



*LET'S
BUILD
TOMORROW
TODAY*

Deploying Next-Generation Firewall with ASA and Firepower Services

BRKSEC-2028

Jeff Fanelli

Technical Solutions Architect – jefanell@cisco.com

Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

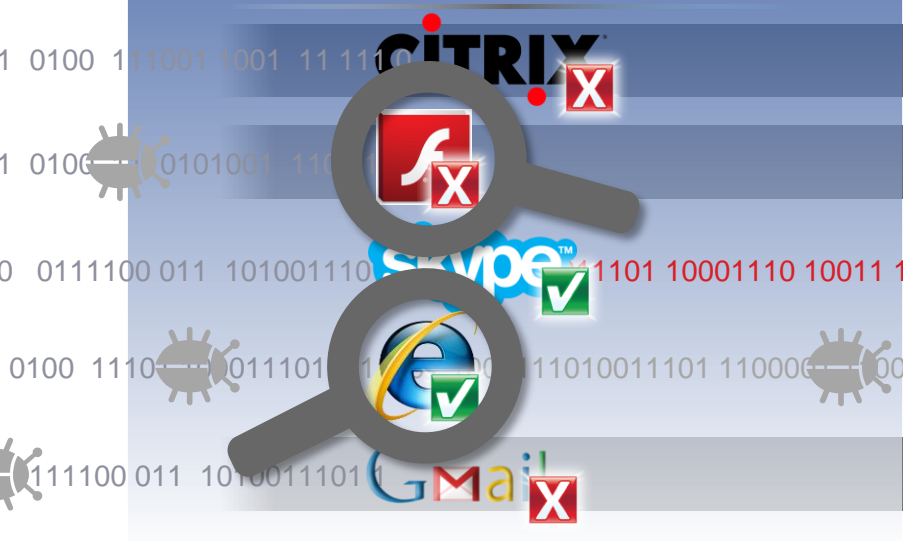
Management and Eventing (“logging”)

The Challenges Come from Every Direction



The Problem with Legacy Next-Generation Firewalls

Focus on the Apps

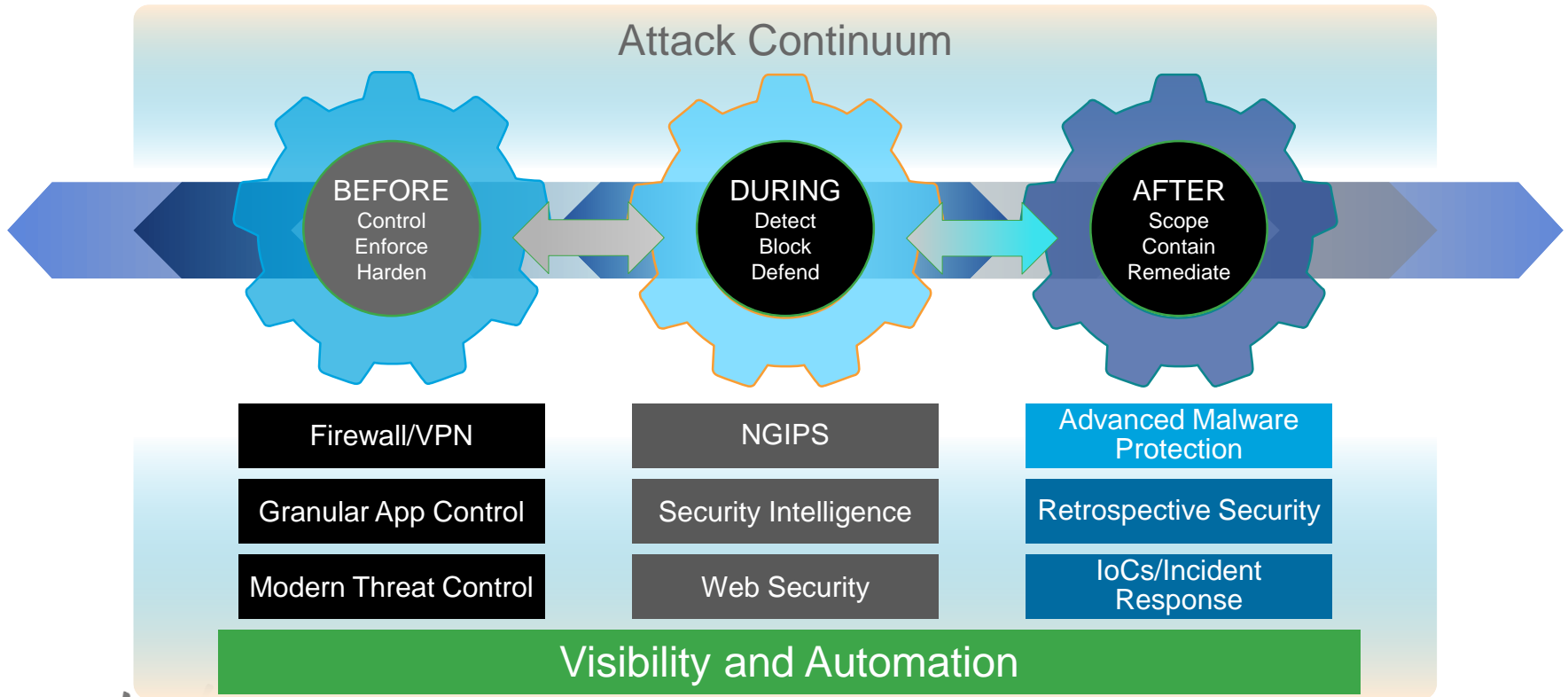


But miss the threat...



Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.

Integrated Threat Defense Across the Attack Continuum



Superior Integrated and Multilayered Protection



- ▶ Cisco ASA is world's most widely deployed, enterprise-class stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced malware protection

Cisco ASA with FirePOWER Services

Base Hardware and Software

New ASA 5585-X Bundle SKUs with FirePOWER Services Module

New ASA 5500-X SKUs running FirePOWER Services Software

FirePOWER Services Spare Module/Blade for ASA 5585-X Series

FirePOWER Services Software

Hardware includes Application Visibility and Control (AVC)

Security Subscription Services

- IPS, URL, Advanced Malware Protection (AMP) Subscription Services

- One- Three- and Five Year Term Options

Management

FireSIGHT Management Centre (HW Appliance or Virtual)

Cisco Security Manager (CSM) or ASDM

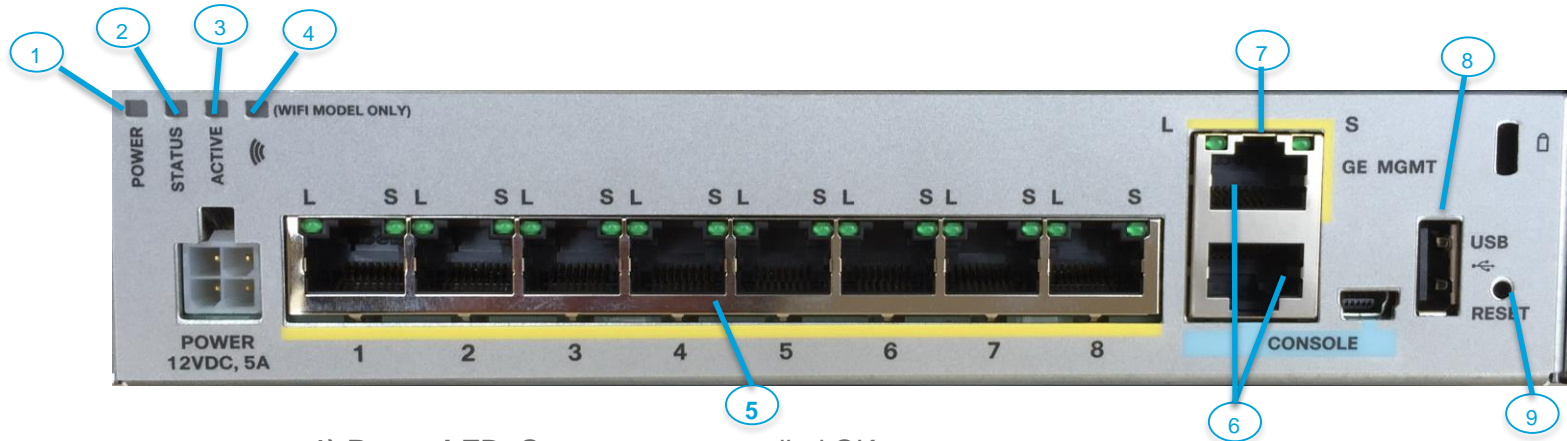
Support

SmartNET

Software Application Support plus Upgrades

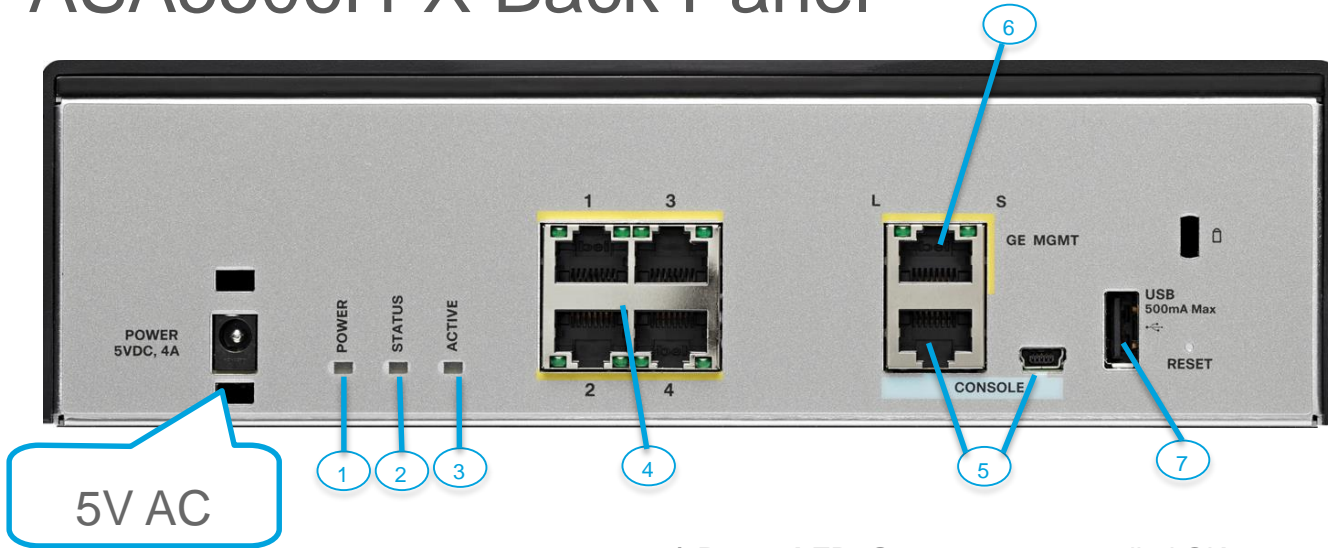


5506/5506W Panel



- 1) **Power LED:** Green -> power applied OK
- 2) **Status LED:** Green blinking -> system is booting up
Green solid -> successful boot
Orange -> error during boot-up
- 3) **Active LED:** Green -> unit is Active in failover pair
Orange -> unit is Standby in failover pair
Off -> not part of a failover pair
- 4) **WLAN Module** – not lit for 5506/Supported in the 5506W
- 5) **GE ports:** Left-side LED Green -> link. Right-side LED blinking -> network activity
- 6) **Console Ports:** RJ-45 and mini-USB Connector. If mini-USB is connected, RJ-45 becomes disconnected
- 7) **GE Management Port**
- 8) **USB port for external storage** – shows up as disk1
- 9) **Reset Pin**

ASA5506H-X Back Panel



Operating
Temperature

-20 to 60°C

- 1) **Power LED:** Green -> power applied OK
- 2) **Status LED:** Green blinking -> system is booting up
Green solid -> successful boot
Orange -> error during boot-up
- 3) **Active LED:** Green -> unit is Active in failover pair
Orange -> unit is Standby in failover pair
Off -> not part of a failover pair
- 4) **GE ports:** Left-side LED Green -> link. Right-side LED blinking -> network activity
- 5) **Console Ports:** RJ-45 and mini-USB Connector.
- 6) **GE Management Port**
- 7) **USB port for external storage** – shows up as disk19)

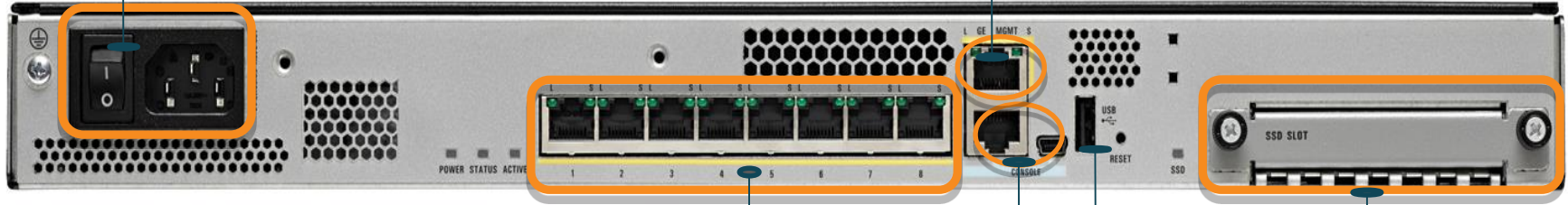
Cisco *live!*

ASA5508-X/5516-X Back Panel



Fixed Power Supply

Dedicated Mgmt Port (1GE)



USB Port

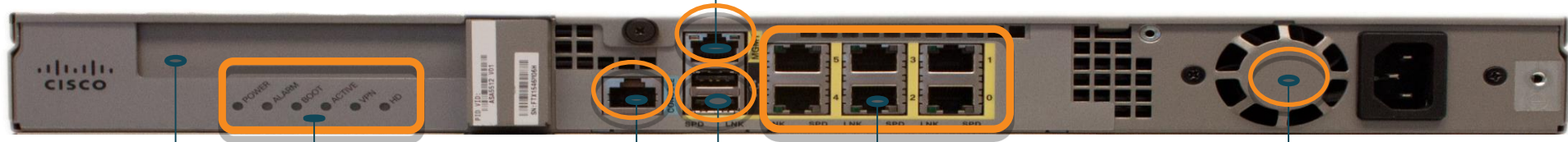
Serial Console
RJ45/USB

SSD

8x GE Ethernet ports

ASA5512-X & 5515-X Back Panel

Dedicated Mgmt Port (1GE)



Status LED's

I/O Expansion Slot

Serial Console

USB Port

6 x 1GE Cu Ports

Fixed Power Supply

ASA5525-X & 5545-X / 5555-X Back Panel



Status LED's

Serial Console

8 x 1GE Cu Ports

Fixed Power Supply

I/O Expansion Slot

USB Port

Dedicated Mgmt Port (1GE)



Status LED's

Serial Console

8 x 1GE Cu Ports

Redundant Hot Swappable PSU

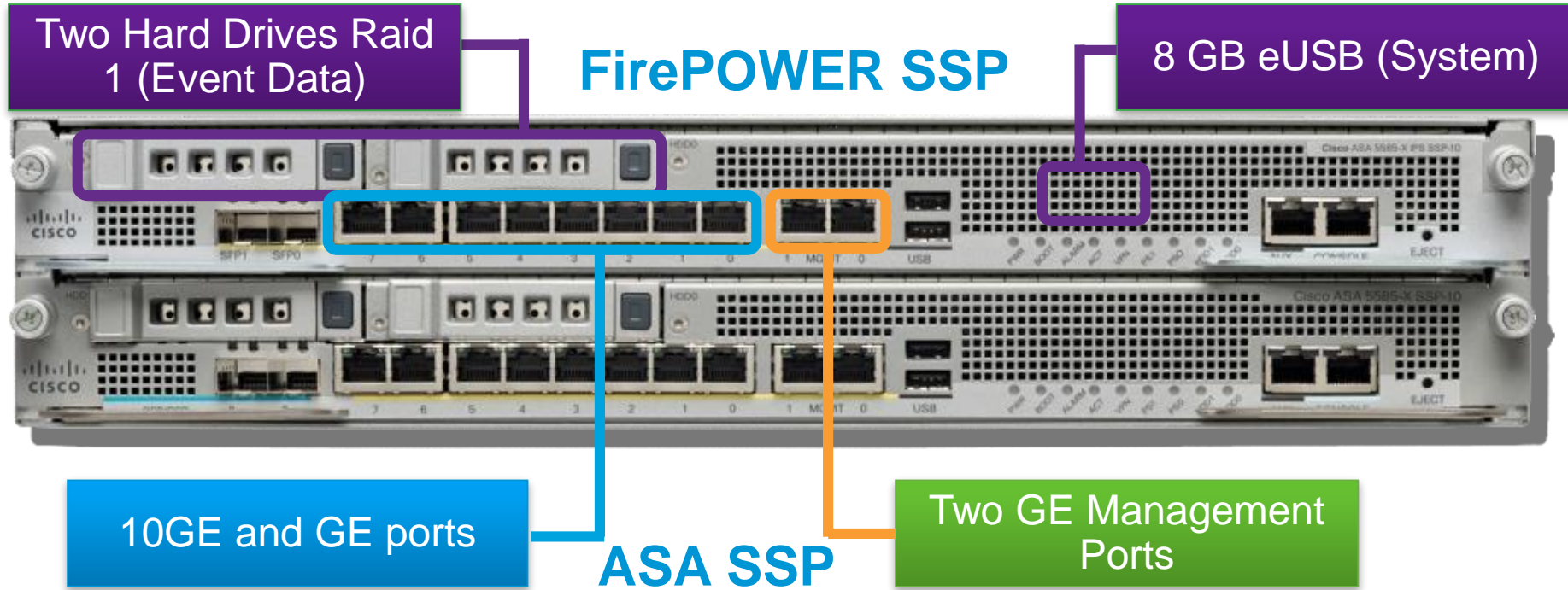
I/O Expansion Slot

USB Port

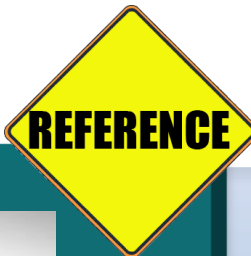
Cisco *live!*

What Platforms Support FirePOWER Hardware Module

- 5585-X + FirePOWER module in top slot – Hardware Module



Desktop 5506-X/5506W-X



Parameters	Value
CPU	Multi-core
RAM	4 GB
Accelerator	Yes
Ports	8x GE data ports, 1 Management Port with 10/100/1000 Base-T
Console Port	RJ45, Mini USB
USB Port	Type 'A' supports 2.0
Memory	64 GB mSata
Cooling	Convection
Power	AC external, No DC



7.92" x 8.92" x 1.73"

What Platforms Support FirePOWER Services as a Software Module?

Maximum AVC and IPS throughput

125 Mbps NGFW
50K Connections
5,000 CPS



ASA 5506-X

250Mbps NGFW
100K Connections
10,000 CPS



ASA 5508-X

150 Mbps NGFW
100K Connections
10,000 CPS



ASA 5512-X

250Mbps NGFW
250K Connections
15,000 CPS



ASA 5515-X

600Mbps NGFW
250K Connections
20,000 CPS



ASA 5516-X

650Mbps NGFW
500K Connections
20,000 CPS



ASA 5525-X

1 Gbps NGFW
750K Connections
30,000 CPS



ASA 5545-X

1.25 Gbps NGFW
1 M Connections
50,000 CPS



ASA 5555-X

Branch Locations

Small/Medium Internet Edge

Cisco *live!*

What Platforms Support FP Hardware Module?

Maximum AVC and IPS throughput



ASA 5585-SSP10

2 Gbps NGFW
500K Connections
40,000 CPS

Campus / Data Centre



ASA 5585-SSP20

3.5 Gbps NGFW
1 M Connections
75,000 CPS



ASA 5585-SSP40

6 Gbps NGFW
1.8 M Connections
120,000 CPS

Enterprise Internet Edge



ASA 5585-SSP60

10 Gbps NGFW
4 M Connections
160,000 CPS

FirePOWER Services for ASA: Sizing Guidance

440 byte HTTP Transactional test in Mbps

IPS uses Balanced Profile, AVC uses Network Discovery: Applications

Model	5516-X	5525-X	5545-X	5555-X	5585-10	5585-20	5585-40	5585-60
FirePOWER IPS <i>or</i> AVC	300	375	575	725	1200	2000	3500	6000
FirePOWER IPS + AVC	200	255	360	450	800	1200	2100	3500
FirePOWER IPS + AVC + AMP	150	205	310	340	550	850	1500	2300

As with all performance discussions, YOUR MILEAGE MAY VARY!!

FirePOWER Services for ASA: Mixed Blade Sizing

440 byte HTTP Transactional test in Mbps

IPS uses Balanced Profile, AVC uses Network Discovery: Applications

Model	5585-X 10/10	5585-X 10/40	5585-X 20/20	5585-X 20/60	5585-X 40/40	5585-X 60/60
FirePOWER IPS or AVC (1 Service)	1200	1200	2000	2000	3500	6000
FirePOWER IPS + AVC (2 Services)	800	1200	1200	2000	2100	3500
FirePOWER IPS+AVC+AMP (3 Services)	550	1200	850	2000	1500	2300

Cisco FireSIGHT Management Centre Appliance

* = Recommended!

						
	750	1500	2000*	3500	4000	Virtual *
Maximum devices managed*	10	35	70	150	300	Virtual FireSIGHT® Management Centre Up to 25 managed devices
Event storage	100 GB	125 GB	1.8 TB	400 GB	4.8/6.3 TB	ASA or FirePOWER appliances
Maximum network map (hosts/users)	2000/2000	50,000/ 50,000	150,000/ 150,000	300,000/ 300,000	600,000/ 600,000	Virtual FireSIGHT® Management for 2 or 10 ASA devices only! Not upgradeable FS-VMW-2-SW-K9 FS-VMW-10-SW-K9
Events per second (EPS)	2000	6000	12,000	10,000	20,000	

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



Management-interface Considerations on ASA5500-X

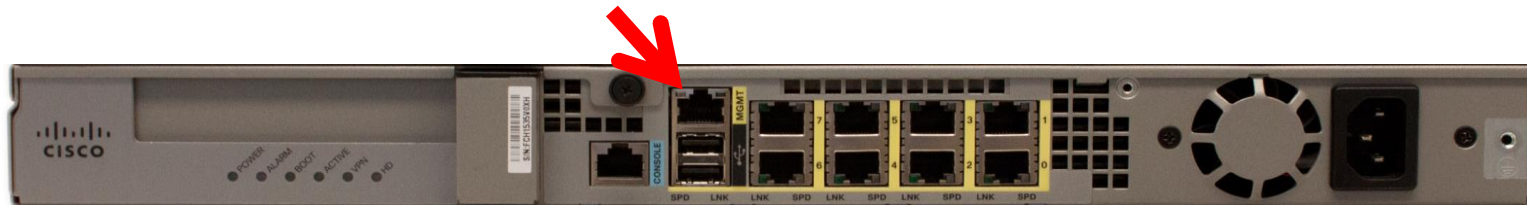
ASA FirePOWER Management Options

Two layers of management access: Initial Configuration and Policy Management

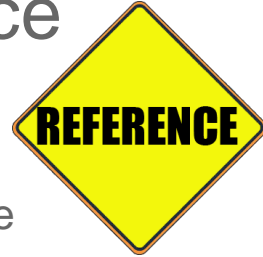
- **Initial Configuration*** must be done via the CLI (command line interface):
 - Session to the module over the ASA backplane on both **ASA5500-X** and **ASA5585-X**
- ASA FirePOWER **policy configuration** is done using **FireSIGHT Management Centre**.
- Traffic **redirection** to FirePOWER services is done from the **ASA** configuration.
- FirePOWER module IP address can be changed through **CLI** or **ASDM** Setup Wizard

ASA5500-X FirePOWER Management Interface

- One **shared** Management interface for ASA and FirePOWER module on ASA5500-X platform
- The FirePOWER module uses Management Interface for
 - all updates (base OS, OS upgrade packages)
 - all feature updates (rules, reputation data)
 - all Management Centre interaction (Mgmt, event-data)
- FireSIGHT policy management is performed through the management interface



ASA5500-X FirePOWER Management Interface Considerations (Cont.)

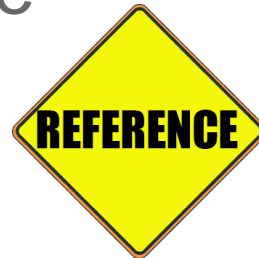


- **Management-only** ASA statement cannot be removed from the M0/0 interface
- If the ASA has a **nameif** assigned to the M0/0 interface, the FirePOWER module must have its management IP address in the same subnet
- You cannot route traffic through the M0/0 interface if **nameif** has been configured on that interface. *The ASA will drop this traffic.*
- If the ASA has no **nameif** assigned to the M0/0 interface, the FirePOWER module functions similarly to hardware module with a dedicated management interface



Communication from the FirePOWER module to external networks that pass through the ASA is inhibited if **nameif** is configured on the Management0/0 interface.

ASA5500-X FirePOWER Management Interface Considerations (Cont.)



- **Best practice is to separate ASA and FirePOWER management interfaces**
- **ASA managed in-band** (from the “inside” interface)
- **FirePOWER module managed via the Management Interface**
- No `nameif` assigned to the ASA M0/0 Interface
- ASA Inside Interface and FirePOWER Management can share **the same Layer 2 domain and IP subnet**
- Access from the “inside” to the FirePOWER module through switch/router, without ASA involvement

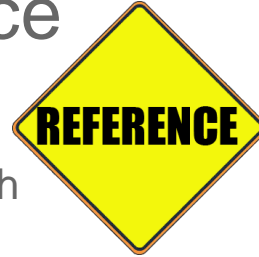


```
FirePOWER# show module SFR detail
Mgmt IP addr: 192.0.2.2
Mgmt Network Mask: 255.255.255.0
Mgmt Gateway:192.0.2.254
```

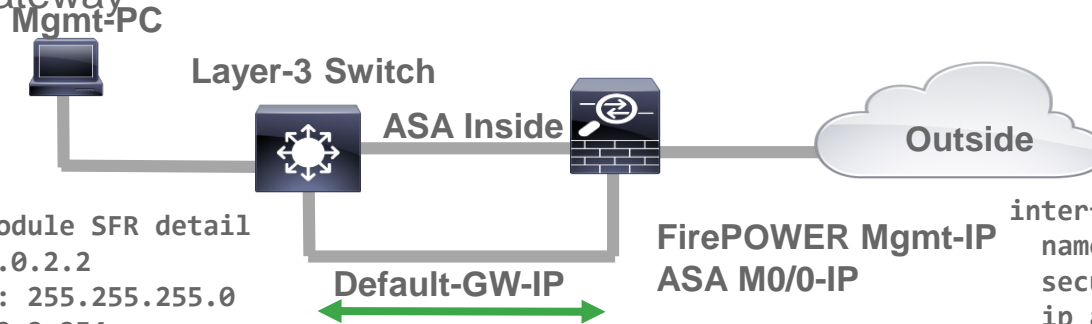
```
interface Management0/0
 no nameif
 security-level 0
 management-only
 no shutdown
```

```
Interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 192.0.2.254
```

ASA5500-X FirePOWER Management Interface Considerations (Cont.)



- Alternative: **Layer 3** Environment for ASA and FirePOWER Management both using M0/0
- **ASA will be managed via the M0/0** Management Interface
- **FirePOWER module will be managed via the M0/0** Management Interface
- ASA and FirePOWER Management share the same Layer 3 subnet
- **Default gateway** of FirePOWER module pointed to an **external router/switch**
- Route on ASA needed to route traffic to FirePOWER module management via the default gateway



```
FirePOWER# show module SFR detail
Mgmt IP addr: 192.0.2.2
Mgmt Network Mask: 255.255.255.0
Mgmt Gateway:192.0.2.254
```

```
FirePOWER Mgmt-IP
ASA M0/0-IP
interface Management0/0
 nameif management
 security-level 0
 ip address 192.0.2.1 255.255.255.0
 no shutdown
```

Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

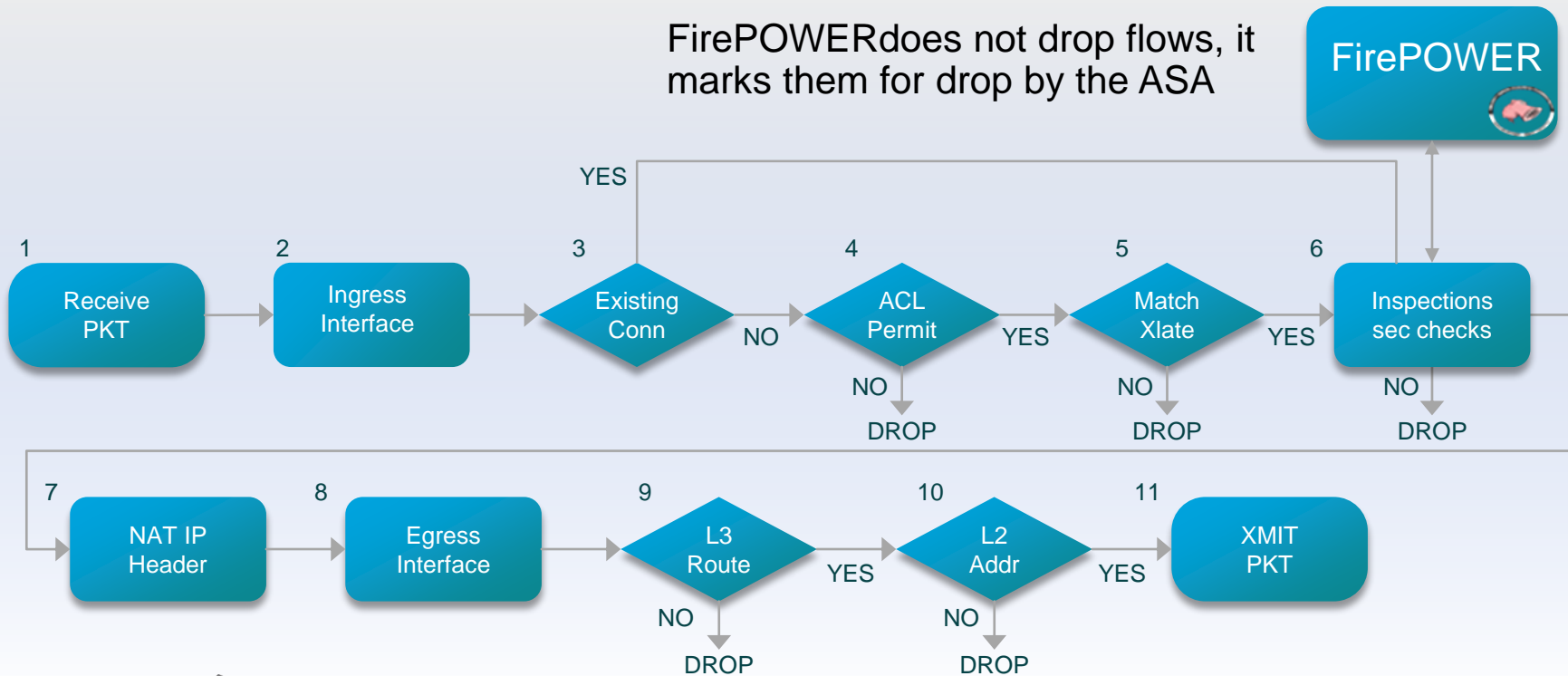
How to configure policies

Management and Eventing (“logging”)

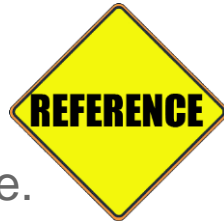
Packet Processing Order of Operations

- ASA Module processes all ingress packets against ACL, Connection tables, Normalisation and CBAC before traffic is forwarded to the FirePOWER Services module
- ASA provides flow normalisation and context-aware selection/filtering to the FirePOWER Services
- Clustered ASA provides flow symmetry and HA to the FirePOWER Services
- Packets and flows are not dropped by FirePOWER Services
 - Packets are marked for Drop or Drop with Reset and sent back to ASA
 - This allow the ASA to clear the connection from the state tables and send resets if needed

Detailed ASA SFR Packet Flow



FirePOWER Flow inspection Commands



Shows the NP rules created to send traffic to the ASA FirePOWER module.

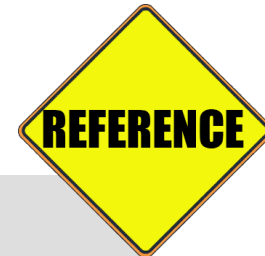
#Show asp table classify domain sfr

```
in id=0x7fffde41ccb0, priority=71, domain=sfr, deny=false
  hits=0, user_data=0x7fffde1153a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=mgmt, output_ifc=any
```

#Show conn

```
TCP outside 10.42.140.13:0 inside 192.168.42.108:41736, idle 0:00:33, bytes 0, flags Ti
TCP outside 10.42.140.12:0 inside 192.168.42.107:58106, idle 0:00:17, bytes 0, flags Ti
TCP outside 10.42.23.12:5060 inside 192.168.42.107:58105, idle 0:01:47, bytes 506817, flags UTxIOX
TCP outside 10.42.140.13:5060 inside 192.168.42.108:41736, idle 0:00:33, bytes 51460, flags UTxIOX
TCP outside 10.42.140.13:5060 inside 192.168.42.108:49141, idle 0:38:31, bytes 48815, flags UFTxIOX
```

FirePOWER Flow inspection Commands



Shows the reason for a frame drop

#Show asp drop

Frame drop:

Unsupported IP version (unsupported-ip-version)	44
No valid adjacency (no-adjacency)	265
No route to host (no-route)	1781
Reverse-path verify failed (rpf-violated)	148
Flow is denied by configured rule (acl-drop)	2312753
First TCP packet not SYN (tcp-not-syn)	4724
TCP failed 3 way handshake (tcp-3whs-failed)	165
TCP RST/FIN out of order (tcp-rstfin-ooo)	10633
TCP packet SEQ past window (tcp-seq-past-win)	2
TCP RST/SYN in window (tcp-rst-syn-in-win)	3
Slowpath security checks failed (sp-security-failed)	87431
Expired flow (flow-expired)	221
DNS Inspect id not matched (inspect-dns-id-not-matched)	1
SFR Module requested drop (sfr-request)	89
FP L2 rule drop (l2_acl)	3898959
Interface is down (interface-down)	651
Dropped pending packets in a closed socket (np-socket-closed)	293
NAT failed (nat-xlate-failed)	580

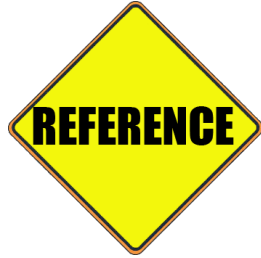
FirePOWER Flow inspection Commands



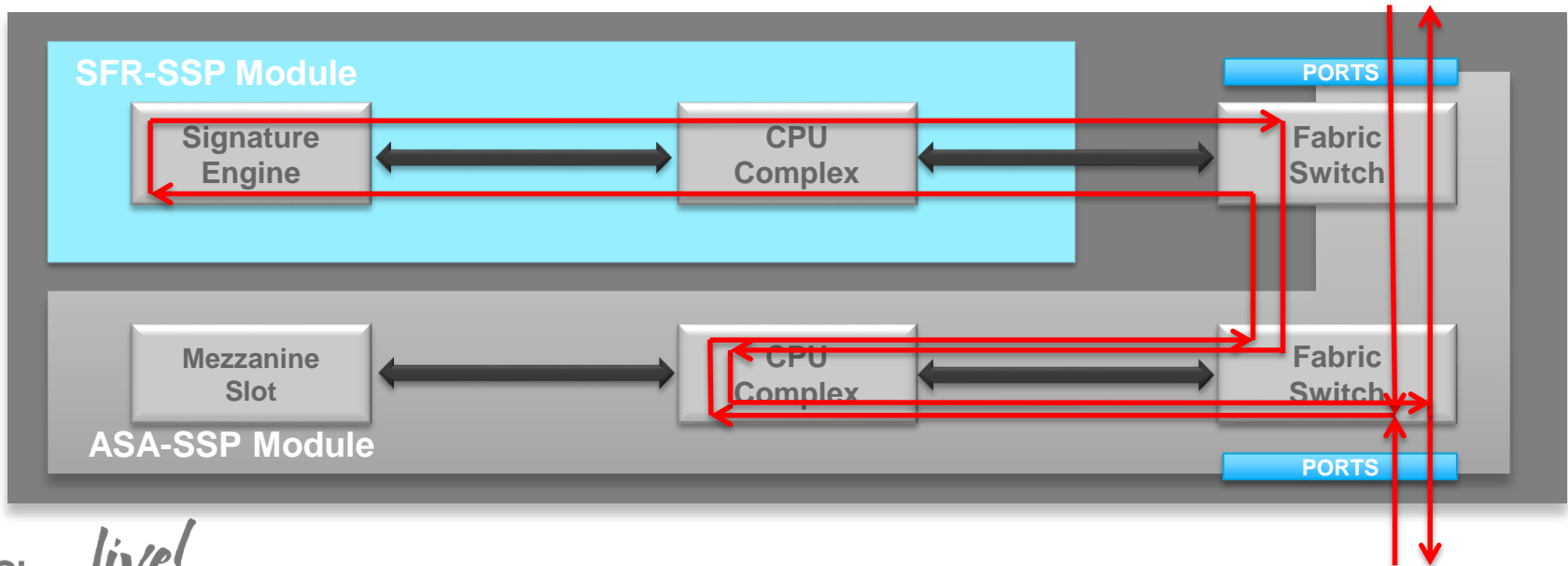
#Show asp drop

sfr-bad-tlv-received	—This occurs when ASA receives a packet from FirePOWER without a Policy ID TLV. This TLV must be present in non-control packets if it does not have the Standby/Active bit set in the actions field.
sfr-request	—The frame was requested to be dropped by FirePOWER due a policy on FirePOWER whereby FirePOWER would set the actions to Deny Source, Deny Destination, or Deny Pkt. If the frame should not have been dropped, review the policies on the module that are denying the flow.
sfr-fail-close	—The packet is dropped because the card is not up and the policy configured was 'fail-close' (rather than 'fail-open' which allows packets through even if the card was down). Check card status and attempt to restart services or reboot it.
sfr-bad-tlv-received	—This occurs when ASA receives a packet from FirePOWER without a Policy ID TLV. This TLV must be present in non-control packets if it does not have the Standby/Active bit set in the actions field.
sfr-request	—The frame was requested to be dropped by FirePOWER due a policy on FirePOWER whereby FirePOWER would set the actions to Deny Source, Deny Destination, or Deny Pkt. If the frame should not have been dropped, review the policies on the module that are denying the flow.
sfr-fail-close	—The packet is dropped because the card is not up and the policy configured was 'fail-close' (rather than 'fail-open' which allows packets through even if the card was down). Check card status and attempt to restart services or reboot it.
sfr-invalid-encap	—This counter is incremented when the security appliance receives a FirePOWER packet with invalid message header, and the packet is dropped.
sfr-bad-handle-received	—Received Bad flow handle in a packet from FirePOWER Module, thus dropping flow. This counter is incremented, flow and packet are dropped on ASA as the handle for FirePOWER flow has changed in flow duration.
sfr-rx-monitor-only	—This counter is incremented when the security appliance receives a FirePOWER packet when in monitor-only mode, and the packet is dropped.

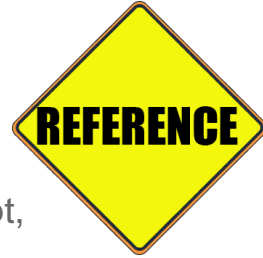
ASA 5585-X Data Port Utilization



- ASA SSP processes all ingress and egress packets
 - No packets are directly processed by FirePOWER module except for the FirePOWER management port.
 - ASA configures and controls the FirePOWER module data ports



Packet Flow Overview



- Packet flow between the solution components
 1. Ingress processing – inbound ACLs, IP defragmentation, TCP normalisation, TCP intercept, protocol inspection, clustering/HA traffic control, VPN decryption, etc.
 2. Sourcefire Services processing – URL filtering, AVC, NGIPS, AMP, etc.
 3. Egress processing – outbound ACLs, NAT, routing, VPN encryption, etc.
- Packets are redirected to the FirePOWER Services module using the Cisco ASA Modular Policy Framework (MPF)
 - MPF is a well known component of ASA architecture.
 - MPF supports fail-open, fail-closed and monitor only options
 - MPF class map, policy map and service policy determine which traffic is send to the FirePOWER Services module
- Example of MPF configuration to send all traffic to the FirePOWER Services module:

```
policy-map global_policy
  class class-default
    sfr fail-open
  service-policy global_policy global
```

Snort IPS

Snort Technology

- The Snort Engine's Basic Architecture
 - The sniffer
 - Preprocessors
 - The detection engine
 - The output and alerting module



Snort Technology

Preprocessors

Handle the task of presenting packets and packet data in a contextually relevant way to the detection engine.

For example: HTTP header seen on non-standard port

Packet fragment
reassembly

Maintaining TCP
state

TCP Stream
reassemble

Protocol
normalization



Snort Technology



Detection Engine:

Accepts the parsed, normalized and stream-reassembled network traffic for inspection against the rule base.

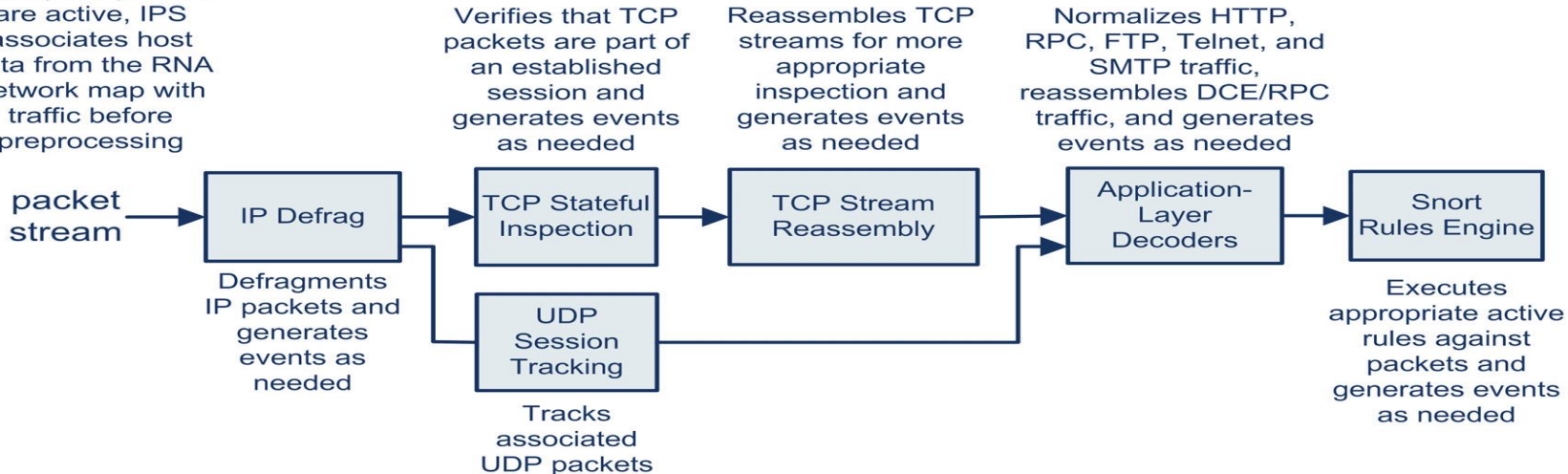
Rules Builder

Inspection against the built rules



Preprocessor Execution Order

If adaptive profiles are active, IPS associates host data from the RNA network map with traffic before preprocessing



URL Filtering

URL Filtering

- Block non-business-related sites by category, reputation, white/black lists.
- Based on user and user group, VLAN, source network or interface zones



URL Filtering

Editing Rule - Web Block List

The screenshot shows the configuration interface for a 'Web Block List' rule. At the top, the rule name is 'Web Block List', it is 'Enabled', and the action is 'Block'. Below this are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Services', 'URLs', 'Policy', 'Logging', and 'Comments'. The 'URLs' tab is active, showing a search bar and a list of categories and reputations. The 'Selected URLs' section on the right contains a list of categories with checkboxes and a scroll bar. At the bottom right, there are 'Save' and 'Cancel' buttons.

Name: Web Block List Enabled **Action:** Block

Categories and URLs

Search by name or value

- Any
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy
- CDNs
- Computer and Internet Info
- Computer and Internet Security

Reputations

- Any
- 5 - Well known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High risk

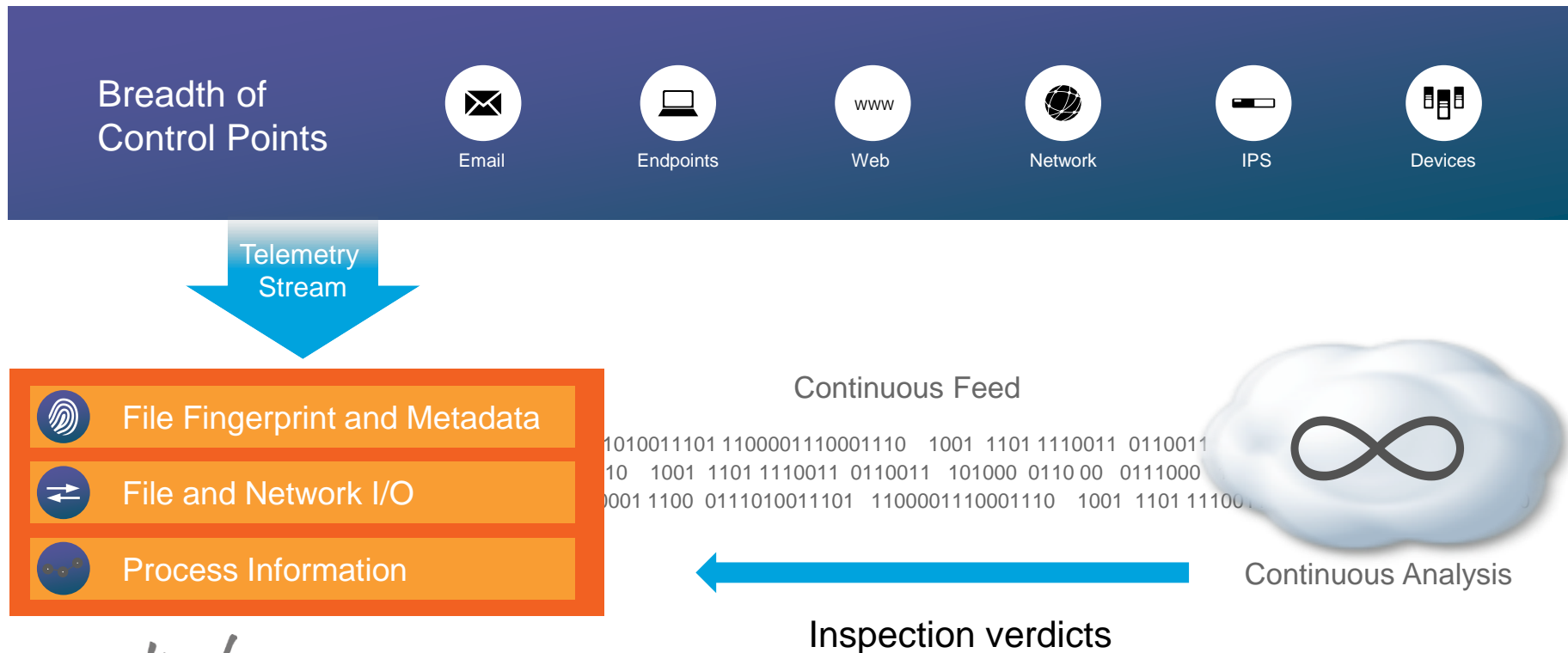
Selected URLs

- Adult and Pornography (Any Reputation)
- Bot Nets (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Gambling (Any Reputation)
- Keyloggers and Monitoring (Any Reputation)
- Malware Sites (Any Reputation)
- Marijuana (Any Reputation)
- Nudity (Any Reputation)
- Open HTTP Proxies (Any Reputation)
- Parked Domains (Any Reputation)
- Pay to Surf (Any Reputation)

Enter URL

Cisco Advanced Malware Protection

AMP Provides Continuous Retrospective Security



Retrospective Analysis: File Trajectory

Quickly Understand the Scope of Malware Problem



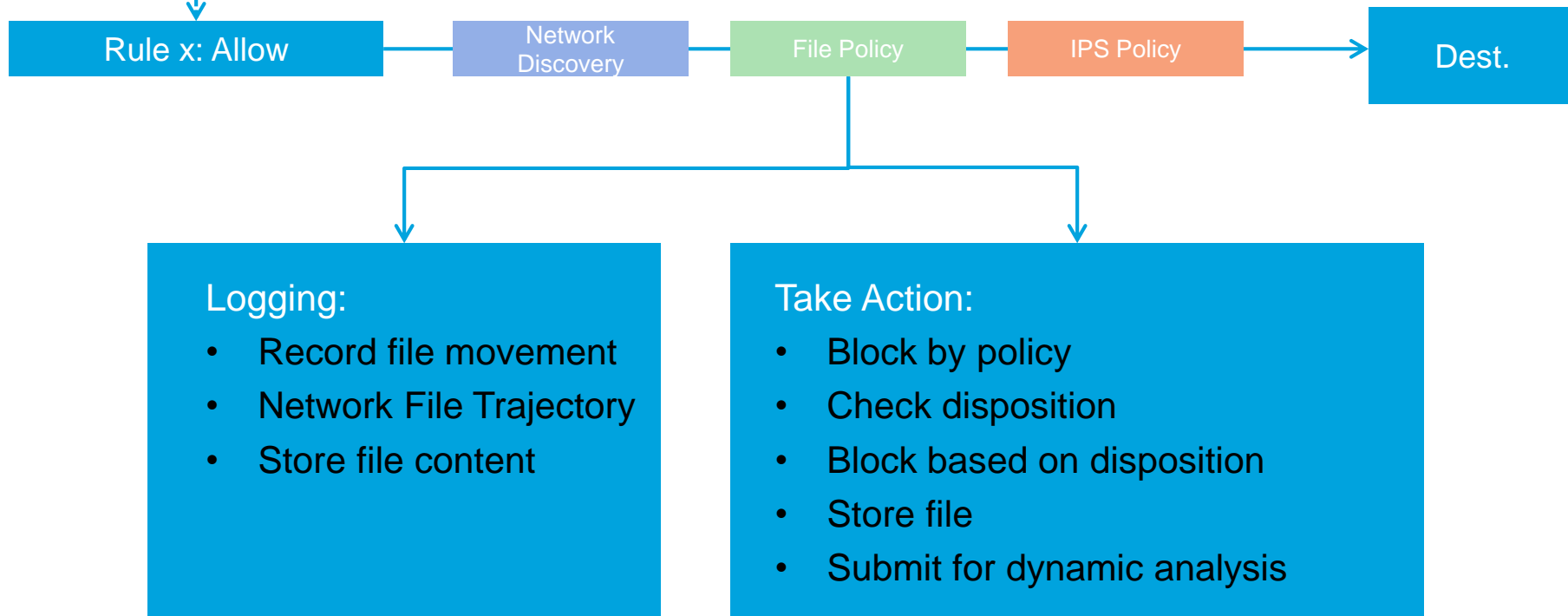
ASA with FirePOWER



Looks **ACROSS** the organisation and answers:

- What systems were infected?
- Who was infected first (“patient 0”) and when did it happen?
- What was the entry point?
- When did it happen?
- What else did it bring in?

Key File Policy Actions



Selection of file policy

Editing Rule - Run Inspection

Name

Enabled

[Move](#)

Action

IPS: Home IDS

Variables: Default Set

Files: Live 2015

Logging: connections, files: dc

Zones Networks VLAN Tags Users Applications Ports URLs

Inspection Logging Comments

Intrusion Policy

Variable Set

File Policy

Add File Rule

Application Protocol

Direction of Transfer

- Any
- HTTP
- SMTMP
- IMAP
- POP3
- FTP

File Type Categories

- Dynamic Analysis
- System files 2
- Graphics 0
- Encoded 0
- PDF files 1
- Executables 6
- Multimedia 2
- Office Documents 16
- Archive 17

Action

- Spero Analysis for MSEXE
- Dynamic Analysis
- Reset Connection

Store Files

- Malware
- Unknown
- Clean
- Custom

File Types

-
- All types in selected Categories
 - FLV (Flash video file)
 - SWF (Flash file)

Selected File Categories and Types

Add

Save

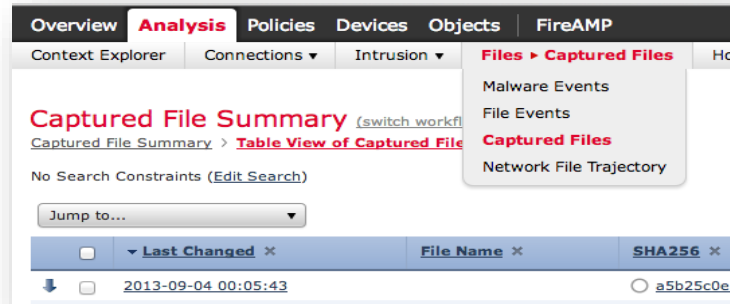
Cancel

File Policy Details

- You can have multiple file policies associated with an Access Control Policy
 - But only one per rule
- File policies can have multiple entries
 - Matched like access control, works down the list
- Archive Management
 - Actions can be taken on files within archives
 - Nested archives are inspected up to a defined depth
- File Carving
 - For dynamic analysis, you need full file content
 - To capture a file, it must be carved out of a stream

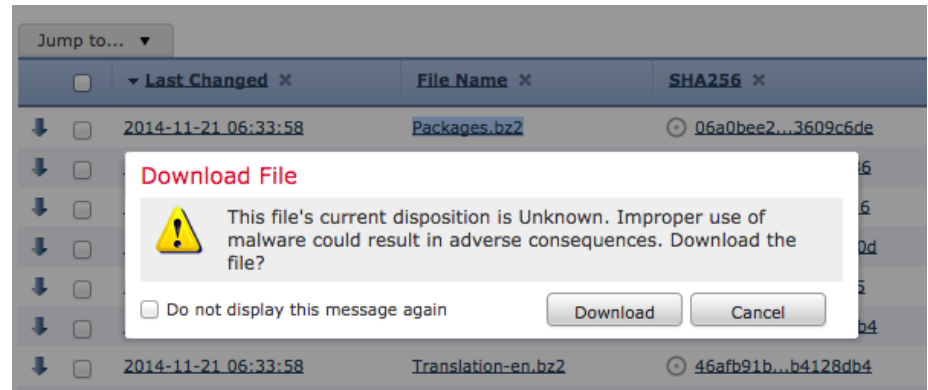
File Capture: Accessing Files #1

- Files can be downloaded from Event Table Views, Network File Trajectory, and the new 'Captured Files' table
- When a file download is requested, FireSIGHT MC looks for device(s) that may have the file stored
 - Multiple appliances may have seen the file
- The file is downloaded from the FirePOWER appliance on to the MC, processed (see next slide), and then a save dialog is presented to the user (or an error) E.g.
 - File Pruned
 - Device not reachable





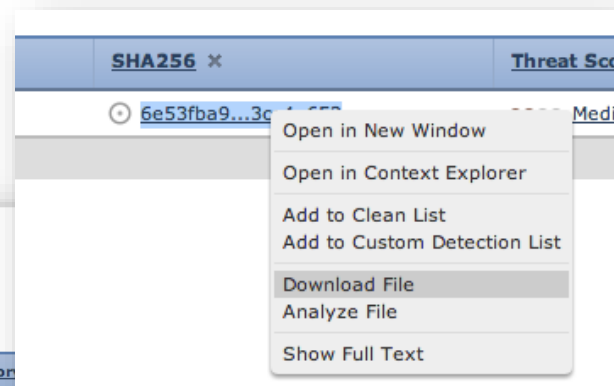
File Capture: Accessing Files #2

- To protect the user from accidental malware execution on download some file processing takes place
 - User is warned when downloading files with a malware, clean, or unknown disposition (different warnings for each)
 - Can be disabled via a “Don’t warn me again” checkbox
 - All files are zipped with a password by default: ‘infected’
 - Password can be changed, or disabled
 - ‘infected’ is an industry standard
 - Warnings, and ZIP password are per user
 - ZIP preference set in event view settings
- ***Working with Malware carries risk!***



Captured Files Table

- Shows all files captured or sent for analysis by the system
 - Threat Score  
 - Storage Status
 - Tip: A dot in the disposition icon = captured
 - Analysis Status (e.g. Pending)













Captured File Summary [\(switch workflow\)](#)

[Captured File Summary](#) > [Table View of Captured Files](#)

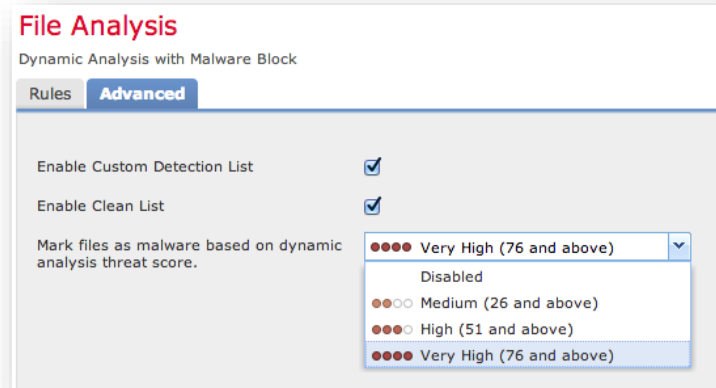
▶ Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

<input type="checkbox"/>	Last Changed	File Name	SHA256	Threat Score	Type	Category	Status
↓ <input type="checkbox"/>	2013-09-27 16:11:22	impapase.exe	 22ce59af...419dc635	 Medium	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-27 09:07:48	dripple.exe	 b3894034...28d4c502	 Very High	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-26 20:32:48	ovatolanceolate.exe	 2cc3816c...edce5f4c	 Low	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-25 15:57:48	servileness.exe	 087bd4cc...0b4f9405	 Very High	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-25 09:39:22	conclutination.exe	 3729934c...45f88ec8	 Very High	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-23 17:57:44	ophiouride.exe	 0594fcb2...e48534aa	 High	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-23 02:12:41	porule.exe	 72f5e68f...0b0f3429	 High	MSEXE	Executables	File Stored
↓ <input type="checkbox"/>	2013-09-13 17:44:14	opercula.exe	 b03a877c...b0370d02		MSEXE	Executables	File Stored Failure (Analysis Timeout)

Threat Score:

- Threat Score is a new rating of how likely a file is malicious after dynamic analysis is performed
 - Higher the number, higher the likelihood
- Files can be marked as malware based on this threat score value threshold (Very high, high, medium)
 - This threat score threshold can be found in File Policy / Advanced
 - Any file with a threat score above this threshold will be treated as malware in the customers deployment



Submitting files for analysis

How to get a threat score

- Files can be submitted for analysis via two methods
 - Manual: Right click action / button in Network File Trajectory
 - Requires that the file has been captured
 - File type support: MDB, FLV, XLS, DOC, PPT, PPTX, XLSX, DOCX, JAR, CAB, Office, New Office, EXE, WRI, SWF (always check documentation for full list)
 - Automatic: Submit based on File Policy and Access Control Policy
 - File type support: MSEXEX, DLL, SCR
 - Will not send known clean files, or known malware files with Threat Scores already calculated
 - Optimizes focus on potential new unknown malware
 - If the CSI Cloud already has a report on a file, it's not needed to be sent again
 - Optimizes focus on potential unknown malware

Dynamic Analysis: Process Overview

- File Detected on FirePOWER
- Calculates hashes
 - Saves a copy if policy dictates*

Hash metadata sent to CSI Cloud

- CSI Cloud Response: E.g.
- Disposition = Unknown
 - Threat Score = Unknown *

File is sent to Dynamic Analysis (if policy dictates)

- Dynamic analysis:*
- Analysis queue Status
 - Error Status
 - Threat Score

ASA / FirePOWER Appliances



1892y...skfhds

FireSIGHT MC



<optional proxy*>

1892y...skfhds

<optional proxy*>

Dynamic Analysis Service* (Files)

Disposition (Metadata / Hashes)

CSI Cloud

How Cisco AMP Works: Network File Trajectory

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type MSEXE

File Category [Executables](#)

Current Disposition Malware

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

10.4.10.183

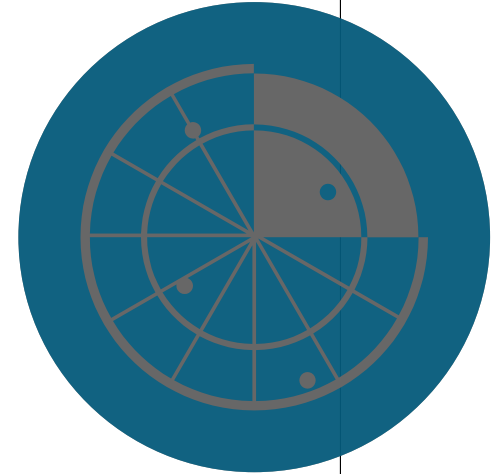
10.5.11.8

10.3.4.51

10.5.60.66

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable



Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type MSEXE

File Category Executables

Current Disposition Malware

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

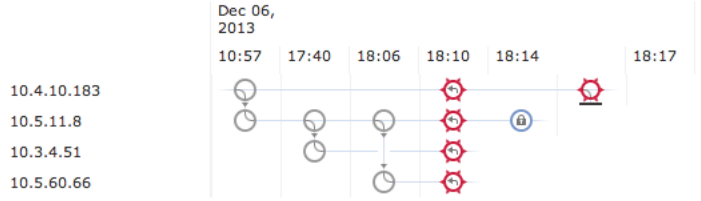
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File **SHA-256** 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

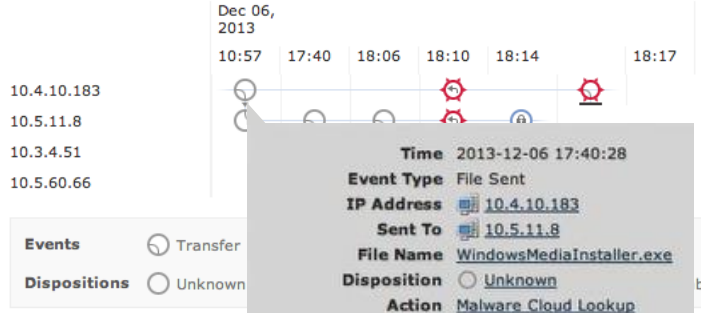
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Events

Time	Event Type	Source IP	Destination IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type MSEXE

File Category [Executables](#)

Current Disposition Malware

Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183

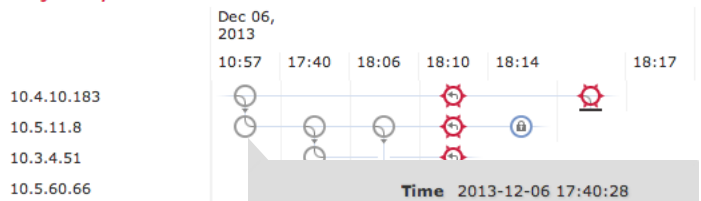
Last Seen 2013-12-06 18:17:27 on 10.4.10.183

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Time 2013-12-06 17:40:28

Event Type File Received

IP Address 10.5.11.8

Received From 10.4.10.183

File Name [WindowsMediaInstaller.exe](#)

Disposition Unknown

Action [Malware Cloud Lookup](#)

Application Protocol HTTP

Client Firefox

At 10:57, the unknown file is accessed from IP 10.4.10.183 to IP: 10.5.11.8

Events

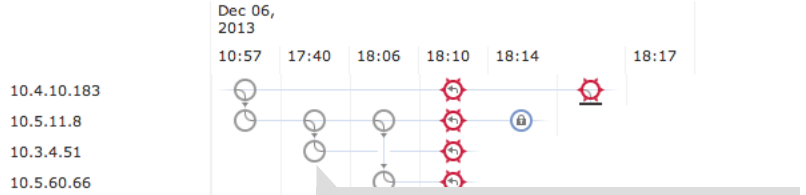
Time	Event	Local	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Unkn... Malware Cloud L... HTTP Firefox Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstalle...	Unkn... NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstalle...	Unkn... NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstalle...	Malwa...
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Malwa... Malware Block HTTP Firefox

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
 File Name [WindowsMediaInstaller.exe](#)
 File Type MSEXE
 File Category Executables
 Current Disposition Malware
 Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
 Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
 Event Count 7
 Seen On 4 hosts
 Seen On Breakdown 2 senders → 3 receivers

Trajectory



Time 2013-12-06 18:06:03
Event Type File Received
IP Address [10.3.4.51](#)
Received From [10.5.11.8](#)
File Name [WindowsMediaInstaller.exe](#)
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Events

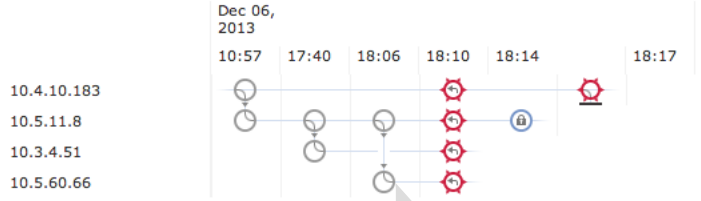
Time	Event Type	Source IP	Destination IP	File Name	Disposition	Application Protocol	Web Ap...	Description
2013-12-06 10:57:13	Retrospec...							
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Unkn...	Malware Cloud L...	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstalle...	Unkn...	NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstalle...	Unkn...	NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...							
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstalle...	Malwa...			
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Malwa...	Malware Block	Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
 File Name [WindowsMediaInstaller.exe](#)
 File Type MSEXE
 File Category Executables
 Current Disposition Malware
 Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
 Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
 Event Count 7
 Seen On 4 hosts
 Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block
 Dispositions Unknown Malware

Time 2013-12-06 18:10:03
Event Type File Received
IP Address [10.5.60.66](#)
Received From [10.5.11.8](#)
File Name [WindowsMediaInstaller.exe](#)
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Events

Time	Event Type	Source IP	Destination IP	File Name	Disposition	Action	Application Protocol	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...								Retrospective Event, Fri Dec 6 ...
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Unknown		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstalle...	Unknown		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstalle...	Unknown		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstalle...	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Malwa...	Malware Block	HTTP	Firefox	

Network File Trajectory for 0517f034...588e1374

File **SHA-256** 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

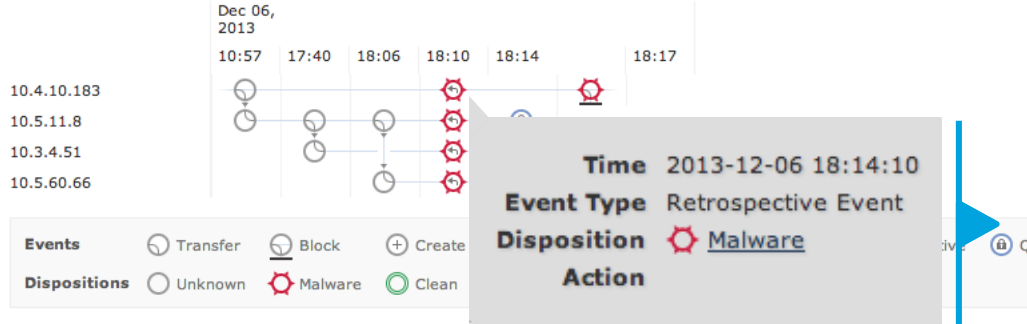
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events

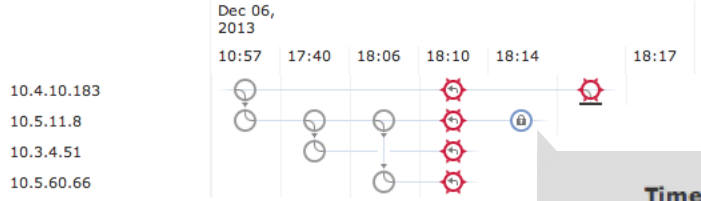
Time	Event Type	Sending IP	Receiving IP	File Name	Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...	
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn... Malware Cloud L...	HTTP Firefox Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...	NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...	NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...	
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...	
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa... Malware Block	HTTP Firefox

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
 File Name [WindowsMediaInstaller.exe](#)
 File Type MSEXE
 File Category Executables
 Current Disposition Malware
 Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183
 Last Seen 2013-12-06 18:17:27 on 10.4.10.183
 Event Count 7
 Seen On 4 hosts
 Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events: Transfer, Block, Create, Move
 Dispositions: Unknown, Malware, Clean, Custom

Time 2013-12-06 18:14:23
Event Type File Quarantined
IP Address 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action

At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Events

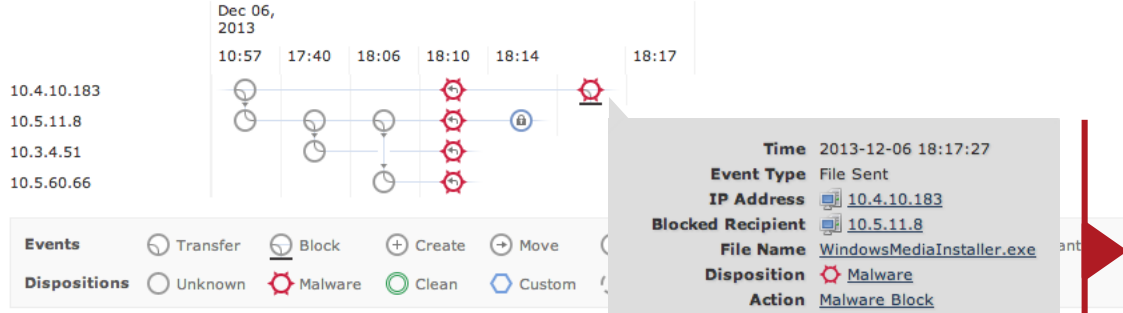
Time	Event Type	Sending IP	Receiving IP	File Name	Disposition	Action	Browser	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...			
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Unkn...	Malware Cloud L...	HTTP Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstalle...	Unkn...		NetBIOS-...	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstalle...	Unkn...		NetBIOS-...	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...			
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstalle...	Malwa...			
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Malwa...	Malware Block	HTTP Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
 File Name [WindowsMediaInstaller.exe](#)
 File Type MSEXE
 File Category [Executables](#)
 Current Disposition Malware
 Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
 Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
 Event Count 7
 Seen On 4 hosts
 Seen On Breakdown 2 senders → 3 receivers

Trajectory



8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognised and blocked.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disposition	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

AMP: File Based Malware Prevention



ASA with
FirePOWER
Services



Dedicated
FirePOWER
Appliance



Web & Email
Security
Appliances



Cloud Based
Web Security
& Hosted Email



Private
Cloud



PC /
MAC



Mobile



Virtual

Fire reputation and file
sandboxing

Continuous &
Zero-Day Detection

Advanced Analytics
And Correlation

Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

Management and Eventing (“logging”)

Functional Distribution of Features

URL Category/Reputation

NGIPS

Application Visibility and Control

Advanced Malware Protection

File Type filtering

File capture

FirePOWER Services

TCP Normalisation

TCP Intercept

IP Option Inspection

IP Fragmentation

Botnet Traffic Filter

NAT

Routing

ACL

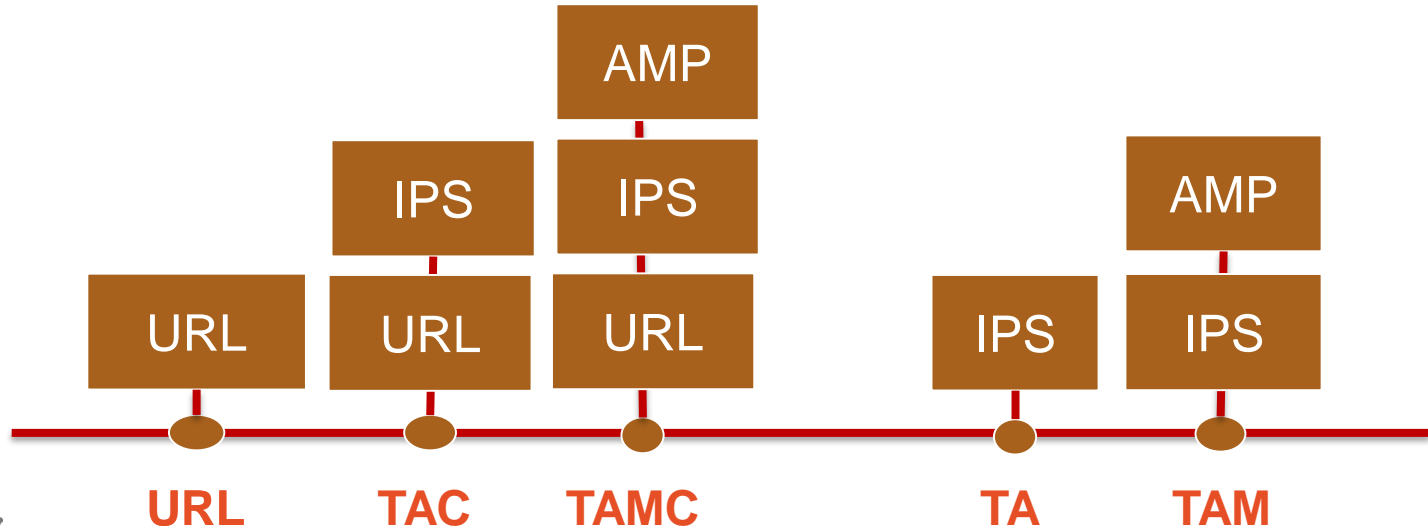
VPN Termination

Failover & Clustering

ASA

Licensing

- Five (5) feature license packages are available
- AVC is part of the default offering
- One (1), three (3) and five (5) year terms are available
- SMARTnet is ordered separately with the appliance



How to Add FirePOWER Services to an ASA-5500-X

- Purchase ASA5500X-SSD120=
 - Adds Solid State Disc drive to ASA platform
 - Two drives required for ASA-5545 / 5555 (mirror redundancy)
- Purchase \$0 ASA55xx-CTRL-LIC=
 - Adds perpetual “Protect and Control” license
- Purchase FS-VMW-x-SW-K9
 - FireSIGHT Management Centre Virtual Appliance
 - 2 and 10 device SKU’s can NOT be upgraded later
- Purchase additional licenses as needed (not required)
 - URL / IPS / AMP offered as 1, 3 or 5 year subscriptions

Agenda

Introduction to NGFW

Software Architecture

Licensing

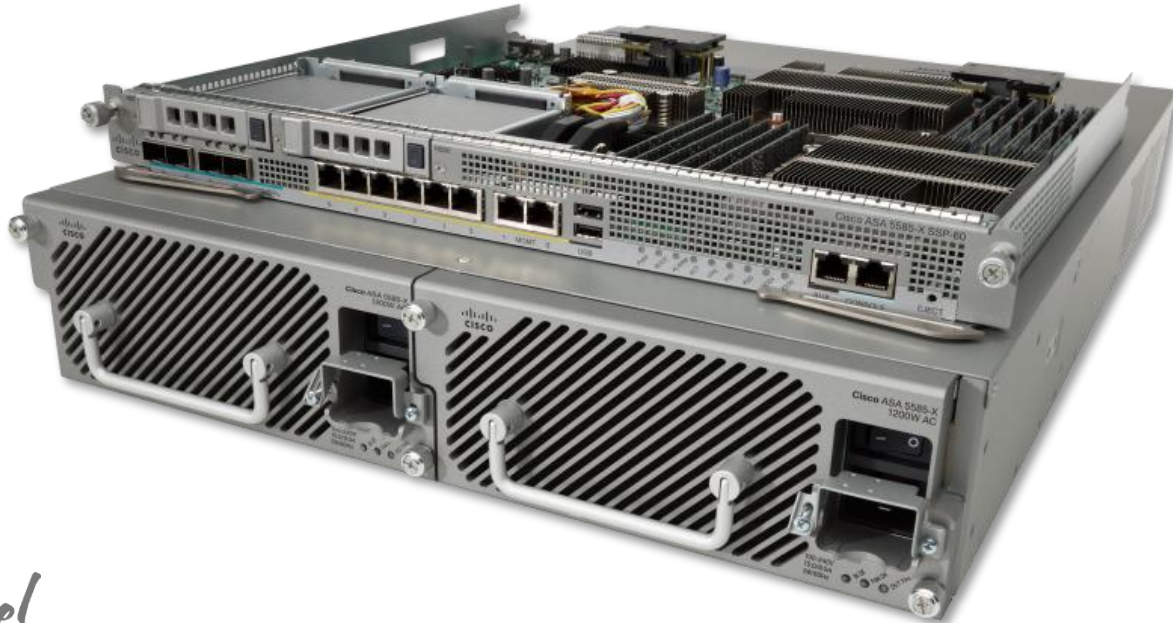
Deployment

How to configure policies

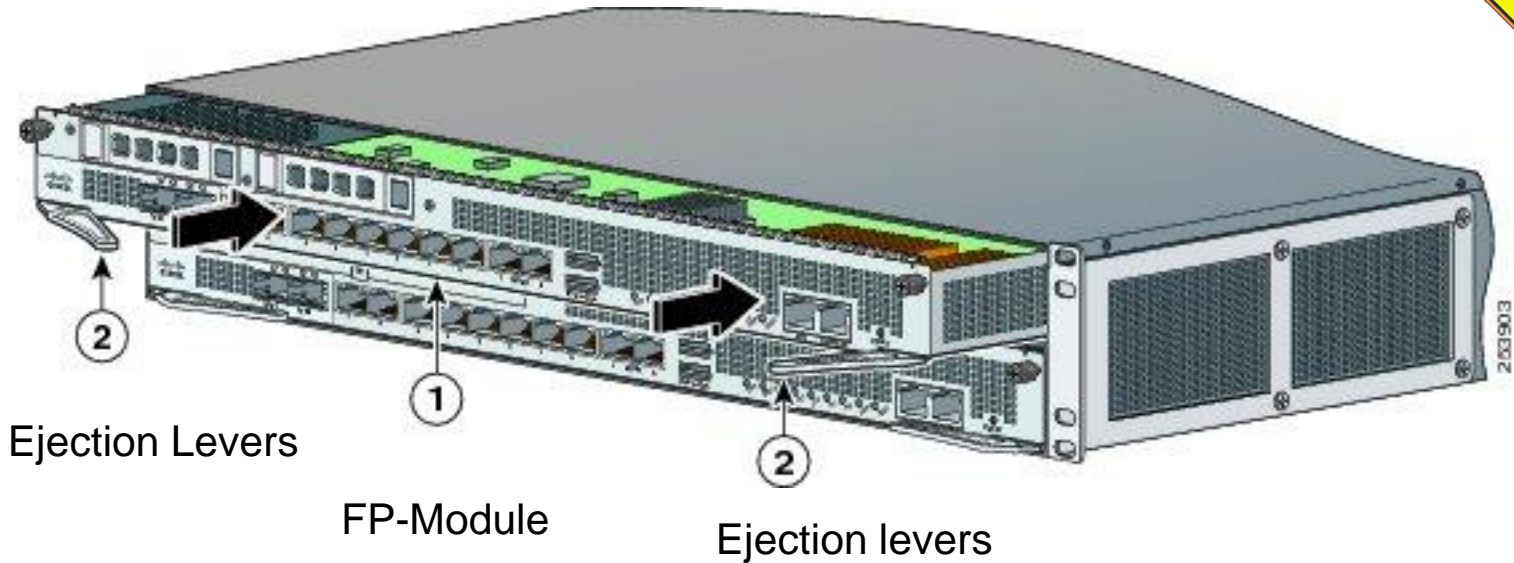
Management and Eventing (“logging”)

How to Deploy FirePOWER on a 5585-X Platform.

Power down the unit and slide the module in the **top** slot

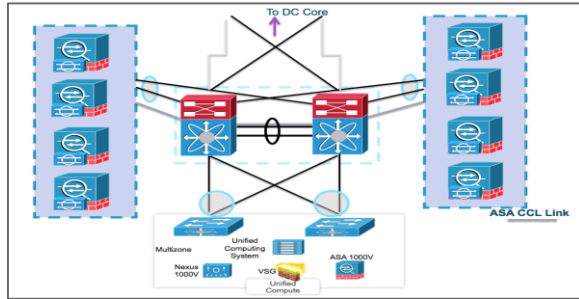


How to Deploy FirePOWER on a 5585-X Platform.



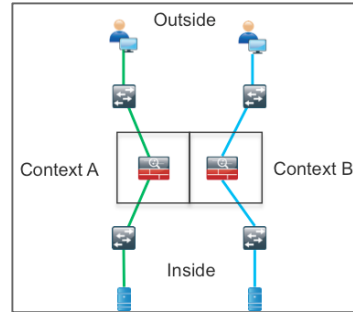
- The module is not hot swappable.
- ASA FP SSP must be at the same level as the SSP model or supported mix blades (10/40 or 20/60)

FirePOWER Services Support All Current ASA Deployment Models



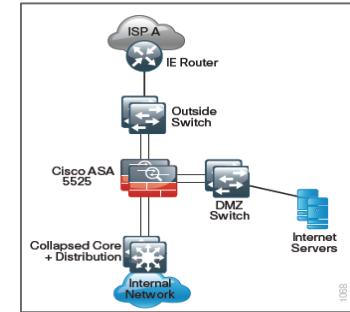
Clustering for linear scalability

- Up to 16x ASA in cluster
- Eliminates Asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently



Multi-context mode for policy flexibility

- Each ASA Interface appears as a separate interface to FirePOWER Services module
- Allows for granular policy enforcement on both ASA and FirePOWER services



HA for increased redundancy

- Redundancy and state sharing (A/S & A/A pair)
- L2 and L3 designs

*State sharing does not occur between FirePOWER Services Modules

Installing FirePOWER Services

Installation Steps



1. Ensure requirements are met
2. Uninstall any existing Cisco IPS or CX module (if applicable)
3. Download ASA FirePOWER Boot Image and System Software packages from Cisco
4. Copy the ASA FirePOWER boot image to the ASA Flash
5. Start the recovery procedure to install the boot image
6. Host the FirePOWER system software package on an HTTP(S) or FTP server
7. Use the initial setup dialogue and system install command to install the system software package
8. Once installed, open a console session to complete the system configuration wizard.
9. Add the FirePOWER sw-module into FireSIGHT Management Centre.
10. Configure ASA to redirect traffic to the module

Requirements



- FirePOWER services is **pre-installed** on ASA5500-X **FirePOWER bundles**
 - I.e. ASA5525-FPWR-BUN SKU
- Installation for FirePOWER services on a ASA5500-X platform requires an **SSD** drive
 - ASA5500-X-SSD12= SKU



Order ASA with SSD

```
ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC"
PID: ASA5515          , VID: V01          , SN: FGL1620413M

Name: "Storage Device 1", DESCR: "Unigen 128 GB SSD MLC, Model Number:
UGB88RRA128HM3-EMY-DID"
PID: N/A              , VID: N/A              , SN: 11000046630
```

Uninstall Classic IPS or CX Software Module (5500)



- Backup IPS configuration via CLI/IDM/IME/CSM or CX configuration via Prime Security Manager
- Shut-down IPS/CX software module:
`sw-module module ips/cxsc shutdown`
- Remove IPS/CX commands from Policy-Map configuration
- Uninstall the IPS software module:
`sw-module module ips/cxsc uninstall`
- Reboot ASA:
`reload`
- Install the FirePOWER software module



Uninstall Classic IPS or CX Software Module (5585)



- Backup IPS configuration via CLI/IDM/IME/CSM or CX configuration via Prime Security Manager
- Shut-down IPS/CX hardware module:
`hw-module module 1 shutdown`
- Remove IPS/CX commands from Policy-Map configuration
- Shut-down and power off the ASA:
`shutdown`
- Remove the IPS/CX module and replace it with the FirePOWER module
- Power On the ASA
- Complete the setup of the FirePOWER module

Installing the Boot Image



- Verify the boot image is present on ASA Flash

```
ciscoasa# show disk0
Directory of disk0:/
113   -rwx   37416960      13:03:22 Jun 10 2014  asa920-104-smp-k8.bin
114   -rwx   17790720      13:04:16 Jun 10 2014  asdm-711-52.bin
118   -rwx   69318656      13:09:10 Jun 10 2014  asasfr-5500x-boot-5.3.1-
152.img
```

- Verify the SSD is present

```
ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC" PID:
ASA5515, VID: V01, SN: FGL1620413M

Name: "Storage Device 1", DESCR: "Unigen 128 GB SSD MLC, Model Number:
UGB88RRA128HM3-EMY-DID"
PID: N/A, VID: N/A, SN: 11000046630
```

- Start the “recovery” procedure to install the boot image

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-boot-5.3.1-152.img
ciscoasa# sw-module module sfr recover boot
```

Verify FirePOWER Services Booted (15 min)



```
ciscoasa# show module sfr details
```

```
Card Type:          FirePOWER Services Software Module
Model:              ASA5545
[OUTPUT OMITTED]
App. version:       5.3.1-152
Data Plane Status: Not Applicable
Console session:    Ready
Status:             Recover
```

- Session into the SFR Boot image and log in

```
ciscoasa# session sfr console
```

```
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

```
Cisco ASA SFR Boot Image 5.3.1
```

```
asasfr login: admin
Password:
```

← Username: Admin
Password Sourcefire

Software Package Installation

- Run the initial SFR-boot setup wizard to configure basic settings such as IP address

```
Cisco ASA SFR Boot 5.3.1 (152)
[asasfr-boot>setup]
Welcome to SFR Setup
Enter a hostname [asasfr]: asafr
Enter an IPv4 address [192.168.8.8]:
[OUTPUT OMITTED]
```



- Download and install the System Software image using **the system install** command

```
[asasfr-boot>system install ftp://10.89.145.63/asasfr-sys-5.3.1-152.pkg]
Verifying

Package Detail
  Description:                Cisco ASA-SFR 5.3.1-152 System Install
  Requires reboot:            Yes

Do you want to continue with upgrade? [y]:

Upgrading
Starting upgrade process ...
Populating new system image...
```

Complete System Configuration

- After a reboot wait for installation to complete and session to the FirePOWER module

```
ciscoasa# session sfr
```

```
Opening console session with module sfr.  
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

```
Sourcefire ASA5525 V5.3.1  
Sourcefire3D login:
```

Username: Admin
Password: Sourcefire



- Complete the system configuration as prompted

```
System initialization in progress. Please stand by.  
You must change the password for 'admin' to continue.  
Enter new password: <new password>  
Confirm new password: <repeat password>  
You must configure the network to continue.  
You must configure at least one of IPv4 or IPv6.  
Do you want to configure IPv4? (y/n) [y]: y  
[OUTPUT OMITTED]
```

FireSIGHT Management Centre Setup

- Identify the FireSIGHT Management Centre that will manage this device

```
> Configure manager add 10.89.145.102 cisco123  
Manager successfully configured.
```

FireSIGHT Management Console
IP address and
registration key



Last step..

Summary of Module Installation

- FirePOWER Services module installs as a software module on Cisco ASA 5500-X platforms and as a hardware module on the Cisco ASA 5585-X
- Both hardware and software modules are managed by the FireSIGHT Management Centre (also known as Defence Centre)
- Traffic is redirected to module using ASA Service Policy
- ASA features and functions are managed using ASDM or CSM including the traffic redirection. FirePOWER policy configuration and other features require FireSIGHT Management Centre

Adding FP Module to FireSIGHT

- Launch FireSIGHT Management Centre and add licenses
- Create an access policy to be used by the FirePOWER Sensor
- Perform initial configuration on module
- Import FirePOWER Sensor and apply policy
- Traffic redirection from ASA

Add License(s) to FireSIGHT

- ◆ Log into FireSIGHT Console
- ◆ System -> Licenses TAB
- ◆ License registered to FireSIGHT MAC address
- ◆ Add + Submit the license(s)

Overview Analysis Policies Devices Objects FireAMP Health **System** Help

Local Updates **Licenses** Monitoring Tools

+ Add New License

Add Feature License

License Key **66:00:50:56:96:5D:35**

License

```
UjVcOjM1OWpzzXjPrwxibhVtmiVyiDE3ODEWnZc4MDSKZmVnDhVvY9pZCAweE17  
Cm1vZGVsX2luZm8gNzJlQjE6V6VJMRmlsdGVyOwo3MkkggQVNBNTU0NTsKbGljZW5z  
ZV90eXB1IFNVQINDUkIQVElPTsKLS0tn+sQNGyUQggEfs0mdcCCc1Km1RixKAW9  
oqzMKGgXBZwt1chb+R9ibBahsY4xP4kWvRkbIRWJOvvy0IxX+cUFujplsR4PB8Nk  
EEsm/sDjT06hoUCI57YzEn/boZb9eUwOq9kxydbGbbTuHMT2hXCx4J7+Xh2st1ps  
ETeX/kPSV+YU5b6+W5kSUcQPuxGx1tvIfc3PgsoFDyFDLD2DNXvm+79Vzsls3  
GXax7kS5khBbWqOfiO8bxXZSX1I76ZnyxNyRDI/q3hcQnpNvwNXw5EFM61pc/tq  
2KYTuJ5FEvuugOWe3xqXiaTpJ9r+FCN9Ent0LRMBkD+6f3ALbr7nafefGKMknOu  
4yBPIJUtauC5og9PEb/Cgm4agrY/bCFnoJzYjOXBjlcJXyqVzTRO+43GQYBInPa9  
uANLwSrif4IWgDex1KhdZi1mEf8WNTHshwASTI7KGX5QbDqCJDLBD2eeqg7HdTW+  
IryvR2ReDFOzrUjdU4g9W4EIS+KX699F9DEY8yPC9W5s8dTvoMiz1nJG3M5O+QKex  
fDrTrzEFAJ89DeA3OzVgIHD6GdskJvbEanFBdyZ2WeGIkjtRkyj8lJlxs5YGAo  
OvwcFc9Rjz69Em9CK9Yj770A7TtT3InbI6VrWeS5HwnMbEvz52N4qWezRixdzDzZ  
dVQqAv1w8Uo=
```

--- END SourceFire Product License ---

Get License Verify License **Submit License**

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to <https://keyserver.sourcefire.com>.

Using the license key, **66:00:50:56:96:5D:35**, follow the on-screen instructions to generate a license.

Return to License Page

Last login on Tuesday, 2014-10-21 at 18:39:28 PM from 192.168.50.54

Create Access Policy for FirePOWER Module

- Navigate to *Policies -> Access Control*.
Click *New Policy*
- Configure *Name & Description* (optional)
- Default Action of *Intrusion Prevention* is best practice
- Available Devices will not show your new ASA FirePOWER sensor until added

New Access Control Policy ? x

Name: ASASFR Access Policy

Description:

Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

Available Devices

Selected Devices

Search

Stand Alone Sensors

sf.example.com

Add to Policy

Save Cancel

Add FirePOWER Sensor into FireSIGHT

- Use the FireSIGHT Management Centre - Device Manager to add the device
- Choose Access Control Policy you configured previously (or Default)

Add Device ? x

Host: 10.89.145.52

Registration Key: cisco123

Group: None

Access Control Policy: Default Access Control

Licensing

Protection:

Control:

Malware:

URL Filtering:

VPN:

Advanced

Register Cancel

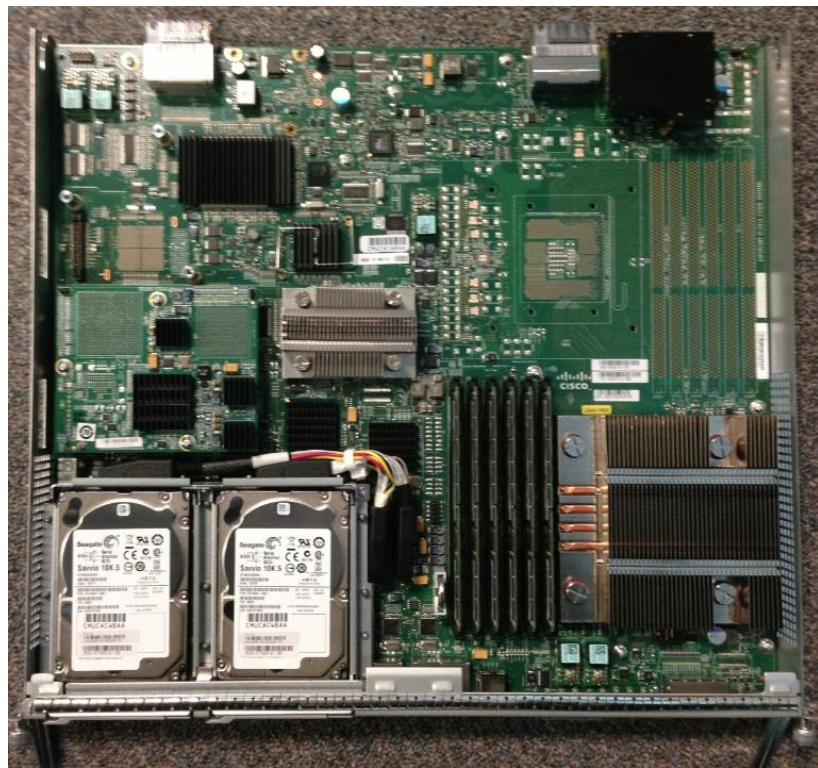
Module IP address and registration key

Licenses applied to FireSIGHT MC



How to Deploy FirePOWER on a 5585-X Platform.

- Power down the unit and slide the module in the **top** slot
- Connect the M0/0 port to the network
- Install boot software
- Partition
- Configure IP address
- Install system software
- Launch FireSIGHT (Defence Centre)
- Install license(s)
- Configure Policies
- Punt traffic up to the FP for filtering



Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

Management and Eventing (“logging”)

Compatibility with ASA Features

- Minimum ASA version: 9.2.2
- Guidelines for traffic sent to the ASA FirePOWER module:
 - Do not configure ASA inspection on HTTP traffic.
 - Do not configure Cloud Web Security Inspection
 - Other application inspections on the ASA are compatible with the FirePOWER module
 - Do not enable Mobile User Security (MUS) Server; it is not compatible with the FirePOWER module
- In ASA Failover/Clustering mode, configuration between different modules is not automatically synchronised (FireSIGHT will handle this)

Configure ASA to Redirect Traffic to the Module

- Traffic Redirection is done using Service Policies as a part of ASA MPF
- Traffic for inspection can be matched based on interface, source/destination, protocol ports and even user identity
- In Multi-context-mode, different FirePOWER policies can be assigned to each context
- MPF can be configured from CLI, ASDM or CSM
- **Fail-open** and **Fail-closed** options are available
- **Monitor-only mode** option for a “passive” deployment.

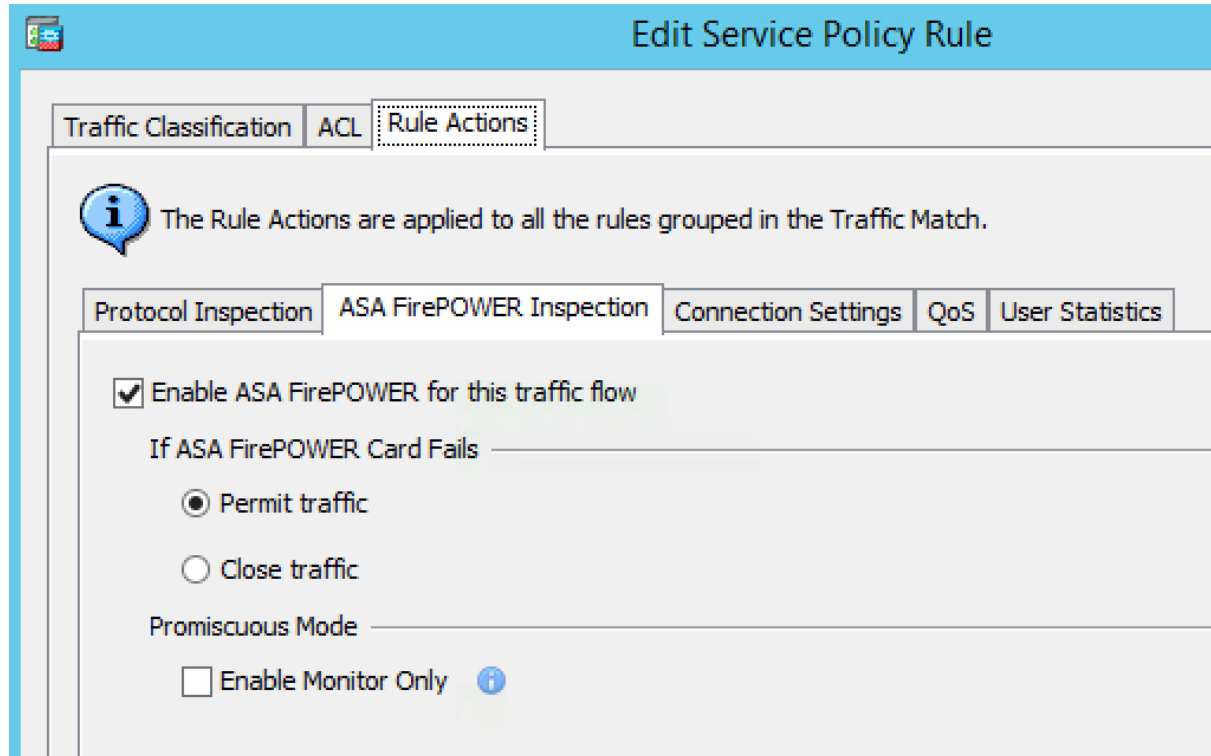
```
policy-map global_policy
  class class-default
    sfr fail-open
```

```
service-policy global_policy global
```



Configure ASA to Redirect Traffic using ASDM

Configure -> Firewall -> Service Policy Rules -> Global Policy



The screenshot shows the 'Edit Service Policy Rule' window in ASDM. The 'Rule Actions' tab is selected, and the 'ASA FirePOWER Inspection' sub-tab is active. The configuration includes a checked checkbox for 'Enable ASA FirePOWER for this traffic flow'. Below this, there are radio buttons for 'Permit traffic' (selected) and 'Close traffic'. There is also an unchecked checkbox for 'Enable Monitor Only' with an information icon.

Edit Service Policy Rule

Traffic Classification | ACL | **Rule Actions**

i The Rule Actions are applied to all the rules grouped in the Traffic Match.

Protocol Inspection | **ASA FirePOWER Inspection** | Connection Settings | QoS | User Statistics

Enable ASA FirePOWER for this traffic flow

If ASA FirePOWER Card Fails _____

Permit traffic

Close traffic

Promiscuous Mode _____

Enable Monitor Only **i**

Examples for the ASA FirePOWER Module



The following example diverts all HTTP traffic to the ASA FirePOWER module, and blocks all HTTP traffic if the module fails for any reason:

```
hostname(config)# access-list ASASFR permit tcp any any eq 80  
hostname(config)# class-map my-sfr-class  
hostname(config-cmap)# match access-list ASASFR  
hostname(config-cmap)# policy-map my-sfr-policy  
hostname(config-pmap)# class my-sfr-class  
hostname(config-pmap-c)# sfr fail-close  
hostname(config-pmap-c)# service-policy my-sfr-policy global
```

Examples for the ASA FirePOWER Module



The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the ASA FirePOWER module, and allows all traffic through if the module fails for any reason.

```
hostname(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list my-sfr-acl
hostname(config)# class-map my-sfr-class2
hostname(config-cmap)# match access-list my-sfr-acl2
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap)# class my-sfr-class2
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap-c)# service-policy my-sfr-policy interface outside
```

User Identification

User identification uses two distinct mechanisms

1. Network discovery

- Understands AIM, IMAP, LDAP, Oracle, POP3 and SIP
- Will only provide limited information when deployed at the Internet edge

2. Sourcefire User Agent (SFUA)

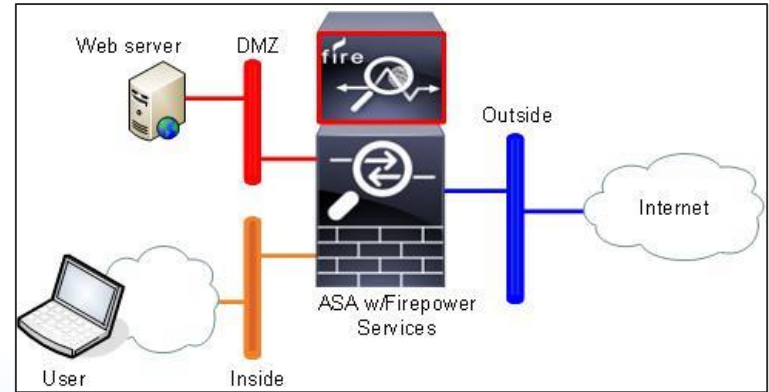
- Installed on a Windows Platform
- Windows server *does not* have to be a domain member
- Communicates with the AD using WMI – starts on port 136 then switches to random TCP ports
- Communicates with FMC through a persistent connection to TCP port 3306 on the FMC
- Endpoints must be domain members
- Well-suited for Internet edge firewalls

Note: This solution does not use the Cisco Context Directory Agent (CDA)

Firewall Policies – Edge Firewall

Use Cases

1. Inbound (Outside->in)
2. Outbound (Inside->Out)



URL Category/Reputation

NGIPS

Application Visibility and Control

Advanced Malware Protection

File Type filtering

File capture

TCP Normalisation

TCP Intercept

IP Option Inspection

IP Fragmentation

Botnet Traffic Filter

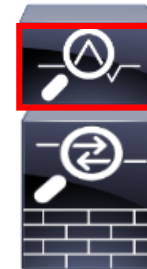
NAT

Routing

ACL

VPN Termination

Failover & Clustering



Firepower Services

ASA

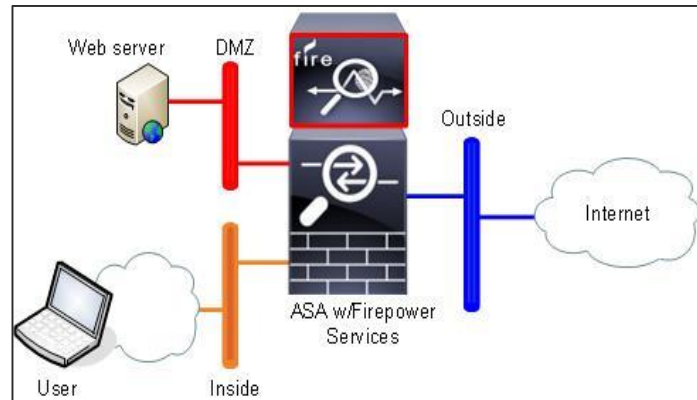
Firewall Policies – Edge Firewall - InBound

Policy Requirements

- Static NAT to a DMZ server
- Policy to control inbound ports (TCP/80, TCP/443, Passive FTP)
- Policy to inspect inbound traffic by SNORT engine (security over connectivity)
- Policy to control file types uploaded to DMZ server

Configuration Steps

- Configure NAT ASA
- Configure Inbound ACLs on outside interface
- Create File policy
- Configure Access policy FireSIGHT MC



Firewall Policies – Edge Firewall - InBound

- Configure NAT ASA

ASDM:

The screenshot shows the 'Edit Network Object' dialog box in ASDM. The 'Name' field is 'WebServer5', 'Type' is 'Host', 'IP Version' is 'IPv4', and 'IP Address' is '10.100.1.5'. The 'Description' is 'Web Server'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Static', and 'Translated Addr' set to '64.100.14.3'. The 'Use one-to-one address translation' checkbox is also checked. Other options like 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness', 'Translate TCP and UDP ports', 'Fall through to interface PAT', and 'Use IPv6 for interface PAT' are unchecked. An 'Advanced...' button is visible at the bottom of the NAT section. At the very bottom of the dialog are 'Help', 'Cancel', and 'OK' buttons.

CLI:

```
object network WebServer5
 host 10.100.1.5
 description Web Server
 nat static 64.100.14.3 net-to-net
```

Firewall Policies – Edge Firewall - InBound

- Configure Inbound ACLs on outside interface

ASDM:

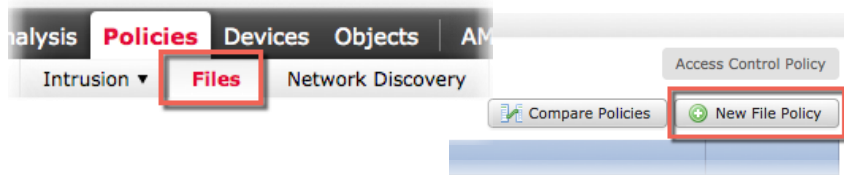
1		any		Any less secur...	IP	ip	Permit	
▼ Outside (1 incoming rule)								
1	<input checked="" type="checkbox"/>	any		WebServer5	TCP	ftp http https	Permit	0
management (0 implicit incoming rules)								

CLI:

```
object-group service DM_INLINE_TCP_1 tcp
  port-object eq ftp
  port-object eq http
  port-object eq https
access-list Outside_access_in line 1 extended permit tcp any object
WebServer5 object-group DM_INLINE_TCP_1
access-group Outside_access_in in interface Outside
```

Firewall Policies – Edge Firewall - InBound

- Create the file policy



Add File Rule

Application Protocol: Any

Direction of Transfer: Upload

Action: Block Malware

- ✓ Detect Files
- ✗ Block Files
- Malware Cloud Lookup
- Block Malware

Store Files

- Malware
- Unknown
- Clean
- Custom

File Type Categories

<input type="checkbox"/> Office Documents	16
<input type="checkbox"/> Archive	17
<input type="checkbox"/> Multimedia	2
<input checked="" type="checkbox"/> Executables	6
<input checked="" type="checkbox"/> PDF files	1
<input type="checkbox"/> Encoded	0
<input type="checkbox"/> Graphics	0
<input type="checkbox"/> System files	2
<input type="checkbox"/> Dynamic Analysis Capable	1

File Types

Search name and description

All types in selected Categories

- BINARY_DATA (Universal Binary/Java B...
- BINHEX (Macintosh BinHex 4 Compress...
- EICAR (Standard Anti-Virus Test File)
- ISHIELD_MSI (Install Shield v5.x or 6.x
- JARPACK (Jar pack file)
- MSEXE (Windows/DOS executable file)
- PDF (PDF file)

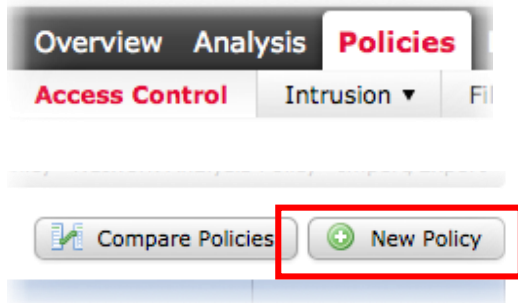
Selected File Categories and Types

- Category: PDF files
- Category: Executables

Add

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC



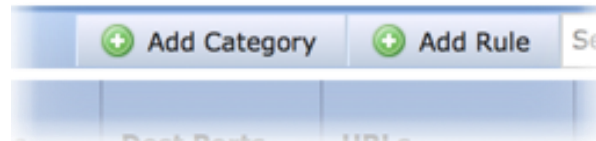
New Access Control Policy

The 'New Access Control Policy' configuration window is shown. It has a title bar with a question mark and a close button. The form contains the following fields and options:

- Name:** PerimeterInBound
- Description:** Inbound Policy
- Default Action:** Block all traffic, Intrusion Prevention, Network Discovery
- Targeted Devices:** (Empty list)
- Available Devices:** A list of devices with a search bar above it. The list includes:
 - ASA
 - Firepower
 - 10.132.10.17
 - 10.132.10.19
 - 10.132.10.7
- Selected Devices:** (Empty list)
- Add to Policy:** A button located between the 'Available Devices' and 'Selected Devices' lists.
- Save** and **Cancel** buttons are located at the bottom right of the window.

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC



Overview Analysis **Policies** Devices Objects AMP Health System Help mark

Access Control Intrusion Files Network Discovery SSL Application Detectors Users Correlation Actions

PerimeterInBound

You have unsaved changes Save Cancel Save and Apply

Inbound policy

Rules Targets (0) Security Intelligence HTTP Responses Advanced

Filter by Device Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Src Ports	Dest Ports	URLs	Action				
Administrator Rules																
<i>This category is empty</i>																
Standard Rules																
<i>This category is empty</i>																
Root Rules																
<i>This category is empty</i>																
Default Action												Intrusion Prevention: Balanced Security and Connectivity				

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC

Add Rule



Name

Enabled

Insert

Action

IPS: no policies

Variables: n/a

Files: no inspection

Logging: no logging

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Inspection

Logging

Comments

Available Networks

Networks

Geolocation

Private Networks

Add to Source

Add to Destination

Source Networks (0)

any

Destination Networks (1)

10.100.1.5

Add

Add

Add

Cancel

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC

Editing Rule - Inbound DMZ Server Policy

The screenshot shows the configuration page for the "Inbound DMZ Server Policy" rule. The rule is enabled and has an "Allow" action. The "Applications" tab is selected, showing a list of available applications and a list of selected applications and filters. The "Applications" tab is highlighted with a red box. The "Available Applications (3149)" list has a search box also highlighted with a red box. The "Selected Applications and Filters (4)" list shows four selected applications: FTP, FTP Data, HTTP, and HTTPS, which are also highlighted with a red box.

Name: Enabled [Move](#)

Action: Allow **IPS:** no policies **Variables:** n/a **Files:** no inspection **Logging:** no logging

Zones **Networks** VLAN Tags Users **Applications** Ports URLs Inspection Logging Comments

Application Filters **Available Applications (3149)** **Selected Applications and Filters (4)**

Search by name

Search by name

User-Created Filters

- Risks (Any Selected)
 - Very Low 1093
 - Low 783
 - Medium 977
 - High 183
 - Very High 113
- Business Relevance (Any Selected)
 - Very Low 821
 - Low 539

050plus
1&1 Internet
1-800-Flowers
1000mercis
100Bao
100ye.com
12306.cn
126.com
17173.com

Viewing 1-100 of 3149

Add to Rule

Applications

- FTP
- FTP Data
- HTTP
- HTTPS

Save Cancel

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC

Add Rule



Name

Enabled

Insert

Action

IPS: Security Over Conne...

Variables: default

Files: PerimeterFirewallAMP

Logging: files: dc

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Inspection

Logging

Comments

Intrusion Policy

Variable Set

File Policy

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC

Editing Rule - Inbound DMZ Server Policy



Name

Enabled

[Move](#)

Action

IPS: Security Over Conne...

Variables: Default Set

Files: PerimeterFirewallAMP

Logging: connections, files:...

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Inspection

Logging

Comments

Log at Beginning of Connection

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Defense Center

Syslog

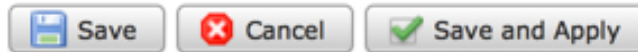
SNMP Trap

Save

Cancel

Firewall Policies – Edge Firewall - InBound

- Configure Access policy FireSIGHT MC



IP Chicken - Whats my IP a... Virtual Defense Center 64bit... Cisco ASDM 7.4(1)

https://10.132.10.9/ddd/#FirewallPolicyEditor;uid=8358a516-0bbc-11e5-b5d9-d81bd5f36c1

Overview Analysis **Policies** Devices Objects AMP

Access Control Intrusion Files Network Discovery SSL Application Detectors Users Correlation Actions

PerimeterInBound

Inbound policy

Rules Targets (0) Security Intelligence HTTP Responses Advanced

Filter by Device Add Category Add Rule Search Rules

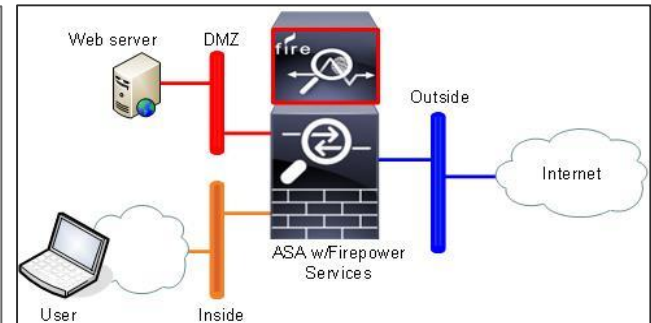
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Src Ports	Dest Ports	URLs	Action				
Administrator Rules																
<i>This category is empty</i>																
Standard Rules																
1	Inbound DMZ Server Policy	any	any	any	10.100.1.5	any	any	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> FTP <input type="checkbox"/> FTP Data	any	any	any	Allow				0
Root Rules																
<i>This category is empty</i>																
Default Action													Intrusion Prevention: Balanced Security and Connectivity			

Firewall Policies – Edge Firewall - Outbound

- Dynamic NAT
- User authentication
- Per user policy
- Application control
- Reputation
- Category
- Policy to inspect outbound traffic by SNORT engine (connectivity over security)
- Policy to control files based on AMP disposition from the Internet

Configuration Steps

- Configure Dynamic Port Address Translation ASA
- Create File policy
- Configure Access policy FireSIGHT MC



Firewall Policies – Edge Firewall - Outbound

- Configure Dynamic Port Address Translation ASA

ASDM:

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address: Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

CLI:

```
nat (Inside,Outside) 1 source dynamic any interface description Dynamic NAT
```

Firewall Policies – Edge Firewall - Outbound

- Create File policy

Edit File Rule



Application Protocol

Action

Direction of Transfer

- Spero Analysis for MSEXE
- Dynamic Analysis
- Reset Connection

Store Files

- Malware
- Unknown
- Clean
- Custom

File Type Categories

- | | |
|---|----|
| <input type="checkbox"/> Office Documents | 16 |
| <input type="checkbox"/> Archive | 17 |
| <input type="checkbox"/> Multimedia | 2 |
| <input type="checkbox"/> Executables | 6 |
| <input type="checkbox"/> PDF files | 1 |
| <input type="checkbox"/> Encoded | 0 |
| <input type="checkbox"/> Graphics | 0 |
| <input type="checkbox"/> System files | 2 |
| <input type="checkbox"/> Dynamic Analysis Capable | 1 |

File Types

-
- 7Z (7-Zip compressed file)
 - ACCDB (Microsoft Access 2007 file)
 - ARJ (Compressed archive file)
 - BINARY_DATA (Universal Binary/Java)
 - BINHEX (Macintosh BinHex 4 Compre)
 - BZ (bzip2 compressed archive)
 - CPIO_CRC (Archive created with the
 - CPIO_NEWC (Archive created with th
 - CPIO_ODC (Archive created with the

Add

Selected File Categories and Types

- Category: System files
- Category: PDF files
- Category: Executables
- Category: Archive
- Category: Office Documents

Save

Cancel

Firewall Policies – Edge Firewall - Outbound

- Configure Access policy FireSIGHT MC

Add Rule



Name

Enabled

Insert

Action

IPS: *no policies*

Variables: *n/a*

Files: *no inspection*

Logging: *no logging*

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Inspection

Logging

Comments

Categories and URLs

- Swimsuits and Intimate Apparel
- Training and Tools
- Translation
- Travel
- Unconfirmed SPAM Sources
- Violence
- Weapons
- Web Advertisements
- Web based email
- Web Hosting Sites

Reputations

- Any
- 5 - Well Known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High Risk

Selected URLs (14)

- Abused Drugs (Any Reputation)
- Adult and Pornography (Any Reputation)
- Alcohol and Tobacco (Any Reputation)
- Bot Nets (Any Reputation)
- Cheating (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Cult and Occult (Any Reputation)
- Gambling (Any Reputation)
- Hacking (Any Reputation)
- Hate and Racism (Any Reputation)

Add to Rule

Add

Add

Cancel

Firewall Policies – Edge Firewall - Outbound

- Configure Access policy FireSIGHT MC

Add Rule



Name Enabled Insert

Action

Intrusion Policy

File Policy

Firewall Policies – Edge Firewall - Outbound

- Configure Access policy FireSIGHT MC

Add Rule

? X

Name Enabled Insert

Action **Variables:** default **Files:** UserProtectionAMP **Logging:** files: dc

Intrusion Policy
 Variable Set

File Policy

Firewall Policies – Edge Firewall - Outbound

- Configure Access policy FireSIGHT MC



Outbound Policy										
2	User OutBound URL Contr	any	any	any	any	any	any	any	any	<ul style="list-style-type: none">Abused Drugs (AAdult and PornogAlcohol and Toba X BlockBot Nets (Any Re(10 more...)

Firewall Policies – Edge Firewall - Outbound

- Configure Access policy FireSIGHT MC

Overview Analysis **Policies** Devices Objects AMP Health System Help mark

Access Control Intrusion Files Network Discovery SSL Application Detectors Users Correlation Actions

PerimeterInBound

Inbound policy

Rules Targets (0) Security Intelligence HTTP Responses Advanced More Capture Types

Filter by Device Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action						
Administrator Rules																		
<i>This category is empty</i>																		
Standard Rules																		
1	Inbound DMZ Server Polic	any	any	any	10.100.1.5	any	any	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> FTP <input type="checkbox"/> FTP Data	any	any	any	Allow						
Outbound Policy																		
2	User OutBound URL Contr	any	any	any	any	any	any	any	any	any	any	Block						
												Abused Drugs (A Adult and Pornog Alcohol and Toba Bot Nets (Any Re (10 more...))						
3	User Outbound Permit	any	any	any	any	any	any	any	any	any	any	Allow						
Root Rules																		
<i>This category is empty</i>																		
Default Action																		
															Intrusion Prevention: Balanced Security and Connectivity			

Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

Management and Eventing (“logging”)

FireSIGHT

FireSIGHT Management Centre

Single console for event, policy, and configuration management

Overview Analysis Policies Devices Objects FireAMP Health System Help jolaughlin

Dashboards Reporting Summary Report Designer

Security Awareness Dashboard (JRS)

Detailed Dashboard (Javed)

Malware Files Threat Summary Flows Applications Traffic GeoDB Intrusions User Activity URL Activity Firesight Show the Last 1 hour Add Widgets

Intrusion Events

Last 1 hour Total

Category	Total
All	662
1	23
2	227
3	405

Security Events by Destination IP

Destination IP	Count
10.131.11.127	7
10.131.12.13	6
131.75.28.98	6
172.16.0.107	4
10.131.10.254	3

Last updated 9 minutes ago

Impact Level 1 Events by Application

Application	Impact Level 1 Events
HTTP	22
Web browser	22
generic audio/video	8
MySQL	1
MySQL client	1

Last updated 9 minutes ago

Total Events by User

Username	Total Events
lucio.david (lucio.david, LDAP)	12
adelaida.blount (adelaida.blount, LDAP)	10
liliana.reilly (liliana.reilly, LDAP)	10

All Intrusion Events

Last updated 9 minutes ago

All Intrusion Events (Not Dropped)

Message	Count
INDICATOR-SHELLCODE x86 OS agnostic Instenv geteip dword xor	33
PROTOCOL-TFTP GET filename overflow attempt (1:1941)	31
SERVER-OTHER Wireshark LWRES (l3sector getaddrsbvname buffer	22
SERVER-MAIL Microsoft Windows Exchange MODPROPS denial of service	21
PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
WEB-CLIENT obfuscated header in PDF (3:16343)	19
FILE-MULTIMEDIA VideoLAN VLC Media Player TY processing buffer	18
SERVER-WEBAPP OpenView Network Node Manager cookie buffer	17
SERVER-WEBAPP HP OpenView Network Node Manager OvOSLocale	17
OS-WINDOWS DCERPC Messenger Service buffer overflow attempt	14
INDICATOR-SHELLCODE x86 fldz get eip shellcode (1:14986)	13
EXPLOIT dhclient subnet mask option buffer overflow attempt	13
SERVER-OTHER McAfee ePolicy Orchestrator Framework Services log	13
INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case	12
BROWSER-IE Microsoft Internet Explorer marquee object handling	11
FILE-OFFICE Microsoft Office Outlook SMB attach by reference code	11
BROWSER-IE Microsoft Internet Explorer oversize recordset object	11
SERVER-OTHER ISC BIND RRSIG query denial of service attempt	11
SERVER-WEBAPP HP OpenView Performance Insight Server backdoor	10

Last updated 5 minutes ago

Total Events by Application

Application	Total Events
HTTP	678
Web browser	626

Create report from any dashboard →

Report Designer

Application Statistics

Provides traffic and intrusion event statistics by application

Connections × Intrusion Events × + Show the Last 1 hour Add Widgets

Allowed Connections by Application

Application	Allowed Connections
<input type="checkbox"/> Sun RPC	191,962
<input type="checkbox"/> Sun RPC client	191,962
<input type="checkbox"/> DNS	177,792
<input type="checkbox"/> HTTP	80,881
<input type="checkbox"/> HTTPS	41,480
+1 <input type="checkbox"/> Direct Connect	23,586
+1 <input type="checkbox"/> Direct Connect	23,586
+1 <input type="checkbox"/> SNMP	20,094
+1 <input type="checkbox"/> Dropbox	13,369
+1 <input type="checkbox"/> SSL	9,756

Last updated less than a minute ago

Unique Applications over Time

Last updated less than a minute ago

Risky Applications

Application	Total Bytes (KB)
<input type="checkbox"/> BitTorrent	41,077.00
<input type="checkbox"/> eDonkey	320.16
<input type="checkbox"/> Ustream.tv	81.63
<input type="checkbox"/> Facebook	34.69
+1 <input type="checkbox"/> Yet ABC	8.89
+1 <input checked="" type="checkbox"/> Facebook Apps	4.16
<input type="checkbox"/> QQ	1.98
+1 <input checked="" type="checkbox"/> MySpace	0.70
-1 <input type="checkbox"/> Gnutella	0.53

Allowed Connections by Business

Business Relevance	Allowed Connections
High	410,375
Medium	331,579
Very High	53,575
Very Low	6,905
Low	28

Last login on Tuesday, 2011-11-15 at 10:23:56 from 10.2.100.129

Allowed Connections by Application Risk

Risk	Allowed Connections
High	584,664
Very Low	138,513
Medium	72,069
Very High	6,923
Low	293

Risky Applications (Config Panel)

Title: Risky Applications

Preset: None

Table: Application Statistics

Field: Application

Aggregate: Total Bytes (KB)

Filter: High Risk Applications with Low Bl

Show: Top

Results: 10

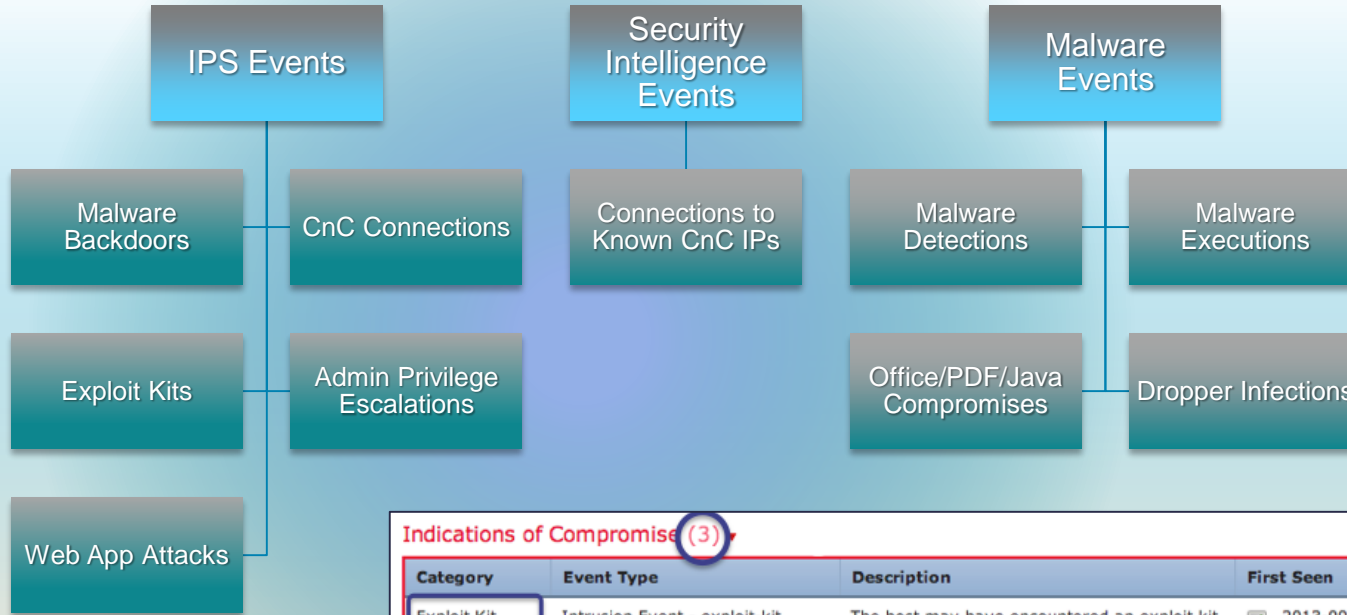
Show Movers:

Color:

Application	Total Bytes (KB)
<input type="checkbox"/> BitTorrent	41,077.00
<input type="checkbox"/> eDonkey	320.16
<input type="checkbox"/> Ustream.tv	81.63
<input type="checkbox"/> Facebook	34.69
+1 <input type="checkbox"/> Yet ABC	8.89
+1 <input checked="" type="checkbox"/> Facebook Apps	4.16
<input type="checkbox"/> QQ	1.98
+1 <input checked="" type="checkbox"/> MySpace	0.70
-1 <input type="checkbox"/> Gnutella	0.53

Last updated 4 minutes ago

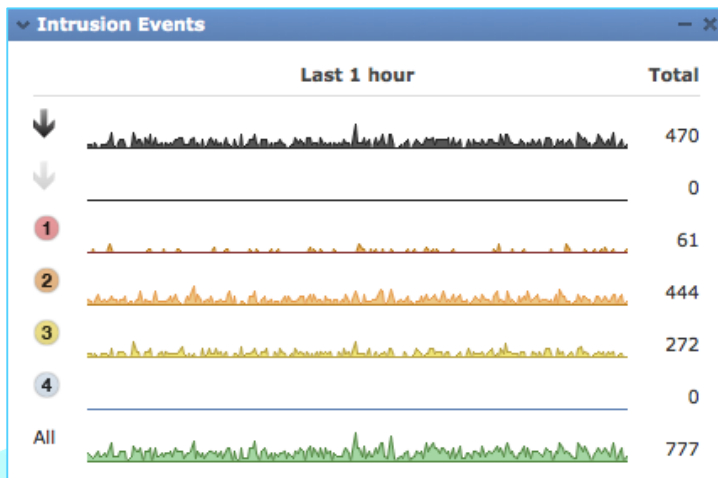
Indications of Compromise (IoCs)



Indications of Compromise (3) Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Impact Assessment



Correlates all intrusion events to an impact of the attack against the target



IMPACT FLAG	ADMINISTRATOR ACTION	WHY
1	Act Immediately, Vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use, but no vuln mapped
3	Good to Know, Currently Not Vulnerable	Relevant port not open or protocol not in use
4	Good to Know, Unknown Target	Monitored network, but unknown host
0	Good to Know, Unknown Network	Unmonitored network

FireSIGHT™ Streamlines Operations


- Recommended Rules


Policy Information


Name:


Description:



Drop when Inline:


 **Base Policy**




 The base policy is up to date (Rule Update 2013-10-09-004-vrt)

 **This policy defines 0 variables**

 **This policy has 9038 enabled rules**

-  558 rules generate events
-  8480 rules drop and generate events

 **FireSIGHT recommends 7154 rule state settings for 7430 hosts**

-  Set 214 rules to generate events
-  Set 3550 rules to drop and generate events
-  Set 3390 rules to disabled

Policy is not using the recommendations. Click to change recommendations

Last generated: 2013 Oct 10 10:15:33

Class-Leading NGFW Context and Visibility Demo

Overview Analysis **Policies** Devices Health System Help jamar

Intrusion Access Control Network Discovery Custom Applications Users Correlation Actions

Interesting Use Cases

Enter a description

Save Cancel Save and Apply Add Category Add Rule Search Rules

Device Targets: 0 devices

#	Name	Source Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	U...	Applications	Services	URLs	Action			
Administrator Rules														
This category is empty.														
Standard Rules														
1	Mobile Security 1	Intern	any	any	Ten	any	any	Android browser Blackberry browser Mobile Safari	any	any	Block		1	
2	Read Only Facebook	Intern	Extern	any	any	any	any	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game; Fill	any	any	Block		0	
3	Web Block List	Intern	Extern	any	any	any	any		any		Block		0	
4	Block All P2P	Intern	Extern	any	any	any	any	Categories: peer to peer	any	any	Block		0	
5	Inbound Email	Extern	Intern	any	any	any	any	SMTP	SMTP	any	Allow		0	
6	Outbound Web Browsing	Extern	Intern	any	any	any	any	HTTP	any	any	Allow		0	
Root Rules														
This category is empty.														
Default Action														
Access Control: Block All Traffic														
1 Row Selected														
Displaying 1 - 6 of 6 rules Page 1 of 1														

SOURCEfire

Summary: Cisco ASA with FirePOWER Services

Industry's First Adaptive, Threat-Focused NGFW



- ▶ Cisco ASA is world's most widely deployed, enterprise-class stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced malware protection

Useful links:

ASA with FirePOWER Services Download link:

<http://software.cisco.com/download/release.html?mdfid=286271171&flowid=70723&softwareid=286277393&release=5.3.1.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

Release Notes:

<http://www.cisco.com/c/en/us/td/docs/security/firesight/531/relnotes/FireSIGHT-System-Release-Notes-Version-5-3-1.html>

Installation guide:

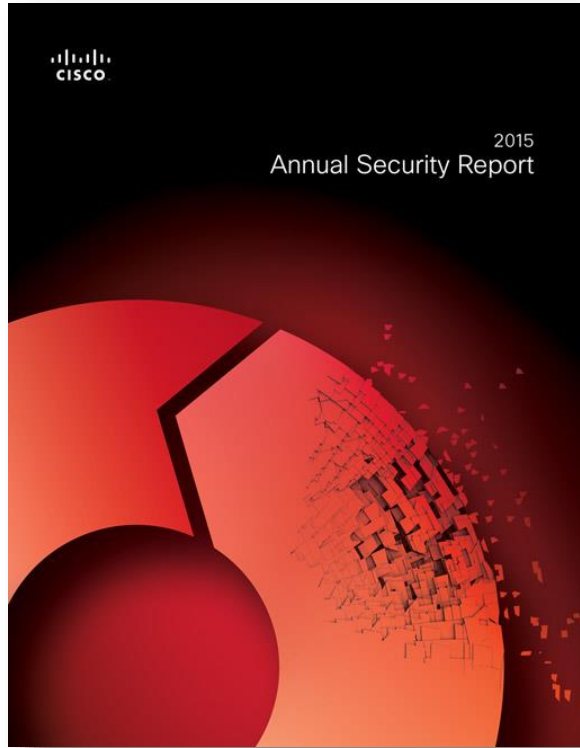
<http://www.cisco.com/c/dam/en/us/td/docs/security/firesight/531/PDFs/FireSIGHT-System-Installation-Guide-Version-5-3-1.pdf>

User guide:

<http://www.cisco.com/c/dam/en/us/td/docs/security/firesight/531/PDFs/FireSIGHT-System-User-Guide-Version-5-3-1.pdf>

Recommended Sessions

- BRKSEC-2018 - Tips and Tricks for Successful Migration from ASA CX & IPS
- BRKSEC-3055 - Troubleshooting Cisco ASA with FirePOWER Services
- BRKSEC-3034 - FireSight Analytics
- BRKSEC-2020 - Firewall Deployment
- BRKSEC-2021 - Firewall Architecture in the Datacenter and Internet Edge
- LABSEC-2339 - Cisco ASA with FirePOWER services



Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015

Q & A

Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could Be a Winner

- Promote your favorite speaker through Twitter and you could win \$200 of Cisco Press products (@CiscoPress)
- Send a tweet and include
 - Your favorite speaker’s Twitter handle **#JEFANELL ← THIS GUY!**
 - Two hashtags: #CLUS #MyFavoriteSpeaker
- You can submit an entry for more than one of your “favorite” speakers
- Don’t forget to follow @CiscoLive and @CiscoPress
- View the official rules at <http://bit.ly/CLUSwin>

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a \$750 Amazon gift card.
- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.



Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at [CiscoLive.com/Online](https://www.ciscolive.com/online)

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you



CISCO

TOMORROW starts here.