How to Configure Mail Security in the Firewall

https://campus.barracuda.com/doc/48660869/

The Barracuda NextGen Firewall X-Series scans SMTP traffic in two steps:

1. SSL Inspection decrypts SSL-encrypted SMTP connections. For incoming connections, your mail server's SSL certificates are used.
2. The DNS blacklist database is queried via a DNS lookup using the sender's IP address. If the DNS reputation database is not available, the email is not modified. If the domain or IP address is blacklisted, the email's subject line is modified to start with `[SPAM]` and the following non-configurable MIME type headers are set:
    - `X-Spam-Prev-Subject:` Your email subject without the [SPAM] tag.
    - `X-Spam-Flag: YES`
    - `X-Spam-Status: Yes`
    - `X-Spam-Level: ***`
3. Email attachments are scanned by the virus scanner. If malware is found, the attachment is stripped from the email and replaced by a customizable text informing the user that the malicious attachment has been removed.

Before you begin

- Enable and configure SSL Inspection. If needed, adjust the SSL Inspection settings to support MTAs requiring SSLv3. For more information, see How to Configure SSL Inspection.

Step 1. Import the mail server certificates

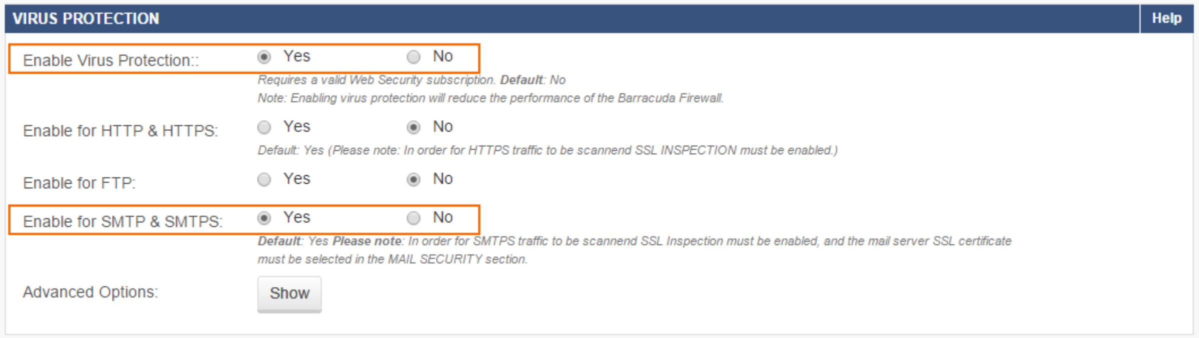
Import the SSL certificates of your internal mail server(s). For more information, see How to Use and Manage Certificates with the Certificate Manager.

Step 2. Enable virus protection for mail traffic

Enable virus scanning and SSL Inspection in the firewall.

1. Go to **FIREWALL > Settings**.
2. In the **Firewall Policy Settings** section, enable **TCP Stream Reassembly**.
3. Make sure that **Application Control** is enabled.
4. In the **Virus Protection** section,
    1. Set **Enable Virus Protection** to **Yes**.

2. Set **Enable for SMTP & SMTPS** to **Yes**.



Enable Virus Protection:: ● Yes ○ No

*Requires a valid Web Security subscription. **Default**: No*
Note: Enabling virus protection will reduce the performance of the Barracuda Firewall.

Enable for HTTP & HTTPS: ○ Yes ● No

Default: Yes (Please note: In order for HTTPS traffic to be scannend SSL INSPECTION must be enabled.)

