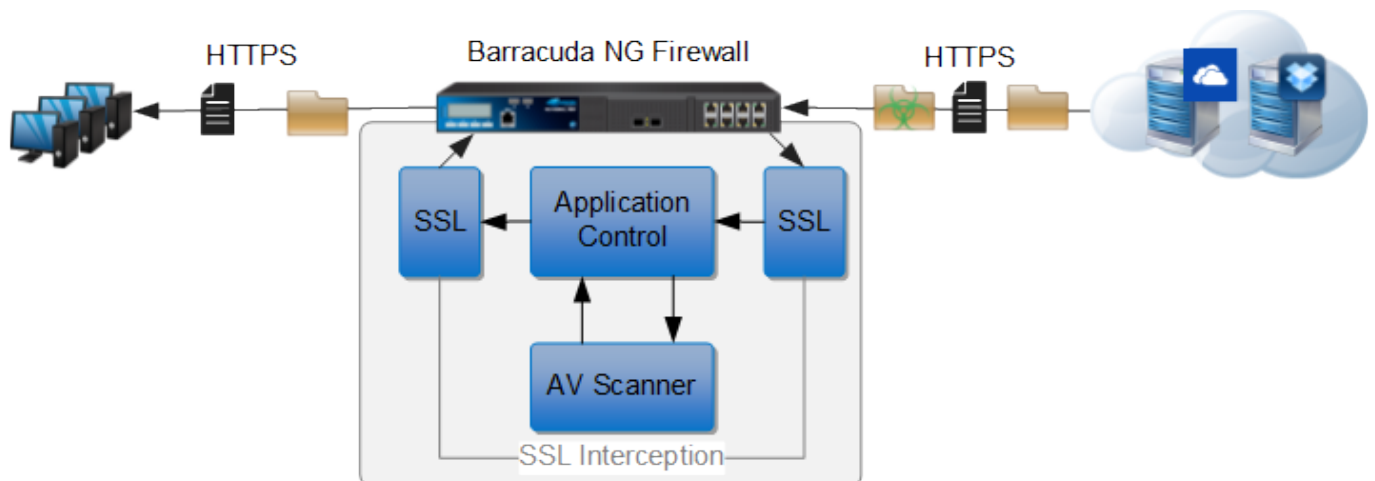


How to Configure Virus Scanning in the Firewall

<https://campus.barracuda.com/doc/43847041>The Barracuda NG Firewall scans incoming traffic for malware on a per access rule basis when AV scanning in the firewall is enabled. If a user downloads a file containing malware, the Barracuda NG Firewall detects and discards the infected file and redirects the user to a warning page. You can combine virus scanning with SSL Interception to also scan SSL encrypted connections.



In this article:

Before You Begin

- Enable Application Control 2.0. For more information, see [How to Enable Application Control 2.0](#).
- Create a Virus Scanner service. For more information, see [Virus Scanner](#)

Step 1. Enable the Virus Scanner Service

Ensure that the Virus Scanner service is enabled.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Virus-Scanner > Service Properties**.
2. Click **Lock**.
3. From the **Enable Service** list, select **yes**.
4. Click **Send Changes** and **Activate**.

Step 2. Configure an AV Engine

Select and configure a Virus Scanner engine. You can use Avira and ClamAV either separately or together. Barracuda NG Firewall F100 and F101 can only use the Avira virus scanning engine.

Using both AV 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**.

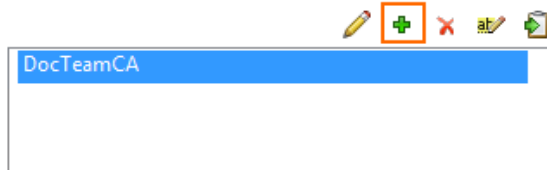
Step 3. Enable SSL Interception and AV Scanning in the Firewall

If you want to scan files that are transmitted over a SSL-encrypted connection, enable SSL Interception and virus scanning in the firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Select the **Enable SSL Interception** check box.
4. Upload your root CA certificate or create a self-signed **Root Certificate**.
5. (Optional) Click the plus sign (+) in the **Trusted Root Certificates** section to add additional root certificates.

