



The bridge to possible

Cisco ISE Performance, Scalability and Best Practices

Pavan Gupta, Technical Marketing Engineer
BRKSEC-2091

CISCO *Live!*

#CiscoLive

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 speaker until June 7, 2024.

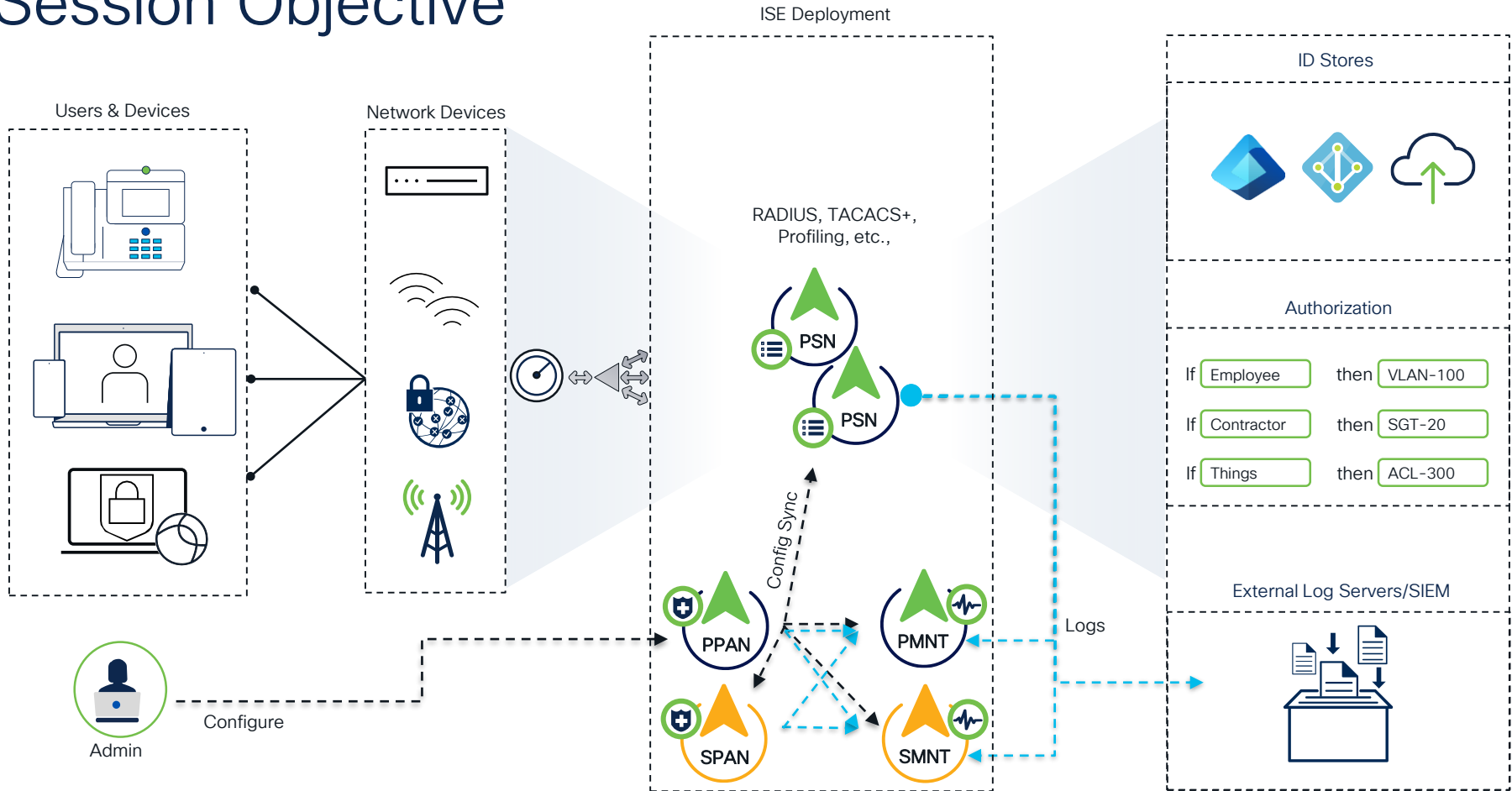




Agenda

- Session Objective & Overview
- Best Practices
 - ISE Deployment Options
 - ISE VM Profiles
 - ISE Personas
 - Latency
 - Certificates
 - Policy Optimization
- Users & Devices Considerations
- Network Devices Best Practices
 - Optimization
 - Accounting
 - Load Balancers

Session Objective



Session Abstract

The first step for Zero Trust is to secure the access given to users, devices including IoT. On top of it, we can then talk about applications and workloads. Cisco ISE plays a significant role in providing access control to the devices connecting over Wired, Wireless, VPN and 5G networks. This session illustrates how to start from design, scale the highly available MAB, Dot1x, Guest & Profiling services over the different mediums.

Security and Network Engineers gain insights into methodologies to consider with and without load balancers in your network, optimize and scale the environment following the best practices.

A Word About Myself



- 14+ years of experience in Network & Security
- Different Roles in ISE Team
- 4+ years in TME Role

Pavan Gupta

Zero Trust

- Never assume trust
- Always verify
- Enforce least privilege
- Reaffirm when trust changes

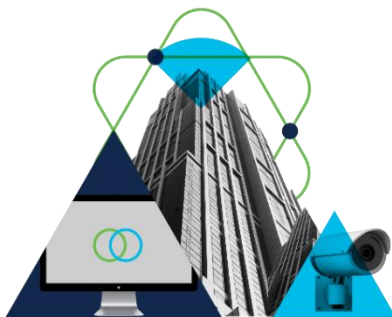
Cisco Secure Zero Trust

A comprehensive approach to securing all access across your people, applications, and environments.



Workforce

Ensure only the right users and secure devices can access applications.



Workplace

Secure all user and device connections across your network, including IoT.







Workloads

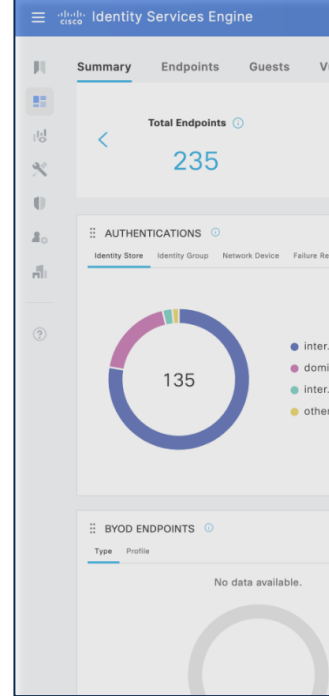
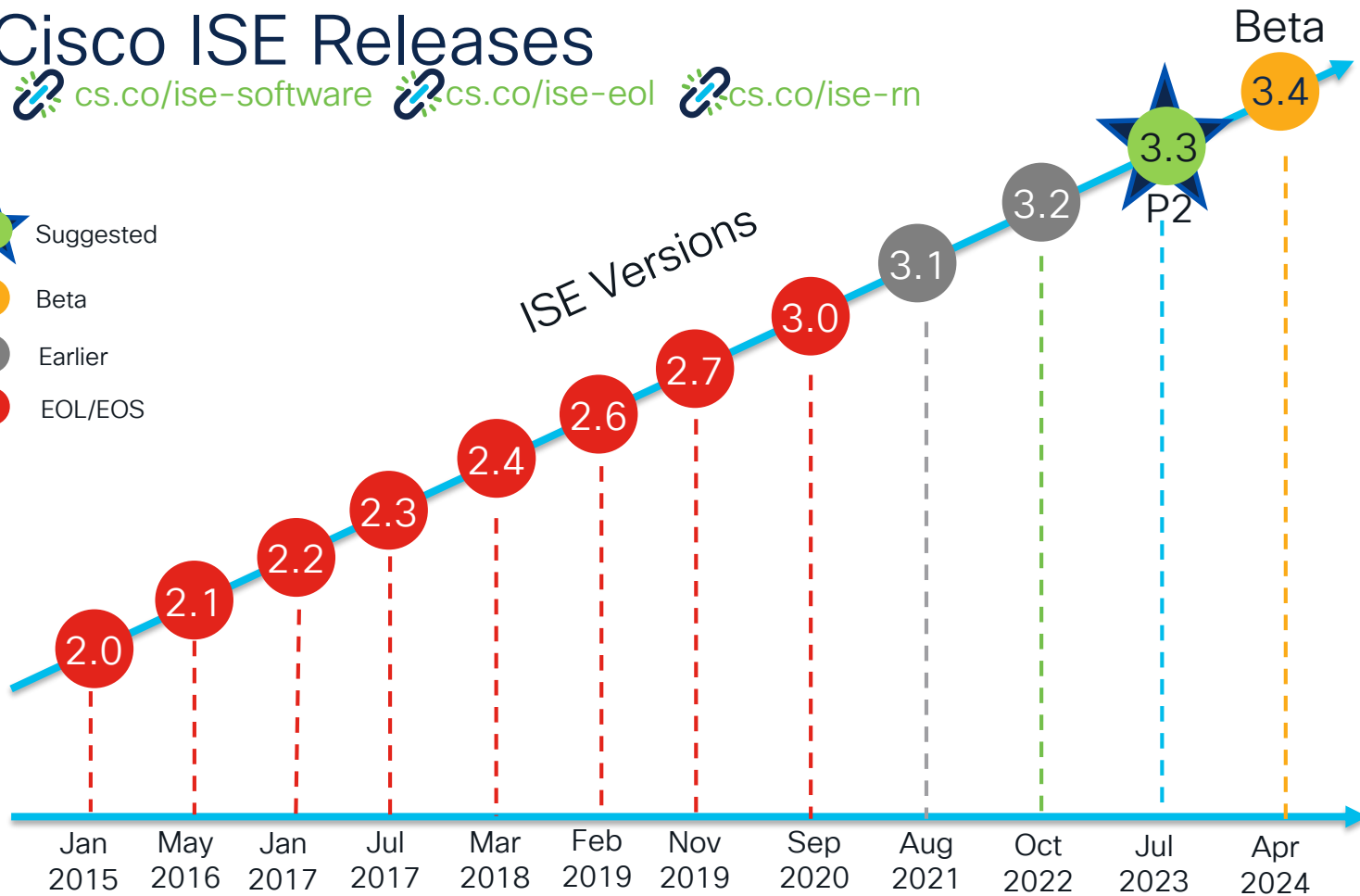
Secure all connections within your apps, across multi-cloud.

Cisco ISE Releases

 cs.co/ise-software  cs.co/ise-eol  cs.co/ise-rn

-  Suggested
-  Beta
-  Earlier
-  EOL/EOS

ISE Versions



Why ISE?



Enhanced UX



ISE 3.X UI navigation and UX was revamped. The Navigation is aligned with other Cisco products to give same kind of experience across all Cisco products.

Device Administration



TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices

Secure Access



Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use **RADIUS** with **802.1X**, **MAB**, **Easy Connect**, or **Passive ID**

Guest Access



Differentiate between **Corporate** and **Guest** users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options

Asset Visibility



Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with **Device Profiling**. Automate access for many different IoT devices

Compliance & Posture



Use **agentless posture**, **AnyConnect**, **MDM**, or **EMM** to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access

Context Exchange



pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase **Network Visibility** and facilitate automated Enforcement.

Segmentation



Group-based Policy allows for segmentation of the network through the use of Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation.

Cisco SDA/DNAC



ISE integrates with **DNA Center** to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)

BYOD



Allow **employees** to use **their own devices** to access network resources by registering their device and downloading certificates for authentication through a simple **onboarding** process

Threat Containment



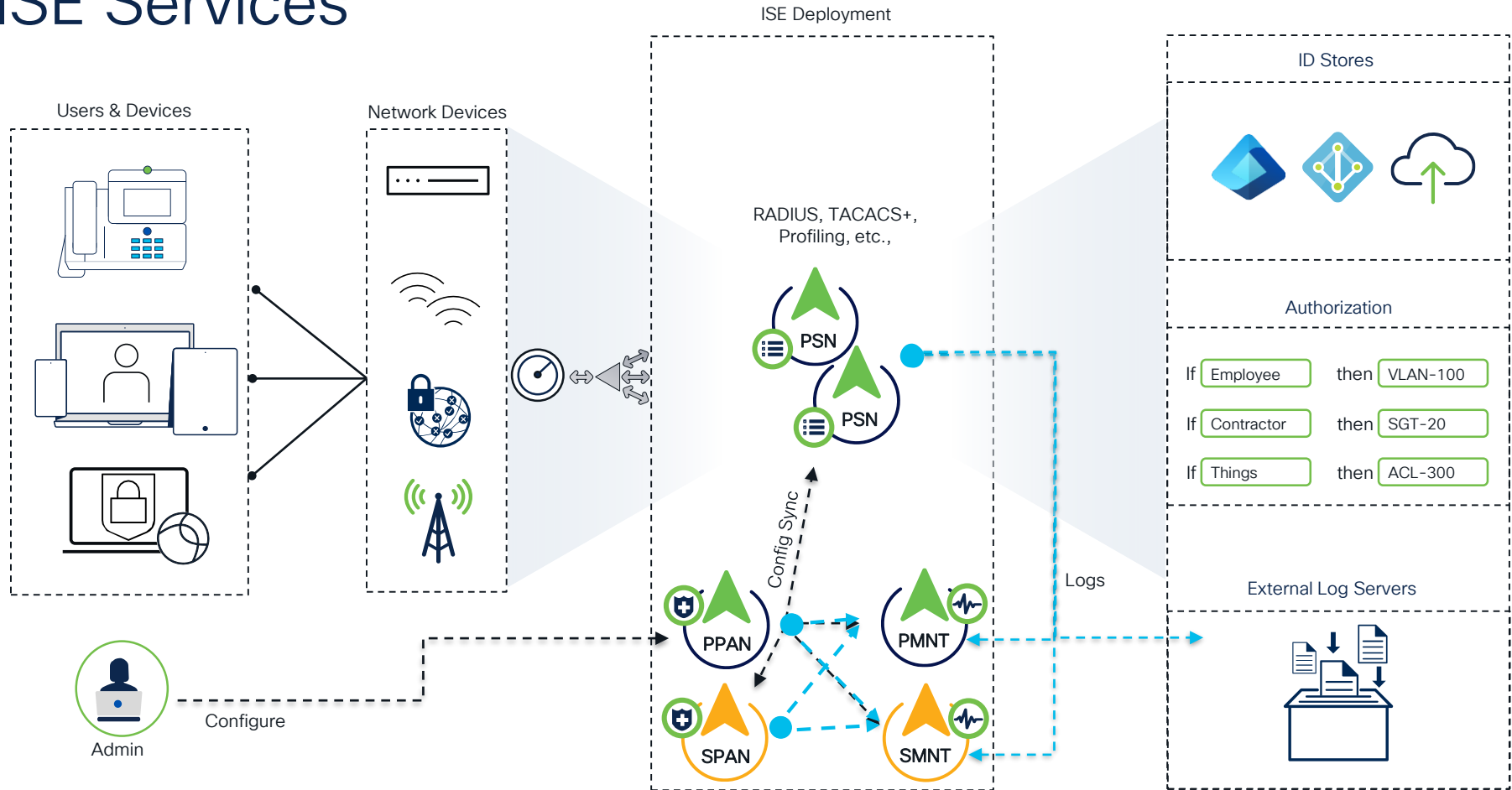
Using a **Threat Analysis tool**, such as Cisco Cognitive **Threat Analytics**, to grade an endpoints threat score and allow network access based upon the results

Enhanced Reporting

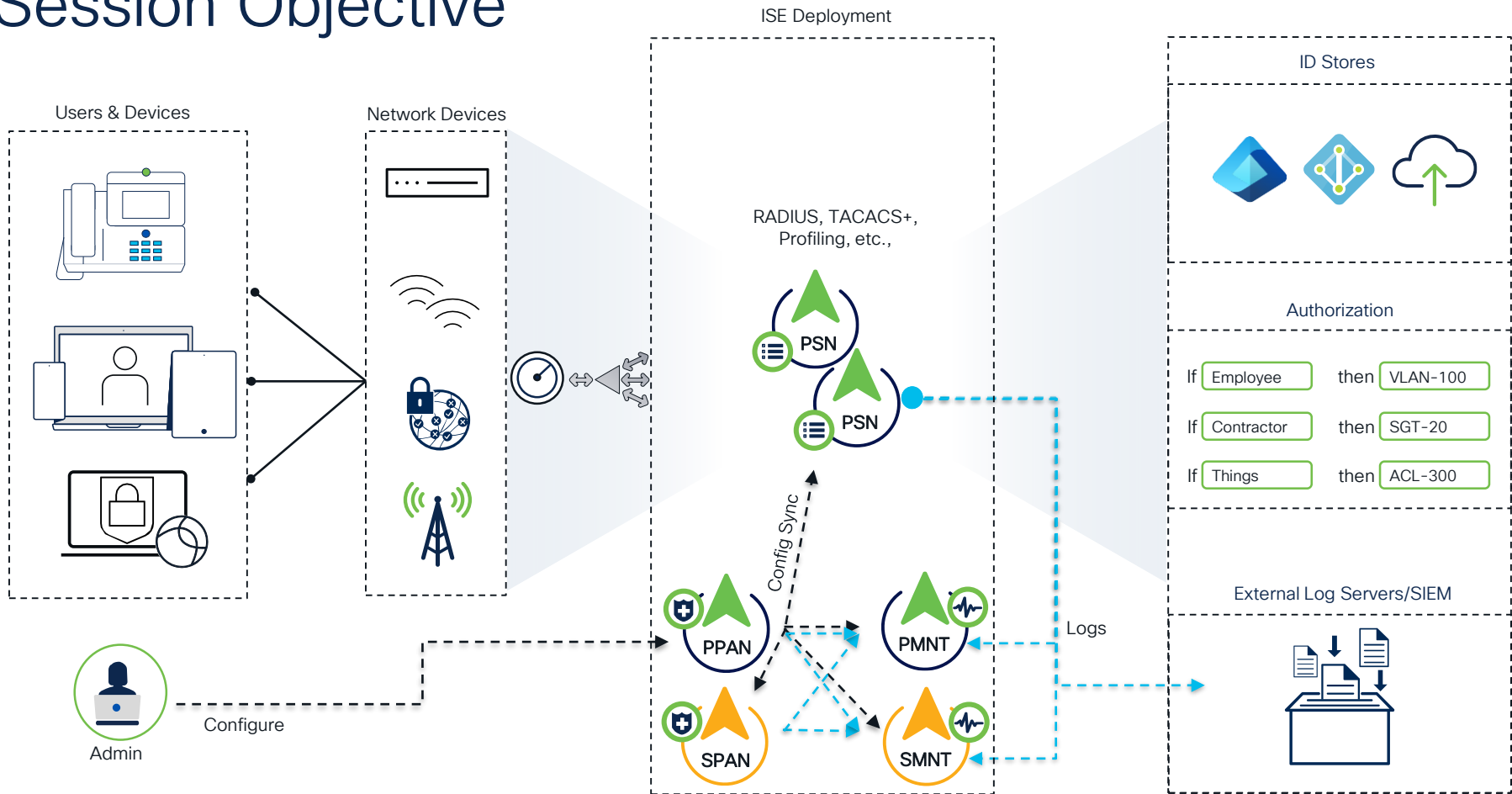


Finally, ISE **provides enhanced reporting** capabilities inhouse for better operations and reporting purposes. Cisco ISE provides you log analytics and infrastructure monitoring and connecting to operational DB and create your dashboards

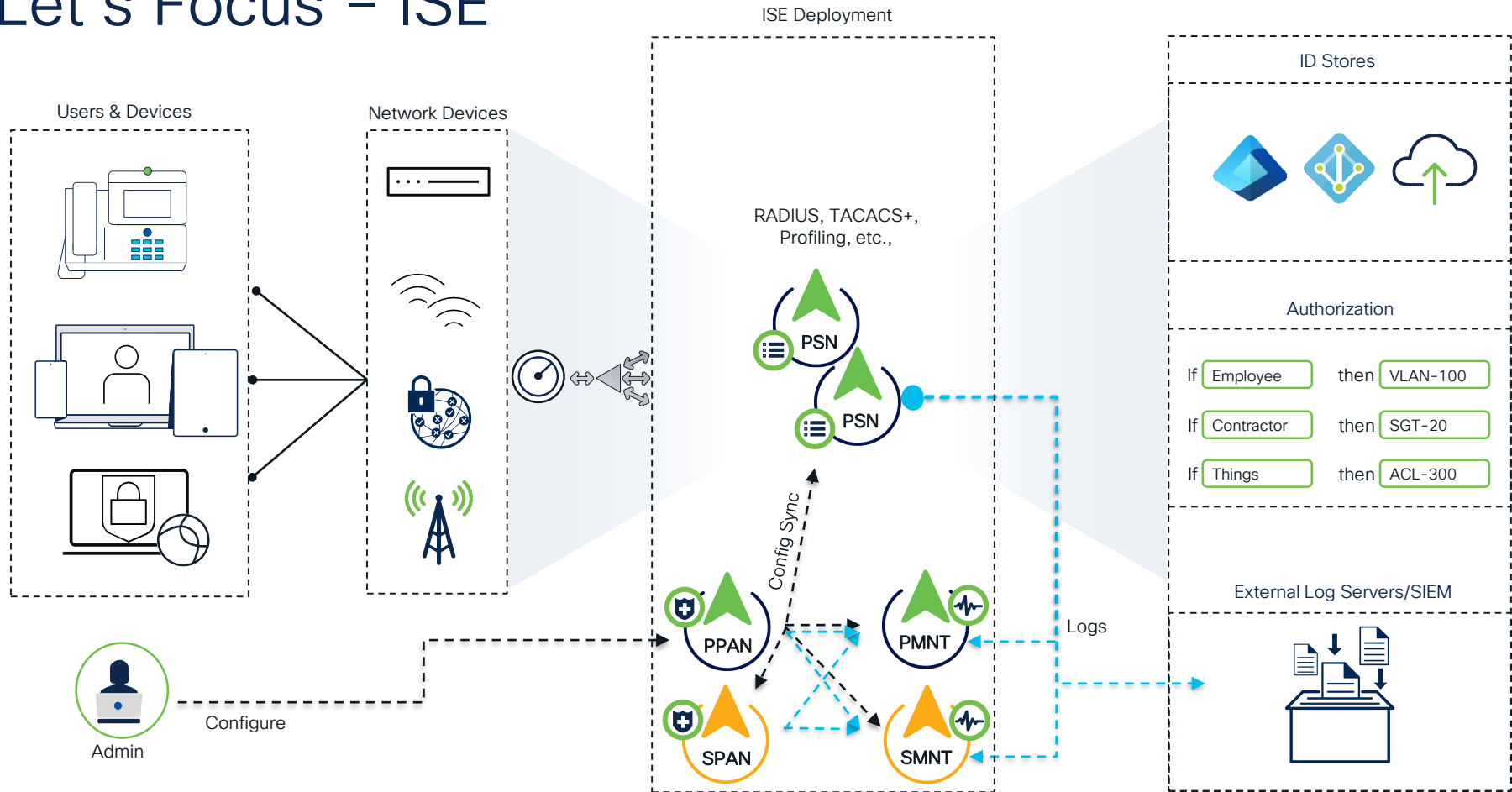
ISE Services



Session Objective



Let's Focus – ISE



- Cisco ISE
 - Supported Platforms
 - Deployment Options
 - Latency amongst nodes - Guidance
 - ISE Node Profiles - Best Practices
 - Scenario Specific Performance
 - Certificates - Recommendations
 - Policies - Best Practices
 - RADIUS & TACACS+ Performances



