Cisco live!

6-9 March 2018 · Melbourne, Australia

Designing ISE for Scale & High Availability

Jason Kunst, Technical Marketing Engineer @nacbot

BRKSEC-3699

Cisco live!

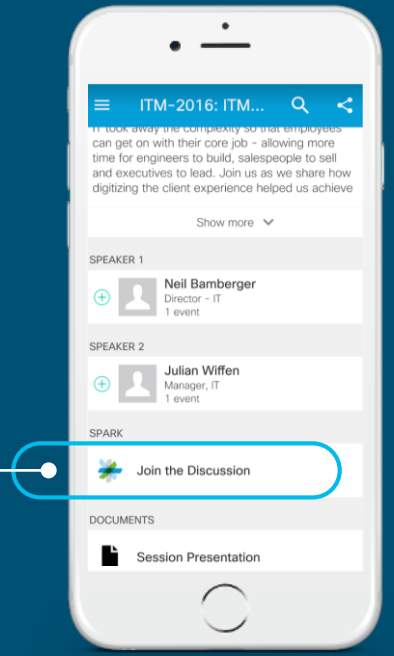
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



Session Abstract

Cisco Identity Services Engine (ISE) delivers context-based access control for every endpoint that connects to your network. This session will show you how to design ISE to deliver scalable and highly available access control services for wired, wireless, and VPN from a single campus to a global deployment.

Focus is on design guidance for distributed ISE architectures including high availability for all ISE nodes and their services as well as strategies for survivability and fallback during service outages. Methodologies for increasing scalability and redundancy will be covered such as load distribution with and without load balancers, optimal profiling design, and the use of Anycast.

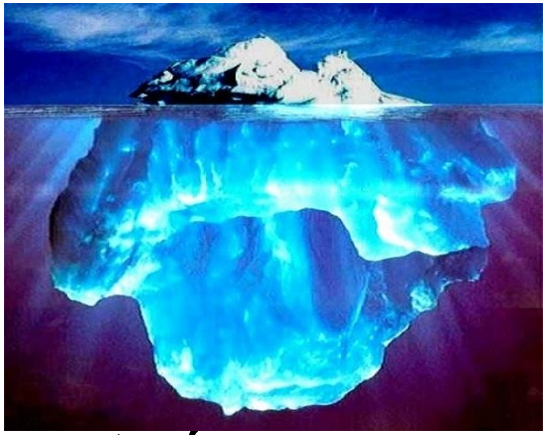
Attendees of this session will gain knowledge on how to best deploy ISE to ensure peak operational performance, stability, and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement.

Important: Hidden Slide Alert

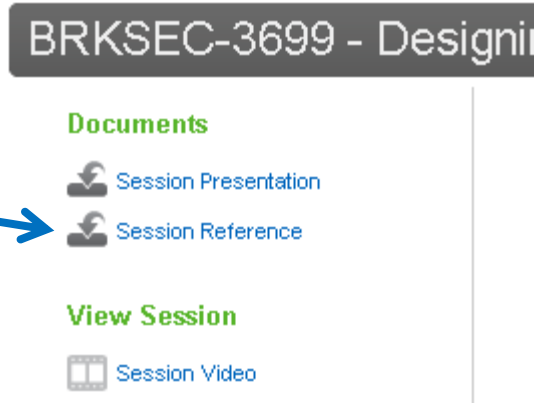
Look for this “For Your Reference” Symbol in your PDF’s

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

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**

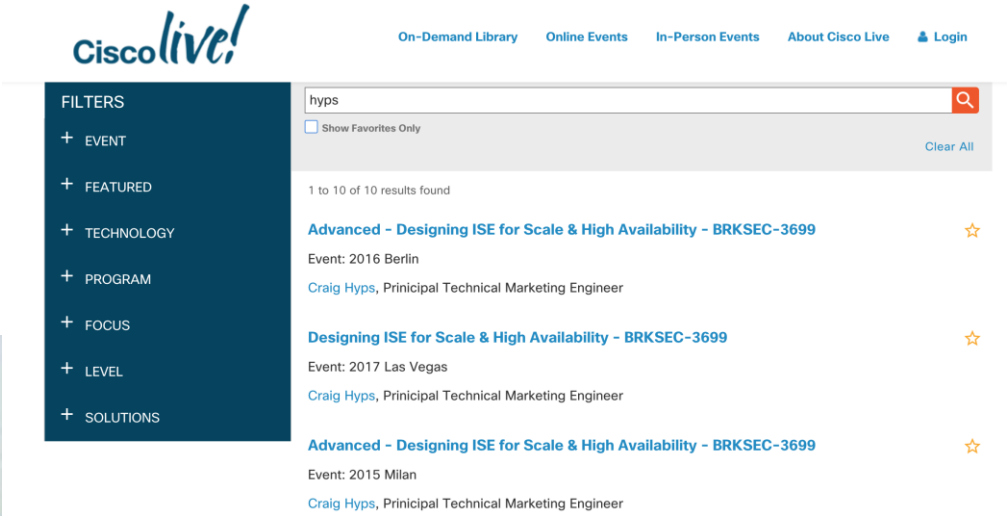
You take the blue pill – the story ends, you walk out of this room and believe whatever you want to believe.

Remember, all I'm offering is the truth – nothing more.

- The Matrix, 1999

You take the red pill – you stay in this room, and I show you how deep the rabbit hole goes.

From the horses mouth



https://www.ciscolive.com/global/on-demand-library/?search=hyps#/

Cisco live!

Cisco live!

Cisco live!

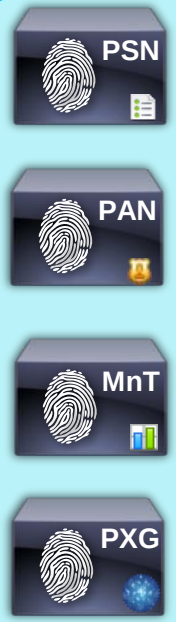
Agenda

- Sizing Deployments and Nodes
- Bandwidth and Latency
- Scaling ISE Services
- RADIUS, AD/LDAP, Passive ID, Guest, Web Services, TACACS+
- Profiling and Database Replication
- MnT (Optimise 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

Deployment Models and Sizing

Node Types



- Policy Service Node (PSN)
  - Makes policy decisions
  - RADIUS/TACACS+ server & provides endpoint/user services

Can run in a single host

- Policy Administration Node (PAN)
  - Interface to configure policies and manage ISE deployment
  - Replication hub for all database config changes
- Monitoring & Troubleshooting Node (MnT)
  - Interface to reporting and logging
  - Destination for syslog from other ISE nodes and optionally NADs
- pxGrid Controller
  - Facilitates sharing of information between network elements

Standalone Deployment

All Personas on a Single Node: PAN, PSN, MnT, pxGrid

- Maximum sessions – Platform dependent
  - 5,000 for 3415
  - 7,500 for 3515
  - 10,000 for 3495
  - 20,000 for 3595

Policy Administration Node

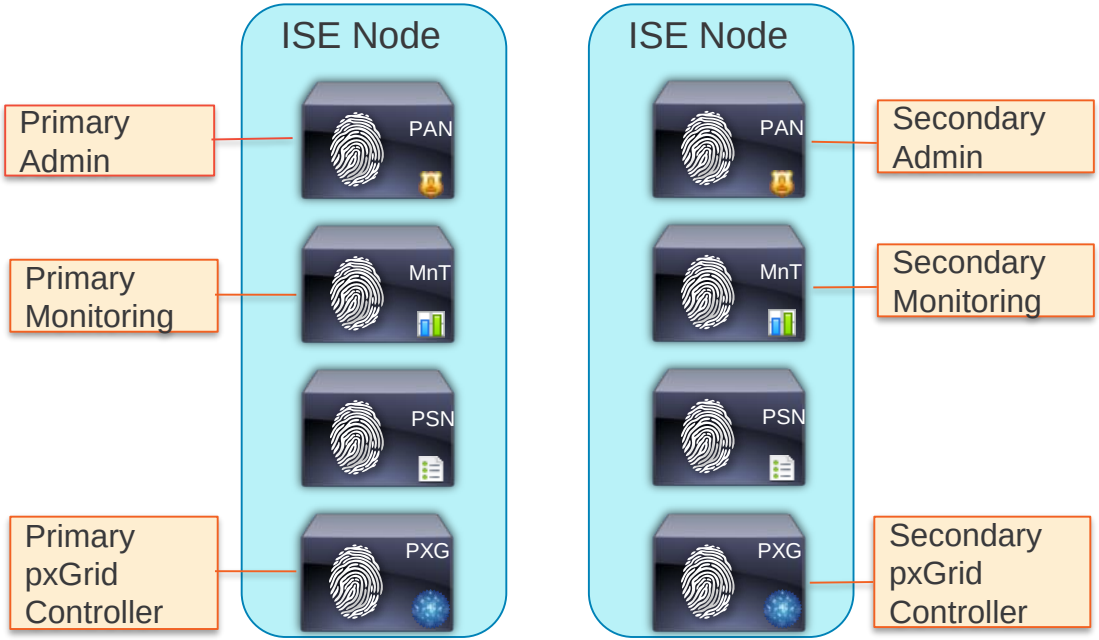
Monitoring and Troubleshooting Node

Policy Service Node

pxGrid Node

Basic 2-Node ISE Deployment (Redundant)

- Maximum sessions– 20,000 (platform dependent—same as standalone)
- Redundant sizing – 20,000 (platform dependent—same as standalone)



Distributed Persona 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
  - 5,000 for 3415 as PAN+MnT
  - 7,500 for 3515 as PAN+MnT
  - 10,000 for 3495 as PAN+MnT
  - 20,000 for 3595 as PAN+MnT

Distributed Persona Deployment

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

- 2 x Admin and 2 x Monitoring (and up to 4 x pxGrid)
- Max PSNs (Platform dependent)
  - 40 using 3495 as PAN and MnT
  - 50 using 3595 as PAN and MnT
- Max sessions (Platform dependent)
  - 250k using 3495 as PAN and MnT
  - 500k using 3595 as PAN and MnT

Sizing Guidance for ISE Nodes

34xx/35xx Scaling by Deployment/Platform/Persona

ISE 2.1+ Max Concurrent Session Counts by Deployment Model and Platform

Size	Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
		3415	5,000	0	1 / 2
		3495	10,000	0	1 / 2
		3515	7,500	0	1 / 2
		3595	20,000	0	1 / 2
		3415 as PAN+MNT	5,000	5 / 2*	2 / 7
		3495 as PAN+MNT	10,000	5 / 2*	2 / 7
		3515 as PAN+MNT	7,500	5 / 2*	2 / 7
		3595 as PAN+MNT	20,000	5 / 2*	2 / 7
optional		3495 as PAN and MNT	250,000	40 / 2	3 / 44
		3595 as PAN and MNT	500,000	50 / 4	3 / 58
		3595 as PAN and Super MnT	500,000	50 / 4	3 / 58

Scaling per PSN	Platform	Max Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3415	5,000
	SNS-3495	20,000
	SNS-3515	7,500
	SNS-3595	40,000

* 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-3415	5,000
	Large	SNS-3495	20,000
	Small (New)	SNS-3515	* 7,500
	Large (New)	SNS-3595	* 40,000
Virtual	S/L	VM	*5,000-40,000

* Under ISE 2.0.1, scaling for Small & Large 35x5 appliance same as Small & Large 34x5 appliance.

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

Sizing Production VMs to Physical Appliances

Summary

Appliance used for sizing comparison	CPU		Memory (GB)	Physical Disk (GB) **
	# Cores	Clock Rate*		
SNS-3415	4	2.4	16	600
SNS-3495	8	2.4	32	600
SNS-3515	6	2.3	16	600
SNS-3595	8	2.6	64	1,200

* 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

ISE 2.2 OVA Template

Summary

- "Eval" OVA for PoC/Lab testing up to 100 Endpoints (no resv)
- All 3xx5 templates reserve CPU and Memory
- If require more custom disk option, then deploy .iso
- Disks up to 2TB supported for greater MnT storage

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600	8	4	200GB	EVAL
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000	16	4	200GB 600GB	PSN/PXG PAN/MnT
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000	32	4	200GB 600GB	PSN/PXG PAN/MnT
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	6	2.0	16,000	16	6	200GB 600GB	PSN/PXG PAN/MnT
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	8	2.0	16,000	64	6	200GB 1.2TB	PSN/PXG PAN/MnT

Example: ISE-2.3.0.298-virtual-200GB-SNS3515.ova

Resource Reservations

ISE Platform Properties

Minimum VM Resource Allocation

Minimum CPU Cores	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	“Super MnT”

- Least Common Denominator used to set platform.
- Example:
  4 cores
  32GB RAM
  = UCS_SMALL

More to come!

Why Do I Care?

Because memory, max sessions, and other table spaces are based on Persona and Platform Profile

ISE 2.2 OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600	8	4	200GB	EVAL
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000	16	4	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000	32	4	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	6	2.0	16,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	8	2.0	16,000	64	6	200GB	PSN/PXG
						1.2TB	PAN/MnT

ISE Platform Properties

Minimum VM Resource Allocation

Minimum CPU Cores	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	“Super MnT”

- Least Common Denominator used to set platform.
- Example:
  4 cores
  32GB RAM
  = UCS_SMALL

Assumes HyperThreading Enabled

ISE 2.2 OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600				
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000				
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000				
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	~~6~~ 12	2.0	16,000				
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	~~8~~ 16	2.0	16,000				

For 35x5 ISE VMs, HyperThreading is Mandatory, unless you double ($$) the *physical* cores allocated to VM !!

