

## How to Enable the Virus Scanner

<https://campus.barracuda.com/doc/73698321/>

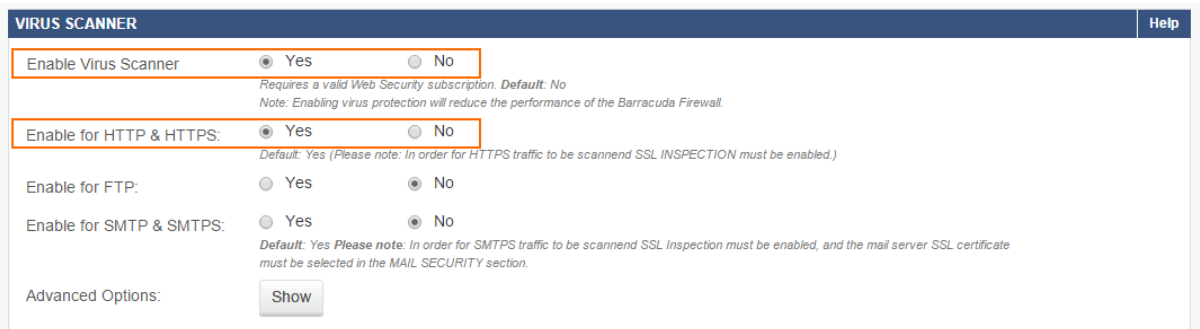
The firewall scans traffic for malware on a per-access-rule basis when virus scanning is enabled. If a user downloads a file containing malware, the firewall detects and discards the infected file and redirects the user to a customizable block page. You can combine virus scanning with SSL Interception and Advanced Threat Protection. A Malware subscription is required.

### Before You Begin

- To scan HTTPS traffic, enable SSL Interception. For more information, see [How to Configure SSL Interception in the Firewall](#).

### Step 1. Enable and Configure the Virus Scanner

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 Scanner** section, set **Enable Virus Scanner** to **Yes**.
  - To scan web traffic, set **Enable for HTTP & HTTPS** to **Yes**. For more information, see [How to Configure Virus Scanning in the Firewall for Web Traffic](#).
  - To scan FTP traffic, set **Enable for FTP** to **Yes**. For more information, see [How to Configure Virus Scanning in the Firewall for FTP Traffic](#).
  - To scan mail traffic, set **Enable for SMTP & SMTPS** to **Yes**. For more information, see [How to Configure Virus Scanning for Mail Traffic](#).



**VIRUS SCANNER** Help

Enable Virus Scanner  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 scanned 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 scanned SSL Inspection must be enabled, and the mail server SSL certificate must be selected in the MAIL SECURITY section.

Advanced Options:

5. (optional) Click **Show** to configure **Advanced Options**.
6. Click **Save**.

### Step 2. Enable the Virus Scanner in Access Rules

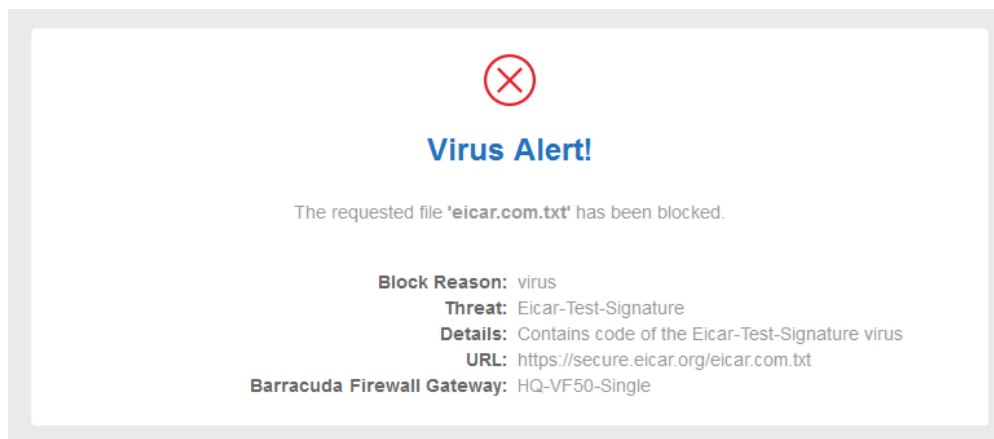
Create or edit an access rule for the connections that you want to apply virus scanning to. Virus

scanning can be enabled for all Pass and DNAT rules.


For more information, see [How to Configure Virus Scanning in the Firewall for Web Traffic](#), [How to Configure Virus Scanning in the Firewall for FTP Traffic](#), and [How to Configure Virus Scanning for Mail Traffic](#).

## Monitoring and Testing

You can test the Virus Scanner setup by downloading EICAR test files from <http://www.eicar.com>. The block page is customizable. For more information, see [How to Configure Custom Block Pages and Texts](#).



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



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		VirusWorm
		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

1. virus\_protection\_http\_68\_02.png
2. virus\_protection\_http\_68\_04.png
3. virus\_protection\_http\_68\_05.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.