Cisco ISE Deployment

Supported Platforms



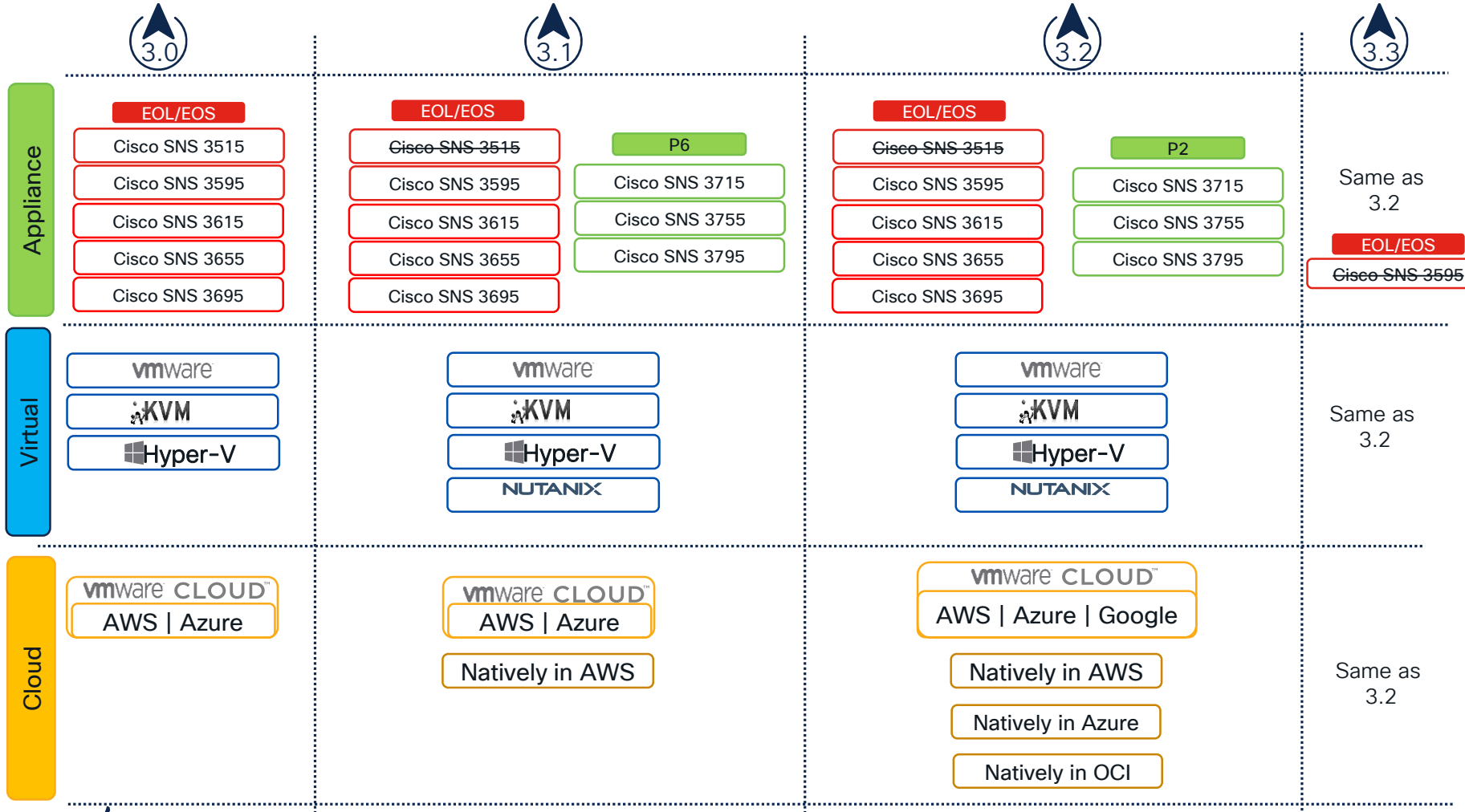
slido



which Cisco ISE Node
Profiles do you use

① Start presenting to display the poll results on this slide.

ISE 3.X Platforms - At Glance



slido



Which platforms did you
deploy Cisco ISE on?

① Start presenting to display the poll results on this slide.

Cisco ISE Node Profiles

Recommendations



Cisco ISE Node Profiles

Models	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3695	Cisco SNS 3715	Cisco SNS 3755	Cisco SNS 3795
VM Specification	16vCPU 32 GB	16vCPU 64 GB	24vCPU 96 GB	24vCPU 256 GB	24vCPU 32GB	40vCPU 96GB	40vCPU 256GB
AWS	c5.4xlarge*	m5.4xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	m5.16xlarge
Azure	Standard_F16s _v2*	Standard_D16s _v4	Standard_F32s _v2* Standard_D32s _v4	Standard_D64s _v4	Standard_F32s _v2* Standard_D32s _v4	Standard_D64s _v4	Standard_D64s _v4
OCI	Optimized3.Flex x* (8 OCPU** and 32 GB)	Standard3.Flex (8 OCPU and 64 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 256 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (32 OCPU and 256 GB)

*This instance is compute-optimized and provides better performance compared to the general-purpose instances.

- Internal Resources Allocated:

- Java Heap Sizes
 - Oracle Memory Sizes
 - Thread Pool Sizes
 - Max Sessions
 - Etc...
- Virtual appliances mapped to physical profiles

Example:

What we check:

#Active profile properties [profile = sns3615, persona = pap_mnt]

Profile differences:

*<sns3615>.tomcat.runtimeThreadPool.maxThreads=200
<sns3755>.tomcat.runtimeThreadPool.maxThreads=300*

Persona differences:

*<sns3615>.oracle.pga=1200
<sns3615>.<mnt>.oracle.pga=2400*

ISE VM Recommendations

- Applies to all virtual platforms – VMWare, KVM, Hyper-V, AHV
- Reserve 100% of CPU and Memory
- Use thick provisioning of disk.
- Do not set resource limits.
- No Snapshots
- Hot vMotion is supported, however,

safe to use
cold vMotion after shutting down the node.

> CPU *	12	▼
▼ Memory *	16384	MB ▼
Reservation	16384	MB ▼
	<input checked="" type="checkbox"/> Reserve all guest memory (All locked)	
Limit	Unlimited	▼ MB ▼
Shares	Normal ▼	163840
Memory Hot Plug	<input type="checkbox"/> Enable	
> Hard disk 1	200	GB ▼
> SCSI controller 0	VMware Paravirtual	
> Network adapter 1	VLAN_200 ▼	
> Network adapter 2	VLAN_200 ▼	

How to find your VM profile

Export Summary

My Reports >

Reports ▾

Audit >

Device Administration >

Diagnostics ▾

AAA Diagnostics

AD Connector Operations

Endpoint Profile Changes

Health Summary

ISE Counters

Key Performance Metrics

Misconfigured NAS

Misconfigured Supplicants

Network Device Session S...

OCSP Monitoring

RADIUS Errors

System Diagnostic

ISE Counters ⓘ

From 2024-05-27 00:00:00.0 To 2024-05-27 13:49:30.0

Filters: ⓘ

* Server ▾

* Is exactly (or equals) ▾

* isenode21 ▾

* Time Range ▾

* Is exactly (or equals) ▾

* Today ▾

Go

Counter Attribute Threshold

Attribute Name	ISE Profile	Threshold
ARP Cache Insert Update R...	EVALUATION	95000
DHCP Endpoint Detected	EVALUATION	8000
DHCP Skip Profiling	EVALUATION	8000
DNS Reverse Lookup Event...	EVALUATION	10000
DNS Endpoint Detected	EVALUATION	8000
Endpoint Oracle Persist Rec	EVALUATION	9000

ISE Deployment

Personas



ISE Personas

Max 2

Policy Administration Node (PAN)

- Administrative GUI
- Policy configuration
- Policy replication
- Deployment Management
- Configuration REST APIs

Max 2

Monitoring & Troubleshooting Node (MNT)

- Receives logs from all nodes
- Handles remote logging targets
- Generates summary Dashboard Views
- Performs scheduled reports
- Handles reporting and operations



Policy Service Node (PSN)

- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD/CP portals
- MDM/Posture queries
- TC-NAC & SXP services

Platform Exchange Grid Node (PXG)

- Runs pxGrid controller
- Authorizes pxGrid Pubs/Subs
- Publishes pxGrid topics to subscribers
- Handles ANC/EPS requests
- REST APIs

Max 50

Max 4

ISE Deployment

Models



ISE Deployment Scale

No. of Endpoints Support - Deployment Wise

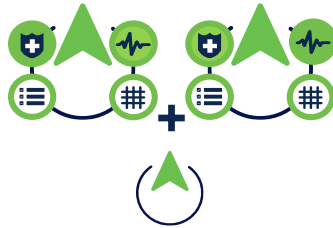
 cs.co/ise-scale

Lab and
Evaluation



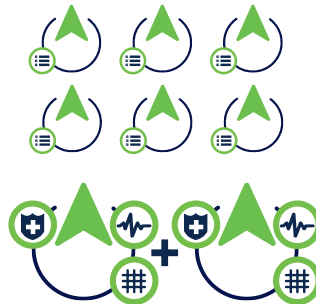
1 x (PAN + MNT + PSN + PXG)

Small



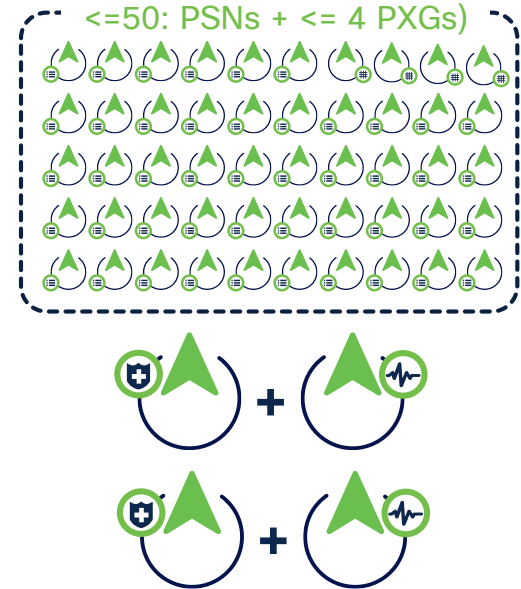
2 x (PAN+MNT+PSN)

Medium



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

Large



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

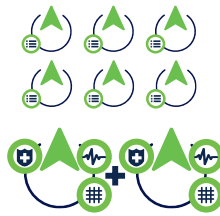
ISE Deployment Scale

 cs.co/ise-scale



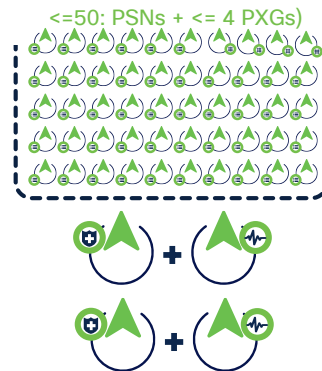
Small

- All Personas on 2 nodes
- Optional 3rd node for:
 - Dedicated PSN/pxGrid/Health Check
 - 3rd node does not increase scale, it is for redundancy and load sharing purposes only!



Medium

- Maximum 8 nodes
- PAN + MnT on same node
- Max 6 dedicated PSNs
- pxGrid can be enabled on max 2 nodes
 - 2 x PAN/MnT/pxGrid + 4 x PSNs + 2 x pxGrid (or)
 - 2 x PAN/MnT/pxGrid + 6 x PSN



Large

- Maximum of 58 nodes
- All personas on dedicated nodes.
- Up to 50 PSNs
- Up to 4 pxGrid nodes
 - 2 x PAN + 2 x MnT + 50 x PSN + 4 x pxGrid

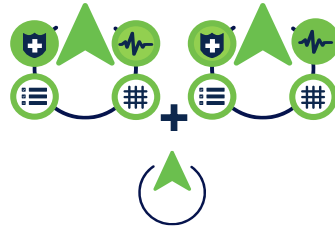
Cisco ISE Deployment

Deployment Scale

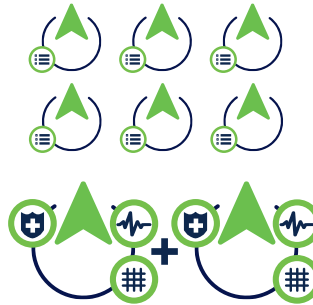


ISE Deployment Scale

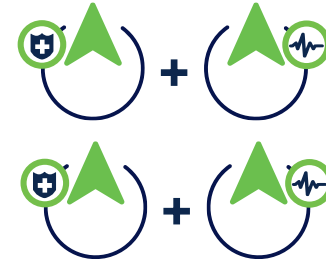
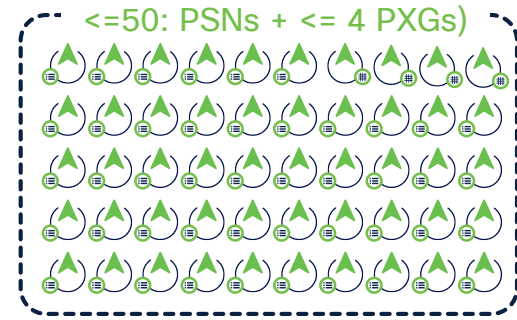
No. of Endpoints Support - Deployment Wise



Small HA Deployment



Medium Deployment



Large Deployment

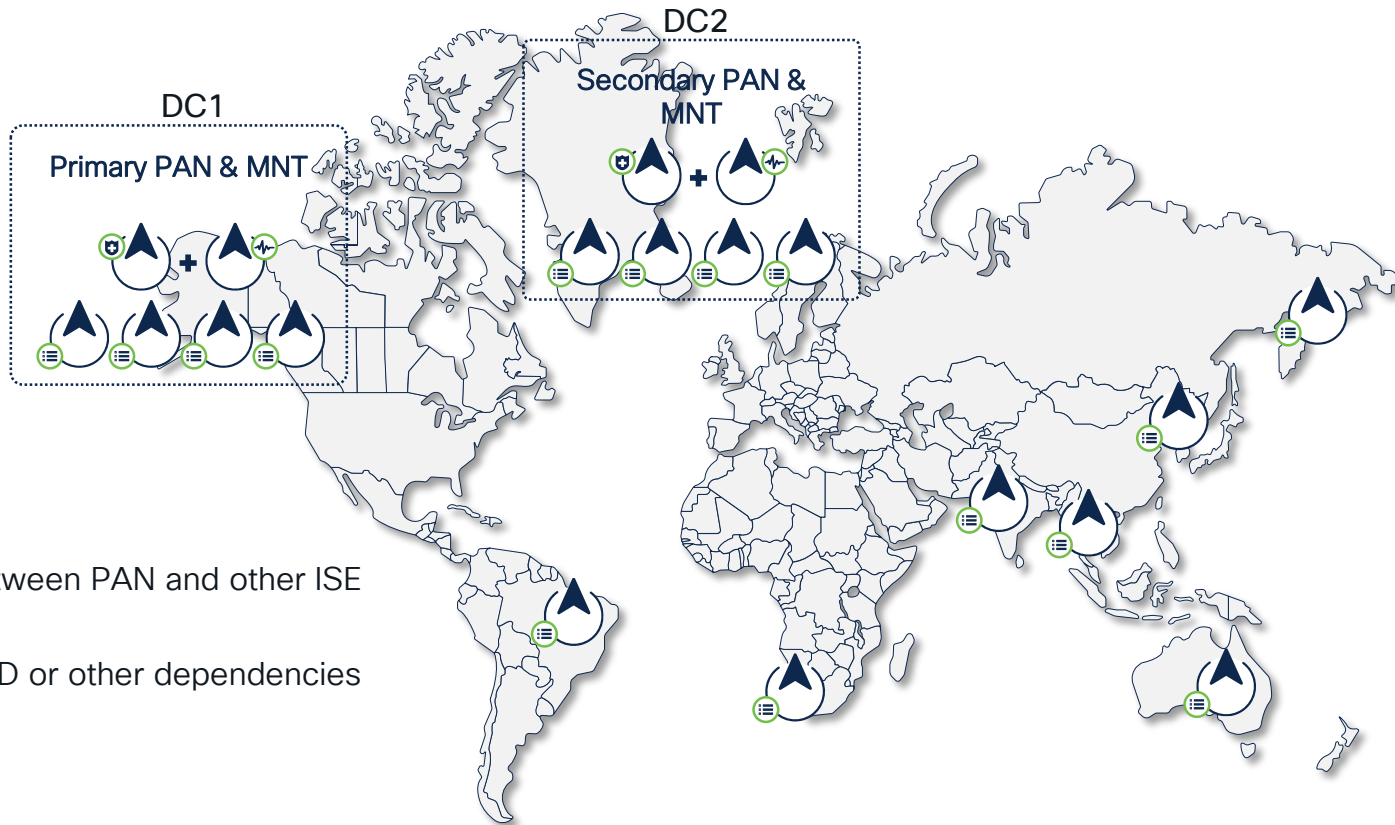
Deployment PAN,MnT,PAN/MnT	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	500,000	Unsupported	Unsupported	500,000	750,000	2,000,000	2,000,000
Medium	20,000	12,500	75,00	25,000	150,000	50,000	150,000
Small	20,000	12,500	25,000	25,000	50,000	50,000	50,000

ISE Deployment

Centralized or Distributed

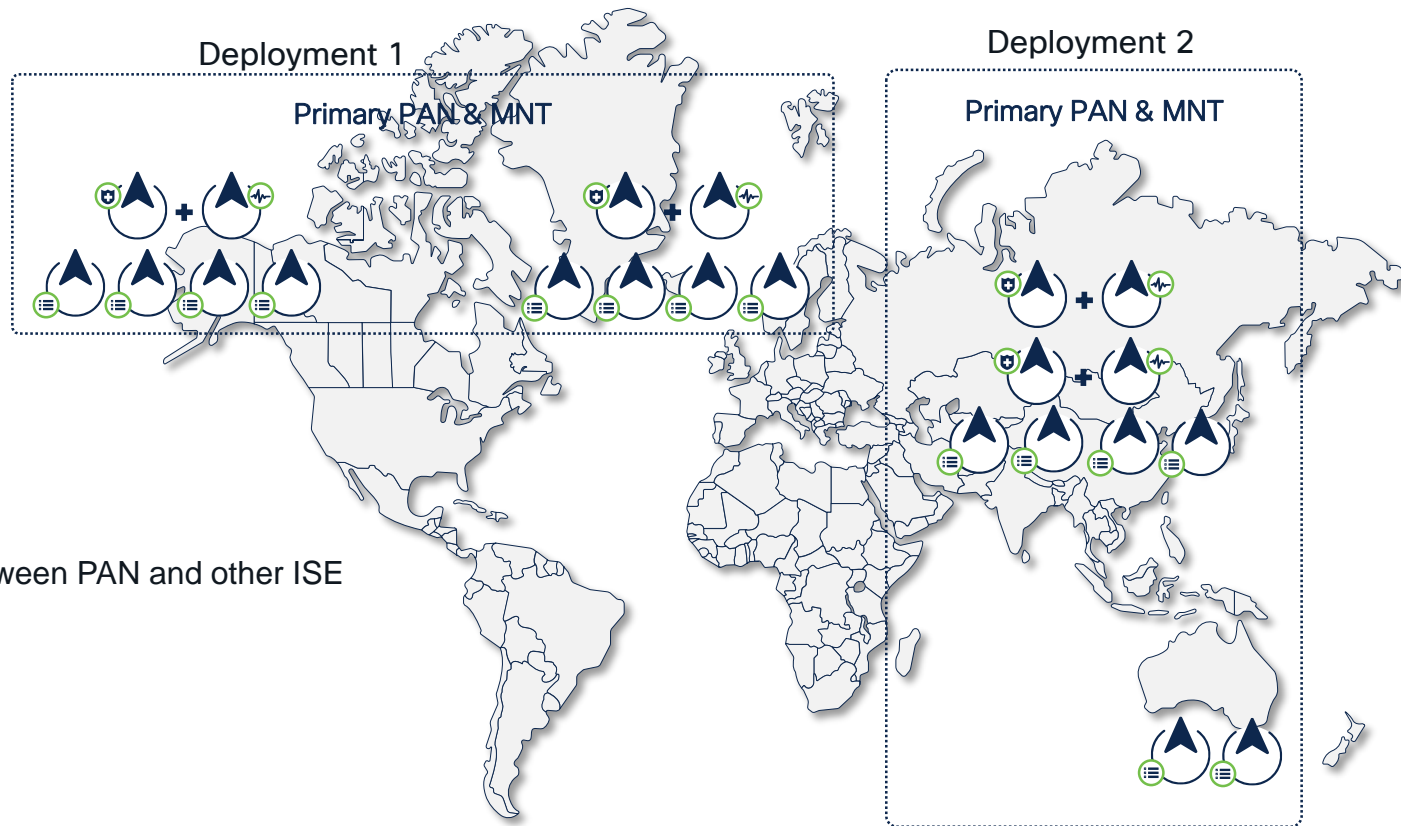


Large Deployment: Centralized or Distributed



- Max 300ms latency between PAN and other ISE nodes (not NADs)
- Co-locate PSNs with AD or other dependencies