CSCvh71644 - VMware OVA templates for SNS-35xx are not detected correctly…

ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

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

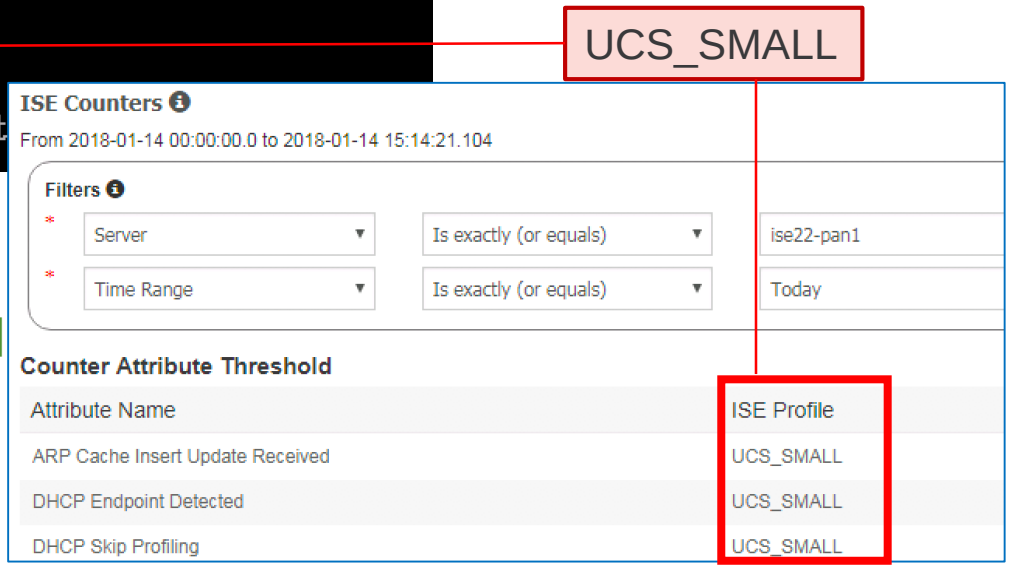
```
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:

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

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

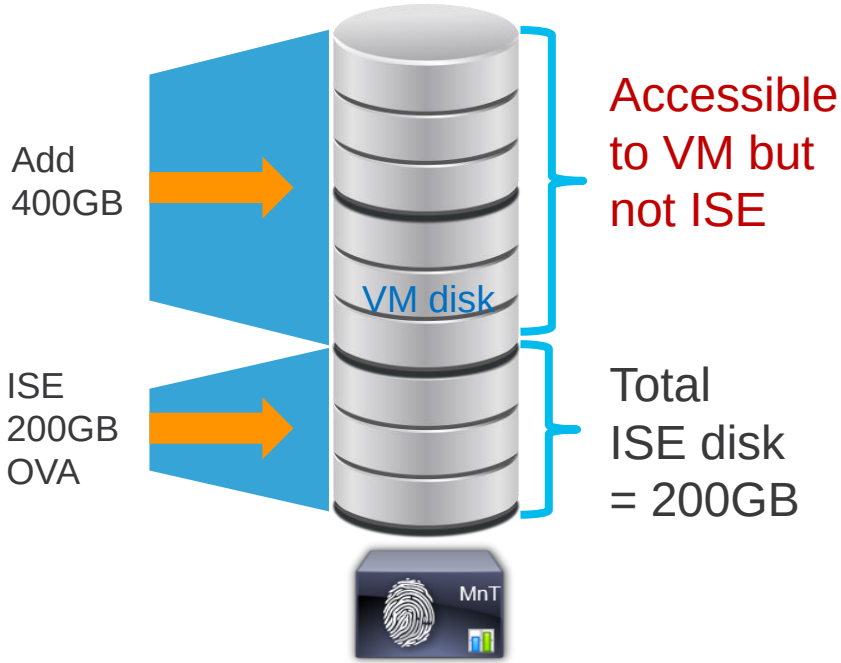
    (Under ISE Profile column)



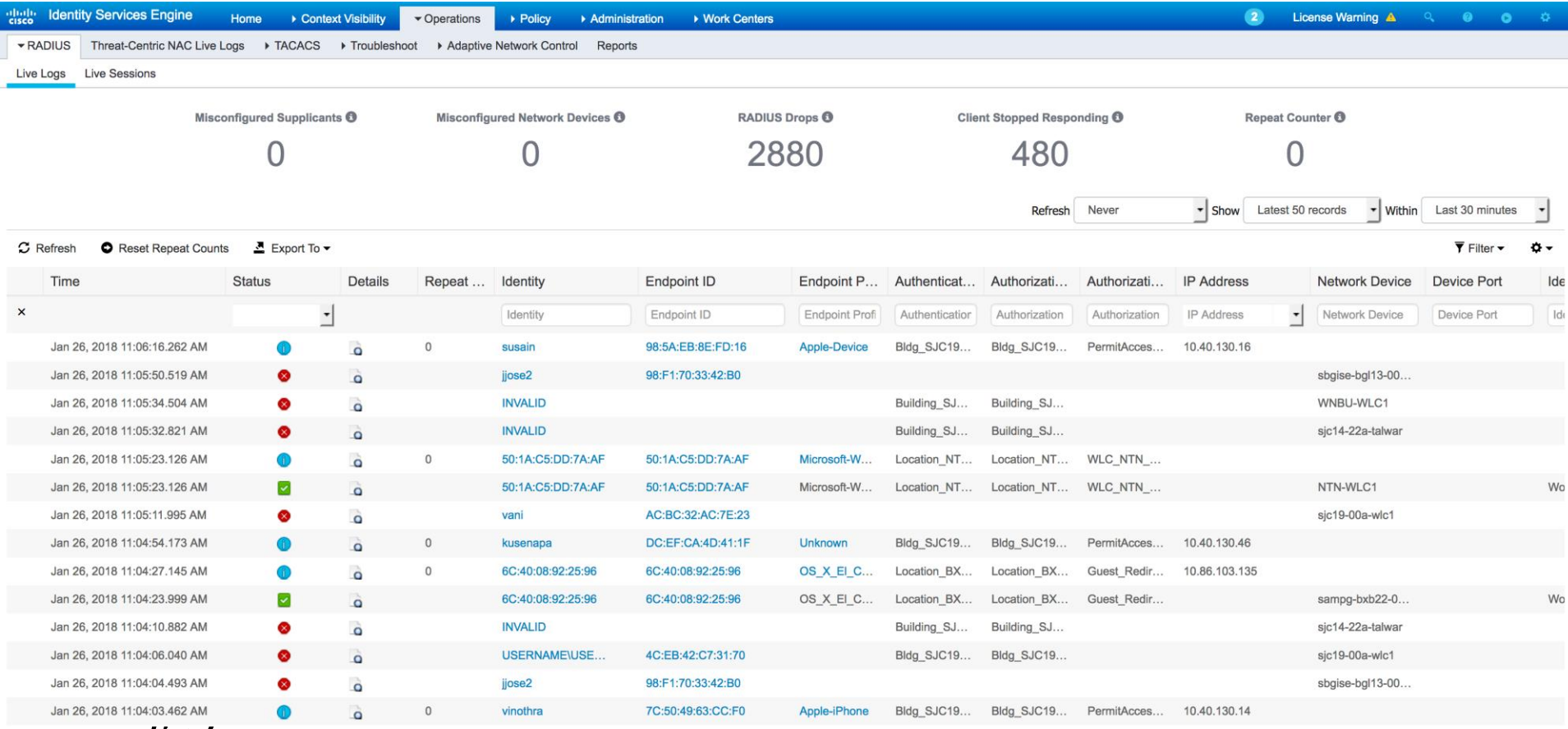
VM Disk Allocation

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 larger OVA (ISE 2.2)



ISE 2.4 MnT -- Fast Access to Logs and Reports



Introducing “Super” MnT

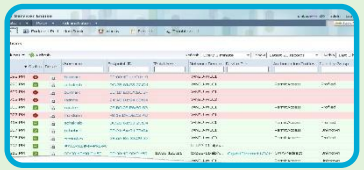
For Any Deployment where High-Perf MnT Operations Required

- Virtual Appliance Only option in ISE 2.4
- 3595 specs + 256 GB
  - 8 cores @ 2GHz min (16000+ MHz)
  - 256GB RAM
  - Up to 2TB* disk w/ fast I/O
- Fast I/O Recommendations:
  - Disk Drives (10k/15k RPM or SSD)
  - Fast RAID w/Caching (ex: RAID 10)
  - More disks (ex: 8 vs 4)

* CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB

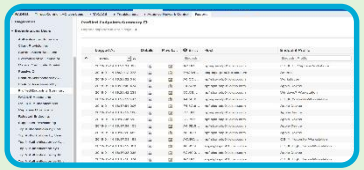
ISE 2.4 MnT Vertical Scaling Scaling Enhancements

Benefits MnT on ALL ISE platforms



Faster Live Log Access

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



Faster Report & Export Performance

- Report related tables pinned into memory for faster retrieval.
- Optimise 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 optimisations resulting in up to 80% efficiencies

Flash Removal

And no Yahoo! User Interface Library (YUI)

- “No Flash”
- C’mon, you mean just a little bit of flash, right?
- No. I’m Saying No Flash! There is no Flash in this product!

MnT Node Log Storage Requirements for RADIUS

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
5,000	504	1007	1510	2577	5154
10,000	252	504	755	1289	2577
25,000	101	202	302	516	1031
50,000	51	101	151	258	516
100,000	26	51	76	129	258
150,000	17	34	51	86	172
200,000	13	26	38	65	129
250,000	11	21	31	52	104
500,000	6	11	16	26	52

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

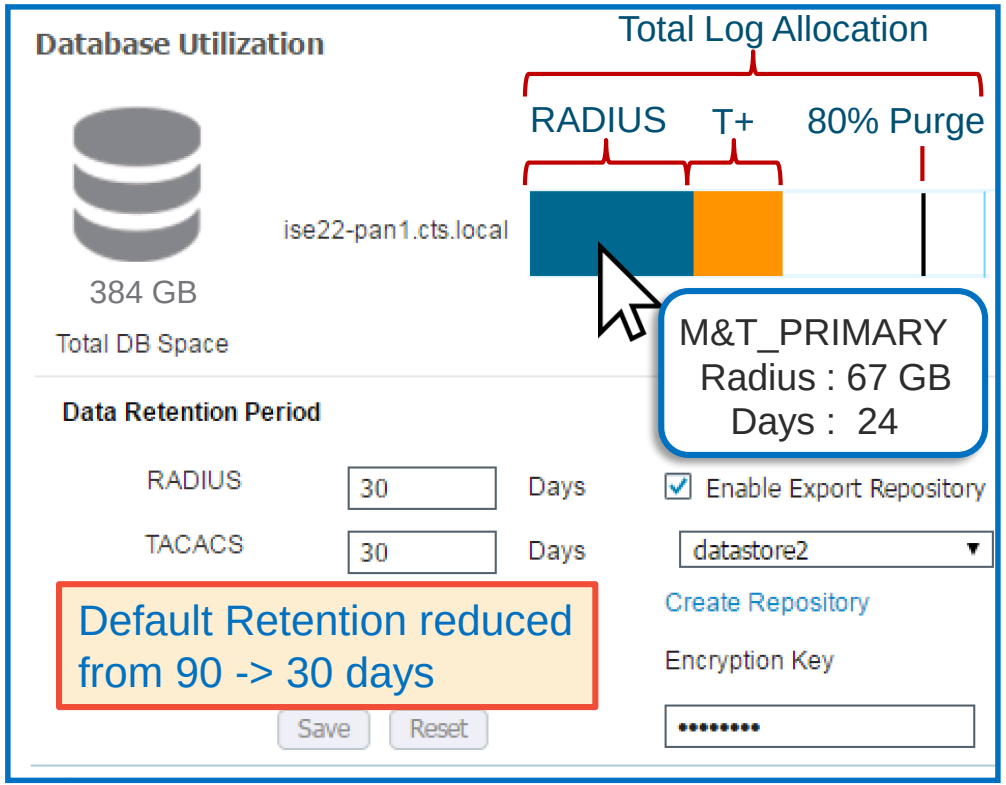
Based on 60% allocation of MnT disk to RADIUS logging
(Prior to ISE 2.2, only 30% allocations)

RADIUS and TACACS+

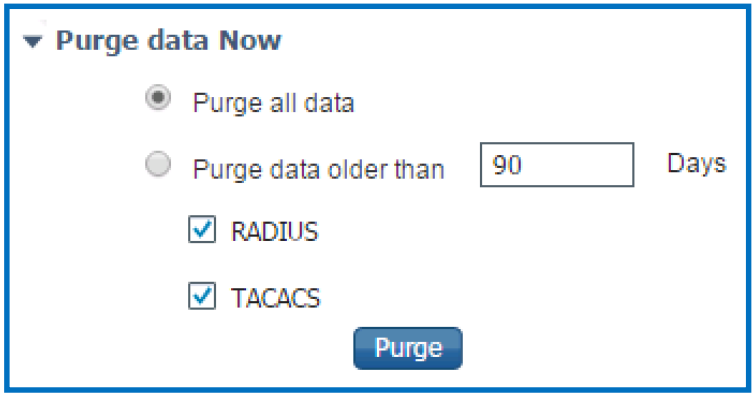
MnT Log Allocation

ISE 2.2+

- Administration > System > Maintenance > Operational Data Purging



- 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



ISE VM Provisioning & Disk IO Guidance

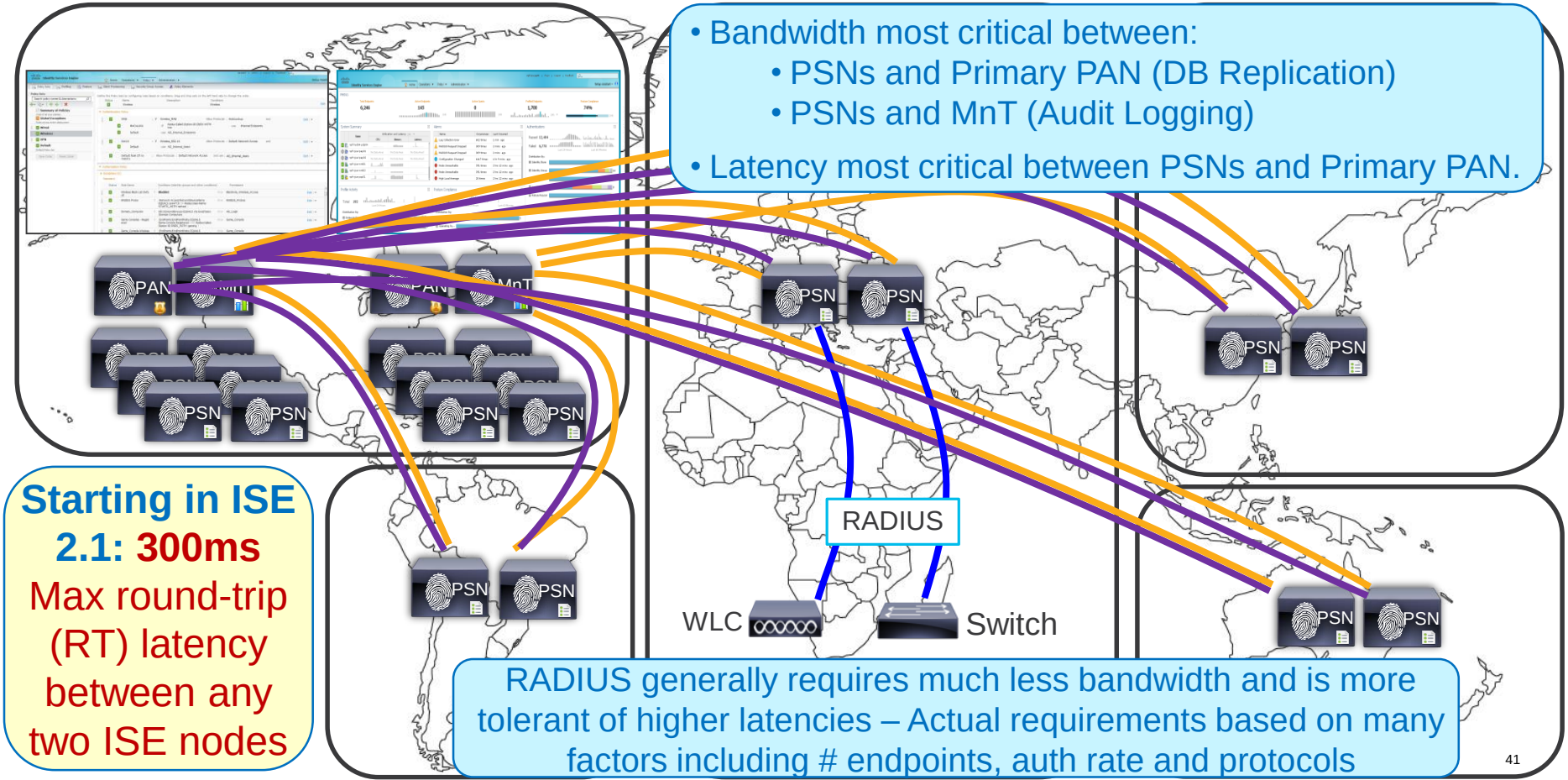
- VMotion supported but storage VMotion not tested.
- Thin Provisioning supported (recommend Thick Provisioning for MnT)
- Hyper-Threading is mandatory for 3595-based VMs (Sizing assumes HT enabled, but HT does not double # physical cores! Reservations based on physical cores)
- IO Performance Requirements:
  - 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*

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

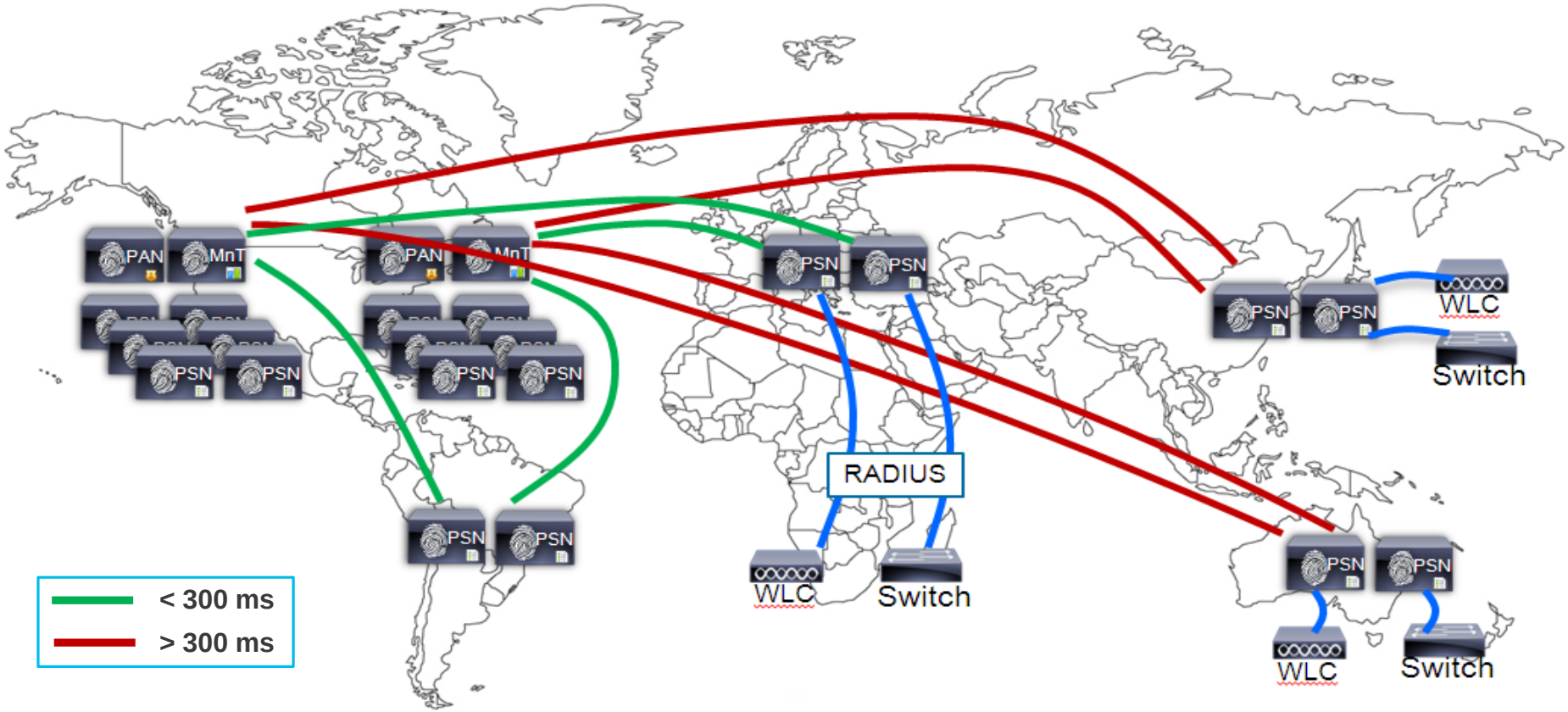
*RAID performance levels: http://www.datarecovery.net/articles/raid-level-comparison.html
http://docs.oracle.com/cd/E19658-01/820-4708-13/appendixa.html

Bandwidth and Latency

Bandwidth and Latency

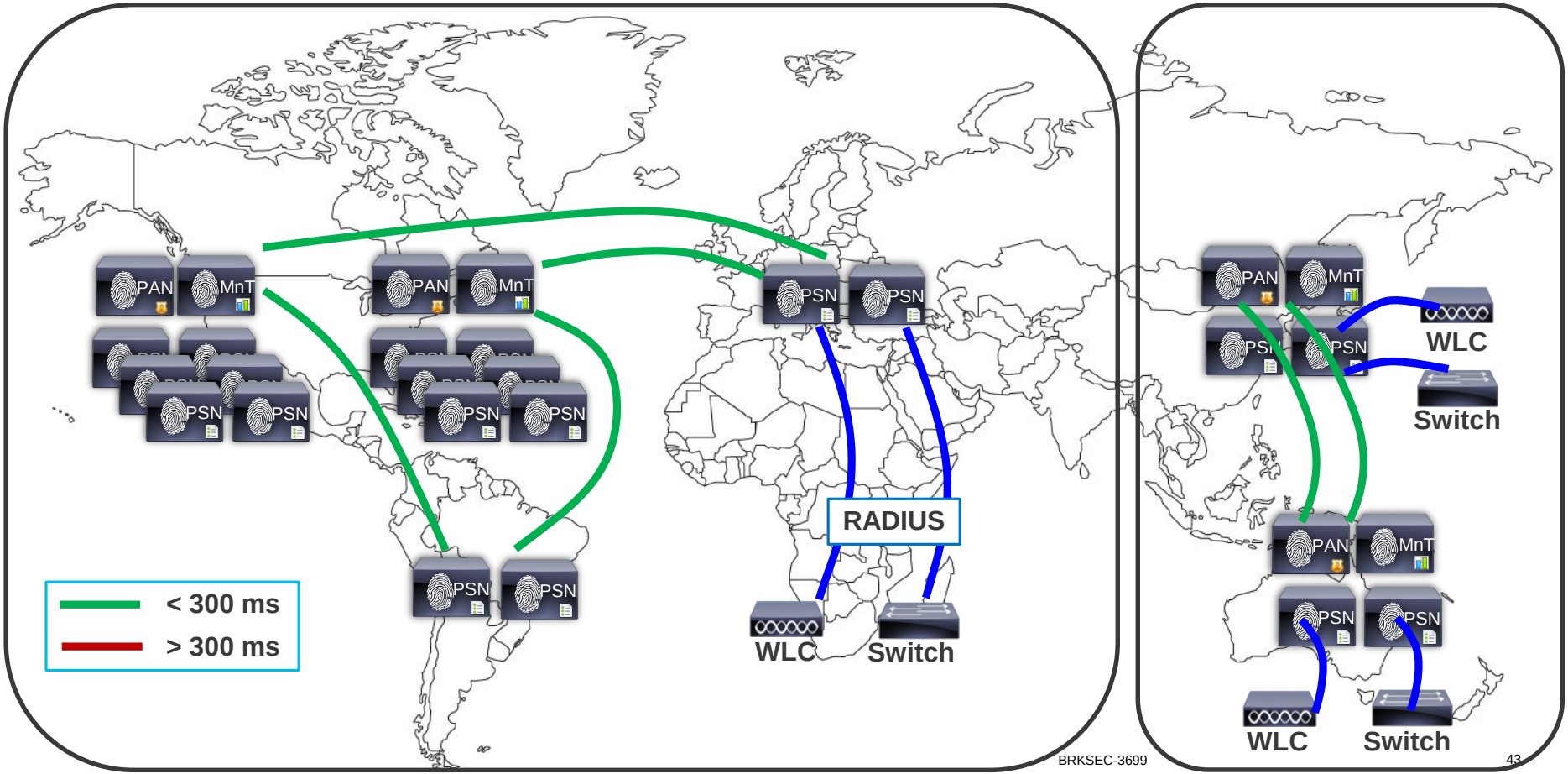


What if Distributed PSNs > 300ms RTT Latency?



Option #1: Deploy Separate ISE Instances

Per-Instance Latency < 300ms



Scaling ISE Services

Scaling ISE Services Agenda

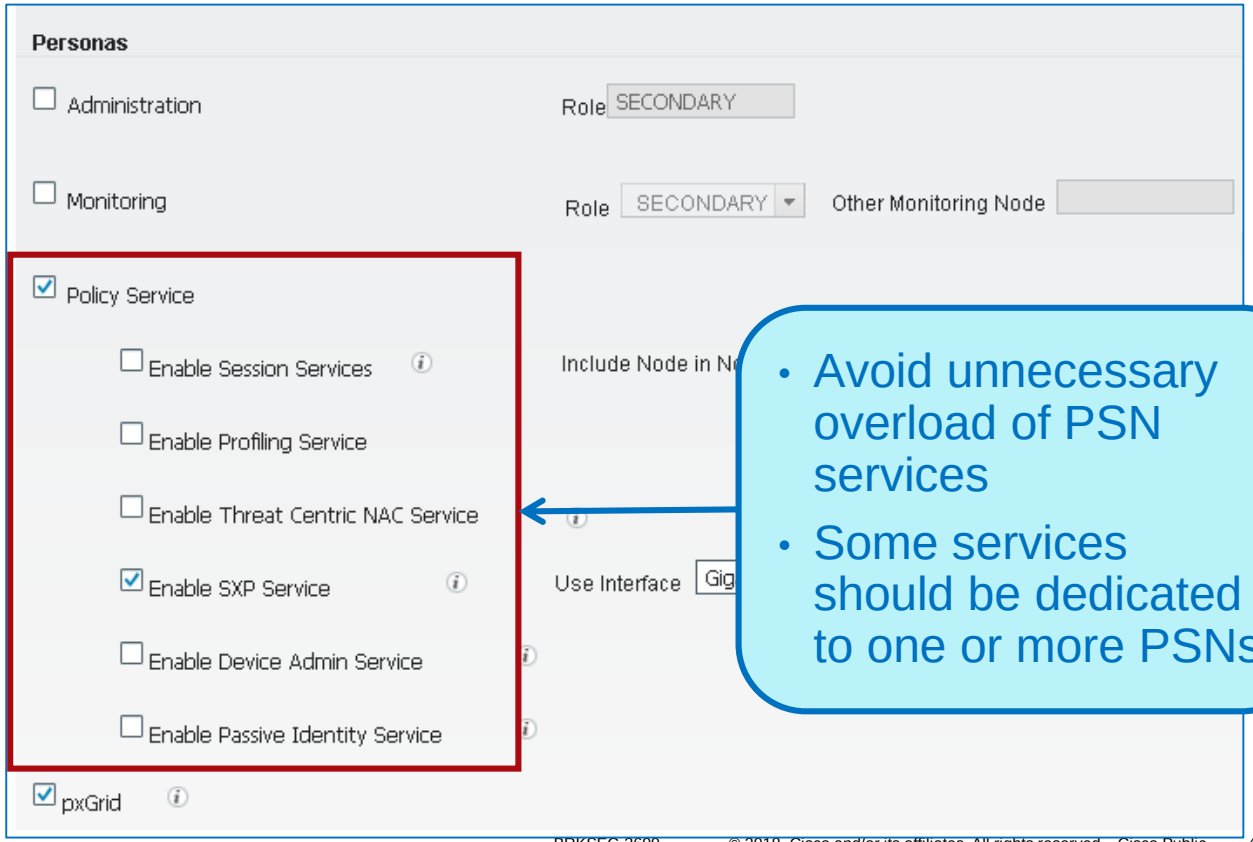
- AAA and Auth Policy Tuning
- Active Directory and LDAP Integration
- Passive Identity and Easy Connect
- Guest and Web Authentication and Location Services
- Compliance Services—Posture and MDM
- TACACS+ Design and Scaling
- Profiling and Database Replication
- MnT (Optimise Logging and Noise Suppression)

ISE Personas and Services

Enable Only What Is Needed !!

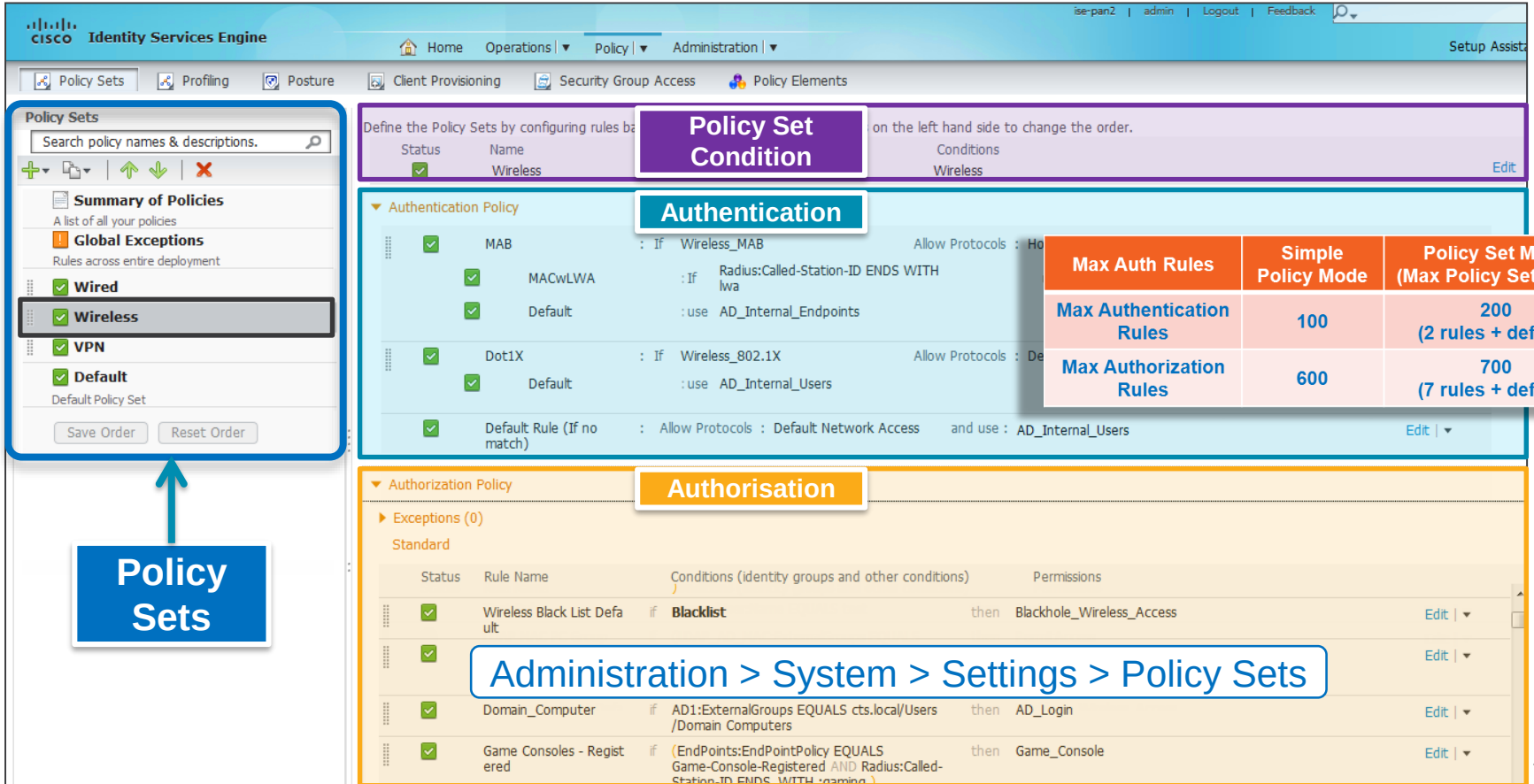
Session Services includes base user services such as RADIUS, Guest, Posture, MDM, BYOD/CA

- ISE Personas:
  - PAN
  - MNT
  - PSN
  - pxGrid
- PSN Services
  - Session
  - Profiling
  - TC-NAC
  - ISE SXP
  - Device Admin (TACACS+)
  - Passive Identity (Easy Connect)



Auth Policy Optimisation (ISE 2.2 and Earlier)

Leverage Policy Sets to Organise and Scale Policy Processing

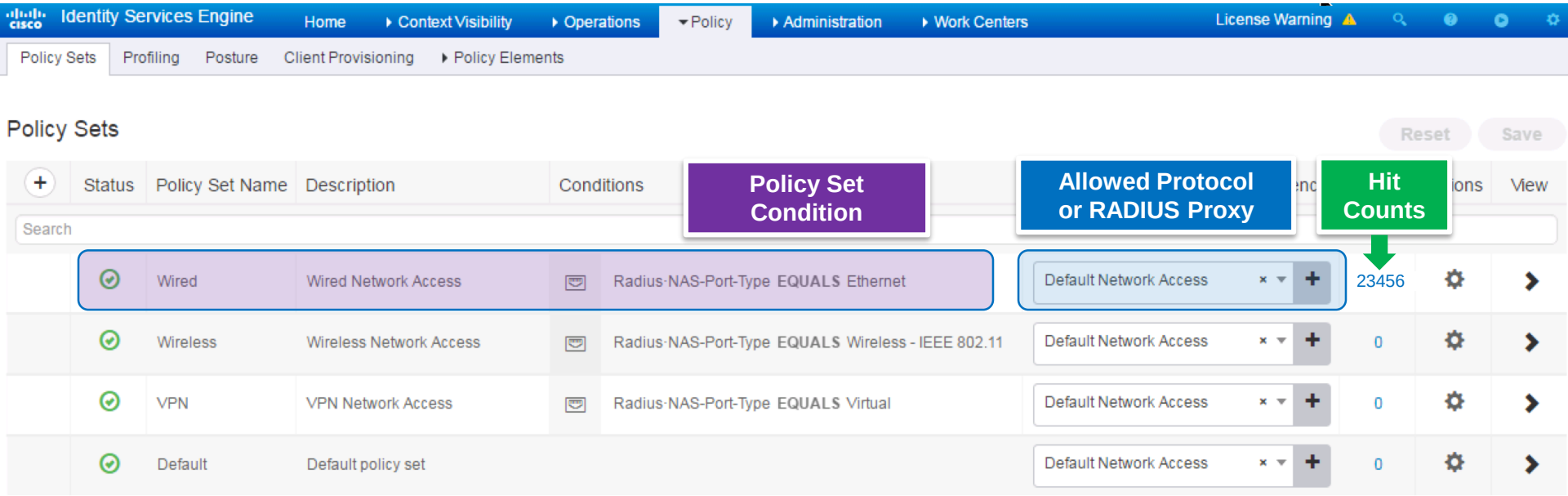


Max Auth Rules	Simple Policy Mode	Policy Set Mode (Max Policy Sets=100)
Max Authentication Rules	100	200 (2 rules + default)
Max Authorization Rules	600	700 (7 rules + default)

Policy Sets

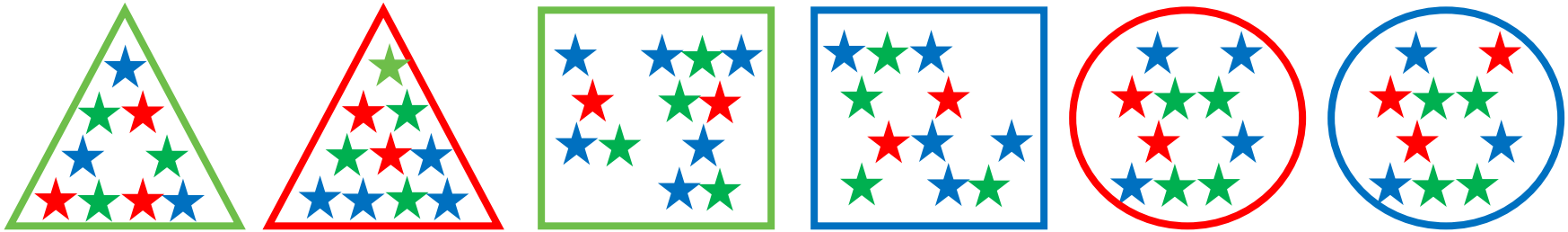
Standard Equipment under new ISE 2.3 Policy User Interface

- No Authentication Outer Rule – Now part of Policy Set



Search Speed Test

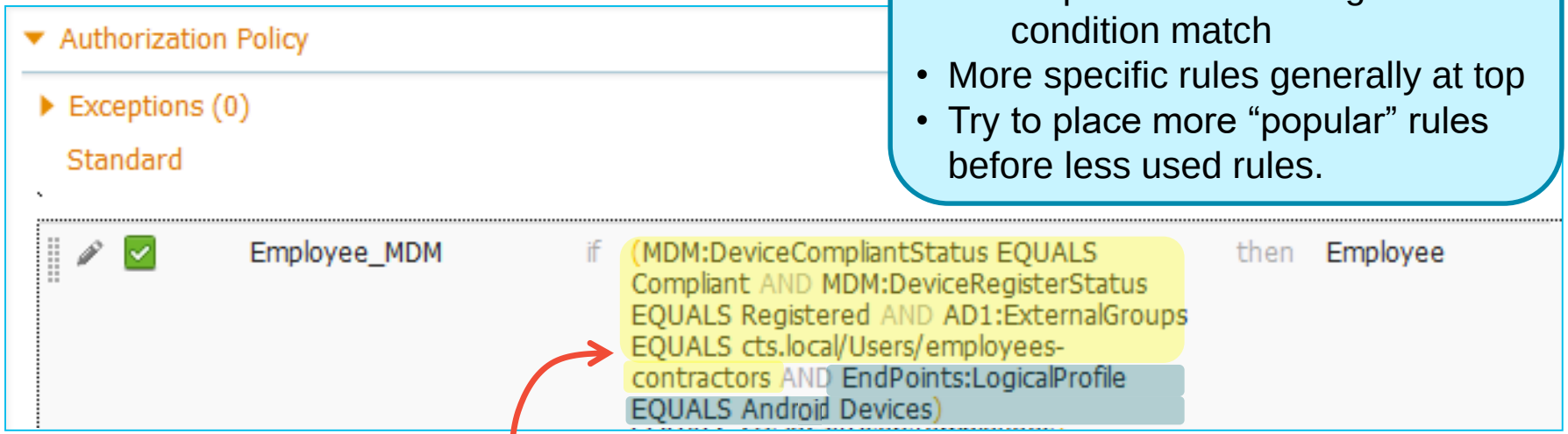
- Find the object where…
  - Total stars = 10
  - Total green stars = 4
  - Total red stars = 2
  - Outer shape = Red Triangle



Auth Policy Optimisation

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.

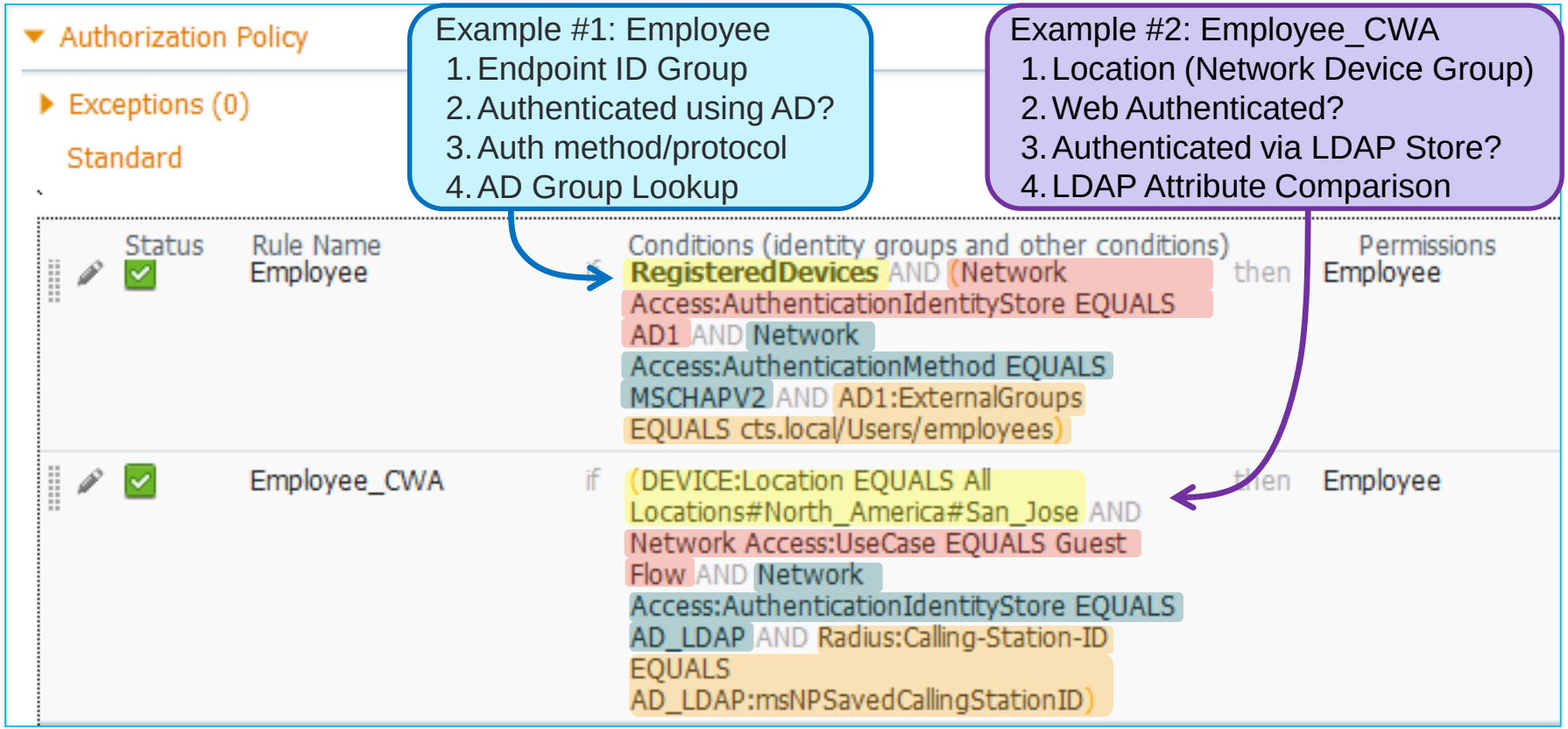


Example of a Poor Rule: Employee_MDM

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

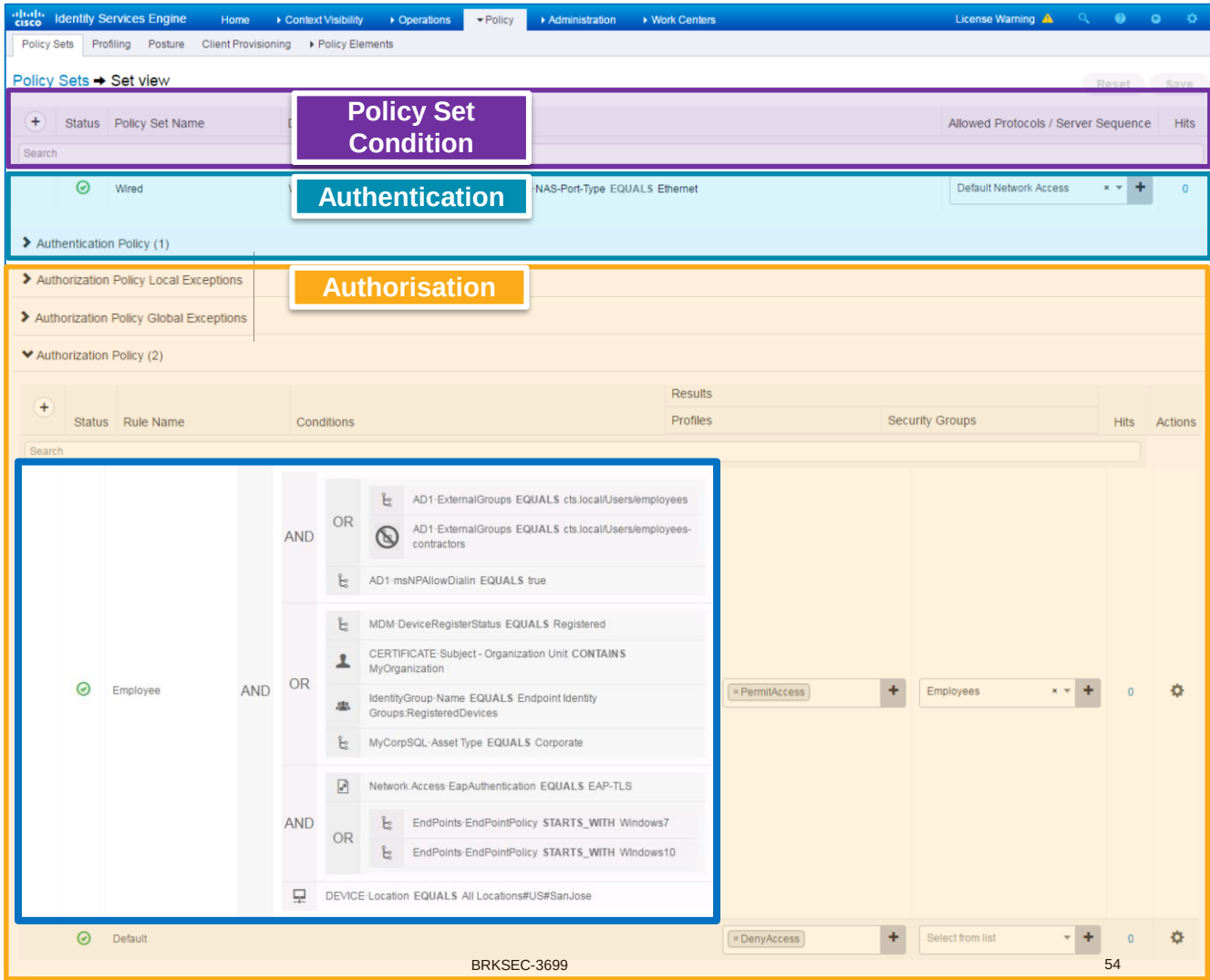
Auth Policy Optimisation

Rule Sequence and Condition Order is Important!



Auth Policy

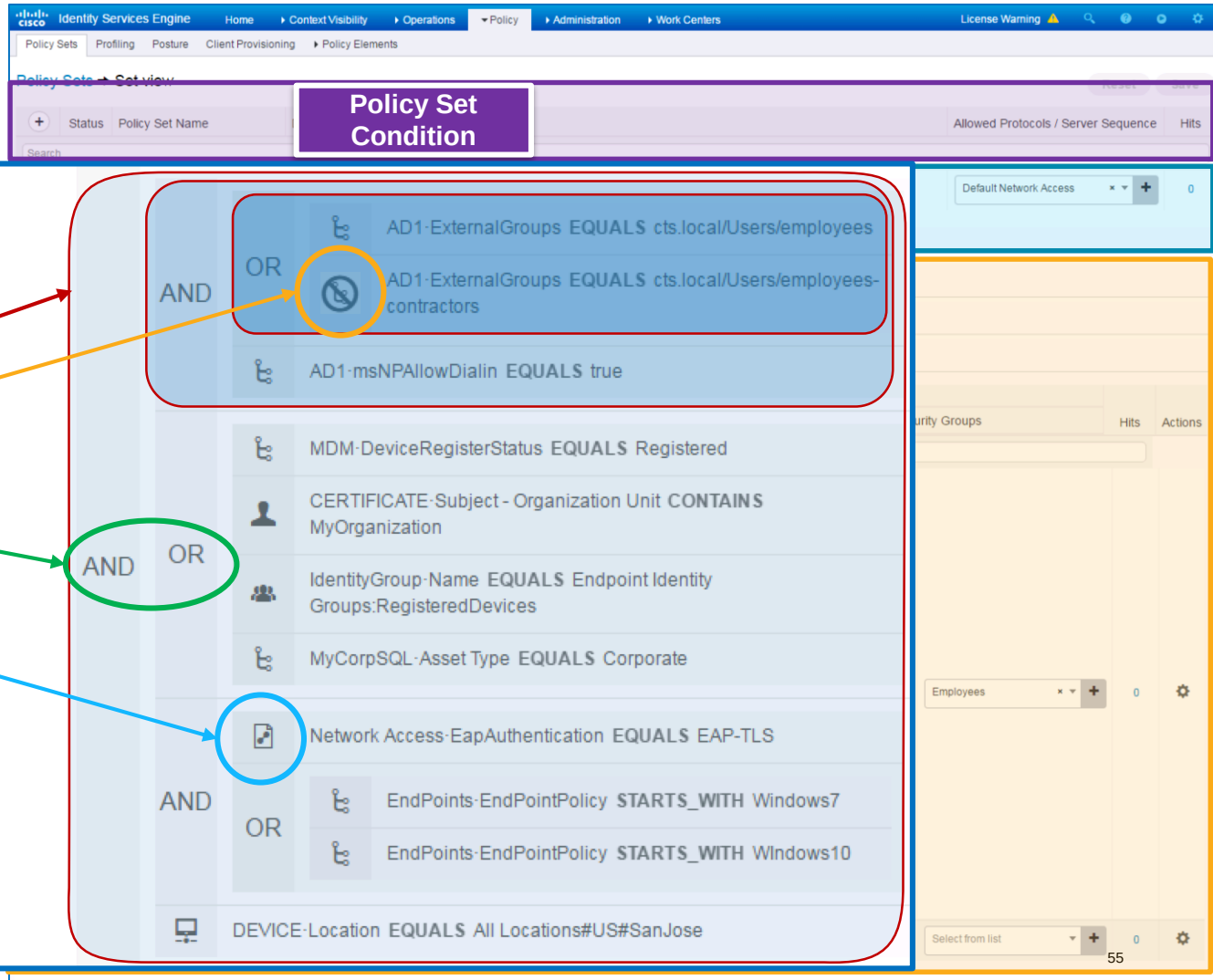
ISE 2.3 Example



Auth Policy

ISE 2.3 Example

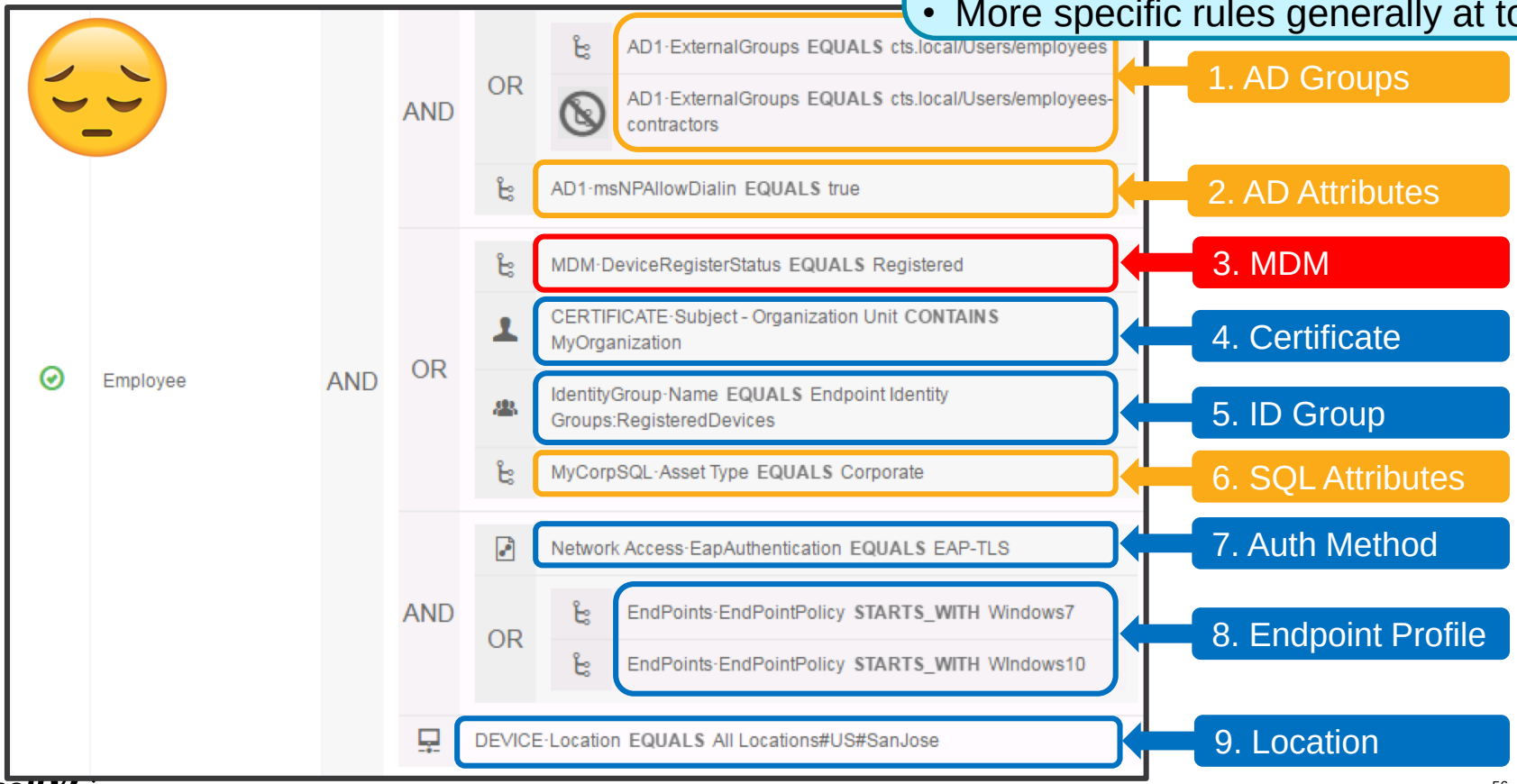
- Nested Conditions
- “IS NOT” insertion
- Simplified Boolean (AND/OR) logic
- Condition Library with Drag & Drop
- Rule Hit Counts



Auth Policy Optimisation

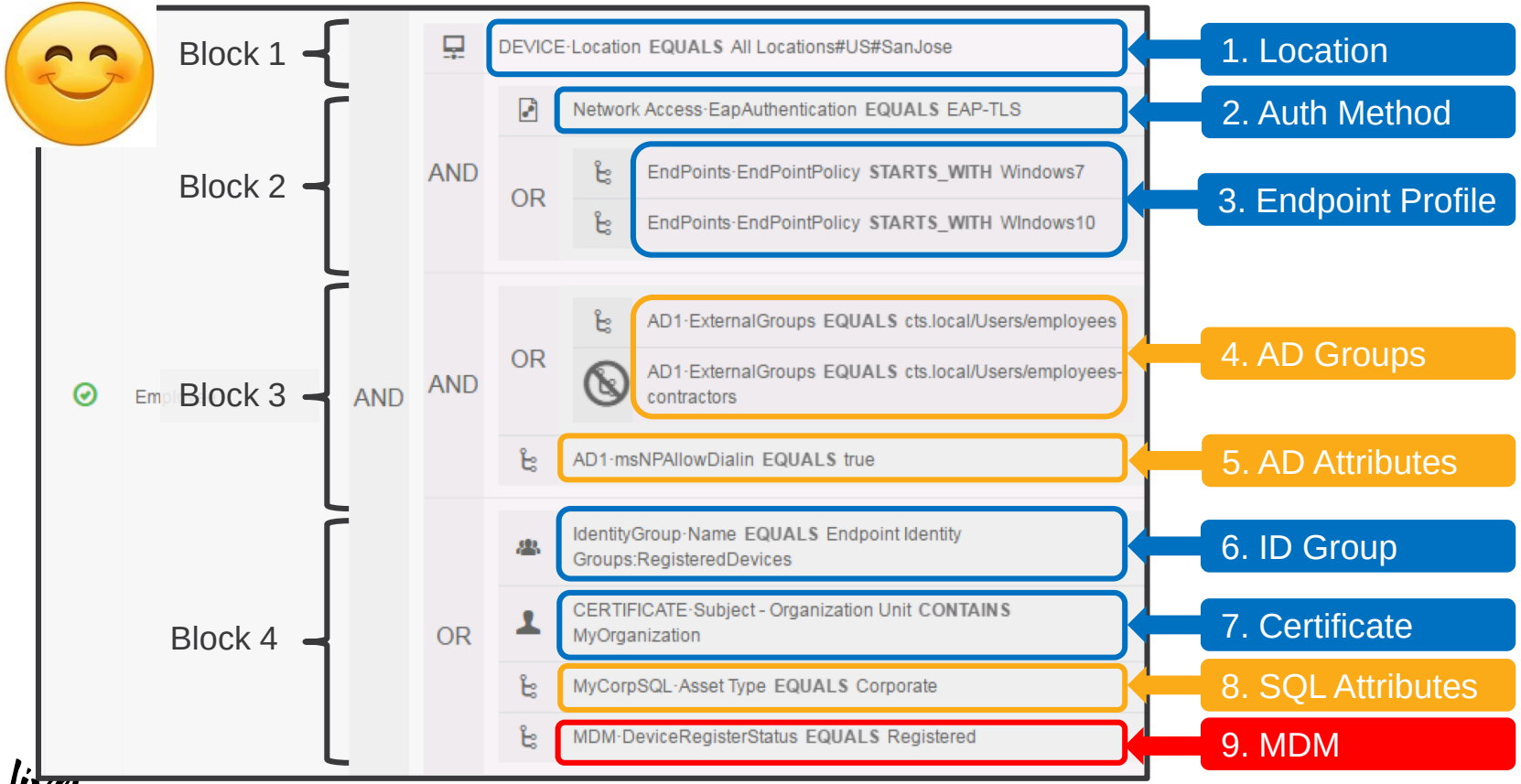
ISE 2.3 Bad Example

- Policy Logic:
  - First Match, Top Down
  - Skip Rule on first negative match
- More specific rules generally at top



Auth Policy Optimisation

ISE 2.3 Better Example!



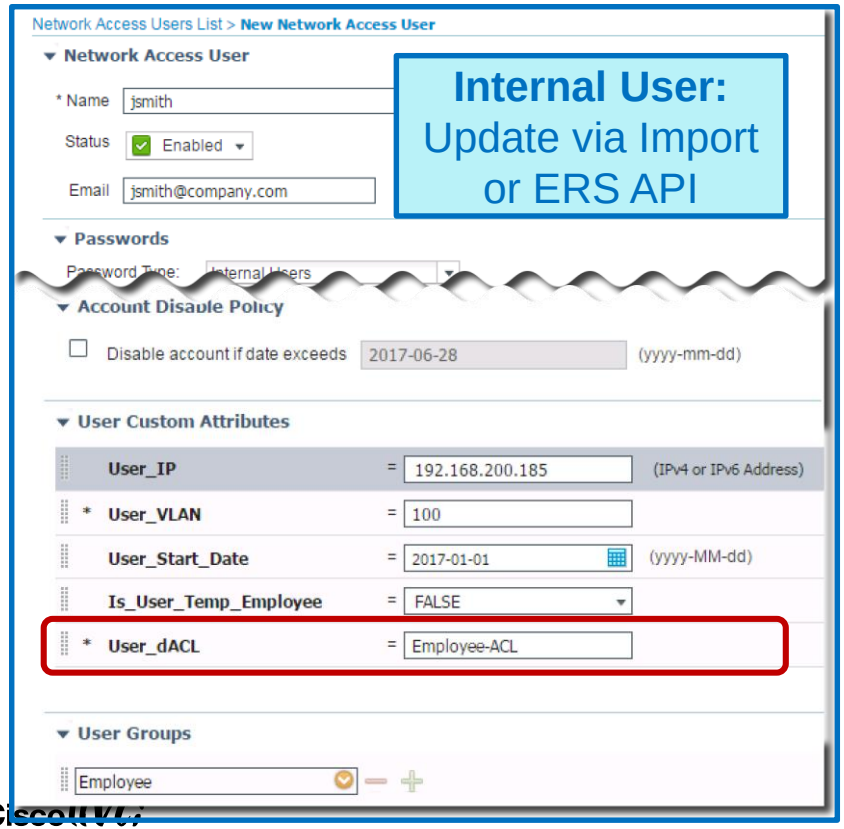
ISE 2.4 Auth Policy Scale

- Max Policy Sets = **200**
  (up from 100 in 2.2; up from 40 in 2.1)
- Max Authentication Rules = **1000**
  (up from 200 in 2.2; up from 100 in 2.1)
- Max Authorisation Rules = **3000**
  (up from 700 in 2.2; up from 600 in 2.1)
- Max Authorisation Profiles = **3200**
  (up from 1000 in 2.2; up from 600 in 2.1)

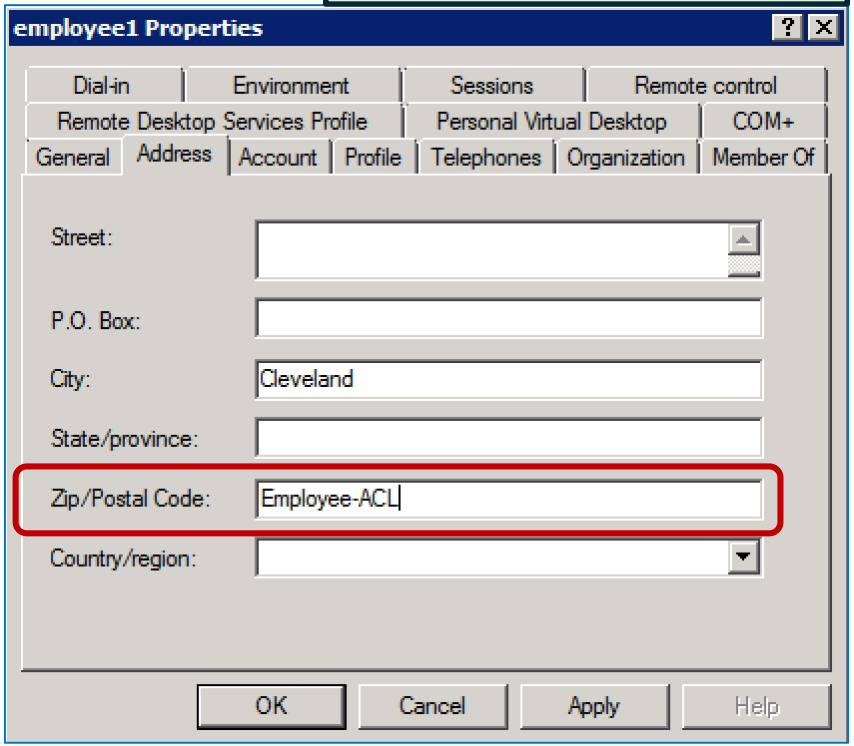
Dynamic Variable Substitution - Example

Populate Internal / External User

External User:
AD / LDAP / SQL / OTP



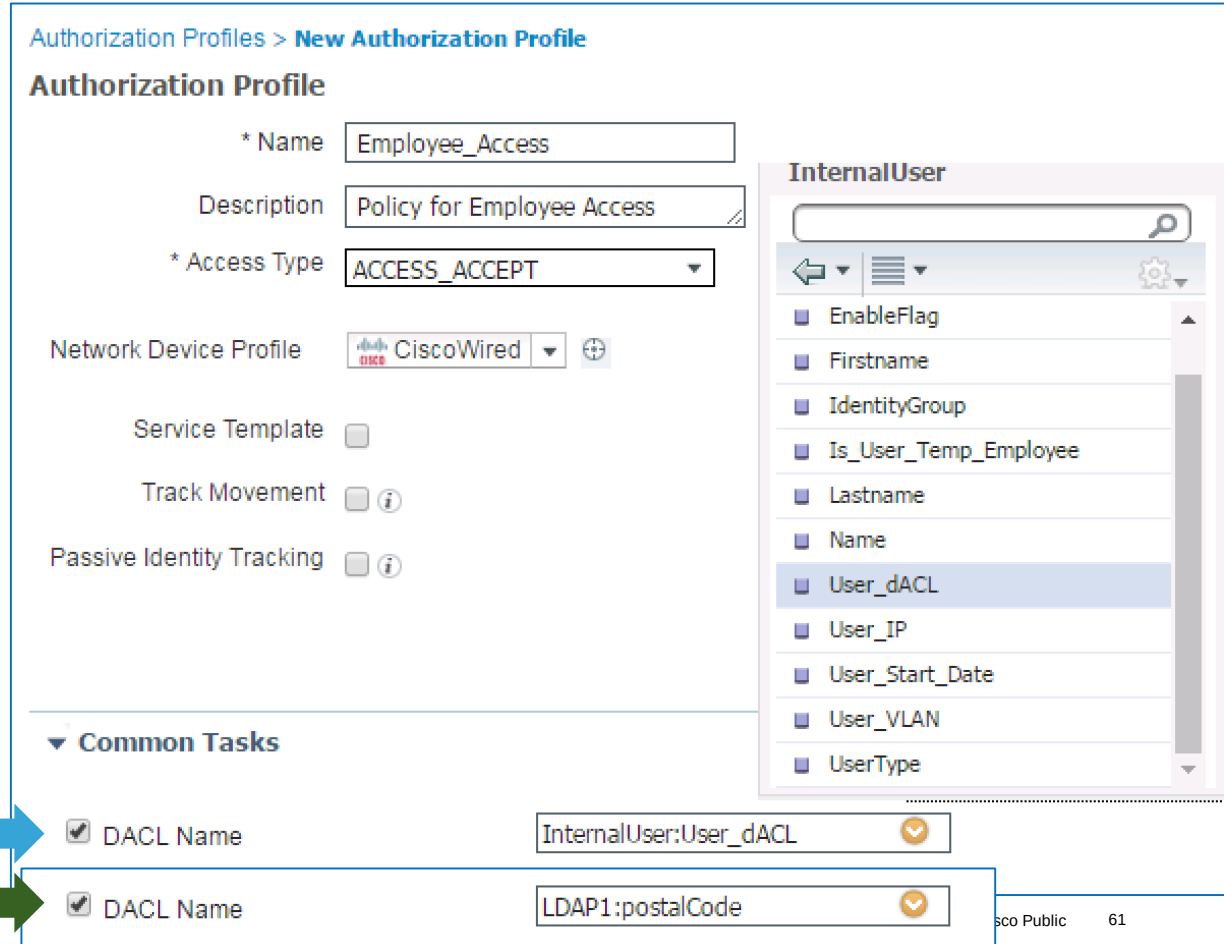
Internal User:
Update via Import or ERS API



Dynamic DACLs in Authorisation Profile

Per-User Policy in 1 rule

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

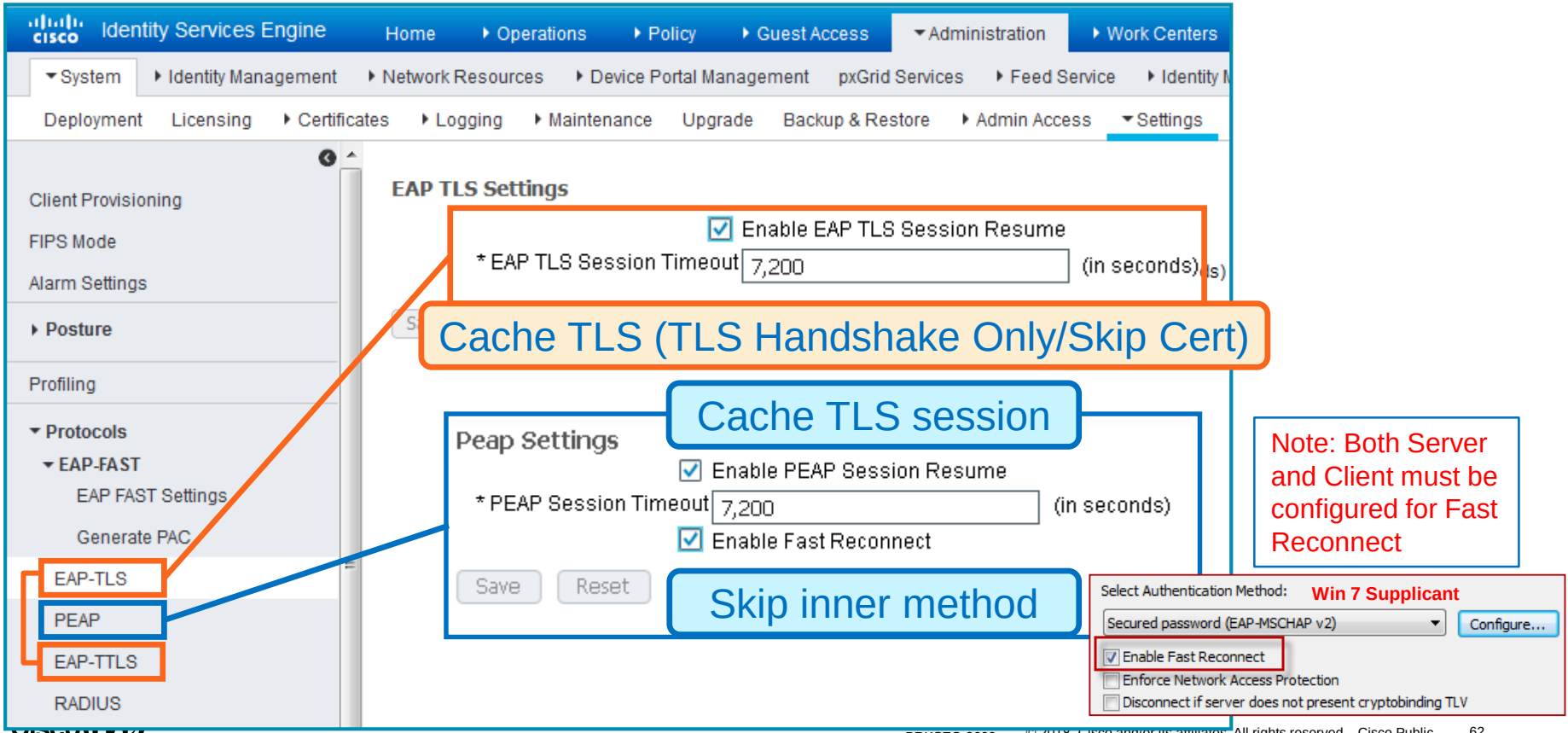


Internal User example

External User example

Enable EAP Session Resume / Fast Reconnect

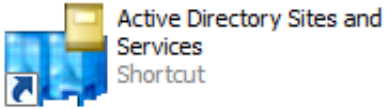
Major performance boost, but not complete auth so avoid excessive timeout value



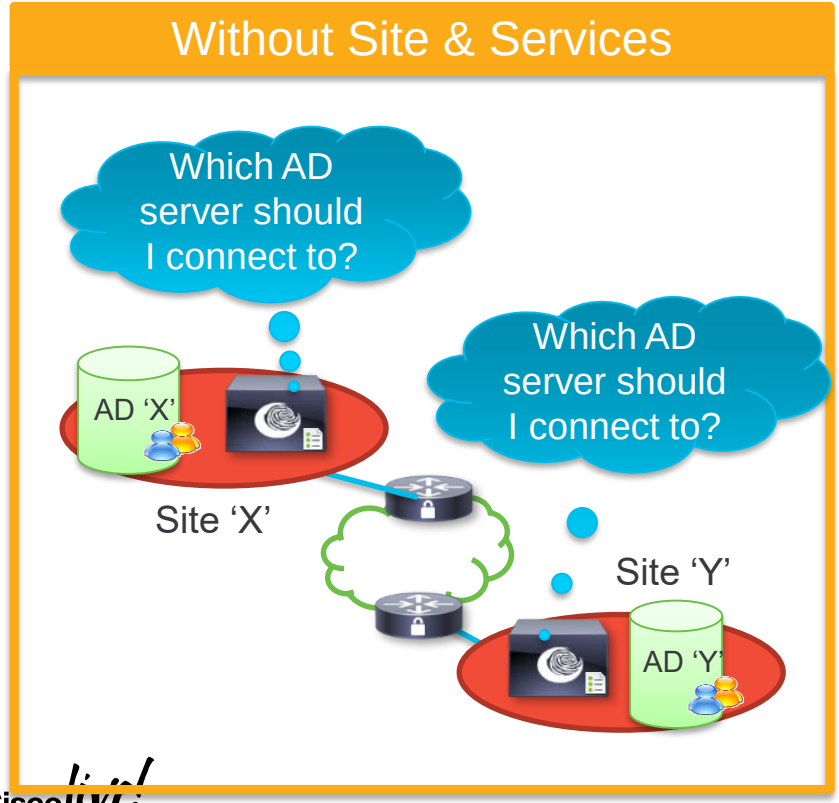
Scaling AD and LDAP Integration

Scaling AD Integration w/ Sites & Services

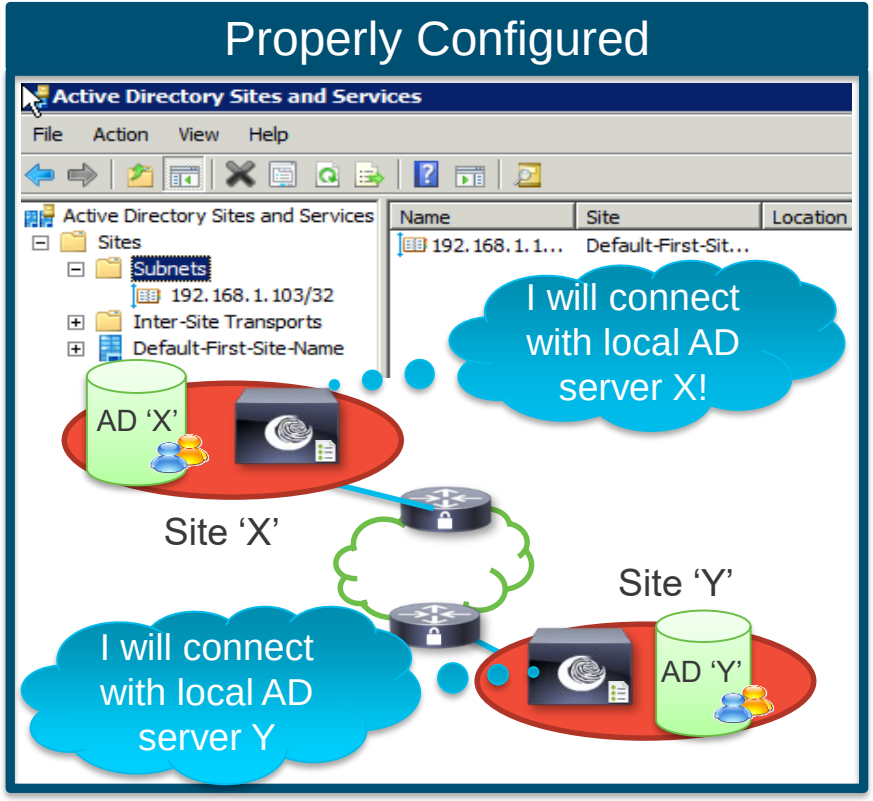
How do I ensure Local PSN is connecting to Local AD controller?



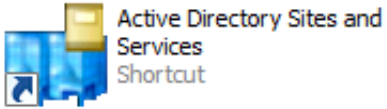
Without Site & Services



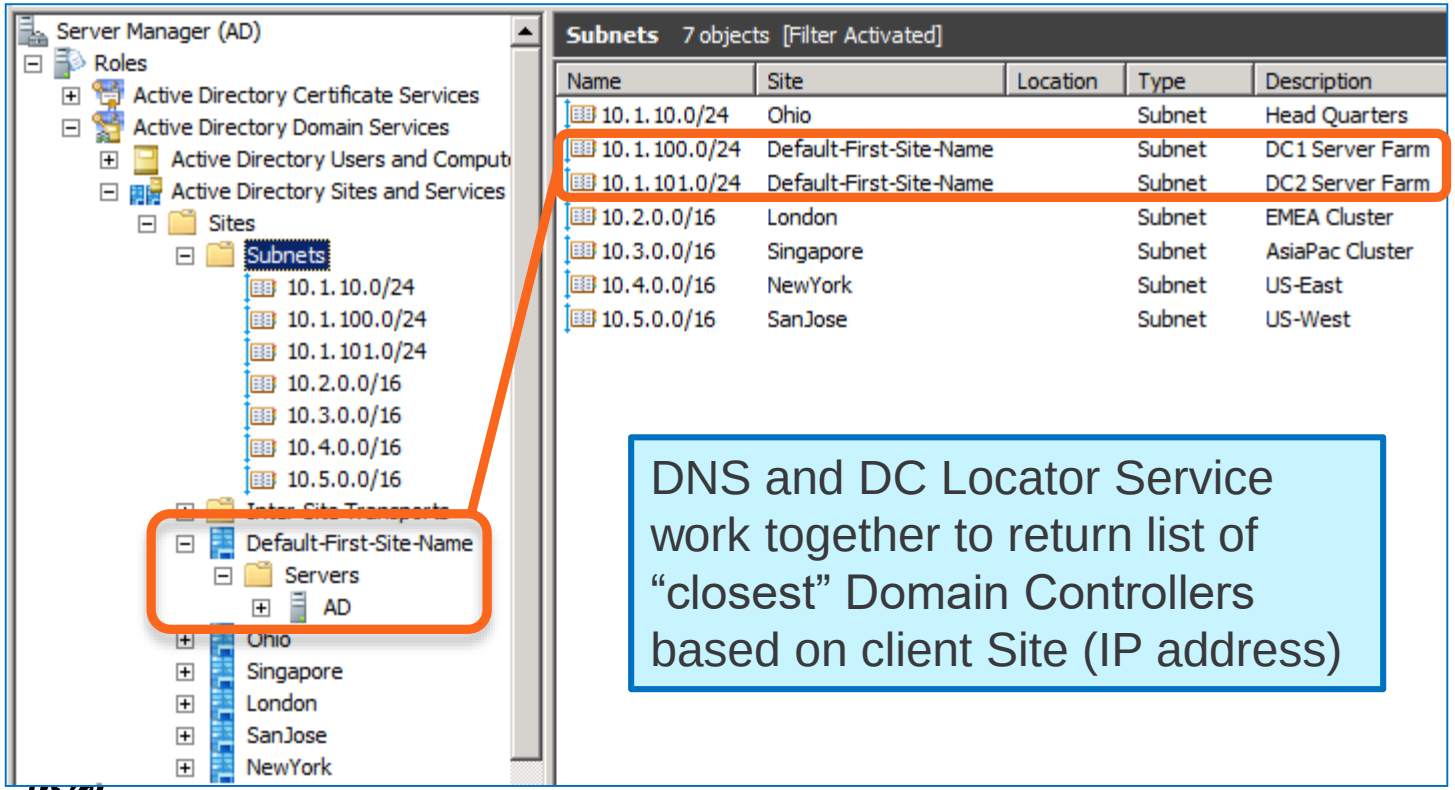
Properly Configured



AD Sites and Services



Links AD Domain Controllers to ISE Servers Based on IP Address

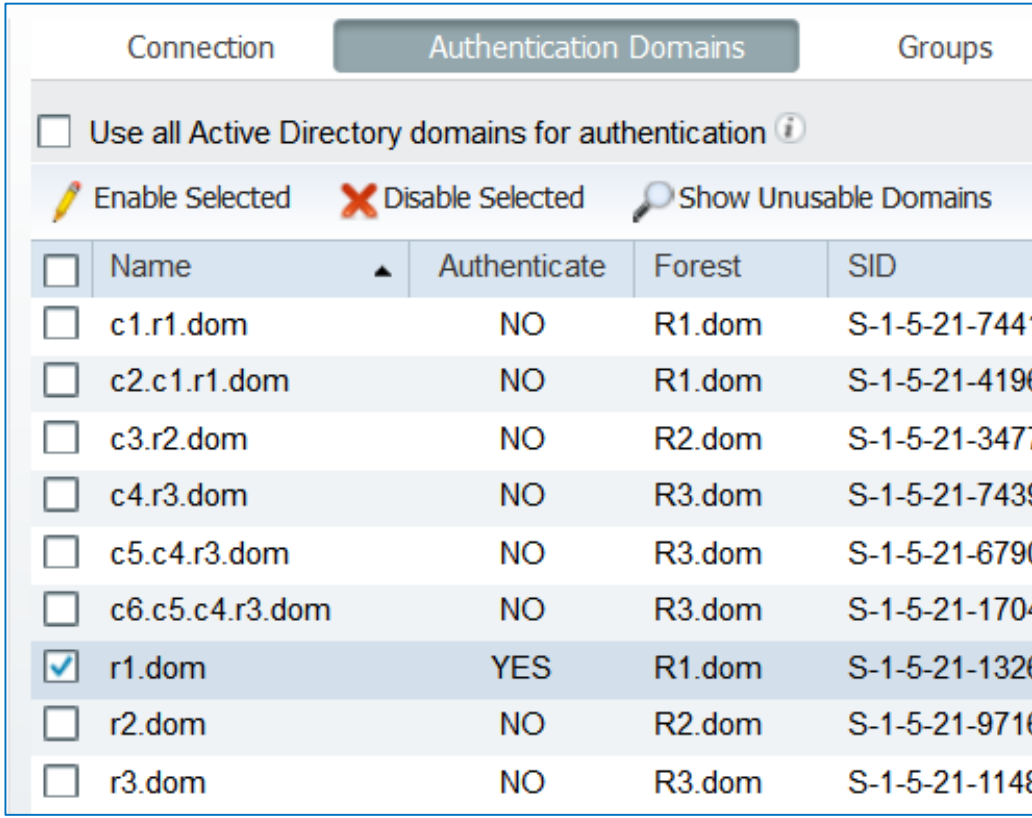


Authentication Domains (Whitelisting)

- “Whitelist” only the domains of interest—those used for authentication!
- In this example, the join point can see many trusted domains but we only care about r1.dom

Enable r1.dom

And disable the rest

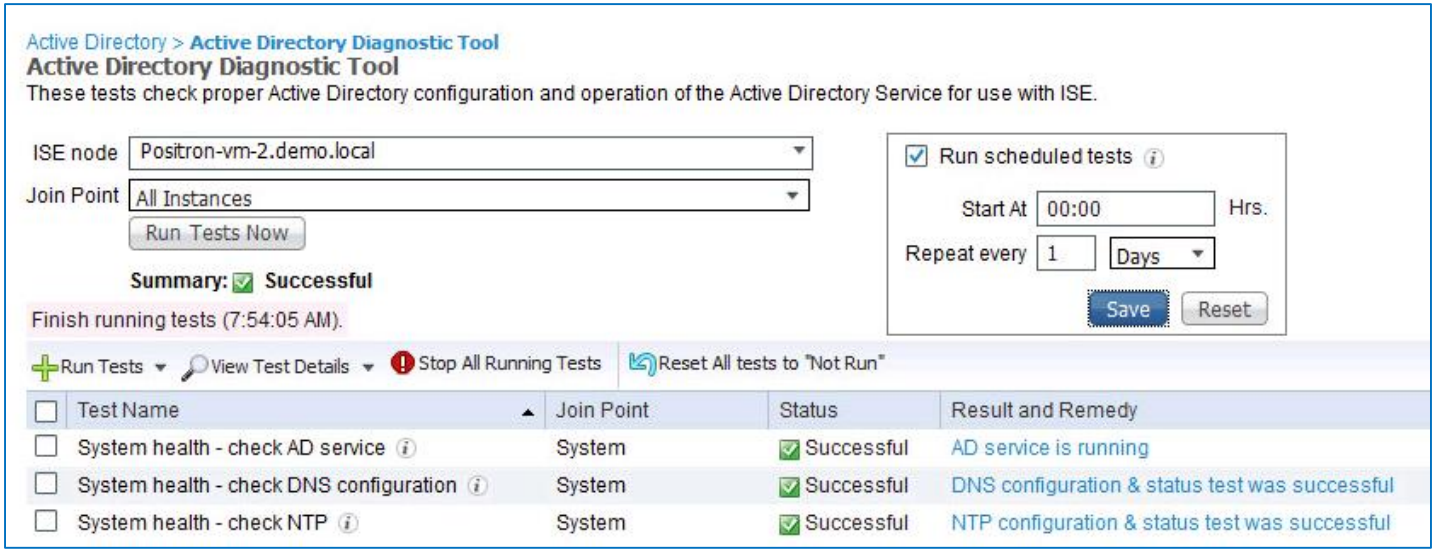


AD Background Diagnostics

Schedule Periodic Testing to Verify AD Connectivity and Health

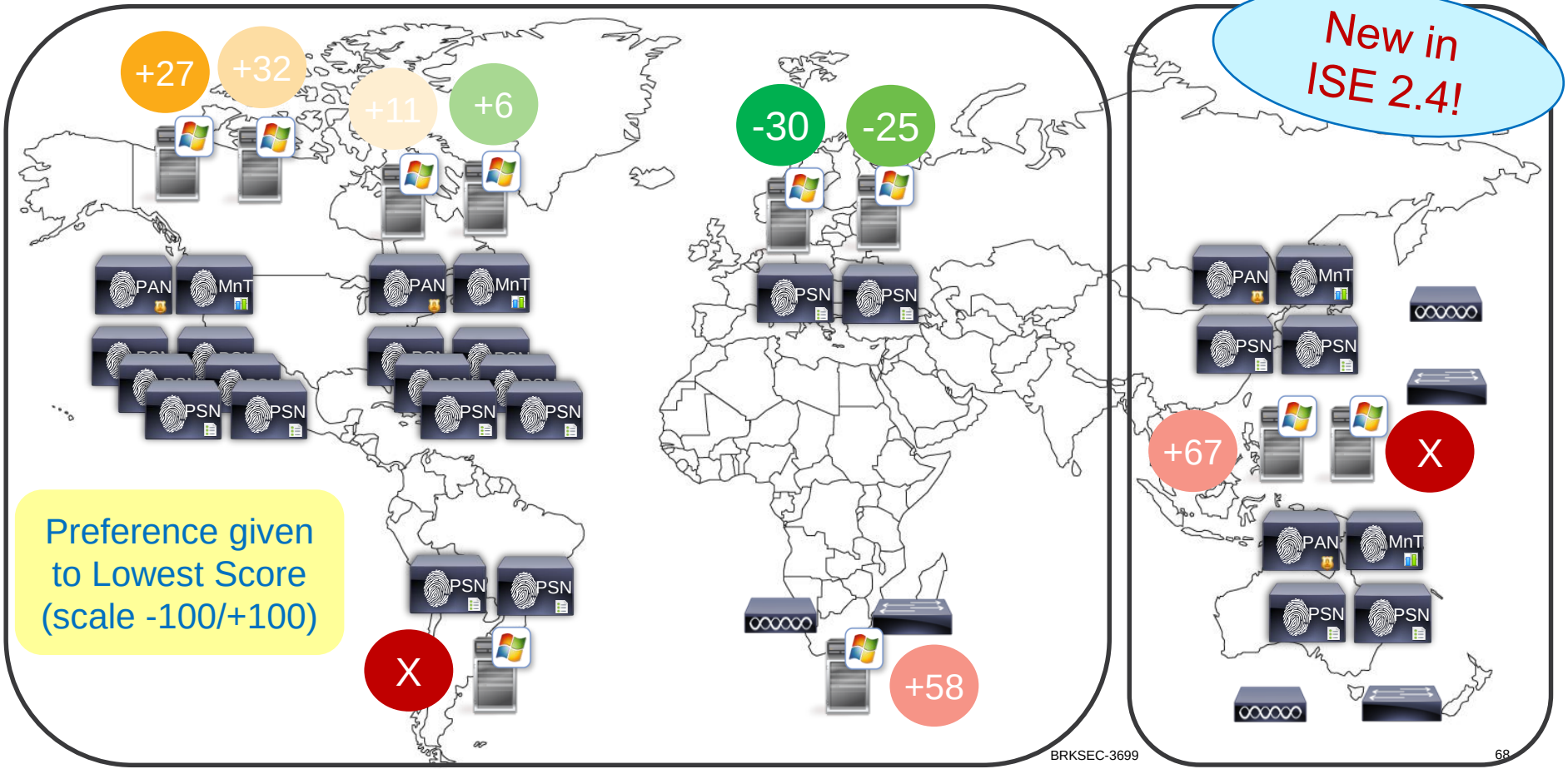
New in ISE 2.4!

- AD diagnostic tests run in the background without interrupting user auth
  - Scheduled to daily at 00:00, by default
  - Alarm is fired if test fails



Enhanced AD Domain Controller Management and Failover

Preferred DC Based on Scoring System



AD Integration Best Practices

BRKSEC-2132 What's new in ISE Active Directory Connector (CiscoLive.com/online) -Chris Murray

- **DNS** servers in ISE nodes must have all relevant AD records (A, PTR, SRV)
- Ensure **NTP** configured for all ISE nodes and AD servers
- Configure **AD Sites and Services**
  (with ISE machine accounts configured for relevant Sites)
- Configure Authentication Domains (**Whitelist domains** used) (ISE 1.3+)
- Use **UPN/fully qualified usernames** when possible to expedite use lookups
- Use **AD indexed attributes*** when possible to expedite attribute lookups
- **Run *Scheduled* Diagnostics** from ISE Admin interface to check for issues.

* Microsoft AD Indexed Attributes:
  http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx
  http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx

BRKSEC-3697 Advanced ISE Services, Tips and Tricks (https://www.ciscolive.com/global/on-demand-library/?#/) 2016 Las Vegas - by Aaron Woland

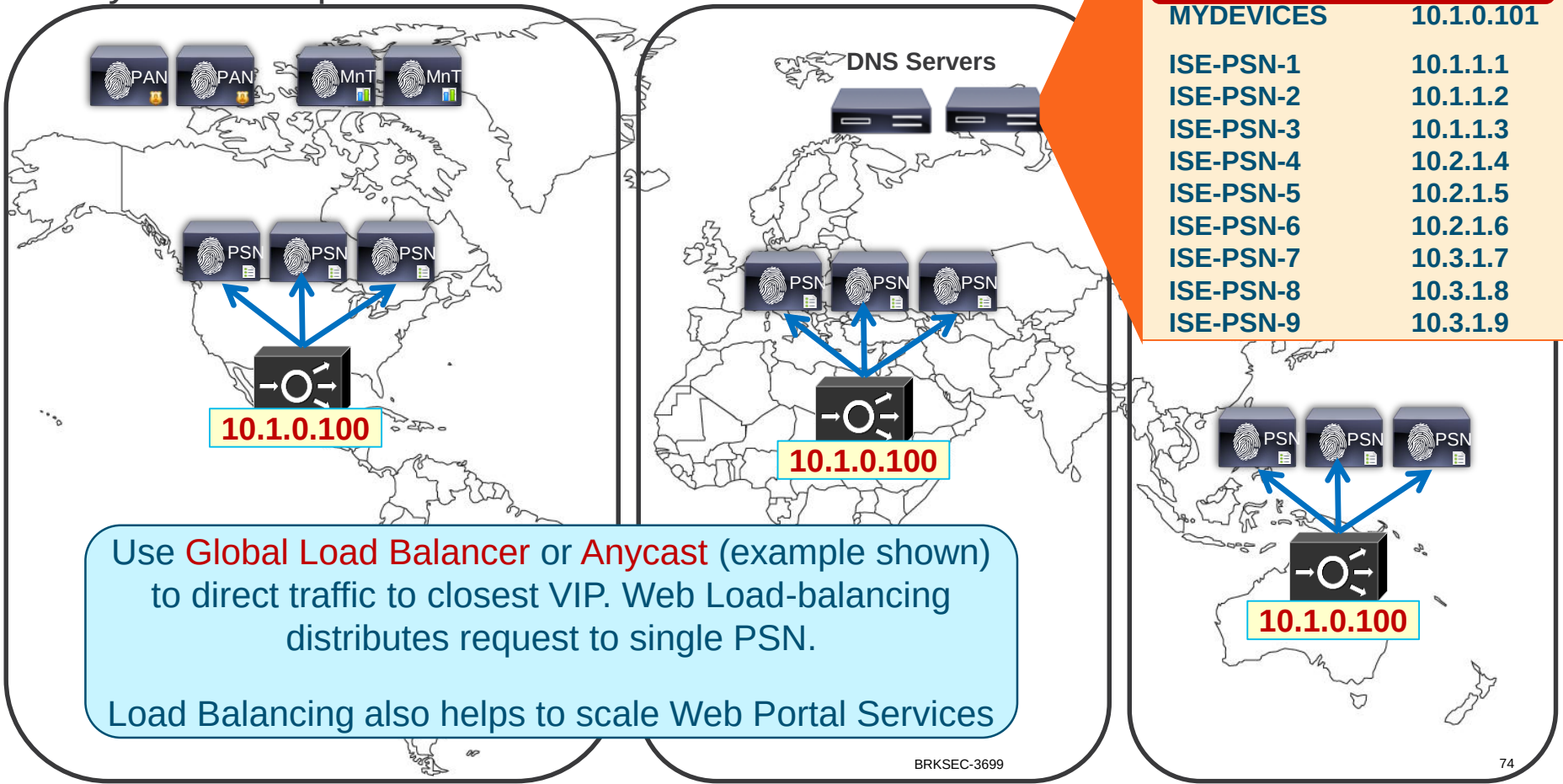
2017 BRKSEC-3697 video content by Craig Hyps

Scaling Passive Identity and Easy Connect

Scaling Guest and Web Authentication 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

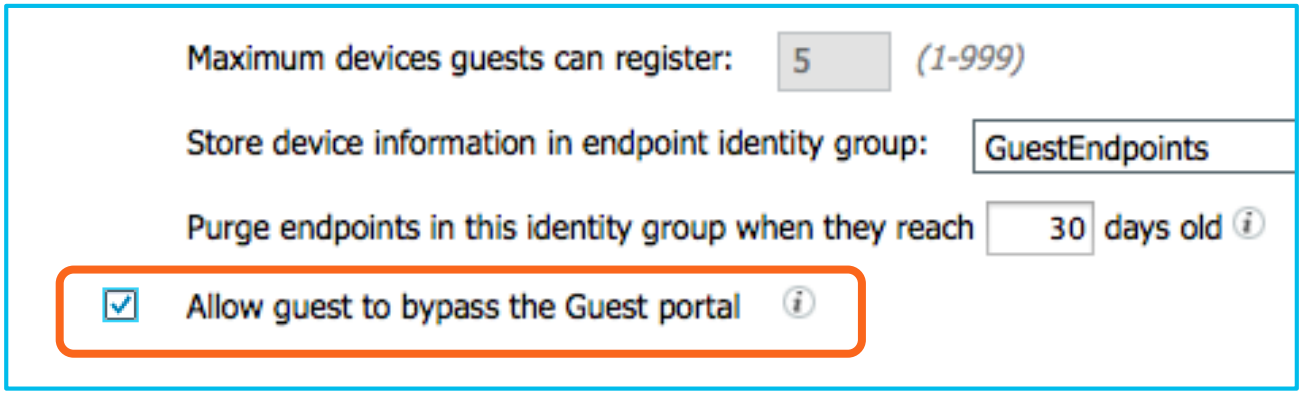
Use Global Load Balancer or Anycast (example shown) to direct traffic to closest VIP. Web Load-balancing distributes request to single PSN.

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



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

New in ISE 2.4

Work Centers > Guest Access > Settings > Logging

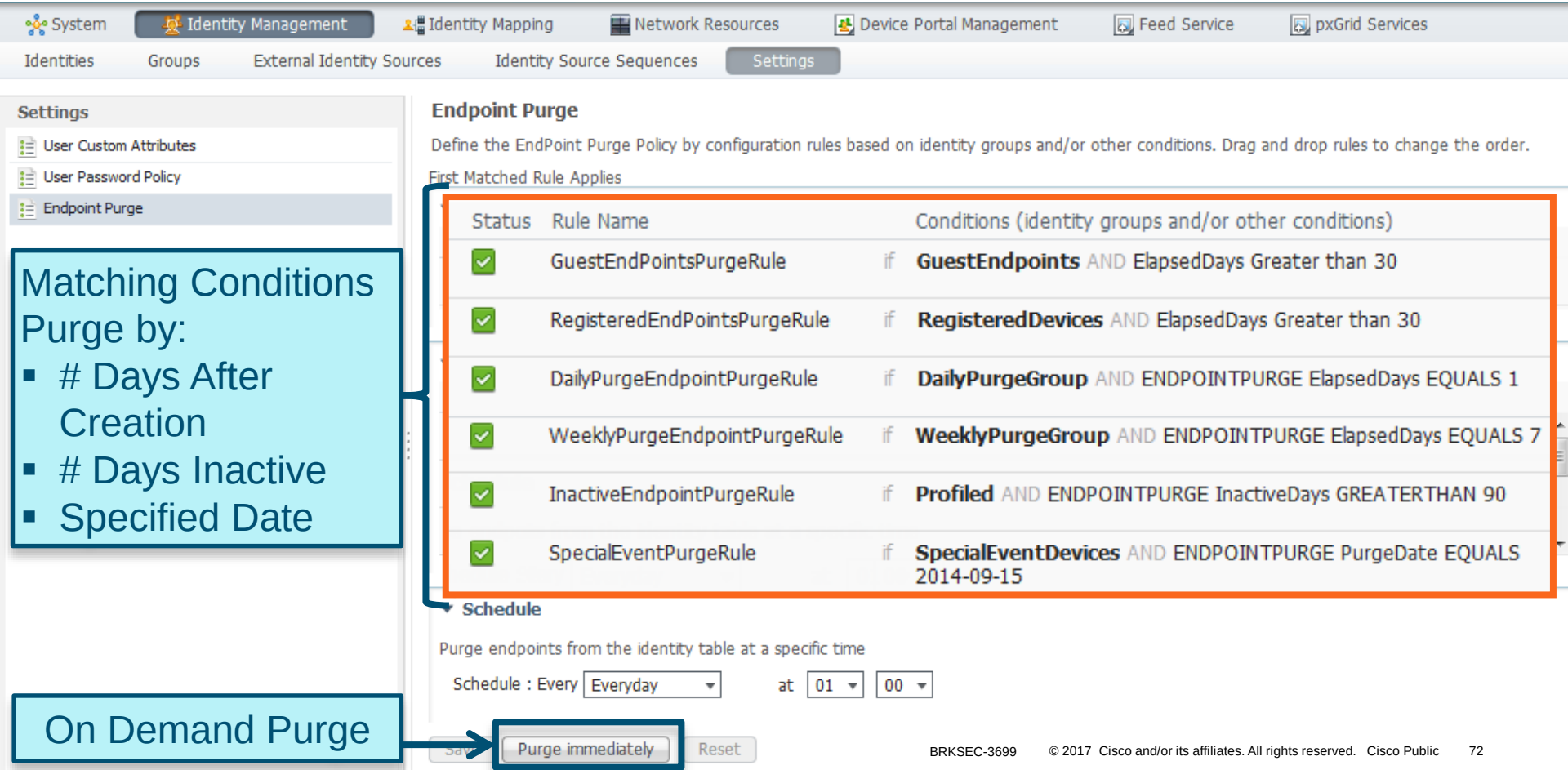
When guest portal is bypassed, authorization is based on endpoint group

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

Reset Save

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.

Endpoint Purging Examples



Matching Conditions Purge by:

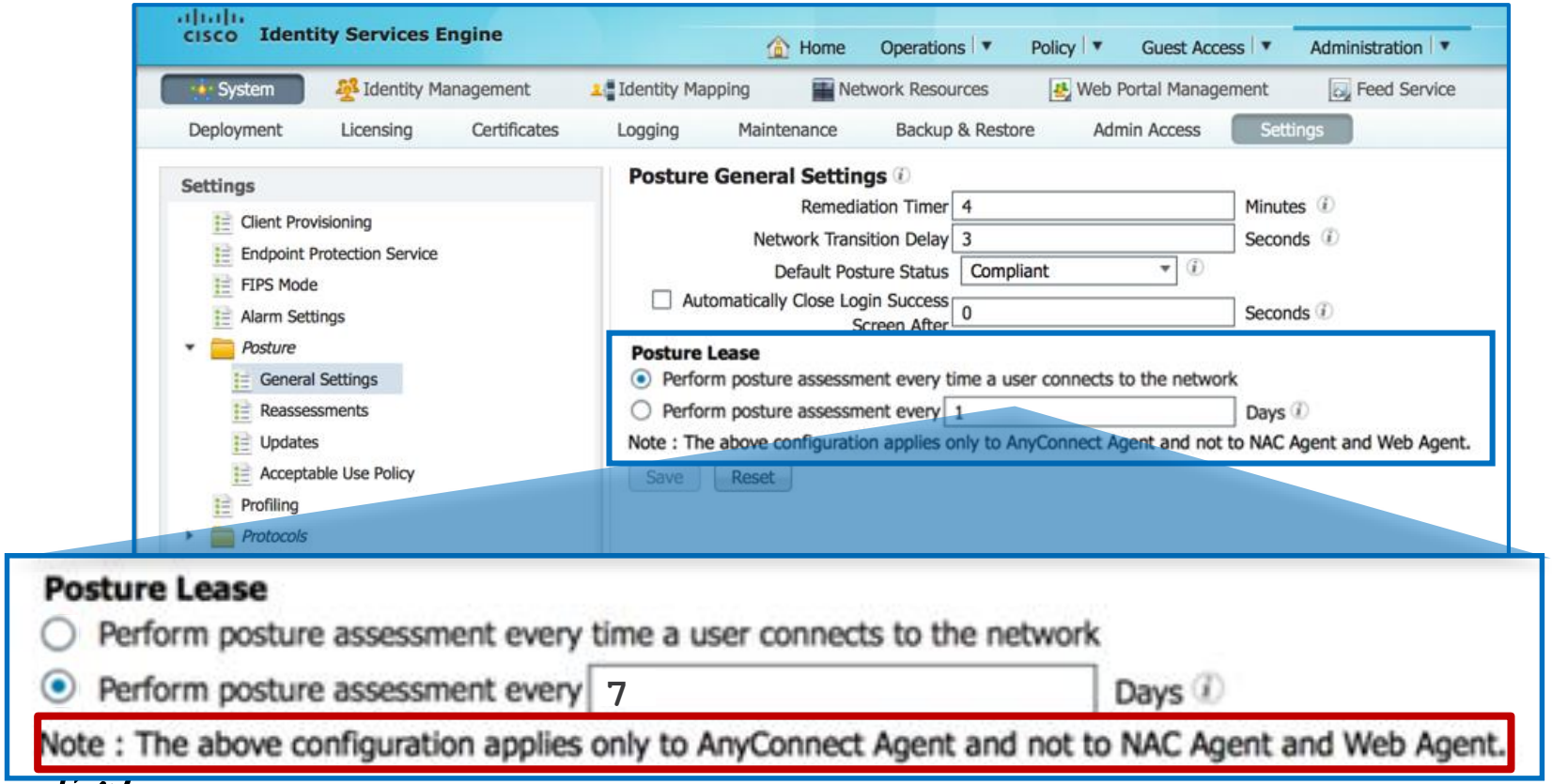
- # Days After Creation
- # Days Inactive
- Specified Date

On Demand Purge

Scaling Posture & MDM

Posture Lease

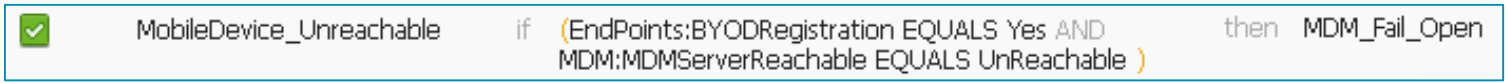
Once Compliant, user may leave/reconnect multiple times before re-posture



MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

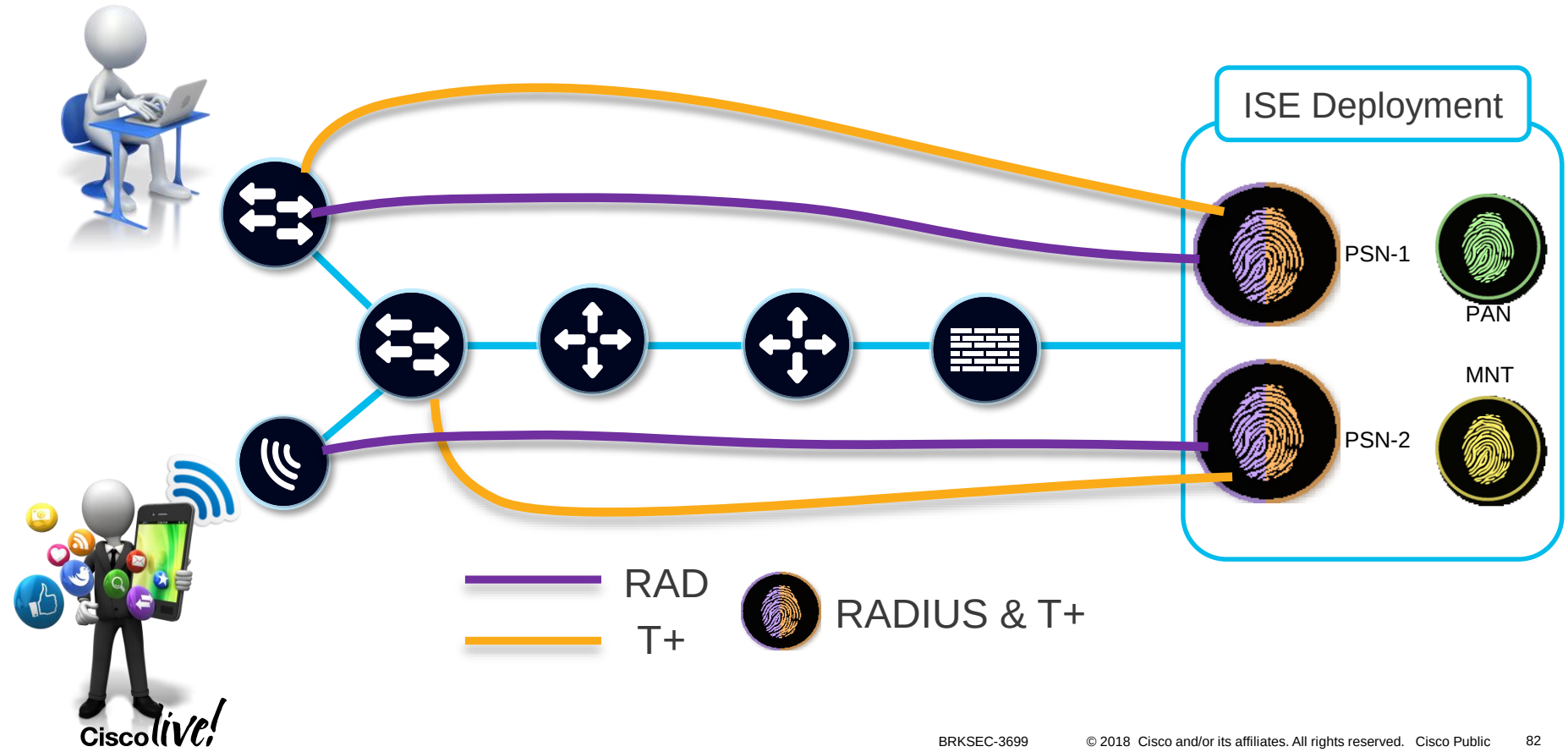
- Scalability ≈ 30 Calls per second per PSN.
  - Cloud-Based deployment typically built for scale and redundancy
    - For cloud-based solutions, Internet bandwidth and latency must be considered.
  - Premise-Based deployment may leverage load balancing
- ISE 1.4+ supports multiple MDM servers – could be same or different vendors.
- Authorisation permissions can be set based on MDM connectivity status:
  - **MDM:MDMServerReachable Equals UnReachable**
    MDM:MDMServerReachable Equals Reachable



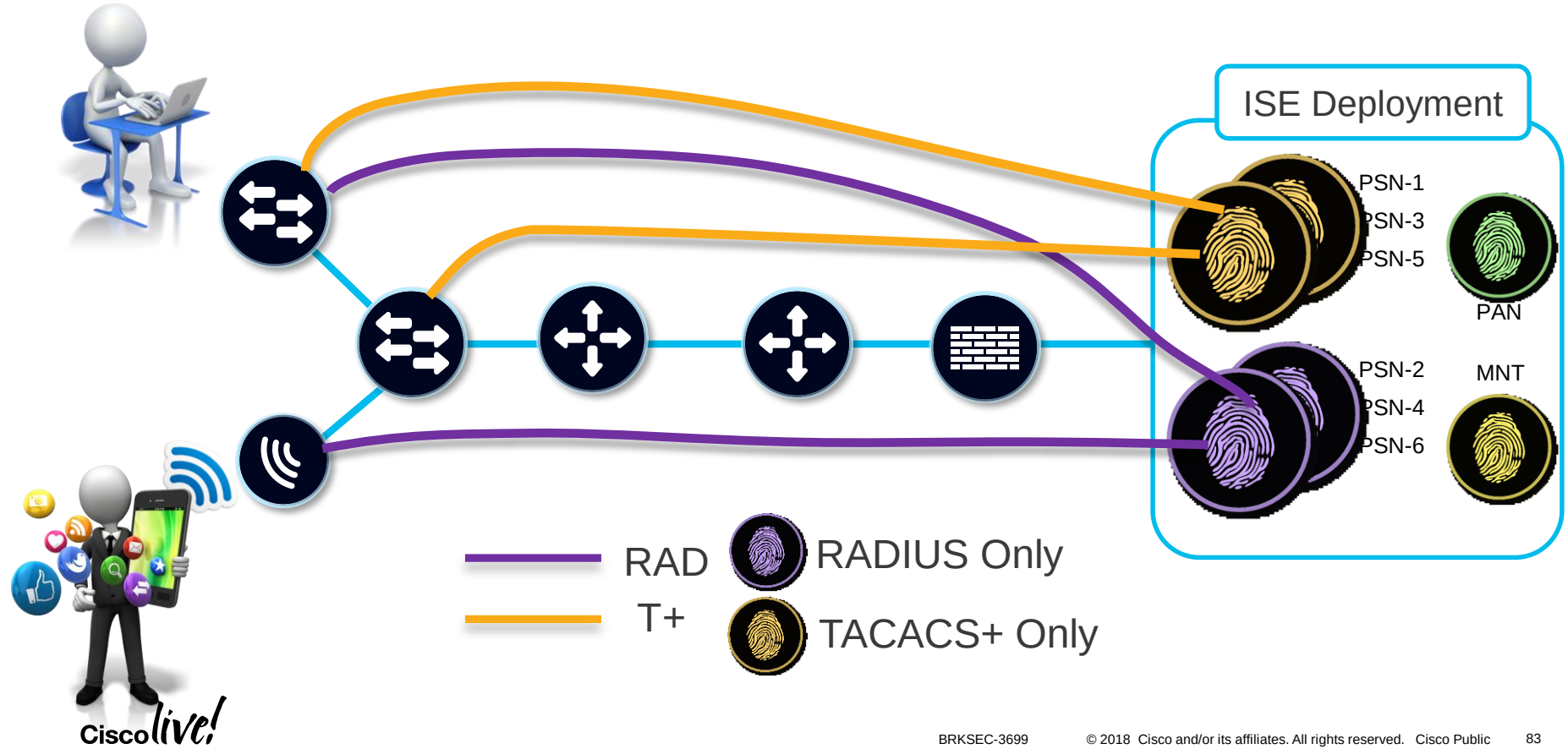
  - All attributes retrieved & reachability determined by single API call on each new session.

TACACS+ Design and Scaling

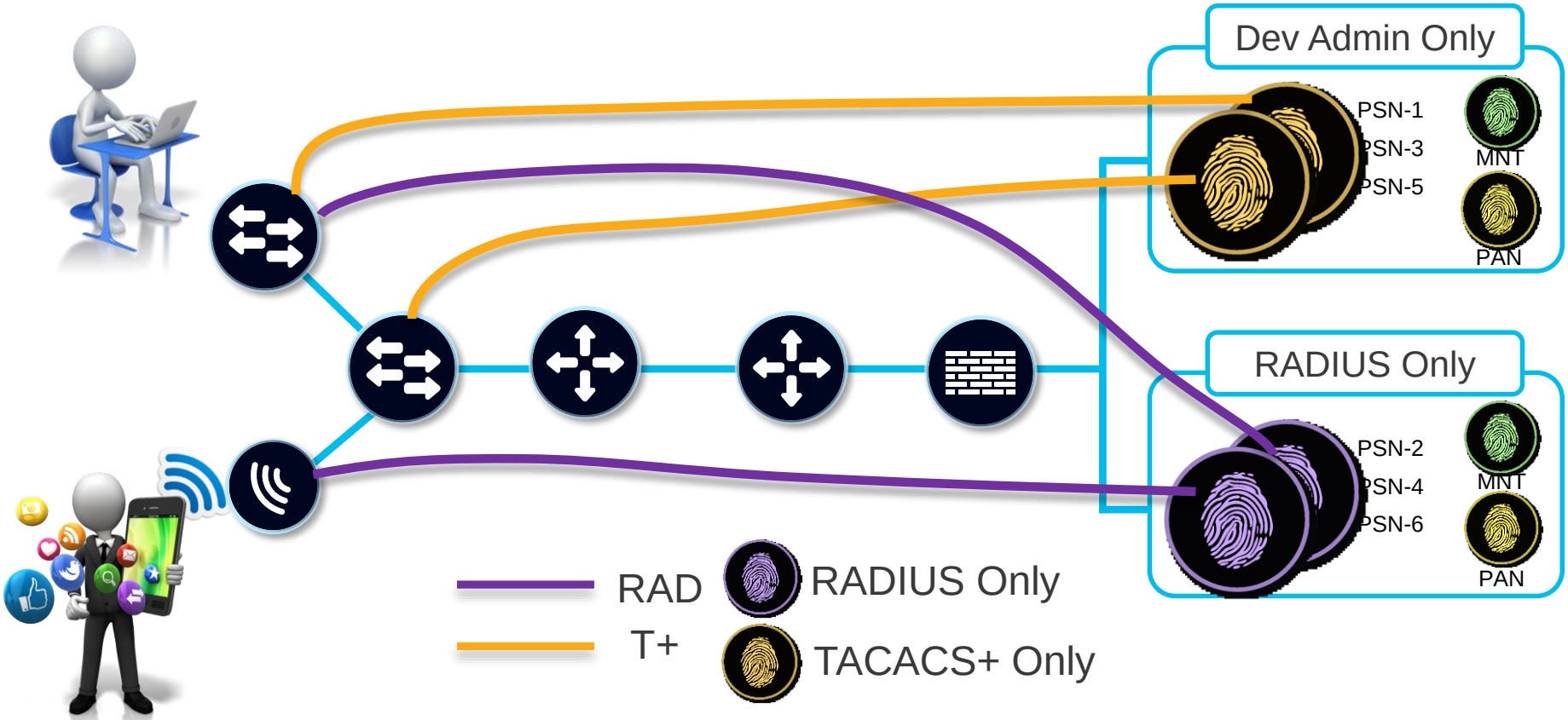
Design #1 – RADIUS & TACACS+ Share PSNs



Design #2 – RADIUS & T+ Use Dedicated PSNs

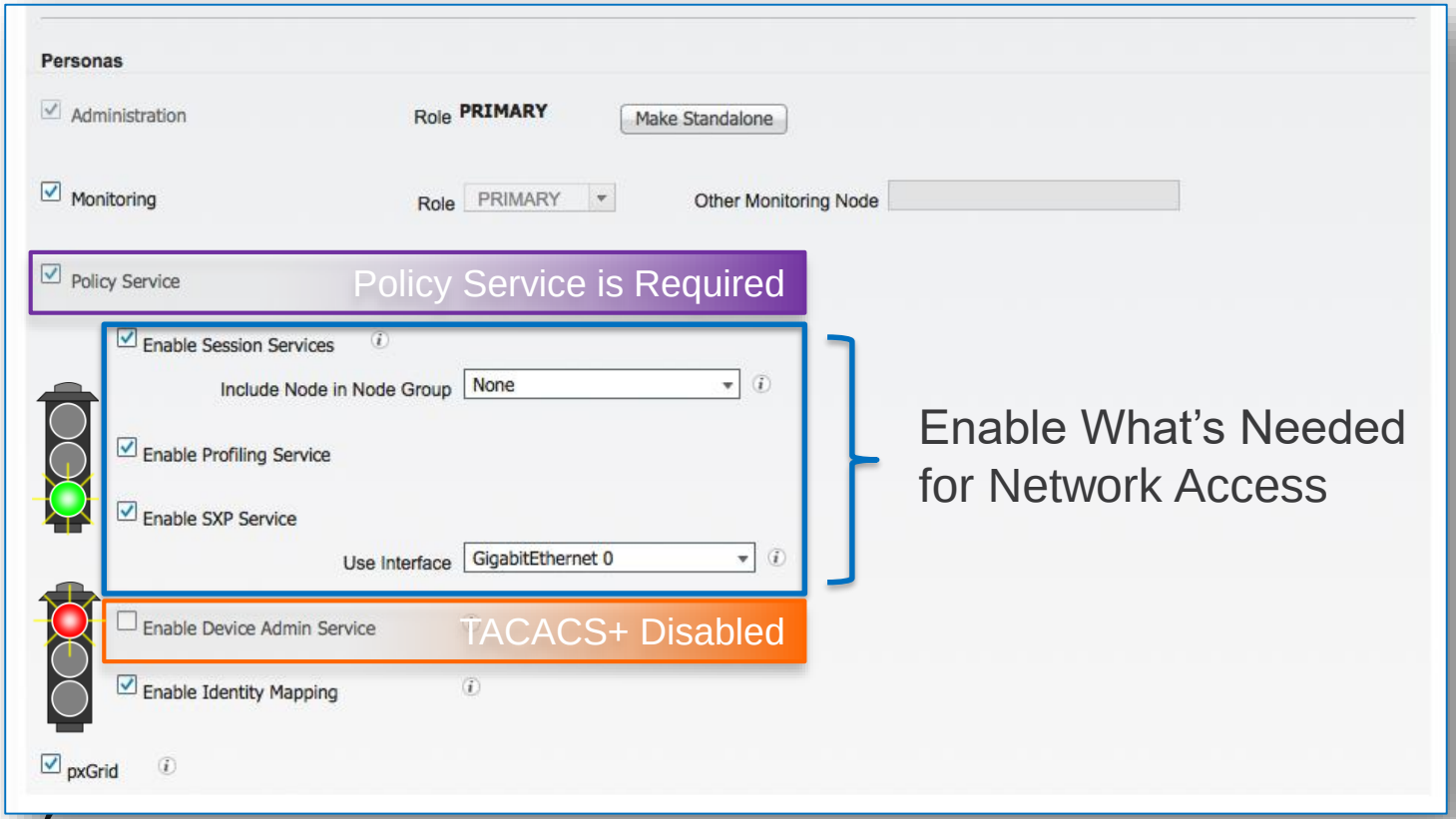


Design #3 – Separate Deployments for RAD & T+



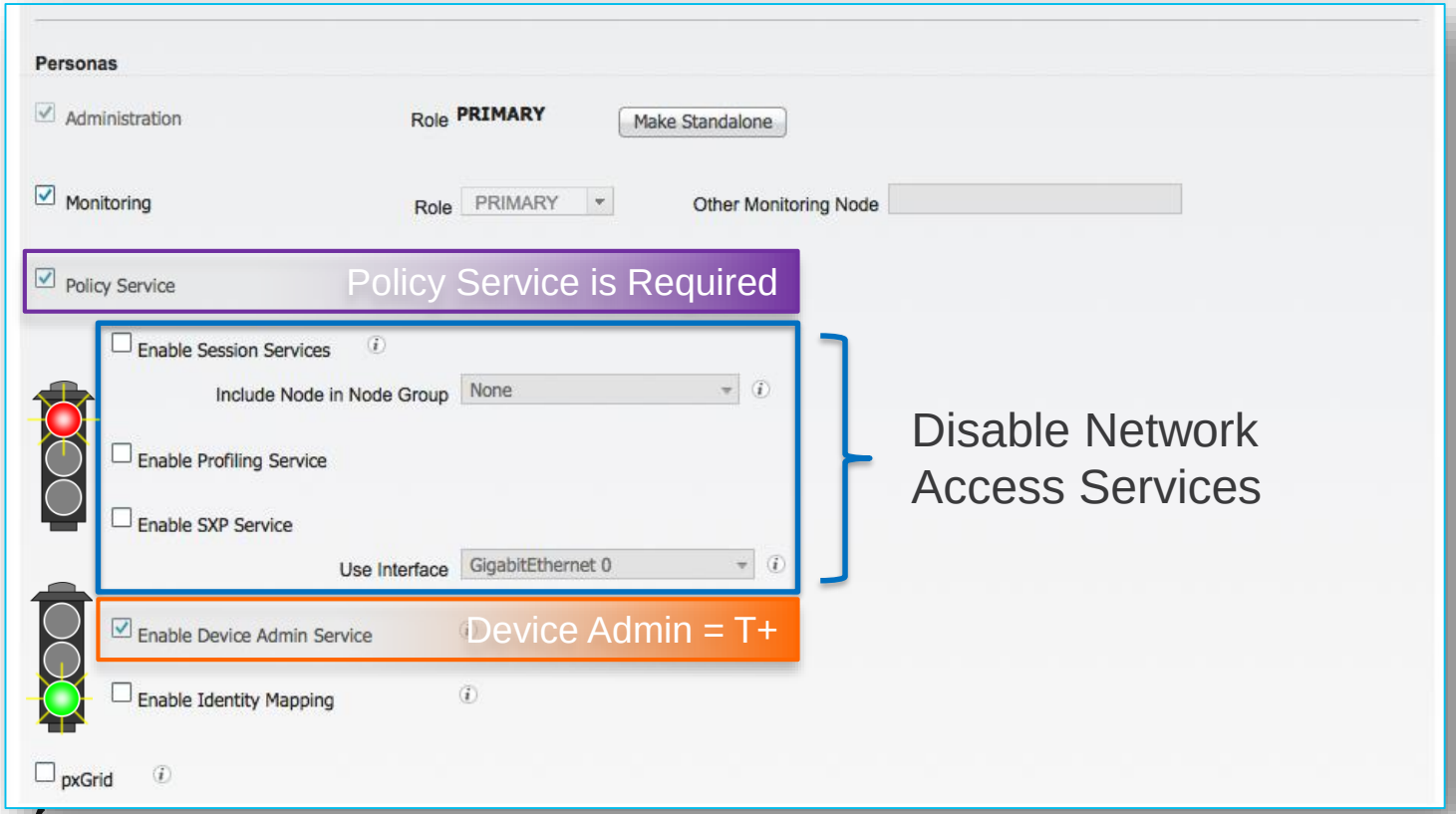
RADIUS Only PSNs

Administration > System > Deployment > [ISE node]



TACACS+ Only PSNs

Administration > System > Deployment > [ISE node]



Options for Deploying Device Admin

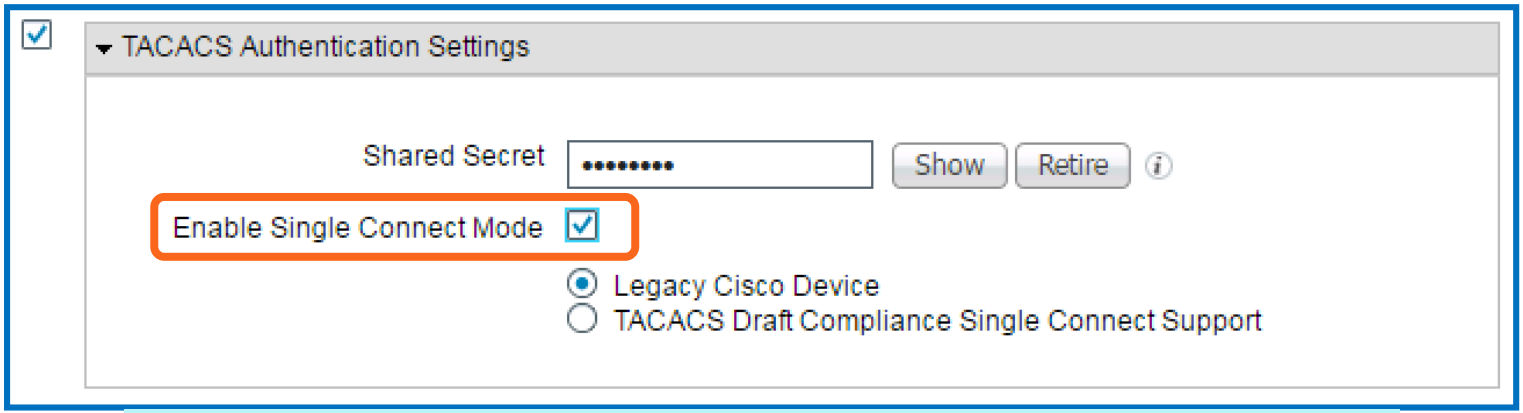
https://communities.cisco.com/docs/DOC-63930

Priorities - **According to Policy and Business Goals**		**Separate Deployment**   RADIUS TACACS	**Separate PSNs**  RADIUS TACACS	**Mixed PSNs**  RADIUS/TACACS
Separation of Configuration/ Duty	Yes: Specialisation for TACACS+			
	No: Shared resources/Reduced $$			
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services			
	No: Avoid underutilised PSNs			
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+			
	No: Focus on “human” device admins			
Separation of Logging Store	Yes: Optimise log retention VM			
	No: Centralised monitoring			

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.



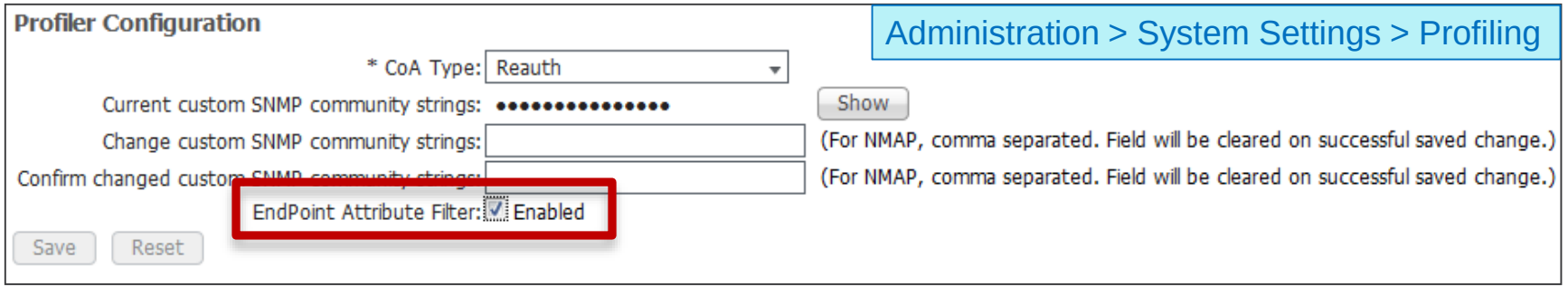
Administration > Network Resources > Network Devices > (NAD)

Scaling Profiling and Database Replication

Endpoint Attribute Filter and Whitelist Attributes

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

- Endpoint Attribute Filter – aka “Whitelist filter”
  - Disabled by default. If enabled, only these attributes are collected or replicated.



- 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.

Whitelist Attributes vs Significant Attributes

Sampling of All Endpoint Attributes

PolicyVersion
OUI
EndPointMACAddress
MatchedPolicy
EndPointMatchedProfile
EndPointPolicy
Total Certainty Factor
EndPointProfilerServer
EndPointSource
StaticAssignment
StaticGroupAssignment
UpdateTime
Description
IdentityGroup
ElapsedDays
InactiveDays
NetworkDeviceGroups
Location
Device Type
IdentityAccessRestricted
IdentityStoreName
ADDomain
AuthState
ISEPolicySetName
IdentityPolicyMatchedRule
AllowedProtocolMatchedRule
SelectedAccessService
SelectedAuthenticationIdentityStores
AuthenticationIdentityStore
AuthenticationMethod
AuthorizationPolicyMatchedRule
SelectedAuthorizationProfiles
CPMSessionID
AAA-Server
OriginalUserName
DetailedInfo
EapAuthentication
NasRetransmissionTimeout
TotalFailedAttempts
TotalFailedTime

UseCase
UserType
GroupsOrAttributesProcessF
ExternalGroups
Called-Station-ID
Calling-Station-ID
DestinationIPAddress
DestinationPort
Device IP Address
MACAddress
MessageCode
NADAddress
NAS-IP-Address
NAS-Port
NAS-Port-Id
NAS-Port-Type
NetworkDeviceName
RequestLatency
Service-Type
Timestamp
User-Name
Egress-VLANID
Egress-VLAN-Name
Airespace-Wlan-Id
Device Port
EapTunnel
Framed-IP-Address
NAS-Identifier
RadiusPacketType
Vlan
VlanName
cafSessionAuthUserName
cafSessionAuthVlan
cafSessionAuthorizedBy
cafSessionDomain
cafSessionStatus
dot1dBasePort
dot1xAuthAuthControlledPort
dot1xAuthAuthControlledPort
dot1xAuthSessionUserName

ifDescr
client-fqdn

IPV4_IDENT

mdns_VSM_srv_identifier

mdns_VSM_txt_identifier
sipDeviceName
sipDeviceVendor
sipDeviceVersion
device-platform
device-platform-version
device-type
AD-Host-Exists
AD-Join-Point
Operating-System

138-udp
139-udp

Whitelist Attributes

161-udp
AAA-Server
AC_User_Agent
AUPAccepted
BYODRegistration
CacheUpdateTime
Calling-Station-ID
cdpCacheAddress
cdpCacheCapabilities
cdpCacheDeviceId
cdpCachePlatform
cdpCacheVersion
Certificate Expiration Date
Certificate Issue Date
Certificate Issuer Name
Certificate Serial Number
ciaddr
CreateTime
Description
DestinationIPAddress
Device Identifier
Device Name
DeviceRegistrationStatus
dhcp-class-identifier
dhcp-requested-address
EndPointPolicy
EndPointPolicyID
EndPointProfilerServer
EndPointSource

FirstCollection
FQDN
Framed-IP-Address
host-name
hrDeviceDescr
IdentityGroup
IdentityGroupID
IdentityStoreGUID
IdentityStoreName
ifIndex
ip
L4_DST_PORT
LastNmapScanTime
lldpCacheCapabilities
lldpCapabilitiesMapSupported
lldpSystemDescription
MACAddress
MatchedPolicy
MatchedPolicyID
MDMCompliant
MDMCompliantFailureReason
MDMDiskEncrypted
MDMEnrolled
MDMImei
MDMJailBroken
MDMManufacturer
MDMModel
MDMOSVersion
MDMPhoneNumber

MDMSerialNumber
MDMServerReachable
MDMUpdateTime
NADAddress
NAS-IP-Address
NAS-Port-Id
NAS-Port-Type
NmapScanCount
NmapSubnetScanID
operating-system
OS Version
OUI
PhoneID
PhoneIDType
PolicyVersion
PortalUser
PostureApplicablePrevious
DeviceRegistrationStatus
ProductRegistrationTimeStamp
StaticAssignment
StaticGroupAssignment
sysDescr
TimeToProfile
Total Certainty Factor
UpdateTime
User-Agent

Triggers Node Group Update and Ownership Change

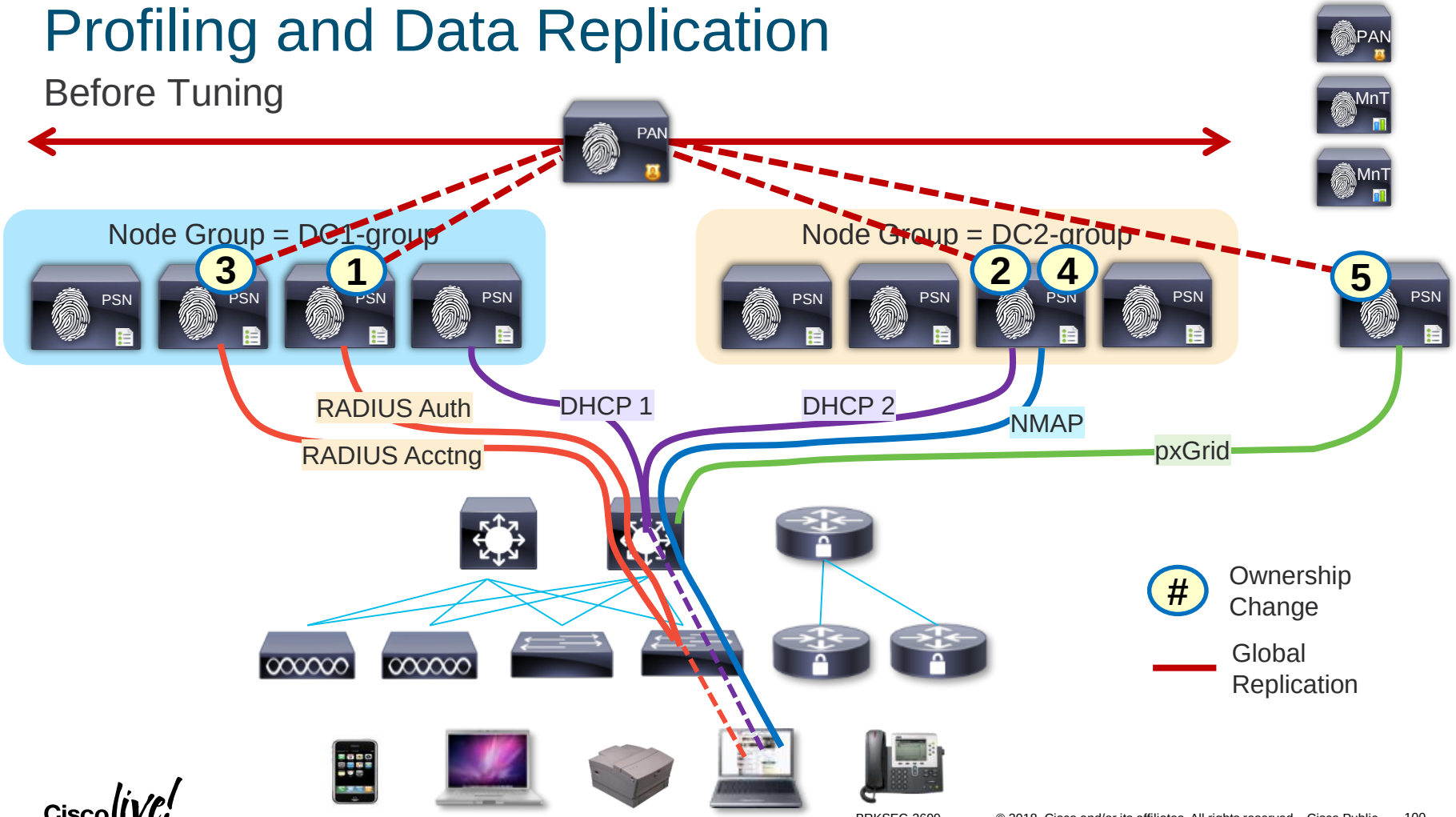
Triggers Global Replication

Significant Attributes

MACADDRESS
MATCHEDVALUE
ENDPOINTPOLICY
ENDPOINTPOLICYVERSION
STATICASSIGNMENT
STATICGROUPASSIGNMENT
NMAPSUBNETSCANID
PORTALUSER
DEVICEREGISTRATIONSTATUS

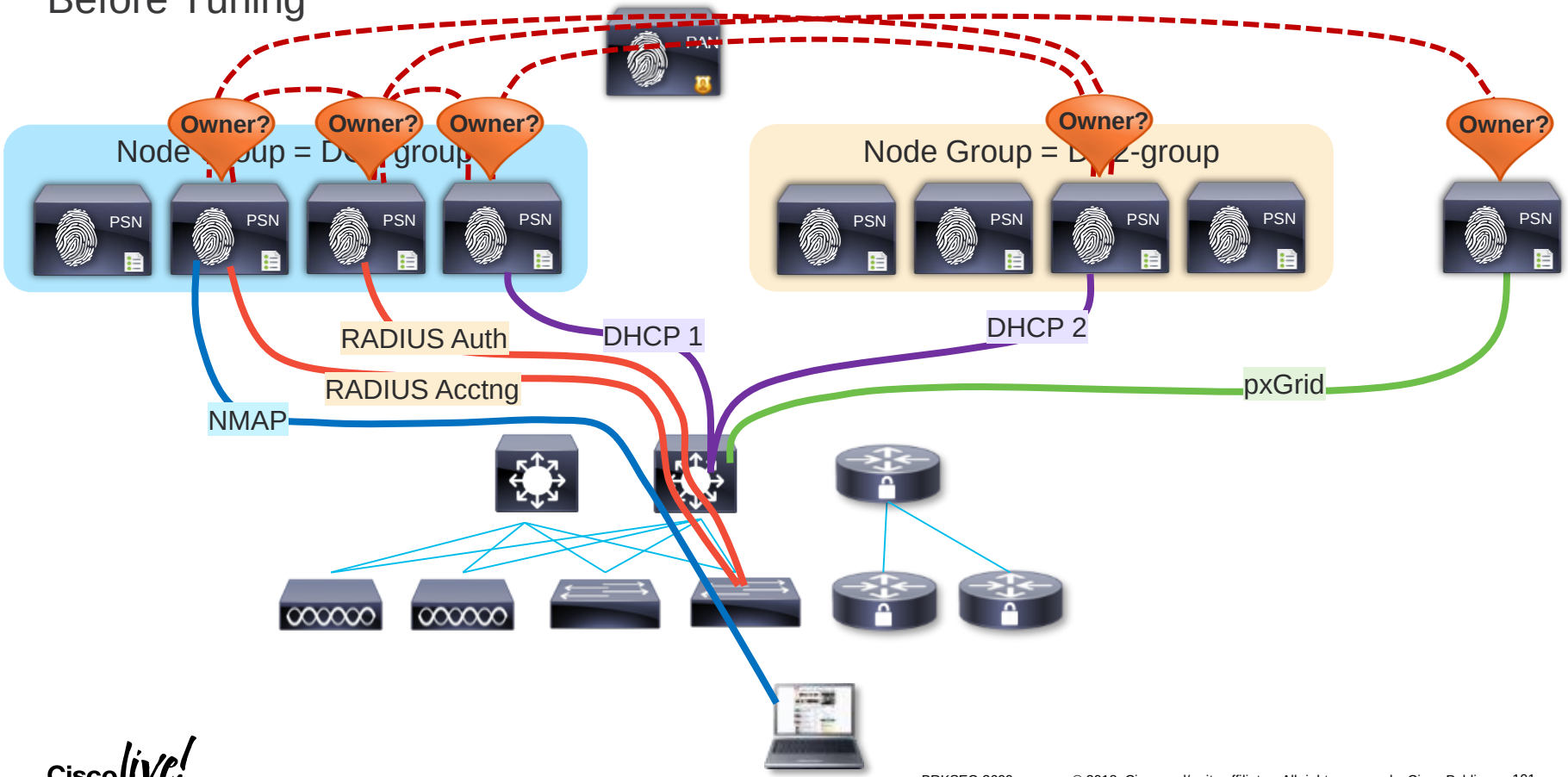
Profiling and Data Replication

Before Tuning



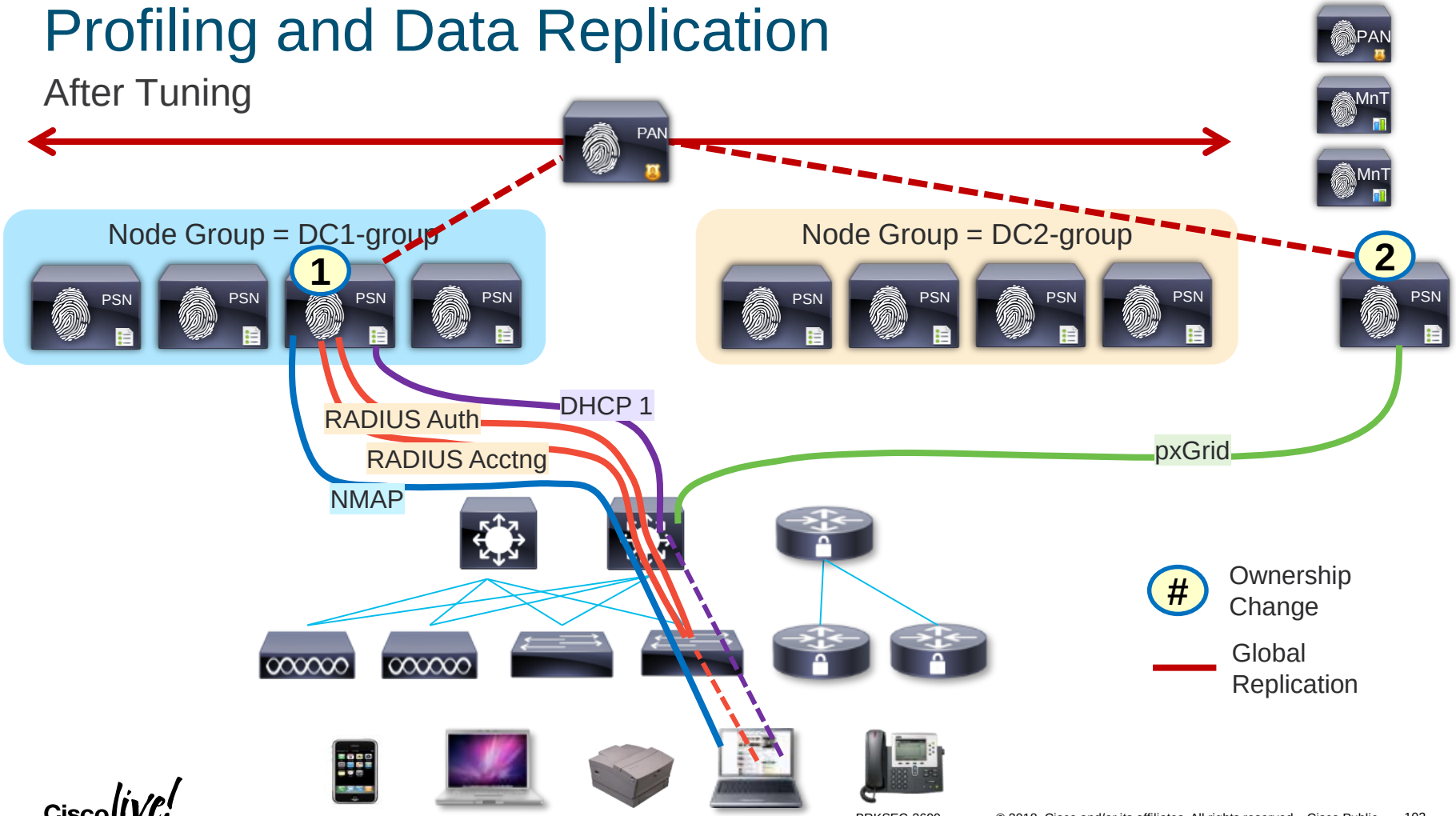
Impact of Ownership Changes

Before Tuning



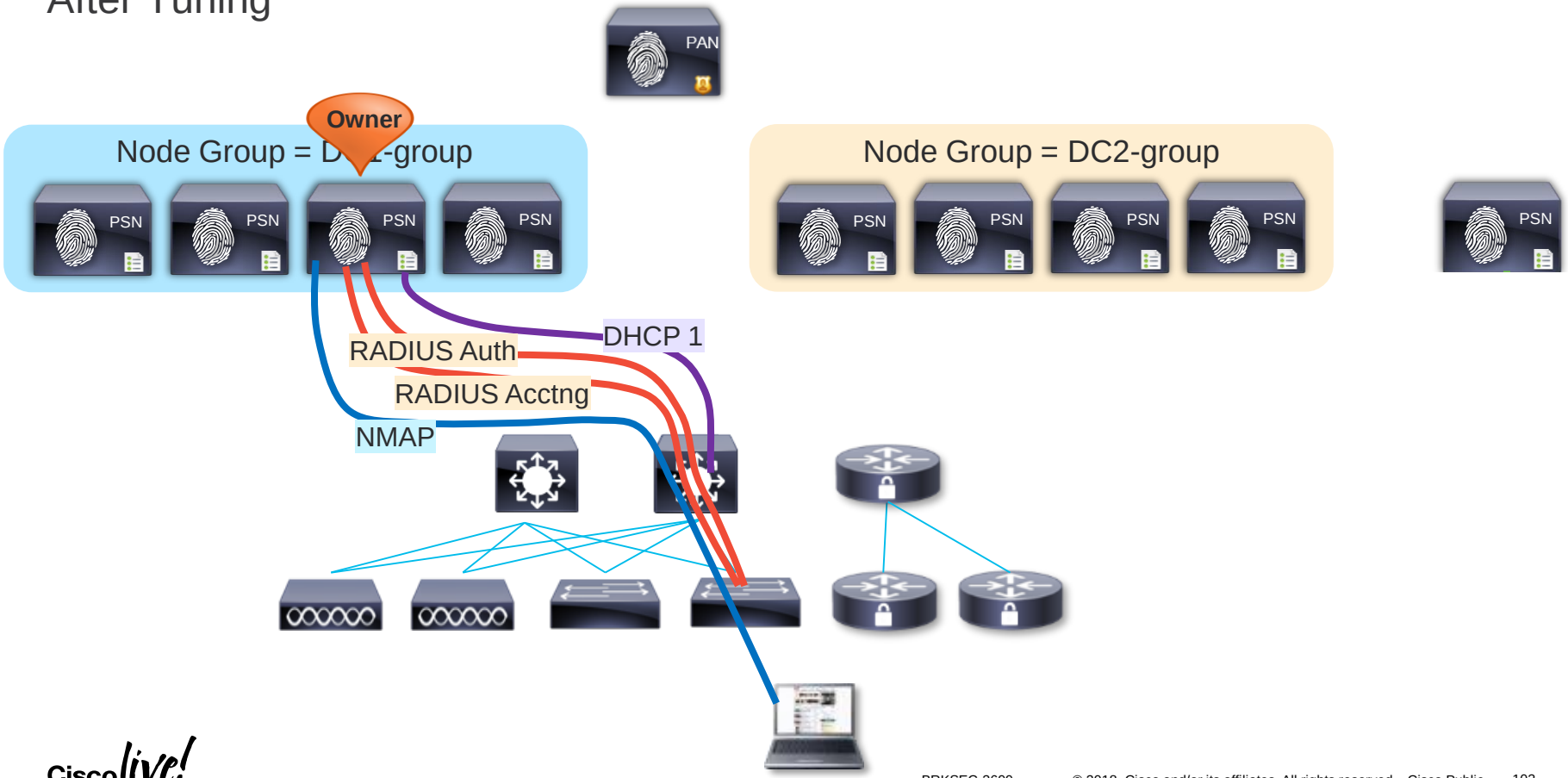
Profiling and Data Replication

After Tuning



Impact of Ownership Changes

After Tuning



ISE Profiling Best Practices

Whenever Possible…

- **Use Device Sensor** on Cisco switches & Wireless Controllers to optimise data collection.
- **Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)**
  - Sending same profile data to multiple PSNs increases inter-PSN traffic and contention for endpoint ownership.
  - For redundancy, consider Load Balancing and Anycast to support a single IP target for RADIUS or profiling using…
    - DHCP IP Helpers
    - SNMP Traps
    - DHCP/HTTP with ERSPAN (Requires validation)
- **Ensure profile data for a given endpoint is sent to the *same* PSN**
  - Same issue as above, but not always possible across different probes
- **Use node groups and ensure profile data for a given endpoint is sent to *same* node group.**
  - Node Groups reduce inter-PSN communications and need to replicate endpoint changes outside of node group.
- **Avoid probes that collect the same endpoint attributes**
  - Example: Device Sensor + SNMP Query/IP Helper
- **Enable Profiler Attribute Filter**

Do NOT send profile data to multiple PSNs !

DO send profile data to single and same PSN or Node Group !

DO use Device Sensor !

DO enable the Profiler Attribute Filter !

ISE Profiling Best Practices

General Guidelines for Probes

- **HTTP Probe:**
  - Use URL Redirects instead of SPAN to centralise collection and reduce traffic load related to SPAN/RSPAN.
  - Avoid SPAN. If used, look for key traffic chokepoints such as Internet edge or WLC connection; use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to ISE. Also difficult to provide HA for SPAN.
- **DHCP Probe:**
  - Use IP Helpers when possible—be aware that L3 device serving DHCP will not relay DHCP for same!
  - Avoid DHCP SPAN. Typically measure of last resort for specific use cases. DHCP Server. HA challenges.
- **SNMP Probe:**
  - For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
  - SNMP Traps primarily useful for non-RADIUS deployments like NAC Appliance—Avoid SNMP Traps w/RADIUS auth.
- **NetFlow Probe:**
  - Use only for specific use cases in centralised deployments—Potential for high load on network devices and ISE.
- **pxGrid Probe:**
  - Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy. Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

Do NOT enable all probes by default !

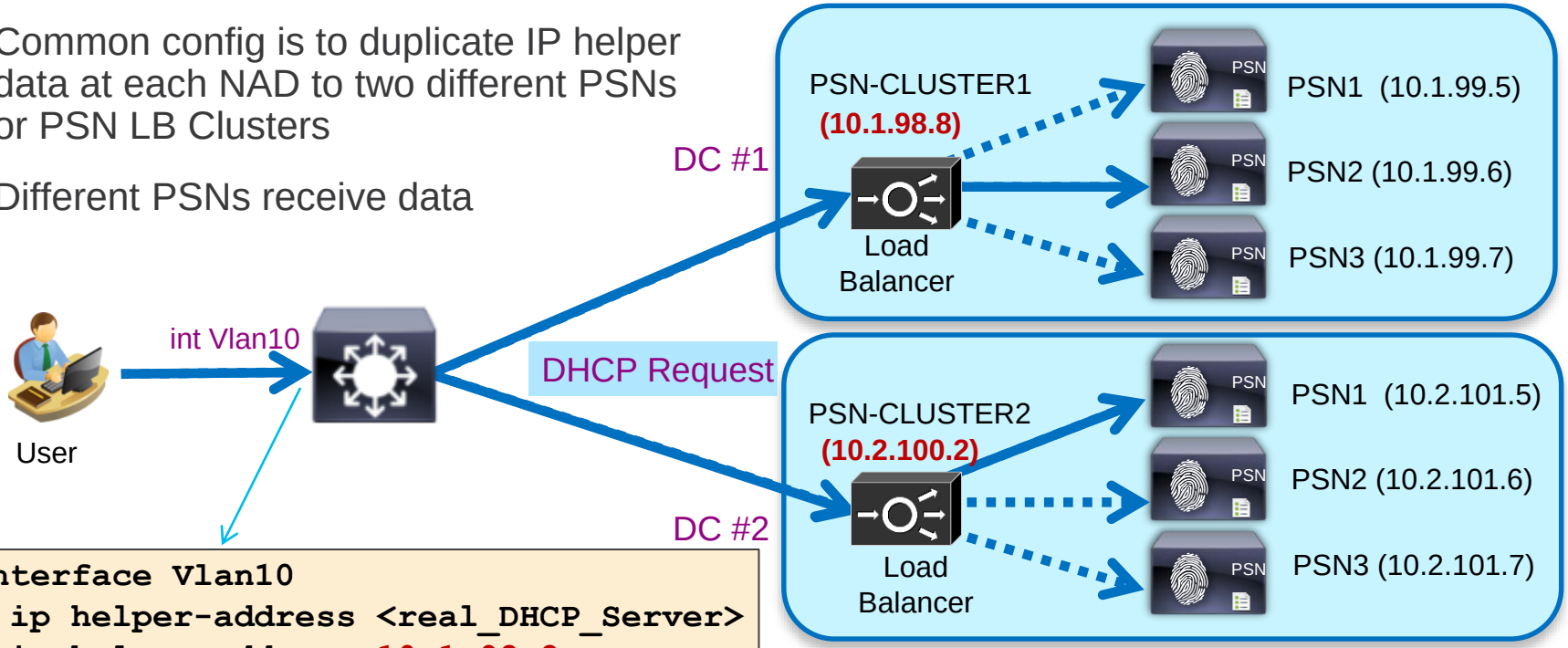
Avoid SPAN, SNMP Traps, and NetFlow probes !

Limit pxGrid probe to two PSNs max for HA – possibly dedicated !

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



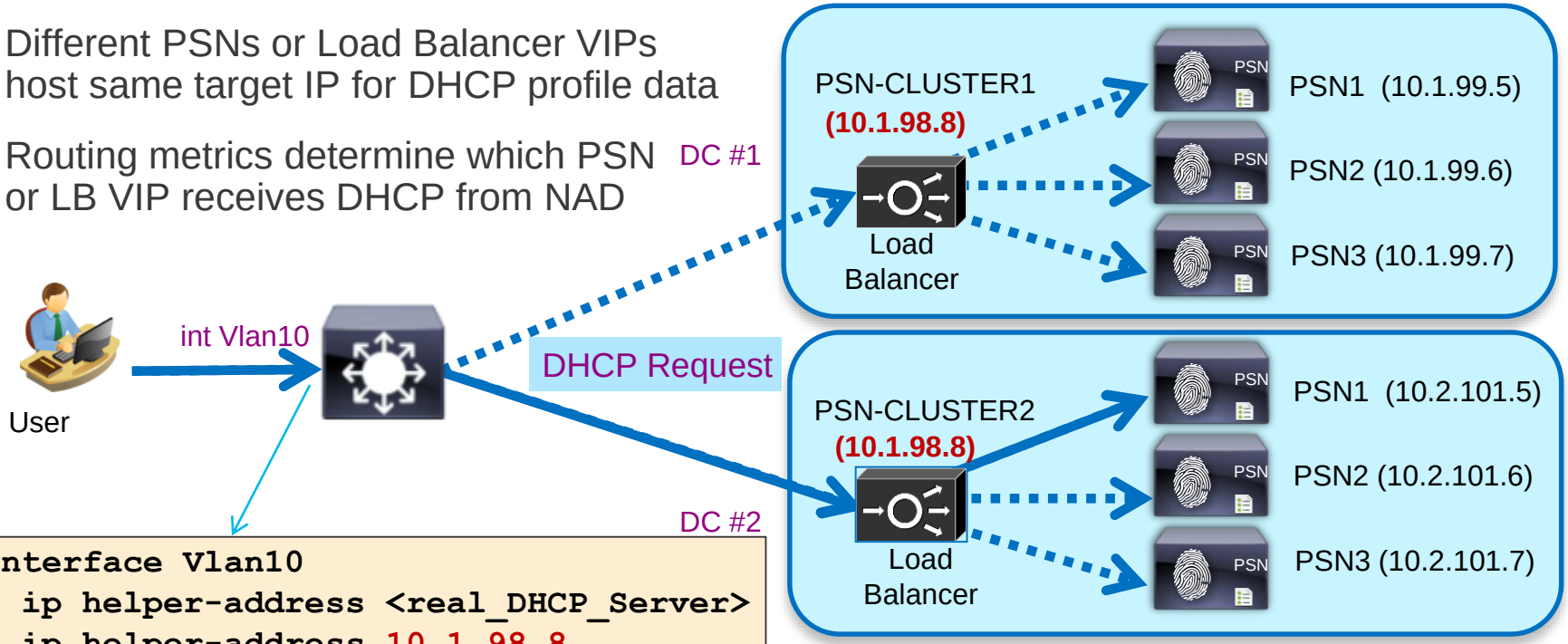

```
interface Vlan10
  ip helper-address <real_DHCP_Server>
  ip helper-address 10.1.98.8
  ip helper-address 10.2.100.2
```

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



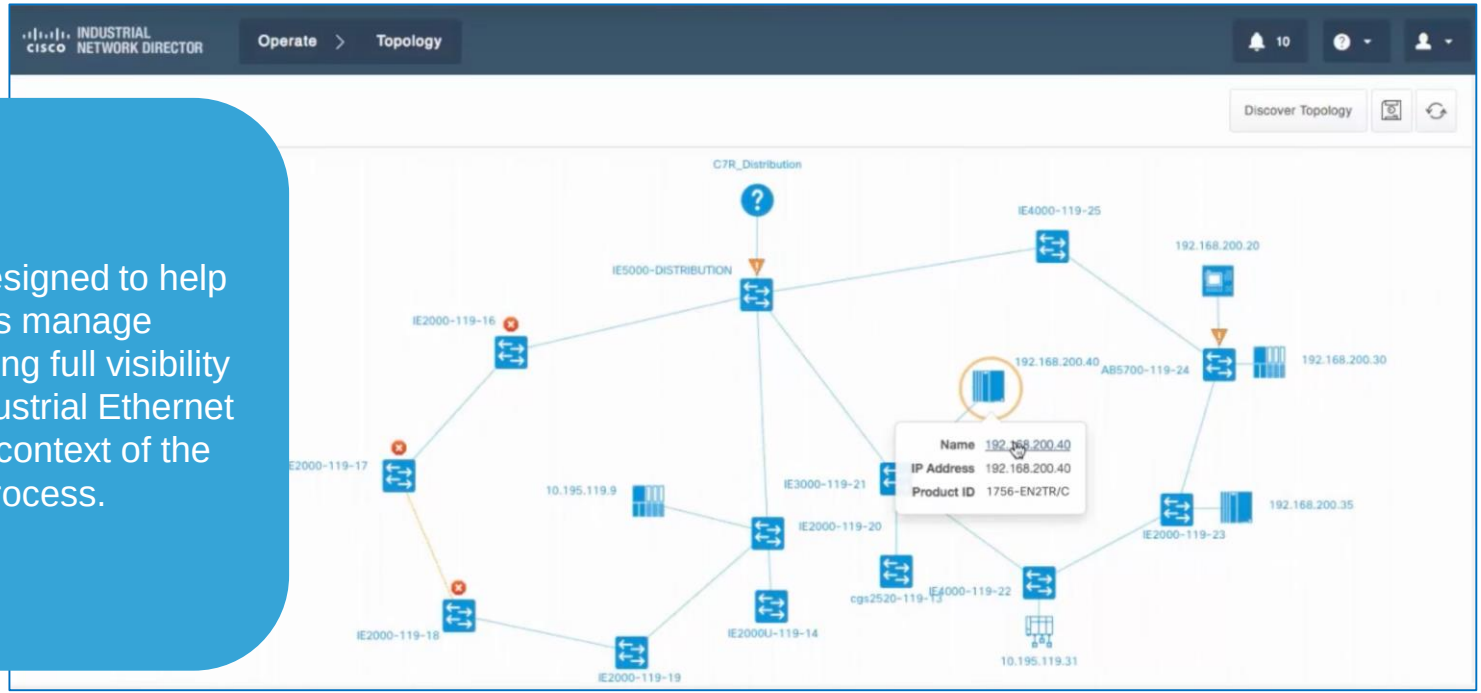

```
interface Vlan10
  ip helper-address <real_DHCP_Server>
  ip helper-address 10.1.98.8
```

Note: LB depicted, but NOT required

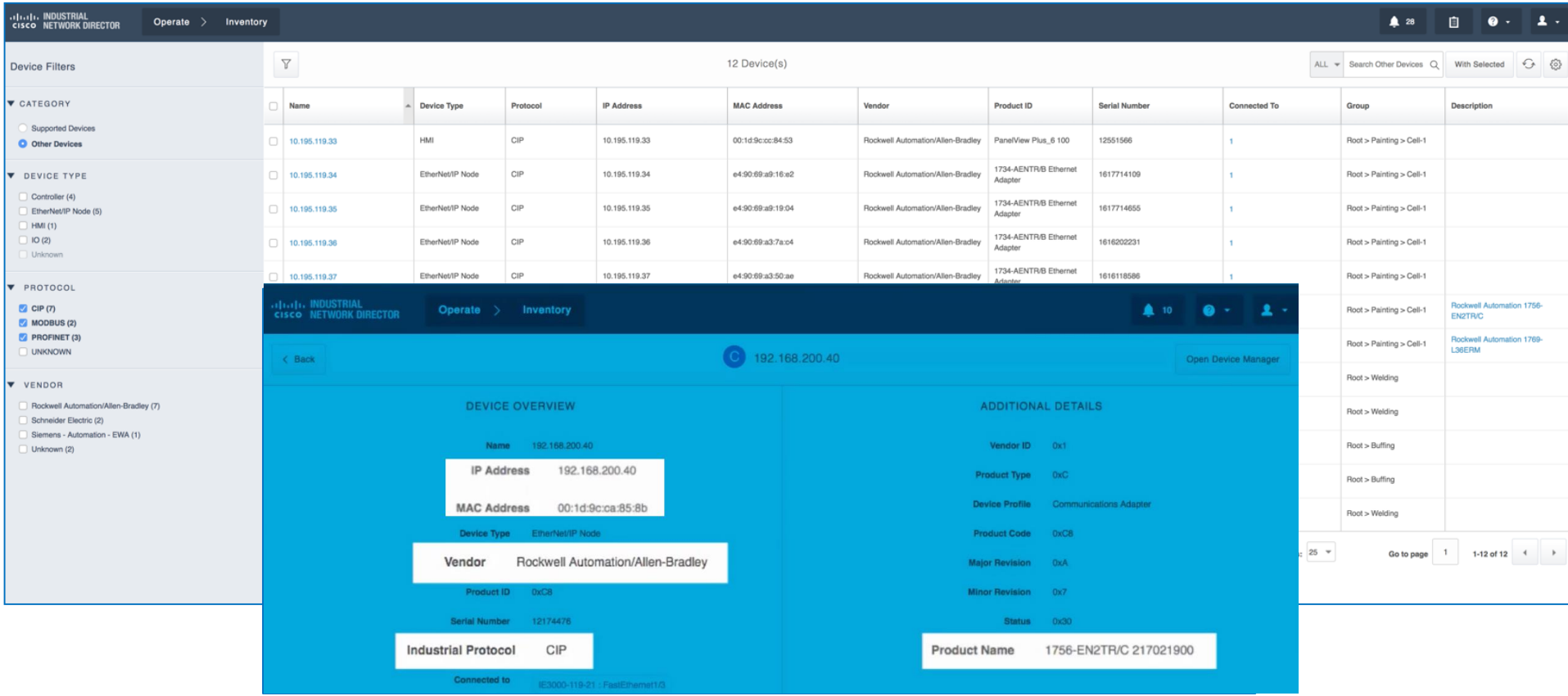
Cisco Industrial Network Director (IND)

www.cisco.com/go/ind

IND is specifically designed to help operations teams manage automation by providing full visibility and control of the Industrial Ethernet infrastructure in the context of the automation process.



IND Inventory

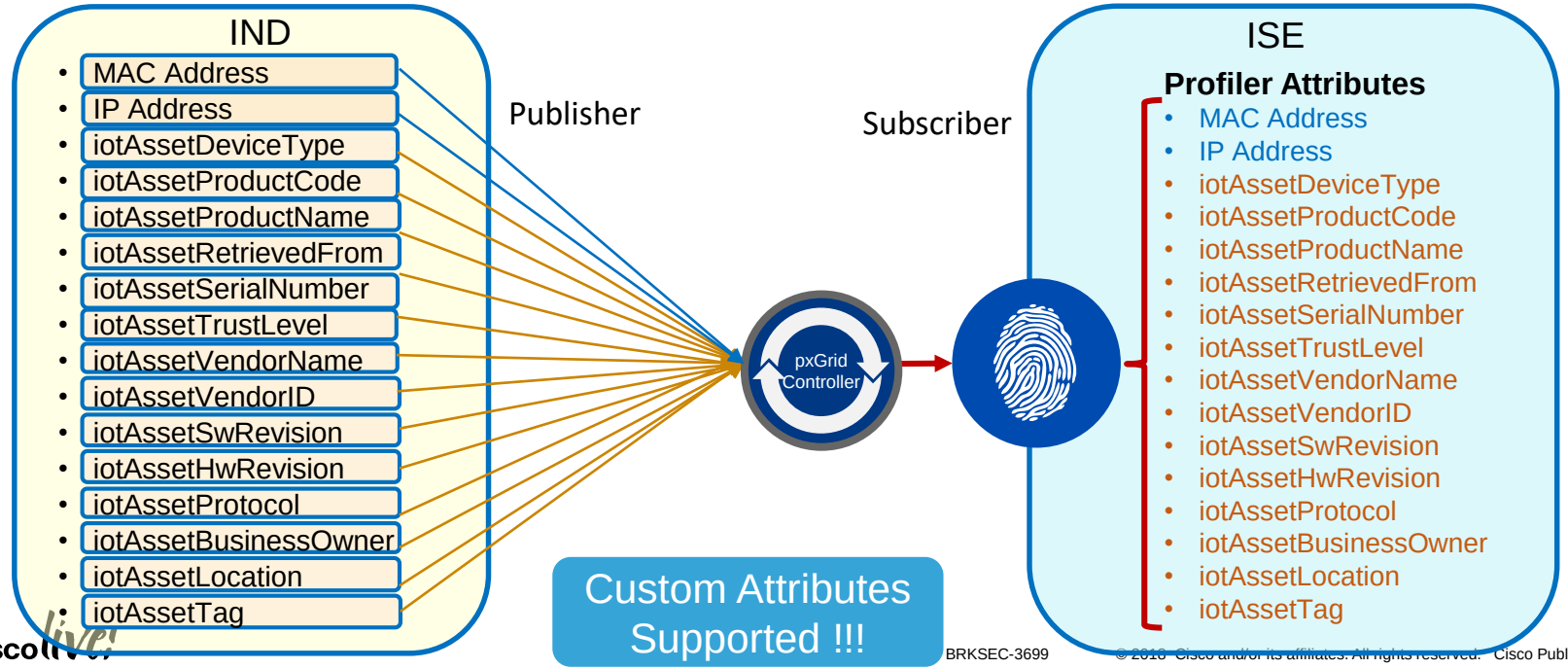


pxGrid Profiler Probe (Context In)

First Integration is with Industrial Network Director (IND)

New in ISE 2.4

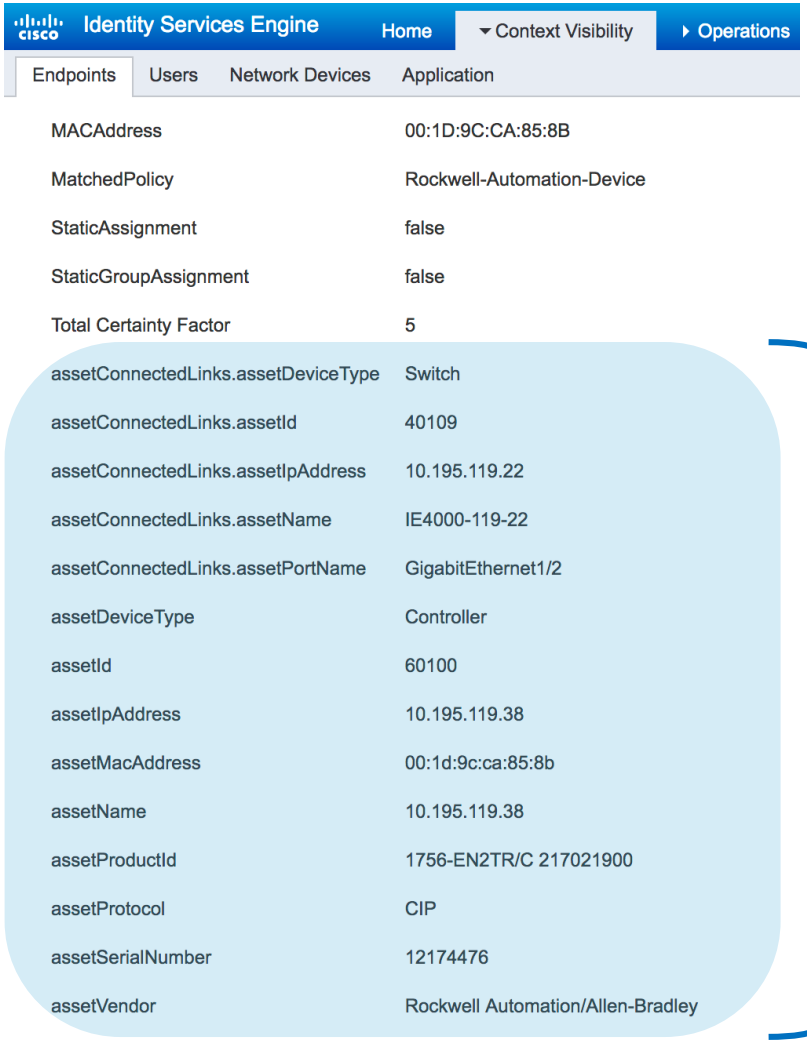
- IND communicates with Industrial Switches and Security Devices and collects detailed information about the connected manufacturing devices.
- IND vX adds pxGrid Publisher interface to communicate IoT attributes to ISE.



pxGrid-In

Probe Attributes

- Endpoint Attribute Details
- Core set of pxGrid Profile attributes
- Vendors can also send custom attributes



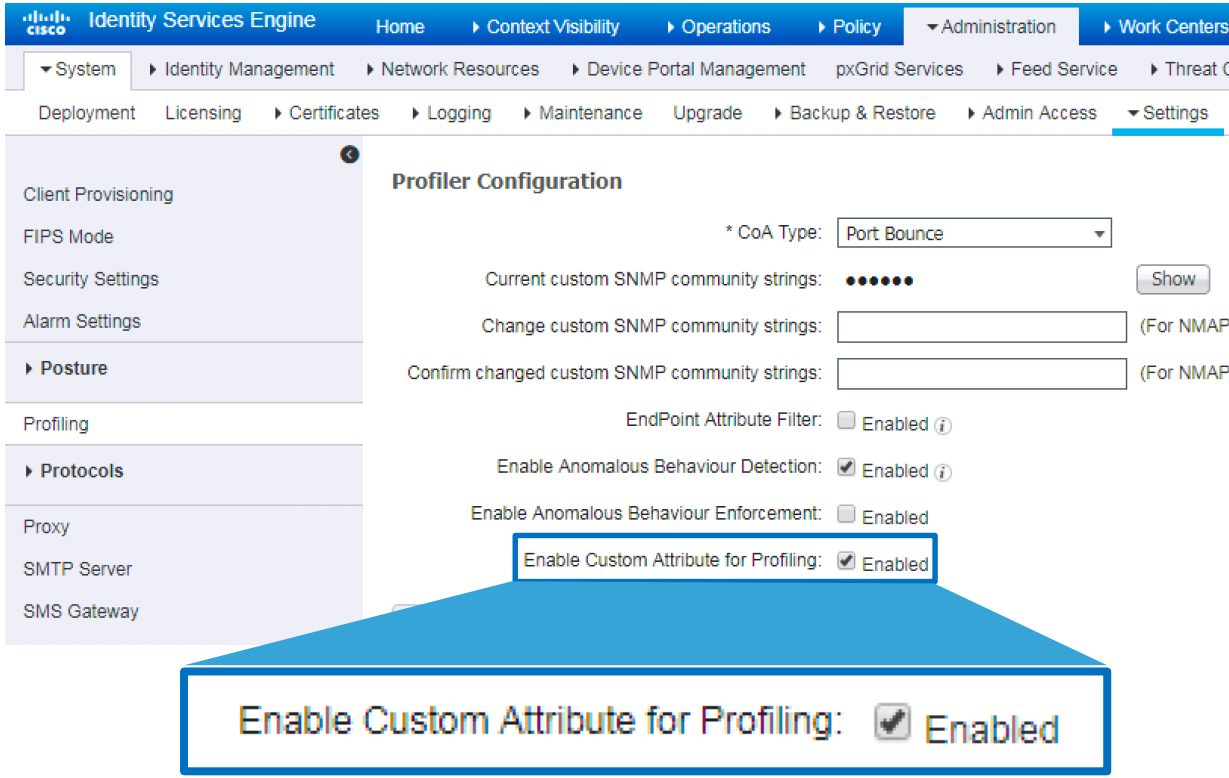
pxGrid Probe Attributes from IND

Profiling Based on Custom Attributes

Performance Hit so Disabled By Default

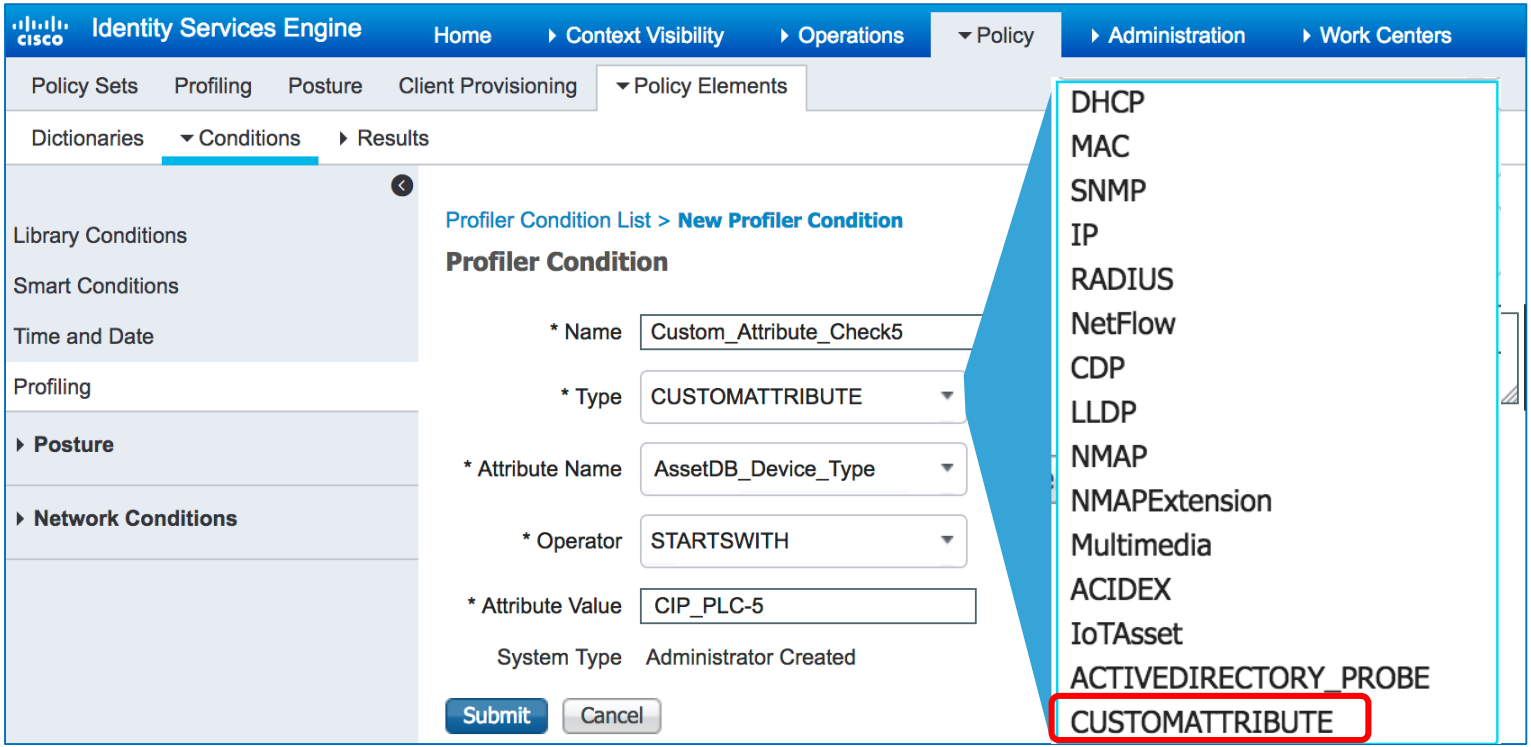
New in ISE 2.4

- Global Setting MUST be **enabled**
- If disabled:
  - Custom Attributes are NOT updated over pxGrid
  - Profiler ignores any conditions based on Custom Attributes, even if Custom Attribute is populated.



Profiler Conditions Based on Custom Attributes

New in ISE 2.4



ISE 2.4 - New Profile Policies by the Numbers

Delivered Via Feed Service

- New Profiles:
  - Xerox – 45
  - HP – 139
  - Brother – 174
  - Cisco AP – 4
  - Fingerbank – 36
  - Audio Code – 7
  - Lexmark - 187
  - Customer – 38

Total = **630**

- Updated Profiles:
  - Xerox – 140
  - HP – 37
  - Brother – 4
  - Lexmark – 4

Total = **185**

New and Updated IoT Profile Libraries (Coming March 2018)

Delivered via ISE Community: https://communities.cisco.com/docs/DOC-66340

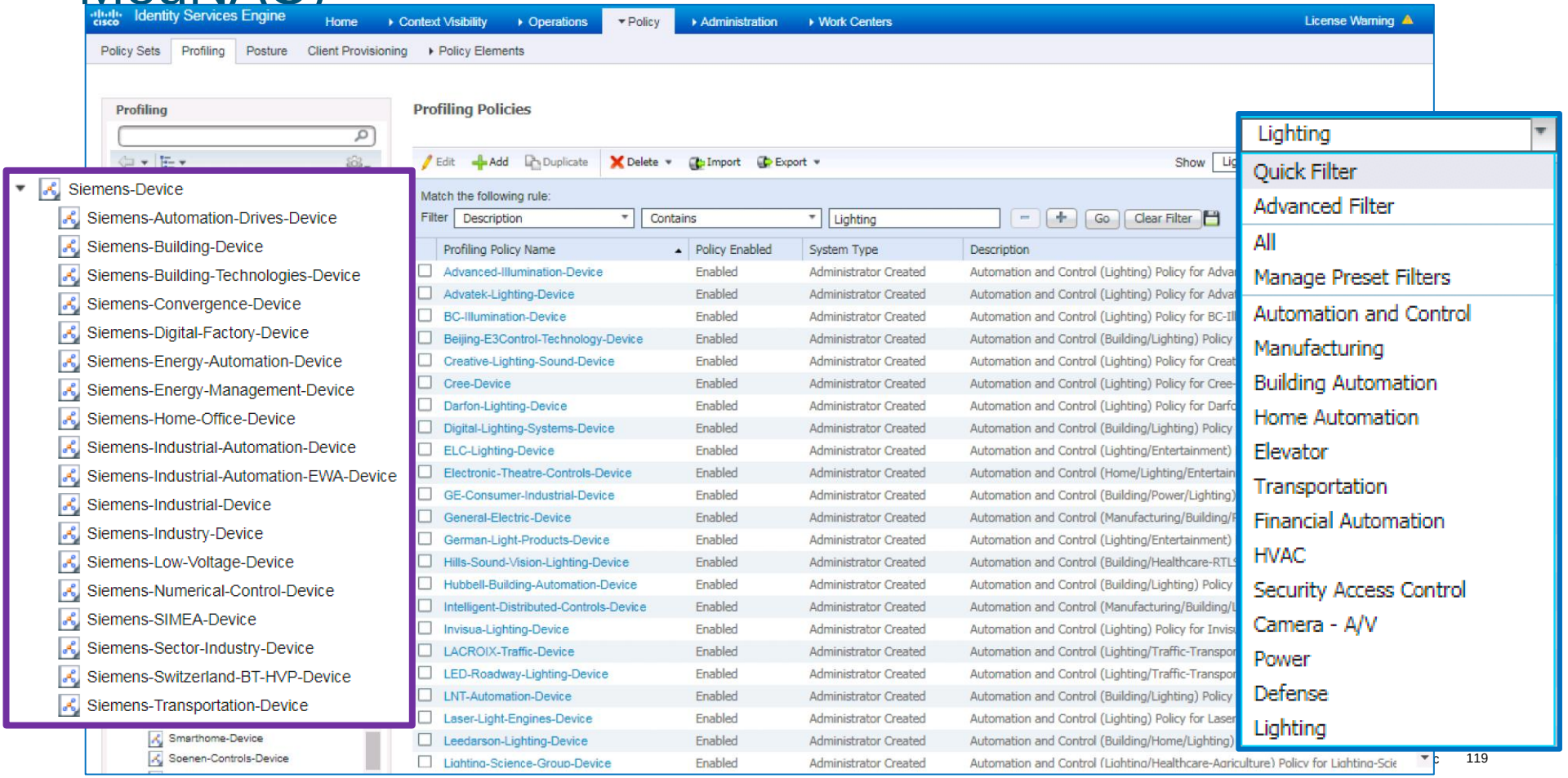
- Automation and Control
  - Industrial / Manufacturing
  - Building Automation
  - Power / Lighting
  - Transportation / Logistics
  - Financial (ATM, Vending, PoS, eCommerce)
  - IP Camera / Audio-Video / Surveillance and Access Control
  - Other (Defence, HVAC, Elevators, etc)
- Windows Embedded
-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








600+ Automation and Control Profiles (~900 with MedNAC)



Why Do I Care About # Profiles?

- ISE 2.1+ supports a MAX of **2000** profiles
- Let's Do the Math…
  - ~600 Base Profiles
  - ~600 New Feed Profiles (2.4)
  - ~275 Medical NAC Profiles
  - ~625 Automation & Control Profiles

  ~2100 Profiles

- No restrictions on profile import, so must check # profiles in library before import large batch of new profiles

Scaling MnT (Optimise Logging and Noise Suppression)

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. Common issue is setting timeouts too low & not throttling misbehaving clients.
- 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 behaviour when above issues occur.
- Bugs in client, NAD, or ISE.

A Few Bad Apples Can Spoil the Whole Bunch

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

Getting More Information With Less Data

Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source

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

Heartbeat frequency

Reauth phones

Switch

Quiet period

Unknown users

Quiet Period

Roaming supplicant

WLC

Client Exclusion

Misbehaving supplicant

LB

LB Health probes

Filtering at Receiving Chain

Detect and reject misbehaving clients

Log Filter

Reject bad supplicant

PSN

PSN

Filter health probes from logging

Count and discard repeated events

Count and discard untrusted events

MNT

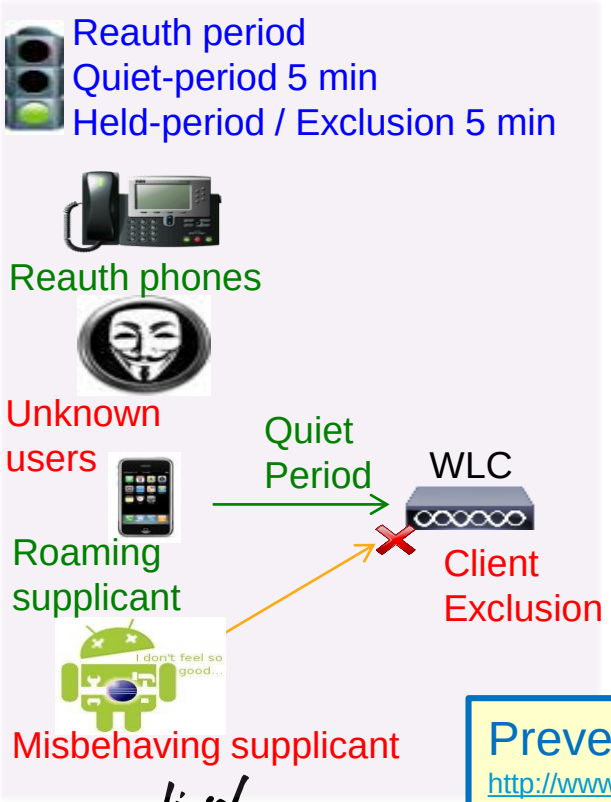
MnT

Count and discard repeats and unknown NAD events

Tune NAD Configuration

Rate Limiting at Wireless Source

BRKSEC-2059 Deploying ISE in a Dynamic Environment - Clark Gambrel



Wireless (WLC)

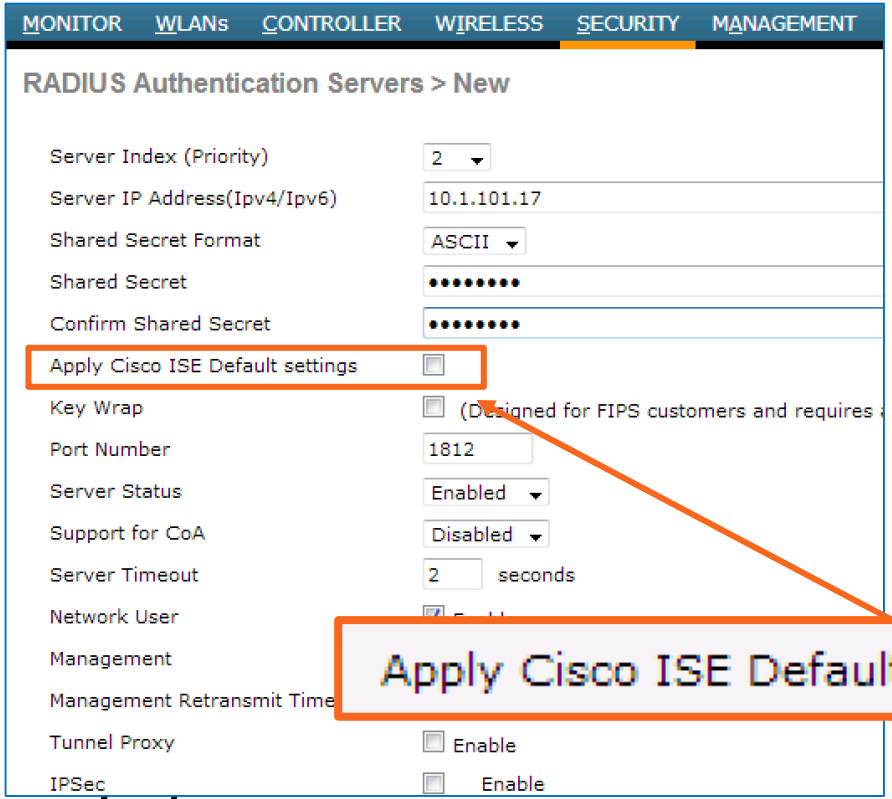
- **RADIUS Server Timeout:** Increase from default of 2 to 5 sec
- **RADIUS Aggressive-Failover:** Disable aggressive failover
- **RADIUS Interim Accounting:** v7.6: Disable; v8.0+: Enable with interval of 0. (Update auto-sent on DHCP lease or Device Sensor)
- **Idle Timer:** Increase to 1 hour (3600 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

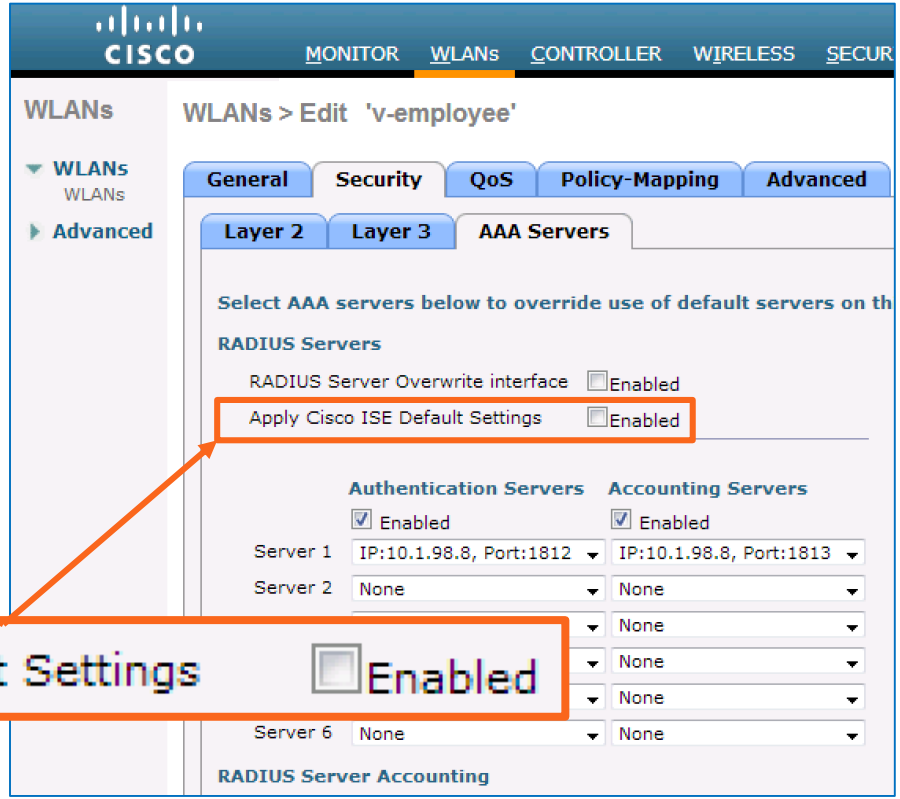
Prevent Large-Scale Wireless RADIUS Network Melt Downs

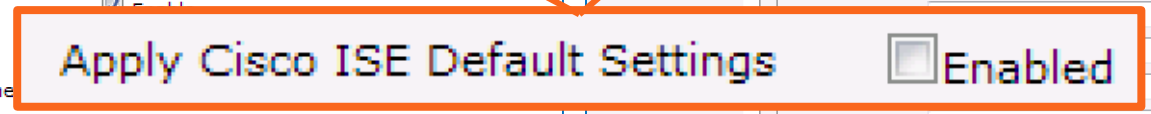
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118703-technote-wlc-00.html

One-Click Setup for ISE Best Practice Config

Added in WLC 8.4







Which WLC Software Should I Deploy?

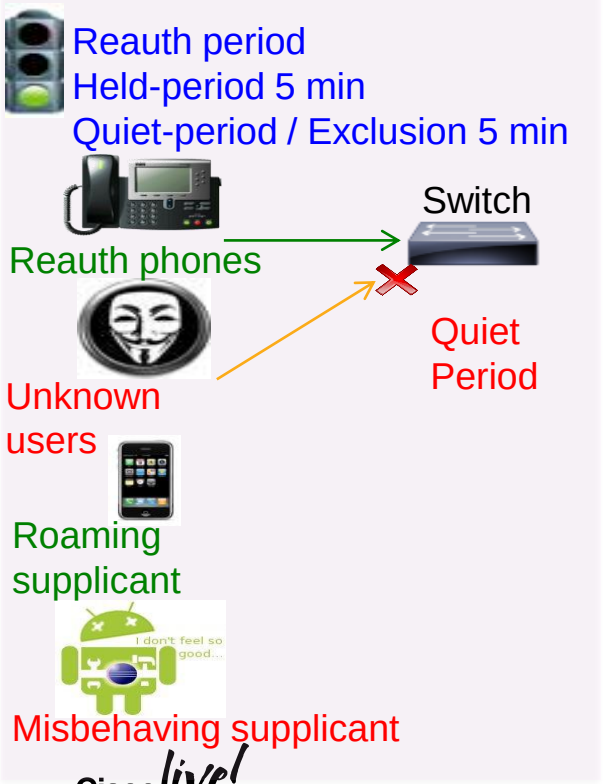
- **8.0.152.0** – Currently the most mature and reliable release.
- **8.2.166.0** – Mature - Recommended when need new feature/hardware support.
- **8.3.133.0** – Less Mature – Recommend if require new features in 8.3.x
- **8.5.110.0** – Cutting edge – Recommend if require new features in 8.5.x
- **8.6.101.0** – Bleeding edge – Only if absolutely require new features in 8.6.x
- Example critical defects resolved in maintenance and new releases:

CDETS	Title
CSCul83594	Session-id is not synchronised across mobility, if the network is open (fixed in 8.6)
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuu68490	duplicate radius-acct update message sent while roaming
CSCus61445	DNS ACL on wlc is not working - AP not Send DTLS to WLC
CSCuq48218	Cisco WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCuo09947	RADIUS AVP #44 (Acct-Session-ID) to be sent in RADIUS authentication messages

https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-TAC-Recommended-AireOS.html

Tune NAD Configuration

Rate Limiting at Wired Source



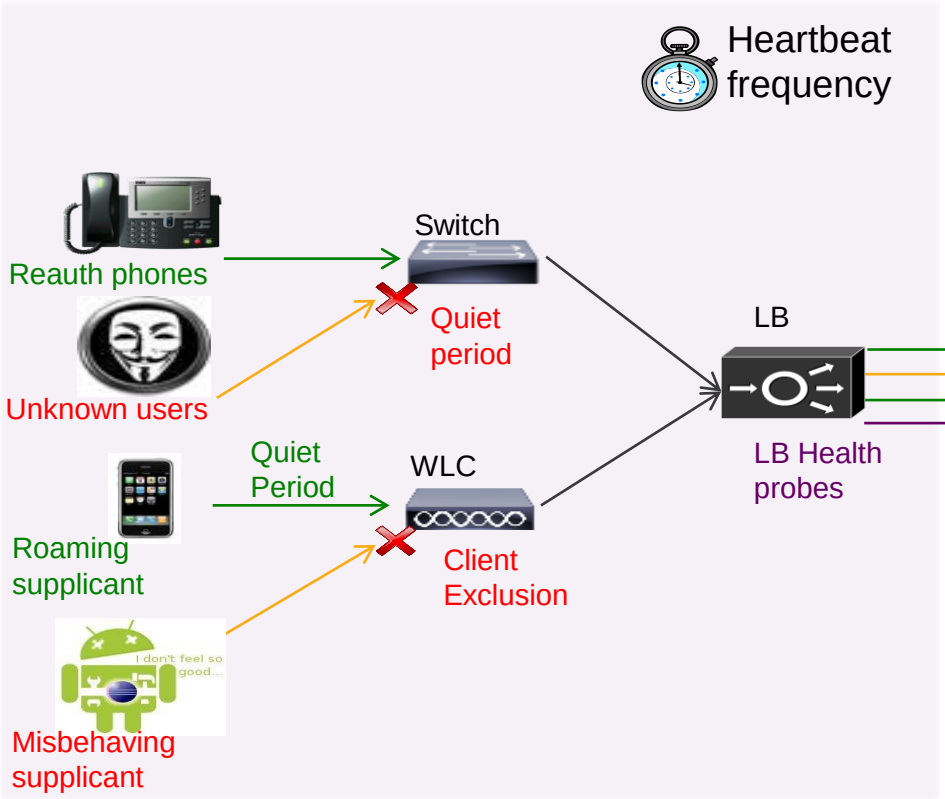
Wired (IOS / IOS-XE)

- **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 persistence 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.

RADIUS Test Probes

Reduce Frequency of RADIUS Server Health Checks

For Your Reference

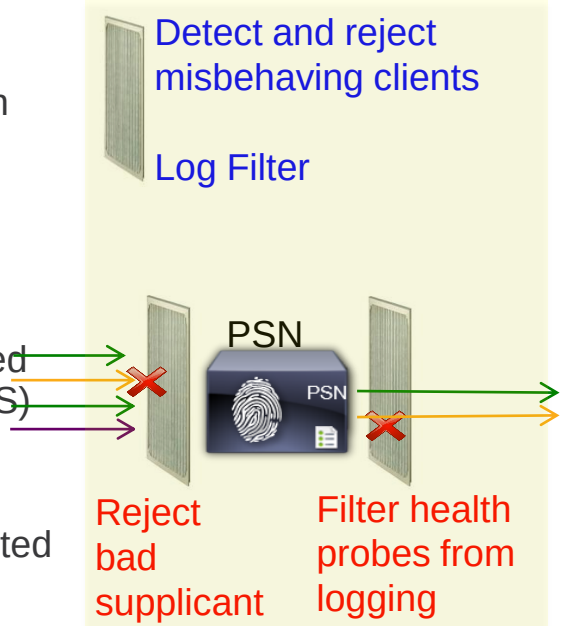


- **Wired NAD**: RADIUS test probe interval set with **idle-time** parameter in radius-server config; Default is 60 minutes
  - No action required
- **Wireless NAD:** If configured, WLC only sends “active” probe when server marked as dead.
  - No action required
- **Load Balancers:** Set health probe intervals and retry values short enough to ensure prompt failover to another server in cluster occurs prior to NAD RADIUS timeout (typically 20-60 sec.) but long enough to avoid excessive test probes.

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



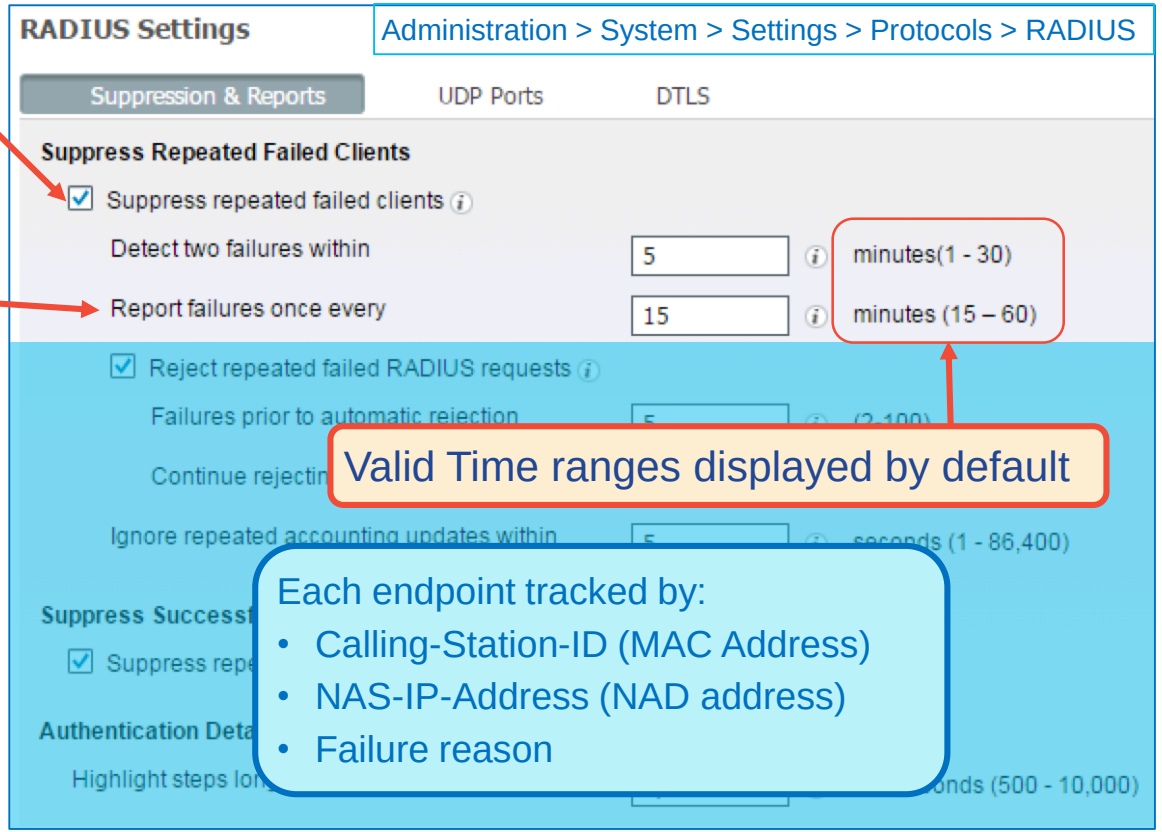
PSN Filtering and Noise Suppression

Dynamic Client Suppression

ISE 2.2+

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

Send alarm with failure statistics



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

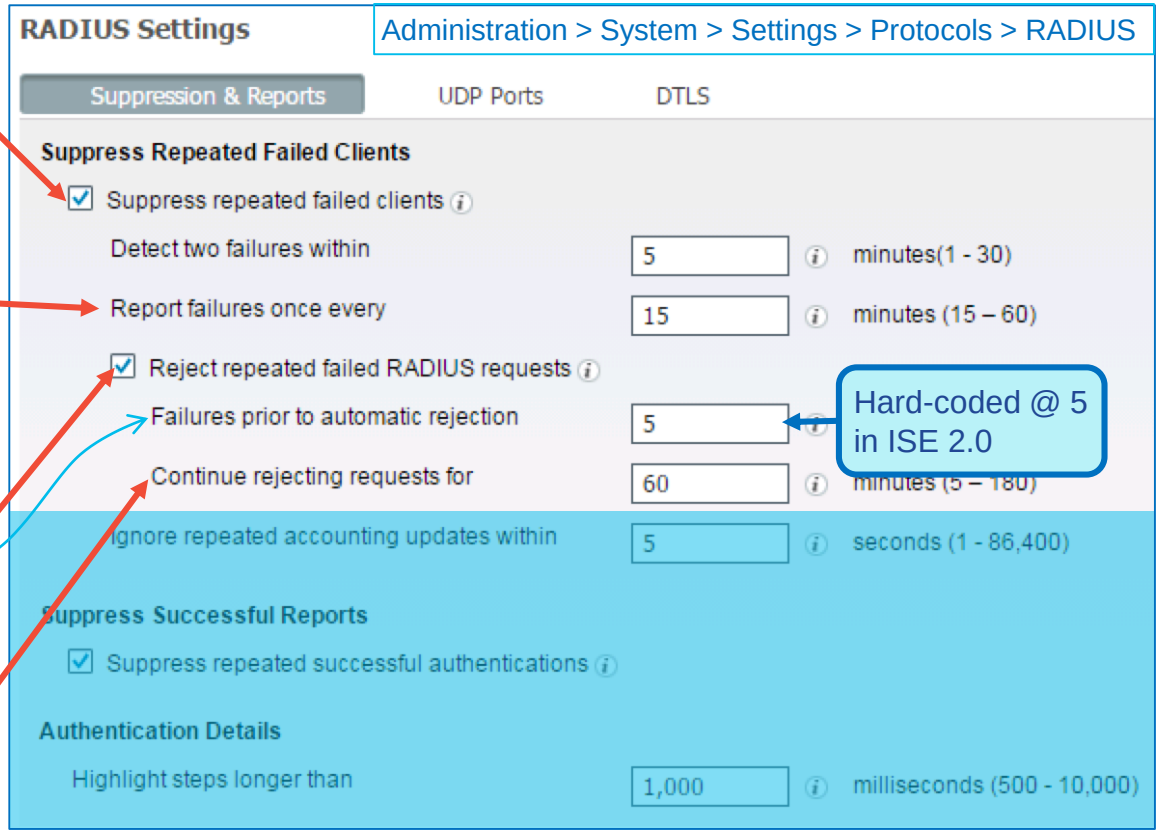
Dynamic Client Suppression

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)

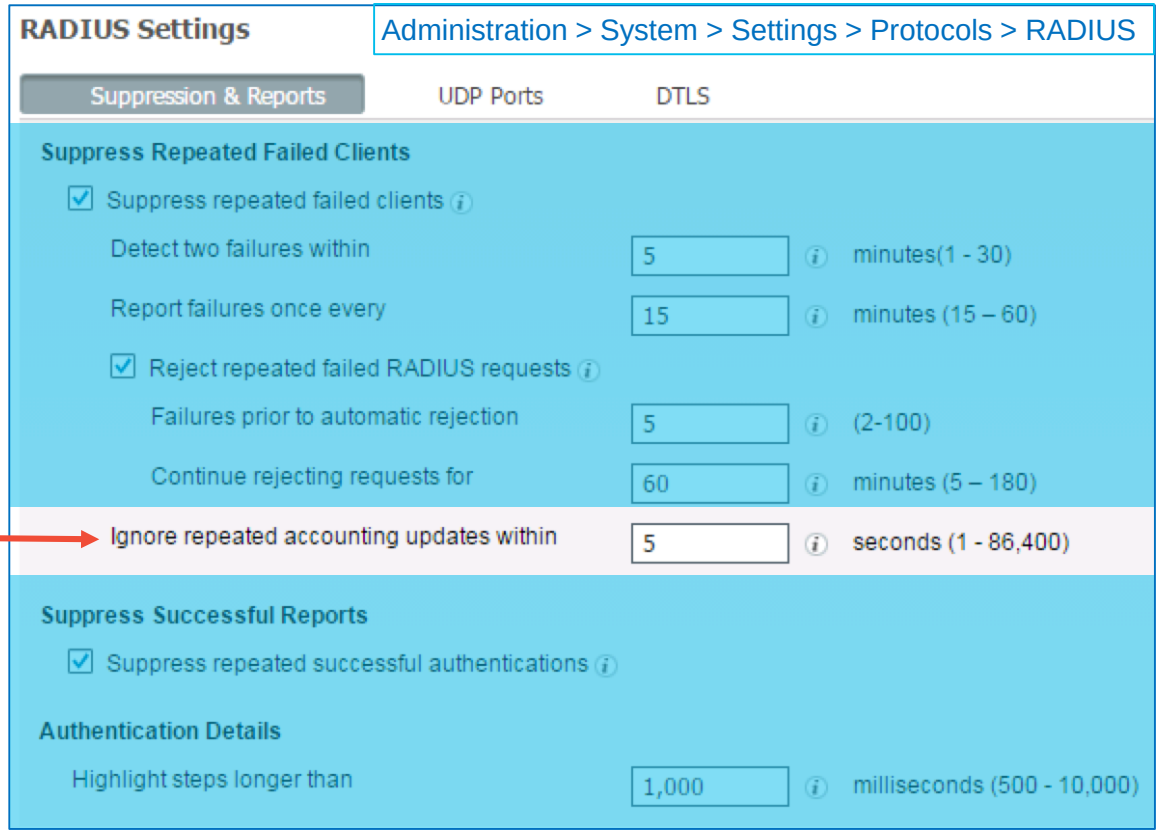
Fully process next request after rejection period expires.



PSN Noise Suppression

Drop Excessive RADIUS Accounting Updates from “Misconfigured NADs”

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



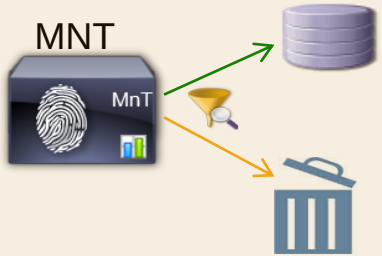
MnT Log Suppression and Smarter Logging

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



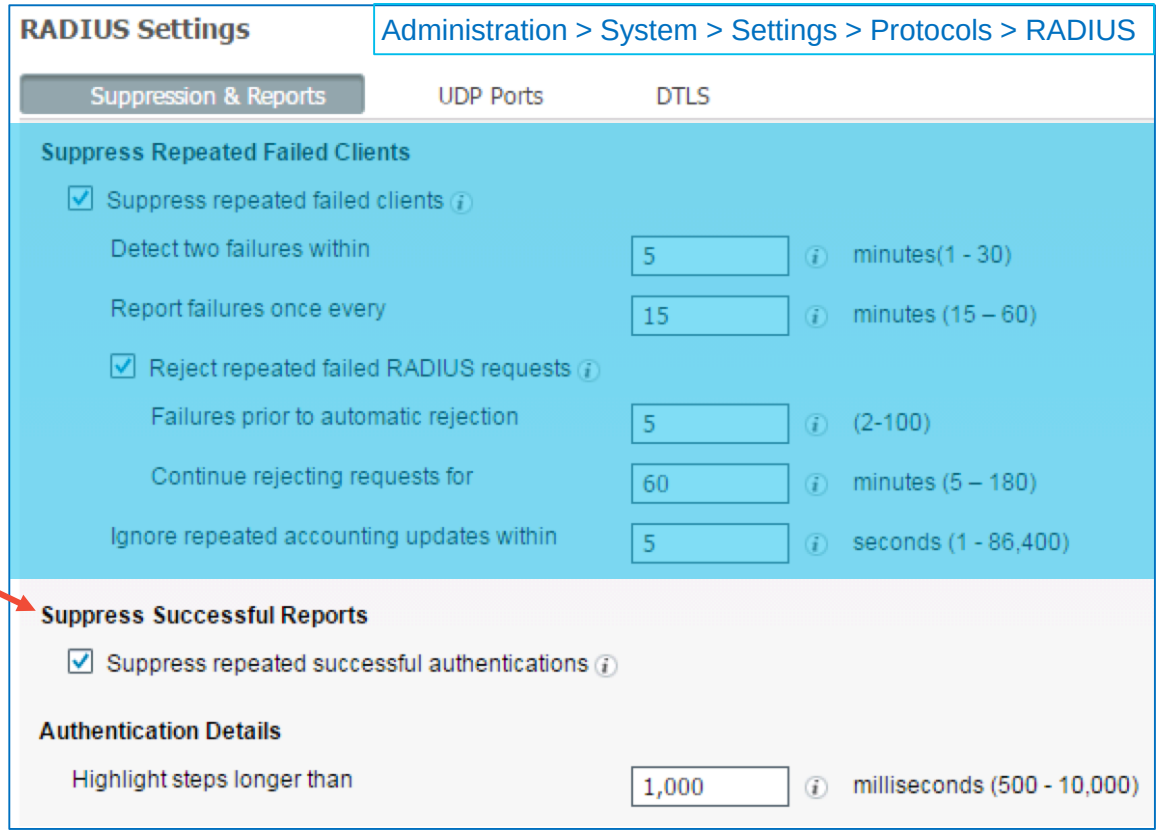
Count and discard repeats and unknown NAD events

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.



MnT Noise Suppression

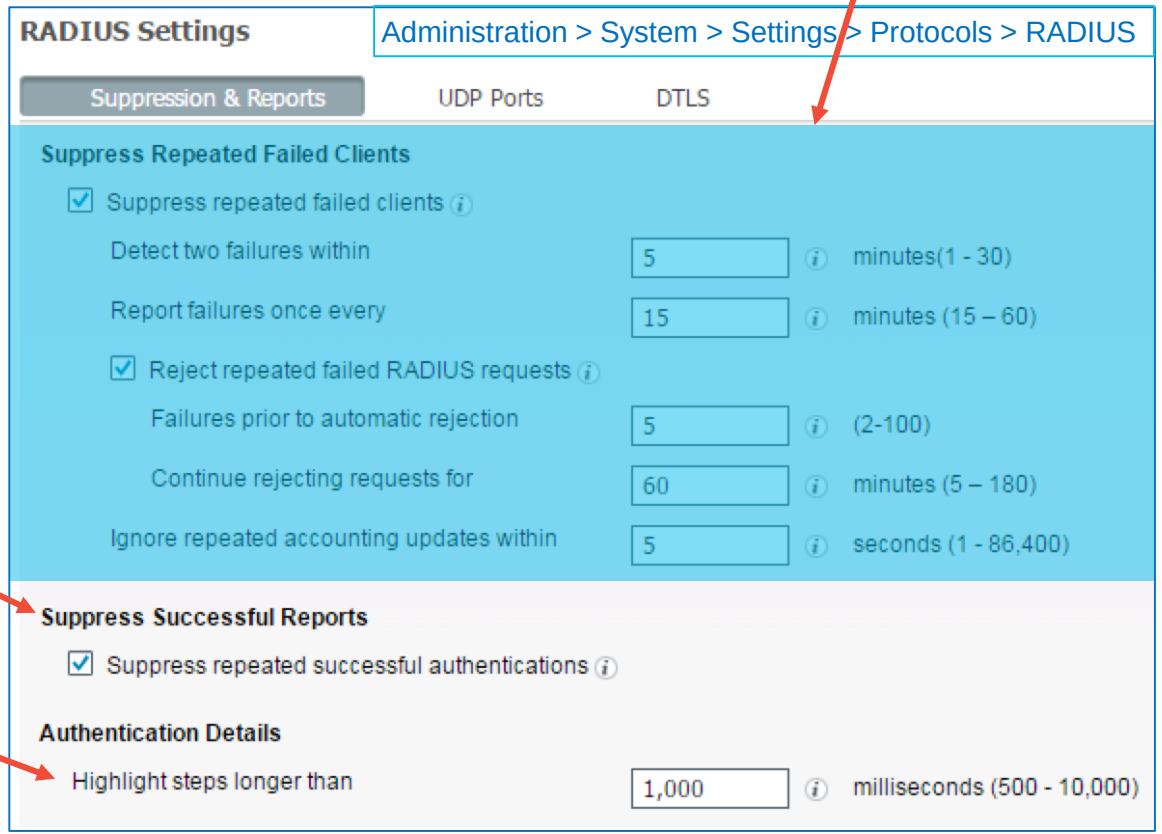
Suppress Storage of Repeated Successful Auth Events

Step latency is visible in Live Logs details

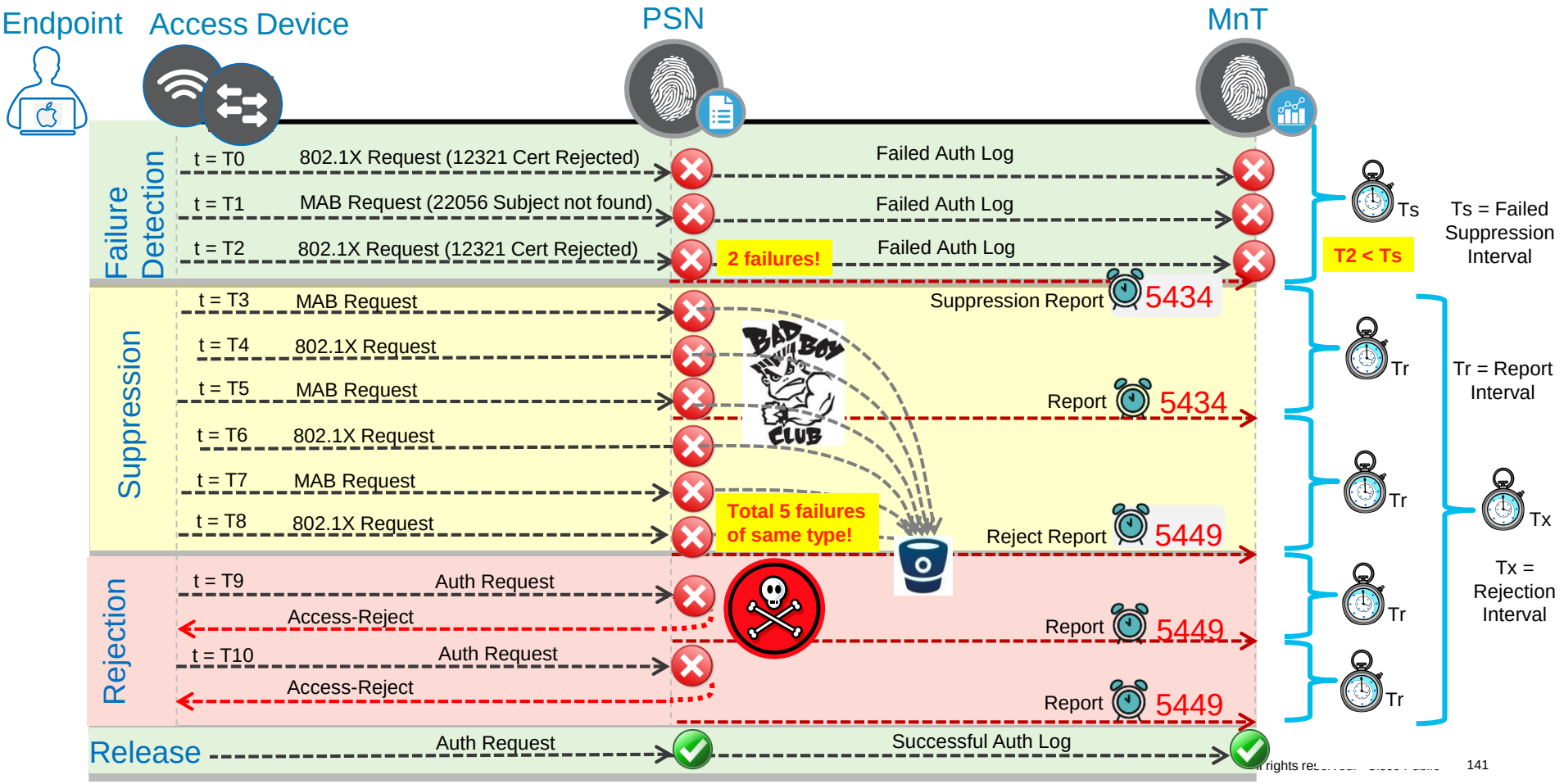
Suppress Successful Reports
= Do not save repeated successful auth events for the same session to MnT DB

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

Detect NAD retransmission timeouts and Log auth steps > threshold.

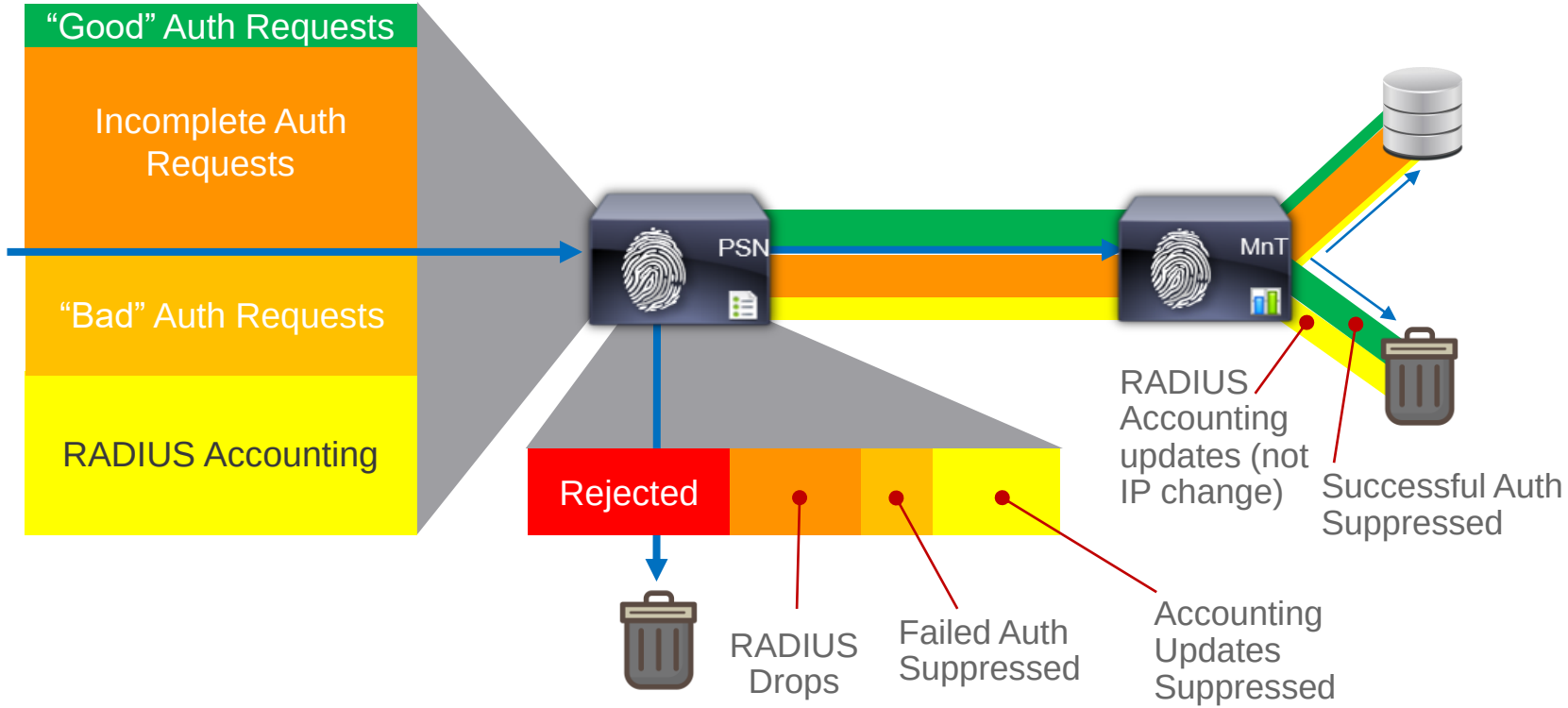


Client Suppression and Reject Timers

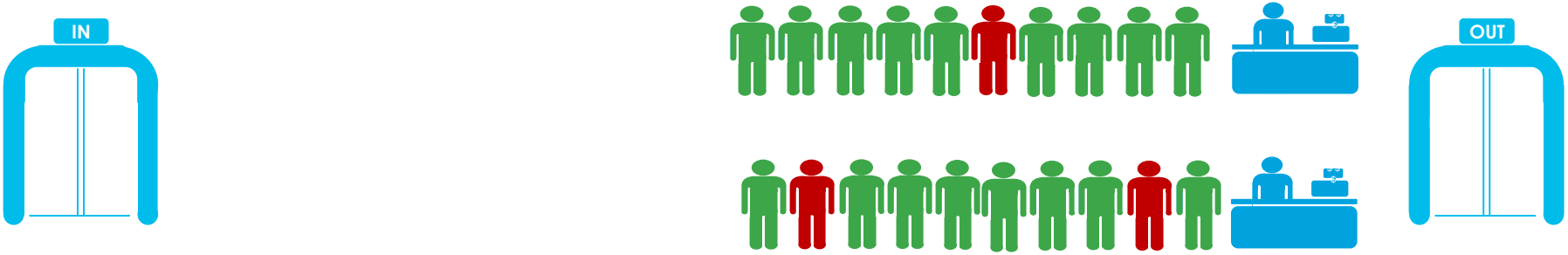


ISE Log Suppression

“Good”-put Versus “Bad”-put



Typical Load Example

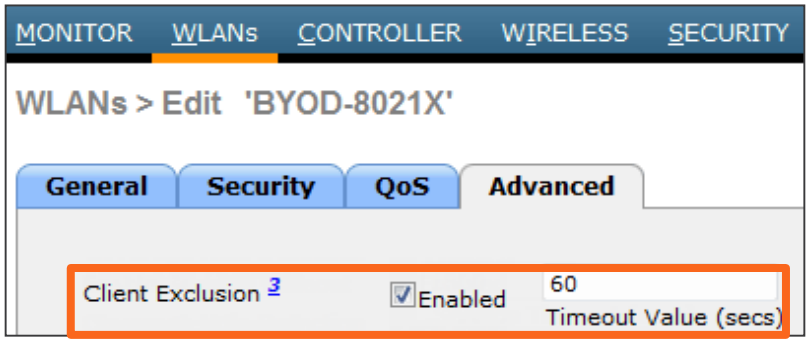


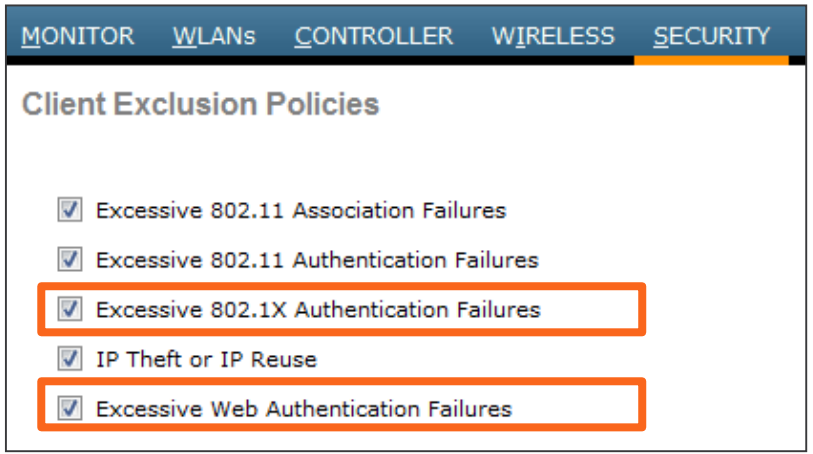
Extreme Noise Load Example

WLC – Client Exclusion

Blacklist Misconfigured or Malicious Clients

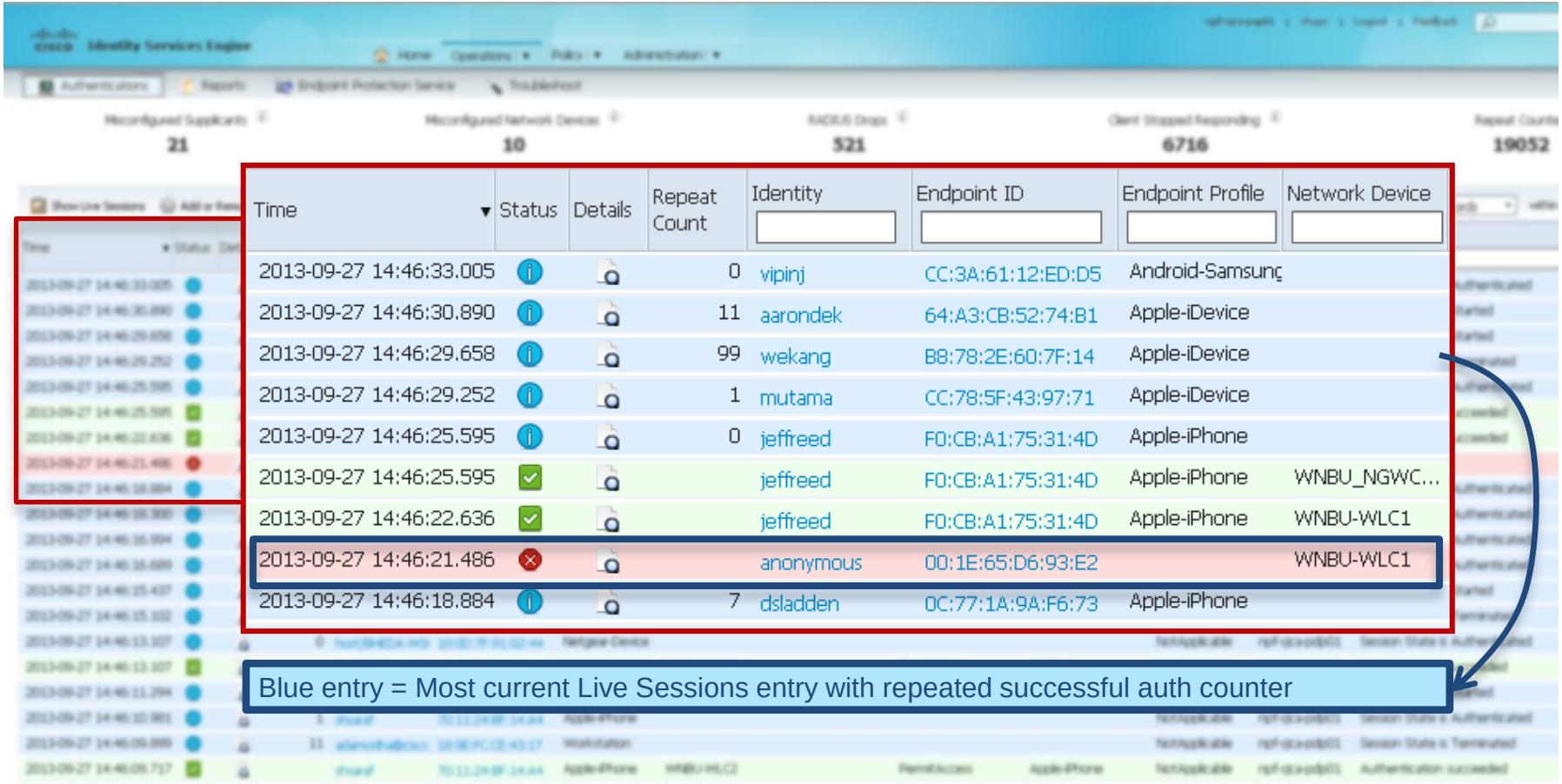
- **Excessive Authentication Failures**—Clients are excluded on the fourth authentication attempt, after three consecutive failures.
- Client excluded for Time Value specified in WLAN settings. Recommend increase to 1-5 min (60-300 sec). **3 min** is a good start.





Note: Diagrams show default values

Live Authentications and Sessions



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 ☑ ⓘ

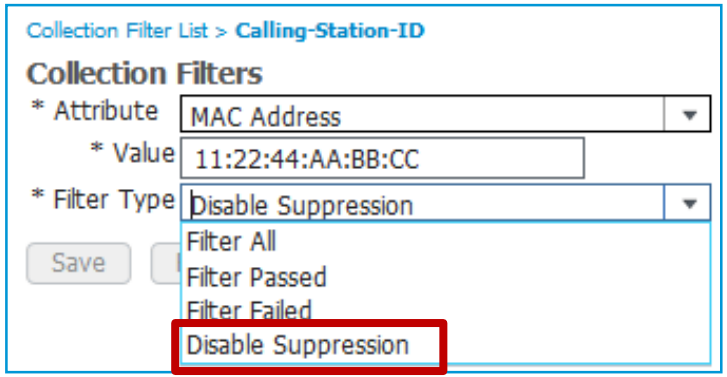
Caution: Do not disable suppression in deployments with very high auth rates.

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

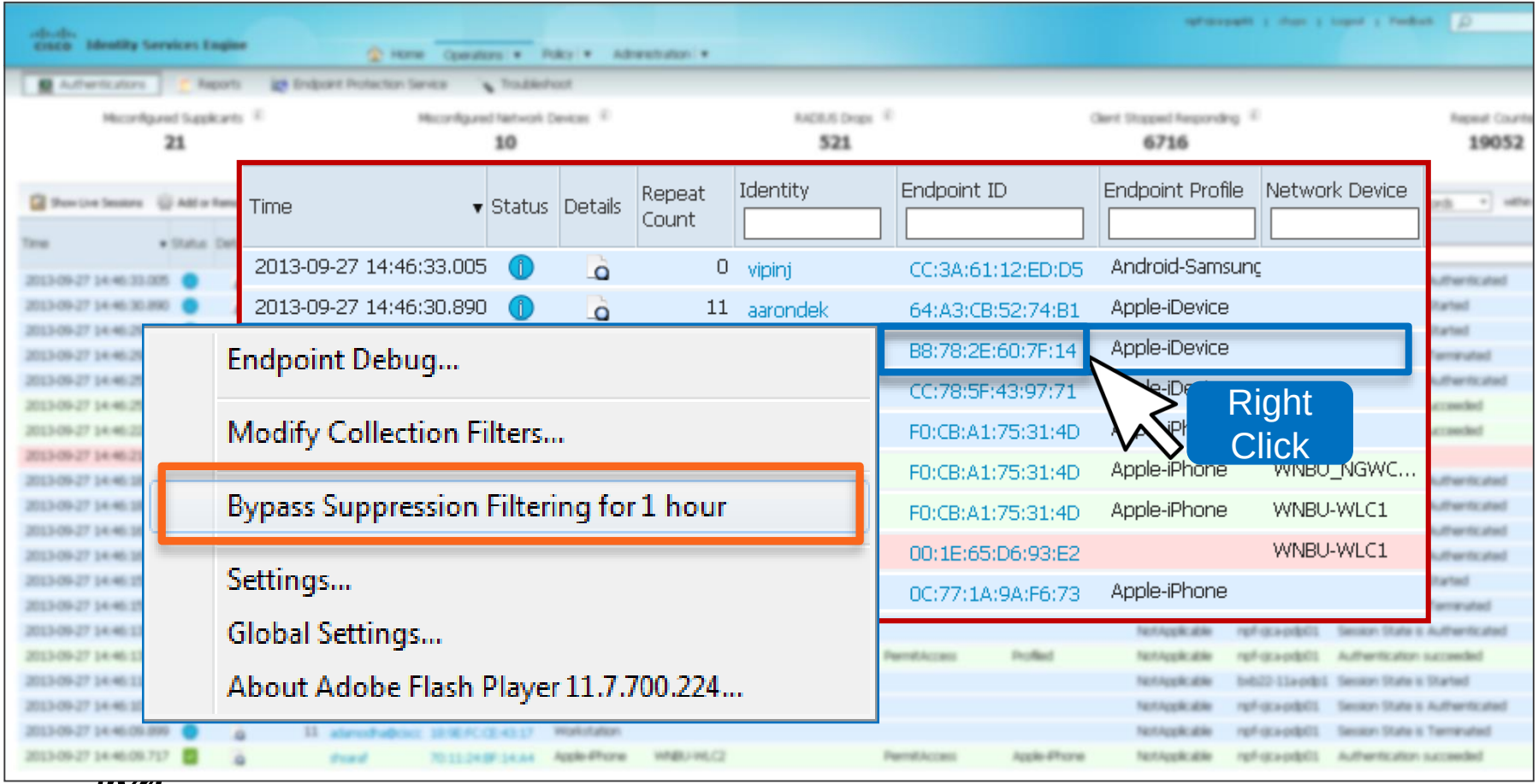
- **Selective Suppression using Collection Filters:** Administration > System > Logging > Collection Filters

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.

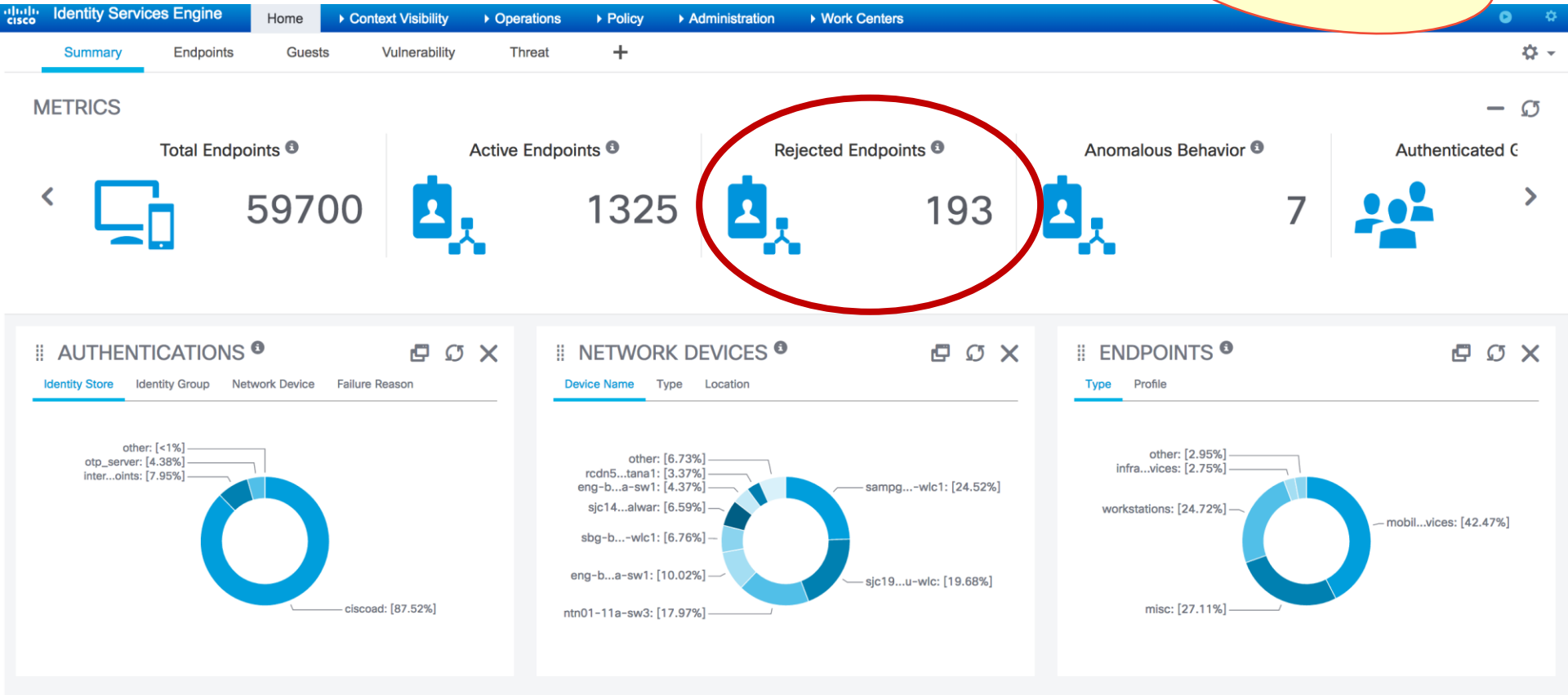


Per-Endpoint Time-Constrained Suppression



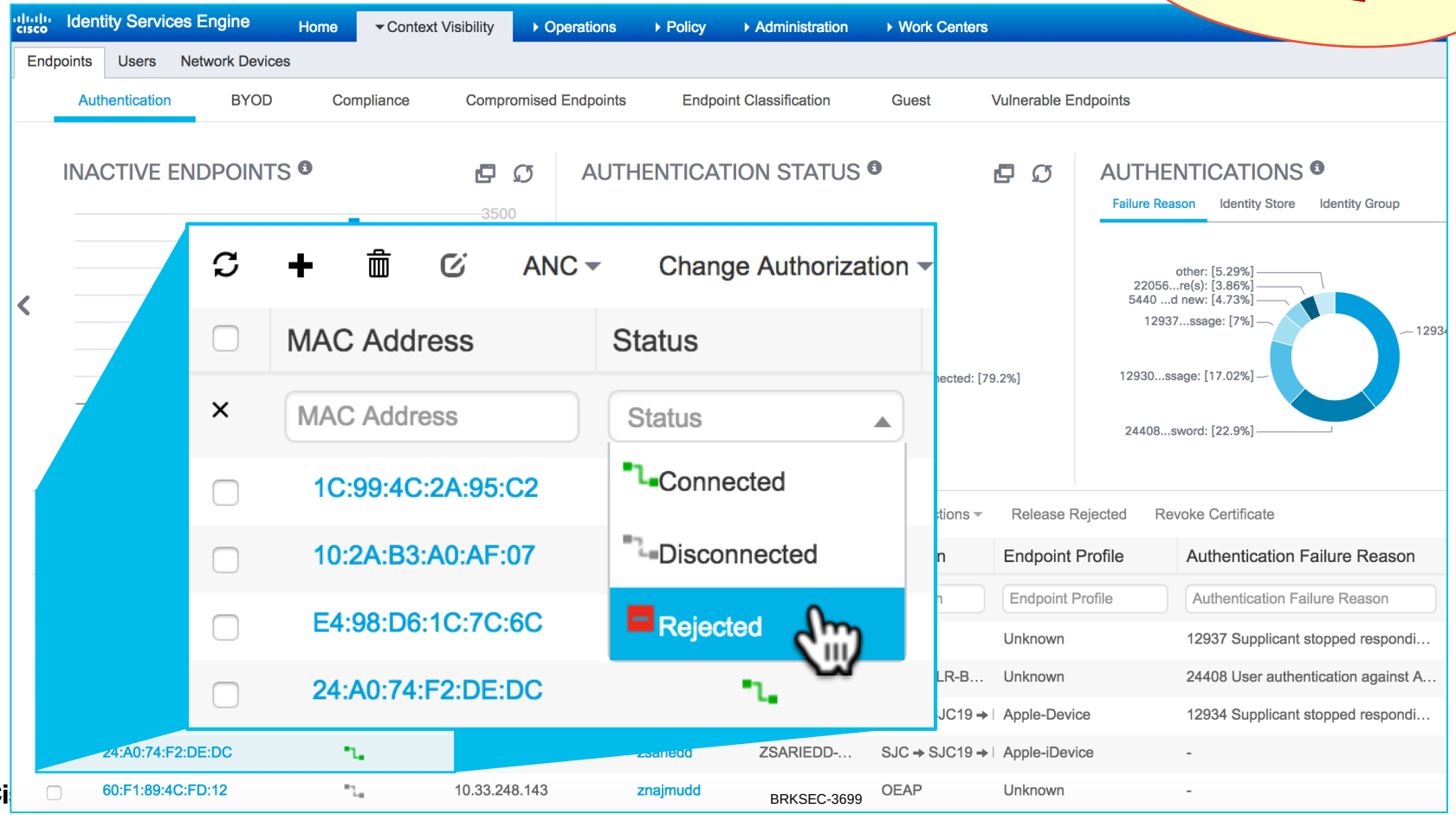
Visibility Into Reject Endpoints!

ISE 2.2+

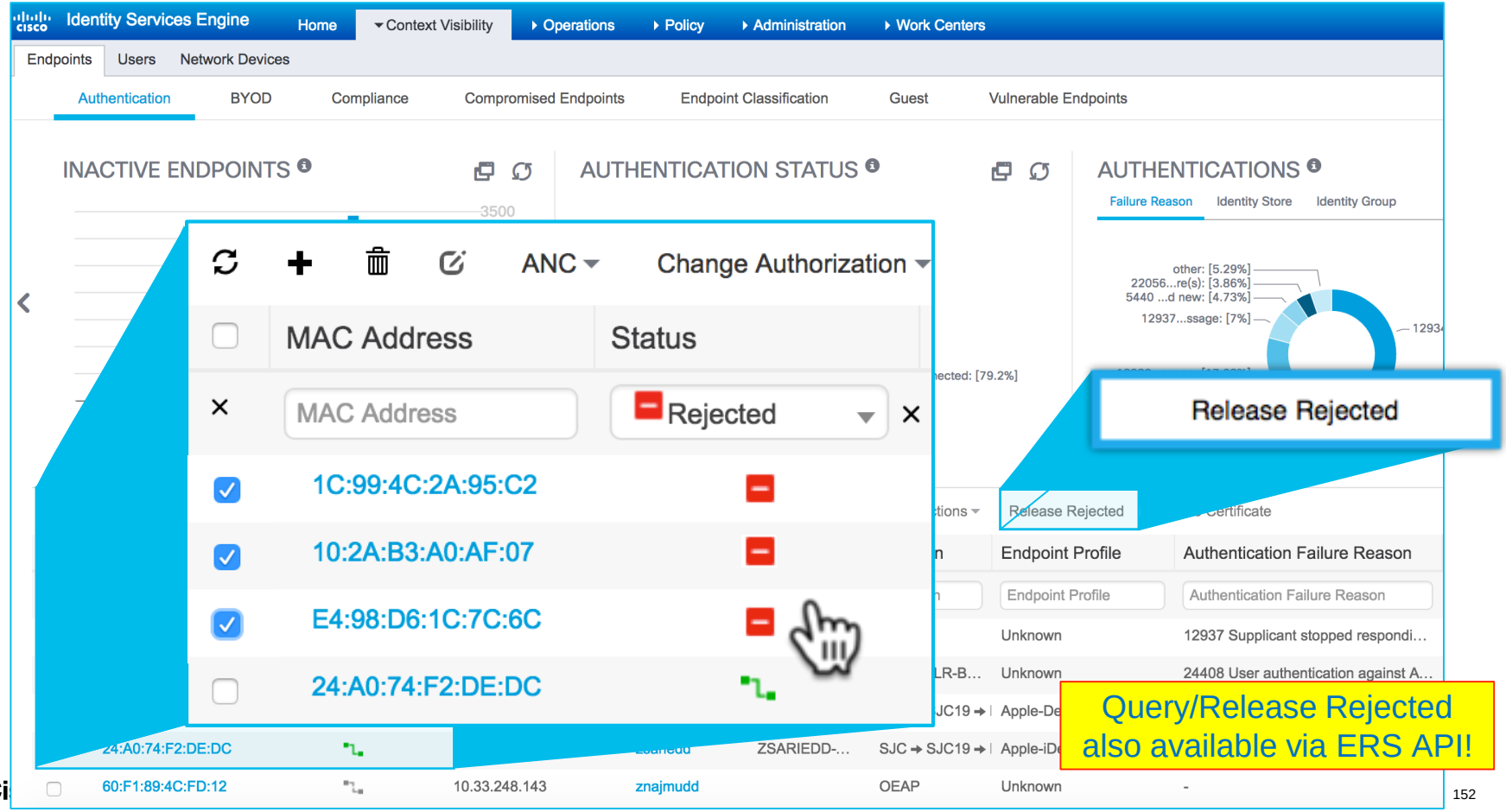


Releasing Rejected Endpoints

ISE 2.2+



Releasing Rejected Endpoints



No Log Suppression

With Log Suppression

Distributed Logging

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

ISE Appliance Redundancy

Appliance Redundancy

In-Box High Availability

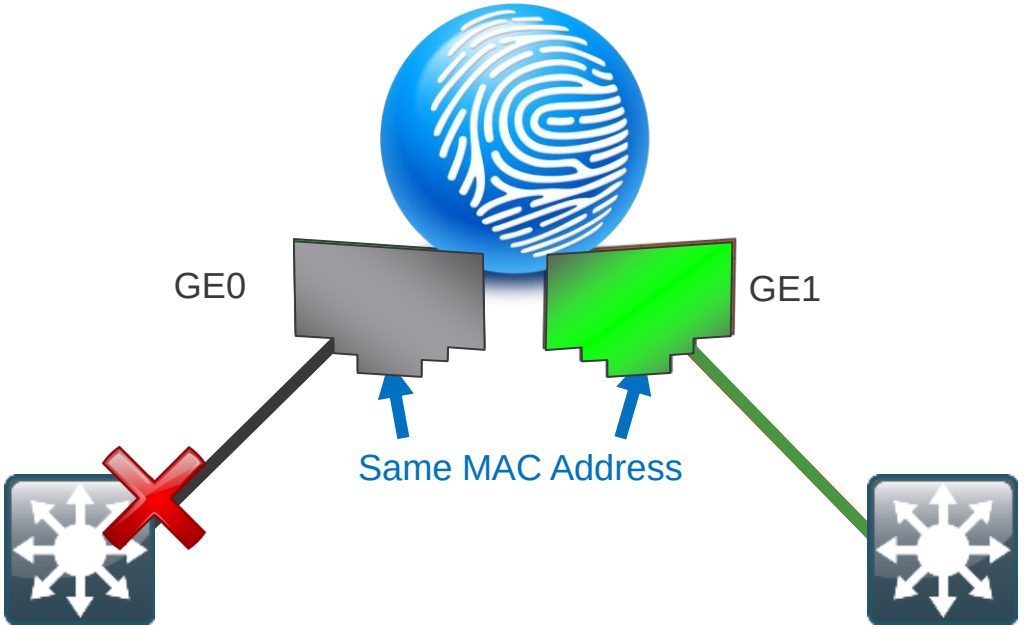
SNS-3500 Series

Platform	SNS-3415 (34x5 Small)	SNS-3495 (34x5 Large)	SNS-3515 (35x5 Small)	SNS-3595 (35x5 Large)
Drive Redundancy	**No** (1) 600GB disk	**Yes** (2) 600-GB	**No** (1) 600GB disk	**Yes** (4) 600GB disk
Controller Redundancy	**No**	**Yes** (RAID 1)	**No** (1GB FBWC Controller Cache)	**Yes** (RAID 10) (1GB FBWC Cache)
Ethernet Redundancy	**Yes*** 4 GE NICs = Up to 2 bonded NICs	**Yes*** 4 GE NICs = Up to 2 bonded NICs	**Yes*** 6 GE NICs = Up to 3 bonded NICs	**Yes*** 6 GE NICs = Up to 3 bonded NICs
Redundant Power	**No** (2nd PSU optional) UCSC-PSU-650W	**Yes**	**No** (2nd PSU optional) UCSC-PSU1-770W	**Yes**

* ISE 2.1 introduced NIC Teaming support for High Availability only (not active/active)

Bonded Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over



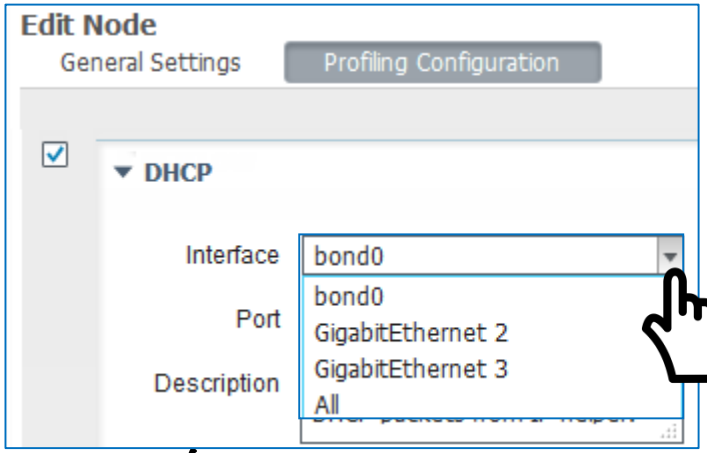
- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

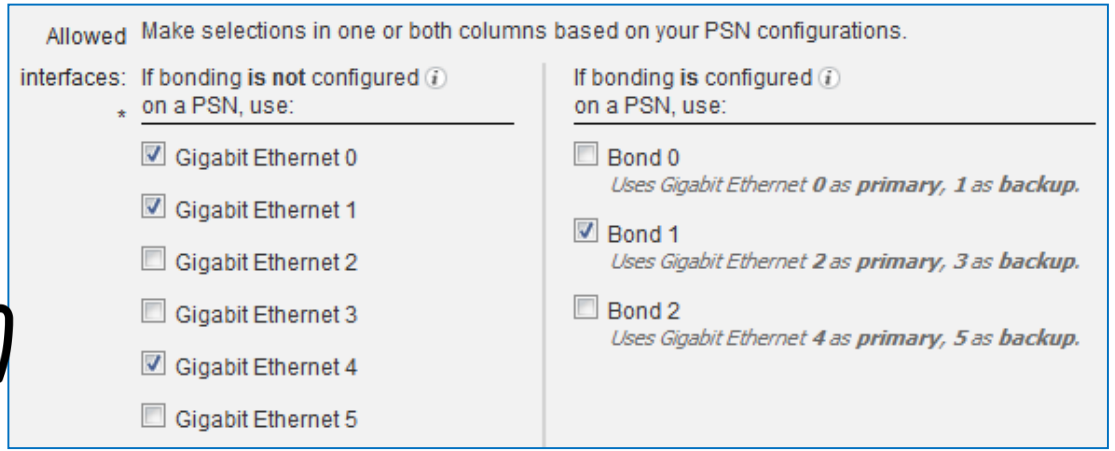
NIC Teaming

NIC Teaming / Interface Bonding

```
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 10.1.100.18 255.255.255.0
!
interface GigabitEthernet 1
  ipv6 address autoconfig
```

- Configured using CLI only!
- GE0 + GE1 Bonding Example:
  `admin(config-GigabitEthernet0)#` **`backup interface GigabitEthernet 1`**
- Requires service restart. After restart, ISE recognises bonded interfaces for Deployment and Profiling; Guest requires manual config of eligible interfaces.





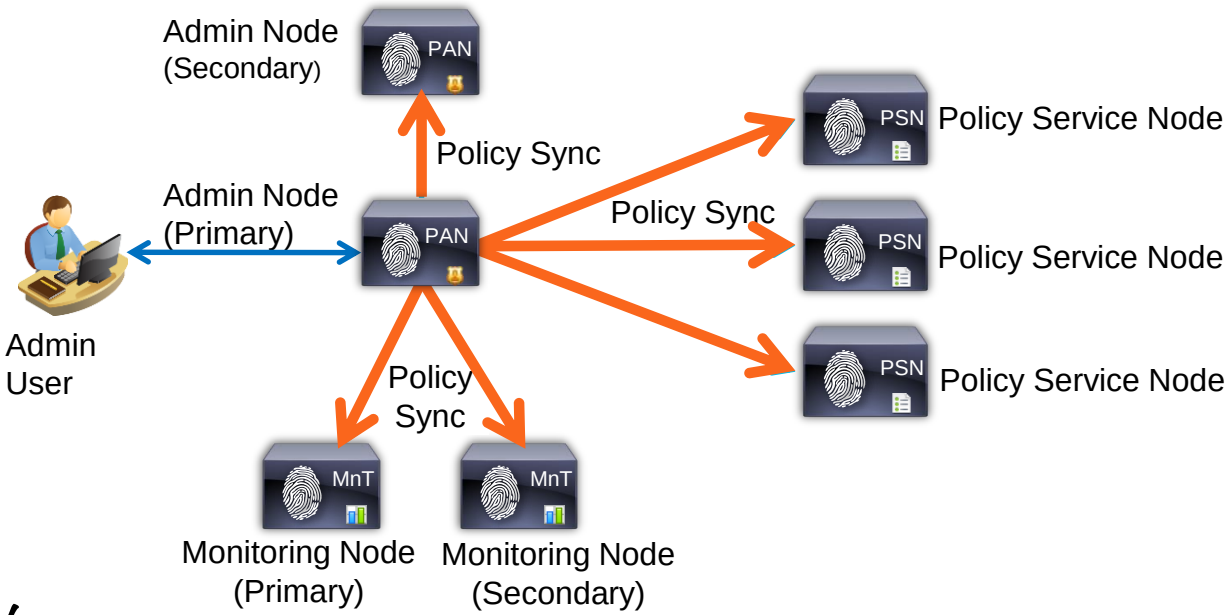
ISE Node/Persona Redundancy

Admin Node HA and Synchronisation

PAN Steady State Operation

- Maximum two PAN nodes per deployment
- Active / Standby

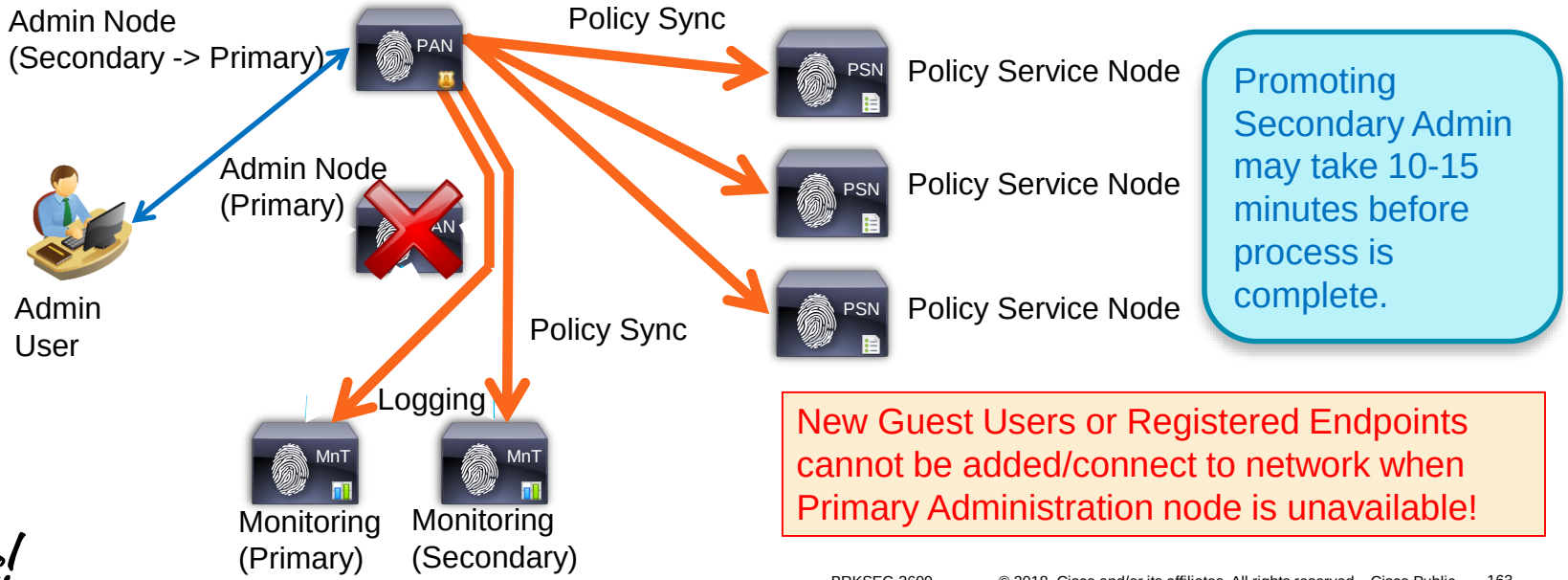
- Changes made to Primary Administration DB are automatically synced to all nodes.



Admin Node HA and Synchronisation

Primary PAN Outage and Recovery

- Prior to ISE 1.4, 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.

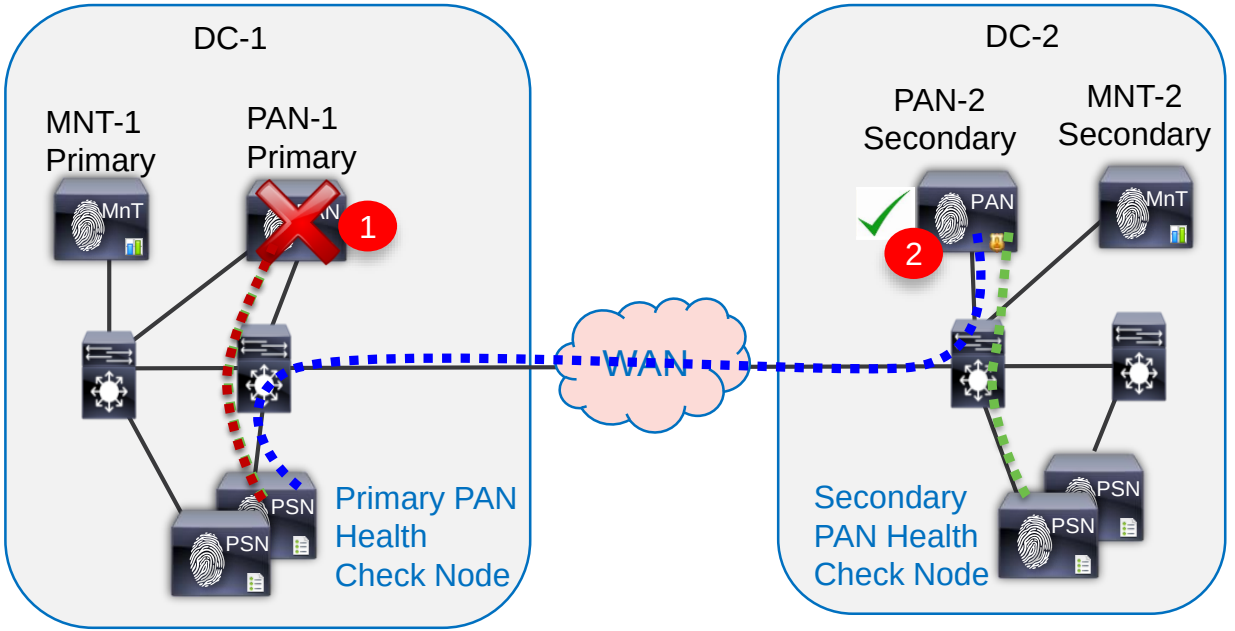


Automatic PAN Switchover

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.

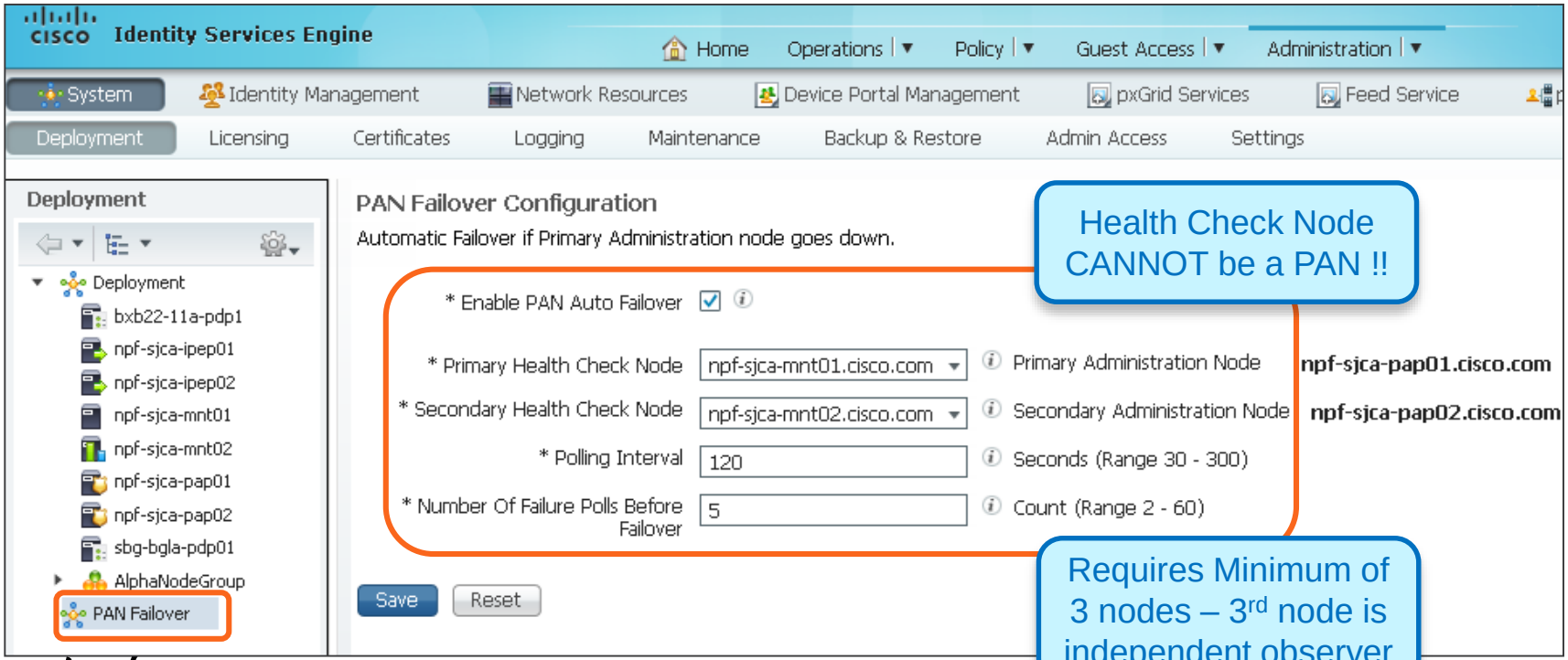


Note: Switchover is NOT immediate. Total time based on polling intervals and promotion time. Expect ~15 - 30 minutes.

PAN Failover

Health Check Node Configuration

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

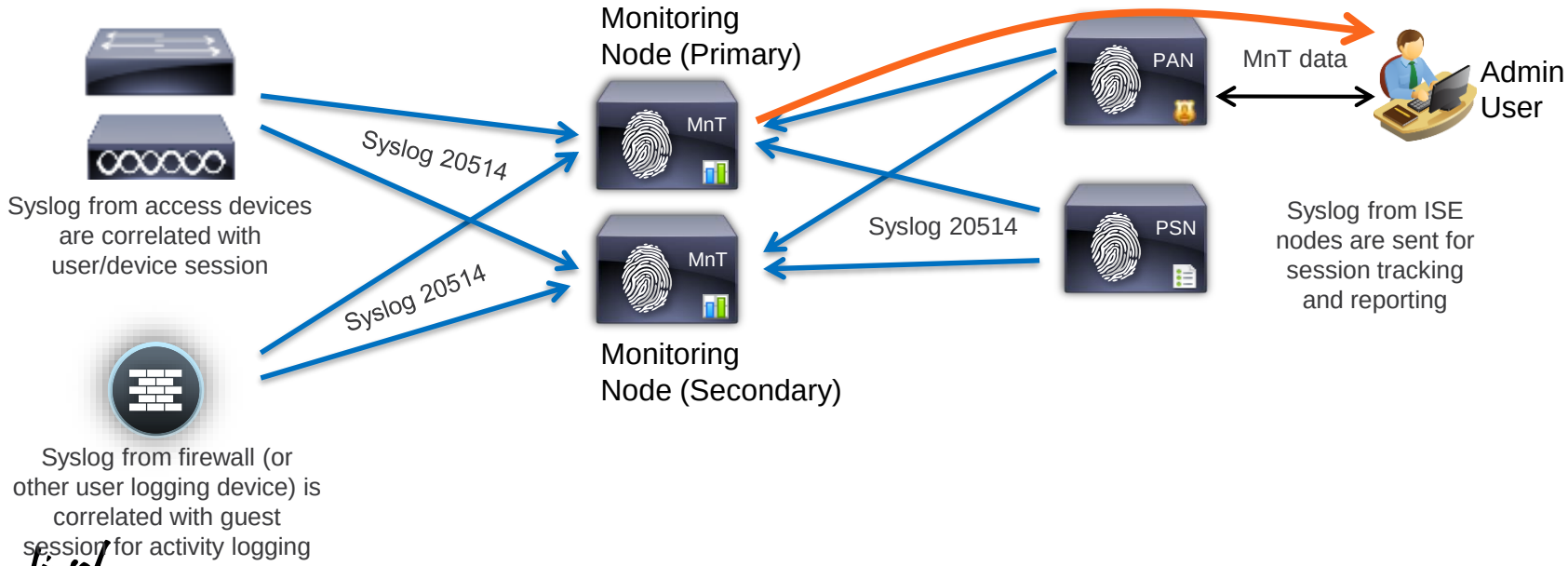


HA for Monitoring and Troubleshooting

Steady State Operation

- Maximum two MnT nodes per deployment
- Active / Active

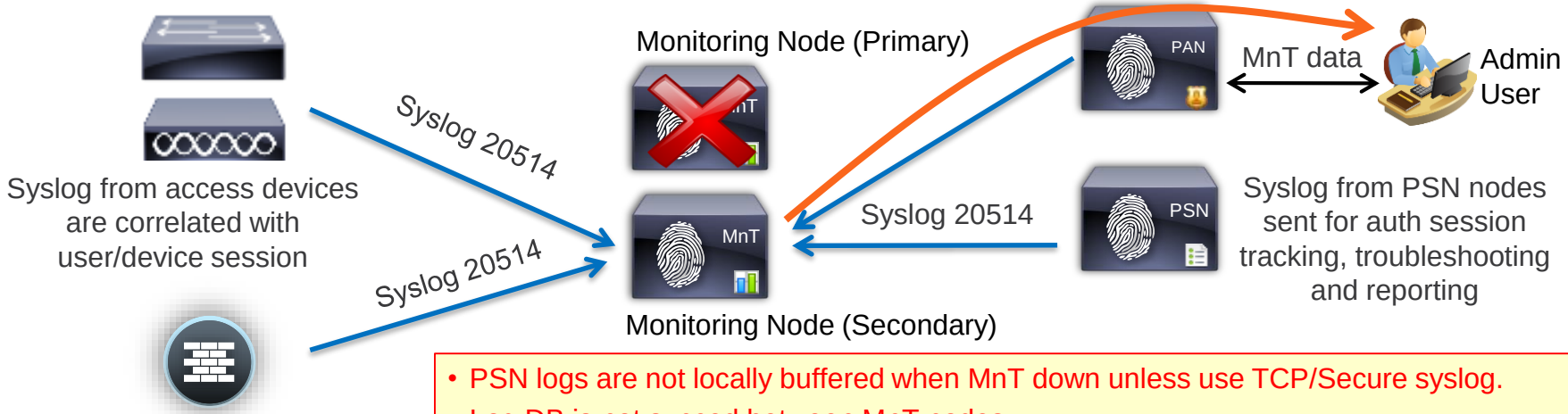
- MnT nodes concurrently receive logging from PAN, PSN, NAD, and ASA
- PAN retrieves log/report data from Primary MnT node when available



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.



- 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 not include data logged during outage
- Backup/Restore required to re-sync MnT database

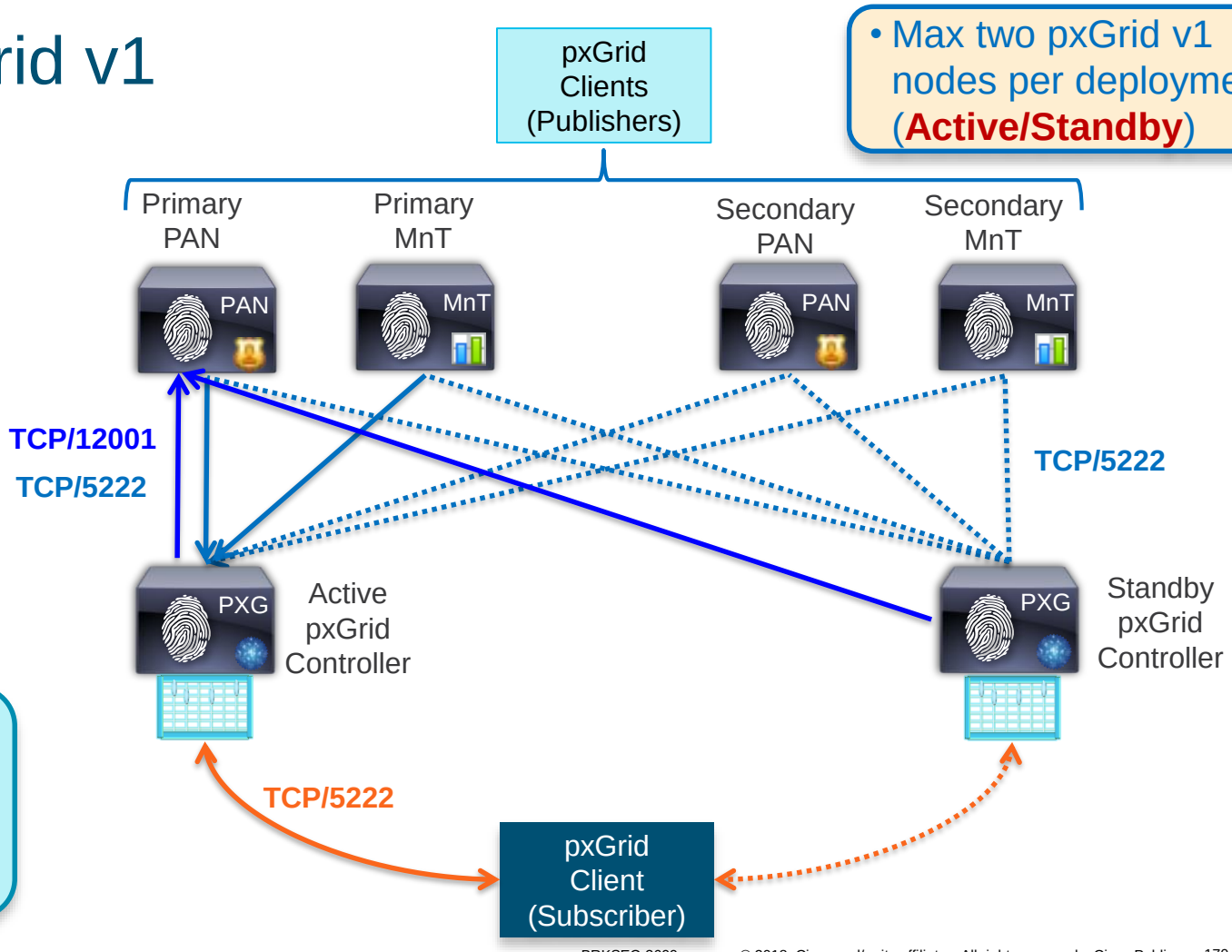
HA for pxGrid v1

Steady State

PAN Publisher Topics:
- Controller Admin
- TrustSec/SGA
- Endpoint Profile

MnT Publisher Topics:
- Session Directory
- Identity Group
- ANC (EPS)

- pxGrid clients can be configured with up to 2 servers.
- Clients connect to single active controller



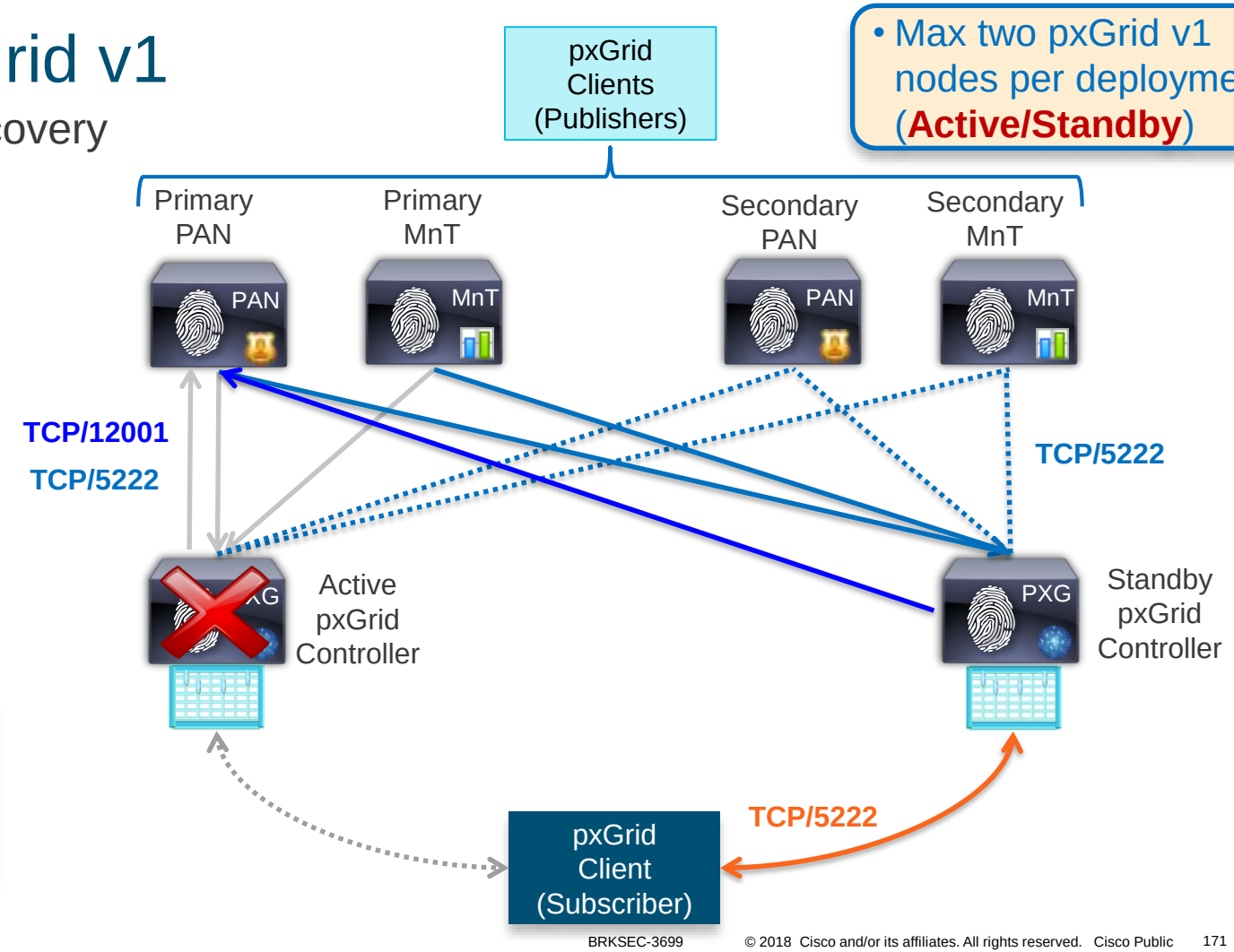
HA for pxGrid v1

Failover and Recovery

PAN Publisher Topics:
- Controller Admin
- TrustSec/SGA
- Endpoint Profile

MnT Publisher Topics:
- Session Directory
- Identity Group
- ANC (EPS)

If active pxGrid Controller fails, clients automatically attempt connection to standby controller.



HA for pxGrid v2 (ISE 2.3+

Steady State

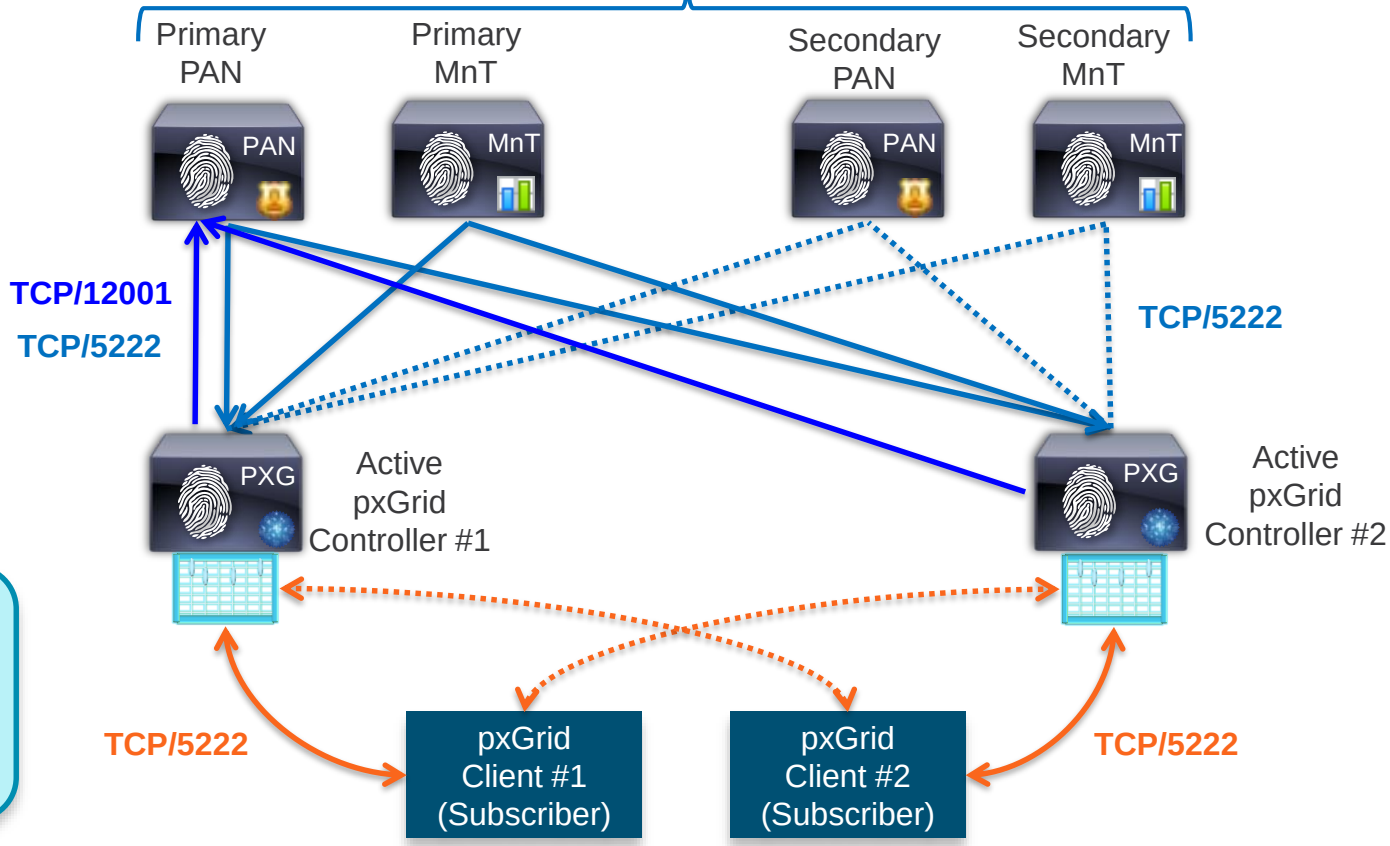
pxGrid Clients (Publishers)

- 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)

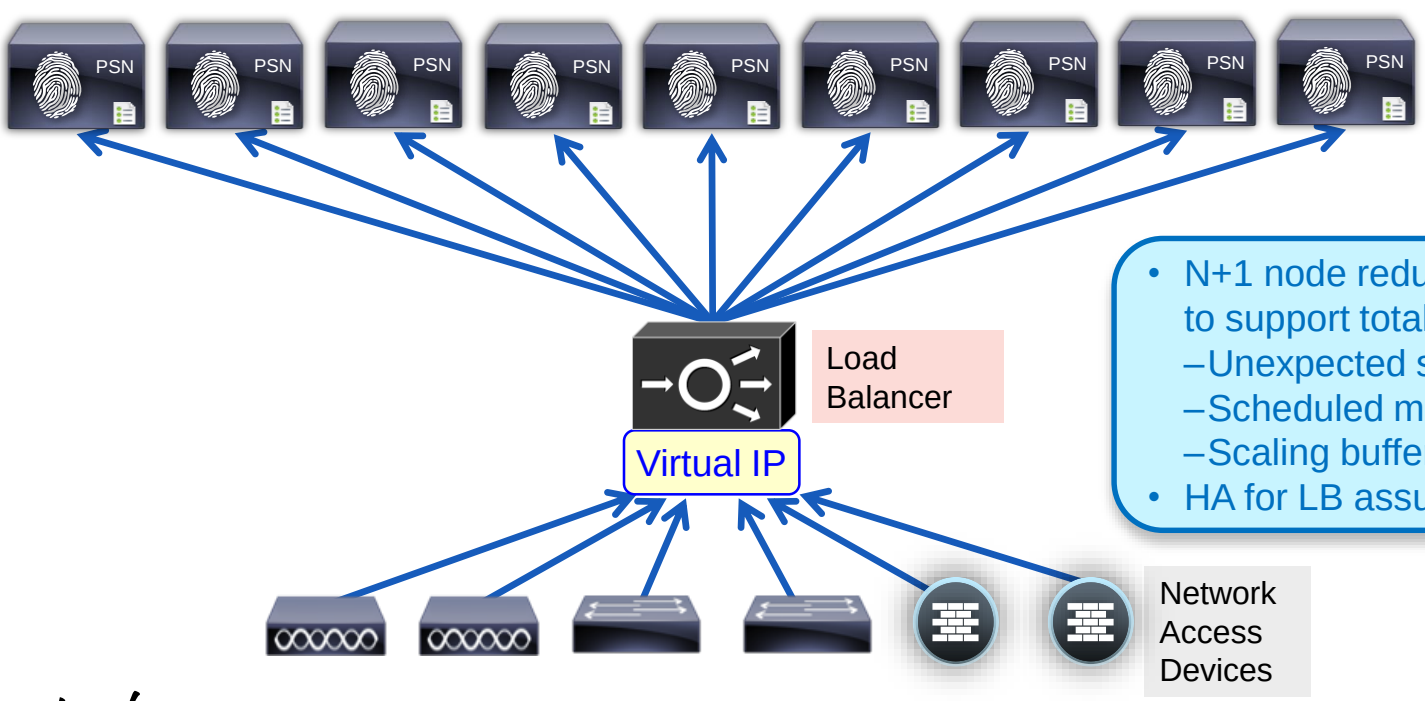
- pxGrid clients can be configured with up to 2 controllers.
- Clients connect to any 2 controllers



PSN Load Balancing

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 AAA requests to LB virtual IP.



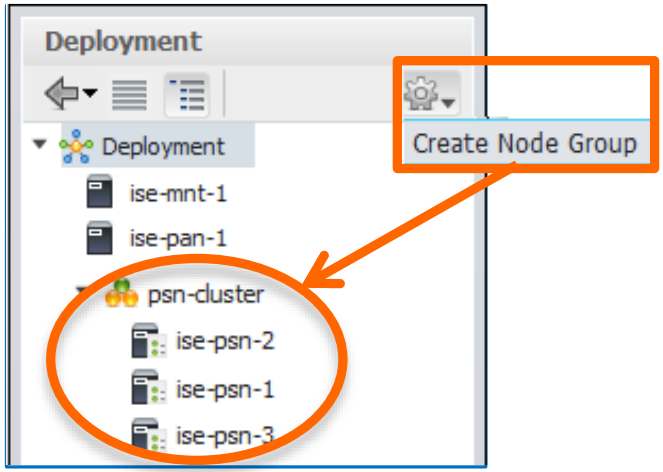
- N+1 node redundancy assumed to support total endpoints during:
  - Unexpected server outage
  - Scheduled maintenance
  - Scaling buffer
- HA for LB assumed

Configure Node Groups for LB Cluster

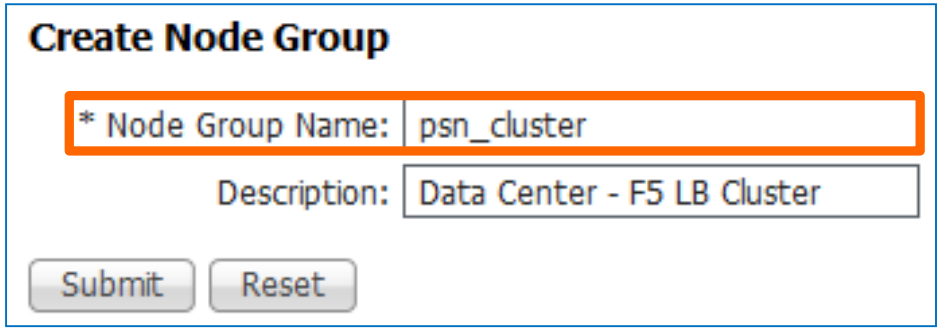
All PSNs in LB Cluster in Same Node Group

- Administration > System > Deployment

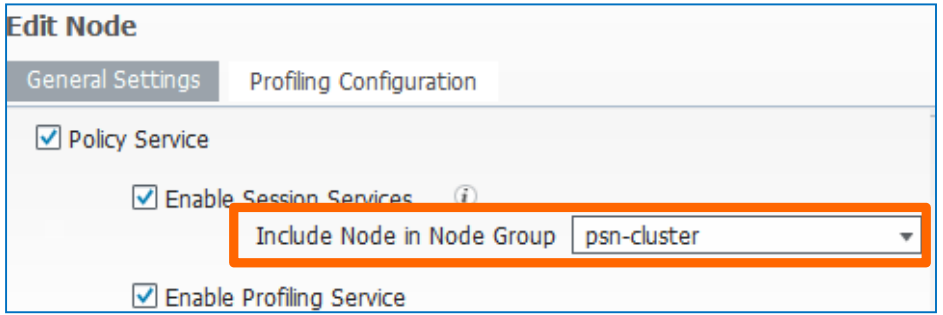
1) Create node group



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



3) Add individual PSNs to node group



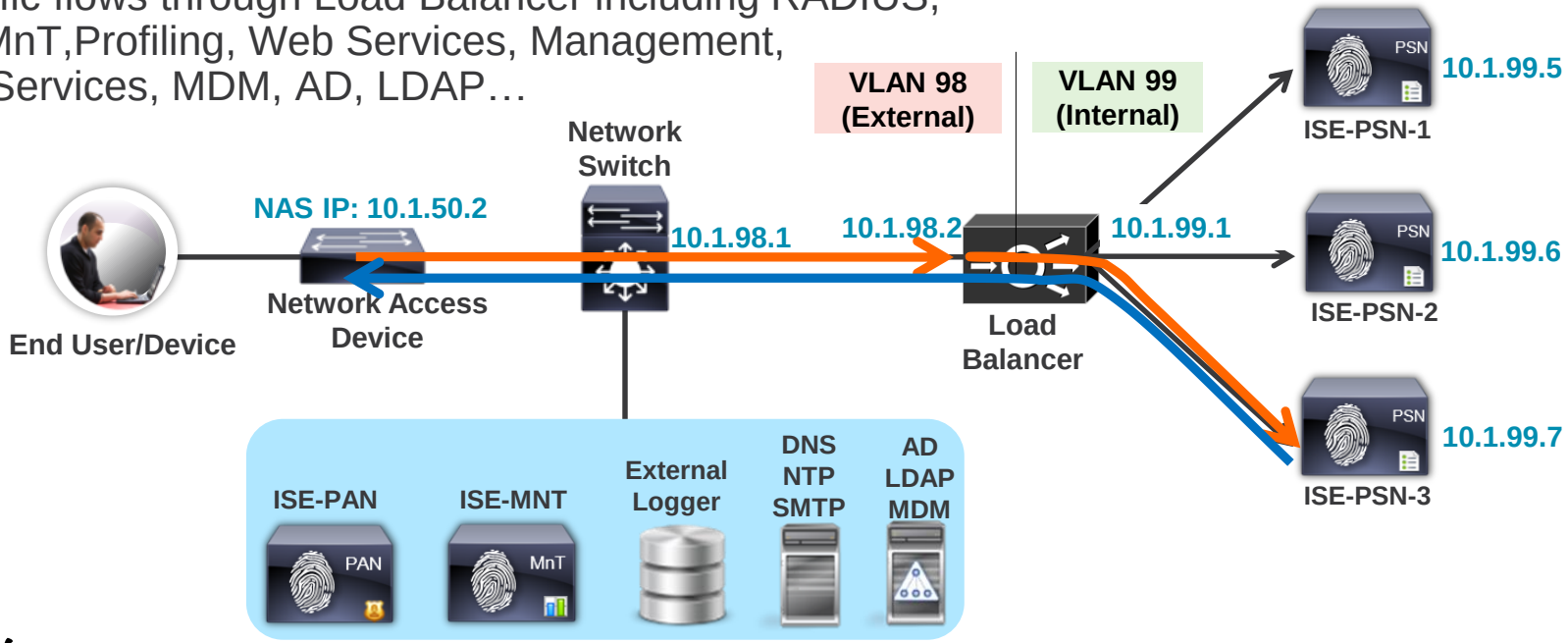
- Node group members can be L2 or L3
- Multicast no longer a requirements since ISE 1.3

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…



Load Balancing Policy Services

- **RADIUS AAA Services**

  Packets sent to LB virtual IP are load-balanced to real PSN based on configured algorithm. Sticky algorithm determines method to ensure same Policy Service node services same endpoint.

- **Web Services:**
  - **URL-Redirected:** Posture (CPP) / Central WebAuth (CWA) / Native Supplicant Provisioning (NSP) / Hotspot / Device Registration WebAuth (DRW), Partner MDM.

    No LB Required! PSN that terminates RADIUS returns URL Redirect with its own certificate CN name substituted for 'ip' variable in URL.

    Direct HTTP/S: Local WebAuth (LWA) / Sponsor / MyDevices Portal, OCSP

    Single web portal domain name should resolve to LB virtual IP for http/s load balancing.

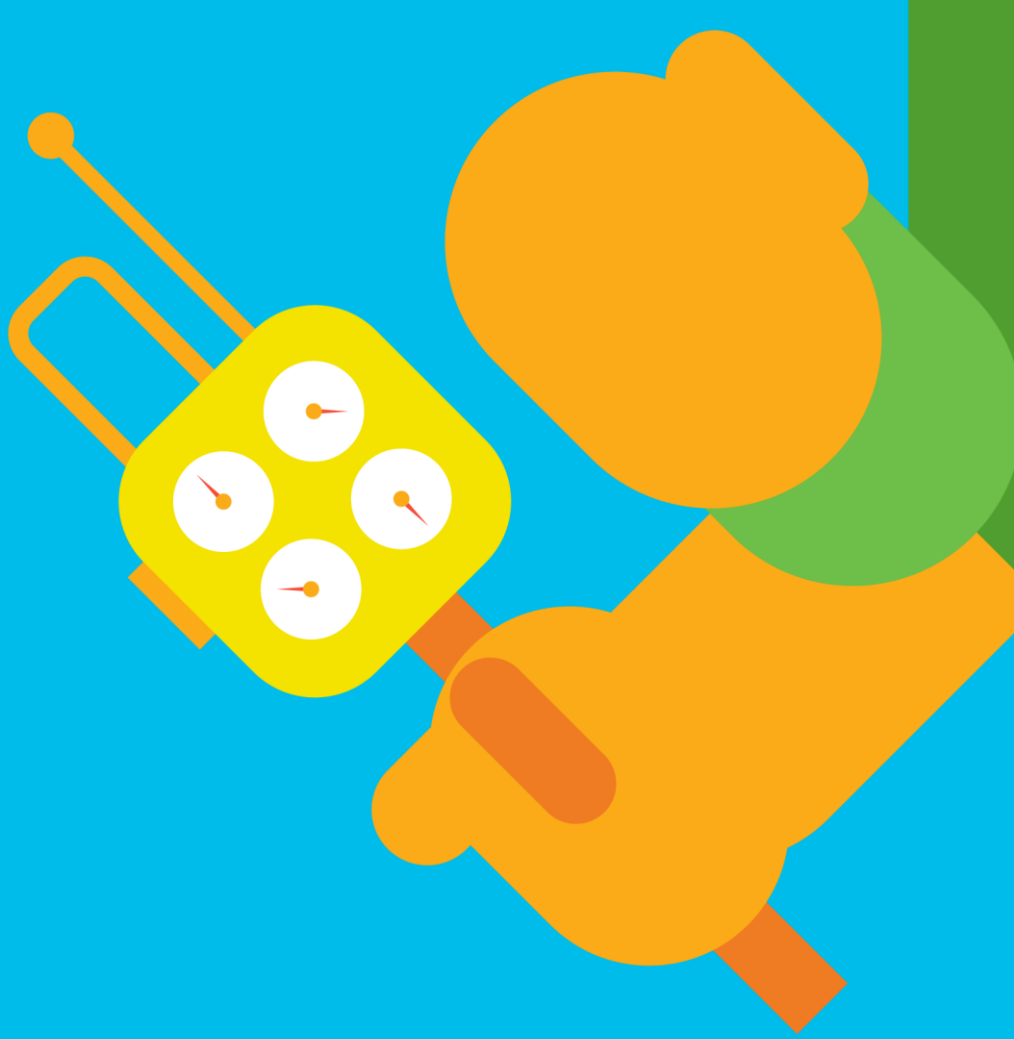
- **Profiling Services:** DHCP Helper / SNMP Traps / Netflow / RADIUS

  LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

- **TACACS+ AAA Services:** (Session and Command Auth and Accounting)

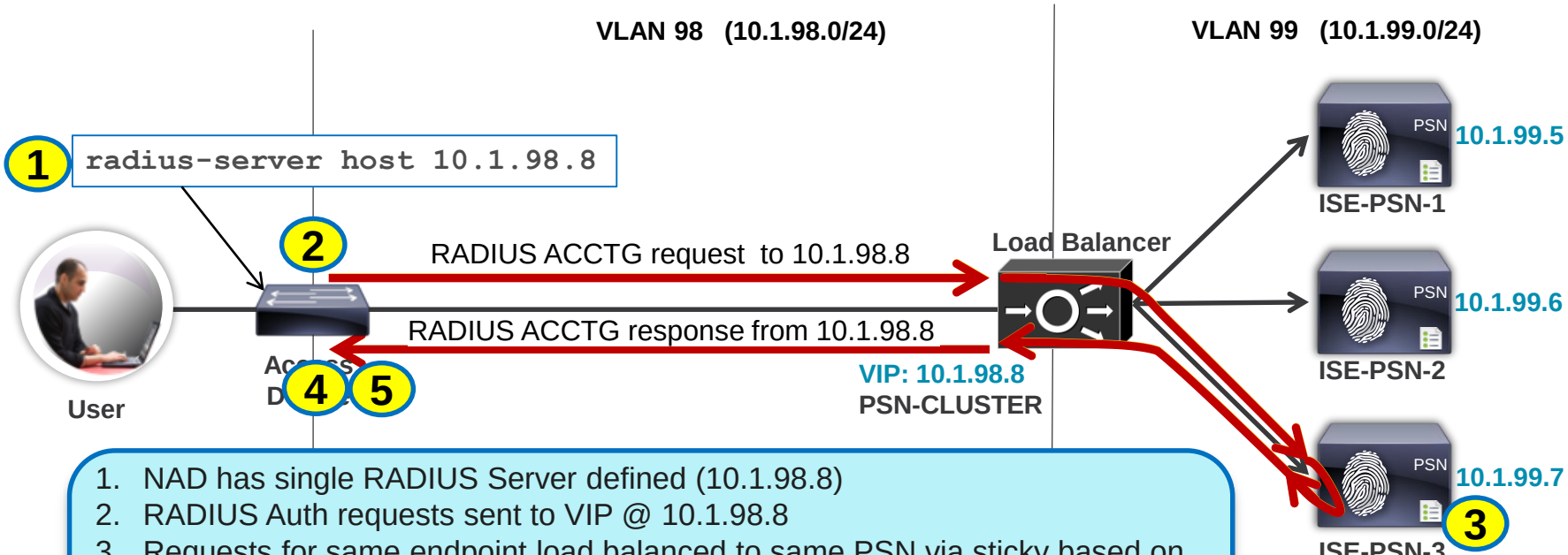
  LB VIP is target for TACACS+ requests. T+ not session based like RADIUS, so not required that requests go to same PSN

Load Balancing RADIUS



Load Balancing RADIUS

Sample Flow

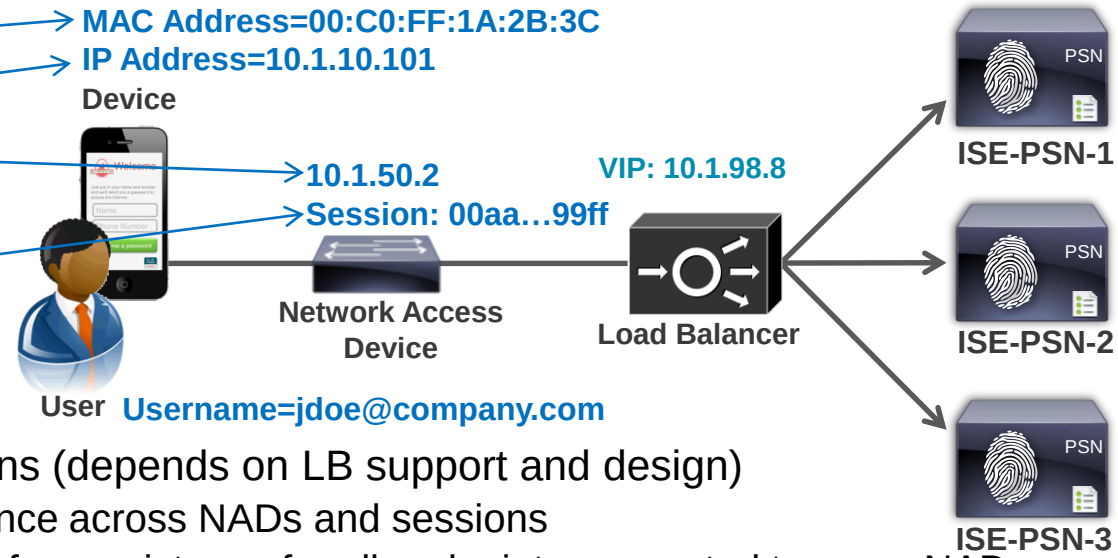


1. NAD has single RADIUS Server defined (10.1.98.8)
2. RADIUS Auth requests sent to VIP @ 10.1.98.8
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS response received from VIP @ 10.1.98.8 (originated by real server ise-psn-3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

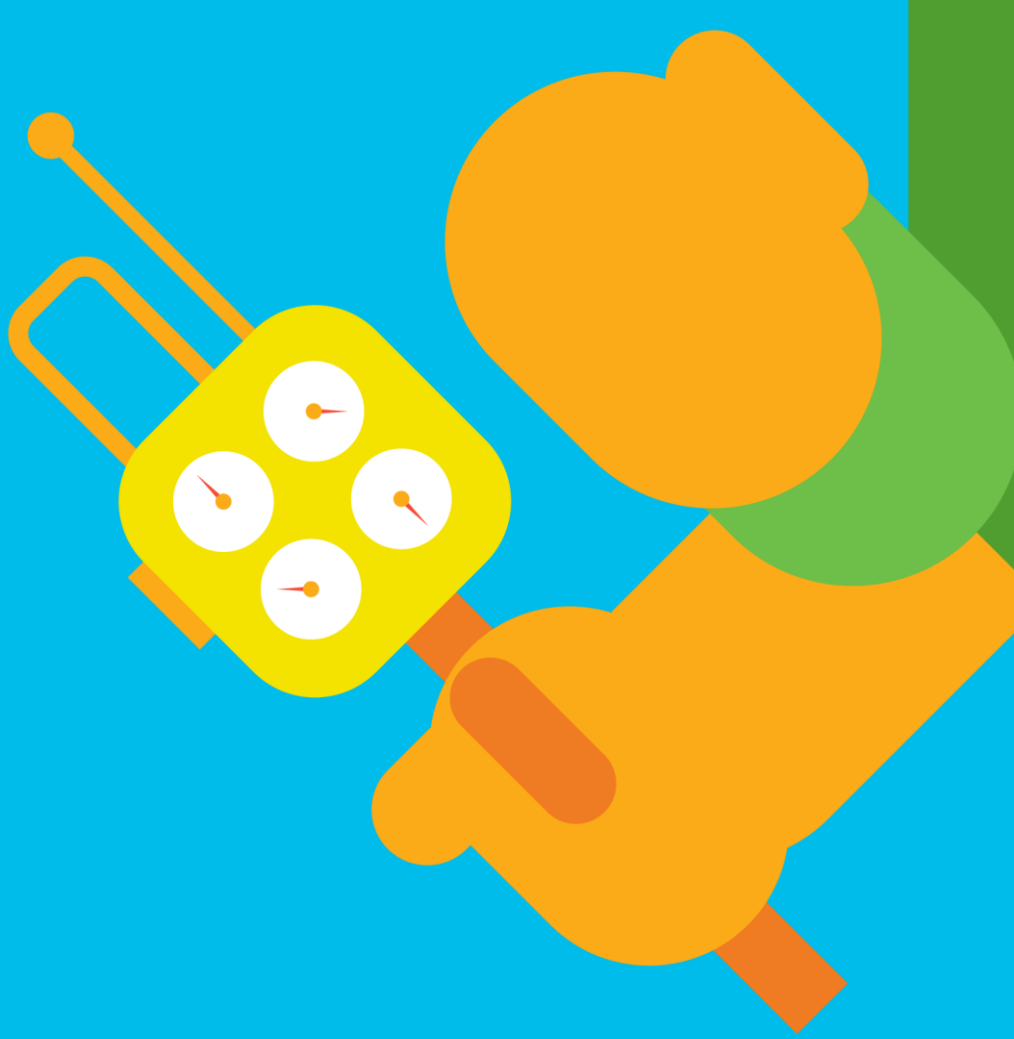
Persistence Attributes

- 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



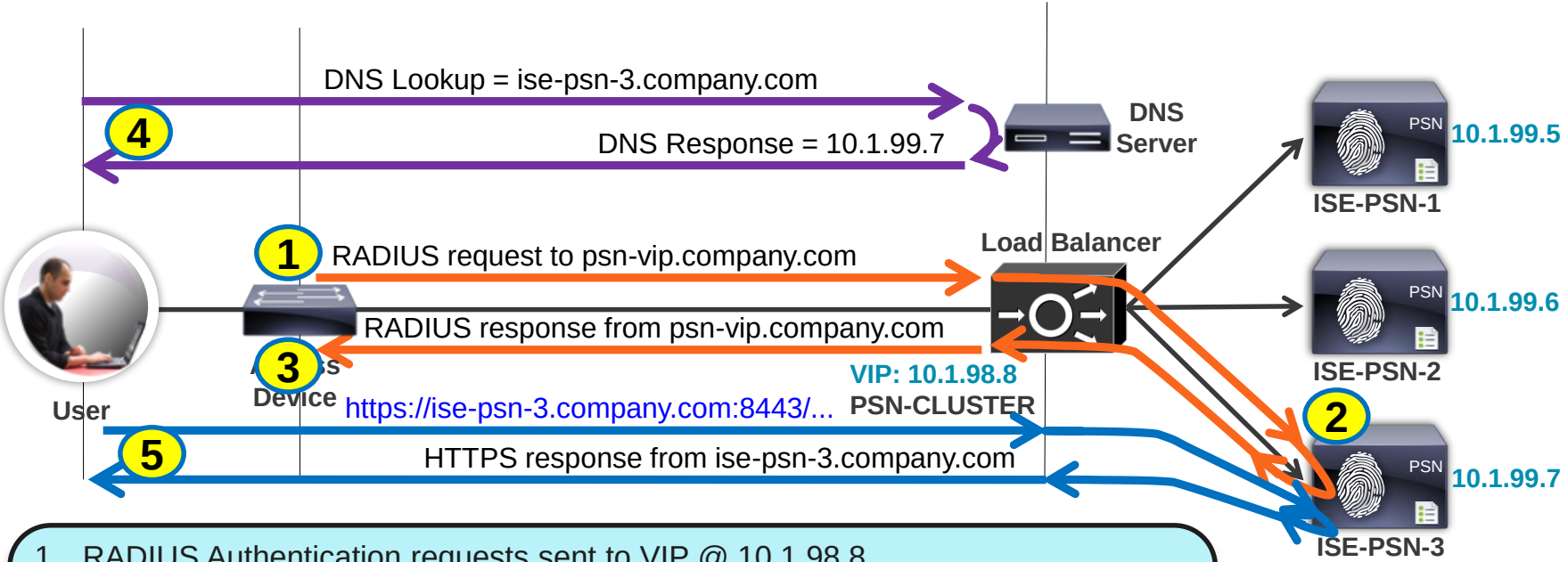
- Best Practice Recommendations (depends on LB support and design)
  1. Calling-Station-ID for persistence across NADs and sessions
  2. Source IP or NAS-IP-Address for persistence for all endpoints connected to same NAD
  3. Audit Session ID for persistence across re-authentications

Load Balancing ISE Web Services



Load Balancing with URL-Redirection

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



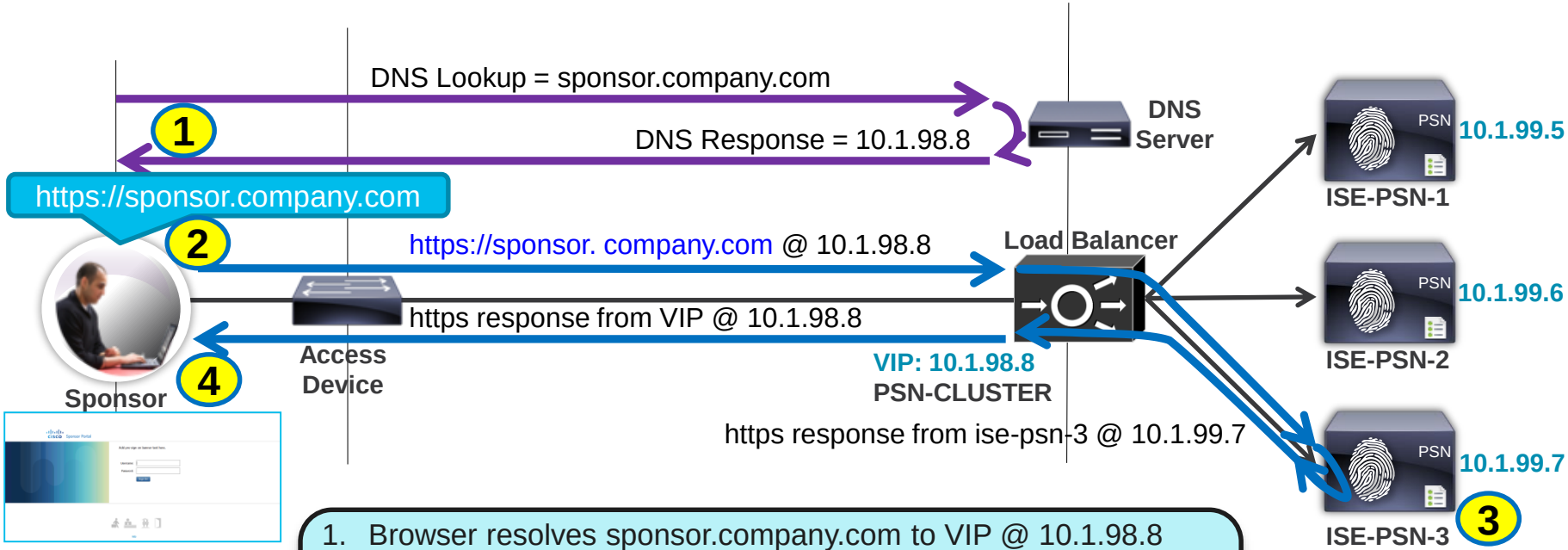
1. RADIUS Authentication requests sent to VIP @ 10.1.98.8
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorisation received from VIP @ 10.1.98.8 (originated by ise-psn-3 @ 10.1.99.7 with URL Redirect to https://ise-psn-3.company.com:8443/...
4. Client browser 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

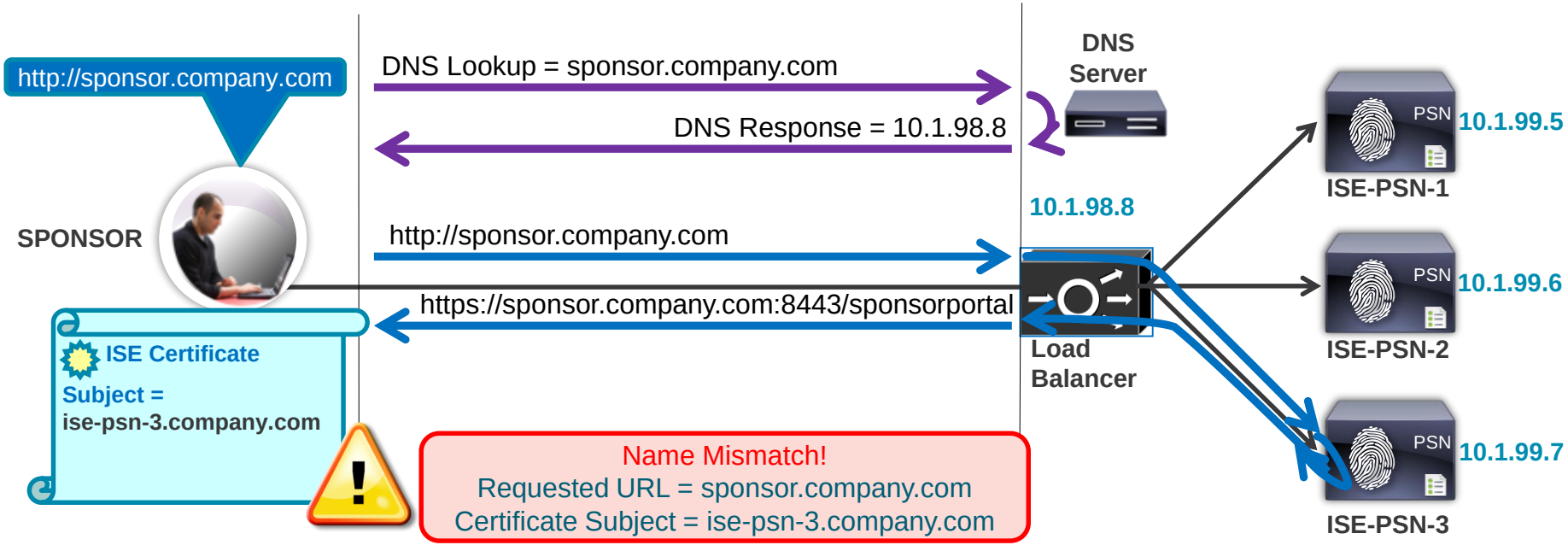
Direct Web Services: Sponsor, My Devices, LWA, OCSP



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.

ISE Certificate without SAN

Certificate Warning - Name Mismatch



ISE Certificate with SAN

No Certificate Warning

SPONSOR

DNS Lookup = sponsor.company.com

DNS Response = 10.1.98.8

DNS Server

http://sponsor.company.com

https://sponsor.company.com:8443/sponsorportal

10.1.98.8

Load Balancer

PSN 10.1.99.5 ISE-PSN-1

PSN 10.1.99.6 ISE-PSN-2

PSN 10.1.99.7 ISE-PSN-3

ISE Certificate

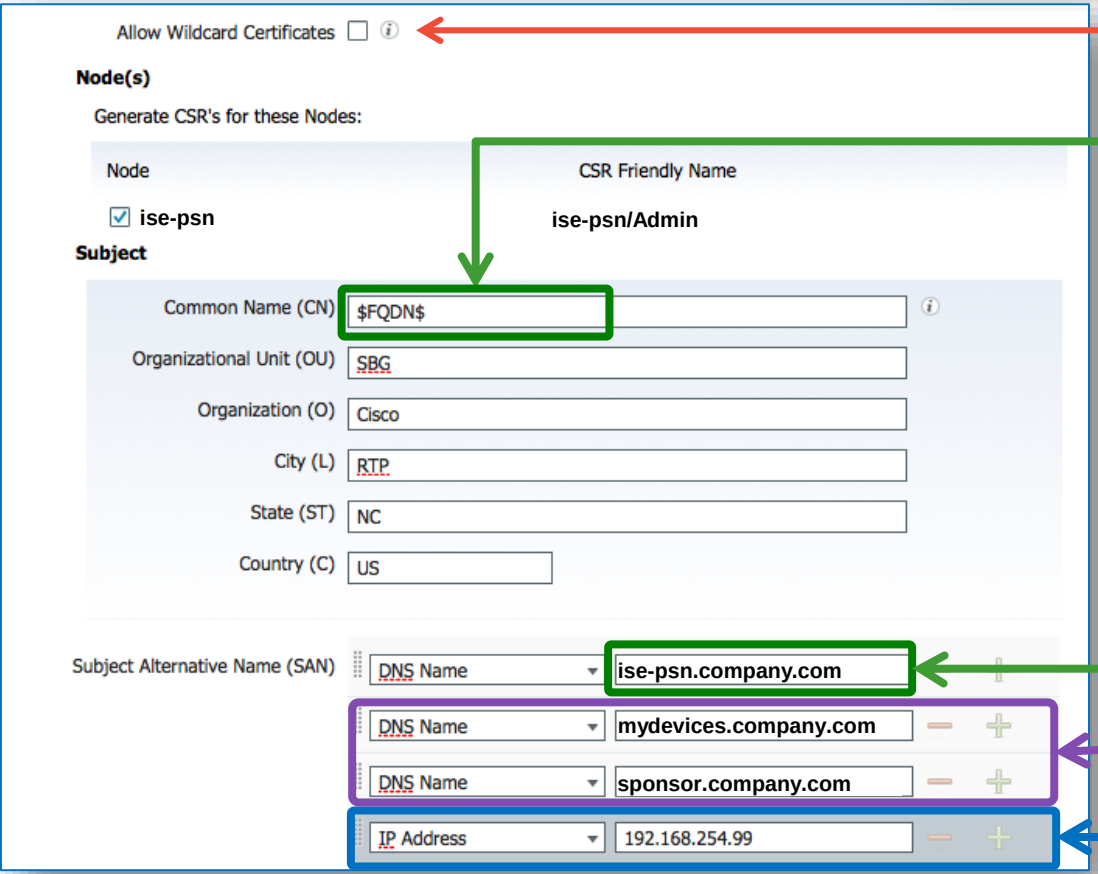
Subject =
ise-psn.company.com

SAN=
ise-psn-1.company.com
ise-psn-2.company.com
ise-psn-3.company.com
sponsor.company.com

Certificate OK!
Requested URL = sponsor.company.com
Certificate SAN = sponsor.company.com

“Universal Certs”

UCC or Wildcard SAN Certificates



Check box to use wildcards

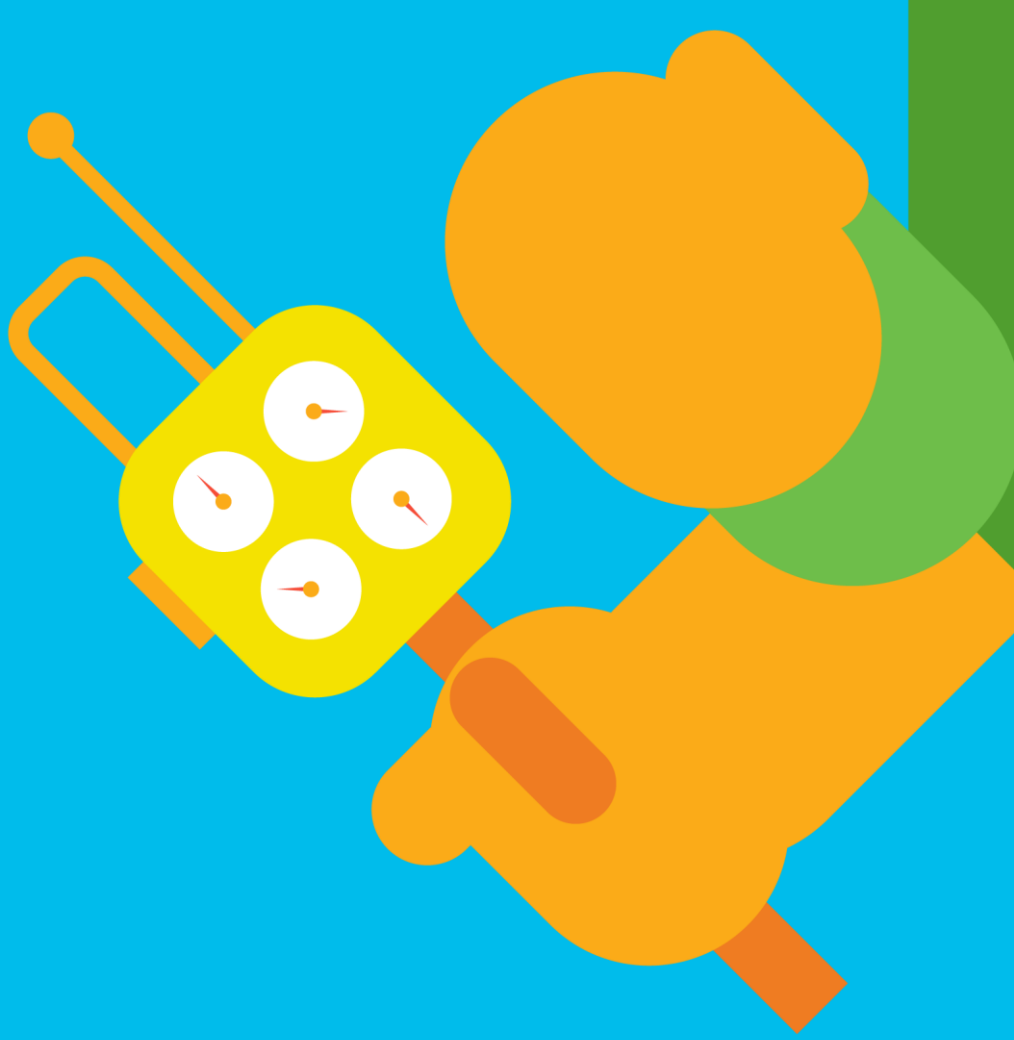
CN must also exist in SAN

Universal Cert options:
- UCC / Multi-SAN
- Wildcard SAN

Other FQDNs or wildcard as “DNS Names”

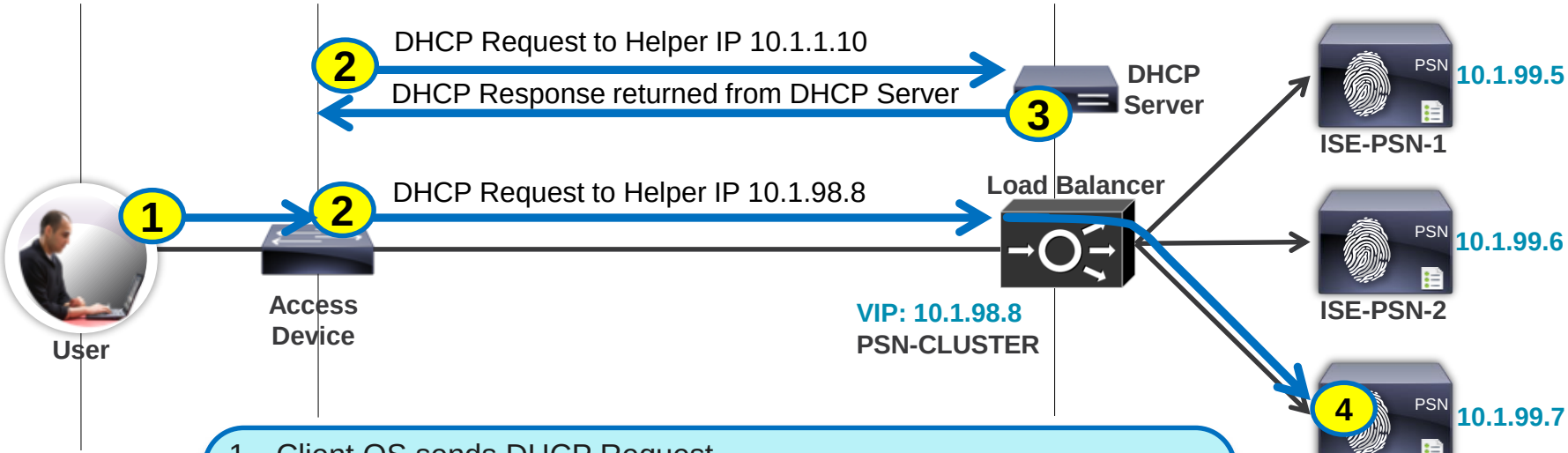
IP Address is also option

Load Balancing ISE Profiling Services



Load Balancing Profiling Services

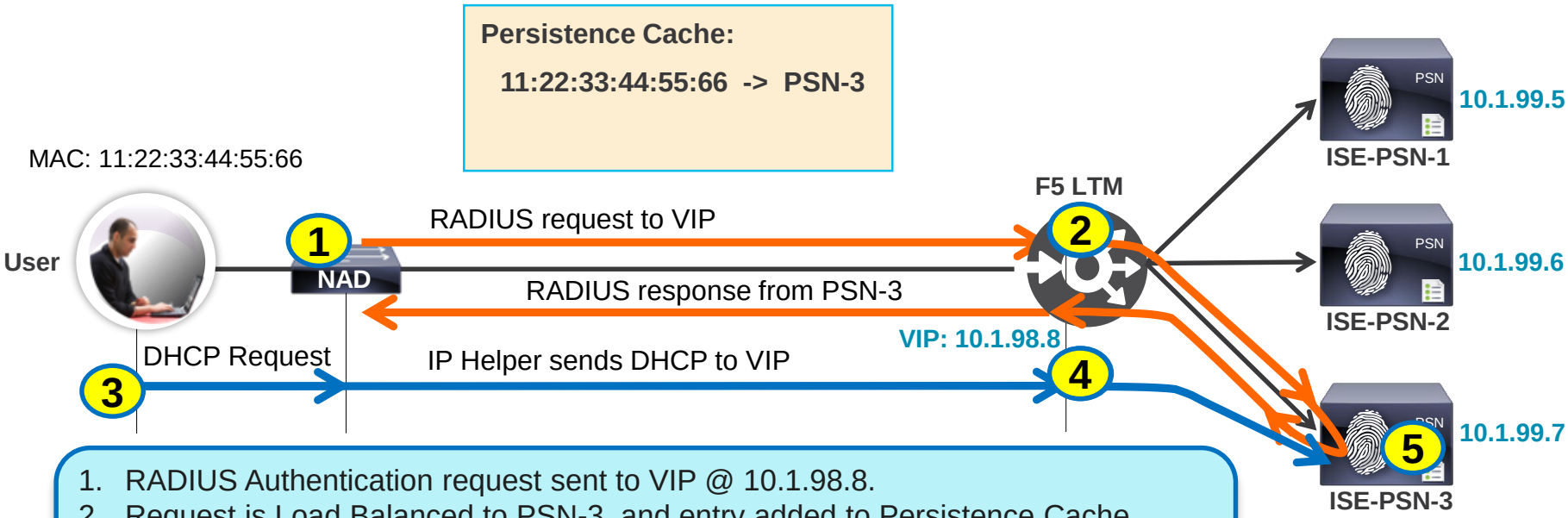
Sample Flow



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.

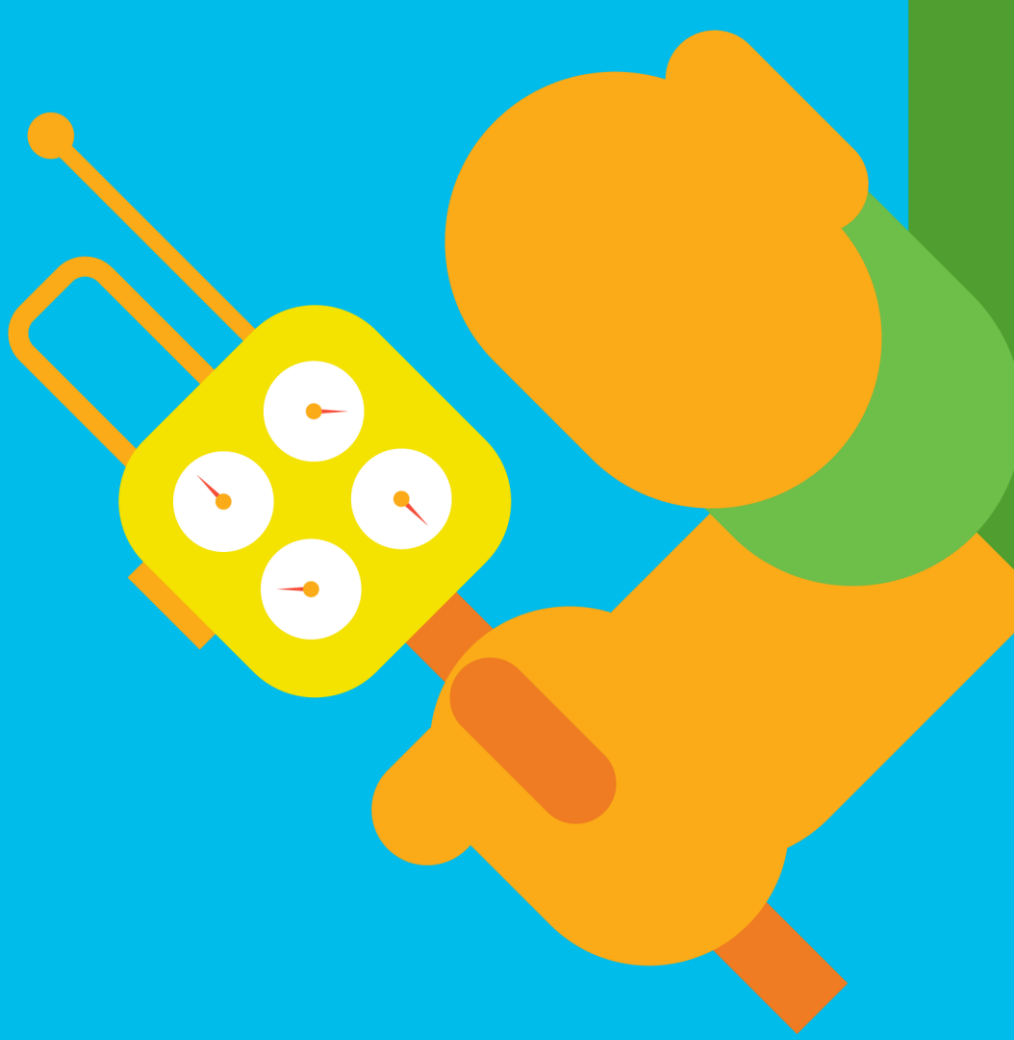
Load Balancing Sticky Guidelines

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 optimising endpoint replication

Load Balancing TACACS+



Vendor-Specific LB Configurations

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

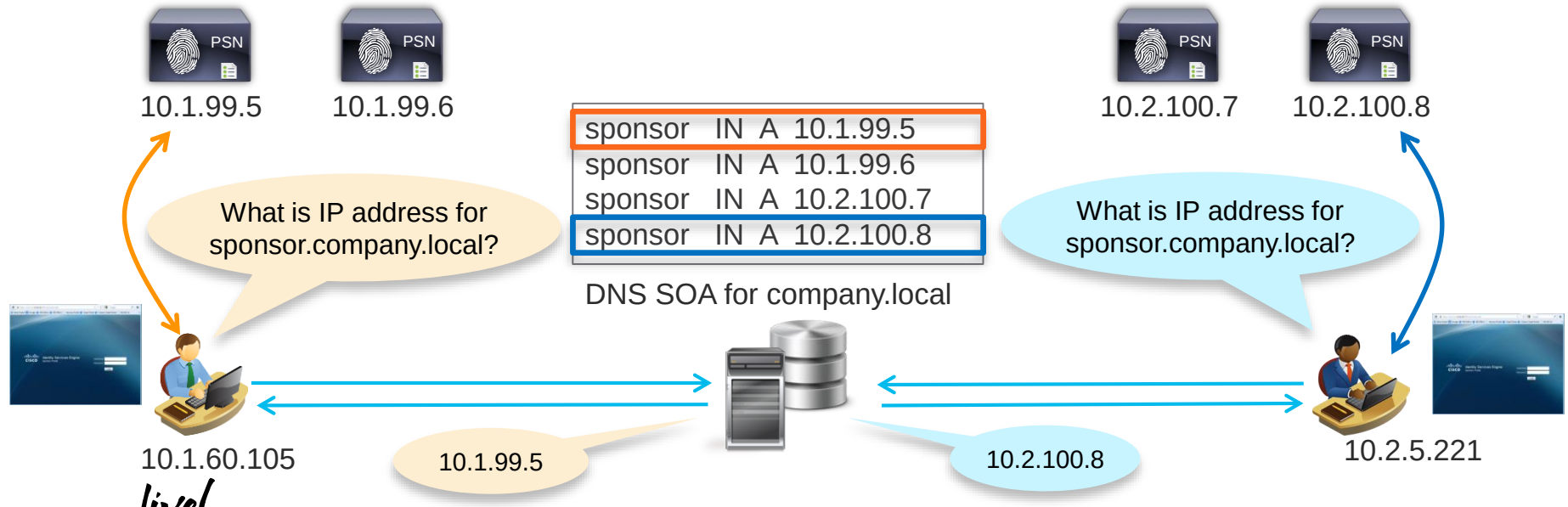
https://communities.cisco.com/docs/DOC-64434

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.

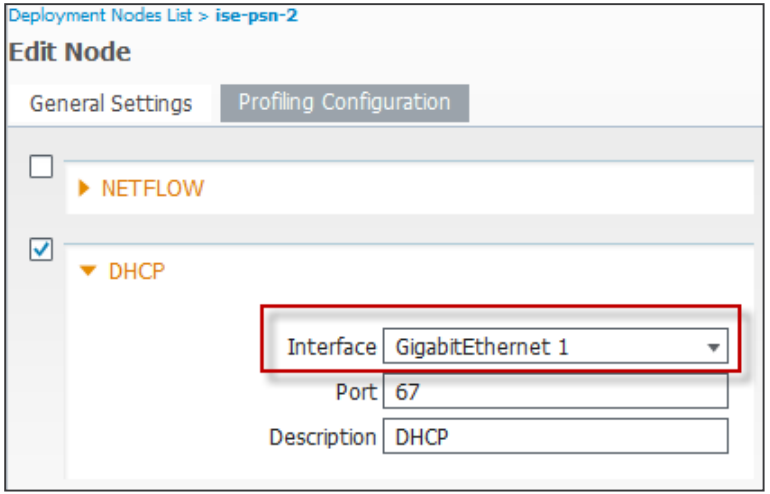


ISE Configuration for Anycast

Anycast address should only be applied to ISE secondary interfaces, or LB VIP, but never to ISE GE0 management interface.

On each PSN that will participate in Anycast…

1. Configure PSN probes to profile DHCP (IP Helper), SNMP Traps, or NetFlow on dedicated interface
2. From CLI, configure dedicated interface with same IP address on each PSN node.



ISE-PSN-1 Example:

```
#ise-psn-1/admin# config t
#ise-psn-1/admin (config)# int GigabitEthernet1
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

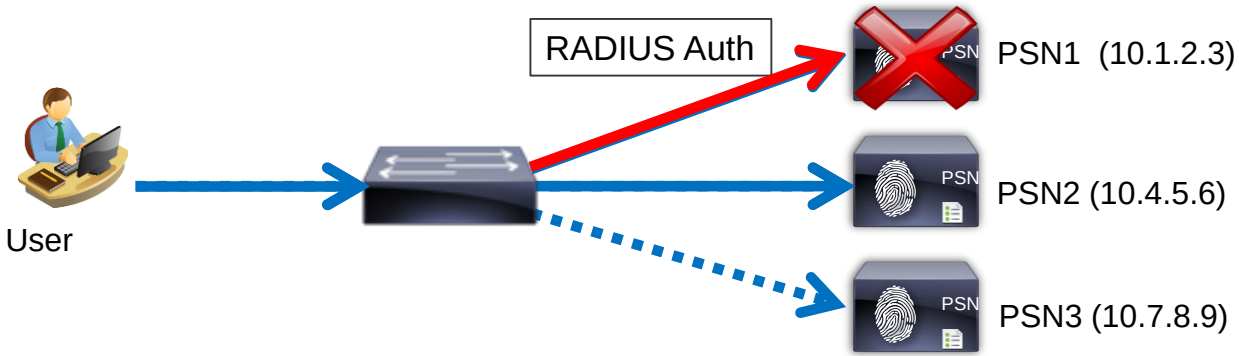
ISE-PSN-2 Example:

```
#ise-psn-1/admin# config t
#ise-psn-1/admin (config)# int GigabitEthernet1
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

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

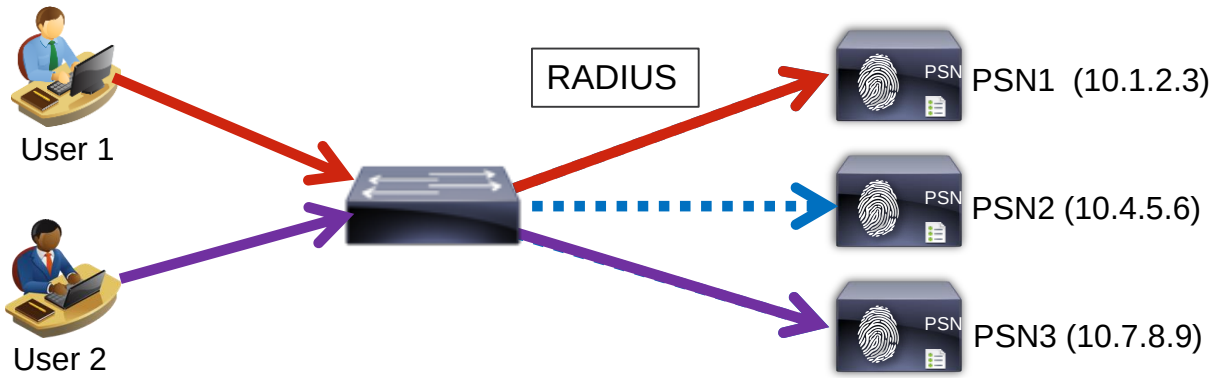



```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

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

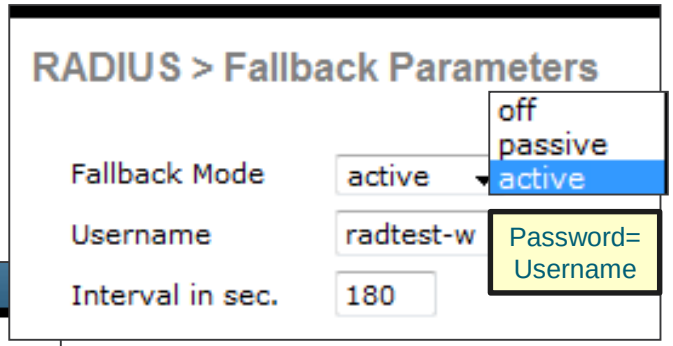
Example shows 3 PSNs in RADIUS group

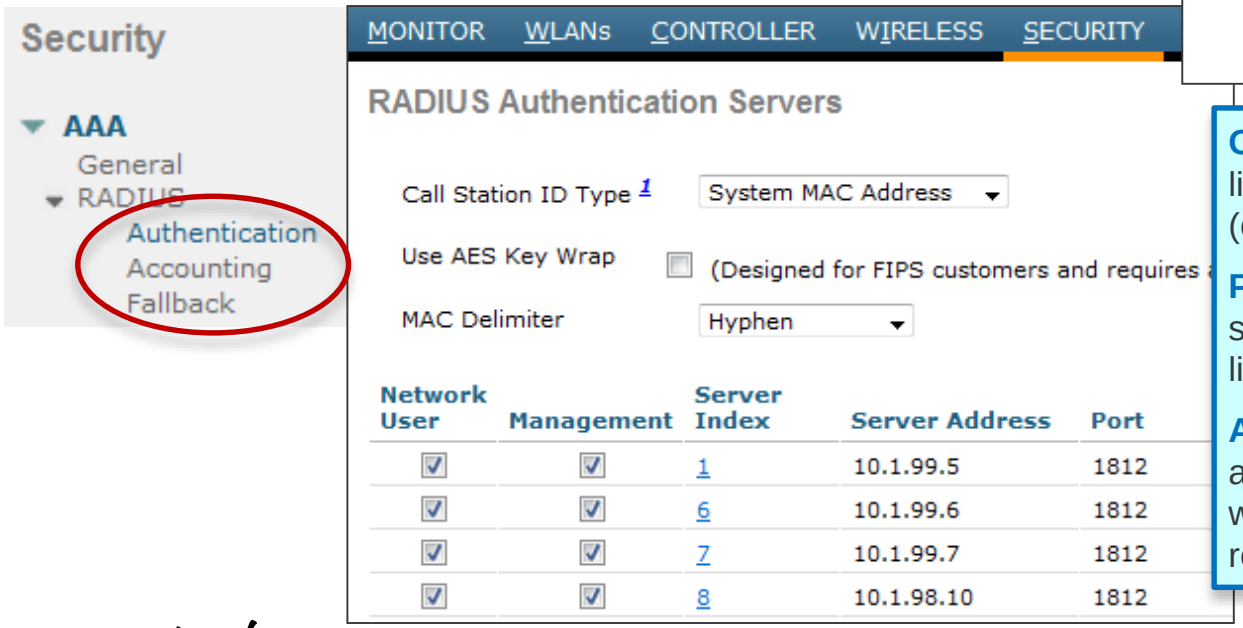
```
cat3750x# test aaa group radius radtest cisco123 new users 4 count 50
AAA/SG/TEST: Sending 50 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
```

NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

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





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.

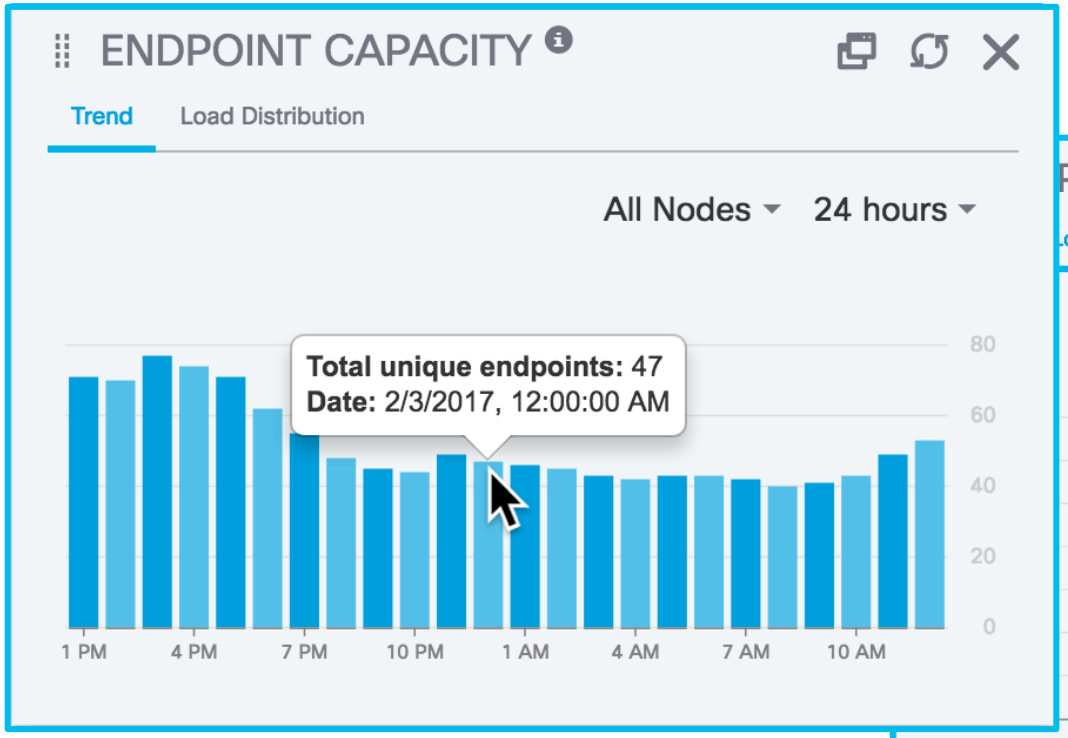
http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008098987e.shtml

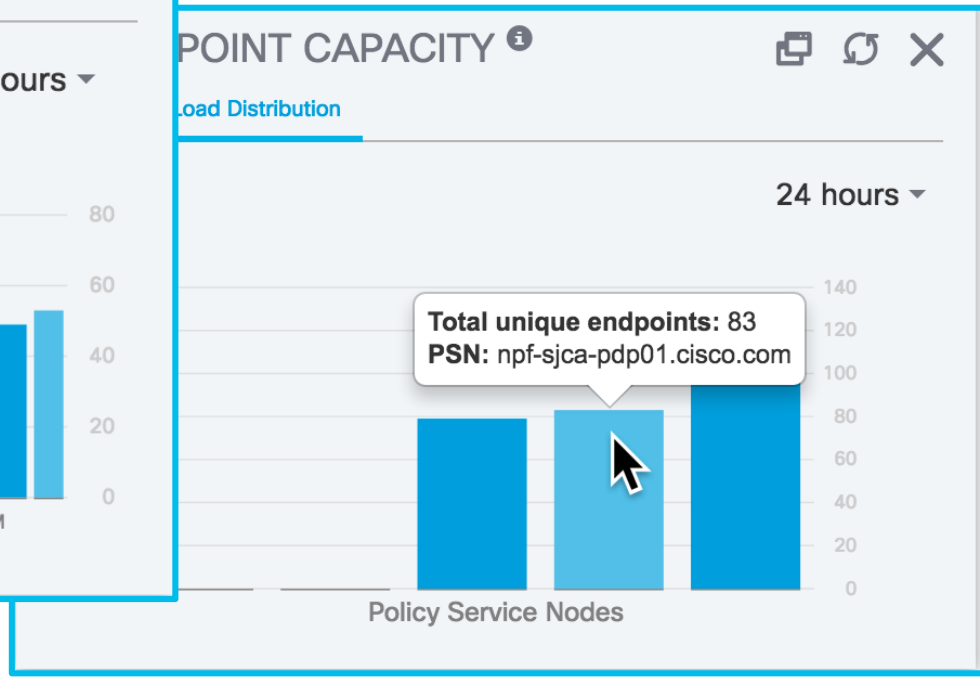
NAD Fallback and Recovery

Monitoring Load and System Health

Endpoint Capacity Report

ISE 2.2+





Key Performance Metrics (KPM)

ISE 2.2+

- KPM Reports added in ISE 2.2: Operations > Reports > Diagnostics > KPM
- Also available from CLI (# application configure ise) since ISE 1.4
- Provide RADIUS Load, Latency, and Suppression Stats

Key Performance Metrics

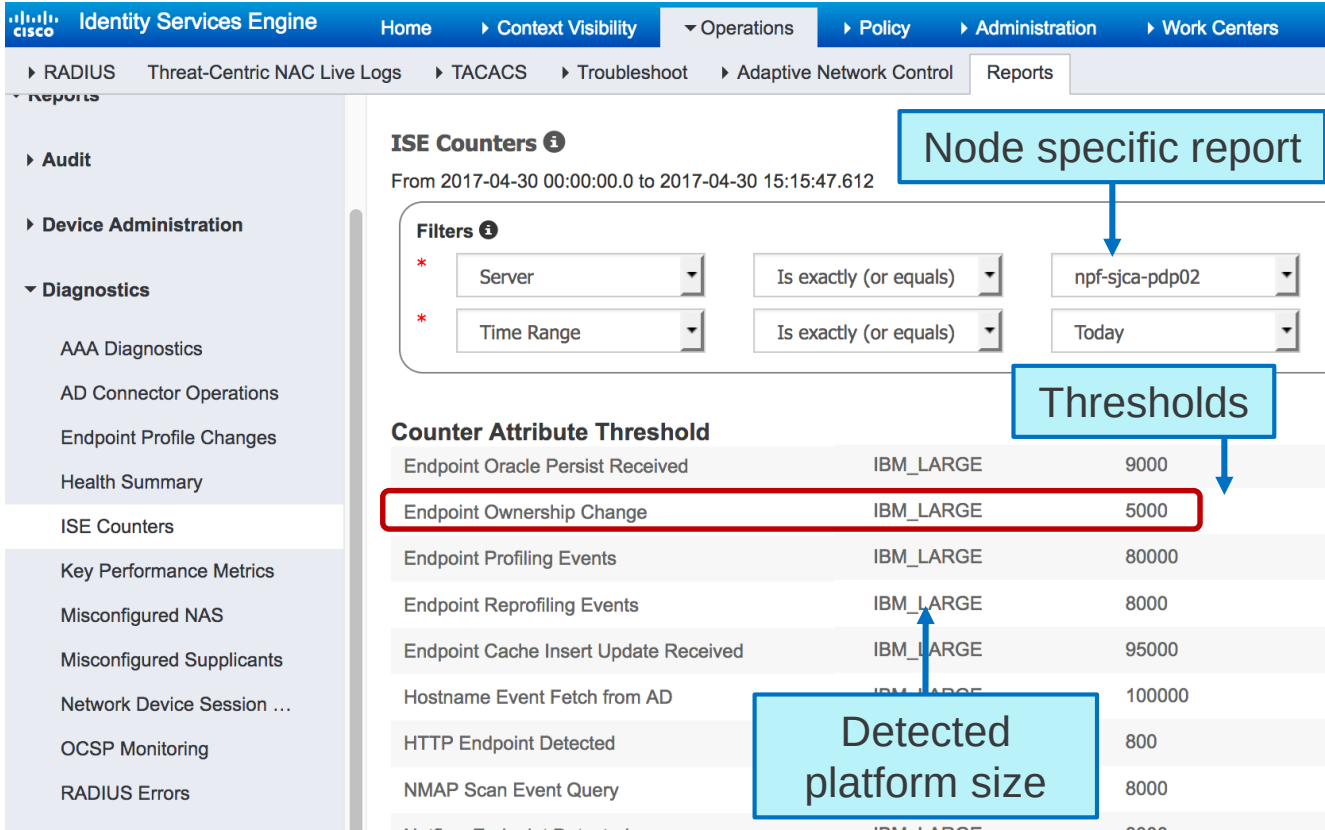
From 2017-01-06 00:00:00.0 to 2017-02-05 22:32:38.128

Logged Time	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



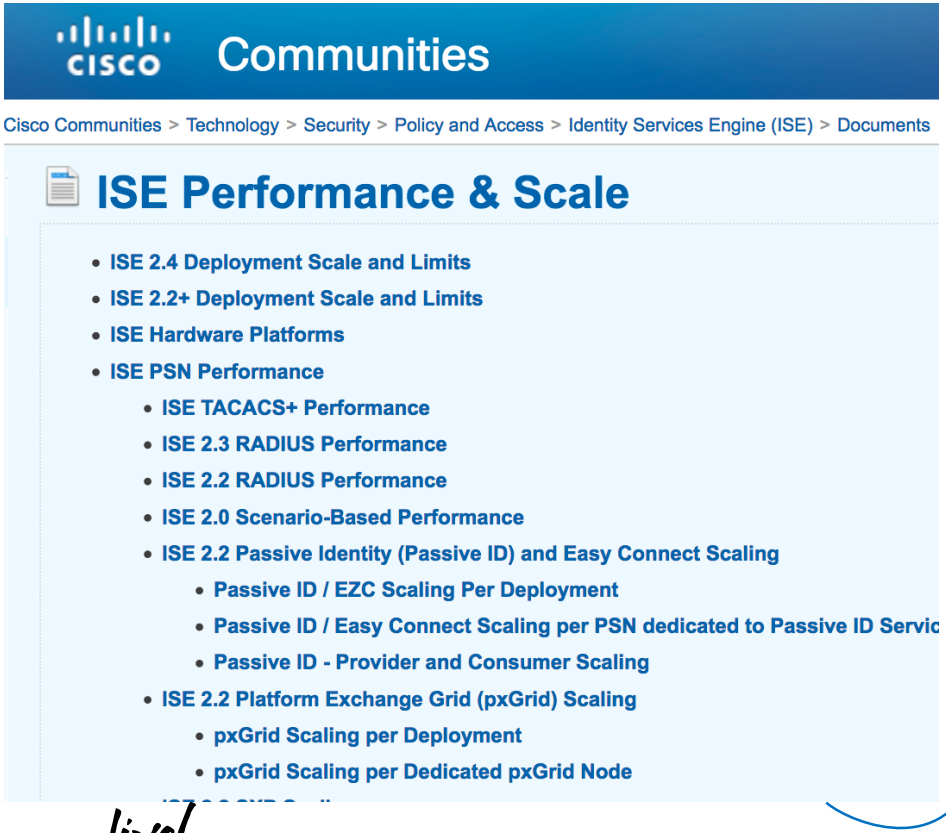
Closing Comments

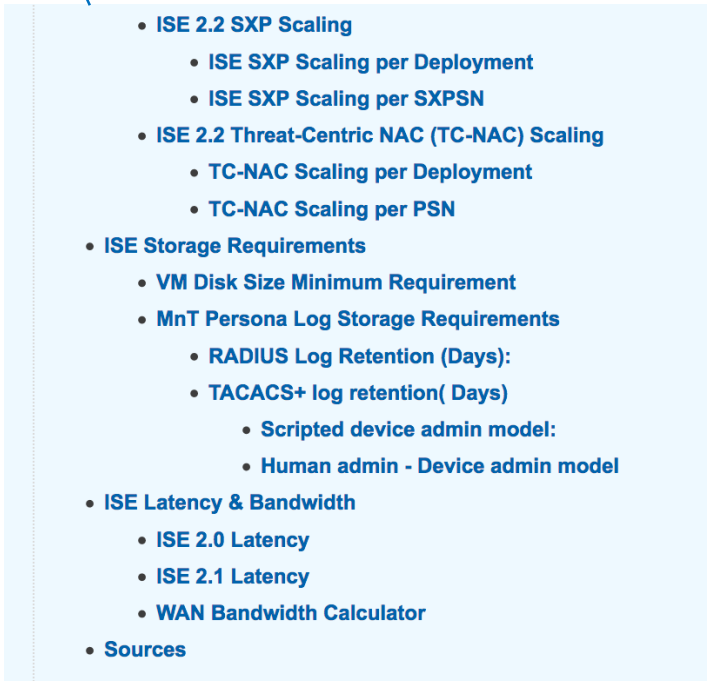
Key Takeaway Points

- CHECK ISE Virtual Appliances for proper resources and platform detection!
- Avoid excessive auth activity through proper NAD / supplicant tuning and Log Suppression
- Minimise 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

Cisco Community Page on Sizing and Scalability

https://communities.cisco.com/docs/DOC-68347

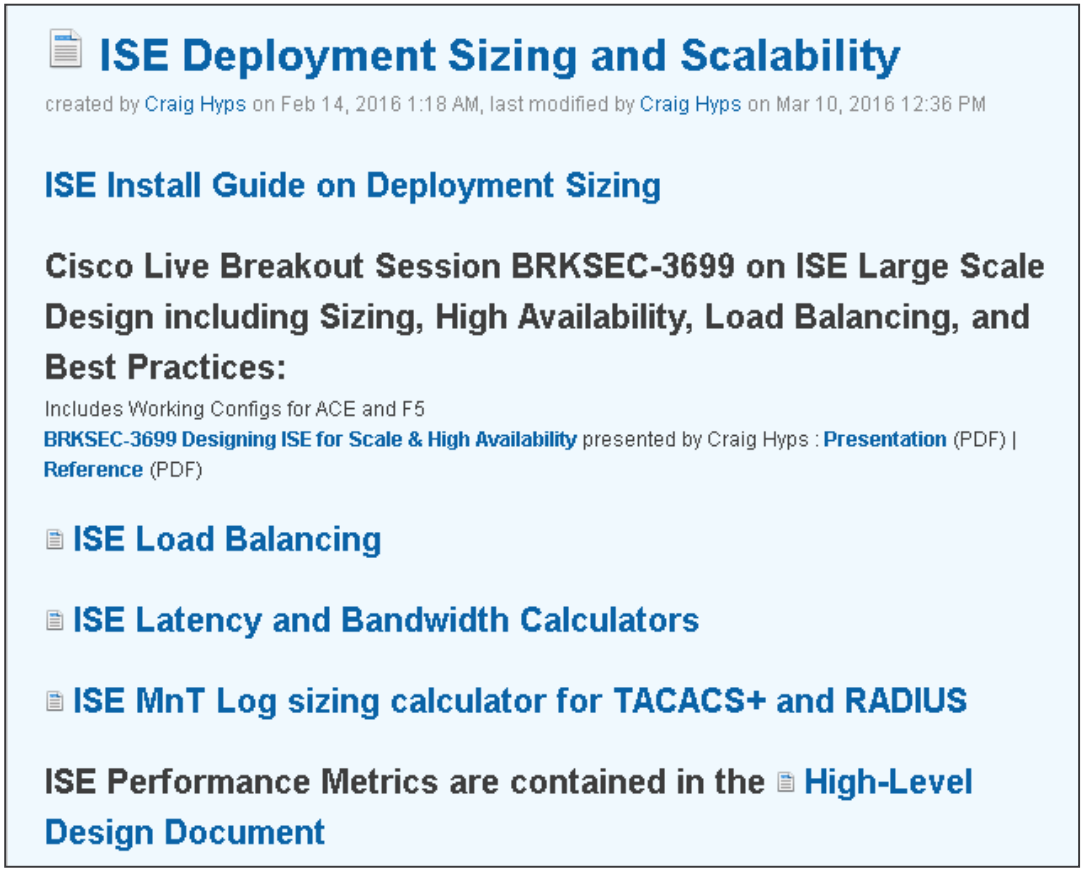




ISE Performance & Scale Resources

https://communities.cisco.com/docs/DOC-65625

- Cisco Live: BRKSEC-3699 *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

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

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

Ciscolive!

Thank you


cisco
You're
Cisco live!