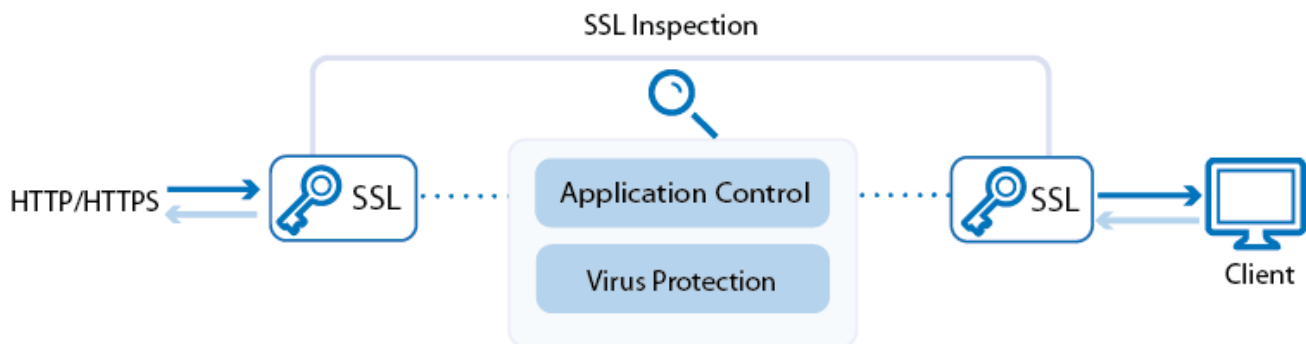


## How to Configure Virus Protection in the Firewall for Web Traffic

<https://campus.barracuda.com/doc/48660783/>

The NextGen Firewall X-Series scans web traffic for malware on a per-access-rule basis when Virus Protection 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 Protection with SSL Inspection to also scan HTTPS connections.



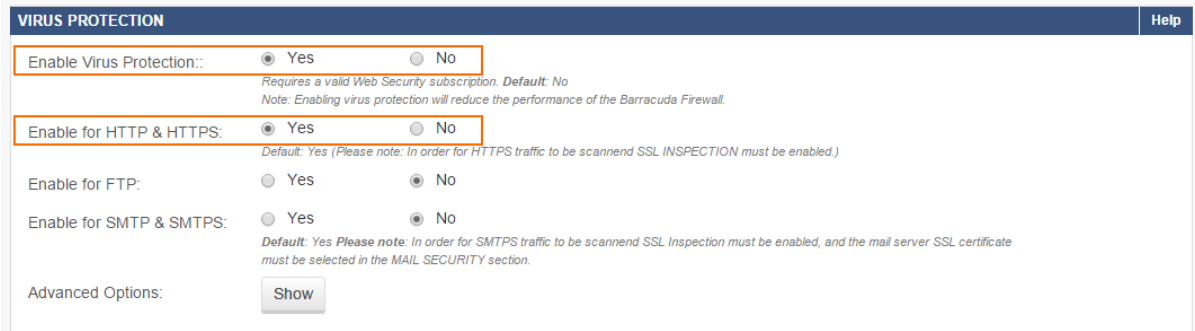
### Before you begin

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

### Step 1. Enable Virus Protection in the firewall

Enable Application Control and Virus Protection.

1. Go to the **FIREWALL > Settings** page.
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 HTTP & HTTPS** to **Yes**.



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

Changing settings for the virus scanner also affects virus scanning for mail traffic.

1. Change the default behavior **If Virus Scanner is not available**.

- **Block All** – (default) Block all files.
- **Allow All** – All pages 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.
- **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. 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. For more information, see **Default MIME Types** in [Virus Protection in the Firewall](#).
- **Exemptions** – Define exemptions from scanning based on IP addresses and hostnames.
- **Archives** – Enable, to scan archives and block archive files that are encrypted and cannot be scanned.
- **Data Trickling** – 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.

3. Click **Save**.

6. Click **Save**.

## Step 2. Enable Virus Protection in access rules

Create or edit an access rule for the HTTP / HTTPS connections that you want to apply Virus Protection to. Virus Protection can be enabled for all Allow and DNAT rules.

