Blue Coat Systems, Inc.
SSL Visibility Appliance

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: March 25, 2015

Partner Information

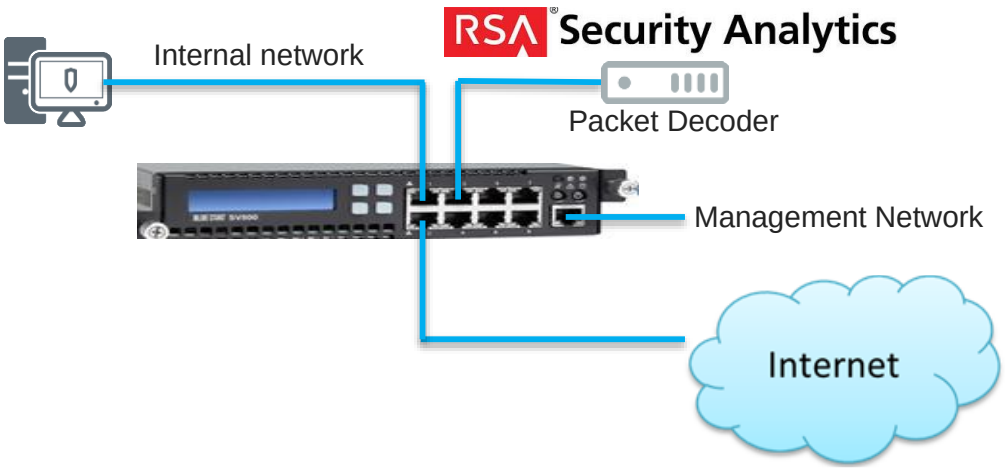
Product Information	
Partner Name	Blue Coat Systems, Inc.
Web Site	www.bluecoat.com
Product Name	SSL Visibility Appliance
Version & Platform	3.8.2-406
Product Description	Use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption is growing tremendously fast worldwide. Today's enterprises typically see that 25% or more of their network traffic uses SSL encryption – and this amount is expected to grow more than 20% annually. Encryption protects data from being viewed in transit over the Internet—but it also creates a serious blind spot for threats, malware, Data Loss Prevention (DLP) and other regulatory or compliance risks. You need to address this dilemma and establish a comprehensive encrypted traffic management strategy that addresses acceptable-use policies for inbound and outbound encrypted traffic, while considering an extensible architecture that will scale and protect the business while also adhering to compliance demands.

Solution Summary

The Blue Coat SSL Visibility Appliance helps organizations mitigate risk by removing the security "blindfold" caused by encrypted traffic in today's networks. It provides the most cost-effective way to manage SSL encrypted traffic while preserving privacy, policy, compliance and the investment in the security infrastructure.

The SSL Visibility Appliance allows agencies to establish, enforce and manage policies for encrypted traffic throughout their networked infrastructure. Using the Host Categorization function, the SSL Visibility Appliance can block, permit and forward SSL encrypted traffic based on numerous, familiar policies, such as whether the traffic contains personal banking or healthcare data. This is accomplished in a similar manner as that used in the Blue Coat ProxySG, PacketShaper and other proven solutions, utilizing the comprehensive Global Intelligence Network for comprehensive, host category and threat updates across the globe

When used in conjunction with RSA Security Analytics the Blue Coat SSL Visibility Appliance can ensure compliance and prevent data loss by providing access to the decrypted plaintext of SSL flows.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Blue Coat SSL Visibility Appliance with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both 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 SSL Visibility components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the Blue Coat SSL Visibility Appliance is properly configured and secured before deploying to a production environment. For more information, please refer to the SSL Visibility Appliance *Administration and Deployment Guide*.**

