Configuring Centralized Web Filtering for Embedded NGX Gateways in SmartCenter

This document describes how to configure Centralized Web Filtering for Check Point Embedded NGX gateways using Check Point SmartCenter R60 and above, with or without the Check Point SmartLSM extension.

Note: Embedded NGX gateways include both Check Point VPN-1 Edge and Nokia IP40 gateways. The Embedded NGX screens that appear in this document relate to VPN-1 Edge gateways.

Note: This document assumes the reader is familiar with the basic concepts of working with SmartCenter.

Introduction to SmartCenter Centralized Web Filtering Service

The SmartCenter Centralized Web Filtering service enables organizations to restrict and monitor access to the World Wide Web. Internet access has become a necessary tool in most organizations for a variety of purposes, such as education, business transactions, and distribution of information. However, most of the information on the Internet is not relevant to these purposes, hence creating the need to control when and where users access the Internet.

Controlling Internet usage helps to:

- **Increase productivity.** Personal Web surfing has become a significant cause of employee productivity loss. By limiting employee access to sites belonging to undesirable categories, you can prevent this problem.

- **Avoid legal liability.** Employees can easily access inappropriate content, such as pornography, copyrighted documents/software/music files, and hate material, through the Web. Such material is bound to legal liabilities for which organizations are held accountable.

- **Hold on to your business values.** Some organizations are built around strong core values. These organizations have an interest in preventing any activity that may undermine those values.

In most cases, an organization can enforce its Web Filtering policy by publishing a set of rules for employees; however enforcing such written rules is not an easy task. In addition, a small business organization usually does not have sufficient resources to invest in an enforcement solution and to keep the enforcement point database updated at all times. A managed Web Filtering service represents a complete solution to these problems.
How Does Centralized Web Filtering Work?

Centralized Web Filtering works as follows:

1. The service provider installs third-party OPSEC Web Filtering software on a machine, as part of SmartCenter deployment.

2. The service provider configures Centralized Web Filtering on SmartCenter.
   For information on configuring Centralized Web Filtering, see “Overview of Centralized Web Filtering Configuration,” page 3.
   Configuring Centralized Web Filtering on SmartCenter includes specifying which UFP server to use. For information on choosing UFP software, see “Prerequisites,” page 3.

3. An Embedded NGX security gateway connects to SmartCenter over an Internet connection and is updated with the Centralized Web Filtering service options.

4. A client behind the gateway generates an HTTP request.
   a. The gateway extracts the requested URL and sends the URL information to the SofaWare Management Server (SMS).
      The SMS is a server located on the SmartCenter machine. It provides each gateway with a security policy, a user interface, configuration updates, and value-added services.
      Note: Only the "host" part of the URL is sent in the UFP server; the "path" part of the URL is ignored.
   b. The SMS queries the UFP server.
   c. The SMS sends the response to the gateway.

5. If access to the site is denied, the gateway generates its own HTTP response, which informs the user that access has been denied and allows them to enter a password in order to override the URL filtering mode.
   Note: URL filtering works for HTTP requests only. HTTPS requests are not supported.
Prerequisites

In order to provide Centralized Web Filtering services to managed gateways, you must install third-party OPSEC (Open Security) UFP (URL Filtering Protocol) software and integrate it with the SmartCenter infrastructure. OPSEC UFP is an OPSEC API that enables integration of third-party applications to categorize, and control access to, specific URL addresses. The UFP API has been adopted by a wide variety of content security vendors. More information about OPSEC can be found at http://www.opsec.com.

Currently, the third-party OPSEC UFP software available to integrate with SmartCenter is:

- SurfControl Web Filter for Check Point Firewall-1 by SurfControl (version 2.x or 5.x).
  

- Websense Enterprise by Websense.
  
  You can download the software from the vendor's Web site at: http://www.websense.com. Downloading the software may require registration.

When using SurfControl version 2.x, access to Web content is restricted according to URL categories. You can control and enforce URL filtering categories for all gateways from SmartCenter. When using SurfControl 5.x (and subsequent versions) or Websense, each URL is checked against a database of URLs that should be blocked.

Note: All software is bound by third-party vendor license agreements. The third-party vendor software is also responsible for the accuracy and relevance of the URL filtering database.

Overview of Centralized Web Filtering Configuration

To configure Centralized Web Filtering

1. Prepare SmartCenter to support Centralized Web Filtering services by doing the following:
   a. Add the desired UFP server to SmartCenter.
      See “Adding the UFP Server,” page 4.
   b. Configure global Centralized Web Filtering settings.

2. Prepare the gateways for Centralized Web Filtering by doing the following:
   a. Create a gateway object for each gateway for which you want to enable Centralized Web Filtering.
      For information, refer to SmartCenter documentation.
   b. Configure Centralized Web Filtering for each gateway object.
   c. Install the policy on each gateway object.
      For information, refer to SmartCenter documentation.

3. Test the configuration by doing the following:
   a. From a gateway, connect to SmartCenter.
      See “Connecting to SmartCenter from a Gateway,” page 9.
   b. On the gateway, create a Web Filtering override user.
   c. On the gateway, test Centralized Web Filtering for blocked sites.
Preparing SmartCenter to Provide Centralized Web Filtering Services

Adding the UFP Server

To add the UFP server to SmartCenter

1. In SmartDashboard, in the left pane under Servers and OPSEC Applications, right-click on OPSEC Applications, and select New > OPSEC Application.

