Example - Configuring an Access Rule for the Barracuda Email Security Gateway

https://campus.barracuda.com/doc/42045987/

When deploying a Barracuda Email Security Gateway behind the Barracuda NextGen Firewall X-Series, configure a **Destination NAT (DNAT)** access rule to route SMTP traffic to the Email Security Gateway. For more information on the Barracuda Email Security Gateway, see: Overview.

This article provides instructions on how to configure an access rule for the following setup:

Before you Begin

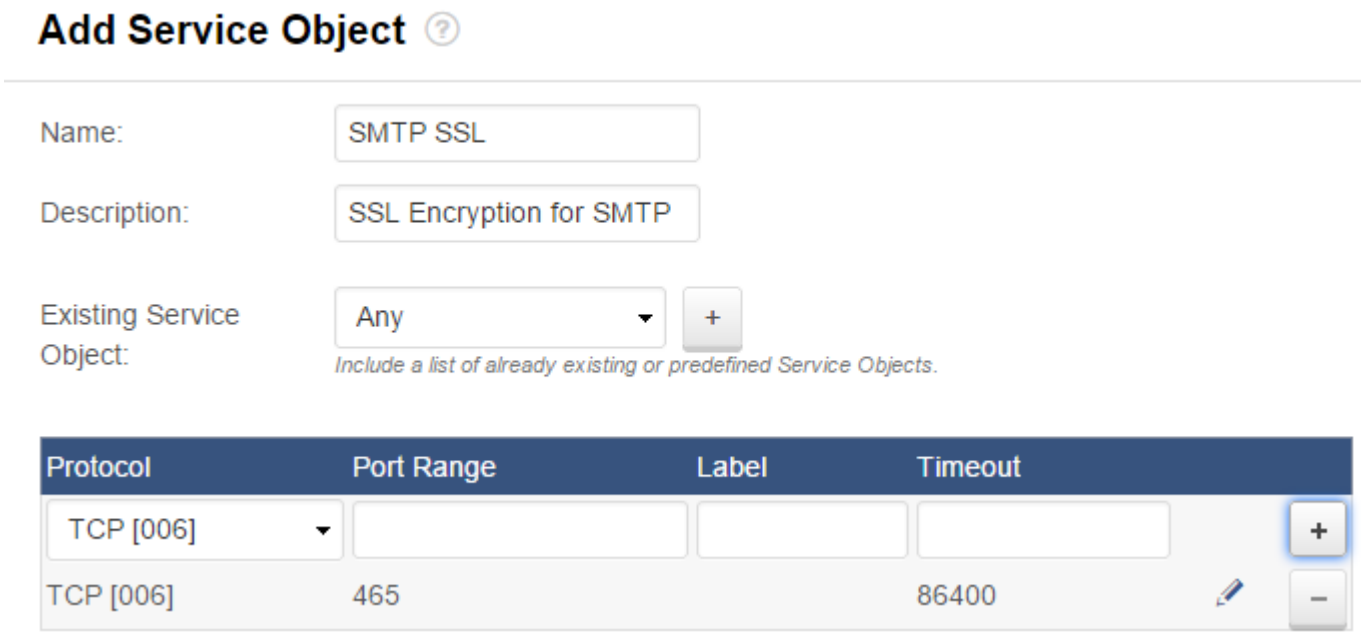
Install and configure the Barracuda Email Security Gateway in your LAN as described in: Deployment Behind the Corporate Firewall.

Step 1. (Optional) Create a Service Object for SMTPS

To also forward SMTPS traffic to your Email Security Gateway, create a service object to redirect the traffic to port 465. For more information, see Service Objects.

Use the following settings:

- **Protocol** – TCP
- **Port Range** – 465

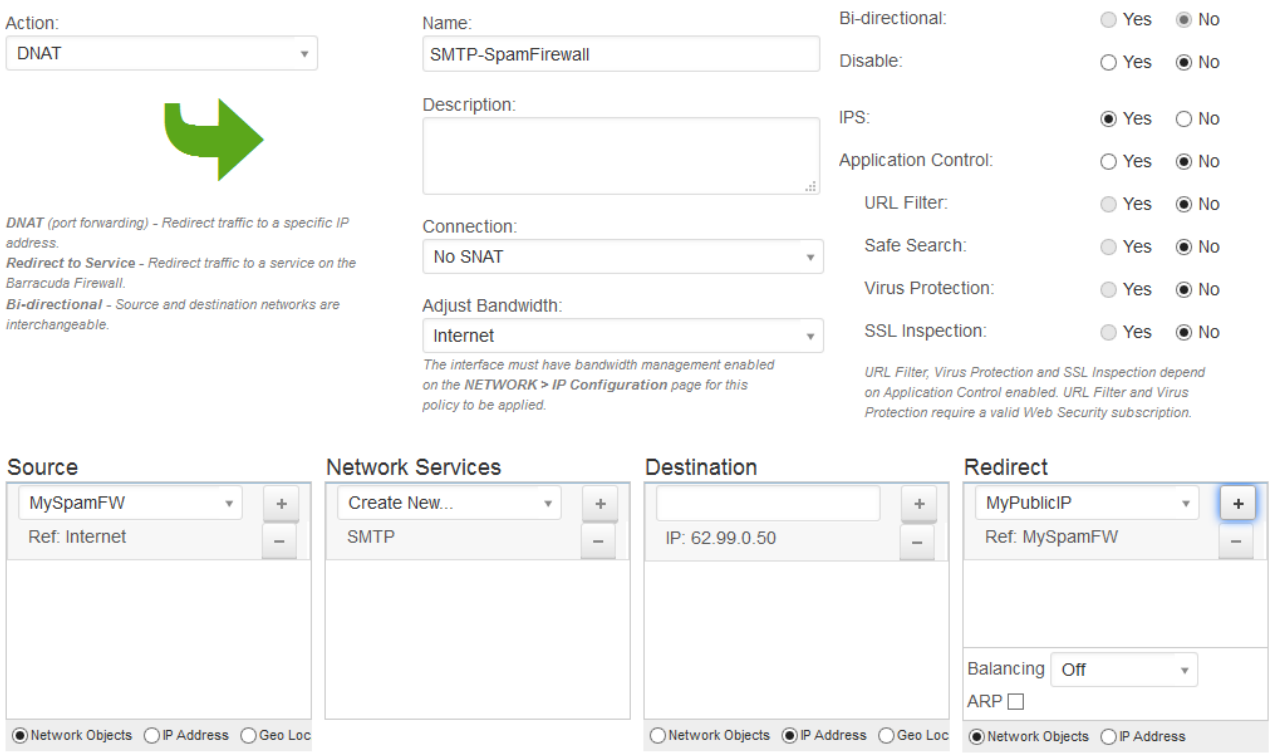


Step 2. Configure a DNAT Access Rule

Create a DNAT access rule that forwards all incoming SMTP traffic to the IP address of the Email Security Gateway.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new firewall rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Connection	Source	Network Services	Destination	Redirected To
DNAT	**No SNAT**	**Internet**	**SMTP, SMTP SSL (optional)**	Enter the public IP address of the X-Series Firewall. E.g.: `62.99.0.50`	Enter the IP address or select the network object for your Barracuda Email Security Gateway. E.g.: `10.10.10.3`



5. Click **Save**.

Step 2. Verify the Order of the Access Rules

Because rules are processed from top to bottom in the rule set, arrange your access rules in the correct order. Make sure that this rule is the first access rule that matches SMTP traffic on the WAN port of the X-Series Firewall.

After adjusting the order of the rules in the rule set, click **Save**.

Figures

1. DNAT_spamfw.png
2. ssl_smtp_67_01.png
3. dnat_smtp_67_00.png