Blue Coat SSL Visibility Appliance Configuration

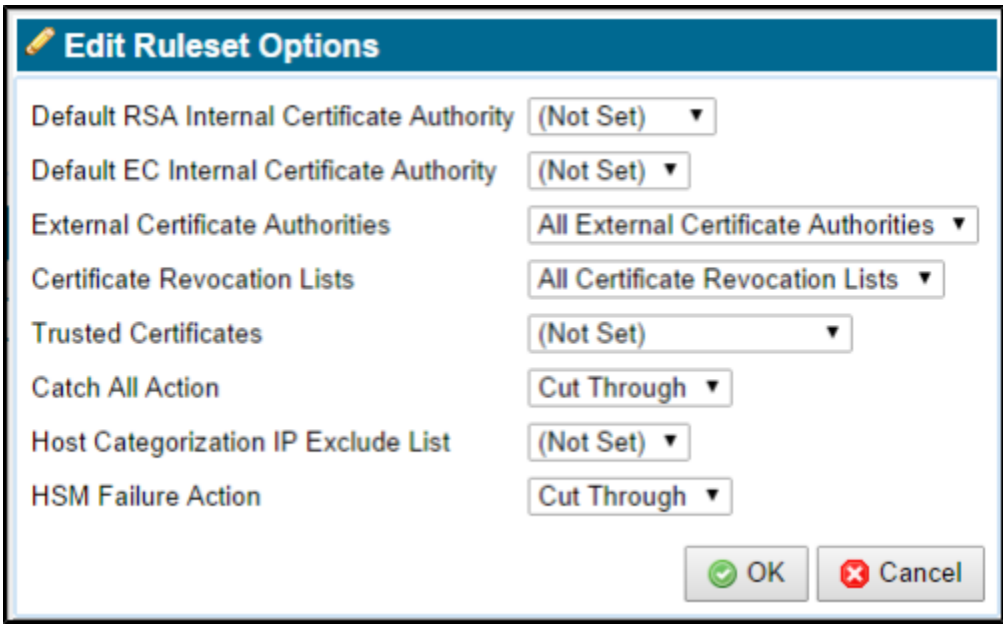
There are three main deployment modes for the SSL Visibility Appliance, with many variants within each mode. The example below provides instructions for deploying the device in **Passive-Inline Mode**. For details on how to configure a segment and its mode of operation refer to the SSL Visibility Appliance *Administration and Deployment Guide*.

Configuring Passive-Inline Mode

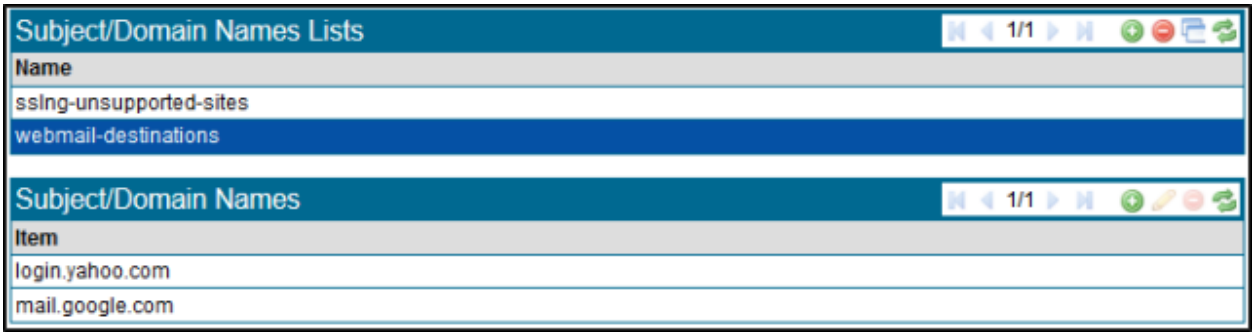
The following example shows the steps for configuring the SSL Visibility Appliance to inspect traffic that is destined for a number of SSL servers that you cannot obtain a copy of the private key and certificate for. This example illustrates the use of certificate resign to inspect traffic and also how to use custom lists to enable a single rule to apply to traffic going to multiple destinations and how to apply policy to SSL traffic that is not being inspected. The steps involved are:

- Create or load an resigning CA certificate and key into the SSL Visibility Appliance
- Create a ruleset that contains rules to inspect traffic going to specific destinations
- Create a list of destinations for use by a single rule
- Create a segment for passive-inline operation
- Activate the segment to start inspection

The next figure shows the edit options screen for a ruleset called passive-inline-example that has already been added to the rulesets on the system. The resigning CA created above is selected as the default Resigning Certificate Authority.



