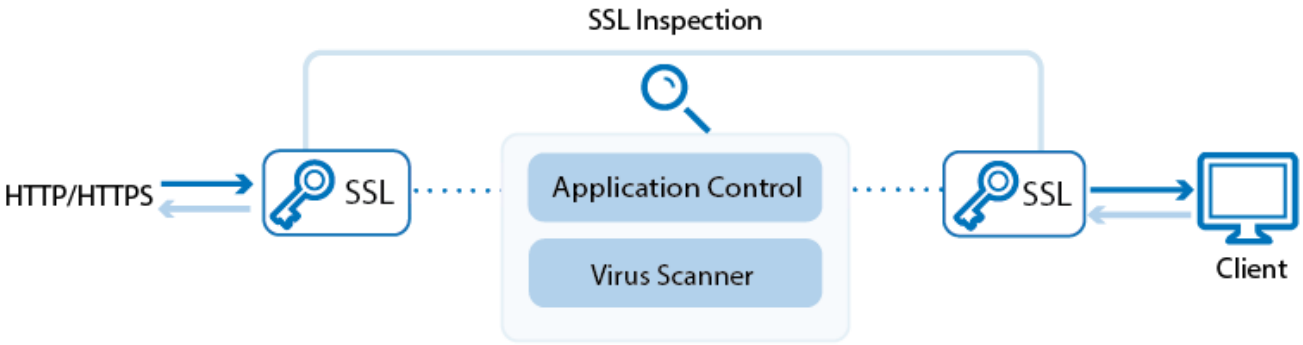
How to Configure Virus Scanning in the Firewall for Web Traffic

https://campus.barracuda.com/doc/79463046/

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 to 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 detects 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 SSL Inspection to also scan HTTPS connections.



Before You Begin

- The **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher.
- Enable Application Control. For more information, see How to Enable Application Control.
- Create a Virus Scanner service. For more information, see Virus Scanner.
- (optional) Enable SSL Inspection. For more information, see SSL Inspection in the Firewall.

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.

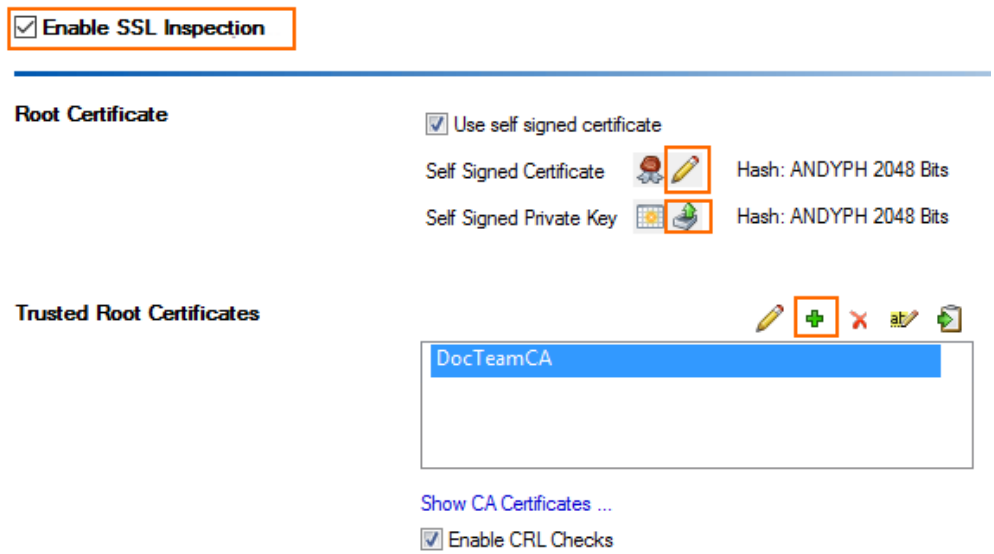
> Using both AV engines significantly increases CPU utilization and load.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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**.

