



Security Tech Update November 2013

Brian Hansen
Systems Engineer
Cisco Danmark

Christian Heinel
Systems Engineer
Cisco Danmark

Christian Bermann
Systems Engineer
Cisco Danmark

Agenda

- Introduction / The New Security Model

- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update

Gennemgang
Gennemgang

- Q & A

Alle

The background of the slide is a night-time photograph of a city skyline, likely San Francisco, with the Golden Gate Bridge visible. Overlaid on this image is a complex digital network diagram. It features numerous blue circular nodes, some of which are connected by thin white lines. There are also green square nodes scattered throughout. A large, faint white circle is centered in the upper half of the image. In the lower-left quadrant, there is a stylized grey logo consisting of two overlapping arrow shapes pointing in opposite directions.

Securing the Network and Data Center

NOW AND INTO THE FUTURE

- Christian Heinel
- Country Lead, Security
- Cisco



Cisco Completes Acquisition of Sourcefire



Who is Sourcefire?



- Founded in 2001
- Security from Cloud to Core
 - Market leader in (NG)IPS
 - New entrant to NGFW space with strong offering
 - Groundbreaking Advanced Malware Protection solution
- Innovative – 52+ patents issued or pending
 - Pioneer in IPS, context-driven security, advanced malware
- World-class research capability
- Owner of major Open Source security projects
 - Snort, ClamAV, Razorback

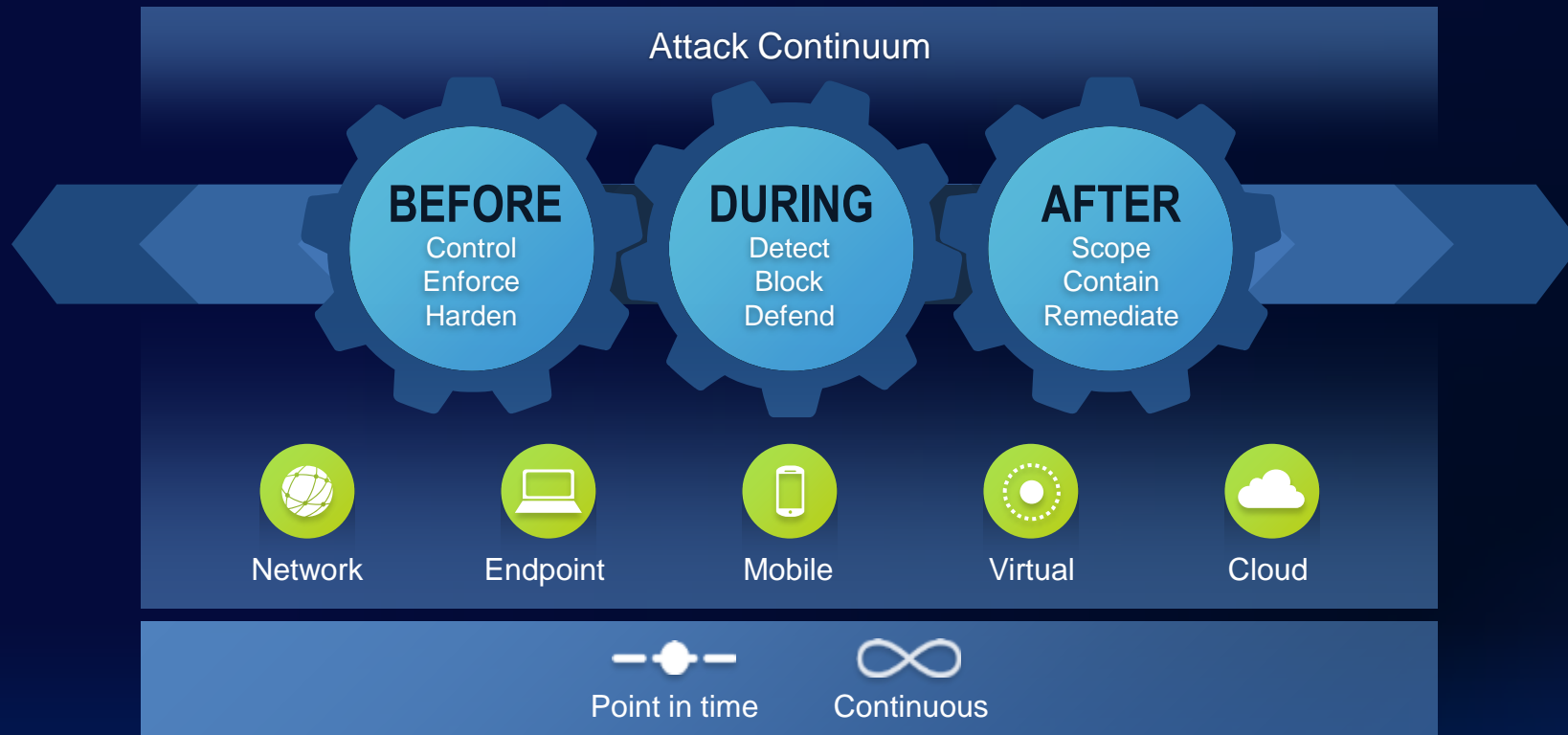


Our Security Perspective

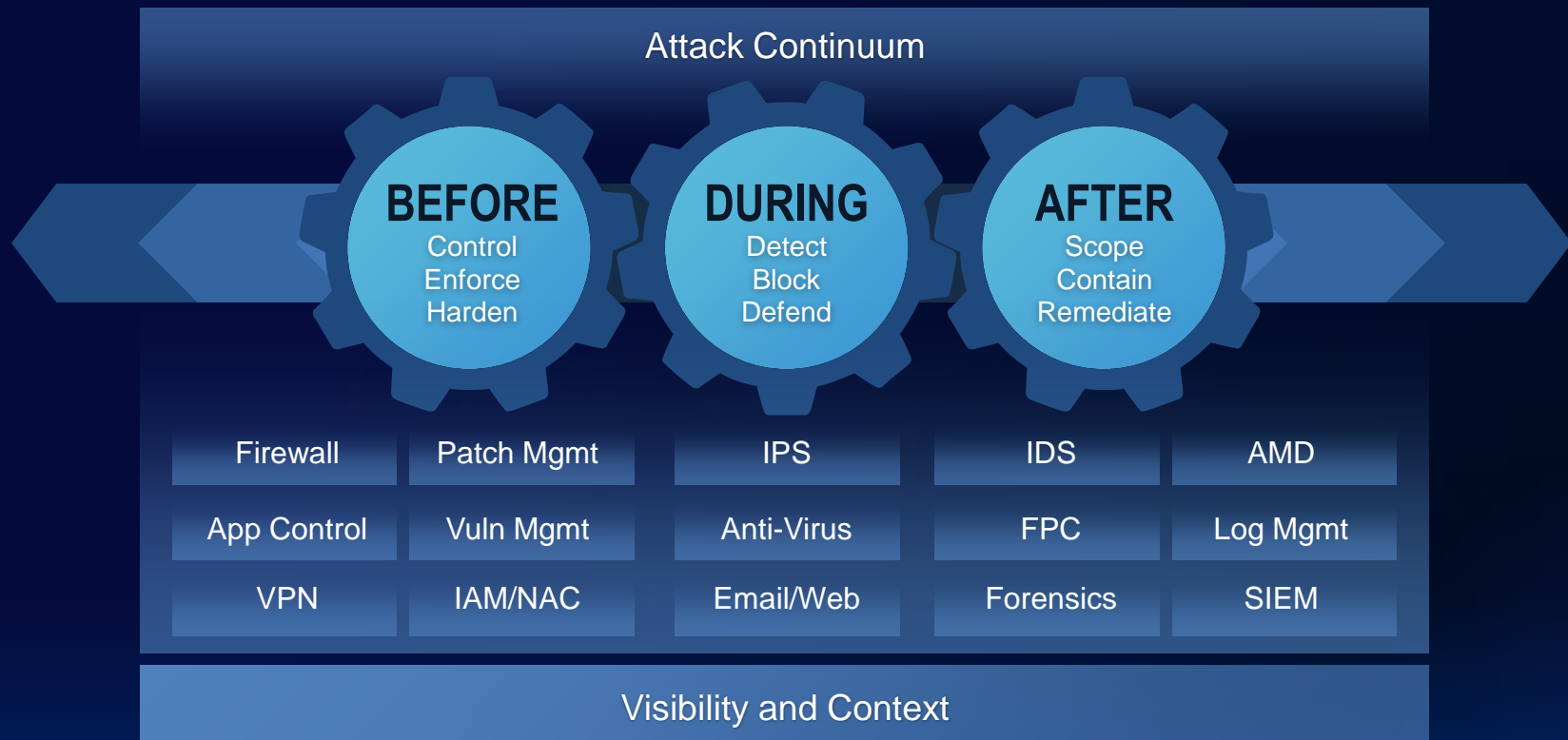
The Problem is THREATS

If you knew you were going
to be compromised, would
you do security differently?

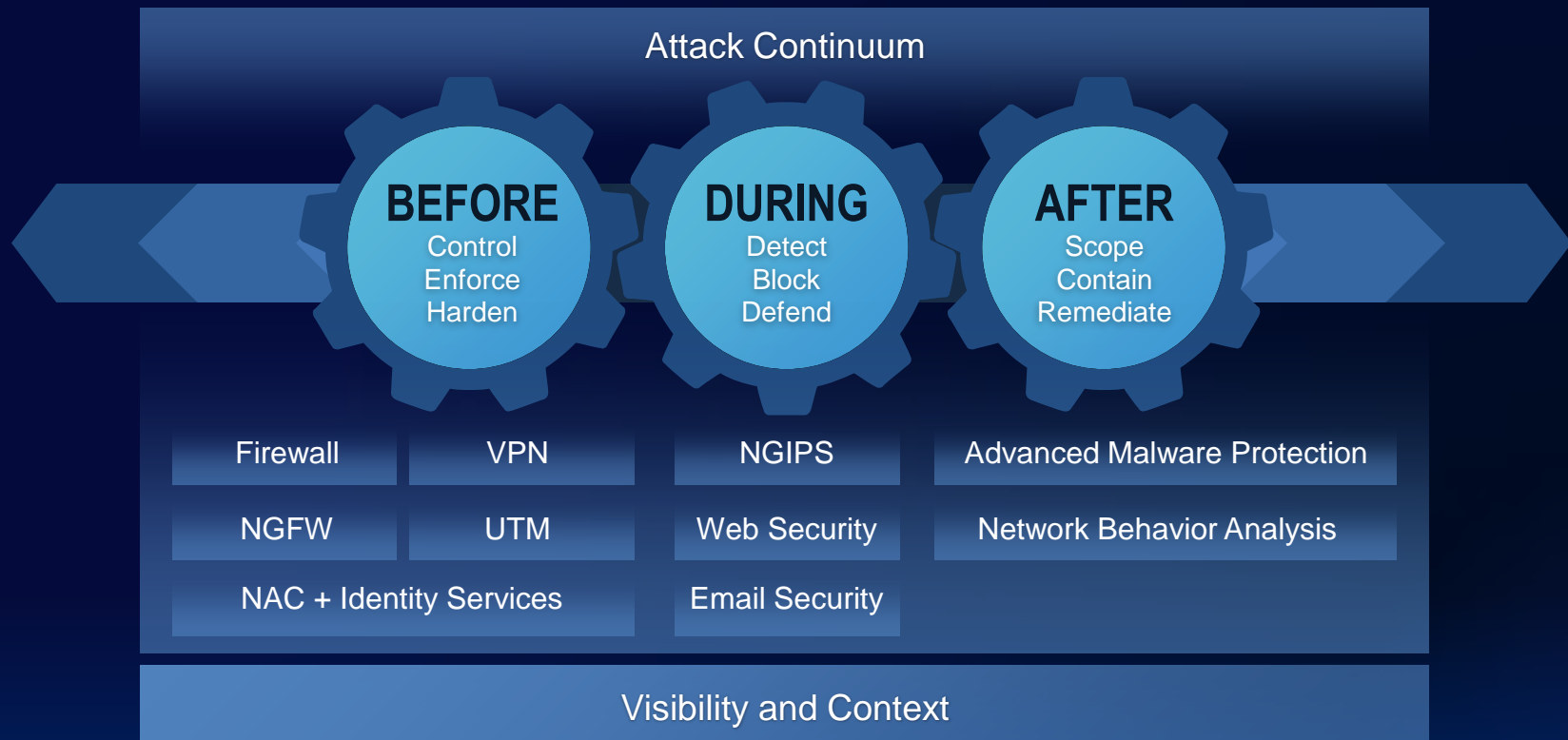
The New Security Model



Mapping Technologies to the Model



Cisco and Sourcefire—Better Together



Comprehensive Security Portfolio

- Cisco
- Sourcefire

Firewall & NGFW

- Cisco ASA 5500-X Series
- Cisco ASA 5500-X w/ NGFW license
- Cisco ASA 5585-X w/ NGFW blade
- FirePOWER NGFW

IPS & NGIPS

- Cisco IPS 4300 Series
- Cisco ASA 5500-X Series integrated IPS
- FirePOWER NGIPS
- FirePOWER NGIPS w/ Application Control
- FirePOWER Virtual NGIPS

Advanced Malware Protection

- FireAMP
- FireAMP Mobile
- FireAMP Virtual
- AMP for FirePOWER license
- Dedicated AMP FirePOWER appliance

Web Security

- Cisco Web Security Appliance (WSA)
- Cisco Virtual Web Security Appliance (vWSA)
- Cisco Cloud Web Security

Email Security

- Cisco Email Security Appliance (ESA)
- Cisco Virtual Email Security Appliance (vESA)
- Cisco Cloud Email Security

NAC + Identity Services

- Cisco Identity Services Engine (ISE)
- Cisco Access Control Server (ACS)

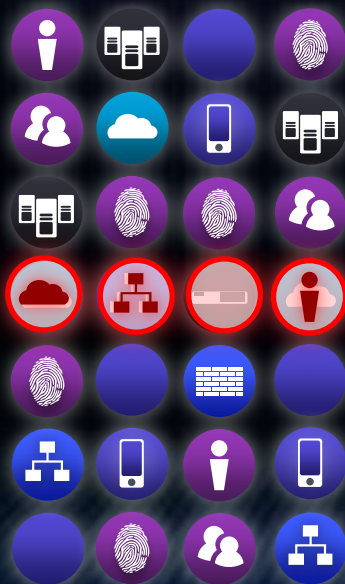
VPN

- Cisco AnyConnect VPN

UTM

- Meraki MX

DETECTED



IDENTIFY ADVANCED CYBER THREATS

Behavioral Analysis Artificial Intelligence

THREAT BEHAVIOR ANALYSIS

Leveraging Network, Web, and Identity Context

MODERN DETECTION ALGORITHMS

Behavioral Analysis Artificial Intelligence

SELF-LEARNING AND EVASION RESISTANCE

Game Theoretic Self Optimization

Cisco Acquires
COGNITIVE SECURITY



Agenda

- Introduction / The New Security Model

- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update

Gennemgang
Gennemgang

- Q & A

Alle

Cisco ASA Next-Generation Firewalls

Brian Hansen
Systems Engineer Security

Tech update D. 19. Nov. 2013

Agenda

Threat landscape

Introduction to Cisco ASA 5500-X Next-Generation Firewall

Feature Overview including Perigrine release

Context-Aware Policy

Context-Aware Security

Management

Summary



Market Dynamics

Mobility



Threat



Cloud



Megatrends Require an Innovative Approach to Security

Threat Evolution

Enterprise
Response

Anti-virus
(host-based)

