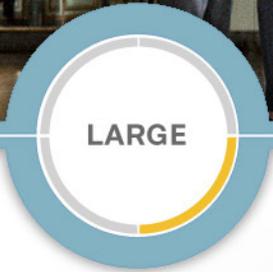




SBA
FOR
GOVT



LARGE



BORDERLESS
NETWORKS

RSA SIEM Partner Guide



SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

Who Should Read This Guide

- Has read the Cisco Security Information and Event Management Deployment Guide and the Internet Edge Deployment Guide
- Wants to connect Borderless Networks to an RSA SIEM solution
- Wants to gain a general understanding of the RSA SIEM solution
- Has a level of understanding equivalent to a CCNA® certification
- Wants to solve compliance and regulatory reporting problems
- Wants to enhance network security and operations
- Wants to improve IT operational efficiency
- Wants the assurance of a validated solution

Related Documents

Related Reading

- **BN** Design Overview
- **BN** Internet Edge Deployment Guide
- **BN** Internet Edge Configuration Guide
- **BN** SIEM Deployment Guide

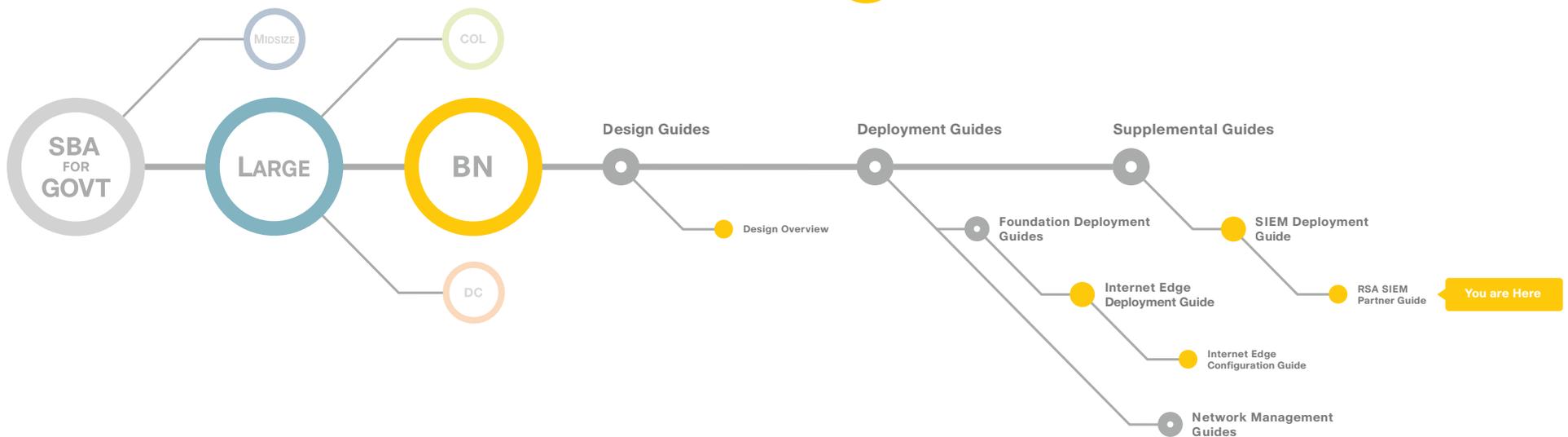


Table of Contents

Introduction	1	Product Overview	3
Cisco SBA for Large Agencies—Borderless Networks.....	1	Products Verified with Cisco SBA.....	16
Agency Benefits	2	Appendix A: SBA for Large Agencies Document System	17

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

Introduction

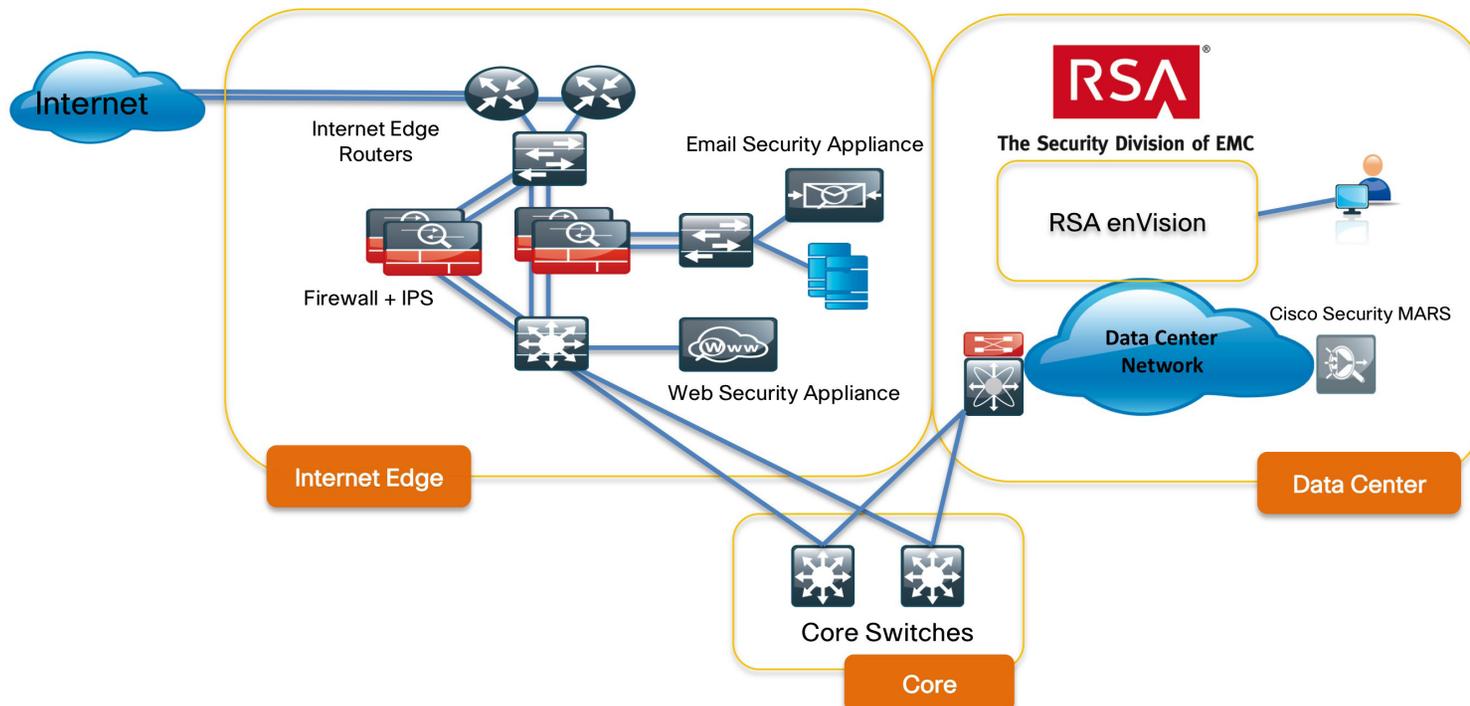
Cisco SBA for Large Agencies—Borderless Networks

The Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks offers partners and customers valuable network design and deployment best practices, helping agencies deliver superior end-user experience that include switching, routing, security and wireless technologies combined with the comprehensive management capabilities for the entire system. Customers can use the guidance provided in the architecture and deployment guides to maximize the value of their Cisco network in a simple, fast, affordable, scalable and flexible manner.

