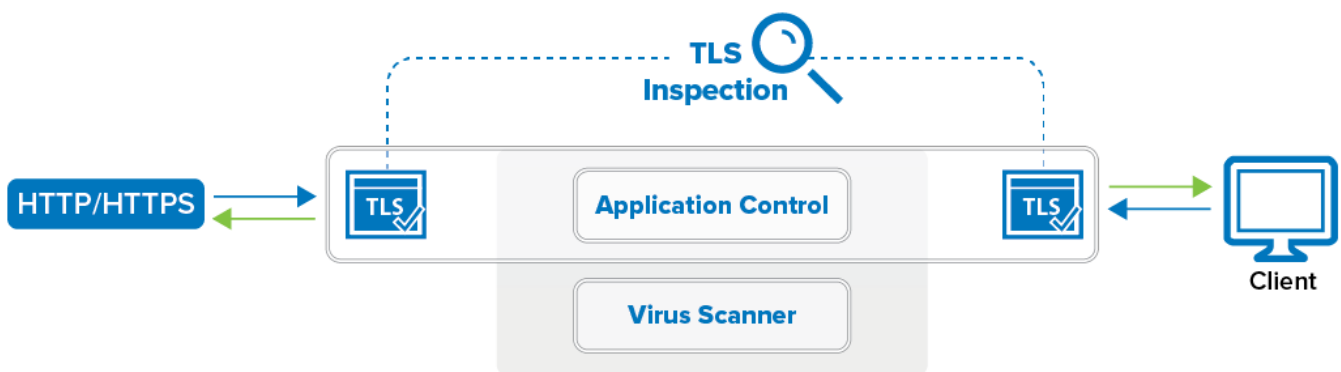


How to Configure Virus Scanning in the Firewall for Web Traffic

<https://campus.barracuda.com/doc/96026315/>

The CloudGen Firewall scans web traffic for malware on a per-access-rule basis when Virus Scanning in the Firewall is enabled. When a user downloads a file, the firewall intercepts and scans the file if it is smaller than the limit set in the large file policy and if the MIME type is listed in the **Scanned MIME types** list. Files matching a MIME type exception are not scanned. To avoid browser timeouts while downloading the file, a very small amount of data is trickled into the browser to keep the connection open. Data trickling ceases while the file is scanned by the virus scanner. If the large file watermark is set to a very high value, browser sessions might time out. In this case, decrease the large file policy value. If the virus scanning services detect malware, the infected file is discarded, and the user is redirected to a customizable block page. The very small partial download from data trickling might still be present on the client. You can combine virus scanning with TLS Inspection to also scan HTTPS connections.



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](#).

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 CloudGen Firewall F100 and F101 can use only the Avira virus scanning engine.

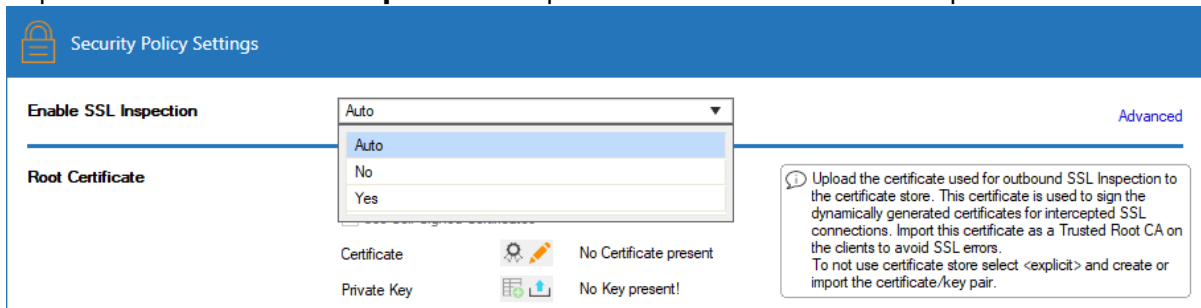
Using both AV engines significantly increases CPU utilization and load.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 TLS Inspection and Virus Scanning in the Firewall

