How to Create Service Objects

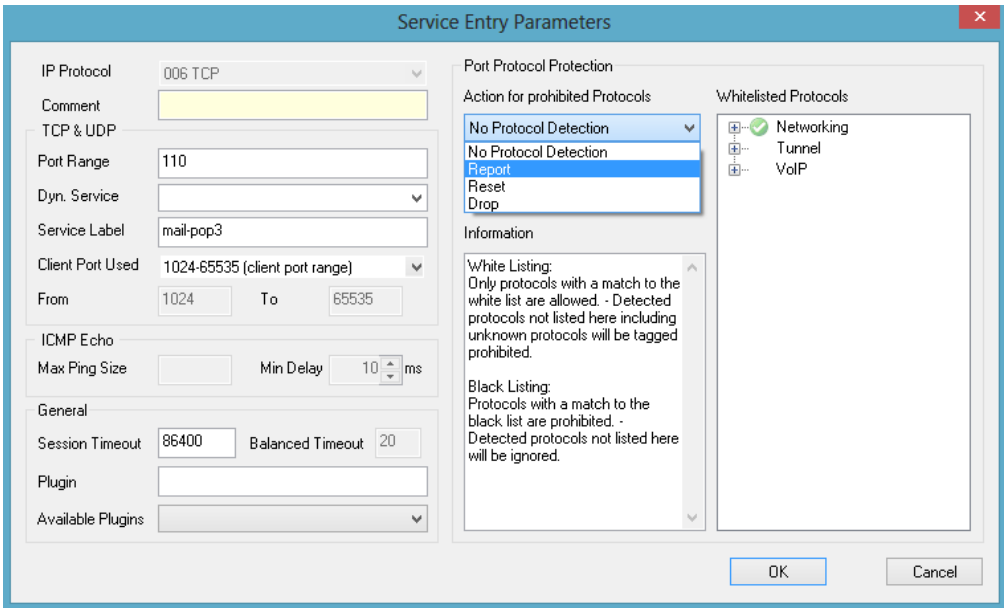
https://campus.barracuda.com/doc/48202940/

Create service objects to reference IP protocols and, if TCP/UDP is used, the destination port numbers, when configuring access rules. The Barracuda NextGen Firewall F-Series provides a range of predefined service objects. When creating a new service object, you can also include (reference to) other service objects that are already configured.

Create 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 on **Services**.
3. Click **Lock**.
4. Right-click the table and select **New.** The **Edit/Create Service Object** window opens.
5. Enter a **Name** for the service object. E.g., `POP3 Service`.
6. If you want to include an already configured service object, select it from the **Any** drop down list and click **New Reference**.
7. Click **New Object**. The **Service Entry Parameters** window opens.
8. From the **IP Protocol** list, select the required protocol. E.g., *006 TCP*

   For TCP- and UDP-based protocols, you can enter a space-delimited list of ports in the **Port Range** field. To use all ports for the protocol, enter an asterisk (*). You can also define a port range, such as `3001-3008`, or enter a combination of port ranges and a space-delimited list of ports. For example: `25 80 8080 3001-3008`
9. In the **Port Protocol Protection** section, select an action from the **Action for prohibited Protocols** list.



10. Click **OK**.

11. Click **Send Changes** and **Activate**.

You can now apply the service object to your access rules.

Apply a Service Object to an Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click on **Access Rules**.
3. Click **Lock**.
4. Double-click the number of the rule you want to apply the service object to, or right-click it and select **Edit Rule**. (You can also create a new rule.)
5. In the **Edit Rule** window, select the **Object Viewer** check box.
6. In the **Object Viewer** window that appears, open the **Services** tab, and drag the service object to the **Service** table in the **Edit Rule** window.
7. Finish your rule configuration.

Service Object Settings

TCP & UDP

- **Port Range** – Port or port range the service is running on.
- **Dyn. Service** – This parameter is required in conjunction with ONCRPC.
- **Service Label** – Here you may enter certain labels. If left empty, well-known service names (available in `/etc/services`) are used.
  > It is highly recommended that you use this parameter only for defining service names that are not well-known (for example, Oracle521).
- **Client Port Used** – The port range the firewall uses for the connection. This port range is only used if a dynamic port allocation is required, e.g., as in the 'proxy dynamic' connection type. If you want to enter a custom port range, select **Manual Entry** and enter the first port in the **From** field and the last port in the **To** field. This parameter is not evaluated when the firewall services checks if the rule matches.

ICMP Echo

- **Max Ping Size** – The maximum size allowed for the ping packet.
- **Min Delay** – The minimum allowed delay for pinging. The 'FW Flood Ping Protection Activated [4002]' event is generated if this limit is not met.

General

- **Session Timeout** – Time in seconds that a session can remain idle until it is terminated by the firewall (default values: TCP: 86400; UDP: 60; ICMP: 20; all other protocols: 120). This timeout is applied to all TCP connections by counting the time that has passed in a session since the last traffic transmission. Similarly, it applies an initial timeout to all stateless protocols counting the time until the source has answered the initial datagram. When the datagram is answered, the **Balanced Timeout** setting comes into effect.
  This parameter can only be used in the forwarding firewall. Setting this parameter in the host firewall has no effect.
- **Balanced Timeout** – The time in seconds that a session-like connection established through a non-connection oriented protocol (all protocols except TCP) can remain idle until it is terminated by the firewall (default values: UDP: 30; ICMP: 10; all other protocols: 120). The balanced timeout comes into effect after the initial datagram sent by the source has been answered and the "session" has been established. Generally, the balanced timeout should be shorter than the session timeout because it is otherwise overridden by the session timeout and never comes into effect. The balanced timeout allows for keeping non-connection oriented "sessions" short and minimizing the amount of concurrent sessions. The larger initial session timeout guarantees that late replies to initial datagrams are not inevitably dropped.
  This parameter is only executable in the forwarding firewall. Setting this parameter in the local firewall takes no effect.
- **Plugin** – The name and parameters of any plugins that you might be required for this object. For more information, see Firewall Plugin Modules.

Port Protocol Protection

- **Action for prohibited Protocols** – From this list, select an action that should be taken if prohibited protocols are detected. For more information, see How to Configure Port Protocol Protection.
- **Detection Policy** – From this list, select the policy to be applied. For more information, see How to Configure Port Protocol Protection.

Figures