How to configure Cisco Web Security Appliance and RSA DLP network to interoperate?

TAC **Document ID: 118141**

Contributed by Jakob Dohrmann and Siddharth Rajpathak, Cisco TAC Engineers.

Jul 31, 2014

Contents

Question:

How to configure Cisco Web Security Appliance and RSA DLP network to interoperate?

Overview:

This document provides extra information beyond the Cisco WSA AsyncOS User Guide and the RSA DLP Network 7.0.2 Deployment Guide to help customers interoperate the two products.

Product Description:

Cisco Web Security Appliance (WSA) is a robust, secure, efficient device that protects corporate networks against web−based malware and spyware programs that can compromise corporate security and expose intellectual property. The Web Security appliance provides deep application content inspection by offering a web proxy service for standard communication protocols such as HTTP, HTTPS, and FTP.

The RSA DLP Suite comprises a comprehensive data loss prevention solution that enables customers to discover and protect sensitive data in the enterprise by leveraging common policies across the infrastructure to discover and protect sensitive data in the datacenter, on the network, and on endpoints. The DLP Suite includes the following components:

- ***RSA DLP Datacenter***. DLP Datacenter helps you locate sensitive data no matter where it resides in the datacenter, on file systems, databases, email systems and large SAN/NAS environments.
- ***RSA DLP Network***. DLP Network monitors and enforces the transmission of sensitive information on the network, such as email and web traffic.
- ***RSA DLP Endpoint***. DLP Endpoint helps you discover, monitor and control sensitive information on endpoints such as laptops and desktops.

The Cisco WSA has the ability to interoperate with RSA DLP Network.

RSA DLP Network includes the following components:

- ***Network Controller***. The main appliance that maintains information about confidential data and content transmission policies. The Network Controller manages and updates managed devices with policy and sensitive content definition along with any changes to their configuration after initial configuration.

- ***Managed devices***. These devices help DLP Network monitor network transmission and report or intercept the transmission:
    - ***Sensors***. Installed at network boundaries, Sensors passively monitor traffic leaving the network or crossing network boundaries, analyzing it for the presence of sensitive content. A Sensor is an out−of−band solution; it can only monitor and report policy violations.
    - ***Interceptors***. Also installed at network boundaries, Interceptors allow you to implement quarantining and/or rejection of email (SMTP) traffic that contains sensitive content. An Interceptor is an in−line network proxy and therefore can block sensitive data from leaving the enterprise.
    - ***ICAP servers***. Special purpose server devices that allow you to implement monitoring or blocking of HTTP, HTTPS, or FTP traffic containing sensitive content. An ICAP server works with a proxy server (configured as an ICAP client) to monitor or block sensitive data from leaving the enterprise

The Cisco WSA interoperates with RSA DLP Network ICAP Server.

Known Limitations

Cisco WSA External DLP integration with RSA DLP Network supports the following actions: Allow and Block. It does not yet support the "Modify / Remove Content" (also called Redaction) action.

Product Requirements for Interoperability

The inter−operability of the Cisco WSA and RSA DLP Network was tested and validated with the product models and software versions in the following table. While functionally speaking this integration may work with variations to the model and software, the following table represents the only tested, validated, and supported combinations. It is strongly recommended to use the latest supported version of both products.

Product	Software Version
Cisco Web Security Appliance (WSA)	AsyncOS versions 6.3 & above
RSA DLP Network	7.0.2