The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. The architecture also provides Cisco-tested configurations and topologies which CCNA-level engineers can use for design and installation, and to support agency needs

Cisco offers a number of options to provide security management capabilities. This guide is focused on our partnership with RSA and their enVision Security Information and Event Manager (SIEM) product.

Figure 1. RSA enVision Integrated into SBA for Large Agencies—Borderless Networks



Agency Benefits

The RSA enVision platform collects event logs generated by Cisco's network and security infrastructure, permanently archives copies of the data, processes the Cisco logs in real time, and generates alerts when it observes suspicious patterns of behavior. Security and IT administrators can interrogate the full volume of stored data through an intuitive dashboard, and advanced analytical software turns the complex, unstructured mass of raw data into structured information, giving administrators actionable insights to help them in three main areas:

Enhancing Security and Risk Mitigation

With real-time security event alerts, monitoring and drill-down forensic functionality, the platform gives administrators a clear view of important information. Because they can see and understand the threats and risks, they can take more effective actions to mitigate those risks.

Simplifying Compliance

Administrators can automatically collect log data about their Cisco network and security infrastructure, as well as file, application, and user activity, helping to simplify the compliance process. Over 1100 included reports are tailored to specific compliance requirements. The solution simplifies compliance with whatever legislation emerges in years to come, because it stores all log data without filtration or normalization and protects it from tampering, providing a verifiably authentic source of archived data.

Optimizing IT and Network Operations

Managed log data is the best source of information about infrastructure performance and user behavior. IT support staff can use the RSA enVision platform to track and manage activity logs for servers, networking equipment, and storage platforms, as well as monitor network assets and the availability and status of people, hardware, and applications. It provides an intelligent forensic tool for troubleshooting infrastructure problems and protecting infrastructure resources, and it assists IT managers in help desk operations and provides granular visibility into specific behaviors by end-users.

Notes

Product Overview

RSA enVision is a feature-rich compliance and security application. It allows you to capture and analyze log information automatically from your network, security, application, operating, and storage environments. The enVision LogSmart Internet Protocol Database (IPDB) provides the architecture to collect and protect all the data automatically, from any network device, without filtering or agents. It gives you an accurate picture of how your network is being used, and by whom. It independently monitors your network to verify security policies, to generate alerts for possible compliance breaches, and to analyze and report on network performance.

enVision is tightly coupled with its underlying appliance operating system and hardware, and together they are a highly scalable platform that provides guaranteed levels of performance.

RSA enVision is made up of three components, as shown in Figure 2:

Application: supports interactive users and runs the suite of analysis tools.

Collector: captures incoming events.

Database: manages access and retrieval of captured events.

The enVision ES series appliances are designed to operate in a stand-alone, non-distributed mode. They have all three enVision components—Application, Collector, and Database—installed on one appliance. The single appliance is a site. Some single appliance sites have an external storage system.

A range of appliances are available; all are based on the same hardware with licensing to suit specific requirements. To choose the most appropriate, look at the number of network devices to be monitored and the number of events per second to process. Table 1 shows the relative capacities of the various enVision ES appliance models.

Figure 2. RSA enVision Platform Architecture

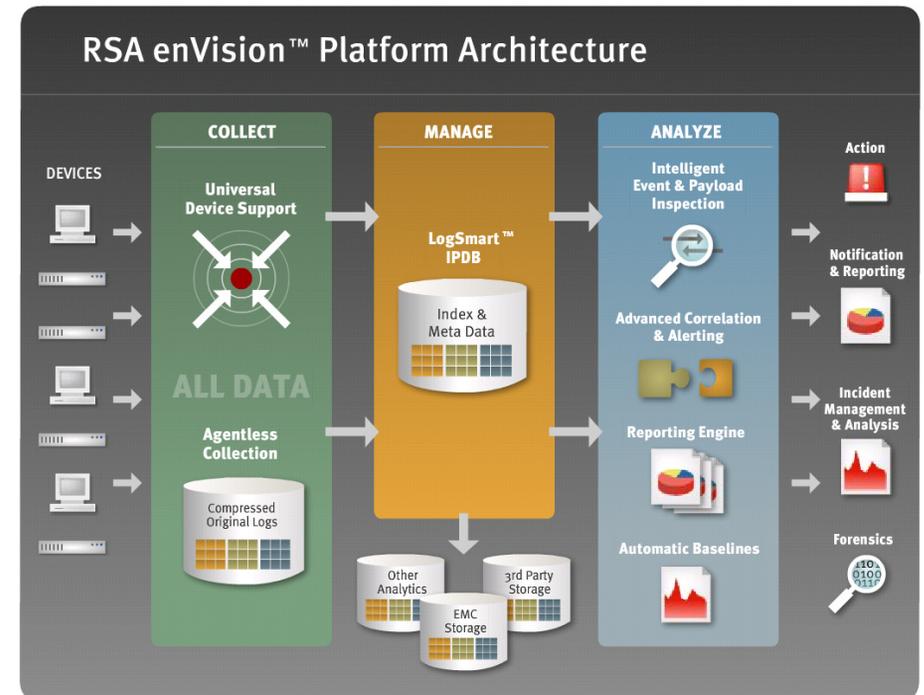


Table 1. Table 1. enVision ES Appliance Capacities

	ES 560	ES 1060	ES 1260	ES 2560	ES 3060	ES 5060	ES 7560
No of Users (Admin)	6	8	9	10	11	12	14
Events Per Second	500	1000	1200	2500	3000	5000	7500

Deploying RSA enVision

Deploying RSA enVision in your Cisco network involves the following procedures, each of which is discussed in the following sections:

1. Install RSA enVision, if you have not already done so.
2. Configure RSA enVision to receive logs from your Cisco devices.
3. Run reports in RSA enVision.
4. Perform maintenance and troubleshooting tasks as required.

