

TOMORROW starts here.



Cisco *live!*

Cisco Security Management

BRKSEC-2060

Sanjay Agarwal

Product Line Manager

Security Management

Agenda



Current Cisco Security Management Portfolio



Cisco Security Manager Operational Use Case



Cisco Prime Security Manager Operational Use Case



Cisco Defence Centre Operational Use Case



Cisco Security Management Strategy



Q & A

What is not Covered

- Prime Infrastructure
- Cisco VNC
- Cisco ISE
- Cisco Meraki
- Cisco ScanSafe
- Cisco WAS

Current Security Management Portfolio

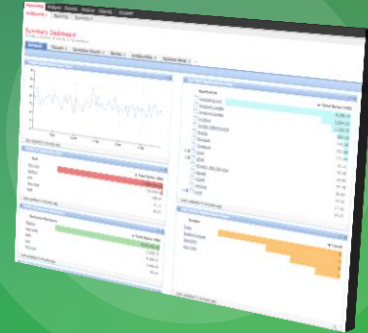
Cisco Prime Security
Manager
CSM



Cisco Prime Security
Manager
PRSM



Cisco Defence Centre
DC



Cisco Security Management Portfolio

CSM Operational Use Case

Medium and Large Enterprise

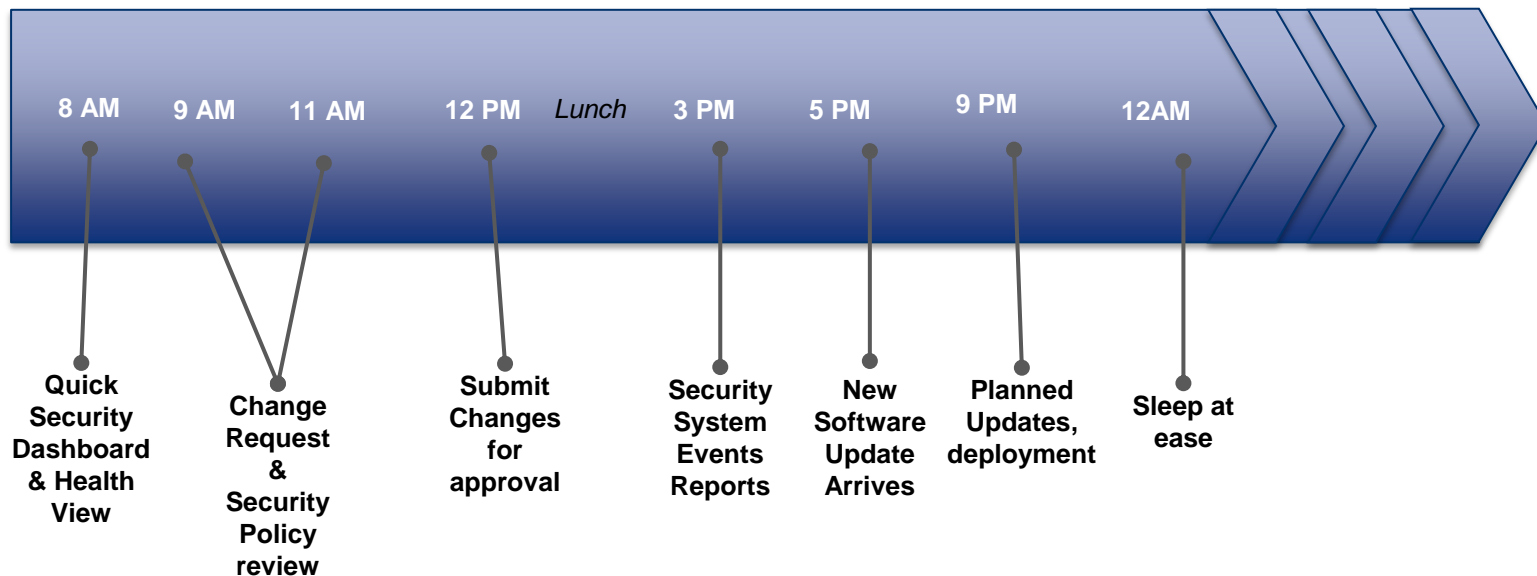
- CSM for enterprise deployments
- Customers looking to manage complete ASA management
- Customers looking for Enterprise class features:
 - Security Dashboard and Health Status
 - Large Complex Policy Management
 - Policy Approval
 - Policy Sharing and Validation
 - Device Configuration
 - Visibility and Events
 - Upgrades and Alerts

CSM in Action

Security Admin



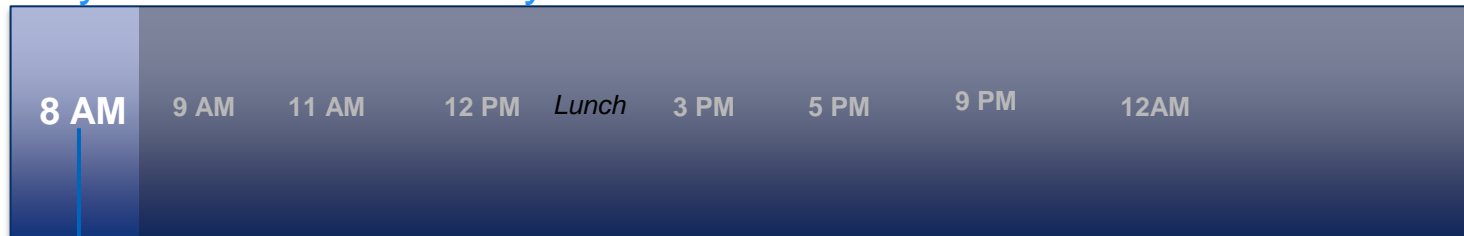
■ Day in the life of Security Administrator



@ Office



■ Day in the life of Security Administrator



Quick Security Dashboard and health view

Challenges

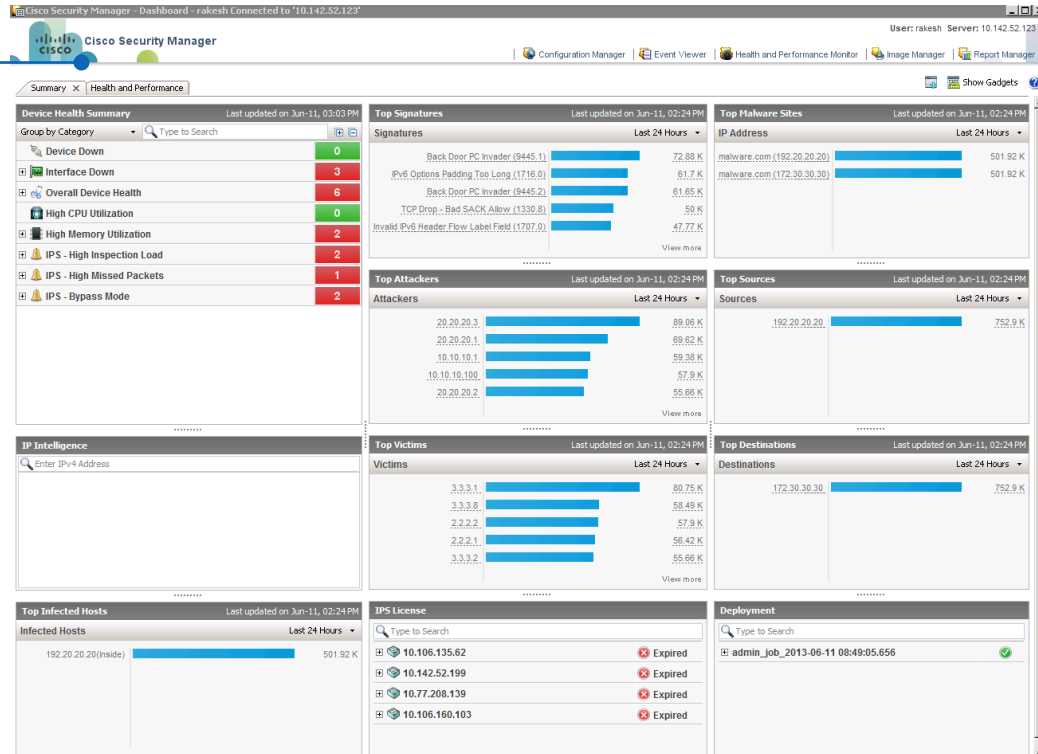
- Did the changes I made yesterday create any problem? Is there anything wrong?
- Is there a possibility of a threat, which I should address immediately?
- What configuration tasks do I need to perform to address my issues?
- Did CSM backup go through successfully last night?

CSM Solution

CSM Dashboard

Your starting point to perform detailed check

- **360 degree view of what's happening on your network**
- **Cross launches any CSM application at a click of a button**
- **Personalise – only see what you want to see about your network**
- **Easy drill down capability to start and investigate security problems**



Landing Page

Device HPM

Cross Launches

Create Dashboard

The screenshot shows the Cisco Security Manager Health and Performance Monitor dashboard. The interface includes a top navigation bar with tabs for Configuration Manager, Event Viewer, Health and Performance Monitor, Image Manager, and Report Manager. The main content area is divided into several sections:

- Device Health Summary:** A table showing device health metrics. A blue arrow points to the 'Device Health Summary' section.
- Top Signatures:** A bar chart showing the top signatures for the last 24 hours.
- Top Malware Sites:** A bar chart showing the top malware sites for the last 24 hours.
- Top Attackers:** A bar chart showing the top attackers for the last 24 hours.
- Top Sources:** A bar chart showing the top sources for the last 24 hours.
- Top Victims:** A bar chart showing the top victims for the last 24 hours.
- Top Destinations:** A bar chart showing the top destinations for the last 24 hours.
- IP Intelligence:** A search box for entering IPv4 addresses.
- Top Infected Hosts:** A bar chart showing the top infected hosts for the last 24 hours.
- IPS License:** A table showing the status of various IPS licenses.
- Deployment:** A search box for deployment information.

Annotations include blue arrows pointing to the 'Health and Performance' tab, the 'Device Health Summary' section, the 'Show Gadgets' button, and the 'Group by Category' dropdown menu. A blue arrow also points to the 'Cross Launches' text.

Group by Category	Count
Device Down	0
Interface Down	3
Overall Device Health	6
High CPU Utilization	0
High Memory Utilization	2
IPS - High Inspection Load	1
IPS - High Missed Packets	1
IPS - Bypass Mode	2

Signature	Count
Back Door.PC.Invader (9445.1)	72.88 K
IPv6.Options.Padding.Too.Long (1716.0)	81.7 K
Back Door.PC.Invader (9445.2)	81.85 K
TCP.Drop.Bad.SACK.Allow (1330.8)	50 K
Invalid.IPv6.Header.Flow.Label.Field (1707.0)	47.77 K

IP Address	Count
malware.com (192.20.20.20)	501.92 K
malware.com (172.30.30.30)	501.92 K

Attacker	Count
20.20.20.3	89.06 K
20.20.20.1	69.62 K
10.10.10.1	59.38 K
10.10.10.100	57.9 K
20.20.20.2	55.66 K

Source	Count
192.20.20.20	752.9 K

Victim	Count
3.3.3.1	80.75 K
3.3.3.8	58.49 K
2.2.2.2	57.9 K
2.2.2.1	56.42 K
3.3.3.2	55.66 K

Destination	Count
172.30.30.30	752.9 K

Infected Host	Count
192.20.20.20 (inside)	501.92 K

License ID	Status
10.106.135.62	Expired
10.142.52.199	Expired
10.77.208.139	Expired
10.106.160.103	Expired

Deployment ID
admin_job_2013-06-11 08:49:05.656

Group by Category dropdown menu options:

- Group by Alert
- Group by Category
- Group by Device
- Group by Technology

Landing Page - Gadgets

The screenshot displays the Cisco Security Manager interface. At the top, there are navigation tabs for Configuration Manager, Event Viewer, Health and Performance Monitor, Image Manager, and Report Manager. The main content area is titled 'Health and Performance' and features a 'Show Gadgets' button. Below this, there are two icons for 'Top Services' and 'Top Malware Ports', with a blue arrow pointing to the 'Top Malware Ports' icon. A 'Description' box instructs users to drag and drop gadgets to the dashboard. The dashboard itself is populated with several gadgets:

- High CPU Utilization:** A table with 5 rows showing metrics like High CPU Utilization (0), High Memory Utilization (2), IPS - High Inspection Load (2), IPS - High Missed Packets (1), and IPS - Bypass Mode (2).
- Top Attackers:** A bar chart showing the top 5 attackers with IP addresses and their respective counts (e.g., 20.20.20.3 with 89.06 K).
- Top Sources:** A bar chart showing the top 1 source with IP address 192.20.20.20 and a count of 752.9 K.
- Top Victims:** A bar chart showing the top 5 victims with IP addresses and their respective counts (e.g., 3.3.3.1 with 80.75 K).
- Top Destinations:** A bar chart showing the top 1 destination with IP address 172.30.30.30 and a count of 752.9 K.
- Top Infected Hosts:** A bar chart showing the top 1 infected host with IP address 192.20.20.20 (inside) and a count of 501.92 K.
- IPS License:** A table listing 4 expired licenses with IP addresses like 10.106.135.62.
- Deployment:** A table listing 1 deployment with IP address admin_job_2013-06-11 08:49:05.656.

Use New Gadgets

Landing Page – Details

Cisco Security Manager User: rakesh Server: 10.142.52.123

Configuration Manager | Event Viewer | Health and Performance Monitor | Image Manager | Report Manager

Summary x Health and Performance Show Gadgets



Device Health Summary





Group by Category


Device Down	0
Interface Down	3
10.106.160.53 Interface 'outside': Protocol Down (Protocol: down, Status: down) First Seen: Jun-10, 12:18 PM Last Seen: Jun-11, 11:43 AM Severity: Critical State: Active Acknowledged By: None Cleared By: None	
10.106.161.200 Interface 'inside': Protocol Down (Protocol: down, Status: down) First Seen: Jun-10, 12:18 PM Last Seen: Jun-11, 11:43 AM Severity: Critical State: Active Acknowledged By: None Cleared By: None	
10.77.208.171 Interface 'Test': Protocol Down (Protocol: down, Status: down) First Seen: Jun-10, 12:18 PM Last Seen: Jun-11, 11:43 AM Severity: Critical State: Active Acknowledged By: None Cleared By: None	
Overall Device Health	6
High CPU Utilization	0
High Memory Utilization	2
IPS - High Inspection Load	2
IPS - High Missed Packets	1
IPS - Bypass Mode	2


Device Health Summary


Device Health Summary Last updated on Jan-02, 01:44 PM IST

Group by Category  


 Device Not Reachable	2
 Interface Down	7
 Overall Device Health Alerts	4
 High Memory Utilization	0



Alert 

 ips-nyk

 Missed Packets are 7%









First Seen: Dec-16, 11:36 AM IST
Severity: Critical
Acknowledged By: None

Device Summary 

 ips-nyk Connected 


Cisco IPS 4260 Sensor (IPS)
Target OS Version: 7.0
Running OS Version: 7.0(1)E4S574V1.4
Address: 192.168.135.3
Owner:

Report Card

-  Connected
-  Device Health
-  Inspection Load
-  Missed Packets
-  IPS in Bypass Mode
-  Memory Usage [View Health Summary](#)
-  Last Deployment: Unknown [View Events](#)
-  License expires in 570 days [View Device Manager](#)

License expires in 570 days [View Image Manager](#)

Last updated: Jan-02, 01:43 PM IST


 Close

Missed Packets are 7%

First Seen: Dec-16, 11:36 AM IST
Severity: Critical
Acknowledged By: None
Cleared By: None

Clear Comments:

Add Notes:

 Acknowledge Alert

- Brings HPM Alerts information to Dashboard
- Can group Alerts by Category, Alert-Type, Device and Technology
- Add comments, Acknowledge or Clear Alert
- View Device Summary

HPM All Device View & Details

The screenshot displays the Cisco HPM (Health Policy Manager) interface. The main window is titled 'Monitoring' and shows a list of devices under the 'All Devices' view. The summary table includes columns for Device Name, Receive Time, Health Status, Connection Status, CPU(%), Memory(%), Version, and Inspection Load(%). Below the table, the details for device 10.77.208.171 are shown, including its name, IP address, firewall mode, and failover status. The interface also features a 'Device Report Card' section with an 'Interface Status' table and performance charts for CPU and Memory utilization over a one-hour period.