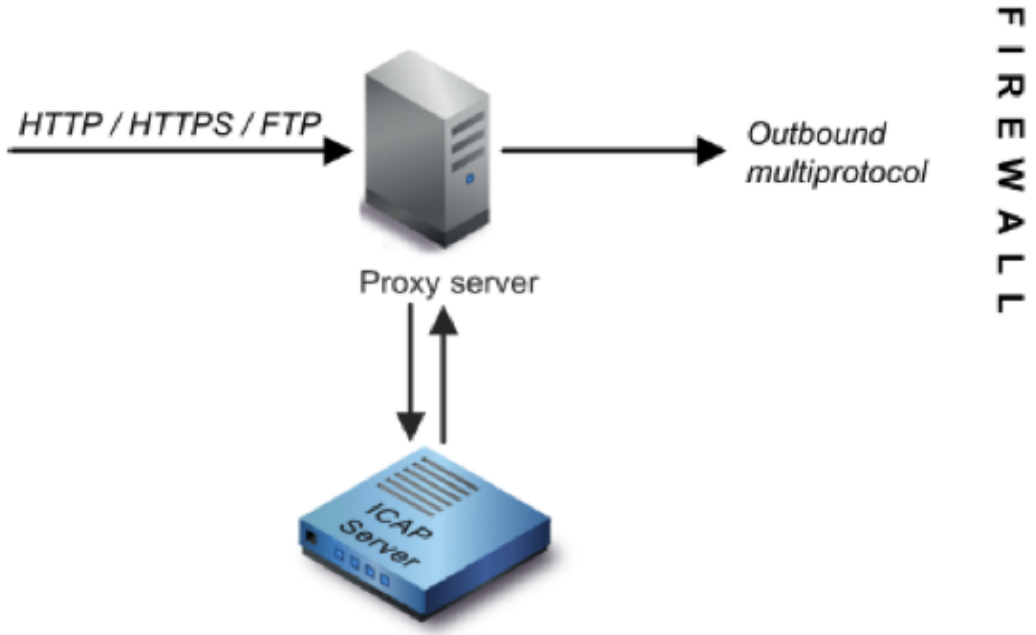
External DLP Feature

Using the External DLP feature of the Cisco WSA, you can forward all or specific outgoing HTTP, HTTPS, and FTP traffic from the WSA to DLP Network. All traffic is transferred using the Internet Control Adaptation Protocol (ICAP).

Architecture

The RSA DLP Network Deployment Guide shows the following generic architecture for inter−operating RSA DLP Network with a proxy server. This architecture is not specific to the WSA, but applies to any proxy that interoperates with RSA DLP Network.

Figure 1: Deployment Architecture for RSA DLP Network and the Cisco Web Security Appliance



Configuring the Cisco Web Security Appliance

1. Define an external DLP system on the WSA that works with the DLP Network ICAP server. For instructions, please see the attached excerpt from the WSA User Guide "User Guide Instructions Defining External DLP Systems".

2. Create one or more External DLP policies that define which traffic the WSA sends to DLP Network for content scanning using the below steps:

- Under ***GUI*** > ***Web Security Manager*** > ***External DLP policies*** > ***Add Policy***
- Click the link under the ***Destinations*** column for the policy group you want to configure
- Under the 'Edit Destination Settings' section, choose ?Define Destinations Scanning Custom Settings? from the drop down menu
- We can then configure the policy to 'Scan all uploads' or to scan uploads to certain domains/sites specified in custom URL categories

Configuring the RSA DLP Network

This document assumes that RSA DLP Network Controller, ICAP Server and Enterprise Manager have been installed and configured.

1. Use RSA DLP Enterprise Manager to configure a Network ICAP Server. For detailed instructions on setting up your DLP Network ICAP server, refer to the RSA DLP Network Deployment Guide. The main parameters you should specify on the ICAP Server configuration page are:
    1. The hostname or IP address of the ICAP Server.
    2. In the ***General Settings*** section of the configuration page, enter the following information:
        - ◊ The amount of time in seconds after which the server is deemed to have timed out in the ***Server Timeout in Seconds*** field.

        - ◊ Select one of the following as a response ***Upon Server Timeout***:
        - ◊ ***Fail Open***. Select this option if you want to allow transmission after a server timeout.
        - ◊ ***Fail Closed***. Select this option if you want to block transmission after a server timeout.
2. Use RSA DLP Enterprise Manager to create one or more Network−specific policies to audit and block network traffic that contains sensitive content. For detailed instructions for creating DLP policies, refer to the RSA DLP Network User Guide or the Enterprise Manageronline help. The main steps to perform are the following:
    1. From the policy template library enable at least one policy that makes sense for your environment and the content you will be monitoring.
    2. Within that policy, setup DLP Network−specific policy violation rules that specify actions the Network product will perform automatically when events (policy violations) occur. Set the policy detection rule to detect all protocols. Set the policy action to "audit and block".

Optionally we can use RSA Enterprise Manager to customize the Network notification that is sent to the user when policy violations occur. This notification is sent by DLP Network as a replacement for the original traffic.

Test the Setup

1. Configure your browser to direct outgoing traffic from your browser to go directly to the WSA proxy.

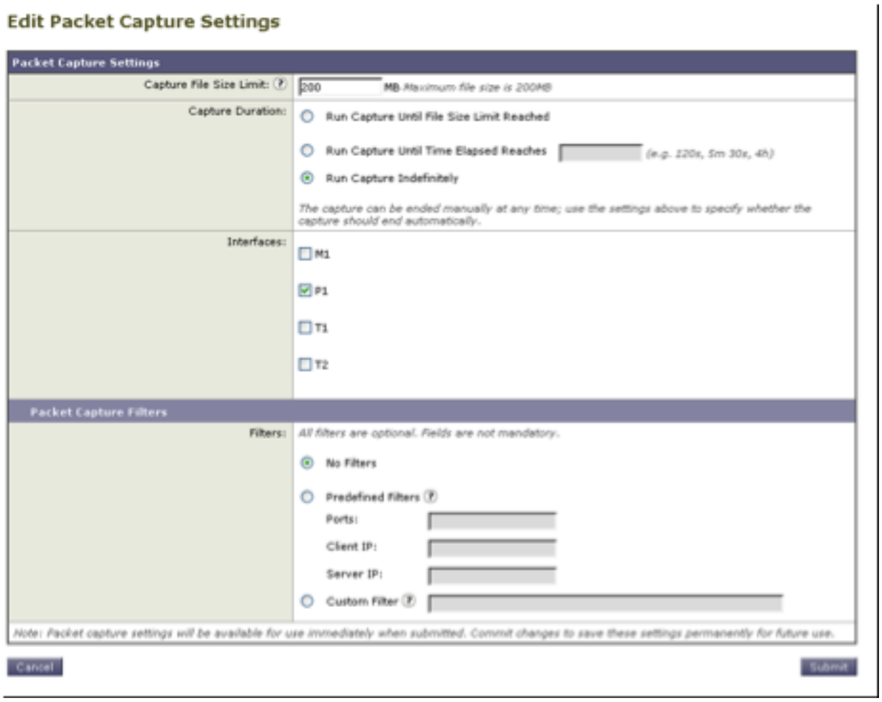
   For example, if you are using the Mozilla FireFox browser, do the following:
    1. In the FireFox browser, select ***Tools > Options***. The Options dialog appears.
    2. Click the ***Network*** tab, then click ***Settings***. The Connection Settings dialog appears.
    3. Select the ***Manual Proxy Configuration*** checkbox, then enter the IP address or hostname of the WSA proxy server in the ***HTTP Proxy*** field and the port number 3128 (the default).
    4. Click ***OK***, then ***OK*** again to save the new settings.
2. Attempt to upload some content that you know is in violation of the DLP Network policy you previously enabled.
3. You should see a Network ICAP discard message in the browser.
4. Use 'Enterprise Manager' to view the resulting event and incident that were created as a result of this violation of policy.

Troubleshooting

1. When configuring an external DLP server on the Web Security appliance for RSA DLP Network, use the following values:

    - ♦ Server Address: The IP address or host name of the RSA DLP Network ICAP server
    - ♦ Port: The TCP port used to access the RSA DLP Network server, typically ***1344***
    - ♦ Service URL Format: ***icap://<hostname_or_ipaddress>/srv_conalarm***
    - ♦ Example: icap://dlp.example.com/srv_conalarm
2. Enable the traffic capturing feature of WSA to capture the traffic between WSA proxy and the Network ICAP server. This is helpful when diagnosing connectivity issues. To do this, do the following:

    - ♦ On WSA GUI, go to the ***Support and Help*** menu in the top right of the user interface. Select ***Packet Capture*** from the menu, then click the ***Edit Settings*** button. The Edit Capture Settings window appears.



Edit Packet Capture Settings

Packet Capture Settings

Capture File Size Limit: 200 MB *Maximum file size is 200MB*

Capture Duration:
- ○ Run Capture Until File Size Limit Reached
- ○ Run Capture Until Time Elapsed Reaches *(e.g. 120s, 5m 30s, 4h)*
- ● Run Capture Indefinitely

The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.

Interfaces:
- □ M1
- ☑ P1
- □ T1
- □ T2

Packet Capture Filters

Filters: *All filters are optional. Fields are not mandatory.*
- ● No Filters
- ○ Predefined Filters
  - Ports:
  - Client IP:
  - Server IP:
- ○ Custom Filter

Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

- In the ***Packet Capture*** Filters section of the screen, enter the IP address of the Network ICAP server in the ***Server IP*** field.
- Click ***Submit*** to save your changes.

3. Use the following custom field in the WSA access logs (Under ***GUI*** > ***System Administration*** > ***Log Subscriptions*** > ***accesslogs***) to get more information:
   - %Xp: External DLP server scanning verdict (0 = no match on the ICAP server; 1 = policy match against the ICAP server and '− (hyphen)' = No scanning was initiated by the external DLP server)

User Guide Instructions Defining External DLP Systems.

Updated: Jul 31, 2014 Document ID: 118141