



FirePOWER Services for Cisco ASA (FPSASA)

Cisco TAC BN team 刘洋

Apr 2015



Objectives

Upon completing this lesson, you will be able to meet the following objectives:

- Describe the key benefits of the Cisco ASA with FirePOWER Services*
- Describe the ASA models that support FirePOWER Services*
- Describe the features and licensing of Cisco ASA with FirePOWER Services*
- Describe the high-level architecture and packet flow of the solution*

NGIPS

- Standard first-gen IPS
- Application awareness and full-stack visibility
- Context awareness
- Content awareness
- Agile engine

NGFW

- Standard first-gen firewall
- Application awareness and full-stack visibility
- Integrated network IPS

“Next-generation network IPS will be incorporated within a next-generation firewall, but most next-generation firewall products currently include first-generation IPS capabilities.”

NGIPS

- Standard first-gen IPS
- Application awareness and full-stack visibility
- Context awareness
- Content awareness
- **Agile engine**

NGFW

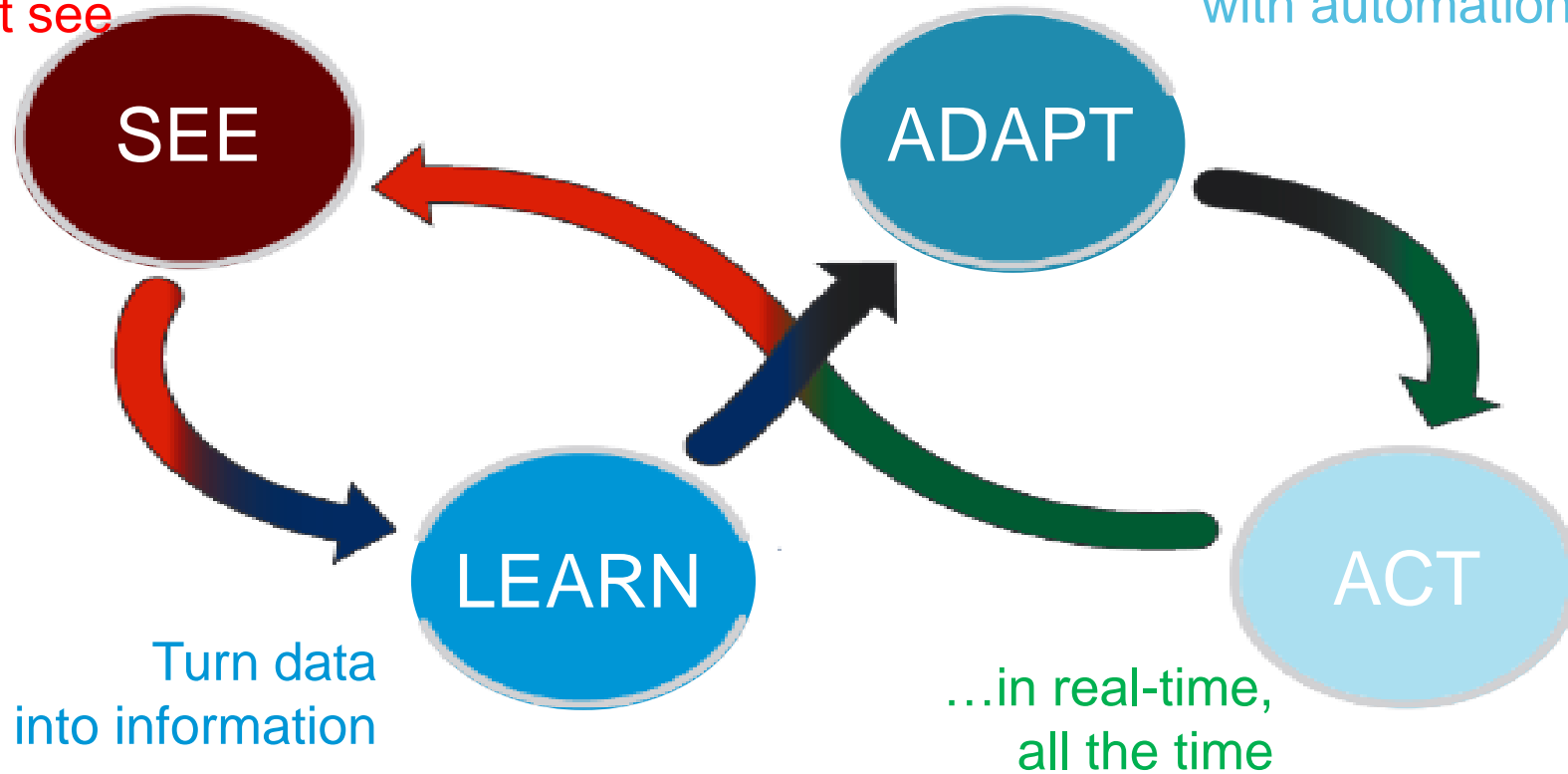
- Standard first-gen firewall
- Application awareness and full-stack visibility
- Integrated network IPS

“Next-generation network IPS will be incorporated within a next-generation firewall, but most next-generation firewall products currently include first-generation IPS capabilities.”

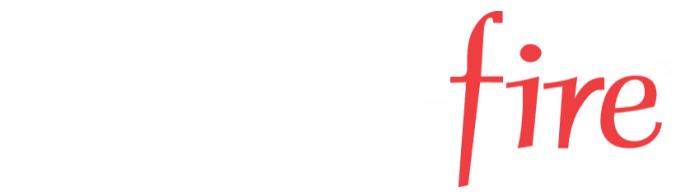
SOURCEfire®

∞
Agile Security®

You can't protect what
you can't see



Better Together



A New, Adaptive Threat-focused NGFW & NGIPS

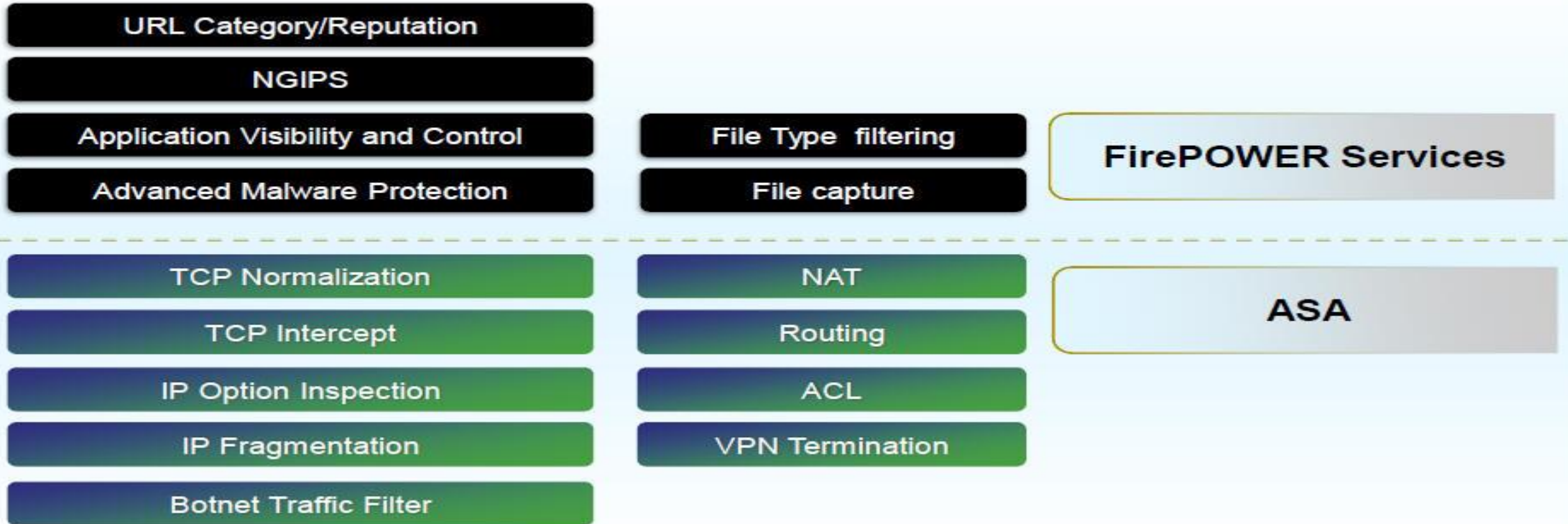
Cisco ASA integrated with the Cisco Sourcefire sensor brings industry-leading network security IPS together with an industry-leading network firewall.

ASA and FirePOWER –Together (NGIPS & NGFW)

The Cisco ASA with FirePOWER Services brings together two mature industry-leading products

- Cisco ASA
 - Best-of-breed stateful inspection firewall
 - Applies NAT to embedded application protocol data
 - Integrates with many other solutions, including: Unified Communications technologies, Active Directory, LDAP etc.
 - Acts as a VPN termination: Site-to-site, remote access, and clientless SSL VPN
 - ASA provides ingress and egress processing for the Sourcefire module
 - Ingress – ACLs, IP defragmentation, TCP normalization, TCP intercept
 - Egress – ACLs, NAT, routing
-
- Sourcefire FirePOWER services
 - URL filtering to enforce acceptable use - Application visibility and control (AVC)
 - Threat protection (NGIPS) and Advanced Malware Protection (AMP)

Functional Distribution of Features



FireSIGHT

A FireSIGHT license is included with your Defense Center and is required to perform host, application, and user discovery ,geographical. on your Defense Center determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering (IP blacklist whitelist).

Control

A Control license allows managed devices to perform user (AD .ldap) and application control.

A Control license requires a Protection license

URL Filtering

A URL Filtering license allows managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts.

A URL Filtering license requires a Protection license

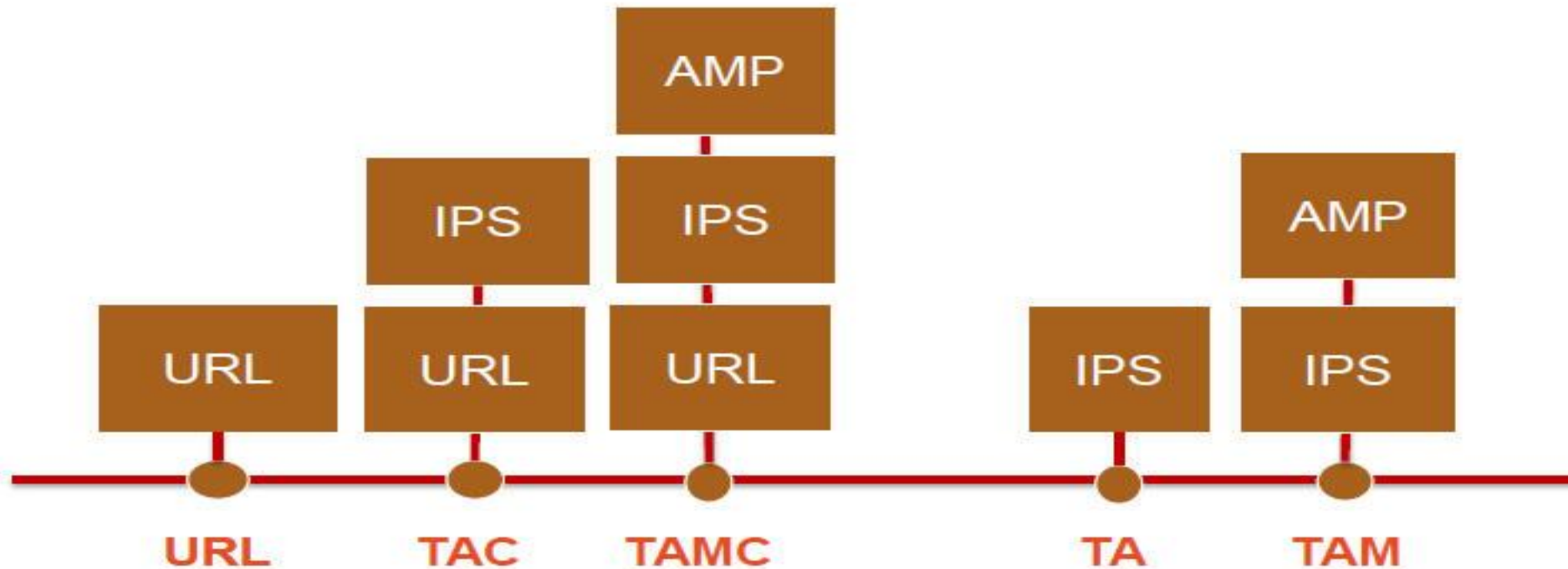
Malware

A Malware license allows managed devices to detect and block malware in files transmitted over your network.
advanced malware protection (AMP)

A Malware license requires a Protection license

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



Cisco FirePOWER Services are supported in software on the Cisco ASA 5500-X platforms, and via FirePOWER Services modules on the Cisco ASA 5585

Cisco Multi-scale Performance

Security for the Internet Edge

**ASA5500x with FirePOWER
Soft module**

**1 Gbps Max
100K Connections
10,000 CPS**



ASA 5512-X

**1.2 Gbps Max
250K Connections
15,000 CPS**



ASA 5515-X

**2 Gbps Max
500K Connections
20,000 CPS**



ASA 5525-X

**3 Gbps Max
750K Connections
30,000 CPS**



ASA 5545-X

**4 Gbps Max
1M Connections
50,000 CPS**



ASA 5555-X

Branch Locations

Small / Medium Internet Edge

Cisco Multi-scale Performance

Security for the Enterprise and Data Center

ASA5585 FirePOWER with Hardware module



ASA 5585-SSP10

**4 Gbps Max
1 Million
Connections
50,000 CPS**



ASA 5585-SSP20

**10 Gbps Max
2 Million
Connections
125,000 CPS**



ASA 5585-SSP40

**20 Gbps Max
4 Million
Connections
200,000 CPS**



ASA 5585-SSP60

**40 Gbps Max
10 Million
Connections
360,000 CPS**

Enterprise Internet Edge and Data Center

Cisco ASA with FirePOWER Services devices are managed via the FireSIGHT Management Center (FMC) ensures management and policy uniformity across all FirePOWER enabled systems

FireSIGHT Management Center Models

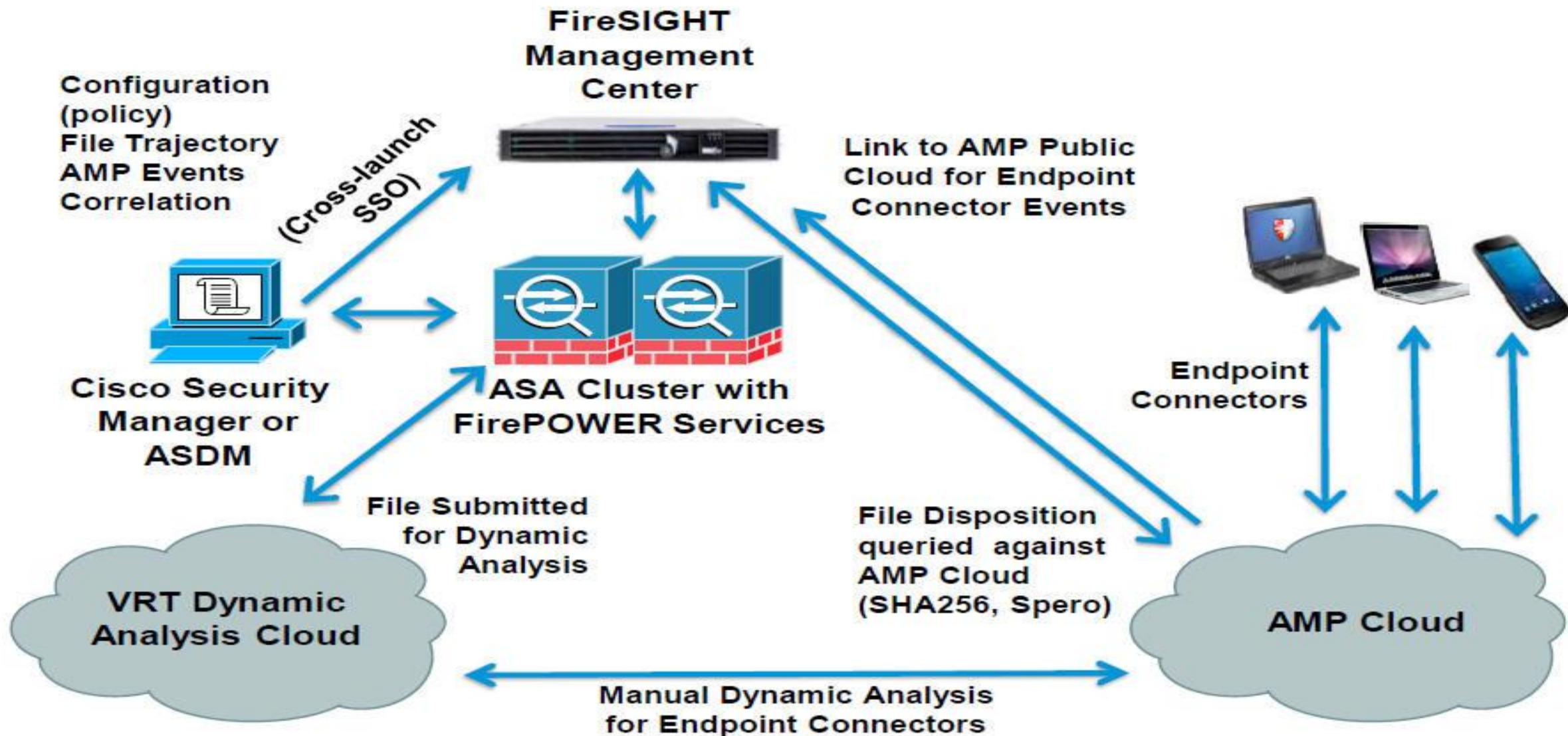
	750	1500	2000	3500	4000	Virtual
Max. Devices Managed	10	35	70	150	300	Virtual FireSIGHT Management Center Up to 25 Managed Devices
Event Storage	100 GB	125 GB	1.8 TB	400 GB	4.8/6.3 TB	
Max. Network Map (hosts / users)	2K/2K	50K/50K	150K/150K	300K/300K	600K/600K	Virtual FireSIGHT Management Center offerings limited to 2 or 10 Managed Devices FS-VMW-2-SW-K9 FS-VMW-10-SW-K9
Events per Sec (EPS)	2000	6000	12000	10000	20000	

FirePOWER Services for ASA Data Sheet (Draft)

- It is planned that FirePOWER Services for ASA will include both a maximum throughput number as well as a 440 Byte HTTP number more relevant for sizing.

Model	5512-X	5515-X	5525-X	5545-X	5555-X	5585-10	5585-20	5585-40	5585-60
Maximum Application Control Throughput in Mbps	300	500	1100	1500	1750	4500	7000	10000	15000
Maximum Application Control and IPS Throughput in Mbps	150	250	650	1000	1250	2000	3500	6000	10000
Application Control or IPS Sizing Throughput in Mbps (440 Byte HTTP)	100	150	375	575	725	1200	2000	3500	6000

Sample Solution Architecture with Management



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)

Packet Flow Overview

Packet flow between the solution components

1. Ingress processing – inbound ACLs, IP defragmentation, TCP normalization, 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)

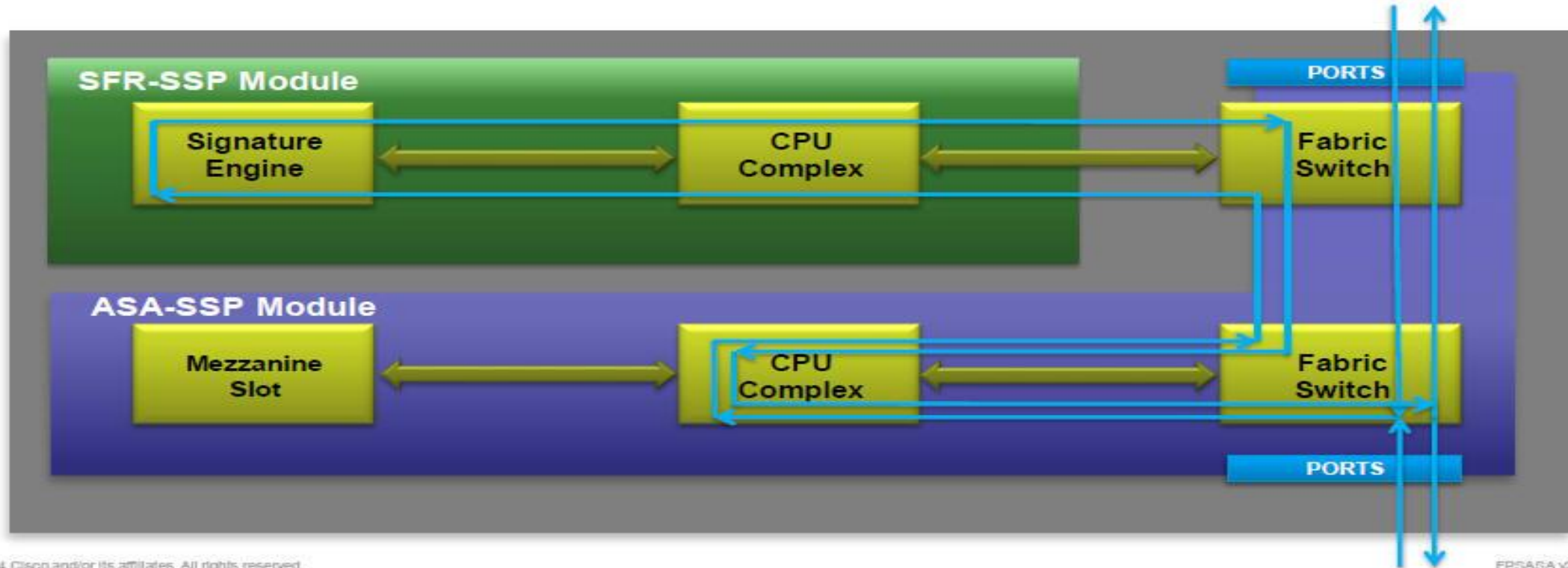
- MPF is a well known component of ASA architecture.
- MPF supports fail-open, fail-closed and monitor only options
- MPF class map, policy map and service policy determine which traffic is send to the FirePOWER Services module:
- Example of MPF configuration to send all traffic to the FirePOWER Services module:

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

ASA 5585-X Data Port Utilization

ASA SSP processes all ingress and egress packets

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





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 synchronized.

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
```




Installation Steps

1. Ensure Prerequisites are met
2. Uninstall any existing Cisco IPS or CX sw-module and relevant service-policy (if applicable)
3. Obtain both the ASA FirePOWER Boot Image and System Software packages from Cisco.com
4. Download 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 dialog 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 Center.
10. Configure ASA to redirect traffic to the module

```
ciscoasa# sw-module module ips shutdown
ciscoasa# sw-module module ips uninstall
ciscoasa# reload
```

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
```


Installing the Boot Image (Cont.)

- After 5-15 minutes, verify the FirePOWER Services boot image is booted

```
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: Admin123

Note

If you installed a new SSD device it may need to be formatted before use. To partition the SSD, use the following command:

```
asasfr-boot> partition
```

```
.....
```

```
Partition Successfully Completed
```

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...
```

If you do not use NTP during “setup” you can manually set system time

Time Source – Either NTP or manually set system time using the following:

```
asasfr-boot> config timezone
asasfr-boot> config time
```

The `show module sfr` command output should show all processes as Up.

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 Center Setup

- Identify the FireSIGHT Management Center that will manage this device

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

FMC IP address and registration key

- Use the FireSIGHT Management Center - Device Manager to add the device

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:

+ Advanced

Register Cancel

Module IP address and registration key

Licenses applied to FireSIGHT MC

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
```



ASA FirePOWER Management Options

- Two layers of management access: Initial Configuration and Policy Management
- Initial Configuration **MUST** be done via the CLI:
 - ASA FirePOWER console port on **ASA5585-X**
 - Management interface M1/0 on **ASA5585-X** FirePOWER blade using **SSH**
 - Management interface M0/0 on **ASA5500-X** using **SSH**
 - Session to the module over the ASA backplane on both **ASA5500-X** and **ASA5585-X**
- ASA FirePOWER policy configuration is done using **FireSIGHT Management Center**.
- ASA configuration including traffic redirection to the module is done from **ASA CLI, ASDM** or **Cisco Security Manager (CSM)**.
- Default FirePOWER module IP address: 192.168.45.45/24
- FirePOWER module IP address can be changed through **CLI** or **ASDM Setup Wizard**

ASA5500-X FirePOWER Management Interface Considerations

- One **shared** Management interface for ASA and FirePOWER module (M0/0) on ASA5500-X platform
- The FirePOWER module needs Management Interface for
 - all updates (base OS, OS upgrade packages)
 - all feature updates (rules, reputation data)
 - all Management Center interaction (Mgmt, event-data)
- ASA can be managed inline e.g. “Inside” or through the Mgmt (M0/0) interface
- The FirePOWER module can only be managed through the Mgmt (M0/0) 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

ASA5500-X FirePOWER Management Interface Considerations (Cont.)

- Best Practice: Layer 2 Environment for ASA and FirePOWER Management
- **ASA managed in-band** (from the “inside” interface)
- **FirePOWER module managed via the M0/0 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



```
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



Requirements

- FirePOWER Hardware Module is included with ASA5585-X **FirePOWER bundles**
 - I.e. ASA5585-S60**F60-BUN** SKU
- A FirePOWER module can be added to an existing ASA
- FirePOWER services software is **pre-installed** on ASA5585-X FirePOWER Hardware Modules
- ASA Chassis needs to be powered-down before inserting the FirePOWER Hardware Module
- Minimum ASA version: **9.2.2**
- FirePOWER hardware module can be reimaged by installing the Boot Image and System Software package via ROMMON using the module's console port

Migrating to FirePOWER Services on ASA5500-X from Classic IPS or CX

- 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

Migrating to FirePOWER Services on ASA5585-X from Classic IPS or CX

- 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

ASA Deployment Modes for FirePOWER Services

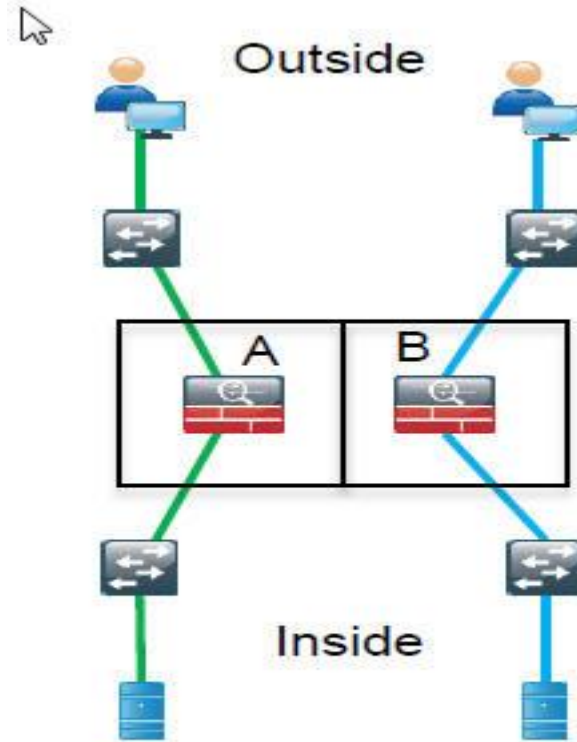
FirePOWER Services is supported in the following ASA deployment modes:

- **Active Standby** for locations where high availability is the primary concern
- **Clustering** for locations where:
 - Asymmetry is a concern
 - High availability is required
 - Horizontal performance scaling is needed
- **Multi-Context** for separation of policy by logical and physical interfaces

Note State sharing does not occur between FirePOWER Service modules within the ASA cluster. FirePOWER configuration is not synced within the cluster

Multi-Context ASA Deployments

- ASA can be configured in multi context mode such that traffic going through the ASA can be assigned different policies
- These interfaces are reported to the FirePOWER blade and can be assigned to security zones that can be used in differentiated policies.
- In this example, you could create one policy for traffic going from Context A Outside to Context A Inside. And then a different policy for Context B Outside to Context B Inside.



Multi-Context ASA Deployments

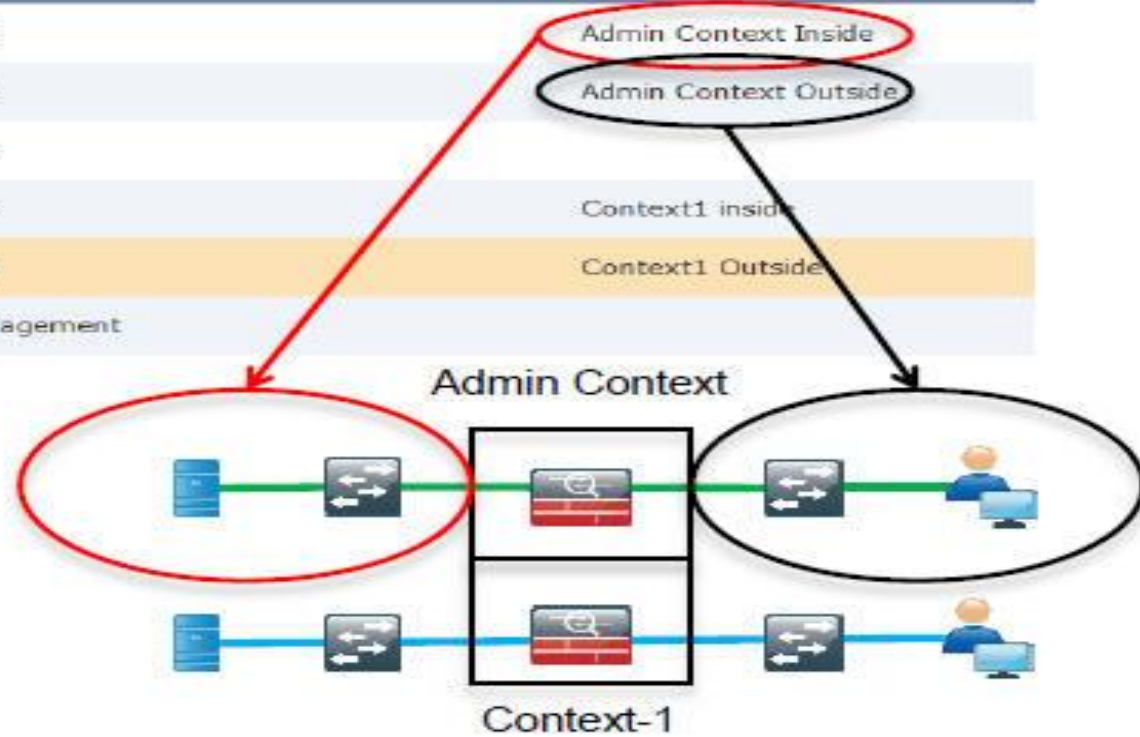
Overview Analysis Policies **Devices** Objects FireAMP

Device Management NAT VPN

10.89.145.91

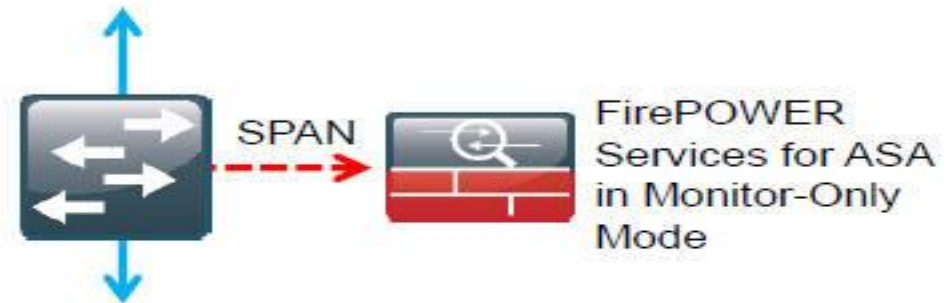
ASAS525

Device	Interfaces	
Name	Type	Security Zone
admin/ctx-admin-inside	ASA	Admin Context Inside
admin/ctx-admin-outside	ASA	Admin Context Outside
admin/publicmgmt	ASA	
context-1/ctx-1-inside	ASA	Context1 inside
context-1/ctx-1-outside	ASA	Context1 Outside
eth0	Management	



FirePOWER Services Demonstration Monitor-Only Mode

- Monitor Mode allows FirePOWER Services to analyze traffic without the ASA being placed in the data path.
- Shows the features and services provided by FirePOWER services without the need to fully configure firewall services on the ASA
- Customer demonstrations are the best way to show proof of value



Thank you.

