

Dubrovnik, Croatia, South East Europe
20-22 May, 2013

Cisco Firewall Update

György Ács – Cisco Systems



Agenda

ASA Next Generation Firewall and Prime Security Manager

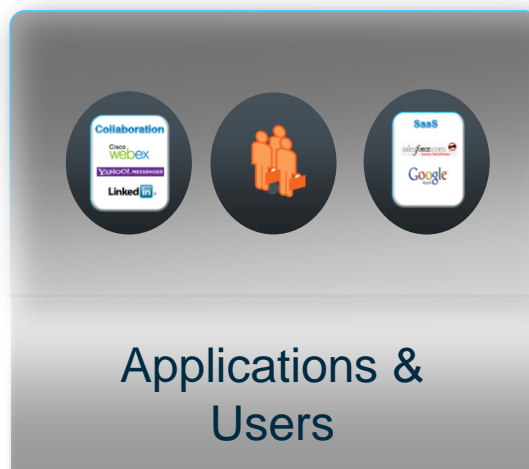
Cisco Security Manager 4.4



ASA Next Generation Firewall (CX)



Firewall Evolution



Phase 1















Phase 2

Phase 3

ASA Next Gen Firewall adds context-aware security to the ASA product line. PRSM provides common management experience.

Application Visibility and Control

Enforcing acceptable usage

1,000+ apps	    
75,000+ MicroApps	    
Application Behavior	   

- **Greatest control and visibility over mobile, collaborative, and web 2.0 applications**
- Ensures security of (and from) port-hopping applications, such as Skype and BitTorrent
- Granular enforcement of behaviors within applications
- Visibility of activity across the network
- Visit <http://asacx-cisco.com>

How ASA Next Gen Firewall Addresses Access Control

Beyond ports and protocols

Who: Identity and Authentication

What: Application, URL Category, Reputation

How: Device, OS, User Agent, Posture

Where: Local, Remote

Next Generation Firewall / ASA CX

Context-Aware Firewall

Active/Passive
Authentication

Application Visibility and
Control

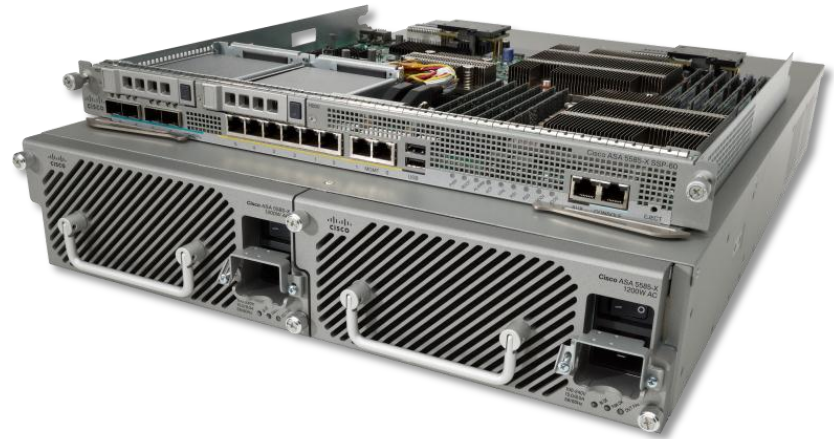
Reputation Filtering

URL Filtering

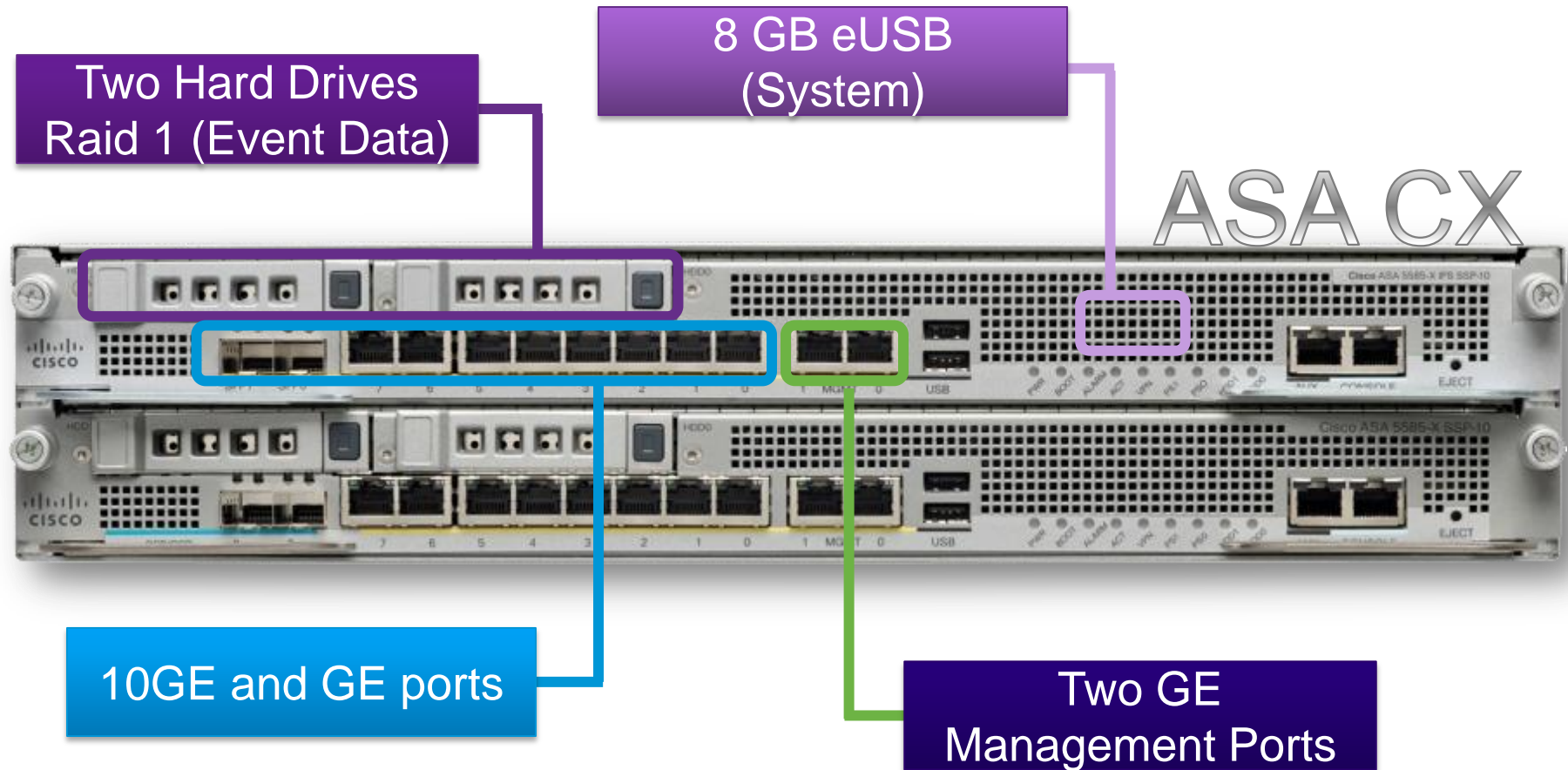
Secure Mobility

SSP-10 and SSP-20 at FCS

On ASA-X from 2012 Dec



ASA CX Module in ASA 5585-X chassis



ASA CX in 5500-X chassis

ASA 5512, 5515, 5525 (1RU 15.5" Chassis Depth)



ASA 5545, 5555 (1RU 19.05" Chassis Depth)



**CX Hard drive Bay(s)
(RAID-1 on ASA 5545/5555
chassis)**

Licenses enable the CX functionality

All CX licenses are subscription based (1,3 or 5 years)

Application Visibility and Control(AVC)

- enables application visibility

- enables application based access control

- e.g. block Skype

WebSecurity Essential(WSE)

- enables URL filtering and Web reputation based access control

- e.g. block „Gaming Sites“

Licenses can be purchased separately

Bundled licenses (AVC+WSE) available

No **User-Counts** apply for any license

All licensing is managed via PRSM-UI

Licenses

4 results

I want to... ▼

Application Visibility and Control license

Expiration date: 11 Mar 2013

Model: Trial license applied to all models

Used Devices:1

PAK: Evaluation Application Visibility and Control License

Device name / Description	IP Address	Software version	Model	Commit version	Device group
ASA CX	localhost	9.1.1 (1)	ASA5515	0	default

Web Security Essentials license

Expiration date: 11 Mar 2013

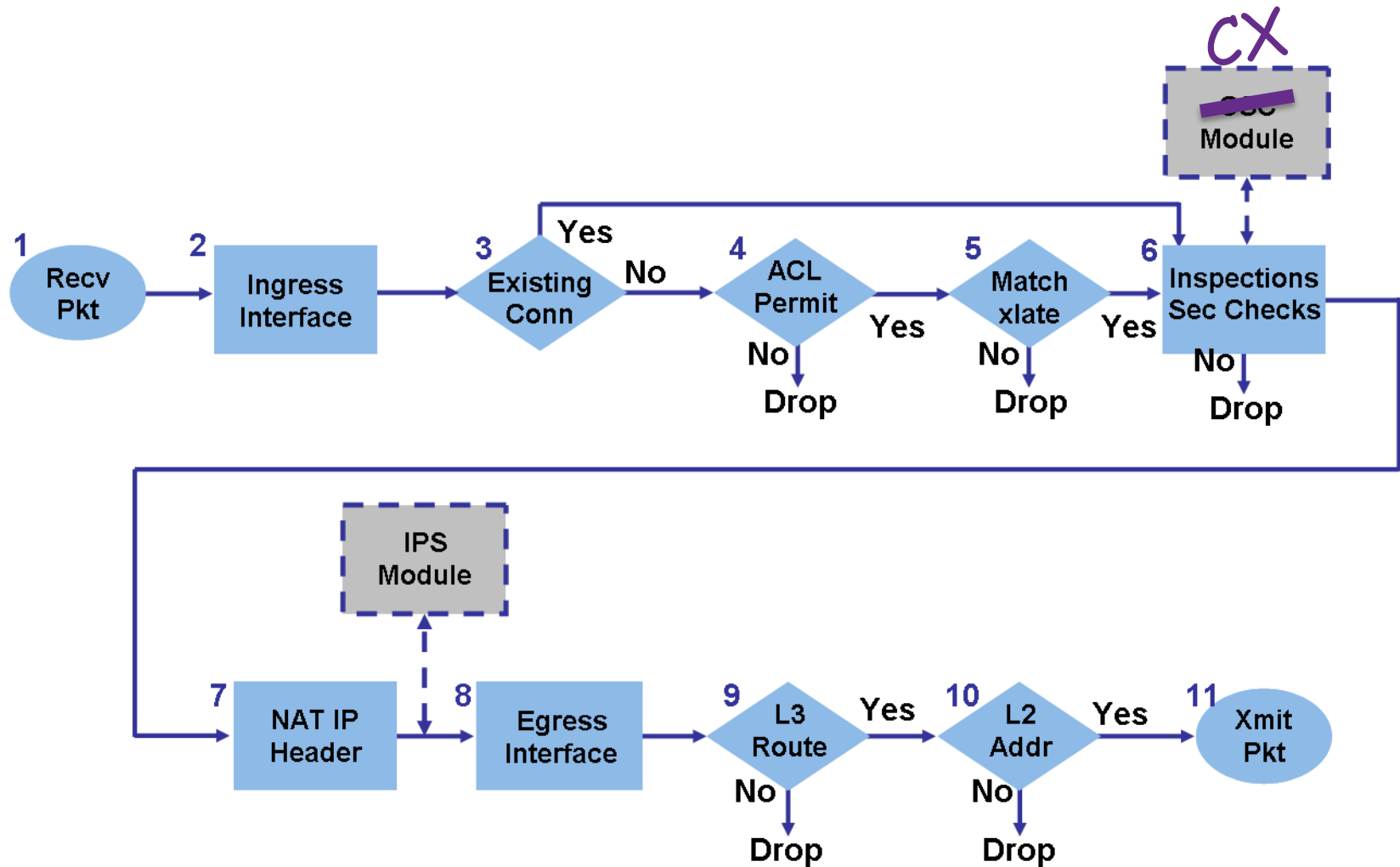
Model: Trial license applied to all models