Device Name	Receive Time	Health Status	Connection Status	CPU(%)	Memory(%)	Version	Inspection Load(%)
10.77.208.171	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	0%	57% 8.4(2)	8.4(2)	
10.106.160.53	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	0%	26% 8.4(4)9	8.4(4)	
10.106.161.50	Wed Jun 12 15:01:00 IST 2013	Normal	Connected	0%	Not Applicable	8.4(4)	
10.106.161.200	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	0%	33% 9.0(1)242	9.0(1)242	
10.106.135.62	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	59%	94% 7.0(1)E4	7.0(1)E4	84%
10.142.52.199	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	68%	94% 7.0(1)E4	7.0(1)E4	92%
10.77.208.139	Wed Jun 12 15:01:00 IST 2013	Critical	Connected	2%	52% 7.1(7)E4	7.1(7)E4	0%

Property	Value
Name	10.77.208.171
IP Address	10.77.208.171
Firewall Mode	ROUTER
Failover Status	Not Configured
Peer Status	--NA--
Model	Cisco ASA-5520 Adaptive Security Appliance
Version	8.4(2)
Context Mode	SINGLE
Host Role	--NA--
Peer Role	--NA--

Metric	Status	Value
Interface Status	Critical	

Name	IP Address	Status	Protocol
outside	20.1.1.2	up	up
inside	2.1.1.1	up	up
Test	21.23.21.2	down	down
mgmt	10.77.208.171	up	up

CPU Utilization (%)
 Time Frame: Last 1 hour
 Average: 0%
 The chart shows a flat line at 0% utilization over the last hour.

Memory Utilization (%)
 Average: 57%
 The chart shows a flat line at 57% utilization over the last hour.

Connections per second
 Average: 0
 The chart shows a flat line at 0 connections per second over the last hour.

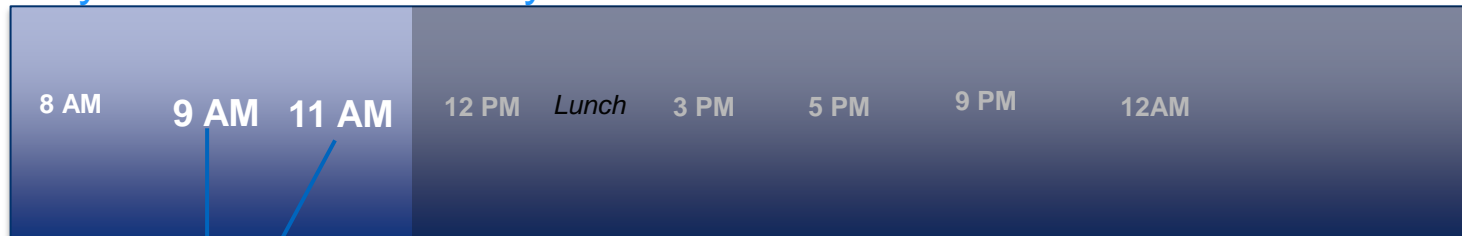
Summary Info

Improve Charts

@ Office



■ Day in the life of Security Administrator



Change
Request &
Security Policy
Review

Challenges

- Why is this change required?
- What needs to change in the network?
- Who needs to approve?
- Will it create any problem?
- How can it be deployed?

CSM Solution

CSM Configuration Manager

Unified Security Policy & Change Management

- Device Discovery and modelling
- Policy Management and validation
- Policy sharing and bundling
- Policy approval workflow
- Policy Object and Services

The screenshot displays the Cisco Security Manager Configuration Manager interface. The main window shows the configuration for a device named 'asa-live' under the 'Local' policy. The 'Permit' tab is active, displaying a table of 18 rules. The table columns include No., Permit, Sources (Network, Security Group, User), Destinations (Network, Security Group, Service), and HitCount. The rules are listed as follows:

No.	Permit	Network	Security Group	User	Network	Security Group	Service	HitCount
1	✓	10.0.0.0/255.0.248.0	-- no tags --	-- no user --	All-Addresses	-- no tags --	tcp/old	0 Never
2	✓	All-Addresses	-- no tags --	-- no user --	All-Addresses	-- no tags --	tcp/old/1-65535	0 Never
3	✓	All-Addresses	-- no tags --	-- no user --	All-Addresses	-- no tags --	try	0 Never
4	✓	All-Addresses	-- no tags --	-- no user --	All-Addresses	-- no tags --	try1	0 Never
5	✓	4.5.6.9	-- no tags --	-- no user --	All-Addresses	-- no tags --	TCP	0 Never
6	✓	All-Addresses	-- no tags --	-- no user --	9.9.9.9	-- no tags --	UDP	0 Never
7	✓	8.9.7.8	-- no tags --	-- no user --	All-Addresses	-- no tags --	TCP	0 Never
8	✓	8.9.7.8	-- no tags --	-- no user --	5.5.5	-- no tags --	TCP	0 Never
9	✓	All-Addresses	-- no tags --	-- no user --	10.3.4.5	-- no tags --	TCP	0 Never
10	✓	All-Addresses	-- no tags --	-- no user --	10.5.6.7	-- no tags --	ICMP	0 Never

The interface also shows a 'Policy Object Manager' window with a table of network objects:

Name	Content	Type	Category	Overrides	Description
1	1.1.2.3	Host			
2	2.2.2.2	Host		✓	
4.3.2.1	6.6.66.6	Host		✓	
4.3.2.1	4.3.2.1	Host		✓	
4001::1	4001::1	Host		✓	
*011::1	22::22	Host		✓	
*011::1_eo5fwfhthg	22::22	Host		✓	
A-10.105.191.70	10.105.191.70	Group		✓	
A-10.109.60.192	10.109.60.192	Group		✓	

Docked Policy Object Manager

1. Select NY-ASA

2. Select Access Rules

3. Launch Policy Object Manager

4. Policy Object Manager is docked below Access Rule

Device: ny-asa
Policy Assigned: -- local --

No.	Permit	Source	User	Destination	Service	Interface	Dir.	Options	Category
Local (23 Rules)									
1	Deny	any	THREATDLABS\Wktg	DataCenter-1	IP	Global	in		None
2	Deny	any	THREATDLABS\Wktg	DataCenter-2	IP	Global	in		None
3	Deny	any	THREATDLABS\Wktg	DataCenter-3	IP	Global	in		None
4	Deny	any	THREATDLABS\Wktg	CSM-Server	IP	Global	in		None
5	Deny	any	THREATDLABS\Br...	DataCenter-1	IP	Global	in		None
6	Deny	any	THREATDLABS\Br...	DataCenter-2	IP	Global	in		None

Policy Object Manager

Name	Content	Category	Overrides	Description
50554	50554		✗	Shared License Port
ALLPORTS	0-65535		✓	
Default Range	1-65535		✗	Default/Any Port Range
HTTPS	443		✗	HTTPS Port
WEBPORTS	3128,443,80,8000,8080		2	WEBPORTS

ACL Hit Count

The screenshot displays the Cisco Security Manager interface. The main window shows the 'Hit Count Query Results' for a selected device (Catalyst6500...). A table lists the 'Selected Access Rules' with columns for Rule, HitCount, Permit, Source, Destination, Service, Interface, and Dir. The 'Local - Default_1' rule is highlighted in yellow, showing a HitCount of 1318. A red circle highlights the 'HitCount' column, and a red arrow points to a pop-up window showing a detailed view of the hit counts for the three rules.

Rule	HitCount
Local - Default_1	1318
Local - Default_2	215
Local - Default_3	215

The main table also shows a detailed view of the 'Local - Default_1' rule with the following data:

Rule	Hit Count	Permit	Service	Interfaces	Direction	Source Address	Source Port	Dest Addresses	Destination Port	ACL Name
Local - Default_1	1318	✓	gre	outside	in	0.0.0.0/0...		0.0.0.0/0...		ad_mdc_outs...

The bottom right of the interface shows a list of rules with their respective hit counts and status icons. The 'HitCount' tab is highlighted in yellow.

- Check if an access rule is encountering hits on live device

Drag-and-drop Objects to Policy

The screenshot displays the Cisco ASA configuration interface. At the top, it shows the device name 'ny-asa', the policy 'Access Rules', and the assigned device 'local device'. Below this is a table of policy rules. Rule 15 is selected, showing its source as 'Engineering_Net' and destination as 'DataCenter-1'. A red dashed arrow points from rule 15 to the 'DataCenter-1' object in the 'Networks/Hosts' object manager window below. A green callout box with the text '1. Select Network/Hosts' points to the left-hand navigation pane. Another green callout box with the text '2. Drag an object to a rule's destination' points to the 'DataCenter-1' object in the object manager window.

Device: **ny-asa**
Policy Assigned: **-- local --**
Policy: **Access Rules**
Assigned To: **local device**
Inherits From: **-- none --**

Filter: (-- none --)

No.	Permit	Source	User	Destination	Service	Interface	Dir.	Options	Category
10	⊘	any	THREATDLABS\\Engg	DataCenter-2	IP	Global	in		None
11	⊘	any	THREATDLABS\\Engg	DataCenter-3	IP	Global	in		None
12	⊘	any	THREATDLABS\\Engg	CSM-Server	IP	Global	in		None
13	⊘	any	-- no user --	7.7.7.8	IP	Global	in		None
14	✓	any	THREATDLABS\\Sales	8.8.8.8	IP	Global	in		None
15	✓	Engineering_Net	THREATDLABS\\Engg	DataCenter-1	IP	Global	in		None
16	✓	Engineering_Net	THREATDLABS\\Engg	DataCenter-2	IP	Global	in		None

Enable Auto Conflict Detection Generate Report Tools Save

ASA 8.3 onwards the device uses Real IP (pre-natted IP) in firewall rules. Use Real IP addresses.

1. Select Network/Hosts

2. Drag an object to a rule's destination

Networks/Hosts

Filter: (-- none --)

Name	IP Address	Category	Overrides	Referenced	Description
any	0.0.0.0/0	Group	⊗	✓	Predefined any network
any.megadownloads.com	megadownloads.com	FQDN	⊗	✓	
Apple.com	www.apple.com	FQDN	⊗	✓	
Cisco.com	www.cisco.com	FQDN	⊗	✓	
CSM-Server	csm-server.threatdlabs.test	FQDN	⊗	✓	
DataCenter-1	10.10.10.0/24	Network	⊥	✓	
DataCenter-2	172.16.10.0/24	Network	⊥	✓	

Displaying: 23 of 23 objects Selected Rows: 1

Policy Sharing and Inheritance

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The main window shows the configuration for a device named 'SD-ISR2851' with the policy 'Access Rules'. A 'Share Policy...' dialog box is open, showing the policy name 'FW-Policy'. An 'Edit Policy Inheritance' dialog box is also open, showing a tree view of available policies, with 'West-Region' selected as the parent policy. The background shows a table of rules with columns for 'No.', 'Permit', and 'Category'. A yellow box highlights the text 'Assigned to : 2 Device(s)' in the interface.

No.	Permit	Category
1	⊘	None
2	✓	None
3	✓	None
4	✓	Cat-C
5	✓	
6	✓	
7	⊘	
8	✓	
9	✓	
16	✓	
17	✓	
18	✓	

Destination	Service	Dir.	Interface	Options
10.2.2.2	tcp/1720	in	outside	LOG
Test2	tcp/Web_Service...	in	outside	LOG
10.1.1.100	tcp/80	in	outside	LOG
any	ICMP-Echo-Reply	in	outside	LOG
any	udp/137	in	outside	LOG
any	udp/138	in	outside	LOG
any	tcp/22	in	outside	LOG
any	udp/53	in	outside	LOG

- Take any device policy/setting and save it for sharing
- Shared policies can be assigned to multiple devices

Global Objects Search & Find-Usage

1. Search for: DataCenter-1

2. Select Policies

3. Right-click and select "Go To". This will show rule that matches this object's usage

Global Search

Search All Categories DataCenter-1

5 results found for DataCenter-1 in All Categories (0.22 seconds)

Click on any of the categories listed below to view the search results

Scope	Rule	Permit	Source	User	Destination
ny-asa - Local	1	no	any	THREATDLABS\Wktg	DataCenter-1
ny-asa - Local	5	no	any	THREATDLABS\Branch	DataCenter-1
ny-asa - Local	9	no	any	THREATDLABS\Engg	DataCenter-1
ny-asa - Local	15	yes	Engineering...	THREATDLABS\Engg	DataCenter-1

Global Search Index Last Updated on 26 Jan 2012 10:18 AM PST
Displaying: 23 of 23 objects

Auto-Conflicts Detection

1. Click on icon "S" to view conflicts of this rule

2. Review the conflicts and recommended action

3. Generate full conflict report

4. Review full conflict report

Rule No	Permit	Source	User	Destination	Service	Interface
Local Rule 9	⊗	any	THREATDLABS\Engg	DataCenter-1	IP	Global
Local Rule 15	✓	Engineering_Net	THREATDLABS\Engg	DataCenter-1	IP	Global

Rule No	Permit	Source	User	Destination	Service	Interface
Local Rule 15	✓	Engineering_Net	THREATDLABS\Engg	DataCenter-1	IP	Global
Local Rule 21	✓	any	THREATDLABS\Engg	any	IP	Global

Rule No	Permit	Source	User	Destination	Service	Interface
Local Rule 14	true	any	THREATDLABS\Sales	8.8.8.8	IP	Global
Local Rule 18	true	any	THREATDLABS\Sales	any	IP	Global

Rule No	Permit	Source	User	Destination	Service	Interface
Local Rule 9	false	any	THREATDLABS\Engg	DataCenter-1	IP	Global
Local Rule 15	true	Engineering_Net	THREATDLABS\Engg	DataCenter-1	IP	Global

Create & Manage Policy Bundle

1. Click on Policy Bundle

2. Select this to display all shared policies

3. Add new policy bundle

4. Drag shared policies to policy bundle

	Type
Shared Policies	
Firewall	
Access Rules	
Global FW Policy	Access Rules
Inspection Rules	
Global Inspection Policy	Inspection Rules
Botnet Traffic Filter Rules	
Global BTF Policy	Botnet Traffic Filter Rules
Identity Options (ASA)	
Global IDFW Settings	Identity Options

Assign Policy Bundle to Devices

The screenshot displays the Cisco Security Manager Configuration Manager interface. The main window is titled "Cisco Security Manager - Configuration Manager - admin Connected to '172.16.1.10'". The menu bar includes File, Edit, View, Policy, Map, Manage, Tools, Launch, and Help. The toolbar contains icons for Device, Map, Policy, Policy Bundle, and other functions. The "Policy Bundle View" pane on the left shows a tree structure with "All Shared Policies" and "Policy Bundles", where "ASA Policy Bundle" is selected. A green callout bubble points to this selection with the text "1. Select policy bundle". The main area shows the "Policy Type: ASA Policy Bundle" and "Policy: ASA Policy Bundle". The "Assignments" tab is active, and a green callout bubble points to it with the text "2. Select Assignment tab". The "Available Devices" pane shows a tree structure with "Device Groups" (Department, Location, All) and "All" (dc-asa, kc-asa). A green callout bubble points to the "dc-asa" device with the text "3. Select and assign devices". The "Assigned Devices" pane shows a list of devices: ny-asa, sf-asa, and la-asa. The interface also includes a search bar, a "Save" button, and a "Cisco" logo.