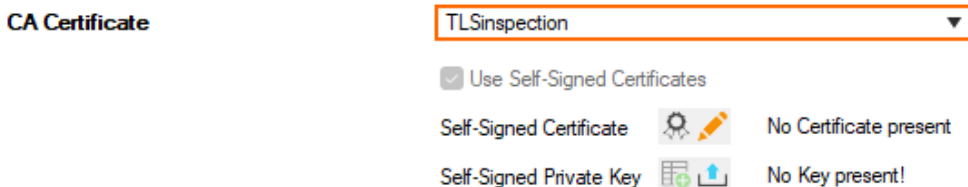
If you want to scan files that are transmitted over a TLS-encrypted connection, enable TLS Inspection and Virus Scanning in the Firewall service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Expand the **Enable TLS Inspection** drop-down list and enable TLS Inspection.

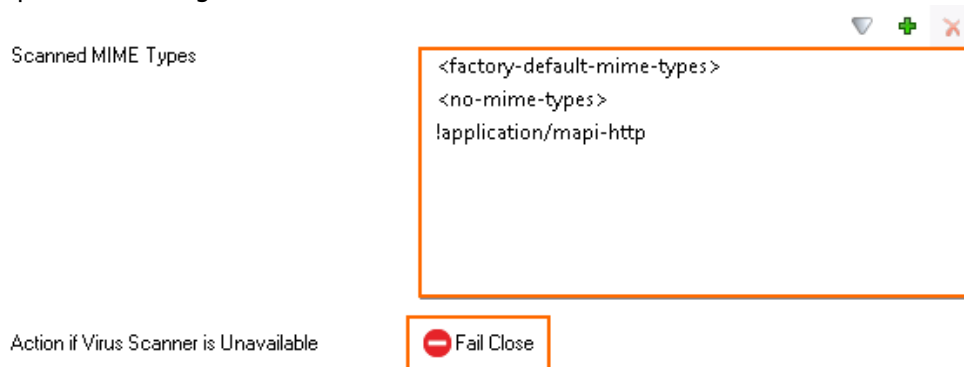


When set to **Auto**, the CloudGen Firewall will check for certificates and automatically enable TLS Inspection as soon as a valid license is detected.

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.
6. In the **Virus Scanner Configuration** section, expand the drop-down list next to **Enable Virus Scanning for**, and select **Yes** for **HTTP**.
7. In the **Scanned MIME types** list, add the MIME types of the files you want to scan. Default: <factory-default-mime-types> and <no-mime-types>. For more information, see [Virus Scanning and ATP in the Firewall](#).
8. (optional) In the **Scanned MIME types** list, add MIME type exceptions. Prepend an "!" to not scan this MIME type. E.g., !application/mapi-http

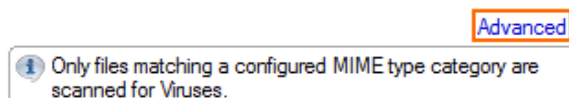
9. (optional) Change the **Action if Virus Scanner is unavailable**.

Scanned MIME Types

<factory-default-mime-types>
<no-mime-types>
!application/mapi-http

Action if Virus Scanner is Unavailable

Fail Close

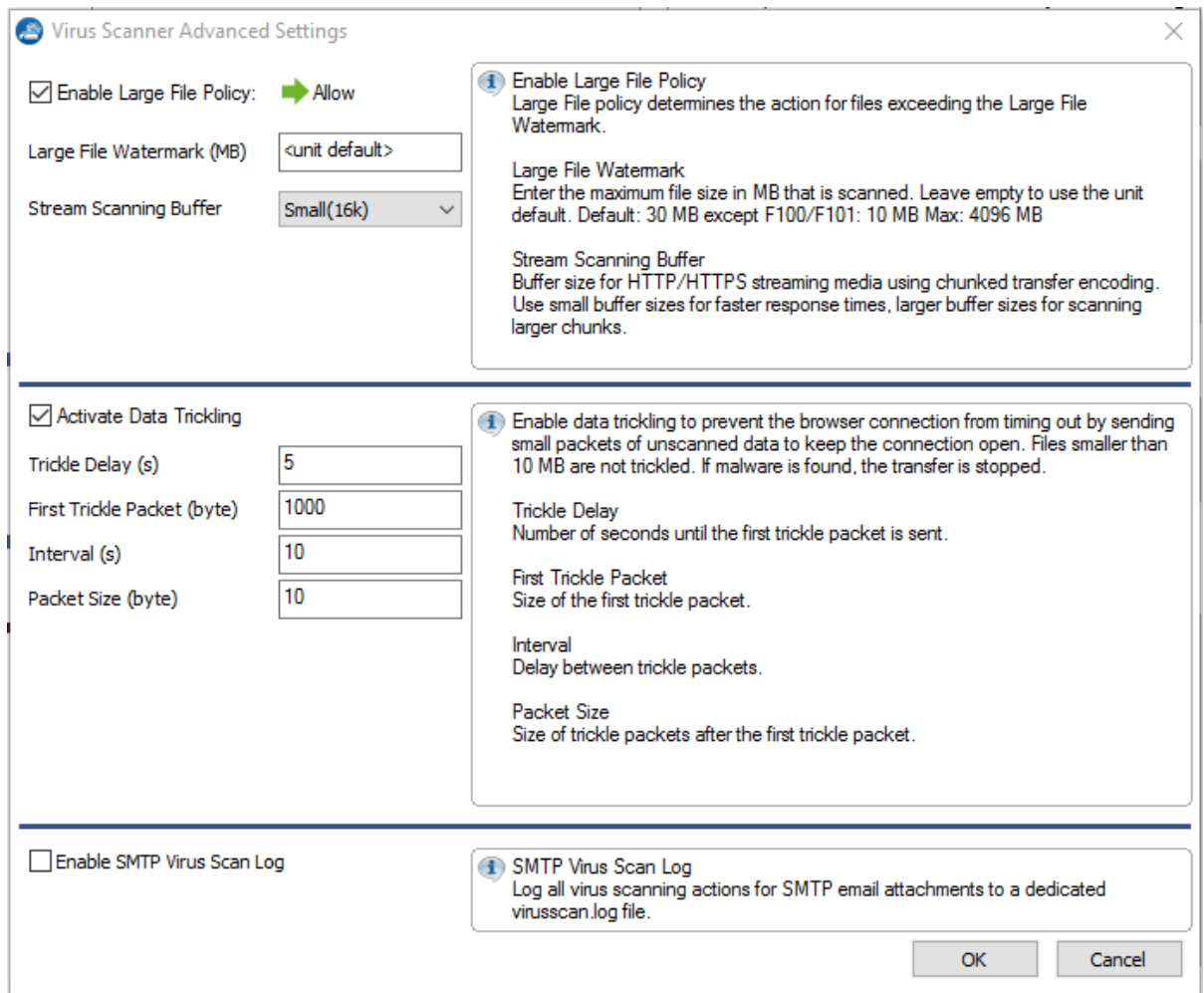
10. (optional) Click **Advanced**:

Advanced

Only files matching a configured MIME type category are scanned for Viruses.

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

- **Large File Policy** – Action taken if the file exceeds the size set as the **Large File Watermark**. Select **Allow** to forward the files unscanned; select **Block** to discard files that are too big to be scanned.
- **Large File Watermark (MB)** – The large file watermark is set to a sensible value for your appliance. The maximum value is 4096 MB.
- **Stream Scanning Buffer** – Select the buffer size for HTTP/HTTPS streaming media using chunked transfer encoding. Select **Small** for faster response times, or **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.



Virus Scanner Advanced Settings

☒ Enable Large File Policy: ➔ Allow

Large File Watermark (MB)

Stream Scanning Buffer

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.

☒ Activate Data Tricking

Trickle Delay (s)

First Trickle Packet (byte)

Interval (s)

Packet Size (byte)

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.

☐ Enable SMTP Virus Scan Log

SMTP Virus Scan Log
Log all virus scanning actions for SMTP email attachments to a dedicated virusscan.log file.

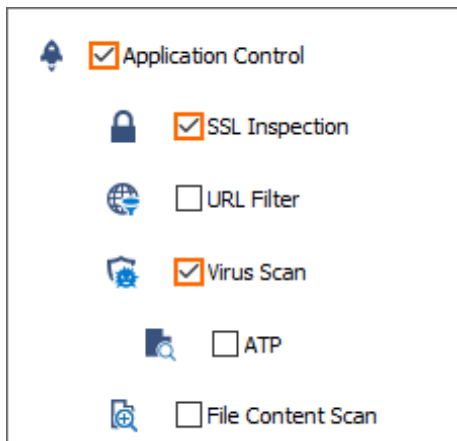
OK Cancel

11. Click **Send Changes** and **Activate**.

Step 3. Edit an Access Rule to Enable Virus Scanning

Virus scanning can be enabled for all Pass and Dst NAT access rules.

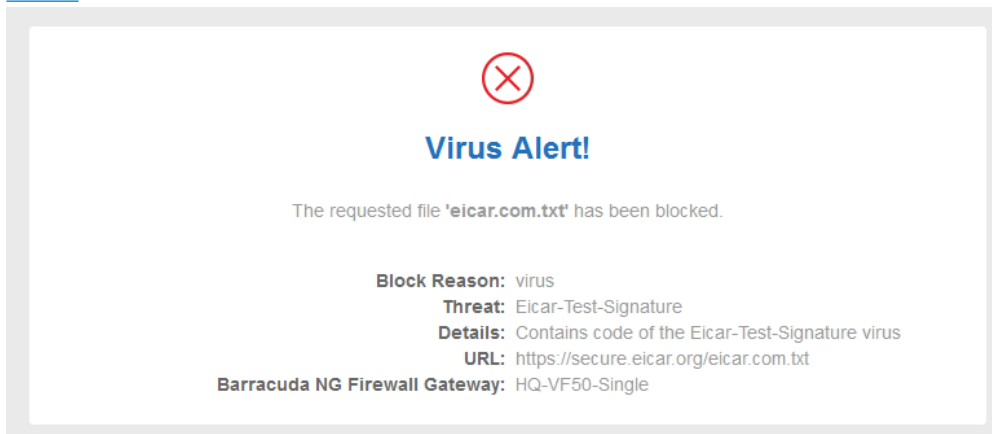
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Double-click to edit the **PASS** or **Dst NAT** access rule.
4. Click the **Application Policy** link and select:
 - **Application Control** – required.
 - **TLS Inspection** – optional.
 - **Virus Scan** – required.



5. If configured, select a policy from the **TLS Inspection Policy** drop-down list. For more information, see [TLS Inspection in the Firewall](#).
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Monitoring and Testing

- Each file blocked by the virus scanner generates a **5005 Virus Scan file blocked** event.
- Test the virus 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 and Texts](#).



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

<div>MonitorLiveHistoryThreat ScanAudit LogShapingUsersDynamicHost RulesForwarding RulesAdd IPS OverridesEntries: 60Max Entries: All</div>													
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 (Eicar-Test-S...		45	1m 18s
⚡	Scan	10.0.10.11		Virus Scan	188.40.238.252			eicar.com.zip		Virus Blocked (Eicar-Test-S...		32	2d 03h...
⚡	Scan	10.0.10.11		Virus Scan	54.77.187.164			miranda-im-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 ATP with virus scanning, see [Advanced Threat Protection \(ATP\)](#).

Figures

1. virus_scanning_https_traffic_tls.png
2. ssl_auto.png
3. outbound_TLS_inspection_02.png
4. AV_SMTP_09.png
5. AV_SMTP_02.png
6. FW_virus_scanning_advanced.png
7. AV_HTTP_01.png
8. virus_scanning_block_page_eicar.png
9. avScanning02.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.