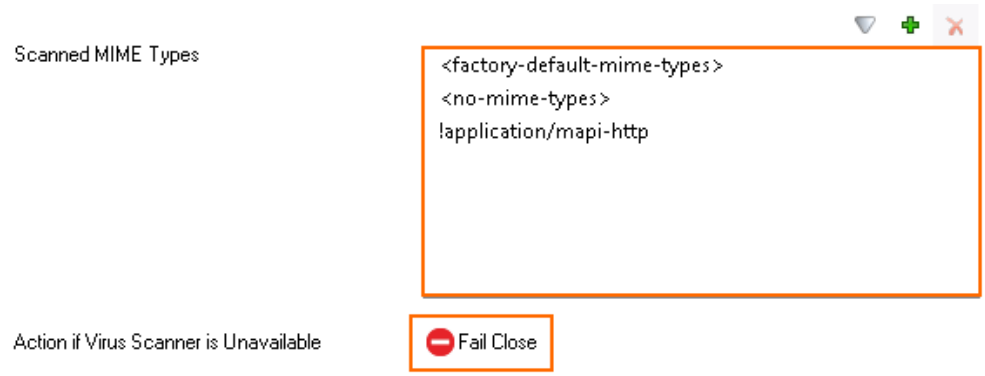
Step 2. Enable SSL Inspection and Virus Scanning in the Firewall

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

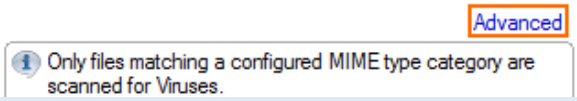
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Select the **Enable SSL Inspection** check box.
4. Upload your root CA certificate, or create a self-signed **Root Certificate**.
5.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



6. In the **Virus Scanner Configuration** section, select **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 a "!" to not scan this MIME type. E.g., !application/mapi-http
9. (optional) Change the **Action if Virus Scanner is unavailable**.

