How to Enable the Virus Scanner

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

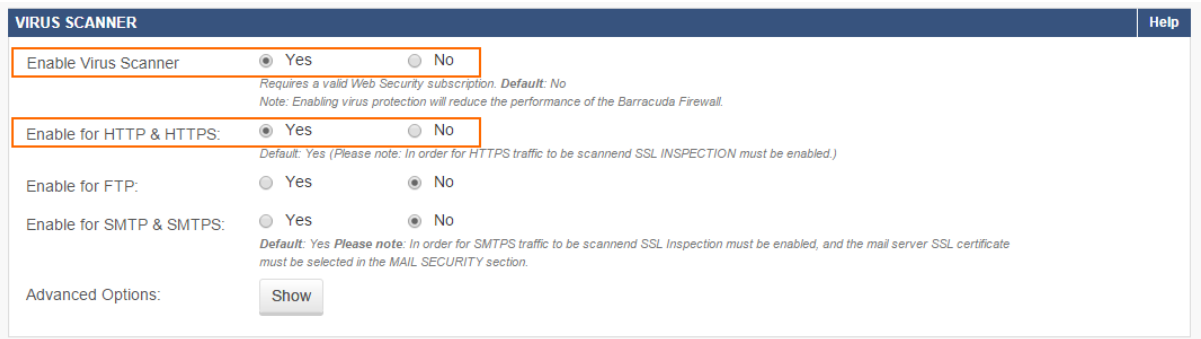
The firewall scans traffic for malware on a per-access-rule basis when virus scanning is enabled. If a user downloads a file containing malware, the firewall detects and discards the infected file and redirects the user to a customizable block page. You can combine virus scanning with SSL Interception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



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

Step 2. Enable the Virus Scanner in Access Rules

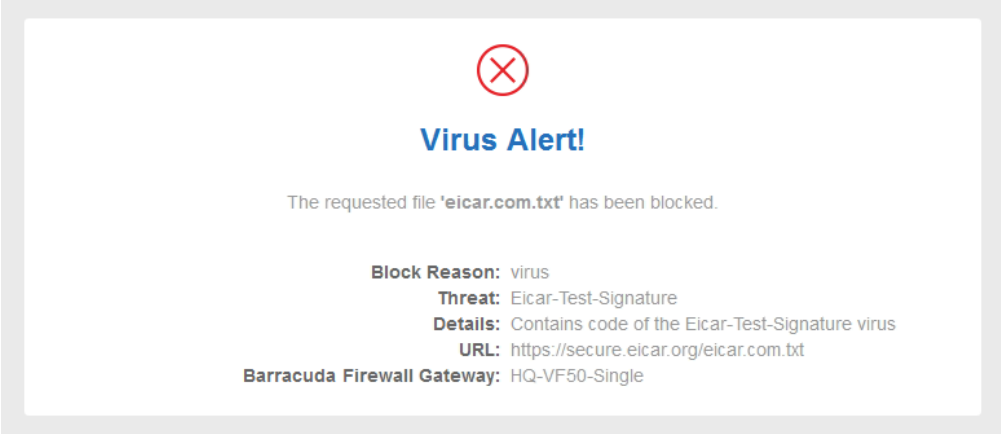
Create or edit an access rule for the connections that you want to apply virus scanning to. Virus

scanning can be enabled for all Pass and DNAT rules.

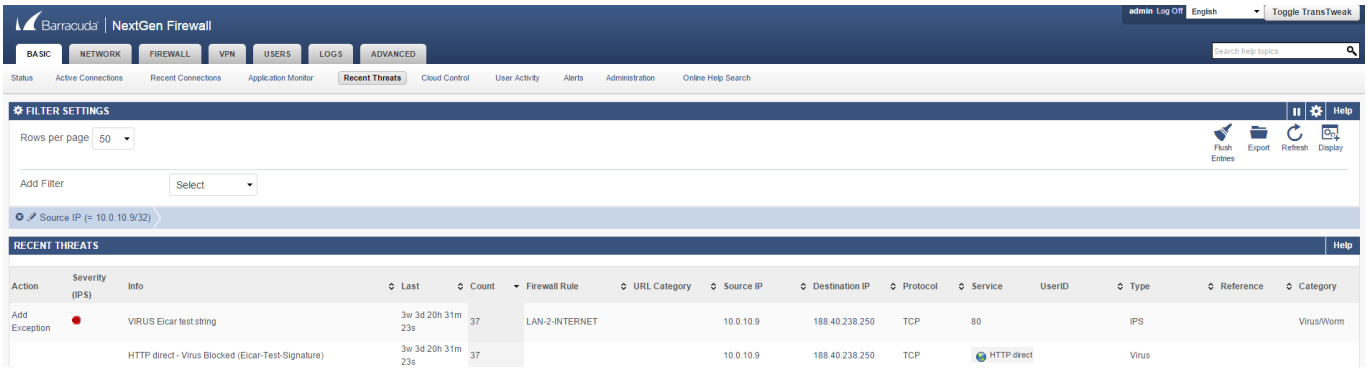
For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic, How to Configure Virus Scanning in the Firewall for FTP Traffic, and How to Configure Virus Scanning for Mail Traffic.

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.



Figures

1. virus_protection_http_68_02.png
2. virus_protection_http_68_04.png
3. virus_protection_http_68_05.png