

How to Configure Port Protocol Protection

<https://campus.barracuda.com/doc/48202787/>

Port Protocol Protection uses deep packet inspection to enforce the used protocol on a port. Port protocol detection can be configured with a positive or negative security model. The white list policy allows only the selected protocols; the blacklist mode allows all protocols that are not selected.

Before you begin

Create a service object. For more information, see [Service Objects](#).

Step 1. Enable Port Protocol Protection

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, click **Application Detection**.
3. From the **Enable Protocol Detection** list, select **yes**.



The screenshot shows a configuration window titled "Application and Port Protocol Protection". Inside the window, there is a label "Enable Protocol Detection" followed by a dropdown menu. The dropdown menu is currently set to "yes" and is highlighted with an orange border. To the right of the dropdown menu is a small icon of a document with a checkmark.

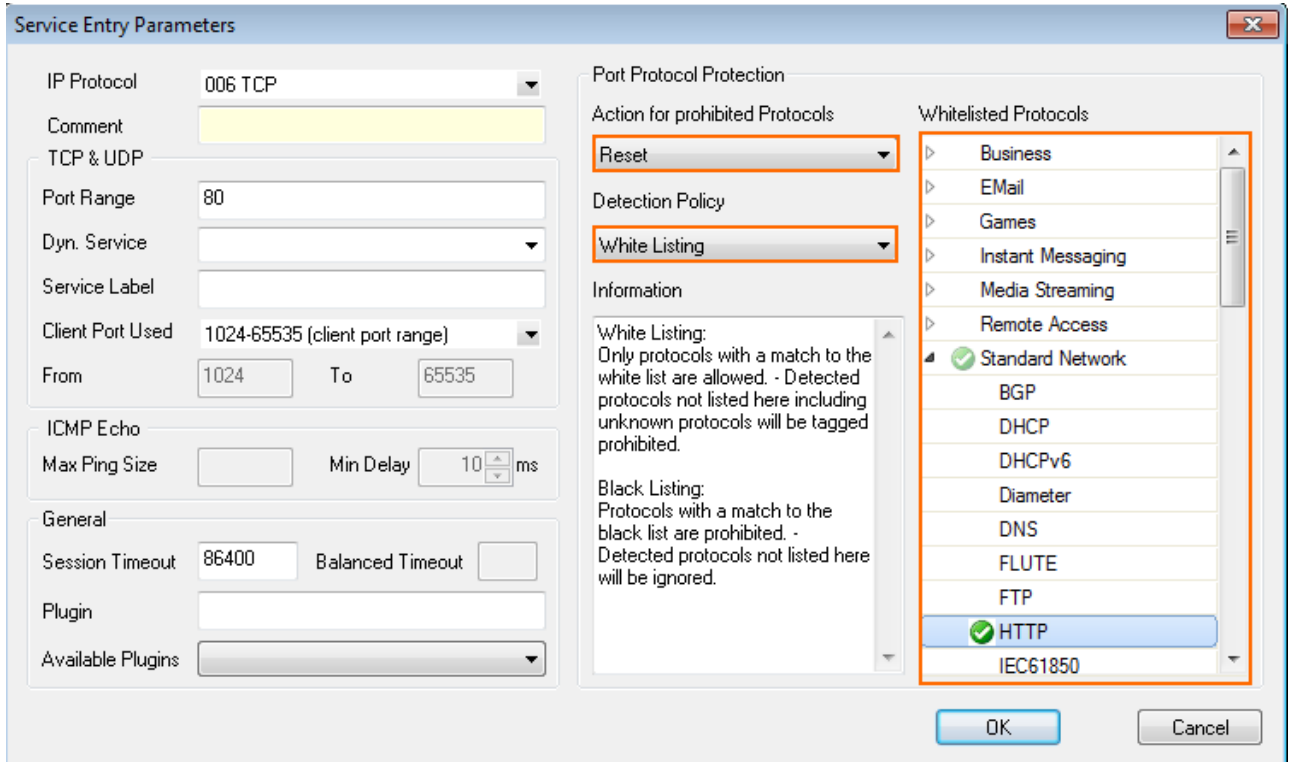
4. Click **Send Changes** and **Activate**.

Step 2. Add Port Protocol Protection to a service object

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Services**.
3. Double-click the service object. The **Edit/Create Service Object** window opens.
4. Double-click the service entry. The **Service Entry Parameters** window opens.
5. From the **Action for prohibited Protocols** list, select the Port Protocol Protection policy:
 - **No Protocol Protection** - Disable Port Protocol Protection.
 - **Report** - Report prohibited protocols on the **FIREWALL > Live** and **FIREWALL > History** pages.
 - **Reset** - Sessions using unallowed protocols are terminated with a TCP RST.
 - **Drop** - The session with the unallowed protocol is kept open, but the traffic is dropped.
6. From the **Detection Policy** list, select **While Listing** or **Black Listing**.
7. In the **Whitelisted Protocol** list, expand the menu items and double-click on every protocol

you want to add to the **Detection policy**.

8. Click **OK**



Service Entry Parameters

IP Protocol: 006 TCP

Comment: [Empty]

TCP & UDP: [Empty]

Port Range: 80

Dyn. Service: [Empty]

Service Label: [Empty]

Client Port Used: 1024-65535 (client port range)

From: 1024 To: 65535

ICMP Echo

Max Ping Size: [Empty] Min Delay: 10 ms

General

Session Timeout: 86400 Balanced Timeout: [Empty]

Plugin: [Empty]

Available Plugins: [Empty]

Port Protocol Protection

Action for prohibited Protocols: Reset

Detection Policy: White Listing

Information

White Listing: Only protocols with a match to the white list are allowed. - Detected protocols not listed here including unknown protocols will be tagged prohibited.

Black Listing: Protocols with a match to the black list are prohibited. - Detected protocols not listed here will be ignored.

Whitelisted Protocols

- Business
- EMail
- Games
- Instant Messaging
- Media Streaming
- Remote Access
- Standard Network
- BGP
- DHCP
- DHCPv6
- Diameter
- DNS
- FLUTE
- FTP
- HTTP
- IEC61850

OK Cancel

9. Click **OK**.

10. Click **Send Changes** and **Activate**.

Figures

1. port_protocol_protection_01.png
2. port_protocol_protection_02.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.