How to Activate Dynamic Firewall Rules for Remote Connections via SSL VPN

https://campus.barracuda.com/doc/41116137/

While you are connected to the SSL VPN, you can enable or disable dynamic firewall rules for the Barracuda NG Firewall. Only dynamic or timed rules are evaluated. However, you must activate these rules for use with SSL VPN connections. Otherwise, the rules will not be visible to administrators that are connected.

In this article:

Create a Dynamic Firewall Rule

Create a dynamic firewall rule. For example, you can create a firewall rule named *box-mgmt-dynamic* with the following settings:

1. **Action** – App Redirect
2. **Dynamic Rule** – Select this check box.
3. **Source** – `0.0.0.0`
4. **Service** – **NGF-MGMT-BOX** (This service object includes all necessary NG Firewall management ports)
5. **Destination** – The WAN IP address.
6. **Local Address** – The box management IP address.

Make sure that you change the default password for the Barracuda NG Firewall. Otherwise, you might introduce a security risk with this type of firewall rule. For security reasons, it may also be important to limit the **Source** to known IP addresses.

Activate the Dynamic Firewall Rule for SSL VPN

1. Open the **SSL-VPN** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **VPN-Service**).
2. In the left menu, click **Dynamic Firewall Rules**.
3. In the **Firewall Rule Activation** table, add an entry for the dynamic firewall rule. For the entry, you can configure the following settings:

Setting	Description

Active	To make the firewall rule visible to SSL VPN users, select this check box.
Visible Name	The name for the firewall rule. For example, `NG Firewall Management`
Link Description	A description of the rule for SSL VPN users. For example, `Here you can activate the dynamic firewall rule for management access.`
Dynamic Rule Selector	In this table, delete the asterisk (*****) that is included by default and add the names of the dynamic firewall rules that you created for the SSL VPN. For example, *box-mgmt-dynamic*. Make sure that you correctly enter the firewall rule names; otherwise, the firewall rules will not be activated for use over SSL VPN connections. If you are using a dynamic rule in a cascaded rule list, enter the name of the rule list. Format the rule list name as *<rulelist>:*. You can also enter the asterisk (*****) as a wildcard character or the question mark (**?**) as a single character wildcard.
Allowed User Groups	In this table, delete the asterisk (*****) that is included by default and add the names of the MSAD groups for administrators. For example, **OU=admins*.*

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

Enable and Disable the Dynamic Rule

While you are connected to the SSL VPN, go to the **Firewall > Dynamic** page on the Barracuda NG Firewall. On this page, you can enable dynamic firewall rules for a specified length of time. If you do not specify a length of time for a firewall rule, it stays enabled until you manually disable it.

For more information on activating dynamic firewall rules, see How to Create and Activate a Dynamic Firewall Rule.