TOMORROW
starts here.

Cisco live!

Advanced Designing ISE for Scale and High Availability

BRKSEC-3699

Craig Hyps (chyps@cisco.com)

Senior Technical Marketing Engineer

#clmel

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.

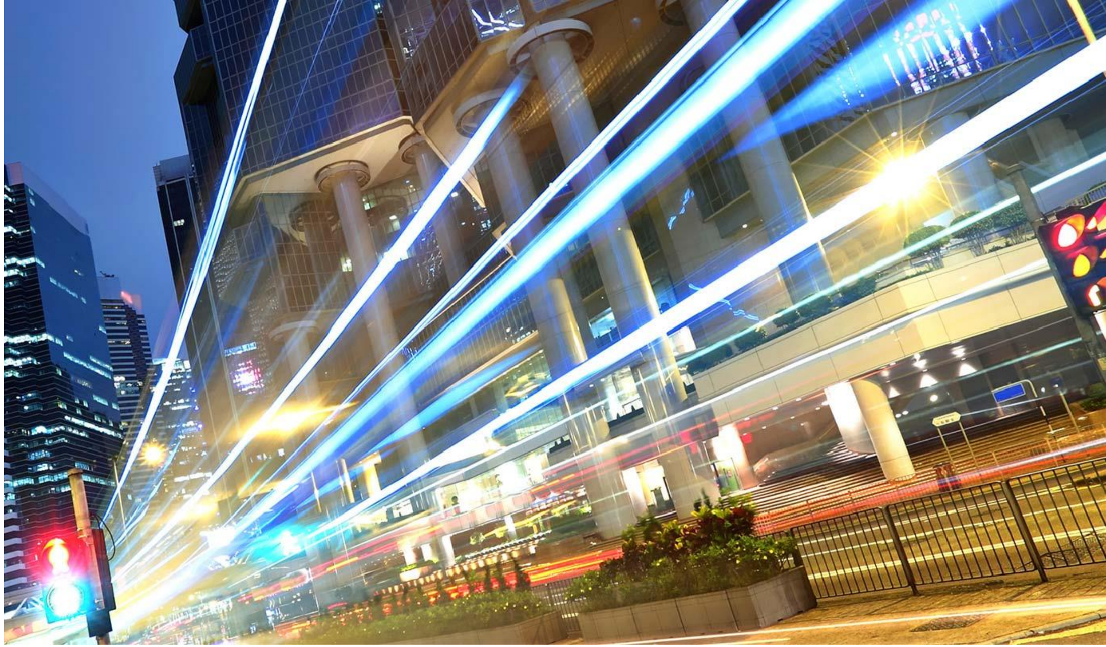
Attendees of this session will gain knowledge on how to best deploy ISE to ensure peak operational performance, stability, and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement.

Housekeeping

- **Reference slides included in published pdf**
- Visit Cisco Live Online: ciscolive.com/online
- **Questions are welcome!**
- Please use the microphone
- Please mute your phone
- Visit the World of Solutions and Meet the Engineer
- **Feedback welcome. Please complete online evaluation**

Agenda

- Sizing Deployments and Nodes
- Scaling ISE Services
  - RADIUS, Auth Policy, AD, Guest, Web Services
  - Profiling and Database Replication
  - MnT (Optimised Logging and Noise Suppression)
- High Availability
  - Admin, MnT, pxGrid, IPN node Failover
  - Certificate Services Redundancy
  - PSN Redundancy and Load Balancing
  - NAD Fallback and Recovery



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.

AUTHENTICATION

DESIGN

802.1X

U

EDIRECTION

A

IS

S

O

A

P

ILING

DE/

ICE REGISTRATION

BYOD

EAP CHAINING

Deployment Sizing

Node Types

- Policy Service Node (PSN)
  - Makes policy decisions
  - RADIUS 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 NADs

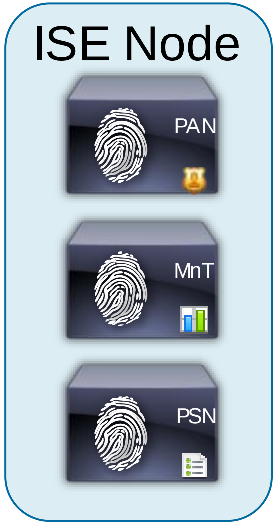
- pxGrid Controller
  - Facilitates sharing of information between network elements

- Inline Posture Node (IPN)
  - Enforces posture policy for legacy or 3rd-party NADs

Standalone Deployment

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

- Maximum endpoints – Platform dependent
  - 2,000 for 33x5
  - 5,000 for 3415
  - 10,000 for 3495



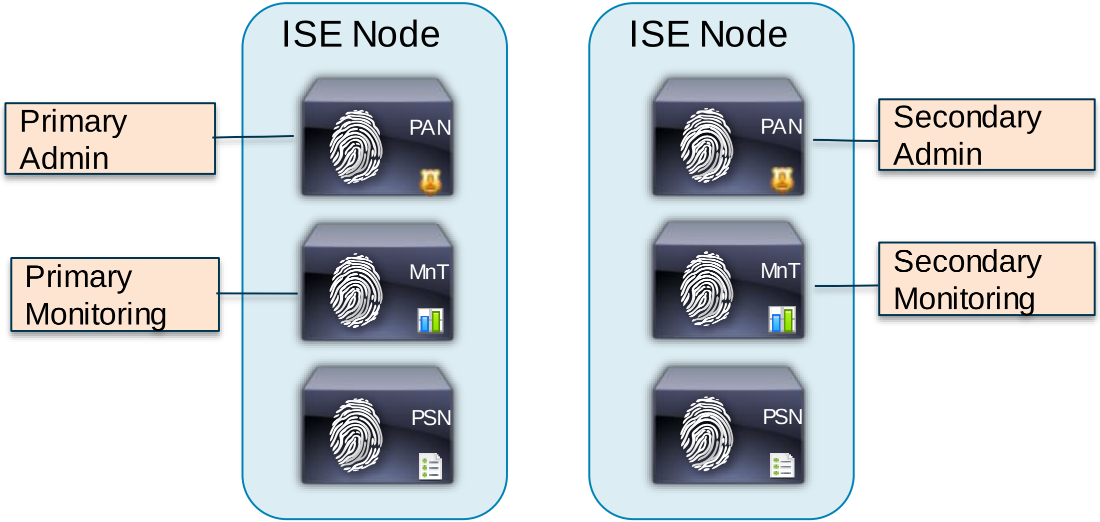
Policy Administration Node

Monitoring and Troubleshooting Node

Policy Service Node

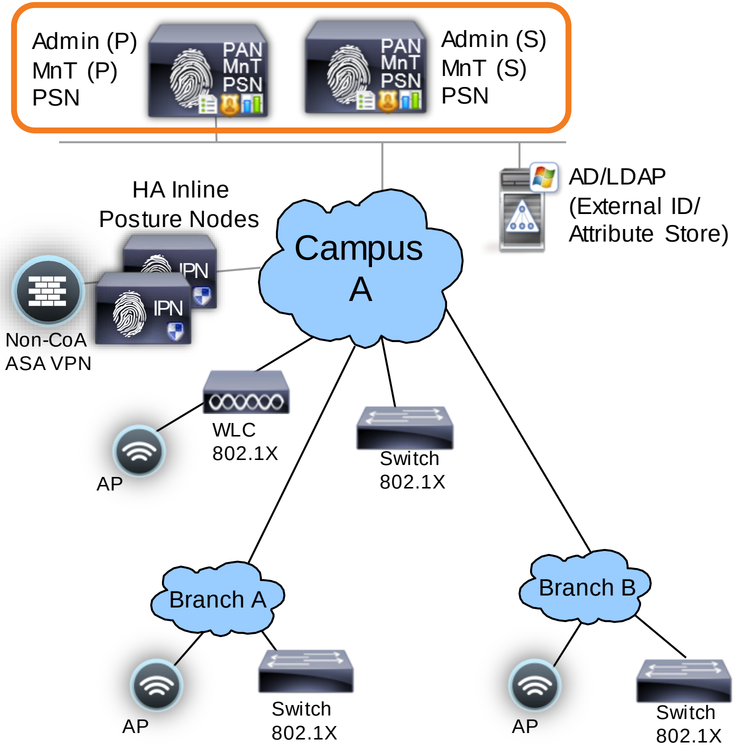
Basic 2-Node ISE Deployment (Redundant)

- Maximum endpoints – 10,000 (platform dependent—same as standalone)
- Redundant sizing – 10,000 (platform dependent—same as standalone)



Basic 2-Node ISE Deployment (Redundant)

Maximum Endpoints = 10,000 (Platform dependent)

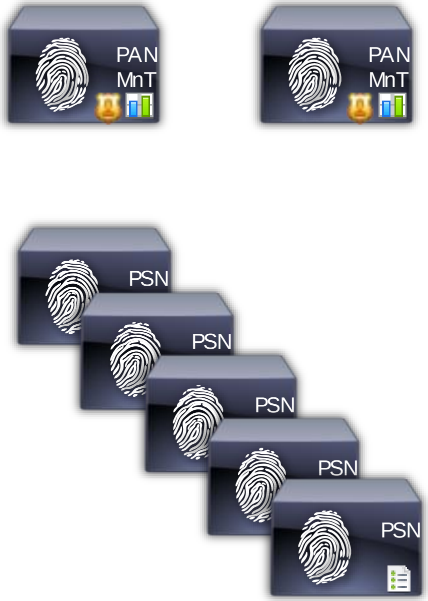


- All Services run on both ISE Nodes
- Set one for Primary Admin / Primary MnT
- Set other for Secondary Monitoring / Secondary Admin
- Max Endpoints is platform dependent:
  - 33x5 = Max 2k endpoints
  - 3415 = Max 5k endpoints
  - 3495 = Max 10k endpoints

Distributed Persona Deployment

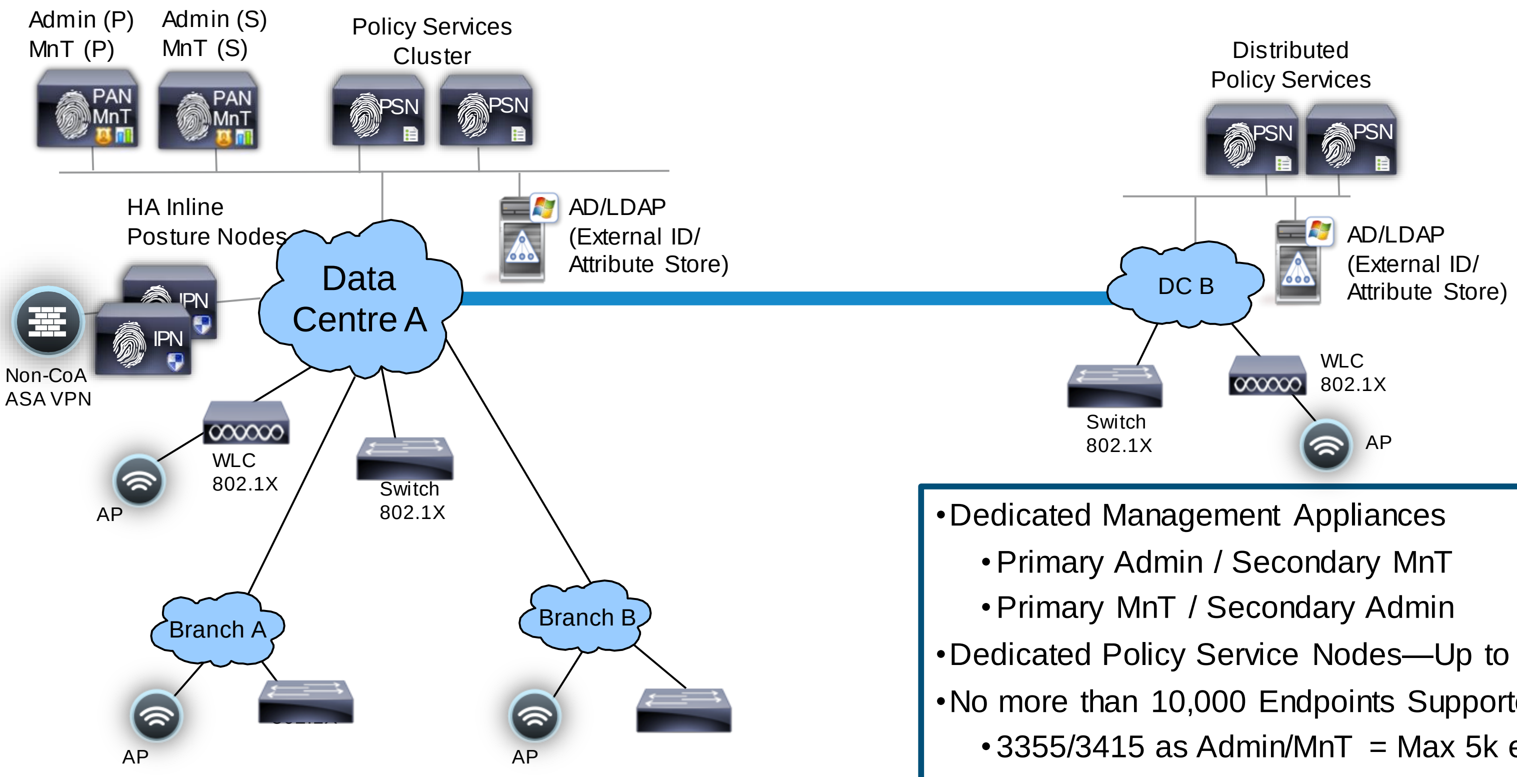
Admin + MnT on Same Appliance; Policy Service on Dedicated Appliance

- 2 x Admin+Monitor
- Max 5 PSNs
- Max endpoints – Platform dependent
  - ➢ 5,000 for 3355 or 3415 as PAN+MnT
  - ➢ 10,000 for 3395 or 3495 as PAN+MnT



Basic Distributed Deployment

Maximum Endpoints = 10,000 / Maximum 5 PSNs

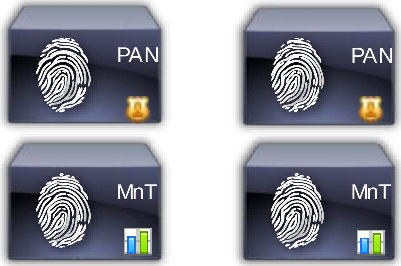


- Dedicated Management Appliances
  - Primary Admin / Secondary MnT
  - Primary MnT / Secondary Admin
- Dedicated Policy Service Nodes—Up to 5 PSNs
- No more than 10,000 Endpoints Supported
  - 3355/3415 as Admin/MnT = Max 5k endpoints
  - 3395/3495 as Admin/MnT = Max 10k endpoints

Distributed Persona Deployment

Dedicated Appliance for Each Persona: Administration, Monitoring, Policy Service

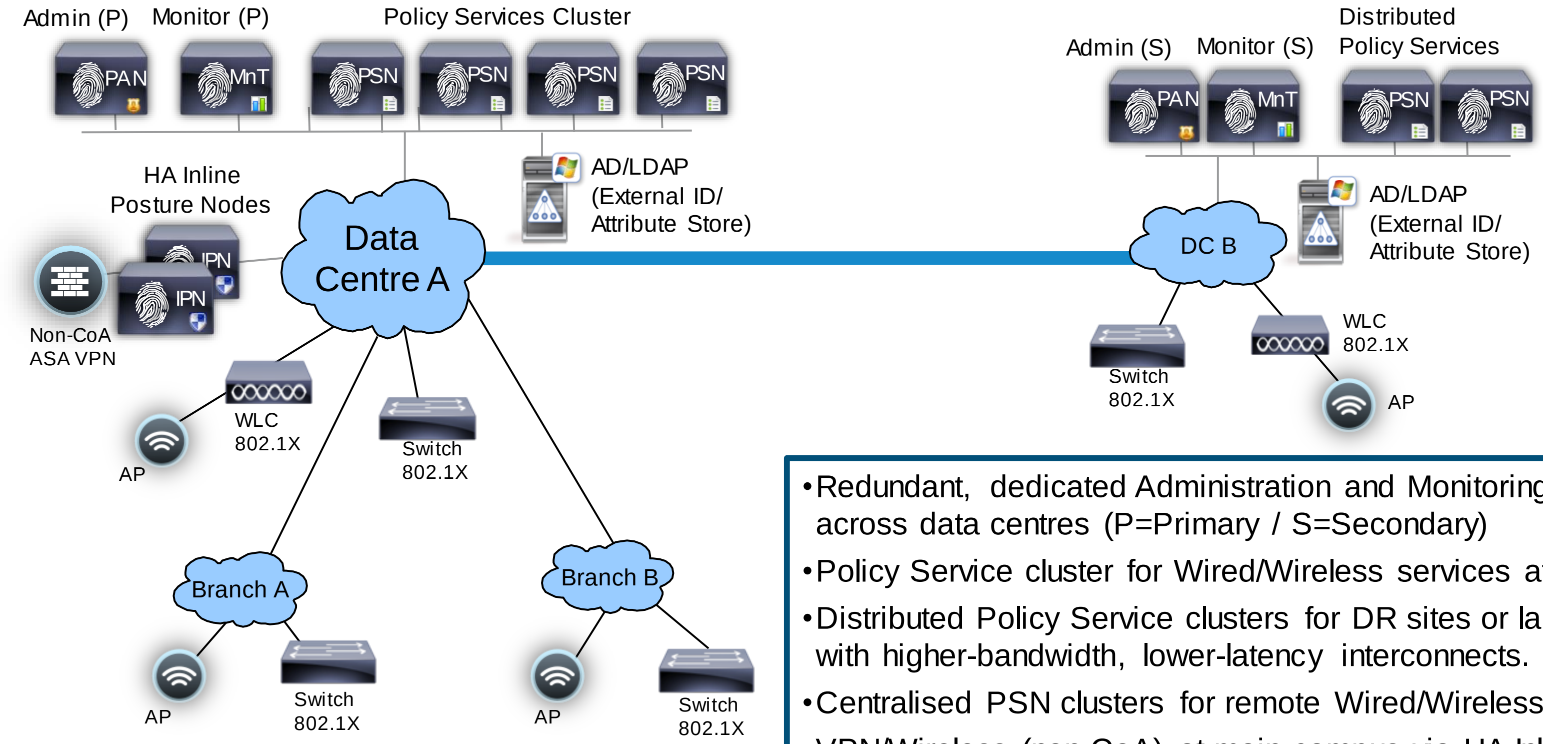
- 2 x Admin
- 2 x Monitoring
- Max 40 PSNs
- Max endpoints (Platform dependent)
  - ➢ 100k using 3395 as PAN and MnT
  - ➢ 250k using 3495 as PAN and MnT



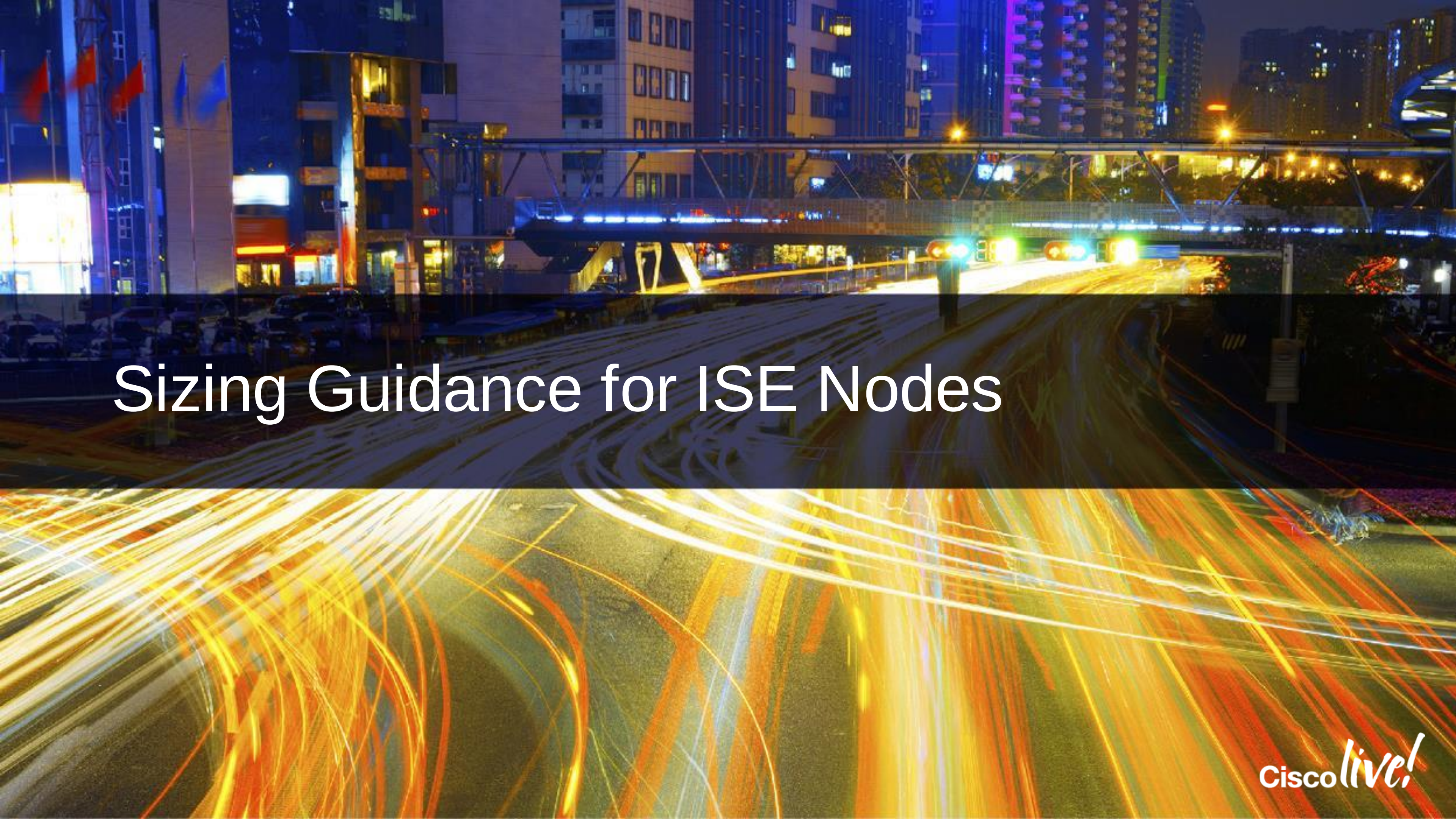
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN
PSN

Fully Distributed Deployment

Maximum Endpoints = 250,000 / Maximum 40 PSNs



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



Sizing Guidance for ISE Nodes

Determining Minimum Appliance Quantity and Platform Type

Persona Deployment	• All Personas running on single or redundant nodes	• Administration and Monitoring co-located on single or redundant nodes • Dedicated Policy Service nodes	• Dedicated Administration node(s) • Dedicated Monitoring node(s) • Dedicated Policy Service nodes
Max Nodes by Type	• 2 Admin+MnT+PSN nodes	• 2 Admin+MnT nodes • 5 Policy Service nodes	• 2 Admin nodes • 2 MnT nodes • 40 Policy Service nodes
Max Endpoints for Entire Deployment	• 2k with ISE-33x5 • 5k with SNS-3415 • 10k with SNS-3495	• 5k with ISE-3355 or SNS-3415 for PAN+MnT • 10k with ISE-3395 or SNS-3495 for PAN+MnT	• 100k with ISE-3395 for PAN and MnT • 250k with SNS-3495 for PAN and MnT

Policy Service Node Sizing

Physical and Virtual Appliance Guidance

- Max Endpoints Per Appliance for Dedicated PSN

Form Factor	Platform Size	Appliance	Maximum Endpoints
Physical	Small	ISE-3315 / ACS-1121	3000
	Medium	ISE-3355	6000
	Large	ISE-3395	10,000
	Small (New)	SNS-3415	5,000
	Large (New)	SNS-3495	20,000
Virtual	S/M/L	VM	3,000-20,000*

* 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

- Inline Posture Specifications

Max Endpoints per any appliance	3000-10,000 (gated by policy service)
Max throughput per any appliance	936 Mbps

Sizing Production VMs to Physical Appliances

Summary

Appliance used for sizing comparison	CPU		Memory (GB)	Physical Disk (GB)*
	# Cores	Clock Rate		
SNS Large (ISE-3495)	8	2.4	32	600
SNS Small (ISE-3415)	4	2.4	16	600

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

VMware OVA Templates (ISE 1.3)

- OVA Templates map to Small and Large hardware appliances
  - EVAL (Evaluation / Lab testing)
  - SNS-3415 (Small)
  - SNS-3495 (Large)
- Simplifies VM deployment
- Ensures proper VMware settings

  Presets:
  - vCPU cores
  - Memory

  With Reservations

  - Disk Storage
  - Network Interfaces

ISE-1.3.x.x-Eval-100-endpoint.ova:

- 2 CPU cores
- 4 GB RAM
- 200 GB disk
- 4 NICs

ISE-1.3.x.x-Virtual-SNS-3415.ova:

- 4 CPU cores
- 16 GB RAM
- 600 GB disk
- 4 NICs

ISE-1.3.x.x-Virtual-SNS-3495.ova:

- 8 CPU cores
- 32 GB RAM
- 600 GB disk
- 4 NICs

ISE VM Production Disk Requirements by Persona

- Thin Provisioning officially supported in ISE 1.3
- VMFS formatted file system support only
- IO Perfomance:
  - ➢ Read 300+ MB/sec and Write 50+ MB/sec
- Recommended storage:
  - ➢ 10k RPM+ disk drives
  - ➢ Caching RAID Controller
  - ➢ RAID mirroring (RAID 5 slower writes)

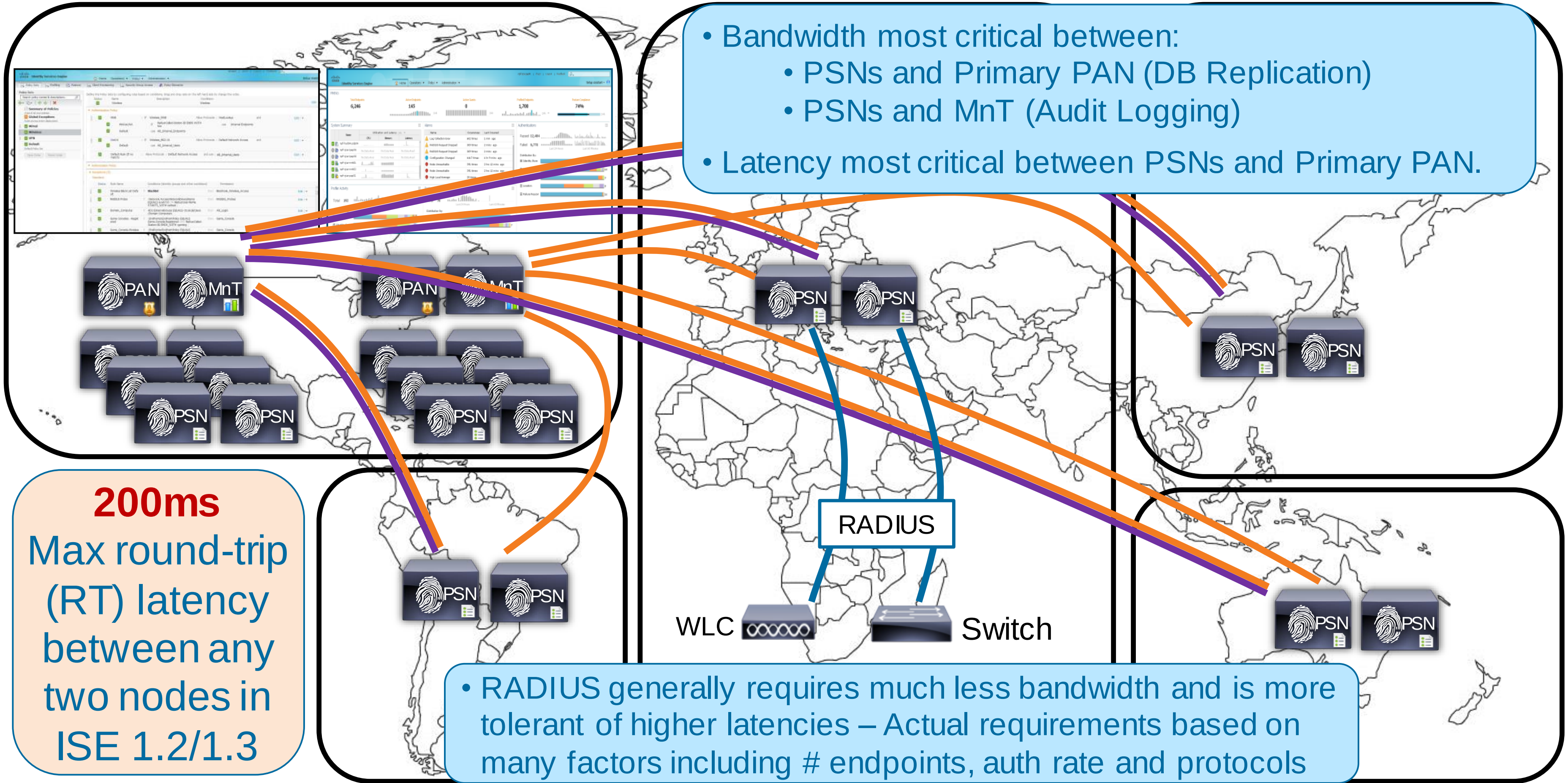
RAID perf levels: http://www.datarecovery.net/articles/raid-level-comparison.html

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

* Upper range sets #days MnT log retention; **500GB min recommended for production. Max hardware appliance disk size = 600GB—Max VM disk size = 2TB**

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

Large Deployments – Bandwidth and Latency

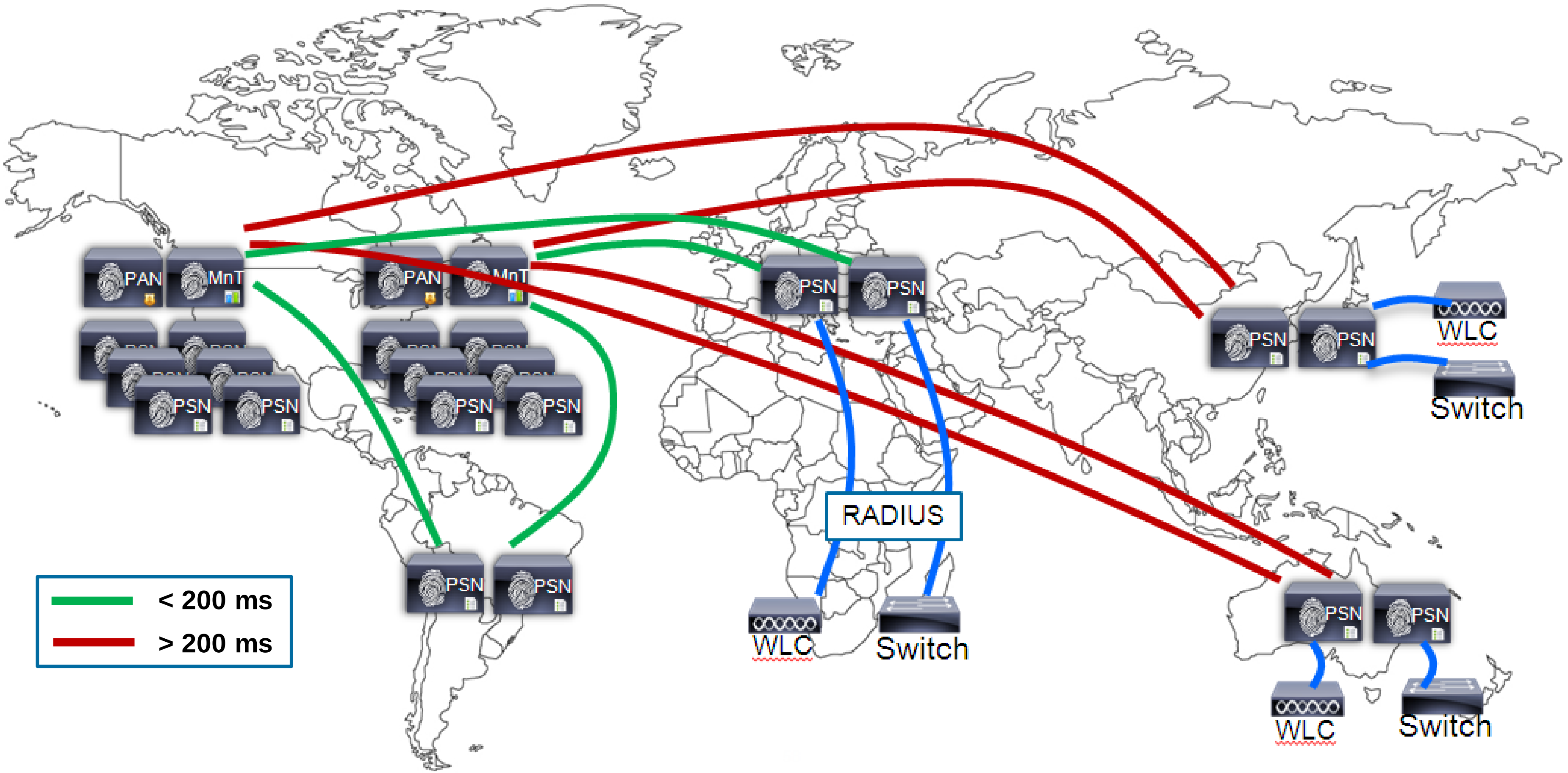


- Bandwidth most critical between:
    - PSNs and Primary PAN (DB Replication)
    - PSNs and MnT (Audit Logging)
- Latency most critical between PSNs and Primary PAN.

200ms
Max round-trip (RT) latency between any two nodes in ISE 1.2/1.3

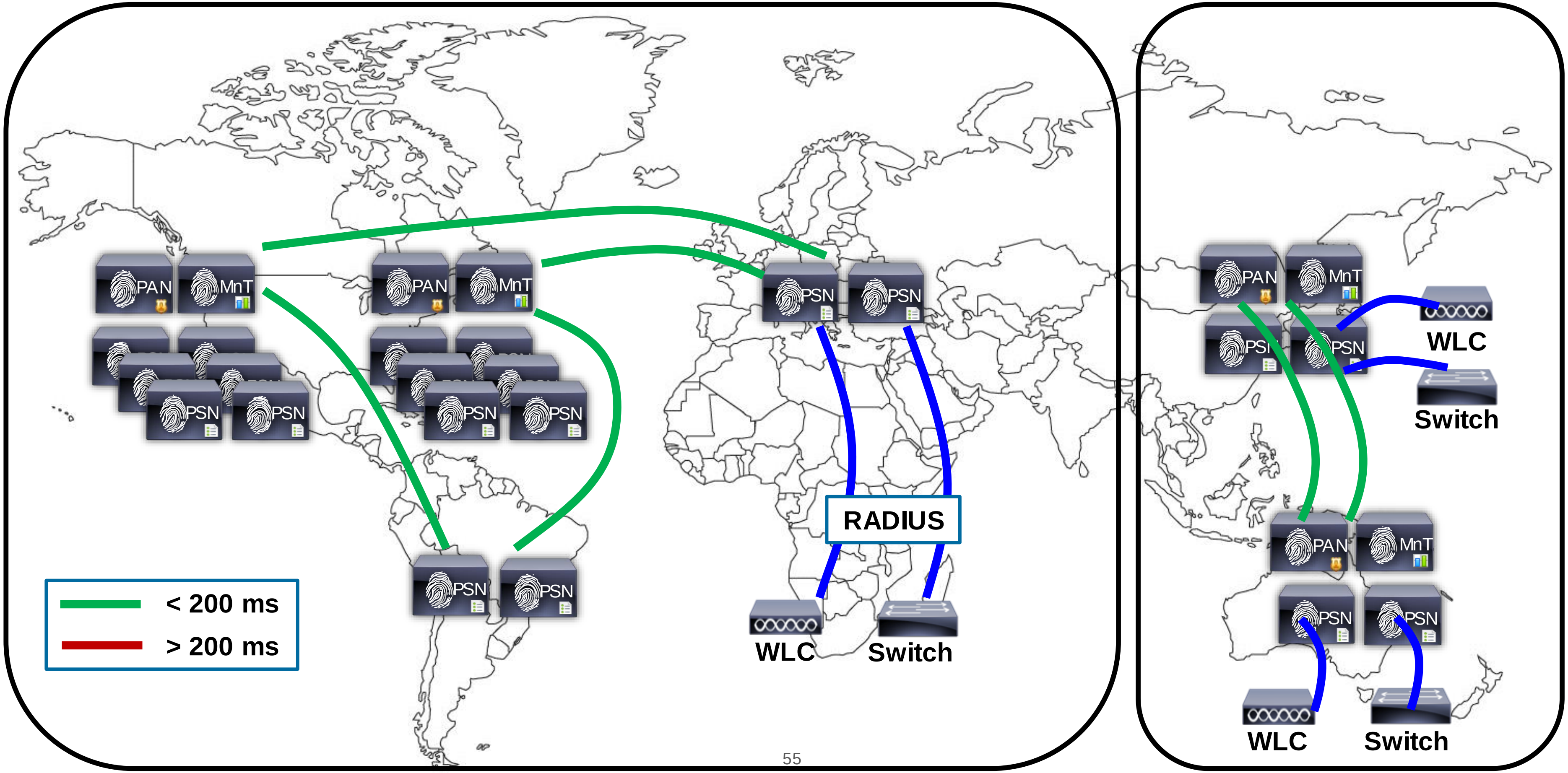
- RADIUS generally requires much less bandwidth and is more tolerant of higher latencies – Actual requirements based on many factors including # endpoints, auth rate and protocols

What if Distributed PSNs > 200ms RTT Latency?

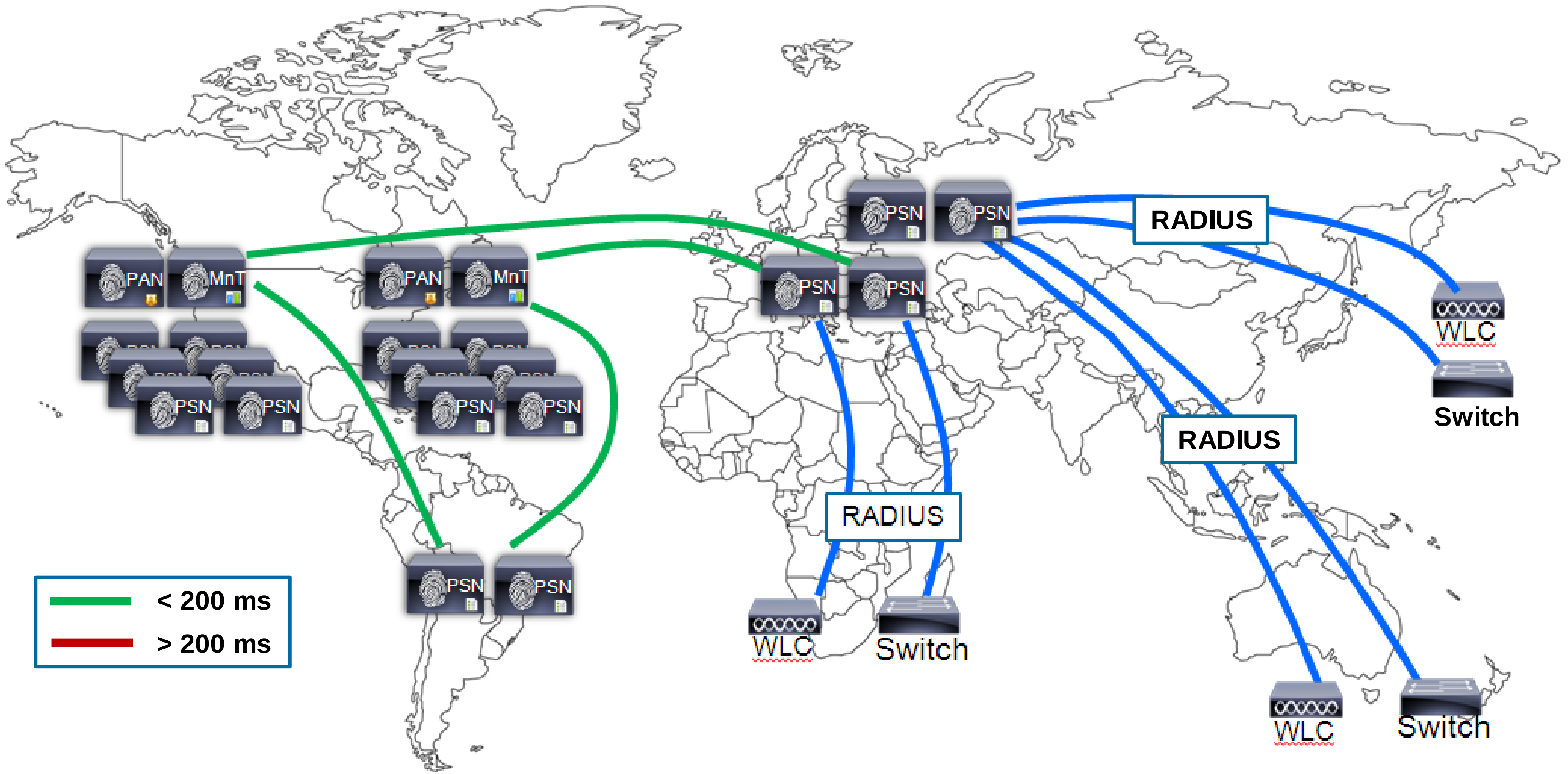


Option #1: Deploy Separate ISE Instances

(Per-Instance Latency < 200ms)

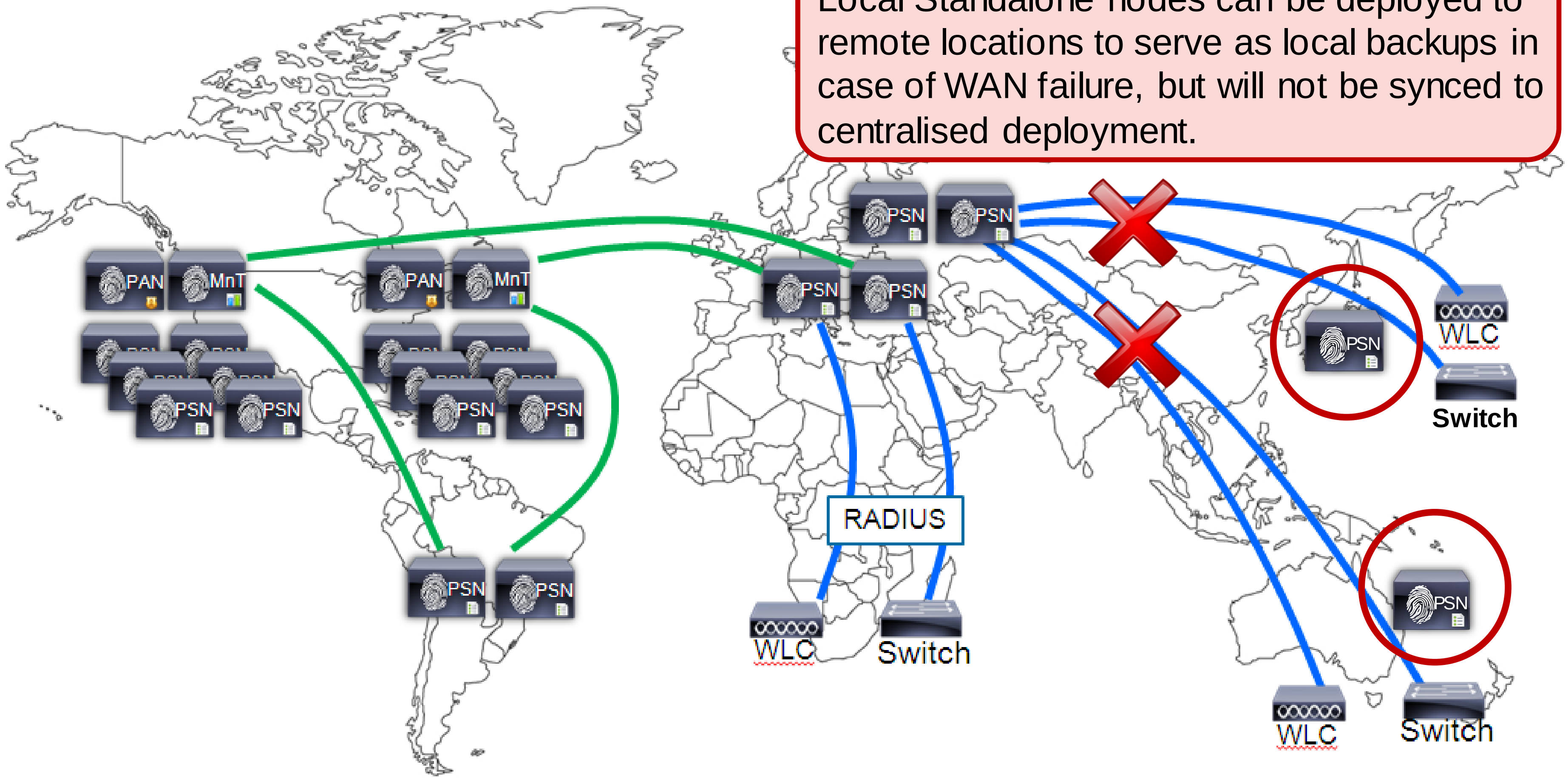


Option #2: Centralise PSNs where Latency < 200ms

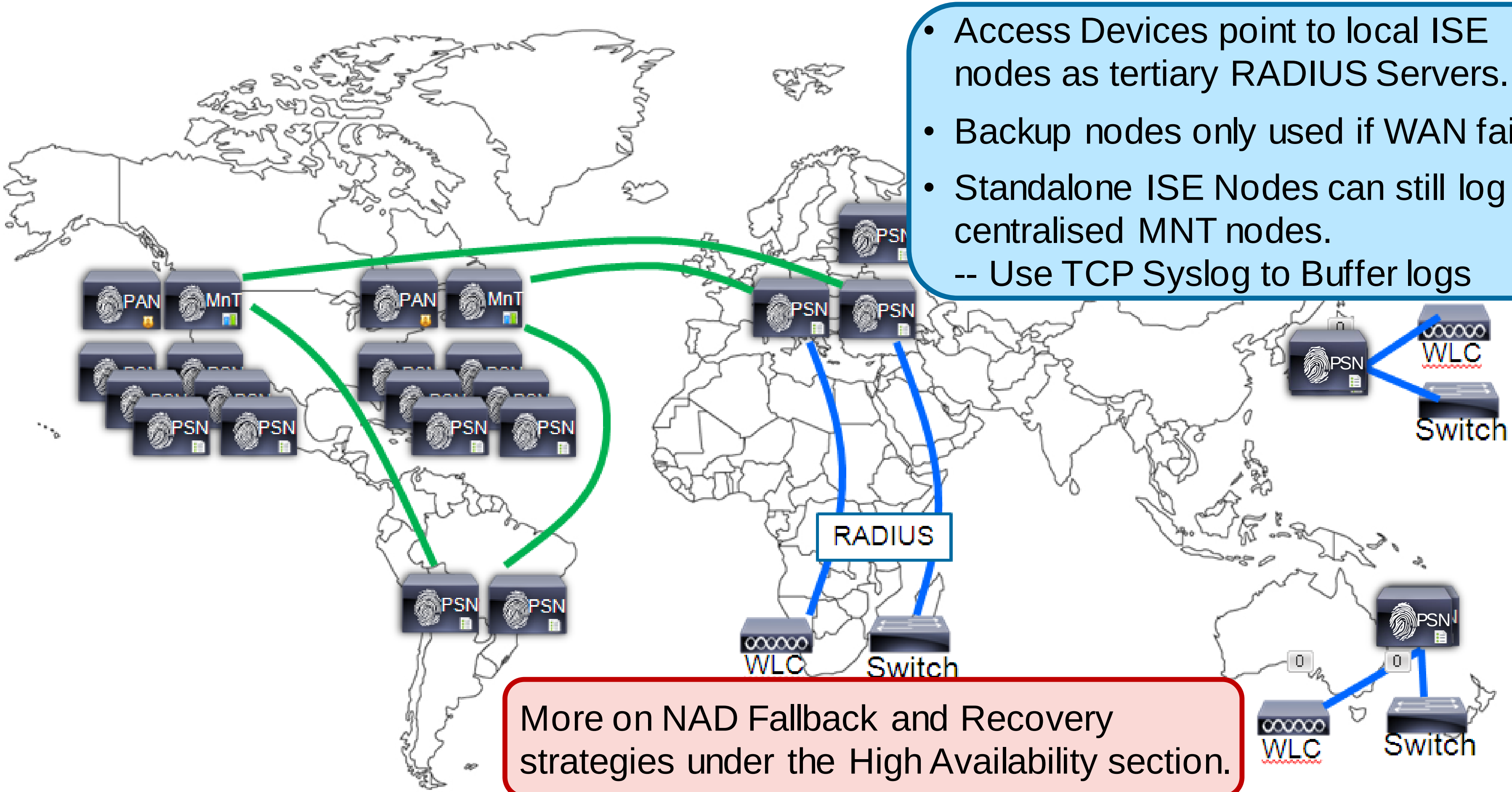


Deploy Local Standalone ISE Nodes as “Standby”

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



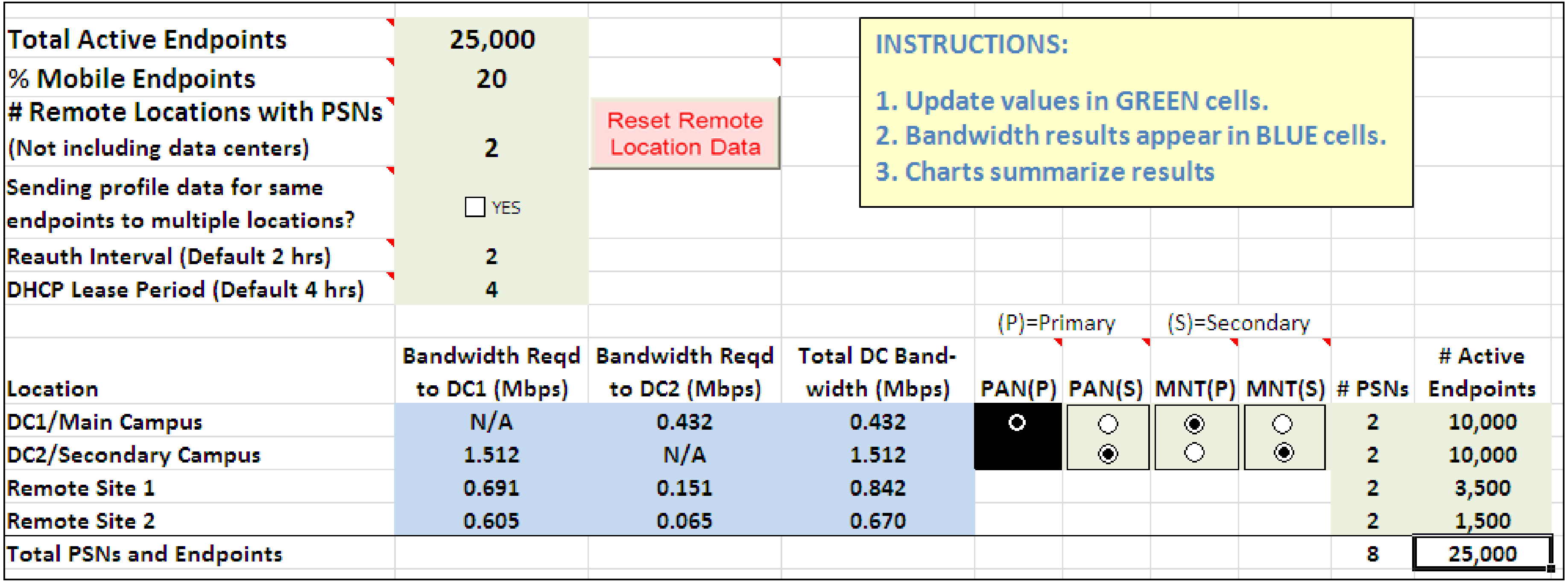
Access Devices Fallback to Local PSNs on WAN Failure



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

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

ISE 1.2 Bandwidth Calculator (Multi-Site)



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

INSTRUCTIONS:

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

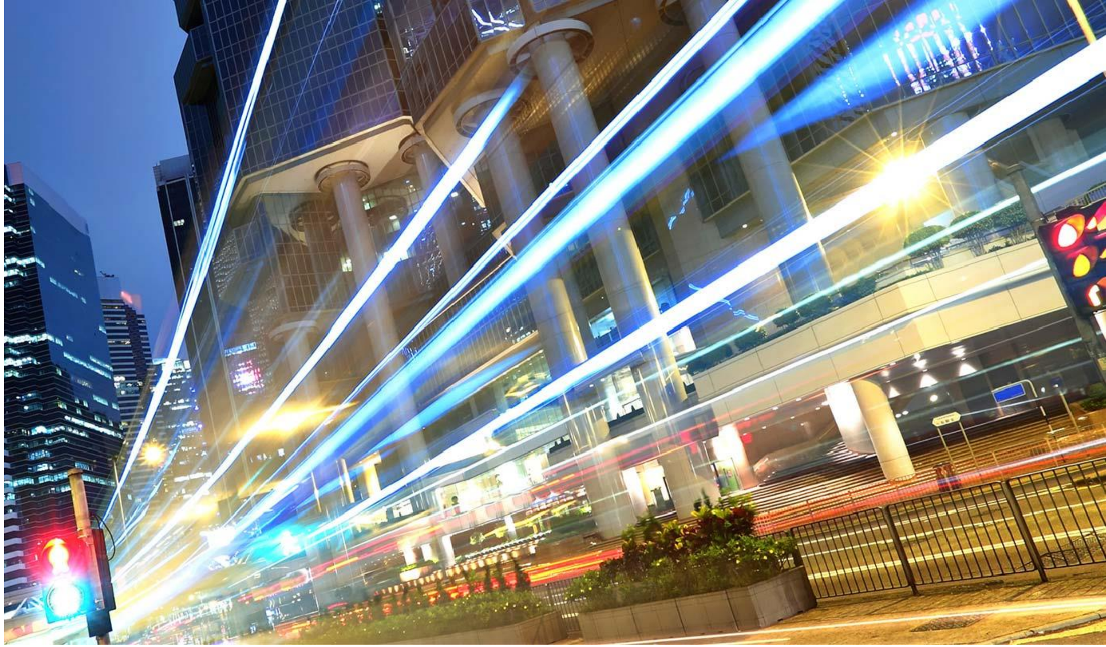
				(P)=Primary		(S)=Secondary			
Location	Bandwidth Reqd to DC1 (Mbps)	Bandwidth Reqd to DC2 (Mbps)	Total DC Band-width (Mbps)	PAN(P)	PAN(S)	MNT(P)	MNT(S)	# PSNs	# Active Endpoints
DC1/Main Campus	N/A	0.432	0.432	○	○	◉	○	2	10,000
DC2/Secondary Campus	1.512	N/A	1.512		◉	○	◉	2	10,000
Remote Site 1	0.691	0.151	0.842					2	3,500
Remote Site 2	0.605	0.065	0.670					2	1,500
Total PSNs and Endpoints								8	25,000

Please contact your Certified ATP Partner/SE to request a WAN bandwidth analysis for your ISE design and deployment. For additional information, ATP Partners and customers can contact sac-support@cisco.com

Scaling ISE Services

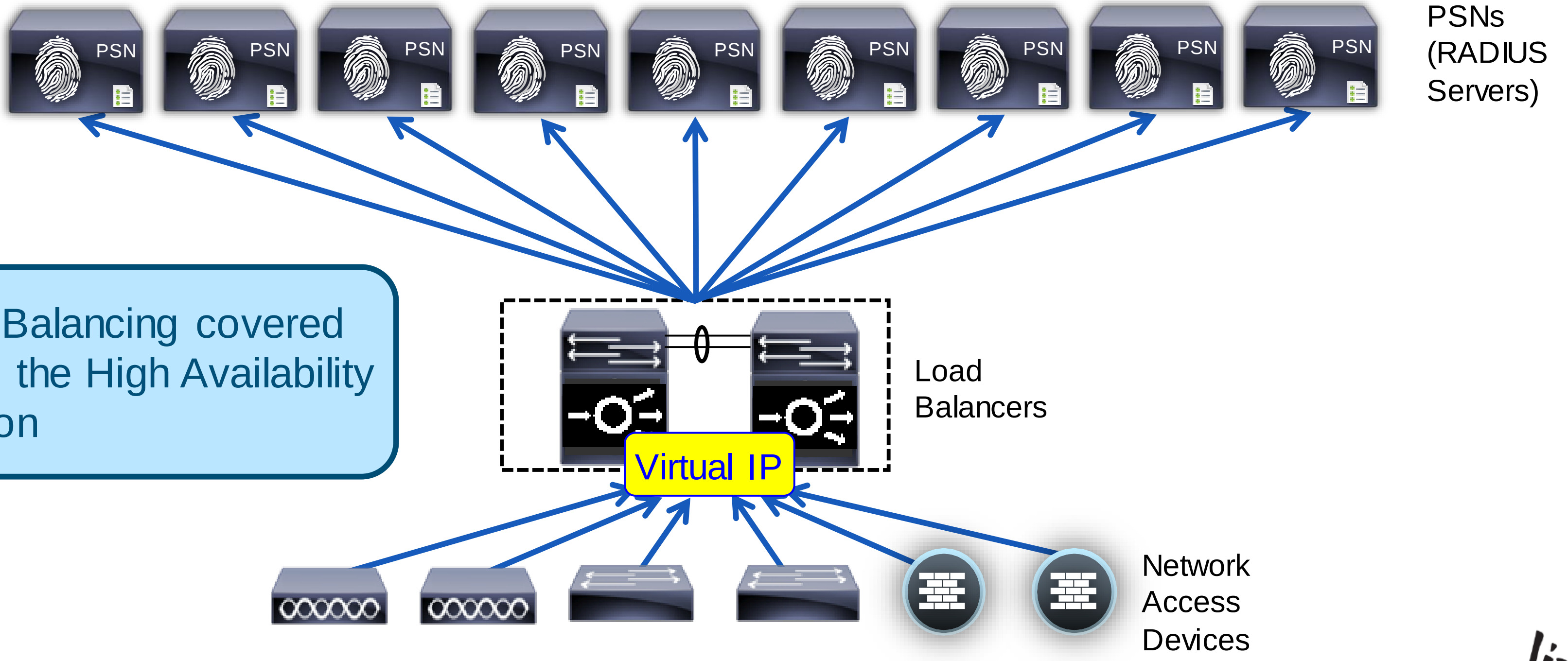
Scaling ISE Services Agenda

- AAA and Auth Policy Tuning
- Active Directory Integration
- Guest and Web Authentication
- Profiling and Database Replication
- MnT (Optimised Logging and Noise Suppression)



Scaling RADIUS, Web, and Profiling Services w/ LB

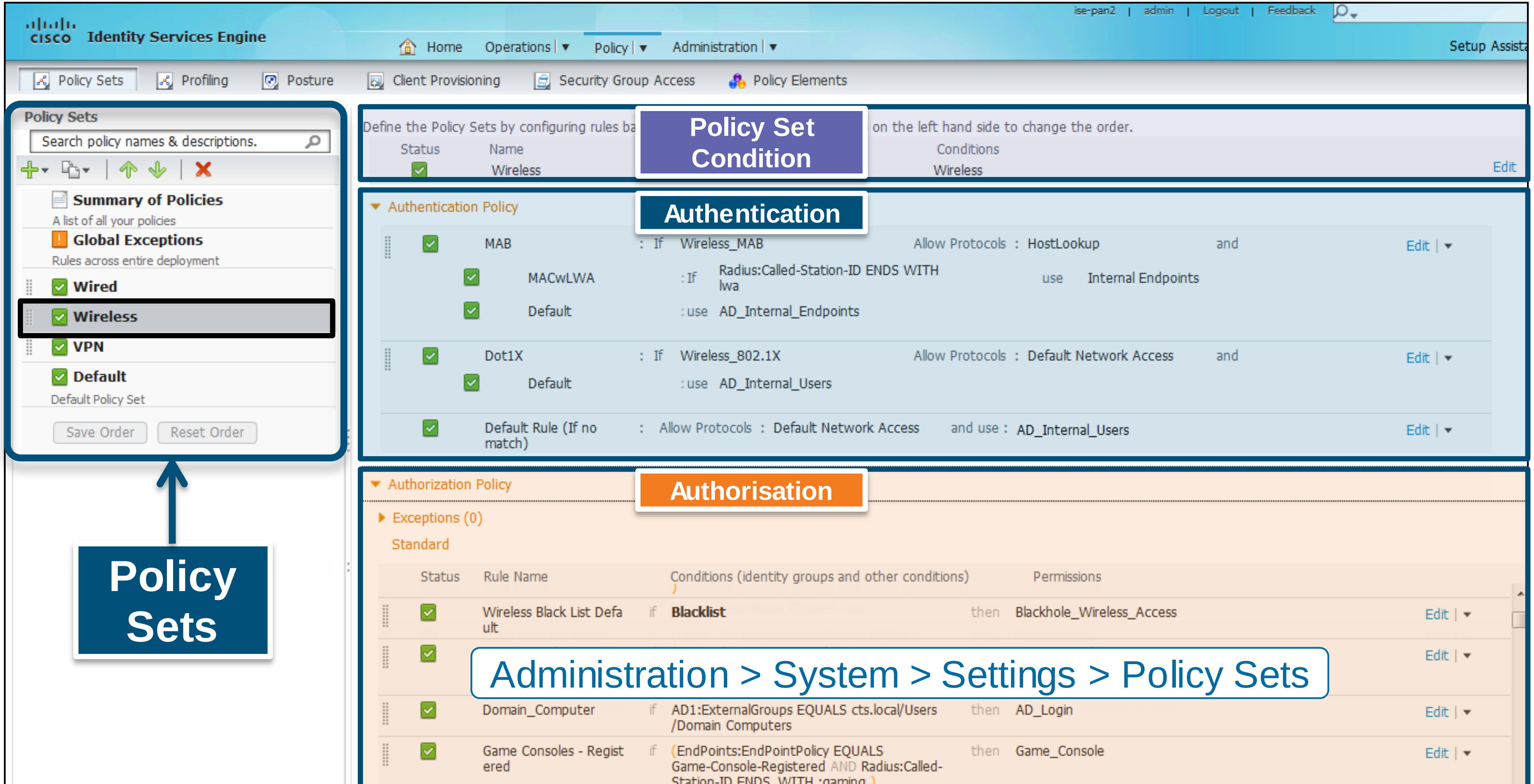
- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS AAA requests to LB virtual IP.



Load Balancing covered under the High Availability Section

Auth Policy Optimisation

Leverage Policy Sets to Organise and Scale Policy Processing



Policy Sets

- **Summary of Policies**
  A list of all your policies
- **Global Exceptions**
  Rules across entire deployment
- ☑ **Wired**
- ☑ **Wireless**
- ☑ **VPN**
- ☑ **Default**
  Default Policy Set

Policy Sets

Define the Policy Sets by configuring rules ba... on the left hand side to change the order.

Status	Name	Conditions	
☑	Wireless	Wireless	Edit

Policy Set Condition

Authentication Policy

Authentication

☑ MAB : If Wireless_MAB Allow Protocols : HostLookup and — Edit | ▾

- ☑ MACwLWA : If Radius:Called-Station-ID ENDS WITH lwa use Internal Endpoints
- ☑ Default : use AD_Internal_Endpoints

☑ Dot1X : If Wireless_802.1X Allow Protocols : Default Network Access and — Edit | ▾

- ☑ Default : use AD_Internal_Users

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : AD_Internal_Users — Edit | ▾

Authorization Policy

Authorisation

Exceptions (0)

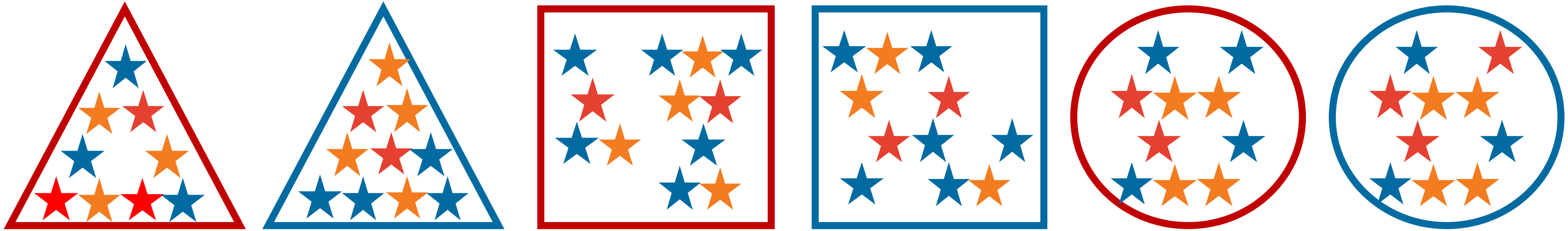
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist**	then	Blackhole_Wireless_Access	Edit | ▾
☑						Edit | ▾
☑	Domain_Computer	if	AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers	then	AD_Login	Edit | ▾
☑	Game Consoles - Registered	if	(EndPoints:EndPointPolicy EQUALS Game-Console-Registered AND Radius:Called-Station-ID ENDS_WITH :gaming)	then	Game_Console	Edit | ▾

Administration > System > Settings > Policy Sets

Search Speed Test

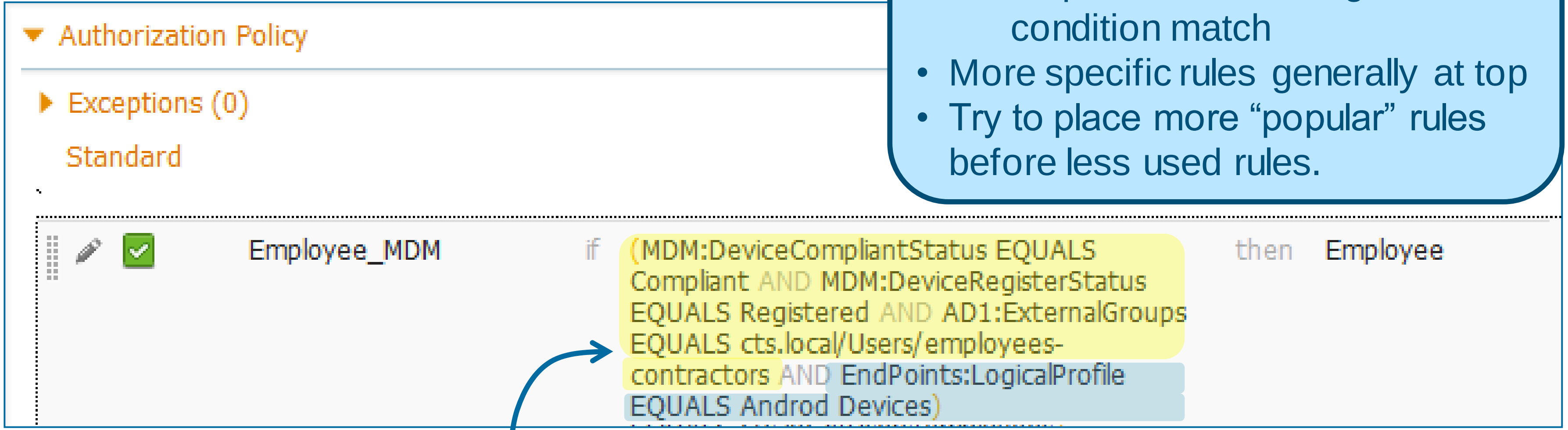
- Find the object where…
  - Total stars = 10
  - Total Orange stars = 4
  - Total Red stars = 2
  - Outer shape is a red circle



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.



Authorization Policy

Exceptions (0)

Standard

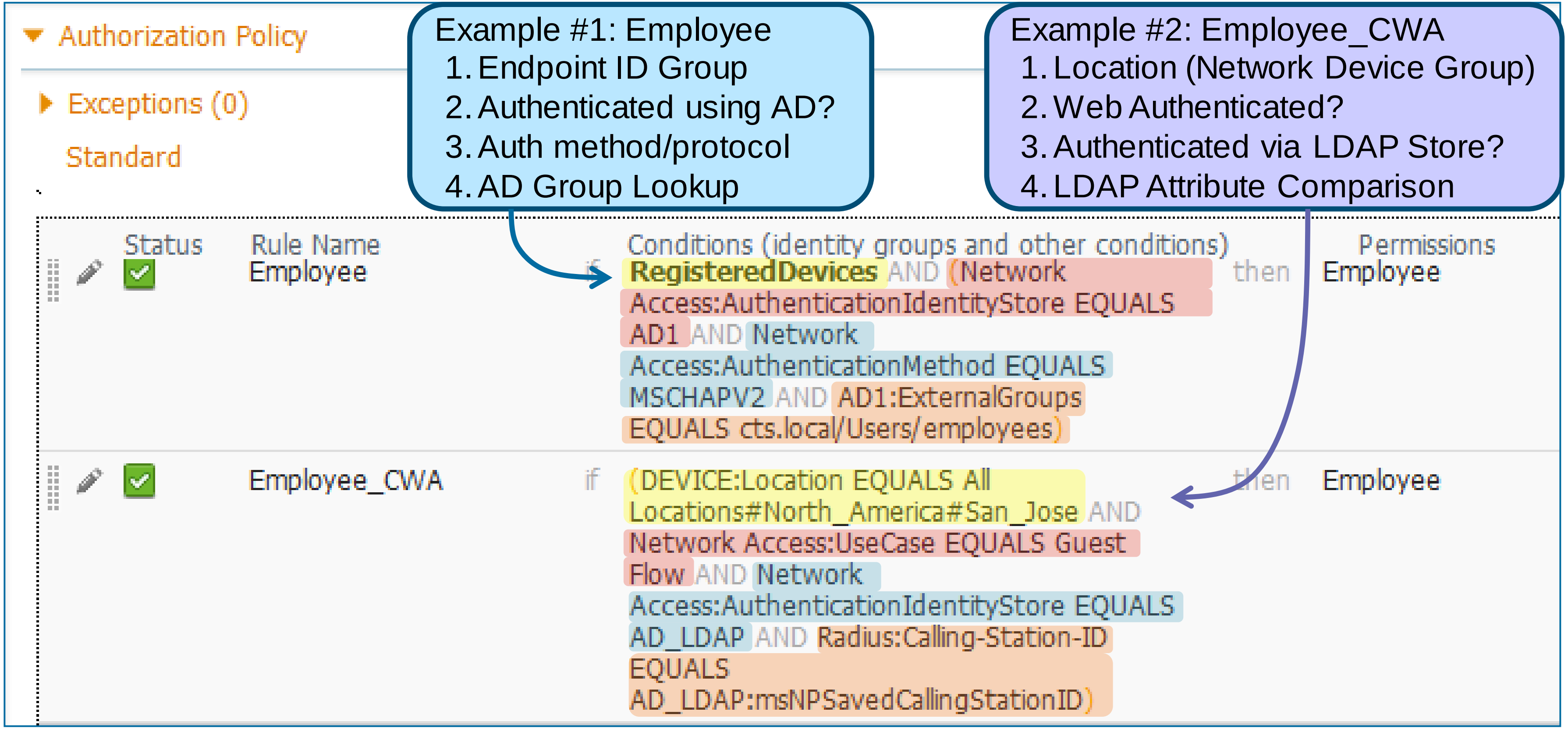
Employee_MDM if (MDM:DeviceCompliantStatus EQUALS Compliant AND MDM:DeviceRegisterStatus EQUALS Registered AND AD1:ExternalGroups EQUALS cts.local/Users/employees-contractors AND EndPoints:LogicalProfile EQUALS Androd Devices) then Employee

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!



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

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

Authorization Policy

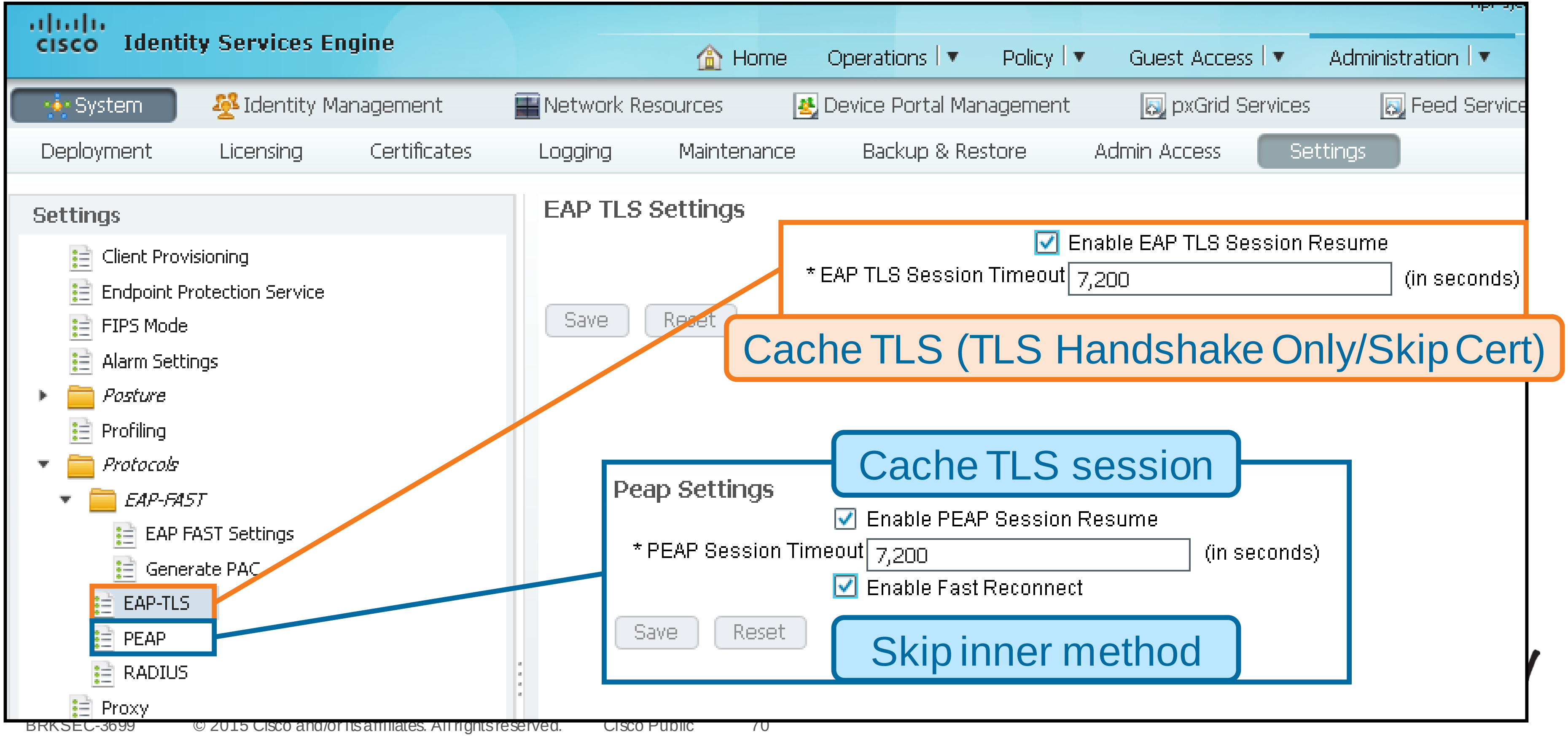
Exceptions (0)

Standard

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

Enable EAP Session Resume / Fast Reconnect

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



EAP TLS Settings

☑ Enable EAP TLS Session Resume

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

Cache TLS (TLS Handshake Only/Skip Cert)

Peap Settings

Cache TLS session

☑ Enable PEAP Session Resume

* PEAP Session Timeout 7,200 (in seconds)

☑ Enable Fast Reconnect

Skip inner method

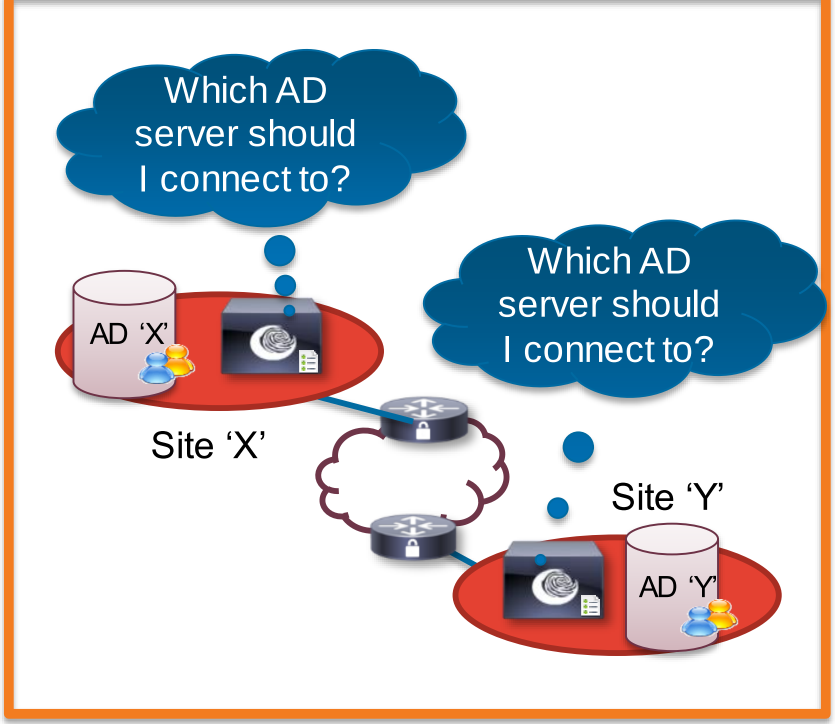
Scaling AD Integration

Scaling AD Integration w/ Sites & Services

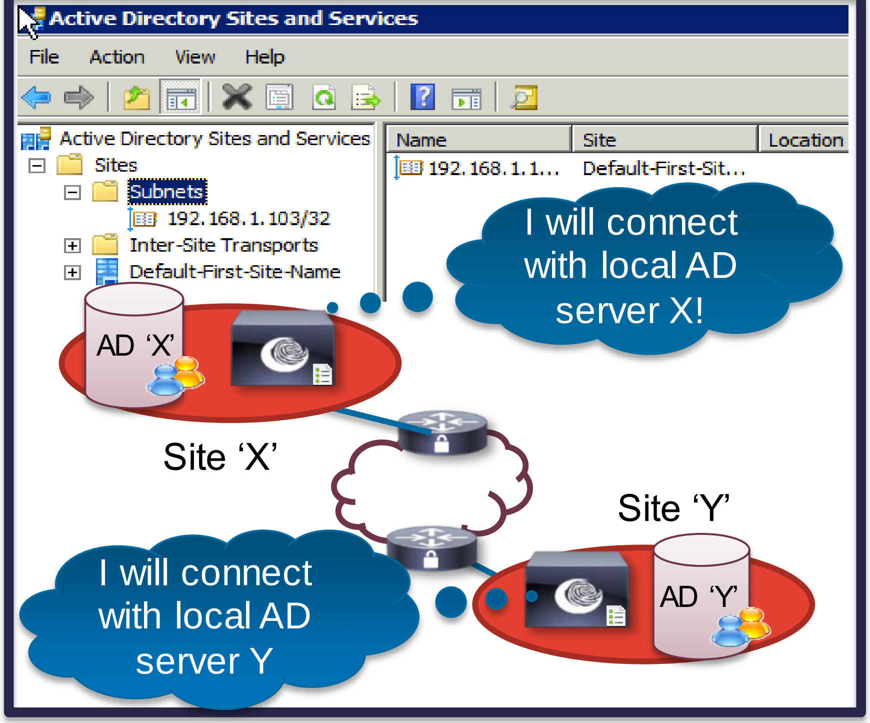
Active Directory Sites and Services
Shortcut

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

Without Site & Services


Which AD server should I connect to?
AD 'X'
Site 'X'
Which AD server should I connect to?
Site 'Y'
AD 'Y'

Properly Configured


Active Directory Sites and Services
File Action View Help
I will connect with local AD server X!
AD 'X'
Site 'X'
Site 'Y'
AD 'Y'
I will connect with local AD server Y

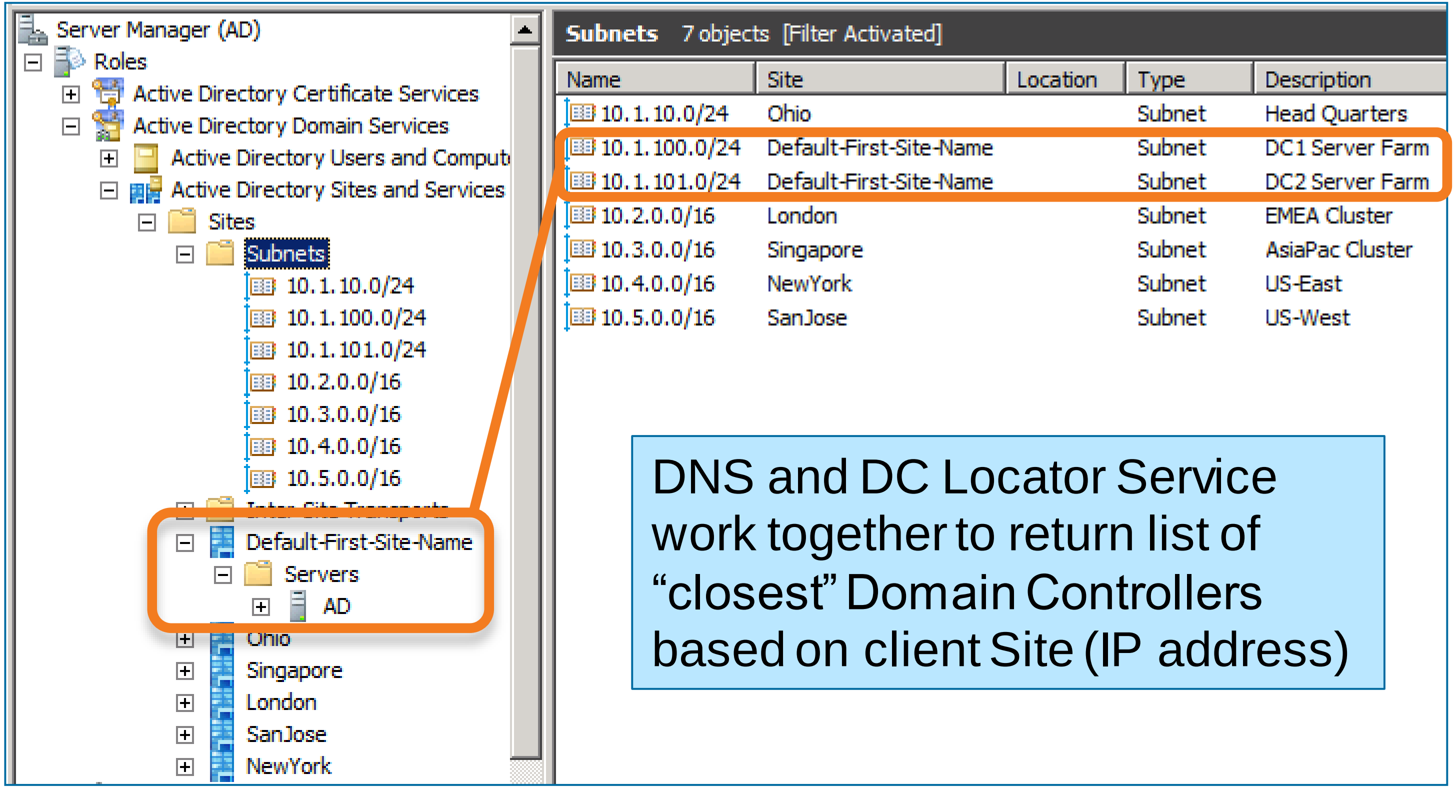
- Active Directory Sites and Services
  - Sites
    - Subnets
      - 192.168.1.103/32
    - Inter-Site Transports
    - Default-First-Site-Name

Name	Site	Location
192.168.1.1...	Default-First-Sit...	

AD Sites and Services

Active Directory Sites and Services
Shortcut

Links AD Domain Controllers to Client IP Networks



```
Server Manager (AD)
⊟ Roles
    ⊞ Active Directory Certificate Services
    ⊟ Active Directory Domain Services
        ⊞ Active Directory Users and Comput
        ⊟ Active Directory Sites and Services
            ⊟ Sites
                ⊟ Subnets
                    10.1.10.0/24
                    10.1.100.0/24
                    10.1.101.0/24
                    10.2.0.0/16
                    10.3.0.0/16
                    10.4.0.0/16
                    10.5.0.0/16
                ⊞ Inter-Site Transports
                ⊟ Default-First-Site-Name
                    ⊟ Servers
                        ⊞ AD
                ⊞ Ohio
                ⊞ Singapore
                ⊞ London
                ⊞ SanJose
                ⊞ NewYork
```

Subnets 7 objects [Filter Activated]

Name	Site	Location	Type	Description
10.1.10.0/24	Ohio		Subnet	Head Quarters
10.1.100.0/24	Default-First-Site-Name		Subnet	DC1 Server Farm
10.1.101.0/24	Default-First-Site-Name		Subnet	DC2 Server Farm
10.2.0.0/16	London		Subnet	EMEA Cluster
10.3.0.0/16	Singapore		Subnet	AsiaPac Cluster
10.4.0.0/16	NewYork		Subnet	US-East
10.5.0.0/16	SanJose		Subnet	US-West

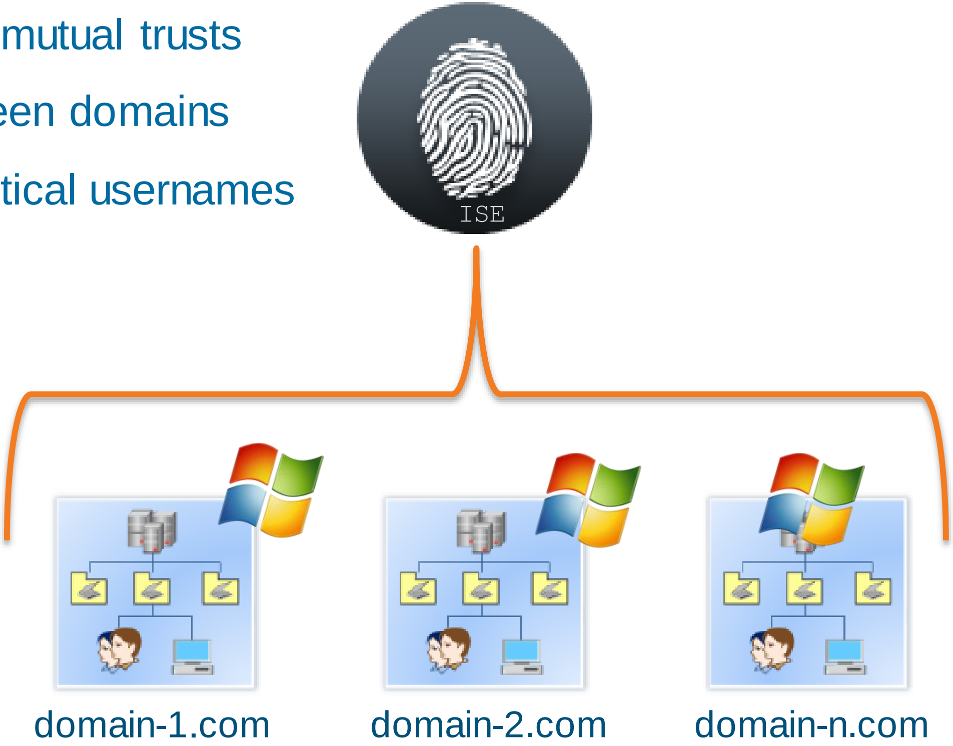
DNS and DC Locator Service work together to return list of "closest" Domain Controllers based on client Site (IP address)

Multi–Forest Active Directory Support

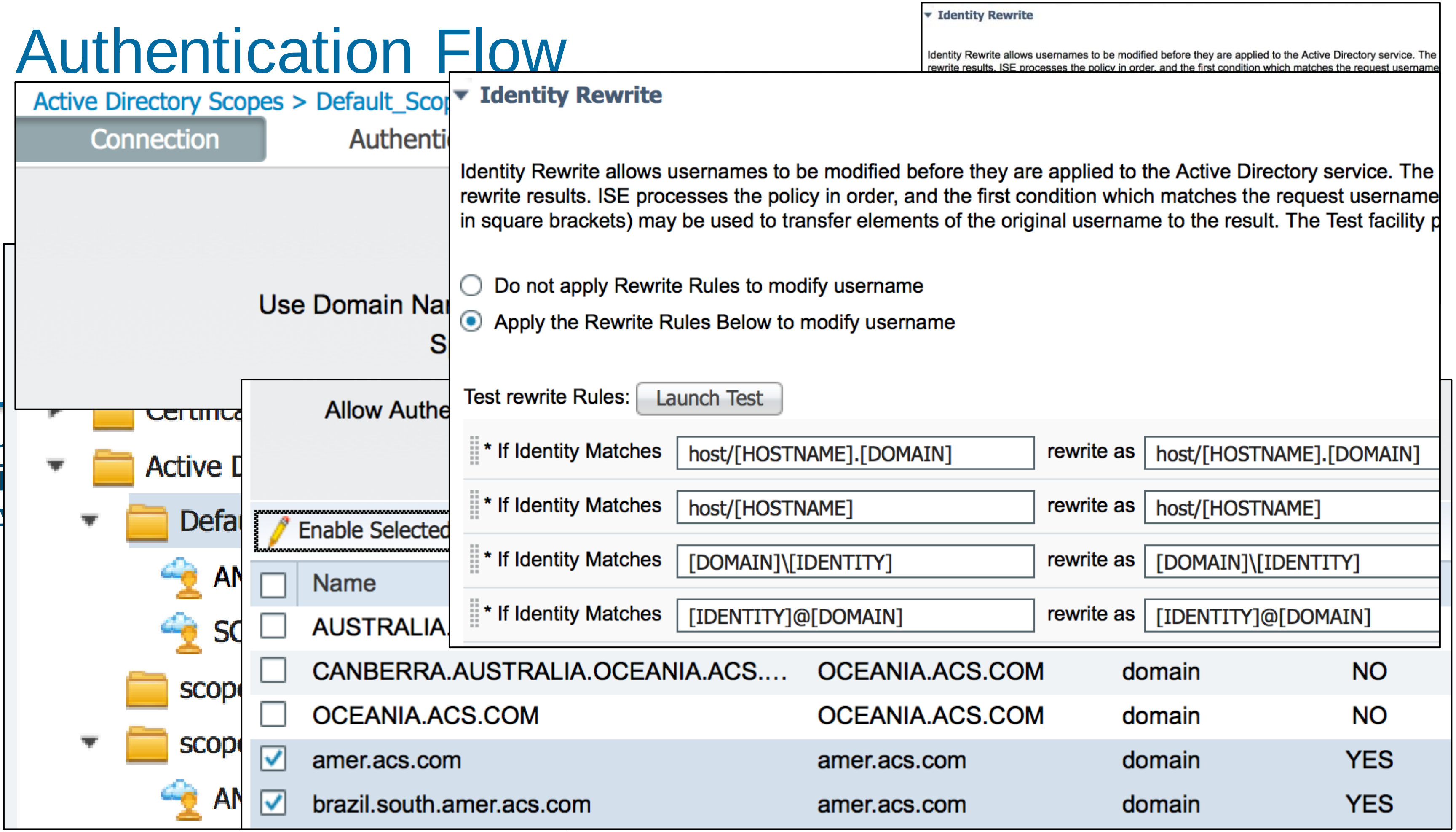
New in ISE 1.3

Scales AD Integration through Multiple Join Points and Optimised Lookups

- ✓ Join up to 50 Forests or Domains without mutual trusts
- ✓ No need for 2-way trust relationship between domains
- ✓ Advanced algorithms for dealing with identical usernames
- ✓ SID-Based Group Mapping
- ✓ PAP via MS-RPC
- ✓ Support for disjointed DNS namespace



AD Authentication Flow



Au
Poli
A

Active Directory Scopes > Default_Scop

Connection | Authenti

Use Domain Na
S

Allow Authe

Certifica
Active D
Defa
AN
SC
scope
scope
AN

✎ Enable Selected

□	Name			
□	AUSTRALIA			
□	CANBERRA.AUSTRALIA.OCEANIA.ACS....	OCEANIA.ACS.COM	domain	NO
□	OCEANIA.ACS.COM	OCEANIA.ACS.COM	domain	NO
☑	amer.acs.com	amer.acs.com	domain	YES
☑	brazil.south.amer.acs.com	amer.acs.com	domain	YES

▾ Identity Rewrite

Identity Rewrite allows usernames to be modified before they are applied to the Active Directory service. The rewrite results. ISE processes the policy in order, and the first condition which matches the request username

▾ **Identity Rewrite**

Identity Rewrite allows usernames to be modified before they are applied to the Active Directory service. The rewrite results. ISE processes the policy in order, and the first condition which matches the request username in square brackets) may be used to transfer elements of the original username to the result. The Test facility p

○ Do not apply Rewrite Rules to modify username
● Apply the Rewrite Rules Below to modify username

Test rewrite Rules: Launch Test

* If Identity Matches	host/[HOSTNAME].[DOMAIN]	rewrite as	host/[HOSTNAME].[DOMAIN]
* If Identity Matches	host/[HOSTNAME]	rewrite as	host/[HOSTNAME]
* If Identity Matches	[DOMAIN]\[IDENTITY]	rewrite as	[DOMAIN]\[IDENTITY]
* If Identity Matches	[IDENTITY]@[DOMAIN]	rewrite as	[IDENTITY]@[DOMAIN]

AD Integration Best Practices

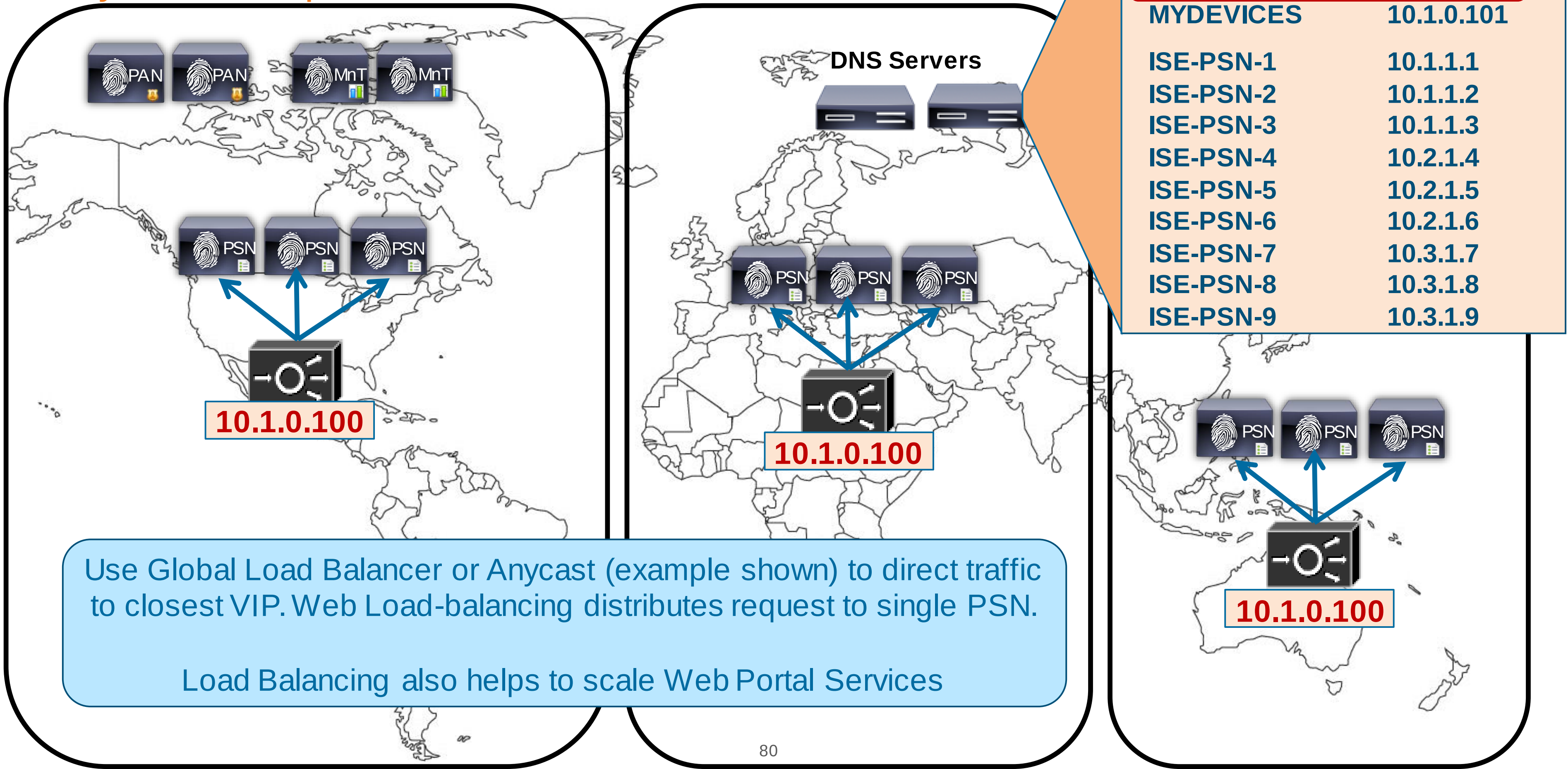
- **DNS** servers in ISE nodes must have all relevant AD records (A, PTR, SRV)
- Ensure **NTP** configured for all ISE nodes and AD servers
- Configure **AD Sites and Services**
  (with ISE machine accounts configured for relevant Sites)
- Configure Authentication Domains (**Whitelist domains** needed) (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 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

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

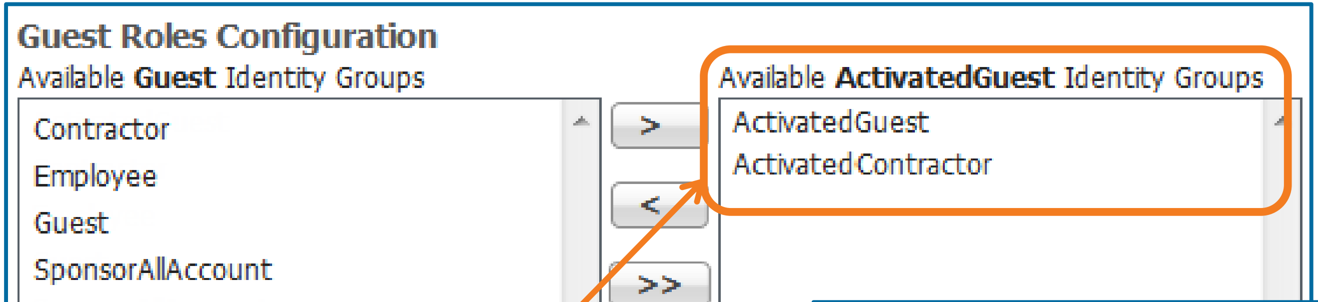
Use Global Load Balancer or Anycast (example shown) to direct traffic to closest VIP. Web Load-balancing distributes request to single PSN.

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



Guest Roles Configuration

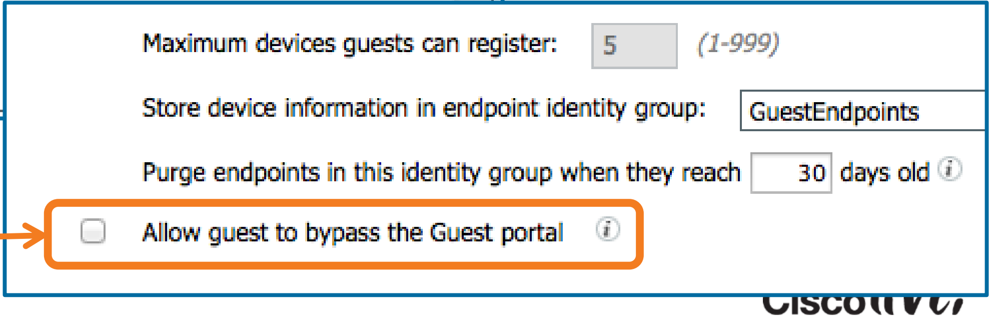
Available **Guest** Identity Groups

- Contractor
- Employee
- Guest
- SponsorAllAccount
- SponsorGroupAccounts
- SponsorOwnAccounts

Available **ActivatedGuest** Identity Groups

- ActivatedGuest
- ActivatedContractor

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



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

Store device information in endpoint identity group: GuestEndpoints

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

☐ Allow guest to bypass the Guest portal

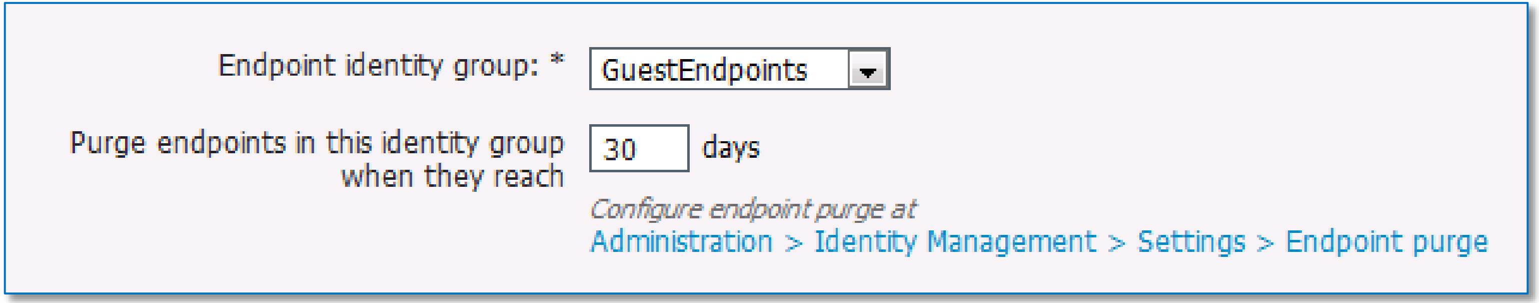
- ISE 1.2 Guest Role
- ISE 1.3 Guest Type

Scaling Web Authentication (ISE 1.3)

“Remember Me” Guest Flows

For ISE 1.2, can “chain” CWA+DRW or NSP to auto-register web auth users, but no auto-purge

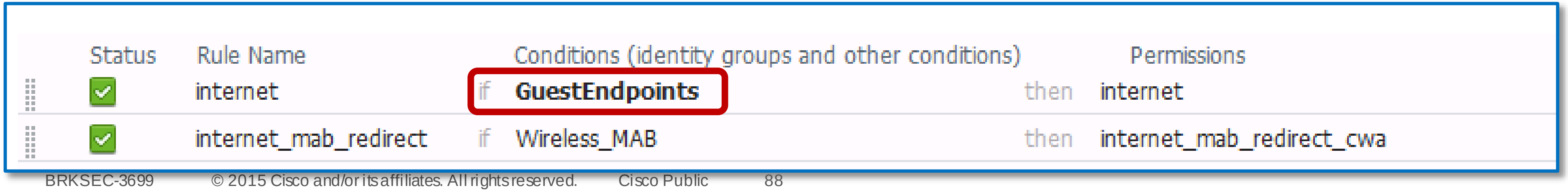
- Device/user logs in to hotspot or credentialed portal
- MAC address automatically registered into GuestEndpoint group
- Authz policy for GuestEndpoint ID Group grants access until device purged



Endpoint identity group: * GuestEndpoints

Purge endpoints in this identity group when they reach 30 days

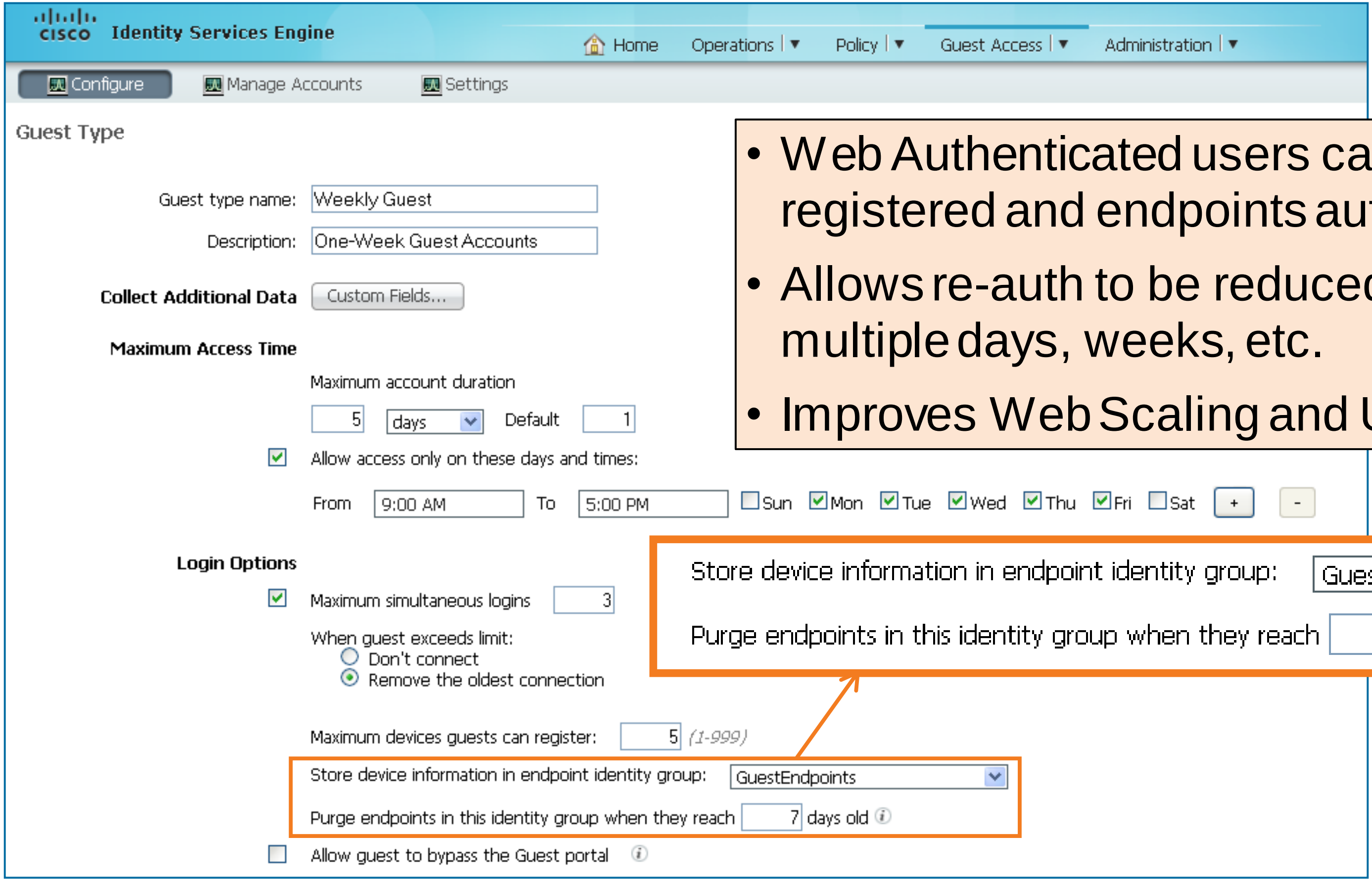
Configure endpoint purge at
Administration > Identity Management > Settings > Endpoint purge



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	internet	if	GuestEndpoints	then	internet
✓	internet_mab_redirect	if	Wireless_MAB	then	internet_mab_redirect_cwa

Automated Device Registration and Purge

New in ISE 1.3



Guest Type

Guest type name: Weekly Guest

Description: One-Week Guest Accounts

Collect Additional Data [Custom Fields...]

Maximum Access Time

Maximum account duration

5 days Default 1

☑ Allow access only on these days and times:

From 9:00 AM To 5:00 PM □Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri □Sat [+] [-]

Login Options

☑ Maximum simultaneous logins 3

When guest exceeds limit:
○ Don't connect
● Remove the oldest connection

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

Store device information in endpoint identity group: GuestEndpoints

Purge endpoints in this identity group when they reach 7 days old

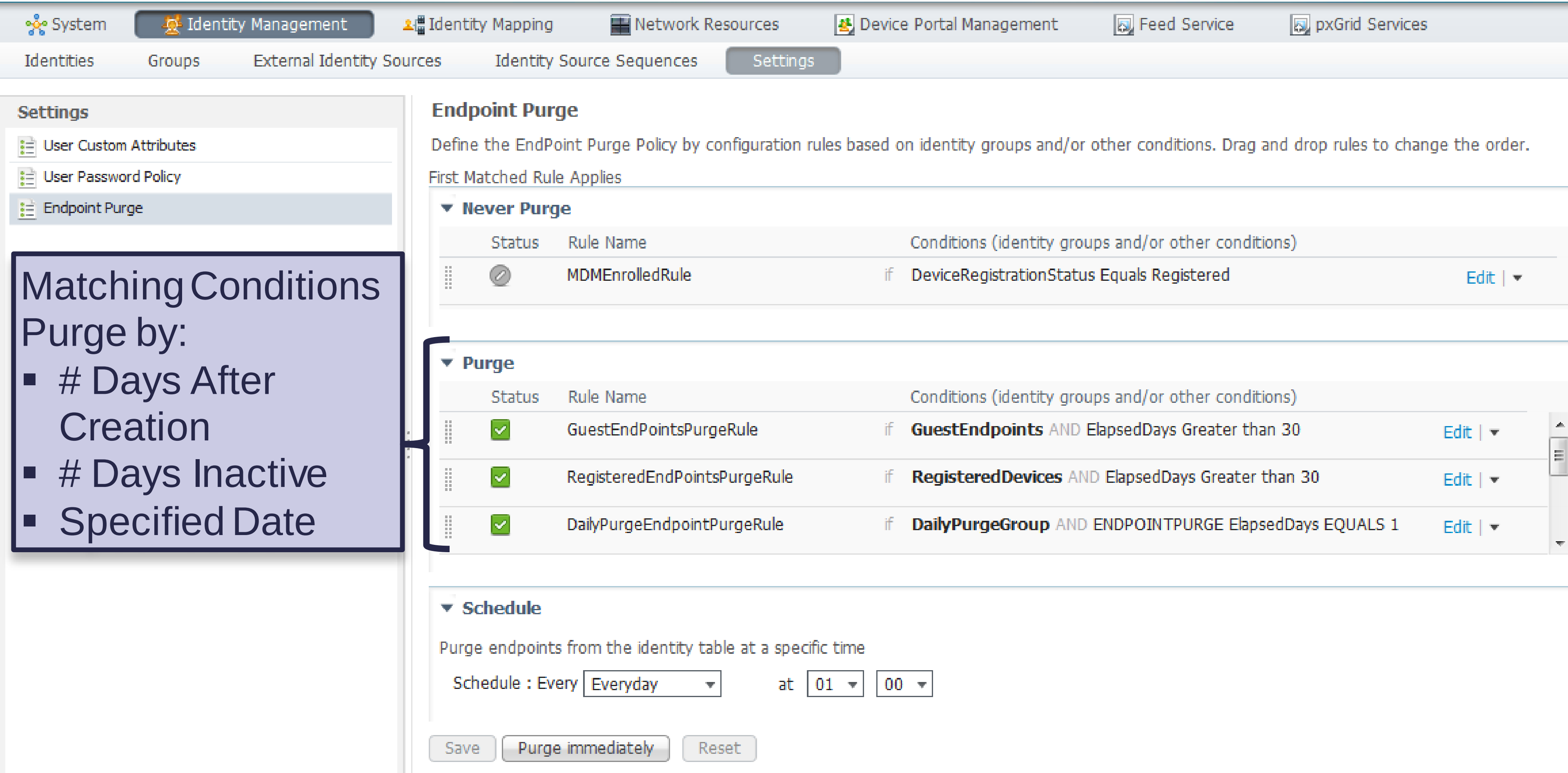
□ Allow guest to bypass the Guest portal

- Web Authenticated users can be auto-registered and endpoints auto-purged.
- Allows re-auth to be reduced to one day, multiple days, weeks, etc.
- Improves Web Scaling and User Experience

Store device information in endpoint identity group: GuestEndpoints

Purge endpoints in this identity group when they reach 7 days old

Endpoint Purging



Matching Conditions Purge by:

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

Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Never Purge

Status	Rule Name		Conditions (identity groups and/or other conditions)
⊘	MDMEnrolledRule	if	DeviceRegistrationStatus Equals Registered

Purge

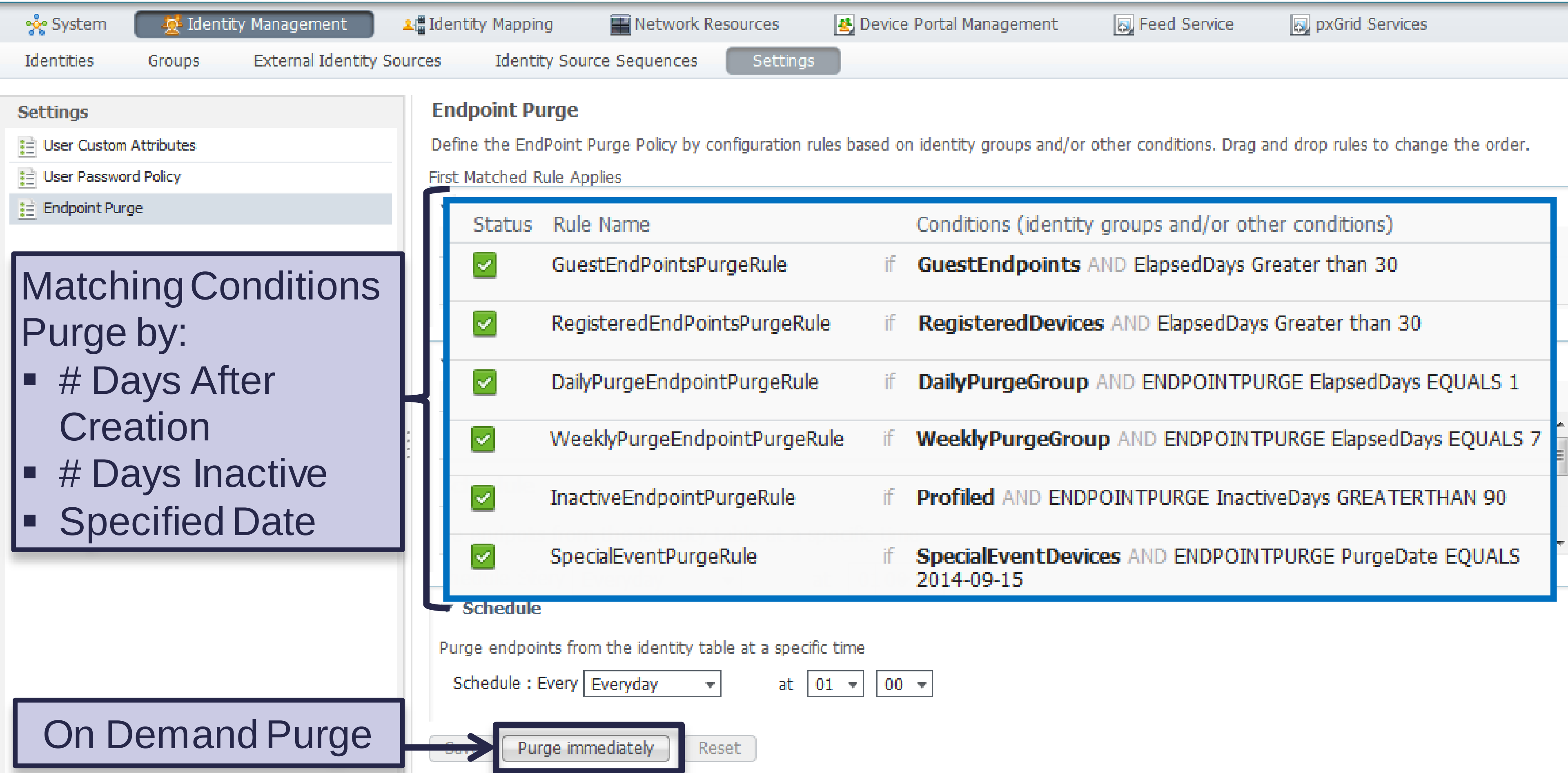
Status	Rule Name		Conditions (identity groups and/or other conditions)
✓	GuestEndPointsPurgeRule	if	**GuestEndpoints** AND ElapsedDays Greater than 30
✓	RegisteredEndPointsPurgeRule	if	**RegisteredDevices** AND ElapsedDays Greater than 30
✓	DailyPurgeEndpointPurgeRule	if	**DailyPurgeGroup** AND ENDPOINTPURGE ElapsedDays EQUALS 1

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every Everyday at 01 00

Endpoint Purging Examples



Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name		Conditions (identity groups and/or other conditions)
✓	GuestEndPointsPurgeRule	if	**GuestEndpoints** AND ElapsedDays Greater than 30
✓	RegisteredEndPointsPurgeRule	if	**RegisteredDevices** AND ElapsedDays Greater than 30
✓	DailyPurgeEndpointPurgeRule	if	**DailyPurgeGroup** AND ENDPOINTPURGE ElapsedDays EQUALS 1
✓	WeeklyPurgeEndpointPurgeRule	if	**WeeklyPurgeGroup** AND ENDPOINTPURGE ElapsedDays EQUALS 7
✓	InactiveEndpointPurgeRule	if	**Profiled** AND ENDPOINTPURGE InactiveDays GREATERTHAN 90
✓	SpecialEventPurgeRule	if	**SpecialEventDevices** AND ENDPOINTPURGE PurgeDate EQUALS 2014-09-15

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every Everyday at 01 00

Matching Conditions Purge by:

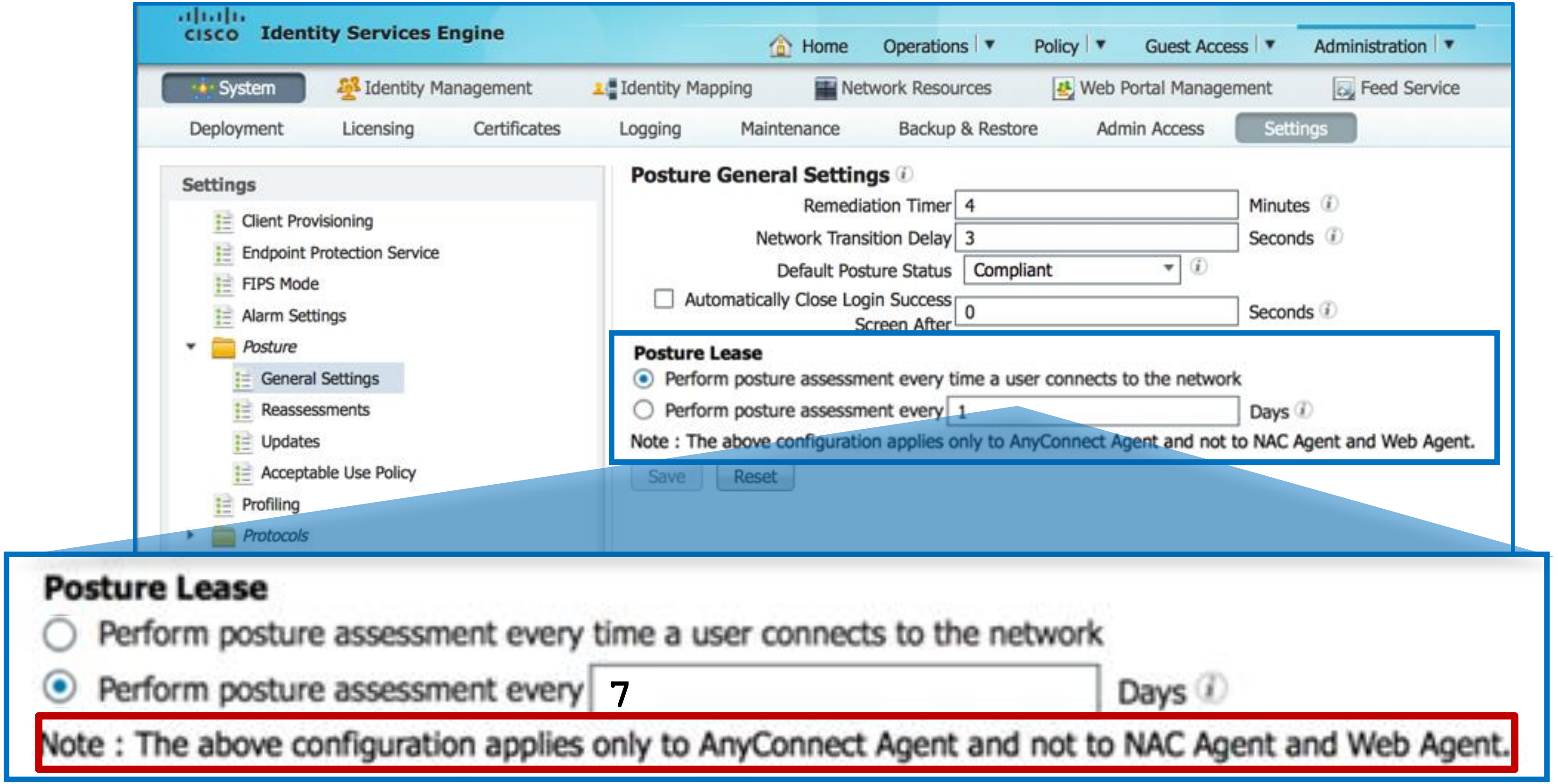
- # Days After Creation
- # Days Inactive
- Specified Date

On Demand Purge

Scaling Posture and MDM

Posture Lease

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



Posture General Settings

Remediation Timer: 4 Minutes

Network Transition Delay: 3 Seconds

Default Posture Status: Compliant ▾

□ Automatically Close Login Success Screen After: 0 Seconds

Posture Lease

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

○ Perform posture assessment every 1 Days

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

Posture Lease

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

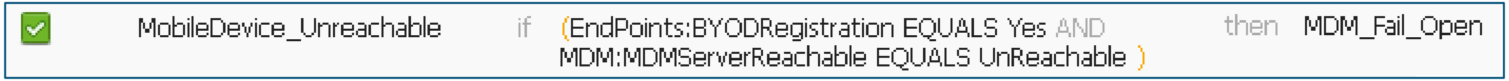
● Perform posture assessment every 7 Days

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

MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

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



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

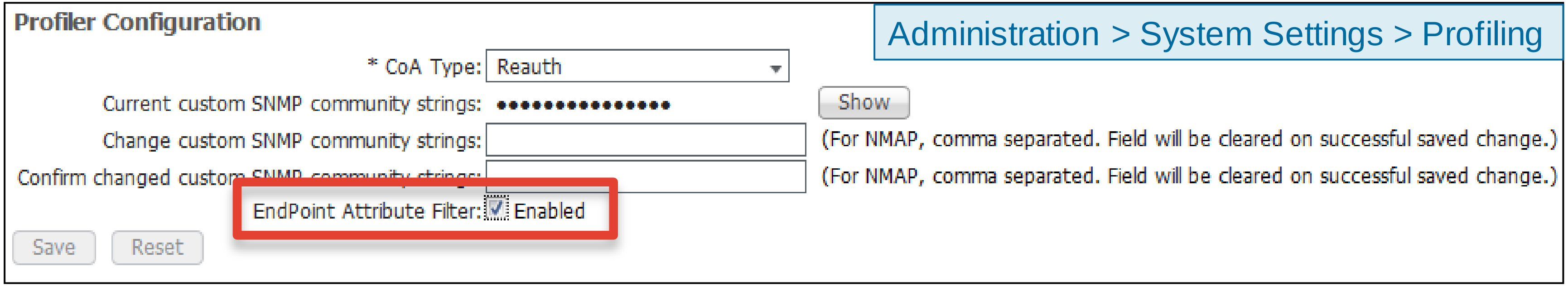
  - All attributes retrieved & reachability determined by single API call on each new session.
- Separate Heartbeat timer added to current 1.2.x and 1.3.0
  - CSCul39011 MDM client is not rejecting queries when MDM server is not responding

Scaling Profiling and Database Replication

Profiling Whitelist Filter

Reduces Data Collection and Replication to Critical (aka Significant) Attributes

- Endpoint Attribute Filter – aka "Whitelist filter" (ISE 1.1.2 and above)
  - Disabled by default. If enabled, only these attributes are collected or replicated.



Profiler Configuration

Administration > System Settings > Profiling

* CoA Type: Reauth

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

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

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

EndPoint Attribute Filter: ☑ Enabled

- 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.

Distributed Deployments – ISE 1

Database Architectural and Replication Model Changes

- Database replication changes from queue-based to message-based transport.
  - No longer uses ping-pong ACK mechanism to replicate data; sends stream of updates until get NAK.
- Conversion to Entity Definition Framework (EDF)
  - Changes from hierarchical Entity-Attribute-Value model to relational database model for significant read-write improvements.
- Move to 64-bit OS
  - Helps to improve performance by making use of larger memory.
- Local Persistence for Profiler DB.
  - Only update PAN for **Significant Attributes**
  - "EndPoint Profiler Server" owns endpoint. If another PSN receives attributes, then requests sync of attributes from prior owner.
  - PAN receives all updates on significant attribute change as fallback.

MAC ADDRESS
ENDPOINT POLICY
STATIC ASSIGNMENT
STATIC GROUP ASSIGNMENT
ENDPOINT IP
POLICY VERSION
MATCHED VALUE (CF)
NMAP SUBNET SCAN ID
PORTAL USER
DEVICE REGISTRATION STATUS

CSCur44879 - Remove IP address as Significant Attribute

Significant Attributes vs. Whitelist Attributes

Updates
Node Group

Significant Attributes

- Change triggers global replication

MACADDRESS
~~ENDPOINTIP~~
MATCHEDVALUE
ENDPOINTPOLICY
ENDPOINTPOLICYVERSION
STATICASSIGNMENT
STATICGROUPASSIGNMENT
NMAPSUBNETSCANID
PORTALUSER
DEVICEREGISTRATIONSTATUS

Updates
Deployment

Whitelist Attributes

- Change triggers PSN-PSN replication and global *ownership* change

Other Attributes

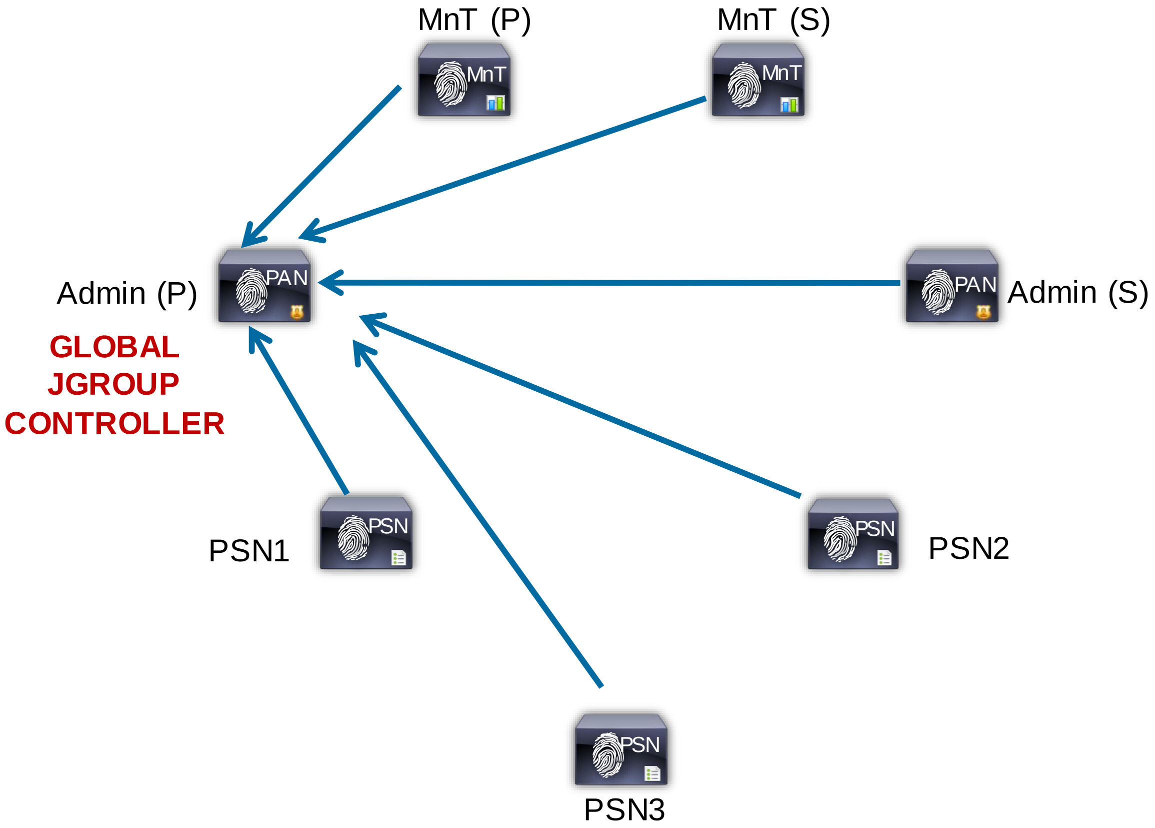
- Dropped if whitelist filter enabled; Otherwise, only locally saved by PSN

Attributes that impact profile

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
MDMPinLockSet
MDMProvider
MDMSerialNumber
MDMServerReachable
MDMUpdateTime
NADAddress
NAS-IP-Address
NAS-Port-Id
NAS-Port-Type
NmapScanCount
NmapSubnetScanID
operating-system
OS Version
OUI
PhoneID
PhoneIDType
PolicyVersion
PortalUser
PostureApplicable
PreviousDeviceRegistrationStatus
Product
RegistrationTimeStamp
StaticAssignment
StaticGroupAssignment
sysDescr
TimeToProfile
Total Certainty Factor
UpdateTime
User-Agent

Inter-Node Communications

JGroup Connections – Global Cluster



▬ TCP/12001 JGroups Tunneled

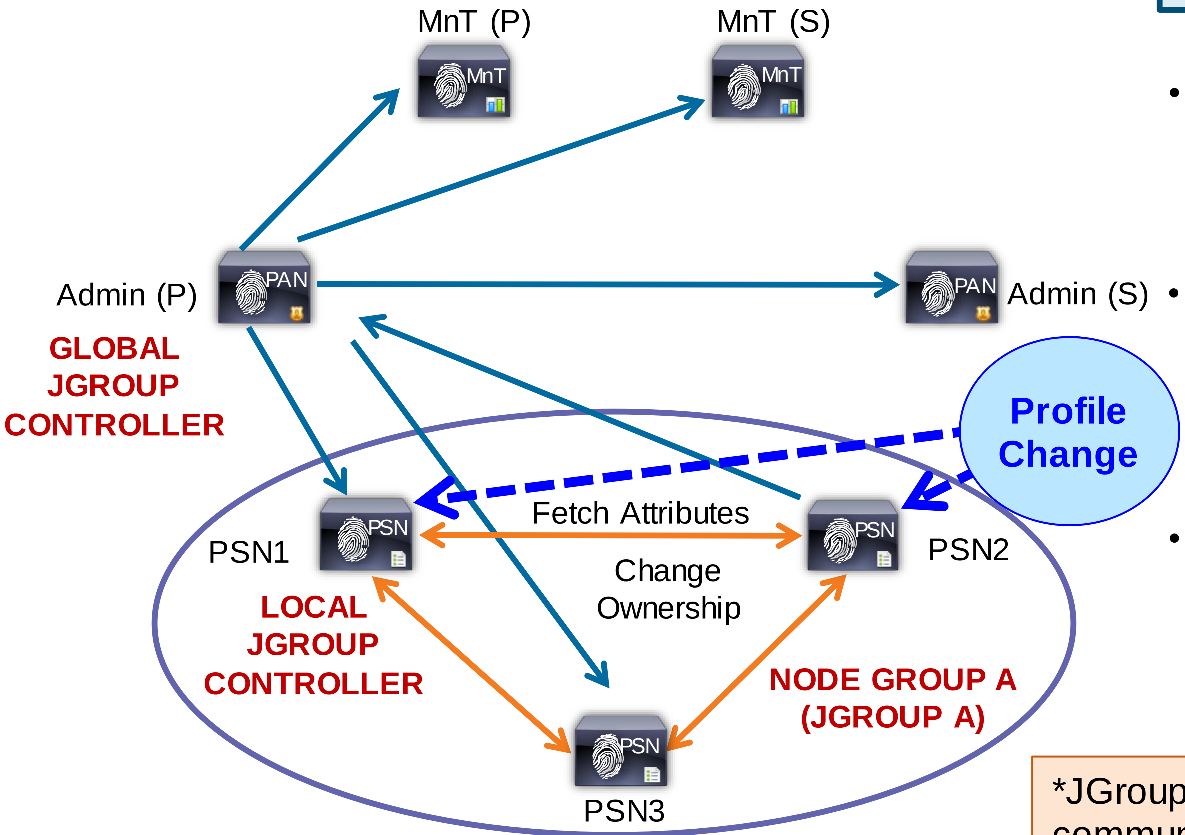
- All Secondary nodes* establish connection to Primary PAN (JGroup Controller) over tunneled connection (TCP/12001) for config/database sync.
- Secondary Admin also listens on TCP/12001 but no connection established unless primary fails/secondary promoted
- All Secondary nodes participate in the Global JGroup cluster.

***Secondary node** = All nodes except Primary Admin node; includes PSNs, MnT and Secondary Admin nodes

Inter-Node Communications

Local JGroups and Node Groups

🟧	TCP/7800 JGroup Peer Communication TCP/7802 JGroup Failure Detection
🟦	TCP/12001 JGroups Tunneled



- Node Groups can be used to define local JGroup* clusters where members exchange heartbeat and sync profile data over IP multicast.
- PSN claims endpoint ownership only if change in whitelist attribute; triggers inter-PSN sync of attributes. Whitelist check always occurs regardless of global attribute filter setting.
- Replication to PAN occurs if significant attribute changes, then sync all attributes via PAN; if whitelist filter enabled, only whitelist attributes synced to all nodes.

*JGroups: Java toolkit for reliable multicast communications between group/cluster members.

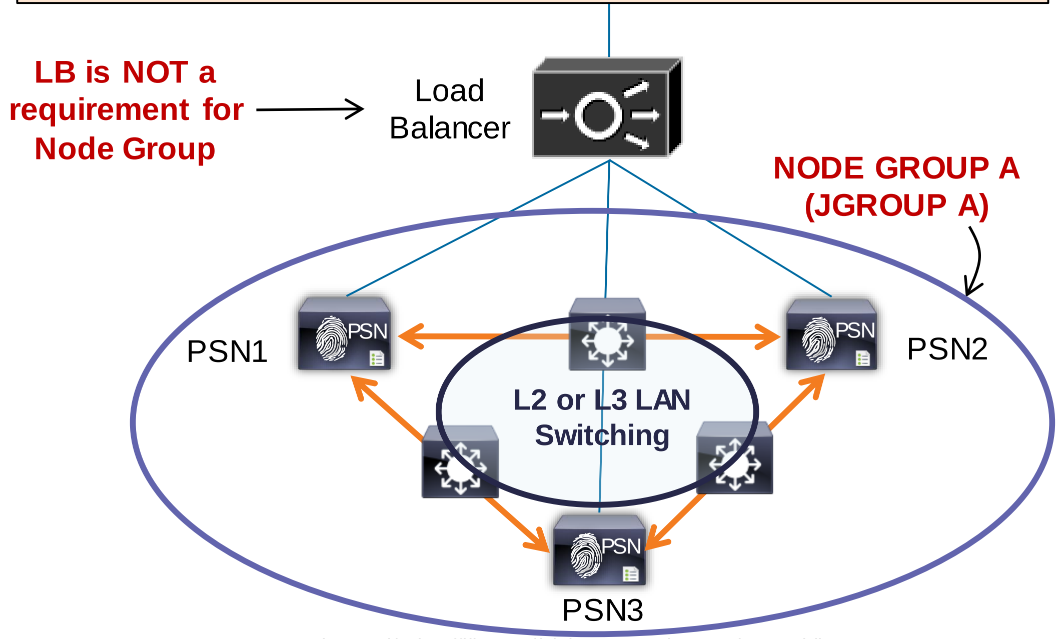
Inter-Node Communications

Local JGroups and Node Groups

🟧 TCP/7800 JGroup Peer Communication
TCP/7802 JGroup Failure Detection

🟦 TCP/12001 JGroups Tunneled

- General classification data for given endpoint should stay local to node group = **whitelist attributes**
- Only certain critical data needs to be shared across entire deployment = **significant attributes**


LB is NOT a requirement for Node Group

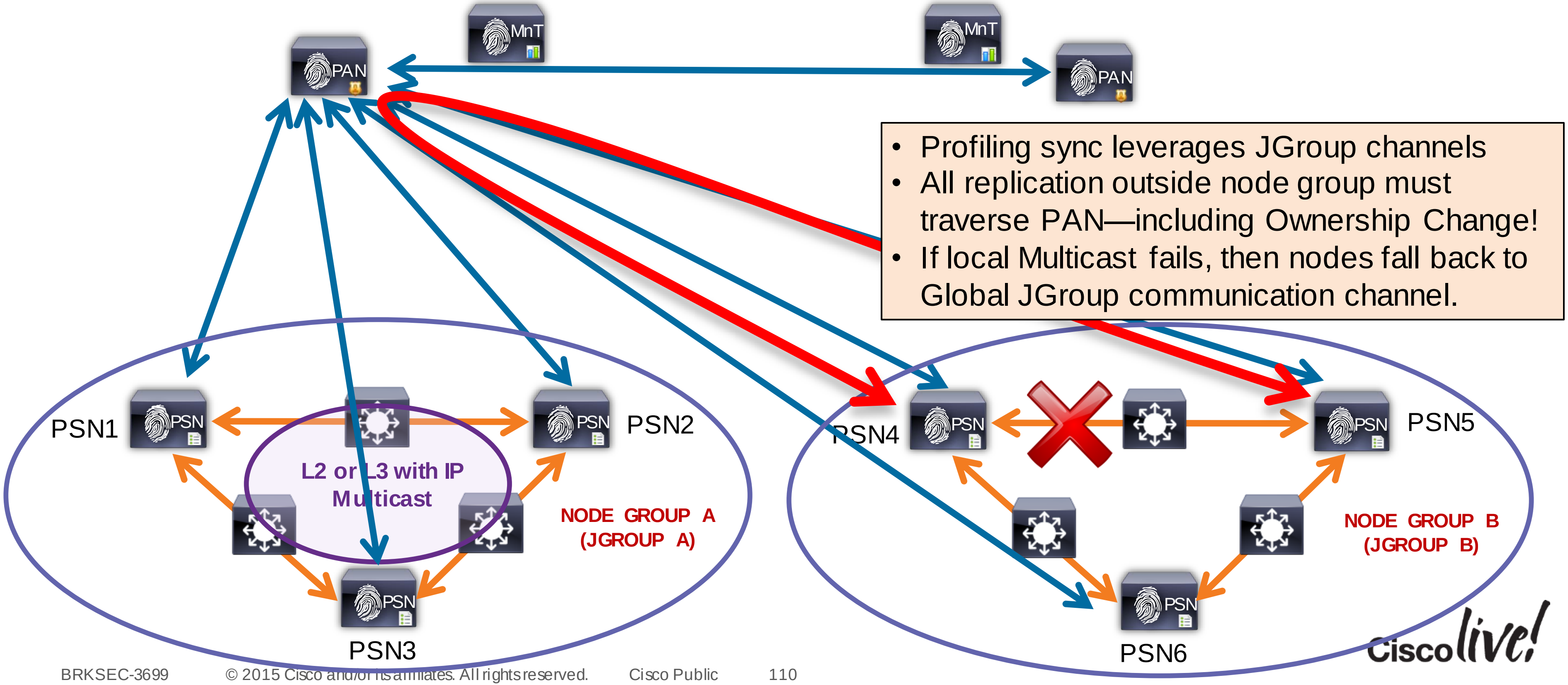
NODE GROUP A (JGROUP A)

- Node groups continue to provide original function of session recovery for failed PSN.
- Profiling sync leverages JGroup channel
- Each LB cluster should be a node group, but LB is NOT required for node groups.
- Node group members should have GE LAN connectivity (L2 or L3)
  - ISE 1.3 no longer uses UDP multicast for Jgroup—uses SSL only.
  - ISE 1.2 uses multicast with TTL=2; max 1 hop)
- Reduces sync updates even if different PSNs receive data – expect few whitelist changes and even fewer critical attribute changes.

Inter-Node Communications

Local JGroups and Node Groups

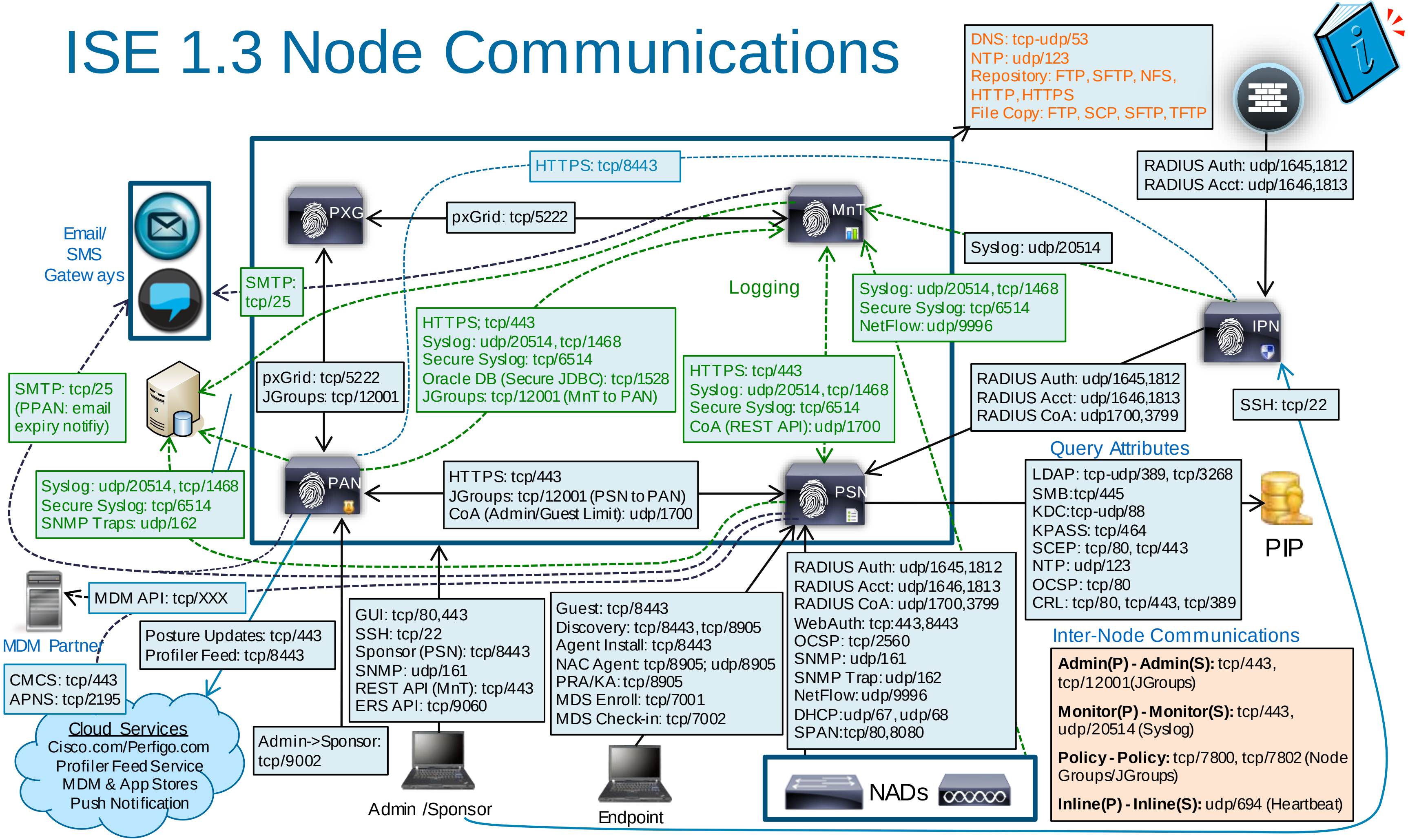
- 🟧 TCP/7800 JGroup Peer Communication
TCP/7802 JGroup Failure Detection
- 🟦 TCP/12001 JGroups Tunneled



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

ISE 1.3 Node Communications

For Your Reference



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

HTTPS: tcp/8443

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813

pxGrid: tcp/5222

Syslog: udp/20514

SMTP: tcp/25

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
NetFlow: udp/9996

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

pxGrid: tcp/5222
JGroups: tcp/12001

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

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

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813
RADIUS CoA: udp1700,3799

SSH: tcp/22

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

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

Query Attributes

LDAP: tcp-udp/389, tcp/3268
SMB:tcp/445
KDC:tcp-udp/88
KPASS: tcp/464
SCEP: tcp/80, tcp/443
NTP: udp/123
OCSP: tcp/80
CRL: tcp/80, tcp/443, tcp/389

MDM API: tcp/XXX

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

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

Guest: tcp/8443
Discovery: tcp/8443, tcp/8905
Agent Install: tcp/8443
NAC Agent tcp/8905; udp/8905
PRA/KA: tcp/8905
MDS Enroll: tcp/7001
MDS Check-in: tcp/7002

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813
RADIUS CoA: udp/1700,3799
WebAuth: tcp:443,8443
OCSP: tcp/2560
SNMP: udp/161
SNMP Trap: udp/162
NetFlow: udp/9996
DHCP:udp/67, udp/68
SPAN:tcp/80,8080

CMCS: tcp/443
APNS: tcp/2195

Admin->Sponsor: tcp/9002

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

Inter-Node Communications

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

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

Policy - Policy: tcp/7800, tcp/7802 (Node Groups/JGroups)

Inline(P) - Inline(S): udp/694 (Heartbeat)

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. If used, make sure probe captures traffic to central DHCP Server. HA challenges.

Do NOT enable all probes by default !

Avoid SPAN, SNMP Traps, and NetFlow probes !

- **SNMP Probe:**
  - Be careful of high SNMP traffic due to triggered RADIUS Accounting updates as a result of high re-auth (low session/re-auth timers) or frequent interim accounting updates.
  - 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 centralized deployments—Potential for high load on network devices and ISE.

Profiling Case Study

ISE 1.1.1 Patch 2 initially helped, but…
Never applied other best practice recommendations.
DB eventually filled and purge issues resulted in DBs falling out of sync / disconnects.

Problem:

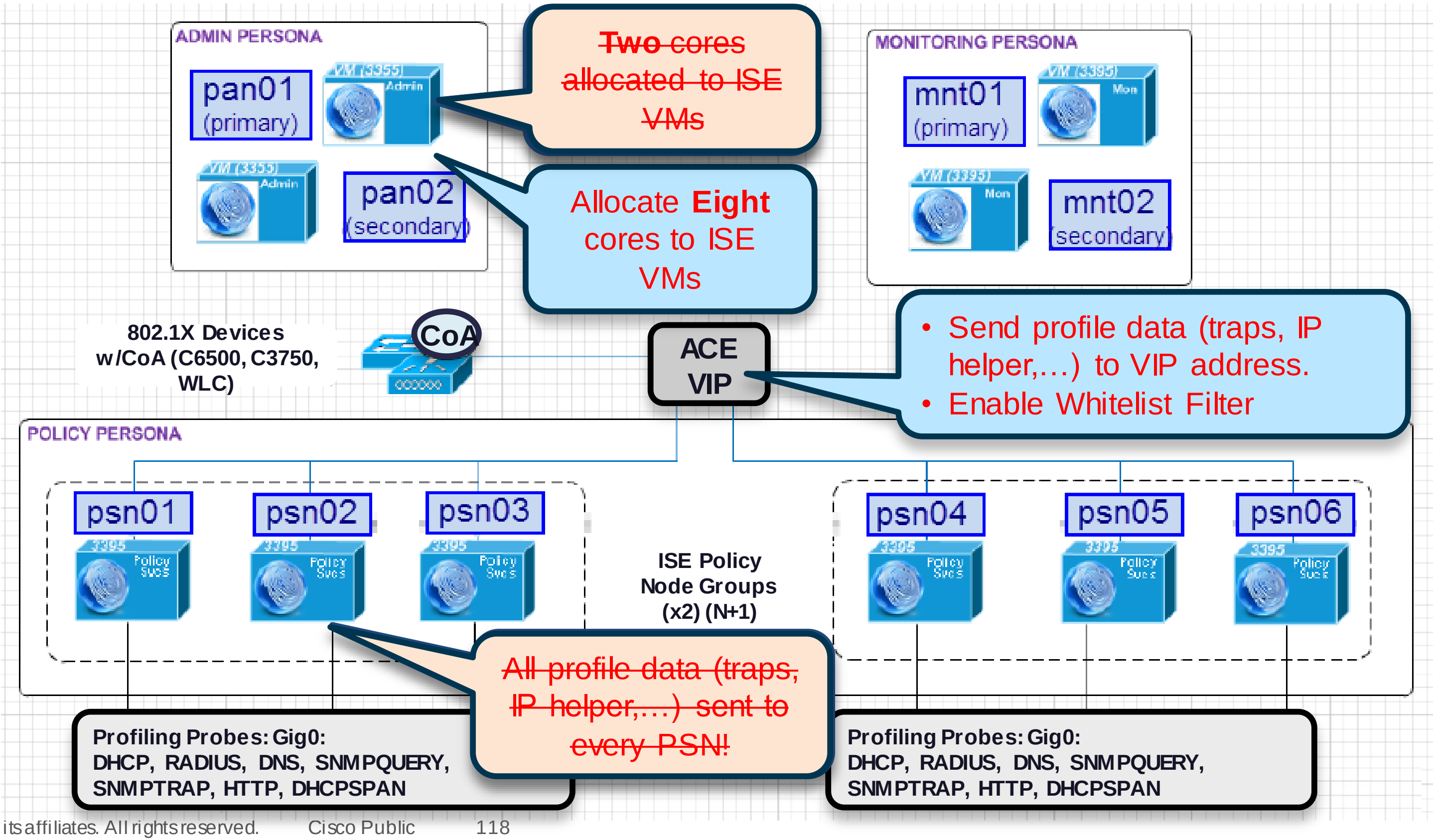
- Running ISE 1.1.1
- High node CPU and BW to Primary PAN
- Short-term Fix = Disable Profiling

Interim Solution:

- Added 2nd core and CPU dropped 33%
- Applied 1.1.1 Patch 2 and CPU dropped 85+% and BW 98+%

Solution:

- Increase VM to specs
- LB profile data to single IP
- Enable whitelist filter
- Upgrade to 1.2.1/1.3



~~Two cores allocated to ISE VMs~~

Allocate **Eight** cores to ISE VMs

- Send profile data (traps, IP helper,…) to VIP address.
- Enable Whitelist Filter

~~All profile data (traps, IP helper,…) sent to every PSN!~~

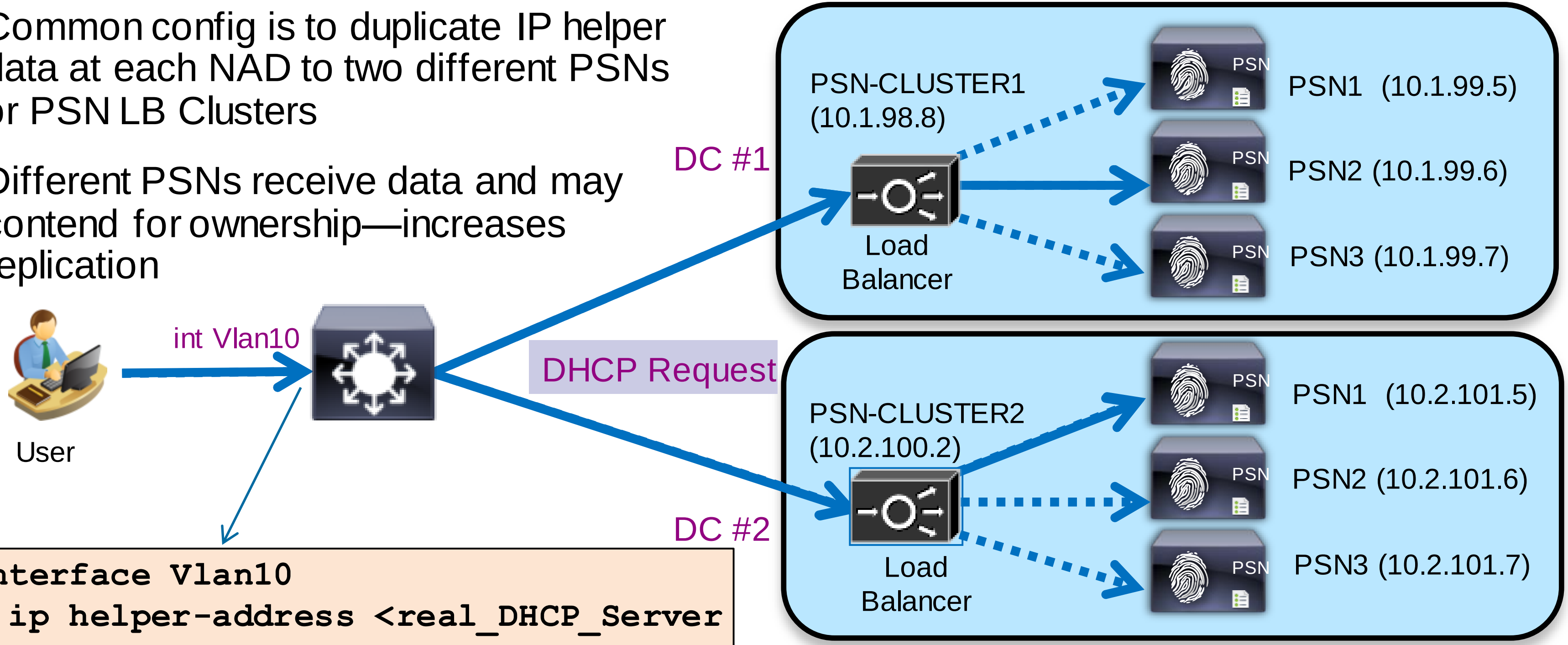
Profiling Probes: Gig0: DHCP, RADIUS, DNS, SNMPQUERY, SNMPTRAP, HTTP, DHCPSPAN

Profiling Probes: Gig0: DHCP, RADIUS, DNS, SNMPQUERY, SNMPTRAP, HTTP, DHCPSPAN

Profiling Redundancy – Duplicating Profile Data

Sending Profile Data for the Same Endpoint to the Same Node Group / PSN

- Common config is to duplicate IP helper data at each NAD to two different PSNs or PSN LB Clusters
- Different PSNs receive data and may contend for ownership—increases replication

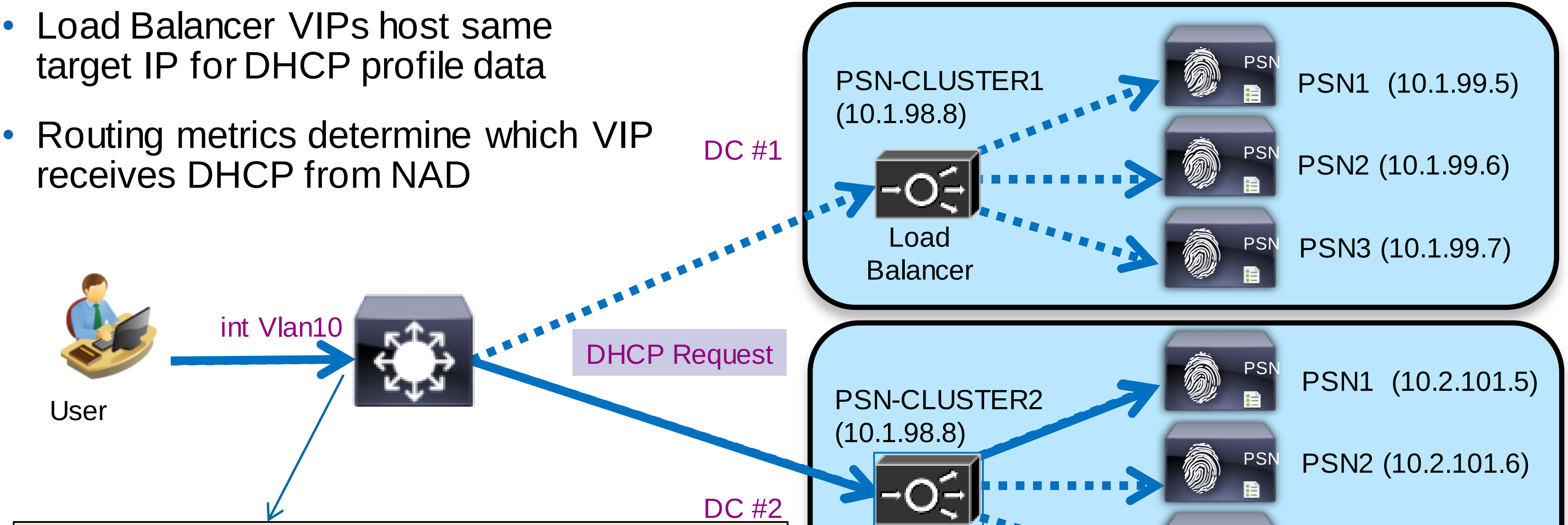


```
interface Vlan10
  ip helper-address <real_DHCP_Server
  ip helper-address 10.1.98.8
  ip helper-address 10.2.100.2
```

Scaling Profiling and Replication

Using Anycast to Limit Profile Data to a Single PSN and Node Group

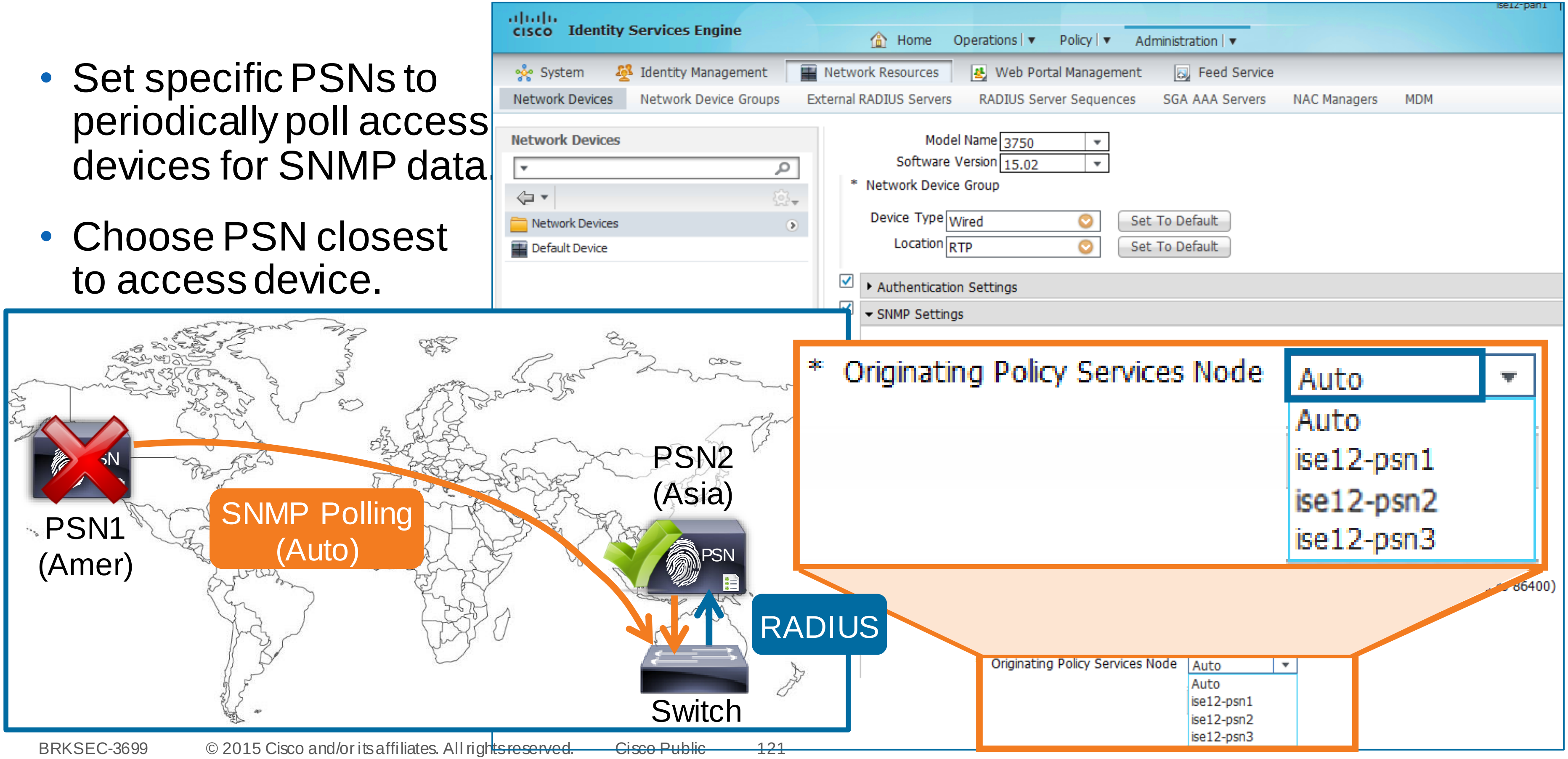
- Load Balancer VIPs host same target IP for DHCP profile data
- Routing metrics determine which VIP receives DHCP from NAD



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

Profiler Tuning for Polled SNMP Query Probe

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



Model Name 3750

Software Version 15.02

* Network Device Group

Device Type Wired

Location RTP

☑ ▸ Authentication Settings

☑ ▾ SNMP Settings

* Originating Policy Services Node: Auto ▾

- Auto
- ise12-psn1
- ise12-psn2
- ise12-psn3

(0 86400)

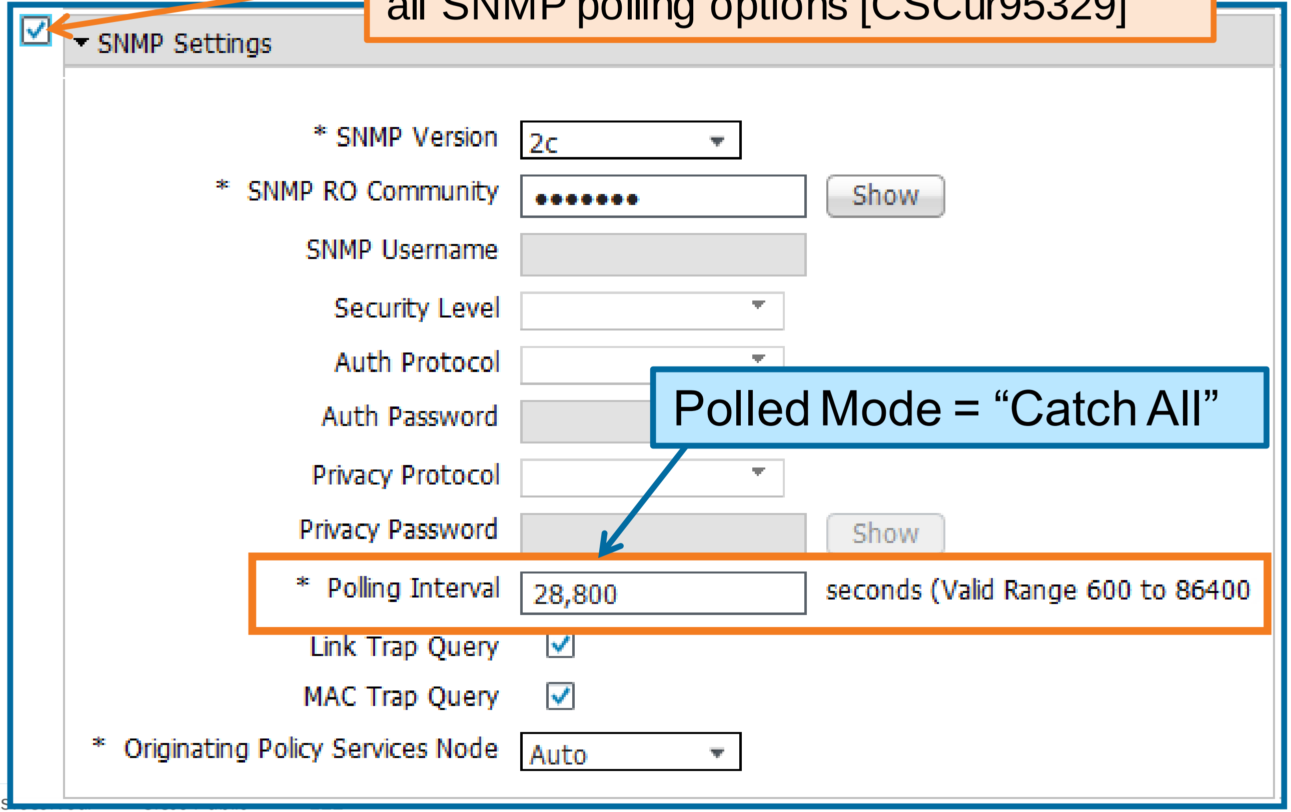
Profiler Tuning for Polled SNMP Query Probe

- Polling Interval

  1.2 Default: 3600 sec (1 hour)

  1.3 Default: 28,800 sec (8 hours) *Recommend minimum

- Setting of “0”: Disables periodic poll but allows triggered & NMAP queries [CSCur95329]
- Triggered query auto-suppressed for 24 hrs per endpoint



Disable/uncheck SNMP Settings: Disables all SNMP polling options [CSCur95329]

Polled Mode = “Catch All”

☑ SNMP Settings

* SNMP Version: 2c

* SNMP RO Community: ••••••• Show

SNMP Username:

Security Level:

Auth Protocol:

Auth Password:

Privacy Protocol:

Privacy Password: Show

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

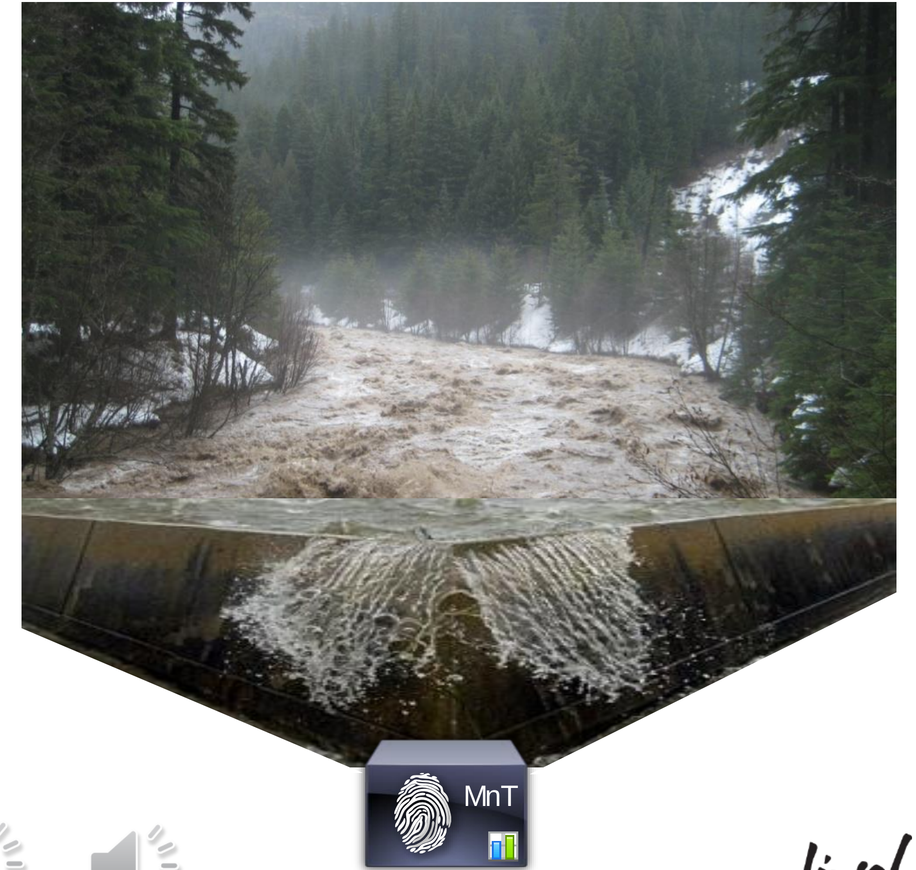
Link Trap Query: ☑

MAC Trap Query: ☑

* Originating Policy Services Node: Auto

Scaling MnT (Optimised Logging and Noise Suppression)

When the Levee Breaks…



"If it keeps on rainin', levee's goin' to break,
When The Levee Breaks *logs* have no place to stay."

*Remix of Led Zeppelin IV, 'When The Levee Breaks'

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.
- Excessive RADIUS health probes from NADs and Load Balancers.
- 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.

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

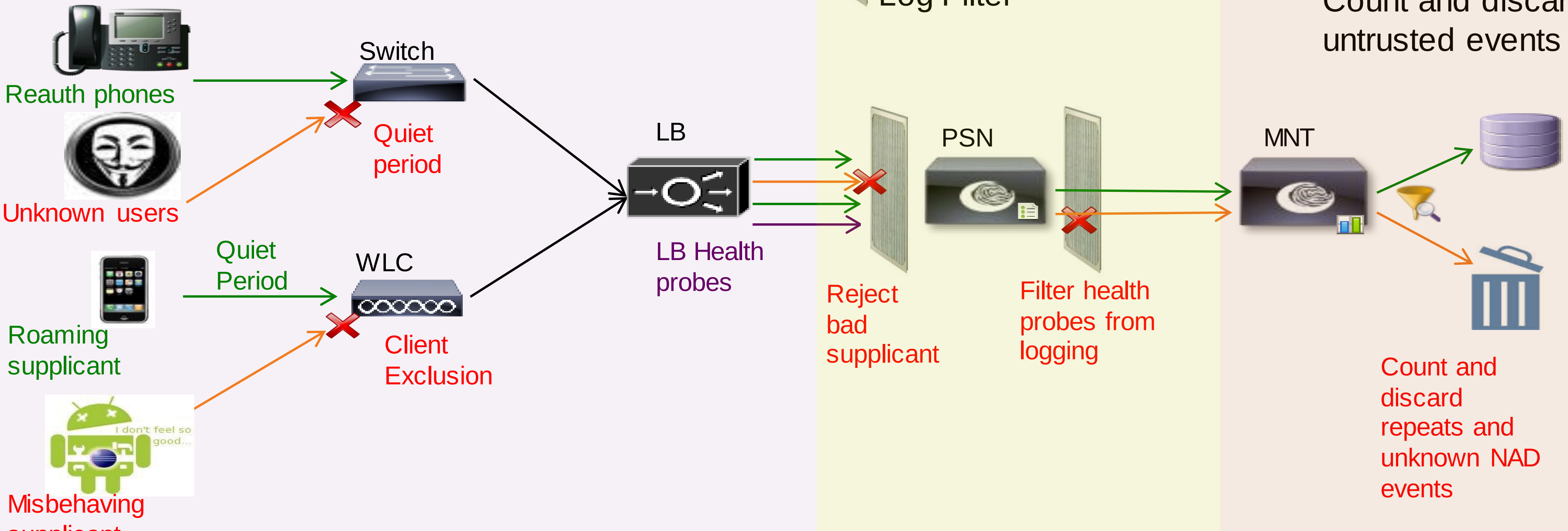
Filtering at Receiving Chain

Detect and reject misbehaving clients

Log Filter

Count and discard repeated events

Count and discard untrusted events



Reauth phones

Switch

Quiet period

Unknown users

Quiet Period

WLC

Client Exclusion

Roaming supplicant

Misbehaving supplicant

LB

LB Health probes

PSN

Reject bad supplicant

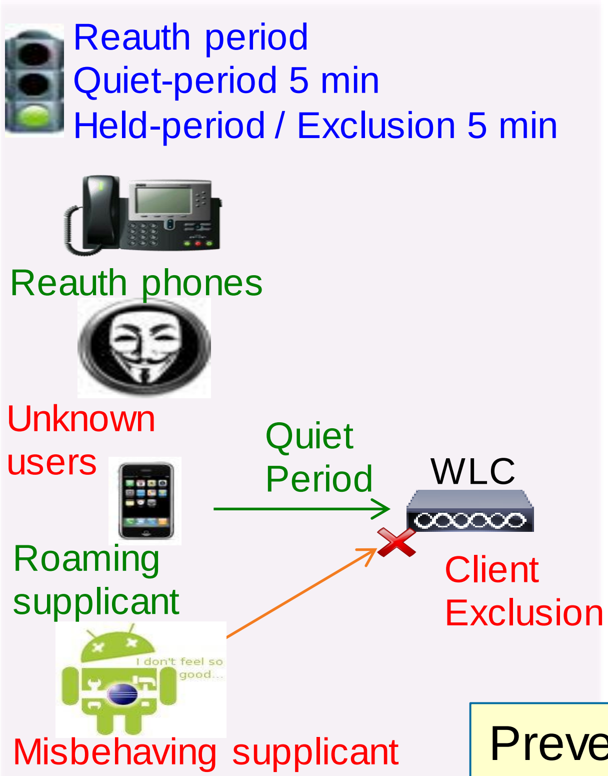
Filter health probes from logging

MNT

Count and discard repeats and unknown NAD events

Tune NAD Configuration

Rate Limiting at **Wireless** Source



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

Reauth phones

Unknown users

Quiet Period

WLC

Roaming supplicant

Client Exclusion

Misbehaving supplicant

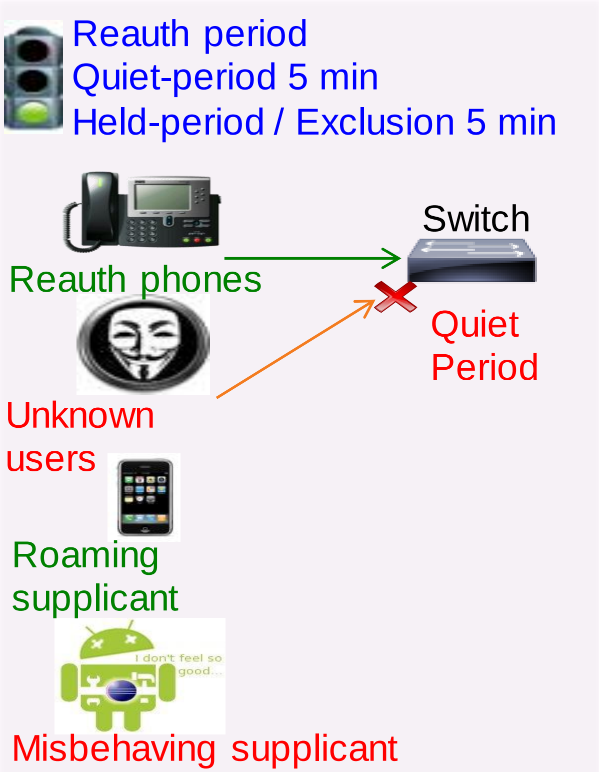
Wireless (WLC)

- **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)
- **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

Tune NAD Configuration (Updated Guidance)

Rate Limiting at **Wired** Source



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

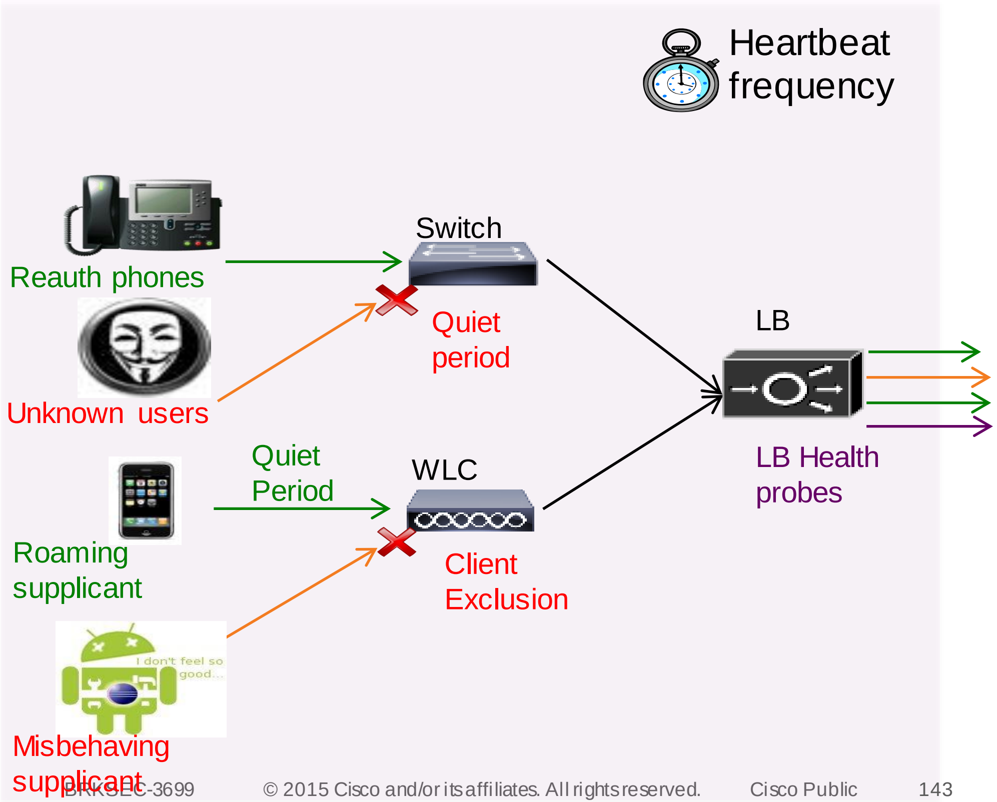
Wired (IOS / IOS-XE)

- **RADIUS Interim Accounting:** Use *newinfo* parameter with long interval (for example, 24 hrs), if available. Otherwise, set 15 mins
- **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.

Load Balancer RADIUS Test Probes

ACE Example

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

    interval *seconds* # Default: 15
  - Retry count for failed probes:

    faildetect *retry_count* # Default: 3
- Sample ACE RADIUS probe configuration:

```
probe radius PSN-PROBE
 port 1812
 interval 20
 faildetect 2
 passdetect interval 90
 credentials radprobe cisco123 secret cisco123
```

- **Recommended setting:** Start with defaults and validate behaviour in specific environment.

F5 Example

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

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

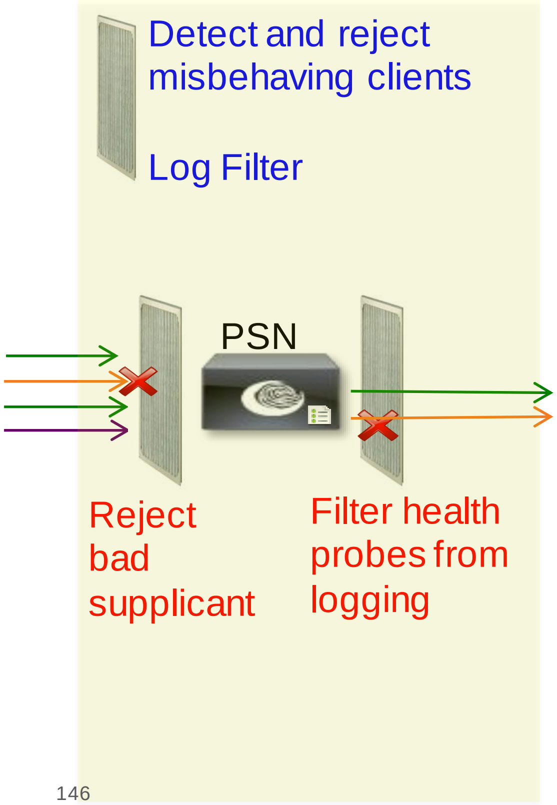
    Timeout *seconds* # Default: 31
- Sample F5 RADIUS probe configuration:

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

PSN Noise Suppression and Smarter Logging

- Filter Noise and Provide Better Feedback on Authentication Issues

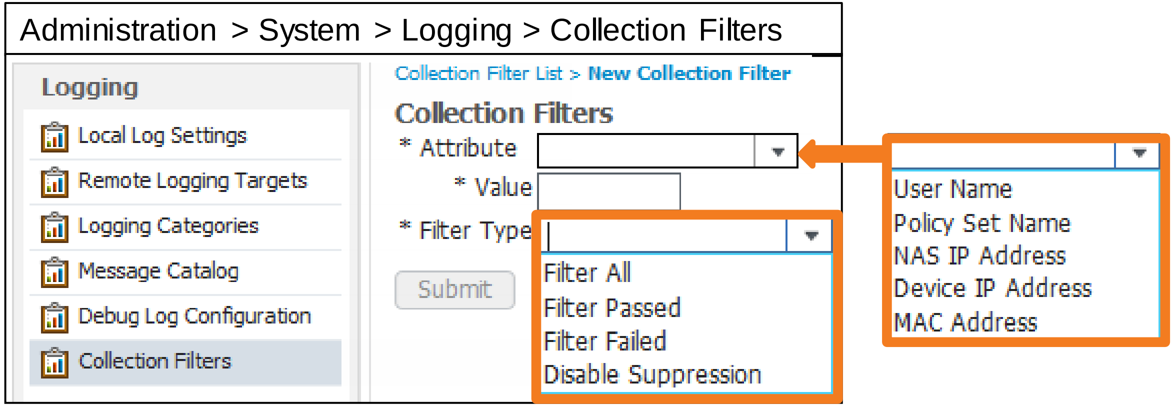
- PSN Collection Filters
- PSN Misconfigured Client Dynamic Detection and Suppression
- PSN Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or Network Access Server (NAS)
- Failure Reason Message and Classification
- Identify RADIUS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


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

PSN - Collection Filters

Static Client Suppression

- PSN static filter based on single attribute:
  - User Name
  - Policy Set Name
  - NAS-IP-Address
  - Device-IP-Address
  - MAC (Calling-Station-ID)
- Filter Messages Based on Auth Result:
  - All (Passed/Fail)
  - All Failed
  - All Passed
- Select Messages to **Disable Suppression** for failed auth @PSN and successful auth @MnT



Administration > System > Logging > Collection Filters

Collection Filters

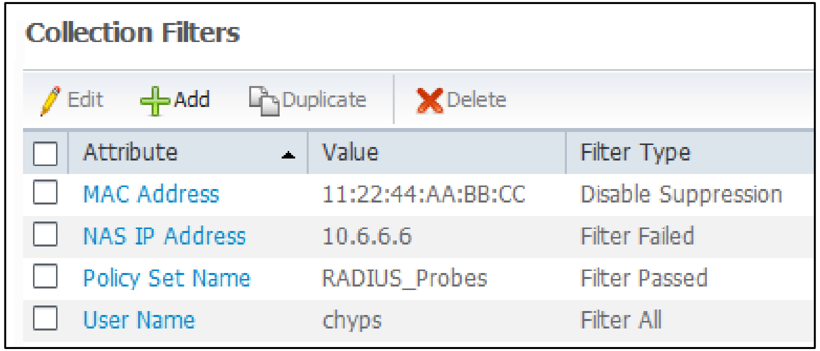
* Attribute

* Value

* Filter Type

Filter All
Filter Passed
Filter Failed
Disable Suppression

User Name
Policy Set Name
NAS IP Address
Device IP Address
MAC Address



Collection Filters

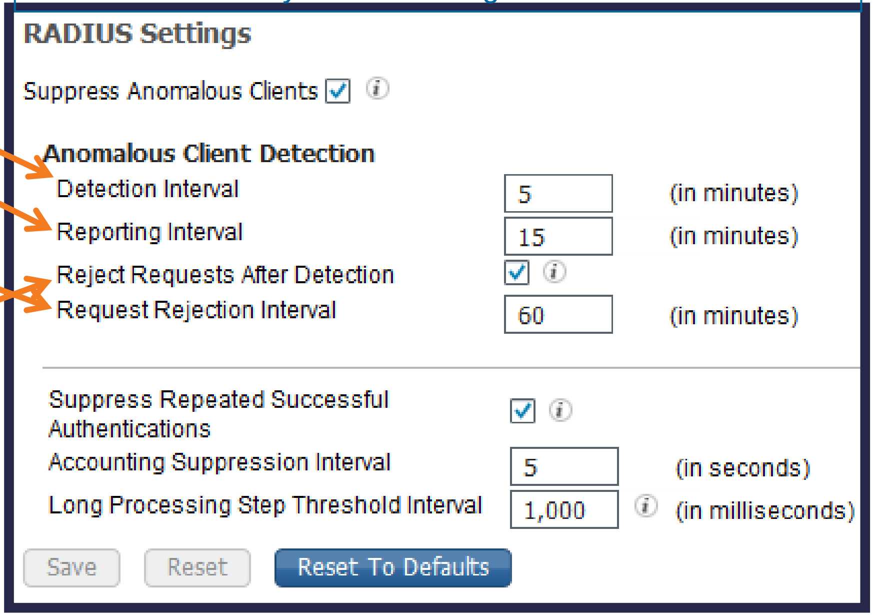
□	Attribute	Value	Filter Type
□	MAC Address	11:22:44:AA:BB:CC	Disable Suppression
□	NAS IP Address	10.6.6.6	Filter Failed
□	Policy Set Name	RADIUS_Probes	Filter Passed
□	User Name	chyps	Filter All

PSN Filtering and Noise Suppression

Misconfigured Client Dynamic Detection and Suppression

- Flag misbehaving supplicants when fail auth more than once per interval
  - Send Alarm with failure stats every interval.
  - Stop sending logs for repeat auth failures for same endpoint during rejection interval.
  - Successful auth clears flag
- Reject matching requests during interval
  - Match these attributes:
    - Supplicant (Calling-Station-ID)
    - NAS (NAS-IP-Address)
    - Failure reason
  - Excludes CoA messages / bad credentials
  - Next request after interval is fully processed.

Administration > System > Settings > Protocols > RADIUS



RADIUS Settings

Suppress Anomalous Clients ☑

Anomalous Client Detection

Detection Interval	5	(in minutes)
Reporting Interval	15	(in minutes)
Reject Requests After Detection	☑	
Request Rejection Interval	60	(in minutes)
Suppress Repeated Successful Authentications	☑	
Accounting Suppression Interval	5	(in seconds)
Long Processing Step Threshold Interval	1,000	(in milliseconds)

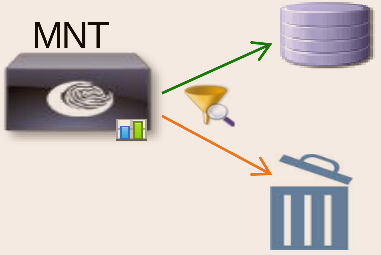
MnT Log Suppression and Smarter Logging

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
- Support larger VM disks to increase logging capacity and retention.

Count and discard repeated events

Count and discard untrusted events



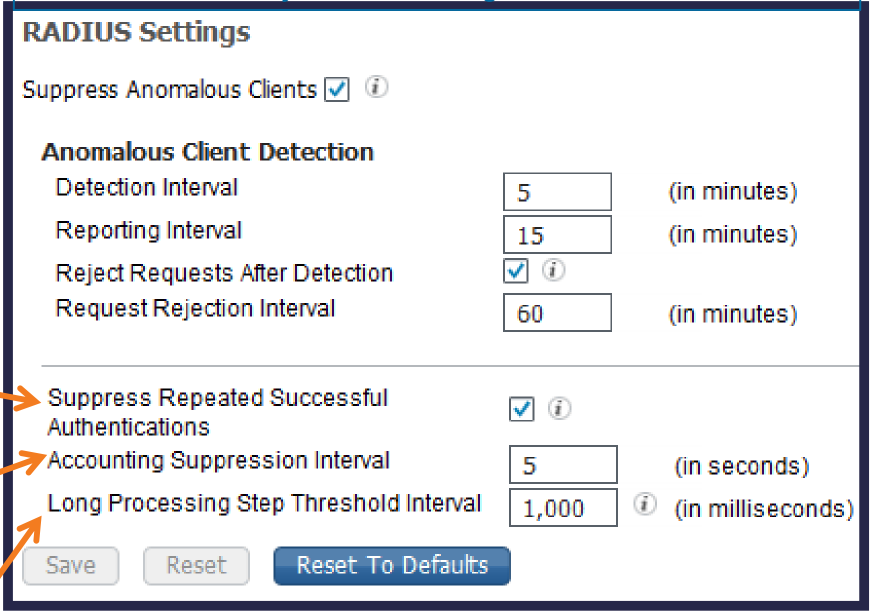
Count and discard repeats and unknown NAD events

MnT Noise Suppression

Suppress Successful Auths and Accounting

- Do not save repeated successful auth events to DB
  (Events will not display in Live Auth log).
- Stop sending Accounting logs for same session during interval.
- Detect and log NAS retransmission timeouts for auth steps that exceed threshold.
  (Step latency is visible in Detailed Live Logs)

Administration > System > Settings > Protocols > RADIUS



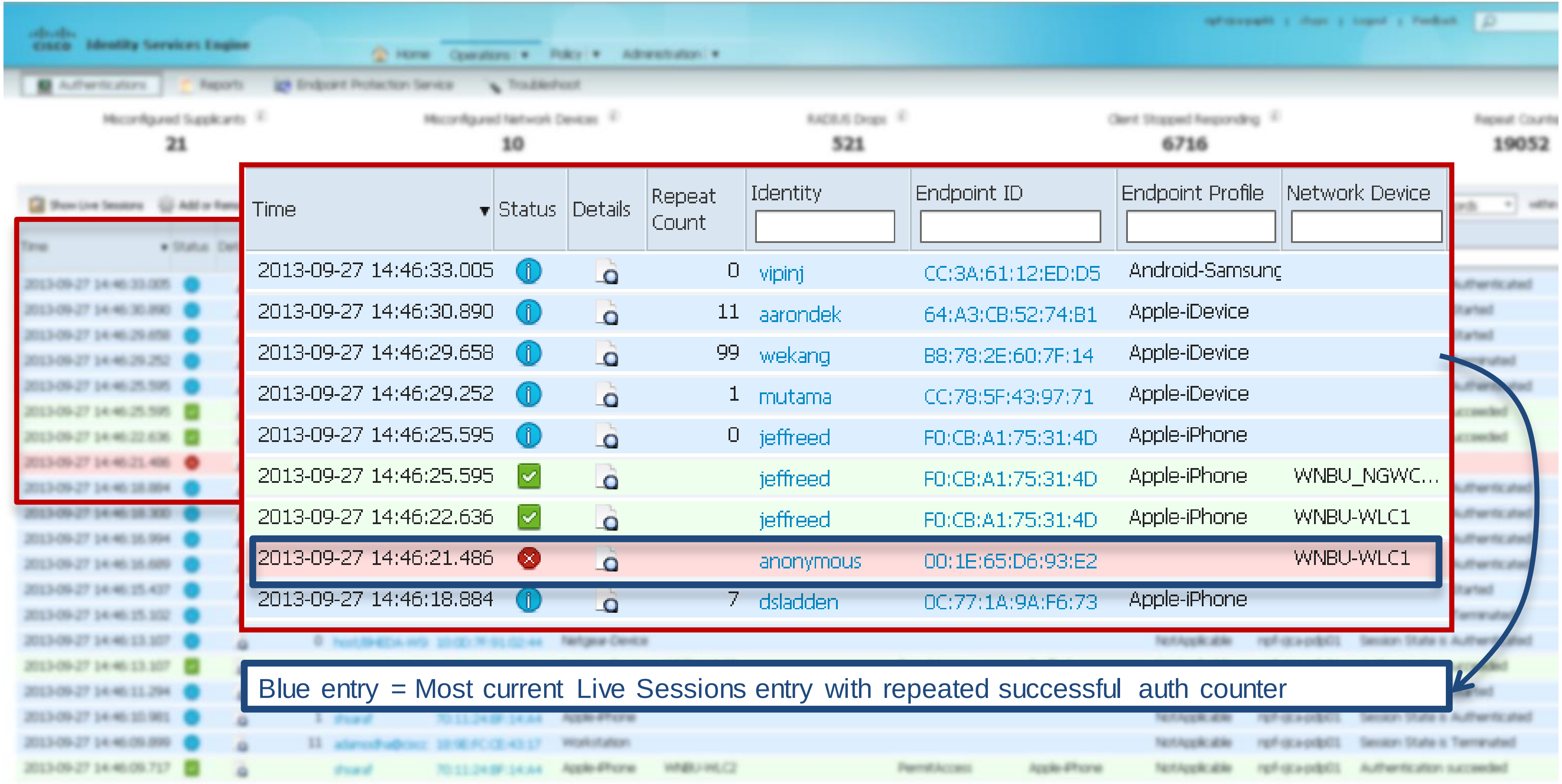
RADIUS Settings

Suppress Anomalous Clients ☑

Anomalous Client Detection

Detection Interval	5	(in minutes)
Reporting Interval	15	(in minutes)
Reject Requests After Detection	☑	
Request Rejection Interval	60	(in minutes)
Suppress Repeated Successful Authentications	☑	
Accounting Suppression Interval	5	(in seconds)
Long Processing Step Threshold Interval	1,000	(in milliseconds)

Live Authentications and Sessions



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

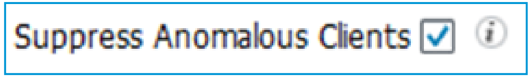
Blue entry = Most current Live Sessions entry with repeated successful auth counter

Authentication Suppression

Enable/Disable

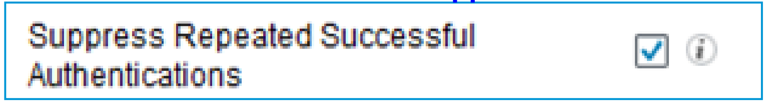
- **Global Suppression Settings:** Administration > System > Settings > Protocols > RADIUS

Failed Auth Suppression



Suppress Anomalous Clients ☑

Successful Auth Suppression



Suppress Repeated Successful Authentications ☑

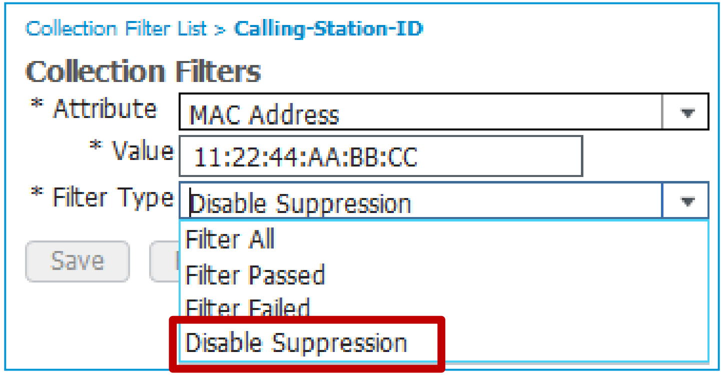
Caution: Do not disable suppression in deployments with very high auth rates.

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

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

Configure specific traffic to bypass Successful Auth Suppression

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



Collection Filter List > Calling-Station-ID

Collection Filters

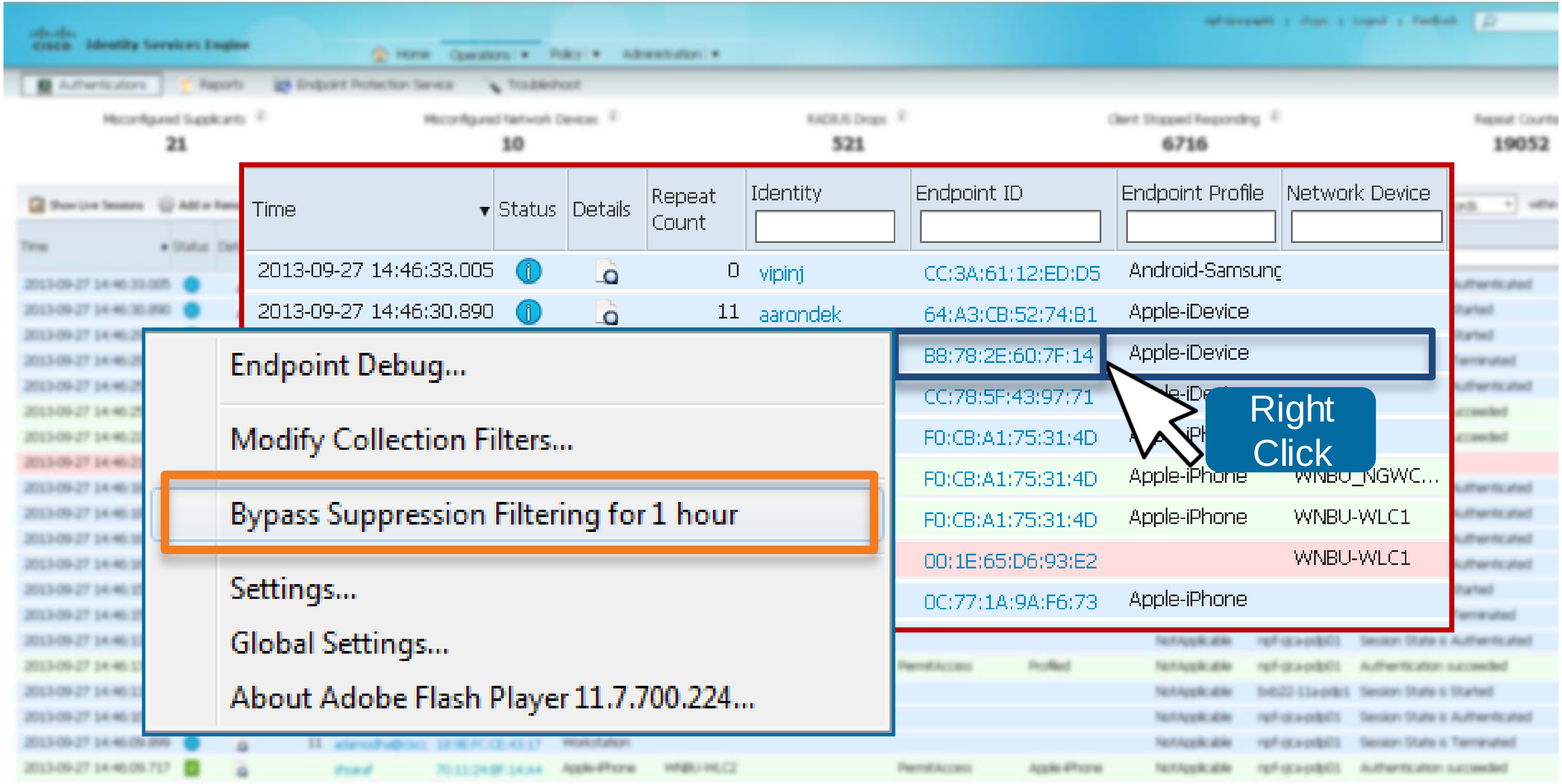
* Attribute: MAC Address

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

* Filter Type: Disable Suppression

Per-Endpoint Time-Constrained Suppression

New in ISE 1.3



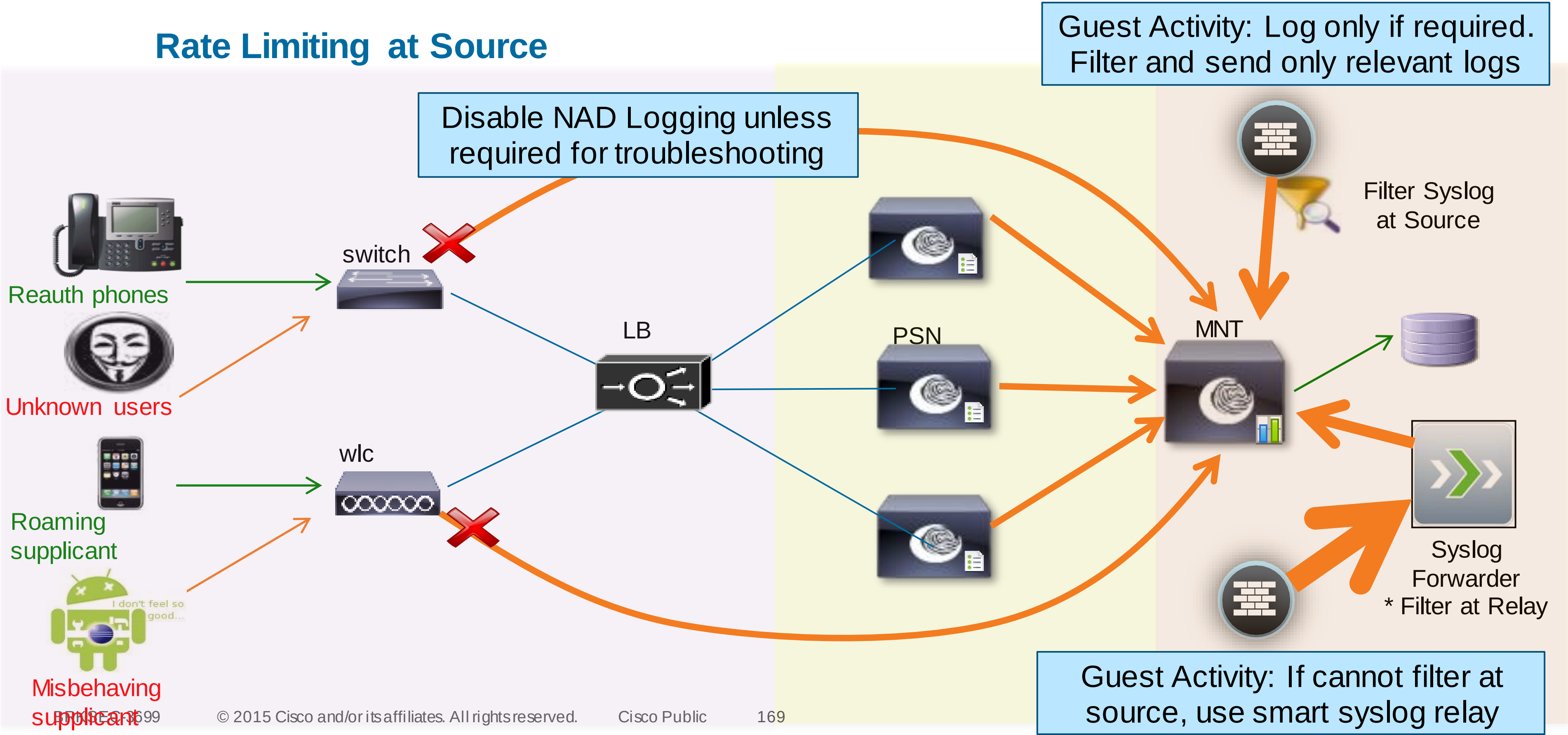
Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	i		0	vipinj	CC:3A:61:12:ED:D5	Android-Samsunç	
2013-09-27 14:46:30.890	i		11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
					B8:78:2E:60:7F:14	Apple-iDevice	
					CC:78:5F:43:97:71	...e-iDe...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

- Endpoint Debug...
- Modify Collection Filters...
- Bypass Suppression Filtering for 1 hour
- Settings...
- Global Settings...
- About Adobe Flash Player 11.7.700.224...

Minimise Syslog Load on MNT

Disable NAD Logging and Filter Guest Activity Logging

Rate Limiting at Source



Disable NAD Logging unless required for troubleshooting

Guest Activity: Log only if required. Filter and send only relevant logs

Guest Activity: If cannot filter at source, use smart syslog relay

- No Log Suppression

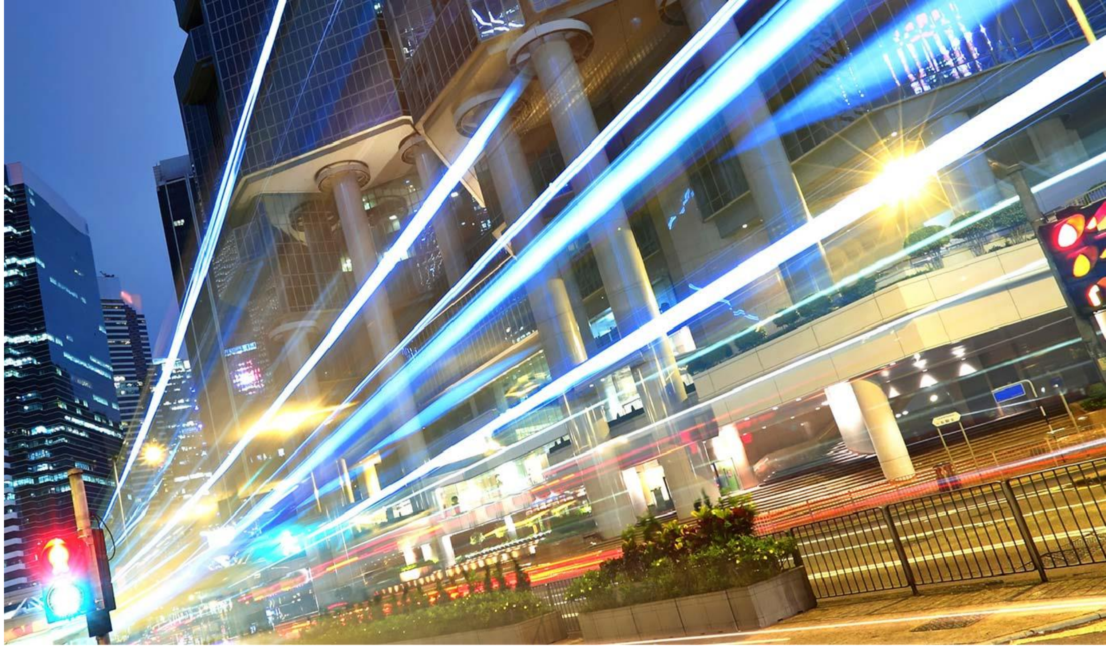
- With Log Suppression

- Distributed Logging

High Availability

High Availability Agenda

- Administration Nodes
- Monitoring Nodes
- pxGrid Nodes
- Inline Posture Nodes
- Policy Service Nodes
  - Load Balancing
  - Non-LB Options
- Network Access Device Fallback and Recovery

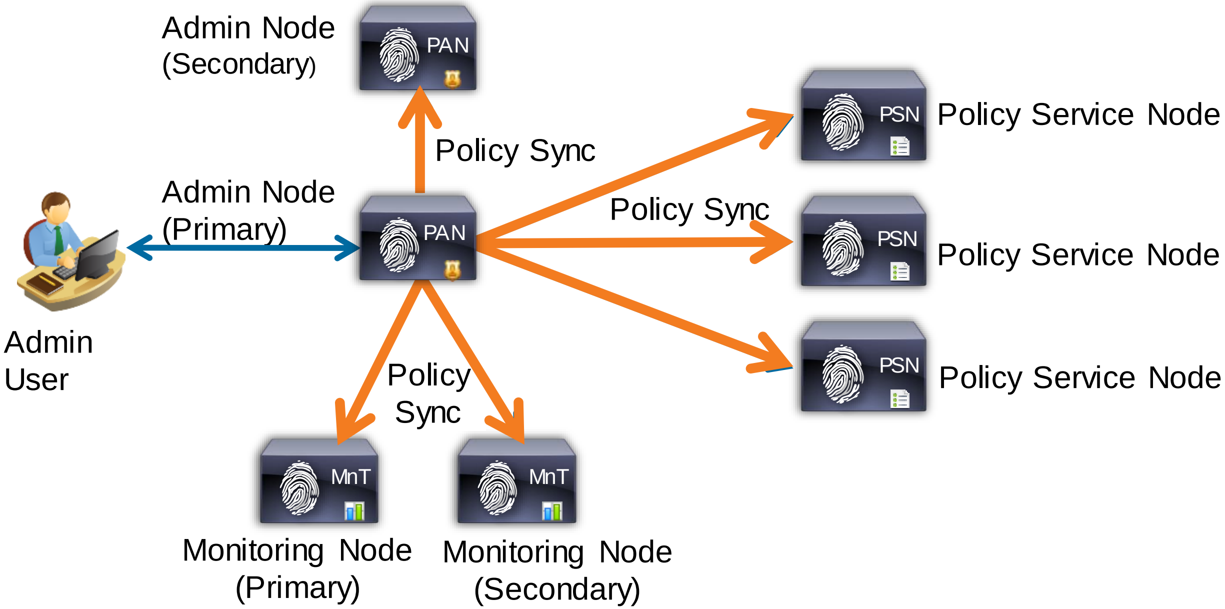


Administration HA and Synchronisation

PAN Steady State Operation

- Maximum two PAN nodes per deployment
- Active / Standby

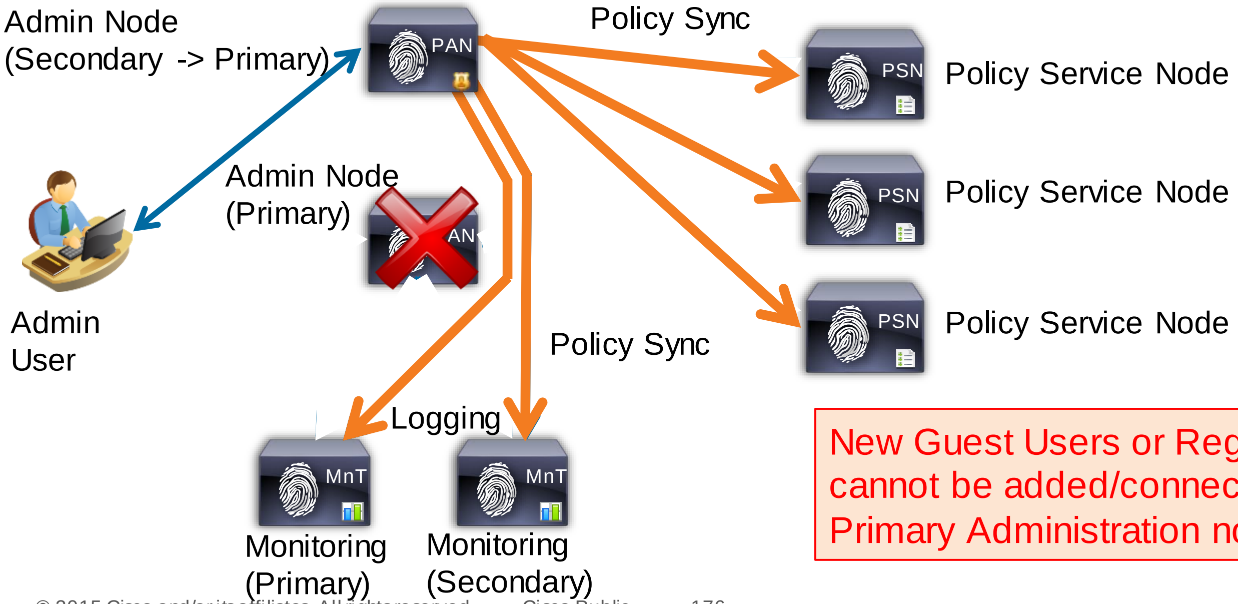
- Changes made to Primary Administration DB are automatically synced to all nodes.



Administration HA and Synchronisation

Primary PAN Outage and Recovery

- Upon Primary PAN failure, admin user must connect to Secondary PAN and manually promote Secondary to Primary; new Primary syncs all new changes.
- PSNs buffer endpoint updates if Primary PAN unavailable; buffered updates sent once PAN available.



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

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

Policy Service Survivability When Admin Down/Unreachable

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

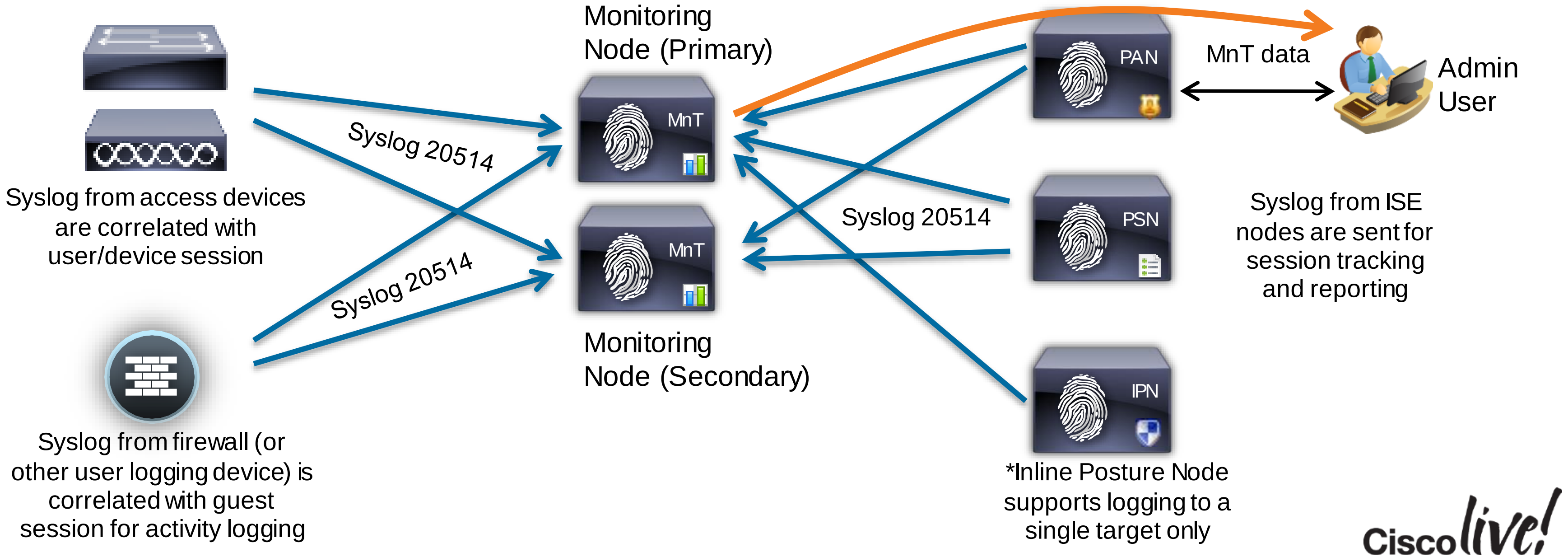
Service	Use case	Works (Y) / Does not work (N)
RADIUS Auth	Existing internal user	Y
	New internal user or endpoint created from Admin (WAN down)	N
	Existing/New AD/LDAP user (Assumes AD/LDAP reachable)	Y
Profiling	Existing endpoint with no profile change	Y
	Existing endpoint with profile change	Y (logs in with local profile)
	New endpoints learned via local profiling or local profile changes	Y
	New endpoints / endpoints changes made via Admin (WAN down)	N
Guest	Existing guests (LWA/CWA)	Y
	New guests (Sponsored, Self-Service, Guest API)	N
	Guest – Change Password	N (user must log in using old password)
	Guest – AUP	Y (displayed for every login)
	Guest – Max Failed Login Enforcement	N
Device Registration	Existing registered device	Y
	New endpoints learned via device registration / registration status	N
Posture	Posture Provisioning and Assessment	Y

HA for Monitoring and Troubleshooting

Steady State Operation

- Maximum two MnT nodes per deployment
- Active / Active

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



Syslog from access devices are correlated with user/device session

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

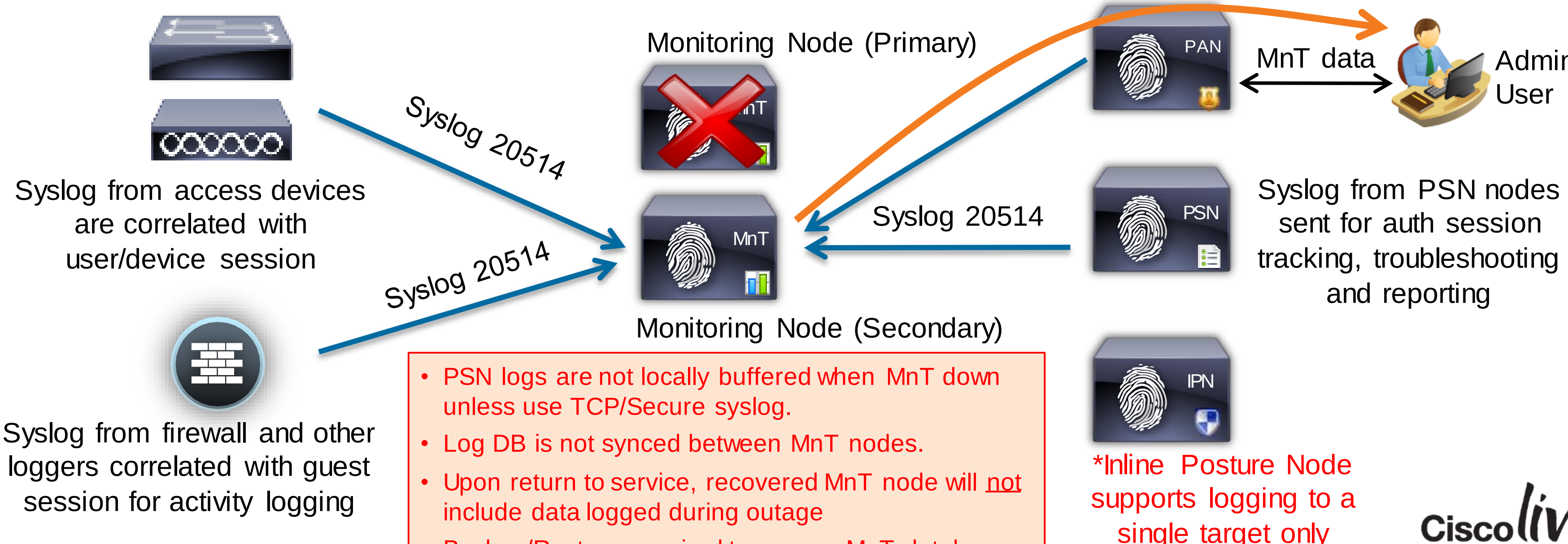
Syslog from ISE nodes are sent for session tracking and reporting

*Inline Posture Node supports logging to a single target only

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; IPN must be reconfigured to send logs to active MnT (only supports one log target).
- PAN auto-detects failure (down for > 5 min) and retrieves log/report data from Secondary MnT node.



Syslog from access devices are correlated with user/device session

Syslog from firewall and other loggers correlated with guest session for activity logging

Syslog from PSN nodes sent for auth session tracking, troubleshooting and reporting

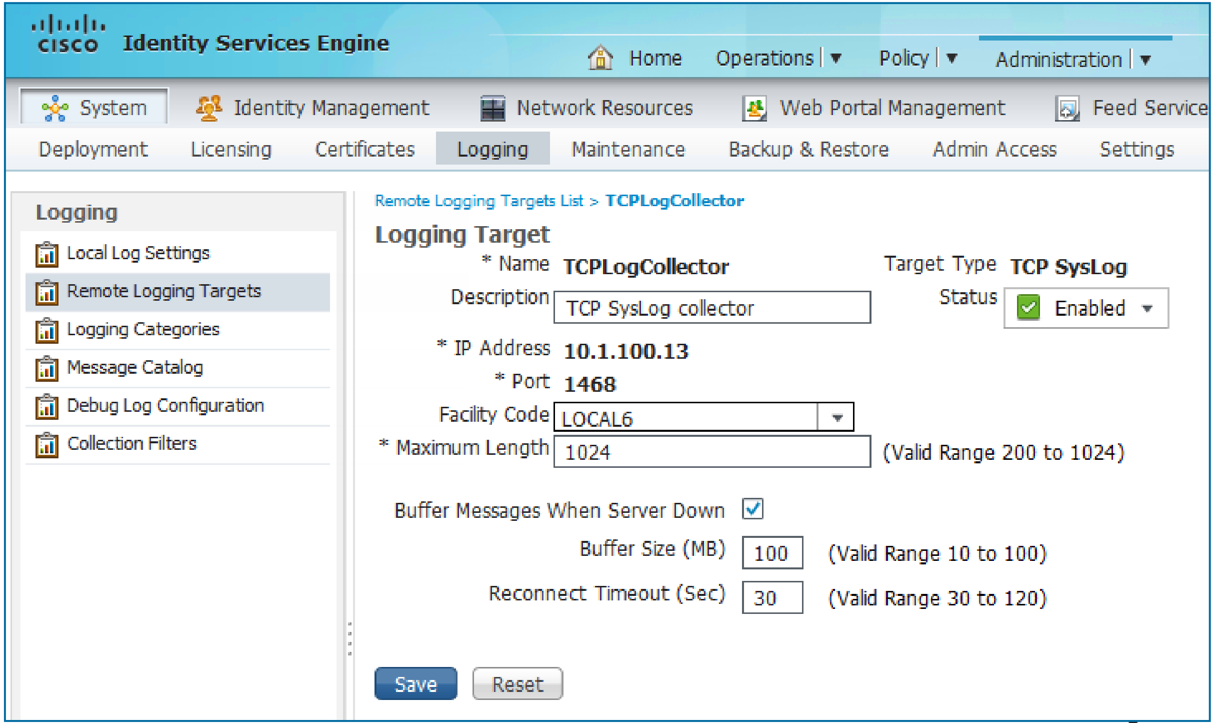
*Inline Posture Node supports logging to a single target only

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

Log Buffering

TCP and Secure Syslog Targets

- Default UDP-based audit logging does not buffer data when MnT is unavailable.
- TCP and Secure Syslog options can be used to buffer logs locally
- Note: Overall log performance will decrease if use these acknowledged options.



Logging Target

* Name	TCPLogCollector	Target Type	TCP SysLog
Description	TCP SysLog collector	Status	☑ Enabled
* IP Address	10.1.100.13		
* Port	1468		
Facility Code	LOCAL6		
* Maximum Length	1024	(Valid Range 200 to 1024)	

Buffer Messages When Server Down	☑	
Buffer Size (MB)	100	(Valid Range 10 to 100)
Reconnect Timeout (Sec)	30	(Valid Range 30 to 120)

HA for pxGrid

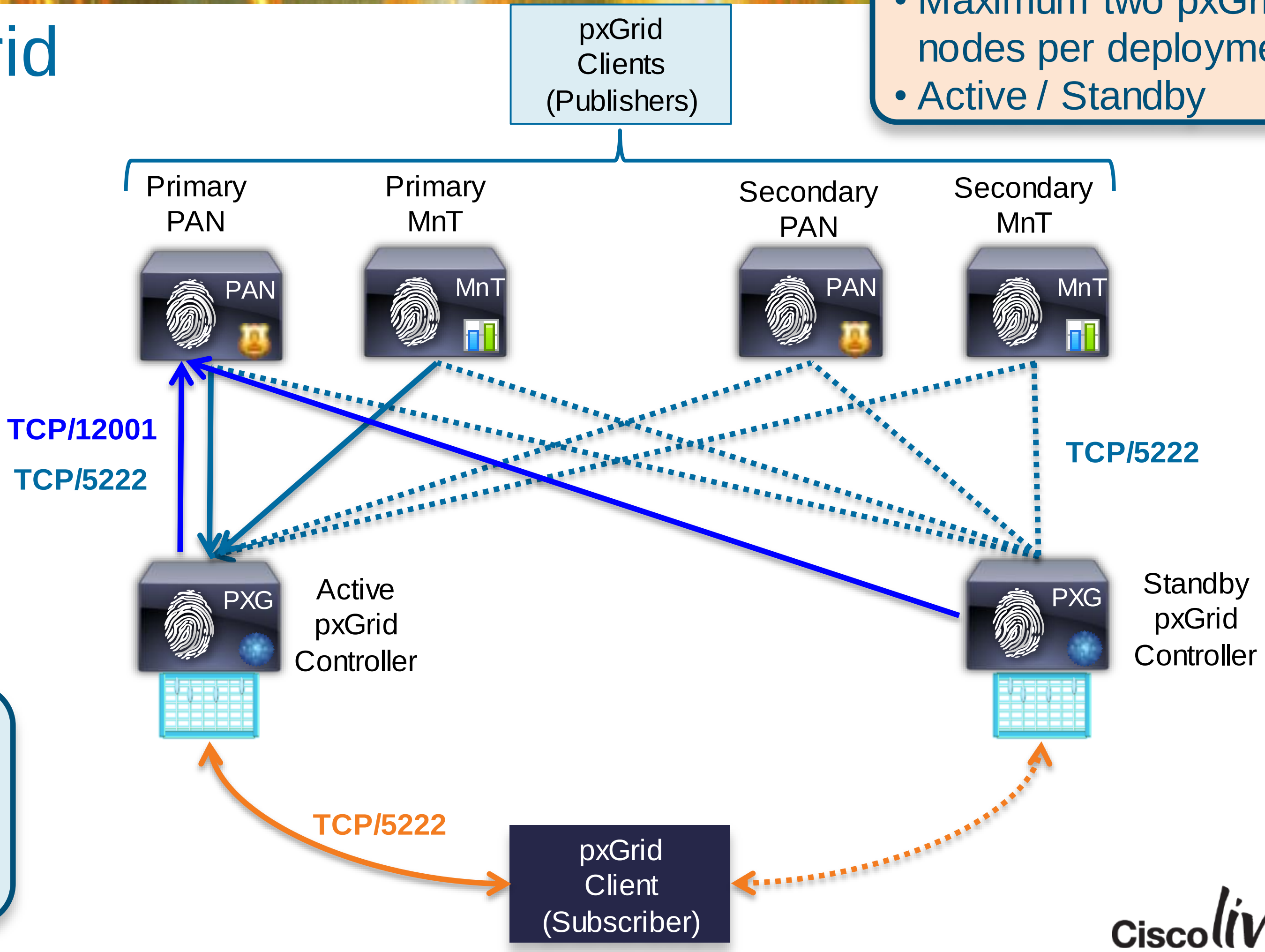
Steady State

- Maximum two pxGrid nodes per deployment
- Active / Standby

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



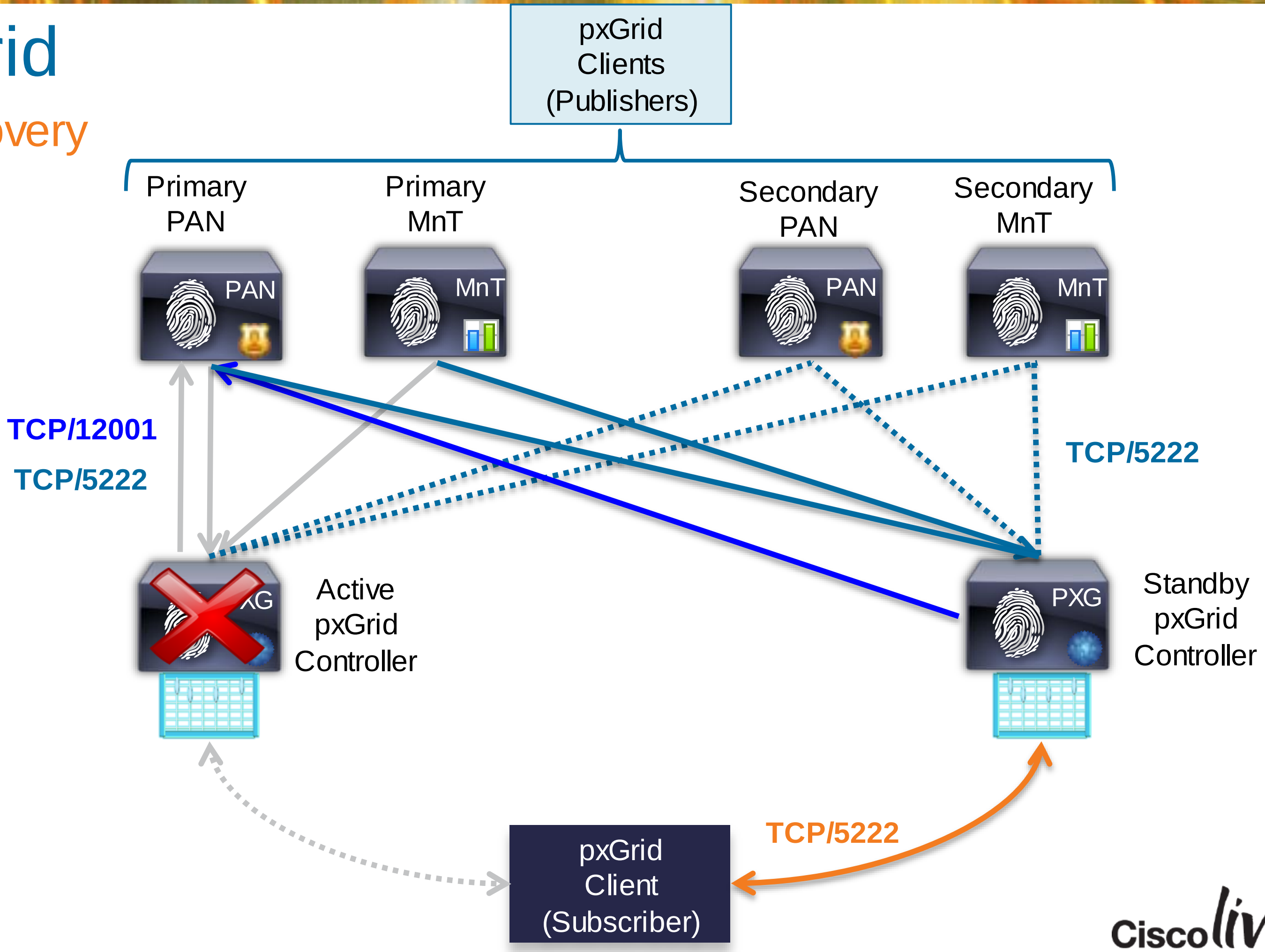
HA for pxGrid

Failover and Recovery

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

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

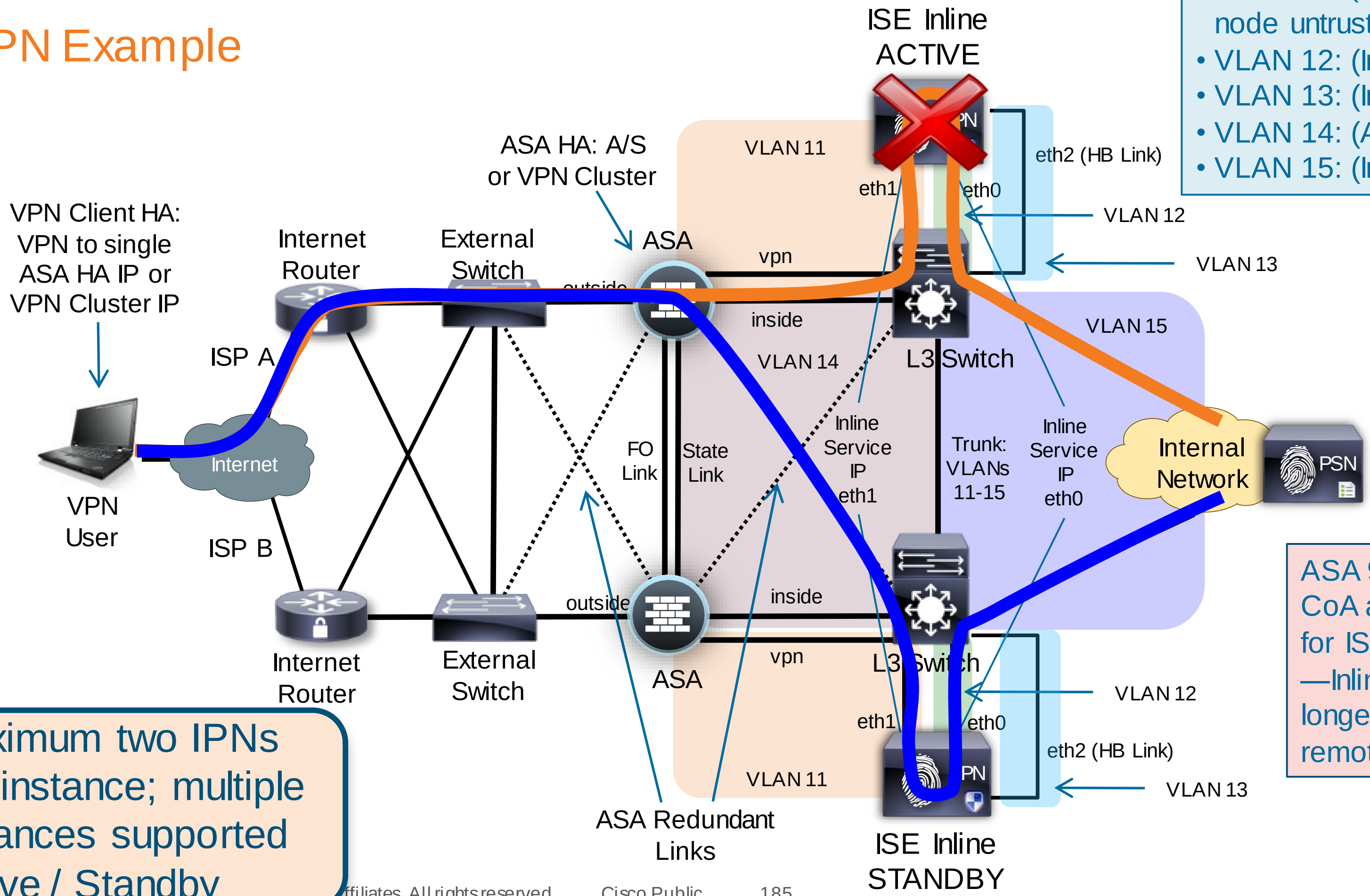
If active pxGrid Controller fails, clients automatically attempt connection to standby controller.



HA for Inline Posture Node

VPN Example

VLANS
- VLAN 11: (ASA VPN; Inline node untrusted)
- VLAN 12: (Inline node trusted)
- VLAN 13: (Inline Heartbeat Link)
- VLAN 14: (ASA Inside)
- VLAN 15: (Internal Network)



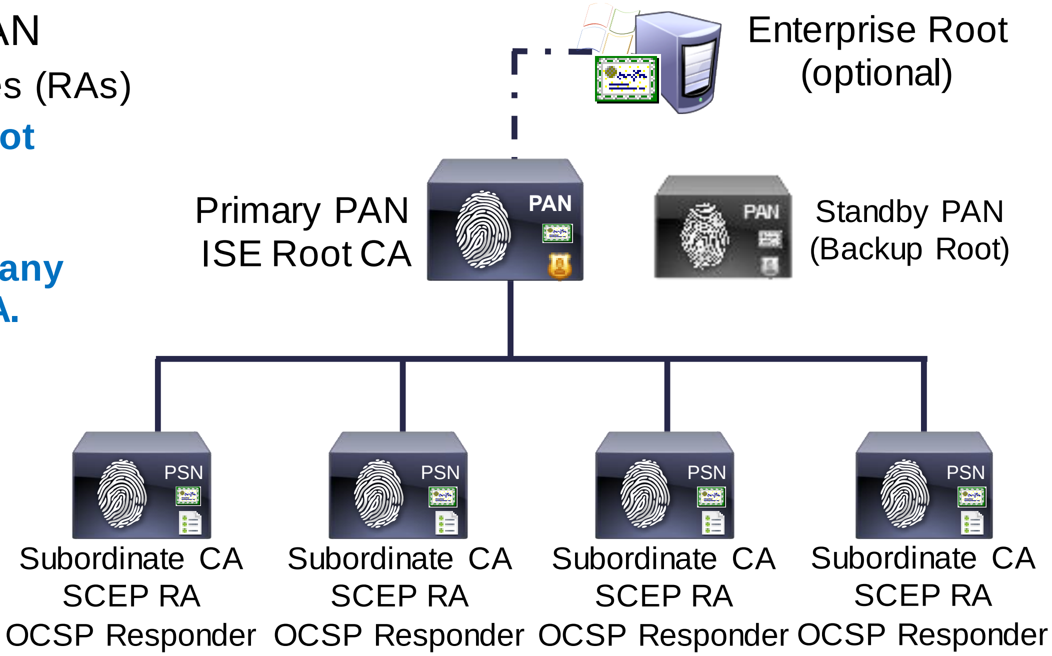
New

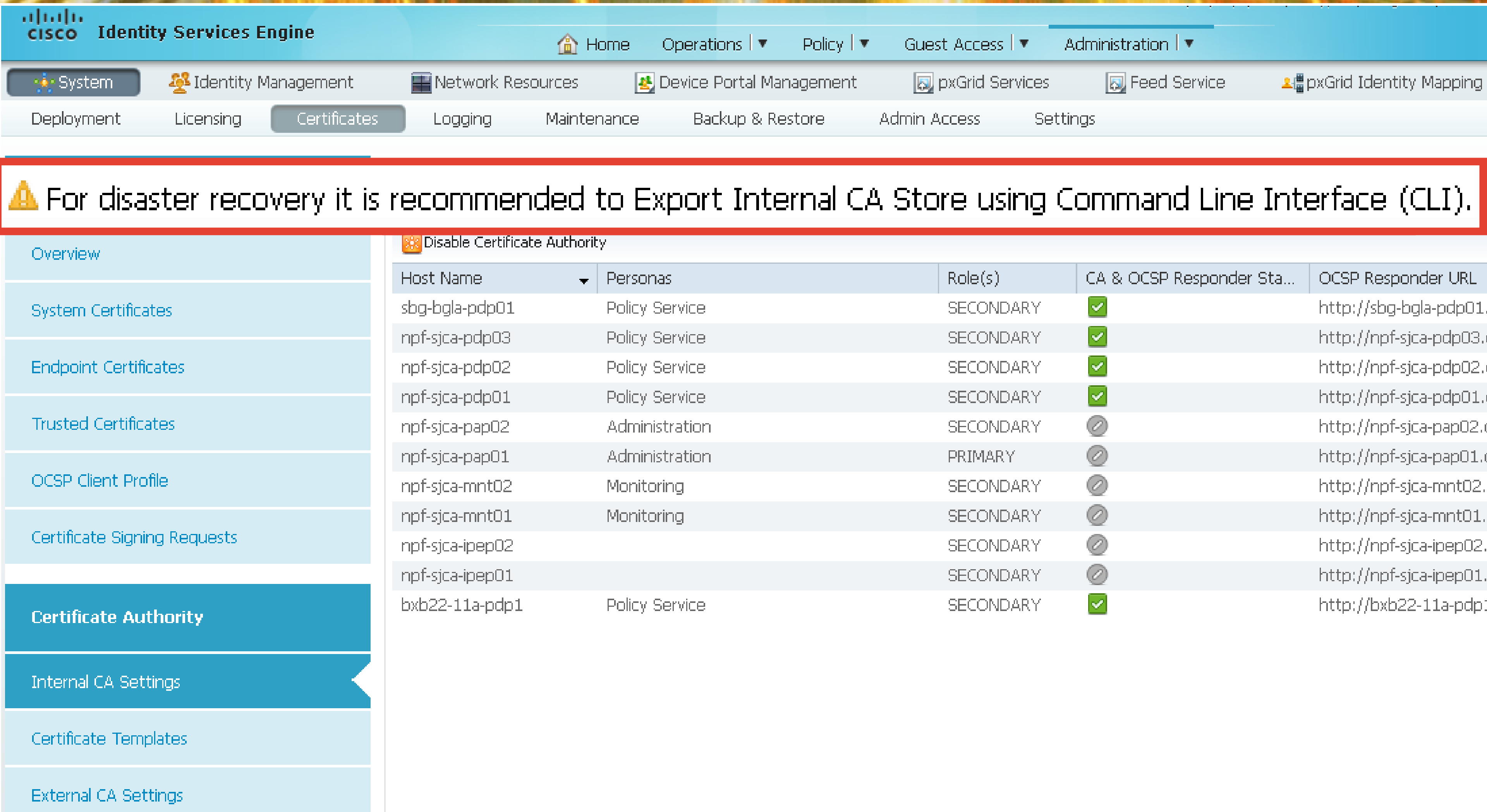
ASA 9.2.1 supports native CoA and URL Redirection for ISE Posture Services—Inline Posture Node no longer a required for remote access ASA VPN.

- Maximum two IPNs per instance; multiple instances supported
- Active / Standby

HA for Internal Certificate Authority

- Primary PAN is Root CA for ISE deployment
  - May be Subordinate to external Root CA or Standalone Root.
- All PSNs are Subordinate CAs to PAN
  - PSNs are SCEP Registration Authorities (RAs)
  - **Each PSN can issue certs even if Root (Primary PAN) fails**
  - Each PSN runs OCSP responder. **OCSP DB replicated so can point to any PSN, or LB PSN cluster for OCSP HA.**
- Promotion of Standby PAN:
  - No effect on sub-CA operation.
  - **To make Standby the Root CA must manually install the Public/ Private keys from Primary PAN.**





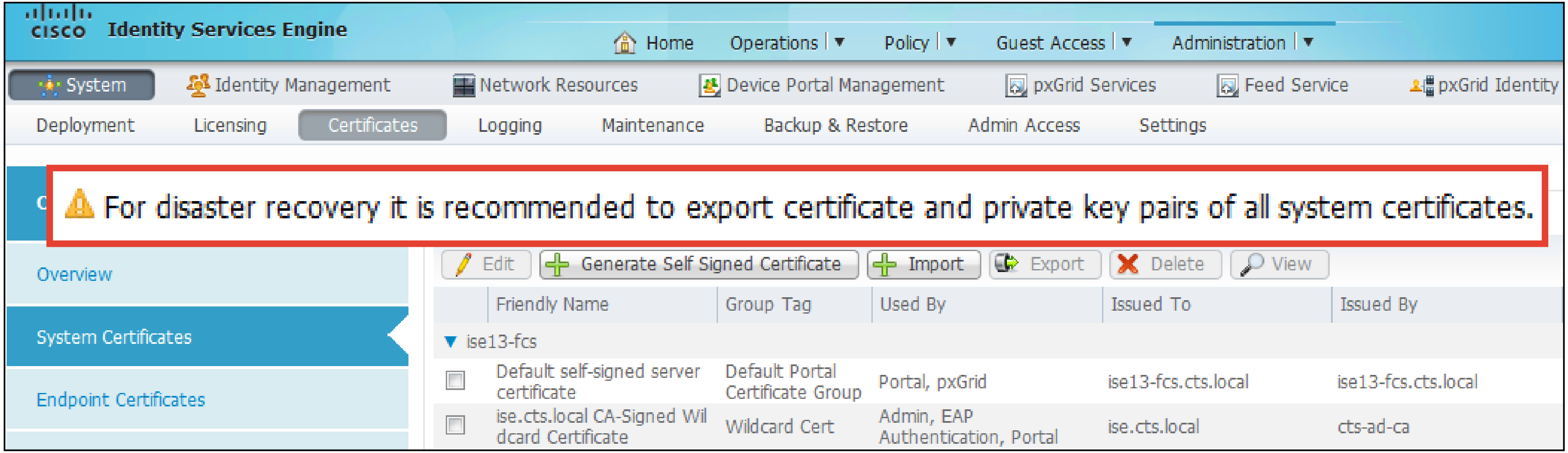
⚠ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

Host Name	Personas	Role(s)	CA & OCSP Responder Sta...	OCSP Responder URL
sbg-bgla-pdp01	Policy Service	SECONDARY	✓	http://sbg-bgla-pdp01.
npf-sjca-pdp03	Policy Service	SECONDARY	✓	http://npf-sjca-pdp03.
npf-sjca-pdp02	Policy Service	SECONDARY	✓	http://npf-sjca-pdp02.
npf-sjca-pdp01	Policy Service	SECONDARY	✓	http://npf-sjca-pdp01.
npf-sjca-pap02	Administration	SECONDARY	⊘	http://npf-sjca-pap02.
npf-sjca-pap01	Administration	PRIMARY	⊘	http://npf-sjca-pap01.
npf-sjca-mnt02	Monitoring	SECONDARY	⊘	http://npf-sjca-mnt02.
npf-sjca-mnt01	Monitoring	SECONDARY	⊘	http://npf-sjca-mnt01.
npf-sjca-ipep02		SECONDARY	⊘	http://npf-sjca-ipep02.
npf-sjca-ipep01		SECONDARY	⊘	http://npf-sjca-ipep01.
bxb22-11a-pdp1	Policy Service	SECONDARY	✓	http://bxb22-11a-pdp1

Certificate Recovery for ISE Nodes

Backup all System Certificates and Key Pairs

- System Certificates for all nodes can be centrally exported with private key pairs from Primary PAN in case needed fro Disaster Recovery.

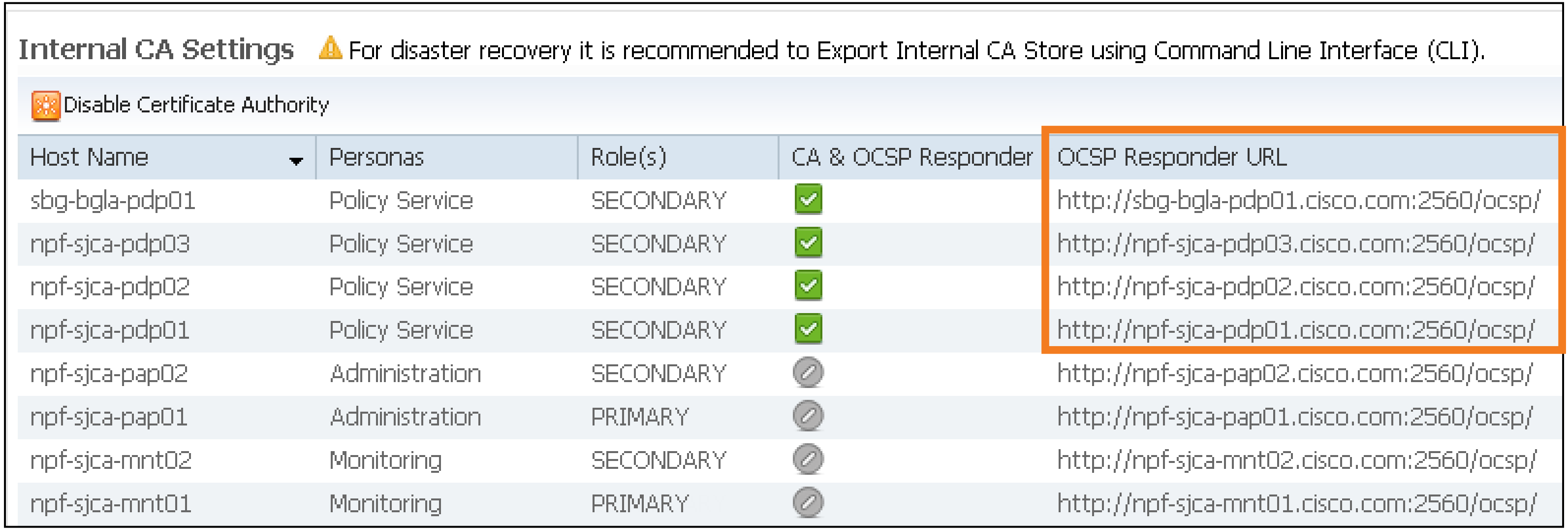


⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Group Tag	Used By	Issued To	Issued By
▼ ise13-fcs					
□	Default self-signed server certificate	Default Portal Certificate Group	Portal, pxGrid	ise13-fcs.cts.local	ise13-fcs.cts.local
□	ise.cts.local CA-Signed Wildcard Certificate	Wildcard Cert	Admin, EAP Authentication, Portal	ise.cts.local	cts-ad-ca

OCSP Responder HA

- Each PSN runs OCSP responder.
- OCSP DB replicated so can point to any PSN, or LB PSN cluster for OCSP HA.



Internal CA Settings ⚠ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

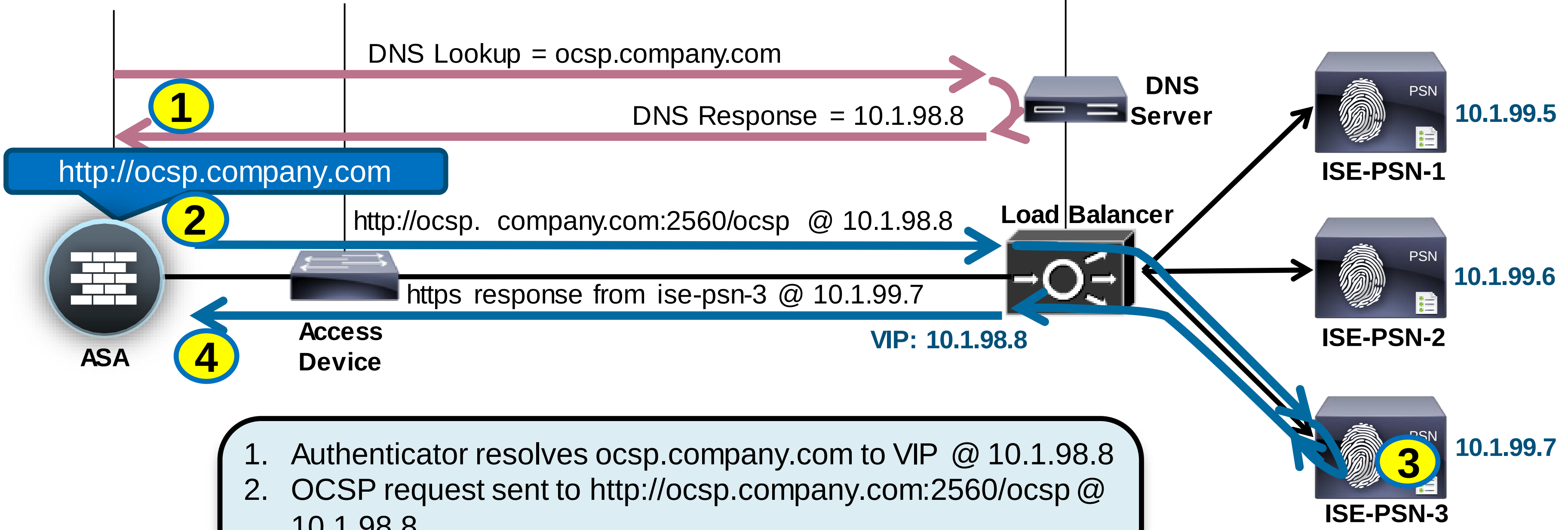
Host Name	Personas	Role(s)	CA & OCSP Responder	OCSP Responder URL
sbg-bgla-pdp01	Policy Service	SECONDARY	✓	http://sbg-bgla-pdp01.cisco.com:2560/ocsp/
npf-sjca-pdp03	Policy Service	SECONDARY	✓	http://npf-sjca-pdp03.cisco.com:2560/ocsp/
npf-sjca-pdp02	Policy Service	SECONDARY	✓	http://npf-sjca-pdp02.cisco.com:2560/ocsp/
npf-sjca-pdp01	Policy Service	SECONDARY	✓	http://npf-sjca-pdp01.cisco.com:2560/ocsp/
npf-sjca-pap02	Administration	SECONDARY	⊘	http://npf-sjca-pap02.cisco.com:2560/ocsp/
npf-sjca-pap01	Administration	PRIMARY	⊘	http://npf-sjca-pap01.cisco.com:2560/ocsp/
npf-sjca-mnt02	Monitoring	SECONDARY	⊘	http://npf-sjca-mnt02.cisco.com:2560/ocsp/
npf-sjca-mnt01	Monitoring	PRIMARY	⊘	http://npf-sjca-mnt01.cisco.com:2560/ocsp/

ASA Remote Access VPN Example:
match certificate OCSP_MAP override ocsp trustpoint ISE_Root 1 url http://ise-ocsp.company.com:2560/ocsp/

Load Balancing OCSP

Sample Flow

Each PSN is an OCSP Responder
Database replication ensures each PSN contains same info for ISE-issued certificates.

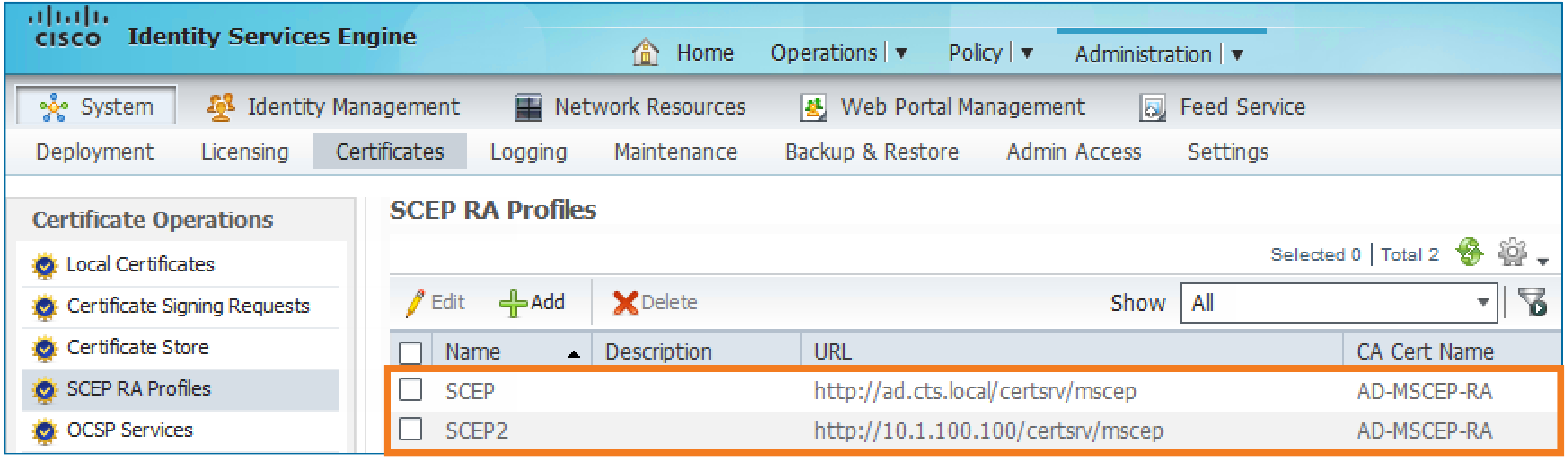


1. Authenticator resolves ocsp.company.com to VIP @ 10.1.98.8
2. OCSP request sent to http://ocsp.company.com:2560/ocsp @ 10.1.98.8
3. Load balancer forwards request to PSN-3 (OCSP Responder) @ 10.1.99.7
4. Authentication receives OCSP response from PSN-3

SCEP Load Balancing for BYOD/NSP (ISE 1.2)

If multiple SCEP CA Servers defined…

- Multiple SCEP Profiles supported—Requests load balanced based on load factor.
  - Load Factor = Average Response Time x Total Requests x Outstanding Requests
  - Average Response Time = Average of last two 20 requests
- SCEP CA declared down if no response after three consecutive requests.
- CA with the next lowest load used; Periodic polling to failed server until online.



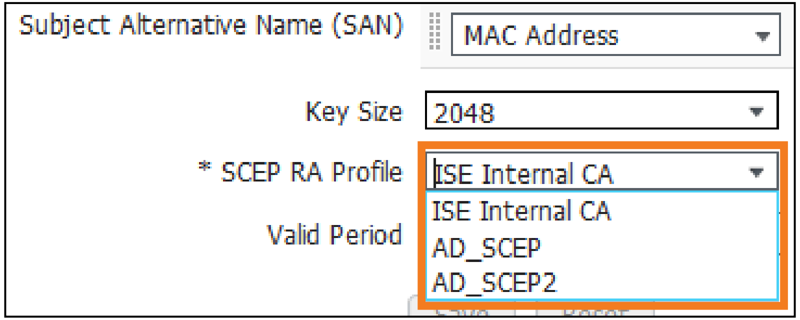
SCEP RA Profiles

□	Name	Description	URL	CA Cert Name
□	SCEP		http://ad.cts.local/certsrv/mscep	AD-MSCEP-RA
□	SCEP2		http://10.1.100.100/certsrv/mscep	AD-MSCEP-RA

SCEP Load Balancing (ISE 1.3)

If multiple SCEP CA Servers defined…

- SCEP Profile defined in Certificate Template —only one can be selected.
- ISE 1.3 supports multiple CA URLs in each profile
- Requests load balanced across CAs

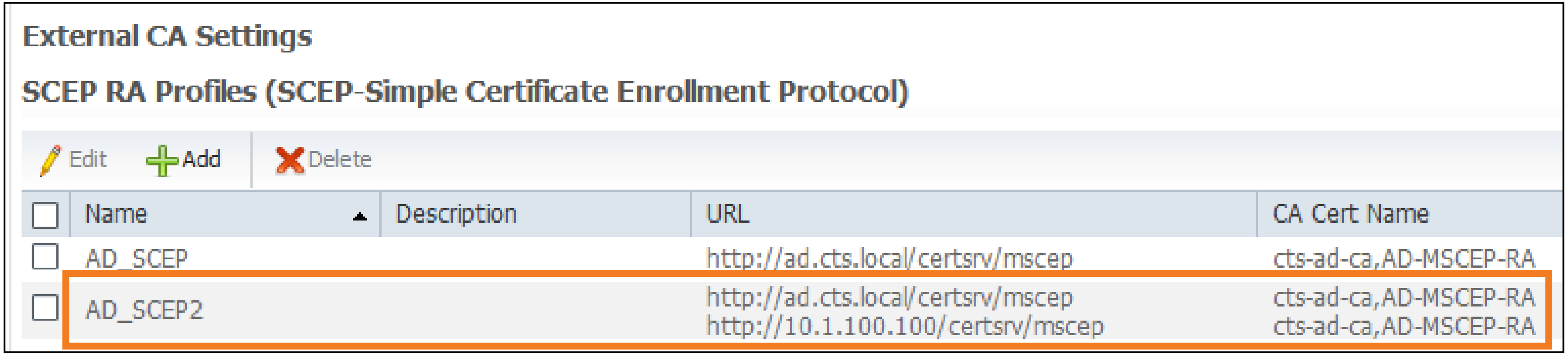


Subject Alternative Name (SAN): MAC Address

Key Size: 2048

* SCEP RA Profile: ISE Internal CA

Valid Period



External CA Settings

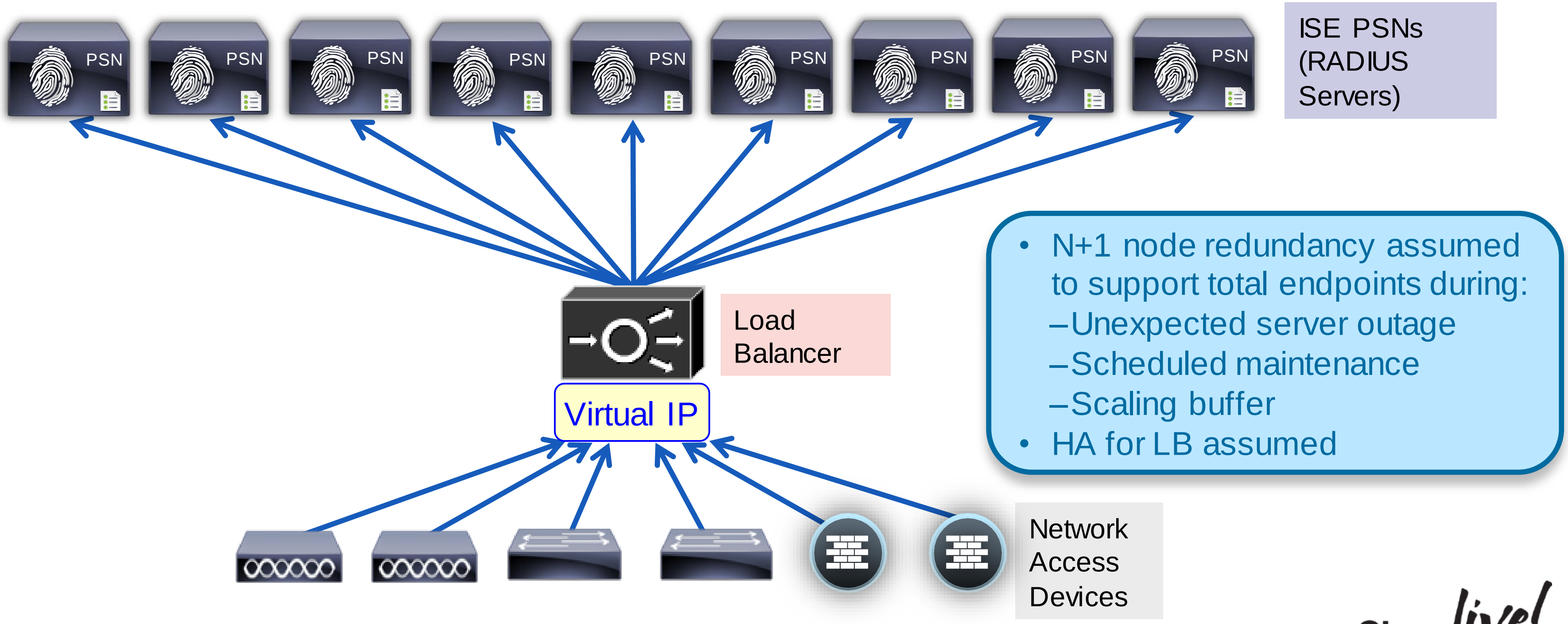
SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

□	Name	Description	URL	CA Cert Name
□	AD_SCEP		http://ad.cts.local/certsrv/mscep	cts-ad-ca,AD-MSCEP-RA
□	AD_SCEP2		http://ad.cts.local/certsrv/mscep http://10.1.100.100/certsrv/mscep	cts-ad-ca,AD-MSCEP-RA cts-ad-ca,AD-MSCEP-RA

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.



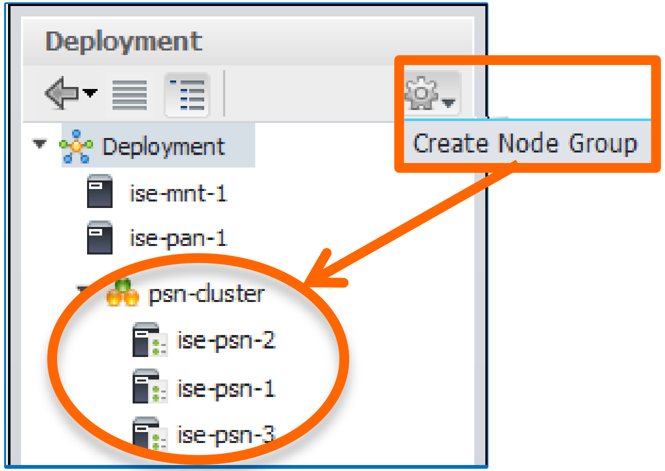
- N+1 node redundancy assumed to support total endpoints during:
  - Unexpected server outage
  - Scheduled maintenance
  - Scaling buffer
- HA for LB assumed

Configure Node Groups for LB Cluster

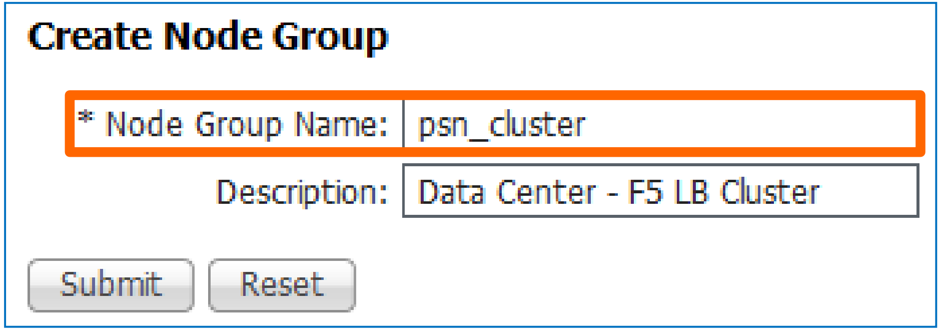
All PSNs in LB Cluster in Same Node Group

- Administration > System > Deployment

1) Create node group



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

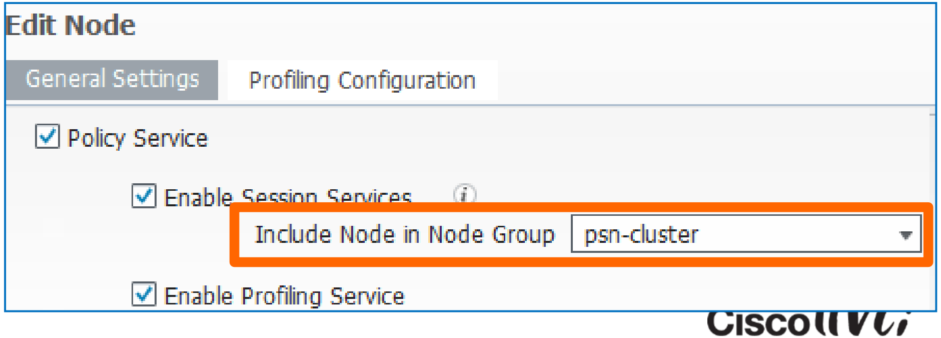


Create Node Group

* Node Group Name: psn_cluster

Description: Data Center - F5 LB Cluster

3) Add individual PSNs to node group



Edit Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group: psn-cluster

☑ Enable Profiling Service

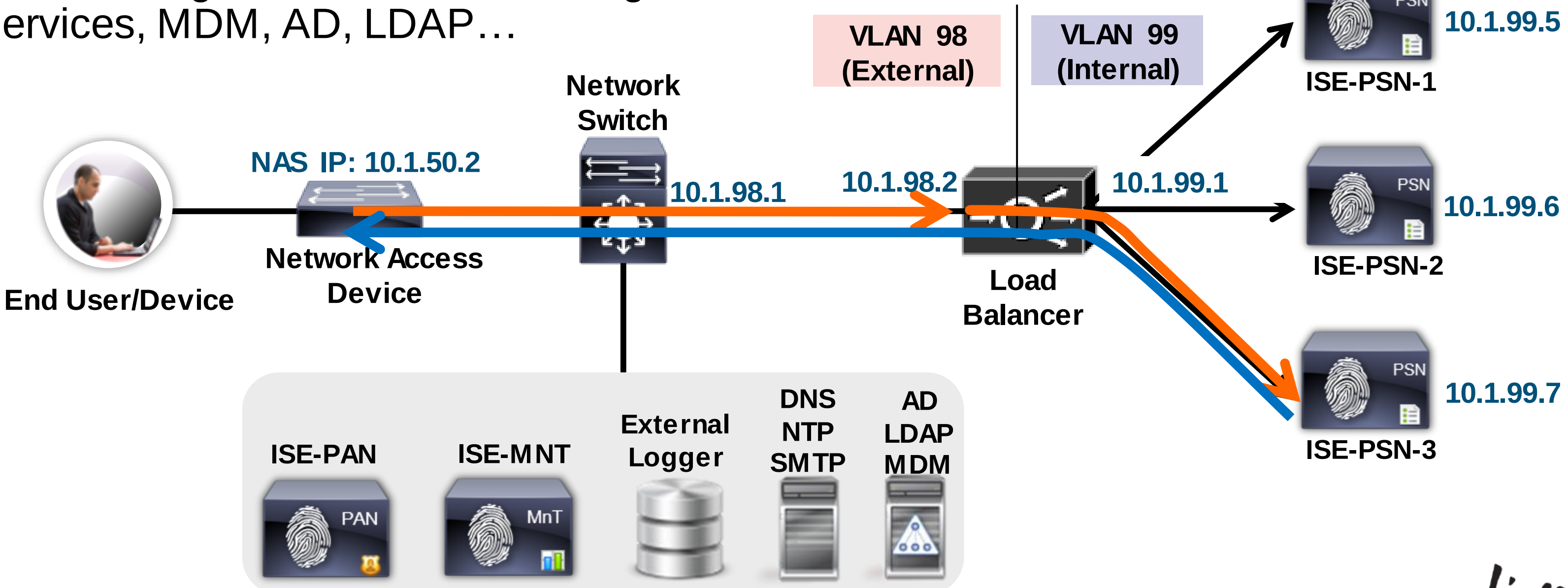
- Node group members can be L2 or L3
- Multicast no longer a requirements in ISE 1.3

Traffic Flow—Fully Inline: Physically Separation

Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

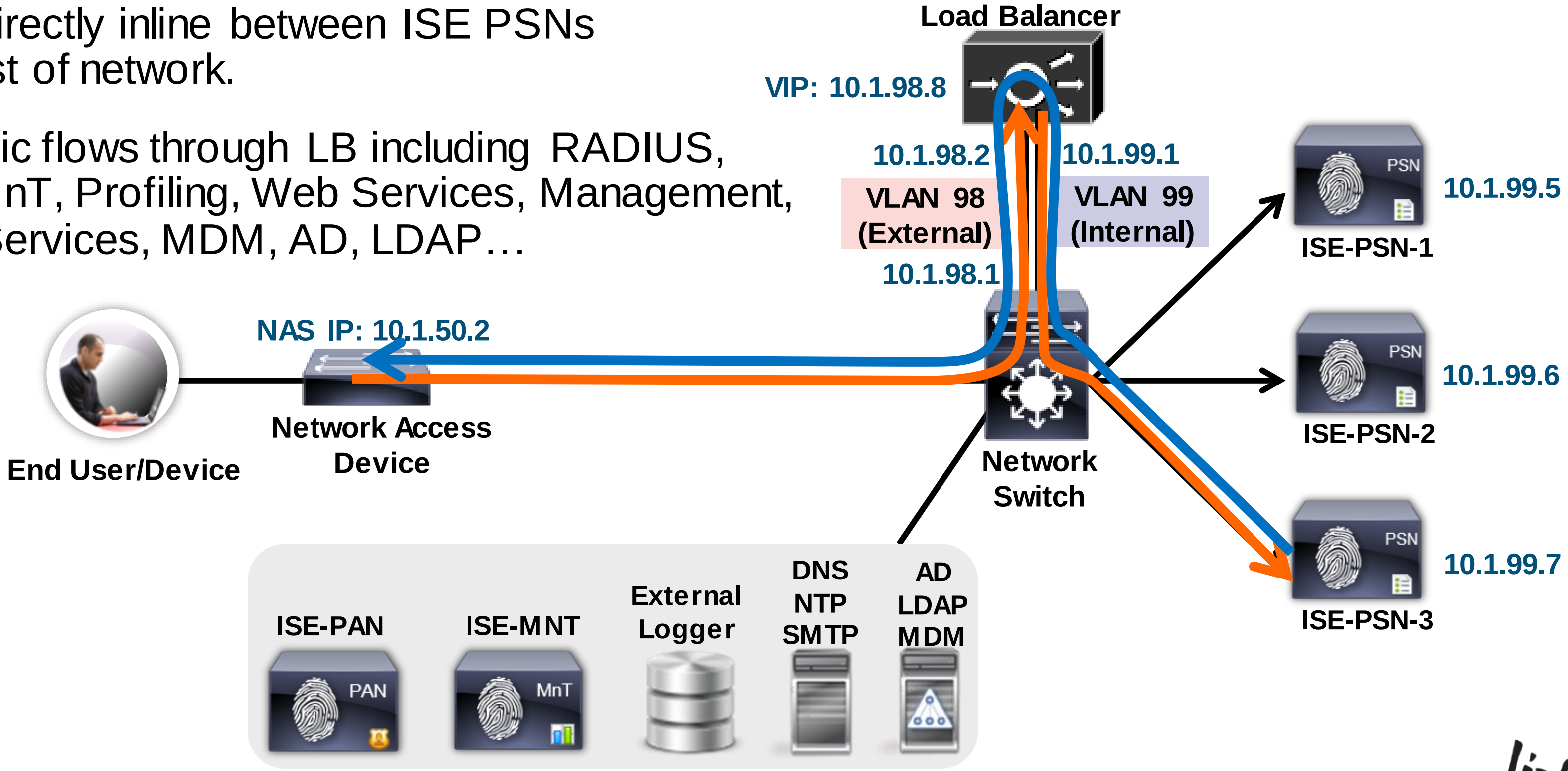
- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT,Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…



Traffic Flow—Fully Inline: VLAN Separation

Logical Network Separation Using Single LB Interface and VLAN Trunking

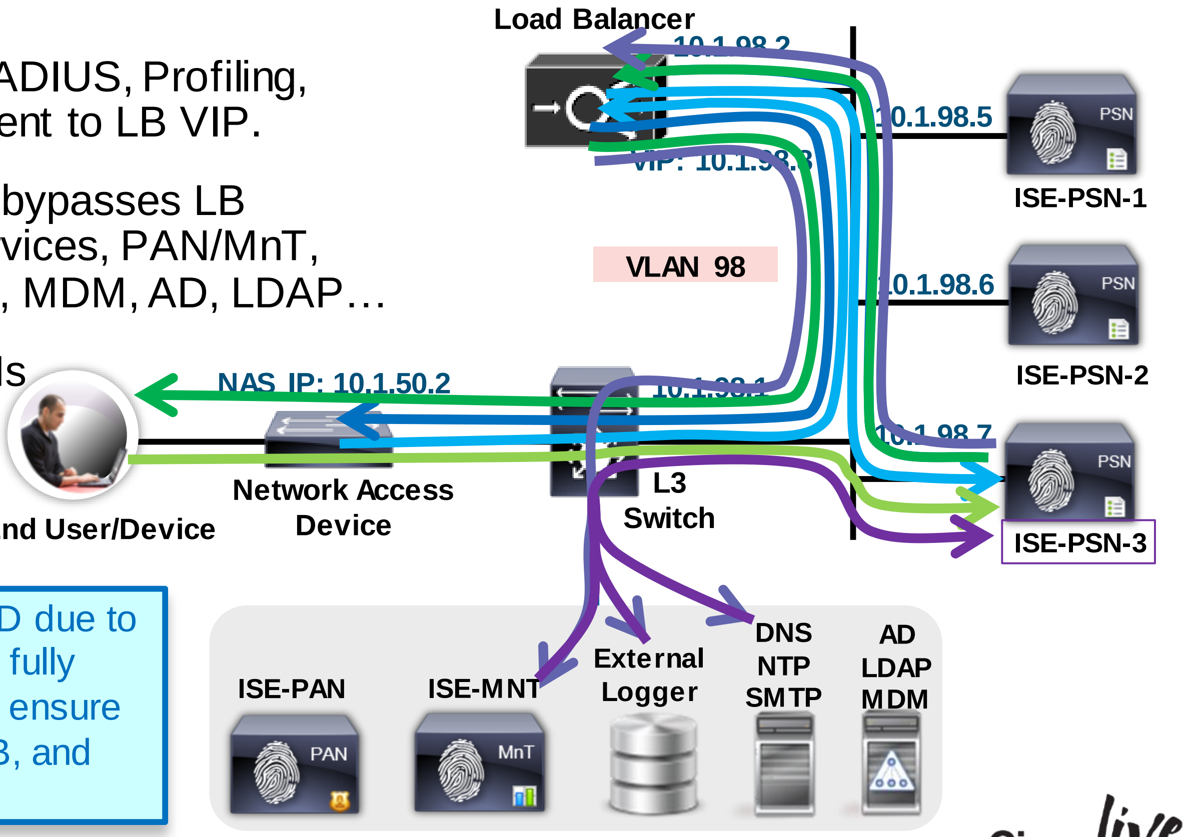
- LB is directly inline between ISE PSNs and rest of network.
- All traffic flows through LB including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…



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

Direct PSN Connections to LB and Rest of Network

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



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

Load Balancing 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 URL-Redirected Services:** Posture (CPP) / Central WebAuth (CWA) / Native Supplicant Provisioning (NSP) / Device Registration WebAuth (DRW)

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

- **Web Direct HTTP/S Services:** Local WebAuth (LWA) / Sponsor / MyDevices Portal, OCSP

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

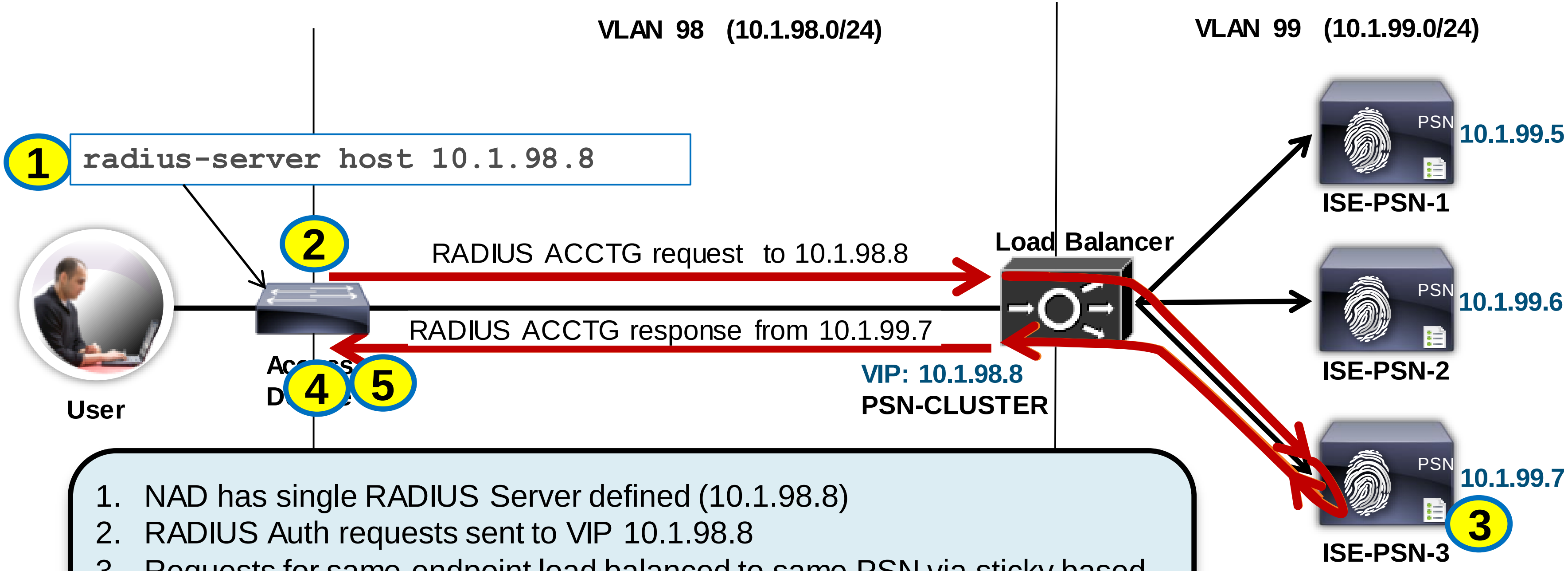
- **Profiling Services:** DHCP Helper / SNMP Traps / Netflow / RADIUS

  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

Load Balancing
RADIUS

Load Balancing RADIUS

Sample Flow

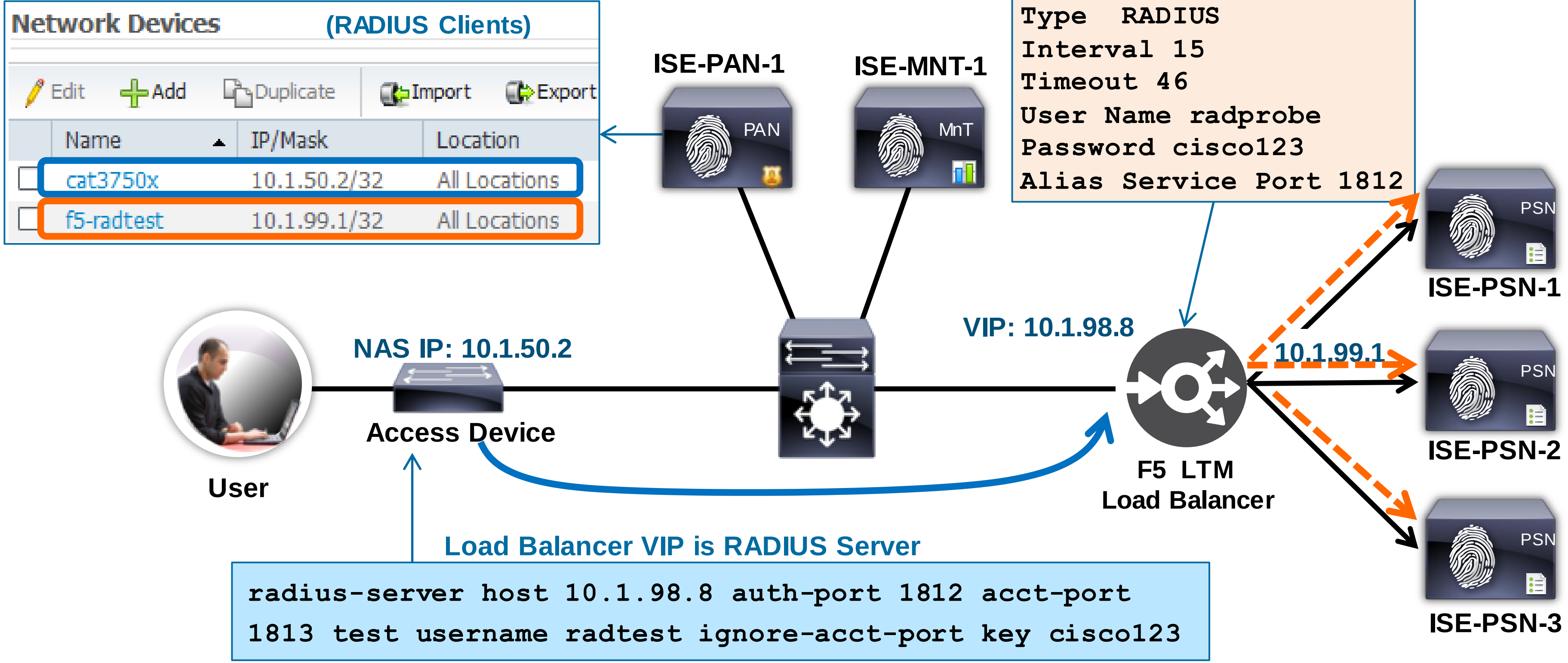


1. NAD has single RADIUS Server defined (10.1.98.8)
2. RADIUS Auth requests sent to VIP 10.1.98.8
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS Response received from real server ise-psn-3 @ 10.1.99.7
5. RADIUS Accounting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

Load Balancer General RADIUS Guidelines

RADIUS Servers and Clients – Where Defined

ISE Admin Node > Network Devices



Network Devices (RADIUS Clients)

Edit · Add · Duplicate · Import · Export

	Name	IP/Mask	Location
□	cat3750x	10.1.50.2/32	All Locations
□	f5-radtest	10.1.99.1/32	All Locations

PSNs are RADIUS Servers for Health Probes

```
Name  PSN-Probe
Type   RADIUS
Interval 15
Timeout 46
User Name radprobe
Password cisco123
Alias Service Port 1812
```

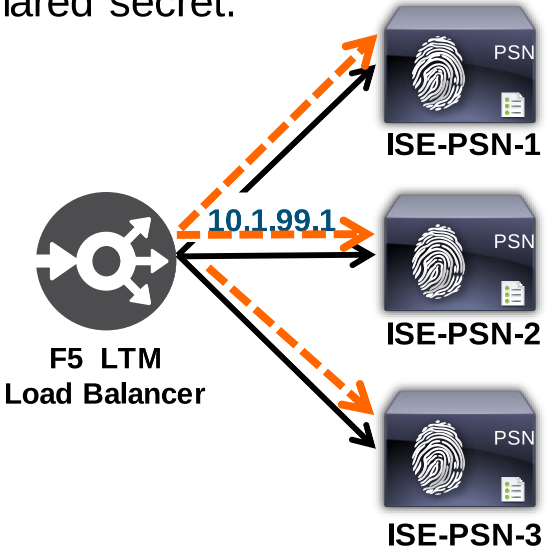
Load Balancer VIP is RADIUS Server

```
radius-server host 10.1.98.8 auth-port 1812 acct-port
1813 test username radtest ignore-acct-port key cisco123
```

Add LB as NAD for RADIUS Health Monitoring

Administration > Network Resources > Network Devices

- Configure Self IP address of LB Internal interface connected to PSN RADIUS interfaces.
- Enable Authentication and set RADIUS shared secret.



PSN

ISE-PSN-1

10.1.99.1

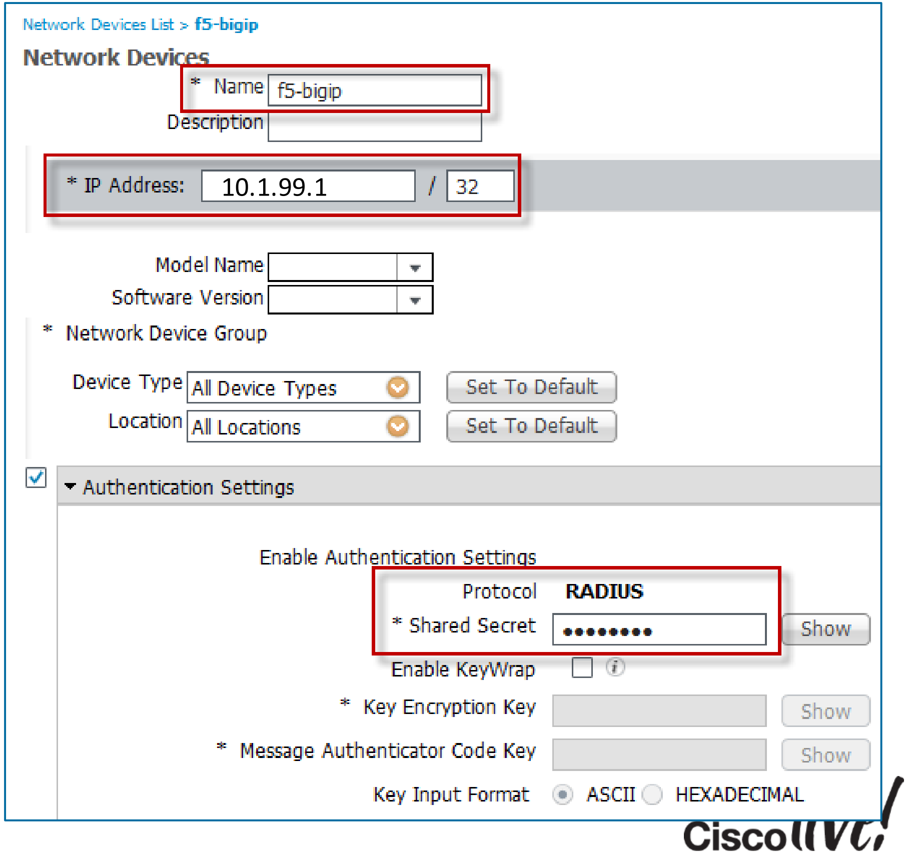
PSN

ISE-PSN-2

F5 LTM
Load Balancer

PSN

ISE-PSN-3



Network Devices List > **f5-bigip**

Network Devices

* Name	f5-bigip
Description	
* IP Address:	10.1.99.1 / 32
Model Name	
Software Version	
* Network Device Group	
Device Type	All Device Types — Set To Default
Location	All Locations — Set To Default

☑ ▾ Authentication Settings

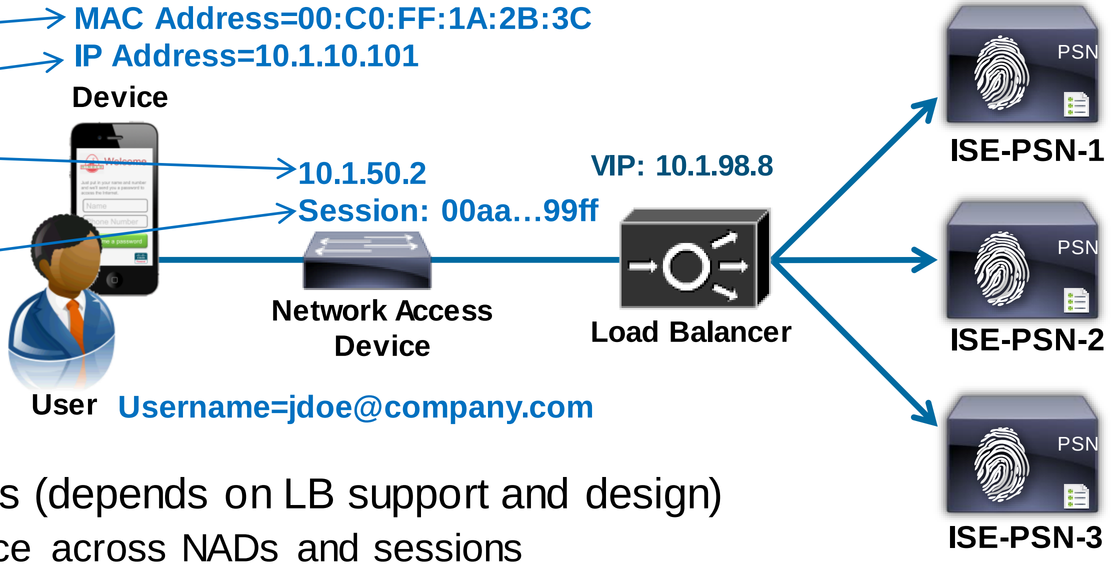
Enable Authentication Settings

Protocol	**RADIUS**
* Shared Secret	•••••••• Show
Enable KeyWrap	□
* Key Encryption Key	Show
* Message Authenticator Code Key	Show
Key Input Format	● ASCII ○ HEXADECIMAL

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 Balancer Stickiness Guidelines

Persistence Attributes

- ACE Example: RADIUS Sticky on IP and Calling-Station-ID (client MAC address)

```
sticky radius framed-ip calling-station-id RADIUS-STICKY
  serverfarm ise-psn
```

- F5 iRule Example: RADIUS Sticky on Calling-Station-ID (client MAC address)

```
ltm rule RADIUS_iRule {
    when CLIENT_ACCEPTED {

persist uie [RADIUS::avp 31]
}
}
```

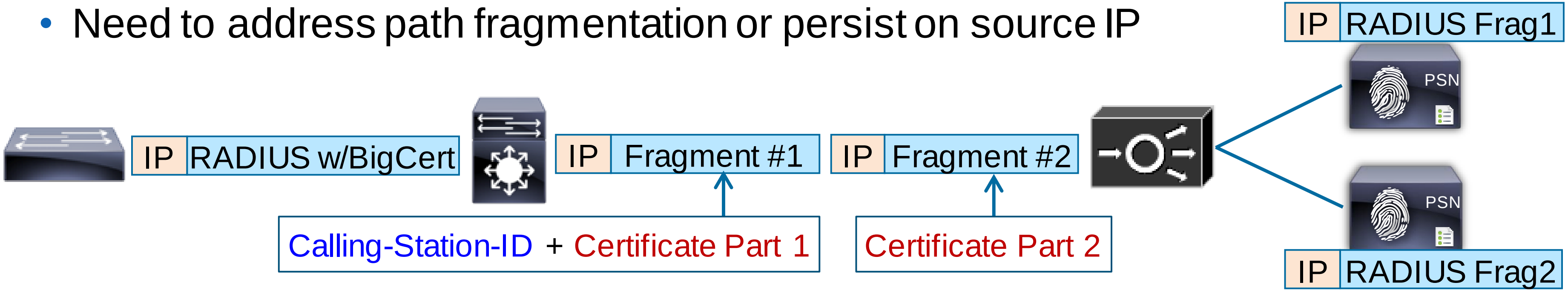
Be sure to monitor load balancer resources when performing advanced parsing.

LB Fragmentation and Reassembly

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

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

LB on Call-ID



LB on Source IP

(No Calling ID in RADIUS packet)

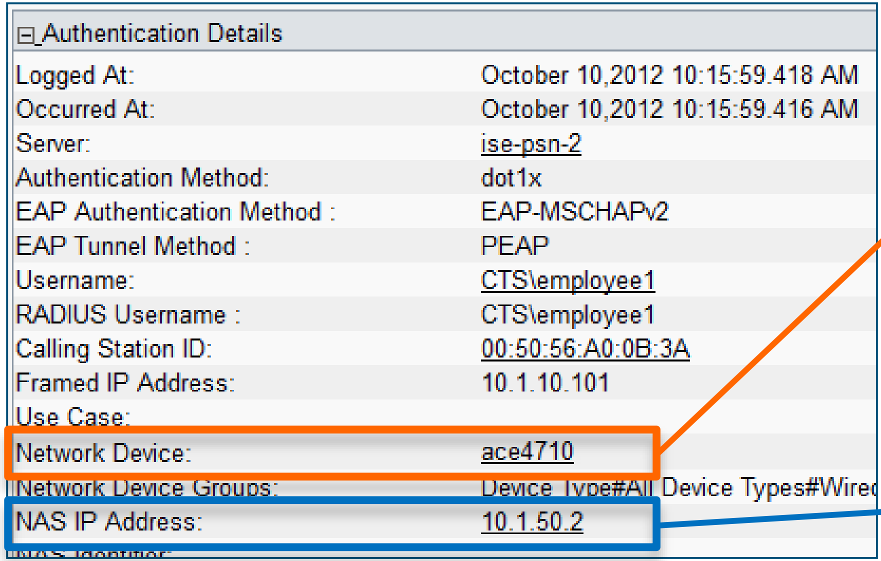
- ACE reassembles RADIUS packet.
- F5 LTM reassembles packets by default except for FastL4 Protocol
  – Must be manually enabled under the FastL4 Protocol Profile
- Citrix NetScaler fragmentation defect—Resolved in NetScaler 10.5 Build 50.10
  – Issue ID 429415 addresses fragmentation and the reassembly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

NAT Restrictions for RADIUS Load Balancing

Why Source NAT (SNAT) Fails for NADs

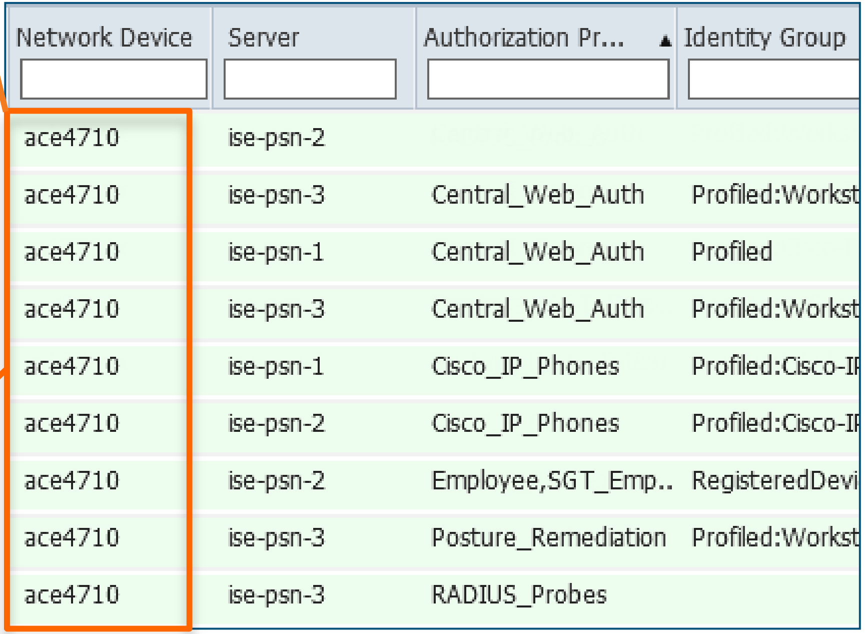
SNAT results in less visibility as all requests appear sourced from LB – makes troubleshooting more difficult.

- With SNAT, LB appears as the Network Access Device (NAD) to PSN.
- CoA sent to wrong IP address



⊟ Authentication Details

Logged At:	October 10,2012 10:15:59.418 AM
Occurred At:	October 10,2012 10:15:59.416 AM
Server:	ise-psn-2
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	CTS\employee1
RADIUS Username :	CTS\employee1
Calling Station ID:	00:50:56:A0:0B:3A
Framed IP Address:	10.1.10.101
Use Case:	
Network Device:	ace4710
Network Device Groups:	Device Type#All Device Types#Wired
NAS IP Address:	10.1.50.2
NAS Identifier:	

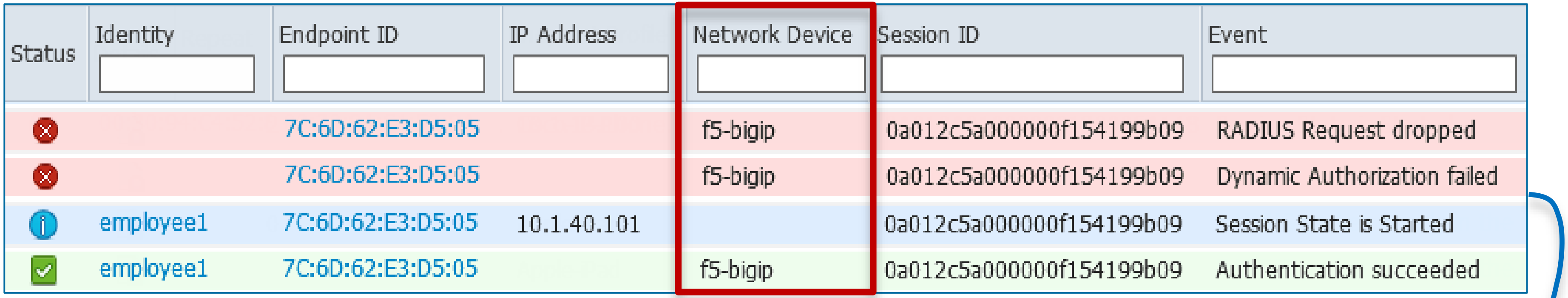


Network Device	Server	Authorization Pr... ▲	Identity Group
ace4710	ise-psn-2	Central_Web_Auth	Profiled:Workst
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workst
ace4710	ise-psn-1	Central_Web_Auth	Profiled
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workst
ace4710	ise-psn-1	Cisco_IP_Phones	Profiled:Cisco-IP
ace4710	ise-psn-2	Cisco_IP_Phones	Profiled:Cisco-IP
ace4710	ise-psn-2	Employee,SGT_Emp..	RegisteredDevi
ace4710	ise-psn-3	Posture_Remediation	Profiled:Workst
ace4710	ise-psn-3	RADIUS_Probes	

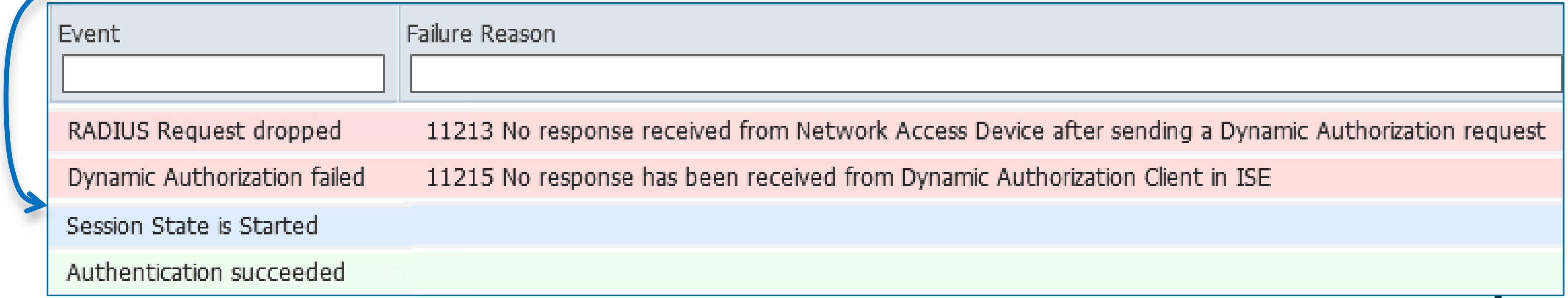
NAS IP Address is correct, but not currently used for CoA

SNAT of NAD Traffic: Live Log Example

Auth Succeeds/CoA Fails: CoA Sent to Load Balancer and Dropped



Status	Identity	Endpoint ID	IP Address	Network Device	Session ID	Event
☒		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	RADIUS Request dropped
☒		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Dynamic Authorization failed
ⓘ	employee1	7C:6D:62:E3:D5:05	10.1.40.101		0a012c5a000000f154199b09	Session State is Started
✓	employee1	7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Authentication succeeded



Event	Failure Reason
RADIUS Request dropped	11213 No response received from Network Access Device after sending a Dynamic Authorization request
Dynamic Authorization failed	11215 No response has been received from Dynamic Authorization Client in ISE
Session State is Started	
Authentication succeeded	

Allow NAT for PSN CoA Requests

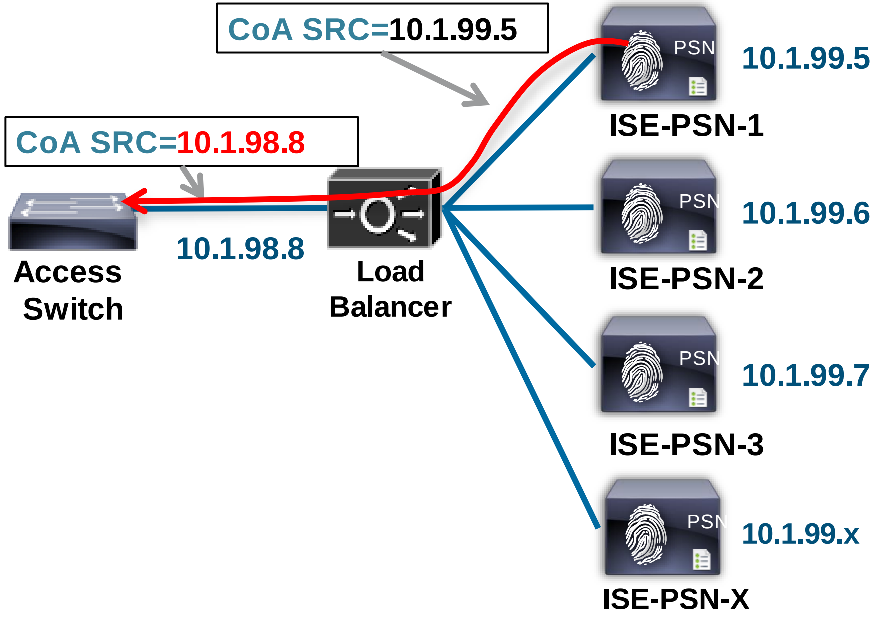
Simplifying Switch CoA Configuration

- Match traffic from PSNs to UDP/1700 (RADIUS CoA) and translate to PSN cluster VIP.
- Access switch config:
  - Before:

```
aaa server radius dynamic-author
 client 10.1.99.5 server-key cisco123
 client 10.1.99.6 server-key cisco123
 client 10.1.99.7 server-key cisco123
 client 10.1.99.8 server-key cisco123
 client 10.1.99.9 server-key cisco123
 client 10.1.99.10 server-key cisco123
 <…one entry per PSN…>
```

  - After:

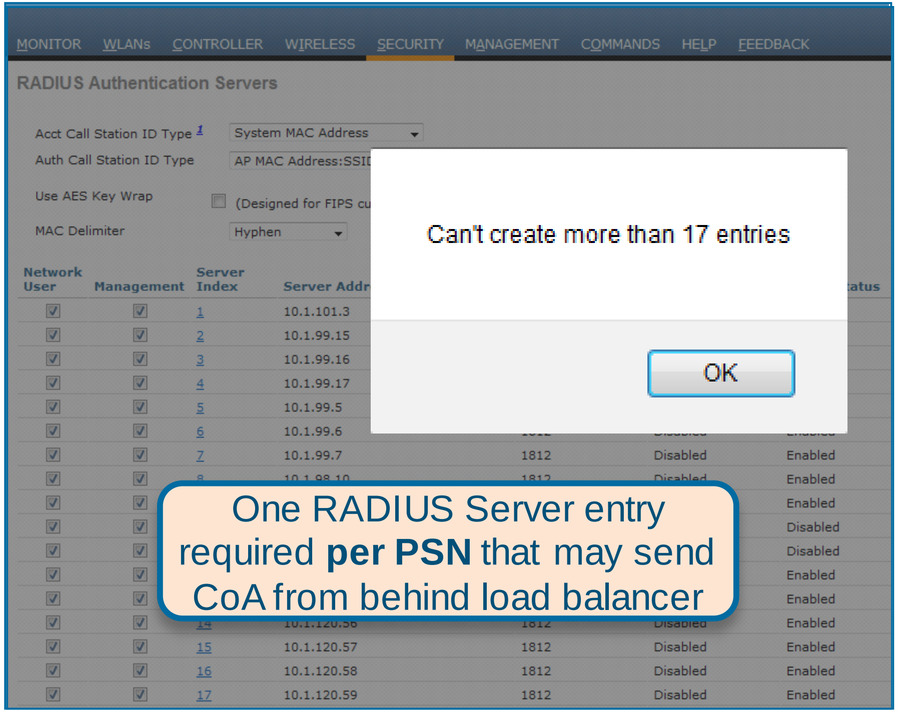
```
aaa server radius dynamic-author
 client 10.1.98.8 server-key cisco123
```



Allow NAT for PSN CoA Requests

Simplifying WLC CoA Configuration

- Before:



RADIUS Authentication Servers

Acct Call Station ID Type [1] System MAC Address

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap □ (Designed for FIPS cu

MAC Delimiter Hyphen

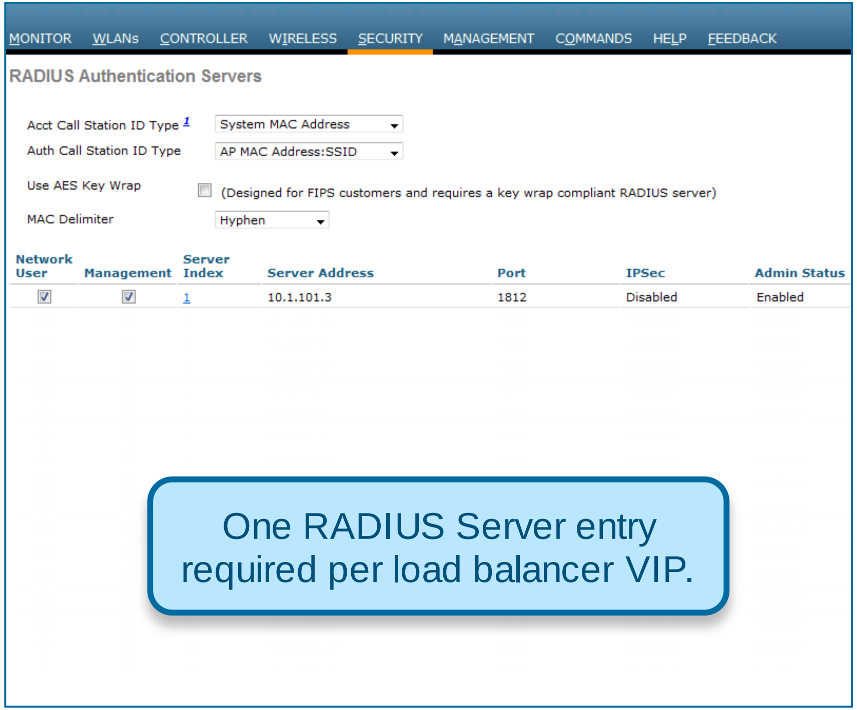
Can't create more than 17 entries

OK

Network User	Management	Server Index	Server Addr			atus
☑	☑	1	10.1.101.3			
☑	☑	2	10.1.99.15			
☑	☑	3	10.1.99.16			
☑	☑	4	10.1.99.17			
☑	☑	5	10.1.99.5			
☑	☑	6	10.1.99.6	1812	Disabled	Enabled
☑	☑	7	10.1.99.7	1812	Disabled	Enabled
☑	☑	8	10.1.98.10	1812	Disabled	Enabled
☑	☑					Enabled
☑	☑					Disabled
☑	☑					Disabled
☑	☑					Enabled
☑	☑					Enabled
☑	☑	14	10.1.120.56	1812	Disabled	Enabled
☑	☑	15	10.1.120.57	1812	Disabled	Enabled
☑	☑	16	10.1.120.58	1812	Disabled	Enabled
☑	☑	17	10.1.120.59	1812	Disabled	Enabled

One RADIUS Server entry required **per PSN** that may send CoA from behind load balancer

- After



RADIUS Authentication Servers

Acct Call Station ID Type [1] System MAC Address

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

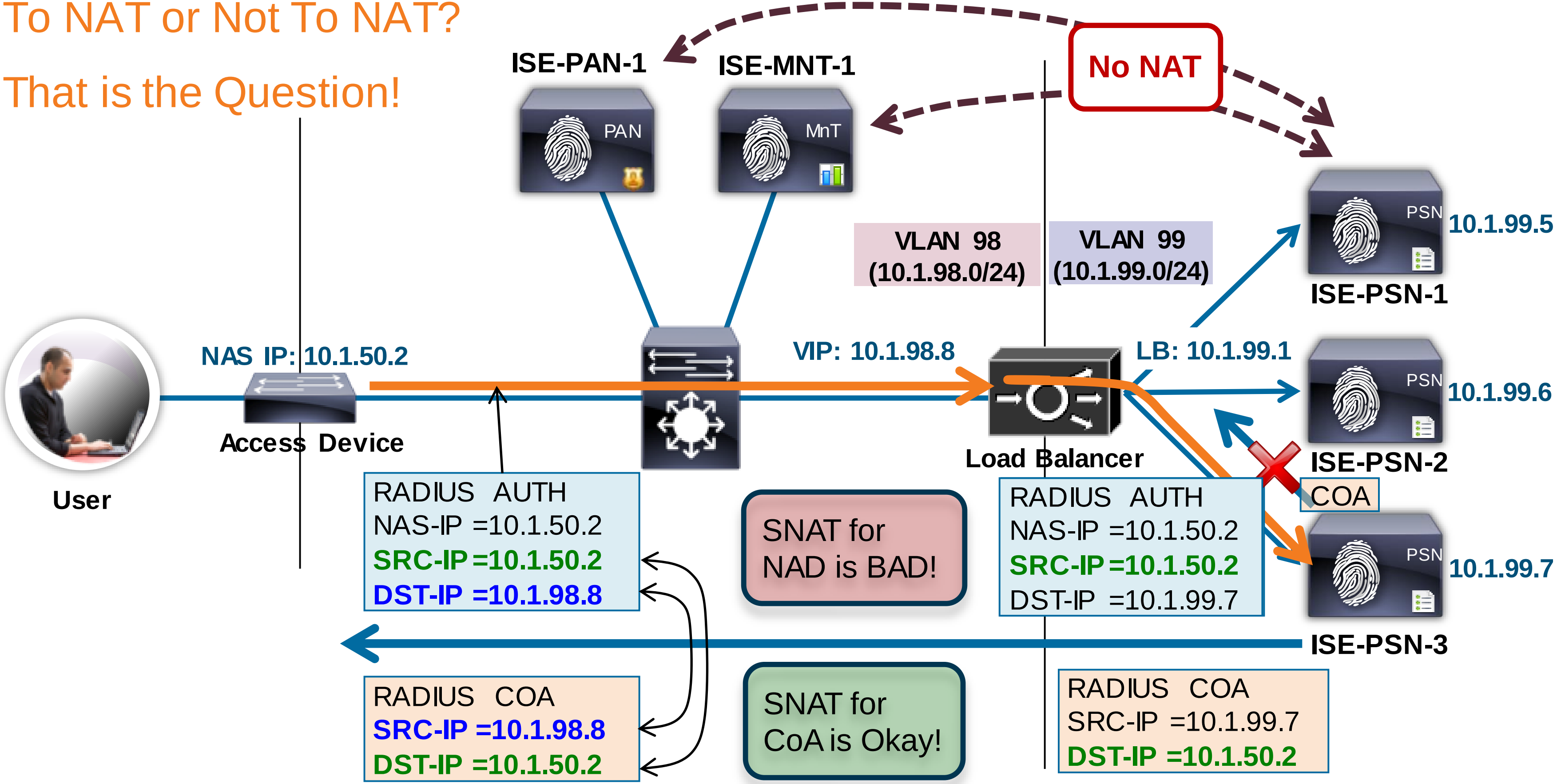
Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
☑	☑	1	10.1.101.3	1812	Disabled	Enabled

One RADIUS Server entry required per load balancer VIP.

NAT Guidelines for ISE RADIUS Load Balancing

To NAT or Not To NAT?

That is the Question!



RADIUS AUTH
NAS-IP =10.1.50.2
SRC-IP =10.1.50.2
DST-IP =10.1.98.8

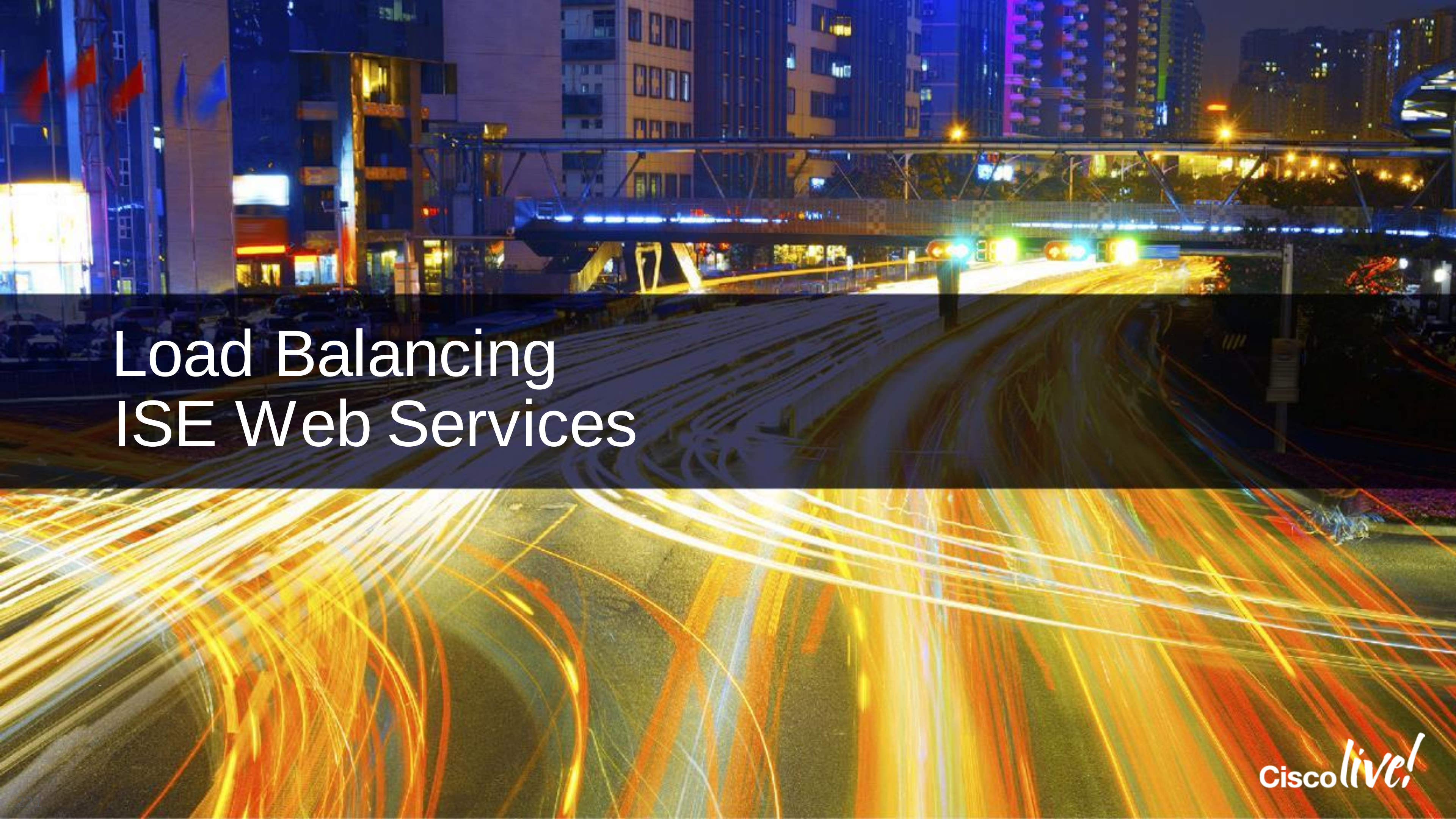
SNAT for NAD is BAD!

RADIUS AUTH
NAS-IP =10.1.50.2
SRC-IP =10.1.50.2
DST-IP =10.1.99.7

RADIUS COA
SRC-IP =10.1.98.8
DST-IP =10.1.50.2

SNAT for CoA is Okay!

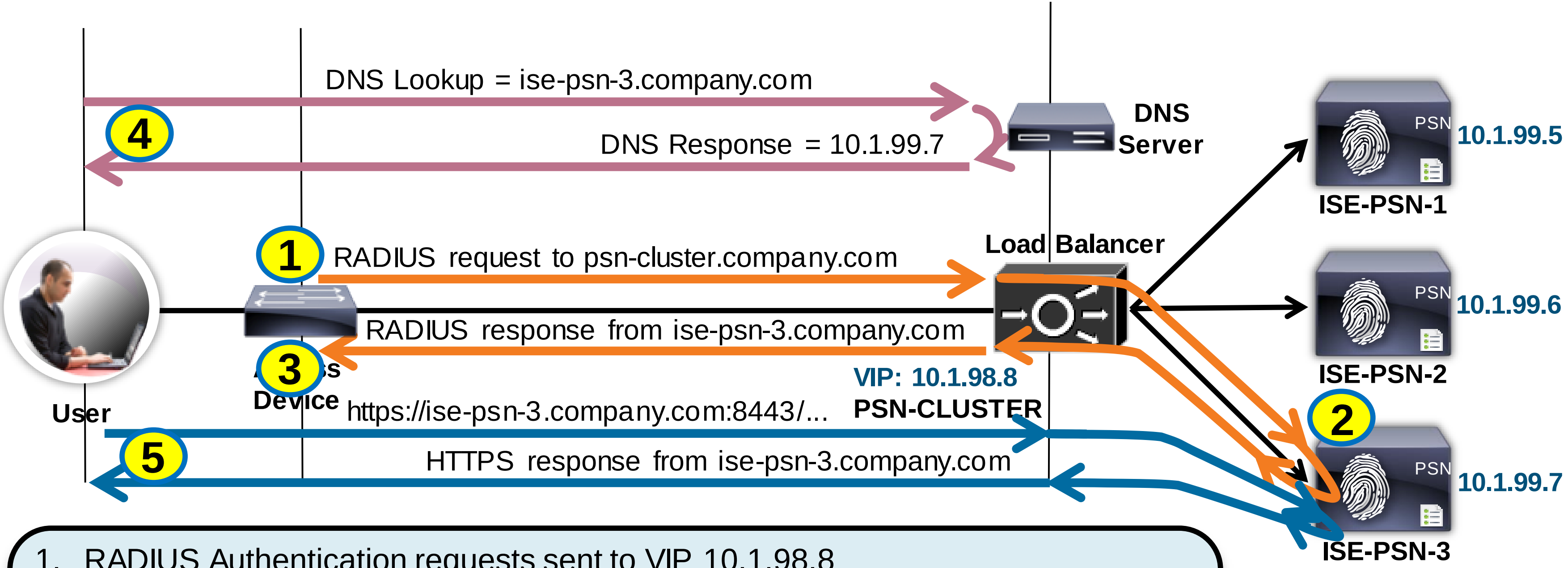
RADIUS COA
SRC-IP =10.1.99.7
DST-IP =10.1.50.2



Load Balancing
ISE Web Services

Load Balancing with URL-Redirection

Sample Flow


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

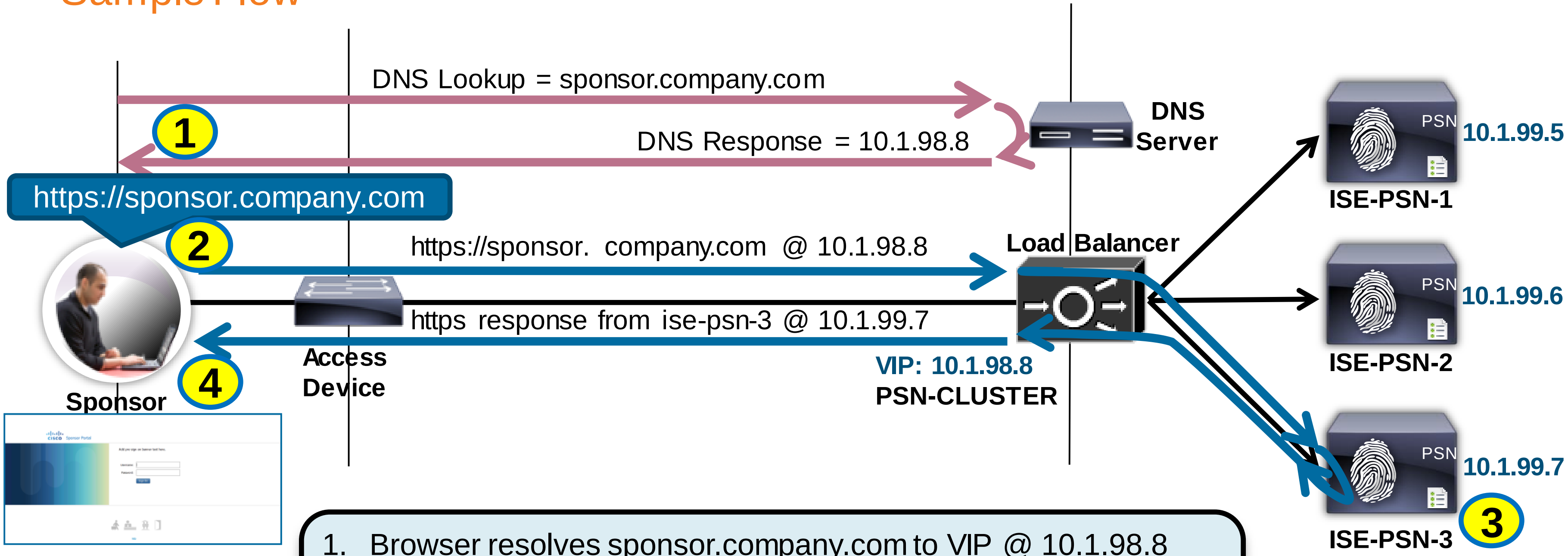
1. RADIUS Authentication requests sent to VIP 10.1.98.8
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorisation received from ise-psn-3 @ 10.1.99.7 with URL Redirect to https://ise-psn-3.company.com:8443/...
4. Client browser redirected and resolves FQDN in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

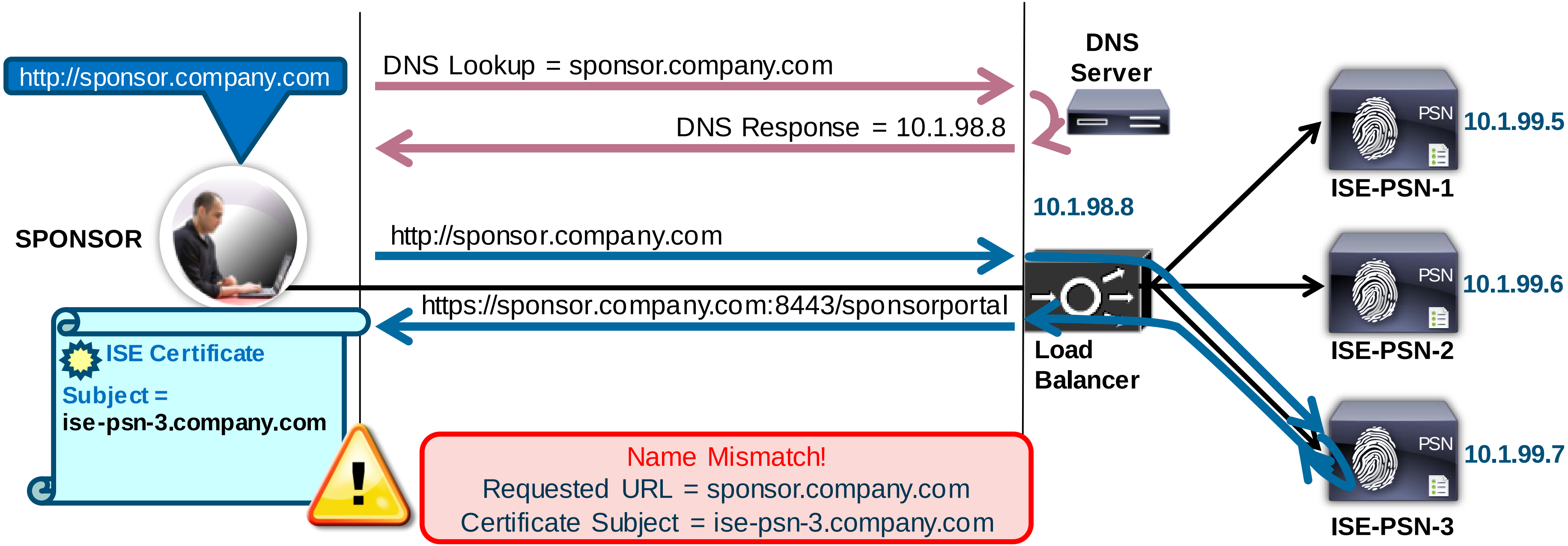
Sample Flow



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

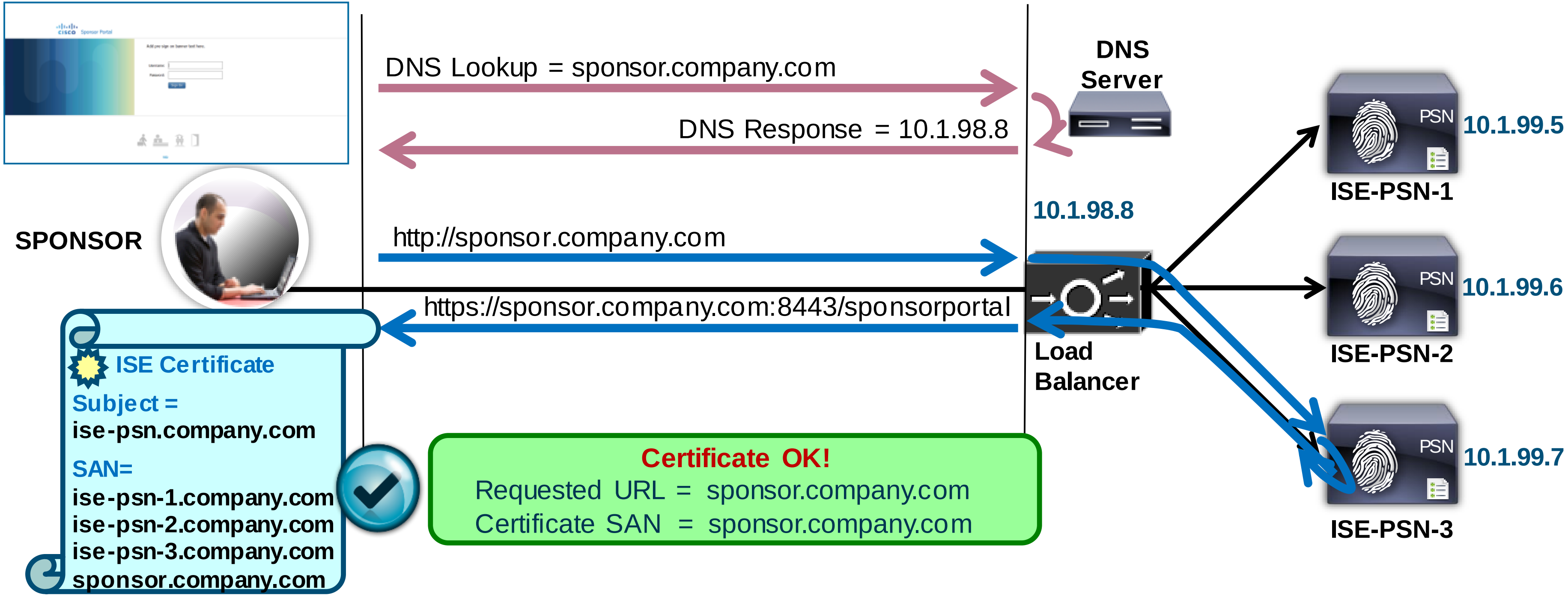
ISE Certificate without SAN

Certificate Warning - Name Mismatch


http://sponsor.company.com
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-3.company.com
Name Mismatch!
Requested URL = sponsor.company.com
Certificate Subject = ise-psn-3.company.com

ISE Certificate with SAN

No Certificate Warning



DNS Lookup = sponsor.company.com

DNS Response = 10.1.98.8

DNS Server

http://sponsor.company.com

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

SPONSOR

10.1.98.8

Load Balancer

ISE-PSN-1 10.1.99.5

ISE-PSN-2 10.1.99.6

ISE-PSN-3 10.1.99.7

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

Load Balancing Preparation

Configure DNS and Certificates

- Configure DNS entry for PSN cluster(s) and assign VIP IP address.

  Example: psn-cluster.company.com

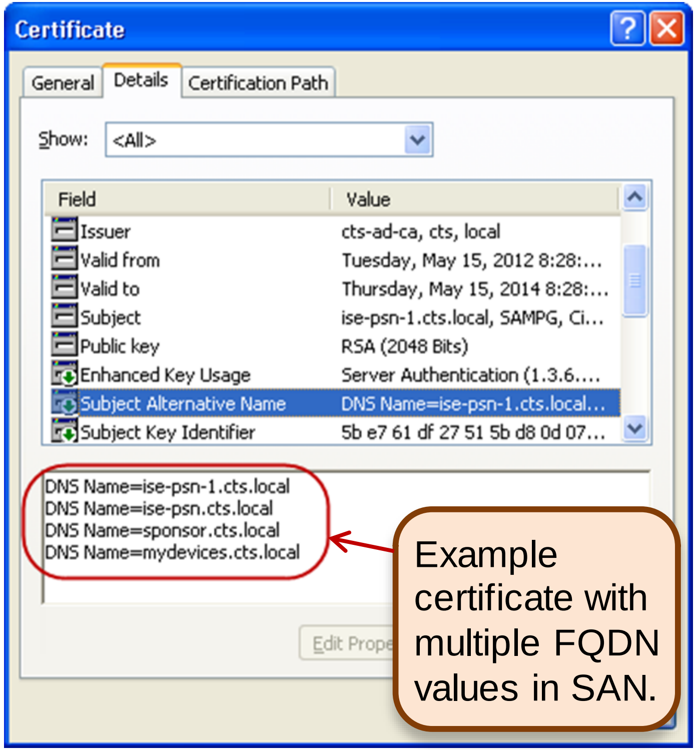
```
DNS SERVER:  DOMAIN = COMPANY.COM

PSN-CLUSTER      IN    A     10.1.98.8
SPONSOR          IN    A     10.1.98.8
MYDEVICES        IN    A     10.1.98.8

ISE-PSN-1        IN    A     10.1.99.5
ISE-PSN-2        IN    A     10.1.99.6
ISE-PSN-3        IN    A     10.1.99.7
```

- Configure ISE PSN server certs with Subject Alternative Name configured for other FQDNs to be used by LB VIP or optionally use wildcards (available in ISE 1.2).

  Example certificate SAN: ise-psn-1.company.com
  psn-cluster.company.com
  sponsor.company.com
  guest.company.com



Show: <All>

Field	Value
Issuer	cts-ad-ca, cts, local
Valid from	Tuesday, May 15, 2012 8:28:...
Valid to	Thursday, May 15, 2014 8:28:...
Subject	ise-psn-1.cts.local, SAMPG, Ci...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=ise-psn-1.cts.local...
Subject Key Identifier	5b e7 61 df 27 51 5b d8 0d 07...

DNS Name=ise-psn-1.cts.local
DNS Name=ise-psn.cts.local
DNS Name=sponsor.cts.local
DNS Name=mydevices.cts.local

Example certificate with multiple FQDN values in SAN.

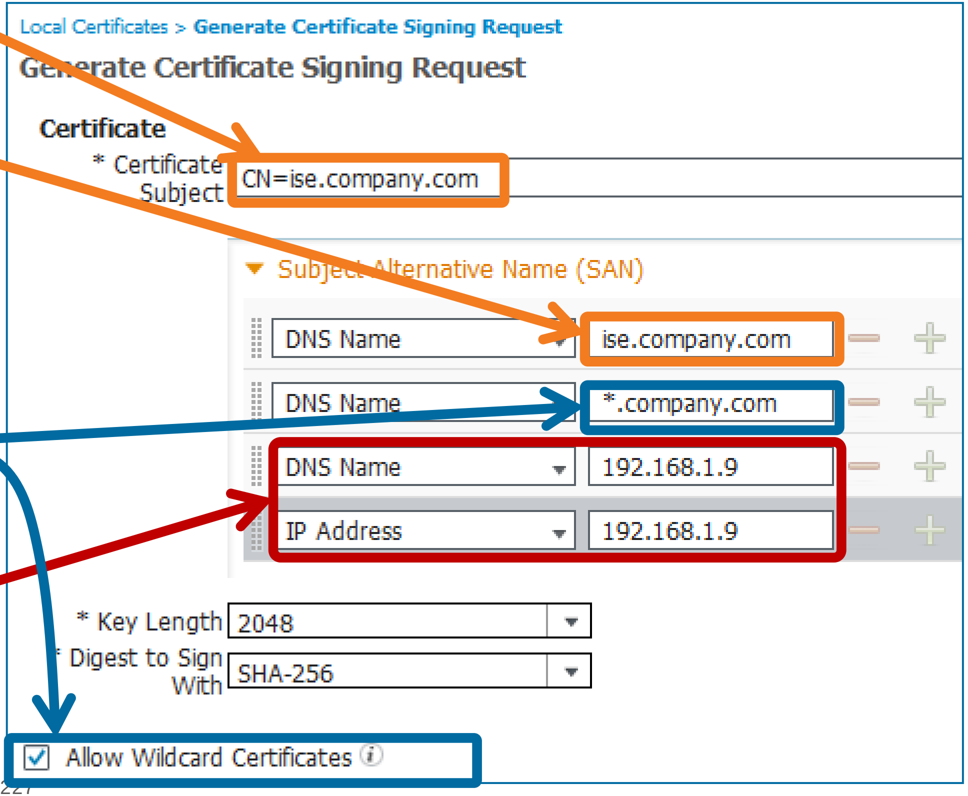
General Best Practices for Universal Certificates

- Use a common FQDN for Subject CN:
  Examples: ise.company.com
  aaa.company.com
- If Subject CN contains FQDN, add same FQDN to SAN
- Multi-Domain/UCC* Certificate: Update SAN with all FQDNs serviced by PSN

  OR

  Wildcard Certificate: Update SAN with wildcard domain using syntax *.company.local
- If required for static IP hosting, add IP addresses as both DNS and IP entries (increases device compatibility)

*UCC = Unified Communications Certificate



Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject: CN=ise.company.com

▾ Subject Alternative Name (SAN)

DNS Name	ise.company.com
DNS Name	*.company.com
DNS Name	192.168.1.9
IP Address	192.168.1.9

* Key Length: 2048

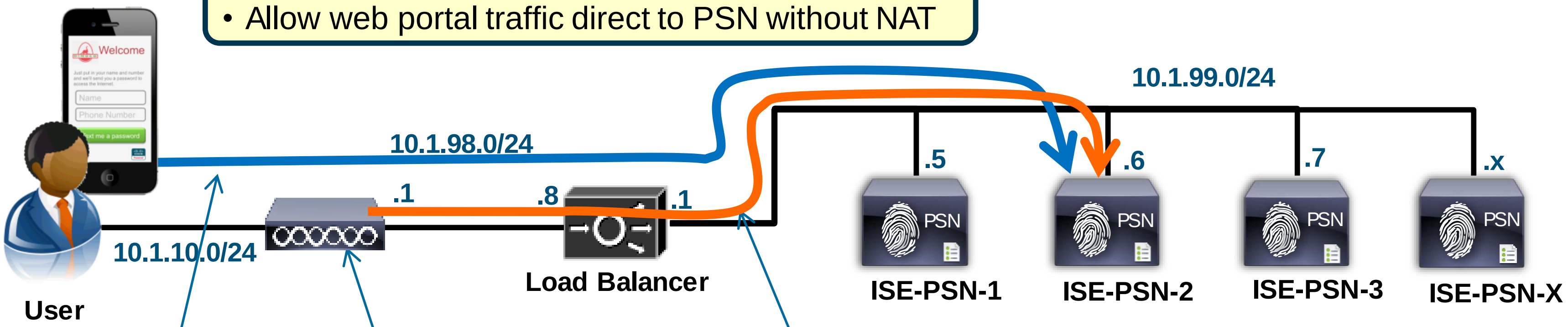
* Digest to Sign With: SHA-256

☑ Allow Wildcard Certificates

Load Balancer NAT Guidelines for Web Traffic

URL-Redirected Traffic with Single PSN Interface

- No NAT Required
- Allow web portal traffic direct to PSN without NAT



RADIUS session load-balanced to PSN @ **10.1.99.6**

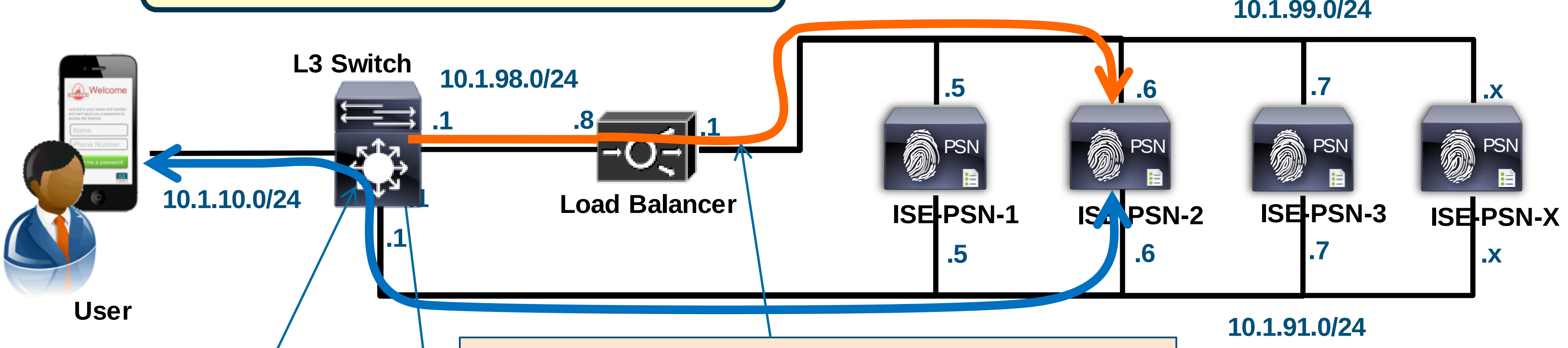
URL Redirect automatically includes FQDN/Interface IP of same PSN @ **10.1.99.6**
https://**ise-psn-2.company.com**:8443/guestportal/Login...

Browser traffic redirected to IP for ise-psn-2.company.com:
https://**10.1.99.6**:8443/guestportal/Login...

SNAT on L3 Switch for Dedicated Web Interfaces (ISE 1.2)

URL-Redirected Traffic with Dedicated PSN Interface for Web Portals (Single LB interface)

- Source NAT portal traffic to simplify routing
- Maintains Path Isolation



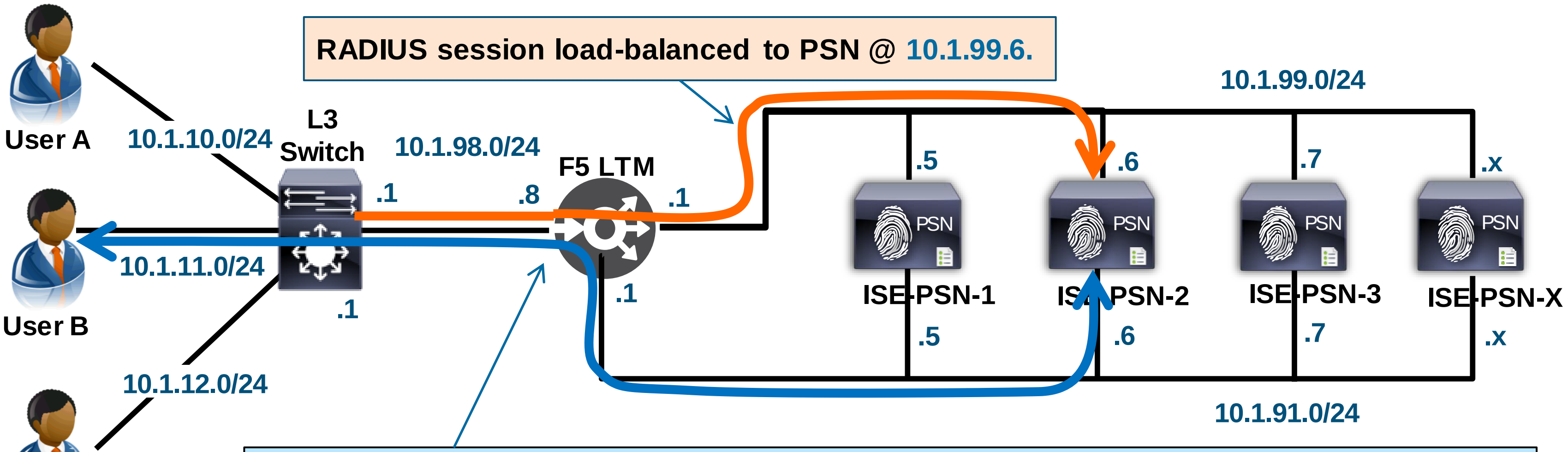
RADIUS session load-balanced to PSN @ **10.1.99.6.**

URL Redirect automatically includes FQDN/Interface IP of Web Portal interface for same PSN @ **10.1.91.6**: https://**ise-psn-2-guest.company.com**:8443/guestportal/Login...

Source NAT web traffic from user networks destined to PSN web interfaces @ 10.1.91.x; translate to 10.1.91.x (or any address block that can be statically added to PSN route table)
Ensures all Web requests received by PSN web interface are returned out same interface.

SNAT on LB for Dedicated Web Interfaces (ISE 1.2)

Direct Access and URL-Redirected Traffic with Dedicated PSN Web Interfaces

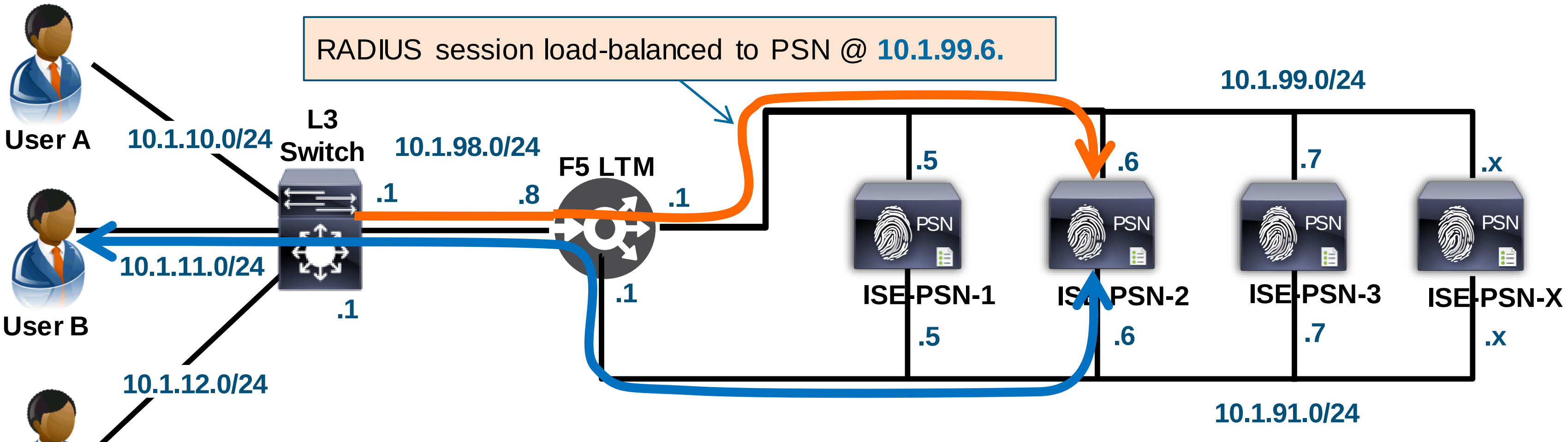


Direct-Access Portals:
Enable SNAT on Virtual Servers for ISE Sponsor, My Devices, and LWA portals.

URL-Redirected Web Portals/Services:
Enable SNAT on F5 LTM IP Forwarding Virtual Servers.

Dedicated Web Interfaces Under ISE 1.3

Direct Access and URL-Redirected Traffic with Dedicated PSN Web Interfaces



Response to traffic received on an interface sent out same interface if default route exists for interface: **No SNAT required!**

Default route 0.0.0.0/0 10.1.99.1 eth0
Default route 0.0.0.0/0 10.1.91.1 eth1

Dedicated Web Interfaces Under ISE 1.3

Symmetric Traffic Flows

- Configure default routes for each interface to support symmetric return traffic

```
ise13-psn-x/admin# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ise13-psn-x/admin(config)#  ip route 0.0.0.0 0.0.0.0 gateway 10.1.91.1
```

- Validate new default route

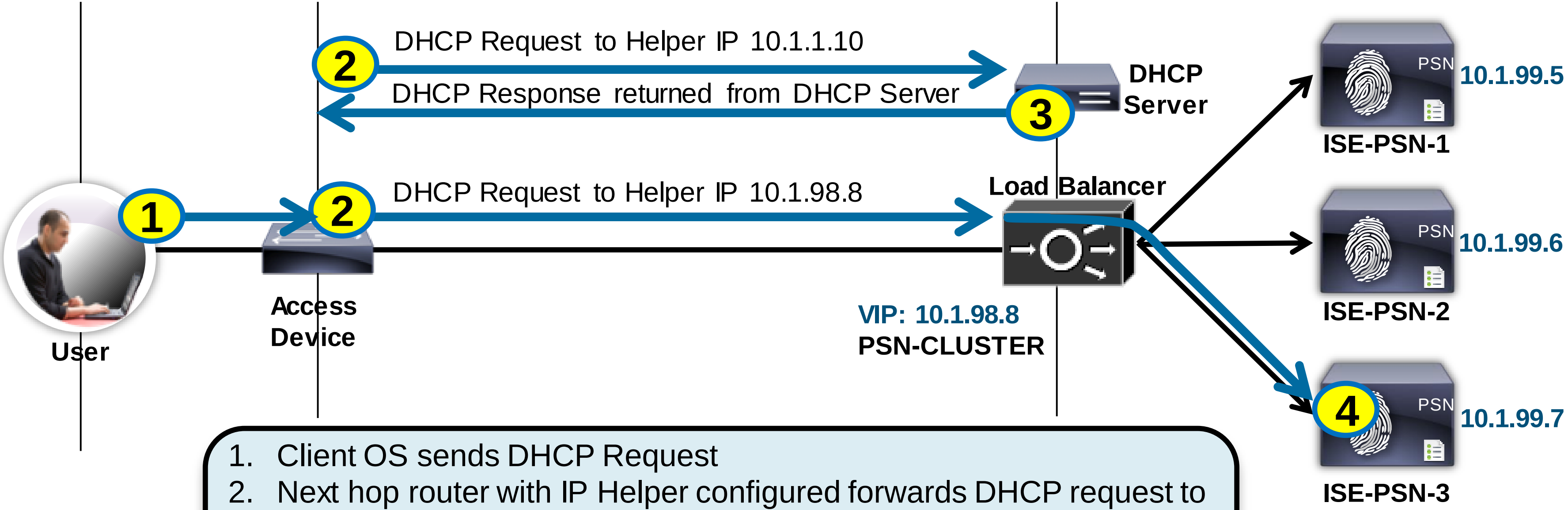
```
ise13-psn-x/admin# sh ip route

Destination          Gateway              Iface
-----------          -------              -----
10.1.91.0/24         0.0.0.0              eth1
10.1.99.0/24         0.0.0.0              eth0
default              10.1.91.1            eth1
default              10.1.99.1            eth0
```

Load Balancing
ISE Profiling Services

Load Balancing Profiling Services

Sample Flow



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

Load Balancing Simplifies Device Configuration

L3 Switch Example for DHCP Relay

- Before

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

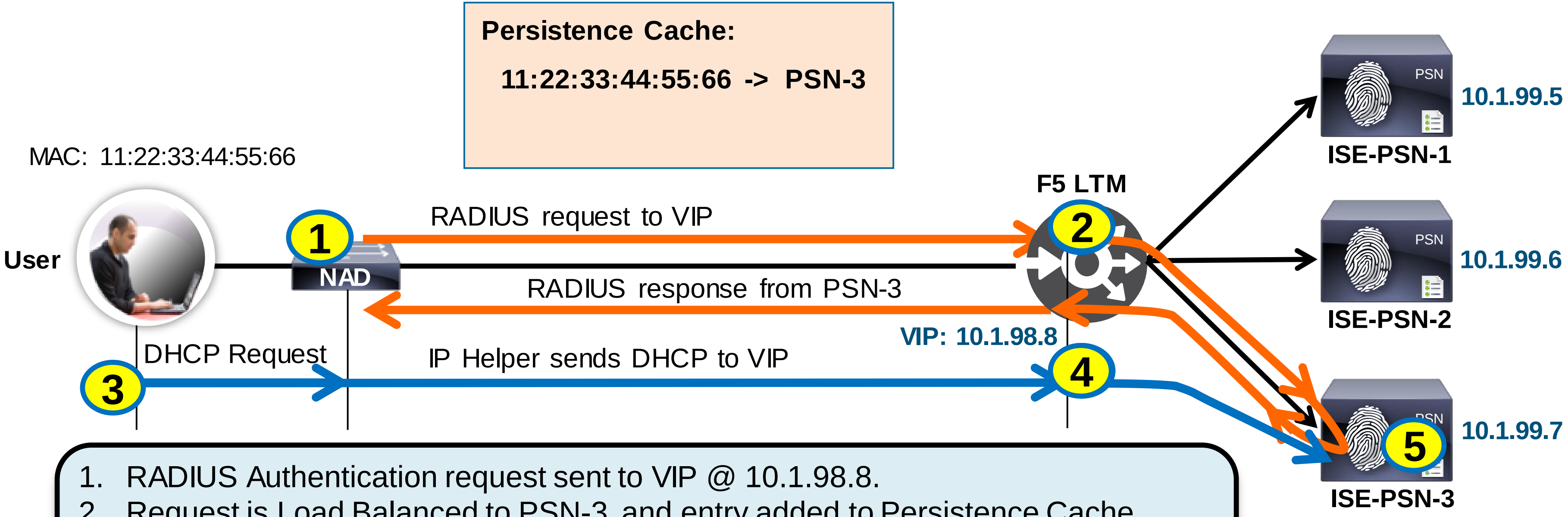
- After

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

Settings apply to each L3 interface servicing DHCP endpoints

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

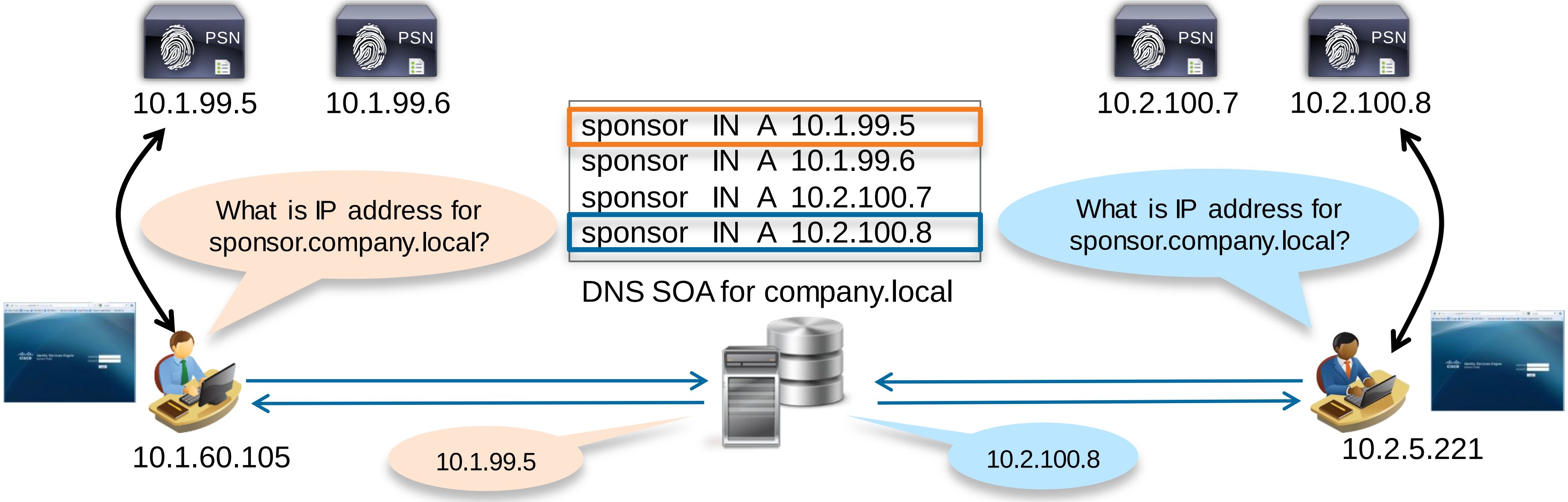
PSN HA Without Load Balancers

How can my company get HA and scalability 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.



PSN 10.1.99.5

PSN 10.1.99.6

PSN 10.2.100.7

PSN 10.2.100.8

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

DNS SOA for company.local

What is IP address for sponsor.company.local?

10.1.60.105

10.1.99.5

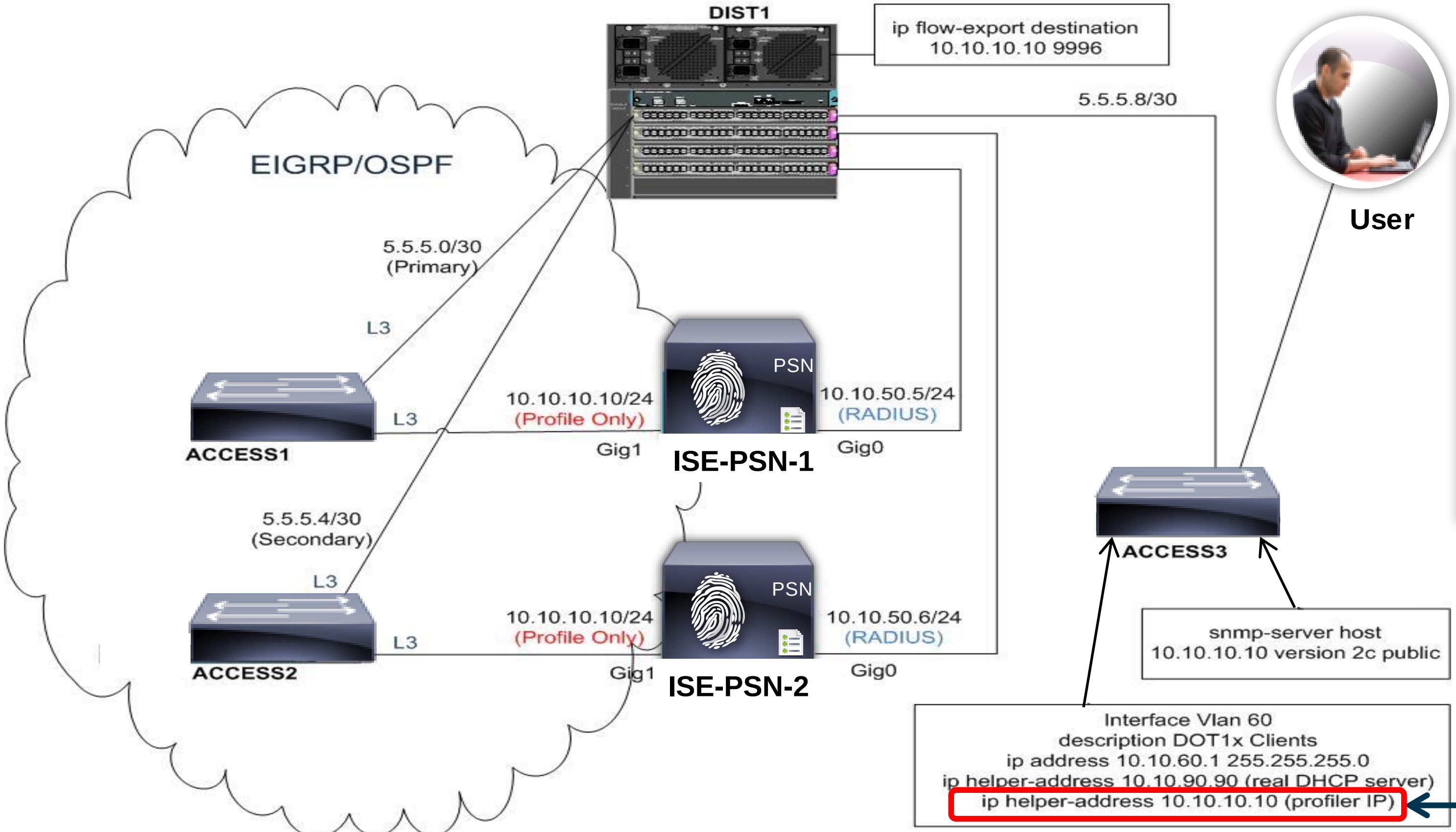
What is IP address for sponsor.company.local?

10.2.5.221

10.2.100.8

Using Anycast for ISE Redundancy

Profiling Example



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

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

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

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

NADs are configured with single Anycast IP address.

Ex: 10.10.10.10

ISE Configuration for Anycast

On each PSN that will participate in Anycast…

1. Configure PSN probes to profile DHCP (IP Helper), SNMP Traps, or NetFlow on dedicated interface

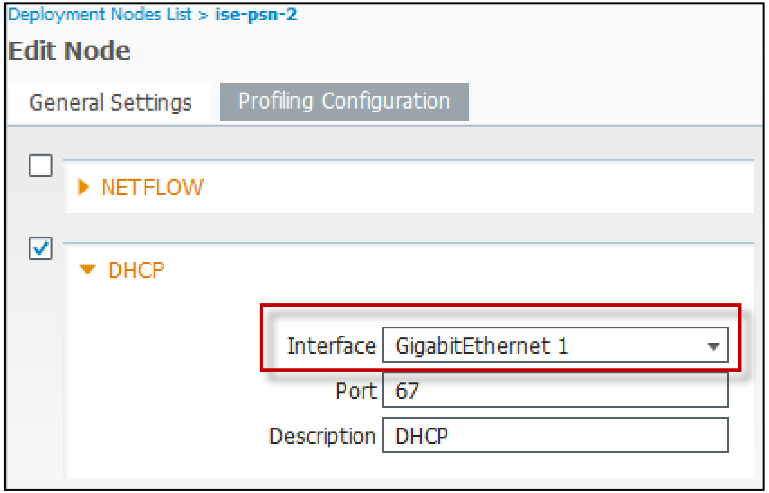
2. From CLI, configure dedicated interface with same IP address on each PSN node.

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
```



□ NETFLOW

☑ DHCP

Interface: GigabitEthernet 1

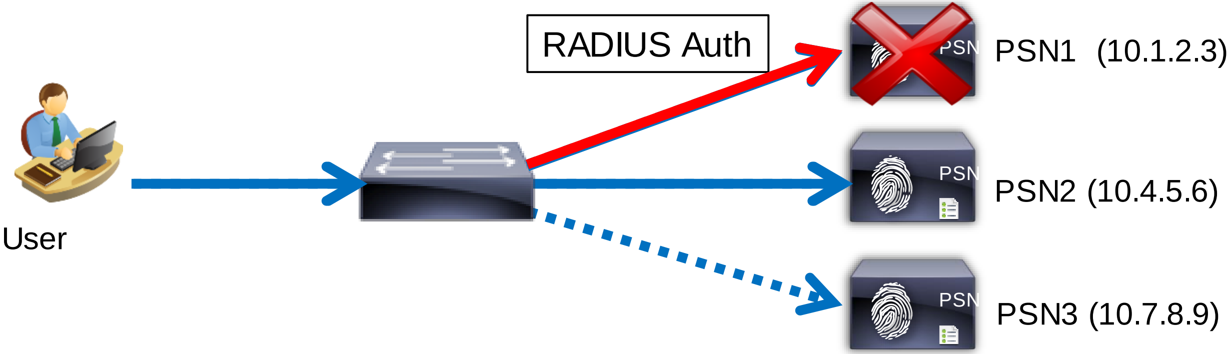
Port: 67

Description: DHCP

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

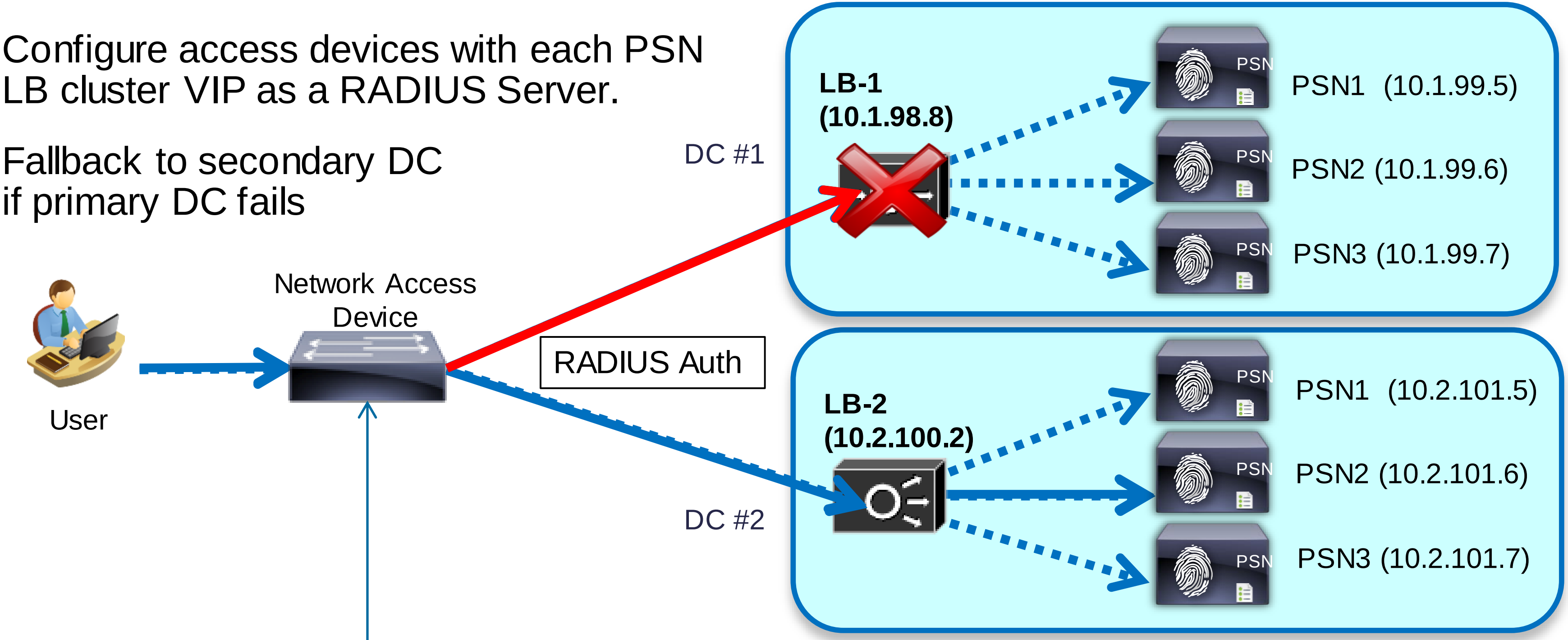


```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

NAD-Based Redundancy to Different LB Clusters

RADIUS Example – Different RADIUS VIP Addresses

- Configure access devices with each PSN LB cluster VIP as a RADIUS Server.
- Fallback to secondary DC if primary DC fails

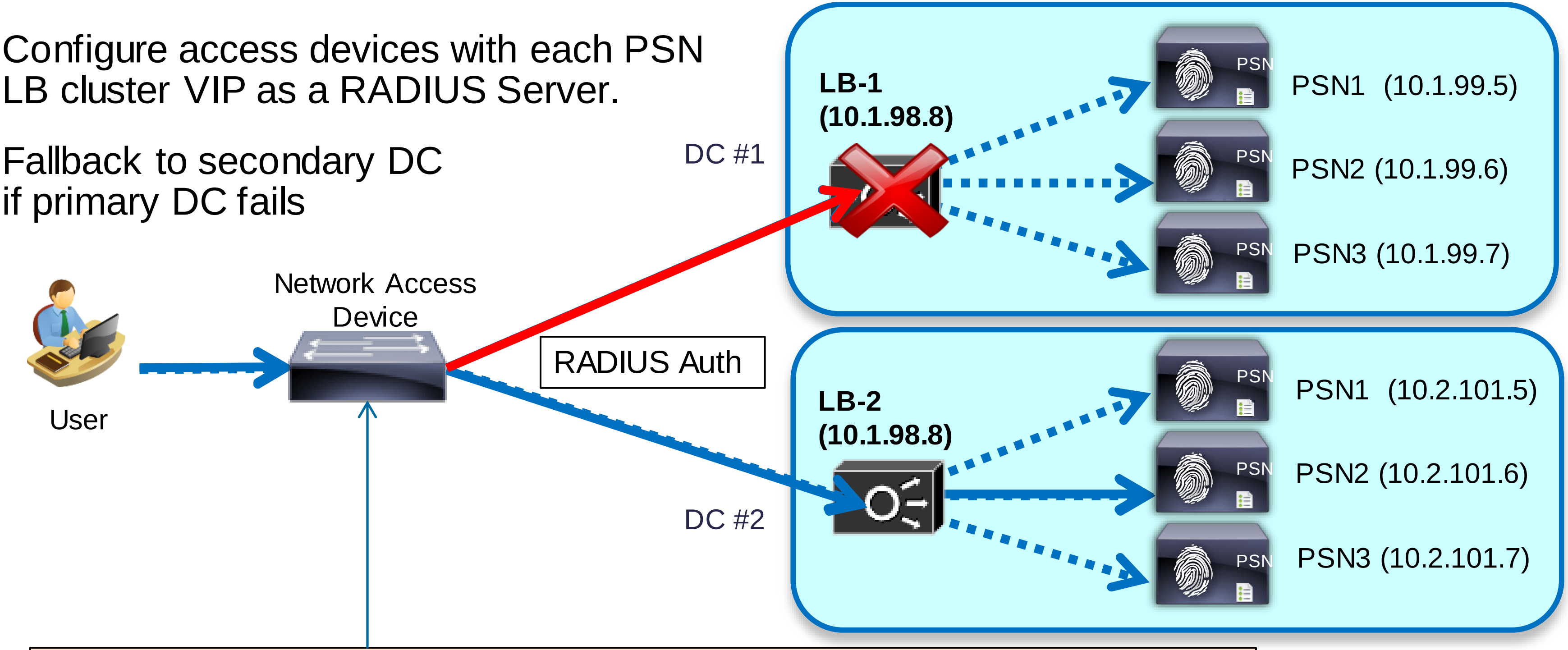


```
radius-server host 10.1.98.8 auth-port 1812 acct-port 1813
radius-server host 10.2.100.2 auth-port 1812 acct-port 1813
```

NAD-Based Redundancy to Different LB Clusters

RADIUS Example – Single RADIUS VIP Address using Anycast

- Configure access devices with each PSN LB cluster VIP as a RADIUS Server.
- Fallback to secondary DC if primary DC fails

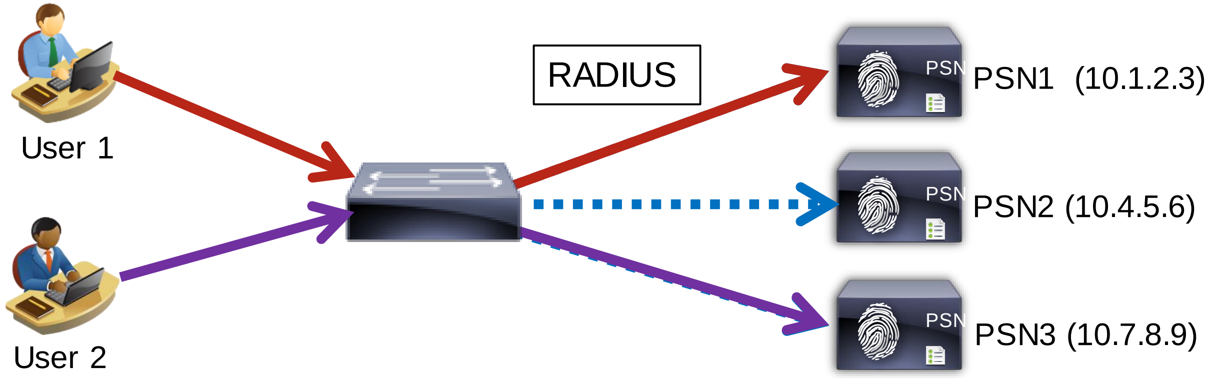


```
radius-server host 10.1.98.8 auth-port 1812 acct-port 1813
```

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.



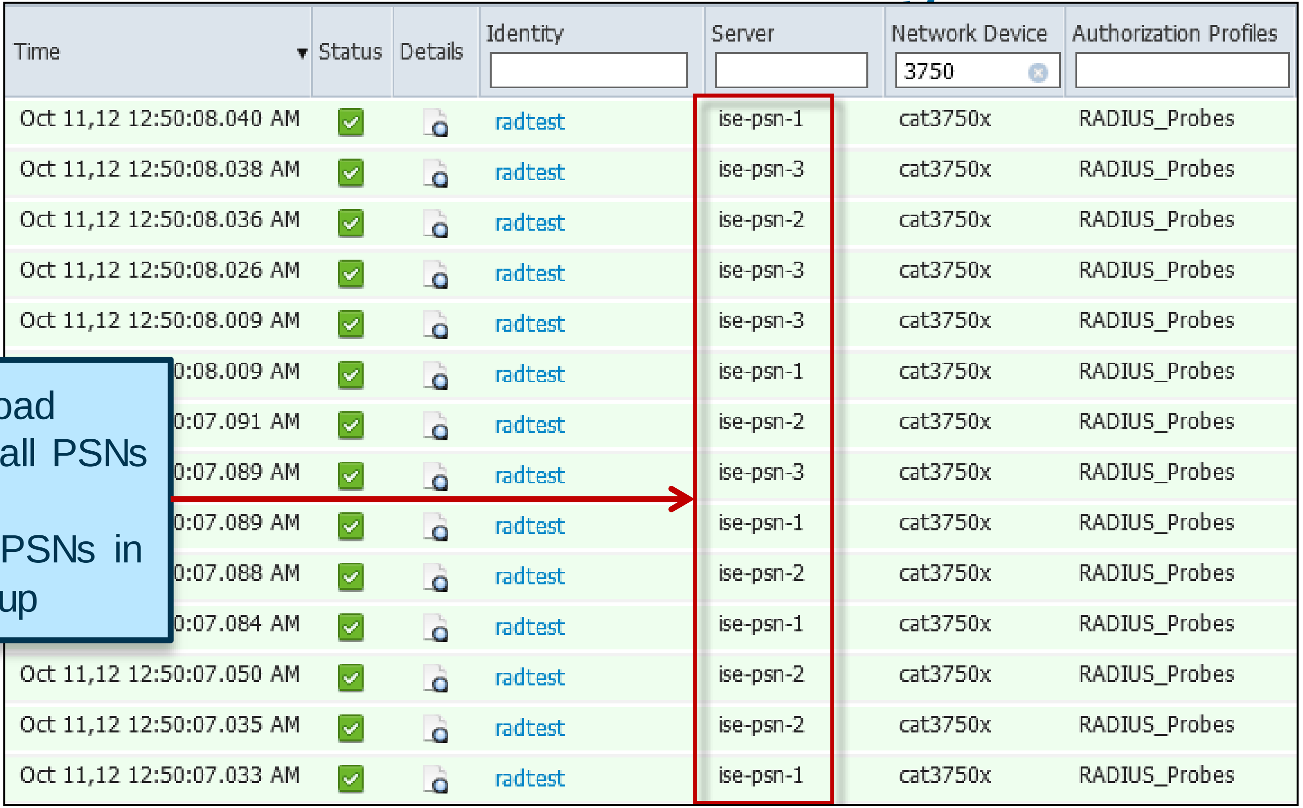
NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

```
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 3750	Authorization Profiles
Oct 11,12 12:50:08.040 AM	☑	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.038 AM	☑	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.036 AM	☑	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.026 AM	☑	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.009 AM	☑	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:08.009 AM	☑	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.091 AM	☑	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.089 AM	☑	🔍	radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:07.089 AM	☑	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.088 AM	☑	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.084 AM	☑	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.050 AM	☑	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.035 AM	☑	🔍	radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.033 AM	☑	🔍	radtest	ise-psn-1	cat3750x	RADIUS_Probes

Reasonable load distribution across all PSNs

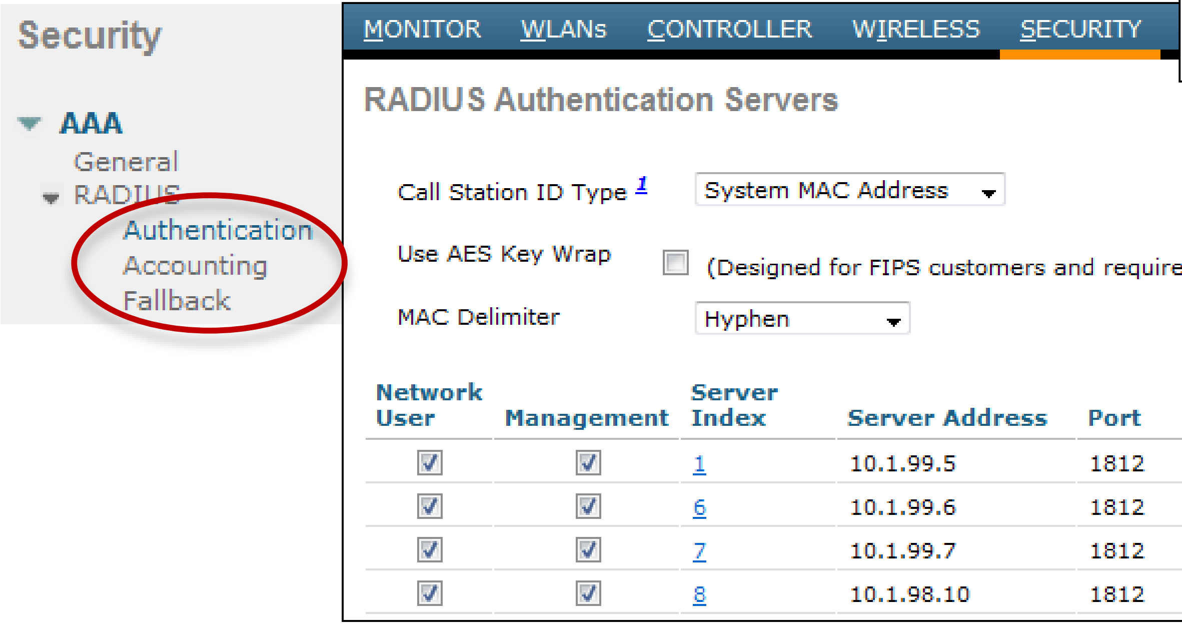
Example shows 3 PSNs in RADIUS group

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

NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

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



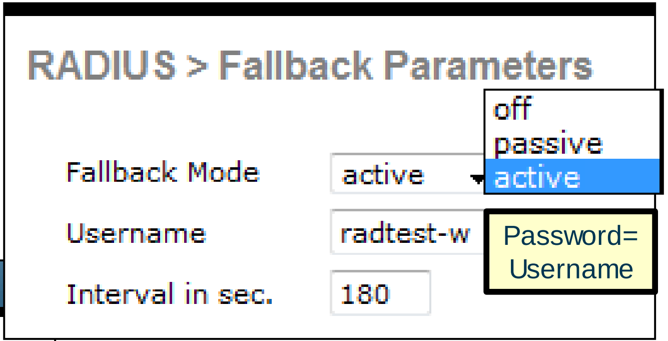
RADIUS Authentication Servers

Call Station ID Type [1] System MAC Address

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

MAC Delimiter Hyphen

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



RADIUS > Fallback Parameters

Fallback Mode active

Username radtest-w

Interval in sec. 180

Password= Username

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.

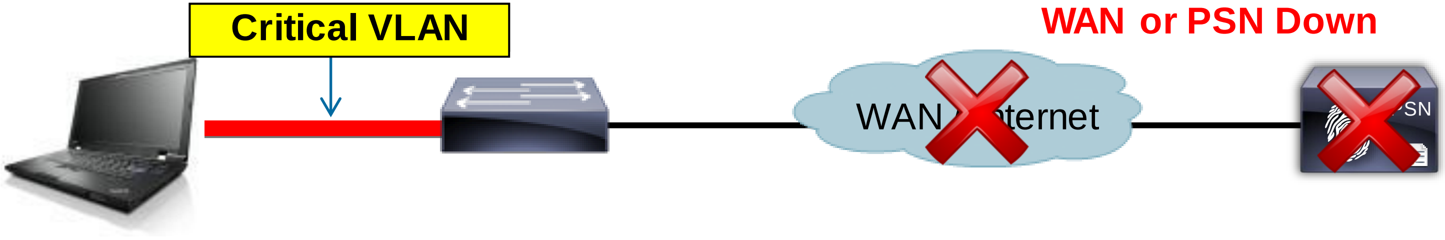
Active = Mark failed server dead then actively probe status per interval w/username until succeed before return to list; always preempt.

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

NAD Fallback and Recovery

Inaccessible Authentication Bypass (IAB)

Also Known As “Critical Auth VLAN” for Data

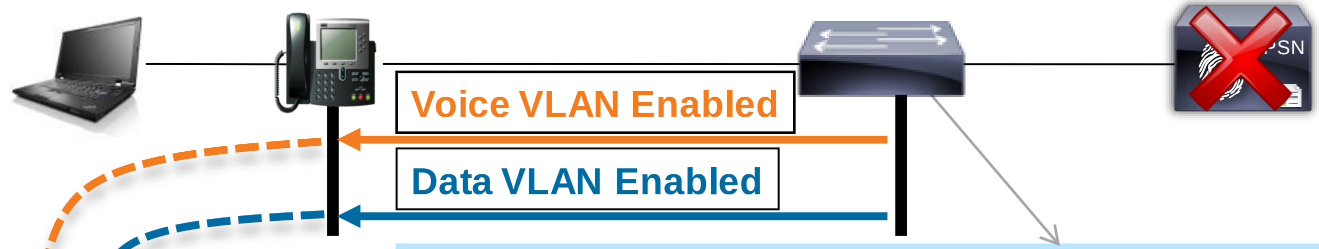


- Switch detects PSN unavailable by one of two methods
  - Periodic probe
  - Failure to respond to AAA request
- Enables port in critical VLAN
- Existing sessions retain authorisation status
- Recovery action can re-initialise port when AAA returns

Critical VLAN can be anything:
- Same as default access VLAN
- Same as guest/auth-fail VLAN
- New VLAN

```
authentication event server dead action authorize vlan 100
authentication event server alive action reinitialize
```

Critical Auth for Data and Voice



```
interface fastEthernet 3/48
 dot1x pae authenticator
 authentication port-control auto
 authentication event server dead action authorize vlan x
 authentication event server dead action authorize voice
```

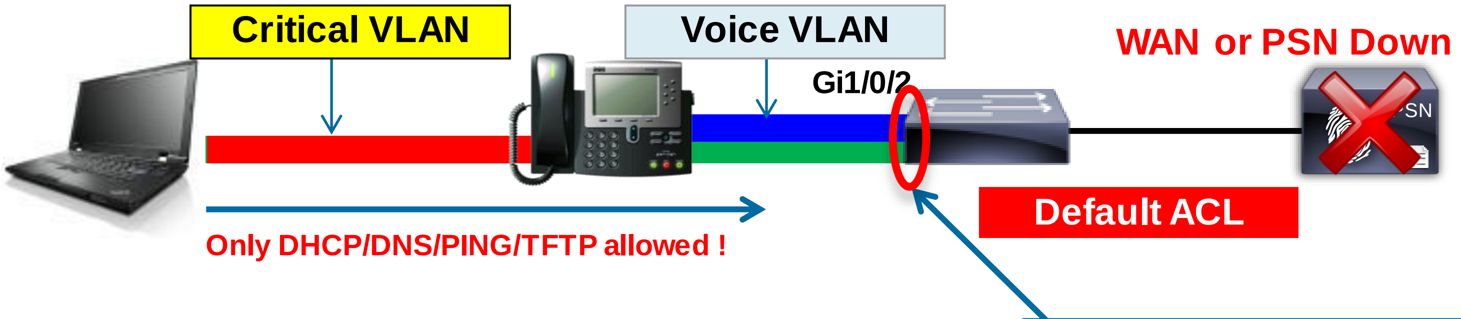
```
# show authentication sessions interface fa3/48
...
```

Critical Authorisation is in effect for domain(s) DATA and VOICE

Default Port ACL Issues with Critical VLAN

Limited Access Even After Authorisation to New VLAN!

- Data VLAN reassigned to critical auth VLAN, but new (or reinitialised) connections are still restricted by existing port ACL!



```
interface GigabitEthernet1/0/2
 switchport access vlan 10 🟩
 switchport voice vlan 13 🟦
 ip access-group ACL-DEFAULT in
 authentication event server dead action reinitialize vlan 11 🟥
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
```

```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
```

Using Embedded Event Manager with Critical VLAN

Modify or Remove/Add Static Port ACLs Based on PSN Availability

- Allows scripted actions to occur based on various conditions and triggers

```
track 1 ip route 10.1.98.0 255.255.255.0 reachability
event manager applet default-acl-fallback
  event track 1 state down maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "ip access-list extended ACL-DEFAULT"
  action 3.0 cli command "1 permit ip any any"
  action 4.0 cli command "end"
event manager applet default-acl-recovery
  event track 1 state up maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "ip access-list extended ACL-DEFAULT"
  action 3.0 cli command "no 1 permit ip any any"
  action 4.0 cli command "end"
```

PROGRIZON

CISCO PARTNER Technology Developer

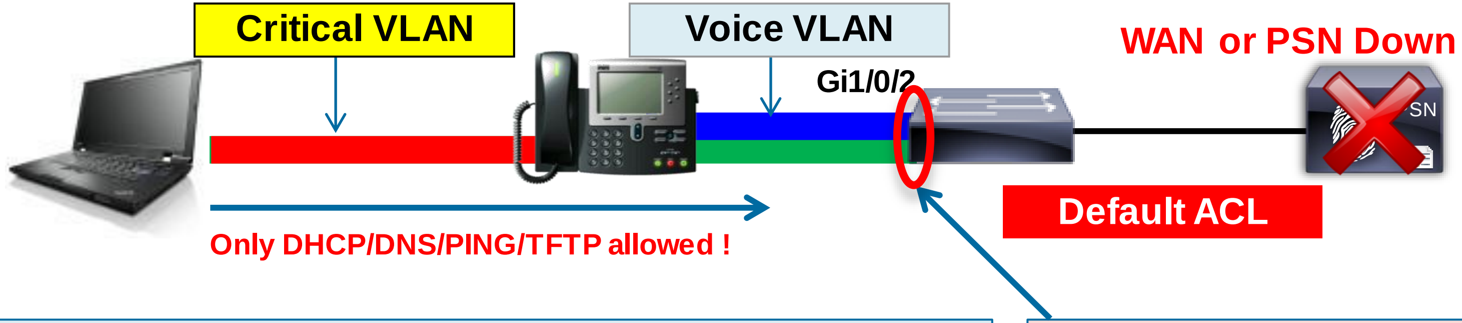
EEM Policy Builder:
www.progrizon.com/support/pb/pb.php

EEM available on Catalyst 3k/4k/6k switches

Critical ACL Using Service Policy Templates

Apply ACL, VLAN, or SGT on RADIUS Server Failure!

- Critical Auth ACL applied on Server Down



```
interface GigabitEthernet1/0/2
 switchport access vlan 10 🟩
 switchport voice vlan 13 🟦
 ip access-group ACL-DEFAULT in
 access-session port-control auto
 mab
 dot1x pae authenticator
 service-policy type control subscriber ACCESS-POLICY
```

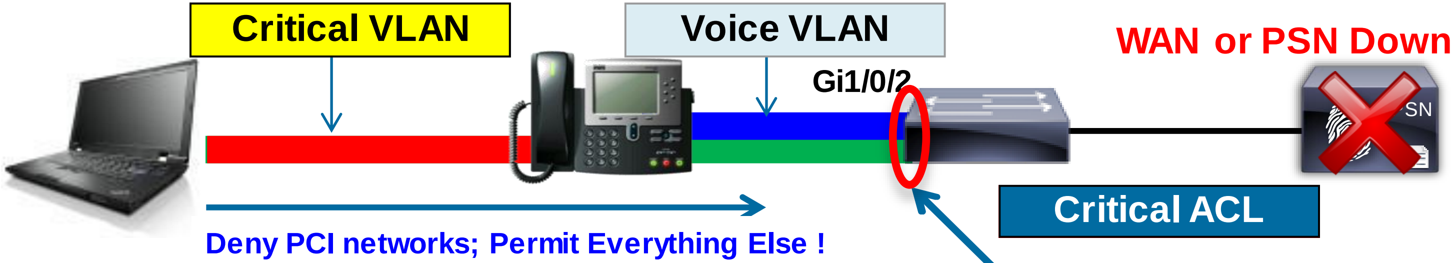
```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
```

Critical ACL Using Service Policy Templates

Apply ACL, VLAN, or SGT on RADIUS Server Failure!

2k/3k/4k: 15.2(1)E
3k IOS-XE: 3.3.0SE
4k: IOS-XE 3.5.0E
6k: 15.2(1)SY

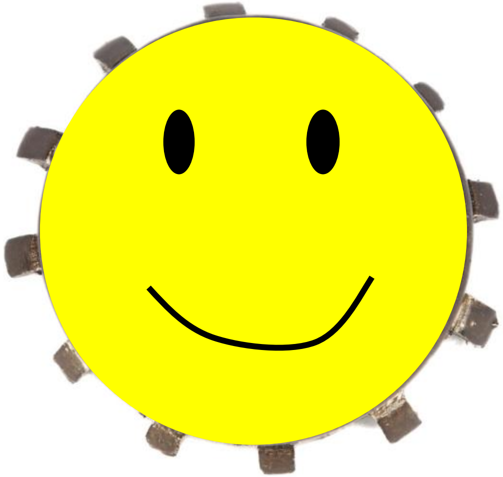
- Critical Auth ACL applied on Server Down



```
policy-map type control subscriber ACCESS-POLICY
 event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 activate service-template CRITICAL-ACCESS
service-template CRITICAL-ACCESS
  access-group ACL-CRITICAL
service-template CRITICAL_AUTH_VLAN
 vlan 10
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
```

```
ip access-list extended ACL-CRITICAL
 remark Deny access to PCI zone scopes
 deny tcp any 172.16.8.0 255.255.240.0
 deny udp any 172.16.8.0 255.255.240.0
 deny ip any 192.168.0.0 255.255.0.0
 permit ip any any
```

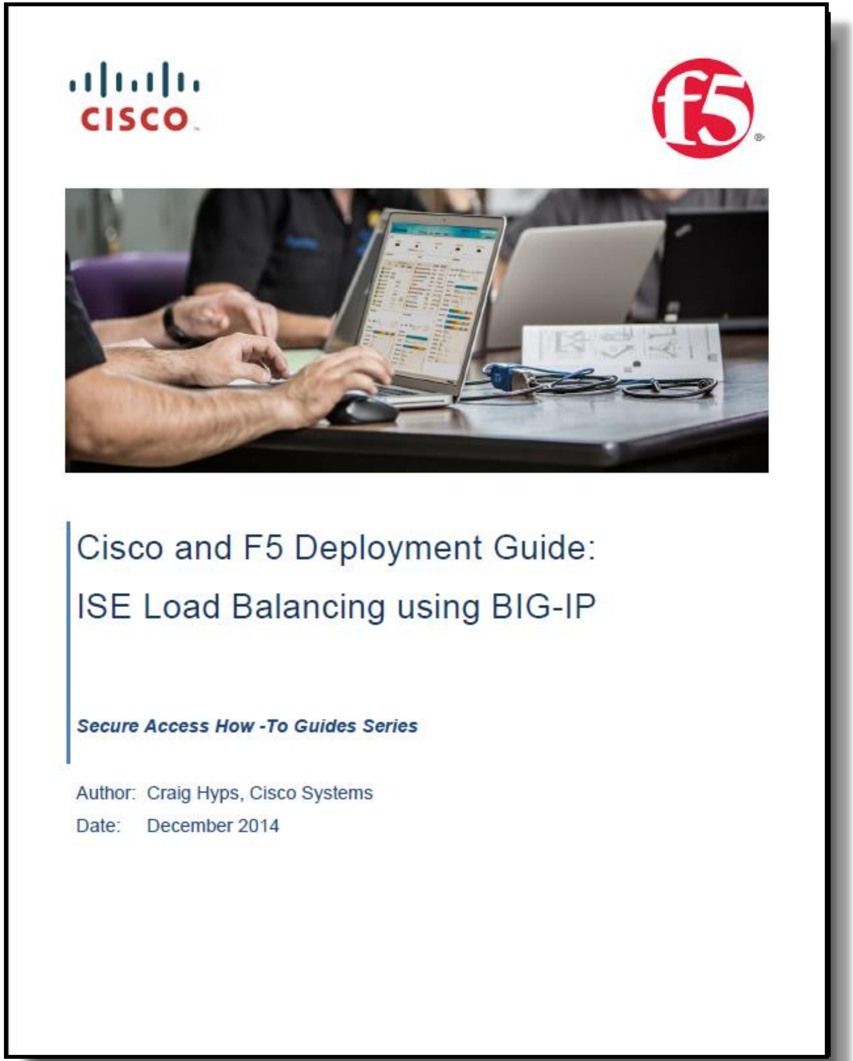
Exiting Large Scale / HA Design Matrix… Okay to Unplug



ISE Scalability and High Availability

Summary Review

- Appliance selection and persona allocation impacts deployment size.
- VM appliances need to be configured per physical appliance sizing specs.
- Profiling scalability tied to DB replication—deploy node groups and optimise PSN collection.
- Leverage ISE 1.2 noise suppression to increase auth capacity and reduce storage reqs.
- ISE 1.3 further enhances scalability with multi-AD and auto-device registration & purge.
- Admin, MnT, pxGrid, and IPN HA based on a Primary to Secondary node failover.
- Load balancers can offer higher scaling and redundancy for PSN clusters.
- Non-LB options include "smart" DNS, AnyCast, multiple RADIUS server definitions in the access devices, and IOS RADIUS LB.
- Special consideration must be given to NAD fallback and recovery options when no RADIUS servers are available including Critical Auth VLANs for data and voice.
- IBNS 2.0 and EEM offer advanced local intelligence in failover scenarios.



Cisco and F5 Deployment Guide:

ISE Load Balancing using BIG-IP

Secure Access How -To Guides Series

Author: Craig Hyps, Cisco Systems

Date: December 2014

Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP:

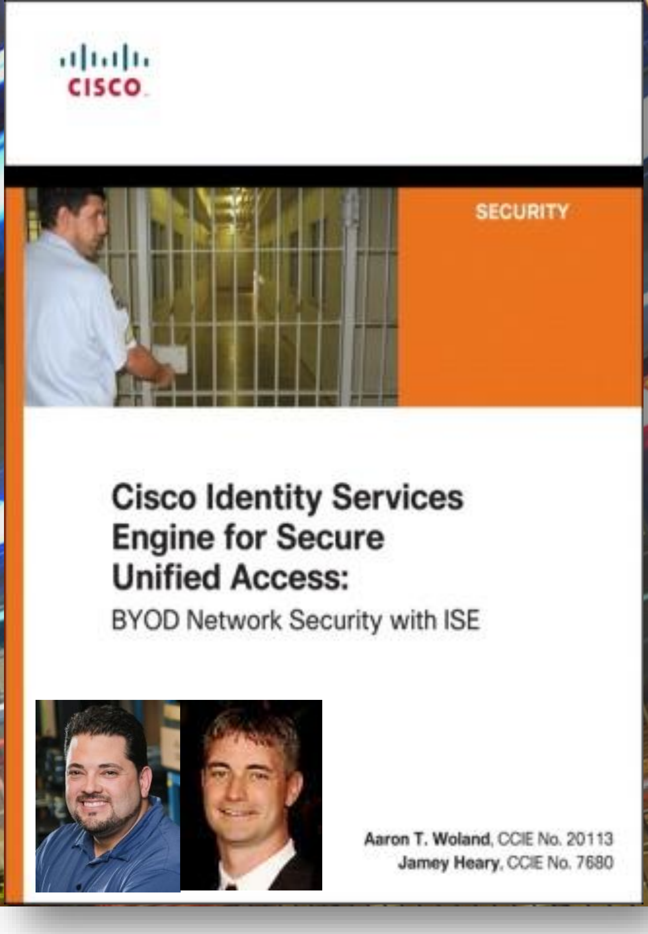
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-95-Cisco_and_F5_Deployment_Guide-ISE_Load_Balancing_Using_BIG-IP_DF.pdf

ISE How-To and Design Guides:

http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

Recommended Reading

- http://amzn.com/1587143259



SECURITY

Cisco Identity Services Engine for Secure Unified Access:

BYOD Network Security with ISE

Aaron T. Woland, CCIE No. 20113
Jamey Heary, CCIE No. 7680

Q & A

Complete Your Online Session Evaluation

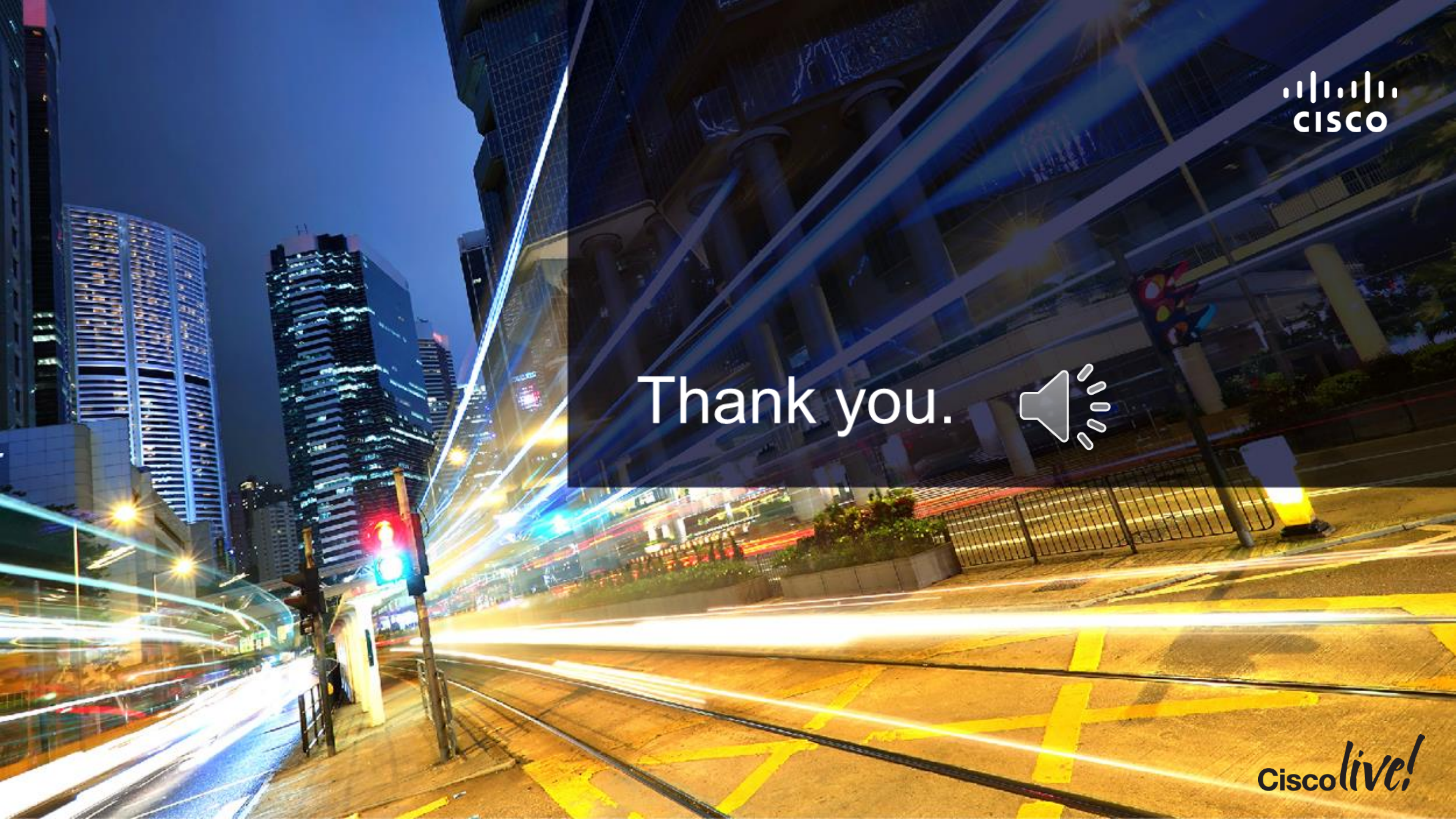
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

CISCO