Installing RSA enVision

The configuration process takes approximately 30 minutes to complete. You cannot change any of the site configuration options after the wizard is finished. The configuration tasks for a single appliance site are as follows

Step 1: Plan the installation

Please see the RSA enVision **Configuration Wizard Planning Worksheet — Single Appliance Site** for more information.

Step 2: Set up the RSA enVision appliance hardware

Step 3: Connect to the appliance

Connect to the appliance using a KVM switch. You can also connect remotely using DRAC instead of using a local KVM. See Appendix B “Dell Remote Access Controller Utility” in the RSA documentation for more information.

The Configuration Wizard starts automatically.

Step 4: Complete the enVision Configuration Wizard



Tech Tip

enVision uses the default IP address **192.168.1.55**. IP address conflicts can occur if the LAN cable is connected to an existing network when you run the configuration wizard. For this reason, you should verify the LAN cable is not connected to an existing network or confirm the IP address is not being used **before** you run the configuration wizard.

If you click **Cancel** at any time while using the wizard, you must restart the wizard to configure your site. To restart the wizard, double-click the **Isconfigurationwizard.exe** file in the **c:\windows\installations** directory.

When the wizard displays the Review Page window, verify that everything is correct on the Review Page. Click **Finish**. (If the Review page is not correct, click **Cancel** and check your hardware setup.)

In the last step, the wizard displays the enVision Configuration Wizard Log window. The log displays the steps the system is performing to configure the site. The system restarts several times while completing the setup.

The appliances restart automatically when the site configuration process is complete.

Step 5: Install updates

Immediately after you configure RSA enVision 4.0, RSA strongly recommends that you download and install two Content Updates: Event Source Update Package and VAM & Signature Content Update Package.

Go to RSA SecurCareOnline <https://knowledge.rsasecurity.com>. Click on **Products**. Under **RSA enVision** click **Content Updates**. Complete the instructions available on that page to download and install the updates.

Step 6: Apply licenses

Apply the license keys that were sent, via email, to the contact person that you provided when you ordered the enVision appliance.

Adding Cisco Devices in RSA enVision to Receive Logs

RSA enVision collects, analyzes, and stores logs from event sources throughout an agency's IT environment. The logs and the descriptive metadata that enVision adds are stored in the LogSmart Internet Protocol Database (IPDB).

Event sources are the assets on the network, such as servers, switches, routers, storage arrays, operating systems, and firewalls.

The enVision administrator configures event sources to send their logs to the Collector or configures the Collector to poll event sources and retrieve their logs. The Collector receives all system logs in their original form, without filtering, normalization, or compression.



Tech Tip

These instructions assume that you are running RSA enVision version 4.0 or newer. Interface elements may be different in older versions, and not all features shown below are supported in versions prior to 4.0.

Process

Receiving Logs from a Cisco ASA 5500 Series Adaptive Security Appliance

Cisco ASA 5500 Series Adaptive Security Appliances generate syslog events. To receive these events in RSA enVision, the adaptive security appliance should be configured to send syslog messages to the enVision appliance, which will automatically recognize that the messages are coming from a new source. If the adaptive security appliance also has a Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM) installed, enVision can be configured to also retrieve IPS events using the SDEE protocol.

Procedure

Configuring syslog on a Cisco ASA 5500

Step 1: Connect to the adaptive security appliance using telnet or SSH.

Step 2: Enter the enable mode by typing:
enable

Step 3: Enter the configure mode by typing:
config terminal

Step 4: Type the following lines:
no logging timestamp
logging host inside 10.4.200.115
(where **10.4.200.115** is the IP address of the enVision appliance)

Step 5: Press **Ctrl + Z** to exit config mode.

Step 6: Type the following command to save the configuration changes:
copy running-config startup-config

Procedure

Configuring IPS SDEE for an AIP-SSM

Step 1: Log in to enVision.

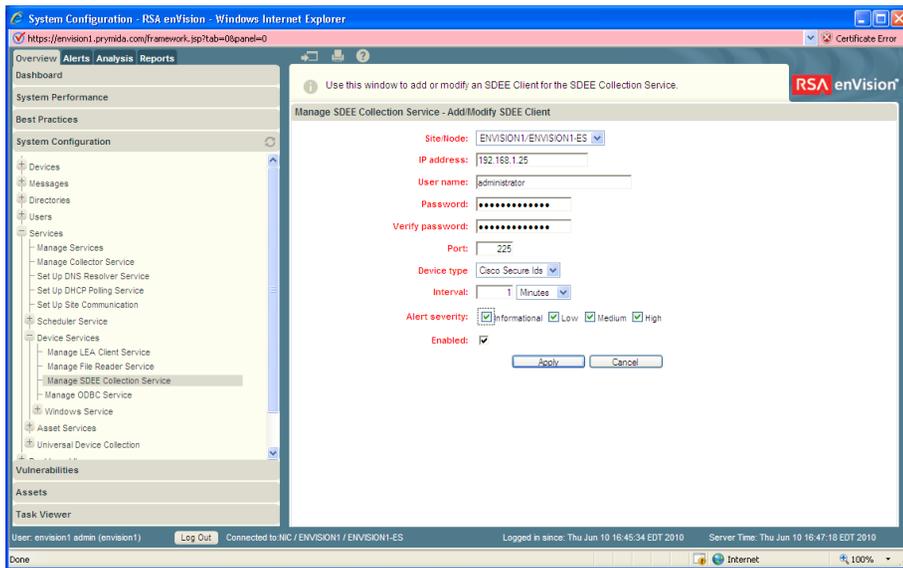
Step 2: Click **Overview > System Configuration > Services > Device Services > Manage SDEE Collection Service** to display the **Manage SDEE Collection Service** window.

Step 3: Perform one of the following actions:

- Click **Add** to add an IPS server.
- Click the IP address of an existing IPS server to modify it.

The system displays the **Add/Modify SDEE Client** window, shown in Figure 3.

Figure 3. Adding an SDEE Client



Step 4: Complete the window with the information shown in Table 2:

Table 2. SDEE Client Configuration Information

Field	Value
IP address	IP address of the IDS sensor or module in the Adaptive Security Appliance
Username	User account on the IDS sensor or module
Password	Password to the user account
Verify password	Password to the user account
Port	The port on which the IDS accepts connections to the SDEE service (by default, 443 for HTTPS)
Device type	Accept the default value Cisco Secure Ids
Alert severity	Defaults to all levels
Enabled	Ensure that this is checked on

Step 5: Click Apply.

The system saves the information and displays the **Manage SDEE Collection Service** window.