Large Deployment: Separate Cubes



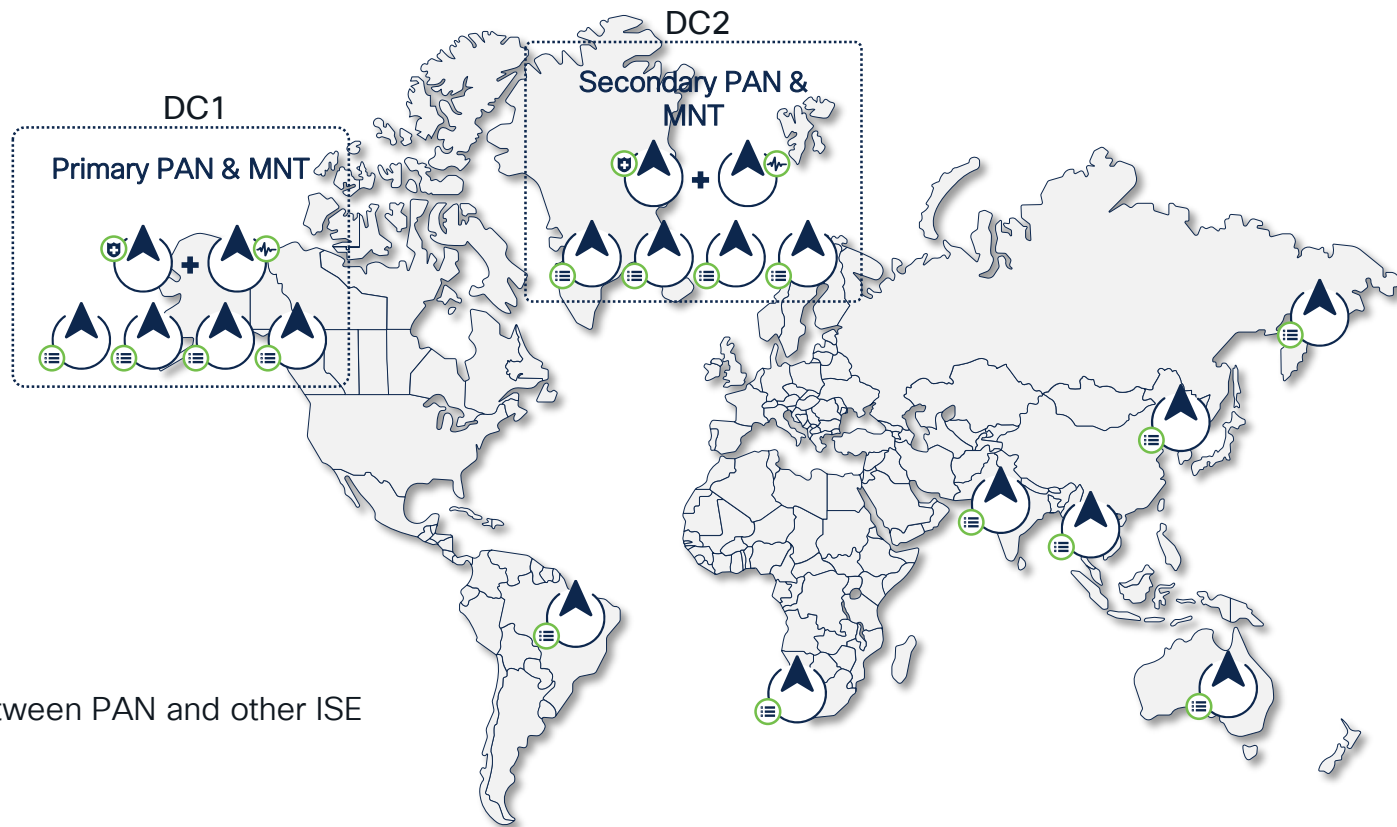
- Max 300ms latency between PAN and other ISE nodes (not NADs)

Cisco ISE Deployment

Latency Guidance



Latency Guidance



- Max 300ms latency between PAN and other ISE nodes (not NADs)

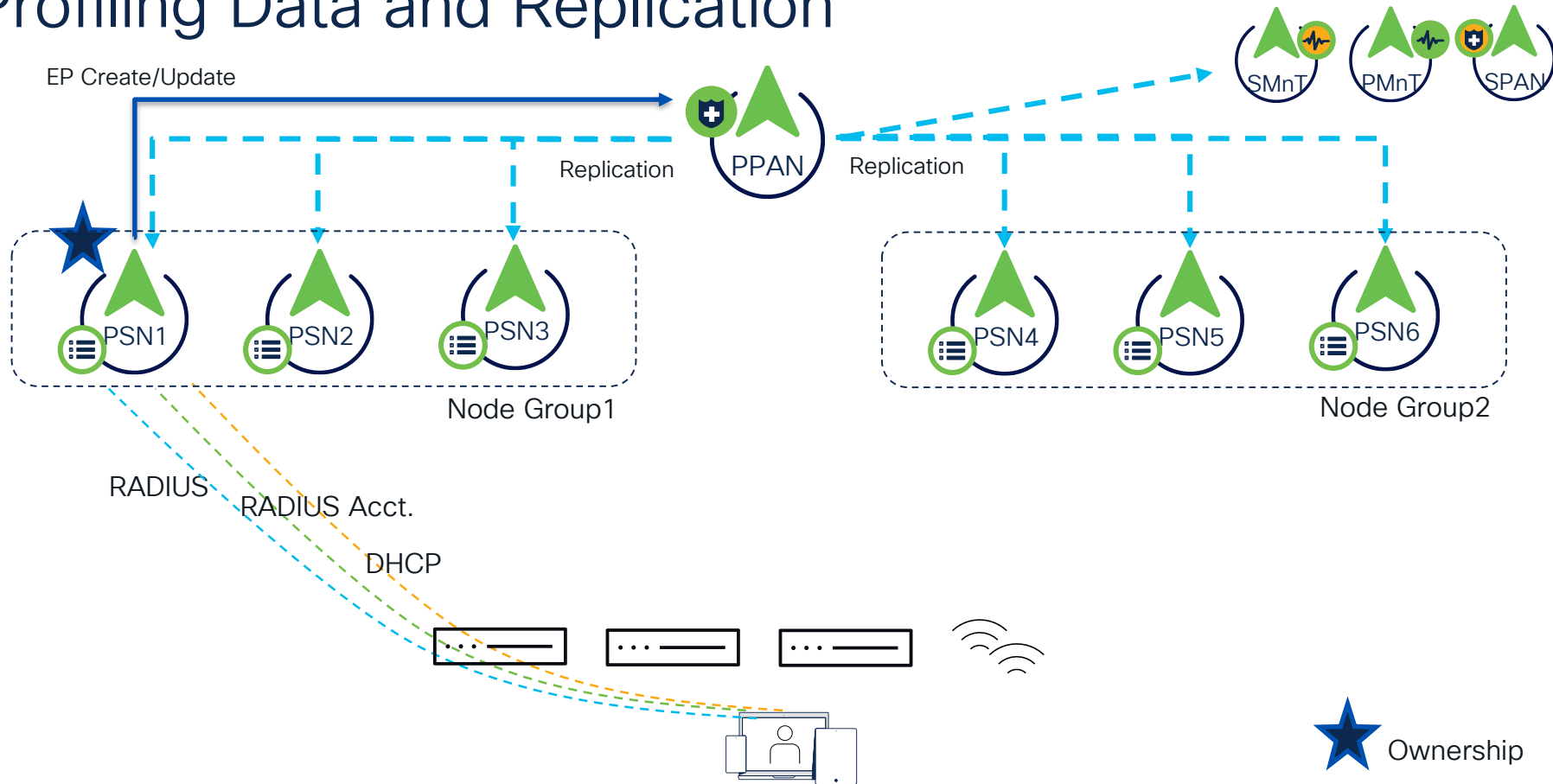
Latency Guidance

- Latency guidance $\leq 300\text{ms}$ – Guard rail; Not a fall off the cliff
- Dependency in Profiling configuration
- Higher Auth/Profiling Rates may require lower latency

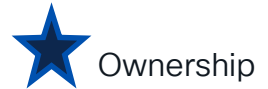
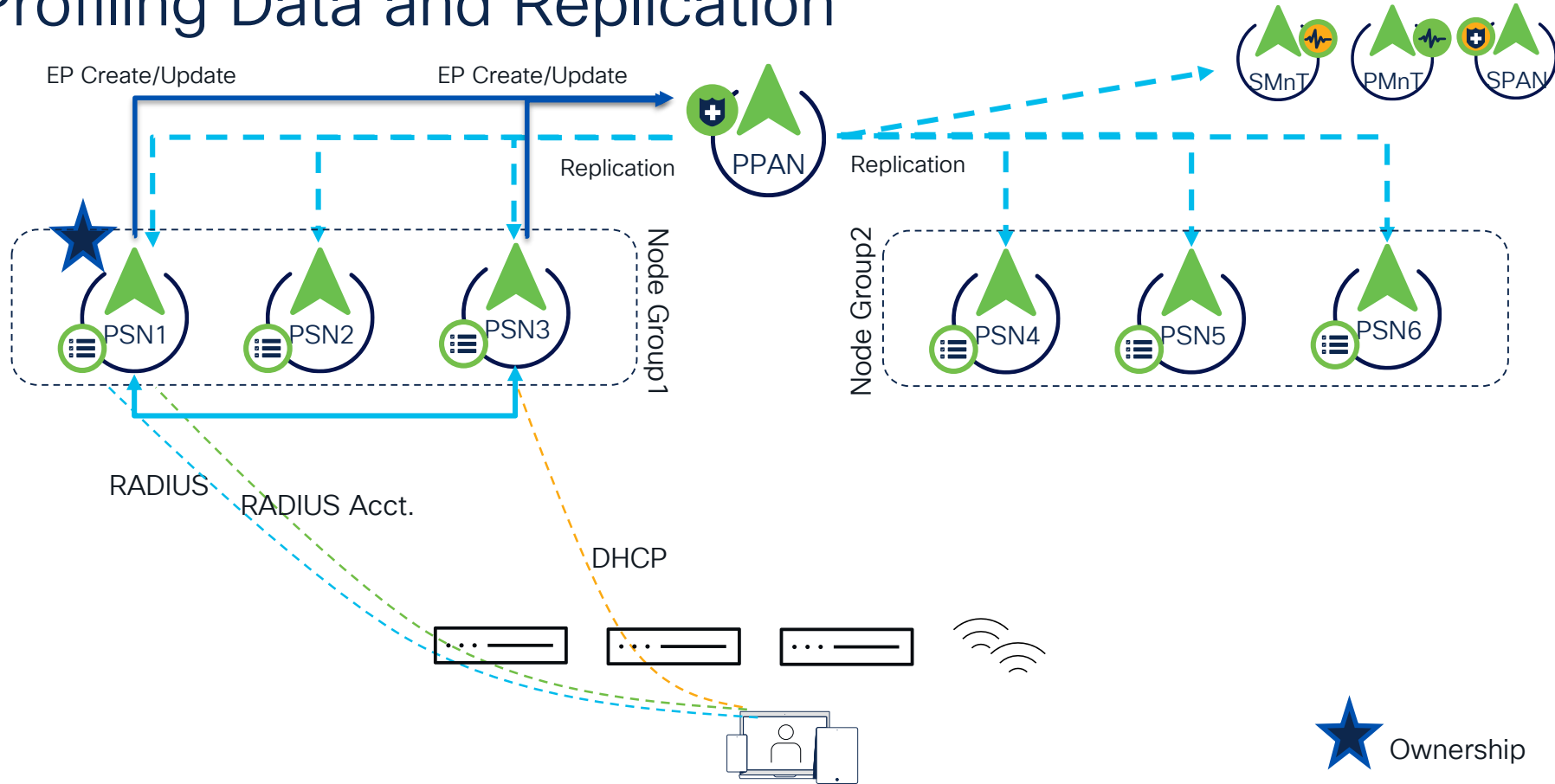


Confused?

Profiling Data and Replication



Profiling Data and Replication



Endpoint Owner Directory

- Enable Endpoint Owner Directory
- More efficient way than legacy profiling data replication
- Legacy Profiling gets endpoint info via PPAN where PPAN becomes bottleneck

Endpoint Owner Directory


Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.

☒ Enable Endpoint Owner Directory

ISE Performance & Scale



- Deployment Types
- Maximum Concurrent Active Sessions
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- Configuration Objects

 cs.co/ise-scale

 Products and Services Solutions Support Learn

Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information /

Performance and Scalability Guide for Cisco Identity Services Engine

 Download  Print

Contents

- [Overview](#)
- [Cisco ISE Node Terminology](#)
- [Different Types of Cisco ISE Deployment](#)
- [Maximum Concurrent Active Endpoints for Different Deployments](#)
- [Cisco ISE Deployment Scale Limits](#)
- [RADIUS Performance](#)
- [TACACS+ Performance](#)
- [Cisco ISE Scenario-Based Performance](#)
- [Cisco ISE Hardware Platforms](#)

Overview

This document lists the performance and scalability metrics for Cisco Identity Services Engine (Cisco ISE).





Cisco ISE Node Terminology

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes.

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage the network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

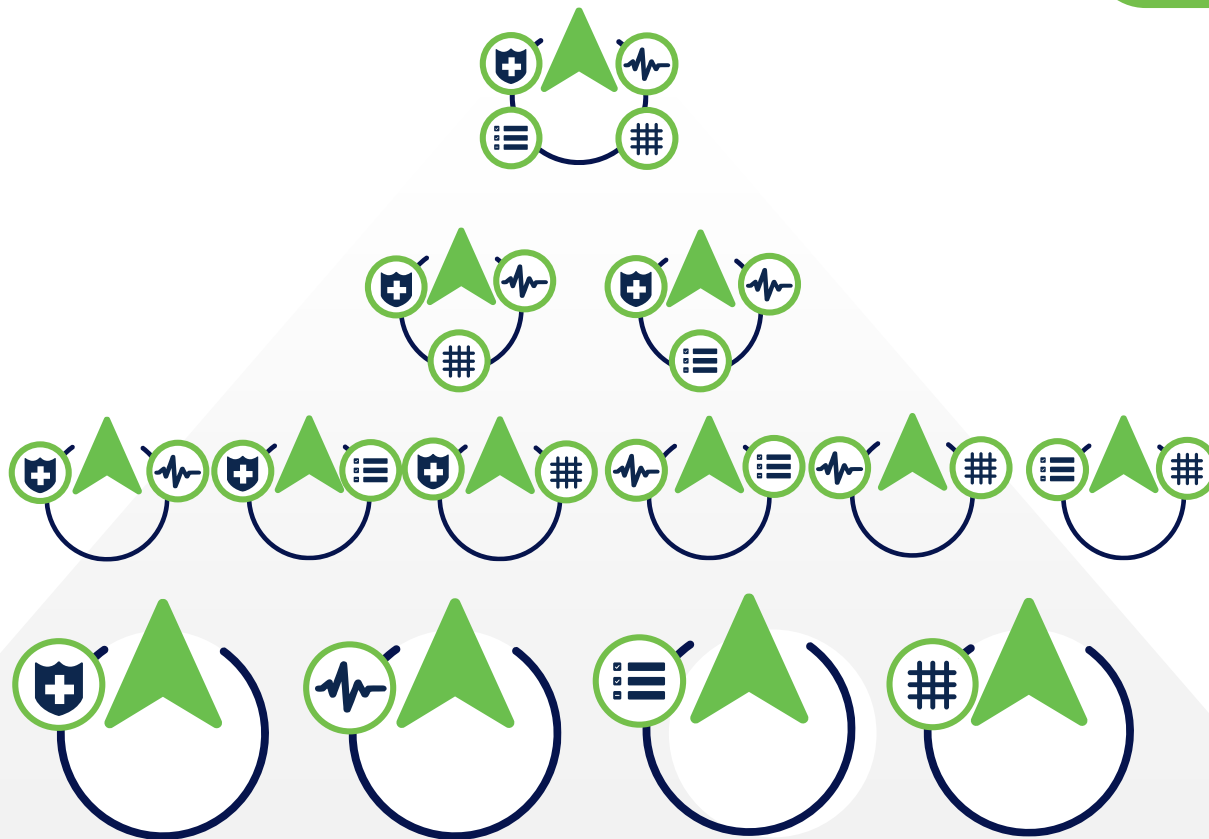
Different Types of Cisco ISE Deployment

Evaluation	Small Deployment	Medium Deployment	Large Deployment
 • All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM	 • All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM		 • <= 50: PSNs + <= 4 PXGs

Shared vs Dedicated ISE Persona

Best Practices

Shared



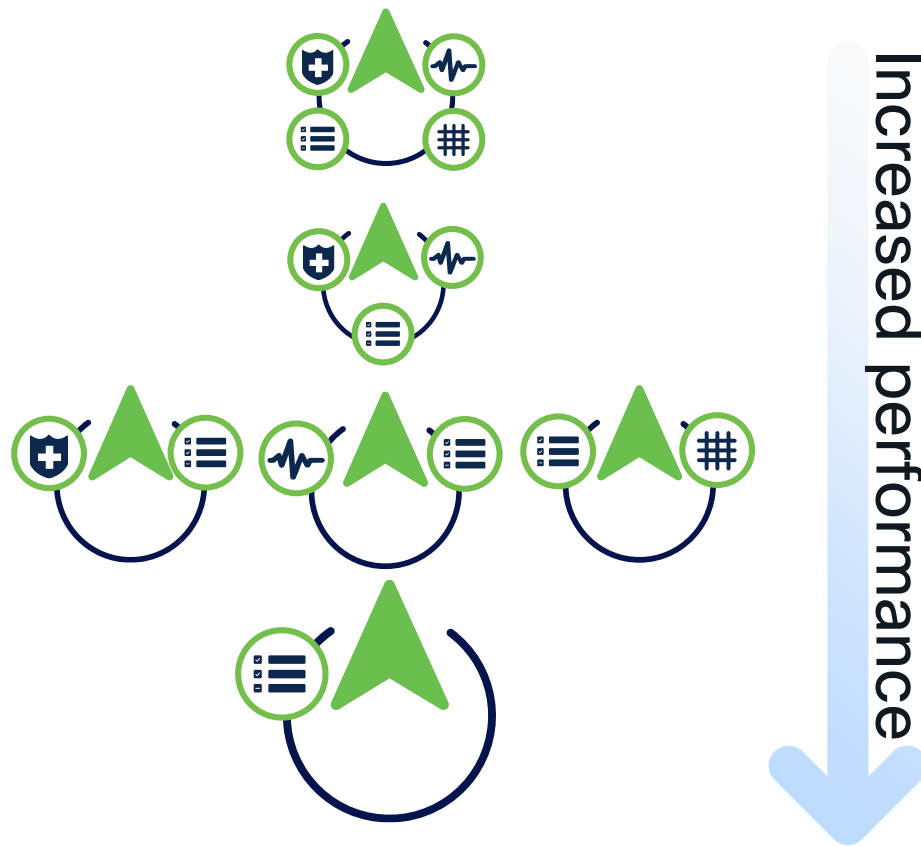
Increased performance

Dedicated

cisco *Live!*

Shared vs Dedicated ISE PSN


Best Practices



RADIUS TPS cs.co/ise-scale


Authentication Rates

Authentication Method	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755/3695/3795
PAP with internal user database	900	1100	1300
PAP with Active Directory	250	250	300
PAP with LDAP Directory	300	300	350
PEAP (MSCHAPv2) with internal user database	150	150	200
PEAP (MSCHAPv2) with Active Directory	150	150	175
PEAP (GTC) with internal user database	150	150	250
PEAP (GTC) with Active Directory	100	150	175
EAP-FAST (MSCHAPv2) with internal user database	350	400	500
EAP-FAST (MSCHAPv2) with Active Directory	200	250	300


[Products and Services](#)
[Solutions](#)
[Support](#)
[Learn](#)

[Support](#) / [Product Support](#) / [Security](#) / [Cisco Identity Services Engine](#) / [Compatibility Information](#) /

Performance and Scalability Guide for Cisco Identity Services Engine

 Download

Contents

- [Overview](#)
 - [Cisco ISE Node Terminology](#)
 - [Different Types of Cisco ISE Deployment](#)
 - [Maximum Concurrent Active Endpoints for Different Deployments](#)
 - [Cisco ISE Deployment Scale Limits](#)
 - [RADIUS Performance](#)
 - [TACACS+ Performance](#)
 - [Cisco ISE Scenario-Based Performance](#)
 - [Cisco ISE Hardware Platforms](#)

Overview

This document lists the performance and scalability metrics for Cisco Identity Services Engine (Cisco ISE).





Cisco ISE Node Terminology

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are the role and personas that a Cisco ISE node assumes.

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage the network and resolve issues. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

Different Types of Cisco ISE Deployment

Evaluation	Small Deployment	Medium Deployment	Large Deployment
 <p>• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM</p>	 <p>• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM</p>		 <p>• <= 50: PSNs + <= 4 PXGs</p>

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

43

RADIUS TPS



cs.co/ise-scale

Authentication Rates

Authentication Method	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755/3695/3795
PAP with internal user database	900	1100	1300
PAP with Active Directory	250	250	300
PAP with LDAP Directory	300	300	350
PEAP (MSCHAPv2) with internal user database	150	150	200
PEAP (MSCHAPv2) with Active Directory	150	150	175
PEAP (GTC) with internal user database	150	150	250
PEAP (GTC) with Active Directory	100	150	175
EAP-FAST (MSCHAPv2) with internal user database	350	400	500
EAP-FAST (MSCHAPv2) with Active Directory	200	250	300

Max TPS

Common Protocol
TPS against Internal
store

Common Protocol
TPS against AD

Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information /

Products and Services Solutions Support Learn

PostgreSQL Engine

Download

Use Case

Cisco ISE Node Technology

Different Types of Cisco ISE Deployment

Maximum Concurrent Active Endpoints for Different Deployments

Cisco ISE Deployment Scale Limits

RADIUS

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona provides advanced network and resource monitoring. It stores log messages and provides reports. It also provides you with the ability to monitor and analyze network events.
pxGrid	A Cisco ISE node with the pxGrid persona provides directory integration and information exchange. It performs the directory integration and provides information exchange with other information systems.

Different Types of Cisco ISE Deployment

Evaluation	Small Deployment	Medium Deployment	Large Deployment
<p>• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM</p>	<p>• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM</p>	<p>• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM</p>	

ISE Deployment

Certificates



ISE System Certificate – Recommendations

Best Practices

- Use Wildcard SAN or Multi-SAN certificates

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

City (L) RTP

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:0
0:00:00:00:00:0D

Subject Alternative Names DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

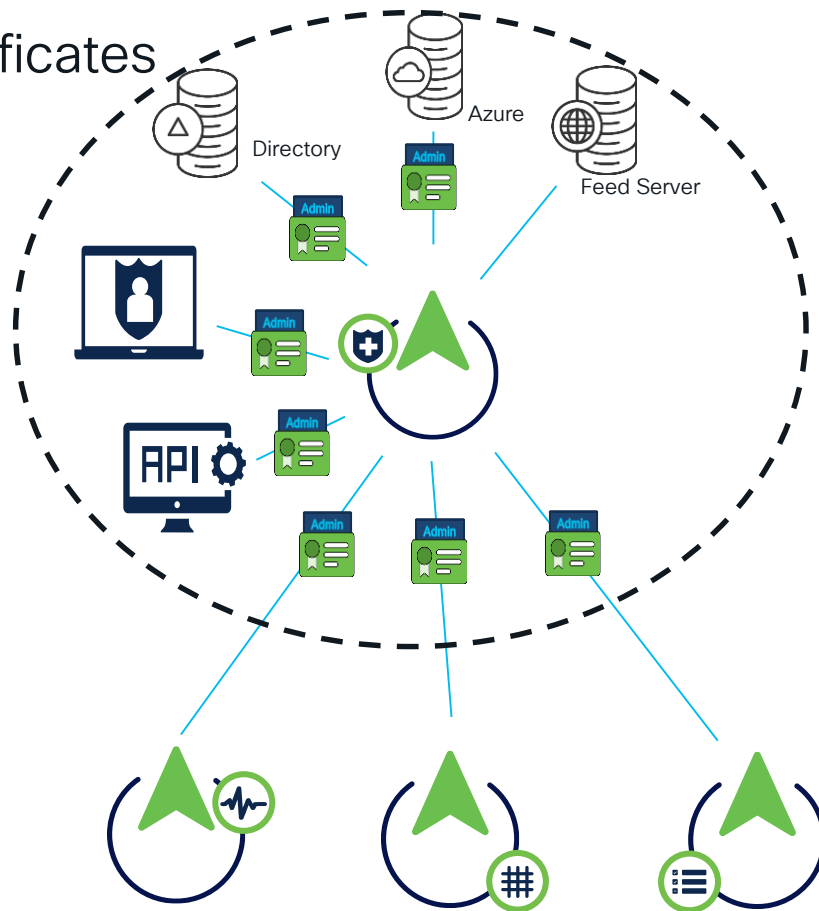
City (L) Durham

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:0
0:00:00:00:00:0E

Subject Alternative Names DNS:zer0k-zer0k.org,DNS:ise-
dunkel.zer0k.org,DNS:ise-
malbock.zer0k.org,DNS:zer0k-
ise1.zer0k.org,DNS:zer0k-ise2.zer0k.org



ISE System Certificate – Recommendations

Best Practices

- Use Wildcard SAN or Multi-SAN certificates

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

City (L) RTP

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:0
0:00:00:00:00:0D

Subject Alternative Names DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

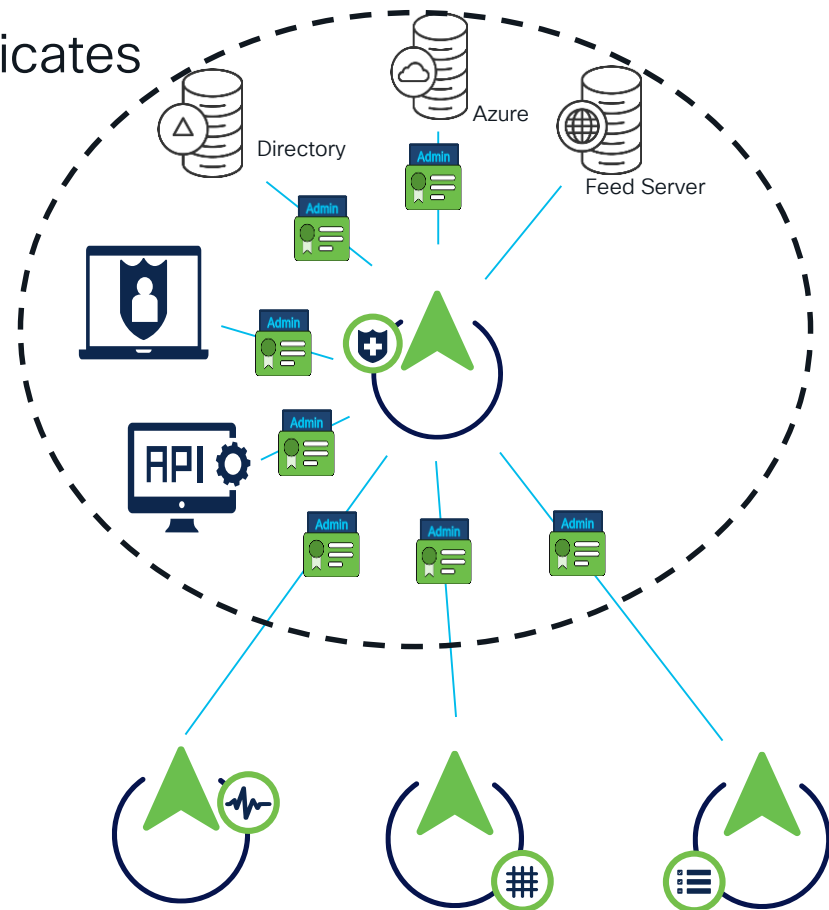
City (L) Durham

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:0
0:00:00:00:00:0E

Subject Alternative Names DNS:zer0k-zer0k.org,DNS:ise-
dunkel.zer0k.org,DNS:ise-
maibock.zer0k.org,DNS:zer0k-
ise1.zer0k.org,DNS:zer0k-ise2.zer0k.org



ISE System Certificate – Recommendations

Best Practices

- Use Wildcard SAN or Multi-SAN certificates

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

City (L) RTP

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:00:00:00:00:00:0D

Subject Alternative Names DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org

Details

Issued To

Common Name (CN) zer0k-ise.zer0k.org

Organization Unit (OU) TAC

Organization (O) Cisco

City (L) Durham

State (ST) NC

Country (C) US

Serial Number 42:00:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:00:00:00:00:0E

Subject Alternative Names DNS:zer0k-zer0k.org,DNS:ise-dunkel.zer0k.org,DNS:ise-maibock.zer0k.org,DNS:zer0k-ise1.zer0k.org,DNS:zer0k-ise2.zer0k.org

ISE System Certificate – Recommendations

Best Practices

- Use Wildcard SAN or Multi-SAN certificates

Wildcard SAN

Details	
Issued To	
Common Name (CN)	zer0k-ise.zer0k.org
Organization Unit (OU)	TAC
Organization (O)	Cisco
City (L)	RTP
State (ST)	NC
Country (C)	US
Serial Number	42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:00:00:00:00:00:00
Subject Alternative Names	DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org

Easy to expand
Less expensive
ISE FQDNs in Subdomain to limit the validity

Multi-SAN

Details	
Issued To	
Common Name (CN)	zer0k-ise.zer0k.org
Organization Unit (OU)	TAC
Organization (O)	Cisco
City (L)	Durham
State (ST)	NC
Country (C)	US
Serial Number	42:00:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:00:00:00:00:00:00
Subject Alternative Names	DNS:zer0k-zer0k.org,DNS:ise-dunkel.zer0k.org,DNS:ise-malbock.zer0k.org,DNS:zer0k-ise1.zer0k.org,DNS:zer0k-ise2.zer0k.org