Policy Bundle Assignment

The screenshot displays the Cisco Security Manager interface with three callout boxes indicating the steps for policy bundle assignment:

- 1. Select Device View:** Points to the 'Device' button in the top menu bar.
- 2. Select assigned policy:** Points to the 'Access Rules' folder in the 'Policies' tree on the left.
- 3. Validate Policy Bundle is assigned:** Points to the 'Global FW Policy' entry in the main table.

The main interface shows the following details:

- Device:** la-asa
- Policy:** Access Rules
- Policy Assigned:** Global FW Policy
- Policy Bundle Assigned:** ASA Policy Bundle
- Assigned To:** 3 Devices
- Inherits From:** -- none --

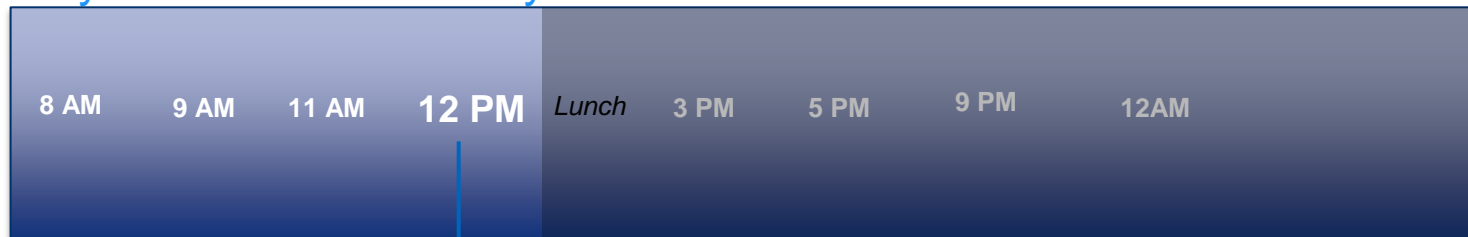
The main table displays the following data:

No.	Permit	Source	Destination	Service	Interfa
Global FW Policy - Mandatory (21 Rules)					
1	✓	Engineering_Net	THREATDLABS\Engg	DataCenter-1	IP DM
2	✓	Engineering_Net	THREATDLABS\Engg	DataCenter-2	IP DM
3	✓	Engineering_Net	THREATDLABS\Engg	DataCenter-3	IP DM
4	✗	any	THREATDLABS\Wktg	DataCenter-1	IP Glo
5	✗	any	THREATDLABS\Wktg	DataCenter-2	IP Glo
6	✗	any	THREATDLABS\Wktg	DataCenter-3	IP Glo
7	✗	any	THREATDLABS\Wktg	CSM-Server	IP Glo
8	✗	any	THREATDLABS\Branch	DataCenter-1	IP Glo

@ Office



■ Day in the life of Security Administrator



Submit
Changes for
approval

Challenges

- Where there any company violations?
- How many changes do I need to submit?
- How should I submit ticket for approval
- Have I completed all my tickets?

Workflow

What Is It?

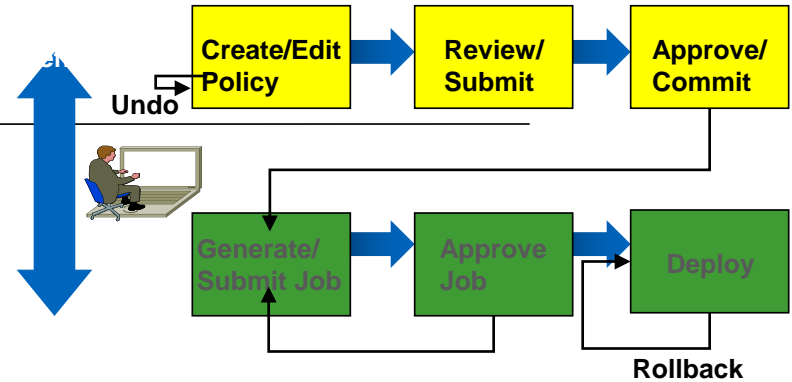
- Provides multiphase workflow for deployment with approvals at each stage

Example

- All policy changes need to be approved
- Deployment to the network must be during the change window

Benefit

- Enables teamwork and collaboration between NetOps and SecOps
- Provides scope of control



- Who Can Modify Device Configs?
- Who Can View Changes?
- Who Can Approve Changes?
- Who Can Deploy Changes to Devices?

Activity Model

- Robust approval workflow can be turned on or off
- Tied to privileges and roll-based model to enable admin controls through job creation and deployment
- Multiple users can be active at same time, and work in separate “activities”
- Activities can be opened for editing or submission later and deployed

The screenshot displays the 'Activity Manager' interface. At the top, there is a table with columns for Activity, State, User, and Last Action. Below the table are buttons for 'Create', 'Open', 'Close', 'Validate', 'Submit', 'Approve', 'Reject', 'Discard', and 'Refresh'. The 'Activity Details' section is active, showing a tree view on the left with 'Workflow' selected. The main area contains configuration options for 'Workflow Control', 'Default Approvers', and 'Workflow History'.

Activity	State	User	Last Action
admin_05.12.05_14:58:15	Approved	admin	Activity approved
admin_05.12.05_15:01:42	Approved	admin	Activity approved
admin_05.12.05_15:02:46	Approved	admin	Activity approved
admin_05.12.05_15:04:04	Approved	admin	Activity approved
admin_05.12.05_15:07:00	Approved	admin	Activity approved
admin_05.12.05_15:20:09	Approved	admin	Activity approved

Workflow Control

- Enable Workflow
- Require Activity Approval
- Require Deployment Approval

Default Approvers

Activity Approval Email:

Job Approval Email:

Workflow History

Keep Activity for: days

Keep Job for: days

Activity Report

What Fields Changed: What Objects Changed



Activity Change Report

User: admin
Session started on: 13-Nov-2006 13:46:01
Current state: Edit Open
Report created on: 13-Nov-2006 17:45:30

Devices

mypix.cisco.com

Access Rule

Access Rule

Operation	No.	Mandatory	Permit	Source	Destination	Service	Interface	Dir.	Category	Enabled
Add	1	true	permit	any,	any,	HTTP, HTTPS, FTP	All-Interfaces	in	None	true
Add	2	true	deny	any,	any,	IP	All-Interfaces	in	None	true

10.89.33.138

Device was discovered

Shared Policies

IPS-IpsEASetting

IpsEASetting: **10.89.33.138_IpsEASetting_1**
163454688687 (Added)

Inherits From	--None--
Affected Devices	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138
New Assignments	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138

IpsEASetting

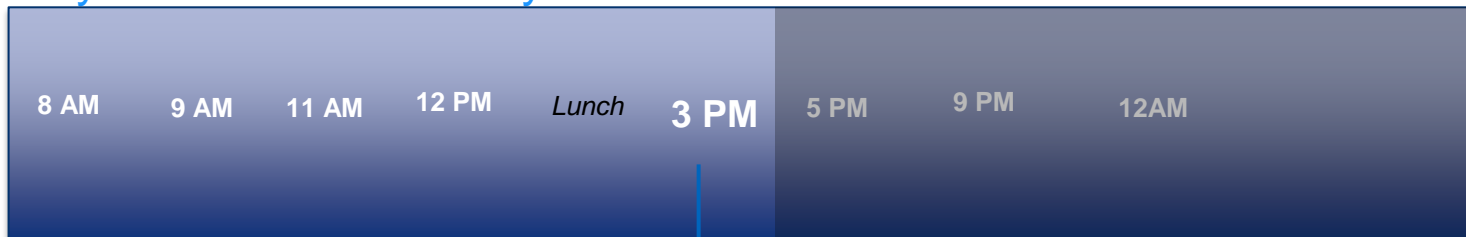
Operation	Global -deny -timeout
Add	3609

IPS-IpsAnomalyDetection

@ Office



▪ Day in the life of Security Administrator



Challenges

- Where there any company violations?
- How many changes do I need to submit?
- How should I submit ticket for approval
- Have I completed all my tickets?

Events

CSM Solution

CSM Event Viewer

View and Troubleshoot
all Security Events

- Real time event management and troubleshooting
- Cross linkages between events and configurations
- Customisable views for monitoring selected devices
- Admin configured objects can be seen in the events (ASA+IPS)
- Tools such as ping, traceroute, and packet tracer for further troubleshooting

The screenshot displays the Cisco CSM Event Viewer interface. The main window is titled "Event Monitoring" and shows a list of events under the "All Device Events" view. The interface includes a search bar, a "View Settings" panel, and a table of events. The table columns are: Receive Time, Severity, Event Type ID, Event Name, Device, Reputation, Source, Source Service, Destination, and Destination Service. The events listed are primarily "Bulk UDP" and "Teardown UDP" events from ASA-13 devices, occurring between 1:09 AM and 1:21 AM on 6/15/10. A "My Views" sidebar on the left shows various predefined and custom views. At the bottom, there is a timeline view for "Event Details" showing the time progression from 2:00 AM to 12:00 AM.

Receive Time	Severity	Event Type ID	Event Name	Device	Reputation	Source	Source Service	Destination	Destination Service
6/15/10 1:21:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:21:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:21:41 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:21:41 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:19:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:19:40 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:17:39 AM	Informational	302010	Connection USAGE	ASA-13					
6/15/10 1:15:43 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:16:43 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:15:43 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:15:43 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:13:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:13:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:13:41 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:13:41 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:11:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:11:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:11:40 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:11:40 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:09:39 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:09:39 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:09:39 AM	Informational	302016	Teardown UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514

Event Viewer Detail

The screenshot displays the Cisco Event Viewer interface. The main window is titled "Event Monitoring" and shows a list of events under the "All Device Events" view. The table below represents the data shown in the main event list:

Receive Time	Severity	Event Type ID	Event Name	Device	Reputation	Source	Source Service	Destination	Destination Service
6/15/10 1:25:44 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:25:44 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:25:44 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:25:44 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:23:42 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:23:42 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:23:42 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:23:42 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:21:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:21:41 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:21:41 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:21:41 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.30	udp/514
6/15/10 1:19:40 AM	Informational	302015	Bulk UDP	ASA-13		10.130.1.13	udp/514	10.130.1.31	udp/514
6/15/10 1:19:40 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.30	udp/514	10.130.1.13	udp/514
6/15/10 1:19:40 AM	Informational	302016	Tear down UDP	ASA-13		10.130.1.31	udp/514	10.130.1.13	udp/514

The "Event Details" pane for the selected event (6/15/10 1:23:42 AM) shows the following information:

Receive Time	6/15/10 1:23:42 AM	Severity	Informational	Event Type ID	302015
Event Name	Bulk UDP	Device	ASA-13	Reputation	
Source	10.130.1.13	Source Service	udp/514	Destination	10.130.1.30
Destination Service	udp/514	Action	bulk	Risk Rating	
Destination Interface	inside	Description	bulk outbound udp connection 29201543 for inside:10.130.1.30/514 (10.130.1.30/514) to		

Real-Time Event Viewer

1. Locate events from Sales-PC

2. Looks for AD user names sales-user

No.	Receive Time	Severity	Device	Source	User Identity	Protocol	Source...	Destin...	Event Name
24	1/26/12 10:32:14 AM	Informational	ny-asa	172.16.1.10		udp	31784	172.16.1.10	Built UDP
25	1/26/12 10:32:14 AM	Informational	ny-asa	172.16.1.10		udp	37455	172.16.1.10	SSLHandsh...
26	1/26/12 10:32:14 AM	Informational	ny-asa	172.16.1.10		udp	37455	172.16.1.10	SSL handsh...
27	1/26/12 10:32:13 AM	Informational	ny-asa	172.16.1.10		tcp	37455	204.15.1.10	Built TCP
28	1/26/12 10:32:13 AM	Informational	ny-asa	172.16.1.10		udp	18701	172.16.1.10	Built UDP
29	1/26/12 10:32:09 AM	Informational	ny-asa	172.16.1.10	THREATDLABS\sales-user	tcp	51403	172.16.1.10	PAT teardown
30	1/26/12 10:32:08 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51401	172.16.1.10	PAT teardown
31	1/26/12 10:32:08 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51410	172.16.1.10	PAT teardown
32	1/26/12 10:32:08 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51402	172.16.1.10	PAT teardown
33	1/26/12 10:32:08 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51411	172.16.1.10	PAT teardown
34	1/26/12 10:32:08 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51400	172.16.1.10	PAT teardown
35	1/26/12 10:32:05 AM	Informational	ny-asa	74.125.53.139		tcp	80	172.16.1.10	NY-PC2 Teardown TCP
36	1/26/12 10:32:05 AM	Informational	ny-asa	74.125.224.71		tcp	80	172.16.1.10	NY-PC2 Teardown TCP
37	1/26/12 10:31:48 AM	Informational	sf-asa	172.16.1.90		udp	514	172.16.1.10	Built UDP
38	1/26/12 10:31:48 AM	Informational	sf-asa	172.16.1.10		udp	514	172.16.1.10	Teardown UDP
39	1/26/12 10:31:39 AM	Informational	ny-asa	72.247.64.170		tcp	80	172.16.1.10	SALES-PC Teardown TCP
40	1/26/12 10:31:38 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51415	172.16.1.10	Built TCP
41	1/26/12 10:31:38 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51415	172.16.1.10	PAT created
42	1/26/12 10:31:38 AM	Informational	ny-asa	72.247.64.170		tcp	80	172.16.1.10	SALES-PC Teardown TCP
43	1/26/12 10:31:38 AM	Informational	ny-asa	72.247.64.170		tcp	80	172.16.1.10	Teardown TCP
44	1/26/12 10:31:38 AM	Informational	ny-asa	72.247.64.170		tcp	80	172.16.1.10	SALES-PC Teardown TCP
45	1/26/12 10:31:38 AM	Informational	ny-asa	72.247.64.170		tcp	80	172.16.1.10	SALES-PC Teardown TCP
46	1/26/12 10:31:38 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51415	172.16.1.10	Built TCP
47	1/26/12 10:31:38 AM	Informational	ny-asa	SALES-PC	THREATDLABS\sales-user	tcp	51415	172.16.1.10	PAT created

Event Monitoring interface showing a table of events and a line graph at the bottom. The table lists events with columns for No., Receive Time, Severity, Device, Source, User Identity, Protocol, Source, Destination, and Event Name. A line graph at the bottom shows event counts over time from 10:14 AM to 10:32 AM.