Process

Receiving Events from Cisco IPS 4200 Series Sensors

Procedure

Configuring Cisco IPS 4200 for enVision

Allow enVision access to the sensor. Complete the following task on the Cisco IPS event source.

1. Log in using administrative credentials.
2. Type the following commands:


```
configure terminal
service host
network-settings
```
3. Configure the access list to allow connections from the enVision host to access the sensor. Here are some examples:
 - To allow connections from a subnet: access-list 10.4.200.0/24
 - To allow connections from a host: access-list 10.4.200.66
4. Exit the configuration mode, confirming to save changes when prompted.

Procedure

Configuring IPS SDEE for IPS 4200

Step 1: Log in to enVision.

Step 2: Click **Overview > System Configuration > Services > Device Services > Manage SDEE Collection Service** to display the **Manage SDEE Collection Service** window.

Step 3: Perform one of the following actions:

- Click **Add** to add an IPS server.
- Click the IP address of an existing IPS server to modify it.

The system displays the **Add/Modify SDEE Client** window, shown in Figure 3 above.

Step 4: Complete the window with the information shown in Table 2.

Step 5: Click Apply.

The system saves the information and displays the **Manage SDEE Collection Service** window.



Tech Tip

enVision uses TCP port 443 (open outbound) to obtain information from this device.

Process

Cisco IronPort Email Security Appliance Configuration Instructions

You must complete these tasks to configure a Cisco IronPort Email Security Appliance (ESA):

1. Configure Log Subscriptions on the Email Security Appliance.
2. Configure the NIC File Reader Service in RSA enVision to read the exported log files; see the **Set Up File Reader Service** topic in the RSA enVision online help for more information.

Procedure

Configure Log Subscriptions

Step 1: Log in to the ESA web interface.

Step 2: Define a Log Subscription for Authentication Logs:

1. Select **System Administration > Log Subscriptions**
2. Click **Add Log Subscription**
3. Choose **Authentication Logs** from the **Log Type** drop-down list
4. In the **Retrieval Method** section, select **SCP on Remote Server**

Under **SCP on Remote Server**, complete the fields as shown in Table 3:

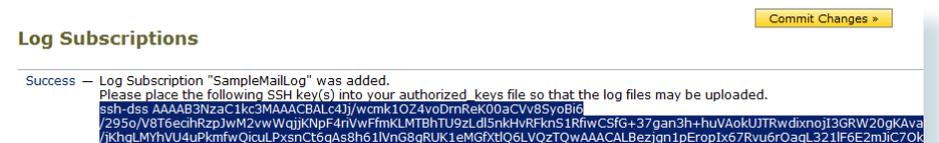
Table 3. SCP Configuration Information for Email Security Appliance Logs

Field	Action
Maximum Time Interval Between Transferring	Type 180 .
Protocol	Select SSH2 .
SCP Host	Enter the IP address of your enVision system.
Directory	Type CISCO_IRONPORT_ESA_ironport-IP-address where ironport-IP-address is the IP address of Cisco IronPort ESA.
Username	Type nic_sshd .

5. Click **Submit**.

An SSH key is generated and displayed as shown in Figure 4.

Figure 4. SSH Key Generation



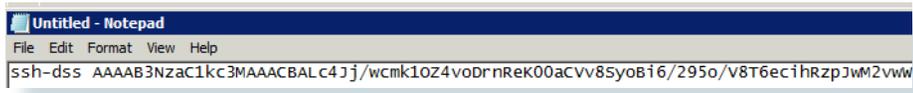
6. Copy the generated SSH key to a new text file, and save the text file. In the following steps of this example, the file name is **id_rsa.pub**.



Tech Tip

The entire SSH key must be on a single line and cannot include any spaces or line breaks within the key. If necessary, remove extraneous spaces using a text editor, as shown in Figure 5.

Figure 5. Checking the SSH Key in a Text Editor



Step 3: To configure a subscription for mail delivery logs, repeat the procedure from Step 2, but choose **IronPort Text Mail Logs** from the **Log Type** drop-down list. Note that the SSH key generated is the same as before, and does not need to be copied again.

Step 4: Repeat Step 2 again, choosing **CLI Audit Logs** as the log type.

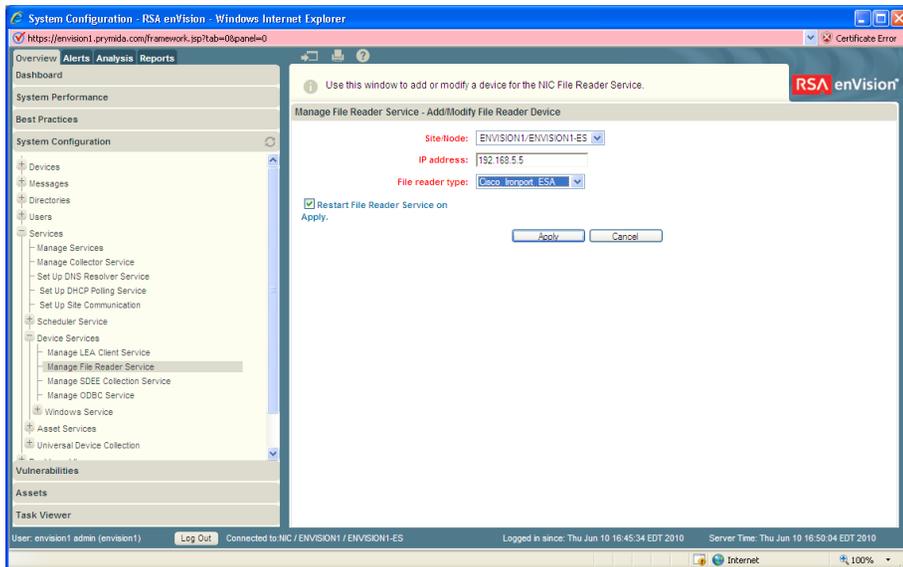
Step 5: Click **Commit Changes** to save all log settings.

Procedure

Configure File Reader Service on enVision

Step 1: Log in to RSA enVision, go to **Overview > System Configuration > Services > Device Services > Manage File Reader Service** and click **Add**. Figure 6 shows the process of adding a new file reader..

Figure 6. Configuring a File Reader Service



Step 2: In the **Add/Modify File Reader Device** window, select **Cisco_IronPort_ESA** from the **File reader type** drop-down list.

