ArcSight SIEM Partner Guide

SBA FOR GOVERNMENT

Revision: H2CY10

Using this Data Security Deployment Guide

This document is for the reader who:

- Has read the ***Cisco Security Information and Event Management Deployment Guide*** and the Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks deployment guides
- Wants to connect Borderless Networks to an Arcsight SIEM solution
- Wants to gain a general understanding of the Arcsight 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

BN — Design Overview

BN — Internet Edge Deployment Guide

BN — Internet Edge Configuration Guide

BN — SIEM Deployment Guide

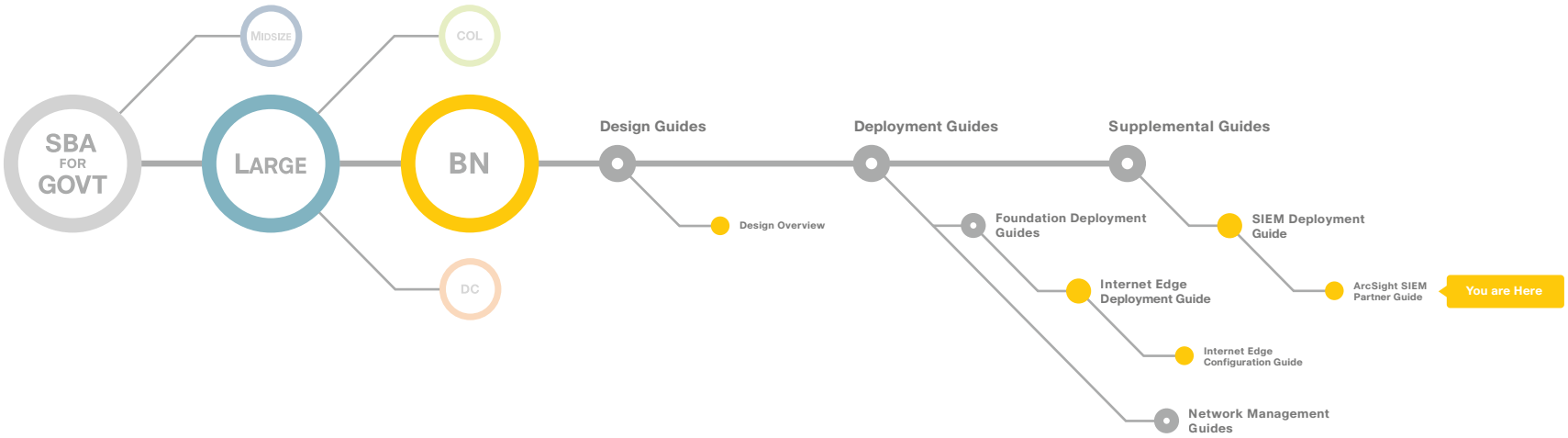


Table of Contents

Cisco SBA for Large Agencies—Borderless Networks

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

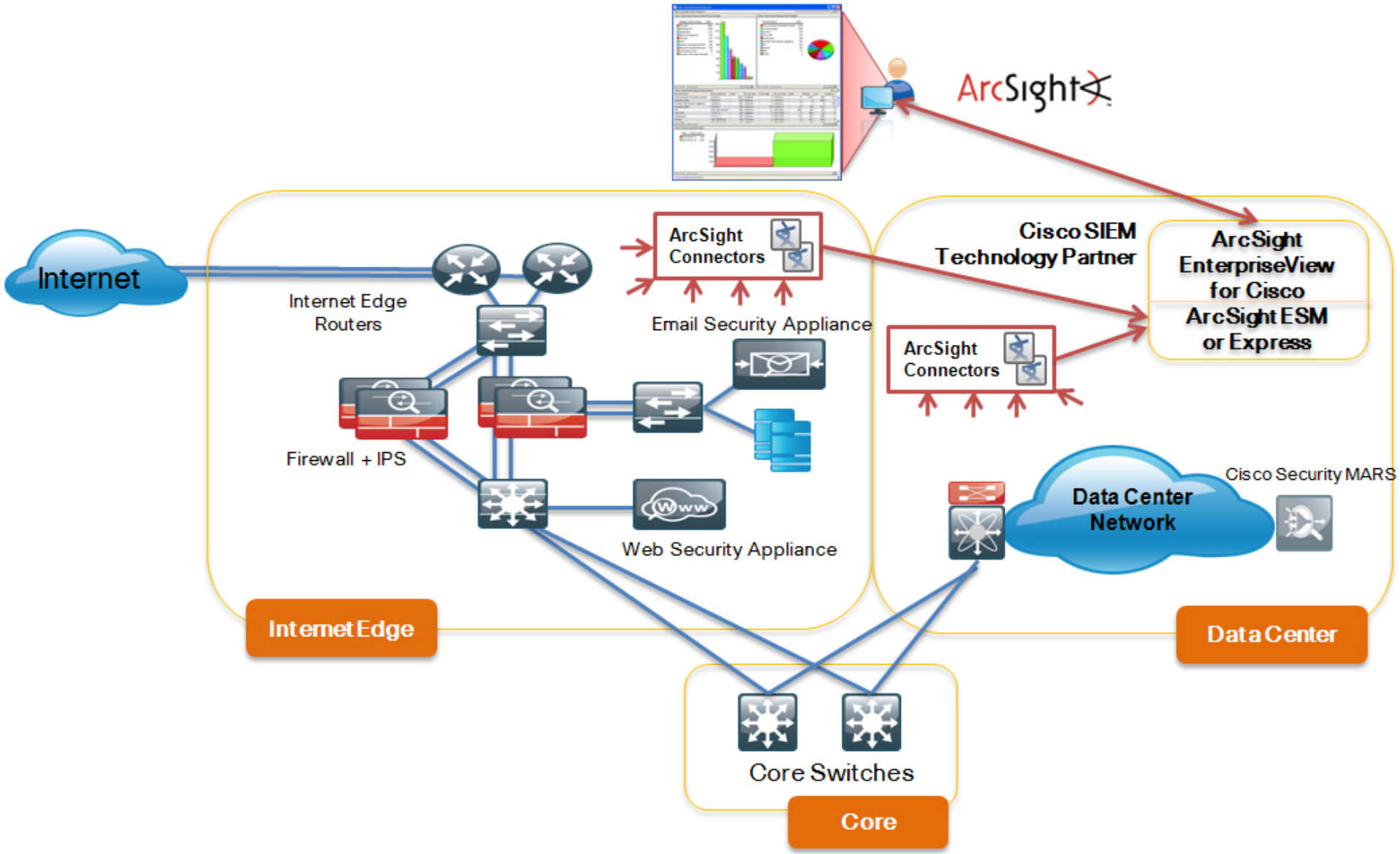
The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. The architecture also provides Cisco-tested configurations and topologies that CCNA-level engineers can use for design and installation, and to support agency needs.