Enable for FTP: ○ Yes ● No

Enable for SMTP & SMTPS: ● Yes ○ No

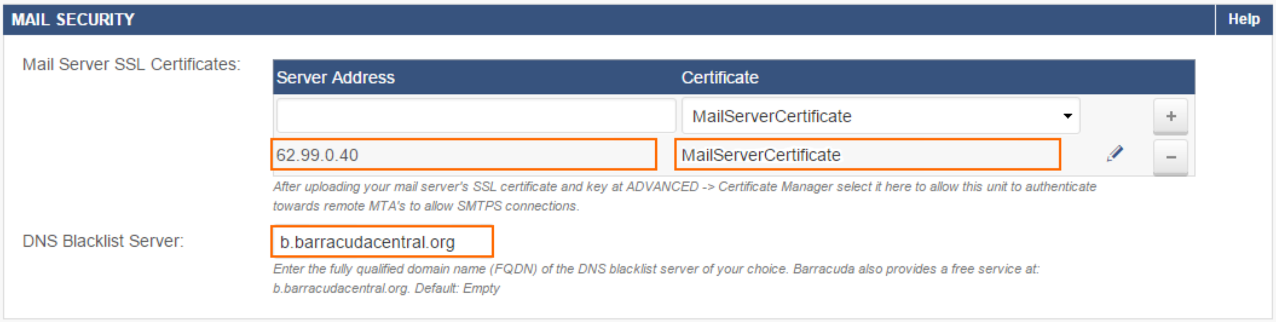
***Default**: Yes **Please note**: In order for SMTPS traffic to be scannend SSL Inspection must be enabled, and the mail server SSL certificate must be selected in the MAIL SECURITY section.*

Advanced Options: Show

5. (optional) Configure advanced virus scanner settings:

   Changing settings for the virus scanner also affects virus scanning for other services.

   1. In the **Advanced Options** section, click **Advanced / Show**.
   2. (optional) Change the default behavior **If Virus Scanner is not available**.
      - **Block All** – (default) All pages will be blocked.
      - **Allow All** – All pages will be allowed.
   3. Configure the following settings:
      - **Block Large Files / Large File Limit** – To block files that exceed the **Large File Limit**, enable **Block Large Files**.The large file policy is set to a sensible value for your appliance. The maximum value is 1024 MB. If disabled, large files will not be scanned. Instead, they will be delivered directly to the client.
      - **Scanned MIME Types** – If applicable, you can add MIME types of files you want the X-Series Firewall to scan to the **Scanned MIME Types** list (see: **Default MIME Types** in Virus Protection in the Firewall). To add a file type, enter the file path and click **+**. To remove a file type, click **-** next to the file entry in the list. Click **Reset to Defaults** to restore the default list.
   4. At the bottom of the page, click **Save**.
6. (Optional) Enable **Advanced Threat Detection**. For more information, see Advanced Threat Protection (ATP/ATD).
7. In the **Mail Security** section, enter the public IP address that your mail server domain's MX record resolves to in the **Mail Server SSL Certificates** section, select the mail server SSL certificate from the **Certificate** list, and click **+**.
8. Enter the FQDN of the **DNS Blacklist Server**. Default: `b.barracudacentral.org`



Mail Server SSL Certificates:

Server Address	Certificate
	MailServerCertificate
62.99.0.40	MailServerCertificate

After uploading your mail server's SSL certificate and key at ADVANCED -> Certificate Manager select it here to allow this unit to authenticate towards remote MTA's to allow SMTPS connections.