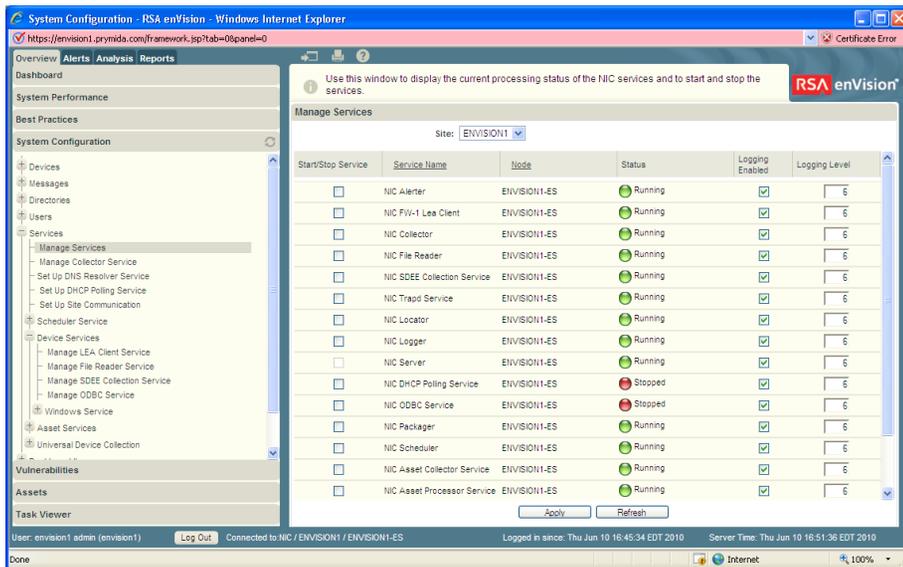
Step 3: In the **Site/Node** field, note the name of the site/node from which you are collecting. You will need this information in step 6 below.

Step 4: Click **Apply**.

Step 5: To have RSA enVision recognize the configuration change:

- On a single-appliance site, enVision starts the NIC File Reader Service, recognizing the configuration change immediately, so no action is necessary.
- On a multiple-appliance site, complete the following:
 1. Wait three minutes.
 2. Go to the **Overview > System Configuration > Services > Manage Services** window. Figure 5 shows the Manage Services window.
 3. Select **Start/Stop Service** to stop the NIC Reader Service on the site/node you noted in Step 3.
 4. Click **Apply**.
 5. Click **Refresh** until the Status column shows the site/node is stopped.
 6. Select **Start/Stop Service** to start the NIC File Reader Service on the site/node you noted in Step 3.
 7. Click **Apply**.
 8. Click **Refresh** periodically until the Status column shows the site/node is running.

Figure 7. The Manage Services Window



Step 6: Copy the text file containing the key that you saved from the Email Security Appliance configuration procedure (named `id_rsa.pub` in this example) to the `bin` folder on your enVision installation. The path to this location depends on the site/node name of your enVision system. For example, with the node shown in Figure 6, the `bin` folder would be located under `E:\nic\4000\ENVISION1-ES\`.

Step 7: On your enVision system, open a command prompt and change directory to `bin` under your enVision installation.

Step 8: To install the public key on enVision, type:

```
add_winsshd_key.bat id_rsa.pub
```

Tech Tip

If your key file is named something other than `id_rsa.pub`, use that name in the command.

Process

Cisco IronPort Web Security Appliance Configuration

To configure a Cisco IronPort Web Security Appliance (WSA), you must complete these tasks:

1. Configure Log Subscriptions on the WSA.
2. Configure the NIC File Reader Service in RSA enVision to read the exported log files; see the Set Up File Reader Service topic in the RSA enVision online help for more information.

Procedure

Configure Log Subscriptions on the WSA

Tech Tip

All logs are optional, however, enVision parses only the logs that are configured as follows.

Step 1: Log in to the WSA web interface.

Step 2: Define a Log Subscription for Access Logs:

1. Select **System Administration > Log Subscriptions**.
2. Click **Add Log Subscription**.
3. Choose **Access Logs** from the **Log Type** drop-down list.
4. Select **Apache** as the **Log Style** and enter the following text in **Custom Fields**:


```
%k %p %u %XF
```
5. In the **Retrieval Method** section, select **SCP on Remote Server**.
6. Configure the SCP parameters as shown in Table 3 of the previous section, except that in this case, the **Directory** should be set as follows: `CISCO_IRONPORT_WSA_ironport-IP-address`, where `ironport-IP-address` is the actual IP address of the device, for example, `CISCO_IRONPORT_WSA_1.2.3.4`.

7. Click **Submit**.
8. Copy the generated SSH Key to a new text file. Save the text file using a name such as `id_rsa.pub`.



Tech Tip

The entire key must be on a single line. Also, remove any spaces from the key.

9. Add subscriptions for any other log file types that may be required. Important log types for security and audit requirements may include **CLI Audit Logs** and **IDS Data Loss Logs**.

Step 3: To configure W3C Logs, repeat the tasks from Step 2 above, selecting **W3C Logs** from the **Log Type** drop-down list. **Selected Log Fields** must be set to these values, in exactly the following order:

```
timestamp
x- elapsed-time
c-ip
s-ip
s-port
x-resultcode-httpstatus
sc-bytes
cs-method
cs-url
cs-username
x-hierarchy-origin
cs-mime-type
x-acntag
x-result-code
cs (User-Agent)
x-webcat-code-full
```



Tech Tip

IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved the first time.

Step 4: Click **Commit Changes**.

Procedure

Configure File Reader Service in enVision

Step 1: Log in to RSA enVision, go to **Overview > System Configuration > Services > Device Services > Manage File Reader Service** and click **Add**. The process of adding a new file reader is shown in Figure 6 above.

Step 2: In the **Add/Modify File Reader Device** window, select **Cisco_Ironport_WSA** from the **File reader type** drop-down list.

Step 3: In the **Site/Node** field, note the name of the site/node from which you are collecting. You will need this information in step 6 below.

Step 4: Click **Apply**.

Step 5: To have RSA enVision recognize the configuration change:

- On a single-appliance site, enVision starts the NIC File Reader Service, recognizing the configuration change immediately, so no action is necessary.
- On a multiple-appliance site, complete the following:
 1. Wait three minutes.
 2. Go to the **Overview > System Configuration > Services > Manage Services** window. Figure 5 in the previous section shows the Manage Services window.
 3. Select **Start/Stop Service** to stop the NIC Reader Service on the **site/node** you noted in Step 3.
 4. Click **Apply**.
 5. Click **Refresh** until the Status column shows the site/node is stopped.
 6. Select **Start/Stop Service** to start the NIC File Reader Service on the site/node you noted in Step 3.
 7. Click **Apply**.
 8. Click **Refresh** periodically until the Status column shows the site/node is running.