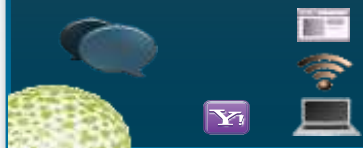
IDS/IPS
(network perimeter)

Reputation (global) &
Sandboxing

Intelligence & Analytics
(cloud)

Threat
Landscape

WORMS



2000

SPYWARE /
ROOTKITS



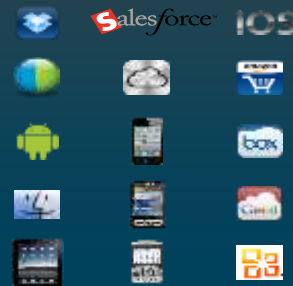
2005

APT's
CYBERWARE



2010

INCREASED ATTACK
SURFACE (MOBILITY &
CLOUD)



Tomorrow

Changing Threat Landscape

Counter-Measures Are Less Effective

1,114,399

websites compromised
per second



Cisco ASA 5500-X Next-Generation Firewalls



Cisco ASA NGFW Feature Overview

Context And Threat Awareness



Robust stateful inspection *and* broad, next-generation functionality

Multiple Form Factors

Context-Aware



- Deep application behavior control
- Industry-leading remote access VPN
- Enterprise-grade URL filtering
- User and device identification

Threat-Aware

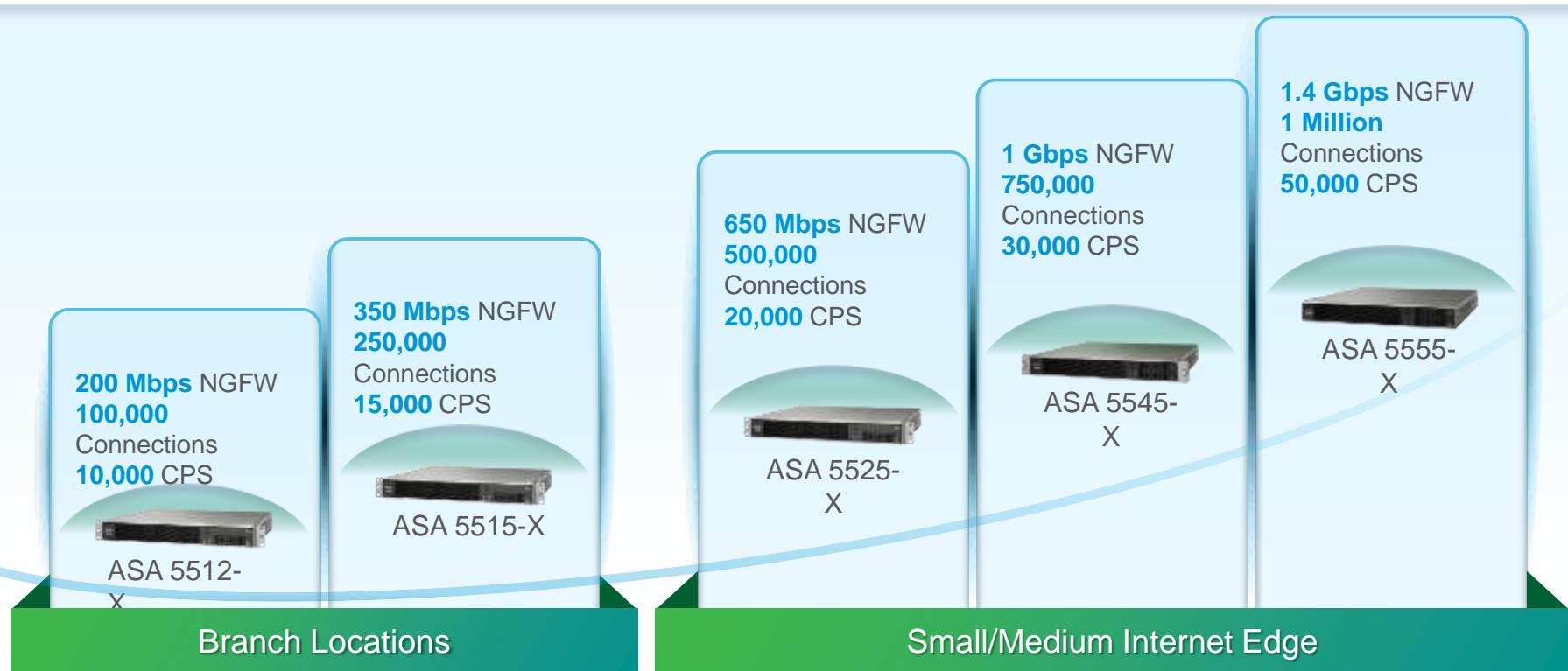


- Industry-leading web reputation for malware protection
- Embedded IPS for APT protection
- Powered by Cisco® SIO - largest global telemetry footprint – email, web, IPS, VPN, third party
- Near-real-time updates

Cisco ASA Stateful Inspection Firewall

MultiScale Performance

Next-Generation Security For The Internet Edge



MultiScale Performance

Next-Generation Security For The Internet Edge

2 Gbps NGFW
500,000 Connections
40,000 CPS



ASA 5585-SSP10

5 Gbps NGFW
1 Million Connections
75,000 CPS



ASA 5585-SSP20

9 Gbps NGFW
1.8 Million Connections
120,000 CPS



ASA 5585-SSP40

13 Gbps NGFW
4 Million Connections
160,000 CPS



ASA 5585-SSP60

Medium Internet Edge

Large Internet Edge

Features: Context-Aware Policy



Full-Spectrum User Identification

Covers Wide Breadth Of Identity Use Cases

Fidelity

NTLM
Kerberos

User Authentication

- Auth-aware apps
- Mac, Windows, Linux
- AD/LDAP user credential

TRUSTSEC*

Network Identity

Group information
Any tagged traffic

AD/LDAP Identity

- Non-auth-aware apps
- Any platform
- AD/LDAP credential

IP Surrogate
AD Agent

Breadth


* Future

Application Visibility And Control

Control Granular Behaviors Of Popular Applications

Broad...	Linkedin		Skype	YouTube	
	Facebook	iTunes	Yahoo	Google+	
... classification of all traffic More than 1200 apps					
MicroApp Engine Deep classification of targeted traffic More than 150,000 MicroApps	Farm Ville   	 		 	
App Behavior Control user interaction with the application	 	 	  	 	


External AVC Portal - – asacx-cisco.com


[Products & Services](#)[Support](#)[How to Buy](#)[Training & Events](#)[Partners](#)


ASA NGFW Services Applications Portal


This tool lets you search and filter applications supported by Cisco ASA NGFW Services, the context-aware firewall.


Featured search keywords


 Facebook

 iCloud

 iTunes

 Google Drive

 Skype

 BitTorrent

Applications (1181)


Recently Added
Application type
Authentication
Blogging
Business
Collaboration
Database
Distributed
Email
Enterprise Applications
Facebook
File Sharing
Games
Google+
Infrastructure

3Com AMP3
Registered with IANA on port 629 TCP/UDP
Type: Infrastructure

4shared
4shared is a web-based file sharing and cloud storage service.
Type: File Sharing

9P
9P (or the Plan 9 Filesystem Protocol or Styx) is a network protocol developed for the Plan 9 from Bell Labs distributed operating system as the means of connecting the components of a Plan 9 system. Files are key objects in Plan 9. They represent windows, network connections, processes, and almost anything else available in the operating system. Unlike NFS, 9P encourages caching and also serves synthetic files.
Type: Distributed

ACA Services
Registered with IANA on port 52 TCP/UDP
Type: Business

New Application Signature Request


Please use the following tool to request a product enhancement or provide support for an application that is not currently available.

[Log a new request](#)

Technical Support for an Existing Application

Please use the following method to log a support request to fix an existing signature that does not function as expected or to request technical support for the product.

[Log a service request](#)

Cisco ASA NGFW Services Context-Aware Security
Cisco ASA NGFW Services Context-Aware Security provides context-aware capabilities for exception visibility and control so your enterprise can take advantage of new applications and devices without compromising security.

Device-Aware

Cisco AnyConnect®
150 million endpoints

Device
OS

Cisco® Identity Services Engine*
BYOD solution

Apple Windows Android iOS

OS Version*

iOS 5

Windows
8

Posture

*



Registry



AV



Files

* Future

Enterprise-Grade URL Filtering

Industry-Leading Coverage And Efficacy

Marketing



Legal



Finance



60
Languages

200
Countries

20
Million URLs

10,000
Customers

Malware – High Volume, Always On, Always Changing



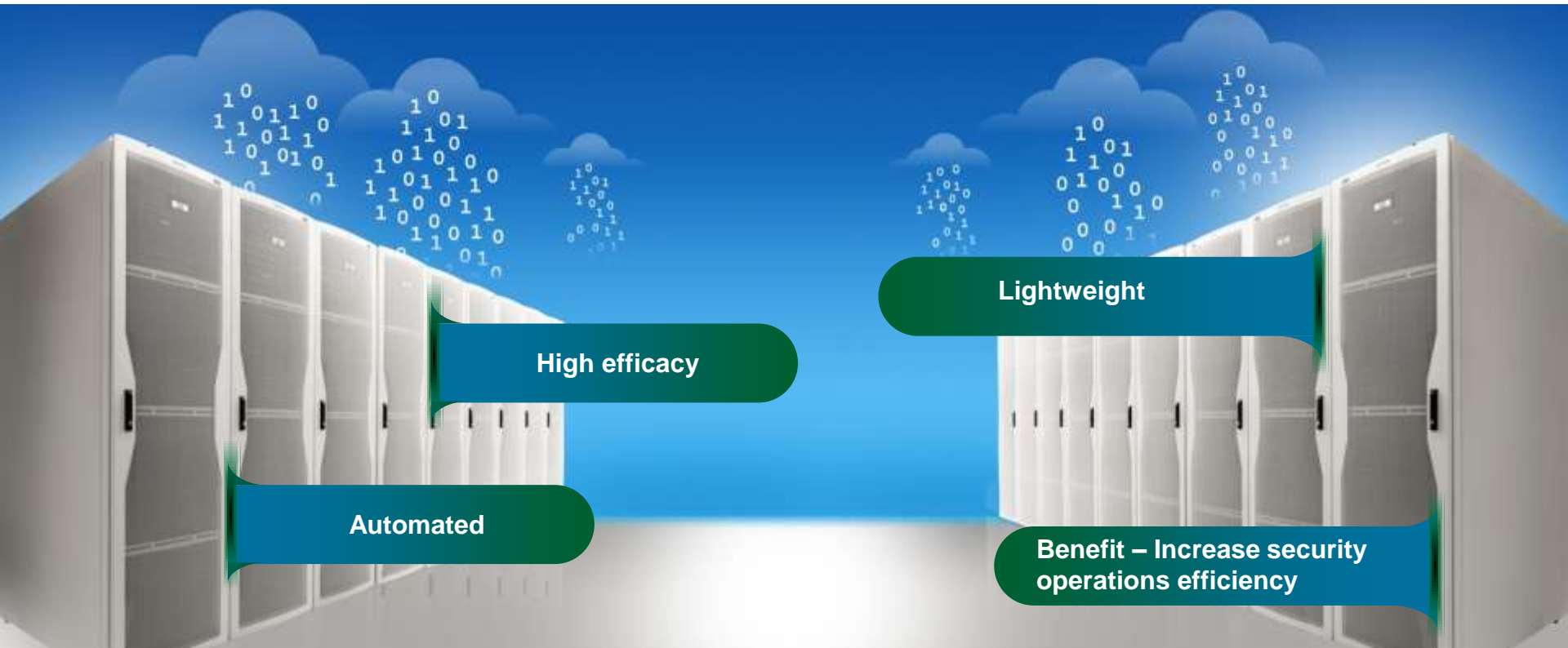
Malware

High volume

Always under attack

Complex and evasive

Cisco SIO – Malware Prevention Starts Here



Malware Prevention Starts Here

Cisco Security Intelligence Operation (SIO)



24 Hours Daily
OPERATIONS

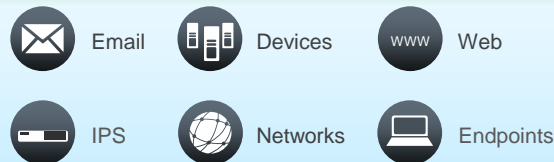
More Than 40
LANGUAGES

More Than \$100
Million
SPENT IN DYNAMIC RESEARCH
AND DEVELOPMENT

More Than 600
ENGINEERS, TECHNICIANS,
AND RESEARCHERS

More Than 80
PH.D, CCIE, CISSP, MSCE

Cisco® SIO



Visibility



Actions



Control

1.6 Million
GLOBAL SENSORS

35%
WORLDWIDE EMAIL TRAFFIC

75 TB
DATA RECEIVED PER DAY

13 Billion
WEB REQUESTS

More Than 150 Million
DEPLOYED ENDPOINTS



Information

3 to 5
MINUTE UPDATES

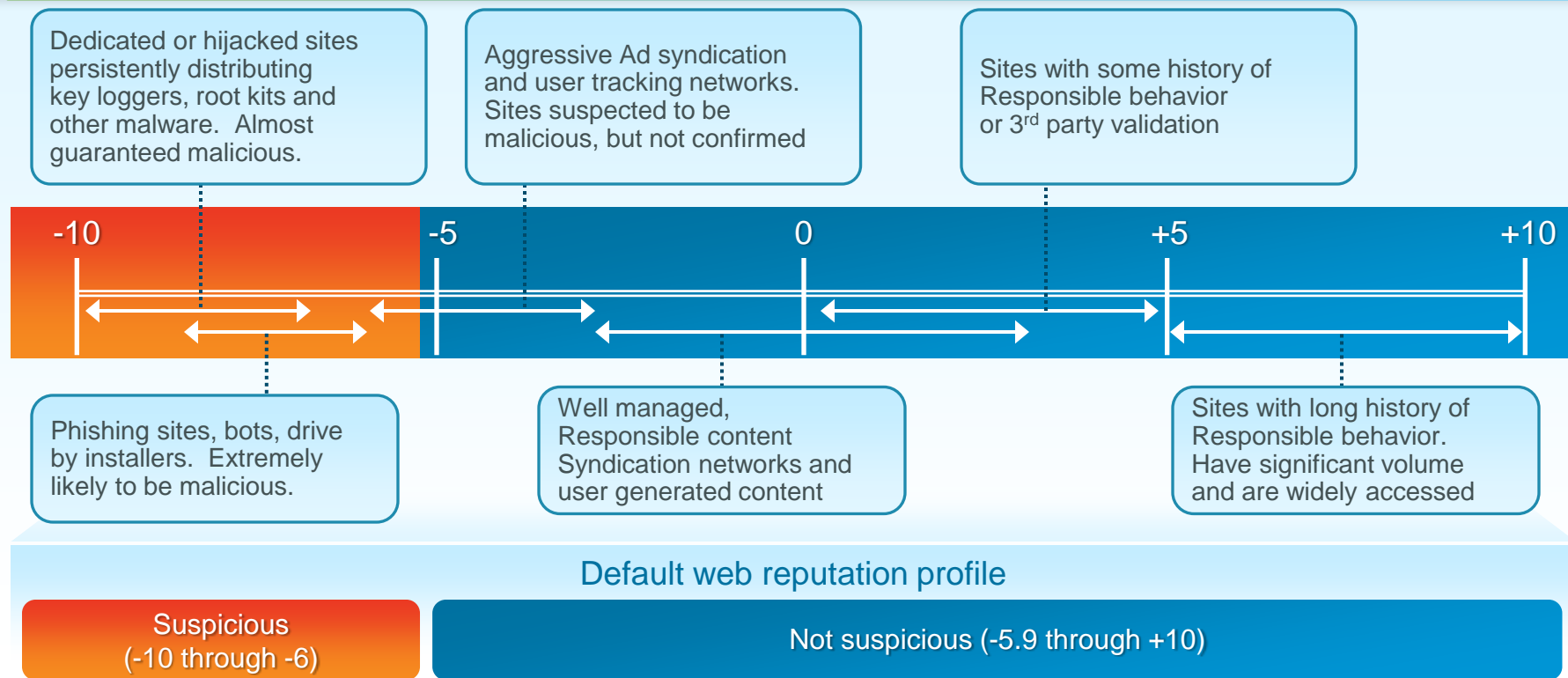
More Than 200
PARAMETERS TRACKED

More Than 5500
IPS SIGNATURES PRODUCED

More Than 70
PUBLICATIONS PRODUCED

More Than 8
Million
RULES PER DAY

Web Security Essentials – Reputation



NEW release



What's new with This release

We have added the following features:

- Support for Active/Standby

PRSM can discover HA configuration and treat HA pair as a single device (policy configuration, reporting)

- Next Generation IPS

- Platform support

Platform support has been added for SSP 40, 60

NGFW is now available on all midrange and all high-end models of ASA

What's new with Peregrine

has added the following features:

- Time ranges
- Interface roles – collections of interfaces that can be used to construct policies
- Rate limits
- Safe Search

Note: Not all features are available for all types of policies.