Enable SSL Interception
Root Certificate
 Use self signed certificate

 Self Signed Certificate  Hash: ANDYPH 2048 Bits

 Self Signed Private Key  Hash: ANDYPH 2048 Bits
Trusted Root Certificates


DocTeamCA

[Show CA Certificates ...](#)
 Enable CRL Checks

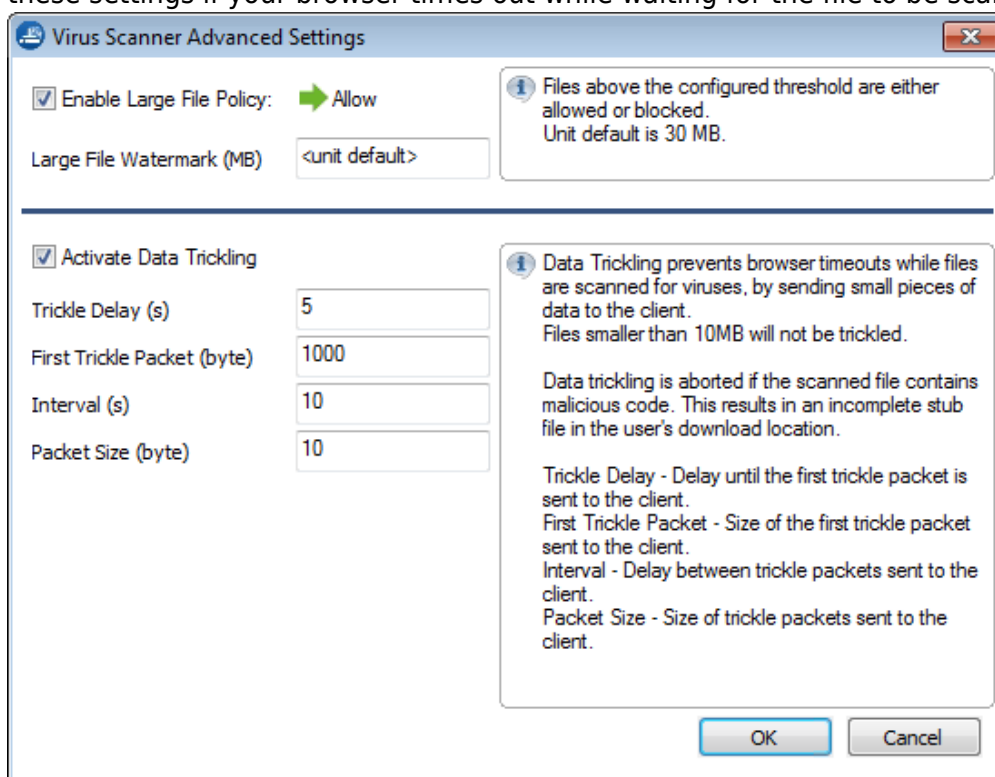
- In the **Virus Scanner Configuration** section, select the **Enable Virus Scanning in the firewall** check box.
- In the **Scanned MIME types** list, add the MIME types of the files that you want the AV scanner to scan.

The default <factory-default-mime-types> includes the most important MIME file types.

application/msword
application/msonenote
application/vnd.openxmlformats-officedocument.wordprocessingml.document
application/vnd.openxmlformats-officedocument.wordprocessingml.template
application/vnd.ms-word.document.macroEnabled.12
application/vnd.ms-word.template.macroEnabled.12
application/vnd.ms-excel
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
application/vnd.openxmlformats-officedocument.spreadsheetml.template
application/vnd.ms-excel.sheet.macroEnabled.12
application/vnd.ms-excel.template.macroEnabled.12
application/vnd.ms-excel.addin.macroEnabled.12
application/vnd.ms-excel.sheet.binary.macroEnabled.12
application/vnd.ms-powerpoint
application/vnd.openxmlformats-officedocument.presentationml.presentation
application/vnd.openxmlformats-officedocument.presentationml.template
application/vnd.openxmlformats-officedocument.presentationml.slideshow
application/vnd.ms-powerpoint.addin.macroEnabled.12
application/vnd.ms-powerpoint.presentation.macroEnabled.12
application/vnd.ms-powerpoint.slideshow.macroEnabled.12

application/pdf
application/x-pdf
application/vnd.pdf
application/vnd.android.package-archive

8. (optional) Change the **Action if Virus Scanner is unavailable**.
9. (optional) Click on **Advanced**:
 - **Large File Policy** - The large file policy is set to a sensible value for your appliance. The maximum value is 4096MB.
 - **Data Tricking 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.



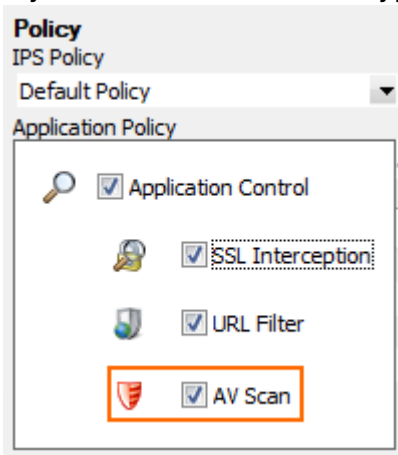
10. Click **Send Changes** and **Activate**.

Step 4. Enable the AV Scanner in the Firewall Rules

You can enable AV scanning for every Pass firewall rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Open the settings for the firewall rule that you want to enable AV scanning for.
4. Click the **Application Policy** link.
5. Select the **Application Control** and **AV Scan** check boxes.

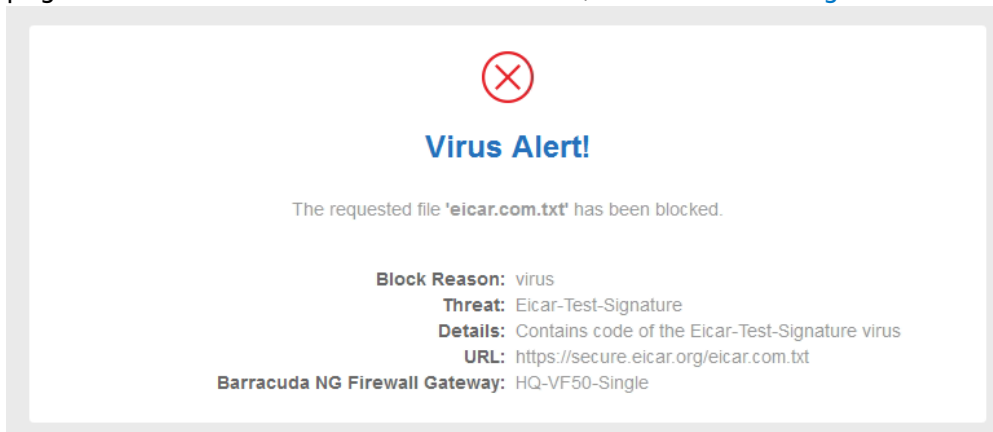
- If you want to scan SSL encrypted traffic, select the **SSL Interception** check box.



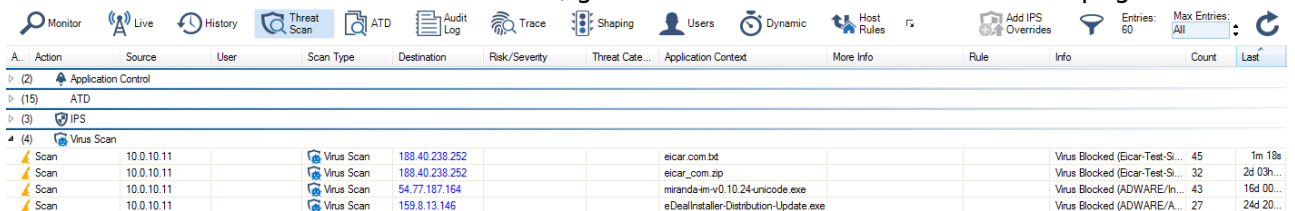
- Click **OK**.
- Click **Send Changes** and **Activate**.

Monitoring and Testing

- Test the AV scan 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](#).



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



A.	Action	Source	User	Scan Type	Destination	Risk/Severity	Threat Cate...	Application Context	More Info	Rule	Info	Count	Last
(2)	Application Control												
(15)	ATD												
(3)	IPS												
(4)	Virus Scan												
	Scan	10.0.10.11		Virus Scan	188.40.238.252			eicar.com.bt			Virus Blocked (Ecar-Test-Si...	45	1m 18s
	Scan	10.0.10.11		Virus Scan	188.40.238.252			eicar_com.zip			Virus Blocked (Ecar-Test-Si...	32	2d 03h...
	Scan	10.0.10.11		Virus Scan	54.77.187.164			miranda-tm-v0.10.24-unicode.exe			Virus Blocked (ADWARE/In...	43	16d 00...
	Scan	10.0.10.11		Virus Scan	159.8.13.146			eDealInstaller-Distribution-Update.exe			Virus Blocked (ADWARE/A...	27	24d 20...

Next Steps

To combine ATD with virus scanning, see [Advanced Threat Detection \(ATD\)](#).

Figures

1. AppControl_SSL_AVScanning.png
2. avScanning03.png
3. FW_virus_scanning_advanced.png
4. avScanning04.png
5. virus_scanning_block_page_eicar.png
6. avScanning02.png

© Barracuda Networks Inc., 2019 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.