Cisco offers a number of options to provide security management capabilities. This guide is focused on our partnership with ArcSight and integration with their products to provide a comprehensive Security Information and Event Management (SIEM) solution.

ArcSight Connectors (Smart Connectors) collect event data from Cisco network devices. They can normalize, categorize, and aggregate event data, and securely and efficiently deliver events to ArcSight ESM or ArcSight Express (which combines ArcSight Logger and ESM functions for smaller installations). ArcSight Console provides the dashboard for the security operations center (SOC). ArcSight web-based consoles can be used for IT operations staff for searching through archived log data and generating compliance reports

Notes

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



Agency Benefits

Agency networks are growing rapidly in size and complexity, linked with suppliers, customers, and operational partners. The network perimeter has dissolved and the notion of external versus internal threats has blurred. As a result, agencies became increasingly focused on correlating network activity with user activity monitoring in the context of transactions on critical assets.

Agencies are looking for a mission-critical IT and security operations solution that provides the agency-wide threat management, real-time correlation/response, and flexible monitoring and reporting capabilities to meet their rigorous regulatory compliance needs.

ArcSight, a leader in SIEM, provides solutions that serve as the mission control center for real-time agency-wide threat management, compliance reporting and automated network response.

The ArcSight EnterpriseView for Cisco application adds powerful predefined content (correlation rules, dashboards and reports) that allows customers to monitor activity, configuration changes, availability, and threats across their Cisco infrastructure. In addition, this application correlates alerts from Cisco infrastructure with security events from rest of the agency, and provides a comprehensive risk and threat management solution to meet regulatory compliance needs.

Next Generation Risk and Threat Management Solution

- Helps security operations keep pace in monitoring Cisco networks
- Correlates identity information from multiple sources, with reputation data from Cisco SensorBase improves accuracy on security alerts
- Enables comprehensive visibility, monitoring and reporting across Cisco product portfolio

Customized Event Correlation, Response, and Reporting for Cisco Infrastructure

- Provides Cisco specific content (rules, reports, dashboards) for rapid return on investment (ROI) with ArcSight EnterpriseView for Cisco
- Collects and correlates events from hundreds of non-Cisco products, and allows you to rapidly respond to threats
- Proactively minimizes or eliminates vulnerabilities that could impact operations.

Faster ROI for Security and IT-Operations and Reduced Compliance Risk

- Compliments Cisco Security MARS deployments by adding compliance reporting and support for event logging from multiple vendors
- Provides a cost-effective long term storage for log data to investigate faults for IT operations
- Streamlines compliance process for various corporate regulations, such as Sarbanes-Oxley, PCI, HIPAA, SB1386, and Basel II.

Technology Partner Solution Overview

ArcSight EnterpriseView for Cisco

ArcSight EnterpriseView for Cisco provides powerful pre-defined content (correlation rules, dashboards and reports) that allows customers to monitor activity, configuration changes, availability, and threats across their Cisco infrastructure. This application (content pack) runs on existing ArcSight SIEM platform installations and depends on SmartConnectors for the Cisco devices to be installed and configured appropriately.

Figure 2. The ArcSight SIEM Architecture

ArcSight SIEM Platform

The ArcSight SIEM Platform is an award-winning set of products for monitoring threat and risk. Most agency networks are effectively borderless; external systems and users access internal systems and data as part of normal operations. In a borderless environment, a comprehensive monitoring platform brings security and visibility without impacting flexible agency operations. All ArcSight SIEM platform products listed below leverage the same monitoring infrastructure (ArcSight SmartConnectors) to capture, normalize, and categorize events and logs from Cisco networking and security devices.

ArcSight ESM

ArcSight ESM protects demanding private and public organizations throughout the world. Using its broad log data collection capability, combined with its powerful event correlation engine, ArcSight ESM can detect sophisticated threats crossing multiple types of security products. ArcSight ESM extends the reach of Cisco threat management and response, by performing sophisticated event correlation of Cisco network events and alerts with a broader set of agency-wide event-sources (systems, databases, and applications). As a result, customers can detect threats in time to take effective action.

ArcSight Logger

ArcSight Logger provides cost-effective long term log management and storage, as well as automated compliance reporting. By storing up to 42 TB of log data on a single appliance while supporting search speeds of millions of events per second across structured and unstructured data. ArcSight Logger brings a flexible means of storing event data from Cisco networking devices for years. ArcSight Logger supports automated reporting for SOX, PCI DSS, NERC and other regulations, integrating Cisco Security MARS data with other agency information.

ArcSight Express

ArcSight Express includes the industry leading real-time correlation and log management technologies from ESM and Logger, in one pre-packaged easy-to-use SIEM solution for the mid-market. Express is referred to as the “security expert in a box”, and has several built-in correlation rules, dashboards, and compliance reports. ArcSight Express provides a rapidly deployable, low cost mid-market solution for monitoring Cisco infrastructure.

ArcSight SmartConnectors

ArcSight SmartConnectors collect event data from network devices, and they normalize the data structure into common schema, add severity, priority, and time zone. SmartConnectors can optionally filter out data that you know is not needed for analysis, saving network bandwidth and storage space. It can aggregate events to reduce the quantity of events of the same type, thus improving efficiency. It can categorize events using the common, human-readable formats, making it easier to use those events to build filters, rules, and reports.