The OPSEC Application Properties dialog box appears displaying the General tab.

2. In the Name field, type a name representing the UFP server.
3. In the Server Entities area, select the UFP check box.
4. In the Vendor drop-down list, select the UFP server’s vendor.
5. In the Product drop-down list, select the product type.
6. In the Version drop-down list, select the product version.
7. Create a new host object for the UFP server, by doing the following:
   a. Click New.

   The Host Node dialog box opens displaying the General tab.

   ![Host Node dialog box](image)

   b. In the Name field, type a name for the UFP server.
   c. In the IP Address field, type the UFP server's IP address.
   d. Click OK.

8. In the Host drop-down list, select the host object you created.
9. Click OK.
Configuring Global Centralized Web Filtering Settings

Note: Centralized Web Filtering settings are configured in SmartCenter. The Embedded NGX gateway administrator cannot change Centralized Web Filtering settings locally, except for temporarily disabling and resuming the service.

Note: When using SmartLSM R60, this procedure enables Centralized Web Filtering for all SmartLSM-managed ROBO gateways. When using SmartCenter R60 and above without the SmartLSM extension, you can enable/disable Centralized Web Filtering for each gateway separately, using the procedure “Configuring Gateway Centralized Web Filtering Settings,” page 8.

To configure global Centralized Web Filtering settings

1. In SmartDashboard, in the Policy menu, choose Global Properties.
   The Global Properties dialog box appears.
2. In the menu, expand VPN, and click the VPN-1 Edge/Embedded tab.
   The VPN-1 Edge/Embedded Gateway tab appears.
3. Select the Centralized web filtering check box.
4. Next to the OPSEC UFP server field, click Edit.
The UFP Configuration Wizard for VPN-1 Edge/Embedded Gateway wizard opens displaying the UFP Server’s general properties dialog box.

5. Click the Existing UFP Server radio button.

6. In the Select drop-down list, select the UFP server you defined in “Adding the UFP Server,” page 4.

7. Click Next.

The UFP category selections dialog box appears.

8. Select the check boxes next to the categories you want to block.

9. Click Next until the end of the wizard, then click Finish.

   The VPN-1 Edge/Embedded tab’s OPSEC UFP server field displays the UFP server you selected.

10. Click OK.

11. In the toolbar, click Save.
Configuring Gateway Centralized Web Filtering Settings

To configure gateway Centralized Web Filtering settings

1. In SmartDashboard, double-click the desired gateway object.
   The VPN-1 Edge/Embedded Gateway dialog box appears displaying the General Properties tab.

2. In the menu, click the Content Filtering tab.
   The Content Filtering tab appears.

3. Select the Use UFP check box.

4. Click OK.
Testing the Configuration
Connecting to SmartCenter from a Gateway

To connect a gateway to SmartCenter

1. Click Services in the main menu, and click the Account tab. The Account page appears.

2. In the Service Account area, click Connect.

   The Services Wizard opens, with the Service Center dialog box displayed.

3. Make sure the Connect to a different Service Center check box is selected.
4. Select **Specified IP** and then in the **Specified IP** field, enter SmartCenter’s IP address, as given to you by your system administrator.

5. Click **Next**.
   - The **Connecting...** screen appears.
   - If the Service Center requires authentication, the **Service Center Login** dialog box appears.

   ![Service Center Login dialog box](image)

   Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider, then click **Next**.

   - The **Connecting...** screen appears.
   - The **Confirmation** dialog box appears with a list of services to which you are subscribed. Make sure that the Dynamic DNS service appears in the list.

   ![Confirmation dialog box](image)
6. Click **Next**.

The **Done** screen appears with a success message.

7. Click **Finish**.

On the **Account** page, the **Web Filtering** service's status is "Connected".
Creating Web Filtering Override Users

A Web Filtering override user is an Embedded NGX user who is authorized to view Web pages without restriction. When access to a site is denied, the Web Filtering override user can enter their user name and password to override the filtering and view the site.

To create a Web Filtering override user

1. Click Users in the main menu, and click the Internal Users tab.
   The Internal Users page appears.

2. Click New User.
   The Account Wizard opens displaying the Set User Details dialog box.

3. Complete the fields as desired.
   Refer to the relevant Embedded NGX user guide for information.

4. Click Next.
The Set User Permissions dialog box appears.

![Set User Permissions dialog box](image1)

The options that appear are dependant on the software and services you are using.

5. Select the **Web Filtering Override** check box.

6. Complete the other fields as desired.

   Refer to the relevant Embedded NGX user guide for information.

7. Click **Finish**.

   The user is saved.

**Testing Centralized Web Filtering for Blocked Sites**

**To test Centralized Web Filtering for a site**

1. Surf to a Web site that belongs to a blocked category.

   For example, if you chose to block gambling-related sites, surf to such a site.

   The **Access Denied** page appears.

![Access Denied page](image2)

2. Enter the username and password of the Web Filtering override user you created.

   The blocked Web site opens.