CISCO

You make **possible**

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

Imran Bashir
Technical Marketing Engineer

BRKSEC-3432

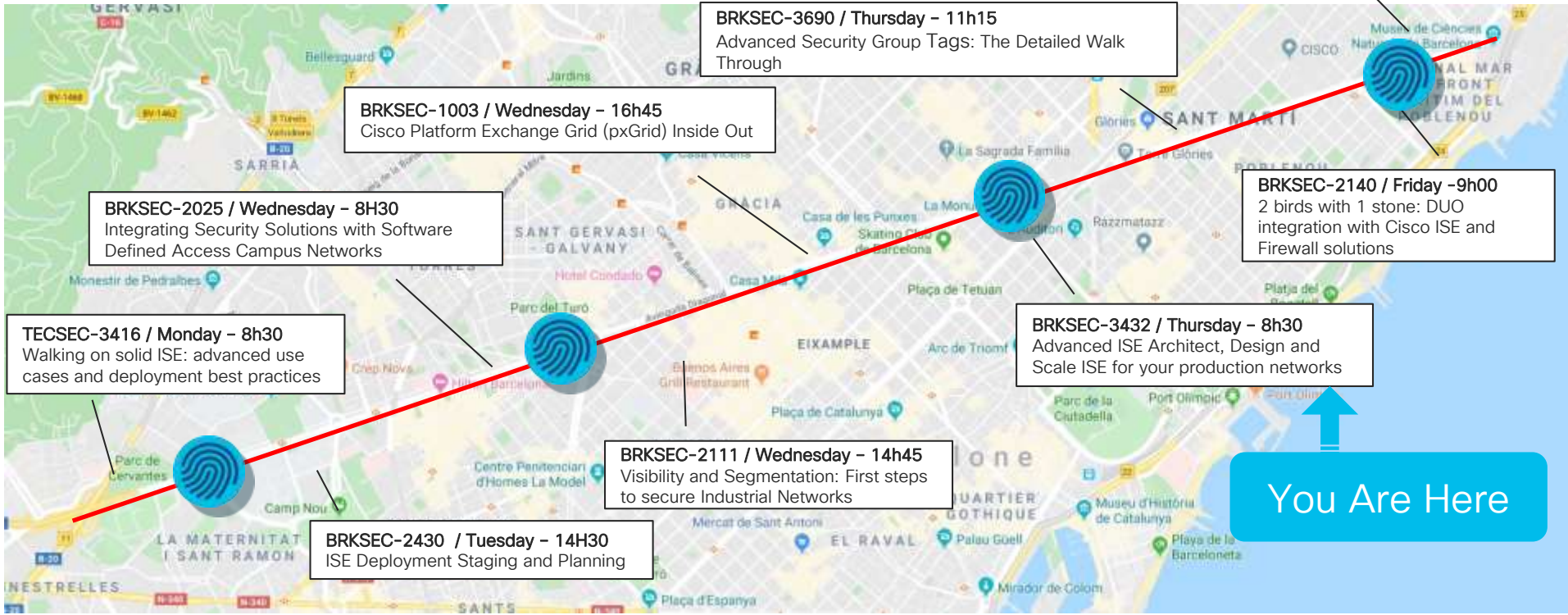
Barcelona | January 27-31, 2020

A bit about your Speaker

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

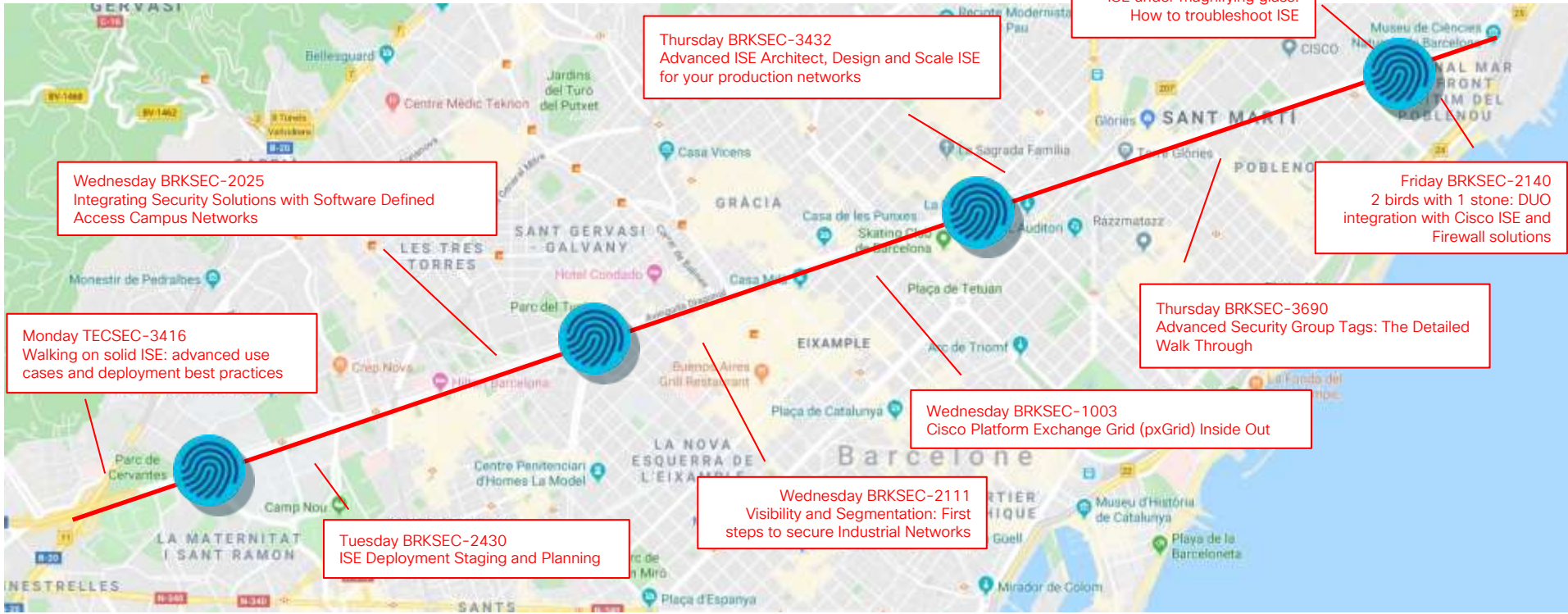
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Diagonal Learning Map



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Diagonal Learning Map



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Abstract

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

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

Attendees of this session will gain knowledge on how to best **design ISE** to ensure peak operational **performance, stability,** and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement. Cisco ISE also enables cross-platform network system collaboration across your IT infrastructure by using pxGrid to monitor security, detect threats, and set network policy. Manage assets, configuration, identity, and access. The session will go through such deployment considerations and common architectures.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important: Hidden Slide Alert

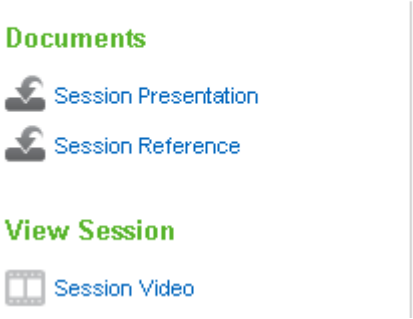
Look for this “For Your Reference” Symbol in your PDF’s

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

For Your Reference

~500 +/- Slides in Session Reference PDF

Available on ciscolive.com



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

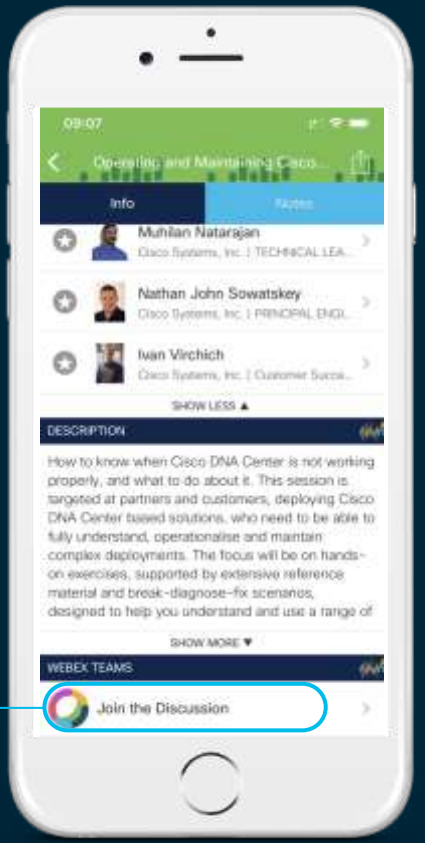
Cisco Webex Teams

Questions?

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

How

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where can I get help after Cisco Live?

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

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

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

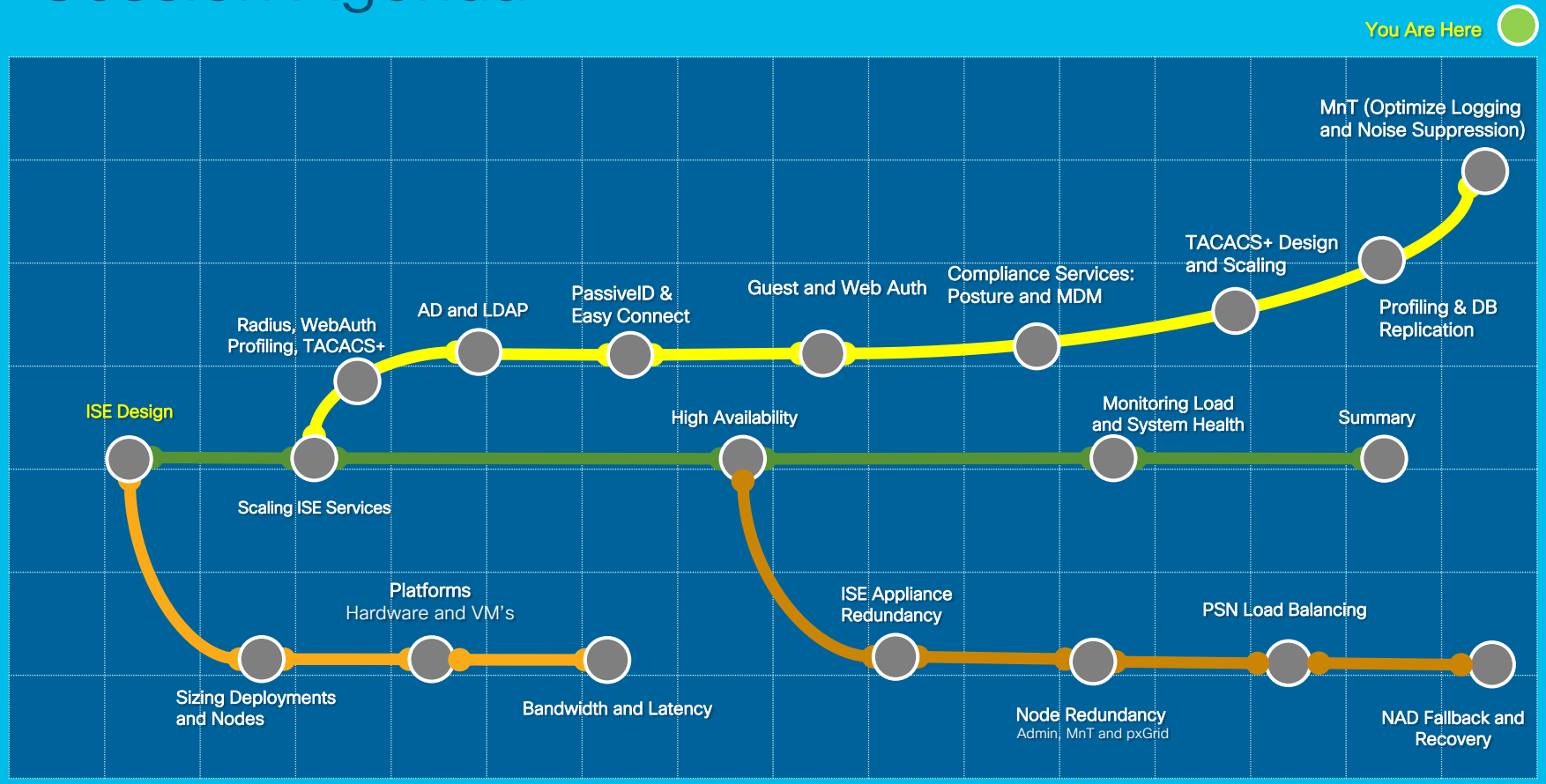
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

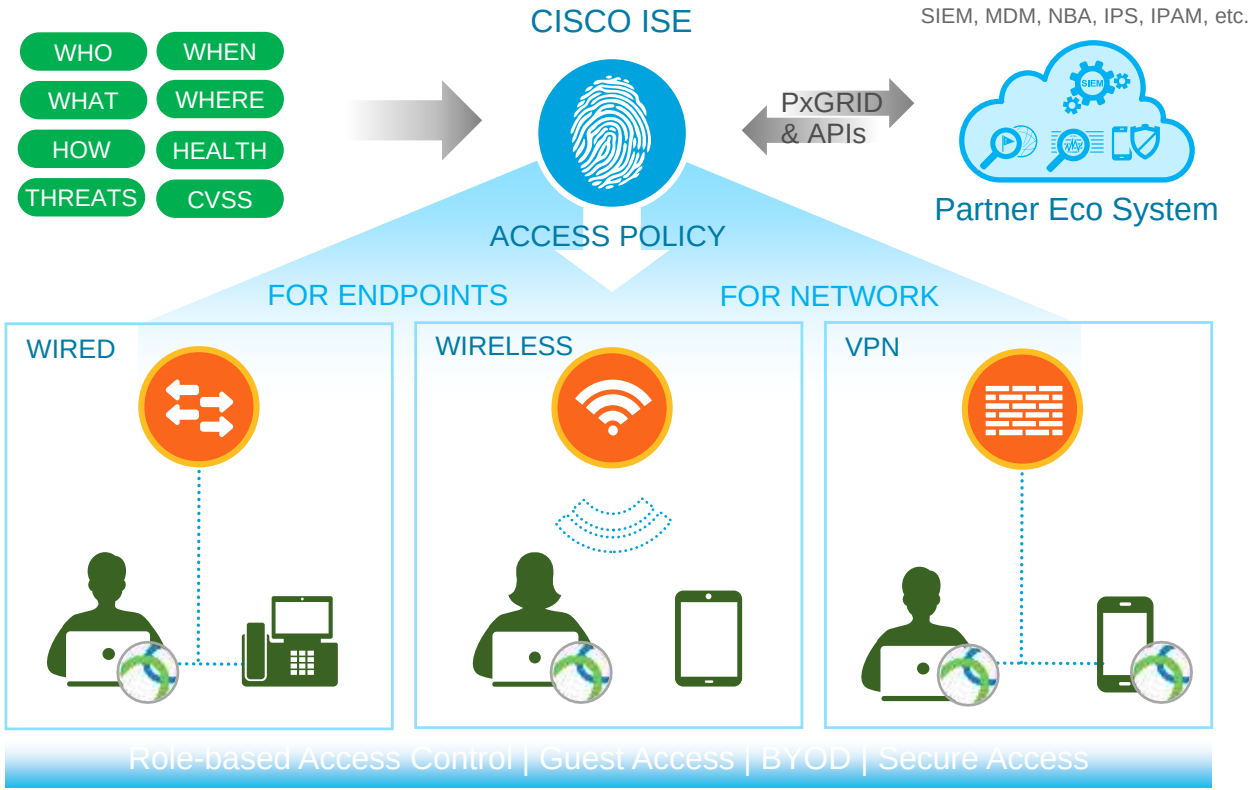
Cisco ISE and Anyconnect

Cisco ISE

Context aware policy service, to control access and threat across wired, wireless and VPN networks

Cisco Anyconnect

Supplicant for wired, wireless and VPN access. Services include: Posture assessment, Malware protection, Web security, MAC Security, Network visibility and more.

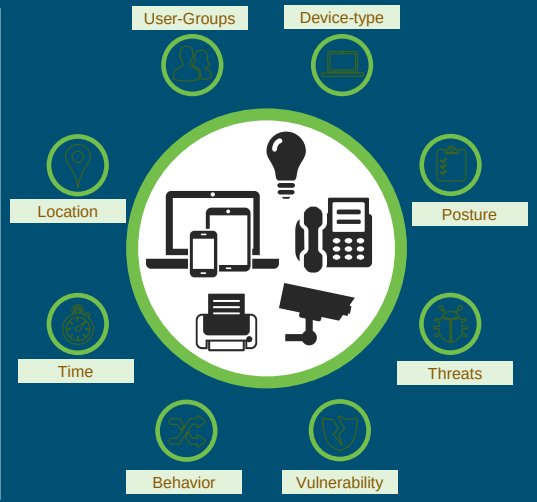


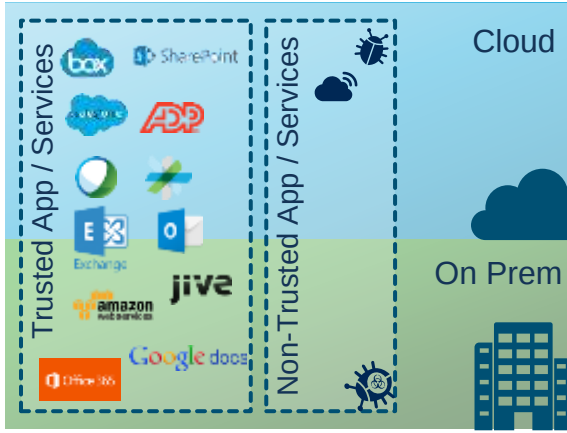
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Managing policy based on ‘Trust’

Connecting Trusted Devices to Trusted Services

CISCO IDENTITY SERVICES ENGINE

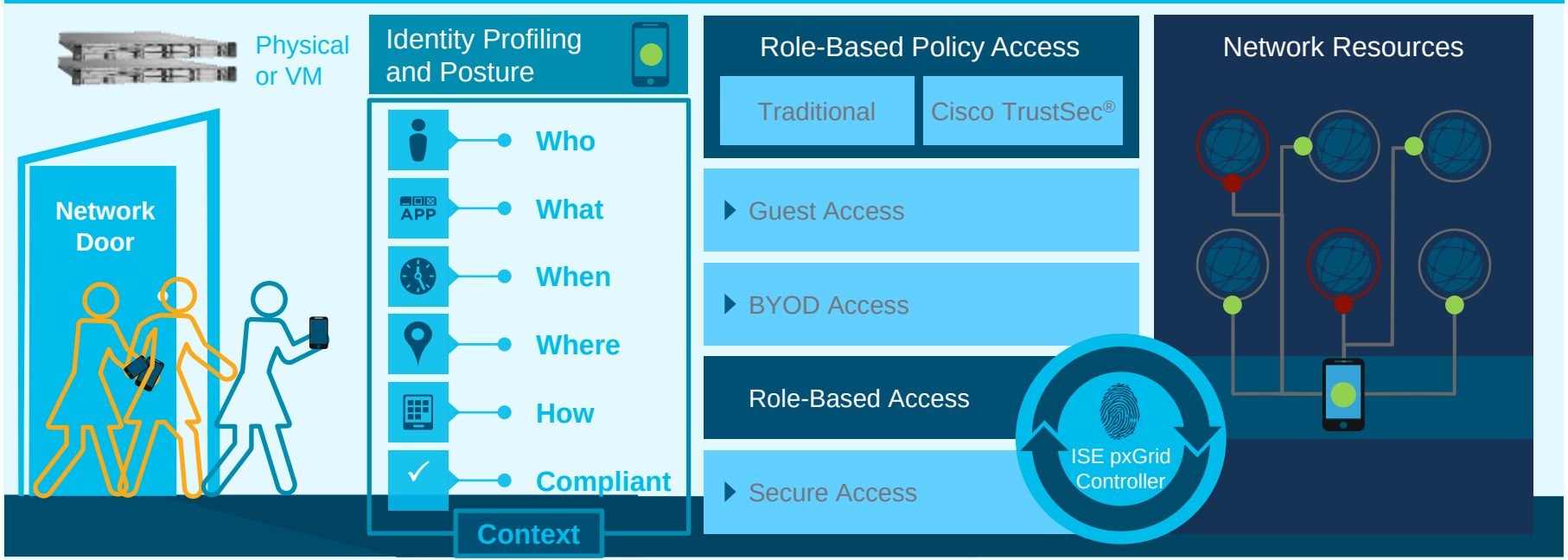




Improved Visibility and Decision	Software-Defined Segmentation, Service Access & Entitlement	Location-Free App/Service Access

Introducing Cisco Identity Services Engine

A centralized security solution that automates context-aware access to network resources and shares contextual data



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Announcing Cisco ISE 2.6

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

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

Announcing ISE 2.6

AnyConnect | Identity Services Engine ... | Policy and Access | TrustSec

7,324 VIEWS | 30 HELPFUL | 18 COMMENTS

yshchary in Cisco Employee

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

What's new in ISE 2.6:

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

MENU

cisco

Products & Services / Security / Network Mobility and Segmentation / Cisco Identity Services Engine / Bulletins /

Cisco Identity Services Engine Software Release Lifecycle Product Bulletin

Download | Print

Updated: May 24, 2018 **Document ID:** 1526606485749279

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

Cisco ISE software release timelines

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

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

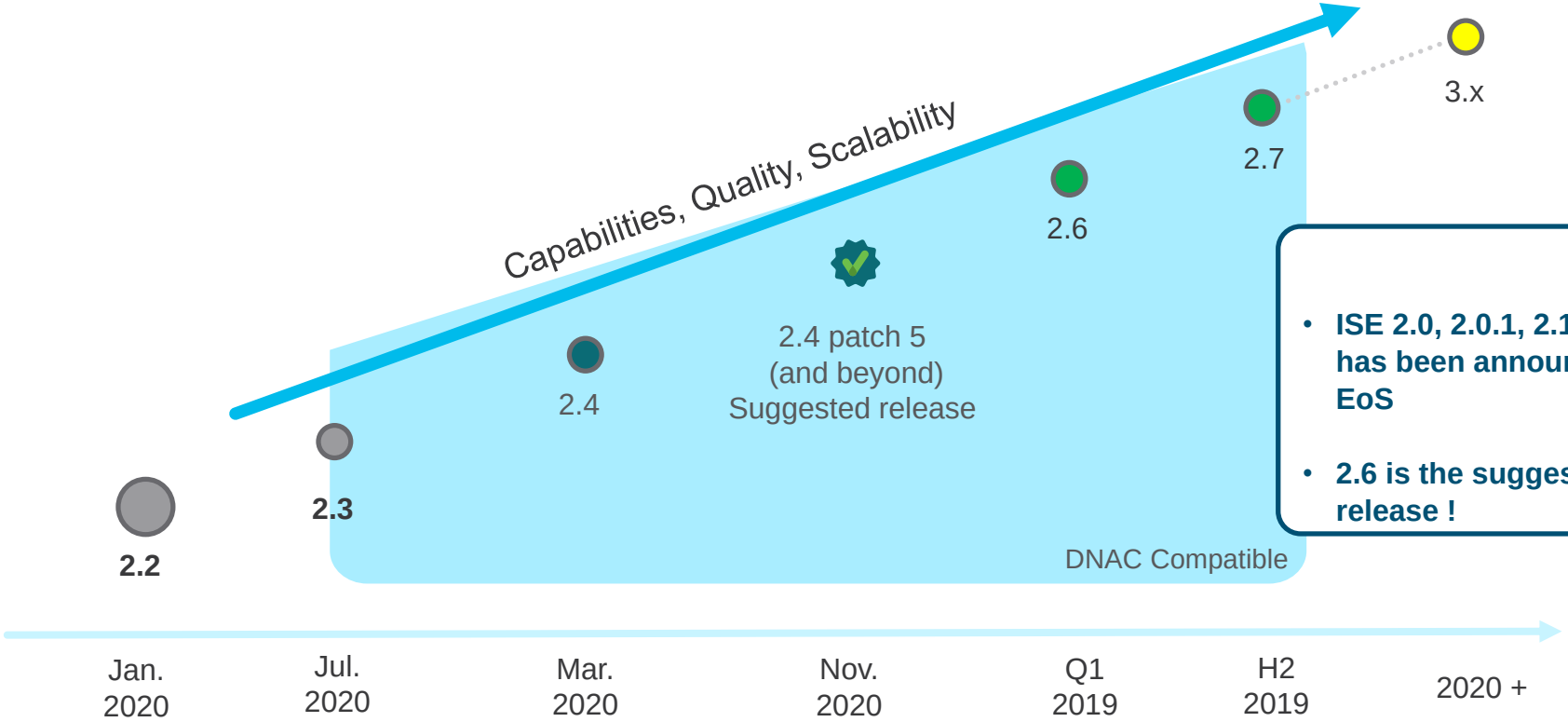
The LTR will typically be even numbered, for example, 2.0, 2.2, 2.4, and so on.

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Releases

Mature Product and Strong Engineering Commitment



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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Upgrade Paths Supported for ISE 2.7

2.2 → 2.7

2.3 → 2.7

2.4 → 2.7

2.6 → 2.7

SNS 36xx → 2.7

SNS 35xx → 2.7

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Faster, better appliances

New SNS-3600 Series hardware

SNS-3615

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

SNS-3655

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

SNS-3695

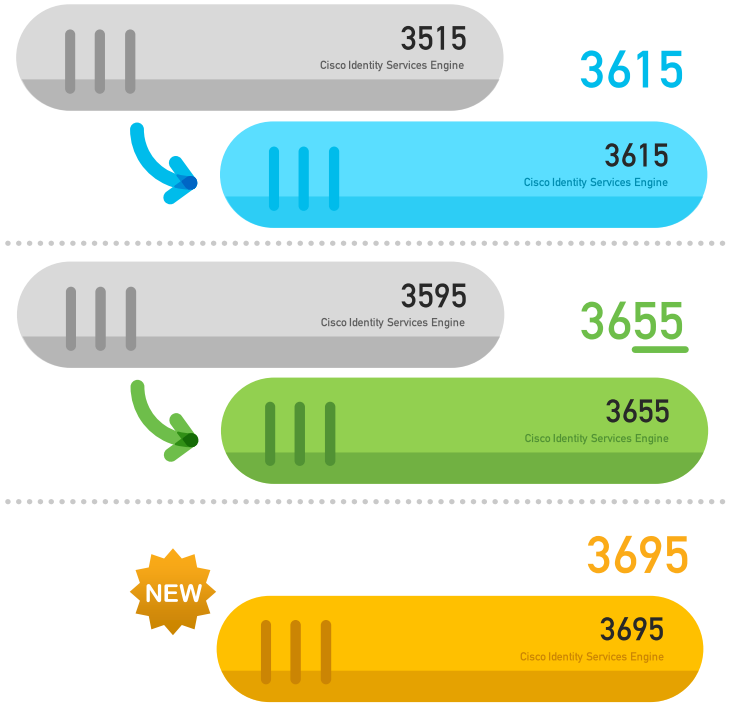
- 50,000 standalone sessions
- 100,000 PSN sessions

ISE Data Sheet and Ordering Guide

Policy Service Node (PSN)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNS-36xx appliances



What are we solving?

- Increased endpoint capacity per appliance and deployment
- UCS M4 Feb 2019 End Of Sale

How do we solve it?

- New appliances based on UCS M5

Prerequisites

- Must be running ISE 2.6
- http://cs.co/ise-feedback

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNS-36xx Specifications (requires 2.6)

	SNS-3615	SNS-3655	SNS-3695
Endpoints supported in a standalone configuration	10,000	25,000	50,000
Endpoints supported per Policy Services Node	10,000	50,000	100,000
Processor	Intel Xeon 2.10 GHz 4110	Intel Xeon 2.10 GHz 4116	Intel Xeon 2.10 GHz 4116
Cores per Processor	8	12	12
Memory	32GB	96GB	256GB
Hard Disk	1 600GB, 6Gb SAS 10K RPM	4 600GB, 6Gb SAS 10K RPM	8 600GB, 6Gb SAS 10K RPM
Hardware RAID	No	Level 10	Level 10
Power Supplies	1 x 770W	2 X 770W	2 X 770W

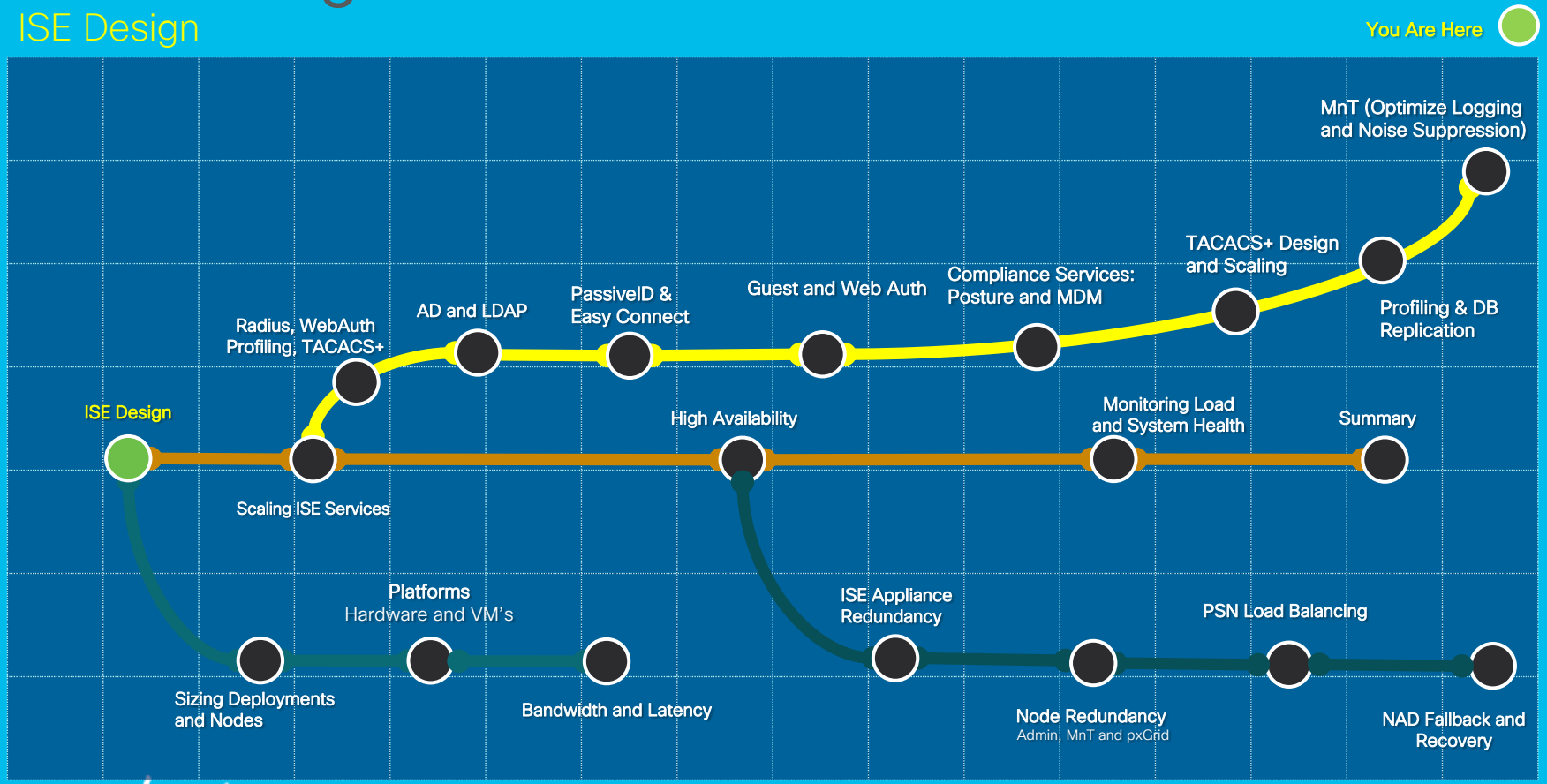
SNS-35xx EOL

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

ht

Session Agenda

ISE Design

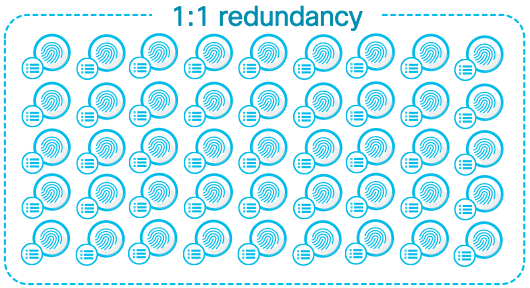


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Design

Increased Scale with ISE 2.6 on 36xx

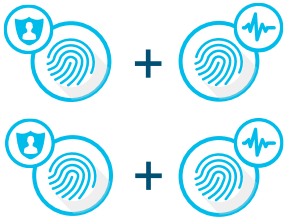
- Applies to both physical and virtual deployment
- Compatible with load balancers



Lab and Evaluation

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

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

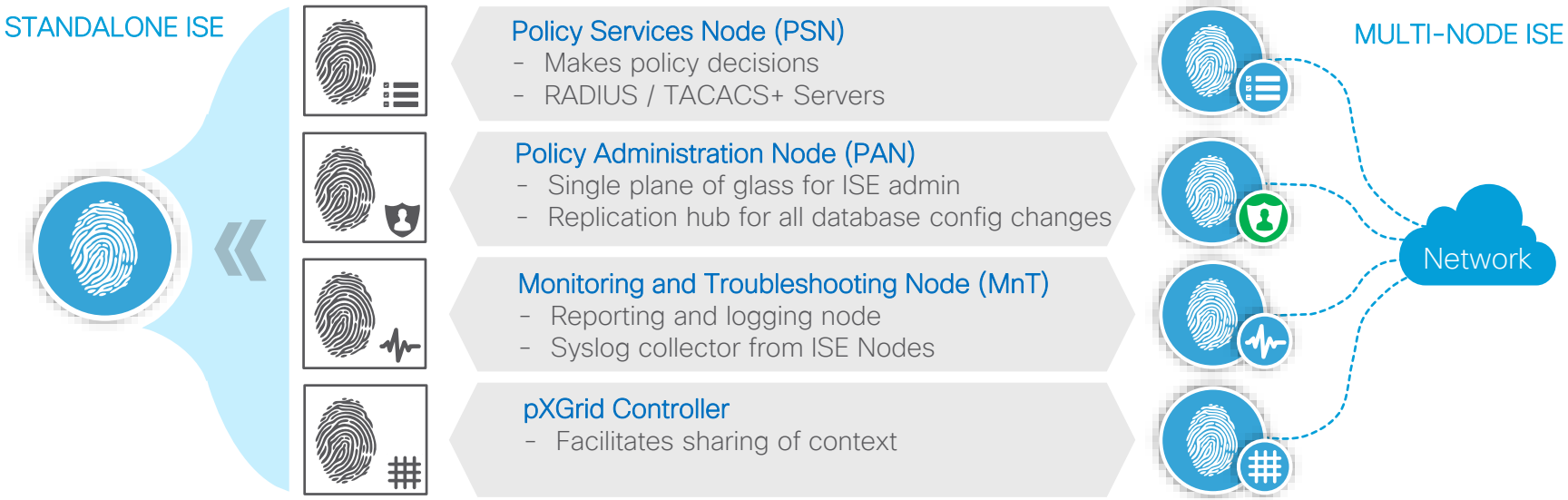


Large Deployment
2 PAN, 2 MNT, <=50 PSN

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE deployment options



	Single Node (Virtual / Appliance)	Multiple Nodes (Virtual / Appliance)
35xx	20,000 Endpoints	500,000 Endpoints
36xx	50,000 Endpoints	2,000,000 Endpoints(3695-PAN&MnT)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Platform Support

2.6 Will Be Supported on These Physical Appliances:

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

Virtual Appliances:

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

Virtual Appliance Operating Systems:

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SNS-36xx appliances scale and orderability

NEW

Appliances	Standalone Sessions	PSN Sessions	Processor	Cores	Memory	Disk	Raid	Network Interfaces
SNS-3615	10,000	10,000	1 – Intel Xeon 2.10 GHz 4110	12	32 GB (2 x 16 GB)	1 (600 GB)	No	2 x 10Gbase-T 4 x 1GBase-T
SNS-3655	25,000	50,000	1 – Intel Xeon 2.10 GHz 4116	12	96 GB (6 x 16 GB)	4 (600 GB)	10	2 x 10Gbase-T 4 x 1GBase-T
SNS-3695	50,000	100,000	1 – Intel Xeon 2.10 GHz 4116	8	256 GB (8 x 32 GB)	8 (600 GB)	10	2 x 10Gbase-T 4 x 1GBase-T
SNS-3515	7,500	7,500	1 – Intel Xeon 2.40 GHz E5-2620	6	16 GB (2 x 8 GB)	1 (600 GB)	No	6 x 1GBase-T
SNS-3595	20,000	40,000	1 – Intel Xeon 2.60 GHz E5-2640	8	64 GB (4 x 16 GB)	4 (600 GB)	10	6 x 1GBase-T

* - Orders placed prior to targeted availability will be on new product hold until targeted availability

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Administration Node (PAN)

For Your Reference

Writeable Access to the Database

- Interface to configure and view policies
- Responsible for policy sync across all PSNs and secondary PAN
- Provides:
  - Licensing
  - Admin authentication & authorization
  - Admin audit
- Each ISE deployment must have at least one PAN
  - Only 1x Primary and 1x Secondary (Backup) PAN possible

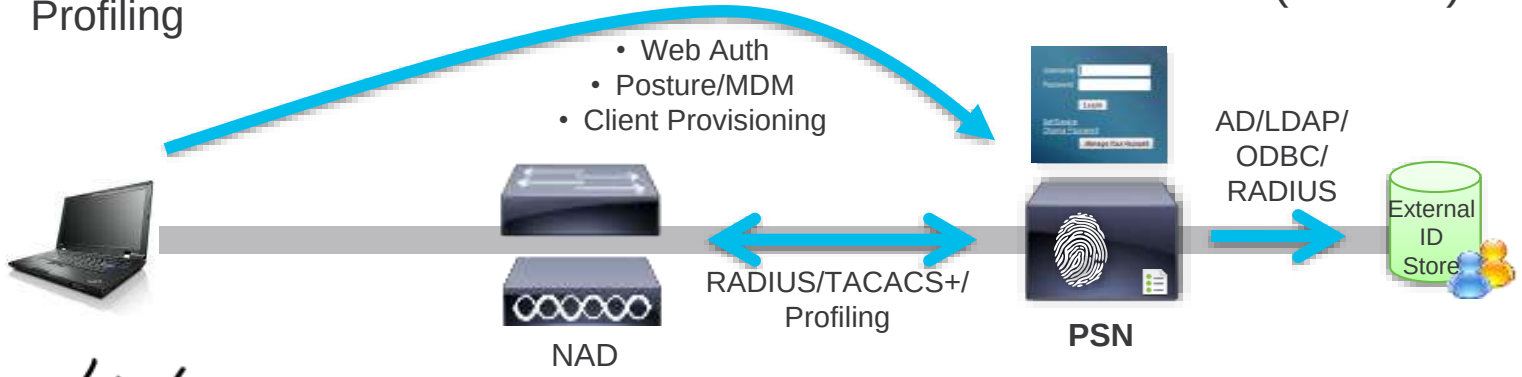
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Service Node (PSN)

RADIUS/TACACS+ Server for the Network Devices

For Your Reference

- Per policy decision, responsible for:
  - Network access (AAA/RADIUS services)
  - Device Admin (TACACS+)
  - Posture
  - BYOD / MDM services
  - Guest access (web portals)
  - Client Provisioning
  - Profiling
- Directly communicates to external identity stores for user authentication
- Provides GUI for sponsors, agent download, guests access, device registration, and device on-boarding
- Each ISE deployment must have one or more PSNs (max 50)

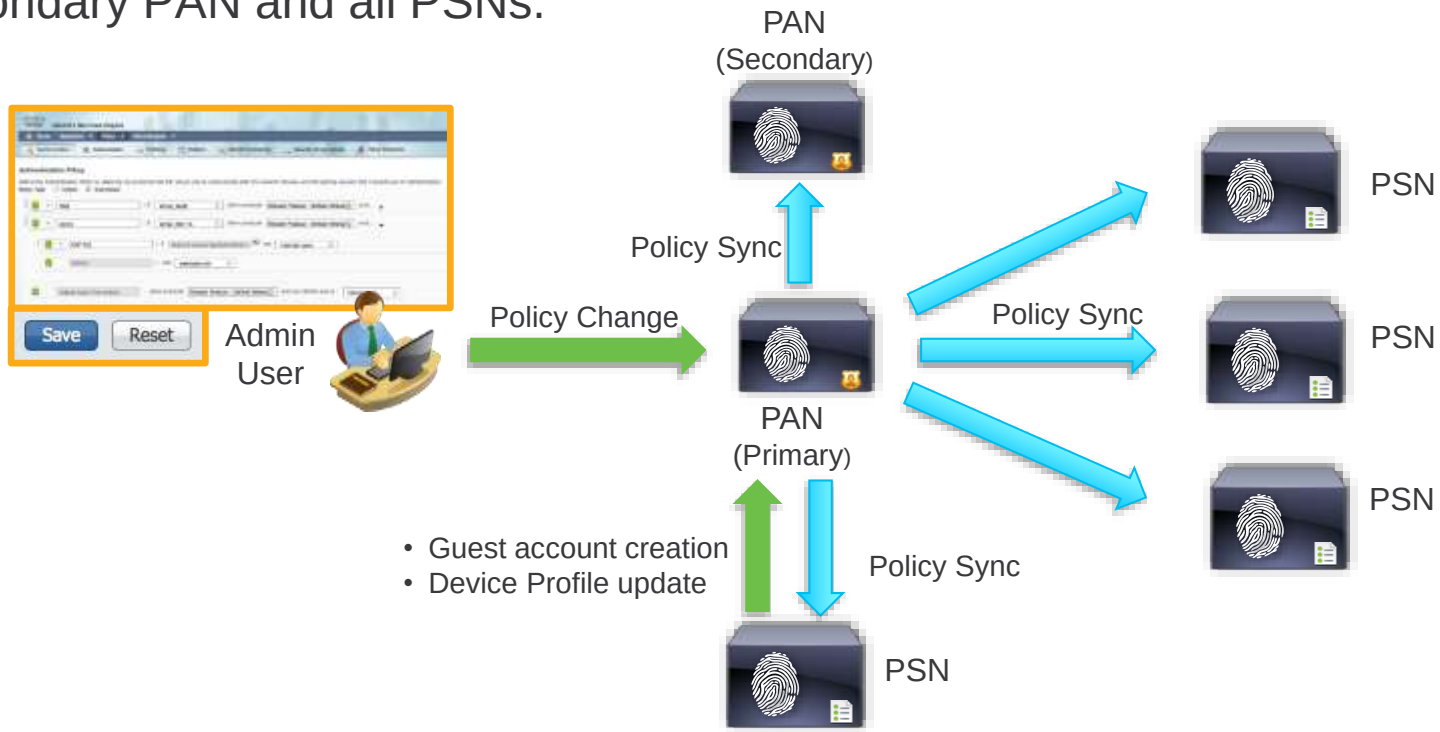


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Synchronization

For Your Reference

- Changes made via Primary PAN DB are automatically synced to Secondary PAN and all PSNs.



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

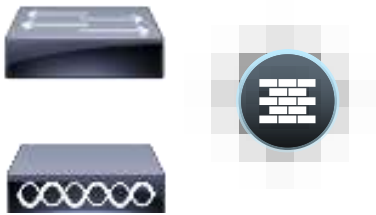
Network Access Device (NAD)

For Your Reference

Also Known as the ‘RADIUS Client’ (or ‘TACACS+ Client’)

- Major Secure Access component that enforces network policies.
- NAD sends request to the PSN for implementing authorization decisions for resources.
- Common enforcement mechanisms:
  - VLAN Assignment/VRF
  - dACLs & named ACLs
  - Scalable Group Tags (SGT)
- Basic NAD types (including 3rd party)
  - Cisco Catalyst Switches
  - Cisco Wireless LAN Controllers
  - Cisco ASA & FTD for VPN

NADs



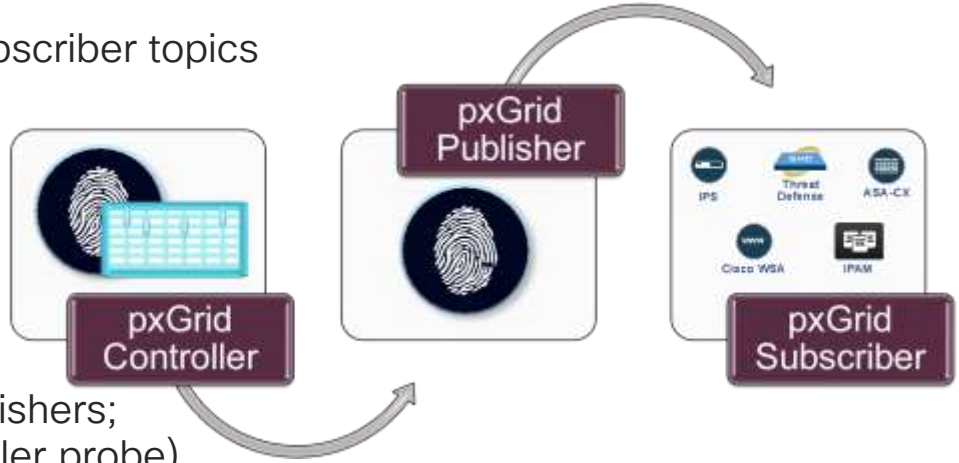
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

pxGrid Controller (PXG)

Context Data Sharing

For Your Reference

- Enabled as pxGrid persona
  - Max 2 nodes
- Control Plane to register Publisher/Subscriber topics
- Authorize and setup pxGrid client communications
- pxGrid Clients subscribe to published topics of interest
- ISE 1.X: ISE is only controller and publisher; 2.0 supports other publishers; 2.4 supports ISE as a subscriber (Profiler probe)
- MnT publishes Session Directory



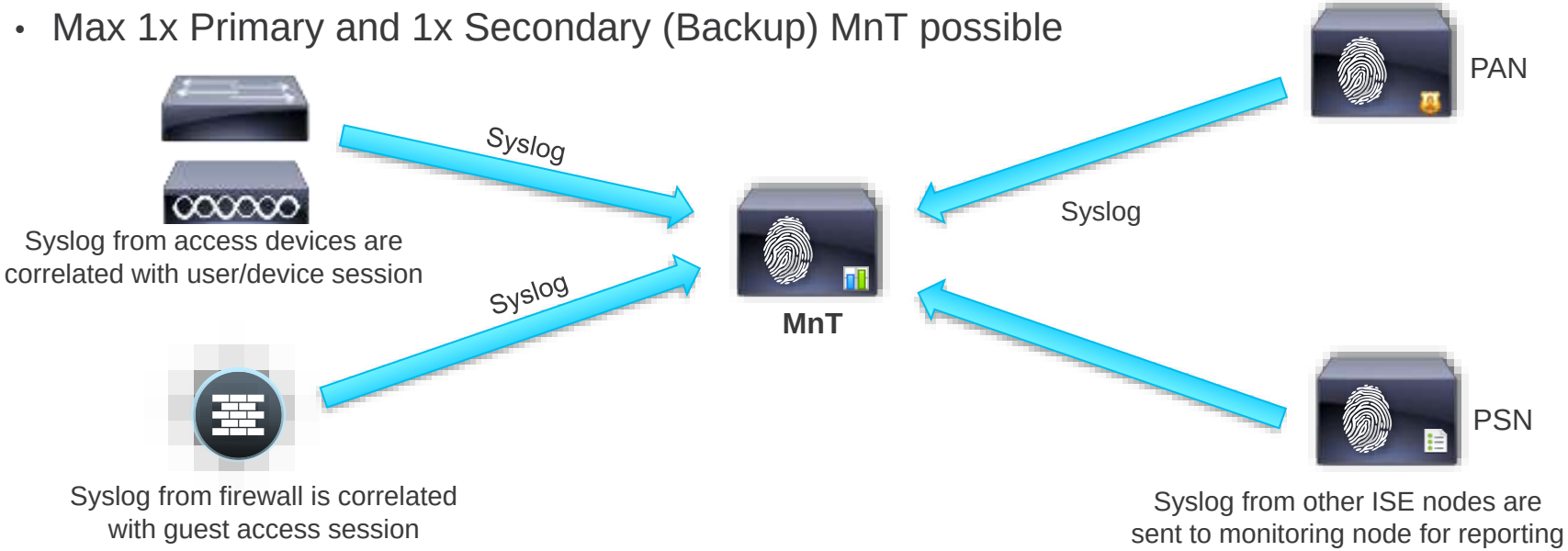
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring and Troubleshooting Node (MnT)

Logging and Reporting

For Your Reference

- MnT node receives logging from PAN, PSN, NAD (RADIUS & TACACS)
- Each ISE deployment must have at least one MnT
  - Max 1x Primary and 1x Secondary (Backup) MnT possible

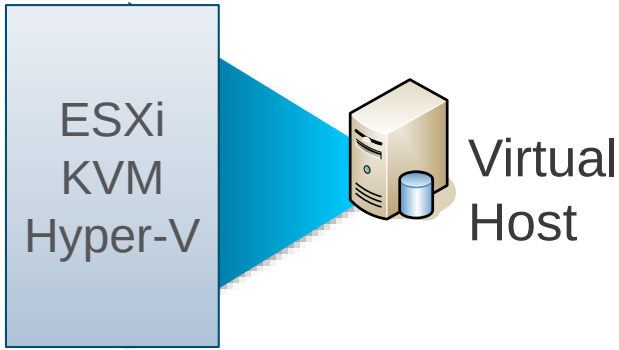


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Platforms

For Your Reference

- Single ISE node (Appliance or VM) can run PAN, MnT, PSN, and pxGrid roles simultaneously
- For scaling beyond 50,000 endpoints, roles will need to be dedicated and distributed across multiple nodes



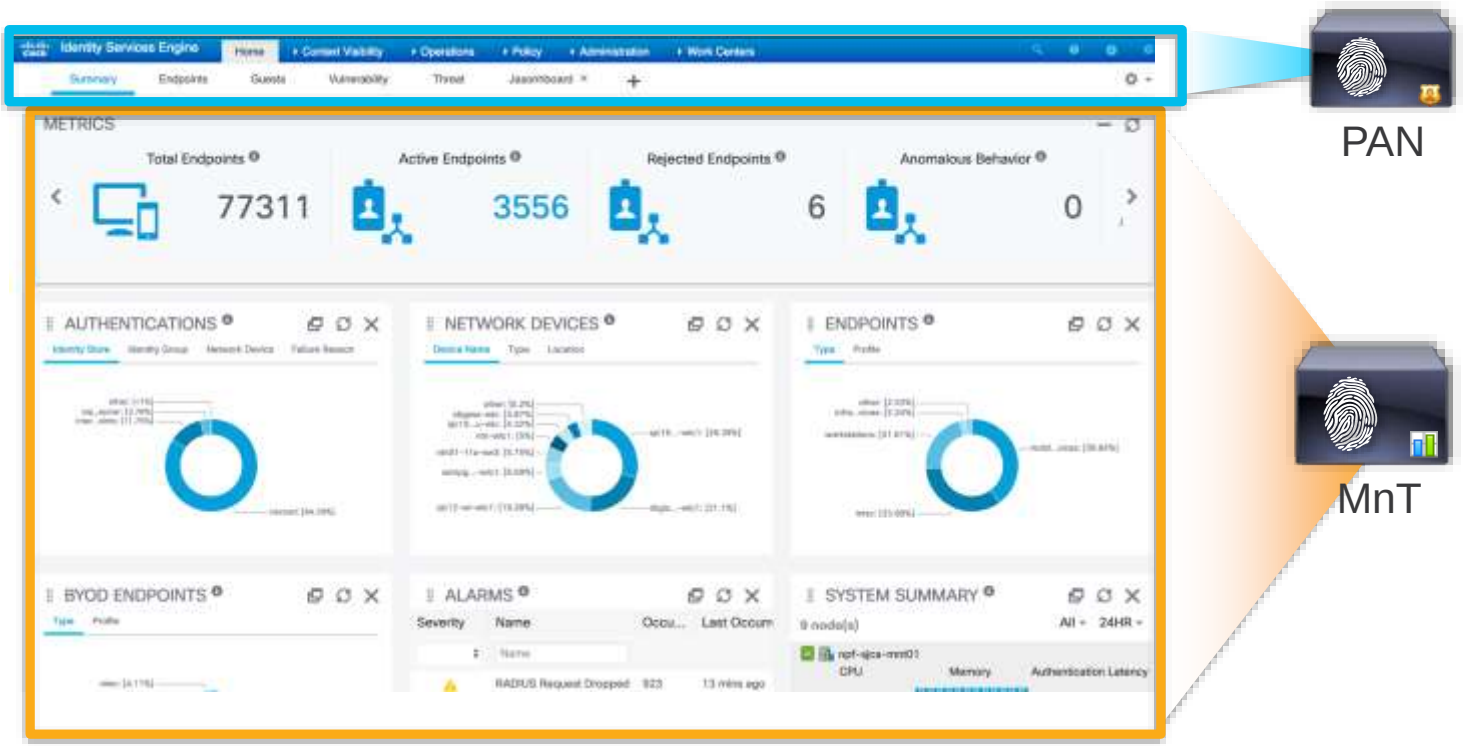
SNS 35xx/36xx or Hardware Appliance

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring and Troubleshooting Node

Dashboard

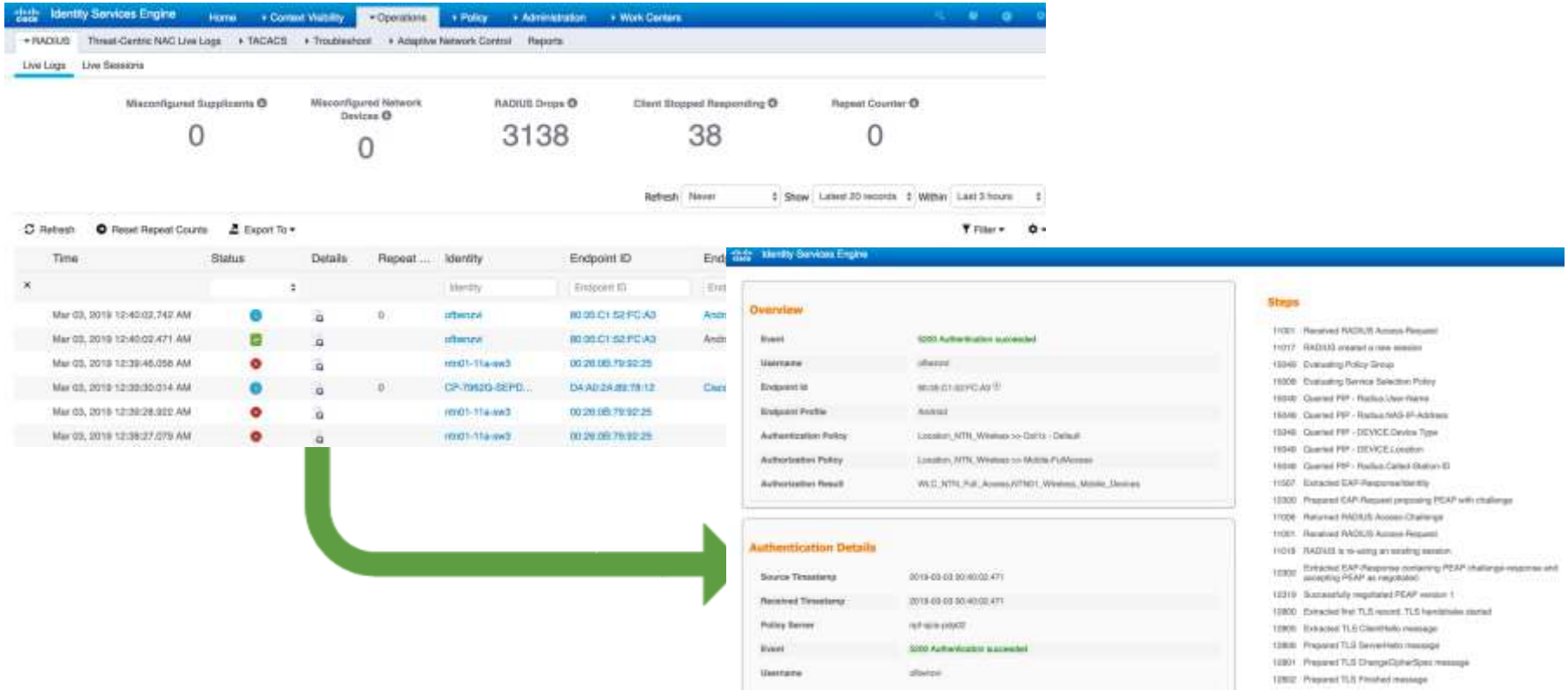
For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring and Troubleshooting Node

For Your Reference



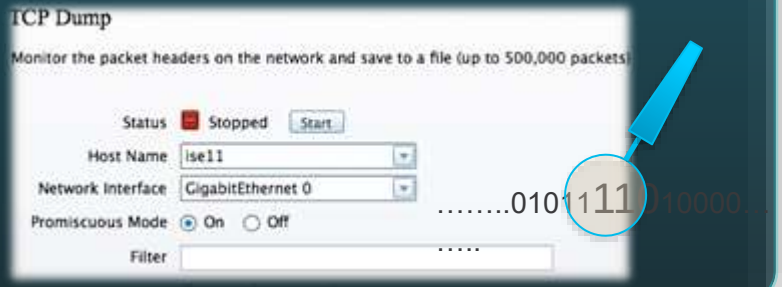
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring and Troubleshooting Tools

For Your Reference

Validate NAD configuration

Capture traffic destined for ISE



Download debugs and support package

Provide API for 3rd party applications

- Session Management
- Troubleshooting
- CRUD
- Change of Authorization

ISE Reporting

For Your Reference

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

- Export Summary
- My Reports
- Reports
  - Audit
  - Device Administration
  - Diagnostics
  - Endpoints and Users
    - Authentication Summary
    - Client Provisioning
    - Current Active Sessions
    - External Mobile Device Man...
    - Manual Certificate Provisioning
    - PassiveID
    - Posture Assessment by Con...
    - Posture Assessment by End...
    - Profiled Endpoints Summary
    - RADIUS Accounting
    - RADIUS Authentications
    - Registered Endpoints

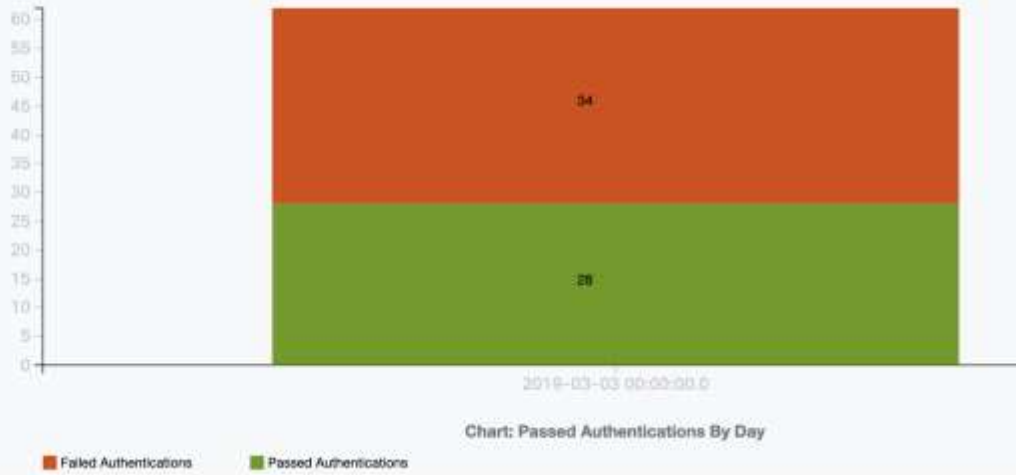
Authentication Summary

Filters

Match All of the following rules.

Time Range | Is exactly (or equals) | Today

Chart: Passed Authentications By Day



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Putting It All Together...

For Your Reference

Network Access Device
Access-Layer Devices
Enforcement Point for all Policy

Monitoring and Troubleshooting
Logging and Reporting Data

Policy Service Node
The "Work-Horse":
RADIUS, Profiling, WebAuth, Posture, Sponsor Portal Client Provisioning

Policy Administration Node: All Management UI Activities & synchronizing all ISE Nodes

Admin

NAD

MnT

PSN

PAN

PXG

User

Policy Sync

RADIUS from NAD to PSN

PSN queries external database directly

Platform eXchange Grid Node: Share context in/out

RADIUS response from PSN to NAD

RADIUS Accounting

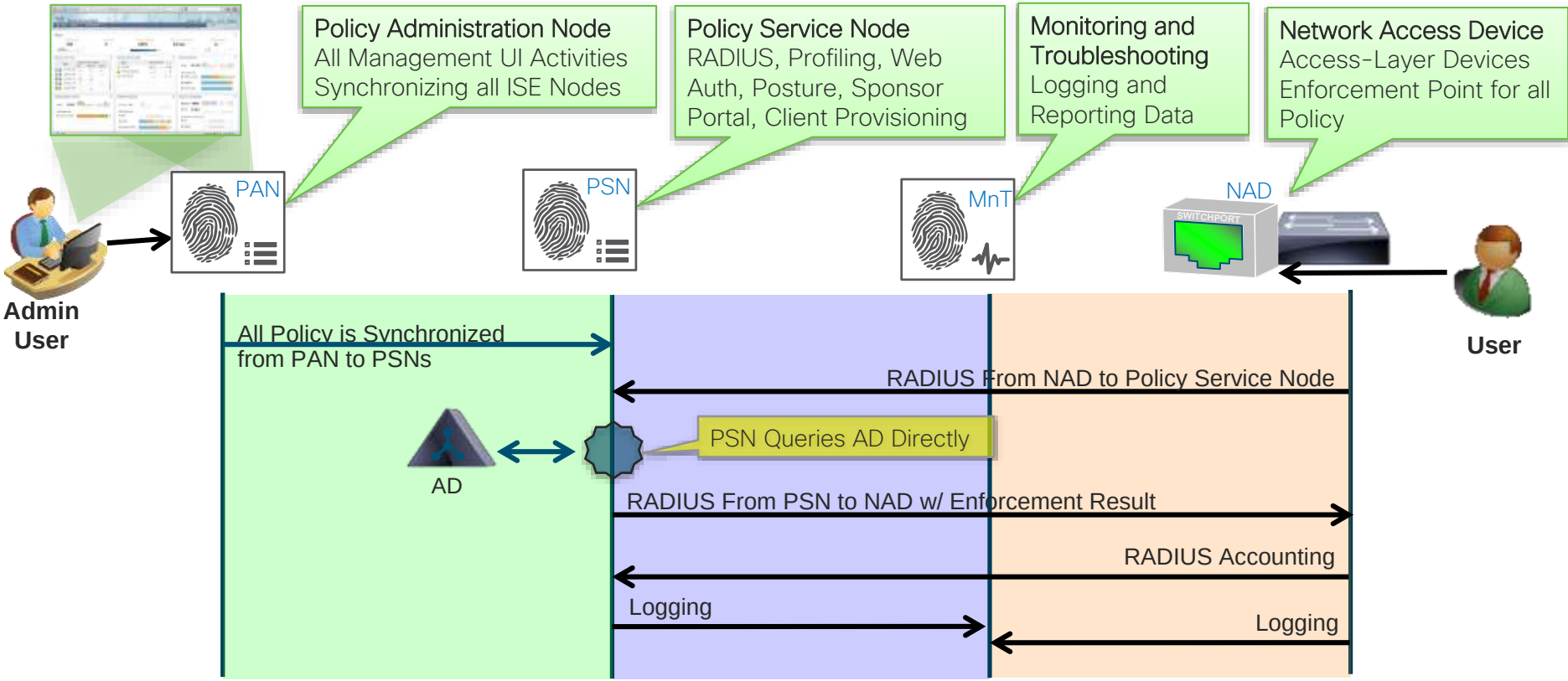
syslog

Publish Config

Publish Sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

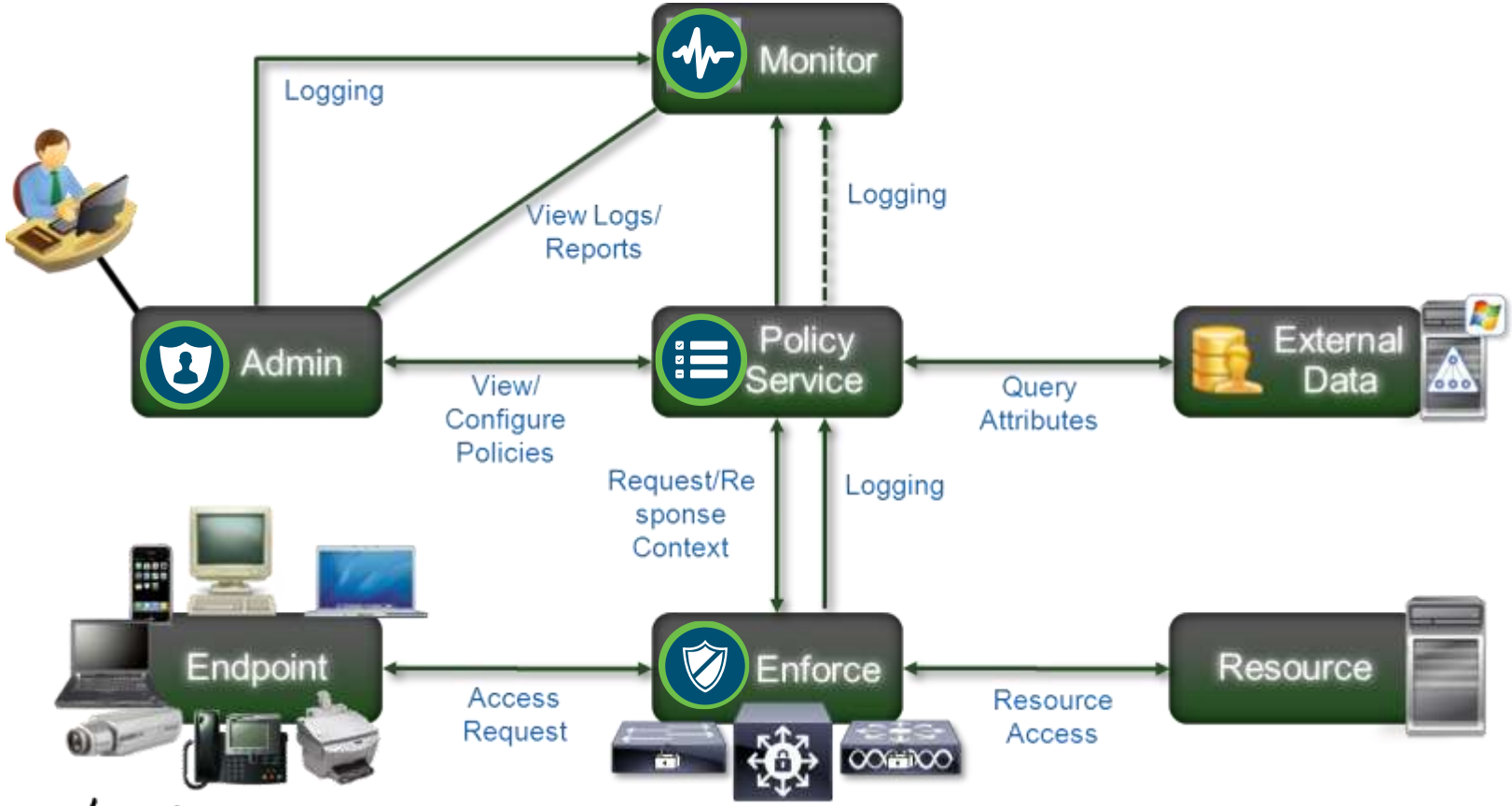
ISE Node Personas = Functional Roles



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Policy Architecture

For Your Reference



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

ISE Design and Deployment Terms

- Persona Deployment

  Standalone = All personas (Admin/MnT/pxGrid/Policy Service) located on same node

  Distributed = Separation of one or more personas on different nodes

- Topological Deployment

  Centralized = All nodes located in the same LAN/campus network

  Distributed = One or more nodes located in different LANs/campus networks separated by a WAN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Standalone Deployment

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

NEW

- Maximum sessions – Platform dependent
  - 7,500 for 3515
  - 10,000 for 3615
  - 20,000 for 3595
  - 25,000 for 3655
  - 50,000 for 3695

Policy Administration Node

Monitoring and Troubleshooting Node

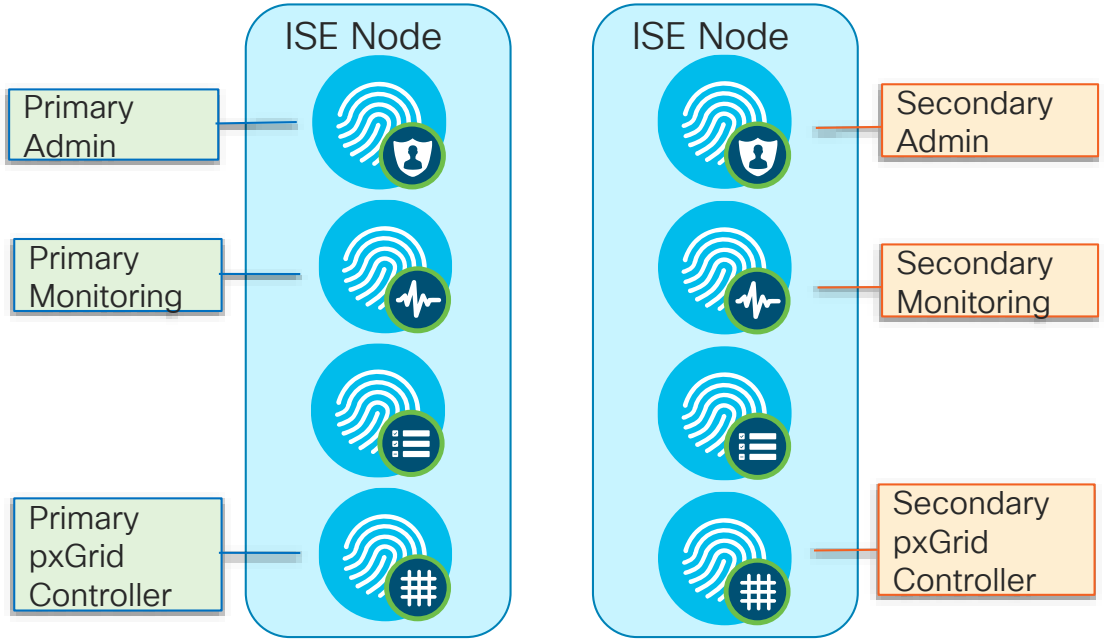
Policy Service Node

pxGrid Node

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Basic 2-Node ISE Deployment (Redundant)

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

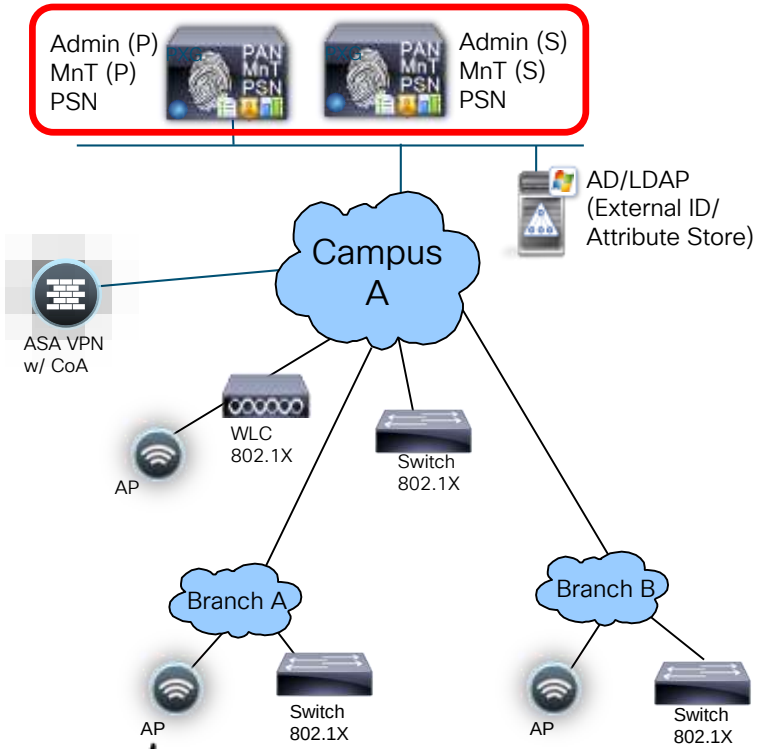


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Basic 2-Node ISE Deployment (Redundant)

For Your Reference

Maximum Sessions = 50,000 (Platform dependent) Centralized



PSN

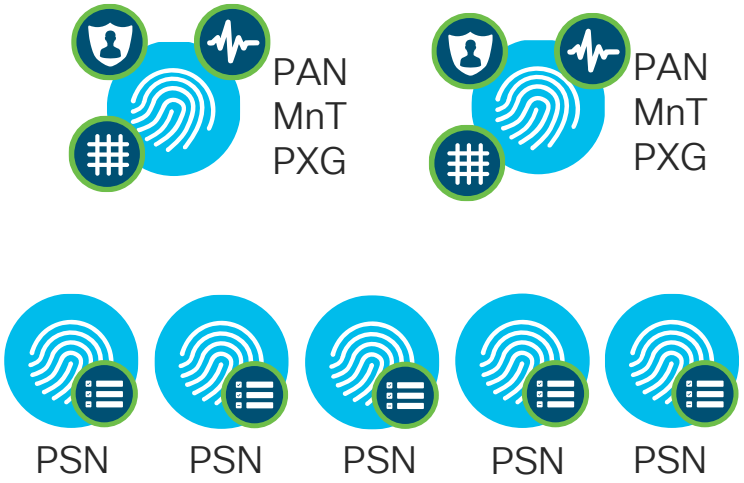
- All Services run on both ISE Nodes
- Set one for Primary Admin / Primary MnT
- Set other for Secondary Monitoring / Secondary Admin
- Max Sessions is platform dependent:
  - 3515 = Max 7.5k sessions
  - 3615 = Max 10k sessions
  - 3595 = Max 20k sessions
  - 3655 = Max 25k sessions
  - 3695 = Max 50k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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hybrid-Distributed Deployment

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

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

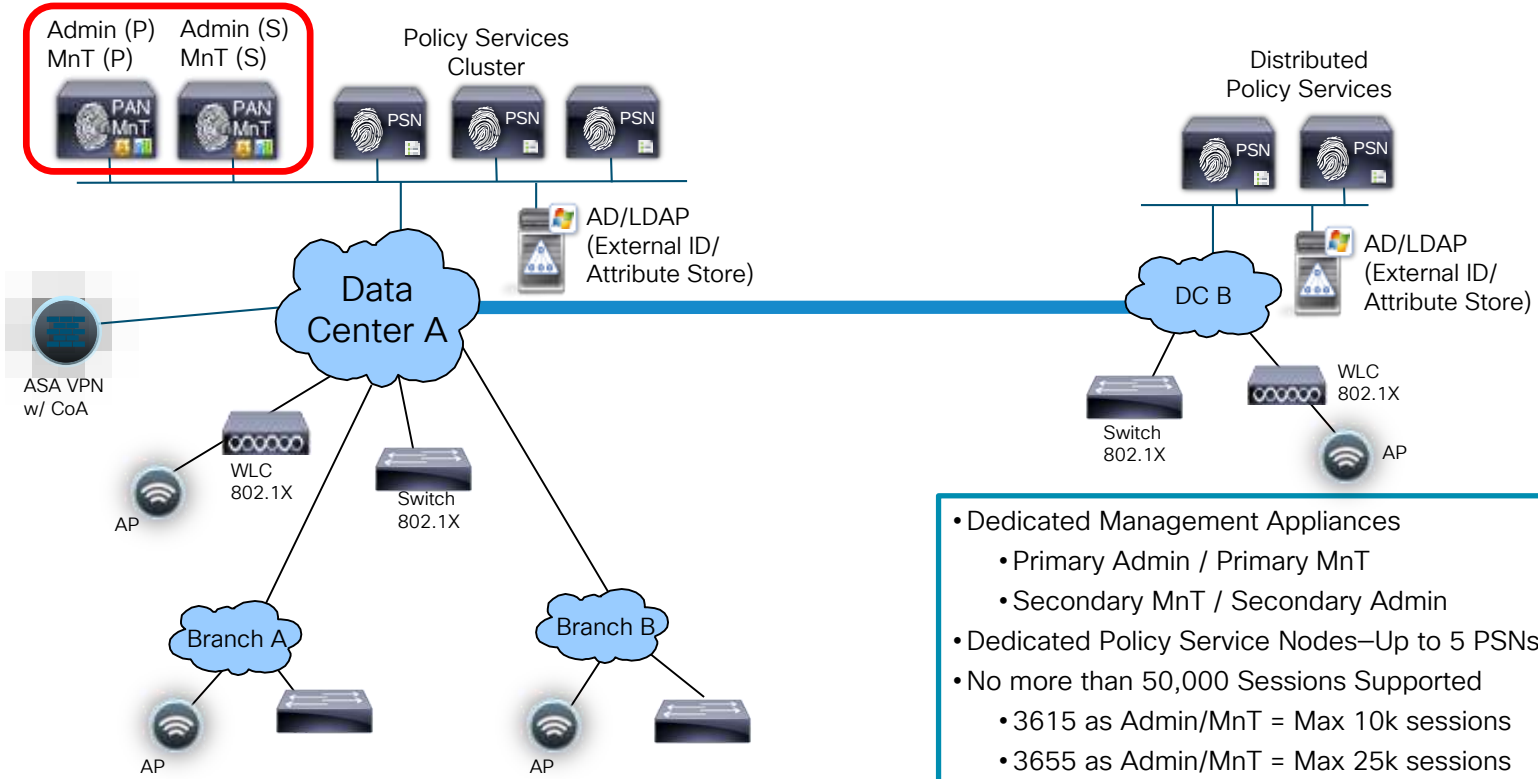


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Basic Hybrid-Distributed Deployment

