CISCO

You make **possible**

Firepower Platform Deep Dive

Andrew Ossipov, Distinguished Engineer

BRKSEC-3035

Barcelona | January 27-31, 2020

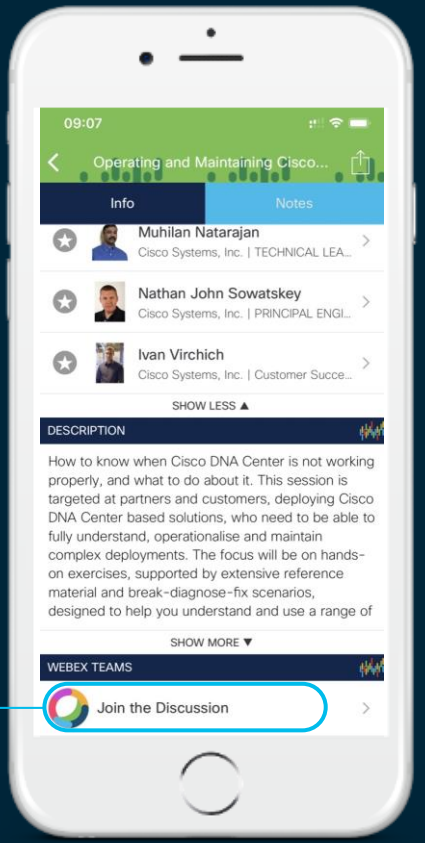
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

NGFW, Solution Architecture, Hybrid Cloud DC

IETF: OpSec and TLS Working Groups

Agenda

- Hardware and Software
- Firepower Threat Defense Overview
- Firepower Security Applications
- Multi-Instance Capability on Firepower 4100 and 9300
- Availability and Scalability
- Deployment Example: FTD Instance on Firepower 4100
- Closing

Hardware and Software

Next Generation Platform Requirements

Modular Chassis	System hardware components can be upgraded independently
Architectural Scale	Leverage the best of security processing components (x86, NPU, Crypto) and scale with Clustering
No Single Failure Point	All hardware and software components are redundant and as independent as possible
Deployment Agnostic	Provide the same benefits in physical, virtual, and hybrid SDN environments

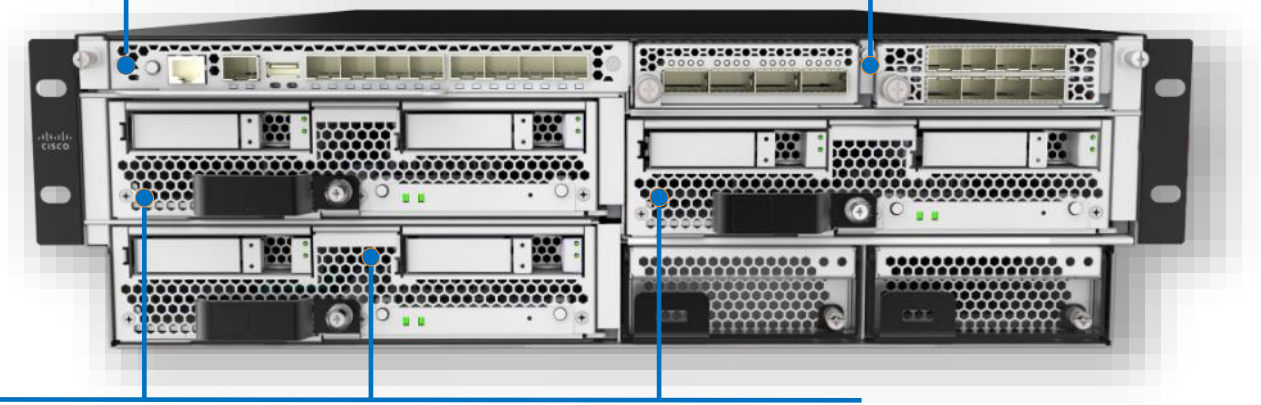
Dynamic service chaining based on policy and context	Service Insertion
Services be added, removed, upgraded, and modified without disrupting existing flows	Rapid Inline Changes
Architecture open to quickly add new services as market evolves	3rd Party Integration
Every chassis configuration and monitoring function is available through REST API	Full Automation

Firepower 9300 Overview

Supervisor
- Application deployment and orchestration
- Network attachment and traffic distribution
- Clustering base layer for ASA or FTD

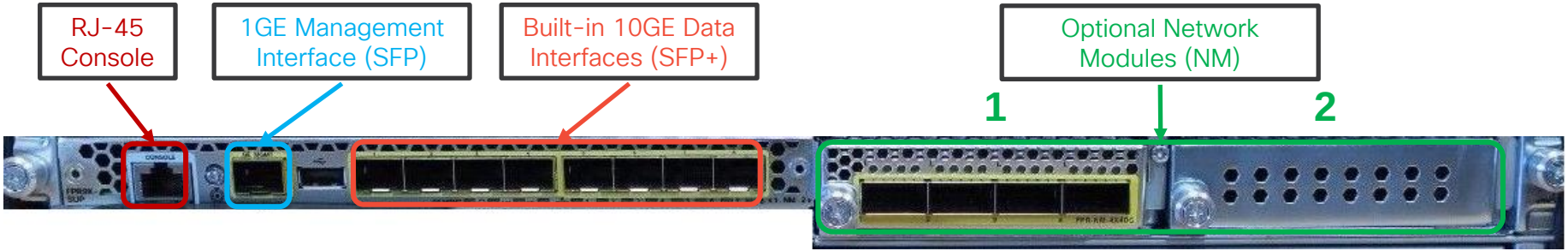
Network Modules
- 10GE, 40GE, 100GE
- Hardware bypass for inline NGIPS

3RU



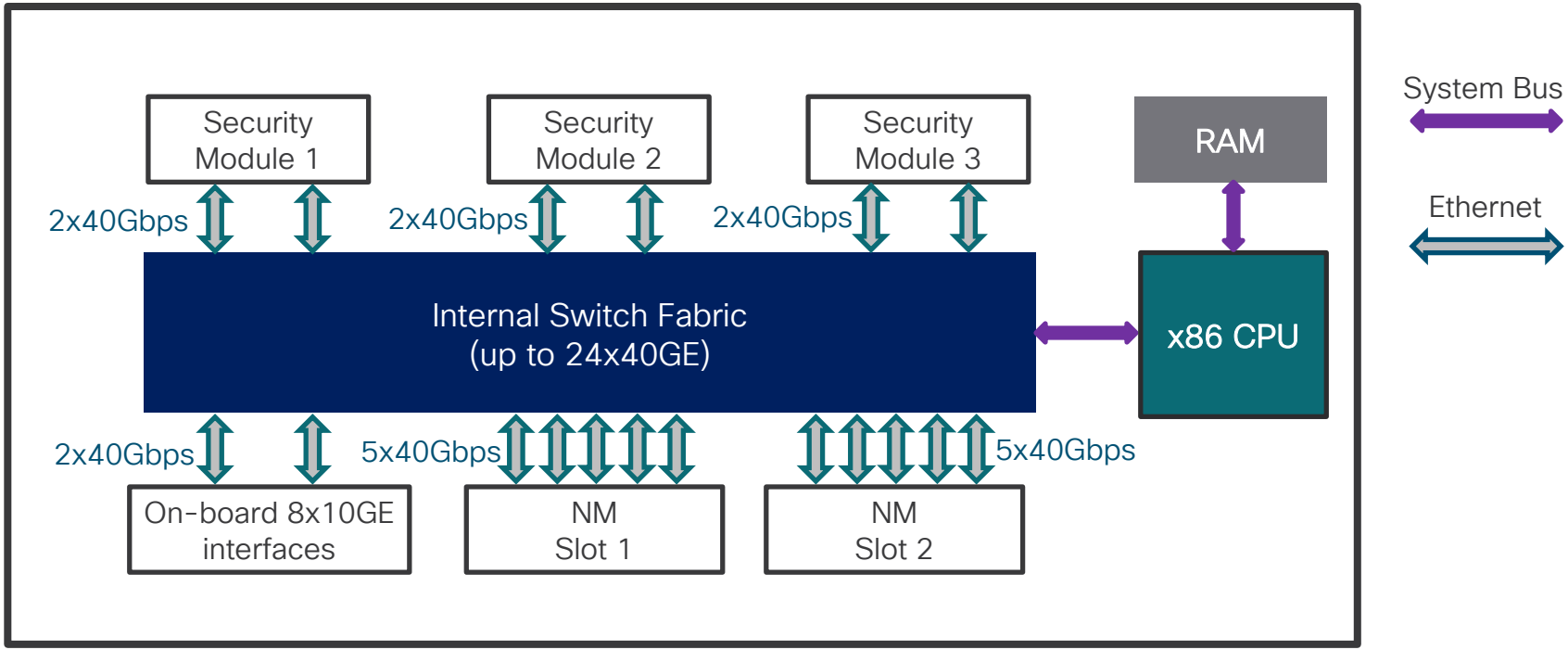
Security Modules
- Embedded Smart NIC and crypto hardware
- Cisco (ASA, FTD) and third-party (Radware DDoS) applications
- Standalone or clustered within and across chassis

Supervisor Module



- Network interface allocation and security module connectivity
  - LACP or Static (in FXOS 2.4.1) Port-Channel creation with up to 16 member ports
  - Up to 500 VLAN subinterfaces for Container instances in FXOS 2.4.1
- Application image storage, deployment, provisioning, and service chaining
- Clustering infrastructure for supported applications
- Smart Licensing and NTP for entire chassis

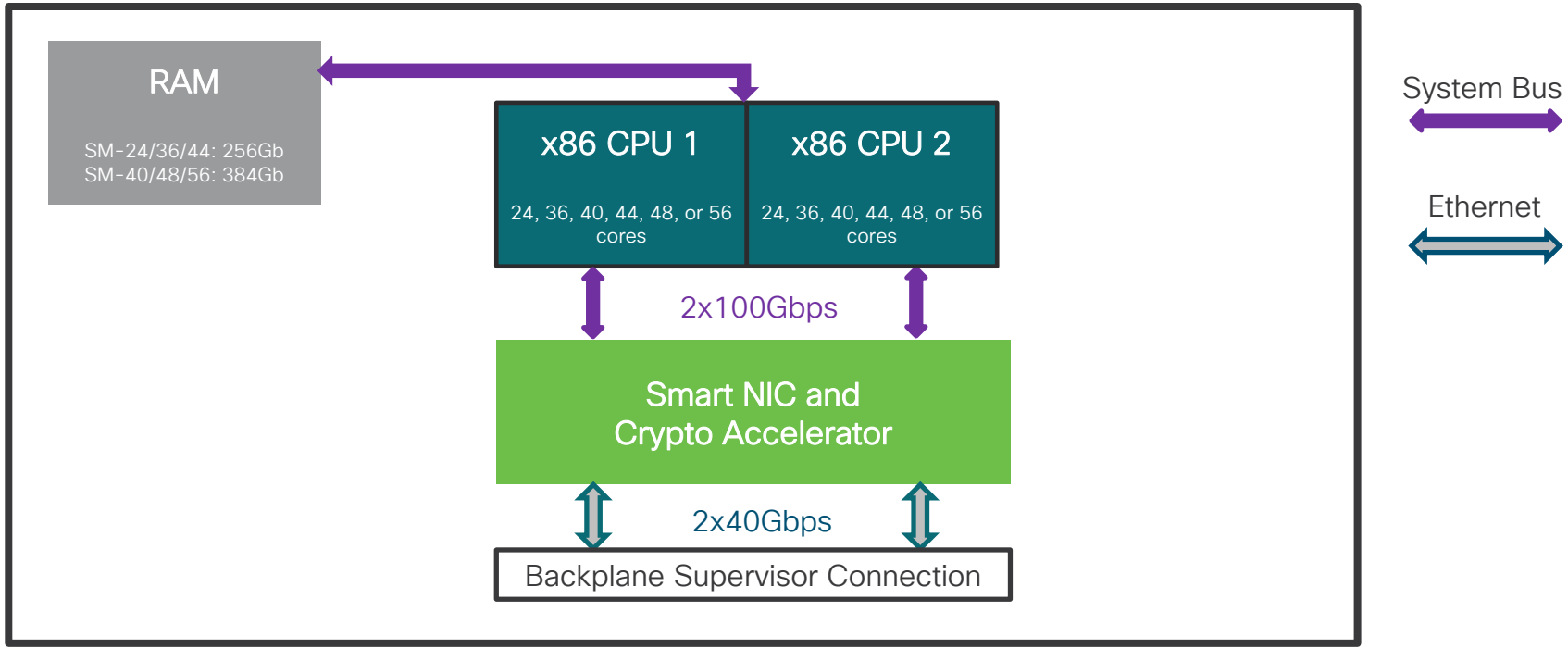
Supervisor Architecture



Firepower 9300 Security Modules

- Built-in hardware Smart NIC and Crypto Accelerator
- Previous generation SM-24, SM-36, and SM-44
  - Dual 800GB SSD in RAID1 by default
  - SM-24 is NEBS Level 3 Certified
- New SM-40, SM-48, and SM-56
  - Dual 1.6TB SSD in RAID1 by default
  - Higher performance on cryptographic operations
- Mixed standalone modules supported in FXOS 2.6.1
  - Mixed modules will be supported with FTD multi-instance clustering in FXOS 2.8.1

Security Module Architecture



Firepower 4100 Overview

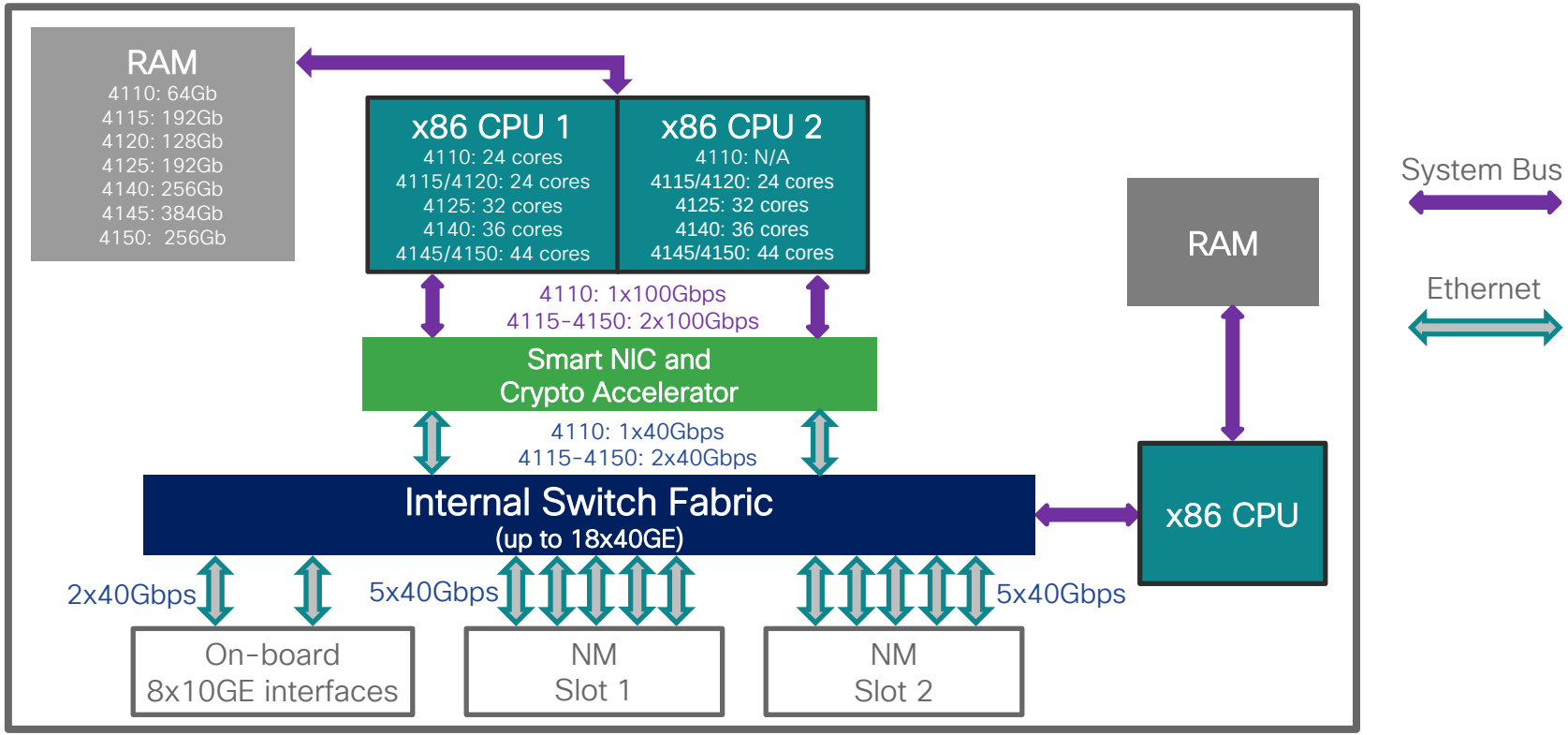
Built-in Supervisor and Security Module
- Same hardware and software architecture as 9300
- Fixed configurations (4110 – 4150)

Solid State Drives
- Independent operation (no RAID)
- Default slot 1 provides 200-800GB of total storage
- Slot 2 adds 400GB of AMP storage

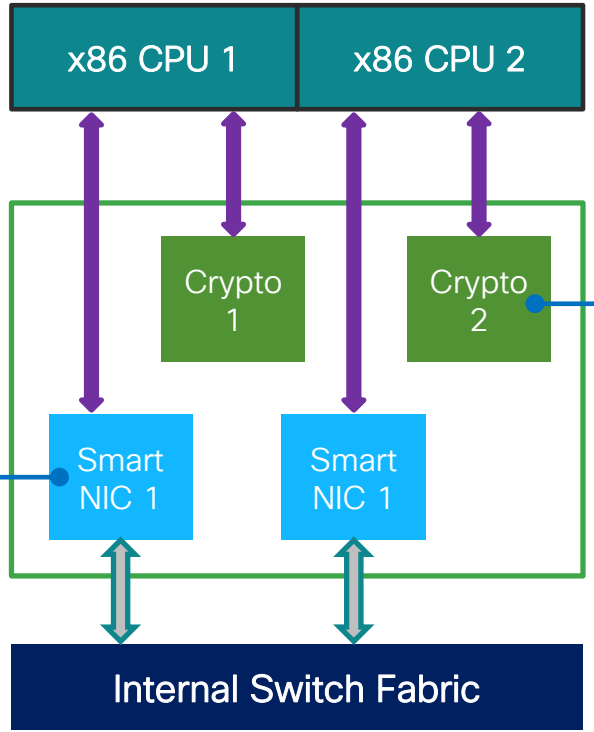
1RU

Network Modules
- 10GE and 40GE interchangeable with 9300
- Partially overlapping fail-to-wire options

Firepower 4100 Architecture



Firepower 4100/9300 Smart NIC and Crypto



Crypto Accelerator
- Single on 4110, dual elsewhere
- Configurable **core bias** to IPsec/TLS on Firepower 4110, 4120, 4140, 4150 and Firepower 9300 SM-24, SM-36, SM-44; shared elsewhere
- IPsec S2S and RAVPN
- TLS/DTLS RAVPN
- TLS inspection assistance

Cisco Programmable NIC
- Single on 4110, dual elsewhere
- 40Gbps connectivity each
- Packet Matching and Rewrite
- Tracks **2M flows** for **Flow Offload**

FXOS 2.3.1

System Bus

Ethernet

Firepower 2100 Overview

Integrated Security Platform for FTD or ASA Application
- Lightweight virtual Supervisor module
- Embedded x86 and NPU with Hardware Crypto Acceleration
- Fixed configurations (2110, 2120, 2130, 2140)
- Dual redundant power supplies on 2130 and 2140 only

SFP/SFP+ Data Interfaces
- 4x1GE on Firepower 2110 and 2120
- 4x10GE on Firepower 2130 and 2140

1RU

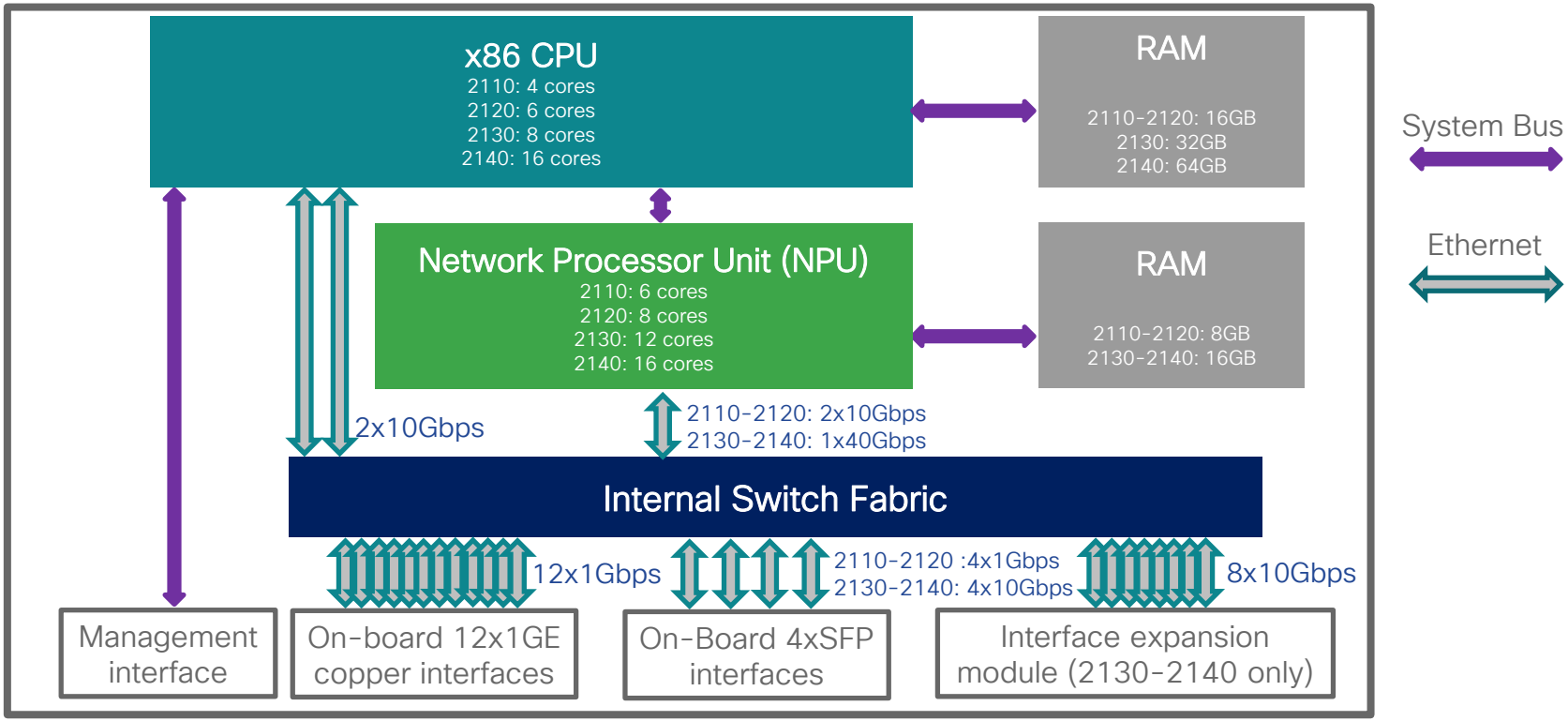
Copper Data Interfaces
- 12x1GE Ethernet

Network Module
- Firepower 2130 and 2140 only
- Same 8x10GE SFP module as on Firepower 4100/9300

Firepower 2100 Functionality

- Designed and optimized for FTD application
  - Data Plane runs on integrated NPU and Crypto module
  - Threat-centric Advanced Inspection Modules run on x86
  - No separate Flow Offload engine
  - Supports ASA application as well
- Single point of management for chassis and application
  - Firepower Device Manager (FDM) with device REST API for on-box
  - Firepower Management Center (FMC) for multi-device

Firepower 2100 Architecture



Firepower 1100 Overview

Integrated Security Appliance with ASA or FTD
- Embedded x86 CPU with QuickAssist Crypto Acceleration
- Fixed non-modular configurations (1120, 1140, 1150 new)

SFP Data Interfaces
- 4x1GE on 1120 and 1140
- 2x1GE, 2x10GE on 1150 new

1RU

Copper Data Interfaces
- 8x1GE Ethernet

Field Replaceable SSD

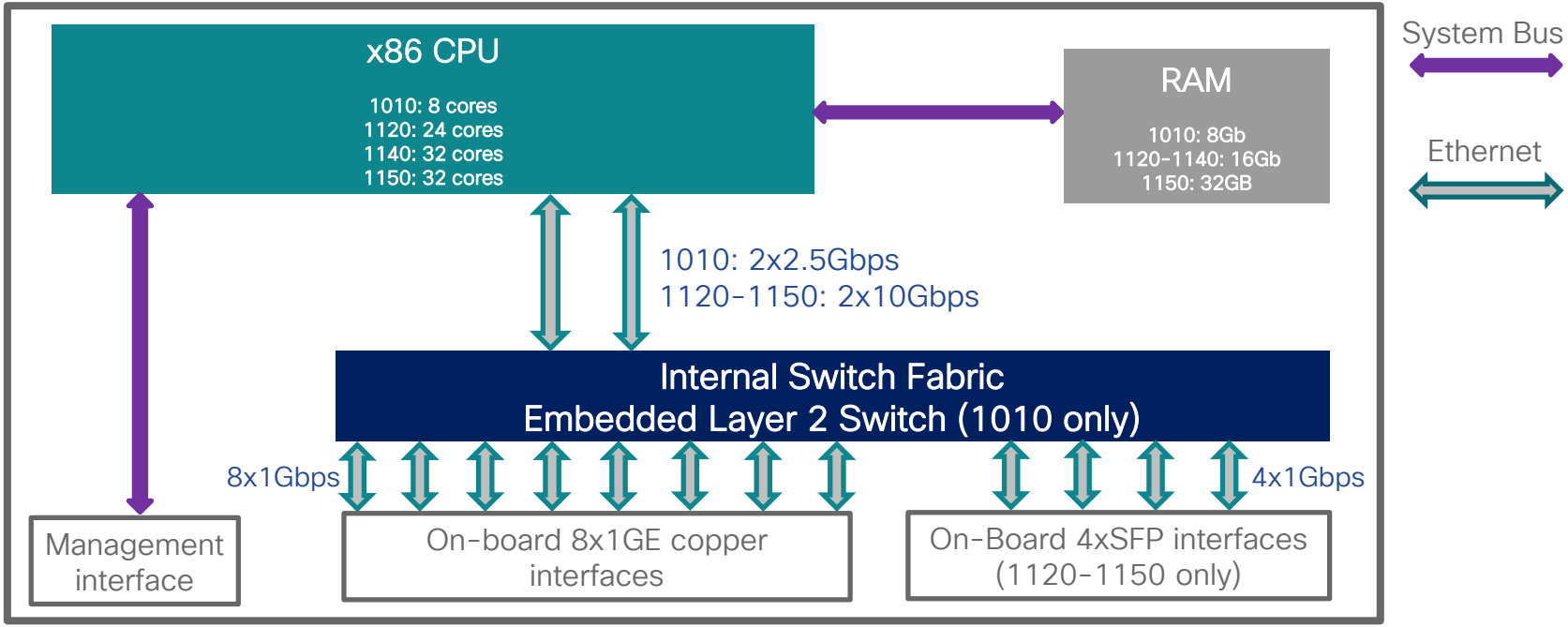
Firepower 1010 Overview

Integrated Security Appliance with ASA or FTD
- Embedded x86 CPU with QuickAssist Crypto Acceleration
- Fixed non-modular configuration

Desktop

Copper Data Interfaces
- 8x1GE Ethernet
- Built-in Layer 2 switch new
- Power over Ethernet (PoE) on ports 7 and 8 new

Firepower 1000 Architecture



Standard Network Interfaces

- Supervisor attaches security modules to network
  - All interfaces are called “Ethernet” and 1-referenced (i.e. Ethernet1/1)
  - All external network ports require fiber or copper transceivers (SFP)
  - Third-party SFP are allowed on best-effort support basis
  - Same-kind OIR is supported for external network modules

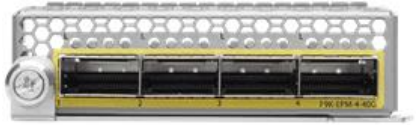
8x1GE

- Firepower 2100 only in **FXOS 2.4.1**
- Single width
- 10M/100M/1GE

8x10GE

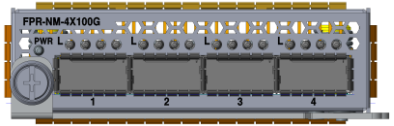
- Firepower 2100, 4100, 9300
- Single width
- 1GE/10GE SFP

4x40GE



- Firepower 4100 and 9300
- Single width
- 4x10GE breakouts for each 40GE port

2x100GE and 4x100GE



- Firepower 9300 only
- Single width in **FXOS 2.4.1**
- QSFP28 connector
- Future 4x25GE breakout
- Legacy double width 2x100 still available

Fail-to-Wire Network Modules

- Fixed interfaces, no removable SFP support; same-kind OIR in FXOS 2.7.1
- NGIPS inline interfaces for standalone FTD 6.1+ only
- Sub-second reaction time to application, software, or hardware failure
  - Designed to engage during unplanned failure or restart events
  - <90ms reaction time for Standby→Bypass with full power failure

8x1GE

- Firepower 2100, 4100
- Single width
- 10M/100M/1GE copper

6x1GE

- Firepower 2100, 4100
- Single width
- 1GE fibre SX

6x10GE

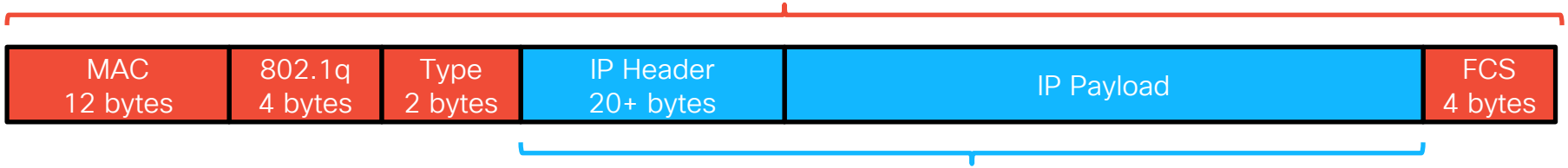
- Firepower 2100, 4100, 9300
- Single width
- 10GE SR or LR

2x40GE

- Firepower 4100 and 9300
- Single width
- 40GE SR4
- No 10GE breakout support

Maximum Transmission Unit (MTU)

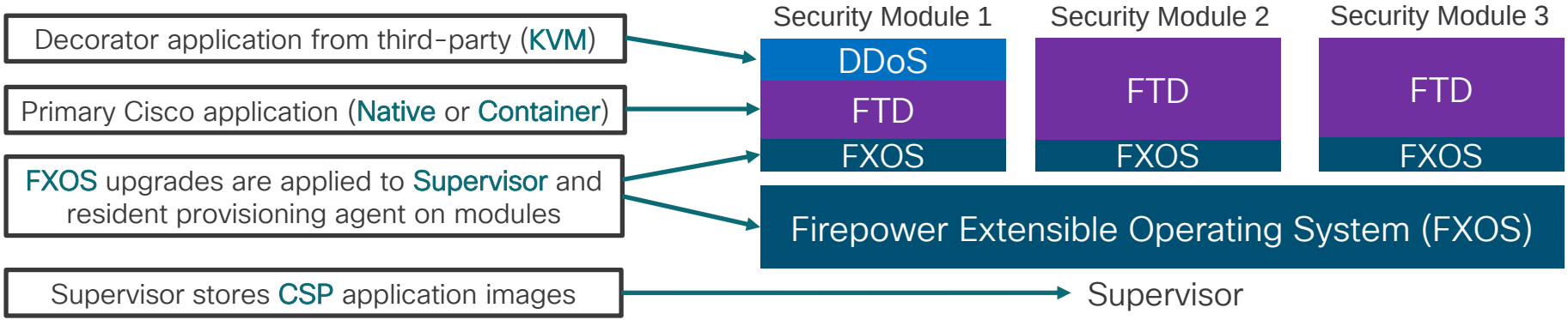
- Layer 2 MTU defines maximum Ethernet frame size on the wire
  - Mostly relevant to switches and other passive Layer 2 devices
  - Frames above the MTU size are discarded, not fragmented
  - 9206 bytes on Firepower 4100/9300 in FXOS 2.1.1; 9216 bytes on 1100/2100



- Layer 3 MTU defines maximum IP packet size with header
  - Relevant to routers and devices that may perform transit IP reassembly
  - Packets larger than configured MTU are fragmented at IP level
  - Configured on per-interface basis on ASA and FTD
  - 9184 bytes on Firepower 4100/9300 in FXOS 2.1.1; 9194 bytes on 1100/2100

Firepower 4100/9300 Software

- Supervisor and security modules use multiple independent images
- All images are digitally signed and validated through Secure Boot
- Security application images are in **Cisco Secure Package** (**CSP**) format



Firepower Platform Bundle

- Platform Bundle contains all Supervisor and module firmware images

  - FXOS creates an environment for security applications
  - Supervisor automatically selects components to upgrade
  - Relevant components are reloaded automatically during the upgrade
- Firepower 1000 and 2100 FTD or ASA bundle includes virtual FXOS

Firepower Supervisor CLI Interface

- FXOS uses object-based CLI representation similar to UCS Manager
  - **scope**, **enter**, or **exit** select a command mode within the hierarchy
  - **create** instantiates a new configuration object within the hierarchy
  - **set** assigns a value to a configuration variable or object
  - **show** displays object content
  - **commit-buffer** applies changes to the running configuration

```
FP9300# scope eth-uplink
FP9300 /eth-uplink # scope fabric a
FP9300 /eth-uplink/fabric # create port-channel 2
FP9300 /eth-uplink/fabric/port-channel* # create member-port 1 11
FP9300 /eth-uplink/fabric/port-channel* # create member-port 1 12
FP9300 /eth-uplink/fabric/port-channel* # set speed 10gbps
FP9300 /eth-uplink/fabric/port-channel* # commit-buffer
FP9300 /eth-uplink/fabric/port-channel # exit
```

- Read-only access on Firepower 1100 and 2100 with **FTD**

Firepower Threat Defense Overview

Security Application Convergence

ASA

- L2-L4 Stateful Firewall
- Scalable CGNAT, ACL, routing
- Application inspection

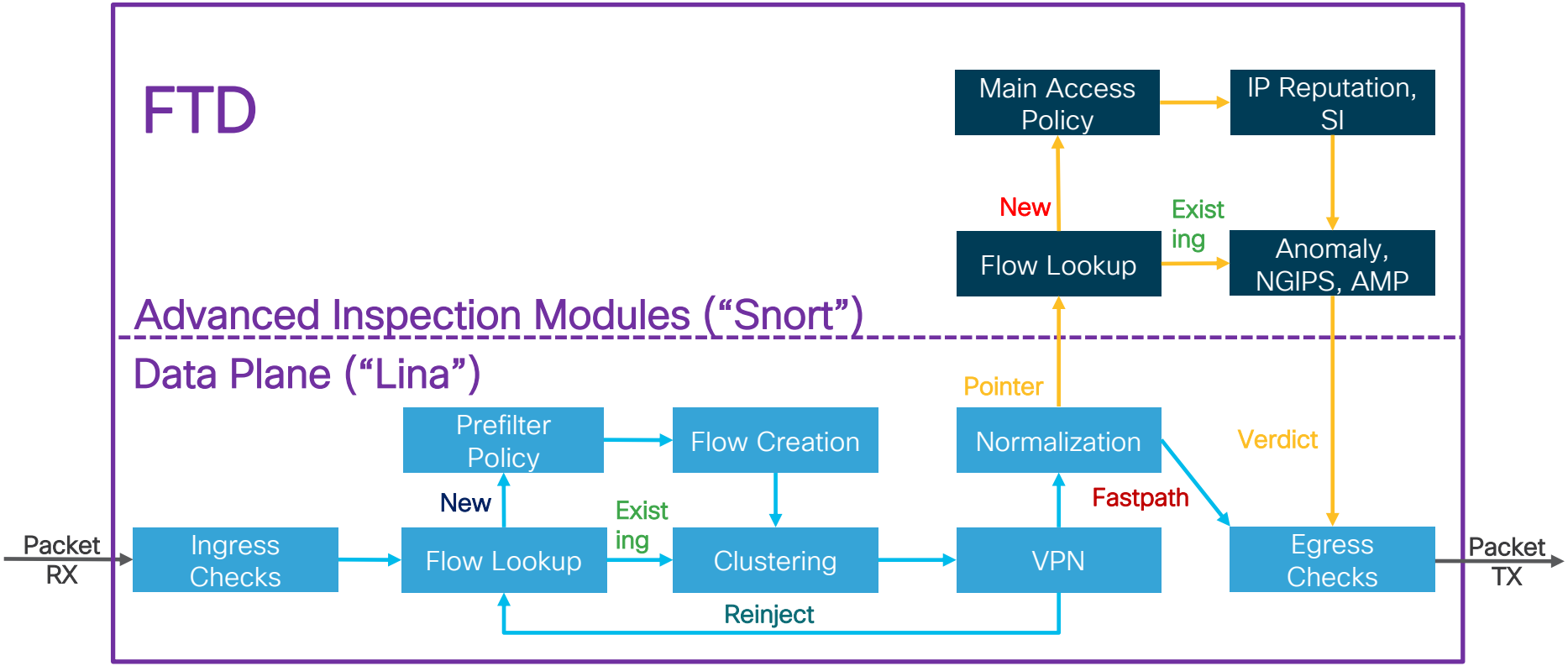
FirePOWER

- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

Firepower Threat Defense (FTD)

- Converged NGFW/NGIPS image on new Firepower and ASA5500-X platforms
- Single point of management with Firepower Management Center (FMC)
- Full FirePOWER functionality for NGFW/NGIPS deployments
- ASA Data Plane with TCP Normalizer, NAT, ACL, dynamic routing, failover, clustering

Architecture and Logical Packet Flow



Monitoring System Utilization

- Data Plane (Lina)

```
ftd# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core          5 sec              1 min              5 min
Core 0        2.0 (2.0 + 0.0)    1.1 (1.1 + 0.0)    0.9 (0.9 + 0.0)
Core 1        3.2 (3.2 + 0.0)    1.8 (1.8 + 0.0)    1.5 (1.5 + 0.0)
[…]
Core 35       0.0 (0.0 + 0.0)    0.0 (0.0 + 0.0)    0.0 (0.0 + 0.0)
```

Data Plane (most transit traffic)

Control Plane (network control and application inspection)

- Advanced Inspection Modules (Snort)

```
ftd# show asp inspect-dp snort
SNORT Inspect Instance Status Info

Id Pid        Cpu-Usage     Conns       Segs/Pkts   Status
           tot (usr | sys)
-- ----- ---------------- ---------- ---------- ----------
0  47430   1% (  1%|  0%) 621           0         READY
1  47434   0% (  0%|  0%) 610           0         READY
[…]
45 47474   2% (  2%|  0%) 572           0         READY
```

Inspection Load

Load Distribution

Processing State

NGFW Interface Modes

- Must choose **routed** or **transparent** at deployment

  - Must configure IP on BVI in transparent mode
- **Integrated Routing and Bridging** combines both in routed mode

- Full feature set and state enforcement
  - VLAN or VxLAN ID must change during traversal

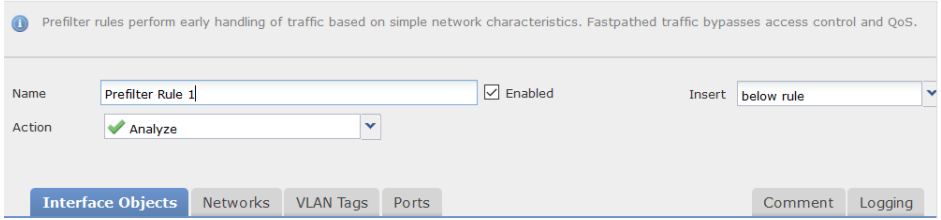
NGIPS Interface Modes

- Any unused interface in routed/transparent can be in NGIPS mode

  - Inline pairing at physical/Etherchannel level; inline sets allow asymmetry
  - True pass-through mode for VLAN
  - LACP pass-through is supported with standalone interfaces in FXOS 2.3.1
- Most classic firewall functionality is disabled
  - All security policies still apply
  - Data Plane tracks connections for HA/clustering with no state enforcement
  - NAT, application inspection, and similar ASA-style functionality is disabled
  - Flow Offload is not triggered

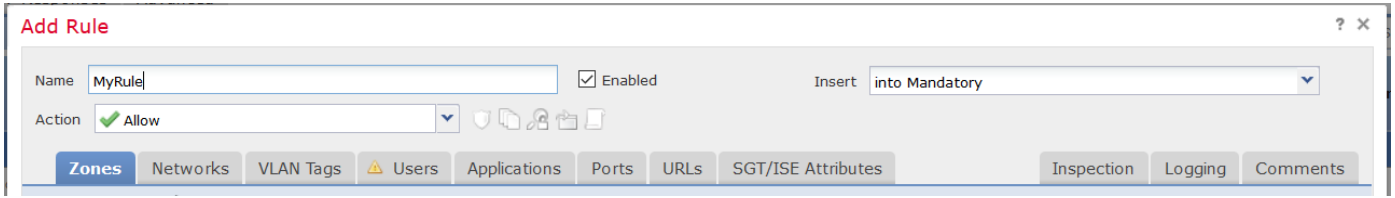
Prefilter Policy

- First access control phase in Data Plane for each new flow
  - Block: Deny the flow without any further processing
  - Fastpath: Allow and process entirely in Data Plane, attempt Flow Offload
  - Analyze: Pass for evaluation in Main ACP, optionally assign tunnel zone
- Not a “high performance” substitute to true NGFW policies
  - Non-NGFW traffic match criteria
  - Limited early IP blacklisting
  - Tunneled traffic inspection
  - Accelerating high-bandwidth and latency-sensitive trusted flows



Main Access Control Policy

- Second and final access control phase in Snort
  - Block [with reset]: Deny connection [and TCP RST]
  - Interactive Block [with reset]: Show HTTP(S) block page [and TCP RST]
  - Monitor: Log event and continue policy evaluation
  - Trust: Push all subsequent flow processing into Data Plane only
  - Allow: Permit connection to go through NGIPS/File inspection
- Appropriate place for implementing NGFW policy rules



  - Policy decisions may require multiple packets

FlexConfig Policies

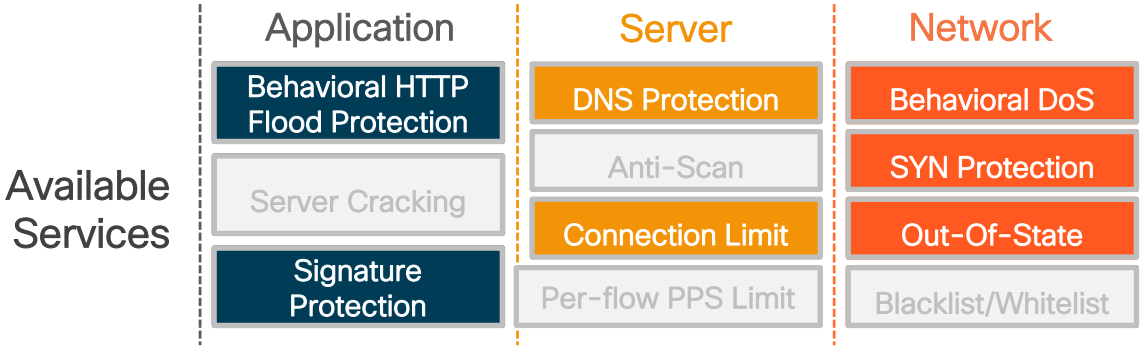
- Device-level free form CLI policies that follow ASA syntax
  - Supports pre-defined object templates and completely custom objects
  - Natively managed feature commands are blocked
  - Must push an object with negated commands to remove
- **FlexConfig** is only supported on best-effort basis
- Deploy **Once**; **Everytime** is for interactions with managed features
- Always select **Append** rather than **Prepend** type

Firepower Security Applications

Security Applications on Firepower 4100/9300

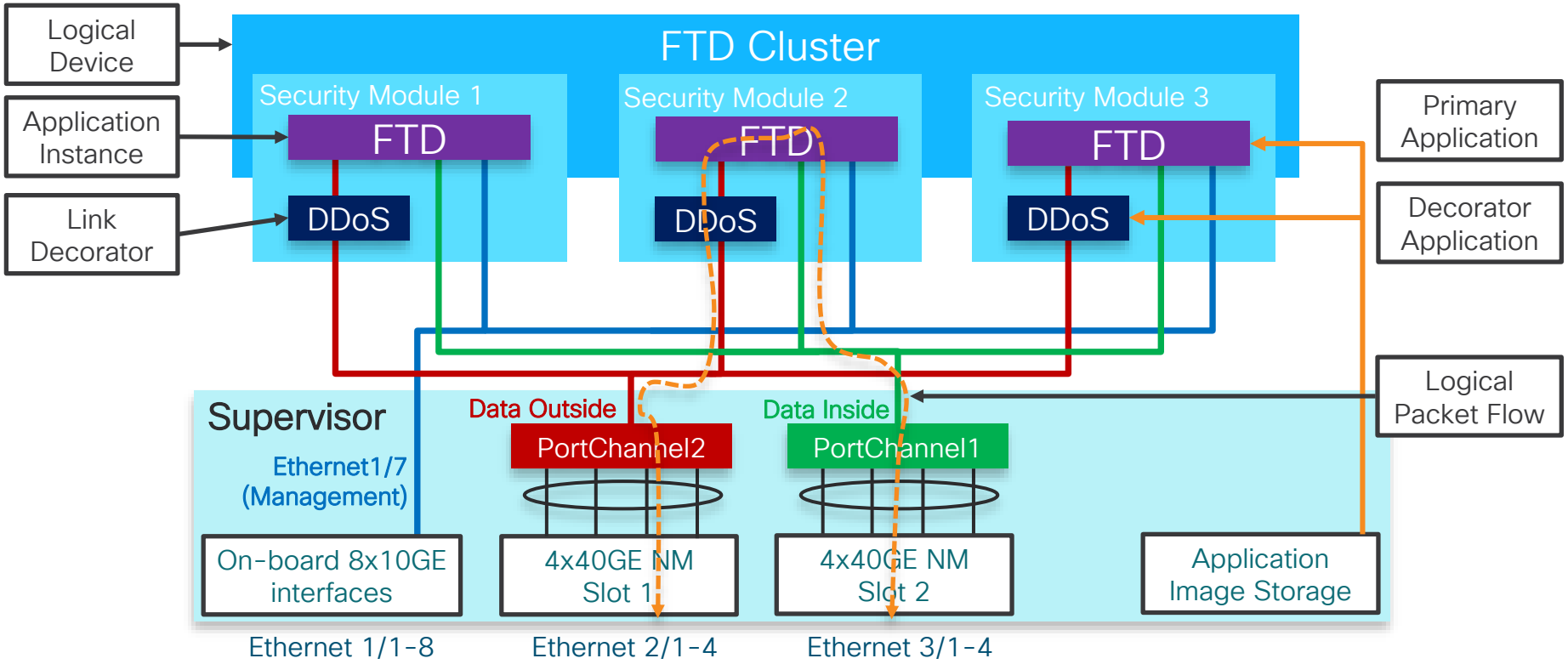
- ASA or FTD are Primary applications in Native or Container mode
  - Native application consumes full hardware resources of an entire module
  - Firepower 4100 and 9300 support multiple FTD Container instances in FXOS 2.4.1
  - Firepower 9300 supports a mix of ASA/FTD application modules in FXOS 2.6.1
- A Decorator application shares a module with a Native primary application
  - Traffic flows from network interfaces through a decorator to primary application
  - Service chaining with Radware vDefensePro decorator and ASA or FTD 6.2+
  - Not supported with Container applications at this time

Radware vDefensePro Summary

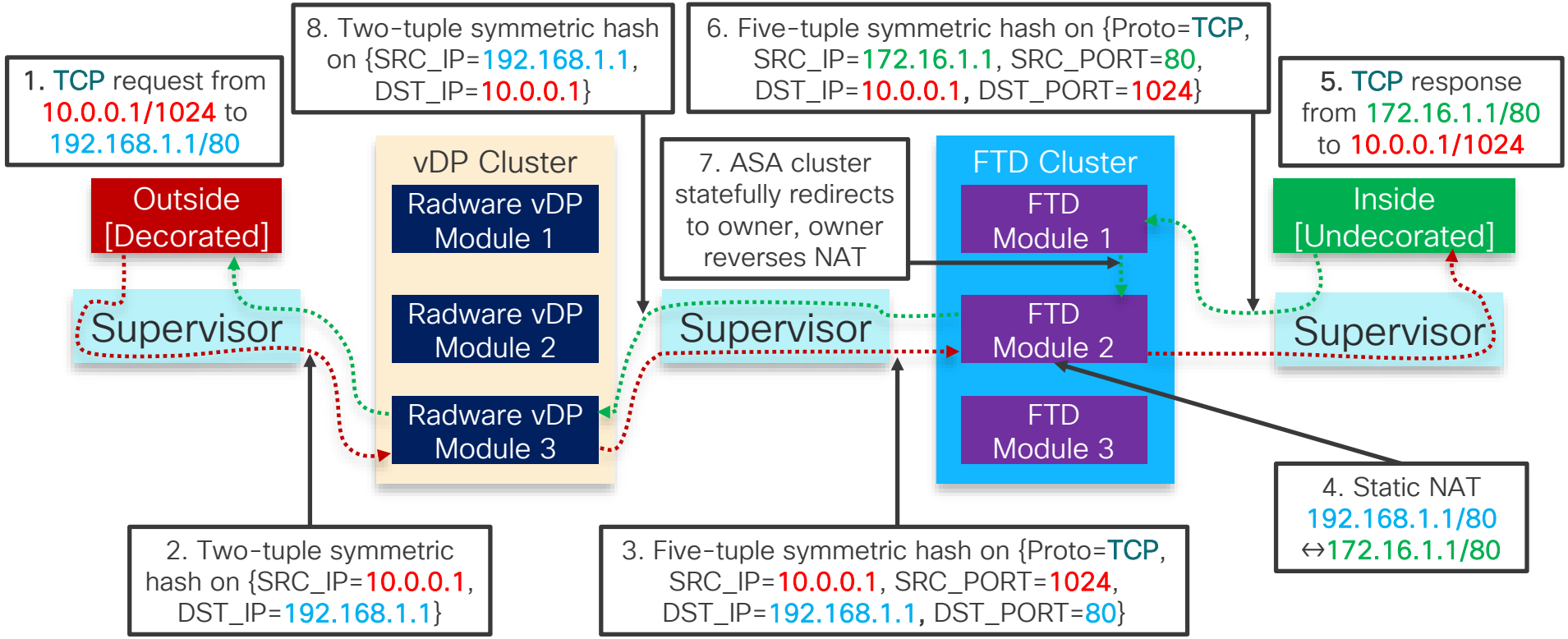


- Supported with ASA and FTD on Firepower 4100 and 9300
  - vDP on Firepower 4110 is not supported with ASA until FXOS 2.4.1
- Up to 18Gbps of Peak traffic per module on 10 assigned CPU cores
  - Assign 2-10 CPU cores at ~2Gbps of Peak traffic per core in FXOS 2.3.1
  - 200Mbps-10Gbps of Peace Time traffic based on a strictly enforced license
  - Linear scaling with intra- and inter-chassis clustering

Firepower 9300 Native Application Deployment



Detailed Inbound Flow with Radware vDP

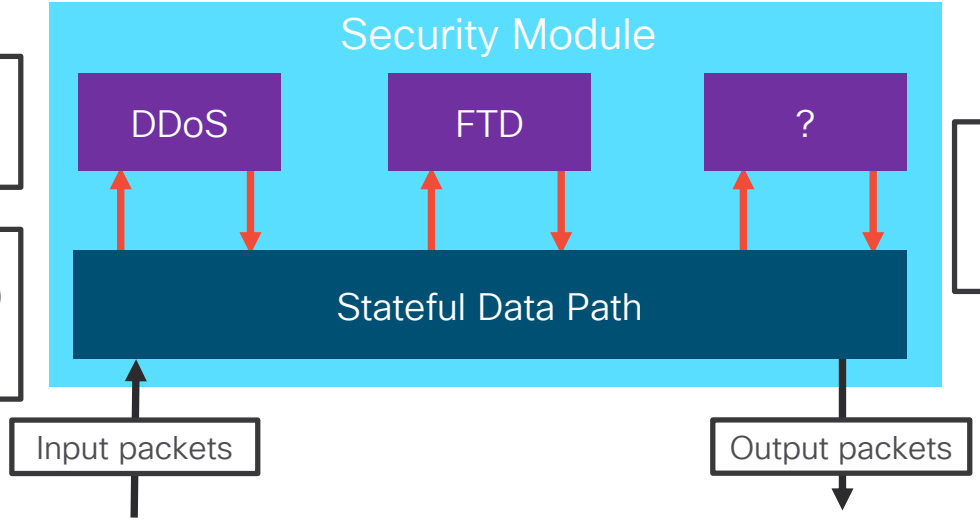


Future Vision: Security Service Chaining

- Contextual policy- and outcome based service insertion
- Meta data exchange with Network Services Header (NSH)

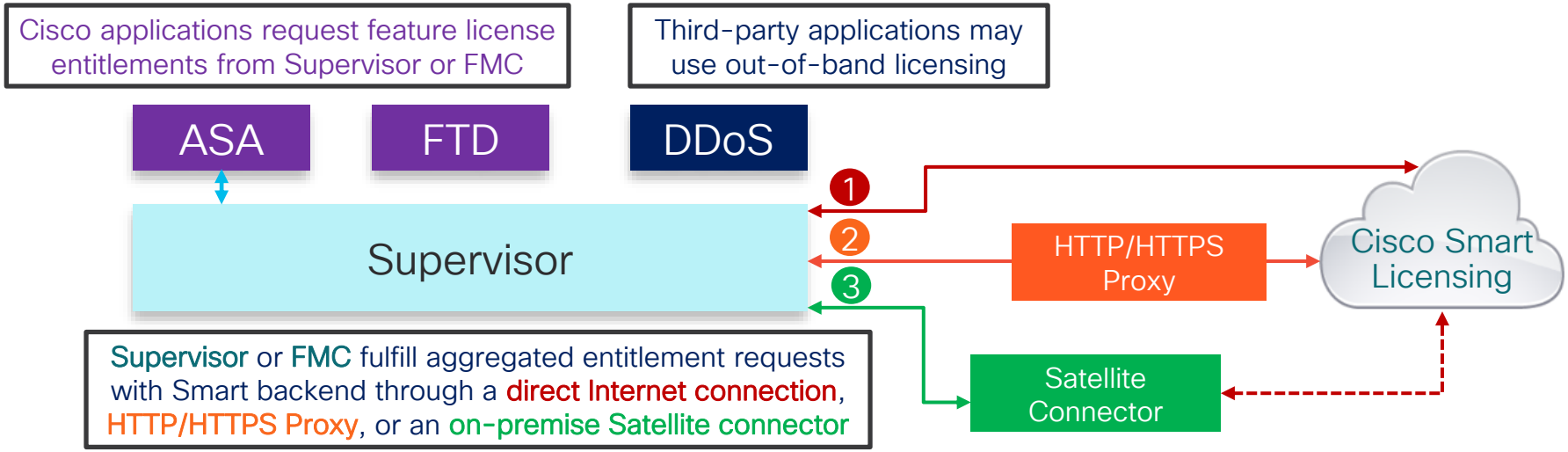
Service Function (SF) processes packet, attaches meta data, and returns to SFF

Service Classifier (SC) and Service Function Forwarder (SFF) direct incoming traffic through necessary services



SF, SC, and SFF may influence service path based on policy, context, and meta data

Smart Licensing



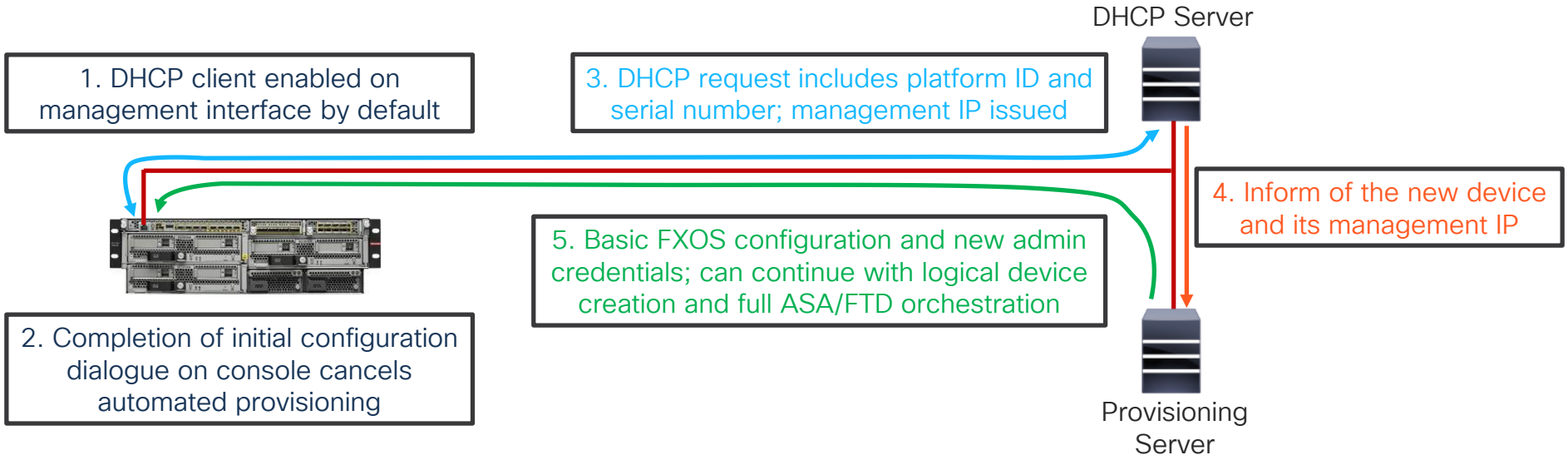
- ASA entitlements: Strong Encryption, Security Contexts, Carrier Inspections
- FTD entitlements: Threat, Malware, and URL Services

Management Overview

- Chassis management is independent from applications
  - On-box chassis manager UI, CLI, and REST
  - SNMP and syslog support for chassis level counters/events on Supervisor
- Applications are managed through their respective interfaces
  - CLI, REST API (except 1100 and 2100), ASDM, CSM, and CDO for ASA
  - Off-box FMC, FMC REST API, and CDO for FTD
  - Device API-driven on-box FDM for FTD
  - Off-box APsolute Vision for Radware vDP
- Future off-box FMC support for both chassis and FTD management
  - Already supported on Firepower 2100

Automated Provisioning on Firepower 4100/9300

- FXOS 2.6.1 added remote provisioning on Firepower 4100 and 9300 only

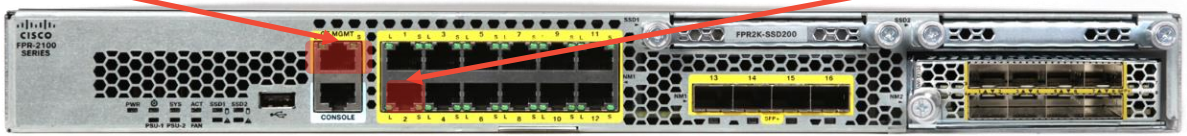


Firepower 1000/2100 Appliance Mode

- ASA 9.13(1) supports Appliance and Platform modes on 1000/2100
  - Default for 2100 upgrades, Platform mode presents ASA and FXOS separately
  - Will be similarly enabled for FTD 6.6 application
- On new installations, Appliance mode abstracts FXOS behind ASA CLI
  - Includes most interface/platform configuration and image management
  - Unified SNMP agent for ASA application and platform (e.g. IF and ENTITY MIBs)
  - Advanced troubleshooting still requires `connect fxos [admin]`
  - Simplified auto-provisioning process with a single management IP

Dedicated Enterprise Management
(DHCP client with ASA/FTD CLI or ASDM/FDM access).

In-band Management via Inside
(DHCP server with ASA CLI/ASDM or FDM, and outbound Internet access).



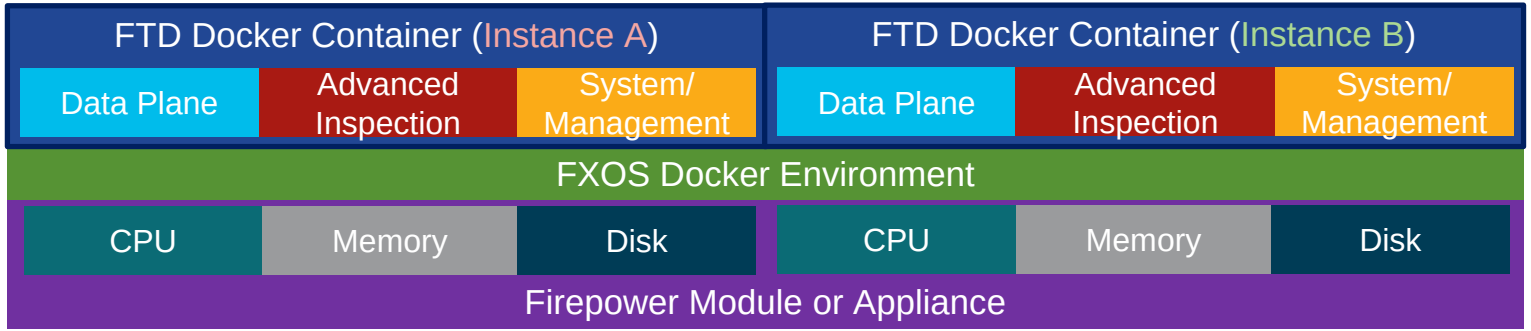
Multi-Instance Capability on Firepower 4100 and 9300

Multi-Instance Capability Summary

- Supported on Firepower 4100 and 9300 only
- Instantiate multiple logical devices on a single module or appliance
  - FTD application in 6.3, a mix of FTD and ASA instances in the future
  - Leverage Docker infrastructure and container packaging
- Complete traffic processing and management isolation
- Physical and logical interface and VLAN separation at Supervisor

Anatomy of a Container Instance

- Each instance uses from 6 logical CPU cores up to the platform maximum
  - User-defined assignment with a 2-core step, skipping 8; e.g.: 6, 10, 12, …
  - Memory size is automatically selected based on configured CPU core count
  - Instance restart is required to change resource configuration, so use stateful HA
- Automatic CPU core allocation between internal components based on size
  - System/Management process always takes 2 logical cores



Instance Scalability by Platform

- Lower of the two limits:

CPU core count divided by at least **6 cores** per instance

Disk space divided by 48Gb of required space per instance

Platform	Total Application CPU Cores	Native CPU Core Allocation (Data Plane/Snort/System)	Total Application Disk	Maximum FTD Instances	
				CPU Bound	Disk Bound
Firepower 4110	22	8/12/2	150Gb	3	~~3~~
Firepower 4115 new	46	16/28/2	350Gb	7	~~7~~
Firepower 4120	46	20/24/2	150Gb	~~7~~	3
Firepower 4125 new	62	24/36/2	750Gb	10	~~15~~
Firepower 4140	70	32/36/2	350Gb	~~11~~	7
Firepower 4145 new	86	32/52/2	750Gb	14	~~15~~
Firepower 4150	86	36/48/2	350Gb	~~14~~	7
Firepower 9300 SM-24	46	20/24/2	750Gb	7	~~15~~
Firepower 9300 SM-36	70	32/36/2	750Gb	11	~~15~~
Firepower 9300 SM-40 new	78	32/44/2	1.55Tb	13	~~32~~
Firepower 9300 SM-44	86	36/48/2	750Gb	14	~~15~~
Firepower 9300 SM-48 new	94	40/52/2	1.55TB	15	~~32~~
Firepower 9300 SM-56 new	110	44/64/2	1.55TB	18	~~32~~

Performance

- All inter-instance communication occurs through Supervisor
- Docker form factor itself has minimal effect on performance
  - Single full-blade instance performance is same as native application
- Main performance impact comes from additional System cores
  - SM-44: 28 System cores with 14 instances → 33% overall impact
  - Price to pay for independent and predicable management
  - Partially offset by a more favorable inter-component CPU core allocation
- Hardware Crypto Engine is supported in FXOS 2.7.1 and FTD 6.5
- Flow Offload support is targeted for FXOS 2.9.1 and FTD 6.7

CPU Core Allocation by Instance Size

Firepower 4110

Core Count	Data Plane/Snort/System Cores
6	2/2/2
10	4/4/2
12	4/6/2
14	4/8/2
16	6/8/2
18	6/10/2
20	8/10/2
22	8/12/2

CPU Core Allocation by Instance Size

Firepower 4115

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	10/16/2
10	4/4/2	30	10/18/2
12	4/6/2	32	12/18/2
14	4/8/2	34	12/20/2
16	6/8/2	36	12/22/2
18	6/10/2	38	14/22/2
20	6/12/2	40	14/24/2
22	8/12/2	42	14/26/2
24	8/14/2	44	16/26/2
26	8/16/2	46	16/28/2

CPU Core Allocation by Instance Size

Firepower 4120 and Firepower 9300 SM-24

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	12/14/2
10	4/4/2	30	12/16/2
12	4/6/2	32	14/16/2
14	6/6/2	34	14/18/2
16	6/8/2	36	16/18/2
18	8/8/2	38	16/20/2
20	8/10/2	40	18/20/2
22	10/10/2	42	18/22/2
24	10/12/2	44	20/22/2
26	10/14/2	46	20/24/2

CPU Core Allocation by Instance Size

Firepower 4125

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	10/16/2	48	18/28/2
10	4/4/2	30	12/16/2	50	20/28/2
12	4/6/2	32	12/18/2	52	20/30/2
14	4/8/2	34	12/20/2	54	20/32/2
16	6/8/2	36	14/20/2	56	22/32/2
18	6/10/2	38	14/22/2	58	22/34/2
20	8/10/2	40	16/22/2	60	24/34/2
22	8/12/2	42	16/24/2	62	24/36/2
24	8/14/2	44	16/26/2		
26	10/14/2	46	18/26/2		

CPU Core Allocation by Instance Size

Firepower 4140 and Firepower 9300 SM-36

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	12/14/2	48	22/24/2	68	32/34/2
10	4/4/2	30	14/14/2	50	22/26/2	70	32/36/2
12	4/6/2	32	14/16/2	52	24/26/2		
14	6/6/2	34	16/16/2	54	24/28/2		
16	6/8/2	36	16/18/2	56	26/28/2		
18	8/8/2	38	16/20/2	58	26/30/2		
20	8/10/2	40	18/20/2	60	28/30/2		
22	10/10/2	42	18/22/2	62	28/32/2		
24	10/12/2	44	20/22/2	64	30/32/2		
26	12/12/2	46	20/24/2	66	30/34/2		

CPU Core Allocation by Instance Size

Firepower 4145

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	10/16/2	48	18/28/2	68	26/40/2
10	4/4/2	30	10/18/2	50	18/30/2	70	26/42/2
12	4/6/2	32	12/18/2	52	20/30/2	72	26/44/2
14	4/8/2	34	12/20/2	54	20/32/2	74	28/44/2
16	6/8/2	36	14/20/2	56	20/34/2	76	28/46/2
18	6/10/2	38	14/22/2	58	22/34/2	78	30/46/2
20	8/10/2	40	14/24/2	60	22/36/2	80	30/48/2
22	8/12/2	42	16/24/2	62	24/36/2	82	30/50/2
24	8/14/2	44	16/26/2	64	24/38/2	84	32/50/2
26	10/14/2	46	16/28/2	66	24/40/2	86	32/52/2

CPU Core Allocation by Instance Size

Firepower 4150 and Firepower 9300 SM-44

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	12/14/2	48	20/26/2	68	28/38/2
10	4/4/2	30	12/16/2	50	20/28/2	70	30/38/2
12	4/6/2	32	14/16/2	52	22/28/2	72	30/40/2
14	6/6/2	34	14/18/2	54	22/30/2	74	30/42/2
16	6/8/2	36	14/20/2	56	24/30/2	76	32/42/2
18	8/8/2	38	16/20/2	58	24/32/2	78	32/44/2
20	8/10/2	40	16/22/2	60	26/32/2	80	34/44/2
22	8/12/2	42	18/22/2	62	26/34/2	82	34/46/2
24	10/12/2	44	18/24/2	64	26/36/2	84	36/46/2
26	10/14/2	46	18/26/2	66	28/36/2	86	36/48/2

CPU Core Allocation by Instance Size

Firepower 9300 SM-40

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	12/14/2	48	20/26/2	68	28/38/2
10	4/4/2	30	12/16/2	50	20/28/2	70	28/40/2
12	4/6/2	32	12/18/2	52	22/28/2	72	30/40/2
14	6/6/2	34	14/18/2	54	22/30/2	74	30/42/2
16	6/8/2	36	14/20/2	56	22/32/2	76	32/42/2
18	6/10/2	38	16/20/2	58	24/32/2	78	32/44/2
20	8/10/2	40	16/22/2	60	24/34/2		
22	8/12/2	42	16/24/2	62	26/34/2		
24	10/12/2	44	18/24/2	64	26/36/2		
26	10/14/2	46	18/26/2	66	28/36/2		

CPU Core Allocation by Instance Size

Firepower 9300 SM-48

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	12/14/2	48	20/26/2	68	28/38/2
10	4/4/2	30	12/16/2	50	20/28/2	70	30/38/2
12	4/6/2	32	14/16/2	52	22/28/2	72	30/40/2
14	6/6/2	34	14/18/2	54	22/30/2	74	32/40/2
16	6/8/2	36	14/20/2	56	24/30/2	76	32/42/2
18	8/8/2	38	16/20/2	58	24/32/2	78	34/42/2
20	8/10/2	40	16/22/2	60	26/32/2	80	34/44/2
22	8/12/2	42	18/22/2	62	26/34/2	82	34/46/2
24	10/12/2	44	18/24/2	64	28/34/2	84	36/46/2
26	10/14/2	46	20/24/2	66	28/36/2	86	36/48/2

CPU Core Allocation by Instance Size

Firepower 9300 SM-48 (Continued)

Core Count	Data Plane/Snort/System Cores
88	38/48/2
90	38/50/2
92	40/50/2
94	40/52/2

CPU Core Allocation by Instance Size

Firepower 9300 SM-56

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
6	2/2/2	28	10/16/2	48	18/28/2	68	28/38/2
10	4/4/2	30	12/16/2	50	20/28/2	70	28/40/2
12	4/6/2	32	12/18/2	52	20/30/2	72	28/42/2
14	6/6/2	34	14/18/2	54	22/30/2	74	30/42/2
16	6/8/2	36	14/20/2	56	22/32/2	76	30/44/2
18	6/10/2	38	14/22/2	58	22/34/2	78	32/44/2
20	8/10/2	40	16/22/2	60	24/34/2	80	32/46/2
22	8/12/2	42	16/24/2	62	24/36/2	82	32/48/2
24	10/12/2	44	18/24/2	64	26/36/2	84	34/48/2
26	10/14/2	46	18/26/2	66	26/38/2	86	34/50/2

CPU Core Allocation by Instance Size

Firepower 9300 SM-56 (Continued)

Core Count	Data Plane/Snort/System Cores	Core Count	Data Plane/Snort/System Cores
88	36/50/2	108	44/62/2
90	36/52/2	110	44/64/2
92	36/54/2		
94	38/54/2		
96	38/56/2		
98	40/56/2		
100	40/58/2		
102	40/60/2		
104	42/60/2		
106	42/62/2		

Estimating Per-Instance Throughput

- Maximum container instance throughput is proportional to CPU core count
  - Step 1: Obtain maximum native instance (full cores) throughput from data sheet
  - Step 2: Divide figure from Step 1 by native Snort cores on slide 50
  - Step 3: Multiply figure in Step 2 by Snort cores for instance size on slides 52-63
- Example: 28-core instance on Firepower 4140
  - 27Gbps of 1024-byte AVC+IPS throughput per data sheet
  - 27Gbps / 36 Snort cores on a full native instance → 750Mbps per core
  - 750Mbps * 14 Snort cores on a 28-core container instance → 10.5Gbps per instance

Features	4110	4115	4120	4125	4140	4145	4150
Throughput: FW + AVC (1024B)	13 Gbps	27 Gbps	22 Gbps	40 Gbps	32 Gbps	53 Gbps	45 Gbps
Throughput: FW + AVC + IPS (1024B)	11 Gbps	26 Gbps	19 Gbps	35 Gbps	27 Gbps	45 Gbps	39 Gbps

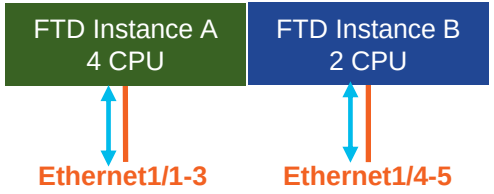
Platform	Total Application CPU Cores	Native CPU Core Allocation (Data Plane/Snort/System)
Firepower 4110	22	8/12/2
Firepower 4120	46	20/24/2
Firepower 4140	70	32/36/2

Core Count	Data Plane/Snort/System Cores
28	12/14/2

Network Interfaces

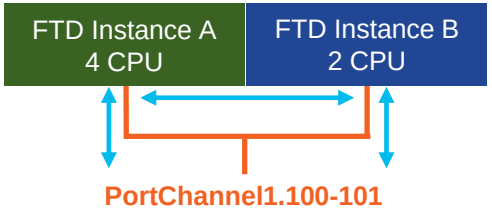
- Supervisor assigns physical, EtherChannel, and VLAN subinterfaces
  - FXOS supports up to 500 total VLAN subinterfaces in FXOS 2.4.1
  - FTD can also create VLAN subinterfaces on physical and EtherChannel interfaces
- Each instance can have a combination of different interface types

Data (Dedicated)



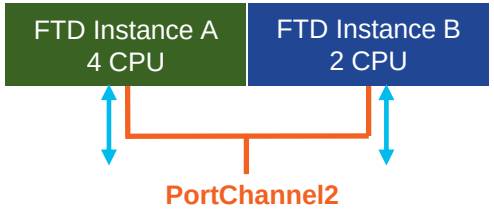
Supported Modes: Routed, Transparent, Inline, Inline-tap, Passive, HA
Supported Traffic: unicast, broadcast, multicast

Data-Sharing (Shared)



Supported Modes: Routed (no BVI members), HA
Supported Traffic: unicast, broadcast, multicast

Mgmt/Firepower-Eventing



Supported Modes: Management, Eventing
Supported Traffic: unicast, broadcast, multicast

MAC Address Restrictions

- Virtual MAC addresses are auto-generated for all instance interfaces
  - All container instance interfaces use A2XX.XXYY.YYYY format

Default prefix derived from a chassis MAC or user-defined

Counter that increments for every interface

- Manual MAC address configuration within FTD is still available
  - Must be unique across all instances on a shared interface (obviously)
  - Must be unique for all Supervisor VLAN subinterfaces under one parent
  - Supervisor faults are raised for all MAC address conflicts

Network Interface Scalability

- Supervisor has strict hardware limits on forwarding tables
  - Use show detail under scope fabric-interconnect to monitor
  - Limits apply across all standalone modules in a chassis or a cluster
- Ingress VLAN Group Entry Count defines maximum FXOS VLAN ID count
  - Up to 500 total entries or unique Supervisor VLAN subinterfaces
  - Re-using same VLAN ID under two parent interfaces consumes 2 entries
- Switch Forwarding Path Entry Count limits shared interfaces
  - Up to 1021 TCAM entries for ingress/egress path programming
  - Each Dedicated data interface consumes at least 2 entries
  - Entries for Shared Data interfaces grow exponentially with instance count

Interface Scalability Best Practices

- Refer to FXOS documentation for real-world examples
- Minimize the number of Shared Data (sub)interfaces
  - A single instance can have up to 10 shared (sub)interfaces
  - A single (sub)interface can be shared with up to 14 instances
- Sharing an interface across a subset of instances scales better
- Share subinterfaces rather than physical interfaces
  - One parent interface is best, multiple parents is also acceptable
  - 2 Dedicated, 10 Shared physical: 69% TCAM usage at 5 instances
  - 10 Dedicated, 10 Shared subinterfaces: 46% TCAM usage at 14 instances

Management and Licensing

- After FXOS 2.4.1 upgrade, must Reinitialize a module to deploy instances
- Different instances look and feel like completely independent FTD devices
  - Software upgrades, restarts, and configuration management are isolated
  - Each FTD instance has separate management IP, so add to FMC separately
  - FTD Expert Mode access is enabled on per-instance basis at provisioning
- No additional feature license to enable multi-instance capability
- Each FTD subscription license is shared by all instances on a module
  - License sharing requires all instances to be managed by a single FMC
  - With multiple FMCs, each requires a separate set of FTD subscriptions

Availability and Scalability

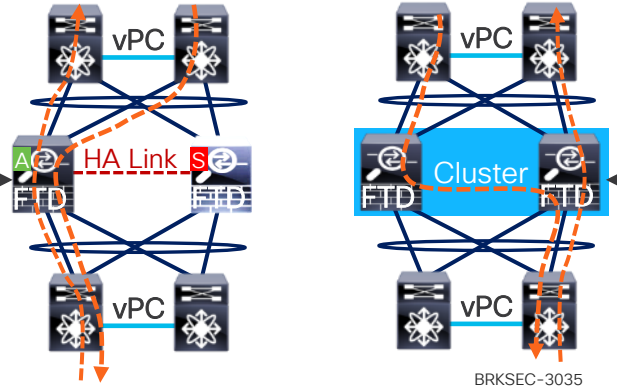
High Availability and Scalability Options

	High Availability	High Scalability (Firepower 9300 only)	High Availability and Scalability (Firepower 4100/9300 only)
ASA	• Active/Standby Failover (2 modules or appliances) • Active/Active Failover (2 modules or appliances)	• Intra-chassis Clustering (≤3 modules, 240Gbps) • Inter-chassis Clustering (≤16 modules, 1.2Tbps)	• Inter-chassis clustering (≤16 modules, 1.2Tbps)
FTD	• Active/Standby HA (2 modules or appliances)	• Intra-chassis Clustering (≤3 modules, 100Gbps)	• Inter-chassis clustering (≤6 modules, 270Gbps)
Radware vDP	–	• Intra-chassis Clustering (≤3 modules, 54Gbps)	• Inter-chassis Clustering (≤16 modules, 288Gbps)

FTD High Availability and Clustering

- FTD inherits failover and clustering infrastructure from ASA
  - Replicates full NGFW/NGIPS configuration and opaque flow state
  - Supports all NGFW/NGIPS interface modes
  - Interface and Snort instance (at least 50%) health monitoring
  - Zero-Downtime upgrades for most applications
- Ensures full stateful flow symmetry in both NGIPS and NGFW modes

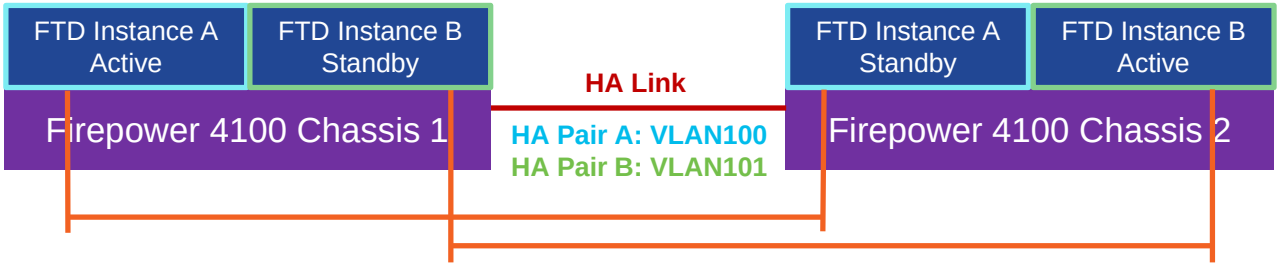
HA/Failover: Both directions of a flow traverse a single active unit



Clustering: All packets for a flow are redirected to connection Owner

Multi-Instance High Availability

- Container instances support inter-chassis HA only
  - Two instances are configured into an Active/Standby HA pair
  - Share single physical HA link with one VLAN per instance pair

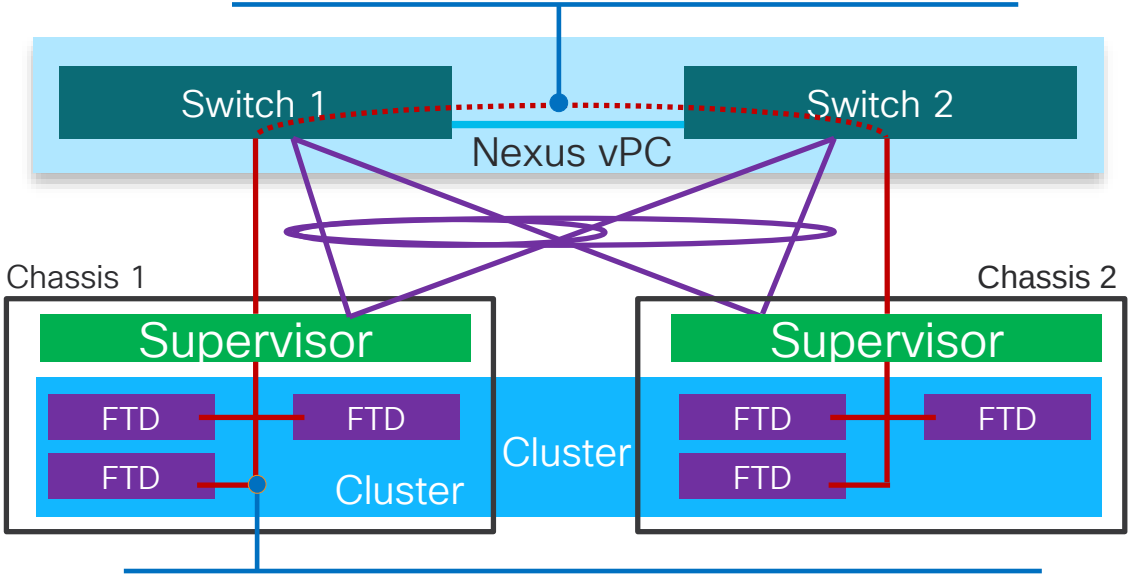


- An HA pair allows differently sized instances for seamless resizing
  - Stateful HA is supported but not guaranteed when downsizing

FTD and ASA Clustering Overview

Inter-Chassis Cluster Control Link

- Cluster of up to 16 modules across 5+ chassis
- Off-chassis flow backup for complete redundancy



Intra-Chassis Cluster Control Link

- Same-application modules can be clustered within chassis
- Bootstrap configuration is applied by Supervisor

Clustering Changes for Firepower 4100/9300

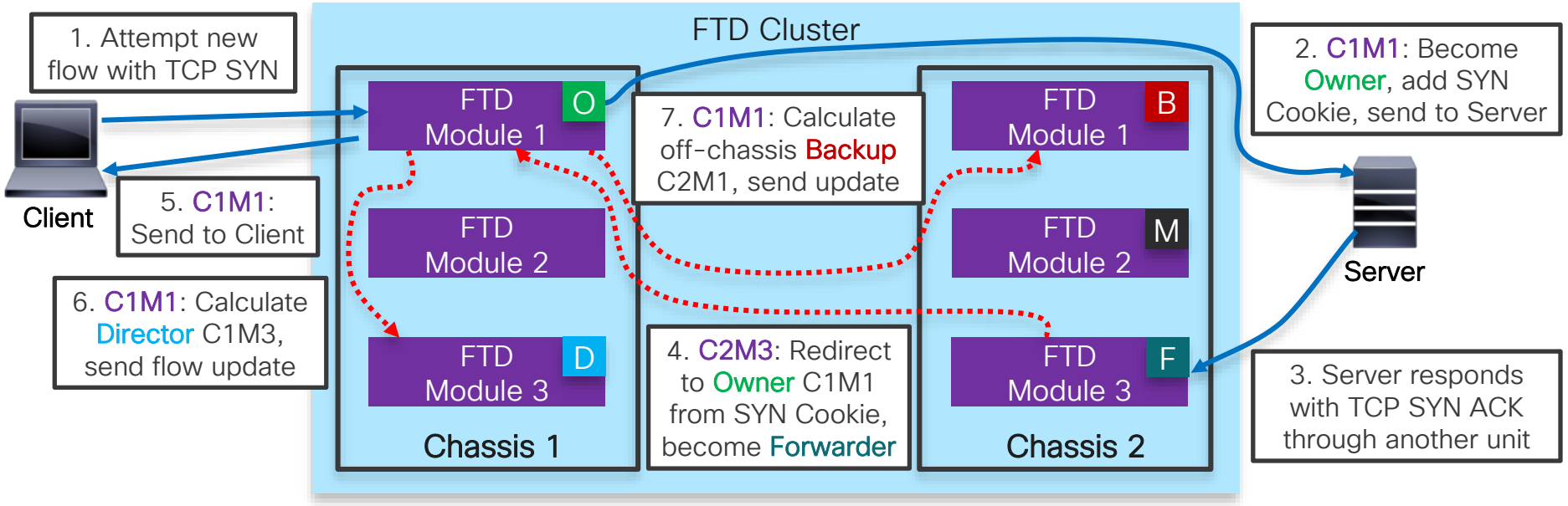
- Only Spanned Etherchannel interface mode is supported
- Remote flow backup for N+1 chassis-level fault tolerance
- Firewall context mode on ASA and SSL/TLS ciphers are replicated
- HTTP flows are not replicated by default until 5 seconds of uptime

```
asa(config)# cluster replication delay http
```

- Chassis- and cluster-level overflow protection syslogs

```
%ASA-6-748008: CPU load 80% of module 1 in chassis 1 (unit-1-1) exceeds overflow
protection threshold CPU 75%. System may be oversubscribed on member failure.
%ASA-6-748009: Memory load 80% of chassis 1 exceeds overflow protection threshold
memory 78%. System may be oversubscribed on chassis failure.
```


New TCP Flow with FTD Inter-Chassis Clustering



M Master

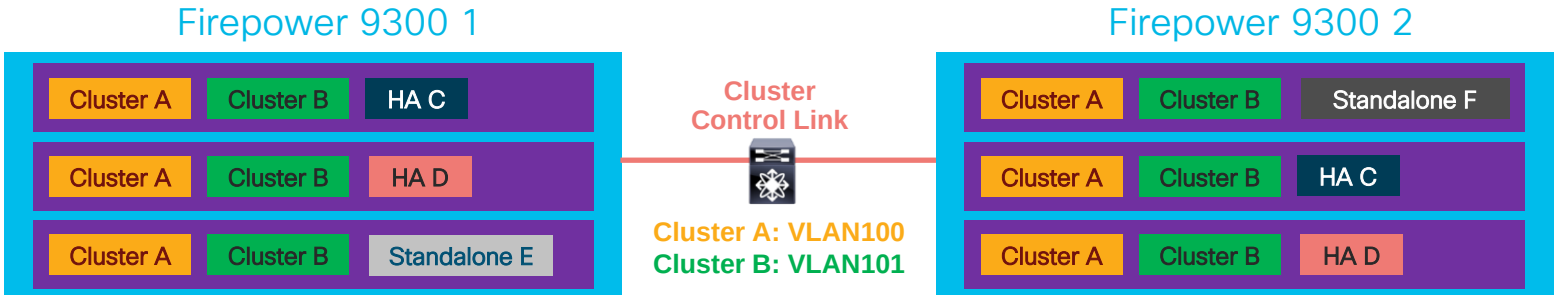
Global Role

O Owner D Director F Forwarder B Off-Chassis Backup

Per-Connection Roles

Multi-Instance Clustering

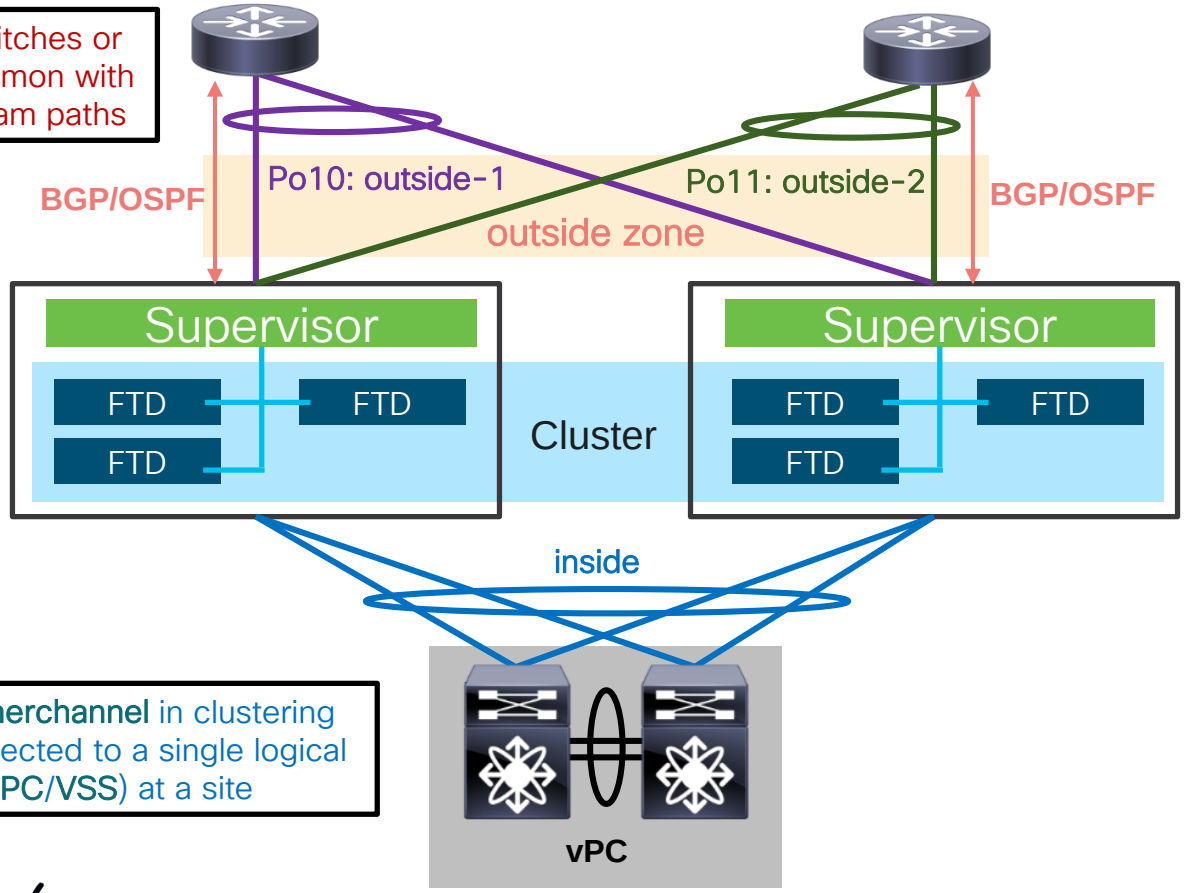
- Targeting FTD 6.6 and FXOS 2.8.1 releases
  - Instance-level clustering with one cluster member instance per module
  - Shared CCL, but no shared data interfaces between instance clusters
  - Unused resources can be used for standalone or HA instances



- Mixed hardware in a cluster for container instances only
  - E.g. Firepower 4120 and 4145, Firepower 9300 SM-24 and SM-44

Equal Cost MultiPath with Traffic Zones

Standalone switches or routers are common with multiple upstream paths



Solution: Create a separate Spanned Etherchannel logical interface per upstream device and group them into a single ECMP Traffic Zone with FlexConfig

Edit FlexConfig Object

Name: ECMP

Description:

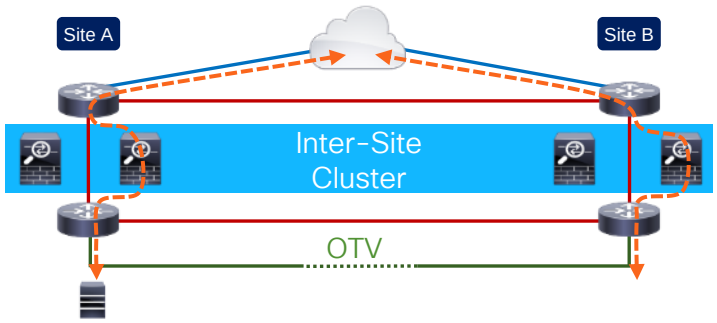
Insert

```
zone OUTSIDE ecmp

interface Port-Channel10
 zone-member OUTSIDE

interface Port-Channel11
 zone-member OUTSIDE
```

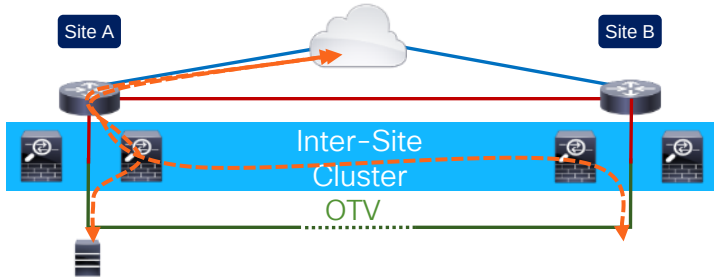
A Spanned Etherchannel in clustering should be connected to a single logical switch (vPC/VSS) at a site

Inter-Site Clustering with ASA or FTD

- North-South insertion with LISP inspection and owner reassignment

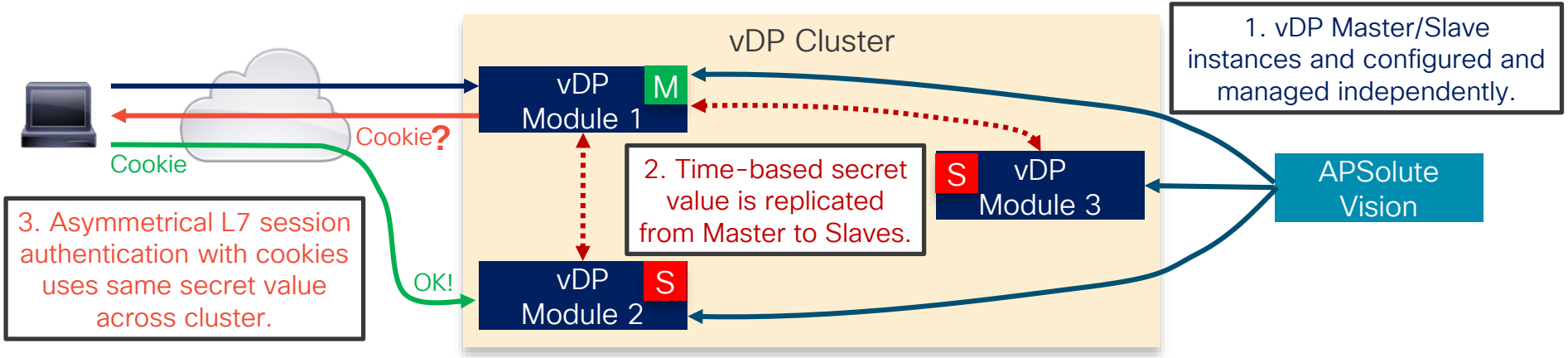


- East-West insertion for first hop redundancy with VM mobility



Radware vDP Clustering

- Requires intra-chassis ASA or FTD clustering for operation
  - Control link is shared with primary application and automatically configured
  - Health checks tie primary application and vDP instances on a module together

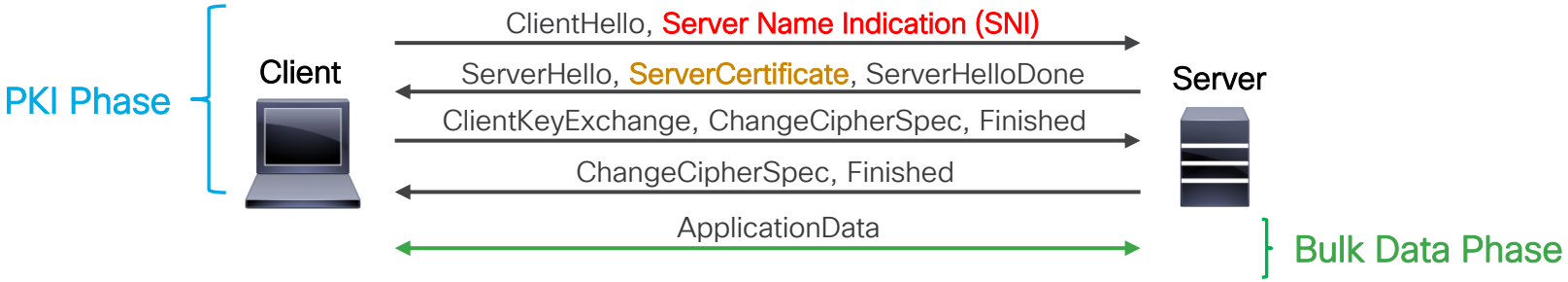


Turbo Performance Mode

- Automatically enabled on all Firepower 9300 modules in FXOS 2.0.1
- Accelerates FTD and ASA performance on demand
- All x86 CPU cores on a module temporarily increase clock frequency
  - Triggered when 25% of ASA or FTD Data Plane cores reach 80% load
  - Disabled when all cores drop below 60% load
  - Boosts performance by 10-20%

Transport Layer Security

- Secure Sockets Layer (SSL) is broken, obsolete and no longer in use
- Transport Layer Security (TLS) is the current generic protocol layer



- Some detectors do not need full session decryption until TLS 1.3
  - Cleartext SNI extension indicates where client may be going – spoofable
  - ServerCertificate contains server identity – legitimate, if CA is trusted

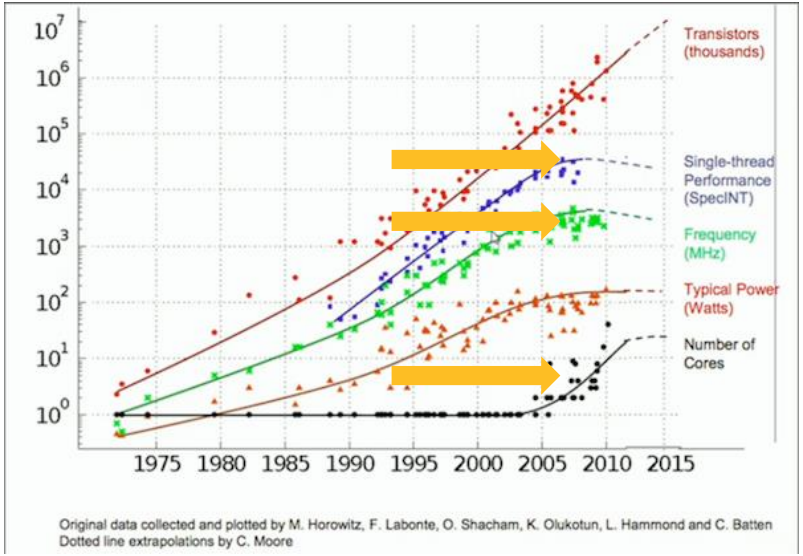
Firepower TLS Inspection

- Standard-based **Man-in-the-Middle** (**MITM**) decryption

- **Public Key Pinning** breaks **Resign** mode
  - Client certificate authentication or custom encryption always break MITM
- **FTD 6.3** enables TLS inspection in hardware on all platforms
  - Up to 6x throughput improvement with large transfers (Bulk Data)
  - Up to 26x connections-per-second improvement with a transactional profile (PKI)
- Passive **TLS Visibility** for **TLS 1.3** is targeted for **FTD 6.7**
  - Enables **AVC** and **URL Categorization** functionality without decryption
  - Minimizes impact on application traffic from **Do Not Decrypt** verdicts

Single-Flow Performance Considerations

- A single stateful flow must be processed by one CPU core at a time
  - Trying to share a complex data structure leads to race conditions
  - Stateless parallel processing leads to out-of-order packets
- No magic trick to single-flow throughput
  - Deploy more powerful CPU cores
  - Reduce the amount of security inspection
- Pay performance price for real security
  - … or deploy a router or a switch instead



Source: https://science.energy.gov/~/media/ascr/ascac/pdf/reports/2013/SC12_Harrod.pdf

Managing Single-Flow Throughput

- Roughly estimated as overall throughput divided by Snort cores on slide 50
  - 43Gbps of 1024-byte AVC+IPS on SM-44 / 48 Snort cores = 900Mbps
  - Similar on most high-end ASA, FirePOWER, and Firepower platforms
  - Egress Optimization improves throughput by up to 20% in FTD 6.4 NGIPS mode
  - Reducing impact on all flows from few superflows is more important
- Checking if an NGFW automatically reduces inspection is easy
  - Transfer multiple benign and malicious files over a single SMB session
  - Use HTTP Pipelining to service multiple requests over one TCP connection
- "What does your security policy tell you to do?"
  - NGFW performance capacity must not dictate your security policy
  - Flow Offload vs Intelligent Application Bypass (IAB)

Flow Offload on Firepower 4100 and 9300

- Trusted flow processing with limited security visibility in Smart NIC
  - Up to 39.7Gbps of single-flow UDP with 1500-byte packets
  - Use for long-lived connections only
- Supports up to 4M offloaded stateful connections in FXOS 2.3.1
- Static offload for unicast flows on ASA with IP/SGACL in MPF

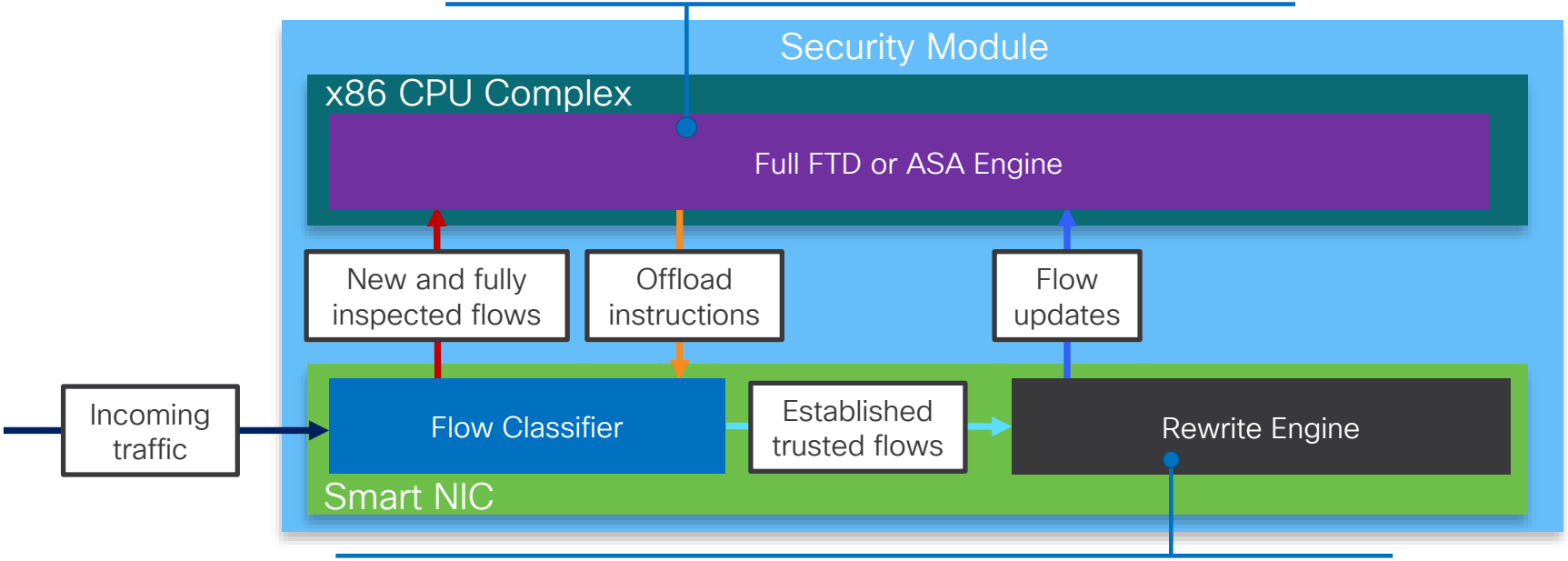
```
policy-map OFFLOAD_POLICY
 class TRUSTED_FLOWS
  set connection advanced-options flow-offload
```

  - Offload multicast in transparent mode with 2 bridge group ports in ASA 9.6(2)
- Prefilter offload policy for IP/TCP/UDP Fastpath rules in FTD 6.1
- Dynamic Flow Offload for Trusted and Whitelisted flows in FTD 6.3

Flow Offload Operation

Full Inspection

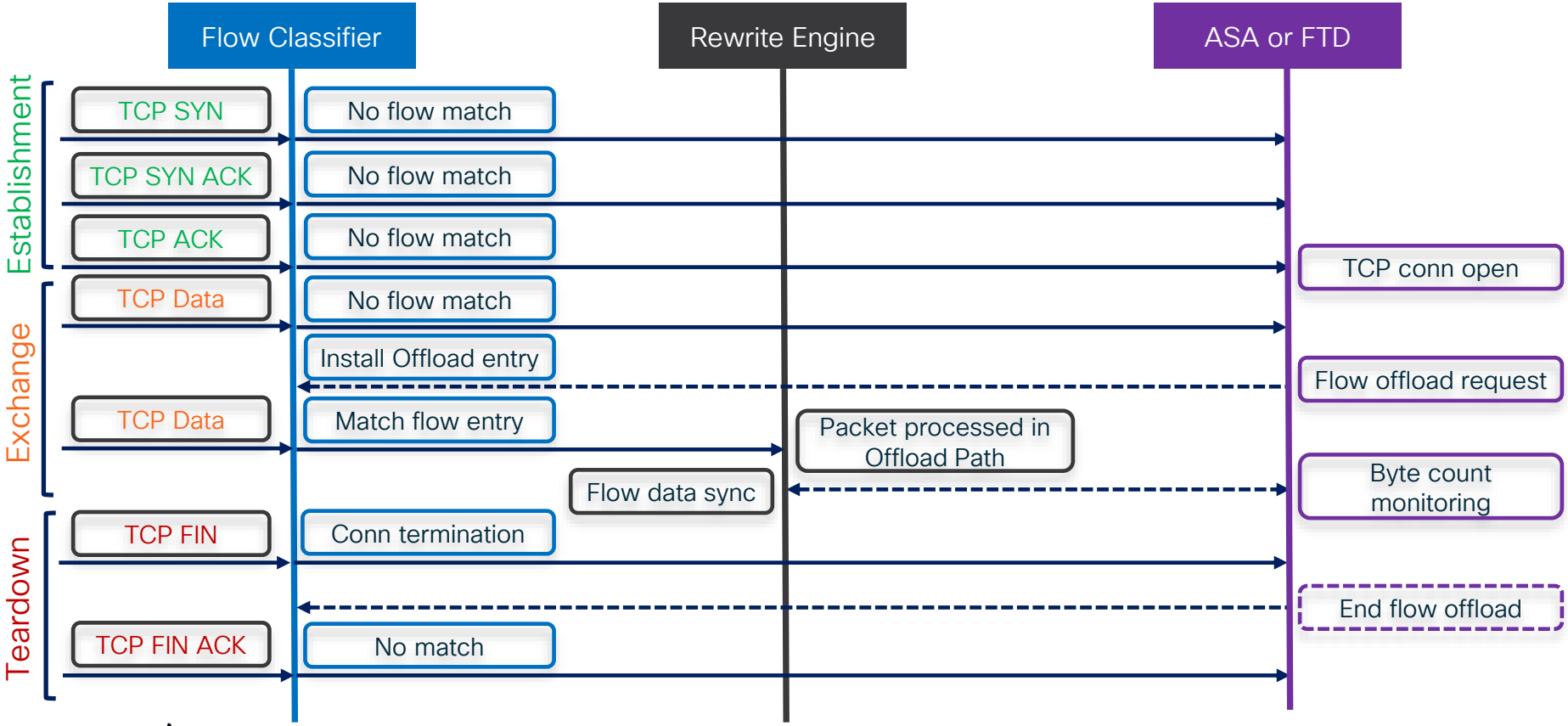
- Dynamically program Offload engine after flow establishment
- Ability to switch between Offload and full inspection on the fly



Flow Offload

- Limited state tracking, NAT/PAT, TCP Seq Randomization
- 20-40Gbps per single TCP/UDP flow, 2.9us UDP latency, 4M tracked flows

TCP Flow Handling with Flow Offload



Deployment Example: FTD Container Instances on Firepower 4100

Firepower Chassis Manager (FCM)

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

FP-MI-LAB 198.18.133.10

Model: **Cisco Firepower 4110 Security Appliance** | Version: **2.7(1.92)** | Operational State: **Operable**

CONSOLE MGMT USB

Power 1 - **Running**

Power 2 - **Running**

Network Module 1: 1 3 5 7 / 2 4 6 8

Network Module 2 : Empty

Network Module 3 : Empty

FAULTS		INTERFACES		DEVICES & NETWORK		LICENSE	INVENTORY		
0(0) CRITICAL	9(9) MAJOR	3 DOWN	5 UP	0 DOWN	1 UP	Smart Agent DISABLED	1(1) Security Engine	6(6) Fans	2(2) Power Supplies

Select All Faults | Cancel Selected Faults | Acknowledge

Severity	Description	Cause	Occurrence	Time	Acknowledg...
MAJOR	The password encryption key has not been set.	password-encryption-ke...	1	2019-03-26T22:20:20.626	no
MAJOR	ether port 1/6 on fabric interconnect A oper state: link-down, reason: Link ...	link-down	1	2019-12-09T23:04:37.989	no
MAJOR	Virtual interface 1061 link state is down	vif-down	2	2020-01-03T17:54:22.690	no
MAJOR	lan Member 1/7 of Port-Channel 40 on fabric interconnect A is down, mem...	membership-down	1	2020-01-03T17:45:28.572	no
MAJOR	lan Member 1/6 of Port-Channel 40 on fabric interconnect A is down, mem...	membership-down	1	2020-01-03T17:45:28.572	no

5 Successful Login in last 24 hrs - View Details | Fri Jan 03 2020 at 17:43:45 from - 198.18.133.36

Logical Device Overview

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

FP-MI-LAB 198.18.133.10

Model: **Cisco Firepower 4110 Security Appliance** | Version: **2.7(1.92)** | Operational State: **Operable**

CONSOLE MGMT USB

Power 1 - **Running**

Power 2 - **Running**

Network Module 1

1 3 5 7

2 4 6 8

Network Module 2 : Empty

Network Module 3 : Empty

FAULTS		INTERFACES		DEVICES & NETWORK		LICENSE	INVENTORY		
0(0)	9(9)	3	5	0	1	Smart Agent	1(1)	6(6)	2(2)
CRITICAL	MAJOR	DOWN	UP	DOWN	UP	DISABLED	Security Engine	Fans	Power Supplies

Devices

Security Module 1

73% (16 of 22) Cores Available

Interface Forwarding Utilization

Ingress VLAN Group Entry Utilisation (Current/Max): 1/500

Switch Forwarding Path Entry Utilisation (Current/Max): 21/1021

5 Successful Login in last 24 hrs - View Details | Fri Jan 03 2020 at 17:43:45 from - 198.18.133.36

Interface Configuration

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

Network Module 1: 1, 3, 5, 7 / 2, 4, 6, 8
CONSOLE | MGMT | USB
Network Module 2 : Empty
Network Module 3 : Empty

All Interfaces | Hardware Bypass

Add New | Filter..

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management								
Port-channel40	data					Full Duplex	no	failed	
Port-channel40.10	data			Instance-1	10				
Ethernet1/6									
Ethernet1/7									
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	failed	
Ethernet1/1	mgmt					Full Duplex	no	up	
Ethernet1/2	data	10gbps	10gbps	Instance-1		Full Duplex	no	up	
Ethernet1/3	data						no	up	
Ethernet1/4	data-sharing	10gbps	10gbps	Instance-1		Full Duplex	no	up	
Ethernet1/5	data	10gbps					no	up	
Ethernet1/8	data	10gbps	10gbps			Full Duplex	no	link-down	

Supervisor VLAN subinterface

Container instance allocation

Cluster Control Link (CCL)

Dedicated management

Dedicated data (Native or Container)

Shared data interface (Container only)

5 Successful Login in last 24 hrs - View Details | Fri Jan 03 2020 at 17:43:45 from - 198.18.133.36

Adding a Supervisor VLAN Subinterface

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

Network Module 1 (1, 3, 5, 7 / 2, 4, 6, 8) — CONSOLE, MGMT, USB
Network Module 2 : Empty
Network Module 3 : Empty

All Interfaces | Hardware Bypass

Add New | Filter..

Interface	Type	Admin Speed	Operation	Auto Negotiation	State
MGMT	Management				
Port-channel40	data	10gbps	indetermin	no	
Port-channel40.10	data				
Ethernet1/6					
Ethernet1/7					

Add Subinterface

Type: Data
Interface: Port-channel40
Subinterface ID: 20
VLAN ID: 20

OK | Cancel

Select Subinterface

Data or Data-Sharing type

Parent physical interface

Subinterface and VLAN ID do not have to match

Port-channel40	data	10gbps	indeterminate			Full Duplex	no	failed	
Port-channel40.10	data			Instance-1	10				
Port-channel40.20	data				20				
Ethernet1/6								down	
Ethernet1/7								down	

Creating an Instance Resource Profile

Overview | Interfaces | Logical Devices | Security Engine | **Platform Settings** | System | Tools | Help | admin

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- Syslog
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- **Resource Profiles**
- Network Control Policy
- Chassis URL

Add

Name	Description	Cores
Default-Small	Auto-created application resource-profile with 4 cpu-cores	6

Add Resource Profile

Name:* Medium

Description:

Number of Cores:* 12 Range : [6 to 22]

Specify even value for number of cores.

OK Cancel

Custom reusable name

Instance size in even number of CPU cores (6-86, except 8)

Adding a Container Instance

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

Logical Device List

(1 instances) 73% (16 of 22) Cores Available

Add new device

Refresh | Add | Standalone | Cluster

Container instances only support Standalone (non-clustered) deployments until FTD 6.6

Instance-1 Standalone Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115	Default-Small	198.18.133.11	198.18.128.1	Ethernet1/1	online

Interface Name	Type
Ethernet1/2	data
Ethernet1/4	data-sharing
Port-channel40.10	data

Attributes

Cluster Operational Status : not-applicable
FIREPOWER-MGMT-IP : 198.18.133.11
MGMT-URL : https://198.18.133.8/
HA-ROLE : standalone
UUID : 72848fd8-2e54-11ea-a8fe-d57c2349646e

Add Standalone

Device Name: Instance-2

Template: Cisco Firepower Threat Defense

Image Version: 6.5.0.115

Instance Type: Container

Before you add the first container instance, you must reinitialize the security module/engine so that the disk has the correct formatting. You only need to perform this action once.

OK | Cancel

Locally significant name

Application type

Application version from locally loaded images

Native and Container instances cannot mix on one module

Assigning FTD Interfaces

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

Save | Cancel

Provisioning - Instance-2

Standalone | Cisco Firepower Threat Defense | 6.5.0.115

One dedicated and one shared data interfaces

Supervisor VLAN subinterface for HA

Data Ports

- Ethernet1/3
- Ethernet1/4
- Ethernet1/5
- Ethernet1/8
- Port-channel40
- Port-channel40.20

Ethernet1/3

Ethernet1/4

Port-channel40.20

Port-channel40

FTD - 6.5.0.115
Click to configure

Configure logical device properties for chassis (4100) or modules (9300)

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115					

Interface Name	Type
Ethernet1/3	data
Ethernet1/4	data-sharing
Port-channel40.20	data

Configuring FTD Instance Size and Management

Overview | Interfaces | Logical Devices | Security Engine | System | Tools | Help | admin

Provisioning - Instance-2
Standalone | Cisco Firepower Threat Defense | 6.5.0.115

Save | Cancel

Data Ports
- Ethernet1/3
- Ethernet1/4
- Ethernet1/5
- Ethernet1/8
- Port-channel40
- Port-channel40.20

Application	Version	Resource Pro
FTD	6.5.0.115	

Interface Name
- Ethernet1/3
- Ethernet1/4
- Port-channel40.20

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information | Settings | Agreement

SM 1 - 16 Cores Available

Resource Profile: Medium

Interface Information

Management Interface: Ethernet1/1

Management

Address Type: IPv4 only

IPv4

Management IP: 198.18.133.12

Network Mask: 255.255.192.0

Network Gateway: 198.18.128.1

OK | Cancel

Pre-created CPU core sizing profile

Dedicated FTD management interface

Management interface addressing: IPv4, IPv6, or both

Dedicated FTD management IP

FTD management interface subnet

Default gateway for FTD management interface

Configuring FTD Device Settings

Overview | Interfaces | Logical Devices | Security Engine | System | Tools | Help | admin

Provisioning - Instance-2
Standalone | Cisco Firepower Threat Defense | 6.5.0.115

Data Ports
- Ethernet1/3
- Ethernet1/4
- Ethernet1/5
- Ethernet1/8
- Port-channel40
- Port-channel40.20

Application	Version	Resource Pro
FTD	6.5.0.115	

Interface Name
- Ethernet1/3
- Ethernet1/4
- Port-channel40.20

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information | **Settings** | Agreement

Permit Expert mode for FTD SSH sessions:	yes
Search domains:	cisco.com
Firewall Mode:	Routed
DNS Servers:	192.168.0.254
Fully Qualified Hostname:	ngfw-2.cisco.com
Password:	••••••••
Confirm Password:	••••••••
Registration Key:	••••••••
Confirm Registration Key:	••••••••
Firepower Management Center IP:	198.18.133.8
Firepower Management Center NAT ID:	ftdb
Eventing Interface:	None

OK | Cancel

- Expert mode access is disabled for container instances by default
- Optional default domain name
- Routed of transparent NGFW mode
- Optional default DNS server
- Optional FTD device FQDN
- FTD management password for CLI
- FMC management registration key must match the device
- FMC real IP address to connect with
- Optional unique identification string to use instead of IP
- Optional interface for FTD events

FTD Instance Installation

Overview | Interfaces | **Logical Devices** | Security Engine | Platform Settings | System | Tools | Help | admin

Refresh | Add

Logical Device List (2 instances) 73% (16 of 22) Cores Available

Instance-2 Standalone Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115	Medium	198.18.133.12	198.18.128.1	Ethernet1/1	installing

Instance-1 Standalone Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115	Default-Small	198.18.133.11	198.18.128.1	Ethernet1/1	online

Monitor logical device deployment status

Overview | Interfaces | **Logical Devices** | Security Engine | Platform Settings

Refresh | Add

Logical Device List (2 instances) 19% (4 of 22) Cores Available

Instance-2 Standalone Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115	Medium	198.18.133.12	198.18.128.1	Ethernet1/1	online

Instance-1 Standalone Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.5.0.115	Default-Small	198.18.133.11	198.18.128.1	Ethernet1/1	online

Adding FTD Instance to FMC

FTD application real management IP

Add Device

Host:† 198.18.133.12

Display Name: FTD-Instance-2

Registration Key:* Cisco123

Group: None

Access Control Policy:* Base_ACP

Smart Licensing

Malware ☑

Threat ☑

URL Filtering ☑

Advanced

Unique NAT ID:† ftdb

Transfer Packets ☑

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from smart license page

Register Cancel

Optional matching identification string to use instead of IP

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (1) | Error (0) | Warning (0) | Offline (0) | Normal (1) | Deployment Pending (0) Search Device Add

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (1)					
FTD-Instance-1 198.18.133.11 - Routed	FTD on Firepower 4110	6.5.0	198.18.133.10 Security Module - 1 (Container)	Base, Threat (2 more...)	Base_ACP

Add new FTD device

Device

High Availability

Stack

Group

Unique display name in FMC

FMC registration key must match logical device configuration

Must assign a default main Access Control Policy

Shared licenses for container instances on single module and FMC

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (2) | Error (0) | Warning (0) | Offline (0) | Normal (2) | Deployment Pending (0) Search Device Add

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
FTD-Instance-1 198.18.133.11 - Routed	FTD on Firepower 4110	6.5.0	198.18.133.10 Security Module - 1 (Container)	Base, Threat (2 more...)	Base_ACP
FTD-Instance-2 198.18.133.12 - Routed	FTD on Firepower 4110	6.5.0	198.18.133.10 Security Module - 1 (Container)	Base, Threat (2 more...)	Base_ACP

Application Use Cases

Application Use Case Summary

- ASA is a powerful and scalable solution for basic stateful segmentation
  - Ease of integration and scaling in large and distributed data centers
  - Infrastructure and Internet edge protection for service providers
  - Scalable and fully featured RAVPN termination

Firewall

- FTD is a comprehensive threat-centric security solution
  - NGIPS for data center and service provider environments
  - NGFW for edge protection and single- or multi-site data centers

NGFW NGIPS

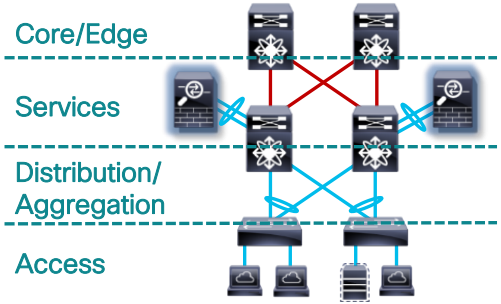
- Radware vDP is a behavioral DDoS mitigation solution
  - Internet edge protection for web commerce and service providers

DDoS

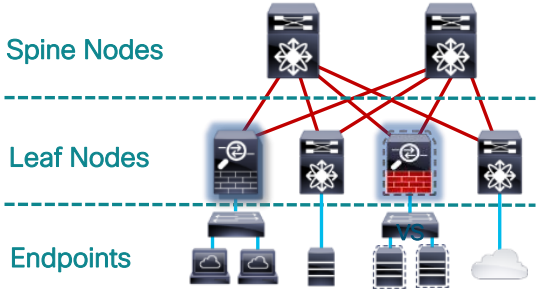
ASA and FTD in Data Center

- Routed or transparent insertion into common data center topologies
  - vPC, VxLAN, PBR, OSPFv2/v3, BGP-4, ECMP, NSF/GR, PIM-SM, BSR, ACI
  - Integrated Routing and Bridging (IRB) in ASA 9.7(1) and FTD 6.2

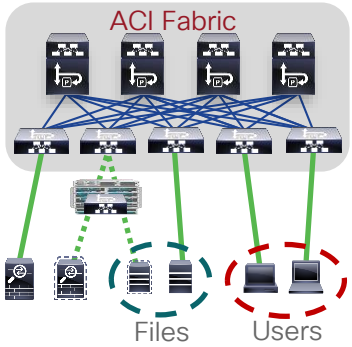
Layer 2 Data Center



Layer 3 Data Center

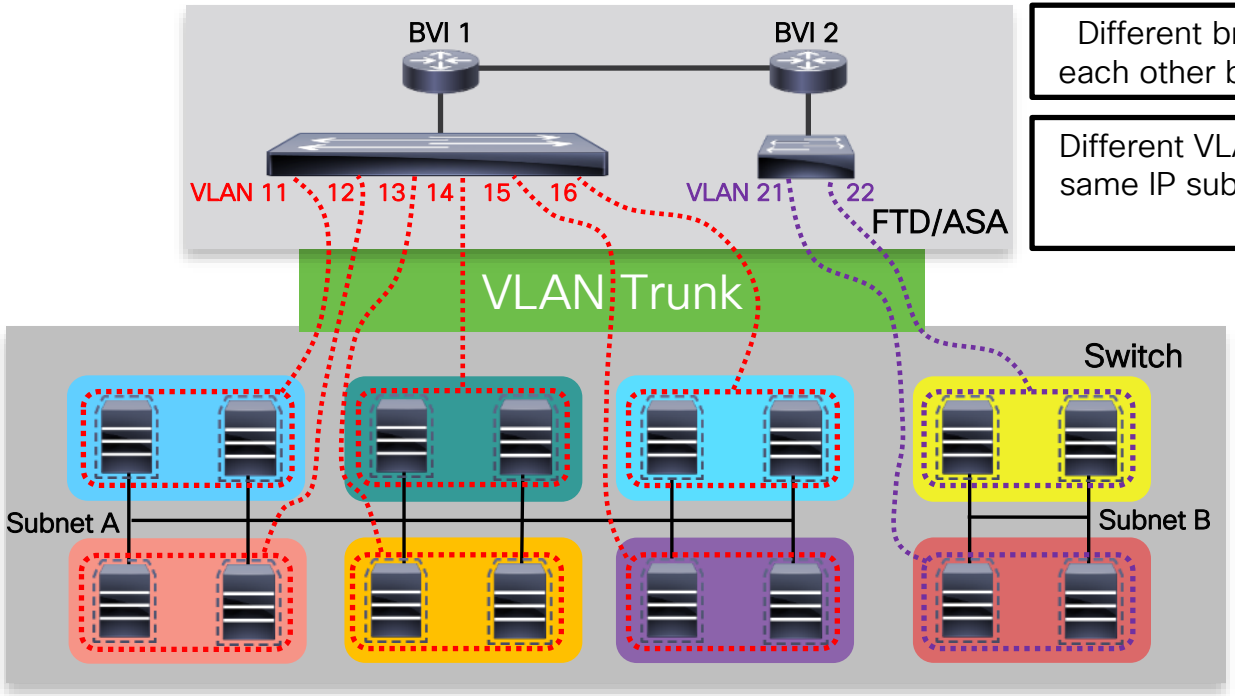


Application Centric Infrastructure



- Scalable IP and Trustsec policies in single or multiple contexts
- Same- and inter-site clustering with LISP integration

Data Center Segmentation with IRB



Different bridge groups (IP subnets) are routed to each other by a single FTD/ASA context or instance

Different VLAN/VxLAN segments (security zones) in same IP subnet are bridged together and separated by transparent FTD/ASA

Each security zone within a subnet is modeled as a separate VLAN (physical hosts) or VxLAN (virtual machines)

A single IP subnet contains endpoints from multiple different security zones

Private VLAN Remapping with ASA

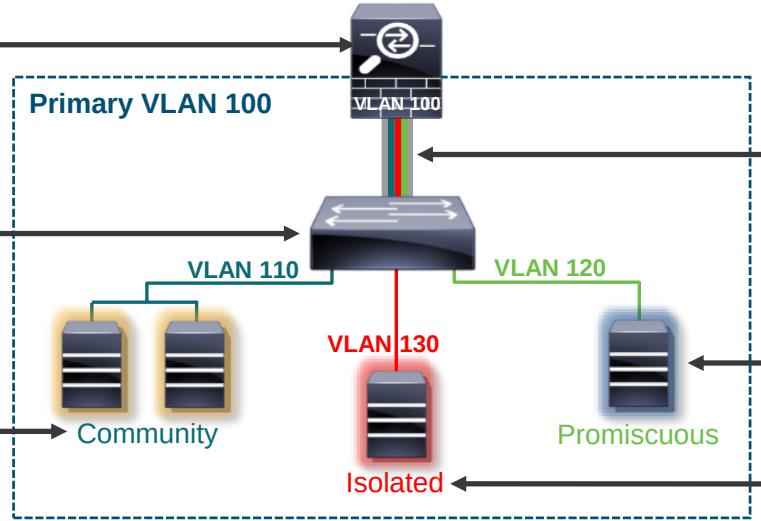
- ASA 9.5(2) can re-map a set of secondary VLANs to a primary VLAN

```
interface Ethernet1/3
 vlan 100 secondary 110, 120, 130
```

ASA maps frames received from **secondary VLANs** to **primary VLAN** subinterface and then processes them normally

Switch assigns ports to **secondary VLANs** and enforces connectivity between different port types within the **primary VLAN**

Community ports can only talk to each other and **promiscuous ports**



Private VLAN trunk transmits upstream traffic for all **secondary** and **primary** VLANs

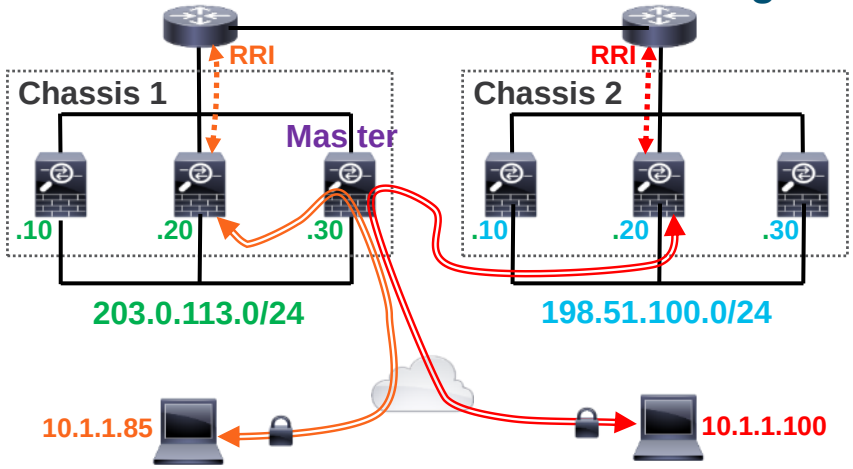
Promiscuous ports can talk to any other port

Isolated ports can only talk to **promiscuous ports**

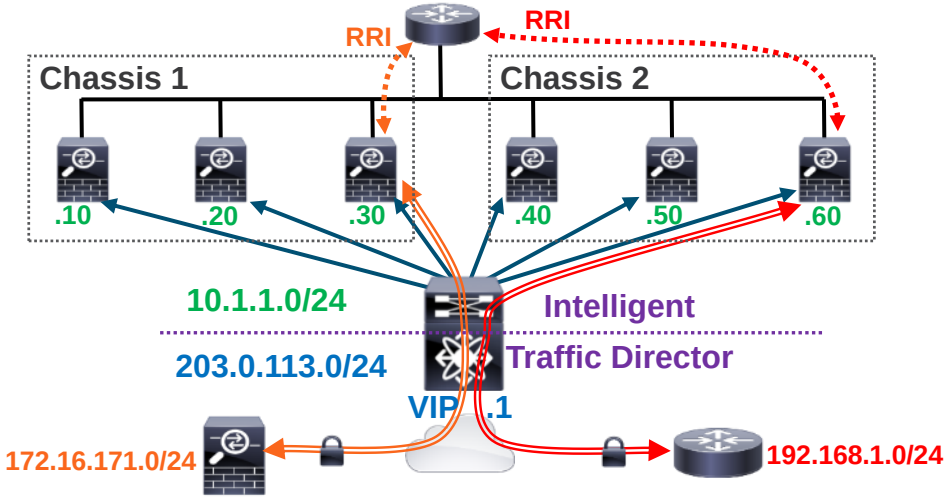
ASA and FTD for Scalable VPN Termination

- Use standalone modules or failover for scaling S2S and RA VPN
  - Reverse Route Injection (RRI) with dynamic crypto maps and OSPF/BGP

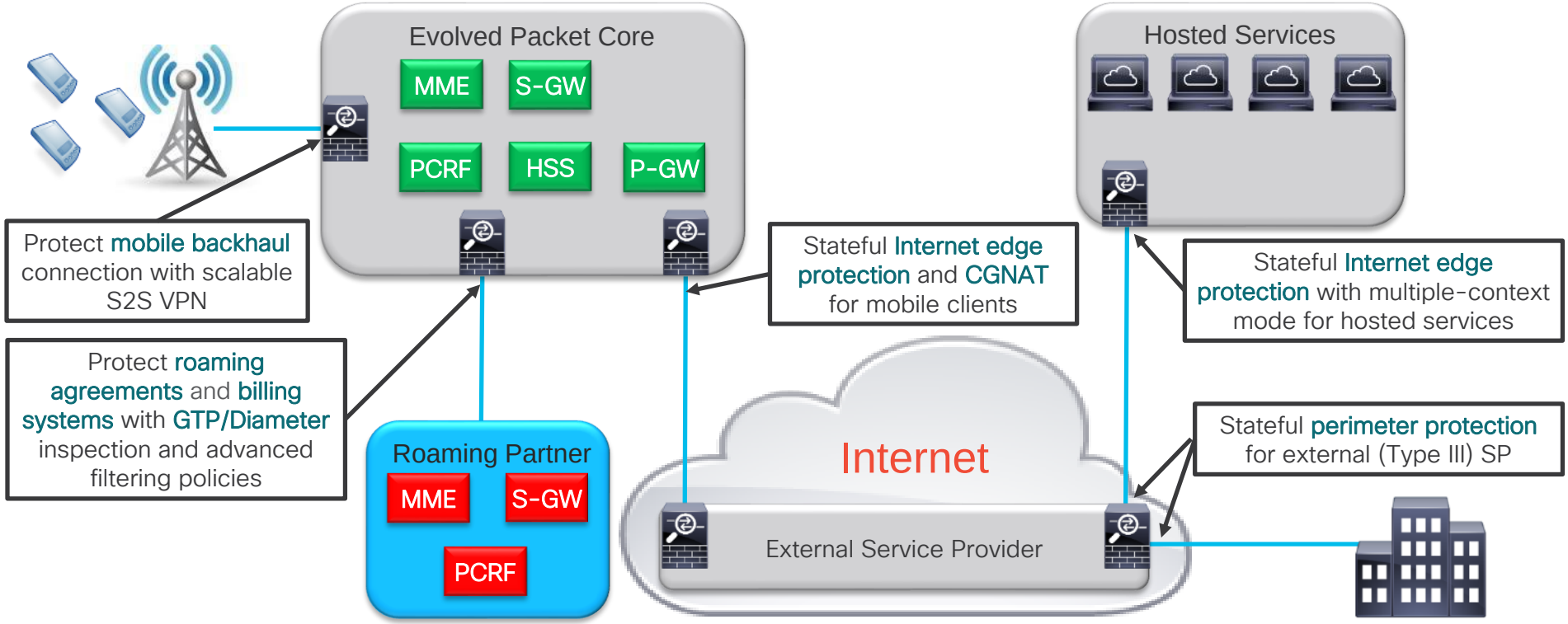
RAVPN with ASA Load-Balancing



ASA/FTD S2S VPN with Nexus ITD



ASA for Service Providers



ASA Application Inspection

- Protocol conformance, NAT/PAT rewrites, dynamic ACL pinholes
- SIP inspection for scalable VoIP environments (>10K calls per second)
- SCTP, Diameter, and GTPv2 inspection for Carriers in ASA 9.5(2)
- TLS Proxy with SIP; multi-core Diameter inspection in ASA 9.6(1)

Endpoints establish an inspected control channel TLS connection over TCP

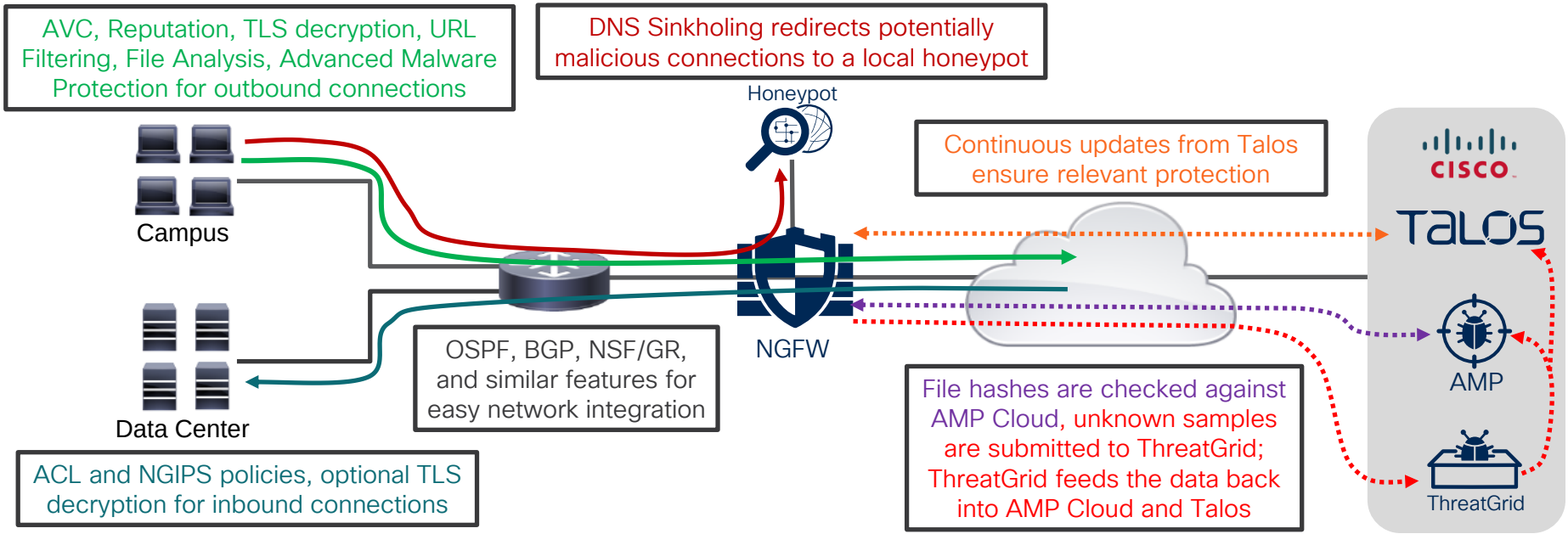
ASA uses pre-configured trustpoints to cut into TLS connection, inspect traffic, and open secondary connections as necessary

Carrier Grade NAT on FTD and ASA

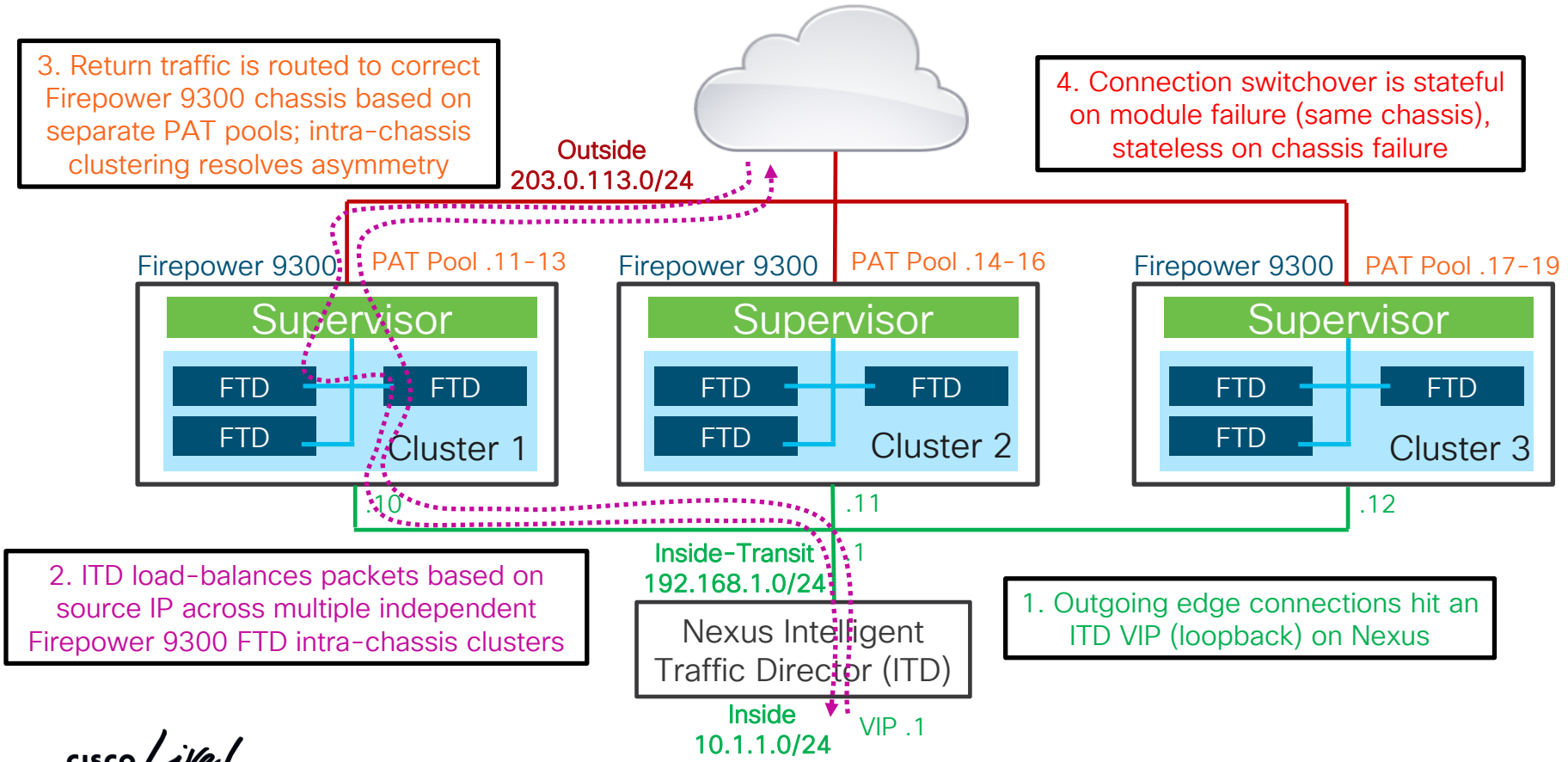
- Fully conforms to RFC6888 except Port Control Protocol (PCP) support
- High single-module capacity and further scalability with clustering
  - 60M+ concurrent NAT translation per module with ASA
  - 500K+ new translation creations per second per module with ASA
- Port Block Allocation for PAT reduces logging volume in ASA 9.5(2)
  - Each PAT client is assigned blocks of ports (512 each by default) for translation
  - A single syslog is recorded for each block allocation event

```
%ASA-6-305014: Allocated TCP block of ports for translation from inside:10.1.1.10 to
outside:20.1.1.10/1024-1535.
%ASA-6-305015: Released TCP block of ports for translation from inside:10.1.1.10 to
outside:20.1.1.10/1024-1535.
```


FTD as NGFW at the Edge

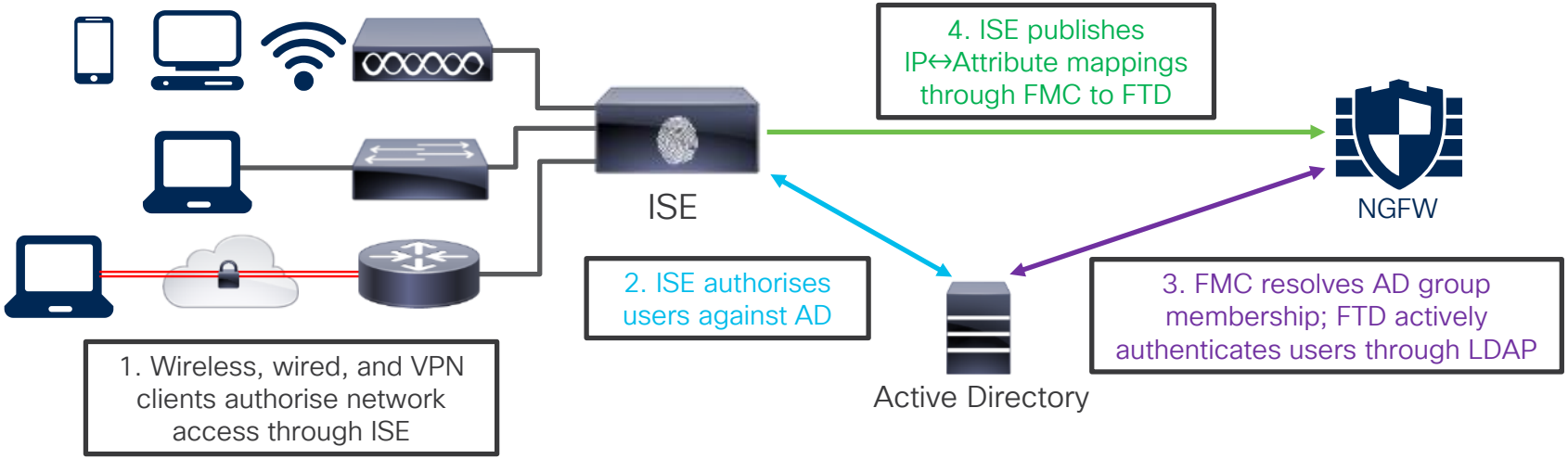


Scalable Edge NGFW with FTD and Nexus ITD



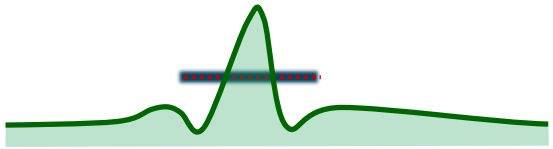
FTD Identity Management with pxGrid

- Extended identity attributes with **Platform eXchange Grid (pxGrid)**
  - User identity, Geolocation, Source Security Group and Tag, Device Type
  - Replaces **Firepower User Agent** with **ISE** or **ISE-PIC**



Behavioral DDoS with Radware vDP

- Behavioral detection for maximum efficacy and low false positives

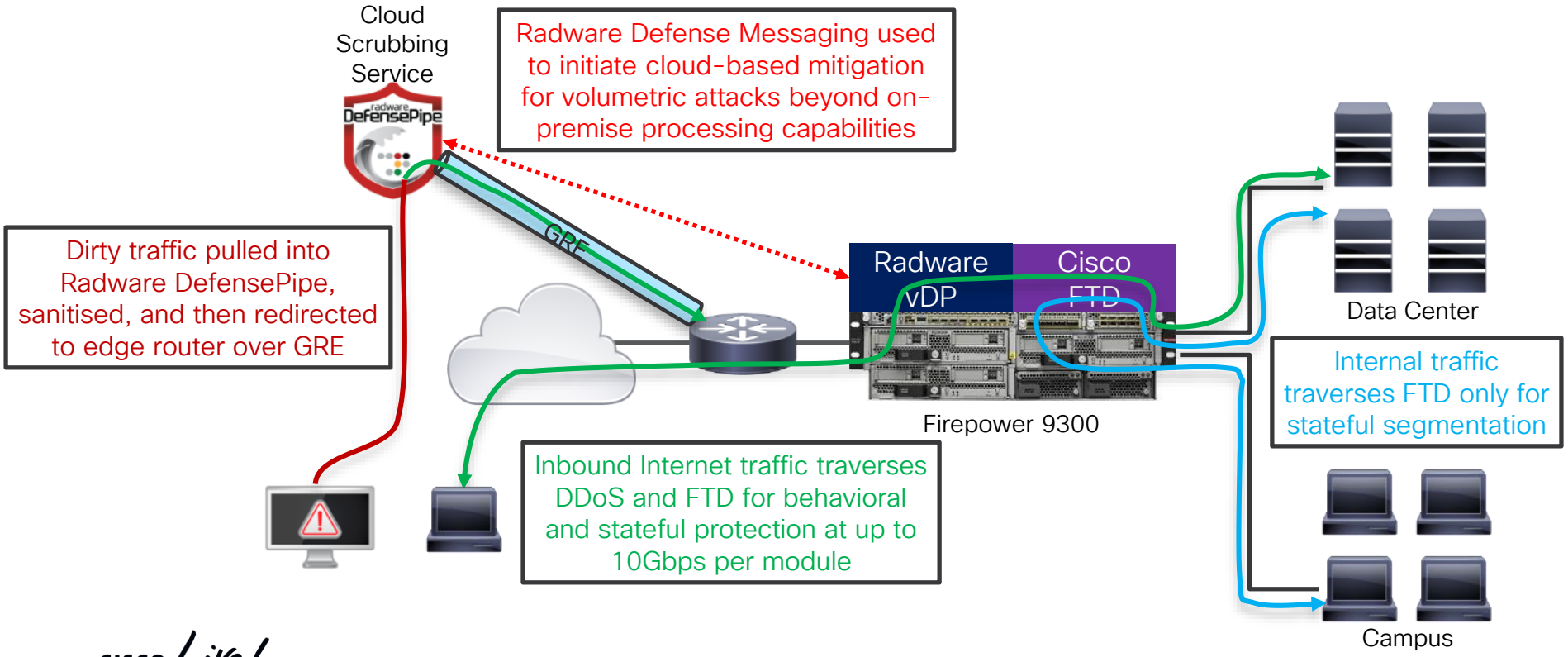


Rate-Based Detection

Behavioural Detection

- Effectively protects web, e-mail, VoIP, and other services
  - Adaptive behavioral DoS against IPv4/IPv6 TCP/UDP/ICMP/IGMP floods
  - SYN flood protection with active Layer 4 challenges
  - DNS flood protection with request/response record tracking
  - Application signature protection for HTTP, SMTP, FTP, POP3, SIP, SMB, SQL
  - Anomaly protection against basic malformed packets

FTD or ASA with DDoS in Enterprise



Closing Remarks

Firepower Platform Summary

- Next-generation security platform architecture
- Security service chaining with Cisco and third-party applications
- Classic stateful firewall, VPN, NGFW, NGIPS, and DDoS protection
- Powerful multi-instance capability with resource reservation
- Intra- and inter-chassis clustering for high scalability
- Flow Offload for real time applications

Questions?

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**