TOMORROW
starts here.

Deploying Next-Generation Firewall with ASA and Firepower Services

BRKSEC-2028

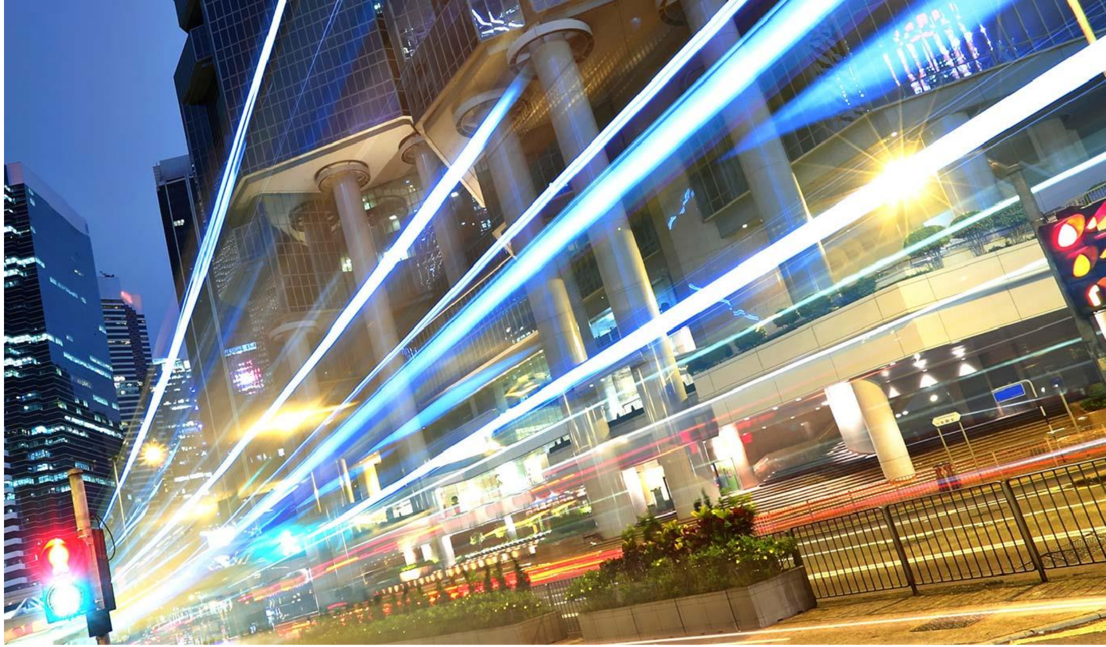
Jeff Fanelli

Technical Solutions Architect

#clmel

Cisco live!

Agenda



Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

Management and Eventing (“logging”)

The Challenges Come from Every Direction

Sophisticated Attackers

Dynamic Threats

Complex Geopolitics

Defenders

Complicit Users

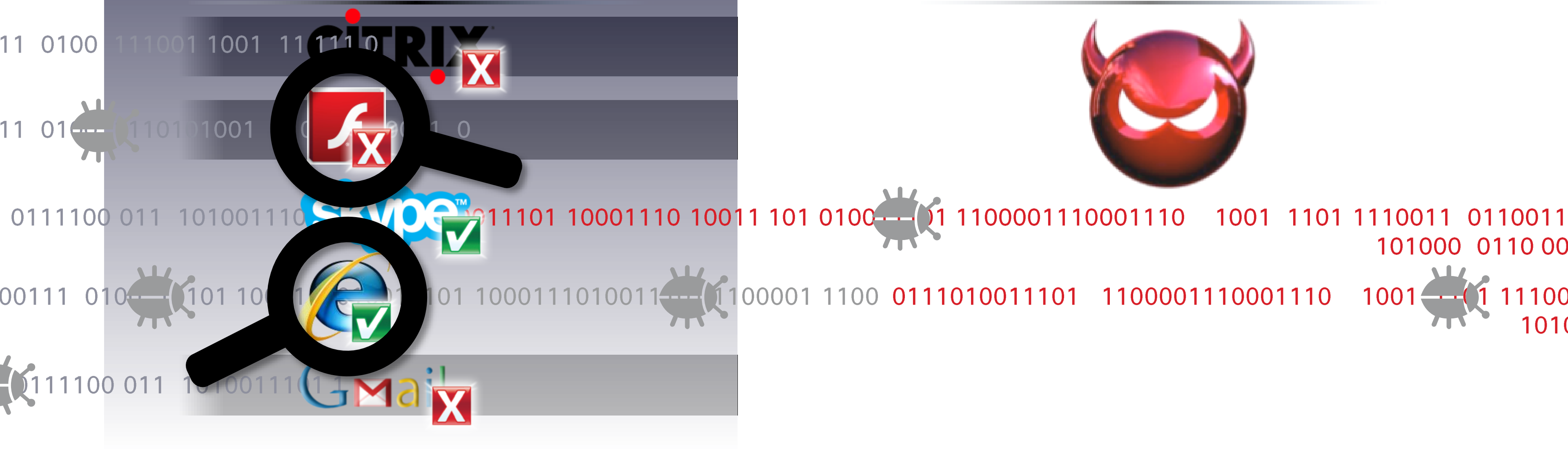
Boardroom Engagement

Misaligned Policies

The Problem with Legacy Next-Generation Firewalls

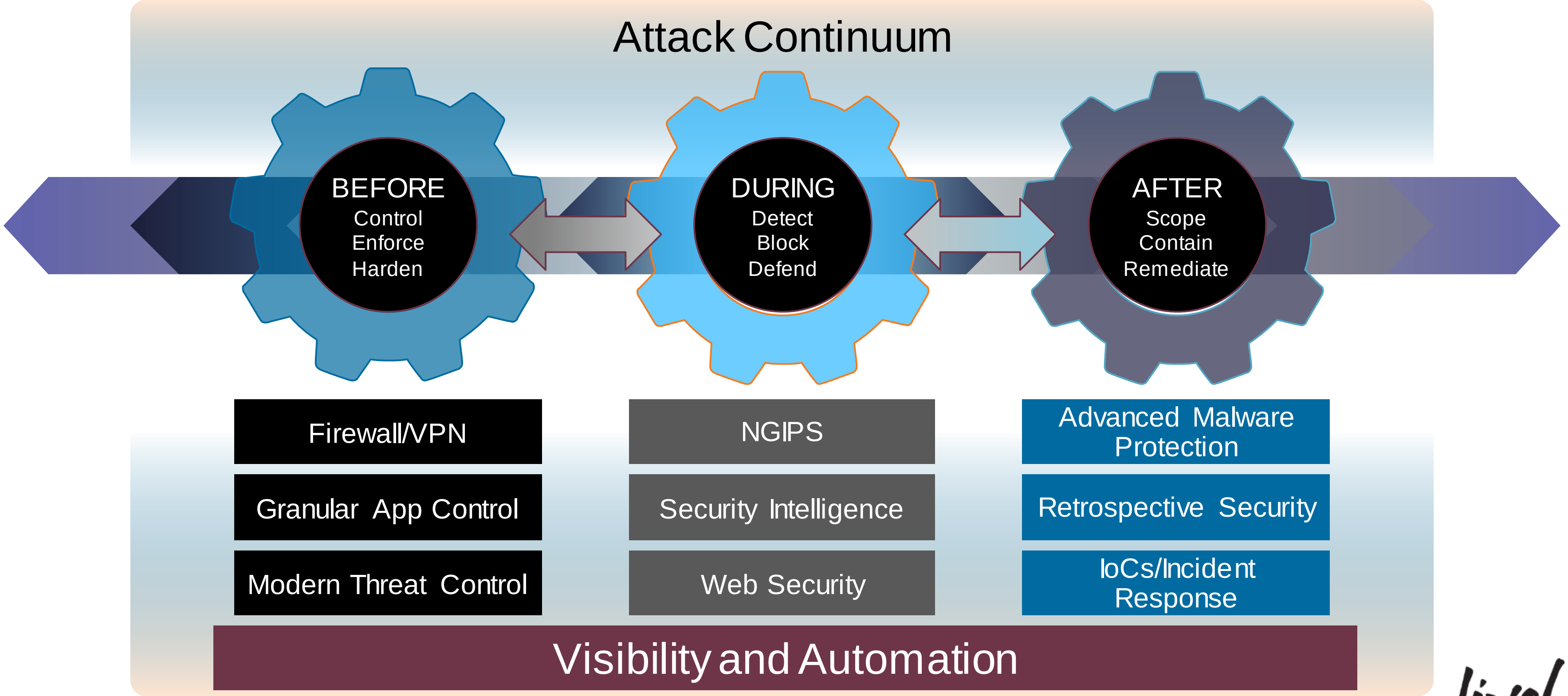
Focus on the Apps

But miss the threat...



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

Integrated Threat Defence Across the Attack Continuum



Attack Continuum

BEFORE
Control
Enforce
Harden

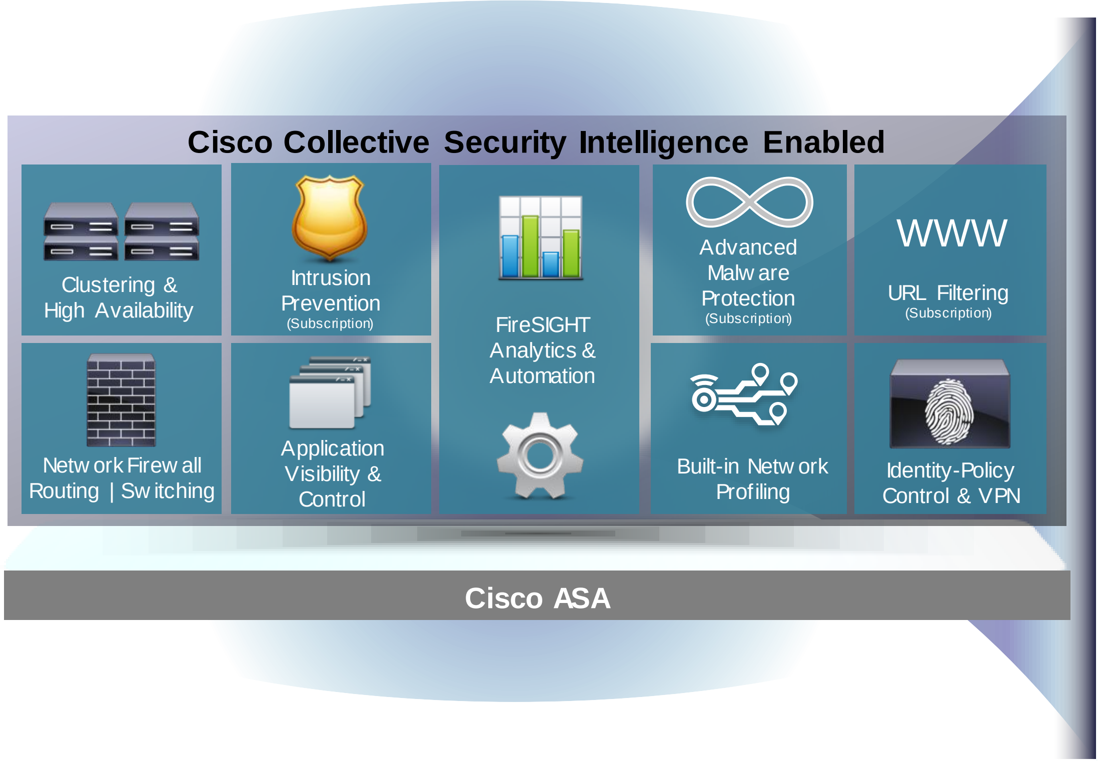
DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

BEFORE	DURING	AFTER
Firewall/VPN	NGIPS	Advanced Malware Protection
Granular App Control	Security Intelligence	Retrospective Security
Modern Threat Control	Web Security	IoCs/Incident Response

Visibility and Automation

Superior Integrated and Multilayered Protection


Cisco Collective Security Intelligence Enabled
Clustering & High Availability
Intrusion Prevention (Subscription)
FireSIGHT Analytics & Automation
Advanced Malware Protection (Subscription)
WWW
URL Filtering (Subscription)
Network Firewall Routing | Switching
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN
Cisco ASA

- ► 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- and Three-Year Term Options

Management

FireSIGHT Management Centre (HW Appliance or Virtual)

Cisco Security Manager (CSM) or ASDM

Support

SmartNET

Software Application Support plus Upgrades

What Platforms Support FirePOWER Services as a Software Module?

Maximum AVC and IPS throughput

300 Mbps NGFW
100K Connections
10,000 CPS

ASA 5512-X

250Mbps NGFW
250K Connections
15,000 CPS

ASA 5515-X

Branch Locations

650Mbps NGFW
500K Connections
20,000 CPS

ASA 5525-X

1 Gbps NGFW
750K Connections
30,000 CPS

ASA 5545-X

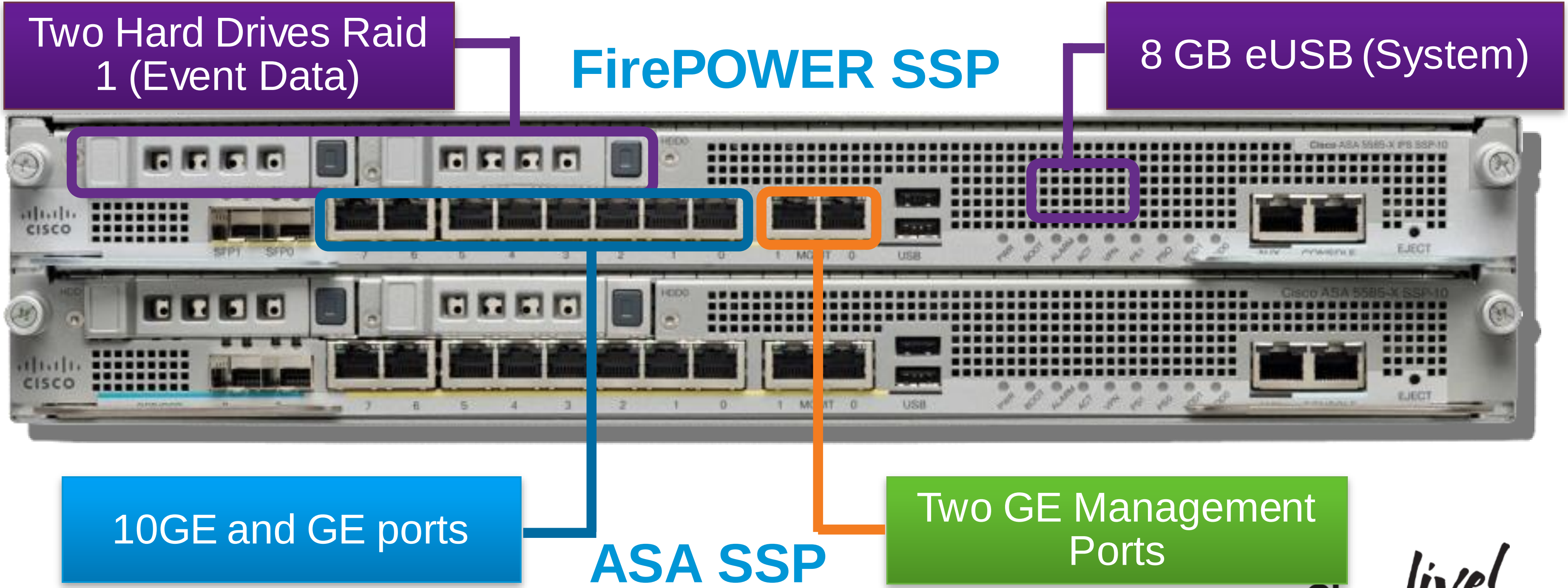
1.25 Gbps NGFW
1 MM Connections
50,000 CPS

ASA 5555-X

Small/Medium Internet Edge

What Platforms Support FirePOWER Hardware Module

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



Two Hard Drives Raid 1 (Event Data)

FirePOWER SSP

8 GB eUSB (System)

10GE and GE ports

ASA SSP

Two GE Management Ports

What Platforms Support FP Hardware Module?

Maximum AVC and IPS throughput

ASA 5585-SSP10

2 Gbps NGFW
500K Connections
40,000 CPS

ASA 5585-SSP20

3.5 Gbps NGFW
1 M Connections
75,000 CPS

Campus / Data Centre

ASA 5585-SSP40

6 Gbps NGFW
1.8 M Connections
120,000 CPS

ASA 5585-SSP60

10 Gbps NGFW
4 M Connections
160,000 CPS

Enterprise Internet Edge

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!**
Events per second (EPS)	2000	6000	12,000	10,000	20,000	**Not upgradeable** **FS-VMW-2-SW-K9** **FS-VMW-10-SW-K9**

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

Management-interface Considerations on ASA5500-X

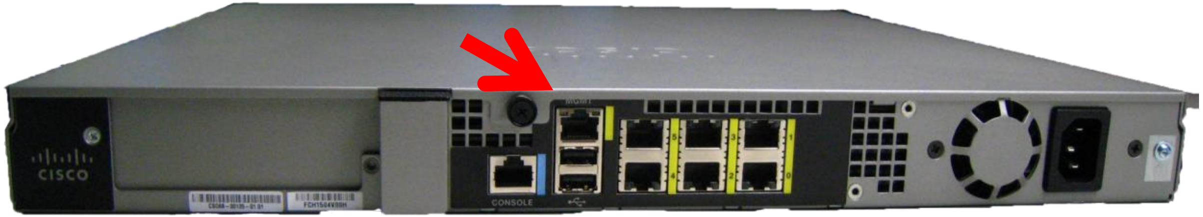
ASA FirePOWER Management Options

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

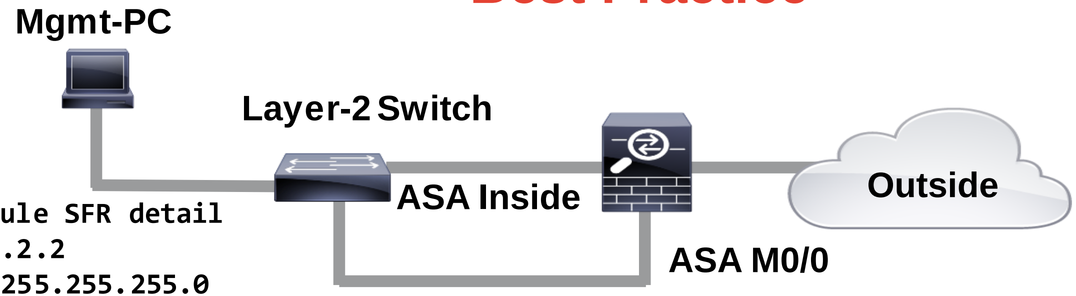
- One **shared** Management interface for ASA and FirePOWER module on ASA5500-X platform
- The FirePOWER module uses Management Interface for
  - all updates (base OS, OS upgrade packages)
  - all feature updates (rules, reputation data)
  - all Management Centre interaction (Mgmt, event-data)
- FireSIGHT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



ASA5500-X FirePOWER Management Interface Considerations (Cont.)

- **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

Best Practice



```
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
```

```
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
```

Agenda

Introduction to NGFW

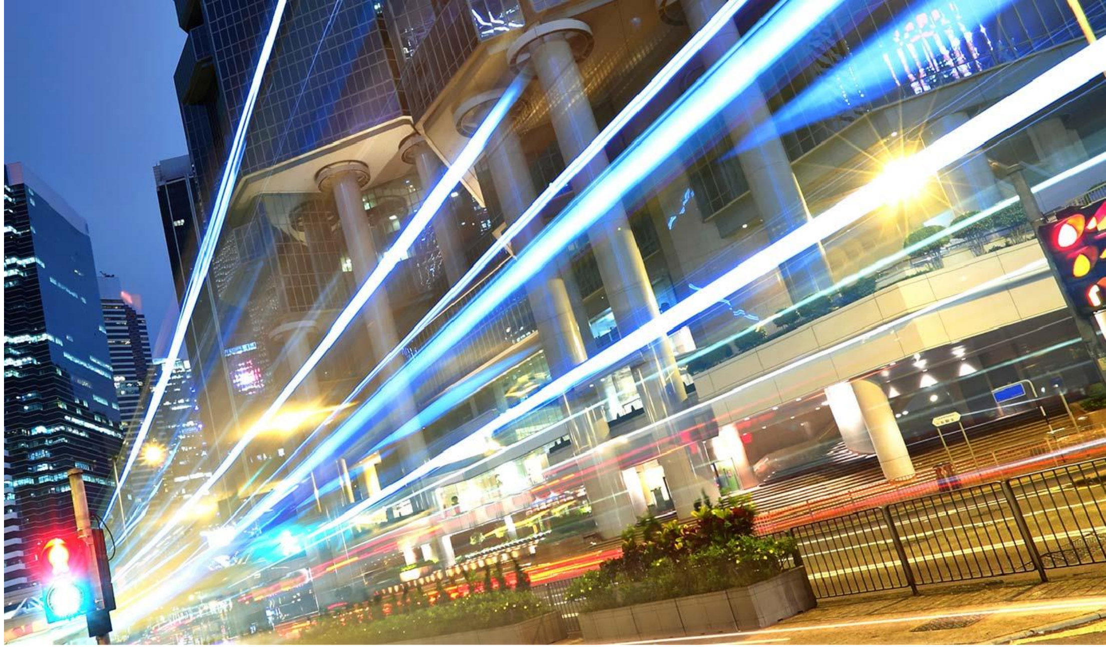
Software Architecture

Licensing

Deployment

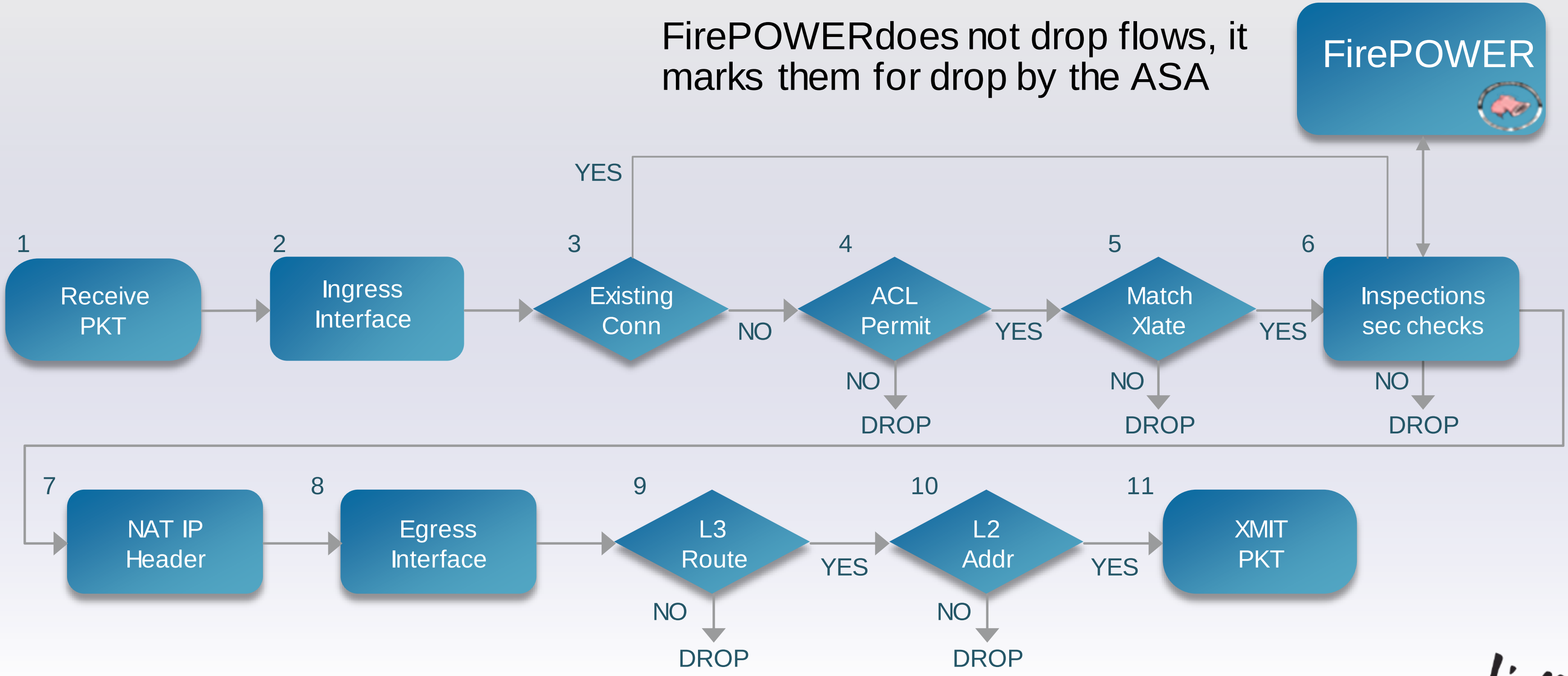
How to configure policies

Management and Eventing



Detailed ASA SFR Packet Flow

FirePOWERdoes not drop flows, it marks them for drop by the ASA



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 normalisation

Snort Technology

Detection Engine:

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

Rules Builder

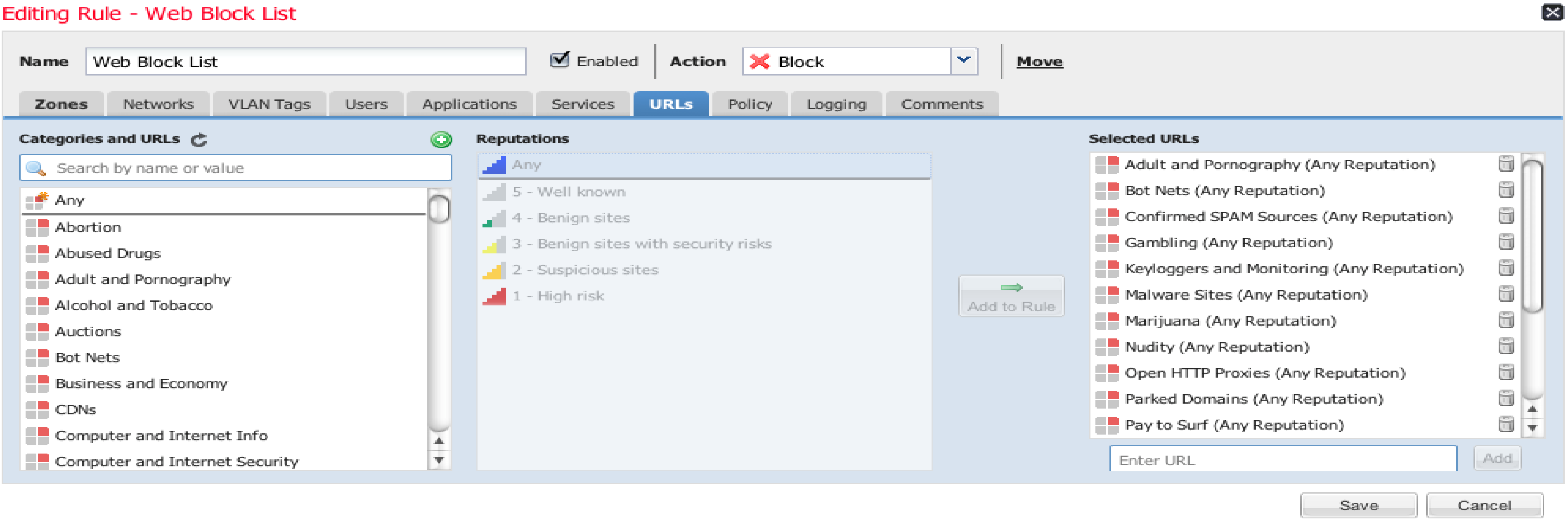
Inspection against the built rules

URL Filtering

URL Filtering

- Block non-business-related sites by category or reputation
- Based on user and user group

URL Filtering



Editing Rule - Web Block List

Name: Web Block List

☑ Enabled

Action: Block

Categories and URLs

- 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)

Cisco Advanced Malware Protection

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

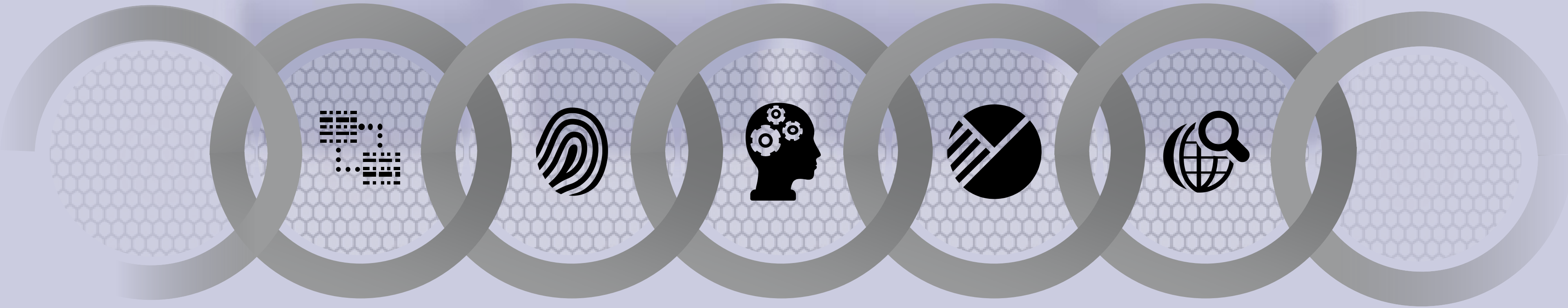
Fire reputation and file sandboxing

Continuous & Zero-Day Detection

Advanced Analytics And Correlation

Advanced Malware Protection

All detection is less than 100%



One-to-One Signature

Fuzzy Finger-Printing

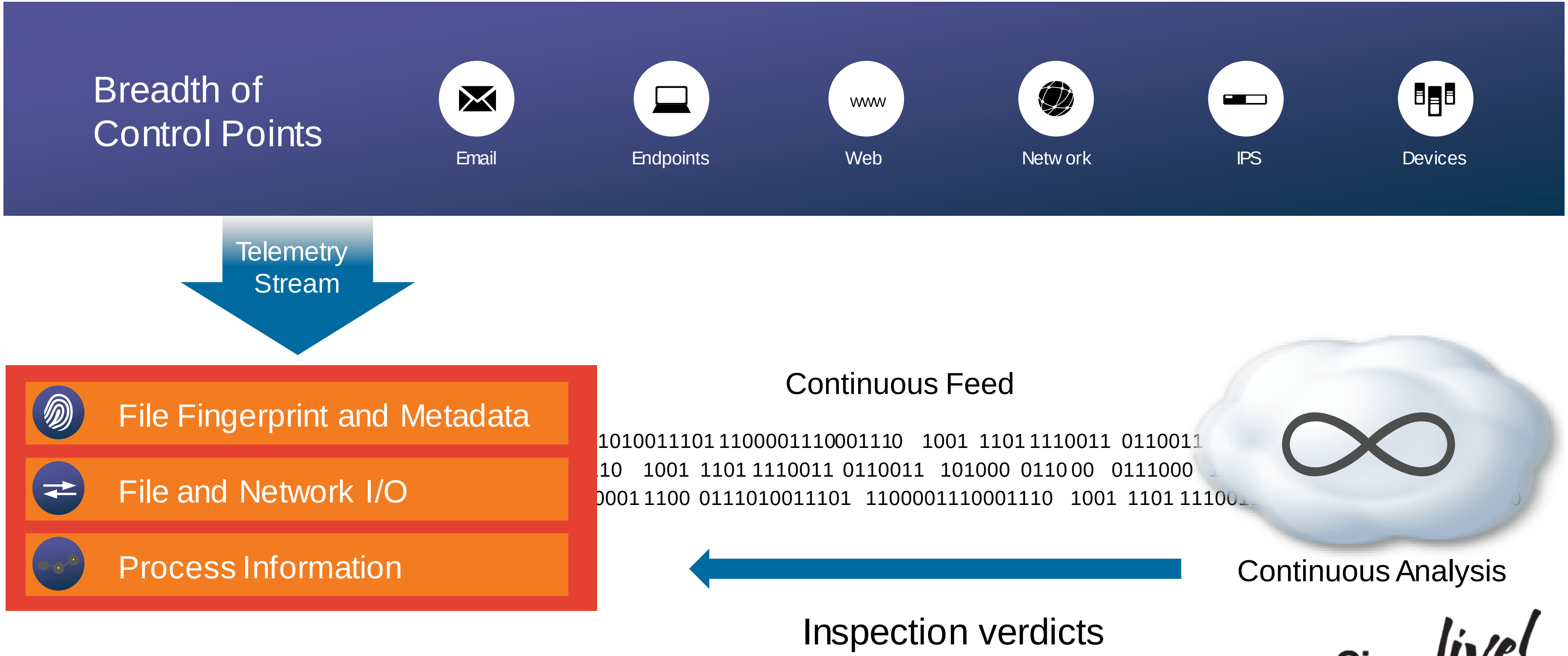
Machine Learning

Advanced Analytics

Dynamic Analysis

Reputation Filtering and File Sandboxing

AMP Provides Continuous Retrospective Security



Breadth of Control Points

Email

Endpoints

Web

Netw ork

IPS

Devices

Telemetry Stream

File Fingerprint and Metadata

File and Network I/O

Process Information

Continuous Feed

1010011101 1100001110001110   1001 1101 1110011 0110011

10   1001 1101 1110011 0110011   101000 0110 00   0111000

0001 1100 0111010011101   1100001110001110   1001 1101 11100

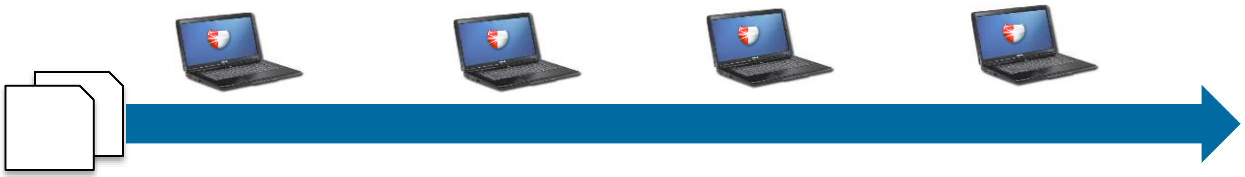
Continuous Analysis

Inspection verdicts

Retrospective Analysis: File Trajectory

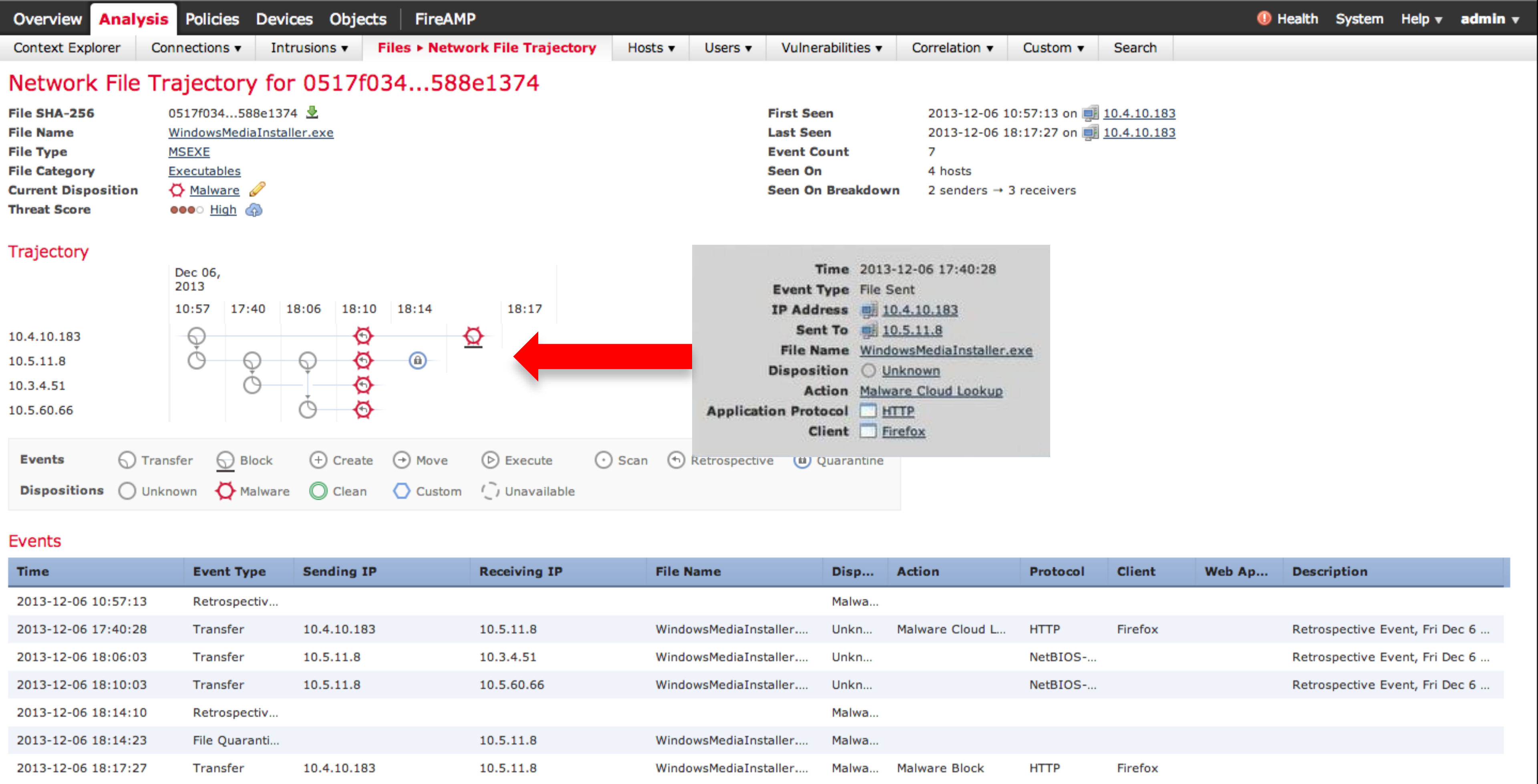
Quickly Understand the Scope of Malware Problem

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?



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 Sent
IP Address	10.4.10.183
Sent To	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

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		

Agenda

Introduction to NGFW

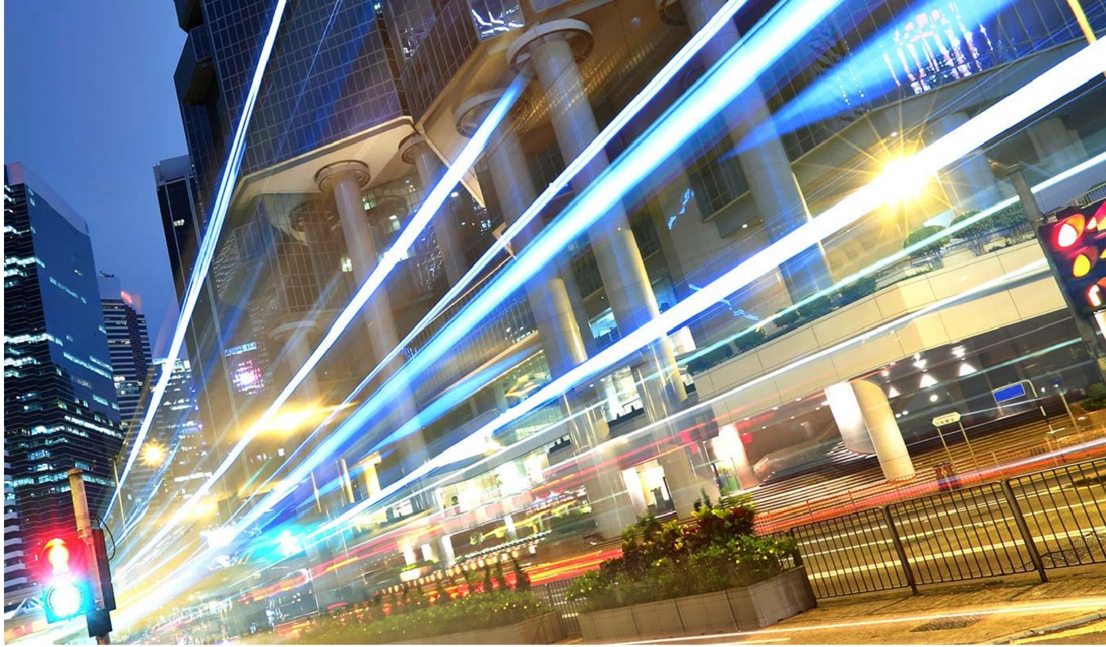
Deployment

Software Architecture

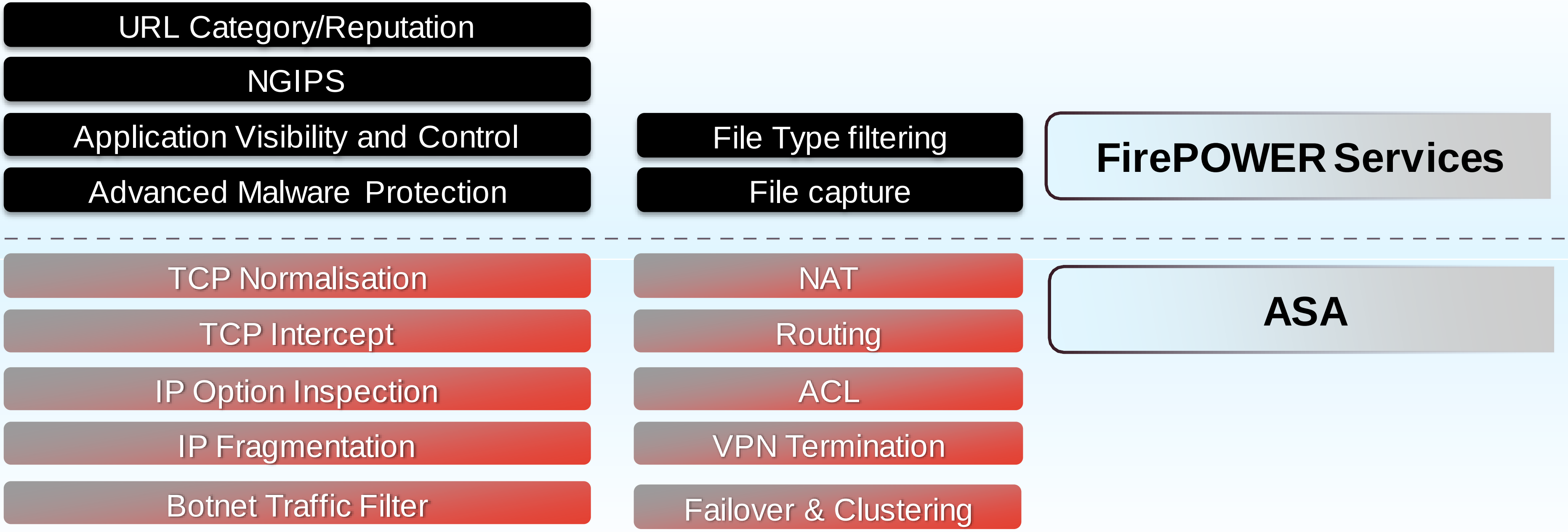
Licensing

How to configure policies

Management and Eventing



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

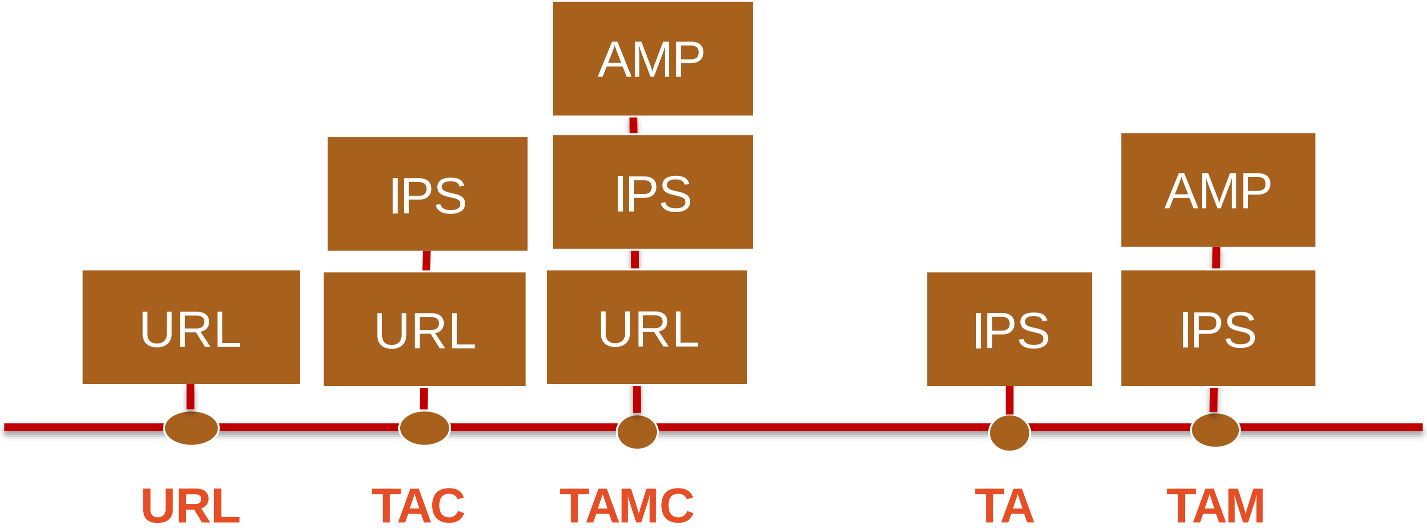
VPN Termination

Failover & Clustering

ASA

Licensing

- Five (5) feature license packages are available
- AVC is part of the default offering
- One (1) and three (3) 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 or 3 year subscriptions

Agenda

Introduction to NGFW

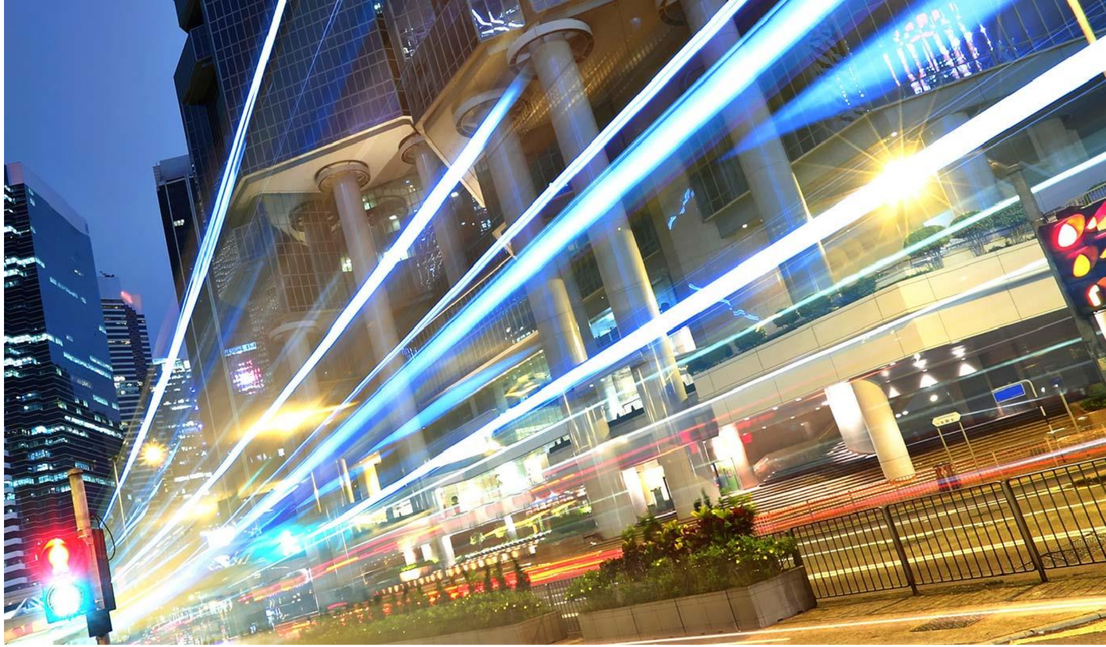
Software Architecture

Licensing

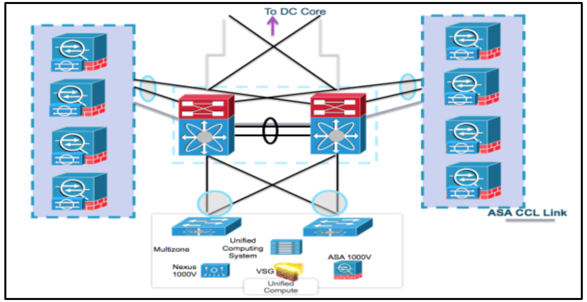
Deployment

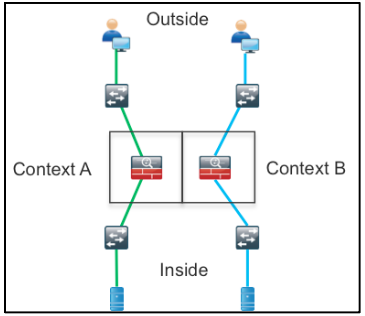
How to configure policies

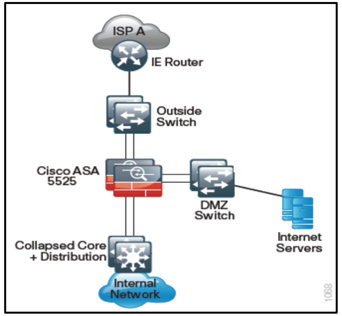
Management and Eventing



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

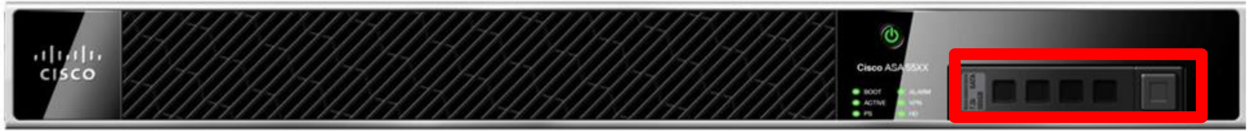
Installing FirePOWER Services

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 OMMITED]
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: Admin123

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:
```

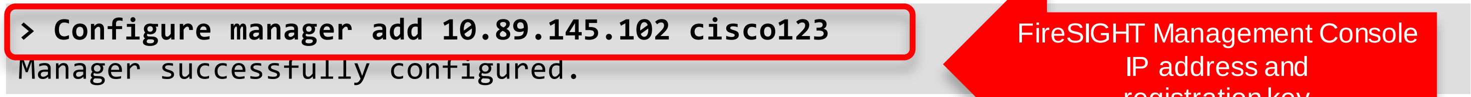
Username: Admin
Password: Sourcefire

- 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

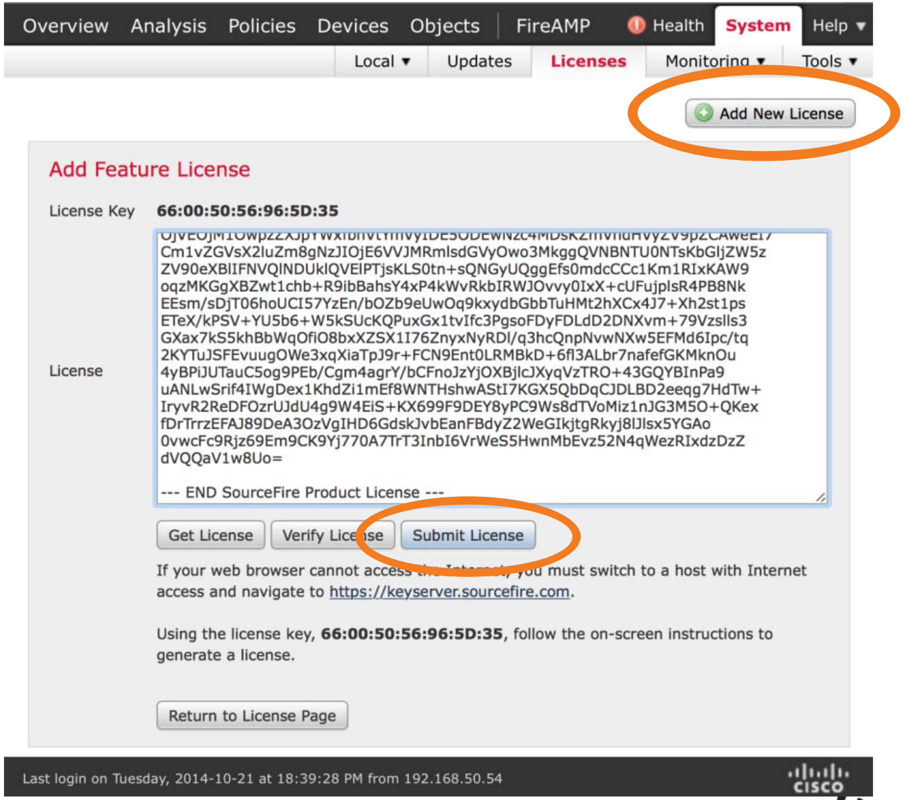
- FirePOWER Services module installs as a software module on Cisco ASA 5500-X platforms and as a hardware module on the Cisco ASA 5585-X
- Both hardware and software modules are managed by the FireSIGHT Management Centre (also known as Defence Centre)
- Traffic is redirected to module using ASA Service 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)



Add Feature License

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

License

```
OjVEOjM1OwpzZXJpYWxfbnVtYmVyIDE5ODEwNzc4MDsKZmVhdHVyZV9pZCAweEI7
Cm1vZGVsX2luZm8gNzJIOjE6VVJMRmlsdGVyOwo3MkggQVNBNTU0NTsKbGljZW5z
ZV90eXBlIFNVQlNDUklQVElPTjsKLS0tn+sQNGyUQggEfs0mdcCCc1Km1RIxKAW9
oqzMKGgXBZwt1chb+R9ibBahsY4xP4kWvRkbIRWJOvvy0IxX+cUFujplsR4PB8Nk
EEsm/sDjT06hoUCI57YzEn/bOZb9eUwOq9kxydbGbbTuHMt2hXCx4J7+Xh2st1ps
ETeX/kPSV+YU5b6+W5kSUcKQPuxGx1tvIfc3PgsoFDyFDLdD2DNXvm+79Vzslls3
GXax7kS5khBbWqOfiO8bxXZSX1I76ZnyxNyRDl/q3hcQnpNvwNXw5EFMd6Ipc/tq
2KYTuJSFEvuugOWe3xqXiaTpJ9r+FCN9Ent0LRMBkD+6fl3ALbr7nafefGKMknOu
4yBPiJUTauC5og9PEb/Cgm4agrY/bCFnoJzYjOXBjlcJXyqVzTRO+43GQYBInPa9
uANLwSrif4IWgDex1KhdZi1mEf8WNTHshwAStI7KGX5QbDqCJDLBD2eeqg7HdTw+
IryvR2ReDFOzrUJdU4g9W4EiS+KX699F9DEY8yPC9Ws8dTVoMiz1nJG3M5O+QKex
fDrTrrzEFAJ89DeA3OzVgIHD6GdskJvbEanFBdyZ2WeGIkjtgRkyj8lJlsx5YGAo
0vwcFc9Rjz69Em9CK9Yj770A7TrT3InbI6VrWeS5HwnMbEvz52N4qWezRIxdzDzZ
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.

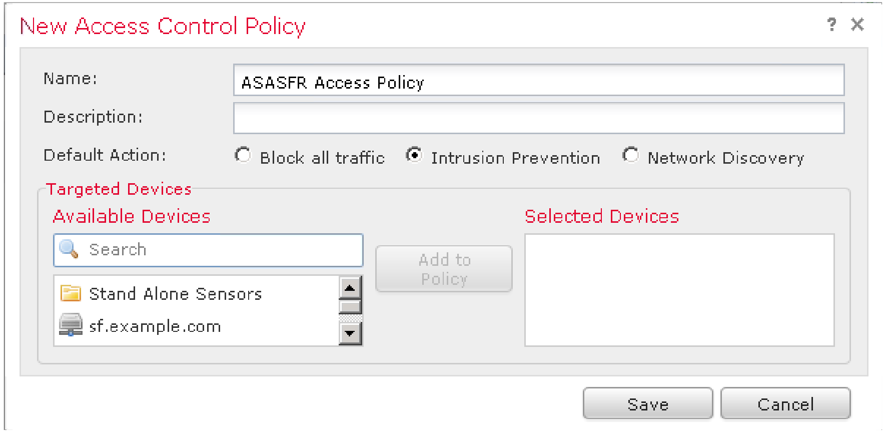
Using the license key, **66:00:50:56:96:5D:35**, follow the on-screen instructions to generate a license.

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

Name: ASASFR Access Policy

Description:

Default Action: ○ Block all traffic ● Intrusion Prevention ○ Network Discovery

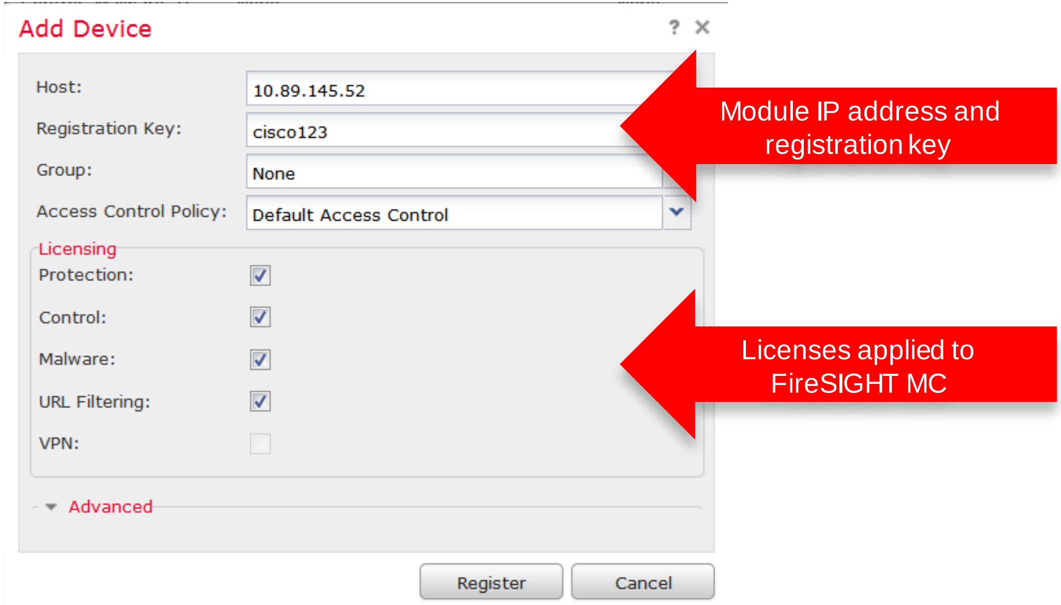
Targeted Devices

Available Devices

Selected Devices

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

Host: 10.89.145.52

Registration Key: cisco123

Group: None

Access Control Policy: Default Access Control

Licensing

Protection: ☑

Control: ☑

Malware: ☑

URL Filtering: ☑

VPN: □

Module IP address and registration key

Licenses applied to FireSIGHT MC

Agenda

Introduction to NGFW

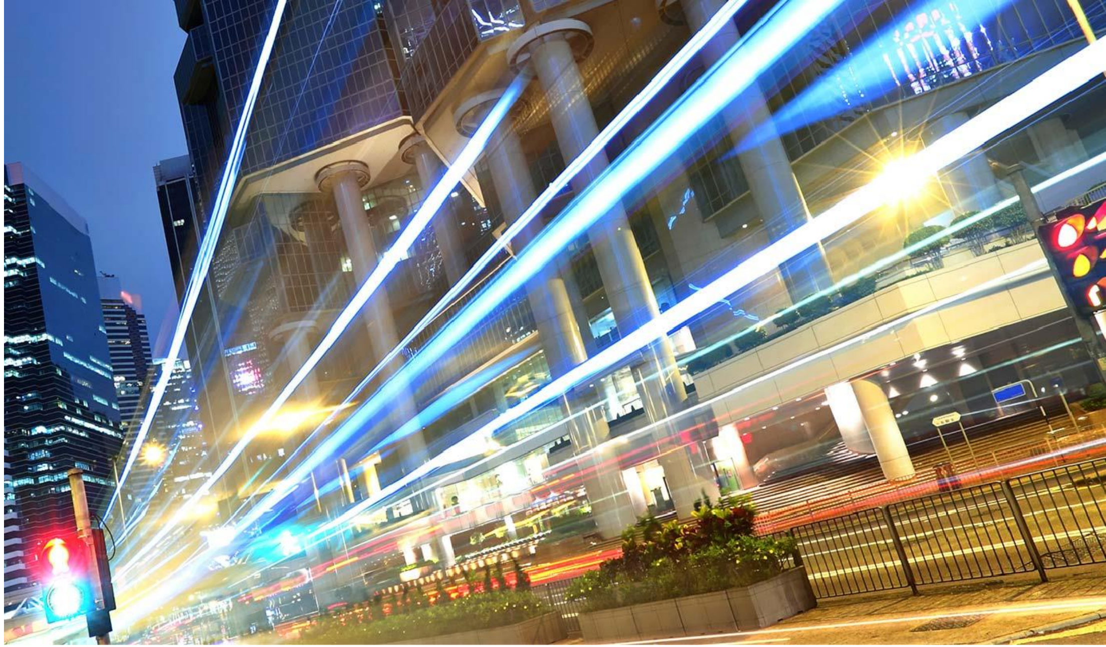
Software Architecture

Licensing

Deployment

Traffic redirection from ASA

Management and Eventing



Compatibility with ASA Features

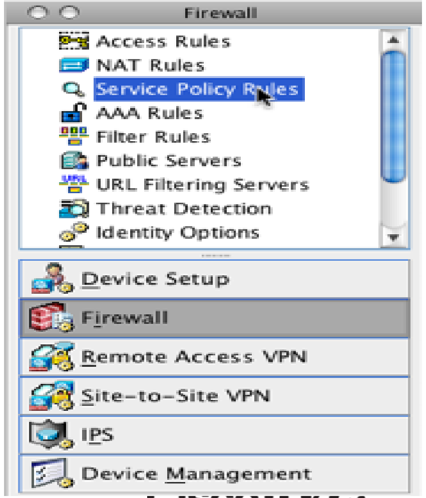
- Minimum ASA version: 9.2.2
- Guidelines for traffic sent to the ASA FirePOWER module:
  - Do not configure ASA inspection on HTTP traffic.
  - Do not configure Cloud Web Security Inspection
  - Other application inspections on the ASA are compatible with the FirePOWER module
  - Do not enable Mobile 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.

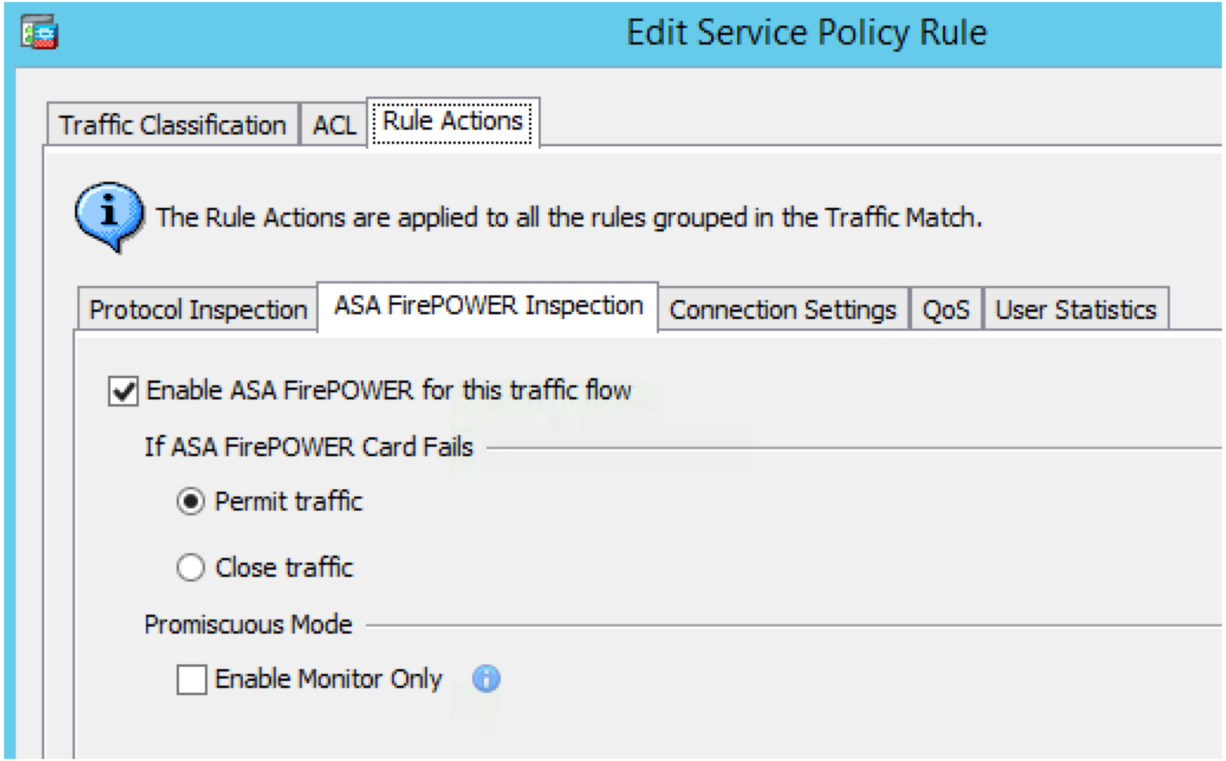
```
policy-map  global_policy
  class  class-default
     sfr  fail-open

service-policy  global_policy global
```



Configure ASA to Redirect Traffic using ASDM

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



Edit Service Policy Rule

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

☑ Enable ASA FirePOWER for this traffic flow

If ASA FirePOWER Card Fails

● Permit traffic

○ Close traffic

Promiscuous Mode

□ Enable Monitor Only

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)

Agenda

Introduction to NGFW

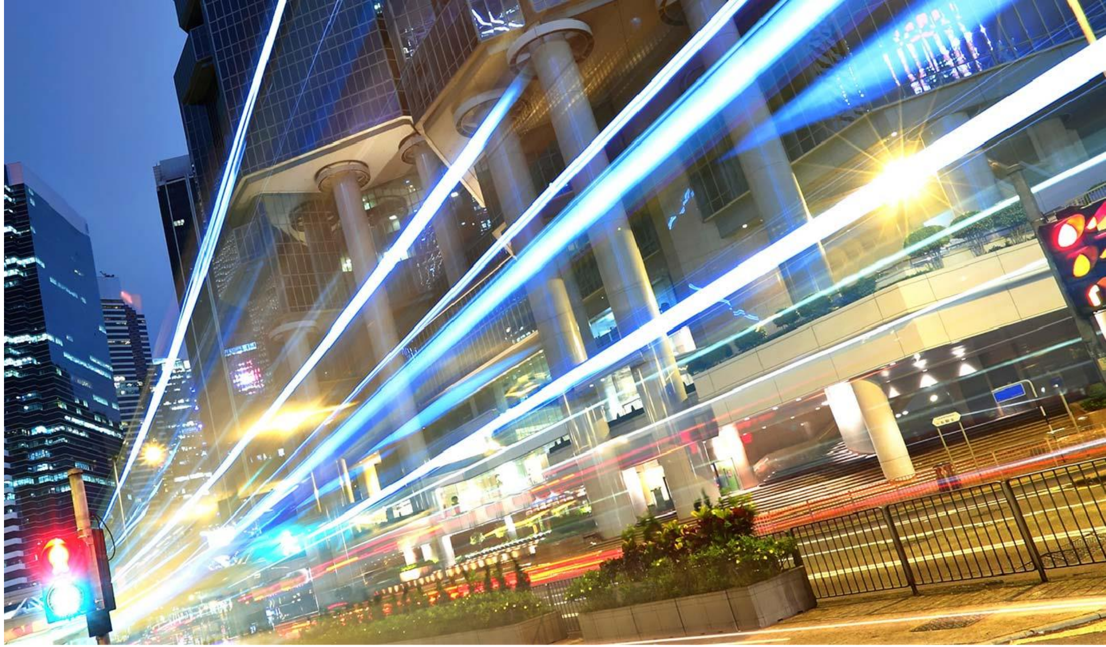
Software Architecture

Licensing

Deployment

How to configure policies

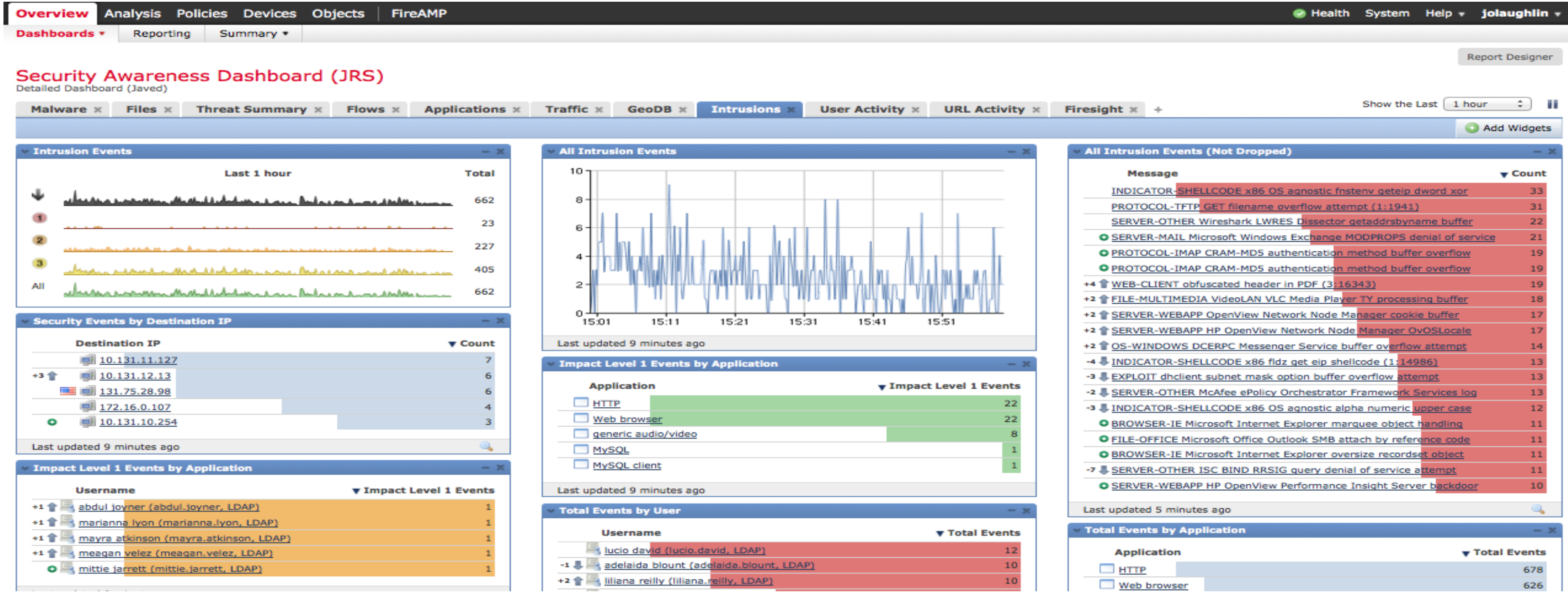
Management and Eventing



FireSIGHT

FireSIGHT Management Centre

Single console for event, policy, and configuration management



Security Awareness Dashboard (JRS)

Detailed Dashboard (Javed)

Intrusion Events

	Last 1 hour	Total
⬇		662
1		23
2		227
3		405
All		662

Security Events by Destination IP

	Destination IP	▼ Count
	10.131.11.127	7
+3 ⬆	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

	Username	▼ Impact Level 1 Events
+1 ⬆	abdul joyner (abdul.joyner, LDAP)	1
+1 ⬆	marianna lyon (marianna.lyon, LDAP)	1
+1 ⬆	mayra atkinson (mayra.atkinson, LDAP)	1
+1 ⬆	meagan velez (meagan.velez, LDAP)	1
○	mittie jarrett (mittie.jarrett, LDAP)	1

All Intrusion Events

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
-1 ⬇	adelaida blount (adelaida.blount, LDAP)	10
+2 ⬆	liliana reilly (liliana.reilly, LDAP)	10

All Intrusion Events (Not Dropped)

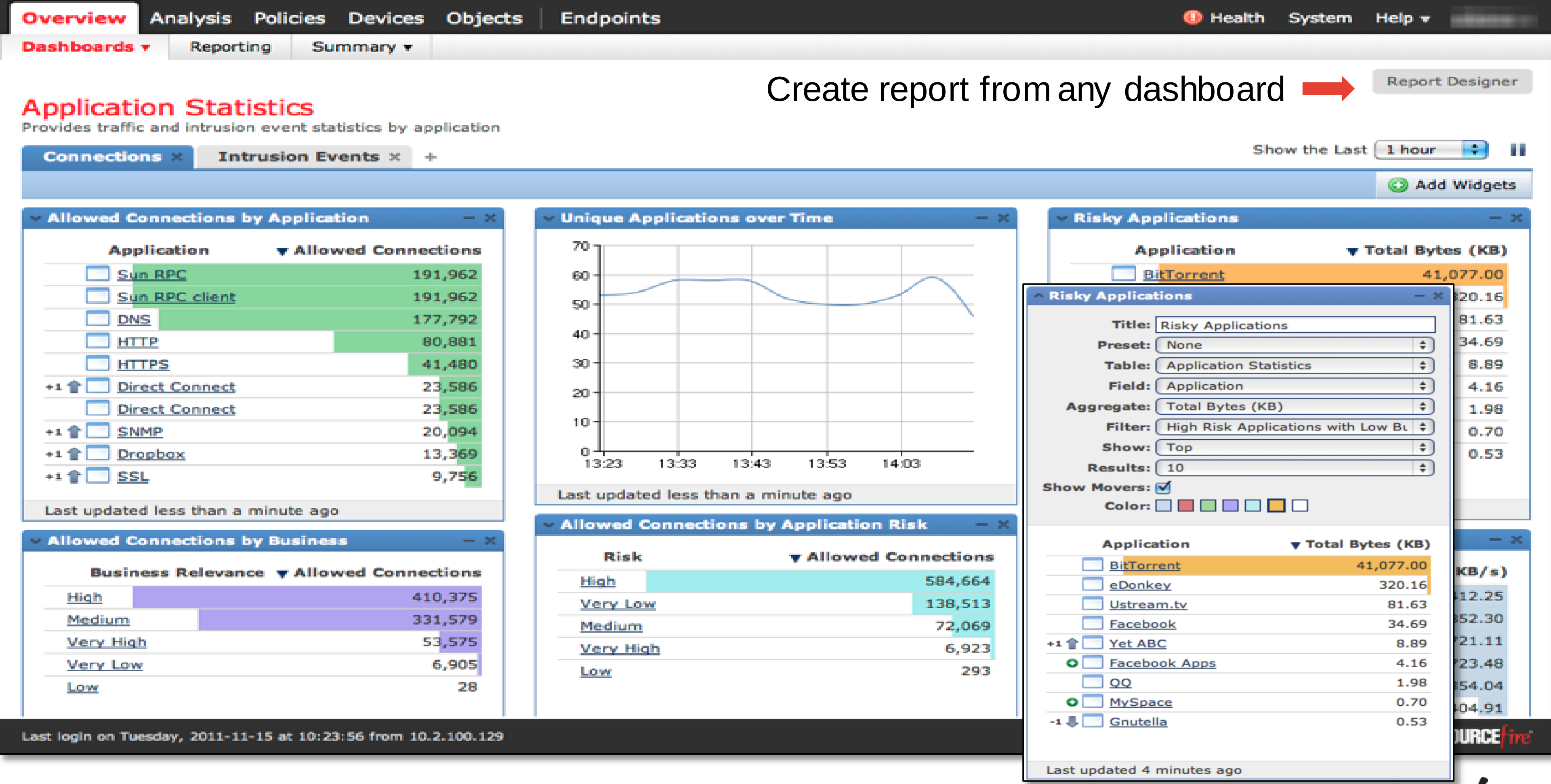
	Message	▼ Count
	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor	33
	PROTOCOL-TFTP GET filename overflow attempt (1:1941)	31
	SERVER-OTHER Wireshark LWRES Dissector getaddrsbyname buffer	22
○	SERVER-MAIL Microsoft Windows Exchange MODPROPS denial of service	21
○	PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
○	PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
+4 ⬆	WEB-CLIENT obfuscated header in PDF (3:16343)	19
+2 ⬆	FILE-MULTIMEDIA VideoLAN VLC Media Player TY processing buffer	18
+2 ⬆	SERVER-WEBAPP OpenView Network Node Manager cookie buffer	17
+2 ⬆	SERVER-WEBAPP HP OpenView Network Node Manager OvOSLocale	17
+2 ⬆	OS-WINDOWS DCERPC Messenger Service buffer overflow attempt	14
-4 ⬇	INDICATOR-SHELLCODE x86 fldz get eip shellcode (1:14986)	13
-3 ⬇	EXPLOIT dhclient subnet mask option buffer overflow attempt	13
-2 ⬇	SERVER-OTHER McAfee ePolicy Orchestrator Framework Services log	13
-3 ⬇	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
-7 ⬇	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



Application Statistics

Provides traffic and intrusion event statistics by application

Allowed Connections by Application

	Application	▼ Allowed Connections
	Sun RPC	191,962
	Sun RPC client	191,962
	DNS	177,792
	HTTP	80,881
	HTTPS	41,480
+1	Direct Connect	23,586
	Direct Connect	23,586
+1	SNMP	20,094
+1	Dropbox	13,369
+1	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)
BitTorrent	41,077.00

Allowed Connections by Business

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

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

Title: Risky Applications

Preset: None

Table: Application Statistics

Field: Application

Aggregate: Total Bytes (KB)

Filter: High Risk Applications with Low Bu

Show: Top

Results: 10

Show Movers: ☑

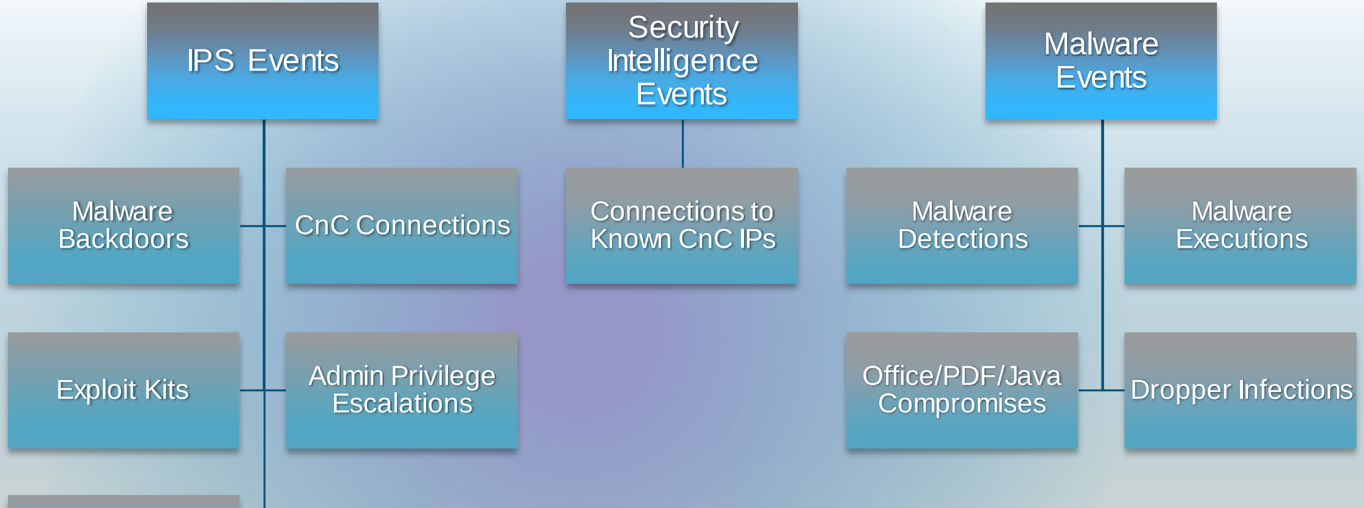
Color: □ 🟥 🟩 🟪 □ 🟧 □

	Application	▼ Total Bytes (KB)
	BitTorrent	41,077.00
	eDonkey	320.16
	Ustream.tv	81.63
	Facebook	34.69
+1	Yet ABC	8.89
⊕	Facebook Apps	4.16
	QQ	1.98
⊕	MySpace	0.70
-1	Gnutella	0.53

Last updated 4 minutes ago

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

Indications of Compromise (IoCs)



IPS Events

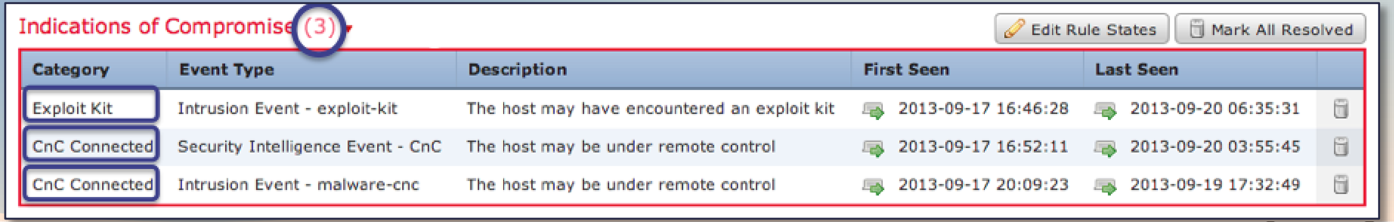
- Malware Backdoors
- CnC Connections
- Exploit Kits
- Admin Privilege Escalations
- Web App Attacks

Security Intelligence Events

- Connections to Known CnC IPs

Malware Events

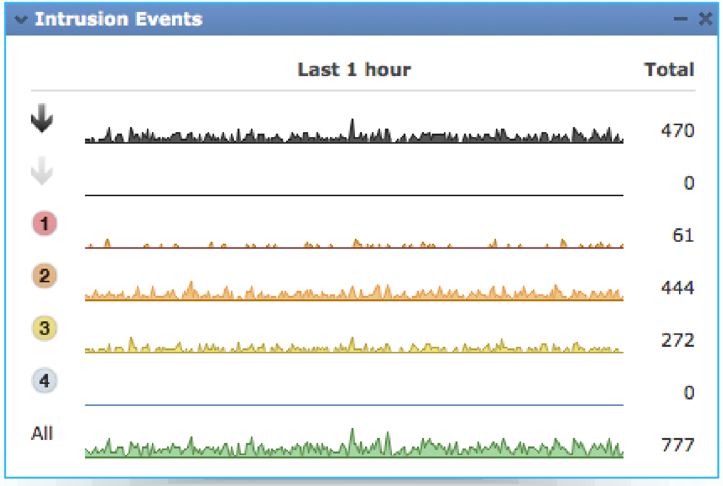
- Malware Detections
- Malware Executions
- Office/PDF/Java Compromises
- Dropper Infections



Indications of Compromise (3)

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



Intrusion Events

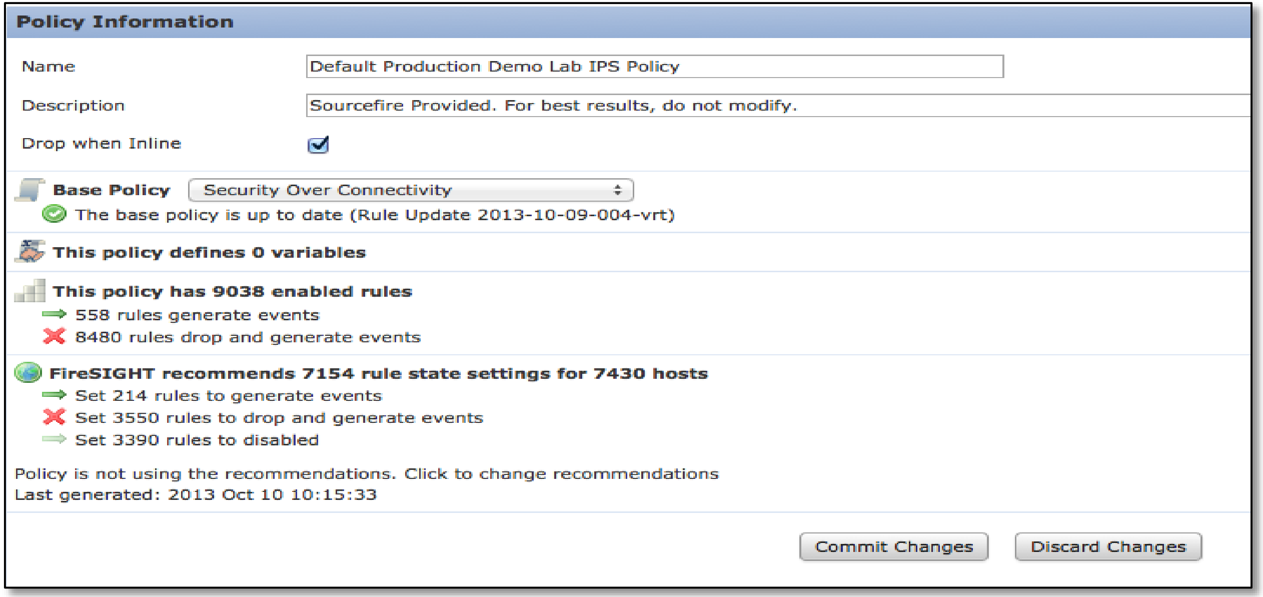
	Last 1 hour	Total
↓		470
↓		0
1		61
2		444
3		272
4		0
All		777

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: Default Production Demo Lab IPS Policy

Description: Sourcefire Provided. For best results, do not modify.

Drop when Inline ☑

Base Policy Security Over Connectivity

✓ 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

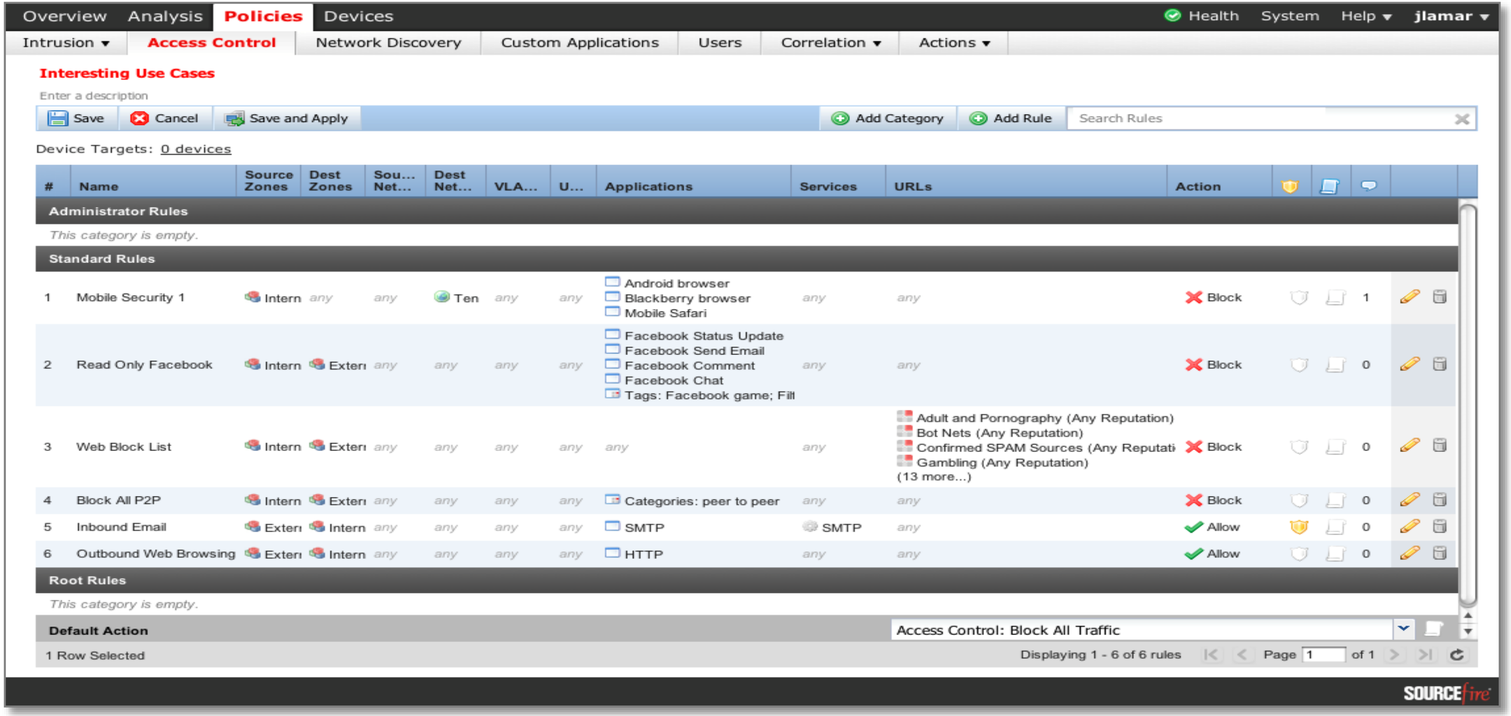
→ Set 214 rules to generate events

✗ 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



Interesting Use Cases

Enter a description

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	Exteri	any	any	any	any	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game; Filt	any	any	Block			0
3	Web Block List	Intern	Exteri	any	any	any	any	any	any	Adult and Pornography (Any Reputation) Bot Nets (Any Reputation) Confirmed SPAM Sources (Any Reputati Gambling (Any Reputation) (13 more…)	Block			0
4	Block All P2P	Intern	Exteri	any	any	any	any	Categories: peer to peer	any	any	Block			0
5	Inbound Email	Exteri	Intern	any	any	any	any	SMTP	SMTP	any	Allow			0
6	Outbound Web Browsing	Exteri	Intern	any	any	any	any	HTTP	any	any	Allow			0
Root Rules														
This category is empty.														

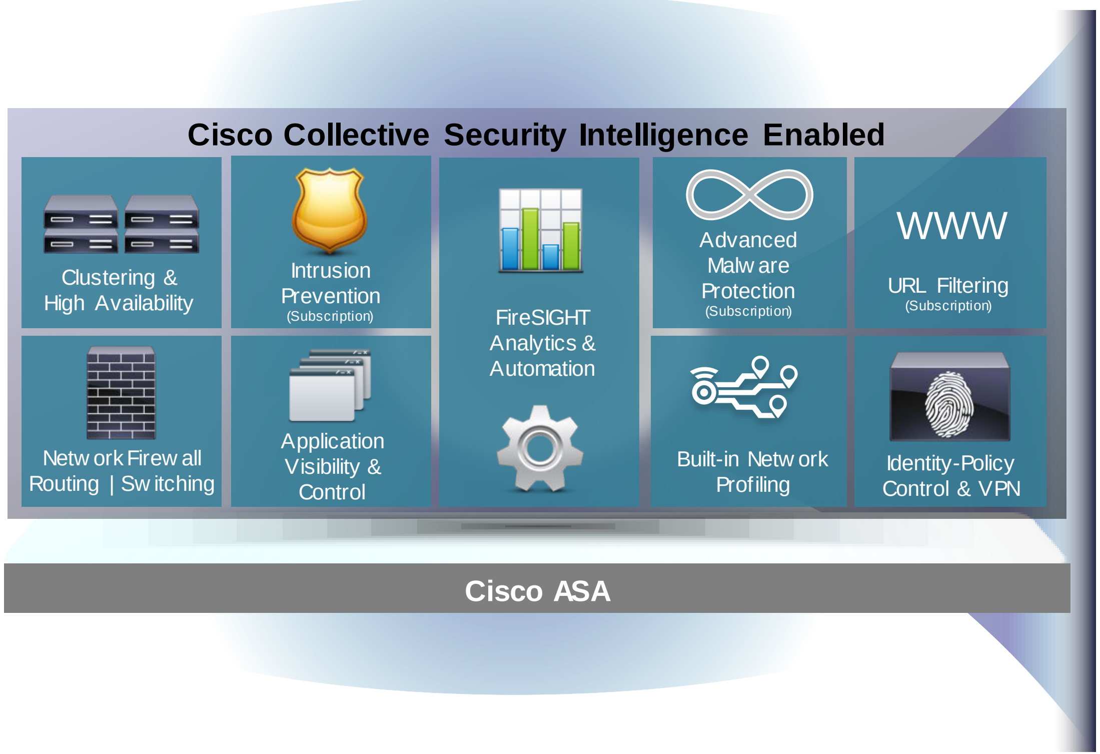
Default Action Access Control: Block All Traffic

1 Row Selected

Displaying 1 - 6 of 6 rules Page 1 of 1

Summary: Cisco ASA with FirePOWER Services

Industry's First Adaptive, Threat-Focused NGFW



Cisco Collective Security Intelligence Enabled
Clustering & High Availability
Intrusion Prevention (Subscription)
FireSIGHT Analytics & Automation
Advanced Malware Protection (Subscription)
WWW
URL Filtering (Subscription)
Network Firewall Routing | Switching
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN
Cisco ASA

- ▶ 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&relind=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:

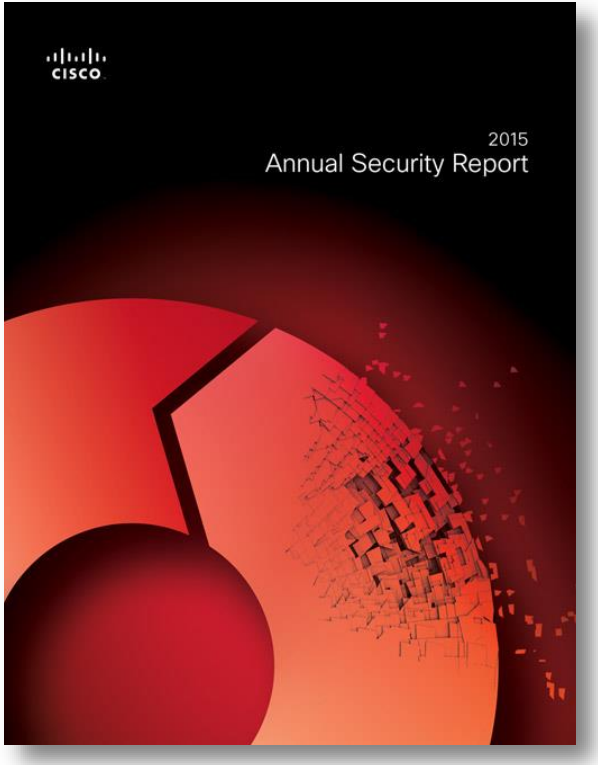
http://www.cisco.com/c/dam/en/us/td/docs/security/firesight/531/PDFs/FireSIGHT-System-Installation-Guide-Version-5-3-1.pdf

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-2088 - Using Cisco FireSIGHT system to protect ICS / IoT Systems
- BRKSEC-2134 - Building a Highly Secure Internet Edge
- BRKSEC-2762 - The FirePOWER Platform and Next Generation Network Security
- BRKSEC-3126 - Configuration and Tuning of FirePOWER Services for ASA
- LABSEC-2339 - Cisco ASA with FirePOWER services



Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015

Q & A

Complete Your Online Session Evaluation

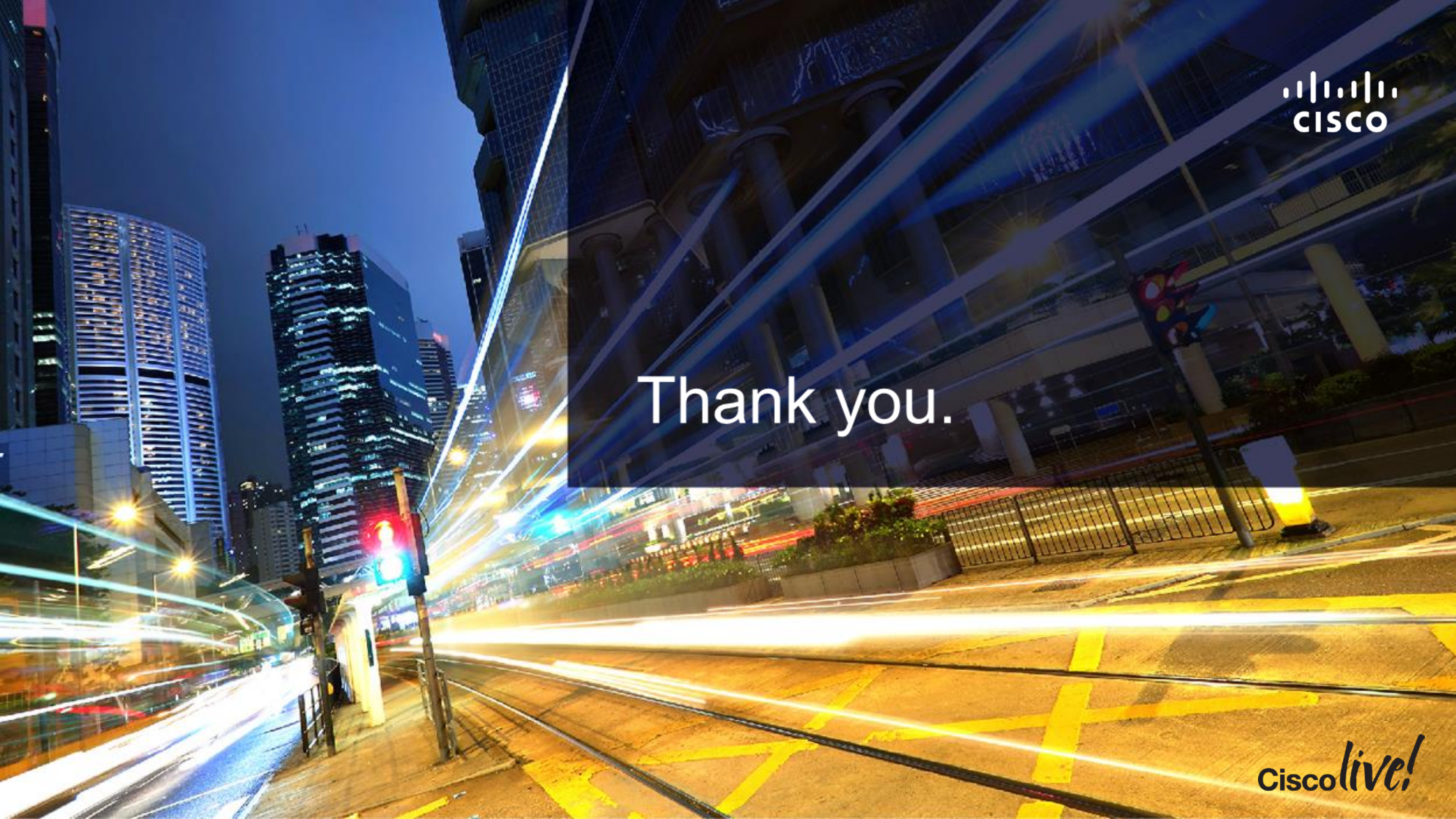
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

cisco