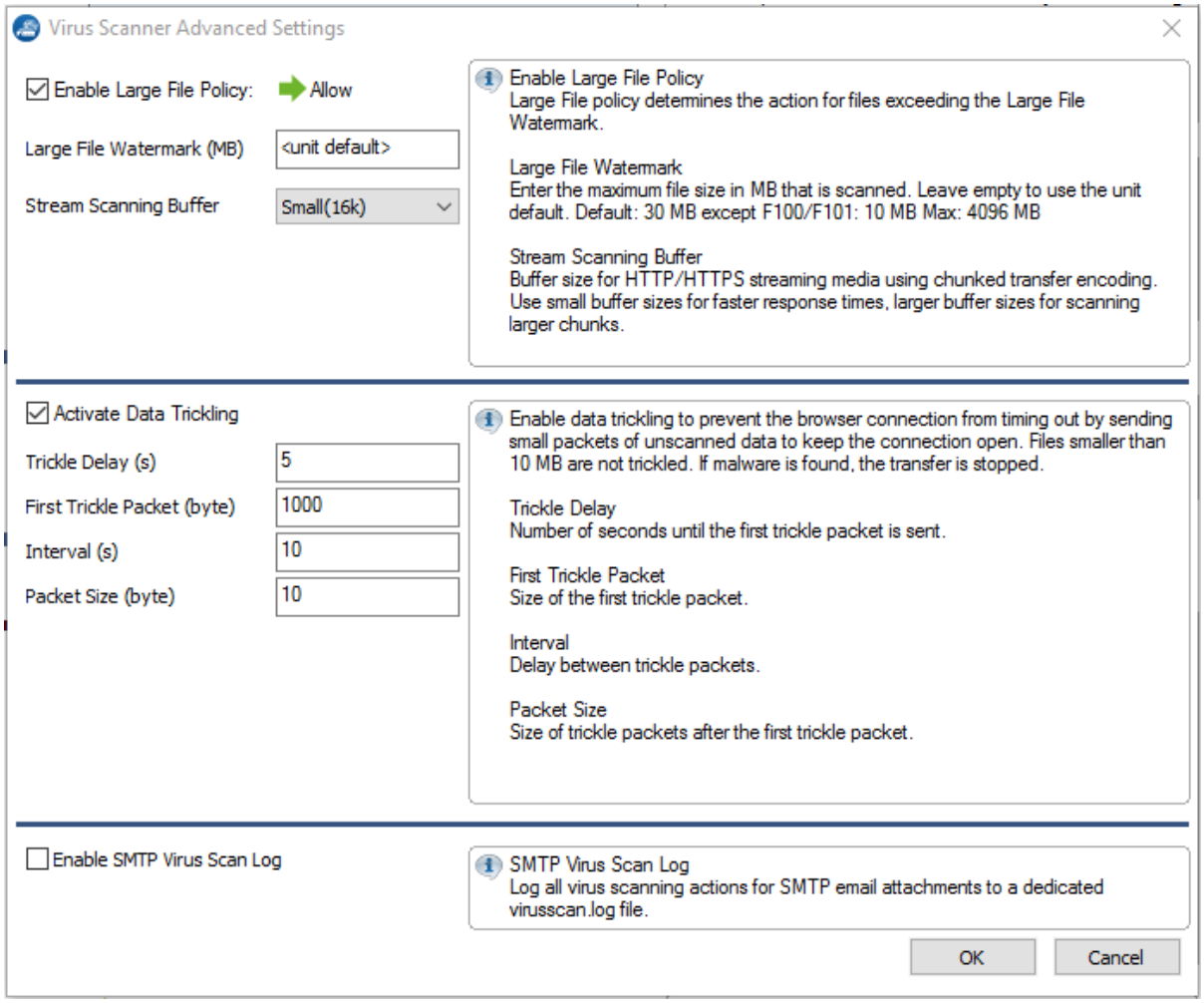


10. (optional) Click **Advanced**:



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.

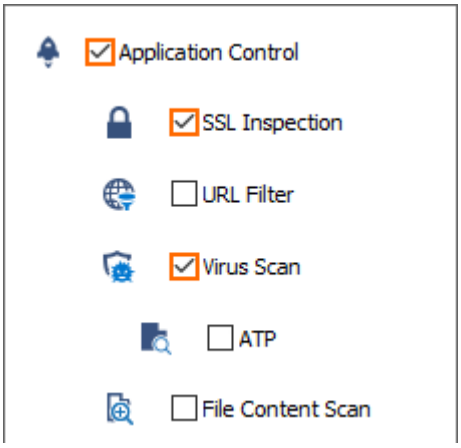


11. Click **Send Changes** and **Activate**.

Step 3. Edit an Access Rule to Enable Virus Scanning

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

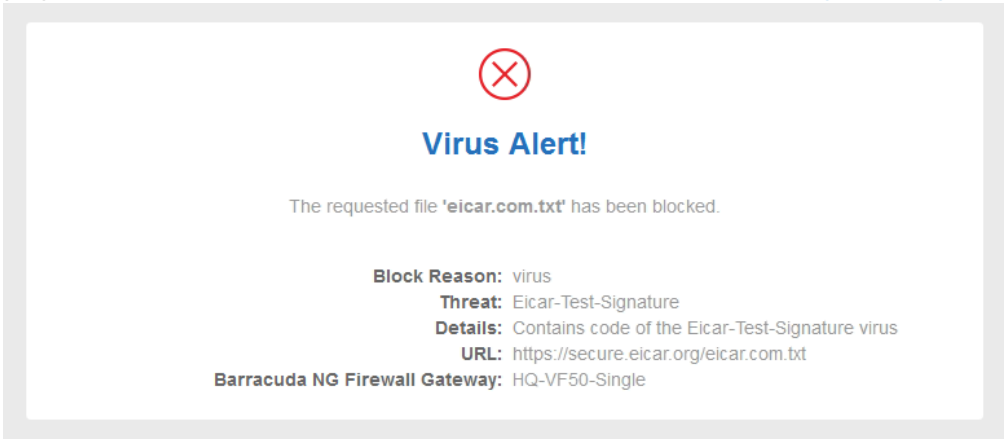
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Double-click to edit the **PASS** or **Dst NAT** access rule.
4. Click **Application Policy** link and select:
   - **Application Control**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



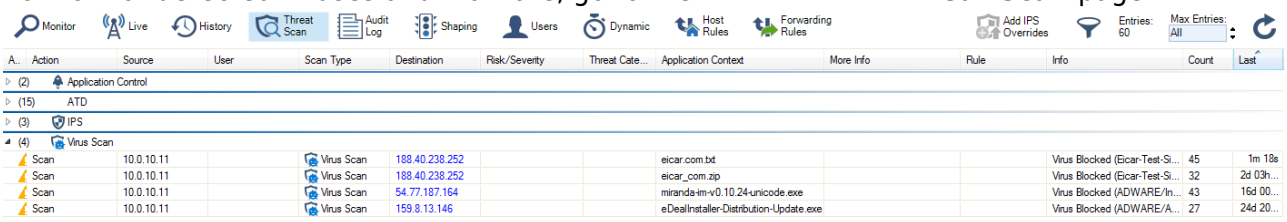
5. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see SSL Inspection in the Firewall.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

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 Response Messages.



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



Next Steps

To combine ATP with virus scanning, see Advanced Threat Protection (ATP).

Figures

1. 61_virus_scanning_https_traffic.png
2. avScanning03.png
3. AV_SMTP_09.png
4. AV_SMTP_02.png
5. FW_virus_scanning_advanced.png
6. AV_HTTP_01.png
7. virus_scanning_block_page_eicar.png
8. avScanning02.png