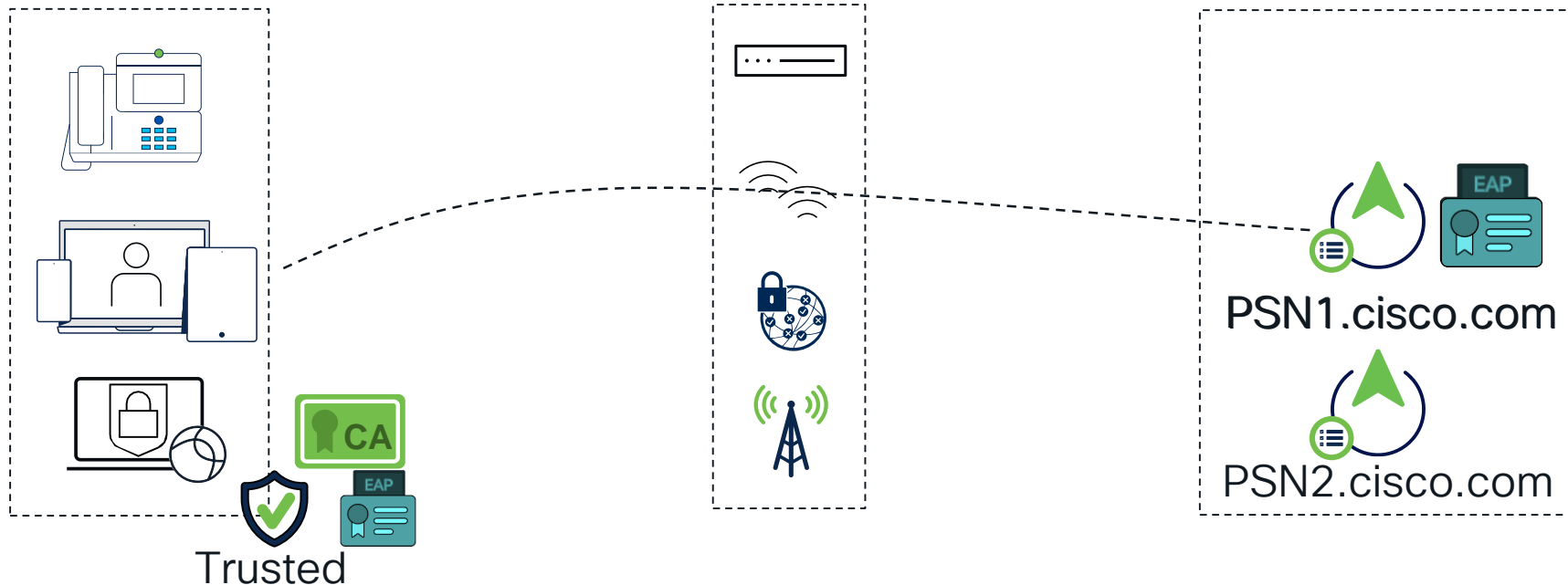
More expensive
Difficult to expand

ISE EAP Certificate - Recommendations

Users & Devices

Network Devices

ISE Deployment

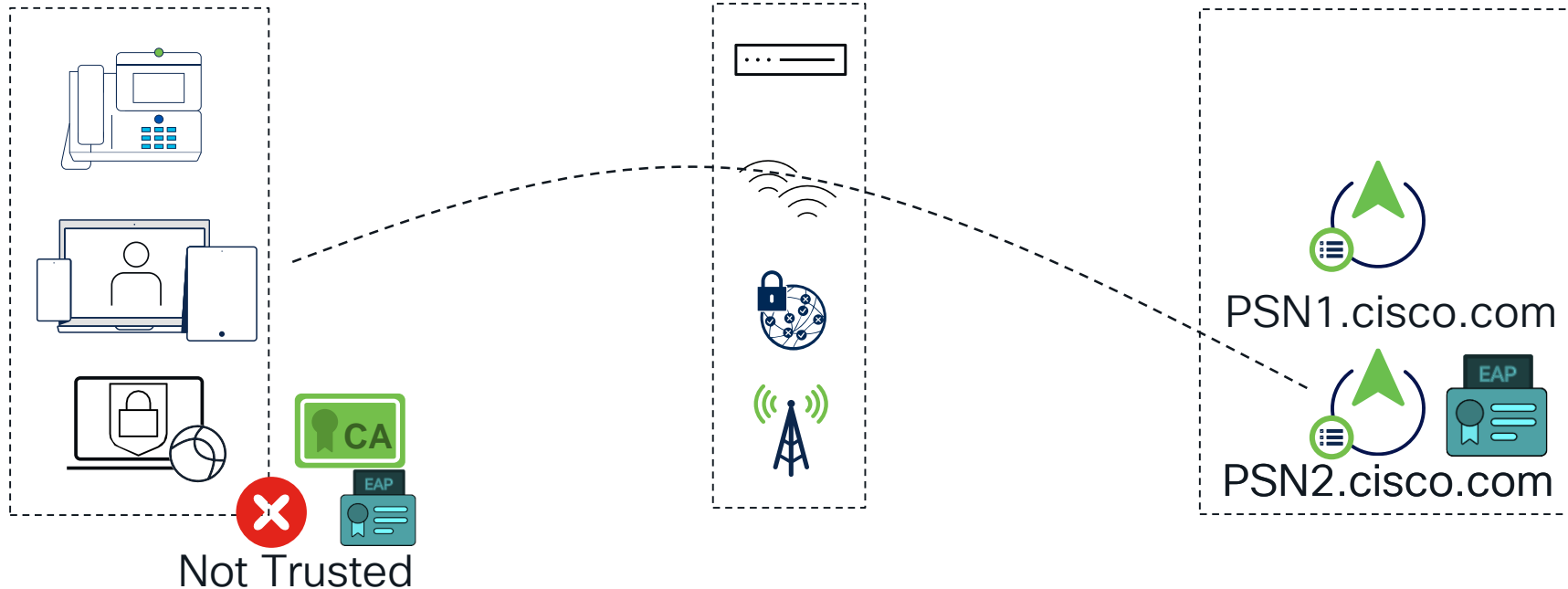


ISE EAP Certificate - Recommendations

Users & Devices

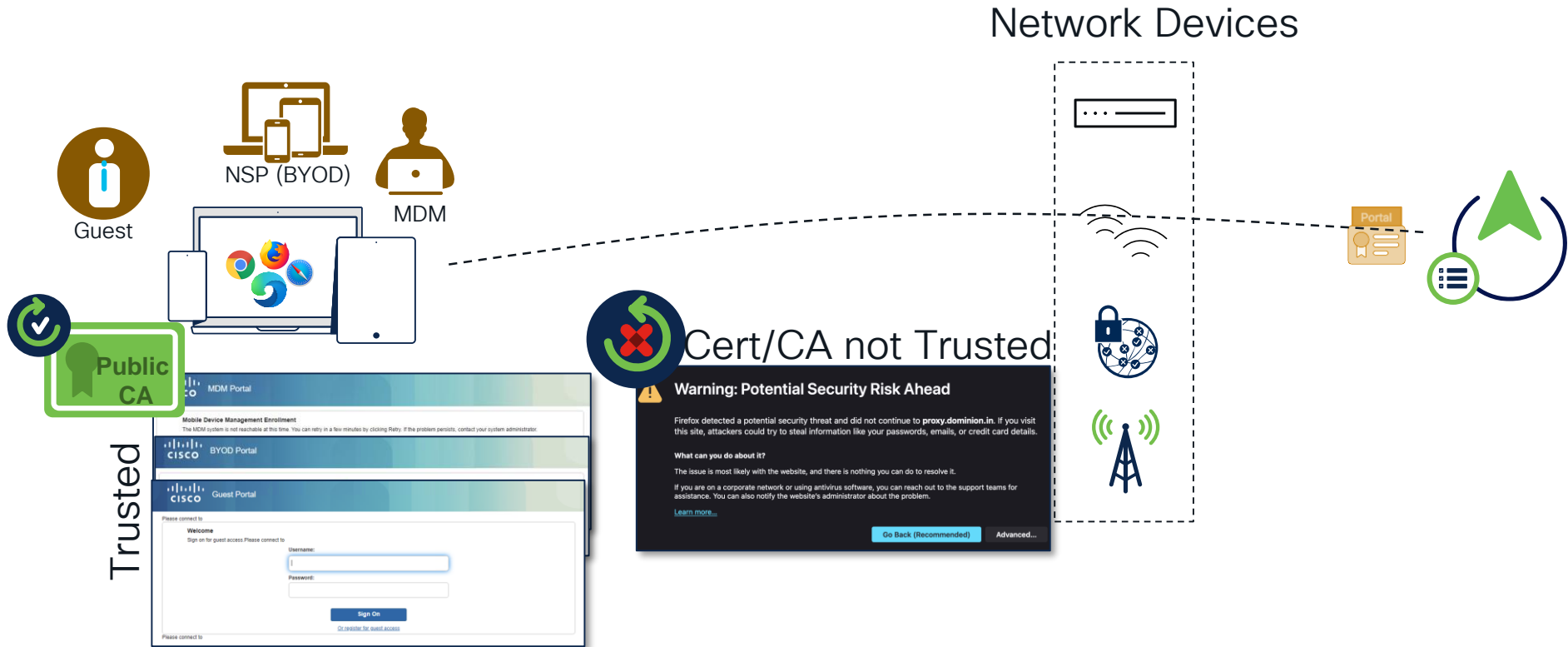
Network Devices

ISE Deployment

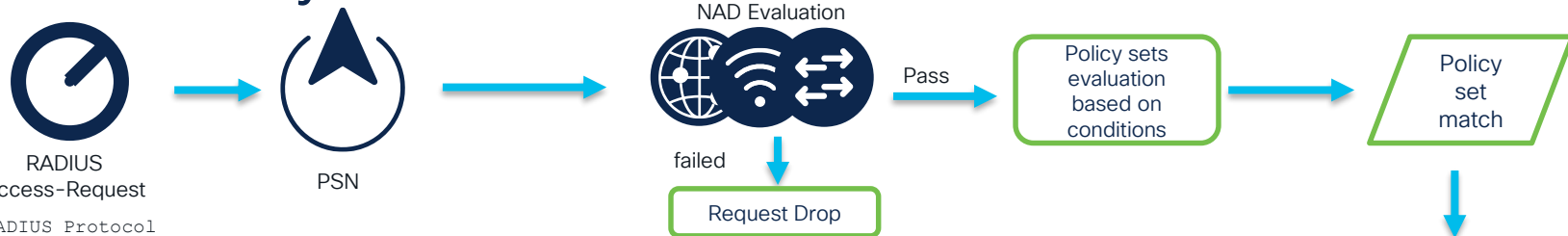


ISE Portal Certificates – Recommendations

Use Public CA – BYOD/Guest/MDM

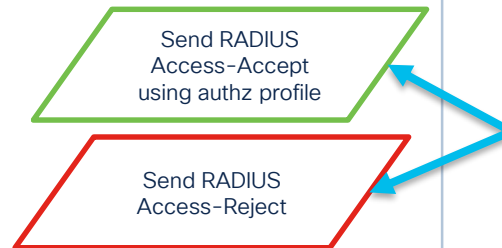


ISE Policy evaluation



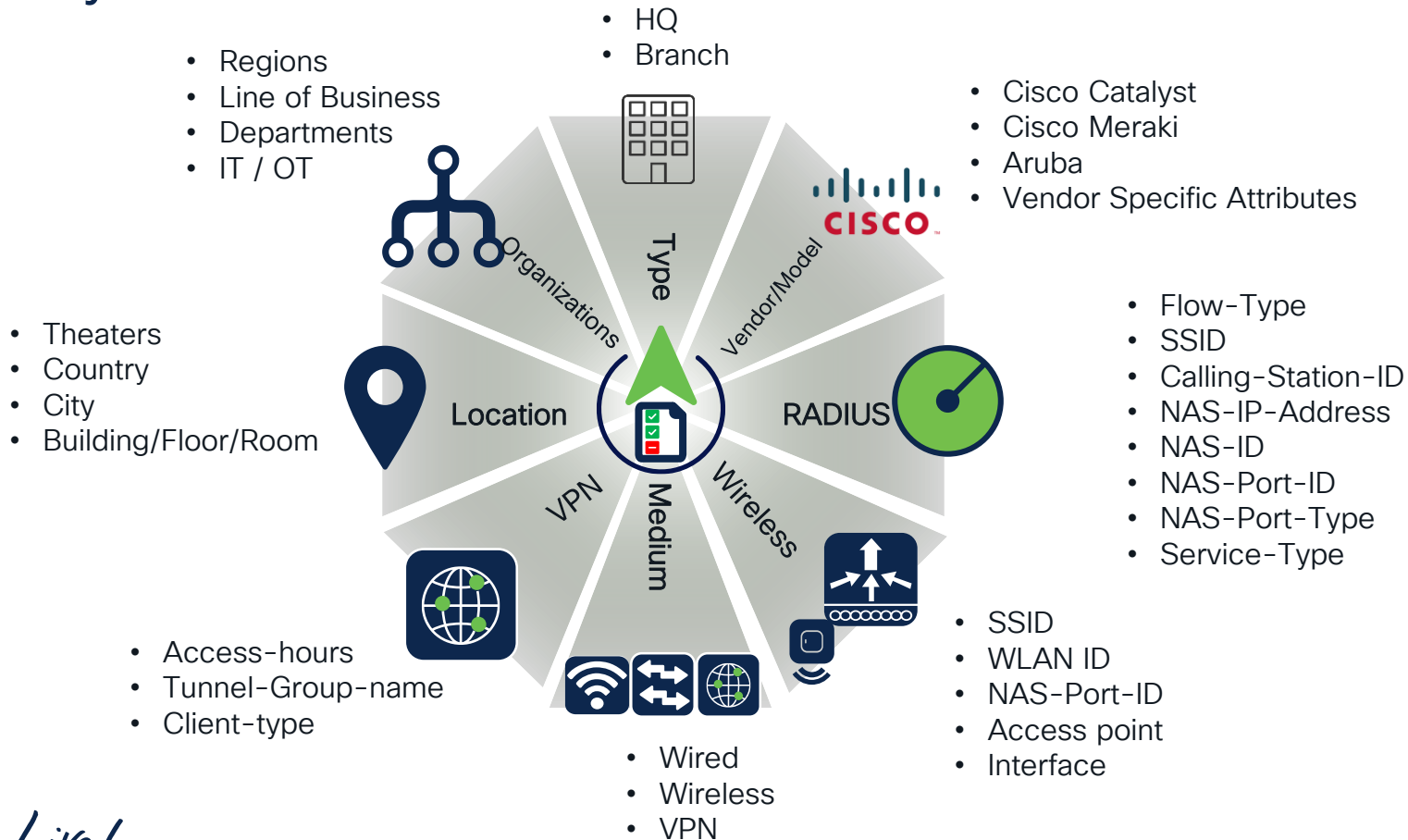
```

RADIUS Protocol
Code: Access-Request (1)
Packet identifier: x0 (0)
Length: 153
Authenticator:29eb293b3a40ea740a8fd33bdb18f1d7
Attribute Value Pairs
> AVP: t=User-Name (1) 1=8 val=pavan
> AVP: t=NAS-IP-Address (4) (=6 val=6.86.227.108
> AVP: t=Calling-Station-Id (31) 1=19 val=02-00-00-00-00-01
> AVP: t=Called-Station-Id (30) 1=27 val=2C-3F-0B-56-E3-6C: Employee
> AVP: t=Framed-MTU (12) (=6 val=1400
> AVP: t=NAS-Port-Type (61) (=6 val=Wireless-802.11 (19)
> AVP: t=Service-Type (6) 1=6 val=Framed (2)
> AVP: t=Connect-Info (77) (=24 val=CONNECT 11Mbps 802.11b
> AVP: t=EAP-Message (79) 1=13 Last Segment [1]
> AVP: t=Message-Authenticator (80) 1=18
val=26f047af6a9a82279dfd6d19b477c31b
> AVP: t=Vendor-Specific (26) 1=36 vnd=ciscoSystems (9)
Type: 26
Length: 36
Vendor ID: ciscoSystems (9)
> VSA: t=Cisco-AVPair (1) (=30 val=linksec-policy=should-secure
> AVP: t=Vendor-Specific (26) 1=80 vnd=ciscoSystems (9)
Type: 26
Length: 80
Vendor ID: ciscoSystems (9)
> VSA: t=Cisco-AVPair (1) (=74 val=ACS: CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT-ALL-IPV4-TRAFFIC-57f6b0d3
> AVP: t=Vendor-Specific (26) (=38 vnd=ciscoSystems (9)
  
```



11007 Could not locate Network Device or AAA Client
 5405 RADIUS Request dropped
 5413 RADIUS Accounting-Request dropped

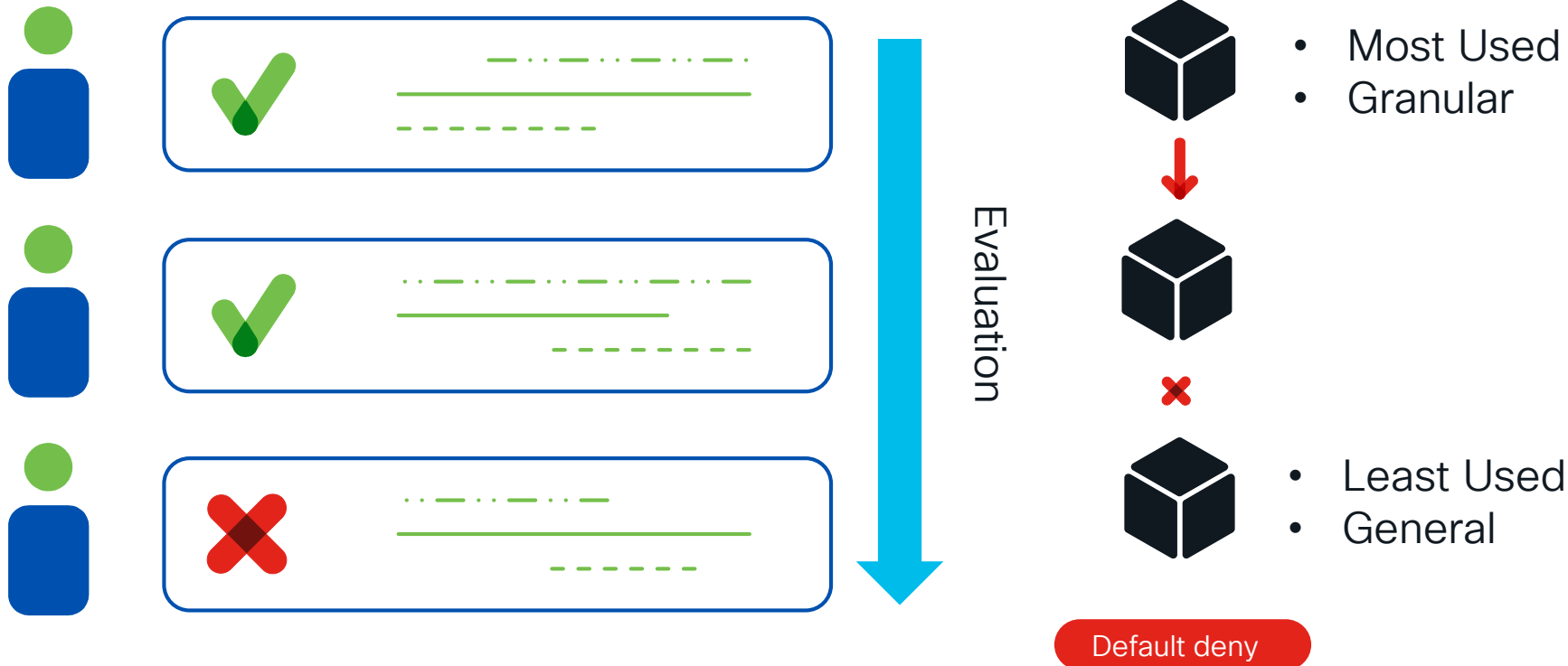
Policy Sets Conditions



Policies Configuration - Recommendations

Best Practices

Evaluation, Defaults and Usage



Policies Configuration – Recommendations

Best Practices

Review and Reorder

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Search						
✓	territory-Policy-Set		territoryEndpoints	TEAP Network Access	641	⚙️	➔
✓	Intune_Integration		Network Access-Protocol EQUALS RADIUS	Default Network Access	5822	⚙️	➔
✓	MDM_Azure		MDM-endpoints	Default Network Access	667	⚙️	➔
			win-posture-endpoints	Default Network Access	39786	⚙️	➔

Policy Sets

Reset Reset Policyset Hitcounts Save




Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Search						
✓	Posture		win-posture-endpoints	Default Network Access	39734	⚙️	
✓	Intune_Integration		Network Access-Protocol EQUALS RADIUS	Default Network Access	5822	⚙️	
✓	MDM_Azure		MDM-endpoints	Default Network Access	667	⚙️	
✓	territory-Policy-Set		territoryEndpoints	TEAP Network Access	641	⚙️	

Review & Reorder

Policies Configuration - Recommendations

Best Practices

Internal Attribute Conditions - > External Attribute Conditions



Non_Compliant_Devices					
TEAP-Chain-Success	AND		Network Access-EapTunnel EQUALS TEAP	Full-Access	
			Network Access-EapChainingResult EQUALS User and machine both succeeded		
			Dominion-domain-ExternalGroups EQUALS dominion.in/TEAP-Group/AD-TEAP-Group		
WorkspaceOne	AND		MDM-MDMServerName EQUALS WorkspaceOne	Full-Access	
			MDM-DeviceRegisterStatus EQUALS Registered		
			wired-or-wireless-dot1x		
MDM-MobileIron-non-compliant	AND		Dominion-domain-ExternalGroups EQUALS dominion.in/MDM-MobileIron/MDM-MobileIron-Group	Restricted-Access	
			MDM-MDMServerName EQUALS MobileIron		
			MDM-DeviceRegisterStatus EQUALS Registered		
			MDM-DeviceCompliantStatus EQUALS NonCompliant		
			wired-or-wireless-dot1x		

Cisco ISE Best Practices

Operations



Enable Suppression – Successful Auths

Best Practices

Suppress Successful Reports



Suppress repeated successful authentications ⓘ

Enable to Suppress Repeated AAA Records

[Reset Repeat Counts](#) [Export To](#)

Time	Status	Details	Identity	Repeat Count	Authentication Pr...
×			▼ Identity		Authentication Protocc
Apr 24, 2023 01:55:20.4...			azureuser@iseiscool.onmicro...	14	EAP-TLS
Apr 24, 2023 01:32:41.0...			14:16:9D:86:D7:3E	13	Lookup
Apr 24, 2023 01:31:52.0...			00:50:56:8E:85:F0	13	Lookup
Apr 24, 2023 01:31:50.6...			00:50:56:8E:70:06	13	Lookup
Apr 24, 2023 01:31:47.5...			00:50:56:8E:C1:38	13	Lookup
Apr 24, 2023 01:31:42.0...			00:50:56:8E:6A:67	13	Lookup
Apr 24, 2023 01:31:41.9...			00:50:56:8E:A9:F6	13	Lookup

Enable Suppression Failed/Misconfigured Clients

Best Practices

- Enable to Identify Misconfigured Supplicants
- Enable to Suppress Repeated Failed Endpoints

- Rejects Repeated Failed Endpoints

Live Logs Live Sessions

Misconfigured Supplicants ⓘ

1

Rejected Endpoints ⓘ

1

Cisco ISE Work Centers · Network Access

Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy

Client Provisioning

Protocols

EAP-FAST

EAP TLS

PEAP

RADIUS

Collection Filters

Proxy Settings

RADIUS Settings

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

- ☒ Suppress Repeated Failed Clients ⓘ
- Detect two failures within 5 Minutes ⓘ
- Report failures once every 15 minutes (15-60) ⓘ
- ☒ Reject RADIUS requests from clients with repeated failures ⓘ
- Failures prior to automatic rejection 5 (2-100) ⓘ
- Continue rejecting requests for 60 minutes (5-180) ⓘ
- Ignore repeated accounting updates within 5 seconds (1 - 86,400) ⓘ

Suppress Successful Reports

- ☒ Suppress repeated successful authentications ⓘ

CISCO Live!

Schedule Your Backup Regularly

Best Practices

☰ Cisco ISE

Administration · System

Evaluation Mode 85 Days 🔍 ? 🖨 ⚙

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade

Health Checks

Backup & Restore

More ▾

Backup & Restore

Policy Export

Backup & Restore

Backup Now ⓘ

☒ Configuration Data Backup

☐ Operational Data Backup

Backup Now

Schedule Backup

		Frequency	Start End Date	Execute At	Schedule Status
Configuration Data Backup	Edit	MONTHLY	04/21/2023 - 04/30/2024	1:00 AM	<input checked="" type="checkbox"/>
Operational Data Backup	Edit	MONTHLY	04/21/2023 - 04/25/2024	4:00 AM	<input checked="" type="checkbox"/>

Operational Data Purging

- By **default**, Data Retention Period is **30 Days**
- Adjust with caution based on the Disk Space availability
- **Export to external Repositories** for your old data before it gets purged.

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this, a secondary navigation bar contains tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance' (which is selected), 'Upgrade', 'Health Checks', and 'Backup & Restore'. On the left side, a sidebar menu lists 'Patch Management', 'Repository', 'Operational Data Purging' (which is highlighted), and 'Localdisk Management'. The main content area is titled 'Database Utilization' and shows a database icon with '310 GB Total DB Space'. Below this, there are two rows of data: 'isenode23.dominion.in' and 'isenode24.dominion.in', each with a corresponding progress bar. At the bottom of the main content area, there are two dashed blue boxes. The first box, titled 'Data Retention Period', contains a table with two rows: 'RADIUS' and 'TACACS', both set to '30 Days'. The second box, titled 'Repository', contains a checkbox for 'Enable Export Repository', a dropdown menu for 'Select a Repository', a 'Create Repository' link, and an 'Encryption Key' field. At the bottom of the main content area, there are 'Save' and 'Reset' buttons.

Node	Database Utilization
isenode23.dominion.in	Progress bar
isenode24.dominion.in	Progress bar

Data Retention Period		
RADIUS	30	Days
TACACS	30	Days

Repository	
<input type="checkbox"/>	Enable Export Repository
Select a Repository	
Create Repository	
Encryption Key	

RADIUS Logs Data Retention



Database Utilization

Database Name	Size	Space
isenode23.dominion.in	310 GB	
isenode24.dominion.in		

Data Retention Period

Protocol	Retention Period	Unit
RADIUS	30	Days
TACACS	30	Days

Repository

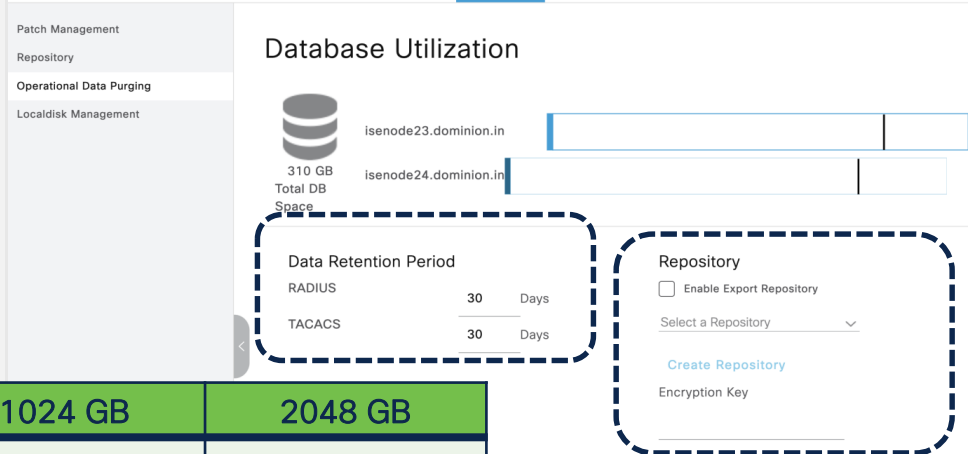
- ☐ Enable Export Repository
- Select a Repository
- Create Repository
- Encryption Key

No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

Best Practices

*The numbers are based on the following assumptions: Ten or more authentications per day per endpoint with logging suppression enabled.

TACACS Logs Data Retention



No. of Authc	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

Best Practices

*Assumption: The script runs against all NADs, 4 sessions per day, and 5 commands per session.

Endpoint Purge Policies

Configure Policies that **you don't want to purge** eg., BYOD

Configure Policies that **you want to purge** eg., Guest, Inactive Endpoints

Schedule the Purge Policies

Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to the list below. First Matched Rule Applies

Never Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)	
<input type="checkbox"/>	EnrolledRule	if DeviceRegistrationStatus Equals Registered	Edit ▼

Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)	
<input checked="" type="checkbox"/>	GuestEndpointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30	Edit ▼
<input checked="" type="checkbox"/>	RegisteredEndpointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30	Edit ▼

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every

Everyday ▼

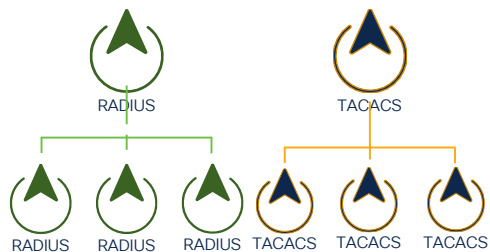
at 03 ▼ 00 ▼

Cisco ISE Best Practices

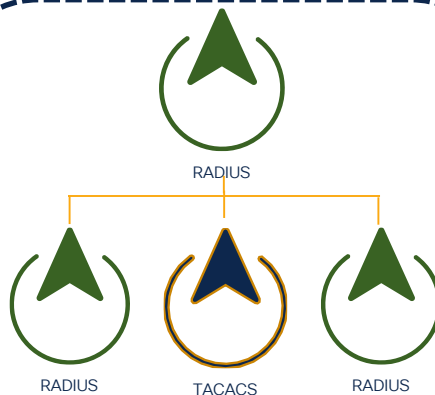
Device Administration - RADIUS &
TACACS



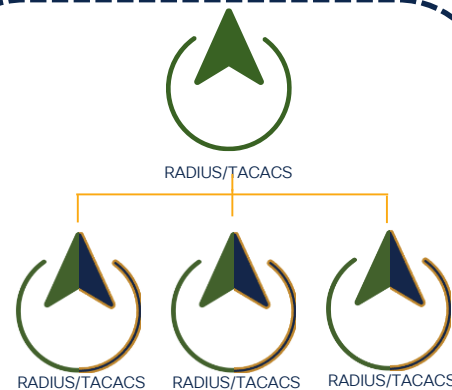
RADIUS & TACACS Deployment Options



Separate ISE
Cubes for RADIUS
& TACACS

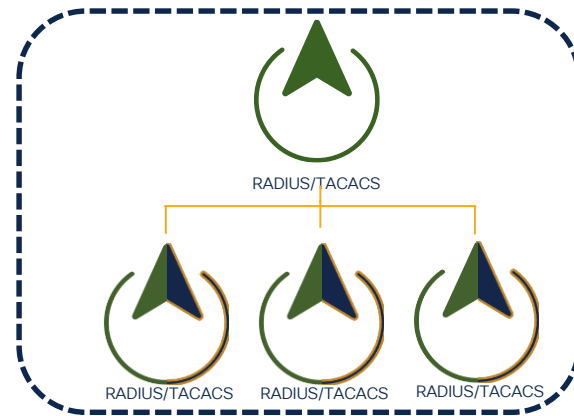
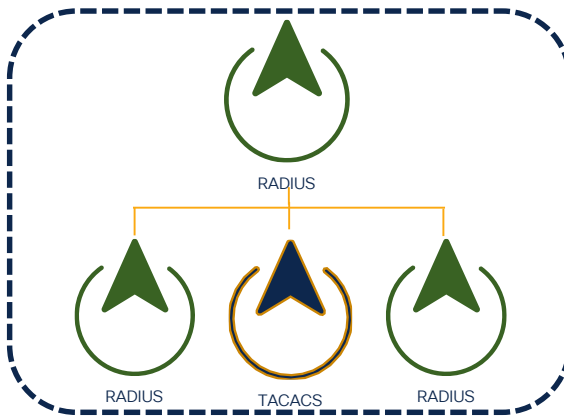
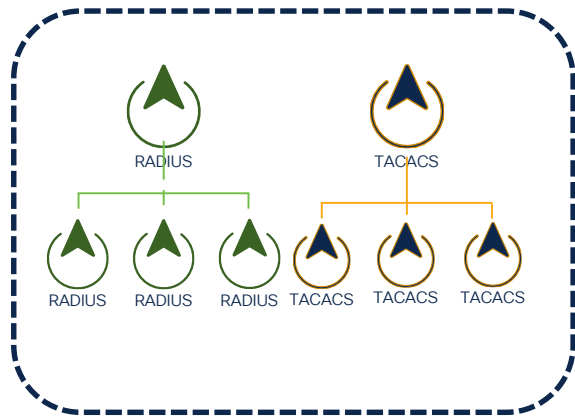


Mixed ISE Cube
with separate
PSNs for RADIUS
and TACACS+



Mixed ISE Cube
where PSNs are
not dedicated to
either

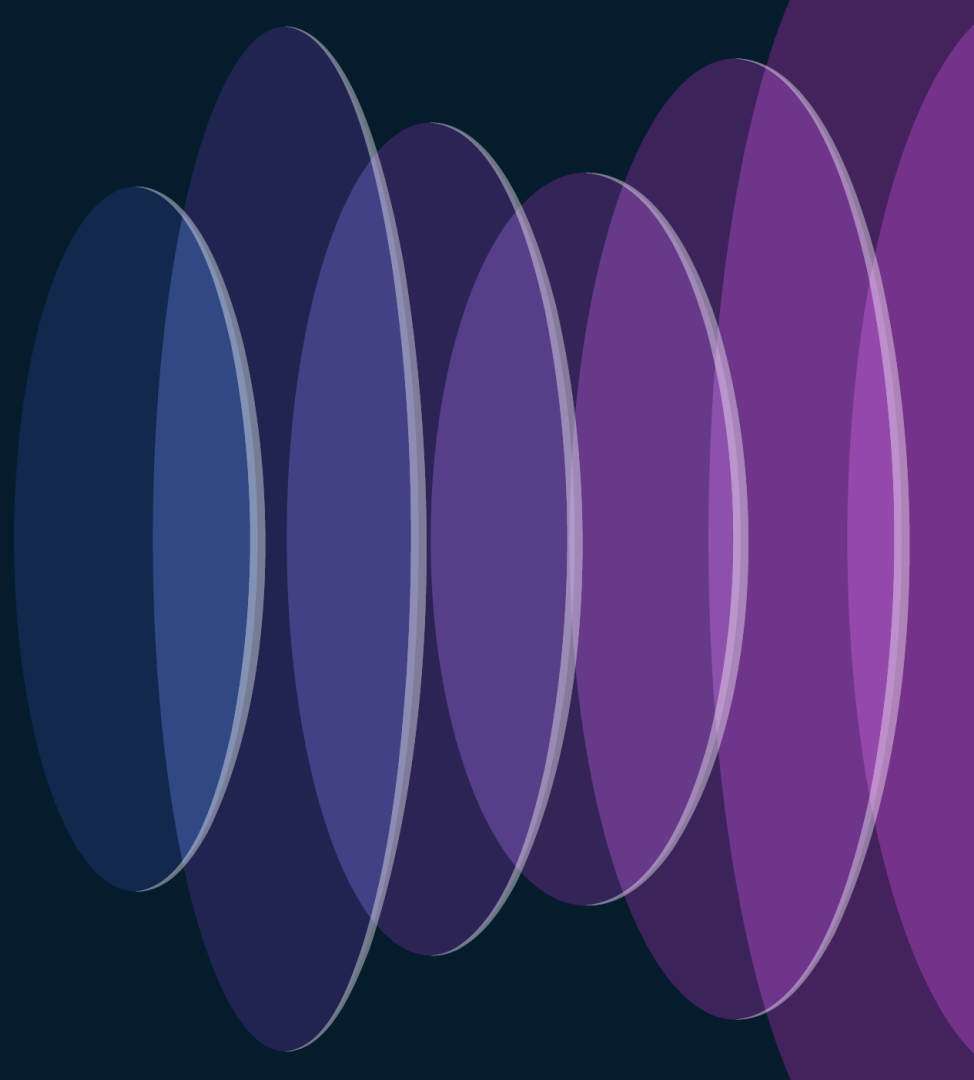
When do we separate TACACS+ and RADIUS?



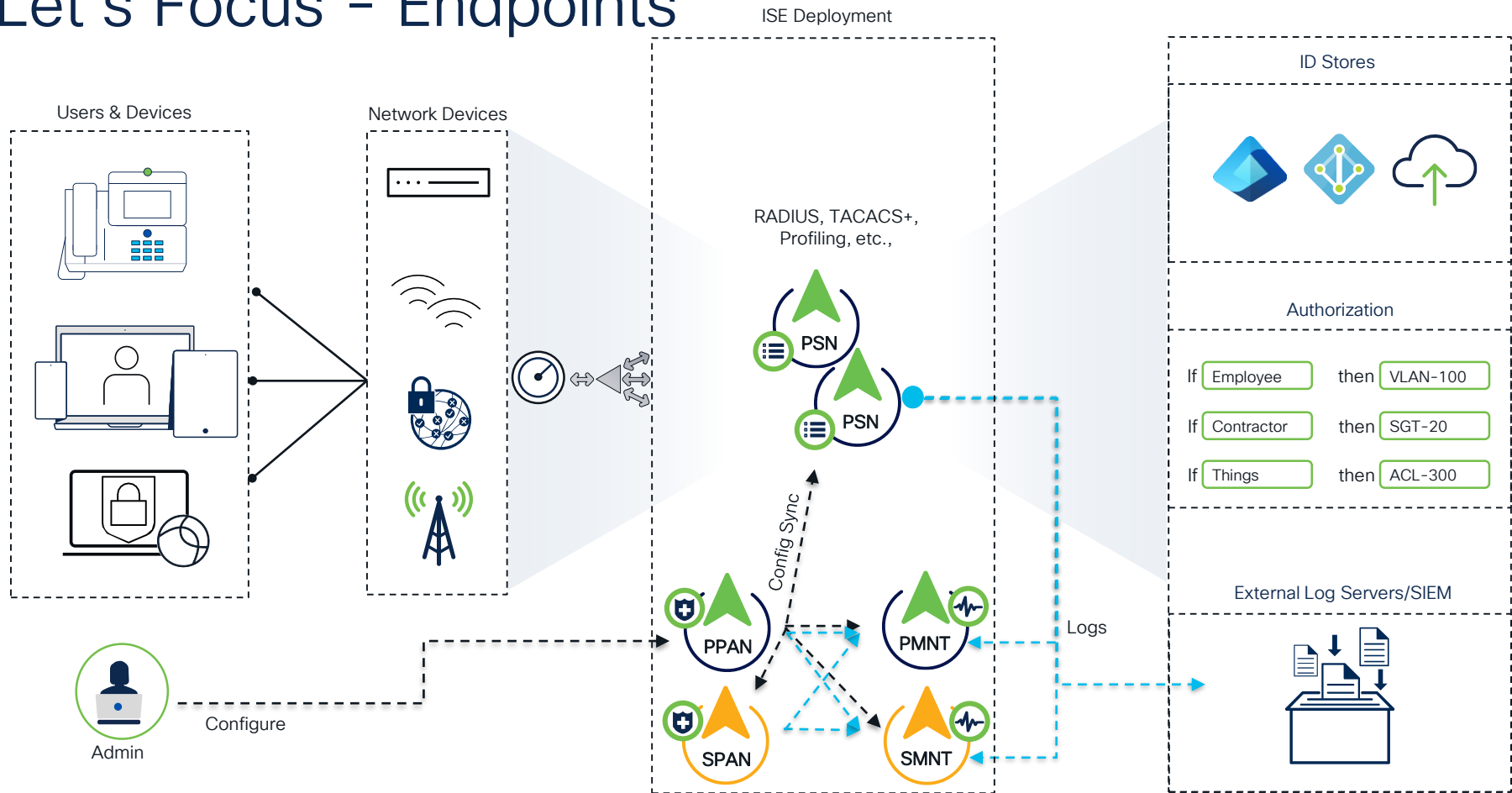
1. How many network devices?
2. Number of TACACS+ & RADIUS sessions
3. Scripts?
4. Network Management Tools
5. Increased log retention on both Deployments
6. Per-PSN utilization and load

Best Practices

Users & Devices

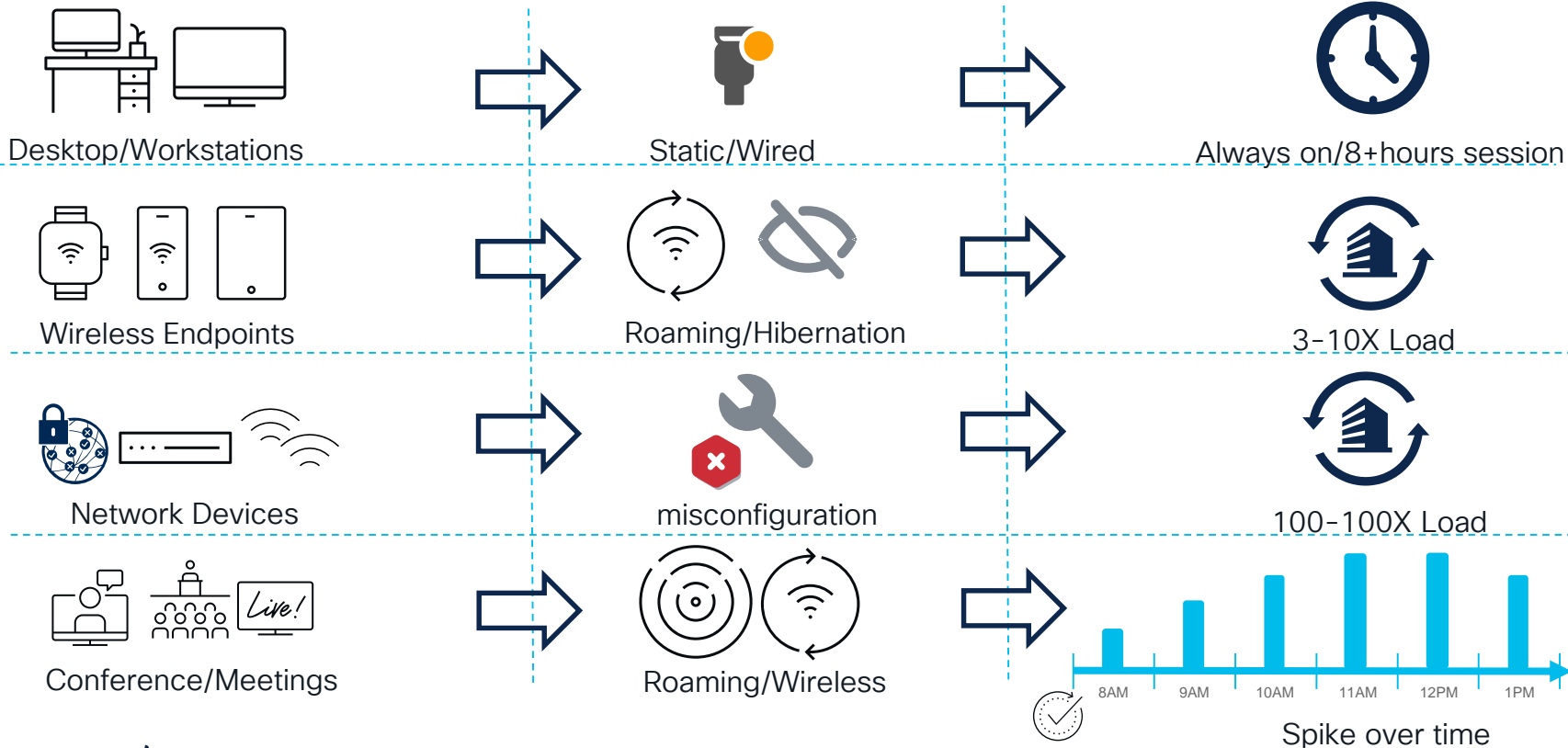


Let's Focus - Endpoints



Consideration on Endpoints

Steady State vs Peak Demand

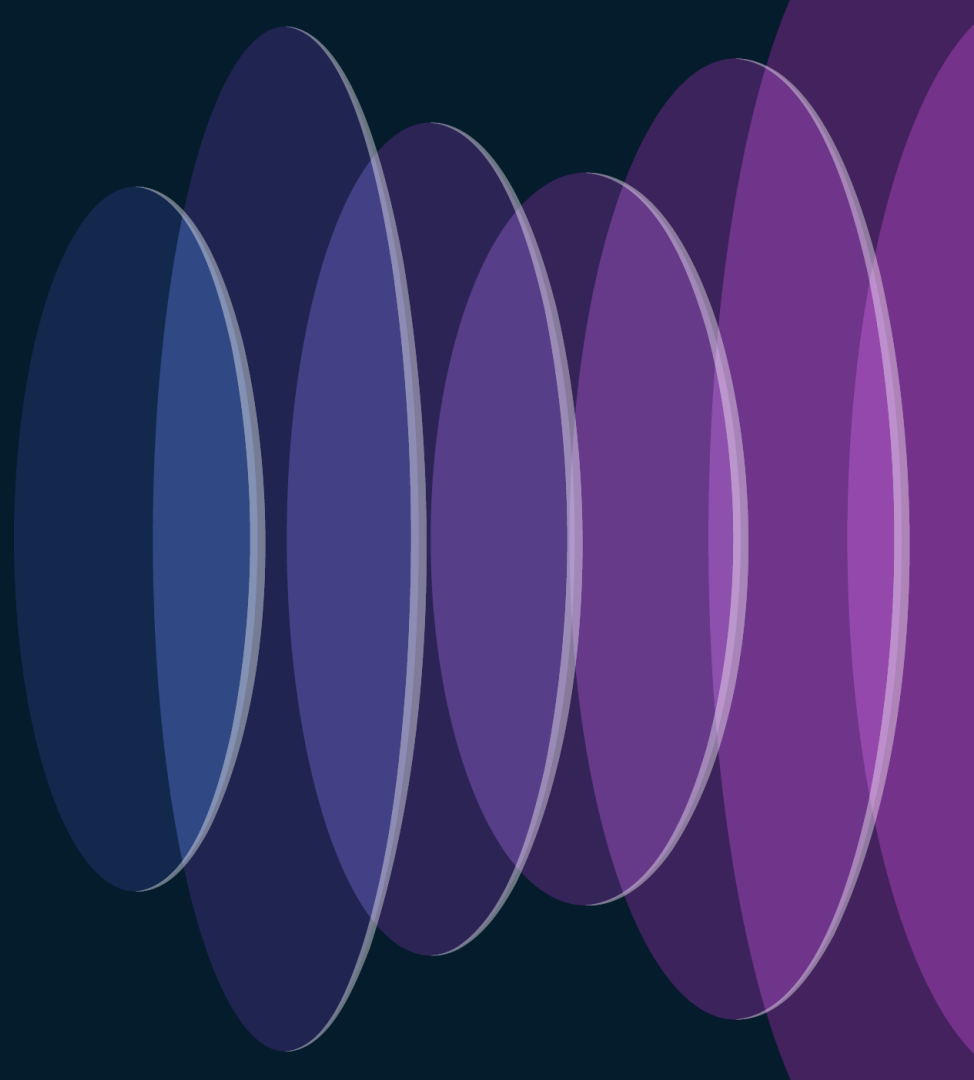


Consideration on Endpoints

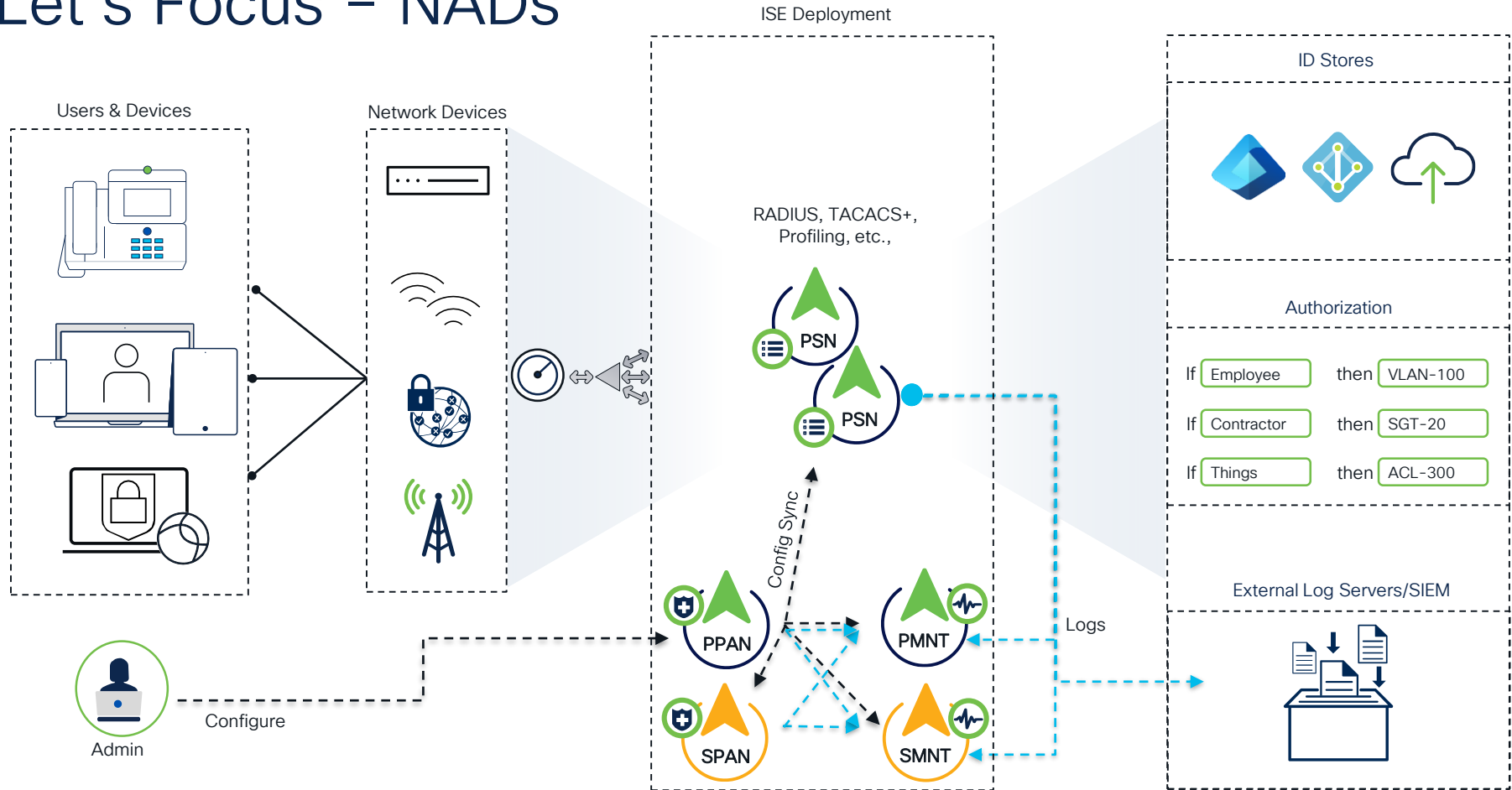
Max. Sessions

PSN Type	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Dedicated PSN (only PSN persona)	40,000	25,000	50,000	50,000	100,000	100,000	100,000
Shared PSN (multiple personas)	20,000	12,500	25,000	25,000	50,000	50,000	50,000

Network Devices



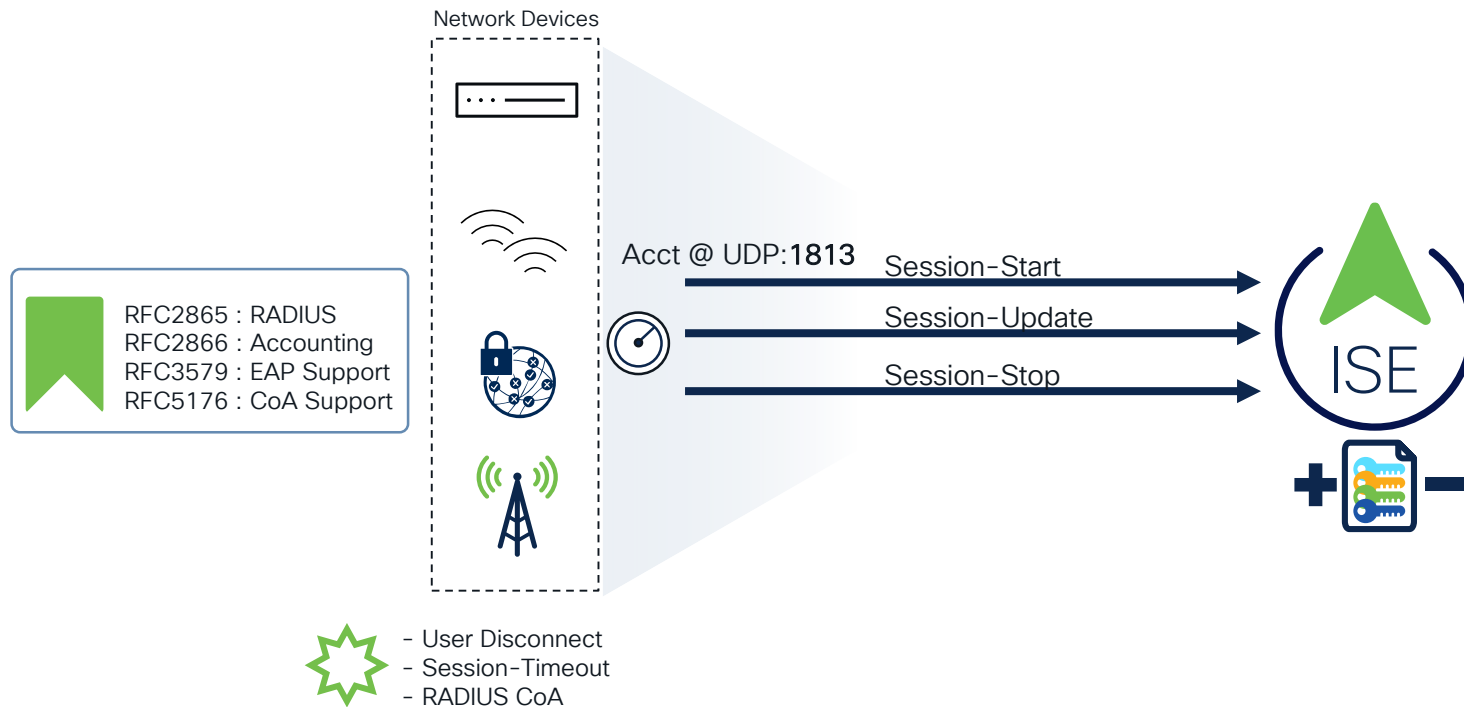
Let's Focus – NADs



Network Devices – Recommendations

Best Practices

Accounting – Start & Stop



Network Devices – Recommendations

Best Practices

Accounting – update



```
aaa authentication login default local
aaa authentication dot1x default group ise
aaa autho
aaa autho
aaa autho
aaa autho
aaa autho
aaa accou
aaa accou
aaa accou
aaa accou
```

