nFX Cinxi One SIEM Partner Guide

netForensics®

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

This document is for the reader who:

- Has read the *Cisco Security Information and Event Management Deployment Guide* and the *Internet Edge Deployment Guide*
- Wants to connect Borderless Networks to a nFX Cinxi One SIEM solution
- Wants to gain a general understanding of the nFX Cinxi One 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

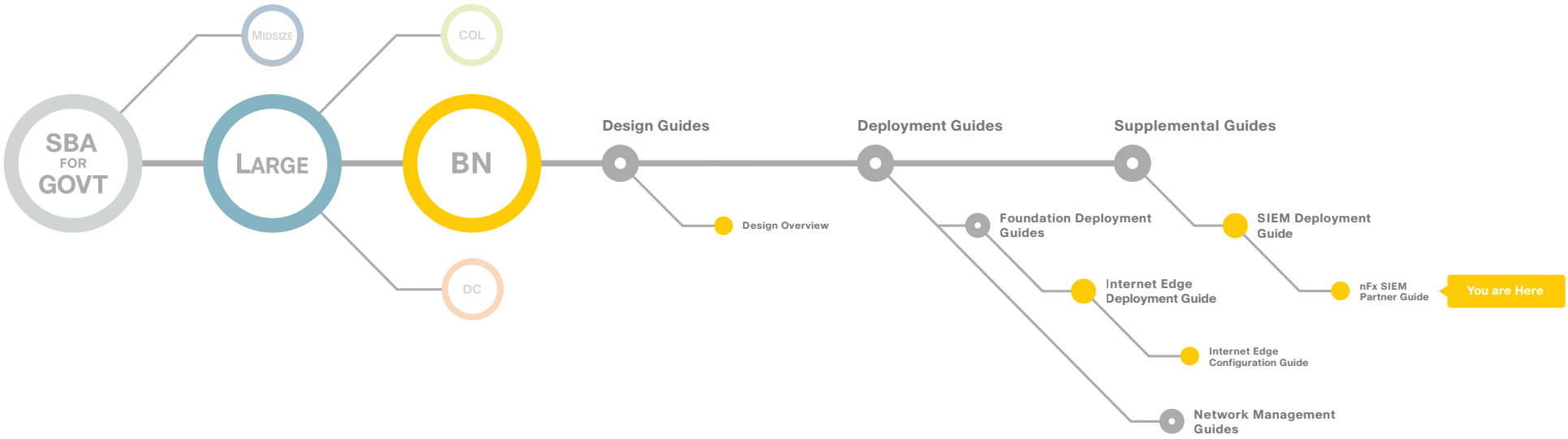


Table of Contents

Introduction

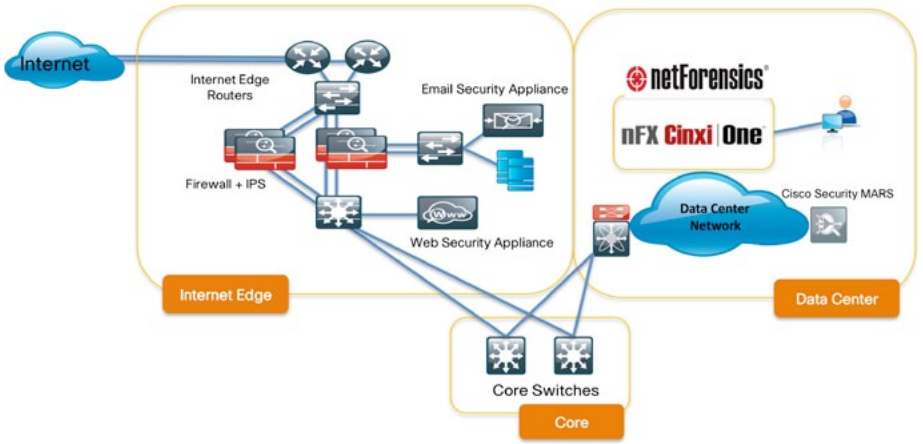
Cisco SBA for Large Agencies—Borderless Networks

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. It 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 Information and Event Management (SIEM) capabilities. This guide is focused on our partnership with netForensics and their nFX Cinxi One product.

Figure 1. nFX Cinxi One Integrated into SBA for Large Agencies—Borderless Networks



Agency Benefits

netForensics helps protect data and maintain compliance, delivering actionable security intelligence to companies worldwide through:

- Security information and event management
- Log management and threat visibility
- Compliance automation and audit readiness
- Solutions for managed security providers

netForensics products seamlessly integrate with Cisco security and networking products, as well as a broad array of multi-vendor technologies. Working with Cisco, netForensics provides agencies with technologies that enable real-time security visibility, rapid threat response, and compliance with complex regulatory mandates.

When agencies deploy netForensics solutions in a Cisco network environment, they get a clear view of their network through in-depth analysis of security events. Through rules-based correlation techniques, nFX Cinxi One can identify security events that would go undetected or be lost in the large volume of data generated by various security devices. nFX Cinxi One collects event data from a wide range of Cisco network and security devices such as routers, firewalls, and intrusion detection systems (IDS). Data from these devices is automatically correlated based on definable rule sets. The nFX solutions uncover similar attacks against different devices or device types. They also identify individual events that alone are harmless, but when combined with other actions in succession suggest an attempted attack.

nFX Cinxi One compiles this information and presents it through a series of dashboards, views, and historical reports. With netForensics solutions, Cisco customers can depend on accurate, comprehensive security information using a single, unified view across all network systems, security devices, and applications. With this critical information, you can understand the complete profile of an attack, open a case to resolve the vulnerability, and track the results of the remediation actions to confirm the issue is resolved.

The integration of netForensics SIEM products and Cisco technologies makes the task of identifying uncommon, subtle, and related events among vast amounts of data achievable.

Notes

Product Overview

The nFX One family includes nFX Cinxi One, an appliance, and nFX SIM One, a software solution. The nFX One family offers advanced solutions for real-time monitoring, event correlation, threat management, and reporting. netForensics helps agencies of all types and sizes meet the most demanding data protection and compliance challenges. With netForensics, you can protect critical data, manage log overload, and ensure audit readiness—regardless of budget, size, and performance requirements. nFX One solutions collect, centralize, and store volumes of diverse data, and deliver understandable, actionable security intelligence. Agencies can easily see the most important security information. This prioritized insight dramatically improves the ability to identify and rapidly respond to the true threats.

nFX Cinxi One appliances offer a low-cost, easy to-use solution for managing the vast amount of security-related data that inundates your agency every day. Cinxi combines log management, real-time event correlation and alerting, remediation, and reporting in a single high-performance solution. It simplifies the time-consuming task of monitoring and managing the compliance and security risks that can affect your agency's operations. The Cinxi line of appliances offers cost-effective yet advanced SIEM solutions with high events per second (EPS) performance, great flexibility, highly available live data storage, and the low total cost of ownership, thanks to netForensics' simple pricing models and the low overhead required to install and maintain the platform.

nFX Cinxi One can be deployed in as little as one hour. nFX Cinxi One:

- Gathers comprehensive data across the spectrum, including real time events and log files, data from applications, file systems, firewalls, scanners, and so on.
- Includes built-in support for over 1000 devices and applications plus an easy device integration tool.
- Correlates and identifies security incidents automatically using powerful MetaRules.
- Includes reporting packs for major regulatory compliance standards: PCI, SOX, HIPAA, GLBA, ISO 27001.
- Provides workflow management with built-in remediation recommendations.

