How to Configure Virus Scanning in the Firewall for SMB

https://campus.barracuda.com/doc/86540691/

Virus scanning covers V2 and V3 for SMB. While a scan is running, data transfer on the session is stopped completely. If malware is found, the whole TCP session is terminated. Content Detection is performed on all files.

SMB file scanning significantly increases CPU utilization and puts a heavy load on your firewall. Use this feature only in exceptional cases!

Step 1. Configure the Virus Scanner Engine(s)

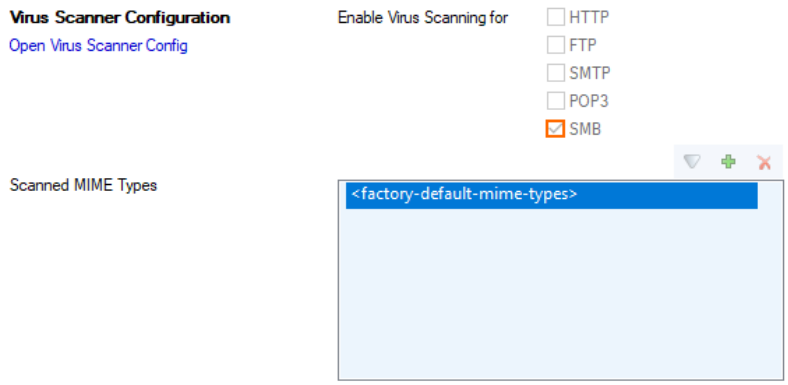
Select and configure a virus scanner engine. You can use Avira and ClamAV either separately or together. Barracuda CloudGen Firewall F100 and F101 can use only the Avira virus scanning engine.

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 the Virus Scanner to Scan SMB Related Traffic

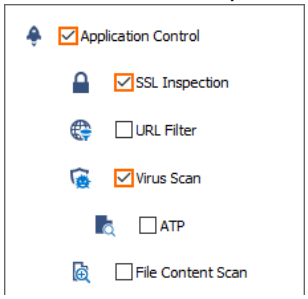
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Scroll down to the section **Virus Scanner Configuration**.
4. Select the check box for **SMB**.
5. Click **Send Changes**.
6. Click **Activate**.



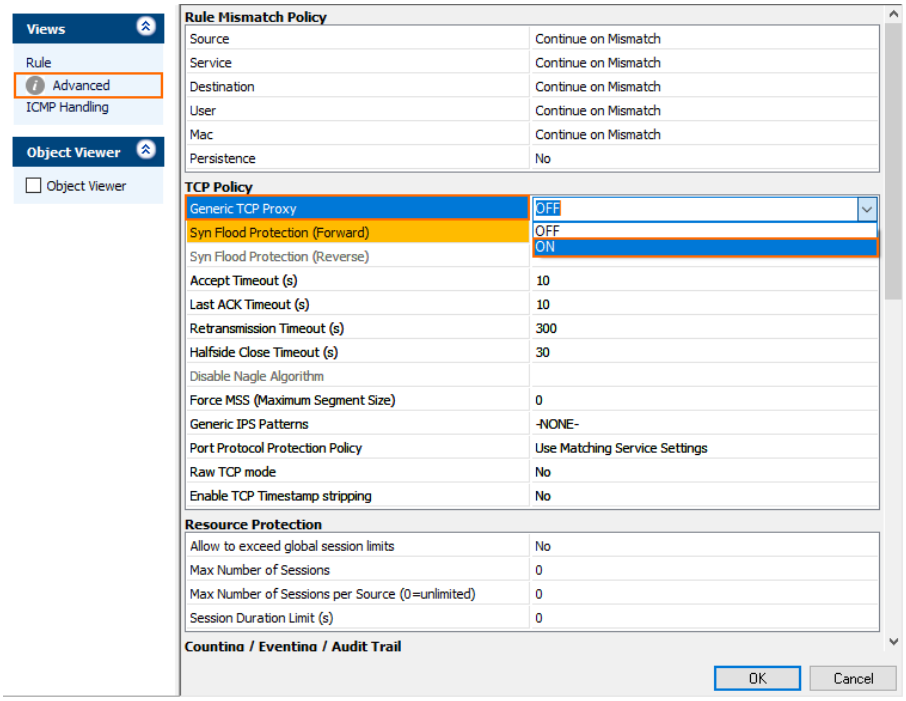
Step 3. Edit an Access Rule to Enable Virus Scanning for Session-Related SMB Traffic

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 **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. In the left menu inside of the **Edit Rule** window, click **Advanced**.
7. Navigate to the first entry **Generic TCP Proxy** in the **TCP Policy section**.
8. For the **Generic TCP Proxy** entry, click in the second column and select **ON**.



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

Figures

1. enable_virus_scanning_for_smb.png
2. allow_app_control.png
3. configure_access_rule.png