Step 6: Copy the text file containing the key that you saved from the Web Security Appliance configuration procedure (named `id_rsa.pub` in this example) to the **bin** folder on your enVision installation. The path to this location depends on the site/node name of your enVision system. For example, with the node shown in Figure 6, the bin folder would be located under `E:\nic\4000\ENVISION1-ES\`.

Step 7: On your enVision system, open a command prompt and change directory to bin under your enVision installation.

Step 8: To install the public key on enVision, type:

```
add_winsshd_key.bat id_rsa.pub
```



Tech Tip

If your key file is named something other than id_rsa.pub, use that name in the command.

Process

Cisco Security MARS Configuration

Important: For Cisco Security MARS, two collection methods are available: the originally supported syslog collection and the newly added File Reader Service to collect raw message logs. The collection methods function differently. The syslog collection method collects Cisco Security MARS log messages. The File Reader Service collects the logs of the event sources which Cisco Security MARS is reporting on. Cisco recommends using the raw message logs, because their coverage is more comprehensive than syslog forwarding. This guide shows how to configure raw message collection.

To configure Cisco Security MARS, you must complete these tasks:

1. Configure the NIC File Reader Service in RSA enVision to read the exported message files; see the **Set Up File Reader Service** topic in the RSA enVision online help for more information.
2. Create a Windows user account on the enVision server
3. Create an SFTP user account
4. Configure the File Reader Service to collect raw message logs

Procedure

Configure File Reader Service in enVision

Step 1: Log in to enVision, go to **Overview > System Configuration > Services > Device Services > Manage File Reader Service**, and click **Add**.

Step 2: Make a note of the value in the **Site/Node** field. This is the site or node from which you are collecting messages.

Step 3: Enter the IP address of your Cisco Security MARS appliance and select **CiscoMars_Syslog** from the **File reader type** drop-down list.



Tech Tip

The "CiscoMars_Syslog" file reader type option is available only if you have installed the March 2010 Event Source Update to enVision 4.0.

Step 4: Click **Apply**.

Step 5: To have RSA enVision recognize the configuration change:

- On a single-appliance site, enVision starts the NIC File Reader Service recognizing the configuration change immediately so no action is necessary.
- On a multiple-appliance site, complete the following:
 1. Wait 3 minutes.
 2. Go to the **Overview > System Configuration > Services > Manage Services** window. Figure 5 in the previous section shows the Manage Services window.
 3. Select **Start/Stop Service** to stop the NIC Reader Service on the **site/node** you noted in Step 3.
 4. Click **Apply**.
 5. Click **Refresh** until the Status column shows the site/node is stopped.
 6. Select **Start/Stop Service** to start the NIC File Reader Service on the site/node you noted in Step 3.
 7. Click **Apply**.
 8. Click **Refresh** periodically until the Status column shows the site/node is running.

Procedure

Create a Windows User Account

Step 1: On the RSA enVision server, click **Start > Administrator Tools > Active Directory Users and Computers**.

Step 2: Right click **Users**, and select **New > User**.

Step 3: In the **New Object – User** window, complete the fields using **ciscomars** as the user log on name.

Step 4: Click **Next**.

Step 5: Enter a password for the account. Click to remove the check mark next to **User must change password at next logon**. Click to select **User cannot change password** and **Password never expires**. Ensure that the account is not disabled. Click **Next**, and then **Finish**.



Tech Tip

The password policy in effect on the RSA enVision system requires at least ten characters, using a mix of upper and lower case letters, numbers, and non-alphanumeric characters (such as %, &, and !). Make a note of this password as you will need this password again at a later step.

Procedure

Create an SFTP User Account

Step 1: Click **Start > Administrative Tools > WinSSHD Control Panel**.

Step 2: On the **Server** tab, click **Edit Settings**.

Step 3: Click **Configuration > Access Control > Windows Accounts**.

Step 4: Select the **nic_sshd** account and click **Copy**.

Step 5: Change the Windows account name to the user account that you created in Active Directory Users and Computers, and complete the fields as follows:

1. Ensure that **Password authentication** is set to **Allowed**.
2. Ensure that **Public key authentication** is set to **Disabled**.

3. Ensure that **Permit SCP** is set to **No**.
4. Ensure that **Permit SFTP** is set to **Yes**.

Step 6: Click **OK**.

Step 7: Click **OK** to commit the changes, and close the WinSSHD Settings window.

Procedure

Configure MARS to Archive Message Logs



Tech Tip

To configure Cisco Security MARS for File Reader Service to collect raw message logs, you must obtain RSA enVision 4.0 Service Pack 3, bug fix (EBF) ENV-32744.

Step 1: Log in to your Cisco Security MARS appliance.

Step 2: Under the Device Configuration and Discovery Information section, click **Admin > System Maintenance > Data Archiving**, and complete the fields as follows:

1. In the **Archiving Protocol** field, select **SFTP**.
2. In the **Remote Host IP** field, enter the IP address of your enVision appliance.
3. In the **Remote Path** field, type */CiscoMars_Syslog_IP address of Cisco MARS*
4. In the **Remote Storage Capacity in Days** field, leave the default as **10** days.
5. In the **Username** field, enter the user name that you created for the SFTP account on enVision.
6. In the **Password** field, enter the password that you created for the SFTP account on enVision.

Step 3: Click **Apply**.

Step 4: Click **Activate**.

Tech Tip

The Activate button remains red until it is clicked.

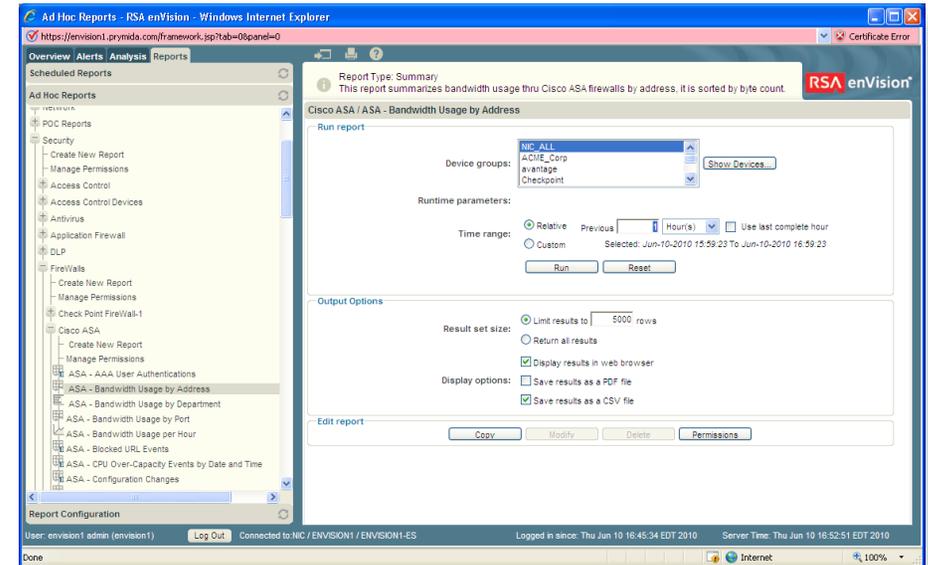
Step 5: Click Close to close the Activating Changes window.