Used Devices:1

PAK: Evaluation Web Security Essential License

Device name / Description	IP Address	Software version	Model	Commit version	Device group
ASA CX	localhost	9.1.1 (1)	ASA5515	0	default

Packet Processing Flow Diagram



Send traffic to CX SSP

Use MPF to direct traffic to the CX blade:

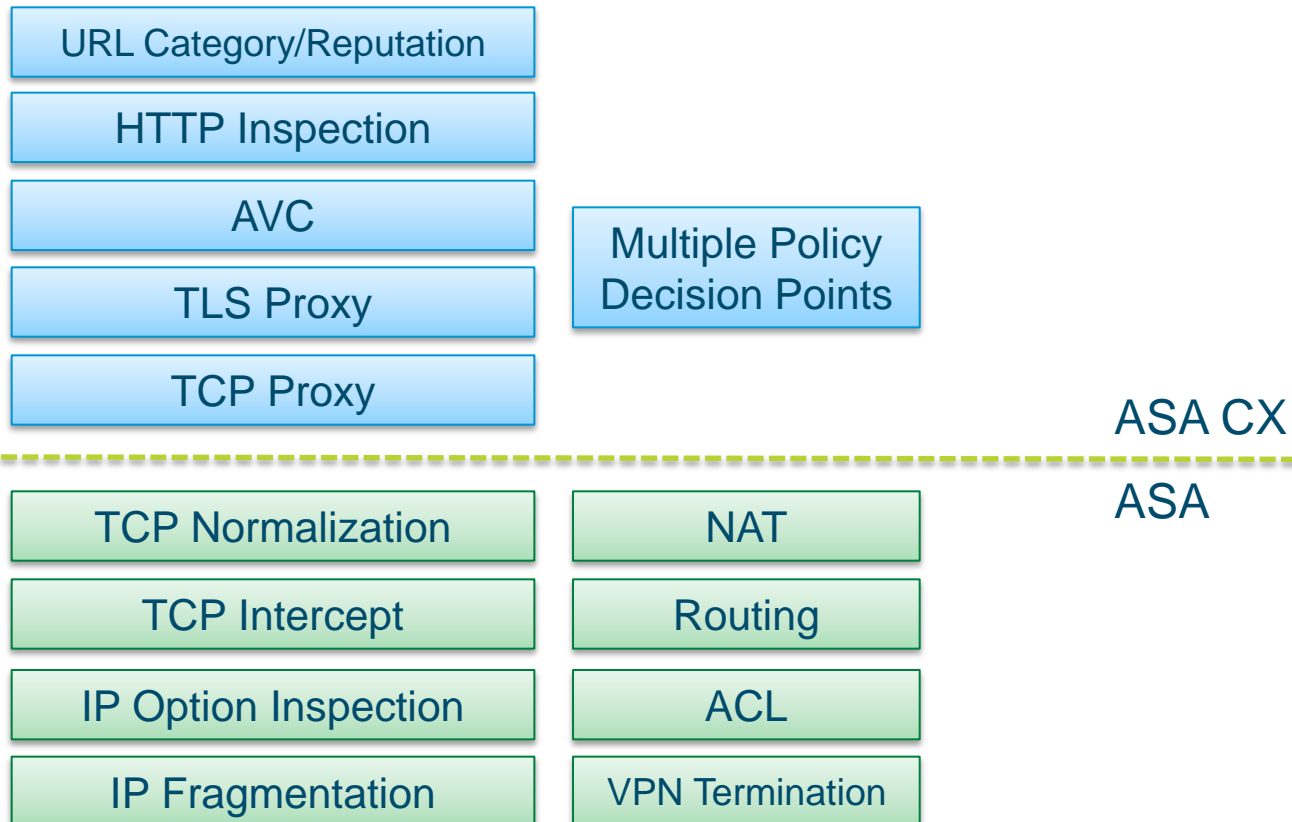
```
policy-map global_policy
  class class-default
    cxsc fail-open auth-proxy

service-policy global_policy global
```

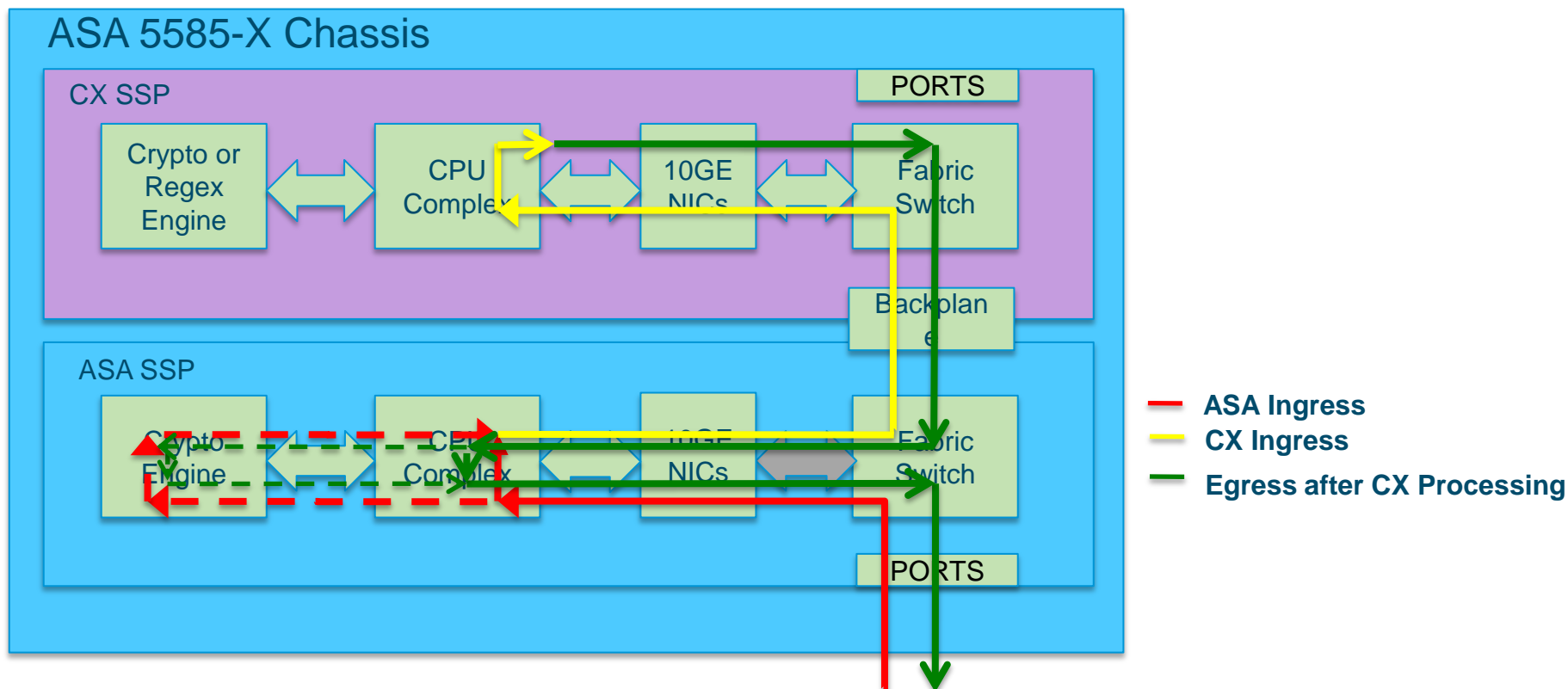
PRSM Multi-device applies this when connecting to CX:



Functionality Distribution



Customer Packet Flow across SSPs

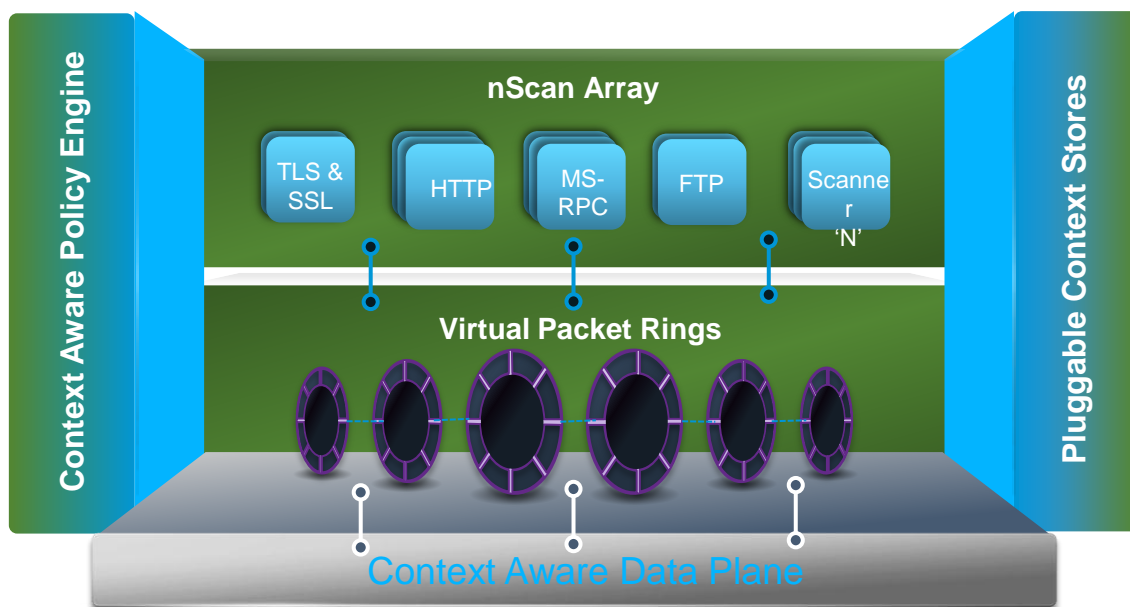


- **ASA SSP Configures and controls CX SSP customer ports**
- **ASA SSP processes all ingress/egress packets**
- **No packets are directly process by CX SSP except for management ports**
- **Packet rate doubles on ASA SSP when traffic is sent to CX SSP**

Cisco ASA CX

Next-Generation Protection. Proven Cisco technology.

