Barracuda Purewire Adapter - *Quick Start Guide*

PUREWIRE WEB SECURITY SERVICE

The Barracuda Purewire Web Security Service is a cloud-based secure Web gateway that protects users from malware, phishing, identity theft, and other harmful activity online. The Barracuda Purewire Adapter is an optional device that forwards Web traffic to the Barracuda Purewire Web Security Service, integrates with your directory service for group-based policies, and caches static Web content locally to save bandwidth.

Prerequisites

How you install the Adapter depends on whether you plan to use a static IP address or use DHCP. The Adapter is configured for DHCP setup by default. If you configure the Adapter with DHCP, the system administrator must set up static DHCP for the Adapter, so that the IP of the Adapter does not change.

If you want to configure the Adapter with a static IP address, you will need the following:

- IP address
- Netmask
- Broadcast Address
- Gateway

You can obtain this information from the network system administrator or by looking up the Adapter's MAC address on the DHCP server to determine what IP address it assigned to the Adapter.

1 Getting Started

This guide provides you with setup instructions for the Barracuda Purewire Adapter. We recommend reading these instructions fully before starting the setup. For additional installation information, such as advanced settings, and for instructions on using the Adapter and Manager, see the Administrator's Guide. To begin setting up your Adapter, you will need the following:

- Barracuda Purewire Adapter, AC Power Cord (included)
- A network cable
- An Authentication Key generated in the Manager application (see the Administrator's Guide)

2 Physical Installation

To install the Barracuda Purewire Adapter:

1. Connect an Ethernet Cable from your network switch to the Ethernet port on the front of the Barracuda Adapter marked LAN.
2. Connect a Standard VGA Monitor, PS2 Keyboard, and AC power cord to the Adapter.
3. Press the POWER button on the front panel to turn the Adapter on.

3 Log on to the Adapter and Configure Network Settings

1. Obtain the Adapter's assigned IP from the monitor.
2. Use a Web browser to access the Adapter User Interface (https) and log in.
3. The default user name is `admin`. The default password is `password`. When you log in to the Adapter for the first time, the default landing page is the Network Settings page on the Network Setup tab.
4. Type the **Hostname** for the Adapter (format: adapter1).
5. Type the **Domain name** for the Adapter (format: purewire.com).
6. Type the **IP address**(es) of the **DNS Server**.
7. Configure the **eth0** network Adapter. DHCP is selected by default. To use a static IP for this Adapter, select the **Static IP address** radio button, and then type the Adapter's **IP address**, **Netmask**, **Broadcast address** (IP address that allows information to be sent to all machines on a given subnet rather than a specific machine), and **Default gateway**.

4 Configure Static Routes

1. If you want to add static routes, click **Add Route**, then enter the:
   i. **Network** (the destination of the route)
   ii. **Netmask**
   iii. **Metric** (used to calculate the best path to a given destination)
   iv. **Gateway** (address)
2. Repeat this step until you have added all the static routes you need, and then click **Save**.

5 Add an Authentication Key

Adding a key enables the Adapter to access to the Barracuda Purewire Web Security Service.

1. On the Network Setup tab, click **Keys**.
2. Paste the key into the field provided. Click **Save**.

6 Choose a User Authentication Method

Click the radio button that applies to your choice:

- **No authentication**—If you do not want to set up authentication, the options discussed in the rest of this section do not appear on the Adapter interface.
- **Windows NT LAN Manager (NTLM)**—NTLM enables network clients to prove their identities without sending a password to the server. You must enable NTLM to identify users and groups for policy enforcement and reporting. If you choose NTLM, you can set options for verifying user information with a Domain Controller, as well as other advanced options.
- **User Identification**—If you choose User Identification, you can configure the Adapter to obtain user information from each Domain Controller.

Configuring NTLM Authentication

1. Choose whether you want to **Verify with a Domain Controller**.
2. If so, type the domain controller hostname (format: hostname.purewire.com), the name of the domain (format: purewire.com), and the user ID (example: administrator) and password

for an account with privileges for querying and reading from the domain controller.