Reporting on RSA enVision

RSA enVision provides over 100 standard reports that gather common network security and traffic analysis statistics into tables and graphs. Administrators can copy and modify these reports or create custom reports to meet specific reporting needs. Administrators and users with the appropriate permissions can create, manage, and run both scheduled and ad hoc reports. Optionally, a report can run once on a specified day or run repeatedly at specified times. RSA enVision can email generated reports to departments and people who need them such as IT, human resources, the CIO office, compliance officers, and managers. RSA enVision provides reports for security, host, network, storage, and other devices. RSA enVision also provides a number of report packages to satisfy compliance needs such as Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

An enVision report consists of a single graph or a single table. For some purposes, a user may need more data than can be included in a single graph or table. RSA enVision can group multiple reports together so they run at the same time. Figure 8 shows the process of setting up a bandwidth usage report.

Figure 8. Setting Up a Report



Queries are similar to reports except that queries are ad hoc only. They generally execute faster, as they are intended to deal with smaller amounts of data than reports. A query returns only tabular data. Analysts might use queries in forensic analysis, for example to drill quickly into an alert or other condition discovered in RSA enVision Event Explorer or to audit some past event. Queries help users and administrators retrieve and examine any data collected by enVision. Query results can be based on IP addresses, dates and times, event message types, and other criteria. Users can generate a query in response to an alert condition appearing in Event Explorer.

Queries use SQL syntax to construct statements for accessing database tables for conditions and events including:

- General traffic flows and events that were allowed
- Accesses that were denied or prevented from happening based on policy
- Status and health parameters
- URL information indicating where users have visited

Users can compose simple or complex queries:

- A simple query is a single logical statement (a single row in the Edit query table).
- A complex query consists of multiple statements (multiple rows in the Edit query table) logically joined using AND or OR. Multiple statements can narrow a query or extract a more accurate set of results for given criteria.

Figure 9. Query Results Display

DeviceAddress	DeviceHostName	Date/Time	MessageID	LocalAddress	LocalHostName	LocalPort	LocalPortName	TranslateAddress	Foreign
10.10.18.2	10.10.18.2	2010-06-10 16:37:58.0	302014	10.10.100.16		443			56.2
10.10.18.2	10.10.18.2	2010-06-10 16:38:02.0	302014	66.28.153.100		80			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:06.0	302014	10.10.18.60		110			45.6
10.10.18.2	10.10.18.2	2010-06-10 16:38:07.0	302014	66.28.153.100		80			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:09.0	302014	207.46.182.140		138			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:11.0	302014	64.58.76.231		80			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:11.0	305003	10.10.16.104		0		172.16.3.112	
10.10.18.2	10.10.18.2	2010-06-10 16:38:13.0	302014	10.10.18.59		79			67.9
10.10.18.2	10.10.18.2	2010-06-10 16:38:18.0	302014	66.28.153.100		53			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:34.0	302014	216.239.33.101		80			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:40.0	302014	10.10.100.16		443			10.1
10.10.18.2	10.10.18.2	2010-06-10 16:38:40.0	302014	10.10.100.16		443			10.1

Maintaining RSA enVision

RSA enVision Event Source Update provides you with updates to event source content outside the normal enVision product release cycle. Each monthly update package contains multiple patches that contain the latest event sources (new event sources and changes to existing event sources) supported by enVision. Every new or updated event source in the package has its own patch.

The Event Source Update package also includes a recent VAM & Signature Content Update. If you install the VAM updates regularly, the versions of some VAM sources included with the Event Source Update may be older than ones already on your system. If so, the Event Source Update will *not* overwrite your newer files.

Packages are not linked to a particular enVision version so you can run an update patch if you have enVision version 3.5.1 or higher. The current package is cumulative containing patches for all new or changed event source XML since 3.5.1.

Tech Tip

To use the correlation rules in the package, you must be running version 3.7.0 or higher. Additionally, some versions of supported event sources require enVision versions newer than 3.5.1.

You can rollback the installation of the package to its pre-update state if necessary. Please contact RSA Customer Support for guidance before you attempt this procedure.

Common Troubleshooting Tips

You can monitor the system health of enVision using the system health features to:

- Report on usage patterns in enVision: The NIC view, **NIC_View**, allows you to monitor the system health - alerting you of possible issues within the enVision software environment.
- Track configuration changes in enVision using Audit Reports: The following standard system reports for the system auditing function are included

Configuration Changes by Action: Lists all the configuration changes with the specified

Configuration Changes by Date/Time: Lists all configuration changes made to the enVision system.

Configuration Changes by Object Type: Lists all configuration changes made against the specified object

Configuration Changes by User: Lists all configuration changes made by the specified user.

User Session Activity by Date/Time: Lists all the successful and failed log in/log out attempts to enVision.

User Session Activity by User: Lists all the successful and failed log in/log out attempts to enVision the specified user.

Handling an Incident on RSA enVision

An incident is an event or set of events that warrants further investigation, such as a disk failure, an unexpected spike in network traffic, or the signature of a known threat. Because of the wealth of data that the RSA enVision platform automatically collects, it can be configured to recognize incidents and issue real-time alerts. The alert is the beginning of the enVision incident-management process.

RSA enVision provides for closed-loop incident management, from configuring alerts, through creating and assigning response tasks, to monitoring incident response and resolution.

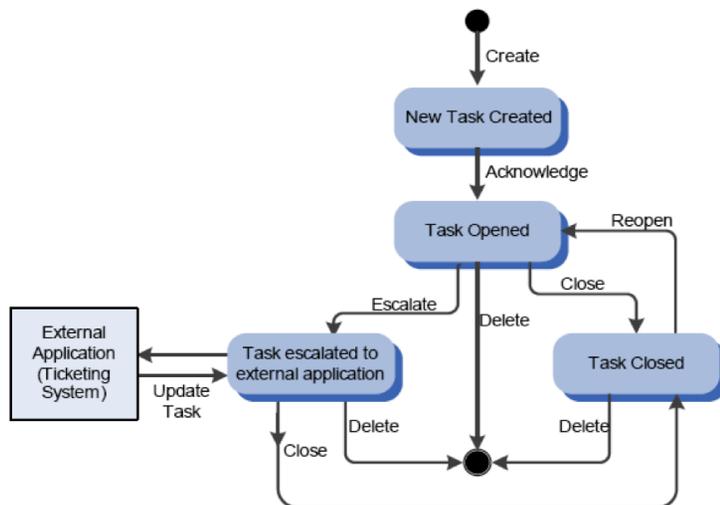
Real-Time Alerts

RSA enVision generates real-time alerts in response to sets of circumstances that the administrator has specified. RSA enVision analyzes all incoming events, and issues an alert immediately when the specified conditions are met. The alert is reported in the enVision GUI and can be directed to other destinations, such as email, instant message, or a text file stored on the local system. An alert can also be configured to automatically generate an incident-response task.

