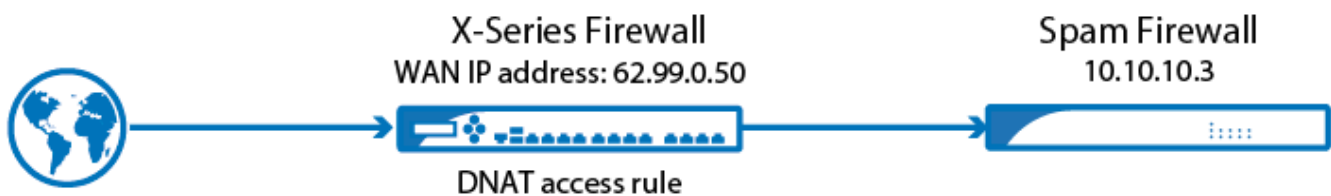


Example - Configuring an Access Rule for the Barracuda Email Security Gateway

<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

Add Service Object

Name:

Description:

Existing Service Object: 
Include a list of already existing or predefined Service Objects.

Protocol	Port Range	Label	Timeout	
TCP [006]	<input type="text"/>	<input type="text"/>	<input type="text"/>	
TCP [006]	465		86400	 

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

Action:

Name:

Bi-directional: ☐ Yes ☒ No

Disable: ☐ Yes ☒ No

Description:

IPS: ☒ Yes ☐ No

Application Control: ☐ Yes ☒ No

URL Filter: ☐ Yes ☒ No

Safe Search: ☐ Yes ☒ No

Virus Protection: ☐ Yes ☒ No

SSL Inspection: ☐ Yes ☒ No

Connection:

Adjust Bandwidth:

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source

Ref: Internet

☒ Network Objects ☐ IP Address ☐ Geo Loc

Network Services

SMTP

Destination

☐ Network Objects ☒ IP Address ☐ Geo Loc

Redirect

Ref: MySpamFW

Balancing

ARP ☐

☒ Network Objects ☐ IP Address

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

© Barracuda Networks Inc., 2024 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.