Table 1. Comparison of ArcSight SIEM Products

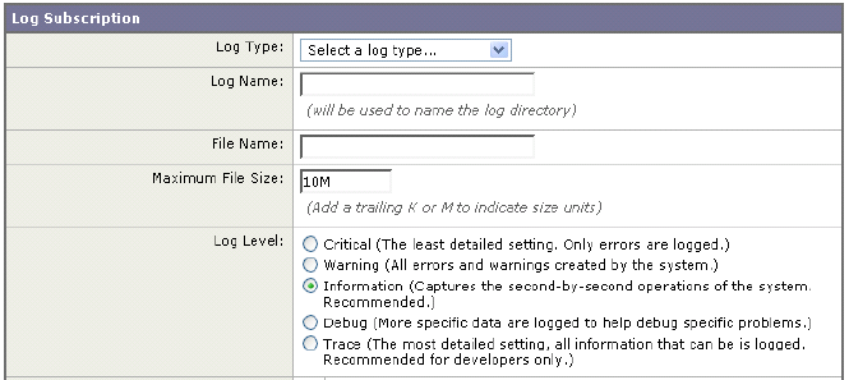
	ArcSight ESM	**ArcSight Logger**	**ArcSight Express**
Description	Real-time Event Correlation and Reporting	Long-term Event Logging and Reporting	Event Correlation and Logging for SMB
No of Users (Admin)	Unlimited	Unlimited	Unlimited
Events Per Second	15K/instance Linearly scalable	100K/instance Linearly scalable	5K/instance Linearly scalable

Deploying ArcSight Express

Following is a brief overview of steps to for set up a Cisco device to send syslog messages to an ArcSight SmartConnector platform, and set up ArcSight SmartConnector to send normalized and categorized Cisco events to any of the following destinations: ArcSight ESM Manager, ArcSight Logger, or ArcSight Express. Refer to the ArcSight SmartConnector Configuration Guide for the specific Cisco device for the detailed setup information.

Setup Cisco Device

1. Configure Log Subscription on Cisco device—type of information recorded and log format
2. Configure the Log Retrieval method—how logs are transferred to ArcSight Connector



Setup ArcSight SmartConnector

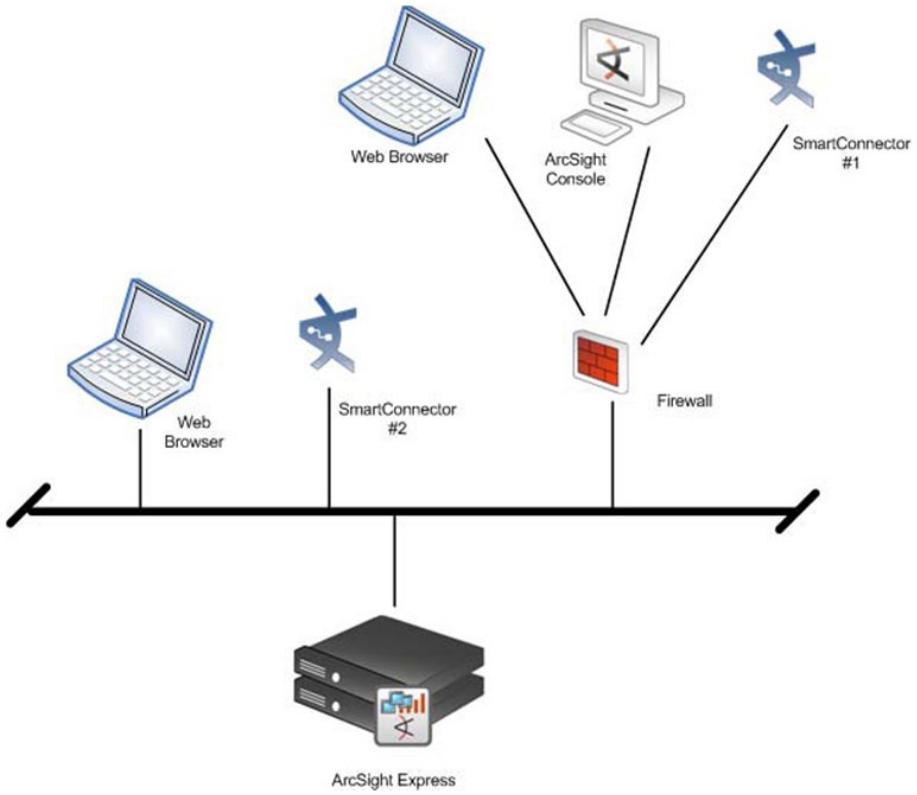
1. Download SmartConnector from ArcSight support website for your specific Cisco device
2. Run SmartConnector Installer
   - Choose install folder and Install Set
   - Select destination of events: Manager, Logger
   - Select destination hostname/port
   - Enter ArcSight admin username and password

ArcSight Express Configuration

This section provides a brief overview of steps to for set up ArcSight Express ("SIEM in a box") a pre-packaged product bundle for small and medium agencies, composed of two appliances. It involves setting up the following. Refer to the ***Configuration Guide: ArcSight Express*** for more details.

- **ArcSight Express:** appliance #1 includes:
  - ArcSight Manager
  - ArcSight Forwarding Connector
  - ArcSight Web (UI)
- **ArcSight Storage:** appliance #2 includes:
  - ArcSight Logger
  - Long-term data storage
  - ArcSight Connector Manager

Figure 3. ArcSight Express Deployment Overview



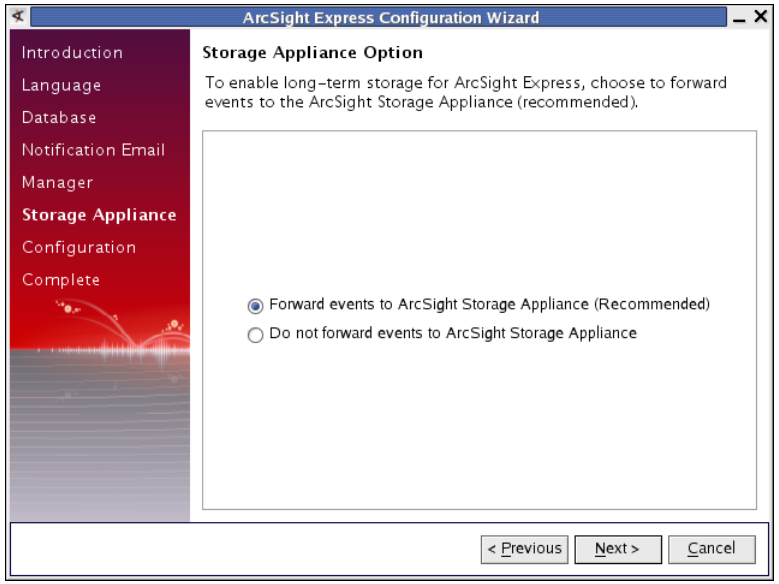
Configure ArcSight Storage Appliance #2 First

1. Define storage volume: where ArcSight Storage Appliance stores event data
2. Create storage groups: apply retention policies for storage volumes
3. Configure Network Time Protocol (NTP) for precise time-stamping of events (highly recommended)
4. Indexing (optional): use default indexing options for better performance. Reboot.
5. Create SmartMessage receivers: to listen on events

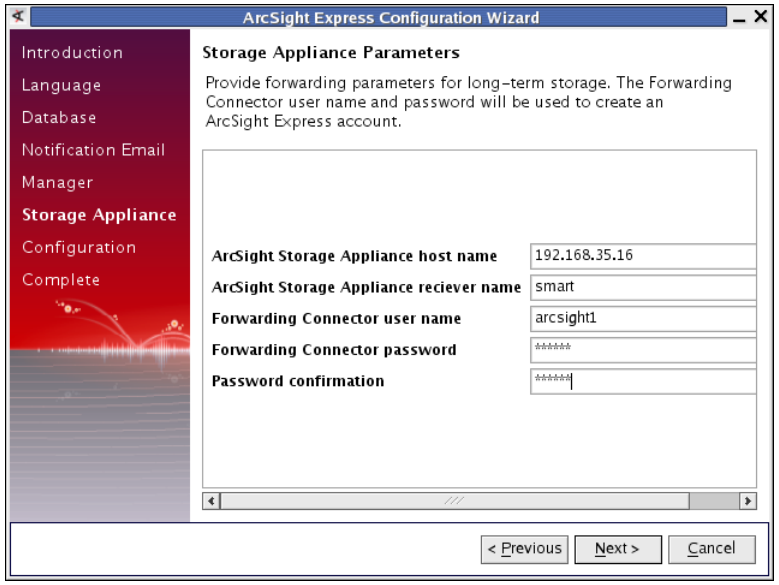
Configure ArcSight Express Appliance #1 Next

1. Configure Oracle Enterprise Linux
2. Configure ArcSight Express software components

3. Select whether you would like to forward events to the ArcSight Storage Appliance for long term storage



4. Enter host name or IP address of the ArcSight Storage appliance and the name of the SmartMessage Receiver created on the ArcSight Storage Appliance.

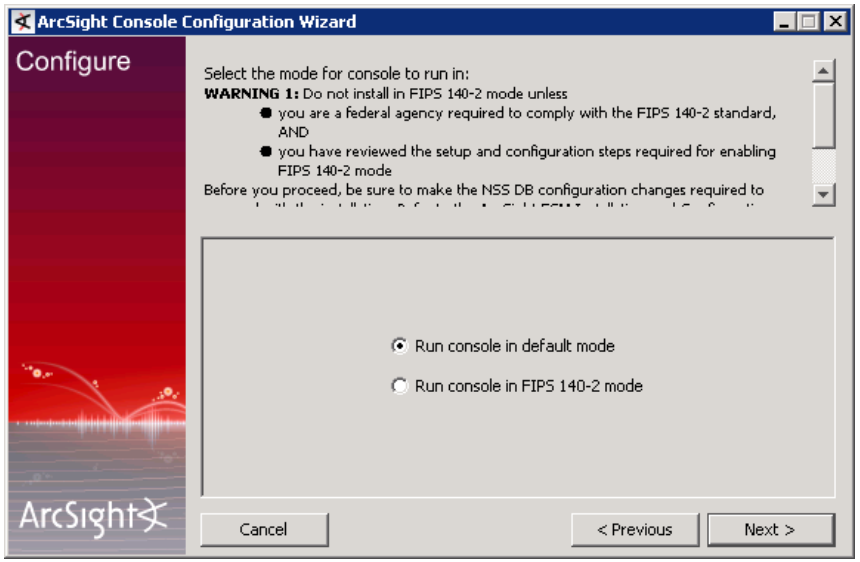


Refer to the ArcSight Express Configuration Guide for more details.

Install the ArcSight Console

ArcSight Console is the primary user interface for performing administrative tasks on ArcSight Express.

1. Install and configure ArcSight Console, and set up connection to ArcSight Manager
2. Create administrative users in ArcSight Express



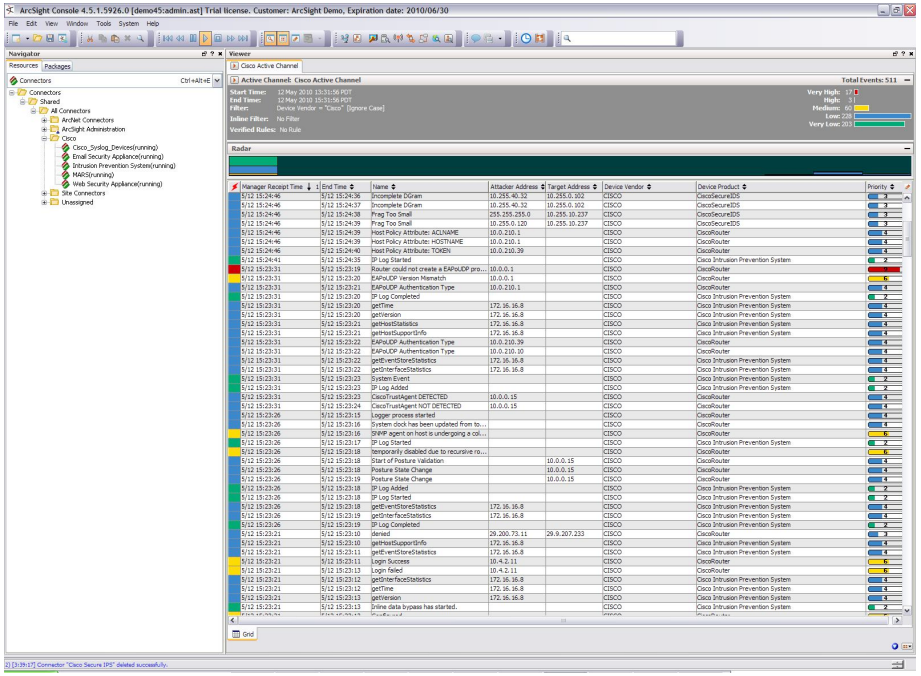
Configure all Cisco SmartConnectors centrally from Connector Manager

You can use the Cisco SmartConnectors that are local to the ArcSight Express appliance. You can also centrally manage multiple remote Cisco SmartConnectors from the ConnectorManager on this appliance. Refer to the ArcSight Express Configuration Guide for more details.

For large agencies, ArcSight Express appliances can be replaced by the following two separate ArcSight products for highly scalable and sophisticated event correlation for security operations, and logging for IT operations. For more details refer to the installation and configuration documents of the respective products listed below.

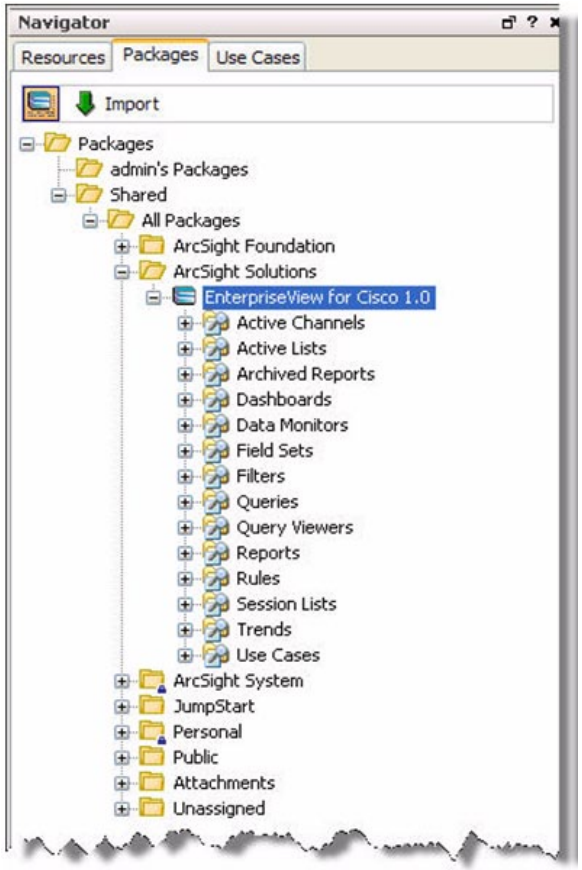
- **ArcSight ESM:** software package includes the following. Refer to the *Installation and Configuration Guide: ArcSight ESM*,
  - ArcSight Manager
  - ArcSight Database
  - ArcSight Console and/or ArcSight Web
- **ArcSight Logger:** appliance includes the following. Refer to the ***ArcSight Logger Getting Started Guide***, and the Installation chapter in the ***ArcSight Logger Administrator's Guide***.
  - ArcSight Logger
  - Long-term data storage—SAN, Storage Volume, Storage Groups

Figure 4. ArcSight Console Showing a List of Cisco SmartConnectors Registered with ArcSight ESM



Install ArcSight EnterpriseView for Cisco Solution Package

1. Download the EnterpriseView for Cisco package from Arcsight software download site (https://software.arcsight.com/)
2. Log into ArcSight Express Console as Administrator, click on **Packages** tab. Click **Import**, select package and follow directions to install package.
3. To verify the package is installed successfully, select **Packages** tab in **Navigator** panel, and expand the **ArcSight Solutions group**.



Notes

Collecting Logs, Events, and Correlated Events

The Cisco Insight Package is a prepackaged set of powerful analysis tools developed by ArcSight that provides that allow you to monitor activity, configuration changes, availability, and threats across Cisco devices in your environment. A comprehensive and easily customizable set of dashboards, active channels, and reports allows you to measure and report on the status of devices and a variety of other activities taking place in your network.

Refer to the *ArcSight Solution Guide: Cisco Insight Package v1.0* for more details on how to collect Cisco logs and events and correlate them with information from the rest of the agency. It provides information on the following:

- Installation and configuration
- Use cases
- Compare, backup and uninstall package

Use cases are targeted collections of presentation, correlation, and data processing resources designed to address a particular requirement or Cisco device. The Cisco Insight Package supports the following use cases:

Use Case	Description
Cisco Overview	The Cisco Overview use case provides high-level reports describing logins, configuration changes, and other events involving Cisco firewalls and Cisco Intrusion Prevention Systems in your environment.
Cisco Cross-Device	The Cisco Cross-Device use case provides information about logins, configuration changes, and bandwidth consumption across all Cisco devices in your environment.
Cisco Generic Firewall	The Cisco Generic Firewall use case identifies and provides firewall information based on events reported by any Cisco firewall device or module in your network.
Cisco Generic Intrusion Prevention System (IPS)	The Cisco Generic IPS use case provides reports and dashboards based on alerts generated by any Cisco IDS/IPS devices or modules.
Cisco Adaptive Security Appliance (ASA)	The Cisco ASA use case provides firewall information based on events reported by Cisco ASA 5500 Series Adaptive Security Appliances.
Cisco IPS Sensor	The Cisco IPS Sensor use case provides event statistics and configuration changes reported by Cisco IPS sensors such as the Cisco IPS 4200 Series appliance, Cisco Catalyst 6500 series Intrusion Detection System Services Module (IDSM), and Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM).
Cisco IOS IPS	The Cisco IOS IPS use case provides event statistics and configuration change information reported by Cisco IOS IPS devices present in your network.
Cisco IronPort Email Security Appliance (ESA)	The Cisco IronPort Email Security Appliance use case identifies and provides web traffic information based on events reported by Email Security Appliances present in your network.
Cisco IronPort Web Security Appliance (WSA)	The Cisco IronPort Web Security Appliance use case identifies and provides web traffic information based on events reported by Web Security Appliances present in your network.
Cisco Network	The Cisco Network use case identifies and provides information based on events reported by Cisco network equipment.

Following are some sample screen shots for Cisco Generic Firewall use cases.

Figure 5. ArcSight Dashboard for Cisco Generic Firewall events

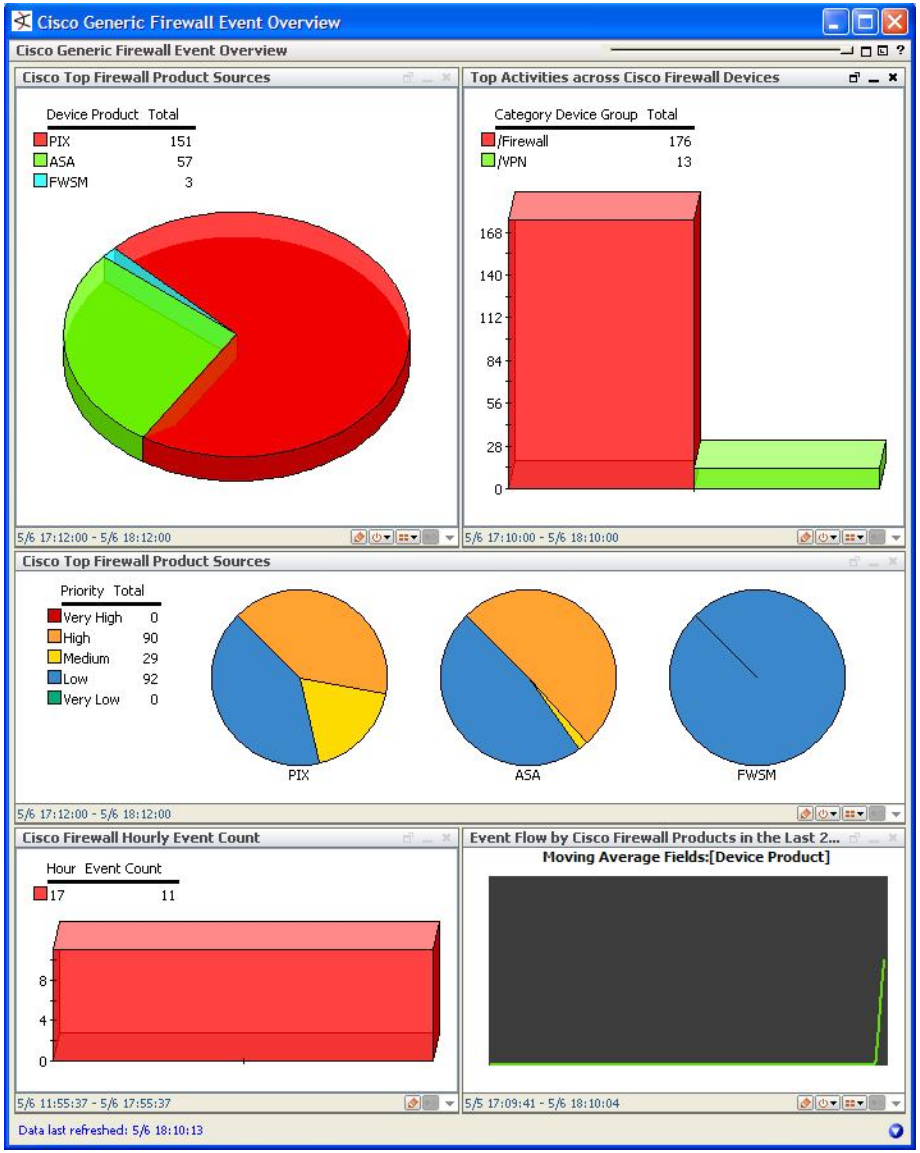
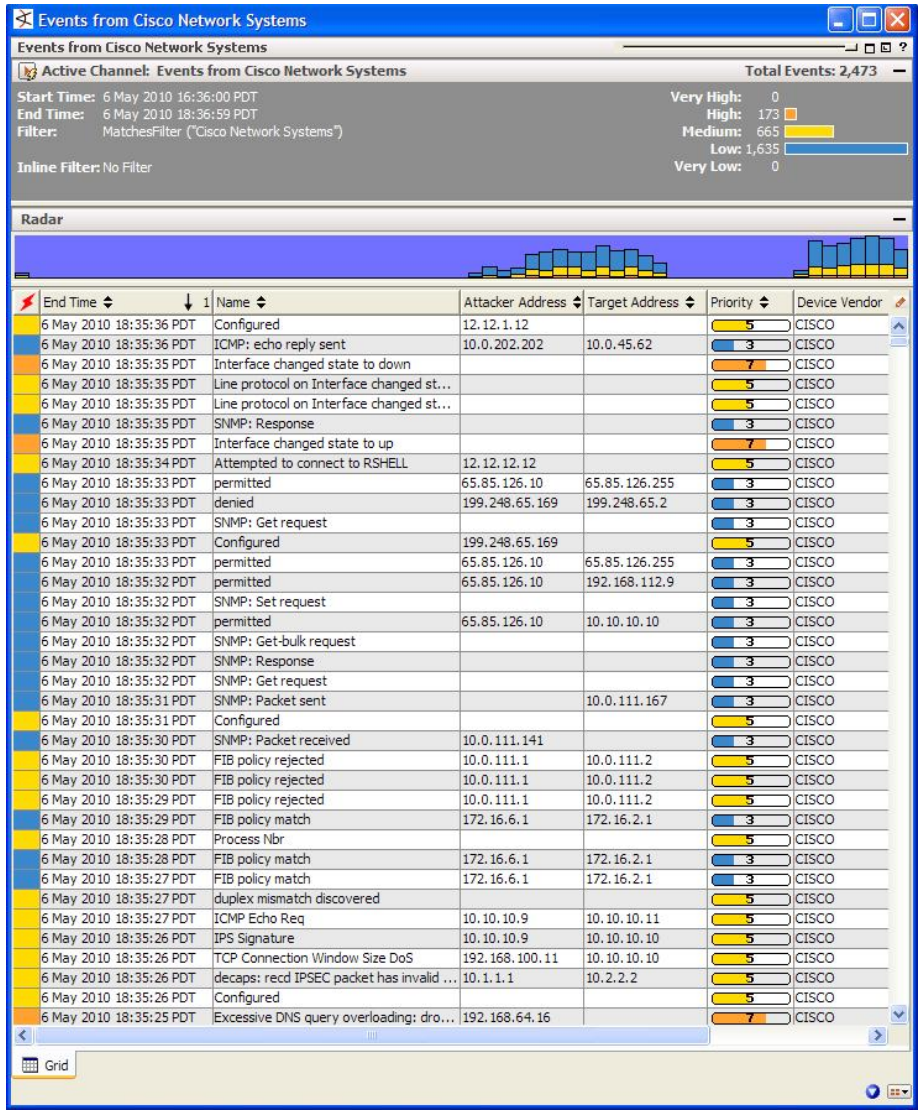


Figure 6. ArcSight Event Viewer displaying all Cisco network events



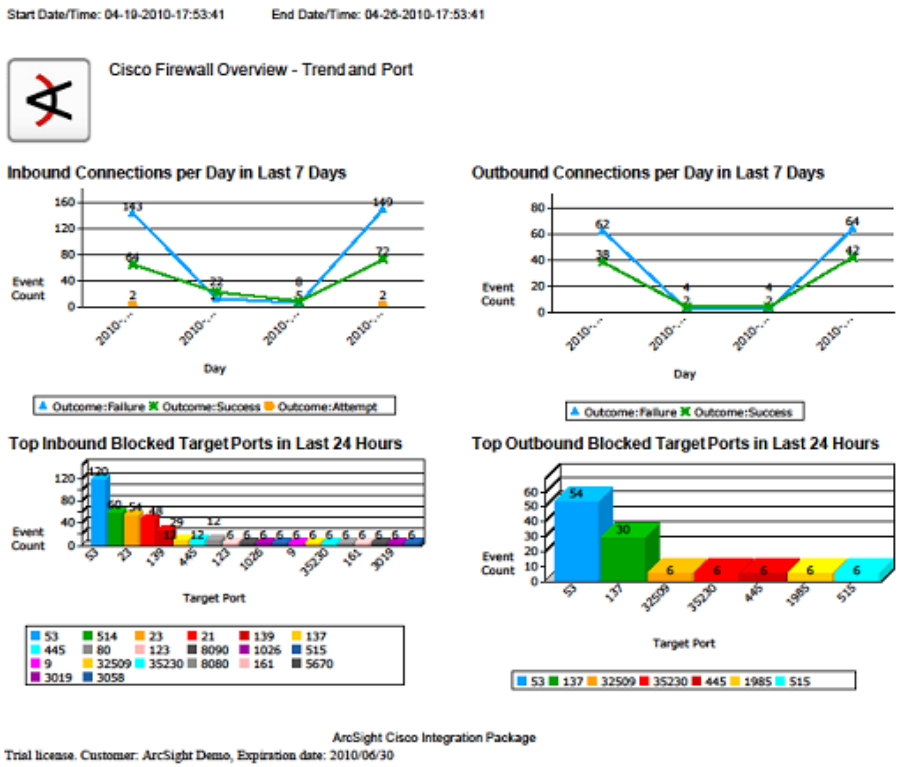
Generating Reports

The *ArcSight Solution Guide: Cisco Insight Package v1.0* describes the several pre-packaged reports that can be used to track logins, configuration changes, and other events involving Cisco devices in your environment. The following table lists the information presentation and data processing resources that support the Cisco Overview use cases in the *ArcSight Solution Guide*.

Cisco Resource	Overview Report Description
Overview of Cisco Configuration Changes	Displays summary information on configuration changes to Cisco devices such as the change count per day, per hour, top affected device, and top involved users.
Cisco Firewall Overview – Top Allowed Systems	Displays summary information about top allowed systems reported by Cisco firewall devices in the last 24 hours such as the top inbound (or outbound) sources and destinations.
Cisco Firewall Overview – Top Denied Systems	Displays summary information about top denied systems reported by Cisco firewall devices in the last 24 hours such as the top inbound (or outbound) blocked sources and destinations.
Overview of Logins Reported by Cisco Devices – Systems	Displays summary information on login attempts recorded by Cisco devices such as the top successful and failed login sources and destinations.
Overview of Logins Reported by Cisco Devices – Trend and Users	Displays summary information on login attempts recorded by Cisco devices such as the attempt count per day, per product, top users with successful and failed logins.
Cisco Intrusion Prevention System Overview	Displays summary information about alerts reported by Cisco IPS devices in the last 24 hours such as alerts per day, the top alerts, top attackers and targets involved.
Cisco Firewall Overview – Trend and Port	Displays summary information on firewall events from Cisco devices such as the inbound (or outbound) connections per day, top inbound (or outbound) blocked ports.

The following figure shows a sample pre-defined report for Cisco Firewall activity.

Figure 7. ArcSight trend reports on Cisco Firewall activity



With the ArcSight Compliance Insight Packages for various regulations (e.g. SOX, PCI, IT Governance) on ArcSight ESM or Express, customers can get pre-defined Compliance Reports for those regulations. Here is a sample compliance report for Sarbanes-Oxley (SOX).

Figure 8. ArcSight Compliance Reports – Sarbanes-Oxley

Notes

Maintaining the SIEM Solution

ArcSight publishes the following product and content updates with the following frequency.

- Content update (categorization, vulnerability mapping): twice a month
- Context update (geolocation of IPs): once a month
- SmartConnector updates: every six weeks
- Periodic correlation content updates
- Periodic software updates

Notes

Common Troubleshooting Tips

These troubleshooting steps help to diagnose and correct problems with getting Cisco events to be consumed and processed by ArcSight. Please refer to the ArcSight Administrator Guides for Arcsight ESM, Logger, and Express, to help with the ArcSight platform-specific trouble shooting.

My device is not one of the listed SmartConnectors.

ArcSight offers an optional feature called the FlexConnector Development Kit which may enable you to create a custom SmartConnector for your device. ArcSight can create a custom SmartConnector. Contact ArcSight Customer Support.

My device is on the list of supported products, but it does not appear in the SmartConnector Configuration Wizard.

Your device is likely served by a syslog sub-connector of either file, pipe, or daemon type.

Device events are not handled as expected.

Check the SmartConnector configuration to make sure that the event filtering and aggregation setup is appropriate for your needs.

SmartConnector is not reporting all events.

Check that event filtering and aggregation setup is appropriate for your needs.

Some Event fields are not showing up in the Console.

Check that the SmartConnector's Turbo Mode and the Turbo Mode of the Manager for the specific SmartConnector resource are compatible. If the Manager is set for a faster Turbo Mode than the SmartConnector, some event details will be lost.

SmartConnector is not reporting any events.

Check the SmartConnector log for errors. If the SmartConnector cannot communicate with the Manager, it will cache events until its cache is full.

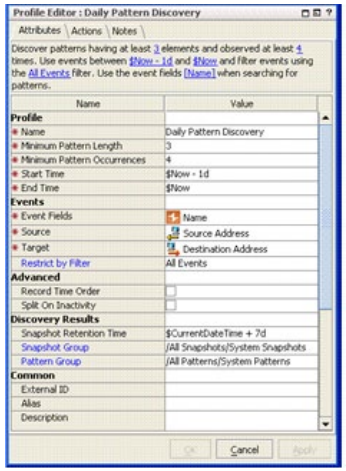
Example of a Day Zero Attack (Malware-Infected Customer Network)

Zero-day attacks occur during the vulnerability window that exists in the time between when vulnerability is first exploited by an attacker, and when the product vendor or security service provider releases a counter-measure (security patch or an IPS signature) to detect that threat.

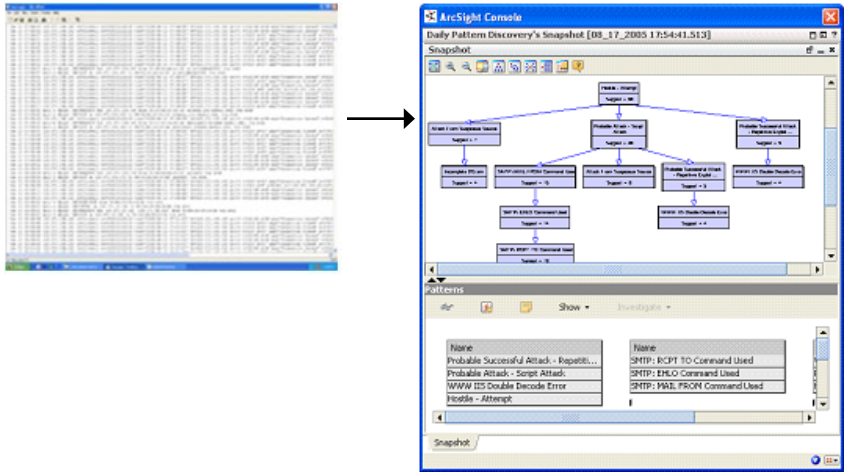
The ArcSight SIEM solution has a patent-pending feature called “Pattern Discovery” that can automatically discover zero-day attacks, detect low-and-slow attacks, and profile new suspicious patterns from current or historical event data. It then allows you to automatically create a rule with a single mouse click, and take any one of the following options to further analyze and respond to such attacks – show related events, show event graph, investigate further, or take a mitigation action if the attack is persistent.

The following steps show the process of setting up Pattern Discovery to detect and mitigate zero-day attacks.

1. Create a profile which allows you to select a subset of events from the event stream, on which the Pattern-Discovery tool can be used. The criteria for filtering event-stream could be event start time, end time, source and/or destination IP address, application protocol or payload.



2. Take a snapshot of qualifying event activity from current or historical events, and choose **Discover Patterns**.



3. The resulting pattern tree displays the transactional relationship of the attack patterns. Right-clicking on a specific cell in the tree allows you to further investigate (e.g. show event graph), or automatically create a rule to mitigate the threat if it is persistent.

Both ArcSight Express and ESM has the Pattern Discovery feature available to detect, further investigate and rapidly respond to unknown (zero-day) attacks.

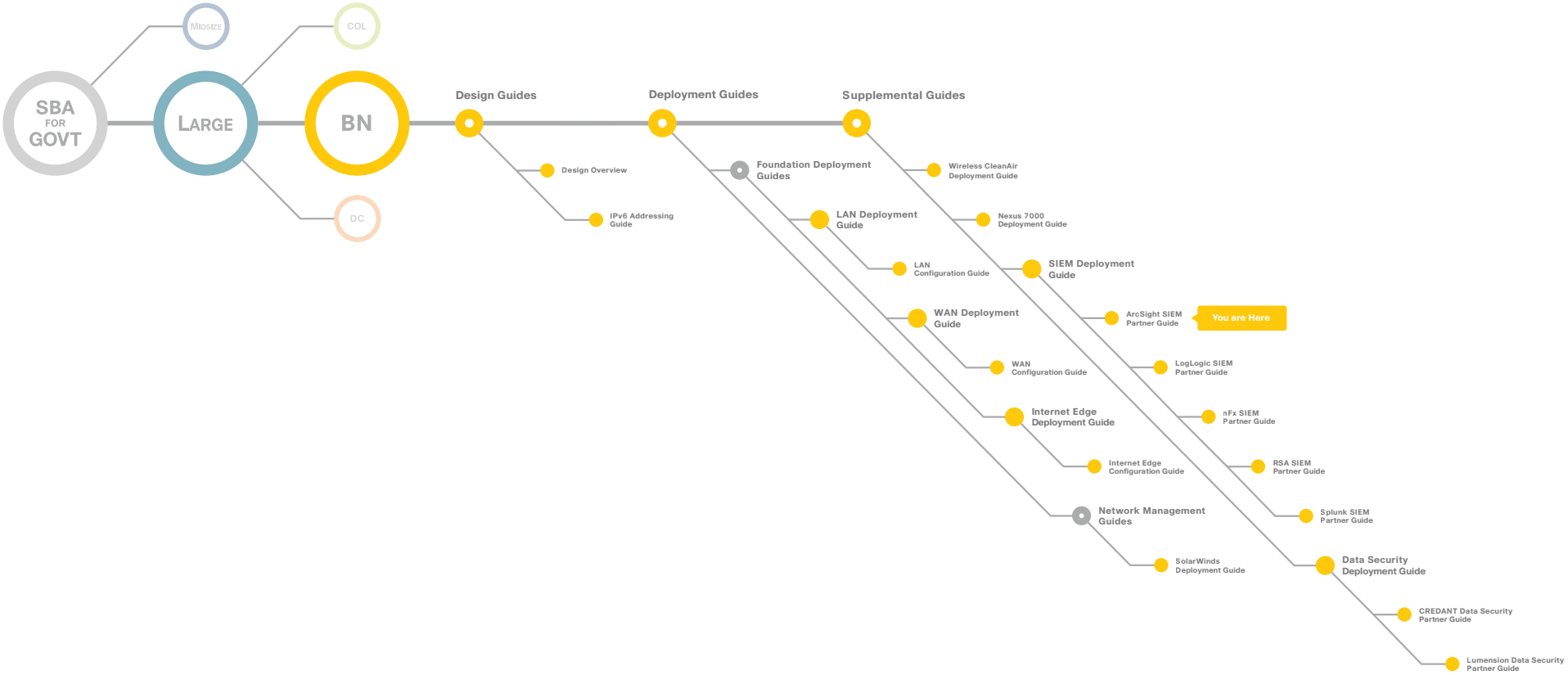
Products Verified with Cisco SBA

ArcSight ESM 4.5.1 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.

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.**

C07-640734-00 12/10