Getting Started with the nFX Cinxi One Interface

The nFX Cinxi One screen consists of two sections: the left with four windows and the right controlled by the main tabs. The **Home tab** includes four sections, each of which can be resized or closed.

- The left section contains four small panes: **Top 10 Incidents, Top 10 Assets, Message/Incident Activity** and **Server Information.**
- The right section is controlled by seven tabs at the top: **Home, Incidents, Cases, Assets, Rules, Reports** and **Administration.** Note that the Administration tab is not visible to users defined with an Analyst role.
  - Unique among the tabs, the Home tab is composed of four separate panes, any of which can be resized or maximized to fill the whole right section of the screen: **Incidents, Topology, Threat Summary,** and **Open Incidents by Rule.**
  - The Home tab also allows using the **Home > New Pane** menu item to launch either an **Assets** pane or a **Case Summary** pane, or both, in the right section of the screen.
  - Default settings for the Home tab can be restored from **Home > Arrange > Default Layout.**

Figure 2. The nFX Cinxi One Interface

Table 1. nFX Cinxi One Performance Overview

	nFX Cinxi One
Number of Administrative Users	6
Events Per Second	115,000 eps
Event Data Formats	Cisco IOS: syslog Cisco ASA 5500 Series: syslog Cisco IPS 4200 Series: Security Device Event Exchange (SDEE) Cisco IronPort Email Security Appliance: Log via FTP Cisco IronPort Web Security Appliance: Log via FTP Cisco Security MARS: Archive via SFTP

Deploying nFX Cinxi One in a Cisco Network

The following sections discuss in more detail how to perform the following tasks on your nFX Cinxi One appliance:

- Add Cisco devices as log sources
- Run reports
- Perform maintenance updates
- Troubleshoot problems
- Conduct a typical incident response

Tech Tip

- This guide assumes that your nFX Cinxi One appliance is already installed and configured. Please refer to your NetForensics documentation for details.

Process

Adding Cisco devices in nFX Cinxi One to receive logs

This section shows the steps required to add several types of Cisco network devices to Cinxi One, in order to allow you to define rules, create incident records, generate reports, and track cases for remediation. This guide discusses the following specific Cisco products:

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco IronPort Email Security Appliance
- Cisco IronPort Web Security Appliance
- Cisco Security MARS
- Cisco Integrated Service Router (ISR)
- Cisco IPS 4200 Series Sensor

Procedure 1 Adding a Cisco ASA 5500 to nFX Cinxi One

The Cisco ASA 5500 Series Adaptive Security Appliance can be configured to forward syslog messages to nFX Cinxi One over UDP port 514 or TCP port 1468 without any special agents or applications. Logging at the desired level must be enabled on the Adaptive Security Appliance. Refer to the **Cisco Security Information and Event Management Deployment Guide** for details.

To configure nFX Cinxi One to receive syslog messages from a Cisco ASA 5500:

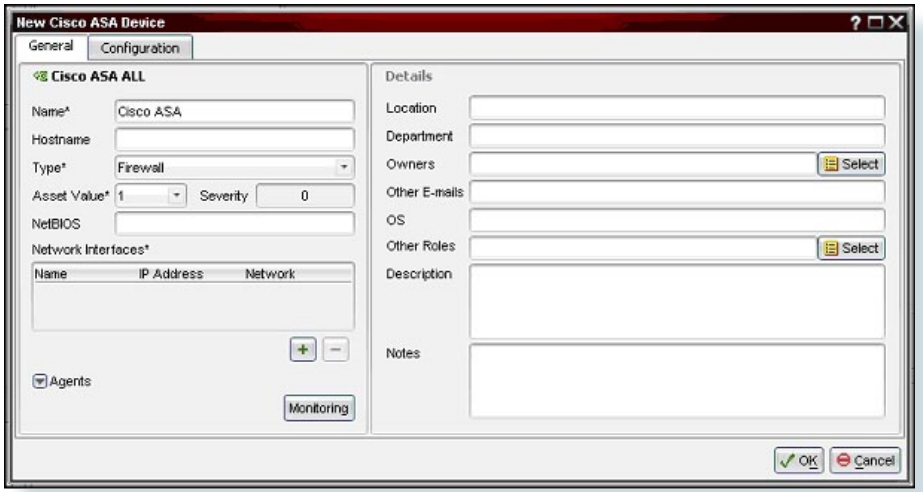
Step 1: In the nFX Cinxi One client, select the **Assets** tab.

Step 2: Click **New**, then select **New Device** to display the **Select Product** popup.

Step 3: Select **Cisco > ASA > All** and click **OK**.

Step 4: Click the "+" sign below the **Network Interfaces** pane in the **New Cisco ASA Device** popup, illustrated in Figure 3.

Figure 3. The New Cisco ASA Device Window



Step 5: Enter the IP address of the adaptive security appliance in the popup, as shown in Figure 4, and click OK.

Figure 4. New Network Interface Configuration

Step 6: In the **New Cisco ASA Device** window, select the **Asset Value** dropdown, and then choose an appropriate value for the device, where 10 is most important. The value entered here is used in calculating the severity level of incidents reported by the device.

Step 7: Populate the other fields as required to facilitate notifying appropriate personnel and categorizing reported incidents according to the agency's needs. The **Owners** field can be used in conjunction with the **Notify Asset Owners** checkbox when setting up notifications in the **Incidents tab.**

Step 8: Click **OK**.

Procedure 2 Adding a Cisco ESA or WSA to nFX Cinxi One

A Cisco Ironport Email Security Appliance or Web Security Appliance can be configured to periodically export log files to an external host. For nFX Cinxi One, the recommended option is to configure the appliance to use the File Transfer Protocol (FTP) to send the log files directly to the Cinxi One appliance. Please refer to the Cisco Security Information and Event Management Deployment Guide for details on the configuration process. The following steps show how to configure nFX Cinxi One to import these log files:

Step 1: Connect to the Cinxi One appliance via SSH using the htadmin account.

Step 2: Enter the htadmin password.

Step 3: Enter **1** for Configure Appliance, enter **2** for Individual Settings Configuration Menu, enter **6** for Message Collection Parameters Menu, and then enter **3** for Enable Incoming FTP Dropbox.

