Understanding SofaWare Management
Portal URL Filtering

*S-box Solutions*

Prepared by

*Rolf Wagner*

Document Date: 3/16/2002

Check Point Software Technologies Inc.
Three Lagoon Drive
Redwood City, CA  94065
Corrections

Your recommendations for additions, modifications and corrections to this document are always welcome. Please send any recommendations or corrections to sofaware@us.checkpoint.com.

Contributors

Amir Goldstein, Zohar Kaufman, Ziv Shenhav, Aron Brand
Introduction

The SofaWare URL Filtering Module (UFM) allows the service provider or enterprise customer to manage the URL Filtering module service. This allows the customer to control access to objectionable web sites. The URL Filtering Protocol (UFP) transparently controls web site access without requiring any configuration on the client side. This document presents the working process of UFP in the SofaWare Management Portal.

The URL Filtering Module (UFM) module can use any OPSEC UFP (URL Filtering Protocol) server. As of 3/15/2002 one OPSEC CVP vendor has been tested with the SofaWare Management Portal (SMP). This vendor is SurfControl - SuperScout for FireWall 1. The UFP API has been adopted by a wide variety of content security vendors. Each customer and end user can select a list of categories that should be blocked. Information on supported URL Filtering software may be found at:

OPSEC UFP

The URL Filtering Module (UFM) module can use any OPSEC UFP (URL Filtering Protocol) server. SofaWare makes use of OPSEC v2 specifications. 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. Each customer and end user can select a list of categories that should be blocked.

SofaWare UFM is used to implement the transparent URL Blocking mechanism. When the end user enters a URL in a browser, the URL is checked against allowed URL’s and either allowed or blocked.

At a high level view the URL Filtering mechanism operates as follows:

Gateway represents a enforcement point such as the S-box with Safe@Home or Safe@Office.
1. The gateway encounters a URL request.
2. The gateway transparently grabs the URL and sends it to the SofaWare Management Server (SMS) for analysis. The SMS sends the URL to the OPSEC UFP-compliant URL Filtering server.
3. The UFP server checks the URL, determines its content and notifies the SMS.
4. The SMS responds back to the S-box and either allows or blocks the URL request. If blocked, the end user will be redirected to a S-box web page that shows that the URL is blocked.

The steps above happen very quickly. The speed of the URL check and response to the end user is similar to a DNS Name query in speed.
SofaWare Management Portal OPSEC UFP Details

The OPSEC UFP provides the API that enables the integration of third-party URL Filtering software with the SofaWare Management Server (SMS). The description below provides a more detailed description. Figure 1 shown below shows an architectural view. Figure 2 below shows an example end user category configuration in the my.firewall interface.

A basic building block of the SofaWare Management Portal is the SofaWare Management Server, UFP Server and CVP server. When building resilient designs, these basic building blocks must be duplicated in order to present highly available “building block units” to the gateways that are being managed. The SofaWare Management Servers communicate with other SofaWare Management Servers that are within the configured “SofaWare Server Group”.

Detailed Process Description

“Gateway” represents a enforcement point such as the S-box with Safe@Home or Safe@Office.

Note: All traffic from S-box to SMS and SMS to URL Filtering Server is UDP.

1. The end user enters a URL in the Internet Browser.
2. The gateway encounters a URL request.
3. The gateway transparently grabs the URL and sends it to the SofaWare Management Server (SMS) for analysis. If you were able to monitor the traffic you would see the S-box send the SMS a URL such as “www.example.com”. If encryption is configured for the management link then all traffic between the S-box and the SofaWare Management Server is encrypted in an IPSEC tunnel.
4. The SofaWare Management Server sends the URL to the OPSEC UFP-compliant URL Process / Filtering server. The URL Filtering Software / process may exist on the SMS server or on a separate server.
5. URL Software analyzes the URL. It performs a category matching against the URL. The UFL software determines what filtering categories the URL matches. See figure 2. As an example the URL “www.example.com” may be categorized by the URL Filtering server as follows. Gambling=yes, Adult/Sexually Explicit=yes, Criminal Skills=no, Hate Speech=no, Violence=yes, Drugs & Alcohol=yes, Unknown Sites = no.
6. The URL filtering software replies back to the SofaWare Management Server with category assignment information.
7. The SofaWare Management Server responds back to the S-box.
8. The S-box takes the category assignments it received from the SofaWare Management Server and analyzes it against the Safe@ local URL filtering settings in my.firewall.
9. As an example; if the URL filtering server gave “www.example.com” a category assignment of Gambling = yes, and the end user selected in my.firewall that Gambling URLs should be blocked ( a “X” mark), then we have a MATCH and the URL request would be blocked. All this happens VERY Quickly. The response time as seen by the end user is very much like a DNS query.
10. If blocked, the end user will be redirected to a S-box web page that shows that the URL is blocked.
11. The end user may enter a by-pass password if they have a correct password.
The URL Filtering Process

Figure 1: System architecture of URL filtering process

Figure 2: my.firewall URL filtering controls
Categories
The my.firewall URL filtering screen in Figure 2 shows a number of categories that are predefined. These categories are configurable from the SofaWare Management Server. The categories are dependent upon the OPSEC URL Filtering Software selected by the client. The selection criteria may be modified on a SMP instance basis.

Modifying URL’s
The administrator may add URL’s to drop or modify the existing URL database. Specific instructions for modifying the URL database are dependent upon the OPSEC URL Filtering Software selected by the client.

Operational Notes
- URL Filtering will operate correctly when a HTTP proxy is used.
- Use of the URL filtering is NOT affected by firewall rules. Firewall rules and URL filtering are two separate and independent functions.
- URL filtering operates when the Safe@ enforcement point establishes a VPN on the behalf of end users.
- Both GET and POST HTTP requests are filtered.
- Override of the Access Denied page is for the current session only. When entering the password in the override page, a browser window will be opened on the end user. The end user will be able to browse with disturbance until the session is closed.
- If URL Filtering is enabled in my.firewall and there is no communication with SofaWare Management Servers, and the customer tries to browse the internet to a site that is not currently in the cache - the customer will be presented with an error page that tells him that URL Filtering Service is down, and that the end user may enter Parental control override mode to continue surfing without problems.

Customer already has UFP Server
Customers may use their existing URL filtering software that they may already have purchased and installed. Several steps will have to be taken to ensure correct URL filtering software integration and contract agreement. The following will have to be reviewed.
1. The customer may have to pay a fee for the SMP UFM integration module.
2. The customer should show their own contract with URL Filtering Software vendor and sign a Waiver with Check Point. The issue with this is that the SMP is seen as one user to the URL filtering software. To the extent necessary Check Point wants to ensure contract compliance to protect Check Point from any legal entanglement.
3. Verify that Check Point and SofaWare has tested the URL Filtering Software that the customer wishes to use.
4. Review the design elements of using the existing URL filtering software servers to ensure best performance.