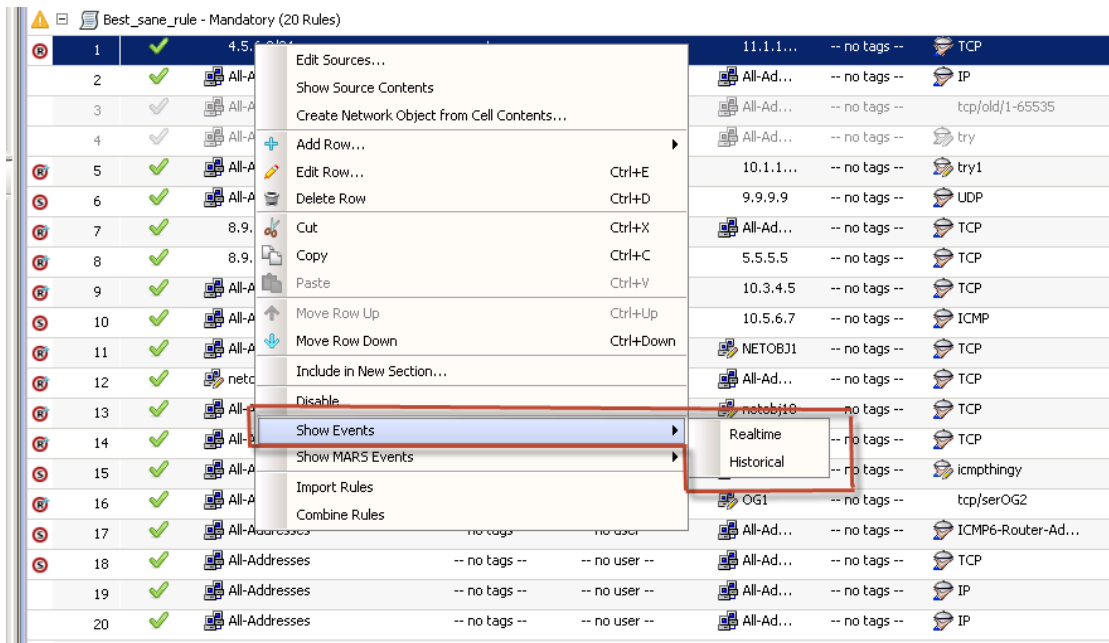
Jump to Policy from Events

The screenshot displays the Cisco Security Manager Event Viewer interface. The main window shows a table of events with columns for Receive Time, Severity, Event Type ID, Event Name, Device, Reputation, and Source. A context menu is open over the selected event, listing various actions such as 'Filter This Value', 'Copy Cell', and 'Go To Policy...'. The 'Go To Policy...' option is highlighted in blue. The background shows the Cisco Security Manager console with a tree view on the left and a policy configuration pane on the right.

Receive Time	Severity	Event Type ID	Event Name	Device	Reputation	Source
6/15/10 12:55:40 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:55:40 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:55:40 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:55:40 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:53:39 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:53:39 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:53:39 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:53:39 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:51:38 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:51:38 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:51:38 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:51:38 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:49:37 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:49:37 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:49:37 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:47:35 ...	Informational	302010	Connect	ASA-13	10.130.1	10.130.1
6/15/10 12:47:33 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:47:33 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:47:33 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:47:33 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:45:32 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:45:32 ...	Informational	302015	Bulk UDP	ASA-13	10.130.1	10.130.1
6/15/10 12:45:32 ...	Informational	302016	Tear-down UDP	ASA-13	10.130.1	10.130.1

Jump to Events from Policy

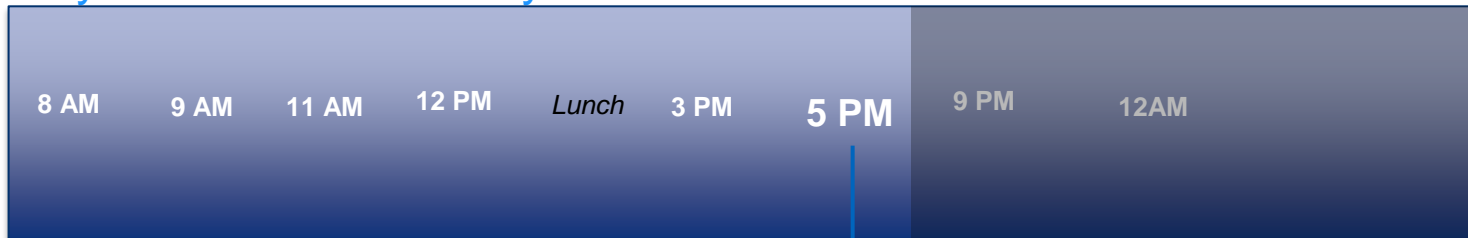
- A new right click menu item 'Show Events'
- When clicked, Event Viewer is launched with filters like Device, Source, Destination, Source/Destination Service, Source User Identity, Action and Source/Destination Security Group Tag/Name.



@ Office



Day in the life of Security Administrator



Challenges

- Are the policies deployed earlier working?
- Trouble shooting existing policies?
- Setting up alerts for critical assets
- Have I completed all my tickets?

SW updates
image
management

CSM Solution

CSM Image Manager

All ASA Software Upgrades Taken Care

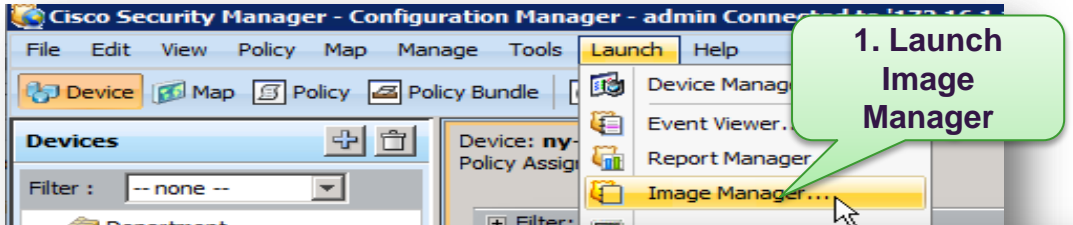
- Consolidated view of all ASA images that will matter for your n/w
- Validates jobs and hardware requirements before upgrade
- Notifications post image upgrades to provide the job status
- Reduces manual errors by doing all requisite checks before and after upgrades
- It can be done in batch.
- There is no requirement to re-discover the device back (except for NAT if moving from pre 8.3 to post 8.3). This is a great benefit from CSM perspective since the complete policy structure is maintained.

The screenshot displays the Cisco Security Manager - Image Manager interface. The window title is "Cisco Security Manager - Image Manager - admin Connected to 'jithakre-demo'". The interface includes a menu bar (File, Launch, Help), a toolbar with icons for installation and release notes, and a search bar. A notification at the top right states "Not updated. Click this button to start update." with a green refresh icon.

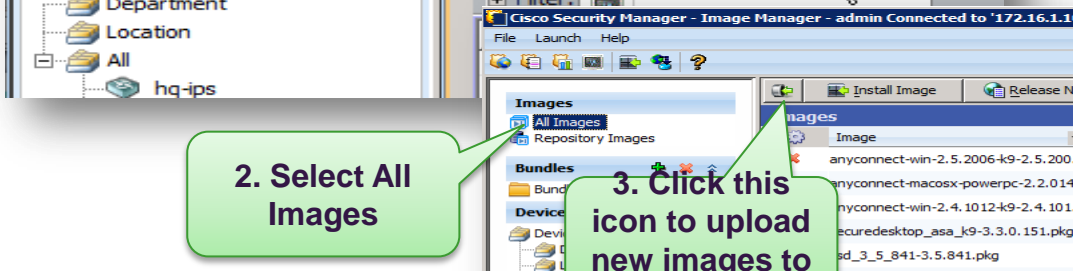
The main content area is titled "All Images" and contains a table with the following columns: Image, Type, Version, Location, Size, Description, and Comment. The table lists various software images, including AnyConnect Images and Cisco Secure Desktop Images, with their respective versions and sizes.

Image	Type	Version	Location	Size	Description	Comment
anyconnect-linux-k9-2.2.0.128.pkg	AnyConnect Image	2.2.0.128	Repository	3.5 MB	AnyConnect Image	
csd_3_6_181-3.6.181.pkg	Cisco Secure Desktop Image	3.6.181	Repository	25.5 MB	Cisco Secure Desktop Image	
anyconnect-macosx-powerpc-k9-2.2.0.128...	AnyConnect Image	2.2.0.128	Repository	3.2 MB	AnyConnect Image	
anyconnect-macosx-k9-2.2.0.140-k9...	AnyConnect Image	2.2.0.140	Repository	3.2 MB	AnyConnect Image	
anyconnect-linux-64-3.0.0.629-k9-3.0.0...	AnyConnect Image	3.0.0.629	Repository	6.3 MB	AnyConnect Image	
anyconnect-linux-2.2.0.140-k9-2.2.0.1...	AnyConnect Image	2.2.0.140	Repository	3.5 MB	AnyConnect Image	
anyconnect-macosx-powerpc-2.3.2016...	AnyConnect Image	2.3.2016	Repository	4.1 MB	AnyConnect Image	
securedesktop_asa-k9-3.3.0.118.pkg	Cisco Secure Desktop Image	3.3.0.118	Repository	4.5 MB	Cisco Secure Desktop Image	
anyconnect-macosx-k9-2.4.1012-k9...	AnyConnect Image	2.4.1012	Repository	4.6 MB	AnyConnect Image	
rdp-plugin-1.0.2.jar	Remote Access Plugin	1.0.2	Repository	850.2 KB	Remote Access Plugin	
anyconnect-win-2.3.2016-k9-2.3.2016...	AnyConnect Image	2.3.2016	Repository	2.5 MB	AnyConnect Image	
anyconnect-linux-3.0.0.629-k9-3.0.0.6...	AnyConnect Image	3.0.0.629	Repository	8.2 MB	AnyConnect Image	
anyconnect-macosx-k9-2.5.2006-k9...	AnyConnect Image	2.5.2006	Repository	6.1 MB	AnyConnect Image	
csd-3.4.0373.pkg	Cisco Secure Desktop Image	3.4.0373	Repository	8.5 MB	Cisco Secure Desktop Image	
anyconnect-linux-2.5.2006-k9-2.5.20...	AnyConnect Image	2.5.2006	Repository	6.3 MB	AnyConnect Image	
securedesktop_asa_k9-3.2.0.136.pkg	Cisco Secure Desktop Image	3.2.0.136	Repository	3.0 MB	Cisco Secure Desktop Image	
csd_3_5_2001-3.5.2001.pkg	Cisco Secure Desktop Image	3.5.2001	Repository	11.8 MB	Cisco Secure Desktop Image	
anyconnect-win-2.4.1012-k9-2.4.10...	AnyConnect Image	2.4.1012	Repository	4.9 MB	AnyConnect Image	
anyconnect-win-2.5.2006-k9-2.5.200...	AnyConnect Image	2.5.2006	Repository	4.4 MB	AnyConnect Image	
csd_3_5_2008-3.5.2008.pkg	Cisco Secure Desktop Image	3.5.2008	Repository	12.3 MB	Cisco Secure Desktop Image	
csd_3_4_2048-3.4.2048.pkg	Cisco Secure Desktop Image	3.4.2048	Repository	9.6 MB	Cisco Secure Desktop Image	
anyconnect-macosx-powerpc-2.4.101...	AnyConnect Image	2.4.1012	Repository	4.6 MB	AnyConnect Image	
anyconnect-macosx-powerpc-2.5.200...	AnyConnect Image	2.5.2006	Repository	6.1 MB	AnyConnect Image	
csd_3_5_841-3.5.841.pkg	Cisco Secure Desktop Image	3.5.841	Repository	11.5 MB	Cisco Secure Desktop Image	

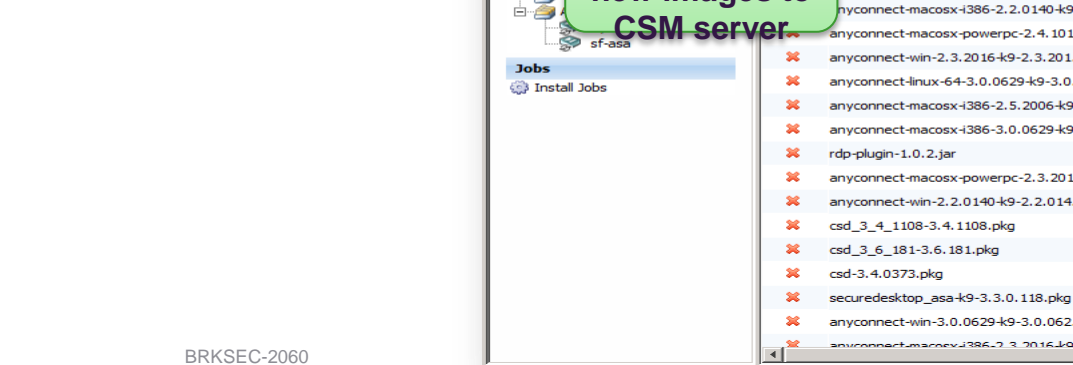
Launch ASA Image Manager



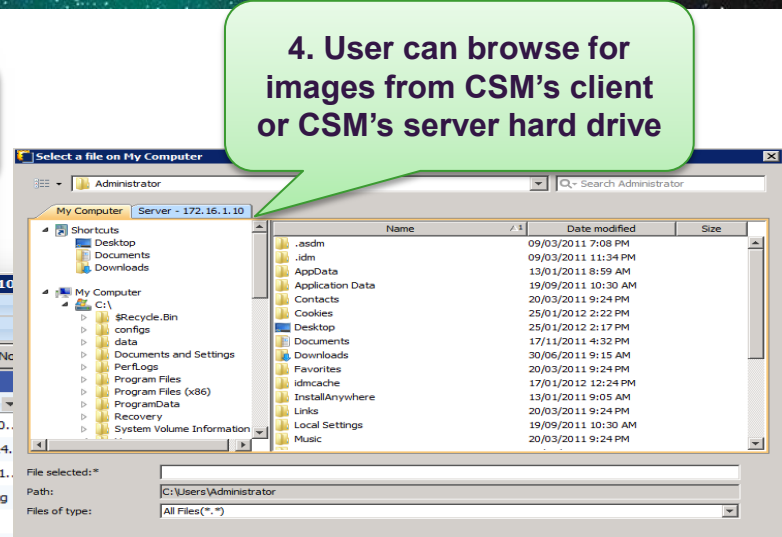
1. Launch Image Manager



2. Select All Images



3. Click this icon to upload new images to CSM server



4. User can browse for images from CSM's client or CSM's server hard drive

Name	Date modified	Size
.asdm	09/03/2011 7:08 PM	
.ldm	09/03/2011 11:34 PM	
AppData	13/01/2011 8:59 AM	
Application Data	19/09/2011 10:30 AM	
Contacts	20/03/2011 9:24 PM	
Cookies	25/01/2012 2:22 PM	
Desktop	25/01/2012 2:17 PM	
Documents	17/11/2011 4:32 PM	
Downloads	30/06/2011 9:15 AM	
Favorites	20/03/2011 9:24 PM	
Idmcache	17/01/2012 12:24 PM	
InstallAnywhere	13/01/2011 9:05 AM	
Links	20/03/2011 9:24 PM	
Local Settings	19/09/2011 10:30 AM	
Music	20/03/2011 9:24 PM	

