Cisco Security Information Event Management Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

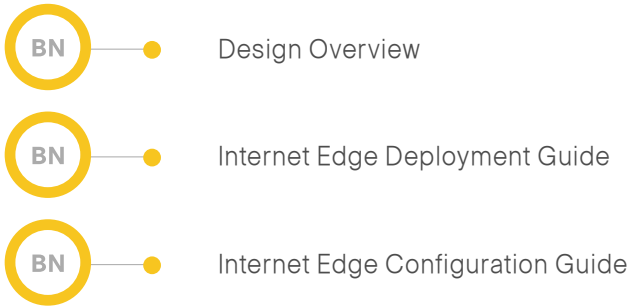
This guide focuses on Cisco products and discusses how those products integrate with any third party SIEM product. It does not cover third party SIEM product configuration details. For third party SIEM product details, refer to the Secure Borderless Networks Technology Partners page: http://www.cisco.com/go/securitypartners

Who Should Read This Guide

- Has read the Internet Edge Deployment Guide
- Wants to connect Borderless Networks to the Cisco SIEM solution
- Wants to gain a general understanding of the Cisco SIEM solution
- Has a CCNA® Security certification or equivalent experience
- Wants to address compliance and regulatory reporting requirements
- Wants to enhance network security and operations
- Wants to improve IT operational efficiency
- Wants the assurance of a validated solution

Related Documents

Related Reading



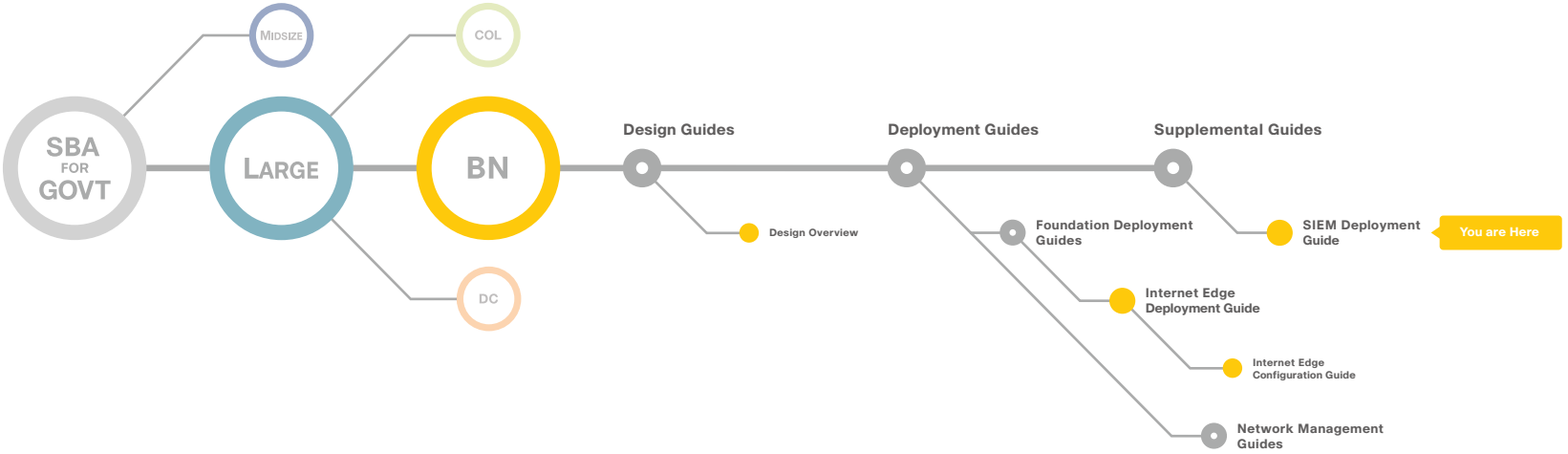


Table of Contents

Introduction

The Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks incorporates many parts, including firewalls, routers, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other devices whose proper operation is essential to the security of the network. These devices may produce significant amounts of event logs and other security-relevant information. Security information and event management (SIEM) products are designed to make the task of collecting, correlating, and acting on this information easier. This guide is a supplement to the SBA for Large Agencies—Borderless Networks architecture, and should be read together with the LAN, WAN, and Internet Edge Deployment Guides; Figure 1 shows how a SIEM integrates into the overall architecture.

Using this Cisco SIEM Deployment Guide

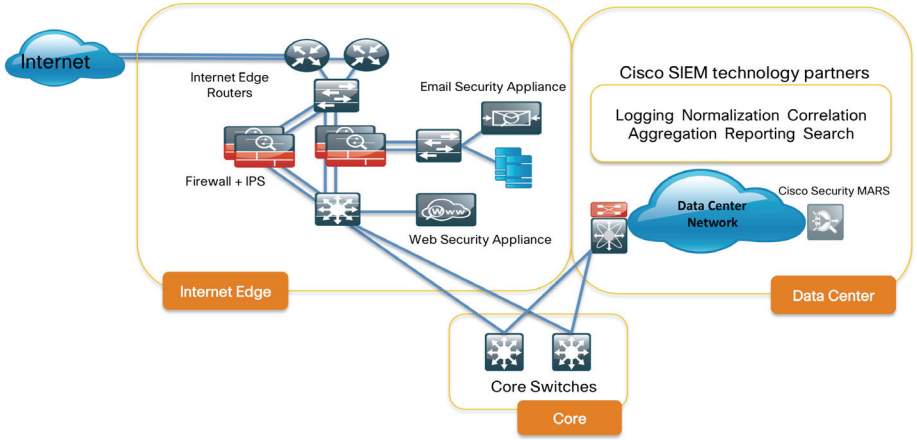
This guide provides a general overview of SIEM technology, as well as best practices, use cases, and deployment considerations for using a SIEM with Cisco infrastructure. This guide is intended to be used together with one of the partner SIEM deployment guides, which contains deployment steps and configurations specific to that partner's product. (Note: In this guide, "Cisco infrastructure" is used to include firewalls, routers, IDS, IPS, and other systems that are sources of security event information.)

The Agency Overview section of this document outlines the operational problems faced by large agencies in managing, storing, tracking, and using security information and event logs. The Technology Overview provides details on fundamental SIEM concepts and important considerations when evaluating SIEM solutions. The guide introduces the Cisco SIEM solution, and describes how this solution fits in the SBA for Large Agencies—Borderless Networks and how it solves operational problems of large agencies. The Configuration Details section discusses best practices and the steps required to deploy Cisco infrastructure with a SIEM partner product.

Agency Overview

Increasing employee mobility, use of video, and globalization are changing the IT environment. Traditional agencies that once viewed themselves as distinct entities with a clearly defined perimeter are now shifting to a borderless model. The borderless model allows cloud-based services, workplace mobility, application integration, and a wide variety of networked devices. As the environment becomes more complex, agencies face growing security challenges with complex regulatory requirements that force them to effectively monitor and report security incidents. Agencies face operational challenges in the area of compliance, enhanced network security, IT and security operations.

Figure 1. SIEM Placement in the SBA for Large Agencies—Borderless Networks



The first challenge for the agency is to comply with regulatory requirements, as well as its own internal policies. Customers need the ability to log, monitor, and report on security incidents in their data infrastructure, and to log, store, and report on large volumes of security event logs. Agencies find themselves having to deal with massive amounts of data being generated by their infrastructure every day.

The second challenge involves enhancing network security of the agency. With threats constantly coming from outside and inside the agency, it is increasingly difficult to weed through the noise of routine security events and determine which threats warrant investigation. Economic pressures to do more with less staff only compound the problem.

Finally, gathering logs from devices and applications throughout the agency can be very costly. Managing the sheer volume of raw logs and events, both in real time and from for long term archive storage is a major effort. Security investigations can require searching many different networked systems and piecing together fragmented bits of information stored in a variety of incompatible formats. Agencies need a unified view of the state of network security in a single dashboard.

Technology Overview

Security Information and Event Management

SIEM technology is used in many large agencies to provide real time reporting and long term analysis of security events. SIEM products evolved from two previously distinct product categories, namely security information management (SIM) and security event management (SEM). Table 1 shows this evolution.

Table 1. SIM and SEM Product Features Incorporated into SIEM

Separate SIM and SEM Products	
Security Information Management:	Security Event Management:
Log collection, archiving, historical reporting, forensics	Real time reporting, log collection, normalization, correlation, aggregation

Combined SIEM Product				
Log collection	Normalization	Correlation	Aggregation	Reporting

SIEM combines the essential functions of SIM and SEM products to provide a comprehensive view of the agency network using the following functions:

- Log collection of event records from sources throughout the agency provides important forensic tools and helps to address compliance reporting requirements.
- Normalization maps log messages from different systems into a common data model, enabling the agency to connect and analyze related events, even if they are initially logged in different source formats.
- Correlation links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
- Aggregation reduces the volume of event data by consolidating duplicate event records.
- Reporting presents the correlated, aggregated event data in real-time monitoring and long-term summaries.

Notes

Cisco SIEM Solution Overview

Agencies have a major investment in Cisco technology, and rely on Cisco to provide secure, robust, scalable, and interoperable solutions.

Cisco is partnering with leading companies through the Cisco Developer Network (CDN) to deliver a SIEM solution that meets the diverse security and reporting needs of agencies. This integration enables customers to select the SIEM tools best suited to their own environments and requirements, and take full advantage of the capabilities of their Cisco network infrastructure.

The SIEM partners' products complement the Cisco Security Management Suite, including Cisco Security Manager and Cisco Security MARS, to provide support for enhanced operational use cases.

The SIEM solution is part of the Cisco SBA for Large Agencies—Borderless Networks design, which offers partners and customers valuable network design and deployment best practices, and helps agencies deliver superior end-user experiences on their networks.

Notes

Cisco SIEM Solution Deployment

The SIEM market is evolving towards integration with business management tools, internal fraud detection, geographical user activity monitoring, content monitoring, and mission-critical application monitoring. SIEM systems are implemented for compliance reporting, enhanced analytics, forensic discovery, automated risk assessment, and threat mitigation.

Compliance

Compliance with monitoring and reporting regulations is often a significant factor in the decision to deploy a SIEM system. Other policy requirements of a specific agency may also play a role. Examples of regulatory requirements include the Health Insurance Portability and Accountability Act (HIPAA) for health care providers in the United States, or the Payment Card Industry's Data Security Standard (PCI-DSS) for organizations that handle payment card information. A SIEM can help the agency to comply with monitoring mandates and document their compliance to auditors.

Enhanced Network Security and Improved IT/Security Operations

Attacks against network assets are a daily occurrence for many agencies. Attack sources can be inside or outside the agency's network. As the boundaries of the agency network expand, the role of network security infrastructure must expand as well.

Typically, security operations staff deploys many security measures, such as firewalls, IDS sensors, IPS appliances, web and email content protection, and network authentication services. All of these can generate significant amounts of information, which the security operations staff can use to identify threats that could harm network security and operations.

For example, when an employee laptop becomes infected by malware, it may discover other systems on the corporate network, and then attempt to attack those systems, spreading the infection. Each system under attack can report the malicious activity to the SIEM. The SIEM system can correlate those individual reports into a single alert that identifies the original infected system and its attempted targets. In this case, the SIEM's ability to collect and correlate logs of failed authentication attempts allows security operations personnel to determine which system is infected, so that it can be isolated from the network until the malware is removed. In some cases, it may be possible to use information from a switch or other network access device to automatically disable the network connection until remediation takes place.

The SIEM can provide this information in both real-time alerts and historical reports that summarize the security status of the agency network over a large data collection, typically on the order of months rather than days. This historical perspective enables the security administrators to establish a baseline for normal network operations, so they can focus their daily effort on any new or abnormal security events.

Configuration Details

Cisco Security Information and Event Solution Configuration

Large agencies have different operational models and therefore different logging requirements, but all should have a policy regarding the capturing, storing, archiving, and monitoring of logs from network infrastructure devices, systems and applications.

This section outlines some of the high-level best practices and sample configurations for enabling logging on Cisco network infrastructure devices. You should understand the following areas before enabling logging:

- Logging and time stamps
- Logging retrieval methods
- Logging level details
- Rate of log generation
- Logging archives

Logging and Time Stamps

The exact time at which a security event occurred is important information, and may need to be correlated across several different devices. The Network Time Protocol (NTP) should be configured wherever possible to synchronize time across networks, applications, and systems.

Logging Retrieval Methods

The following table shows the logging methods for each type of security device that is addressed in this guide:

Table 2. Logging Methods

Security Device	Logging Method	Protocol Details
Cisco IOS-based router	syslog	UDP port 514
Cisco ASA 5500 Series	syslog	UDP port 514 or TCP port 1468
Cisco IPS 4200 Series	SDEE	HTTP or HTTPS
Cisco Security MARS	Raw message archive	SFTP or NFS
Cisco IronPort Email Security Appliance	Log file export	SCP or FTP
Cisco IronPort Web Security Appliance	Log file export	SCP or FTP

Tech Tip

Use TCP-based syslog where possible, because TCP delivery is reliable, and data forwarding will stop if the device cannot write to log servers.

Logging Level Details

Standard syslog implementations define eight severity levels for messages, identfied by a number from zero to seven, with lower severities representing more severe or important events. The configured log level determines the lowest priority message that is eligible to be logged. For example, if the log level is set to 5 for notifications, messages of level 6 or 7 are not logged. Unless specifically required, avoid setting the log level to 7, because debugging level messages create significant extra traffic, usually of little security interest. A device's logging level should be chosen to strike a balance between collecting enough information to meet security requirements, while keeping overall impact on systems and network resources as low as possible.

Table 3. Syslog Message Levels

Log Level	Severity Keyword	Meaning	Default Behavior
0	emergencies	System is unusable	logged
1	alerts	Immediate action needed	logged
2	critical	Critical conditions	logged
3	errors	Error conditions	logged
4	warnings	Warning conditions	logged
5	notifications	Normal but significant conditions	logged
6	informational	Informational messages	logged
7	debugging	Debugging messages	not logged

Logging Archives

Log management solutions need to have a substantial amount of storage to hold all of the log messages. Some regulations may require agencies to keep logs for a certain number of days or months or years.

Rate of Log Generation

The volume of traffic flowing through your network, the complexity of your policy rules, and the logging configuration of your devices will affect the amount of security information that is logged. Excessive logging can cause performance problems, increase network load, and make it harder to extract useful information from the SIEM product. Log levels should be set according to the importance of the assets being protected, and will vary according to each agency's environment and requirements. For example, a database administrator might enable extensive auditing and logging on a critical financial application, and lower levels for most other applications. To help understand the actual volume of logs generated, it can be helpful to set up a syslog receiver on a separate system, and monitor the rate of incoming messages. Also keep in mind that the amount of information logged during an attack may increase significantly compared to normal levels.

Notes

Tuning Cisco Infrastructure

The following processes show how to configure your Cisco security infrastructure components to send log messages and event records to the SIEM system.

Process

Tuning Cisco ASA 5500 Adaptive Security Appliances

1. Syslog Message Tuning

Procedure 1 Syslog Message Tuning

Cisco ASA 5500 series appliances provide full security information with logging set to level 6 – Informational. This can still generate a large number of messages. As an alternative to changing the log level for the entire device, disabling selected syslog messages of limited interest can help to reduce message load while still retaining as much security information as possible. On Cisco ASA 5500 appliances, log messages include a six-digit numeric code that identifies the event. The first three digits indicate the class of event. For example, codes beginning with 611 are associated with VPN client operations, and a message prefixed with %ASA-6-611102 is a user authentication failure. Refer to the Cisco ASA 5500 Series System Log Messages documentation for your software version for details.

At logging level Informational, Cisco recommends disabling the following messages, as they are of little interest for SIEM analysis:

```
305010: The address translation slot was deleted
305011: A TCP, UDP, or ICMP address translation slot was
created
305012: The address translation slot was deleted
To disable these messages, use the following configuration
commands:
no logging message 305010
no logging message 305011
no logging message 305012
```

For more aggressive tuning, you may also consider disabling the following messages:

```
302014: A TCP connection between two hosts was deleted
302016: A UDP connection slot between two hosts was deleted
```

If dynamic Network Address Translation (NAT) is not configured on the appliance, message 302013 (for TCP connection slot creation) can also be disabled.

Cisco ASA 5500 Series appliances also allow you to change the severity level at which a message is logged. For example, message ID 111009, which records the execution of exec commands on the appliance, is by default logged at level 7 – Debug. The following configuration command would cause this event to be logged at Informational level instead:

```
logging message 111009 level 6
```

ASA Botnet Filtering

Cisco ASA provides reputation-based control for an IP address or domain name, similar to the control that IronPort® SenderBase® provides for e-mail and web servers. The Botnet Traffic Filter generates detailed syslog messages numbered 338nnn. Messages differentiate between incoming and outgoing connections, blacklist, whitelist, or greylist addresses, and many other variables. For example, syslog messages 338001 and 338002 are generated when traffic to or from a blacklisted domain is detected.

```
ASA-4-338002: Dynamic filter permitted black listed TCP
traffic from inside: 10.1.1.45/6798 (209.165.201.1/7890) to
outside: 209.165.202.129/80 (209.165.202.129/80), destination
209.165.202.129 resolved from dynamic list: bad.example.com

hostname# show dynamic-filter reports top malware-sites

                        Connections          Threat
Site                      logged    dropped  Level    Category
-------------------------------------------------------------

bad1.example.com            11         0       2       Botnet
(10.67.22.34)

bad2.example.com             8         8       3       Virus
(209.165.200.225)

bad1.cisco.                  6         6       3       Virus
example(10.131.36.158)

bad2.cisco.                  2         2       3       Trojan
example(209.165.201.1)

horrible.example.            2         2       3       Botnet
net(10.232.224.2)

nono.example.                1         1       3       Virus
org(209.165.202.130)
```

Process

Cisco IPS 4200 Series Sensors

1. Tuning IPS Events for SIEM Products

IPS sensors may be deployed in the DMZ, at the network edge, in the data center, and at other points within the network, depending on security requirements. The location of an IPS will influence the tuning of which events, protocols, and applications it considers to be significant for reporting purposes. An un-tuned IPS will generate a significant number of events, most of which will not be related to actual intrusion attempts. For example, a ping-based network reconnaissance attack may be a routine event at the Internet edge, but if the same pattern is detected within the agency's own data center, it may be a warning sign that a server has been compromised.

Cisco IPS systems use SDEE to provide XML-based security event records to clients, such as a SIEM collector, over HTTP or HTTPS. In this case, unlike with syslog, the SIEM is acting as a client, and contacts the IPS to request the information. In order to do this, the SIEM must be configured with the IP address or host name of the IPS, and a username and password to authenticate its requests.

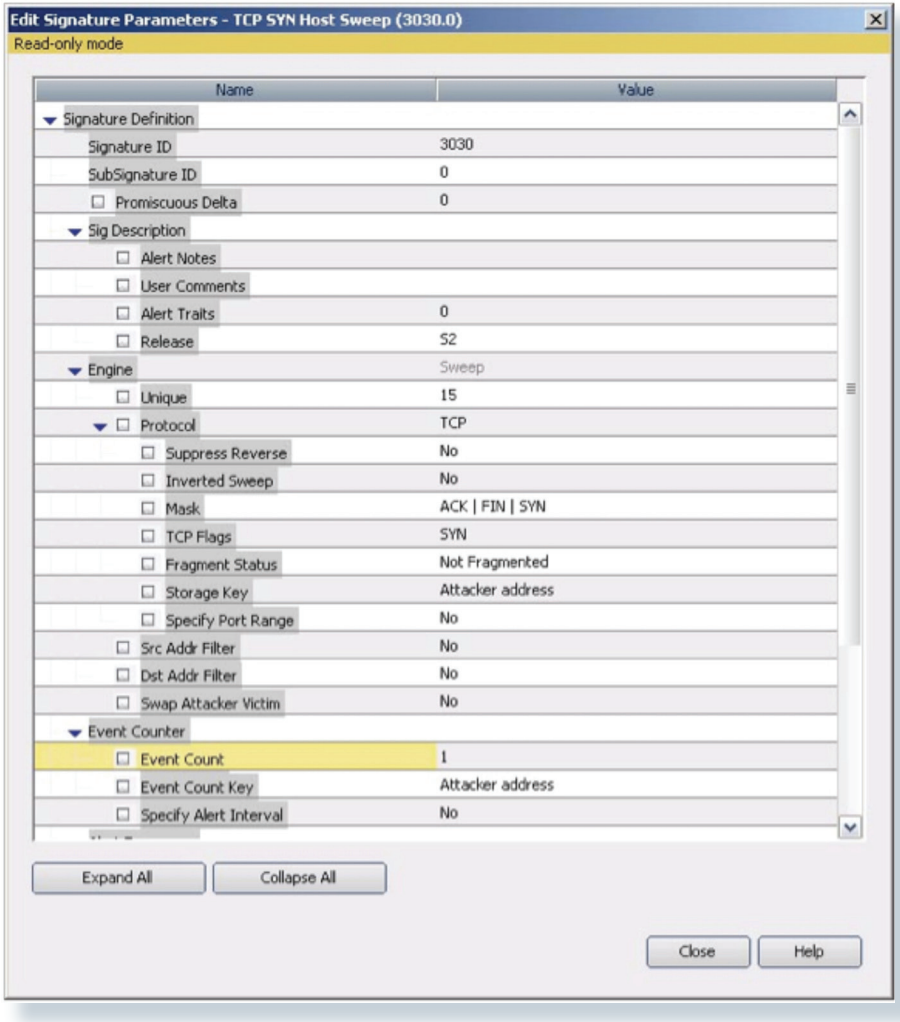
Procedure 1 Tuning IPS Events for SIEM Products

IPS sensor events can be tuned in different ways, depending on requirements. Here are some techniques that can be used in certain environments to reduce the number of messages being sent to the SIEM.

Changing Event Count for the Signature

This technique can significantly reduce message traffic, saving SIEM processing time and storage space. Use the Intrusion Prevention System Device Manager (IDM) to configure the IPS sensor to send alerts only when the same signature is seen more than a certain number of times overall, or a certain number of times for a given set of addresses (for example, the attacking IP). For more fine-grained control, event counts can be adjusted for individual signatures in the Edit Signature Parameters window, as shown in Figure 2. For example, a small number of ping probes may not be of great interest, but a large number within a short time to or from the same address could indicate an attack in progress.

Figure 2. Adjusting Event Counts for a Signature



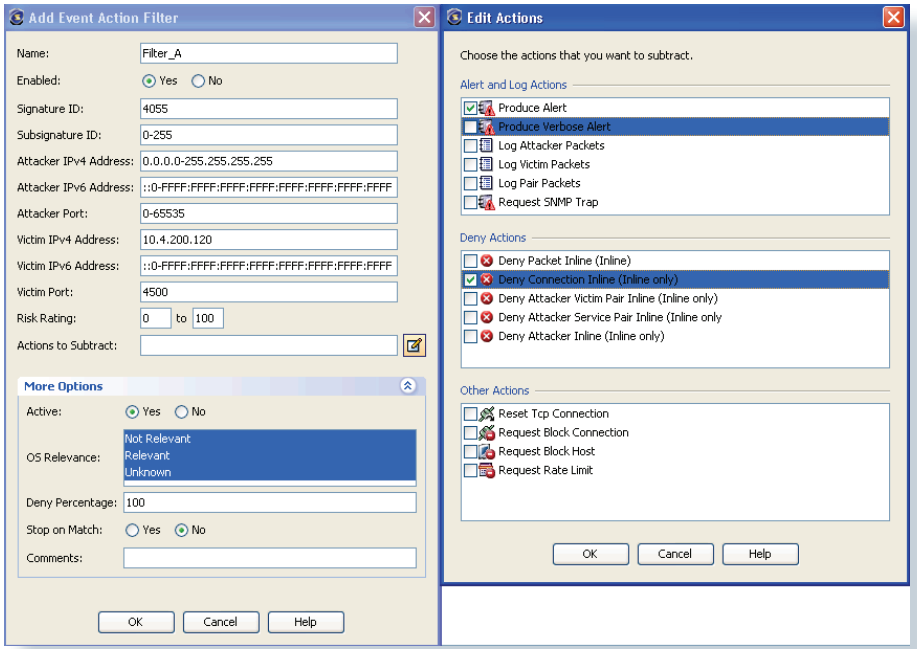
Disabling Signatures

Signatures that are not being used in an agency can be retired. Retired signatures will not be used to generate alerts, but can be reactivated later if requirements change. Retiring unused signatures can help to improve sensor performance. For more information about signature tuning, please see the following case study of Cisco's own Computer Security Incident Response Team (CSIRT): http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/CSIRT_Network-Based_Intrusion_Prevention_System_Case_Study.pdf

Event Action Filter

Administrators can use Event Action Filters to modify the actions taken when an event matching the filter occurs. This allows alert responses to be modified to suit specific exception cases. For example, a ping sweep of a network could be a normal event when it originates from a system used by the network administrators to run security checks, but would be an indicator of a possible compromise if the same traffic pattern originated from an employee's laptop. Figure 3 shows the Add Event Action Filter window in IDM.

Figure 3. The Add Event Action Filter Window



Global Correlation Logging

Cisco Global Correlation is a feature that allows IPS devices to access information from the Cisco SensorBase Network, a dynamic worldwide database of threats, to learn which networks and hosts on the Internet have a reputation for malicious activity. This information can improve the effectiveness and accuracy of the IPS, by taking reputation into account when evaluating network traffic.

There are three main features of global correlation:

- Global Correlation Inspection uses knowledge of current attack sources to influence alerting and blocking of undesirable traffic. Reputation scores are included in SDEE event records, so they are visible in the SIEM.
- Reputation Filtering can immediately block packets from sites that are known to be malicious, without the need to undergo full signature analysis. Separate log messages are not generated for these addresses, but statistics are kept.
- Network Participation allows IPS sensors to send aggregated statistics back to the Cisco SensorBase Network. This participation is optional, anonymous, and strictly confidential.

Process

Cisco Routers

1. Configuring Routers to Send Logs to SIEM
2. ACL Logging on Cisco Routers

Cisco routers can record information about a variety of events, many of which have security significance. Cisco routers support syslog, SNMP, and NetFlow as a means of transport and information for third party SIEM products.

Procedure 1 Configuring Routers to Send Logs to SIEM

We recommend configuring log time stamps to include the date and time with millisecond precision, and the time zone. Use the following global configuration command to configure a logging time stamp:

```
service timestamps log datetime msec show-timezone localtime
```

The following configuration example configures a Cisco router to send logging information to a SIEM whose IP address is 10.4.200.111:

```
logging host 10.4.200.111
logging on
```

Cisco routers can also use a local log buffer to store log messages. Buffered logging is often preferable to sending log messages to the console or to a monitor session. Console logging in particular can increase the router's CPU load. Buffered log messages can also be useful for troubleshooting, if the SIEM is unreachable when the log message is generated. The following configuration example creates a 16KB logging buffer and specifies message severity level 6 – Informational. The example also shows how to disable logging to the console and to terminal monitor sessions.

```
no logging console
no logging monitor
logging buffered 16384 6
```

The following example shows how to configure logging level 6 – Informational for syslog:

```
logging trap 6
```

To ensure that all log messages sent by the router appear to come from the same interface address, in this case the Ethernet0 interface, configure the following:

```
logging source-interface interface Ethernet0
```

Procedure 2 ACL Logging on Cisco Routers

ACLs that include access control entries (ACEs) with the log or log-input keyword are called log-enabled ACLs. They provide detailed information when a permit or deny ACL is triggered and can be useful for troubleshooting, but they can be CPU intensive and should be used with care. The following example shows a log-enabled ACL.

```
access-lists 101 deny tcp any any eq 12345 log
access-lists 101 deny tcp any any eq 12345 log-input
```

To limit the performance impact of ACL logging, configure rate limiting as in the following example:

```
logging rate-limit 100 except 4
```

Log-enabled ACLs can cause packets to be process switched, increasing CPU load on the router. To limit the performance impact of ACL logging, configure a logging interval to restrict the number of logged, and therefore process switched, packets in a specific time interval. Keep in mind that, as with any tuning, this involves a trade-off between the volume of log messages and the level of detail captured in the logs. The following example would restrict logging to one packet per eight milliseconds:

```
ip access-list logging interval 8
```

Similarly, configuring a logging threshold determines how many packets must match an ACE before they are logged, as in the following example:

```
ip access-list log-update threshold 11
```

Process

Cisco IronPort Web Security Appliance

1. Sending WSA Logs to SIEM

Cisco IronPort Web Security Appliances can generate log files for monitoring web traffic. These files are controlled by Log Subscription configuration options under System Administration in the management interface.

Log Types

There are many types of log files that can be produced; two types of log files are of particular interest for security operations:

Access logs record web proxy activities

Traffic logs record Layer 4 Traffic Monitoring (L4TM) activities

These logs can be stored in the commonly used Apache, Squid, or Squid Detail formats.

Log Retrieval Methods

SIEM products can receive appliance logs through SCP or FTP file transfer, or syslog. Syslog has a greater impact on performance, and is not supported for all log types; Cisco recommends using SCP, or FTP if SCP is unavailable.

Procedure 1 Sending WSA Logs to SIEM

Follow these steps in the Web Security Appliance web management interface to send access logs to a SIEM:

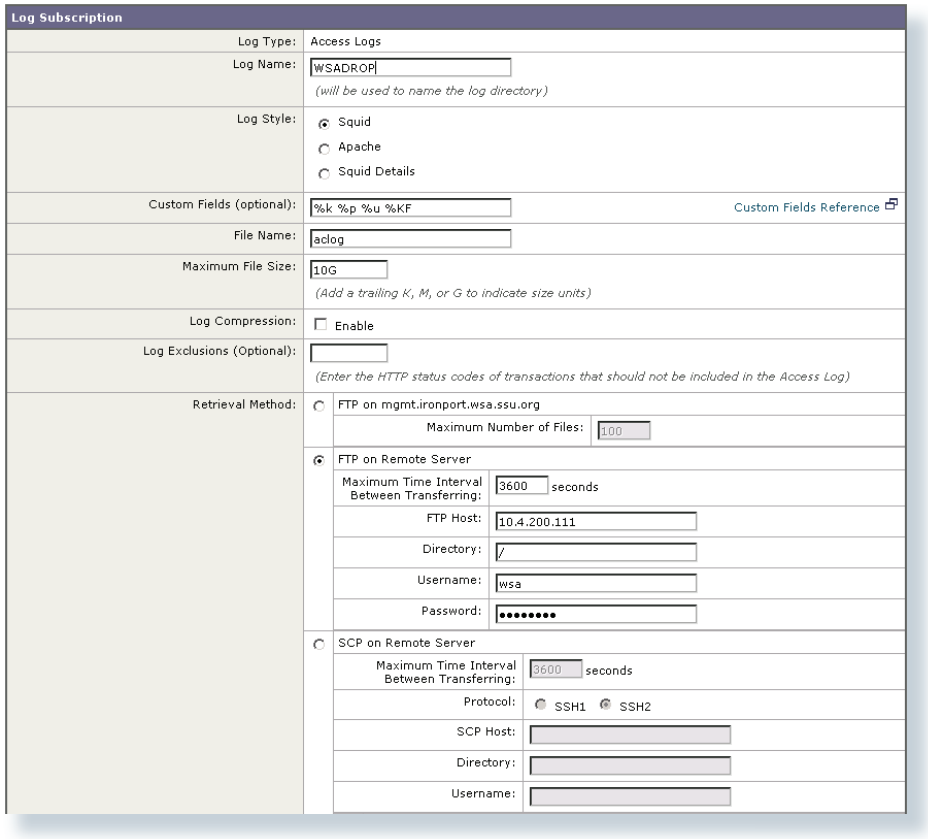
Step 1: Navigate to the **System Administration** > **Log Subscriptions** page.

Step 2: Click **Add Log Subscription**. The New Log Subscription page appears, as shown in Figure 4.

Step 3: Select **Access Log** from the **Log Type** menu.

Step 4: Enter a name for the log subscription in the **Log Name** field. Note that this name will be used for the directory that the appliance uses to store these logs. The example shown in Figure 4 uses WSADROP as the name.

Figure 4. Log Configuration Example for Cisco IronPort Web Security Appliance



Step 5: Choose one of the common predefined formats for recording the access logs, or use the **Custom Field**s field to create your own format. In the example shown in Figure 4, we select Squid.

Step 6: Choose how to transfer the log file from the appliance by selecting a **Retrieval Method**. In the example in Figure 4, FTP is selected. When choosing this method, the following information must be entered:

- Maximum time between file transfers
- FTP server hostname or IP address
- Directory on FTP server to store the log files
- Username and password of a user with write access to that directory

Tech Tip

FTP log transfers only support passive mode FTP.

The appliance rolls over log files based on settings configured on the 'Log Subscription' global settings page. Log files can also be sent on demand by clicking the 'Rollover Now' button.

Step 7: Submit and commit the changes.

Process

Cisco IronPort Email Security Appliance

1. Sending ESA Logs to SIEM

Cisco IronPort Email Security Appliances support the following logging options and parameters:

Log Types

Most logs on the appliance are recorded as plain text, except for mail delivery logs, which are stored as binary files for efficiency. There are many types of logs supported on the appliance: delivery logs, bounce logs, status logs, anti-spam logs, anti-virus logs, reporting logs, and tracking logs.

Log Format

Mail delivery logs can be stored in text format or in Qmail format.

Log Retrieval Methods:

SIEM products can receive appliance logs through SCP or FTP file transfer, or syslog. Syslog has a greater impact on performance, and is not supported for all log types, so using one of the file transfer methods is recommended.

Procedure 1 Sending ESA Logs to SIEM

Follow these steps in the Email Security Appliance web management interface to send mail logs to a SIEM:

Step 1: Navigate to the **System Administration** > **Log Subscriptions** page.

Step 2: Click **Add Log Subscription**. The New Log Subscription page appears.

Step 3: Select IronPort Text Mail Log from the Log Type menu.

Step 4: Enter a name for the log subscription in the Log Name field. Note that this name will be used for the directory that the appliance uses to store these logs. The example shown in Figure 5 uses mail_logs as the name.

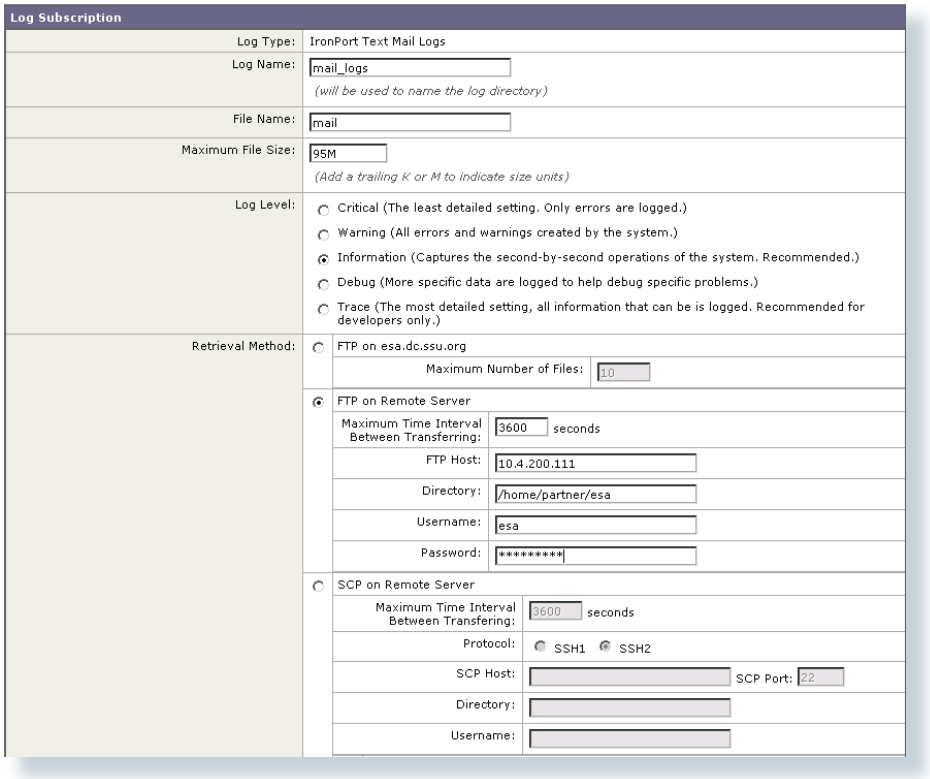
Step 5: Choose how to transfer the log file from the appliance by selecting a Retrieval Method. In the example, FTP is selected. When choosing this method, the following information must be entered:

- Maximum time between file transfers
- FTP server hostname or IP address
- Directory on FTP server to store the log files
- Username and password of a user with write access to that directory

Tech Tip

FTP log transfers only support passive mode FTP.

Figure 5. Log Configuration Example for Cisco IronPort Email Security Appliance



Step 6: Submit and commit the changes.

Process

Cisco Security MARS

1. Configuring Cisco Security MARS to Archive Data

If the Cisco Security Monitoring, Analysis, and Response System (MARS) is deployed in an agency for monitoring and correlating events from Cisco devices, the data from MARS can also be imported into a third-party SIEM solution. In a heterogeneous environment, using a third-party SIEM solution allows Cisco and non-Cisco device information to be consolidated and correlated. For more details, refer to the third-party SIEM deployment guides in the technology partner zone.

Homogeneous Network (Cisco Only)	Heterogeneous Network	Heterogeneous Network
Cisco Security MARS	MARS (already deployed)	Third Party SIEM Solutions
	Third Party SIEM Solutions	

Procedure 1 Configuring Cisco Security MARS to Archive Data

Cisco Security MARS can archive data using the Secure FTP (SFTP) or Network File System (NFS) protocols. For security deployments, we recommend using SFTP. A MARS archive process runs nightly at 2:00 a.m., and creates a directory on the receiving system to contain that day's data. Raw event records are exported from MARS every ten minutes. The archive time parameters are not configurable.

