Possibilities

#CiscoLive

Advanced ISE
Architect, Design and Scale ISE for your production networks

Imran Bashir
Technical Marketing Engineer
BRKSEC-3432

A bit about your Speaker

- Imran Bashir
- Technical Marketing Engineer at Cisco Systems.
- ~10 Years with Cisco Systems
- Before Cisco Systems, Several Startups
- Focus on Enterprise Security Products
- Several Sessions and White Papers on Security topics

Cisco Security Experts ?

Cisco ISE Experts ?

AAA Port configurations ?

How many on ISE 2.4 ?

How many on ISE 2.6 ?

How many using SNS-35xx ?

500
100
0
1
2
3

Session Abstract

In today's world of constant attacks, malware and Ransomware, its important to design, deploy and manage your network with an identity aware secure access platform. Cisco ISE is plays an architectural role for many security solutions and is also one of the main pillars in the overall Cisco's Software defined Access Architecture.

This session will show you how to **deliver scalable and highly available access control services** using ISE for wired, wireless, and VPN from a single campus to a global deployment. Methodologies for **increasing scalability and redundancy** will be covered such as **load distribution** with and without load balancers, optimal profiling design, lessons learned from the trenches, as well as serviceability tips and tricks to help you gain optimal value and productivity from ISE.

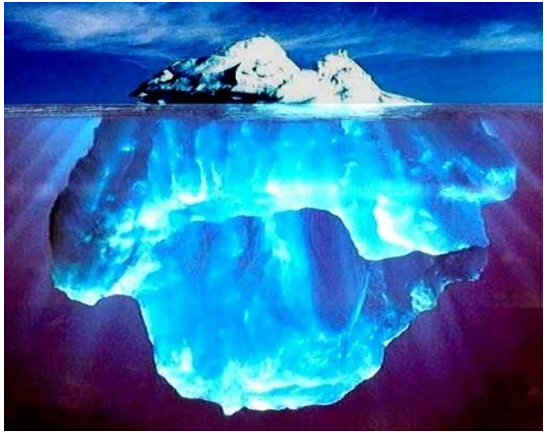
Attendees of this session will gain knowledge on how to best **design ISE** to ensure peak operational **performance, stability,** and to support large volumes of

Important: Hidden Slide Alert

Look for this “For Your Reference” Symbol in your PDF’s

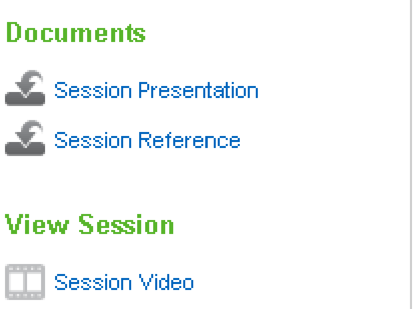
There is a tremendous amount of hidden content, for you to use later!

For Your Reference



~500 +/- Slides in Session Reference PDF

Available on ciscolive.com



Documents

Session Presentation

Session Reference

View Session

Session Video

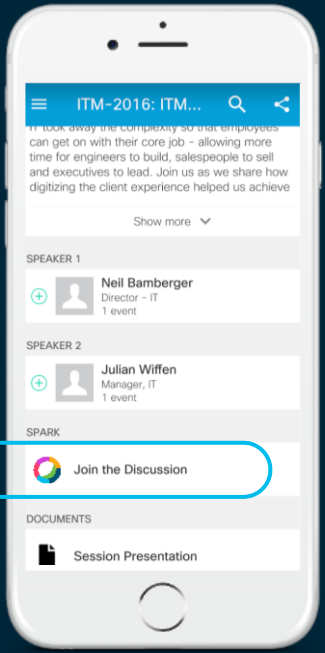
Cisco Webex Teams

Questions?

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

How

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



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

cs.co/ciscolivebot# 3432

Where can I get help after Cisco Live?

ISE Public Community	http://cs.co/ise-community

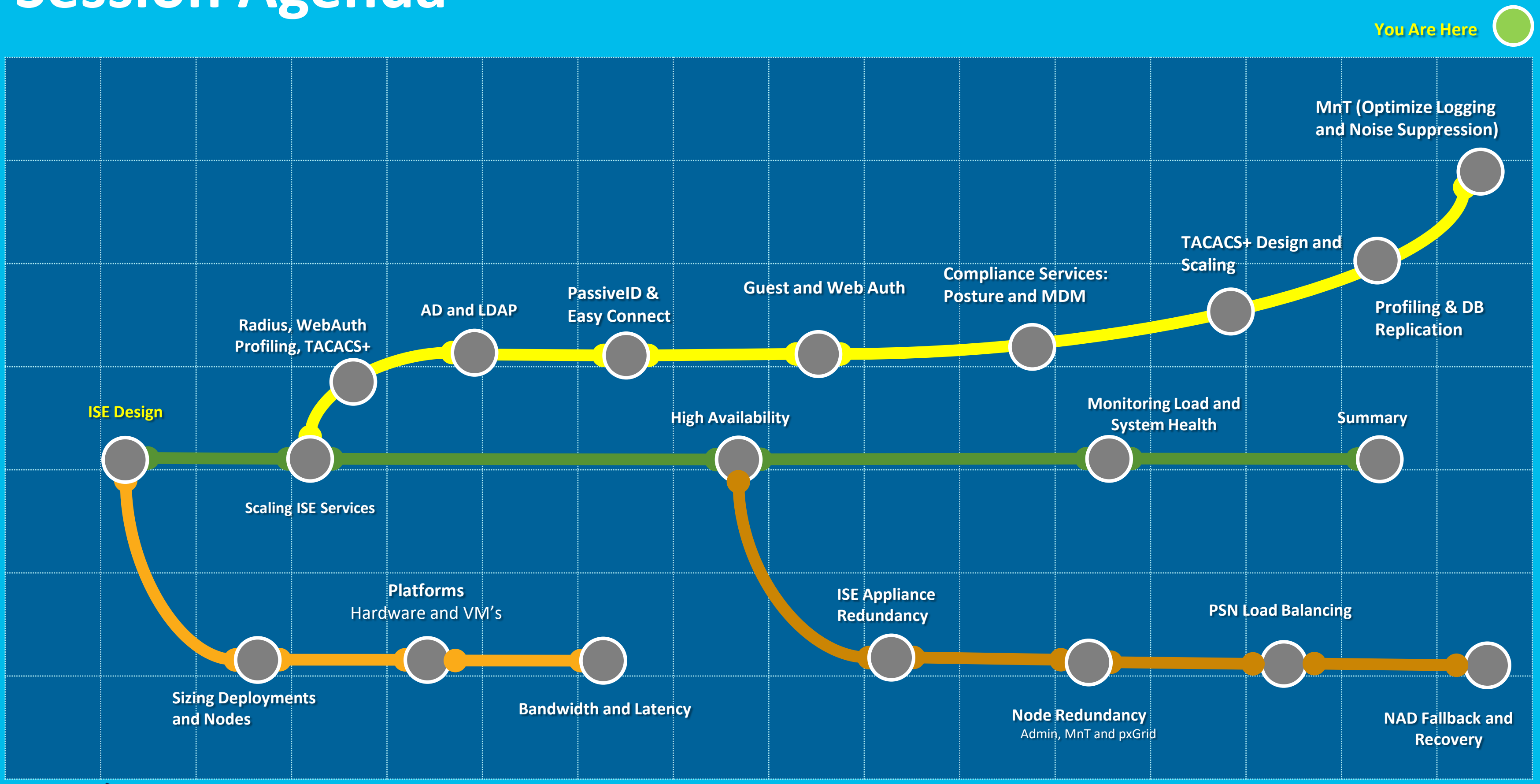
Questions answered by ISE TMEs and other Subject Matter Experts – the same persons that support your local Cisco and Partner SEs!

ISE Compatibility Guides	http://cs.co/ise-compatibility
ISE Design Guides	http://cs.co/ise-guides

Agenda

- ISE Design
- Sizing Deployments and Nodes
- Bandwidth and Latency
- Scaling ISE Services
  - RADIUS, AD/LDAP, Passive ID, Guest, Web Services, TACACS+
  - Profiling and Database Replication
  - MnT (Optimize Logging and Noise Suppression)
- High Availability
  - Appliance Redundancy
  - Admin, MnT, and pxGrid Nodes
  - Certificate Services Redundancy
  - PSN Redundancy with and without Load Balancing
  - NAD Fallback and Recovery
- Monitoring Load and System Health

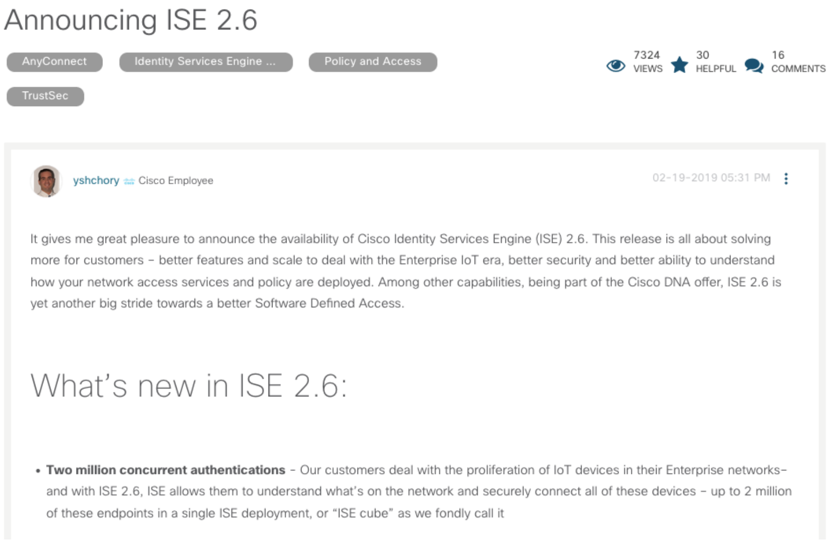
Session Agenda


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Announcing Cisco ISE 2.6

ISE 2.6 is the Long-term (LTR) “suggested release”

- https://community.cisco.com/t5/security-blogs/announcing-ise-2-6/ba-p/3805409
- https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/bulletin-c25-740738.html

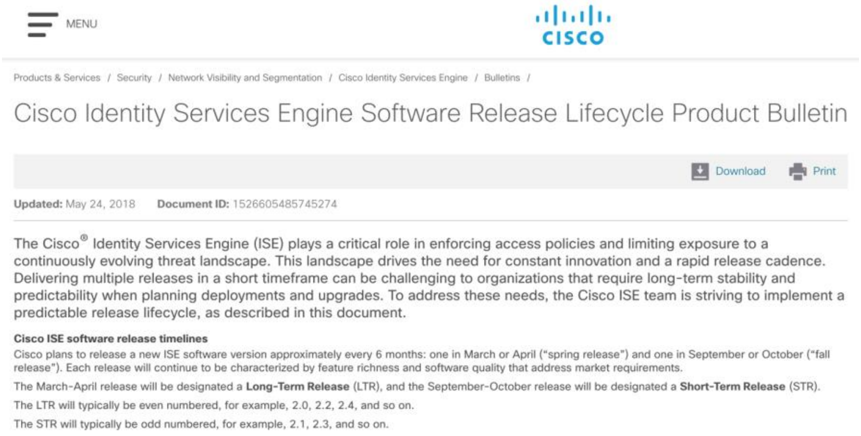


Announcing ISE 2.6

It gives me great pleasure to announce the availability of Cisco Identity Services Engine (ISE) 2.6. This release is all about solving more for customers – better features and scale to deal with the Enterprise IoT era, better security and better ability to understand how your network access services and policy are deployed. Among other capabilities, being part of the Cisco DNA offer, ISE 2.6 is yet another big stride towards a better Software Defined Access.

What’s new in ISE 2.6:

- **Two million concurrent authentications** – Our customers deal with the proliferation of IoT devices in their Enterprise networks– and with ISE 2.6, ISE allows them to understand what’s on the network and securely connect all of these devices – up to 2 million of these endpoints in a single ISE deployment, or “ISE cube” as we fondly call it



MENU
Products & Services / Security / Network Visibility and Segmentation / Cisco Identity Services Engine / Bulletins /
Download
Print

Cisco Identity Services Engine Software Release Lifecycle Product Bulletin

Updated: May 24, 2018 **Document ID:** 1526605485745274

The Cisco® Identity Services Engine (ISE) plays a critical role in enforcing access policies and limiting exposure to a continuously evolving threat landscape. This landscape drives the need for constant innovation and a rapid release cadence. Delivering multiple releases in a short timeframe can be challenging to organizations that require long-term stability and predictability when planning deployments and upgrades. To address these needs, the Cisco ISE team is striving to implement a predictable release lifecycle, as described in this document.

Cisco ISE software release timelines

Cisco plans to release a new ISE software version approximately every 6 months: one in March or April (“spring release”) and one in September or October (“fall release”). Each release will continue to be characterized by feature richness and software quality that address market requirements.

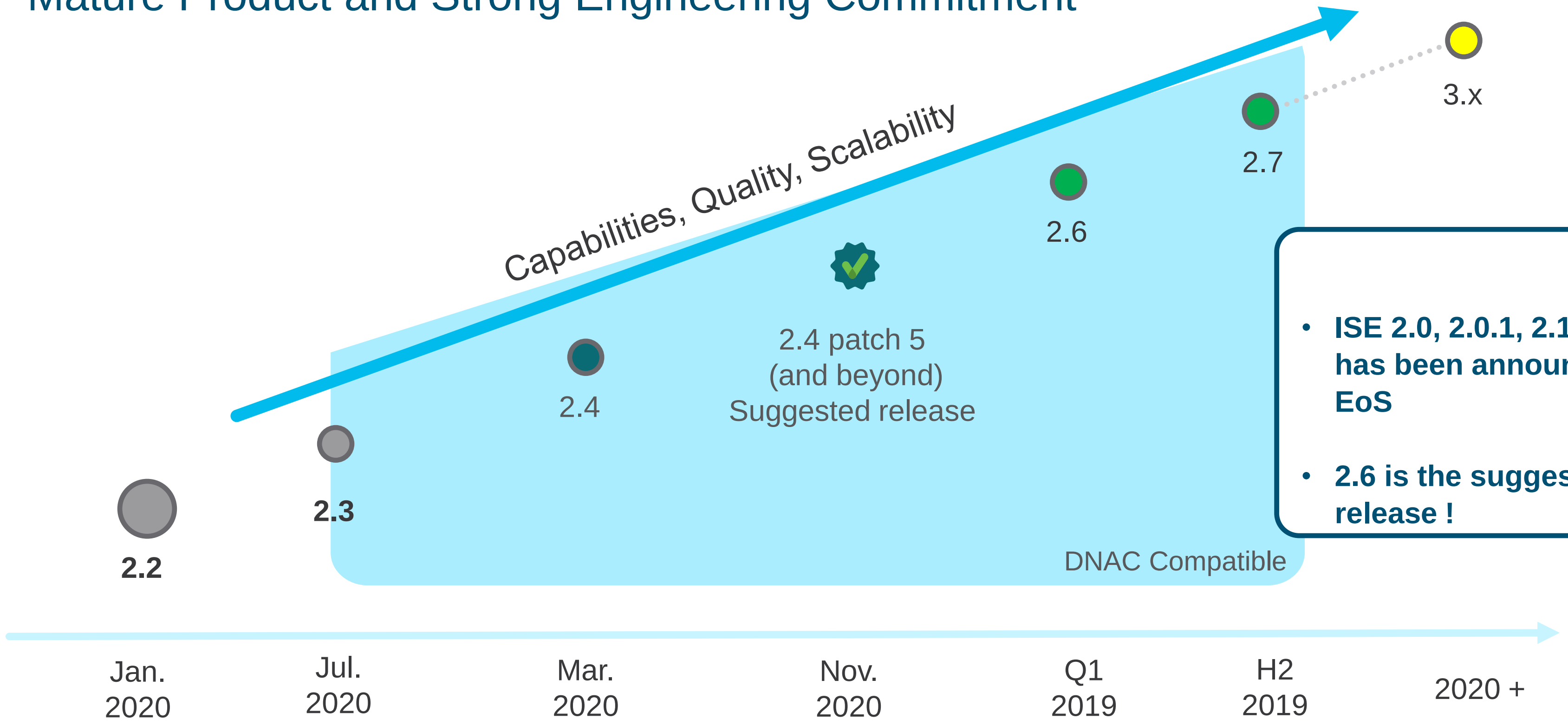
The March-April release will be designated a **Long-Term Release** (LTR), and the September-October release will be designated a **Short-Term Release** (STR).

The LTR will typically be even numbered, for example, 2.0, 2.2, 2.4, and so on.

The STR will typically be odd numbered, for example, 2.1, 2.3, and so on.

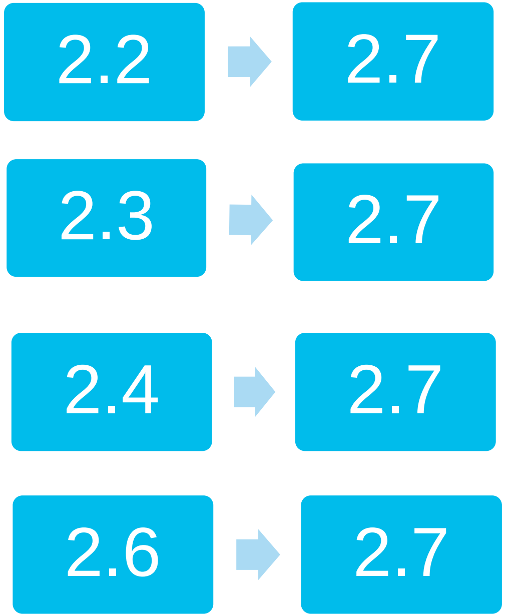
ISE Releases

Mature Product and Strong Engineering Commitment



- **ISE 2.0, 2.0.1, 2.1 & 2.3 has been announced EoS**
- **2.6 is the suggested release !**

Upgrade Paths Supported for ISE 2.7

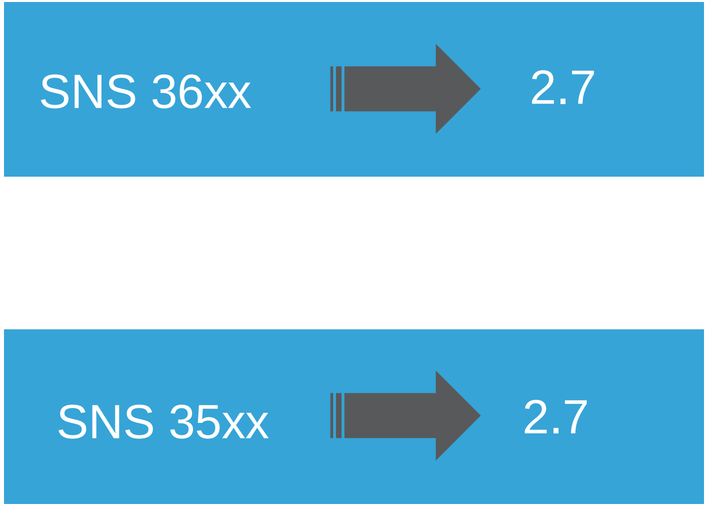


2.2 → 2.7

2.3 → 2.7

2.4 → 2.7

2.6 → 2.7

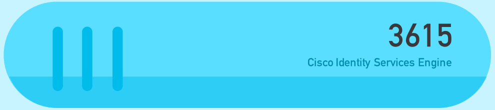


SNS 36xx → 2.7

SNS 35xx → 2.7

Faster, better appliances

New SNS-3600 Series hardware



SNS-3615

- 10,000 standalone sessions
- 10,000 PSN sessions

SNS-3655

- 25,000 standalone sessions
- 50,000 PSN sessions

SNS-3695

- 50,000 standalone sessions
- 100,000 PSN sessions

ISE Data Sheet and Ordering Guide

Policy Service Node (PSN)

Which Service has most impact on replication ?

Profiling

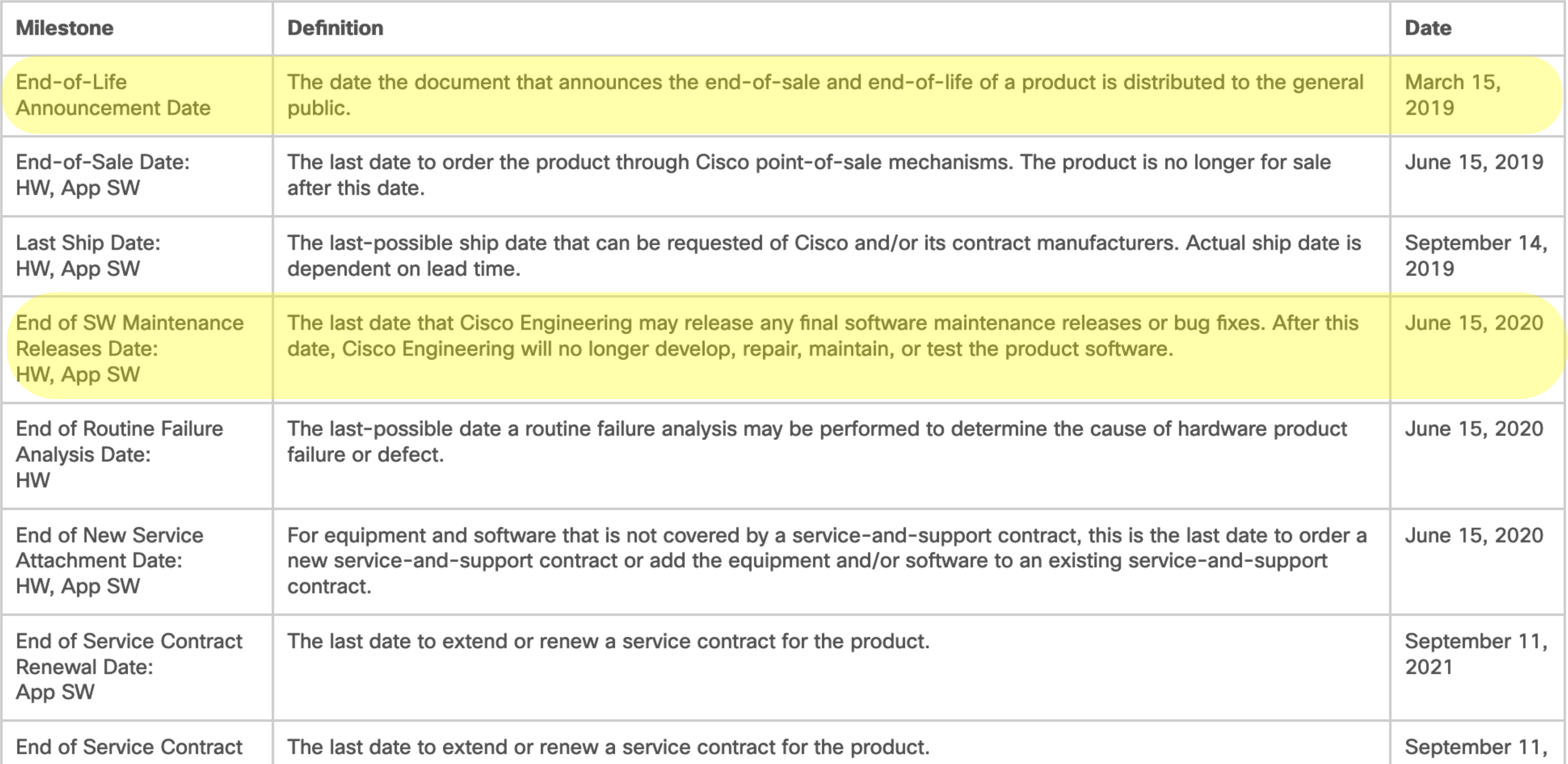
Guest Access Management

Device Administration

Access Control

BYOD & enterprise mobility

SNS-35xx EOL

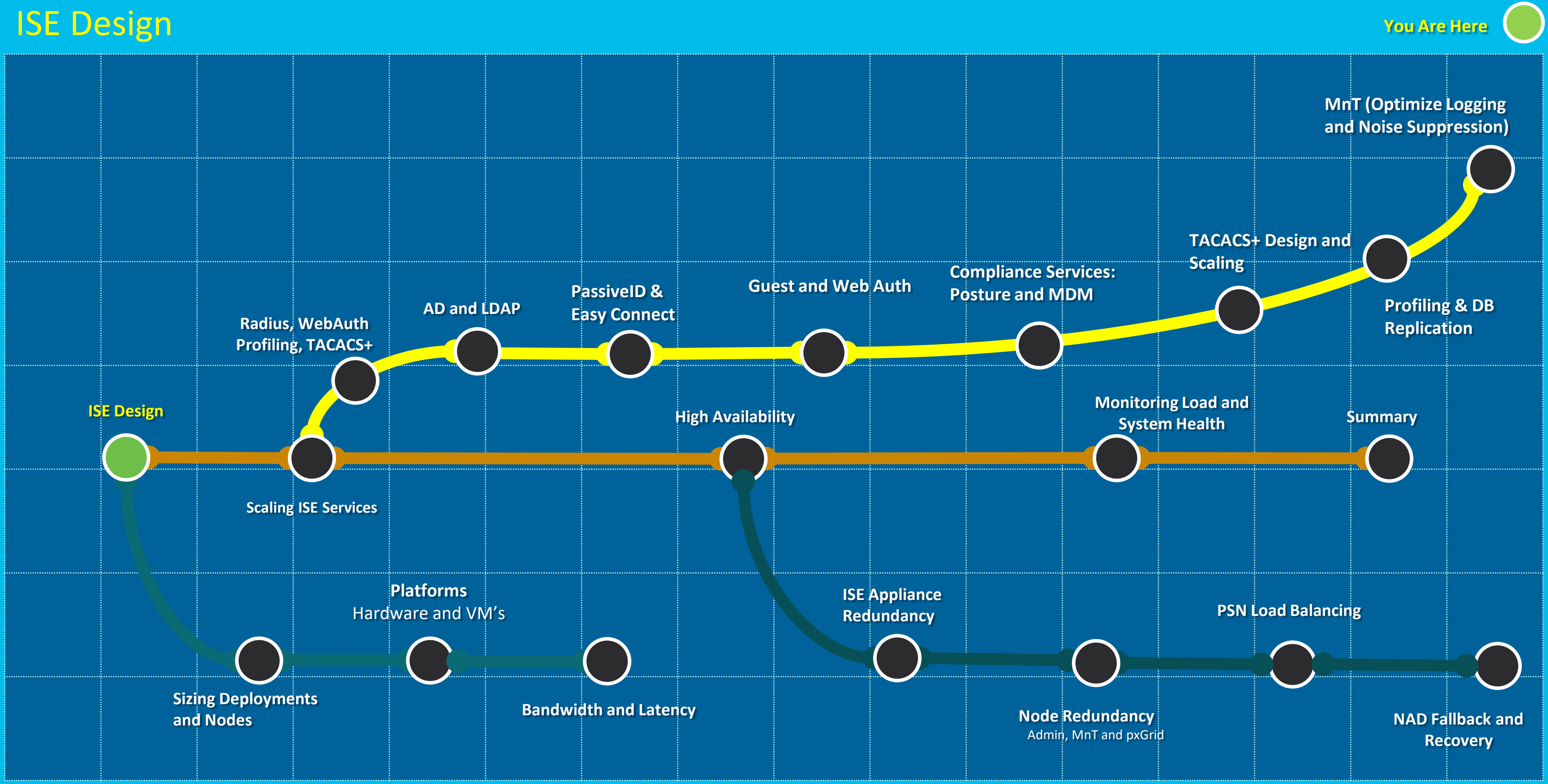


Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	March 15, 2019
End-of-Sale Date: HW, App SW	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	June 15, 2019
Last Ship Date: HW, App SW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	September 14, 2019
End of SW Maintenance Releases Date: HW, App SW	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.	June 15, 2020
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.	June 15, 2020
End of New Service Attachment Date: HW, App SW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	June 15, 2020
End of Service Contract Renewal Date: App SW	The last date to extend or renew a service contract for the product.	September 11, 2021
End of Service Contract	The last date to extend or renew a service contract for the product.	September 11,

ht

Session Agenda

ISE Design



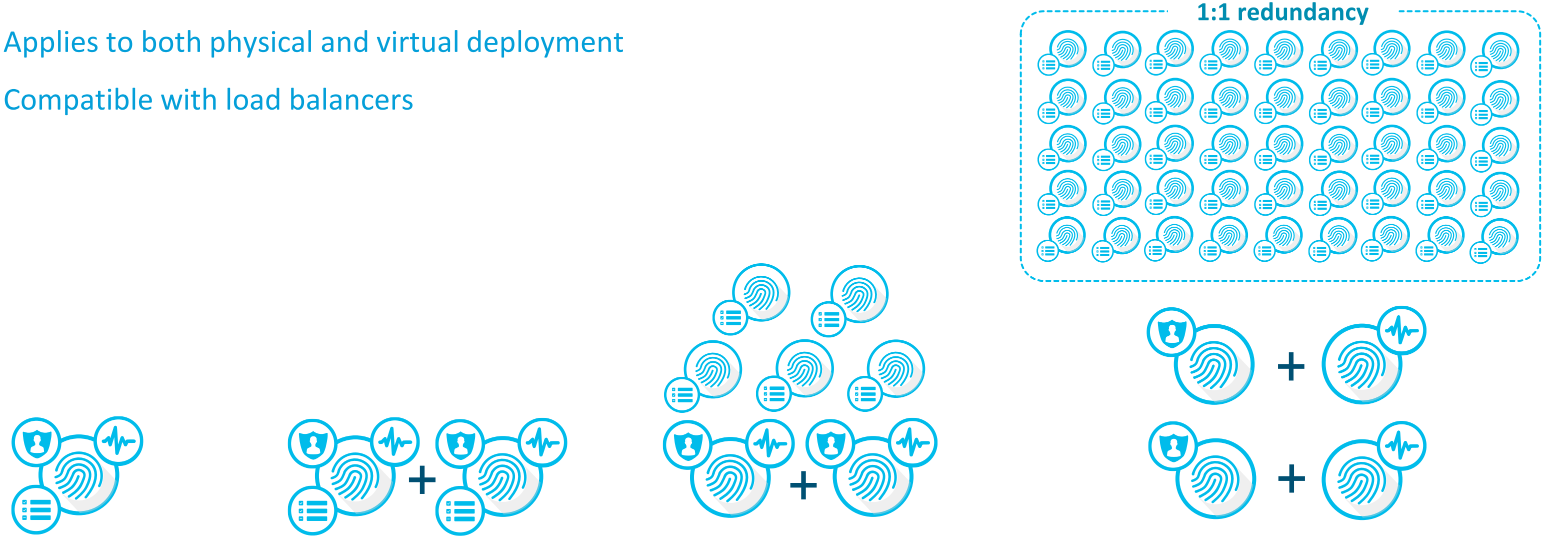
You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Cisco*live!*

ISE Design

Increased Scale with ISE 2.6 on 36xx

- Applies to both physical and virtual deployment
- Compatible with load balancers



Lab and Evaluation

Small HA Deployment
2 x (PAN+MNT+PSN)

Small Multi-node Deployment
2 x (PAN+MNT), <= 5 PSN

Large Deployment
2 PAN, 2 MNT, <=50 PSN

35xx	100 Endpoints	20,000 Endpoints	500,000 Endpoints
36xx	100 Endpoints	50,000 Endpoints	2,000,000 Endpoints(3695-PAN&MnT)

Platform Support

2.6 Will Be Supported on These Physical Appliances:

- (M4) Cisco SNS-3515-K9
- (M4) Cisco SNS-3595-K9
- (M5) Cisco SNS-3615-K9 - NEW
- (M5) Cisco SNS-3655-K9 - NEW
- (M5) Cisco SNS-3695-K9 - NEW

Virtual Appliances:

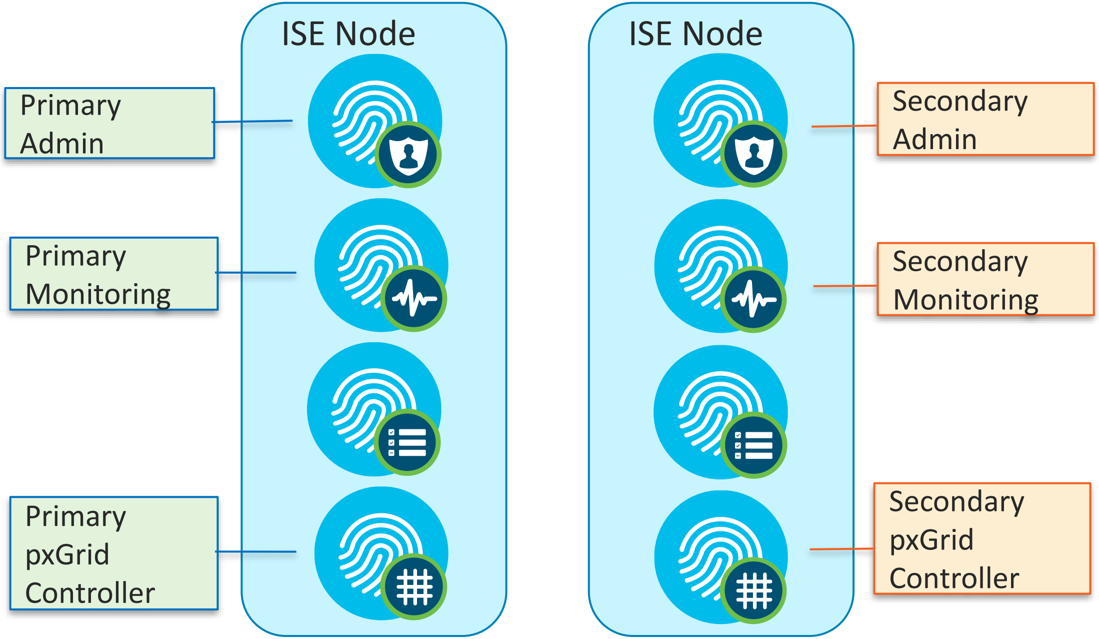
- Cisco R-ISE-VMS-K9=
- Cisco R-ISE-VMM-K9=
- Cisco R-ISE-VML-K9=

Virtual Appliance Operating Systems:

- VMWare
- Linux KVM – RHEL, Ubuntu
- Microsoft Hyper-V

Basic 2-Node ISE Deployment (Redundant)

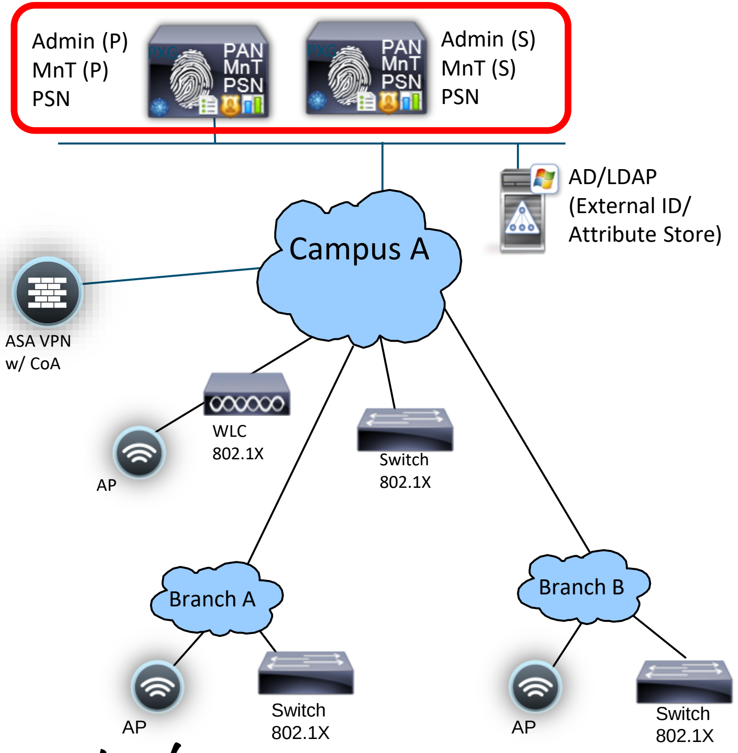
- Maximum sessions– 50,000 (platform dependent—same as standalone)
- Redundant sizing – 50,000 (platform dependent—same as standalone)



Basic 2-Node ISE Deployment (Redundant)

Maximum Sessions = 50,000 (Platform dependent) Centralized

For Your Reference



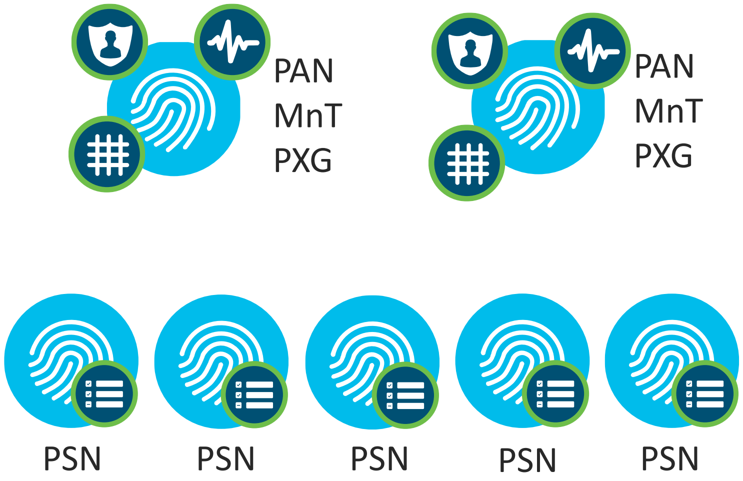
PSN

- All Services run on both ISE Nodes
- Set one for Primary Admin / Primary MnT
- Set other for Secondary Monitoring / Secondary Admin
- Max Sessions is platform dependent:
  - 3515 = Max 7.5k sessions
  - 3615 = Max 10k sessions
  - 3595 = Max 20k sessions
  - 3655 = Max 25k sessions
  - 3695 = Max 50k sessions

Hybrid-Distributed Deployment

Admin + MnT on Same Appliance; Policy Service on Dedicated Appliance

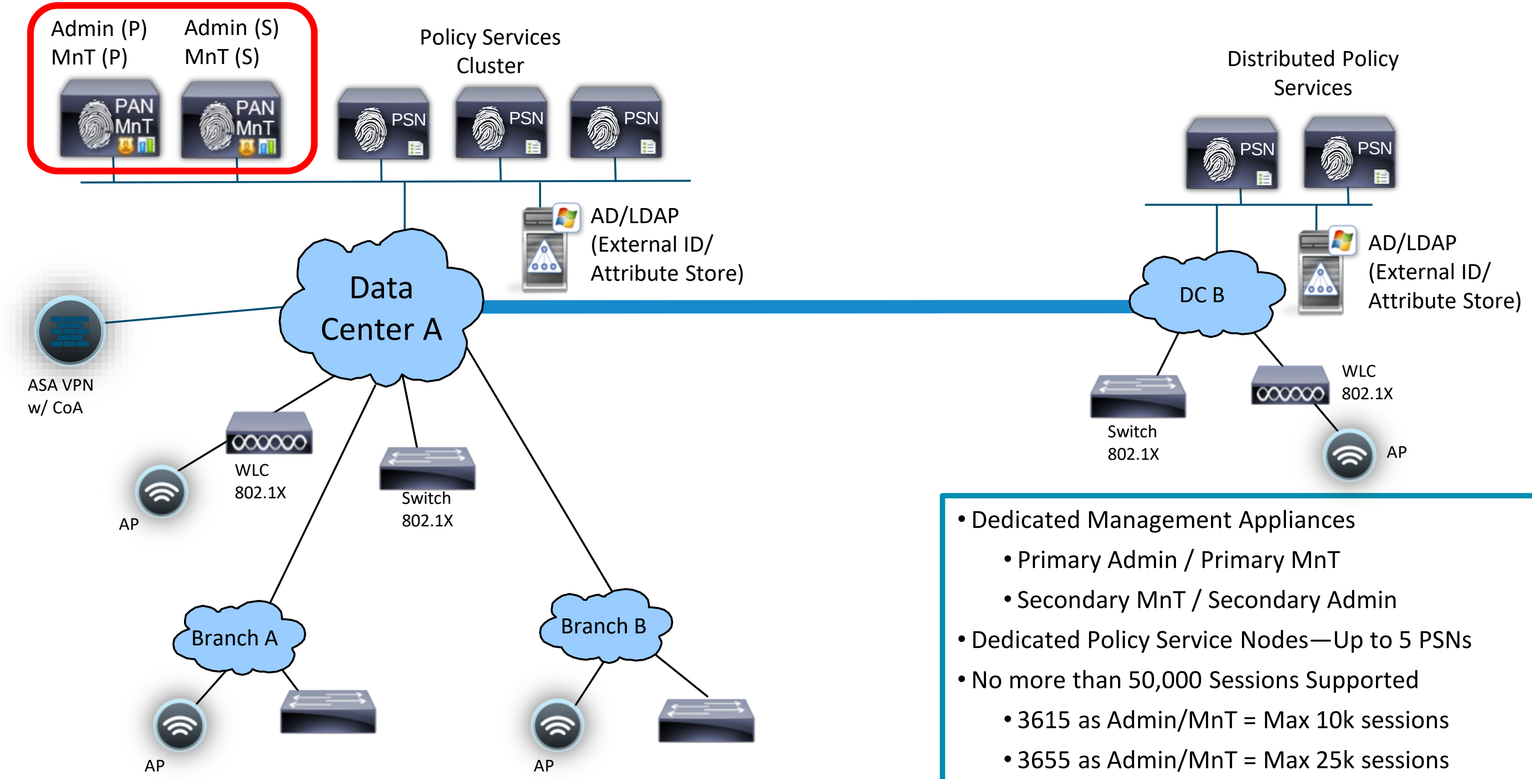
- 2 x Admin+Monitor+pxGRID
- Max 5 PSNs
  - Optional: Dedicate 2 of the 5 for pxGrid
- Max sessions – Platform dependent
  - 7,500 for 3515 as PAN+MnT
  - 10,000 for 3615 as PAN+MnT
  - 20,000 for 3595 as PAN+MNT
  - 25,000 for 3655 as PAN+MnT
  - 50,000 for 3695 as PAN+MnT



Basic Hybrid-Distributed Deployment

For Your Reference

Maximum Sessions = 50,000 / Maximum 5 PSNs

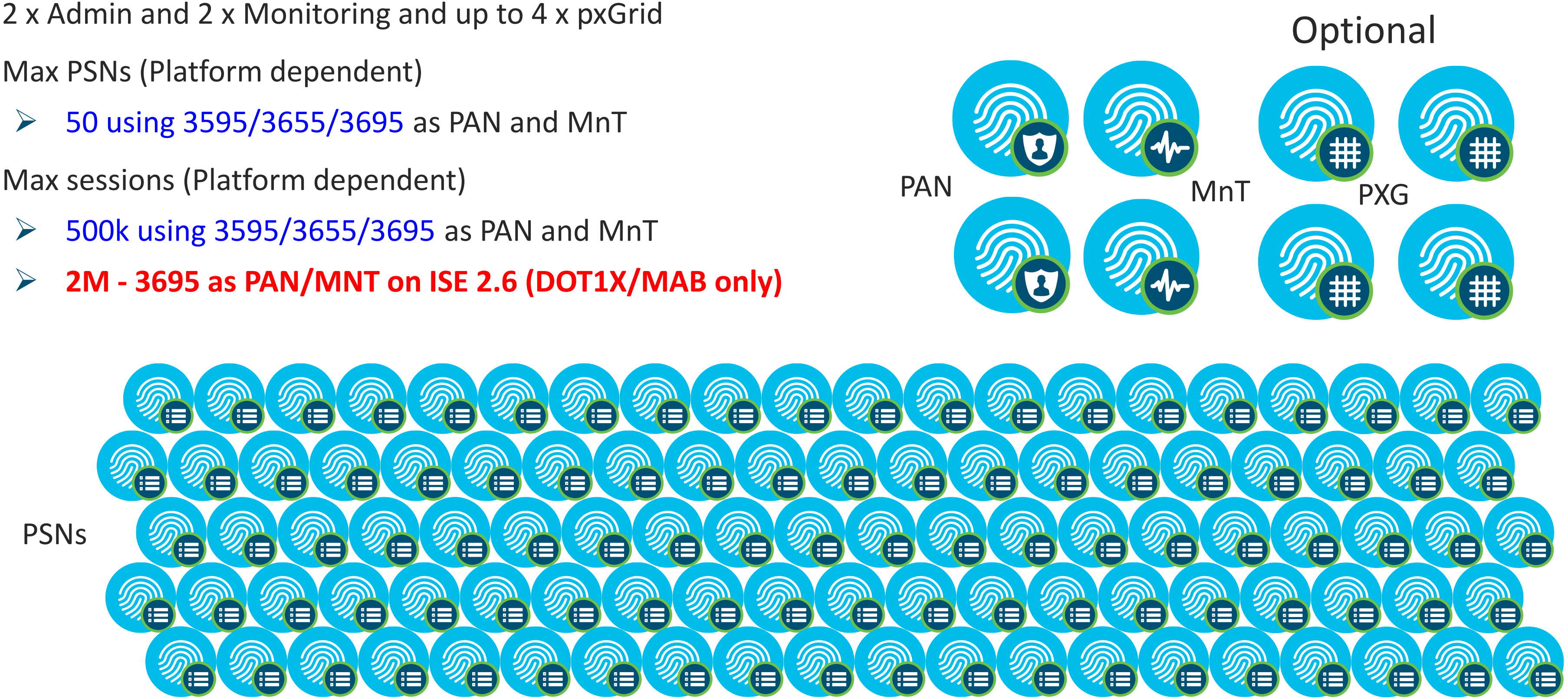


- Dedicated Management Appliances
  - Primary Admin / Primary MnT
  - Secondary MnT / Secondary Admin
- Dedicated Policy Service Nodes—Up to 5 PSNs
- No more than 50,000 Sessions Supported
  - 3615 as Admin/MnT = Max 10k sessions
  - 3655 as Admin/MnT = Max 25k sessions
  - 3695 as Admin/MnT = Max 50k sessions

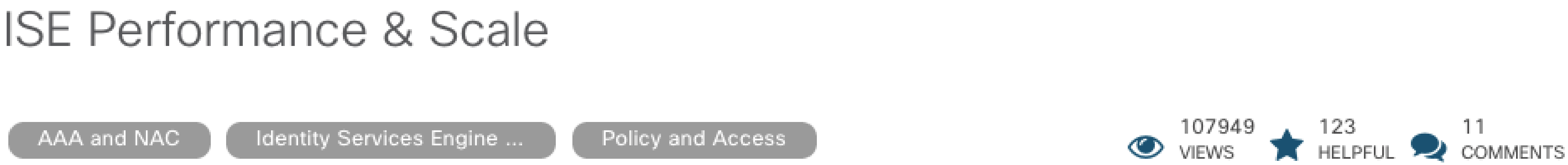
Dedicated-Distributed Persona Deployment

Dedicated Appliance for Each Persona: Admin, Monitoring, pxGrid, Policy

- 2 x Admin and 2 x Monitoring and up to 4 x pxGrid
- Max PSNs (Platform dependent)
  - ➢ 50 using 3595/3655/3695 as PAN and MnT
- Max sessions (Platform dependent)
  - ➢ 500k using 3595/3655/3695 as PAN and MnT
  - ➢ **2M - 3695 as PAN/MNT on ISE 2.6 (DOT1X/MAB only)**



Scaling per use case



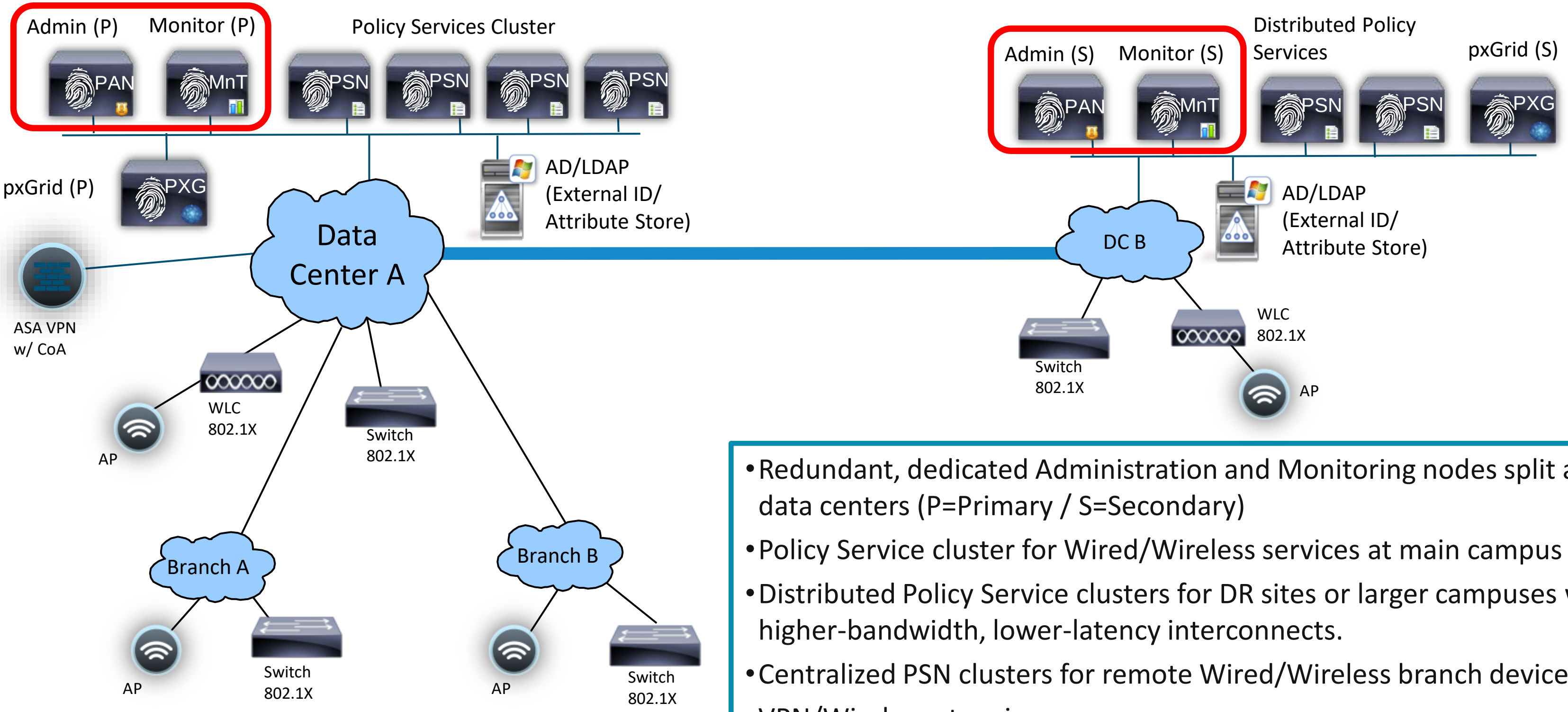
ISE Performance & Scale

https://community.cisco.com/t5/security-documents/ise-performance-amp-scale/ta-p/3642148#toc-hId-1418220509

Fully Dedicated-Distributed Deployment

Maximum Sessions = 2M - Maximum 50 PSNs

For Your Reference

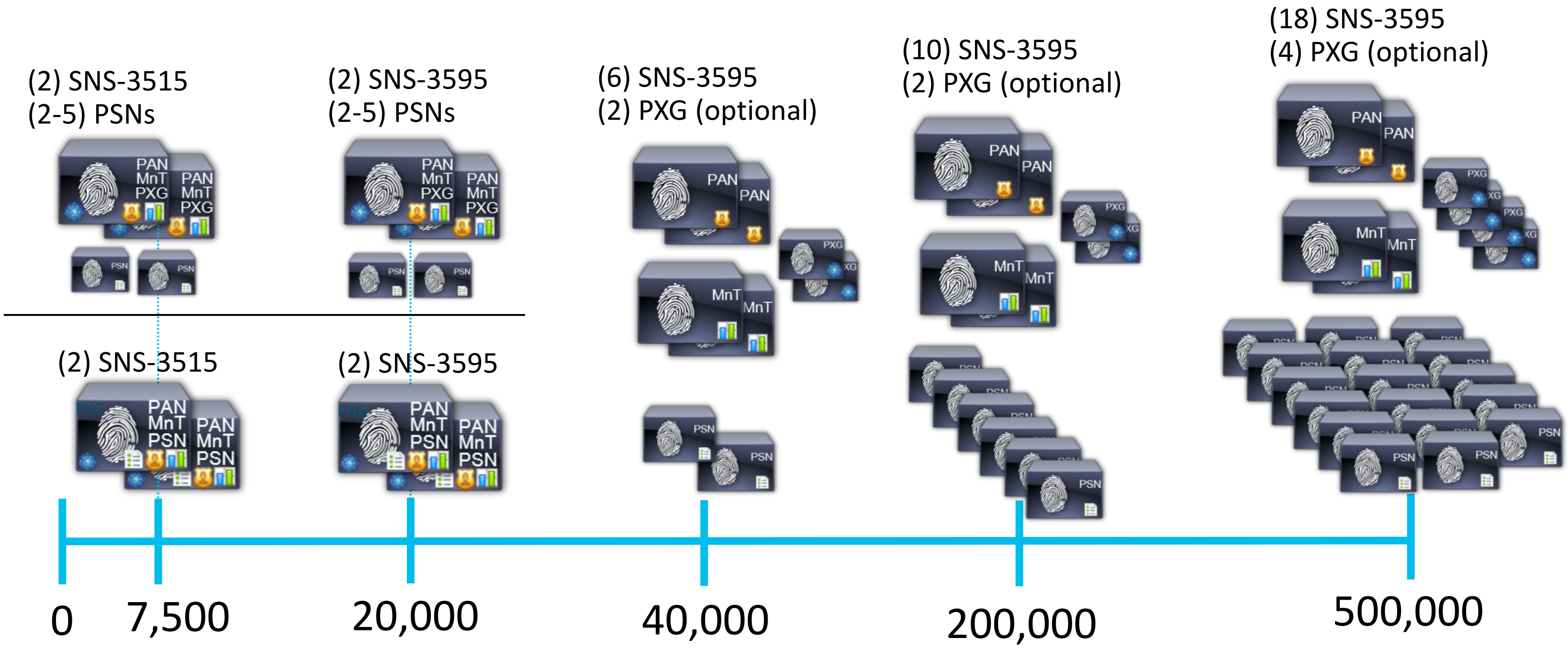


- Redundant, dedicated Administration and Monitoring nodes split across data centers (P=Primary / S=Secondary)
- Policy Service cluster for Wired/Wireless services at main campus
- Distributed Policy Service clusters for DR sites or larger campuses with higher-bandwidth, lower-latency interconnects.
- Centralized PSN clusters for remote Wired/Wireless branch devices
- VPN/Wireless at main campus

For Your Reference

Session Scaling by Deployment Model 35xx

Minimum Nodes (Redundancy Included) ISE <2.6

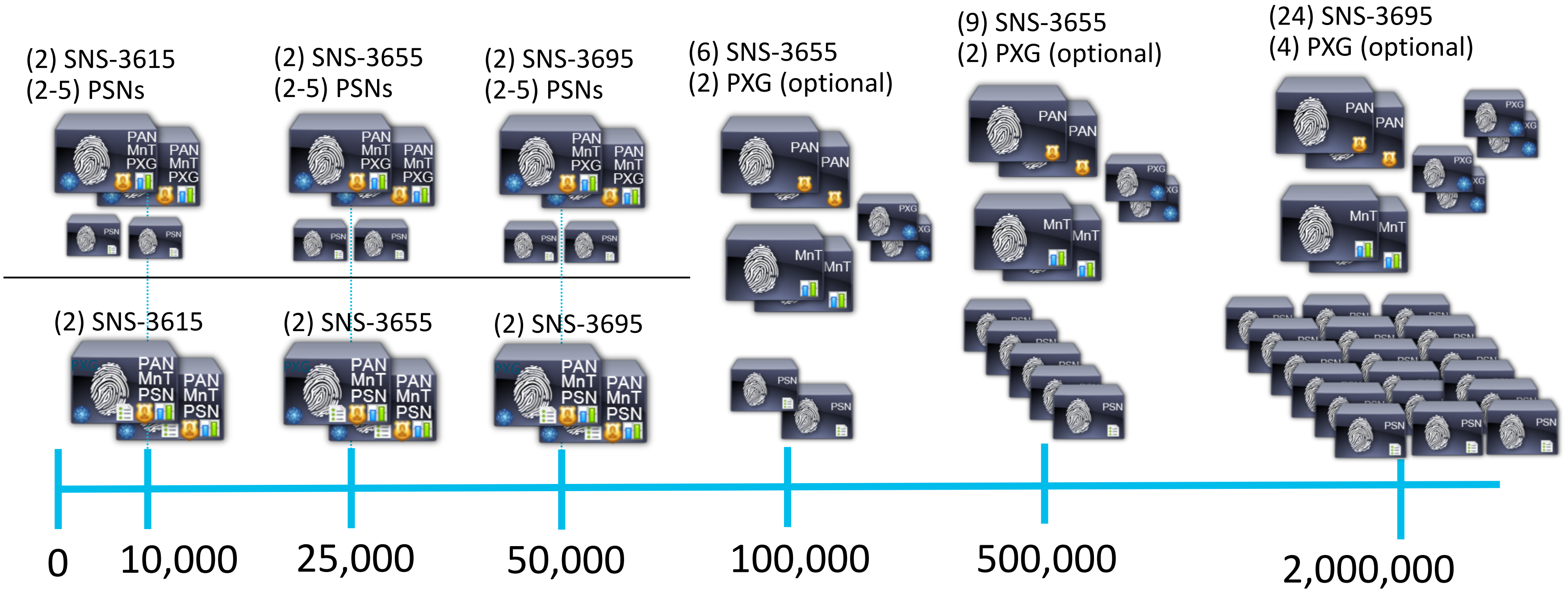


Cisco live!

For Your Reference

Session Scaling by Deployment Model 36xx

Minimum Nodes (Redundancy Included) from ISE 2.6



(2) SNS-3615
(2-5) PSNs

(2) SNS-3655
(2-5) PSNs

(2) SNS-3695
(2-5) PSNs

(6) SNS-3655
(2) PXG (optional)

(9) SNS-3655
(2) PXG (optional)

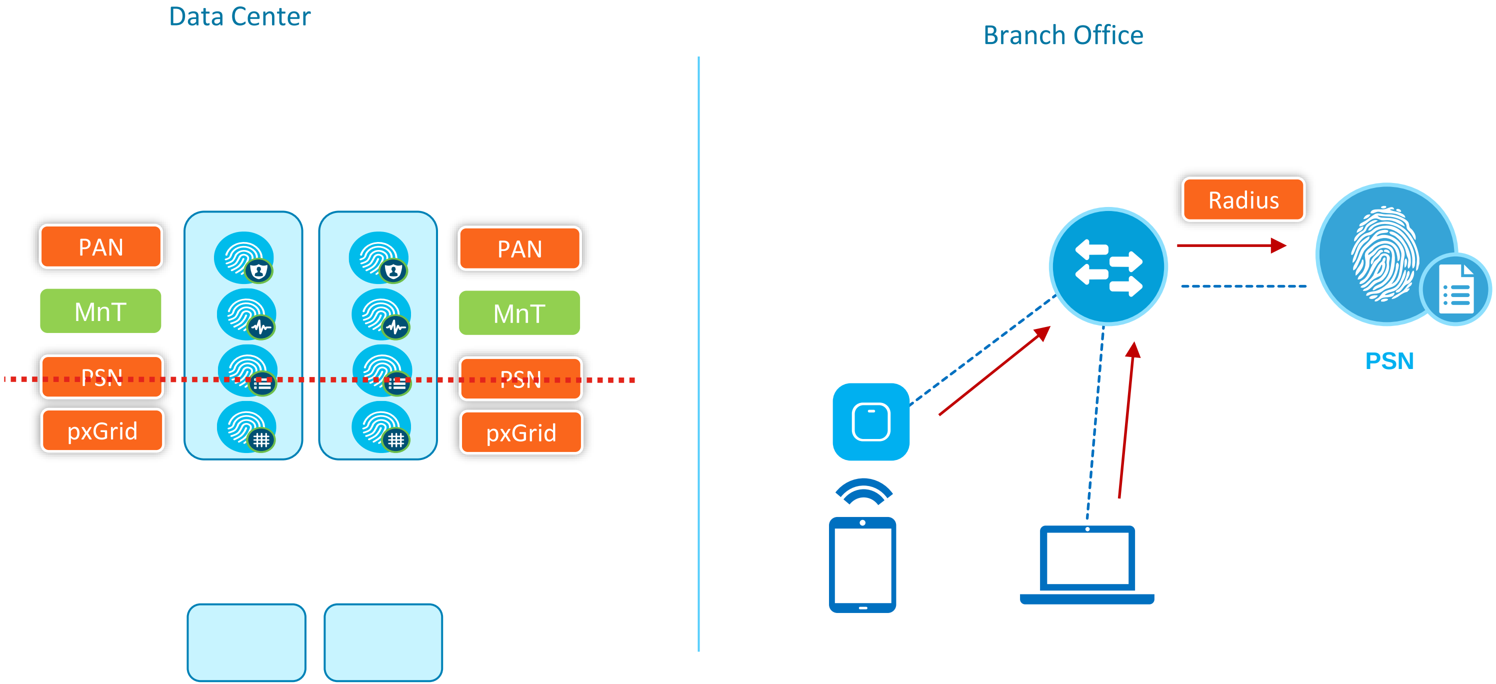
(24) SNS-3695
(4) PXG (optional)

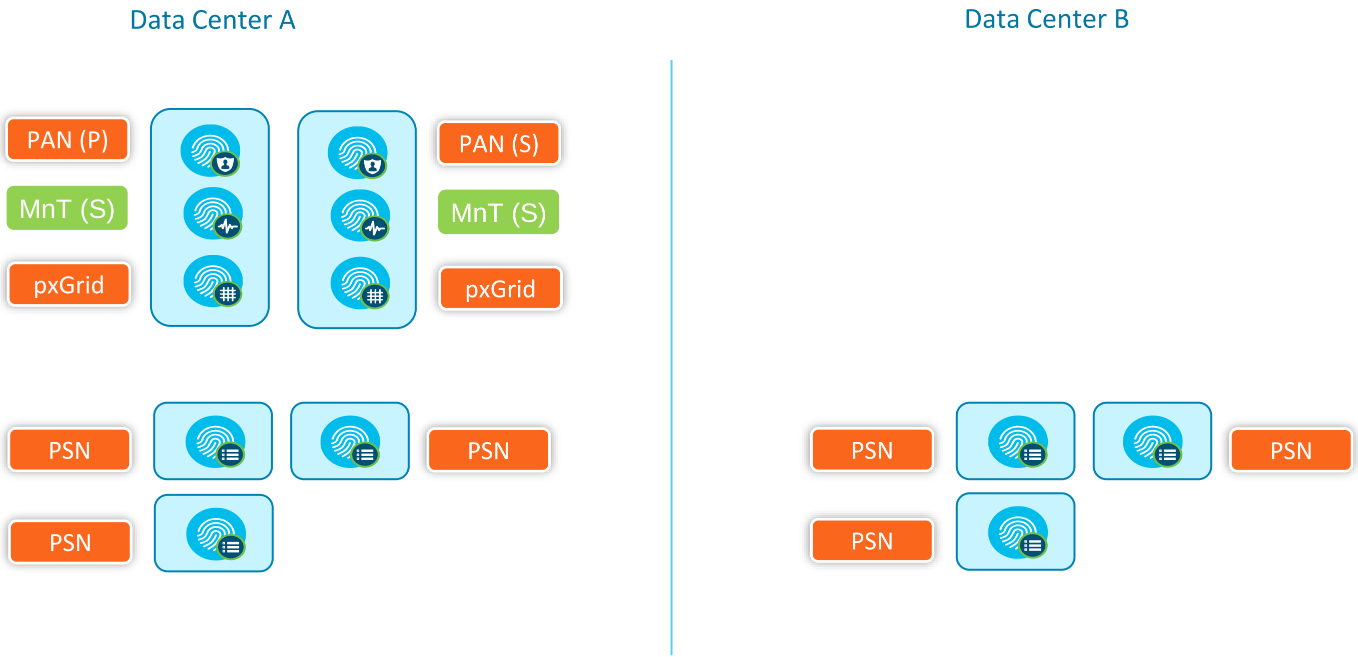
(2) SNS-3615

(2) SNS-3655

(2) SNS-3695

Why design is Important


Data Center
PAN
MnT
PSN
pxGrid
PAN
MnT
PSN
pxGrid
Branch Office
Radius
PSN



Data Center A

PAN (P)

MnT (S)

pxGrid

PAN (S)

MnT (S)

pxGrid

PSN

PSN

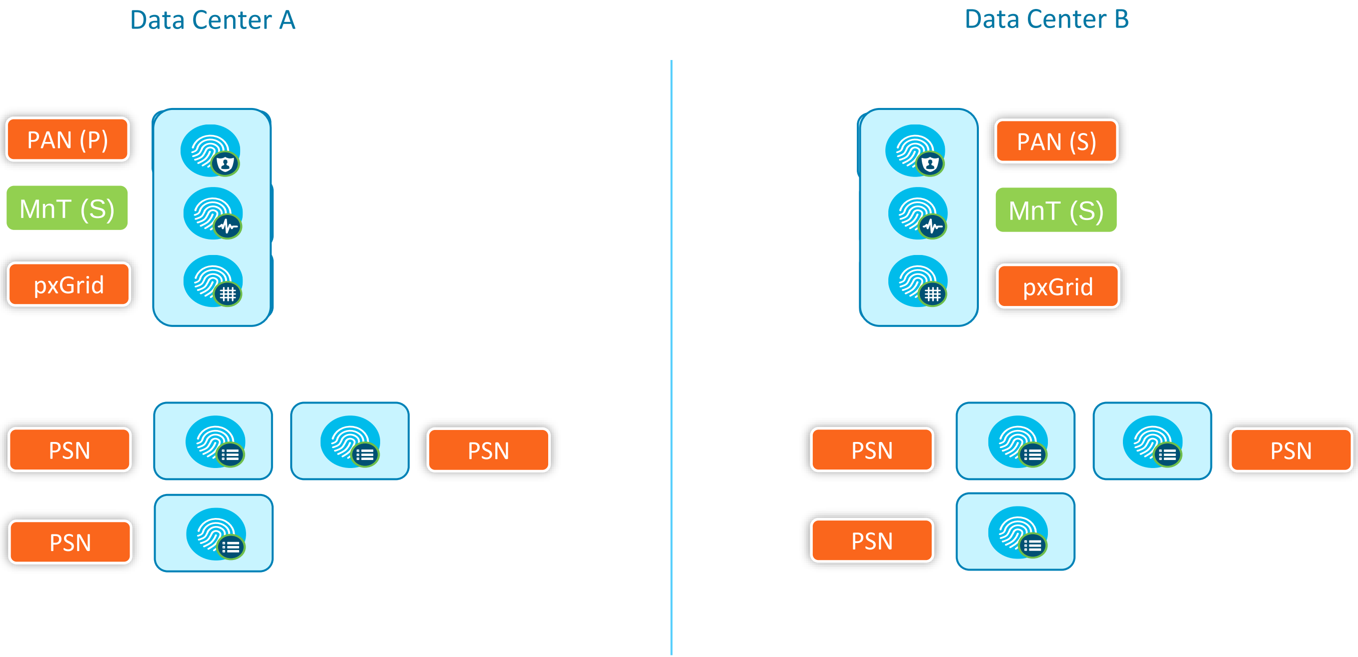
PSN

Data Center B

PSN

PSN

PSN


Data Center A
PAN (P)
MnT (S)
pxGrid
PSN
PSN
PSN
Data Center B
PAN (S)
MnT (S)
pxGrid
PSN
PSN
PSN

Cisco live!

Scaling ISE

ISE Scaling Improvements

ISE 2.6+ - community link

For Your Reference

- Max concurrent active sessions per deployment = 2M (up from 500k)
  - 2M
  - Requires PAN/MnT nodes to be 3695 or VM equivalent

New in ISE 2.6

- Max Internal Endpoints = **2M** (up from 1.5M)

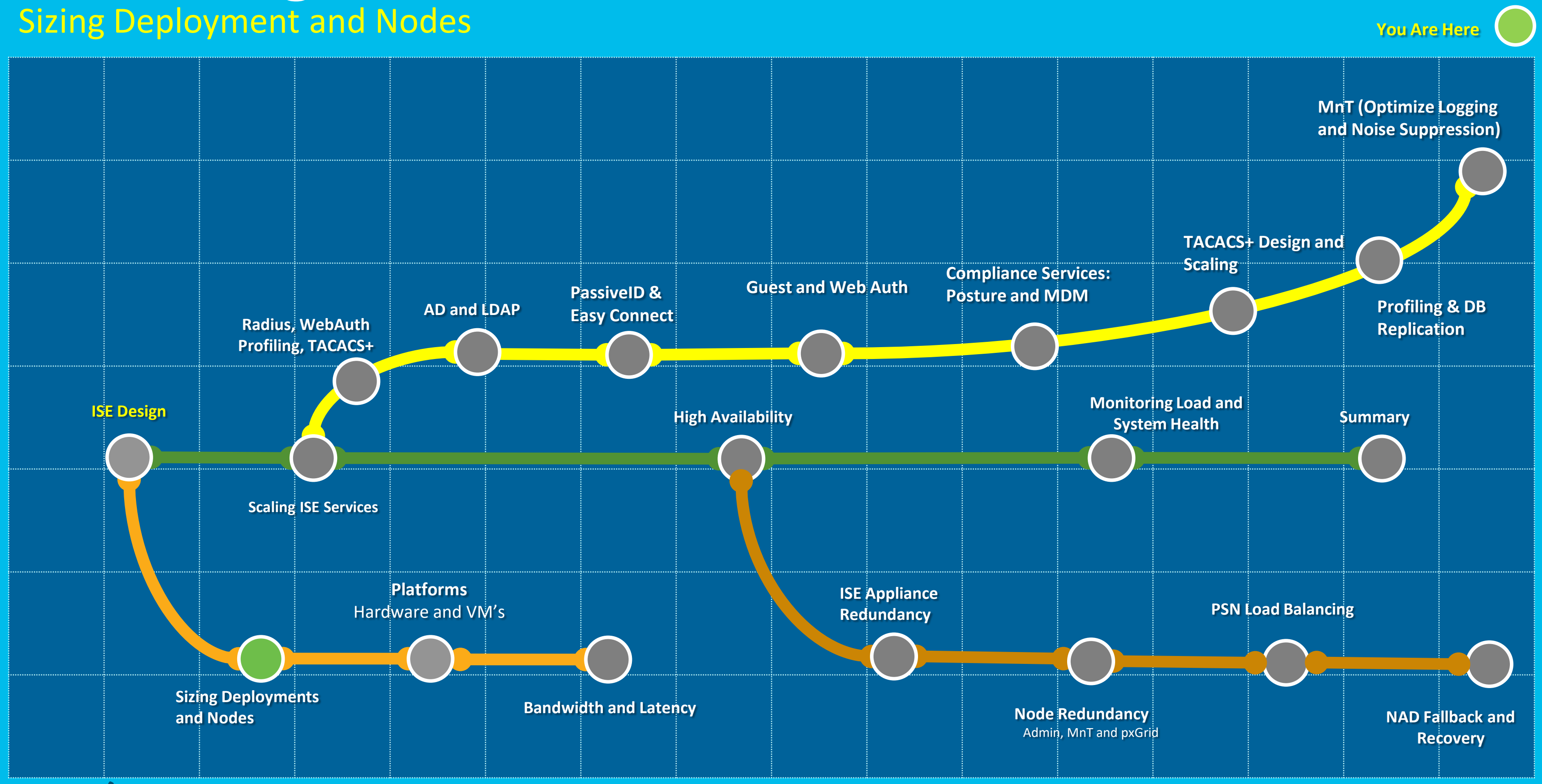
New in ISE 2.6

- Max Internal Users = **300k**
- Max Network Access Devices = **100k**
- Max Network Device Groups = **10k**
- Max PSNs per deployment = **50** Increased scale based on deployment model (max sessions):

	Standalone or PAN+MnT deployment	Dedicated PSN
SNS-3615	**10,000**	**10,000**
SNS-3655	**25,000**	**50,000**
SNS-3695	**50,000**	**100,000**

Session Agenda

Sizing Deployment and Nodes


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Scaling by Deployment/Platform/Persona (36xx)

Max Concurrent Session Counts by Deployment Model/Platform 2.7

For Your Reference

- By Deployment

Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
	3615	10,000	0	1 / 2
	3655	25,000	0	1 / 2
	3695	50,000	0	1 / 2
	3615 as PAN+MNT	10,000	5 / 2*	2 / 7
	3655 as PAN+MNT	25,000	5 / 2*	2 / 7
	3695 as PAN+MNT	50,000	5 / 4*	2 / 7
	3655 as PAN and MNT	500,000	50 / 4	3 / 58
	3695 as PAN & MNT	500k (2M RAD ONLY)	50 / 4	3 / 58

Max Active Sessions != Max Endpoints; ISE 2.6+ supports 2M Endpoints

- By PSN

Scaling per PSN	Platform	Max Active Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3615	10,000
	SNS-3655	50,000
	SNS-3695	100,000

*Each dedicated pxGrid node reduces PSN count by 1 (Medium deployment only)

Policy Service Node Sizing

Physical and Virtual Appliance Guidance

- Max Sessions Per Appliance for Dedicated PSN

Form Factor	Platform Size	Appliance	Maximum Sessions
Physical	Small	SNS-3515	7,500
	Large	SNS-3595	40,000
	Small	SNS-3615	10,000
	Medium	SNS-3655	50,000
	Large	SNS-3695	100,000
Virtual	S/M/L	VM	*7,500-100,000

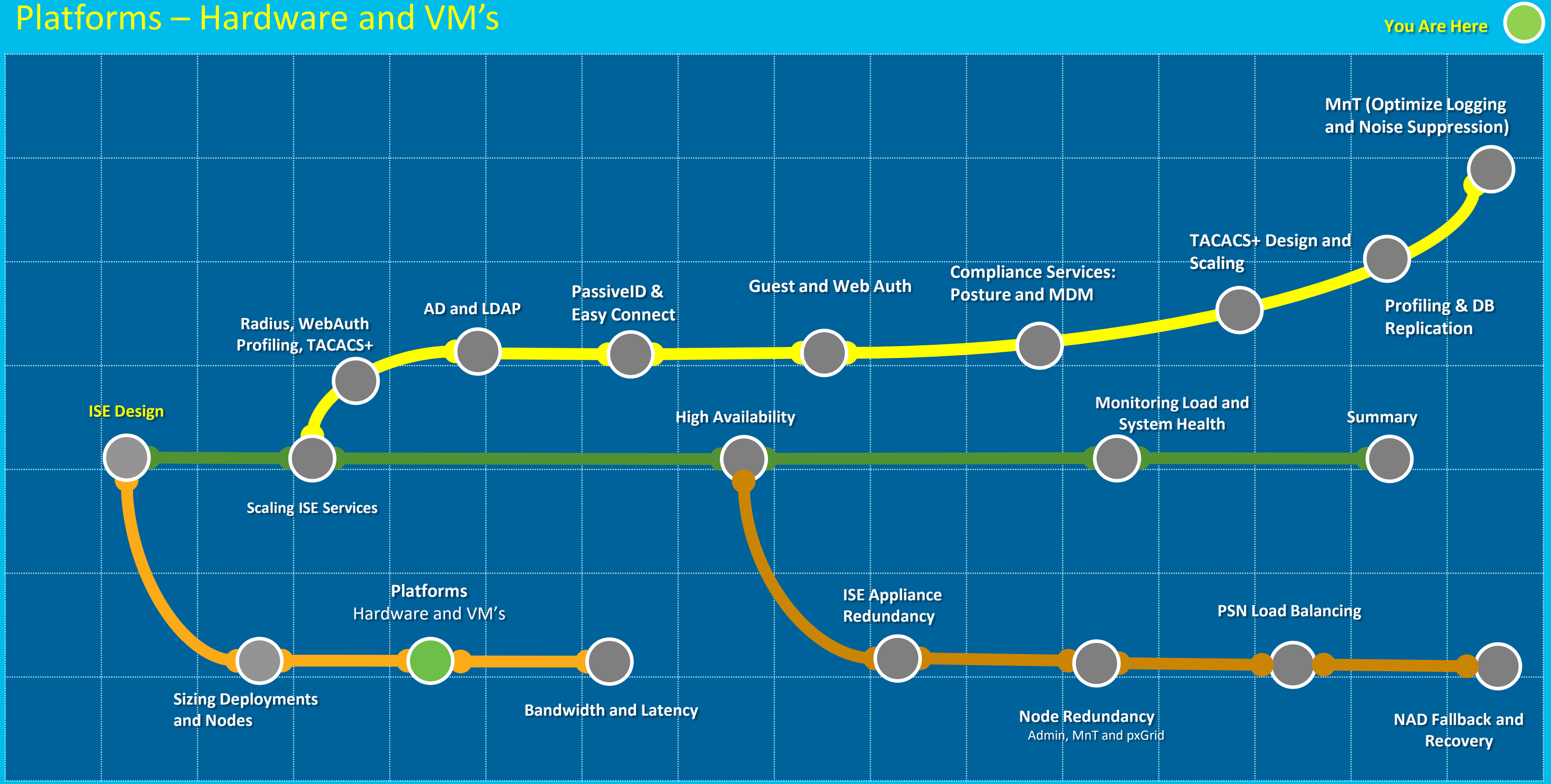
SNS appliances have unique UDI from manufacturing. If use general UCS appliance, then must deploy as VM

General VM appliance sizing guidance:

1) Select physical appliance that meets required persona and scaling requirements
2) Configure VM to match or exceed the ISE physical appliance specifications
3) 2.4 patch 9 / 2.6 required for SNS-36xx scale

Session Agenda

Platforms – Hardware and VM's


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Cisco live!

Sizing Production VMs to Physical Appliances

Summary

Appliance used for sizing comparison	CPU		Memory (GB)	Physical Disk (GB) **
	# Cores	Clock Rate*		
SNS-3515	6	2.4	16	600
SNS-3595	8	2.6	64	1,200
SNS-3615	8	2.1	32	600
SNS-3655	12	2.1	96	1,200
SNS-3695	12	2.1	256	1,200/2,400

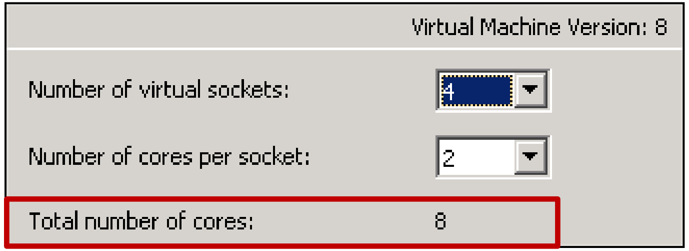
* Minimum VM processor clock rate = 2.0GHz per core (same as OVA).

** Actual disk requirement is dependent on persona(s) deployed and other factors. See slide on Disk Sizing.

Warning: # Cores not always = # Logical processors / vCPUs due to **Hyper Threading** ***REQUIRED***

Configuring CPUs in VMware

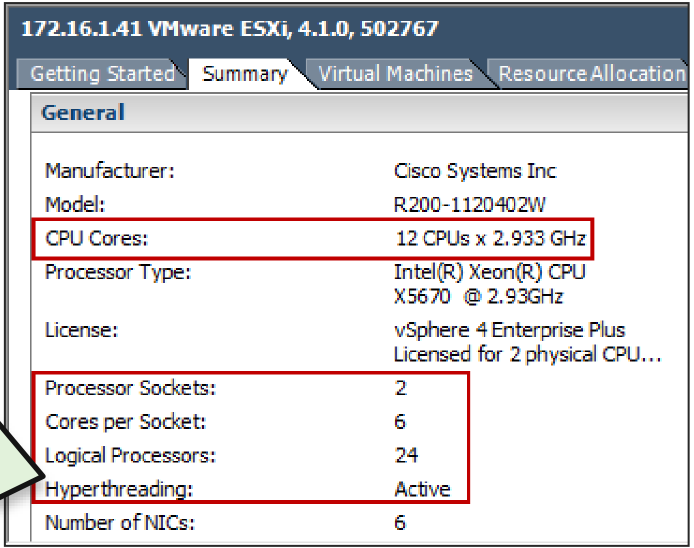
- ESXi 5.x Example



Virtual Machine Version: 8

Number of virtual sockets:	4
Number of cores per socket:	2
Total number of cores:	8

Configure CPU based on cores. If HT enabled, logical CPUs effectively doubled, but # physical cores is same.

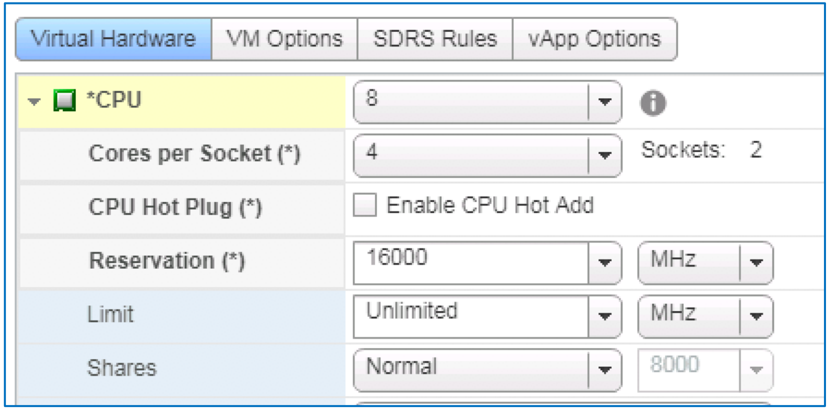


172.16.1.41 VMware ESXi, 4.1.0, 502767

General

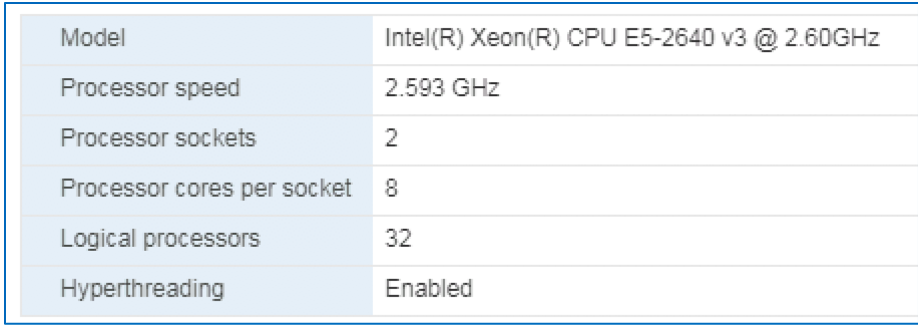
Manufacturer:	Cisco Systems Inc
Model:	R200-1120402W
CPU Cores:	12 CPUs x 2.933 GHz
Processor Type:	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
License:	vSphere 4 Enterprise Plus Licensed for 2 physical CPU...
Processor Sockets:	2
Cores per Socket:	6
Logical Processors:	24
Hyperthreading:	Active
Number of NICs:	6

- ESXi 6.x Example



*CPU	8	
Cores per Socket (*)	4	Sockets: 2
CPU Hot Plug (*)	□ Enable CPU Hot Add	
Reservation (*)	16000	MHz
Limit	Unlimited	MHz
Shares	Normal	8000

For Your Reference



Model	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Processor speed	2.593 GHz
Processor sockets	2
Processor cores per socket	8
Logical processors	32
Hyperthreading	Enabled

Profiling for Platform ?

Small
SNS 3615

Medium
SNS 3655

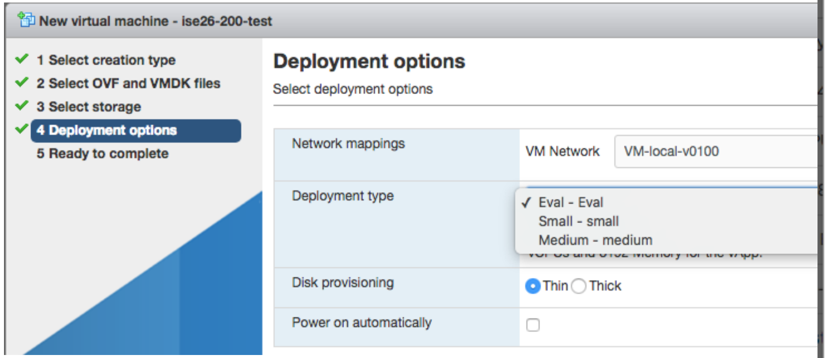
Large
SNS 3695

ISE now supports deployment options in OVA

ESX embedded UI has a bug with (doesn't work with 2 options) 600, 1.2TB

Vcenter works for all OVA files

ESXi embedded host client



New virtual machine - ise26-200-test

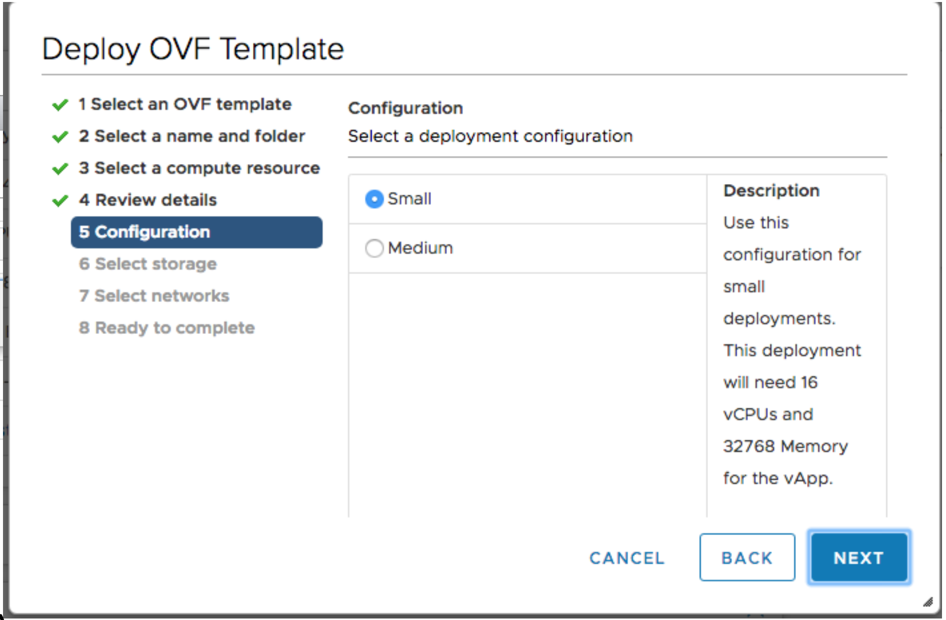
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

Network mappings	VM Network	VM-local-v0100
Deployment type	✓ Eval - Eval Small - small Medium - medium	
Disk provisioning	● Thin ○ Thick	
Power on automatically	□	

vCenter 6x with HTML5



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Ready to complete

Configuration

Select a deployment configuration

● Small	**Description** Use this configuration for small deployments. This deployment will need 16 vCPUs and 32768 Memory for the vApp.
○ Medium	

https://kb.vmware.com/s/article/2150338 — Supported functionality in the HTML5 vSphere Client for vSphere 6.5 & vSphere 6.7 (2150338)

ISE 2.7 OVA Files

Reduced amount of files – using deployment options

OVA FileName	Deployment Options	Platform Profile	# of vCPUs (HT enabled)	Memory (GB)	Disk Capacity (GB)
ISE-2.7.0.356-virtual-SNS3615-SNS3655-300.ova	Eval	eval	2	8	200
	small	sns3615	16	32	
	medium	sns3655	24	96	
ISE-2.7.0.356-virtual-SNS3615-SNS3655-600.ova	Small	sns3615	16	32	600
	Medium	sns3655	24	96	
ISE-2.7.0.356-virtual-SNS3655-SNS3695-1200.ova	Medium	sns3655	24	96	1,200
	Large	sns3695	24	256	
ISE-2.7.0.356-virtual-SNS3695-2400.ova	**LARGE MNT**	sns3695	24	256	2,400

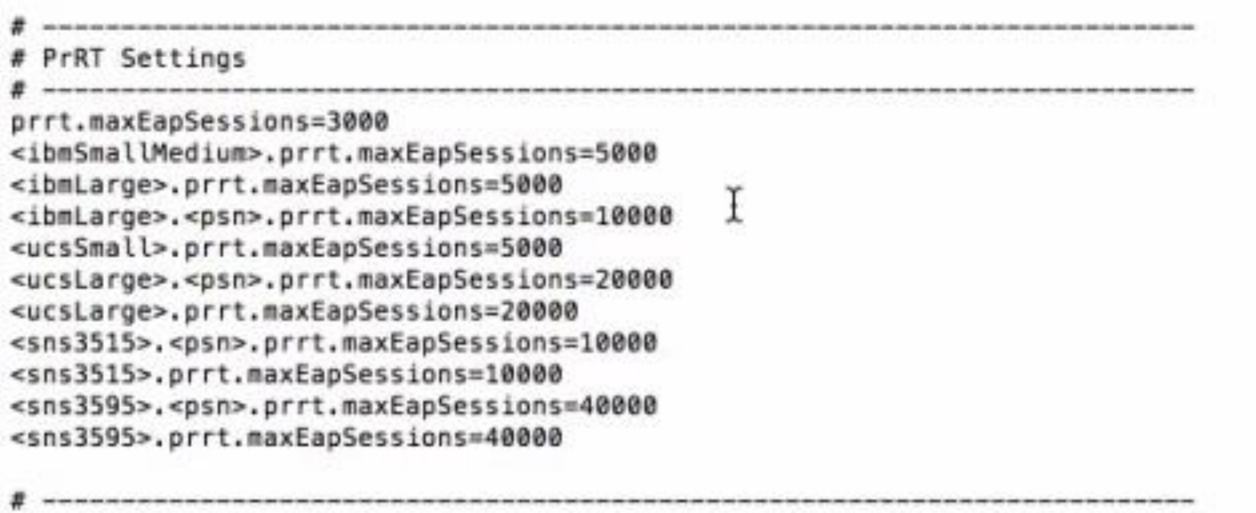
Cisco live!

ISE 2.6 OVA Files

Platform Profile – Lets look at the code

The rules for platform selection are defined in PlatformProfileServiceImpl.java

Min



```
# ---------------------------------------------------------------------------
# PrRT Settings
# ---------------------------------------------------------------------------
prrt.maxEapSessions=3000
<ibmSmallMedium>.prrt.maxEapSessions=5000
<ibmLarge>.prrt.maxEapSessions=5000
<ibmLarge>.<psn>.prrt.maxEapSessions=10000
<ucsSmall>.prrt.maxEapSessions=5000
<ucsLarge>.<psn>.prrt.maxEapSessions=20000
<ucsLarge>.prrt.maxEapSessions=20000
<sns3515>.<psn>.prrt.maxEapSessions=10000
<sns3515>.prrt.maxEapSessions=10000
<sns3595>.<psn>.prrt.maxEapSessions=40000
<sns3595>.prrt.maxEapSessions=40000

# ---------------------------------------------------------------------------
```

ile Tag

ledium

16 256 "Super MnT" <custom>

ISE Platform Properties

How Does ISE Detect the Size of my Virtual Machine?

For Your Reference

- *During Installation,* ISE checks # CPU cores, RAM, and Disk Space allocated and assigns platform profile
- Profile recalculated if...
  - *Resources change* (RAM/CPU cores)
  - *Persona changes* on ISE (node-config.rc).
- Note: Disk size changes NEVER get updated in ISE without reimage.
- Persona change from ISE deployment page will trigger profile recalculation.
- May be out of sync due to upgrade of resources after initial install
  - Migration from eval/PoC
  - Resources added to meet version or capacity requirements

ISE Platform Properties

Minimum VM Resource Allocation for SNS35xx/36xx

Minimum CPUs	Minimum RAM	Minimum Disk	Platform Profile
2	16	200GB	EVAL
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	"Super MnT" <custom>
16	32	200GB	SNS_3615
24	96	200GB	SNS_3655
24	256	200GB	SNS_3695

35xx

36xx

More to come! On 2.4

- Least Common Denominator used to set platform.
- Example:
  4 cores
  16 GB RAM
  = EVAL

NEW

35xx/36xx Newer platforms require hyperthreading

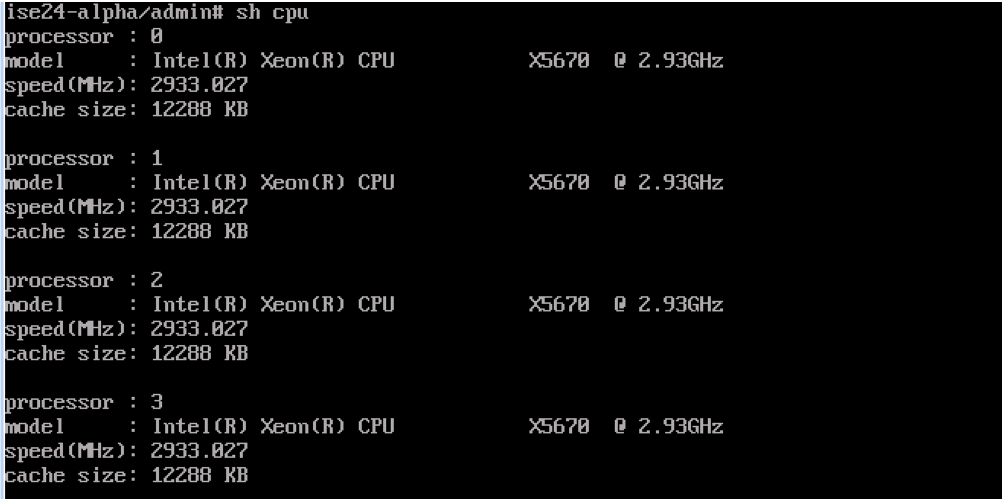
- Small -3515 & 3615
- Medium - 3595 & 3695
- Large - 3695

Platform Detection and Sizing

For Your Reference

Verify what ISE is seeing

- CPU
  - `# sh cpu`
- Mem
  - `# sh mem`
- Detected Platform
  - `# sh tech-support`



```
ise24-alpha/admin# sh cpu
processor : 0
model      : Intel(R) Xeon(R) CPU           X5670  @ 2.93GHz
speed(MHz): 2933.027
cache size: 12288 KB

processor : 1
model      : Intel(R) Xeon(R) CPU           X5670  @ 2.93GHz
speed(MHz): 2933.027
cache size: 12288 KB

processor : 2
model      : Intel(R) Xeon(R) CPU           X5670  @ 2.93GHz
speed(MHz): 2933.027
cache size: 12288 KB

processor : 3
model      : Intel(R) Xeon(R) CPU           X5670  @ 2.93GHz
speed(MHz): 2933.027
cache size: 12288 KB
```

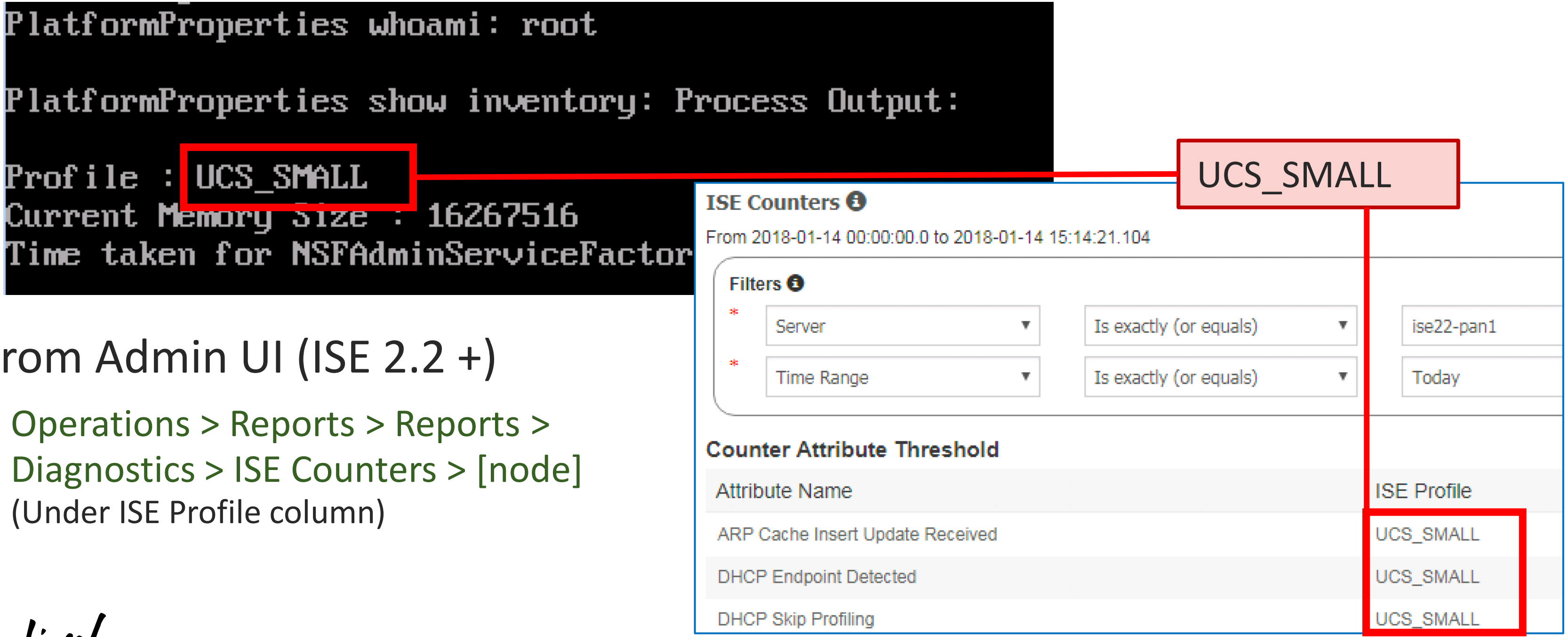
```
PlatformProperties show inventory: Process Output:

Profile : UCS_SMALL
Current Memory Size : 15927532
```

ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

- From CLI…
  - `ise-node/admin#` **`show tech | begin PlatformProperties`**



```
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:

Profile : UCS_SMALL
Current Memory Size : 16267516
Time taken for NSFAdminServiceFactor
```

UCS_SMALL

ISE Counters

From 2018-01-14 00:00:00.0 to 2018-01-14 15:14:21.104

Filters

*	Server	Is exactly (or equals)	ise22-pan1
*	Time Range	Is exactly (or equals)	Today

Counter Attribute Threshold

Attribute Name	ISE Profile
ARP Cache Insert Update Received	UCS_SMALL
DHCP Endpoint Detected	UCS_SMALL
DHCP Skip Profiling	UCS_SMALL

- From Admin UI (ISE 2.2 +)
  - Operations > Reports > Reports > Diagnostics > ISE Counters > [node]
    (Under ISE Profile column)

ISE VM Disk Storage Requirements

For Your Reference

Minimum Disk Sizes by Persona 2.x

- Upper range sets #days MnT log retention
- Min recommended disk for MnT = 600GB
- Max hardware appliance disk size = 1.2TB (3595/3655) 2.4TB (3695)
- Max virtual appliance disk size = 1.99TB (<2.6) 2.4TB (2.6)

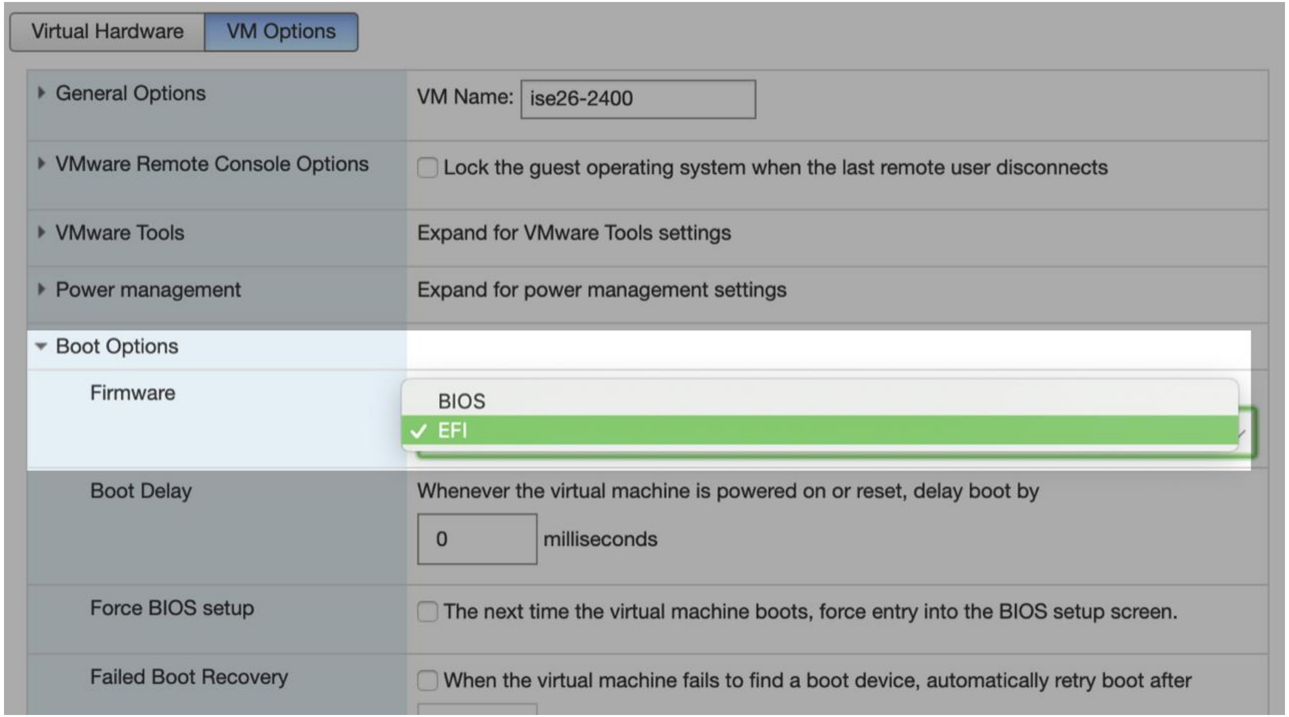
** Variations depend on where backups saved or upgrade files staged (local or repository), debug, local logging, and data retention requirements.

Persona	Disk (GB)
Standalone	200+*
Administration (PAN) Only	200-300**
Monitoring (MnT) Only	200+*
Policy Service (PSN) Only	200
PAN + MnT	200+*
PAN + MnT + PSN	200+*

ISE VM Disk Storage Requirements

For Your Reference

- 2.0TB+ requires EFI (default is BIOS) – tested up to 2.4TB



General Options — VM Name: ise26-2400

VMware Remote Console Options — □ Lock the guest operating system when the last remote user disconnects

VMware Tools — Expand for VMware Tools settings

Power management — Expand for power management settings

Boot Options

Firmware — BIOS / ✓ EFI

Boot Delay — Whenever the virtual machine is powered on or reset, delay boot by 0 milliseconds

Force BIOS setup — □ The next time the virtual machine boots, force entry into the BIOS setup screen.

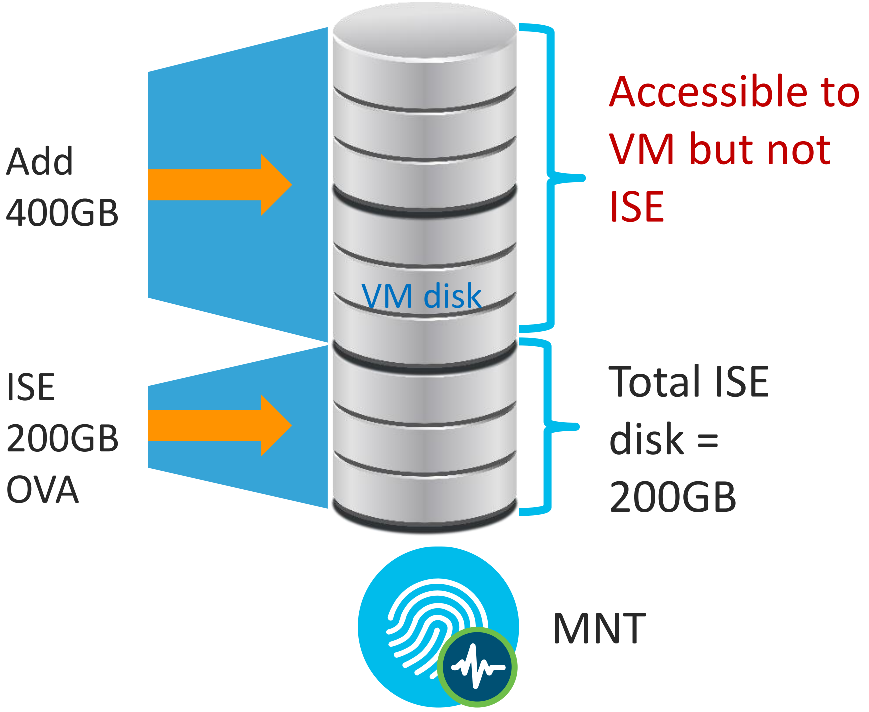
Failed Boot Recovery — □ When the virtual machine fails to find a boot device, automatically retry boot after

VM Disk Allocation

For Your Reference

CSCvc57684 Incorrect MnT allocations if setup with VM disk resized to larger without ISO re-image

- ISE OVAs prior to ISE 2.2 sized to 200GB. Often sufficient for PSNs or pxGrid nodes but not MnT.
- Misconception: Just get bigger tank and ISE will grow into it!
- No auto-resize of ISE partitions when disk space added after initial software install
- Requires re-image using .iso
- Alternatively: Start with a larger OVA



MnT Node Log Storage Requirements for RADIUS

For Your Reference

Days Retention Based on # Endpoints and Disk Size (ISE 2.2+)

Total Disk Space Allocated to MnT Node

Total Endpoints

	200 GB	400 GB	600 GB	1024 GB	2048 GB	2400 GB (2.6 +)
5,000	504	1007	1510	2577	5154	6665
10,000	252	504	755	1289	2577	3081
25,000	101	202	302	516	1031	1233
50,000	51	101	151	258	516	617
100,000	26	51	76	129	258	309
150,000	17	34	51	86	172	206
200,000	13	26	38	65	129	155
250,000	11	21	31	52	104	125
500,000	6	11	16	26	52	63
2M	1	2	4	6	12	14

Based on 60% allocation of MnT disk to RADIUS logging
(Prior to ISE 2.2, only 30% allocations)

ISE 2.2 = 50% days increase over 2.0/2.1

ISE 2.3 = 25-33% increase over 2.2

ISE 2.4 = 40-60% increase over 2.2

Assumptions:

- 10+ auths/day per endpoint
- Log suppression enabled
- ~approzimations

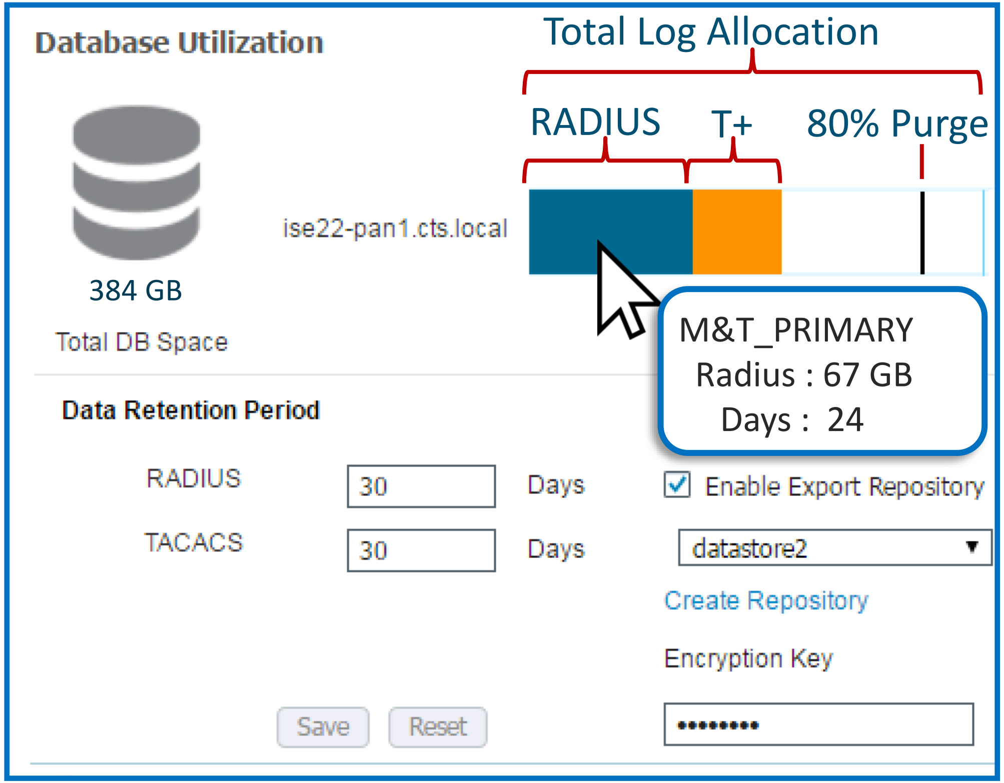
RADIUS and TACACS+

MnT Log Allocation

For Your Reference

ISE 2.2+

- Administration > System > Maintenance > Operational Data Purging



Database Utilization

384 GB

Total DB Space

ise22-pan1.cts.local

M&T_PRIMARY
Radius : 67 GB
Days : 24

Data Retention Period

RADIUS	30	Days
TACACS	30	Days

☑ Enable Export Repository

datastore2 ▾

Create Repository

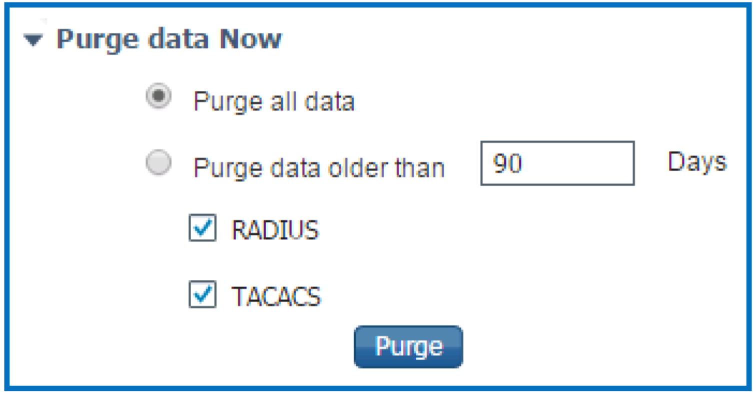
Encryption Key

•••••••••

Save Reset

- 60% total disk allocated to both RADIUS and TACACS+ for logging

  (Previously fixed at 30% and 20%)
- Purge @ 80% (First In-First Out)
- Optional archive of CSV to repository



▾ **Purge data Now**

● Purge all data

○ Purge data older than 90 Days

☑ RADIUS

☑ TACACS

Purge

ISE VM Disk Provisioning Guidance

- Please! No Snapshots!
  - **Snapshots NOT supported**; no option to quiesce database prior to snapshot.
- VMotion supported but storage motion not QA tested.
  - **Recommend avoid VMotion** due to snapshot restrictions.
- Thin Provisioning supported
  - **Thick Provisioning highly recommended**, especially for PAN and MnT)
- No specific storage media and file system restrictions.
  - For example, VMFS is not required and NFS allowed *provided* storage is supported by VMware and meets ISE IO performance requirements.

IO Performance Requirements:

- ➢ Read 300+ MB/sec
- ➢ Write 50+ MB/sec

Recommended disk/controller:

- ➢ 10k RPM+ disk drives
  - ➢ Supercharge with SSD !
- ➢ Caching RAID Controller
- ➢ RAID mirroring

Slower writes using RAID 5*

*RAID performance levels:
http://www.datarecovery.net/articles/raid-level-comparison.html
http://docs.oracle.com/cd/E19658-01/820-4708-13/appendixa.html

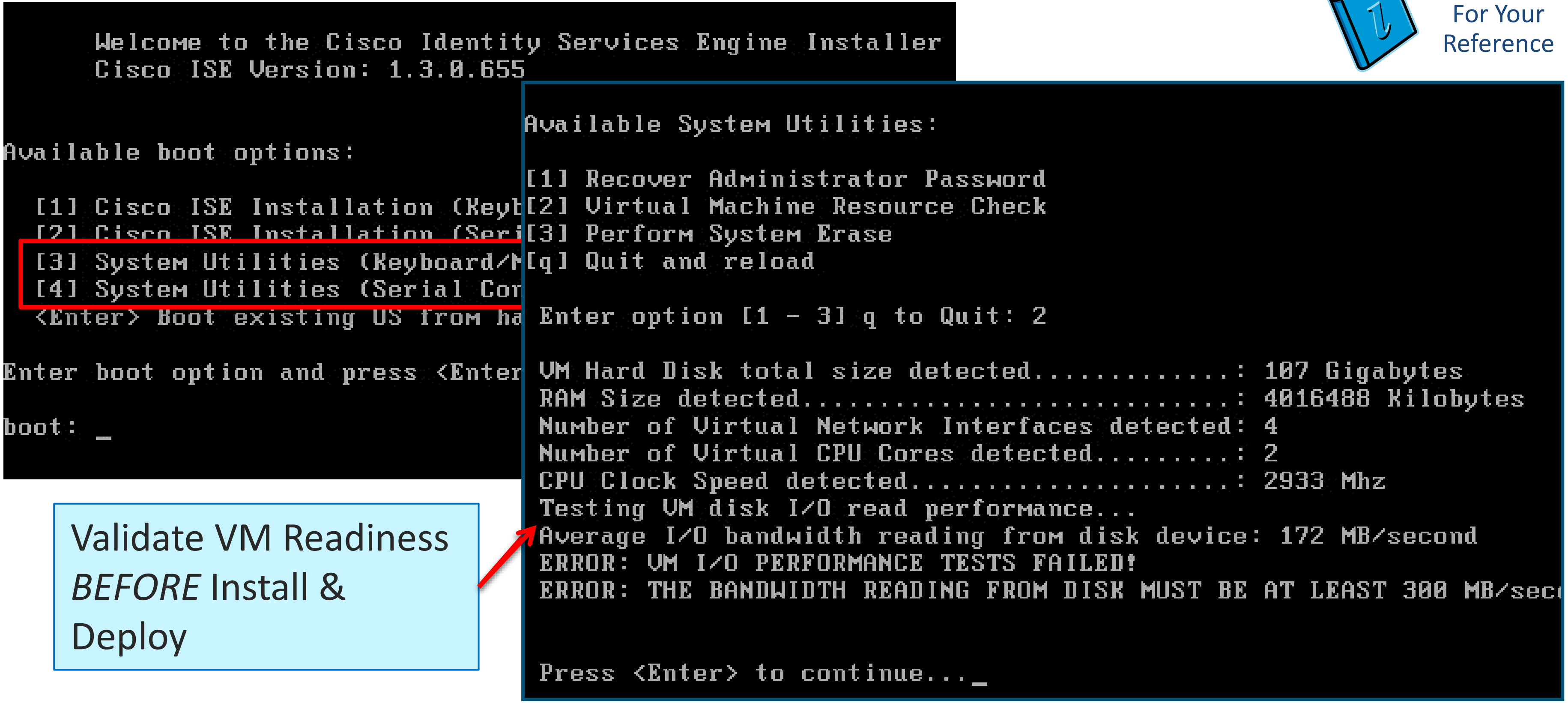
ISE VM Provisioning Guidance

- Use reservations (built into OVAs)
- Do not oversubscribe!

Customers with VMware expertise may choose to disable resource reservations and over-subscribe, but do so at own risk.

VM Appliance Resource Validation *Before* Install

For Your Reference



```
     Welcome to the Cisco Identity Services Engine Installer
     Cisco ISE Version: 1.3.0.655


Available boot options:

  [1] Cisco ISE Installation (Keyb
  [2] Cisco ISE Installation (Seri
  [3] System Utilities (Keyboard/M
  [4] System Utilities (Serial Con
  <Enter> Boot existing OS from ha

Enter boot option and press <Enter

boot: _
```

```
Available System Utilities:

[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

 Enter option [1 - 3] q to Quit: 2

 VM Hard Disk total size detected.............: 107 Gigabytes
 RAM Size detected............................: 4016488 Kilobytes
 Number of Virtual Network Interfaces detected: 4
 Number of Virtual CPU Cores detected.........: 2
 CPU Clock Speed detected.....................: 2933 Mhz
 Testing VM disk I/O read performance...
 Average I/O bandwidth reading from disk device: 172 MB/second
 ERROR: VM I/O PERFORMANCE TESTS FAILED!
 ERROR: THE BANDWIDTH READING FROM DISK MUST BE AT LEAST 300 MB/seco


 Press <Enter> to continue..._
```

Validate VM Readiness *BEFORE* Install & Deploy

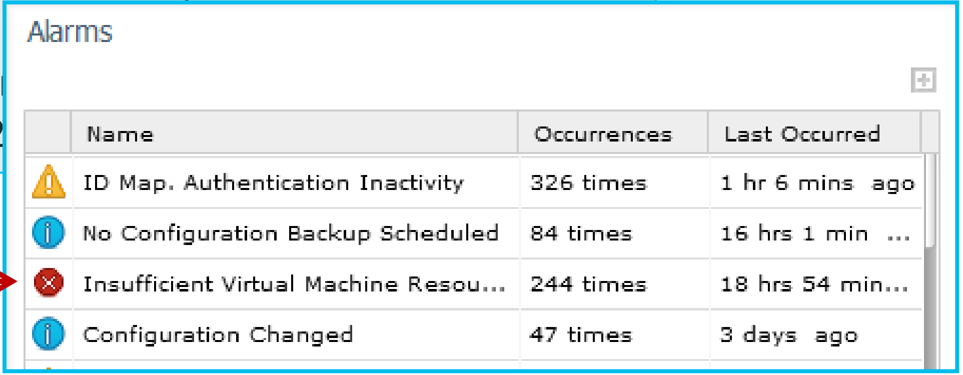
VM Appliance Resource Validation *After* Install

ISE continues to test I/O read/write performance on 3-hour intervals

For Your Reference

```
ise-psn2/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
*****************************************
Average I/O bandwidth writing to disk device: 194 MB/second
Average I/O bandwidth reading from disk device: over 1024 MB/second
I/O bandwidth performance within supported guidelines
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 1.47342 s,
Disk I/O bandwidth filesystem read test, readi
314572800 bytes (315 MB) copied, 0.0504592
```

Alarm generated if 24-hr average below requirements

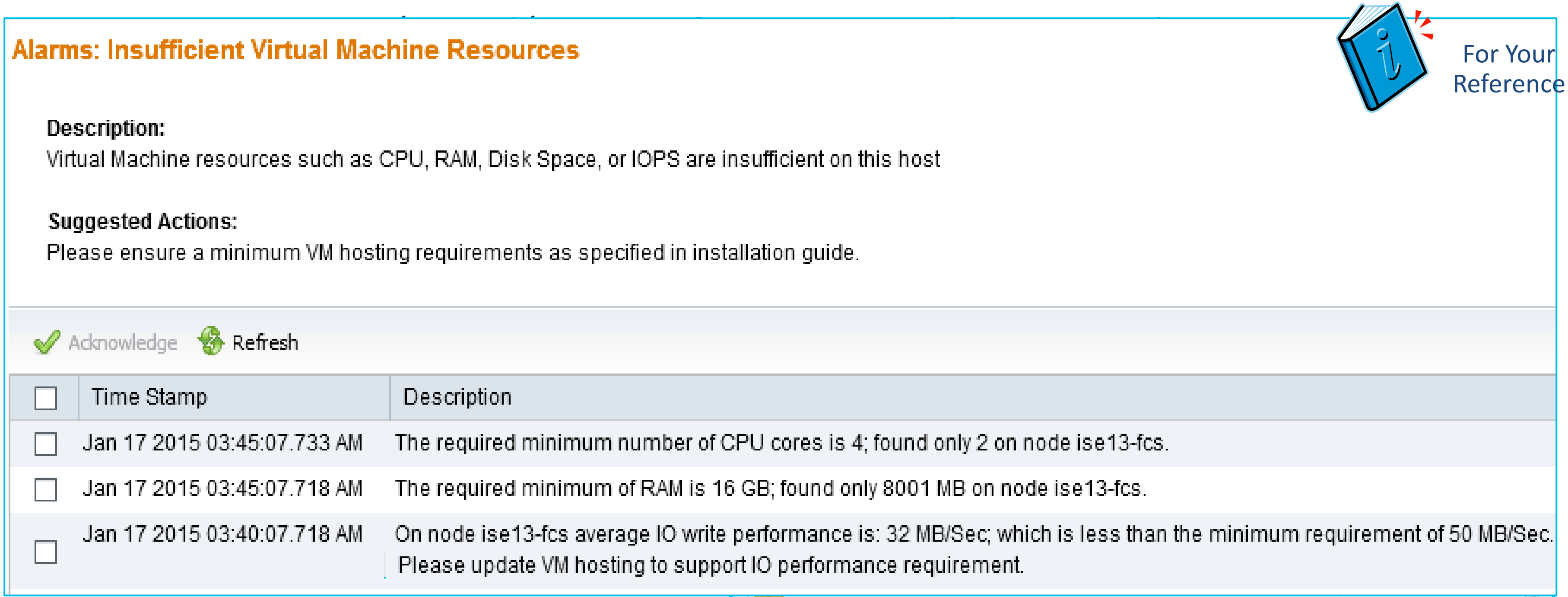


Alarms

	Name	Occurrences	Last Occurred
⚠	ID Map. Authentication Inactivity	326 times	1 hr 6 mins ago
ℹ	No Configuration Backup Scheduled	84 times	16 hrs 1 min ...
⊗	Insufficient Virtual Machine Resou...	244 times	18 hrs 54 min...
ℹ	Configuration Changed	47 times	3 days ago

VM Appliance Resource Validation *After* Install

For Your Reference



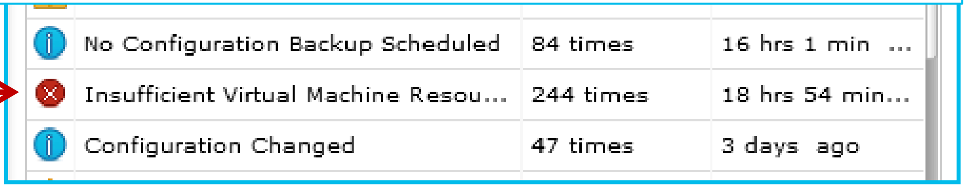
Alarms: Insufficient Virtual Machine Resources

Description:
Virtual Machine resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host

Suggested Actions:
Please ensure a minimum VM hosting requirements as specified in installation guide.

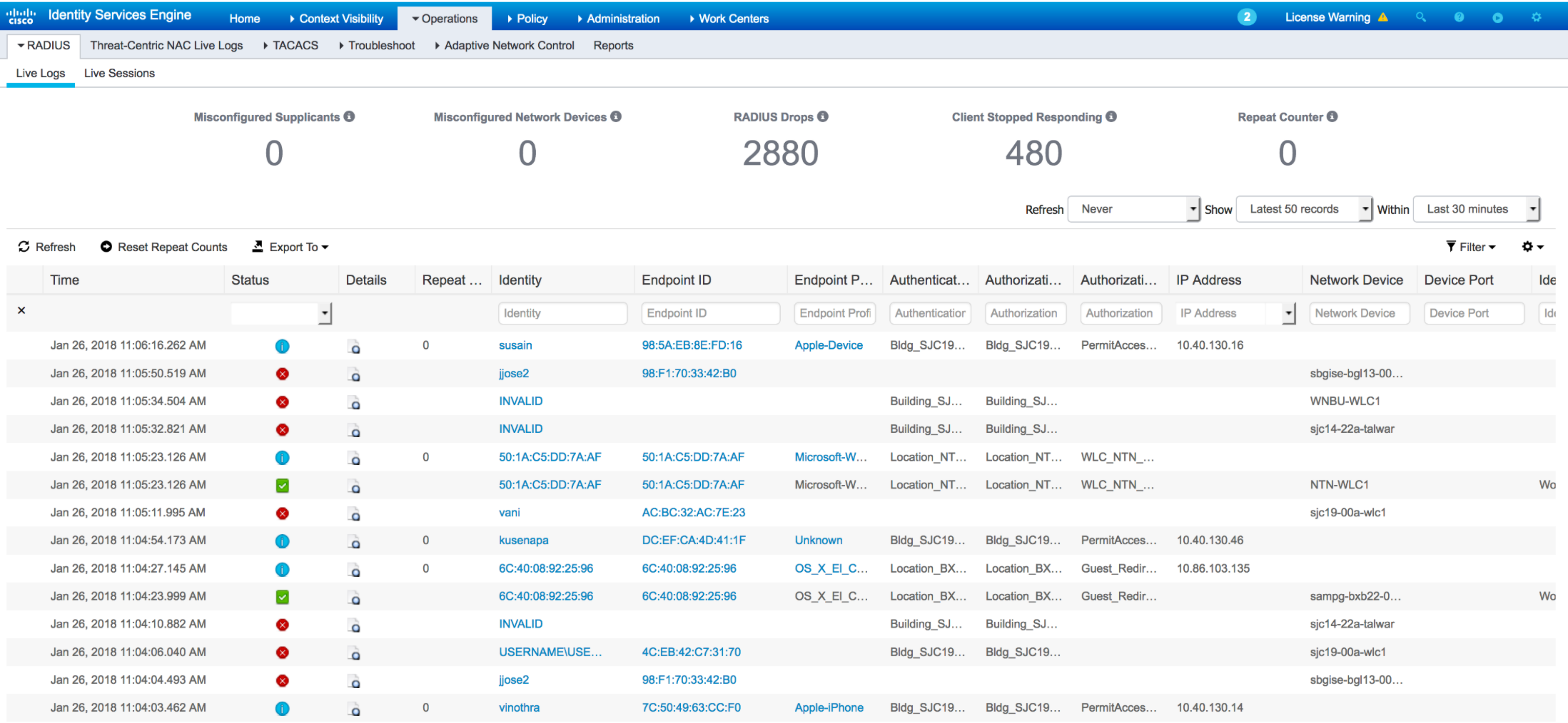
□	Time Stamp	Description
□	Jan 17 2015 03:45:07.733 AM	The required minimum number of CPU cores is 4; found only 2 on node ise13-fcs.
□	Jan 17 2015 03:45:07.718 AM	The required minimum of RAM is 16 GB; found only 8001 MB on node ise13-fcs.
□	Jan 17 2015 03:40:07.718 AM	On node ise13-fcs average IO write performance is: 32 MB/Sec; which is less than the minimum requirement of 50 MB/Sec. Please update VM hosting to support IO performance requirement.

Alarm generated if 24-hr average below requirements



ⓘ	No Configuration Backup Scheduled	84 times	16 hrs 1 min ...
⊗	Insufficient Virtual Machine Resou...	244 times	18 hrs 54 min...
ⓘ	Configuration Changed	47 times	3 days ago

ISE 2.4+ MnT+ Fast Access to Logs and Reports



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	2880	480	0

Refresh Never Show Latest 50 records Within Last 30 minutes

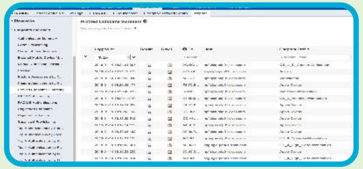
	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Ide
×					Identity	Endpoint ID	Endpoint Profi	Authenticatior	Authorization	Authorization	IP Address	Network Device	Device Port	Ide
	Jan 26, 2018 11:06:16.262 AM	ⓘ	🔍	0	susain	98:5A:EB:8E:FD:16	Apple-Device	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.16			
	Jan 26, 2018 11:05:50.519 AM	✖	🔍		jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
	Jan 26, 2018 11:05:34.504 AM	✖	🔍		INVALID			Building_SJ...	Building_SJ...			WNBU-WLC1		
	Jan 26, 2018 11:05:32.821 AM	✖	🔍		INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
	Jan 26, 2018 11:05:23.126 AM	ⓘ	🔍	0	50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN_...				
	Jan 26, 2018 11:05:23.126 AM	✓	🔍		50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN_...		NTN-WLC1		Wo
	Jan 26, 2018 11:05:11.995 AM	✖	🔍		vani	AC:BC:32:AC:7E:23						sjc19-00a-wlc1		
	Jan 26, 2018 11:04:54.173 AM	ⓘ	🔍	0	kusenapa	DC:EF:CA:4D:41:1F	Unknown	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.46			
	Jan 26, 2018 11:04:27.145 AM	ⓘ	🔍	0	6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_El_C...	Location_BX...	Location_BX...	Guest_Redir...	10.86.103.135			
	Jan 26, 2018 11:04:23.999 AM	✓	🔍		6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_El_C...	Location_BX...	Location_BX...	Guest_Redir...		sampg-bxb22-0...		Wo
	Jan 26, 2018 11:04:10.882 AM	✖	🔍		INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
	Jan 26, 2018 11:04:06.040 AM	✖	🔍		USERNAME\USE...	4C:EB:42:C7:31:70		Bldg_SJC19...	Bldg_SJC19...			sjc19-00a-wlc1		
	Jan 26, 2018 11:04:04.493 AM	✖	🔍		jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
	Jan 26, 2018 11:04:03.462 AM	ⓘ	🔍	0	vinothra	7C:50:49:63:CC:F0	Apple-iPhone	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.14			

ISE 2.4+ MnT Vertical Scaling Scaling Enhancements

Benefits MnT on ALL ISE platforms

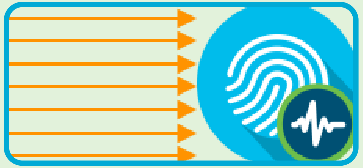
Faster Live Log Access

- Run session directory tables from pinned memory
- Tables optimized for faster queries



Faster Report & Export Performance

- Report related tables pinned into memory for faster retrieval.
- Optimize tables based on platform capabilities.



Collector Throughput improvement

- Added Multithreaded processing capability to collector.
- Increased collector socket buffer size to avoid packet drops.

Major Data Reduction

- Remove detailed BLOB data > 7 days old (beyond 2.3 reductions)
- Database optimizations resulting in up to 80% efficiencies

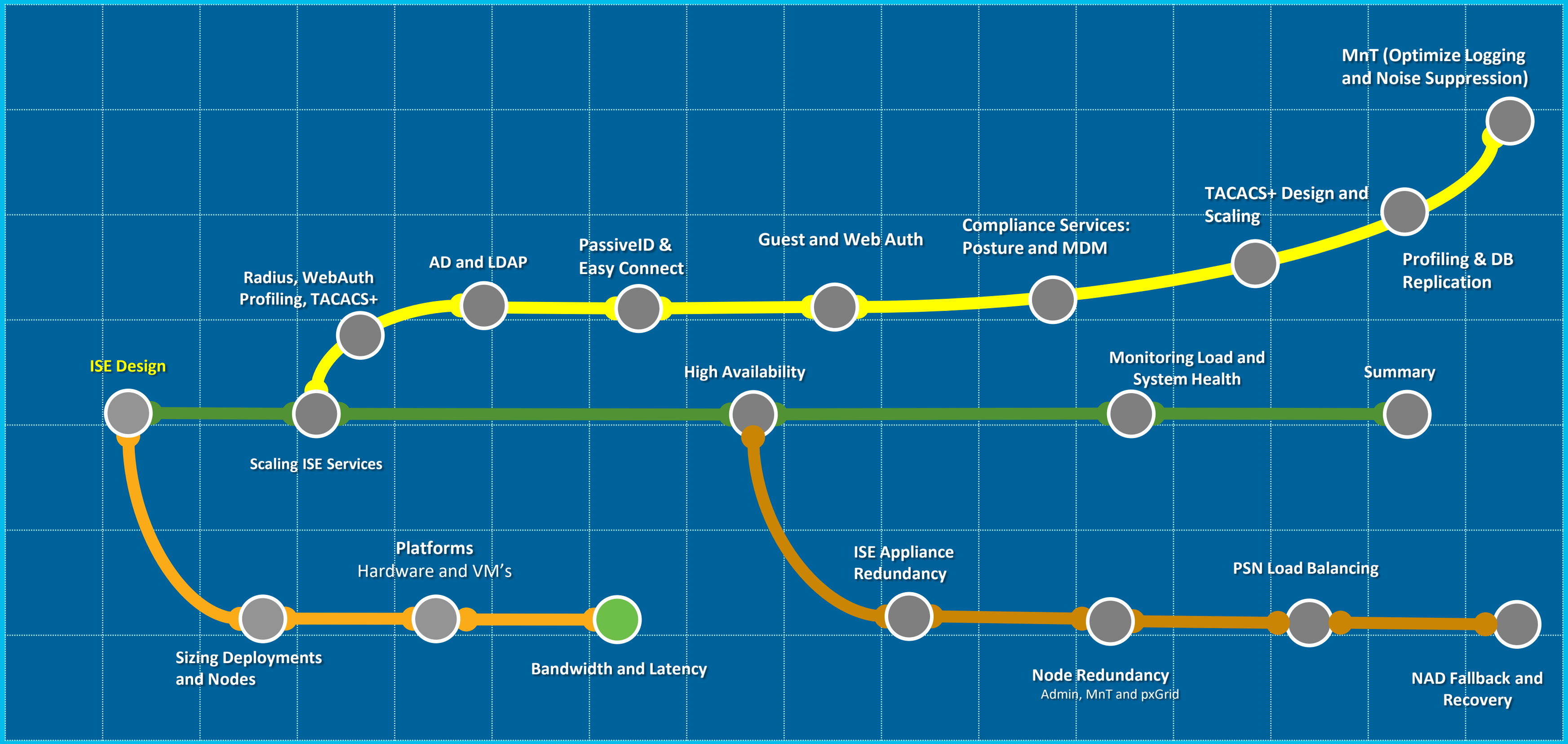
Where is my Super MnT VM ?

Appliance	SNS-3595 (Super MnT VM)	SNS-3695 Appliance
Processor	1 – Intel Xeon 2.60 GHz E5-2640	1 – Intel Xeon 2.10 GHz 4116
Cores per processor	8	12
Memory	256 GB	256 GB (8x32GB)
Hard Disk	4 x 600-GB 6Gb SAS 10K RPM	8 x 600-GB 6Gb SAS 10K RPM
Hardware RAID	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network Interfaces	6 x 1GBase-T	2 X 10Gbase-T 4 x 1GBase-T
Power Supplies	2 x 770W	2 x 770W

Session Agenda

Bandwidth and Latency

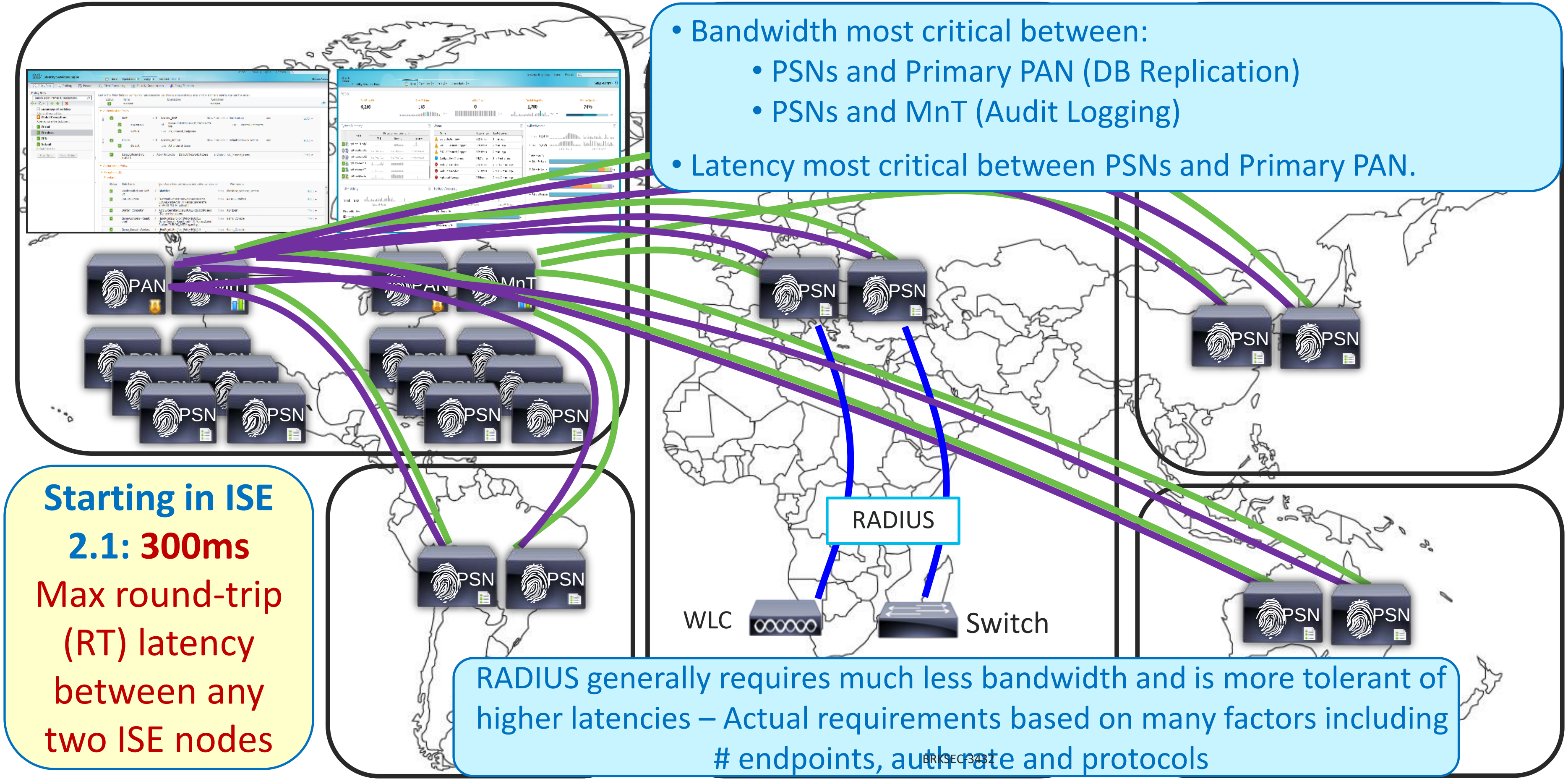
You Are Here ●



MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Bandwidth and Latency

- Bandwidth most critical between:
  - PSNs and Primary PAN (DB Replication)
  - PSNs and MnT (Audit Logging)
- Latency most critical between PSNs and Primary PAN.



Starting in ISE 2.1: 300ms

Max round-trip (RT) latency between any two ISE nodes

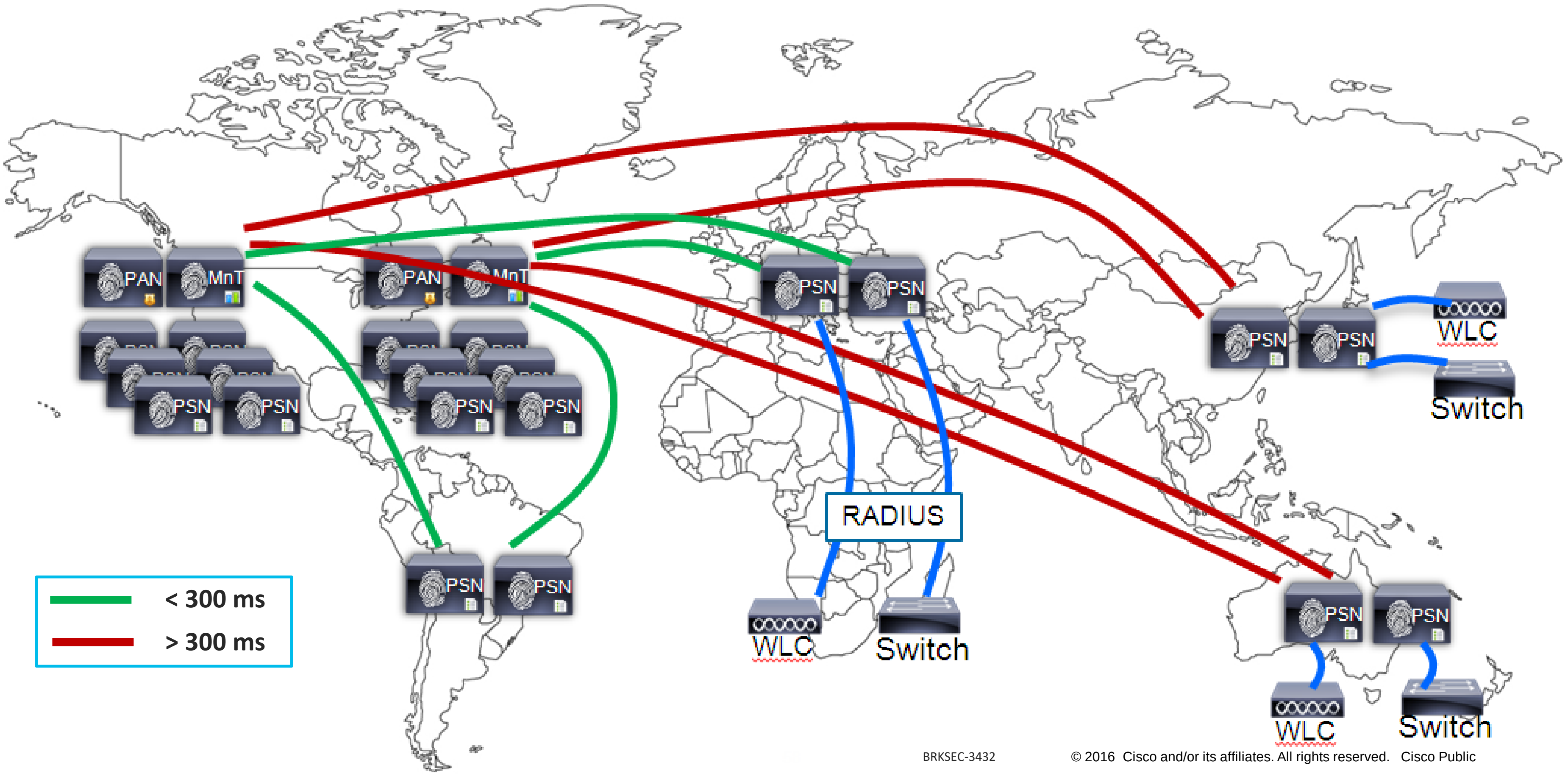
RADIUS generally requires much less bandwidth and is more tolerant of higher latencies – Actual requirements based on many factors including # endpoints, auth rate and protocols

Have I Told You My Story Over Latency Yet?

“Over Latency?” “No. I Don’t Think I’ll Ever Get Over Latency.”

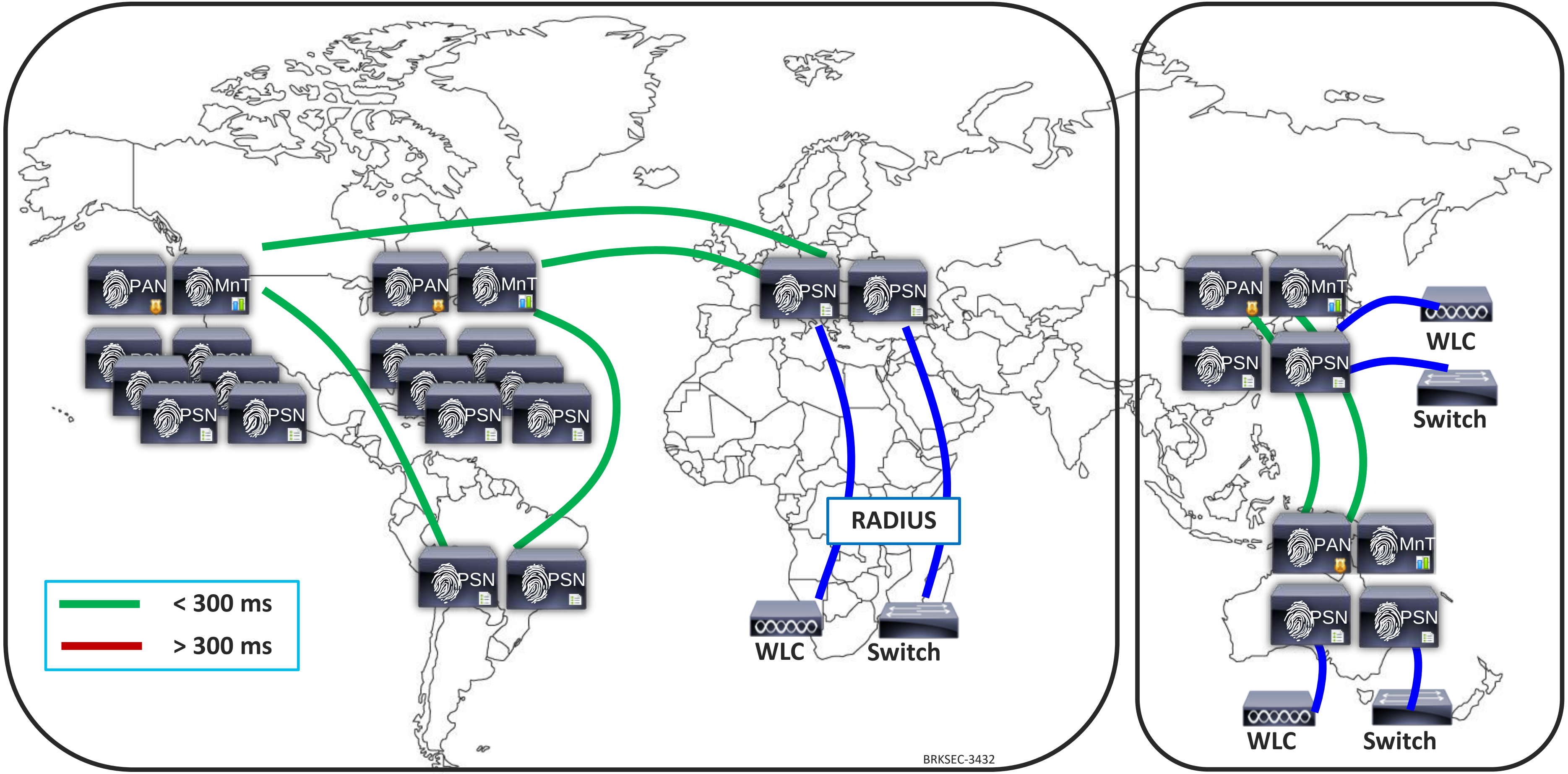
- Latency guidance is not a “fall off the cliff” number, but a guard rail based on what QA has tested.
- Not all customers have issues with > 300ms while others may have issues with <100ms latency due to overall ISE design and deployment.
- Profiler config is primary determinant in replication requirements between PSNs and PAN which translates to latency.
- When providing guidance, max 300ms roundtrip latency is the correct response from SEs for their customers to design against.

What if Distributed PSNs > 300ms RTT Latency?



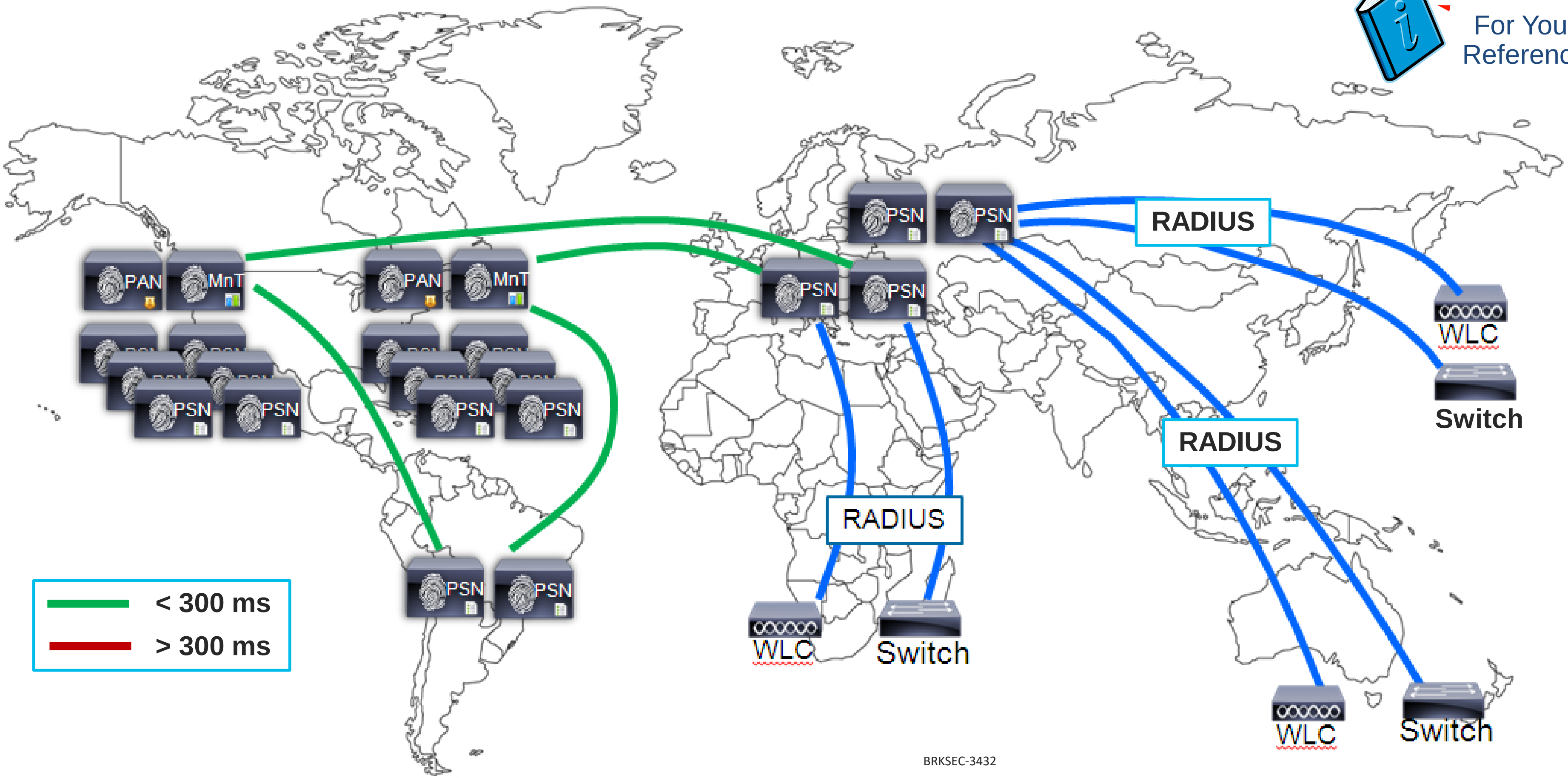
Option #1: Deploy Separate ISE Instances

Per-Instance Latency < 300ms



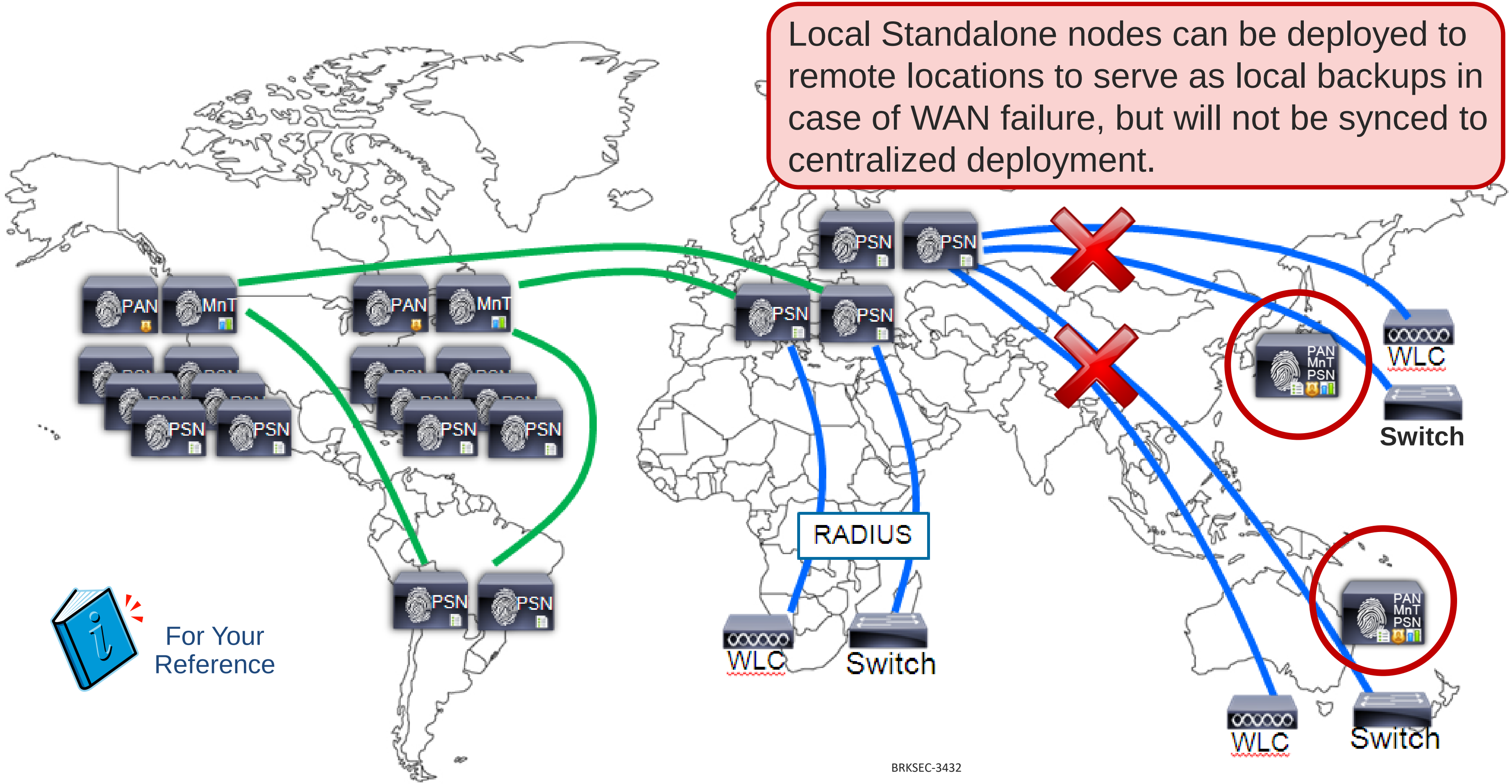
Option #2: Centralize PSNs Where Latency < 300ms

For Your Reference



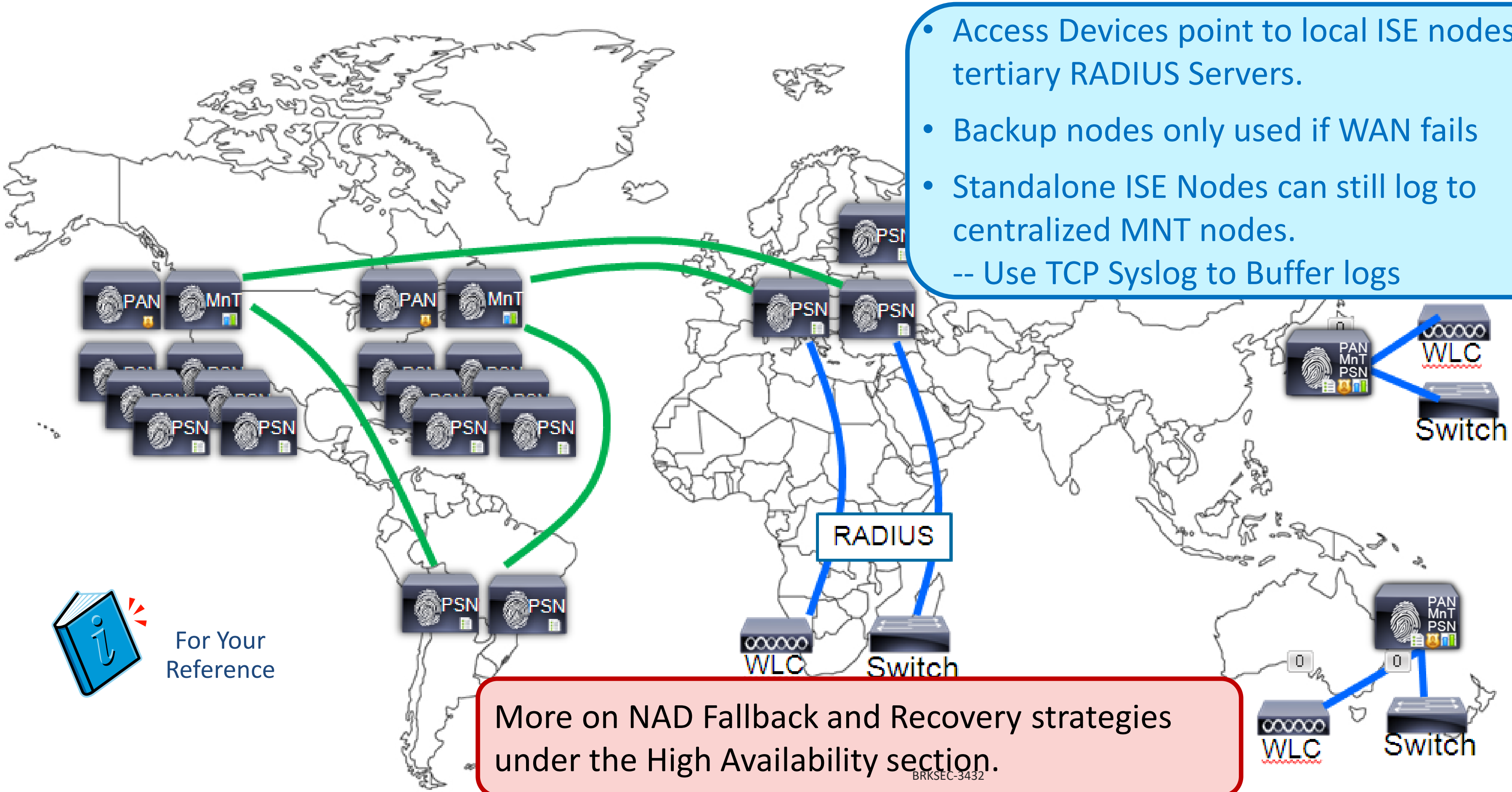
Deploy Local Standalone ISE Nodes as "Standby"

Local Standalone nodes can be deployed to remote locations to serve as local backups in case of WAN failure, but will not be synced to centralized deployment.



For Your Reference

Access Devices Fallback to Local PSNs on WAN Failure

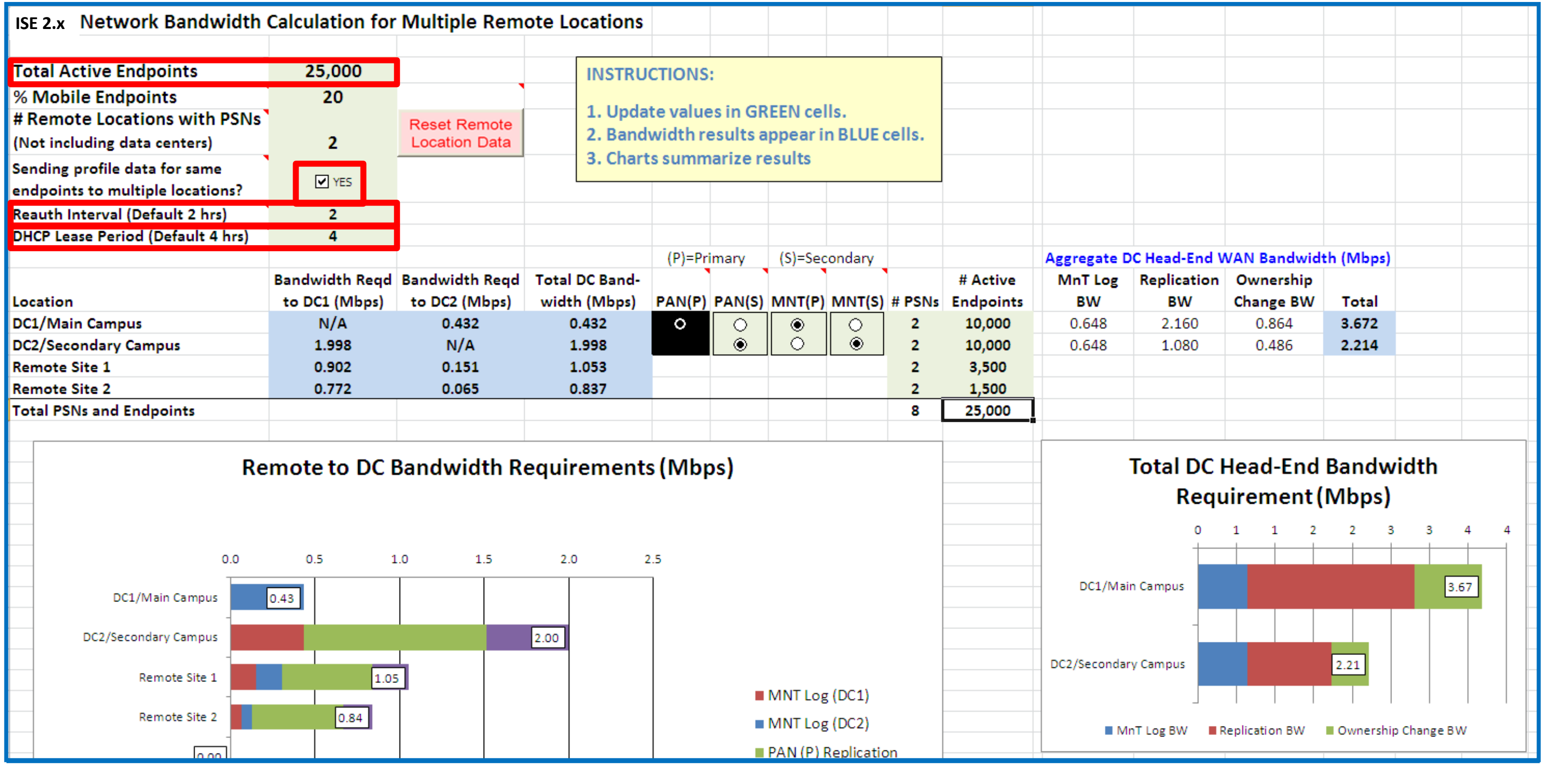


- Access Devices point to local ISE nodes as tertiary RADIUS Servers.
- Backup nodes only used if WAN fails
- Standalone ISE Nodes can still log to centralized MNT nodes.
  -- Use TCP Syslog to Buffer logs

For Your Reference

More on NAD Fallback and Recovery strategies under the High Availability section.

ISE Bandwidth Calculator – Updated for ISE 2.1+



ISE 2.x **Network Bandwidth Calculation for Multiple Remote Locations**

Total Active Endpoints	25,000
% Mobile Endpoints	20
# Remote Locations with PSNs (Not including data centers)	2
Sending profile data for same endpoints to multiple locations?	☑ YES
Reauth Interval (Default 2 hrs)	2
DHCP Lease Period (Default 4 hrs)	4

Reset Remote Location Data

INSTRUCTIONS:

1. Update values in GREEN cells.
2. Bandwidth results appear in BLUE cells.
3. Charts summarize results

(P)=Primary (S)=Secondary

Aggregate DC Head-End WAN Bandwidth (Mbps)

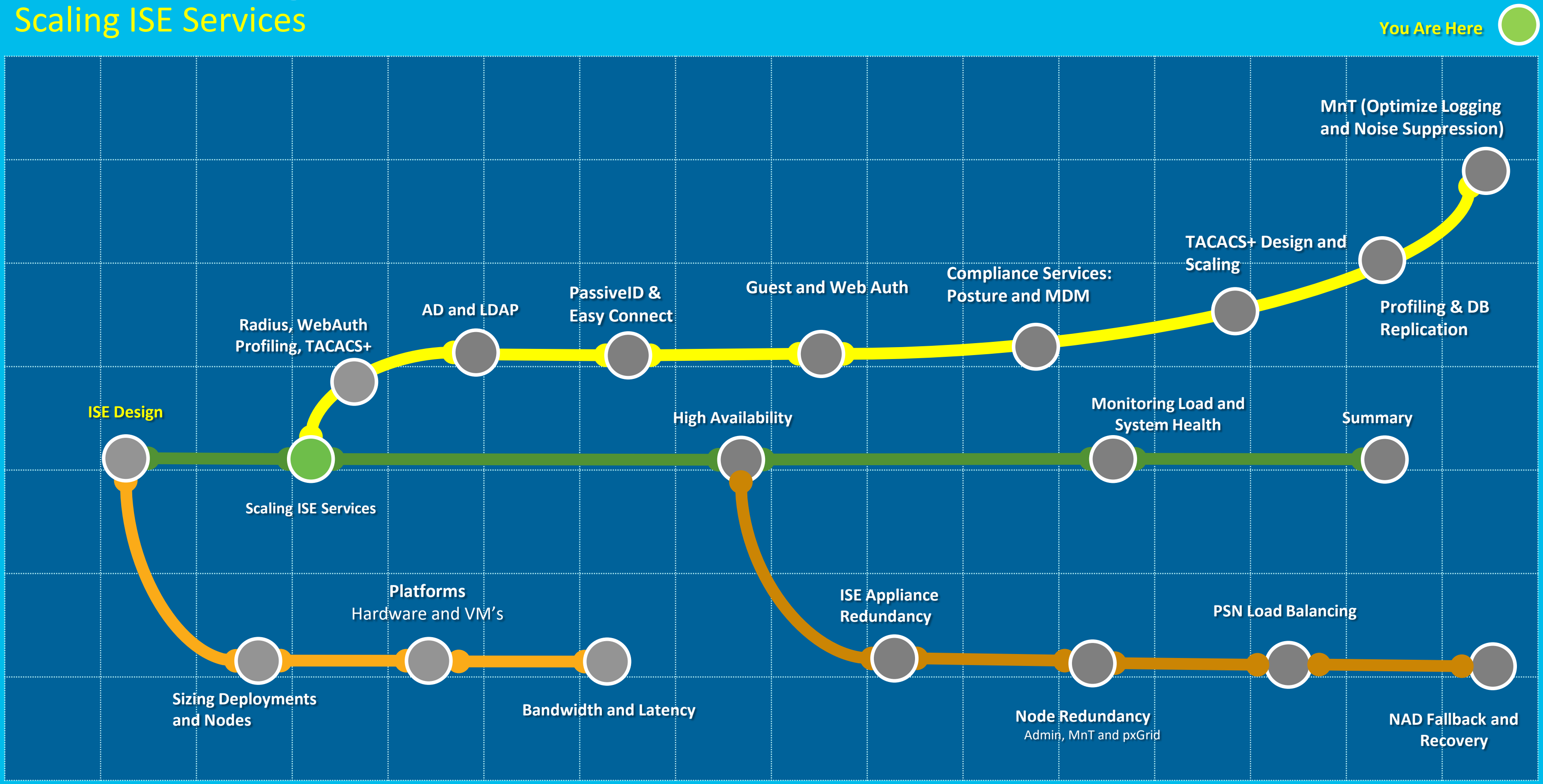
Location	Bandwidth Reqd to DC1 (Mbps)	Bandwidth Reqd to DC2 (Mbps)	Total DC Band-width (Mbps)	PAN(P)	PAN(S)	MNT(P)	MNT(S)	# PSNs	# Active Endpoints	MnT Log BW	Replication BW	Ownership Change BW	Total
DC1/Main Campus	N/A	0.432	0.432	○	○	●	○	2	10,000	0.648	2.160	0.864	3.672
DC2/Secondary Campus	1.998	N/A	1.998		●	○	●	2	10,000	0.648	1.080	0.486	2.214
Remote Site 1	0.902	0.151	1.053					2	3,500				
Remote Site 2	0.772	0.065	0.837					2	1,500				
Total PSNs and Endpoints								8	25,000				

Note: Bandwidth required for RADIUS traffic is not included. Calculator is focused on inter-ISE node bandwidth requirements.

Available to customers @ https://community.cisco.com/t5/security-documents/ise-latency-and-bandwidth-calculators/ta-p/3641112

Session Agenda

Scaling ISE Services



You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

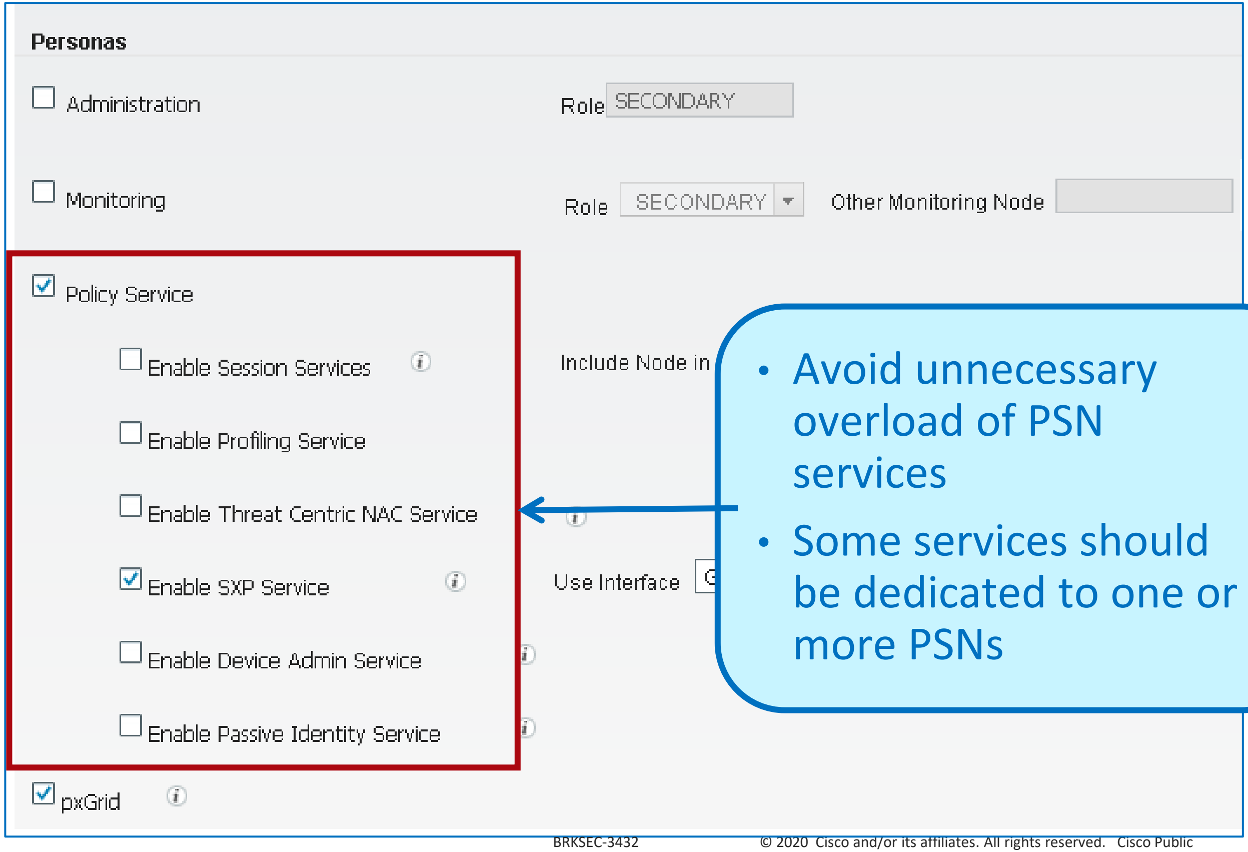
ISE Personas and Services

Enable Only What Is Needed !!

Session Services includes base user services such as RADIUS, Guest, Posture, MDM, BYOD/CA

- ISE Personas:
  - PAN
  - MNT
  - PSN
  - pxGrid

- PSN Services
  - Session
  - Profiling
  - TC-NAC
  - ISE SXP
  - Device Admin (TACACS+)
  - Passive Identity (Easy Connect)



Personas

☐ Administration — Role: SECONDARY

☐ Monitoring — Role: SECONDARY — Other Monitoring Node:

☑ Policy Service
- ☐ Enable Session Services
- ☐ Enable Profiling Service
- ☐ Enable Threat Centric NAC Service
- ☑ Enable SXP Service
- ☐ Enable Device Admin Service
- ☐ Enable Passive Identity Service

Include Node in

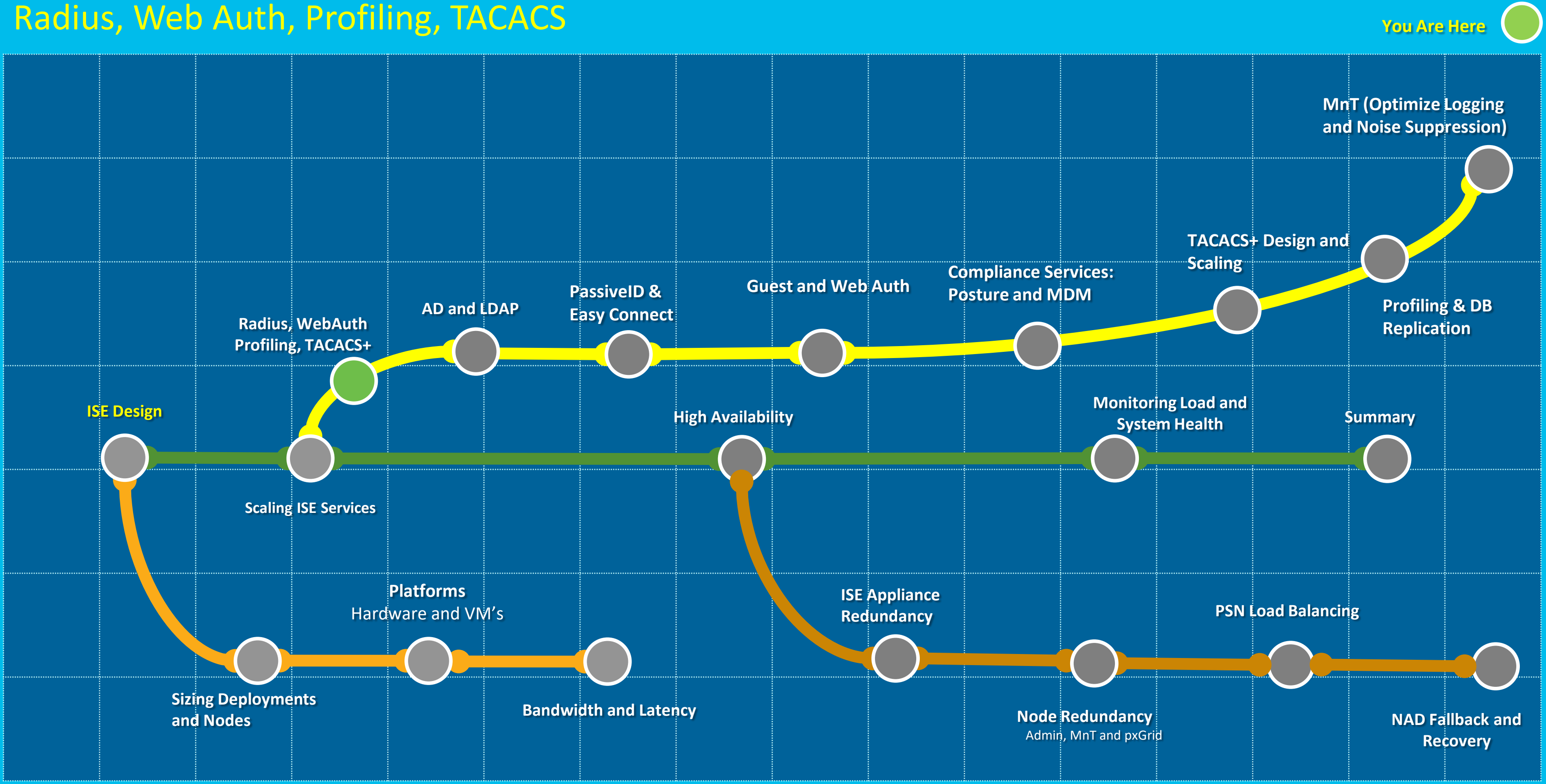
Use Interface

☑ pxGrid

- Avoid unnecessary overload of PSN services
- Some services should be dedicated to one or more PSNs

Session Agenda

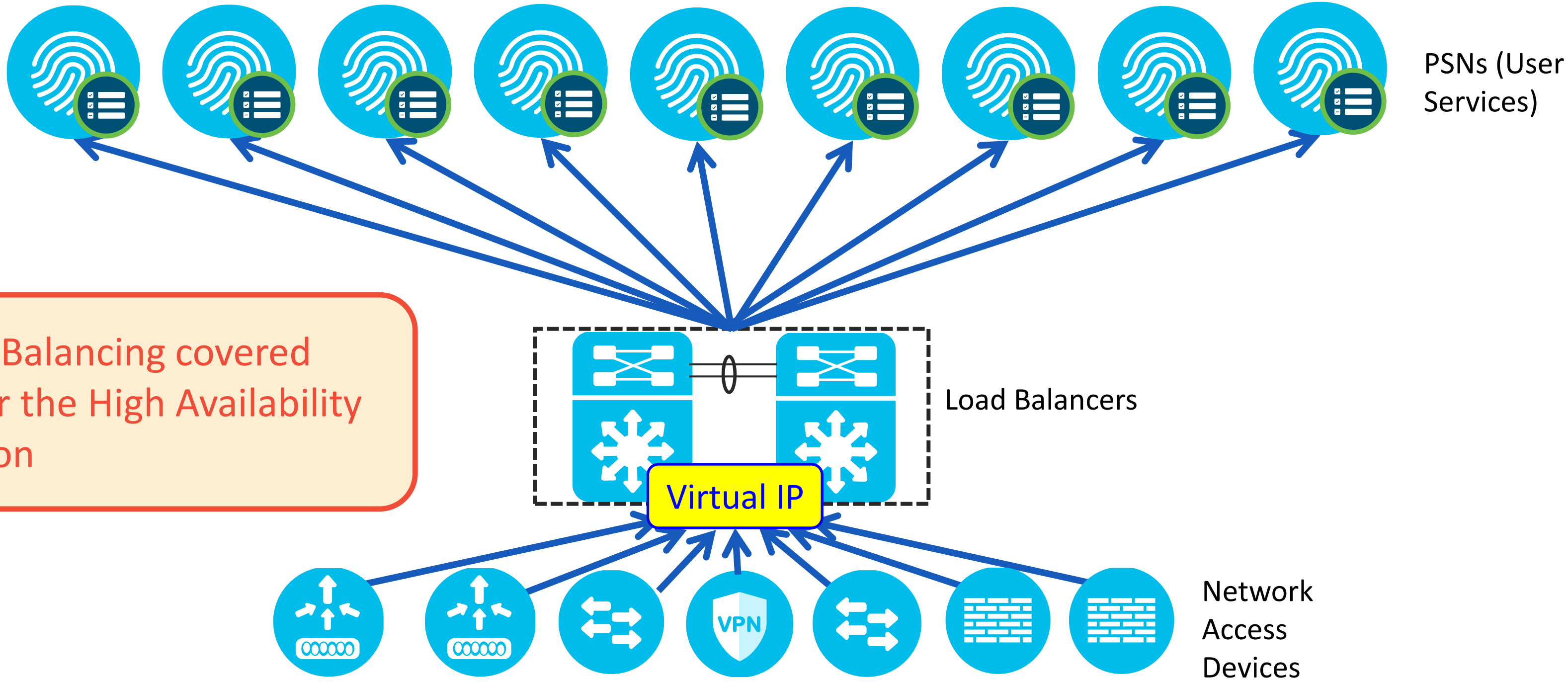
Radius, Web Auth, Profiling, TACACS



You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Scaling RADIUS, Web, Profiling, and TACACS+ w/LB

- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS and TACACS+ AAA requests to LB virtual IP.

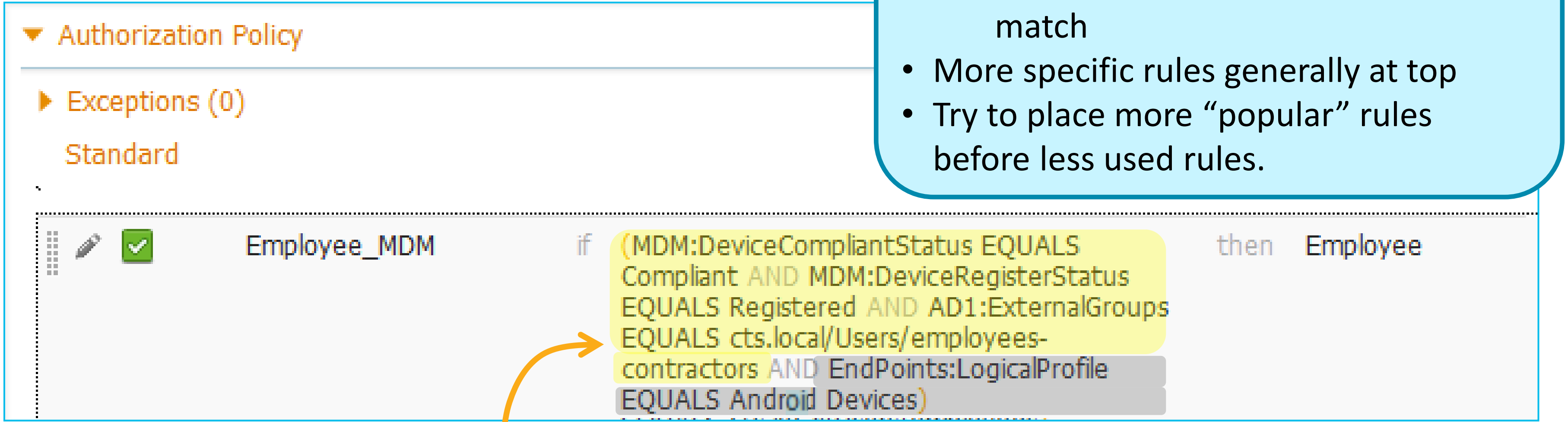


Load Balancing covered under the High Availability Section

Auth Policy Optimization

Avoid Unnecessary External Store Lookups

- Policy Logic:
  - First Match, Top Down
  - Skip Rule on first negative condition match
- More specific rules generally at top
- Try to place more "popular" rules before less used rules.



Authorization Policy

Exceptions (0)

Standard

Employee_MDM if (MDM:DeviceCompliantStatus EQUALS Compliant AND MDM:DeviceRegisterStatus EQUALS Registered AND AD1:ExternalGroups EQUALS cts.local/Users/employees-contractors AND EndPoints:LogicalProfile EQUALS Android Devices) then Employee

Example of a Poor Rule: Employee_MDM

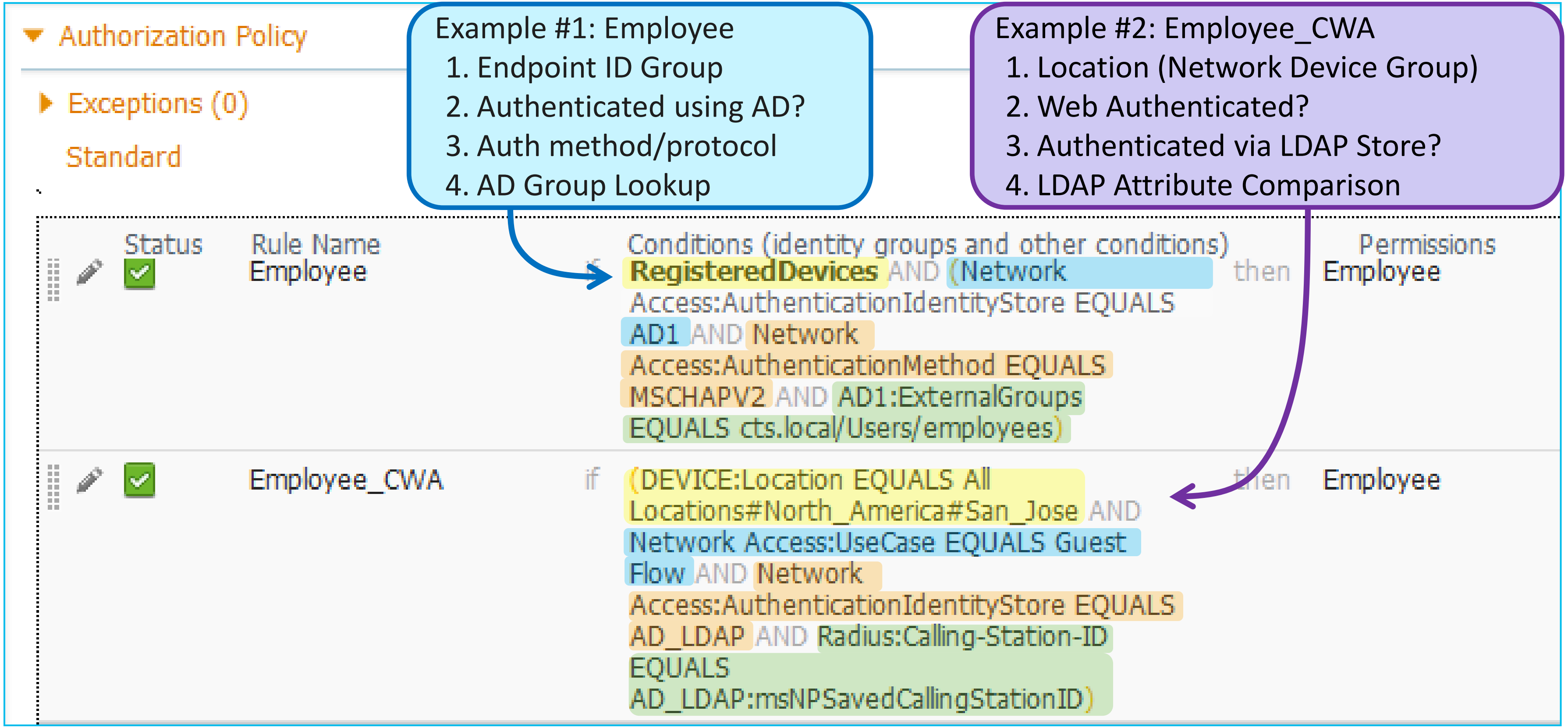
- All lookups to External Policy and ID Stores performed first, then local profile match!

For Your Reference

Auth Policy Optimization

Rule Sequence and Condition Order is Important!

For Your Reference



Example #1: Employee
1. Endpoint ID Group
2. Authenticated using AD?
3. Auth method/protocol
4. AD Group Lookup

Example #2: Employee_CWA
1. Location (Network Device Group)
2. Web Authenticated?
3. Authenticated via LDAP Store?
4. LDAP Attribute Comparison

Authorization Policy

Exceptions (0)

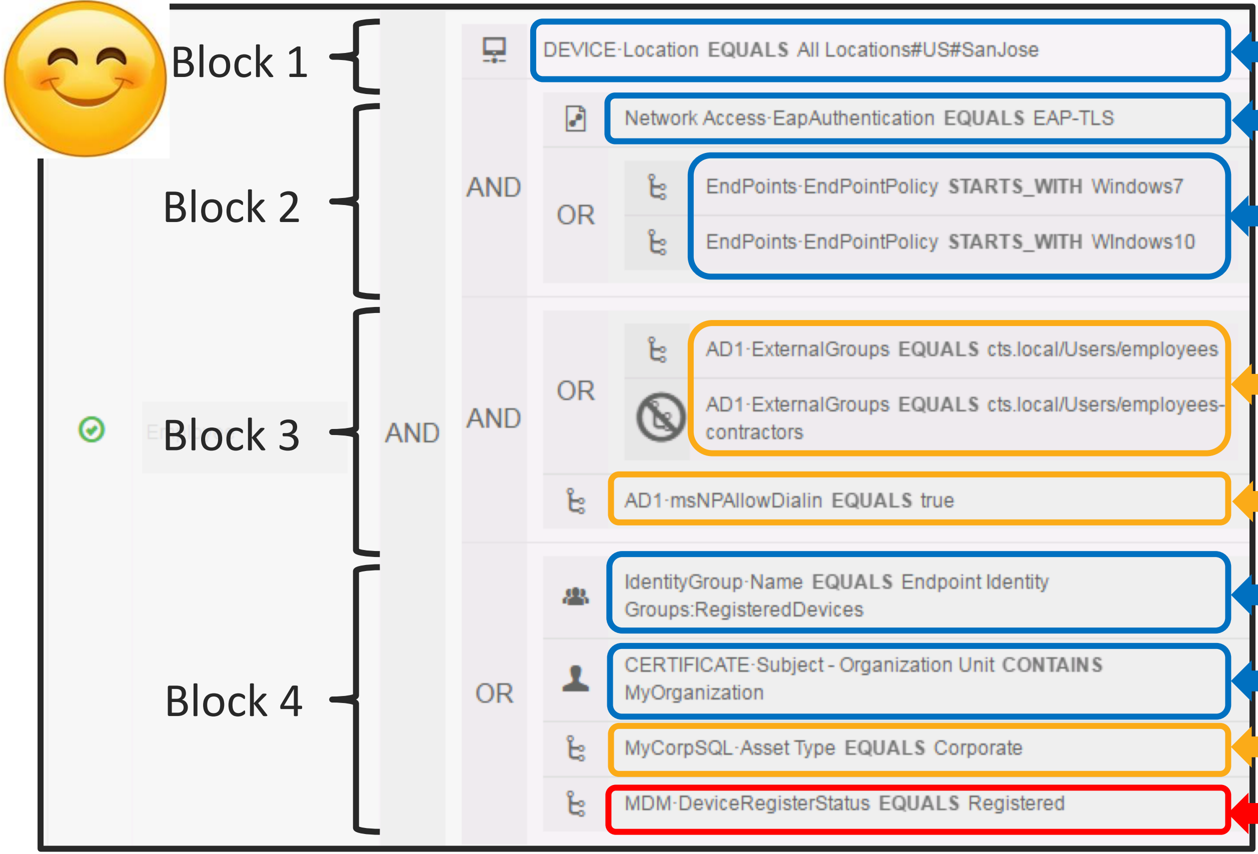
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Employee	if	RegisteredDevices AND (Network Access:AuthenticationIdentityStore EQUALS AD1 AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND AD1:ExternalGroups EQUALS cts.local/Users/employees)	then	Employee
✓	Employee_CWA	if	(DEVICE:Location EQUALS All Locations#North_America#San_Jose AND Network Access:UseCase EQUALS Guest Flow AND Network Access:AuthenticationIdentityStore EQUALS AD_LDAP AND Radius:Calling-Station-ID EQUALS AD_LDAP:msNPSavedCallingStationID)	then	Employee

Auth Policy Optimization

ISE 2.3 + Better Example!

For Your Reference



Block 1

DEVICE·Location EQUALS All Locations#US#SanJose

AND

Block 2

Network Access·EapAuthentication EQUALS EAP-TLS

OR

EndPoints·EndPointPolicy STARTS_WITH Windows7

EndPoints·EndPointPolicy STARTS_WITH Windows10

AND

Block 3

AND

OR

AD1·ExternalGroups EQUALS cts.local/Users/employees

AD1·ExternalGroups EQUALS cts.local/Users/employees-contractors

AD1·msNPAllowDialin EQUALS true

Block 4

OR

IdentityGroup·Name EQUALS Endpoint Identity Groups:RegisteredDevices

CERTIFICATE·Subject - Organization Unit CONTAINS MyOrganization

MyCorpSQL·Asset Type EQUALS Corporate

MDM·DeviceRegisterStatus EQUALS Registered

1. Location
2. Auth Method
3. Endpoint Profile
4. AD Groups
5. AD Attributes
6. ID Group
7. Certificate
8. SQL Attributes
9. MDM

For Your Reference

ISE 2.4+ Auth Policy Scale

- Max Policy Sets = **200**
  (up from 100 in 2.2)
- Max Authentication Rules = **1000**
  (up from 200 in 2.2)
- Max Authorization Rules = **3000**
  (up from 700 in 2.2)
- Max Authorization Profiles = **3200**
  (up from 1000 in 2.2)

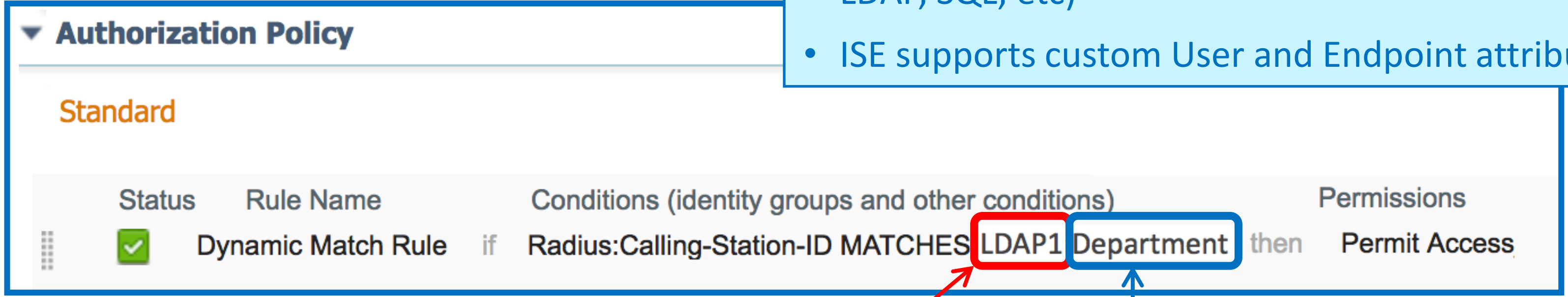
Dynamic Variable Substitution

For Your Reference

Rule Reduction

- Match conditions to unique values stored per-User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc)
- ISE supports custom User and Endpoint attributes

- Authorization Policy Conditions



Authorization Policy

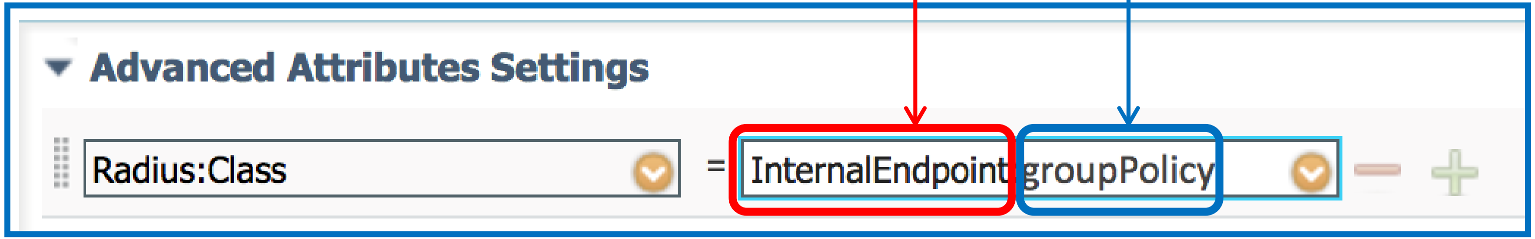
Standard

	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	☑	Dynamic Match Rule	if	Radius:Calling-Station-ID MATCHES LDAP1 Department	then	Permit Access

ID Store

Attribute

- Authorization Profile Conditions



Advanced Attributes Settings

Radius:Class = InternalEndpoint groupPolicy

Dynamic DACLs in Authorization Profile

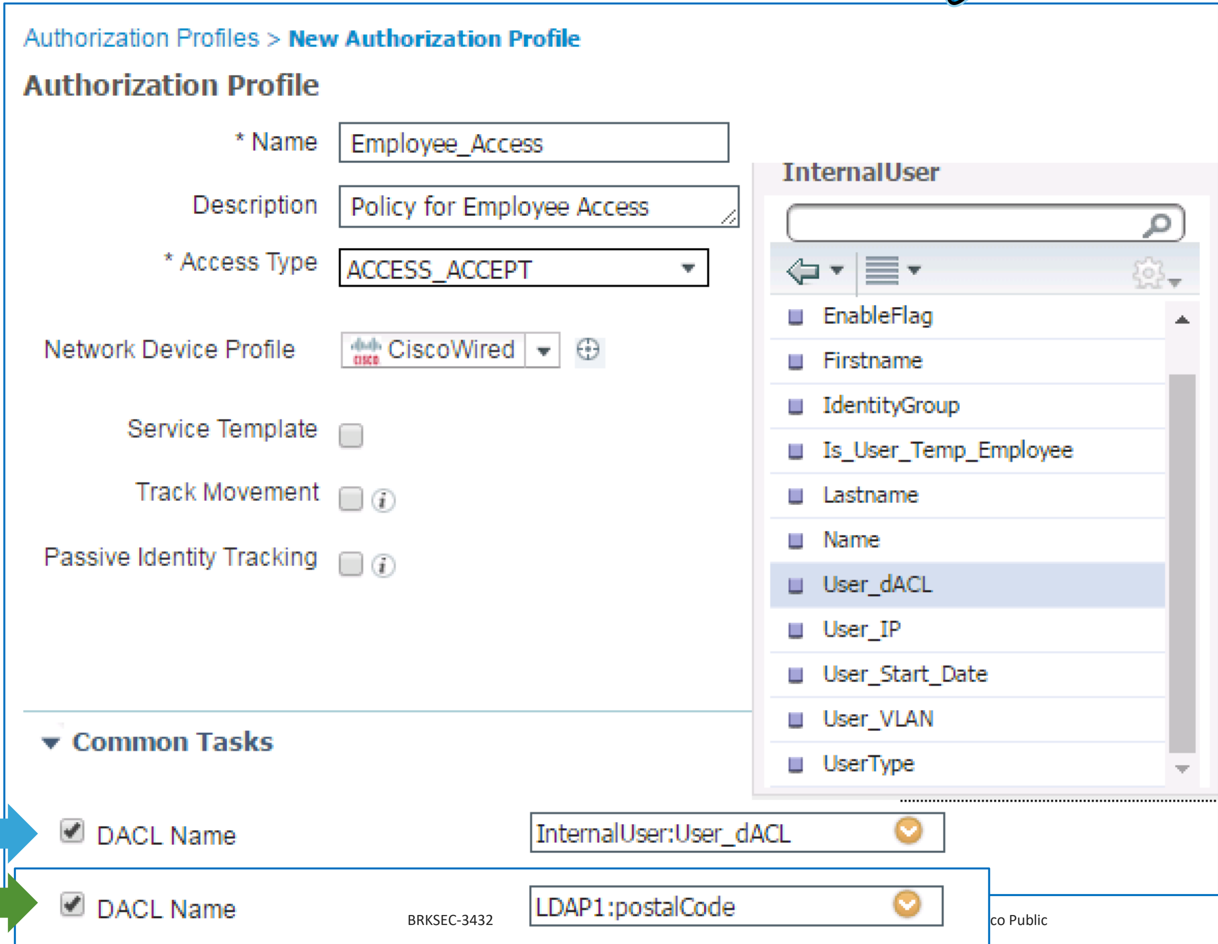
For Your Reference

Per-User Policy in 1 rule

1. Populate attribute in internal or external ID store.
2. Reference attribute in Authorization Profile under dACL

Internal User example

External User example



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: Employee_Access

Description: Policy for Employee Access

* Access Type: ACCESS_ACCEPT

Network Device Profile: CiscoWired

Service Template: □

Track Movement: □

Passive Identity Tracking: □

Common Tasks

☑ DACL Name: InternalUser:User_dACL

☑ DACL Name: LDAP1:postalCode

InternalUser

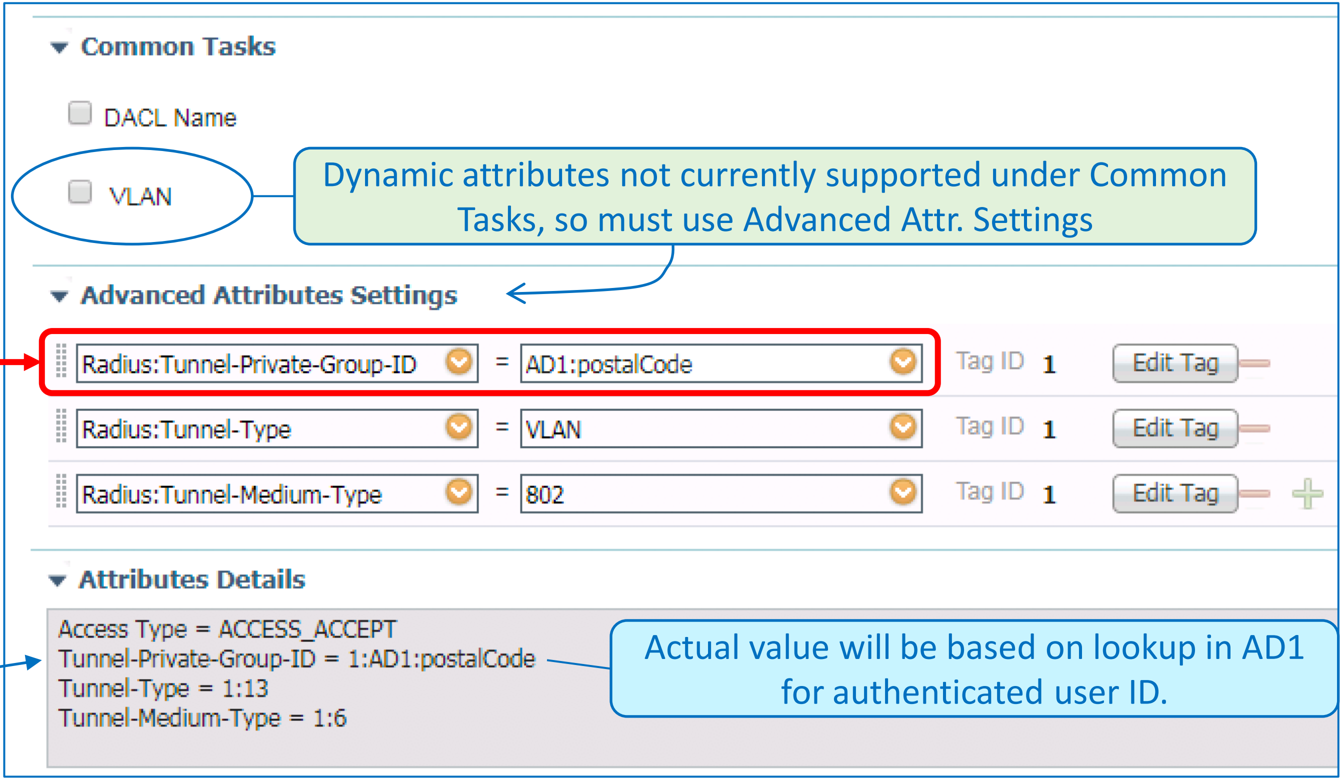
- EnableFlag
- Firstname
- IdentityGroup
- Is_User_Temp_Employee
- Lastname
- Name
- User_dACL
- User_IP
- User_Start_Date
- User_VLAN
- UserType

Dynamic VLANs in Authorization Profile

For Your Reference

Per-User/Endpoint Policy in Single Authorization Rule

- Set VLAN number of name in unique attribute in local or external ID store.
- Ex: AD1:postalcode
- VLAN value will be retrieved and replaced with variable name:



▾ Common Tasks

□ DACL Name

□ VLAN

Dynamic attributes not currently supported under Common Tasks, so must use Advanced Attr. Settings

▾ Advanced Attributes Settings

Radius:Tunnel-Private-Group-ID	=	AD1:postalCode	Tag ID	1	Edit Tag
Radius:Tunnel-Type	=	VLAN	Tag ID	1	Edit Tag
Radius:Tunnel-Medium-Type	=	802	Tag ID	1	Edit Tag

▾ Attributes Details

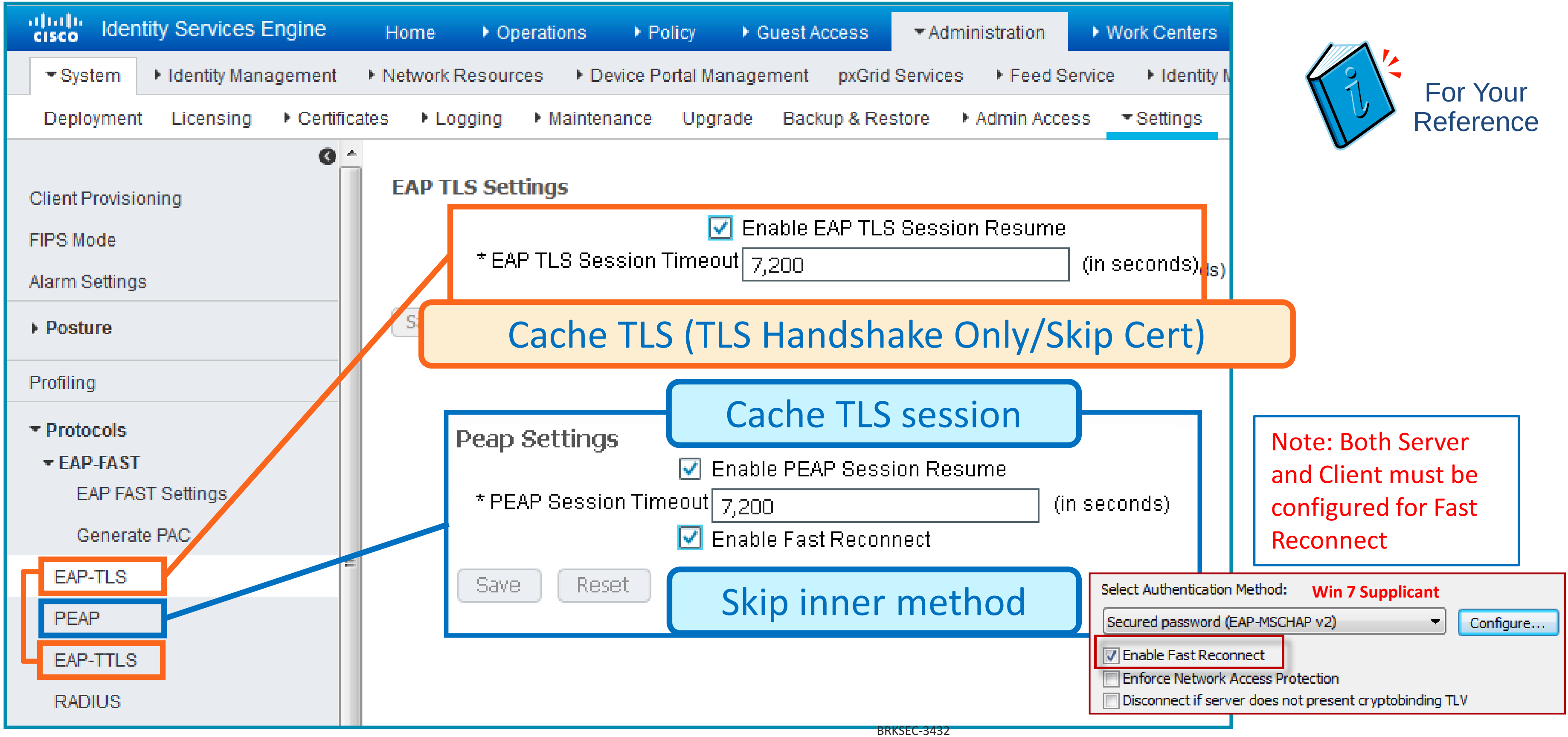
```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:AD1:postalCode
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Actual value will be based on lookup in AD1 for authenticated user ID.

Enable EAP Session Resume / Fast Reconnect

Major performance boost, but not complete auth so avoid excessive timeout value

For Your Reference



EAP TLS Settings

☑ Enable EAP TLS Session Resume

* EAP TLS Session Timeout 7,200 (in seconds)

Cache TLS (TLS Handshake Only/Skip Cert)

Cache TLS session

Peap Settings

☑ Enable PEAP Session Resume

* PEAP Session Timeout 7,200 (in seconds)

☑ Enable Fast Reconnect

Skip inner method

Note: Both Server and Client must be configured for Fast Reconnect

Win 7 Supplicant

Select Authentication Method: Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

☐ Enforce Network Access Protection

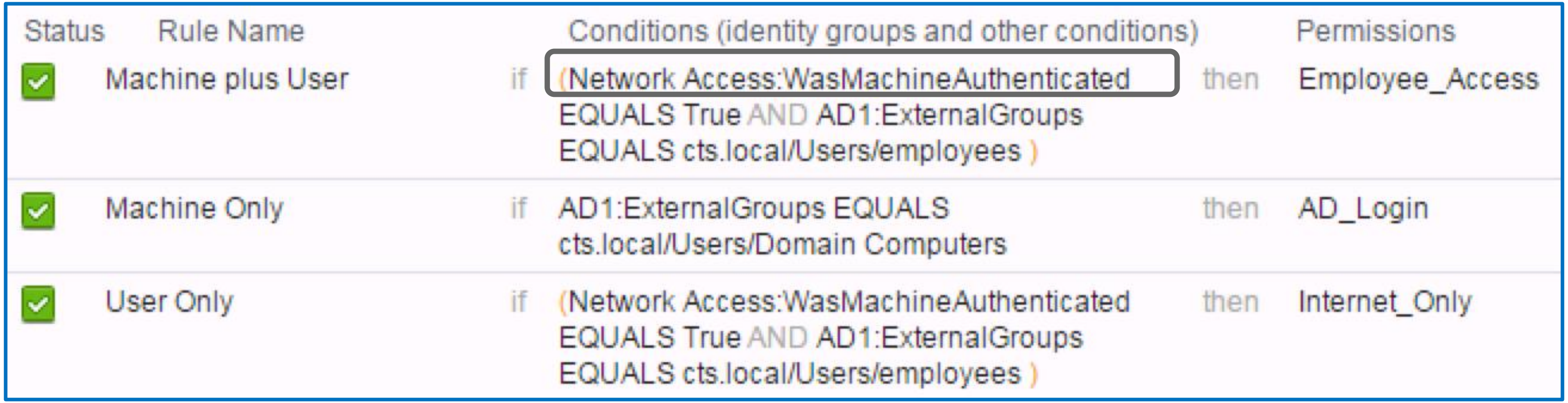
☐ Disconnect if server does not present cryptobinding TLV

Machine Access Restrictions (MAR)

For Your Reference

Couples Machine + User Authentication

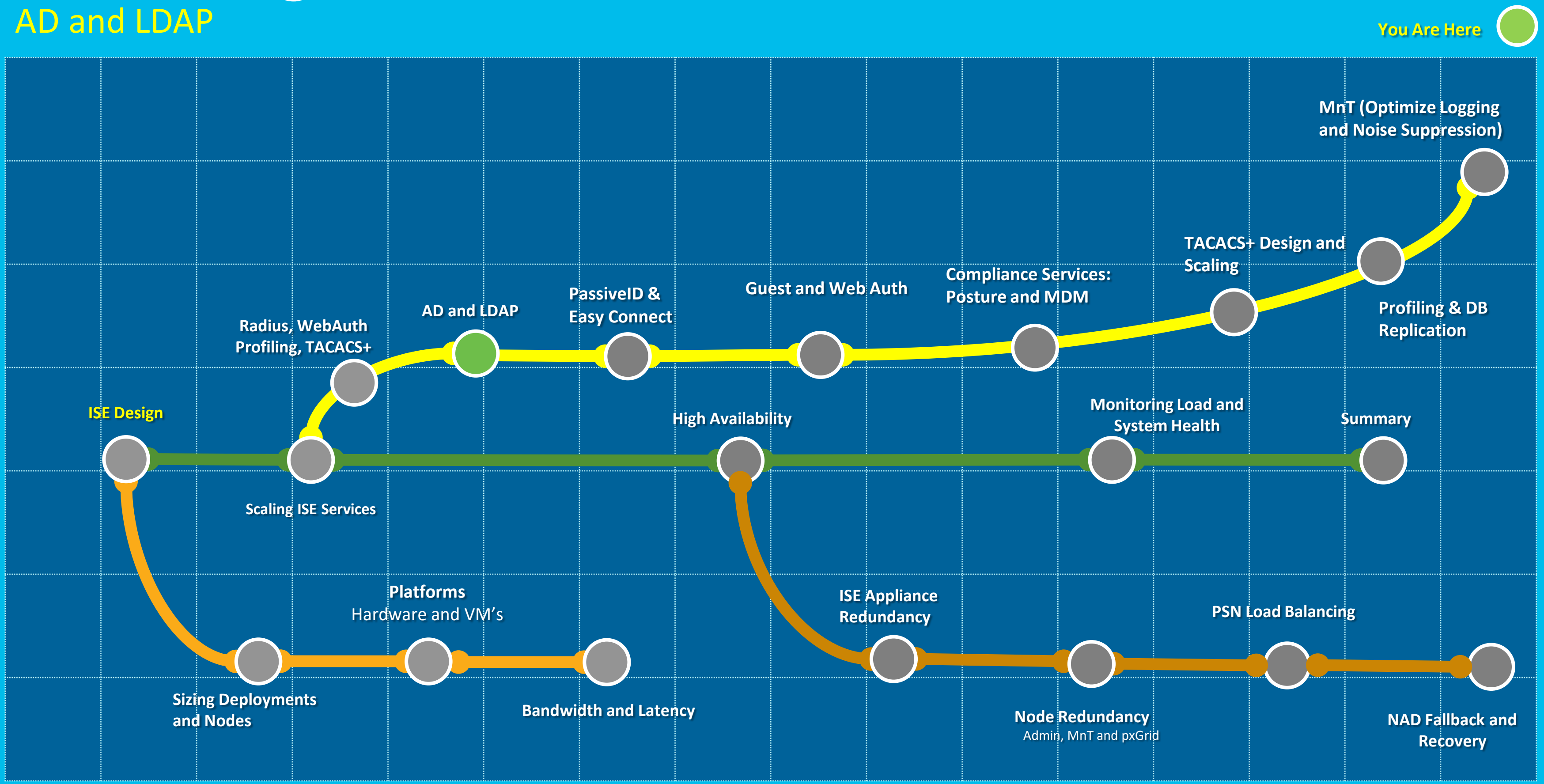
- MAR caches a Machine Authentication via Calling-Station-ID (MAC Address)
- User can be required to have existing cache entry to pass authorization.
- Susceptible to sync issues, especially if cache expires, requiring client restart



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Machine plus User	if	(Network Access:WasMachineAuthenticated EQUALS True AND AD1:ExternalGroups EQUALS cts.local/Users/employees)	then	Employee_Access
☑	Machine Only	if	AD1:ExternalGroups EQUALS cts.local/Users/Domain Computers	then	AD_Login
☑	User Only	if	(Network Access:WasMachineAuthenticated EQUALS True AND AD1:ExternalGroups EQUALS cts.local/Users/employees)	then	Internet_Only

Session Agenda

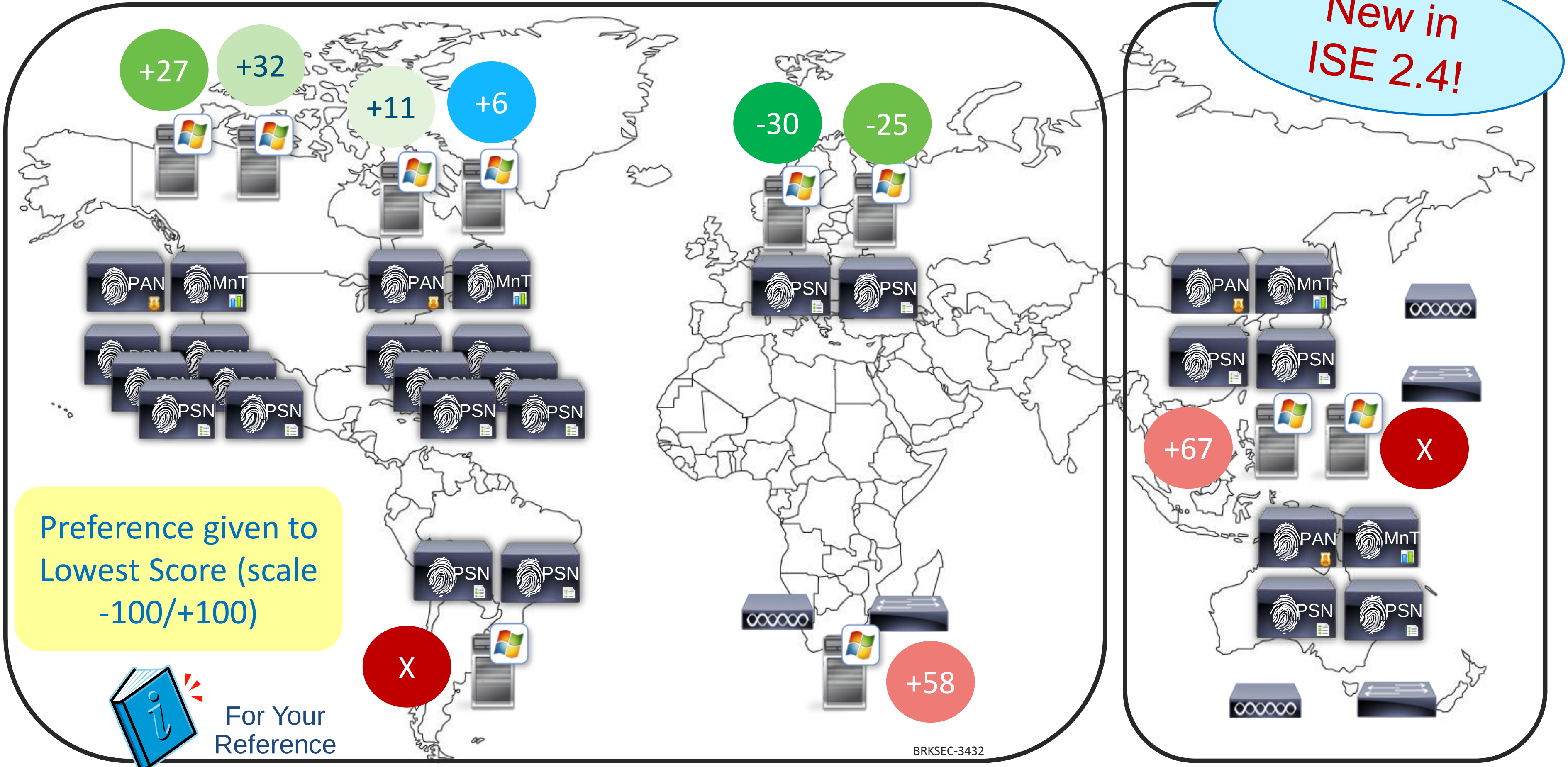
AD and LDAP


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Enhanced AD Domain Controller Management and Failover

Preferred DC Based on Scoring System

New in ISE 2.4!



Preference given to Lowest Score (scale -100/+100)

For Your Reference

Microsoft LDAP Changes - CSCvs67071

LDAP channel binding

- CVE-2017-8563
- Registry setting
- LDAP authentication over SSL/TLS more secure

LDAP Signing

- unsigned SASL/ non-SSL/TLS
- Look at summary event 2887
- http://go.microsoft.com/?linkid=9645087

My Lab testing:

- AD is not impacted
- Clear LDAP Text 389 fails – Secure LDAP 636 works

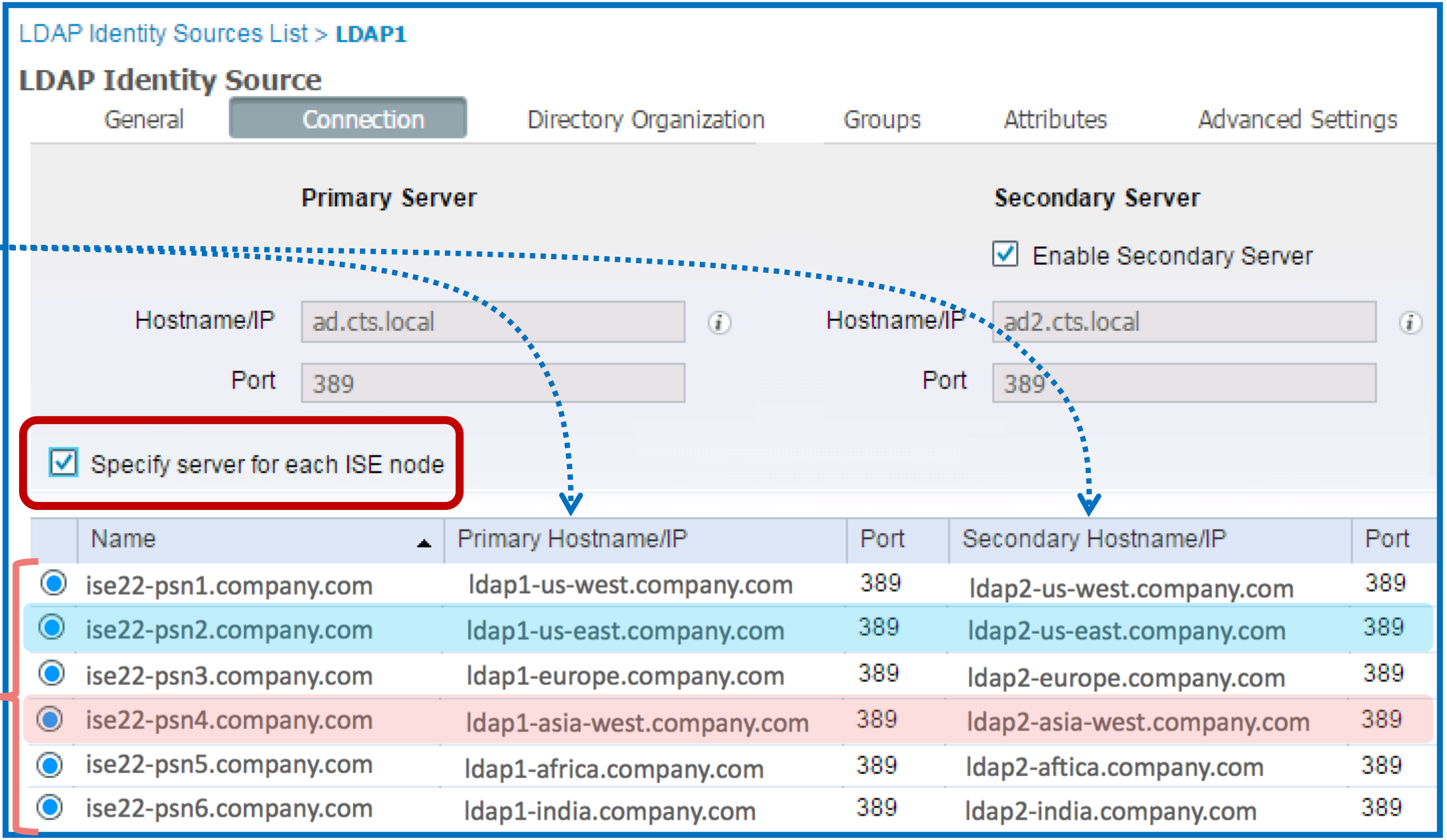
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-update-now/ba-p/921536

Per-PSN LDAP Servers

For Your Reference

Added in ISE 2.2!

- Assign unique Primary and Secondary to each PSN
- Allows each PSN to use local or regional LDAP Servers



LDAP Identity Sources List > **LDAP1**

LDAP Identity Source

Primary Server

Hostname/IP: ad.cts.local

Port: 389

Secondary Server

☑ Enable Secondary Server

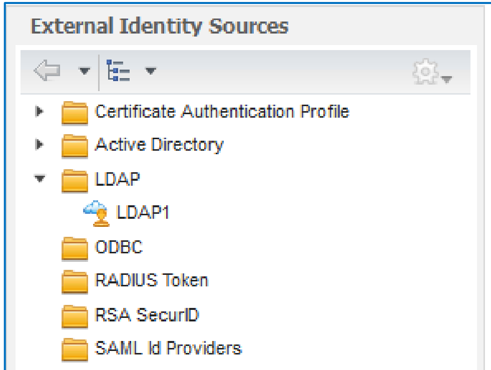
Hostname/IP: ad2.cts.local

Port: 389

☑ Specify server for each ISE node

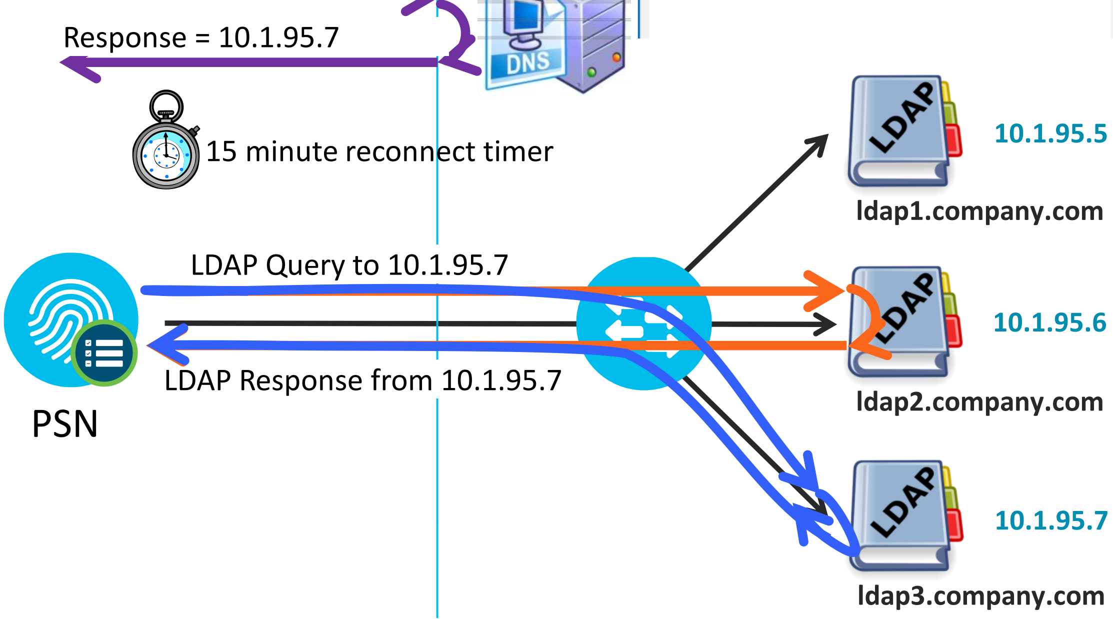
	Name	Primary Hostname/IP	Port	Secondary Hostname/IP	Port
●	ise22-psn1.company.com	ldap1-us-west.company.com	389	ldap2-us-west.company.com	389
●	ise22-psn2.company.com	ldap1-us-east.company.com	389	ldap2-us-east.company.com	389
●	ise22-psn3.company.com	ldap1-europe.company.com	389	ldap2-europe.company.com	389
●	ise22-psn4.company.com	ldap1-asia-west.company.com	389	ldap2-asia-west.company.com	389
●	ise22-psn5.company.com	ldap1-africa.company.com	389	ldap2-aftica.company.com	389
●	ise22-psn6.company.com	ldap1-india.company.com	389	ldap2-india.company.com	389

Load Balancing LDAP Servers



External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
  - LDAP1
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers



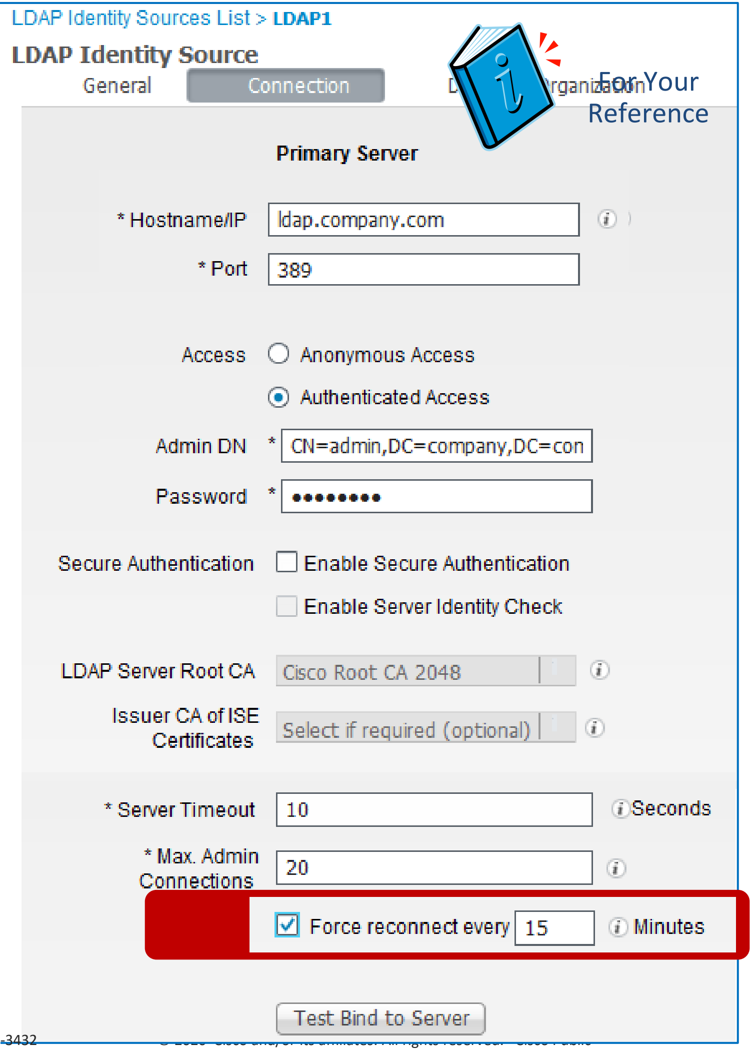
Lookup2 = ldap.company.com

Response = 10.1.95.7

15 minute reconnect timer

LDAP Query to 10.1.95.7

LDAP Response from 10.1.95.7



LDAP Identity Sources List > LDAP1

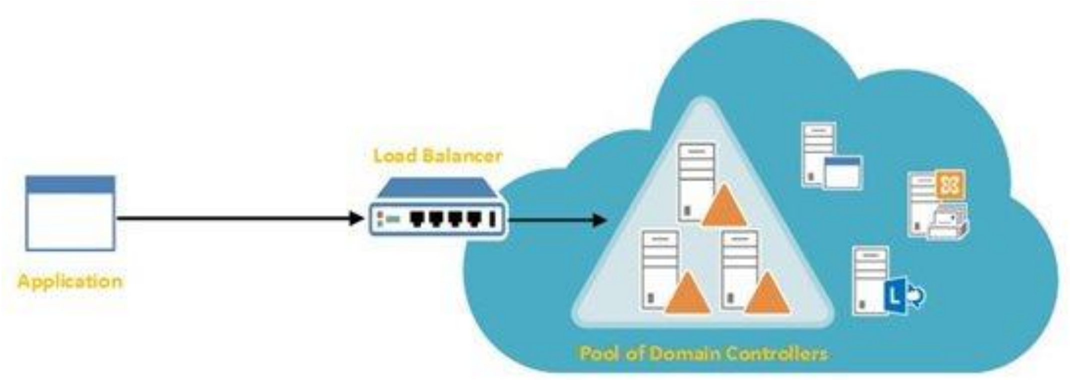
LDAP Identity Source

For Your Reference

Primary Server

* Hostname/IP	ldap.company.com
* Port	389
Access	○ Anonymous Access ● Authenticated Access
Admin DN *	CN=admin,DC=company,DC=con
Password *	●●●●●●●●●
Secure Authentication	□ Enable Secure Authentication □ Enable Server Identity Check
LDAP Server Root CA	Cisco Root CA 2048
Issuer CA of ISE Certificates	Select if required (optional)
* Server Timeout	10 Seconds
* Max. Admin Connections	20
☑ Force reconnect every	15 Minutes

Microsoft X-Directory load balance

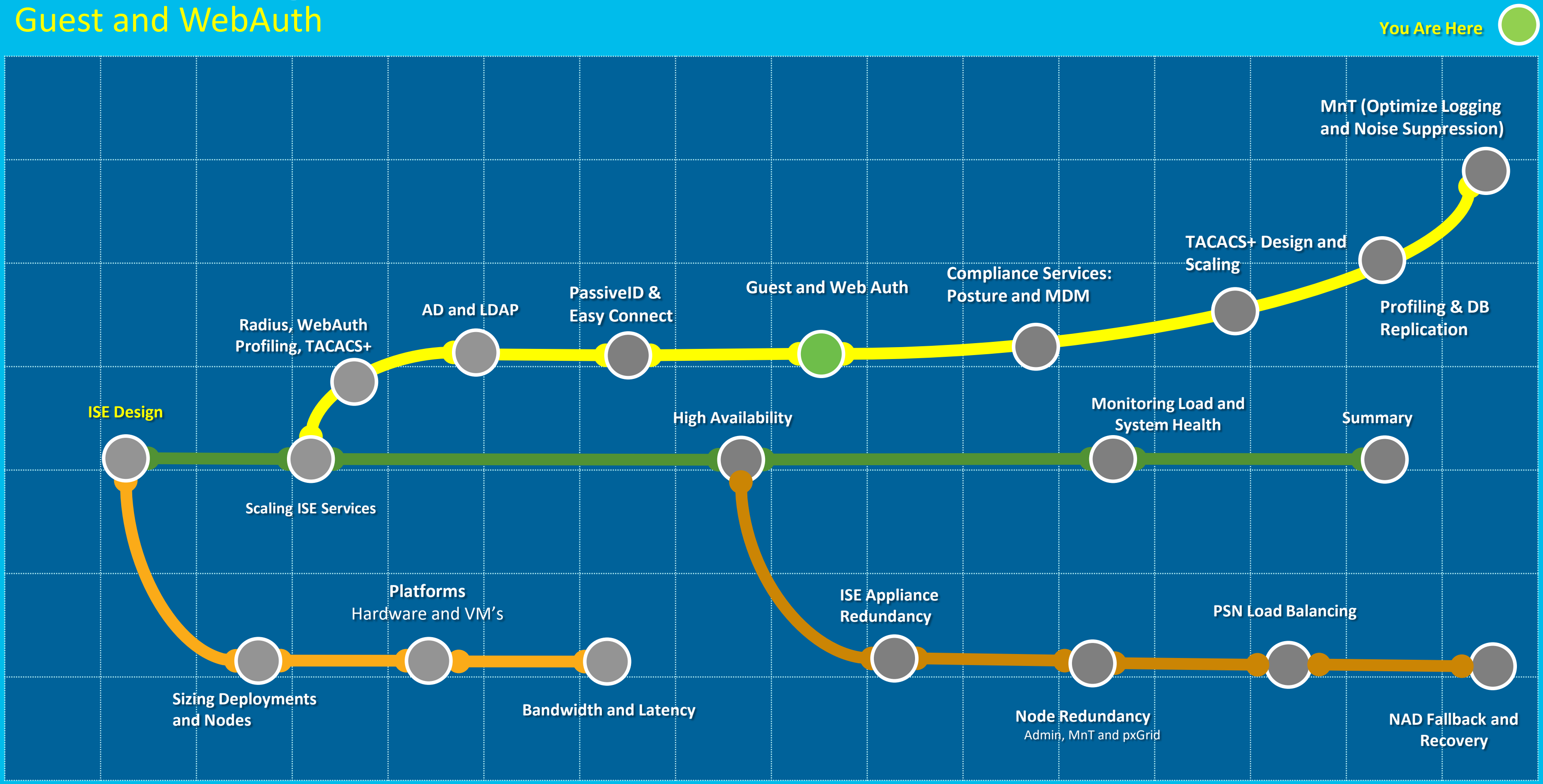


In this article we talked about Load Balancers and whether they are effective to use or not in an Active Directory infrastructure. Although implementing a Load Balancer and configuring Domain Controllers behind a VIP may work in short time, but they will repeatedly generate Kerberos errors and difficulties and clients will fail because of their inability to follow appropriate SPN. Note that by client I mean an AD-unaware application which is trying to work with LDAP.

https://social.technet.microsoft.com/wiki/contents/articles/33547.load-balancers-and-active-directory.aspx

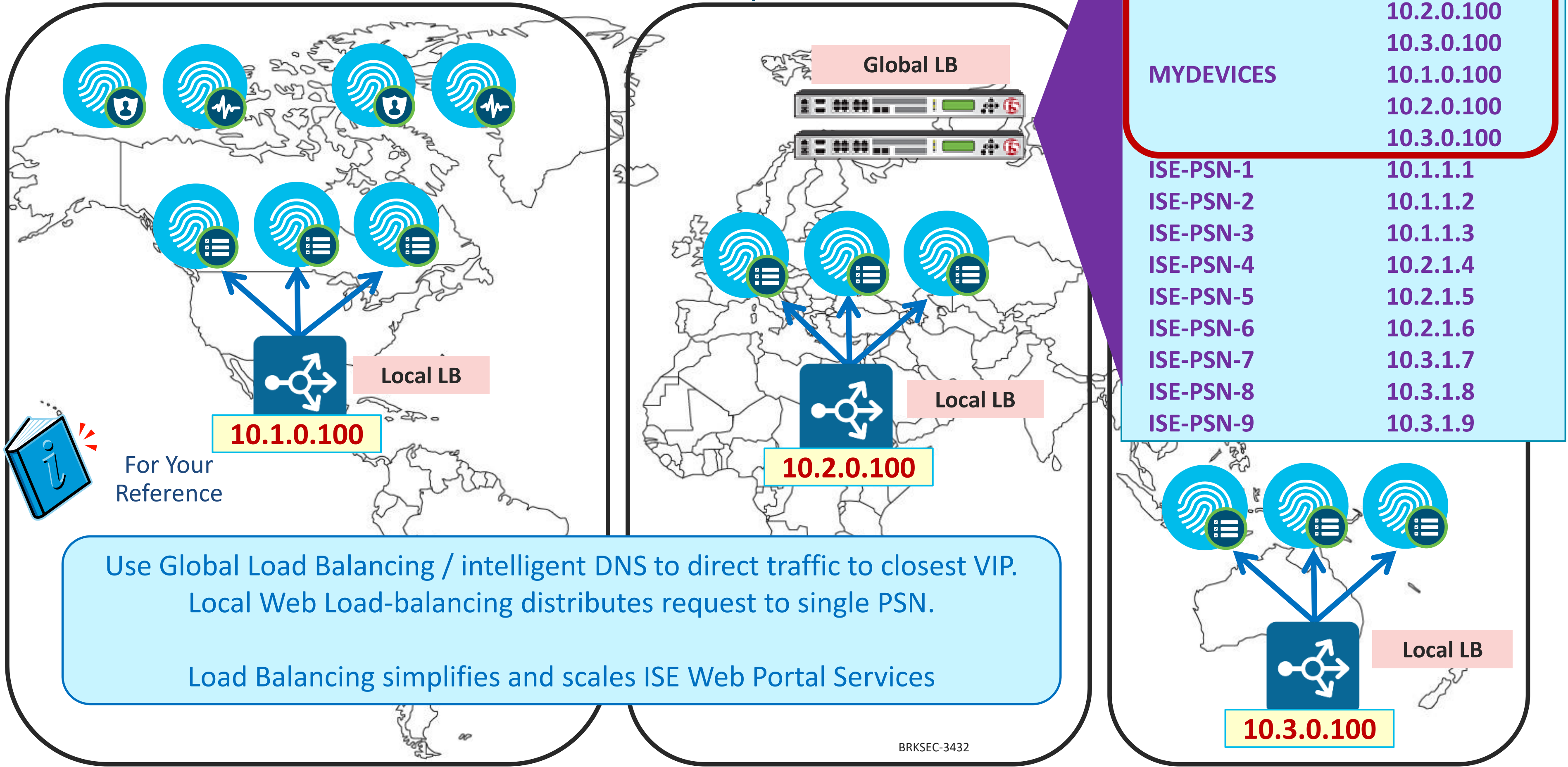
Session Agenda

Guest and WebAuth


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Scaling Global Sponsor / MyDevices

Global Load Balancers / "Smart DNS" Example



DNS SERVER: DOMAIN = COMPANY.COM

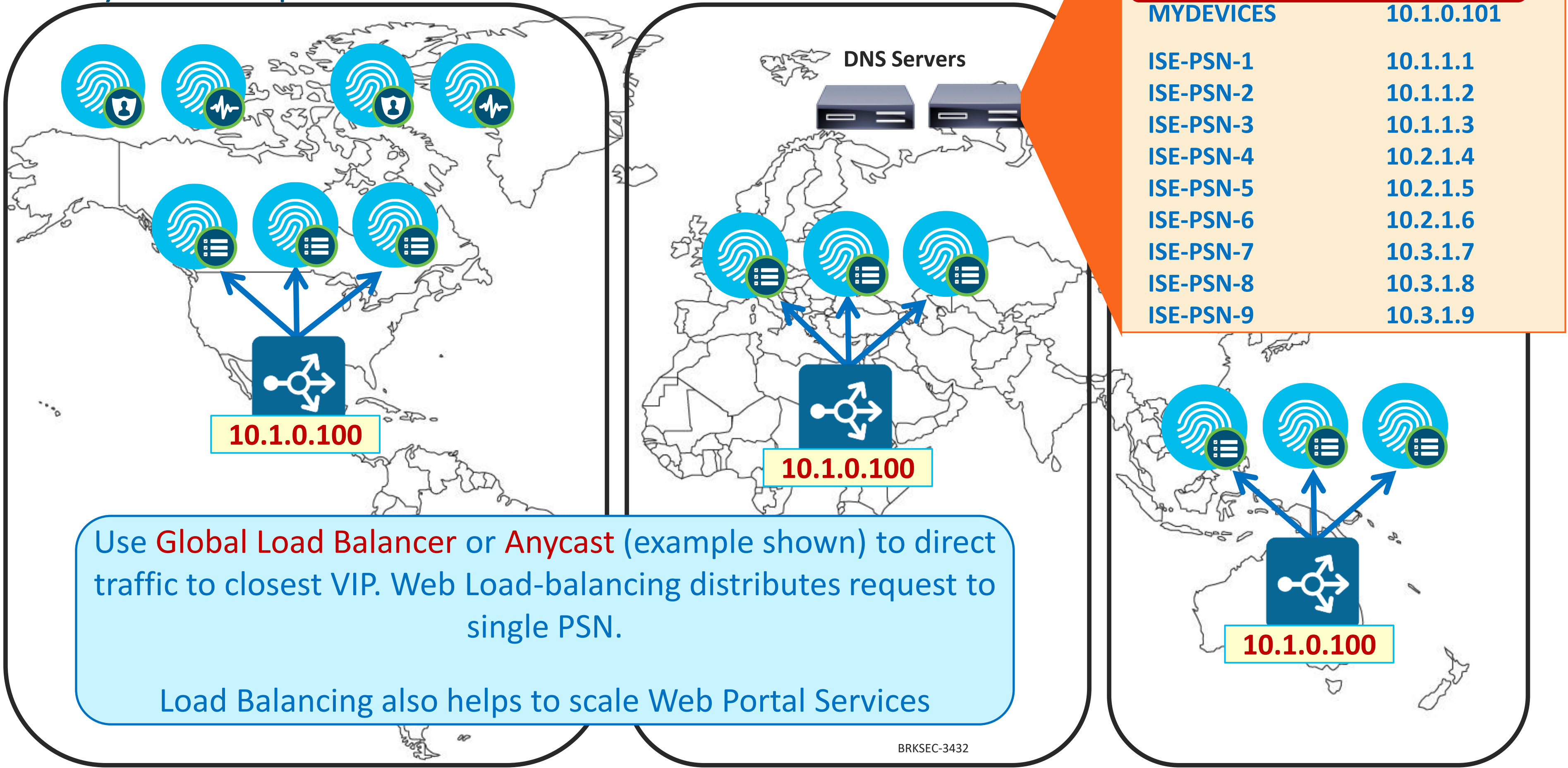
SPONSOR	10.1.0.100
	10.2.0.100
	10.3.0.100
MYDEVICES	10.1.0.100
	10.2.0.100
	10.3.0.100
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

Use Global Load Balancing / intelligent DNS to direct traffic to closest VIP.
Local Web Load-balancing distributes request to single PSN.

Load Balancing simplifies and scales ISE Web Portal Services

Scaling Global Sponsor / MyDevices

Anycast Example



DNS SERVER: DOMAIN = COMPANY.COM

SPONSOR	10.1.0.100
MYDEVICES	10.1.0.101
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

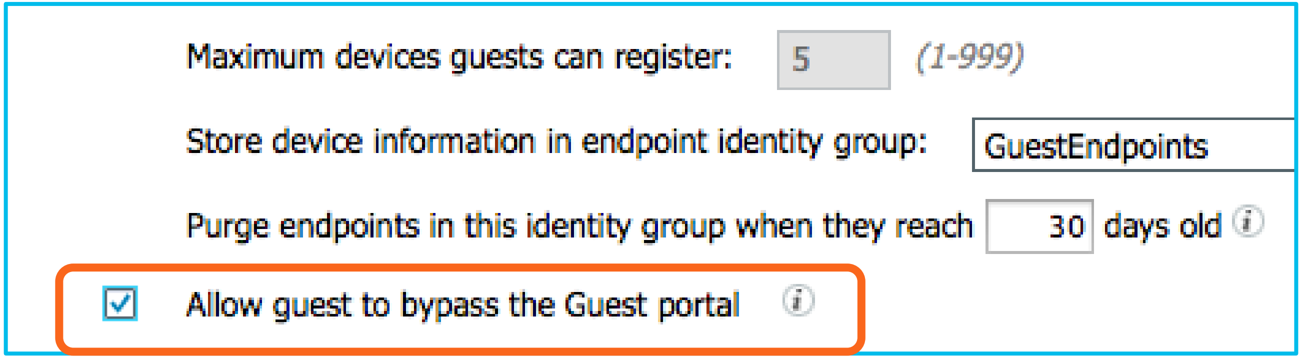
Use Global Load Balancer or Anycast (example shown) to direct traffic to closest VIP. Web Load-balancing distributes request to single PSN.

Load Balancing also helps to scale Web Portal Services

Scaling Guest Authentications Using 802.1X

“Activated Guest” allows guest accounts to be used without ISE web auth portal

- Guests auth with 802.1X using EAP methods like PEAP-MSCHAPv2 / EAP-GTC
- 802.1X auth performance generally much higher than web auth



Maximum devices guests can register: 5 (1-999)

Store device information in endpoint identity group: GuestEndpoints

Purge endpoints in this identity group when they reach 30 days old

☑ Allow guest to bypass the Guest portal

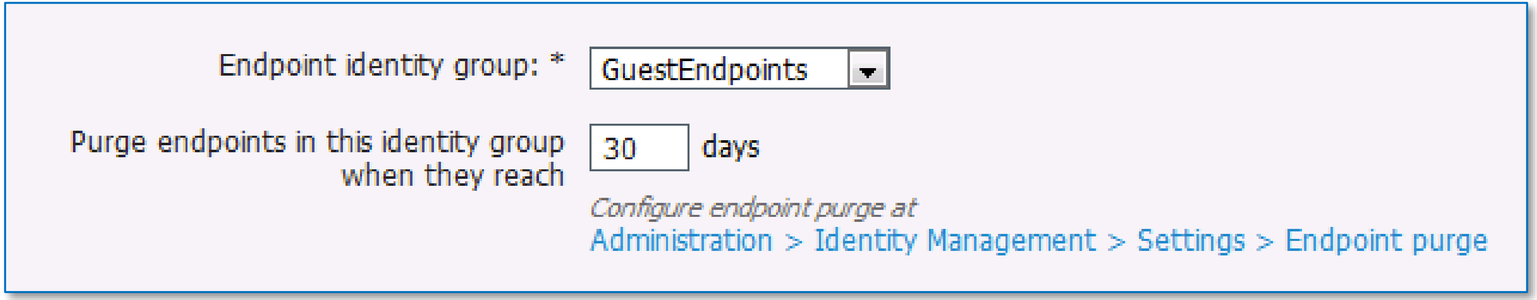
Warning: Watch for expired guest accounts, else high # auth failures !

Note: AUP and Password Change cannot be enforced since guest bypasses portal flow.

Scaling Web Auth

“Remember Me” Guest Flows

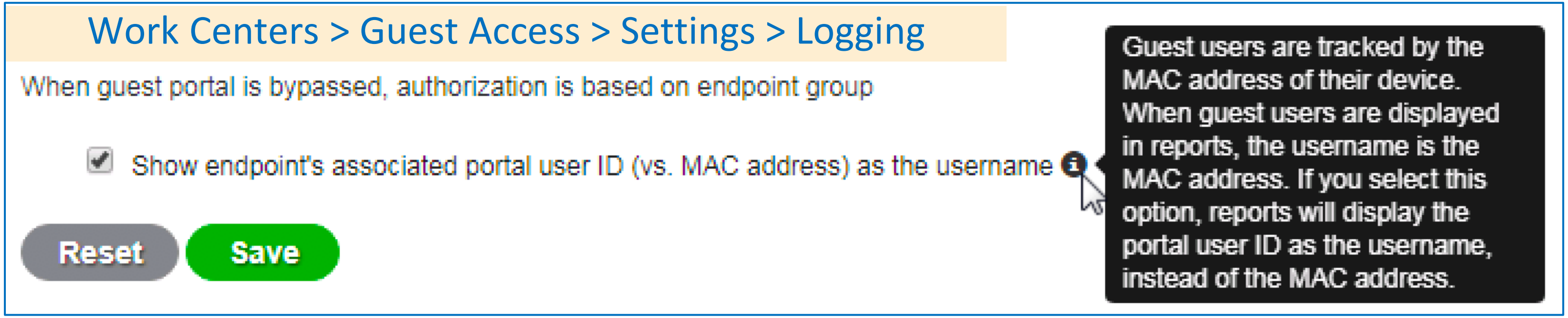
- User logs in to Hotspot/CWA portal and MAC address auto-registered into GuestEndpoint group
- AuthZ Policy for GuestEndpoints ID Group grants access until device purged



Endpoint identity group: * GuestEndpoints ▾

Purge endpoints in this identity group when they reach 30 days

Configure endpoint purge at
Administration > Identity Management > Settings > Endpoint purge



Work Centers > Guest Access > Settings > Logging

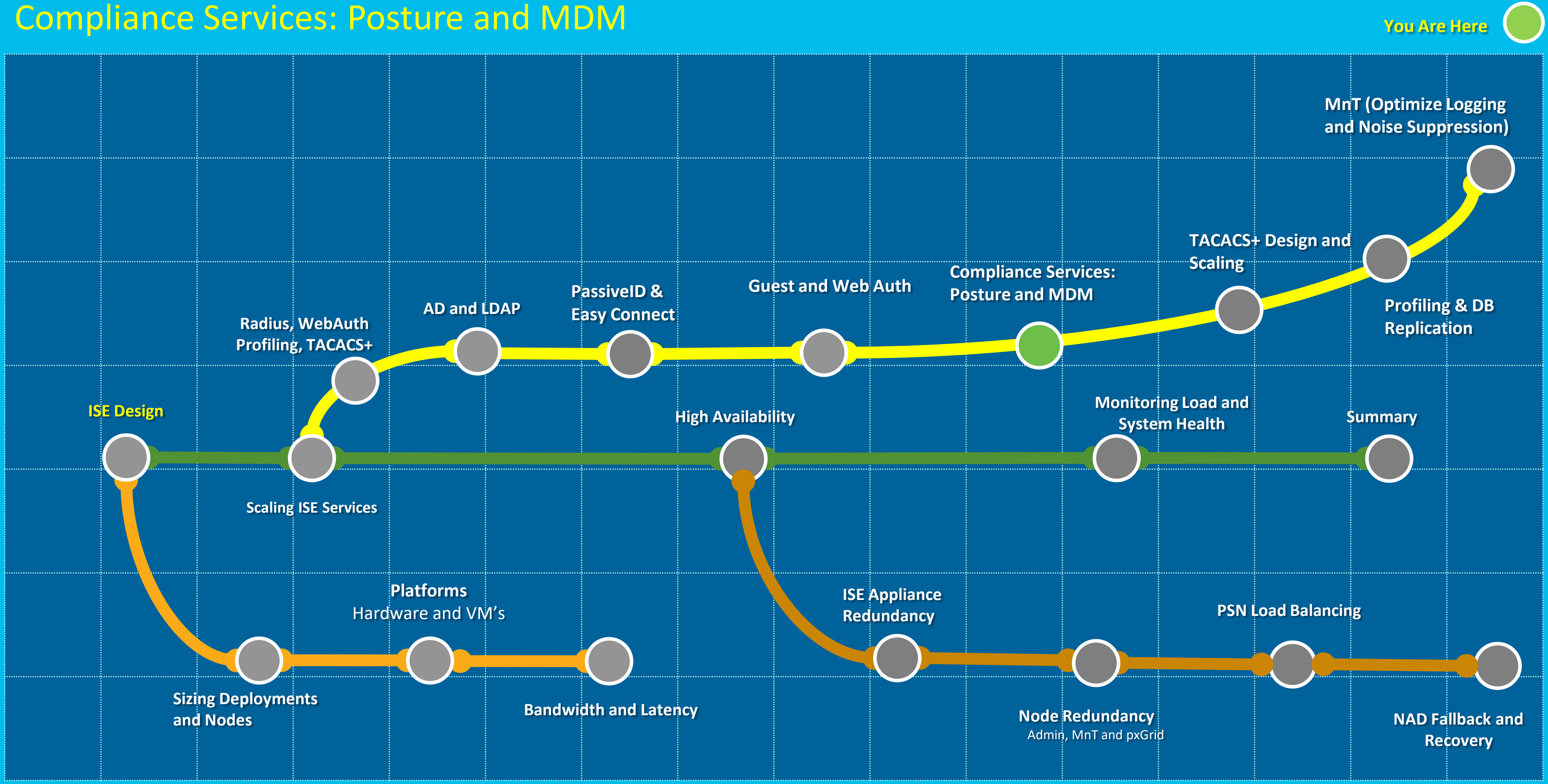
When guest portal is bypassed, authorization is based on endpoint group

☑ Show endpoint's associated portal user ID (vs. MAC address) as the username ℹ

Guest users are tracked by the MAC address of their device. When guest users are displayed in reports, the username is the MAC address. If you select this option, reports will display the portal user ID as the username, instead of the MAC address.

Session Agenda

Compliance Services: Posture and MDM


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

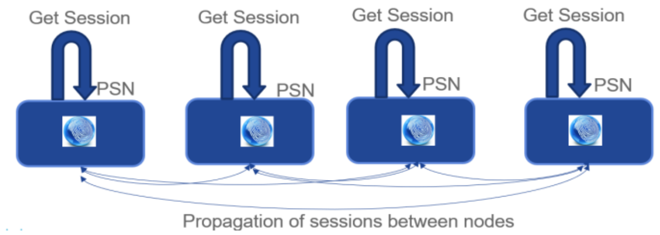
ISE 2.6 introduced ~~LSD~~ LDD

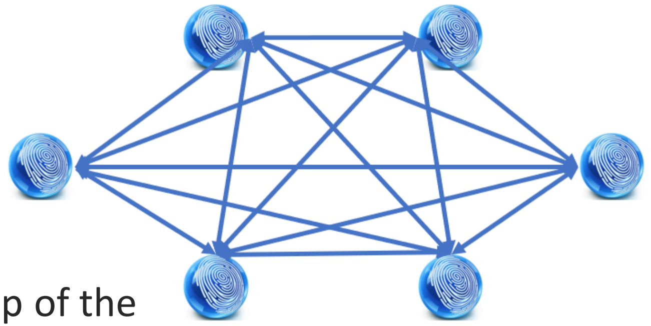
ISE Architecture on LDD

NEW

Session exists in local PSN and MnT node

- Each new session data propagated to all PSNs (in cluster) using Rabbit MQ
- Sessions data cached locally via Redis DB
- Full-Mesh Routing Message Bus
  - No bottlenecks, one hop delivery, truly distributed, persona agnostic

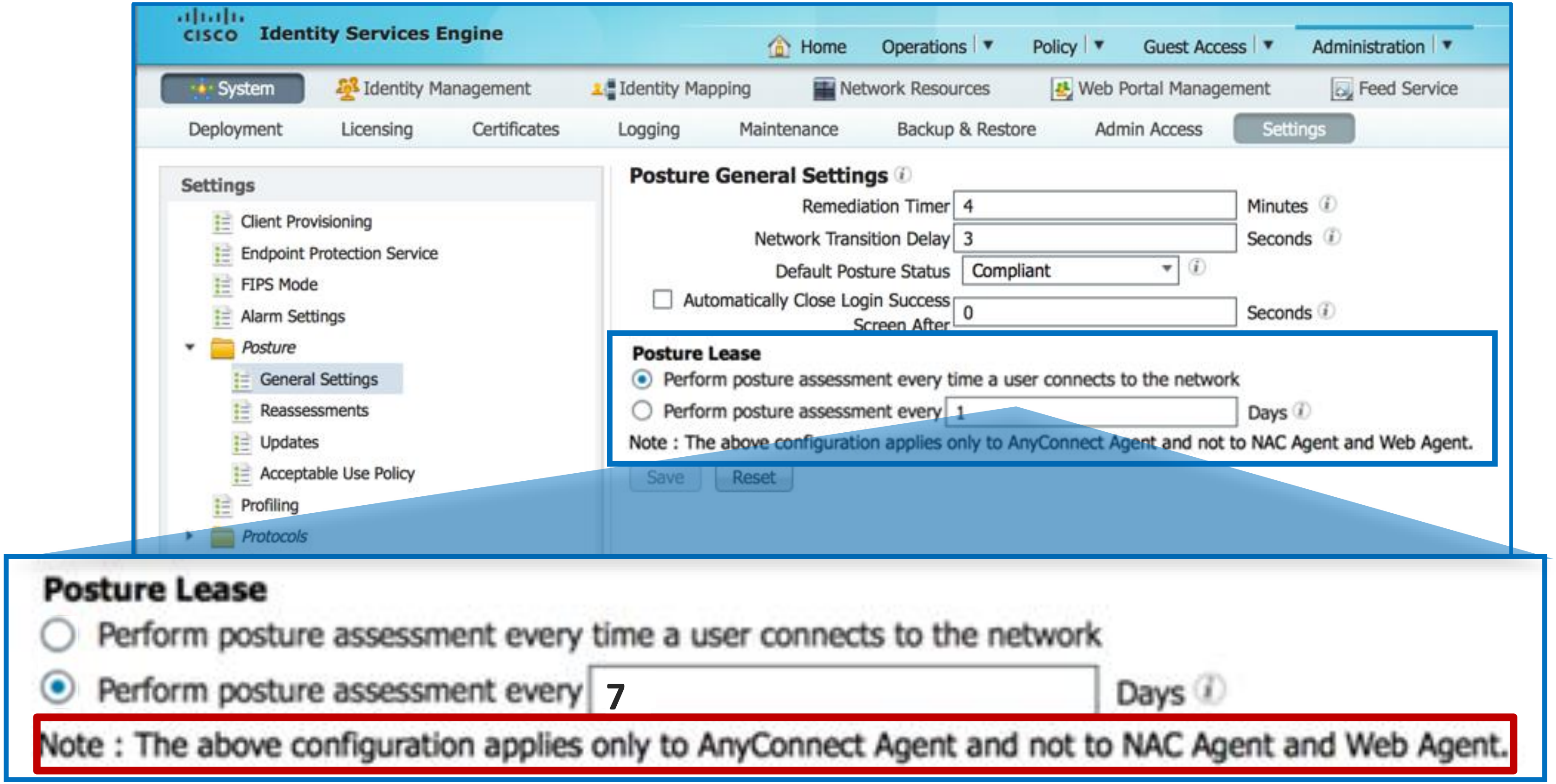




NODE Groups is not same as LDD, LDD just shares the ownership of the endpoint. MAR Cache is shared between node groups

Posture Lease

Once Compliant, user may leave/reconnect multiple times before re-posture



Posture General Settings

Remediation Timer: 4 Minutes

Network Transition Delay: 3 Seconds

Default Posture Status: Compliant

□ Automatically Close Login Success Screen After: 0 Seconds

Posture Lease

● Perform posture assessment every time a user connects to the network

○ Perform posture assessment every 1 Days

Note : The above configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.

Posture Lease

○ Perform posture assessment every time a user connects to the network

● Perform posture assessment every 7 Days

Note : The above configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.

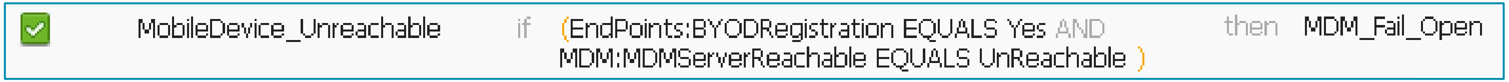
MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

- Scalability ≈ 30 Calls per second per PSN.
  - Cloud-Based deployment typically built for scale and redundancy
    - For cloud-based solutions, Internet bandwidth and latency must be considered.
  - Premise-Based deployment may leverage load balancing

- ISE 1.4+ supports multiple MDM servers – could be same or different vendors.

- Authorization permissions can be set based on MDM connectivity status:
  - **MDM:MDMServerReachable Equals UnReachable**
    MDM:MDMServerReachable Equals Reachable



✓ MobileDevice_Unreachable if (EndPoints:BYODRegistration EQUALS Yes AND MDM:MDMServerReachable EQUALS UnReachable) then MDM_Fail_Open

  - All attributes retrieved & reachability determined by single API call on each new session.

Scaling MDM

ISE 2.4 adds support for managing MDM Attributes via ERS API

Prepopulate MDM Enrollment and/or Compliance via ERS API

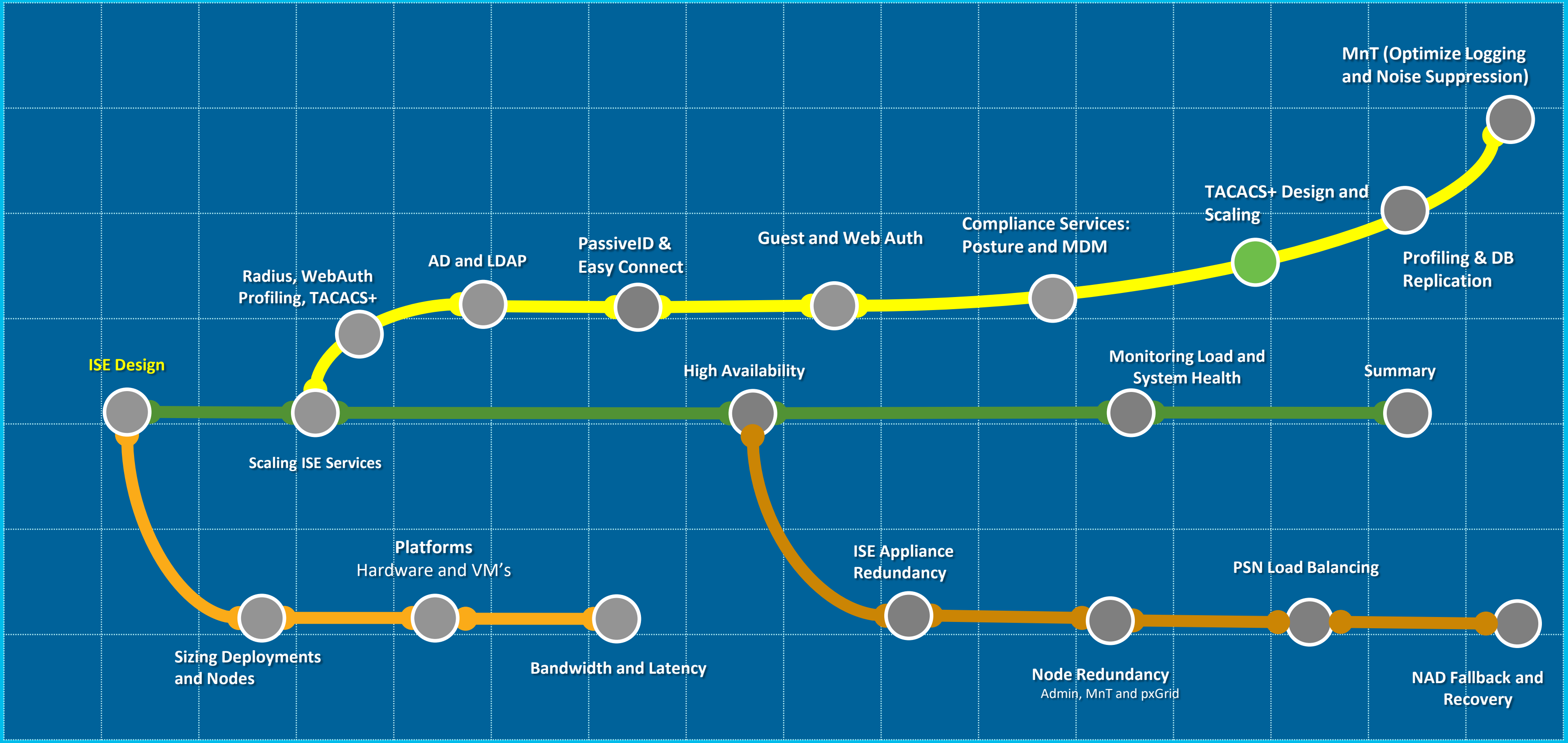
```
<groupId>groupId</groupId>
<identityStore>identityStore</identityStore>
<identityStoreId>identityStoreId</identityStoreId>
<mac>00:01:02:03:04:05</mac>
<mdmComplianceStatus>false</mdmComplianceStatus>
<mdmEncrypted>false</mdmEncrypted>
<mdmEnrolled>true</mdmEnrolled>
<mdmIMEI>IMEI</mdmIMEI>
<mdmJailBroken>false</mdmJailBroken>
<mdmManufacturer>Apple Inc.</mdmManufacturer>
<mdmModel>iPad</mdmModel>
<mdmOS>iOS</mdmOS>
<mdmPhoneNumber>Phone Number</mdmPhoneNumber>
<mdmPinlock>true</mdmPinlock>
<mdmReachable>true</mdmReachable>
<mdmSerial>AB23D0E45BC01</mdmSerial>
<mdmServerName>AirWatch</mdmServerName>
<portalUser>portalUser</portalUser>
<profileId>profileId</profileId>
<staticGroupAssignment>true</staticGroupAssignment>
<staticProfileAssignment>false</staticProfileAssignment>
```

```
<customAttributes>
  <customAttributes>
    <entry>
      <key>MDM_Registered</key>
      <value>true</value>
    </entry>
    <entry>
      <key>MDM_Compliance</key>
      <value>false</value>
    </entry>
    <entry>
      <key>Attribute_XYZ</key>
      <value>Value_XYZ</value>
    </entry>
  </customAttributes>
</customAttributes>
```

Session Agenda

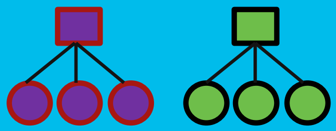
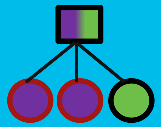
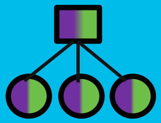
Compliance Services: Posture and MDM

You Are Here ●


MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
Profiling & DB Replication
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Options for Deploying Device Admin

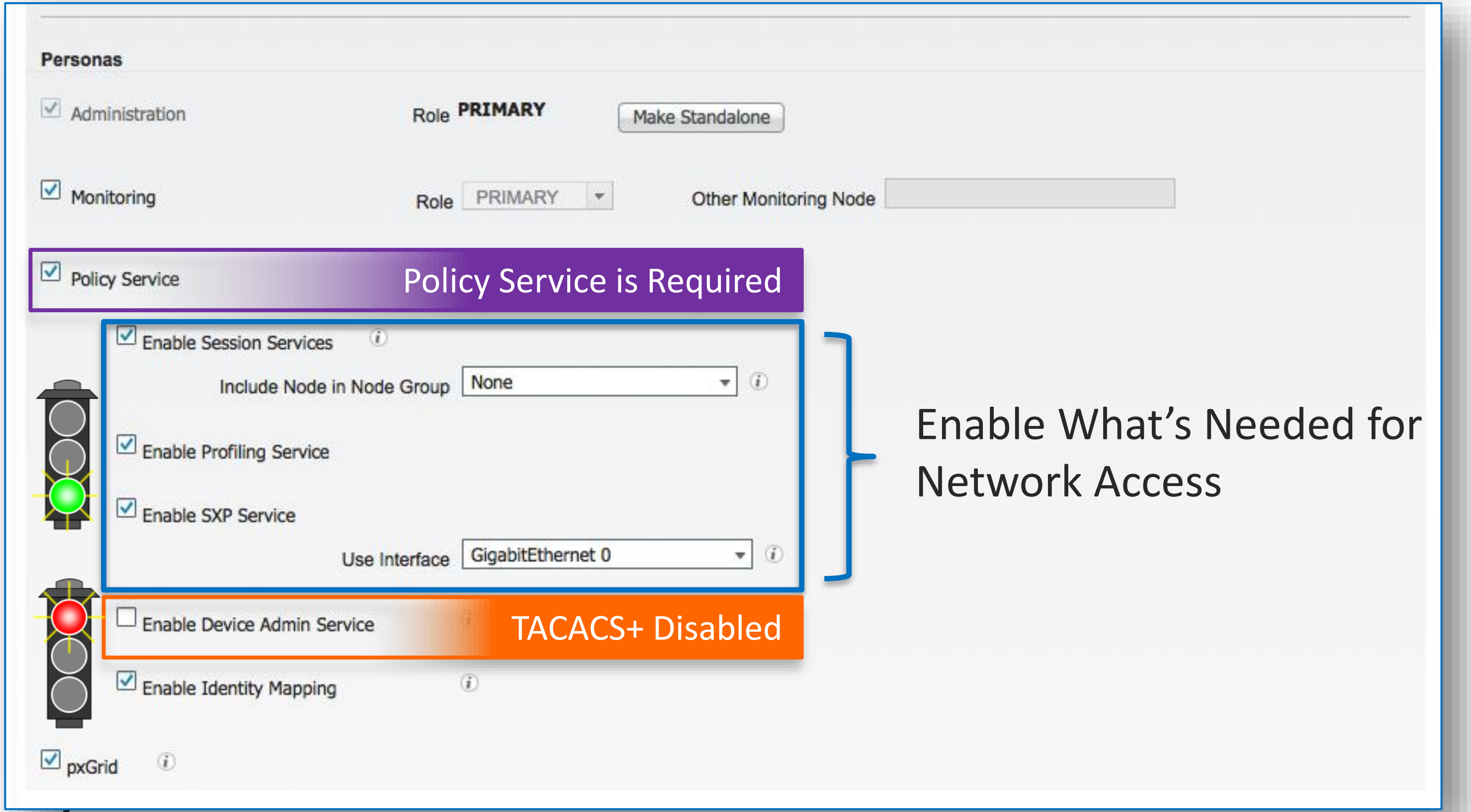
https://community.cisco.com/t5/security-documents/ise-tacacs-deployment-amp-sizing-guidance/ta-p/3612253

Priorities according to Policy and Business Goals		Separate Deployment  RADIUS TACACS	Separate PSNs  RADIUS TACACS	Mixed PSNs  RADIUS/ TACACS
Separation of Configuration/ Duty	Yes: Specialization for TACACS+	🟩	🟥	🟥
	No: Shared resources/Reduced $$	🟥	🟨	🟩
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services	🟩	🟨	🟥
	No: Avoid underutilized PSNs	🟥	🟨	🟩
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+	🟩	🟩	🟥
	No: Focus on "human" device admins	🟥	🟨	🟩
Separation of Logging Store	Yes: Optimize log retention VM	🟩	🟥	🟥
	No: Centralized monitoring	🟥	🟩	🟩

RADIUS Only PSNs

For Your Reference

Administration > System > Deployment > [ISE node]



Personas

☑ Administration Role **PRIMARY** Make Standalone

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

Policy Service is Required

☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

☑ Enable SXP Service

Use Interface: GigabitEthernet 0

□ Enable Device Admin Service

TACACS+ Disabled

☑ Enable Identity Mapping

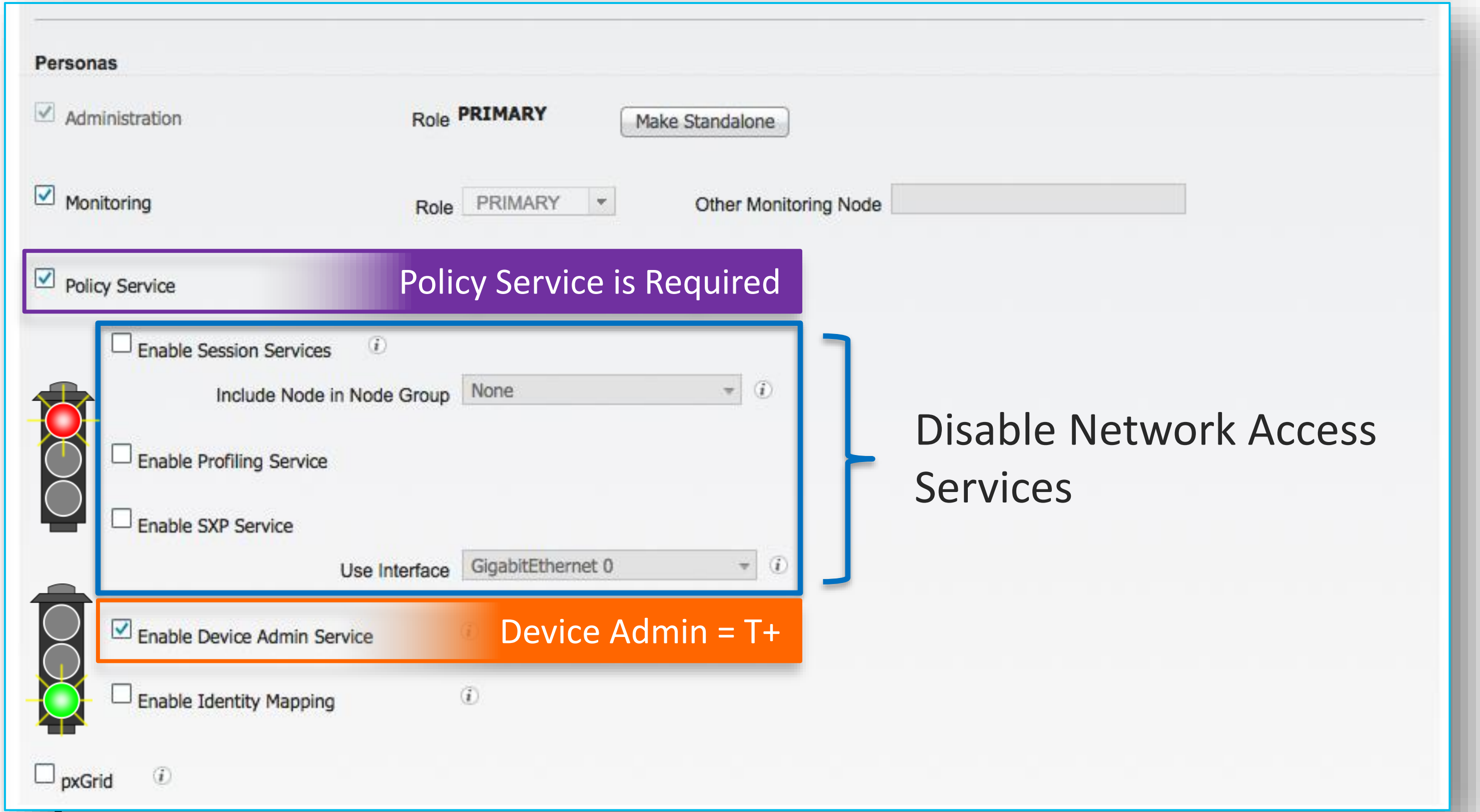
☑ pxGrid

Enable What’s Needed for Network Access

TACACS+ Only PSNs

For Your Reference

Administration > System > Deployment > [ISE node]



Personas

☑ Administration Role **PRIMARY** Make Standalone

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

Policy Service is Required

□ Enable Session Services

Include Node in Node Group None

□ Enable Profiling Service

□ Enable SXP Service

Use Interface GigabitEthernet 0

☑ Enable Device Admin Service

Device Admin = T+

□ Enable Identity Mapping

□ pxGrid

Disable Network Access Services

ISE 2.7 TACACS+ Multi-Service Scaling (RADIUS and T+)

Max Concurrent RADIUS + TACACS+ TPS by Deployment Model and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Standa-alone	All personas on same node	3615	0	10,000	100
		3655	0	25.000	100
		3695	0	50,000	100
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3655 as PAN+MNT	* 5 / 3+2	25,000	250 / 3,000
		3695 as PAN+MNT	* 5 / 3+2	50,000	250 / 3,000
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	* 50 / 47+3	500,000	2,500 / 6,000
		3595 as PAN and MNT	* 50 / 47+3	500,000 (2M)	2,500 / 6,000

* Device Admin service enabled on same PSNs also used for RADIUS OR Split RADIUS and T+ PSNs

Each dedicated T+ PSN node reduces dedicated RADIUS PSN count by 1

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3615		10,000	2,000
	SNS-3655		50,000	3,000
	SNS-3695		100,000	3,000

ISE 2.7 TACACS+ Multi-Service Scaling (TACACS+ Only)

Max Concurrent TACACS+ TPS by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Stand-alone	All personas on same node	3615	0	N/A	1,000
		3655/3695	0	N/A	1,500
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT	* 5 / 2	N/A	** 2,000 / 2,000
		3655/3695 as PAN+MNT	* 5 / 2	N/A	** 3,000 / 3,000
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	* 50 / 4	N/A	** 5,000 / 5,000
		3695 as PAN and MnT	* 50 / 5	N/A	** 10,000 / 10,000

* Device Admin service can be enabled on each PSN; minimally 2 for redundancy.

** Max log capacity for MNT

- By PSN

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3615		10,000	2,000
	SNS-3655/3695		50,000/100,000	3,000

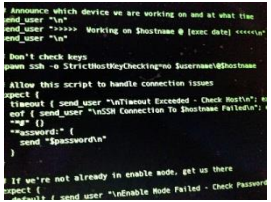
TACACS+ MnT Scaling

Human Versus Automated Device Administration

- Consider the “average” size syslog from TACACS+ based on following guidance:

Each TACACS+ Session	Each Command Authorization (per session)
Authentication: 2kB	Command authorization: 2kB
Session authorization: 2kB	Command accounting : 1kB
Session accounting: 1kB	

- “Human” Device Admin Example:
  - For a normal “human” session we may expect to see 10 commands, so a session would be approximately: [5kB + (10 * 3kB)) = 35kB. Suppose a maximum of 50 such sessions per admin per day from 50 admins (and few organizations have > 50 admins)
    - 50 human admins would generate < 1 TPS average, ~60k logs/day, or ~90MB/day.
- Automated/Script Device Admin Example:
  - Consider a script that runs 4 times a day against 30,000 devices, (for example, to backup config on all devices). Generally the interaction will be short, say 5 commands:
    - Storage = 30,000 * 4 * [5kB + (5 * 3kB)] = ~2.4 GB/day
    - Total TPS = 30k * 4 * [3 + (5 * 2)] = 1.56M logs = 18 TPS average; 1300 TPS peak.



```
 Announce which device we are working on and at what time
end_user "\n"
end_user ">>>>>  Working on $hostname @ [exec date] <<<<<\n"
end_user "\n"

 Don't check keys
pawn ssh -o StrictHostKeyChecking=no $username\@$hostname

 Allow this script to handle connection issues
xpect {
 timeout { send_user "\nTimeout Exceeded - Check Host\n"; e
 eof { send_user "\nSSH Connection To $hostname Failed\n"; 
 "*#" {}
 "*assword:" {
   send "$password\n"
 }

 If we're not already in enable mode, get us there
xpect {
 default { send user "\nEnable Mode Failed - Check Passwor
```

TACACS+ Multi-Service Scaling

For Your Reference

Required TACACS+ TPS by # Admins and # NADs

		Session Authentication and Accounting Only				Command Accounting Only (10 Commands / Session)				Command Authorization + Acctg (10 Commands / Session)			
		Avg TPS	Peak TPS	Logs/Day	Storage/ day	Avg TPS	Peak TPS	Logs/Day	Storage/ day	Avg TPS	Peak TPS	Logs/Day	Storage/ day
Human Admin	# Admins					Based on 50 Admin Sessions per Day							
	1	< 1	< 1	150	< 1MB	< 1	< 1	650	1MB	< 1	<1	1.2k	2MB
	5	< 1	< 1	750	1MB	< 1	< 1	3.3k	4MB	< 1	<1	5.8k	9MB
	10	< 1	< 1	1.5k	3MB	< 1	< 1	6.5k	8MB	< 1	1	11.5k	17MB
	25	< 1	< 1	3.8k	7MB	< 1	1	16.3k	19MB	< 1	2	28.8k	43MB
	50	< 1	1	7.5k	13MB	< 1	2	32.5k	37MB	1	4	57.5k	86MB
	100	< 1	1	15k	25MB	1	4	65k	73MB	2	8	115k	171MB
Script Admin	# NADs					Based on 4 Scripted Sessions per Day							
	500	< 1	5	6k	10MB	< 1	22	26k	30MB	1	38	46k	70MB
	1,000	< 1	10	12k	20MB	1	43	52k	60MB	1	77	92k	140MB
	5,000	< 1	50	60k	100MB	3	217	260k	300MB	5	383	460k	700MB
	10,000	1	100	120k	200MB	6	433	520k	600MB	11	767	920k	1.4GB
	20,000	3	200	240k	400MB	12	867	1.04M	1.2GB	21	1.5k	1.84M	2.7GB
	30,000	5	300	480k	600MB	18	1.3k	1.56M	1.7GB	32	2.3k	2.76M	4.0GB
	50,000	7	500	600k	1GB	30	2.2k	2.6M	2.9GB	53	3.8k	4.6M	6.7GB

Peak values based on 5-minute burst to complete each batch request.

TACACS+ Multi-Service Scaling

For Your Reference

Required TACACS+ TPS by # Admins and # NADs

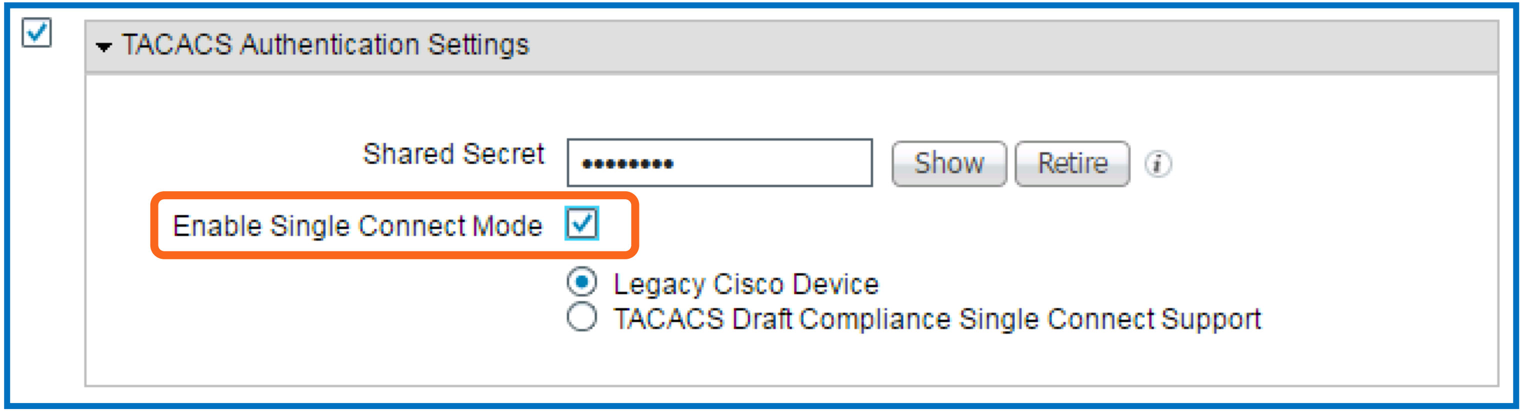
		Session Authentication and Accounting Only				Command Accounting Only (10 Commands / Session)				Command Authorization + Acctg (10 Commands / Session)			
		Avg TPS	Peak TPS	Logs/Day	Storage/ day	Avg TPS	Peak TPS	Logs/Day	Storage/ day	Avg TPS	Peak TPS	Logs/Day	Storage/ day
Human Admin	# Admins					Based on 50 Admin Sessions per Day							
	1	< 1	< 1	150	< 1MB	< 1	< 1	650	1MB	< 1	<1	1.2k	2MB
	5	< 1	< 1	750	1MB	< 1	< 1	3.3k	4MB	< 1	<1	5.8k	9MB
	10	< 1	< 1	1.5k	3MB	< 1	< 1	6.5k	8MB	< 1	1	11.5k	17MB
	25	< 1	< 1	3.8k	7MB	< 1	1	16.3k	19MB	< 1	2	28.8k	43MB
	50	< 1	1	7.5k	13MB	< 1	2	32.5k	37MB	1	4	57.5k	86MB
	100	< 1	1	15k	25MB	1	4	65k	73MB	2	8	115k	171MB
Script Admin	# NADs					Based on 4 Scripted Sessions per Day							
	500	< 1	5	6k	10MB	< 1	22	26k	30MB	1	38	46k	70MB
	1,000	< 1	10	12k	20MB	1	43	52k	60MB	1	77	92k	140MB
	5,000	< 1	50	60k	100MB	3	217	260k	300MB	5	383	460k	700MB
	10,000	1	100	120k	200MB	6	433	520k	600MB	11	767	920k	1.4GB
	20,000	3	200	240k	400MB	12	867	1.04M	1.2GB	21	1.5k	1.84M	2.7GB
	30,000	5	300	480k	600MB	18	1.3k	1.56M	1.7GB	32	2.3k	2.76M	4.0GB
	50,000	7	500	600k	1GB	30	2.2k	2.6M	2.9GB	53	3.8k	4.6M	6.7GB

Peak values based on 5-minute burst to complete each batch request.

Single Connect Mode

Scaling TACACS+ for High-Volume NADs

- Multiplexes T+ requests over single TCP connection
  - All T+ requests between NAD and ISE occur over single connection rather than separate connections for each request.
- Recommended for TACACS+ “Top Talkers”
- Note: TCP sockets locked to NADs, so limit use to NADs with highest activity.



☑ ▾ TACACS Authentication Settings

Shared Secret: •••••••••

Enable Single Connect Mode ☑

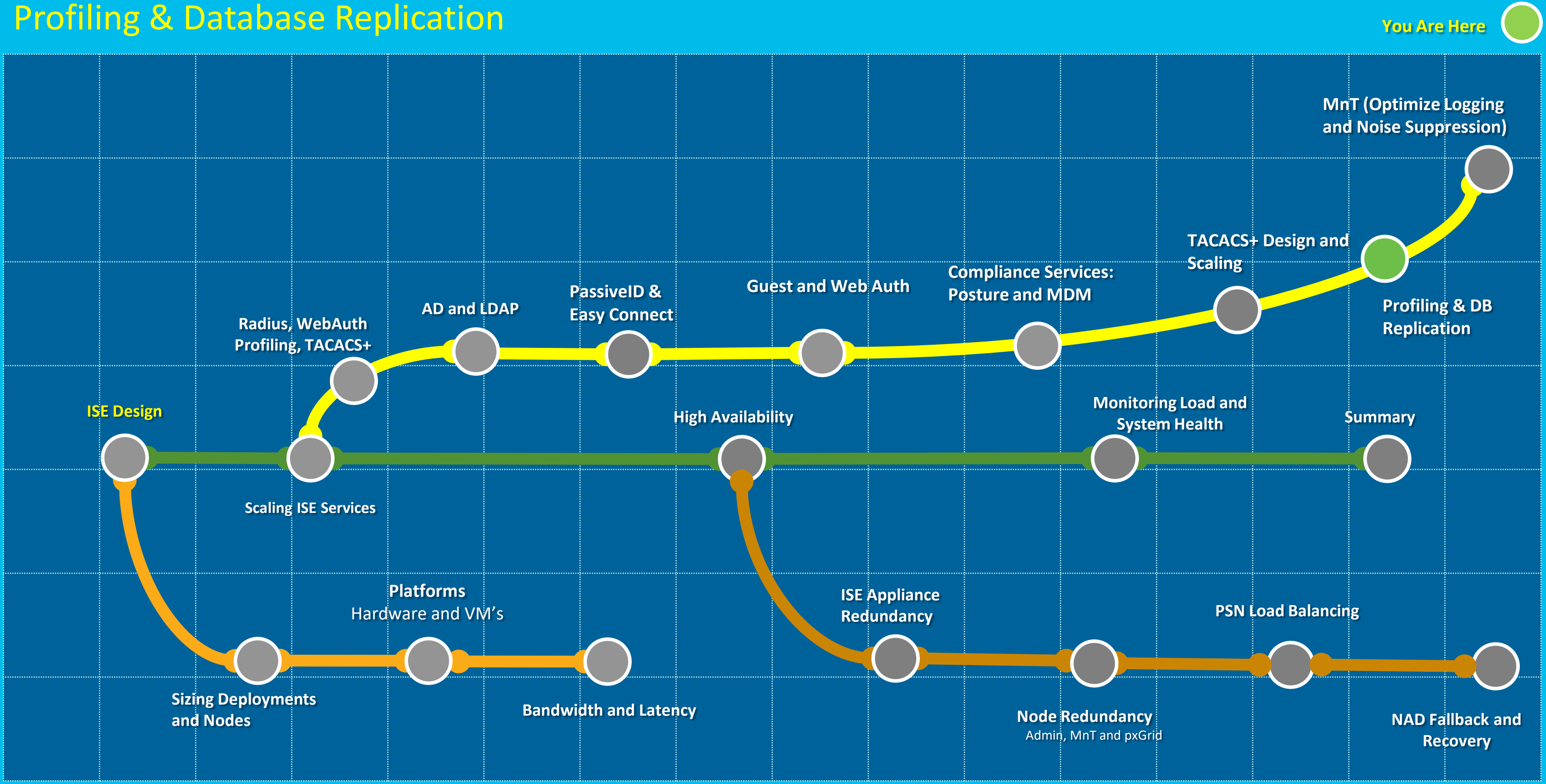
● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

Administration > Network Resources > Network Devices > (NAD)

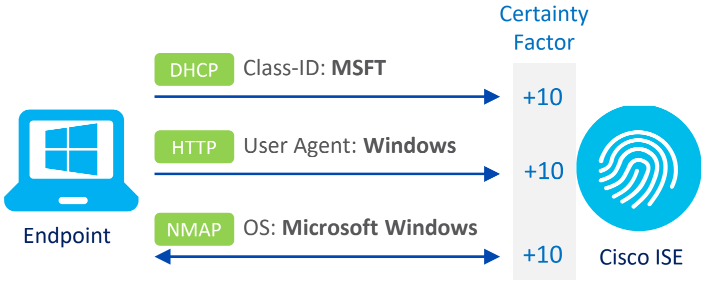
Session Agenda

Profiling & Database Replication


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

ISE profiles based on ‘profiling policies’

The minimum ‘certainty metric’ in the profiling policy evaluates the matching profile for an endpoint.

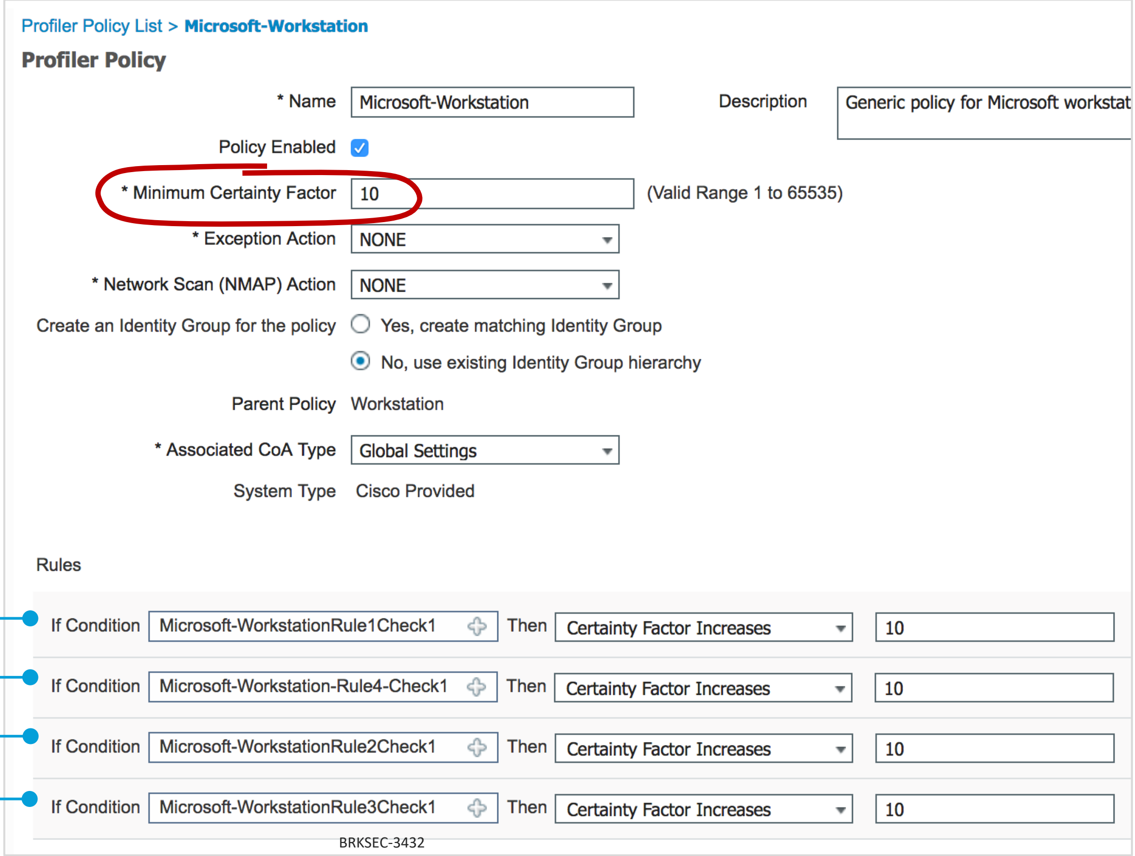


DHCP:dhcp-class-identifier CONTAINS MSFT

DHCP:dhcp-class-identifier CONTAINS MS-UC-Client

IP:User-Agent CONTAINS Windows

NMAP:operating-system CONTAINS Microsoft Windows



Profiler Policy List > **Microsoft-Workstation**

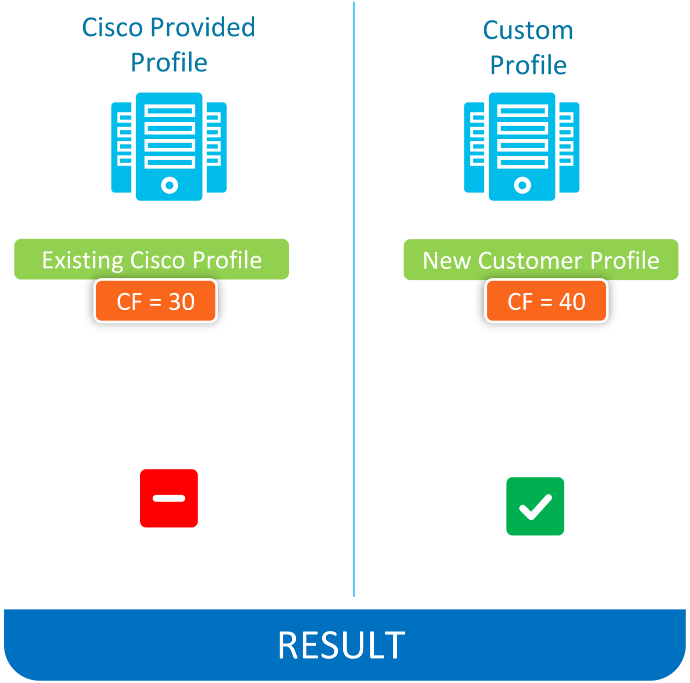
Profiler Policy

* Name	Microsoft-Workstation	Description	Generic policy for Microsoft workstat
Policy Enabled	☑		
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	NONE		
Create an Identity Group for the policy	○ Yes, create matching Identity Group ● No, use existing Identity Group hierarchy		
Parent Policy	Workstation		
* Associated CoA Type	Global Settings		
System Type	Cisco Provided		

Rules

If Condition	Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-Workstation-Rule4-Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule3Check1	Then	Certainty Factor Increases	10

Profiles Precedence



Cisco Provided Profile

Existing Cisco Profile

CF = 30

−

Custom Profile

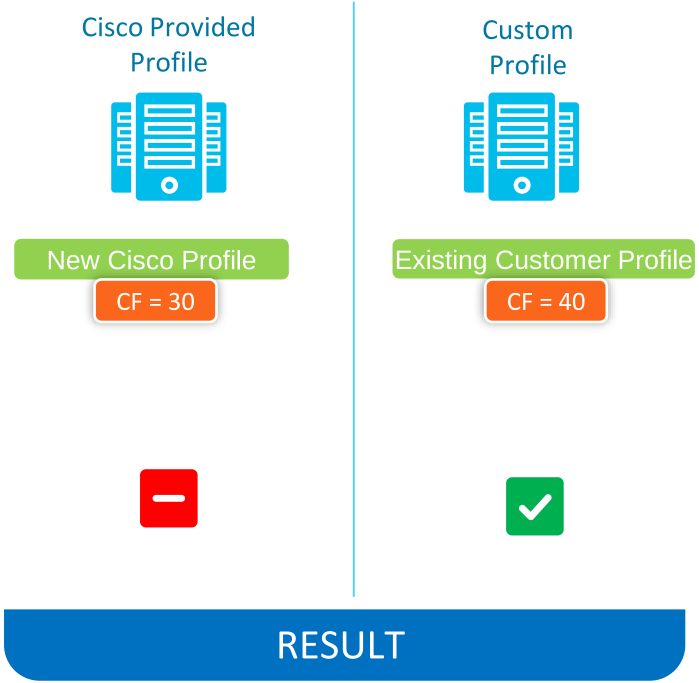
New Customer Profile

CF = 40

✓

RESULT

Profiles Precedence



Cisco Provided Profile

New Cisco Profile

CF = 30

🟥

Custom Profile

Existing Customer Profile

CF = 40

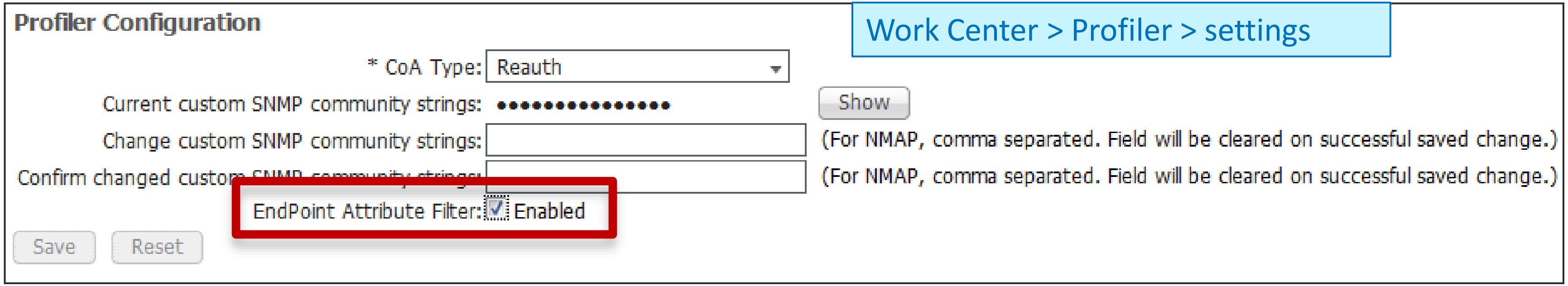
✓

RESULT

Endpoint Attribute Filter and Whitelist Attributes

Reduces Data Collection and Replication to Subset of Profile-Specific Attributes

- Endpoint Attribute Filter – aka “Whitelist filter”
  - Enabled by defauly, only these attributes are collected or replicated.



Work Center > Profiler > settings

Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ●●●●●●●●●●●●●●● Show

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

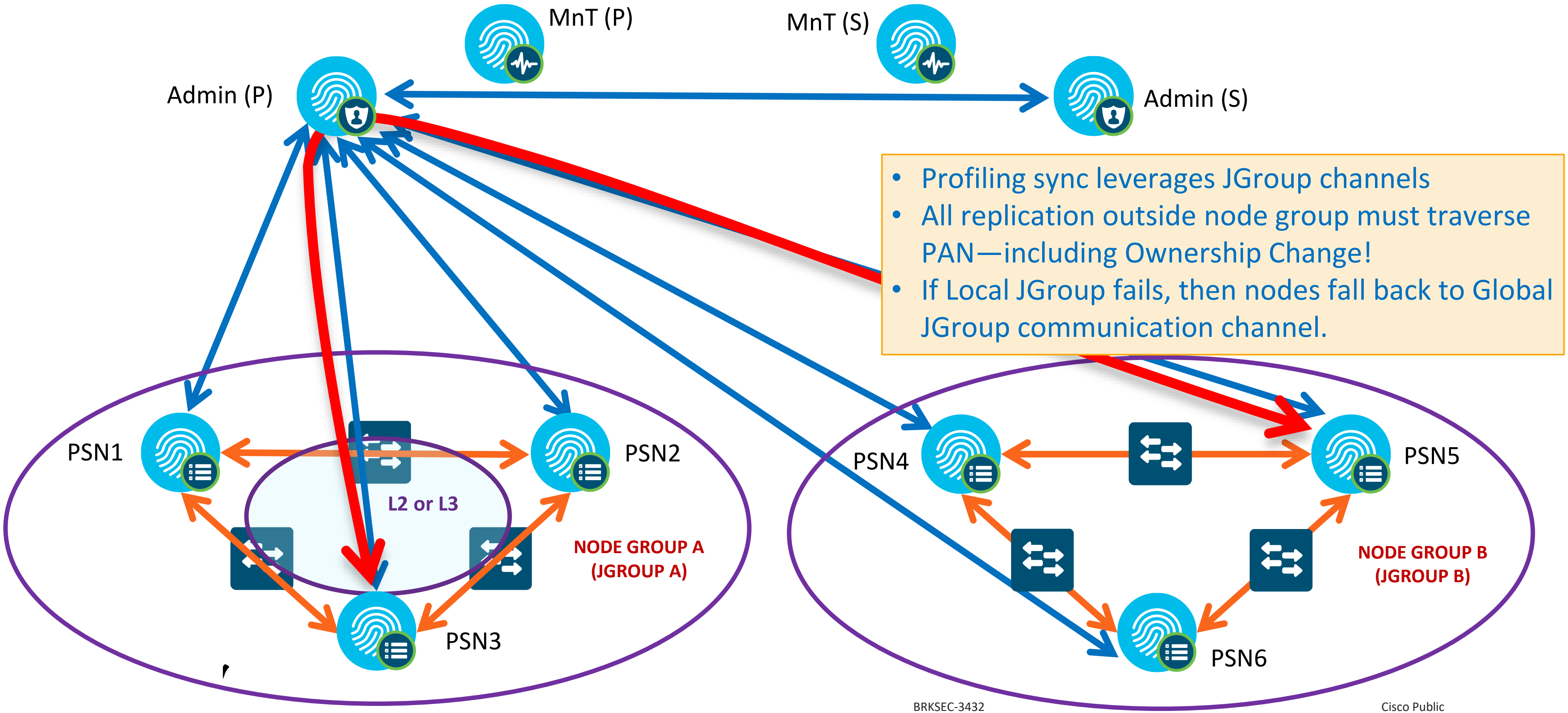
EndPoint Attribute Filter: ☑ Enabled

Save Reset

- Whitelist Filter limits profile attribute collection to those required to support default (Cisco-provided) profiles and critical RADIUS operations.
  - Filter must be disabled to collect and/or replicate other attributes.
  - Attributes used in custom conditions are automatically added to whitelist.

Inter-Node Communications pre 2.7

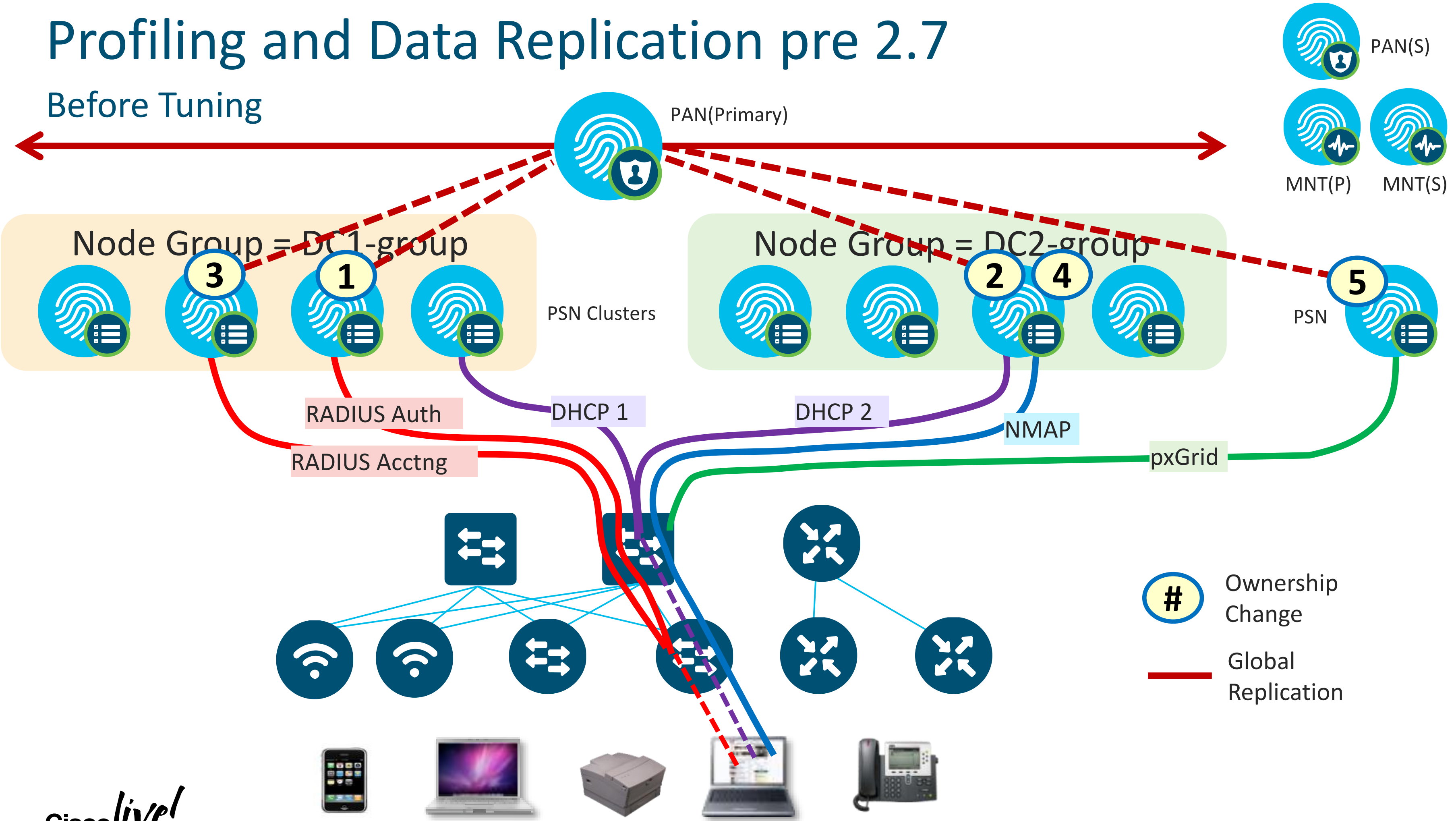
Local JGroups and Node Groups



- Profiling sync leverages JGroup channels
- All replication outside node group must traverse PAN—including Ownership Change!
- If Local JGroup fails, then nodes fall back to Global JGroup communication channel.

Profiling and Data Replication pre 2.7

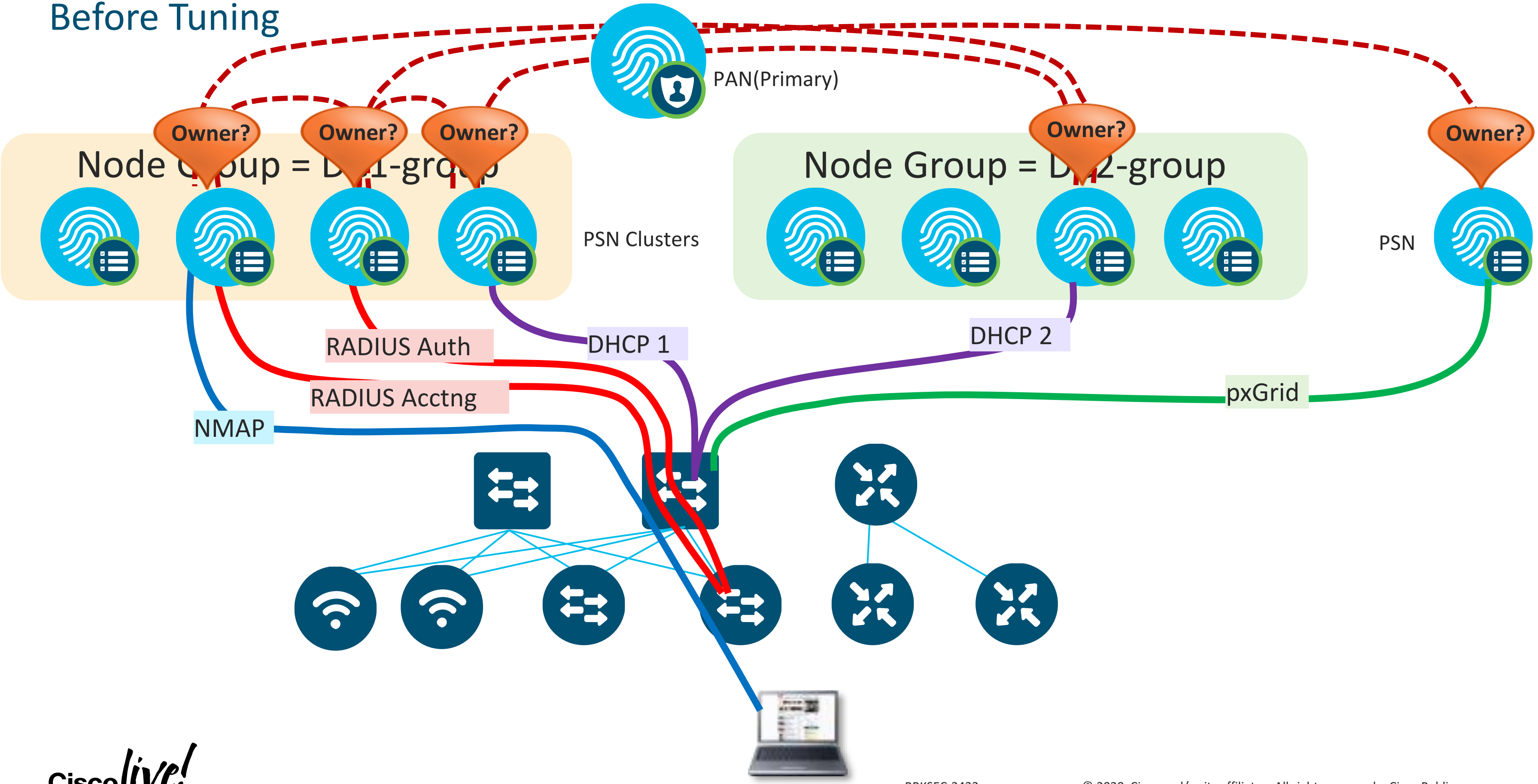
Before Tuning



Cisco live!

Impact of Ownership Changes pre 2.7

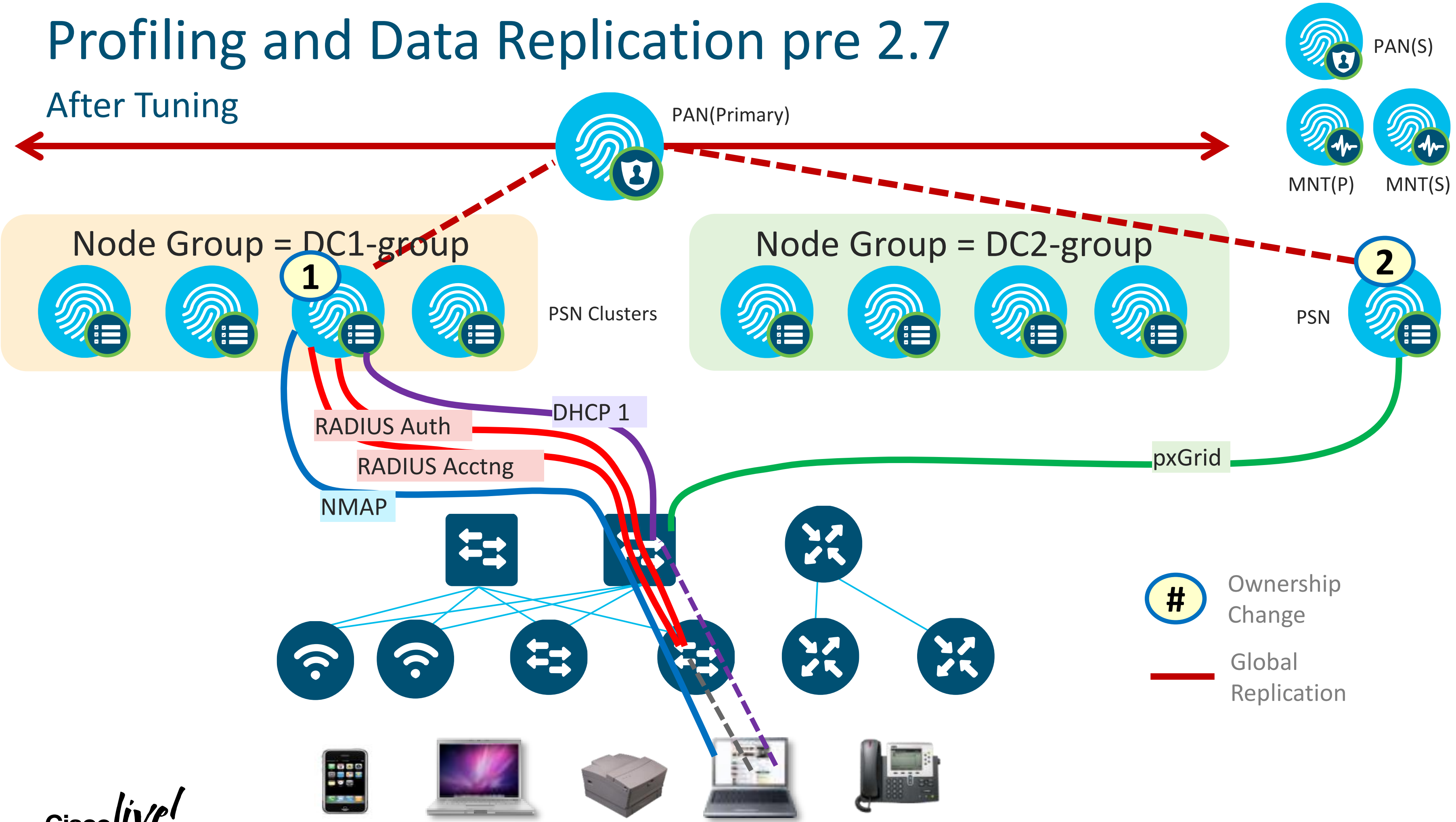
Before Tuning



Cisco live!

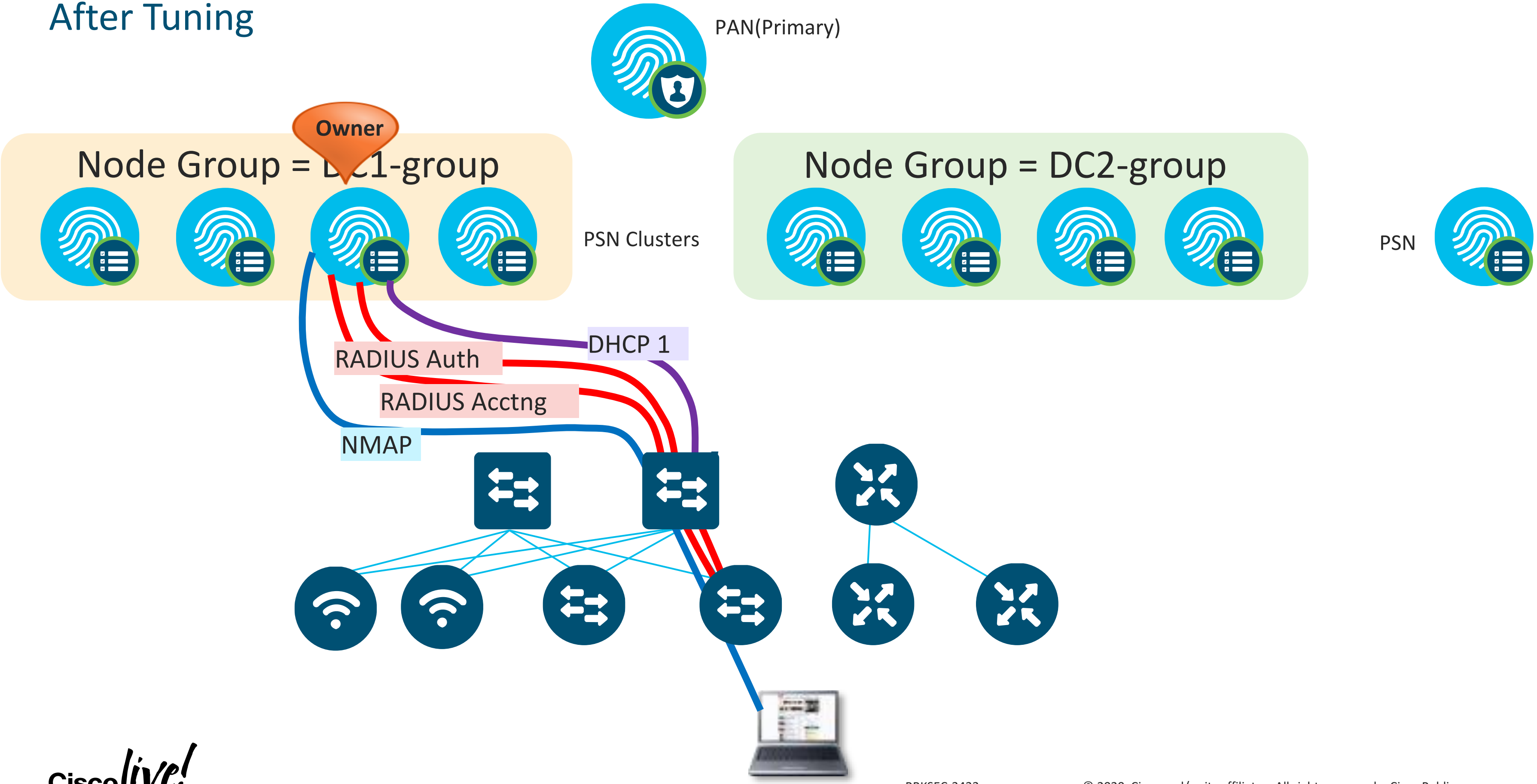
Profiling and Data Replication pre 2.7

After Tuning



Impact of Ownership Changes pre 2.7

After Tuning



Reliable Profiling Services
End Point Ownership Changes 2.7

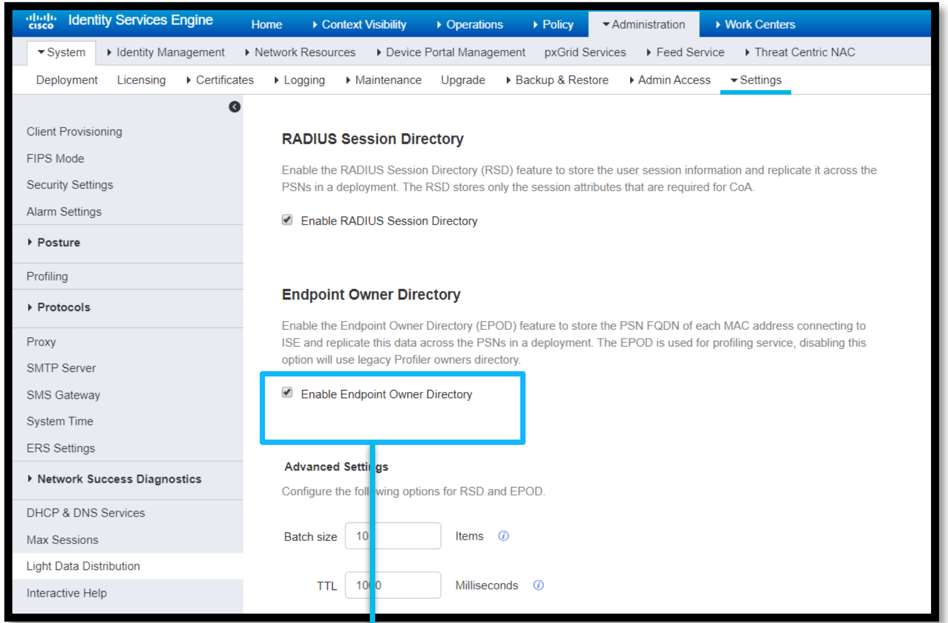
	Endpoint Ownership	Static Endpoints	Feed Download
Before	Multiple PSNs that received probe response would compete for endpoint ownerhsip leading to issues with CoA.	Endpoints classified statically would get reclassified if profiling probes are received.	Can’t get only OUI updates via profiler feed download. Full package would disrupt custom profiling policies.
After	PSNs wont flap ownership of endpoints, except for new authentication.	Endpoints classified statically wont be reclassified unless the static mapping is removed.	New OUI only package available for download and update of existing policies

With EPO/LDD feature enabled, endpoint ownership will not change frequently.

Ownership changes only in the below scenarios :

- **When there is a successful auth for an endpoint or when the node is down**
- **When we import endpoints or create in GUI and later endpoint is read by another probe (DHCP).**

Enable Endpoint Ownership – 2.7



RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

☑ Enable RADIUS Session Directory

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

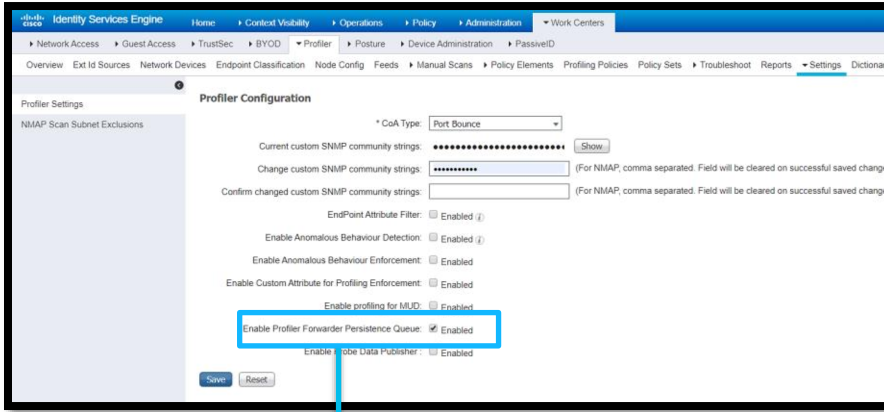
Advanced Settings

Configure the following options for RSD and EPOD.

Batch size: 10 Items

TTL: 1000 Milliseconds

Enabled by default



Profiler Configuration

* CoA Type: Port Bounce

Current custom SNMP community strings: ••••••••••••••••••••••••

Change custom SNMP community strings: •••••••••••• (For NMAP, comma separated. Field will be cleared on successful saved chang

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved chang

EndPoint Attribute Filter: □ Enabled

Enable Anomalous Behaviour Detection: □ Enabled

Enable Anomalous Behaviour Enforcement: □ Enabled

Enable Custom Attribute for Profiling Enforcement: □ Enabled

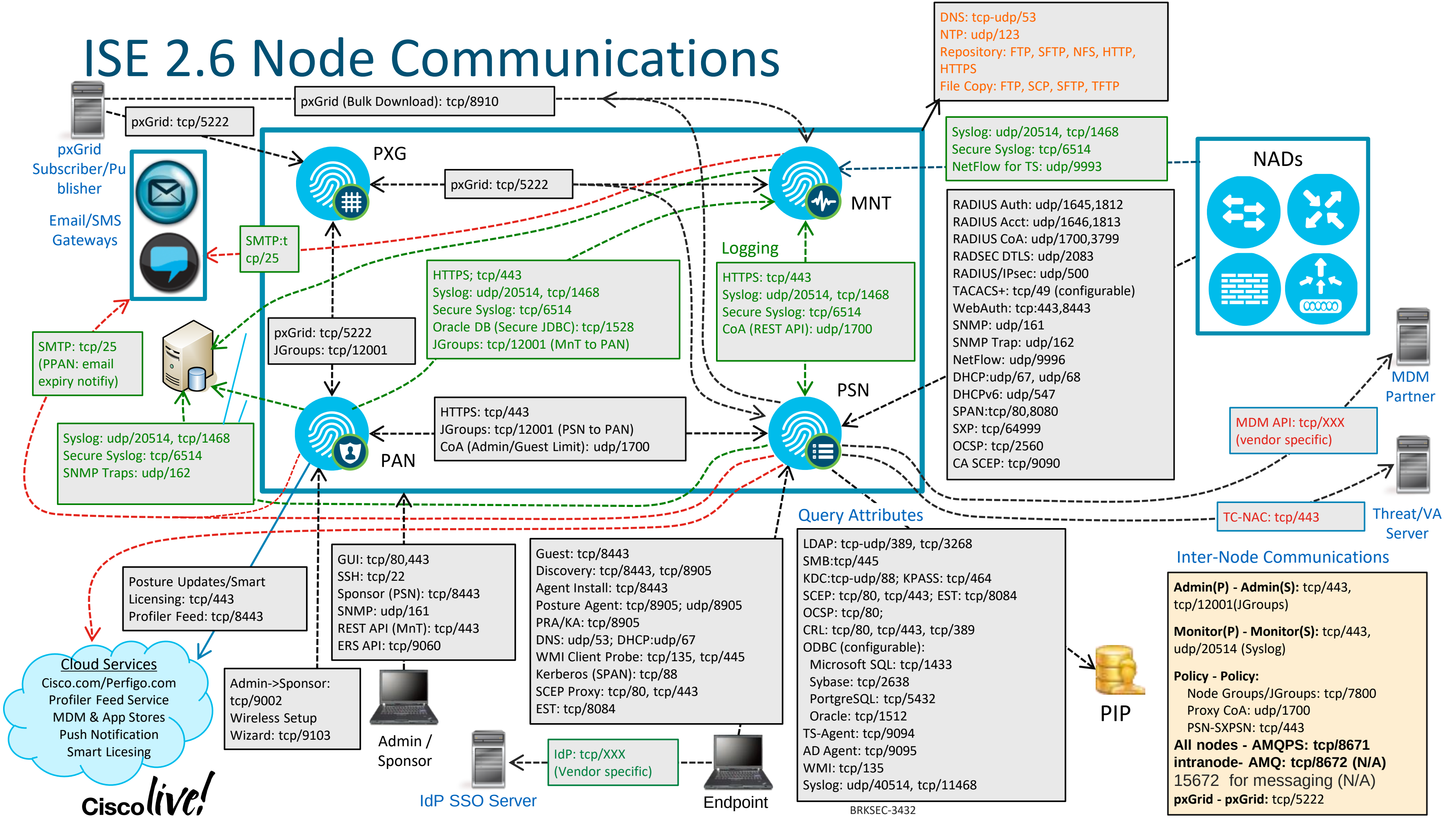
Enable profiling for MUD: □ Enabled

Enable Profiler Forwarder Persistence Queue: ☑ Enabled

Enable Probe Data Publisher : □ Enabled

RMQ enabling page

ISE 2.6 Node Communications



DNS: tcp-udp/53
NTP: udp/123
Repository: FTP, SFTP, NFS, HTTP, HTTPS
File Copy: FTP, SCP, SFTP, TFTP

pxGrid (Bulk Download): tcp/8910

pxGrid: tcp/5222

pxGrid: tcp/5222

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
NetFlow for TS: udp/9993

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813
RADIUS CoA: udp/1700,3799
RADSEC DTLS: udp/2083
RADIUS/IPsec: udp/500
TACACS+: tcp/49 (configurable)
WebAuth: tcp:443,8443
SNMP: udp/161
SNMP Trap: udp/162
NetFlow: udp/9996
DHCP:udp/67, udp/68
DHCPv6: udp/547
SPAN:tcp/80,8080
SXP: tcp/64999
OCSP: tcp/2560
CA SCEP: tcp/9090

SMTP:tcp/25

SMTP: tcp/25
(PPAN: email expiry notifiy)

HTTPS; tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
Oracle DB (Secure JDBC): tcp/1528
JGroups: tcp/12001 (MnT to PAN)

HTTPS: tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
CoA (REST API): udp/1700

pxGrid: tcp/5222
JGroups: tcp/12001

HTTPS: tcp/443
JGroups: tcp/12001 (PSN to PAN)
CoA (Admin/Guest Limit): udp/1700

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
SNMP Traps: udp/162

MDM API: tcp/XXX
(vendor specific)

TC-NAC: tcp/443

Posture Updates/Smart Licensing: tcp/443
Profiler Feed: tcp/8443

GUI: tcp/80,443
SSH: tcp/22
Sponsor (PSN): tcp/8443
SNMP: udp/161
REST API (MnT): tcp/443
ERS API: tcp/9060

Guest: tcp/8443
Discovery: tcp/8443, tcp/8905
Agent Install: tcp/8443
Posture Agent: tcp/8905; udp/8905
PRA/KA: tcp/8905
DNS: udp/53; DHCP:udp/67
WMI Client Probe: tcp/135, tcp/445
Kerberos (SPAN): tcp/88
SCEP Proxy: tcp/80, tcp/443
EST: tcp/8084

LDAP: tcp-udp/389, tcp/3268
SMB:tcp/445
KDC:tcp-udp/88; KPASS: tcp/464
SCEP: tcp/80, tcp/443; EST: tcp/8084
OCSP: tcp/80;
CRL: tcp/80, tcp/443, tcp/389
ODBC (configurable):
  Microsoft SQL: tcp/1433
  Sybase: tcp/2638
  PortgreSQL: tcp/5432
  Oracle: tcp/1512
TS-Agent: tcp/9094
AD Agent: tcp/9095
WMI: tcp/135
Syslog: udp/40514, tcp/11468

Cloud Services
Cisco.com/Perfigo.com
Profiler Feed Service
MDM & App Stores
Push Notification
Smart Licesing

Admin->Sponsor: tcp/9002
Wireless Setup Wizard: tcp/9103

IdP: tcp/XXX
(Vendor specific)

Inter-Node Communications

Admin(P) - Admin(S): tcp/443, tcp/12001(JGroups)

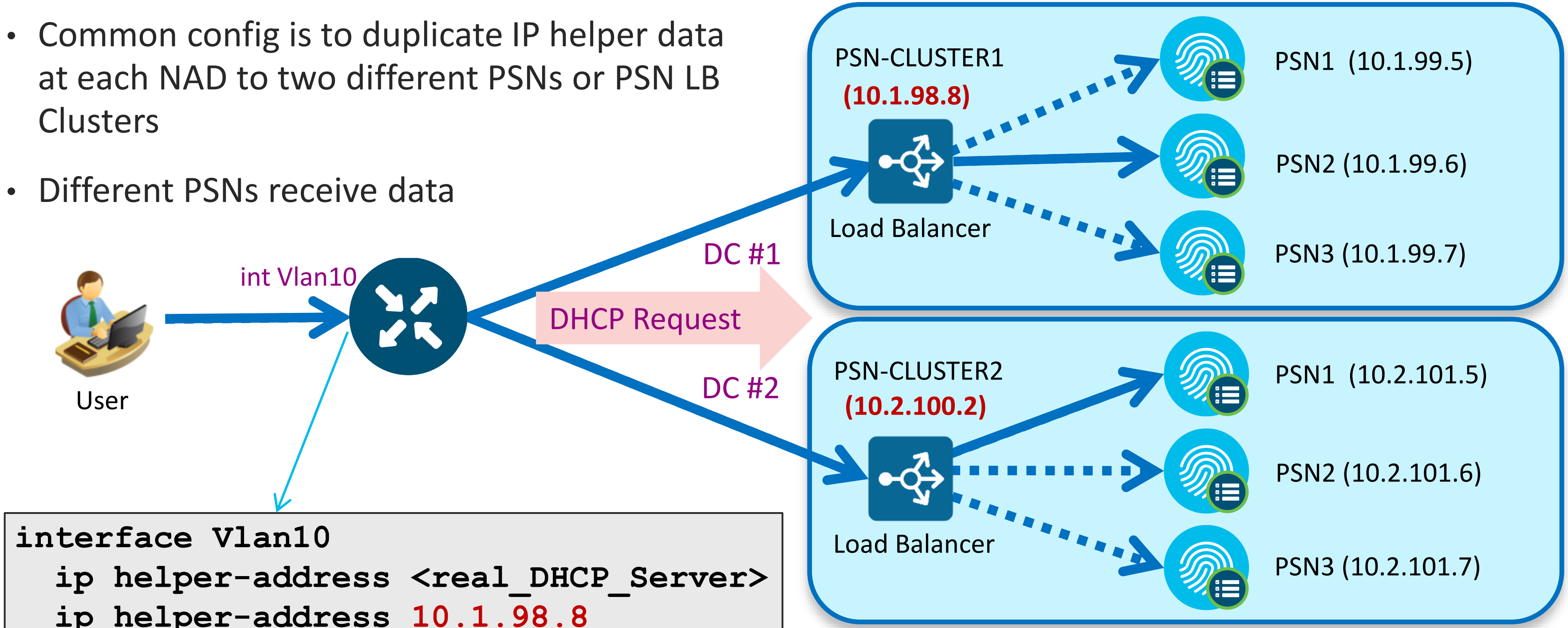
Monitor(P) - Monitor(S): tcp/443, udp/20514 (Syslog)

Policy - Policy:
  Node Groups/JGroups: tcp/7800
  Proxy CoA: udp/1700
  PSN-SXPSN: tcp/443
All nodes - AMQPS: tcp/8671
intranode- AMQ: tcp/8672 (N/A)
15672 for messaging (N/A)
pxGrid - pxGrid: tcp/5222

Profiling Redundancy – Duplicating Profile Data

Different DHCP Addresses
- Provides Redundancy but Leads to Contention for Ownership = Replication

- Common config is to duplicate IP helper data at each NAD to two different PSNs or PSN LB Clusters
- Different PSNs receive data



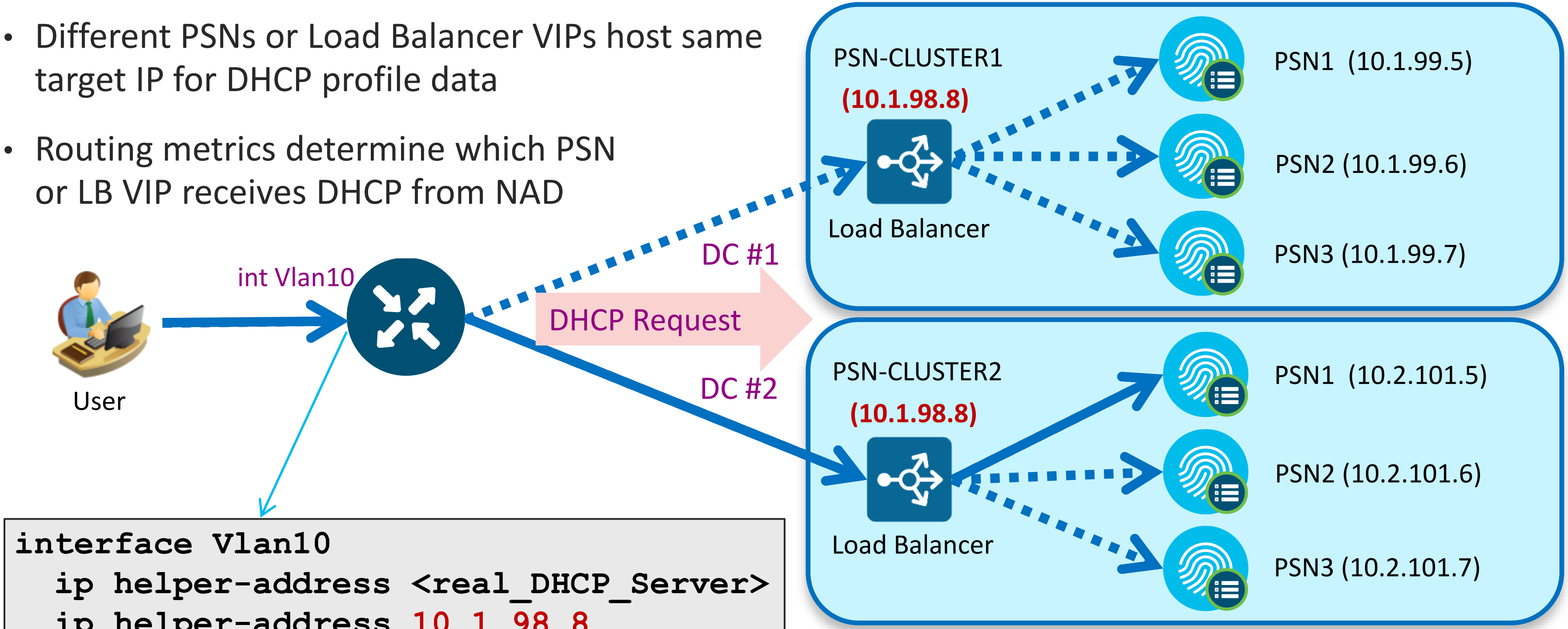
```
interface Vlan10
  ip helper-address <real_DHCP_Server>
  ip helper-address 10.1.98.8
  ip helper-address 10.2.100.2
```

Note: LB depicted, but NOT required

Scaling Profiling and Replication

Single DHCP VIP Address using Anycast
- Limit Profile Data to a Single PSN and Node Group

- Different PSNs or Load Balancer VIPs host same target IP for DHCP profile data
- Routing metrics determine which PSN or LB VIP receives DHCP from NAD

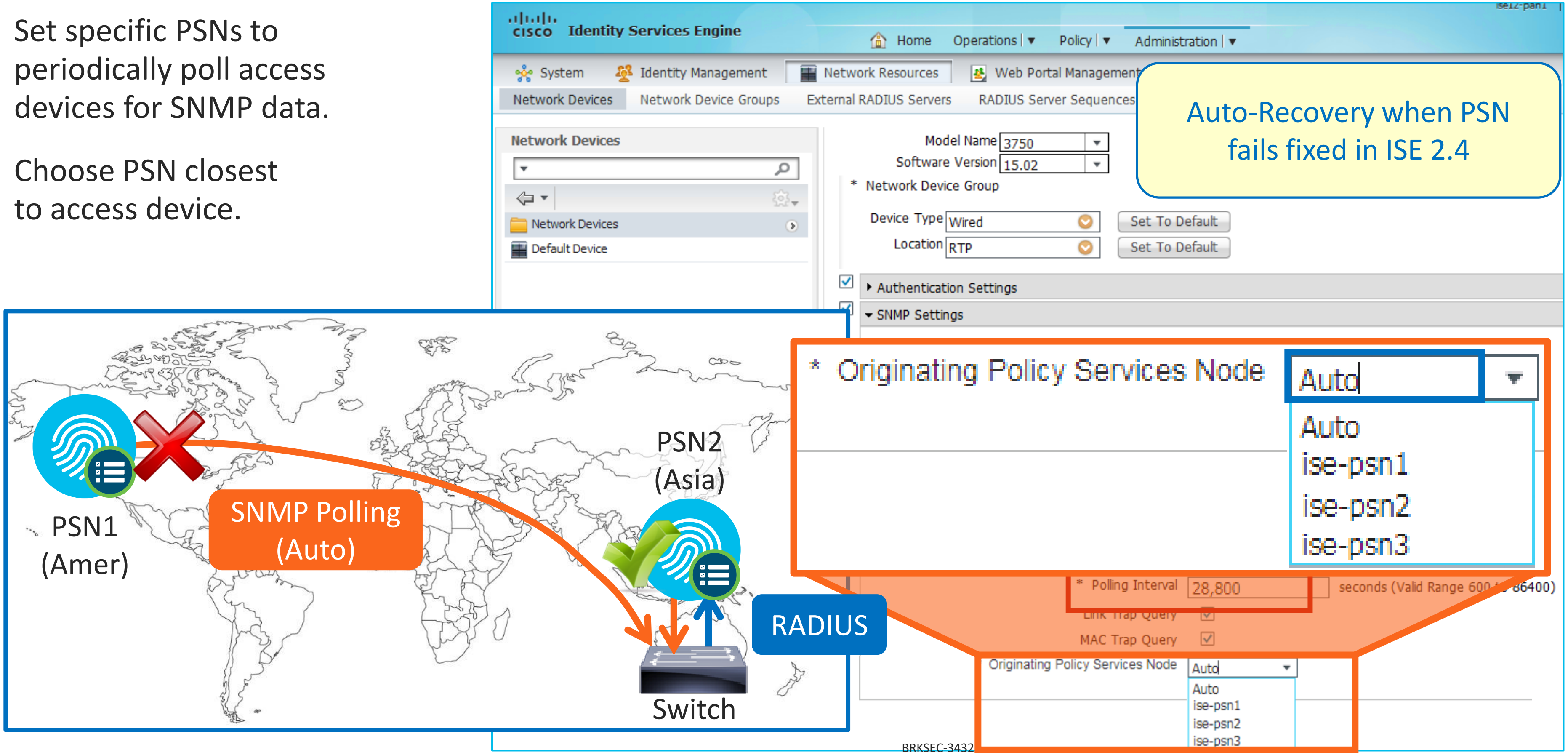


```
interface Vlan10
  ip helper-address <real_DHCP_Server>
  ip helper-address 10.1.98.8
```

Note: LB depicted, but NOT required

Profiler Tuning for Polled SNMP Query Probe

- Set specific PSNs to periodically poll access devices for SNMP data.
- Choose PSN closest to access device.



Auto-Recovery when PSN fails fixed in ISE 2.4

Model Name 3750

Software Version 15.02

* Network Device Group

Device Type Wired

Location RTP

☑ Authentication Settings

☑ SNMP Settings

* Polling Interval 28,800 seconds (Valid Range 600 to 86400)

Link Trap Query ☑

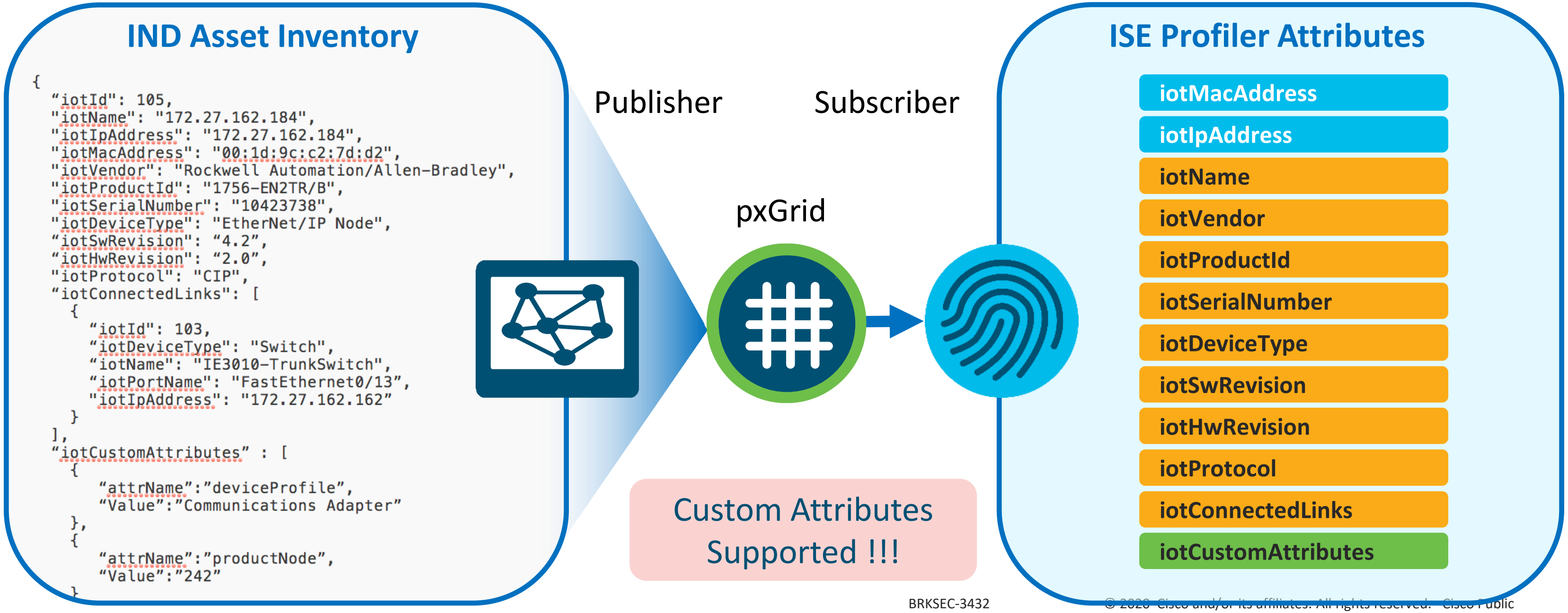
MAC Trap Query ☑

* Originating Policy Services Node Auto

pxGrid Profiler Probe (Context In)

First Integration with Cisco Industrial Network Director (IND)

- IND communicates with Industrial Switches and Security Devices and collects detailed information about the connected manufacturing devices.
- IND v1.3 adds pxGrid Publisher interface to communicate IoT attributes to ISE.



IND Asset Inventory

```
{
  “iotId": 105,
  "iotName": "172.27.162.184",
  "iotIpAddress": "172.27.162.184",
  "iotMacAddress": "00:1d:9c:c2:7d:d2",
  "iotVendor": "Rockwell Automation/Allen-Bradley",
  "iotProductId": "1756-EN2TR/B",
  "iotSerialNumber": "10423738",
  "iotDeviceType": "EtherNet/IP Node",
  “iotSwRevision": “4.2”,
  “iotHwRevision": “2.0”,
  "iotProtocol": "CIP",
  “iotConnectedLinks": [
    {
      “iotId": 103,
      “iotDeviceType": "Switch",
      “iotName": "IE3010-TrunkSwitch",
      “iotPortName": "FastEthernet0/13”,
      "iotIpAddress": "172.27.162.162”
    }
  ],
  “iotCustomAttributes” : [
    {
       “attrName”:”deviceProfile”,
       “Value”:”Communications Adapter”
    },
    {
       “attrName”:”productNode”,
       “Value”:”242”
    }
```

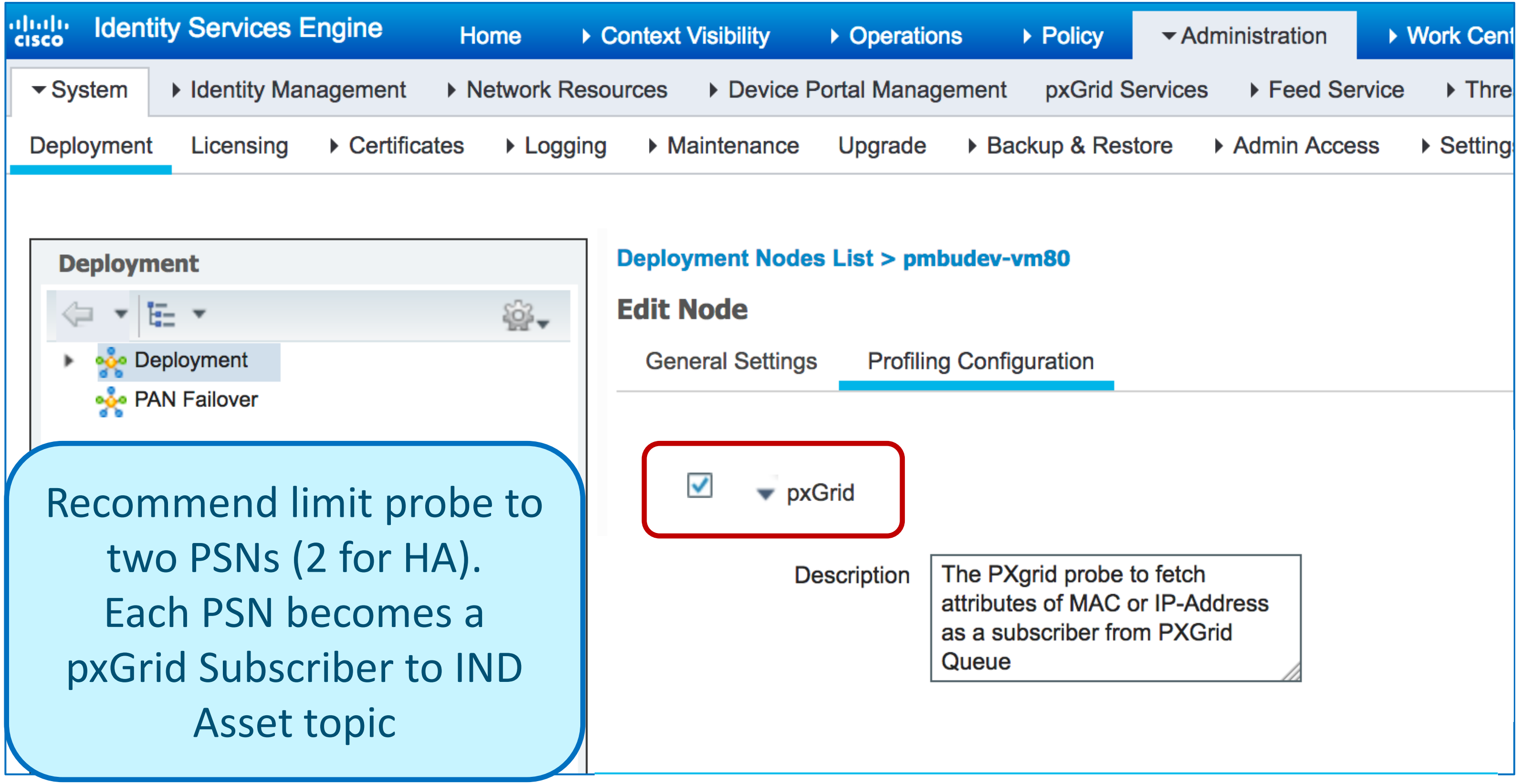
ISE Profiler Attributes

- iotMacAddress
- iotIpAddress
- iotName
- iotVendor
- iotProductId
- iotSerialNumber
- iotDeviceType
- iotSwRevision
- iotHwRevision
- iotProtocol
- iotConnectedLinks
- iotCustomAttributes

Custom Attributes Supported !!!

pxGrid Profiler Probe

For Your Reference



Deployment Nodes List > pmbudev-vm80

Edit Node

General Settings | Profiling Configuration

☑ pxGrid

Description: The PXgrid probe to fetch attributes of MAC or IP-Address as a subscriber from PXGrid Queue

Recommend limit probe to two PSNs (2 for HA). Each PSN becomes a pxGrid Subscriber to IND Asset topic

New and Updated IoT Profile Libraries

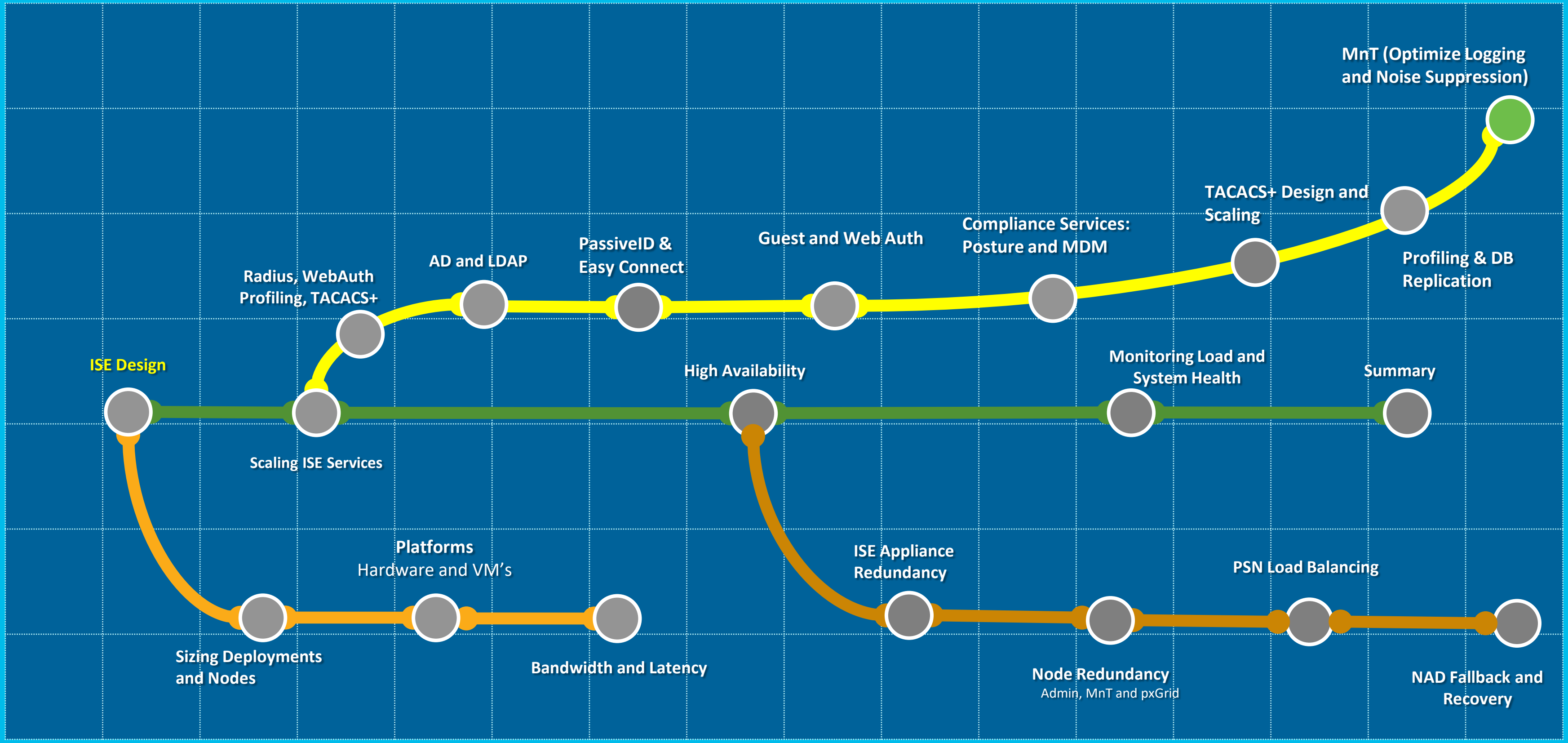
Delivered via ISE Community: https://community.cisco.com/t5/security-documents/ise-endpoint-profiles/ta-p/3641187

- Automation and Control
  - Industrial / Manufacturing
  - Building Automation
  - Power / Lighting
  - Transportation / Logistics
  - Financial (ATM, Vending, PoS, eCommerce)
  - IP Camera / Audio-Video / Surveillance and Access Control
  - Other (Defense, HVAC, Elevators, etc)
- Windows Embedded
- Medical NAC Profile Library – Updated

Session Agenda

MnT (Optimize Logging and Noise Suppression)

You Are Here ●



MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Cisco*live!*

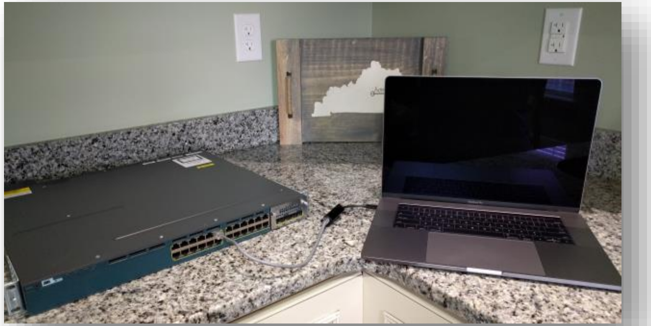
The Fall Out From the Mobile Explosion and IoT

- Explosion in number and type of endpoints on the network.
- High auth rates from mobile devices—many personal (unmanaged).
  - Short-lived connections: Continuous sleep/hibernation to conserve battery power, roaming, …
- Misbehaving supplicants: Unmanaged endpoints from numerous mobile vendors may be misconfigured, missing root CA certificates, or running less-than-optimal OS versions
- Misconfigured NADs. Often timeouts too low & misbehaving clients go unchecked/not throttled.
- Misconfigured Load Balancers—Suboptimal persistence and excessive RADIUS health probes.
- Increased logging from Authentication, Profiling, NADs, Guest Activity, …
- System not originally built to scale to new loads.
- End user behavior when above issues occur.
- Bugs in client, NAD, or ISE.

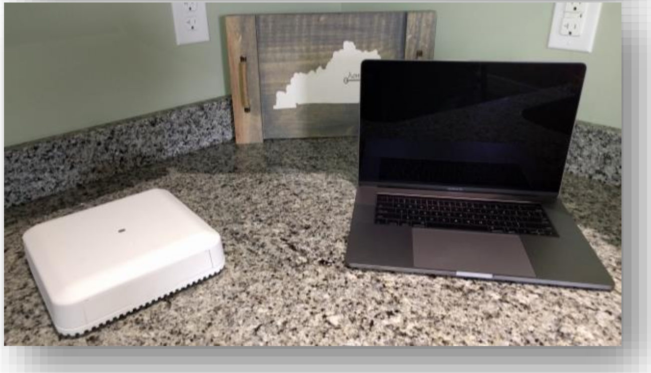
Advice: Sizing

Endpoint Behavior

- Different Endpoints behave differently on a network
- Because of this we need to consider the types of endpoints when sizing deployments
- Mobile (handheld) devices are the most demanding due to wireless/power restrictions
- Based on observations from many deployments, a 1x/2x/5x ratio is a good rule of thumb



=1X

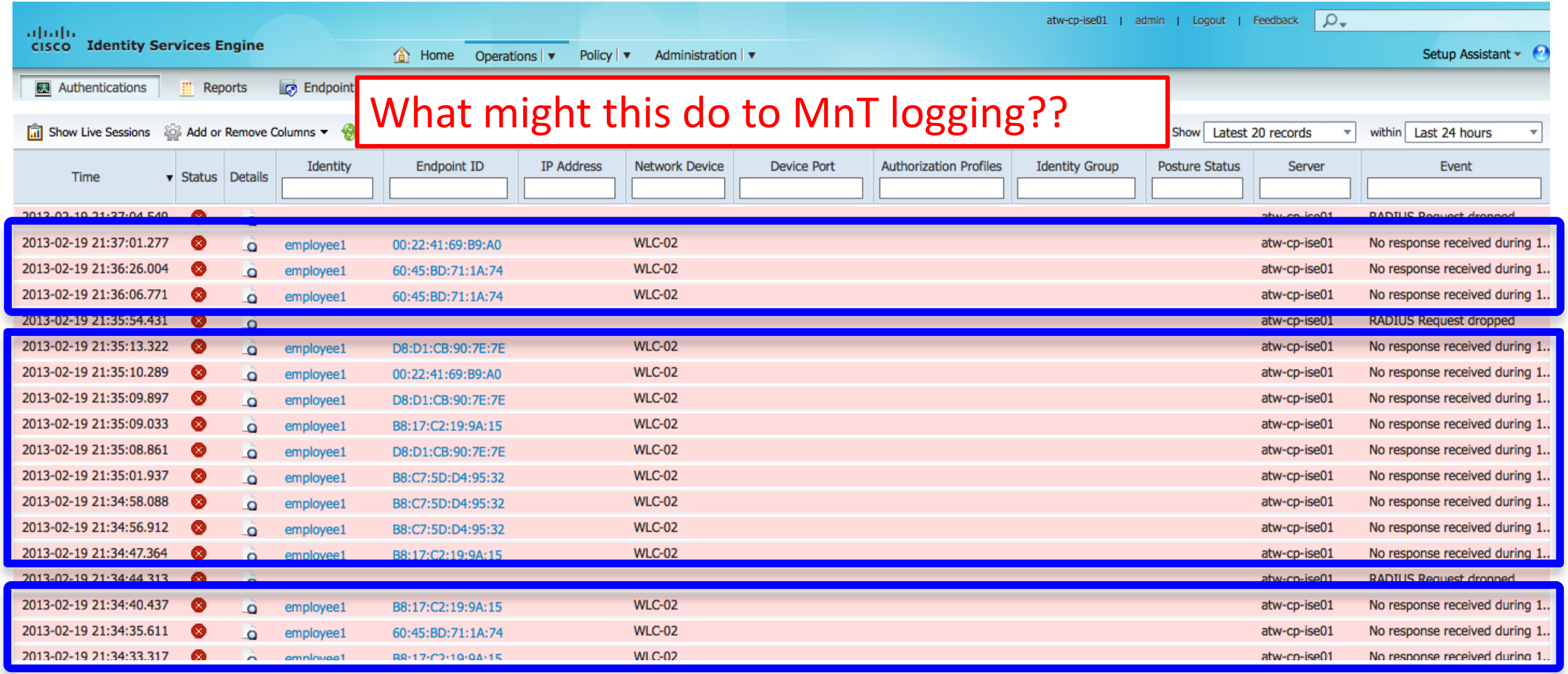


=2X

=5X

No Response Received From Client

For Your Reference



What might this do to MnT logging??

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2013-02-19 21:37:04.549	☒										atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:37:01.277	☒		employee1	00:22:41:69:B9:A0		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:36:26.004	☒		employee1	60:45:BD:71:1A:74		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:36:06.771	☒		employee1	60:45:BD:71:1A:74		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:54.431	☒										atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:35:13.322	☒		employee1	D8:D1:CB:90:7E:7E		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:10.289	☒		employee1	00:22:41:69:B9:A0		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:09.897	☒		employee1	D8:D1:CB:90:7E:7E		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:09.033	☒		employee1	B8:17:C2:19:9A:15		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:08.861	☒		employee1	D8:D1:CB:90:7E:7E		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:35:01.937	☒		employee1	B8:C7:5D:D4:95:32		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:58.088	☒		employee1	B8:C7:5D:D4:95:32		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:56.912	☒		employee1	B8:C7:5D:D4:95:32		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:47.364	☒		employee1	B8:17:C2:19:9A:15		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:44.313	☒										atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:34:40.437	☒		employee1	B8:17:C2:19:9A:15		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:35.611	☒		employee1	60:45:BD:71:1A:74		WLC-02					atw-cp-ise01	No response received during 1..
2013-02-19 21:34:33.317	☒		employee1	B8:17:C2:19:9A:15		WLC-02					atw-cp-ise01	No response received during 1..

Clients Misbehave!

- Example education customer:
  - ONLY 6,000 Endpoints (all BYOD style)
  - 10M Auths / 9M Failures in a 24 hours!
  - 42 Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS).
- Supplicant List:
  - Kyocera, Asustek, Murata, Huawei, Motorola, HTC, Samsung, ZTE, RIM, SonyEric, ChiMeiCo, Apple, Intel, Cybertan, Liteon, Nokia, HonHaiPr, Palm, Pantech, LgElectr, TaiyoYud, Barnes&N
- 5411 No response received during 120 seconds on last EAP message sent to the client
  - This error has been seen at a number of Escalation customers
  - Typically the result of a misconfigured or misbehaving supplicant not completing the EAP process.

Challenge: How to reduce the flood of log messages while increasing PSN and MNT capacity and tolerance

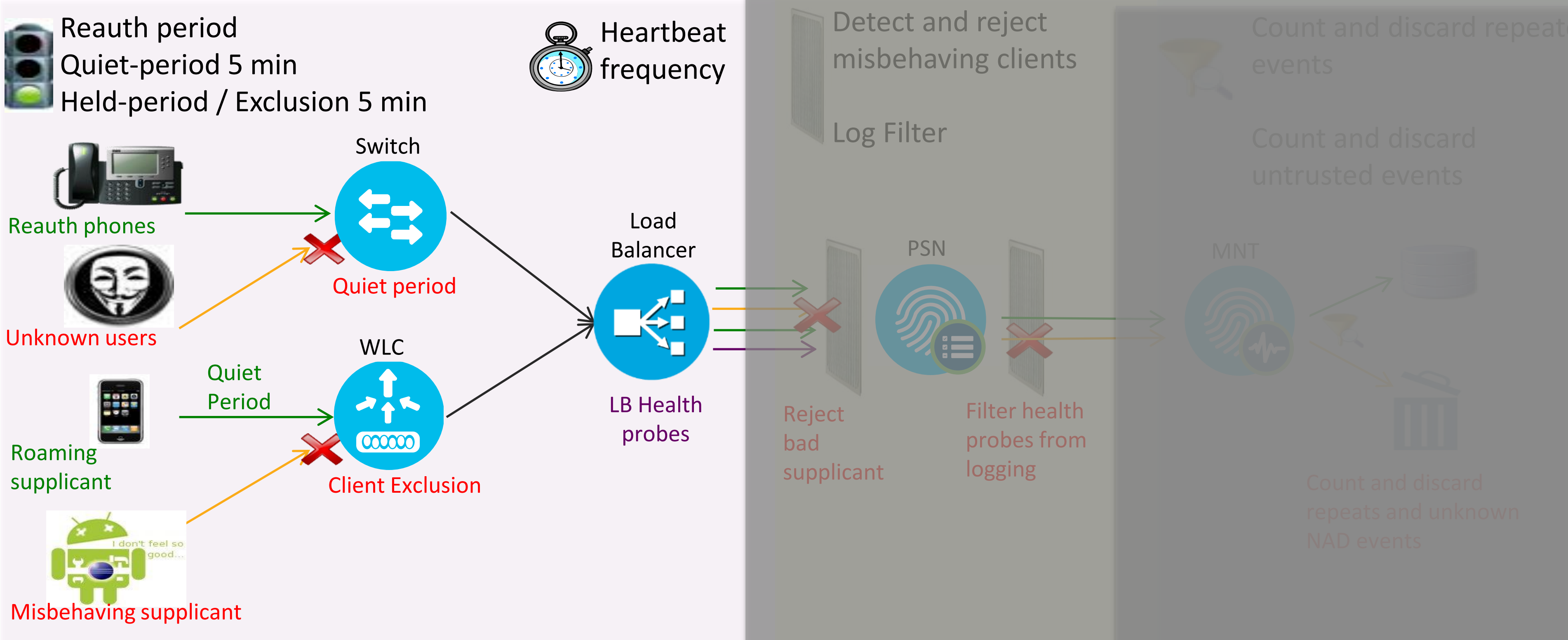
2

Getting More Information With Less Data

Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source

Filtering at Receiving Chain



Reauth period
Quiet-period 5 min
Held-period / Exclusion 5 min

Heartbeat frequency

Detect and reject misbehaving clients

Log Filter

Count and discard repeat

events

Count and discard untrusted events

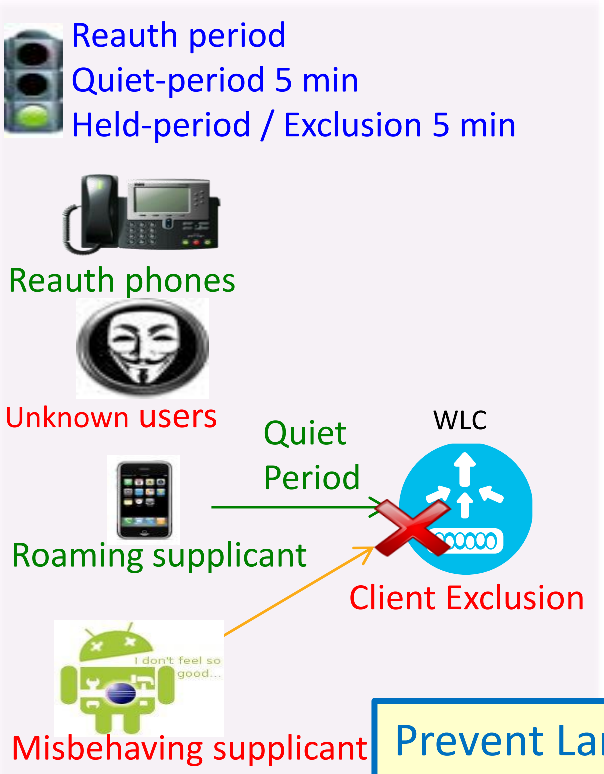
Tune NAD Configuration

Rate Limiting at Wireless Source

BRKSEC-2059

Deploying ISE in a Dynamic Environment

Clark Gambrel



Wireless (WLC)

- **RADIUS Server Timeout:** Increase from default of 2 to 5 sec
- **RADIUS Aggressive-Failover:** Disable aggressive failover
- **RADIUS Interim Accounting:** v7.6: Disable; v8.0+: Enable with interval of 0. (Update auto-sent on DHCP lease or Device Sensor)
- **Idle Timer:** Increase to 1 hour (3600 sec) for secure SSIDs
- **Session Timeout:** Increase to 2+ hours (7200+ sec)
- **Client Exclusion:** Enable and set exclusion timeout to 180+ sec
- **Roaming:** Enable CCKM / SKC / 802.11r (when feasible)
- **Bugfixes:** Upgrade WLC software to address critical defects

Prevent Large-Scale Wireless RADIUS Network Melt Downs

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118703-technote-wlc-00.html

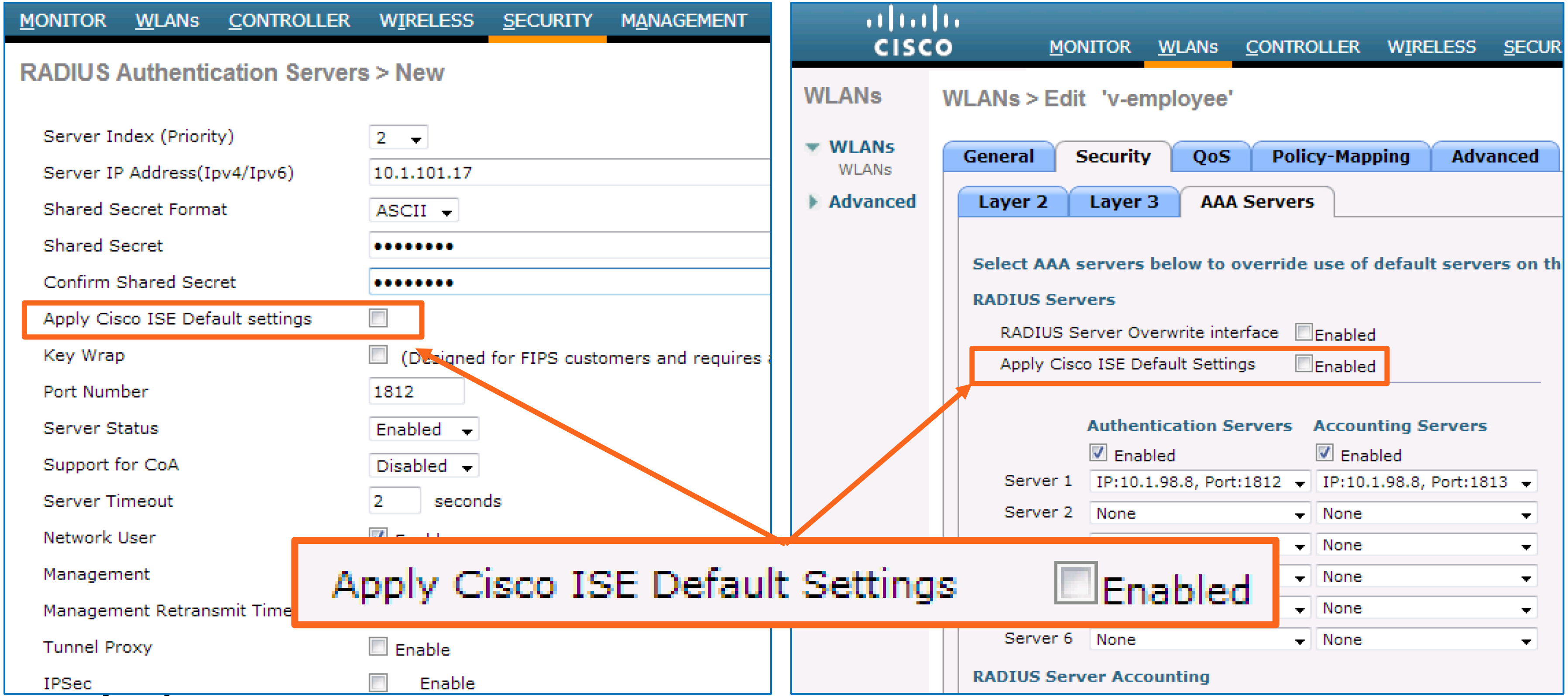
Wired & Wireless recommended links

Best Practices and Guides

- Top 6 settings for AireOS and ISE Wireless
- ISE and Catalyst 9800 series integration guide
- ISE Guest Access Prescriptive Deployment Guide
- Cisco ISE BYOD Prescriptive Deployment Guide
- ISE Secure Wired Access Prescriptive Deployment Guide

One-Click Setup for ISE Best Practice Config

Added in WLC 8.4



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	10.1.101.17
Shared Secret Format	ASCII
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Apply Cisco ISE Default settings	□
Key Wrap	□ (Designed for FIPS customers and requires a
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	2 seconds
Network User	☑
Management	
Management Retransmit Time	
Tunnel Proxy	□ Enable
IPSec	□ Enable

WLANs > Edit 'v-employee'

Select AAA servers below to override use of default servers on th

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

Apply Cisco ISE Default Settings □ Enabled

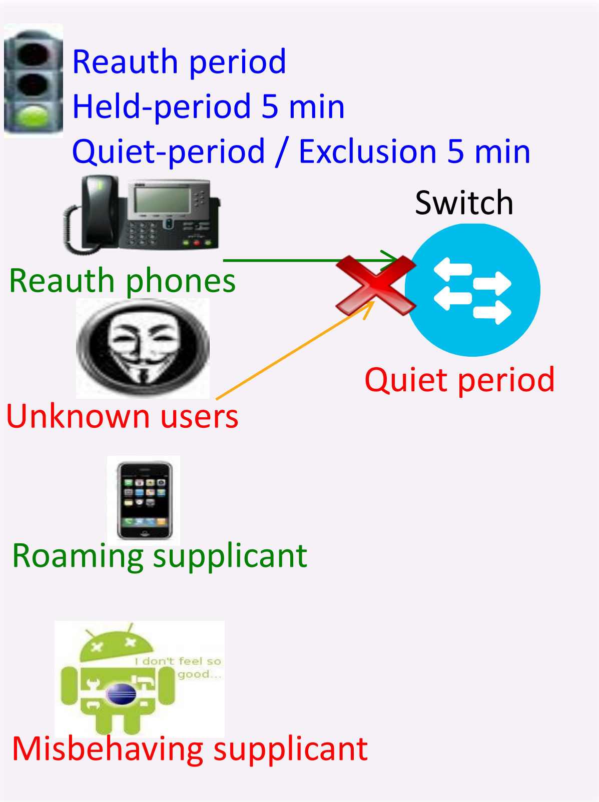
	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.1.98.8, Port:1812	IP:10.1.98.8, Port:1813
Server 2	None	None
		None
		None
		None
Server 6	None	None

RADIUS Server Accounting

Apply Cisco ISE Default Settings □ Enabled

Tune NAD Configuration

Rate Limiting at Wired Source



Reauth period
Held-period 5 min
Quiet-period / Exclusion 5 min

Switch

Reauth phones

Unknown users

Quiet period

Roaming supplicant

Misbehaving supplicant

Wired (IOS / IOS-XE)

- **RADIUS Interim Accounting:** Use *newinfo* parameter with long interval (for example, 24-48 hrs), if available. Otherwise, set 15 mins. If LB present, set shorter than RADIUS persist time.
- **802.1X Timeouts**
  - held-period: Increase to 300+ sec
  - quiet-period: Increase to 300+ sec
  - ratelimit-period: Increase to 300+ sec
- **Inactivity Timer:** Disable or increase to 1+ hours (3600+ sec)
- **Session Timeout:** Disable or increase to 2+ hours (7200+ sec)
- **Reauth Timer:** Disable or increase to 2+ hours (7200+ sec)
- **Bugfixes:** Upgrade software to address critical defects.

Load Balancer RADIUS Test Probes

Citrix Example

- Probe frequency and retry settings:
  - Time interval between probes:

    interval *seconds* # Default: 5
  - Number of retries

    retries *number* # Default: 3
- Sample Citrix probe configuration:

```
add lb monitor PSN-Probe RADIUS -respCode 2
-userName citrix_probe -password citrix123
-radKey cisco123 -LRTM ENABLED –interval 10
–retries 3 -destPort 1812
```

- **Recommended setting:** Failover must occur before RADIUS timeout (typically 15-35 sec) while avoiding excessive probing

F5 Example

- Probe frequency and retry settings:
  - Time interval between probes:

    Interval *seconds* # Default: 10
  - Timeout before failure = 3*(interval)+1:

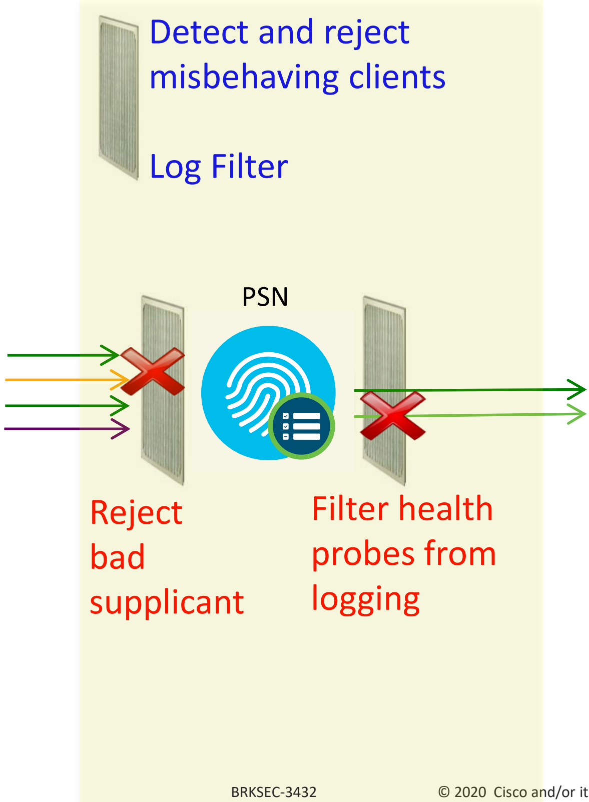
    Timeout *seconds* # Default: 31
- Sample F5 RADIUS probe configuration:

```
Name PSN-Probe
Type  RADIUS
Interval 10
Timeout 31
Manual Resume No
Check Util Up Yes
User Name f5-probe
Password f5-ltm123
Secret cisco123
Alias Address * All Addresses
Alias Service Port 1812
Debug No
```

PSN Noise Suppression and Smarter Logging

Filter Noise and Provide Better Feedback on Authentication Issues

- PSN Collection Filters
- PSN Misconfigured Client Dynamic Detection and Suppression
- PSN Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or Network Access Server (NAS)
- Failure Reason Message and Classification
- Identify RADIUS Request From Session Started on Another PSN
- Improved Treatment for Empty NAK List


Detect and reject misbehaving clients
Log Filter
PSN
Reject bad supplicant
Filter health probes from logging

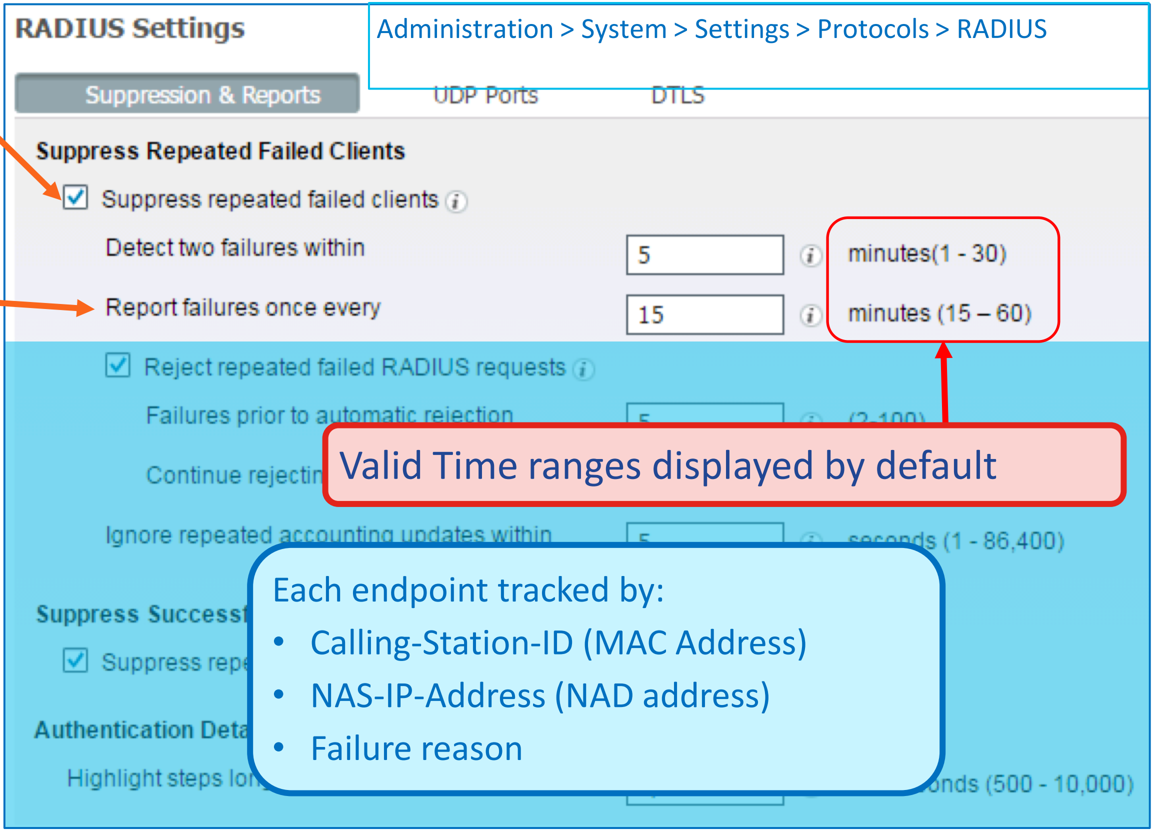
PSN Filtering and Noise Suppression

Dynamic Client Suppression

Updated in ISE 2.2!

Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics



Administration > System > Settings > Protocols > RADIUS

RADIUS Settings

Suppress Repeated Failed Clients

☑ Suppress repeated failed clients

Detect two failures within	5	minutes(1 - 30)
Report failures once every	15	minutes (15 – 60)

☑ Reject repeated failed RADIUS requests

Failures prior to automatic rejection	5	(2-100)
Continue rejectin		
Ignore repeated accounting updates within	5	seconds (1 - 86,400)

Suppress Successf

☑ Suppress repe

Authentication Deta

Highlight steps lon ... onds (500 - 10,000)

Valid Time ranges displayed by default

Each endpoint tracked by:

- Calling-Station-ID (MAC Address)
- NAS-IP-Address (NAD address)
- Failure reason

PSN Filtering and Noise Suppression

Dynamic Client Suppression

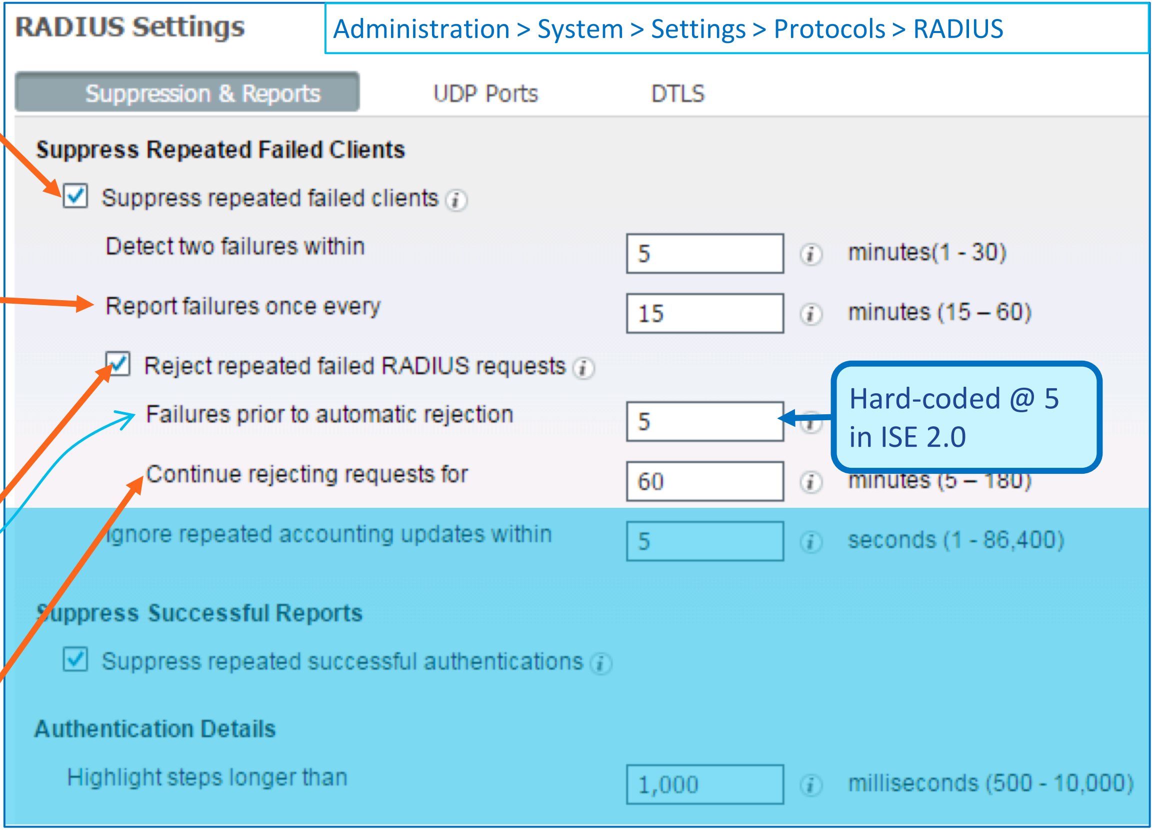
Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics

Send immediate Access-Reject (do not even process request) IF:

1) Flagged for suppression
2) Fail auth total X times for same failure reason (inc 2 prev)

Fully process next request after rejection period expires.



RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppress Repeated Failed Clients

☑ Suppress repeated failed clients

Detect two failures within: 5 minutes(1 - 30)

Report failures once every: 15 minutes (15 – 60)

☑ Reject repeated failed RADIUS requests

Failures prior to automatic rejection: 5

Hard-coded @ 5 in ISE 2.0

Continue rejecting requests for: 60 minutes (5 – 180)

Ignore repeated accounting updates within: 5 seconds (1 - 86,400)

Suppress Successful Reports

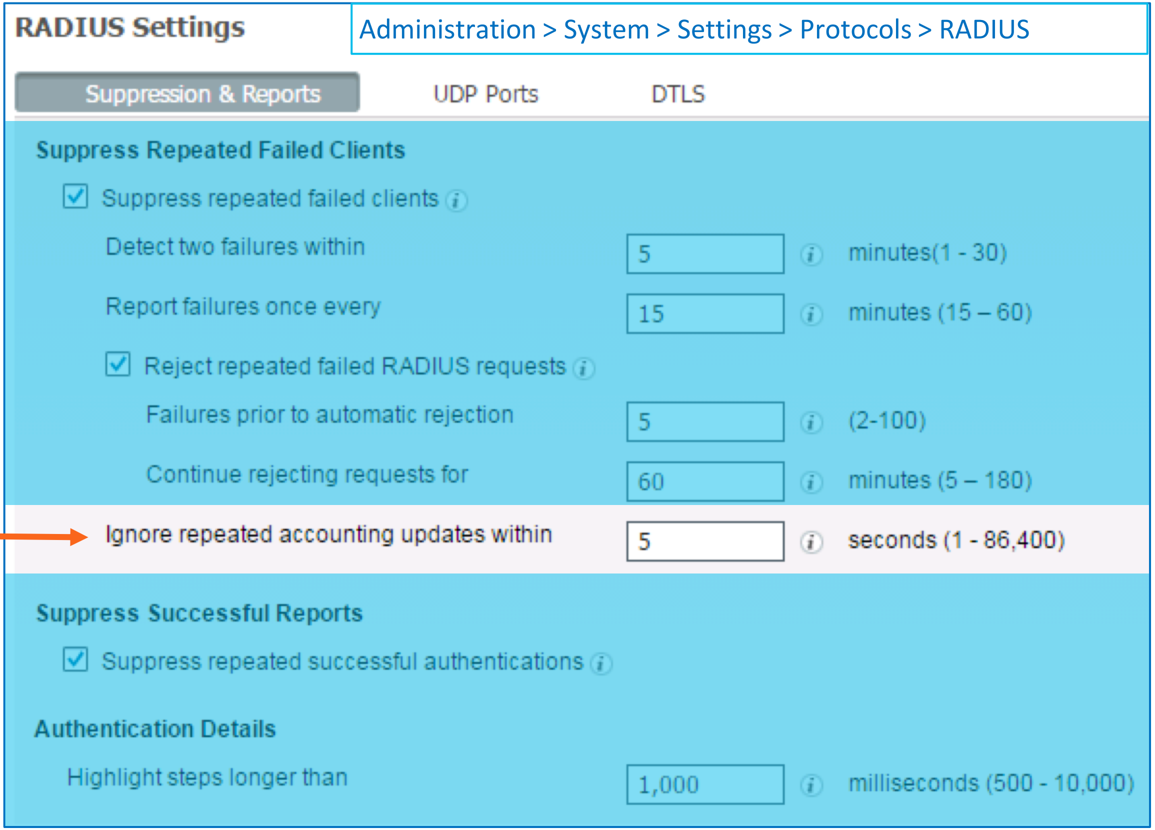
☑ Suppress repeated successful authentications

Authentication Details

Highlight steps longer than: 1,000 milliseconds (500 - 10,000)

PSN Noise Suppression

Drop Excessive RADIUS Accounting Updates from “Misconfigured NADs”



RADIUS Settings

Administration > System > Settings > Protocols > RADIUS

Suppress Repeated Failed Clients

☑ Suppress repeated failed clients

Detect two failures within: 5 minutes(1 - 30)

Report failures once every: 15 minutes (15 – 60)

☑ Reject repeated failed RADIUS requests

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

Authentication Details

Highlight steps longer than: 1,000 milliseconds (500 - 10,000)

Allow 2 RADIUS Accounting Updates for same session in specified interval, then drop.

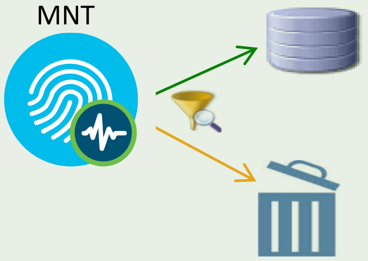
MnT Log Suppression and Smarter Logging

Drop and Count Duplicates / Provide Better Monitoring Tools

- Drop duplicates and increment counter in Live Log for “matching” passed authentications
- Display repeat counter to Live Sessions entries.
- Update session, but do not log RADIUS Accounting Interim Updates
- Log RADIUS Drops and EAP timeouts to separate table for reporting purposes and display as counters on Live Log Dashboard along with Misconfigured Supplicants and NADs
- Alarm enhancements
- Revised guidance to limit syslog at the source.
- MnT storage allocation and data retention limits
- More aggressive purging
- Allocate larger VM disks to increase logging capacity and retention.

Count and discard repeated events

Count and discard untrusted events



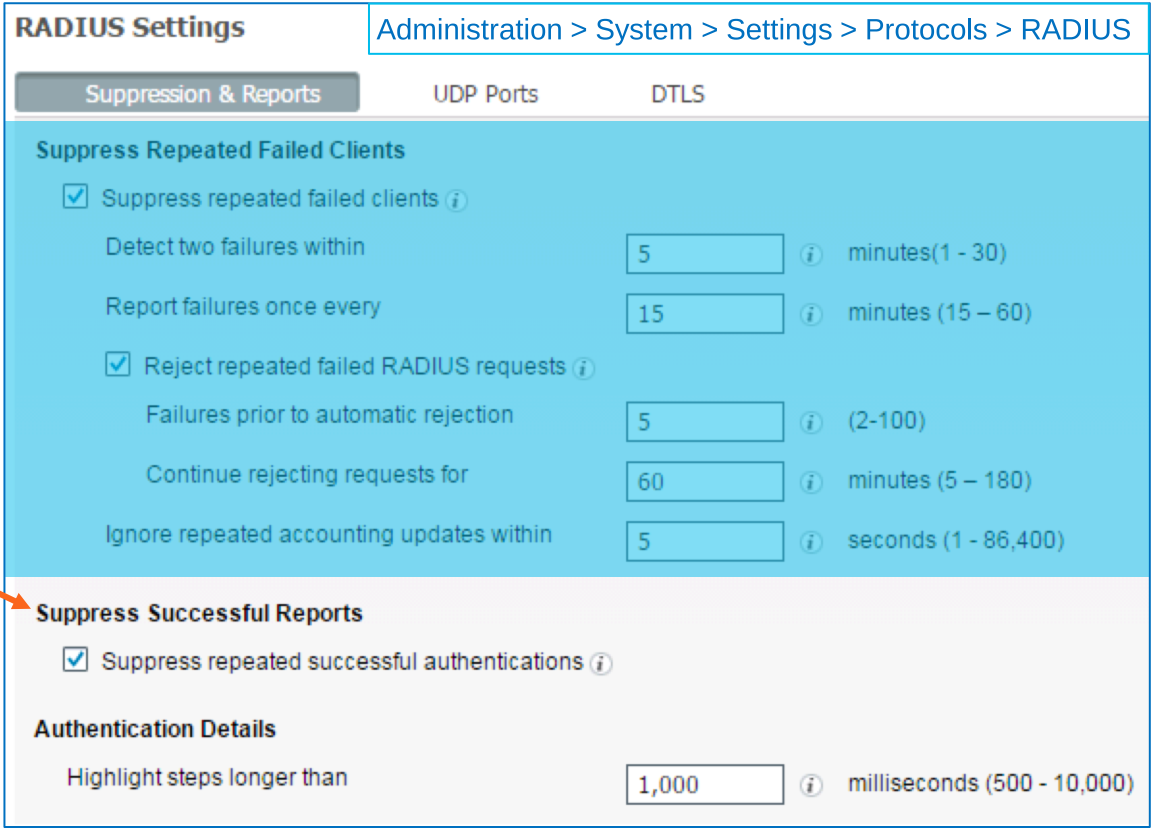
Count and discard repeats and unknown NAD events

MnT Noise Suppression

Suppress Storage of Repeated Successful Auth Events

Suppress Successful Reports
= Do not save repeated successful auth events for the same session to MnT DB

These events will not display in Live Authentications Log but do increment Repeat Counter.



RADIUS Settings

Administration > System > Settings > Protocols > RADIUS

Suppress Repeated Failed Clients

☑ Suppress repeated failed clients

Detect two failures within	5	minutes(1 - 30)
Report failures once every	15	minutes (15 – 60)

☑ Reject repeated failed RADIUS requests

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

Authentication Details

Highlight steps longer than	1,000	milliseconds (500 - 10,000)

MnT Noise Suppression

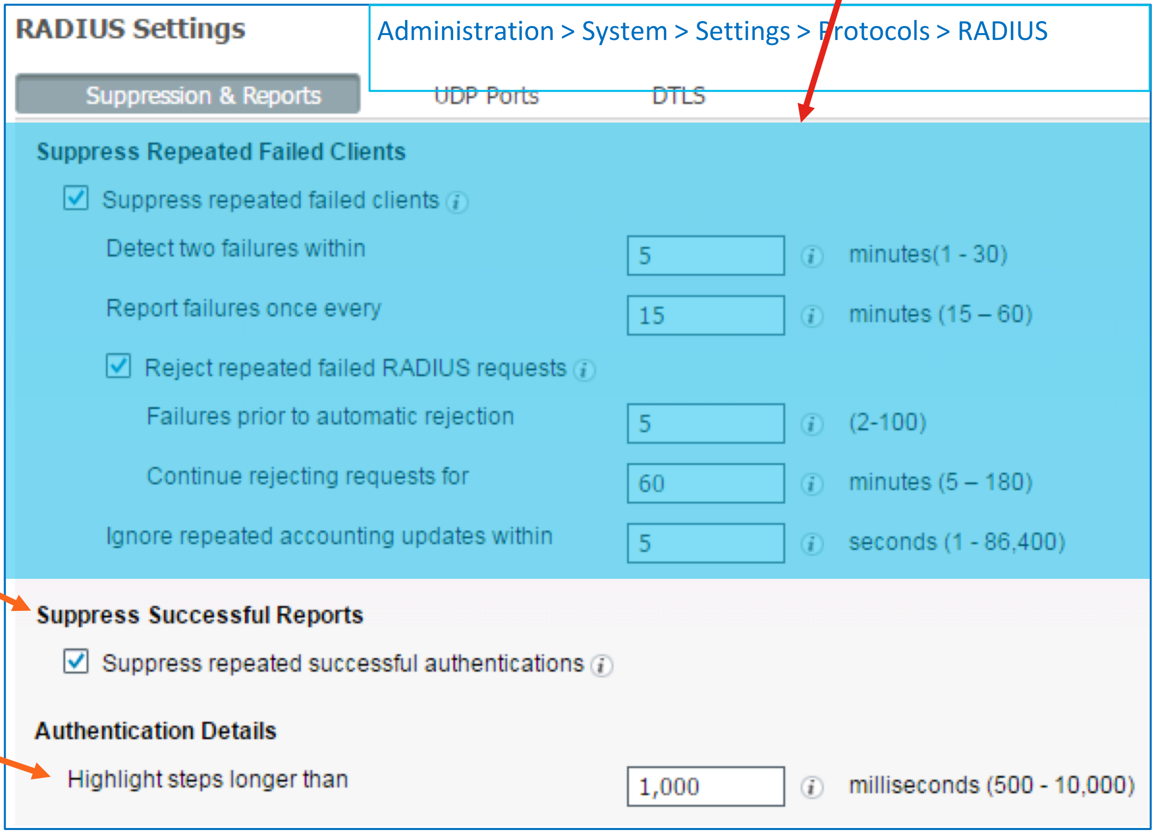
Suppress Storage of Repeated Successful Auth Events

Step latency is visible in Live Logs details

Suppress Successful Reports
= Do not save repeated successful auth events for the same session to MnT DB

These events will not display in Live Authentications Log but do increment Repeat Counter.

Detect NAD retransmission timeouts and Log auth steps > threshold.



Administration > System > Settings > Protocols > RADIUS

RADIUS Settings

Suppress Repeated Failed Clients

☑ Suppress repeated failed clients

Detect two failures within 5 minutes(1 - 30)

Report failures once every 15 minutes (15 – 60)

☑ Reject repeated failed RADIUS requests

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)

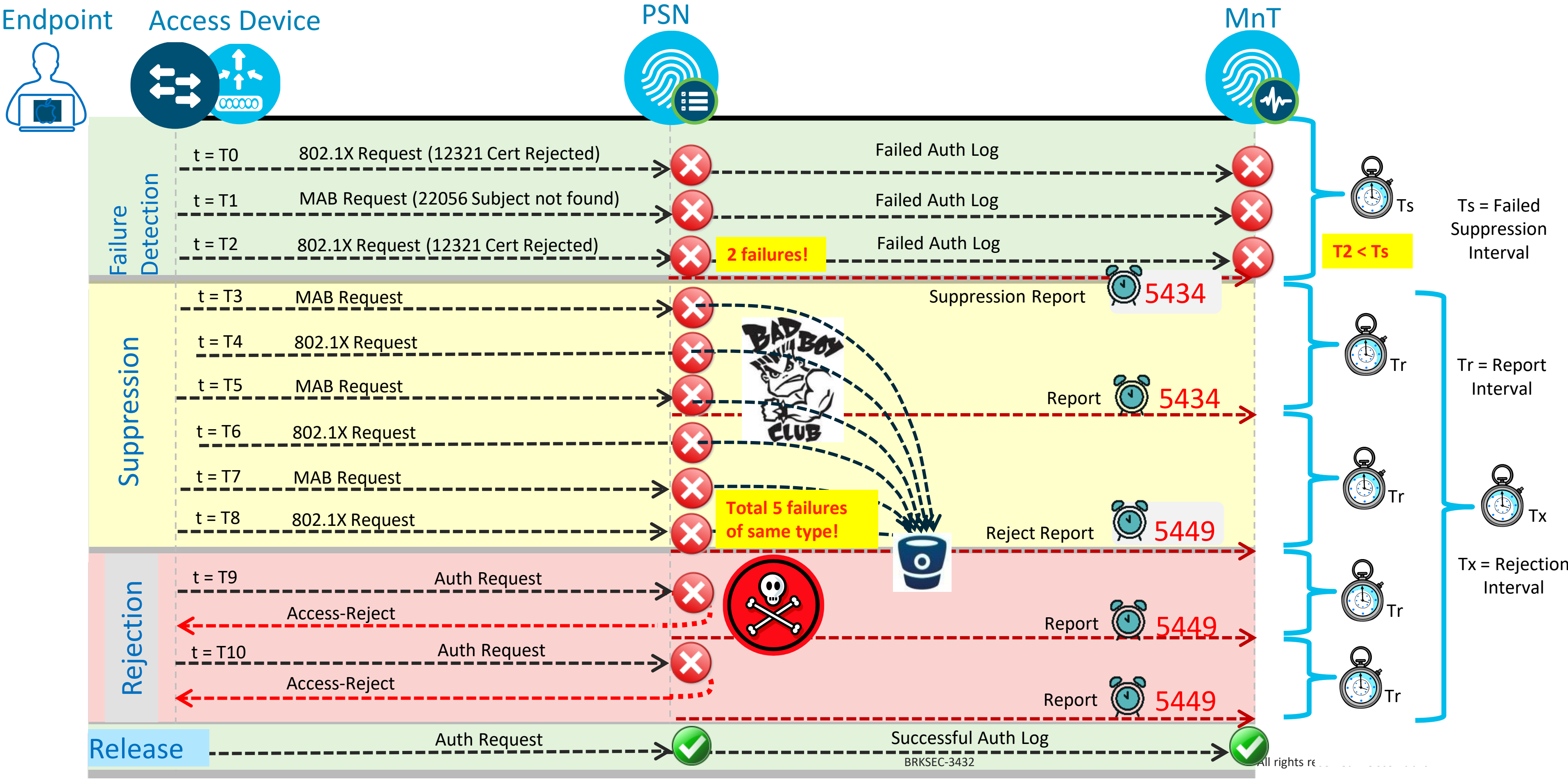
Suppress Successful Reports

☑ Suppress repeated successful authentications

Authentication Details

Highlight steps longer than 1,000 milliseconds (500 - 10,000)

Client Suppression and Reject Timers



Endpoint

Access Device

PSN

MnT

Failure Detection

t = T0 802.1X Request (12321 Cert Rejected)

Failed Auth Log

t = T1 MAB Request (22056 Subject not found)

Failed Auth Log

t = T2 802.1X Request (12321 Cert Rejected)

2 failures!

Failed Auth Log

Ts

T2 < Ts

Ts = Failed Suppression Interval

Suppression

t = T3 MAB Request

Suppression Report 5434

t = T4 802.1X Request

t = T5 MAB Request

Report 5434

Tr

Tr = Report Interval

t = T6 802.1X Request

t = T7 MAB Request

t = T8 802.1X Request

Total 5 failures of same type!

Reject Report 5449

Tr

Tx

Tx = Rejection Interval

Rejection

t = T9 Auth Request

Access-Reject

Report 5449

Tr

t = T10 Auth Request

Access-Reject

Report 5449

Tr

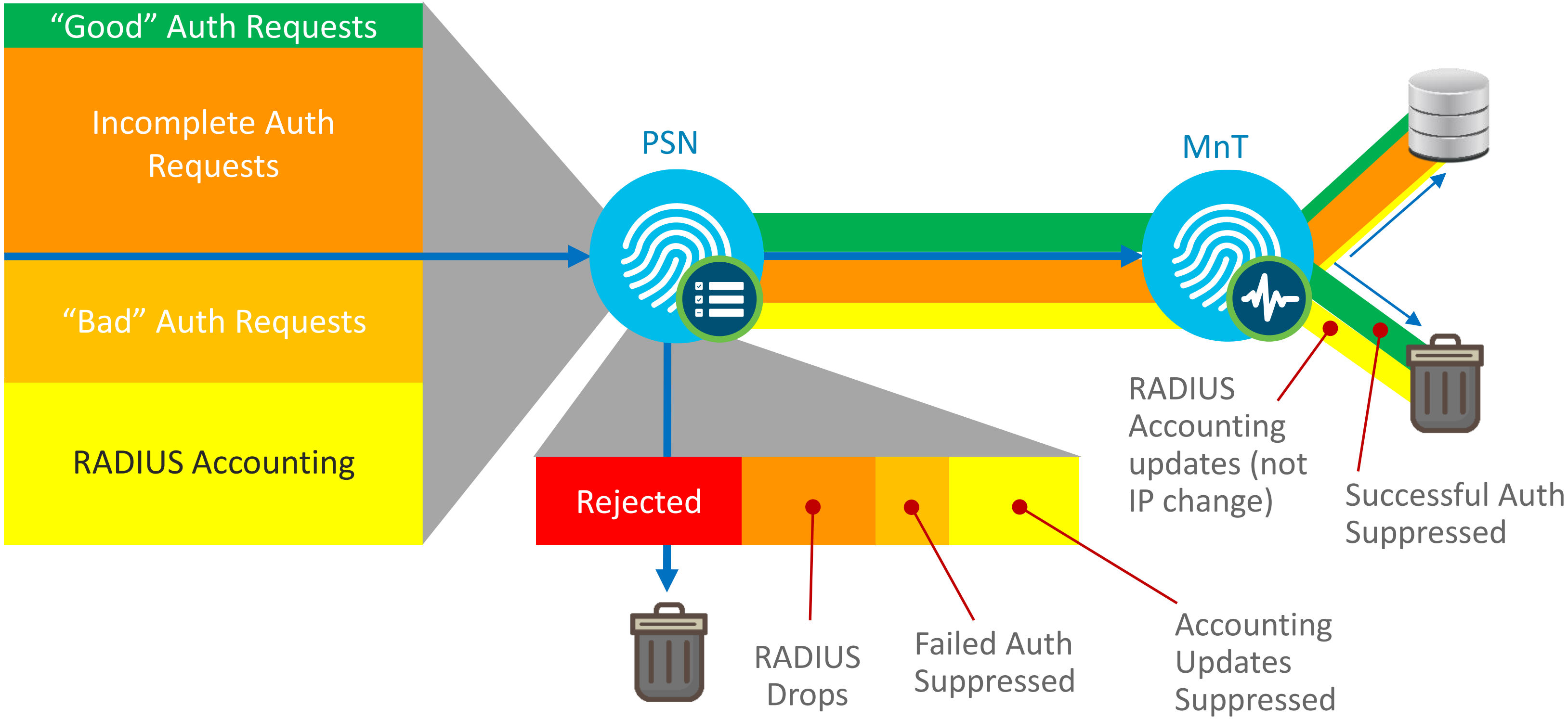
Release

Auth Request

Successful Auth Log

ISE Log Suppression

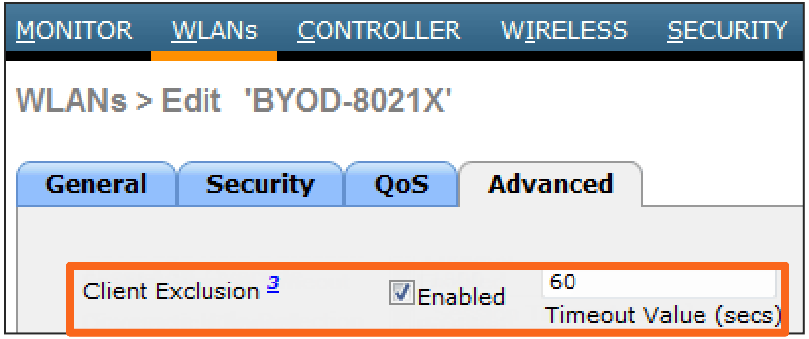
"Good"-put Versus "Bad"-put



WLC – Client Exclusion

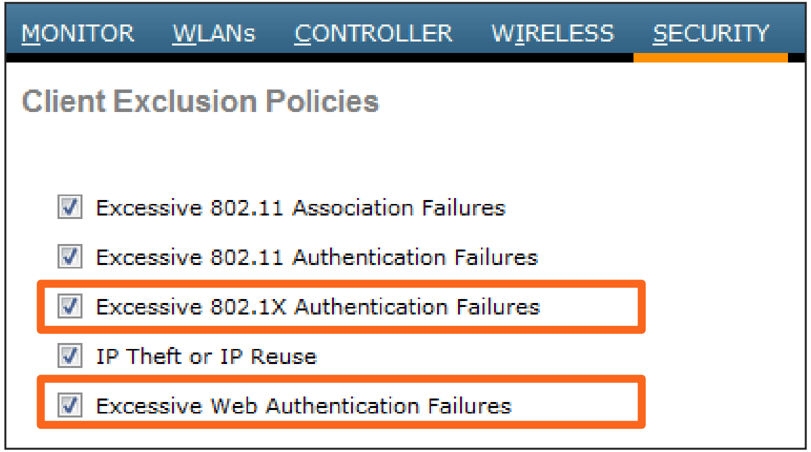
Blacklist Misconfigured or Malicious Clients

- **Excessive Authentication Failures**—Clients are excluded on the fourth authentication attempt, after three consecutive failures.
- Client excluded for Time Value specified in WLAN settings. Recommend increase to 1-5 min (60-300 sec). **3 min** is a good start.



WLANs > Edit 'BYOD-8021X'

Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)



Client Exclusion Policies

☑ Excessive 802.11 Association Failures

☑ Excessive 802.11 Authentication Failures

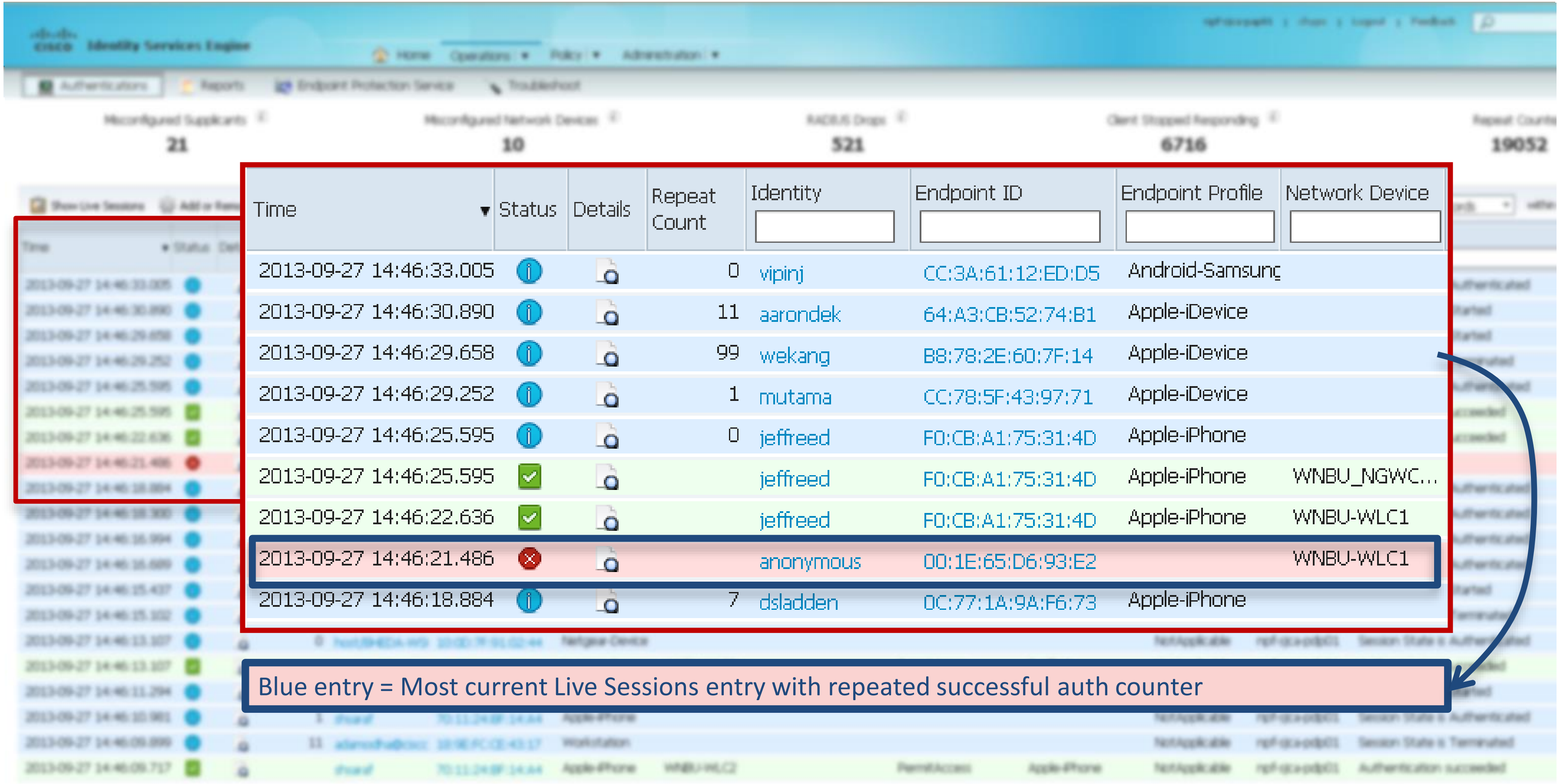
☑ Excessive 802.1X Authentication Failures

☑ IP Theft or IP Reuse

☑ Excessive Web Authentication Failures

Note: Diagrams show default values

Live Authentications and Sessions



Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	ℹ	🔍	0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890	ℹ	🔍	11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:29.658	ℹ	🔍	99	wekang	B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:29.252	ℹ	🔍	1	mutama	CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:25.595	ℹ	🔍	0	jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	
2013-09-27 14:46:25.595	✓	🔍		jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
2013-09-27 14:46:22.636	✓	🔍		jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21.486	✗	🔍		anonymous	00:1E:65:D6:93:E2		WNBU-WLC1
2013-09-27 14:46:18.884	ℹ	🔍	7	dsladden	0C:77:1A:9A:F6:73	Apple-iPhone	

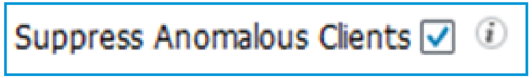
Blue entry = Most current Live Sessions entry with repeated successful auth counter

Authentication Suppression

Enable/Disable

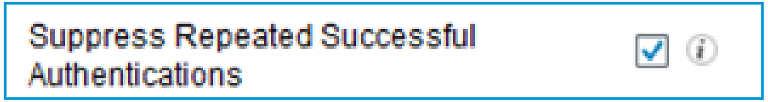
- **Global Suppression Settings:** Administration > System > Settings > Protocols > RADIUS

Failed Auth Suppression



Suppress Anomalous Clients ☑

Successful Auth Suppression



Suppress Repeated Successful Authentications ☑

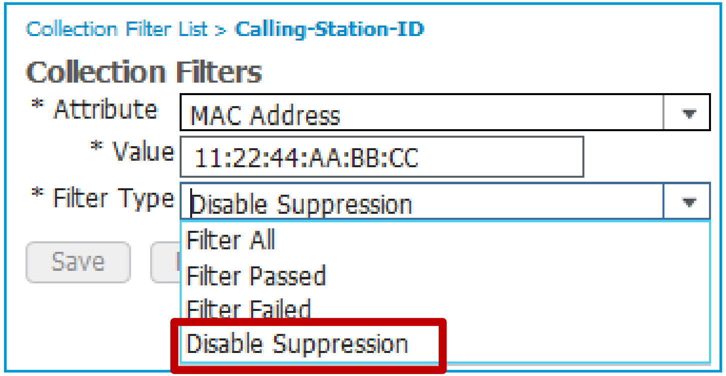
Caution: Do not disable suppression in deployments with very high auth rates.

It is highly recommended to keep Auth Suppression enabled to reduce MnT logging

- **Selective Suppression using Collection Filters:** Administration > System > Logging > Collection Filters

Configure specific traffic to bypass Successful Auth Suppression

Useful for troubleshooting authentication for a specific endpoint or group of endpoints, especially in high auth environments where global suppression is always required.



Collection Filter List > Calling-Station-ID

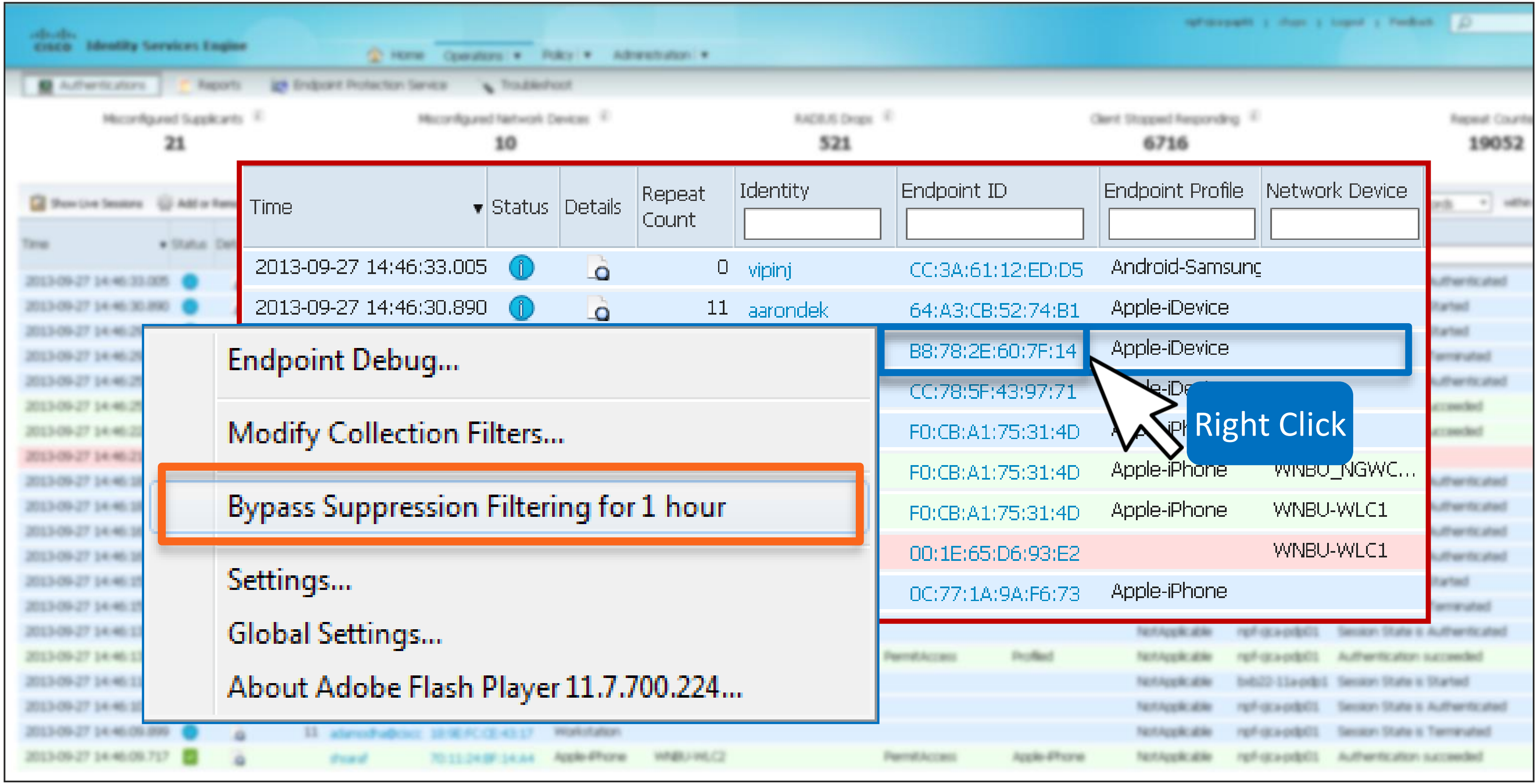
Collection Filters

* Attribute: MAC Address

* Value: 11:22:44:AA:BB:CC

* Filter Type: Disable Suppression

Per-Endpoint Time-Constrained Suppression

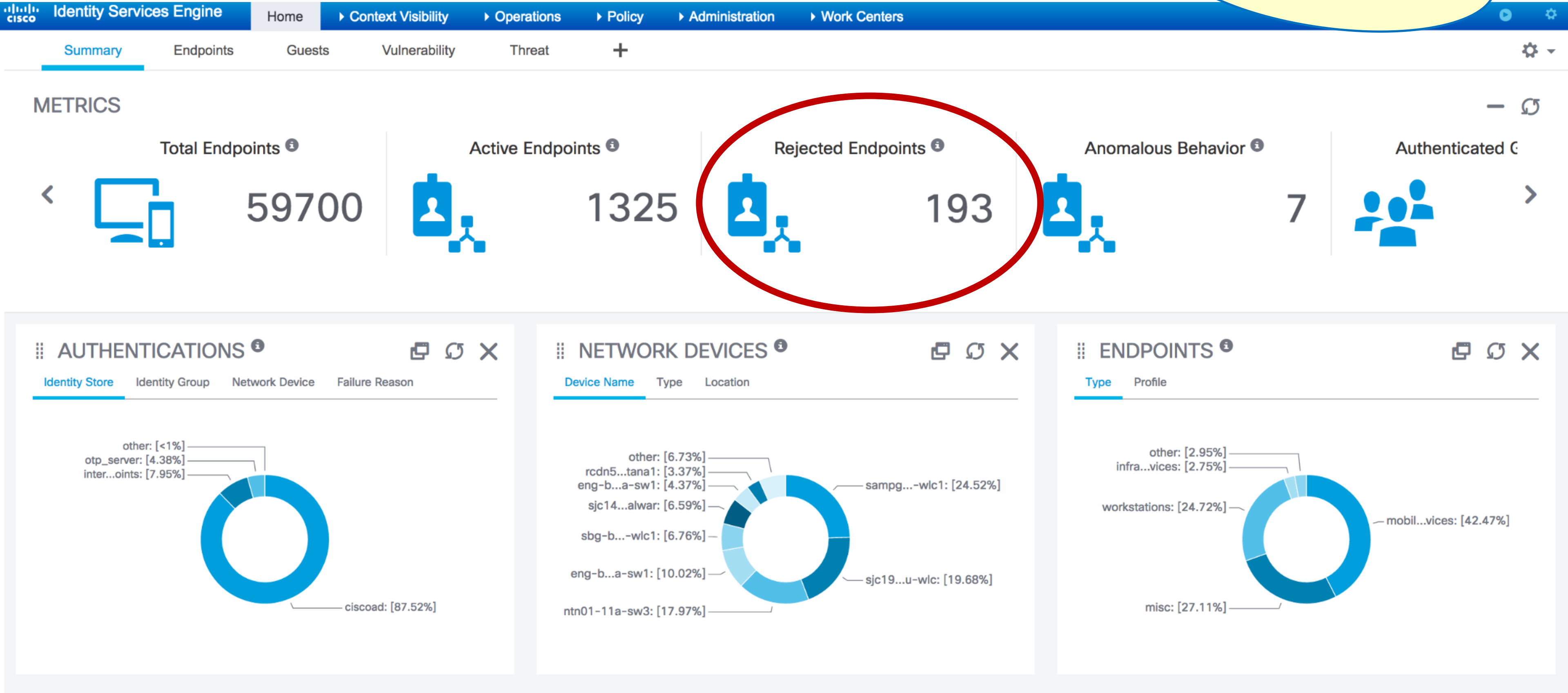


Identity Services Engine
Misconfigured Supplicants 21
Misconfigured Network Devices 10
RADIUS Drops 521
Client Stopped Responding 6716
Repeat Counter 19052
Endpoint Debug...
Modify Collection Filters...
Bypass Suppression Filtering for 1 hour
Settings...
Global Settings...
About Adobe Flash Player 11.7.700.224...
Right Click

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	i		0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890	i		11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
					B8:78:2E:60:7F:14	Apple-iDevice	
					CC:78:5F:43:97:71	[illegible]	
					F0:CB:A1:75:31:4D	[illegible]	
					F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
					F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
					00:1E:65:D6:93:E2		WNBU-WLC1
					0C:77:1A:9A:F6:73	Apple-iPhone	

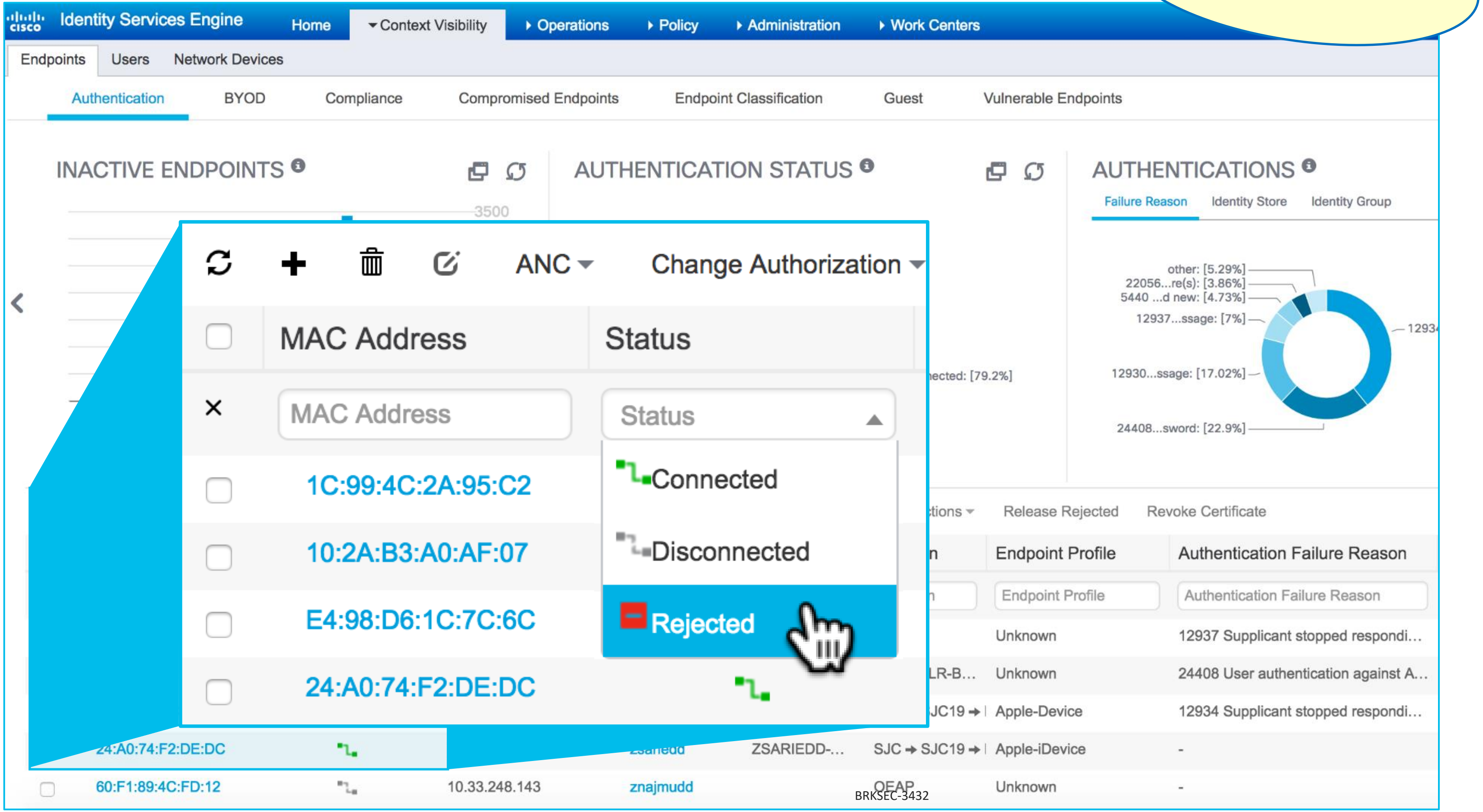
Visibility into Reject Endpoints!

ISE 2.2!



Releasing Rejected Endpoints

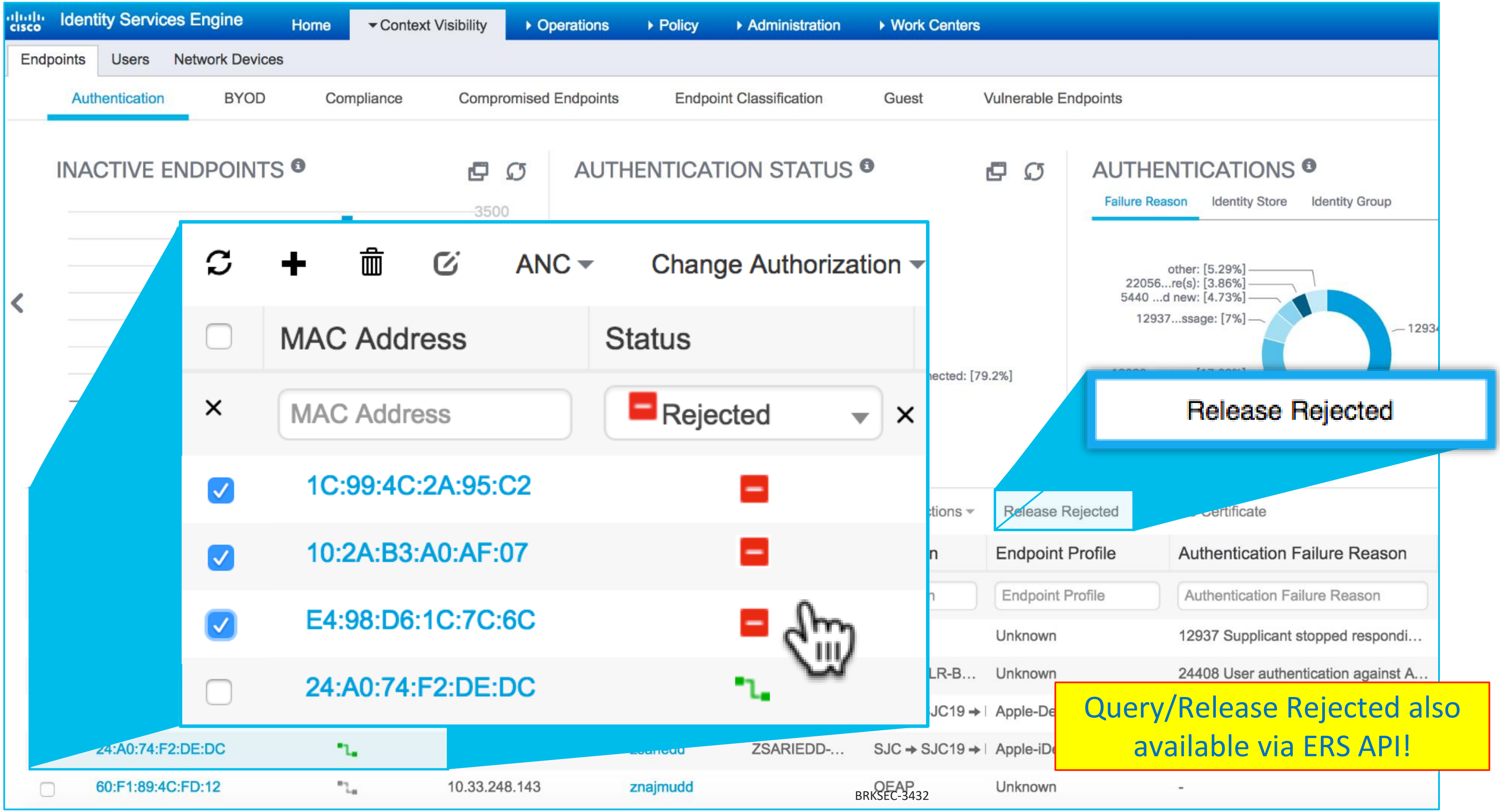
ISE 2.2!



□	MAC Address	Status
×	MAC Address	Status ▲
□	1C:99:4C:2A:95:C2	
□	10:2A:B3:A0:AF:07	
□	E4:98:D6:1C:7C:6C	
□	24:A0:74:F2:DE:DC	

					n	Endpoint Profile	Authentication Failure Reason
						Unknown	12937 Supplicant stopped respondi…
					LR-B…	Unknown	24408 User authentication against A…
					JC19 →	Apple-Device	12934 Supplicant stopped respondi…
24:A0:74:F2:DE:DC			zsariedd	ZSARIEDD-…	SJC → SJC19 →	Apple-iDevice	-
60:F1:89:4C:FD:12		10.33.248.143	znajmudd		OEAP	Unknown	-

Releasing Rejected Endpoints



☐	MAC Address	Status
×	MAC Address	🟥 Rejected ×
☑	1C:99:4C:2A:95:C2	🟥
☑	10:2A:B3:A0:AF:07	🟥
☑	E4:98:D6:1C:7C:6C	🟥
☐	24:A0:74:F2:DE:DC	⮓

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason
						Unknown	12937 Supplicant stopped respondi...
					...LR-B...	Unknown	24408 User authentication against A...
					...JC19 →	Apple-De...	
24:A0:74:F2:DE:DC	⮓		...zsariedd	ZSARIEDD-...	SJC → SJC19 →	Apple-iD...	
☐ 60:F1:89:4C:FD:12	⮓	10.33.248.143	znajmudd	OEAP...		Unknown	-

Query/Release Rejected also available via ERS API!

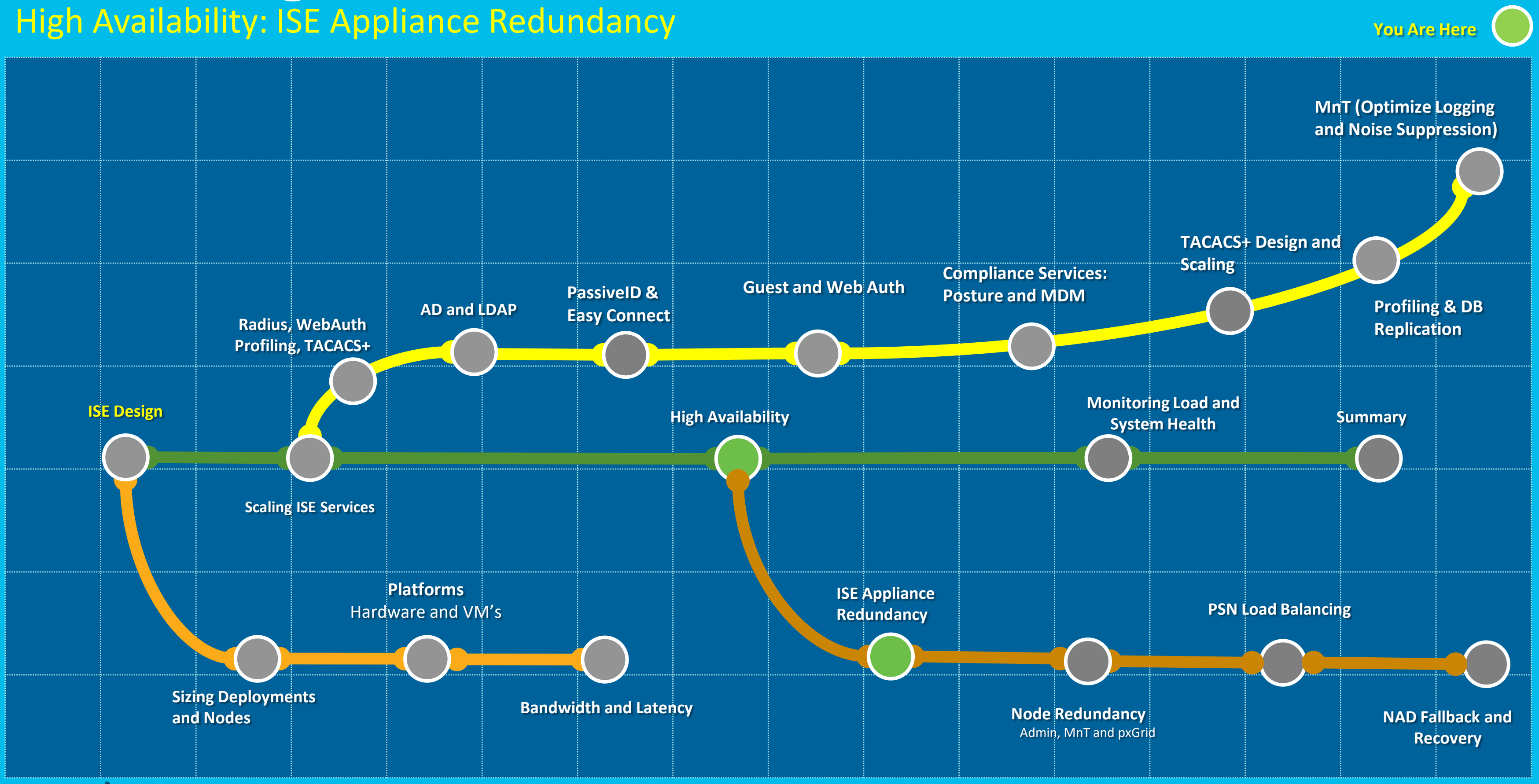
High Availability

High Availability Agenda

- ISE Appliance Redundancy
- ISE Node Redundancy
  - Administration Nodes
  - Monitoring Nodes
  - pxGrid Nodes
- HA for Certificate Services
- Policy Service Node Redundancy
  - Load Balancing
  - Non-LB Options
- NAD Fallback and Recovery

Session Agenda

High Availability: ISE Appliance Redundancy


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
PSN Load Balancing
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Appliance Redundancy

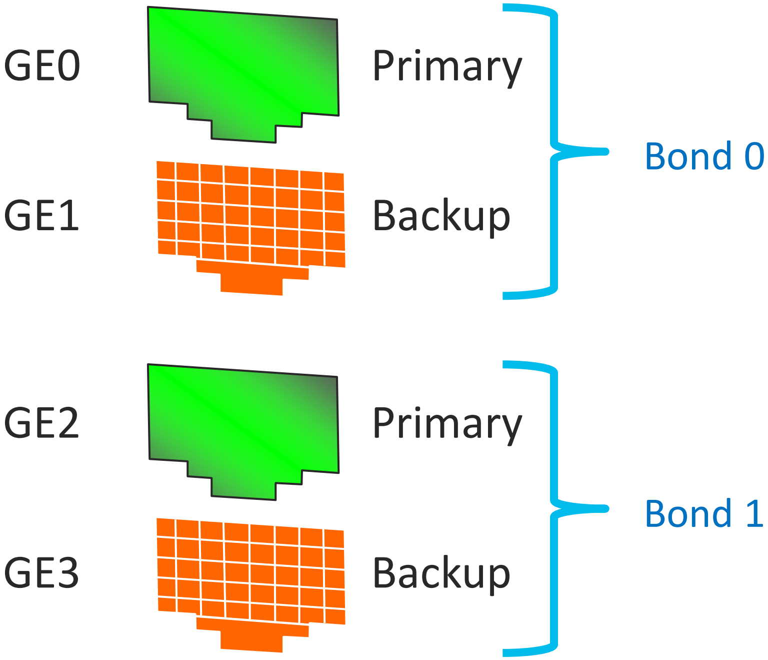
In-Box High Availability

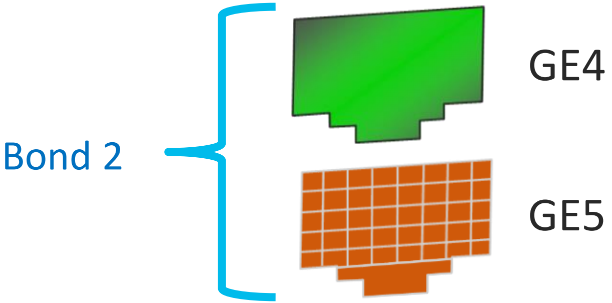
Platform	SNS-3615 (36x5 Small)	SNS-3655 (36x5 Medium)	SNS-3695 (36x5 Large)
Drive Redundancy	**No** (1) 600GB disk	**Yes** (4) 600-GB	**Yes** (8) 600-GB
Controller Redundancy	**No**	**Yes** Level 10 Cisco 12G SAS Modular RAID	**Yes** Level 10 Cisco 12G SAS Modular RAID
Ethernet Redundancy	**Yes*** 2 X 10Gbase-T 4 x 1GBase-T Up to 3 bonded NICs	**Yes*** 2 X 10Gbase-T 4 x 1GBase-T Up to 3 bonded NICs	**Yes*** 2 X 10Gbase-T 4 x 1GBase-T Up to 3 bonded NICs
Redundant Power	**No** (2nd PSU optional) UCSC-PSU1-770W	**Yes**	**Yes**

NIC Teaming

Network Card Redundancy

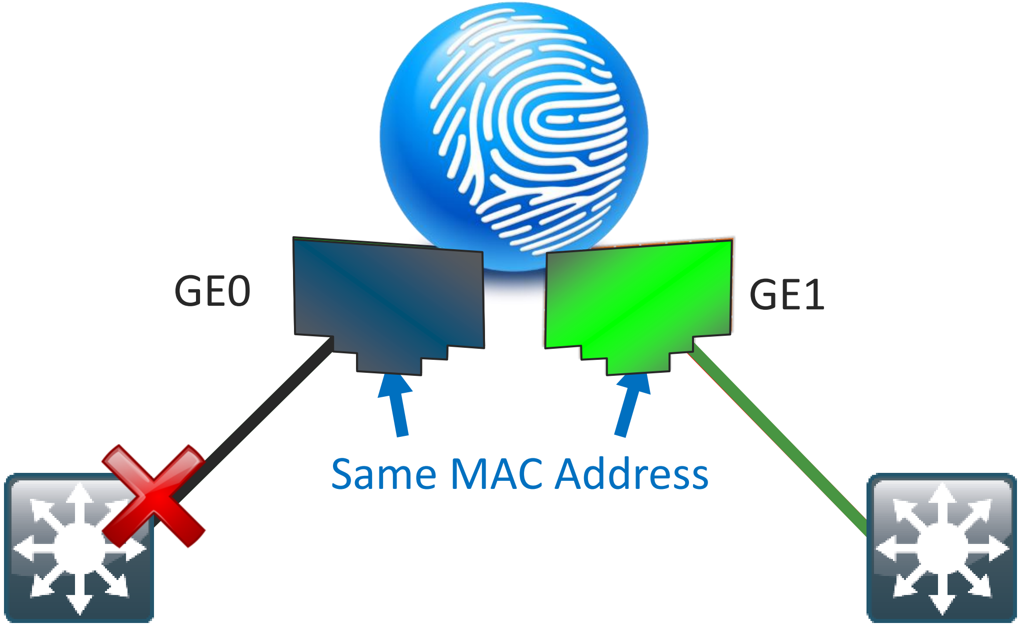
- For Redundancy only–NOT for increasing bandwidth.
- Up to (3) bonds in ISE 2.1
- Bonded Interfaces Preset–Non-Configurable





NIC Teaming Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over

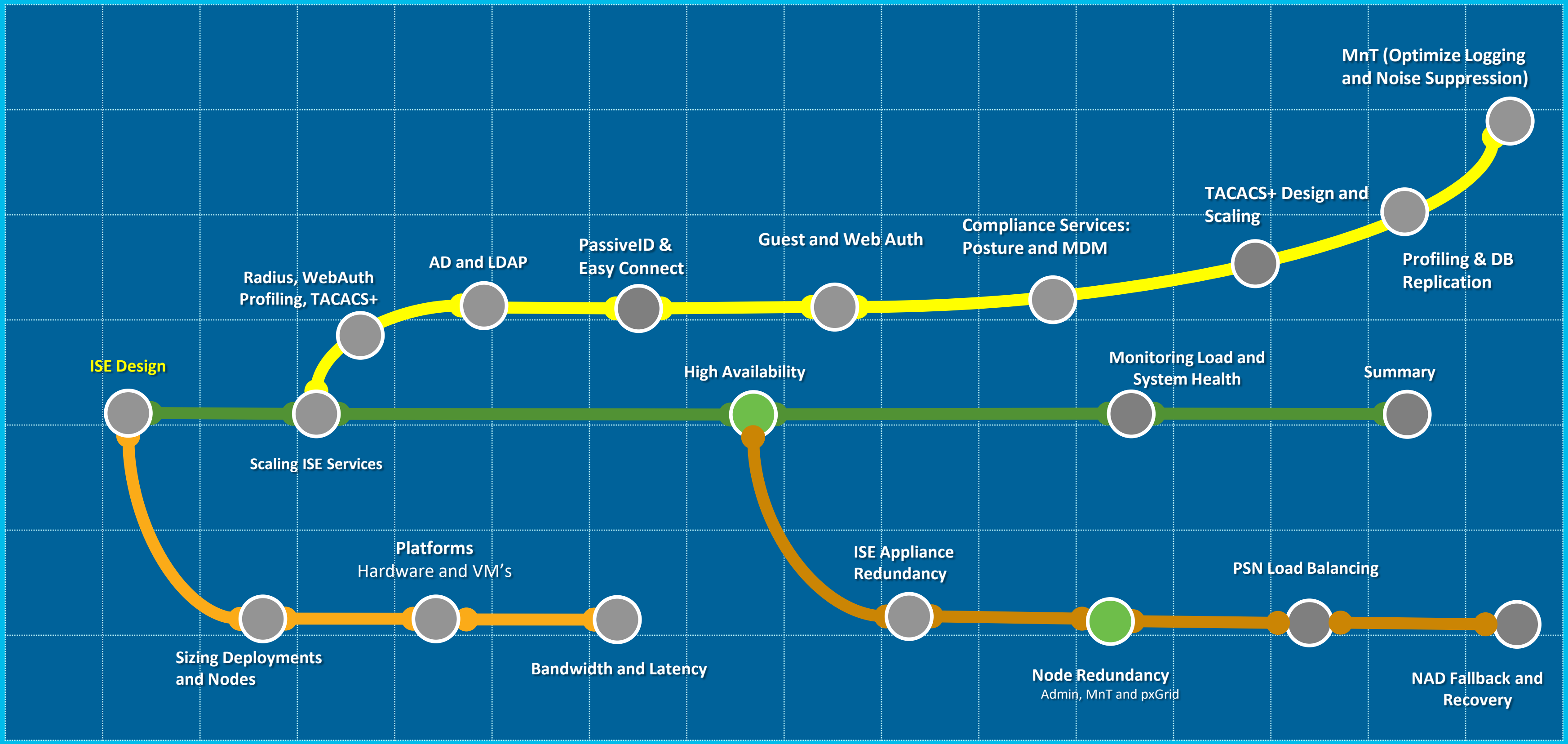


- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

Session Agenda

Node Redundancy: Admin, MnT and pxGrid

You Are Here



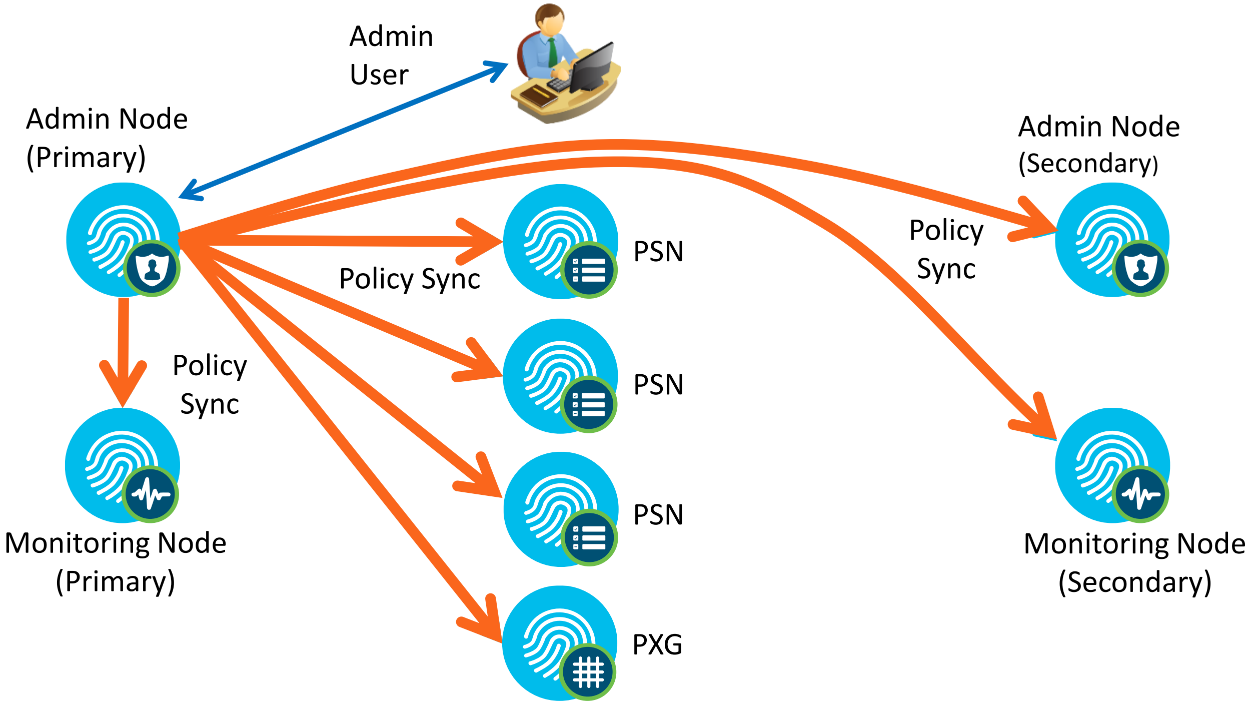
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

Admin Node HA and Synchronization

PAN Steady State Operation

- Changes made to Primary Administration DB are automatically synced to all nodes.

- Maximum two PAN nodes per deployment
- Active / Standby

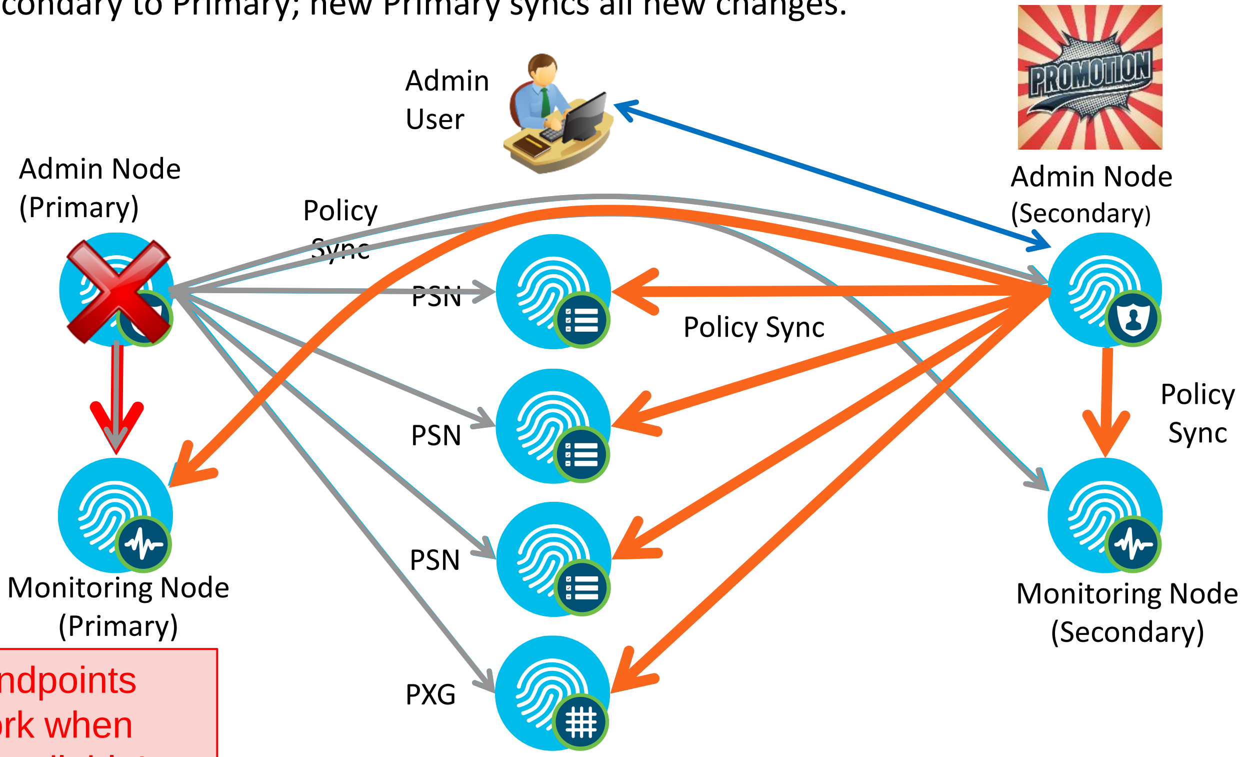


Admin Node HA and Synchronization

Primary PAN Outage and Recovery

- Prior to ISE 1.4 or without auto failover, upon Primary PAN failure, admin user must connect to Secondary PAN and **manually promote** Secondary to Primary; new Primary syncs all new changes.
- PSNs buffer endpoint updates if Primary PAN unavailable; buffered updates sent once PAN available.

Promoting Secondary Admin may take 10-15 minutes before process is complete.



New Guest Users or Registered Endpoints cannot be added/connect to network when Primary Administration node is unavailable!

Policy Service Survivability When Admin Down/Unreachable

Which User Services Are Available if Primary Admin Node Is Unavailable?

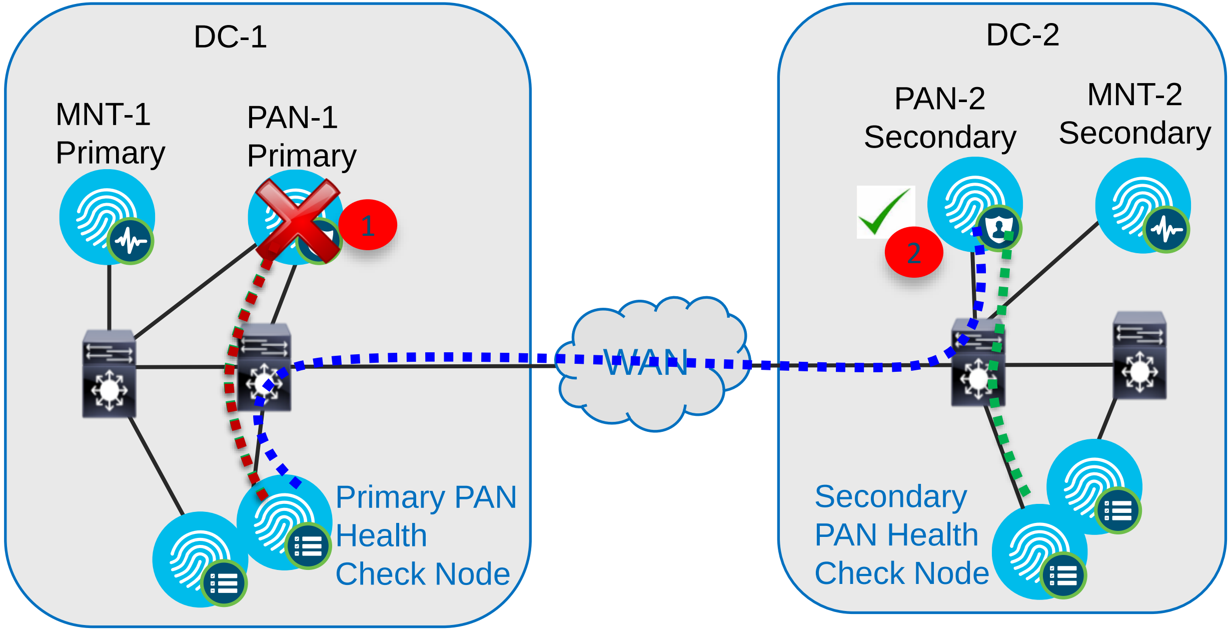
Service	Use case	Works (Y / N)
RADIUS Auth	Generally all RADIUS auth should continue provided access to ID stores	Y
Guest	All existing guests can be authenticated, but new guests, self-registered guests, or guest flows relying on device registration will fail.	N
Profiler	Previously profiled endpoints can be authenticated with existing profile. New endpoints or updates to existing profile attributes received by owner should apply, but not profile data received by PSN in foreign node group.	Y
Posture	Provisioning/Assessment work, but Posture Lease unable to fetch timer.	Y
Device Reg	Device Registration fails if unable to update endpoint record in central db.	N
BYOD/NSP	BYOD/NSP relies on device registration. Additionally, any provisioned certificate cannot be saved to database.	N
MDM	MDM fails on update of endpoint record	N
CA/Cert Services	See BYOD/NSP use case; certificates can be issued but will not be saved and thus fail. OCSP functions using last replicated version of database	N
pxGrid	Clients that are already authorized for a topic and connected to controller will continue to operate, but new registrations and connections will fail.	N
TACACS+	TACACS+ requests can be locally processed per ID store availability.	Y

Automatic PAN Switchover

Introduced ISE 1.4

Don’t forget, after switchover admin must connect to PAN-2 for ISE management!

- Primary PAN (PAN-1) down or network link down.
- If Health Check Node unable to reach PAN-1 but can reach PAN-2
  → trigger failover
- Secondary PAN (PAN-2) is promoted by Health Check Node
- PAN-2 becomes Primary and takes over PSN replication.

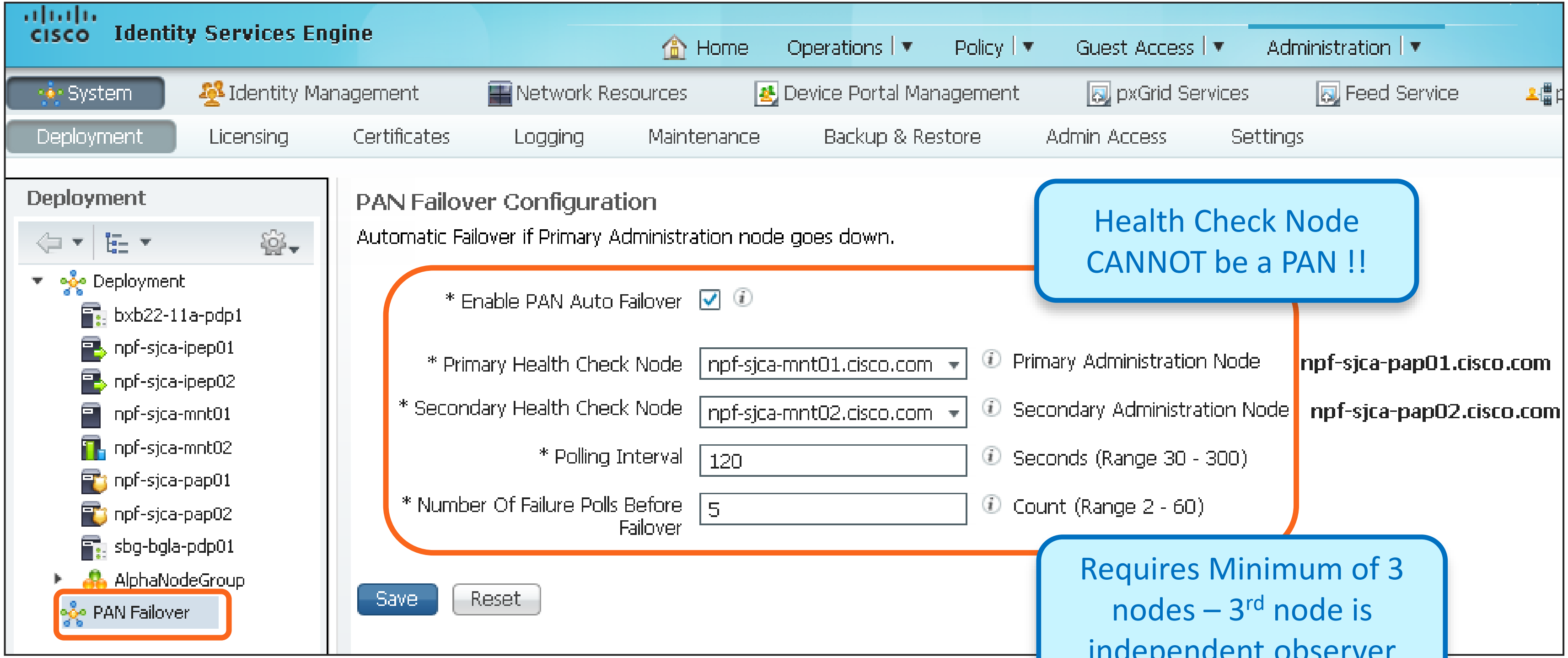


Note: Switchover is NOT immediate. Total time based on polling intervals and promotion time. Expect ~15 - 30 minutes.

PAN Failover

Health Check Node Configuration

- Configuration using GUI only under Administration > System > Deployment > PAN Failover



PAN Failover Configuration

Automatic Failover if Primary Administration node goes down.

* Enable PAN Auto Failover ☑

* Primary Health Check Node: npf-sjca-mnt01.cisco.com — Primary Administration Node npf-sjca-pap01.cisco.com

* Secondary Health Check Node: npf-sjca-mnt02.cisco.com — Secondary Administration Node npf-sjca-pap02.cisco.com

* Polling Interval: 120 — Seconds (Range 30 - 300)

* Number Of Failure Polls Before Failover: 5 — Count (Range 2 - 60)

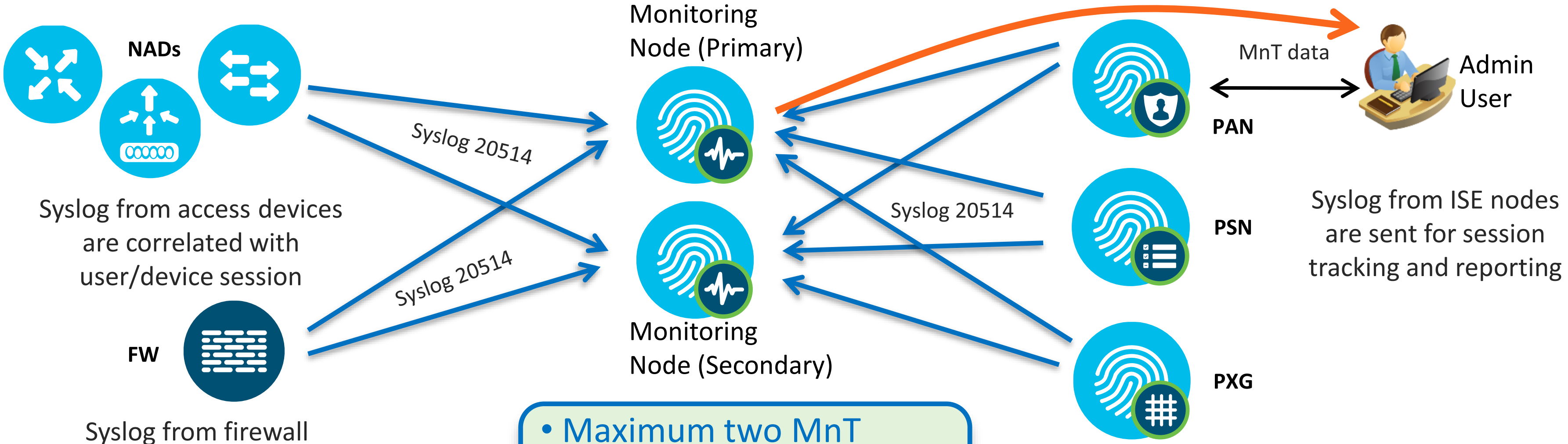
Health Check Node CANNOT be a PAN !!

Requires Minimum of 3 nodes – 3rd node is independent observer

HA for Monitoring and Troubleshooting

Steady State Operation

- MnT nodes concurrently receive logging from PAN, PSN, NAD, and ASA
- PAN retrieves log/report data from Primary MnT node when available



Syslog from access devices are correlated with user/device session

Syslog from ISE nodes are sent for session tracking and reporting

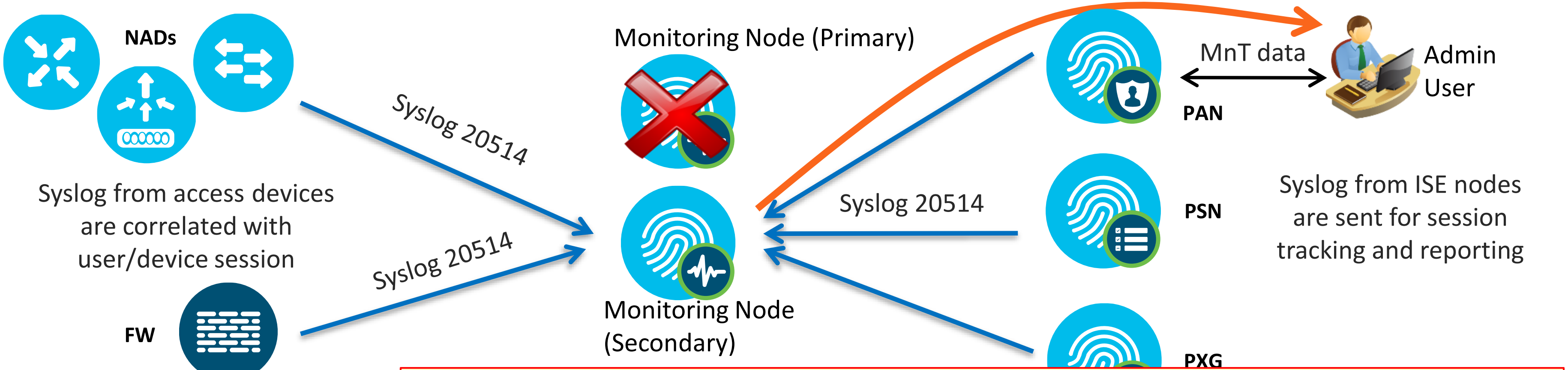
Syslog from firewall (or other user logging device) is correlated with guest session for activity logging

- Maximum two MnT nodes per deployment
- Active / Active

HA for Monitoring and Troubleshooting

Primary MnT Outage and Recovery

- Upon MnT node failure, PAN, PSN, NAD, and ASA continue to send logs to remaining MnT node
- PAN auto-detects Active MnT failure and retrieves log/report data from Secondary MnT node.
- Full failover to Secondary MnT may take from 5-15 min depending on type of failure.



Syslog from access devices are correlated with user/device session

Syslog from ISE nodes are sent for session tracking and reporting

Syslog from firewall (or other user logging device) is correlated with guest session for activity logging

- PSN logs are not locally buffered when MnT down unless use TCP/Secure syslog.
- Log DB is not synced between MnT nodes.
- Upon return to service, recovered MnT node will <u>not</u> include data logged during outage
- Backup/Restore required to re-sync MnT database

ISE 2.6+: Rabbit MQ

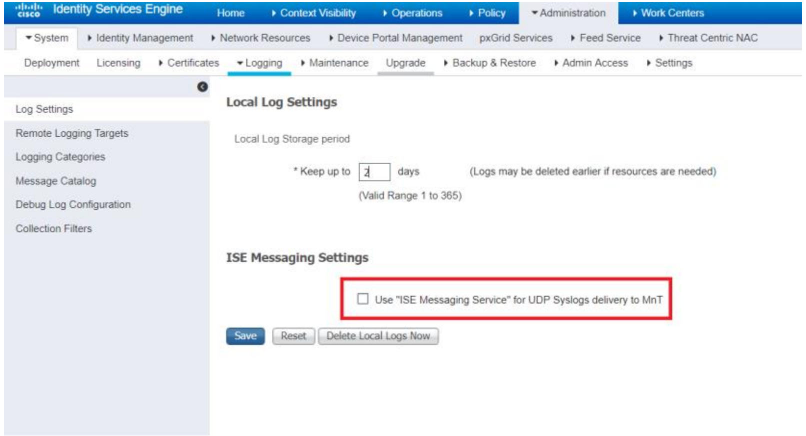
A new type of architecture for ISE messaging services

- Move forward in terms of robustness, reliability , Scalability and code quality
- Introduced in 2.6 for Secure Syslog (WAN survivability)

ISE 2.7: Syslogs over ISE Messaging

WAN survivability and securing Syslog using Rabbit MQ

- Syslogs can use secure ISE Messaging instead of UDP
- Messages buffered on PSN while MNT is down
  - Buffer is 4GB otherwise overflow, 200 per/sec 1kb message, 1.5 hrs filled
- Max TPS ~5000



Local Log Settings

Local Log Storage period

* Keep up to 2 days (Logs may be deleted earlier if resources are needed)

(Valid Range 1 to 365)

ISE Messaging Settings

☐ Use "ISE Messaging Service" for UDP Syslogs delivery to MnT

HA for pxGrid v2 (ISE 2.3+)

Steady State

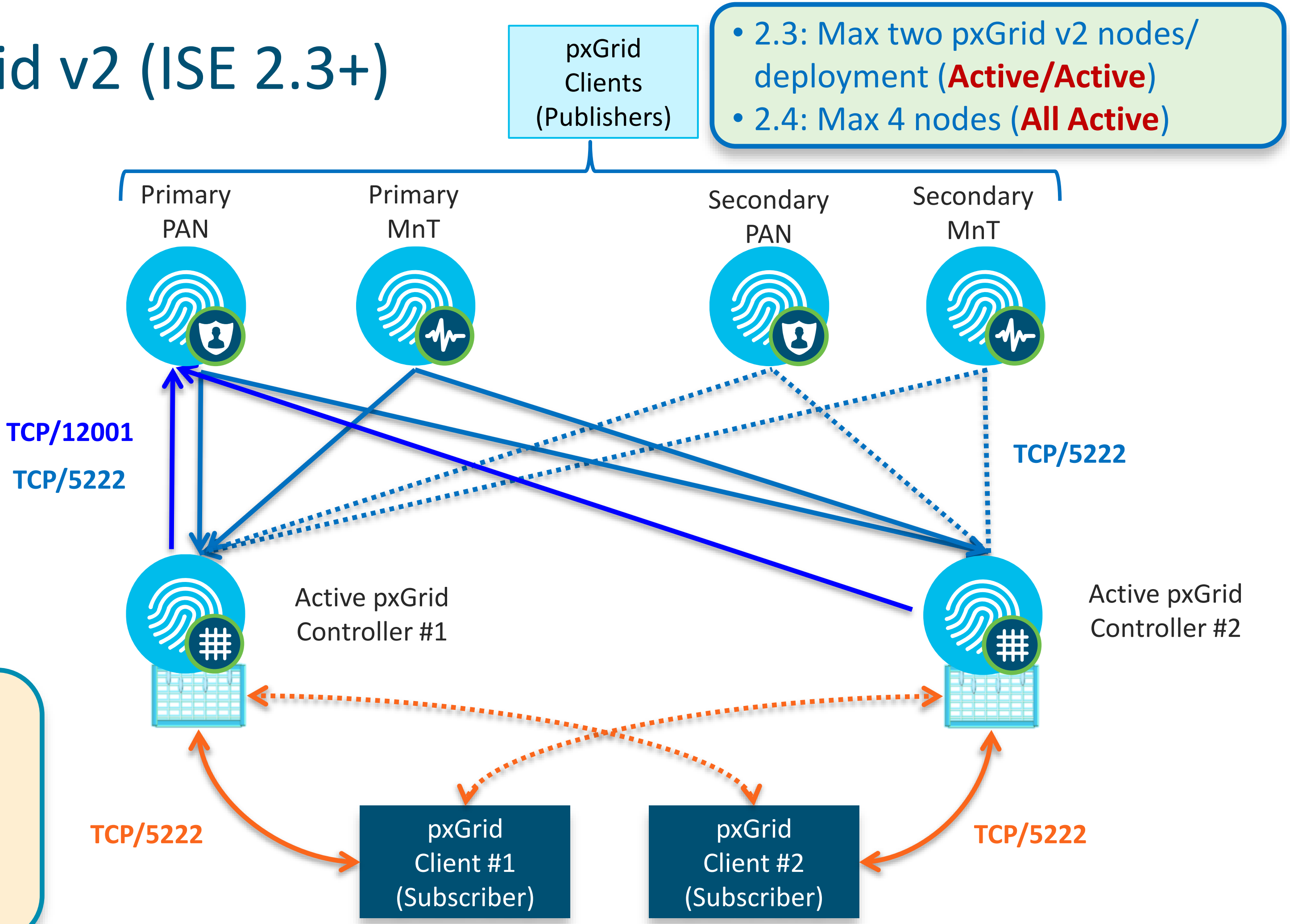
- 2.3: Max two pxGrid v2 nodes/ deployment (**Active/Active**)
- 2.4: Max 4 nodes (**All Active**)

PAN Publisher Topics:

- Controller Admin
- TrustSec/SGA
- Endpoint Profile

MnT Publisher Topics:

- Session Directory
- Identity Group
- ANC (EPS)



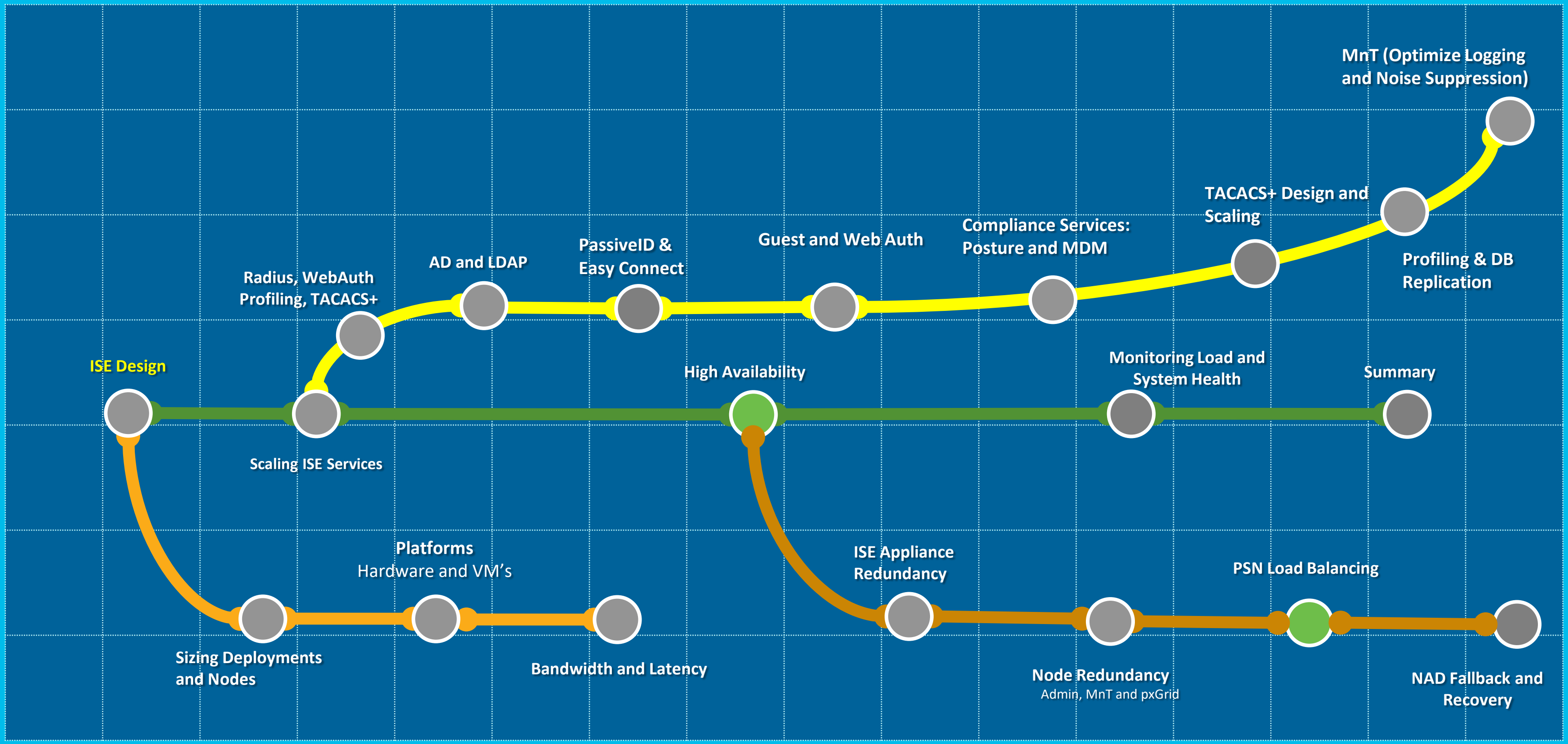
pxGrid Clients (Publishers)
Primary PAN
Primary MnT
Secondary PAN
Secondary MnT
TCP/12001
TCP/5222
TCP/5222
Active pxGrid Controller #1
Active pxGrid Controller #2
TCP/5222
TCP/5222
pxGrid Client #1 (Subscriber)
pxGrid Client #2 (Subscriber)

- pxGrid clients can be configured with multiple servers for redundancy.
- Clients connect to single active controller for given domain

Session Agenda

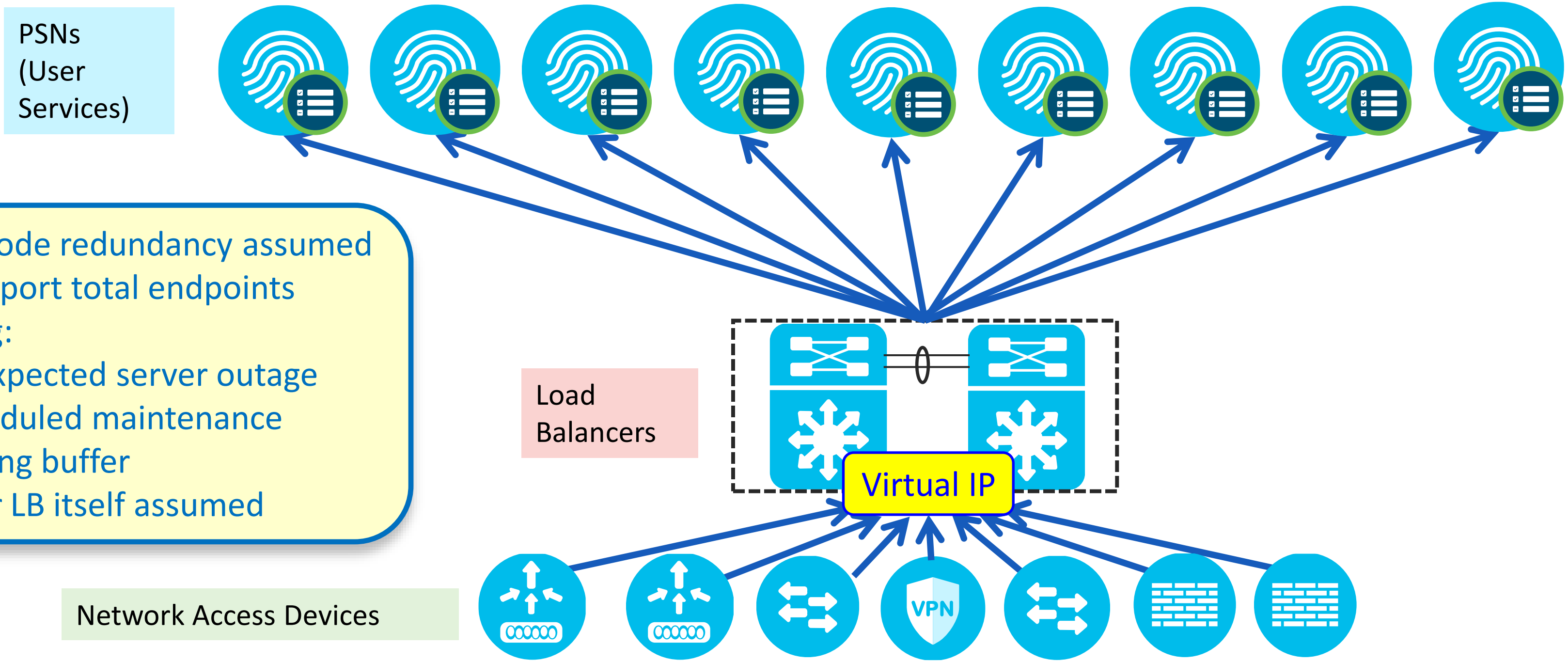
PSN Load Balancing

You Are Here


MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Load Balancing RADIUS, Web, and Profiling Services

- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS and TACACS+ AAA requests to LB virtual IP.



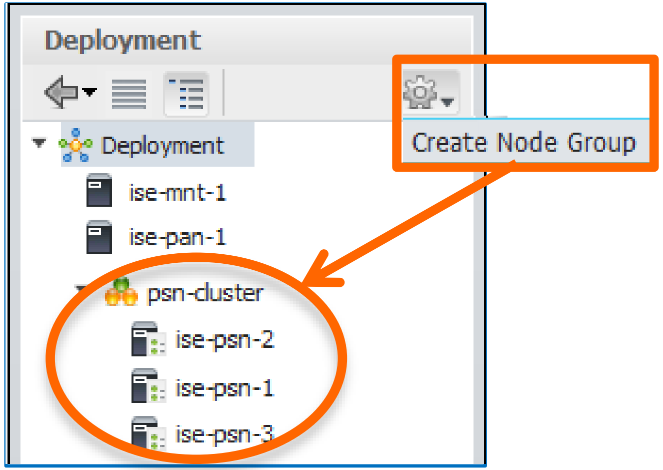
- N+1 node redundancy assumed to support total endpoints during:
  - Unexpected server outage
  - Scheduled maintenance
  - Scaling buffer
- HA for LB itself assumed

Configure Node Groups for LB Cluster

Place all PSNs in LB Cluster in Same Node Group

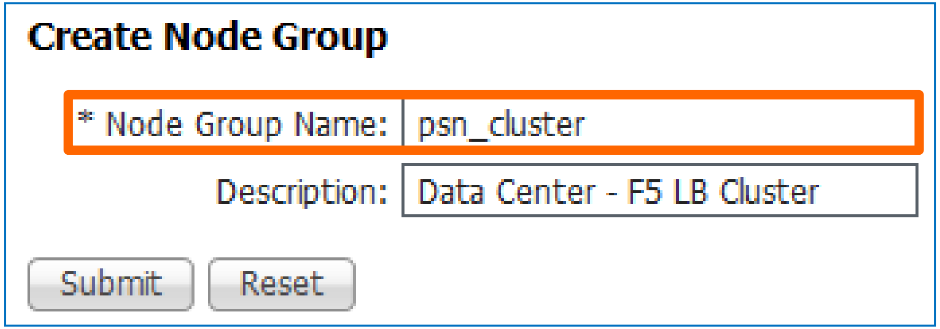
- Administration > System > Deployment

1) Create node group



- Node group members can be L2 or L3
- Multicast not required

2) Assign name (and multicast address if ISE 1.2)



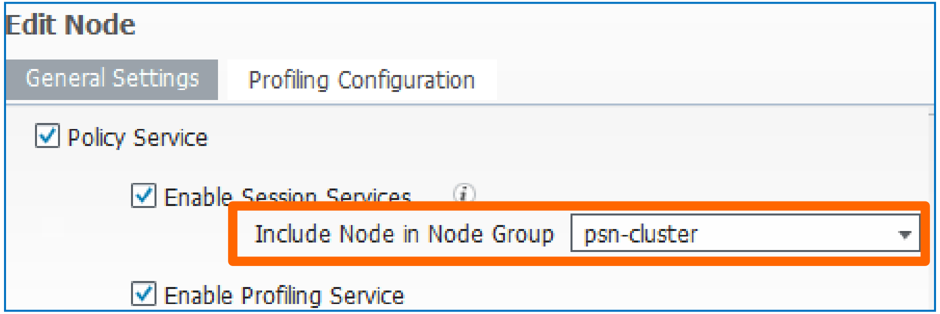
Create Node Group

* Node Group Name: psn_cluster

Description: Data Center - F5 LB Cluster

Submit Reset

3) Add individual PSNs to node group



Edit Node

General Settings | Profiling Configuration

☑ Policy Service

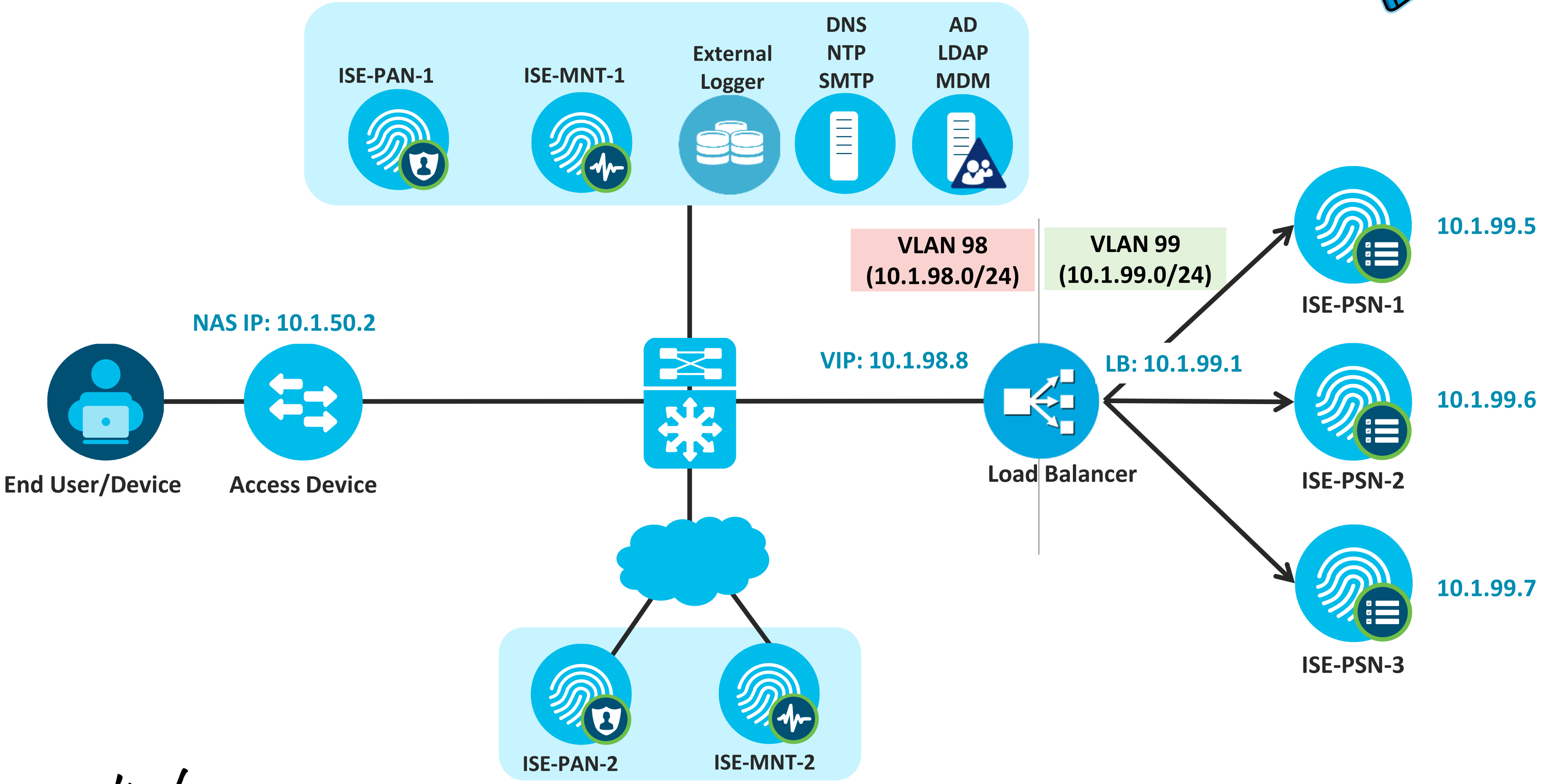
☑ Enable Session Services

Include Node in Node Group: psn-cluster

☑ Enable Profiling Service

High-Level Load Balancing Diagram

For Your Reference

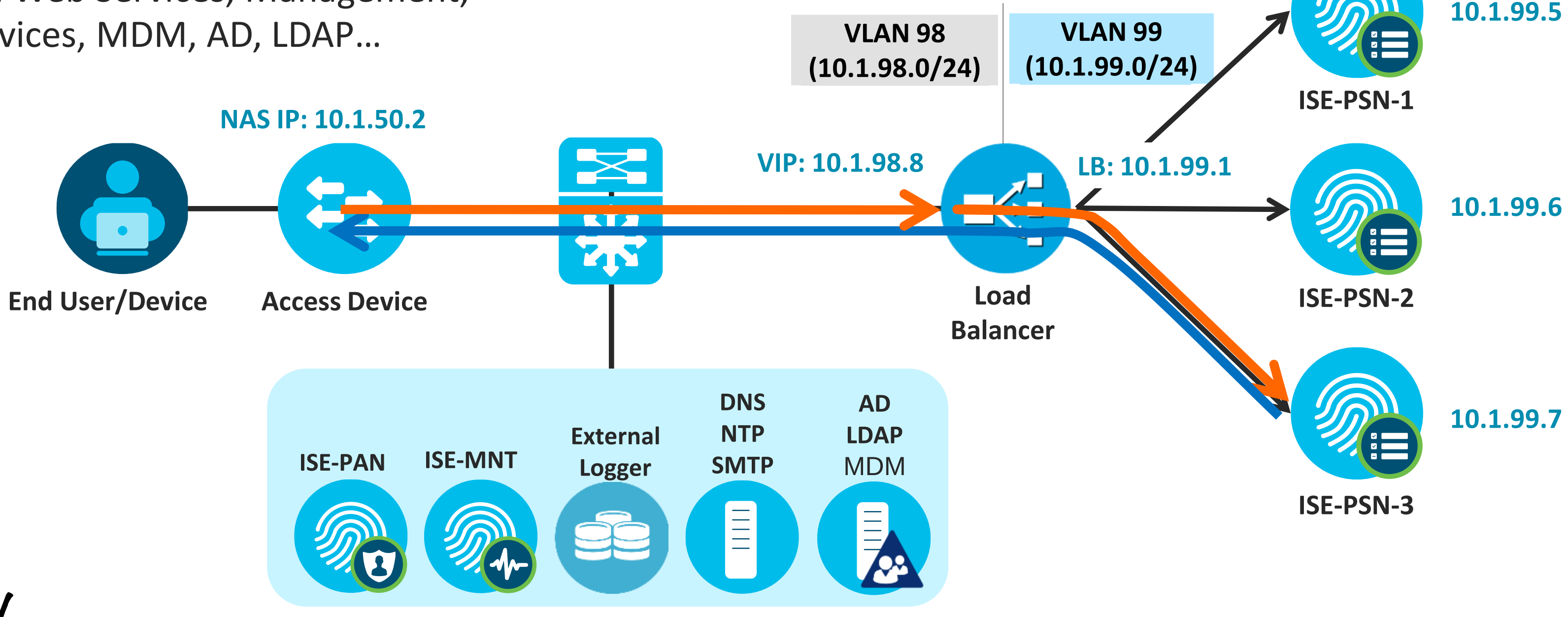


Traffic Flow—Fully Inline: Physical Separation

Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

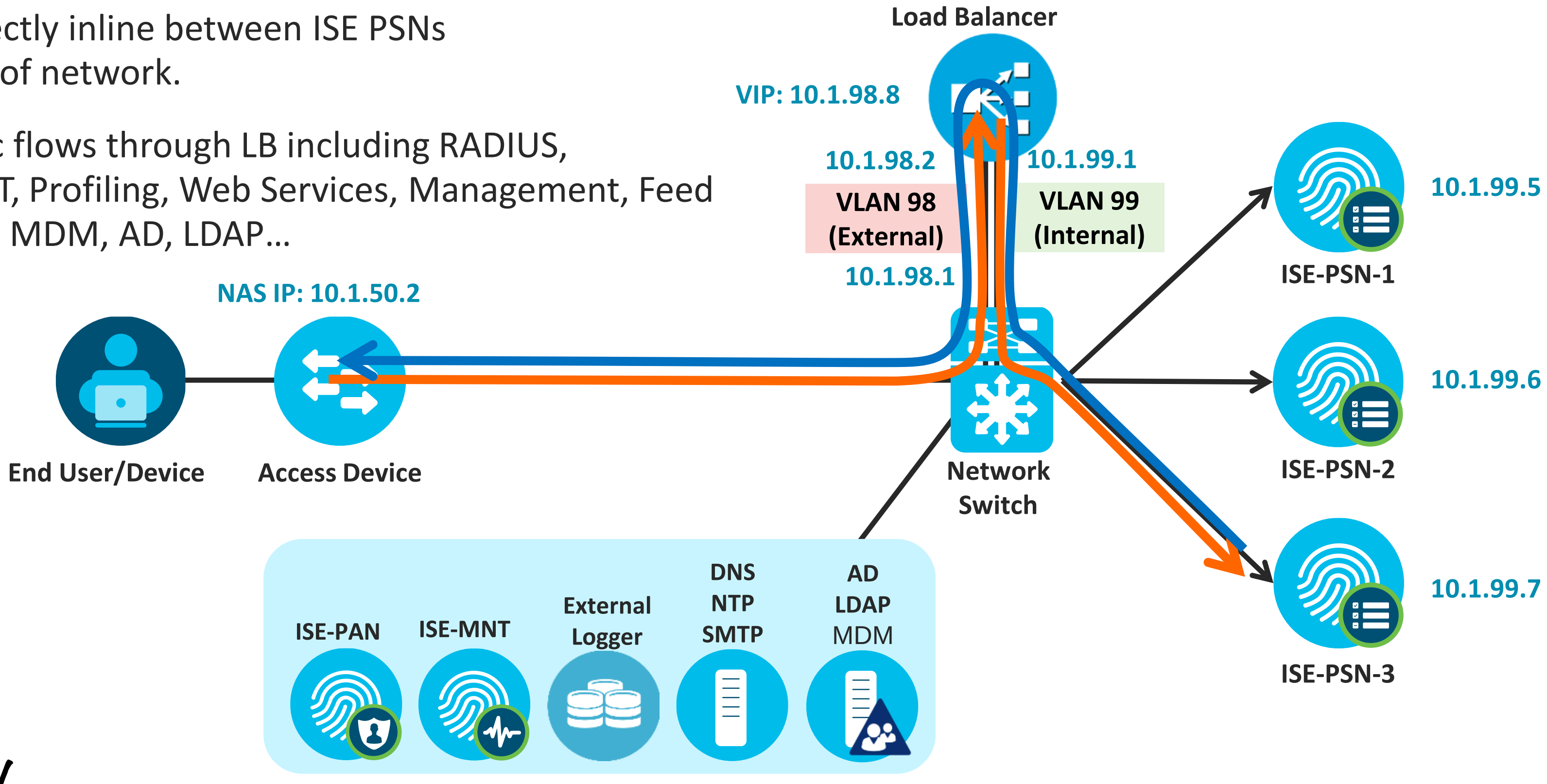
- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…



Traffic Flow—Fully Inline: VLAN Separation

Logical Network Separation Using Single LB Interface and VLAN Trunking

- LB is directly inline between ISE PSNs and rest of network.
- All traffic flows through LB including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…

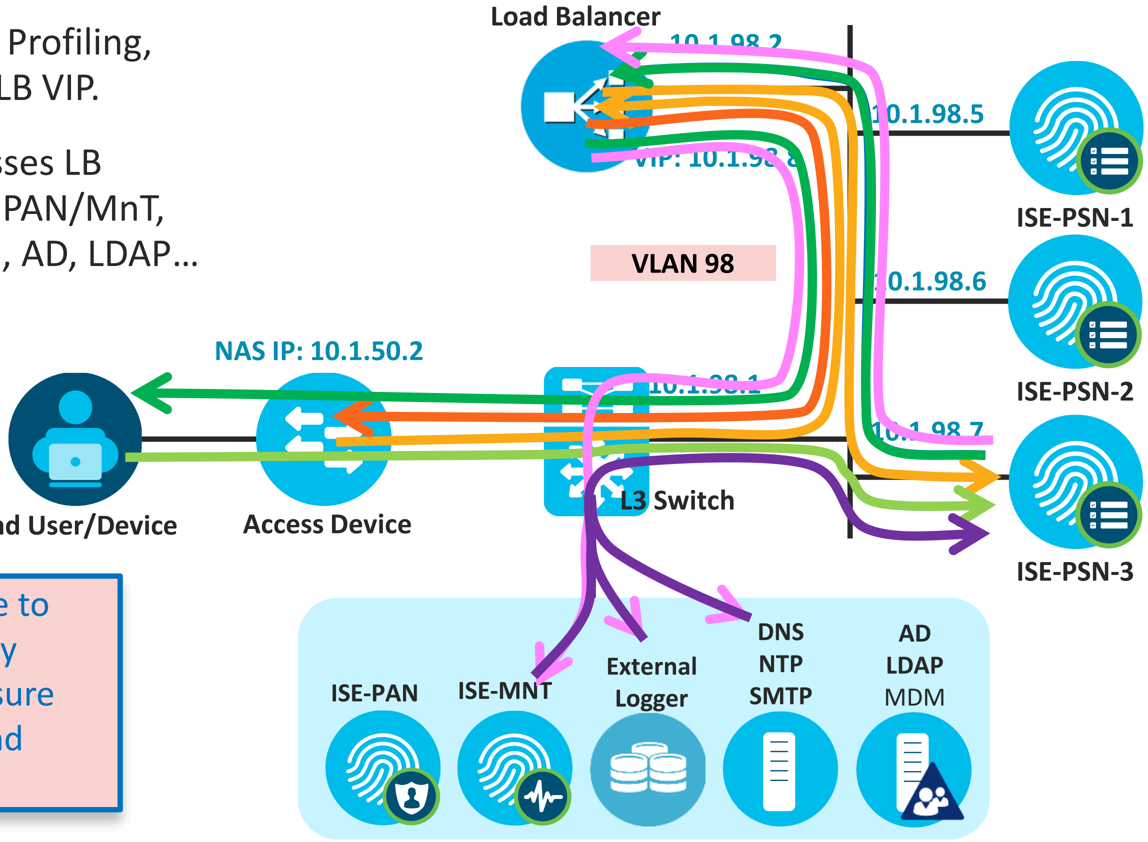


Partially Inline: Layer 2/Same VLAN (One PSN Interface)

Direct PSN Connections to LB and Rest of Network

- All inbound LB traffic such RADIUS, Profiling, and directed Web Services sent to LB VIP.
- Other inbound non-LB traffic bypasses LB including redirected Web Services, PAN/MnT, Management, Feed Services, MDM, AD, LDAP…
- All outbound traffic from PSNs sent to LB as DFGW.
- LB must be configured to allow Asymmetric traffic

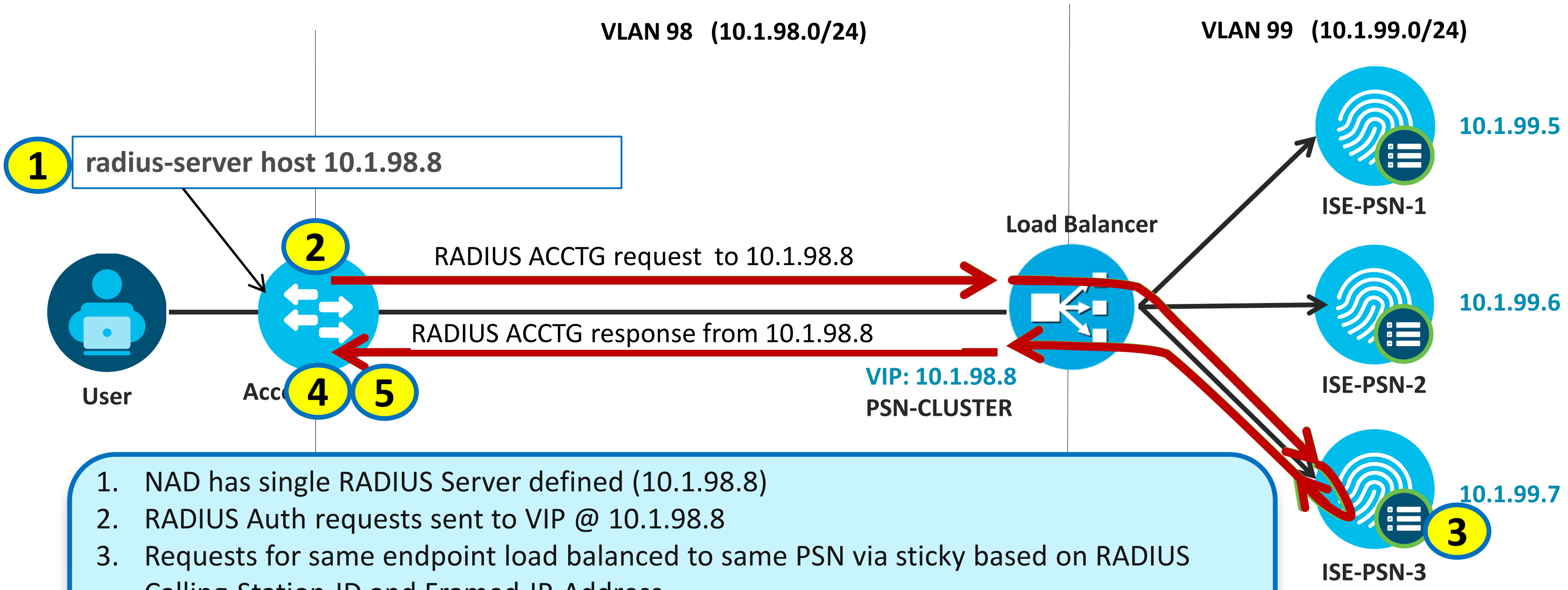
Generally NOT RECOMMENDED due to traffic flow complexity—must fully understand path of each flow to ensure proper handling by routing, LB, and end stations.



Load Balancing RADIUS

Load Balancing RADIUS

Sample Flow

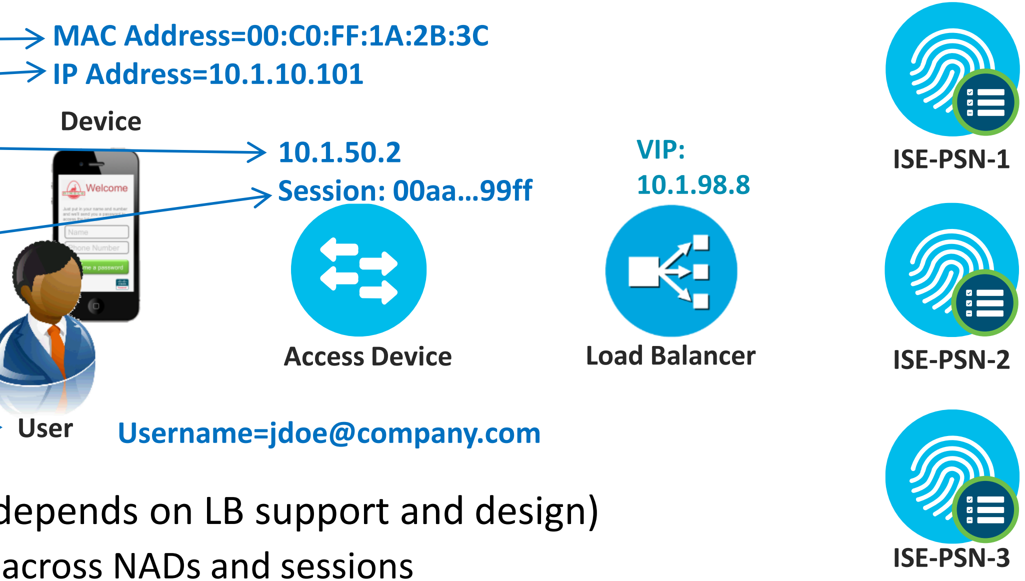


1. NAD has single RADIUS Server defined (10.1.98.8)
2. RADIUS Auth requests sent to VIP @ 10.1.98.8
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS response received from VIP @ 10.1.98.8
   (originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. RADIUS Accounting sent to/from same PSN based on sticky

Load Balancer Persistence (Stickiness) Guidelines

Persistence Attributes

- Common RADIUS Sticky Attributes
  - **Client Address**
    - Calling-Station-ID
    - Framed-IP-Address
  - **NAD Address**
    - NAS-IP-Address
    - Source IP Address
  - **Session ID**
    - RADIUS Session ID
    - Cisco Audit Session ID
  - **Username**



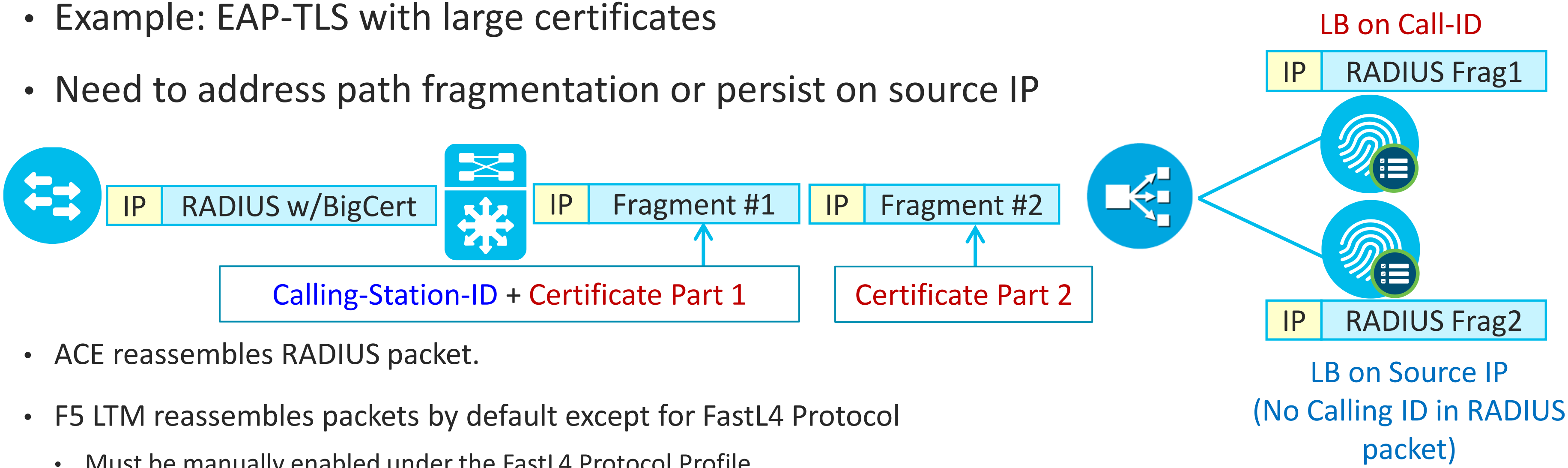
- Best Practice Recommendations (depends on LB support and design)
  1. Calling-Station-ID for persistence across NADs and sessions
  2. Source IP or NAS-IP-Address for persistence for all endpoints connected to same NAD
  3. Audit BRKSEC3432 for persistence across re-authentications

LB Fragmentation and Reassembly

Be aware of load balancers that do not reassemble RADIUS fragments!

Also watch for fragmented packets that are too small. LBs have min allowed frag size and will drop !!!

- Example: EAP-TLS with large certificates
- Need to address path fragmentation or persist on source IP

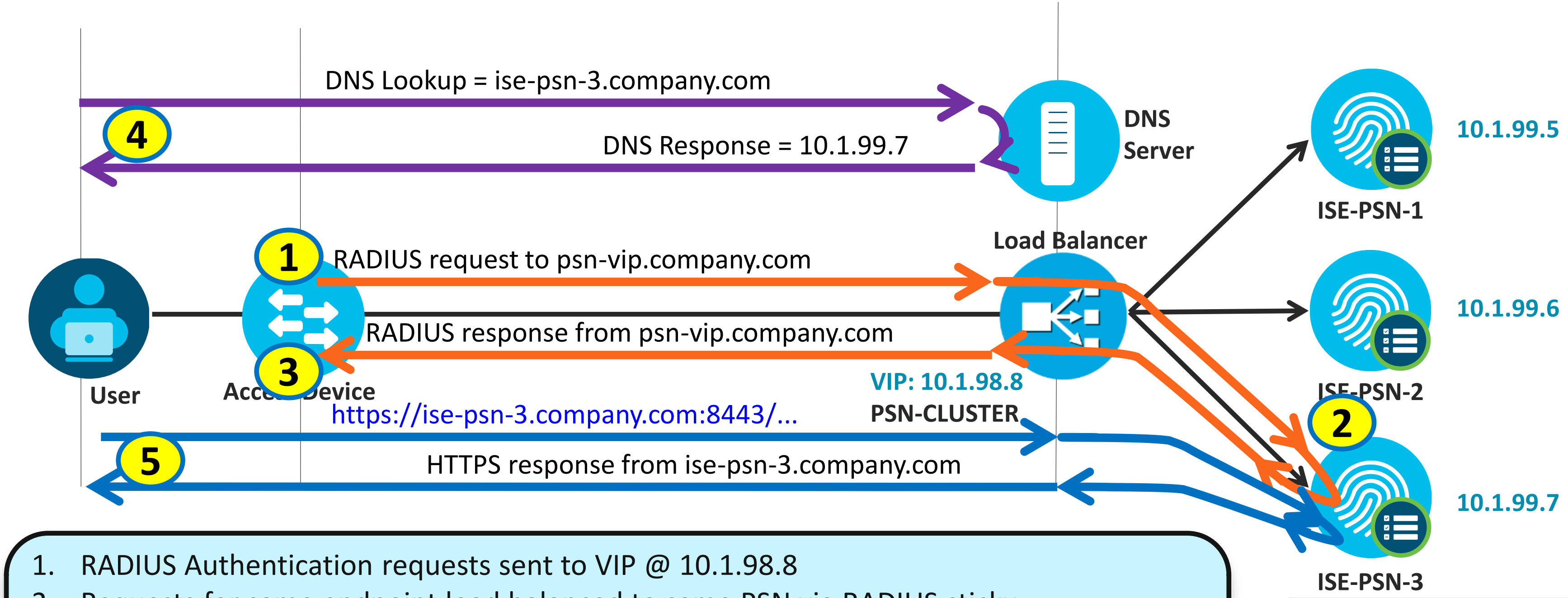


- ACE reassembles RADIUS packet.
- F5 LTM reassembles packets by default except for FastL4 Protocol
  - Must be manually enabled under the FastL4 Protocol Profile
- Citrix NetScaler fragmentation defect—Resolved in NetScaler 10.5 Build 50.10
  - Issue ID 429415 addresses fragmentation and the reassembly of large/jumbo frames

Load Balancing ISE Web Services

Load Balancing with URL-Redirection

URL Redirect Web Services: Hotspot/DRW, CWA, BYOD, Posture, MDM


DNS Lookup = ise-psn-3.company.com
4
DNS Response = 10.1.99.7
DNS Server
ISE-PSN-1
10.1.99.5
Load Balancer
1
RADIUS request to psn-vip.company.com
RADIUS response from psn-vip.company.com
3
User
Access Device
VIP: 10.1.98.8
PSN-CLUSTER
ISE-PSN-2
10.1.99.6
2
https://ise-psn-3.company.com:8443/...
5
HTTPS response from ise-psn-3.company.com
10.1.99.7
ISE-PSN-3

1. RADIUS Authentication requests sent to VIP @ 10.1.98.8
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorization received from VIP @ 10.1.98.8 (originated by ise-psn-3 @ 10.1.99.7 with URL Redirect to https://ise-psn-3.company.com:8443/...
4. Client browser redirected and resolves FQDN in URL to real server address.
5. User sends web request directly to same PSN that serviced RADIUS request.

ISE Certificate

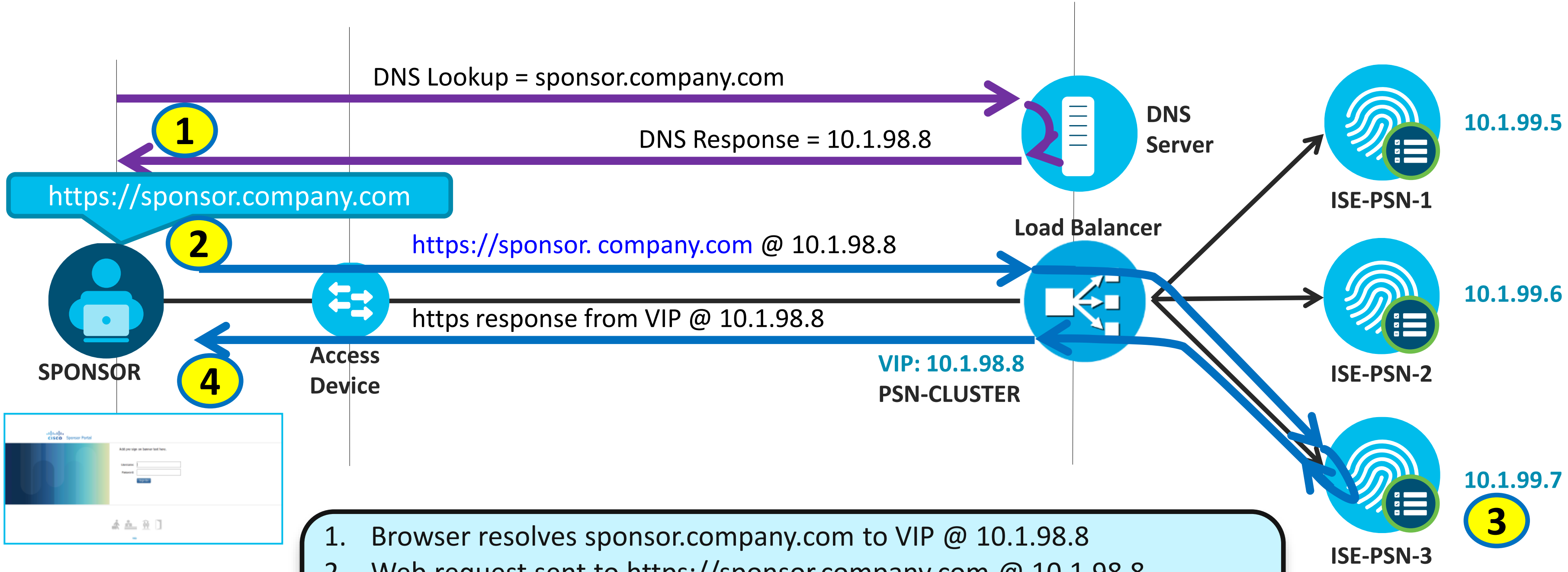
Subject CN =

ise-psn-3.company.com

Load Balancing Non-Redirected Web Services

For Your Reference

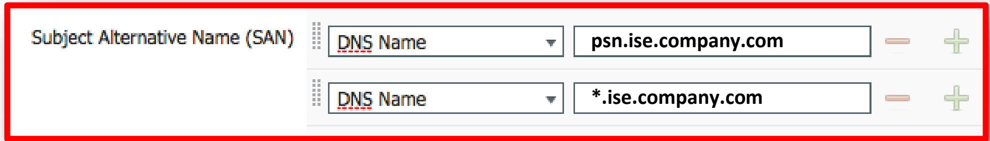
Direct Web Services: Sponsor, My Devices, LWA, OCSP



1. Browser resolves sponsor.company.com to VIP @ 10.1.98.8
2. Web request sent to https://sponsor.company.com @ 10.1.98.8
3. ACE load balances request to PSN based on IP or HTTP sticky
4. HTTPS response received from ise-psn-3 @ 10.1.99.7 → translated to VIP @ 10.1.98.8 when passes through LB.

“Universal Certs”

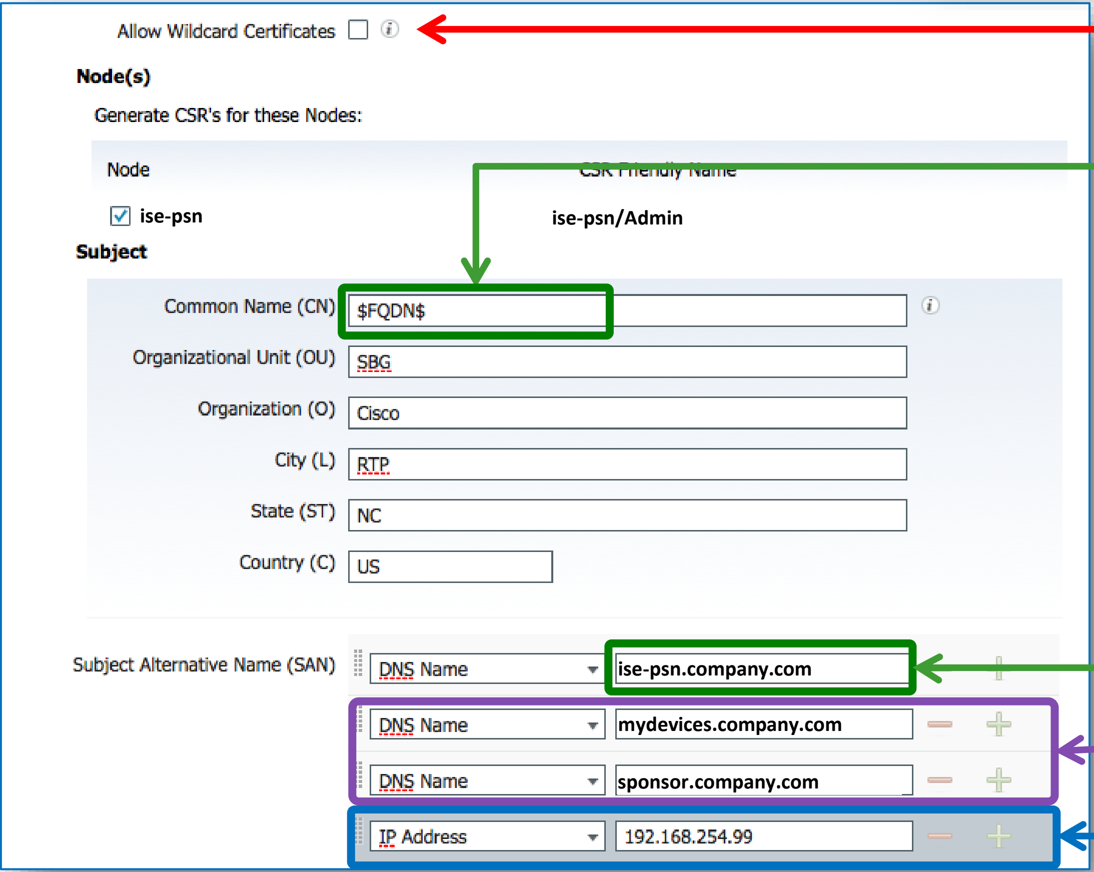
UCC or Wildcard SAN Certificates



Subject Alternative Name (SAN)

DNS Name	psn.ise.company.com
DNS Name	*.ise.company.com

Check box to use wildcards



Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise-psn	ise-psn/Admin

Subject

Common Name (CN)	$FQDN$
Organizational Unit (OU)	SBG
Organization (O)	Cisco
City (L)	RTP
State (ST)	NC
Country (C)	US

Subject Alternative Name (SAN)

DNS Name	ise-psn.company.com
DNS Name	mydevices.company.com
DNS Name	sponsor.company.com
IP Address	192.168.254.99

CN must also exist in SAN

Universal Cert options:

- UCC / Multi-SAN
- Wildcard SAN

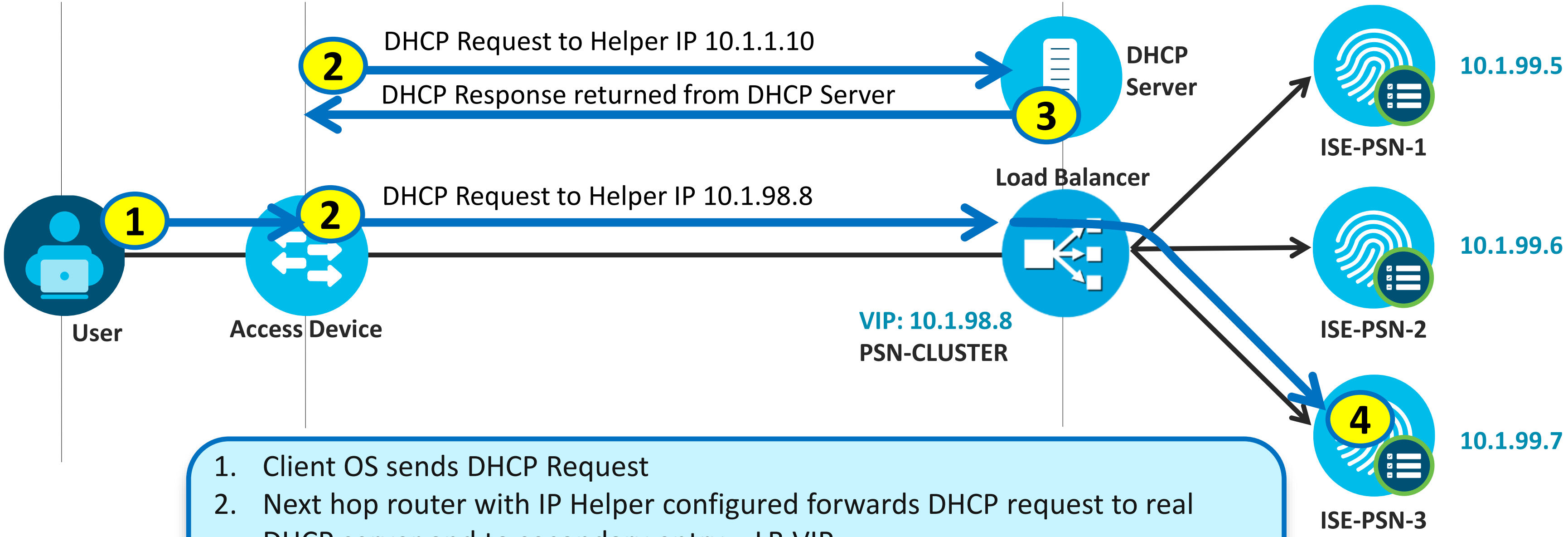
Other FQDNs or wildcard as “DNS Names”

IP Address is also option

Load Balancing ISE Profiling Services

Load Balancing Profiling Services

Sample Flow



1. Client OS sends DHCP Request
2. Next hop router with IP Helper configured forwards DHCP request to real DHCP server and to secondary entry = LB VIP
3. Real DHCP server responds and provide client a valid IP address
4. DHCP request to VIP is load balanced to PSN @ 10.1.99.7 based on source IP stick (L3 gateway) or DHCP field parsed from request.

Load Balancing Simplifies Device Configuration

L3 Switch Example for DHCP Relay

- Before

```
!
interface Vlan10
 description EMPLOYEE
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.100.100   <--- Real DHCP Server
 ip helper-address 10.1.99.5  <--- ISE-PSN-1
 ip helper-address 10.1.99.6  <--- ISE-PSN-2
!
```

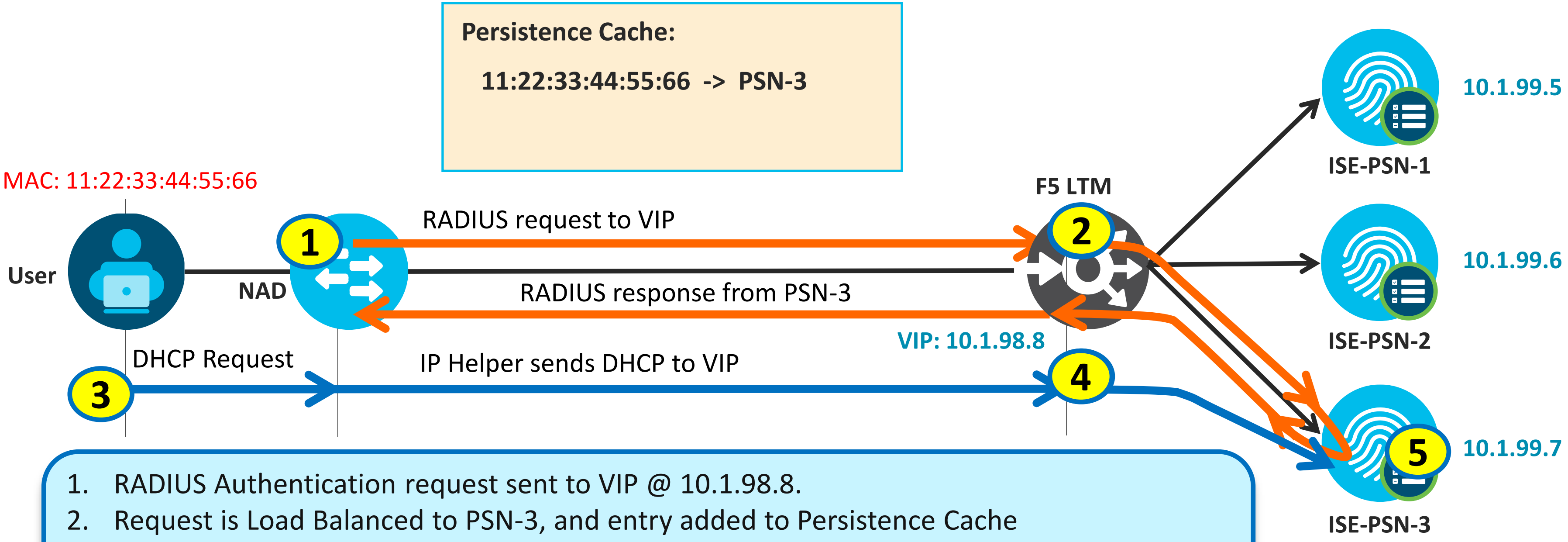
Settings apply to each L3 interface servicing DHCP endpoints

- After

```
!
interface Vlan10
 description EMPLOYEE
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.100.100   <--- Real DHCP Server
 ip helper-address 10.1.98.8  <--- LB VIP
!
```

Load Balancing Sticky Guidelines

Ensure DHCP and RADIUS for a Given Endpoint Use Same PSN



1. RADIUS Authentication request sent to VIP @ 10.1.98.8.
2. Request is Load Balanced to PSN-3, and entry added to Persistence Cache
3. DHCP Request is sent to VIP @ 10.1.98.8
4. Load Balancer uses the same "Sticky" as RADIUS based on client MAC address
5. DHCP is received by *same* PSN, thus optimizing endpoint replication

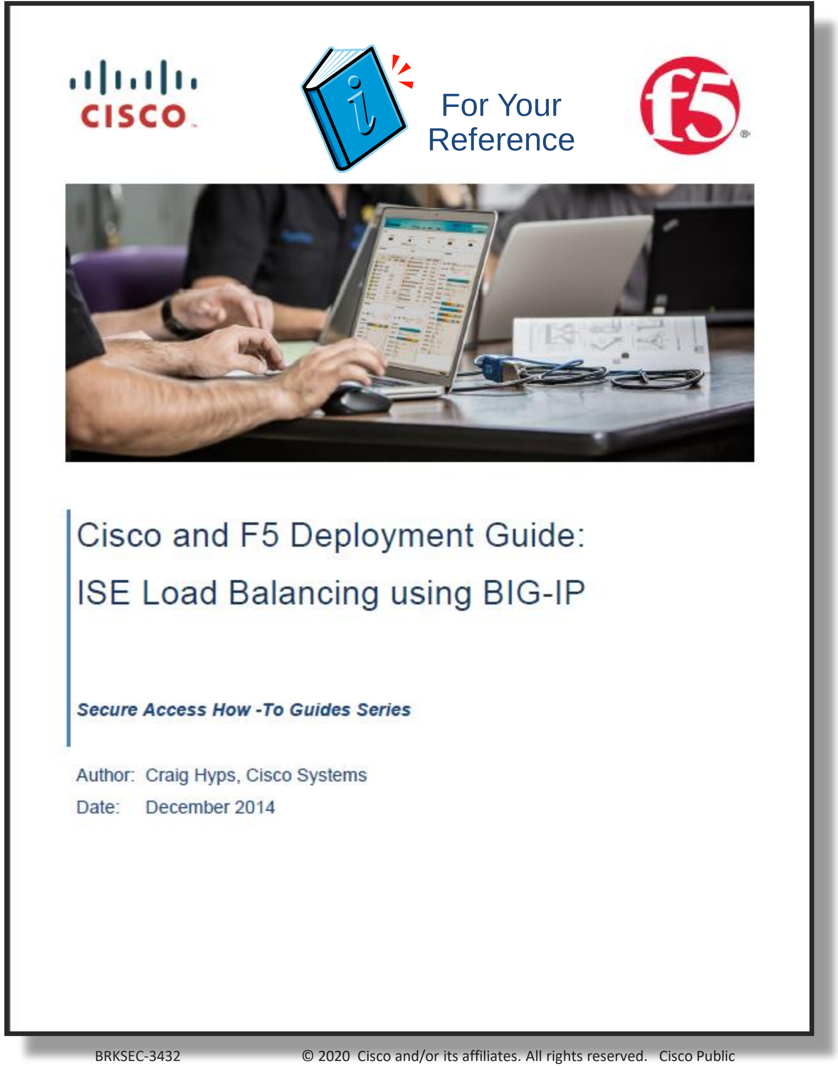
Vendor-Specific LB Configurations

- F5 LTM
- Citrix NetScaler
- Cisco ACE
- Cisco ITD (Note)

https://community.cisco.com/t5/security-documents/ise-load-balancing/ta-p/3648759

F5 LTM

- **Cisco Communities**
  https://community.cisco.com/t5/security-documents/ise-load-balancing/ta-p/3648759
- **Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP:**
  https://community.cisco.com/t5/security-documents/how-to-cisco-amp-f5-deployment-guide-ise-load-balancing-using/ta-p/3631159
- **Linked from F5 website under Cisco Alliance page > White Papers:**
  https://f5.com/solutions/technology-alliances/cisco
- **Configuring F5 LTM for Cisco ISE LB:**
  https://community.cisco.com/t5/security-documents/configuring-f5-ltm-for-cisco-ise-load-balancing/ta-p/3642134
- **BRKSEC-3699** Reference Presentation Complete working config + screenshots
  https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94152



For Your Reference

Cisco and F5 Deployment Guide:

ISE Load Balancing using BIG-IP

Secure Access How -To Guides Series

Author: Craig Hyps, Cisco Systems

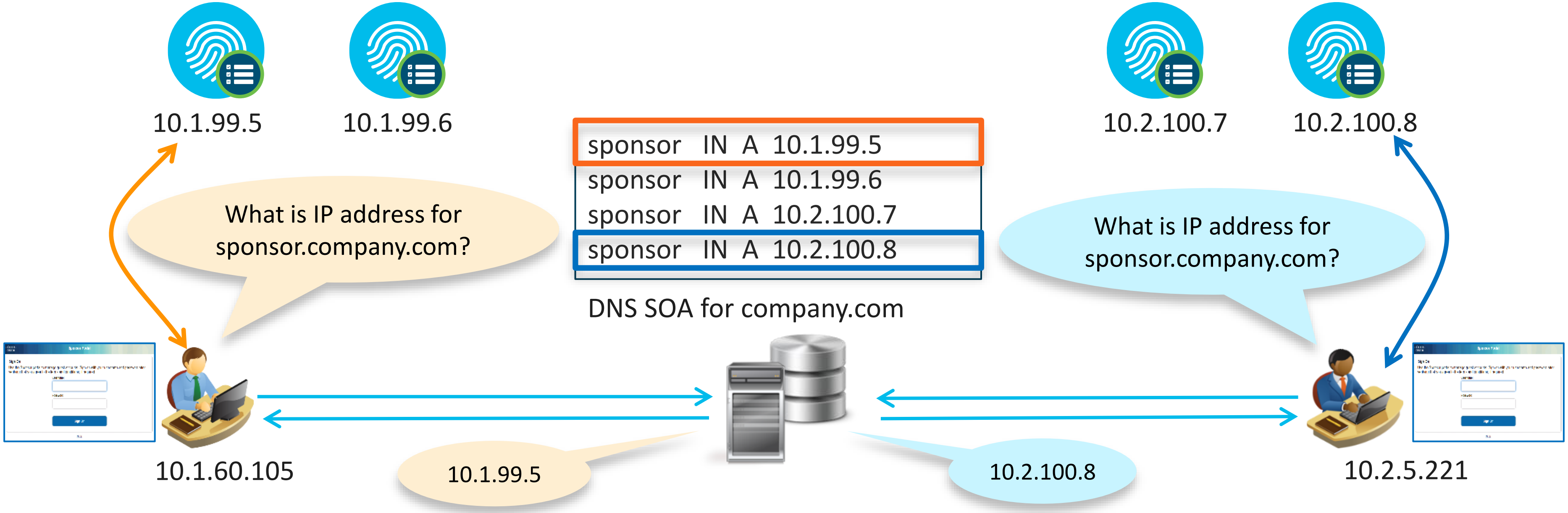
Date: December 2014

PSN HA Without Load Balancers

Load Balancing Web Requests Using DNS

Client-Based Load Balancing/Distribution Based on DNS Response

- Examples:
  - Cisco Global Site Selector (GSS) / F5 BIG-IP GTM / Microsoft’s DNS Round-Robin feature
- Useful for web services that use static URLs including LWA, Sponsor, My Devices, OCSP.



10.1.99.5 10.1.99.6 10.2.100.7 10.2.100.8

```
sponsor   IN  A  10.1.99.5
sponsor   IN  A  10.1.99.6
sponsor   IN  A  10.2.100.7
sponsor   IN  A  10.2.100.8
```

DNS SOA for company.com

What is IP address for sponsor.company.com?

What is IP address for sponsor.company.com?

10.1.60.105

10.1.99.5

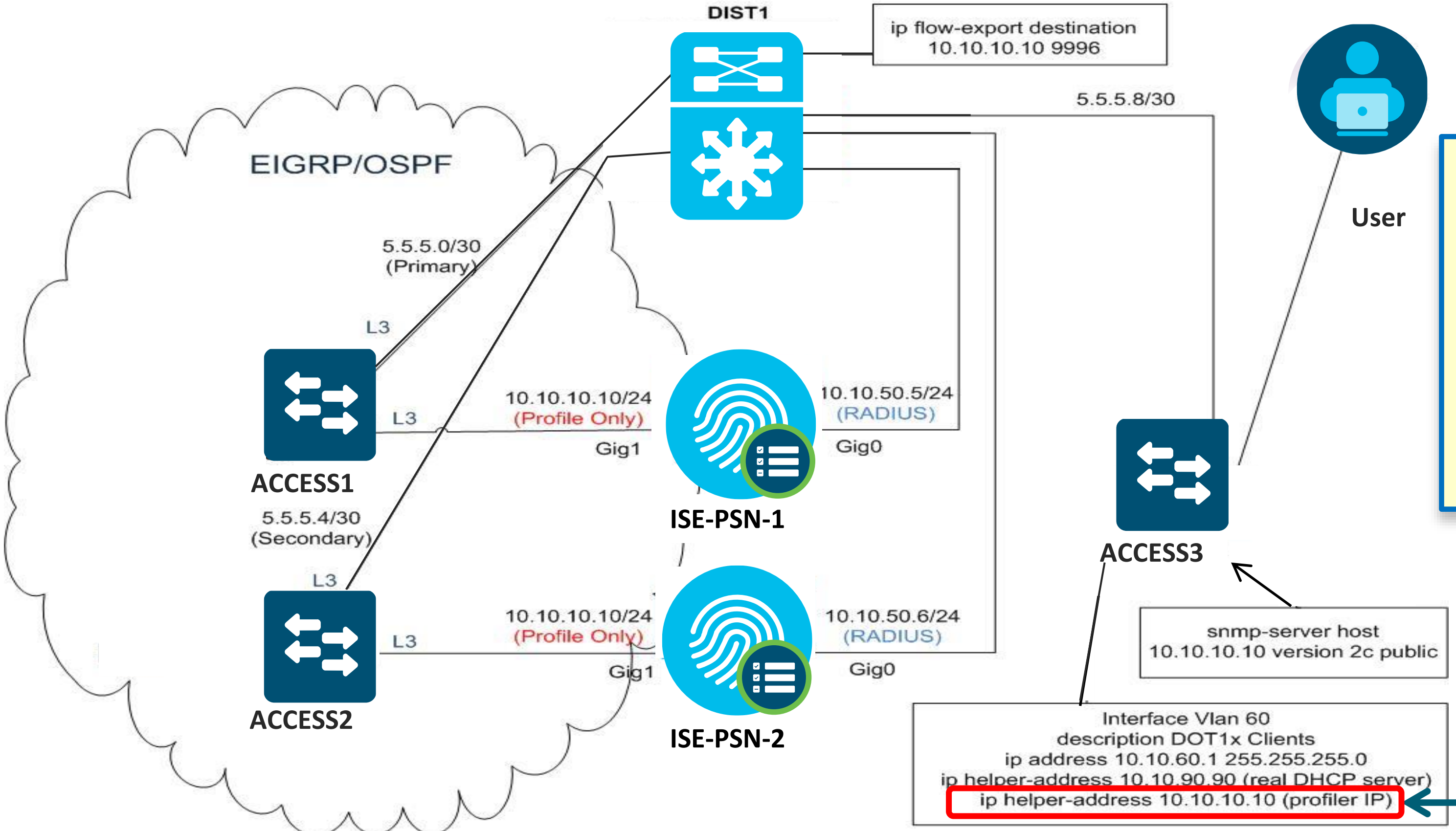
10.2.100.8

10.2.5.221

Using Anycast for ISE Redundancy

Profiling Example

For Your Reference



```
ip flow-export destination
10.10.10.10 9996
```

```
snmp-server host
10.10.10.10 version 2c public
```

```
Interface Vlan 60
description DOT1x Clients
ip address 10.10.60.1 255.255.255.0
ip helper-address 10.10.90.90 (real DHCP server)
ip helper-address 10.10.10.10 (profiler IP)
```

Provided dedicated interface or LB VIPs used, Anycast may be used for Profiling, Web Portals (Sponsor, Guest LWA, and MDP) and RADIUS AAA!

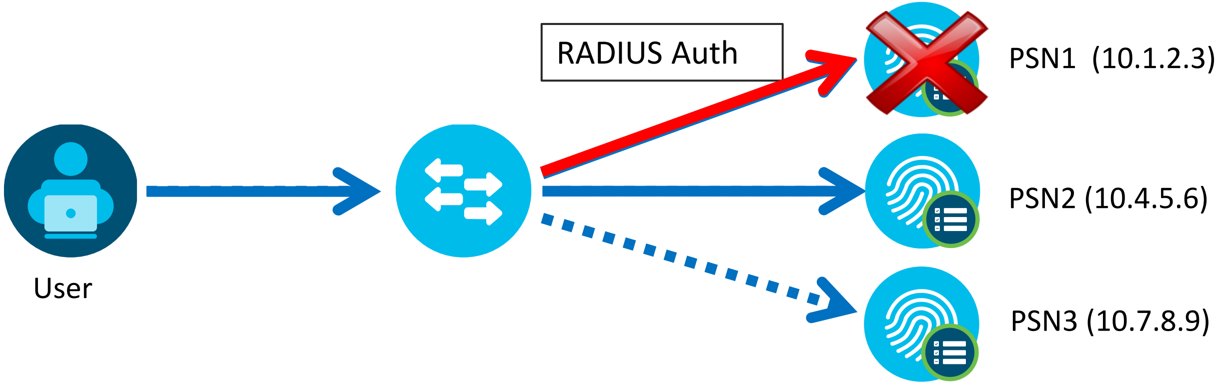
NADs are configured with single Anycast IP address.

Ex: 10.10.10.10

NAD-Based RADIUS Server Redundancy (IOS)

Multiple RADIUS Servers Defined in Access Device

- Configure Access Devices with multiple RADIUS Servers.
- Fallback to secondary servers if primary fails

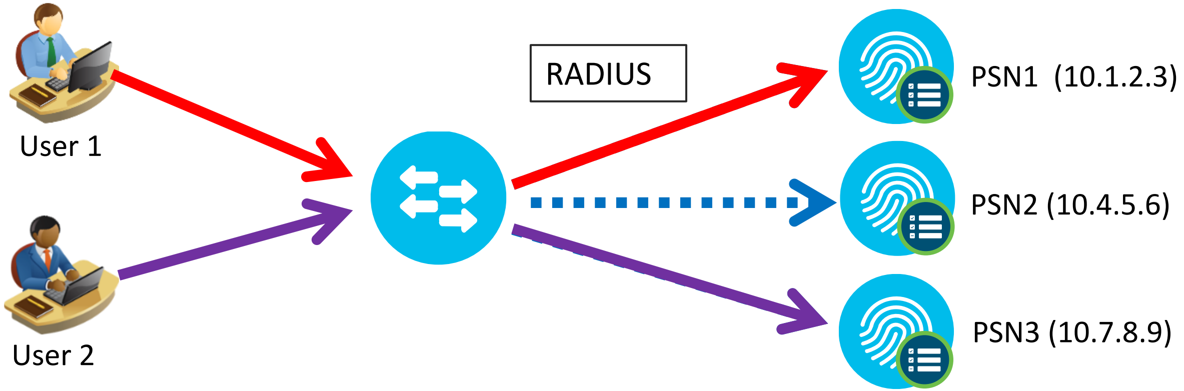


```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

IOS-Based RADIUS Server Load Balancing

Switch Dynamically Distributes Requests to Multiple RADIUS Servers

- RADIUS LB feature distributes batches of AAA transactions to servers within a group.
- Each batch assigned to server with least number of outstanding transactions.



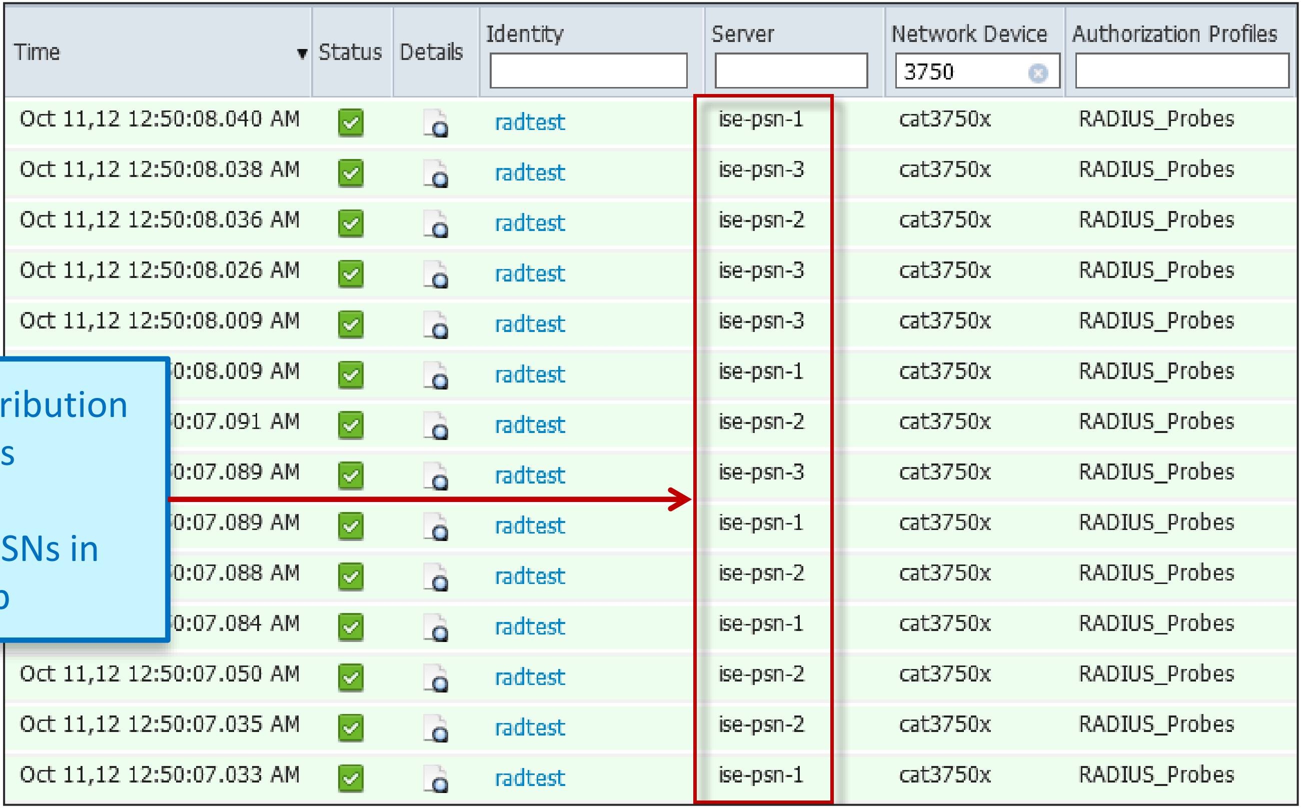
NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
radius-server load-balance method least-outstanding batch-size 5
```

IOS-Based RADIUS Server Load Balancing

Sample Live Log

- Use **test aaa group** command from IOS CLI to test RADIUS auth requests



Time	Status	Details	Identity	Server	Network Device	Authorization Profiles
					3750	
Oct 11,12 12:50:08.040 AM	✓	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.038 AM	✓	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.036 AM	✓	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.026 AM	✓	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.009 AM	✓	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:08.009 AM	✓	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.091 AM	✓	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.089 AM	✓	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:07.089 AM	✓	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.088 AM	✓	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.084 AM	✓	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.050 AM	✓	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.035 AM	✓	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.033 AM	✓	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes

Reasonable load distribution across all PSNs

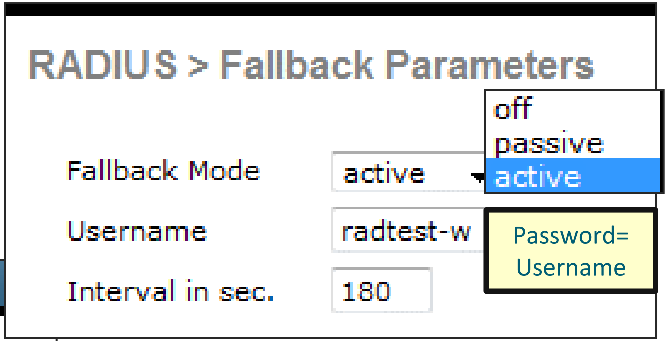
Example shows 3 PSNs in RADIUS group

```
cat3750x# test aaa group radius radtest cisco123 new users 4 count 50
AAA/SG/TEST: Sending 50 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
```

NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

- Multiple RADIUS Auth & Accounting Server Definitions
- RADIUS Fallback options: **none, passive,** or **active**



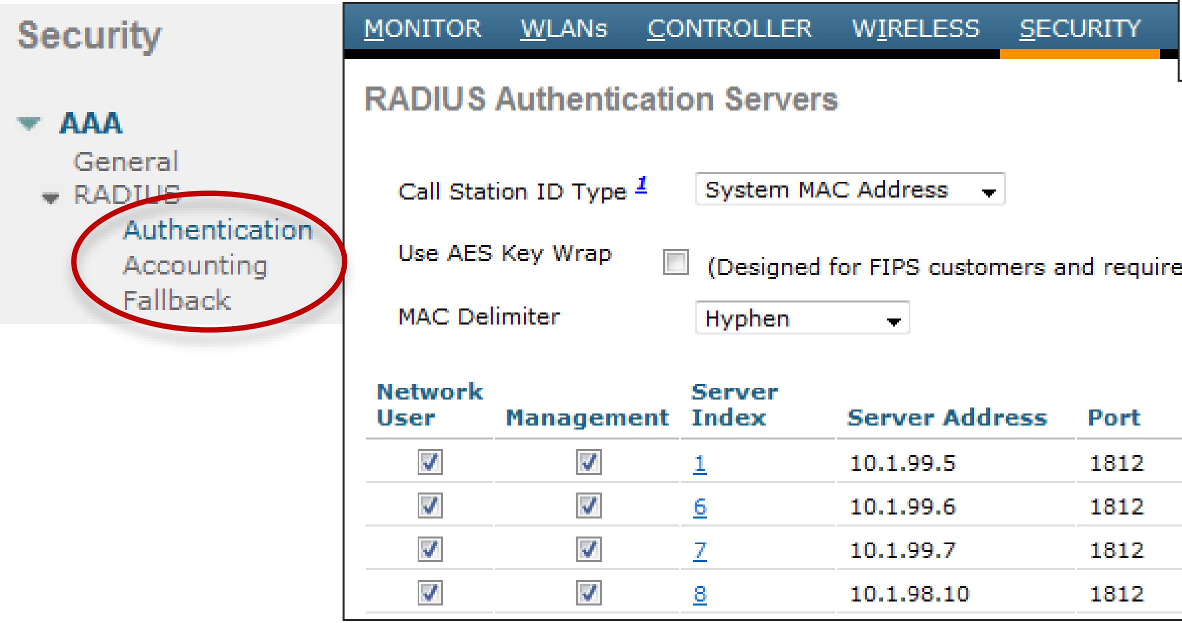
RADIUS > Fallback Parameters

Fallback Mode: active (off / passive / active)

Username: radtest-w

Interval in sec.: 180

Password= Username



RADIUS Authentication Servers

Call Station ID Type [1]: System MAC Address

Use AES Key Wrap □ (Designed for FIPS customers and requires a

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port
☑	☑	1	10.1.99.5	1812
☑	☑	6	10.1.99.6	1812
☑	☑	7	10.1.99.7	1812
☑	☑	8	10.1.98.10	1812

Off = Continue exhaustively through list; never preempt to preferred server (entry with lowest index)

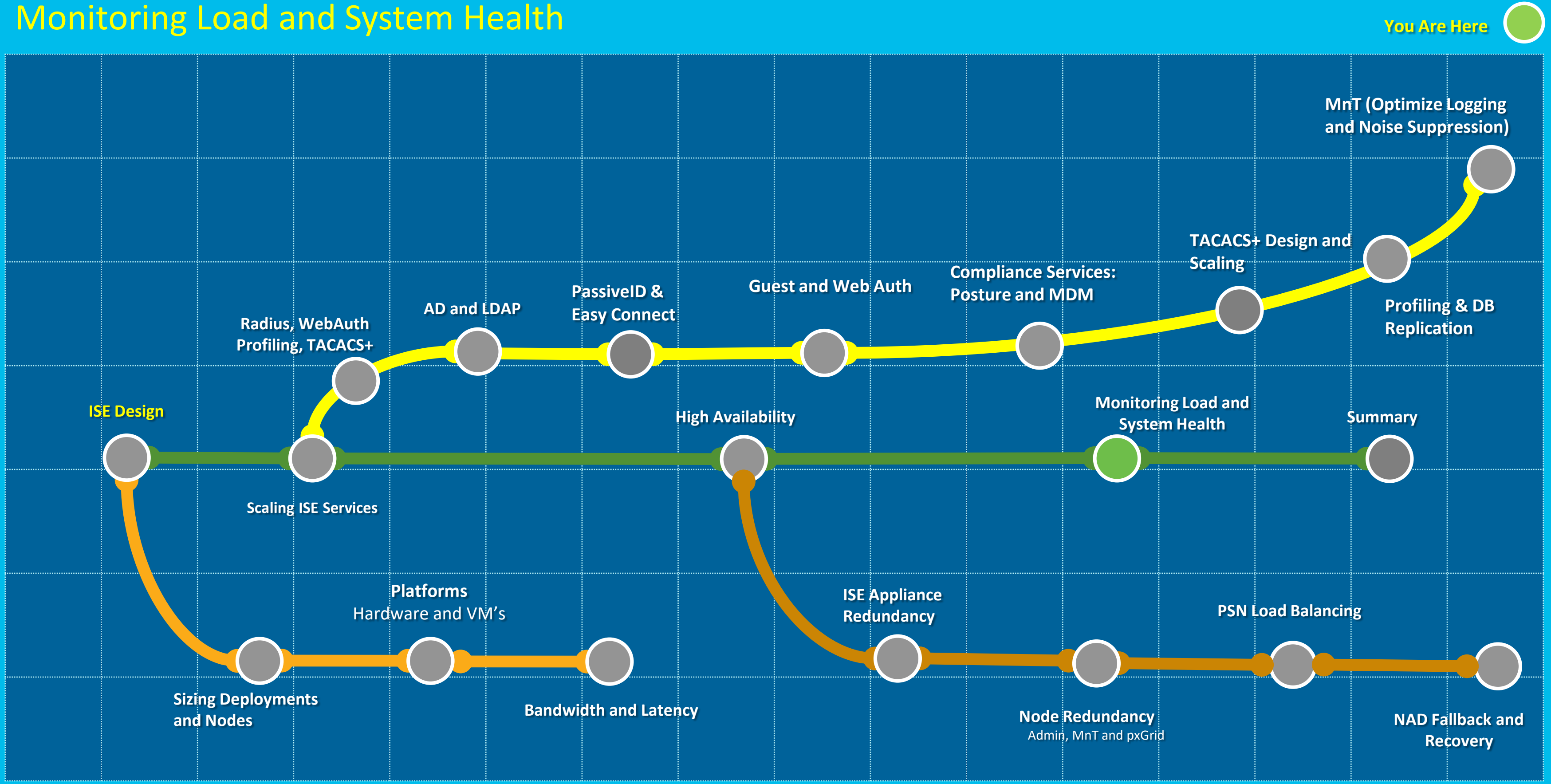
Passive = Quarantine failed RADIUS server for interval then return to active list w/o validation; always preempt.

Active = Mark failed server dead then actively probe status per interval w/username until succeed before return to list; always preempt.

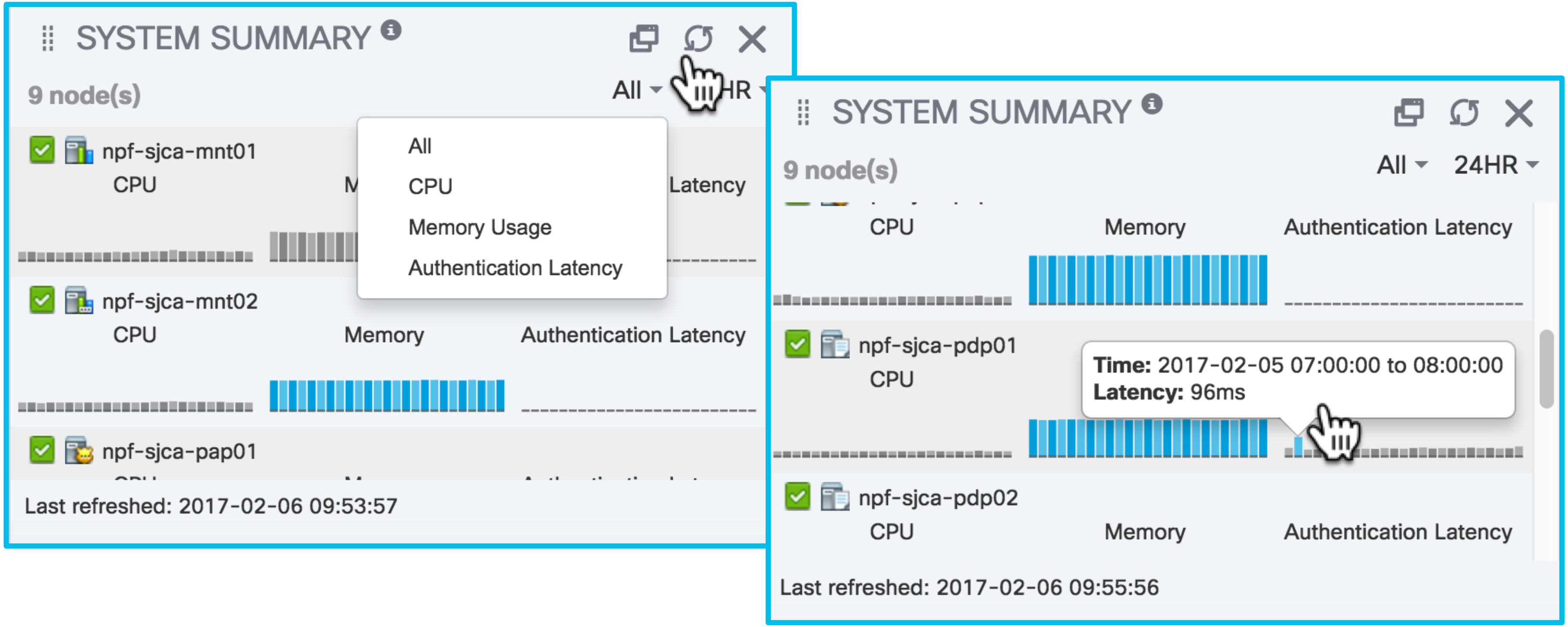
http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008098987e.shtml

Session Agenda

Monitoring Load and System Health


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
Scaling ISE Services
High Availability
Monitoring Load and System Health
Summary
Platforms
Hardware and VM's
Sizing Deployments and Nodes
Bandwidth and Latency
ISE Appliance Redundancy
Node Redundancy
Admin, MnT and pxGrid
PSN Load Balancing
NAD Fallback and Recovery

Home Dashboard - High-Level Server Health



Last refreshed: 2017-02-06 09:53:57

Time: 2017-02-05 07:00:00 to 08:00:00
Latency: 96ms

Last refreshed: 2017-02-06 09:55:56

Server Health/Utilization Reports

Operations > Reports > Diagnostics > Health Summary

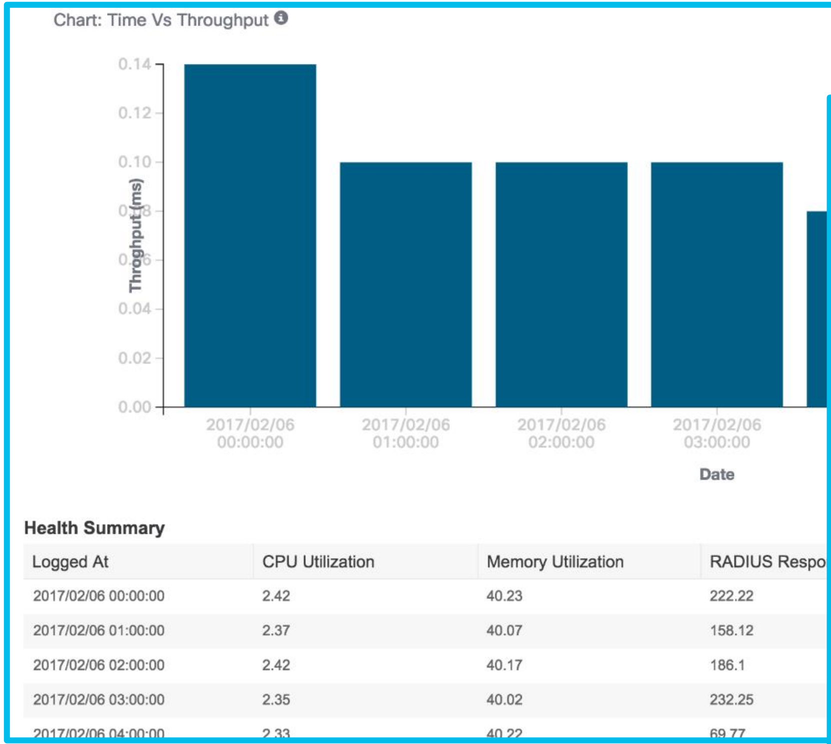
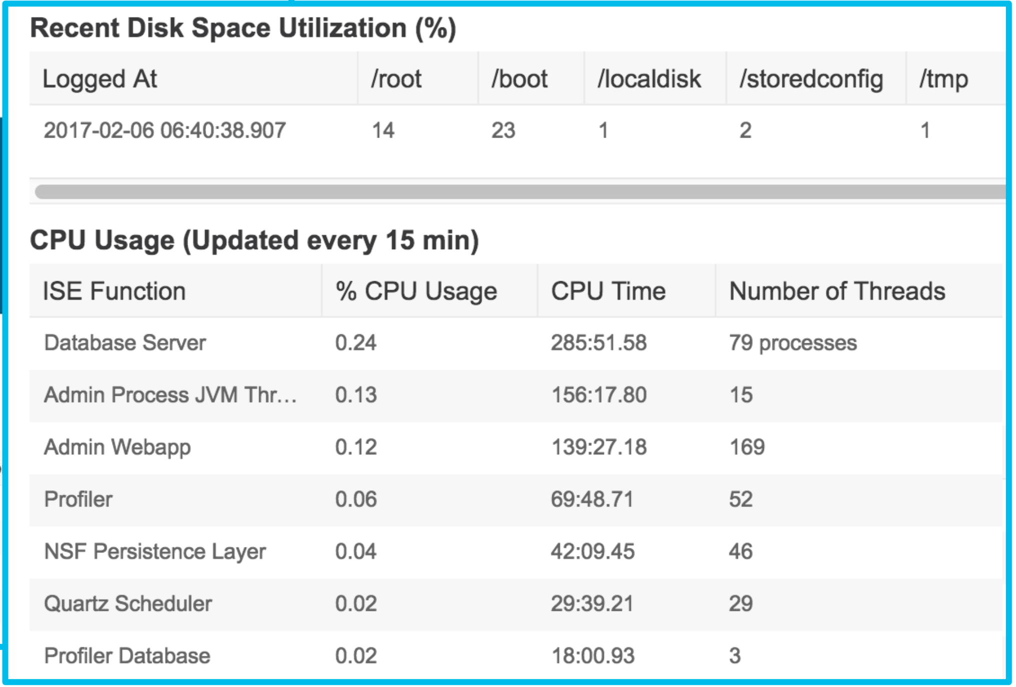


Chart: Time Vs Throughput

Health Summary

Logged At	CPU Utilization	Memory Utilization	RADIUS Respo
2017/02/06 00:00:00	2.42	40.23	222.22
2017/02/06 01:00:00	2.37	40.07	158.12
2017/02/06 02:00:00	2.42	40.17	186.1
2017/02/06 03:00:00	2.35	40.02	232.25
2017/02/06 04:00:00	2.33	40.22	69.77


Recent Disk Space Utilization (%)

Logged At	/root	/boot	/localdisk	/storedconfig	/tmp
2017-02-06 06:40:38.907	14	23	1	2	1

CPU Usage (Updated every 15 min)

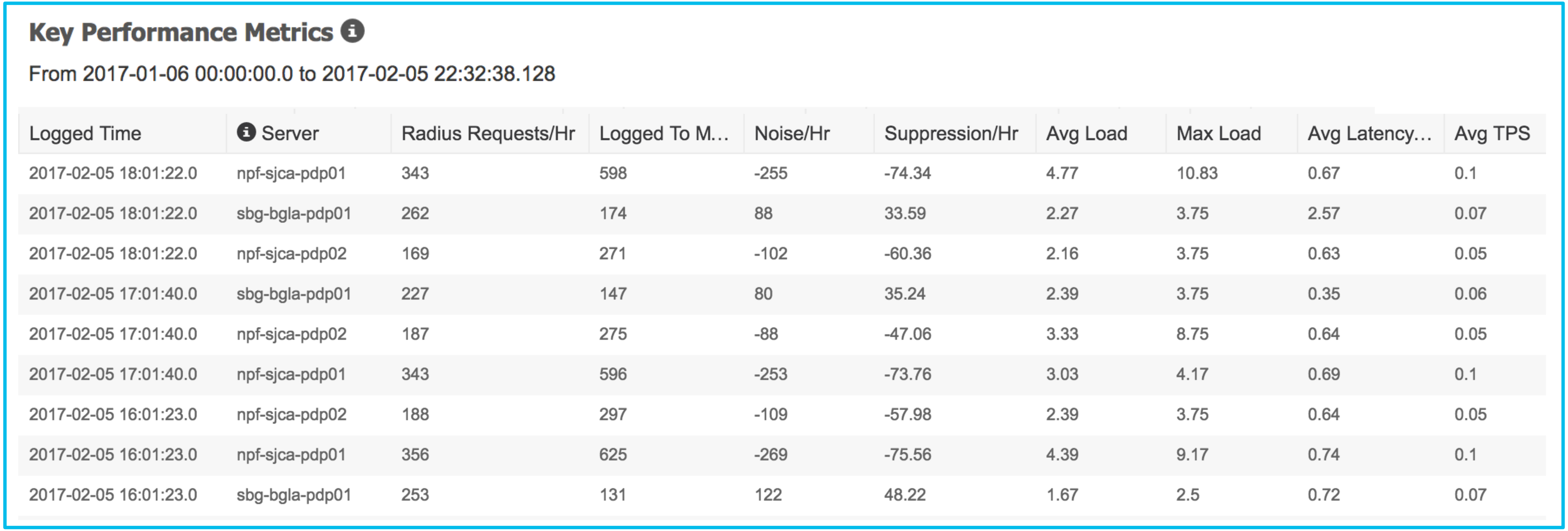
ISE Function	% CPU Usage	CPU Time	Number of Threads
Database Server	0.24	285:51.58	79 processes
Admin Process JVM Thr...	0.13	156:17.80	15
Admin Webapp	0.12	139:27.18	169
Profiler	0.06	69:48.71	52
NSF Persistence Layer	0.04	42:09.45	46
Quartz Scheduler	0.02	29:39.21	29
Profiler Database	0.02	18:00.93	3

Key Performance Metrics (KPM)

KPM Reports added in ISE 2.2: Operations > Reports > Diagnostics > KPM

Also available from CLI (# application configure ise)

Provide RADIUS Load, Latency, and Suppression Stats



Key Performance Metrics ℹ

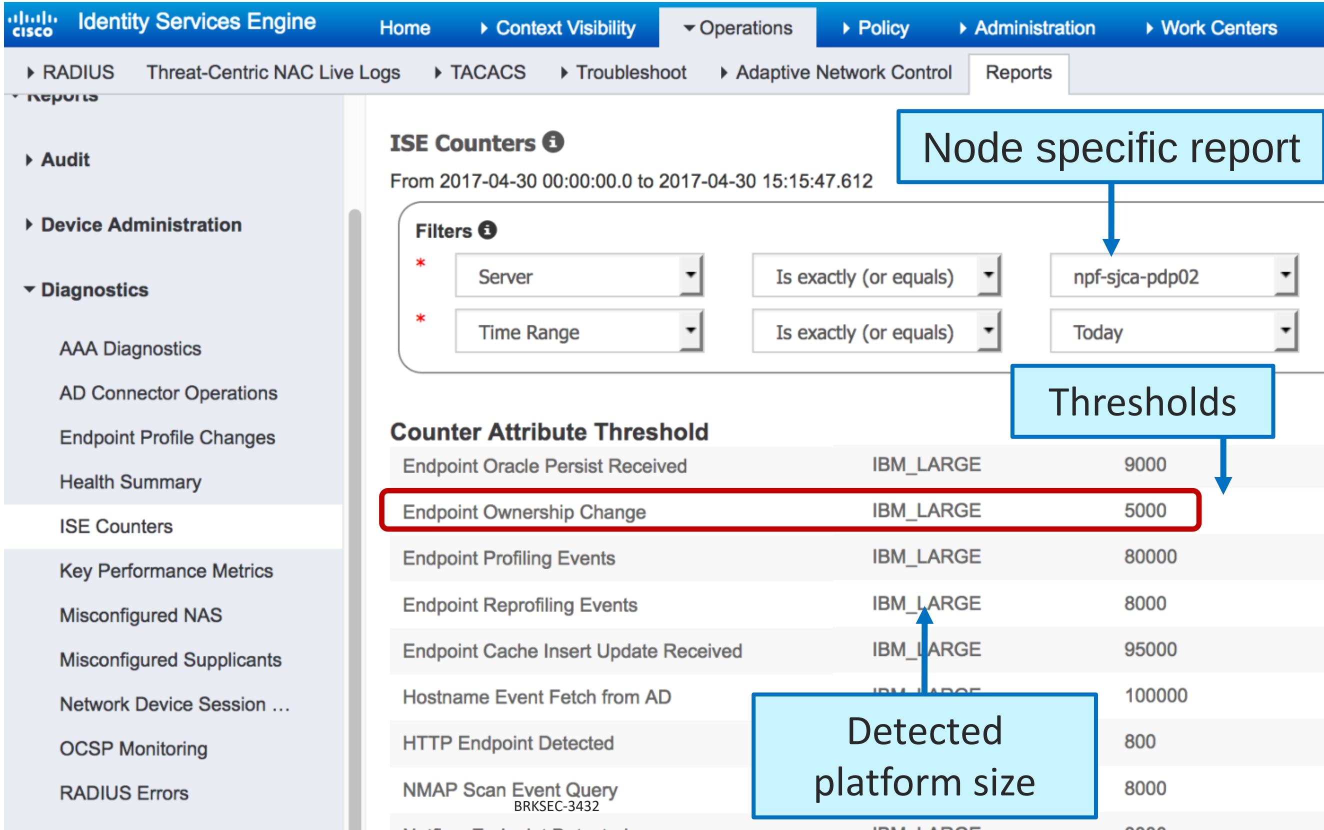
From 2017-01-06 00:00:00.0 to 2017-02-05 22:32:38.128

Logged Time	ℹ Server	Radius Requests/Hr	Logged To M...	Noise/Hr	Suppression/Hr	Avg Load	Max Load	Avg Latency...	Avg TPS
2017-02-05 18:01:22.0	npf-sjca-pdp01	343	598	-255	-74.34	4.77	10.83	0.67	0.1
2017-02-05 18:01:22.0	sbg-bgla-pdp01	262	174	88	33.59	2.27	3.75	2.57	0.07
2017-02-05 18:01:22.0	npf-sjca-pdp02	169	271	-102	-60.36	2.16	3.75	0.63	0.05
2017-02-05 17:01:40.0	sbg-bgla-pdp01	227	147	80	35.24	2.39	3.75	0.35	0.06
2017-02-05 17:01:40.0	npf-sjca-pdp02	187	275	-88	-47.06	3.33	8.75	0.64	0.05
2017-02-05 17:01:40.0	npf-sjca-pdp01	343	596	-253	-73.76	3.03	4.17	0.69	0.1
2017-02-05 16:01:23.0	npf-sjca-pdp02	188	297	-109	-57.98	2.39	3.75	0.64	0.05
2017-02-05 16:01:23.0	npf-sjca-pdp01	356	625	-269	-75.56	4.39	9.17	0.74	0.1
2017-02-05 16:01:23.0	sbg-bgla-pdp01	253	131	122	48.22	1.67	2.5	0.72	0.07

Serviceability Counter Framework (CF)

The Easy Way: MnT auto-collects key metrics from each node!

- Enable/disable from 'app configure ise'
- Enabled by default
- Threshold are hard set by platform size
- Alarm sent when exceed threshold
- Running count displayed per collection interval



ISE Counters

From 2017-04-30 00:00:00.0 to 2017-04-30 15:15:47.612

Filters

* Server	Is exactly (or equals)	npf-sjca-pdp02
* Time Range	Is exactly (or equals)	Today

Counter Attribute Threshold

Endpoint Oracle Persist Received	IBM_LARGE	9000
Endpoint Ownership Change	IBM_LARGE	5000
Endpoint Profiling Events	IBM_LARGE	80000
Endpoint Reprofiling Events	IBM_LARGE	8000
Endpoint Cache Insert Update Received	IBM_LARGE	95000
Hostname Event Fetch from AD	IBM_LARGE	100000
HTTP Endpoint Detected	[illegible]	800
NMAP Scan Event Query	[illegible]	8000

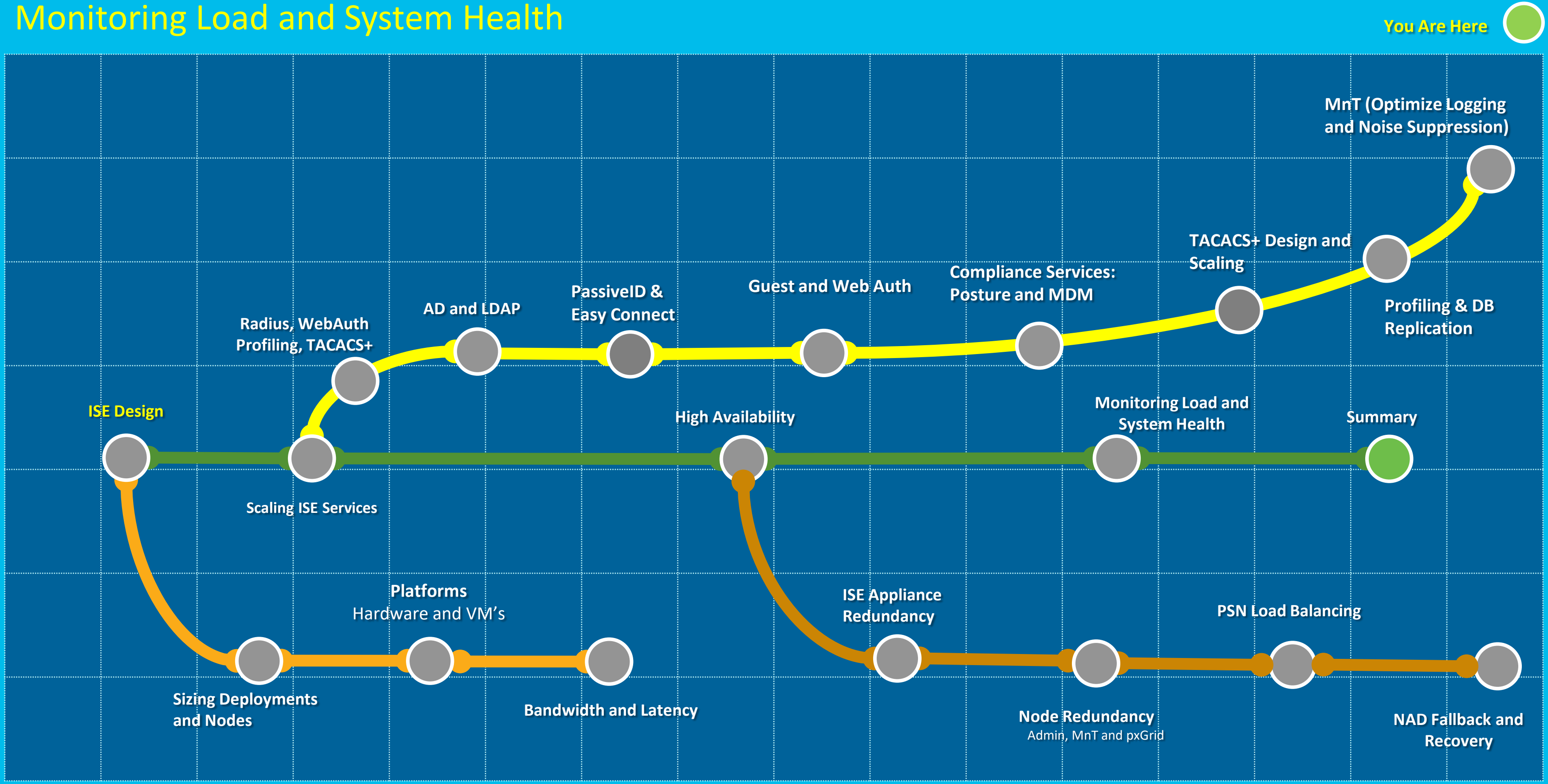
Node specific report

Thresholds

Detected platform size

Session Agenda

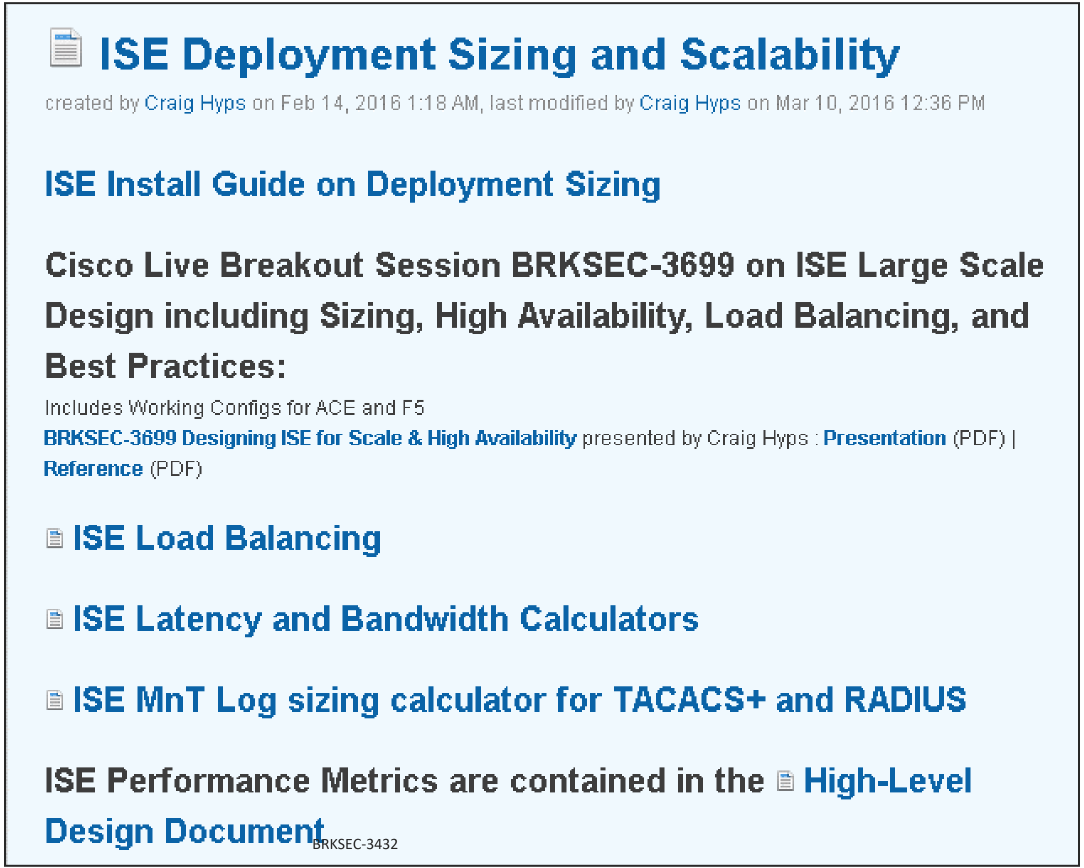
Monitoring Load and System Health


You Are Here
MnT (Optimize Logging and Noise Suppression)
TACACS+ Design and Scaling
Profiling & DB Replication
Compliance Services: Posture and MDM
Guest and Web Auth
PassiveID & Easy Connect
AD and LDAP
Radius, WebAuth Profiling, TACACS+
ISE Design
High Availability
Monitoring Load and System Health
Summary
Scaling ISE Services
Platforms
Hardware and VM's
ISE Appliance Redundancy
PSN Load Balancing
Sizing Deployments and Nodes
Bandwidth and Latency
Node Redundancy
Admin, MnT and pxGrid
NAD Fallback and Recovery

ISE Performance & Scale Resources

https://community.cisco.com/t5/security-documents/ise-performance-amp-scale/ta-p/3642148

- Cisco Live: BRKSEC-3432 *Reference version*
- ISE Load Balancing Design Guide
- Performance and Scale guidance in HLD template
- Calculators for Bandwidth and Logging



ISE Deployment Sizing and Scalability

created by Craig Hyps on Feb 14, 2016 1:18 AM, last modified by Craig Hyps on Mar 10, 2016 12:36 PM

ISE Install Guide on Deployment Sizing

Cisco Live Breakout Session BRKSEC-3699 on ISE Large Scale Design including Sizing, High Availability, Load Balancing, and Best Practices:

Includes Working Configs for ACE and F5

BRKSEC-3699 Designing ISE for Scale & High Availability presented by Craig Hyps : **Presentation** (PDF) | **Reference** (PDF)

ISE Load Balancing

ISE Latency and Bandwidth Calculators

ISE MnT Log sizing calculator for TACACS+ and RADIUS

ISE Performance Metrics are contained in the High-Level Design Document

For Your Reference

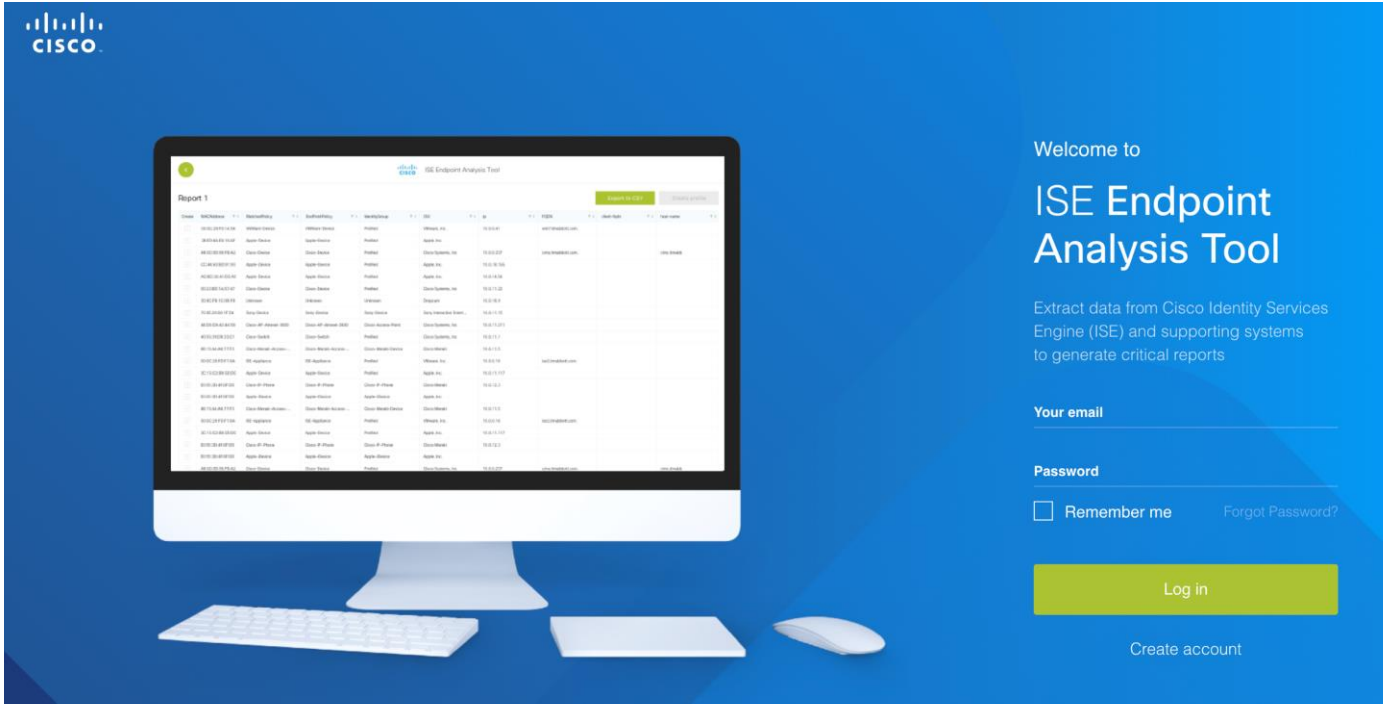
Additional Resources

Public Resources

ISE Public Community	http://cs.co/ise-community
ISE Compatibility Guides	http://cs.co/ise-compatibility
ISE Ecosystem Guides	http://cs.co/ise-guides
ISE Guest	http://cs.co/ise-guest
ISE Feedback	http://cs.co/ise-feedback
ISE Resources	http://cs.co/ise-resources
ISE Software & Eval	http://cs.co/ise-eval

ISE Endpoint Analysis Tool

http://iseeat.cisco.com



Welcome to

ISE Endpoint Analysis Tool

Extract data from Cisco Identity Services Engine (ISE) and supporting systems to generate critical reports

Your email

Password

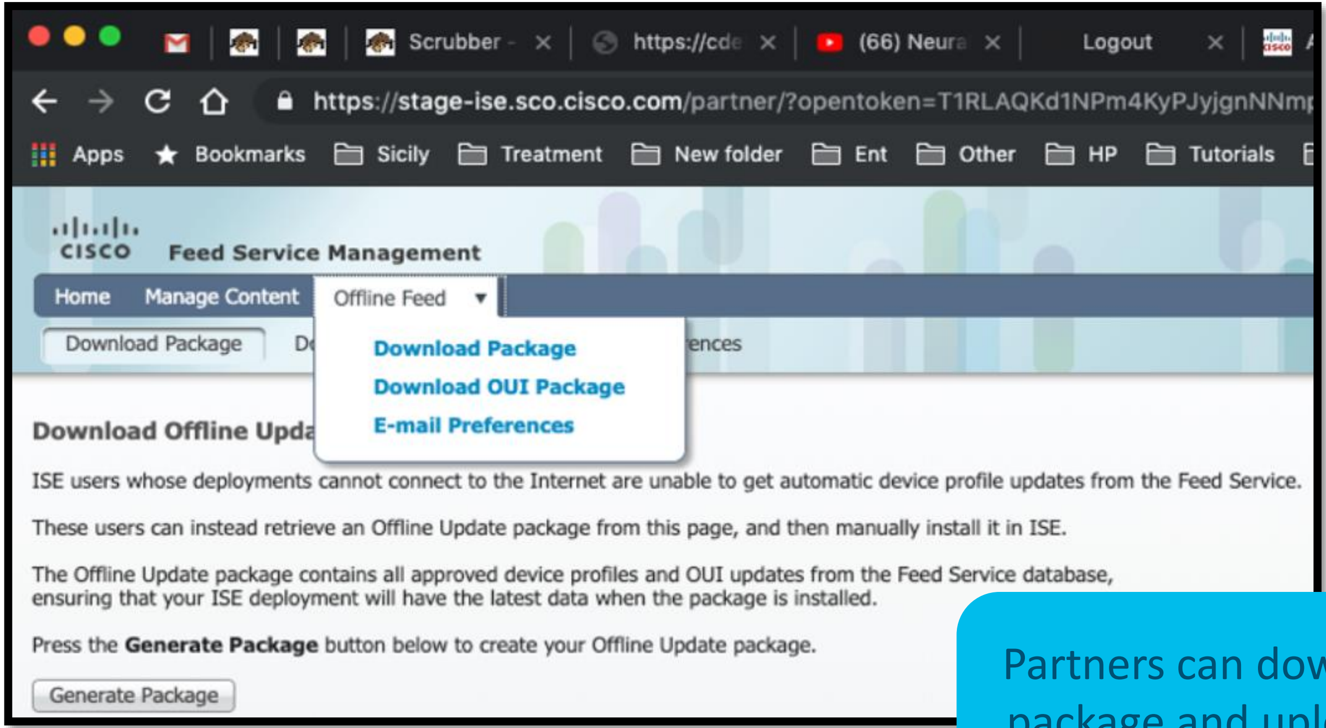
□ Remember me Forgot Password?

Log in

Create account

ISE 2.7 Update

New Partner Portal- 2.7



Download Offline Upda

ISE users whose deployments cannot connect to the Internet are unable to get automatic device profile updates from the Feed Service.

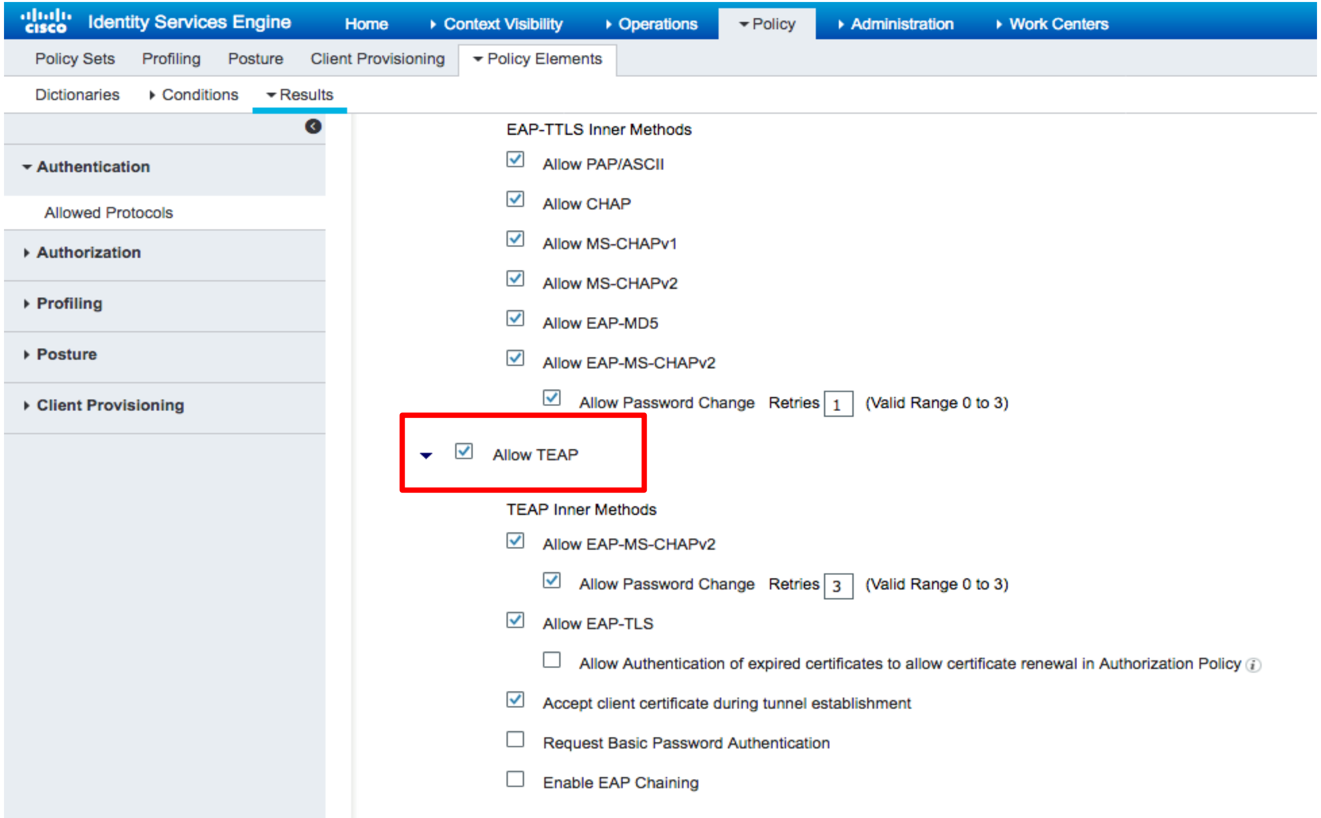
These users can instead retrieve an Offline Update package from this page, and then manually install it in ISE.

The Offline Update package contains all approved device profiles and OUI updates from the Feed Service database, ensuring that your ISE deployment will have the latest data when the package is installed.

Press the **Generate Package** button below to create your Offline Update package.

Partners can download just the feed OUI package and upload to offline feed page in ISE just to update the OUI.

TEAP Support -ISE Configuration



EAP-TTLS Inner Methods

☑ Allow PAP/ASCII

☑ Allow CHAP

☑ Allow MS-CHAPv1

☑ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow TEAP

TEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☑ Accept client certificate during tunnel establishment

□ Request Basic Password Authentication

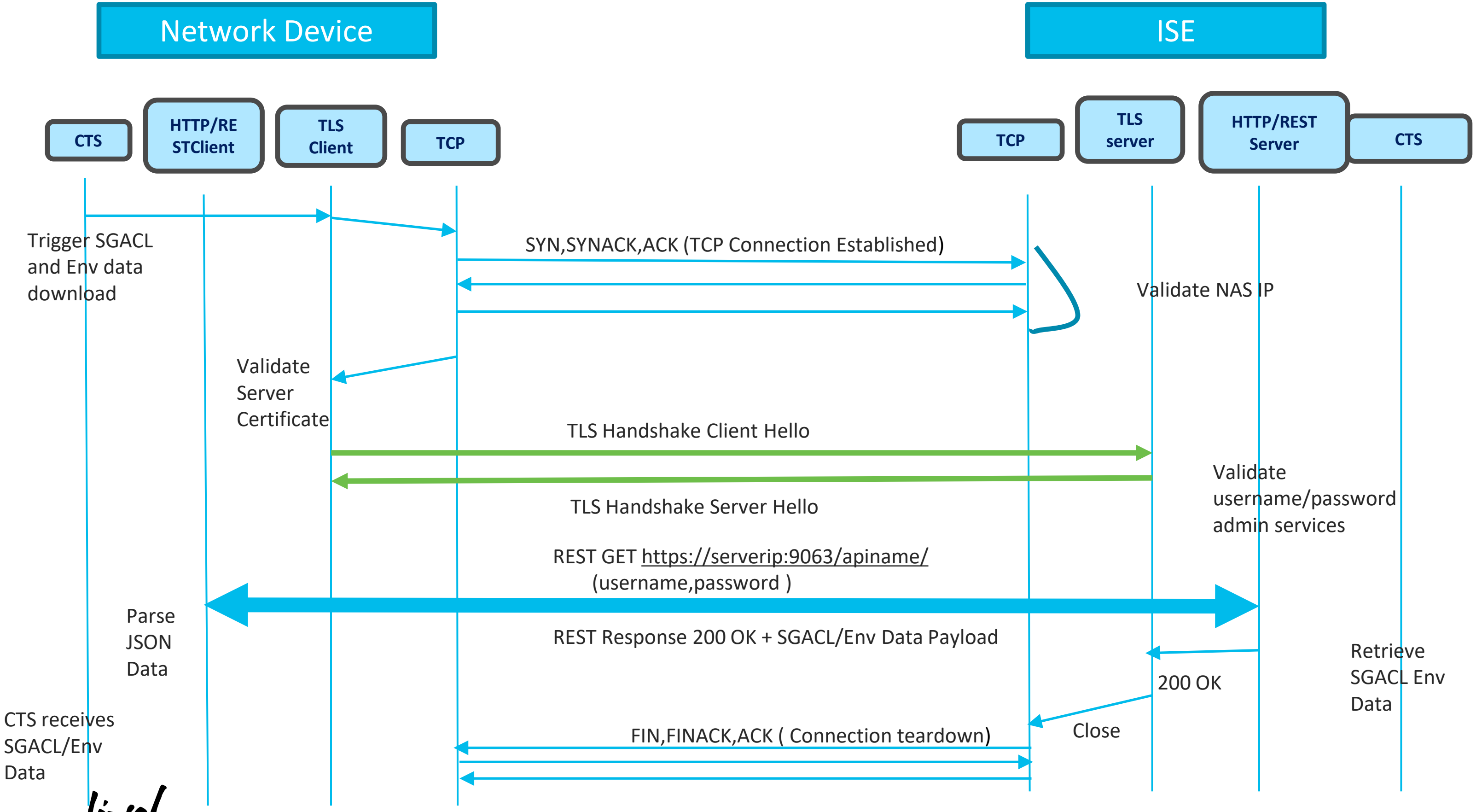
□ Enable EAP Chaining

Streamlining Policy Downloads

- HTTPS Download (using TLS 1.2) for policies and environment data with ISE 2.7 and IOS-XE 17.1.1
- Reliable transport, avoids PAC mechanisms being needed
- Future versions will provide additional policy download assurance capabilities
- Caveats:
- First release will not operate with ISE Server Load Balancing
    - Devices will send requests to a single PSN ! (but IOS-XE will provide a randomization option)
- First release will not provide IPv6 server list over HTTPS

Streamlining Policy Downloads

HTTPS Download (using TLS 1.2)
Policy and Environment Data
ISE 2.7 and IOS-XE 17.1.1



Network Device
ISE
CTS
HTTP/RESTClient
TLS Client
TCP
TCP
TLS server
HTTP/REST Server
CTS
Trigger SGACL and Env data download
SYN,SYNACK,ACK (TCP Connection Established)
Validate NAS IP
Validate Server Certificate
TLS Handshake Client Hello
TLS Handshake Server Hello
Validate username/password admin services
REST GET https://serverip:9063/apiname/ (username,password)
Parse JSON Data
REST Response 200 OK + SGACL/Env Data Payload
Retrieve SGACL Env Data
200 OK
Close
CTS receives SGACL/Env Data
FIN,FINACK,ACK (Connection teardown)

Key Takeaway Points

- CHECK ISE Virtual Appliances for proper resources and platform detection!
- Avoid excessive auth activity through proper NAD / supplicant tuning and Log Suppression
- Minimize data replication by implementing node groups and profiling best practices
- Leverage load balancers for scale, high availability, and simplifying network config changes
- Be sure to have a local fallback plan on you network access devices

Please fill out the survey

Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

Possibilities

#CiscoLive