > Name-for-your-VPN-Connection**.
 - b. An animated icon will appear while the connection is being made.
 - c. When connected, the icon will change to show a padlock.

Additional Configurations

Configuring the client with SSL VPN installed in a DMZ

1. Configure a client configuration as detailed in the previous section. At this point Network Connect clients will only be able to route through to other machines within the DMZ
2. Configure an *up* command in order to publish a route to the clients to tell them how to get to the main LAN. To do so, you will need to determine the default gateway address that the SSL VPN server uses. This gateway should be able to route to the main LAN from the DMZ.

Example: If you have a DMZ network address of 192.168.1.0/24, with the SSL VPN server on IP 192.168.1.100 and its default gateway is 192.168.1.1, then the network address of the main LAN would be 192.168.50.0/24. The *up* command to publish for such a route would be:

Windows clients:

```
route add 192.168.50.0 mask 255.255.255.0 192.168.1.1
```

Linux/Mac clients:

```
route add -net 192.168.50.0 netmask 255.255.255.0 gw 192.168.1.1
```

3. Save the configuration. When launched, this configuration should automatically publish this new route 10-15 seconds after the Network Connect client is launched.

Configuring Client Up/Down Commands

Up commands are executed when a remote client initially connects to the protected network. The typical purpose of these commands is to publish a route to the main LAN when the SSL VPN server is installed in a DMZ. *Down* commands are executed when the remote client disconnects, usually to undo items added by the up commands.

The up and down commands are more often used in the Client Interface configuration in addition to when the interface starts and stops. Configuration of these commands is done by editing the Commands section of the Server Interface.

Up Commands

An up command is one that will be executed once the interface has started, e.g. the `$(IPADDR)` variable being replaced for the actual IP address. Any command executable from a script file is usable. The commands listed here are themselves executed from a temporary script file. Much like the `$(IPADDR)` token, there are a number of them that can be used, some of which are listed in the table below.

| Option | Description |
|--------------------------|--|
| <code>\$(IPADDR)</code> | The IP address of the interface |
| <code>\$(DEVICE)</code> | The name of the TAP device created by the <code>ifconfig</code> command. |
| <code>\$(NETADDR)</code> | The network address for this interface |
| <code>\$(SUBNET)</code> | The subnet mask for this interface |
| <code>\$(CIDR)</code> | The CIDR string for this interface |
| <code>\$(MTU)</code> | The MTU of the interface |
| <code>\$(BADDR)</code> | The broadcast address of the network |

Down Commands

Similar to the 'Up' command parameter, only these commands will be executed when the interface is stopped.

Sample Up command for Mac Clients:

```
#!/bin/bash -x
mkdir -p /etc/resolver
echo "nameserver xx.xx.xx.xx" > /etc/resolver/example.co.uk killall lookupd exit 0
```

where `xx.xx.xx.xx` and `example.co.uk` are the DNS server IP and DNS suffix respectively

Sample Down command for Mac Clients:

```
#!/bin/bash -x
rm -Rf /etc/resolver/example.co.uk
killall lookupd
exit 0
```

where `example.co.uk` is the DNS suffix

Configuring DHCP

You may also edit the DHCP configuration used for assigning an IP address to a client using the Barracuda Network Connector. The parameters configured in the DHCP tab are pushed to the client prior to the actual connection, to allow the client to configure any necessary components such as DNS servers, WINS servers and NTP servers.

The **RESOURCES > Network Connector** page displays the current status of the interface and the available options that be performed on the associated interface. Start an interface by selecting the More... option and choosing **Start**.

The configurable items are detailed below:

- **IP Address Range Start/End:** The starting and ending entries in the IP address range to be used for DHCP address assignment. Only IP addresses in the specified range will be allocated by the Barracuda Network Connector to connecting clients. **Note:** The range of IP addresses specified here must not be a part of an existing DHCP scope.
- **Domain name:** The connection-specific DNS suffix. If an FQDN is not provided by the connecting client, then the supplied value will appended to the client's host name for any queries that require domain information.
- **Primary DNS:** The IP address of the primary domain name server.
- **Secondary DNS:** The IP address of the secondary DNS.
- **Primary WINS:** The IP address of the primary WINS server (NetBIOS over TCP/IP Name Server).
- **Secondary WINS:** secondary WINS server.
- **NBDD server:** The IP address of the primary NBDD server (NetBIOS over TCP/IP Datagram Distribution Server)
- **NTP server:** The IP address of the primary NTP server (Network Time Protocol).
- **NetBIOS Scope-Id:** The scope ID for NetBIOS over TCP/IP. The NetBIOS scope ID is a character string that is appended to the NetBIOS name, and is used to provide an extended naming service for the NetBIOS over TCP/IP (known as NBT) module. The primary purpose of a NetBIOS scope ID is to isolate NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID. The NetBIOS scope ID on two hosts must match, or the two hosts will not be able to communicate. The NetBIOS Scope ID also allows computers to use the same computer name, as they have different scope IDs. The Scope ID becomes a part of the NetBIOS name, making the name unique.
- **NetBIOS over TCP/IP type:** The node type for NetBIOS over TCP/IP.
- **Disable NetBIOS over TCP/IP:** Select to disable NetBIOS over TCP/IP.

The following additional parameters can be accessed for use in the Commands tab.

| Option | Description |
|--------------------|------------------|
| \${DOMAIN} | Domain name |
| \${PRIMARY_DNS} | Primary DNS IP |
| \${SECONDARY_DNS} | Secondary DNS IP |
| \${PRIMARY_WINS} | Primary WINS IP |
| \${SECONDARY_WINS} | Secondary WINS |
| \${NTP} | NTP server |
| \${NBDD} | NBDD server |
| \${NB_SCOPE_ID} | NetBIOS scope Id |