Step 4: Enter **99** for Return to Individual Settings Configuration Menu.

Step 5: Enter **99** for Return to Configure Appliance, enter **6** for Apply Changes, press **Y** to confirm, and then enter **99** for Return to Main Menu.

Step 6 (optional): In the Main Menu, enter **2** for the Password Management Menu, and enter **3** for Set FTP Password. After you have set the new password, enter **99** for Return to Main Menu.

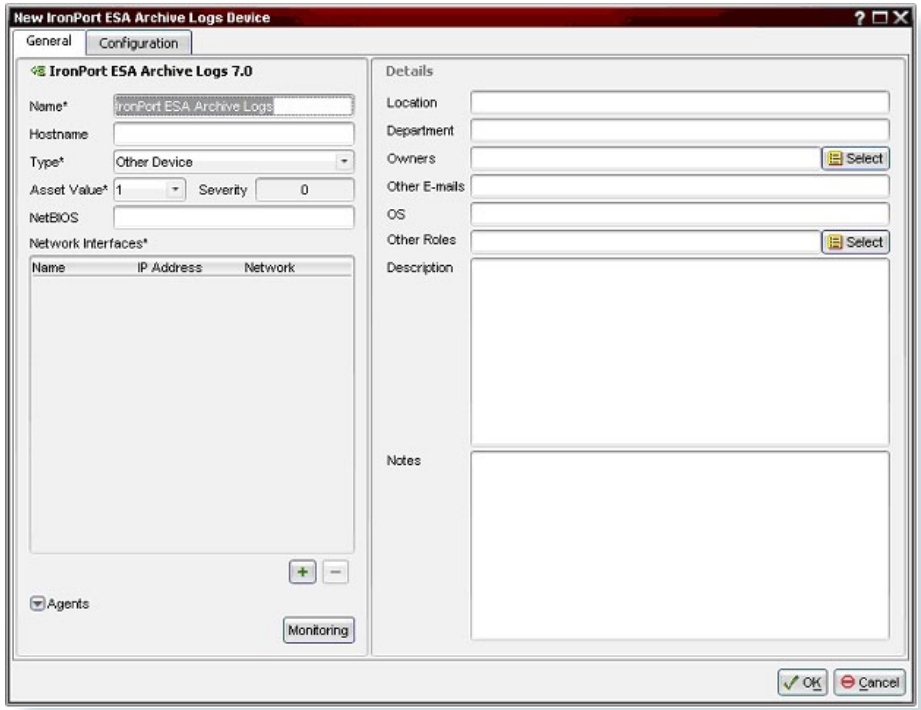
Step 7: Enter **10** for Exit.

Step 8: Launch the nFX Cinxi One client and log in.

Step 9: Select the **Assets** tab, click **New**, and then click **New Device**. The Select Product popup appears.

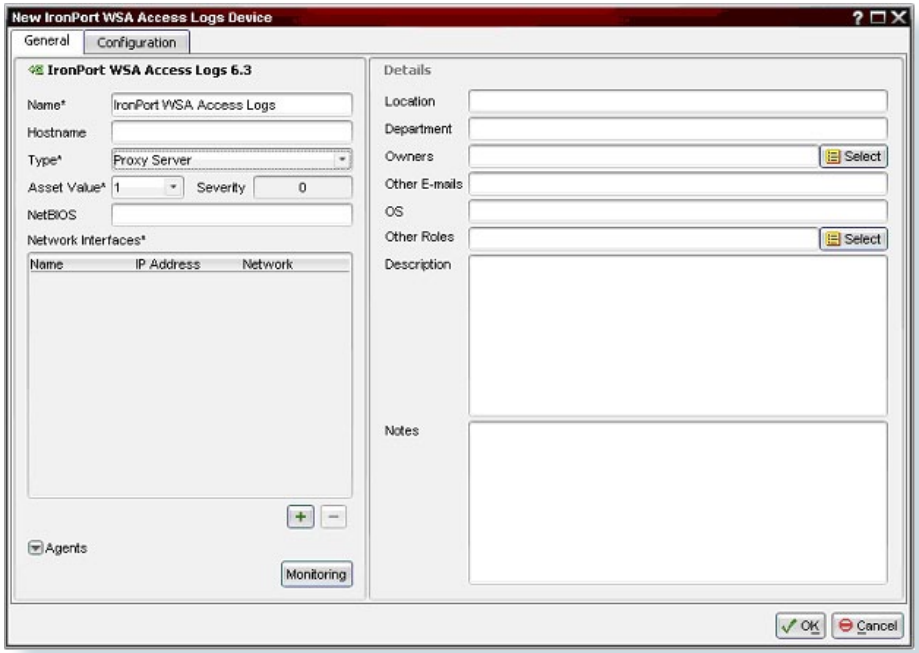
Step 10: For a Cisco IronPort Email Security Appliance, double-click **IronPort**, click **ESA Archive Logs**, click **7.0**, and then click **OK**. The **New IronPort ESA Archive Logs Device** popup appears, shown in Figure 5.

Figure 5. New IronPort ESA Archive Logs Device Window



For a Cisco IronPort Web Security Appliance, double-click **IronPort**, click **WSA Archive Logs**, click **6.3**, and then click **OK**. The **New IronPort WSA Access Logs Device** popup appears, shown in Figure 6.

Figure 6. New IronPort WSA Access Logs Device



Step 11: Under Network Interfaces, click on the plus (+) button.

Step 12: Enter the IP address in the popup and click **OK**.

Figure 7. New Network Interface Configuration

Step 13: In the **New IronPort WSA Access Logs Device** window, select the **Asset Value** dropdown and then an appropriate value for the device, where 10 is the most important. The value entered here is used in calculating the severity level of incidents reported by the device.

Step 14: Populate the other fields as required to facilitate notifying appropriate personnel and categorizing reported incidents according to the agency's needs. The **Owners** field can be used in conjunction with the **Notify Asset Owners** checkbox when setting up notifications in the **Incidents** tab.

Step 15: Click **OK**.

Procedure 3 Adding Cisco Security MARS to nFX Cinxi One

Cisco Security MARS can send archives of raw messages and other appliance logs to a remote location using either the Network File System (NFS) or Secure FTP (SFTP) protocols. nFX Cinxi currently supports only raw messages archive files. Please refer to the Cisco Security Information and Event Management Deployment Guide for details on how to configure Cisco Security MARS archives. The following steps show how to configure Cinxi One to import the archived messages from an external server using FTP.

Tech Tip

Cisco Security MARS can use either NFS or SFTP to upload the archives to the external server, but Cinxi One uses only unencrypted, passive mode FTP to download them.

