URL Filtering with Endpoint Security
R77.30.02 and higher

Administration Guide
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point R77.30.02 and higher
For more about this release, see the Endpoint Security home page http://supportcontent.checkpoint.com/solutions?id=sk112793.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=51688.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on URL Filtering with Endpoint Security R77.30.02 and higher Administration Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08 September 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
URL Filtering with Endpoint Security

In This Section:

- URL Filtering ...................................................................................................................4
- Supported Features for Endpoint Security URL Filtering ............................................4
- Installing URL Filtering ..................................................................................................5
- Configuring URL Filtering Policy Rules .........................................................................5

URL Filtering

Check Point URL Filtering can work together with Endpoint Security to bring URL Filtering capabilities and policies to endpoint computers.

Supported Features for Endpoint Security URL Filtering


These features are NOT supported for Endpoint Security:

- Application Control.
- Limits and Limit objects.
- Hit Count and Hits.
- Identity Awareness Captive Portal and use of Networks inside an Access Role (a Network in an Access Role is ignored by Endpoint Security).
- Option to Block all requests when the web service is unavailable (requests will be allowed in case of web service failure).
- URL Filtering features that were new for R76 and higher: Categorize HTTPS sites, Enforce safe search in search engines, Categorize cached pages and translated pages in search engines, IPv6.
- HTTPS Inspection and HTTPS Inspection on Non-Standard Ports settings in SmartDashboard (Endpoint Security always inspects HTTPS traffic, regardless of settings in SmartDashboard).
- The Application Control and URL Filtering tab Overview and Gateways pages do not show Endpoint Security events.
- UserCheck Interaction Options: Redirect to External Portal.
- User defined alerts for tracking (regular, extended and complete logs are supported).
- Customizing the UserCheck portal as described in sk83700 http://supportcontent.checkpoint.com/solutions?id=sk83700 (multiple languages supported).
This behavior is different in URL Filtering for Endpoint Security than what is described in the *R77 Application Control and URL Filtering Administration Guide*:

- When URL Filtering is installed on an Endpoint Security client, all Endpoint Security UserCheck messages show automatically and do not require separate installation of the UserCheck client. This includes messages in the Endpoint Security client and web browser.
- For UserCheck notifications that are not in a web browser: After a message shows for a domain, it is suppressed and will only show again at two hour intervals.
  For UserCheck notifications in a web browser: Messages show each time they apply.

**Installing URL Filtering**


**Configuring URL Filtering Policy Rules**

Endpoint Security URL Filtering uses the URL Filtering policy from SmartDashboard. Configure the policy in SmartDashboard and install it on the Endpoint Management object. The policy will be installed automatically on the Endpoint Security clients also. To configure the URL Filtering policy, see the *R77 Application Control and URL Filtering Administration Guide* [http://downloads.checkpoint.com/dc/download.htm?ID=24853](http://downloads.checkpoint.com/dc/download.htm?ID=24853).

**Important** - Install the URL Filtering policy from the SmartDashboard on the Network Security Management Server only. When the Network Security Management Server and the Endpoint Security Management Server are on different computers, if you install the URL Filtering policy from SmartDashboard on the Endpoint Security Management Server, unexpected issues can occur.

**Note** - If an Access Role contains objects that were not scanned by the Endpoint Security Active Directory Scanner, rules are not enforced on the unscanned users and computers.

In SmartEndpoint, you can:

- See information about the policy configured in SmartDashboard
- Configure trusted processes that are not inspected by URL Filtering
- Configure the sources of UserCheck messages in cases when the user is blocked.
- Disable the policy (causes the Endpoint Security not to enforce URL Filtering)
- Disable SSL connection inspection (configure in GuiDBedit)
SmartDashboard Policy Information

In the Management Information action of the URL Filtering Policy, you can see information about the policy configured in SmartDashboard. Click the action and select More Details to see:

- The name and IP address of the server that the URL Filtering SmartDashboard policy was installed from.
- The time the policy was installed and the policy name

If the policy from the SmartDashboard is not installed, the message shows: Waiting for Policy Installation.

Configuring Trusted Processes

To configure Trusted Processes that will not be inspected by URL Filtering:

1. In the URL Filtering rule, open the Trusted Processes Action configuration window.
2. Select an action or create a new action.
3. For each trusted process, click Add.
4. Enter the new trusted process parameters:
   - Process name (mandatory) - full or relative path
   - MD5 checksum
   - Original process name
5. Click OK.
6. Click OK to save all trusted processes.

Configuring the Source of UserCheck Messages

You can configure where users will receive UserCheck messages from:

- Receive UserCheck messages from both Endpoint and Gateway - Endpoint Security and the gateway both show UserCheck messages
- Suppress UserCheck message from Endpoint when receiving from Gateway - Endpoint Security does not show a UserCheck message if a trusted gateway shows the UserCheck message. To use this option, you must configure one or more Trusted Gateways.

To configure the source of UserCheck messages:

1. In the URL Filtering rule, open the URL Activity Protection Action configuration window.
2. Select an action or create a new action.
3. Configure trusted gateways if you want to suppress UserCheck messages from Endpoint Security when receiving from the gateway:
   a) Click Add.
   b) In the window that opens, enter the Gateway Name, Gateway IP address, and the Fingerprint.
      Note - See the procedure below to get the Fingerprint of a trusted gateway.
   c) Click OK.
4. Click OK.
To get the Fingerprint of a trusted gateway:

1. In SmartDashboard of the Network Security Management Server, where the trusted gateway is defined, double-click the gateway object to open the gateway Properties window.
2. Go to the UserCheck tab.
3. If the portal does not use an auto-generated certificate, and a Fingerprint is shown in the Certificate section, see sk103255 http://supportcontent.checkpoint.com/solutions?id=sk103255. Do not continue with this procedure.
4. If the portal uses auto-generated certificate, go to the IPSec VPN tab. IPSec VPN must be selected in the General Properties tab.
5. In the Repository of Certificates Available to the Gateway, click View for the relevant certificate.
6. Scroll to the bottom of the Certificate View table. The last row in the table shows the fingerprint of the gateway.

This is an example of a valid fingerprint: SANG KANE TAR COP GREW HALF BUN WALL BASK HERD GEAR BETA

Disabling the Policy

If you disable the policy, Endpoint Security does not enforce URL Filtering.

To disable the URL Filtering Policy:
Right-click the URL activity Protection action and select Disable Policy.

Disabling SSL Connection Inspection

To disable SSL connection inspection:

1. In GuiDBedit, go to Other > ep_orgp_urlf_policy_tbl > Do not inspect trusted processes by Endpoint URL Filtering.
2. Change the value of turn_off_ssl to true.
3. Save the database and close the GuiDBedit.
4. Install policy from the SmartEndpoint.