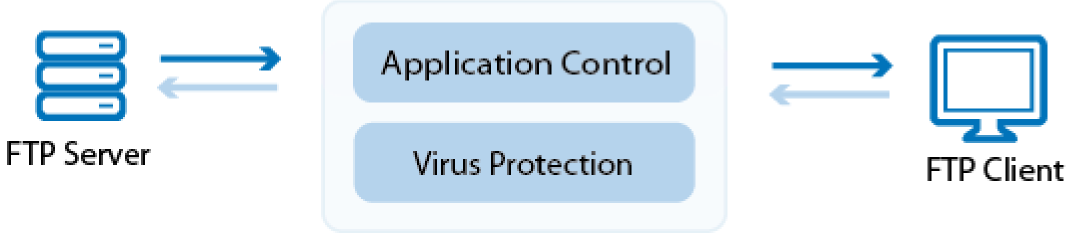
How to Configure Virus Scanning in the Firewall for FTP Traffic

https://campus.barracuda.com/doc/48660787/

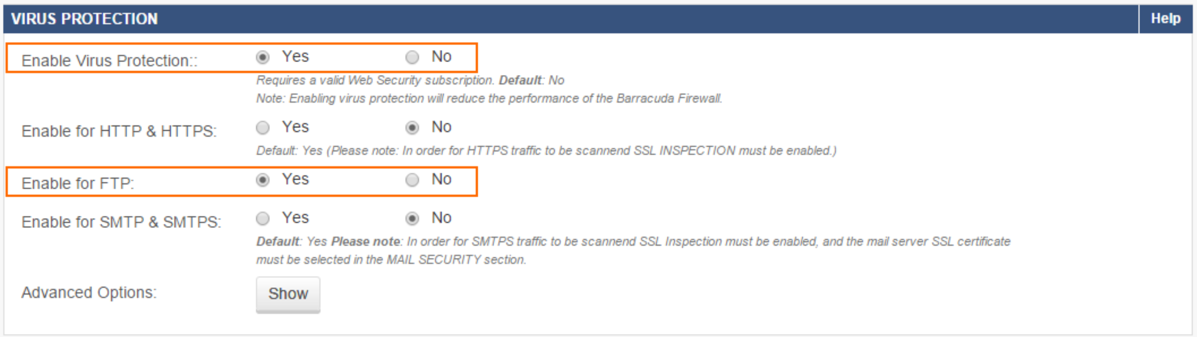
The X-Series Firewall scans FTP traffic for malware on a per-access-rule basis when FTP virus scanning in the firewall is enabled. Both active and passive FTP is supported; SSL-encrypted FTP is not supported. Depending on the access rule, you can either protect your FTP server from uploads containing malware, or scan files downloaded from external FTP servers. Since the FTP protocol does not contain any MIME-type information, all files are scanned regardless of the MIME-type list configured for the virus scanner. When an FTP download is initiated, the FTP client creates a local, zero-byte file. Normally, the transferred data would be written to this file until the download is finished. However, if the file is determined to be malware, the connection is terminated immediately, leaving the zero-byte file or file fragment (if data trickling is enabled) on the client. Depending on the FTP client, it may attempt to download the file multiple times; each time the connection will be reset by the firewall.



Step 1. Enable Virus Protection for FTP

Enable support for virus scanning FTP connections in the firewall.

1. Go to the **FIREWALL > Settings** page.
2. Make sure that **Application Control** is enabled.
3. In the **Virus Protection** section,
    1. Set **Enable Virus Protection** to **Yes**.
    2. Set **Enable for FTP** to **Yes**.



VIRUS PROTECTION — Help

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

4. (optional) Click **Show** to configure **Advanced Options**:

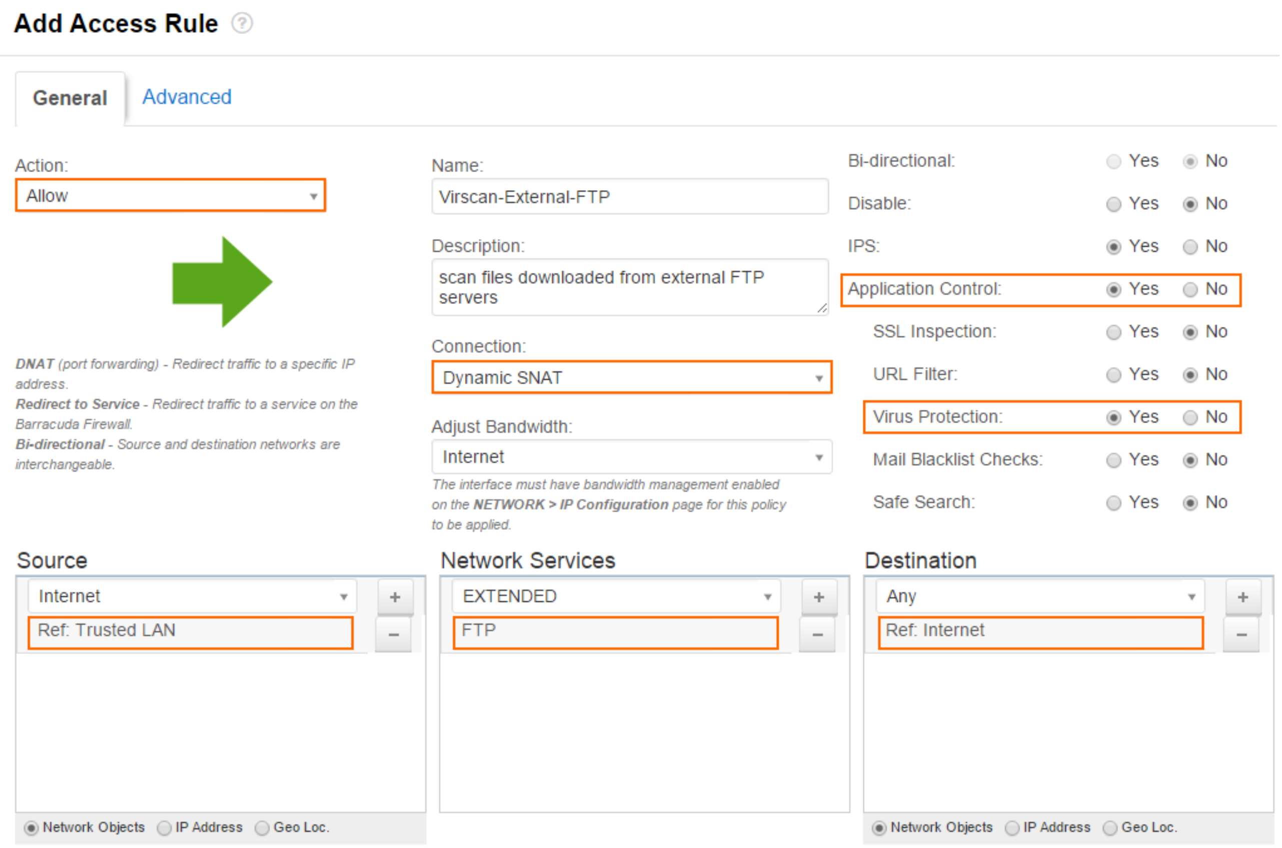
    Changing settings for the virus scanner also affects virus scanning for other services.

    1. Change the default behavior **If Virus Scanner is not available**.
        - **Block All** – (default) Block all files.
        - **Allow All** – All files will be allowed.
    2. 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.
        - **Data Trickling** – Change how fast and how much data is transmitted. Change these settings if your FTP client times out while waiting for the file to be scanned.
    3. Click **Save**.
5. Click **Save**.

Step 2. Create an access rule for FTP client downloads

To scan files downloaded from external FTP servers, create a matching access rule and enable Application Control and Virus Protection.

1. Go to **FIREWALL > Firewall Rules**.
2. Create an access rule with the following settings:
    - **Action** – Select **Allow**.
    - **Connection** – Select **Dynamic SNAT**.
    - **Source** – Select **Trusted LAN**, and click **+**.
    - **Network Services** – Select **FTP**, and click **+**.
    - **Destination** – Select **Internet**, and click **+**.
3. Enable **Application Control** 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: Virscan-External-FTP

Description: scan files downloaded from external FTP servers

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: Internet — Ref: Trusted LAN
● Network Objects ○ IP Address ○ Geo Loc.

