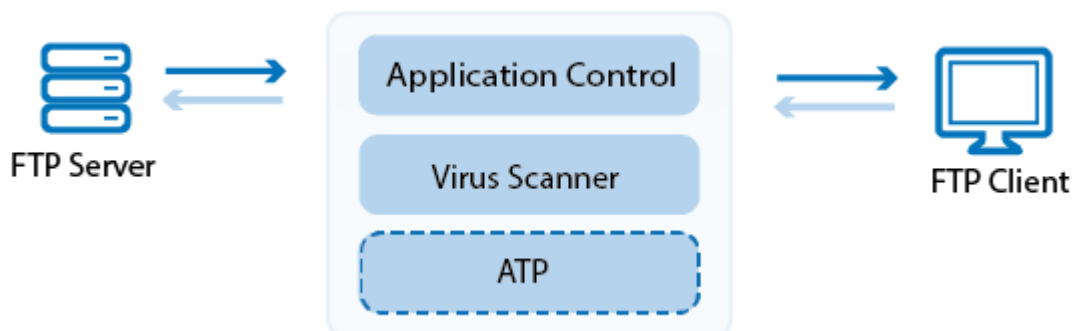


How to Configure Virus Scanning in the Firewall for FTP Traffic

<https://campus.barracuda.com/doc/53248932/>

The F-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; outgoing SSL-encrypted FTPS connections are also 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. Scanning incoming traffic for FTPS servers is not supported. 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. If ATP is enabled, files passed by the virus scanner are then uploaded to be analyzed in the Barracuda ATP Cloud. ATP can be used only in the **deliver first, then scan** mode for FTP client connections. Files uploaded to FTP servers behind the firewall cannot be scanned by ATP.



Before You Begin

- Enable Application Control. For more information, see [How to Enable Application Control](#).
- Create a Virus Scanner service. For more information, see [Virus Scanner](#).
- (optional) Configure File Content Filtering in the Firewall. For more information, see [File Content Filtering in the Firewall](#)
- (optional) Configure ATP in the Firewall. For more information, see [How to Configure ATP in the Firewall](#).
- (optional) Configure SSL Interception for outbound FTPS traffic. For more information, see [How to Configure SSL Interception in the Firewall](#).

Step 1. Configure the Virus Scanner Engine(s)

Select and configure a virus scanner engine. You can use Avira and ClamAV either separately or together. Barracuda NextGen Firewall F100 and F101 can only use Avira.

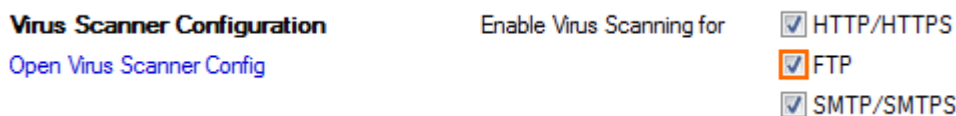
Using both virus scanner engines significantly increases CPU utilization and load.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. Click **Lock**.
3. Enable the virus scanner engines of your choice:
 - Enable the Avira AV engine by selecting **Yes** from the **Enable Avira Engine** list.
 - Enable the ClamAV engine by selecting **Yes** from the **Enable ClamAV** list.
4. Click **Send Changes** and **Activate**.

Step 2. Enable Virus Scanning for FTP

Enable support for virus scanning FTP connections in the Firewall service.