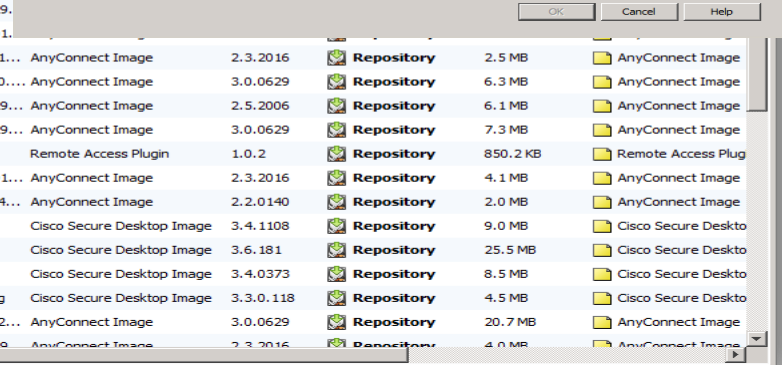


Image Name	Image Type	Version	Repository	Size	Icon
anyconnect-win-2.5.2006-k9-2.5.2006	AnyConnect Image	2.3.2016	Repository	2.5 MB	AnyConnect Image
anyconnect-macosx-powerpc-2.2.014	AnyConnect Image	3.0.0629	Repository	6.3 MB	AnyConnect Image
anyconnect-win-2.4.1012-k9-2.4.1012	AnyConnect Image	2.5.2006	Repository	6.1 MB	AnyConnect Image
securedesktop_asa_k9-3.3.0.151.pkg	AnyConnect Image	3.0.0629	Repository	7.3 MB	AnyConnect Image
sd_3_5_841-3.5.841.pkg	AnyConnect Image	1.0.2	Repository	850.2 KB	Remote Access Plug
anyconnect-macosx-i386-2.2.0140-k9	AnyConnect Image	2.3.2016	Repository	4.1 MB	AnyConnect Image
anyconnect-win-2.3.2016-k9-2.3.2016	AnyConnect Image	2.2.0140	Repository	2.0 MB	AnyConnect Image
anyconnect-linux-64-3.0.0629-k9-3.0.0629	AnyConnect Image	3.4.1108	Repository	9.0 MB	Cisco Secure Deskto
anyconnect-macosx-i386-2.5.2006-k9	AnyConnect Image	3.6.181	Repository	25.5 MB	Cisco Secure Deskto
anyconnect-macosx-i386-3.0.0629-k9	AnyConnect Image	3.4.0373	Repository	8.5 MB	Cisco Secure Deskto
rdp-plugin-1.0.2.jar	Remote Access Plugin	3.3.0.118	Repository	4.5 MB	Cisco Secure Deskto
anyconnect-macosx-powerpc-2.3.2016	AnyConnect Image	3.0.0629	Repository	20.7 MB	AnyConnect Image
anyconnect-win-2.2.0140-k9-2.2.0140	AnyConnect Image	2.3.2016	Repository	4.0 MB	AnyConnect Image
csd_3_4_1108-3.4.1108.pkg	Cisco Secure Desktop Image				
csd_3_6_181-3.6.181.pkg	Cisco Secure Desktop Image				
csd-3.4.0373.pkg	Cisco Secure Desktop Image				
securedesktop_asa-k9-3.3.0.118.pkg	Cisco Secure Desktop Image				
anyconnect-win-3.0.0629-k9-3.0.0629	AnyConnect Image				
anyconnect-macosx-i386-2.3.2016-k9	AnyConnect Image				

Assign Images to Devices

1. Select an Secure Desktop image

2. Click Install Image

3. Select additional image if needed

4. Click on Next

5. Select devices: sf-asa

Image Assignments - Select Devices or Images

Image	Type	Version
anyconnect-...	AnyConnect I...	2.5.2006
anyconnect-...	AnyConnect I...	2.2.0140
anyconnect-...	AnyConnect I...	2.4.1012
csd_3_5_841...	Cisco Secure ...	3.5.841
anyconnect-...	AnyConnect I...	2.2.0140
anyconnect-...	AnyConnect I...	2.4.1012
anyconnect-...	AnyConnect I...	2.3.2016
anyconnect-...	AnyConnect I...	3.0.0629
anyconnect-...	AnyConnect I...	2.5.2006
anyconnect-...	AnyConnect I...	3.0.0629
rdp-plugin-1	Remote Acce...	1.0.2

Image Assignments - Select Devices

List of Devices:

- All
 - ny-asa
 - sf-asa

List of Selected Devices:

- sf-asa

Configure Image Update Job

1. Click Start Validation

2. Click Warnings to view details

3. Select Schedule tab

4. Select future date/time or NOW

5. Adjust other parameters

1. Click Start Validation

Device	Image	Validation
sf-asa	securedesktop_asa_k9-3.3.0.151.pkg	Warning

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2		
5	6	7	8	9		

On Error
 Stop Installation
 Continue Installation

Backup Current Image
 Yes
 No

Install images to devices in
 Parallel
 Sequential

Install image and reboot device
 Install image and reboot device
 Install image, but do not reboot device
 Only copy image onto devices

Review Image Update Job Status

1. Device in Configuration Manager shows update is in progress

Device Name: sf-asa
Device Type: Cisco ASA-5505 Adaptive Security Appliance
IP Address: 172.16.1.90
IP Type: Static
Host.Domain: sf-asa
OS Type: ASA
Target OS Version: 8.4(1)
Running OS Version: 8.4(1)
Device State: Update in Progress

The screenshot shows the Configuration Manager interface with a tree view on the left containing 'Department', 'Location', and 'All' folders. Under 'All', there are sub-folders for 'hq-ips', 'ny-asa', 'ny-asa-ssm', and 'sf-asa'. The 'sf-asa' folder is selected, and a callout box displays its details. The 'Policies' section on the left shows 'Firewall' rules like AAA, Access, IPv6, Inspection Rules, Botnet Traffic Filter Rules, Settings, and Web Filter Rules.

2. Review Job results

Name	Last Action	Status	Changed By	Description	Schedule
Image install Job - 26 Jan 2012 14:29:54	26 Jan 2012 14:34:38	Deployed	admin	Image install Job added ...	

Summary	Details	History
Status:	Deploying	
Image Management Job Name:	Image install Job - 26 Jan 2012 14:29:54	
Devices To Be Deployed:	1	
Devices Deployed Successfully:	0	
Devices Deployed With Errors:	0	

The screenshot shows the Image Manager interface with a 'Jobs' table and a summary section. The 'Jobs' table has columns for Name, Last Action, Status, Changed By, Description, and Schedule. The summary section has tabs for Summary, Details, and History, and displays key metrics for the job.

Review Device Installed Images & Status

The screenshot displays the Cisco Security Manager - Image Manager interface. The left sidebar shows a tree view with 'Devices' expanded to 'ny-asa'. The main pane shows device details for 'sf-asa' and a table of installed images.

1. Select sf-asa

2. Review Device software information

3. Review device's flash information

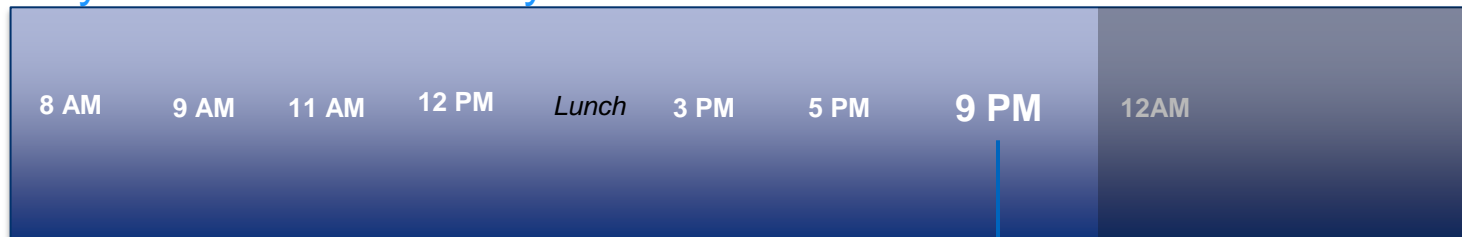
4. Review other information

Storage	Running Images	Compatible Images	History
disk0:/8_3_1_0_startup_cfg.sav			Unknown Image
disk0:/securedesktop_asa_k9-3.3.0.151.pkg			Cisco Secure Desktop Image
disk0:/upgrade_startup_errors_201009082035.log			Unknown Image
securedesktop-asa-3... 1.7 MB	disk0:/securedesktop-asa-3.1.1.29-k9.pkg		Cisco Secure Desktop Image
8_2_1_0_startup_cf... 2.6 KB	disk0:/8_2_1_0_startup_cfg.sav		Unknown Image
asa831-k8.bin 15.2 MB	disk0:/asa831-k8.bin		ASA System Software
nat_ident_migrate 0 B	disk0:/nat_ident_migrate		Unknown Image
cd_urn_..._10_cfg...	disk0:/cd_urn_..._10_cfg...		Unknown Image

@ Office



■ Day in the life of Security Administrator



Challenges

- Are the policies deployed earlier working?
- Trouble shooting existing policies?
- Setting up alerts for critical assets
- Have I completed all my tickets?

Deployment

Scalable Distributed Deployment

What Is It?

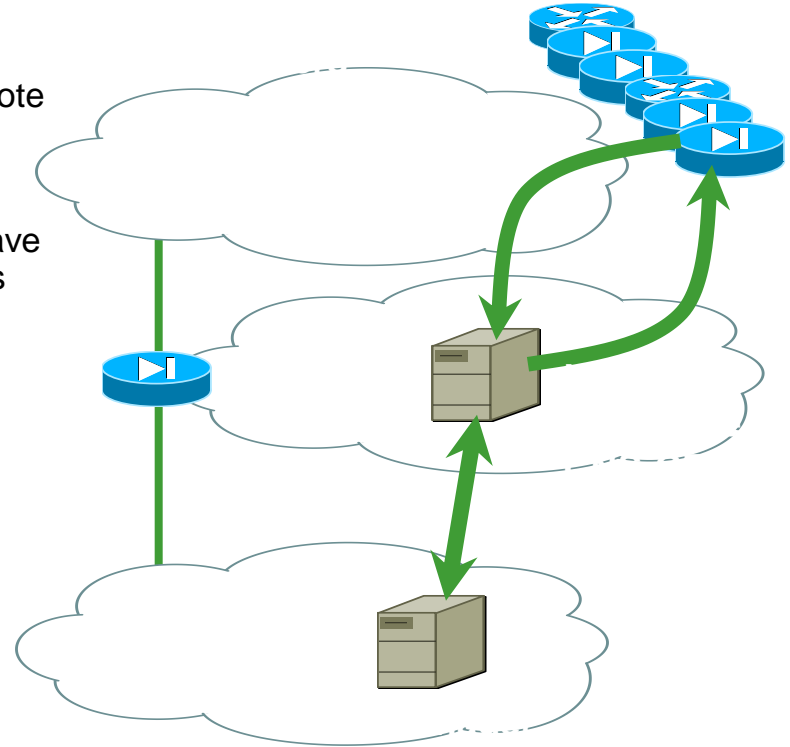
- Simplified distributed deployment method for 1000s remote devices

Example

- Update large numbers of remote firewalls, which may have dynamic addresses, intermittent links, or NAT addresses
- Update both configurations and software images
- Devices self updated whenever they come online
- Scales through Web technologies

Benefit

- Helps customers with 1000s of teleworkers and remote locations with minimal technical staff at the remote site




Deployment Manager

- Deployment choices: deploy to file, device, token server, AUS, etc.
- Schedule job deployments with notification and approval
- Lets users select devices to deploy and provides deployment report

The screenshot shows the Deployment Manager application window. At the top, there is a title bar with the text "Deployment Manager". Below the title bar is a section titled "Deployment Job Table (5/5 loaded)". This section contains a table with the following columns: Name, Last Action, Status, Changed By, and Description. The table lists five deployment jobs, with the first one being "Deployed" and the others "Failed".

Name	Last Action	Status	Changed By	Description
admin_job_2005-12-05 15:07:4...	05-Dec-2005 15:08:04	Deployed	admin	Auto Created Deployment Job i...
admin_job_2005-12-05 15:04:2...	05-Dec-2005 15:04:27	Failed	admin	Auto Created Deployment Job i...
admin_job_2005-12-05 15:02:0...	05-Dec-2005 15:02:08	Failed	admin	Auto Created Deployment Job i...
admin_job_2005-12-05 15:00:0...	05-Dec-2005 15:01:21	Failed	admin	Auto Created Deployment Job i...
admin_job_2005-12-05 14:56:2...	05-Dec-2005 14:57:05	Failed	admin	Auto Created Deployment Job i...

Below the table are five buttons: Deploy, Refresh, Redeploy, Abort, and Rollback. Below the buttons is a section titled "Summary" with a "Details" tab. The Summary section displays the following information:

Deployment Job Name: admin_job_2005-12-05 15:07:43.718
Deployment Status: Deployed
Progress Status:  3 out of 4 devices completed. (75%)
Number Of Devices To Be Deployed: 4
Number Of Devices Deployed Successfully: 3
Number Of Devices Deployed With Errors: 0

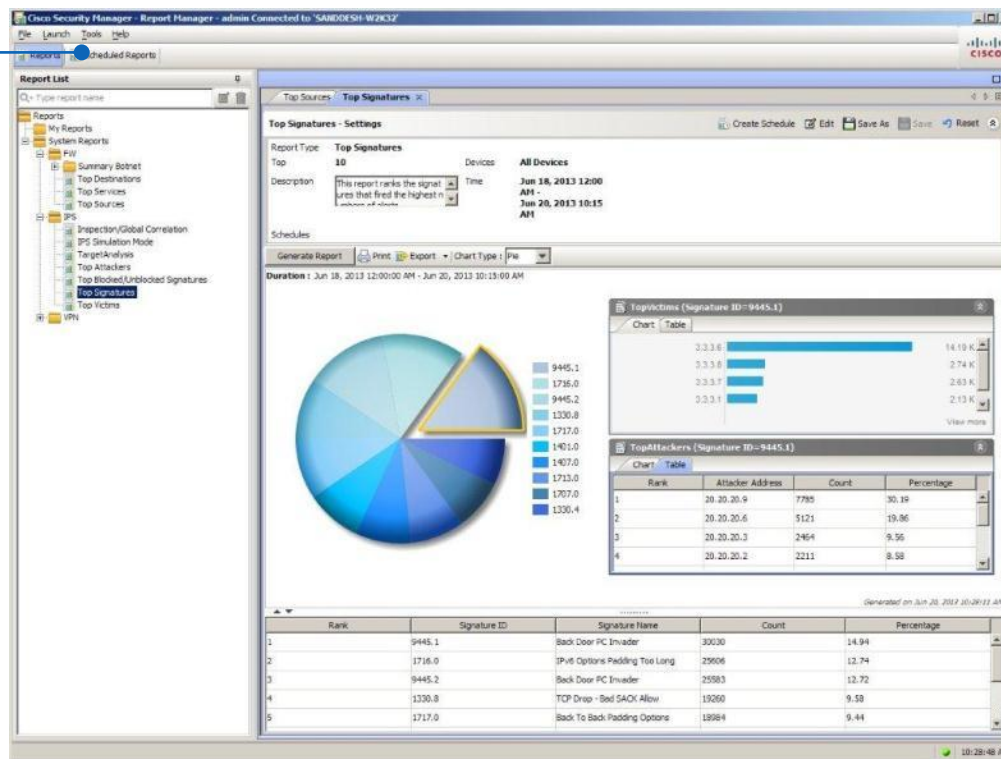
At the bottom right of the window are "Close" and "Help" buttons.