DNS Blacklist Server: b.barracudacentral.org

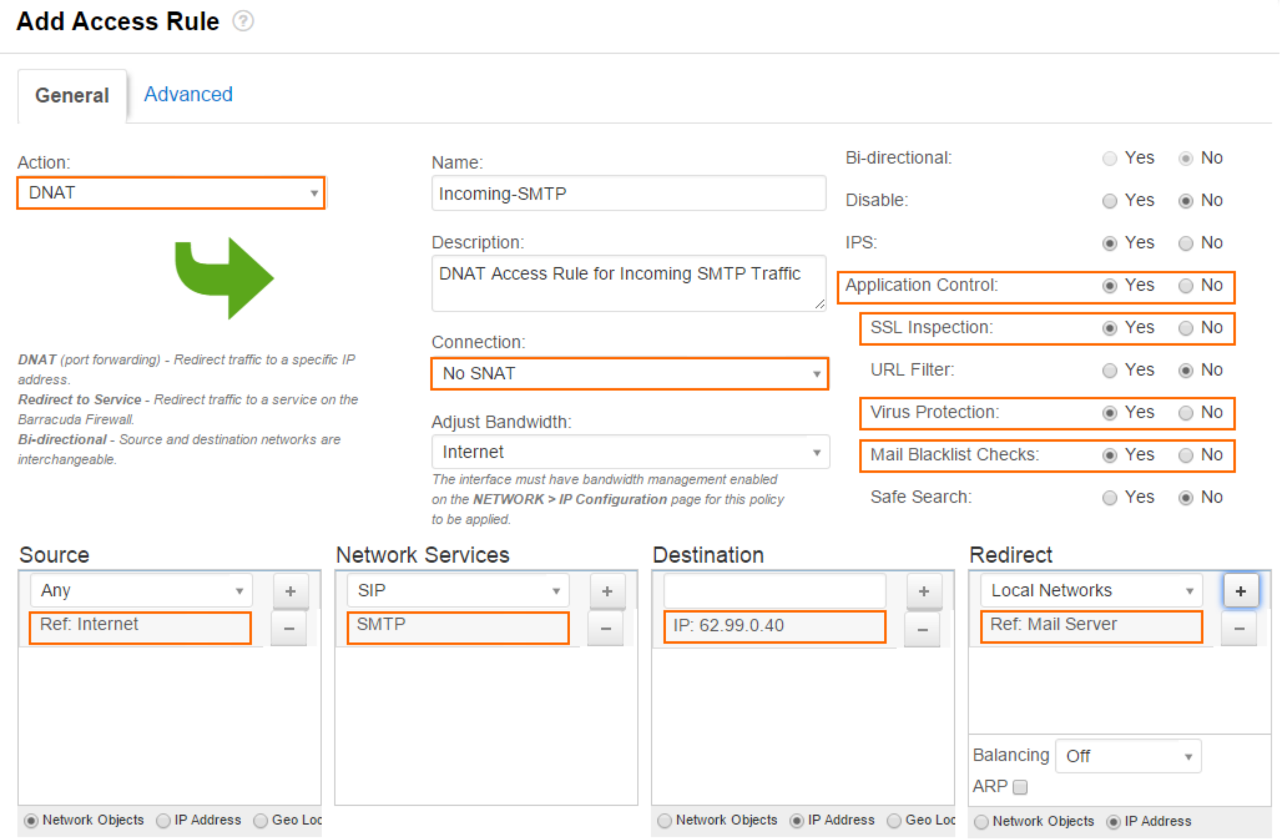
Enter the fully qualified domain name (FQDN) of the DNS blacklist server of your choice. Barracuda also provides a free service at: b.barracudacentral.org. Default: Empty

9. Click **Save**.

Step 3. Create a DNAT access rule for incoming SMTP traffic

Enable Application Control, SSL Interception, and Virus Protection in the access rule.

1. Go to **FIREWALL > Firewall Rules**.
2. Create an access rule with the following settings:
    - **Action** – Select **DNAT**.
    - **Connection** – Select **No SNAT**.
    - **Source** – Select **Internet**, and click **+**.
    - **Network Services** – Select **SMTP**, and click **+**.
    - **Destination** – Enter the public IP address that your mail server domain's MX record resolves to, and click **+**.
    - **Redirect** – Enter the IP address(es), or select a network object for your internal mail server(s), and click **+**.
3. Enable **Application Control**, **SSL Inspection**, **Virus Protection**, and **Mail Blacklist Checks**.



Add Access Rule

Action: DNAT

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: Incoming-SMTP

Description: DNAT Access Rule for Incoming SMTP Traffic

Connection: No SNAT

Adjust Bandwidth: Internet

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

Bi-directional: ○ Yes ● No
Disable: ○ Yes ● No
IPS: ● Yes ○ No
Application Control: ● Yes ○ No
SSL Inspection: ● Yes ○ No
URL Filter: ○ Yes ● No
Virus Protection: ● Yes ○ No
Mail Blacklist Checks: ● Yes ○ No
Safe Search: ○ Yes ● No

Source: Any; Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc

Network Services: SIP; SMTP

Destination: IP: 62.99.0.40
○ Network Objects ● IP Address ○ Geo Loc

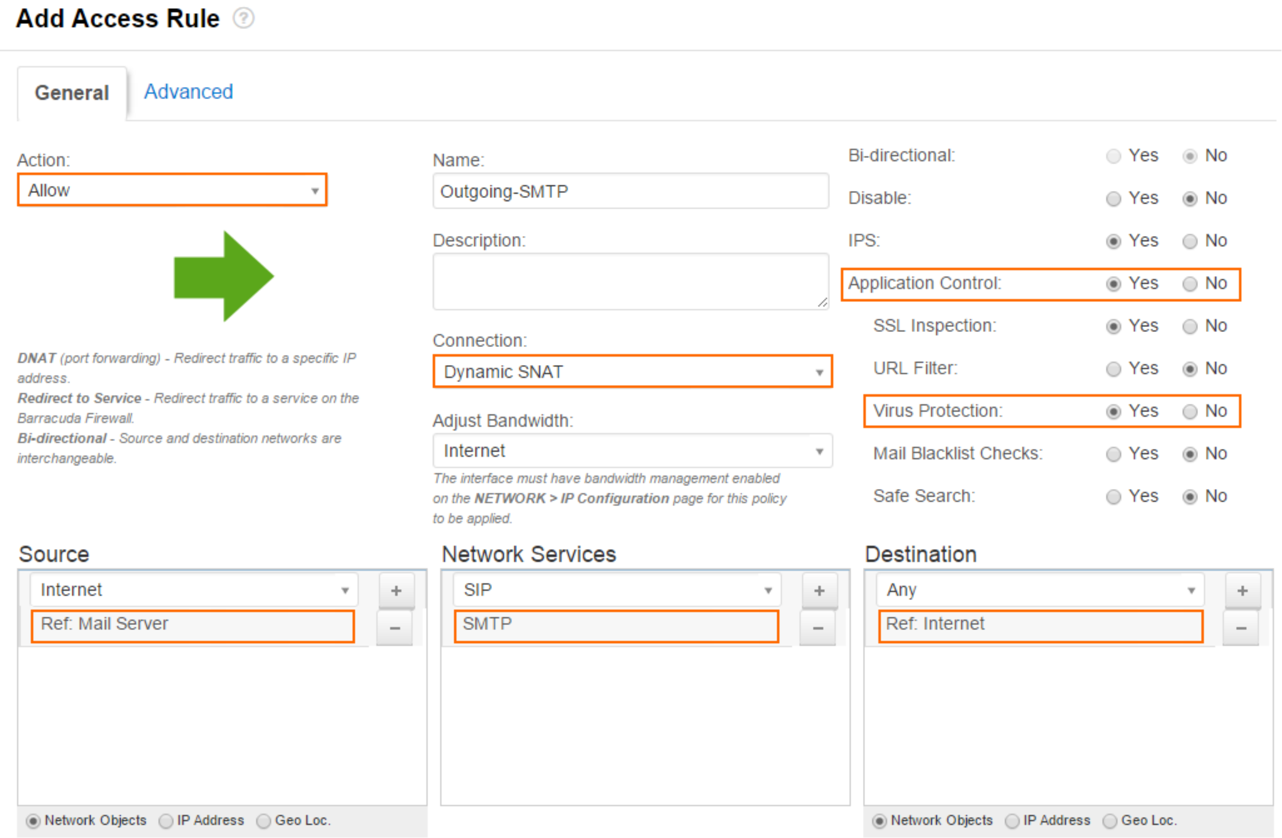
Redirect: Local Networks; Ref: Mail Server
Balancing: Off
ARP □
○ Network Objects ● IP Address

4. Click **Save**.

Step 4. (optional) Create an access rule for outgoing SMTP connections

Create an access rule to scan outgoing SMTP traffic from your internal mail server or mail clients for malware.

1. Go to **FIREWALL > Firewall Rules**.
2. Create an access rule with the following settings:
   - **Action** – Select **Allow**.
   - **Connection** – If used for an internal mail server, create and select a connection object using the public IP address that your mail server's MX record resolves to as the source IP address. If this rule applies to SMTP clients, select **Dynamic SNAT**.
   - **Source** – Create and select a network object containing your mail server IP addresses, or for SMTP client connections the network containing the SMTP clients, and click **+**.
   - **Network Services** – Select **SMTP** for outgoing mail server traffic, or create a service object for TCP port 587 for outgoing mail client traffic, and click **+**.
   - **Destination** – Select **Internet**, and click **+**.
3. Enable **Application Control**, **SSL Inspection**, and **Virus Protection**.



Add Access Rule

General | Advanced

Action: Allow

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: Outgoing-SMTP

Description:

Connection: Dynamic SNAT

Adjust Bandwidth: Internet

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

Bi-directional:	○ Yes	● No
Disable:	○ Yes	● No
IPS:	● Yes	○ No
Application Control:	● Yes	○ No
SSL Inspection:	● Yes	○ No
URL Filter:	○ Yes	● No
Virus Protection:	● Yes	○ No
Mail Blacklist Checks:	○ Yes	● No
Safe Search:	○ Yes	● No

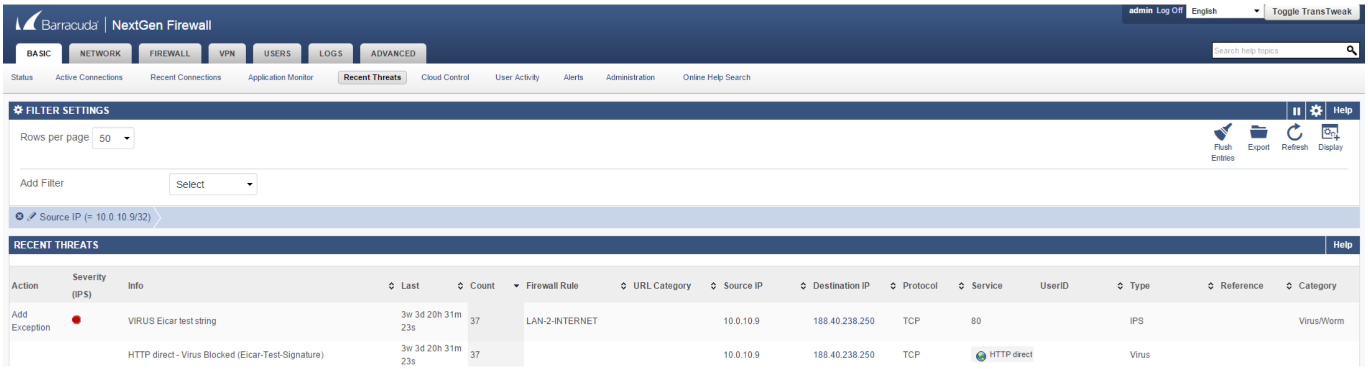
Source	Network Services	Destination
Internet	SIP	Any
Ref: Mail Server	SMTP	Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc.		● Network Objects ○ IP Address ○ Geo Loc.

4. Click **Save**.

Monitoring and testing

You can test the virus scanner setup by sending EICAR test files from http://www.eicar.com via email to a mail server located behind the firewall.

To monitor detected viruses and malware, go to the **BASIC > Recent Threats** page.



FILTER SETTINGS

Rows per page: 50

Add Filter: Select

Source IP (= 10.0.10.9/32)

RECENT THREATS

Action	Severity (IPS)	Info	Last	Count	Firewall Rule	URL Category	Source IP	Destination IP	Protocol	Service	UserID	Type	Reference	Category
Add Exception	●	VIRUS Eicar test string	3w 3d 20h 31m 23s	37	LAN-2-INTERNET		10.0.10.9	188.40.238.250	TCP	80		IPS		Virus/Worm
		HTTP direct - Virus Blocked (Eicar-Test-Signature)	3w 3d 20h 31m 23s	37			10.0.10.9	188.40.238.250	TCP	HTTP direct		Virus		

Next steps

- Customize the text used to replace removed email attachments. For more information, see Custom Block Pages.

Figures

1. virus_protection_smtp_68_00.png
2. virus_protection_smtp_68_01.png
3. virus_protection_smtp_68_02.png
4. virus_protection_smtp_68_03.png
5. virus_protection_68_05.png