3. If needed, click **Advanced NTLM Settings** and set the options for:
   - **NTLM Helpers**—increase this value for larger numbers of users
   - **Maximum Challenge Reuses**
   - **Maximum Challenge Lifetime** (in seconds)
4. Click Save.

Configuring User Identification Authentication

The **Authentication Options** box displays the **Timeouts** group, which lets you specify the amount of time a user can be logged in before Adapter attempts to obtain user information. You can also specify the polling interval at which Adapter obtains user information.

Regardless of Whether You Chose User Identification or NTLM

1. Indicate how you want to handle any **Unidentifiable Traffic**. You can block unidentified traffic or allow it and apply either global policies or the policies of a group you indicate.
2. Specify any destinations and client addresses that are not subject to authentication.
   - **Destination exceptions –** Add exceptions one per line, and do not include the protocol (such as https:// or http://).
   - **Client exceptions** – Add exceptions one per line. Specify IP address ranges in either /CIDR or /NETMASK notation.
     CIDR Example: 192.168.0.0/24 for 256 addresses 192.168.0.0 to 192.168.0.255.
     Netmask Example: 192.168.0.0/255.255.255.0 for 256 addresses 192.168.0.0 to 192.168.0.255.

7 Specify Group Lookup Location for LDAP or Active Directory

You can use existing user and group data from a directory or you can create groups on the Barracuda Purewire Web Security Service. If using a directory, the Adapter must be in the same broadcast network as the AD server.

On the Network Setup tab, select Group Lookup. Select the **Look up user groups** checkbox, type the required information, and then click **Save**:

- **Directory Server Hostname**—The fully-qualified DNS hostname of the Directory server (format: hostname.purewire.com)
- **User Name**—The user name of an account with sufficient privileges to query the groups in the directory (format: DOMAIN\username)
- **Password**—The password for the account (no spaces)
- **Base DN**—The base DN (Distinguished Name) that is the starting point in the Directory hierarchy at which your search will begin (format: cn=users,dc=purewire,dc=com where cn is the common name, dc is a domain component, and entries are separated by commas)
- **UID Field**—The name of the field containing user IDs (recommended defaut: sAMAccountName)

8 Connect to the Upstream Proxy

1. On the Network Setup tab, select Upstream Proxy.
2. Enter the **Host name** and **Port number** for the Barracuda Purewire Web Security Service (provided by Barracuda Networks).
3. The Adapter is configured to fail closed (blocking traffic) in the rare event that it should be unavailable. If you prefer it to fail open (allowing all traffic), select the **Fail Open** checkbox.
4. Click **Save**.

9 Configure WCCP

Note: Skip this step if you are not using WCCP.

Adapters support Web Cache Communication Protocol (WCCP) v2 as a method for accepting traffic. WCCP is a content-routing protocol that forwards traffic from one or more WCCP-enabled network devices to the Adapter. For more information about configuring WCCP, see the Administrator's Guide.

1. On the Network Setup tab, select WCCP.
2. Select the **Enable WCCP** checkbox.
3. Choose the method for forwarding traffic.
4. Choose the assignment method for forwarding traffic. The assignment method determines how traffic is distributed across the WCCP clients if they are grouped. Choose either Hash or Mask.
5. Click **Add New** in the **Forwarding Network Devices** area to configure the IP addresses of any devices that will forward traffic to the Adapter via WCCP.
6. Click **Save**.

10 Define Client Proxy Setup

Note: Skip this step if you are not using PAC files for proxying.

If you use the Adapter itself to host the PAC file, adding networks to the exception list automatically creates the PAC file.

1. On the Network Setup tab, select **Client Proxy Setup**.
2. Type the Adapter's **IP address** or **hostname**. The clients that need to access the PAC file must be able to resolve the hostname via DNS. If necessary, use a fully qualified domain name (format: adapter1.purewire.com).
3. You can add internal networks to the exceptions list if you want traffic to those networks to bypass the proxy. Click **Add New** to add exceptions.