Cisco Catalyst 9800-CL Wireless Controller
17.11.1

Welcome admin

Configuration > Security > AAA

Edit AAA Server Group

AAA Server Group: ISE
Protocol: RADIUS
Accounting Mode: ☐ Simultaneous ☒ Single
Reactivation Mode: ☒ Depletion ☐ Timed
Dead Time: 10 minutes
Max Failed Attempts: 3

☒ Enable interim accounting update
☒ Update Interval: 24 Hours
☐ Enable Active Directory Agent mode

Tune Wired NAD Configuration

Best Practices

Rate Limiting at **Wired** Source



```
interface GigabitEthernet1/0/14
description "this is connected to endpoints"
switchport access vlan 105
switchport mode access
device-tracking attach-policy IPDT_POLICY
ip flow monitor monitor-in input
ip flow monitor monitor-out output
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate 7200
authentication timer inactivity 3600
mab
snmp trap mac-notification change added
snmp trap mac-notification change removed
snmp trap link-status permit duplicates
dot1x pae authenticator
dot1x timeout quiet-period 300
dot1x timeout tx-period 10
dot1x timeout ratelimit-period 300
dot1x timeout held-period 300
service-policy input remotedesktop
ip nbar protocol-discovery
ip dhcp snooping trust
end
```

9800 WLC Client Exclusions

Configuration > Security > Wireless Protection Policies

Rogue Policies Rogue AP Rules **Client Exclusion Policies**

Select all events	<input checked="" type="checkbox"/>
Excessive 802.11 Association Failures	<input checked="" type="checkbox"/>
Excessive 802.1X Authentication Failures	<input checked="" type="checkbox"/>
Excessive 802.1X Authentication Timeout	<input checked="" type="checkbox"/>
IP Theft or IP Reuse	<input checked="" type="checkbox"/>
Excessive Web Authentication Failures	<input checked="" type="checkbox"/>

Configuration > Tags & Profiles > Policy

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec)	<input type="text" value="3600"/>	<i>Info</i>
Idle Timeout (sec)	<input type="text" value="300"/>	
Idle Threshold (bytes)	<input type="text" value="0"/>	
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="120"/>	

9800 WLC Client Exclusions

Tweaking EAP Timers

- Clients excluded on
 - 6th 802.1x failure
 - 5th 802.1x timeout
- Advanced EAP timers should be tweaked to allow exclusion before client restarts.

Configuration > Security > **Advanced EAP**

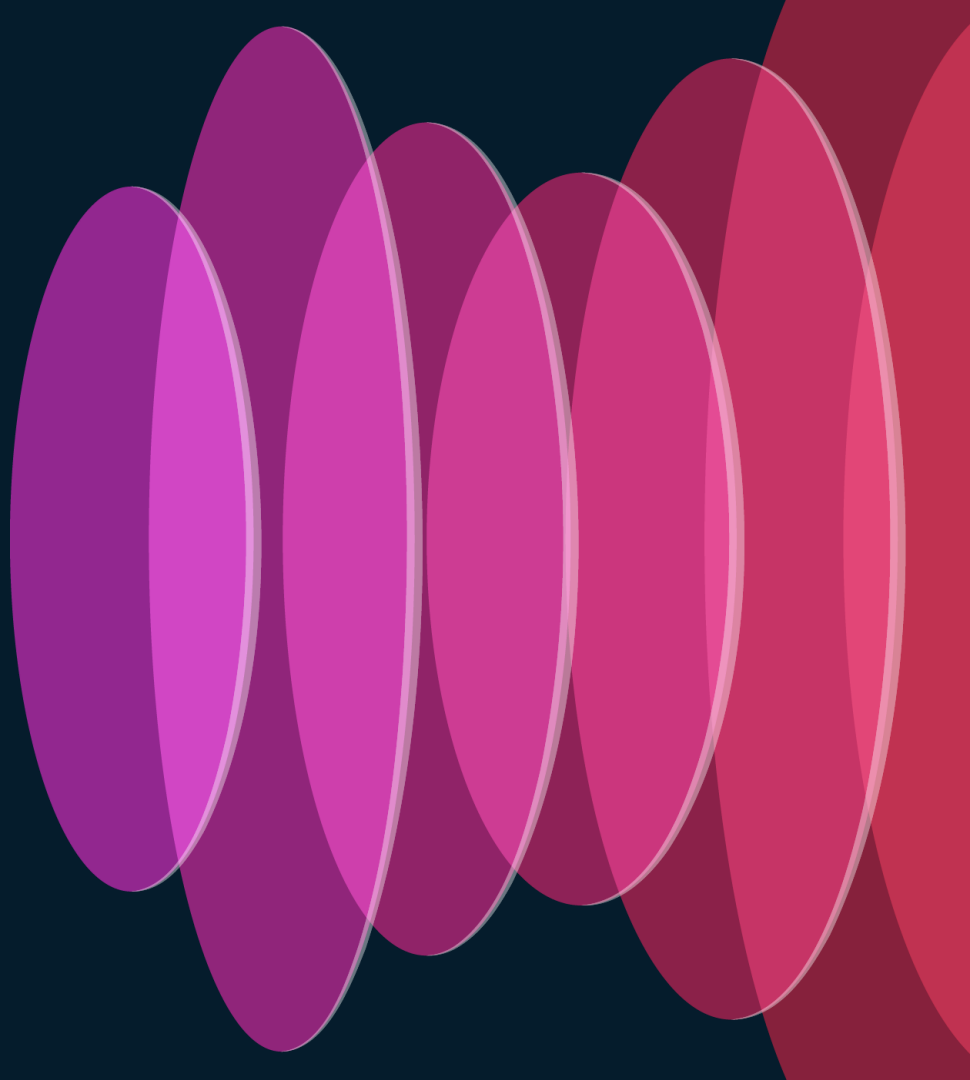
EAP-Identity-Request Timeout (sec)*	5
EAP-Identity-Request Max Retries*	5
EAP Max-Login Ignore Identity Response	<input checked="" type="checkbox"/> DISABLED
EAP-Request Timeout (sec)*	5
EAP-Request Max Retries*	5
EAPOL-Key Timeout (ms)*	1000
EAPOL-Key Max Retries*	2
EAP-Broadcast Key Interval (sec)*	3600

Number of RADIUS Servers

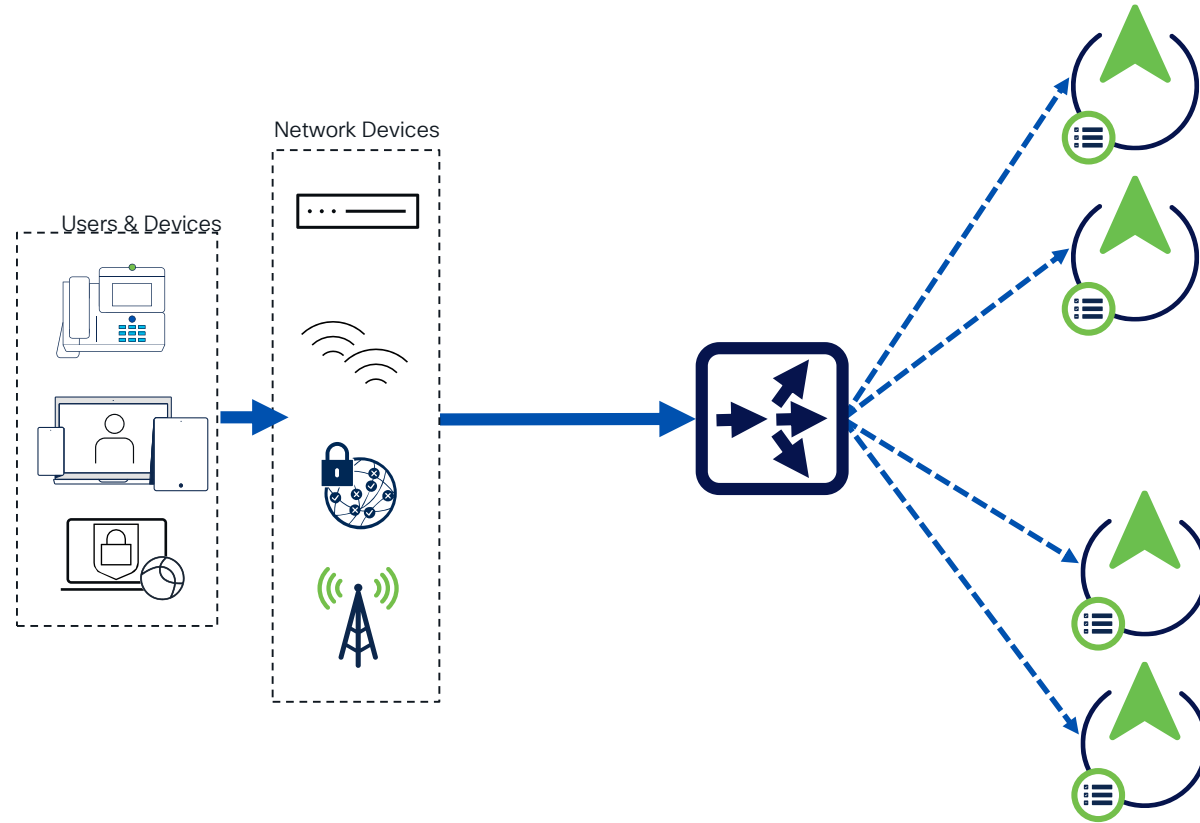
Best Practices

- Keep it to **3 or less**
- 3 retries at 5 seconds means 15 seconds per server.
- Devices won't wait long enough to make more worth while.
- More adds more chance for cascading failures.
- Need more? Add a load balancer!
- Use a **dead timer** of 10 minutes or more.
 - If all servers are exhausted the top server will be tried before the deadtime expires.

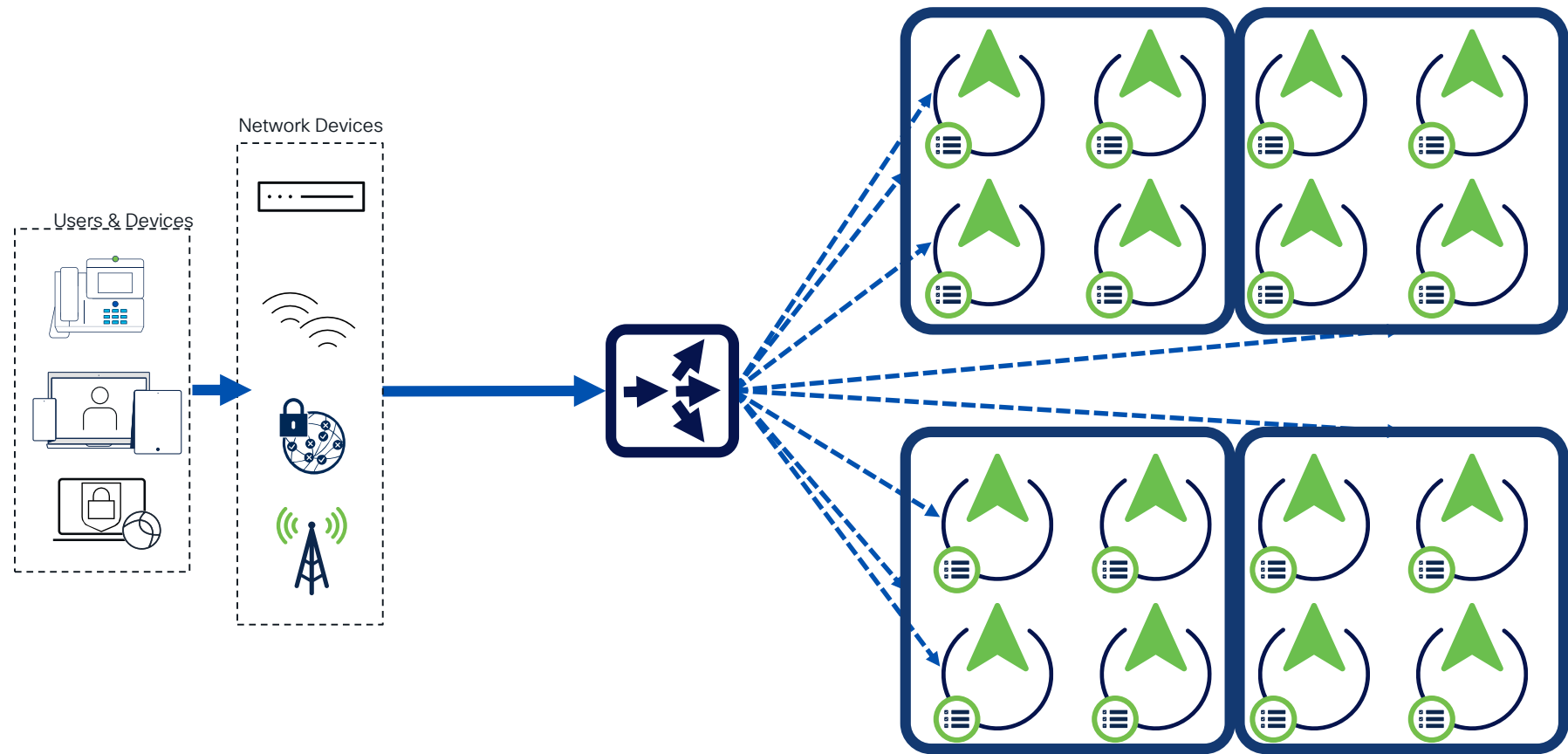
Load Balancing



Load Balancing to multiple PSNs



Load Balancing to multiple PSN groups



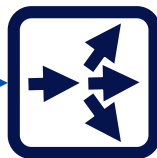
Load Balancing to multiple PSN groups

VIP = Virtual IP

Network Devices



192.168.102.105

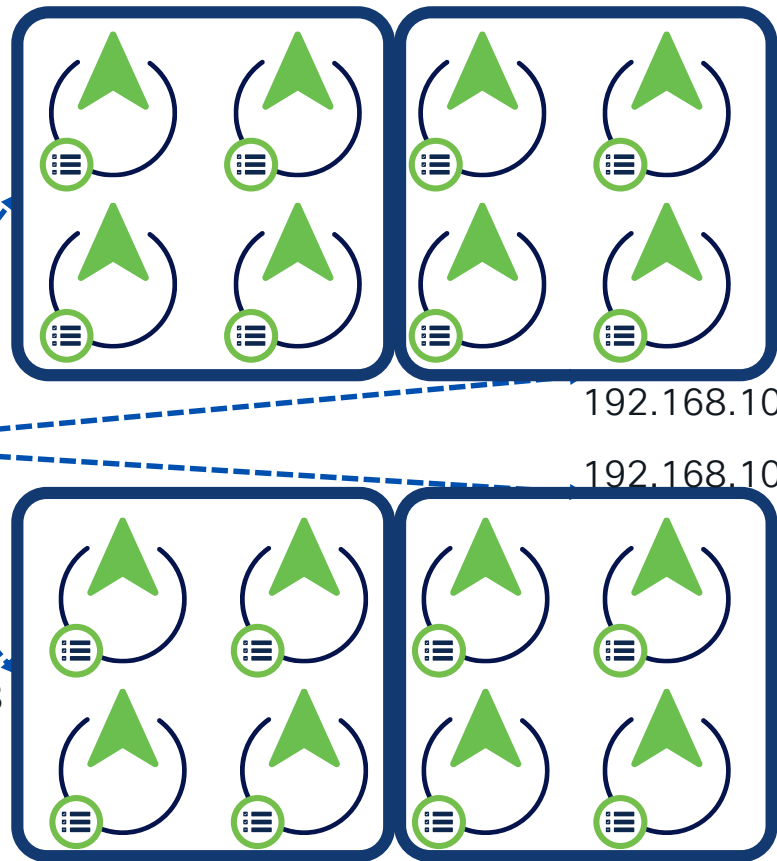


192.168.102.106

192.168.102.107

192.168.102.108

192.168.102.105:1812
192.168.102.106:1812
192.168.102.107:1812
192.168.102.108:1812



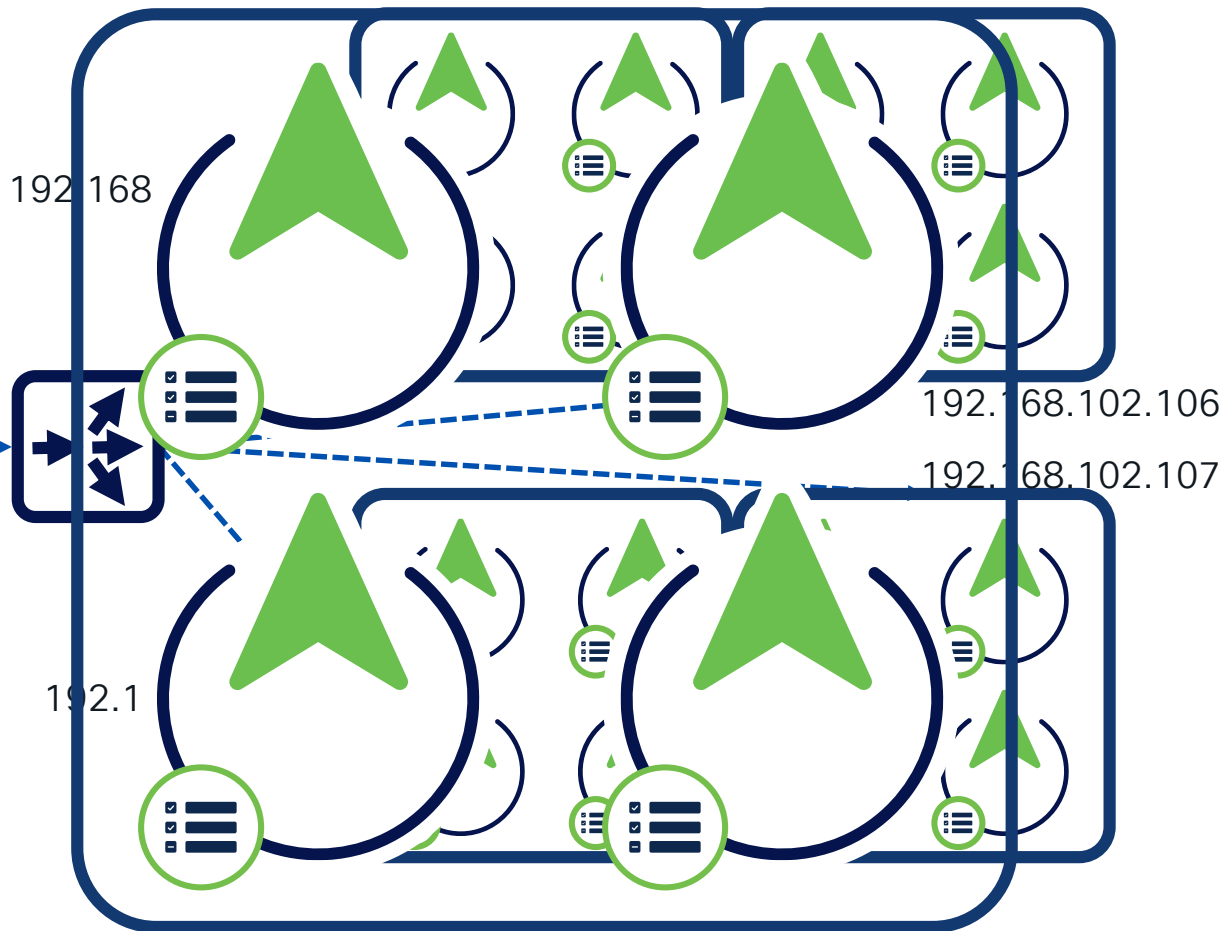
Load Balancing to multiple PSN groups

VIP = Virtual IP

Network Devices

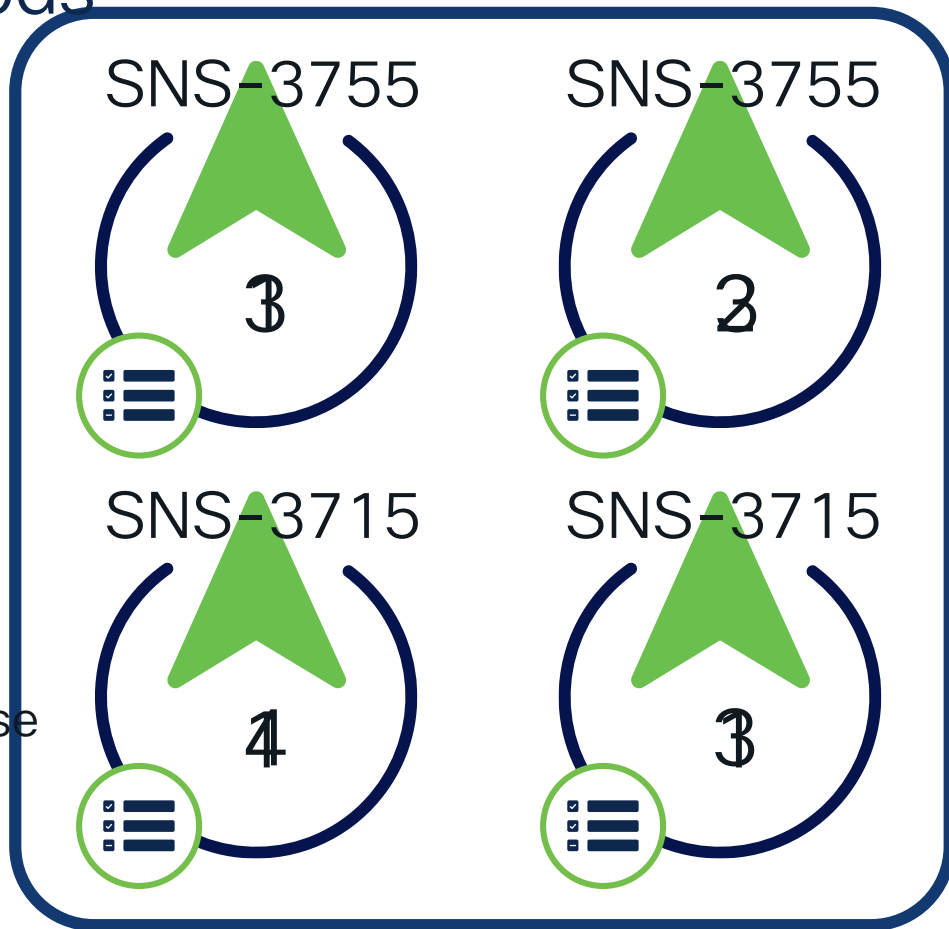


192.168.102.105:1812
192.168.102.106:1812
192.168.102.107:1812
192.168.102.108:1812



Load Balancing Methods

- RR** Round Robin
- WRR** Weighted Round Robin
- #** Hash
- L-#** Least # of connections
 - `least_time first_byte`
- LtC** Least time to connect
 - `least_time first_byte`
- LtR** Least time to receive response
 - `least_time last_byte`
- ?R?** Random



Health Checks

Health Checks keep monitoring the health of servers

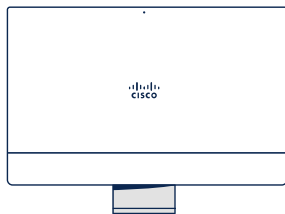
If a server is unresponsive or returns errors, the server is marked dead and is removed from the load balancer rotation pool

If a server has recovered and returns proper responses, it will be added back to the load balancer rotation pool



Session Persistence

Load Balancing Algorithms



Source
NAT



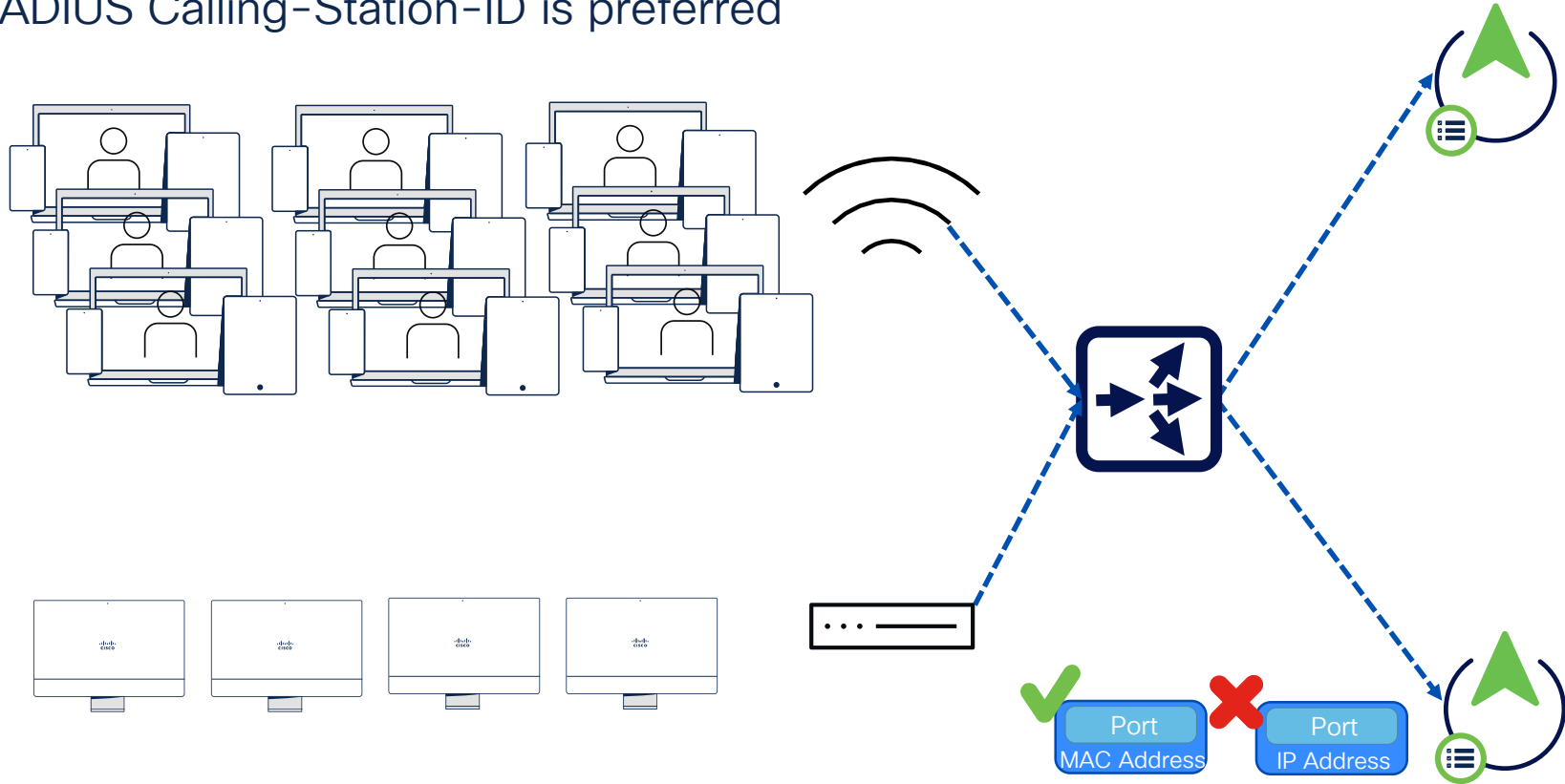
- Persistence/Affinity/Stickiness - Must
- RADIUS Calling-Station-ID:Source Port (or)
- RADIUS Calling-Station-ID:Source Port:Protocol

```
> aaa server radius dynamic-author
> client 192.168.100.4 server-key ISEisC00L
> client 10.1.100.25 server-key ISEisC00L
```

Session Persistence – IP vs MAC

RADIUS Calling-Station-ID is preferred

Best Practices



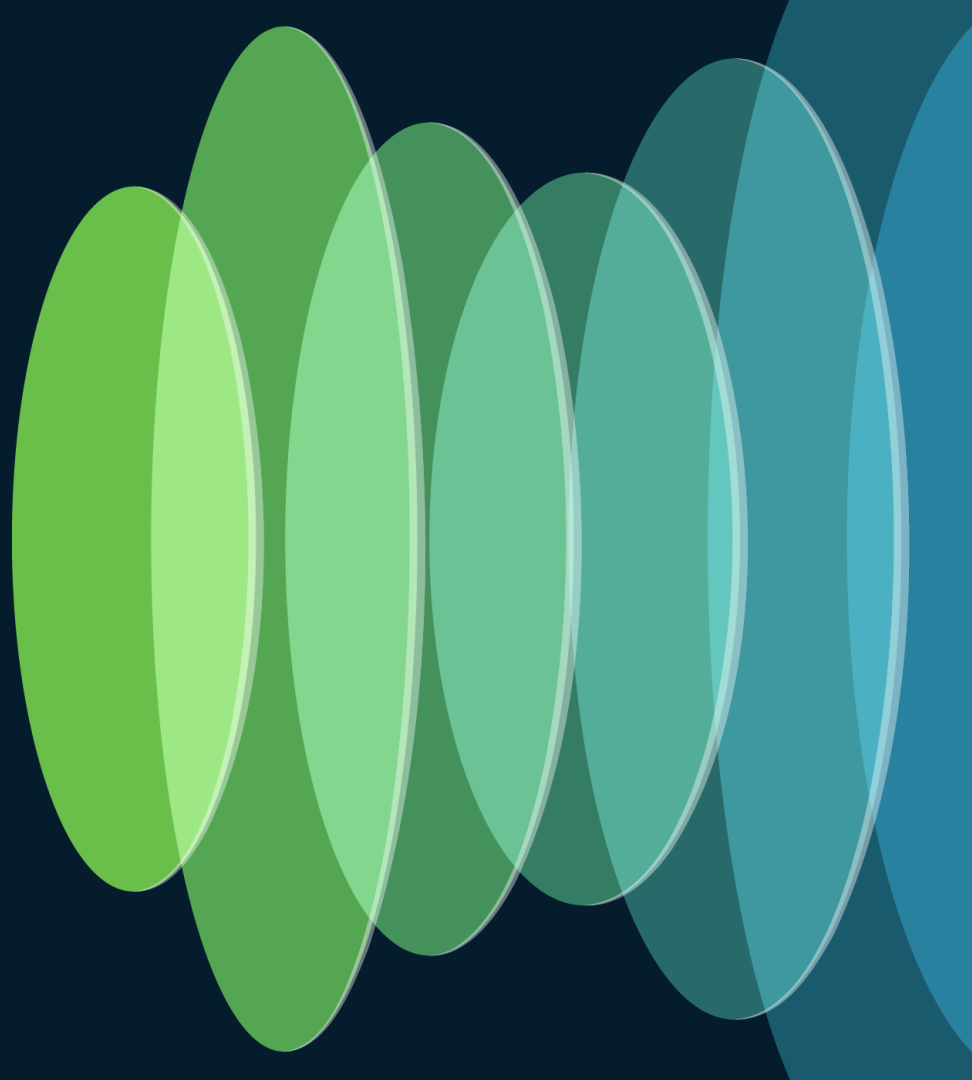
Load Balancer for ISE Best Practice Check List

- Persistence (**Stickyness**) is a must!
- Persistence based on **Calling-Station-ID** is best
- **DO NOT** Round Robin Traffic
- Use the **vendor specific guides** from the community:

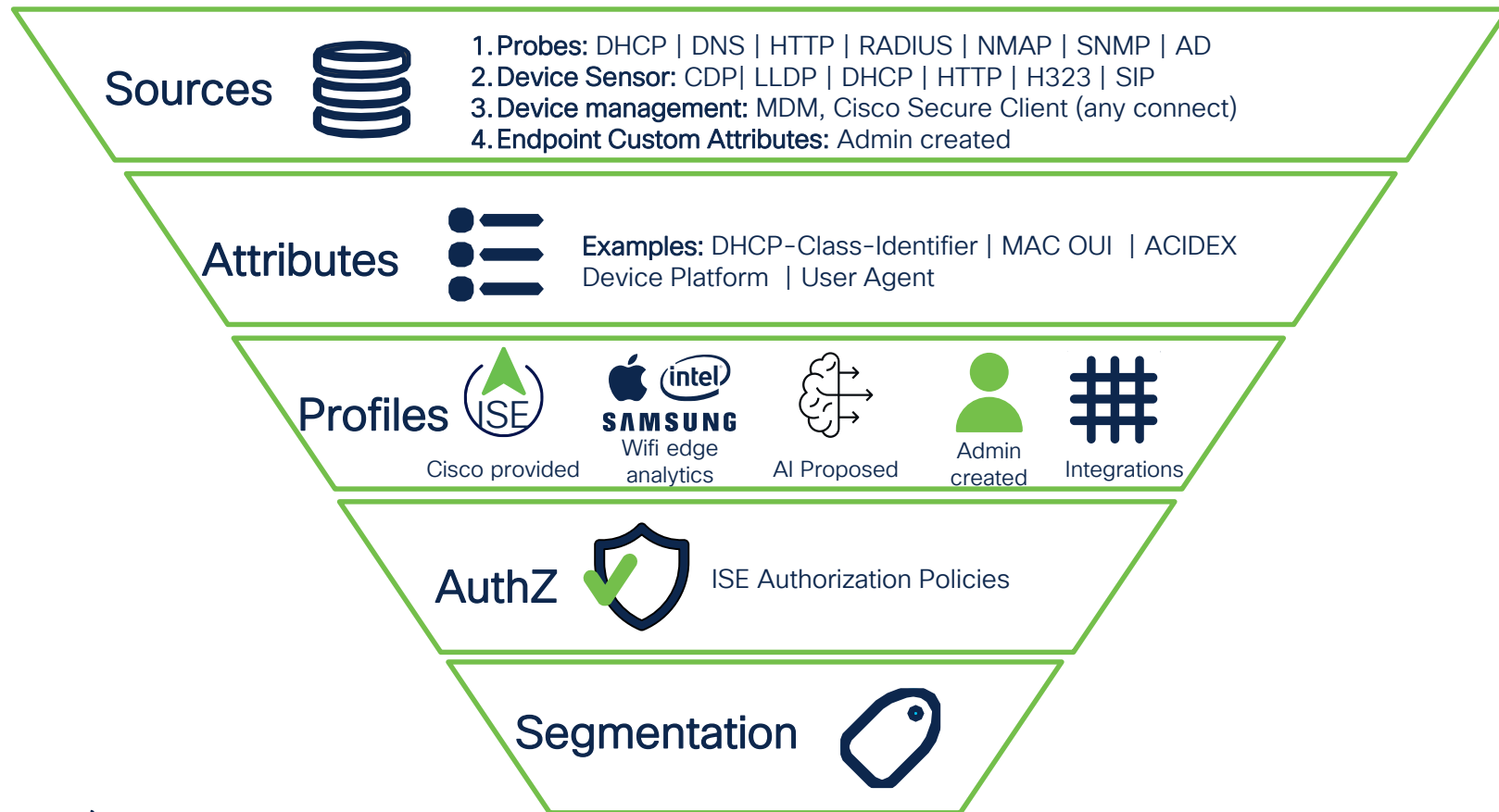


Best Practices

Profiling



Turning Probes Into Profiles, Profiles Into Protection



Use Node Groups

Best Practices

Identity Services Engine

Administration / System

Evaluation Mode 89 Days



- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Help

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade

Health Checks

Backup & Restore

More

☐ Dedicated MnT

Defaults



Policy Service



Enable Session Services

Include Node in Node Group

None



Enable Profiling Service



Enable Threat Centric NAC Service



> Enable SXP Service



Enable Device Admin Service



Enable Passive Identity Service



pxGrid

Node groups are regional PSN clusters

ISE Profiling Probes

Identity Services Engine Administration / System

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Deployment Licensing Certificates Logging Maintenance Upgrade Health Check

Deployment

Deployment Nodes List > iseee

Edit Node

General Settings **Profiling Configuration**

NETFLOW

DHCP Interface

GigabitEthernet 0

67

Description

The DHCP probe listens for

NETFLOW

DHCP

DHCPSPAN

HTTP

RADIUS

Network Scan (NMAP)


DNS

SNMPQUERY

SNMPTRAP

Active Directory

pxGrid



Do not turn on all probes thinking “more is better” without understanding their potential performance impact!

Profiling Probe Selection Best Practices

Probe	Key Profiling Attributes
RADIUS	MAC Address (OUI), IP Address, NDG values
RADIUS w/Device Sensor	CDP/LLDP, DHCP, User-Agent, mDNS, H323/SIP
RADIUS w/ACIDex	MAC Address (OUI), UDID, Operating System, Platform/Device Type
SNMP	MAC Address (OUI), CDP/LLDP, ARP tables
DHCP	DHCP
DNS	FQDN
HTTP	User-Agent
NetFlow	Protocol, Source/Dest IP, Source/DestPorts
NMAP	OS, Common and custom ports, Service Version Info, SMB & SNMP data
AD	Operating System and Version, AD Domain
pxGrid	IoT Asset, Custom Attributes
Custom Attributes	Customer defined

Use WiFi Edge Analytics

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

Enable

- ☒ RADIUS Profiling
- ☒ HTTP TLV Caching
- ☒ DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

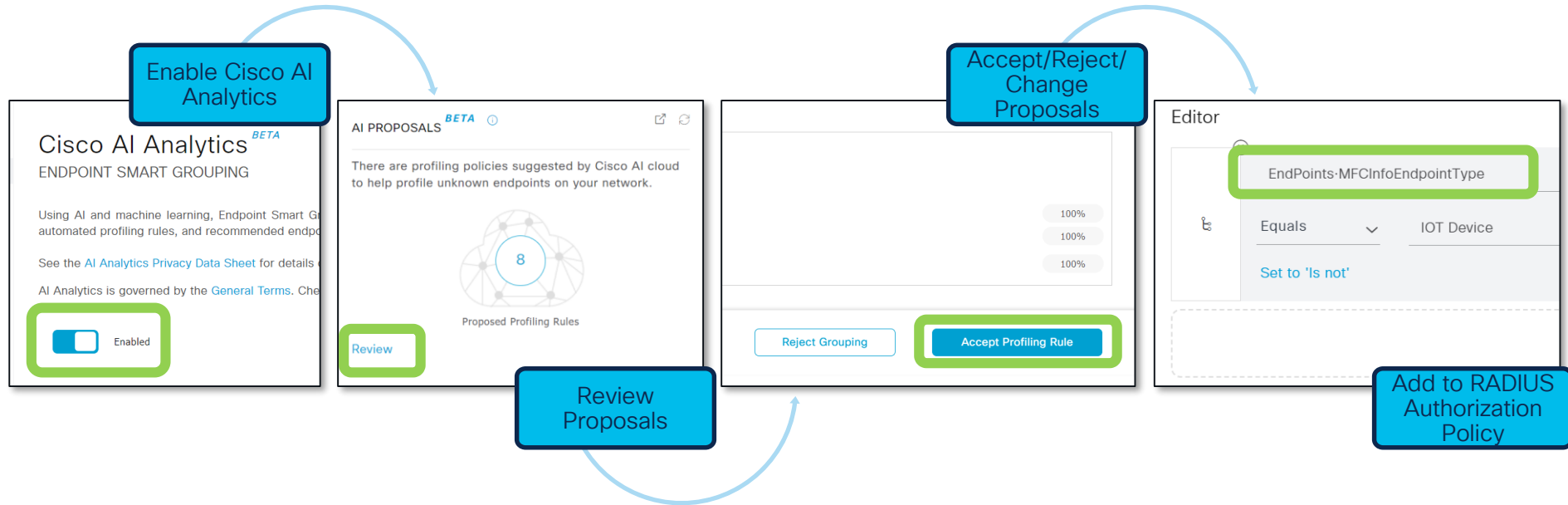
URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Best Practices

Cisco AI Analytics Simplifies the Profiling Process



Recommendations

References

- ISE YouTube Channel
[cs.co/ise-videos](https://www.cisco.com/ise-videos)
- ISE Resources
[cs.co/ise-resources](https://www.cisco.com/ise-resources)
- ISE Webinars
[cs.co/ise-webinars](https://www.cisco.com/ise-webinars)
- ISE Community
[cs.co/ise-community](https://www.cisco.com/ise-community)
- ISE Integration Guides
[cs.co/ise-guides](https://www.cisco.com/ise-guides)
- Network Access Device Capabilities
[cs.co/nad-capabilities](https://www.cisco.com/nad-capabilities)
- ISE Comptability
[cs.co/ise-compatibility](https://www.cisco.com/ise-compatibility)
- ISE Licensing & Evaluations
[cs.co/ise-licensing](https://www.cisco.com/ise-licensing)

Catalyst Leadership in Enterprise Networks

A Platform based Approach

Catalyst Center and Meraki Dashboard

28M Network Devices Managed
 ↑ 50% Y/Y 19M APs | 6M Switches | 2.5M Routers | 830M Clients

13M
 Devices on
 Catalyst Center



15.3M
 Devices on
 Meraki Dashboard



Catalyst 9000 Family



100,000+ Customers, Millions of Switches

“Catalyst 9K continues to be the fastest ramping product in the company's history”
 - Chuck Robbins, CEO Cisco Systems

cisco Live!

Secure Networking

Common Policy

Secure Equipment Access

SD-Access (LISP & EVPN)

High-speed Encryption

Digital Experience

Campus Automation

AI Endpoint Analytics

Digital Experience ThousandEyes

AI Ops & Assurance

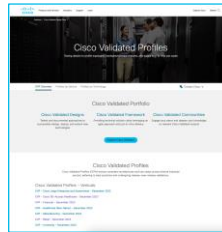
Operational Simplicity

Cloud Managed Catalyst

Infrastructure as a Code

S3 & CloudWatch Integration

Visibility, Control & Rollback



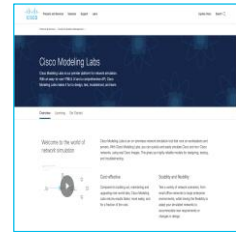
Cisco Validated Profiles (CVP)



Industry Validated Reports



Industry Certifications



Cisco Modeling Labs

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**.

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: pavagupt@cisco.com



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive