LogLogic SIEM Partner Guide

SBA FOR GOVERNMENT

Revision: H2CY10

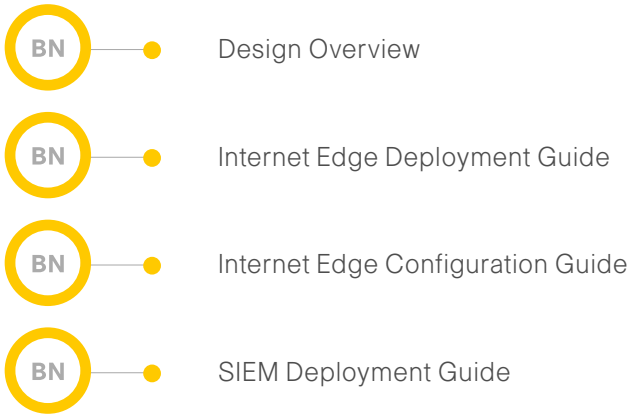
Using this SIEM Partner Guide

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 LogLogic SIEM solution
- Wants to gain a general understanding of the LogLogic 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

Before reading this guide



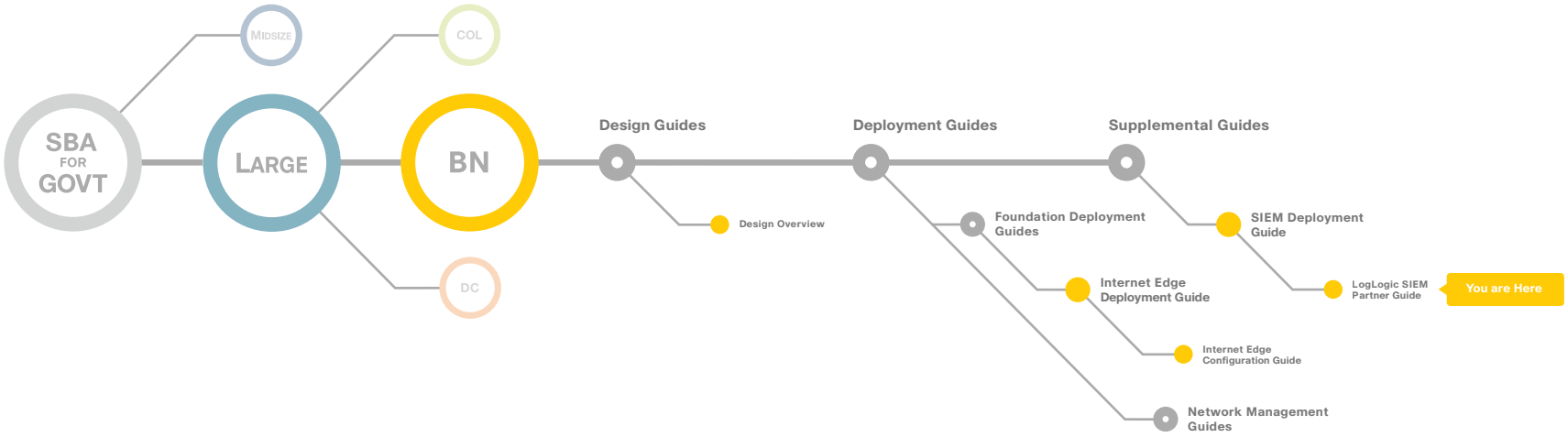


Table of Contents

Cisco SBA for Large Agencies—Borderless Networks

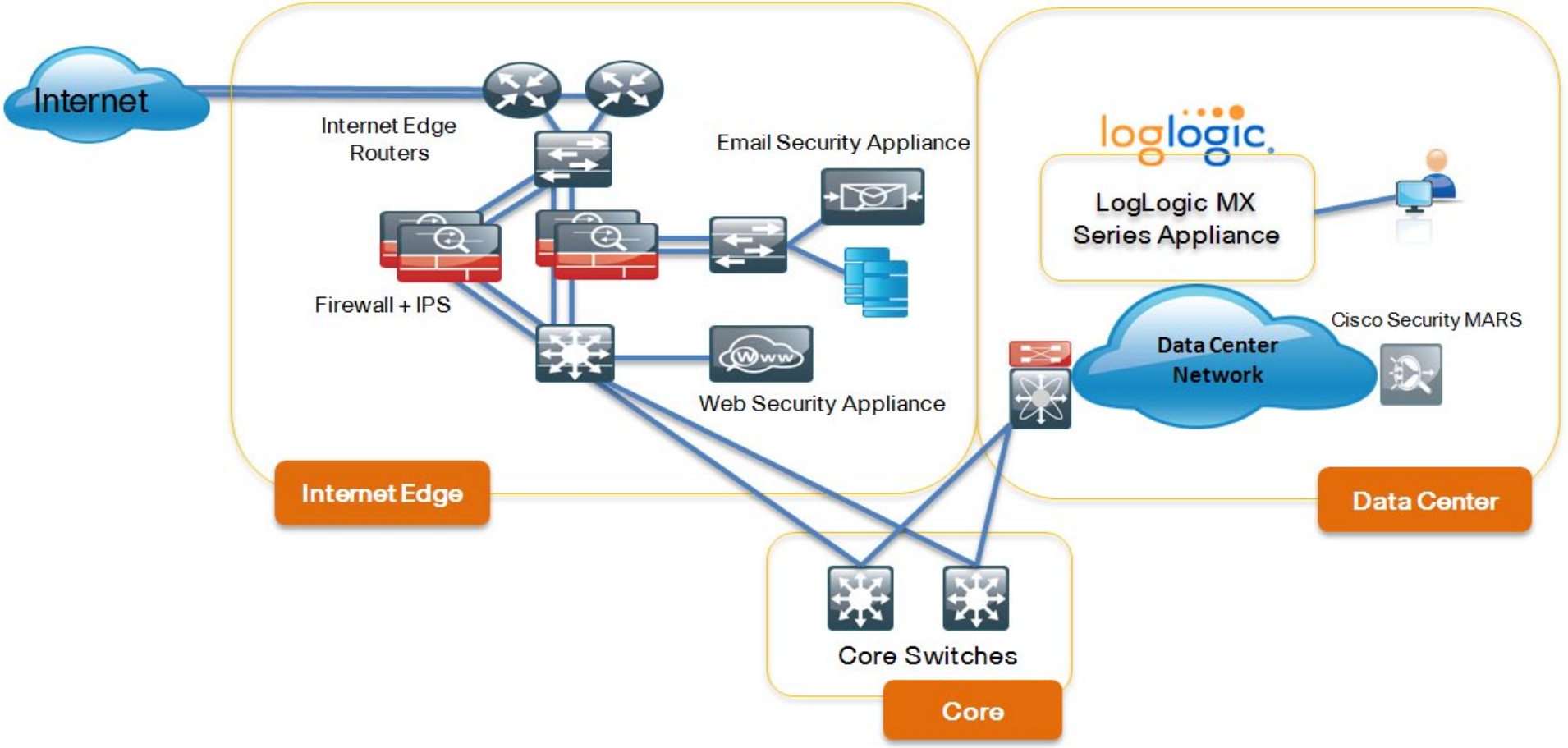
The Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks offers partners and customers valuable network design and deployment best practices, helping agencies deliver superior end-user experience that include switching, routing, security and wireless technologies combined with 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 Loglogic and their MX Series Security Information and Event Manager (SIEM) product.

Notes

Figure 1. LogLogic MX Series Appliance Integrated into SBA for Large Agencies—Borderless Networks



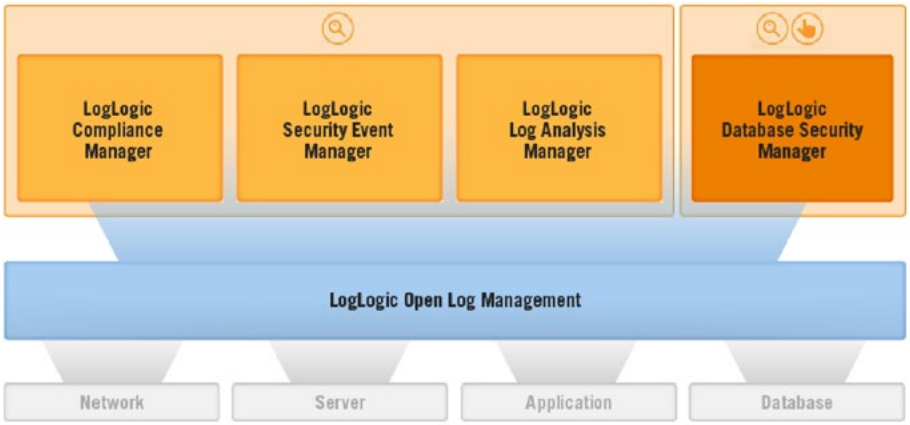
Agency Benefits

LogLogic offers a comprehensive suite of log and security management products that help large agencies to:

- Achieve regulatory compliance
- Protect valuable customer information
- Improve the efficiency of IT operations

The LogLogic logging, security, and IT search products shown in Figure 2 provide support for a broad range of Cisco networking, security, communication and infrastructure products.

Figure 2. Components of the LogLogic Log Management Platform



Compliance Reporting Benefits

LogLogic provides support for a number of compliance mandates, including PCI, SOX/COBIT, HIPAA, FISMA, ITIL, ISO, and NERC. LogLogic compliance reporting solutions are easily installed on top of the log management infrastructure, and immediately begin producing detailed compliance reports for key Cisco security and networking products.

Compliance Management Solutions & Benefits

LogLogic's Compliance Manager provides auditing and workflow solutions for PCI and SOX/COBIT compliance reports. This includes the following key benefits:

- Ensure and prove compliance review timeliness
- Access top-down executive views of compliance posture
- Dramatically improve audit speed and accuracy
- Reduce the cost of compliance
- Map data against agency policies
- Automate IT compliance functions

Security Benefits

Using LogLogic's extensive logging and IT Search capabilities, agencies can improve their security posture and provide detailed forensics support for security incidents. Security benefits of the LogLogic solution include the following:

- The **LogLogic Open Log Management** platform provides first-level alerting through pattern matching and log learning technology. LogLogic's Open Log Management platform also provides rapid searches against a complete record of user and system activity.
- **LogLogic Security Event Manager** adds sophisticated correlation and contextual analysis for advanced threat monitoring and fraud detection, helping to automate the incident management and response process.
- **LogLogic Database Security Manager** provides in-depth database threat and activity monitoring and can protect, amongst others, against SQL injection attacks. LogLogic Database Security Manager can also block suspicious activities in real-time.

IT Operations and Performance Management Benefits

LogLogic's scalable log collection, indexing, searching, and behavioral analytics solutions allow IT organizations to gain visibility and control over their valuable assets and resources. This allows these organizations to increase network and application performance, availability, and accountability. Additional benefits include the following:

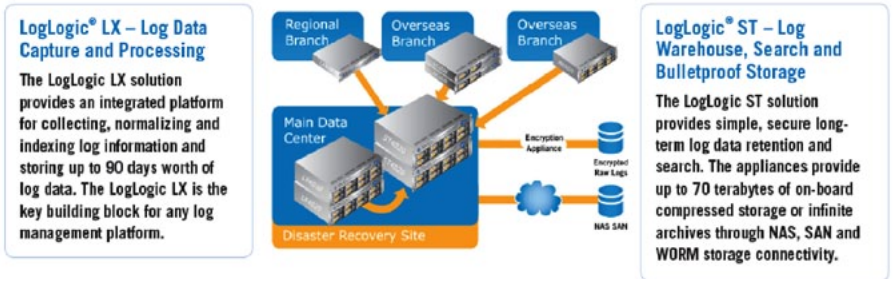
- **The LogLogic Open Log Management** platform monitors system behavior in real time. Advanced behavioral algorithms detect degradation in performance before it causes downtime. LogLogic's advanced alerting and search features also detect obscure error conditions as they happen, and help to identify the root cause.
- **The LogLogic Open Log Management** platform includes a free reporting package for the IT Infrastructure Library (ITIL), making it easier to implement best practices in the area of service desk management and change management.
- **The LogLogic Open Log Management** platform can monitor user and system activity of virtual applications and cross-correlate information from various applications.

Notes

LogLogic Open Log Management Products

The LogLogic product family includes the MX, LX, and ST Log Management Intelligence (LMI) appliances. These products all work in conjunction with Cisco products to provide advanced log collection, storage, archival, alerting, compliance and reporting solutions. The LogLogic product family is designed for scalability, performance, and to be quickly installed with rapid access to information and reports.

Figure 3. LogLogic LX and ST Appliances



The LogLogic MX solution is designed specifically for the mid-market, delivering comprehensive assurance for log data compliance mandates. Each LogLogic MX appliance includes a LogLogic Compliance and Control Suite with more than 100 customizable alerts and reports covering identity and access management, user activity, change, security, operational continuity and IT performance. The software platform on this single form factor appliance also incorporates one-year on-board log archival and storage capabilities, as well as indexed log data for fast Google-like search. In addition, each appliance includes one year of LogLogic maintenance and support.

LogLogic MX appliances integrate with the LogLogic Compliance Suite to cater to specific mid-market requirements. This mid-market, enterprise-grade functionality includes:

- **Reporting, search, and collection performance**—the ability to process custom log sources and easily customize reports previously reserved for enterprise customers.
- **Chain of custody features for built-in raw log archives**—enterprise-grade log data archival protection through checksum management.
- **Open web services API and aftermarket applications**—custom portal development and operational process automation through a fully featured SOA and web services API.

Figure 4. Comparison of LogLogic Appliances

LogLogic Appliances	MX3020	LX1020	LX4020	ST1020	ST2020-SAN	ST4020
						
Max Sustained MPS	1,000	5,000	10,000	75,000	150,000	150,000
Max Device Count	2000	16,000	16,000	16,000	16,000	16,000
Usable Storage (GB)	2,000	1,000	4,000	1,000	Up to 512TB	7,000
Rack Units	2U	1U	2U	1U	1U	2U

LogLogic Compliance Suites

LogLogic Compliance Suites turn log data into automated reports and alerts for monitoring controls and requirements for PCI, SOX/COBIT, HIPAA, HITECH, FISMA, ITIL, ISO, and NERC. Each Compliance Suite is a field installable option on MX product lines. Key features of the Compliance Suites include:

- **Agile Log Reporting**—Lets administrators create highly customized reports from easy-to-use templates. Lets administrators create reports for different mandates in seconds with no vendor intervention.
- **Log Learning**—Powerful and intelligent dynamic learning lets administrators set alerts based on changes to individual Cisco devices, groups of Cisco devices, or the network.
- **Log Forensics**—Indexing and Google-like search algorithms allow near-instant data retrieval - search terabytes of unaltered, unfiltered data in seconds.
- **Open Log Routing**—Routes raw data, reports and alerts to existing SIEM, network management, trouble ticket, and LogLogic Compliance Manager products.
- **Log Process Audit**—Enables network activity audits to provide proof of compliance or critical information for legal proceedings.

Table 1. Comparison of LogLogic MX, ST, and LX Appliances

	MX Appliance	ST Appliance	LX Appliances
Description	All-in-one log collection, reporting, management and compliance solution for SMB	Enterprise scalable log collection, storage, archive, search, and alerting	Enterprise scalable log analytics, reporting, and compliance reporting
Number of Users (Admin)	unlimited	unlimited	unlimited
Events Per Second (eps)	1000 eps	75,000 – 150,000 eps	5,000 – 10,000 eps

Notes

Deploying Loglogic MX Solution

This section outlines the steps required to configure the LogLogic appliances to process log data from Cisco devices.

Setting up the LogLogic Appliance

This section provides an overview on setting up the LogLogic appliance using the GUI. Specifically, this section goes over the following steps:

1. Connecting the appliance to a network
2. Logging into the appliance
3. Configuring log source auto-identification
4. Configuring network settings
5. Setting the time zone and time

Setting up the appliance is extremely fast and simple.

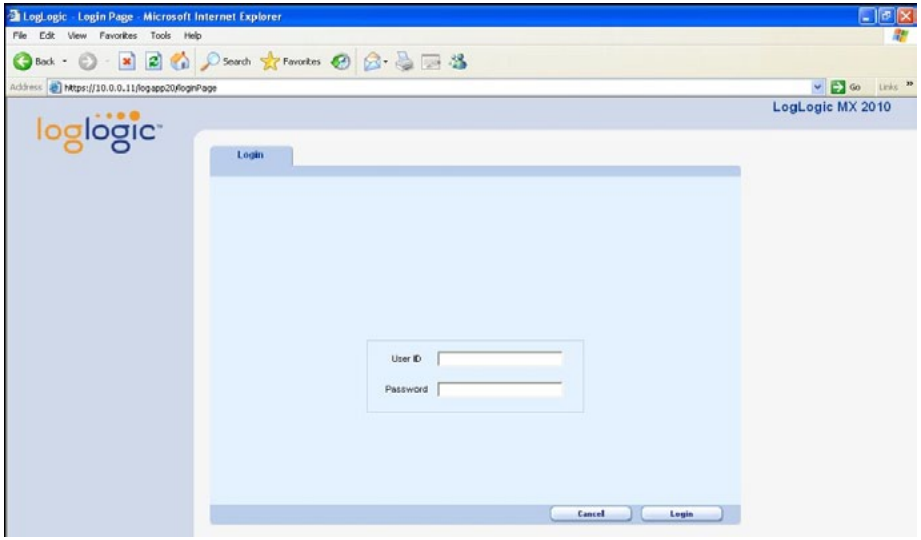
Step 1: Connecting the Appliance to a Network

The LogLogic appliance initially uses a default network address of 10.0.0.11 with a network mask of 255.255.255.0. Use a switch or an Ethernet crossover cable to make a direct connection between the appliance and a workstation configured with a 10.0.0.0/24 address.

Step 2: Logging in to the Appliance

1. Open a web browser on your workstation and connect to the appliance by entering https://10.0.0.11 in the browser address line.
2. Click **YES** to accept the certificate. A login screen appears, as shown in Figure 5.
3. Enter the default username (admin) and password (admin). The Appliance displays the End User License Agreement (EULA).
4. Accept the EULA. The Appliance asks you to enter a new password, which must contain at least one number.
5. Enter a new password. The Appliance displays the navigation menu, and a warning that the time is not yet set on the Appliance. You can ignore this warning; it is addressed later in this procedure.
6. Create a secondary administrative account.

Figure 5. The Login Screen



Step 3: Configuring Log Source Auto-Identification

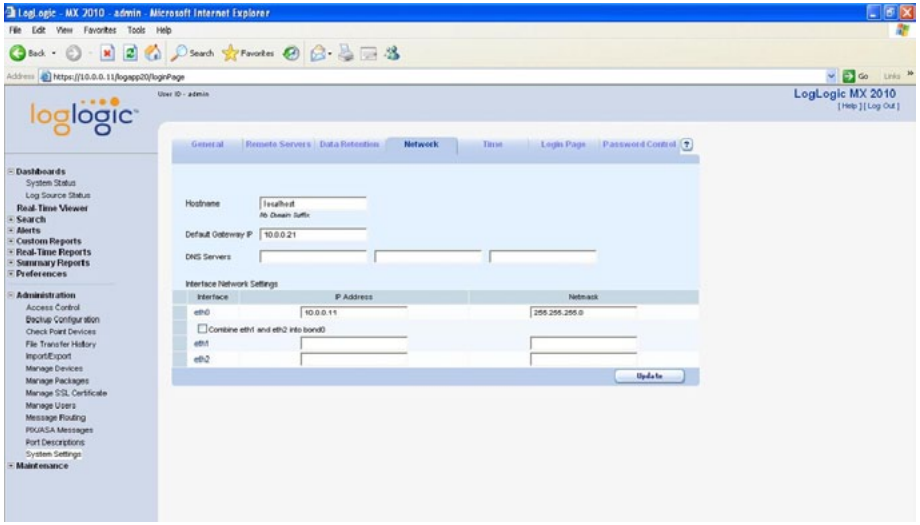
The auto-identification feature allows the appliance to quickly discover the actual Cisco product name and use this as the name of the device. Not all devices can be auto-identified, but for those that can, this feature is extremely handy in helping to easily identify the device.

1. Expand the **Administration** option in the left margin of the browser window.
2. Under Administration, select **System Settings**. The **General** tab appears.
3. Next to **Auto-identify Log Sources**, select **Yes**.
4. If you want to enable SSH connections to the appliance, next to **Enable SSH Daemon at Startup**, select **Yes**.
5. Click **Update**.

Step 4: Configuring Network Settings

1. Under **System Settings > Administration**, select the **Network** tab, shown in Figure 6.
2. Configure the IP address information for your network, then click **Update**.
3. Select **Reboot Later**. The following step, in which you configure time settings, will also prompt for a reboot, so both network and time settings can be applied at the same time.

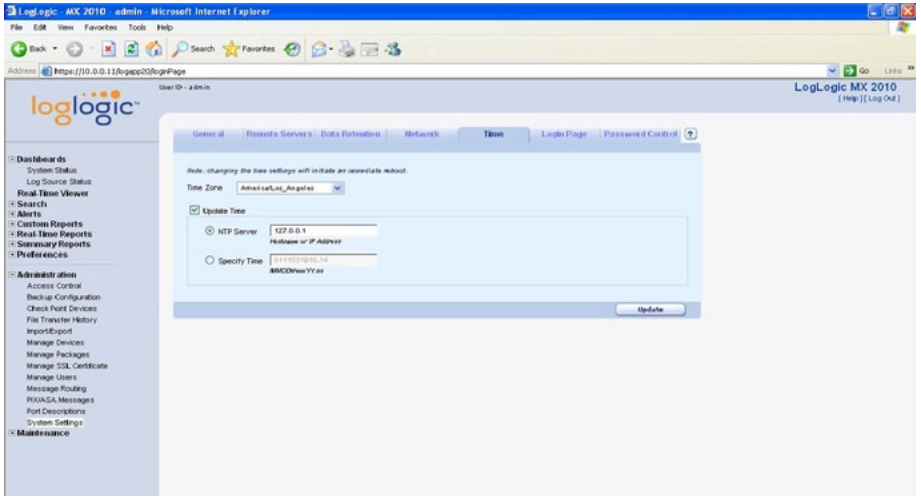
Figure 6. The Network Settings Tab



Step 5: Setting the Time Zone and Time

1. Under **Administration > System Settings**, select the **Time** tab, shown in Figure 7.
2. Select the appropriate time zone from the **Time Zone** drop-down menu.
3. Select **Update Time** to define how to synchronize the appliance clock with your local time.
4. Cisco recommends using the Network Time Protocol (NTP) to ensure that information is logged with consistent timestamps. Select **NTP Server** and provide the address of a time source that is reachable from your network.
5. Click **Update**. When notified that the appliance will be rebooted to apply the settings, click **OK**.

Figure 7. Configuring System Time and Time Zone



Reader Tip

Time zone configuration is important to the operation of the appliance. If you select an incorrect time zone, your reports and CLI access might not function properly. To ensure consistency of log timestamps, make sure that the NTP time source used by your appliance is the same one used by your routers, firewalls, and other network devices.

Sending Logs from Cisco Devices to a LogLogic MX Appliance

Sending Syslog Messages from Cisco Routers and Firewalls to the LogLogic Appliance

This section describes the steps required to configure a Cisco ASA 5500 Series Adaptive Security Appliance or a Cisco Integrated Services Router (ISR) to send syslog messages to a LogLogic appliance.

Configuring a Cisco ASA 5500 to Generate Syslog Events

Enter the following global-configuration command:

```
logging host inside ip-address-of-loglogic
```

For example, if the LogLogic appliance has IP address 10.4.200.112, enter: logging host inside 10.4.200.112

Press Ctrl + Z to exit config mode, and then type the following command to save the configuration changes:

```
copy running-config startup-config
```

Configuring a Cisco ISR to Generate Syslog Events

Enter the following global-configuration command:

```
logging ip-address-of-loglogic
```

For example, if the LogLogic appliance has IP address 10.4.200.112, enter: logging 10.4.200.112

Press Ctrl + Z to exit config mode, and then type the following command to save the configuration changes:

```
copy running-config startup-config
```

Note that no special configuration steps are required on the LogLogic appliance in order to receive syslog messages.

Retrieving Event Records from Cisco Intrusion Prevention System (IPS) Sensors

This section describes the configuration steps on a Cisco IPS 4200 Series device to allow a LogLogic appliance to collect security events using the Security Device Event Exchange (SDEE) protocol.

Configuring a Cisco IPS 4200 for SDEE

To allow SDEE to function properly, the IPS must allow access to its HTTP or HTTPS service, and must also provide a username and password that the LogLogic appliance can use to authenticate its requests. The viewer privilege is sufficient to retrieve SDEE events, so a good security practice is to create a separate username for this purpose with the minimum privilege level required. For example, to create a user named “sensor”, type the following configuration command on the IPS:

```
username sensor privilege viewer
```

The IPS will prompt you to choose the password for the user.

Setting Up a LogLogic Universal Collector to Retrieve SDEE Events from Cisco IPS 4200 Series Sensors

This section provides an overview on setting up the LogLogic Universal Collector (UC) and Universal Collector Manager (UCM) using the GUI in order to collect Cisco IPS events via SDEE.

Prior to configuring the UC ensure that you meet the following prerequisites:

- Proper UCM and UC application up and running (please refer to the LogLogic UC documentation for details)
- User configured on the Cisco IPS sensor with at least viewer privilege
- HTTP or HTTPS server running on the Cisco IPS sensor

Step 1: Log Source Settings

In the UC GUI, go to **Collector Management > Add a log source** and select **Cisco IDS/IPS through SDEE**. Specify the address of the LogLogic LMI appliance to which the logs will be forwarded, and then create the Cisco IPS host entry, making sure to specify the IP address.

Step 2: Log Collector Settings

Select the collector you want to use (we recommend that you use a remote log collector), and then select the way the server is connecting to the log collector.

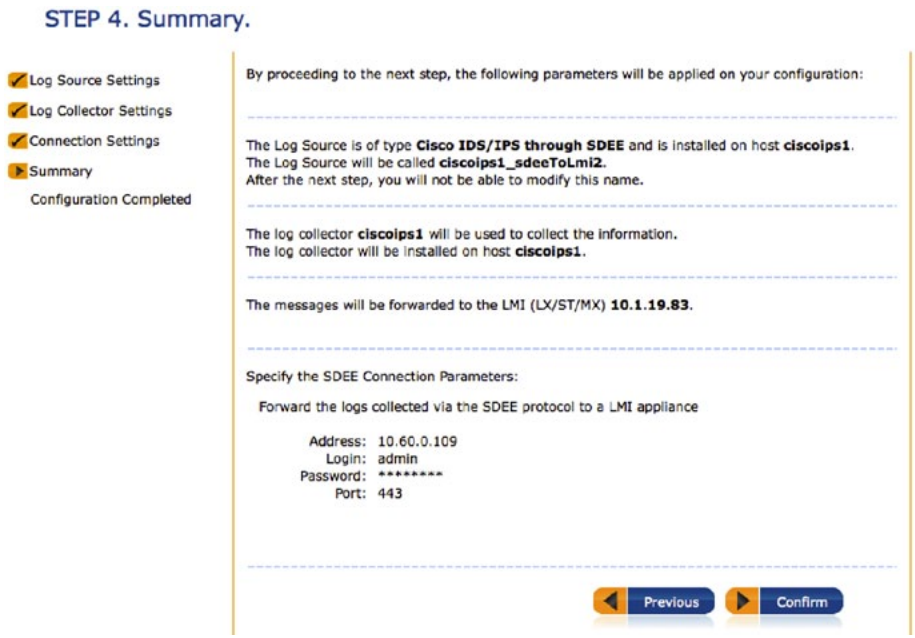
Step 3: Connection Settings

Specify the SDEE Connection Parameters of the Cisco IPS sensor, including IP address, login name, password, and port.

Step 4: Summary

Confirm the configuration as shown in Figure 8, and the UC configuration will be updated automatically.

Figure 8. Final Step of Configuring Universal Collector for SDEE



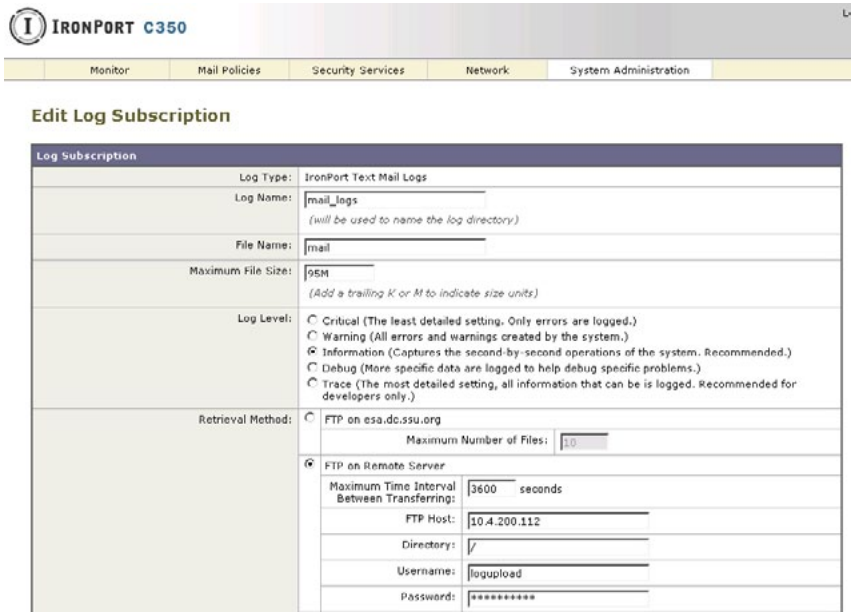
Sending Cisco IronPort Email Security Appliance Logs to an Intermediate Host

This section describes the configuration steps involved to send logs from a Cisco IronPort Email Security Appliance to an FTP server on your network, from which the LogLogic appliance will then retrieve them. There are numerous logs maintained by the Cisco IronPort Email Security Appliance; in the example below, we demonstrate how to export the IronPort Text Mail Logs.

Configuring a Log Subscription for Mail Logs

1. In the Email Security Appliance web management interface, go to **System Administration > Log Subscriptions** and click **Add Log Subscription**.
2. Select **IronPort Text Mail Logs** from the **Log Type** drop-down list.
3. Provide a **Log Name**, which will be used to name the directory created on the FTP server to hold the log files, and a **File Name**, which will be used as the basis for the individual log file names within that directory.
4. Next to **Retrieval Method**, select **FTP on Remote Server** and supply the FTP information for an intermediate host on your network, to which the Cisco IronPort Email Security Appliance will push the log files, as shown in Figure 9.

Figure 9. Log Subscription Configuration on the Cisco IronPort Email Security Appliance



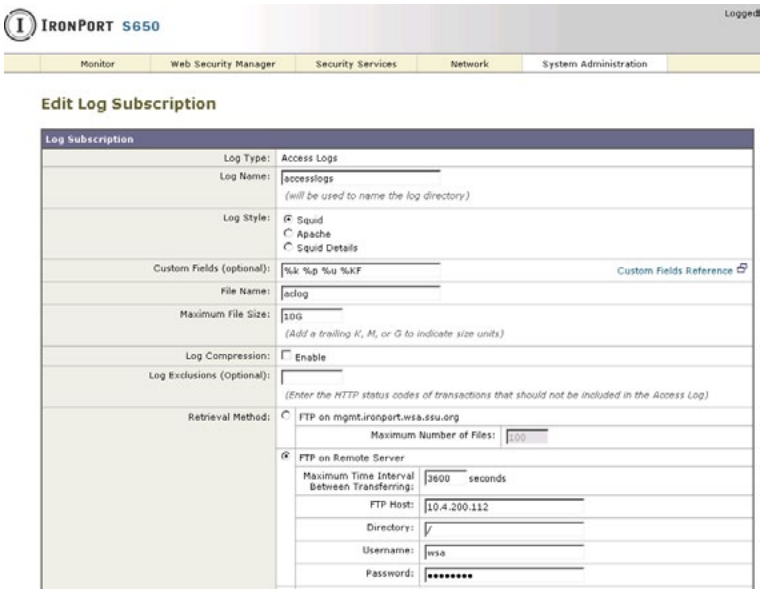
Sending Cisco IronPort Web Security Appliance Logs to an Intermediate Host

This section describes the configuration steps involved to send logs from a Cisco IronPort Web Security Appliance to an FTP server on your network, from which the LogLogic appliance will then retrieve them. There are numerous logs maintained by the Cisco IronPort Web Security Appliance; in the example below, we demonstrate how to export Access Logs.

Configuring a Log Subscription for Access Logs

1. In the Web Security Appliance management interface, go to **System Administration > Log Subscriptions** and click **Add Log Subscription**.
2. Select **Access Logs** from the **Log Type** drop-down list. Leave Log Style set to the default value of **Squid**.
3. Provide a **Log Name**, which will be used to name the directory created on the FTP server to hold the log files, and a **File Name**, which will be used as the basis for the individual log file names within that directory.
4. Next to **Retrieval Method**, select **FTP on Remote Server** and supply the FTP information for an intermediate host on your network, to which the Cisco IronPort Web Security Appliance will push the log files, as shown in Figure 10.

Figure 10. Log Subscription Configuration on the Cisco IronPort Web Security Appliance



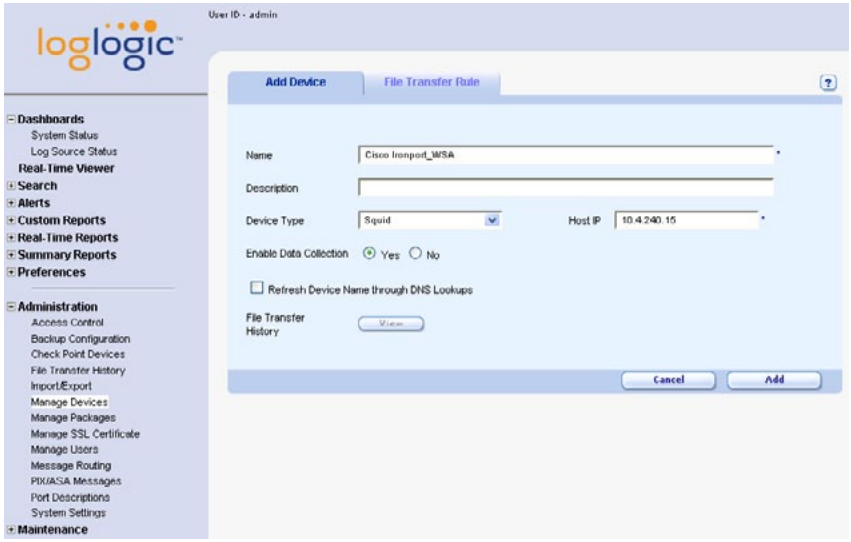
Configuring the LogLogic Appliance to Receive Logs from Cisco IronPort Web and Email Security Appliances

This section shows how to configure LogLogic to import the log files from the intermediate FTP server, configured in the previous procedure. Use the **Add File Transfer** tab to add a remote log source from which you intend to transfer files. After you have added all the remote log sources, you can specify rules using the **File Transfer Rules** feature.

Step 1: Add the FTP Server as a New Device

1. In the LogLogic web management interface, go to **Administration > Manage Devices** and select the **Devices tab**
2. Click **Add New**.
3. In the **Name** field, type a name for the log source.
4. Type an optional description in the **Description** field.
5. From the **Device Type** drop-down menu, select the type of logs to be transferred; for example, for Access Logs from a Cisco IronPort Web Security Appliance, select **Squid**.
6. In the **Host IP** field, type the IP address of the FTP server from which you want to transfer files.
7. Set **Enable Data Collection** to **Yes**.
8. Click **Add**.

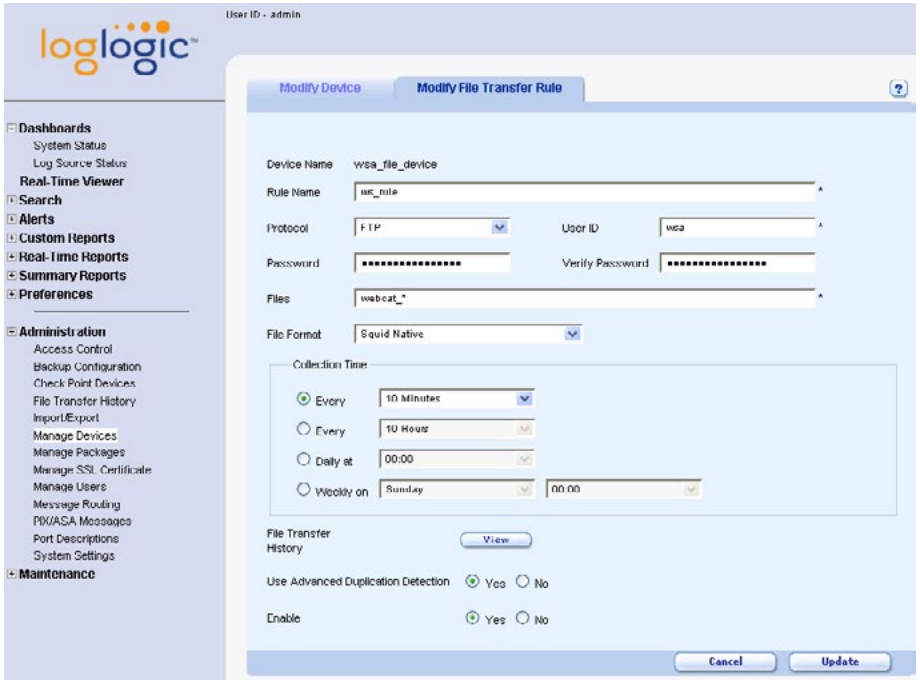
Figure 11. Adding a New Device



Step 2: Define a File Transfer Rule

1. Select the **File Transfer Rule** tab.
2. Ensure that the device you created in Step 1 is selected, and click **Add Rule**
3. In the resulting **Add File Transfer Rule** tab, enter a name for this rule in the **Rule Name** field
4. Leave **Protocol** set to **FTP**, and enter the FTP configuration information in the **User ID**, **Password**, and **Verify Password** fields.
5. In the **Files** field, enter the path and file name of the log files on the FTP server. Note that the file name will be the same as the log file name on the Cisco IronPort Email or Web Security Appliance.
6. Under **Collection Time**, select the desired file collection interval.
7. Set **Enable** to **Yes**.
8. Click **Add**.

Figure 12. Configuring a File Transfer Rule



Exporting Event Records from Cisco Security MARS to the LogLogic Appliance

This section describes the configuration steps involved to enable archive file export on Cisco Security MARS.

Configuring Cisco Security MARS to Export Archive Files

The Cisco Security MARS appliance can export archive copies of events, sessions, and raw messages (ES files). The archives can be saved to an external network-attached storage (NAS) system or other host using the Network File System (NFS) or Secure FTP (SFTP) protocols. Raw event records are exported at ten-minute intervals.

You can use the same server to archive the data for more than one Cisco Security MARS appliance; however, you must specify a unique directory in the path for each appliance that you want archive. If you use the same base directory, the appliances overwrite each other's data, effectively corrupting the images.

For information on enabling archive file export, please see the "Backup, Recover, Restore, and Standby Server Options" chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide* at the following URL: http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/initial/configuration/bckRstrSby.html#wp1270005.

Adding Devices Monitored by the LogLogic Appliance

This guide assumes that you have already configured Cisco Security MARS to receive event logs from the other Cisco devices on your network. Those logs are passed along from Cisco Security MARS to the LogLogic appliance in the raw event records, exactly in the form they were received. To load the records into LogLogic, perform the following steps. Note that while Cisco Security MARS uses either NFS or SFTP to export its logs, the LogLogic appliance can use any supported transfer mechanism to import the files.

Step 1: Add the File Server as a New Device

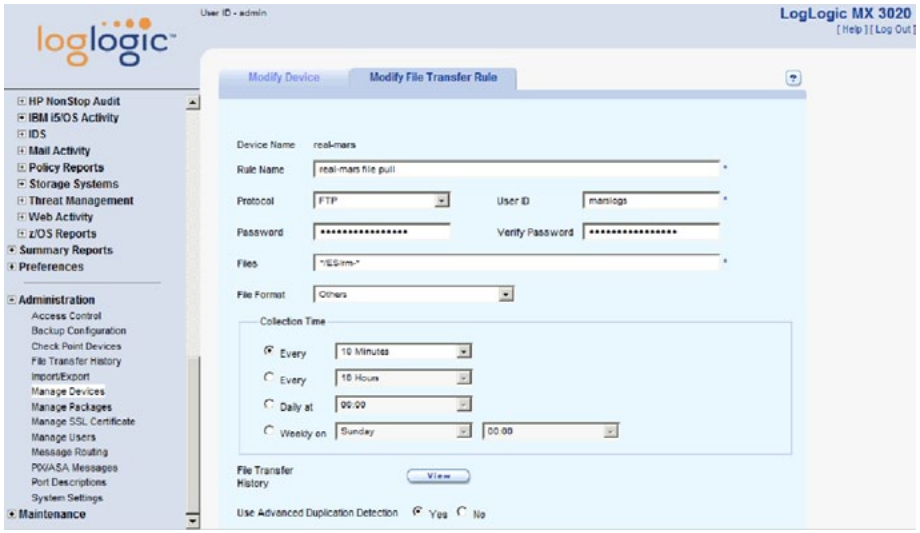
1. In the LogLogic web management interface, go to **Administration** > **Manage Devices** and select the **Devices** tab
2. Click **Add New.**
3. In the **Name** field, type a name for the log source.
4. Type an optional description in the **Description** field.
5. From the **Device Type** drop-down menu, select **Other File Device**.

6. In the **Host IP** field, type the IP address of the server from which you want to transfer files.
7. Set **Enable Data Collection** to **Yes**.
8. Click **Add**.

Step 2: Define a File Transfer Rule

1. Select the **File Transfer Rule** tab.
2. Ensure that the device you created in Step 1 is selected, and click **Add Rule.**
3. In the resulting **Add File Transfer Rule** tab, enter a name for this rule in the **Rule Name** field
4. Select the appropriate **Protocol**, and enter the required configuration.
5. In the **Files** field, enter the ***/ES/rm-*** to collect all of the raw message files.
6. Under **Collection Time**, select the desired file collection interval. Remember that Cisco Security MARS exports archive files at ten-minute intervals, regardless of the LogLogic configuration.
7. Set **Enable** to **Yes**.
8. Click **Add**.

Figure 13. File Transfer Configuration for Cisco Security MARS



Notes

Searching and Generating Reports

LogLogic's searching and reporting capabilities enable users to search, analyze and make sense of log data from a wide variety of connected log sources quickly and effectively. Users can use LogLogic's reporting capabilities to create customizable real-time reports, send information to executives at regular intervals, and perform ad-hoc searches for troubleshooting or issue remediation. The LogLogic solution ships with built-in intelligence and report templates for access control, user accounting, network connectivity and policy, IDS and VPN activity, and web surfing activity. Report templates can easily be customized to suit the end-user's particular reporting requirements. Reports can be generated, emailed, and exported as PDF or CSV files on demand.

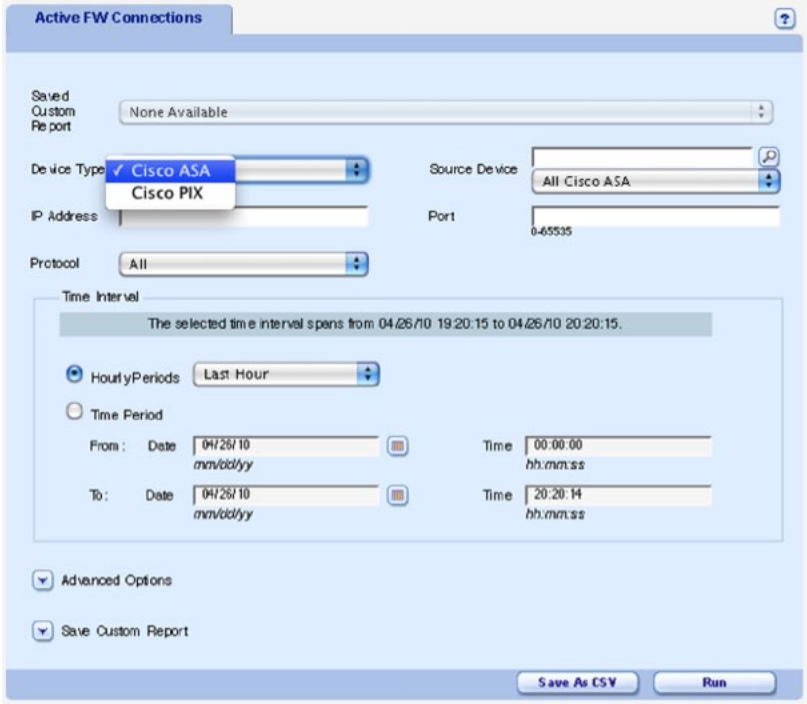
In addition, LogLogic also offers high-speed full-text indexed raw log data search capabilities. This combines keyword search features with data querying features into one overall search process. The keyword search for log messages uses Boolean expressions; AND, OR, and NOT are applied as logical operators to help users focus searches on the messages of interest. Data querying settings assure that all messages satisfying specified criteria (not just those assumed to be most relevant) are delivered, sorted by time. LogLogic's index search delivers only those messages which fully satisfy the Boolean search criteria. Finally, advanced regular expression searches add more power to searches.

Generating Reports

Report Configuration

Real-time reports are can be configured and customized freely. LogLogic's dynamic report configuration page provides options for the users to customize everything pertaining to the summarization and presentation of the reports. For example, the following figure shows that users can choose the devices or device groups as well as the timeframe in which the reports should be run. Users can choose to run reports for the last hour, or specify a time range, as illustrated in Figure 14.

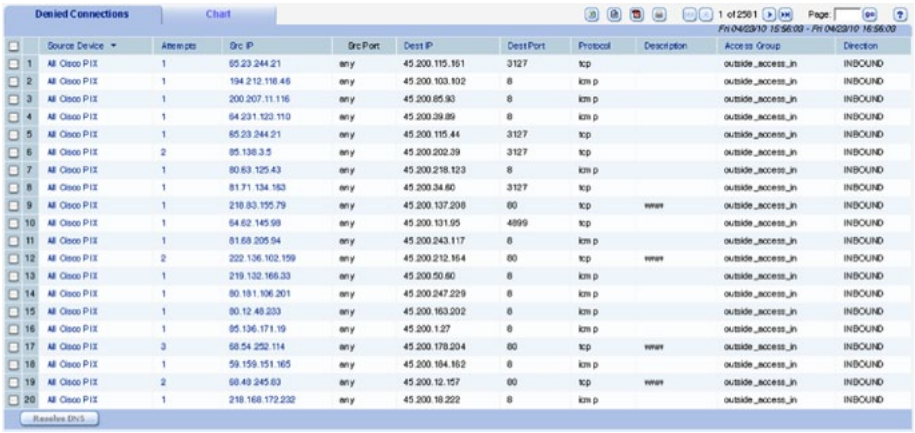
Figure 14. Reporting Active Firewall Connections



Report Results

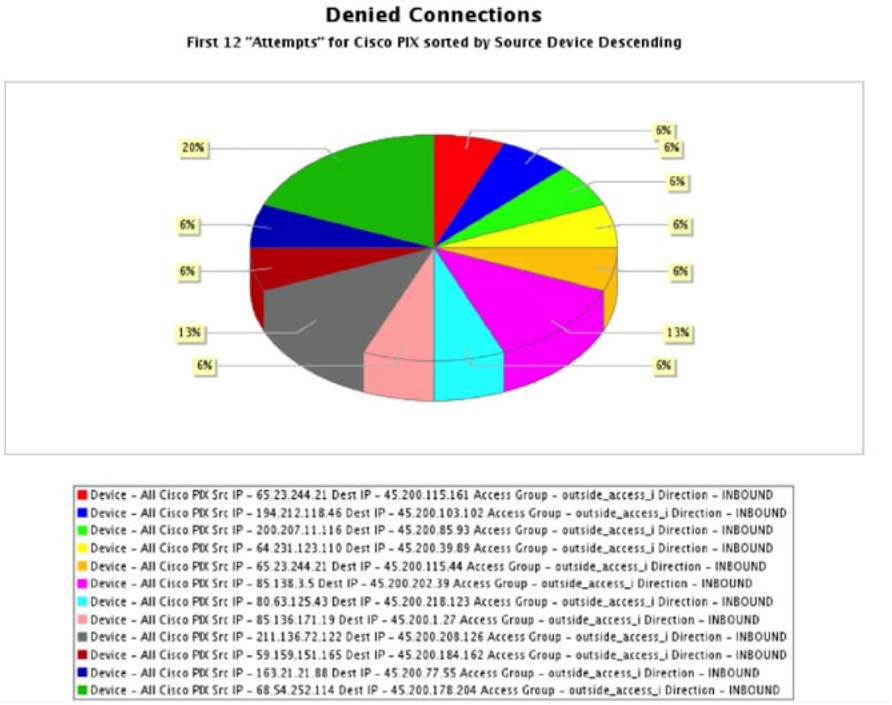
After the report configuration parameters are chosen, pressing the **Run** button on the lower right of the screen will cause the specified report to be executed. An example **Denied Connections** report is shown in Figure 15.

Figure 15. A Sample Report



In addition, by selecting the **Chart** tab, a chart of the associated report will be displayed.

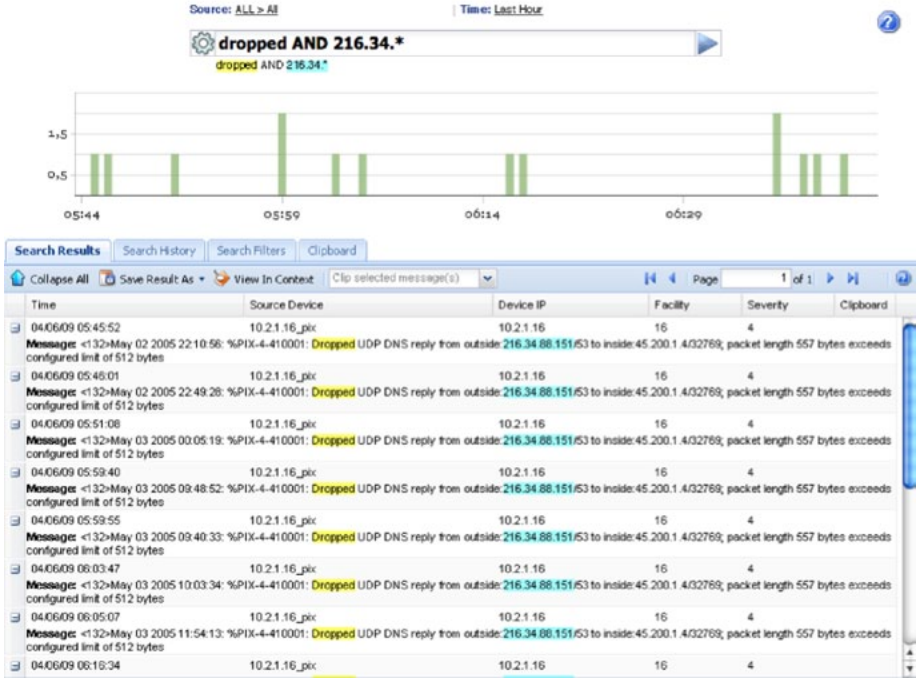
Figure 16. A Sample Chart



Index Search

Index searches are accessed via the **Search** > **IndexSearch** navigation menu item. An example Index Search result is show in Figure 17.

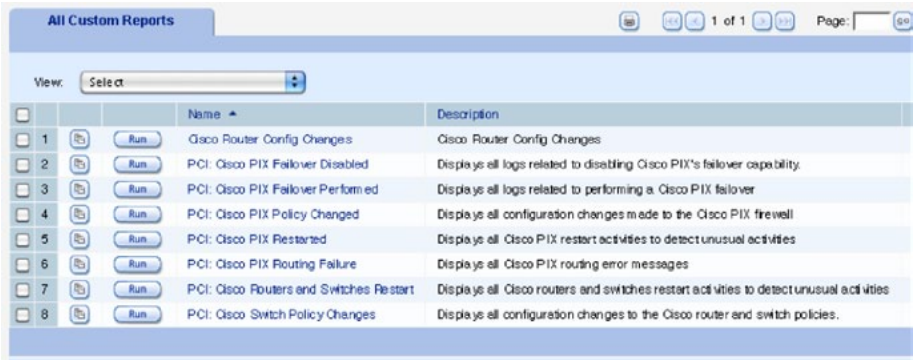
Figure 17. Index Search Example



Compliance Reports

LogLogic Compliance Suites deliver automated process validation, reporting and alerts based on infrastructure data to evidence, and enforce agency and IT policies related to compliance. By automating compliance reporting and alerting based on critical infrastructure data collected and stored by LogLogic Appliances, the LogLogic Compliance Suites reduce complexity and resource requirements for implementing control frameworks like PCI, COBIT/SOX, HIPAA, HITECH, FISMA, ITIL, ISO, and NERC. Each LogLogic Compliance Suite delivers 100+ reports and 75+ alerts—both easily customizable—specifically tuned to a particular control framework, for execution on LogLogic Appliances.

Figure 18. Customized Compliance Reports



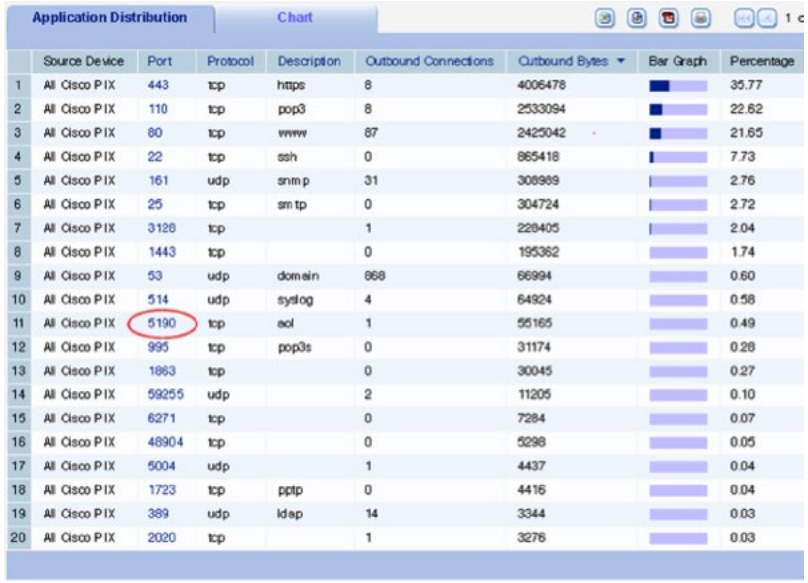
Notes

LogLogic Example

The following example scenario shows how an Application Distribution report, using logs from an agency's Cisco ASA 5500 Series firewall, can reveal anomalous patterns in network usage, and help to detect malicious or other undesirable activity.

The Application Distribution report can be used to validate that corporate network policies, such as permissible network applications, network bandwidth QoS, and so on, are being followed. The report can be accessed in the web interface by going to **Real-Time Reports > Connectivity > Application Distribution**. An example report is shown in Figure 19. The example shows fairly common network traffic, including web browsing on ports 80 and 443, email traffic on ports 25 and 110, domain lookups, and management traffic. However, note the highlighted outbound TCP session on port 5190, associated with AOL Instant Messenger (AIM) traffic. In our example, this calls for closer investigation, possibly because the agency's network policies do not permit this chat client to be used.

Figure 19. Application Distribution Report Example



Application Distribution | Chart

	Source Device	Port	Protocol	Description	Outbound Connections	Outbound Bytes	Bar Graph	Percentage
1	All Cisco PIX	443	tcp	https	8	4006478		35.77
2	All Cisco PIX	110	tcp	pop3	8	2533094		22.62
3	All Cisco PIX	80	tcp	www	87	2425042		21.65
4	All Cisco PIX	22	tcp	ssh	0	865418		7.73
5	All Cisco PIX	161	udp	snmp	31	308969		2.76
6	All Cisco PIX	25	tcp	smtp	0	304724		2.72
7	All Cisco PIX	3128	tcp		1	228405		2.04
8	All Cisco PIX	1443	tcp		0	195362		1.74
9	All Cisco PIX	53	udp	domain	868	66994		0.60
10	All Cisco PIX	514	udp	syslog	4	64924		0.58
11	All Cisco PIX	5190	tcp	aol	1	55165		0.49
12	All Cisco PIX	995	tcp	pop3s	0	31174		0.28
13	All Cisco PIX	1863	tcp		0	30045		0.27
14	All Cisco PIX	59255	udp		2	11205		0.10
15	All Cisco PIX	6271	tcp		0	7284		0.07
16	All Cisco PIX	48904	tcp		0	5298		0.05
17	All Cisco PIX	5004	udp		1	4437		0.04
18	All Cisco PIX	1723	tcp	pptp	0	4416		0.04
19	All Cisco PIX	389	udp	ldap	14	3344		0.03
20	All Cisco PIX	2020	tcp		1	3276		0.03

Clicking on the 5190 port number in the Application Distribution report shows details about the individual connections, and reveals that there are a number of internal users at IP address 45.200.x.y interacting with AOL servers. In this example scenario, this indicates widespread policy violations, suggesting the need to adjust outgoing firewall rules, and also to increase user awareness of the acceptable use policy on the network.

Figure 20. Detailed Investigation Example

Accepted Connections | Chart

	Source Device	Source IP	Destination IP	Port	Description	Messages	In Bytes	Out Bytes
1	All Cisco PIX	205.188.12.92	45.200.1.229	tcp /5190	aol	9	46925	0
2	All Cisco PIX	64.12.28.236	45.200.1.229	tcp /5190	aol	7	337633	0
3	All Cisco PIX	205.188.248.144	45.200.1.229	tcp /5190	aol	6	10878	0
4	All Cisco PIX	64.12.24.188	45.200.99.238	tcp /5190	aol	5	125510	0
5	All Cisco PIX	64.12.201.36	45.200.99.246	tcp /5190	aol	5	9460	0
6	All Cisco PIX	45.200.99.246	64.12.201.36	tcp /5190	aol	4	0	7568
7	All Cisco PIX	207.200.122.170	45.200.40.45	udp /5190	aol	4	19995	0
8	All Cisco PIX	64.12.29.75	45.200.99.238	tcp /5190	aol	3	10302	0
9	All Cisco PIX	64.12.161.185	45.200.99.254	tcp /5190	aol	3	2063	0
10	All Cisco PIX	64.12.28.236	45.200.99.246	tcp /5190	aol	3	105254	0
11	All Cisco PIX	45.200.1.229	64.12.28.236	tcp /5190	aol	2	0	70495
12	All Cisco PIX	64.12.26.56	45.200.99.254	tcp /5190	aol	2	12303	0
13	All Cisco PIX	205.188.153.121	45.200.99.246	tcp /5190	aol	2	1398	0
14	All Cisco PIX	64.12.24.188	45.200.1.218	tcp /5190	aol	1	26	0
15	All Cisco PIX	207.200.122.163	45.200.1.231	udp /5190	aol	1	24	0
16	All Cisco PIX	205.188.12.96	45.200.99.249	tcp /5190	aol	1	17164	0
17	All Cisco PIX	64.12.165.89	45.200.99.246	tcp /5190	aol	1	886	0
18	All Cisco PIX	64.12.161.185	45.200.1.218	tcp /5190	aol	1	630	0
19	All Cisco PIX	205.188.72.10	45.200.1.213	tcp /5190	aol	1	70609	0
20	All Cisco PIX	64.12.28.208	45.200.1.225	tcp /5190	aol	1	6216	0

Products Verified with Cisco SBA

LogLogic MX 3020 Appliance version 4.9.0.1 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

Contact Information

End Users

- Please contact sales@loglogic.com with any questions
- Submit an inquiry about Loglogic Products and the Cisco SBA for Large Agencies—Borderless Networks

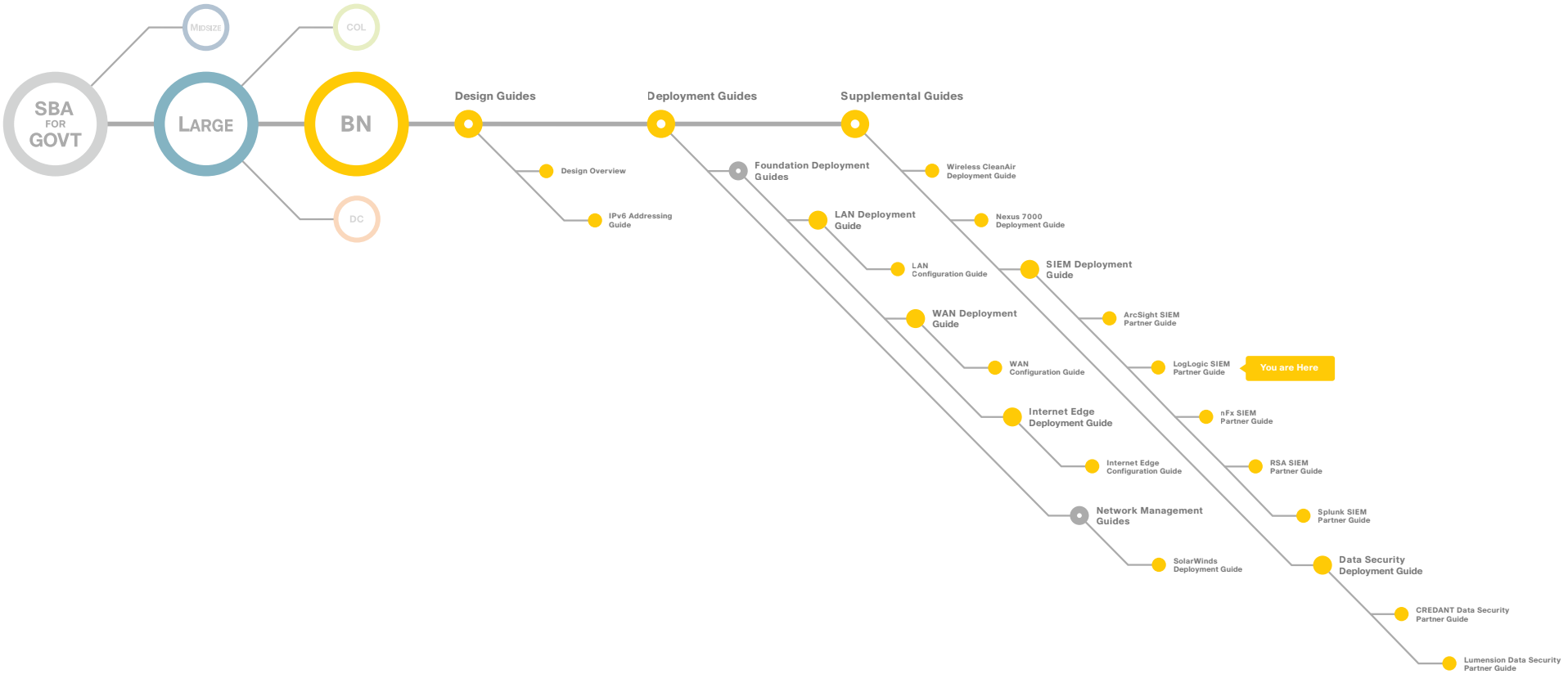
Resellers

- Please contact info@loglogic.com for any questions
- For more information on how to become a LogLogic reseller, please visit the Partner Section at http://www.loglogic.com

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

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.**

C07-641093-00 12/10