- Context Aware
 - Most comprehensive controls – applications, users, and devices
 - Most widely deployed remote access
 - Business-class web security
- Threat Aware
 - Protection from zero-day threats
 - Analyzes global data from multiple threat vectors
 - Reputation analysis via human and machine intelligence



Robust stateful inspection *and* broadest context-aware controls

Policy types

Authentication

- How to identify user?



Decryption

- What to decrypt?



Access

- Allow or Deny?

Policy types - Screenshot




Access

Access

Used by device roles: **default**

Policy type: Access

Number of Policies: 1

Features enabled:   

Source	Destination	Application	Action/Conditions
1 ANY	ANY		Allow




Auth

Authentication

Used by device roles: **default**

Policy type: Authentication

Number of Policies: 1

Features enabled:   

Source	Destination	Action/Conditions
1 ANY	ANY	Use Identity When Available Realm: seclabs




Decryption

Decryption

Used by device roles: **default**

Policy type: Decryption

Number of Policies: 0

Features enabled:   

Source	Destination	Action/Conditions
There are no policies in this policy set		

Access

Allow or Deny the transaction
based on full context

Other possible actions:

- Create Event (on by default)
- Capture Packets (off by default)

Also applied to HTTP Traffic:

- File Filtering Profile
Apply added filtering based on MIME
type
- Reputation Profile
Apply added filtering based reputation
score of destination
(default profile drops -6.0 and below
and is not active)

The screenshot shows the 'Create Policy' configuration page in Cisco Connect. It includes fields for 'Policy Name', 'Enable Policy' (set to On), 'Eventing' (set to On), 'Policy Action' (set to Allow), and 'Capture packets' (set to Off). Below these are three object selection fields: 'Source' (Any), 'Destination' (Any), and 'Application / Service' (Any), each with a 'Create new object' link. A 'Profile' section contains 'File filtering' and 'Web reputation' dropdown menus, each with a 'Create new profile' link. At the bottom are 'Tags' and 'Ticket ID' input fields.

Create Policy

Policy Name *

Enable Policy ☒ On ☐ Off

Eventing ☒ On ☐ Off

Policy Action ☒ Allow ☐ Deny

Capture packets ☐ On ☒ Off

Source
[Create new object](#)

Destination
[Create new object](#)

Application / Service
[Create new object](#)

▼ Profile

File filtering
[Create new profile](#)

Web reputation
[Create new profile](#)

Tags

Ticket ID

Decryption

Decrypt TLS/SSL traffic
across any port

Self-signed (default)
certificate or customer
certificate/key

Based on FQDN, URL
Category, User/Group,
Device type,
IP address, or Port

FQDN and URL
Category are
determined using
server certificate

Create Policy

Policy Name *

Enable Policy ☒ On ☐

Source
[Create new object](#)
For URL objects used in decryption policies, URLs containing paths are ignored.

Destination
[Create new object](#)

Service
[Create new object](#)

Action ▼

Web reputation ▼
[Create new profile](#)

Tags

Ticket ID

Authentication Realm

Realm: Logical group of trusted Directory Servers (AD or LDAP)

Active Directory

- One Realm
- One Domain (joins the domain)
- AD Agent for passive authentication
- Kerberos, NTLM, or Basic for active authentication

LDAP

- Multiple Realms
- Basic authentication only

The screenshot shows the 'Create Policy' configuration page in Cisco Connect. It includes fields for 'Policy Name', 'Enable Policy' (a toggle switch set to 'On'), and three dropdown menus for 'Source', 'Destination', and 'Service', each with a 'Create new object' link below it. The 'Source' dropdown is set to 'Any'. Below these are fields for 'Realm' (set to 'budlabsec.com') and 'Action' (set to 'Get identity using AD agent'). A question 'Do you want to use active authentication if AD agent cannot identify user?' is followed by a 'Yes' toggle switch. At the bottom, the 'Authentication type' dropdown is open, showing options: 'Basic', 'NTLM', 'Kerberos', and 'Advanced'. The 'Exclude user agent' checkbox is also visible.

Create Policy

Policy Name *

Enable Policy ☒ On

Source Any
[Create new object](#)

Destination Any
[Create new object](#)

Service Any
[Create new object](#)

Realm budlabsec.com

Action Get identity using AD agent

Do you want to use active authentication if AD agent cannot identify user?
☒ Yes

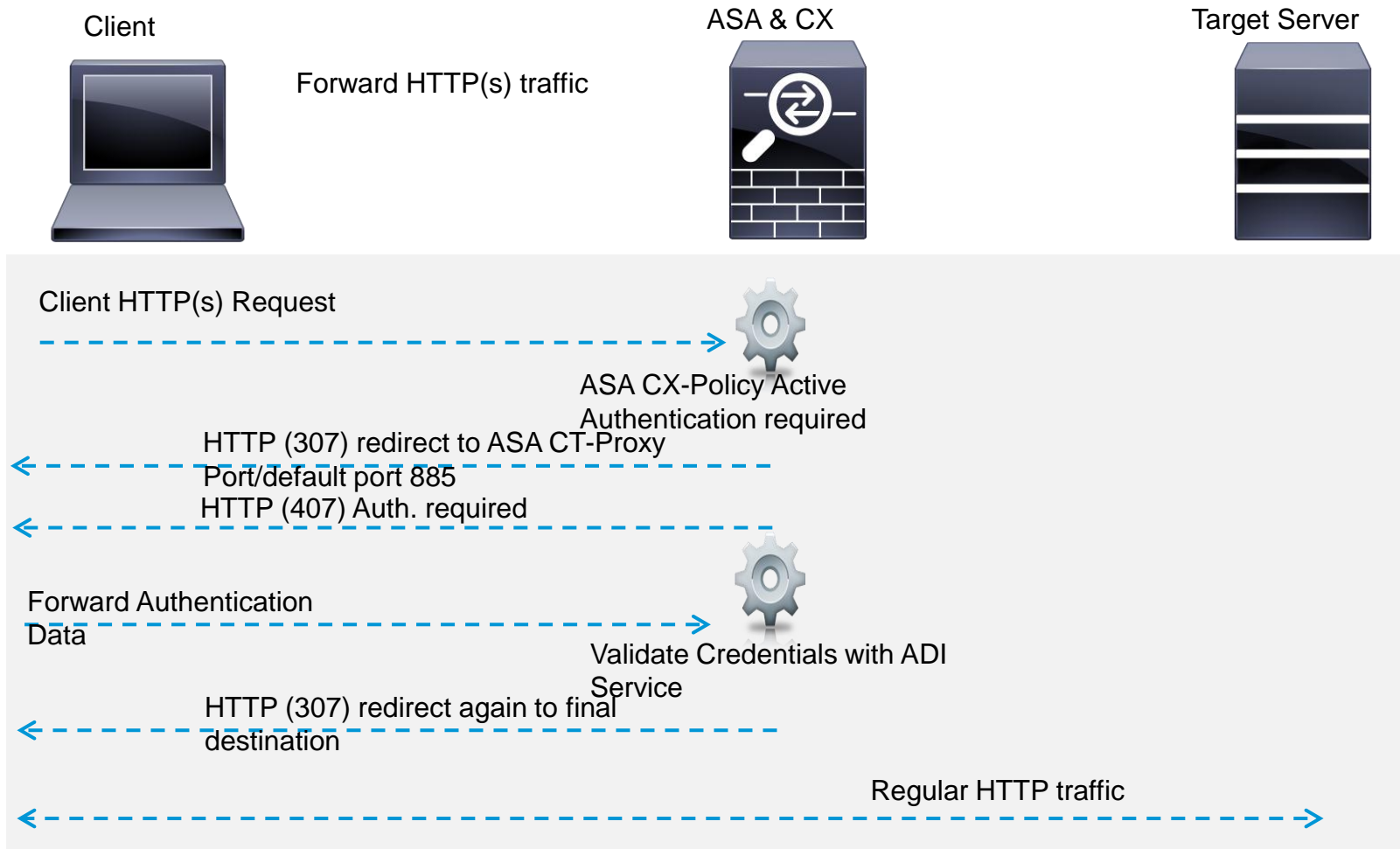
Authentication type Basic

Exclude user agent

Basic
NTLM
Kerberos
Advanced

Active or passive Authentication options

Example active authentication



Enable policy

On

Policy Action

Allow

Ticket ID

Enter Ticket ID

Tags

Enter keyword tags

▼ Source

Any

[Create new object](#)

▼ Destination

Any

[Create new object](#)

▼ Application

Any

[Create new object](#)

▼ Profile

File filtering action profile

Select one File filtering profile

[Create new profile](#)

Web reputation action profile

Select one Web reputation profile

[Create new profile](#)

▼ Policy properties

Eventing

On

Capture packets

Off

Save policy




Cancel

Policy Example 1

Facebook games blocking for engineers

Filter Enter filter criteria **Filter** 3 results

Access Policy set type: Access
Number of Policies: 4

Features enabled:   

Source	Destination	Action/Conditions
1 ANY	ANY	Game System
2 ANY	ANY	Webmail
3 engineers	ANY	Facebook Applications: Games
4 ANY	ANY	Conditional Allow

Any traffic flow that does not match one of the access policies is allowed without conditions.

Identity group

Selected from the system defined list

Action : Deny!

Deny

Conditional Allow
Profiles:
bad reputation

Delete policy Edit policy Duplicate policy Add above Move up Move down

Policy Example 2 - Objects

Block Unacceptable Sites

Edit URL object Help Close

Name* unacceptable sites Status
Committed

Object type URL object

Description Created
January 4, 2013 by admin

Tags TEST

Ticket ID Enter Ticket ID

Include

URL

Web category Games Adult Gambling Illegal Downloads Pornography

URL objects

Exclude

URL None

Web category None

URL objects None

URL strings may include wildcards (*). When a domain or host name is entered, all subdomains will be matched (e.g. "example.com" will match traffic to both "example.com" and "mail.example.com"). In situations where only the domain can be determined (e.g. decryption policies), URLs specifying a resource path are ignored.

