



Websense Web Security Gateway: Integrating the Content Gateway component with Third Party Data Loss Prevention Applications

November, 2010

Contents

Solution Summary	3
Solution Diagram	3
Introduction	4
How it works:.....	4
Before You Begin	4
Configuring the Websense Content Gateway ICAP Client.....	5
Configuring the ICAP Server	7

Solution Summary

Websense® Web Security Gateway provides real-time content scanning and Web site classification to protect network computers from malicious Web content while controlling employee access to dynamic, user-generated Web 2.0 content.

Web content has evolved from a static information source to a sophisticated platform for 2-way communications, which can be a valuable productivity tool when adequately secured. The dilemma for administrators is how much access to allow. Web 2.0 sites rely primarily on HTTP/HTTPS protocols, which cannot be blocked without halting all Internet traffic. Malicious content can use this means of entry into a company network.

Websense Web Security Gateway contains a high-performance Web proxy – Websense Content Gateway, that supports deep content inspection.

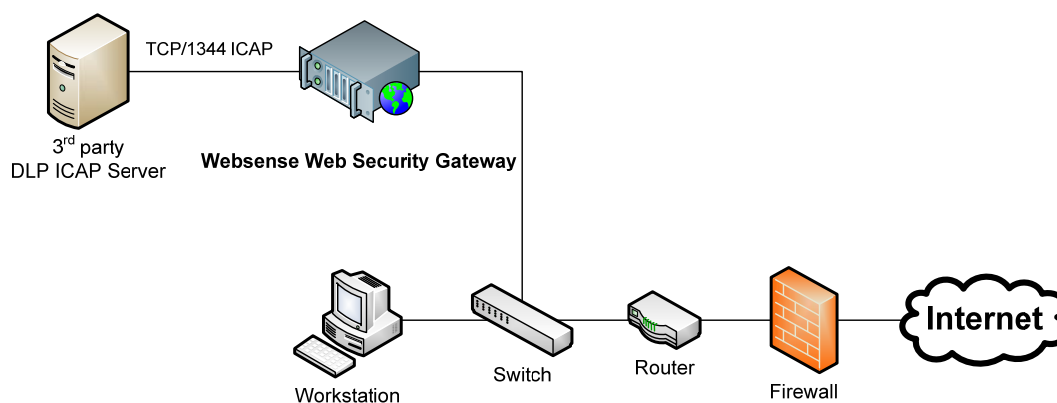
The Websense Content Gateway module offers:

- Automatic categorization of dynamic Web 2.0 sites
- Automatic categorization of new, unclassified sites
- HTTPS content inspection
- Enterprise proxy caching capabilities

Websense Content Gateway supports the ICAP v1 protocol for integration with third party data loss prevention (DLP) applications, such as Symantec Data Loss Prevention (formerly Vontu Data Loss Prevention), and RSA Data Loss Prevention. Data loss prevention applications deliver multi-protocol monitoring and blocking of sensitive data leaving the network. DLP is available in various configurations, one of which utilizes a HTTP/HTTPS/FTP proxy with ICAP client such as the Websense Content Gateway for monitoring and blocking of sensitive data.

This document provides instructions on configuring Websense Content Gateway as an ICAP client for non-Websense DLP products acting as the ICAP server.

Solution Diagram



Introduction

Websense Content Gateway supports integration with Symantec Data Loss Prevention and RSA Data Loss Prevention through the ICAP v1 (Internet Content Adaptation Protocol) interface.

Symantec and RSA sites can apply their DLP tools to the flow of traffic that transits Content Gateway on its way to the Internet. The integration facilitates off-loading of HTTP POST, HTTPS POST (if SSL Manager is enabled), and FTP PUT to a designated DLP server for content analysis and policy enforcement. In this configuration, Content Gateway acts as an ICAP client communicating with the DLP application, which acts as an ICAP server.

How it works:

1. Content Gateway intercepts outbound content and provides that content to the DLP application via ICAP v1.
2. The DLP application determines if the Web posting or FTP upload is allowed or blocked.
 - The determination is based on policy.
 - The disposition is communicated to Content Gateway.
 - The DLP application logs the transaction.
3. Content Gateway acts on the determination.
 - a. If the content is blocked, it is not transmitted to the remote host and the DLP application returns a block page to the sender.*
 - b. If the content is allowed, it is forwarded to its destination.

Transaction details are logged by the DLP application, per its configuration.

**Block page handling*

When a request is blocked and the DLP server sends a block page in response:

- Content Gateway forwards the block page to the sender in a 403 Forbidden message.
- The block page must be larger than 512 bytes or some user agents (e.g., Internet Explorer) will substitute a generic error message.


Before You Begin

This section provides instructions for integrating with the third party DLP application. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

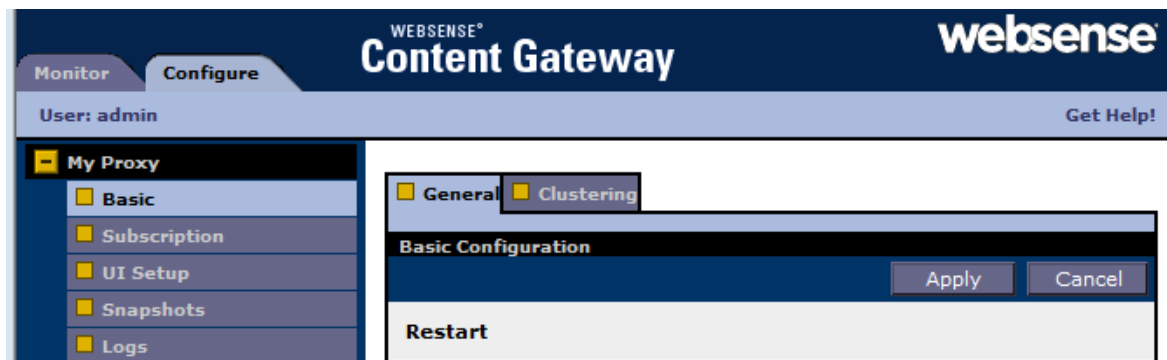
All vendor products and components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Websense Content Gateway ICAP Client

 **Note:** This document assumes that the administrator has deployed and configured Websense Content Gateway to proxy HTTP(S) and/or FTP traffic as outlined in the *Deploying with Websense Content Gateway Guide*. Ensure that all proxy traffic is working properly before beginning any of the procedures listed below.

The Content Gateway ICAP v1 interface supports Websense Data Security Suite, Symantec Data Loss Prevention, RSA Data Loss Prevention, and other applications that act as ICAP servers.

To configure integration with ICAP, log on to **Content Gateway Manager** and go to the **Configure > My Proxy > Basic > General** page.



1. In the **Networking** section of the Features table, select Data Security **On**, and select **ICAP**.

Features		
Feature	On	Off
Protocols		
FTP	<input checked="" type="radio"/>	<input type="radio"/>
HTTPS	<input checked="" type="radio"/>	<input type="radio"/>
Networking		
ARM	<input checked="" type="radio"/>	<input type="radio"/>
WCCP	<input type="radio"/>	<input checked="" type="radio"/>
DNS Proxy	<input type="radio"/>	<input checked="" type="radio"/>
Virtual IP	<input type="radio"/>	<input checked="" type="radio"/>
Data Security	<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/> Integrated on-box		
<input checked="" type="radio"/> ICAP		

2. Click **Apply**, and then click **Restart** (top of page).

3. Navigate to **Configure > Networking > ICAP > General**.



General

ICAP Server Configuration

ICAP Service URI

- Specifies the URI of the Data Security Suite (DSS) Protector appliance. The format is `icap://hostname:port/path`. For example: `icap://ICAP_machine:1344/reqmod`.

Analyze HTTPS Content

☒ Analyze Traffic

- Should content decrypted by SSL manager be sent to DSS for analysis or sent directly to the destination?

☐ Ignore Traffic

Analyze FTP Uploads

☒ Enabled

- Should native FTP proxy uploads be sent to DSS for analysis?

☐ Disabled

Action for Communication Errors

☐ Permit Traffic

- Permit traffic or send a block page if Websense Content Gateway receives an error while communicating with the ICAP service.

☒ Block Traffic

Action for Large files

☒ Permit Traffic

- Permit traffic or send a block page if files larger than the size limit specified in DSS are sent. The default size limit is 12 MB.

☐ Block Traffic

4. In the **ICAP Service URI** field, enter the Uniform Resource Identifier (URI) for the ICAP server.

A URI is similar to a URL, but the URI ends with a directory, rather than a page. Obtain the identifier from your DLP application administrator. Enter the URI in the following format:

`icap://hostname:port/path`

For *hostname*, enter the IP address or hostname of the DLP server.

The default ICAP port is 1344.

Path is the path of the ICAP service on the host machine.

For example:

`icap://ICAP_machine:1344/REQMOD`

You do not need to specify the port if you are using the default ICAP port 1344.

5. Under **Analyze HTTPS Content**, indicate if decrypted traffic should be sent to the DLP server for analysis or sent directly to the destination. You must be running SSL Manager to send HTTPS traffic to the DLP server.
6. Under **Analyze FTP Uploads**, select whether to send FTP upload requests to the DLP server for analysis. The FTP proxy feature must be enabled to send FTP traffic to the DLP server.
7. Under **Action for Communication Errors**, select whether to permit traffic or send a block page if Content Gateway encounters an error while communicating with the DLP server.
8. Under **Action for Large Files**, select whether to permit traffic or send a block page if a file larger than the size limit specified by the DLP server is sent.
9. Click **Apply**.

NOTE: If you change the URI, you must restart Content Gateway. Other changes do not require a restart.

Configuring the ICAP Server

Configure the Symantec or RSA DLP server for ICAP per the vendor's product documentation.