Maximum Sessions = 50,000 / Maximum 5 PSNs

For Your Reference



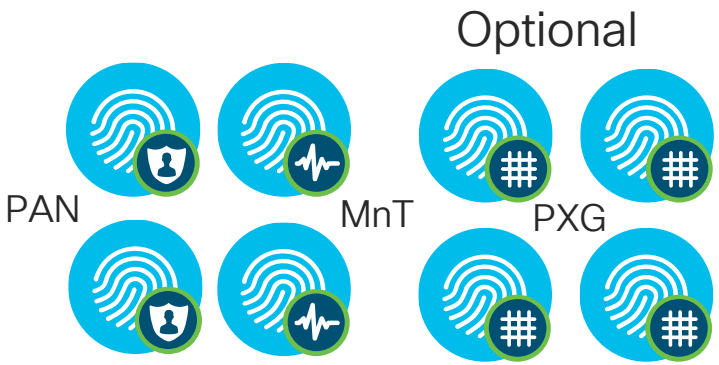
- Dedicated Management Appliances
  - Primary Admin / Primary MnT
  - Secondary MnT / Secondary Admin
- Dedicated Policy Service Nodes–Up to 5 PSNs
- No more than 50,000 Sessions Supported
  - 3615 as Admin/MnT = Max 10k sessions
  - 3655 as Admin/MnT = Max 25k sessions
  - 3695 as Admin/MnT = Max 50k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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dedicated-Distributed Persona Deployment

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

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling per use case

ISE Performance & Scale

AAA and NAC | Identity Services Engine ... | Policy and Access

107949 VIEWS | 123 HELPFUL | 11 COMMENTS

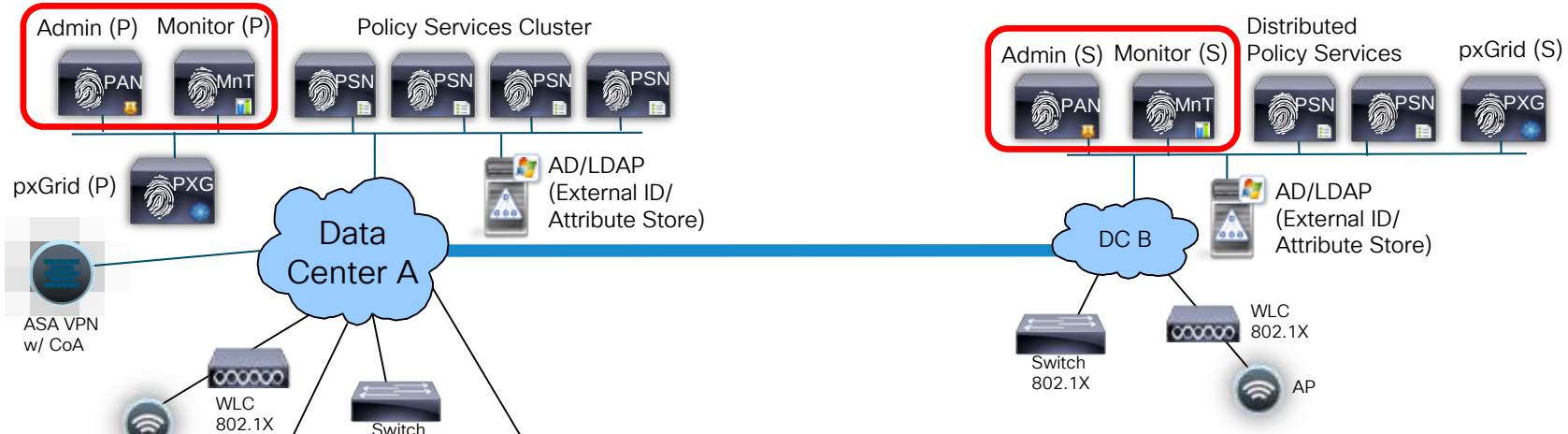
https://community.cisco.com/t5/security-documents/ise-performance-amp-scale/ta-p/3642148#toc-hId-1418220509

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fully Dedicated-Distributed Deployment

Maximum Sessions = 2M - Maximum 50 PSNs

For Your Reference

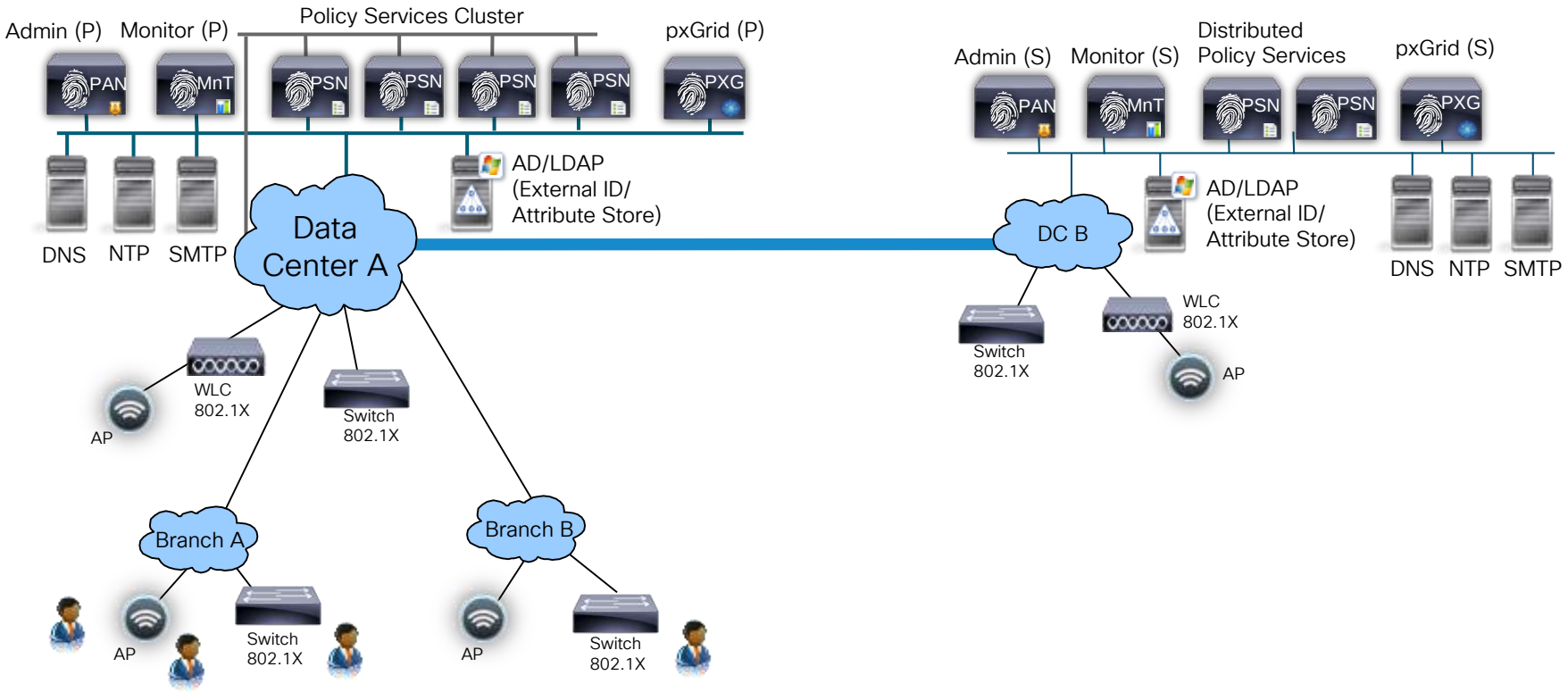


- Redundant, dedicated Administration and Monitoring nodes split across data centers (P=Primary / S=Secondary)
- Policy Service cluster for Wired/Wireless services at main campus
- Distributed Policy Service clusters for DR sites or larger campuses with higher-bandwidth, lower-latency interconnects.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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multi-Interface Routing

For Your Reference

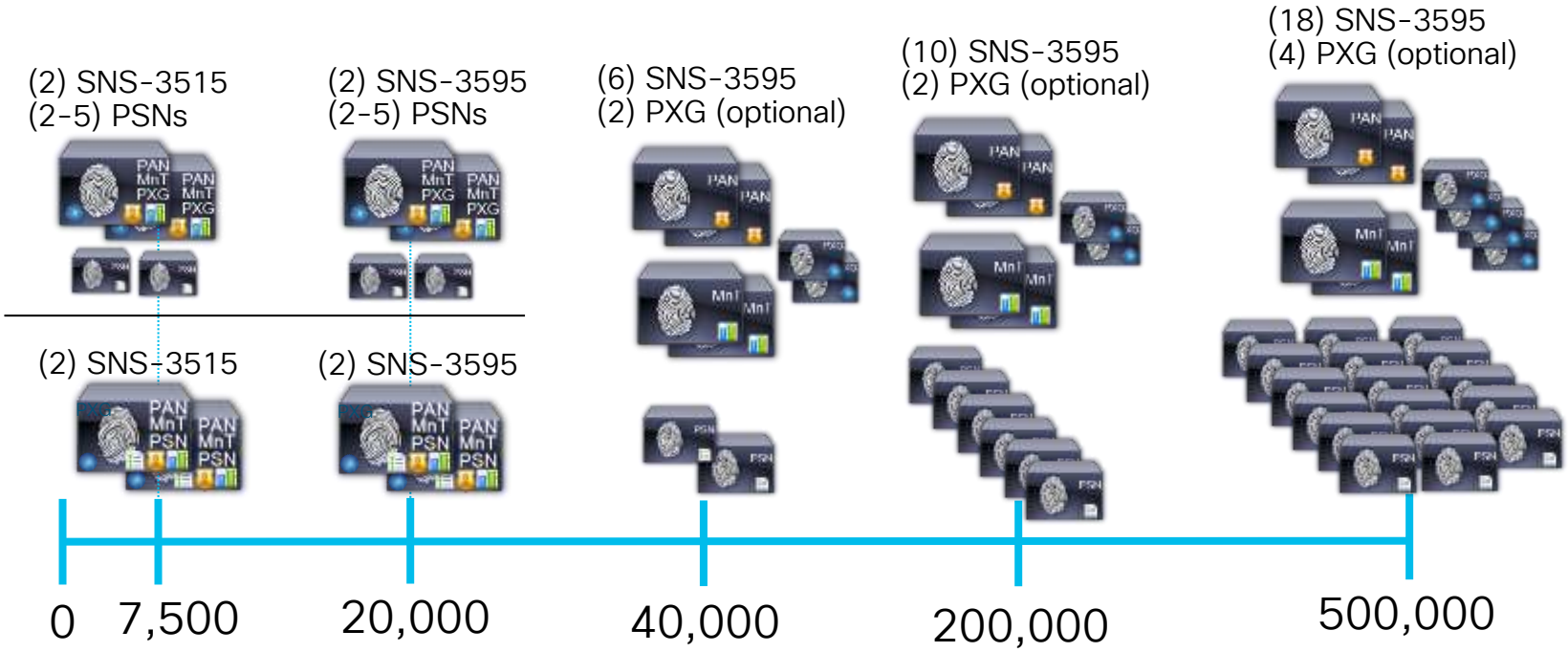


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Scaling by Deployment Model 35xx

For Your Reference

Minimum Nodes (Redundancy Included) ISE <2.6

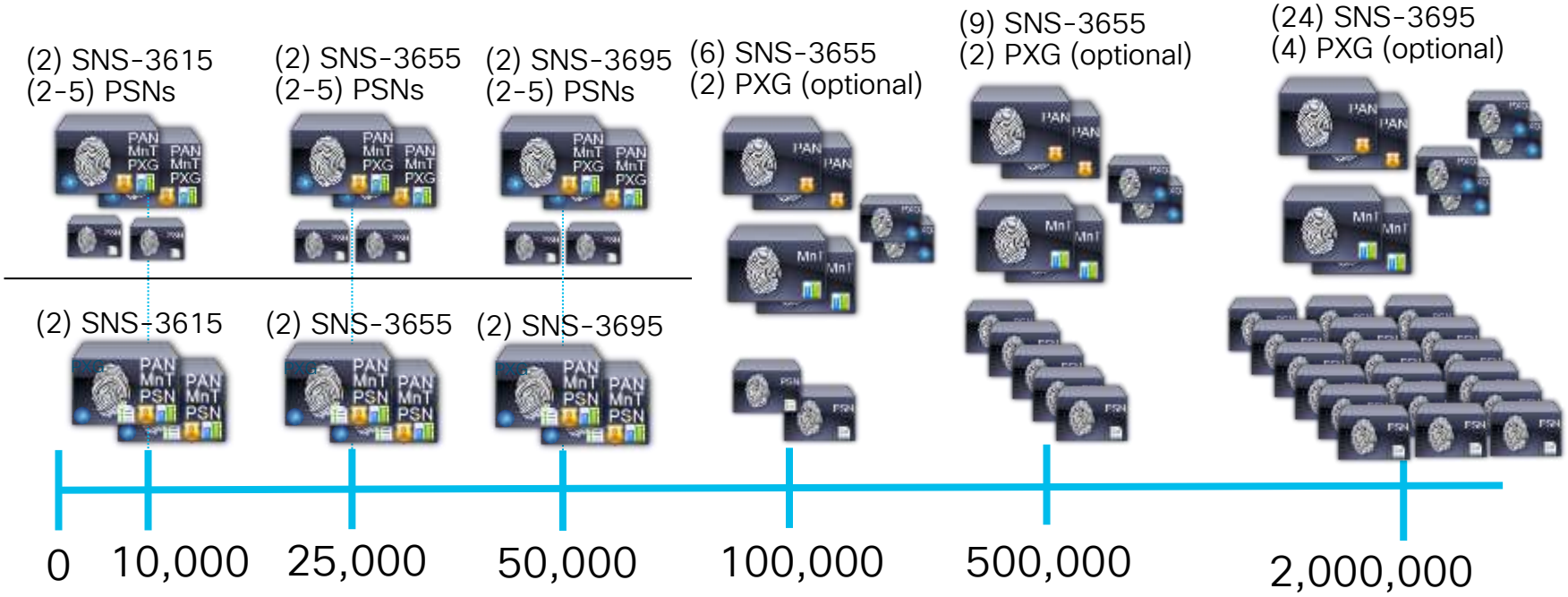


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Session Scaling by Deployment Model 36xx

Minimum Nodes (Redundancy Included) from ISE 2.6



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling ISE

ISE Scaling Improvements

ISE 2.1-2.4

For Your Reference

- Max concurrent active sessions per deployment = **500k** (up from 250k)
  - Requires PAN and MnT nodes to be 3595 or VM equivalent
- Max Internal Endpoints = **1.5M** (up from 1M)
- Max Internal Users = **300k** (up from 25k)
- Max Network Access Devices = **100k** (up from 30k)
- Max Network Device Groups = **10k** (up from 100) ← ISE 2.3+
- Max PSNs per deployment = **50** (up from 40)
- Increased scale based on deployment model (max sessions):

	Standalone or PAN+MnT deployment	Dedicated PSN
SNS-3515	7,500	7,500
SNS-3595	20,000	40,000

ISE Scaling Improvements

For Your Reference

ISE 2.6+ – community link

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

New in ISE 2.6

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

New in ISE 2.6

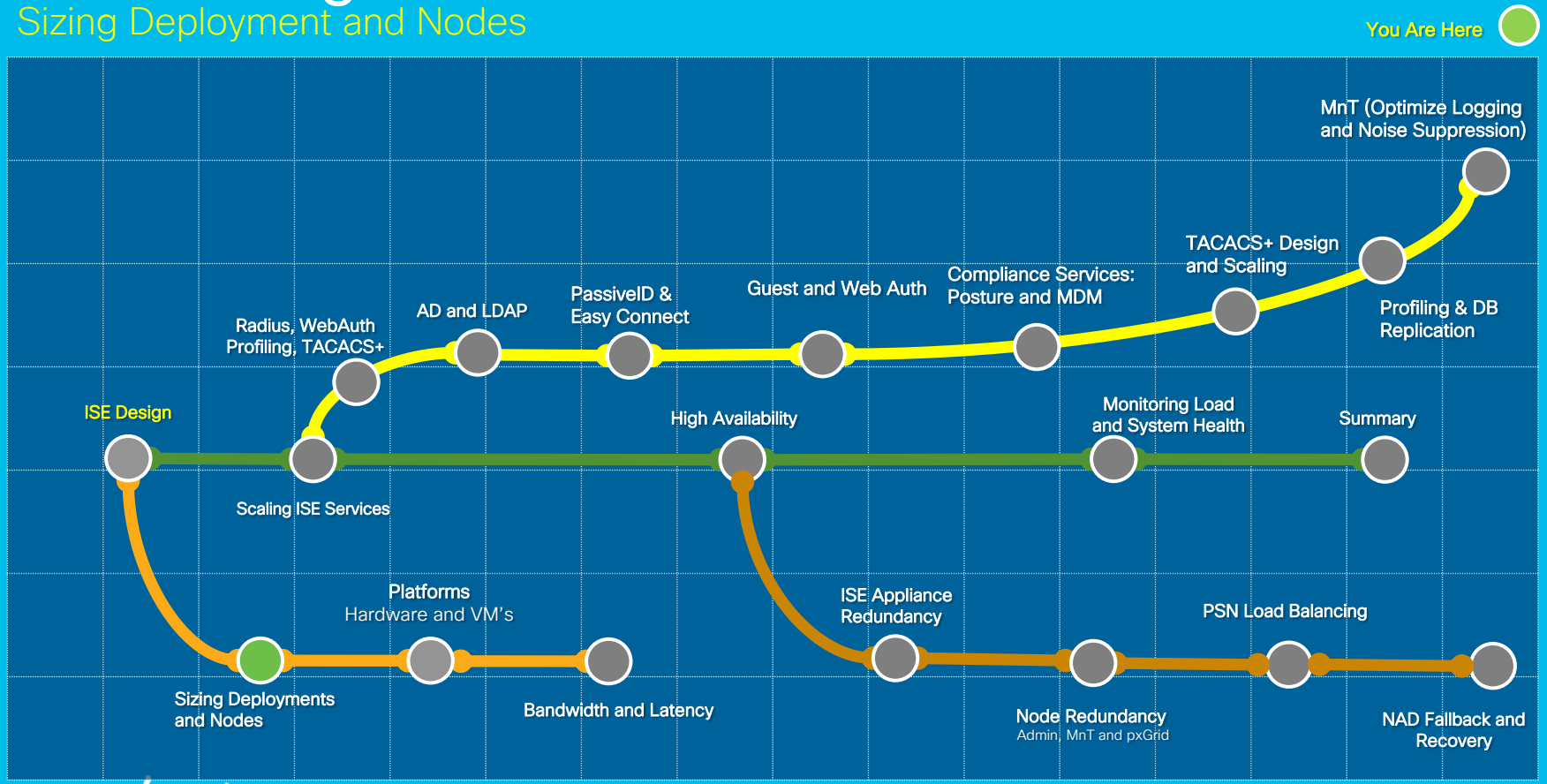
- Max Internal Users = 300k
- Max Network Access Devices = 100k
- Max Network Device Groups = 10k
- Max PSNs per deployment = 50 Increased scale based on deployment model (max sessions):

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

Sizing Deployment and Nodes



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling by Deployment/Platform/Persona (35xx)

Max Concurrent Session Counts by Deployment Model and Platform

For Your Reference

- By Deployment

Deployment Model		Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
Stand-alone	All personas on same node	3515	7,500	0	1 / 2
		3595	20,000	0	1 / 2
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	7,500	5 / 2*	2 / 7
		3595 as PAN+MNT	20,000	5 / 2*	2 / 7
Dedicated	Dedicated PAN and MnT nodes	3595 as PAN and MNT	500,000	50 / 4	3 / 58
		3595 as PAN and Large MNT	500,000	50 / 4	3 / 58

Max Active Sessions != Max Endpoints; ISE 2.1-2.4 supports 1.5M Endpoints

- By PSN

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

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling by Deployment/Platform/Persona (36xx)

Max Concurrent Session Counts by Deployment Model/Platform 2.7

For Your Reference

- By Deployment

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

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

- By PSN

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

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Service Node Sizing

Physical and Virtual Appliance Guidance

- Max Sessions Per Appliance for Dedicated PSN

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

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

General VM appliance sizing guidance:

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

Appliance Hardware Specifications 34/35xx

For Your Reference

Basis for Virtual Appliance Sizing and Redundancy - 35xx required for 2.4

- ISE SNS Appliance Specifications

SNS-3500 Series

Platform	SNS-3415 (34x5 Small)	SNS-3495 (34x5 Large)	SNS-3515 (35x5 Small)	SNS-3595 (35x5 Medium)
Processor	1 x QuadCore Intel Xeon CPU E5-2609 @ 2.40 GHz (4 total cores)	2 x QuadCore Intel Xeon CPU E5-2609 @ 2.40 GHz (8 total cores)	1 x 6-Core Intel Xeon CPU E5-2620 @ 2.30 GHz (6 total cores)	1 x 8-Core Intel Xeon CPU E5-2640 @ 2.60 GHz+20MB Cache (8 total cores)
Memory	16 GB	32 GB	16 GB	64 GB
Hard disk	1 x 600-GB 10k SAS HDD (600 GB total disk space)	2 x 600-GB 10k SAS HDDs (600 GB total disk space)	1 x 600-GB 10k SAS HDD (600 GB total disk space)	4 x 600-GB 10k SAS HDDs (1.2 TB total disk space)
RAID	No	Yes (RAID 1)	No (1GB FBWC Controller Cache)	Yes (RAID 10) (1GB FBWC Cache)
Ethernet NICs	4x Integrated Gigabit NICs	4 x Integrated Gigabit NICs	2 x Integrated GE Ports 4x mLOM GE Ports (6 total LAN ports)	2 x Integrated GE Ports 4x mLOM GE Ports (6 total LAN ports)
Redundant Power?	No (2nd PSU optional)	Yes	No (2nd PSU optional)	Yes

EOL/EOS

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Appliance Hardware Specifications 36xx

For Your Reference

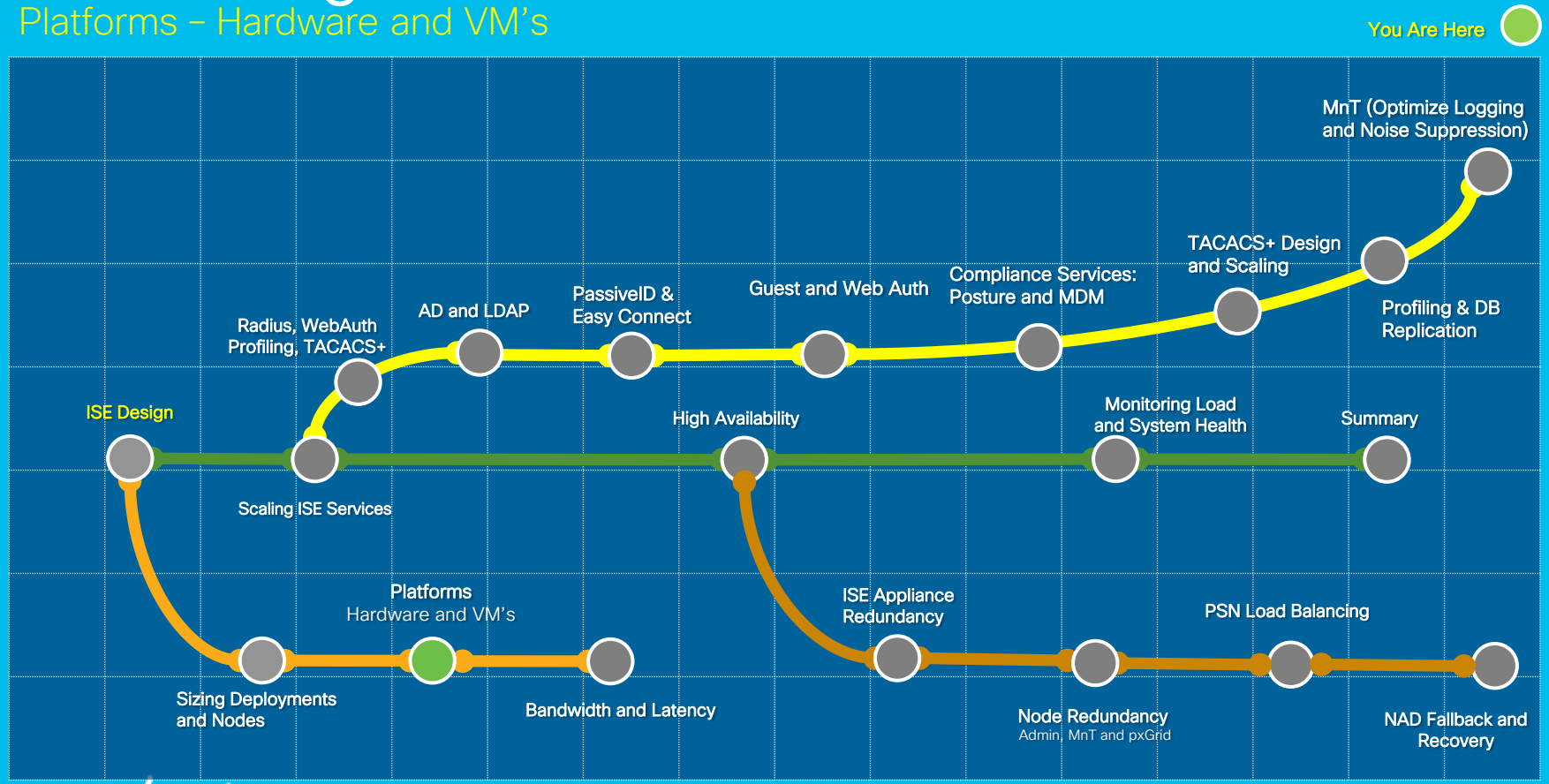
Basis for Virtual Appliance Sizing and Redundancy – supports ISE 2.4+

Platform	SNS-3615 (36x5 Small)	SNS-3655 (36x5 Medium)	SNS-3695 (36x5 Large)
Processor	Intel Xeon CPU 4410 @ 2.10 GHz (8 total cores)	Intel Xeon CPU 4416 @ 2.10 GHz (12 total cores)	Intel Xeon CPU 4416 @ 2.10 GHz (12 total cores)
Memory	32 GB	96 GB	256 GB
Hard disk	1 x 600-GB, 6Gb 10k SAS HDD (600 GB total disk space)	4 x 600-GB, 6Gb 10k SAS HDDs (1200 GB total disk space)	8 x 600-GB, 6Gb 10k SAS HDDs (2400G total disk space)
RAID	No	Level 10	Level 10
Ethernet NICs	2x 10Gbase-T 4x 1GBase-T	2x 10Gbase-T 4x 1GBase-T	2x 10Gbase-T 4x 1GBase-T
Redundant Power?	1x 770W Optional UCSC-PSU1-770W	2x 770W	2x 770W

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

Platforms – Hardware and VM's



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sizing Production VMs to Physical Appliances

Summary

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

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

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

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuring CPUs in VMware

- ESXi 5.x Example

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

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

172.16.1.41 VMware ESXi, 4.1.0, 502767

Getting Started | Summary | Virtual Machines | Resource Allocation

General

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

- ESXi 6.x Example

Virtual Hardware | VM Options | SDRS Rules | vApp Options

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

For Your Reference

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

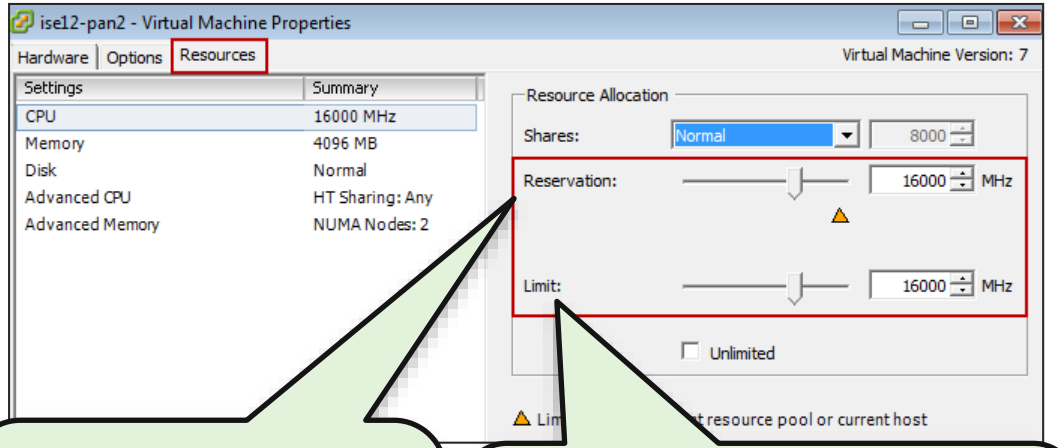
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Setting Memory Allocations in VMware

For Your Reference

Guest VM Resource Reservations and Limits

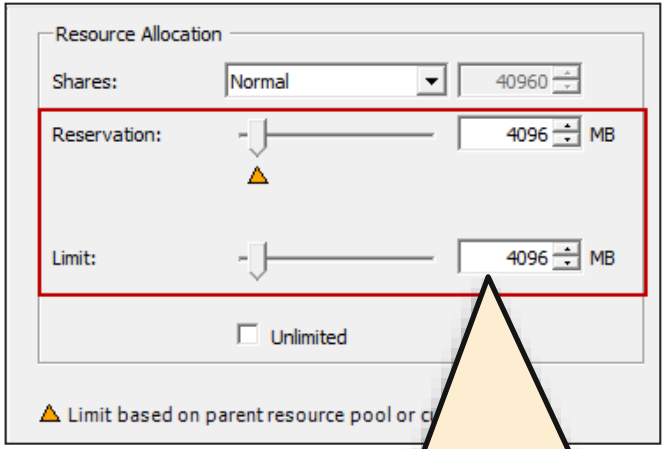
- CPU Example



Set Reservation to Minimum VM appliance specs to ensure required CPU resources available and not shared with other VMs.

Optionally set CPU allocation limit >= Min ISE VM specs to prevent over-allocation when actual CPU assigned exceeds ISE VM requirements.

- Memory Example



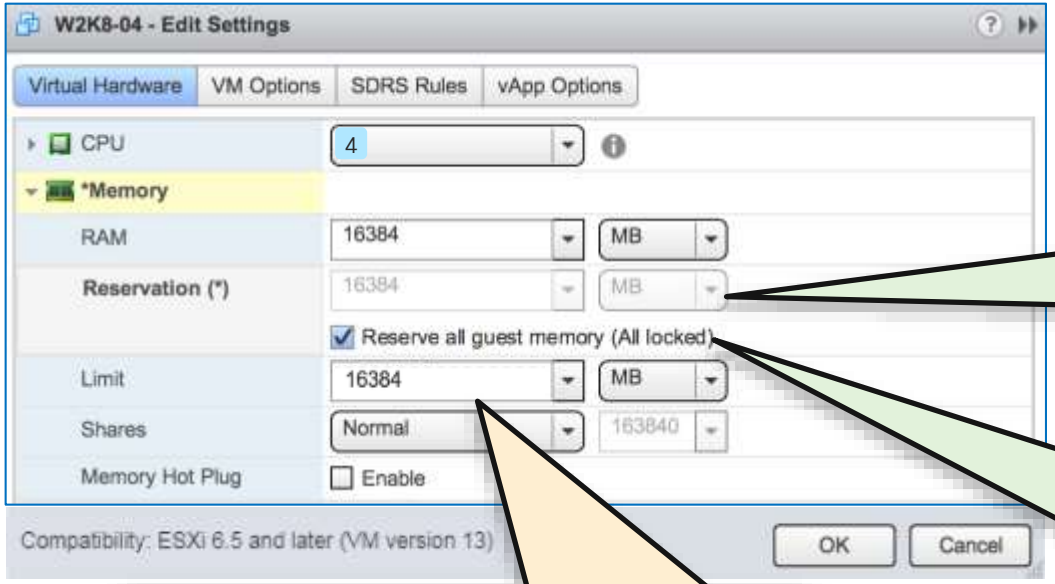
Similar settings apply to Max Allocation and Min Reservations for Memory.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Setting CPU and Memory Allocations in VMware

Guest VM Resource Reservations and Limits

For Your Reference



Set Reservation to Minimum VM appliance specs to ensure required CPU resources available and not shared with other VMs.

"All Locked" is optional. It allows VM to automatically adjust reservations to Memory allocation setting. Otherwise, changes to mem allocation require manual adjustment to reservations.

Similar settings apply to Max Allocation and Min Reservations for Memory.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE OVA Templates

Summary

- "Eval" OVA for PoC/Lab testing up to 100 Endpoints (no resv), 8 gig min if using dot1x/mab only
- All 3xx5 templates reserve CPU and Memory and require hyperthreading
- If require more custom disk option, then deploy .iso
- Disks up to 2.4TB supported for greater MnT storage – requires EFI BIOS in vmware
- ISE 2.6 required for 36xx specs

OVA Template Name ISE-[version]-virtual-	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
eval.ova	2	2.0	4,000	8	4	200GB	EVAL
SNS3515-[disk].ova	6	2.0	12,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3595-[Disk].ova	8	2.0	16,000	64	6	200GB	PSN/PXG
						1.2TB	PAN/MnT
SNS3615-[Disk].ova	8	2.0	16,000	32	6	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3655-[Disk].ova	12	2.0	24,000	96	6	200GB	PSN/PXG
						1.2TB	PAN/MnT
SNS3695-[Disk].ova	12	2.0	24,000	256	6	2.4TB	PAN/MnT

Resource Reservations

Examples:

- ISE-2.3.0.298-virtual-200GB-SNS3515.ova
- ISE-2.4.0.357-virtual-SNS3515-Small-200GBHD-16GBRAM-12CPU.ova

For Your Reference

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling for Platform ?

Small
SNS 3615

Medium
SNS 3655

Large
SNS 3695

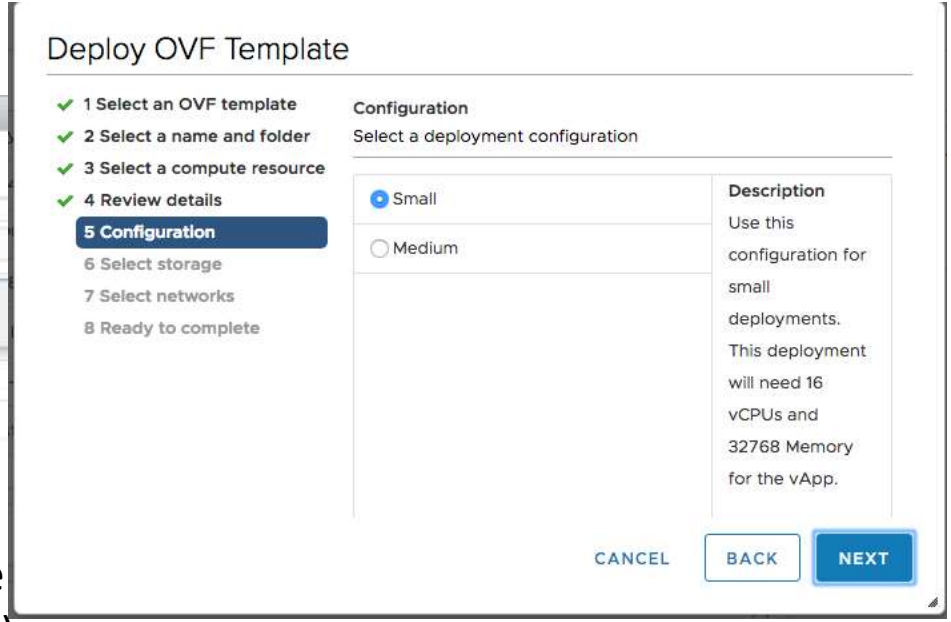
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE now supports deployment options in OVA

ESX embedded UI has a bug with (doesn't work with 2 options) 600, 1.2TB
Vcenter works for all OVA files

vCenter 6x with HTML5

ESXi embedded host client



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.7 OVA Files

Reduced amount of files – using deployment options

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6 OVA Files

Platform Profile – Lets look at the code

The rules for platform selection are defined in PlatformProfileServiceImpl.java

Min

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

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

ile Tag

Medium

16 256 Super Mini <custom>

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why Do I Care?

For Your Reference

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Platform Properties

Minimum VM Resource Allocation – OLD INFO

For Your Reference

Minimum CPUs	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	SNS_3595 <large>

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

Assumes HyperThreading Enabled

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Platform Properties

How Does ISE Detect the Size of my Virtual Machine?

For Your Reference

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Platform Properties

Minimum VM Resource Allocation for SNS35xx/36xx

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

35xx/36xx Newer platforms require hyperthreading

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

NEW

35xx

More to come! On 2.4

36xx

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE OVA Templates

Vmware 6.5 support for ISE 2.4, 6.x supported for 2.6 OVAs

For Your Reference

Description :	ISE 2.4 vCenter 6.0 and 6.5 compatable OVA file - Virtual SNS-3515 200GB (recommend for PSN or PxGrid)
Release :	2.4.0
Release Date :	07-Dec-2018
FileName :	ISE-2.4.0.357-6.5OVA-SNS3515-Small-200GBHD-16GBRAM-12CPU.ova
Size :	13261.56 MB (13905756160 bytes)
MD5 Checksum :	2812b80fb43797d53cee0e266ba89f83
SHA512 Checksum :	c9c54d1a0fae13e6c1ab788ee4d4fd5a ...

Release Notes for 2.4.0 Security Advisory Field Notices

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE OVA Templates

Vmware 6.5

For Your Reference

Platform.properties

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

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


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Platform Detection and Sizing

NEW

Platform	CPU Slots	CPU	Total Physical Cores	Assume Hyper-Threading Enabled	Total Logical Processors
SNS-3515	1	Intel Xeon E5-2620	6	Yes	12
SNS-3595	1	Intel Xeon E5-2640	8	Yes	16
SNS-3615	1	Intel Xeon 4110	8	Yes	16
SNS-3655	1	Intel Xeon 4116	12	Yes	24
SNS-3695	1	Intel Xeon 4116	12	Yes	24

EVAL	< 16 GB & < 4 CPU cores
sns3515 (SNS-3515)	>=16 GB RAM; >=12 CPU cores
sns3595 (SNS-3595)	>=64 GB RAM; >=16 cores CPU
superMNT <custom>	>=256 GB RAM; >=16 cores CPU
sns3615 (SNS-3615)	>=32 GB RAM; >=16 cores CPU
sns3655 (SNS-3655)	>=96 GB RAM; >=24 cores CPU
sns3695 (SNS-3695)	>=256 GB RAM; >=24 cores CPU

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Platform Detection and Sizing

For Your Reference

Verify what ISE is seeing

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

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

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

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

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

```
PlatformProperties show inventory: Process Output:

Profile : UCS_SMALL
Current Memory Size : 15927532
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

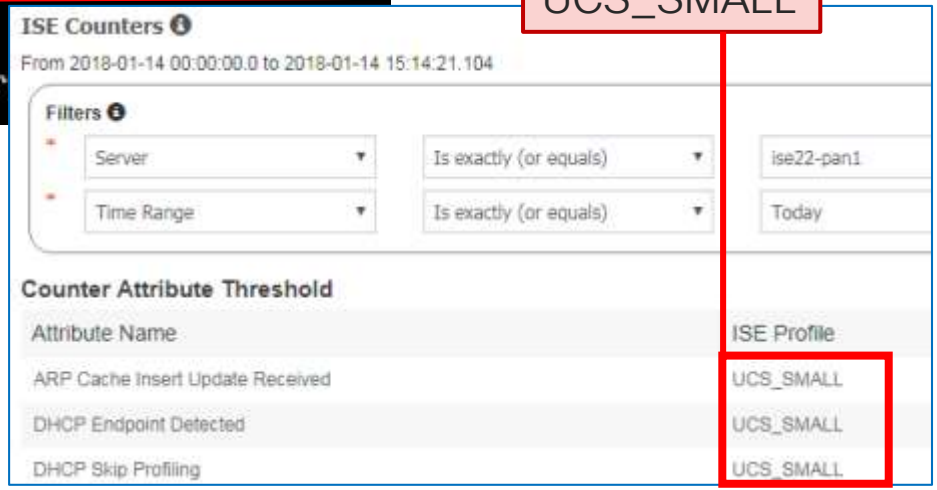
ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

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

```
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:

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

UCS_SMALL



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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Platform Properties

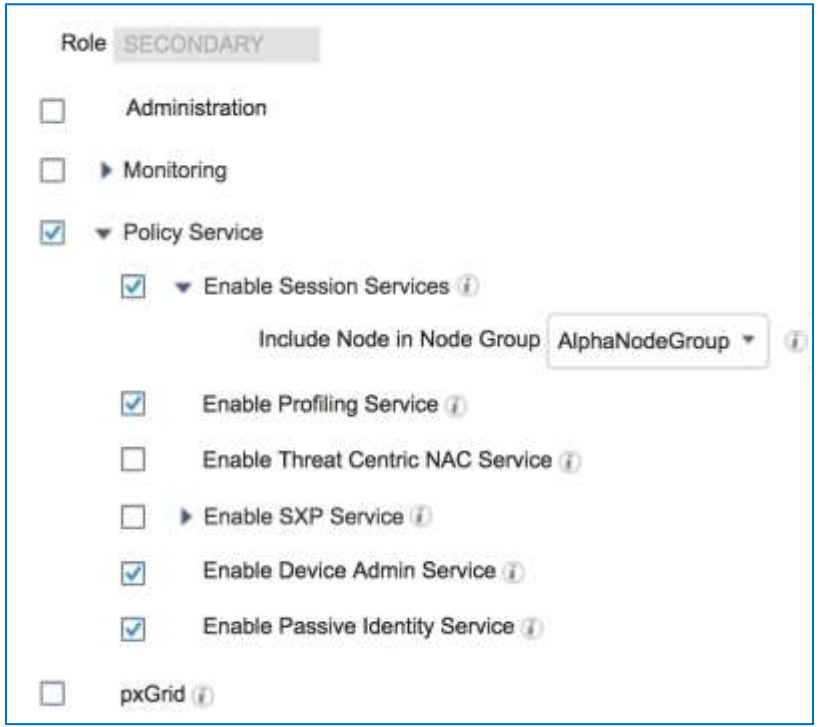
For Your Reference

Forcing ISE to Recognize New Resource Allocations

- From CLI…
  - Requires TAC support to make changes via root patch
  - May be required if application server stuck (cannot acceess Admin UI)

- From Admin UI…
  - Administration > Deployment > [node]
  - Toggle persona change

    (Make change, save, then revert) such as Device Admin or a service not currently in user.



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Hypervisor Support

For Your Reference

- ISE 1.0+ — VMware ESXi 5.x / 6.x
- ISE 2.0+ — RHEL 7.0 or Ubuntu 14.04 LTS
- ISE 2.2+ — MS Windows 2012 R2 or later

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Virtual OS and NIC Support

Note: NIC order normal if < 4 VM NICs.

OVAs have 4 NICs, so E1000 NICs used to avoid order confusion.

For Your Reference

- ISE 2.0/2.1
  - VMware ESXi 5.x / 6.x
  - Linux KVM
- ISE 2.2+
  - VMware ESXi 5.x / 6.x
  - Linux KVM
    - RHEL 7.0 or Ubuntu 14.04 LTS
  - Microsoft Hyper-V on 2012R2 or later
- ISE 2.6+
  - Linux KVM RHEL 7.3
  - Release notes & install guide

Bootable USB: http://www.linuxliveusb.com/

Notes for VMware Virtual Appliance installs using ISO image (OVA recommended):

- Choose Redhat Linux 7 (64-bit) (ISE 2.0.1+)
- Manually enter resource reservations

Virtual Network Interfaces

- Choose either E1000 or VMXNET3 (default)
- ISE 2.0+ supports up to (6) Network Adapters
- ESX Adapter Ordering Based on NIC Selection:

ADE-OS	ISE	E1000	VMXNET3
eth0	GE0	1	4
eth1	GE1	2	1
eth2	GE2	3	2
eth3	GE3	4	3
eth4	GE4	5	5
eth5	GE5	6	6

ISE VM Disk Storage Requirements

For Your Reference

Minimum Disk Sizes by Persona 2.x

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

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

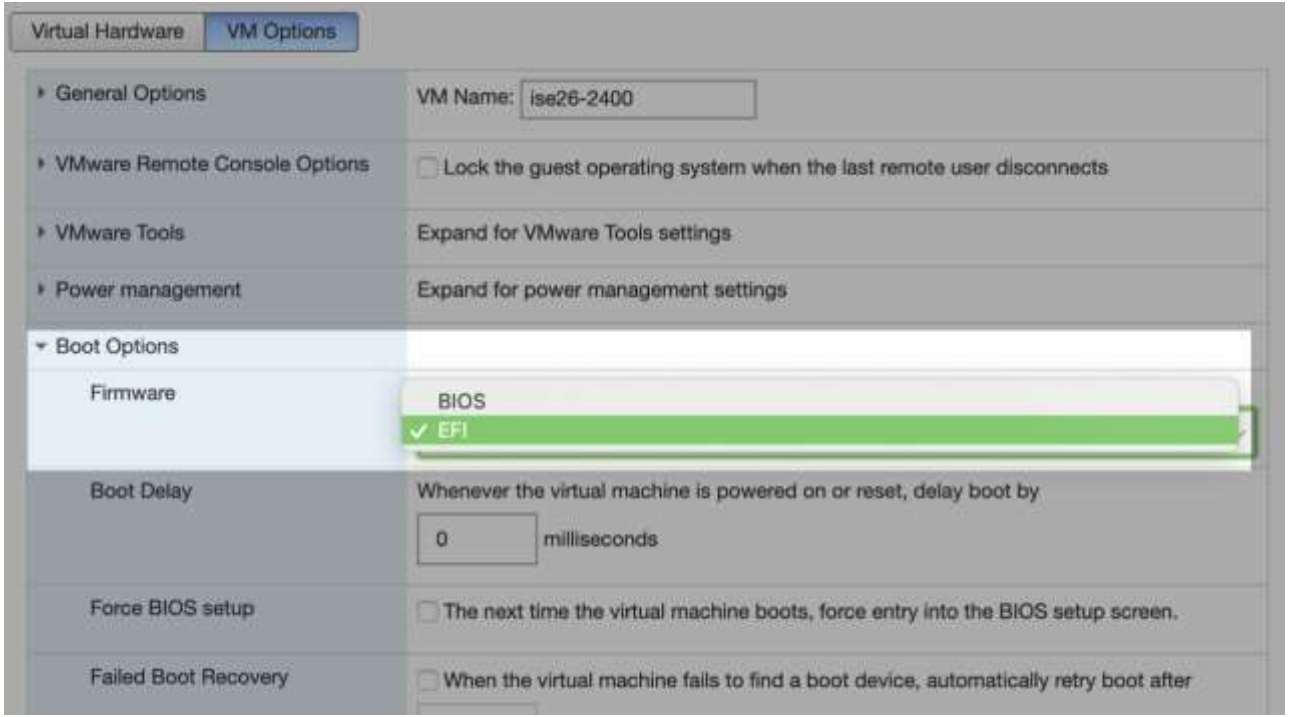
Persona	Disk (GB)
Standalone	200+*
Administration (PAN) Only	200-300**
Monitoring (MnT) Only	200+*
Policy Service (PSN) Only	200
PAN + MnT	200+*
PAN + MnT + PSN	200+*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE VM Disk Storage Requirements

For Your Reference

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



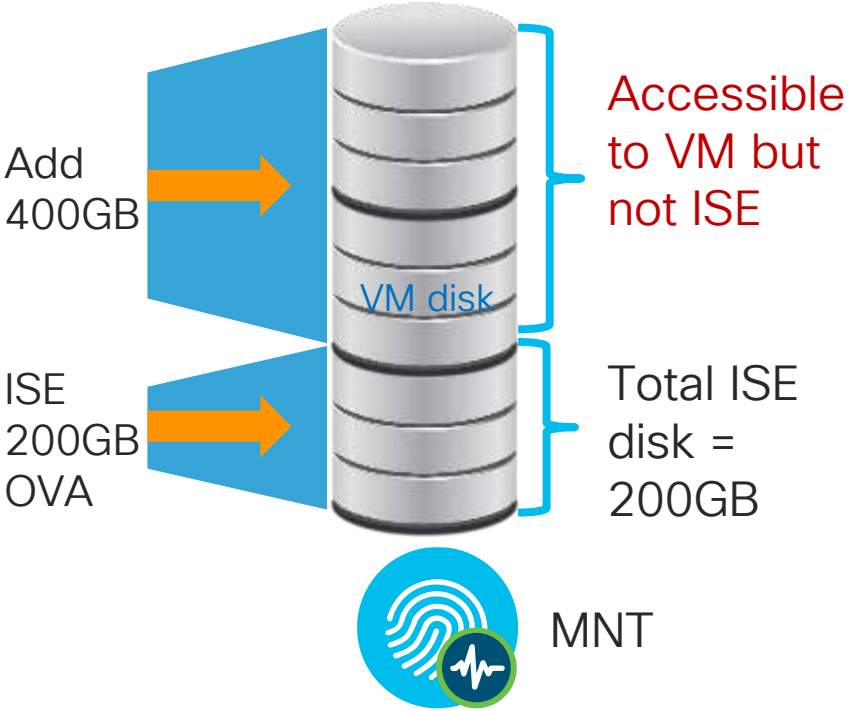
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

VM Disk Allocation

For Your Reference

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

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Node Log Storage Requirements for RADIUS

For Your Reference

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

Total Disk Space Allocated to MnT Node

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

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

ISE 2.2 = 50% days increase over 2.0/2.1

ISE 2.3 = 25-33% increase over 2.2

ISE 2.4 = 40-60% increase over 2.2

Assumptions:

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

For Your Reference

MnT Node Log Storage Requirements for T+

Days Retention Based on # Managed Network Devices and Disk Size

Total Disk Space Allocated to MnT Node

Total NADs	200 GB	400 GB	600 GB	1024 GB	2048 GB	2400 GB
100	12,583	25,166	37,749	64,425	128,850	154,016
500	2,517	5,034	7,550	12,885	25,770	30,804
1,000	1,259	2,517	3,775	6,443	12,885	15,402
5,000	252	504	755	1,289	2,577	3,081
10,000	126	252	378	645	1,289	1,541
25,000	51	101	151	258	516	617
50,000	26	51	76	129	258	309
75,000	17	34	51	86	172	206
100,000	13	26	38	65	129	155

ISE 2.3+ optimizations do not apply to T+ logging

Assumptions:

- Script runs against all NADs
- 4 sessions/day
- 5 commands/ session

Based on 60% allocation of MnT disk to TACACS+ logging
(Prior to ISE 2.2, only 20% allocations)

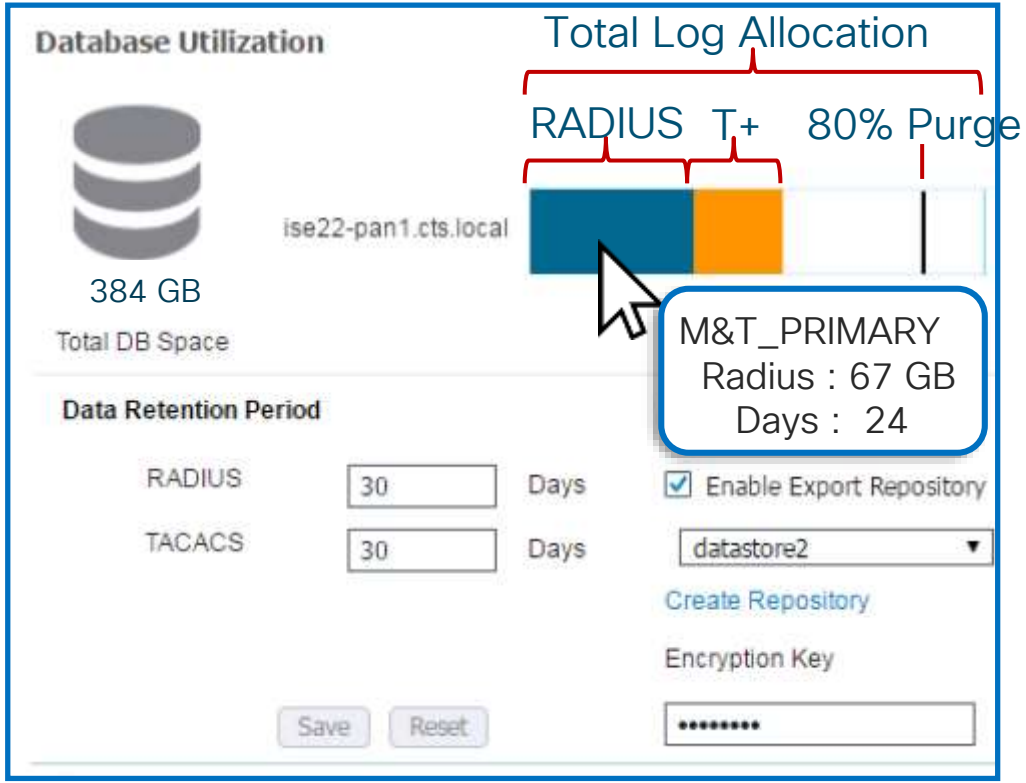
RADIUS and TACACS+

MnT Log Allocation

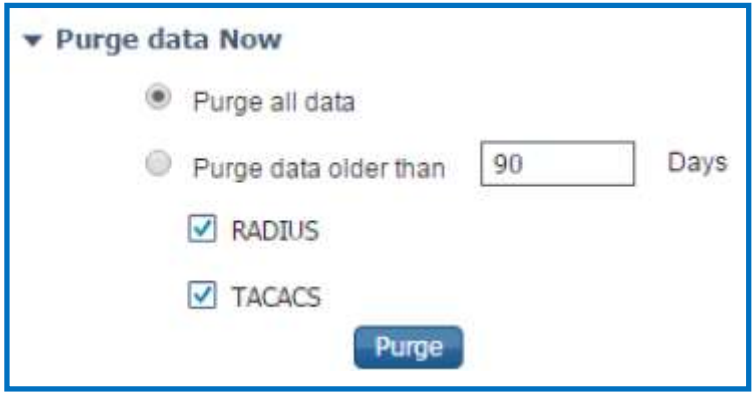
For Your Reference

ISE 2.2+

- Administration > System > Maintenance > Operational Data Purging



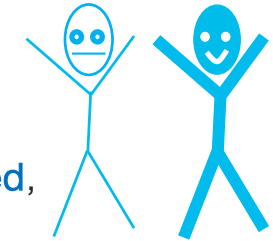
- 60% total disk allocated to both RADIUS and TACACS+ for logging
  (Previously fixed at 30% and 20%)
- Purge @ 80% (First In-First Out)
- Optional archive of CSV to repository



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE VM Disk Provisioning Guidance

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



IO Performance Requirements:

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

Recommended disk/controller:

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

  Slower writes using RAID 5*

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE VM Provisioning Guidance

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Disk IO Performance Testing

Sample Tests With and Without RAID Controller Caching

For Your Reference

- Caching Disabled
  - Average Write ~ 25 MB/s

```
Displaying VM IO performance metrics
****************************************
104857600 bytes (105 MB) copied, 6.73469 seconds, 15.6 MB/s
104857600 bytes (105 MB) copied, 3.22354 seconds, 32.5 MB/s
104857600 bytes (105 MB) copied, 9.72238 seconds, 10.8 MB/s
104857600 bytes (105 MB) copied, 4.59899 seconds, 22.8 MB/s
104857600 bytes (105 MB) copied, 2.7162 seconds, 38.6 MB/s
104857600 bytes (105 MB) copied, 3.91479 seconds, 26.8 MB/s
104857600 bytes (105 MB) copied, 2.05225 seconds, 51.1 MB/s
104857600 bytes (105 MB) copied, 12.922 seconds, 8.1 MB/s
104857600 bytes (105 MB) copied, 3.09572 seconds, 33.9 MB/s
```

- Caching Enabled
  - Average Write ~ 300 MB/s
  - > 10x increase!

```
Displaying VM IO performance metrics
****************************************
104857600 bytes (105 MB) copied, 0.181695 seconds, 577 MB/s
104857600 bytes (105 MB) copied, 0.610613 seconds, 172 MB/s
104857600 bytes (105 MB) copied, 0.202946 seconds, 517 MB/s
104857600 bytes (105 MB) copied, 0.371386 seconds, 282 MB/s
104857600 bytes (105 MB) copied, 0.302722 seconds, 346 MB/s
104857600 bytes (105 MB) copied, 0.446572 seconds, 235 MB/s
104857600 bytes (105 MB) copied, 0.739407 seconds, 142 MB/s
104857600 bytes (105 MB) copied, 0.858859 seconds, 122 MB/s
104857600 bytes (105 MB) copied, 0.605648 seconds, 173 MB/s
104857600 bytes (105 MB) copied, 0.212591 seconds, 493 MB/s
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Disk IO Performance Testing

For Your Reference

Sample Tests Using Different RAID Config and Provisioning Options

- 2x Write performance increase using Eager vs Lazy 0
  - Note: IO performance equalizes once disk blocks written
- 5x Write performance increase using RAID 10 vs RAID 5

	RAID Config	Read	Write	Write Perf ↑ over 1	Write Perf ↑ over 2	Write Perf ↑ over 3
1	RAID 5: 4-Disk Lazy Zero	697 MB/s	9 MB/s	NA	NA	NA
2	RAID 5: 4-Disk Eager Zero	713 MB/s	16 MB/s	78% (~2x)	NA	NA
3	RAID 10: 4-Disk Eager Zero	636 MB/s	78 MB/s	767% (~10x)	388% (~5x)	NA
4	RAID 10: 8-Disk Eager Zero	731 MB/s	167 MB/s	1756% (~20x)	944% (~10x)	114% (~2x)

Read Performance roughly the same

Write Performance impact by RAID config

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

VM Appliance Resource Validation *Before* Install

For Your Reference

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

Available boot options:

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

Enter boot option and press <Enter

boot: _
```

```
Available System Utilities:

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

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

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


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

Validate VM Readiness *BEFORE* Install & Deploy

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

VM Appliance Resource Validation *During* Install

```
Enter username[admin]:
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Virtual machine detected, configuring VMware tools...
Testing VM disk I/O performance...
Average I/O bandwidth writing to disk device: 18 MB/second
Average I/O bandwidth reading from disk device: 683 MB/second
WARNING: VM I/O PERFORMANCE TESTS FAILED!
         The bandwidth writing to disk must be at least 50 MB/second,
         and bandwidth reading from disk must be at least 300 MB/second.
         Continuing installation, however this VM should not be used for
         production use until disk performance is addressed.  You can
         use the 'show tech-support' CLI to retest VM I/O performance
         after installation completes.

Do not use 'Ctrl-C' from this point on...


Installing Applications...
Installing ISE ...
```

For Your Reference

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

VM Installation – Absolute Minimum Requirements

- ISE 2.x install will not even proceed without:
  - 4GB RAM
  - 2 CPU Cores
  - 100GB Disk
- Rec minimum 8GB RAM & 200Gig Disk
- Absolute minimum settings used for ~20 sessions in *evaluation* setup only.

For Your Reference

```
Starting installer, one moment...
anaconda 19.31.123-1 for Red Hat Enterprise Linux 7.1 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
00:53:58 Running pre-installation scripts
```

```
Starting installer, one moment...
anaconda 19.31.123-1 for Red Hat Enterprise Linux 7.1 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
```

```
Starting installer, one moment...
anaconda 19.31.123-1 for Red Hat Enterprise Linux 7.1 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
02:17:31 Running pre-installation scripts
***** checking for supported platform
***** Virtual Machine host detected...
***** Hard disk(s) total size detected: 53 Gigabyte
***** Physical RAM size detected: 4047884 Kbytes
***** Number of network interfaces detected: 1
***** Number of CPU cores detected: 2
***** Clock speed of CPU in MHz: 2933
***** Verifying RAM requirement...
***** ERROR: UNSUPPORTED VM CONFIGURATION.
***** THE INSTALLER DETECTED LESS THAN REQUIRED 100 GIGABYTES
***** DISK SPACE FOR THE VM INSTALLATION.
***** Exiting installation...
```

VM Appliance Resource Validation *After* Install

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

For Your Reference