Before adding any rules to this ruleset we will create a list of Domain Names (DN) that will allow a single rule to apply to SSL sessions to multiple destinations.

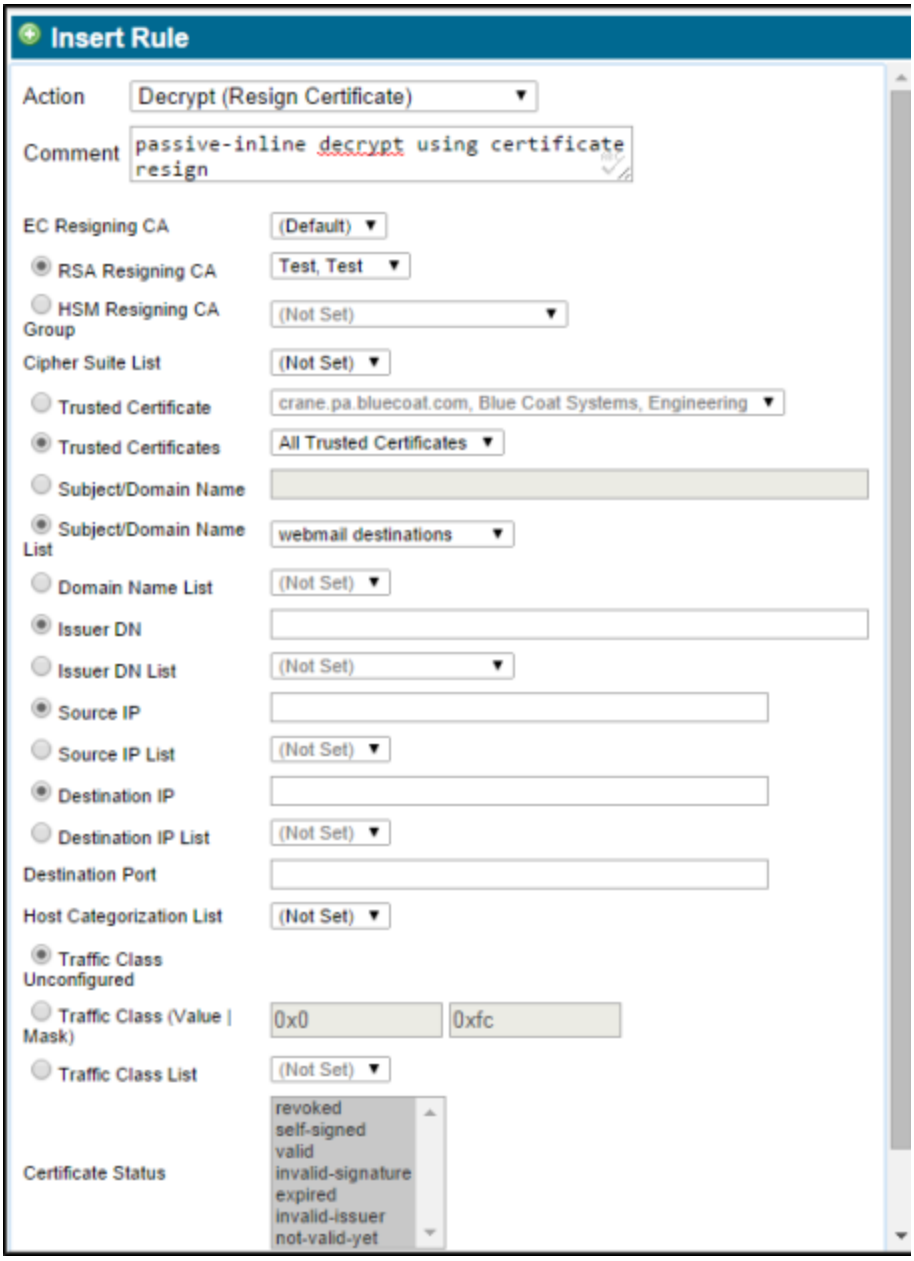


The list was created by clicking on the Add icon in the **Subject/Domain Names List** area and giving the new list the name **webmail destinations**. After creation, the empty list was selected in the **Subject/Domain Names List** area and then the **Add** icon was clicked in the **Domain Names List** area allowing a name to be added to the list. Two **Domain Names** have been added to the list. At the bottom of the screen is **a Policy Changes** notification block with buttons to Apply or Cancel the change. Click **Apply** to complete the process and to save the new list.

Creating a Ruleset

Now that the list exists we can go back to the ruleset and add a rule to use this list. The radio button beside **Subject DN List** is checked and **webmail destinations** has been selected from the drop down menu.

In this example, the Destination Port could be set to 443. The effect of this rule will be to inspect any traffic going to a server that has a DN which is in the **webmail destinations** list and where the destination port number is 443. If there was any traffic to one of the servers on the list that had a destination port number other than port 443 then this rule would not be triggered.



Having created the rule, click on **OK**. As the default action for this ruleset is **cut-through** any SSL traffic which does not match the rule will be cut through and will not be inspected. If we wanted to prevent traffic to a specific SSL site then another rule could be added to the ruleset that matched on the specific Domain Name for that site and had an action to drop the traffic.