Policy Sharing

New with
NGFW 9.2

#	Source	Destination	Application/Service	Action/Conditions	Shared/Local	Interface roles
Device intrusion prevention On Device malware protection On						
▶ Universal Top CX Access Policy Set (0)					Universal	
▼ ASA4 policies (1)					ASA4	
1	Any	Any	Facebook Behavior	Allow Conditions	ASA4	Any to Any
▼ Production Units (2)					Shared(2)	
1	Any	Inappropriate websites	Any	Deny Conditions	ASA4	Any to Any
2	Any	Boarding websites	Any	Warn Conditions	Shared (2)	Any to Any
▼ Universal Bottom CX Access Policy S...					Universal	
1	Any	Any	Media Behavior	Allow Conditions Bandwidth limit 80 Kbps	All Devices	Any to Any
2	Any	Any	Any	Allow Conditions Outbound connections only	All Devices	Any to Any

- Policy sets can have different scopes:
 - Universal – policy set is shared by all devices
 - Shared – policy set is shared among some devices
 - Local – policy set only applies to one device
- At the top is the universal top context-aware access policy set, applied first
- At the bottom is the universal bottom context-aware access policy set, applied last

Safe Search

New with
NGFW 9.2

Allows context-aware access policies only

Blocks searches on supported search engines if:

- Safe Search is enabled in a matching access policy and Safe Search is disabled in a browser

Blocks searches on supported search engines if:

- Google
- Yahoo
- Bing
- Ask
- Duckduckgo

Create Policy

Policy Name * XYZ

Enable Policy ☒ On ☐ Off

Eventing ☒ On ☐ Off

Policy Action

Capture packets ☒ On ☐ Off

Source

Destination

Application / Service

Profile

Bandwidth limit

Safe search ☒ On ☐ Off

File filtering

NG IPS Threat Profiles

Available in newest release

- Risk Based Control
- 3 ranges
 - Block and Monitor
 - Allow and Monitor
 - Don't Monitor
- Customizable exceptions

Help

Edit Threat profile

Name Status Committed

Object type Threat profile

Description

Tags

Created June 17, 2013 by admin

Last modified June 17, 2013 by admin

Ticket ID

100 70 30 0

High Significant Potential Unlikely

← Increasing risk to your network →

Advanced threat settings

Select threats from the list and apply specific action. The system will take the selected action irrespective of the score and probability settings.

Exceptions

Threat name	Action	
Worm: W32/Conficker.worm	<input type="text" value="Deny"/>	<input type="button" value="Remove"/>

Access Policy configuration for NGFW IPS

Available in release

- Threat Profile Field
- Use Custom IPS Profile or the Device Level profile
- Different profiles can be applied to different subset of traffic
- Selection criteria include 5-tuple, user and application

Create Policy

Policy Name *

Enable Policy ☒ On ☐ Off

Policy Action

Eventing ☒ On ☐ Off

Capture packets ☒ On ☐ Off

Source

Destination

Application / Service

Profile

Bandwidth limit

Safe search ☒ On ☐ Off

File filtering

Web reputation

Threat profile

Interface roles

Tags

Ticket ID

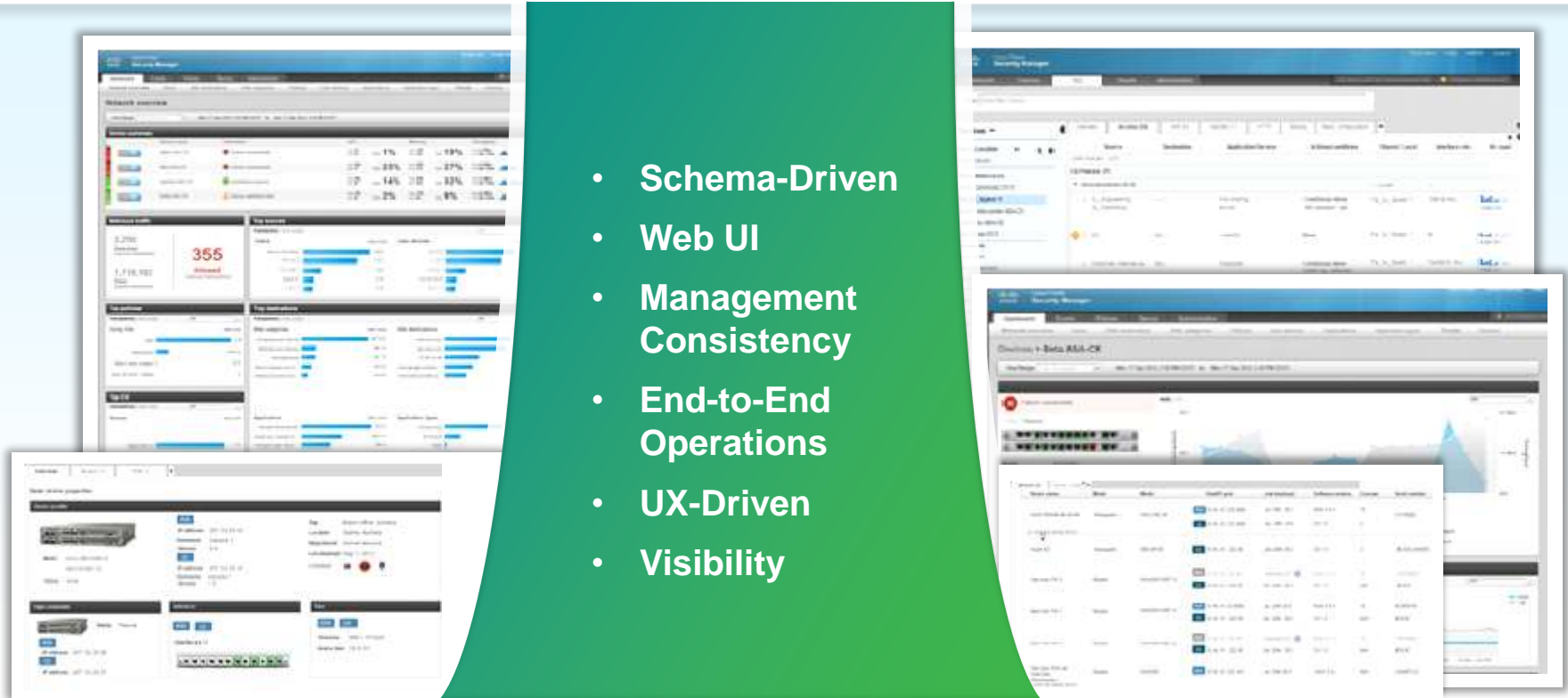
* required fields

Management



Cisco Prime Security Manager

- Schema-Driven
- Web UI
- Management Consistency
- End-to-End Operations
- UX-Driven
- Visibility



Cisco Prime Security Manager

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

Dashboard



Navigate Down to Events

Creation time	Event type	Device	Severity	Message	Source	Destination IP	Destination port	Application	Application port	Response status	Event category
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request
2013-03-14 12:07:00	HTTP Request	10.10.10.1	Info	HTTP/1.1 200 OK	10.10.10.1	10.10.10.1	80	HTTP	80	200	HTTP Request

Visibility & Control

View Event

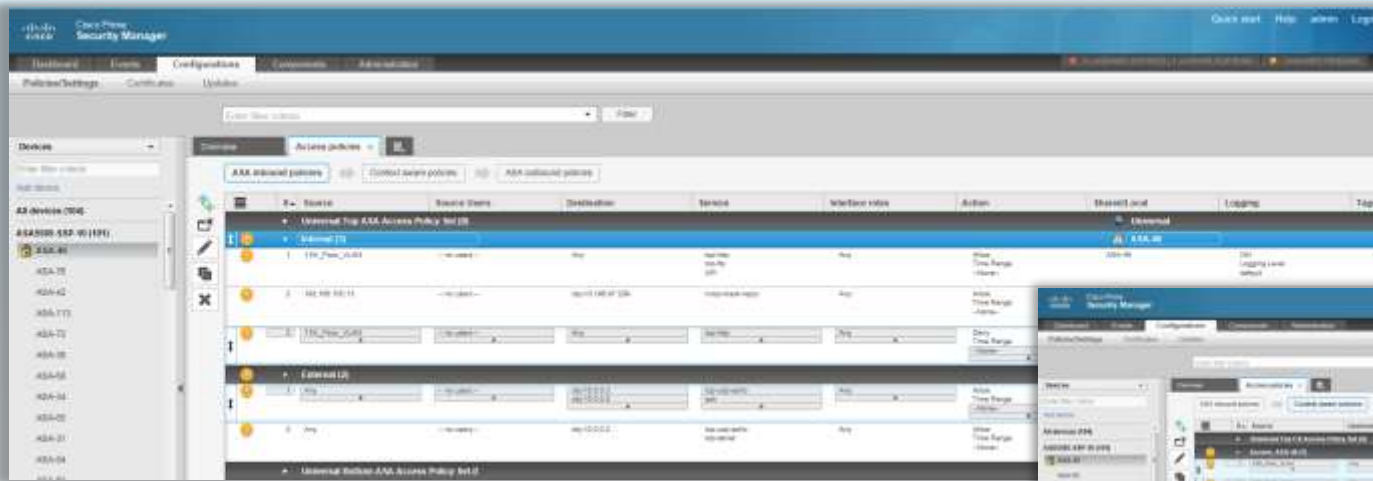
A screenshot of the 'View Event' screen in Cisco Prime Security Manager. It displays a detailed view of a specific event, including a 'Description' tab with a timeline of the event, a 'Details' tab with various fields like 'Source', 'Destination', and 'Application', and a 'Log' tab showing the raw log data. The interface is designed for easy navigation and detailed analysis of security events.

Map Events to Policies

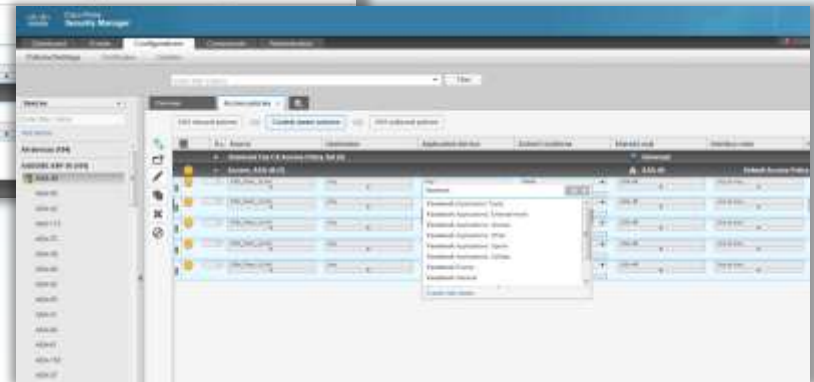
A screenshot of the 'Map Events to Policies' screen in Cisco Prime Security Manager. It shows a table with columns for 'Policy Name', 'Policy ID', 'Policy Type', 'Policy Status', and 'Policy Action'. The table lists several policies, including 'Default Policy', 'Default Policy', and 'Default Policy'. The interface allows users to view and manage the mapping of events to specific security policies.

Cisco Prime Security Manager

Manage Classic Firewall Rule Sets As Well As NGFW From One Console



FW access policies



NGFW Services (AVC, WSE, IPS) policies

Agenda

- Introduction / The New Security Model
- **ASA-CX Next Generation FW**
- **ASA-CX Next Generation FW**

Gennemgang
Demo

Pause – 10 min

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update
- Q & A

Gennemgang
Gennemgang

Alle

Agenda

- Introduction / The New Security Model

- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min KAGE & KAFFE

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update

Gennemgang
Gennemgang

- Q & A

Alle

Agenda

- Introduction / The New Security Model
- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min

- **ISE 1.2 Gennemgang & Whats New**
- ISE 1.2 MDM integration

Gennemgang
Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update
- Q & A

Gennemgang
Gennemgang

Alle

ISE 1.2 og MDM integration

Christian Helmundt Bermann
Systems Engineer - Security

November, 2013

Agenda

- ISE 1.2 news
- MDM integration
- Demo video

Cisco Secure Access Enabled by ISE

Policy Management



Identity Services Engine (ISE)



Prime Infrastructure

Policy Information



User Directory



Profiling from Cisco Infrastructure



Posture from End-Point Agents

Policy Enforcement



Cisco Infrastructure: Switches, Wireless Controllers, Firewalls, Routers

ISE 1.2 News











ISE 1.2 Features

- Upgrade Process Shortened and Simplified
- DB Changes: Improved Scaling/WAN Replication
- Policy Sets (ACS Parity)
- Logical Profile Groups & Profile as Attribute
- 3rd Party MDM Integration
- Re-Written Reporting w/ Scheduling
- 3rd Party MAB Support
- 64-Bit Architecture
- Appliance Refresh (UCS-Based)
- Higher Capacity Per Node / Deployment
- Localization: 10 New Languages
- External RESTful Services (ERS) API
- Registration Status as an Attribute
- Bootstrap Wizard
- Windows 2012 Support
- TCP and Secure Syslog
- Custom CoA Action Per Profile
- View Logs from CLI (no Support Bundle Needed)
- Live Sessions Log
- Search & Session Trace Tool
- Web Portals: Mobile Friendly, Multi-Interface, New Themes
- Guest: Max Session Limit, Activated Guest Role, Extend Duration/Reactivate Expired, Change Time, CoA on Guest Expiry/Delete
- dACL Checker
- Profiler: Feed Service, configurable SNMP strings
- Backup / Restore Progress Bars, Cancel, Schedule
- Licensing for Both Primary & Sec Admin Nodes
- Optimized Logging and Simplified Alarming
- Certificates: Wildcard Certs, Custom SAN, New Cert Fields, Cisco Mfg Certs Loaded, Cert Expiry Alarms.
- VMware Cloning and vMotion Support
- Service Templates for SANet
- Common Criteria

ISE 1.2 Alarms

- Alarms now displayed as dashlet on ISE Home Page.

- Following alarms are added or enhanced in ISE 1.2
 - Misconfigured supplicant
 - Misconfigured NAS
 - Detect Slow Authentications
 - RADIUS Request Dropped with more accurate failure reasons
 - Excessive Accounting Messages
 - Mixing RADIUS Request between ISE PSN's due to NAD/LB behavior.