```
ise-psn2/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
****************************************
Average I/O bandwidth writing to disk device: 194 MB/second
Average I/O bandwidth reading from disk device: over 1024 MB/second
I/O bandwidth performance within supported guidelines
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 1.47
Disk I/O bandwidth filesystem read test,
314572800 bytes (315 MB) copied, 0.05
```

Alarm generated if 24-hr average below requirements

Alarms

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

VM Appliance Resource Validation *After* Install

For Your Reference

Alarms: Insufficient Virtual Machine Resources

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

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

Acknowledge Refresh

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

Alarm generated if 24-hr average below requirements

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

General ISE VM Configuration Guidelines

For Your Reference

Oversubscription of CPU, Memory, or Disk storage NOT recommended – All VMs should have 1:1 mapping between virtual hardware and physical hardware.

CPU: Map 1 VM vCPU core to 1 physical CPU core.

- Total CPU allocation should be based on physical CPU cores, not logical cores, but with HT enabled, you must allocate double the # logical CPUs to ISE VM.

Memory: Sum of VM vRAM may not exceed total physical memory on the physical server.

- Additional 1 GB+ of physical RAM must be provisioned for hypervisor itself (this is to cover overhead to run VMs). Refer to hypervisor release notes for actual requirements.

Disk: Map 1 GB of VM vDisk to 1 GB of physical storage.

- Additional disk space may be required for VMware operations including snapshots.

In general, OVAs help simplify install + reserve resources, but be aware of custom disk sizes and CSCvh71644 – OVAs allocating only ½ required CPUs (OK in 2.4+)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introducing “Super” MnT

For Any Deployment where High-Perf MnT Operations Required

- ISE 2.4 Virtual Appliance Only option
  - Requires Large VM License
- 3595 specs + 256 GB (3695 appliance/VM 2.6)
  - 8 cores @ 2GHz min (16000+ MHz)
    = 16 logical processors
  - 256GB RAM
  - Up to 2TB* disk w/ fast I/O
- Fast I/O Recommendations:
  - Disk Drives (10k/15k RPM or SSD)
  - Fast RAID w/Caching (ex: RAID 10)
  - More disks (ex: 8 vs 4)

MnT

* CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB, fixed in 2.6

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4+ MnT+ Fast Access to Logs and Reports

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Live Logs | Live Sessions

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

Refresh: Never | Show: Latest 50 records | Within: Last 30 minutes

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Ide
				Identity	Endpoint ID	Endpoint Prof	Authentication	Authorization	Authorization	IP Address	Network Device	Device Port	Id
Jan 26, 2018 11:06:16.262 AM			0	sussin	98:5A:EB:8E:FD:16	Apple-Device	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.16			
Jan 26, 2018 11:05:50.519 AM				jose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:05:34.504 AM				INVALID			Building_SJ...	Building_SJ...			WNBU-WLC1		
Jan 26, 2018 11:05:32.821 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:05:23.126 AM			0	50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN_...				
Jan 26, 2018 11:05:23.126 AM				50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN_...		NTN-WLC1		Wo
Jan 26, 2018 11:05:11.995 AM				vani	AC:BC:32:AC:7E:23						sjc19-00a-wlc1		
Jan 26, 2018 11:04:54.173 AM			0	kusanape	DC:EF:CA:4D:41:1F	Unknown	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.46			
Jan 26, 2018 11:04:27.145 AM			0	6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_El_C...	Location_BX...	Location_BX...	Guest_Redir...	10.86.103.138			
Jan 26, 2018 11:04:23.999 AM				6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_El_C...	Location_BX...	Location_BX...	Guest_Redir...		sampg-bxb22-0...		Wo
Jan 26, 2018 11:04:10.882 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:04:06.040 AM				USERNAME\USE...	4C:EB:42:C7:31:70		Bldg_SJC19...	Bldg_SJC19...			sjc19-00a-wlc1		
Jan 26, 2018 11:04:04.493 AM				jose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:04:03.462 AM			0	vinothra	7C:50:49:63:CC:F0	Apple-iPhone	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.14			

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4+ MnT Vertical Scaling Scaling Enhancements

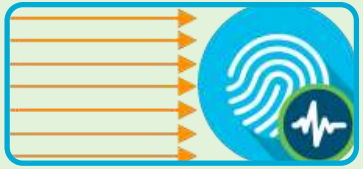
Benefits MnT on ALL ISE platforms

Faster Live Log Access

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

Faster Report & Export Performance

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



Collector Throughput improvement

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

Major Data Reduction

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 MnT Vertical Scaling Scaling Enhancements

For Your Reference

- Differentiated the data/columns into 2 parts.
  - --Details data, for short retention and is amounting around 80% of the MNT DB.
  - --Reports data, for long term retention and is amounting to 20%.
- Normalized big tables, Radius auth/ Radius acc into multiple small tables as per the observed data patterns.
- Reduced redundant data volume by de-duplicating (sample data volume of 14 Million records reduced to 1k-3k records in normalized tables).
- The data size got reduced by approximately 80% after Normalization/De-duplication.
- Tables with more recent data like live logs are pinned to memory.
- Tables containing frequently searched data like Endpoints, NADs and Auth data is also pinned to memory.
- Tables with details data has been separated and not pinned to memory.
- Purging has been removed for Endpoints, NADs etc.,
- Retaining max one week data of Radius Auth details.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 MnT Vertical Scaling Scaling Enhancements

Results

For Your Reference

Scaling:

- Normalisation and Deduplication helped to reduce data size drastically.
- With the separated main report data, we are able to store 20 times more than current data for same disk usage.
- We are able to store 2 Million endpoints at least 4-6 months after the changes.

Performance:

- Search timings on the normalized tables improved from 10 min to 0.2 – 4 seconds, due to their small sized tables(in kb and mb only)
- By reducing the data size more data is pinned to memory that improved overall performance.
- Time taken to generate report with NAD search resulted in 548409 records got reduced from 7 minutes to 3 seconds
- Time taken to generate report with Endpoint search resulted in 8 records got reduced from 8 minutes to 0.4 seconds

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

ISE 2.4 Super MnT

Scale Test Results/Observations

Scenarios	Results (256GB RAM + 4 HDDs)	Results (256GB RAM + 8 HDDs)	Performance Gain
Live Log: initial load of live log page	30 Sec	10 Sec	67%
Live Log : show 100 records within Last 3 hours	20 Sec	5 Sec	75%
Live Log with Filters: Identity (Scale)	55 Sec	25 Sec	55%
Live Log with Filters: (Network device name)	40 Sec	15 Sec	63%
Reports: single session Today Launch	42 Sec	5 Sec	88%
Reports: single session 30 Days Launch	180 Sec	75 Sec	58%

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

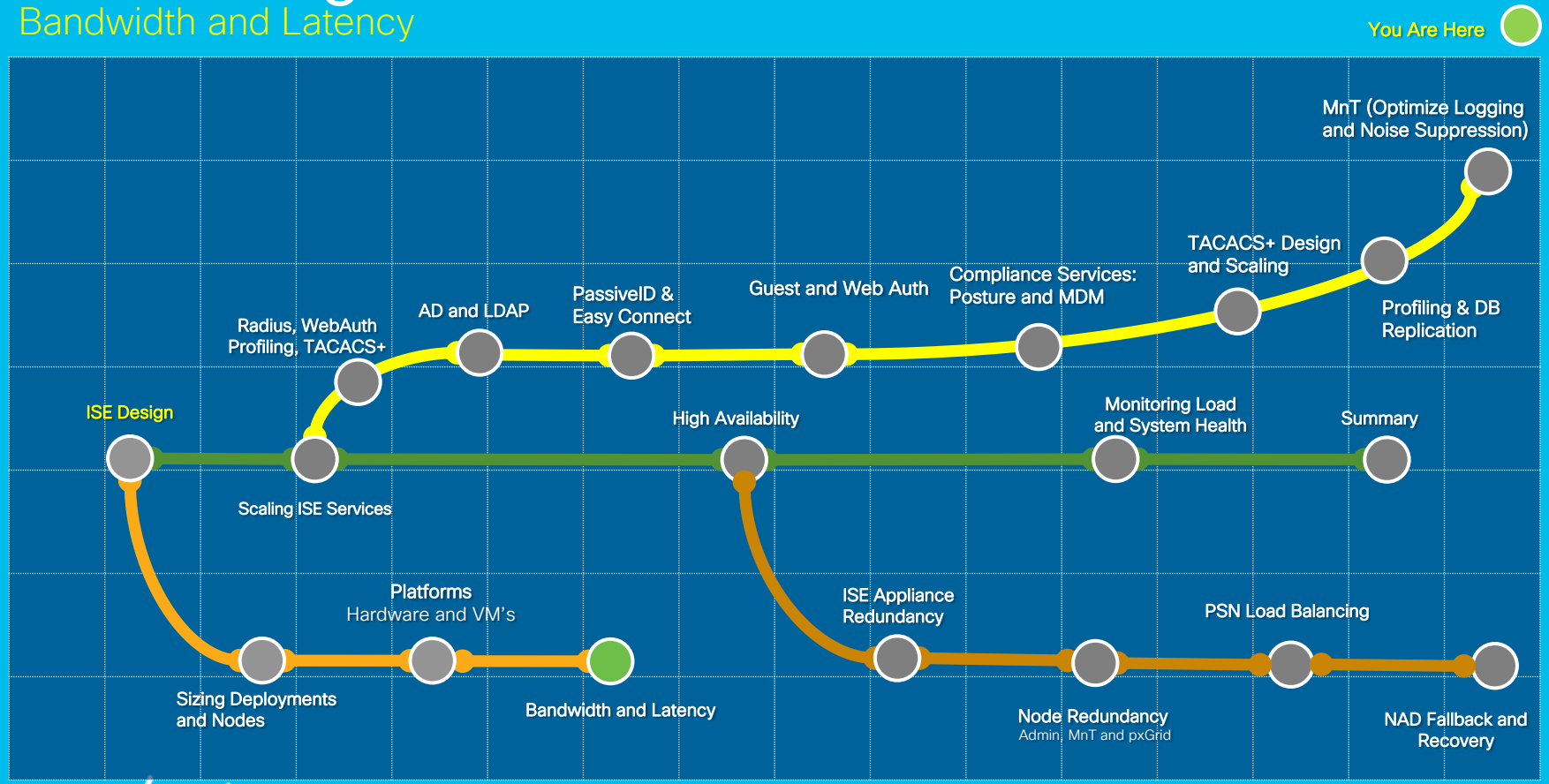
Where is my Super MnT VM ?

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

Bandwidth and Latency

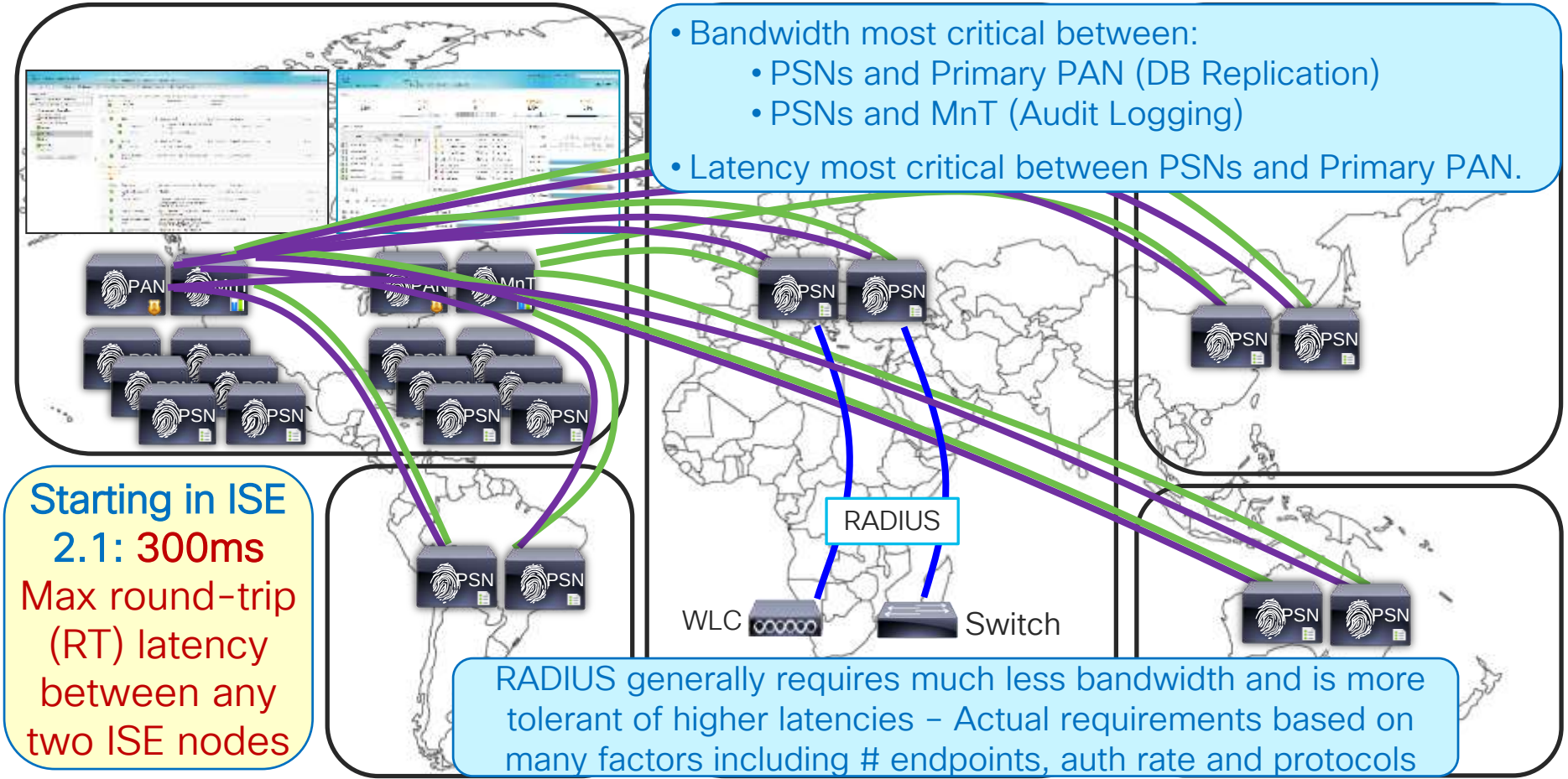


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Bandwidth and Latency

Bandwidth and Latency

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



Starting in ISE 2.1: 300ms Max round-trip (RT) latency between any two ISE nodes

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

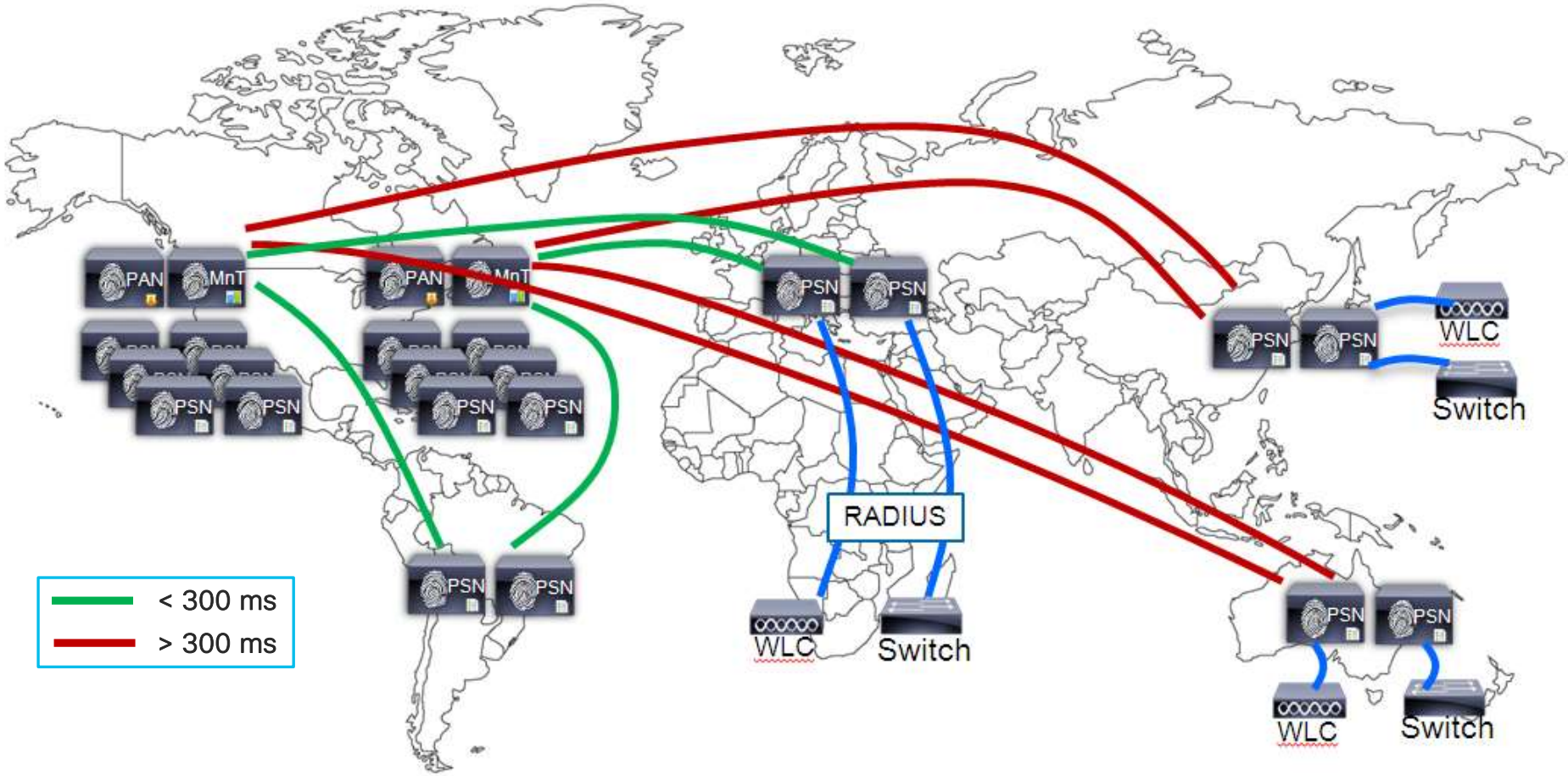
Have I Told You My Story Over Latency Yet?

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

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

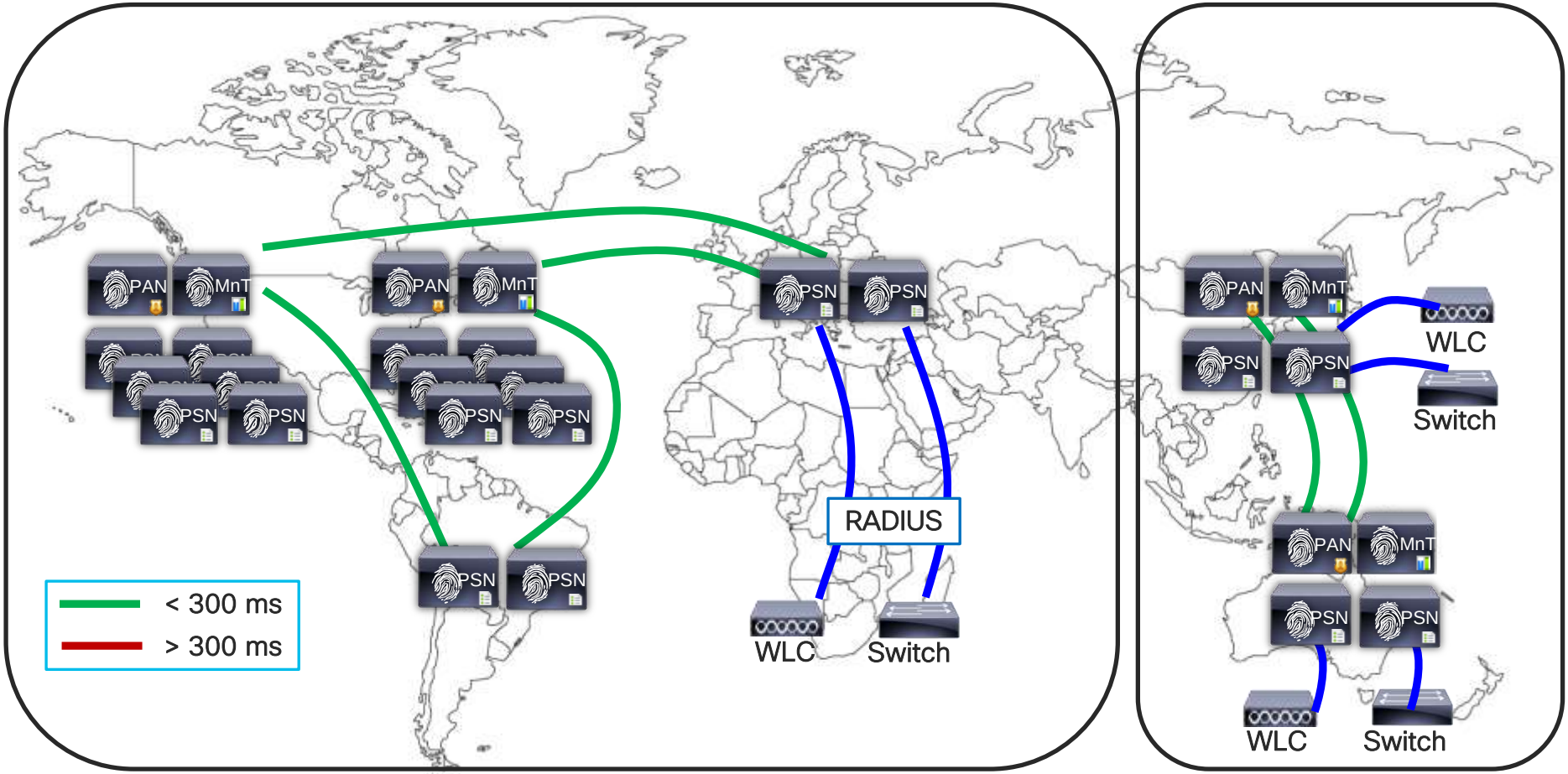
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

What if Distributed PSNs > 300ms RTT Latency?

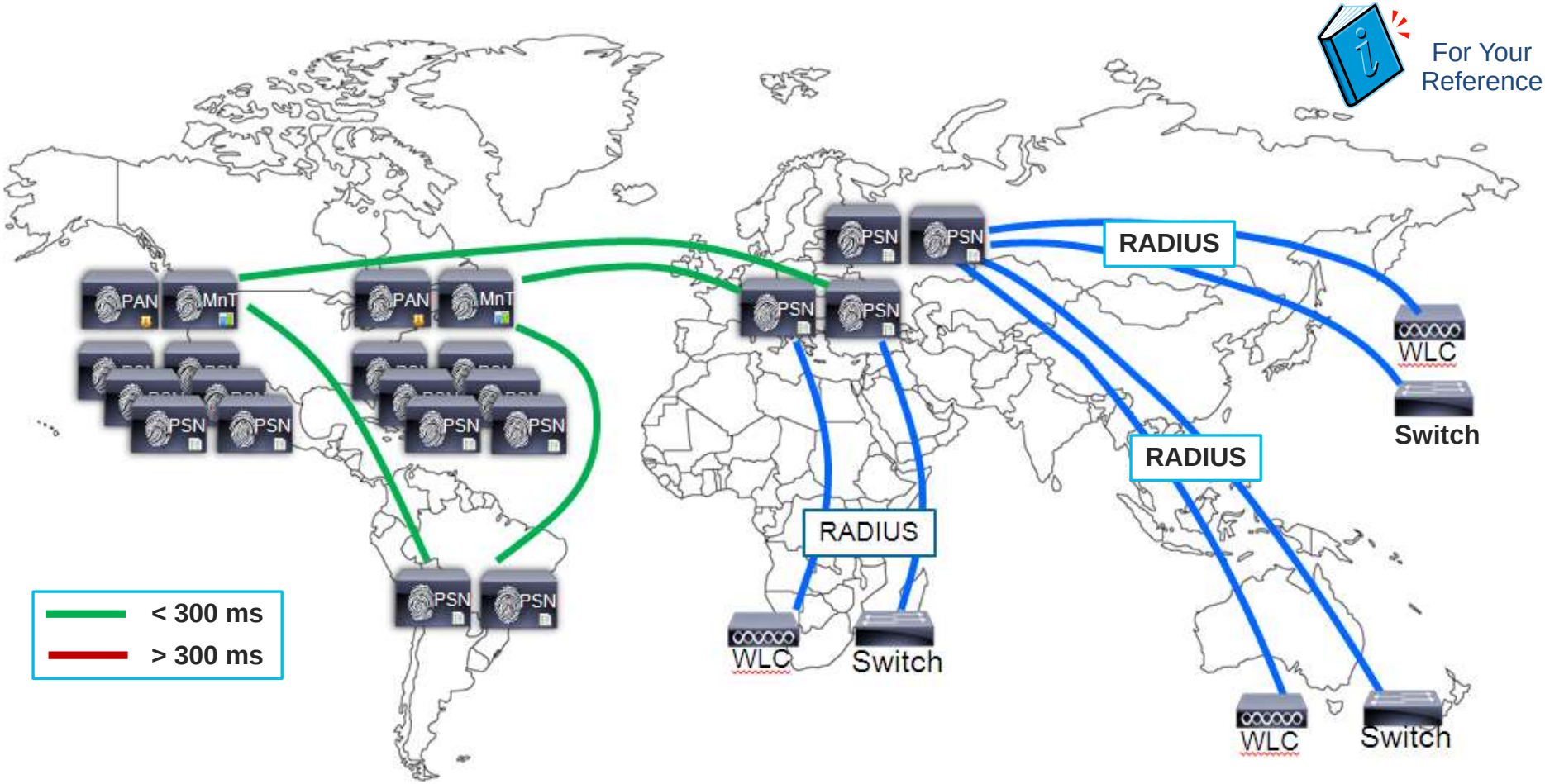


Option #1: Deploy Separate ISE Instances

Per-Instance Latency < 300ms

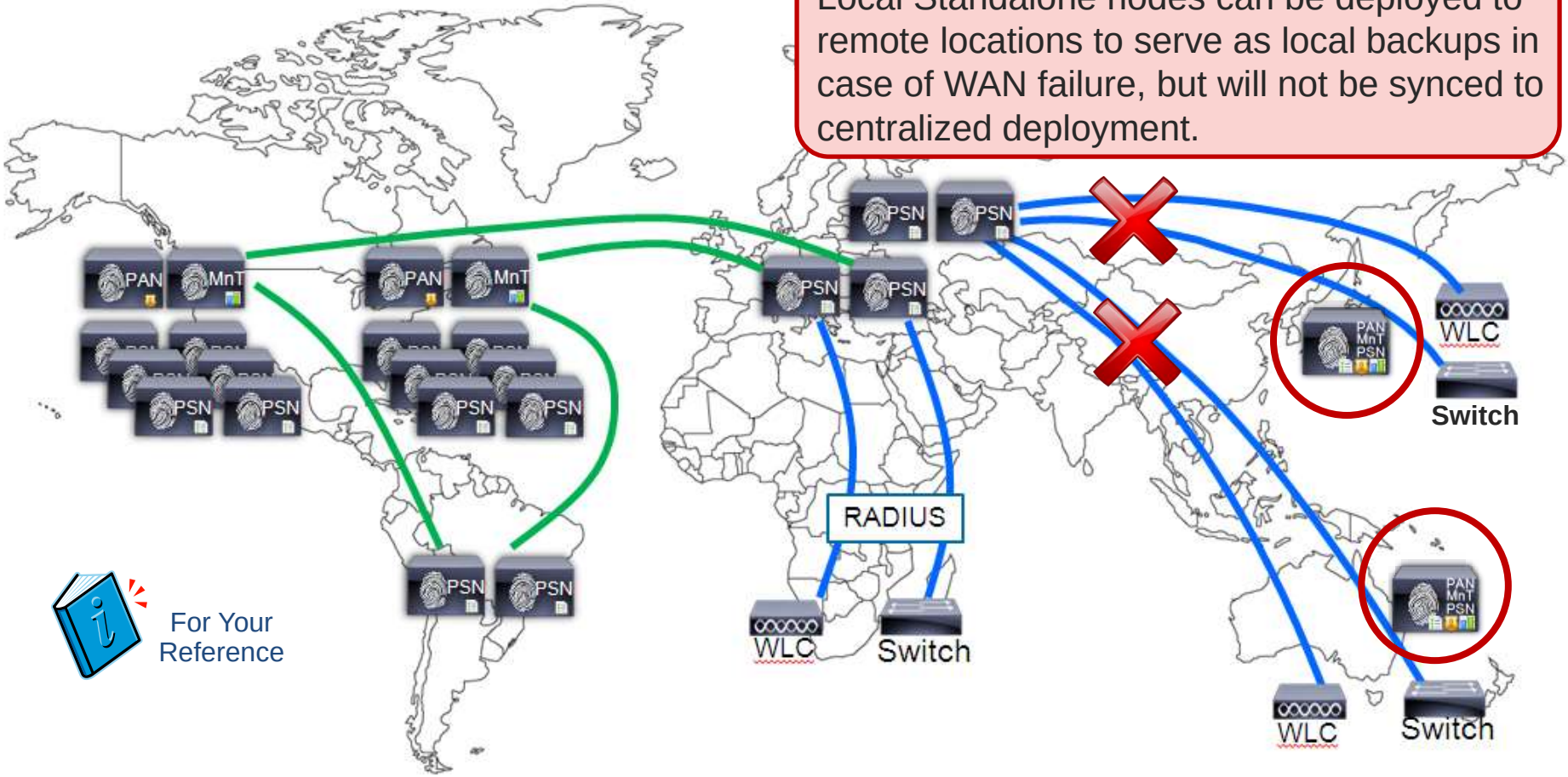


Option #2: Centralize PSNs Where Latency < 300ms



Deploy Local Standalone ISE Nodes as “Standby”

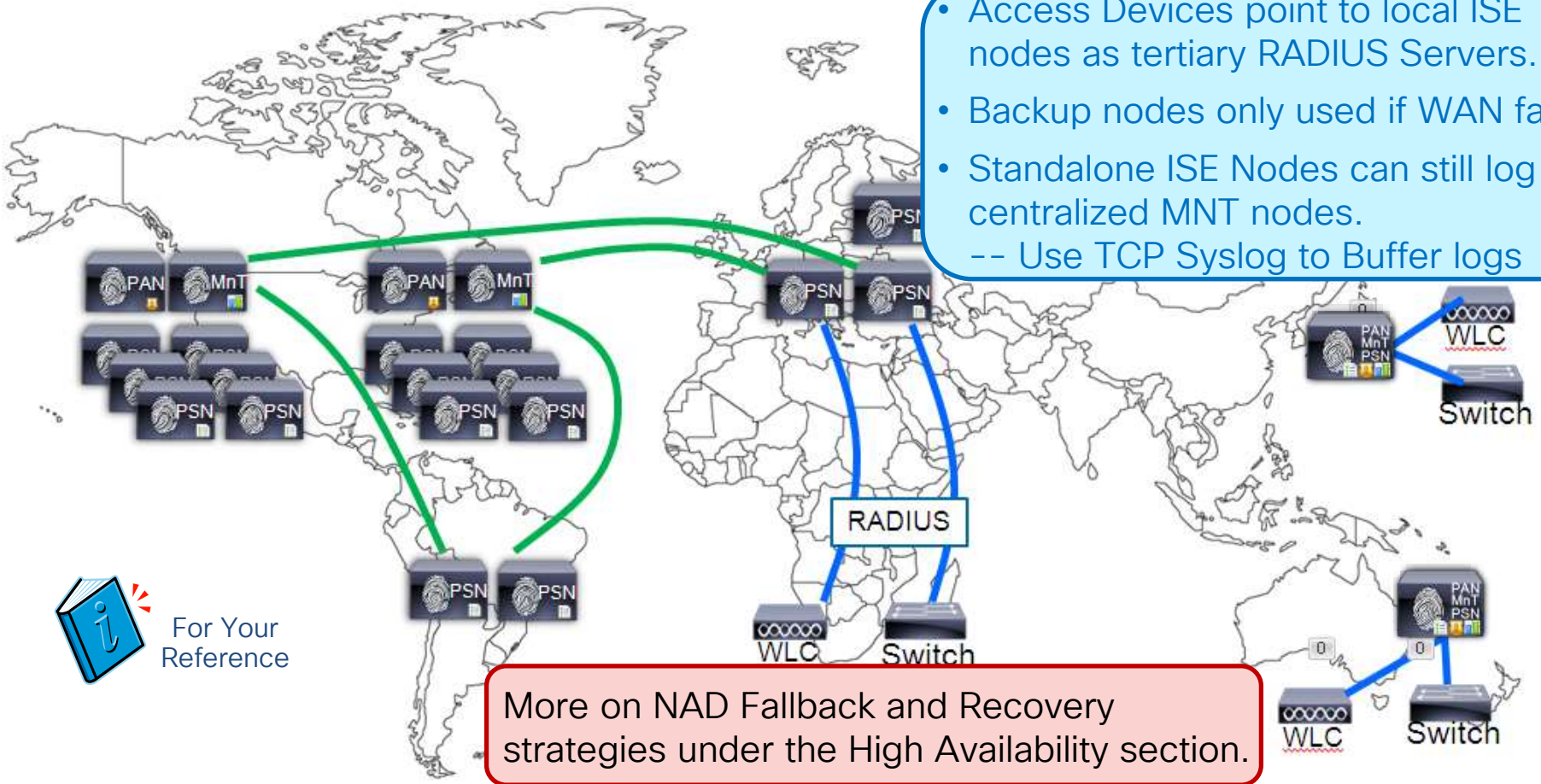
Local Standalone nodes can be deployed to remote locations to serve as local backups in case of WAN failure, but will not be synced to centralized deployment.



For Your Reference

Access Devices Fallback to Local PSNs on WAN Failure

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



For Your Reference

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

ISE Bandwidth Calculator (Single-Site)

For Your Reference

ISE 1.x Network Bandwidth Calculation for Single Remote Location	
Total Active Endpoints in ISE	25,000
% Mobile Endpoints in ISE Deployment	20
Reauth Interval (hrs)	2
DHCP Lease Period (hrs)	4
Total Active Endpoints at Remote Site	10,000
% Mobile Endpoints at Remote Site	20
# PSN nodes at Remote Site	2
Secondary PAN node at Remote Site? (1=yes, 0=no)	1
Secondary MnT node at Remote Site? (1=yes, 0=no)	1
Sending profile data for same endpoints to multiple locations? (1=yes, 0=no)	0
Total BW Required for WAN Link from Remote Site to Primary	1.51

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Bandwidth Calculator – Updated for ISE 2.1+

ISE 2.x Network Bandwidth Calculation for Multiple Remote Locations

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

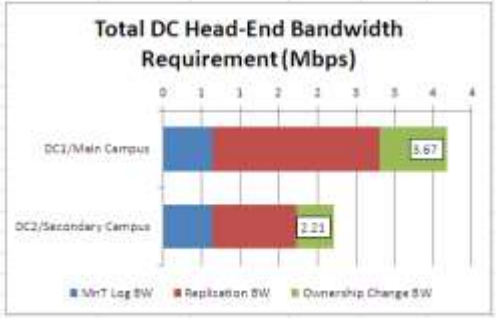
Reset Remote Location Data

INSTRUCTIONS:

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

(P)=Primary (S)=Secondary

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



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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Bandwidth Calculator Assumptions

For Your Reference

- ISE Auth Suppression enabled
- Profiling Whitelist Filter enabled
- One node group per location

- **Max round-trip latency between any two ISE nodes is currently set at 300ms**

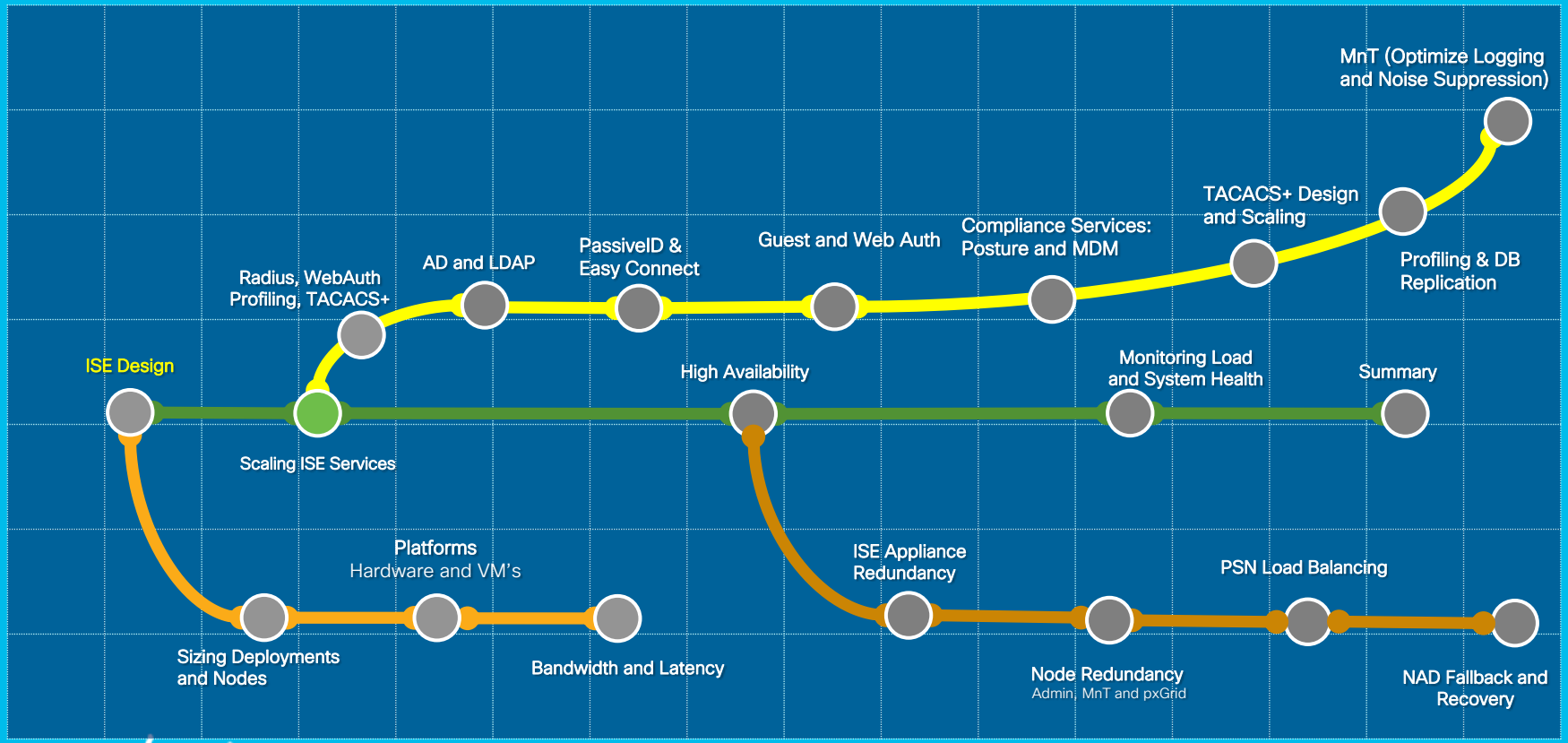
- For Single-Site calculation, primary PAN and MnT nodes are deployed in primary DC to which bandwidth is calculated; For Multi-Site calculation, primary PAN is deployed in primary DC.
- Mobile endpoints authenticate/reauthenticate as frequently as 10/hr and refresh IP 1/hr
- Non-Mobile endpoints authenticate/reauthenticate no more than once per Reauth Interval and refresh IP address no more than once per DHCP renewal (1/2 Lease Period)
- Bandwidth required for NAD or Guest Activity logging is not included. These logging activities are highly variable and should be treated separately based on deployment requirements.
- Bandwidth required for general RADIUS auth and accounting traffic is not included. RADIUS traffic is generally less significant but actual requirement is highly contingent on multiple factors including total active endpoints, reauth intervals, and the authentication protocols used.
- Deployments where all ISE nodes are deployed in one location are not considered by this calculator. All nodes deployed in the same location are assumed to be connected by high-speed LAN links (Gigabit Ethernet or higher)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling ISE Services

Session Agenda

Scaling ISE Services



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling ISE Services Agenda

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

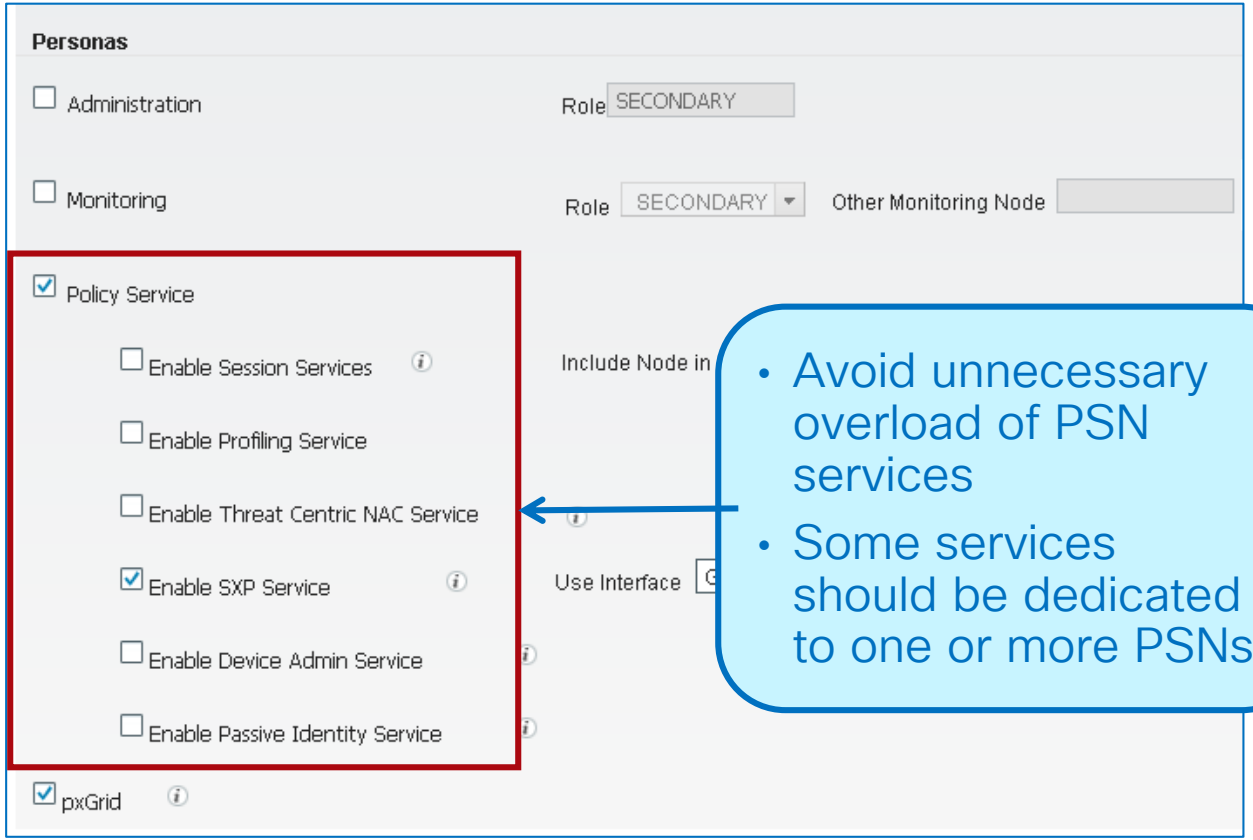
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Personas and Services

Enable Only What Is Needed !!

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

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



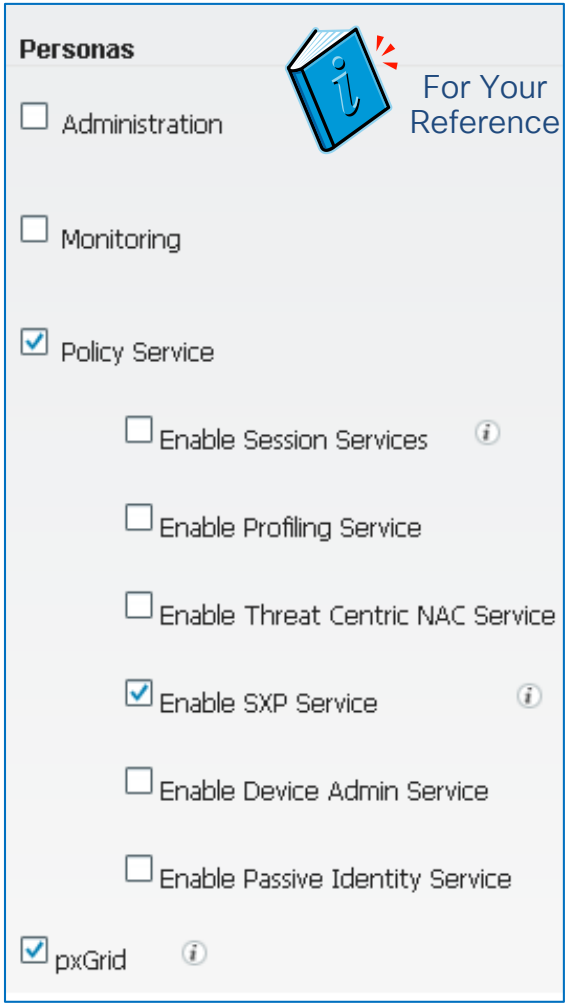
- Avoid unnecessary overload of PSN services
- Some services should be dedicated to one or more PSNs

cisco Live!

ISE Personas and Services

Maximum Personas and PSN nodes running service

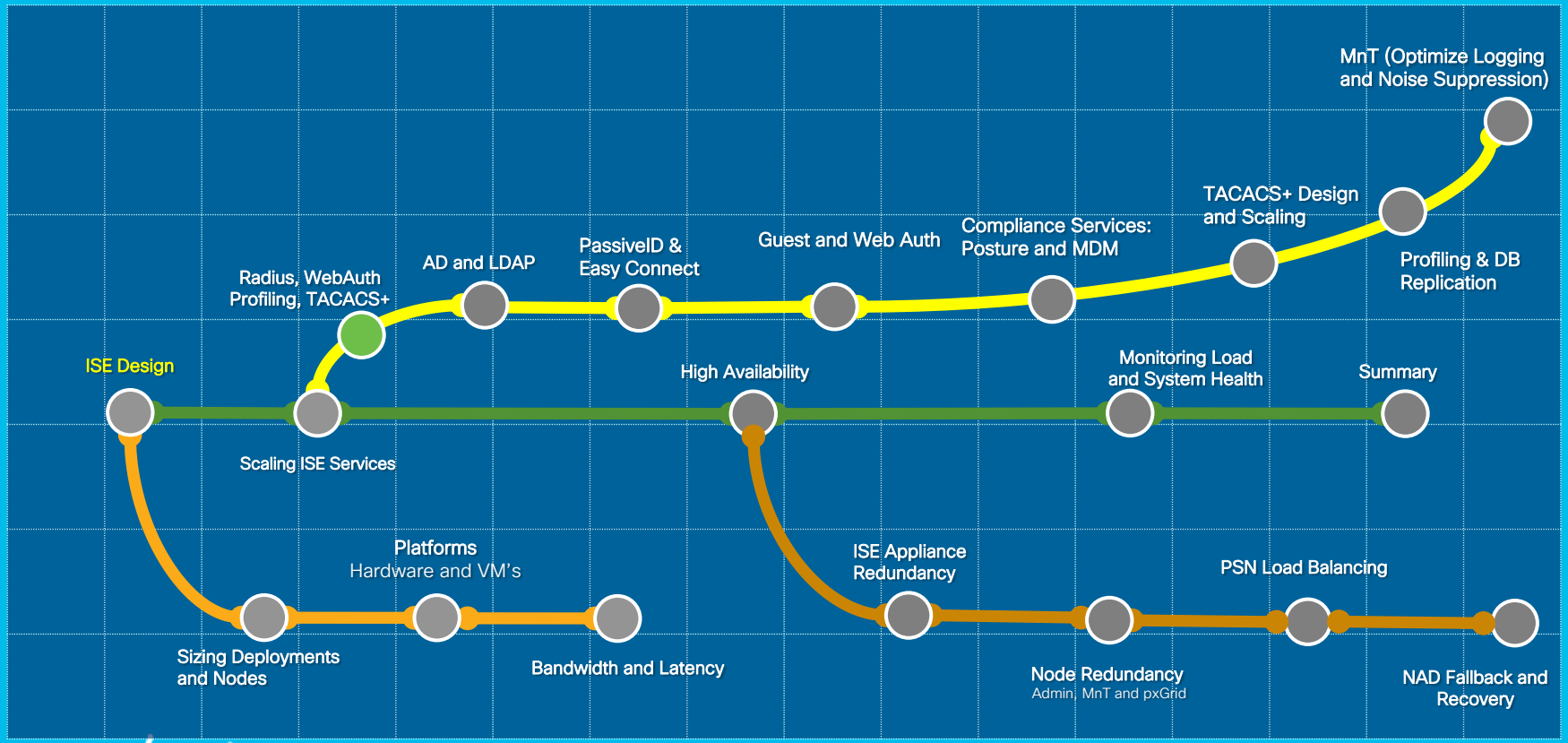
Persona / Service	Maximum Nodes	Comments
PAN	2	Admin UI restricts to 2
MnT	2	Admin UI restricts to 2
pxGrid	4	Increased from 2 in ISE 2.4
PSN	50	Requires 3595/3655/3695 PAN/MnT
Session	50	
Profiling	50	Typically enabled w/Session
TC-NAC	1	Admin UI restricts to 1
ISE SXP	4	Up to 2 SXPSN pairs
Device Admin (T+)	50	Typically 2 sufficient
Passive Identity	Multiple	2+ recommended for WMI



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

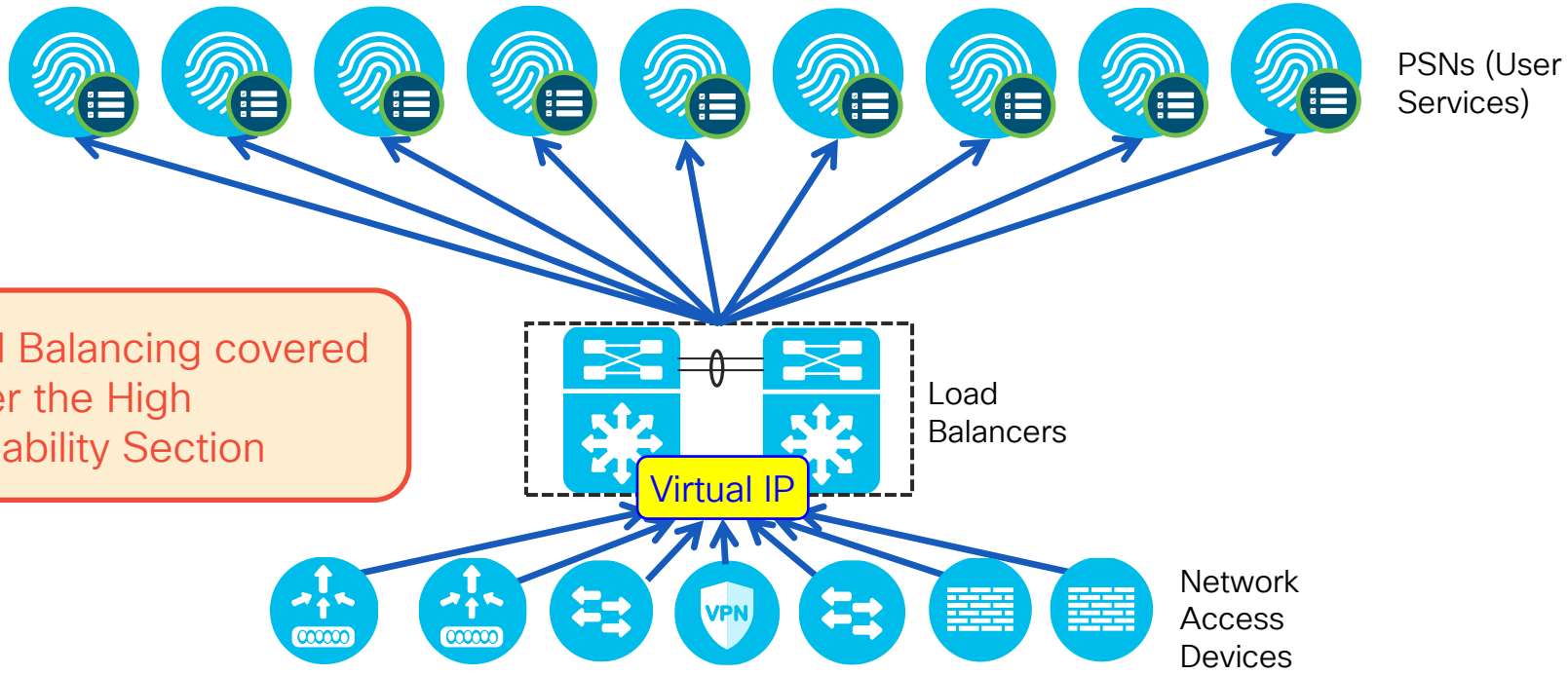
Radius, Web Auth, Profiling, TACACS



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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



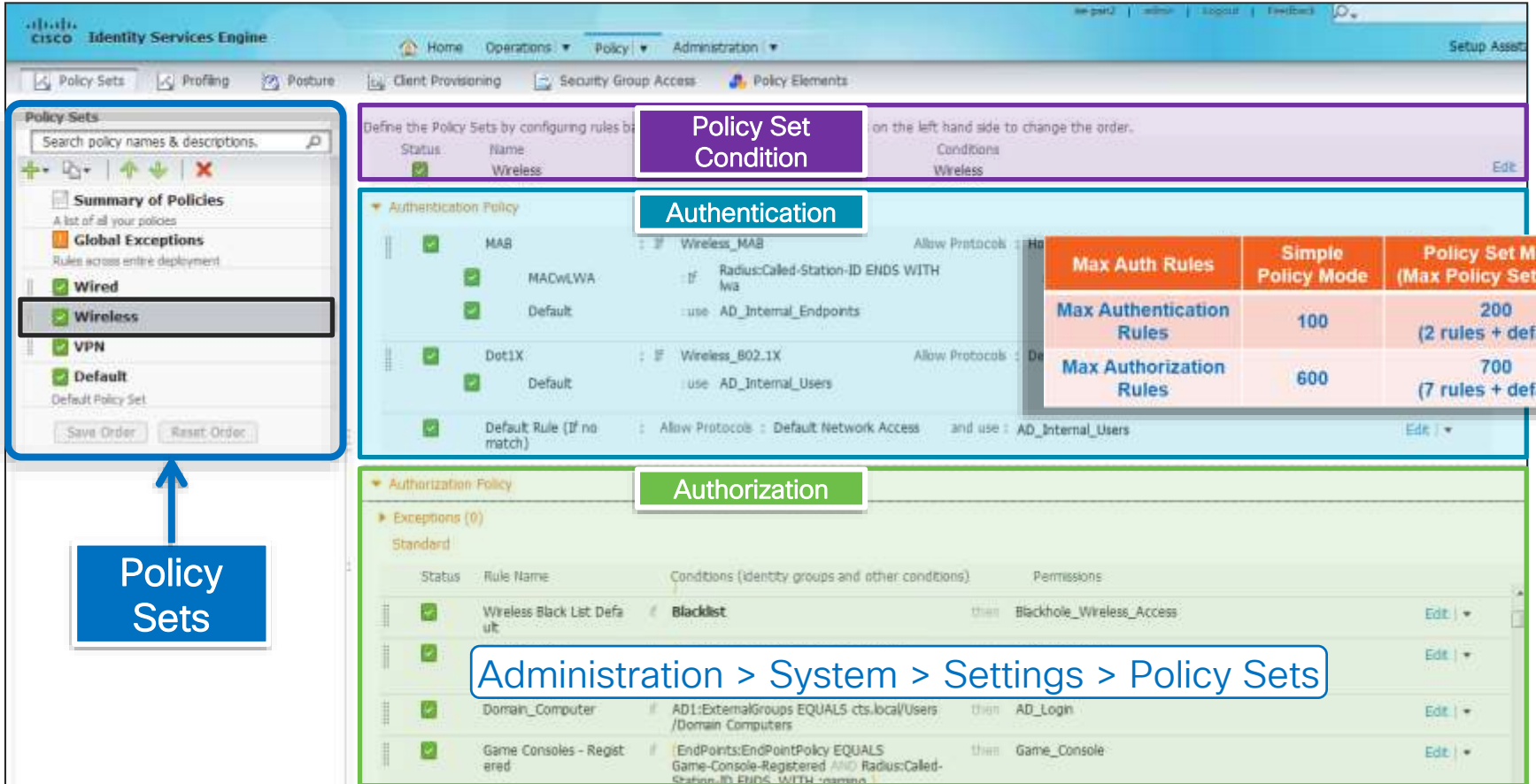
Load Balancing covered under the High Availability Section

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization (ISE 2.2 and Earlier)

For Your Reference

Leverage Policy Sets to Organize and Scale Policy Processing



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

Policy Sets

For Your Reference

Standard Equipment under new ISE 2.3 Policy User Interface

- No Authentication Outer Rule – Now part of Policy Set

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Policy Sets

Reset | Save

Policy Set Condition

Allowed Protocol or RADIUS Proxy

Hit Counts

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
		Wired	Wired Network Access	Radius·NAS-Port-Type EQUALS Ethernet	Default Network Access	23456		
		Wireless	Wireless Network Access	Radius·NAS-Port-Type EQUALS Wireless - IEEE 802.11	Default Network Access	0		
		VPN	VPN Network Access	Radius·NAS-Port-Type EQUALS Virtual	Default Network Access	0		
		Default	Default policy set		Default Network Access	0		

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization

Avoid Unnecessary External Store Lookups

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

Authorization Policy

Exceptions (0)

Standard

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

Example of a Poor Rule: Employee_MDM

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

For Your Reference

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization

Rule Sequence and Condition Order is Important!

For Your Reference

Authorization Policy

Exceptions (0)

Standard

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

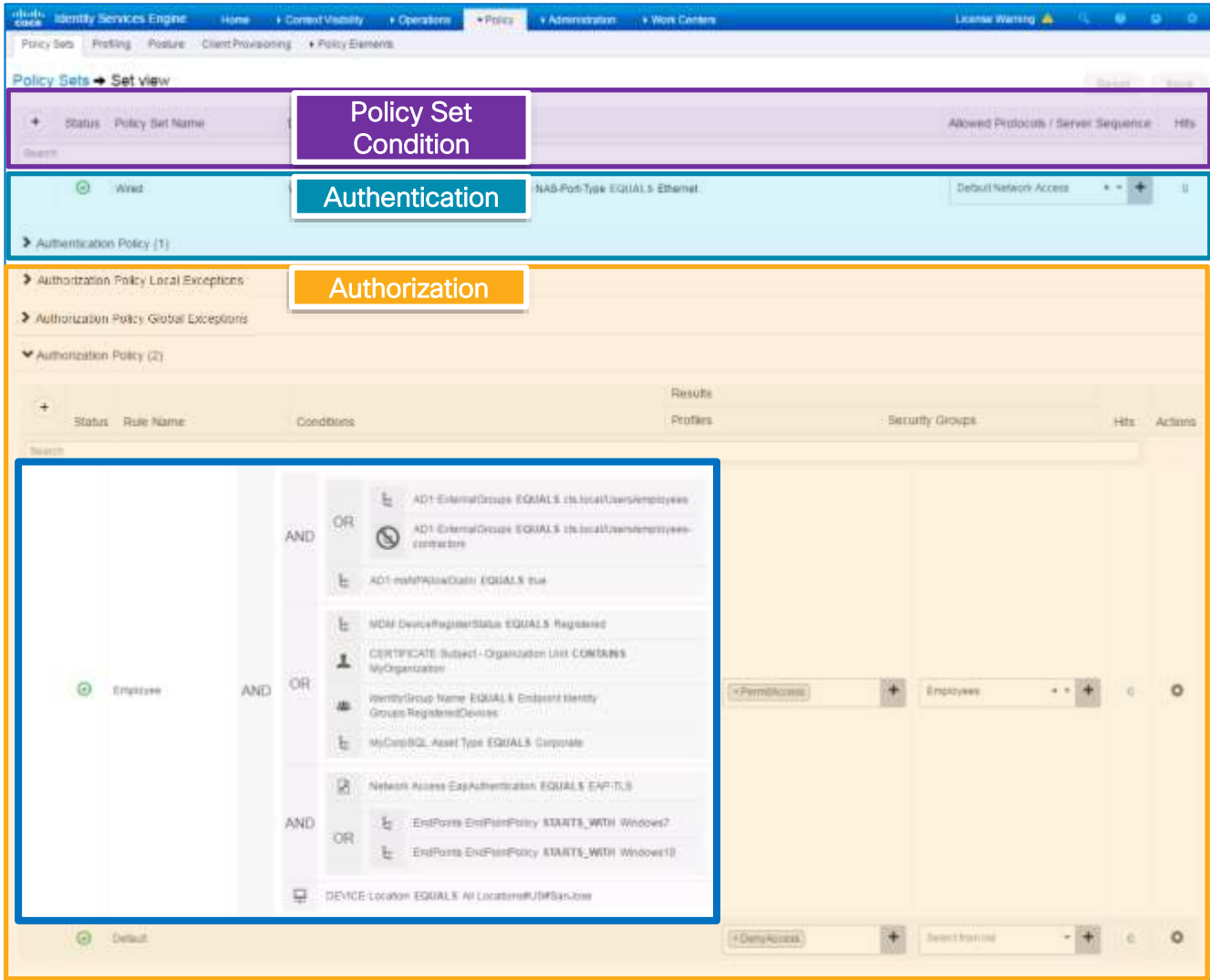
Example #2: Employee_CWA
1. Location (Network Device Group)
2. Web Authenticated?
3. Authenticated via LDAP Store?
4. LDAP Attribute Comparison

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

Auth Policy

ISE 2.3 Example

For Your Reference



cisco Live!

Auth Policy

ISE 2.3 Example

For Your Reference

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

Policy Set Condition

AND
OR
AD1-ExternalGroups EQUALS cts.local/Users/employees
AD1-ExternalGroups EQUALS cts.local/Users/employees-contractors
AD1-msNPAllowDialin EQUALS true

AND
OR
MDM-DeviceRegisterStatus EQUALS Registered
CERTIFICATE-Subject - Organization Unit CONTAINS MyOrganization
IdentityGroup-Name EQUALS Endpoint Identity Groups:RegisteredDevices
MyCorpSQL-Asset Type EQUALS Corporate

Network Access-EapAuthentication EQUALS EAP-TLS

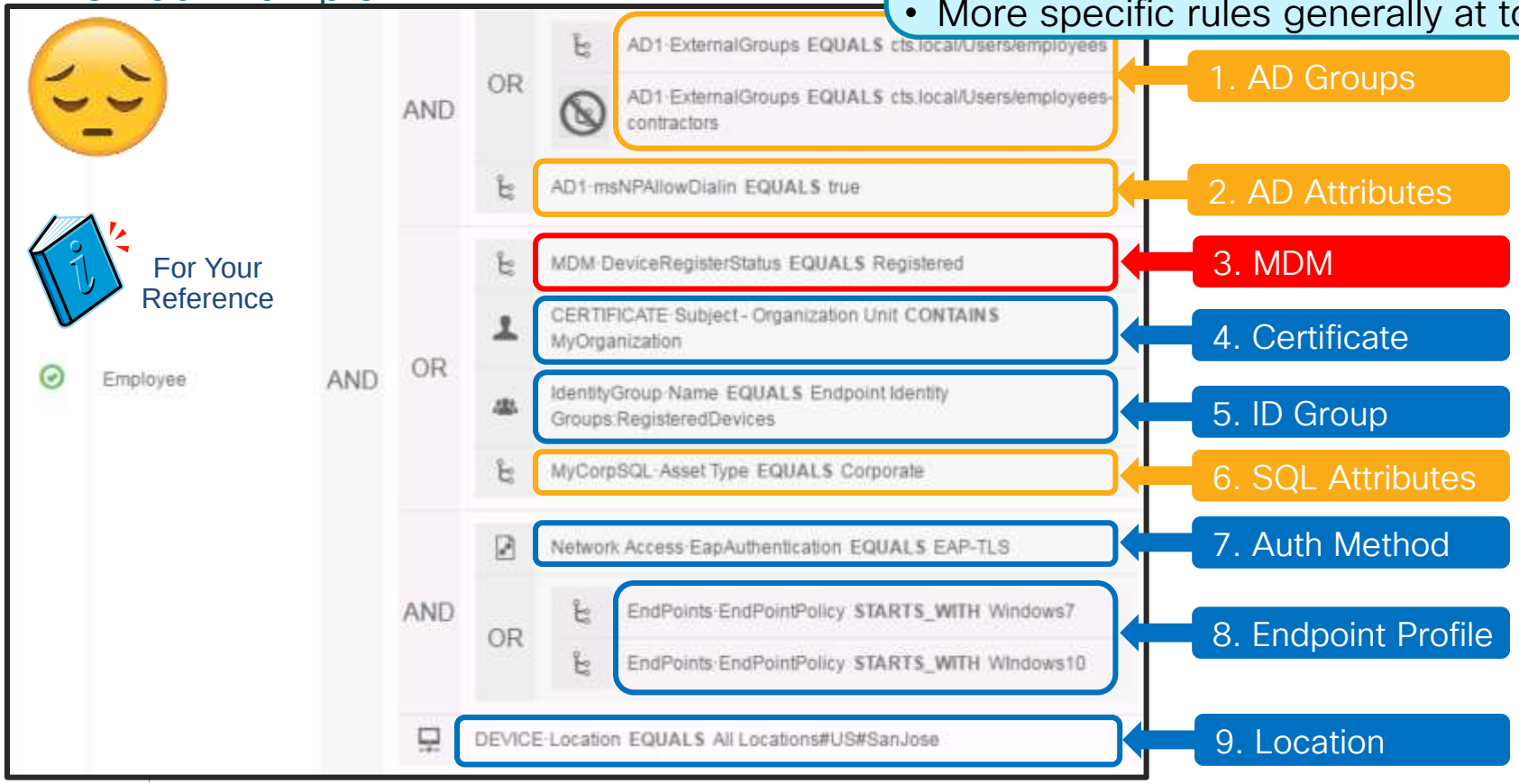
AND
OR
EndPoints-EndPointPolicy STARTS_WITH Windows7
EndPoints-EndPointPolicy STARTS_WITH Windows10

DEVICE-Location EQUALS All Locations#US#SanJose

Auth Policy Optimization

ISE 2.3 Bad Example

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization

ISE 2.3 + Better Example!

For Your Reference

Block 1

DEVICE:Location EQUALS All Locations#US#SanJose

1. Location

Block 2

AND

Network Access:EapAuthentication EQUALS EAP-TLS

2. Auth Method

OR

EndPoints:EndPointPolicy STARTS_WITH Windows7

EndPoints:EndPointPolicy STARTS_WITH Windows10

3. Endpoint Profile

Block 3

AND

AND

OR

AD1:ExternalGroups EQUALS cts.local/Users/employees

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

4. AD Groups

AD1:msNPAllowDialin EQUALS true

5. AD Attributes

Block 4

OR

IdentityGroup:Name EQUALS Endpoint Identity Groups:RegisteredDevices

6. ID Group

CERTIFICATE:Subject - Organization Unit CONTAINS MyOrganization

7. Certificate

MyCorpSQL:Asset Type EQUALS Corporate

8. SQL Attributes

MDM:DeviceRegisterStatus EQUALS Registered

9. MDM

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

ISE 2.4+ Auth Policy Scale

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Custom User Attributes

New Attribute Types in ISE 2.2 include IP / Boolean / Date

For Your Reference

Administration > Identity Management > Settings

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

- User Custom Attributes
- User Authentication Settings
- Endpoint Purge
- Endpoint Custom Attributes

User Custom Attributes

Predefined User Attributes (for reference)

Total 9 | Show All

Mandatory	Attribute Name	Data Type
	AllowPasswordChangeAfterLogin	String
	Description	String
	EmailAddress	String
	EnableFlag	String
	EnablePassword	String
	Firstname	String

User Custom Attributes

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
Client_IP	Static IP address assignment	IP	192.168.200.0		☑

Save | Reset

String
Int
Enum
Float
Password
Long
IP
Boolean
Date

Dynamic Variable Substitution

For Your Reference

Rule Reduction

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

- Authorization Policy Conditions

Authorization Policy

Standard

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

ID Store

Attribute

- Authorization Profile Conditions

Advanced Attributes Settings

Radius:Class = InternalEndpoint groupPolicy

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic Variable Substitution – Example

For Your Reference

Define Custom User Attributes

User Custom Attributes

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
User_IP	Static IP address assignment	IP	192.168.200.0		☐
User_VLAN	Per-User VLAN assignment	Int	Min value : 100, Max value : 200	100	☑
User_Start_Date	Hire Date	Date		2017-01-01	☐
Is_User_Temp_Employee	Temporary Employee Tracker	Boolean		FALSE	☐
User_dACL	Per-User ACL assignment	String	String Max length	20	☑

Save Reset

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic Variable Substitution – Example

For Your Reference

Populate Internal / External User

External User:
AD / LDAP / SQL / OTP

Internal User:
Update via Import or ERS API

Network Access Users List > New Network Access User

Network Access User

* Name: jsmith
Status: Enabled
Email: jsmith@company.com

Passwords

Password Type: Internal Users

Account Disable Policy

Disable account if date exceeds: 2017-06-28 (yyyy-mm-dd)

User Custom Attributes

User_IP	=	192.168.200.185	(IPv4 or IPv6 Address)
* User_VLAN	=	100	
User_Start_Date	=	2017-01-01	(yyyy-MM-dd)
Is_User_Temp_Employee	=	FALSE	
* User_dACL	=	Employee-ACL	

User Groups

Employee

employee1 Properties

Dial-in | Environment | Sessions | Remote control
Remote Desktop Services Profile | Personal Virtual Desktop | COM+
General | Address | Account | Profile | Telephones | Organization | Member Of

Street:
P.O. Box:
City: Cleveland
State/province:
Zip/Postal Code: Employee-ACL
Country/region:

OK | Cancel | Apply | Help

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic DACLs in Authorization Profile

For Your Reference

Per-User Policy in 1 rule

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

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: Employee_Access

Description: Policy for Employee Access

* Access Type: ACCESS_ACCEPT

Network Device Profile: CiscoWired

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name: InternalUser:User_dACL

DACL Name: LDAP1:postalCode

InternalUser

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

Internal User example

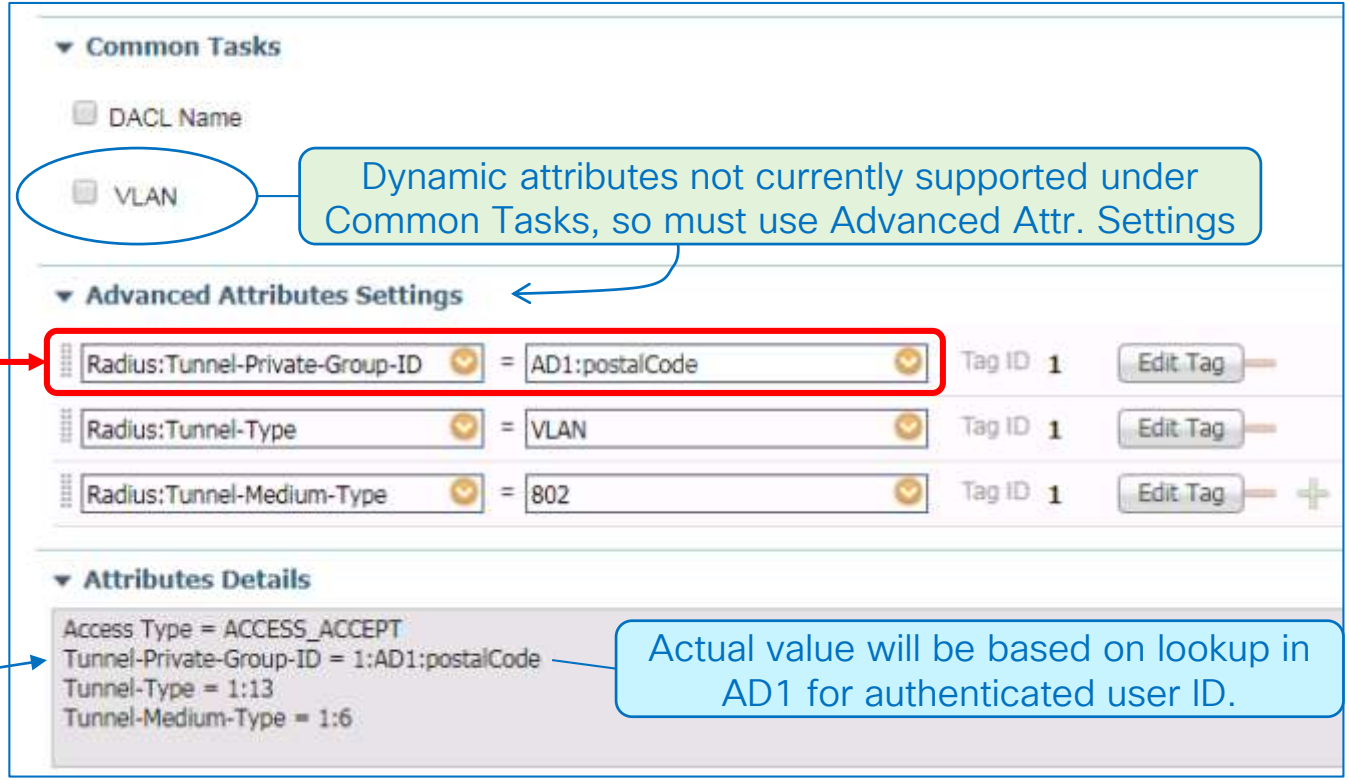
External User example

Dynamic VLANs in Authorization Profile

Per-User/Endpoint Policy in Single Authorization Rule

For Your Reference

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enable EAP-Fast Session Resume

For Your Reference

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

Identity Services Engine | Home | Operations | Policy | Guest Access | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Identity

Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Backup & Restore | Admin Access | Settings

- Client Provisioning
- FIPS Mode
- Alarm Settings
- Posture
- Profiling
- Protocols
  - EAP-FAST
    - EAP FAST Settings
    - Generate PAC
  - EAP-TLS
  - PEAP
  - EAP-TTLS

EAP FAST Settings

* Authority Identity Info Description: Identity Services Engine

* Master Key Generation Period: 1 Weeks

Revoke all master keys and PACs: Revoke

Cache TLS Session

PAC-less Session Resume

☑ Enable PAC-less Session Resume

* PAC-less Session Timeout: 7,200 (in seconds)

Save | Reset

PAC = Protected Authentication Credential
PACs used to establish Phase One TLS tunnel without certs.

Note: Both Server and Client must be configured for Session Resume

Enable EAP Session Resume / Fast Reconnect

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

Identity Services Engine | Home | Operations | Policy | Guest Access | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Identity M

Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Backup & Restore | Admin Access | Settings

- Client Provisioning
- FIPS Mode
- Alarm Settings
- Posture
- Profiling
- Protocols
  - EAP-FAST
    - EAP FAST Settings
    - Generate PAC
  - EAP-TLS
  - PEAP
  - EAP-TTLS
  - RADIUS

EAP TLS Settings

☑ Enable EAP TLS Session Resume

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

Cache TLS (TLS Handshake Only/Skip Cert)

Cache TLS session

Peap Settings

☑ Enable PEAP Session Resume

* PEAP Session Timeout 7,200 (in seconds)

☑ Enable Fast Reconnect

Save | Reset

Skip inner method

Select Authentication Method: Win 7 Supplicant

Secured password (EAP-MSCHAP v2) | Configure...

☑ Enable Fast Reconnect

☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

For Your Reference

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

For Your Reference

Stateless Session Resume for EAP-TLS

- EAP-TLS Session resumption allows the reuse of a recently valid TLS session ticket - improving performance for clients making multiple requests. This improves performance from the clients' perspective, because it eliminates the need for a new (and time-consuming) TLS handshake to be conducted each time a request is made.
- Cisco ISE supports session ticket extension as described in RFC 5077
- When Stateless resume is enabled in ISE it allows EAP-TLS session resumption without requiring the session state to be stored at the server
- Cisco ISE creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ISE to resume a session
- When a user reconnects within the configured EAP-TLS session timeout period, ISE resumes the EAP-TLS session and reauthenticates the user with TLS handshake only, without a certificate check.
- The Stateless session resumption is supported in the distributed deployment, so that a session ticket issued by one node is accepted by another node.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Stateless Session Resume

ISE 2.2+

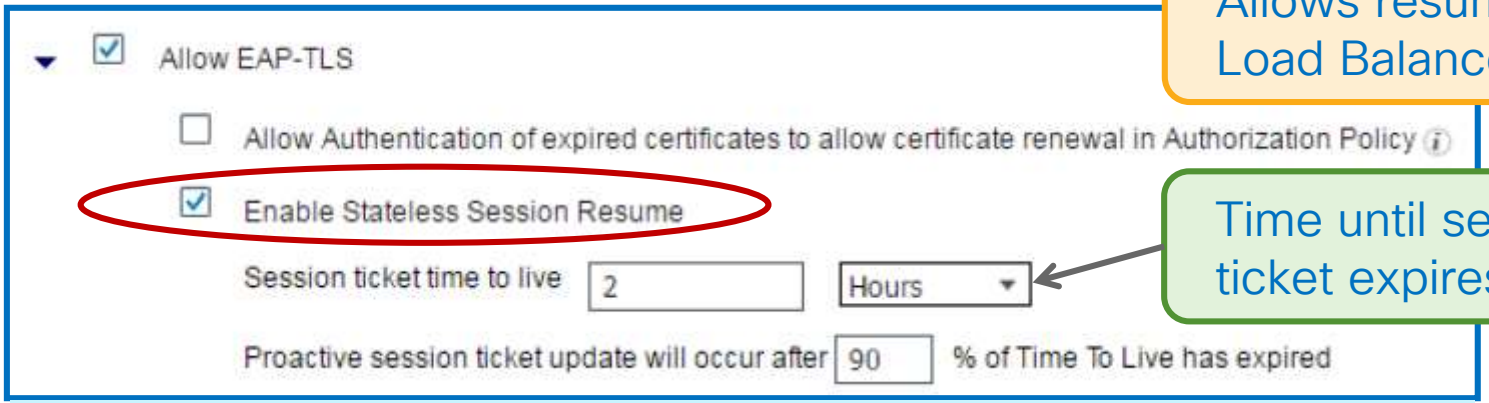
For Your Reference

Allows Session Resume Across All PSNs

- Session ticket extension per RFC 5077

  [Transport Layer Security (TLS) Session Resumption without Server-Side State]

- ISE issues TLS client a session ticket that can be presented to any PSN to shortcut reauth process (Default = Disabled)



Allows resume with Load Balancers

Time until session ticket expires

Policy > Policy Elements > Results > Authentication > Allowed Protocols

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

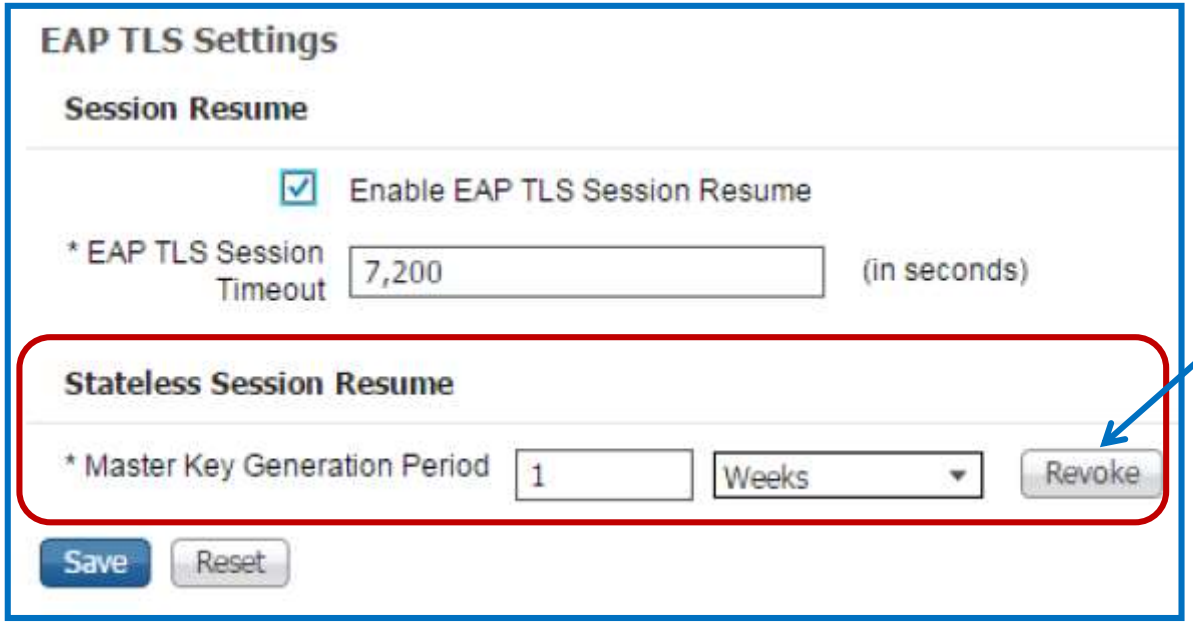
ISE 2.2 Stateless Session Resume

Master Key Generation Period

New in ISE 2.2!

For Your Reference

- Master Key Generation Period = Time until new master key is regenerated.



Cancel all previously generated master keys and tickets

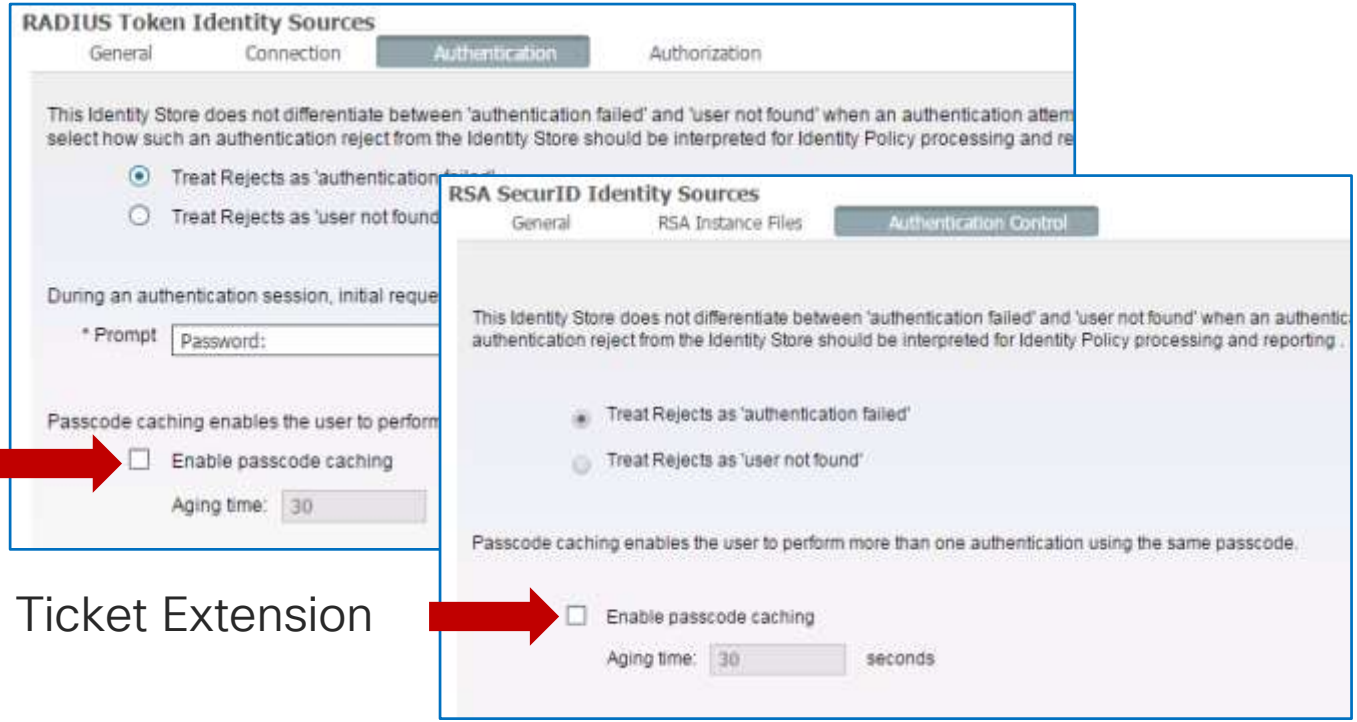
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

OTP Token Caching

Password Caching for RSA SecureID and RADIUS Token Servers

For Your Reference

- Allows re-use of passcode for specified interval.
- Per-PSN cache –not replicated across PSNs.
- Cache entry deleted if pass-word mismatch
- RFC 5077 Session Ticket Extension supported



Administration > Identity Management > External Identity Stores

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine Access Restrictions (MAR)

Couples Machine + User Authentication

For Your Reference

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

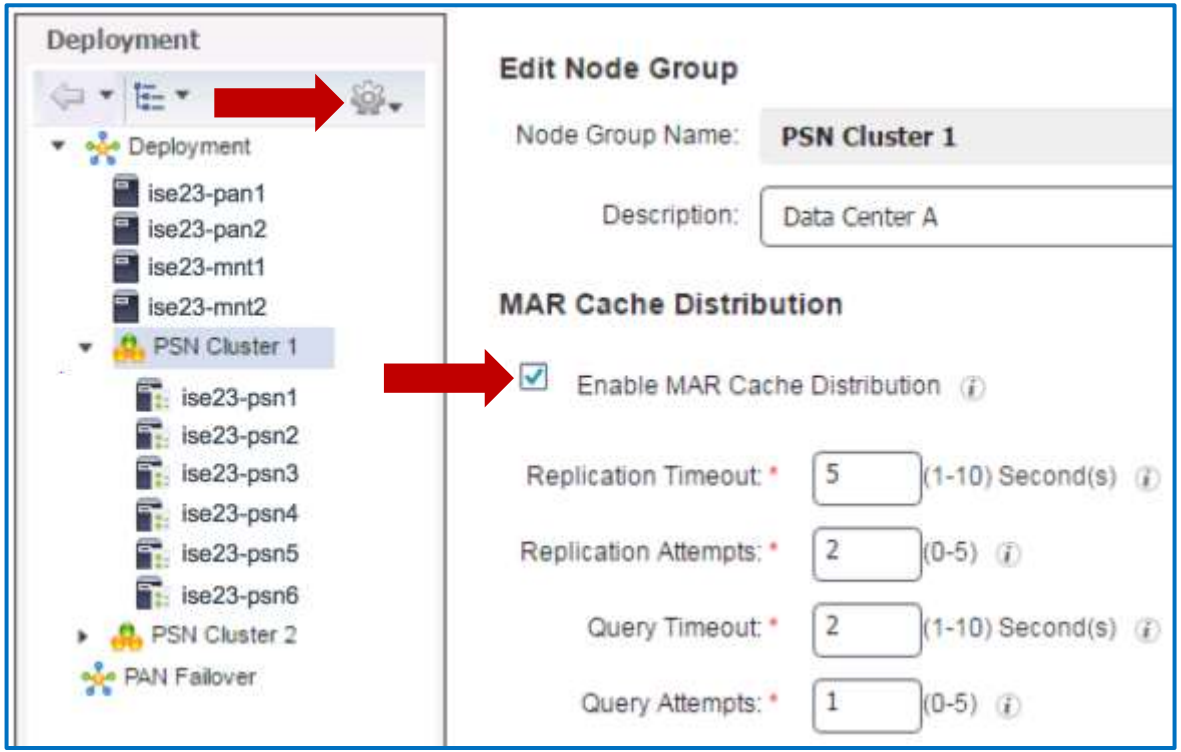
MAR Cache Persistence and Distribution

For Your Reference

Save MAR Cache After PSN Restart / Synchronize Cache Across PSNs

Administration > System > Deployment

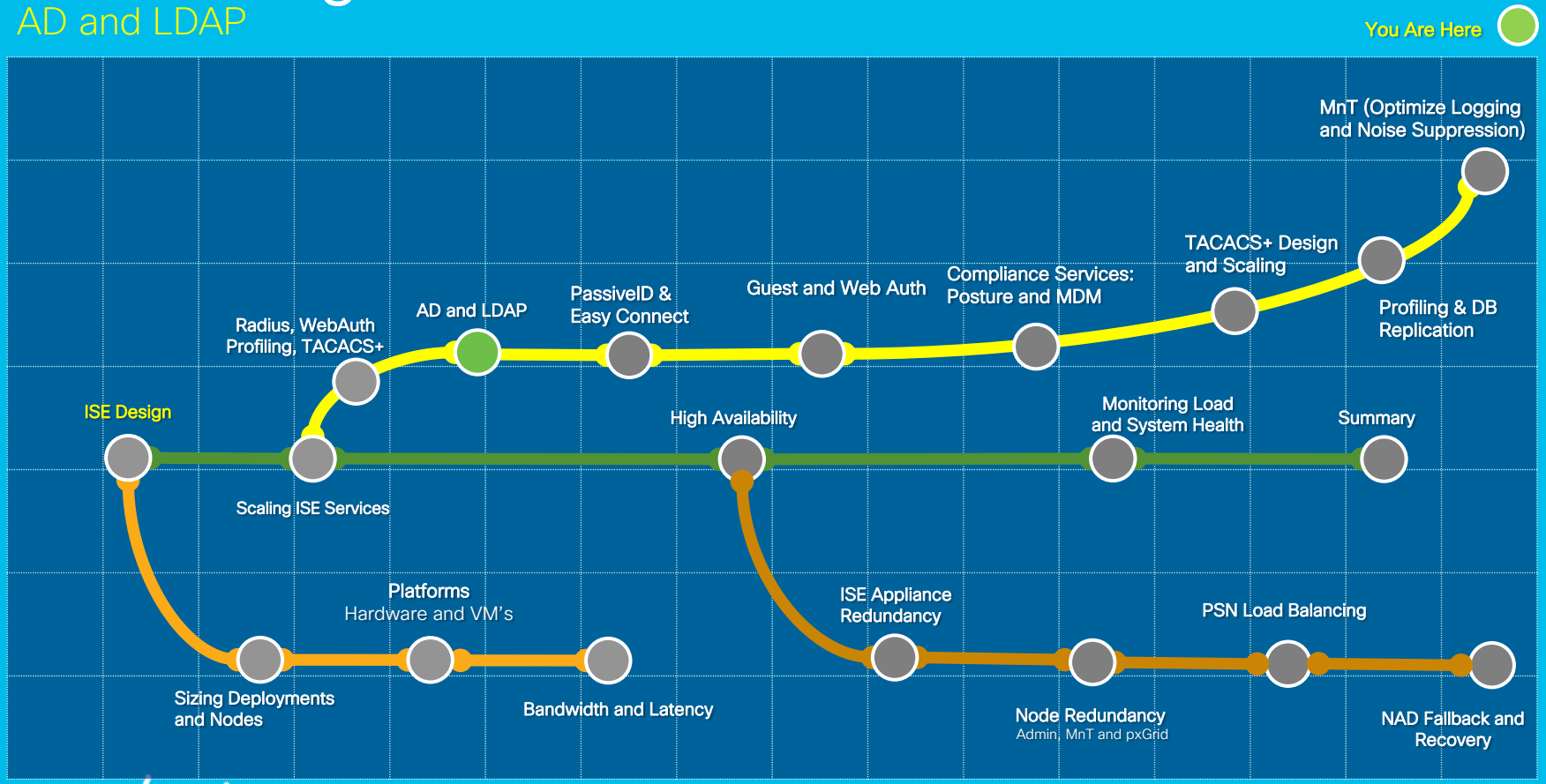
- ISE 2.1 added **MAR Cache Persistence**
  ➠ Store cache & persist after node restart
- ISE 2.3 adds **MAR Cache Distribution**
  ➠ Replicate cache across all PSNs in same node group
- Configurable per-Node Group



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

AD and LDAP



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

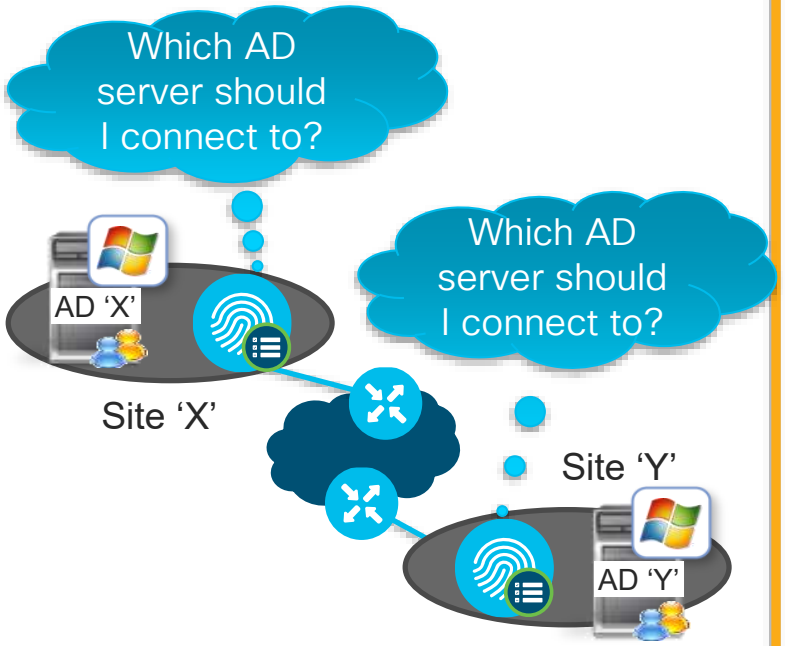
Scaling AD and LDAP Integration

Scaling AD Integration w/ Sites & Services

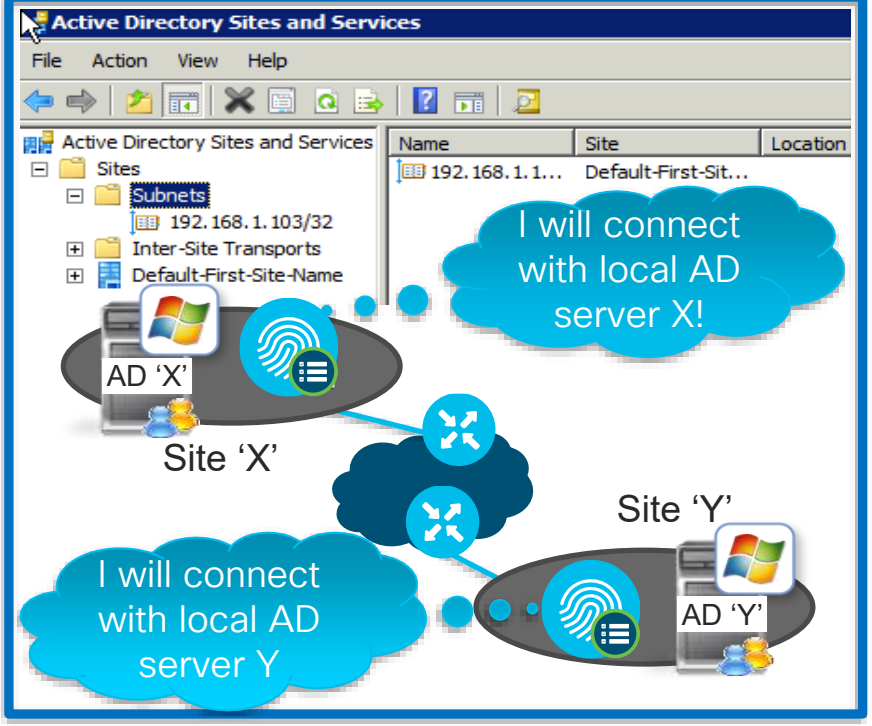
How do I ensure Local PSN is connecting to Local AD controller

Active Directory Sites and Services
Shortcut

Without Site & Services



Properly Configured



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

AD Sites and Services

Active Directory Sites and Services
Shortcut

For Your Reference

Links AD Domain Controllers to ISE Servers Based on IP Address

- 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)

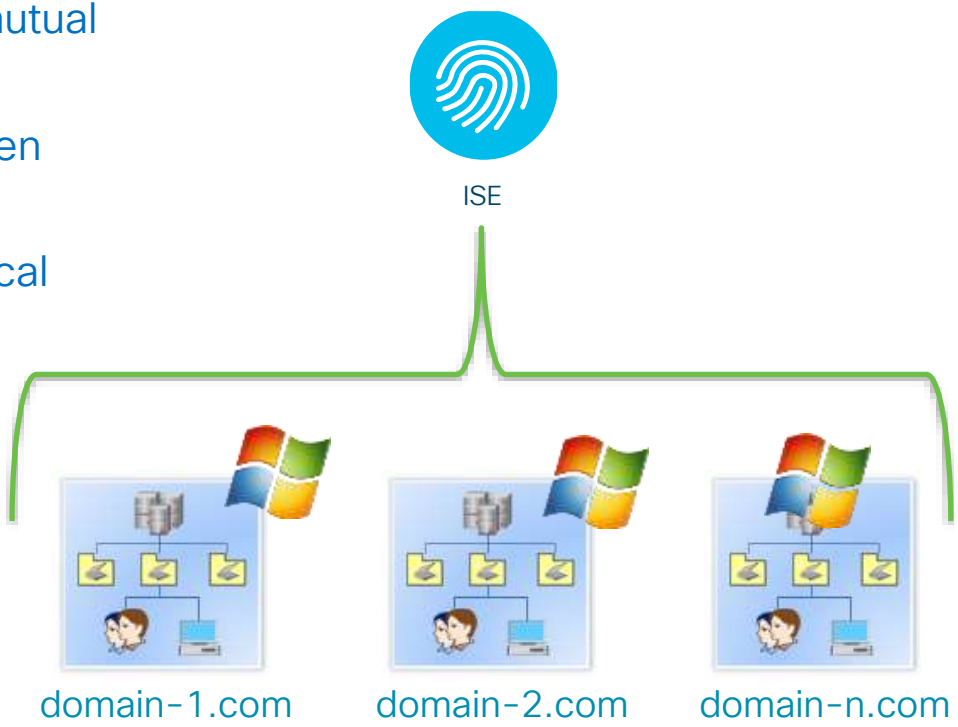
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multi-Forest Active Directory Support

For Your Reference

Scales AD Integration through Multiple Join Points and Optimized 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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

AD Authentication Flow

Active Directory Scopes > Default_Scop

Connection | Authenti

Use Domain Nar

S

Au

Poli

A

Certifica

Active D

Defau

AN

SC

scope

scope

AN

Allow Authe

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 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]

For Your Reference

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

AD Authentication Flow

For Your Reference

Active Directory Scopes > Default_Scope,scope2 > AMER.ACS.COM

Connection | Authentication Domains | Groups | Attributes

Scope **Default_Scope,scope2**

* Domain Name AMER.ACS.COM

Use Domain Name as Identity Store Name (First 32 characters)

Specify Identity Store Name

* Identity Store Name AMER.ACS.COM

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]

AuthC Policy to AD → Scope (Optional) → AD Instance → Identity Rewrite (Optional) → Target AD

Domain List (Optional)

External Identity Sources

- Certificate Authentication Profile
- Active Directory
  - Default_Scope
    - AMER.ACS.COM
    - SOUTH.AMER.ACS.COM
  - scope1
  - scope2
    - AMER.ACS.COM

Allow Authentication to: All Domains with sufficient Trust to the Joined Domain

Only the Domains listed in the table below

The Table below will be used to control the domains for authentication

Enable Selected | Disable Selected

Name	Forest	Type	Authenticate
AUSTRALIA.OCEANIA.ACS.COM	OCEANIA.ACS.COM	domain	NO
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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Authentication Domains (Whitelisting)

For Your Reference

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

Enable r1.dom

And disable the rest

Connection | Authentication Domains | Groups

☐ Use all Active Directory domains for authentication

Enable Selected | Disable Selected | Show Unusable Domains

Name	Authenticate	Forest	SID
c1.r1.dom	NO	R1.dom	S-1-5-21-744
c2.c1.r1.dom	NO	R1.dom	S-1-5-21-419
c3.r2.dom	NO	R2.dom	S-1-5-21-347
c4.r3.dom	NO	R3.dom	S-1-5-21-743
c5.c4.r3.dom	NO	R3.dom	S-1-5-21-679
c6.c5.c4.r3.dom	NO	R3.dom	S-1-5-21-170
☑ r1.dom	YES	R1.dom	S-1-5-21-132
r2.dom	NO	R2.dom	S-1-5-21-971
r3.dom	NO	R3.dom	S-1-5-21-114

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Authentication Domains – Unusable Domains

For Your Reference

- Domains that are unusable, e.g. 1-way trusts, are hidden automatically
- There's an option to reveal these and see the reason

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Run the AD Diagnostic Tool

For Your Reference

Check AD Joins at Install & Periodically to Verify Potential AD Connectivity Issues

Run Tests | View Test Details | Stop All Running Tests | Reset All tests to "Not Run"

Test Name	Join Point	Status	Result and Remedy
DNS A record high level API query	cisco.com	Successful	Address record found
DNS A record low level API query	cisco.com	Successful	Address record found
DNS SRV record query	cisco.com	Failed	Response contains no answer. Check DNS configuration.
DNS SRV record size	cisco.com	Failed	Response contains no answer. Check DNS configuration.
Kerberos check SASL connectivity to AD	cisco.com	Successful	SASL connectivity test to AD was successful
Kerberos test bind and query to ROOT DSE ...	cisco.com	Successful	ROOT_DSE was successfully reached
Kerberos test obtaining join point TGT	cisco.com	Successful	TGT was obtained successfully
LDAP test - DC locator	cisco.com	Successful	DCs availability test was successful List of RPC/LDAP a...

- The DNS SRV errors can actually mean something else
  - The response was too big...and retried with TCP, etc.
  - A sniffer can confirm
  - AD Sites or DNS configuration changes are required to get that optimized

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

AD Background Diagnostics

Schedule Periodic Testing to Verify AD Connectivity and Health

New in ISE 2.4!

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

For Your Reference

Active Directory > **Active Directory Diagnostic Tool**

Active Directory Diagnostic Tool

These tests check proper Active Directory configuration and operation of the Active Directory Service for use with ISE.

ISE node: Positron-vm-2.demo.local

Join Point: All Instances

Run Tests Now

Summary: **Successful**

Finish running tests (7:54:05 AM).

Run scheduled tests

Start At 00:00 Hrs.

Repeat every 1 Days

Save Reset

Run Tests | View Test Details | Stop All Running Tests | Reset All tests to "Not Run"

Test Name	Join Point	Status	Result and Remedy
System health - check AD service	System	Successful	AD service is running
System health - check DNS configuration	System	Successful	DNS configuration & status test was successful
System health - check NTP	System	Successful	NTP configuration & status test was successful

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Validating DNS from ISE node CLI

- Checking SRV records for Global Controllers (GC)

```
psn/admin# nslookup _ldap._tcp.gc._msdcs.myADdomainName querytype SRV
```

- Checking SRV records for Domain Controllers (DC)

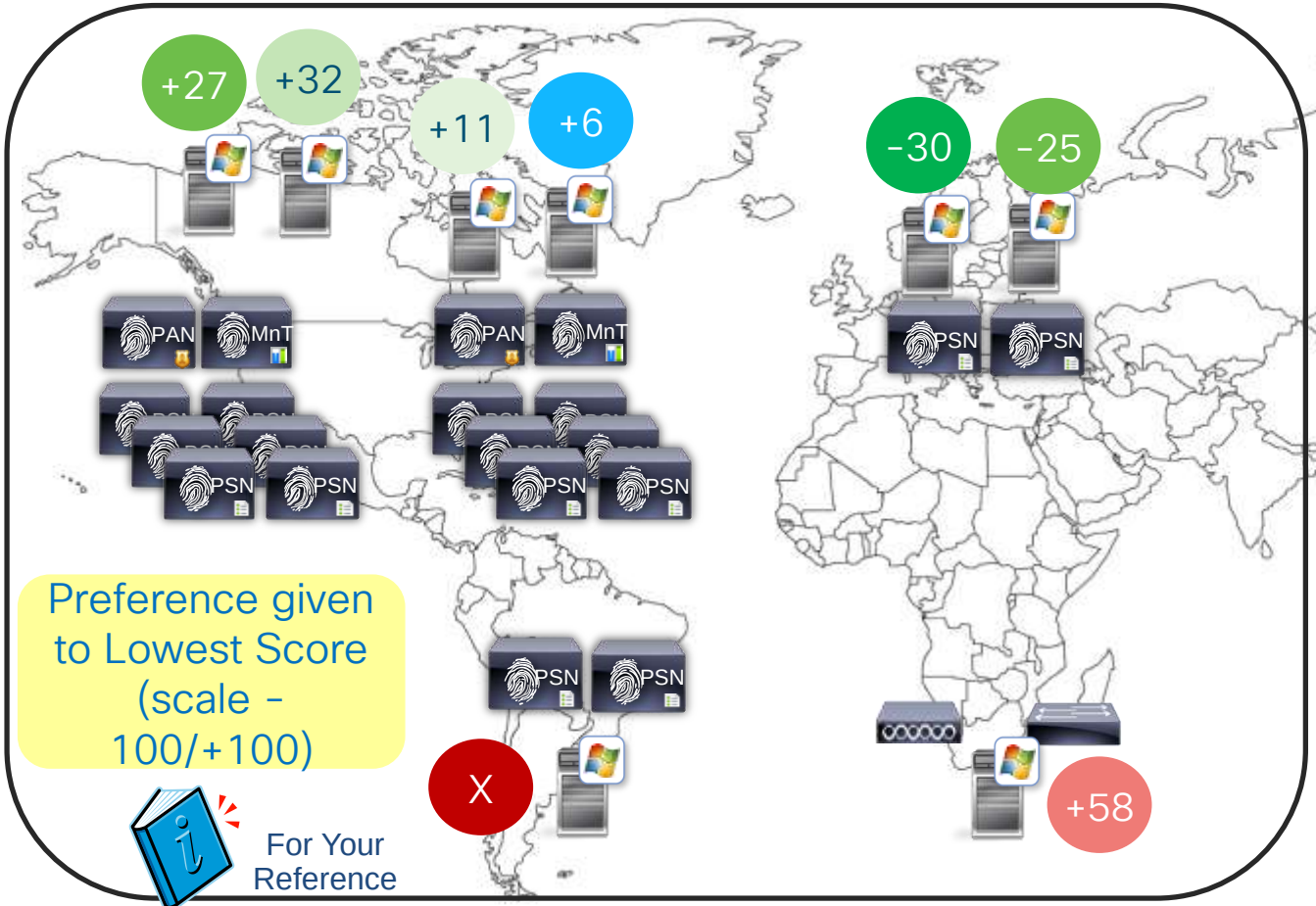
```
psn/admin# nslookup _ldap._tcp.dc._msdcs.myADdomainName querytype SRV
```

- More details on Microsoft AD DNS queries: https://technet.microsoft.com/en-us/library/cc959323.aspx

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enhanced AD Domain Controller Management and Failover

Preferred DC Based on Scoring System



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

For Your Reference

ISE 2.4 DC Selection and Failover

DC Scoring System Determines Priority List

For Your Reference

- Scoring Rules
  - DC with lowest score preferred
  - Score range: -100 / +100
  - System error: score +25
  - Timeout: score +10
  - Slow CLDAP ping: score +1
  - Successful CLDAP ping: score -1

Scores and Scoring Events only viewable in debug logs

- DC failover:
  - Collect DCs that respond CLDAP ping during the limited time period after the first DC answered: first DC answer time + 200ms. All responded DCs will be stored and assigned an initial score or updated an existing score.
  - If the DC site is different than the client site, run the per-site DNS query and repeat the DC discovery process as above.
  - Select a DC with minimal score from the list of responded DCs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Microsoft LDAP Changes - CSCvs67071

LDAP channel binding

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

LDAP Signing

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

My Lab testing:

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

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

Per-PSN LDAP Servers

For Your Reference

Added in ISE 2.2!

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

LDAP Identity Sources List > **LDAP1**

LDAP Identity Source

General | Connection | Directory Organization | Groups | Attributes | Advanced Settings

Primary Server

Hostname/IP: ad.cts.local

Port: 389

Secondary Server

☑ Enable Secondary Server

Hostname/IP: ad2.cts.local

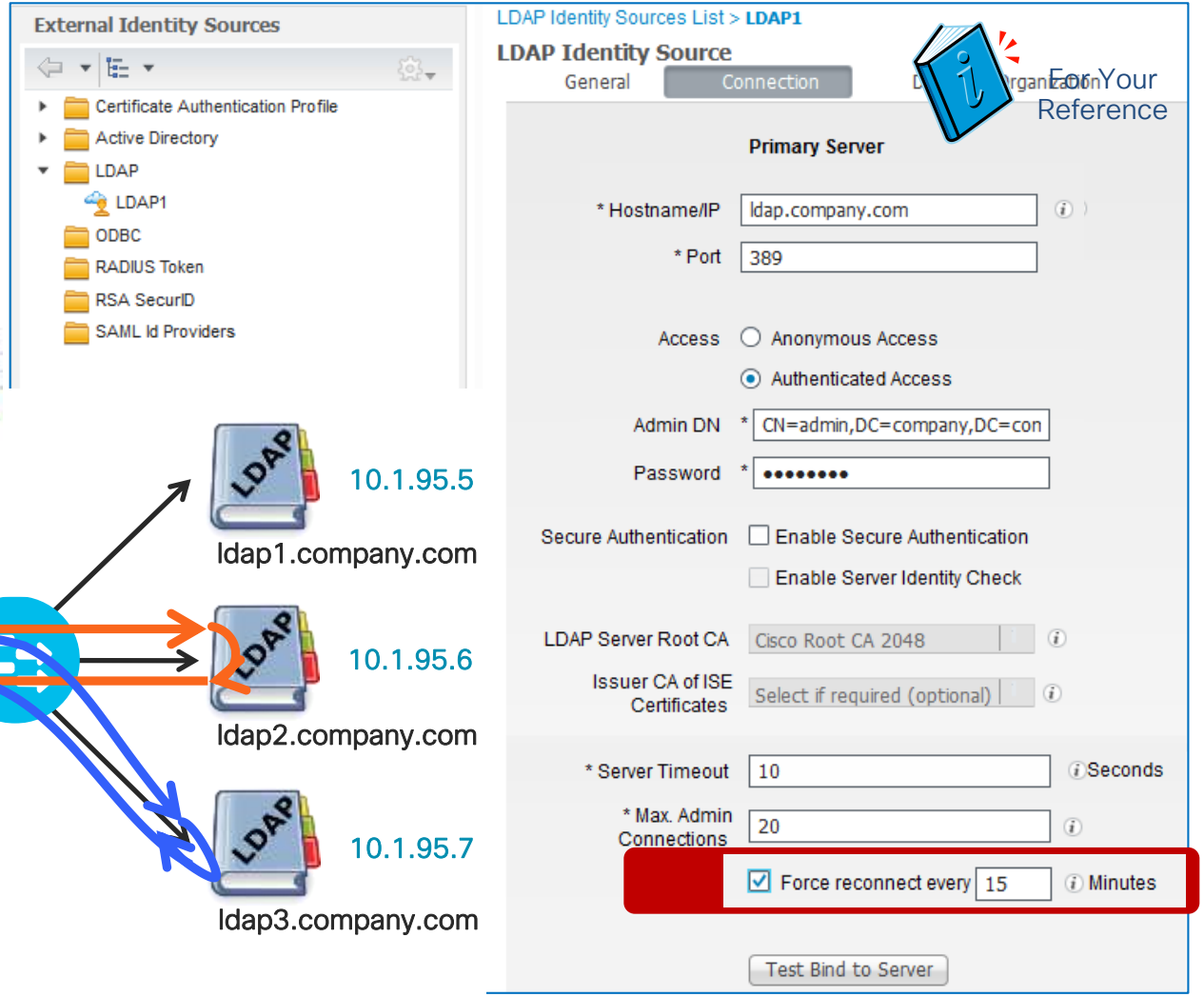
Port: 389

☑ Specify server for each ISE node

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing LDAP Servers



Lookup2 = ldap.company.com

Response = 10.1.95.7

15 minute reconnect timer

LDAP Query to 10.1.95.7

LDAP Response from 10.1.95.7

PSN

10.1.95.5
ldap1.company.com

10.1.95.6
ldap2.company.com

10.1.95.7
ldap3.company.com

AD Integration Best Practices

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

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

For Your Reference

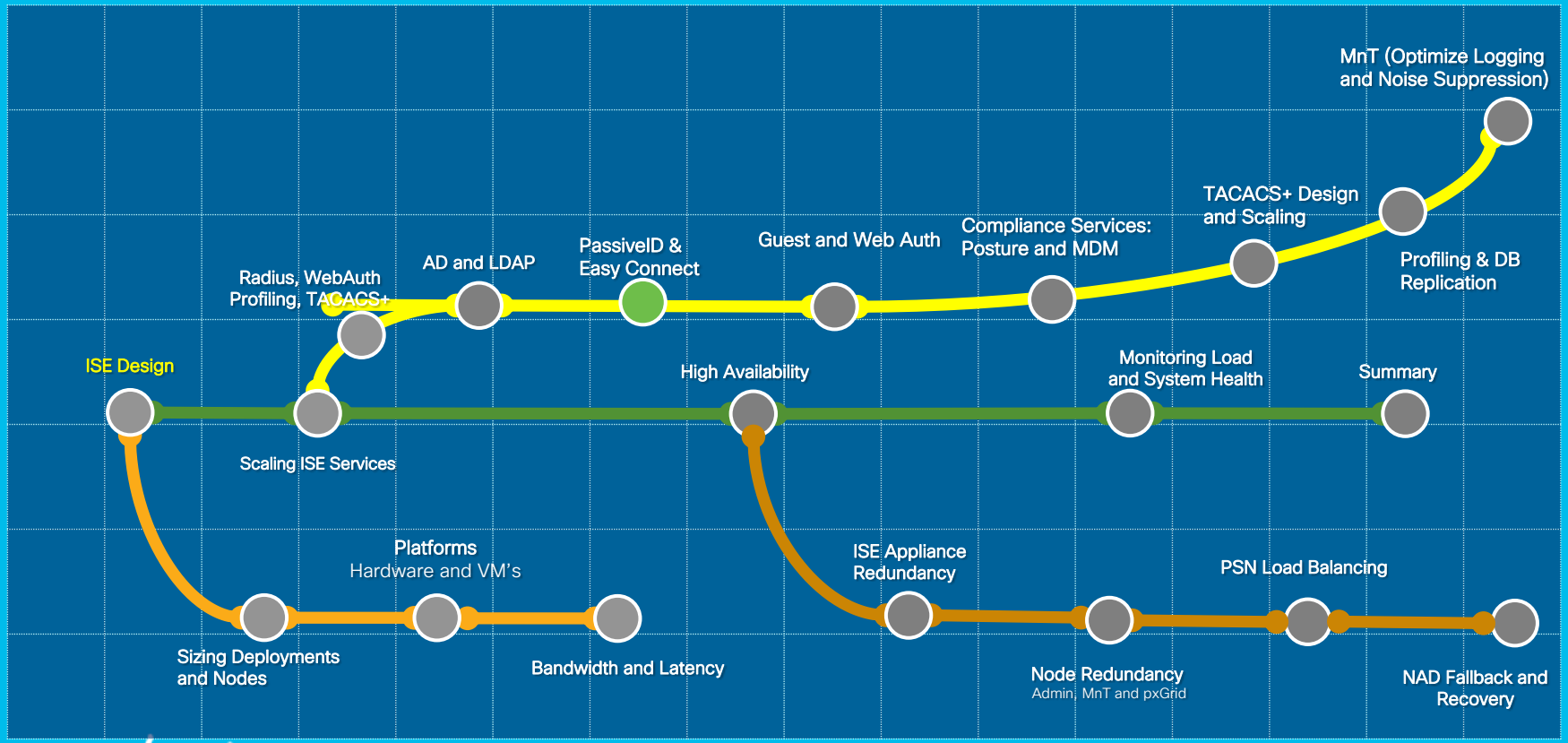
* Microsoft AD Indexed Attributes:
http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx
http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Passive Identity and Easy Connect

Session Agenda

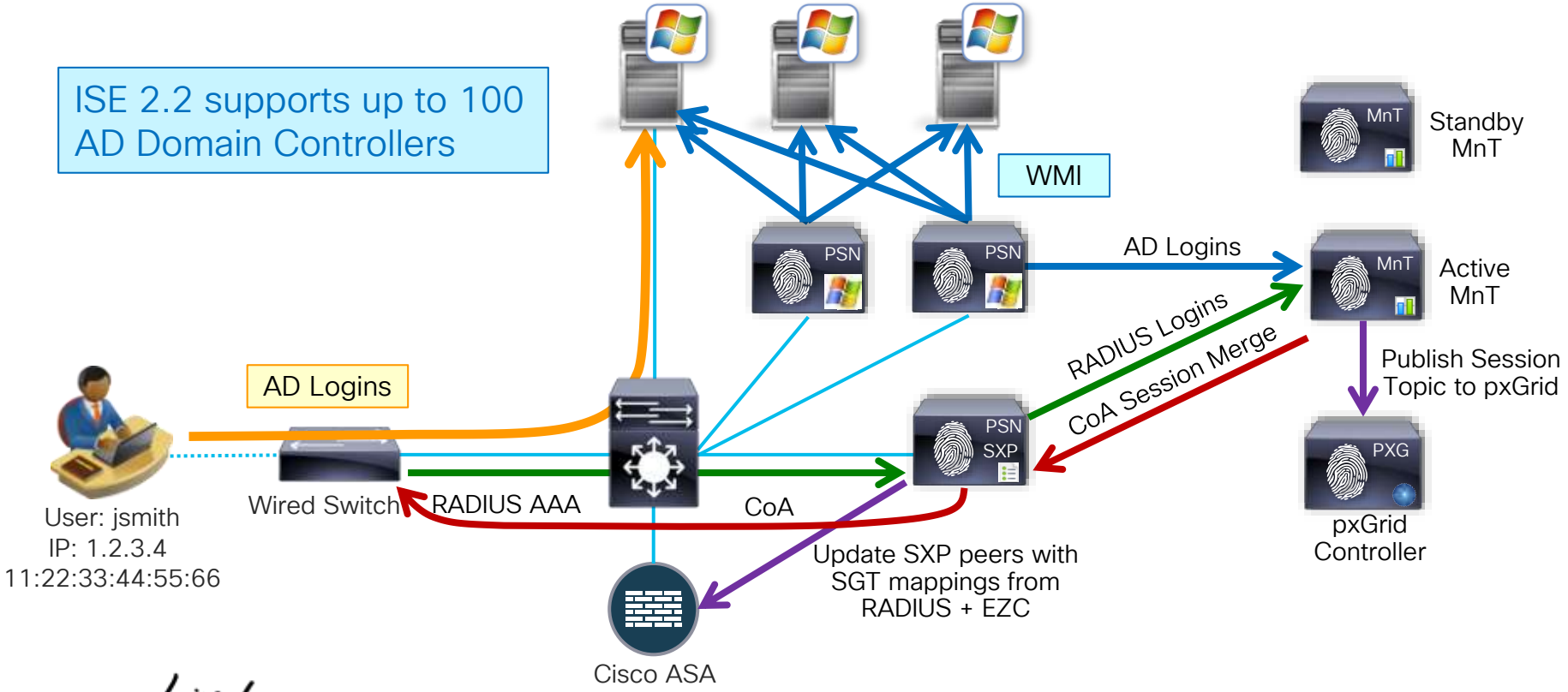
AD and LDAP



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Passive Identity / Easy Connect Architecture

For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Easy Connect

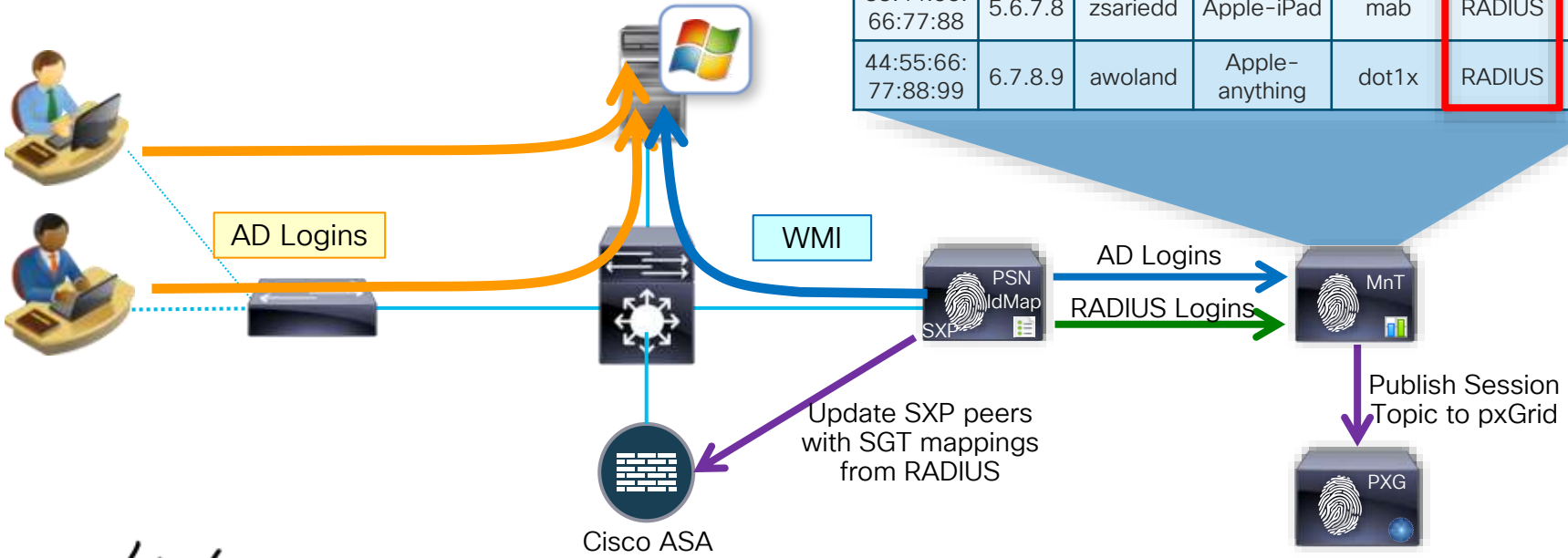
For Your Reference

Consuming Both AD and RADIUS Logins

1.2.3.4	chyps
2.3.4.5	imbashir

Windows Event log	
IP Address	Username

ISE Session Directory						
MAC	IP	Uname	Profile	Method	Source	SGT
	1.2.3.4	chyps			Identity Mapping	
	2.3.4.5	imbashir			Identity Mapping	
22:33:44:55:66:77	3.4.5.6	hslai	Samsung Galaxy	dot1x	RADIUS	10
33:44:55:66:77:88	5.6.7.8	zsariedd	Apple-iPad	mab	RADIUS	20
44:55:66:77:88:99	6.7.8.9	awoland	Apple-anything	dot1x	RADIUS	10



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

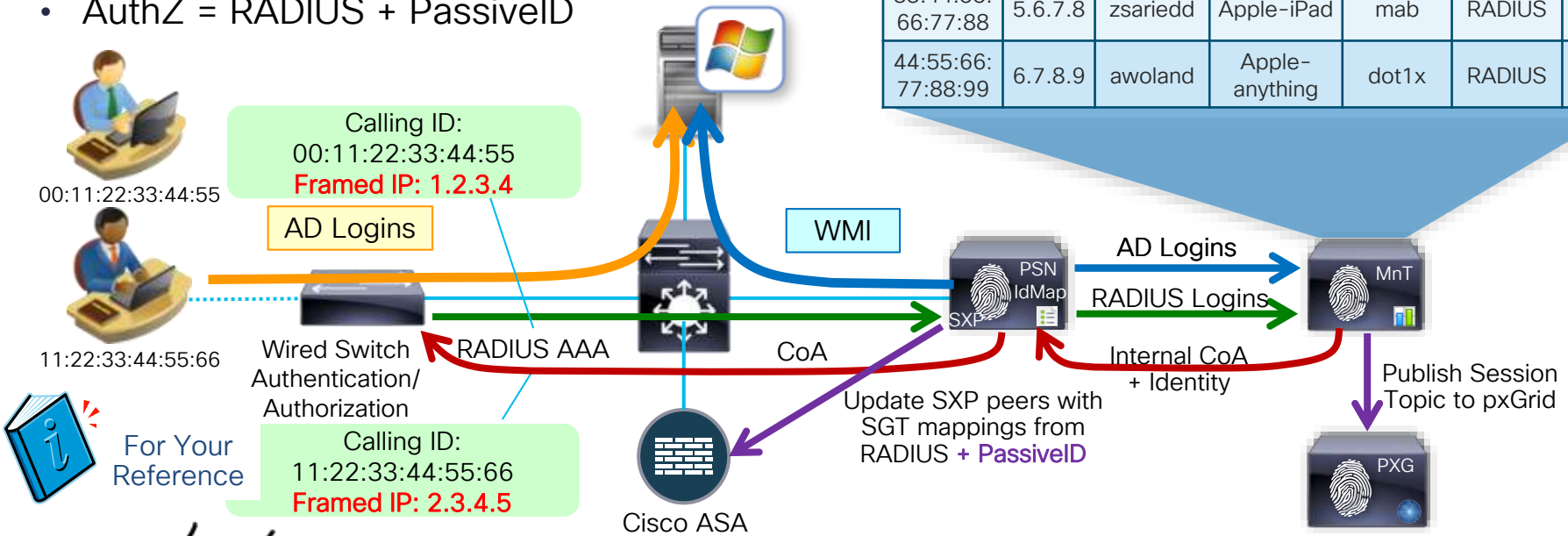
Easy Connect Enforcement

Merging RADIUS and AD Login Identity

- Merge *active* RADIUS Identity with *passive* AD Identity
- AuthZ = RADIUS + PassiveID

Windows Event log	
IP Address	Username
1.2.3.4	chyps
2.3.4.5	imbashir

ISE Session Directory						
MAC	IP	Uname	Profile	Method	Source	SGT
00:11:22:33:44:55	1.2.3.4	chyps	Windows7-WS	Dot1x +PsvID	IdMap+RADIUS	10
11:22:33:44:55:66	2.3.4.5	imbashir	Windows 10	MAB +PsvID	IdMap+RADIUS	30
22:33:44:55:66:77	3.4.5.6	hslai	Samsung Galaxy	dot1x	RADIUS	10
33:44:55:66:77:88	5.6.7.8	zsariedd	Apple-iPad	mab	RADIUS	20
44:55:66:77:88:99	6.7.8.9	awoland	Apple-anything	dot1x	RADIUS	10



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

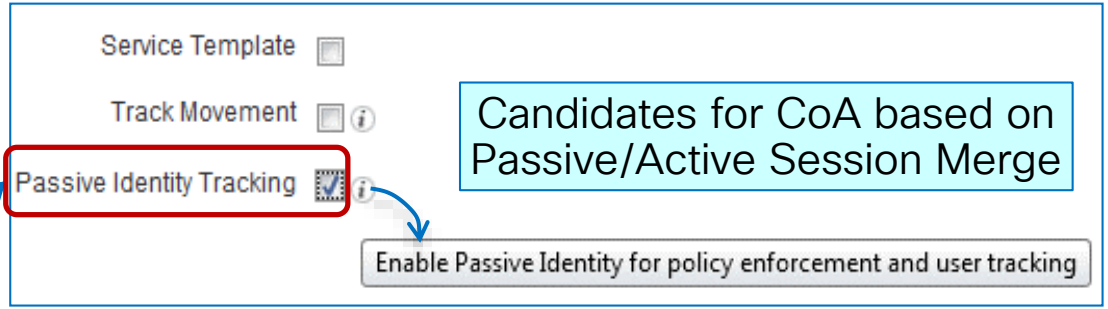
PassiveID/EZC

Scaling Summary

- Limit Passive Identity Service to 2 PSN nodes (dedicated) for WMI
- Limit tracking to ISE sessions where require update to authorization based on PassiveID
- Filter out login events not used for PassiveID
- Limit DCs to those where AD logins used for PassiveID
- Use AD event log forwarding to acquire logs for other DCs

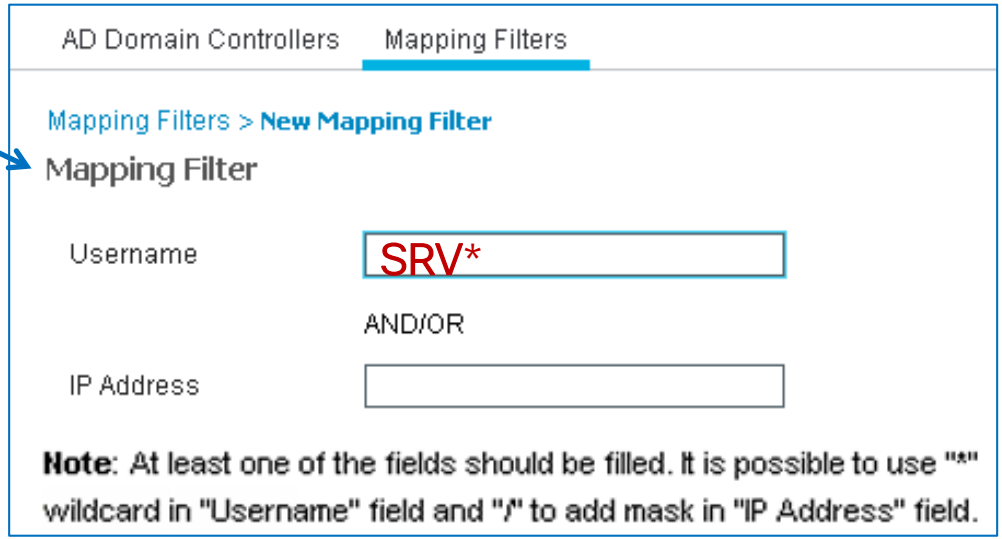
Google “windows event forwarding”

Policy > Policy Elements > Authorization > Authorization Profiles

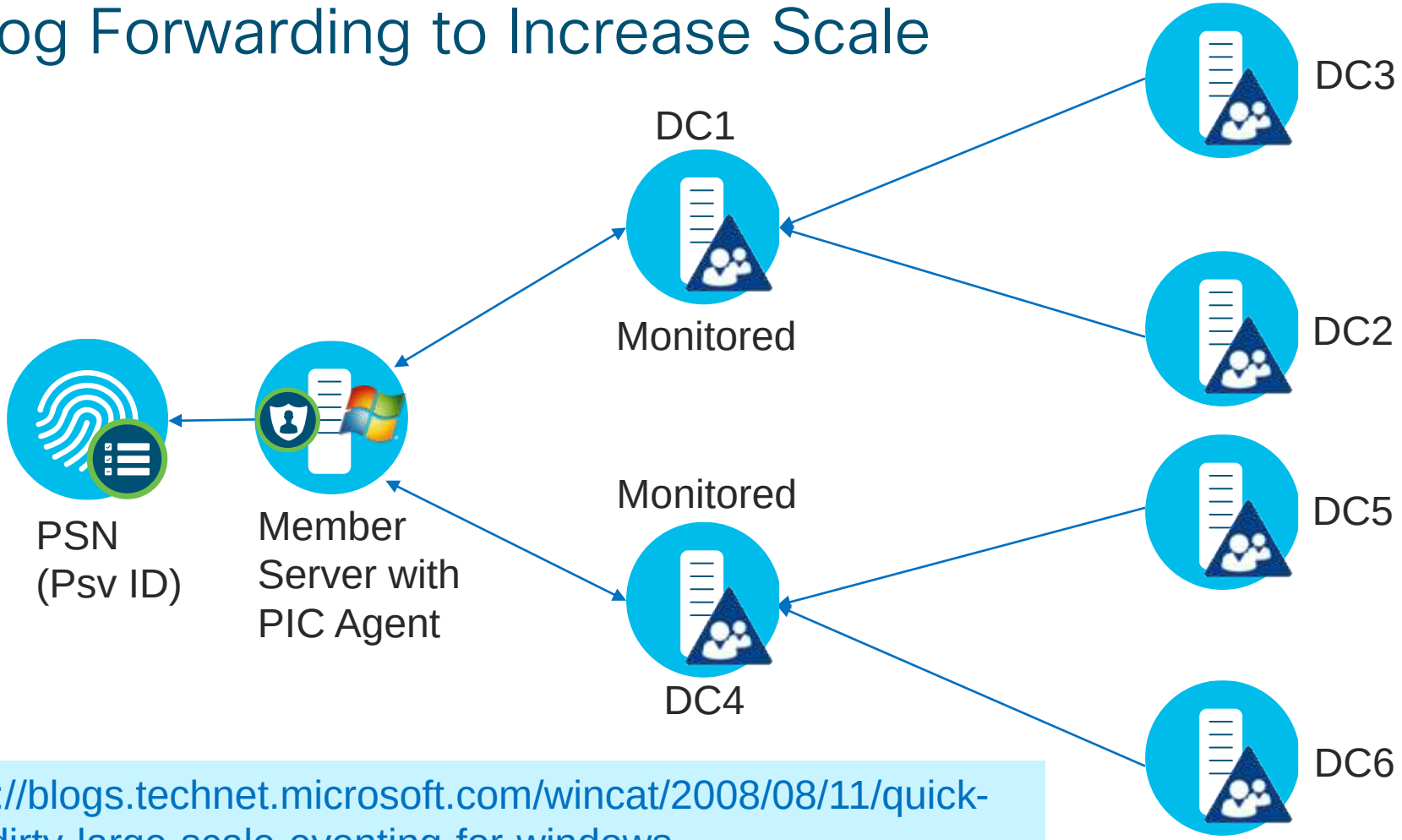


Candidates for CoA based on Passive/Active Session Merge

Administration > PassiveID > Mapping Filters



Log Forwarding to Increase Scale



https://blogs.technet.microsoft.com/wincat/2008/08/11/quick-and-dirty-large-scale-eventing-for-windows

ISE 2.2 Passive ID and Easy Connect Multi-Service S

For Your Reference

Max Concurrent Passive ID/Easy Connect Sessions by Deployment and Platform

Scaling per Deployment Model	Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max Passive ID Sessions	Max Merged/EZC Sessions (subset of RADIUS/Psv ID)
Standalone: All personas on same node (2 nodes redundant)	3415	0	5,000	50,000	500
	3495	0	7,500	100,000	1,000
	3515	0	10,000	100,000	1,000
	3595	0	20,000	300,000	2,000
Hybrid: PAN+MnT on same node and Dedicated PSNs (Minimum 4 nodes redundant)	3415 as PAN+MNT	5 / 3 + 2	5,000	50,000	500 / 2,500
	3495 as PAN+MNT	5 / 3 + 2	10,000	100,000	1,000 / 5,000
	3515 as PAN+MNT	5 / 3 + 2	7,500	100,000	1,000 / 5,000
	3595 as PAN+MNT	5 / 3 + 2	20,000	300,000	2,000 / 10,000
Dedicated PAN and MnT nodes (Minimum 6 nodes redundant)	3495 as PAN and MNT	38 + 2	250,000	100,000	25,000
	3595 as PAN and MNT	48 + 2	500,000	300,000	50,000

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max Passive ID Sessions	Max Merged/EZC Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3415	Dedicated PSNs (2 for HA)	5,000	50,000	10,000
	SNS-3495		20,000	100,000	25,000
	SNS-3515		7,500	100,000	15,000
	SNS-3595		40,000	300,000	50,000

Shared PSNs (up to 5) OR PSNs dedicated to RADIUS (up to 3) and Passive ID Service (2 for HA)

ISE 2.4 Passive ID & Easy Connect Multi-Service Scaling

Max Concurrent Passive ID/Easy Connect Sessions by Deployment and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max Passive ID Sessions	Max Merged/EZC Sessions (subset of RADIUS/Psv ID)
Stand-alone	All personas on same node	3515	0	7,500	100,000	1,000
		3595	0	20,000	300,000	2,000
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	5 / 3 + 2	7,500	100,000	1,000 / 5,000
		3595 as PAN + MNT	5 / 3 + 2	20,000	500,000	2,000 / 10,000
Dedicated	Each Persona on Dedicated Node	3515 as PAN and MNT	48 + 2	500,000	500,000	500,000
		3595 as PAN and Large MnT	48 + 2	500,000	1M	500,000

Shared PSNs (up to 5) OR PSNs dedicated to RADIUS (up to 3) and Passive ID Service (2 for redundancy)

Number of PSNs dedicated to Passive Identity (Minimum 2 for HA)

- By PSN

Scaling per PSN	Platform		Max RADIUS per PSN	Max Passive ID	Max Merged/EZC per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515		7,500	100,000	10,000
	SNS-3595		40,000	300,000	50,000

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6 Passive ID & Easy Connect Multi-Service Scaling

Max Concurrent Passive ID/Easy Connect Sessions by Deployment and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max Passive ID Sessions	Max Merged/EZC Sessions (subset of RADIUS/Psv ID)
Stand-alone	All personas on same node	3615	0	10,000	100,000	1,000
		3655	0	25,000	300,000	2,000
		3695	0	50,000	300,000	2,000
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT	5 / 3 + 2	10,000	100,000	1,000 / 5,000
		3655 as PAN + MNT	5 / 3 + 2	25,000	500,000	2,000 / 10,000
		3695 as PAN+MNT	5 / 3 + 2	50,000	500,000	2,000 / 10,000
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	48 + 2	500,000	500,000	500,000
		3695 as PAN and MnT	48 + 2	500,000 (2M)	2M	500,000

Shared PSNs (up to 5) OR PSNs dedicated to RADIUS (up to 3) and Passive ID Service (2 for redundancy)

Number of PSNs dedicated to Passive Identity (Minimum 2 for HA)

- By PSN

Scaling per PSN	Platform		Max RADIUS per PSN	Max Passive ID	Max Merged/EZC per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3615		10,000	100,000	10,000
	SNS-3655		50,000	500,000	50,000
	SNS-3695		100,000	2M	50,000

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.7 Passive ID & Easy Connect Multi-Service Scaling

Max Concurrent Passive ID/Easy Connect Sessions by Deployment and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max Passive ID Sessions	Max Merged/EZC Sessions (subset of RADIUS/Psv ID)
Stand-alone	All personas on same node	3615	0	10,000	100,000	1,000
		3655	0	25,000	300,000	2,000
		3695	0	50,000	300,000	2,000
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT	5 / 3 + 2	10,000	100,000	1,000 / 5,000
		3655 as PAN + MNT	5 / 3 + 2	25,000	500,000	2,000 / 10,000
		3695 as PAN+MNT	5 / 3 + 2	50,000	500,000	2,000 / 10,000
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	48 + 2	500,000	500,000	500,000
		3695 as PAN and MnT	48 + 2	500,000 (2M)	2M	500,000

Shared PSNs (up to 5) OR PSNs dedicated to RADIUS (up to 3) and Passive ID Service (2 for redundancy)

Number of PSNs dedicated to Passive Identity (Minimum 2 for HA)

- By PSN

Scaling per PSN	Platform		Max RADIUS per PSN	Max Passive ID	Max Merged/EZC per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3615		10,000	100,000	5000
	SNS-3655		50,000	500,000	25,000
	SNS-3695		100,000	2M	50,000

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

pxGrid v1 Multi-Service Scaling

ISE 2.2+ Max pxGrid Operations by Deployment Model and Platform

Scaling per Deployment Model	Platform	Max ded. PSNs	Max ded. pxGrid	Max RADIUS Sessions per Deployment	Max pxGrid Subscribers per Deployment
Standalone: All personas on same node (2 nodes redundant)	3515/3615	0	0	7,500/10,000	2
	3595/3655	0	0	20,000/25,000	2
	3695	0	0	50,000	2
Hybrid: PAN+MnT+PXG on same node and dedicated PSNs -OR- PAN+MnT and ded. PSN & PXG (Minimum 4 nodes redundant)	3515/3615 as PAN+MNT+PXG	5 / 3	0 / 2	7,500/10,000	5 / 15
	3595/3655 as PAN+MNT+PXG	5 / 3	0 / 2	20,000/25,000	5 / 15
	3595 as PAN+MNT+PXG	5 / 3	0 / 2	50,000	5 / 15
All personas on Dedicated nodes (Minimum 6 nodes redundant)	3595 as PAN and MNT	50	2	500,000	25
	3695 as PAN and MNT	50	2	500,000 (2M)	25

Scaling per PXG Node	Platform			Max RADIUS per PSN	Max Subscribers per PXG
Dedicated pxGrid nodes (Max Publish Rate Gated by Total Deployment Size)	SNS-3515/3615			7,500/10,000	15
	SNS-3595/3655			40,000/50,000	25
	SNS-3695			100,000	25

Dedicated PSNs (up to 5) when pxGrid on PAN+MNT OR Split PSNs (up to 3) and pxGrid (up to 2 for HA)

pxGrid v2 Multi-Service Scaling

ISE 2.4+ Max pxGrid Operations by Deployment Model and Platform

Deployment Model		Platform	Max dedicated PSNs	Max dedicated pxGrid	Max RADIUS Sessions per Deployment	Max pxGrid Subscribers per Deployment
Stand-alone	All personas on same node	3515/3615	0	0	7,500/10,000	20
		3595/3655	0	0	20,000/25,000	30
		3695	0	0	50,000	30
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	35/3615 as PAN+MNT+PXG	5 / 3	0 / 2	7,500/10,000	140 / 400
		3595/3655	5 / 3	0 / 2	20,000/25,000	160 / 600
		3695	5 / 2	0 / 3	50,000	160 / 600
Dedicated	Each Persona on Dedicated Node	3595/3655 as PAN and MNT	50	4	500,000	800 (200 each)
		3695 as PAN and MnT	50	4	500,000 / 2M	800 (200 each)

Dedicated PSNs (up to 5) when pxGrid on PAN+MNT
OR Split 5 nodes between dedicated PSNs and pxGrid

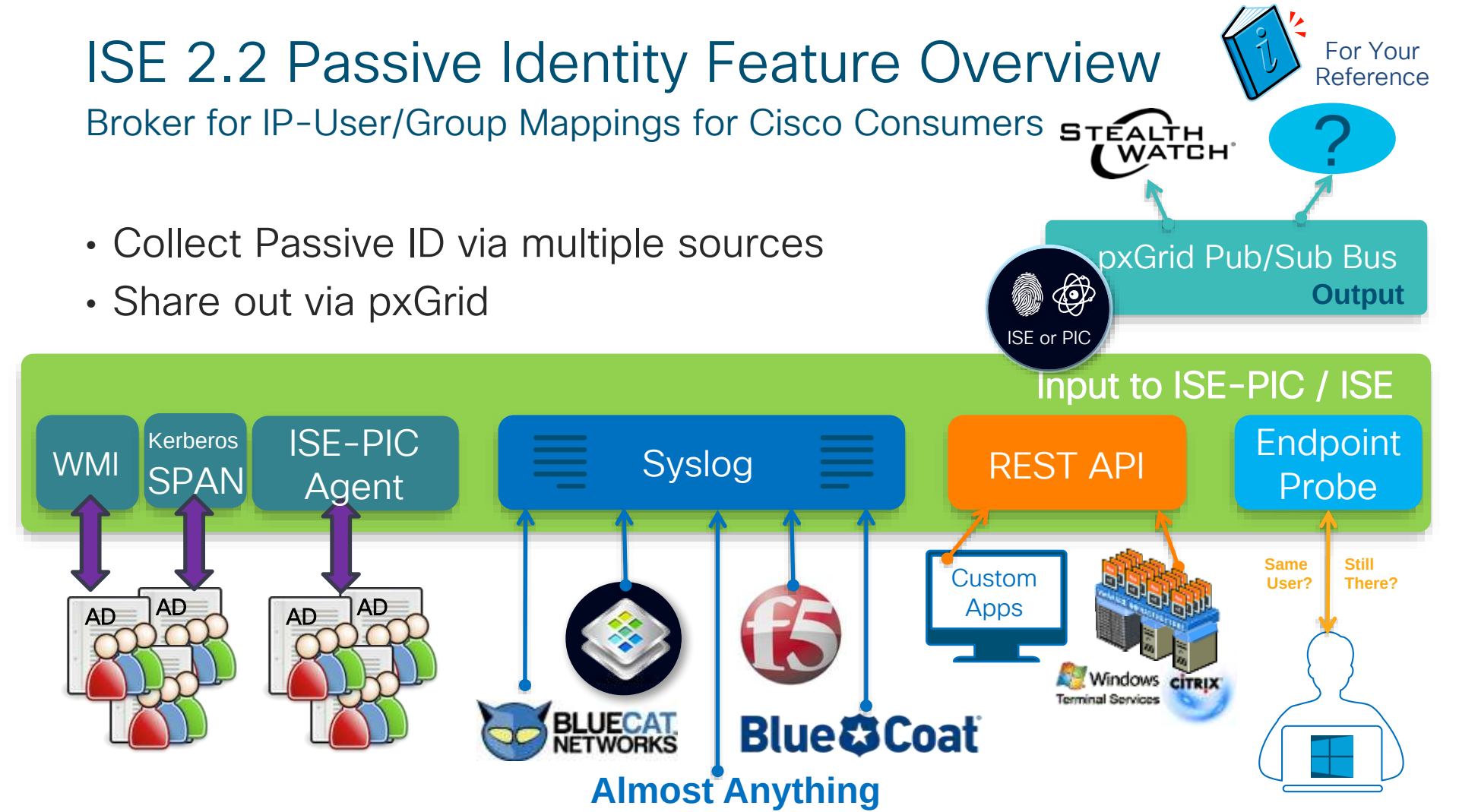
* ISE 2.3 introduced pxGrid v2.0 based on WebSockets

Scaling per pxGrid Node	Platform		Max RADIUS per PSN	Max Subscribers per PXG
Dedicated pxGrid nodes (Max Publish Rate Gated by Deployment Size)	SNS-3515/3615		7,500/10,000	200
	SNS-3595/3655		40,000/50,000	200
	SNS-3695		100,000	200

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.2 Passive Identity Feature Overview

Broker for IP-User/Group Mappings for Cisco Consumers



- Collect Passive ID via multiple sources
- Share out via pxGrid

ISE-PIC (Passive Identity Connector) Scaling

Max Passive ID Sessions and pxGrid Subscribers by Virtual Platform 35xx 2.4 & 36xx 2.7

ISE-PIC Deployment	Max # Appliances	Max RADIUS Sessions	Max Passive ID Sessions	Max pxGrid Subscribers
35/615 Virtual Appliance	1 (2 for HA)	0	100,000	20
3595/3655	1 (2 for HA)	0	300k/500k	20
3695 Virtual Appliance	1 (2 for HA)	0	2M	20

ISE Passive ID / ISE-PIC	35xx/36xx Virtual Appliance
Max AD Forest/Domain Join Points (user/group queries)	50
Max AD Domain Controllers supported via WMI or ISE AD Agent	100
Max AD Agents (assuming 1:1 agent to DC)	100
Recommended # DCs per Agent (agent on DC)	1
Recommended # DCs per Agent (agent on member server)	10
Recommended # PSNs enabled for WMI (Passive ID service)	2
Max REST API Providers	50
Max REST API EPS	1,000
Max Syslog Providers	70
Max Syslog EPS	400
Max Endpoints Probed per Interval	100,000

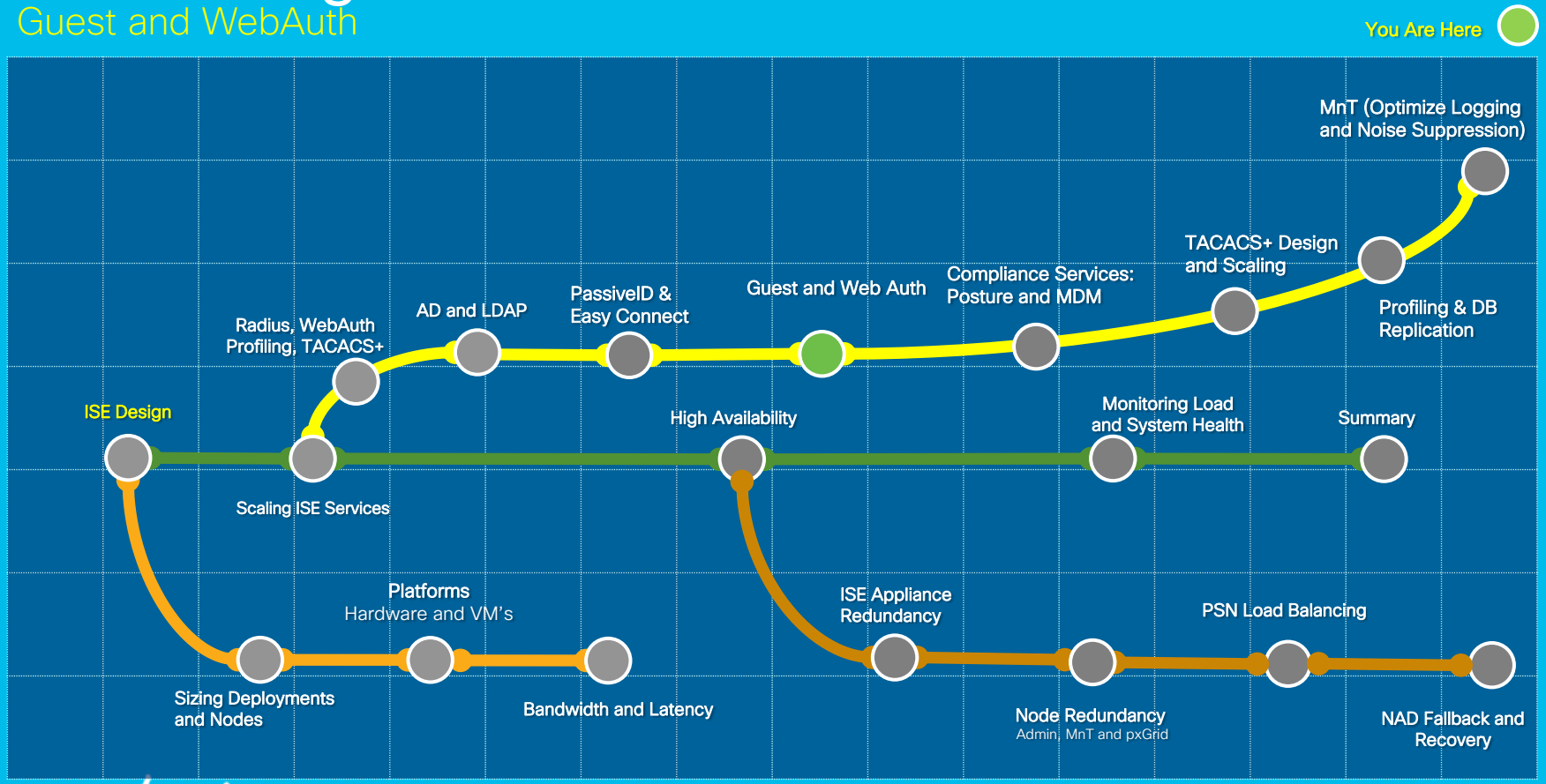
- ISE-PIC currently delivered as virtual appliance only
- Sizing based on SNS-3515/3595 specifications

Passive ID scale applies to **BOTH** ISE 2.7 and ISE-PIC

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

Guest and WebAuth

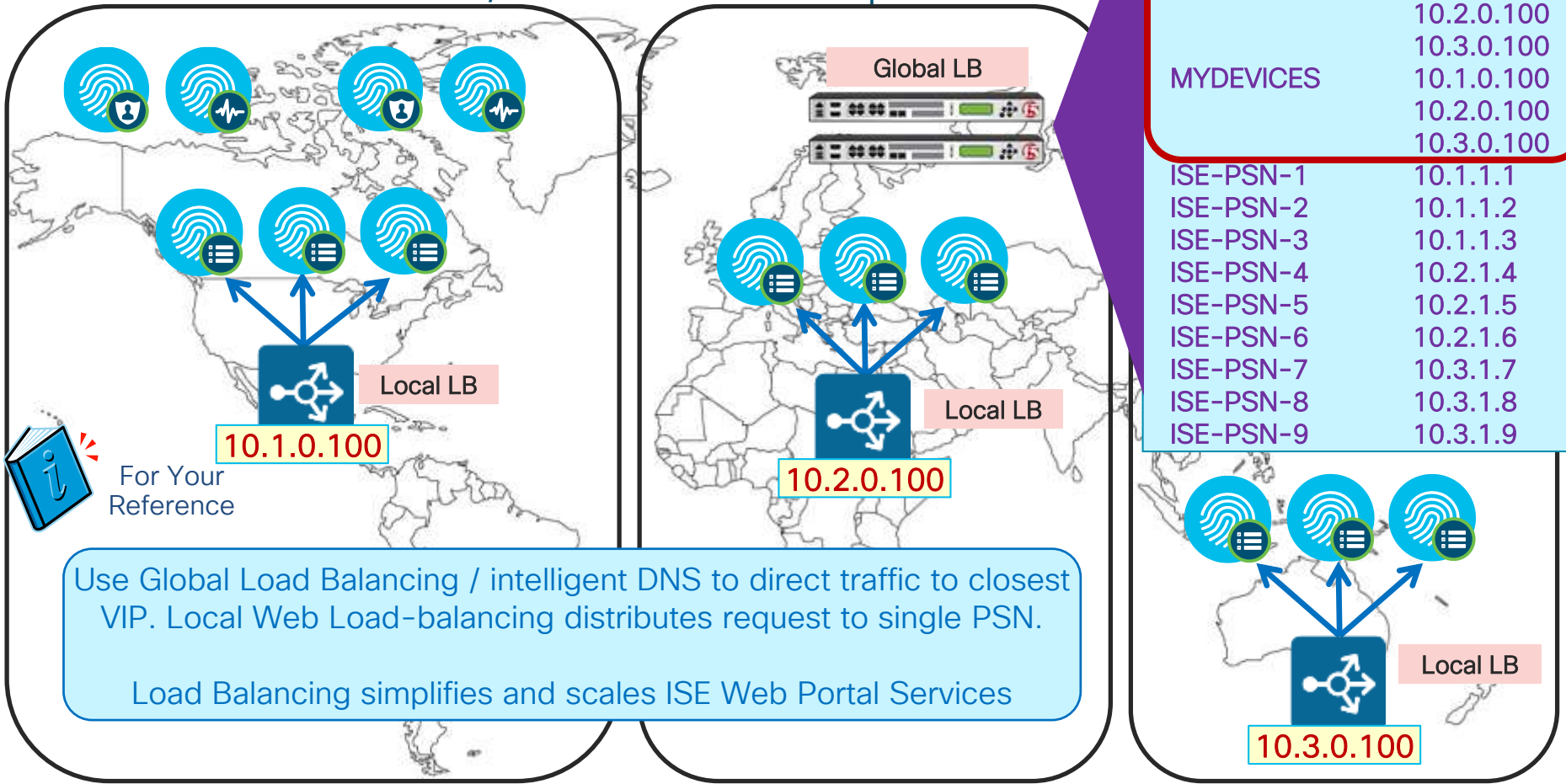


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Guest and Web Authentication Services

Scaling Global Sponsor / MyDevices

Global Load Balancers / “Smart DNS” Example



DNS SERVER: DOMAIN = COMPANY.COM

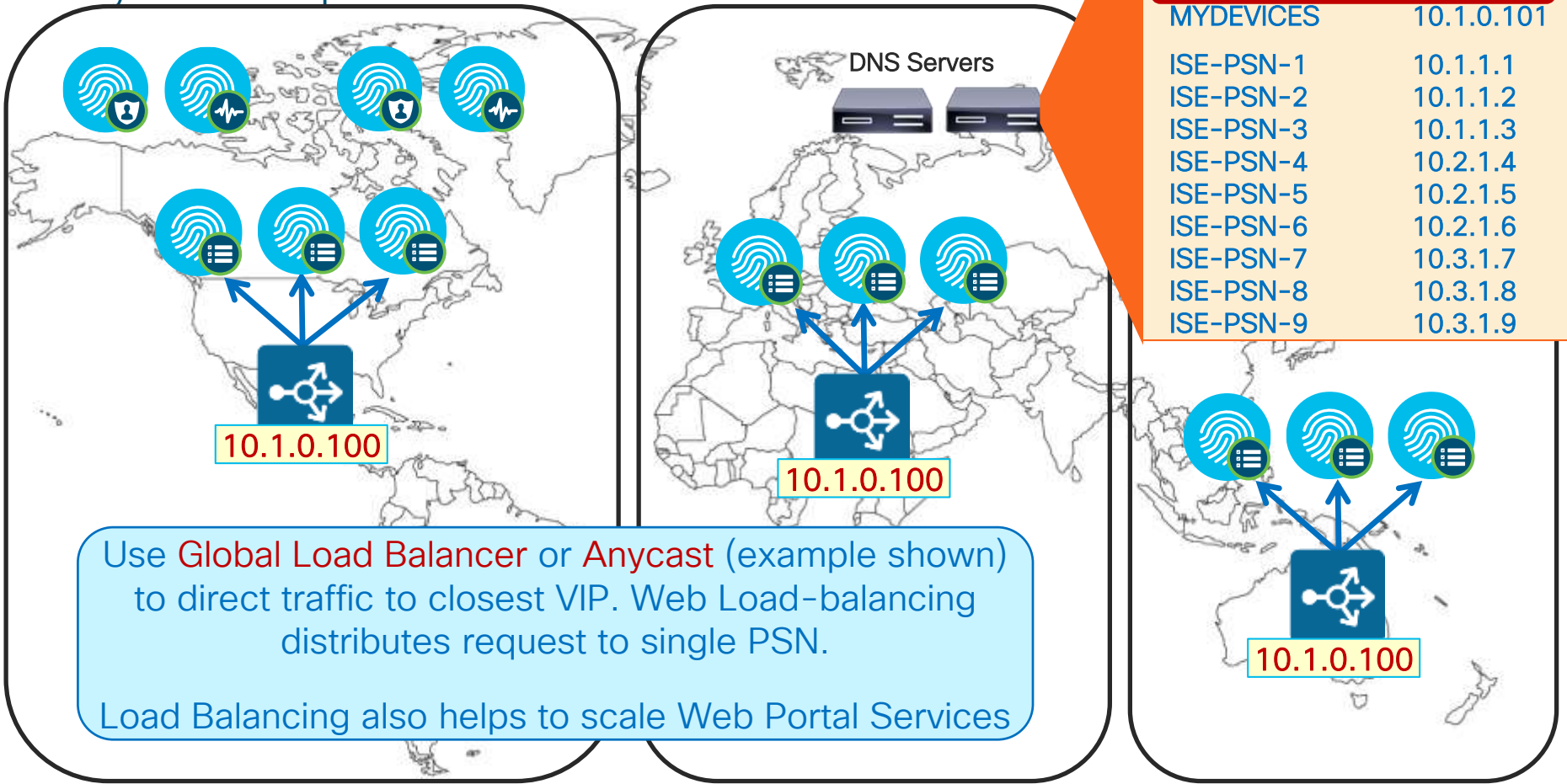
SPONSOR	10.1.0.100
	10.2.0.100
	10.3.0.100
MYDEVICES	10.1.0.100
	10.2.0.100
	10.3.0.100
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

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

Load Balancing simplifies and scales ISE Web Portal Services

Scaling Global Sponsor / MyDevices

Anycast Example



DNS SERVER: DOMAIN = COMPANY.COM	
SPONSOR	10.1.0.100
MYDEVICES	10.1.0.101
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

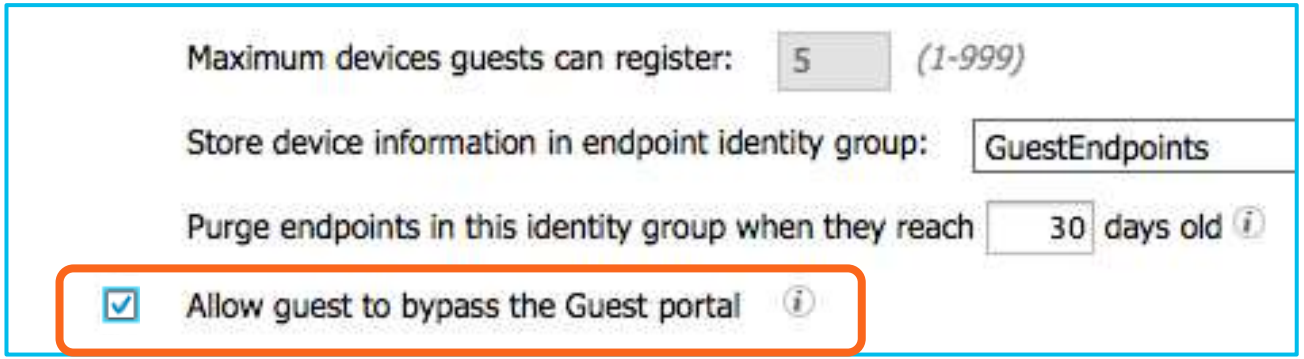
Use Global Load Balancer or Anycast (example shown) to direct traffic to closest VIP. Web Load-balancing distributes request to single PSN.

Load Balancing also helps to scale Web Portal Services

Scaling Guest Authentications Using 802.1X

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

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



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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Web Auth

“Remember Me” Guest Flows

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

Endpoint identity group: * GuestEndpoints

Purge endpoints in this identity group when they reach 30 days

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

Work Centers > Guest Access > Settings > Logging

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

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

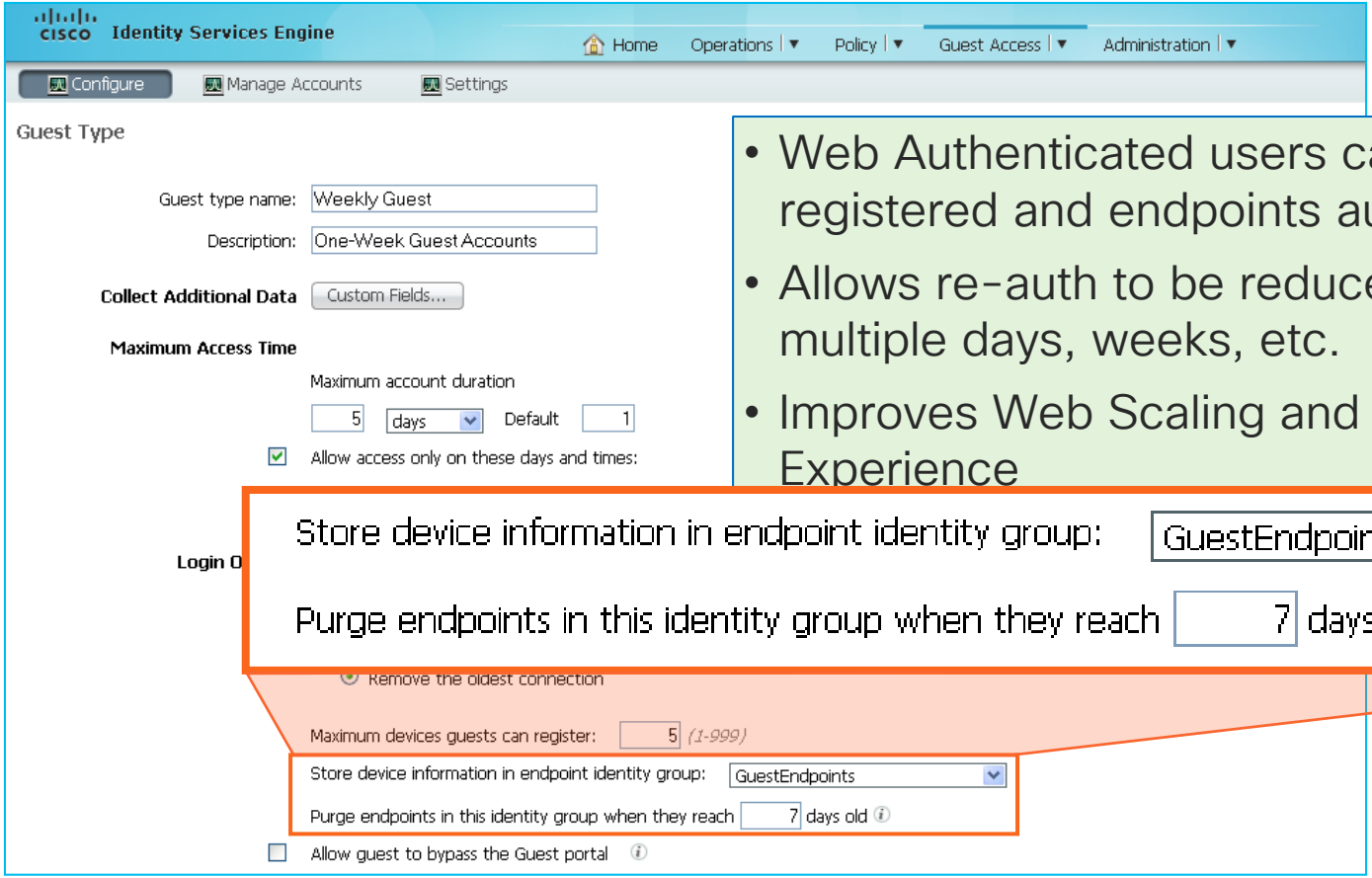
Reset Save

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Automated Device Registration and Purge

For Your Reference



- 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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Endpoint Purging

For Your Reference

System | Identity Management | Identity Mapping | Network Resources | Device Portal Management | Feed Service | pxGrid Services

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Settings

- User Custom Attributes
- User Password Policy
- Endpoint Purge

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	Edit |

Purge

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

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every Everyday at 01 00

Save | Purge immediately | Reset

Matching Conditions Purge by:

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

Endpoint Purging Examples

For Your Reference

System | Identity Management | Identity Mapping | Network Resources | Device Portal Management | Feed Service | pxGrid Services

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Settings

- User Custom Attributes
- User Password Policy
- Endpoint Purge

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

Purge immediately | Reset

Matching Conditions Purge by:

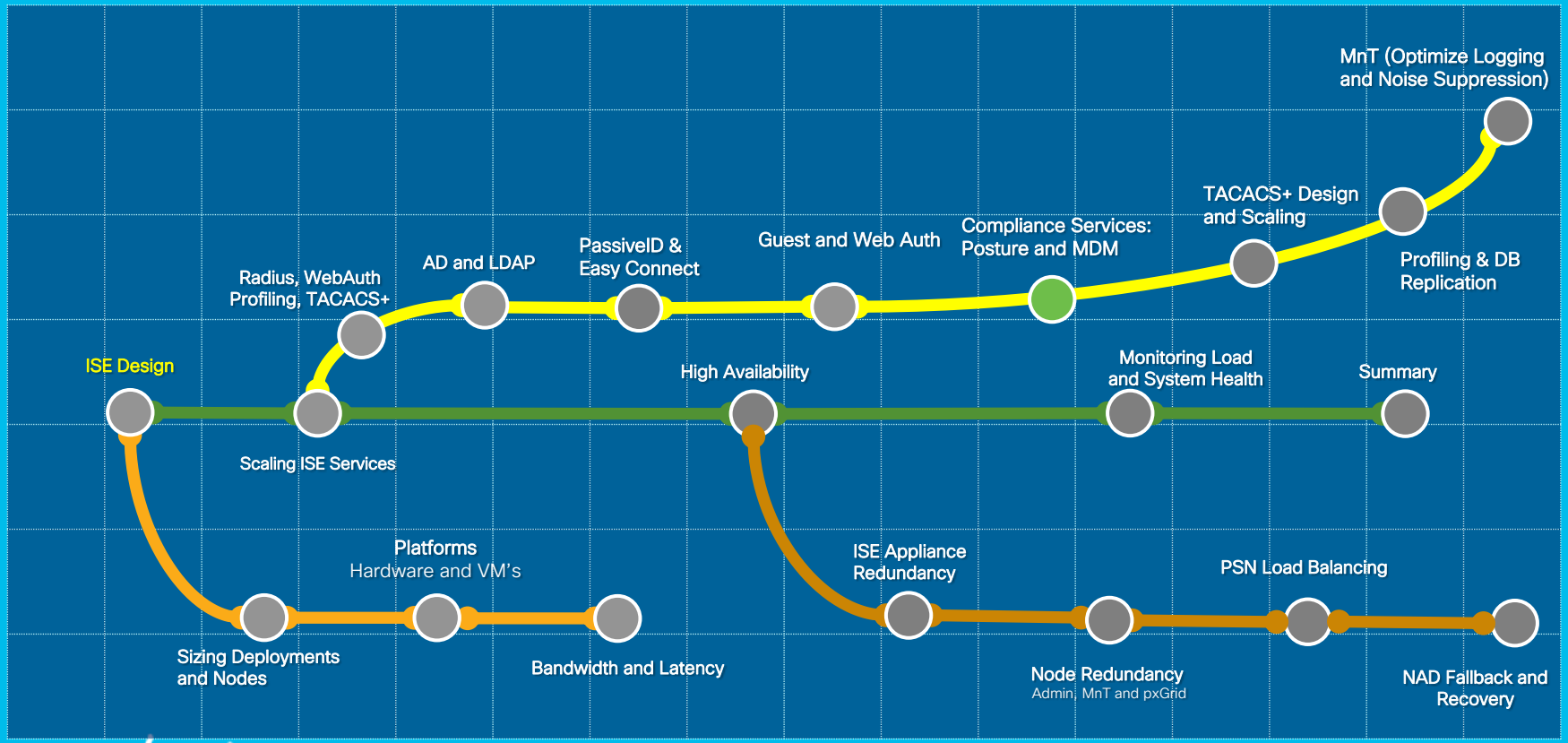
- # Days After Creation
- # Days Inactive
- Specified Date

On Demand Purge

Session Agenda

Compliance Services: Posture and MDM

You Are Here



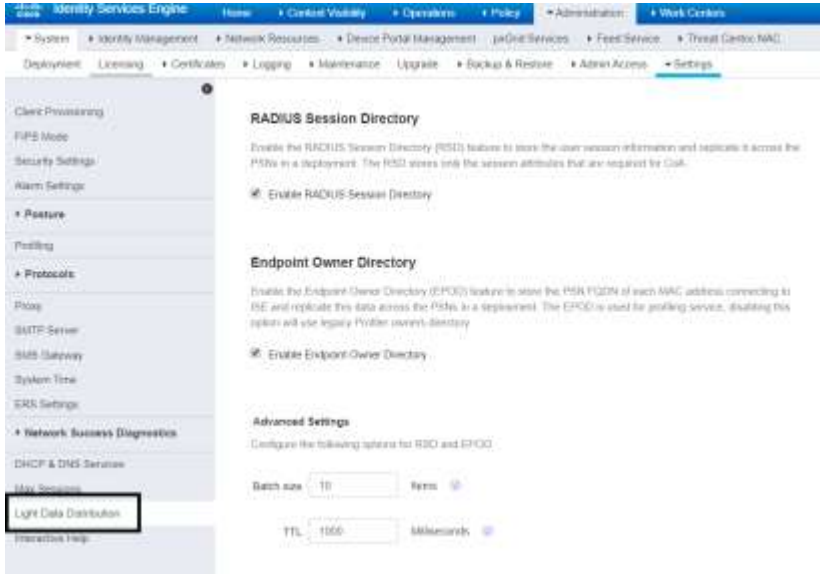
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Posture & MDM

ISE Light Data Directory

User device session information shared across the deployment

- Avoids using MnT or PAN nodes as a single point of truth or failure.
- LDD stores a light session information and replicates it across the deployment using RabbitMQ
- Allows future Infrastructure development for WAN survivability –PAN/MnT unreachable

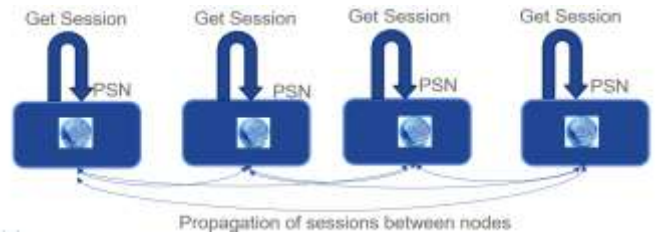


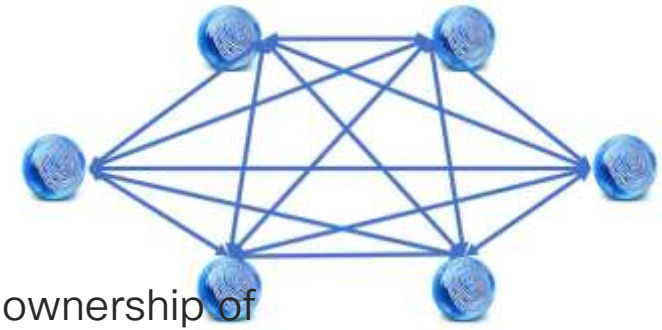
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Architecture on LDD

Session exists in local PSN and MnT node

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



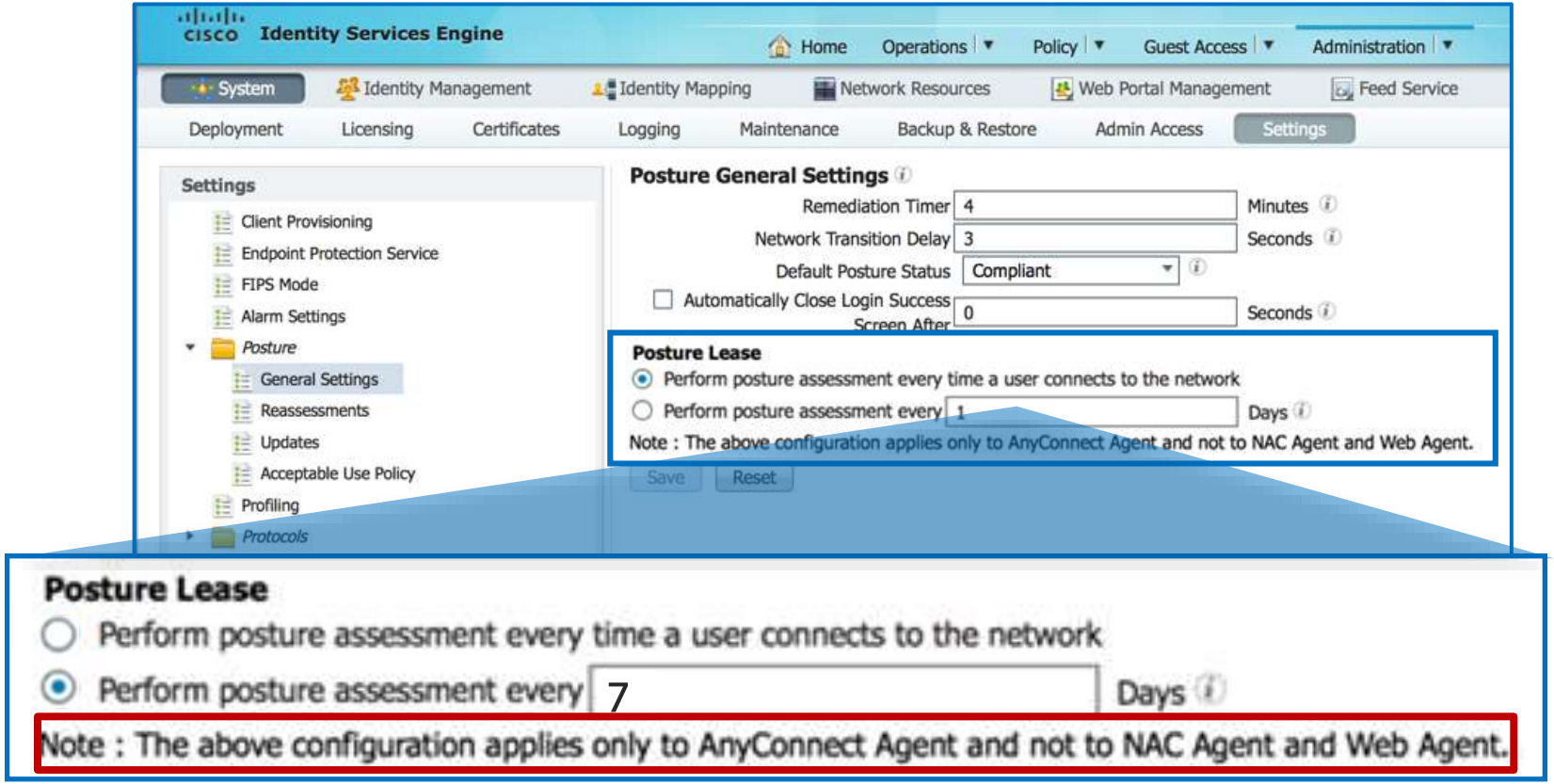


NODE Groups is not same as LDD, LDD just shares the ownership of the endpoint. MAR Cache is shared between node groups

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Posture Lease

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

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

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling MDM

ISE 2.4 adds support for managing MDM Attributes via ERS API

Prepopulate MDM Enrollment and/or Compliance via ERS API

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

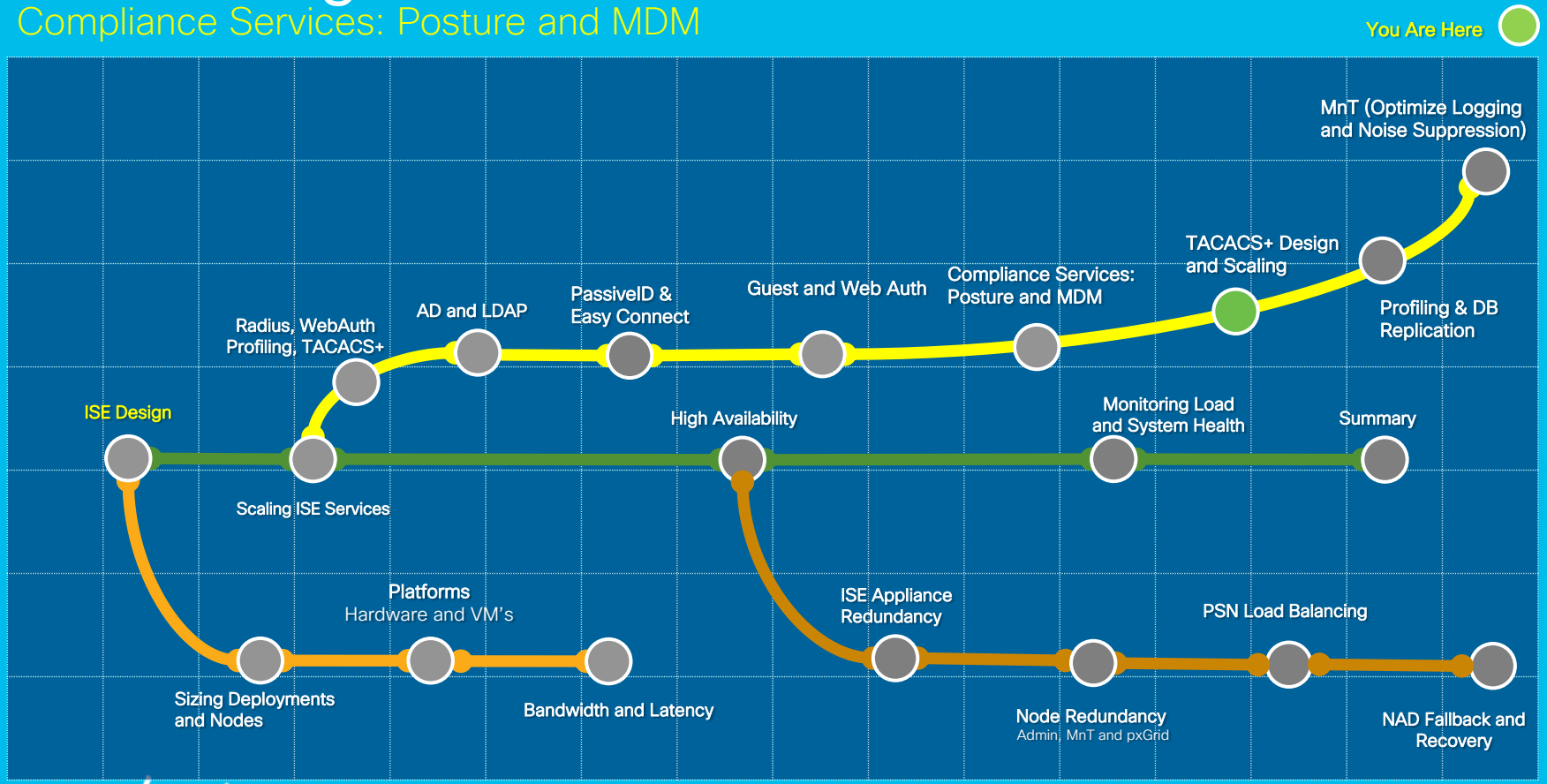
```
<customAttributes>
  <customAttributes>
    <entry>
      <key>MDM_Registered</key>
      <value>true</value>
    </entry>
    <entry>
      <key>MDM_Compliance</key>
      <value>false</value>
    </entry>
    <entry>
      <key>Attribute_XYZ</key>
      <value>Value_XYZ</value>
    </entry>
  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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Scaling

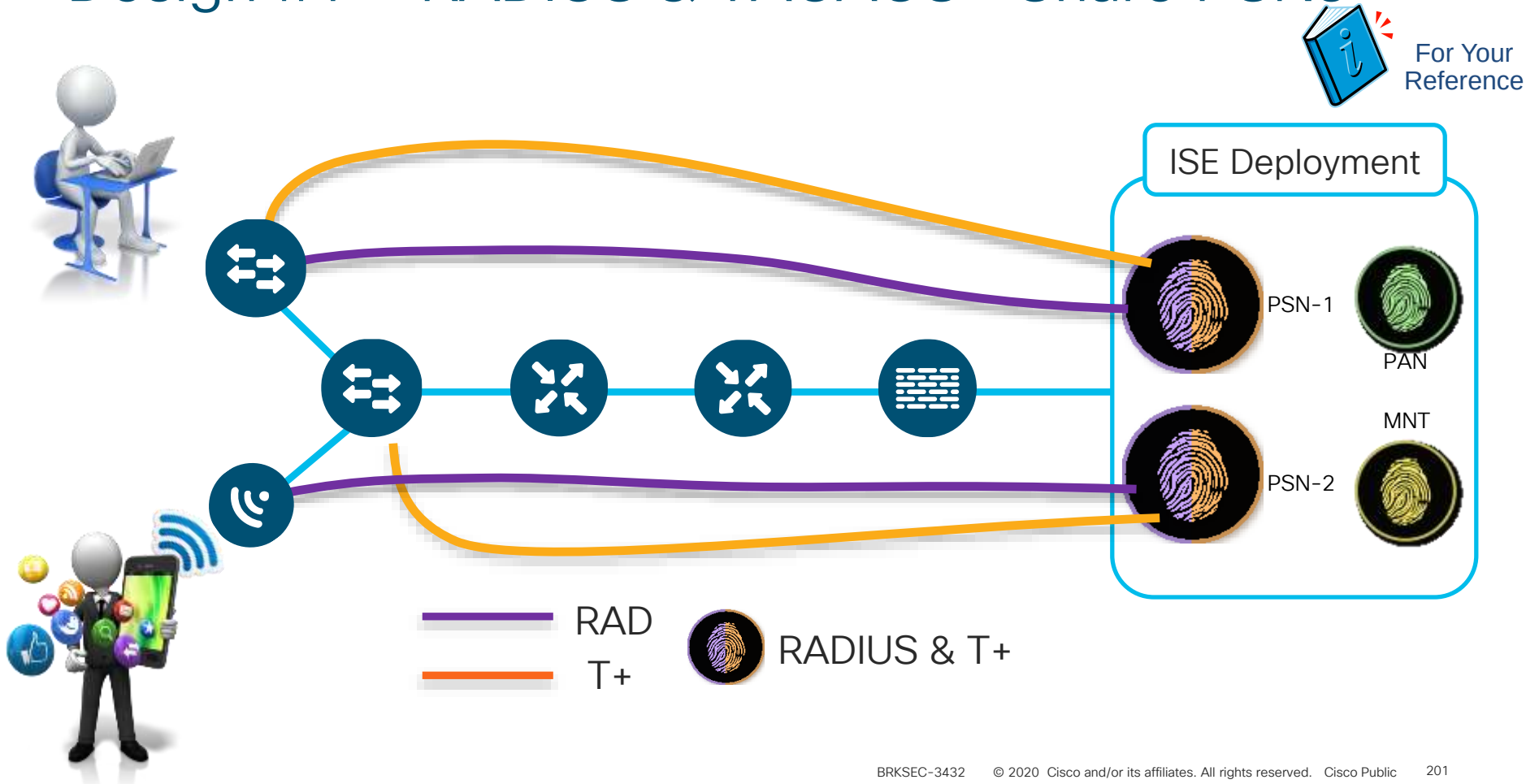
Session Agenda

Compliance Services: Posture and MDM



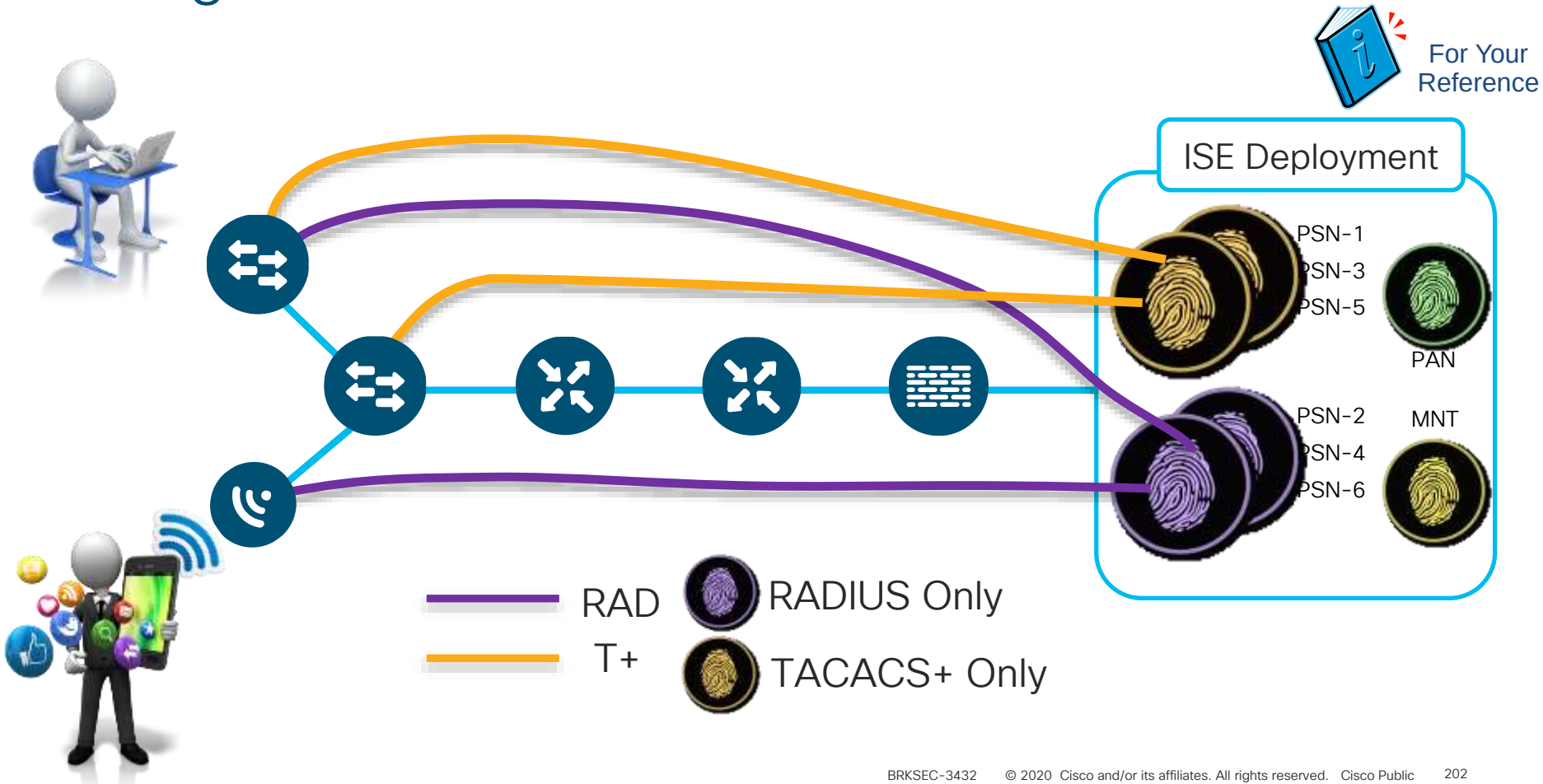
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design #1 – RADIUS & TACACS+ Share PSNs



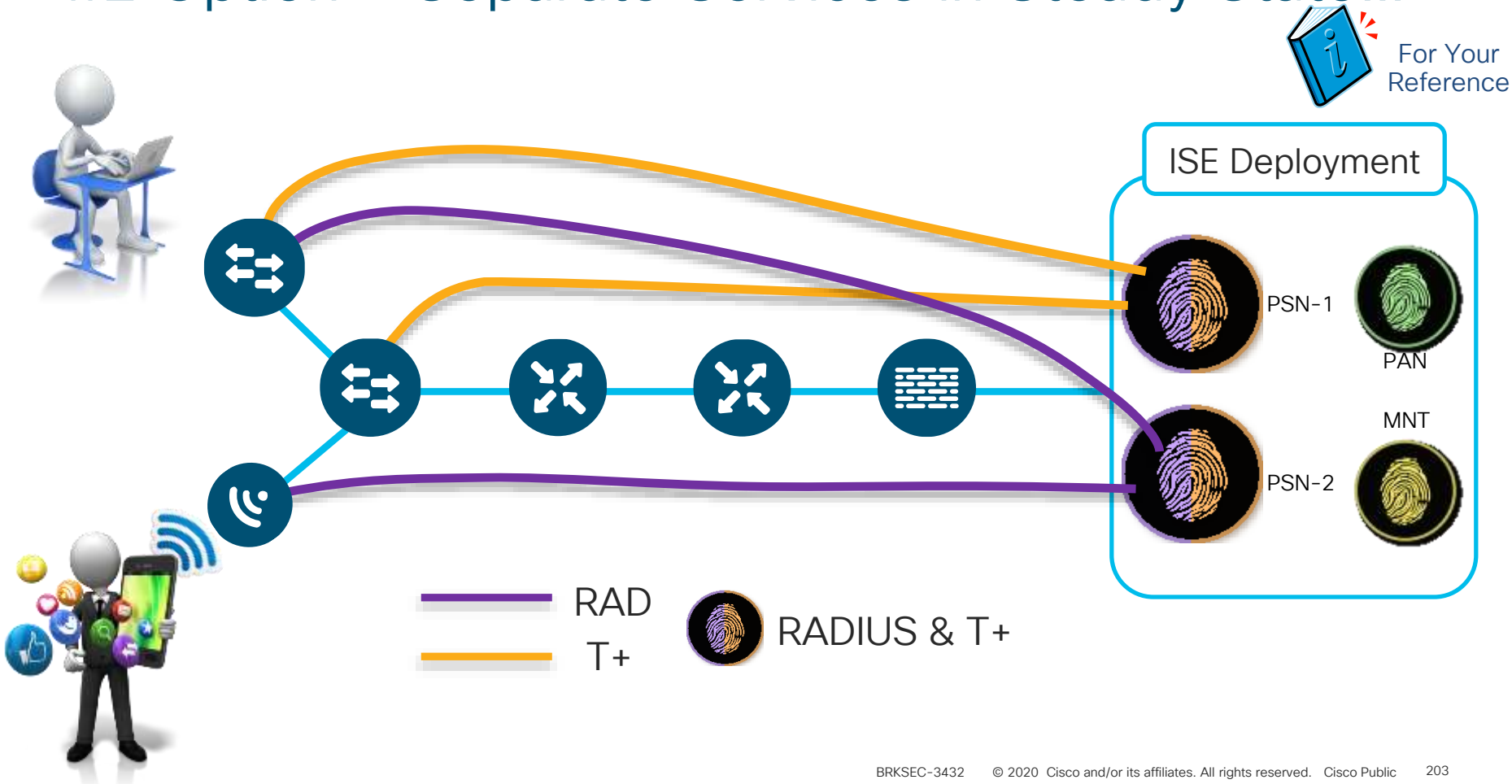
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design #2 – RADIUS & T+ Use Dedicated PSNs



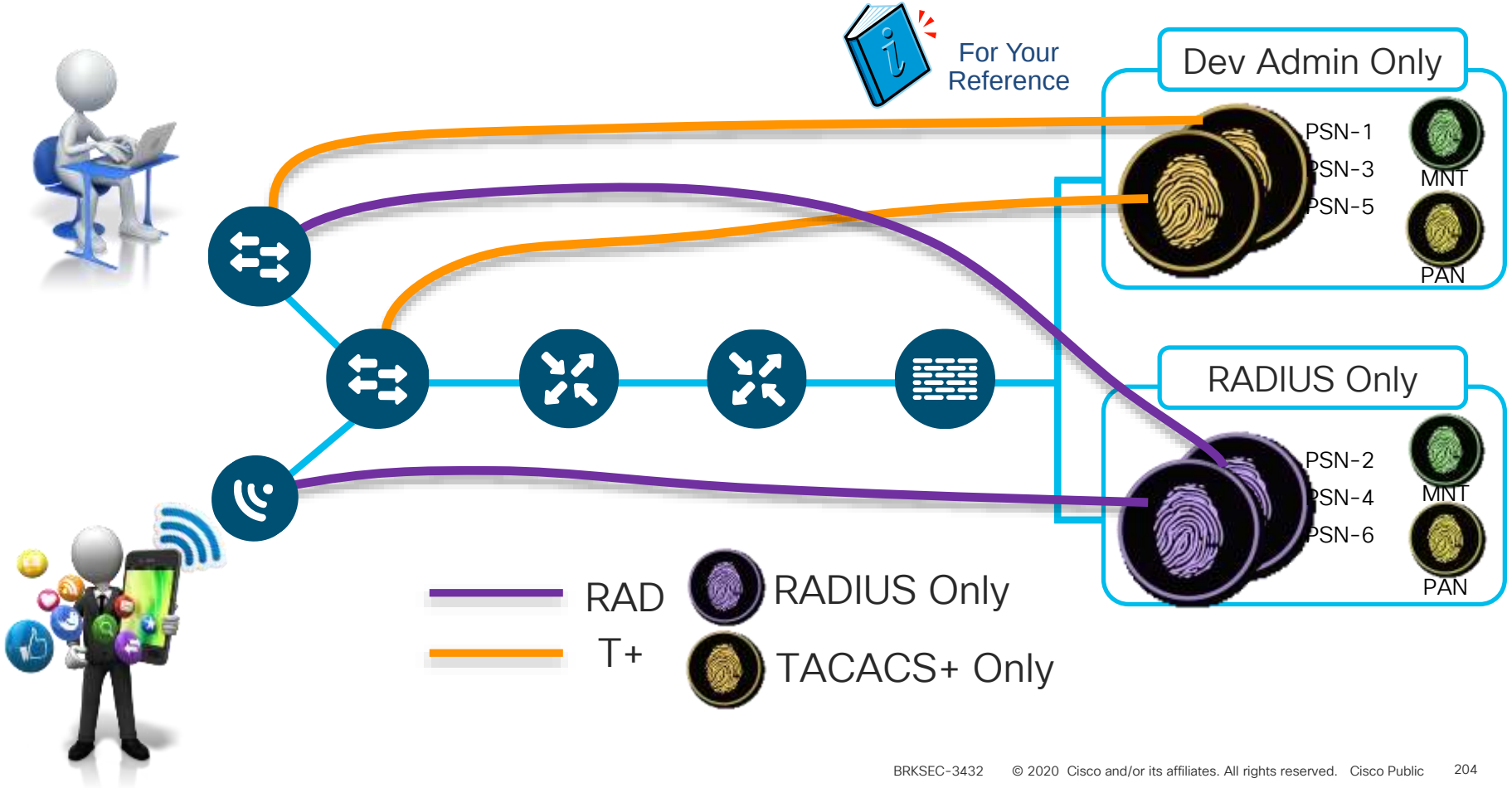
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

#2 Option – Separate Services in Steady State…



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

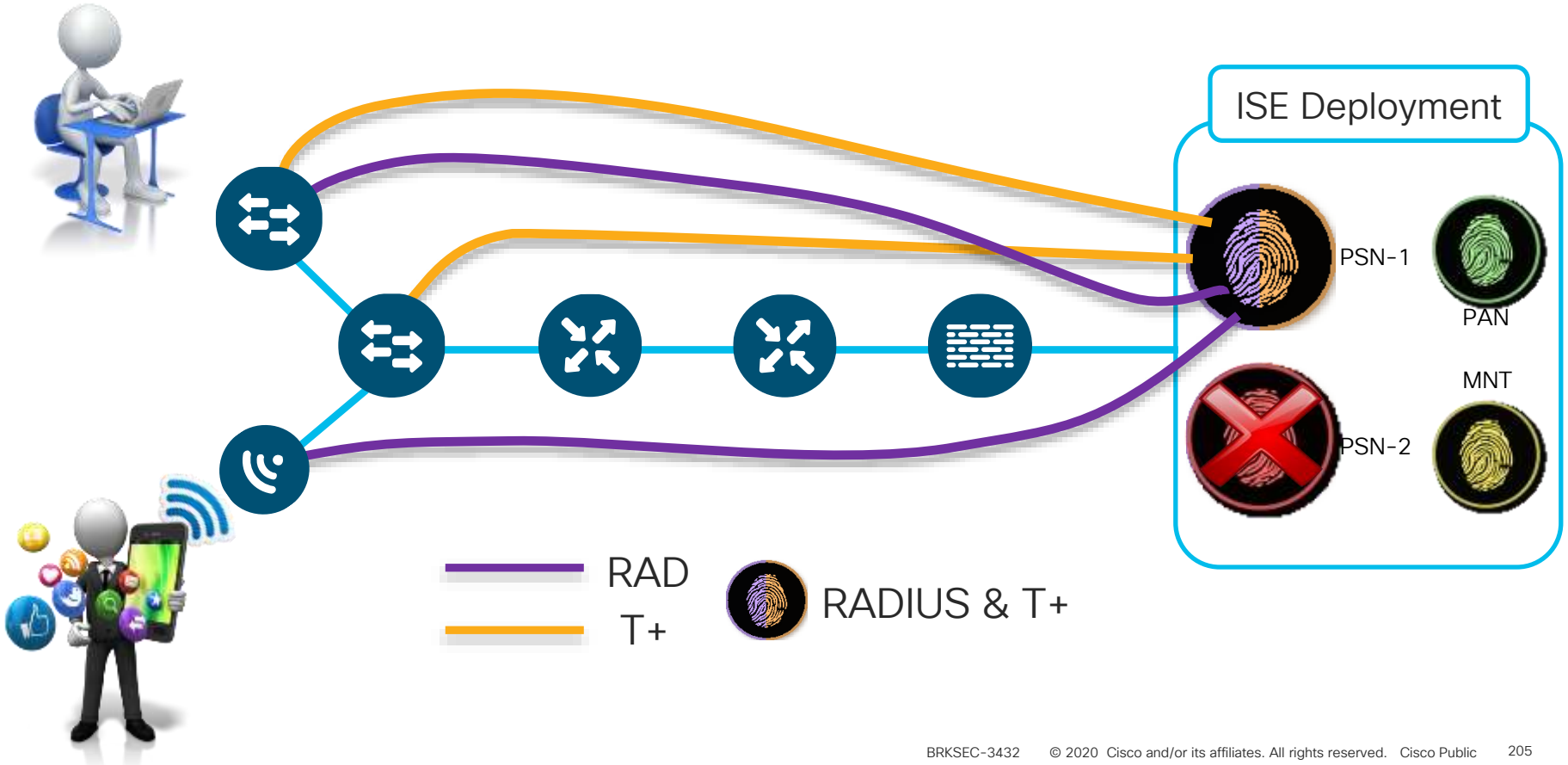
Design #3 – Separate Deployments for RAD & T+



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

...Fallback to other Service Node on Failure

For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Options for Deploying Device Admin

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

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

RADIUS Only PSNs

For Your Reference

Administration > System > Deployment > [ISE node]

Personas

- [x] Administration — Role **PRIMARY** — Make Standalone
- [x] Monitoring — Role PRIMARY — Other Monitoring Node
- [x] Policy Service — Policy Service is Required
  - [x] Enable Session Services
    - Include Node in Node Group: None
  - [x] Enable Profiling Service
  - [x] Enable SXP Service
    - Use Interface: GigabitEthernet 0
  - [ ] Enable Device Admin Service — TACACS+ Disabled
  - [x] Enable Identity Mapping
- [x] pxGrid

Enable What's Needed for Network Access

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Only PSNs

For Your Reference

Administration > System > Deployment > [ISE node]

Personas

- [x] Administration — Role **PRIMARY** — Make Standalone
- [x] Monitoring — Role PRIMARY — Other Monitoring Node
- [x] Policy Service — Policy Service is Required
  - [ ] Enable Session Services
    - Include Node in Node Group: None
  - [ ] Enable Profiling Service
  - [ ] Enable SXP Service
    - Use Interface: GigabitEthernet 0
  - [x] Enable Device Admin Service — Device Admin = T+
  - [ ] Enable Identity Mapping
- [ ] pxGrid

Disable Network Access Services

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Design

For Your Reference

3 Basic ISE Deployment Models for Device Administration

	Dedicated Deployments	Dedicated PSNs	Integrated
Architecture	PAN/MNT: T+ RADIUS + PSN:TACACS+ + PSN:TACACS+ PAN/MNT: + PSN:RADIUS + PSN:RADIUS	PAN/MNT: RADIUS & TACACS+ + PSN:TACACS+ + PSN:RADIUS + PSN:TACACS+ + PSN:RADIUS ...	PAN/MNT: RADIUS & TACACS+ + PSN:RADIUS & TACACS+ + PSN:RADIUS & TACACS+ + PSN:RADIUS & TACACS+ + PSN:RADIUS & TACACS+
Cons	• Separate ISE deployments to maintain • Cost of additional PAN and MNT nodes for the second deployment	• Per-PSN utilization may be low for a dedicated function • May need additional PSNs for distributed coverage	• Potential need for cross-department admin access depending on the organization • Load from Network Access may impact Device Administration services and vice versa
Pros	• Complete separation of policy & operations for Device Administration and Network Access	• Centralized policy & monitoring for all AAA • Scale Device Admin independently from Network Access as needed	• Centralized policy & monitoring for all AAA • Same configuration for all PSNs • Scale all AAA needs incrementally by adding a PSN when or where needed

Whether you dedicate a separate instance for TACACS+ is more of a security and operational policy decision. If separated in ACS today, then continue doing so if that model serves you well. If you wish to combine both TACACS+ Device Administration and RADIUS into same deployment, then dedicating nodes to TACACS+ service may be the best option for a large organization to prevent user services from impacting device admin services and vice versa.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.3 TACACS+ Scaling (RADIUS and T+)

For Your Reference

Max Concurrent TACACS+ TPS by Deployment Model and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS
Stand-alone	All personas on same node (2 nodes redundant)	3415	0	5,000	50
		3495	0	10,000	50
		3515	0	7,500	50
		3595	0	20,000	50
Hybrid	PAN + MnT on same node; Dedicated PSN (Minimum 4 nodes redundant)	3415 as PAN+MNT	* 5 / 3+2	5,000	100 / 500
		3495 as PAN+MNT	* 5 / 3+2	10,000	100 / 1,000
		3515 as PAN+MNT	* 5 / 3+2	7,500	100 / 1,000
		3595 as PAN+MNT	* 5 / 3+2	20,000	100 / 1,500
Dedicated	Each persona dedicated (Min 6 nodes redundant)	3495 as PAN and MNT	* 40 / 38+2	250,000	1,000 / 2,000
		3595 as PAN and MNT	* 50 / 48+2	500,000	1,000 / 3,000

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Deployment Maximums)	SNS-3415		5,000	500
	SNS-3495		20,000	1,000
	SNS-3515		7,500	1,000
	SNS-3595		40,000	1,500

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4+ TACACS+ Multi-Service Scaling (RADIUS and T+)

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

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Standa-alone	All personas on same node	3515	0	7,500	100
		3595	0	20,000	100
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	* 5 / 3+2	7,500	250 / 2,000
		3595 as PAN+MNT	* 5 / 3+2	20,000	250 / 3,000
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	* 50 / 47+3	500,000	2,500 / 4,000
		3595 as PAN and Large MNT	* 50 / 47+3	500,000	2,500 / 6,000

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

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

- By PSN

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515		7,500	2,000
	SNS-3595		40,000	3,000

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

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

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

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

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

ISE 2.3 TACACS+ Scaling (TACACS+ Only)

For Your Reference

Max Concurrent TACACS+ TPS by Deployment Model and Platform

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Stand-alone	All personas on same node (2 nodes redundant)	3415	0	N/A	500
		3495	0	N/A	1,000
		3515	0	N/A	1,000
		3595	0	N/A	1,500
Hybrid	PAN + MnT on same node; Dedicated PSN (Minimum 4 nodes redundant)	3415 as PAN+MNT	* 5 (2 rec.)	N/A	2,500 (1,000)
		3495 as PAN+MNT	* 5 (2 rec.)	N/A	5,000 (2,000)
		3515 as PAN+MNT	* 5 (2 rec.)	N/A	5,000 (2,000)
		3595 as PAN+MNT	* 5 (2 rec.)	N/A	** 7,500 (3,000)
Dedicated	Each persona dedicated (Min 6 nodes redundant)	3495 as PAN and MNT	* 40 (2 rec.)	N/A	** 20,000 (2,000)
		3595 as PAN and MNT	* 50 (2 rec.)	N/A	** 25,000 (3,000)

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3415	** Currently exceeds max MNT log capacity	5,000	500
	SNS-3495		20,000	1,000
	SNS-3515		7,500	1,000
	SNS-3595		40,000	1,500

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 TACACS+ Multi-Service Scaling (TACACS+ Only)

Max Concurrent TACACS+ TPS by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Stand-alone	All personas on same node	3515	0	N/A	1,000
		3595	0	N/A	1,500
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	* 5 / 2	N/A	**2,000 / 2,000
		3595 as PAN+MNT	* 5 / 2	N/A	**3,000 / 3,000
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	* 50 / 4	N/A	**5,000 / 5,000
		3595 as PAN and Large MnT	* 50 / 5	N/A	**10,000 / 10,000

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

** Max log capacity for MNT

- By PSN

Scaling per PSN	Platform		Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515		7,500	2,000
	SNS-3595		40,000	3,000

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

Max Concurrent TACACS+ TPS by Deployment Model and Platform

- By Deployment

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

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

** Max log capacity for MNT

- By PSN

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Other TACACS+ Scale Facts

- Max T+ Command Sets — 200 (20 lines each command set)
- Max T+ Profiles — 50

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ MnT Scaling

Human Versus Automated Device Administration

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

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

- “Human” Device Admin Example:
  - For a normal “human” session we may expect to see 10 commands, so a session would be approximately: [5kB + (10 * 3kB)) = 35kB. Suppose a maximum of 50 such sessions per admin per day from 50 admins (and few organizations have > 50 admins)
    - 50 human admins would generate < 1 TPS average, ~60k logs/day, or ~90MB/day.

- Automated/Script Device Admin Example:
  - Consider a script that runs 4 times a day against 30,000 devices, (for example, to backup config on all devices). Generally the interaction will be short, say 5 commands:
    - Storage = 30,000 * 4 * [5kB + (5 * 3kB)] = ~2.4 GB/day
    - Total TPS = 30k * 4 * [3 + (5 * 2)] = 1.56M logs = 18 TPS average; 1300 TPS peak.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Multi-Service Scaling

For Your Reference

Required TACACS+ TPS by # Admins and # NADs

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

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

TACACS+ Multi-Service Scaling

For Your Reference

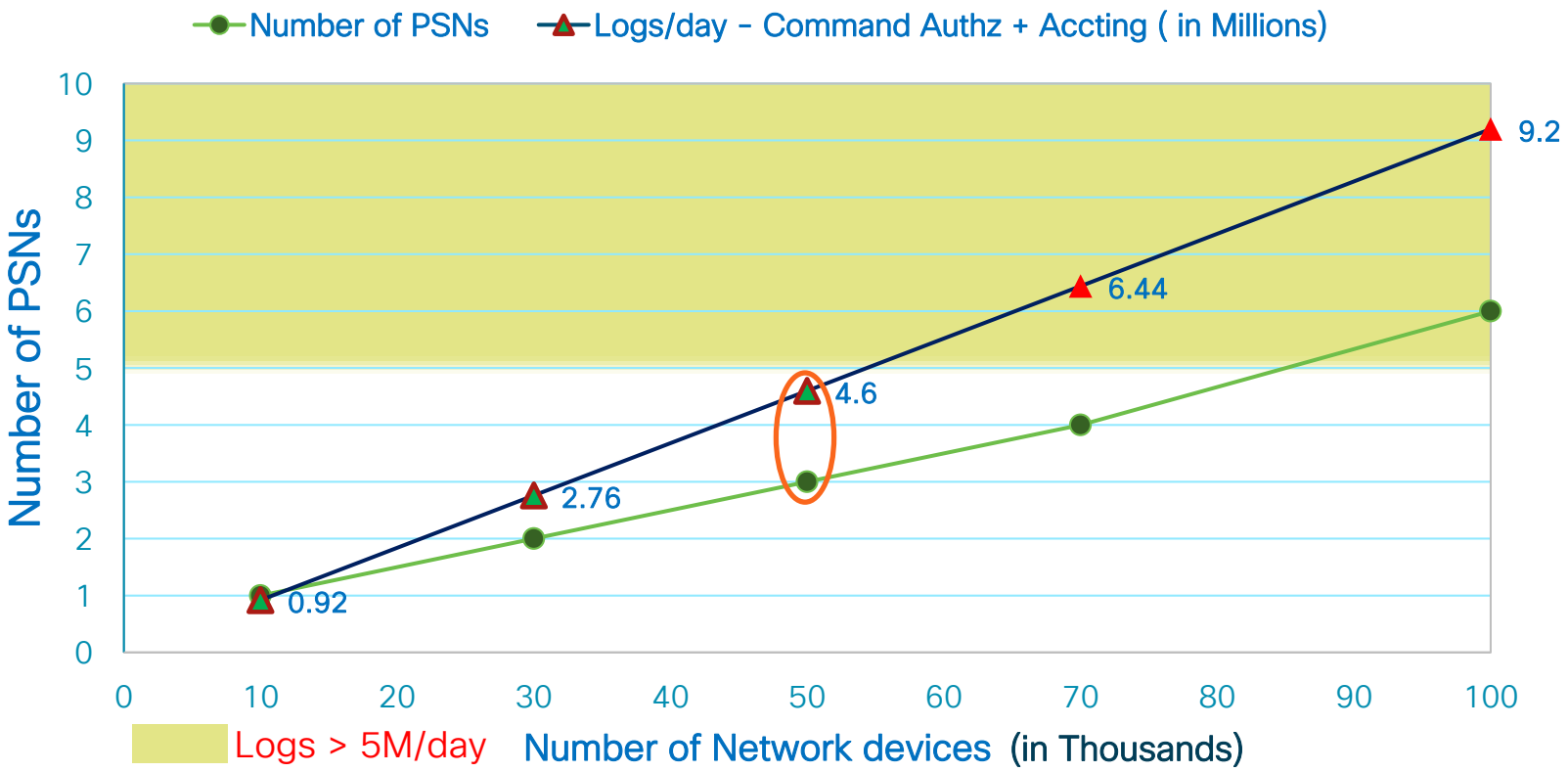
Required TACACS+ TPS by # Admins and # NADs

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

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

Scaling PSNs vs Logs per day

For Your Reference

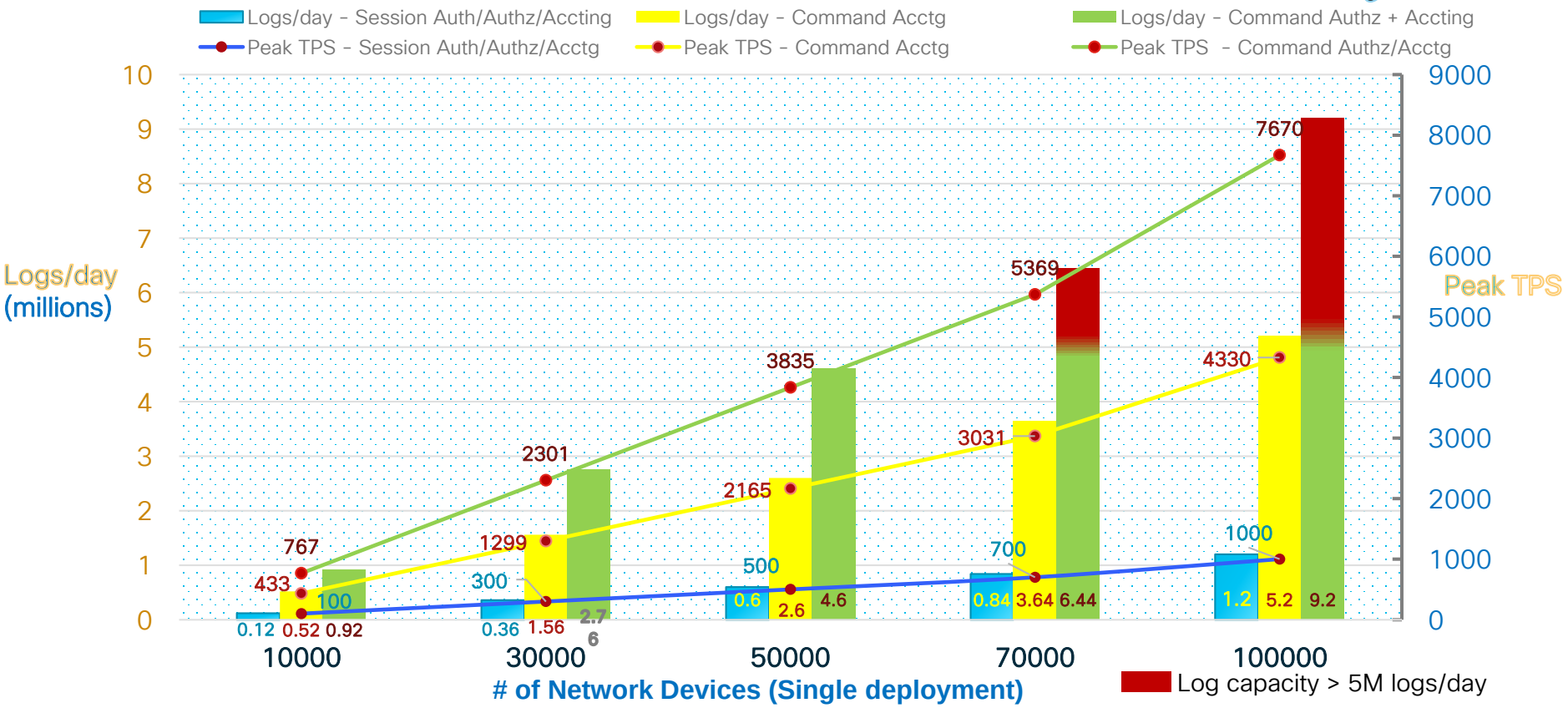


Note: Based on 4 TACACS+ sessions/day across Network Devices and 10 Commands/Session

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Logs/Day vs Peak TPS

For Your Reference



Note: Based on 4 TACACS+ sessions/day across Network devices and 10 commands/session

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Node Log Storage Requirements for TACACS+

Days Retention Based on # Managed Network Devices and Disk Size

For Your Reference

Total Disk Space Allocated to MnT Node

Total NADs	200 GB	400 GB	600 GB	1024 GB	2048 GB	2400GB
100	12,583	25,166	37,749	64,425	128,850	154,016
500	2,517	5,034	7,550	12,885	25,770	30,804
1,000	1,259	2,517	3,775	6,443	12,885	15,402
5,000	252	504	755	1,289	2,577	3081
10,000	126	252	378	645	1,289	1541
25,000	51	101	151	258	516	617
50,000	26	51	76	129	258	309
75,000	17	34	51	86	172	206
100,000	13	26	38	65	129	155

Assumptions:

- Script runs against all NADs
- 4 sessions/day
- 5 commands/ session

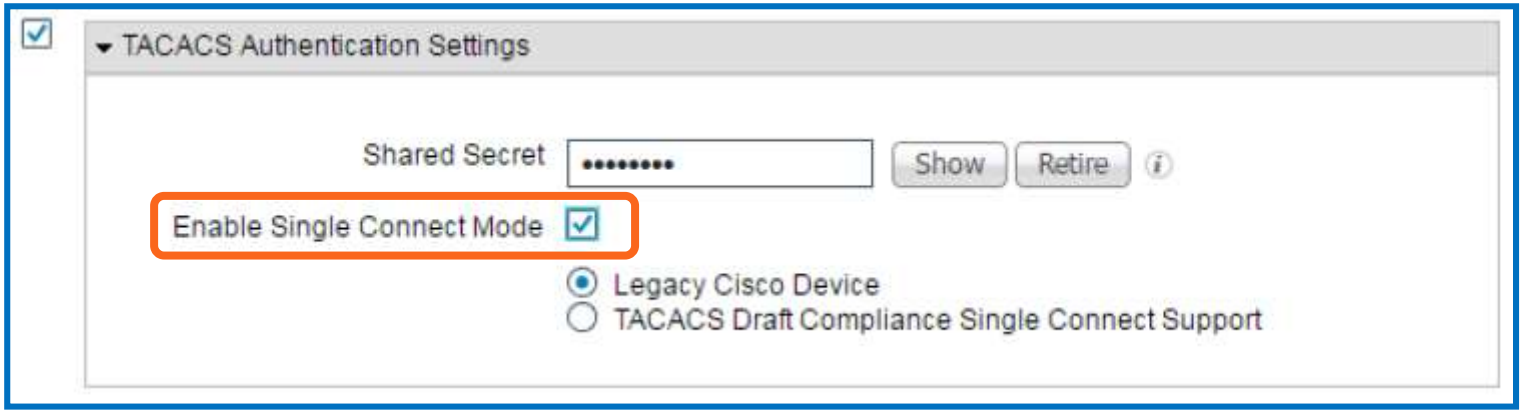
Based on 60% allocation of MnT disk to TACACS+ logging

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Connect Mode

Scaling TACACS+ for High-Volume NADs

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



Administration > Network Resources > Network Devices > (NAD)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Internal User Cache for T+ Authorization

New in ISE 2.3

Scaling TACACS+ for High-Volume Admin Users

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Identities | User Identity Groups | Ext Id Sources | Network Resources | Policy Elements | Device Admin Policy Sets | Reports | Settings

Connection Settings | Password Change Control | Session Key Assignment

Protocol Session Timeout *	5	Minutes (Range 1-9999)
Connection Timeout *	10	Minutes (Range 1-9999)
Maximum Packet Size *	32768	kb (Range 4096-65536)
Single Connect Support	☑	
Username Prompt *	Username:	
Password Prompt *	Password:	
Default Shared Secret Retirement Period *	7	Days (Range 1-99)
Authorization cache timeout *	0	Minutes (Range 0-5)

Global Setting for Single Connect Mode (enabled by default)

First authorization caches

1) User Name
2) User Specific Attributes (Ex: Group ID, custom attributes)

Successive requests served from cache

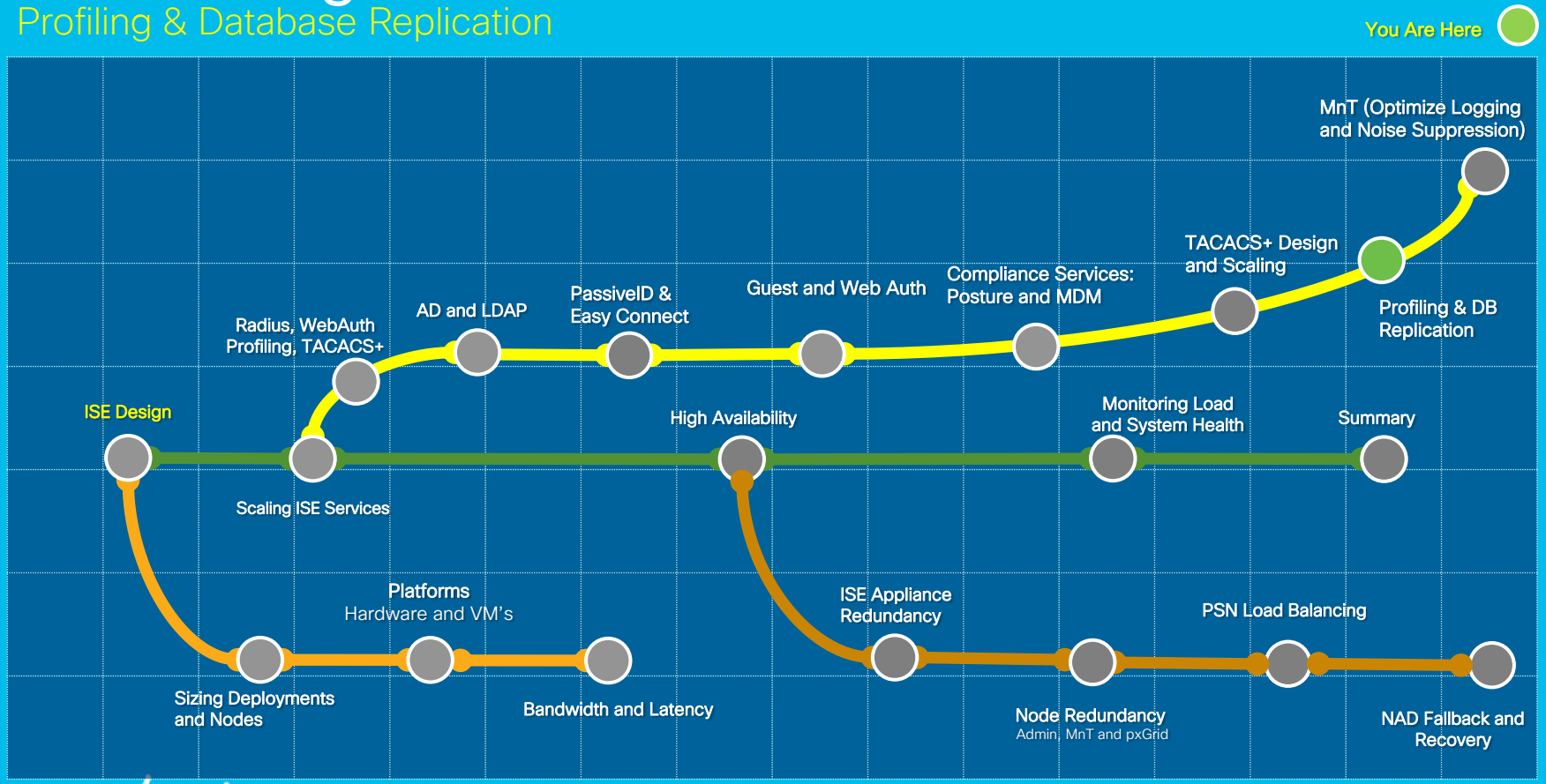
Default = 0 <<Cache Disabled>>

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Profiling and Database Replication

Session Agenda

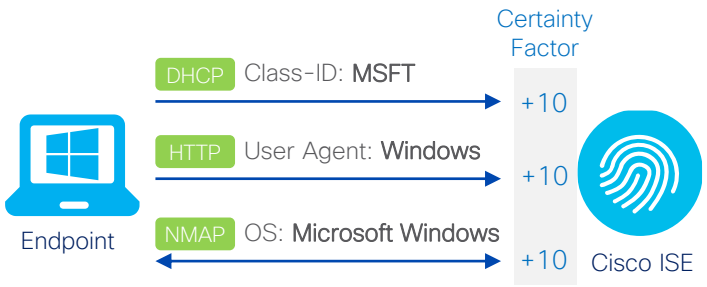
Profiling & Database Replication

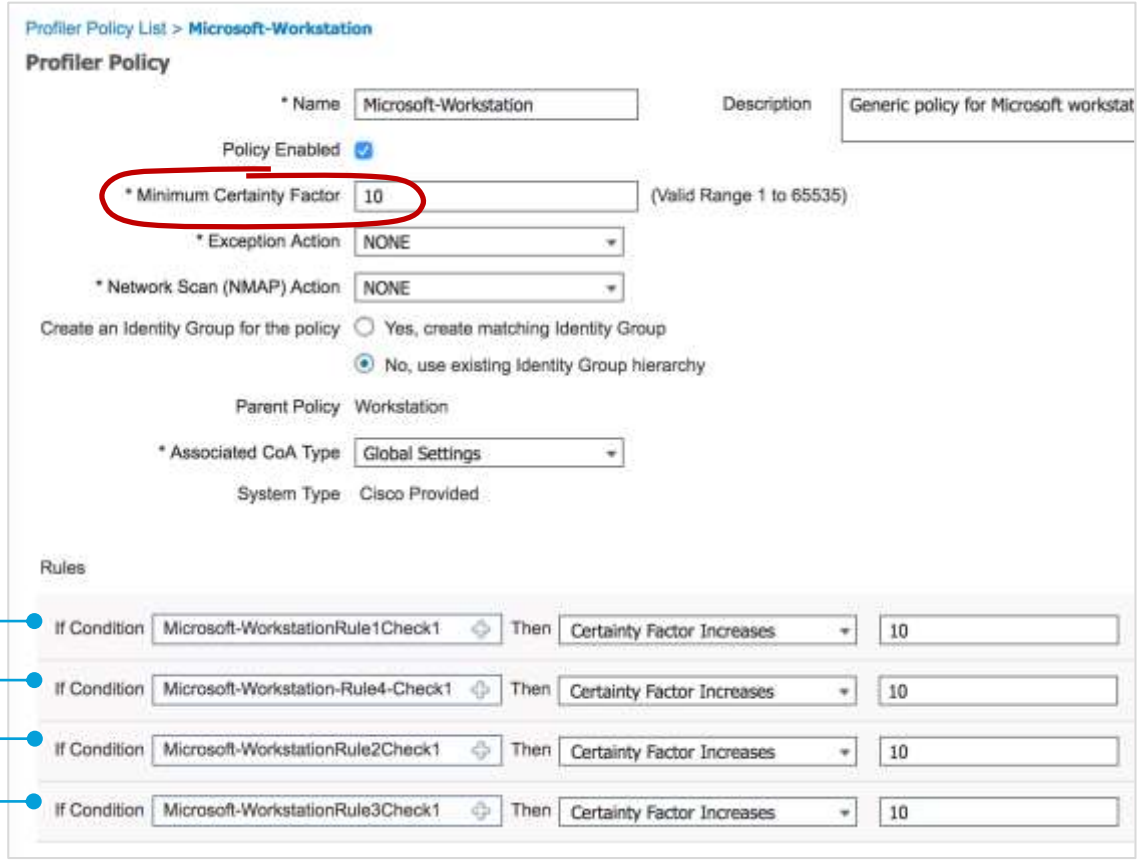


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE profiles based on ‘profiling policies’

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





DHCP:dhcp-class-identifier CONTAINS MSFT

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

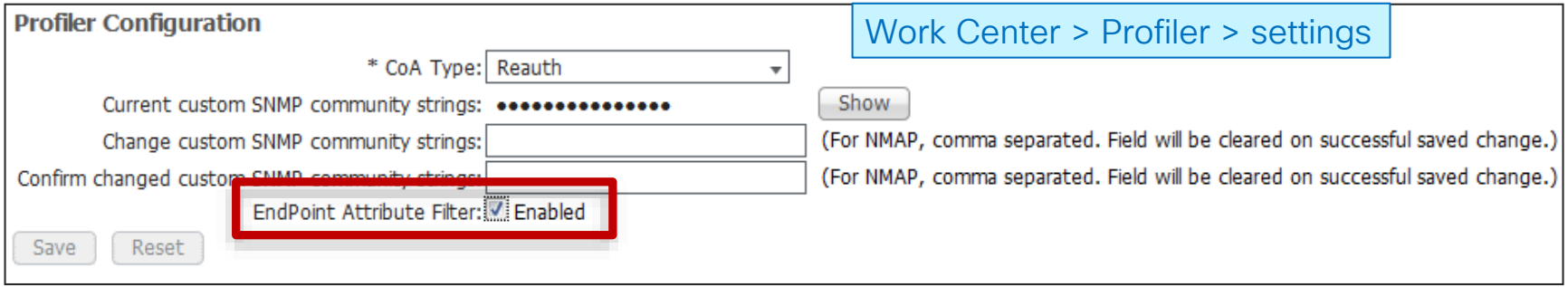
IP:User-Agent CONTAINS Windows

NMAP:operating-system CONTAINS Microsoft Windows

Endpoint Attribute Filter and Whitelist Attributes

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

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



- 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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Significant Attributes

When Does Database Replication Occur?

For Your Reference

- **Configuration Database** (Replication on Significant Attribute change)
  - Managed by Primary PAN and replicated to all Secondary Nodes
  - Stores ISE policy config, endpoint records, internal users, guest database, user certificates, etc.
  - Profiling is primary contributor to database replication
- **Local Persistence/Cache Database** (Replication on Whitelist Attribute change)
  - Locally stores endpoint profile updates.
  - Last PSN to learn new whitelisted attributes becomes endpoint owner (tracked by "EndPoint Profiler Server"
  - If another PSN receives newer attributes, it requests attribute sync from prior owner and takes ownership, then notifies other PSNs.
  - Only update PAN for Significant Attribute changes
  - PAN replicates all attributes on significant attribute change.

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Significant Attributes vs. Whitelist Attributes

For Your Reference

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

Updates Node Group

161-udp	FirstCollection	MDM
AAA-Server	FQDN	MDMProvid
AC_User_Agent	Framed-IP-Address	MDMSerialNumber
AUPAccepted	host-name	MDMServerReachable
BYODRegistration	hrDeviceDescr	MDMUpdateTime
CacheUpdateTime	IdentityGroup	NADAddress
Calling-Station-ID	IdentityGroupID	NAS-IP-Address
cdpCacheAddress	IdentityStoreGUID	NAS-Port-Id
cdpCacheCapabilities	IdentityStoreName	NAS-Port-Type
cdpCacheDeviceId	ifIndex	NmapScanCount
cdpCachePlatform	ip	NmapSubnetScanID
cdpCacheVersion	L4_DST_PORT	operating-system
Certificate Expiration Date	LastNmapScanTime	OS Version
Certificate Issue Date	lldpCacheCapabilities	OUI
Certificate Issuer Name	lldpCapabilitiesMapSupported	PhoneID
Certificate Serial Number	lldpSystemDescription	PhoneIDType
ciaddr	MACAddress	PolicyVersion
CreateTime	MatchedPolicy	PortalUser
Description	MatchedPolicyID	PostureApplicablePrevious
DestinationIPAddress	MDMCompliant	DeviceRegistrationStatus
Device Identifier	MDMCompliantFailureReason	Product
Device Name	MDMDiskEncrypted	RegistrationTimeStamp
DeviceRegistrationStatus	MDMEnrolled	StaticAssignment
dhcp-class-identifier	MDMImei	StaticGroupAssignment
dhcp-requested-address	MDMJailBroken	sysDescr
EndPointPolicy	MDMManufacturer	TimeToProfile
EndPointPolicyID	MDMModel	Total Certainty Factor
EndPointProfilerServer	MDMOSVersion	UpdateTime
EndPointSource	MDMPhoneNumber	User-Agent

Whitelist Attributes vs Significant Attributes

Sampling of All Endpoint

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

UseCase
UserType
GroupsOrAttributesProcessPol
ExternalGroups
Called-Station-ID
Calling-Station-ID
DestinationIPAddress
DestinationPort
Device IP Address
MACAddress
MessageCode
NADAddress
NAS-IP-Address
NAS-Port
NAS-Port-Id
NAS-Port-Type
NetworkDeviceName
RequestLatency
Service-Type
Timestamp
User-Name
Egress-VLANID
Egress-VLAN-Name
Airespace-Wlan-Id
Device Port
EapTunnel
Framed-IP-Address
NAS-Identifier
RadiusPacketType
Vlan
VlanName
cafSessionAuthUserName
cafSessionAuthVlan
cafSessionAuthorizedBy
cafSessionDomain
cafSessionStatus
dot1dBasePort
dot1xAuthAuthControlledPorol
dot1xAuthAuthControlledPortStatus
dot1xAuthSessionUserName

ifDescr
client-fqdn

IPV4_IDENT

mdns_VSM_srv_identifier

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

138-udp
139-udp

Whitelist Attributes

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

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

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

Triggers Node Group Update and Ownership Change

Triggers Global Replication

Significant Attributes

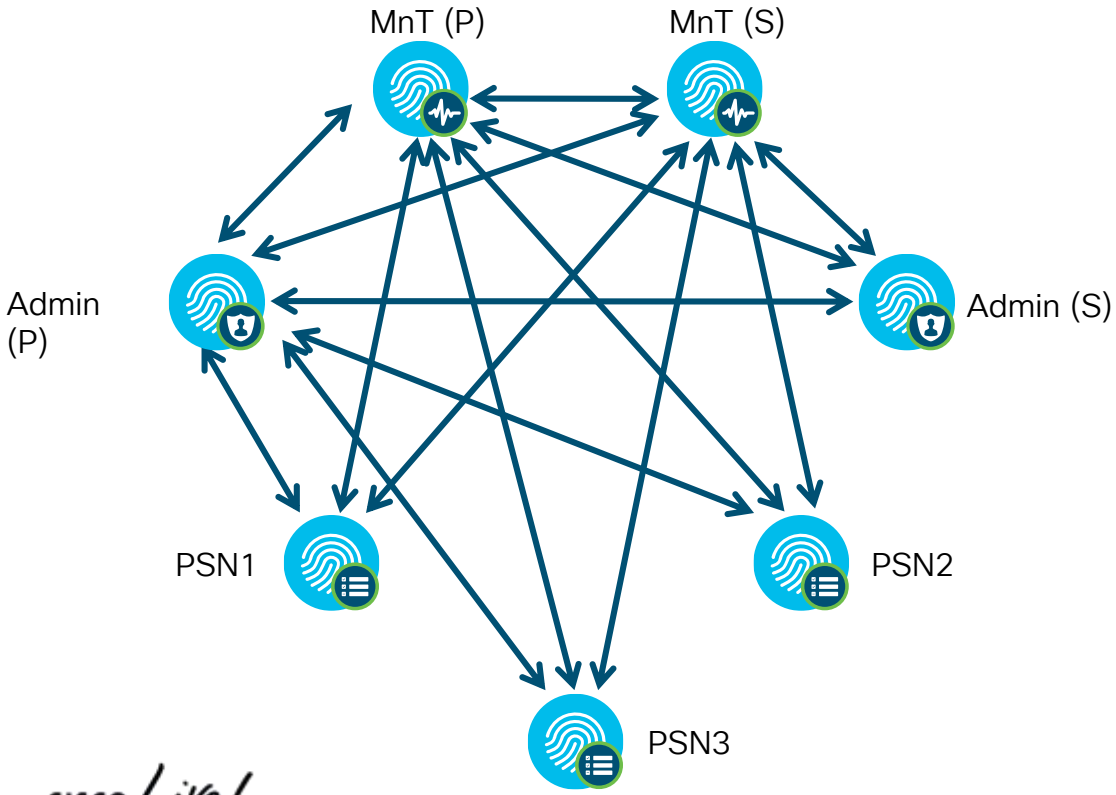
MACADDRESS
MATCHEDVALUE
ENDPOINTPOLICY
ENDPOINTPOLICYVERSION
STATICASSIGNMENT
STATICGROUPASSIGNMENT
NMAPSUBNETSCANID
PORTALUSER
DEVICEREGISTRATIONSTATUS

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Inter-Node Communications

Database Operations

For Your Reference



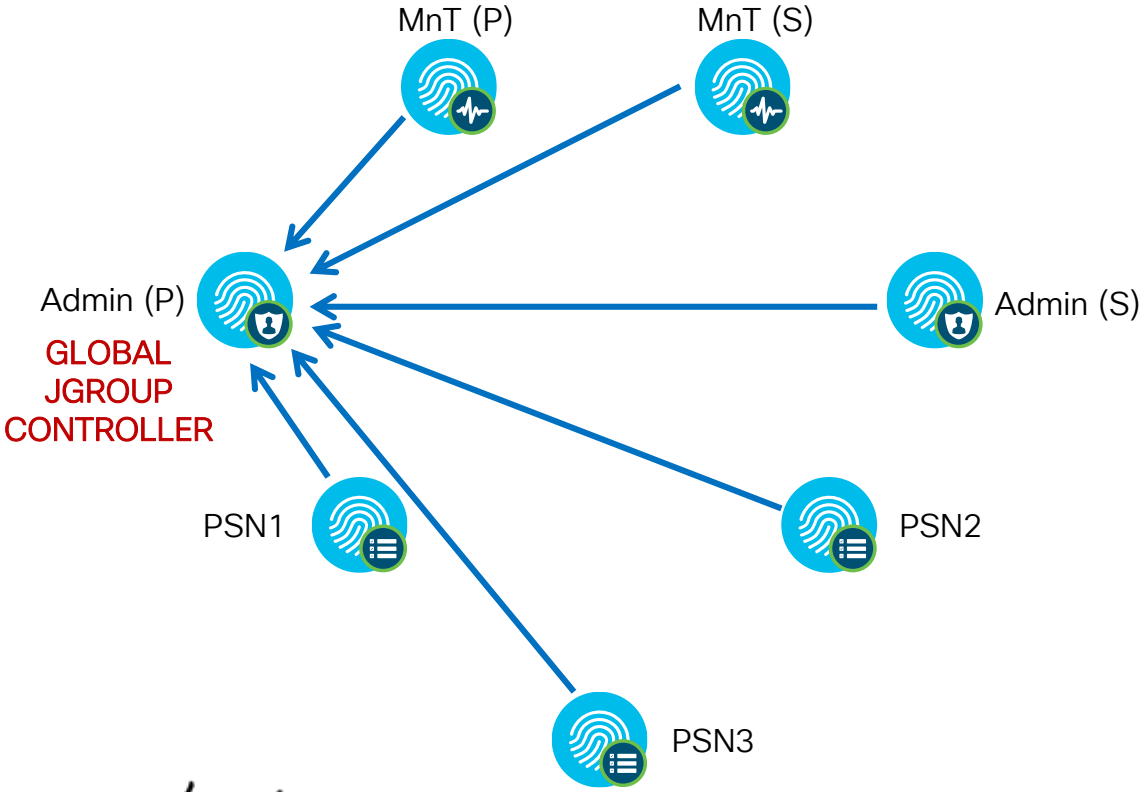
TCP/443 HTTPS (SOAP)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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, pxGrid, and Secondary Admin nodes

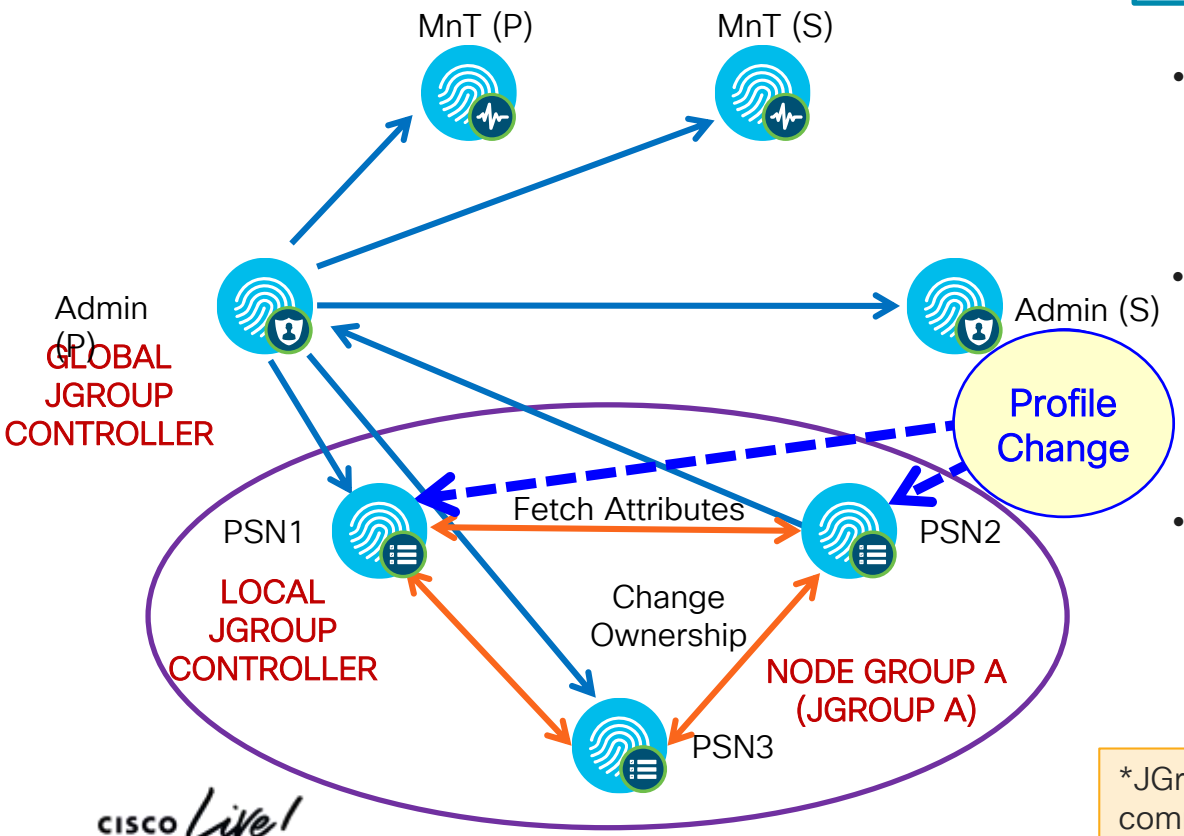
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Inter-Node Communications

Local JGroups and Node Groups

TCP/7800 JGroup Peer Communication
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 SSL (TLS v1.2).
- PSN claims endpoint ownership only if change in whitelist attribute; triggers ownership update to local PSNs. Whitelist check always occurs regardless of global whitelist filter.
- 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.

cisco Live!

Inter-Node Communications

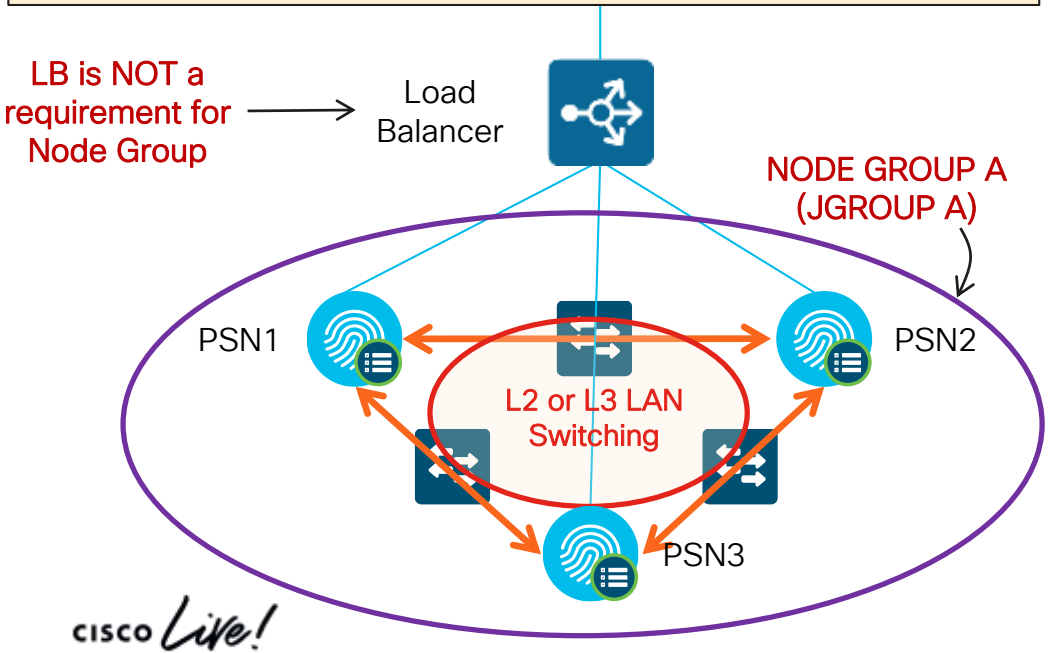
Local JGroups and Node Groups

For Your Reference

TCP/7800 JGroup Peer Communication
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**

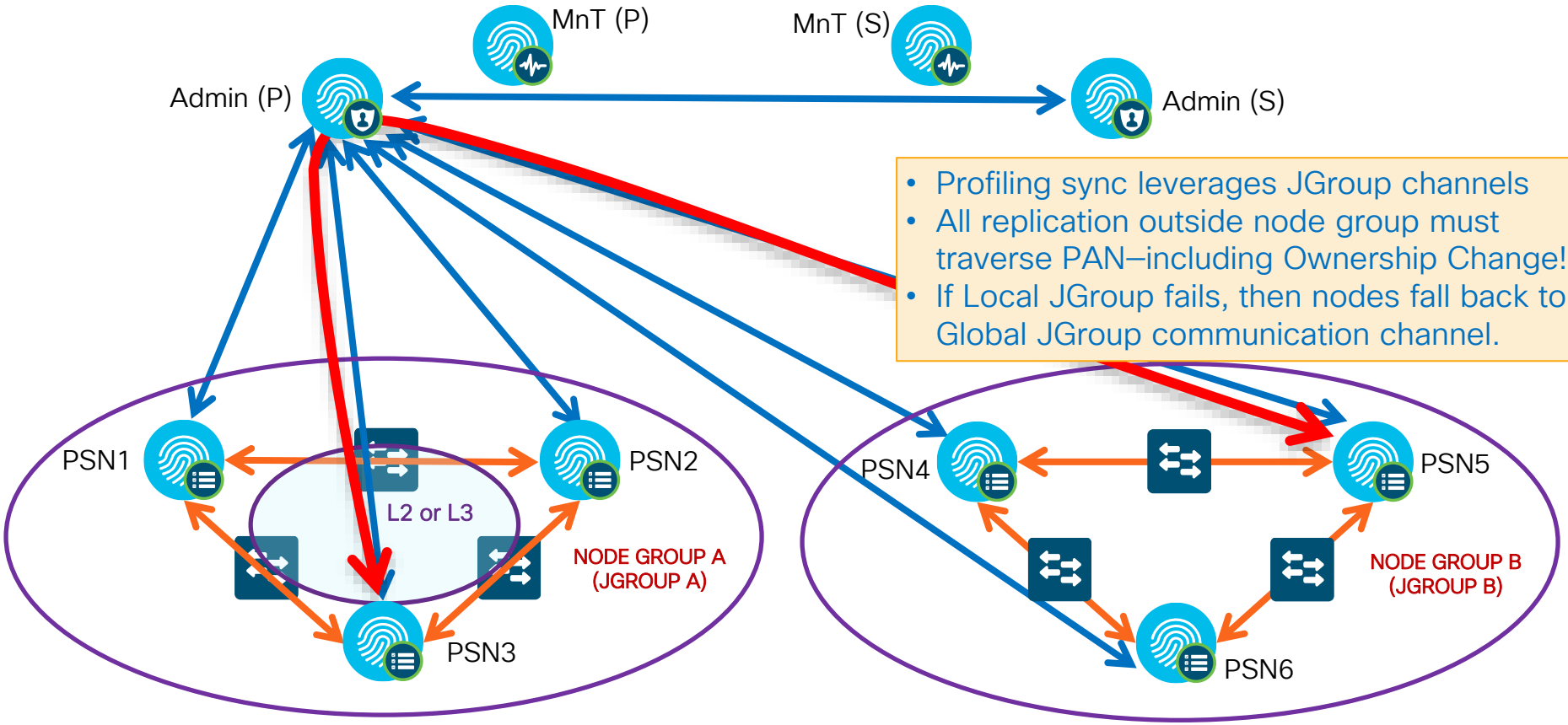


- Node groups continue to provide original function of session recovery for failed PSN.
- Profiling sync leverages JGroup channel
- Each LB cluster should be a node group, but LB is NOT required for node groups.
- Node group members should have GE LAN connectivity (L2 or L3)
  - ISE 2.0+ uses TLSv1.2
- Reduces sync updates even if different PSNs receive data – expect few whitelist changes and even fewer critical attribute changes.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Inter-Node Communications pre 2.7

Local JGroups and Node Groups



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

For Your Reference

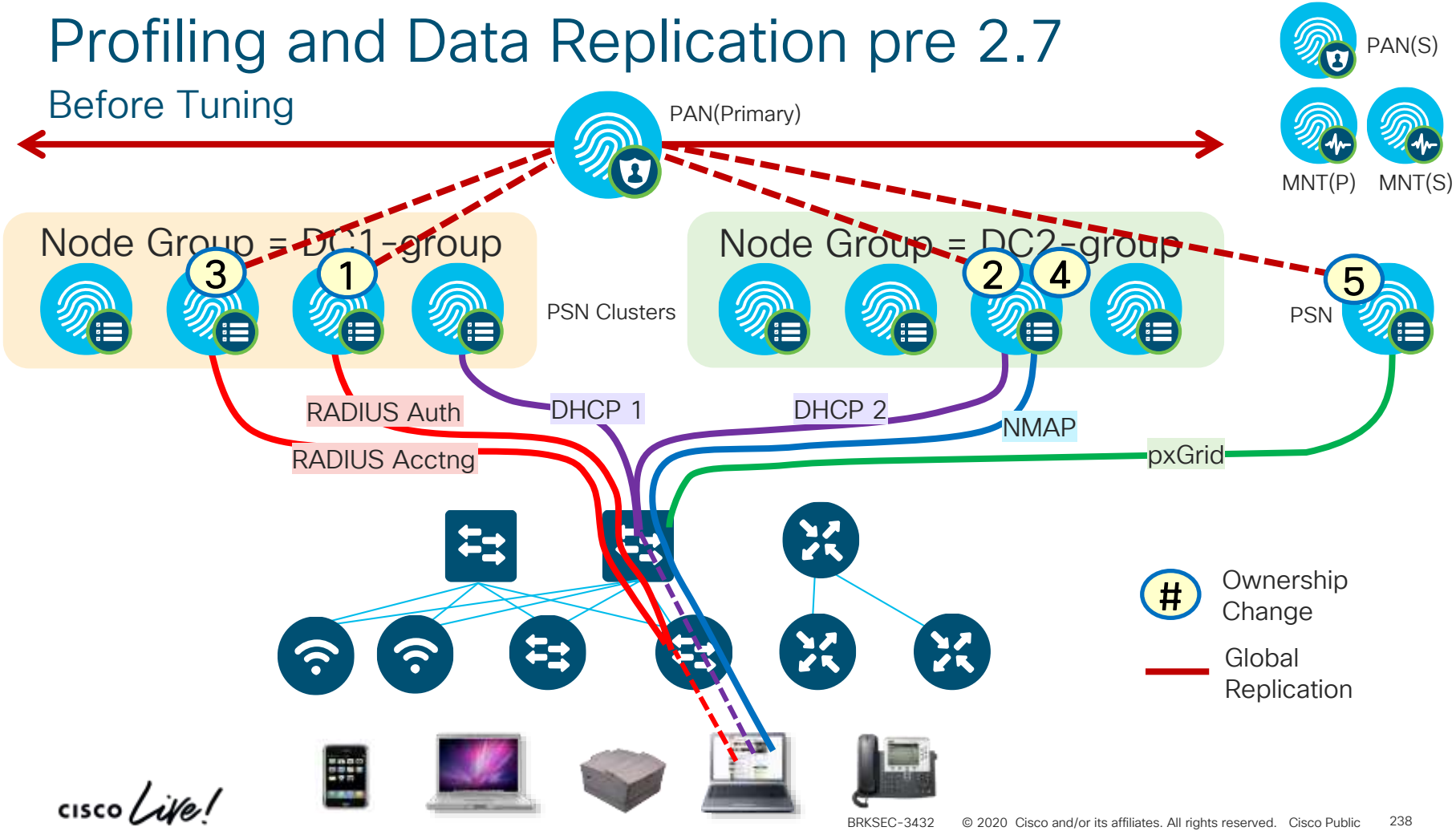
AD Connector Ports

Protocol	Port	Authenticated	Notes
DNS (TCP/UDP)	53	No	May use DNSSEC
MSRPC (TCP)	445	Yes	
Kerberos (TCP/UDP)	88	Yes (Kerberos)	MS AD/KDC
Kpasswd	464	No	
LDAP (TCP/UDP)	389	Yes. Encrypted & Authenticated with SASL, not LDAP/S	Just like native MS Domain Member
Global Catalog (TCP)	3268	Yes. Encrypted & Authenticated with SASL, not LDAP/S	Just like native MS Domain Member
NTP	123	No	
IPC	80	Yes, using creds from RBAC system.	ISE REST Library

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling and Data Replication pre 2.7

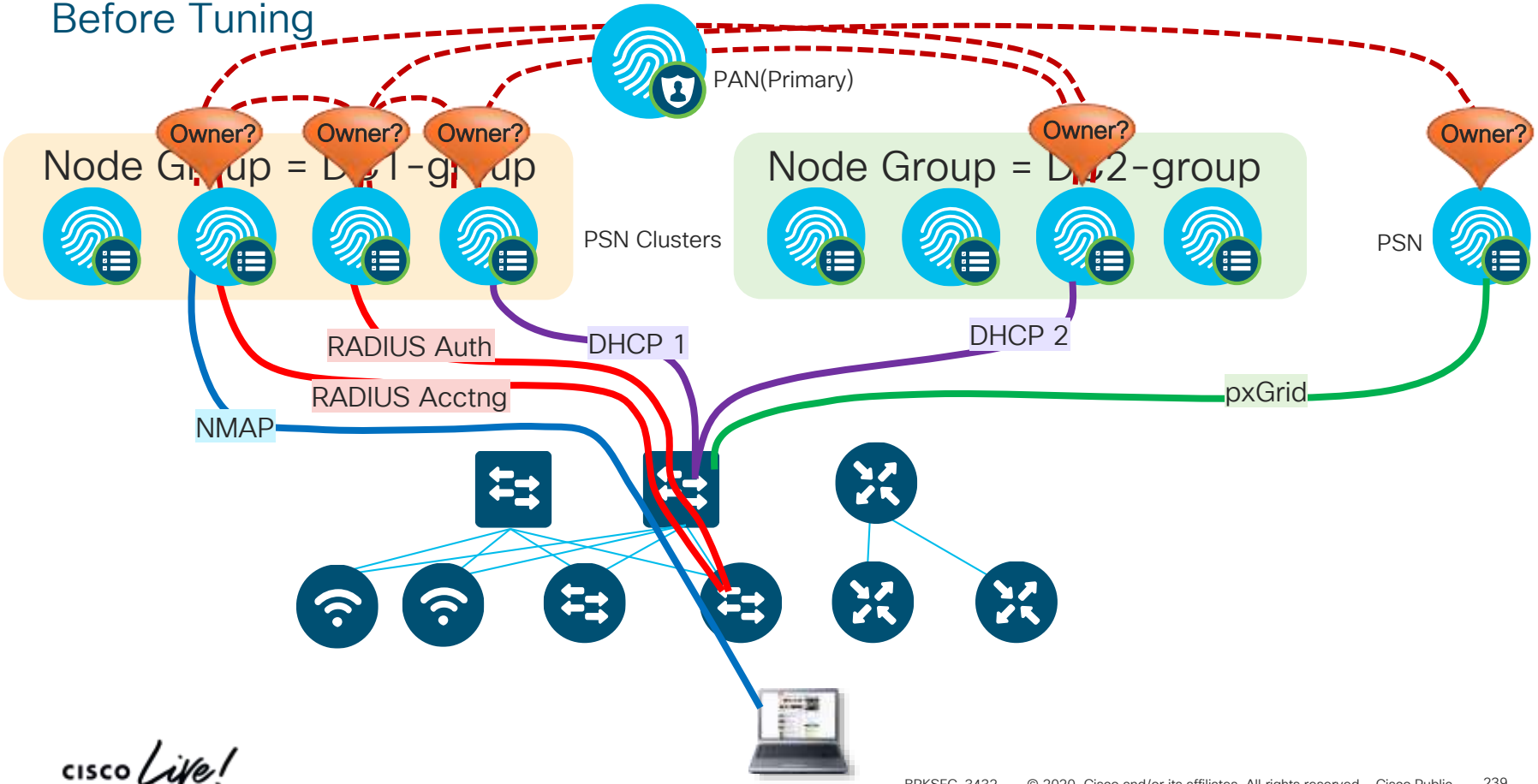
Before Tuning



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Impact of Ownership Changes pre 2.7

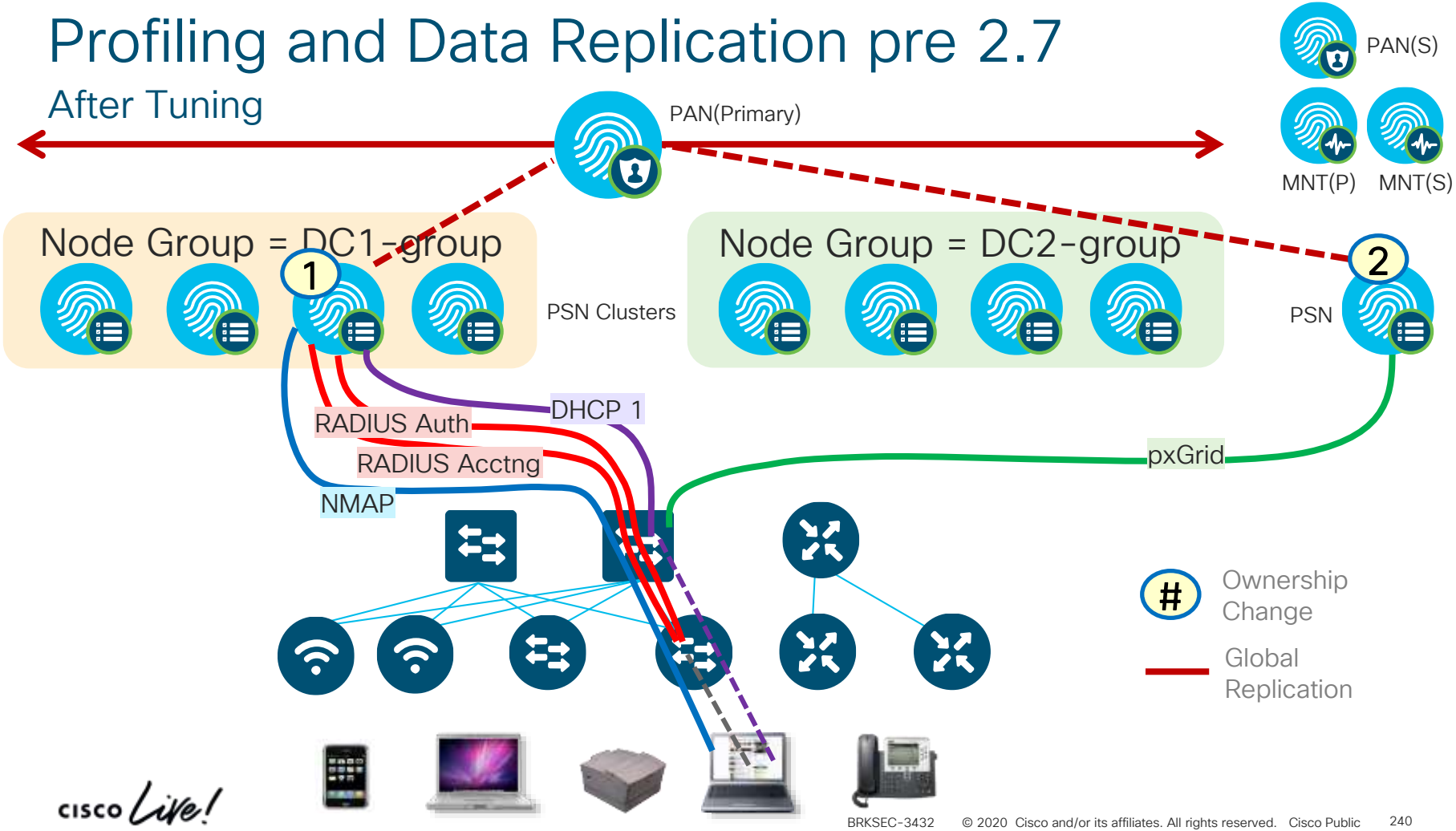
Before Tuning



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling and Data Replication pre 2.7

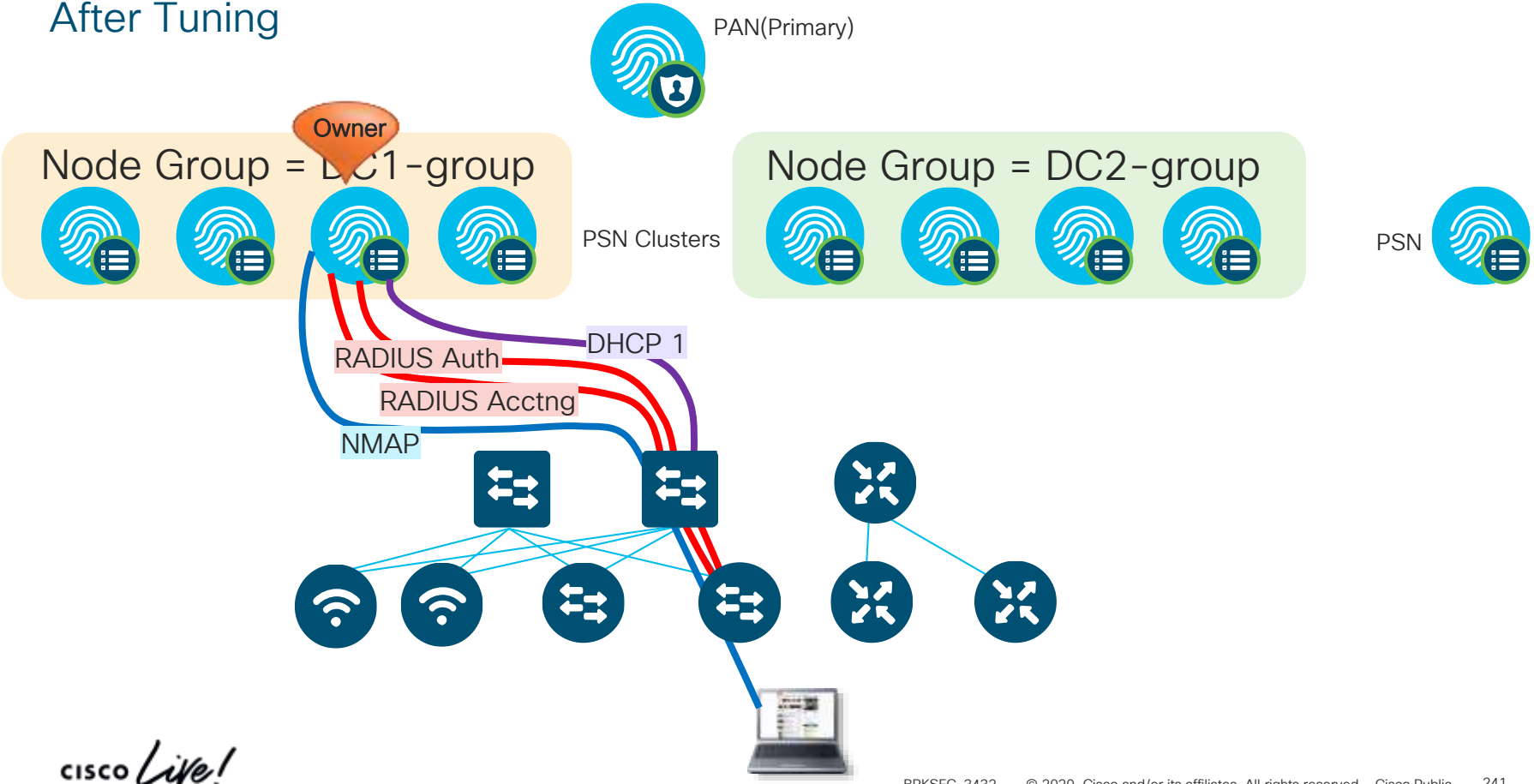
After Tuning



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Impact of Ownership Changes pre 2.7

After Tuning



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reliable Profiling Services
End Point Ownership Changes 2.7

Before

Endpoint Ownership

Multiple PSNs that received probe response would compete for endpoint ownerhsip leading to issues with CoA.

Static Endpoints

Endpoints classified statically would get reclassified if profiling probes are received.

Feed Download

Can't get only OUI updates via profiler feed download. Full package would disrupt custom profiling policies.

After

Endpoint Ownership

PSNs wont flap ownership of endpoints, except for new authentication.

Static Endpoints

Endpoints classified statically wont be reclassified unless the static mapping is removed.

Feed Download

New OUI only package available for download and update of existing policies

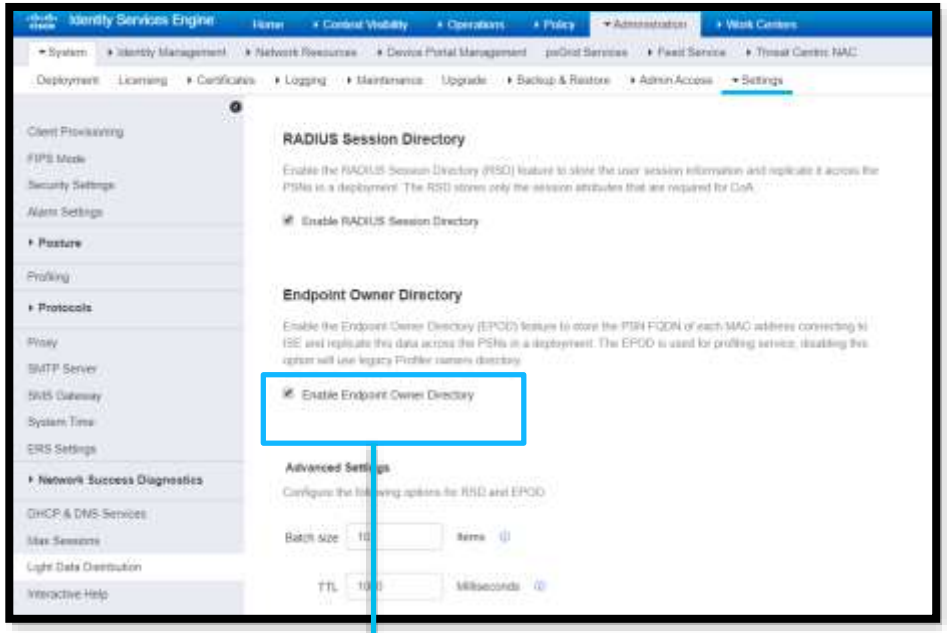
With EPO/LDD feature enabled, endpoint ownership will not change frequently.

Ownership changes only in the below scenarios :

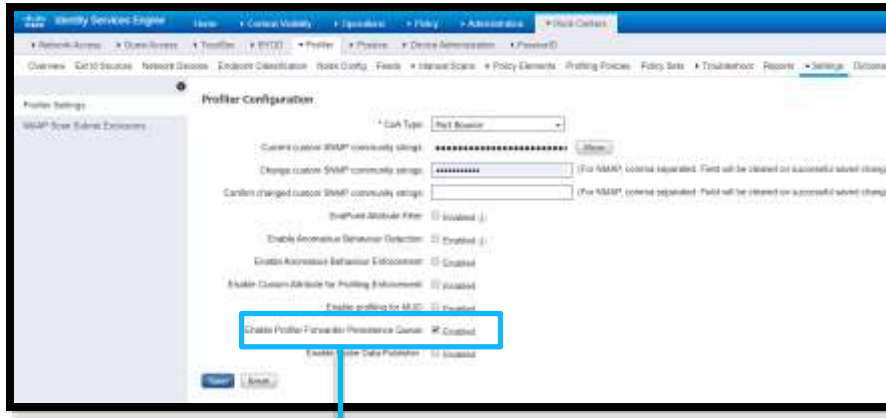
- When there is a successful auth for an endpoint or when the node is down
- When we import endpoints or create in GUI and later endpoint is read by another probe (DHCP).

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enable Endpoint Ownership – 2.7



Enabled by default



RMQ enabling page

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Profiling Best Practices

Whenever Possible…

- Use Device Sensor on Cisco switches & Wireless Controllers to optimize 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 Group Replication-PSN communication required 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 !

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Profiling Best Practices

For Your Reference

Whenever Possible…

- **Use Device Sensor** on Cisco switches & Wireless Controllers to optimize 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**

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Profiling Best Practices

General Guidelines for Probes

- HTTP Probe:
  - Use URL Redirects instead of SPAN to centralize 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 on the probe relays and not the defaults, ISE will not relay DHCP for same!
  - Avoid DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server. HA challenges.
- SNMP Probe:
  - For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
  - SNMP Traps primarily useful for non-RADIUS deployments like NAC Appliance—Avoid SNMP Traps w/RADIUS auth.
- NetFlow Probe:
  - Use only for specific use cases in centralized deployments—Potential for high load on network devices and ISE.
- pxGrid Probe:
  - Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy.
  - Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

Do NOT enable all probes by default !

Avoid SPAN, SNMP Traps, and NetFlow probes !

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Profiling Best Practices

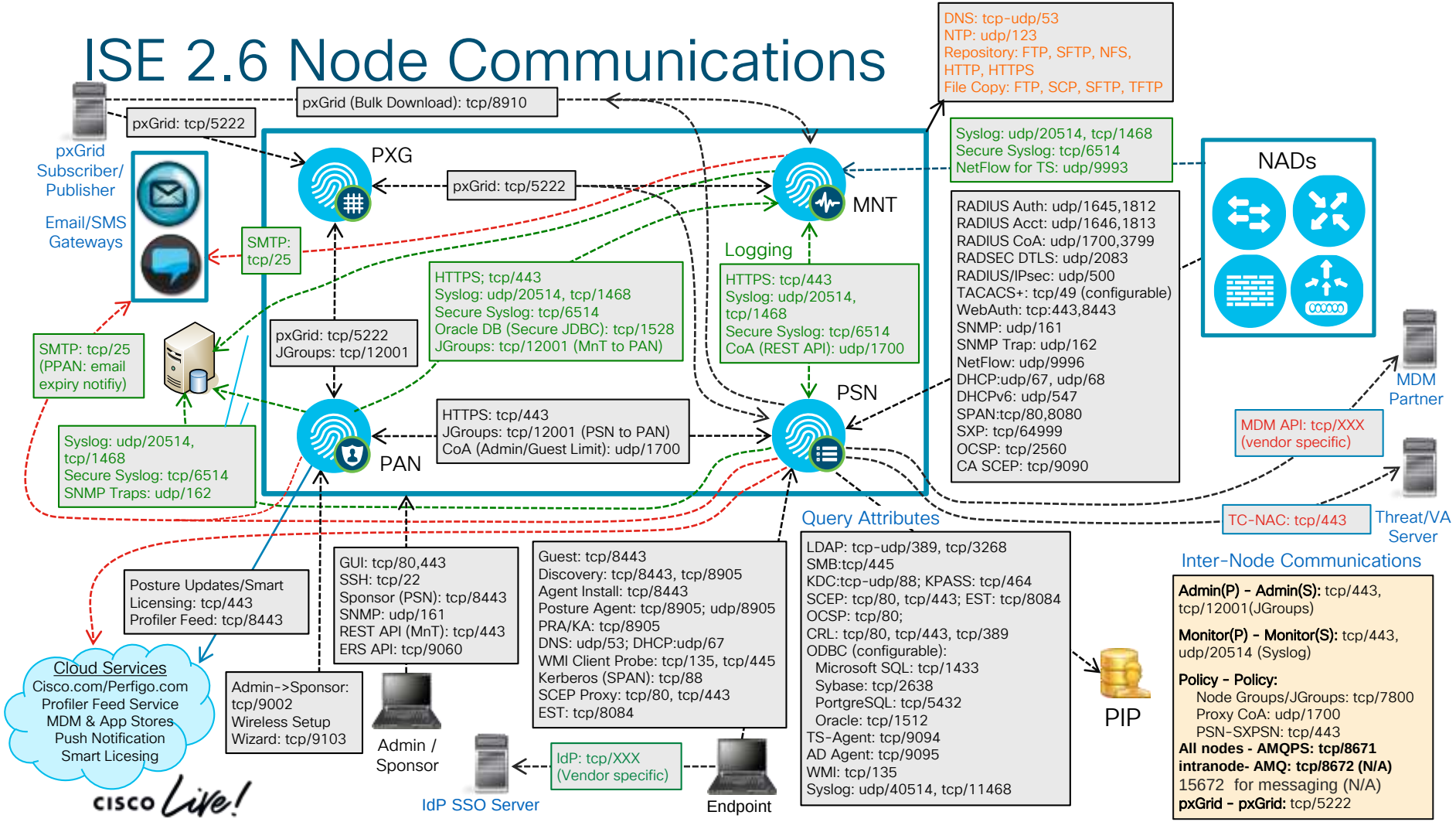
For Your Reference

General Guidelines for Probes

- **HTTP Probe:**
  - Use URL Redirects instead of SPAN to centralize 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.
- **SNMP Probe:**
  - For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
  - SNMP Traps primarily useful for non-RADIUS deployments like NAC Appliance—Avoid SNMP Traps w/RADIUS auth.
- **NetFlow Probe:**
  - Use only for specific use cases in centralized deployments—Potential for high load on network devices and ISE.
- **pxGrid Probe**
  - Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy.
  - Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

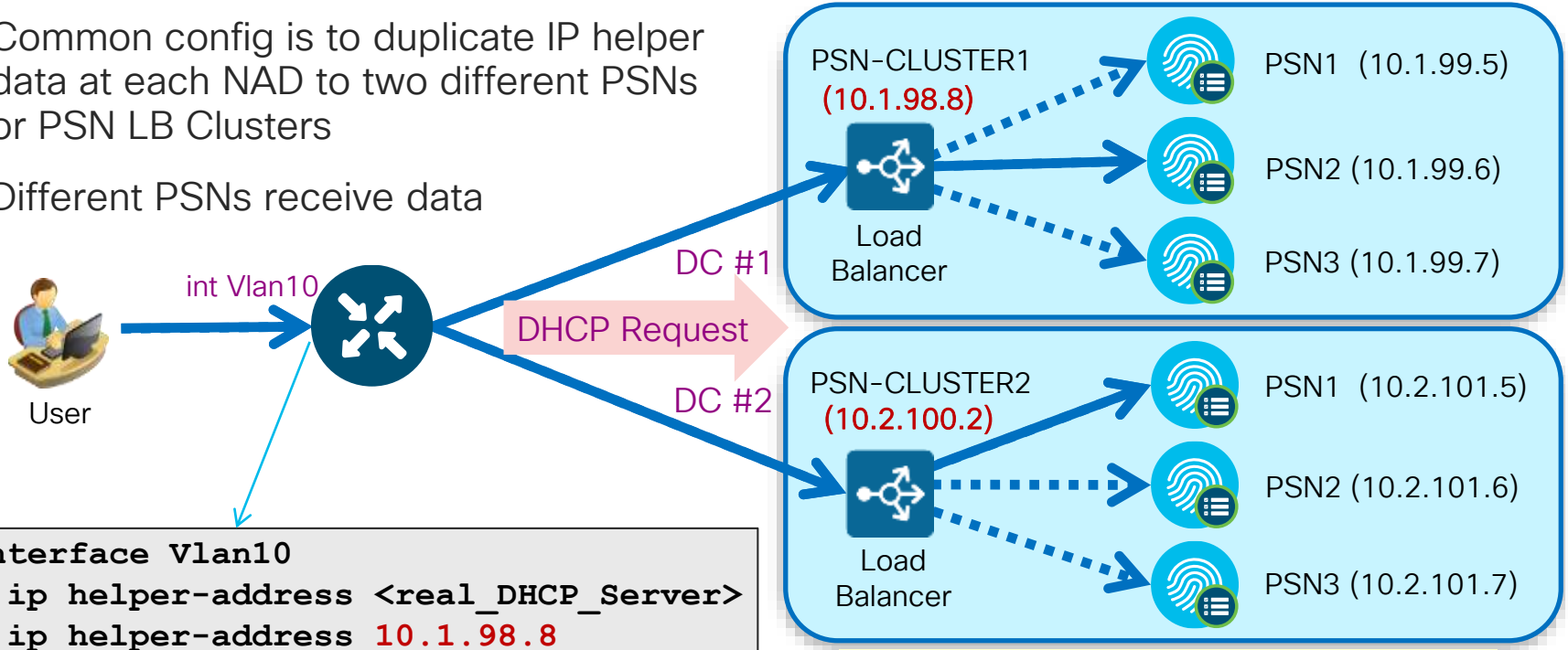
ISE 2.6 Node Communications



Profiling Redundancy – Duplicating Profile Data

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

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




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

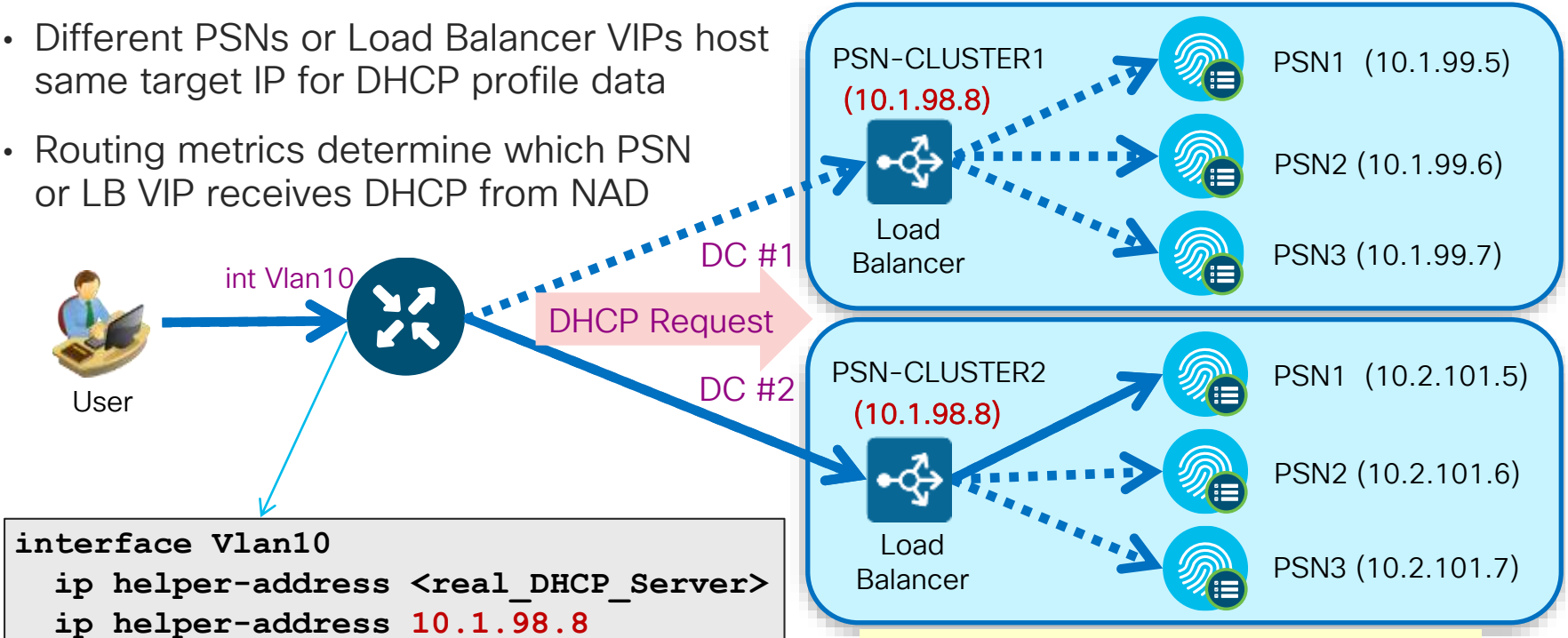
Note: LB depicted, but NOT required

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Profiling and Replication

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

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



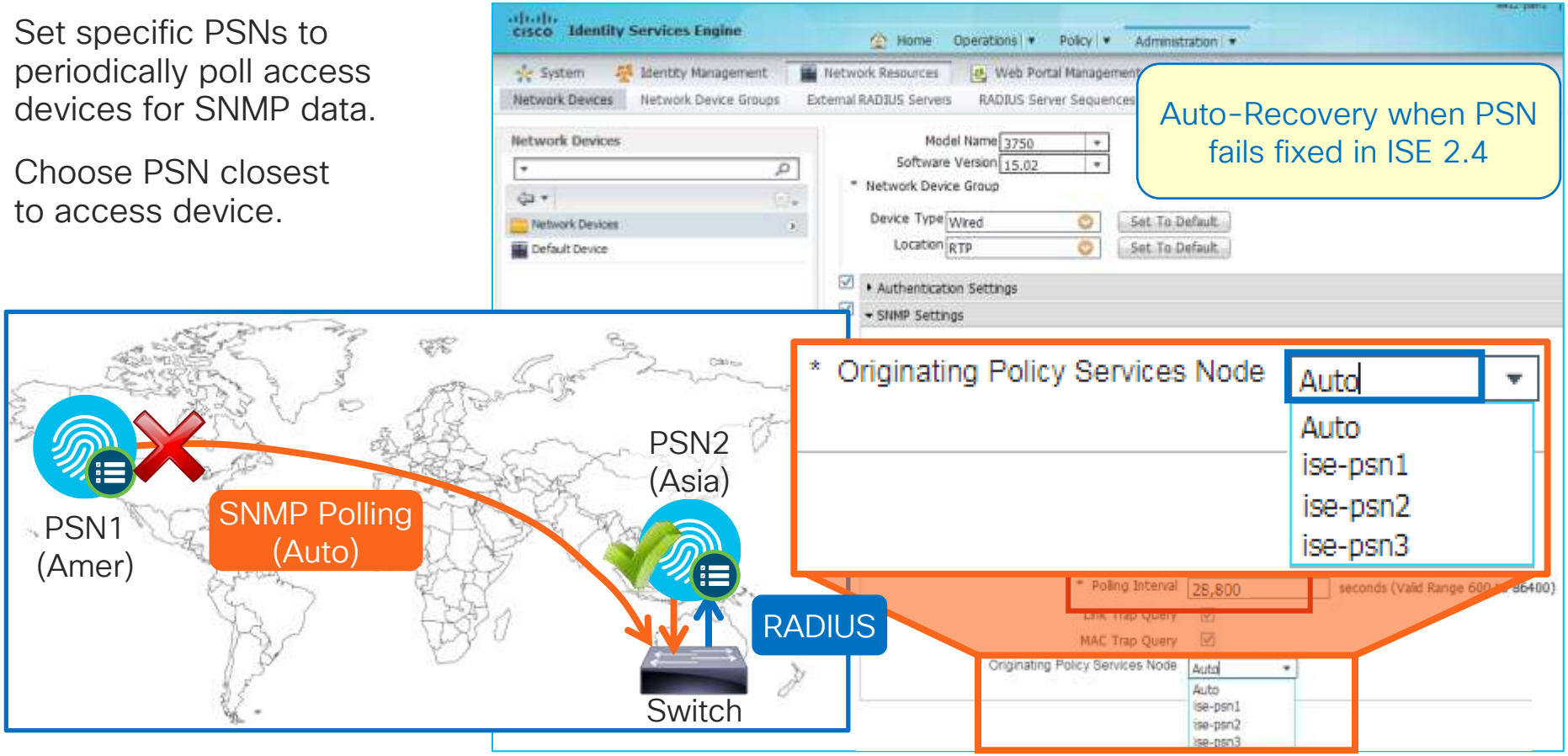

```
interface Vlan10
  ip helper-address <real_DHCP_Server>
  ip helper-address 10.1.98.8
```

Note: LB depicted, but NOT required

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiler Tuning for Polled SNMP Query Probe

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



Profiler Tuning for Polled SNMP Query Probe

For Your Reference

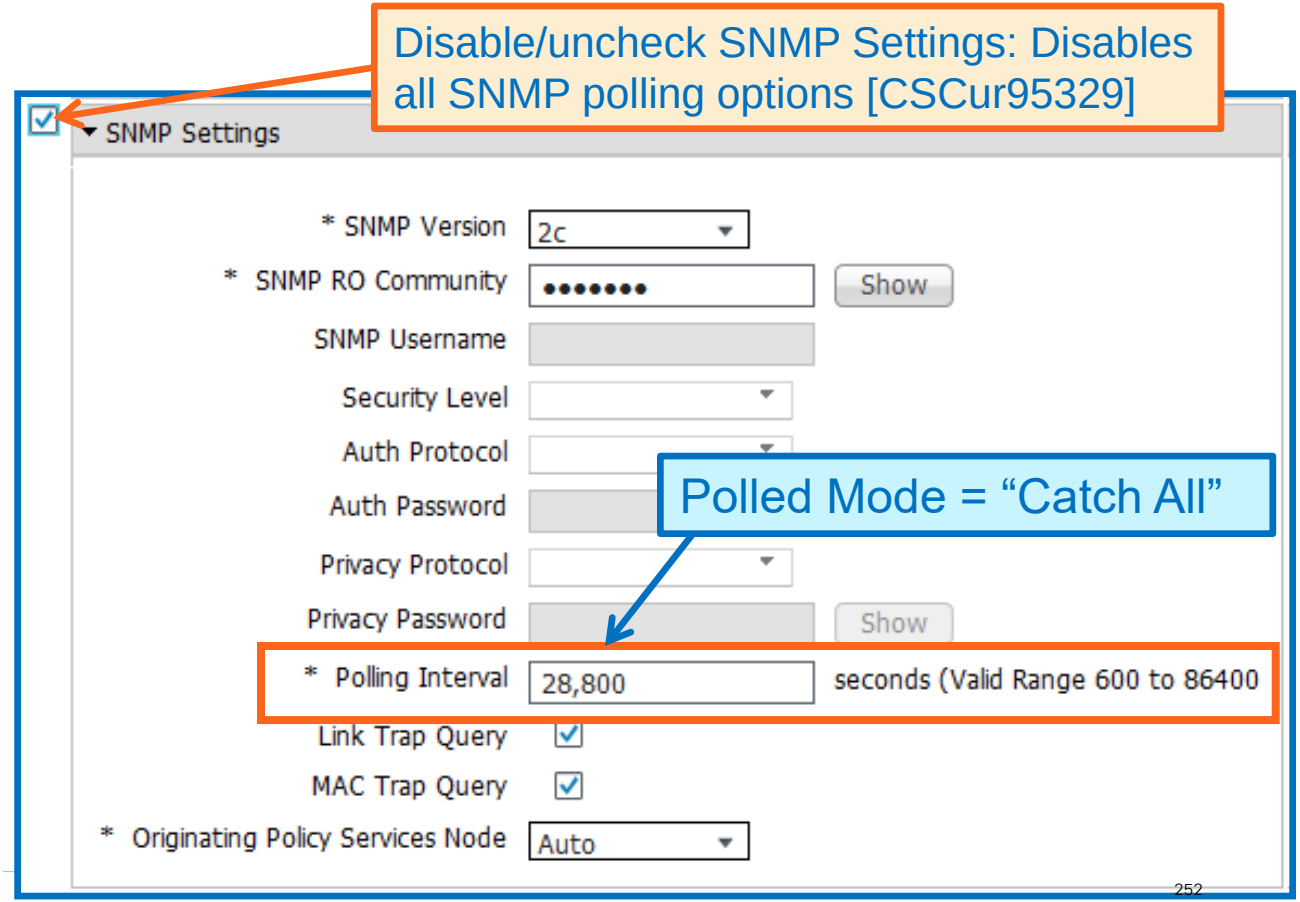
- Polling Interval

  1.2 Default: 3600 sec (1 hour)

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

- Setting of "0": Disables periodic poll but allows triggered & NMAP queries [CSCur95329]

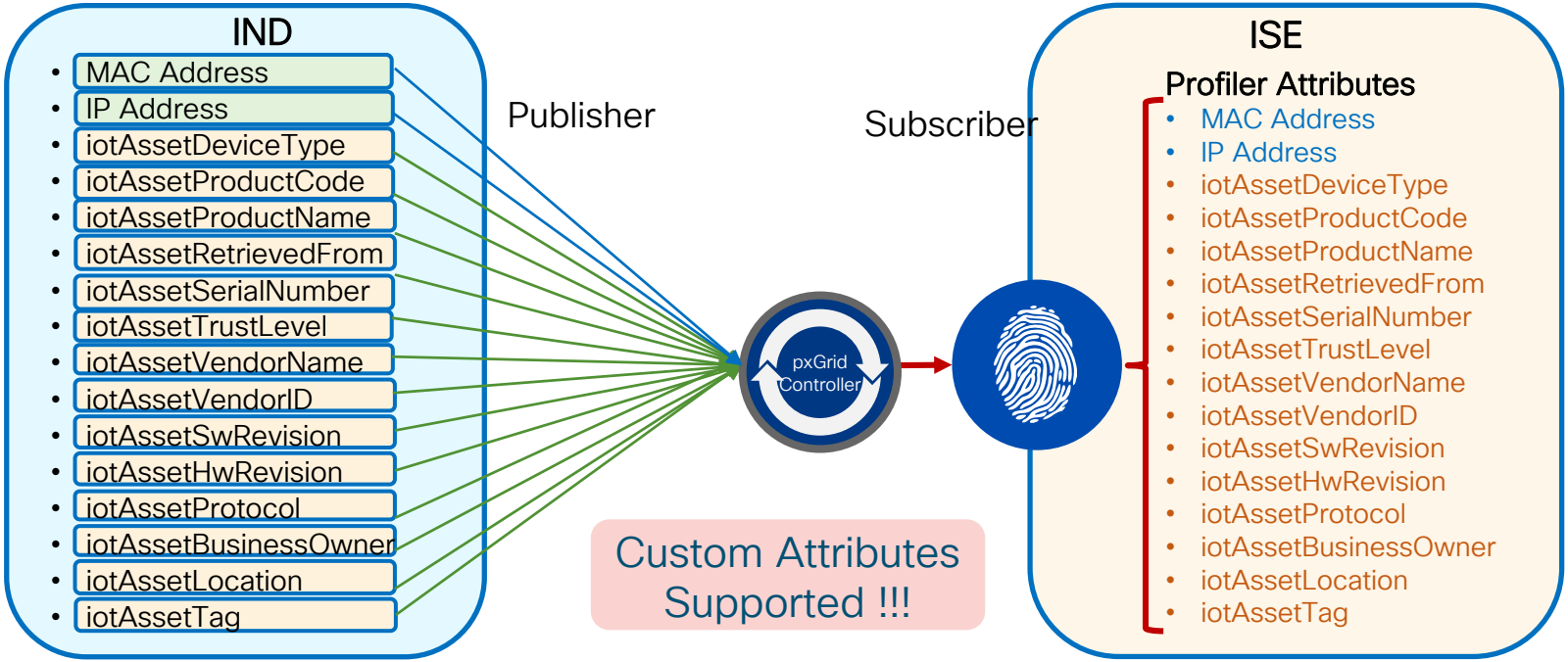
- Triggered SNMP query auto-suppressed for 24 hrs per endpoint



pxGrid Profiler Probe (Context In)

First Integration is with Industrial Network Director (IND)

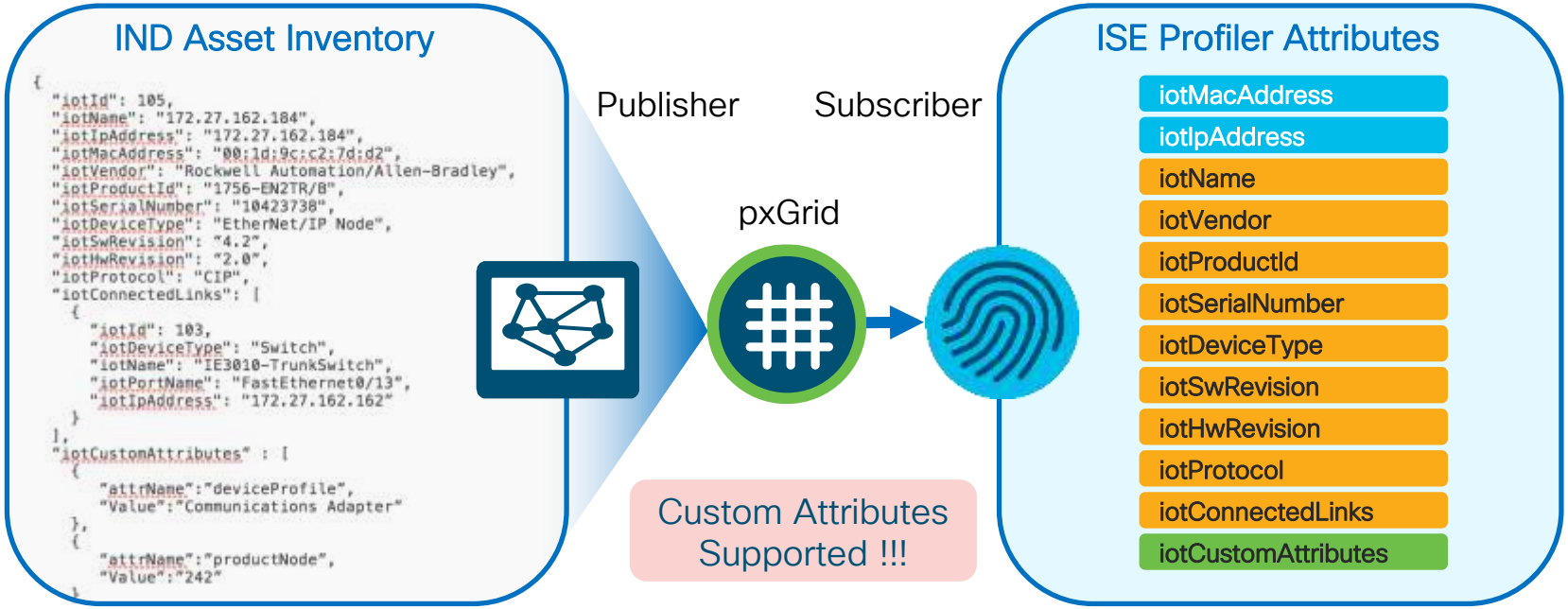
- IND communicates with Industrial Switches and Security Devices and collects detailed information about the connected manufacturing devices.
- IND vX adds pxGrid Publisher interface to communicate IoT attributes to ISE.



pxGrid Profiler Probe (Context In)

First Integration with Cisco Industrial Network Director (IND)

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



pxGrid ISE Subscription

Web Clients (pxGrid v2 Clients)

- Service name: com.cisco.endpoint.asset
- Topic: /topic/com.cisco.endpoint.asset

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

All Clients | Web Clients | Capabilities | Live Log | Settings | Certificates | Permissions

ISE as pxGrid Subscriber to Endpoint Asset topic

IND as pxGrid Publisher

For Your Reference

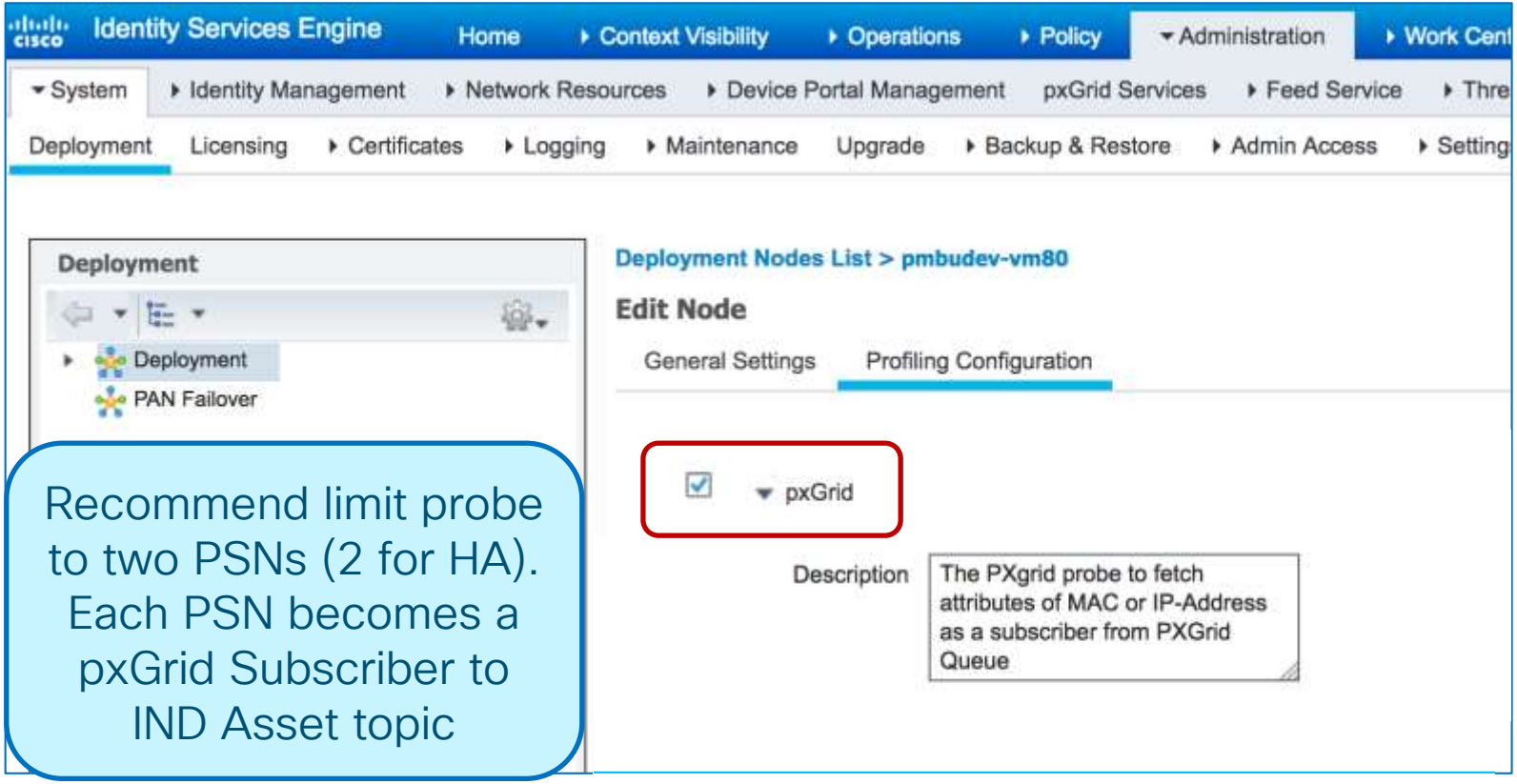
Refresh

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
Client Name						IP Address	
ise-fanout-pmbudev-v...	pmbudev-vm38	pmbudev-vm38:0	CN=pmbudev-v...	/topic/wildcard		127.0.0.1	ON
ise-admin-pmbudev-v...	pmbudev-vm38	pmbudev-vm38:1	CN=pmbudev-v...			192.168.118.108	ON
ise-fanout-pmbudev-v...	pmbudev-vm38	pmbudev-vm38:2	CN=pmbudev-v...	/topic/distributed	/topic/distributed	192.168.118.108	ON
ise-mnt-pmbudev-vm38	pmbudev-vm38	pmbudev-vm38:3	CN=pmbudev-v...	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...	192.168.118.108	ON
ise-bridge-pmbudev-v...	pmbudev-vm38	pmbudev-vm38:4	CN=pmbudev-v...			127.0.0.1	ON
cli	pmbudev-vm38	pmbudev-vm38:5	CN=test		/topic/com.cisco.endp...	0.157.140.72	ON
ise-admin-pmbudev-v...	pmbudev-vm38	pmbudev-vm38:6	CN=pmbudev-v...	/topic/com.cisco.endpoint.asset		192.168.118.108	ON

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

pxGrid Profiler Probe

For Your Reference



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

Profiler Conditions Based on Custom Attribu

New in ISE 2.4

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Dictionaries | Conditions | Results

- Library Conditions
- Smart Conditions
- Time and Date
- Profiling
- Posture
- Network Conditions

Profiler Condition List > New Profiler Condition

Profiler Condition

* Name	Custom_Attribute_Check5
* Type	CUSTOMATTRIBUTE
* Attribute Name	AssetDB_Device_Type
* Operator	STARTSWITH
* Attribute Value	CIP_PLC-5
System Type	Administrator Created

Submit | Cancel

DHCP
MAC
SNMP
IP
RADIUS
NetFlow
CDP
LLDP
NMAP
NMAPExtension
Multimedia
ACIDEX
IoTAsset
ACTIVEDIRECTORY_PROBE
CUSTOMATTRIBUTE

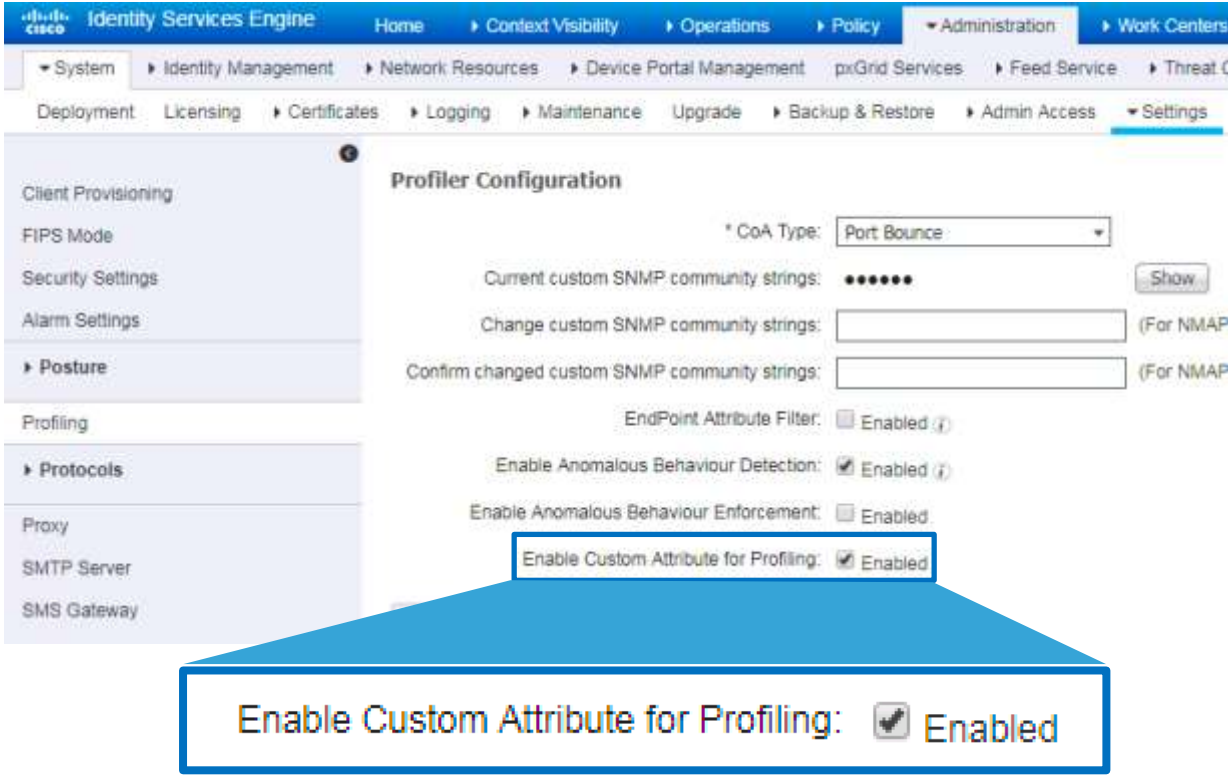
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling Based on Custom Attributes

Performance Hit if too many attibrutes, Disabled By Default

New in ISE 2.4

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 – New Profile Policies by the Numbers

Delivered Via Feed Service

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

Total = 630

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

Total = 185

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 New Profiles

Hierarchy Update

For Your Reference

- Original issue: When new Printer model introduced, just gets profiled as generic device such as Xerox-Device, or HP-Device.
- With new hierarchy, when a new Xerox Phaser Printer, for example, is released, it is profiled as Xerox Phaser Printer, and later updated via Feed to specific model.
- Hierarchy repeated for other printer company products (Xerox, HP, Brother, Lexmark). Example:
  - HP Printers: HP-Device > HP-Printer > [HP-Brand-Printer] > [Specific-HP-Brand-Printer]

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Printer Profile Hierachy

New Profiles and Optimized Categories

For Your Reference

BEFORE

- Xerox-Device
  - Xerox-4127
  - Xerox-700-Digital-Color-Press
  - Xerox-Color-1000-Press
  - Xerox-Color-560
  - Xerox-ColorQube-8570dn
  - Xerox-ColorQube-8570dt
  - Xerox-ColorQube-8570dx

AFTER

- Xerox-Device
  - Xerox-Printer
    - Xerox-4127-Printer
    - Xerox-700-Digital-Color-Press
    - Xerox-AltaLink-Printer
      - Xerox-AltaLink-B8045
      - Xerox-AltaLink-B8055
      - Xerox-AltaLink-B8065
      - Xerox-AltaLink-B8075

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

New and Updated IoT Profile Libraries

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

700+ Automation and Control Profiles (1000+ inc. MedNAC)

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Profiling

- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device
  - Siemens-Industrial-Automation-EWA-Device
  - Siemens-Industrial-Device
  - Siemens-Industry-Device
  - Siemens-Low-Voltage-Device
  - Siemens-Numerical-Control-Device
  - Siemens-SIMEA-Device
  - Siemens-Sector-Industry-Device
  - Siemens-Switzerland-BT-HVP-Device
  - Siemens-Transportation-Device
- Smarthome-Device
- Scenen-Controls-Device

Profiling Policies

Edit | Add | Duplicate | Delete | Import | Export | Show

Match the following rule:

Filter | Description | Contains | Lighting | Go | Clear Filter

Profiling Policy Name	Policy Enabled	System Type	Description
Advanced-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Adva
Advatek-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Adva
BC-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for BC-Il
Beijing-E3Control-Technology-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy
Creative-Lighting-Sound-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Creat
Cree-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Cree
Darfon-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Darfo
Digital-Lighting-Systems-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy
ELC-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment)
Electronic-Theatre-Controls-Device	Enabled	Administrator Created	Automation and Control (Home/Lighting/Entertain
GE-Consumer-Industrial-Device	Enabled	Administrator Created	Automation and Control (Building/Power/Lighting)
General-Electric-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/
German-Light-Products-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment)
Hills-Sound-Vision-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Healthcare-RTLS
Hubbell-Building-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy
Intelligent-Distributed-Controls-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/
Invisua-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Invisu
LACROIX-Traffic-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transpo
LED-Roadway-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transpo
LINT-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy
Laser-Light-Engines-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Laser
Leedarson-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Home/Lighting)
Lightino-Science-Group-Device	Enabled	Administrator Created	Automation and Control (Lighting/Healthcare-Agriculture) Policy for Lightino-Sci

Lighting

- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- Automation and Control
- Manufacturing
- Building Automation
- Home Automation
- Elevator
- Transportation
- Financial Automation
- HVAC
- Security Access Control
- Camera - A/V
- Power
- Defense
- Lighting

Automation and Control Profile Library

https://communities.cisco.com/docs/DOC-66340

For Your Reference

•

Content tagged with *ise-endpoint-profile*

OS_X-Workstation(Generic_LAN)-Policy.xml
2 months ago in Identity Services Engine (ISE)

Apple-MacBook-Air-Policy.xml
2 months ago in Identity Services Engine (ISE)

Cisco ISE Medical NAC Profile Library
3 months ago in Identity Services Engine (ISE)

Dropcam-Camera.xml
3 months ago in Identity Services Engine (ISE)

cisco Communities

Welcome, Craig Hyps | Help | Logout

Find a Community | Partners | Global | Developer | Cisco Customer Connection

Cisco Communities > Technology > Security > Policy and Access > Identity Services Engine (ISE) > Documents

ISE Endpoint Profiles

Version 7

created by Craig Hyps on Mar 14, 2016 4:38 PM, last modified by hslai on Aug 14, 2017 1:32 PM

- Get Endpoint Profiles
- How to Contribute Endpoint Profiles

Share

Tweet

We encourage Cisco ISE customers and partners to share custom ISE Endpoint Profiles that are not included with ISE or distributed via the Profiler Feed Service. In some cases, the profiles provided here may modify those provided in the shipping product or via Feed Service.

Cisco is not responsible for profiles shared to the community. As with all new profiles, it is highly recommended that they first be installed in a lab environment to verify functionality and potential impact.

Posted profiles may be unique to a specific vertical market, as in the case of the Cisco ISE Medical NAC Profile Library. In other cases, the profiles may not have been fully validated by the Cisco ISE Profiling team, but are posted "as-is" to offer a quicker method to deliver new profiles of potential interest.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why Do I Care about # Profiles?

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

  2300+ Profiles

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling Bandwidth

For Your Reference

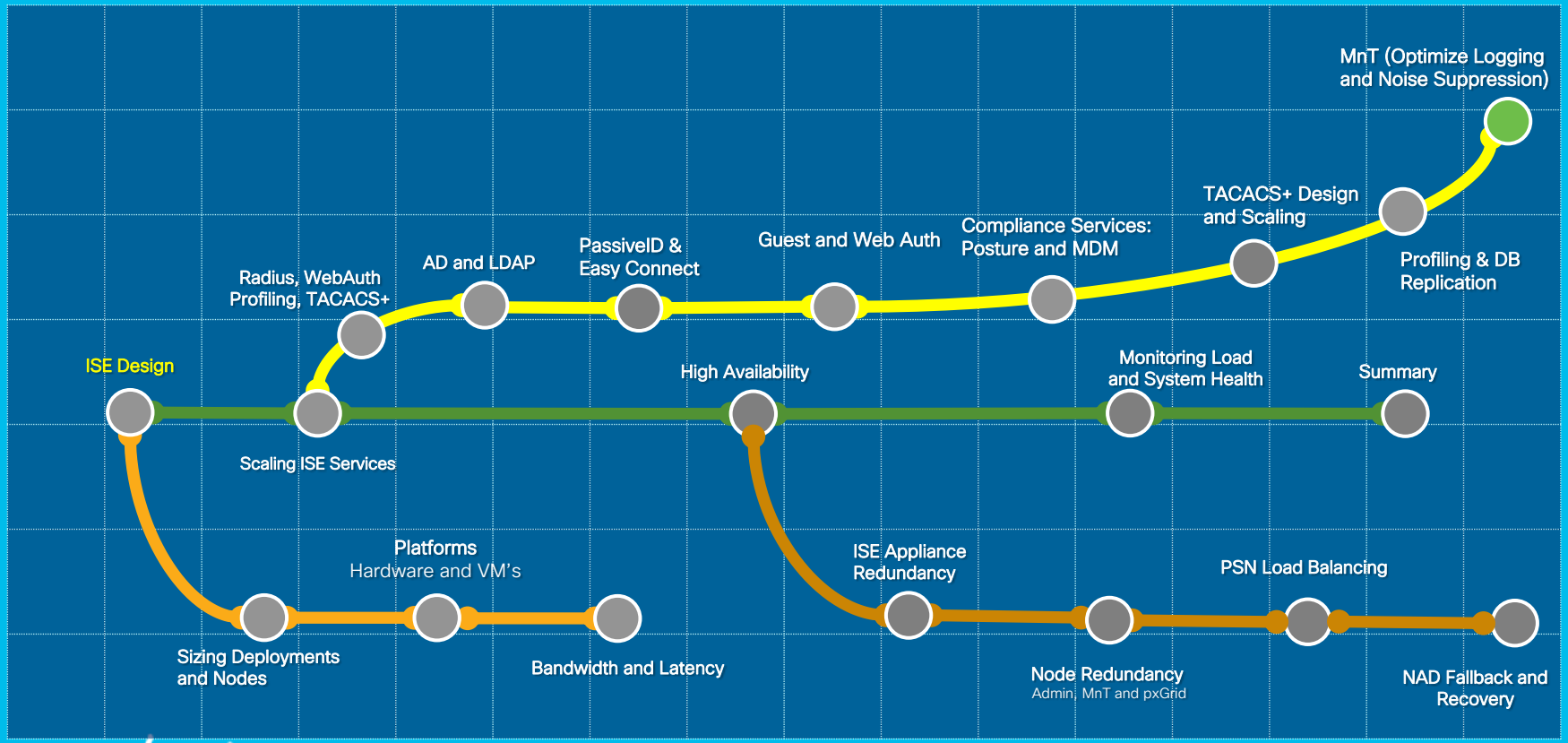
Factors Impacting Bandwidth Consumption for Profiling (Not Logging/Replication)

- Profiling traffic will be probe specific and dependent on many factors including:
- RADIUS Probe itself does not consume additional bandwidth unless tied to Device Sensor.
- RADIUS traffic generated by Device Sensor will depend on switch DS config, i.e. all events or only changes, functions enabled, and filters set.
- SNMP Query is based on configured polling interval (NAD based) and NAD sizes (for example, bigger switches with more active ports/connections will result in higher SNMP bandwidth).
- SNMP Query (Port based) can also be triggered by SNMP Traps or RADIUS Accounting State, but current code should limit to one query per 24hrs.
- SNMP Traps will depend on # endpoints and connection events. Note that SNMP trap processing only supported for Wired.
- DHCP-related profile traffic will be dependent on lease timers and connection and reauth rates. Reauth rates can be triggers by idle and session timers or CoA where session terminates/port bounces and triggers DHCP). Traffic is multiplied by the number of PSN targets configured which is why I advocate limiting targets to no more than two or possibly one using Anycast.
- DHCP SPAN option will likely consume more bandwidth, especially if not filtered on DHCP only, as it collects all DHCP including bidirectional traffic flows. Also, since no simple methods for SPAN HA, may need to send multiple SPANs to different PSNs (not pretty and another reason why I don't generally recommend SPAN option).
- HTTP via redirects does not consume additional bandwidth
- HTTP via SPAN may consume a lot of bandwidth and will depend on SPAN config, where placed, traffic volume, and whether capture is filtered for only HTTP. Note, we will not parse HTTPS SPAN traffic. Like DHCP SPAN, multiple targets required for redundancy.
- NMAP is triggered, but only 3 attempts on newly discovered Unknowns or policy triggered. Additional endpoint SNMP queries will be endpoint specific. For most part, it should be fairly quiet. There is manual nmap scan option, but this should be used with care to avoid excessive ISE or network load. As manual process, requires deliberate admin trigger.
- DNS is triggered based on new IP discovery, but for most part should be quiet.
- Netflow can add a large amount of traffic and highly dependent on Netflow config on source and the traffic volume. Like SPAN challenges, volume is multiple by # PSN Netflow targets unless leverage something like Anycast for redundancy.

Scaling MnT (Optimize Logging and Noise Suppression)

Session Agenda

MnT (Optimize Logging and Noise Suppression)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

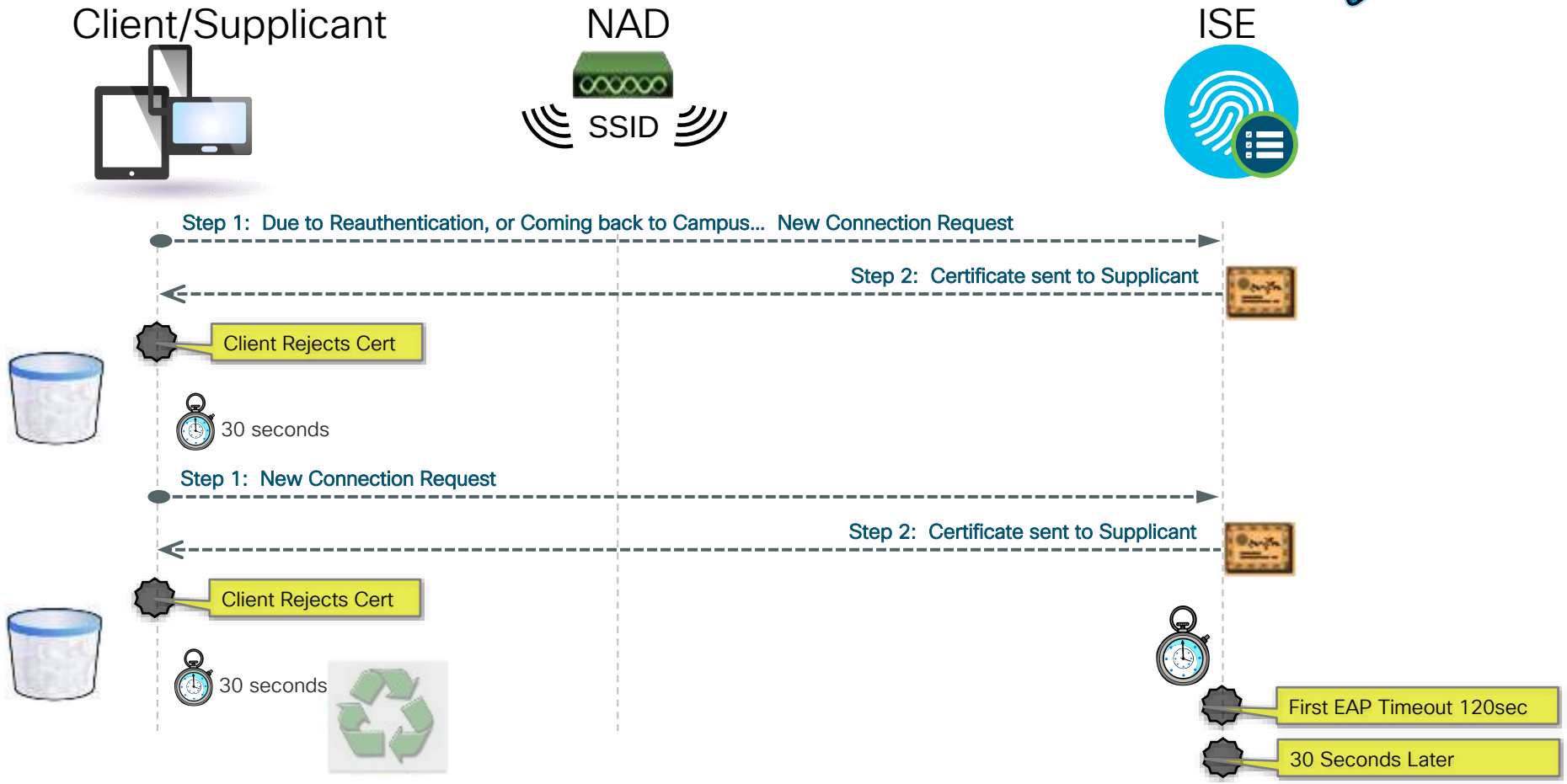
The Fall Out From the Mobile Explosion and IoT

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Repeats Every 30 Seconds

For Your Reference



No Response Received From Client

For Your Reference

Identity Services Engine

atw-cp-ise01 | admin | Logout | Feedback

Home | Operations | Policy | Administration | Setup Assistant

Authentications | Reports | Endpoint

What might this do to MnT logging??

Show Live Sessions | Add or Remove Columns | Show Latest 20 records within Last 24 hours

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

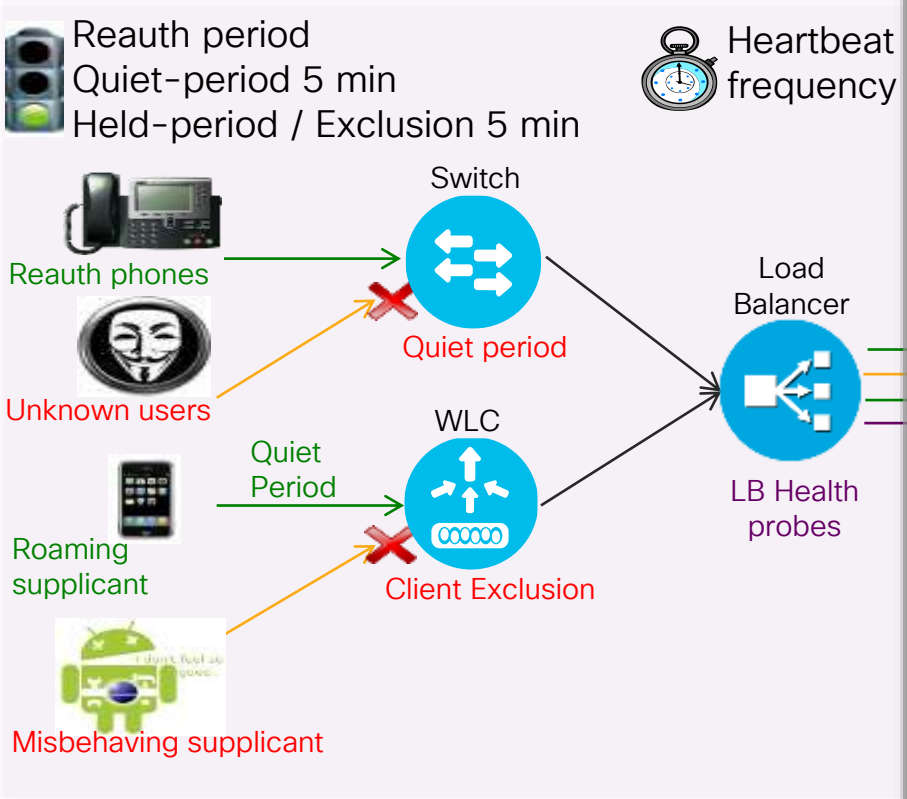
Challenge: How to reduce the flood of log messages while increasing PSN and MNT capacity and tolerance

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

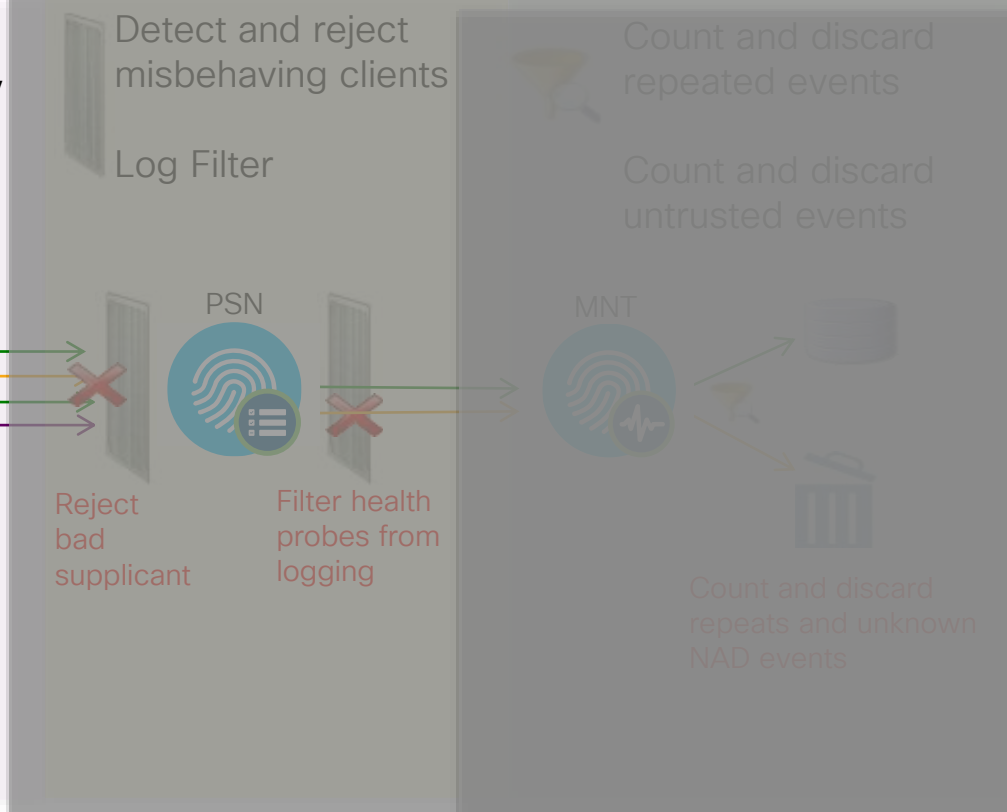
Getting More Information With Less Data

Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source



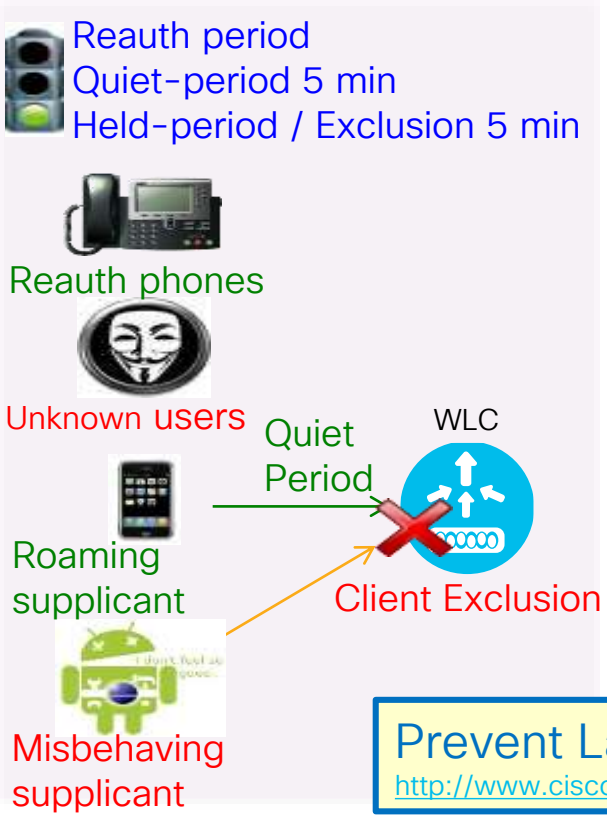
Filtering at Receiving Chain



Tune NAD Configuration

Rate Limiting at Wireless Source

BRKSEC-2059
Deploying ISE in a Dynamic Environment
Clark Gambrel



Wireless (WLC)

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

Prevent Large-Scale Wireless RADIUS Network Melt Downs
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118703-technote-wlc-00.html

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Public Doc on Recommended Wireless Settings

For Your Reference

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

Worldwide [change] | Welcome, Craig Hyps | Account | Log Out | My Cisco

cisco | Products & Services | Support | How to Buy | Training & Events | Partners

Wireless, LAN (WLAN)

Prevent Large-Scale Wireless RADIUS Network Melt Downs

- HOME
- SUPPORT
- TECHNOLOGY SUPPORT
- WIRELESS / MOBILITY
- WIRELESS, LAN (WLAN)
- TROUBLESHOOT AND ALERTS
- TROUBLESHOOTING TECHNOTES
  - **Prevent Large-Scale Wireless RADIUS Network Melt Downs**

Contents

TAC

Document ID: 118703
Updated: Jan 05, 2015

Contributed by Aaron Leonard, Shankar Ramanathan, and Jesse Dubois, Cisco TAC Engineers.

Download PDF | Print

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired & Wireless recommended links

Best Practices and Guides

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

One-Click Setup for ISE Best Practice Config

Added in WLC 8.4

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

RADIUS Authentication Servers > New

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

Apply Cisco ISE Default Settings ☐ Enabled

CISCO MONITOR WLANs CONTROLLER WIRELESS SECUR

WLANs

WLANs > Edit 'v-employee'

- WLANs
  - WLANs
- Advanced

General | Security | QoS | Policy-Mapping | Advanced

Layer 2 | Layer 3 | AAA Servers

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

RADIUS Servers

RADIUS Server Overwrite interface ☐ Enabled

Apply Cisco ISE Default Settings ☐ Enabled

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

RADIUS Server Accounting

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

WLC – RADIUS Server Settings

For Your Reference

RADIUS Server Timeout

- WLC default to receive response from the RADIUS Server is 2 sec; max=30 seconds
- Recommend increase to larger value, for example 5 sec.

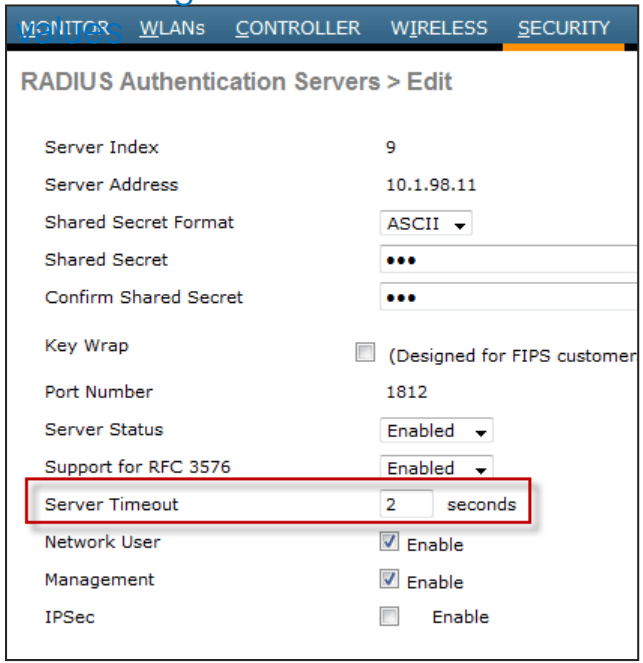
RADIUS Aggressive-Failover

- (Cisco Controller)>**config radius aggressive-failover disable**
- If this is set to 'enable' (default), the WLC will failover to next server after 5 retransmissions for a given client.
- Recommend disable to prevent single misbehaving client from failing over and disrupting other client sessions unless there are 3 consecutive tries for 3 different users (i.e. the radius-server is unresponsive for multiple users).

RADIUS Interim Accounting

- v7.x: Recommend disable (default setting). If required, increase default from 600 sec to 900 sec (15 minutes)
- v8.x: Recommend enable with Interval set to 0.

Note: Diagrams show default values



WLAN > Security > AAA Servers

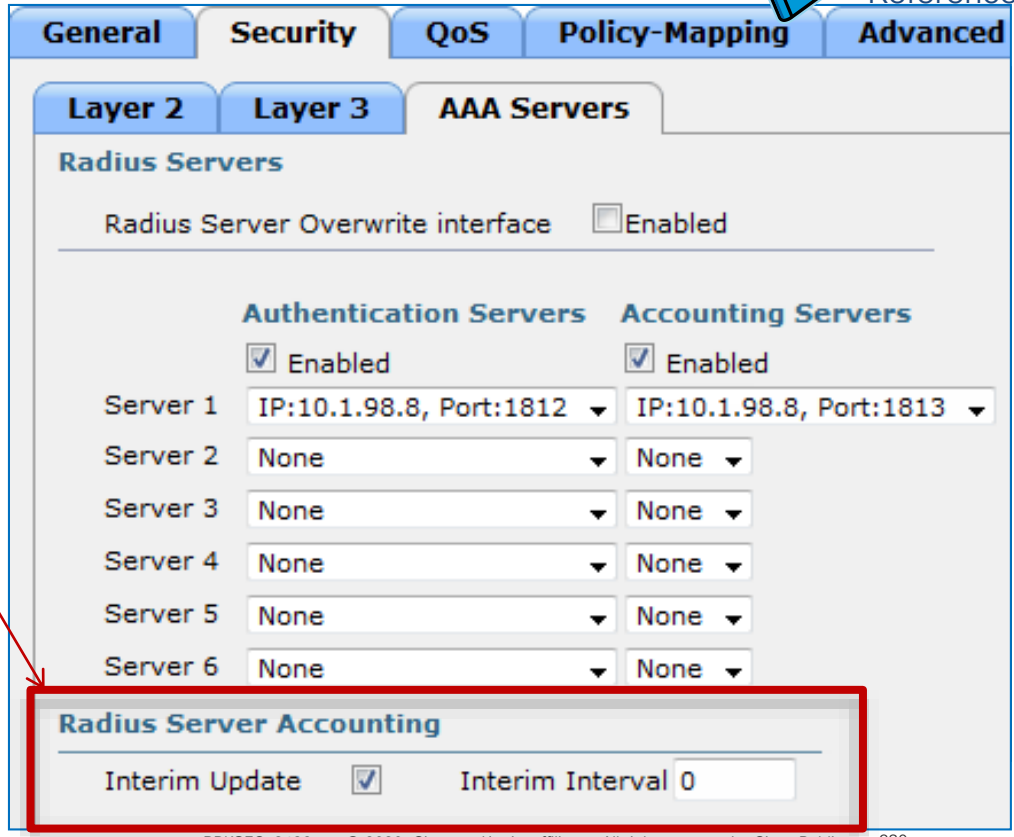
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

RADIUS Accounting Update Behavior in WLC v8.x

Interim Update

For Your Reference

- WLC 7.6:
  - Recommended setting: Disabled
  - Behavior: Only send update on IP address change
  - Device Sensor updates not impacted
- WLC 8.0:
  - Recommended setting: Enabled with Interval set to 0
  - Behavior: Only send update on IP address change
  - Device Sensor updates not impacted
- Upgrade maps settings correctly



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

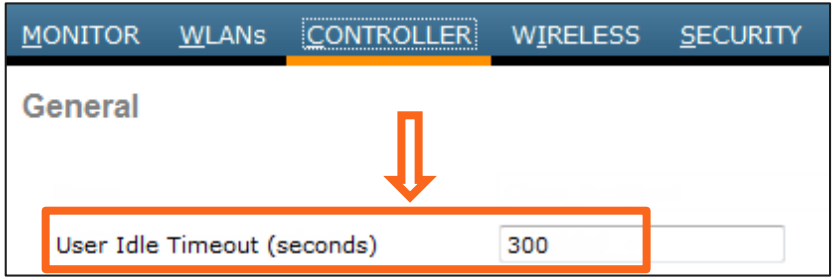
For Your Reference

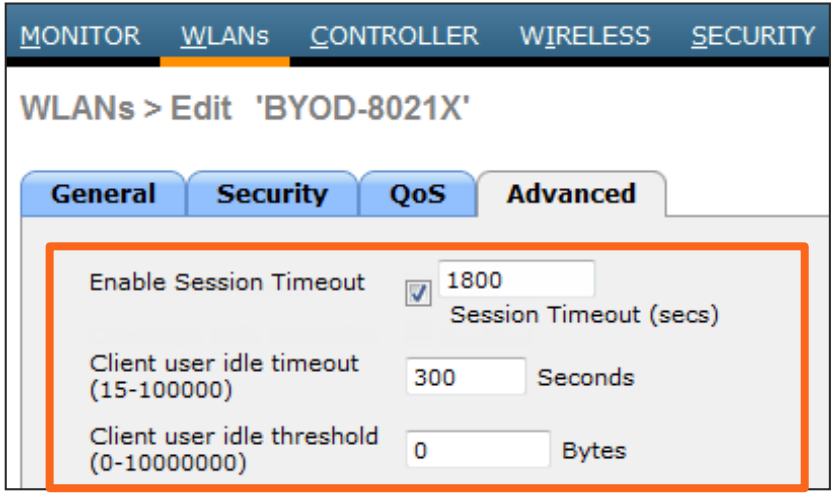
WLC – Authentication Settings

Reduce the # Auths and ReAuths

- Increase Idle Timer to 1 hour (3600 sec) for secure (802.1X) SSIDs.
  - Open SSIDs may require lower idle timer to prevent overload from casual associations.

- Increase reauth/session timers to 2+ hrs (7200+ sec)





Note: Diagrams show default values

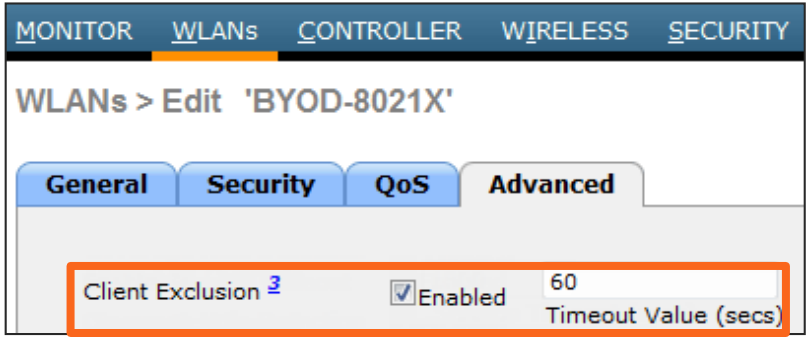
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

WLC – Client Exclusion

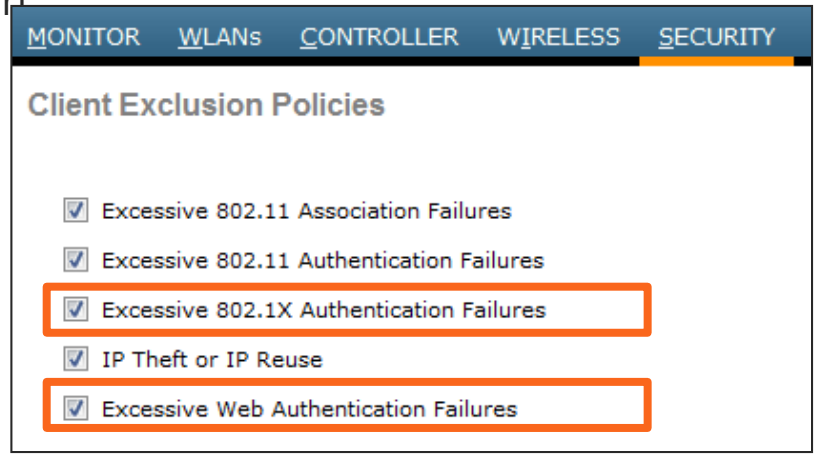
Blacklist Misconfigured or Malicious Clients

For Your Reference

- **Excessive 802.1X Authentication Failures**–Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- **Excessive Web Authentication Failures**–Clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- Client excluded for Time Value specified in WLAN settings. Recommend increase to 1-5 min (60-300 sec). **3 min** is a good start



Note: Diagrams show default values



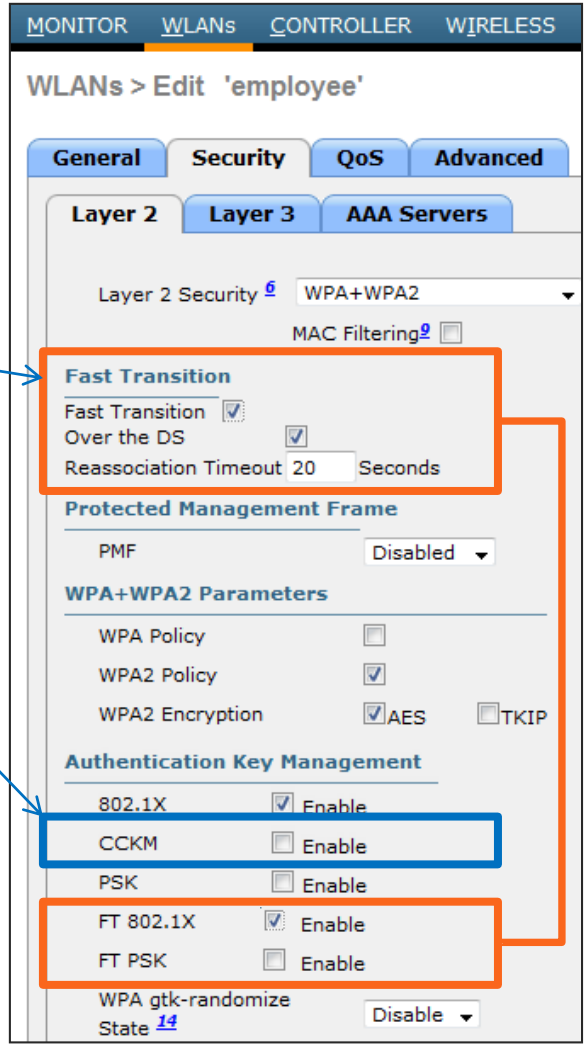
Wireless Roaming

For Your Reference

Key Caching to Avoid Reauth when Roaming

- 802.11r (aka Fast Transition)
  - Enable where supported and feasible; For example, large Apple deployments.
  - Apple support added in iOS6
- CCKM – Cisco Centralized Key Management
  - Clients must support CCKM; CCXv4 feature
- SKC (Sticky PMKID Caching)
  - Requires WLC 7.2
  - Works only with WPA2 WLANs
  - Recommended if clients do not support CCKM or OKC (Opportunistic PMKID Caching)

> config wlan security wpa wpa2 cache sticky enable *wlan_id*



Which WLC Software Should I Deploy?

8.0.152.0 – Currently the most mature and reliable release.

8.2.167.6 – Mature - Recommended when need new feature/hardware support.

8.3.141.0 – Less Mature – Recommend if require new features in 8.3.x

8.5.124.55 – Cutting edge – Recommend if require new features in 8.5.x

8.6.101.0 – Bleeding edge – Only if absolutely require new features in 8.6.x
8.7.102.0 – Only if absolutely require new features in 8.7.x

Example critical defects resolved in maintenance and new releases:

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

TAC Recommended AireOS Builds

For Your Reference

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

- **Recommended Releases:** This document describes the way in which the customers can find the most reliable WLC software available. The Cisco Wireless TAC recommends AireOS builds from each train of released AireOS software. These recommendations may be updated weekly.
- **Escalation Builds:** In some cases, the TAC recommended build may be an "escalation" build. Such builds are not available on CCO (Cisco.com), but have important bugfixes (beyond what is available in CCO code), and will have been operating in production at customer sites for several weeks. Such builds are fully Business Unit (BU) and TAC supported.
- To request a TAC recommended escalation build, open a Cisco TAC case on your WLC contract.
  - **AireOS 7.6:** Not recommended. The recommended migration path is to AireOS 8.0.
  - **AireOS 8.0**: TAC recommends 8.0.152.0.
  - **AireOS 8.1:** 8.1.131.0 is final maintenance release of AireOS 8.1. Recommend upgrade to 8.2.
  - **AireOS 8.2:** For new features or hardware after 8.0, TAC recommends 8.2.167.6 (8.2MR7).
  - **AireOS 8.3:** For new features or hardware introduced after 8.2, TAC recommends 8.3.141.0.
  - **AireOS 8.4:** Short lived release with no maintenance planned, and is deferred; 8.5 is recommended.
  - **AireOS 8.5:** For new features or hardware after 8.3, TAC recommends 8.5.124.55 (8.5MR3 interim)
  - **AireOS 8.6:** BU and TAC support the 8.6.101.0 release; required for features avail post 8.5.
  - **AireOS 8.6:** BU and TAC support the 8.7.102.0 release; required for features avail post 8.6.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless Controllers Under Extreme Load (8.1

For Your Reference

- 5508 and WISM2
  - 8 queues per server (max 17 servers configurable)
- 8510/7510
  - 16 queues per server (max 17 servers configurable)
- For all platforms, each queue = 0-255 unique IDs. So total 256*8 = 2048 requests/server.
- Example using 5508/WISM2 :
  - We will have unique source port per queue.
  - Total 8 unique source ports.
- Queue is selected based on MAC address Hashing.

	Server 1	Server2
Queue 1	src port 1	src port 1
Queue 2	src port 2	src port 2
Queue 3	src port 3	src port 3
Queue 4	src port 4	src port 4
Queue 5	src port 5	src port 5
Queue 6	src port 6	src port 6
Queue 7	src port 7	src port 7
Queue 8	src port 8	src port 8

Related defects:
CSCus51456,CSCur33085
CSCue37368, CSCuj88508

Before 8.1, separate queues added for Auth and Accounting, but all servers share same two queues. (CSCud12582, CSCul96254)

In 8.1, queues are not divvied or shared between Auth and Accounting-both will have separate queues

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Wireless Best Practices

Anchor Configurations

- RADIUS Accounting with Anchor Controllers
  - Guest Anchors: Disable RADIUS Accounting on Guest Anchor WLAN (Enable on Foreign Only)
  - Campus Anchors: In campus roaming scenario where all controllers need to be "primary" for same SSID, cannot disable RADIUS Accounting.
  - Open SSIDs will always issue new BRKSEC3432 with RADIUS accounting update with new ID, so disconnects original connection and user is re-authenticated.
    - CSCul83594 Sev6 - Session-id is not synchronized across mobility if the network is open
    - CSCue50944 Sev6 - CWA Mobility Roam Fails to Foreign with MAC Filtering BYOD

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless Best Practices

Roaming Considerations

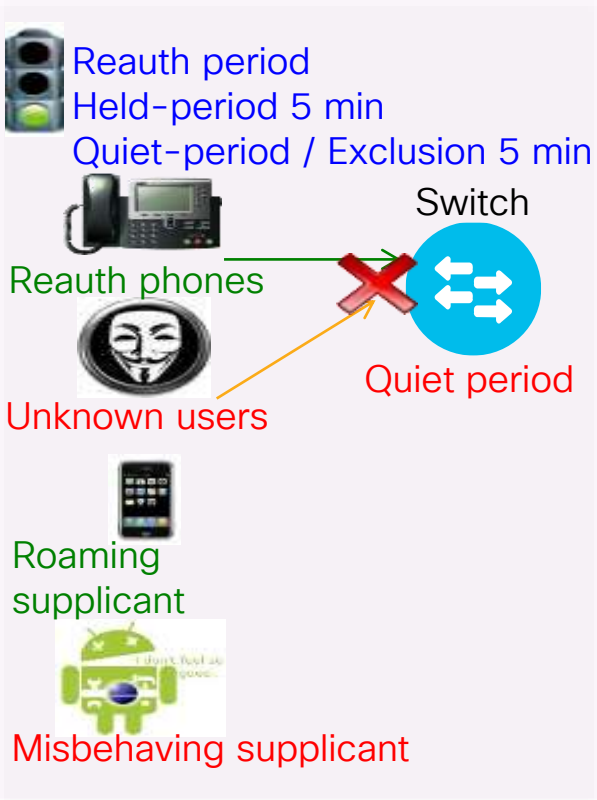
For Your Reference

- BRKSEC3432s can change when roam between controllers (L2 or L3 roaming); Going between APs to same controller should fine.
- Secure SSIDs (802.1X): L2/L3 roaming between controllers should handle without reauth—all roams are basically symmetric with tunnel back to foreign controller
- Open SSIDs (MAB, WebAuth):
  - Avoid multiple controllers with open SSIDs – otherwise, will get new BRKSEC3432 (reauth) regardless if L2 or L3 roam. [CSCul83594Session-id is not synchronized across mobility, if the network is open (fixed in 8.6)]
  - Reauth any time change IP. For open SSID, it will always issue new SSID.
- Options:
  - Stateful Controller Switchover
  - Deploy higher-capacity controllers instead of many smaller ones.
- 802.11r will work with 7.6 or 8.0 and can be applied to entire WLAN—not tested under 7.6 so warning provided.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tune NAD Configuration

Rate Limiting at Wired Source



Wired (IOS / IOS-XE)

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired – RADIUS Interim Accounting

For Your Reference

All IOS and IOS-XE Platforms

- Command:

  switch(config)# **aaa accounting update [newinfo] [periodic** *number* **[jitter maximum** *max-value* **]]**

- Recommendation:

  switch(config)# **aaa accounting update** [**newinfo periodic 1440 | periodic 15**]

  Note: If RADIUS Load Balancing used, set lower than persistence interval to stick with same PSN.

- Reference:
  - When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report.
  - When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number (in minutes). The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.
  - Jitter is used to provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent at exact intervals, you should disable jitter by setting it to 0.

Caution: Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network

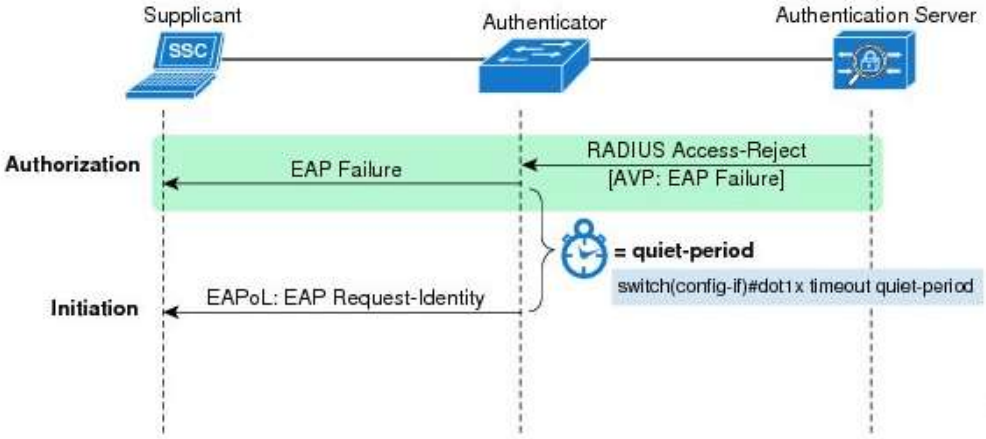
Wired - 802.1X Timeout Settings

All IOS and IOS-XE Platforms

For Your Reference

- switch(config-if)# **dot1x timeout held-period** 300 | **quiet-period** 300 | **ratelimit-period** 300

held-period seconds	Supplicant waits X seconds before resending credentials after a failed attempt. Default 60.
quiet-period seconds	Switch waits X seconds following failed authentication before trying to re-authenticate client. Default: 120. • Cisco 7600 Default: 60.
ratelimit-period seconds	Switch ignores EAPOL-Start packets from clients that authenticated successfully for X seconds. Default: rate limiting is disabled.



Throttles misconfigured/misbehaving clients:

Quite-Period = 300 sec
= Wait 5 minutes after failed 802.1X auth.

Ratelimit-Period = 300 sec
= Ignore additional auth requests for 5 min. after successful 802.1X auth.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired - 802.1X Timeout Settings

Command Details

For Your Reference

- Wired - All IOS and IOS XE platforms
  - switch(config-if)# **dot1x timeout held-period 300 | quiet-period 300 | ratelimit-period 300**

held-period seconds	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). • The range is from 1 to 65535. The default is 60.
quiet-period seconds	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 120. • For the Cisco 7600 series Switch, the range is from 0 to 65535. The default is 60.
ratelimit-period seconds	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wired – Authentication Settings

For Your Reference

Reduce the # Auths and ReAuths

- **Disable or Increase Inactivity Timer to 1+ hours; Disable /increase Reauth to 2+ hours**

switch(config-if)# **authentication ?**

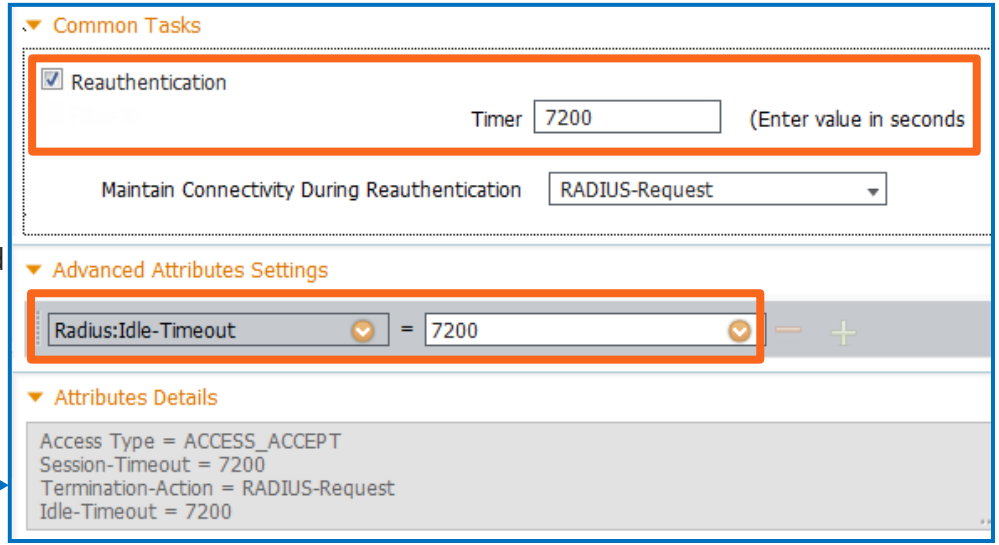
- periodic — Enable or Disable Reauthentication for this port
- timer — Set authentication timer values

switch(config-if)# **authentication timer ?**

- inactivity — Interval in seconds after which if there is no activity from the client then it will be unauthorized (default OFF)
- reauthenticate — Time in seconds after which an automatic re-authentication should be initiated (default 1 hour)

Enable inactivity timer with caution for non-user / MAB endpoints.

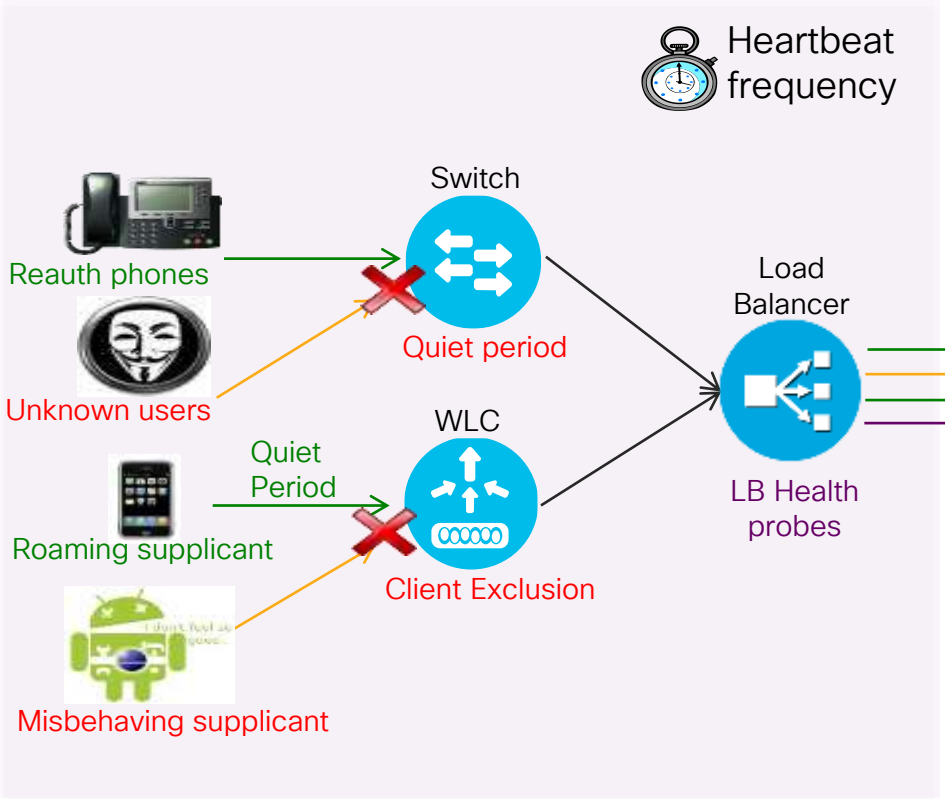
- On the Server Side (ISE), Idle and Session / Reauth timers are configured in the Authorization Profile



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

RADIUS Test Probes

Reduce Frequency of RADIUS Server Health Checks



- **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.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD RADIUS Test Probes

IOS Switch Test Probes

For Your Reference

- By default, IOS Switches and WLC validate health through active authentications.
- Optional: IOS can send separate RADIUS test probes via **idle-time** setting.
- **Recommendation: Keep default interval = 60 minutes**
- Older command syntax :

```
radius-server host 10.1.98.8 auth-port 1812 acct-port 1813 test
username radtest ignore-acct-port idle-time 120 key cisco123
```

- Newer command syntax:

```
radius server psn-cluster1
  address ipv4 10.1.98.8 auth-port 1812 acct-port 1813
  automate-tester username radtest ignore-acct-port idle-time 120
  key cisco123
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancer RADIUS Test Probes

Citrix Example

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

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

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

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

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

F5 Example

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

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

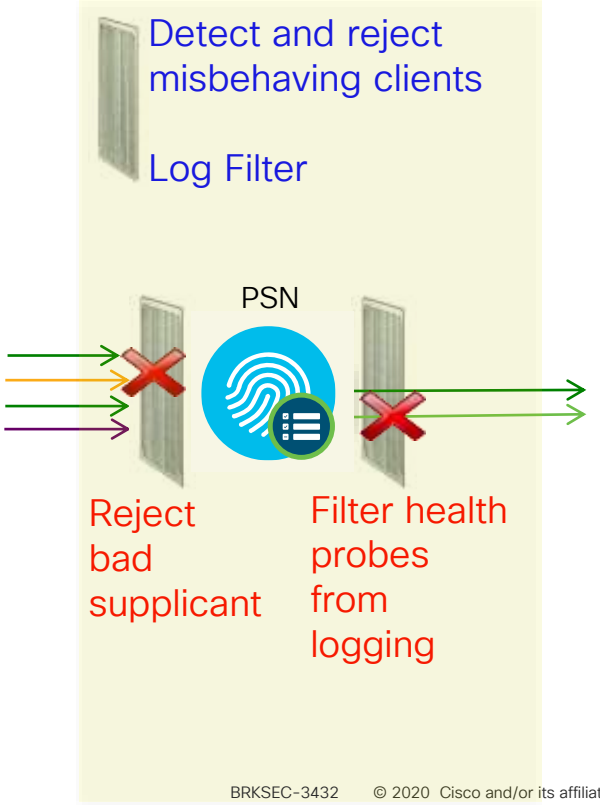
    Timeout *seconds* # Default: 31
- Sample F5 RADIUS probe configuration:

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

PSN Noise Suppression and Smarter Logging

Filter Noise and Provide Better Feedback on Authentication Issues

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

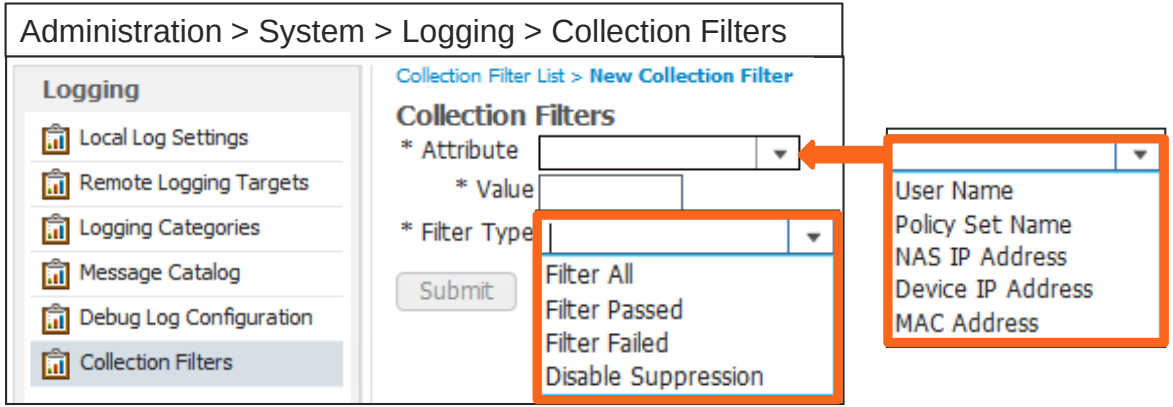


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

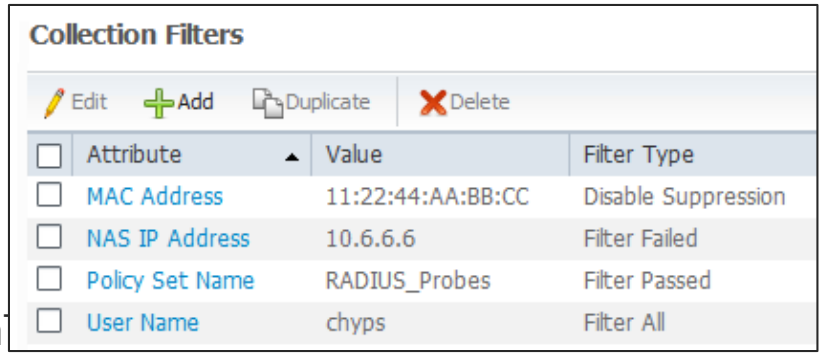
PSN - Collection Filters

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 @Mn



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Filtering and Noise Suppression (pre-ISE 2.2)

Misconfigured Client–Dynamic Detection and Suppression

For Your Reference

- Flag misbehaving supplicants when fail auth more than once per Detection Interval
  - Alarm sent inc. failure stats each Report Interval
  - Stop sending logs for repeat auth failures for same endpoint during Rejection Interval.
  - Successful auth clears flag
- Once flagged, if fail auth 5 more times of same failure reason→ Access-Reject
  - Match these attributes:
    - Calling-Station-ID (MAC Addr)
    - NAS-IP-Address (NAD)
    - 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)

Save | Reset | Reset To Defaults

CSCuj03131 Lower "Request Rejection Interval" minimum to 5 minutes (from 30 minutes)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Filtering and Noise Suppression

Dynamic Client Suppression

Updated in ISE 2.2!

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

Send alarm with failure statistics

RADIUS Settings

Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- [x] Suppress repeated failed clients
  - Detect two failures within 5 minutes(1 - 30)
  - Report failures once every 15 minutes (15 – 60)
- [x] Reject repeated failed RADIUS requests
  - Failures prior to automatic rejection
  - Continue rejectin
  - Ignore repeated accounting updates within seconds (1 - 86,400)

Suppress Successf

- [x] Suppress repe

Authentication Deta

Highlight steps lon onds (500 - 10,000)

Valid Time ranges displayed by default

Each endpoint tracked by:

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Filtering and Noise Suppression

Dynamic Client Suppression

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

Send alarm with failure statistics

Send immediate Access-Reject (do not even process request) IF:
1) Flagged for suppression
2) Fail auth total X times for same failure reason (inc 2 prev)

Fully process next request after rejection period expires.

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- [x] Suppress repeated failed clients
  - Detect two failures within: 5 minutes(1 - 30)
  - Report failures once every: 15 minutes (15 – 60)
- [x] Reject repeated failed RADIUS requests
  - Failures prior to automatic rejection: 5
  - Continue rejecting requests for: 60 minutes (5 – 180)
  - Ignore repeated accounting updates within: 5 seconds (1 - 86,400)

Hard-coded @ 5 in ISE 2.0

Suppress Successful Reports

- [x] Suppress repeated successful authentications

Authentication Details

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Noise Suppression

Drop Excessive RADIUS Accounting Updates from “Misconfigured NADs”

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

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- [x] Suppress repeated failed clients
  - Detect two failures within: 5 minutes(1 - 30)
  - Report failures once every: 15 minutes (15 – 60)
  - [x] Reject repeated failed RADIUS requests
    - Failures prior to automatic rejection: 5 (2-100)
    - Continue rejecting requests for: 60 minutes (5 – 180)
  - Ignore repeated accounting updates within: 5 seconds (1 - 86,400)

Suppress Successful Reports

- [x] Suppress repeated successful authentications

Authentication Details

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

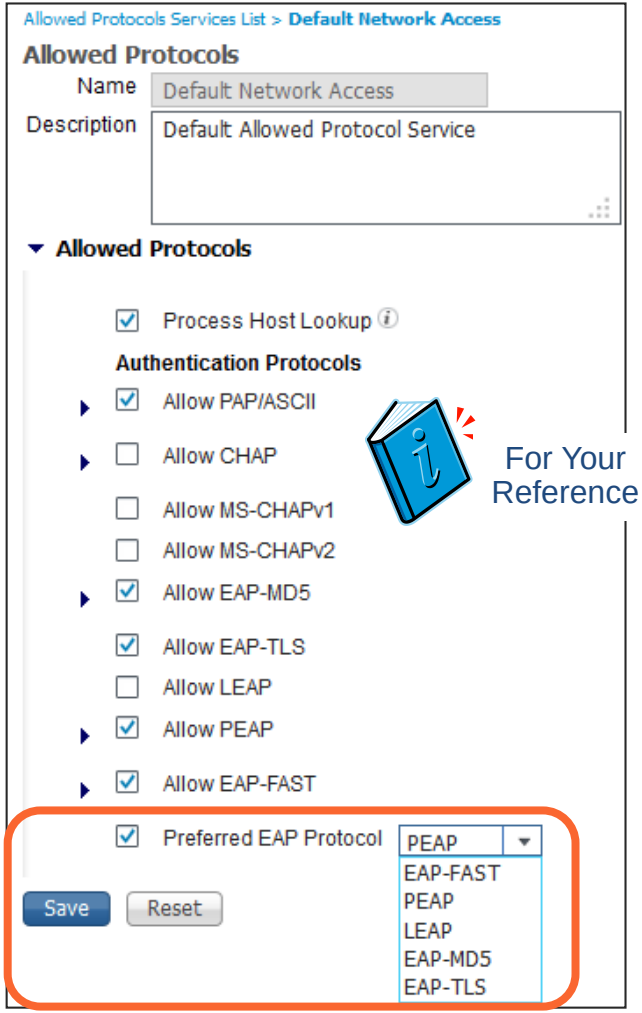
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enhanced EAP Session Handling

Improved Treatment for Empty NAK List

- Best Effort for Supplicants that Improperly Reply with Empty NAK List: PSN suggests the most secure or preferred EAP protocol configured (per Allowed Protocols list).
  - Some supplicants may reply with NAK and not suggest alternative protocol (empty NAK list).
  - ISE will now suggest other supported protocols rather than fail auth.
- Set Preferred EAP Protocol on ISE to most common method used by network.
  - This sets the list of proposed EAP methods sent to supplicant during auth negotiation.
  - Value is disabled by default.

Policy > Policy Elements > Results Authentication > Allowed Protocols



For Your Reference

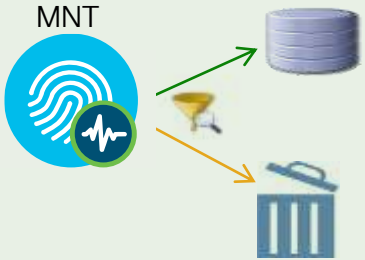
MnT Log Suppression and Smarter Logging

Drop and Count Duplicates / Provide Better Monitoring Tools

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

Count and discard repeated events

Count and discard untrusted events



Count and discard repeats and unknown NAD events

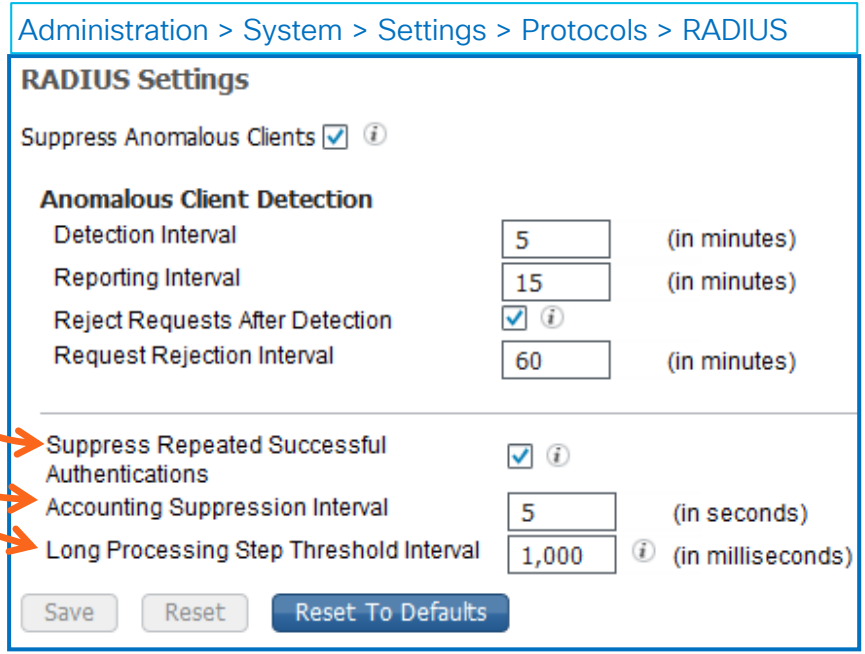
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Noise Suppression (pre-ISE 2.2)

Suppress Successful Auths and Accounting

For Your Reference

- Suppress Repeated Successful Auths
  = Do not save repeated successful auth events to MnT DB
  (Events will not display in Live Auth log).
- Accounting Suppression Interval
  = Allow 2 log updates for same session, then suppress any more updates in interval
  (Range 1 sec – 1 day)
- Long Processing Step Threshold Interval
  = Detect and log NAD retransmission timeouts for auth steps that exceed threshold.
  (Step latency is visible in Detailed Live Logs)



CSCur42723 Increase "Accounting Suppression Interval" maximum to 24 hrs (from 30 minutes)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Noise Suppression

Suppress Storage of Repeated Successful Auth Events

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

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

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- [x] Suppress repeated failed clients
  - Detect two failures within: 5 minutes(1 - 30)
  - Report failures once every: 15 minutes (15 – 60)
  - [x] Reject repeated failed RADIUS requests
    - Failures prior to automatic rejection: 5 (2-100)
    - Continue rejecting requests for: 60 minutes (5 – 180)
  - Ignore repeated accounting updates within: 5 seconds (1 - 86,400)

Suppress Successful Reports

- [x] Suppress repeated successful authentications

Authentication Details

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Noise Suppression

Suppress Storage of Repeated Successful Auth Events

Step latency is visible in Live Logs details

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

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

Detect NAD retransmission timeouts and Log auth steps > threshold.

RADIUS Settings

Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- [x] Suppress repeated failed clients
  - Detect two failures within: 5 minutes(1 - 30)
  - Report failures once every: 15 minutes (15 – 60)
  - [x] Reject repeated failed RADIUS requests
    - Failures prior to automatic rejection: 5 (2-100)
    - Continue rejecting requests for: 60 minutes (5 – 180)
  - Ignore repeated accounting updates within: 5 seconds (1 - 86,400)

Suppress Successful Reports

- [x] Suppress repeated successful authentications

Authentication Details

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

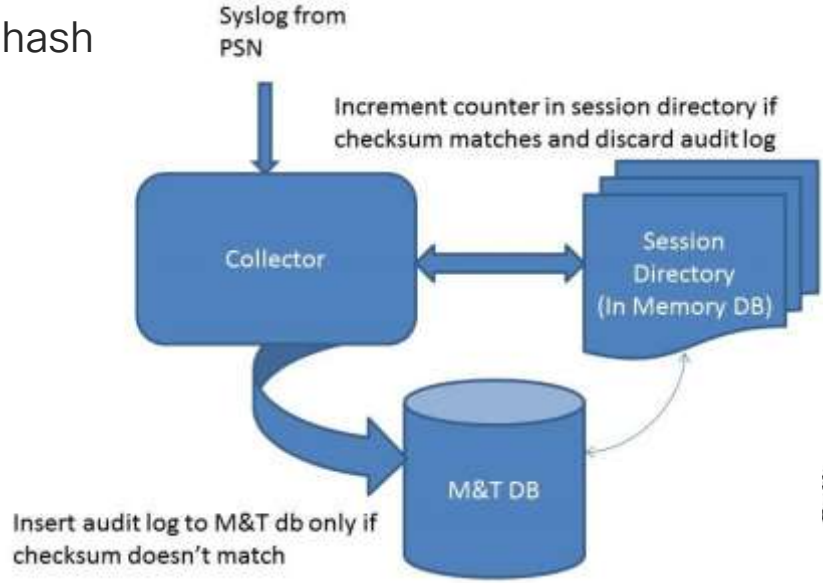
MnT Duplicate Passed Auth Suppression

For Your Reference

Drop and Count Duplicates

- Unique session entries determined by hash created based on these attributes:
  - Called Station Id
  - User Name
  - Posture Status
  - CTS Security Group
  - Authentication Method
  - Authentication Protocol
  - NAS IP Address
  - NAS Port Id
  - Selected Authorization Profile

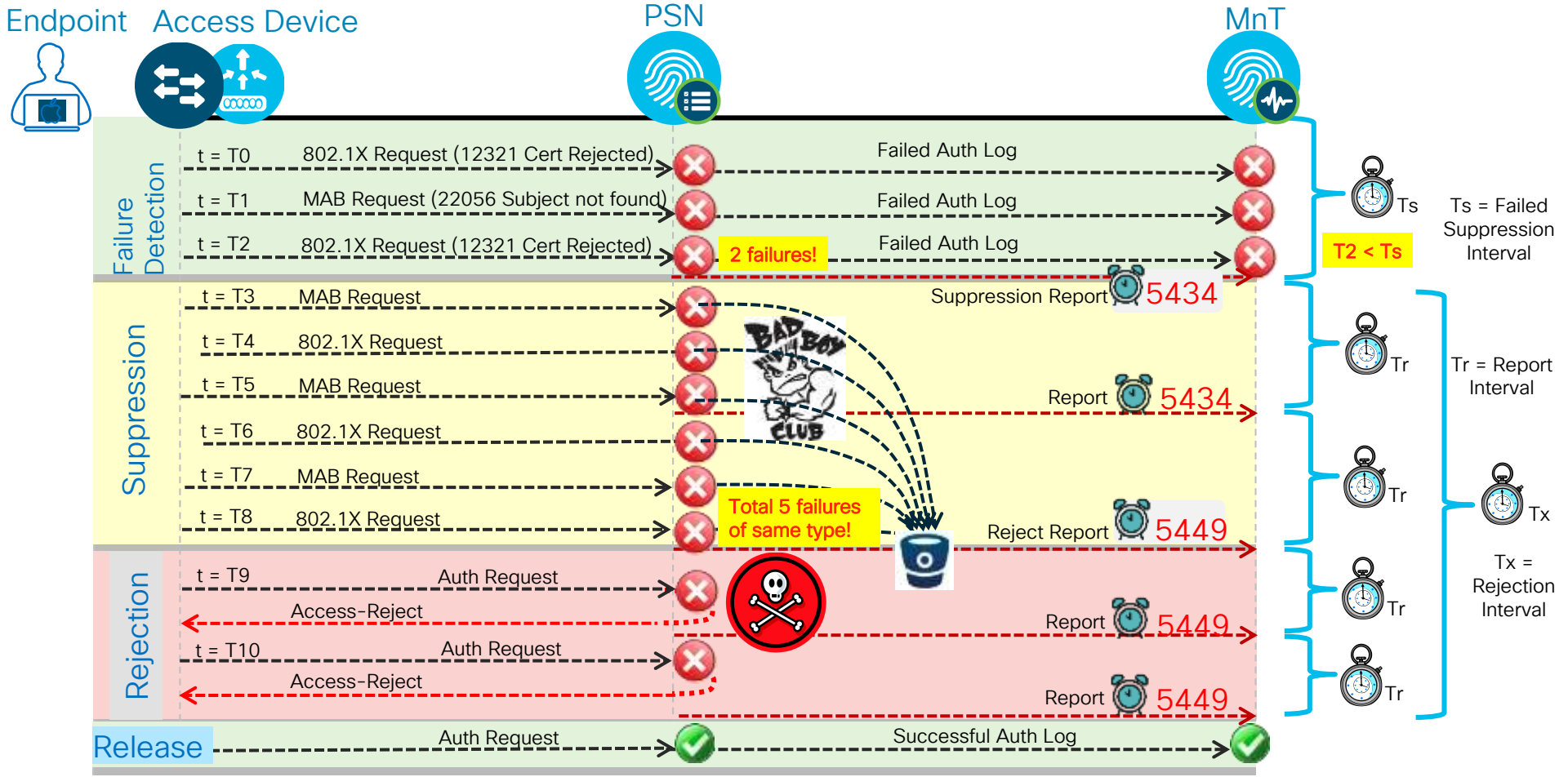
5eaf59f1e6cd6aa6113ca1463c779c3f (MD5 hash)



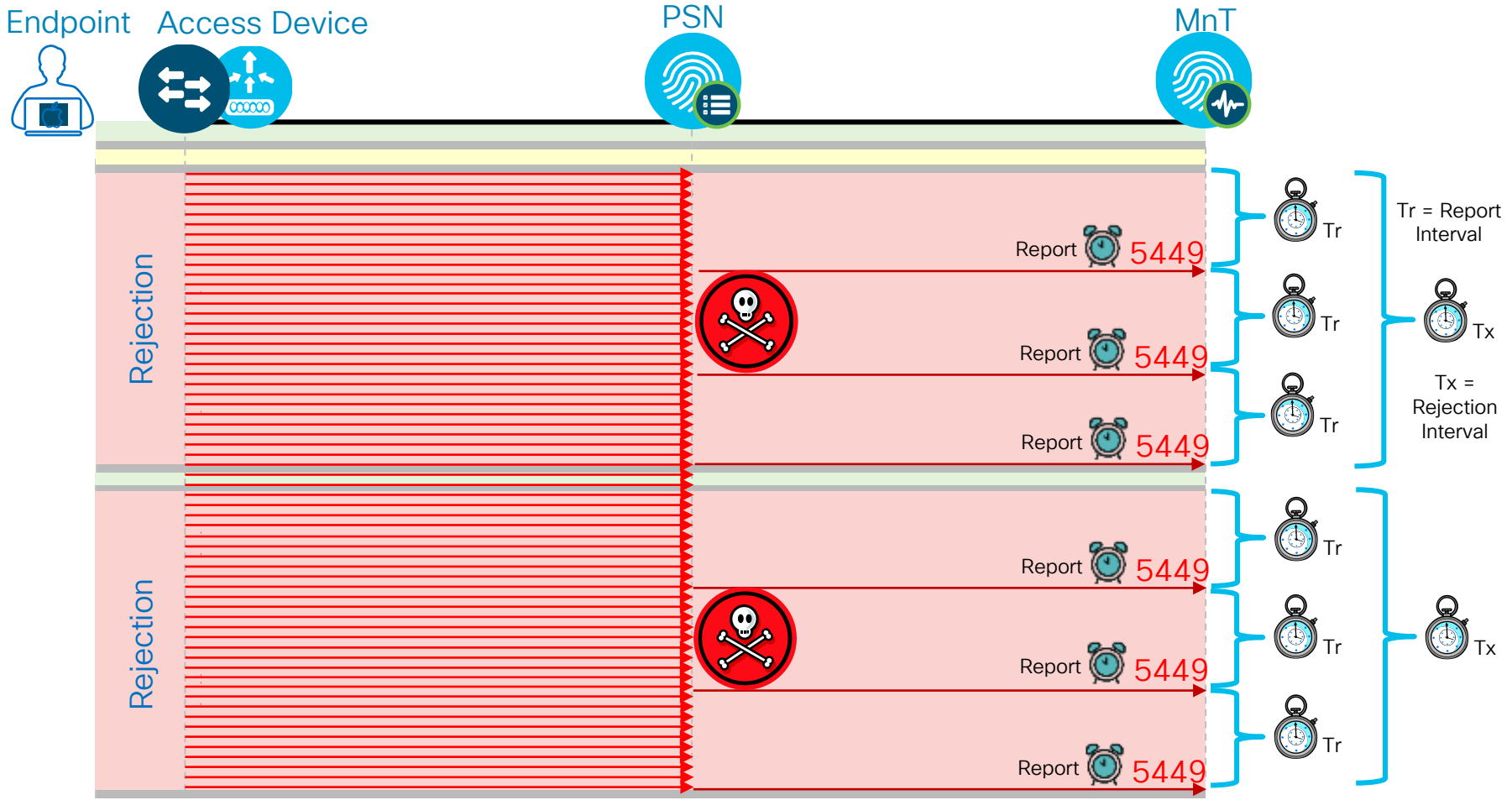
- "Discard duplicate" logic not applicable to failed auths as these are not cached in session
- Except for IP address changes, RADIUS Accounting (Interim) updates are dropped from storage, but do update session

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Suppression and Reject Timers

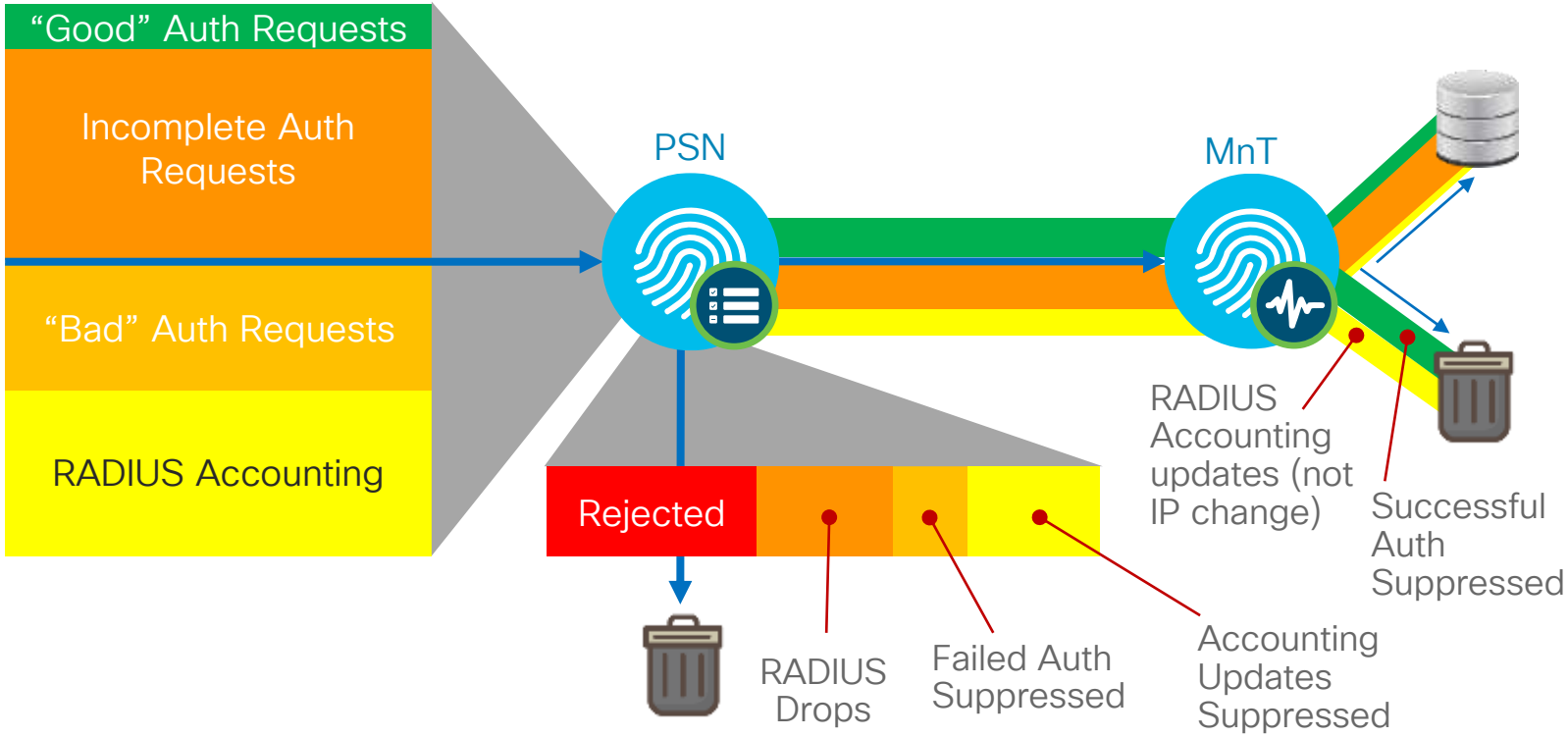


Client Suppression and Reject Timers



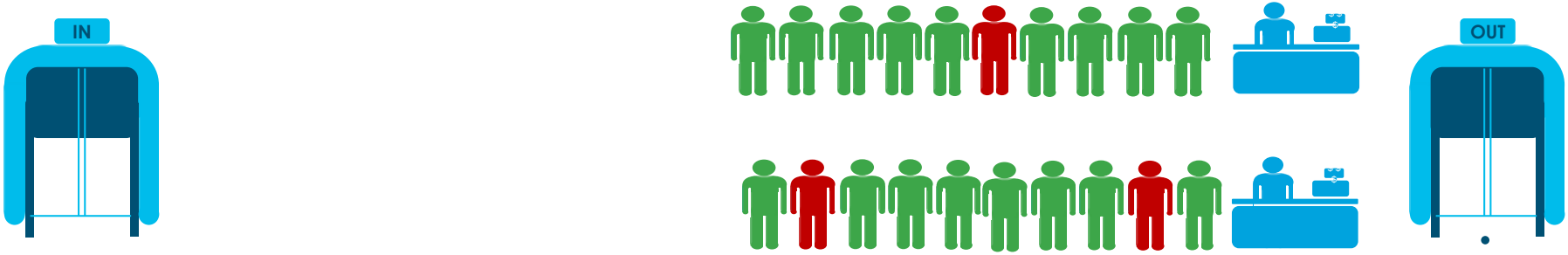
ISE Log Suppression

“Good”-put Versus “Bad”-put



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Typical Load Example



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

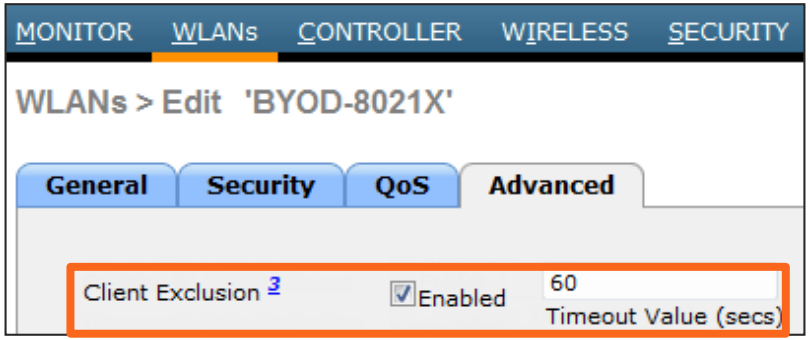
Extreme Noise Load Example

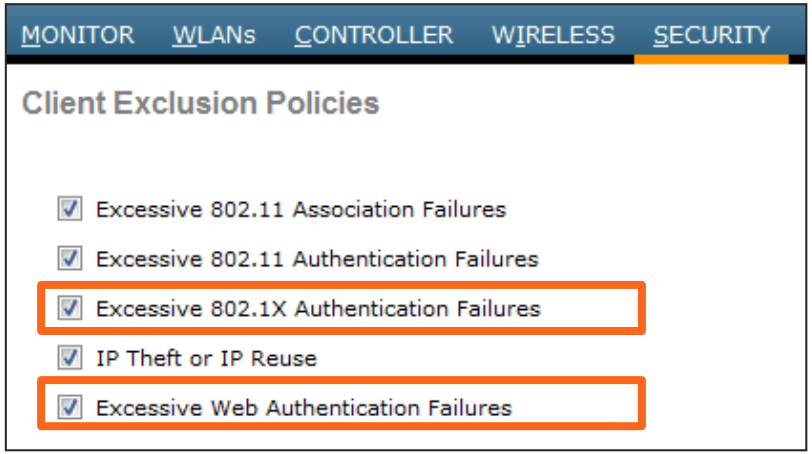
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

WLC – Client Exclusion

Blacklist Misconfigured or Malicious Clients

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





Note: Diagrams show default values

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

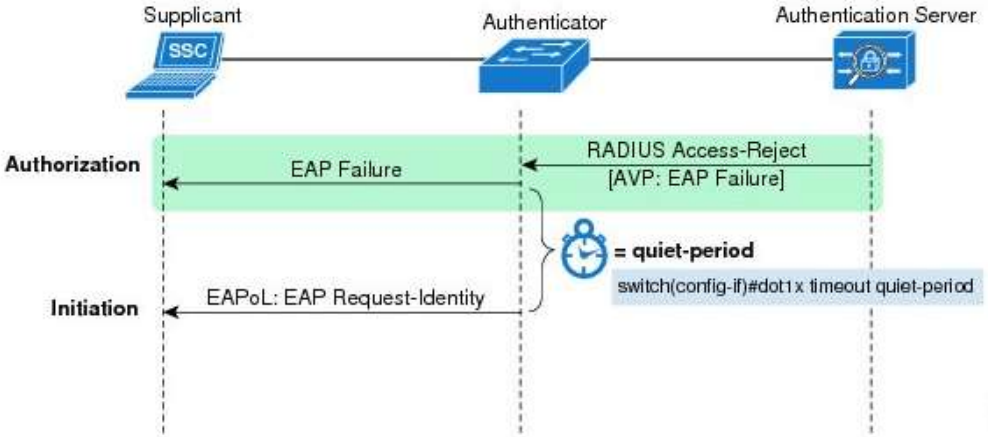
Wired - 802.1X Timeout Settings

All IOS and IOS-XE Platforms

For Your Reference

- switch(config-if)# **dot1x timeout held-period** 300 | **quiet-period** 300 | **ratelimit-period** 300

held-period seconds	Supplicant waits X seconds before resending credentials after a failed attempt. Default 60.
quiet-period seconds	Switch waits X seconds following failed authentication before trying to re-authenticate client. Default: 120. • Cisco 7600 Default: 60.
ratelimit-period seconds	Switch ignores EAPOL-Start packets from clients that authenticated successfully for X sec. Default: rate limiting is disabled.



Throttles misconfigured/misbehaving clients:

Quite-Period = 300 sec
= Wait 5 minutes after failed 802.1X auth.

Ratelimit-Period = 300 sec
= Ignore additional auth requests for 5 min. after successful 802.1X auth.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Live Authentications and Sessions

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005			0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890			11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:29.658			99	wekang	B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:29.252			1	mutama	CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:25.595			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			7	dsladden	0C:77:1A:9A:F6:73	Apple-iPhone	

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

Save

- Filter All
- Filter Passed
- Filter Failed
- Disable Suppression

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Per-Endpoint Time-Constrained Suppression

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005			0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890			11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
					B8:78:2E:60:7F:14	Apple-iDevice	
					CC:78:5F:43:97:71		
					F0:CB:A1:75:31:4D		
					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...

Right Click

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visibility into Reject Endpoints!

ISE 2.2!

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Summary | Endpoints | Guests | Vulnerability | Threat

METRICS

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated C
59700	1325	193	7	

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

other: [<1%]
otp_server: [4.38%]
inter...oints: [7.95%]
ciscoad: [87.52%]

NETWORK DEVICES

Device Name | Type | Location

other: [6.73%]
rcdn5...tana1: [3.37%]
eng-b...a-sw1: [4.37%]
sjc14...alwar: [6.59%]
sbg-b...-wlc1: [6.76%]
eng-b...a-sw1: [10.02%]
rtn01-11a-sw3: [17.97%]
sampg...-wlc1: [24.52%]
sjc19...u-wlc: [19.68%]

ENDPOINTS

Type | Profile

other: [2.95%]
infra...vices: [2.75%]
workstations: [24.72%]
mobil...vices: [42.47%]
misc: [27.11%]

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Releasing Rejected Endpoints

ISE 2.2!

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Endpoints | Users | Network Devices

Authentication | BYOD | Compliance | Compromised Endpoints | Endpoint Classification | Guest | Vulnerable Endpoints

INACTIVE ENDPOINTS | AUTHENTICATION STATUS | AUTHENTICATIONS

Failure Reason | Identity Store | Identity Group

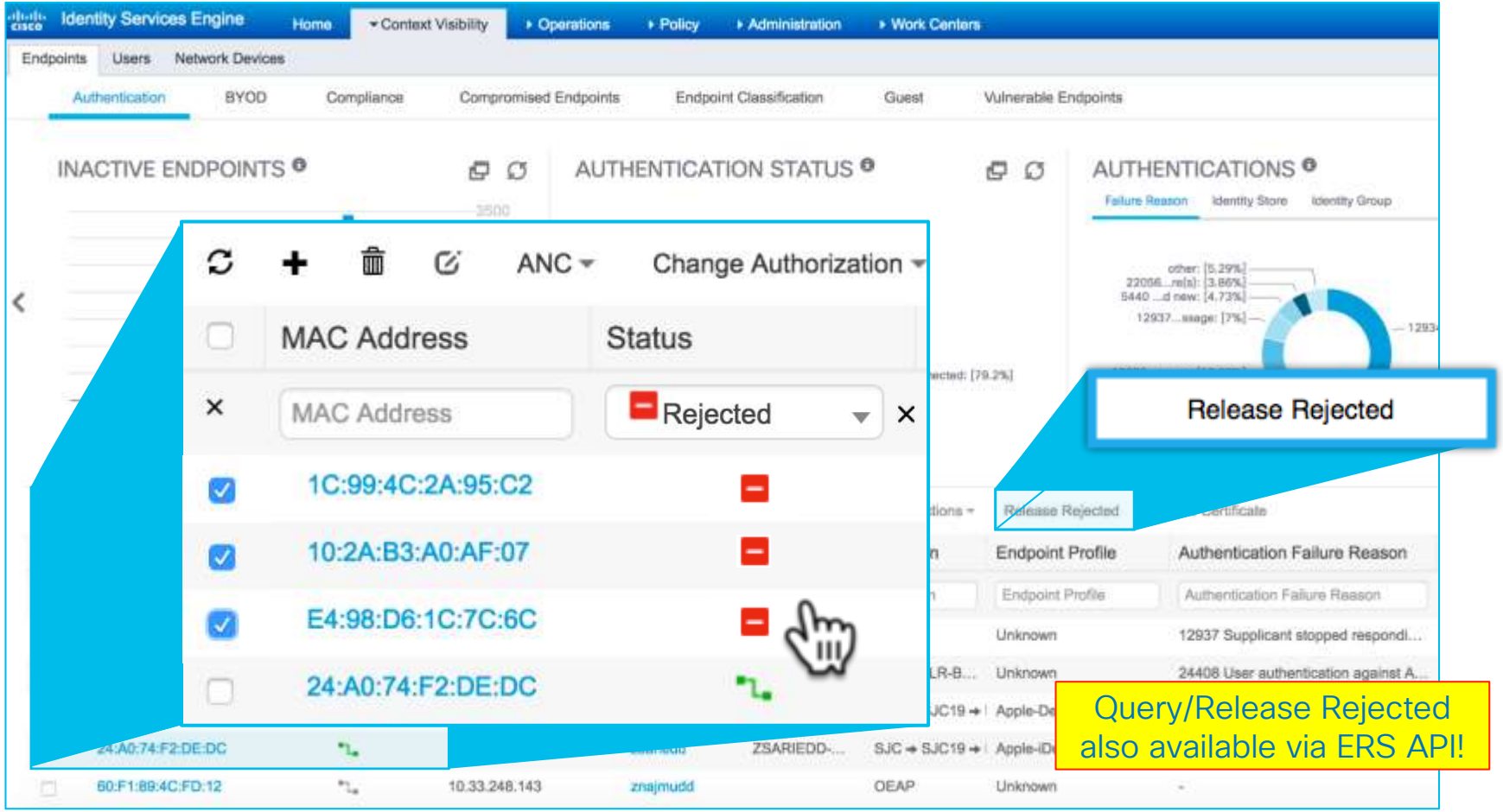
ANC | Change Authorization

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

Release Rejected | Revoke Certificate

Endpoint Profile	Authentication Failure Reason
Unknown	12937 Supplicant stopped respondi...
Unknown	24408 User authentication against A...
Apple-Device	12934 Supplicant stopped respondi...
Apple-iDevice	-
Unknown	-

Releasing Rejected Endpoints

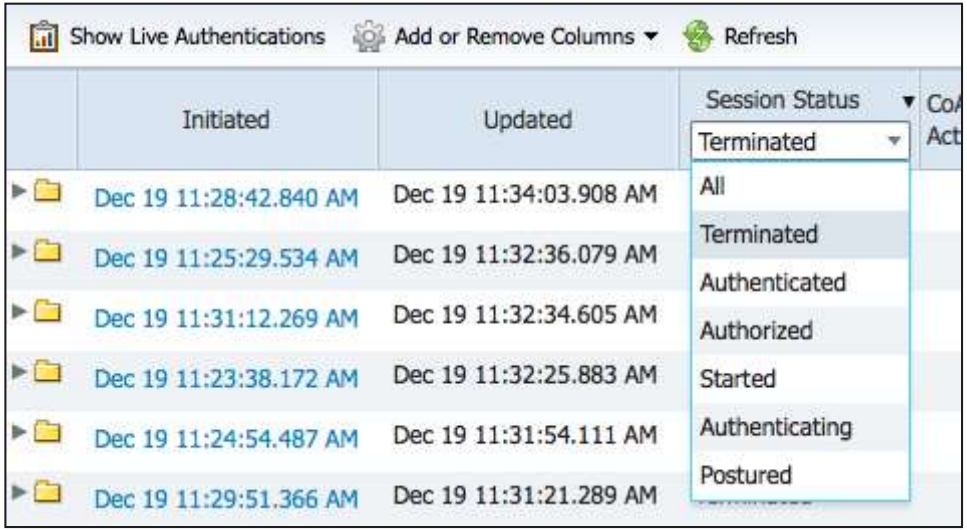


Sessions States

For Your Reference

Sessions can have one of 6 states as shown in the Live Sessions drop-down.

- NAD START --> Authenticating
- NAD SUCCESS --> Authorized
- NAD FAIL / ACCT STOP / AUTH FAIL --> Terminated
- POSTURED --> Postured
- AUTH PASS --> Authenticated
- ACCT START / UPDATE --> Started



The first two happen only for wired switchports with epm logging enabled and MnT nodes are configured to receive these logs via syslog from the NAD

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Clearing Stale ISE Sessions

For Your Reference

RADIUS Accounting is Primary method to maintain sessions – Start/Update/Stop!
If RADIUS Accounting not sent (or not received due to network or PSN load drops), ISE will rely on Session Purge operation to clear stale sessions

Automatic Purge: A purge job runs approximately every 5 minutes to clear sessions that meet any of the following criterion:

1. Endpoint **disconnected** (Ex: failed authentication) **in the last 15 minutes** (grace time allotted in case of authentication retries)
2. Endpoint **authenticated in last hour but no accounting start or update received**
3. Endpoint idle–**no activity** (auth / accounting / posturing / profiling updates) **in the last 5 days**

- Note: Session is cleared from MnT but does not generate CoA to prevent negative impact to connected endpoints. In other words, MnT session is no longer visible but it is possible for endpoint to still have network access, but no longer consumes license.

Manual Purge via REST API: HTTP DELETE API can manually delete inactive sessions.

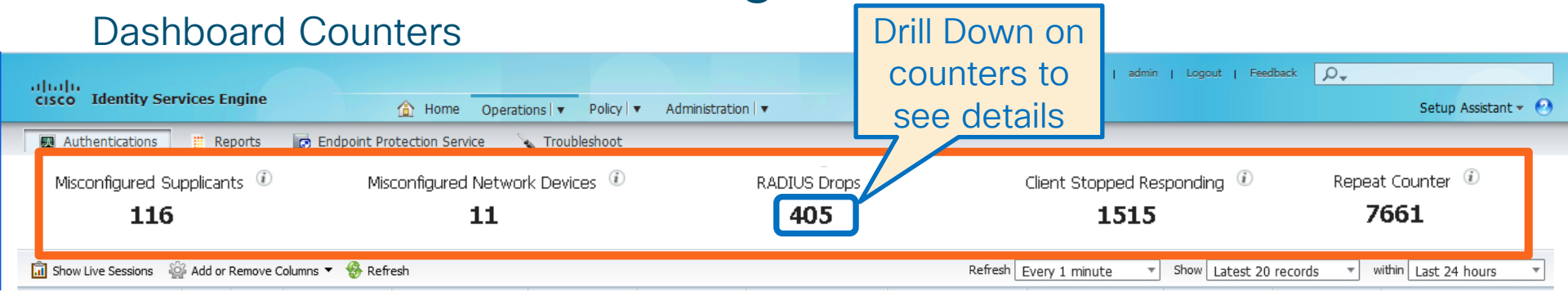
- An example web utility that supports HTTP DELETE operation is cURL. It is a free 3rd-party command line tool for transferring data with HTTP/HTTPS: http://www.cisco.com/en/US/docs/security/ise/1.2/api_ref_guide/ise_api_ref_ch2.html#wp1072950

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Live Authentications Log

Dashboard Counters

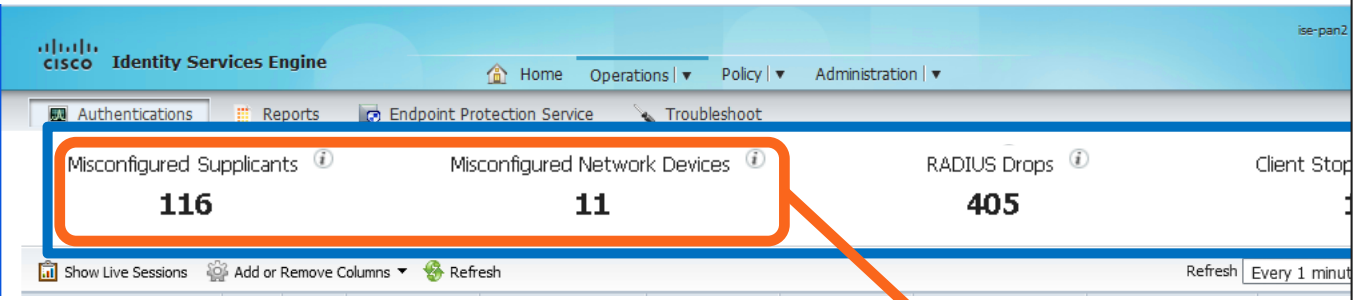


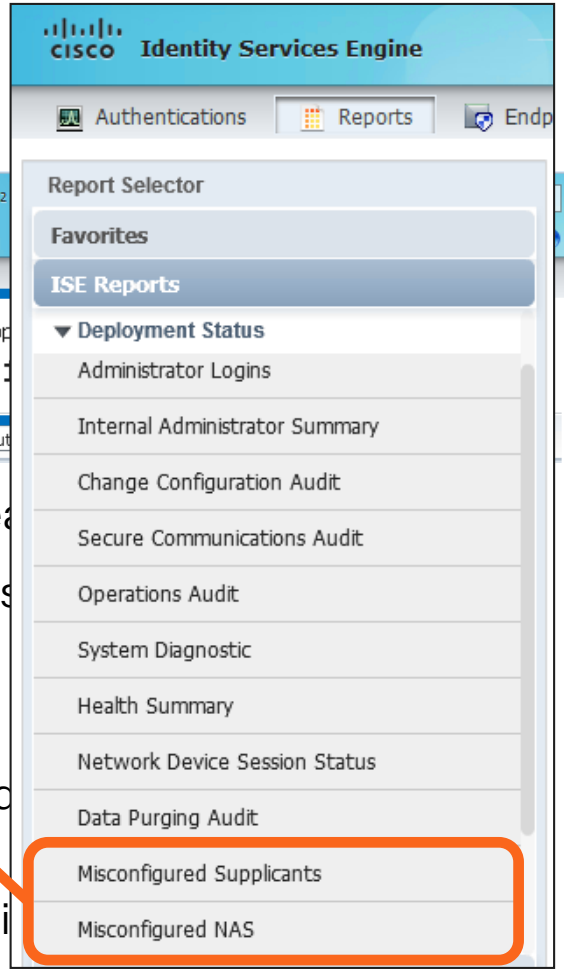
- **Misconfigured Supplicants:** Supplicants failing to connect repeatedly in the last 24 hours
- **Misconfigured Network Devices:** Network devices with aggressive accounting updates in the last 24 hours
- **RADIUS Drops:** RADIUS requests dropped in the last 24 hours
- **Client Stopped Responding:** Supplicants stopped responding during conversations in the last 24 hours
- **Repeat Counter:** Successful authentication requests repeated in the last 24 hours with no change in identity content, network device, and authorization.

Live Authentications Log

For Your Reference

Dashboard Counters



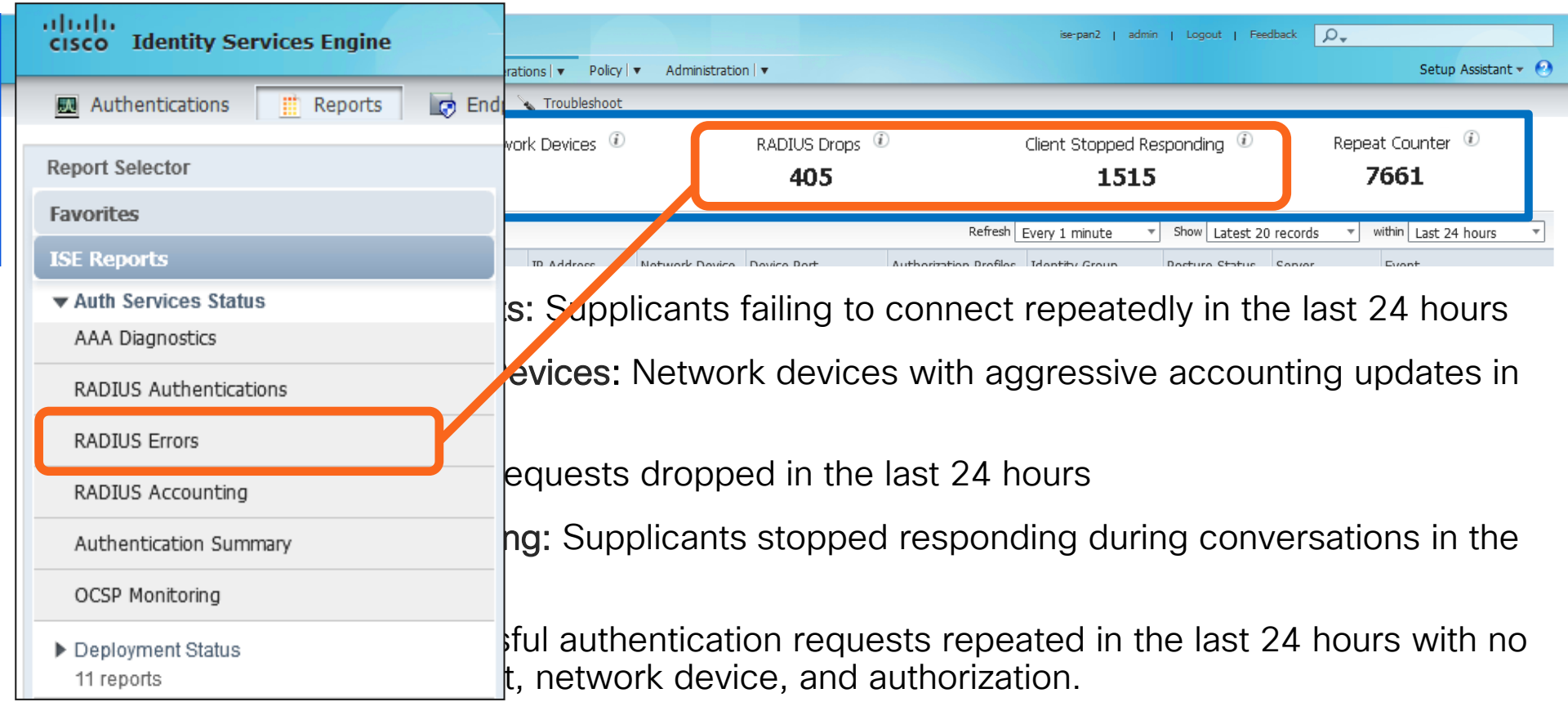


- **Misconfigured Supplicants:** Supplicants failing to connect repea
- **Misconfigured Network Devices:** Network devices with aggress the last 24 hours
- **RADIUS Drops:** RADIUS requests dropped in the last 24 hours
- **Client Stopped Responding:** Supplicants stopped responding c last 24 hours
- **Repeat Counter:** Successful authentication requests repeated i change in identity content, network device, and authorization.

Live Authentications Log

Dashboard Counters

For Your Reference



s: Supplicants failing to connect repeatedly in the last 24 hours

evices: Network devices with aggressive accounting updates in

equests dropped in the last 24 hours

ng: Supplicants stopped responding during conversations in the

sful authentication requests repeated in the last 24 hours with no
t, network device, and authorization.

Counters – Misconfigured Supplicants

Endpoints That Continuously Fail Authentication

For Your Reference

Identity Services Engine

Misconfigured Supplicants

Endpoint Details	Failure Reason	Failed Attempts	Resolution
Endpoint Id : 50:46:5D:19:1F:4F Username : baye Radius Username : baye Network Device Name : bxb22-11-alpha-wlc1 Access Type : Wireless#WLC Location : BXB NAS IP Address : 10.86.102.138	24408 User authentication against Active Directory failed since user has entered the wrong password	1	User authentication against Active Directory failed since user has entered the wrong password Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Endpoint Id : C4:71:FE:D7:1D:F5 Username : anonymous Radius Username : ajtdmw Network Device Name : WNBU_NGWC_OTA_22_SW1 Access Type : Wireless#WLC#NGWC Location : SJC#WNBU NAS IP Address : 10.34.149.5	24206 User disabled	1	User marked disabled in Internal database. Check whether the user account in Internal database is enabled
Endpoint Id : 80:60:07:07:5F:53 Username : ryhom Radius Username : ryhom Network Device Name : WNBU-WLC1 Access Type : Wireless#WLC Location : SJC#WNBU NAS IP Address : 10.32.34.2	12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate	1	PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Counters – Misconfigured NAS

Access Devices That Send Excessive or Invalid RADIUS Accounting

For Your Reference

Identity Services Engine

Misconfigured NAS

Network Device Ip	Failure Reason	Failed Attempts	Resolution
10.34.76.212	12929 NAS sends RADIUS accounting update messages too frequently	34180	NAS sends RADIUS accounting update messages too frequently Verify NAS configuration. Verify known NAS issues.
10.32.37.6	12929 NAS sends RADIUS accounting update messages too frequently	8014	NAS sends RADIUS accounting update messages too frequently Verify NAS configuration. Verify known NAS issues.
10.86.102.138	12929 NAS sends RADIUS accounting update messages too frequently	5330	NAS sends RADIUS accounting update messages too frequently Verify NAS configuration. Verify known NAS issues.
10.32.34.2	12929 NAS sends RADIUS accounting update messages too frequently	404	NAS sends RADIUS accounting update messages too frequently Verify NAS configuration. Verify known NAS issues.
10.34.80.38	11038 RADIUS Accounting-Request header contains invalid Authenticator field	8	ISE cannot validate the Authenticator field in the header of the RADIUS Accounting-Request packet. Note that the Authenticator field should not be confused with the Message-Authenticator RADIUS attribute. Ensure that the RADIUS Shared Secret configured on the AAA client matches that configured for the selected Network Device on the ISE server. Also, ensure that the AAA client has no hardware problems or problems with RADIUS compatibility.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Counters – RADIUS Drops

Duplicate Session Attempts, Undefined NAD, Secret Mismatch, Non-Conforming, Etc.

For Your Reference

Identity Services Engine

RADIUS Drops

Endpoint Details	Failure Reason	Failed Attempts	Resolution
Endpoint Id : 00:23:33:41:97:78 Username : Radius Username : mafan Network Device Name : WNBU-sjc14-00a-homeap1 Access Type : Wireless#WLC Location : OEAP NAS IP Address : 171.70.35.131	5441 Endpoint started new EAP session while the packet of previous EAP session is being processed. Dropping new session.	66	Endpoint started new EAP session while the packet of previous EAP session is being processed Verify known NAD or supplicant issues and published bugs. Verify NAD and supplicant configuration.
Endpoint Id : C4:71:FE:D7:1C:48 Username : Radius Username : ajtdmw Network Device Name : WNBU_NGWC_OTA_22_SW1 Access Type : Wireless#WLC#NGWC Location : SJC#WNBU NAS IP Address : 10.34.149.5	5441 Endpoint started new EAP session while the packet of previous EAP session is being processed. Dropping new session.	59	Endpoint started new EAP session while the packet of previous EAP session is being processed Verify known NAD or supplicant issues and published bugs. Verify NAD and supplicant configuration.
Endpoint Id : C4:71:FE:D7:16:3F Username : Radius Username : ajtdmw Network Device Name : WNBU_NGWC_OTA_KATANA1	5441 Endpoint started new EAP session while the packet of previous EAP session is being	53	Endpoint started new EAP session while the packet of previous EAP session is being processed Verify known NAD or supplicant issues and

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Counters – Clients Stopped Responding

Supplicants That Fail to Complete EAP Authentication

For Your Reference

Identity Services Engine

Clients Stopped Responding

Endpoint Details	Failure Reason	Failed Attempts	Resolution
Endpoint Id : 00:1B:D4:54:6E:7D Username : anonymous	12930 Supplicant stopped responding to ISE after sending it the first PEAP message	8329	Supplicant stopped responding to ISE after sending it the first PEAP message Verify that supplicant is configured properly to conduct a full EAP conversation with ISE. Verify that NAS is configured properly to transfer EAP messages to/from supplicant. Verify that supplicant or NAS does not have a short timeout for EAP conversation. Check the network that connects the Network Access Server to ISE.
Endpoint Id : 18:3D:A2:68:3D:80 Username : asengupt	24408 User authentication against Active Directory failed since user has entered the wrong password	3100	User authentication against Active Directory failed since user has entered the wrong password Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Endpoint Id : 00:1E:65:D6:93:E2 Username : anonymous	12110 PAC verification failed	1232	Received from the client a PAC that failed to pass verification. Verify that the client's supplicant is properly configured. Try restarting the client's supplicant service or the client's computer if necessary.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Counters – Repeat Count

Endpoint Tally of Successful Re-authentications

For Your Reference

Identity Services Engine

Repeat Count Details

Time Range: From 01/16/2014 02:49:50 PM to 01/17/2014 02:49:49 PM

Generated At: 2014-01-17 14:49:49.047

Repeat Count	Initiated	Updated	Session Time	Identity	Endpoint ID
16,748	Fri Jan 17 14:49:42 PST 2014	Fri Jan 17 14:49:44 PST 2014	2s	vjorge	D4:CA:6D:14:7D:7A
4,709	Fri Jan 17 14:49:22 PST 2014	Fri Jan 17 14:49:26 PST 2014	6s	vjorge	D4:CA:6D:14:84:A3
3,641	Fri Jan 17 09:09:49 PST 2014	Fri Jan 17 09:09:49 PST 2014	31d22h1m...	host/VINVERMA-WS	68:7F:74:EF:C7:E8
2,100	Mon Nov 11 12:36:57 PST 2013	Fri Jan 17 14:29:43 PST 2014	67d1h52m2s	00:50:60:08:55:8B	00:50:60:08:55:8B
1,704	Fri Jan 17 13:43:03 PST 2014	Fri Jan 17 14:32:55 PST 2014	3d9h37m35s	pausmit2	00:23:68:B2:74:3D
543	Fri Jan 17 14:48:56 PST 2014	Fri Jan 17 14:48:56 PST 2014	12s	zhlu	64:20:0C:3A:AB:8C

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Repeat Counter

Successful Authentication Suppression

For Your Reference

- Global Repeat Counter displayed in Live Authentications Log dashboard:

Repeat Counter
21587

- Session Repeat Counter displayed in Live Authentication and Sessions Log
  - Can reset counters for **all sessions** or **individual session**

Show Live Authentications | Add or Remove Columns | Refresh | Reset Repeat Counts

	Initiated	Updated	Session Status	CoA Action	Repeat Count	Endpoint ID	Identity	IP Address
			All					
▶	2013-04-05 05:09:15.652	2013-04-05 05:09:17.698	Started		9	7C:6D:62:E3:D5:05	employee1	10.1.40.100

- Be sure to enable display under “Add or Remove Columns”

Add or Remove Columns
- Reset to Default
- Show All Columns
- Initiated
- Updated
- Account Session Time
- Session Status
- CoA Action
- Repeat Count

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 1.2 Alarms

For Your Reference

- Alarms displayed as dashlet on ISE Home Page
  - Following alarms are added or enhanced in ISE 1.2
    - Misconfigured supplicant
    - Misconfigured NAS
    - Detect Slow Authentications
    - RADIUS Request Dropped with more accurate failure reasons
    - Excessive Accounting Messages
    - Mixing RADIUS Request between ISE PSN's due to NAD/LB behavior.

Alarms

Name	Occurrences	Last Occurred
Health Status Unavailable	352 times	less than 1 min ago
RADIUS Request Dropped	131 times	2 mins ago
High Load Average	1161 times	41 mins ago
EAP Connection Timeout	30 times	1 hr 48 mins ago
License Expiration	140 times	2 hrs 4 mins ago
Authentication Inactivity	151 times	2 hrs 46 mins ago
Configuration Changed	2333 times	7 hrs 5 mins ago

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Minimize Syslog Load on MNT

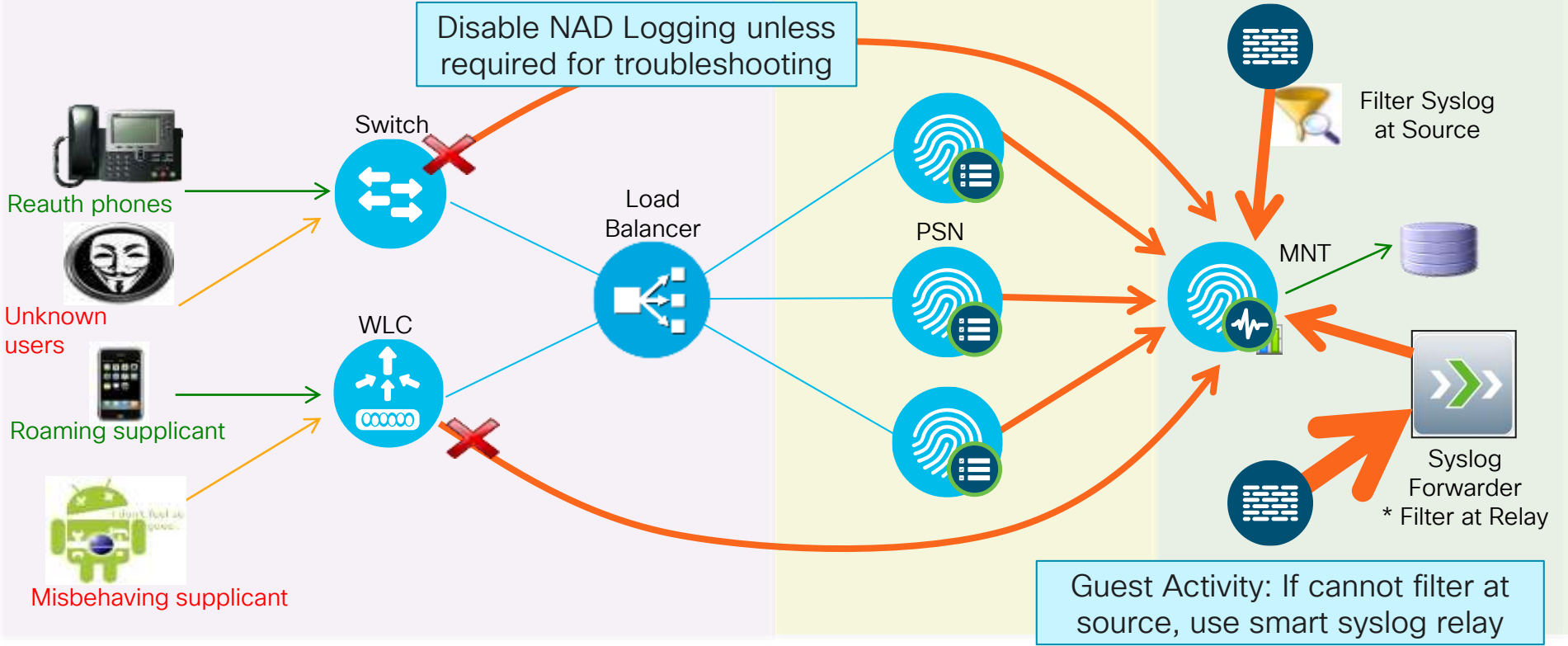
Disable NAD Logging and Filter Guest Activity Logging

For Your Reference

Rate Limiting at Source

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

Disable NAD Logging unless required for troubleshooting



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

NAD Logging

Disable by Default

For Your Reference

- Recommended enable for troubleshooting purposes only.
- If logging configured, the correct commands should include….