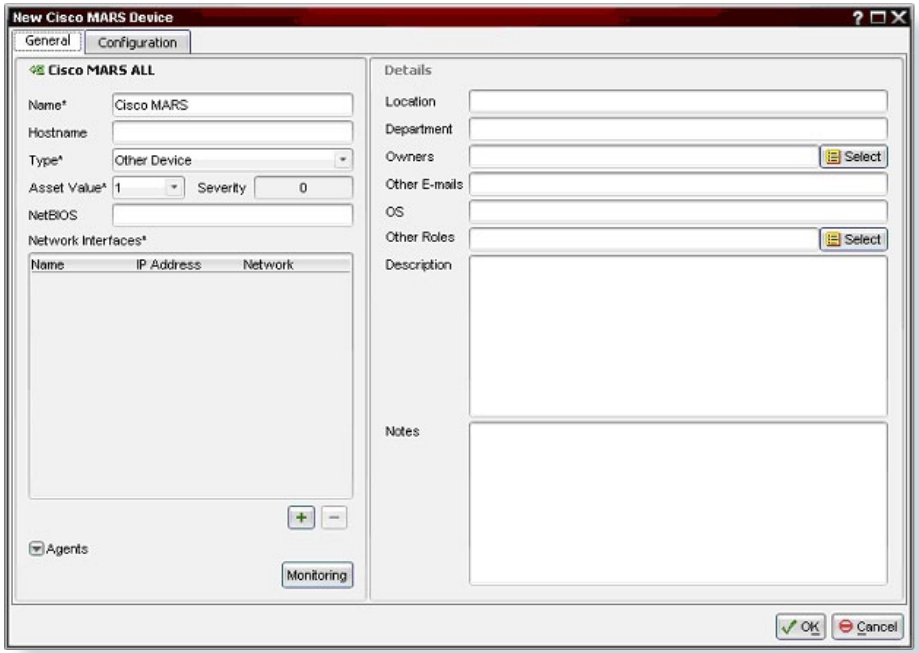
Step 1: In the nFX Cinxi One client, select the **Assets** tab.

Step 2: Click **New** and then select **New Device**. The **Select Product** popup appears.

Step 3: Select **Cisco > MARS > All** and click **OK**. The **New Cisco MARS Device** popup appears, shown in Figure 8.

Step 4: Under Network Interfaces, click the plus (+) button.

Figure 8. The New Cisco MARS Device Window



Step 5: In the **New Network Interface** pop-up, enter the IP address of the FTP server on which the archives reside, and click **OK**.

Step 6: In the **New Cisco MARS Device** window, select the **Asset Value** dropdown and then select an appropriate value for the device, where 10 is the most important. The value entered here is used in calculating the severity level of incidents reported by the device.

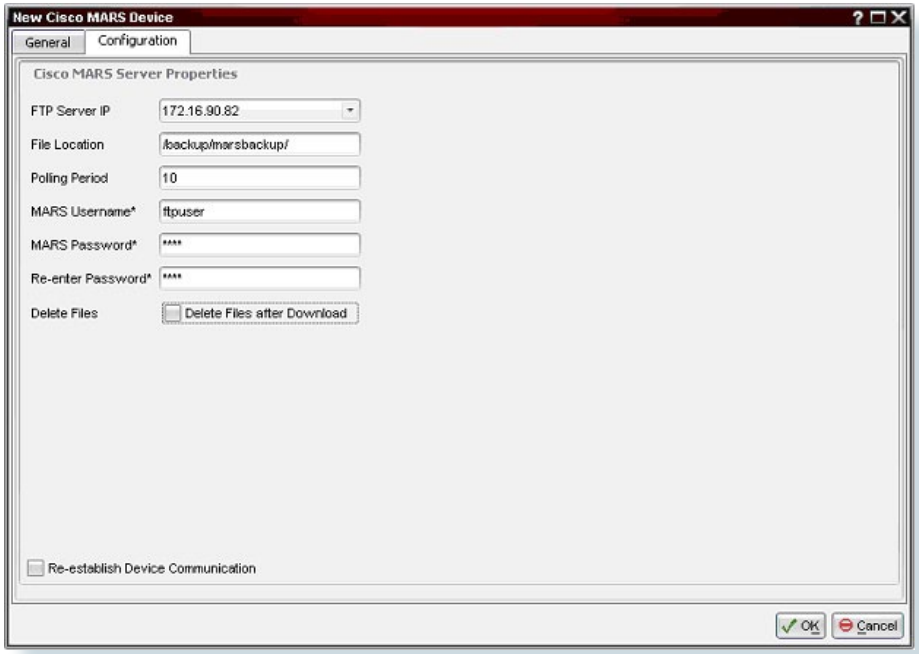
Step 7: Populate the other fields as required to facilitate notifying appropriate personnel and categorizing reported Incidents according to the agency's needs. You can use the **Owners** field in conjunction with the **Notify Asset Owners** checkbox when setting up notifications in the incidents tab.

Step 8: Select the **Configuration** tab and fill out following information about the FTP server as shown in Figure 9:

- File Location: Type the file path to the archives on the server.
- Polling Period: Type how frequently nFX Cinxi One should poll the FTP server for new files. This period is in minutes.
- MARS Username: Type the FTP username that will be used to download the archives.
- MARS Password: Type the password for the above user.
- Delete Files: If this option is checked, nFX Cinxi One deletes the archive files from the remote server after a successful download. Confirm that the FTP user has the right to delete files on the remote server.

Step 9: Click **OK**.

Figure 9. FTP Configuration for Archive Retrieval



Interpretation of Cisco Security MARS Raw Messages Archive Logs

Cisco Security MARS raw messages archive logs contain the raw messages exactly as they were received by Cisco Security MARS from the end security devices. When nFX Cinxi One retrieves raw messages archive logs, it internally processes them as if they were individual alerts coming from the end security devices. Each raw message in the raw messages archive log file contains four fields:

- Event ID
- Receiving time
- Reporting Device Name
- <length>@<raw message data>

Tech Tip

Currently, Cinxi One only supports syslog messages from Cisco ASA and Cisco IOS devices, and SDEE events from Cisco IPS sensors through this Cisco Security MARS raw messages archive export mechanism.

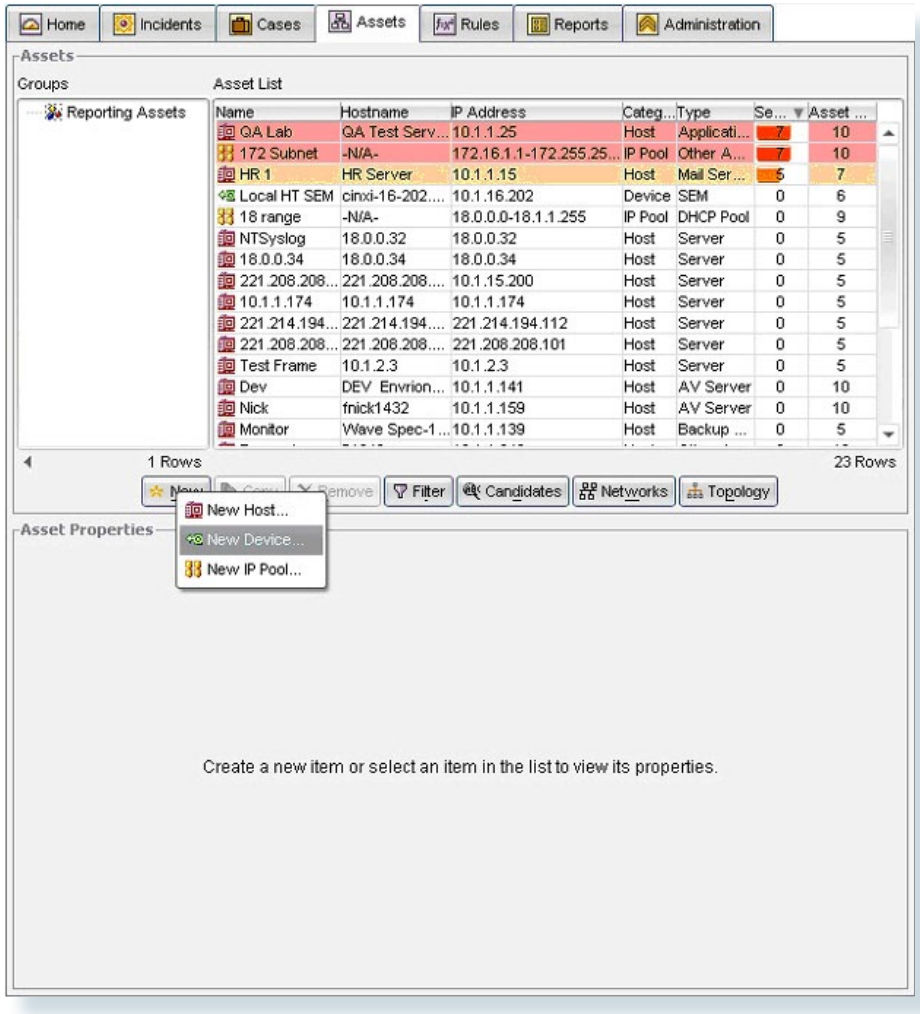
Procedure 4 Adding Cisco ISRs to nFX Cinxi One

Cisco Integrated Services Routers (ISRs) send syslog messages to nFX Cinxi One on UDP port 514. There is no agent needed on Cisco IOS or the nFX Cinxi One SIEM.

Step 1: In the nFX Cinxi One client, select the **Assets** tab.

Step 2: Click **New** and then select **New Device**. The Select Product popup appears.

Figure 10. The Assets Tab

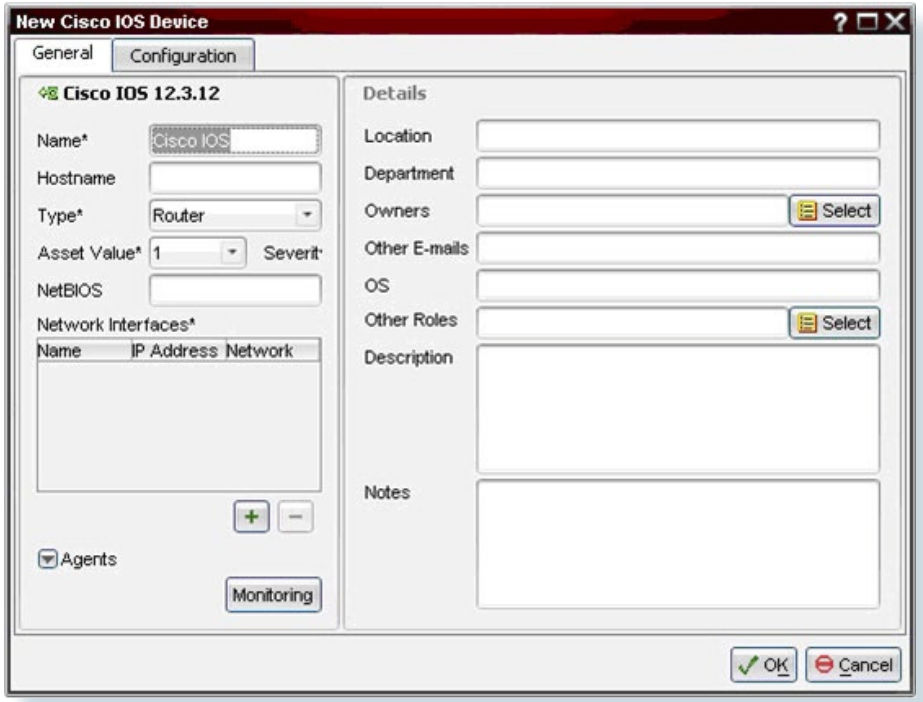


Step 3: Select Cisco > IOS, select the appropriate software version, and then click OK. The New Cisco IOS Device popup appears.

Step 4: Under Network Interfaces, click the plus (+) button.

Step 5: Enter the following information: name, hostname, type, asset value and IP address.

Figure 11. The New Cisco IOS Device Window



Step 6: Click OK.

Procedure 5 Adding Cisco IPS Sensors to nFX Cinxi One

The nFX Cinxi One SIEM has an agent that can connect via HTTPS to Cisco IPS sensors using SDEE and download XML-formatted event logs containing the alerts that were monitored on the network; these alerts can trigger specific rules on nFX Cinxi One.

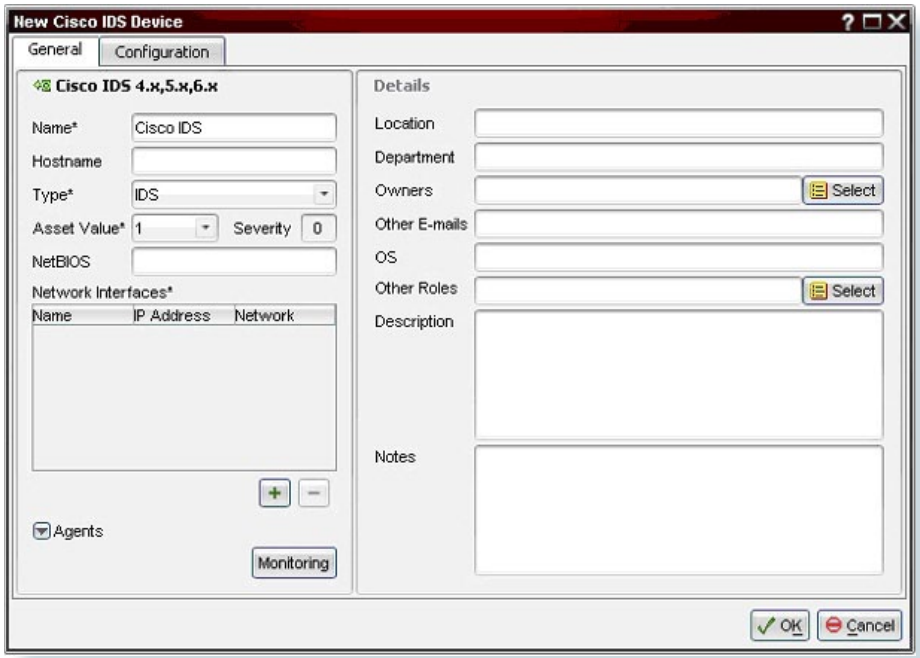
Step 1: In the nFX Cinxi One client, select the **Assets** tab.