* required fields

Save object Cancel

Selected
from the
predefine
d list

Policy Example 2 - Policy

Block Unacceptable Sites

Filter Filter 3 results

Access Policy set type: Access

Source=any

Destination = unacceptable sites

Empty means Protocol = any

Action = Deny

2	ANY	unacceptable sites		Deny
Delete policy Edit policy Duplicate policy Add above Move up Move down				
3	ANY	ANY	Webmail	Deny
4	engineers	ANY	Facebook Applications: Games	Deny
5	ANY	ANY		Conditional Allow Profiles: bad reputation

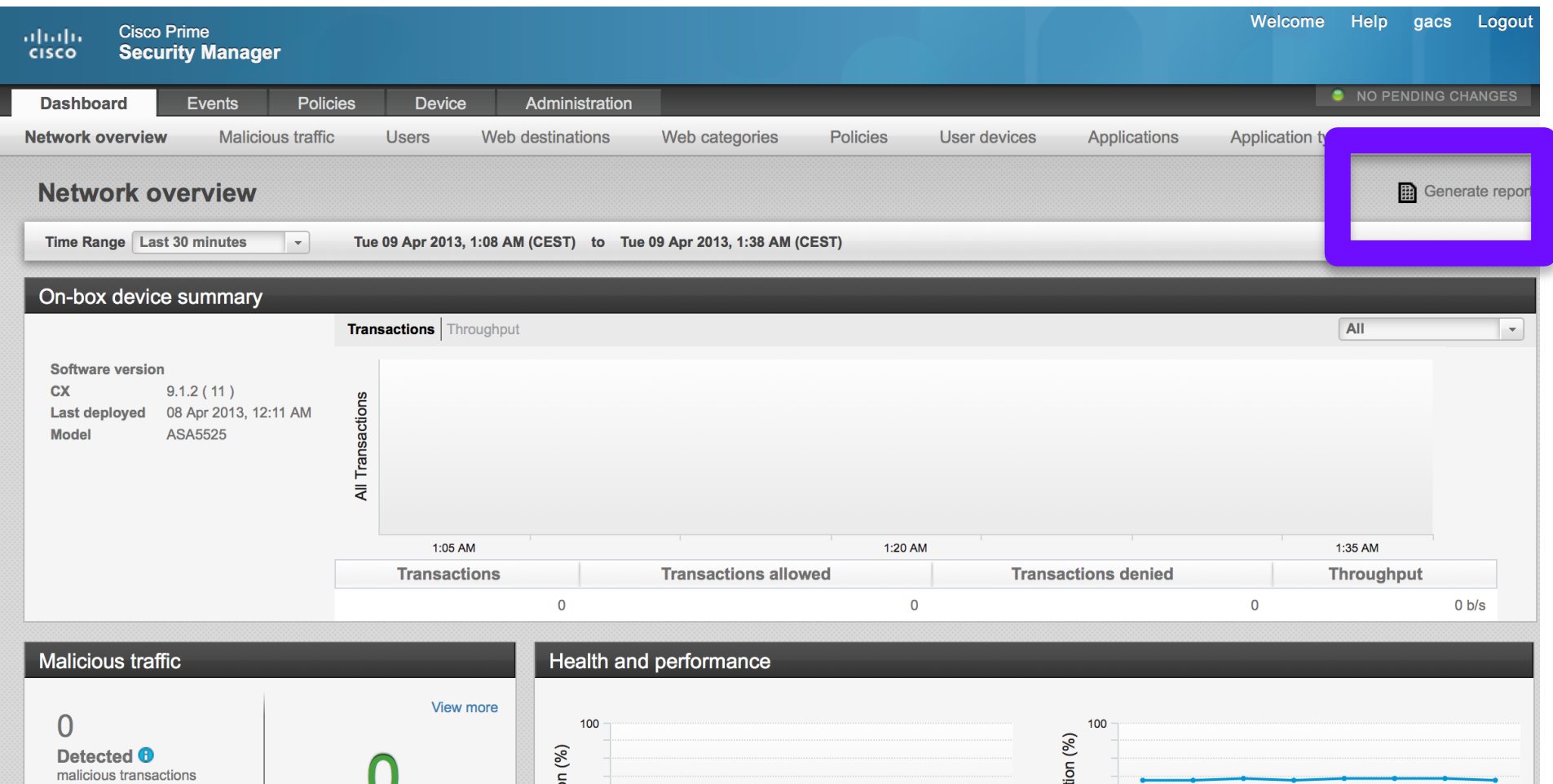
Any traffic flow that does not match one of the access policies is allowed without conditions.

Demo

Next Generation Firewall and PRSM



Next Generation Firewall – Reporting from 9.1(2)



Reports

Generate report

[Help](#)

Please choose options to generate a report. Your report will be generated in PDF format.

Report type

Application and web destination

Administrative

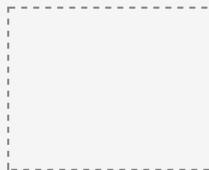
User and device

Application and web destination

Time range

Last 30 minutes

Report logo



Upload logo

100 pixels wide, 80 pixels tall, .jpg, .gif or .png,
8KB max








[Use default logo](#)

Cancel

Generate

Top 25 applications by transactions

08 Apr 2010, 01:46:00 PM (CEST) to 08 Apr 2013, 02:46:00 PM (CEST)

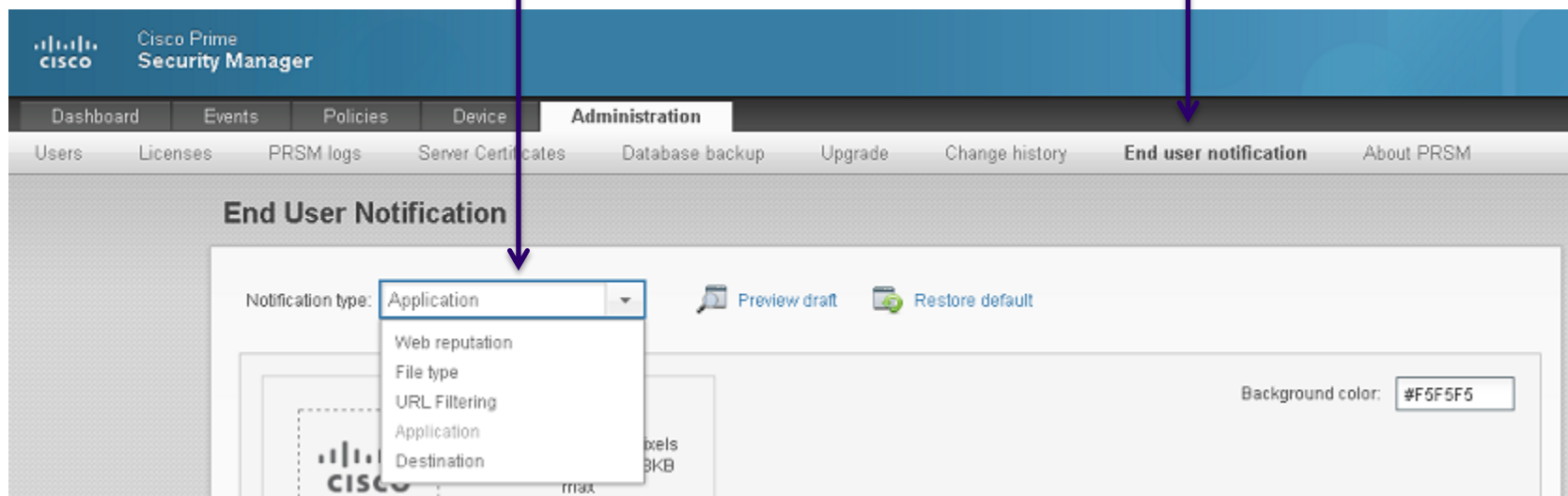
	Application	Transactions			Bytes			Top 5 by transactions				
		Total	Allowed	Denied	Total	Sent	Received	Users		Web destinations		
1	HyperText Transfer Protocol		1.0 K	1.0 K	19	11.0 MB	893.0 KB	10.0 MB	10.1.1.24 budlabsec.com\ldtest2	1.0 K 34	www.cisco.com index.hu ichef.bbc.co.uk static.bbc.co.uk www.static-cisco.com	210 184 181 136 59
2	Facebook General		475	475	0	4.0 MB	316.0 KB	4.0 MB	10.1.1.24	475	static.ak.fbcdn.net profile.ak.fbcdn.net www.facebook.com creative.ak.fbcdn.net pixel.facebook.com	135 124 104 30 16
3	Transport Layer Security Protocol		384	378	6	1.0 MB	556.0 KB	796.0 KB	10.1.1.24	384	www.cisco.com cisco.com	161 38
4	Generic Search Engine Traffic		264	264	0	804.0 KB	247.0 KB	556.0 KB	10.1.1.24	264	polling.bbc.co.uk newsrss.bbc.co.uk www.bbc.co.uk indapass.hu sa.bbc.co.uk	221 22 9 6 5
5	Facebook Messages and Chat		49	49	0	131.0 KB	84.0 KB	47.0 KB	10.1.1.24	49	www.facebook.com 2-act.channel.facebook.com 6-act.channel.facebook.com 4-act.channel.facebook.com 3-act.channel.facebook.com	37 4 3 2 1
6	Google Analytics		38	38	0	45.0 KB	31.0 KB	13.0 KB	10.1.1.24	38	www.google-analytics.com	38
7	Ads and Tracking		33	33	0	41.0 KB	18.0 KB	23.0 KB	10.1.1.24	33	ad.doubleclick.net b.scorecardresearch.com ad.yieldmanager.com fls.doubleclick.net pix04.revsci.net	16 7 3 3 2

Customizable End User Notification


Allows an eligible admin to define the end user notifications that are shown to clients whose web traffic is denied by the http inspector.