Alarms 			
	Name	Occurrences	Last Occurred
	Health Status Unavailable	352 times	less than 1 min ago
	RADIUS Request Dropped	131 times	2 mins ago
	High Load Average	1161 times	41 mins ago
	EAP Connection Timeout	30 times	1 hr 48 mins ago
	License Expiration	140 times	2 hrs 4 mins ago
	Authentication Inactivity	151 times	2 hrs 46 mins ago
	Configuration Changed	2333 times	7 hrs 5 mins ago

Live Authentications and Sessions

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, and Administration. Below these, there are sections for Misconfigured Supplicants (21), Misconfigured Network Devices (10), RADIUS Drops (521), Client Shipped Responding (6716), and Repeat Counts (19052). The main table displays Live Sessions with columns: Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, and Network Device. A red box highlights a list of sessions, and a blue box highlights a specific session with a failed status. A blue arrow points from the blue box to a text box explaining the status.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	Info		0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890	Info		11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:29.658	Info		99	wekang	B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:29.252	Info		1	mutama	CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:25.595	Info		0	jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	
2013-09-27 14:46:25.595	Success			jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
2013-09-27 14:46:22.636	Success			jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21.486	Failure			anonymous	00:1E:65:D6:93:E2		WNBU-WLC1
2013-09-27 14:46:18.884	Info		7	dsladden	0C:77:1A:9A:F6:73	Apple-iPhone	

Blue entry = Most current Live Sessions entry with repeated successful auth counter

PSN Filtering and Noise Suppression

Misconfigured Client Dynamic Detection and Suppression

- Flag misbehaving supplicants when fail auth more than once per interval
 - Send Alarm with failure stats every interval.
 - Stop sending logs for repeat auth failures for same endpoint during rejection interval.
 - Successful auth clears flag
- Reject matching requests during interval
 - Match these attributes:
 - Supplicant (Calling-Station-ID)
 - NAS (NAS-IP-Address)
 - Failure reason
 - Excludes CoA messages / bad credentials
 - Next request after interval is fully processed.
- Do not save repeated successful auth events to DB (events will not display in Live Auth log).
- Stop sending Accounting logs for same session during interval.
- Detect and log NAS retransmission timeouts for auth steps that exceed threshold.

Administration > System > Settings > Protocols > RADIUS

RADIUS Settings

Suppress Anomalous Clients ☒ ⓘ

Anomalous Client Detection

Detection Interval (in minutes)

Reporting Interval (in minutes)

Reject Requests After Detection ☒ ⓘ

Request Rejection Interval (in minutes)

Suppress Repeated Successful Authentications ☒ ⓘ

Accounting Suppression Interval (in seconds)

Long Processing Step Threshold Interval ⓘ (in milliseconds)

PSN - Collection Filters

Static Client Suppression

- PSN static filter based on single attribute:

User Name
Policy Set Name
NAS-IP-Address
Device-IP-Address
MAC (Calling-Station-ID)

Administration > System > Logging > Collection Filters

Logging

- Local Log Settings
- Remote Logging Targets
- Logging Categories
- Message Catalog
- Debug Log Configuration
- Collection Filters

Collection Filter List > New Collection Filter

Collection Filters

* Attribute * Value * Filter Type

Submit





Filter All
Filter Passed
Filter Failed
Disable Suppression

User Name
Policy Set Name
NAS IP Address
Device IP Address
MAC Address

- Filter Messages Based on Auth Result:

All (Passed/Fail)
All Failed
All Passed

- Select Messages to **Disable Suppression** for failed auth @PSN and successful auth @Mn

Collection Filters			
			
<input type="checkbox"/>	Attribute	Value	Filter Type
<input type="checkbox"/>	MAC Address	11:22:44:AA:BB:CC	Disable Suppression
<input type="checkbox"/>	NAS IP Address	10.6.6.6	Filter Failed
<input type="checkbox"/>	Policy Set Name	RADIUS_Probes	Filter Passed
<input type="checkbox"/>	User Name	chyps	Filter All

Web Portal Port/Interface Settings

- Before ISE 1.2:
 - All web services supported on Management interface (eth0) only.
 - URL Redirection always uses CN value of node certificate to populate redirect URL:
https://<Cert_CN_FQDN>:8443/...

Every service enabled on every port and sharing same ports

- **With ISE 1.2:**
 - **All interfaces enabled for all web services by default.**
 - **Redirect URL populated with 1st service-enabled interface; host FQDN for GE0; interface IP for all other interfaces (GE1-GE3)**

Web Portal Settings

Admin Portal Settings

HTTP Port

HTTPS Port

Blacklist Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces ☒ GigabitEthernet 0
☒ GigabitEthernet 1
☒ GigabitEthernet 2
☒ GigabitEthernet 3

Guest Portal and Client Provisioning Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces ☒ GigabitEthernet 0
☒ GigabitEthernet 1
☒ GigabitEthernet 2
☒ GigabitEthernet 3

My Devices Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces ☒ GigabitEthernet 0
☒ GigabitEthernet 1
☒ GigabitEthernet 2
☒ GigabitEthernet 3

Sponsor Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces ☒ GigabitEthernet 0
☒ GigabitEthernet 1
☒ GigabitEthernet 2
☒ GigabitEthernet 3

Ports restricted to 8000-8999; upgrade retains original setting even if outside this range.

Policy Sets

- Before (1.1.x):
 - Single Authentication and Authorization Policy
- Many Different Sub-Policies and Use Cases:
 - Location-Based Policies
 - Mergers: Company A vs. B
 - Access Method
 - Wired/WirelessVPN
 - On-Boarding / BYOD Policies
 - Policies for Modes:
 - Monitor / Low-Impact / Closed
 - Third Party Devices

Authorization Policy

Define the Authorization Policy by configuring rules based on

First Matched Rule Applies

Real Policy From Cisco's Own ALPHA

WHAT IF THIS WAS IT'S OWN POLICY TABLE

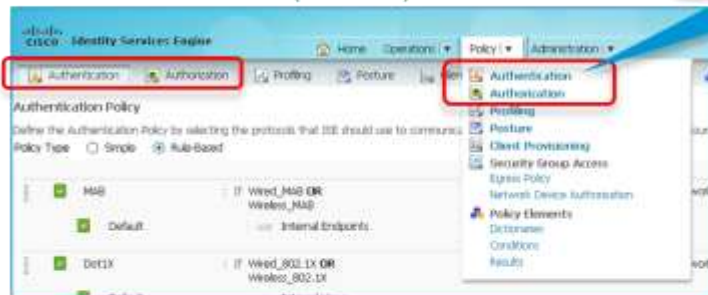
WHAT IF THIS WAS IT'S OWN POLICY TABLE

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	EAP-Chaining	Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapChainingDefault EQUALS User and machine both succeeded	Wired-PerMSLS	0.00
✓	Wireless-Block-List-Default	Blocklist AND Wireless_802.11	Blocklist-Wireless_Access	0.00
✓	Hyd-Block-List-Devices	Blocklist AND DEVICE:Device Type EQUALS All Device Types:WirelessWLC AND DEVICE:Location EQUALS All Locations:IND-HYD	HYD-Blocklist_Access	0.00
✓	Hyd-Wireless-Reg-Mobile	RegisteredDevices AND DEVICE:Device Type EQUALS All Device Types:WirelessWLC AND DEVICE:Location EQUALS All Locations:IND-HYD AND Endpoints:MassDeployable EQUALS No	WLC-HYD-Y101-Pull-Access	0.00
✓	Hyd-Android-Google-Store	RegisteredDevices AND DEVICE:Device Type EQUALS All Device Types:WirelessWLC AND DEVICE:Location EQUALS All Locations:IND-HYD AND Network Access:EapAuthentication NOT EQUALS EAP-TLS AND Session:Device-OS EQUALS Android	HYD-Google_Store	0.00
✓	NSP-Policy-Android	Session:Device-OS EQUALS Android	WLC_STORE-Android	0.00
✓	NSP-Policy-Unknown_Big22	Wireless_802.11 AND Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.34.2	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_Big3	Wireless_802.11 AND Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND DEVICE:Location EQUALS All Locations:R08 AND Airspace:Airspace-When-Id EQUALS 1	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_RTP-DEAP	Wireless_802.11 AND Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND DEVICE:Location EQUALS All Locations:RTP-DEAP	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_Big24	Wireless_802.11 AND Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.34.2	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_NQWC1	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.148.4	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_NQWC2	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.145.4 AND Airspace:Airspace-When-Id EQUALS 1	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_NQWC4	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.148.4	NSP-Auto-Profile	0.00
✓	NSP-Policy-Unknown_NQWC3	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.15.344 AND Airspace:Airspace-When-Id EQUALS 13	NSP-Auto-Profile	0.00
✓	Big22-Switch-Demo	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.15.344 AND Airspace:Airspace-When-Id EQUALS 1	PermitAccess	0.00
✓	NSP-Policy-Unknown_NQWC1	Network Access:AuthenticationMethod EQUALS RSCNAPV2 AND Network Access:Device IP Address EQUALS 10.31.148.3	NSP-Auto-Profile	0.00
✓	Edison-Switch-Debug	Wireless_802.11 AND DEVICE:Device Type EQUALS All Device Types:WirelessWLC:NQWC AND DEVICE:Location EQUALS All Locations:FSJC:FSJCH	PermitAccess	0.00

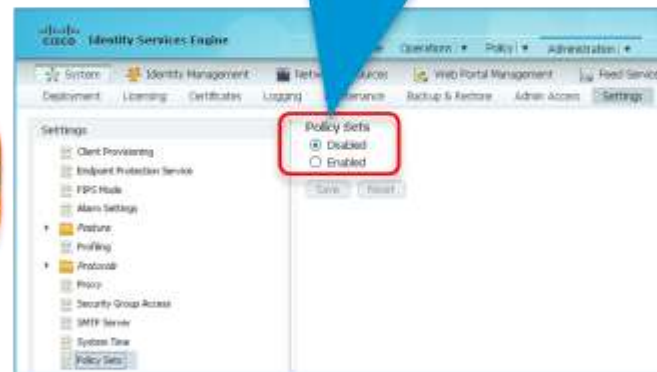
Policy Sets

Introduction (Cont.)

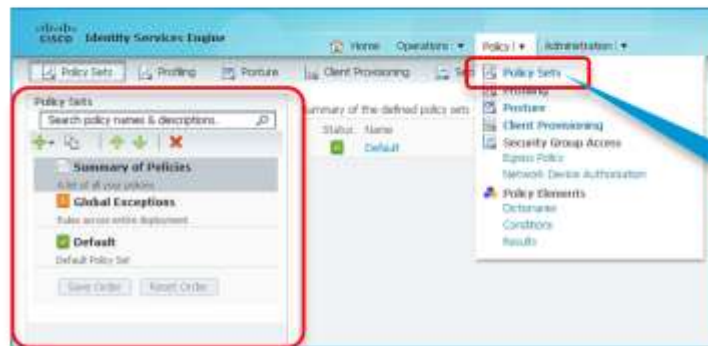
1 Simple Policy mode – notice the authentication and authorization policies in the menu



2 **NEW**
To switch from Simple Policy mode into Policy Set mode, select Enabled and Save (Administration → System → Settings | Policy Sets)



3 **new**
Policy Sets mode – notice the changes in the menu



Logical Profiles == Clean Policies



- Before ISE 1.2:

iDevices	if Apple-iDevice OR Apple-iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry OR HTC-Phone OR MotorolaDroid-Device OR SymbianOS-Device OR Android	then	PermitAccess
Default	if no matches, then		WebAuth

- With ISE 1.2:

Profiled Cisco IP Phones	if Cisco-IP-Phone	then	Cisco_IP_Phones
I-Devices	if EndPoints:LogicalProfile EQUALS i-Devices	then	PermitAccess
Employees	if AD1:ExternalGroups EQUALS cts.local/Users /Employees	then	PermitAccess AND Employee

Global Search



Search Example

- Search using keywords
- Examples:
 - Username
 - IP address
 - MAC address
 - Posture status

The screenshot shows a network management dashboard with a search bar at the top right containing the text 'apple-ipad'. A search results modal is open, displaying the following information:

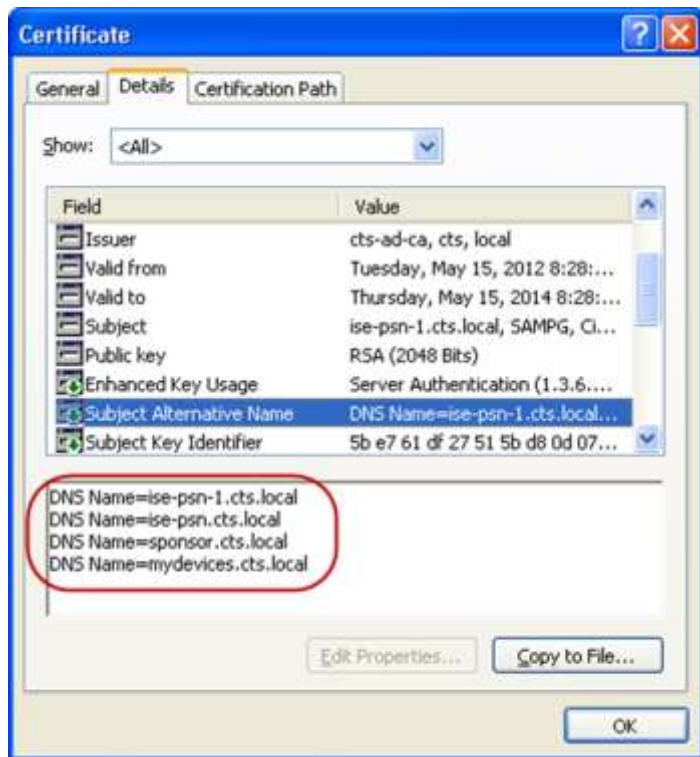
- Search Results:** 0 Connected, 0 Failed, 2 Disconnected, 2 Total.
- Distribution Panel:** A green-bordered box highlights a list of smart buckets:
 - Authorization Profile (2)
 - Failure Reason (1)
 - Identity Group (2)
 - Identity Store (2)
 - Location (1)
 - Network Device (1)
 - Network Device Type (1)
 - Operating System (1)
 - Posture Status (1)
 - Security Group (1)
 - User Type (1)
- Search Results List:** Two entries for 'Apple-iPad' are shown, each with a play button icon.
 - Entry 1: employee1, D8:A2:5E:6B:41:83, - NorthAmeric... Switches#Ac... NSP
 - Entry 2: employee1, B8:C7:5D:D4:95:32, - NorthAmeric... Switches#Ac... MDM-OnBoard
- Export Results:** A green-bordered button at the bottom right of the modal.

The background dashboard includes sections for 'Active Guests' (0), 'Alarms' (a table of events), and 'Posture Compliance' (Total 0).

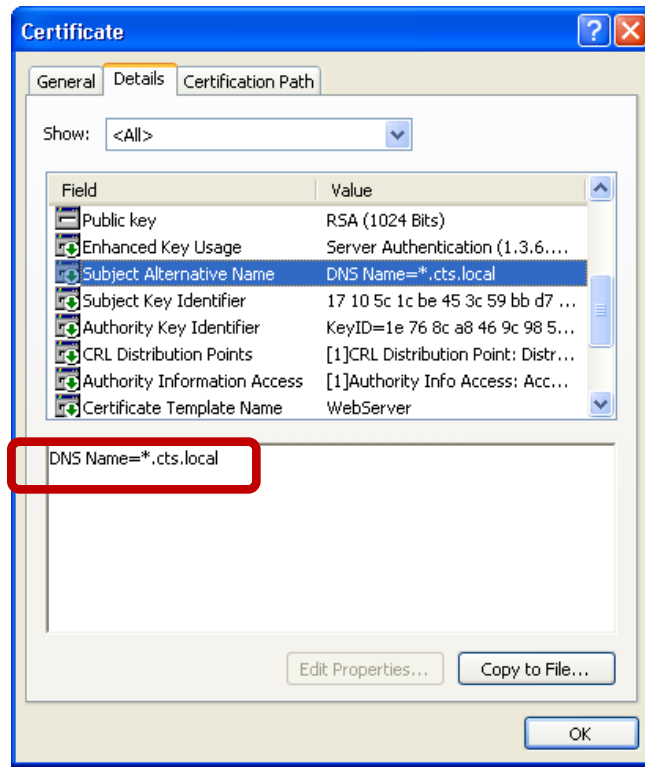
Name	Occurrence
EAP Connection Timeout	1
No Configuration Backup Scheduled	2
High RADIUS Latency	1
COA Failed	3
Configuration Changed	122
RADIUS Request Dropped	36
Unknown NAD	13

Distribution By:	Count
Posture Status	No Data
Operating System	No Data

Custom SANs and Wildcard Certificates




One cert **PER** PSN required



One cert for **ALL** PSNs


ISE 1.2—New Portal Themes and Localizations


Sponsor Portal


 **CISCO** Sponsor Portal

Welcome admin1 | [My Settings](#) | [Sign Out](#)

Manage Guest Accounts

 Create Account

 Import Accounts

 Create Random Accounts

Account List

<input type="checkbox"/>	Username	Status	First Name	Last Name	Email Address
<input type="checkbox"/>	anemzwji	Awaiting Initial Login	jackdoe		jackdoe@company.com
<input type="checkbox"/>	jguest01	Awaiting Initial Login	Jim	Guest	jeff@comp.com
<input type="checkbox"/>	jsmith01	Awaiting Initial Login	John	Smith	John.Smith@company.com

74

74

Mobile-Friendly Portals

The screenshot shows a web browser window with the title "Guest Portal". The page has a green header bar with the text "Guest Portal". Below the header, there is a login form with the following elements:

- A "Username:" label followed by a text input field.
- A "Password:" label followed by a text input field.
- A blue "Sign On" button.
- A "Change Password" link with an information icon.

Below the login form is the Cisco logo. At the bottom of the page, there is a green box with the text "Web Auth Portal".

The screenshot shows a web browser window with the title "My Devices Portal". The page has a green header bar with the text "My Devices Portal". Below the header, there is a "Device Registration" form with the following elements:

- A "Welcome" message.
- A message: "This device has not been registered. Click the 'Register' button to configure your device to use the secure network."
- A "Device ID:" label followed by a text input field containing the value "D0-A2-5E-8B-47-85".
- A "Description:" label followed by a text input field.
- A blue "Register" button.

Below the registration form is the Cisco logo. At the bottom of the page, there is a green box with the text "My Devices Portal".

Web Authentication

Mobile Portal Example

- Checkbox in web portal configuration
- Detects mobile devices and automatically resizes screen display

Guest Portal

Username:
guestuser

Password:
.....

Sign On

Multi-Portal

General Operations Custom

Guest Portal Policy Configuration
Guest users should agree to an acceptable use policy

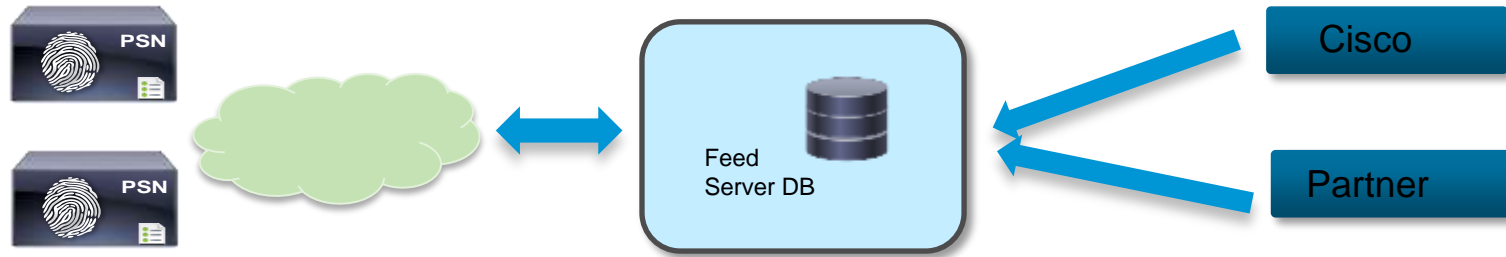
☐ Not Used
☒ First Login
☐ Every Login

☒ Enable Self-Provisioning Flow
☒ Enable Mobile Portal
☒ Allow guest users to change password
☐ Require guest users to change password at expiration
☐ Guest users should download the posture client
☐ Guest users should be allowed to do self service



Profiler Feed Service

Zero Day availability



Feed Service

Profiler Feed Service Configuration

☒ Enable Profiler Feed Service

Administrator Notification Options

☒ Notify administrator when download occurs

Administrator email address

Notifications
Supported

- No need to wait for new ISE version
- Zero day support for popular endpoints is added using Feed Server

Enable Profiler Feed Service

Enabling the Profiler Feed Service will instruct the ISE system to contact CISCO for new and updated profiles created since the last ISE update. If the Cisco feed server is not reachable or other errors occur they will be reported in the profiler feed server report.

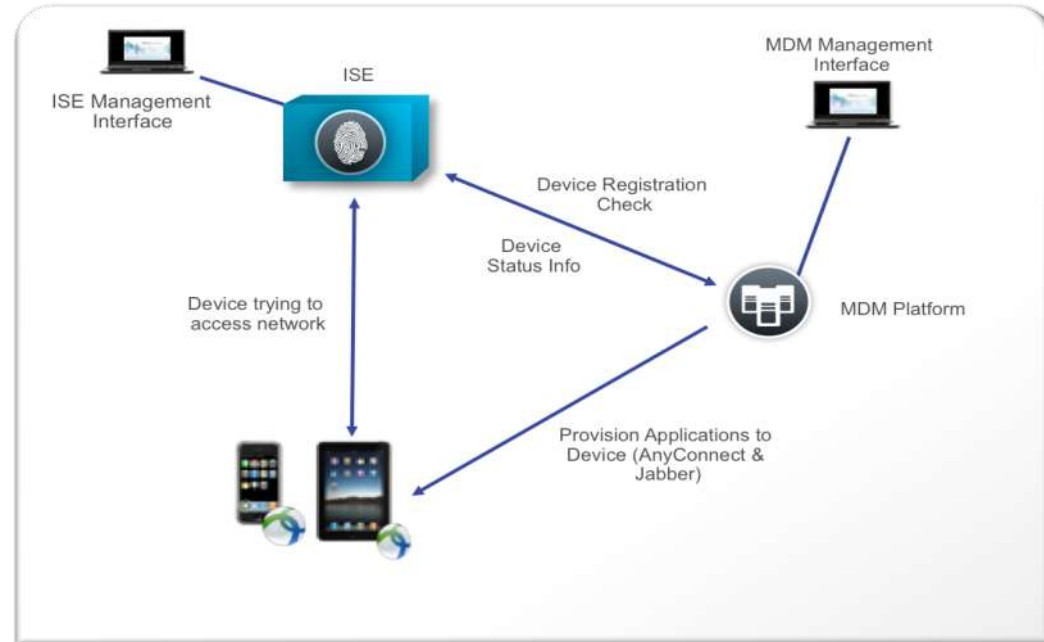
OK

MDM Integration



ISE Partner MDM

- MDM device registration via ISE
 - Non registered clients redirected to MDM registration page
- Restricted access
 - Non compliant clients will be given restricted access based on policy
- Endpoint MDM agent
 - Compliance
 - Device applications check
- Device action from ISE
 - Device stolen -> wipe data on client



Version: 5.0



Version: 6.2



Version: 7.1



Version: 2.3



MDM Compliance Checking

Compliance and Attribute Retrieval via API

- Compliance based on:

General Compliant or ! Compliant status

OR

Disk encryption enabled

Pin lock enabled

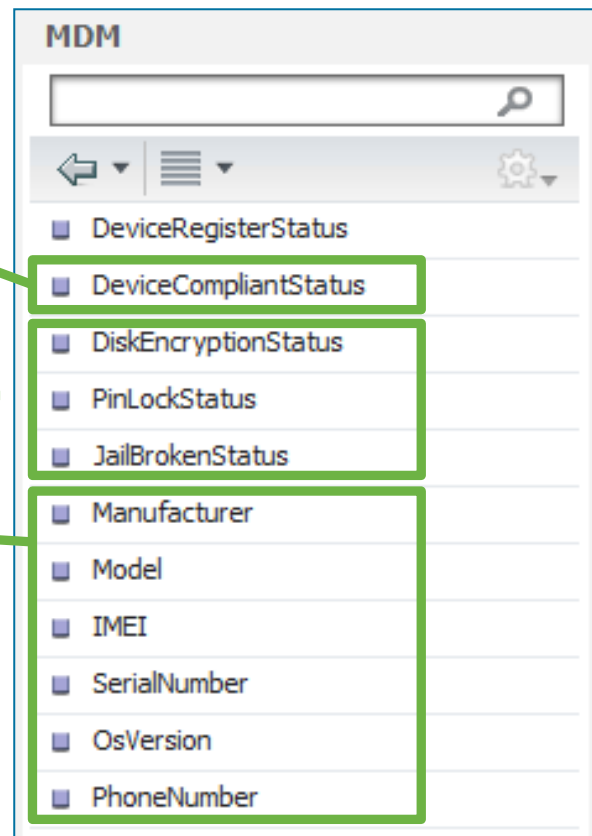
Jail broken status

Macro level

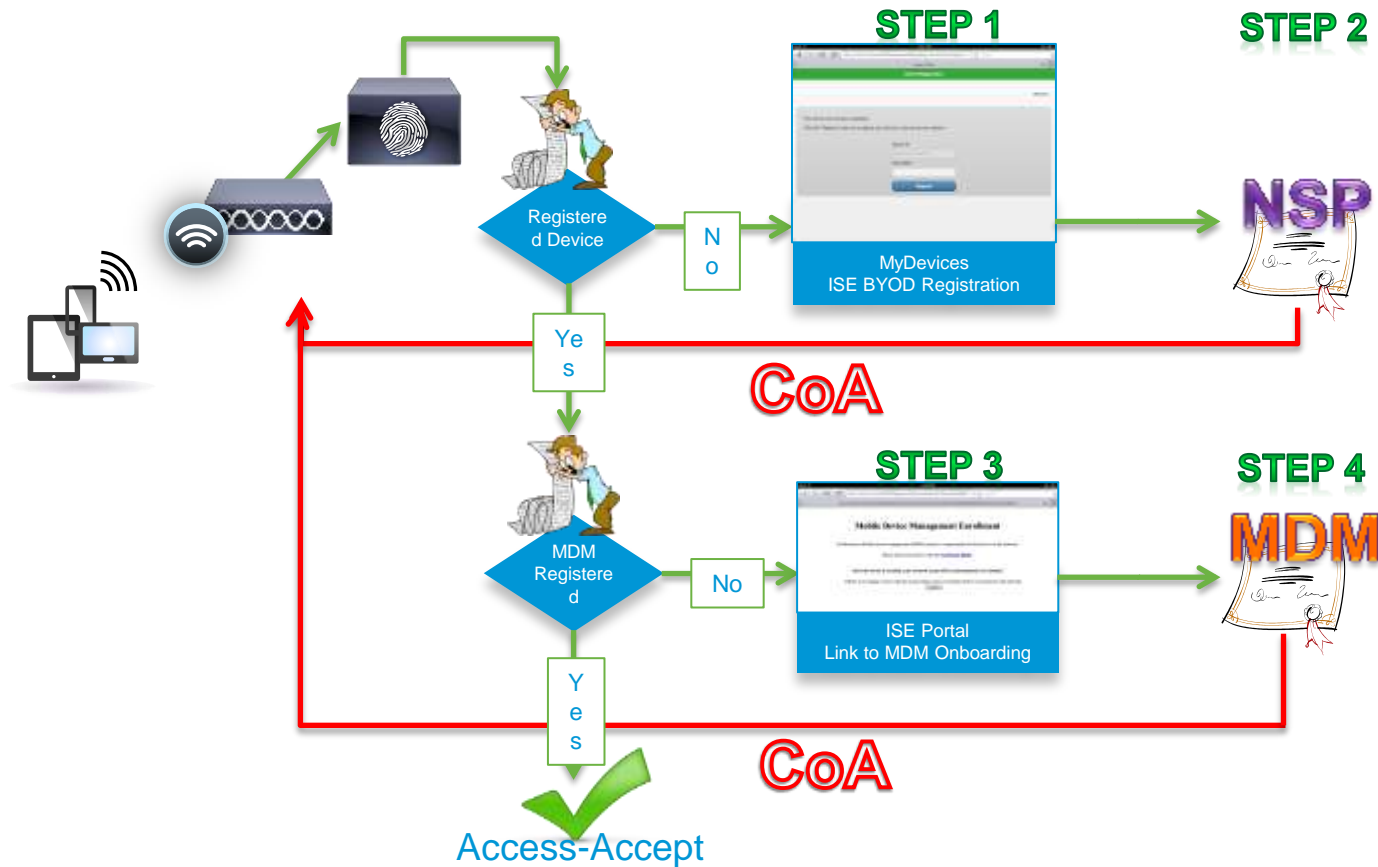
Micro level

- MDM attributes available for policy conditions
- “Passive Reassessment”: Bulk recheck against the MDM server using configurable timer.

If result of periodic recheck shows that a connected device is no longer compliant, ISE sends a CoA to terminate session.



MDM Onboarding Flow



Notes from Xenmobile install

- Needs APN cert for Apple device (cannot install w/o?)
 - Generate CSR on CA for Apple devices
 - Send CSR to support@zenprise.com
 - Submit the MDM signed CSR to Apple
 - Complete the CSR on the CA server
-
- Install setting up postgres account
 - Most install is default settings
 - If you need to abort install pay attention to the postgresSQL

Communication

- HTTPS/443
- From ISE to MDM
- Trust between ISE and MDM
 - ISE has no list of Trusted root CA's
 - Export MDM site certificate and import into local certificate store of ISE
 - Account for ISE to access MDM API – Administrator role

Dictionary attributes

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Operations, Policy, and Administration. Below this, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main content area is divided into three sections: Dictionaries, Conditions, and Results. The Dictionaries section is active, and the MDM dictionary is selected in the left-hand navigation pane. The Dictionary Attributes page for the MDM dictionary is displayed, showing a list of attributes with their internal names and descriptions. A red box highlights the 'Dictionary Attributes' link in the top navigation bar, and another red box highlights the 'MDM' entry in the left-hand navigation pane.