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 **HTTP+S**, and click +.
  - **Destination** – Select **Internet**, and click +.
3. Enable **Application Control** and **Virus Protection**.
  4. (optional) Enable **SSL Inspection**.

**Edit 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:  
HTTP-HTTPS-Traffic

Description:  
Enable virus scanning of HTTP/S traffic for local network users.

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**  

Any

Ref: Trusted LAN

**Network Services**  

HTTP

HTTP+S

**Destination**  

Any

Ref: Internet


☒ Network Objects ☐ IP Address ☐ Geo Loc.

☒ Network Objects ☐ IP Address ☐ Geo Loc.

5. Click **Save**.

## 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 [Custom Block Pages](#).

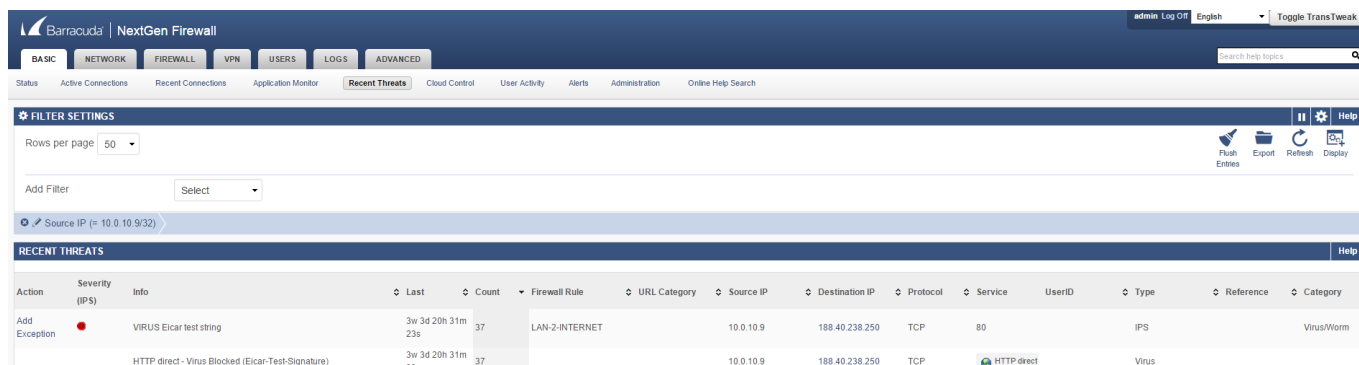
  

## Virus Alert!

The requested file '**eicar.com.txt**' has been blocked.

**Block Reason:** virus  
**Threat:** Eicar-Test-Signature  
**Details:** Contains code of the Eicar-Test-Signature virus  
**URL:** <https://secure.eicar.org/eicar.com.txt>  
**Barracuda Firewall Gateway:** HQ-VF50-Single

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



The screenshot shows the Barracuda NextGen Firewall web interface. The top navigation bar includes tabs for BASIC, NETWORK, FIREWALL, VPN, USERS, LOGS, and ADVANCED. The 'RECENT THREATS' tab is selected. Below the navigation bar, there is a 'FILTER SETTINGS' section with a 'Rows per page' dropdown set to 50 and an 'Add Filter' button. The main content area displays a table of recent threats. The table has columns for Action, Severity (IPS), Info, Last, Count, Firewall Rule, URL Category, Source IP, Destination IP, Protocol, Service, UserID, Type, Reference, and Category. Two threats are listed: 'VIRUS Eicar test string' and 'HTTP direct - Virus Blocked (Eicar-Test-Signature)'. Both threats have a severity of 37 and are categorized as 'VirusWorm' and 'Virus' respectively.

Action	Severity (IPS)	Info	Last	Count	Firewall Rule	URL Category	Source IP	Destination IP	Protocol	Service	UserID	Type	Reference	Category
Add Exception	37	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
	37	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\_01.png
2. virus\_protection\_http\_68\_02.png
3. virus\_protection\_http\_68\_03.png
4. virus\_protection\_http\_68\_04.png
5. virus\_protection\_http\_68\_05.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.