CSM Solution

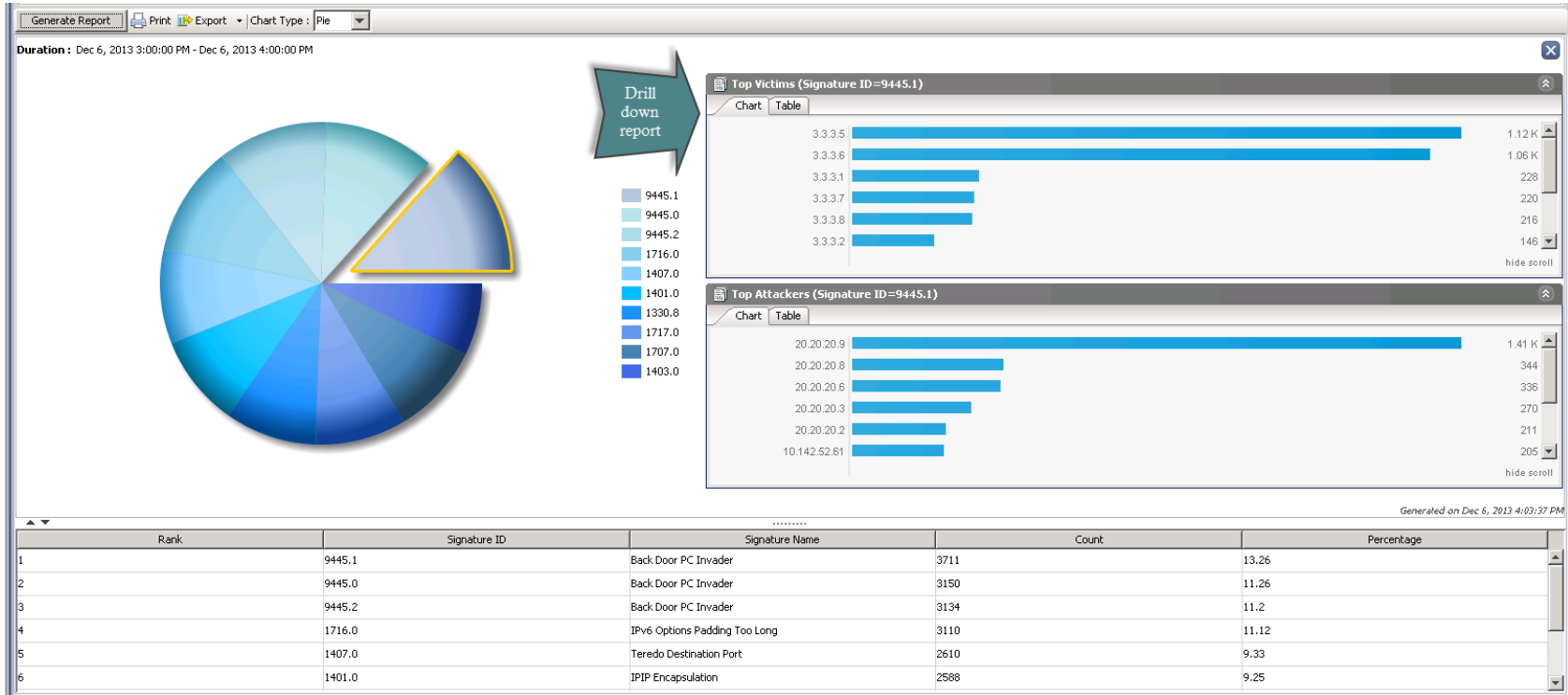
CSM Report Manager

Standard Reports with Drilldown Capabilities

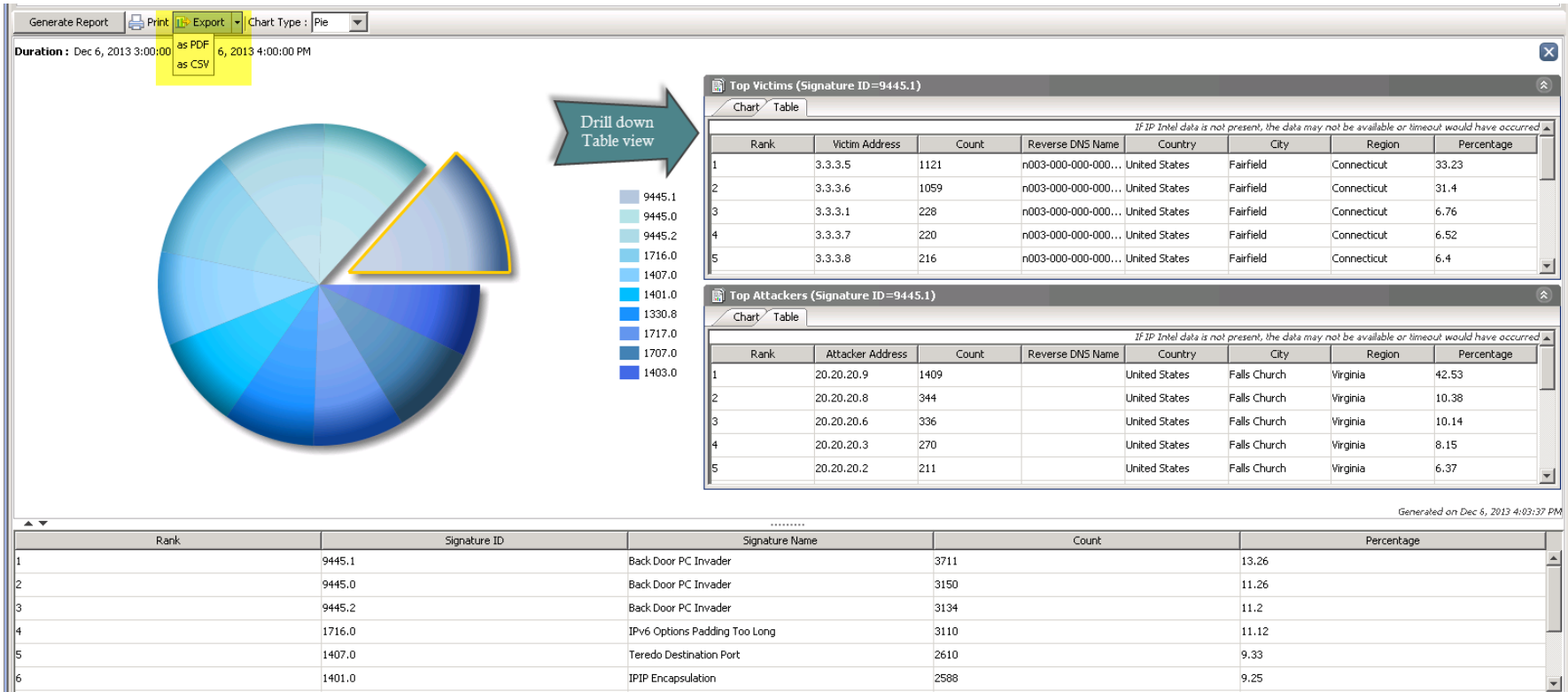
- Out of box systems reports for FW, IPS, and VPN
- Ability to export reports to most commonly used formats
- Users can define and save custom views of standard reports
- Drill down from reports to relevant data points through the application



Sample Drill Down Report



Some More....



Send Report via Email

Security Manager Notification: Schedule ff run successful on Wed Dec 11 20:00:13 CET 2013

Wednesday, December 11, 2013 8:00:43 PM

From admin@domain.com

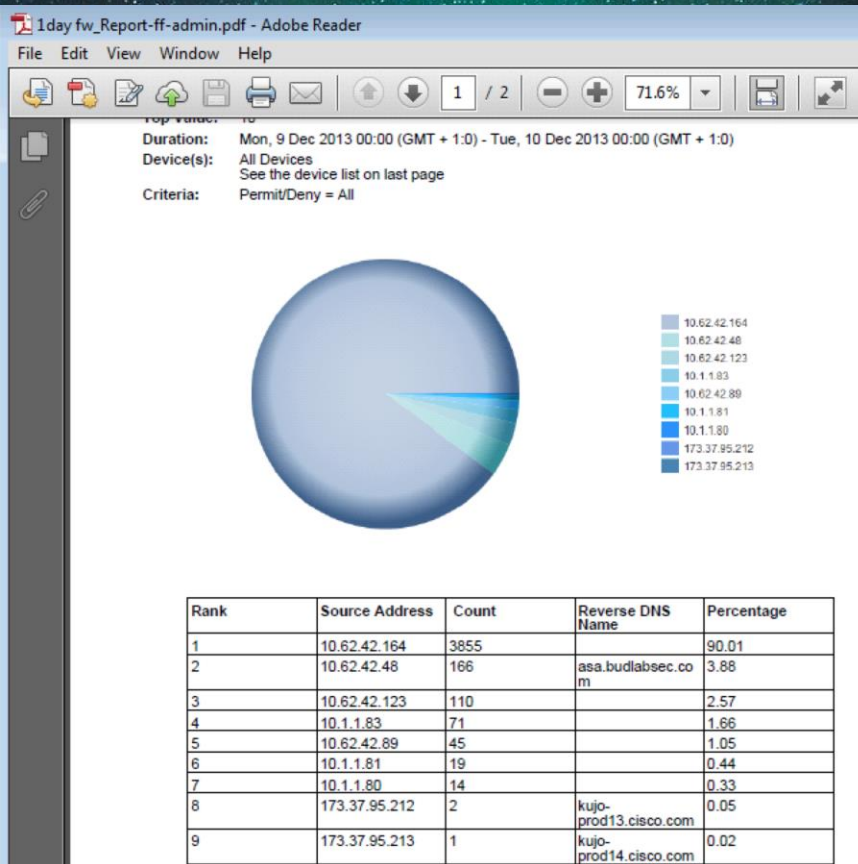
To gacs@budlabsec.com

Attachments 1day_fw_Report-ff-admin.pdf

Dear User,

Schedule **ff** succeeded in generating **1day fw** report on Wed Dec
11 20:00:13 CET 2013

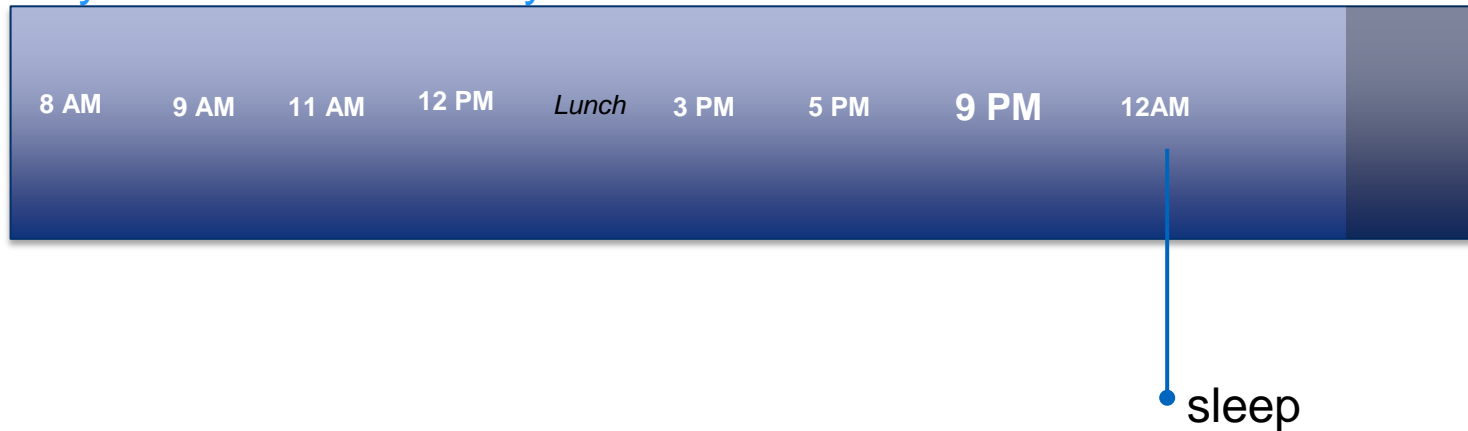
Attached:pdf



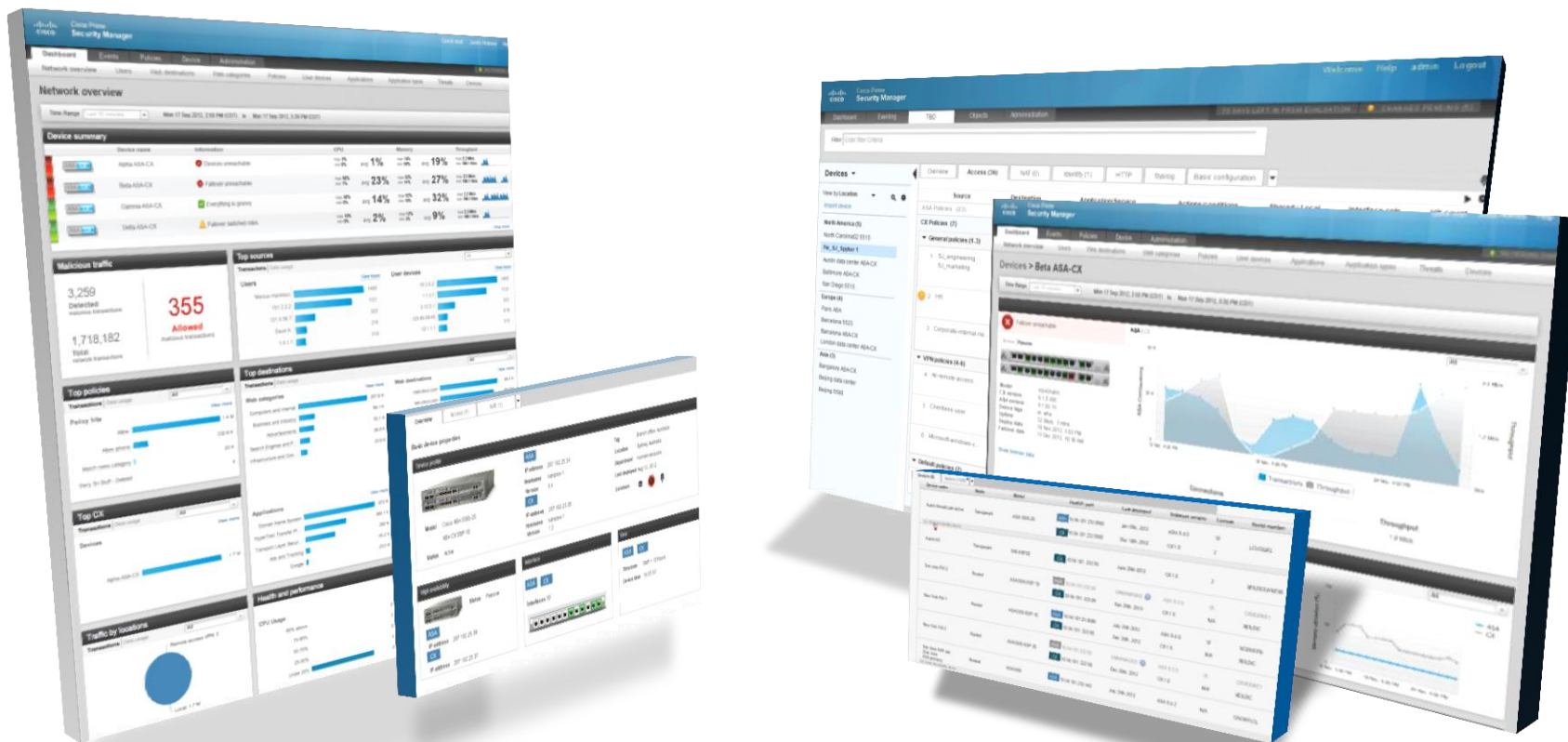
@ Office



■ Day in the life of Security Administrator



Cisco Prime Security Manager



PRSM

SMB to Med Enterprise

- Primarily for Cisco NG firewall or called “CX”
- Focus on easy to use simple deployments
- Basic ASA management
- Focus on NGFW features
 - L7 Applications
 - URL filtering
 - NGIPS
 - Basic ASA management