The following steps are shown in Figure 6:

Step 1: In the Cisco Security MARS web management interface, navigate to Admin > System Maintenance > Data Archiving

Step 2: Select SFTP as the Archiving Protocol.

Step 3: Enter the IP address of the remote host that will receive the archives.

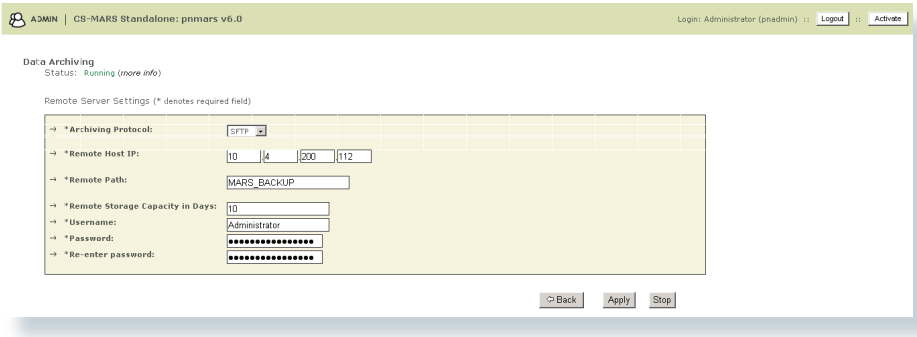
Step 4: Enter the path to be used for file storage on the receiving system.

Step 5: Accept the default of 10 days of remotely stored data. Because the archived event logs will be imported into the SIEM, this value is not usually important.

Step 6: Enter a username and password to authenticate the SFTP transfers.

Step 7: Apply and activate the configuration.

Figure 6. Configuring Data Archiving in Cisco Security MARS



Finally, configure the SIEM to import the archive data as detailed in the Deployment Guide for your specific SIEM solution.

Products Verified with Cisco SBA

Partner products have 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.

Additional Information

Technology partner solution guides can be found here: http://www.cisco.com/go/securitypartners

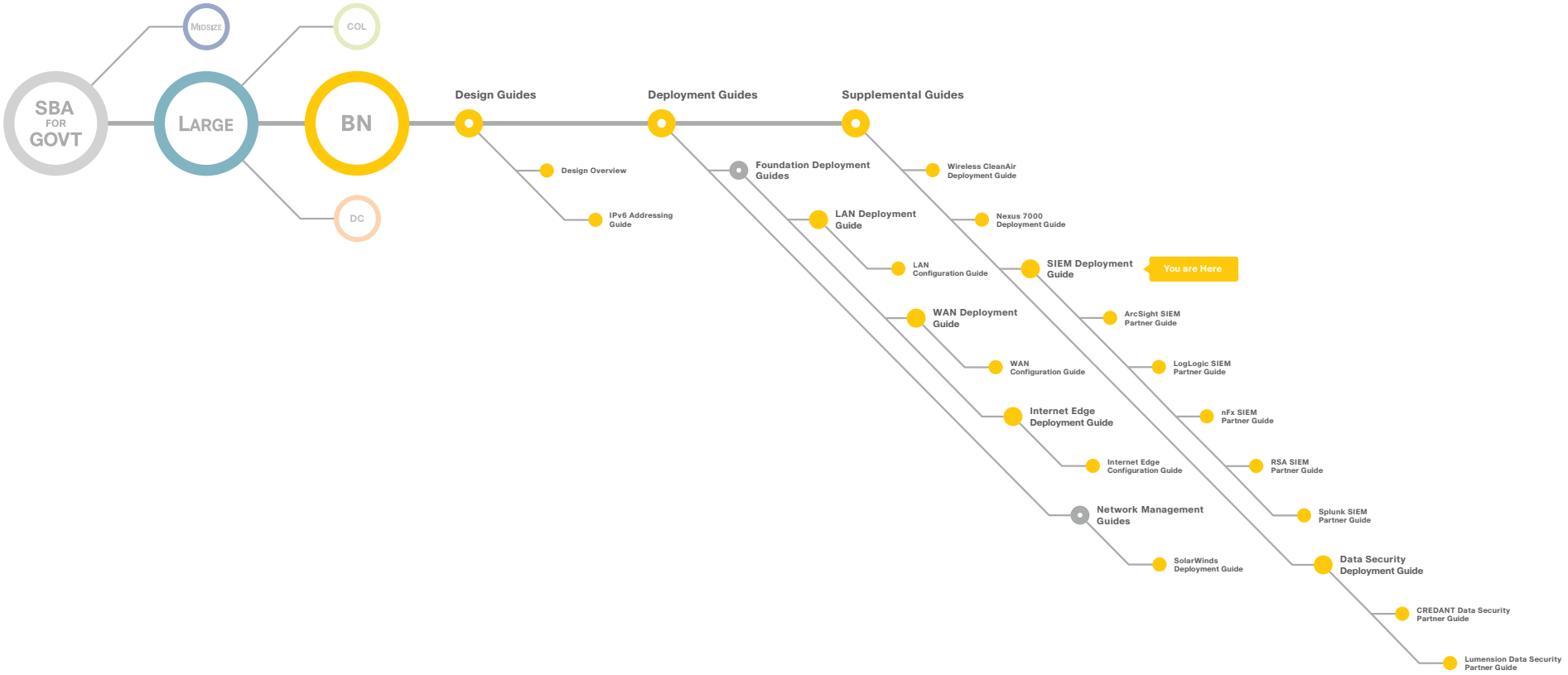
Security Management Information

http://www.cisco.com/en/US/products/ps5739/Products_Sub_Category_Home.html

Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks

http://oreilly.com/catalog/9780596518165

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.**

C07-640737-00 12/10