How to Define Port Protocol Protection

https://campus.barracuda.com/doc/46209201/

Layer 7 Application Control is a legacy feature of the Barracuda NextGen Firewall F-Series. Barracuda Networks recommends using Application Control instead

Port Protocol Protection uses deep packet inspection to make sure that a port is only used by the protocols that you allow on it. It addresses the limitations of firewall rules in being able to detect if a port is being used by prohibited protocols.

You define Port Protocol Protection policies in a firewall service object. You can define a policy in an existing service object or after creating a new service object. For more information, see How to Create Service Objects.

Note: A Port Protocol Protection policy for HTTP has already been configured in the **HTTP-Enforced** service object. To configure HTTP port policies, you can use this service object instead of creating a new one.

To enable and configure Port Protocol Protection policies, complete the steps in the following sections:

Enable Port Protocol Protection

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. From the **Configuration** menu in the left navigation pane, select **Application Detection**.
3. From the **Enable Protocol Detection** list, select *yes*. Note: When you enable Port Protocol Protection, you also enable Layer 7 Application Control.
4. Click **Send Changes** and **Activate**.

Specify a Port Protocol Protection Policy

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, select **Services**.
3. Double-click the required service object. The **Edit/Create Service Object** window opens.
4. Double-click the required protocol. The **Service Entry Parameters** window opens.
5. From the **Action for prohibited Protocols** list, select a Port Protocol Protection policy for

handling prohibited services. You can select any of the following policies:

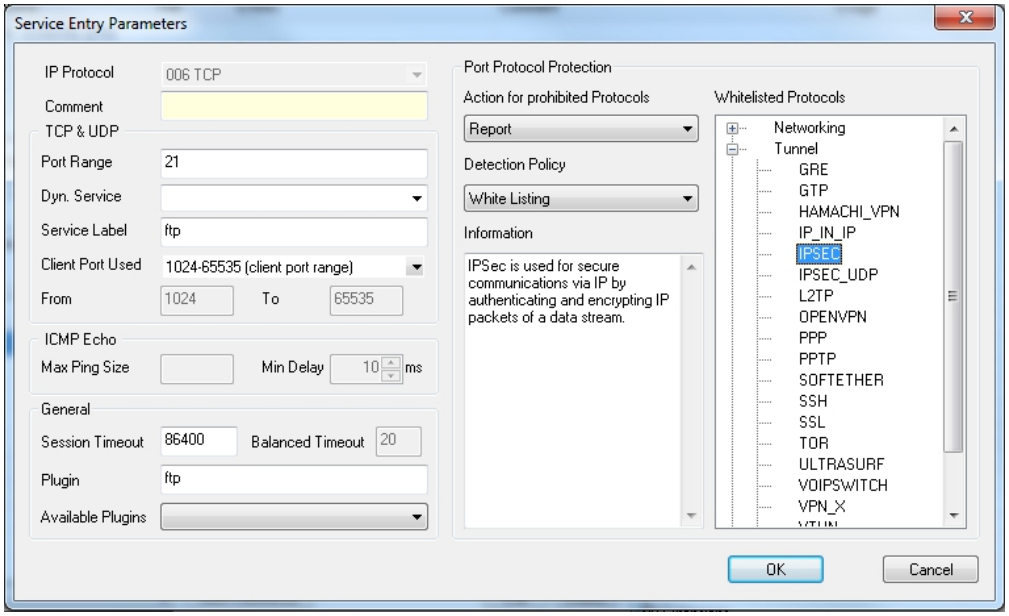
Policy	Description
No Protocol Protection	Disable Port Protocol Protection.
Report	Report prohibited protocols in the access cache.
Reset	Send a TCP RST packet to terminate the session with the prohibited protocol.
Drop	Drop the traffic but keep the session with the prohibited protocol.

Select the Detection Policy

You can configure Port Protocol Protection to inspect and compare traffic against a list of prohibited or allowed protocols. From the **Detection Policy** list in the **Service Entry Parameters** window, you can select *White Listing* or *Black Listing*.

- *White Listing* **–** Only allows the protocols that you specify. All other protocols are prohibited and will be handled according to the specified Port Protocol Protection policy.
  - From the **Detection Policy** list, select **White Listing**.
  - In the **Whitelisted Protocols** table, double-click the allowed protocols.
- *Black Listing* **–** Only prohibits the protocols that you specify. The selected protocols are handled according to the specified Port Protocol Protection policy. All other protocols are allowed.
  - From the **Detection Policy** list, select **Black Listing**.
  - In the **Blacklisted Protocols** table, double-click the prohibited protocols.

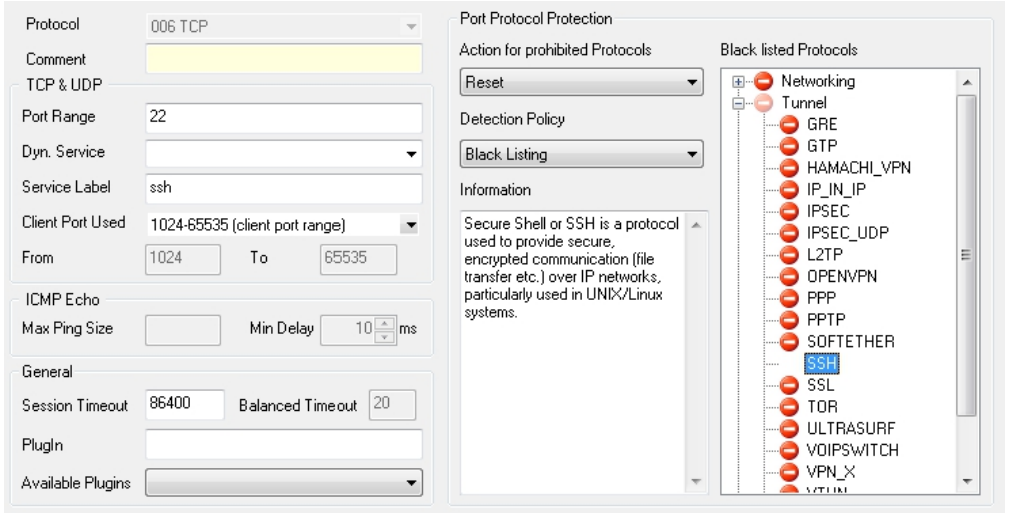
Port Protocol Protection in service object configuration:



Example: Port Protocol Protection Policy for the SSH Service

Figure 2 displays an example of a Port Protocol Protection Policy for the SSH service to avoid unwanted traffic that is forwarded by a firewall rule. This Port Protocol Protection Policy allows SSH Traffic but resets the session if any of the selected protocols are detected.

Example Port Protection Policy:



- After specifying the settings, don´t forget to click **Send Changes** and **Activate**.

Figures

1. ppp.jpg
2. p_prot.jpg