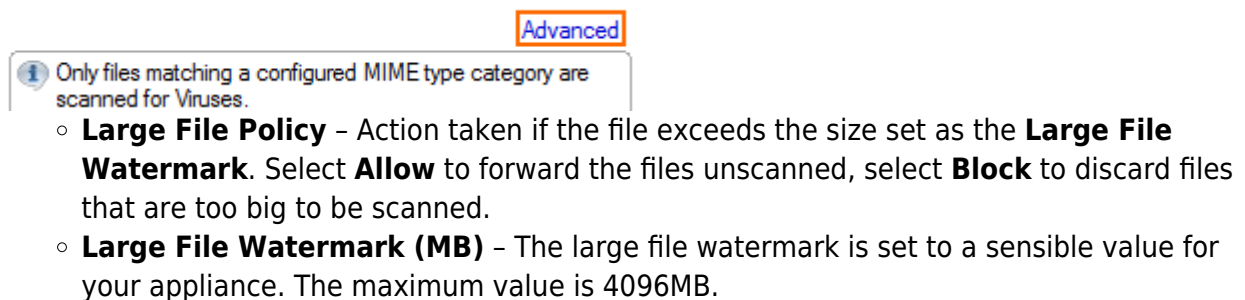
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Virus Scanner Configuration** section, select the **FTP** check box.



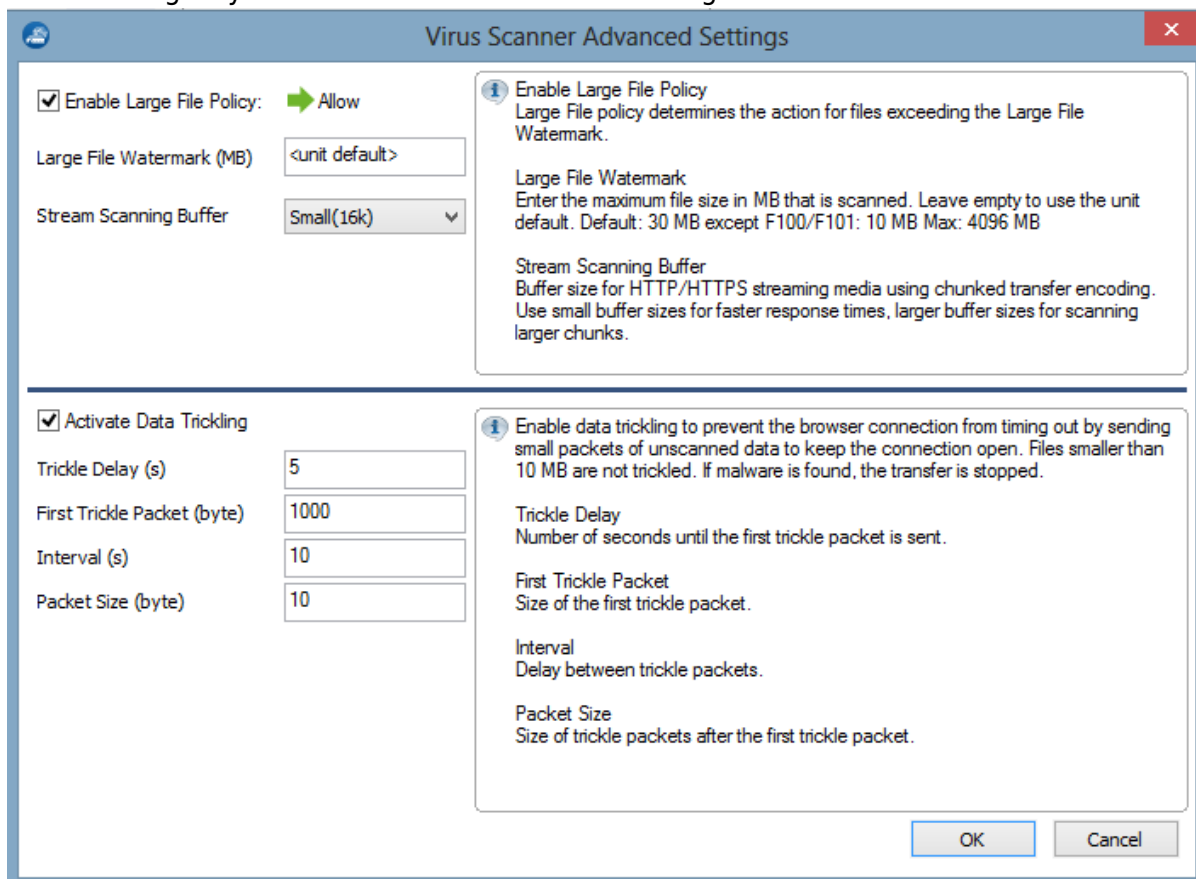
4. (optional) Change the **Action if Virus Scanner is unavailable**.