Step 2: Click **New**, then select **New Device**. The Select Product popup appears.

Step 3: Select **Cisco > IPS**, select the appropriate software version, and then click **OK**. The New Cisco IPS Device popup appears.

Step 4: Under Network Interfaces, click the plus (+) button.

Figure 12. The New Cisco IPS Device Window



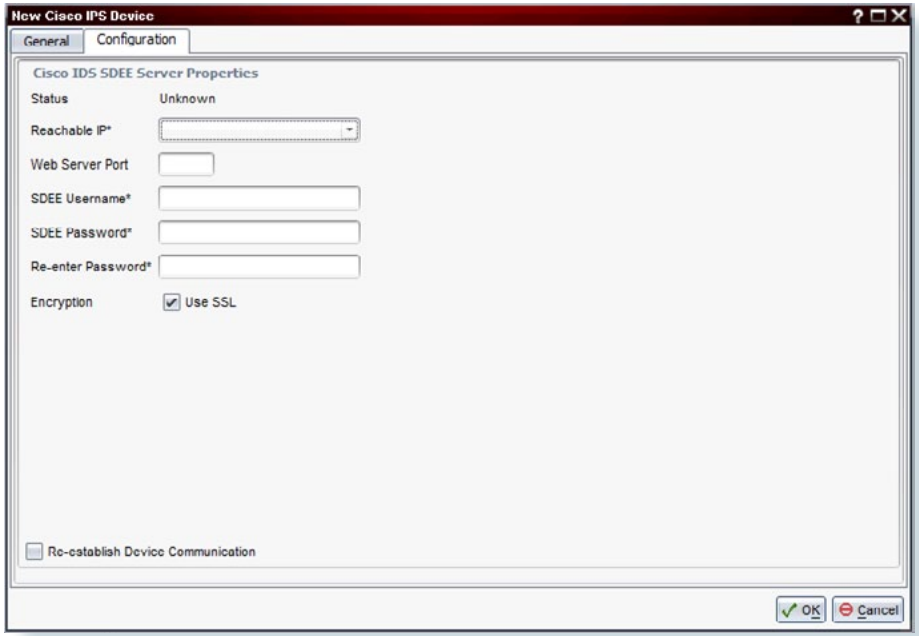
Step 5: Enter the following information: name, hostname, type, asset value and IP address.

Step 6: Select the **Configuration** tab and fill out the information for the IDS agent.

- Enter in the IP address of the IPS in the **Reachable IP** field
- Enter 443 in the **Web Server Port** field
- In the **SDEE Username** and **SDEE Password** fields, enter the credentials of a user on the IPS that will be used to retrieve the event logs
- Confirm the password in the **Re-enter the Password** field
- Next to **Encryption**, select the **Use SSL** checkbox

Step 7: Click **OK**.

Figure 13. The Configuration Tab of the New Cisco IPS Device Window



Process

Reporting on nFX Cinxi One

Reports are easy to create in nFX Cinxi One. nFX Cinxi One's Reports tab provides 138 reports in nine categories as noted below. nFX Cinxi One can generate reports in .rpt or .csv format, as well as customized by time period, IP address range, audit category, and maximum number of messages. You can schedule report generation and can configure user notifications for report generation.

You can generate any report on the fly by selecting it and setting its report criteria. The criteria available vary with the report. For example, device IP is not a criterion for the User Workload report. Source and destination IP and port are not criteria for the Events by Category report but are criteria for the Event Report.

Figure 14. Cinxi One Report of Device Activity

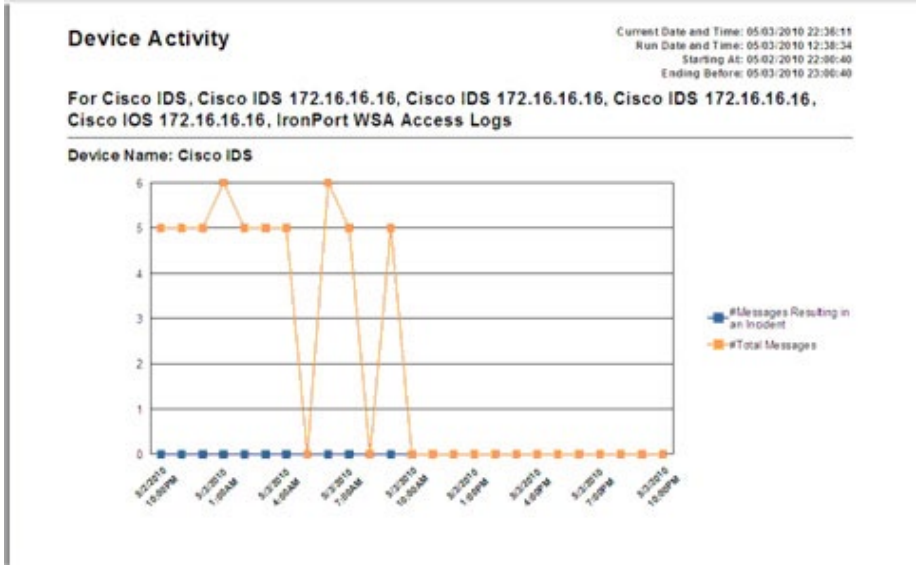
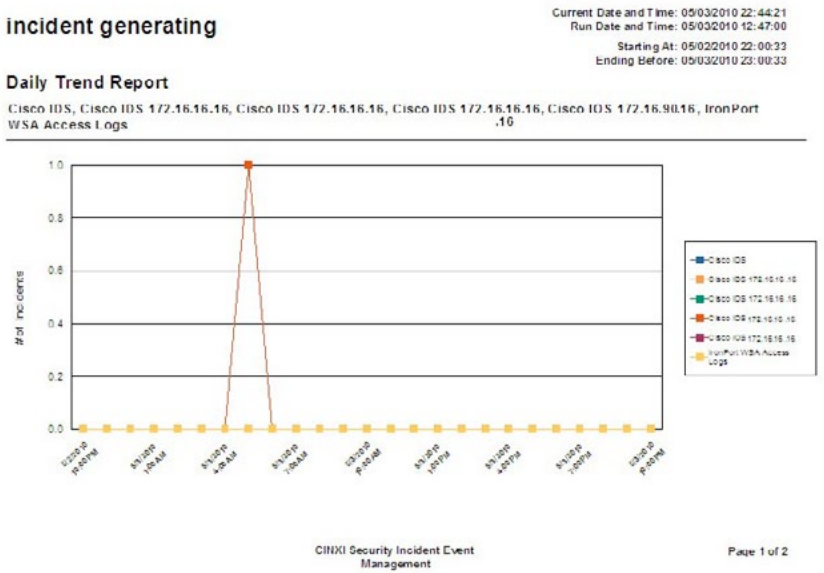