Incident-Response Tasks

RSA enVision can group events into tasks for the purpose of investigation, and assign the tasks to analysts (or to an intermediate dispatcher) for response. Analysts display and work with the tasks in RSA enVision Event Explorer. Managers and administrators can monitor the analysts' progress in the enVision GUI.

Figure 10. Incident Handling Workflow



Monitoring Alerts by Creating Tasks

In enVision, the administrator can specify the creation of a task based on a correlated alert. When the alert fires, enVision creates the task and sends it to Event Explorer for resolution or to an external application, such as a third-party ticketing system.

Managing Tasks in RSA enVision Event Explorer

When enVision forwards tasks to Event Explorer, Event Explorer displays a list of tasks and the details of individual tasks.

Depending on the Event Explorer user's permissions (as set by the enVision administrator), the user assigned to a task can acknowledge the task, view and edit task data, assign the task to another analyst, and close or delete the task. The user can also escalate the task to an external application, such as a ticketing system. The external application can update tasks and send the updates back to Event Explorer.

Multiple users can access the same task from different Event Explorer clients. Event Explorer displays a warning message if different users attempt to make conflicting changes to the task.



Tech Tip

If you used the 30-day trial version of enVision for setting up your network, be sure to convert it to full a license before the end of the 30-day evaluation period. All settings will be maintained in the conversion from the 30-day trail to the full license.

Products Verified with Cisco SBA

RSA enVision 4.0 has been verified with Cisco SBA using the following software versions:

- Cisco ASA 5500 Series 8.2(1)
- Cisco IOS Software Release 15.0(1)M2
- Cisco IOS XE Release 2.6.1
- Cisco Intrusion Prevention System 7.0.(2)E3
- Cisco IronPort AsyncOS Version 7.1 for Email
- Cisco IronPort AsyncOS Version 6.3 for Web
- Cisco Security MARS 6.0.5.

How to Contact Us

End Users

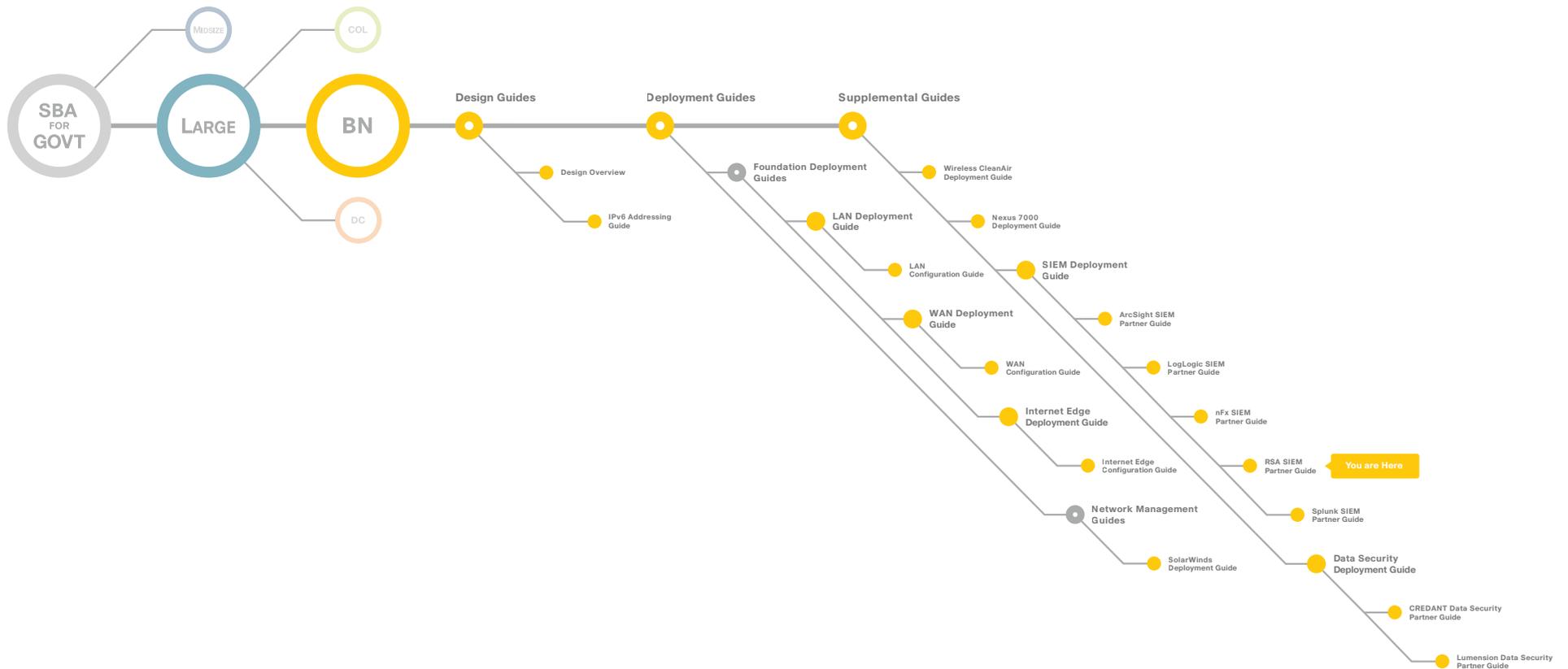
- Please contact RSA, The Security Division of EMC, via <https://www.rsa.com/go/contactsales.asp> for any questions
- [Submit an inquiry](#) about enVision and the Cisco SBA for Large Agencies—Borderless Networks

Resellers

- Please contact RSA, The Security Division of EMC, via <https://www.rsa.com/go/contactsales.asp> for any questions
- For more information on how to become a RSA reseller, please visit the Partner Section of RSA's website

For more information on the RSA and Cisco Partnership, please visit <http://www.cisco.com/go/securitypartners>.

Appendix A: SBA for Large Agencies Document System





SMART BUSINESS ARCHITECTURE



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-641099-00 02/11