5. (optional) Click on **Advanced**:



- **Stream Scanning Buffer** – Select the buffer size for HTTP/HTTPS streaming media using chunked transfer encoding. Select **Small** for faster response times, **Big** to scan larger chunks before forwarding the stream to the client.
- **Data Trickling Settings** – Change how fast and how much data is transmitted. Change these settings if your browser times out while waiting for the file to be scanned.



The screenshot shows the "Virus Scanner Advanced Settings" dialog box. It is divided into two main sections. The top section is for "Large File Policy" and "Stream Scanning Buffer". The bottom section is for "Data Tricking".

Large File Policy Section:

- Enable Large File Policy: ➔ Allow
- Large File Watermark (MB):
- Stream Scanning Buffer:

Data Tricking Section:

- Activate Data Tricking
- Trickle Delay (s):
- First Trickle Packet (byte):
- Interval (s):
- Packet Size (byte):

Informational text on the right side of the dialog explains the settings:


- Enable Large File Policy:** Large File policy determines the action for files exceeding the Large File Watermark. Large File Watermark: Enter the maximum file size in MB that is scanned. Leave empty to use the unit default. Default: 30 MB except F100/F101: 10 MB Max: 4096 MB. Stream Scanning Buffer: Buffer size for HTTP/HTTPS streaming media using chunked transfer encoding. Use small buffer sizes for faster response times, larger buffer sizes for scanning larger chunks.
- Enable data trickling:** to prevent the browser connection from timing out by sending small packets of unscanned data to keep the connection open. Files smaller than 10 MB are not trickled. If malware is found, the transfer is stopped. Trickle Delay: Number of seconds until the first trickle packet is sent. First Trickle Packet: Size of the first trickle packet. Interval: Delay between trickle packets. Packet Size: Size of trickle packets after the first trickle packet.