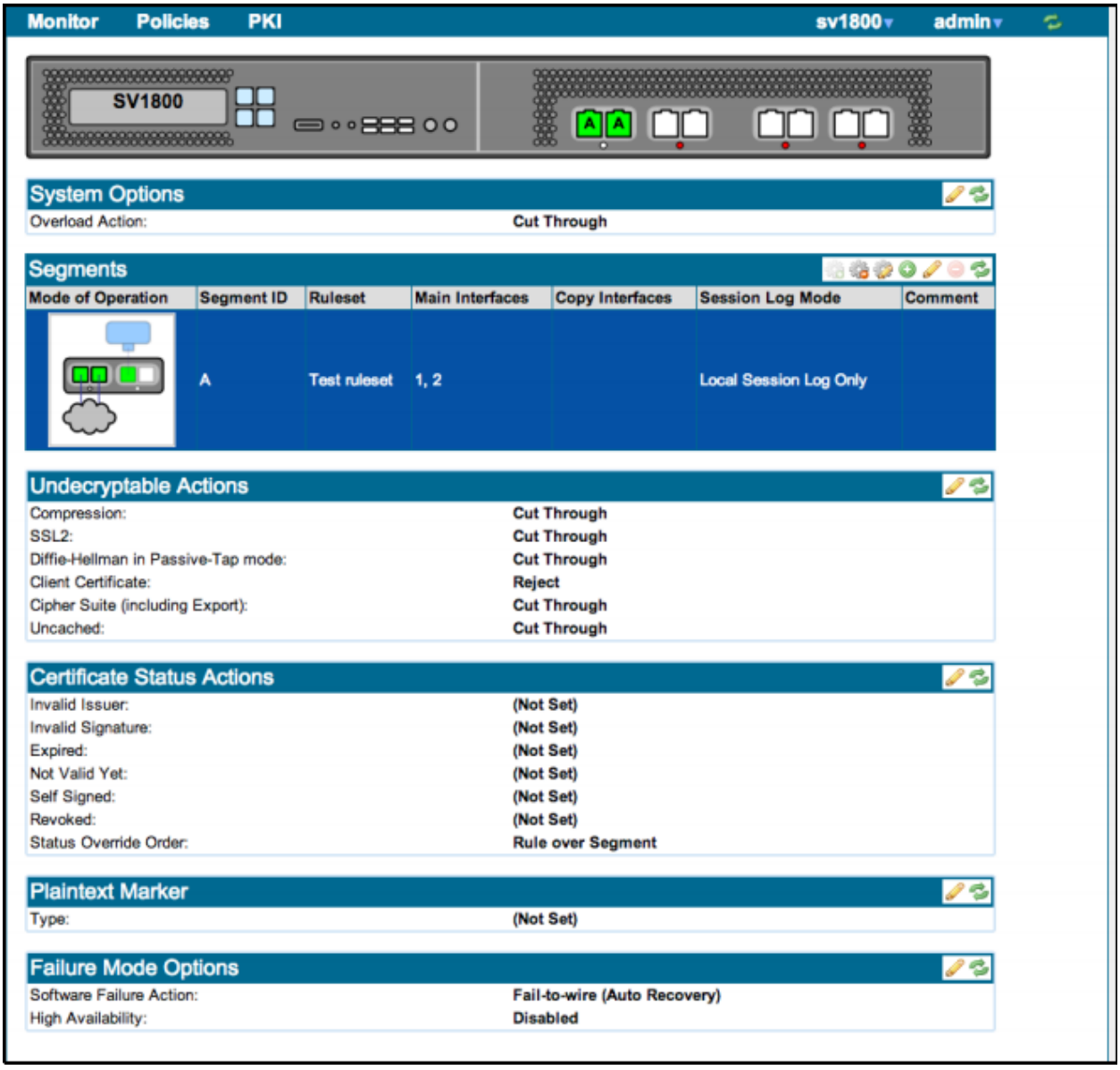
Creating a Segment

The final part of the process is to create a segment, configure it to use the ruleset just created and then to activate it.

To create a Segment, go to the **Policies/Segments** menu. You will see the **Segments** information. To create a new segment, click on the button in the **Segments** table and follow the same process as in the

earlier example but choosing a Passive-Inline segment type. At the bottom of the screen is a **Policy Changes** notification block with Apply and Cancel to Apply or Cancel the change. Click **Apply** to complete the process and to save the CA to disk. The figure shows the segment after it has been completed, saved and activated. Notice that:

- The ruleset created above is configured as the ruleset to be used for this segment.
- The session log has been turned on for this segment
- Interfaces 1, 2 and 3 used by this segment and are all currently down
- The segment ID is A



The final figure shows the segment status once it is active and the interface numbers which indicate how the device should be wired up to the network. In this example:

- Interfaces 1 and 2 connect to the network making the SSL Visibility Appliance a bump-in-the-wire
- Interface 3 connects to your RSA Security Analytics Packet Decoder.

The green background indicates that the segment is active. If there is SSL traffic to the server then the SSL Session Log and SSL Statistics screens should show this. See Section "SSL Session Log" for details on the session log and other monitoring tools. The details for the passive-inline segment configured in an earlier example (segment A) are shown on the next figure.