Network Services: EXTENDED — FTP

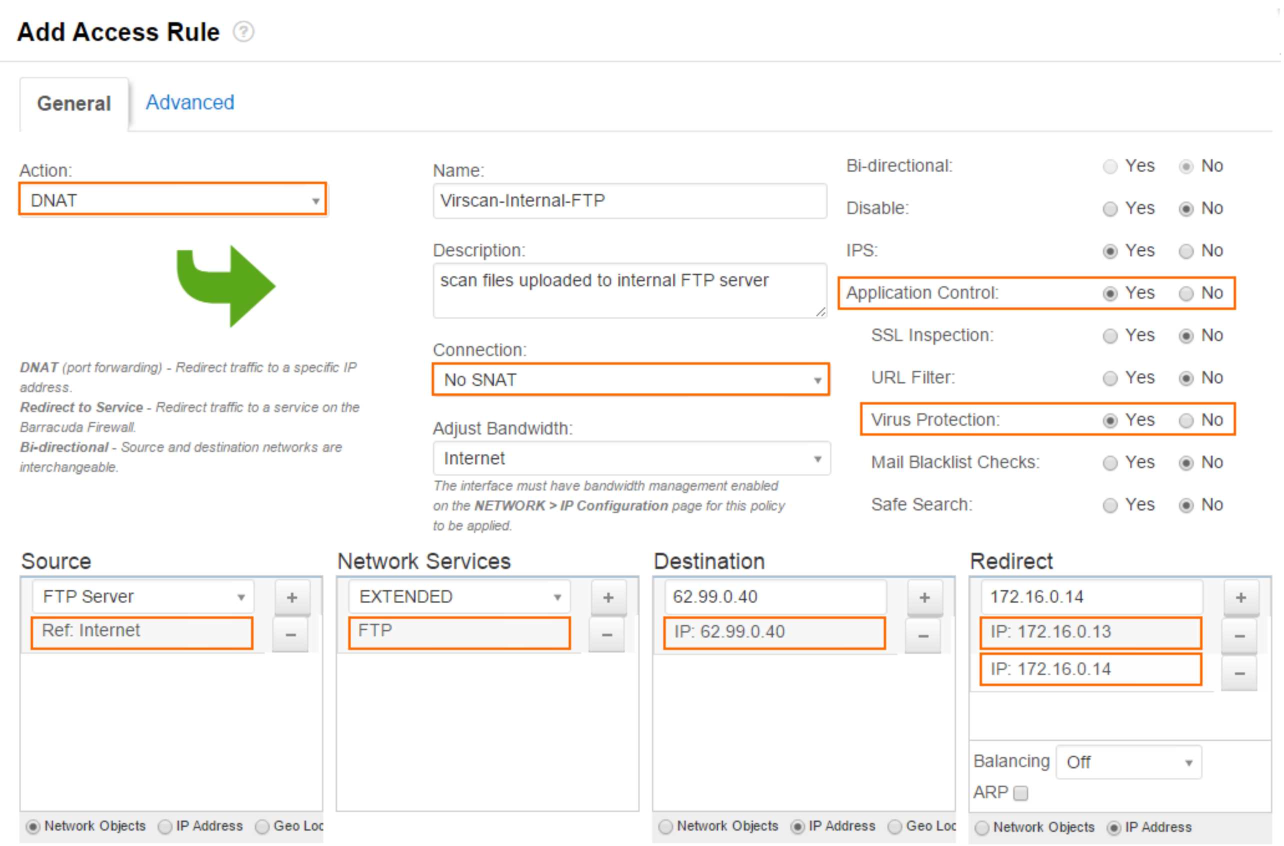
Destination: Any — Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc.

4. Click **Save**.

Step 3. (optional) Create a DNAT access rule to protect an internal FTP server

To protect an internal FTP server from receiving infected files, create a matching DNAT access rule, and enable Application Control and Virus Protection.

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 **FTP**, and click **+**.
    - **Destination** – Enter the public IP address or FQDN used for your FTP server, and click **+**.
    - **Redirect** – Enter the IP address(es) of your internal FTP server(s), and click **+**.
3. Enable **Application Control** and **Virus Protection**.



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: Virscan-Internal-FTP

Description: scan files uploaded to internal FTP server

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: FTP Server
Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc

Network Services: EXTENDED
FTP

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

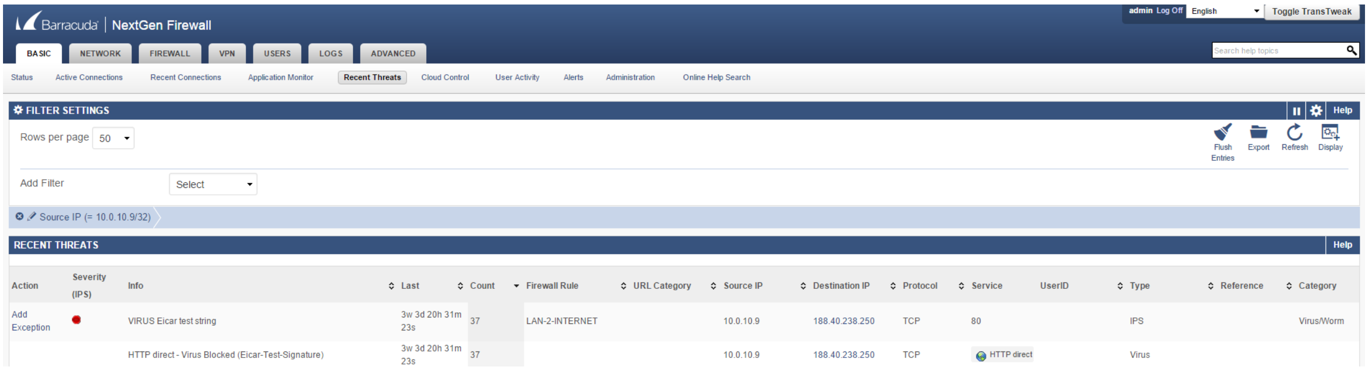
Redirect: 172.16.0.14
IP: 172.16.0.13
IP: 172.16.0.14
Balancing: Off
ARP □
○ Network Objects ● IP Address

4. Click **Save**.

Monitoring and testing

You can test the virus scanner setup by downloading EICAR test files from an FTP server. Files that are malware are not downloaded. 0-byte stub files are created by the FTP client.

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



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		

Figures