Buttons: OK, Cancel

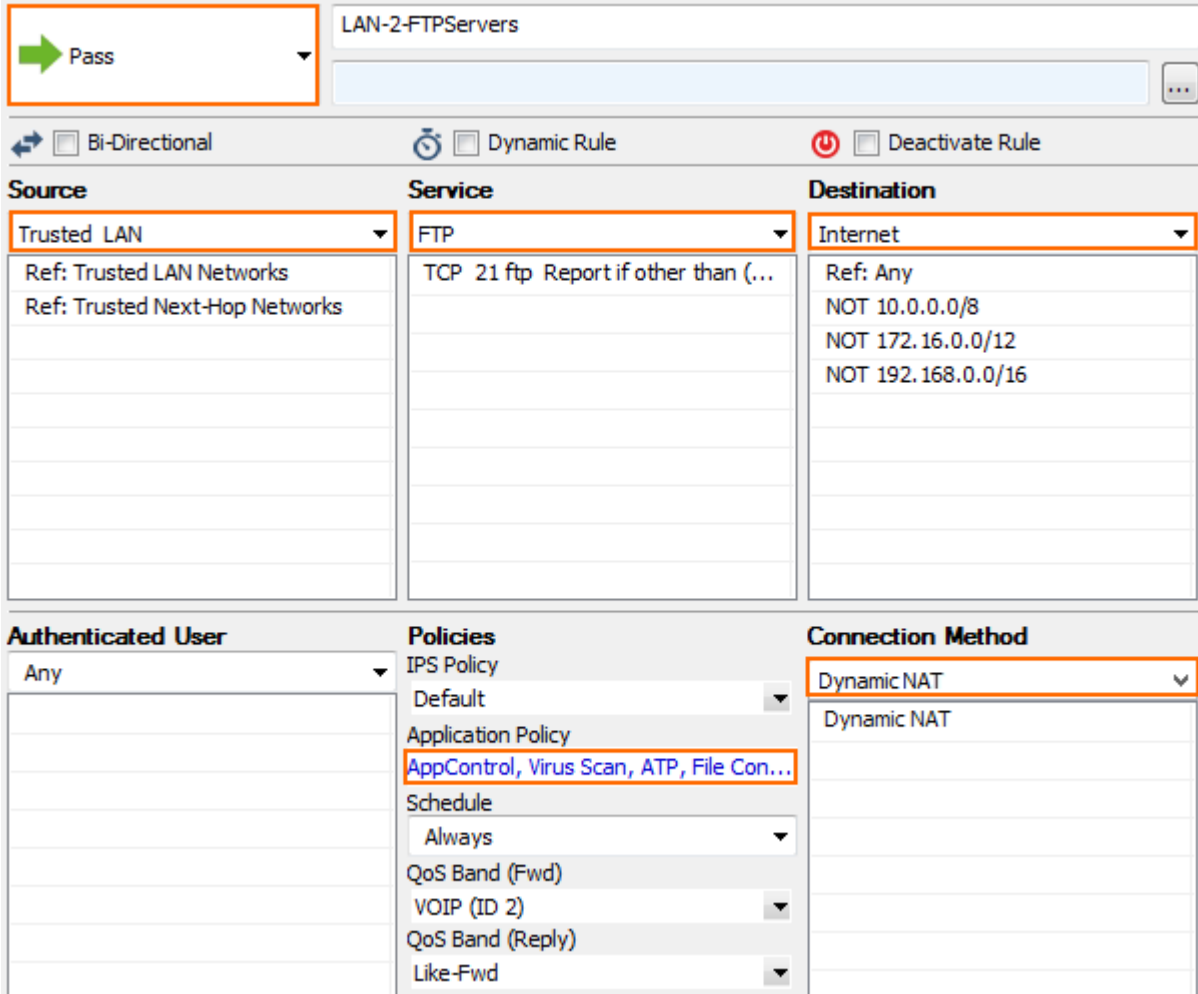
6. Click **Send Changes** and **Activate**.

Step 4. Create 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 Scanning.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your incoming SMTP traffic:

- **Action** – Select **PASS**.
- **Source** – Select **Trusted Networks**.
- **Destination** – Select **Internet**.
- **Service** – Select **FTP**.
- **Connection Method** – Select **Dynamic NAT**.



LAN-2-FTPServers

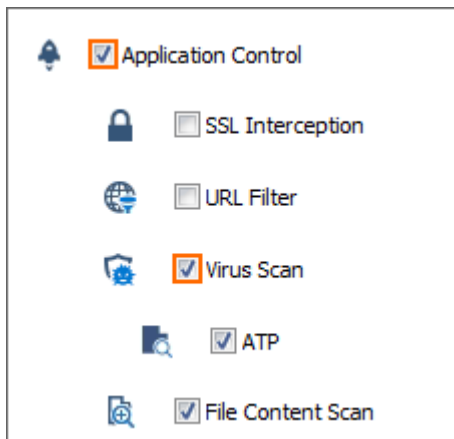
Pass

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source	Service	Destination
Trusted LAN	FTP	Internet
Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks	TCP 21 ftp Report if other than (...)	Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Application Policy AppControl, Virus Scan, ATP, File Con... Schedule Always QoS Band (Fwd) VOIP (ID 2) QoS Band (Reply) Like-Fwd	Dynamic NAT


7. Click on the **Application Policy** link and select:
- **Application Control** – required.
 - **SSL Interception** – optional.
 - **Virus Scan** – required.
 - **ATP** – optional.
 - **File Content Scan** – optional.

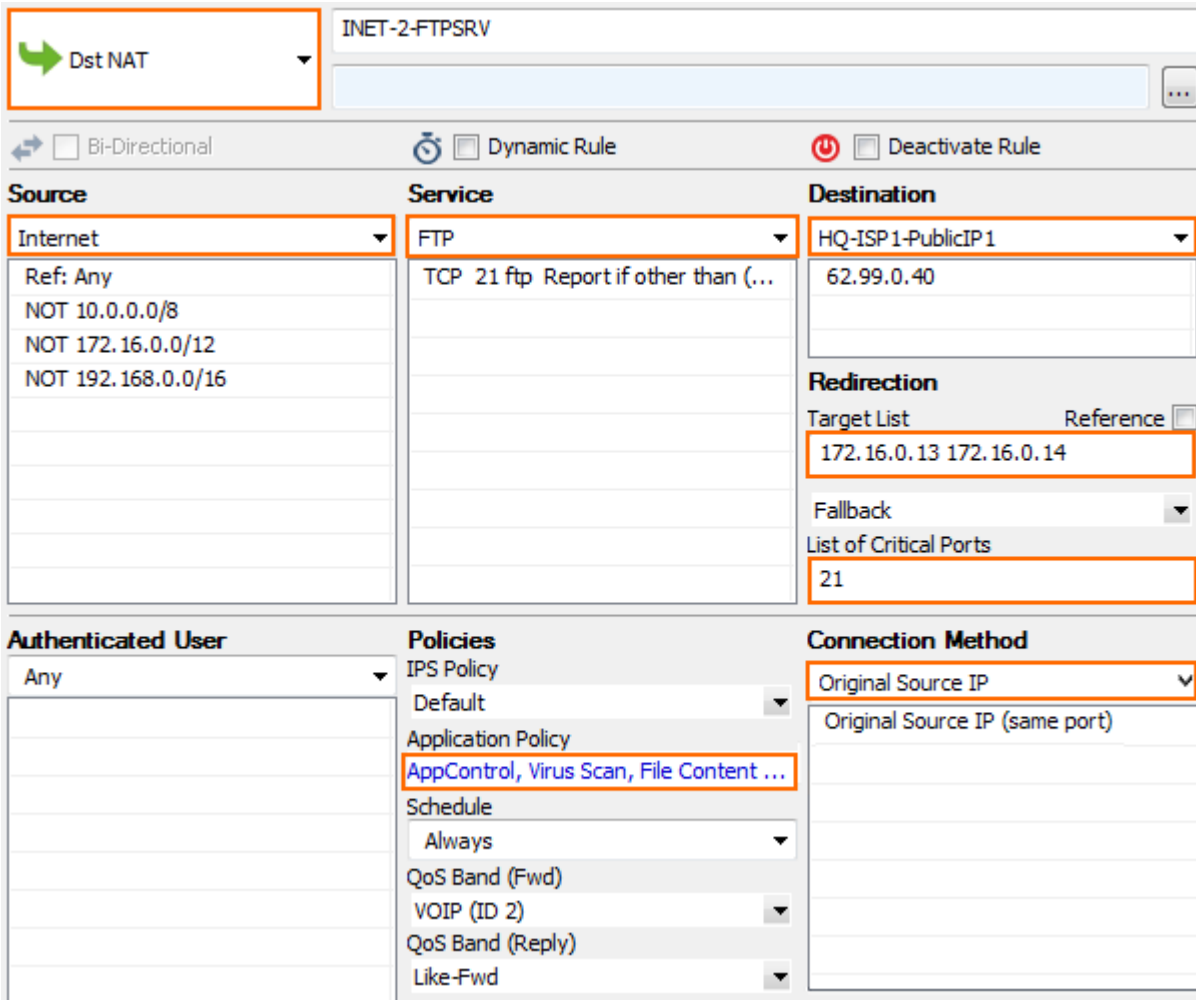


8. Click **Send Changes** and **Activate**.

Step 5. (optional) Create a Dst NAT Access Rule to Protect Internal FTP Server

To protect an internal FTP server from receiving infected files, create a matching Dst NAT access rule, and enable Application Control, Virus Scanning, and, as an option, File Content Scan. Using ATP for incoming FTP connections is not supported.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your incoming SMTP traffic:
 - **Action** – Select **Dst NAT**.
 - **Source** – Select **Internet**.
 - **Service** – Select **FTP**.
 - **Destination** – Enter the public IP address the FQDN or the FTP server resolves to.
 - **Redirection** – Enter the IP address of your internal FTP server. Enter multiple IP addresses separated by a space to enable failover or basic load balancing support. For more information, see [How to Create a Destination NAT Access Rule](#).
 - **Connection Method** – Select **Original Source IP**.



INET-2-FTPSRV

Dst NAT

Bi-Directional Dynamic Rule Deactivate Rule

Source	Service	Destination
Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16	FTP TCP 21 ftp Report if other than (...)	HQ-ISP1-PublicIP1 62.99.0.40

Redirection

Target List Reference

172.16.0.13 172.16.0.14

Fallback

List of Critical Ports

21

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Application Policy AppControl, Virus Scan, File Content ... Schedule Always QoS Band (Fwd) VOIP (ID 2) QoS Band (Reply) Like-Fwd	Original Source IP Original Source IP (same port)

7. Click on the **Application Policy** link and select:
 - **Application Control** - required.
 - **Virus Scan** - required.
 - **File Content Scan** - optional.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Monitoring and Testing

Test the Virus Scanning 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.

Host: 172.16.0.13 Username: mzoller Password: ●●●●●● Port: Quickconnect ▼

Status: Insecure server, it does not support FTP over TLS.
 Status: Connected
 Status: Retrieving directory listing...
 Status: Directory listing of "/home/mzoller" successful
 Status: Retrieving directory listing of "/home/mzoller/infected" ...
 Status: Directory listing of "/home/mzoller/infected" successful

Local site: C:\Users\mzoller\Documents\TMP\				Remote site: /home/mzoller/infected				
Filename	Filesize	Filetype	Last modified	Filename	Filesize	Filetype	Last modified	Permissi
..				..				
infected_ZP_file.zip	0	Compressed (zipp...	30.10.2015 10:32:27	infected_ZP_file.zip	12.298.217	Comprese...	30.10.2015 10:4...	0644
infected_PDF.zip	0	Compressed (zipp...	30.10.2015 10:32:27	infected_PDF.zip	32.717.072	Comprese...	30.10.2015 10:4...	0644
eicarcom2.zip	0	Compressed (zipp...	30.10.2015 10:32:24	eicarcom2.zip	308	Comprese...	30.10.2015 10:4...	0644

To monitor detected viruses and malware, go to the **FIREWALL > Threat Scan** page.

Monitor Live History Threat Scan Audit Log Shaping Users Dynamic Host Rules Forwarding Rules

Traffic Selection Forward, Local In, Local Out, IPv4, IPv6 ▼

A..	Action	Source	User	Scan Type	Destination	Risk/Severity	Threat Cate...	Application Cont...	More Info	R...	Info	Count	Last
▶ (2)	IPS												
▲ (3)	Virus Scan												
▲	Scan	10.0.10.11		Virus Scan	172.16.0.13			LAN-2-FTPServers			Virus Blocked (Eicar-Test-Signature)	1	5s
▲	Scan	10.0.10.11		Virus Scan	172.16.0.13			LAN-2-FTPServers			Virus Blocked (Eicar-Test-Signature)	1	5s
▲	Scan	10.0.10.11		Virus Scan	172.16.0.13			LAN-2-FTPServers			Virus Blocked (Eicar-Test-Signature)	1	7s

Next Steps

- To combine ATP with virus scanning, see [Advanced Threat Protection \(ATP\)](#) and [How to Configure ATP in the Firewall](#).
- To combine virus scanning with file content filtering, see [File Content Filtering in the Firewall](#).

Figures

1. virus_scanning_ftp_traffic_atp-01.png
2. AV_FTP_05.png
3. AV_FTP_06.png
4. AV_SMTP_02.png
5. FW_virus_scan_advanced.png
6. FW_Rule_Add01.png
7. AV_FTP_01.png
8. AV_FTP_07.png
9. FW_Rule_Add01.png
10. AV_FTP_03.png
11. AV_FTP_FTP_Client.png
12. AV_FTP_Threat_Monitor.png

© Barracuda Networks Inc., 2020 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.