PRSM

In Action (Operations)

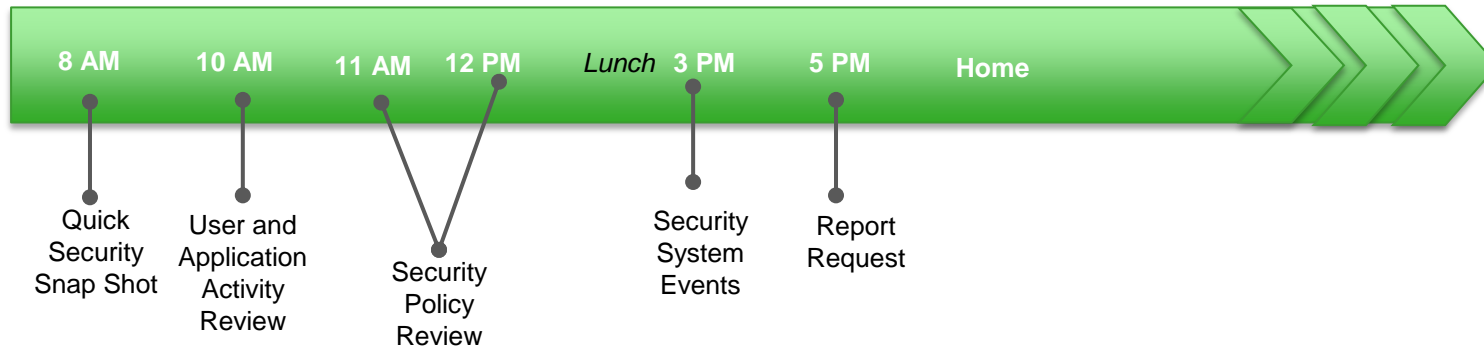
- Dashboard
- New Policy Model
- Events
- Reports

PRSM in Action

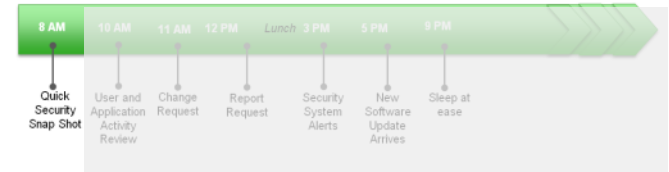
Security Admin



■ Day in the life of Security Administrator



Quick Security Snap Shot



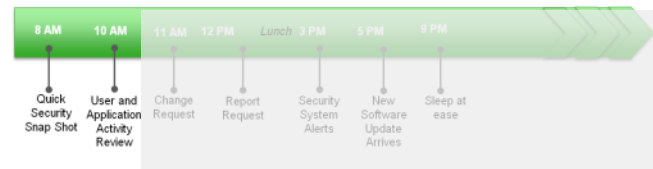
To be added

User and Application Activity Review

Top 25 applications by transactions

02 Feb 2014, 03:30:39 AM (UTC) to 03 Feb 2014, 03:30:39 AM (UTC)

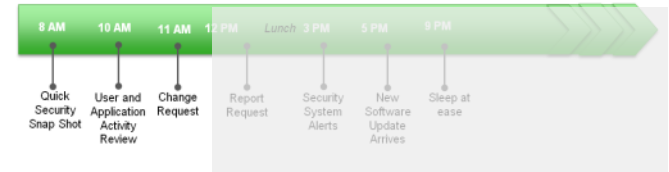
	Application	Transactions			Bytes			Top 5 by transactions		
		Total	Allowed	Denied	Total	Sent	Received	Users	Web destinations	
1	HyperText Transfer Protocol	99.0 K	96.0 K	2.0 K	2.0 GB	29.0 MB	2.0 GB	ADRI\Ranj Sharma 9.0 K ADRI\Vikram Kulkarni 8.0 K ADRI\Dilbert Geek 8.0 K ADRI\Ami Kurosawa 8.0 K ADRI\Sean Darrell 8.0 K	www.best-of-web.com 535 www.mars.com 493 www.hollywoodtuna.com 438 updates.ironport.com 420 www.northamericanwhitetail.com 404	
2	SharePoint	2.0 K	2.0 K	8	81.0 MB	793.0 KB	81.0 MB	ADRI\Jane Radcliff 488 ADRI\Ira Blue 370 ADRI\Vikram Kulkarni 207 ADRI\Harry Houdini 200 ADRI\Ranj Sharma 195	www.nsc.org 270 www.sru.edu 257 www.health.nsw.gov.au 178 www.rightathome.com 168 www.northern.edu 158	
3	Generic Search Engine Traffic	871	838	33	11.0 MB	227.0 KB	11.0 MB	ADRI\Jane Radcliff 117 ADRI\Ira Blue 105 ADRI\Sean Darrell 86 ADRI\Wicki Dustin 74 ADRI\Harry Houdini 66	www.korea.net 85 www.cowboy.com 84 www.tom.com 74 www.thefreesite.com 72 www.yam.com 61	
4	Transport Layer Security Protocol	698	602	96	3.0 MB	1.0 MB	2.0 MB	ADRI\Jane Radcliff 110 ADRI\Ira Blue 103 ADRI\Ranj Sharma 62 ADRI\Nina Chemski 54 ADRI\Rita Meter 54	www.cisco.com 26 news-tags.cisco.com 6 cisco-tags.cisco.com 6 www.static-cisco.com 2	
5	Domain Name System	536	536	0	119.0 KB	18.0 KB	100.0 KB	ADRI\Rita Meter 301 172.16.1.240 207 172.16.1.100 28		
6	SSL	501	501	0	496.0 MB	1.0 MB	494.0 MB	172.16.1.80 251 172.16.1.120 250		
7	eBay	223	205	18	4.0 MB	78.0 KB	4.0 MB	ADRI\Rita Meter 209 ADRI\Vikram Kulkarni 5 ADRI\Ranj Sharma 5 ADRI\Ira Blue 1 ADRI\Sean Darrell 1	i.ebayimg.com 143 ir.ebaystatic.com 18 srx.main.ebayfm.com 16 rtm.ebaystatic.com 14 www.ebay.com 10	
8	Binary over HTTP	176	69	107	2.0 MB	37.0 KB	2.0 MB	ADRI\Nina Chemski 46 ADRI\Harry Houdini 44 ADRI\Jane Radcliff 17 ADRI\Dilbert Geek 14 ADRI\Sean Darrell 14	download.registrysmart.com 8 download.errorsmsmart.com 6 carlo20.dyn dns.org 6 banner.cd poker.com 6 lmon2web.org 5	
9	Flash Video	140	140	0	40.0 MB	38.0 KB	40.0 MB	ADRI\Sean Darrell 17 ADRI\Ira Blue 16 ADRI\Jane Radcliff 16 ADRI\Ami Kurosawa 14 ADRI\Vikram Kulkarni 13	www.cyberbee.com 18 www.yamaha.com 6 www.lostvectors.com 4 www.learningplanet.com 4 www.groovygirls.com 4	

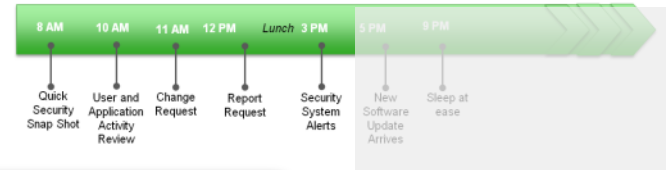


PRSM New Policy Model

The screenshot displays the Cisco PRSM interface with several callouts highlighting key features of the new policy model:

- Device Selector:** A callout pointing to the 'Devices' dropdown menu on the left sidebar.
- ASA Policy Tab:** A callout pointing to the 'ASA policies (22)' tab in the top navigation bar.
- CX Policy Tab:** A callout pointing to the 'Context aware policies (22)' tab in the top navigation bar.
- Device Configuration Tab:** A callout pointing to the 'Basic configuration' tab in the top navigation bar.
- Policy Sharing:** A callout pointing to the 'Shared (3)' section in the policy configuration area.
- 5-Tuple Rule base:** A callout pointing to the 'General policies (1-3)' section, which lists policies like 'S_J_engineering' and 'HR'.
- Install On:** A callout pointing to the 'Install this policy on' dropdown menu, which lists devices like 'North Carolina02 5515' and 'Fw_SJ_Spyker 1'.





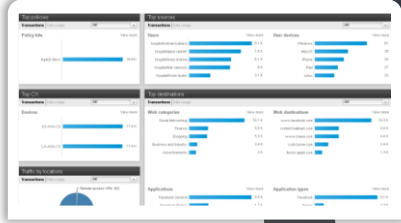
Receive Time	Event Type	Device	Username	Source	Destination Host	Destination Port	Application	Reputation Score	Web Category
01/23/2013 23:37:38	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	80	Facebook Ge...	5.9	Social Networking
01/23/2013 23:37:35	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:33	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:33	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:32	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:25	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443		4.0	Social Networking
01/23/2013 23:37:25	HTTP Complete	LA-ASA-CX	vicki dustin	vicki dustin	www.facebook.com	443	Facebook Ge...	4.0	Social Networking

Cisco Prime Security Manager in Action

Key Benefits

- Greater visibility and control
- Enhanced threat response and mitigation
- Unified management for core ASA firewall and NGFW services
- Straightforward migration to ASA 5500-X NGFW
- Intuitive, easy-to-use GUI

Dashboard



Navigate Down to Events

Receive Time	Event Type	Device	Username	Source	Destination Host	Destination Port	Application	Reputation Score	Web Category
01/23/2013 23:37:30	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	80	Facebook Ge	5.9	Social Networking
01/23/2013 23:37:36	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Co	4.0	Social Networking
01/23/2013 23:37:33	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Co	4.0	Social Networking
01/23/2013 23:37:32	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Co	4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Co	4.0	Social Networking
01/23/2013 23:37:27	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Co	4.0	Social Networking
01/23/2013 23:37:25	HTTP Complete	LA-ASA-CX	vicki_dustin	vicki_dustin	www.facebook.com	443	Facebook Ge	4.0	Social Networking

Visibility & Control

View Event

HTTP Complete (Event ID: 1546142) Time stamp: Wed 23 Jan 2013, 11:57 PM

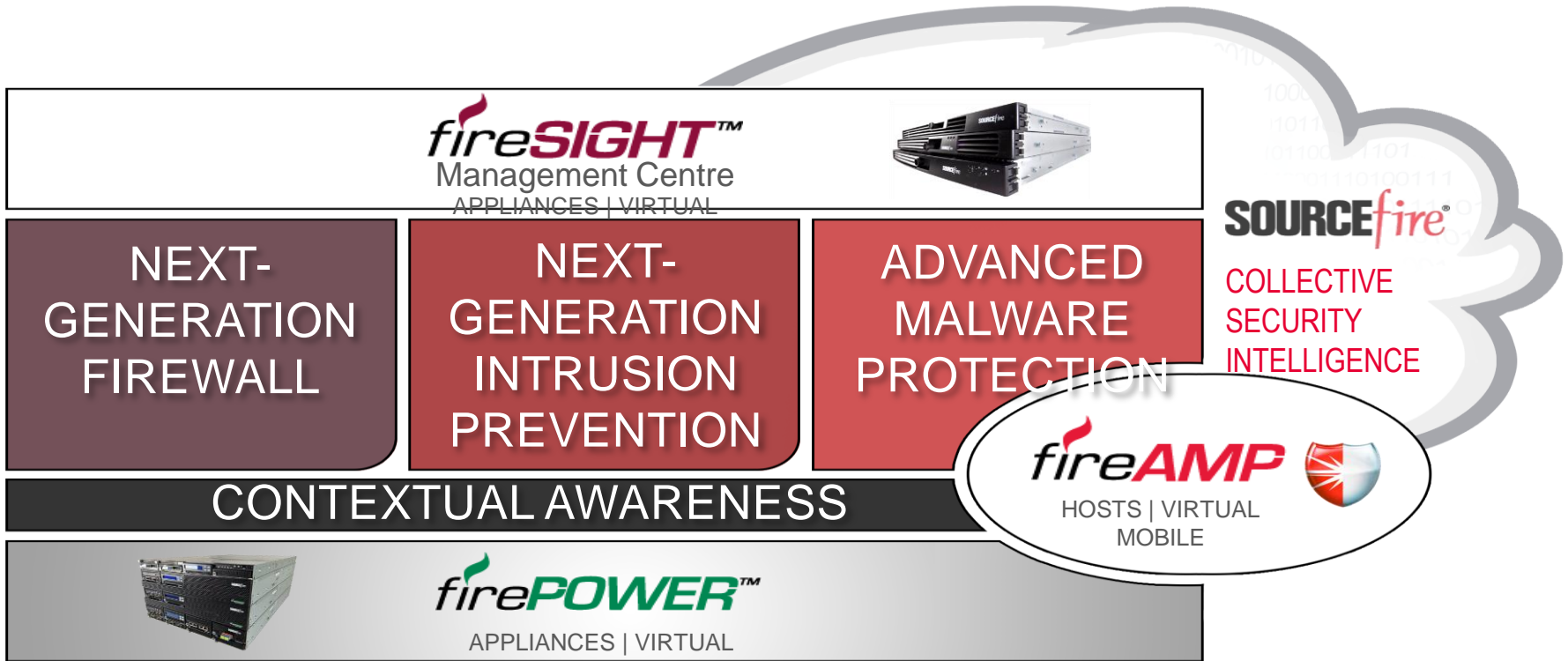
An HTTP transaction passed policy controls and completed normally.

Event details		Destination	Transaction
Source	User: vicki_dustin	IP address: 41.158.79.26	Flow ID: 1546142
	Device: Inside	Port: 80	Transaction ID: 157
	IP address: 58.85.0.19	Service: http	Component name: HTTP
	Port: 8080	URL: www.facebook.com	HTTP verb: GET
	URL: http://www.facebook.com	Host request: 538	Total bytes: 1043
	Parent device: none	URL category: SocialNetworking	Response content type: text/html
	Parent device: none	Web reputation: 5.9	HTTP response code: 200
			HTTP app detected: OTHER
			Configuration version: 1.0.0
			Event status: Error status

Map Events to Policies

#	Source	Destination	Application/Service	Actions/conditions	Install on	Interface role	Hit count	Eventing	Packet capture
s1 track policies (1-14)									
▼ Policies created from monitoring (1-2)									
1	Engineering	Data center 1 Data center 2	ICMP NTP TCP	Deny Weekends and evenings Expires Aug 12th 2014	Universal	Inside	144 in last 24h	OFF	OFF
2	Engineering	Data center 1 Data center 2	ICMP NTP TCP	Allow Expires Aug 12th 2014	Local	Outside	144 in last 24h	OFF	OFF
DMZ (1-14)									

Cisco/Sourcefire Product Portfolio



FireSIGHT Sees “Everything”



CATEGORIES	EXAMPLES	SOURCEFIRE NGIPS & NGFW	TYPICAL IPS	TYPICAL NGFW
Threats	Attacks, Anomalies	✓	✓	✓
Users	AD, LDAP, POP3	✓	✗	✓
Web Applications	Facebook Chat, Ebay	✓	✗	✓
Application Protocols	HTTP, SMTP, SSH	✓	✗	✓
File Transfers	PDF, Office, EXE, JAR	✓	✗	✓
Malware	Conficker, Flame	✓	✗	✗
Command & Control Servers	C&C Security Intelligence	✓	✗	✗
Client Applications	Firefox, IE6, BitTorrent	✓	✗	✗
Network Servers	Apache 2.3.1, IIS4	✓	✗	✗
Operating Systems	Windows, Linux	✓	✗	✗
Routers & Switches	Cisco, Nortel, Wireless	✓	✗	✗
Mobile Devices	iPhone, Android, Jail	✓	✗	✗
Printers	HP, Xerox, Canon	✓	✗	✗
VoIP Phones	Avaya, Polycom	✓	✗	✗
Virtual Machines	VMware, Xen, RHEV	✓	✗	✗

Contextual Awareness

Information Superiority



FireSIGHT Enables Automation



IT Insight

Spot rogue hosts, anomalies, policy violations, and more



Impact Assessment

Threat correlation reduces actionable events by up to 99%



Automated Tuning

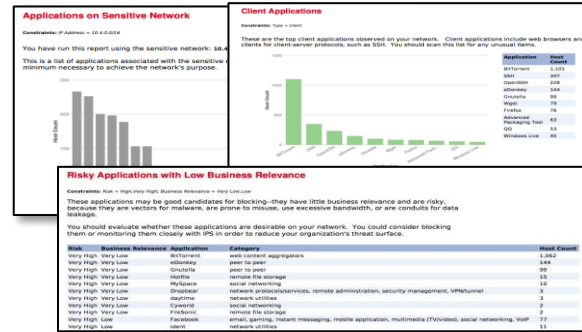
Adjust IPS policies automatically based on network change



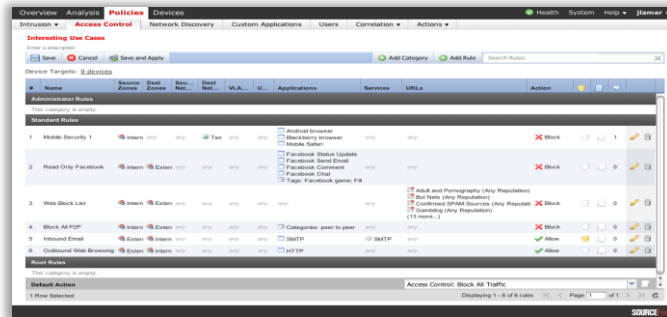
User Identification

Associate users with security and compliance events

FireSIGHT Management Centre v5 Benefits

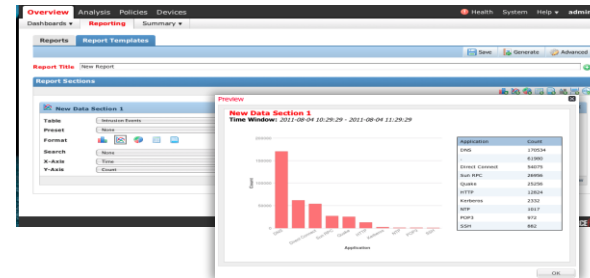


Innovative Admin Experience



Simplified Policy Model

New Reporting Engine

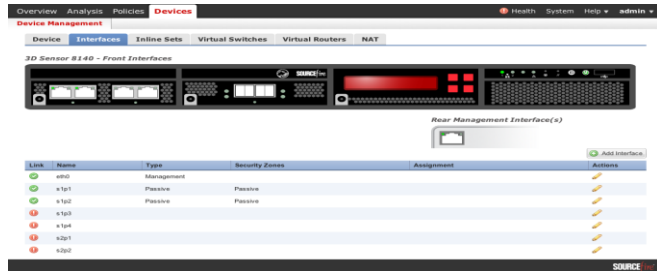


Flexible Report Creator

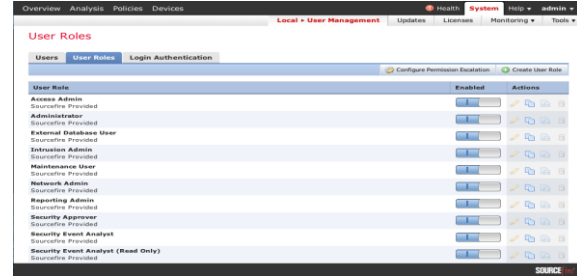
FireSIGHT Management Centre v5 Benefits

Country Name	Count	Initiator IP	Initiator Location	Responder IP
United States	162			
Germany				
China				
Japan		76.100.209.66	USA	10.4.32.112
France		10.4.10.131		10.4.32.112
Russia		10.4.10.131		10.4.32.112
North Korea		10.4.10.131		10.4.32.112
Pakistan		10.4.33.95		10.5.32.206
Iran		89.188.101.82	ISR	10.5.32.206
Iran		200.189.215.85	BRA	10.4.33.44
		10.4.31.237		10.5.32.206
		10.4.11.216		10.5.39.206

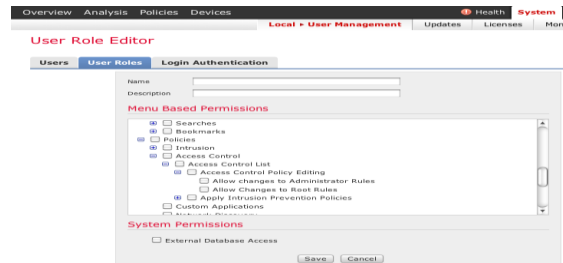
Geolocation in Events & Dashboards



New Device Management



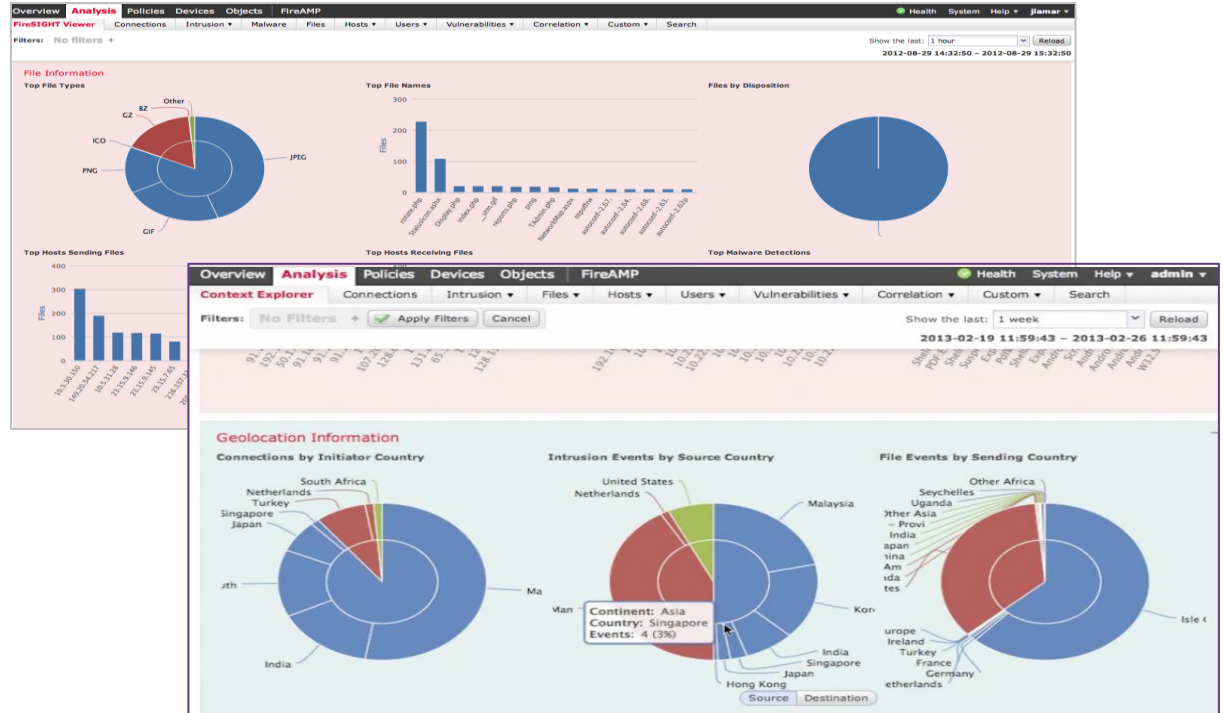
Security & Network Admin Roles



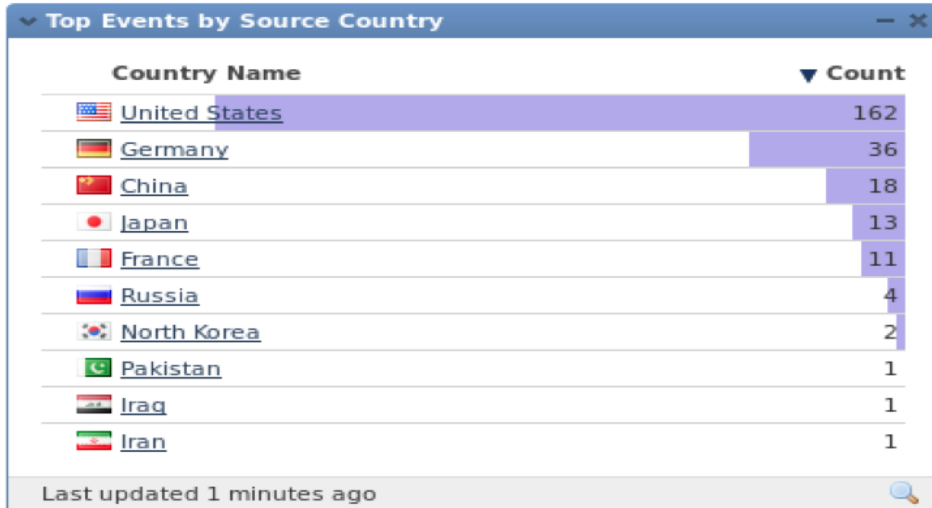
Admin Role Editor

Context Explorer

- Visualisation
- Explore Large Volumes of Security Data
- Identify Risky Hosts and Applications
- See Low Productivity and Bandwidth Misuse
- Acquire Actionable Intelligence



Geolocation



Initiator IP	Initiator Location	Responder IP
 76.100.209.66	 USA	 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.33.95		 10.5.32.206
 89.188.101.82	 ISR	 10.5.32.206
 200.189.215.85	 BRA	 10.4.33.44
 10.4.31.237		 10.5.32.206
 10.4.11.216		 10.5.39.206



- Visualise and map countries, cities of hosts, events

Devices Supported by CS Manager

- Security Appliances
 - PIX 500 Series
 - ASA 5500 Series w/ AIP-SSM
 - IPS 4200 Series Sensors
- IOS Routers
 - 70, 90, 800, 1600, 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7300, 7500, 7600 Series
 - NM-CIDS
- Catalyst 6500/7600 Services Modules
 - FWSM
 - IDSM-2
 - VPNSM
 - VPN SPA
- Catalyst 6500 Series Switches

ASA/CX Installation Workflow



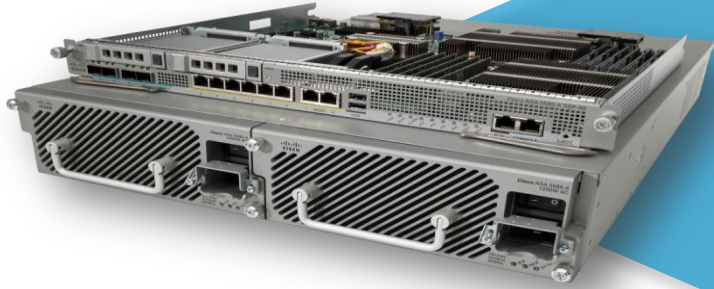
- New customers buying ASA and CX
 - Manufacturing installs CX completely before shipping
 - CX is booted automatically when ASA is started
 - Login to CX console from ASA CLI and setup management IP
 - Configure CXSC redirection on ASA for traffic redirection

- Customers who already own an ASA
 - Install one or two SSDs on ASA depending on the model*
 - Copy **9.1.1 ASA image** which supports CX onto flash filesystem
 - CX uses 3GB space on ASA flash filesystem, so ensure we have more than 3GB free space on ASA flash
 - Reload ASA with **9.1.1 version**
 - Follow the bootstrapping steps

ASA Support

Supported OS & Models

Peregrine



9.0 +

5510
5512-X
5515-X
5520,
5525-X
5540
5545-X
5550
5555-X
5585-10
5585-20
5585-40
5585-60

PRSM Offerings

Virtual & Appliance



Intel Dual Core 8GB
RAM, 500 GB HDD,
ESXi 4.0, 5.0

Starting at \$ 3,000

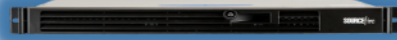
100 Devices
(ASA/CX) max: 5000
policies, 10000
objects, 15K eps

2.47 Ghz, 16GB
RAM, 6TB HDD

Starting at \$ 24,000

FireSIGHT Management

Centre Appliances



DC750

DC1500

DC3500

	DC750	DC1500	DC3500
Max. Devices Managed*	10	35	150
Max. IPS Events	20M	30M	150M
Event Storage	100 GB	125 GB	400 GB
Max. Network Map (hosts / users)	2k / 2k	50k / 50k	300k / 300k
High Availability Features	Lights-out Management (LOM)	RAID 1, LOM, High Availability pairing (HA)	RAID 5, LOM, HA, Redundant AC Power

* Max number of devices is dependent upon sensor type and event rate



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO™