The bridge to possible

Cisco Secure Firewall Platforms

Deep Dive

Luke Bromirski

mr0vka@infosec.exchange

@lbromirski

BRKSEC-2239

cisco Live!

Cisco Webex App

Questions?

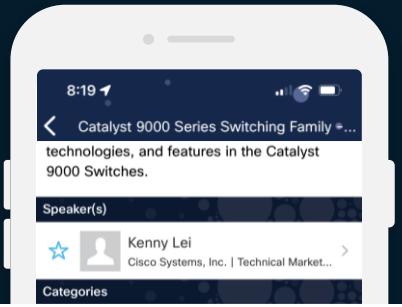
Use Cisco Webex App to chat with the speaker after the session

How

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

Webex spaces will be moderated by the Firewall Platform Team until June 7, 2024.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2239



Your Speaker

- CCIE #15929 (R&S/SP)
  CCDE #2012::17
- running community projects:
  BGP Blackholing PL, AS 112 cluster in Poland, PLNOG co-founder
- https://lukasz.bromirski.net/
- Leading **Firewall Platform Team** at Cisco Security Business Group

For years, that session was delivered by...

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

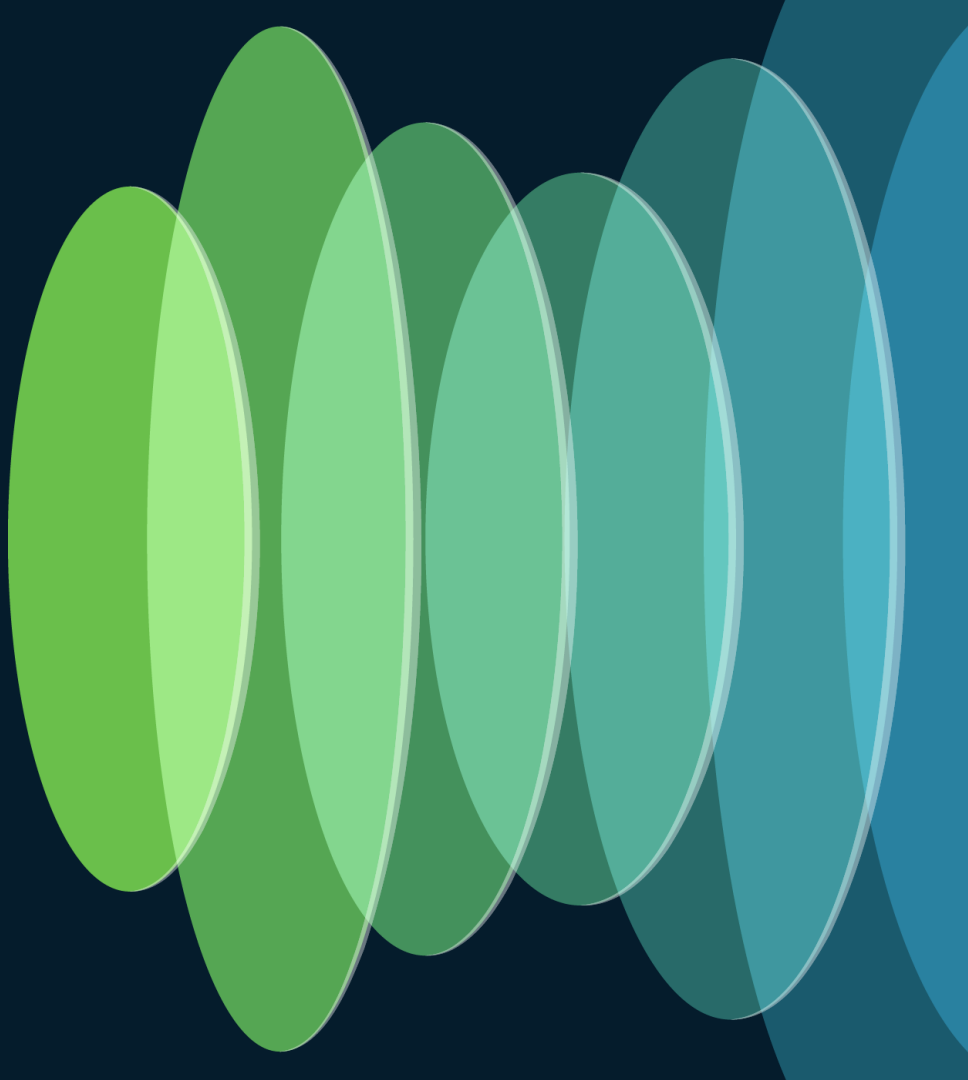
Portfolio CTO for Cloud and Network Security

Firewall Architecture, Threat Visibility, Hybrid Cloud

Agenda

- Platforms
- Innovations in
  - Threat
  - Performance
- Designing for High Availability
- Designing for Multi-Tenancy
- Designing for Internet Edge

Platforms



Cisco Secure Firewall

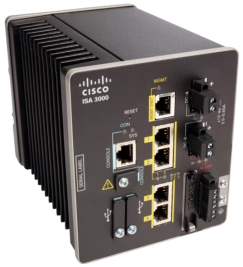
Physical appliances

Cisco Secure Firewall hardware appliances
running either ASA or FTD application

Private & Public cloud

Cisco Multicloud Defense, ASAv and FTDv application
Running on all major public cloud and private cloud hypervisors

IoT and integrations



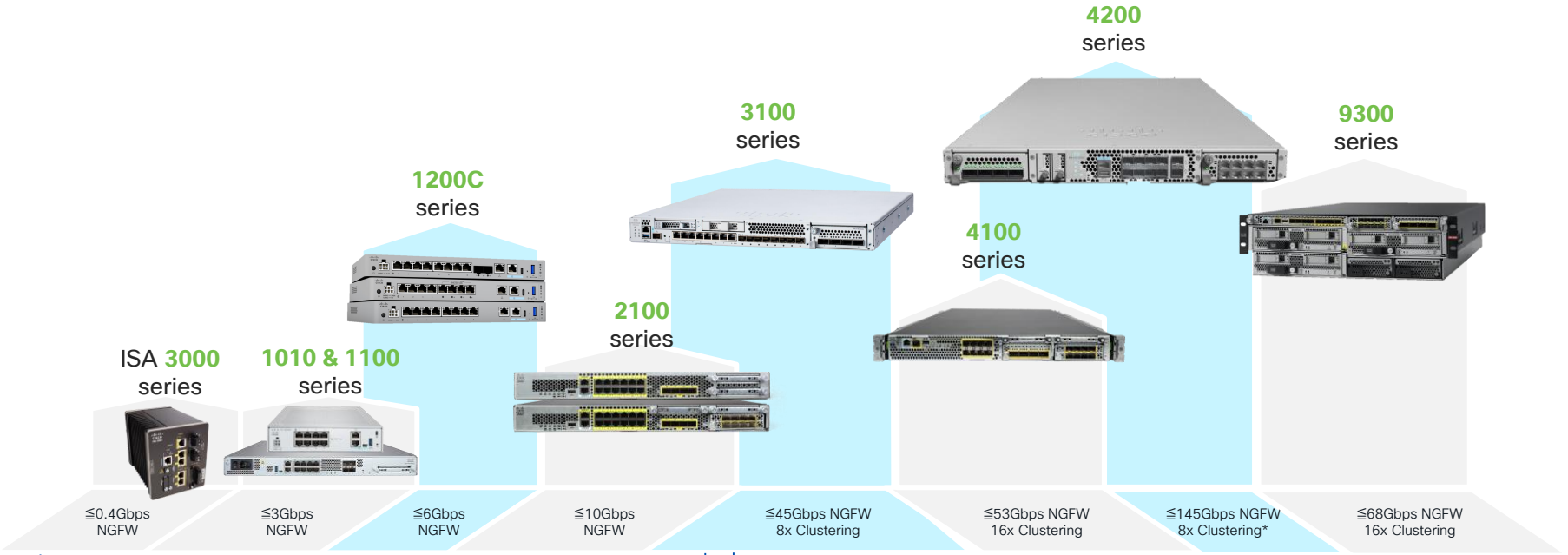
ISA 3000
Running either ASA or FTD application

Catalyst 9000
ASAc running as a VM

Meraki MX
Snort 3 running in container

Cisco Secure Firewall Hardware

Full coverage, from IoT/OT & Branch / SASE edge to Enterprise/Carrier Class modular chassis



Secure Firewall 4200 Series

FTD 7.4

ASA 9.20

- 3 models – 4215/4225/4245
  - 32-128 (64-256) cores (4245 has two CPUs)
  - 8x1/10/25G SFP/SFP+ and two Network Module bays
  - 256GB-1TB of RAM
  - Two NVMe slots, 1.8TB of RAID1 protected space
  - AC redundant PS
- Advanced FPGA and one to four VPN crypto hardware accelerators
- Clustering support on all models, up to 8 nodes
  - 16x clustering will come in future releases
- Up to 145Gbps for NGFW traffic profiles (~3x over 4100)
  - up to 45Gbps with 50% of TLS 1.2/1.3 mix
  - up to 140Gbps for IPsec traffic
- Up to 190Gbps for ASA traffic profiles (>2x over 4100)

Secure Firewall 4200 Series Overview

FTD 7.4

ASA 9.20

Appliance-Mode Security Platform for FTD or ASA Application

- Fixed configurations: 4215, 4225, 4245
- Lightweight virtual Supervisor module w/Multi-Instance and Clustering
- Integrated Datapath FPGA w/Flow Offload and Crypto Engines
- Rear dual redundant power supplies and triple fan trays

SFP Data Interfaces

- 8x1/10/25GE/**50**GE

1RU

NVMe Drives

- Up to 2x900GB in RAID1 on 4215/4225 (SED)
- Up to 2x1.8TB in RAID1 on 4245 (SED)

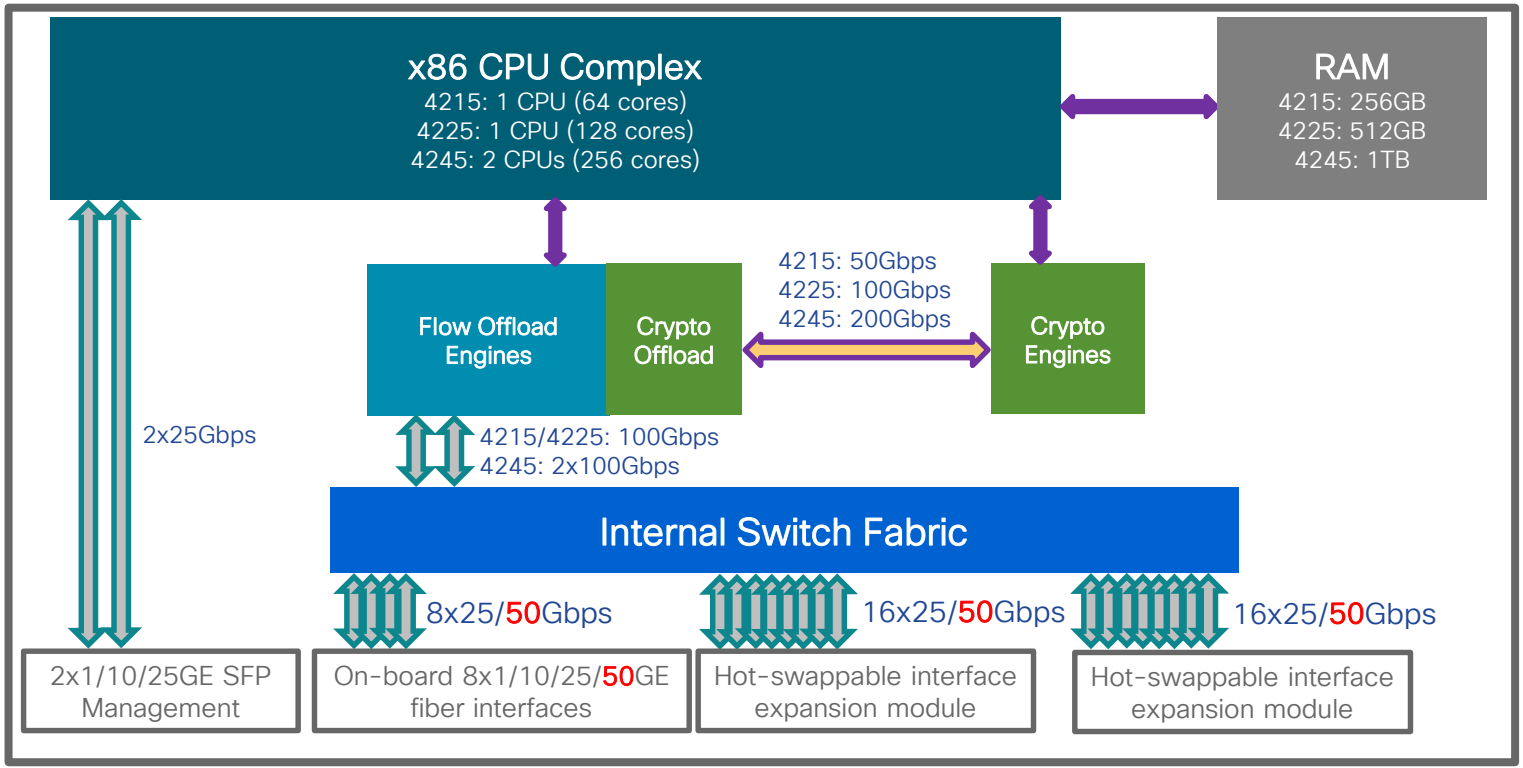
Expansion Network Modules

- Standard: 8x1/10GE, 8x1/10/25/**50**GE, 4x10/40GE, 2x100GE, 4x40/100/200GE, **2x200/400GE** SFP+ (with 7.6)
- Fail-to-Wire: 8x1GE Copper; 6x10GE or 6x25GE SFP+ (SR and LR variants)

Secure Firewall 4200 Series Architecture

FTD 7.4

ASA 9.20



Secure Firewall 4200 Performance

FTD 7.4

ASA 9.20

	4215	4225	4245
FW+AVC+IPS HTTP 1024B Avg Packet	65Gbps	85Gbps	145Gbps
IPsec VPN HTTP 1024B Avg Packet	45Gbps (45Gbps per tunnel)	80Gbps (57Gbps per tunnel)	140Gbps (57Gbps per tunnel)
TLS Decryption HTTP 1024B Avg Packet 50% Flows Decrypted	20Gbps	30Gbps	45Gbps

Up to 3x ↑ Boost in FW+AVC+IPS

Up to 6x ↑ Boost in IPsec VPN

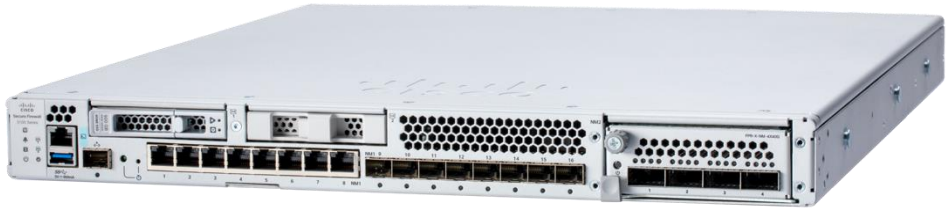
Up to 5x ↑ Boost in TLS Decrypt

Secure Firewall 3100 Series

FTD 7.1

ASA 9.17

- 5 models – 3105 & 3110/20/30/40
  - single CPU, 12-32 cores
  - 8x1G TX
  - 8x1/10G or 8x1/10/25G plus NetMod bay
  - 64-256GB of RAM
  - two SSD slots
  - AC/DC redundant PS (400W)
- Advanced NPU and VPN crypto hardware
- Clustering support on 3110-3140, up to 8x
- 17-45 Gbps for FW+AVC+IPS with 1024 bytes average packet size
- 11-39.4 Gbps for IPsec with 1024 bytes average packet size with release 7.2



Secure Firewall 3100 Series Overview

FTD 7.1

ASA 9.17

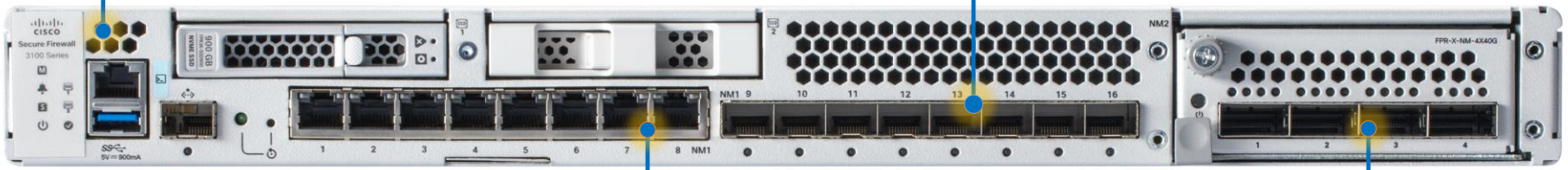
Appliance-Mode Security Platform for FTD or ASA Application

- Fixed configurations: 3105, 3110, 3120, 3130, 3140
- Lightweight virtual Supervisor module w/Multi-Instance and Clustering
- Integrated Datapath FPGA w/Flow Offload and Crypto Engine
- Rear dual redundant power supplies and fan trays

SFP Data Interfaces

- 8x1/10GE on Firepower 3105-3120
- 8x1/10/25GE on Firepower 3130-3140

1RU



Copper Data Interfaces

- 8x10/100/1000BaseT

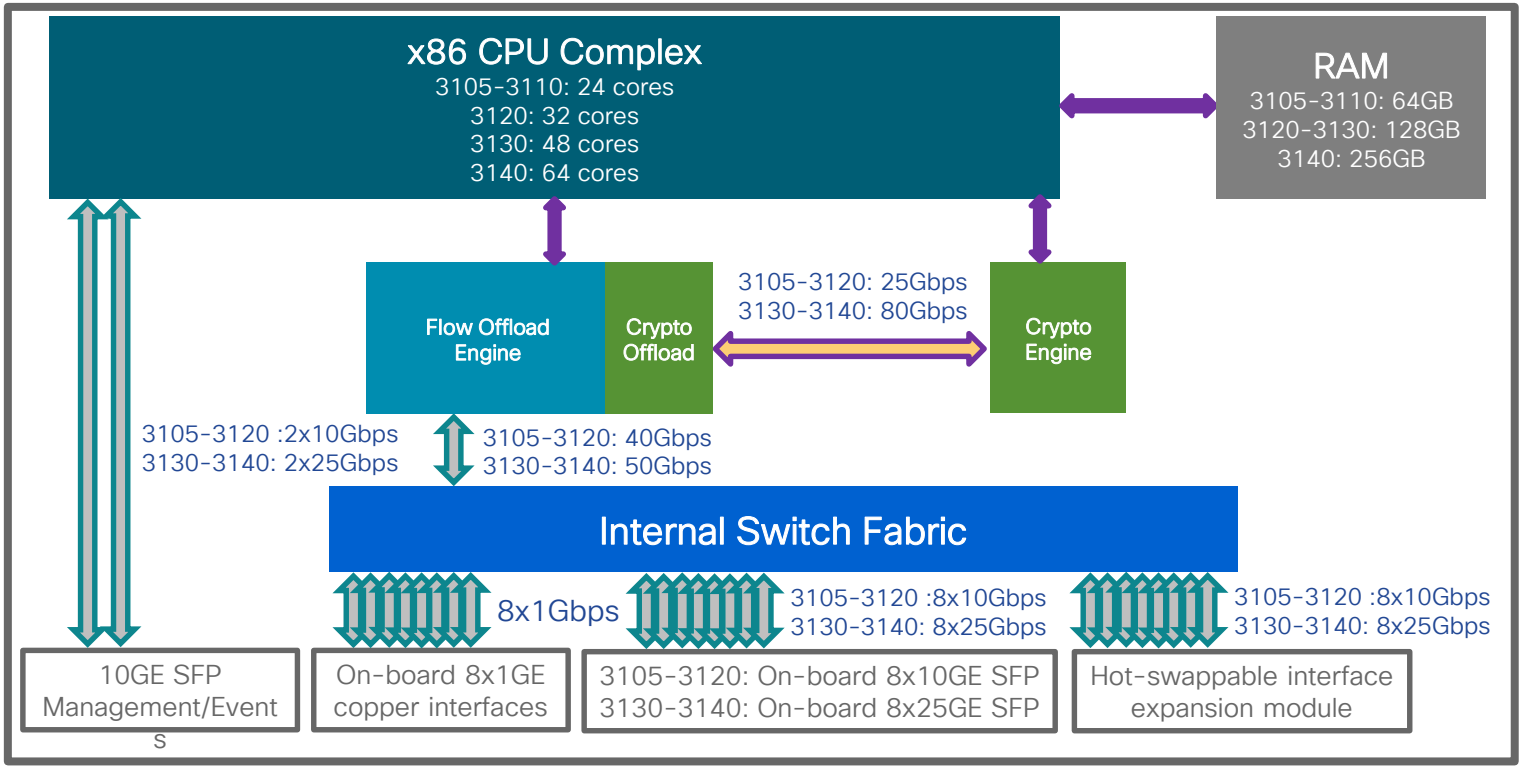
Network Module

- 8x1/10/25GE or 6x10/25GE FTW on Firepower 3105-3120
- 4x40GE, 2x40GE FTW and 2x100GE on Firepower 3130-3140
- 8x10/100/1000BaseT & 6x1GE, 6x10GE, 6x25GE SFP FTW

Secure Firewall 3100 Series Architecture

FTD 7.1

ASA 9.17



System Bus

Ethernet

Chip-to-Chip Link

Secure Firewall 1200C Series

FTD 7.6

ASA 9.22

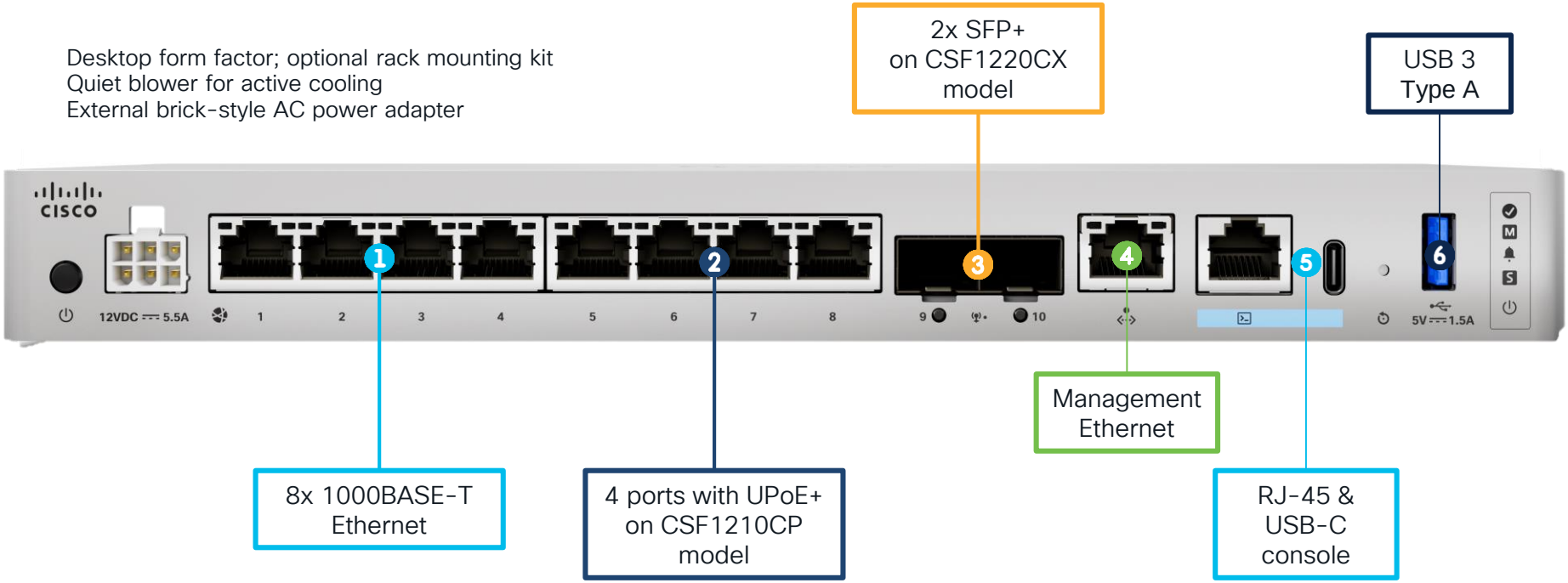
- 3 compact models – 1210CE, CP, 1220CX
  - 8 core SoC ARM design
  - 16GB of RAM
  - 240GB of NVMe storage
  - Fixed 8x1GE:
    - 1210CP – 4x1GE with UPoE+ support (120W total, max of 90W per port)
    - 1220CX – plus 2x 1/10G SFP+
- Multiple SoC-embedded accelerators
  - encryption/decryption
  - traffic processing
- Up to 2.6Gbps (450B) or up to 6Gbps (1024B) for NGFW traffic profiles (~10x over 1010, ~3x over 11xx)
- Up to 5Gbps for IPsec VPN, and up to 1.7Gbps for TLS 1.2/1.3

Secure Firewall 1200C Series Overview

FTD 7.6

ASA 9.22

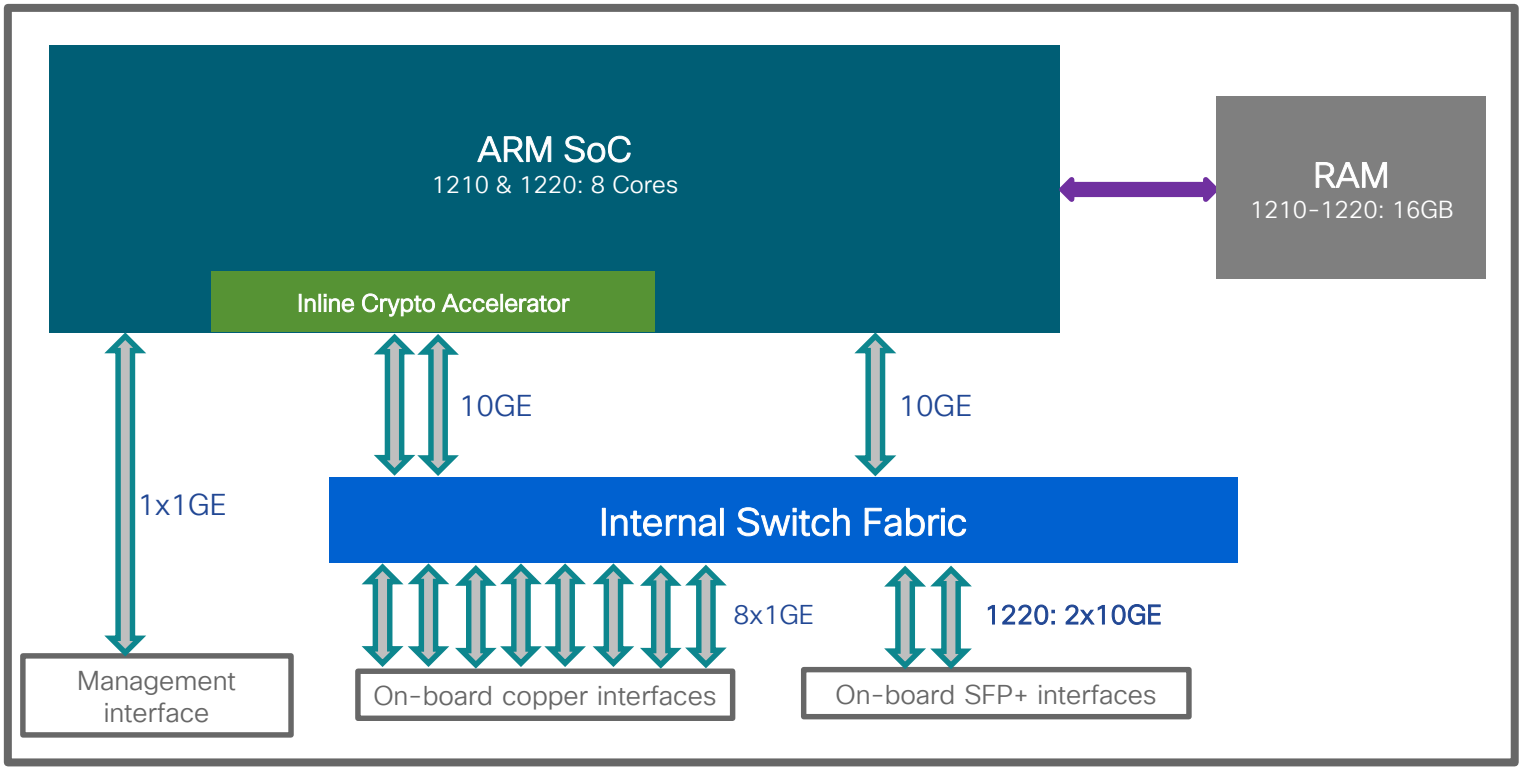
Desktop form factor; optional rack mounting kit
Quiet blower for active cooling
External brick-style AC power adapter



Secure Firewall 1200C Series Architecture

FTD 7.6

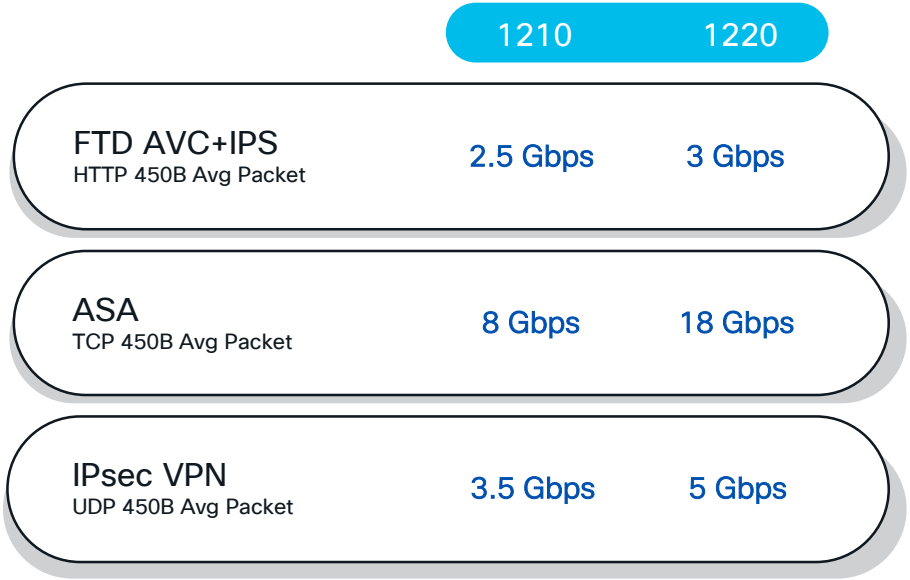
ASA 9.22



Secure Firewall 1200C Performance

FTD 7.6

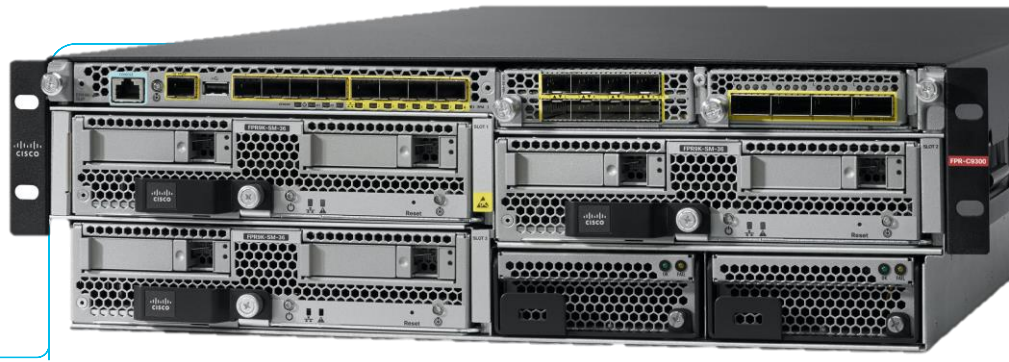
ASA 9.22



All performance estimates are subject to change in final release.

Secure Firewall 9300 Series

- 1 chassis, choice of three Service Modules
  - central Supervisor with switching fabric – 2x40GE towards each Service Module, 5x40GE towards Network Module bays
  - 8xSFP/SFP+ ports built-in plus one SFP management port
  - two Network Module bays – choice of 1/10/40/100GE interfaces & FTW
  - each Service Module can run either ASA or FTD – support for mixed mode operation
  - AC/DC redundant PS (3000W)
- Advanced NPU and VPN crypto hardware on each Service Module
- Clustering support on all models – up to 16x
- up to 64 Gbps for FW+AVC+IPS with 1024 bytes average packet size per Service Module
- up to 51 Gbps for IPsec with 1024 bytes average packet size with release 7.2 per Service Module



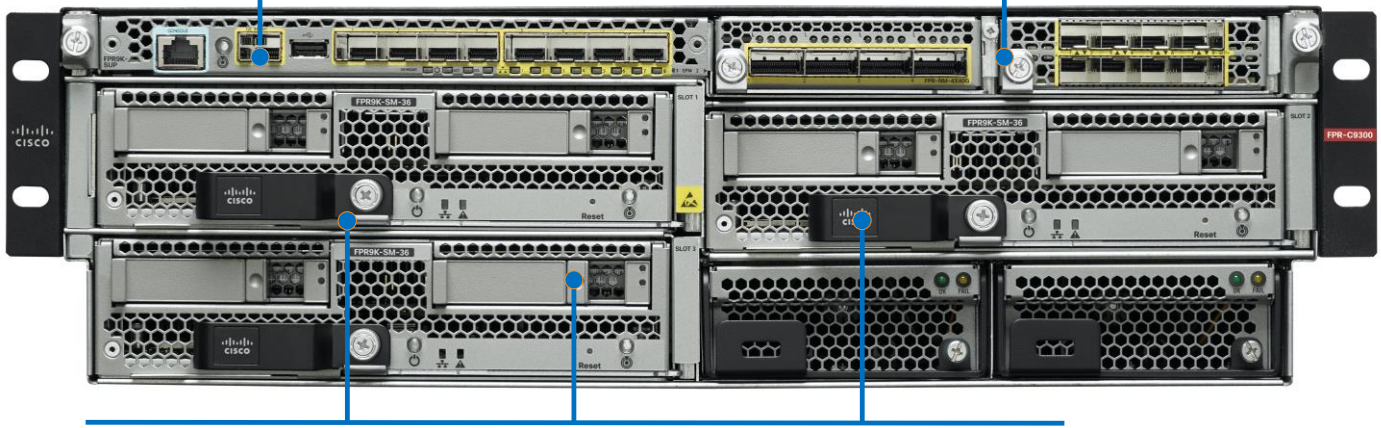
REFERENCE

Secure Firewall 9300 Series 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

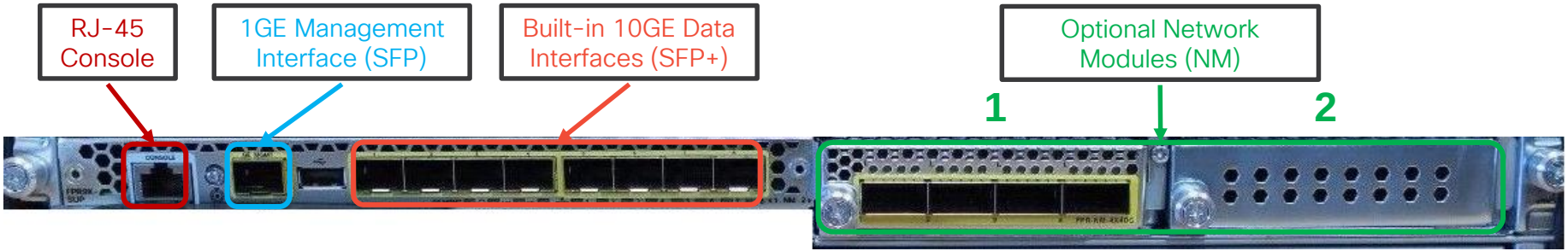
3RU



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

Secure Firewall 9300 Series

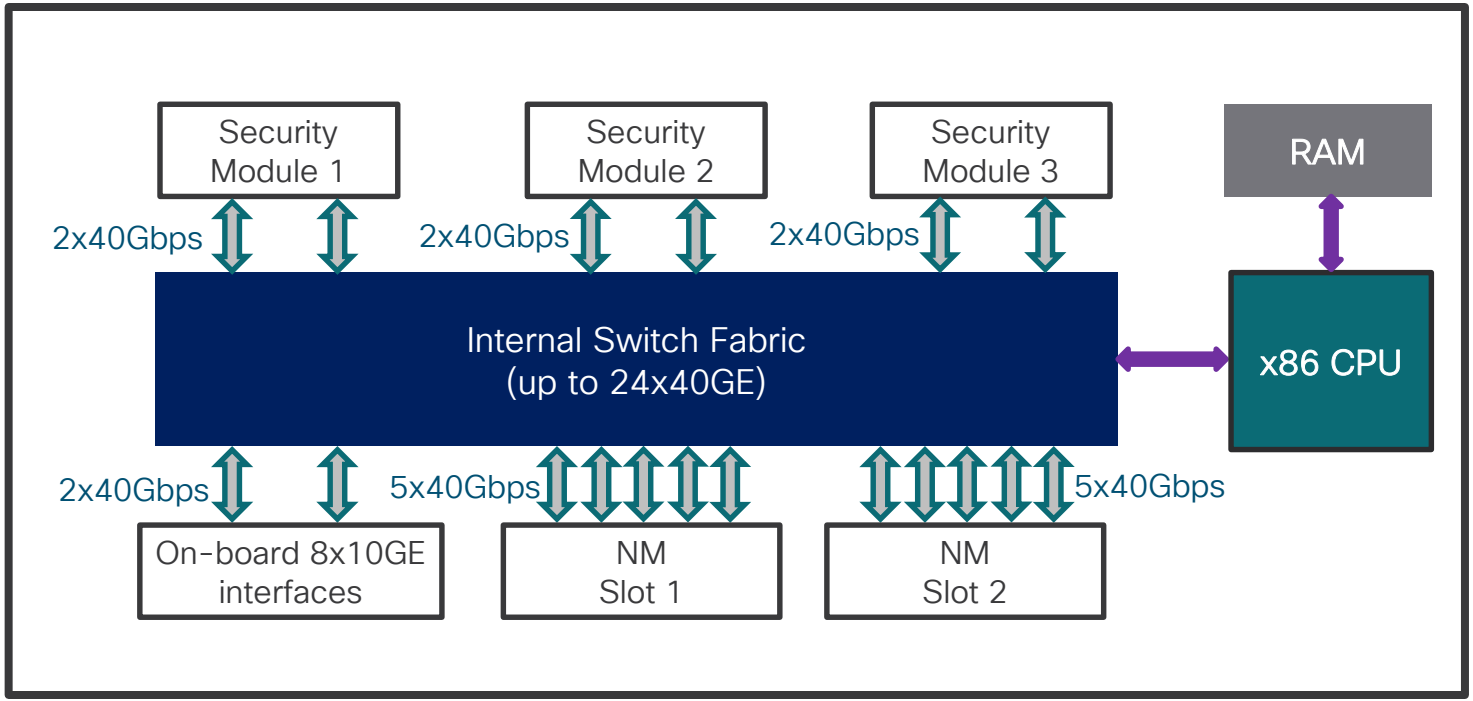
Supervisor Module



- 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

Secure Firewall 9300 Series

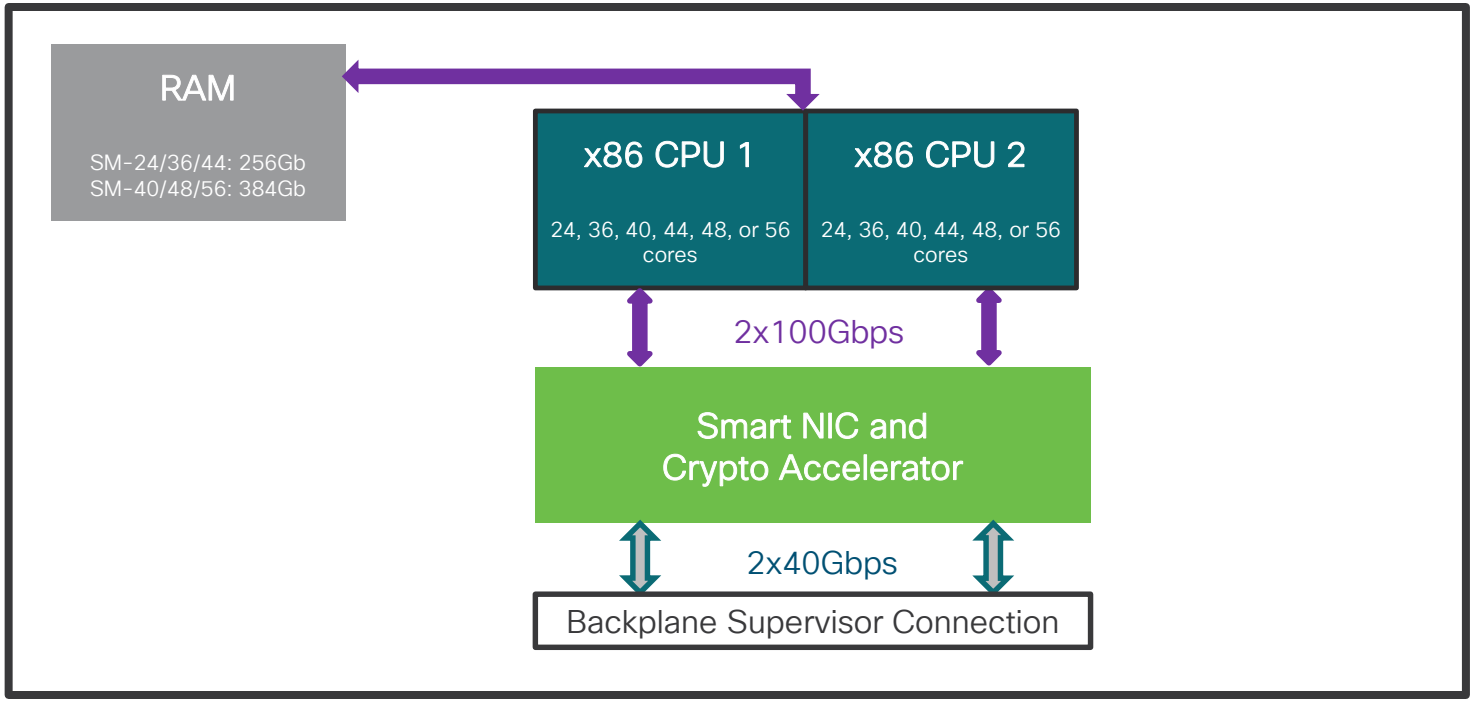
Supervisor Architecture



REFERENCE

Secure Firewall 9300 Series

Security Module Architecture



REFERENCE

REFERENCE

Secure Firewall 9300 Series

Security Modules

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

Secure Firewall 4100 Series

- 4 models, 4112/4115/4125/4145
  - 12-44 CPU physical cores
  - 8xSFP/SFP+ built-in
  - two Network Module bays
  - AC/DC redundant PS (1100W AC/950W DC)
- Advanced NPU and VPN crypto hardware
- Clustering support on all models, 16x
- 53 Gbps for FW+AVC+IPS with 1024 bytes average packet size
- 24 Gbps for IPsec with 1024 bytes average packet size with release 7.2

Secure Firewall 4100 Series Overview

REFERENCE

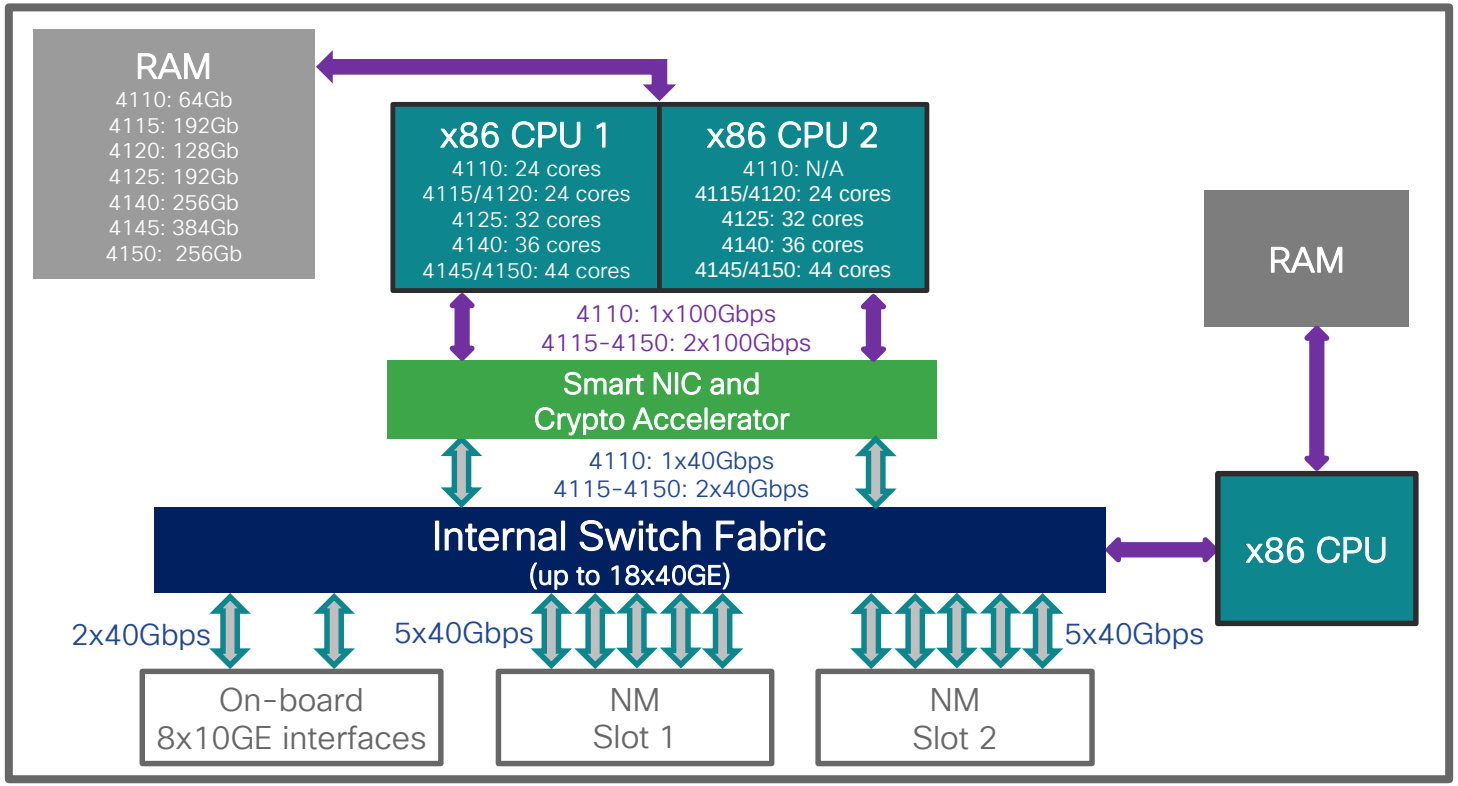
Built-in Supervisor and Security Module
- Same hardware and software architecture as 9300
- Fixed configurations (4110-4150)

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

Secure Firewall 4100 Series Architecture

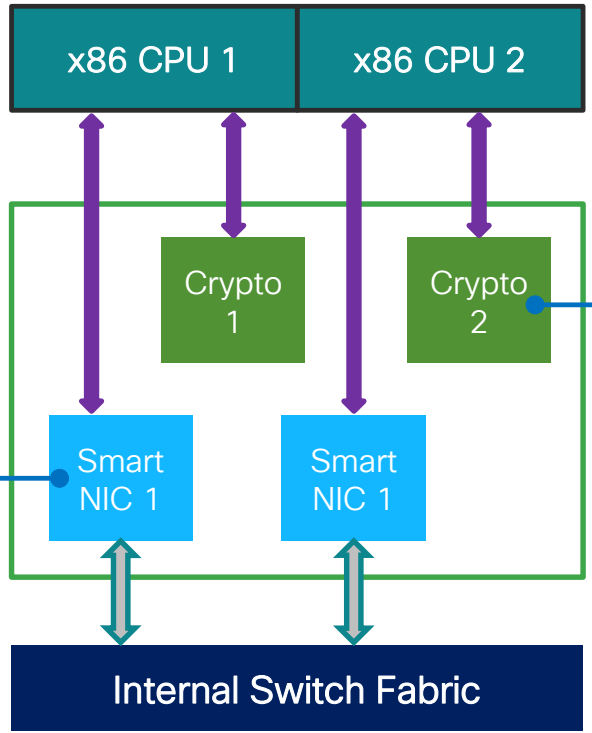


REFERENCE

Secure Firewall 4100/9300 Series

Smart NIC and Crypto

REFERENCE



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

Secure Firewall 2100 Series

- 4 models (2110, 2120, 2130, 2140)
  - 4-16 cores
  - 12x1G TX
  - 4x SFP (2110/20) or 4x SFP+ (2130/40)
  - 16-64GB of RAM
  - one 200GB SSD disk with one optional for redundancy
  - 250-400W AC (2110-2140)
    350W DC (2130-2140) power supply
- Advanced x86 processing with multi-core NPU
- 2.5Gbps to 10Gbps for FW+AVC+IPS with 1024 bytes average packet size
- 365Mbps to 1.4Gbps for TLS decryption performance
- 950Mbps to 3.5Gbps for IPsec with 1024 bytes average packet size

REFERENCE

Secure Firewall 2100 Series 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

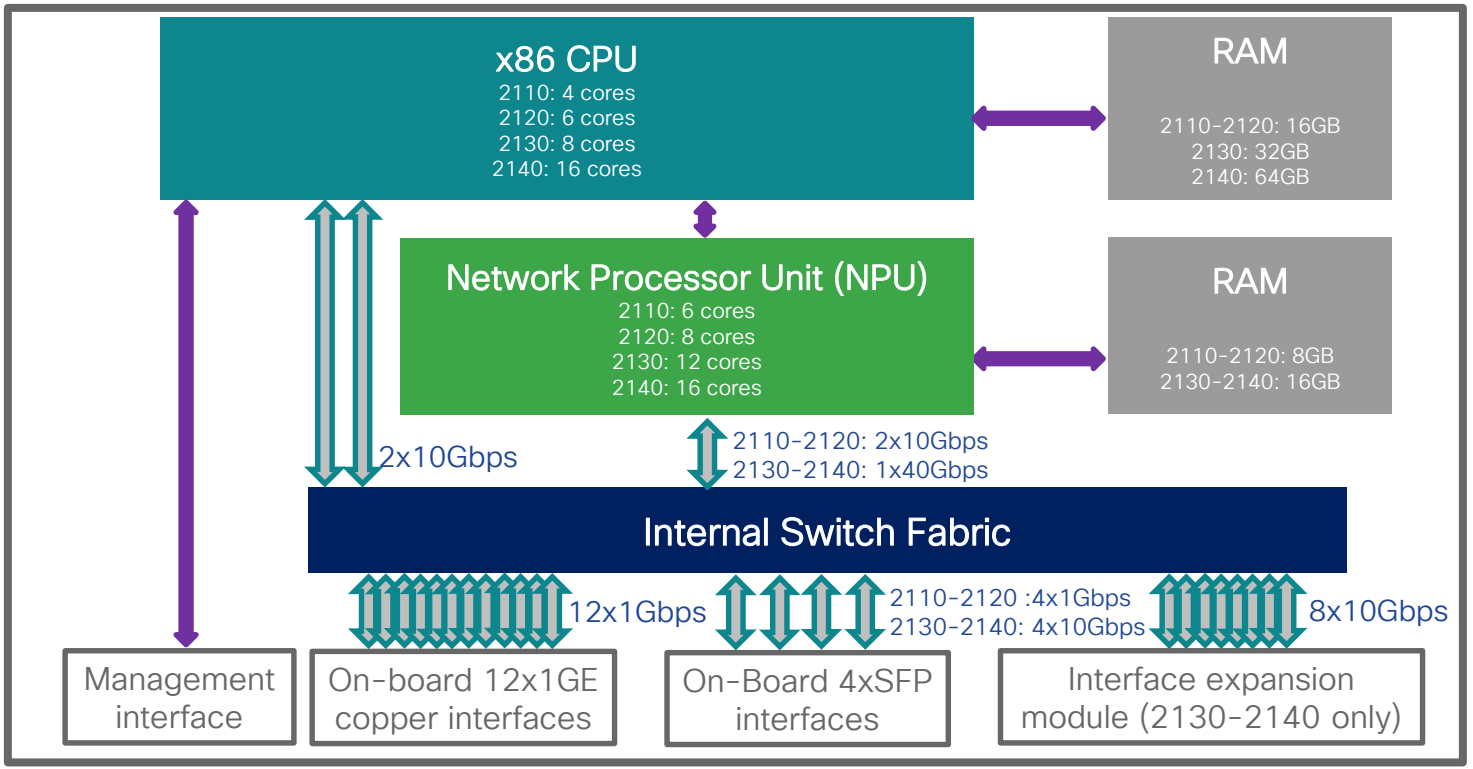
Copper Data Interfaces

- 12x1GE Ethernet

Network Module

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

Secure Firewall 2100 Series Architecture



REFERENCE

Secure Firewall 1010/1010E

- 1 model – 1010/1010E
  - 4 physical cores
  - 8x1G TX, 2 ports (7/8) with PoE IEEE 802.3at on 1010
  - 8GB of RAM
  - one 200GB SSD disk
  - AC 115W (1010) or 55W (1010E)
- Advanced x86 + QAT (IPsec & TLS) processing
- 0.85Gbps for FW+AVC+IPS with 1024 bytes average packet size
- 195Mbps for TLS decryption performance
- 400Mbps for IPsec with 1024 bytes average packet size

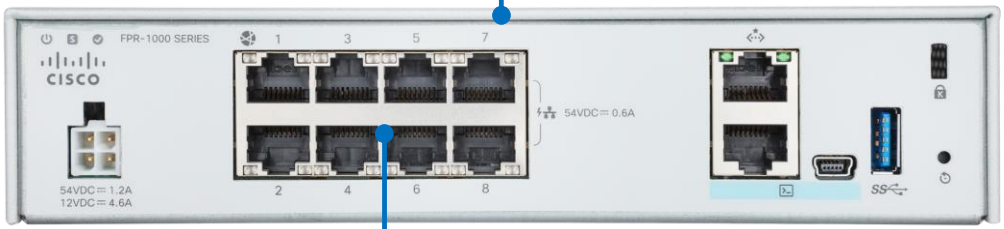
Secure Firewall 1100 Series

- 3 models – 1120, 1140 & 1150
  - 12-16 physical cores
  - 8x1G TX
  - 4x SFP (1120/1140) or 2x SFP + 2x SFP+ (1150)
  - 8-32GB of RAM
  - one 200GB SSD disk
  - AC 100W (1120/1140/1150) power supply
- Advanced x86 + QAT (IPsec & TLS) processing
- 2.3Gbps to 5Gbps for FW+AVC+IPS with 1024 bytes average packet size
- 850Mbps to 1.4Gbps for TLS decryption performance
- 1.2Gbps to 2.4Gbps for IPsec with 1024 bytes average packet size

REFERENCE

Secure Firewall 1010/E Overview

Desktop



Integrated Security Appliance with ASA or FTD

- Embedded x86 CPU with QuickAssist Crypto Acceleration
- Fixed non-modular configuration

Copper Data Interfaces

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

Secure Firewall 1100 Series Overview

REFERENCE

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

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

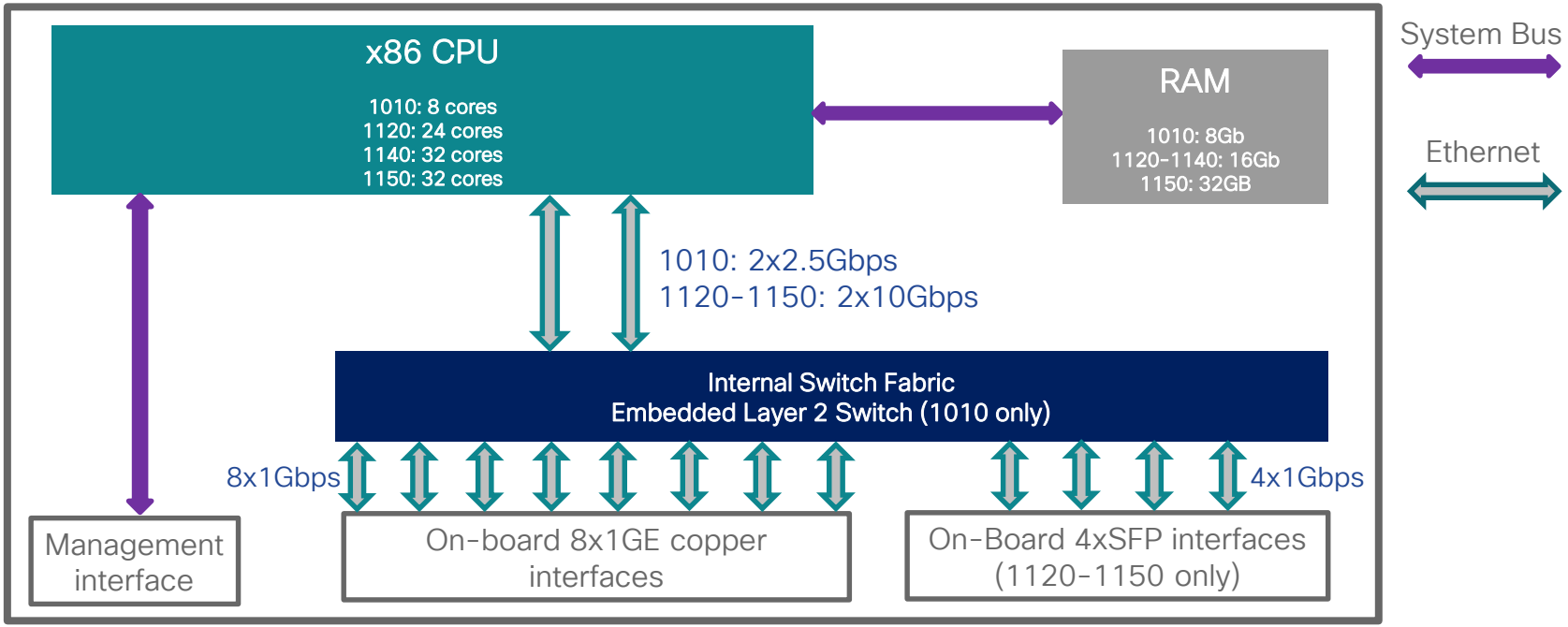
1RU

Copper Data Interfaces
- 8x1GE Ethernet

Field Replaceable SSD

Secure Firewall 1100 Series Architecture

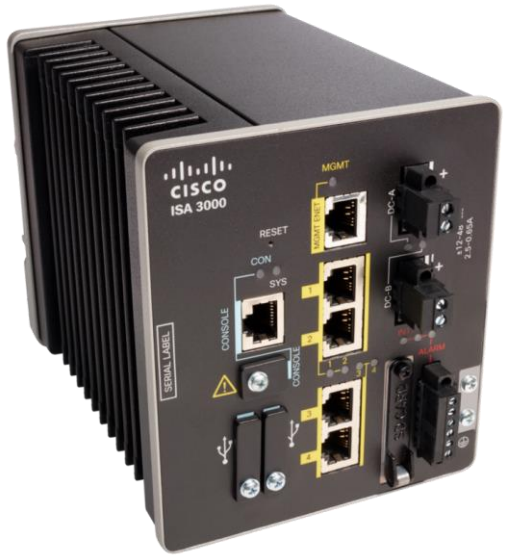
REFERENCE



REFERENCE

Secure Firewall ISA 3000 Series

- 2 models
  - Intel 4-core Atom CPU, I-Temp compliant
  - 4x 10/100/1000TX or 2x10/100/1000TX & 2xSFP; dedicated 10/100/1000 Management Port
  - 8GB of RAM, 16GB of flash memory + mSATA 64GB with 1GB removable SD flash card
  - Dual internal DC power supplies
- Built for harsh environments and temperature ranges (-40F to 158F; -40C to 70C)
- Hardened for vibration, shock, surge, and electrical noise immunity
- Broad OT protocol coverage (universal to all Snort 3 based sensors): BACnet, CIP, COSEM, COTP, DNP3, GOOSE, GSE, ECP, FDC, Honeywell CS/NIF Server & Esperion DSA Server monitor, IEC 60870-5-104, IEC 61850 MMS, Modbus, Omron FINS, OPC-UA, Q.931, Siemens S7, SRC, TPKT – plus all (3000+) OpenAppID applications
- Can run either ASA or FTD code



Secure Firewall FMC 1700/2700/3700

REFERENCE

- 3 models – 1700/2700/4700
  - 1x AMD CPU (8-24 cores)
  - 2x10G NIC for connectivity (Intel X710), 2x10/25G (Intel E810XXVDA2) additional ports in 4700
  - 32-128GB of RAM
  - 2.4TB-120TB of HDD space
  - 240GB SSD recovery disk
- 50 (1700), 300 (2700) and 1000 (4700) sensors supported
- 30, 60, 400M IPS events supported
- 5/12/30k FPS flow rate
- 50, 150, 600k network hosts

Secure Firewall Network Modules

2100/4100/9300 and 3100/4200 portfolio

3100 network modules		SW release
FPR3K-XNM-8X10G	8x 1/10G SFP+	7.1
FPR3K-XNM-8X25G	8 port 1/10/25G SFP+	7.1 (3130/40)
FPR3K-XNM-4X40G	4x 40G QSFP+ (breakout supported to 4x10G)	7.2 (3130/40)
FPR3K-XNM-8X1GF	8x 1GE TX FTW	7.3
FPR3K-XNM-6X1SXF	6x 1GE SX FTW	7.2.3/7.3.1
FPR3K-XNM-6X10SRF/LRF	6x10G FTW	7.2.3/7.3.1
FPR3K-XNM-6X25SRF/LRF	6x25G FTW	7.2.3/7.3.1
FPR-X-NM-2X100G	2x100G QSFP/QSFP28 (40/100G + breakout to 4x10G or 4x25G supported)	7.4.1

4200 network modules		SW release
FPR4K-XNM-8X1GF	8x 1G FTW	7.4.0
FPR4K-XNM-6X10SRF/LRF	6x10G FTW (SR or LR)	
FPR4K-XNM-6X25SRF/LRF	6x 25G FTW (SR or LR)	
FPR4K-XNM-8X10G	8x 1/10G SFP/SFP+	
FPR4K-XNM-8X25G	8x 1/10/25G SFP/SFP+	
FPR4K-XNM-4X40G	4x 40G QSFP+	
FPR4K-XNM-2X100G	2x100G QSFP/QSFP28 (supports 10/25/XXXX?)	
FPR4K-XNM-4X200G	4x200G QSFP+ (supports 40/100G)	
FPR4K-XNM-2X400G	2x400G (supports 200G)	7.6

All FTW modules have built–in optics, and it's fixed.
Same-kind OIR is supported.

Secure Firewall Network Modules

2100/4100/9300 and 3100/4200 portfolio

2100 network modules	
FPR2K-NM-8X10G	8 port SFP+
FPR2K-NM-8X1G	8 port SFP
FPR2K-NM-6X1SX-F	6 port 1G SX Fiber FTW
FPR2K-NM-6X10SR-F	6 port 10G SR FTW
FPR2K-NM-6X10LR-F	6 port 10G LR FTW
FPR2K-NM-8X1G-F	8 port 1G Copper FTW

4100 network modules		SW release
FPR4K-NM-8X1G-F	8x1GE FTW	
FPR4K-NM-6X1SX-F	6x 1GE SX FTW	
FPR4K-NM-6X10SR/LR-F	6x 10G FTW (SR or LR)	
FPR4K-NM-8X10G	8x 1/10G SFP+	
FPR4K-NM-2X40G-F	2x 40G FTW	
FPR4K-NM-4X40G	4x 40G QSFP+	
FPR4K-NM-2X100G	2x 100G QSFP/QSFP28	7.3.1 (4112/15/ 4125/45)

All FTW modules have built–in optics, and it's fixed.
Same-kind OIR is supported.

Secure Firewall Network Modules

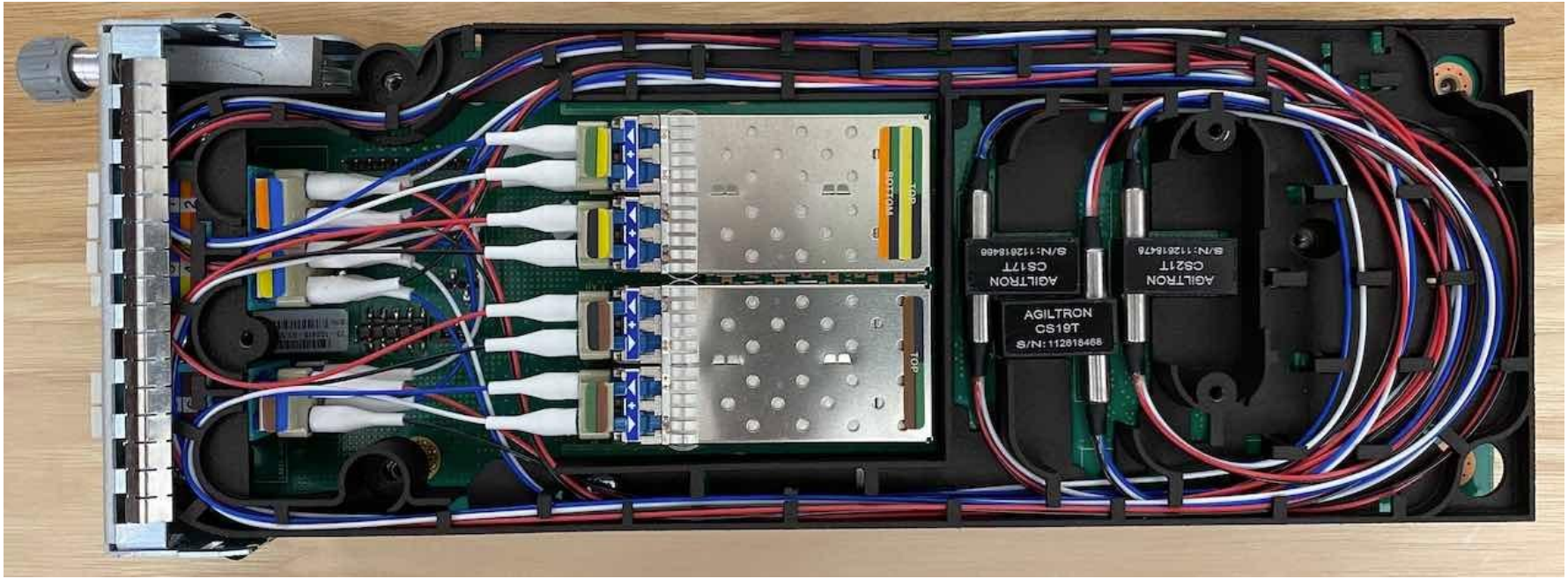
2100/4100/9300 and 3100/4200 portfolio

9300 network modules		SW release
FPR9K-NM-8X10G	8x 10G SFP+	every release
FPR9K-NM-6X10SR-F/LR-F	6x 10G FTW Does not support hot-swapping.	FXOS 2.0.1
FPR9K-NM-4X40G	4x 40G QSFP+	every release
FPR9K-NM-2X40G-F	2x 40G FTW Does not support hot-swapping.	FXOS 2.0.1
FPR9K-DNM-2X100G	2x 100G QSFP28 (doube-wide) Does not support hot-swapping.	FXOS 1.1.4
FPR9K-NM-2X100G	2x 100G QSFP28	FXOS 2.4.1
FPR9K-NM-4X100G	4x 100G QSFP28	FXOS 2.4.1

All FTW modules have built–in optics, and it's fixed.
Same-kind OIR is supported.

Secure Firewall Network Modules

Fail-to-Wire network module internals



Last Day of Support (LDoS)

Please plan migration to 1200, 3100 or 4200 series

2020

Oct 31, 2020
- FP8250
- FP8260
- FP8270
- FP8290

2022

Aug 31, 2022
- ASA 5512
- ASA 5515
- ASA 5505

Dec 31, 2022
- FP7010
- FP7020
- FP7030
- FP8020
- FP8030
- FP8040

2023

May 31, 2023
- ASA 5585

Sep 30, 2023
- ASA 5506W

2024

Jun 30, 2024
- FP7050
- FP7110
- FP7115
- FP7120
- FP7125
- FP8350
- FP8360
- FP8370
- FP8390

We're here!

2025

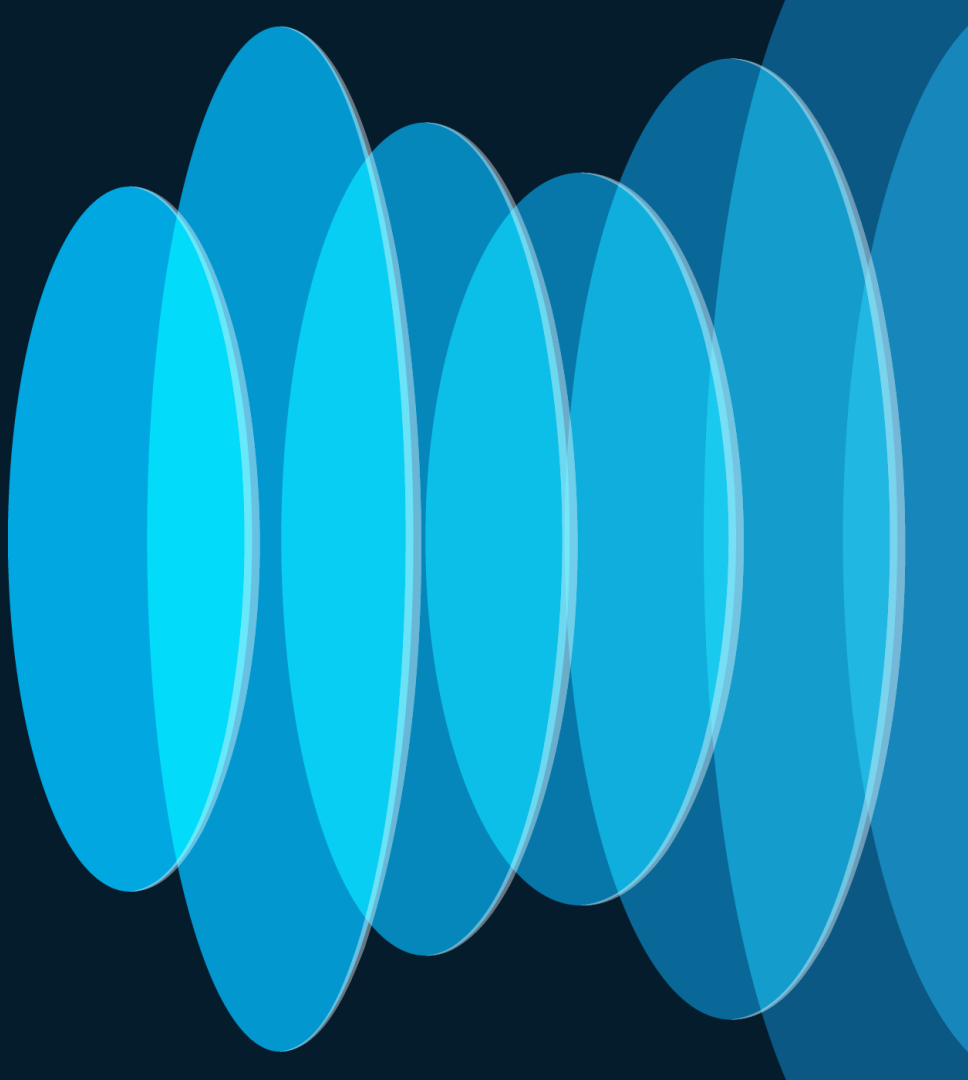
August 31, 2025
- 4120
- 4140
- 4150
- 9300 SM-24
- 9300 SM-36
- 9300 SM-44

Sep 30, 2025
- ASA 5525
- ASA 5545
- ASA 5555

2026

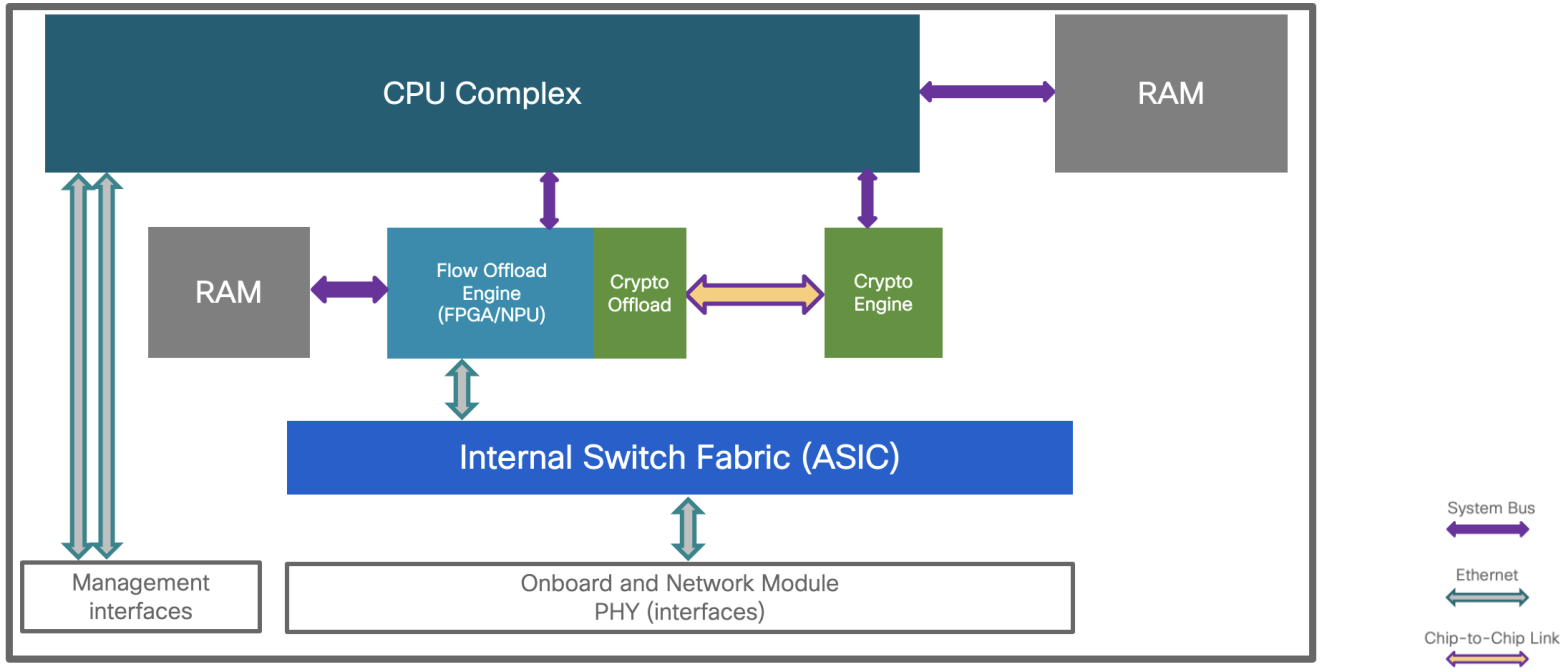
Aug 31, 2026
- ASA 5506
- ASA 5508
- ASA 5516

Performance Updates



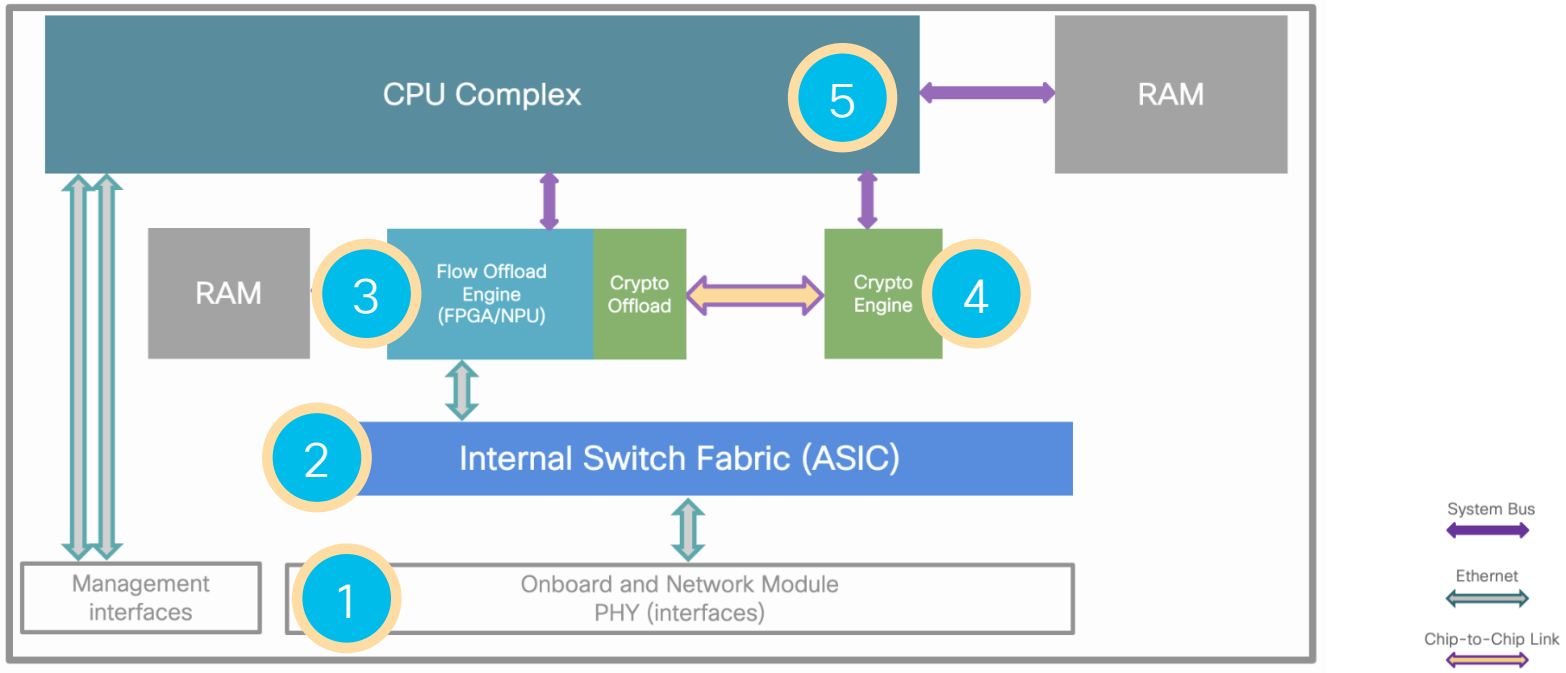
Generalized architecture view

Cisco Firepower Threat Defense Architecture



Generalized architecture view

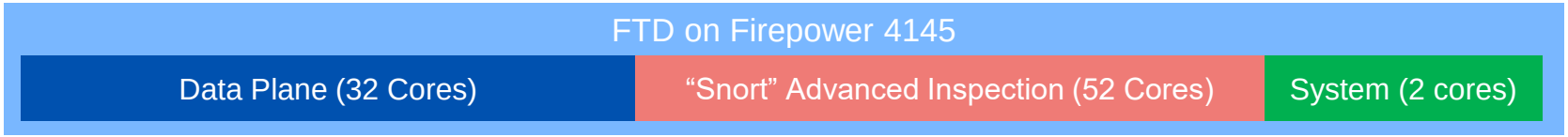
Critical flow components



Configurable CPU Core Allocation

FTD 7.3+

- FTD had a static CPU core allocation between Data Plane and Snort

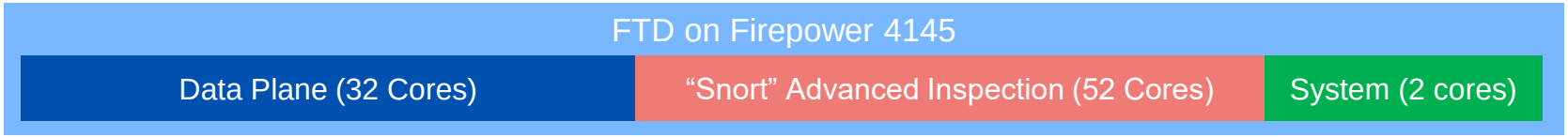


- Tailor FTD to a specific use case with a configurable allocation
  - Select from a few templates in FTD 7.3; dynamic in the future
  - VPN headend or basic stateful firewall would use more Data Plane cores
  - Heavy IPS and file inspection would bias toward more “Snort” cores
- 7.4.1 brings support for 3100 & 4200
  - support already on FTDv, 4100, 9300

Configurable CPU Core Allocation

FTD 7.3+

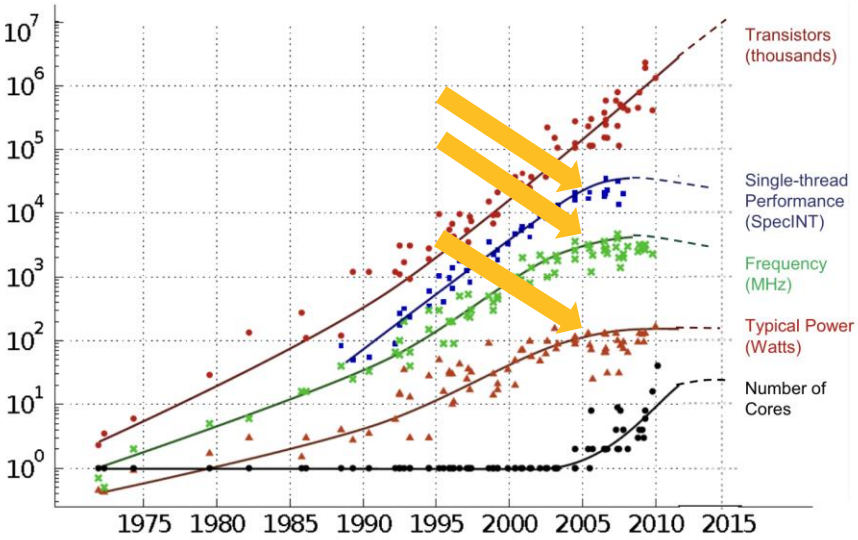
- FTD had a static CPU core allocation between Data Plane and Snort



Name	Core allocation
Default	Normal for balanced FTD system
VPN heavy with prefilter	90% cores for data plane, 10% for Snort
VPN heavy	60% cores for data plane, 40% for Snort
IPS heavy	30% cores for data plane, 70% for Snort

Single-Flow Performance Considerations

- A single stateful flow must be processed by one processor 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.osti.gov/-/media/ascr/ascac/pdf/reports/2013/SC12_Harrod.pdf
https://www.lanl.gov/conferences/salishan/salishan2011/3moore.pdf

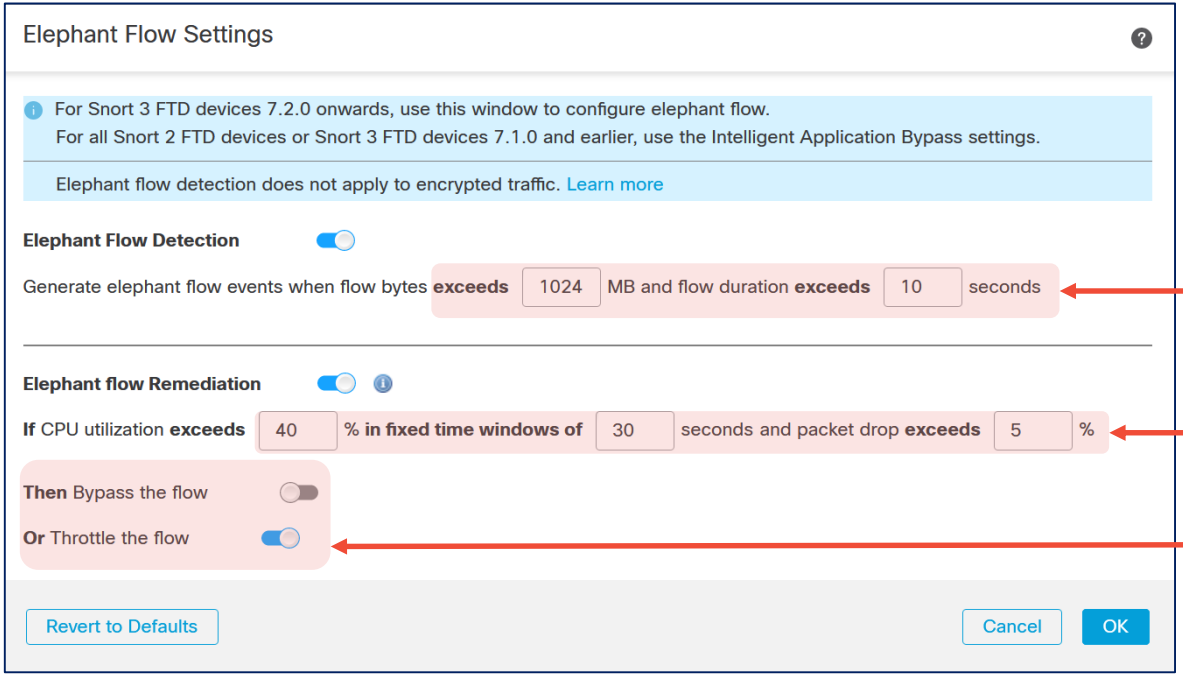
Managing Single-Flow Throughput

- Roughly estimated as overall throughput divided by Snort cores
  - 145Gbps of 1024-byte AVC+IPS on 4245 / 65 Snort cores = ~2.3Gbps
  - 65Gbps of 1024-byte AVC+IPS on 4215 / 15 Snort cores = ~4.43Gbps
  - Egress Optimization improves throughput by up to 20% in FTD 6.4 NGIPS mode, and in some VPN scenarios with 7.0
  - Reducing impact on all flows from few Superflows is more important
- "What does your security policy tell you to do?"
  - NGFW performance capacity must not dictate your security policy
  - Flow Offload vs Snort 3 Elephant Flow Offload (7.2+) or Intelligent Application Bypass (IAB) (pre 7.2)

FTD 7.2

Elephant Flow Detection

Per-flow tracking replaces Intelligent Application Bypass (IAB)



Throughput threshold to qualify as an Elephant Flow

Optional flow-specific CPU resource consumption and packet drop thresholds for remediation.

Optional flow remediation actions.

DTLS cryptographic acceleration

3100 & 4200 superpower capability

FTD 7.6

ASA 9.22

- DTLS is still popular for RAVPN use cases
- Supports DTLS 1.2 acceleration on:
  - 3105, 3110, 3120, 3130, 3140
  - 4215, 4225, 4245
- Feature mix:
  - HA is supported for both ASA & FTD
  - Not supported yet on:
    - Multi-context (ASA)
    - Multi-instance (FTD)
    - clustered configurations

DTLS cryptographic acceleration

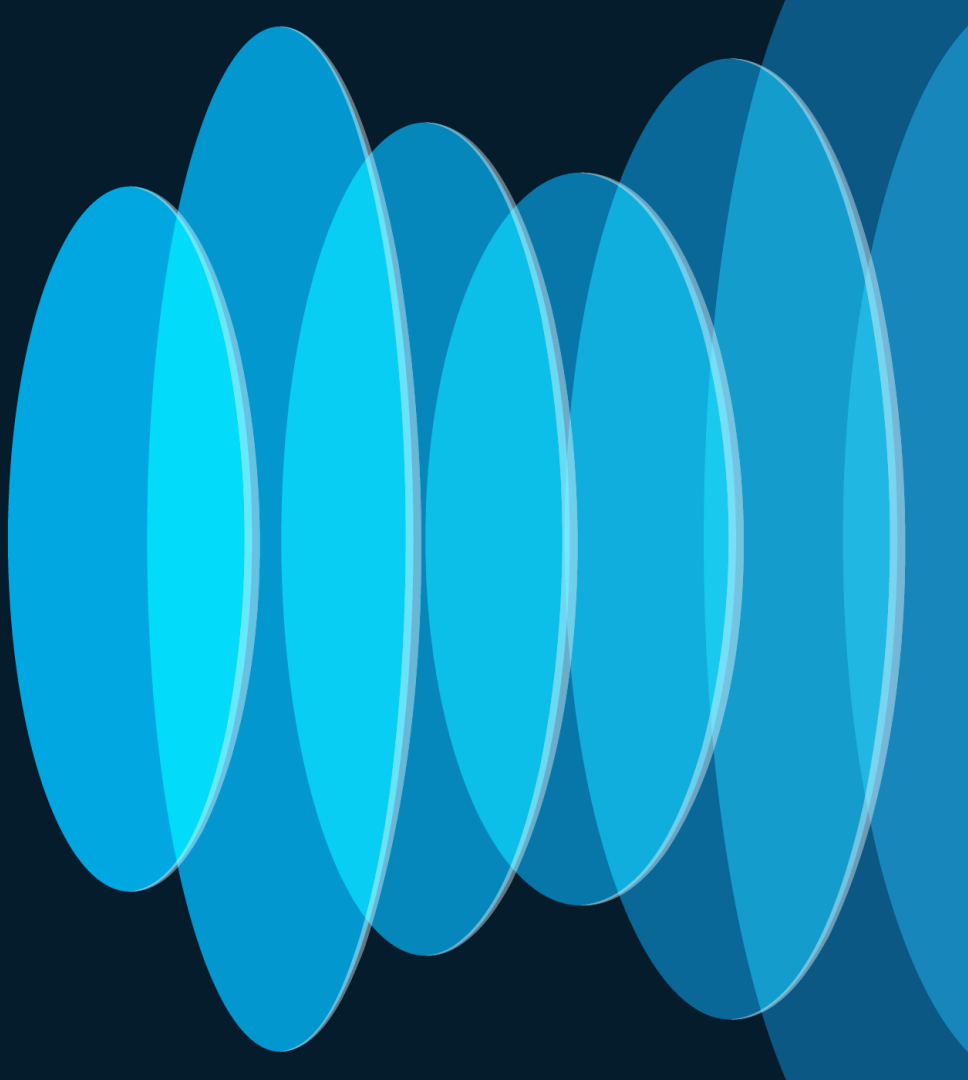
3100 & 4200 superpower capability

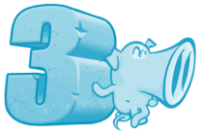
FTD 7.6

ASA 9.22

	3110	3140	4215	4245
DTLS 1.2 **CPU** 450B TCP Avg Packet	2.5 Gbps	8 Gbps	10 Gbps	25 Gbps
DTLS 1.2 **FPGA** 450B TCP Avg Packet	4 Gbps	12 Gbps	15 Gbps	35 Gbps
Improvement	60%	50%	50%	40%

Threat Updates





Snort 3 IPS Engine

FTD 7.0+

- Thwart modern threats with the trusted NGIPS engine update
  - Much higher efficacy and performance with a multi-threaded architecture
  - Native support for modern protocols -- HTTP/2, HTTP/3 and QUIC
  - Improved human-readable signature language
  - Tunable inspection level within a single policy with Rule Groups
- Multiple must-have new capabilities require Snort 3
  - Encrypted Visibility Engine (EVE) for ML-enabled security
  - Comprehensive Portscan attack detection and prevention
  - Native TLS 1.3 Decryption
  - Elephant Flow detection and impact mitigation

Snort 3 Machine Learning engine

FTD 7.6

From signatures to models

- New capability brings Machine Learning to Snort 3 system
- LSP updates will carry models to defend against unknown attacks of given type
  - 7.6 will initially support SQL injection attacks
- Example new type of rule:

alert (gid:411; sid:1; rev:1; msg:"(kaizen) potential threat found in http parameters via Neural Network Based Exploit Detection"; metadata: policy max-detect-ips alert, rule-type preproc; classtype:unknown;)

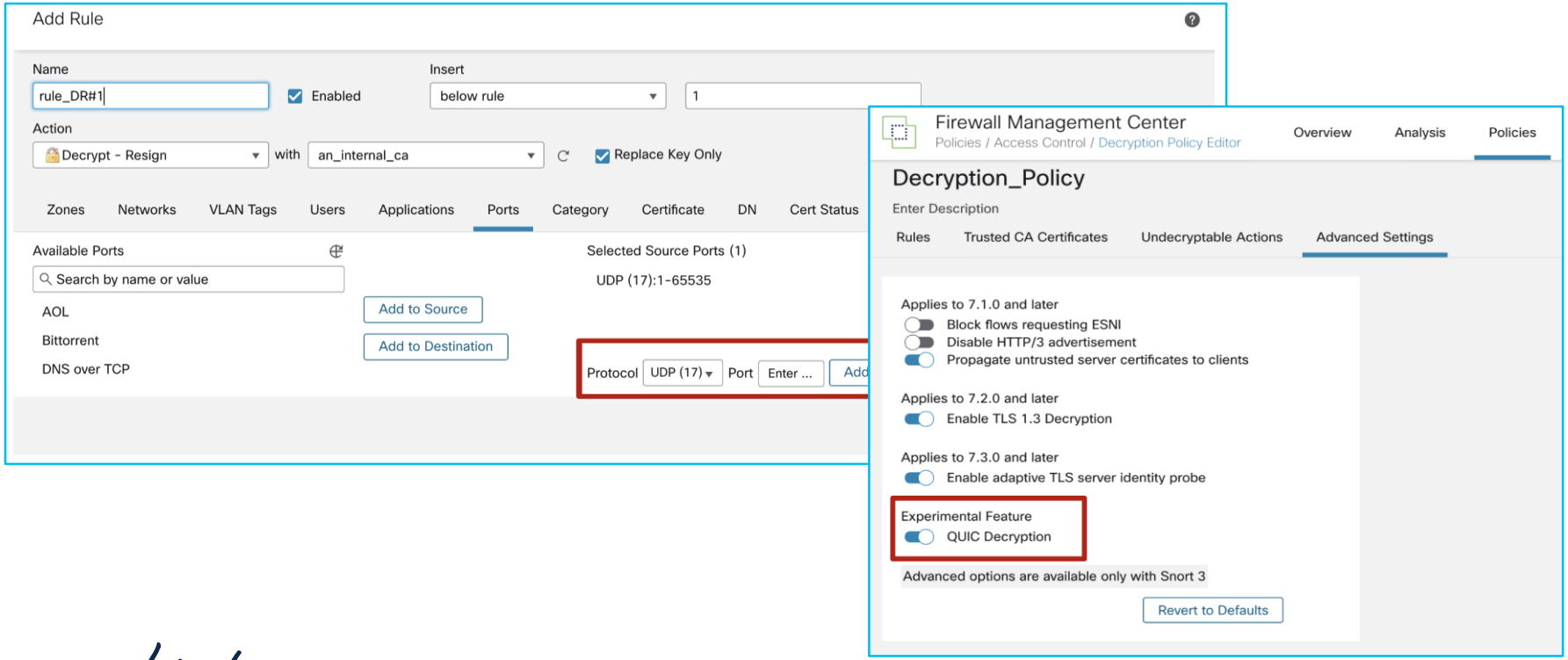
- Hand-testing prototype:

```
$ snort \
 -q --talos --plugin-path . \
 --lua 'kaizen = { model = "model.tflite" };' \
 -r 2023-26876-none-none-XXXX-1.pcap

URI: "/admin.php?page=history&filter_image_id=1&filter_user_id=12 UNION ALL SELECT
CONCAT(0x41414141,username,0x3a,password,0x41414141) from piwigo_users where id=1-- --"
LSTM output: 0.988226

##### 2023-26876-none-none-XXXX-1.pcap #####
        [200:1:0] (SnortML) exploit payload detected (alerts: 1)
```

Snort 3 QUIC support

Support of HTTP/3 inspection over QUIC

FTD 7.6

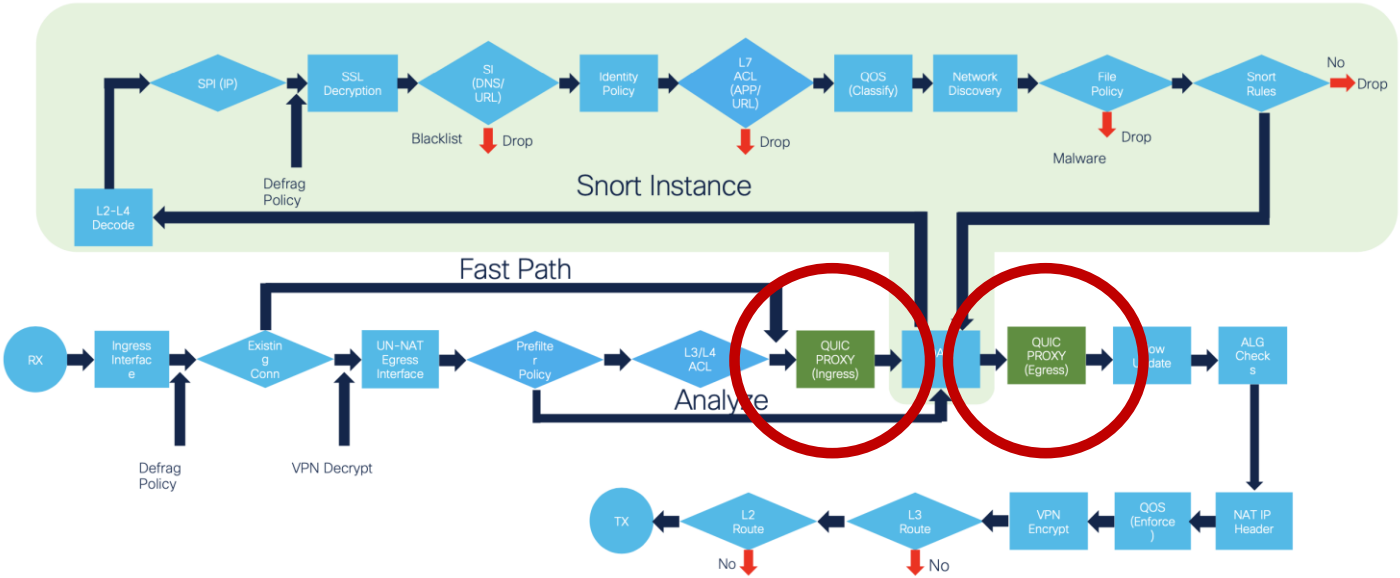


Snort 3 QUIC support

FTD 7.6

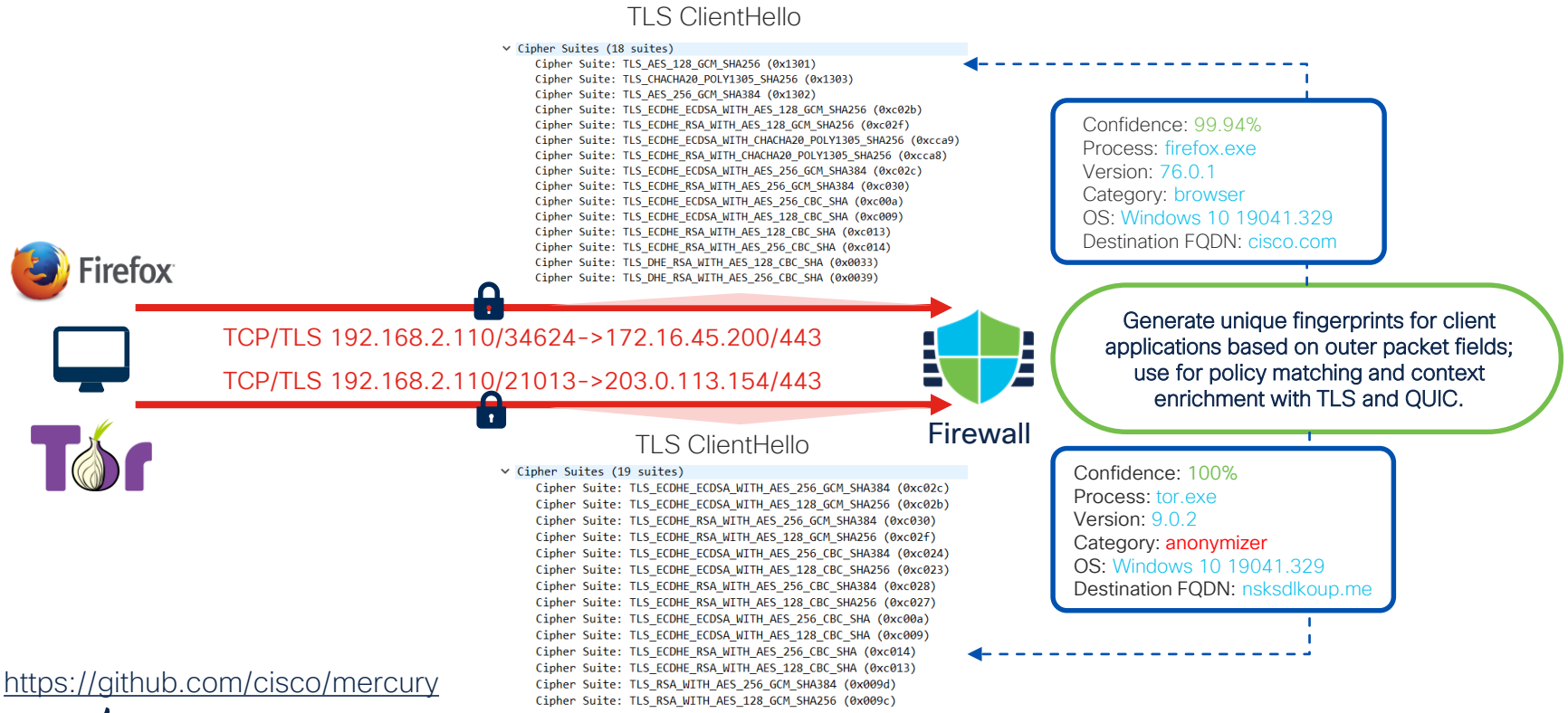
Support of HTTP/3 inspection over QUIC

- Over 7% of sites support it today, will grow over time as major content providers are investing in developing it



Encrypted Visibility Engine (EVE)

FTD 7.1



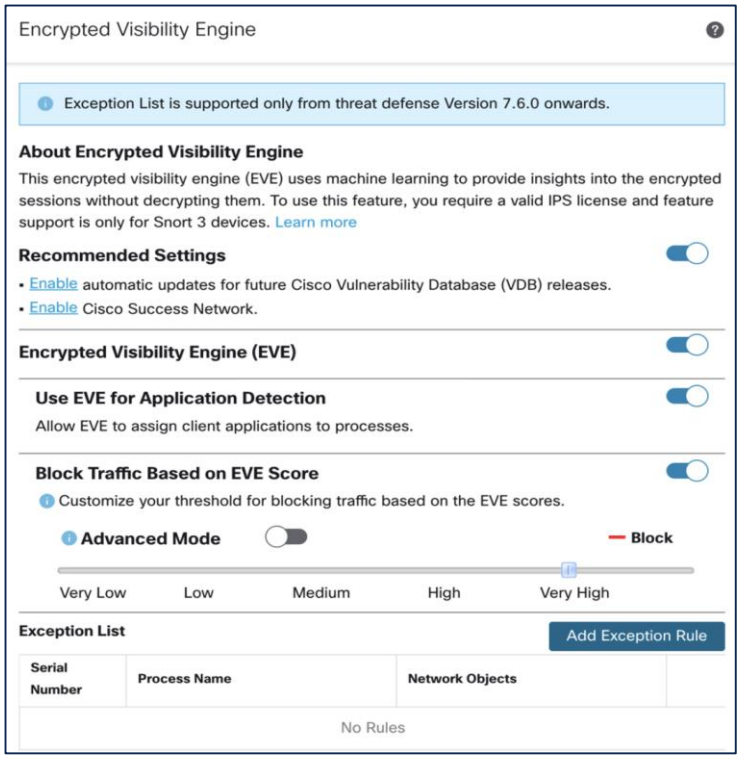
https://github.com/cisco/mercury

EVE block exceptions

FTD 7.6

When EVE is used to block traffic, you can define exceptions

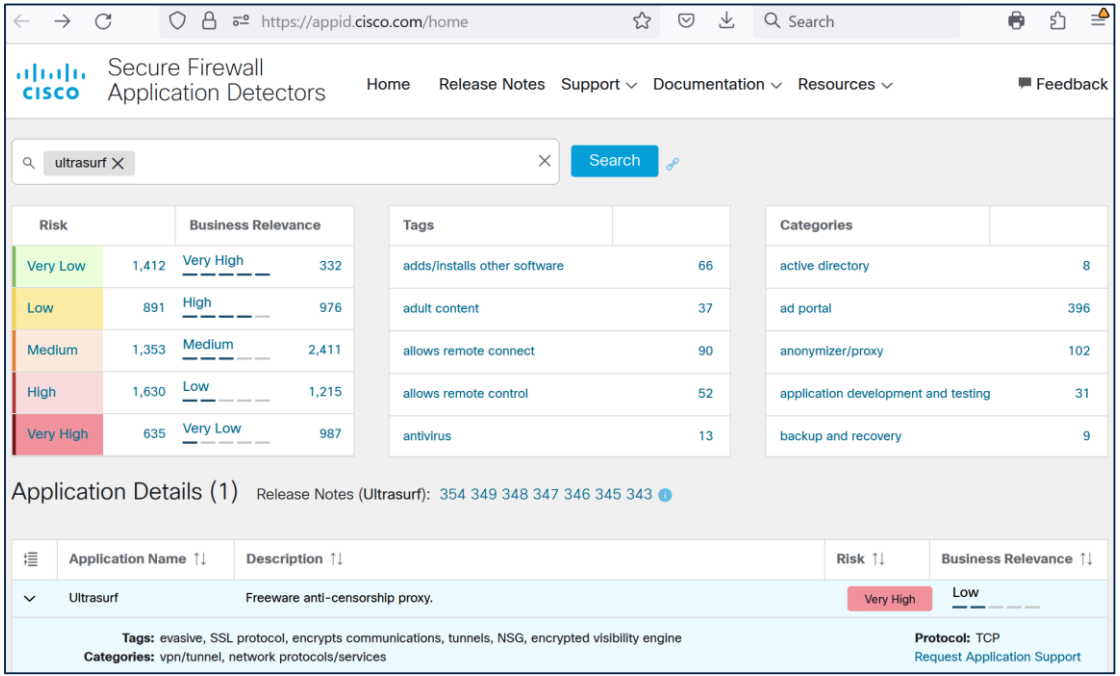
- Currently supported:
  - destination network based exception
  - process name based exception



AppID Portal: https://appid.cisco.com

Mirrors full AppID information that is available in FMC

Now



Cisco Vulnerability Database (VDB) Release Notes 365

365

(Type a VDB release between 343 - 365)

Encrypted Visibilty Engine Reference Details:

```
/*
  disclaimer: EVE resource files are automatically generated with
     real-world data. Older, less-relevant data is aged out, which
     leads to natural churn and can result in some month-to-month
     variations in the data.
*/

resources version: 2023.05.18

stats:
  general:
    total fingerprints:         39,860
    total labeled fingerprints: 6,930
    total connections:          2,680,300,185
    fingerprints per protocol:
      http: 3,677
       tls: 3,130
      quic: 123

  Threat Grid:
    total fingerprints: 801
    total connections:  3,041,256
```

Full AppID database update information, including EVE fingerprint data.

”What’s maximum size of policy I can use?”

ACE = Access Control Entry, ACP = Access Control Policy

- Starting from 7.2, FTD by default uses OGS on greenfield deployments
  - OGS = Optimized Group Search
  - OGS allows for higher scale for policies and connections per second, at the expense of per-packet performance
- With 7.6, OGS implementation was upgraded, to handle more corner cases, execute with higher scale and provide hit counters (and timestamps) also on folded entries
- While FMC will warn you before deploying rulesets close to those limits, please use following slide as guidance only and consult your Partner or Cisco Security Specialist before deploying policies

REFERENCE

Maximum supported policy sizes for FTD

As of release 7.4

Appliance model	Maximum tested FTD ACEs	UI Rule Count (assuming 1 rule expands to 50 ACEs)	UI Rule Count (assuming 1 rule expands to 100 ACEs)
1010/1010E	10,000	200	100
1120	90,000	1,800	900
1140	110,000	2,200	1,100
1150	185,000	3,700	1,850
1200C	50,000	1,000	500
2110	60,000	200	100
2120	100,000	1,800	900
2130	250,000	2,200	1,100
2140	500,000	3,700	1,850

REFERENCE

Maximum supported policy sizes for FTD

As of release 7.6

Appliance model	Maximum tested FTD ACEs	UI Rule Count (assuming 1 rule expands to 50 ACEs)	UI Rule Count (assuming 1 rule expands to 100 ACEs)
3105	2,750,000	55,000	27,500
3110	2,750,000	55,000	27,500
3120	3,000,000	60,000	30,000
3130	3,500,000	70,000	35,000
3140	4,000,000	80,000	40,000
4112	2,000,000	40,000	20,000
4115	4,000,000	80,000	40,000
4125	5,000,000	100,000	50,000
4145	8,000,000	160,000	80,000

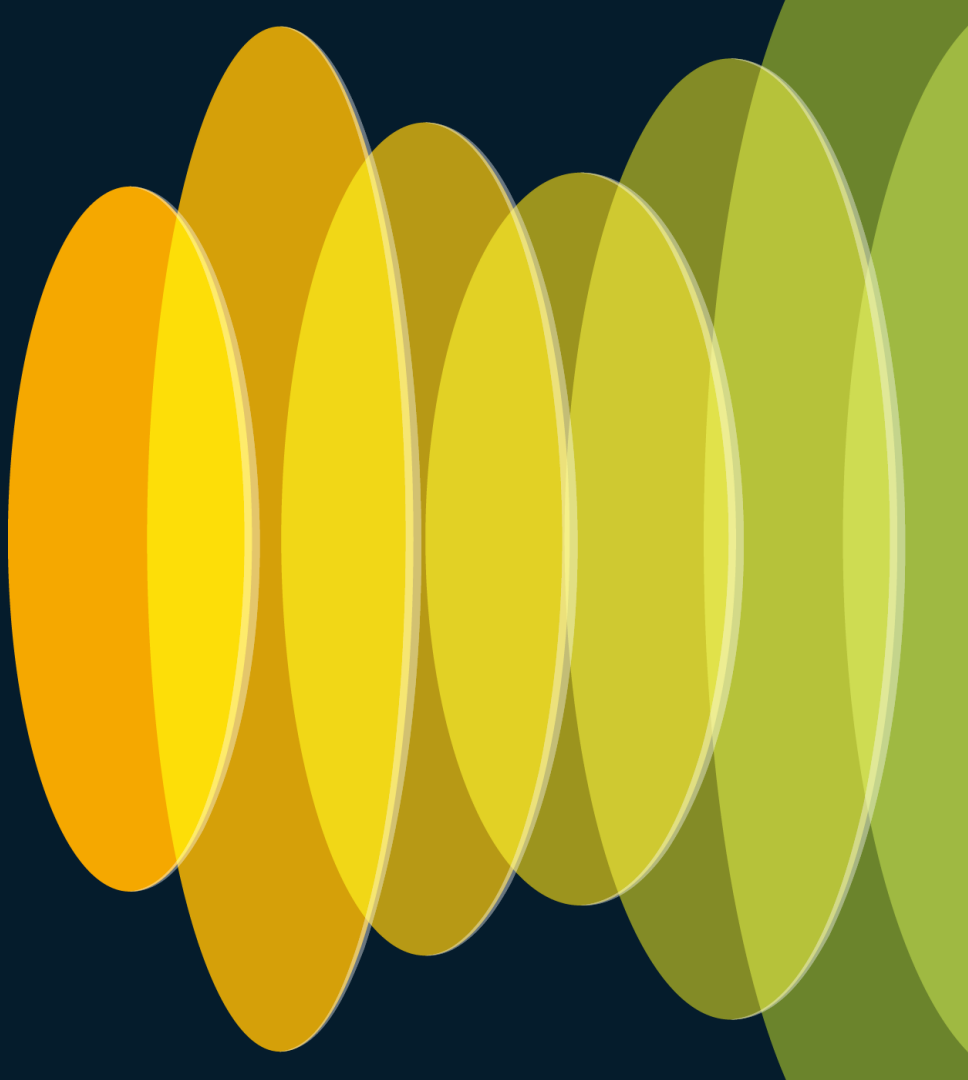
REFERENCE

Maximum supported policy sizes for FTD

As of release 7.6

Appliance model	Maximum tested FTD ACEs	UI Rule Count (assuming 1 rule expands to 50 ACEs)	UI Rule Count (assuming 1 rule expands to 100 ACEs)
4215	6,000,000	120,000	60,000
4225	8,000,000	160,000	80,000
4245	10,000,000	200,000	100,000
9300 w/SM-40	6,000,000	120,000	60,000
9300 w/SM-48	8,500,000	170,000	85,000
9300 w/SM-56	9,500,000	190,000	95,000

Designing for High Availability



cisco Live!

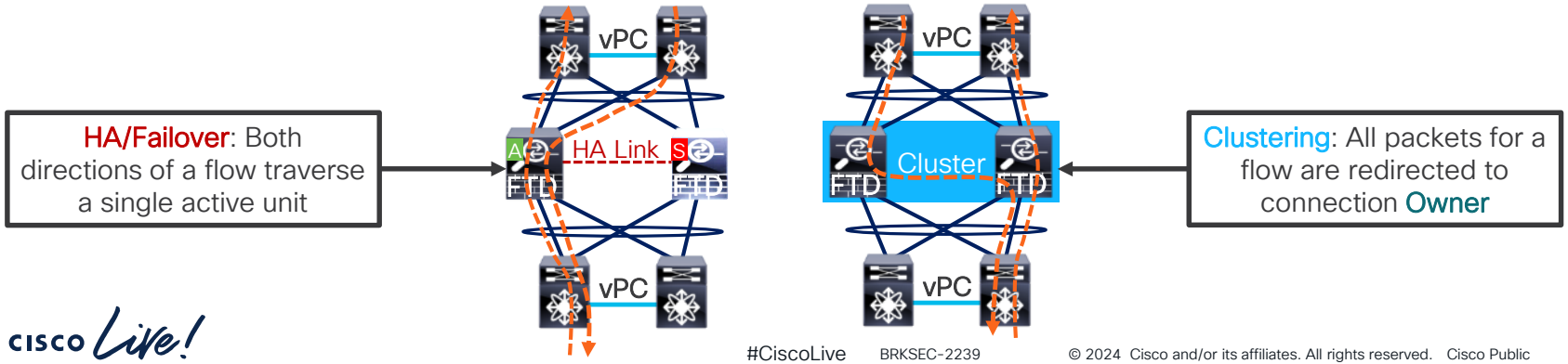
How to achieve high scale & redundancy?

That's a philosophical question

- HA or Clustering
- HA = Active/Standby (Active/Active for ASA with multi-context)
- Clustering = true horizontal scaling: with every device added you add capacity to handle traffic and scale to do so

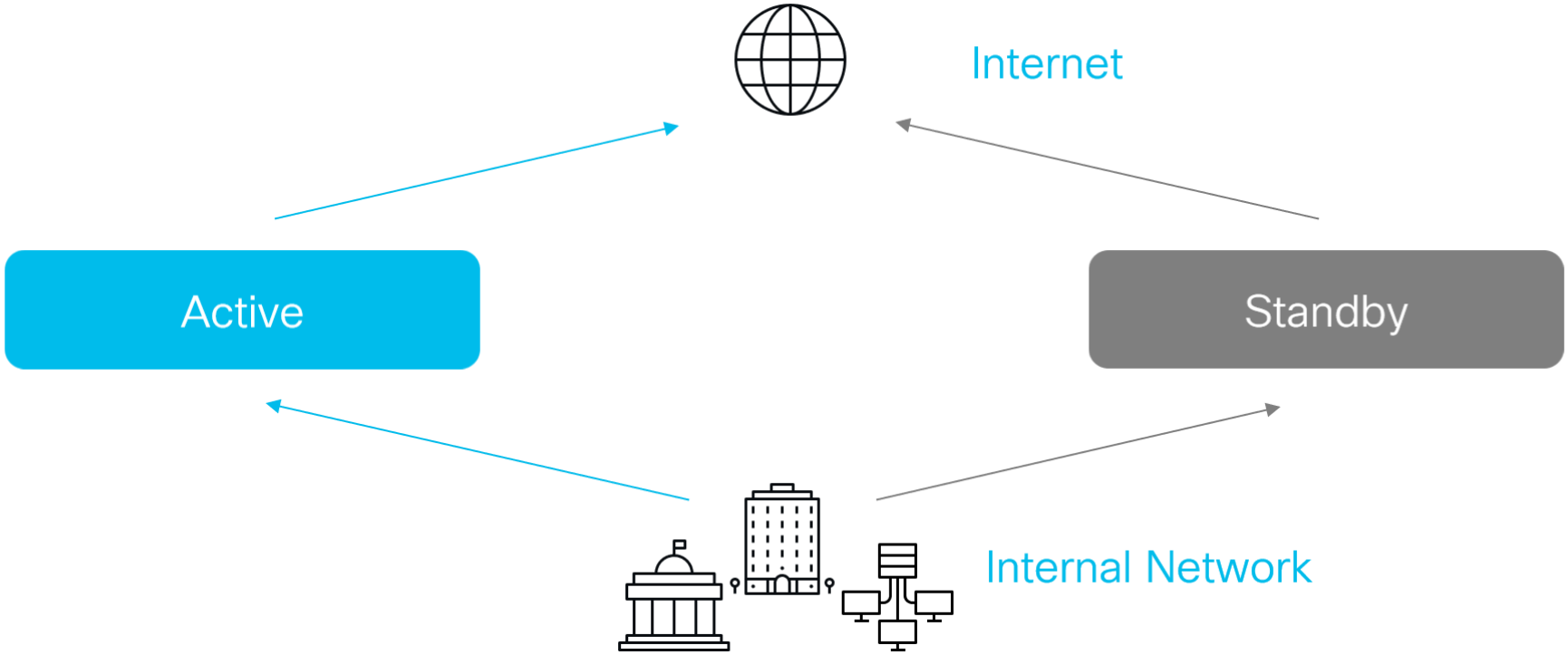
FTD High Availability and Clustering

- 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



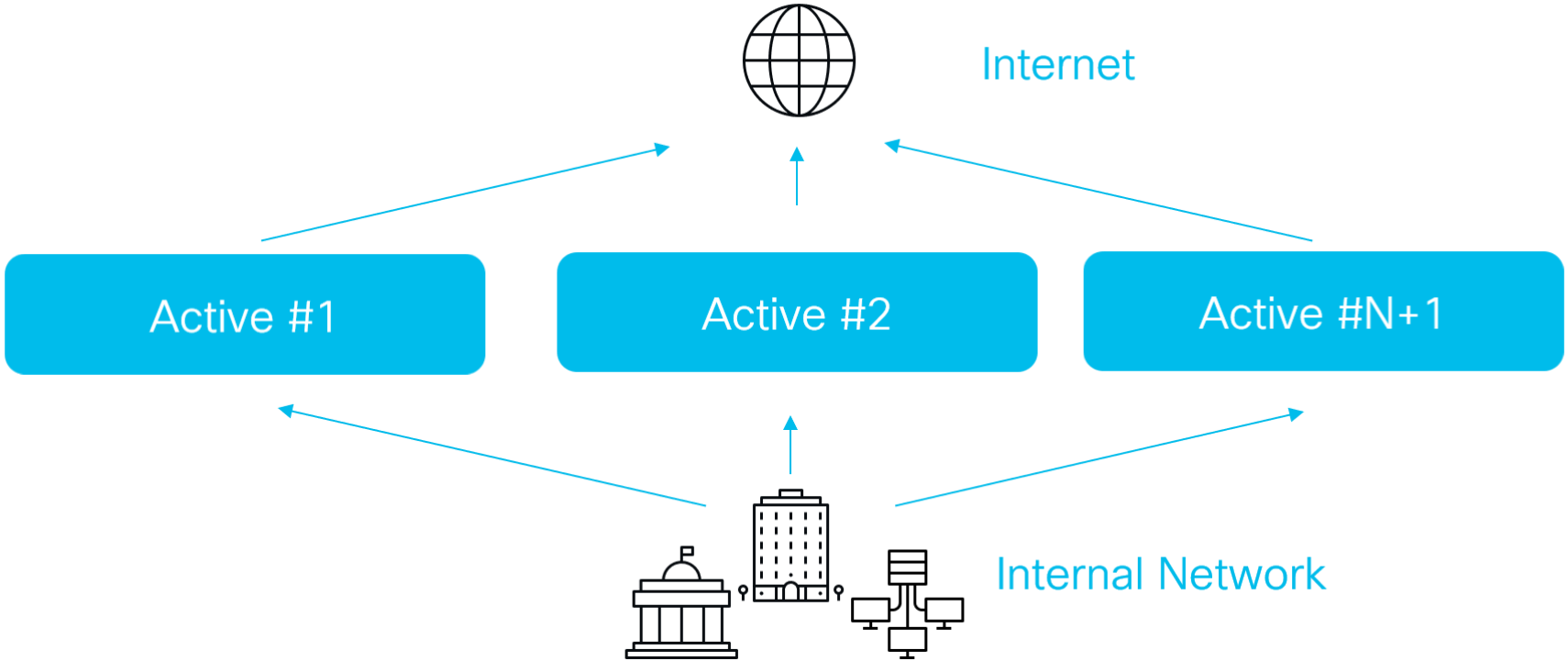
How to achieve high scale & redundancy?

Let’s start from basics – Active/Standby setup

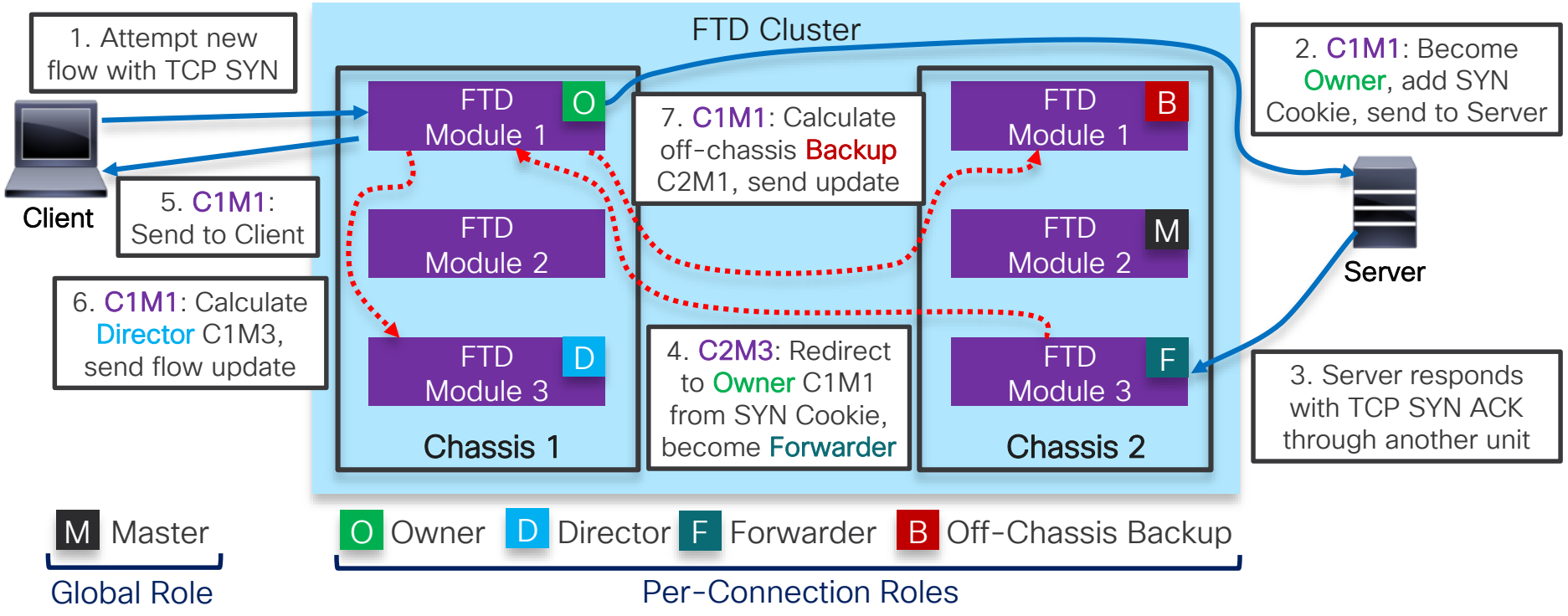


How to achieve high scale & redundancy?

Better setup – cluster – N+1 scale and redundancy, now in L2 & L3



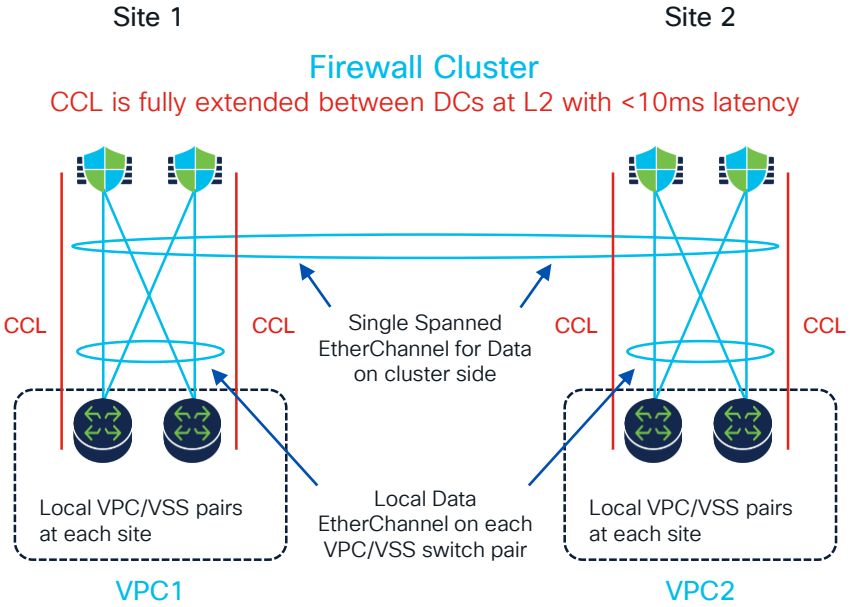
New TCP Flow with FTD Inter-Chassis Clustering



How to achieve high scale & redundancy?

Advanced setup – geo-redundant cluster, with traffic localization

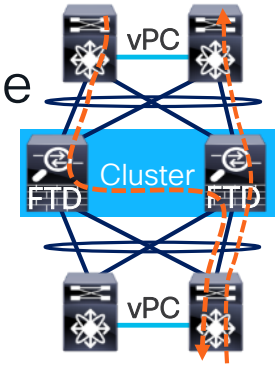
- North-South insertion with LISP inspection and owner reassignment
- East-West insertion for first hop redundancy with VM mobility
- Underlying fabric can be anything transporting Ethernet with RTT up to 20ms



Clustering for Virtual Firewalls

FTD 7.1+

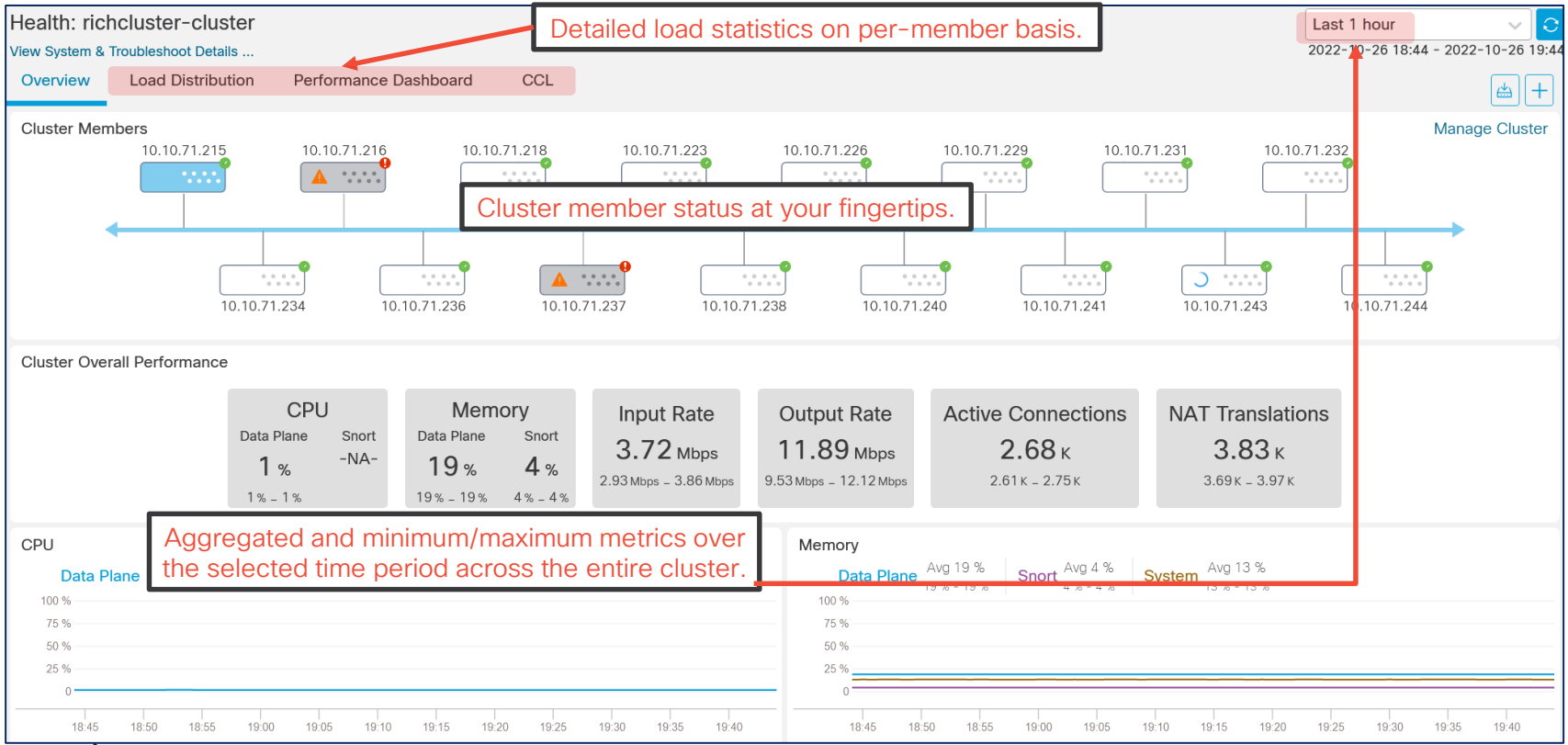
ASA 9.17+



- Clustering combines multiple firewalls into one logical device
  - Seamless scalability up to 16 FTD units with no traffic disruption
  - Stateful handling of asymmetric traffic and failure recovery
  - Single point of management and unified reporting
- Better elasticity and failure handling in hybrid cloud with clustering
  - aws Google Cloud Platform Azure KVM vmware
  - Individual data interface IP addresses instead of a single Port-channel
  - VxLAN-based Cluster Control Link for unicast control plane
  - No source NAT requirement for handling traffic asymmetry
  - Existing flow re-hosting on failure in supported environments

Cluster Health Dashboard

FMC 7.3



Individual Mode Clustering

FTD 7.6

ASA 9.22

Fully routed mode for 3100 and 4200

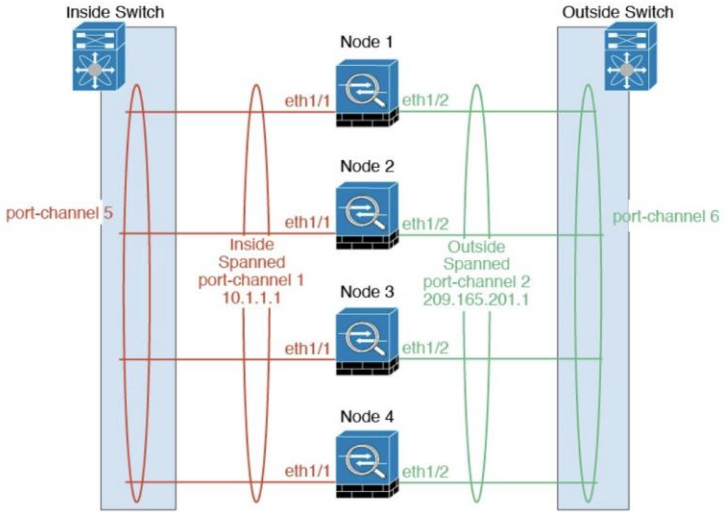
- On legacy ASA hardware, both spanned and routed clustering modes were supported
- Since then, we supported only spanned as that was initially most popular for Enterprise/DC high scale deployments
- With routed mode gaining more and more popularity (ECMP/UCMP), we're bringing routed/individual mode back
- Each unit runs its own as independent routing instance
- Feature supported with multi-context mode (ASA), but not (yet) on Multi-Instance as clustering is only coming

Individual Mode Clustering

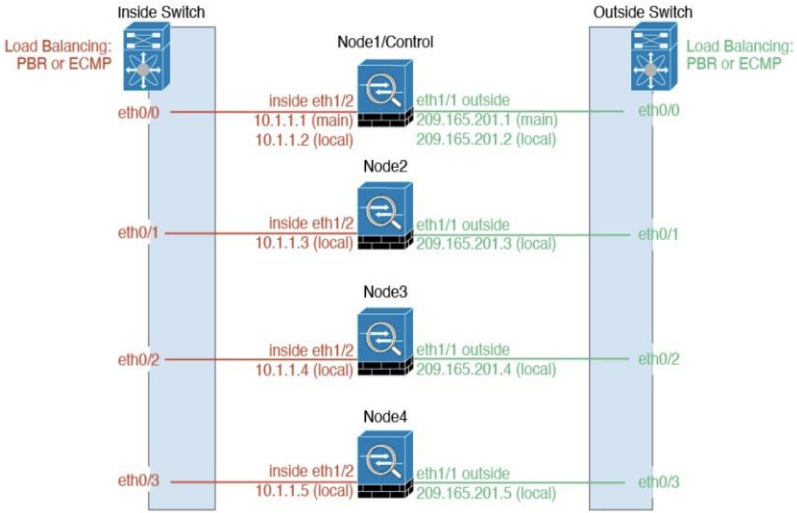
Fully routed mode for 3100 and 4200

FTD 7.6

ASA 9.22



Spanned Mode



Individual Mode

Individual Mode Clustering

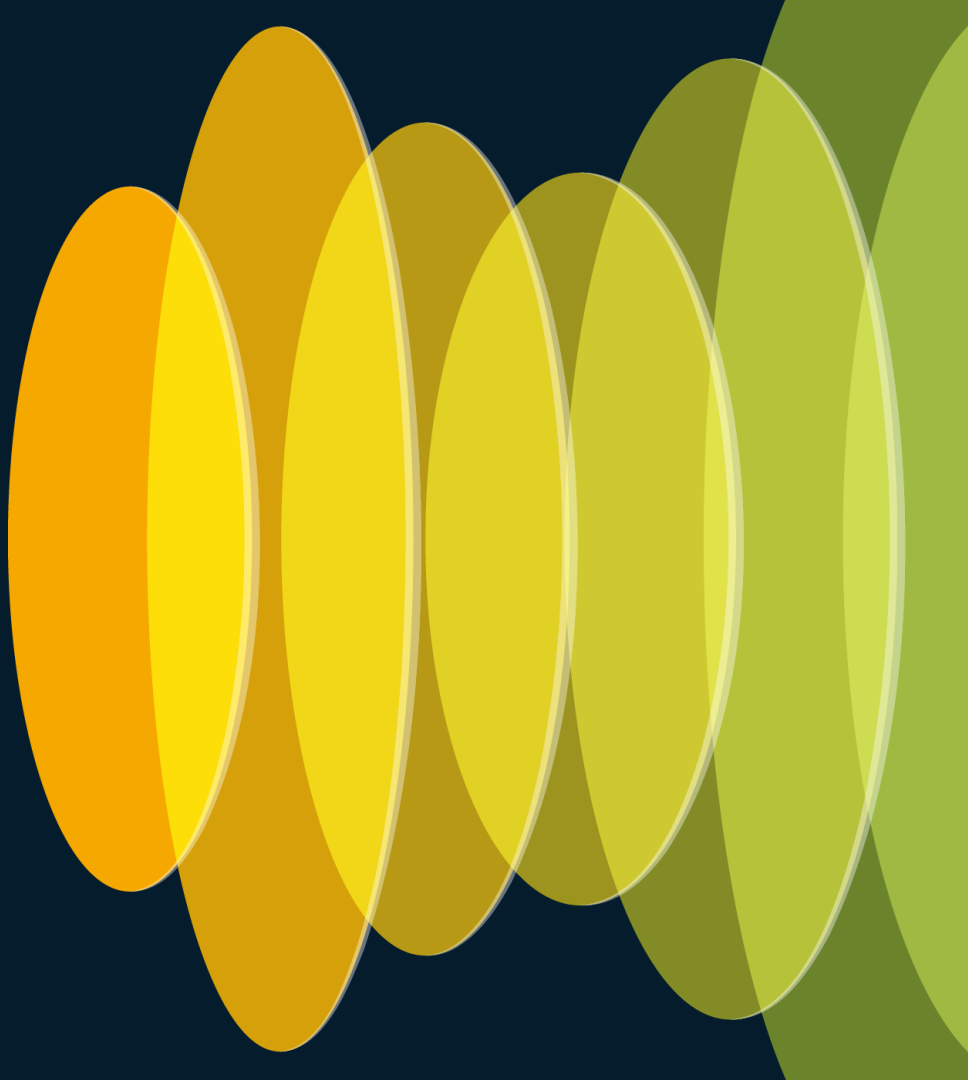
Fully routed mode for 3100 and 4200

FTD 7.6

ASA 9.22

Appliance model	Spanned Mode Cluster	Individual Mode Cluster
Layer used for ingress/egress traffic	L2	L3
Data Interface	Grouped to form a single spanned EtherChannel across all nodes	Each data interface has its own IP address received from cluster pool
Data Traffic Load Balancing	Handled by EtherChannel (upstream and downstream switches)	Uses ECMP/UCMP or PBR for load balancing (upstream and downstream routers)
Routing Modes	Routed or Transparent mode	Routed mode only

Designing for Multi-Tenancy

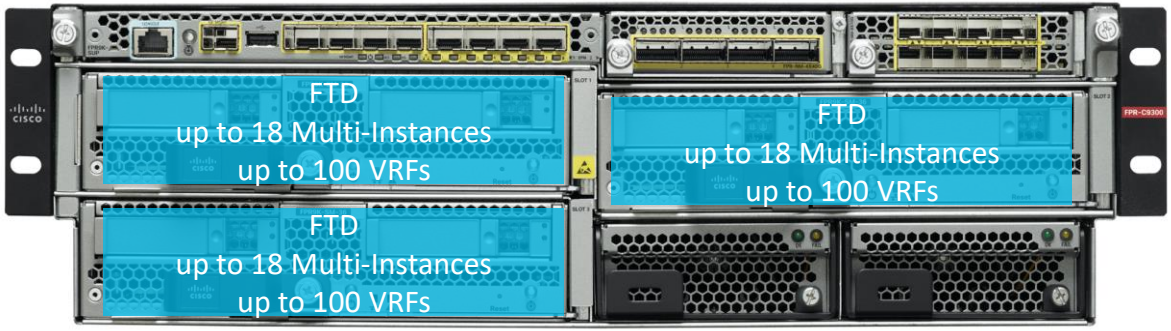


cisco Live!

Multi-tenancy at scale

Granular RBAC, separation using domains, VRFs and Multi-Instance

- Users see only devices assigned within their domain (up to 1024)
- FMC RBAC provides granular separation of duties between operators
- Multi-Instance and VRFs can be mixed in the same environment



Firepower 9300 service chaining – ASA + FTD

Unique capability for chassis with multiple Service Modules

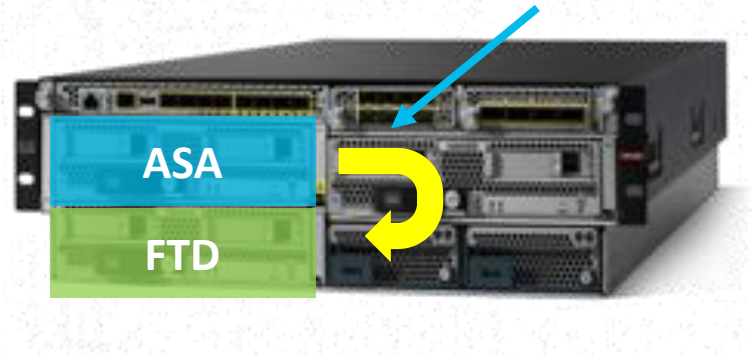
- Example configuration:
  - SM-40 for ASA RA VPN duties
    up to 20k tunnels, and up to 15Gbps DTLS throughput
    with 450 byte packets
  - SM-56 for FTD NGFW/NGIPS duties
    up to: 64Gbps of NGFW (IPS+AVC) throughput,
    35M connections, 490K CPS, 12Gbps TLS inspection
    (50% of overall traffic)

Incoming AnyConnect users – full RA VPN feature set on ASA

Incoming traffic to NGFW/NGIPS protected services in DMZ

Outgoing traffic from NGFW/NGIPS protected users & AnyConnect users (if working with centralized internet access)

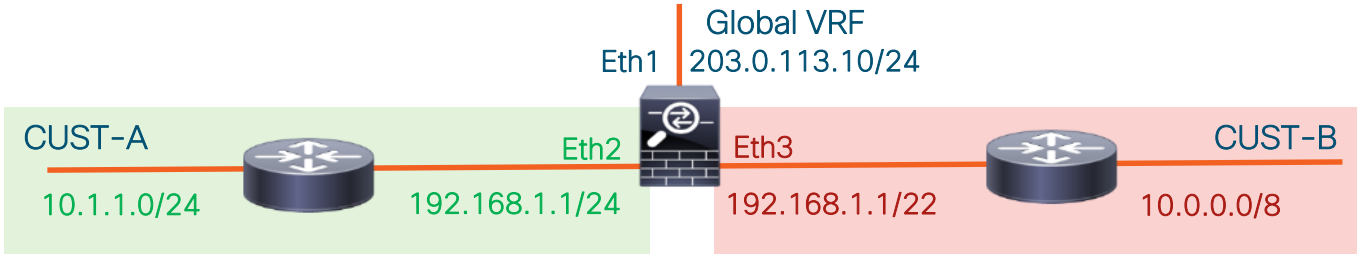
Decrypted traffic from AnyConnect sessions terminated at ASA moves to inspection by NGFW/NGIPS, on the way back is again encrypted by ASA and sent to remote endpoint



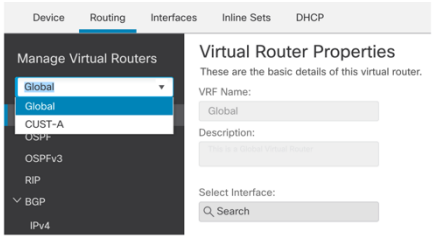
Available from FXOS 2.6(1), ASA 9.12(1) and FTD 6.4.0:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/release/notes/fxos261_rn.html#id_113895

Virtual Routing and Forwarding (VRF) Lite

- Starting from FTD 6.6, interfaces can be in different Routing Domains
  - Overlapping IP address support between user and Global VRF
  - Traffic forwarding between different VRF with static routes and NAT

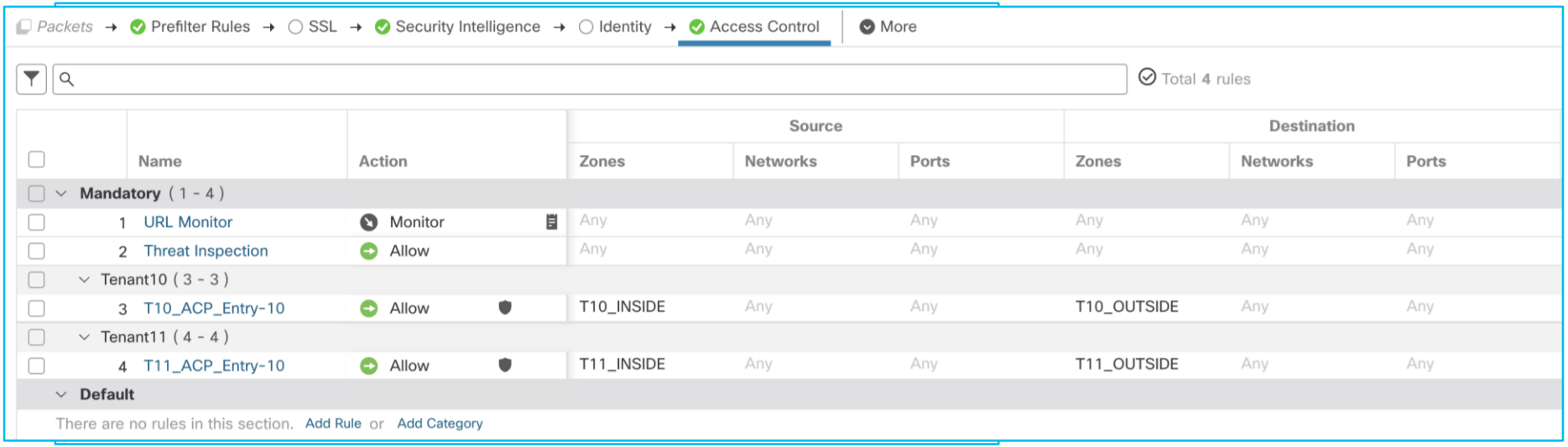


- Existing single security policy across all VRFs, no per-VRF rules
  - Connection events are enriched with VRF ID for usability
- Can be combined with FTD multi-instance



Multi-tenancy at scale

“How to achieve massive scale for Fun & Profit”



REFERENCE

VRF Scalability as for FTD 7.6

Current generation platforms

Platform	VRF Count	Platform	VRF Count	Platform	VRF Count
1010/1120	5	3105	10	4215	100
1140	10	3110	15	4225	100
1150	10	3120	25	4245	100
		3130	50		
1210CE/CP	5	3140	100	9300 SM-44	100
1220CX	10			9300 SM-48	100
				9300 SM-56	100
2110	10	4112	60		
2120	20	4115	80		
2130	30	4125	100	FTDv	30
2140	40	4145	100	ISA 3000	10

VRF Scalability as of last FTD version supported

Previous generation platforms

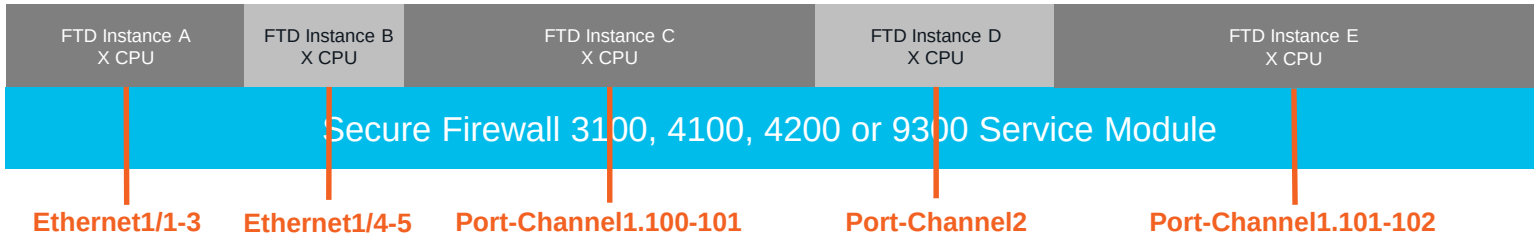
Platform	VRF Count	Platform	VRF Count
ASA5508-X	10	9300 SM-24	100
ASA5516-X	10	9300 SM-36	100
ASA5525-X	10	9300 SM-40	100
ASA5545-X	20		
ASA5555-X	20		
4110	60		
4120	80		
4140	100		
4150	100		

Multi-Instance Capability Summary

FTD 7.6

Supported on 3100, 4100, 4200 and 9300

- Instantiate multiple logical devices on a single module or appliance
  - FTD application in 6.3 for 4100 and 9300
  - FTD application in 7.4 for 4200 and 7.4.1 for 3100
  - Leverage Docker infrastructure and container packaging
- Allows tenant management separation, independent instance upgrade and resource protection



Multi-Instance Scale Summary

1/3

REFERENCE

Appliance model	Initial FTD support	Management Solution	Maximum number of instances
Virtual FTD (FTDv)	-	-	-
1010/11xx	-	-	-
1200C	-	-	-
3105	-	-	-
3110	7.4.1	FMC	3
3120	7.4.1	FMC	5
3130	7.4.1	FMC	7
3140	7.4.1	FMC	10

Reference:
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html

REFERENCE

Multi-Instance Scale Summary
2/3

Appliance model	Initial FTD support	Management Solution	Maximum number of instances
4110	6.3.0	FMC & FXOS	3
4120	6.3.0	FMC & FXOS	3
4140	6.3.0	FMC & FXOS	7
4150	6.3.0	FMC & FXOS	7
4112	6.6.0 / 2.8.1	FMC & FXOS	3
4115	6.4.0 / 2.6.1	FMC & FXOS	7
4125	6.4.0 / 2.6.1	FMC & FXOS	10
4145	6.4.0 / 2.6.1	FMC & FXOS	14

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-instance/multi-instance_solution.html

REFERENCE

Multi-Instance Scale Summary
3/3

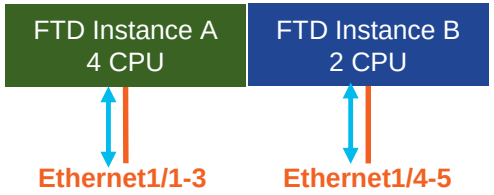
Appliance model	Initial FTD support	Management Solution	Maximum number of instances
4215	7.6.0	FMC	10
4225	7.6.0	FMC	15*
4245	7.6.0	FMC	34
9300 SM-24	6.3.0	FMC & FXOS	7
9300 SM-36	6.3.0	FMC & FXOS	11
9300 SM-44	6.3.0	FMC & FXOS	14
9300 SM-40	6.4.0 / 2.6.1	FMC & FXOS	13
9300 SM-48	6.4.0 / 2.6.1	FMC & FXOS	15
9300 SM-56	6.4.0 / 2.6.1	FMC & FXOS	18

Network Interfaces

Multiple modes for Secure Firewall appliances

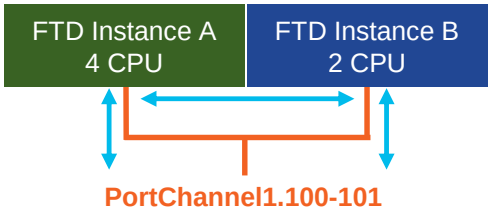
- Physical, EtherChannel, and VLAN subinterfaces are an option
  - FXOS supports up to 500 total VLAN subinterfaces since FXOS 2.4.1
  - FTD can also create VLAN subinterfaces on physical and EtherChannel interfaces
  - Each instance can have a combination of different interface types

Data (Dedicated)



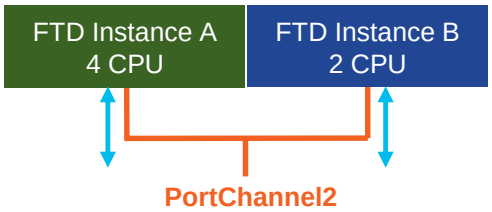
Supported Modes: Routed, Transparent, Inline, Inline-tap, Passive, HA
Supported Traffic: unicast, broadcast, multicast

Data-Sharing (Shared)



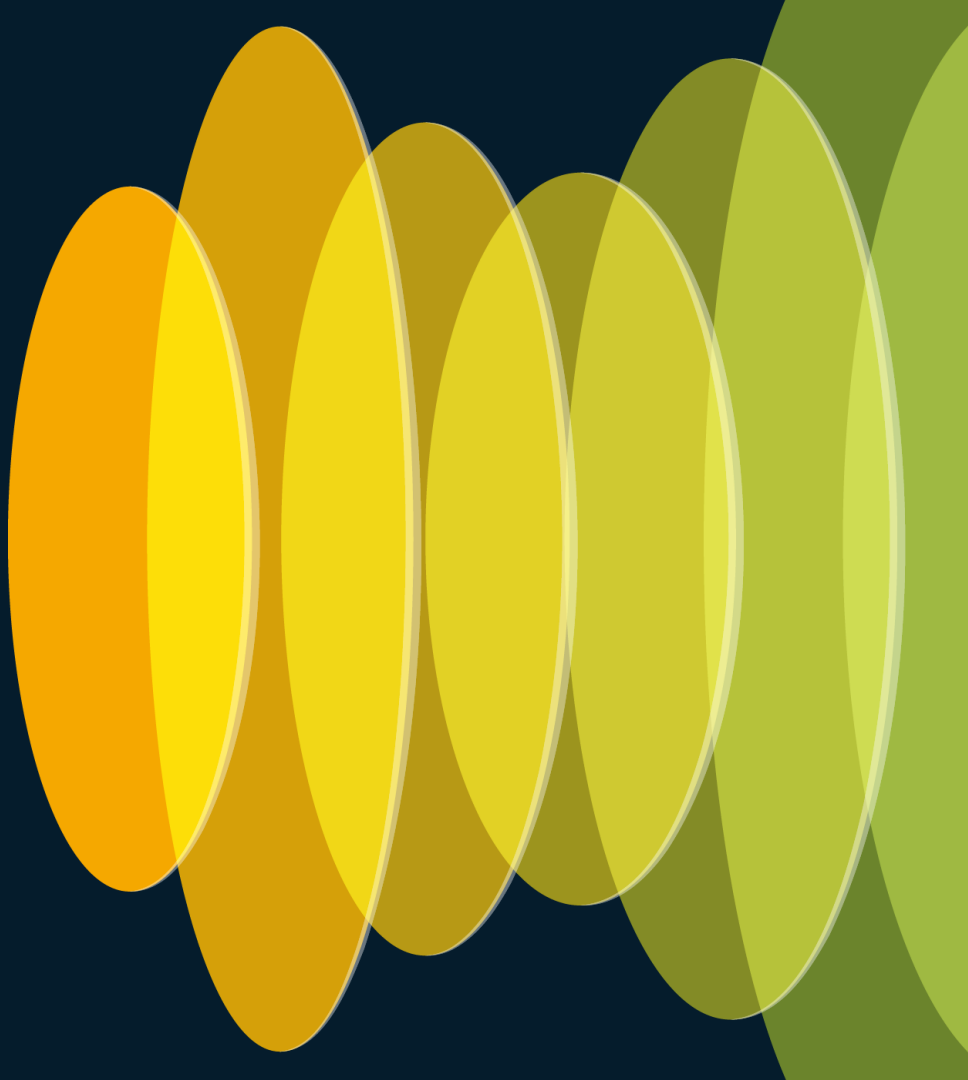
Supported Modes: Routed (no BVI members), HA
Supported Traffic: unicast, broadcast, multicast

Mgmt/Firepower-Eventing



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

Designing for Internet Edge



cisco Live!

Routing on Cisco Firewall at the edge

- Multiple use cases
  - Redundant/optimal internet access
  - SDWAN scenarios
  - Internal network routing architecture
- Both ASA and FTD support all major routing protocols:
  - RIP, OSPFv2, OSPFv3, IS-IS, EIGRP and BGP
  - PIM-SM for multicast routing (with IGMPv1/v2)

How we test our FTD appliances?

REFERENCE

Appliance model	Maximum # of BGP routes tested	Maximum # of BGP neighbors
1010/1100	5k / 10k	5
1200C	50k	100
3100	100k	500 (w/BFD)
4100	200k	500 (w/BFD)
4200	200k	500 (w/BFD)
9300	200k	500 (w/BFD)

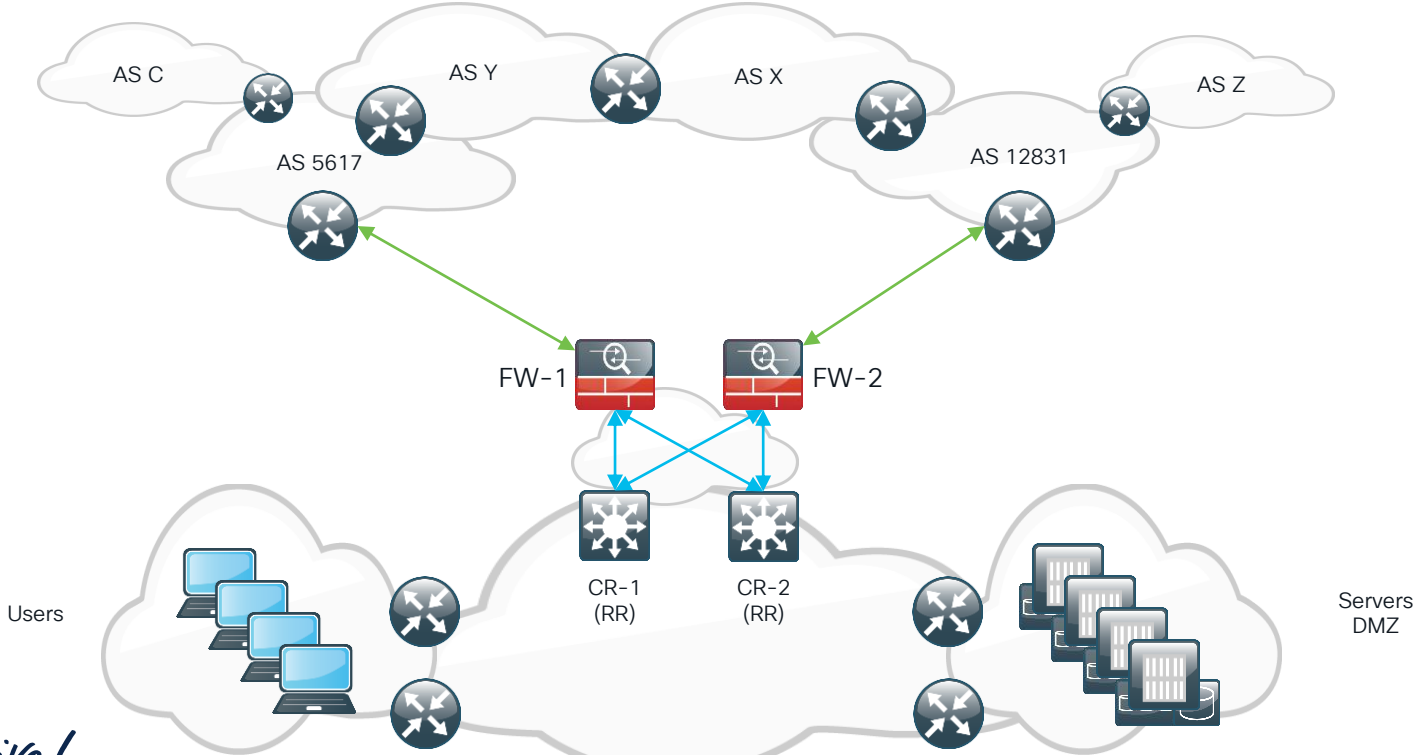
How we test our FTD appliances?

REFERENCE

Appliance model	Maximum # of BGP routes tested	Maximum # of BGP neighbors
5505	5k	2
5512	20k	20
5525	15k	60
5545	15k	100
5555	15k	100
5508	10k	10
5516	10k	10
ASA 5585 SSP-10	20k	200
ASA 5585 SSP-60	100k	500

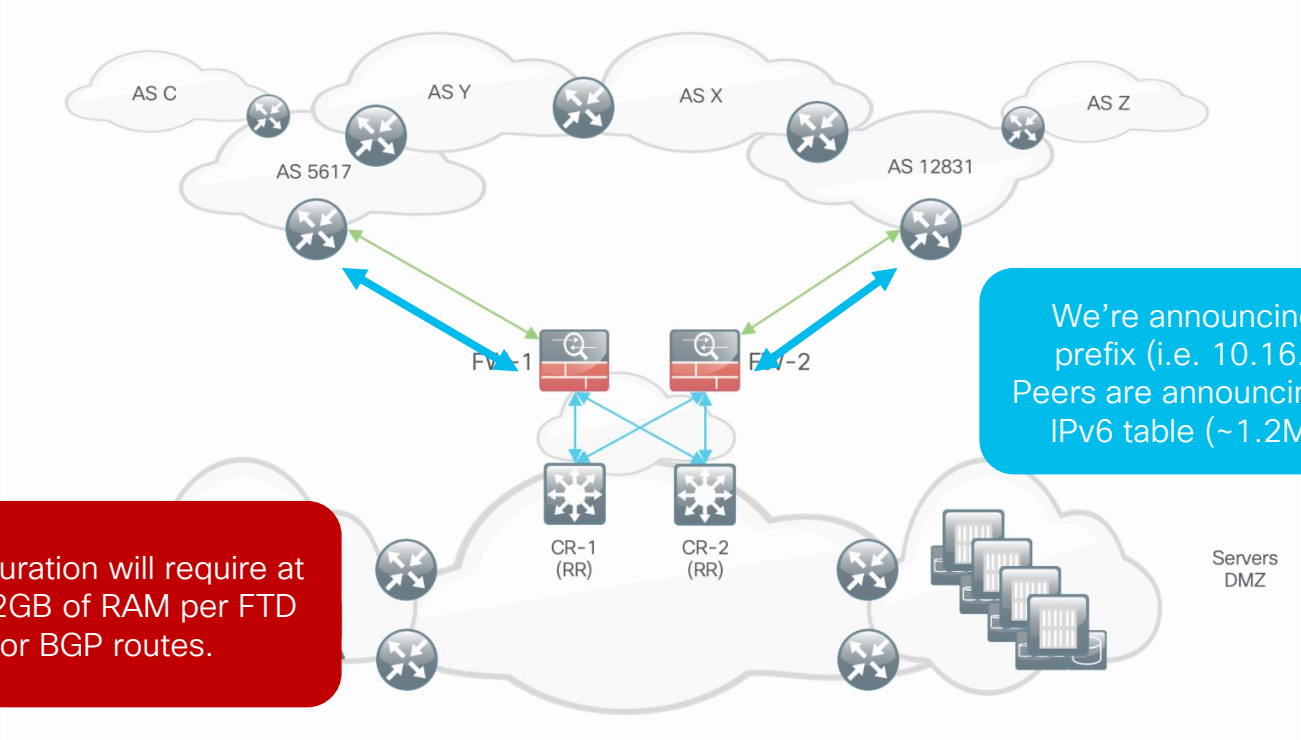
Internet access scenario - BGP

Topology and major assumptions



Internet access scenario - eBGP

Option 1: full BGP routes



We're announcing our own prefix (i.e. 10.16.24.0/24). Peers are announcing full IPv4 & IPv6 table (~1.2M prefixes)

This configuration will require at least 1.5-2GB of RAM per FTD just for BGP routes.

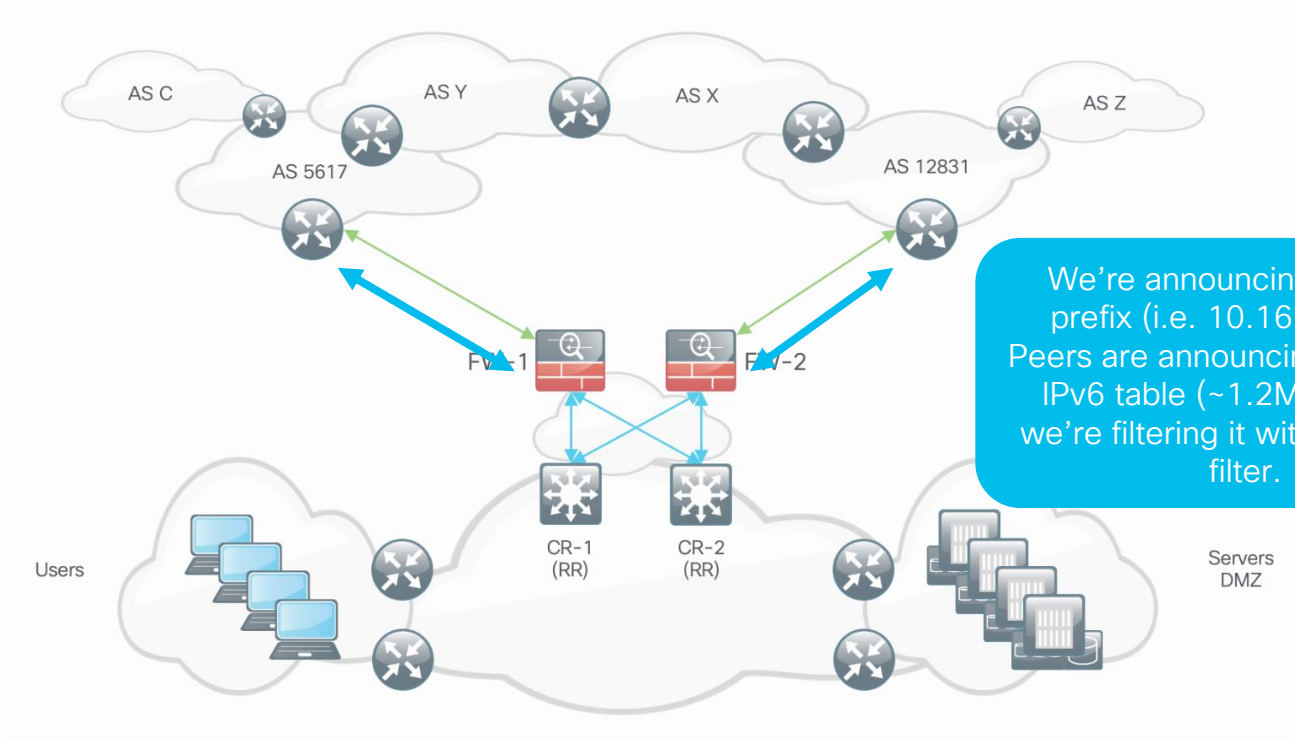
Internet access scenario – eBGP

Option 1: full BGP routes

```
> show bgp ipv4 unicast summary
BGP router identifier 95.130.5.229, local AS number 65001
BGP table version is 941583, main routing table version 941583
941582 network entries using 188316400 bytes of memory
941582 path entries using 75326560 bytes of memory
150370/150370 BGP path/bestpath attribute entries using 31276960 bytes of memory
125950 BGP AS-PATH entries using 7850244 bytes of memory
10813 BGP community entries using 1427692 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 304197856 total bytes of memory
BGP activity 941582/0 prefixes, 941582/0 paths, scan interval 60 secs

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
85.232.240.179  4      57355 150556  4       941583    0    0 00:00:40  941582

> show memory
Free memory:       3117802117 bytes (38%)
Used memory:       5044823176 bytes (62%)
-------------    ------------------
Total memory:      8162625293 bytes (100%)

Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the firewall process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
```

Internet access scenario - eBGP

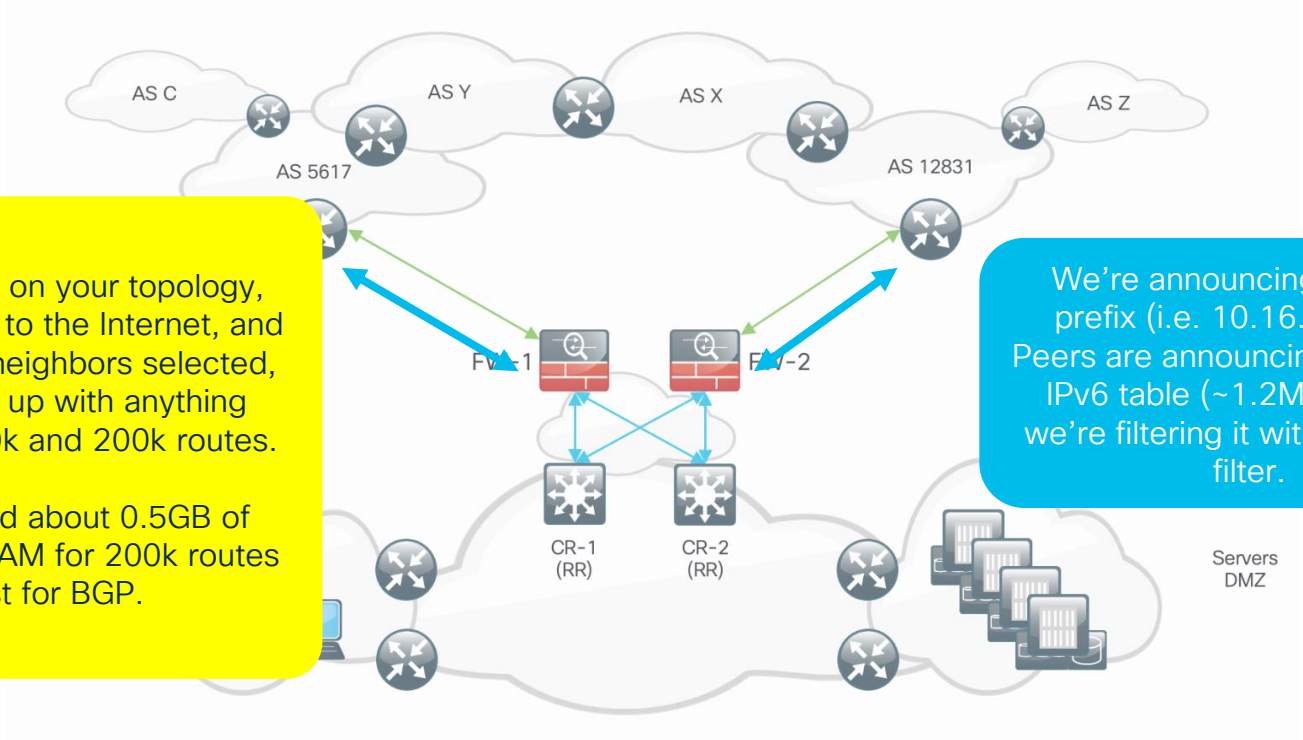
Option 2: partial BGP routes - limit AS_PATH to 2-3 (neighbor++)



We're announcing our own prefix (i.e. 10.16.24.0/24). Peers are announcing full IPv4 & IPv6 table (~1.2M prefixes), we're filtering it with AS_PATH filter.

Internet access scenario - eBGP

Option 2: partial BGP routes - limit AS_PATH to 2-3 (neighbor++)



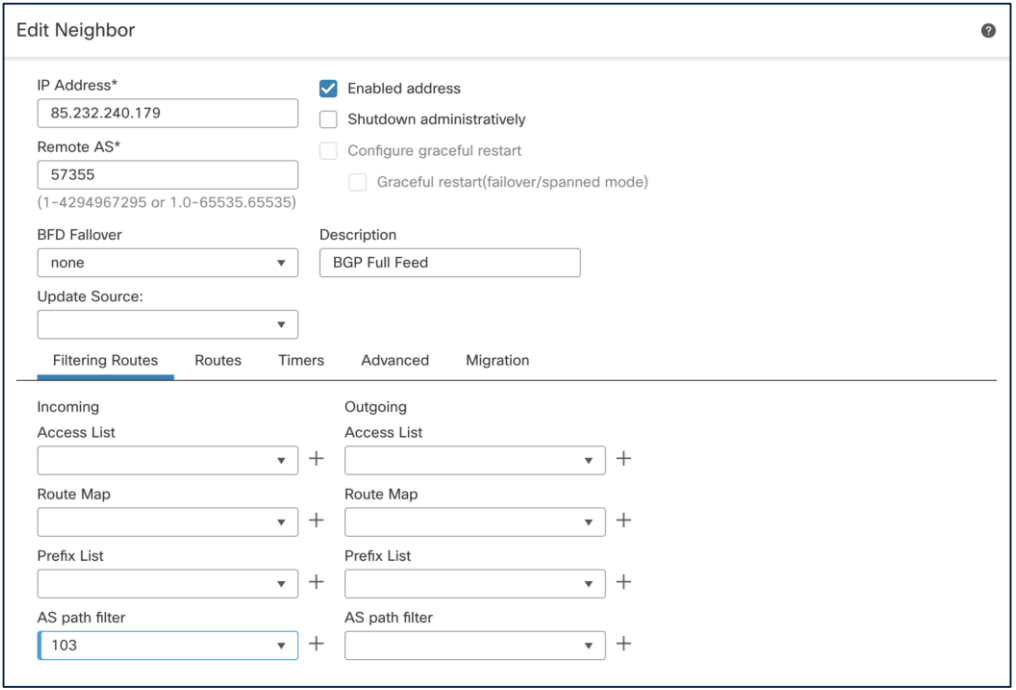
Depending on your topology, connectivity to the Internet, and number of neighbors selected, you'll end up with anything between 30k and 200k routes.

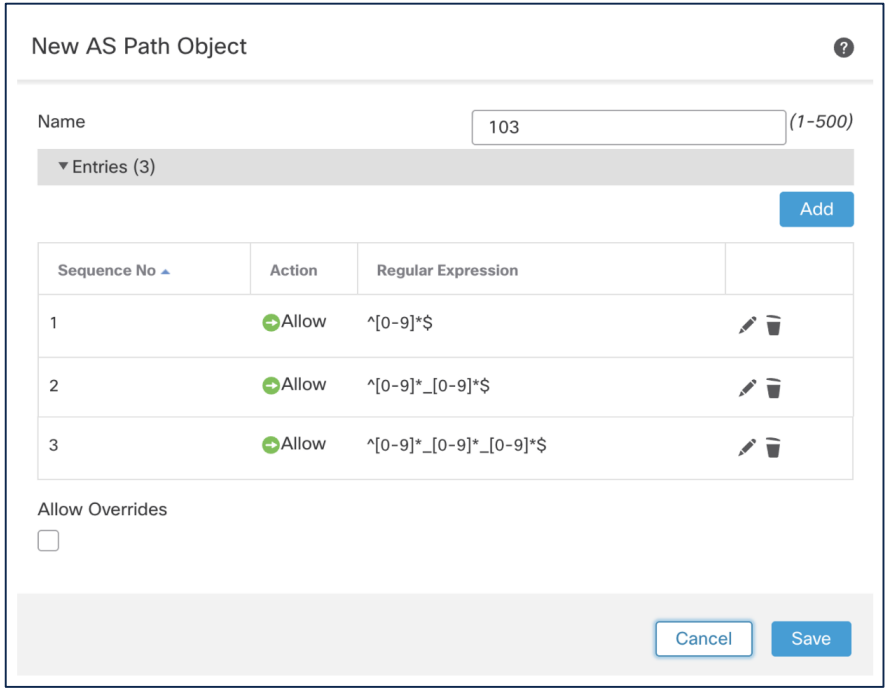
You'll need about 0.5GB of additional RAM for 200k routes just for BGP.

We're announcing our own prefix (i.e. 10.16.24.0/24). Peers are announcing full IPv4 & IPv6 table (~1.2M prefixes), we're filtering it with AS_PATH filter.

Internet access scenario - eBGP

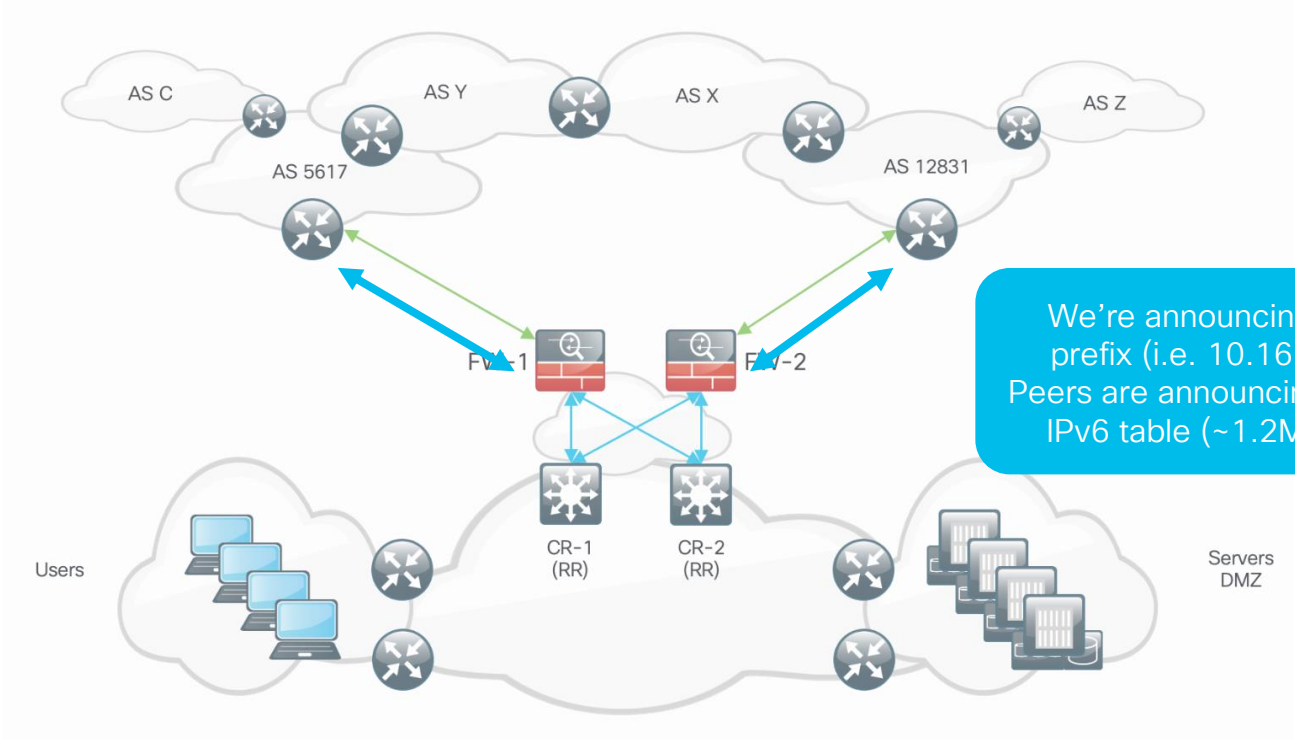
Option 2: partial BGP routes - limit AS_PATH to 2-3 (neighbor++)





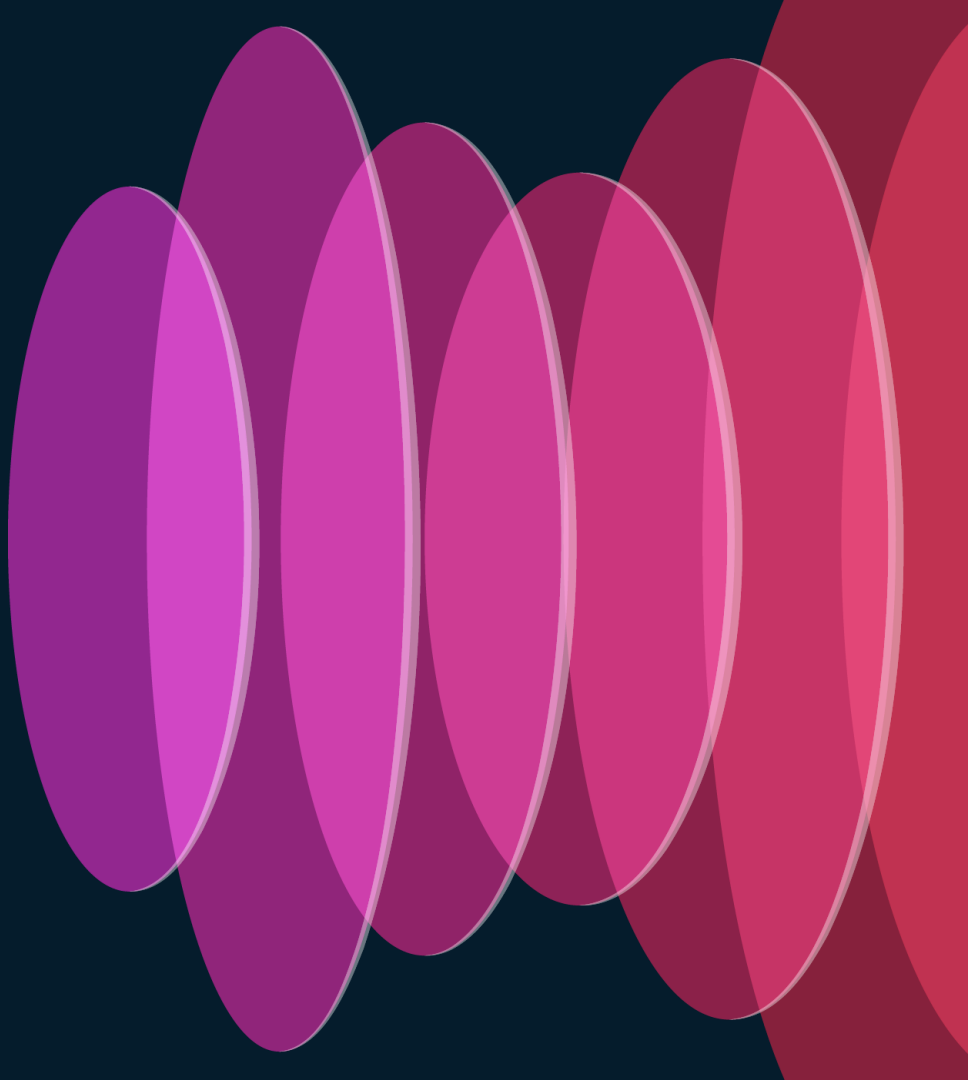
Internet access scenario – eBGP

Option 3: only default routing, BGP used as link keepalive



We're announcing our own prefix (i.e. 10.16.24.0/24). Peers are announcing full IPv4 & IPv6 table (~1.2M prefixes)

Summary



Cisco Security Beta Programs

Influence product design

Design research participants shape the look, feel, & functionality of new product features and offerings

Attention to Feedback

Beta customer bugs and enhancements receive high visibility & priority

Top notch communication

Private conference calls with product team

Training

Customers receive early training & experience with new features

Customer Support

Feature experts will be on-hand & responsive to your issues

Sign Up Now: https://cs.co/security-beta

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Secure Firewall Learning Map

START

Monday, June 3 | 2:30 p.m.

BRKSEC-2515

Harnessing Identity-Based Firewalling on the Meraki MX Powered by the Meraki Full Stack

Monday, June 3 | 4:00 p.m.

BRKSEC-1036

Quantum Ready Firewalls

Tuesday, June 4 | 10:30 a.m.

BRKSEC-2086

Optimizing Security and Agility: Leveraging SD-WAN with Cisco Secure Firewall

Tuesday, June 4 | 1:00 p.m.

BRKSEC-3320

Pig-in-the-middle - TLS Decryption and Encrypted Visibility Engine Deep Dive on Cisco Secure Firewall

Wednesday, June 5 | 2:30 p.m.

BRKSEC-2166

Cloud Management of Cisco Secure Firewall

Thursday, June 6 | 8:30 a.m.

FINISH

BRKSEC-2236

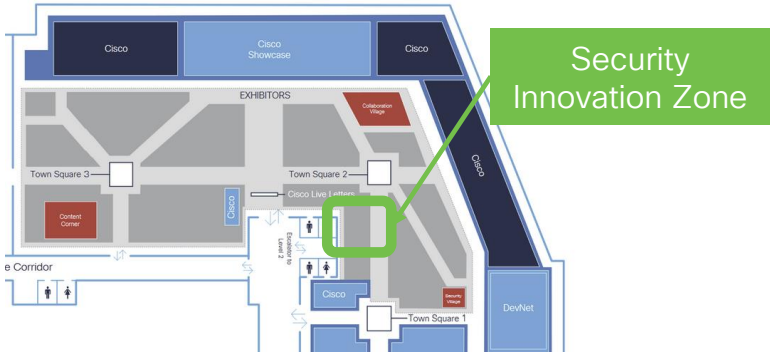
Keeping Up on Network Security with Cisco Secure Firewall

Continue your education

- Hear Tom Gillis at the Security Deep Dive Keynote KDDSEC-1000!

  Securing User to Application and Everything in Between
  Wednesday, June 5 | 1 – 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



Thank you