Dictionary Attributes

Name	Internal Name	Description
<input type="checkbox"/> DeviceCompliantStatus	compliant_status	Compliant status of device on MDM
<input type="checkbox"/> DeviceRegisterStatus	register_status	Status of device registration on MDM
<input type="checkbox"/> DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
<input type="checkbox"/> IMEI	imei	IMEI
<input type="checkbox"/> JailBrokenStatus	jail_broken	Is device jail broken
<input type="checkbox"/> Manufacturer	manufacturer	Manufacturer name
<input type="checkbox"/> MDMServerReachable	MDMServerReachable	MDM server reachability
<input type="checkbox"/> Model	model	Device model
<input type="checkbox"/> OsVersion	os_version	Device Operating System
<input type="checkbox"/> PhoneNumber	phone_number	Phone number
<input type="checkbox"/> PinLockStatus	pin_lock_on	Device Pin lock status
<input type="checkbox"/> SerialNumber	serial_number	Device serial number

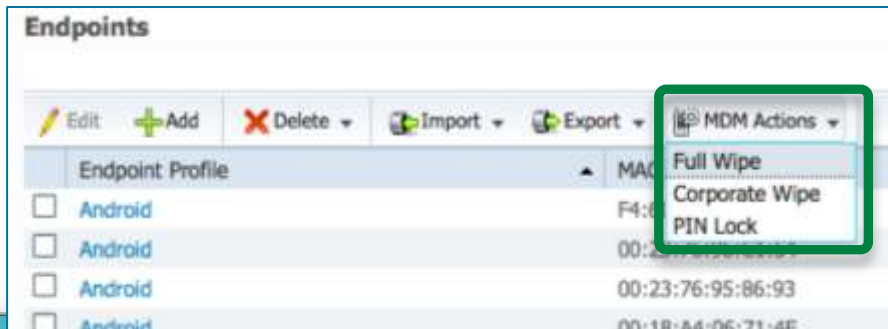
MDM Integration

Remediation

- User / Administrator can issue remote actions (Example: remote wiping the device)

MyDevices Portal

ISE Endpoints Directory



Options

- Edit
- Reinstate
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

MDM Onboarding

Authorization Profile

- Same MDM Redirect used for both:
 - Registration with MDM Server
 - Compliance and Remediation with MDM Server policy
- Redirect ACL must allow access to MDM Server and remediation resources

Remediation may include access to Apple App Store and Google Play (Android) to access MDM agents

MDM Redirect is a
Common Task under Web
Redirection

▼ Common Tasks

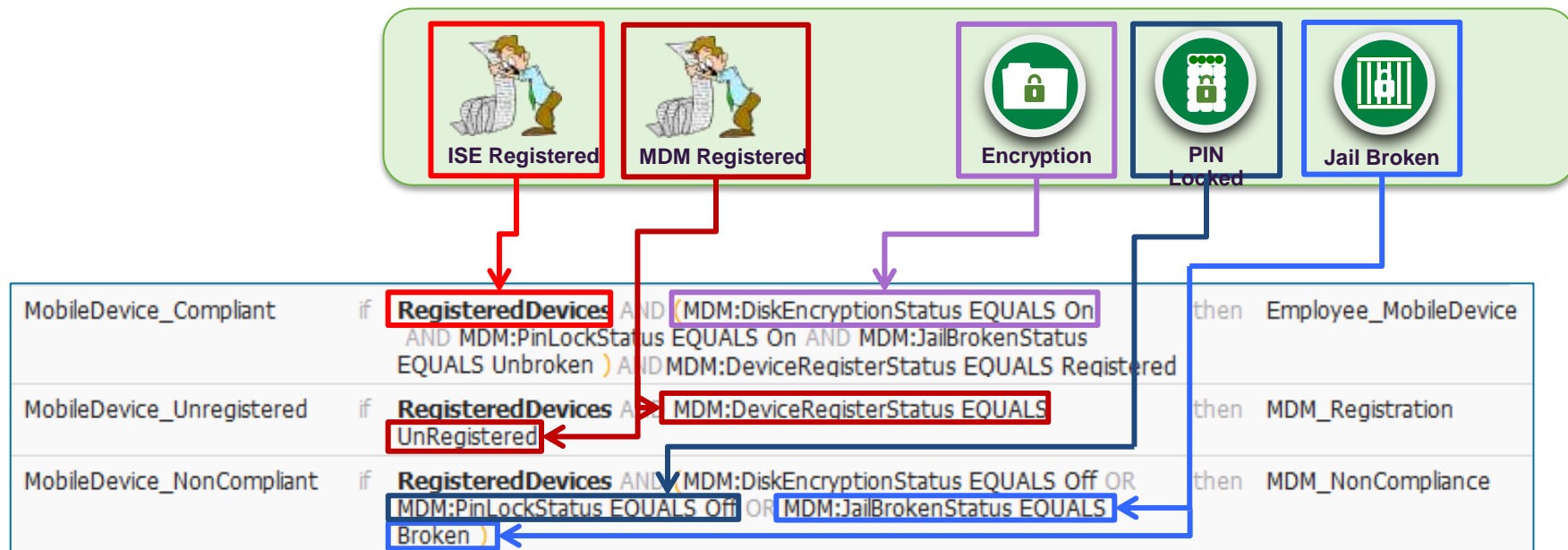
- ☒ Web Redirection (CWA, DRW, MDM, NSP, Posture)

MDM Redirect	▼
Centralized Web Auth	
Device Registration Web Auth	
MDM Redirect	
Native Supplicant Provision	
Posture Discovery	

ACL

MDM Authorization Policy

Registration and Compliance



MDM API

Display MDM Server Connection Info

- First URL to try when troubleshooting to verify MDM server connection, info, and API credentials: https://<MDM_Server>/ciscoise/mdminfo

```
- <ise_api>
  <name>mdminfo</name>
  <api_version>1</api_version>
  <api_path>/ciscoise/mdm/api</api_path>
  <redirect_url>https://mi.cts.local/mifs/c/d/clientdownload.html</redirect_url>
  <query_max_size>5000</query_max_size>
  <messaging_support>true</messaging_support>
  <vendor>MobileIron</vendor>
  <product_name>Mobile Device Manager</product_name>
  <product_version>VSP 5.8.0 Build 204 (Branch portland-vsp-release)</product_version>
</ise_api>
```

Path for MDM API calls

URL used for MDM client registration

Demo video



DEMO video

- Video

Agenda

- Einführung / The New Security Model

- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- Cisco CyberThreat Defense
- Content Security Update

Gennemgang
Gennemgang

- Q & A

Alle

Agenda

- Introduction / The New Security Model

- **ASA-CX Next Generation FW**
- ASA-CX Next Generation FW

Gennemgang
Demo

Pause – 10 min

- ISE 1.2 Gennemgang
- ISE 1.2 MDM integration

Demo / video

Pause – 10 min

- **Cisco CyberThreat Defense**
- Content Security Update

Gennemgang
Gennemgang

- Q & A

Alle



Cisco Cyber threat Defense solution

Brian Hansen
Systems Engineer Security

Tech update D. 19. Nov. 2013

Agenda

Threat landscape

Introduction to Cyber Threat Defense solution

Cisco Cyber Threat Defense solution

Summary



Market Dynamics

Mobility



Threat



Cloud



Megatrends Require an Innovative Approach to Security

Threat Evolution

Enterprise
Response

Anti-virus
(host-based)

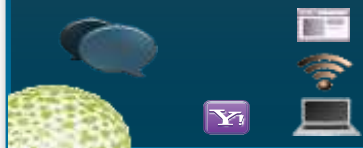
IDS/IPS
(network perimeter)

Reputation (global) &
Sandboxing

Intelligence & Analytics
(cloud)

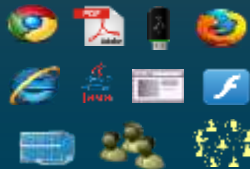
Threat
Landscape

WORMS



2000

SPYWARE /
ROOTKITS



2005

APT's
CYBERWARE



2010

INCREASED ATTACK
SURFACE (MOBILITY &
CLOUD)



Tomorrow

Changing Threat Landscape

Counter-Measures Are Less Effective

1,114,399

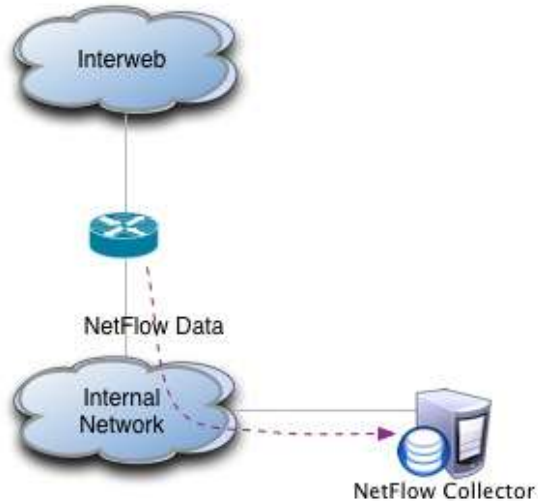
websites compromised
per second



Cisco Cyber Threat Defense

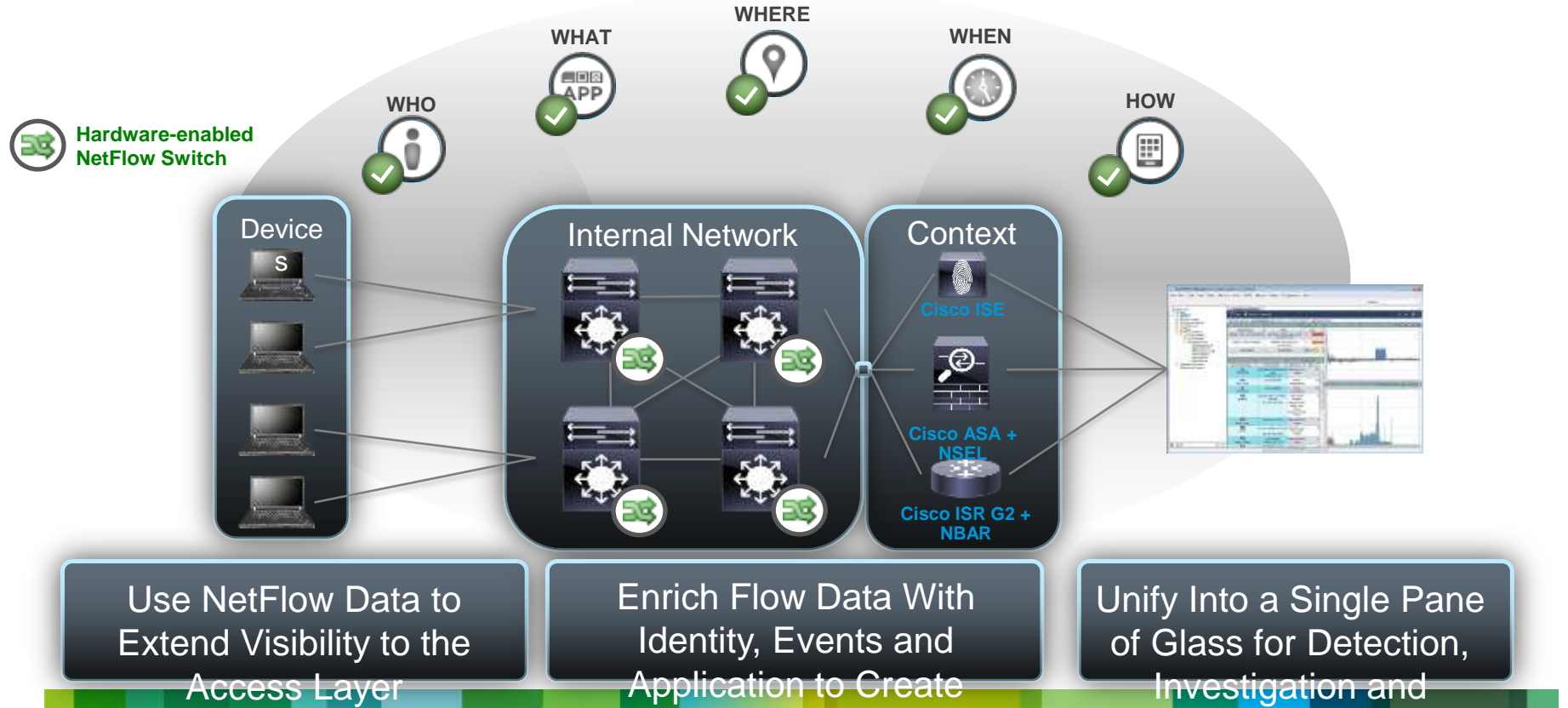


NetFlow: The Key Enabling Technology

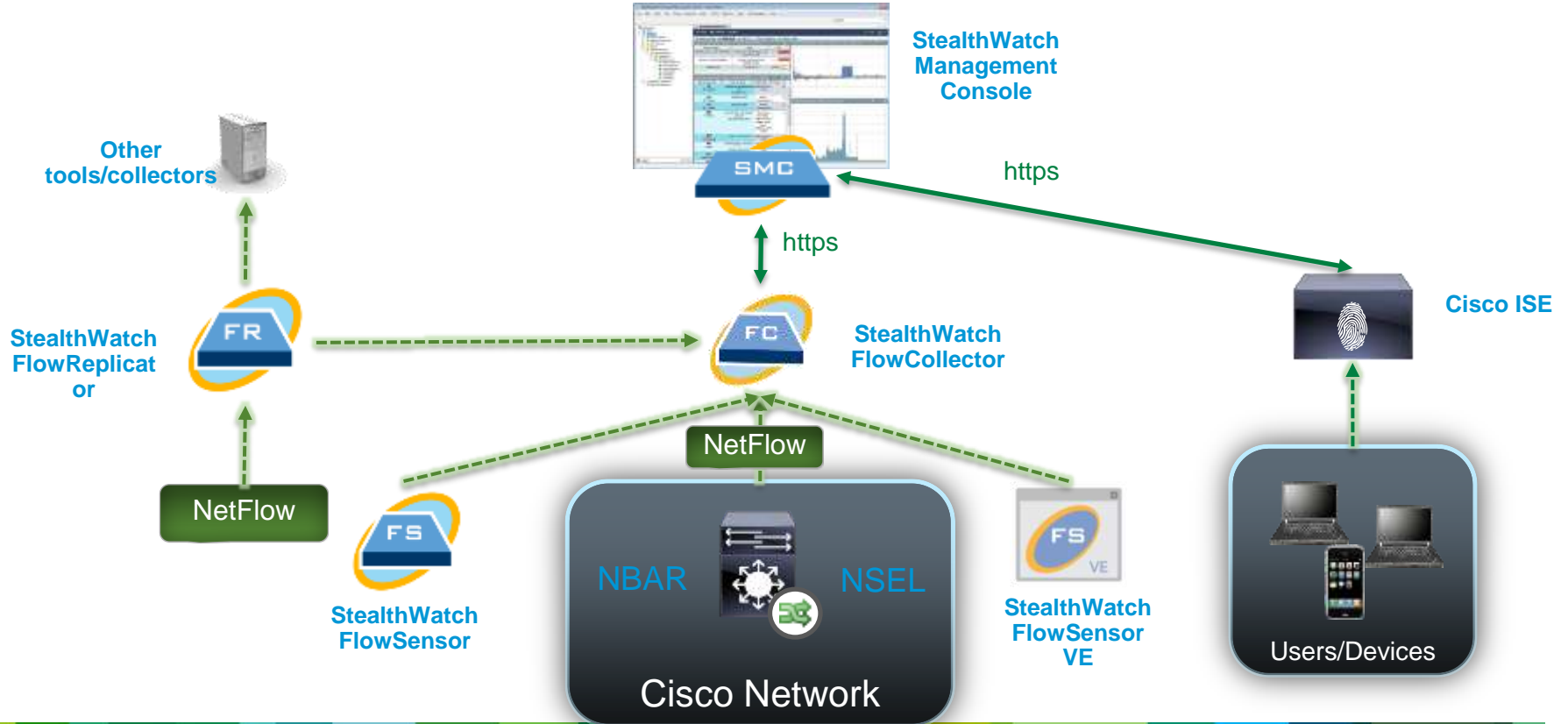


Usage →	<ul style="list-style-type: none">• Packet count• Byte count	<ul style="list-style-type: none">• Source IP address• Destination IP address	← From/To
Time →	<ul style="list-style-type: none">• Start sysUpTime• End sysUpTime	<ul style="list-style-type: none">• Source TCP/UDP port• Destination TCP/UDP port	← Application
Port utilization →	<ul style="list-style-type: none">• Input ifIndex• Output ifIndex	<ul style="list-style-type: none">• Next hop address• Source AS number• Dest. AS number• Source prefix mask• Dest. prefix mask	← Routing and peering
QoS →	<ul style="list-style-type: none">• Type of Service• TCP flags• Protocol		

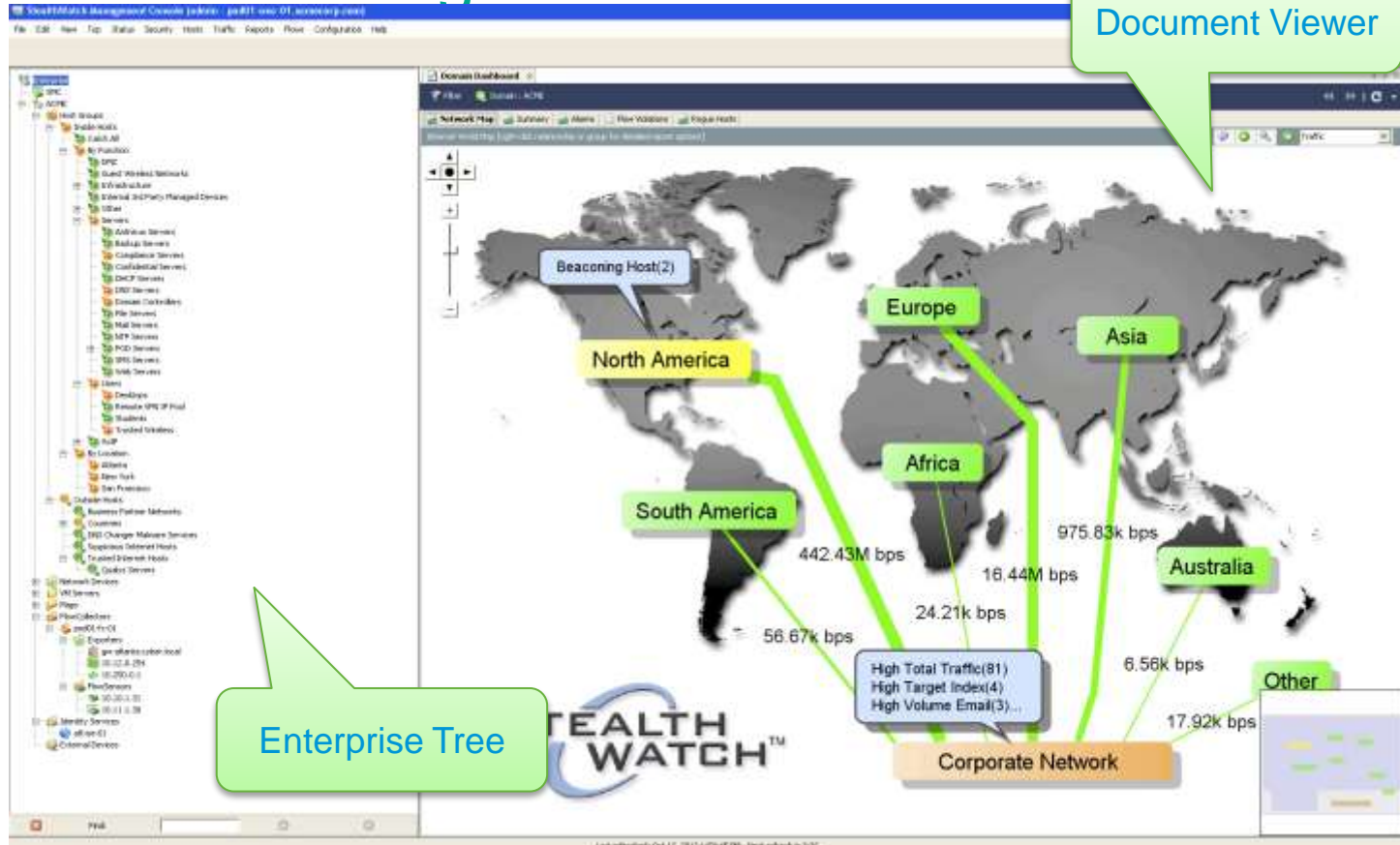
Leverage the Network for Threat Defense



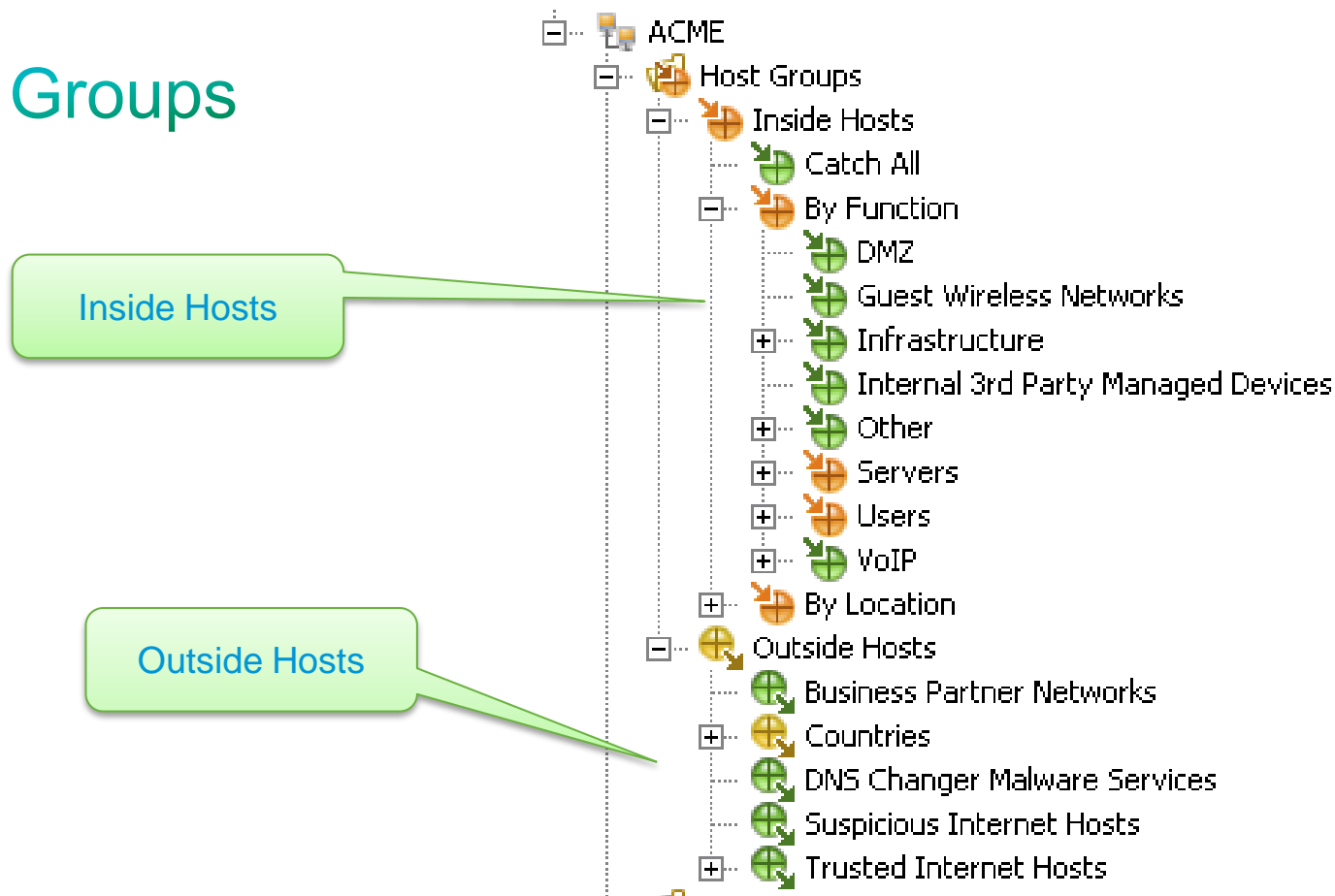
Cyber Threat Defense Solution Components



Stealthwatch Management Console



Host Groups



Drilling into a single flow yields a plethora of information

Using the Cisco Cyber Threat Defense Solution

➤ The Cisco Cyber Threat Defense Solution provides the necessary visibility and tools to facilitate:

1. Detecting suspect data loss
2. Identifying reconnaissance activity
3. Detecting command and control channels
4. Detecting internally spreading malware

➤ Refer to How-To Guides for guidance

<http://www.cisco.com/go/cybersecurity>

Detecting Suspect Data Loss

➤ Data is often exfiltrated over stealthy channels

- Hidden inside normal communication payloads

 - Payload padding

- Encrypted over standard ports

 - TCP port 80, TCP port 443, etc.

- Standard applications and protocols (ex. SFTP, HTTP, HTTPS)

➤ Detection requires deep visibility into user and device behaviour

- Historical data transfers—to establish patterns of communication

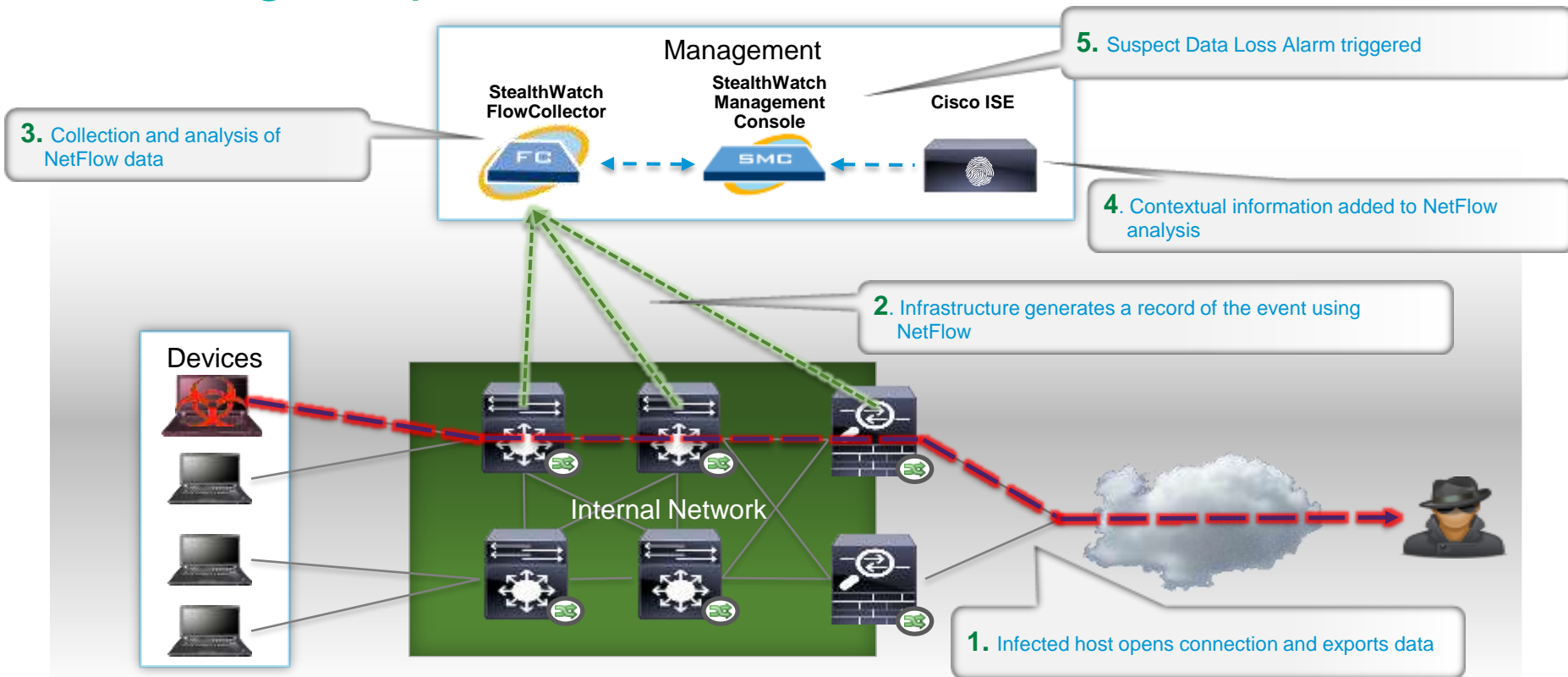
- Applications—is their behaviour “normal”?

- Time of day—why is Bob transferring data at 2:00 am?

- Countries—do we really do business with North Korea?

- Asymmetric traffic—a lot of data leaving the organization

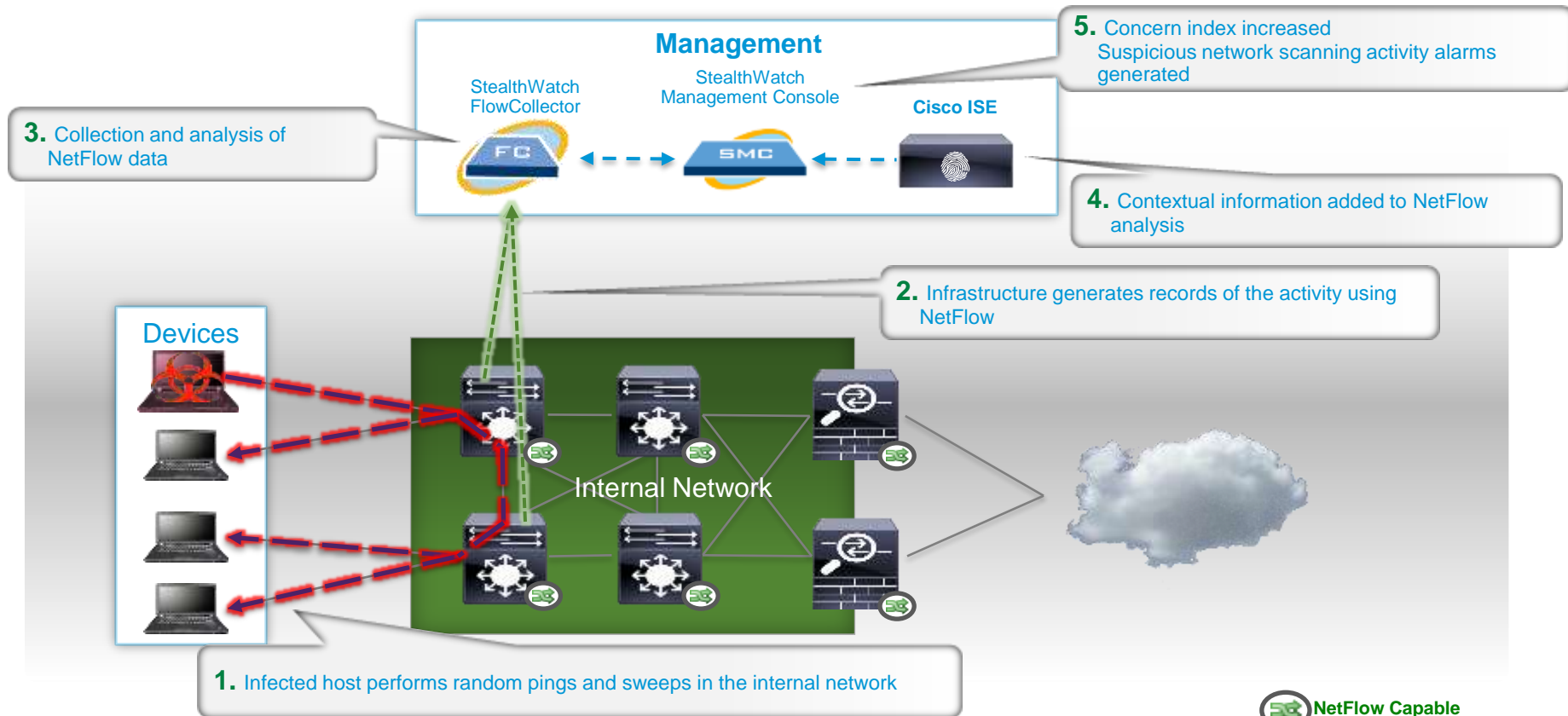
Detecting Suspect Data Loss



Identifying Reconnaissance Activity

- Having gained an operational presence on the network an attacker attempts to gain information about the network
- Often involves pings, sweeps and port scans as the attacker attempts to discover devices and services on the network
- Some of this activity may be low and slow, requiring a long history of flow data to detect
- This activity will often violate baseline behaviour of an individual
 - Increased DNS queries
 - Pings directed at the subnet
 - Port scanning
 - More ...
- Pervasive visibility throughout the network, at multiple levels (access, distribution, core) improves the ability to detect

Identifying Reconnaissance Activity



Detecting Command and Control

➤ Infections “phone home” over stealthy channels

- Standard protocols (ex. HTTP)

- Encrypted over standard ports (ex. 80, 443)

- Initiated from inside to bypass firewall

- Long and slow

- More ...

➤ Visibility of historical user behaviour required for detection

- Countries

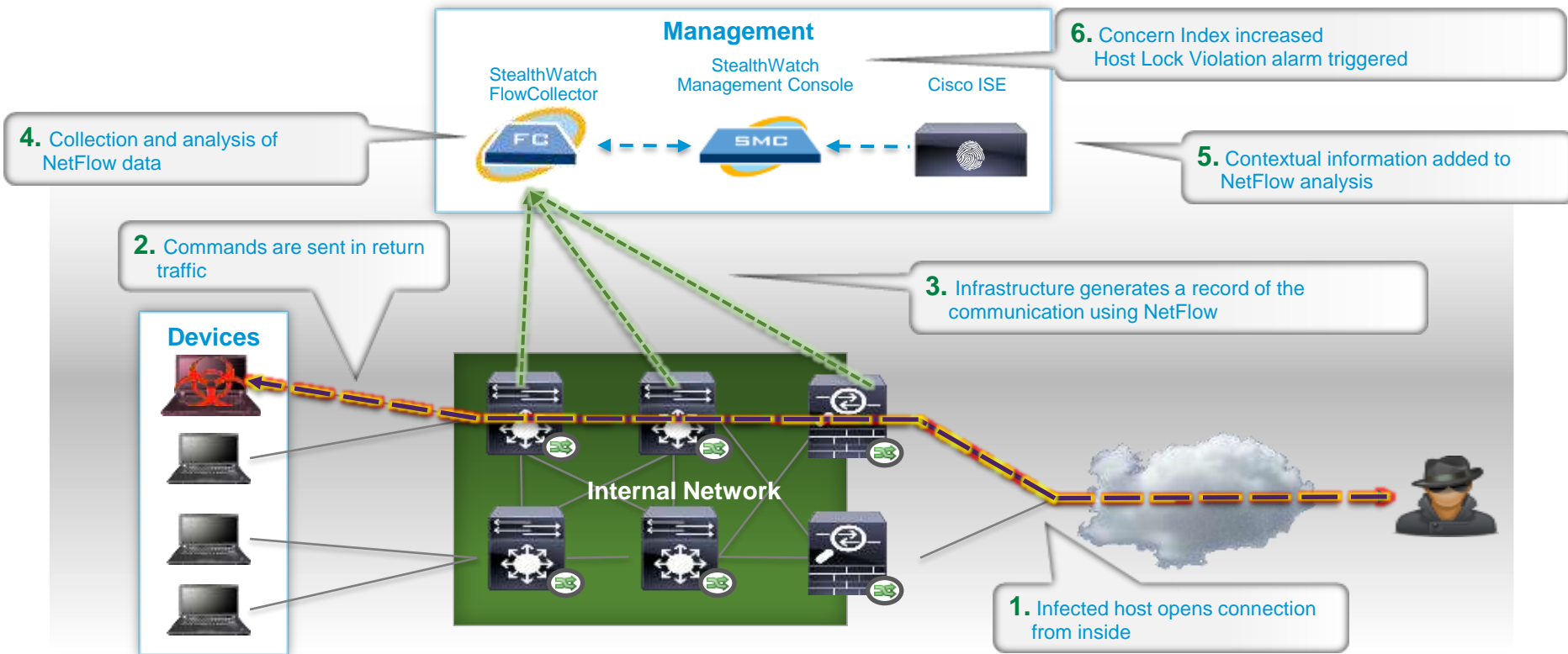
- Applications

- Uploads/Downloads

- Time of day

- More

Detecting Command and Control



 **NetFlow Capable**

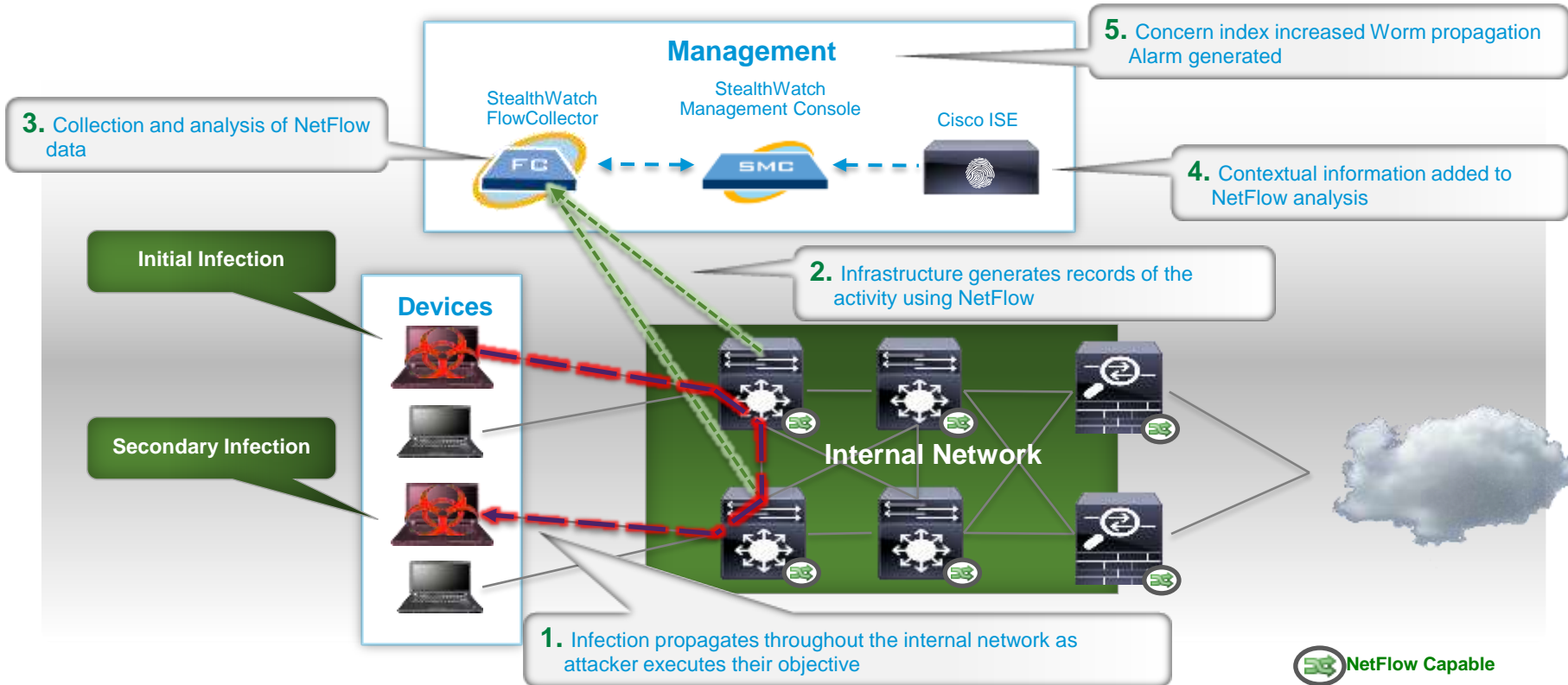
Detecting Internally Spreading Malware

- Once instantiated on the network malware can spread laterally

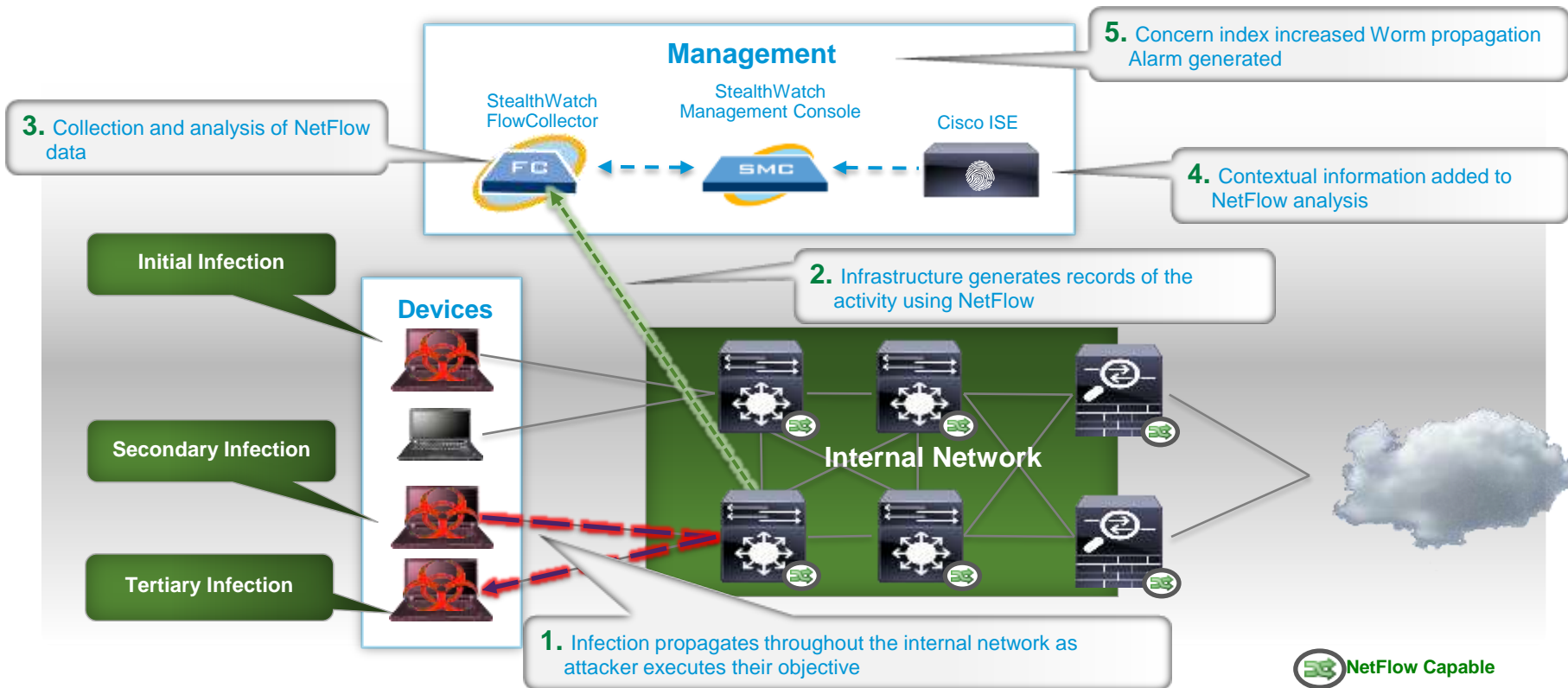
Ex. Stuxnet

- Lateral spread in access, distribution and core go undetected using “traditional” perimeter detection and mitigation measures
- Attackers will strategically/intelligently control the spread of their infections:
 - Selecting target devices (ex. Data centre)
 - Selecting target individuals (ex. CFO)
 - Selecting attack speed (ex. Fast and noisy or low and slow)
 - More ...
- Visibility of user/device level flows over long period of time required for detection

Detecting Internally Spreading Malware



Detecting Internally Spreading Malware

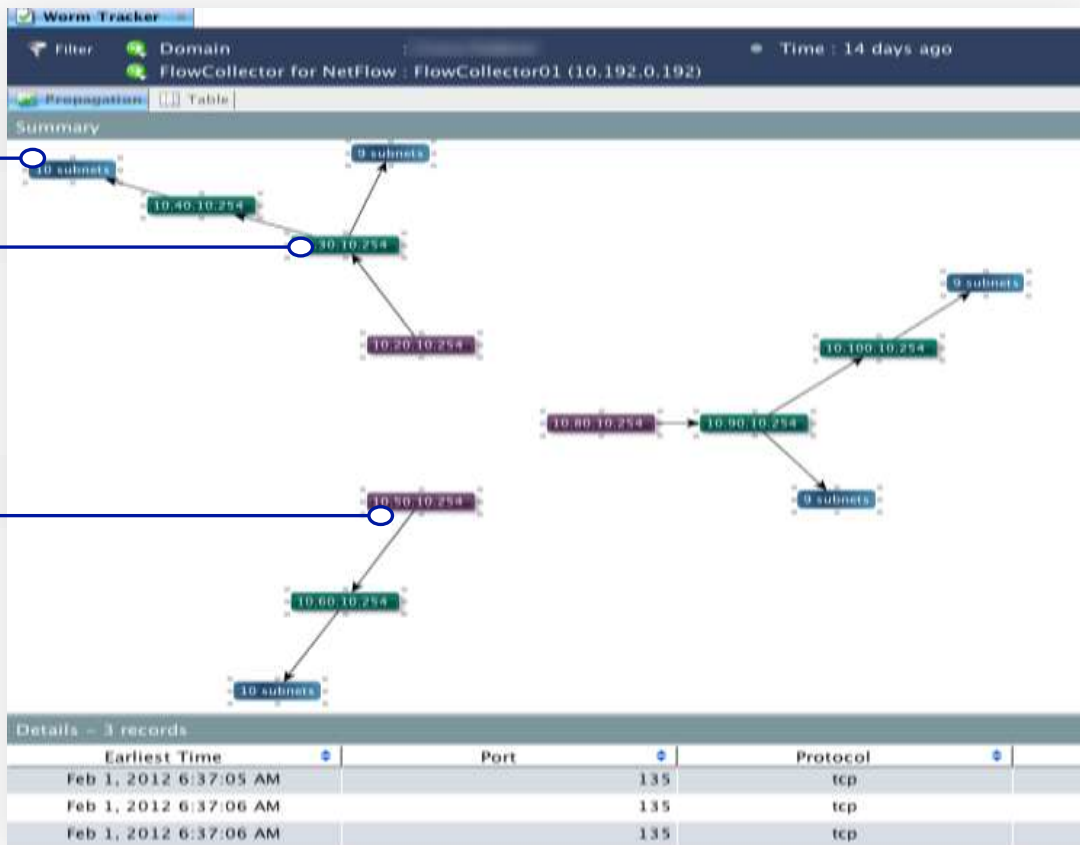


Infection Tracking

Tertiary Infection

Secondary Infection

Initial Infection



Summary

Threat Defense Solution

➤ The Cisco Cyber Threat Defense Solution provides the necessary visibility and tools to facilitate:

1. Detecting suspect data loss
2. Identifying reconnaissance activity
3. Detecting command and control channels
4. Detecting internally spreading malware

➤ Refer to How-To Guides for guidance

<http://www.cisco.com/go/cybersecurity>