Segments Status

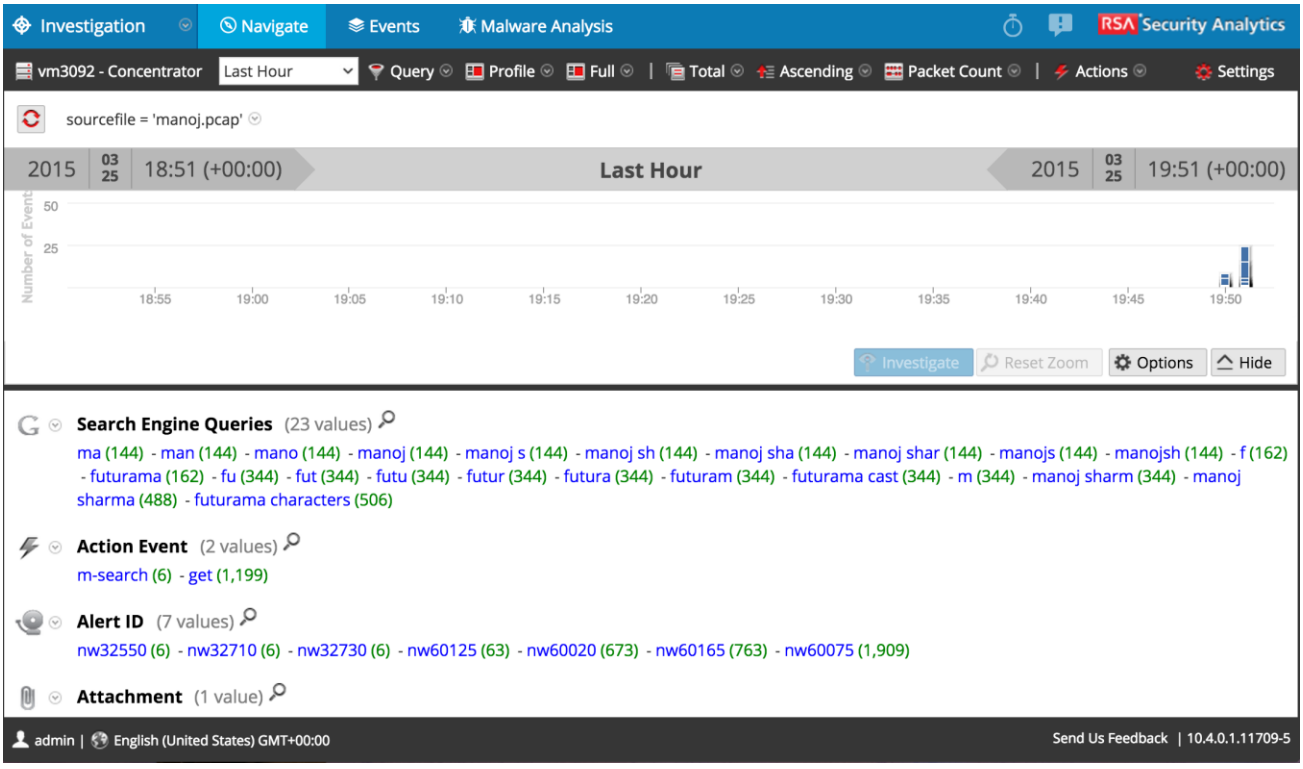
Segment ID	Main Interfaces	Copy Interfaces	Interfaces Down	Main Mode	Failures
A	1, 2			Passive-Inline	

RSA Security Analytics Configuration

There is no additional configuration required in RSA Security Analytics other than to have to appropriate parsers installed in order to analyze the type of SSL traffic you are decrypting.

> **Note: For HTTP content that is gzip encoded, some of the associated metadata may not be available in Security Analytics. It is possible however to fully reconstitute the decrypted TCP session when performing an investigation.**

Once the Security Analytics Packet Decoder has captured traffic and sent it to the Concentrator, you should see the related metadata when performing an investigation -- for example, a decrypted Google Search using the **Search_Engines** parser:



Certification Checklist for RSA Security Analytics

Date Tested: March 21st 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4	Virtual Appliance
SSL Visibility Appliance	SV800	3.8.2-406

Security Analytics Test Case	Result
Outbound SSL Decryption	
HTTPS	
Google Search	✓
Bing Search	✓
Facebook	✓
YouTube	✓
Twitter	✓
LinkedIn	✓
Reddit	✓
WEBMAIL	
GMail	✓
Yahoo	✓
Live	✓
Inbound SSL Decryption	
HTTPS	
Web Server	✓

JEC

✓ = Pass ✗ = Fail N/A = Non-Available Function