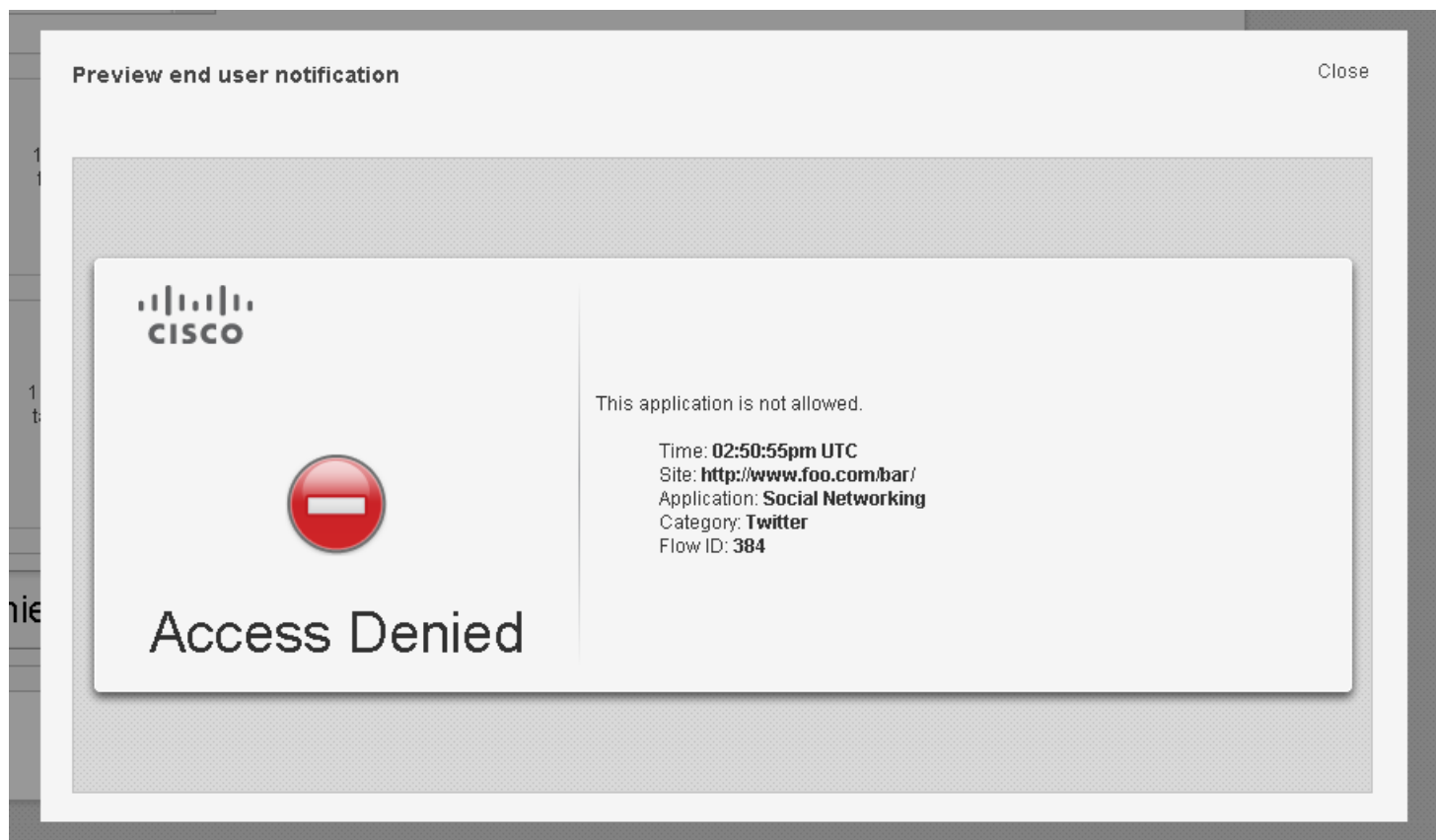
There are five notification types, each for a different category of deny reason, and each with a predefined default message.

To change an EUN, navigate to **Administration > End user notification**, then choose the notification type you wish to change.



Customizable EUN – Preview draft

The user may click  [Preview draft](#) to get a look at how the EUN will look when displayed to clients, with example values filled in for the template variables.



CX Monitor-mode Feature

Two new modes on ASA 9.1.2 (upcoming) for redirecting traffic to CX 9.1.2 service blade acting as a passive device and monitoring traffic:

ASA CXSC monitor-only redirection

ASA traffic-forward to CX

Restrictions for CX in monitor mode

No policy enforcement

Doesn't support active authentication

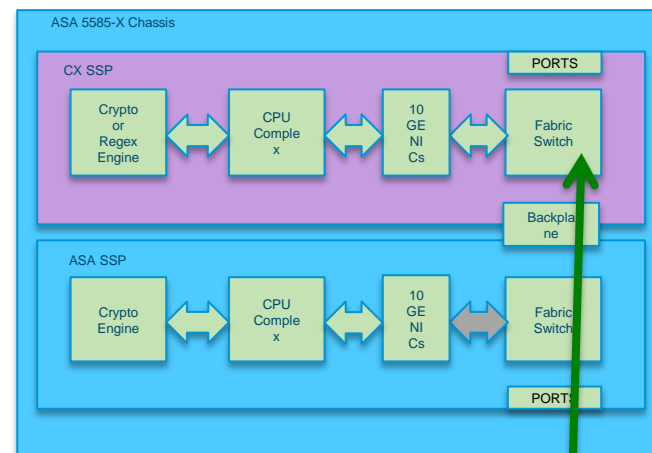
Doesn't support decryption

Some traffic that needs TCP proxying will not have associated events or reports.

Clients and servers are more than 1 hop away from ASA.

Monitor-mode only supported on SDM PRSM

ASA-CX in monitor-mode can't be imported by PRSM in MDM mode



Web Security Portfolio Basics



Firewall Integrated
(ASA CX)



Cloud
(Cloud Web Security)



Appliance, Physical & Virtual
(Web Security Appliance)

Web/URL Filtering	✓	✓	✓
Application Controls	Ports (all) Protocols (all)	Ports (80, 443) Protocols (HTTP(S))	Ports (21, 80, 443) Protocols (HTTP(S), FTP)
Malware Protection	Basic (reputation)	Advanced (reputation + content analysis)	Advanced (reputation + content analysis)
Remote User Security	VPN Backhaul	Direct to cloud	VPN Backhaul
Deployment	On the firewall	Cloud forward via ASA, ISR, WSA, AnyConnect	On Premise Redirect
Policy & Reporting	On Premise	In the Cloud	On Premise
Licensing / Subscription	Based on ASA model 1Y / 3Y / 5Y	Based on user count 1Y / 3Y / 5Y	Based on user count 1Y / 3Y / 5Y

Web Security Positioning



Solution :

Firewall Integrated (ASA CX)

Cloud (Cloud Web Security)

Appliance, Physical & Virtual (Web Security Appliance)

When The Requirements Are...

- Next gen firewall capabilities
- Application control for port-hopping and evasive applications like Skype
- URL filtering

- Cloud based service
- Web security for small branches with direct internet access
- Web security for roaming or mobile users without backhauling over VPN
- Anti-Virus/Anti-Malware scanning

- On-premise proxy
- Anti-Virus/Anti-Malware scanning
- DLP for Web
- SOCKS Proxy
- FTP Proxy
- Caching
- On-premise logs
- Video/Audio bandwidth throttling

- Web/URL Filtering
- Web Application Controls
- Reputation filtering for malicious sites & IPs

Agenda

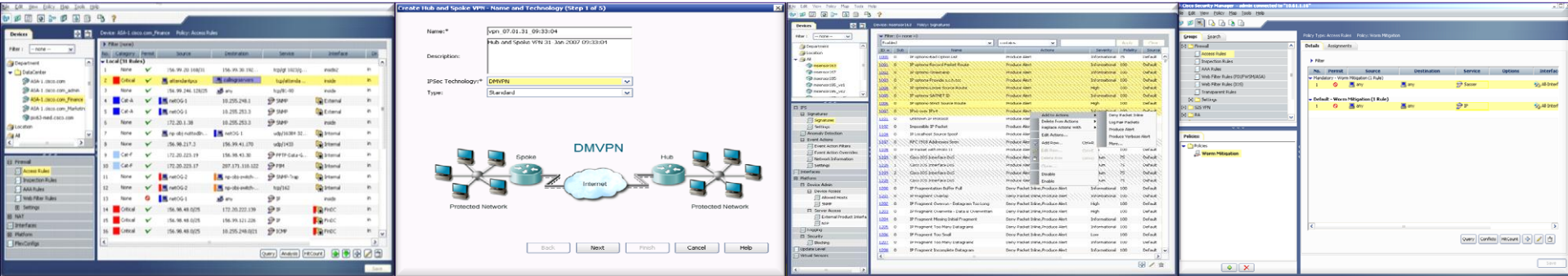
Next Generation Firewall and Prime Security Manager

Cisco Security Manager 4.4



Cisco Security Manager

Integrated Security Solution Management



Firewall

VPN

IPS

Operation

- | | | | |
|---|---|--|--|
| <ul style="list-style-type: none"> • Support for PIX, ASA, FWSM, ASASM, IOS/ISR/ASR • IDFW & AD integration, shared objects & policy grouping, inheritance • Powerful analysis tools: conflict detection, rule combiner, hit counts... • Botnet Traffic Filter & ScanSafe integration | <ul style="list-style-type: none"> • Support for PIX, ASA, VPNM, VPNSPA, IOS/ISR/ASR Routers • Support for wide array of VPN technologies such as: GRE IPsec, DMVPN, GETVPN, Easy VPN, and SSL VPN • VPN Wizard for 5-Step Point-and-Click VPN Creation | <ul style="list-style-type: none"> • Support for IPS Sensors/SSP Modules and IOS IPS • Automatic policy based IPS Sensor software and signature updates • Signature Update Wizard allowing easy review/editing prior to deployment • Global Correlation Support & CSIO integration | <ul style="list-style-type: none"> • Unified Security Management for > 250 security platforms • Robust multi-users support with leading RBAC & WorkFlow for change management & control • Efficiently manage up to 500 devices per server • Multiple views for task optimization • Events, Reports, HPM & |
|---|---|--|--|

Efficient Policy Provisioning & Enforcement Tools

The image displays four overlapping screenshots of the Cisco Security Manager (CSM) Configuration Manager interface, each highlighting a different view for policy provisioning and enforcement.

- Device View:** Shows the configuration for a specific device, 'la-asa'. It lists assigned policies, including 'Global FW Policy' and 'ASA Policy Bundle'. A table of rules is visible, with columns for No., Permit, Source, User, Destination, and Service.
- Map View:** Displays a network topology diagram with nodes representing devices and lines representing connections. A context menu is open, showing options like 'Edit Firewall Policies', 'Edit Firewall Settings', 'Device Properties...', 'Clone Device...', 'Copy Policies Between Devices...', and 'Share Device Policies...'.
- Policy View:** Shows the configuration for a specific policy, 'Global FW Policy'. It displays a table of rules with columns for No., Permit, Source, User, Destination, and Service. The 'Permit' column shows status indicators (green checkmarks and red X's).
- Policy Bundle View:** Shows the configuration for a policy bundle, 'ASA Policy Bundle'. It displays a table of rules with columns for No., Permit, Source, User, Destination, and Service. The 'Permit' column shows status indicators (green checkmarks and red X's).

Each screenshot includes a menu bar with options like File, Edit, View, Policy, Map, Manage, Tools, Launch, and Help. The interface also features a left-hand navigation pane with categories like Devices, Policies, Policy Types, and Policy Bundles.

Proactive Monitoring & Maintenance Tools

The image displays four overlapping screenshots of Cisco Security Manager tools, each with a yellow label overlay:

- Event Manager:** Shows the 'Event Monitoring' interface with a list of events. The 'View Settings' table includes columns for No., Receive Time, Severity, Event, and Event Name. The table contains 8 rows of event data.
- Image Manager:** Shows the 'Images' interface with a table of installed images. The table includes columns for Image, Type, Version, Location, Size, Description, and Comment. It lists various Cisco Secure Desktop and AnyConnect images.
- Report Manager:** Shows the 'Report List' interface with a tree view of reports. A 'Top Signatures - Settings' dialog is open, showing a duration of Feb 23, 2012 12:00:00 PM to Feb 23, 2012 1:00:00 PM. A pie chart is visible in the background.
- Health & Performance Manager:** Shows the 'Monitoring' interface with a 'Summary' tab. It displays a table of device health and performance metrics, including CPU usage and memory usage. Below the table are two line graphs for CPU and Memory usage over time.

Please see it : <http://www.ciscocsm.autovod.com>

Cisco Security



[Main](#) [Contents](#) [Presentation](#) [Transcript](#) [Search](#) [Feedback](#)

POWERED BY AUTOVOD

Cisco Security Manager - Enterprise Deployment

Contents

Select a topic from the main table of contents. Review the brief description or click on the expand/collapse icon to reveal greater detail about the content contained within. The total running time is posted for each Module identifying the time commitment to complete the specific content of interest.

Title	Running Time	Progress
Role Based Access Control	6 min	21%
Multi-User Management	5 min	0%
Configuration Versioning and Rollback	5 min	3%
Change Workflow	10 min	0%
Alert Notifications	5 min	75%
Scheduled Deployment	4 min	0%
Backup/Restore of CSM Data	4 min	0%
CSM API	9 min	5%
IPS Signatures and Event Actions	9 min	0%
IPS Operations	9 min	0%
IPS Reports	6 min	0%
Sharing a Local Policy	6 min	0%
Object Overrides	8 min	0%
Interface Role	4 min	0%
Inheritance	3 min	0%
Policy Bundles	5 min	0%
Cisco Security Manager	10 min	0%

ASA 9.x Cluster Management

Clustering feature only supported in ASA 9.0(1)+ only for ASA 5580 and 5585 platforms

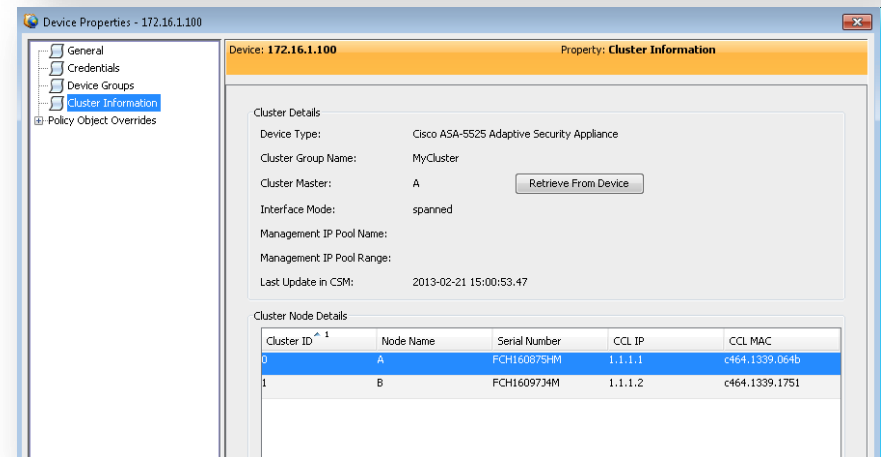
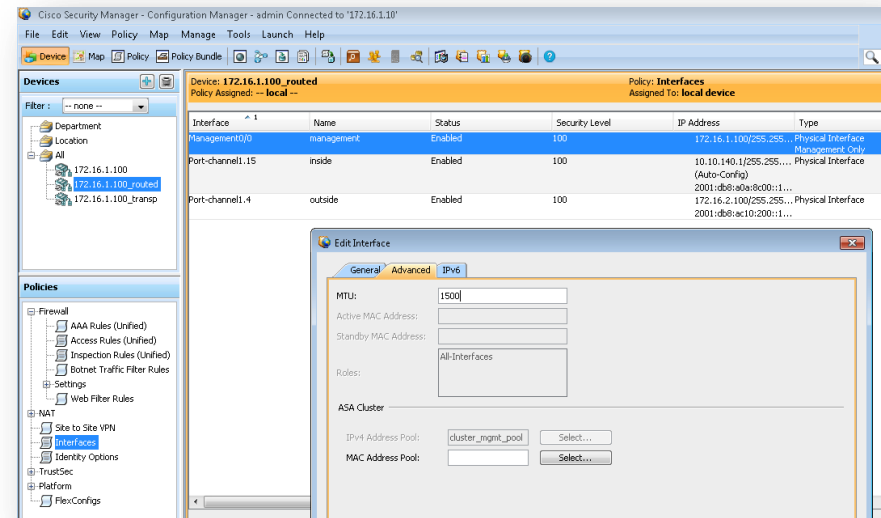
Supported types: L2 (spanned) & L3 clusters (Individual)

CSM does NOT configure or manage cluster bootstrap settings. Use ASDM or CLI to activate clustering before importing it to CSM

CSM discovers and manages a cluster of devices by communicating with cluster's Management IP address (master)

In Multi-Context Load Balancing Mode, import cluster's Admin context to CSM using Management IP address, cluster members info will be imported via Master

Details of discovered devices in a cluster are in the Device Properties > Cluster Information



HPM: Firewall Cluster Monitoring & Alerts

Firewall cluster can have up to 8 nodes. HPM monitors cluster master, nodes status (up/down) and throughput of cluster

All cluster members are monitored as devices in cluster's tree

New alerts, 'Node Down' and 'Master Changed' are added.

The top screenshot shows the 'Monitoring' window with a table of devices and their status. The table has columns for Device Name, Receive Time, Health Status, Connection Status, CPU(%), Memory(%), and Version. The data is as follows:

Device Name	Receive Time	Health Status	Connection Status	CPU(%)	Memory(%)	Version
172.16.1.100	Thu Mar 14 11:59:09 PDT 2013	Normal	Connected	0%	Not Available	9.1(1)
172.16.1.100_routed	Thu Mar 14 12:01:59 PDT 2013	Normal	Up	0%	Not Applicable	0.9(1.1)
A	Thu Mar 14 12:01:59 PDT 2013	Normal	Up	0%	Not Applicable	0.9(1.1)
B	Thu Mar 14 12:01:59 PDT 2013	Normal	Up	0%	Not Applicable	0.9(1.1)
172.16.1.100_transp	Thu Mar 14 12:02:04 PDT 2013	Normal	Connected	0%	Not Applicable	9.1(1)
A	Thu Mar 14 12:02:04 PDT 2013	Normal	Up	0%	Not Applicable	0.9(1.1)
B	Thu Mar 14 12:02:04 PDT 2013	Normal	Up	0%	Not Applicable	0.9(1.1)

The bottom screenshot shows the 'Alerts configuration' window. It has tabs for IPS, FW, and VPN. The 'Notifications' section has an 'Email Addresses' field. The 'Settings' section has 'Expand All' and 'Collapse All' buttons. The 'Failover Peer Status' section has a checkbox for 'Failover Peer Status'. The 'Interface Status' section has a checkbox for 'Interface Status' and a dropdown for 'Consider for Device Health'. The 'Master Changed' section has a checkbox for 'Master Changed'. The 'Cluster Node Status' section has a checkbox for 'Cluster Node Status' and a dropdown for 'Consider for Device Health'. The 'CPU Usage' section has a checkbox for 'CPU Usage' and a dropdown for 'Consider for Device Health'. The 'Memory Usage' section has a checkbox for 'Memory Usage' and a dropdown for 'Consider for Device Health'. The 'Priority Devices' section has a dropdown for 'Occurrence' and a text field for '1 times'. The 'Standard Devices' section has a dropdown for 'Occurrence' and a text field for '1 times'. The 'Help' button is at the bottom left. The 'Save', 'Revert', and 'Cancel' buttons are at the bottom right.

Unified Access Rules Management

Supports Unified Access Lists containing both IPv4 & IPv6 addresses and objects.

CSM introduced three new policies

- Access Rules (Unified)

- AAA Rules (Unified)

- Inspection Rules (Unified)

Previous Access Rules, AAA Rules and Inspection Rules are still usable on ASA 9.x device

IPv6 Access Rules are not applicable for ASA 9.0 devices, use Unified Rules

User can convert previous policy on ASA 8.x (Access Rules, AAA Rules and Inspection Rules) to Unified Rules

The top screenshot shows the 'Policies' tree in the ASA configuration interface. The 'Access Rules (Unified)' policy is highlighted. A context menu is open over it, showing options like 'Clone Policy...', 'Convert to Access Rules (Unified)', 'Rename Policy...', 'Add to Policy Bundle...', 'Inherit Access Rules...', 'New Access Rules Policy...', and 'Delete Policy...'. The 'Convert to Access Rules (Unified)' option is selected.

The bottom screenshot shows the details of the 'Access Rules (Unified)' policy assigned to 'Demo Access Rules'. The table below lists the rules:

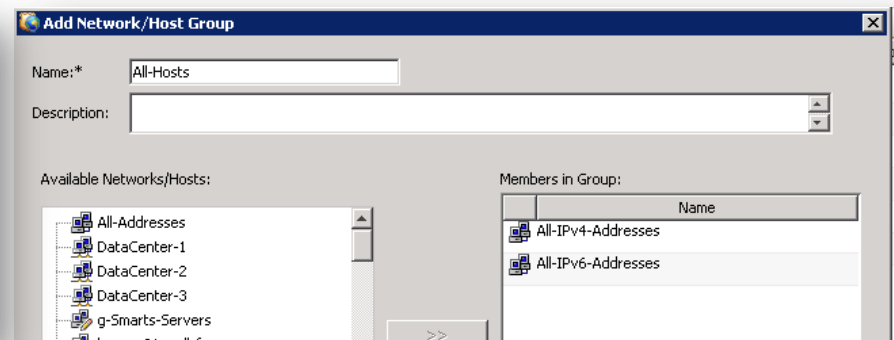
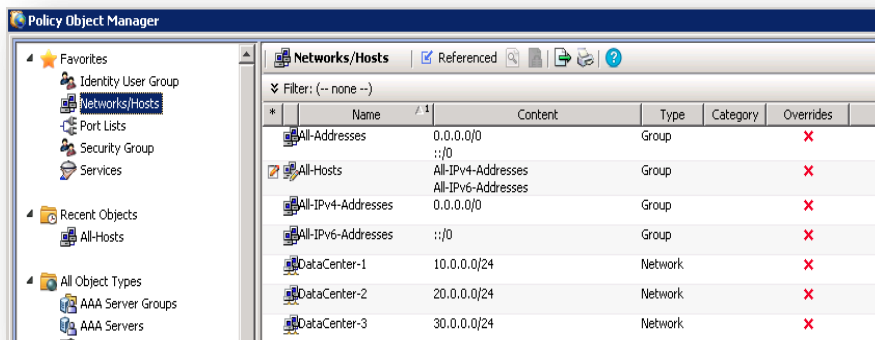
No.	Permit	Network	Security Sources	User	Destinations	Service	HitCount	
Demo Access Rules - Mandatory (9 Rules)								
1	✓	All-IPv4-Addresses	ISE-Group1	-- no user --	All-Addresses	-- no tags --	ICMP	0
2	✓	All-IPv6-Addresses	ISE-Group1	-- no user --	All-Addresses	-- no tags --	ICMP6	0
3	✓	All-Addresses	ISE-Group2	-- no user --	DataCenter-1	-- no tags --	HTTPS	0
4	✓	All-Addresses	ISE-Group3	-- no user --	DataCenter-2	-- no tags --	HTTP	0
5	✓	All-Addresses	ISE-Group1	-- no user --	DataCenter-3	-- no tags --	HTTPS	0
6	✓	All-Addresses	-- no tags --	AD-Group1	DataCenter-1	-- no tags --	HTTP	0
7	✓	All-Addresses	-- no tags --	AD-Group2	DataCenter-2	-- no tags --	HTTPS	0
8	✓	All-Addresses	-- no tags --	AD-Group3	DataCenter-3	-- no tags --	HTTP	0
9	✓	All-Addresses	ISE-Group1	-- no user --	DataCenter-1	-- no tags --	tcp/80	0
			ISE-Group2		DataCenter-2		ICMP	
			ISE-Group3		DataCenter-3		ICMP6	
Demo Access Rules - Default (Empty)								

At the bottom, there is a checkbox for 'Enable conflict detection' and a 'Generate Report' button. A note at the bottom states: 'ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules. Use Real IP addresses.'

New Unified Network Objects

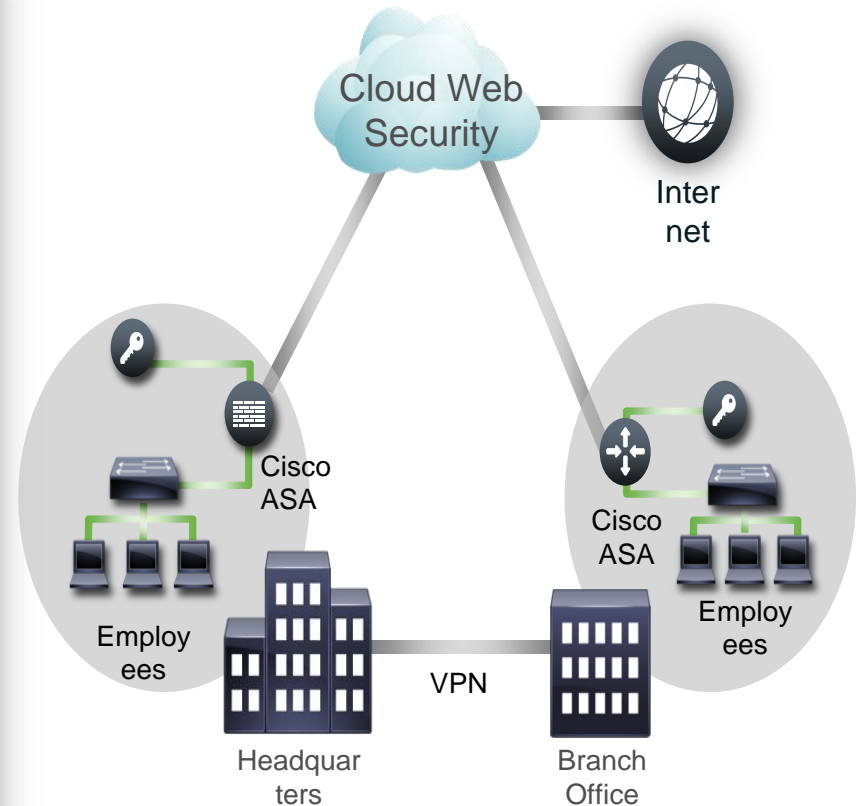
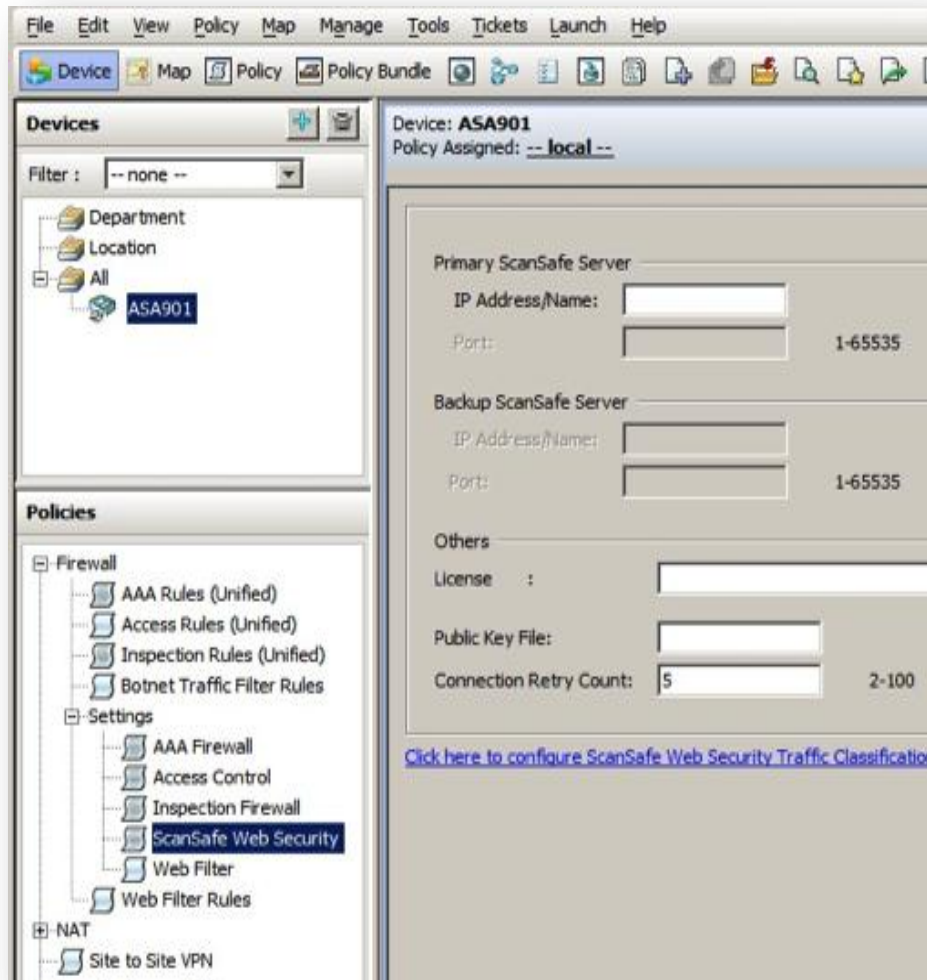
Supports both IPv4 & IPv6 Network objects as common type

The new network object group allows mix of both IPv4 and IPv6 addresses/objects



ScanSafe Web Security

Supports ScanSafe Web Security settings for single mode or multi-contexts system mode

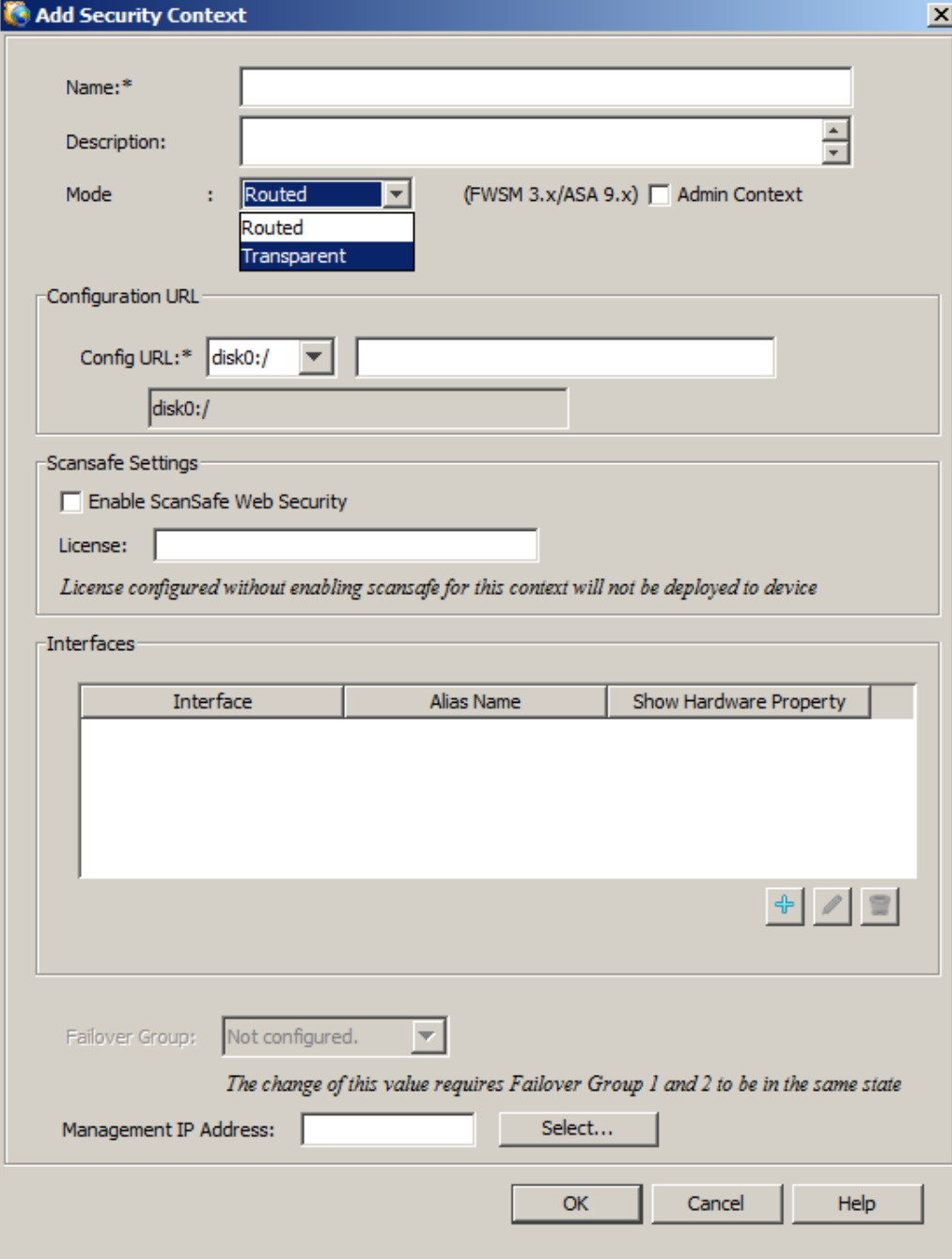


ASA Mixed Mode Support

ASA 9.x supports virtual contexts in mixed firewall modes (routed or transparent)

CSM also supports correct feature sets on individual virtual context based on its firewall mode.

Mixed mode support at par with FWSM/ASASM



The image shows a screenshot of the "Add Security Context" dialog box in a network management application. The dialog is titled "Add Security Context" and contains several sections for configuring a new security context.

Name: A text field for entering the context name.

Description: A text field for entering a description.

Mode: A dropdown menu currently set to "Routed". Below it, a list shows "Routed" and "Transparent" as options. To the right, text indicates "(FWSM 3.x/ASA 9.x)" and a checkbox for "Admin Context".

Configuration URL: A section containing a "Config URL: *" field with a dropdown set to "disk0:/". Below this is a text field containing "disk0:/".

Scansafe Settings: A section with a checkbox for "Enable ScanSafe Web Security". Below it is a "License:" text field. A note states: "License configured without enabling scansafe for this context will not be deployed to device".

Interfaces: A table with three columns: "Interface", "Alias Name", and "Show Hardware Property". The table is currently empty. Below the table are three icons: a plus sign (+), a pencil (edit), and a trash can (delete).

Failover Group: A dropdown menu currently set to "Not configured.". A note below it states: "The change of this value requires Failover Group 1 and 2 to be in the same state".

Management IP Address: A text field followed by a "Select..." button.

Buttons: At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

S2S VPN Policy Management Updates

VPN in Multi-context mode

Supports S2S VPN in multi-context running routed mode

Existing S-2-S VPN supports for single context device in CSM are identical for multi-context devices

ASA 9.x doesn't support RAVPN in multi-context, RAVPN is disabled in CSM for multi-context devices

VPN in Cluster mode

CSM supports S2S configuration on devices which are in cluster

When an ASA device in cluster is added in CSM, failover will be disabled

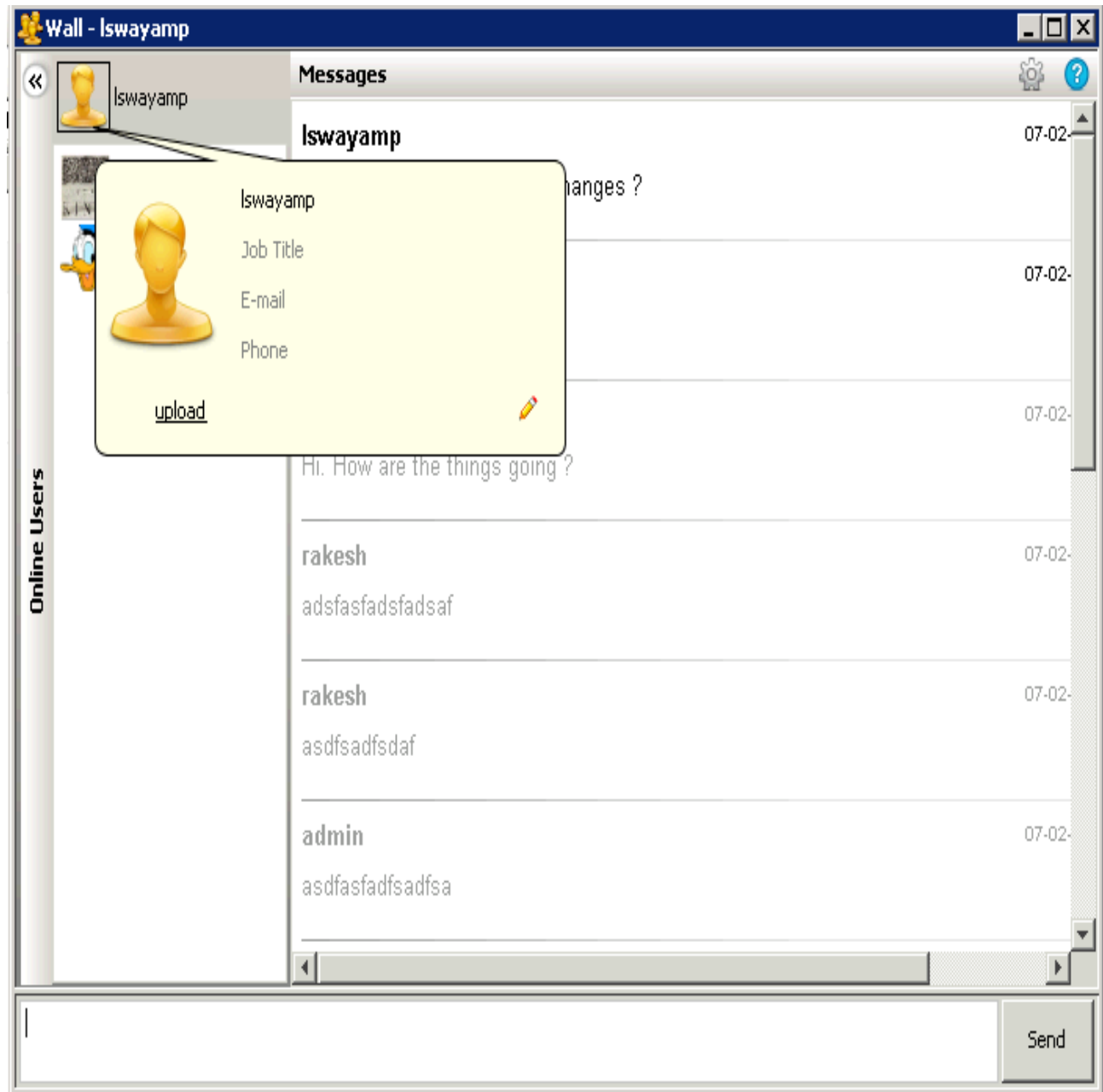
All RAVPN (SSL and IPsec) is disabled in CSM for devices in cluster mode

VPN Support in ASA-SM device

CSM supports S2S as well as RAVPN on ASA-SM

The support is at par with the VPN support on 558x platform

Wall UI



Device Status View – Alerts

The screenshot displays the Cisco Security Manager - Configuration Manager interface. The top menu bar includes File, Edit, View, Policy, Map, Manage, Tools, Tickets, Launch, and Help. The main window is divided into several sections:

- Devices:** A tree view on the left shows a hierarchy of Department, Location, and All. Under 'All', there are four devices: IPS Device 01, ASA Device 9.1, ASA Device 8.4, and ASA Device 9.0.
- Health and Performance Monitor:** A summary box showing Critical: 3, Warning: 0, and Normal: 1.
- Deployment Manager:** A summary box showing Fail: 0, Pending: 1, and Pass: 4.
- Device State:** A summary box showing Critical: 0, Warning: 1, and Normal: 3.

The main table displays a list of devices with columns: Display Name, Managed, Monitored, Alerts, Connection, State, Deployment, Additional Information, and Running OS Versi. The table is filtered by 'Filter: (-- none --)'. A tooltip is shown over the 'Alerts' column for 'ASA Device 8.4', indicating two critical alerts: 'License Expiration is Critical' and 'Device Health Critical'.

Shows summary of alerts on specified device

Display Name	Managed	Monitored	Alerts	Connection	State	Deployment	Additional Information	Running OS Versi
IPS Device 01	+	+	+	+	+	+		7.0(8p10)E45615.0
ASA Device 9.1	+	+	+	+	+	+		9.1(1)
ASA Device 8.4	+	+	+	+	+	+		8.4(5)
ASA Device 9.0	+	+	+	+	+	+		9.0(1)242

TrustSec Settings

two new policies for configuring TrustSec

:

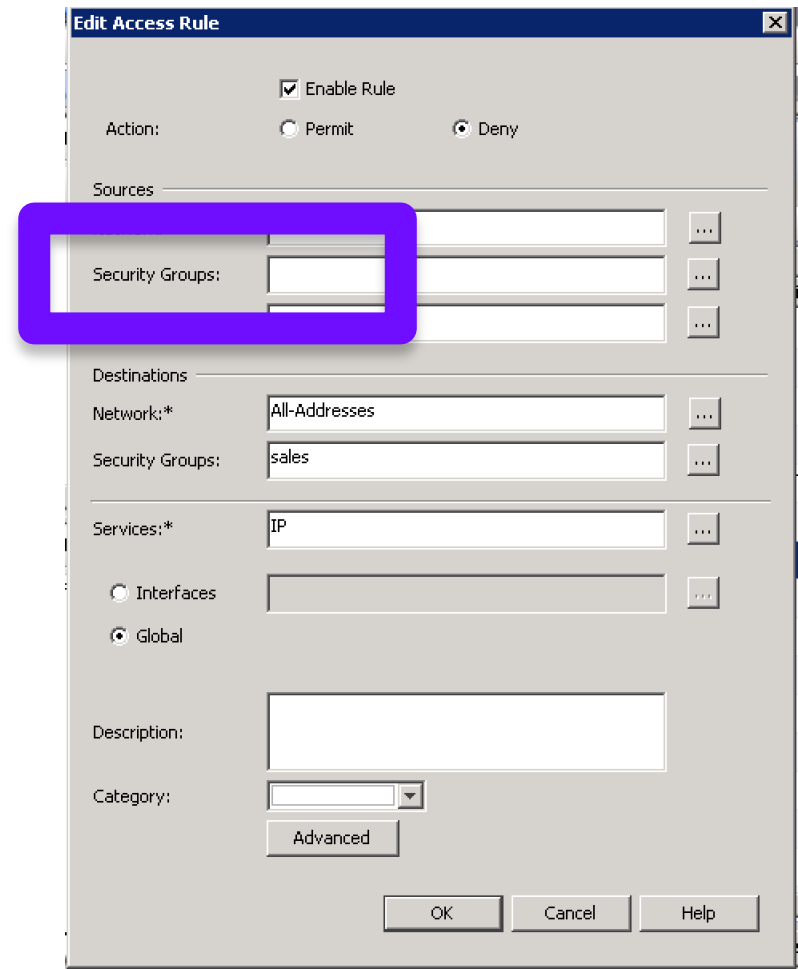
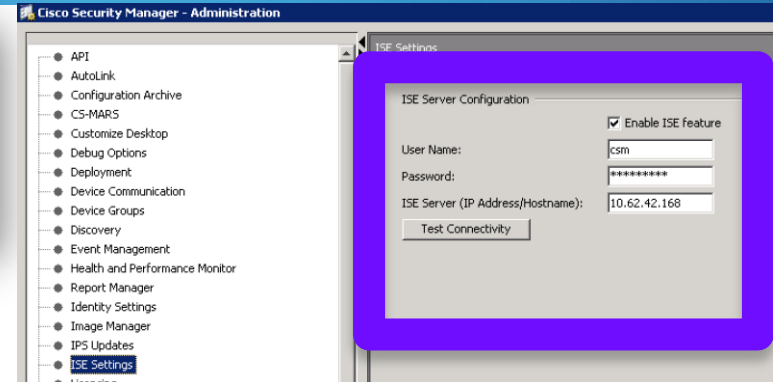
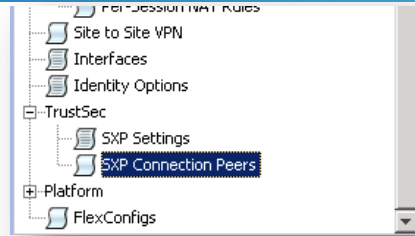
1. SXP Settings
2. SXP Connection Peers

only on ASA 9.0 and above

Settings : timers, enabling the SXP and configuring the server group which is used to communicate with the ISE (Identity Service Engine)

In admin settings CSM also maintains username, password, IP address of the ISE server that it can communicate with.

CSM communicates with ISE to fetch the names/tags for usage in unified firewall rules and security group policy objects



Agenda

Next Generation Firewall and Prime Security Manager

Cisco Security Manager 4.4



Thank you.



Segue Slide

