CISCO
SECURE

CISCO The bridge to possible

Cisco Tech Club Security update

Secure Firewall 4200 a ISE 3.3 / SNS 3700

Milan Habrcetl
Cisco Cyber Security Specialist
July 25th, 2023

Agenda

- Firepower 4200
- ISE update / SNS 3700

Agenda

- Firepower 4200

Cisco Secure Firewall

Physical appliances

Cisco Secure Firewall hardware appliances
running either ASA or FTD application

Private & Public cloud

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
ASA running as a VM

Meraki MX
Snort 3 running in container

Cisco Secure Firewall 7.4 and 7.4.1 *

Aggressive feature velocity provides a rich feature set for Cisco Secure Firewalls, 4200 series included

Zero Trust Micro segmentation

Protecting application environments with integrated firewall & workload protection

Securing Multicloud environments

New CSPs & Hypervisor, Flexible & Tiered Licensing, Cloud FW-aaS, Horizontal Scaling

Securing Hybrid Worker

Simplified remote worker security - advance posture, passwordless authentication & new unified client

Modern NGIPS

Superior threat visibility & performance with Snort 3

Visibility & Enforcement in encrypted traffic

Delivering threat & application visibility with TLS 1.3 decryption, Server Identity and Encrypted Visibility Engine

Simplified Branch Deployments

New WAN capabilities for intelligent path selection and direct internet access

Secure Dynamic Attribute Connector

Enabling strong policies for infrastructure without fixed IP addresses

Scalable Analytics, Threat Response & Orchestrator

Accelerate detection & remediation – “See x, Do y”

With 300+ agile features, usability improvements, software optimizations

Now offering newer RTMs, Marketplace offerings, Flexible & Tiered Licensing

* Note that 7.4 will only be available on the 4200. Other platforms require 7.4.1.

Cisco Secure Firewall Hardware Portfolio

650 Mbps AVC+IPS

1.5-2.2 Gbps AVC+IPS

2.3-20 Gbps AVC+IPS

17-45 Gbps AVC+IPS
8 - 22.4 Gbps IPsec VPN
8 Node Cluster:
With 3140, up to AVC+IPS(1024B) = 288 Gbps

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS
Sixteen node cluster:
Up to 680 Gbps AVC
Up to 675 Gbps AVC+IPS

Stand-alone device:
70-150 Gbps AVC
70-145 Gbps AVC+IPS
Sixteen node cluster:
Up to 1.7 Tbps AVC
Up to 1.6 Tbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Sixteen node cluster:
AVC+IPS
SM40*16n = 704 Gbps
SM48*16n = 830 Gbps
SM56*16n = 950 Gbps

1010

1120/40/50

2110/20/30/40

3105/10/20/30/40

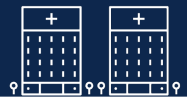
4112/15/25/45

NEW

4215/25/45

9300 Series
SM-40
SM-48
SM-56

SMB



Branch Office

Mid Enterprise

Large Enterprise

Data Center

Service Provider

All appliances can run either ASA or FTD applications, FP9300 can run both on different SMs

Introducing the Cisco Secure Firewall 4200 Series

Superior Performance

- Achieve High Performance Packet Processing with powerful hardware, a wide range of high performing network interfaces with a 1 RU footprint.
- Gain visibility into encrypted traffic with crypto-accelerated architecture, speeding up TLS and IPsec decryption.

Outstanding ROI

- Grow your security infrastructure as your business grows with clustering capability of up to 16 firewall devices.
- Ensure business uptime with hot-swappable network modules, including fail-to-wire interfaces.

1RU, 16X clustering, 200G interface support, 2X interface module bays, dual SSD, dual mgt interface

Introducing the Cisco Secure Firewall 4200 Series

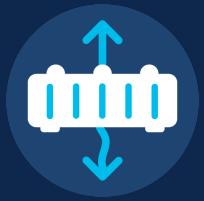
Crypto Acceleration

A specially built circuit to provide encryption/decryption acceleration

Crypto-acceleration using an FPGA (Field-programmable gate array)

Flow Offload

Flow offload engine processes packets in hardware up through layer 4



Interface Flexibility

Support for 1G,10G,25G,40G,100G,200G interfaces across 2 Network Modules

FIPS Compliance

Supports all FIPS 140-3 requirements

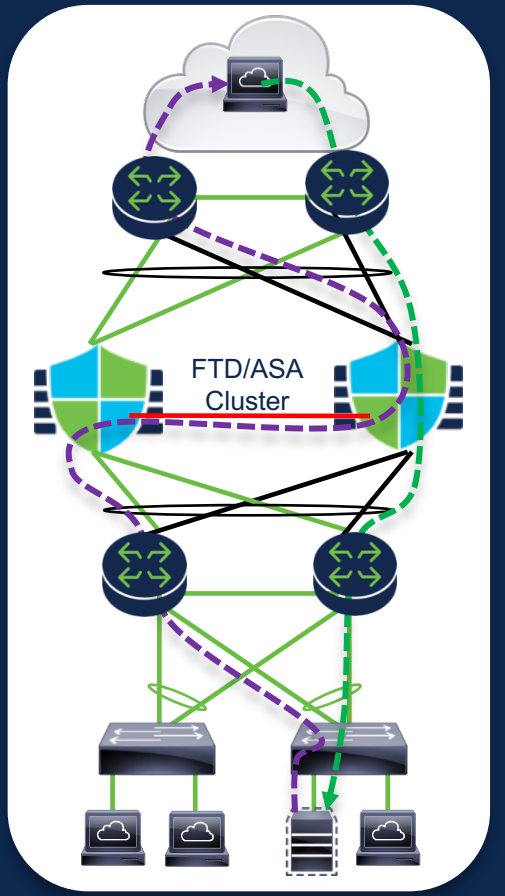
Selected Performance Metrics – Current Estimates

Metric	4215	4225	4245
Throughput* FW+AVC+IPS	71 Gbps	89 Gbps	149 Gbps
Throughput* IPsec VPN (Fastpath)	51 Gbps	86 Gbps	145 Gbps
Maximum number of VPN peers	20000	25000	30000
Maximum concurrent connections with AVC	15 M	30 M	60 M
Maximum new connections per second (ASA code)	1.5 M	1.8 M	2.1 M

* Stateful Inspection 1024 Byte Packets

Scalable Security with Clustering

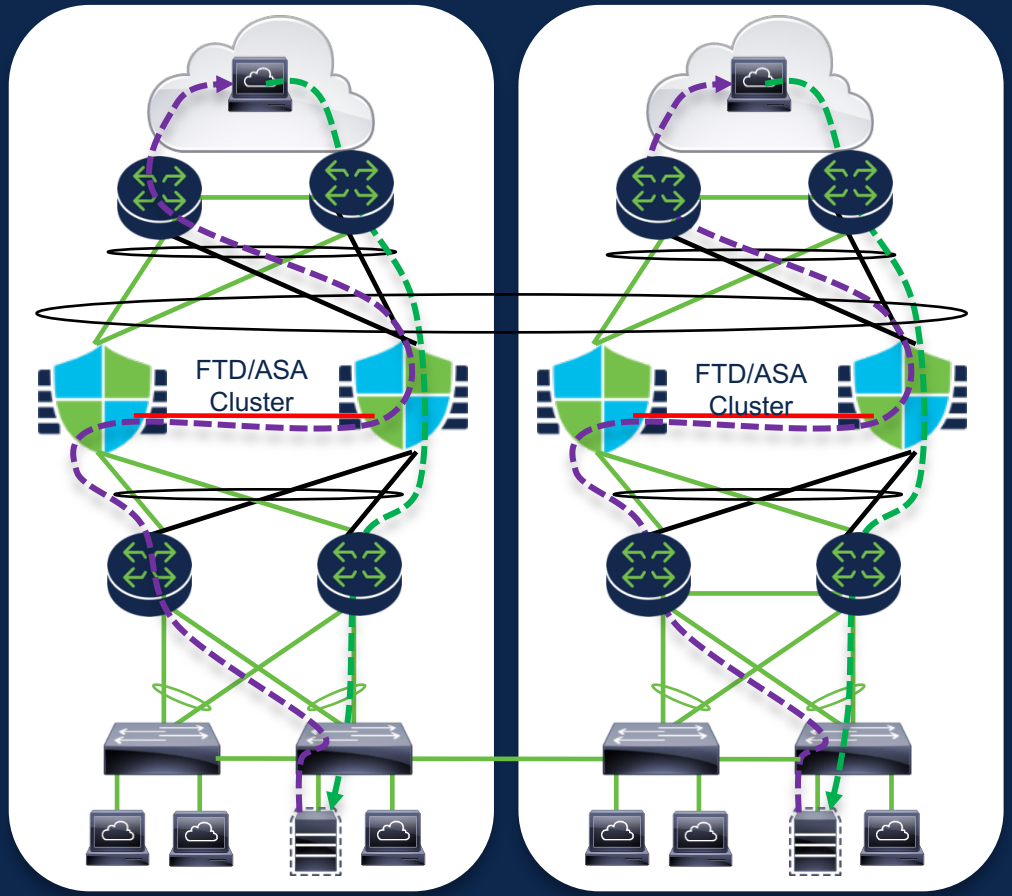
- Combines multiple Cisco Secure Firewalls into a single logical device
  - Allows pay as you grow sizing – nodes can be added to existing clusters
  - Up to 16 nodes, depending on platform
  - Example: 16 node 4245 cluster provides 1.6 Tbps throughput (FW+AVC+IPS)
- EtherChannel with LACP provides resilience
- Resolves routing asymmetry
  - All packets in a (bidirectional) flow are redirected to the *flow owner* (the first node to see the flow).
  - Essential for inspection of asymmetric flows



Inter-Site Clustering

- A single cluster can span multiple data centers
- Each node has a *site ID*
  - Nodes share site specific MAC addresses for egress*
  - Nodes share site specific IP addresses for egress*
- LISP integration to enhance site mobility (Such as Vmotion) by moving the flow owner
- Facilitates ACI Anycast Services Gateway integration for ACI multi-pod

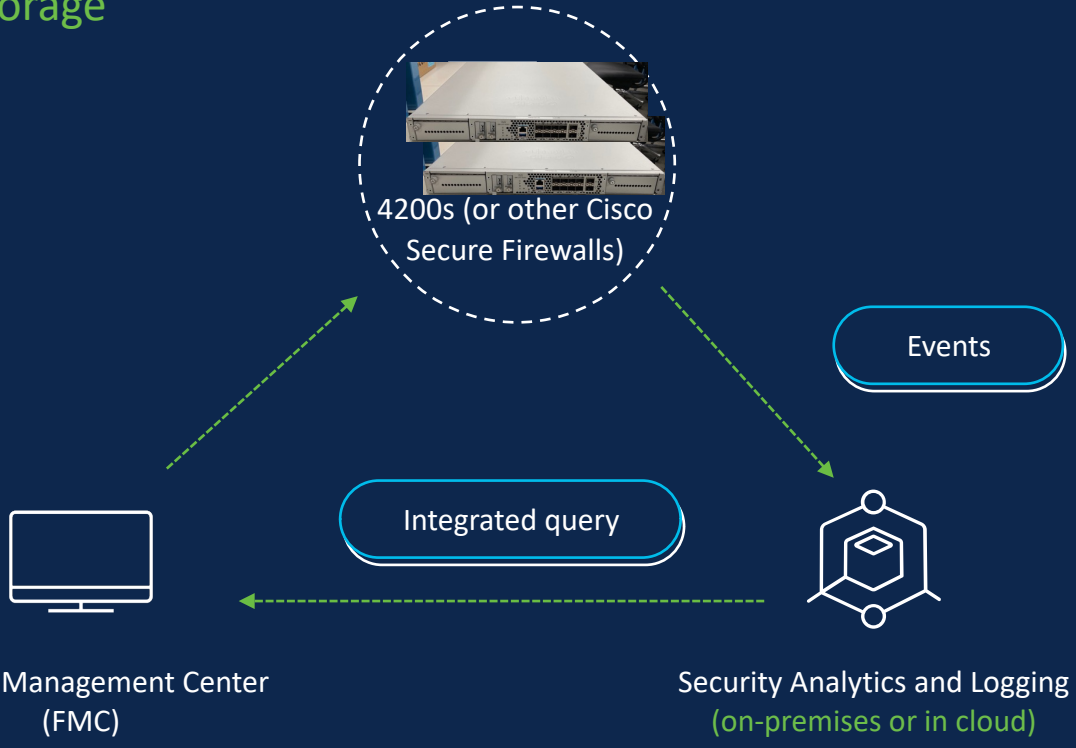
*ingress uses global MAC & IP addresses



Scalable Event Aggregation On-Premises and In Cloud

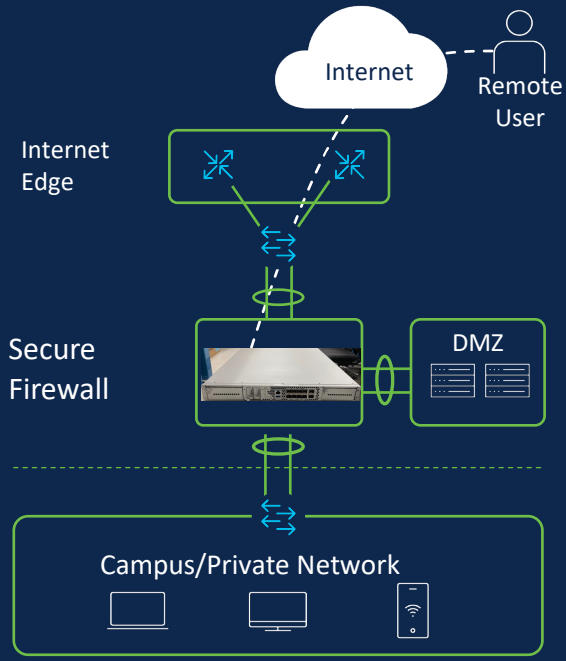
High event scale with long term storage

- External event storage at massive scale (100K eps), in cloud or on-premise
- Firewall Management Center (FMC) can be in cloud or on-premise
- ML-powered behavioral and flow analysis available on events
- Based on Secure Network Analytics (Stealthwatch) technology



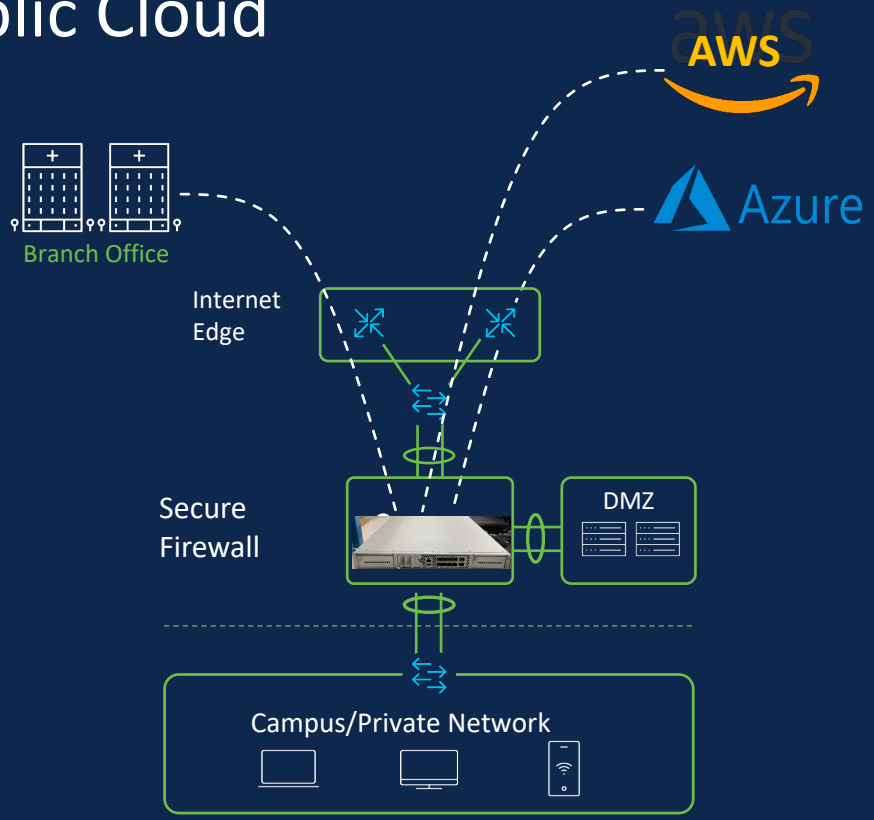
Use Case: Securing Hybrid Workers

- Hardware architecture designed to accelerate TLS/DTLS decryption
- Can support high volume RA VPN traffic
- Up to 30000 simultaneous VPN client connections
- Can load balance between multiple 4200s
- Dynamic profile, posture and policy assessment
- Continuous Trusted Access
- Best of breed threat protection, Snort 3, & Talos
- Unified security client services (VPN, threat defense, NVM, SSE, posture)

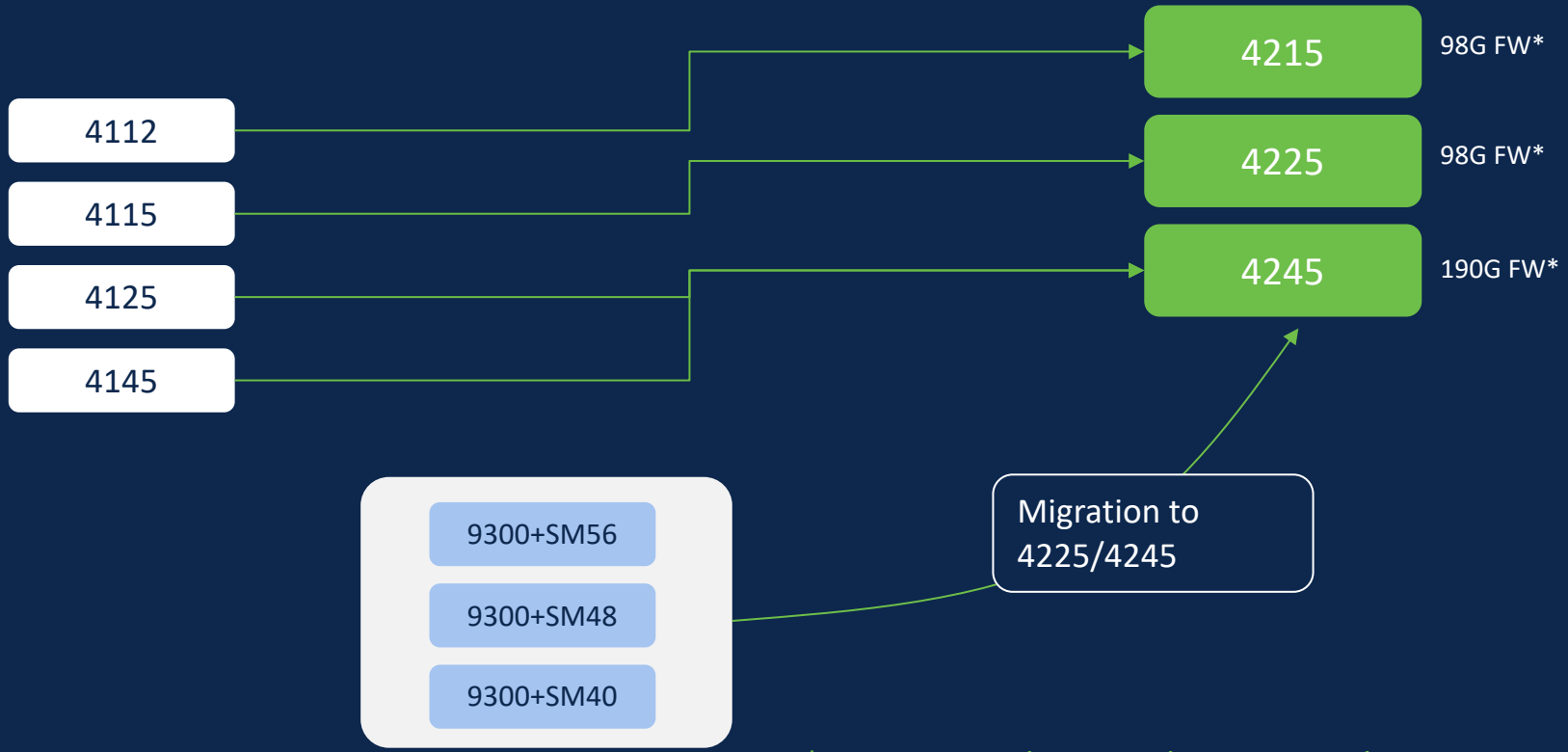


Use Case: Branch Offices or Public Cloud

- Hardware architecture designed to accelerate IPsec decryption
- Can support high volume site-to-site VPN traffic
- Create thick pipes to branch offices, public cloud, and other remote datacenters
  - 4115 – up to 50.6 Gbps
  - 4225 – up to 85.5 Gbps
  - 4245 – up to 148.3 Gbps
  - On Cisco Secure Firewall ASA, can be scaled much higher by clustering
  - On Cisco Secure Firewall FTD, can be scaled using Nexus ITD



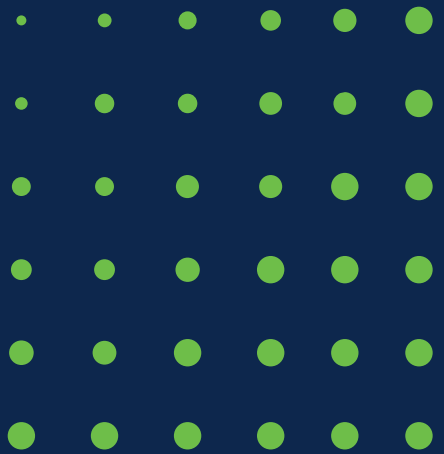
Proposed Portfolio Migration Overview



*__NOTE__: ASA only@1500-byte UDP packet

Hardware Architecture

Engineered to Provide Security



Chassis

Dimensions 1.73” Height
(1 RU) 19" Wide, 32" Deep

Fixed Front Panel

1. 1 USB 3.0, Type A connector
2. 2x1/10G Management Port
3. Qty 8 1/10/25 G SFP28 data ports
4. 1 RJ45 console port
5. Qty 2 slots for SSD :
   - ✓ 1.8TB each, 3.6TB System
   - ✓ Optional SW RAID1

Front Panel

6 2 Netmod Slots

- Hot swappable
- Different bandwidth Netmods
  - ✓ 1G, 10G, 25G, 40G,100G, 200G, 400G (Coming)
  - ✓ Fail to wire, standard

Back Panel

7 Power Supply

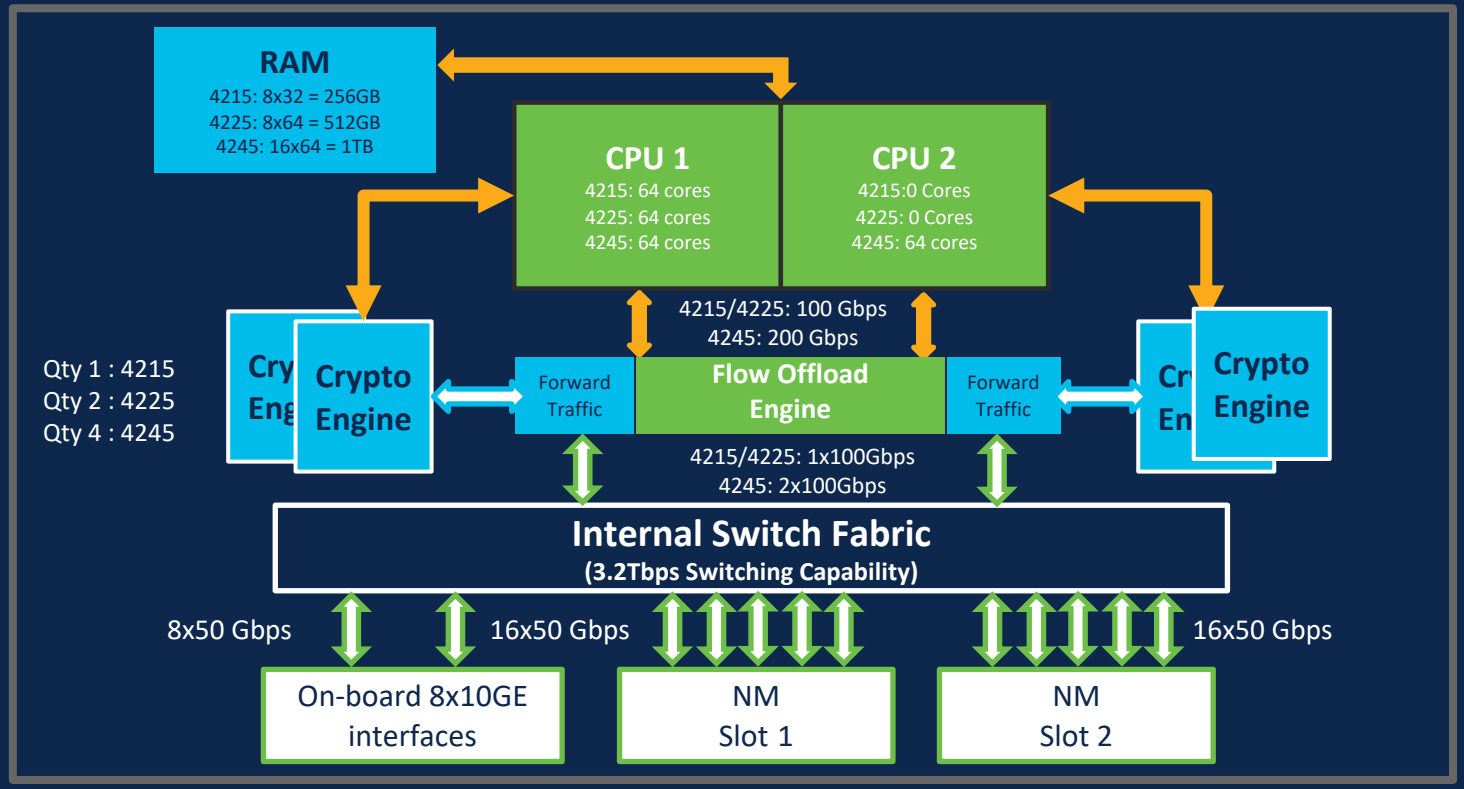
- Qty 2 AC Hot swappable Power Modules
- 1+1 Power Redundancy
  - 1900 W AC

8 Fan Modules

- Rear accessible, Hot swappable Fan Modules
- ~2 Mins support for Fan module replacement

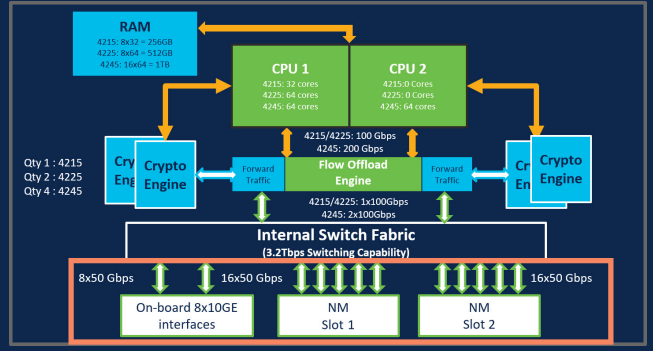
cisco SECURE

High-Level Hardware Architecture

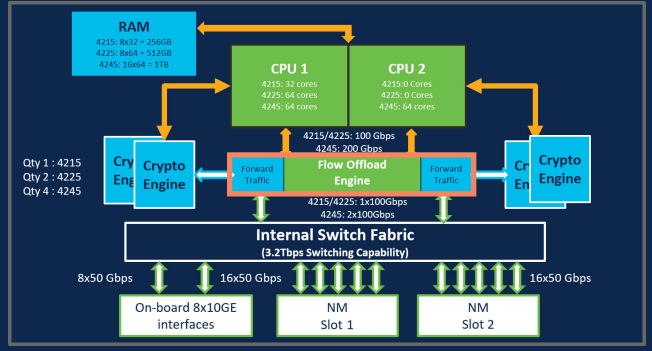


Flexible Interface Architecture

- 2 x 1/10/25 G Management Port
- 8 x built in 1/10/25 G SFP28 data ports
- 2 x netmod slots
  - Hot swappable
  - 1G, 10G, 25G, 40G,100G, 200G, 400G (Coming)
  - Fail to wire, standard
  - See the Network Modules section of this document for further discussion.

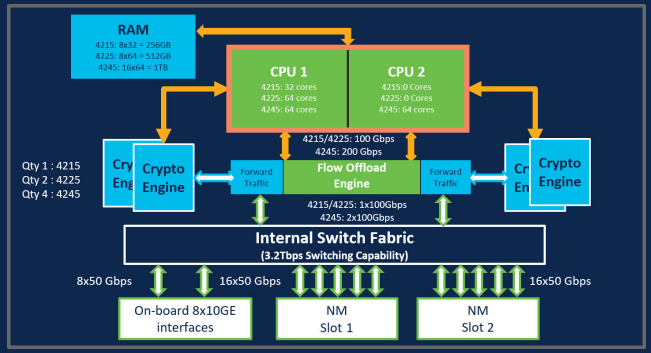


High Performance Packet Processing
Flow Offload and Dynamic Flow Offload

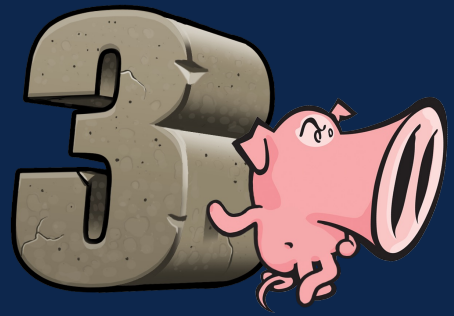


- All 4200s include specialized hardware capable of stateful flow processing up through layer 4
  - Flow does not need to transit the system bus or engage the CPU complex
  - Flow offload engine supports up to 32M concurrent flows for IPv4 and 12M for IPv6
  - Example: the 4245 can do up to 125Gbps in a single TCP flow
- Static flow offload
  - Trusted flows can be specified by the administrator (using prefilter policies for FTD or service-policy for ASA)
- Dynamic flow offload
  - Snort deep packet inspection does not always require to inspection of the entire flow
  - Flows can be dynamically offloaded once inspection is completed

Threat Protection Provided by Snort



- Threat protection is provided by Snort 3
- Snort 3 features include
  - Elephant Flow detection/throttle/bypass
  - Rearchitected port scan detection & blocking
  - Improved SMB support (v3, multi-channel)
  - Support for HTTP/2 and QUIC protocols
- In the 4200 series, a powerful CPU complex provides Snort with the horsepower for high performance deep packet inspection
  - 4215/4225 – 64 physical core CPU
  - 4245 – 2 X 64 physical core CPUs
  - A single source process utilize multiple cores



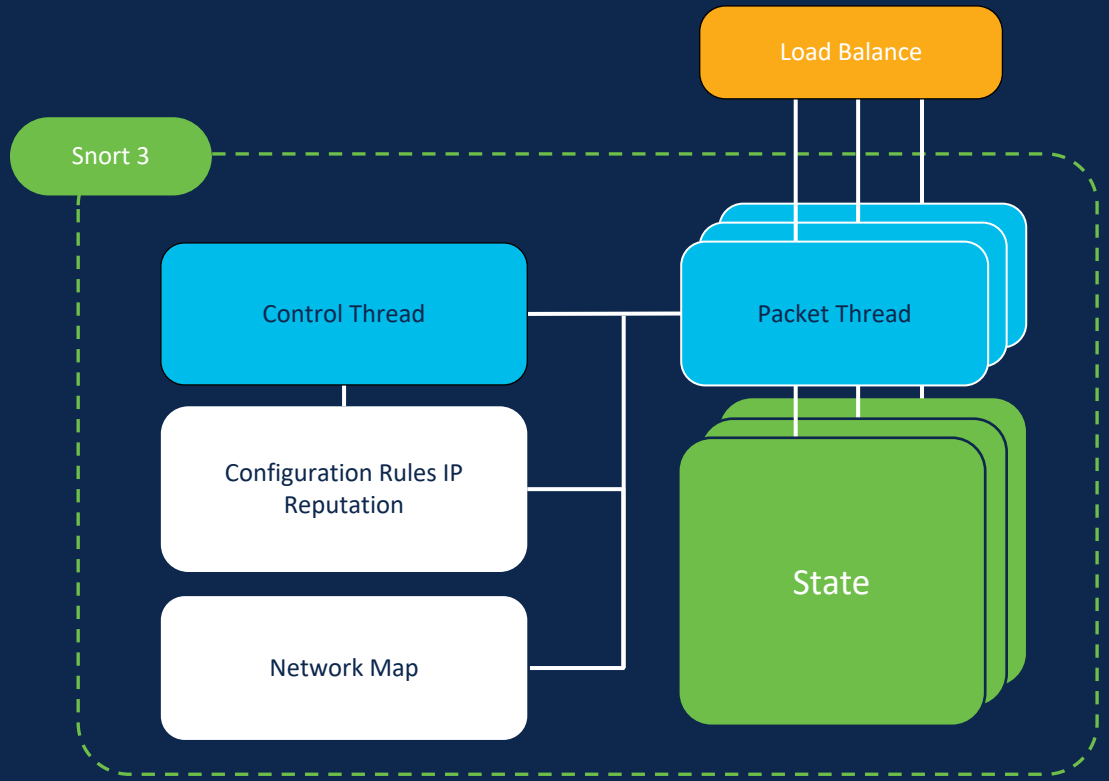
Snort 3 Architecture

Designed to take advantage of multi-processor architecture

- A single Snort process
- Dedicated core for control thread
- Most of the other cores are available for data processing thread

One copy of config and network map:

- Uses less memory
- Supports more IPS rules and larger network map than Snort 2



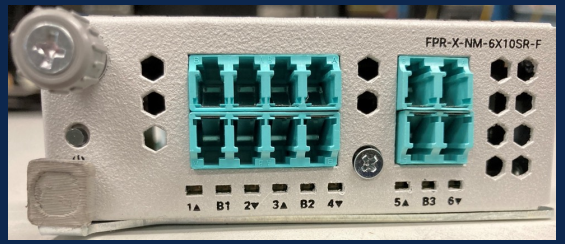
Bump-in-the-Wire Dedicated IPS/IDS

4200 supports inline pairs

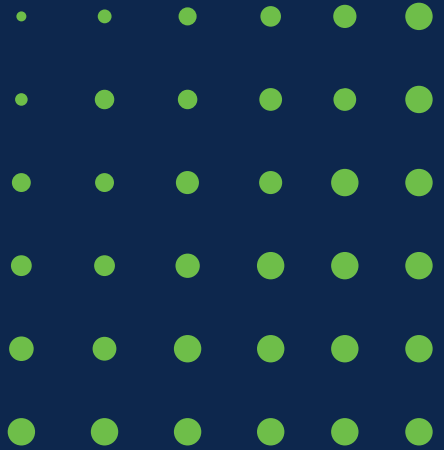
- Inline pairs can be aggregated to form inline sets to boost IPS/IDS throughput

Inline pairs can use any data ports

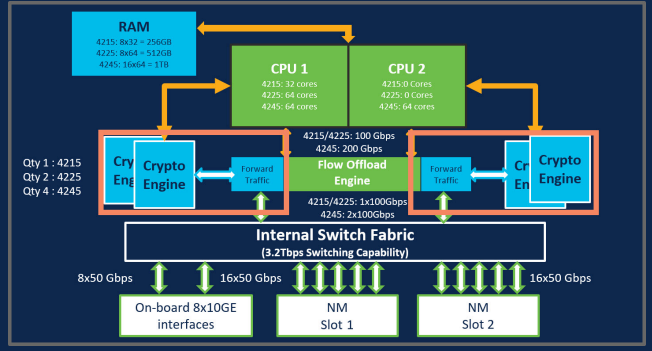
- Build in data interfaces
- All supported network modules
- Special fail-to-wire netmods
  - Provide fault tolerance across device failure
  - See the Network Modules section of this document for further discussion.



Encrypted Traffic Visibility



Hardware Crypto Acceleration

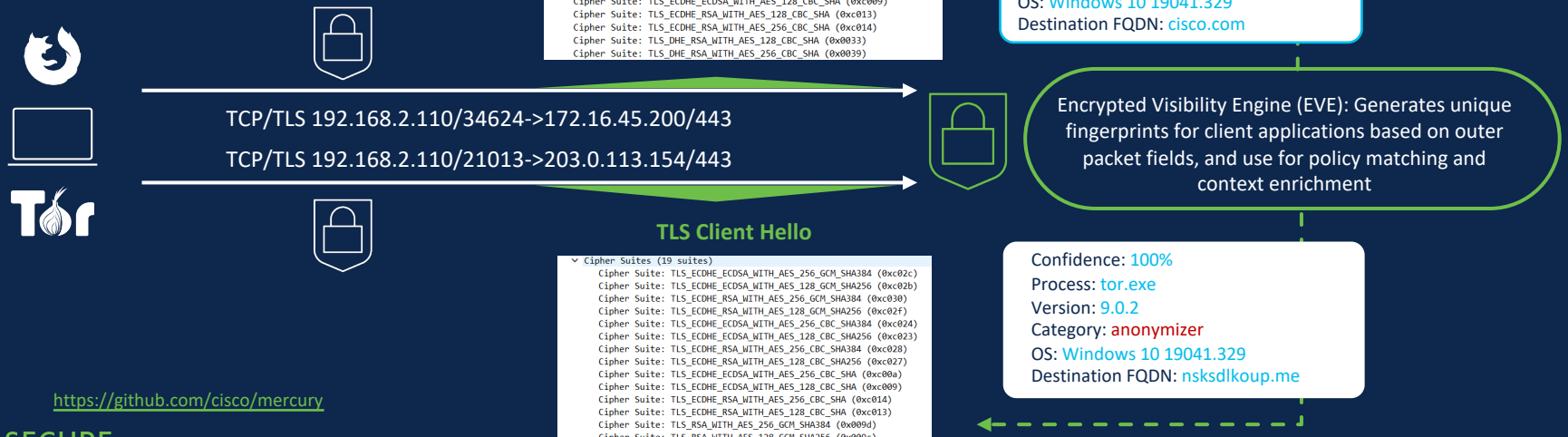


- Hardware Crypto Accelerator chips can perform IPsec Encryption/Decryption in hardware
  - 4215 – Nitrox V
  - 4225 – 2 x Nitrox V
  - 4245 – 4 x Nitrox V
- Dedicate inter-chip links between the crypto acceleration chip and the flow offload engine
  - Allows traffic to be decrypted and encrypted without adding traffic to the system bus.
- 4200 series includes support for full-stack TLS decryption including TLS 1.3

Encrypted Visibility Engine

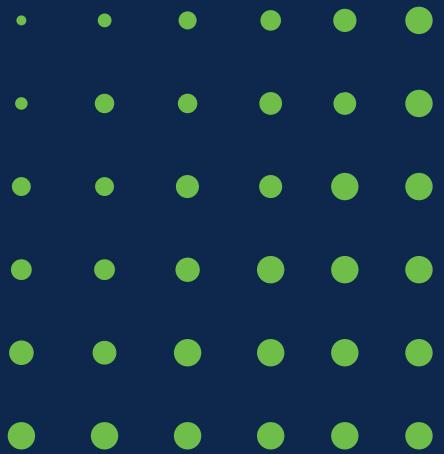
Visibility for TLS & QUIC traffic without Decryption

- Without decryption, using AI/ML can identify applications & URL category
- Can identify malicious applications
- Preserves privacy & compliances
- Maintains firewall performance



https://github.com/cisco/mercury

Network Modules



2x100 Gbps Network Module Overview

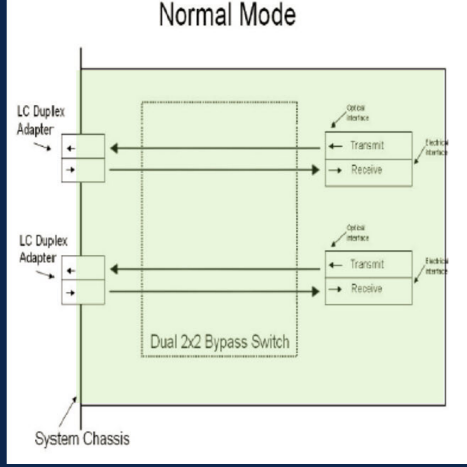
- Hot pluggable 2X40/100G QSFP/QSFP28 netmod
- Supports port breakout modes (4x10/25G)
- Supports MACsec with 256-bit key at all supported speeds
- Ethernet data transferred to/from the netmod over 8 SERDES lanes
- Maximum bandwidth supported by the HW is 200 Gbps full duplex
- Control interface is one lane of PCIe

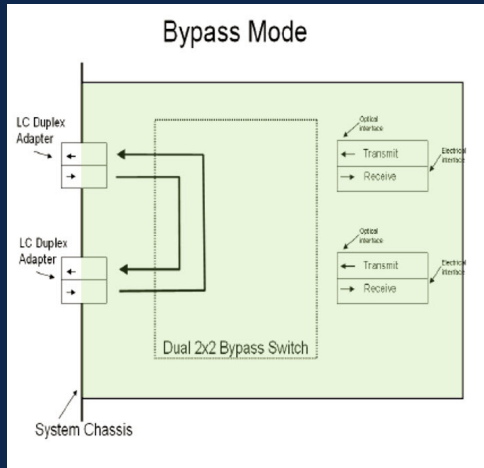
4x200 Gbps Network Module Overview

- Hot pluggable 4x40/100/200G QSFP/QSFP28/QSFP56 netmod
- Supports port breakout modes (4x10/25/50G)
- Supports MACsec with 256-bit key at all supported speeds
- Ethernet data transferred to/from the netmod over 16 SERDES lanes
- Maximum bandwidth supported by the HW is 800 Gbps full duplex
- Control interface is one lane of PCIe

Fail-To-Wire Optical Switch

- Main component: opto-mechanical fiberoptic 2x2 bypass switch
- Connects optical channels by redirecting incoming optical signals into selected output fibers.
- Opto-mechanical configuration and activated via an electrical control signal
- Latching operation preserves the selected optical path after the drive signal has been removed or in the event of power failure.
- Electrical position sensors available to SW via the FPGA registers





Copper Fail-To-Wire Netmod Architecture

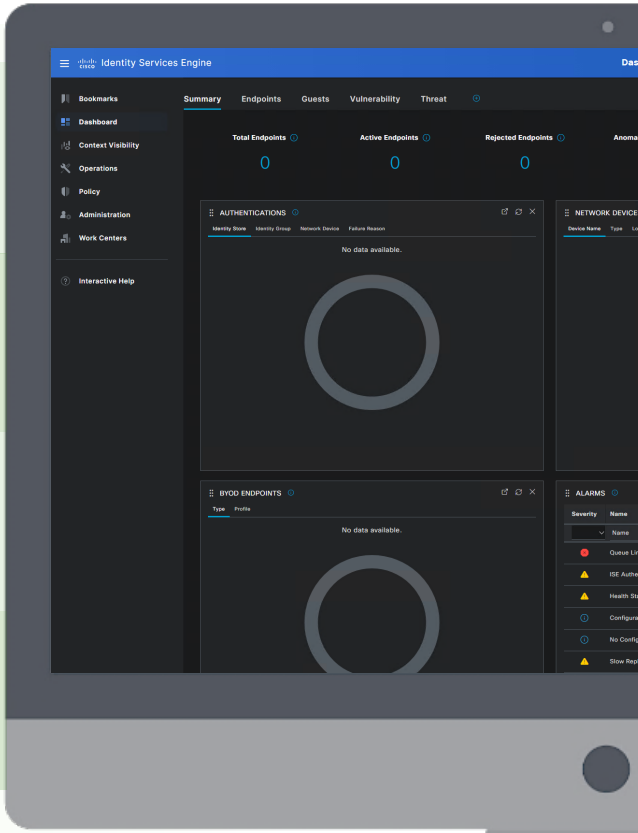
- Main component: relays on the daughter card
- Relay device connects copper channels by redirecting incoming electrical signal to the corresponding port within the port-pair
- Achieved using an electro-mechanical configuration and activated via an electrical control signal
- Each port supports 10/100/1000Base-T data rates.
- The front panel ports are 1000Base-T with RJ45 supporting 100m Cat5 cable (or equivalent) when in non-bypass mode
- Supports FW field upgrade (FPGA and power sequencer)

Agenda

- ISE update / SNS 3700

ISE 3.3 Release Highlights (Release Date: 10-Jul-2023)

Navigation Improvements	NEW Split Upgrade Process	ISE Ciphers Control	Controlled Restart after Admin Certificate Renewal
API Support for LDAP	pxGrid Direct visibility enhancements	pxGrid Context-In Enhancement	Posture for ARM64-based endpoints
Use Wi-Fi Edge Analytics data for ISE profiling	IPv6 Support (Guest Portal, Posture, Profiling)	IPv6 Support for Agentless Posture	Machine Learning Based Profiling
	Multi-Factor Classification (MFC) on ISE	Custom Attribute Reprofiling Trigger	



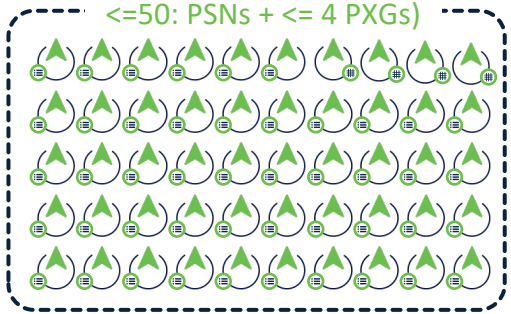
ISE Deployment Scale

cs.co/ise-scale

2.6+

Same for physical, virtual, & cloud instances

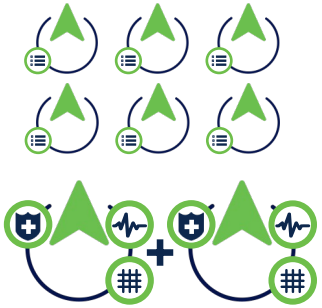
Compatible with load balancers



Lab and Evaluation

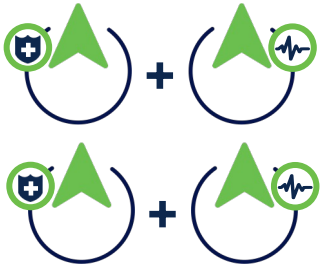
Small HA Deployment

2 x (PAN+MNT+PSN)



Medium Multi-node Deployment

2 x (PAN+MNT+PXG), <= 6 PSN



Large Deployment

2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

100 Endpoints	Up to 50,000 Endpoints	Up to 2,000,000 Endpoints	3600
100 Endpoints	Up to 100,000 Endpoints	Up to 2,000,000 Endpoints	3700

ISE Nodes – Mix and Match

Physical Appliances	Virtual Machines	Cloud Instances

SNS-3795
SNS-3755
SNS-3715
SNS-3695
SNS-3655
SNS-3615
SNS-3595

KVM

Microsoft

NUTANIX

vmware

aws

Azure

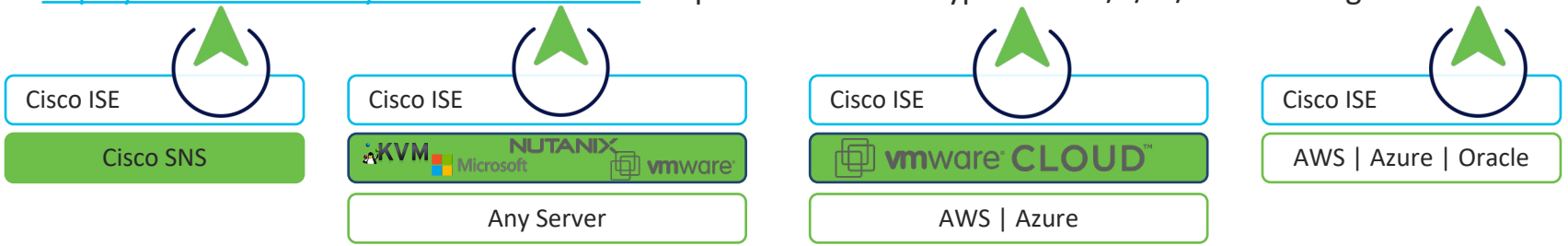
ORACLE

Future

Google

ISE 3.3 Supported Platforms

See Deploy Cisco ISE Natively on Cloud Platforms for provider instance types and XS/S/M/L node sizing



Appliances	Standalone Sessions	PSN Sessions	Processor	Cores	Memory	Disk	RAID	Network Interfaces
SNS-3615	12,500	25,000	1 – Intel Xeon 2.10 GHz 4110	8	32 GB (2 x 16 GB)	1 (600GB)	No	2x10Gbase-T 4x1GBase-T
SNS-3655	25,000	50,000	1 – Intel Xeon 2.10 GHz 4116	12	96 GB (6 x 16 GB)	4 (600 GB)	10	2x10Gbase-T 4x1GBase-T
SNS-3695	25,000	50,000	1 – Intel Xeon 2.10 GHz 4116	12	256 GB (8 x 32 GB)	8 (600 GB)	10	2x10Gbase-T 4x1GBase-T
SNS-3715	25,000	50,000	1 – Intel Xeon 2.10 GHz 4310	12	32 GB (2 x 16 GB)	1 (600GB) HD or 1 (800GB) SSD or 1 (960GB) SED	No	2x10Gbase-T 4x10GE SFP
SNS-3755	50,000	100,000	1 – Intel Xeon 2.30 GHz 4316	20	96 GB (6 x 16 GB)	4 (600GB) HD or 4 (800GB) SSD or 4 (960GB) SED	10	2x10Gbase-T 4x10GE SFP
SNS-3795	50,000	100,000	1 – Intel Xeon 2.30 GHz 4316	20	256 GB (8 x 32 GB)	8 (600GB) HD or 8 (800GB) SSD or 8 (960GB) SED	10	2x10Gbase-T 4x10GE SFP

EoL/EoS 8/2023

PSN

PSN

* SNS-3595 no longer supported with ISE 3.3
* VMWare version 6.7+ required


cisco
SECURE