Figure 15. Cinxi One Report of Incident Trends



Process

Updating nFX Cinxi One

nFX Cinxi One allows users to choose when to look for updates, which updates to download, and when to install them. When users with admin rights log into the appliance, Cinxi One asks them if they want to look for updates. If the user chooses to do so, Cinxi One displays the available updates to the user so the user can choose what to download and install. Users control updates at all times. As an added plus, there is no need to reboot the appliance. Users might be asked to logout and log back in, depending on the type of update.

Figure 16. Prompting for Updates

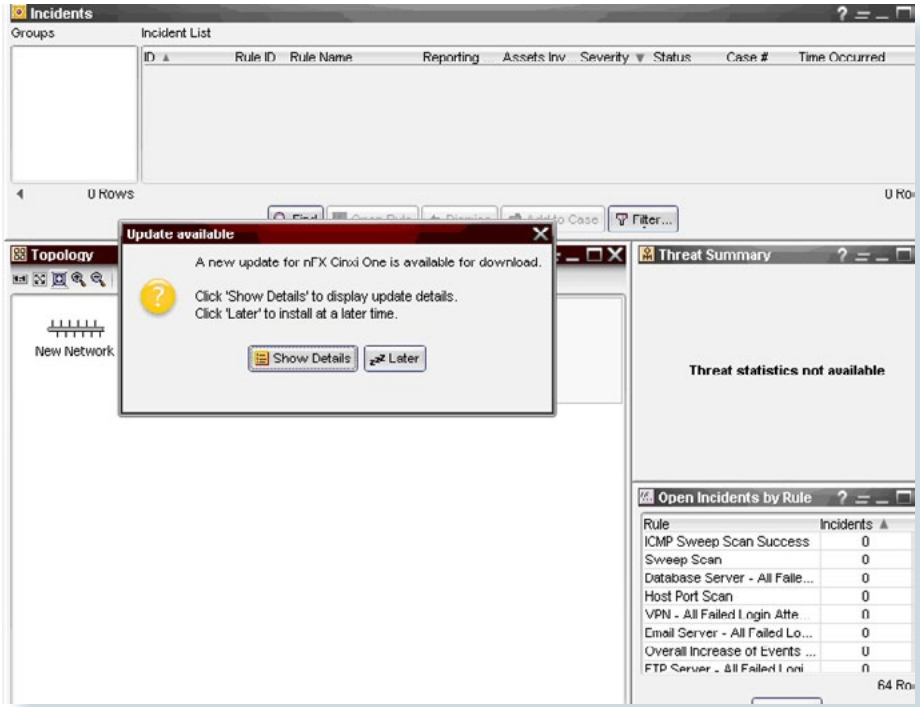
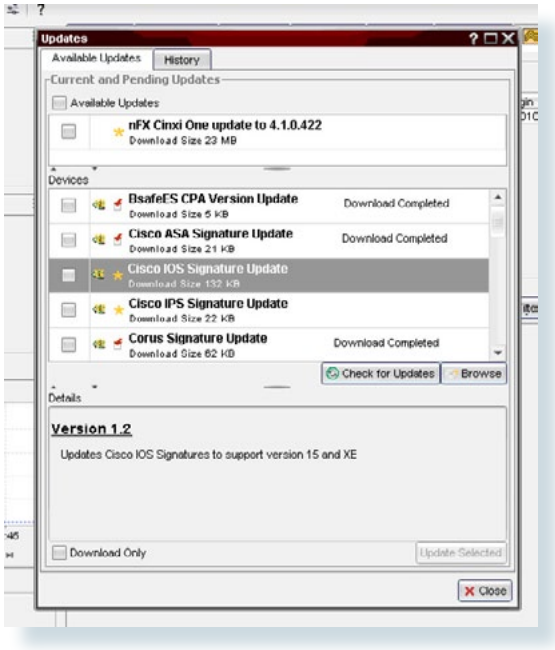


Figure 17. Selecting Updates to Install



Common Troubleshooting Tips

Q: What do I do if I notice I am not receiving any logs some of the time?

A: Steps for troubleshooting messages:

1. Use **Tools > Monitor** to see raw messages. Verify that Cinxi One is receiving messages from the device.
2. Make sure that the asset is set up as a device, and that Cinxi One supports that version.
3. Use **Reports > Message Search Reports > Event Report** and verify that you can find a specific message from step 1 using this report.
4. In **Reports > Message Search Reports > Events by Category,** verify that the device messages are getting categorized and that the message from step 3 appears in this report.

Q: Some events started to appear on the device, but no incidents were created because of those messages, even though there are rules that should trigger an incident. What do I do?

A: The message flow is: Device => Raw messages => Messages/Events => Events/Category => Category/Rules. Rules fire based on the monitored category in the Rule Configuration tab. Using the above troubleshooting steps, does this rule include the event category? Do the events coming in match the rule parameters (quantity, time)?

Q: Is it possible I am not receiving messages because the disk is full?

A: To see if this is causing the problem, check disk usage from the Console in the lower left corner: **Server Information > Disk.**

Handling an Incident on nFX Cinxi One

nFX Cinxi One helps agencies detect network issues like zero-day attacks or malware infection.

For example, suppose that the Cinxi One correlation engine detects an outbreak either by seeing antivirus or IPS alarms from one or more downstream devices, or by using its own detection (for example, seeing traffic on ports known to be used by Trojans and other malware). When this occurs, an incident or incidents are generated by the correlation engine and appear on the nFX Cinxi One Home Tab and Incidents Tab, among other places.

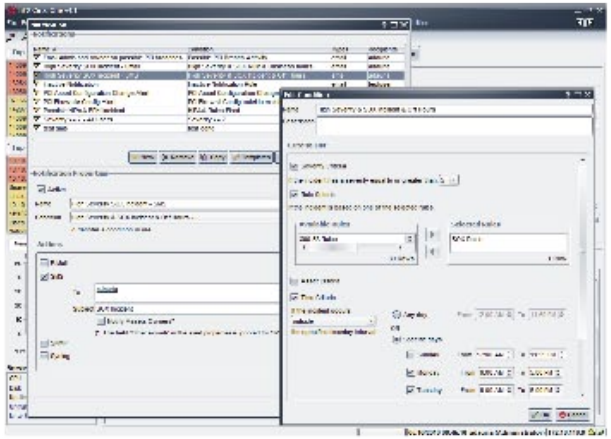
nFX Cinxi One can send out alerts so that users can immediately know if there is an issue. Analysts would determine what incidents would warrant an alert such as high severity incidents involving key servers and/or malware rules.

Additionally, the alert interface includes high level overview, incident details, and views of the parsed/normalized events that triggered the incident, as well as the raw messages from these events. Each incident also includes guidance about the rule and appropriate first and second level responses. These responses are included for all out-of-box rules. Analyst response includes determining what is happening, stopping it from continuing, and then investigating and remediating the root cause.

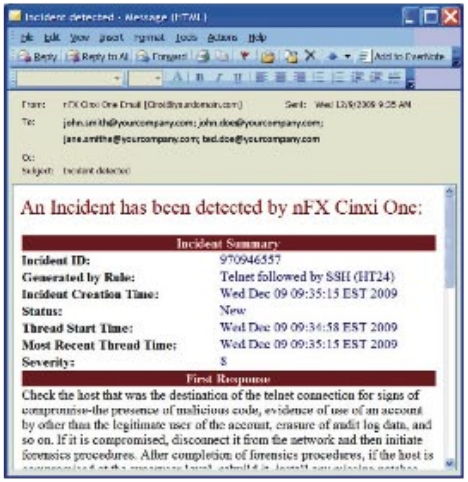
The entire process can be managed in the Cases facility of Cinxi One.

Flow for Incident Handling of Malware

Configuration: User has the ability to configure the notification alert conditions

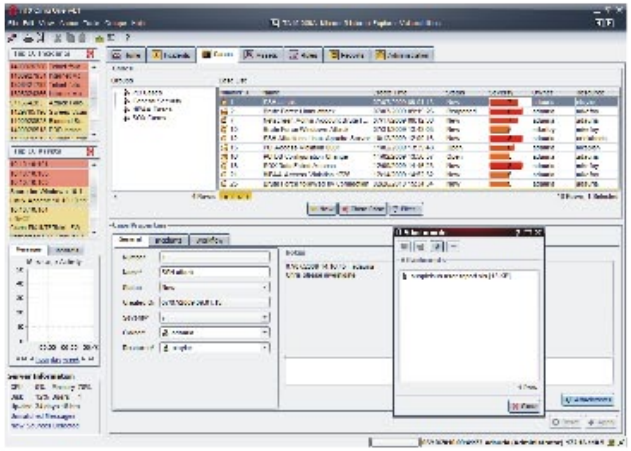


Notification when outbreak detected: Sample incident notification via email



Incident General View with response suggestions

Case Management View with report attached



Products Verified with Cisco SBA

nFx Cinxi One v4.1 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 info@netForensics.com or any questions
- Submit an inquiry about nFX Cinxi One and the Cisco SBA for Large Agencies—Borderless Networks

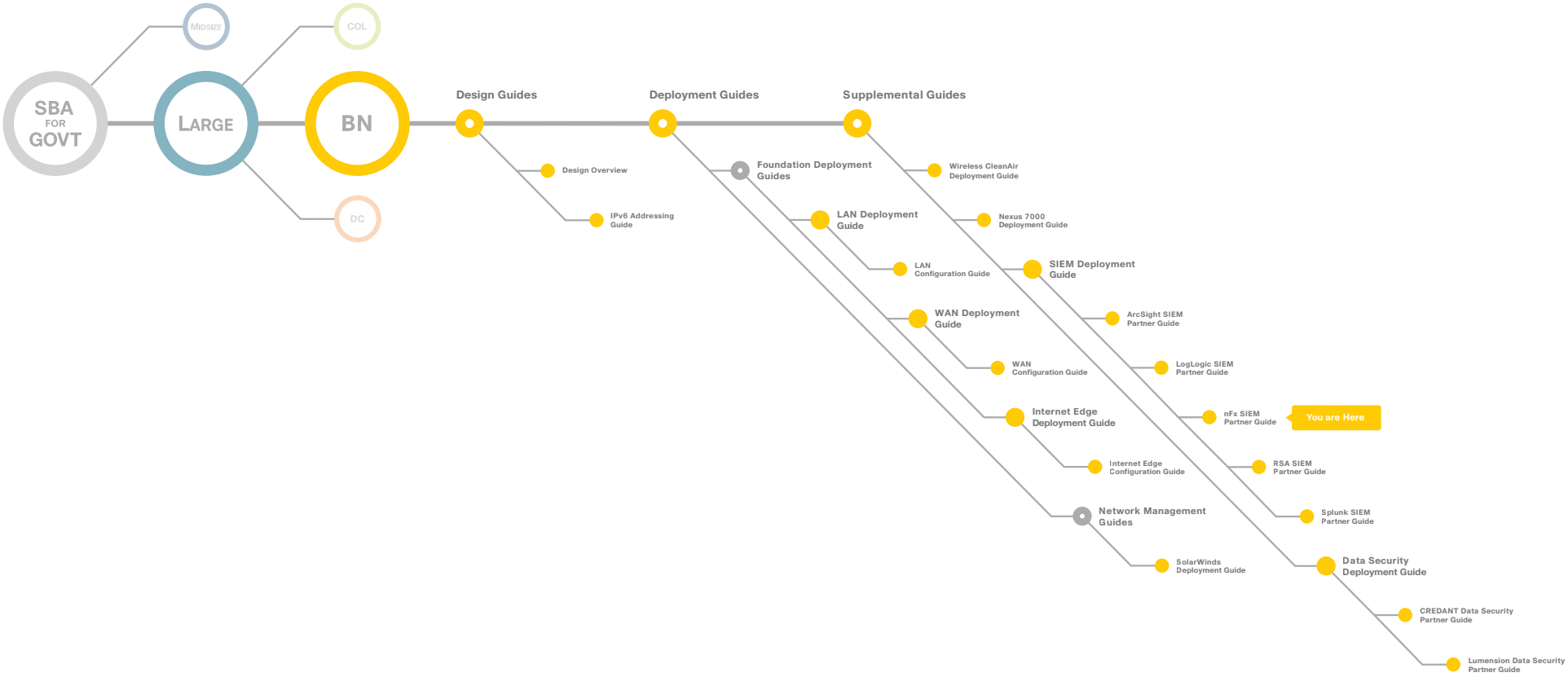
Resellers

- Please contact partners@netForensics.com for any questions
- For more information on how to become a nFx reseller, please visit the Partner Section of our website at http://www.netforensics.com/partners/

For more information on the nFx and Cisco Partnership, please visit the Cisco Resource Center.

Notes

Appendix A:
SBA for Large Agencies Document System



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.**

C07-641098-00 12/10