```
!
epm logging
logging origin-id                # where origin-id = IP address A.B.C.D
logging source-interface <interface-id>
                                 # where interface-id IP address = A.B.C.D
logging host <MNT1> transport udp port 20514
logging host <MNT2> transport udp port 20514
                                 # Optional for redundancy, but not
!                                required for troubleshooting purposes
```

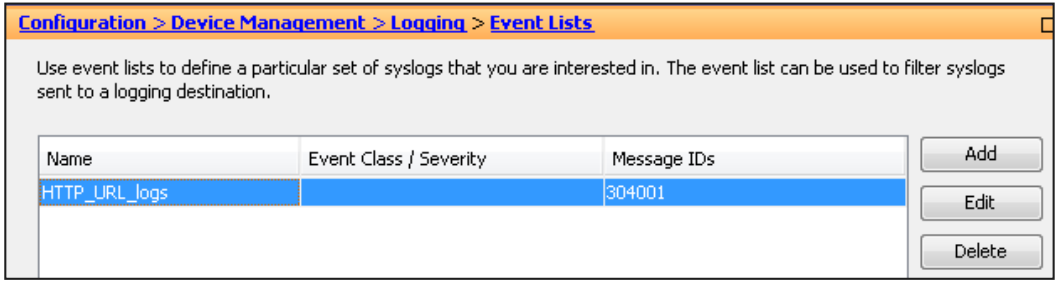

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Guest Activity Logging

For Your Reference

Enable with purpose—only send logs of interest that apply to guest sessions.

ISE only parses log messages that include IP address of active guest account



ASA Example:

- Create Service Policy to inspect HTTP traffic for guest subnet
- Filter messages ID # 304001: accessed URLs

Log Filtering:

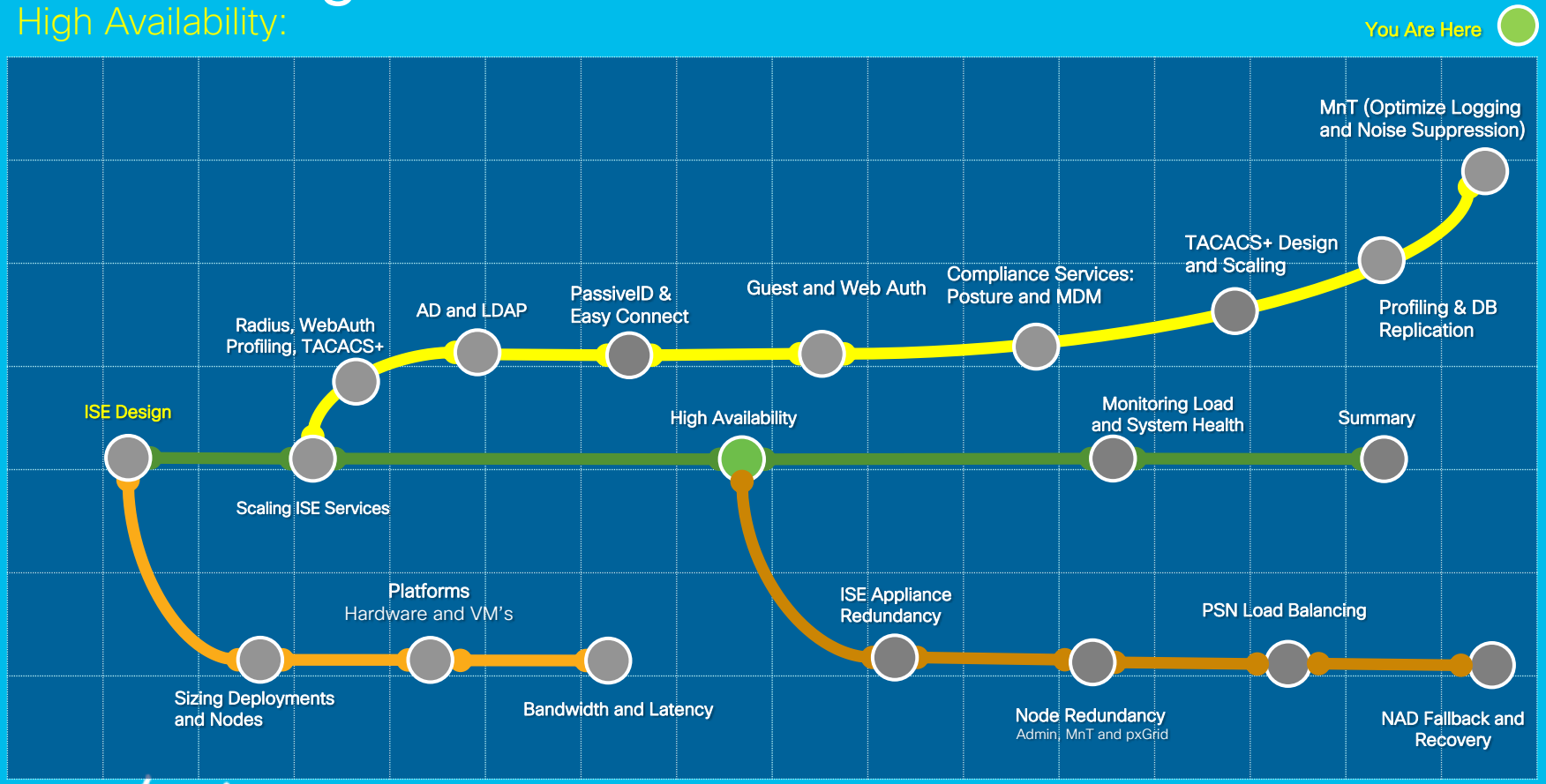
- If NAD supports, configure filters to limit logs only to those needed/usable by MnT.
- If unable to filter at NAD, use Syslog Relay to filter and forward desired messages.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Availability

Session Agenda

High Availability:



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Availability Agenda

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Critical Services

External Services that can impact the Health of your ISE Deployment

For Your Reference

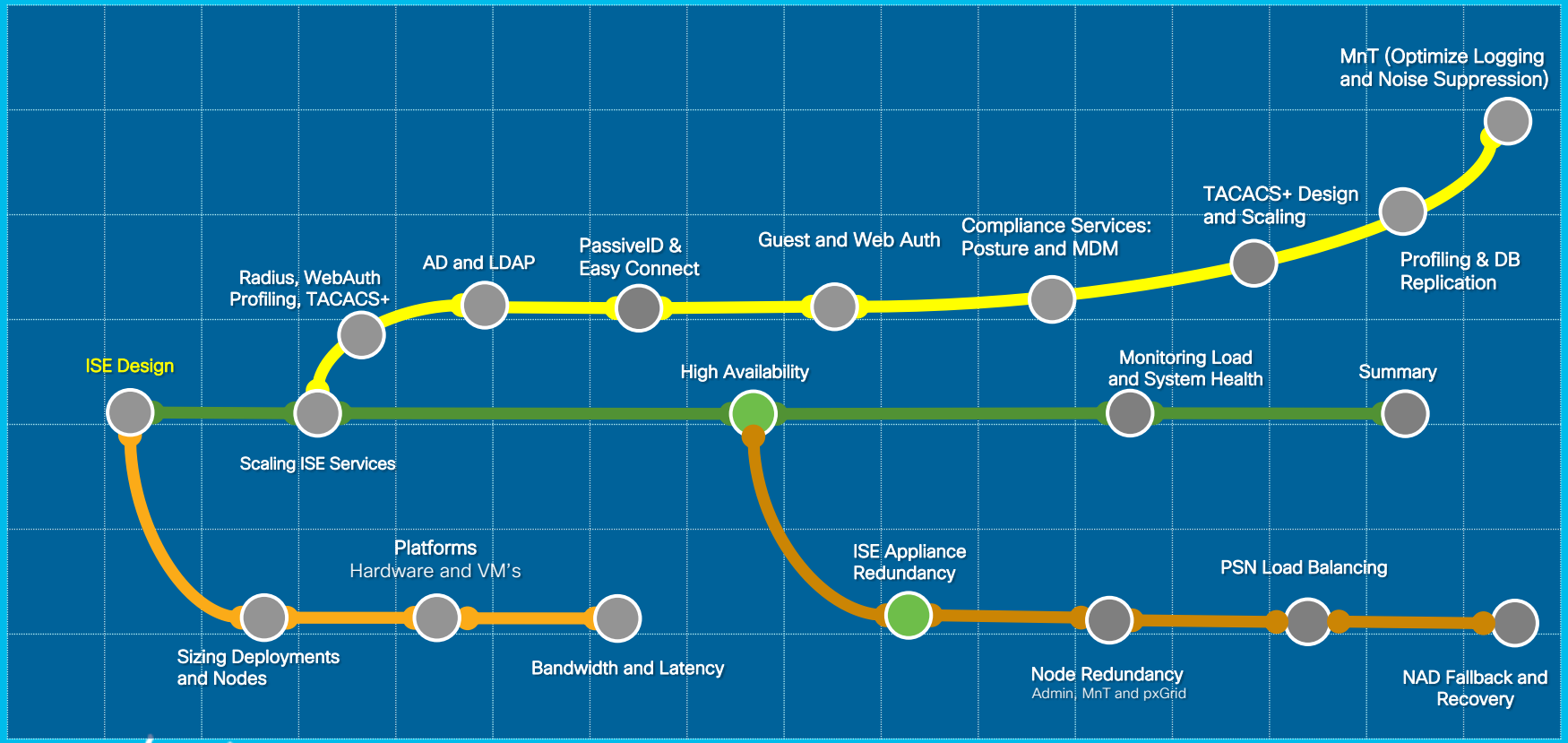
- DNS and NTP
- Certificate Services: CA, OCSP/CRL Servers
- ID Stores (AD, LDAP, ODBC, OTP, SAML/IdP, external RADIUS)
- Compliance Servers (MDM/EMM, Posture Remediation, Patch Managers, etc)
- TC-NAC: Threat and Vulnerability Assessment services
- Feed Services – (Posture, Profiling, Licensing)
  - Rely on Proxy? Offline packages required?
- SMTP for guest/admin notification
- Data Repositories (FTP, SCP, HTTP)
- Load Balancers front-ending ISE services

HA for services external to ISE is outside the scope of this session, but be aware of potential impact from single points of failure or performance bottlenecks in any component of the system.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Agenda

High Availability: ISE Appliance Redundancy



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Appliance Redundancy

Appliance Redundancy

In-Box High Availability

SNS-3500 Series

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

EOL/EOS

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Appliance Redundancy

In-Box High Availability

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NIC Redundancy Update

NIC Teaming / Interface Bonding

For Your Reference

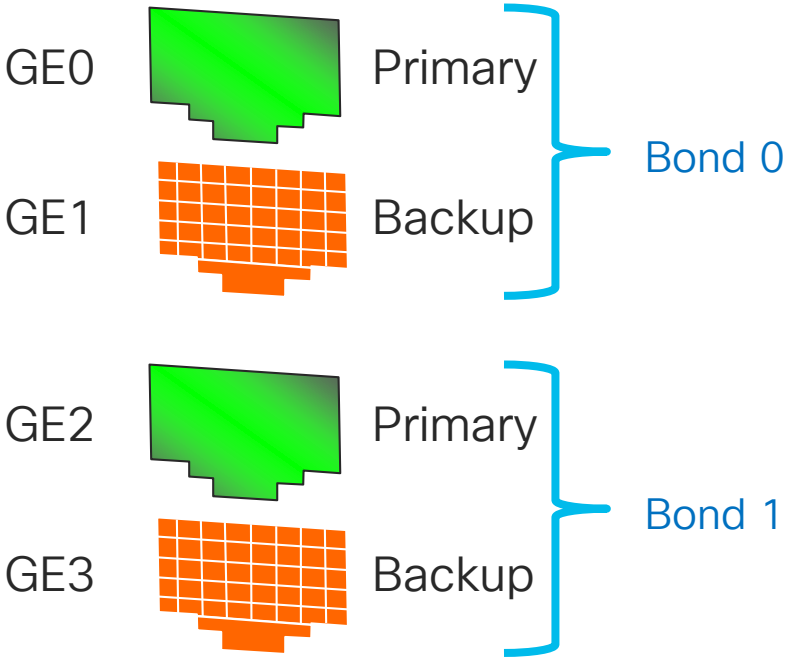
- For Redundancy only – NOT a Performance and Scale feature in 2.1.
- Allows one interface to serve as a hot backup for another primary interface.
- Up to (3) bonds in ISE 2.1. [Up to (6) Network Interfaces supported in ISE 2.0]
- NIC Teaming pairs specific interfaces into Bonded interfaces

Individual Interfaces	Bonded Interfaces	Comments
Gigabit Ethernet 0	Bond 0	GE 0 is primary, GE 1 is backup
Gigabit Ethernet 1		
Gigabit Ethernet 2	Bond 1	GE 2 is primary, GE 3 is backup
Gigabit Ethernet 3		
Gigabit Ethernet 4	Bond 2	GE 4 is primary, GE 5 is backup
Gigabit Ethernet 5		

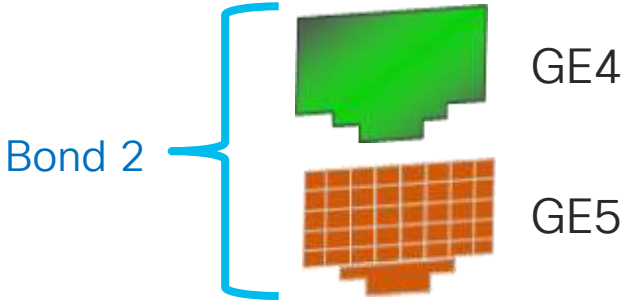
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NIC Teaming

Network Card Redundancy



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

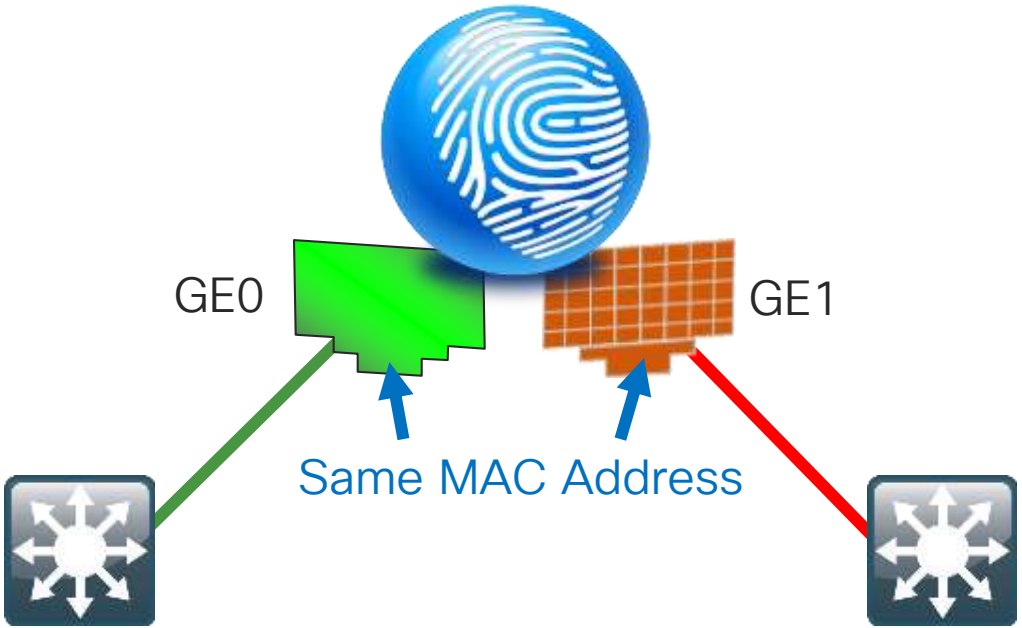


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NIC Teaming Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over

For Your Reference

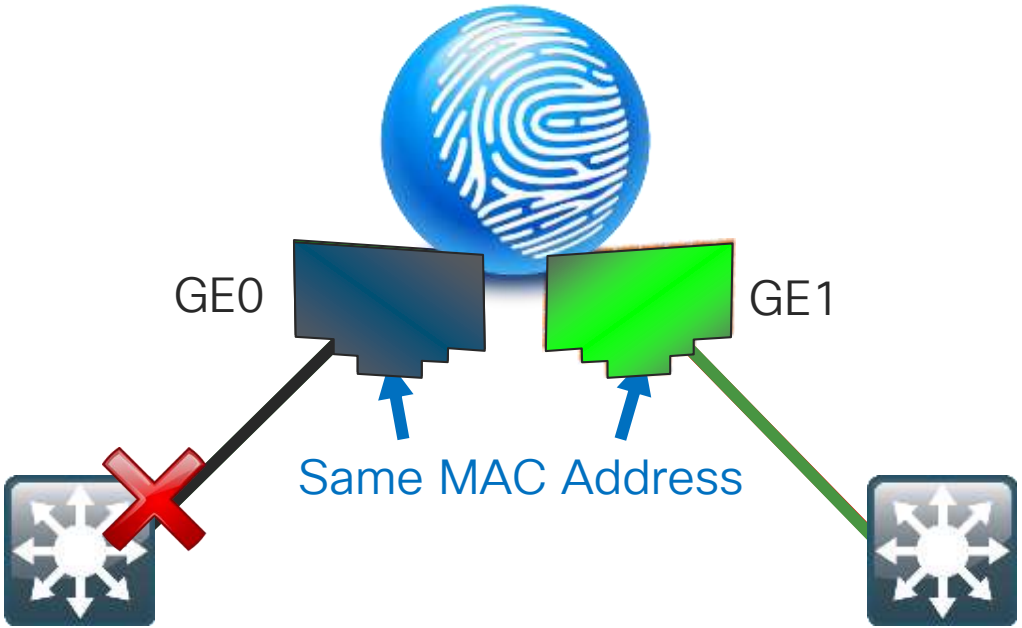


- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NIC Teaming Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over



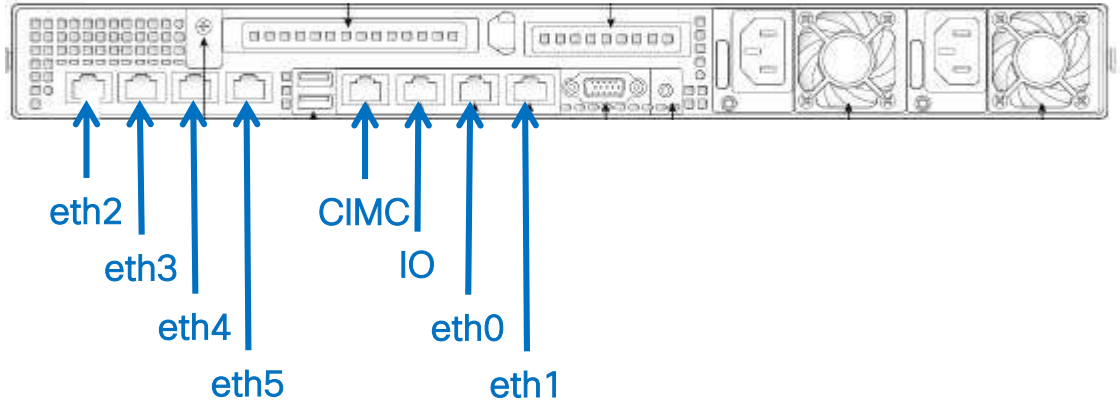
- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

NIC Teaming

- Bond 0 = eth0 + eth1
- Bond 1 = eth2 + eth3
- Bond 2 = eth4 + eth5



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configured at the CLI

Add the Backup Interface to the Primary Interface Configuration

For Your Reference

```
ise-psn1/admin(config-GigabitEthernet)# do sho int
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST>  mtu 1500
        inet 10.1.100.245  netmask 255.255.255.0  broadcast 10.1.100.255
        inet6 fe80::250:56ff:feb8:783b  prefixlen 64  scopeid 0x20<link>
        inet6 2001:db8::250:56ff:feb8:783b  prefixlen 64  scopeid 0x0<global>
        inet6 2001:db8::856d:cd6d:e5a3:155f  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b8:78:3b  txqueuelen 0  (Ethernet)
        RX packets 9102447  bytes 4493061475 (4.1 GiB)
        RX errors 0  dropped 48852  overruns 0  frame 0
        TX packets 7634687  bytes 1939631607 (1.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST>  mtu 1500
        ether 00:50:56:b8:78:3b  txqueuelen 1000  (Ethernet)
        RX packets 9030026  bytes 4449311176 (4.1 GiB)
        RX errors 0  dropped 20  overruns 0  frame 0
        TX packets 7634687  bytes 1939631607 (1.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST>  mtu 1500
        ether 00:50:56:b8:78:3b  txqueuelen 1000  (Ethernet)
        RX packets 72421  bytes 43750299 (41.7 MiB)
        RX errors 0  dropped 48832  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- IP on Bond Only
- Shared MAC Address

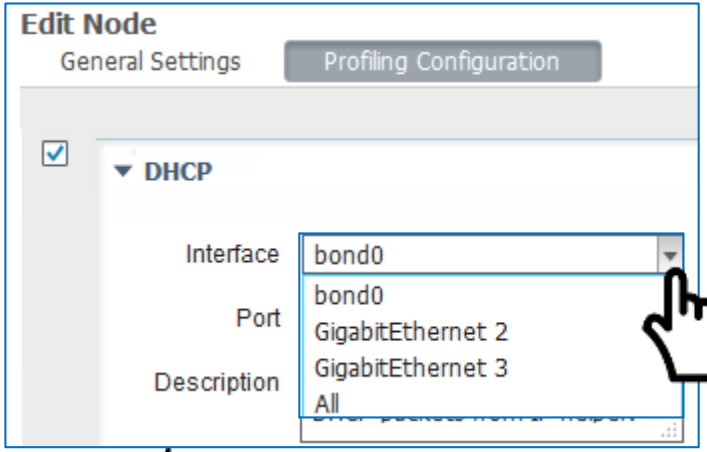
- No IP address on Physical Interface
- Same MAC Address

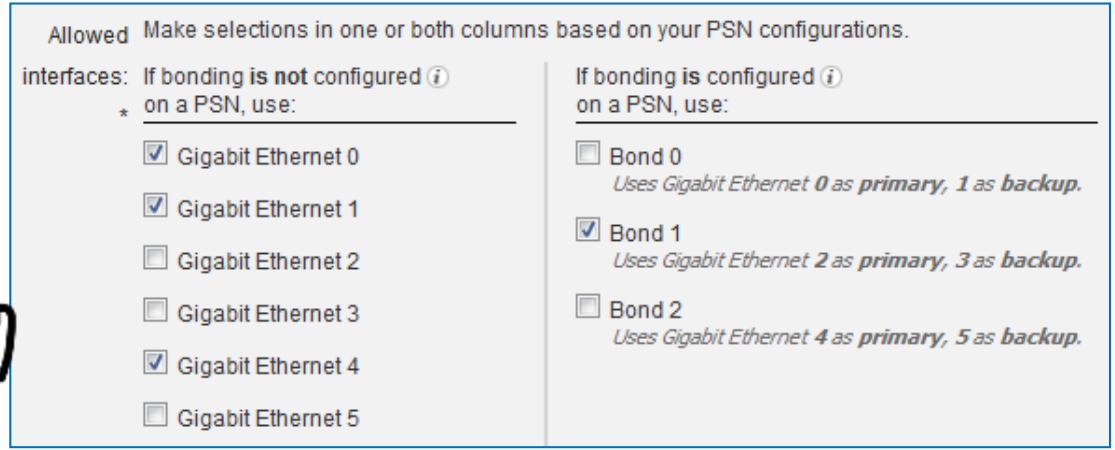
NIC Teaming

NIC Teaming / Interface Bonding

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

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





© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debugging NIC Bonding

For Your Reference

To help debug the assignment of interfaces to a portal on individual PSNs, detailed log messages are written to /opt/CSCOcpm/logs/guest.log on each node.

- Example

```
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces specified in the portal settings: [eth0]
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces on this node: [bond0, eth2, eth3]
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces from portal settings that are available on this node: []
INFO  [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interface eth0 is selected for portal 'Hotspot Guest Portal (default)', but eth0 and eth1 are bonded together as interface bond0, so the portal cannot listen on eth0 alone. However, since bond0 is not selected for this portal, the bonded interface will not be used.
```

- Another example:

```
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces specified in the portal settings: [eth0, bond0]
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces on this node: [bond0, eth2, eth3]
DEBUG [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces from portal settings that are available on this node: [bond0]
INFO  [localhost-startStop-1][] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interface eth0 is selected for portal 'Hotspot Guest Portal (default)', but eth0 and eth1 are bonded together as interface bond0, so the portal cannot listen on eth0 alone. Since bond0 is also selected for this portal, the bonded interface will be used instead.
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Virtual Appliance High Availability

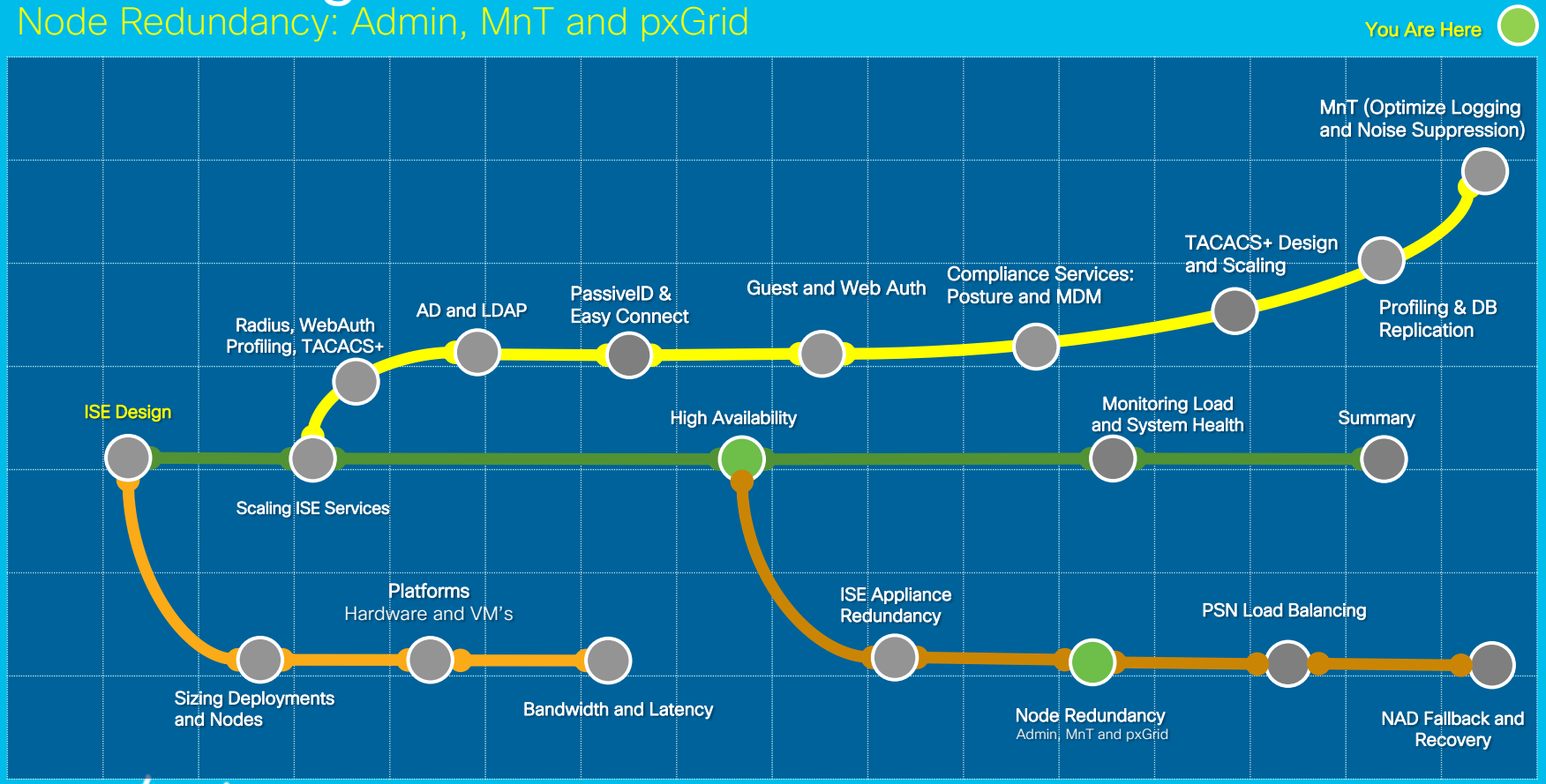
- EtherChannel and other VM Host redundancy features should be transparent to ISE running as VM Guest
- VMotion officially supported since ISE 1.2, but issues seen with live Snapshots and VMotion therefore not recommend
- Live snapshots <u>not</u> recommended as an ISE backup strategy. There is no quiescing of database. If snapshots used:
  - Shut down ISE server prior to taking snapshot.
  - Can be used in advance of upgrades; once upgrade successful, delete snapshot
  - Leverage ISE Backup services and store to remote device to create data archives
  - Optionally log data to external loggers/SIEMs for log redundancy or longer term retention.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Node/Persona Redundancy

Session Agenda

Node Redundancy: Admin, MnT and pxGrid



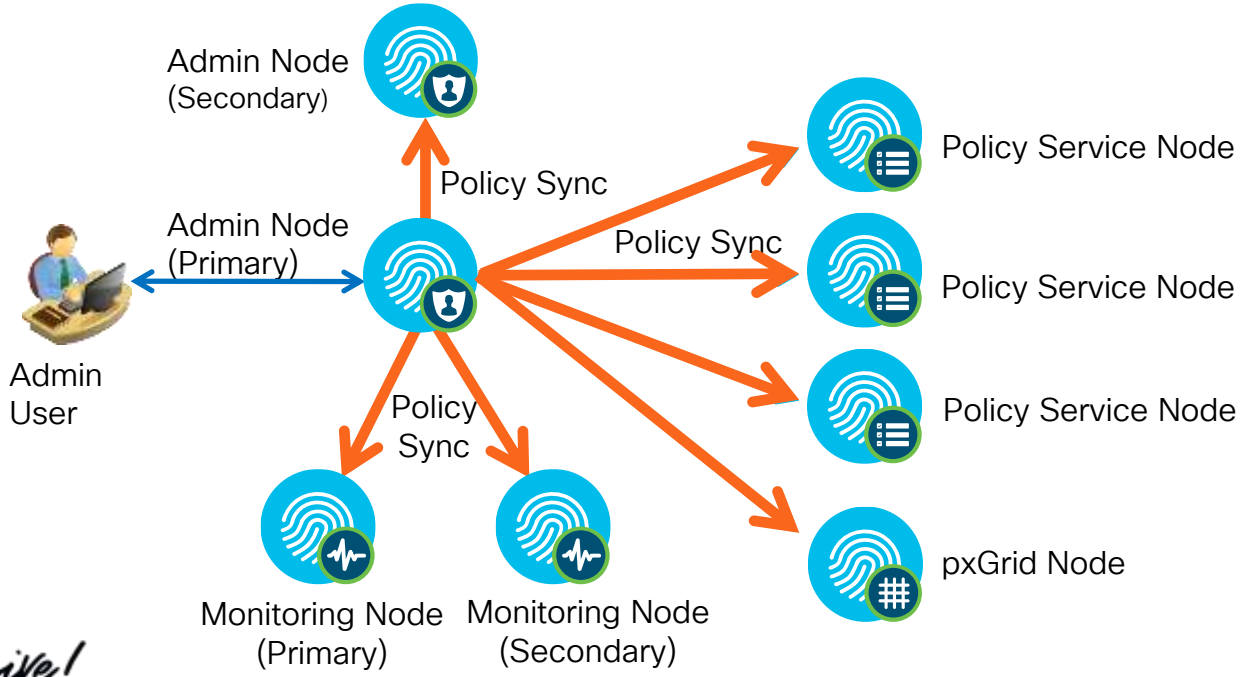
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Admin Node HA and Synchronization

- Maximum two PAN nodes per deployment
- Active / Standby

PAN Steady State Operation

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



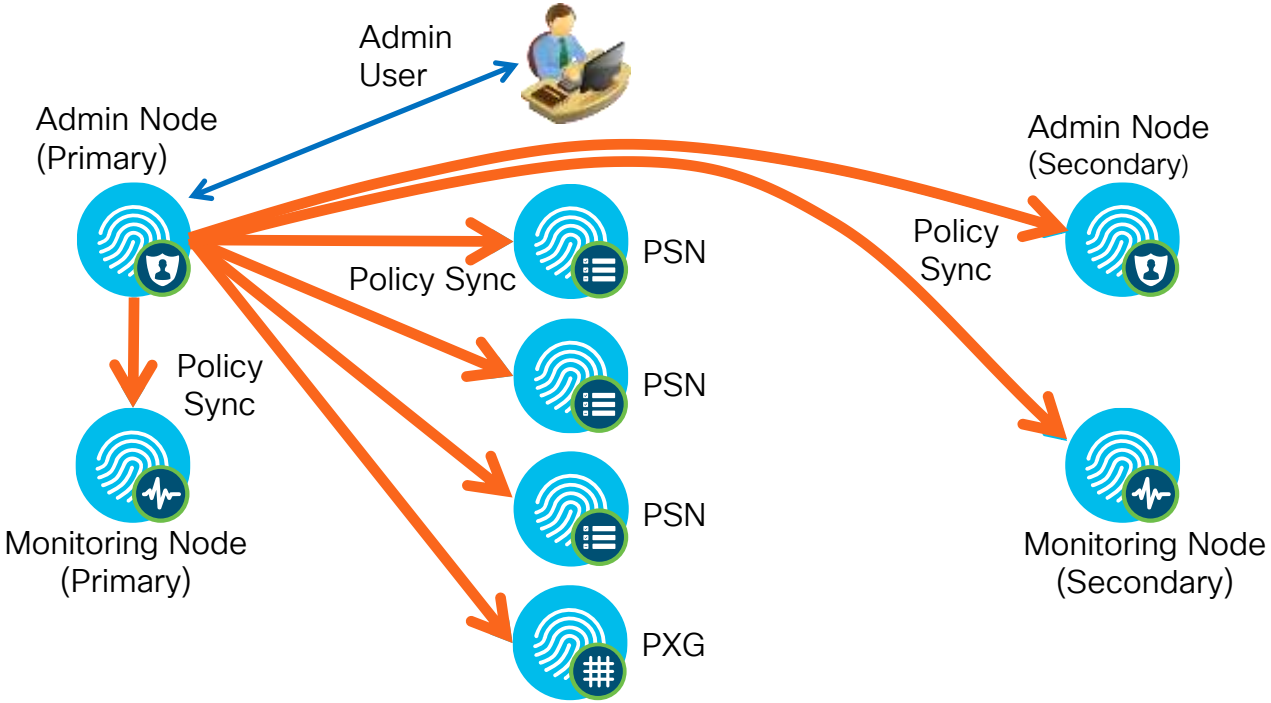
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Admin Node HA and Synchronization

PAN Steady State Operation

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

- Maximum two PAN nodes per deployment
- Active / Standby



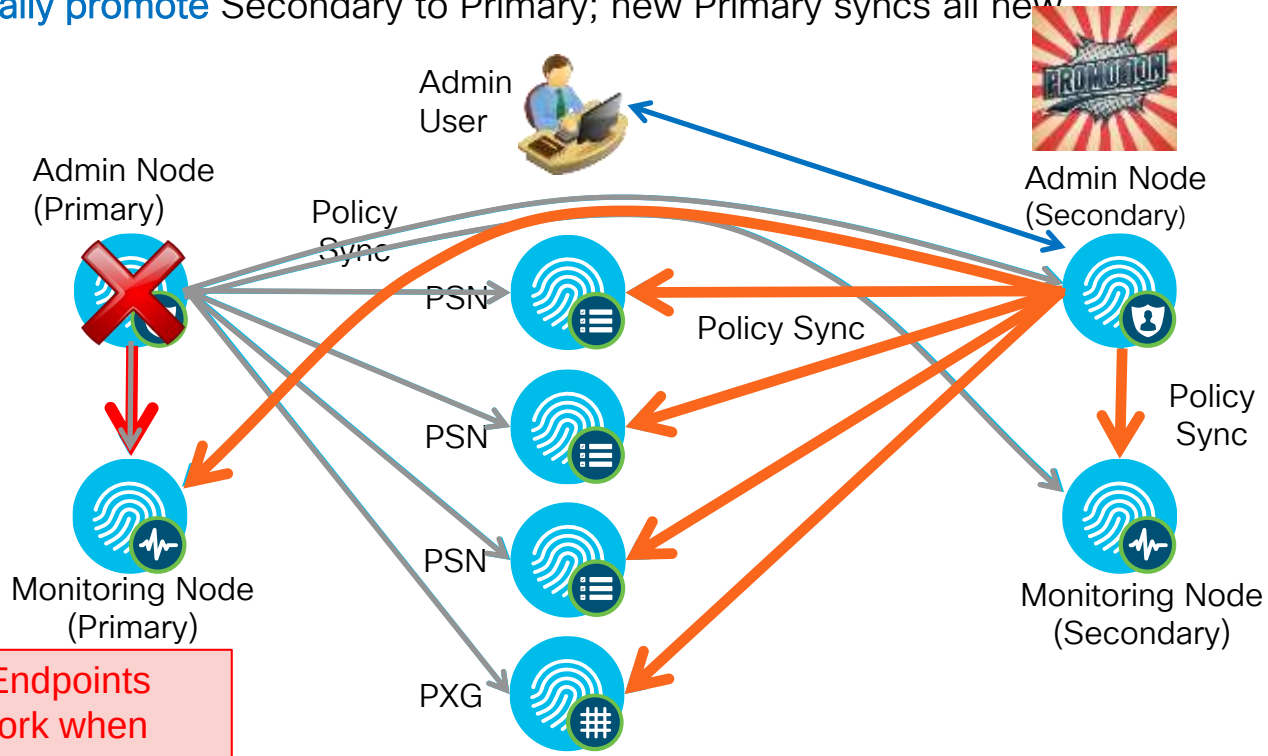
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Admin Node HA and Synchronization

Primary PAN Outage and Recovery

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

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



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Service Survivability When Admin Down/Unreachable

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

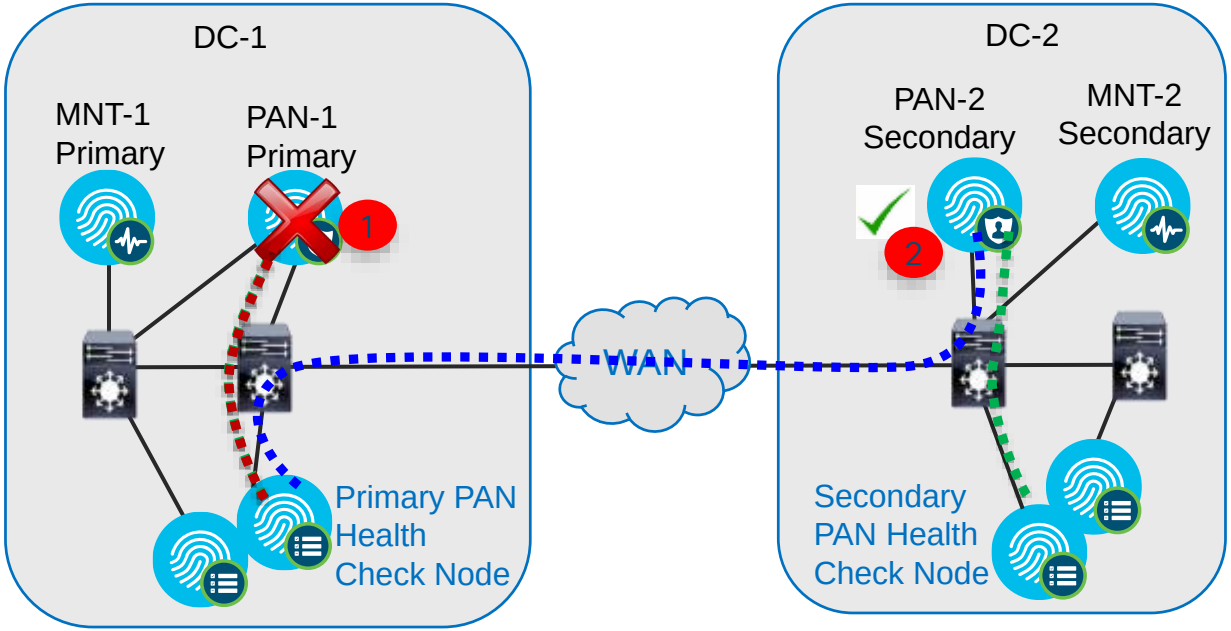
Service	Use case	Works (Y / N)
RADIUS Auth	Generally all RADIUS auth should continue provided access to ID stores	Y
Guest	All existing guests can be authenticated, but new guests, self-registered guests, or guest flows relying on device registration will fail.	N
Profiler	Previously profiled endpoints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

Automatic PAN Switchover

Introduced ISE 1.4

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

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



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Admin Failover

“Automated Promotion/Switchover”

For Your Reference

- Primary PAN and secondary PAN can be in different subnets/locations
- Secondary nodes close to the respective PANs act as their health monitors
- Health Monitors:
  - Maximum 2; Could be same node (recommend 2 if available)
  - Requires distributed deployment.
  - Can be any node—other than Admin node (or same node where Admin persona present)
  - Recommend node(s) close to PAN to be monitored to differentiate between local versus broader network outage, but should not be on SAME server if virtual appliance.
- Monitor Process:
  - Secondary node monitoring the health of the Primary PAN node is the Active monitor
  - On Failure detection, Health Monitor for Primary PAN node initiates switchover by sending request to the Secondary PAN to become new primary PAN

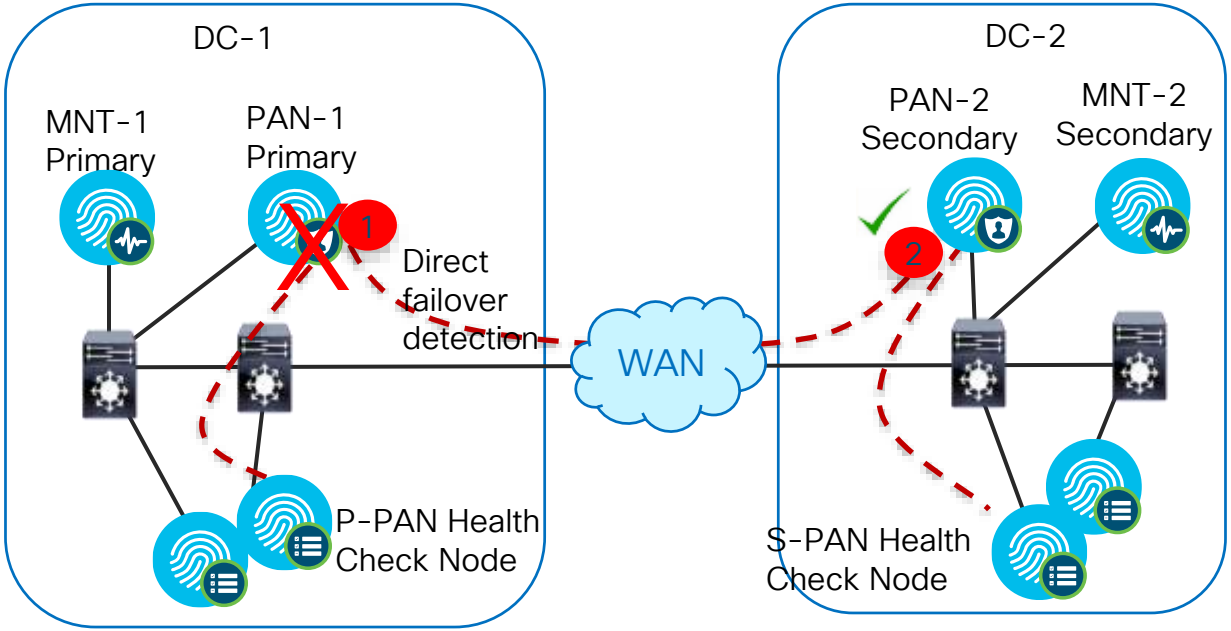
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAN Failover Scenario

Scenario 1

For Your Reference

- Primary PAN (PAN-1) down
- Secondary PAN (PAN-2) takes over



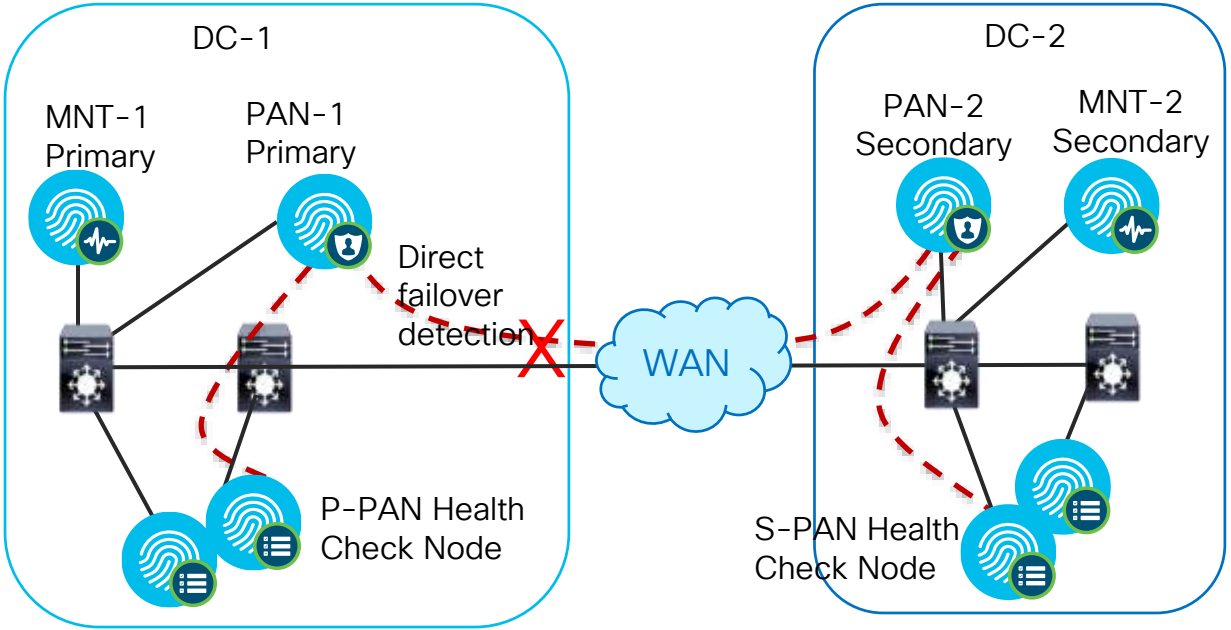
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAN Failover Scenario

Scenario 2

For Your Reference

- Connection between Primary PAN and Secondary PAN is down.
- Connection between PAN and Health Check Node is up
- Direct Failover detection between PANs will cause false switchover and data out of sync
- Using an external monitor can avoid false switchover



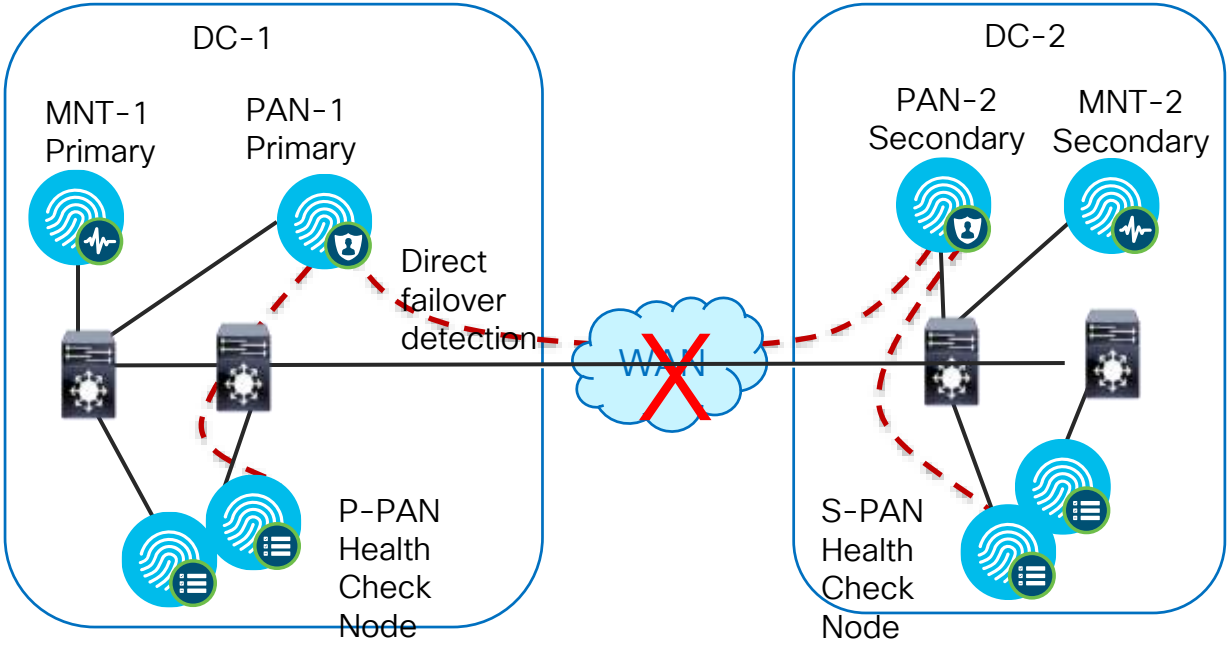
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAN Failover Scenario

Scenario 3

For Your Reference

- Connectivity between the data centers is down
- Complete network split
- Cannot be handled by PAN Failover
- Local WAN survivability required



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAN Failover

Health Check Node Configuration

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

cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service

Deployment | Licensing | Certificates | Logging | Maintenance | Backup & Restore | Admin Access | Settings

Deployment

- Deployment
  - bxb22-11a-pdp1
  - npf-sjca-ipep01
  - npf-sjca-ipep02
  - npf-sjca-mnt01
  - npf-sjca-mnt02
  - npf-sjca-pap01
  - npf-sjca-pap02
  - sbg-bgla-pdp01
  - AlphaNodeGroup
  - PAN Failover

PAN Failover Configuration

Automatic Failover if Primary Administration node goes down.

* Enable PAN Auto Failover	☑		
* Primary Health Check Node	npf-sjca-mnt01.cisco.com	Primary Administration Node	npf-sjca-pap01.cisco.com
* Secondary Health Check Node	npf-sjca-mnt02.cisco.com	Secondary Administration Node	npf-sjca-pap02.cisco.com
* Polling Interval	120	Seconds (Range 30 - 300)	
* Number Of Failure Polls Before Failover	5	Count (Range 2 - 60)	

Save | Reset

Health Check Node CANNOT be a PAN !!

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

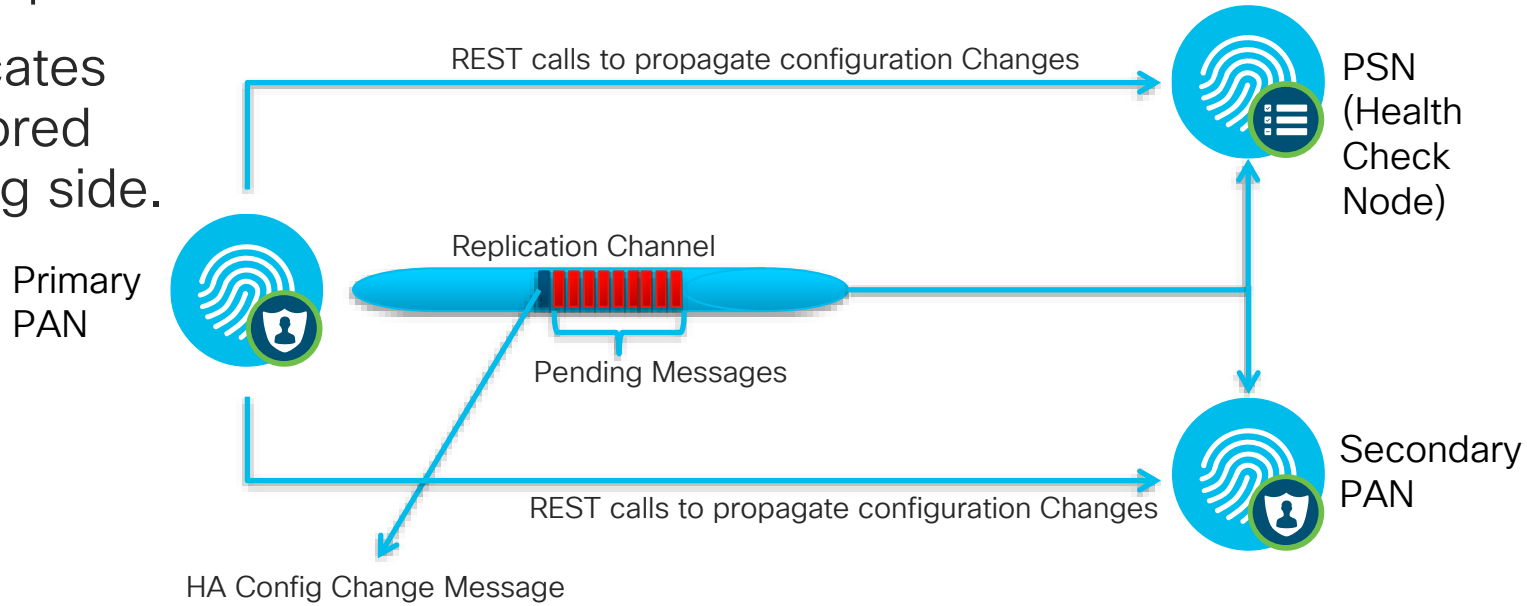
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

HA Config Changes Sent via Instant Relay

ISE 2.1+

For Your Reference

- High priority HA Configuration messages sent via REST *in addition to* standard replication channel
- Any duplicates safely ignored at receiving side.



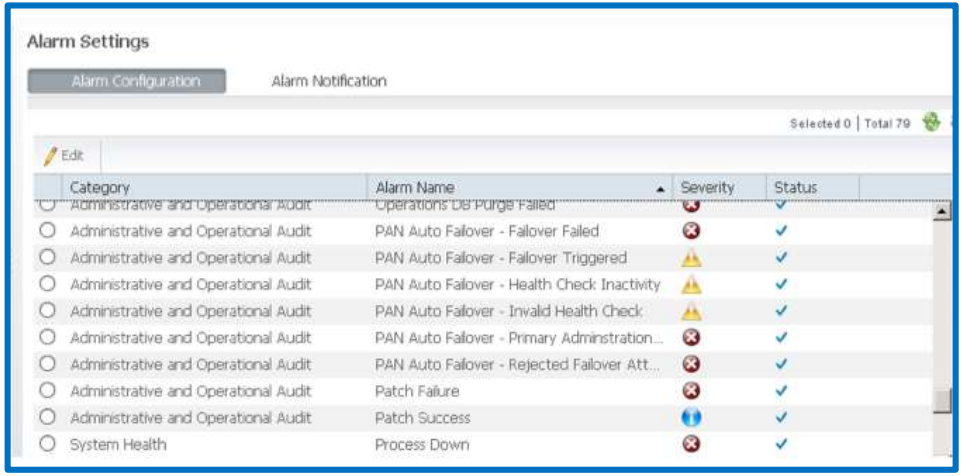
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Alarms in PAN Auto-Failover

For Your Reference

Critical Alarms

- Health check node finds primary PAN down
- Health check node makes a promotion call to secondary PAN
- Health check node is not able to make promotion request to secondary PAN
- Secondary PAN rejects the promotion request made by the health check node



Category	Alarm Name	Severity	Status
Administrative and Operational Audit	Operations DB Purge Failed		
Administrative and Operational Audit	PAN Auto Failover - Failover Failed		
Administrative and Operational Audit	PAN Auto Failover - Failover Triggered		
Administrative and Operational Audit	PAN Auto Failover - Health Check Inactivity		
Administrative and Operational Audit	PAN Auto Failover - Invalid Health Check		
Administrative and Operational Audit	PAN Auto Failover - Primary Adminstration...		
Administrative and Operational Audit	PAN Auto Failover - Rejected Failover Att...		
Administrative and Operational Audit	Patch Failure		
Administrative and Operational Audit	Patch Success		
System Health	Process Down		

Warning Alarms

Invalid auto-failover monitoring

- Mostly because health check node is out of sync
- PAN Auto-failover is disabled but primary PAN is receiving health check probes
- Primary PAN receives health probes from invalid health check node
- Secondary PAN info with the health check node is not correct
- Node receiving the health probe says it is not the correct primary PAN node

No health-check probes received

- Primary PAN does not receive the health check probes though it is configured

Promotion of secondary PAN is called by the health check node

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAN Auto-Failover Alarm Details

For Your Reference

Drill down on specific alarm to get Detailed Alarm information in a new page

Name	Occurrences	Last Occurred
PAN Auto Failover - Failover Trig...	3 times	less tha 1 m...
PAN Auto Failover - Primary Adm...	8 times	1 min ago
Configuration Changed	63 times	4 mins ago
ISE Authentication Inactivity	66 times	19 mins ago

cisco Identity Services Engine

Alarms: PAN Auto Failover - Primary Adminstration Node Down

Description:
Primary administration node is down or is not reachable from its health check node

Suggested Actions:
Bring up the Primary administration node or wait for failover to happen

Acknowledge Refresh

Time Stamp	Description
Apr 16 2015 17:23:31.884 PM	Unable to communicate to the Primary administration node ise-1.demo.local
Apr 08 2015 22:16:29.331 PM	Unable to communicate to the Primary administration node ise-2.demo.local
Apr 08 2015 18:53:46.226 PM	Unable to communicate to the Primary administration node ise-1.demo.local
Apr 07 2015 23:44:16.755 PM	Unable to communicate to the Primary administration node ise-1.demo.local
Apr 07 2015 23:19:18.412 PM	Unable to communicate to the Primary administration node ise-2.demo.local
Apr 07 2015 19:10:14.752 PM	Unable to communicate to the Primary administration node ise-2.demo.local
Apr 07 2015 18:59:04.811 PM	Unable to communicate to the Primary administration node ise-2.demo.local
Apr 07 2015 18:28:24.751 PM	Unable to communicate to the Primary administration node ise-2.demo.local

cisco Identity Services Engine

Alarms: PAN Auto Failover - Failover Triggered

Description:
Successfully triggered the promotion of the secondary administration node to primary role.

Suggested Actions:
Wait for promotion of secondary administration node to complete and bring up the old primary administration node.

Acknowledge Refresh

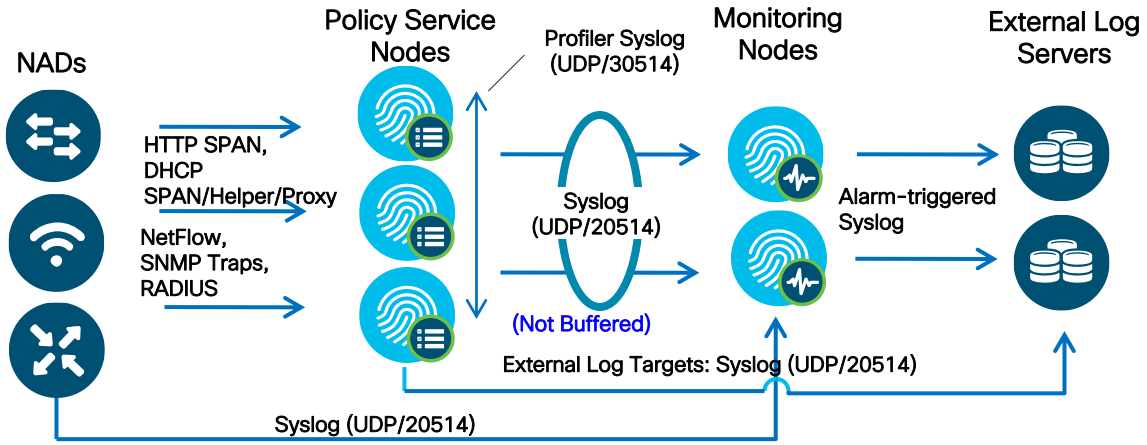
Time Stamp	Description
Apr 16 2015 17:24:39.133 PM	Promotion call made to PAN ise-2.demo.local successfully
Apr 08 2015 18:55:09.393 PM	Promotion call made to PAN ise-2.demo.local successfully
Apr 07 2015 23:30:25.201 PM	Promotion call made to PAN ise-1.demo.local successfully

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MnT Distributed Log Collection

For Your Reference

- ISE supports distributed log collection across all nodes to optimize local data collection, aggregation, and centralized correlation and storage.
- Each ISE node collects logs locally from itself; Policy Service nodes running Profiler Services may also collect log (profile) data from NADs.
- Each node transports its Audit Logging data to each Monitoring node as Syslog—these logs are not buffered unless use TCP/Secure Syslog
- NADs may also send Syslog directly to Monitoring node on UDP/20514 for activity logging, diagnostics, and troubleshooting.

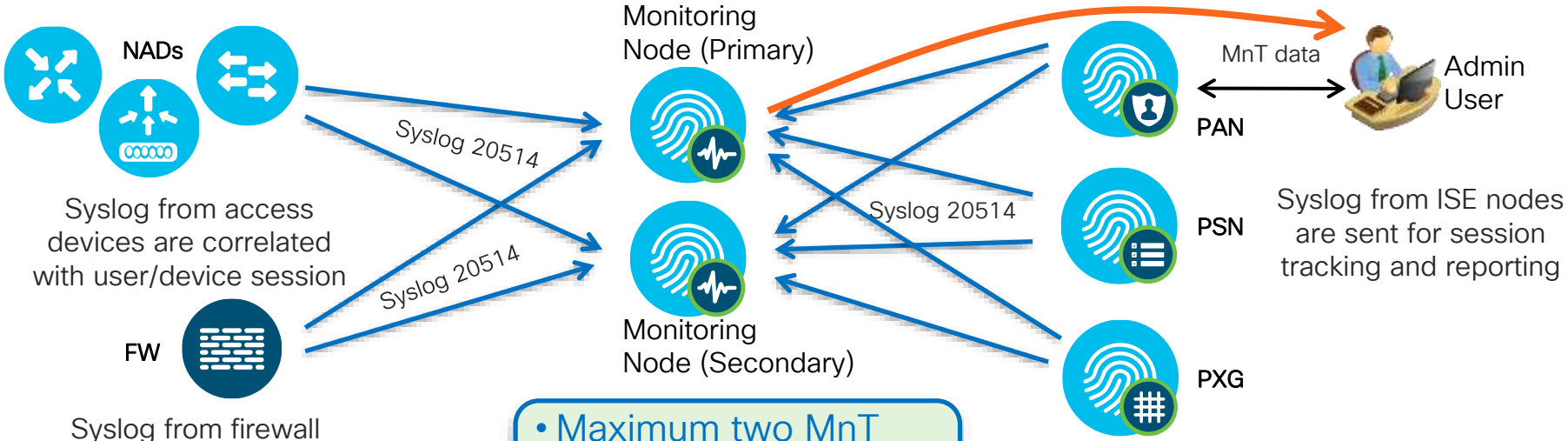


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

HA for Monitoring and Troubleshooting

Steady State Operation

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

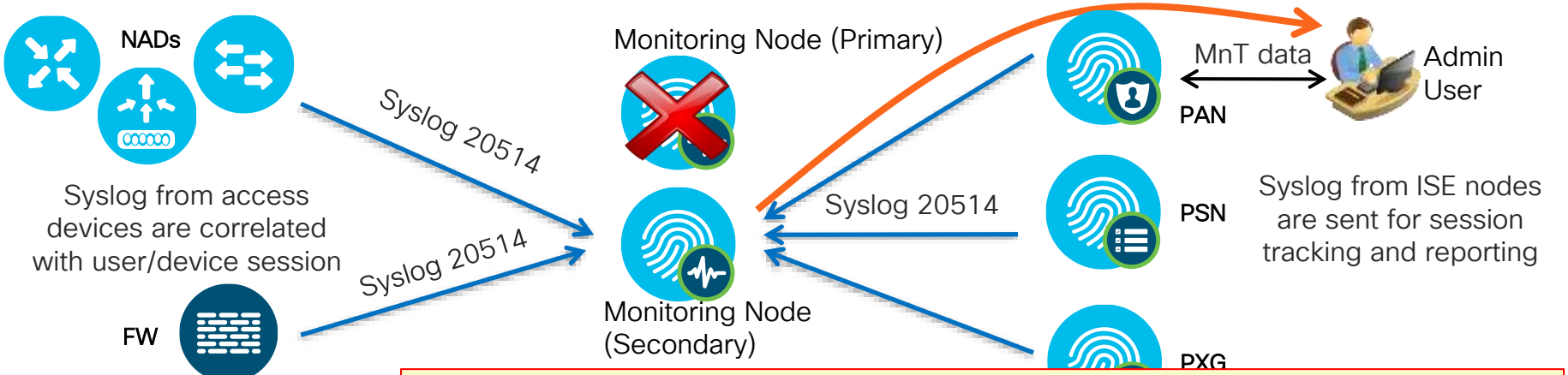


- Maximum two MnT nodes per deployment
- Active / Active

HA for Monitoring and Troubleshooting

Primary MnT Outage and Recovery

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

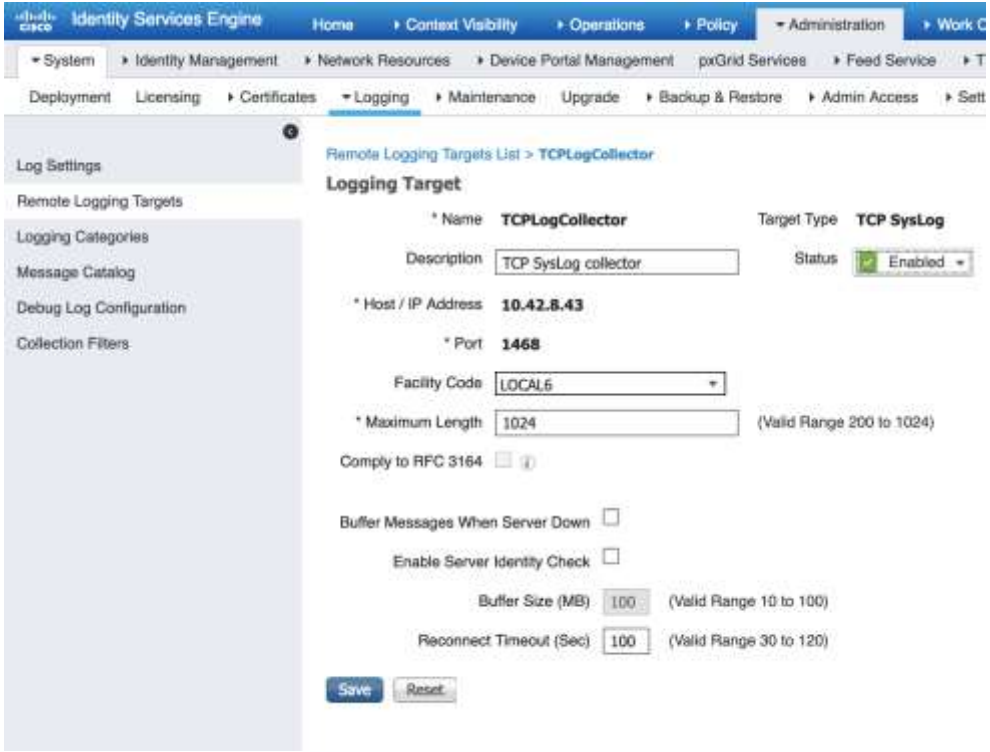


- PSN logs are not locally buffered when MnT down unless use TCP/Secure syslog.
- Log DB is not synced between MnT nodes.
- Upon return to service, recovered MnT node will not include data logged during outage
- Backup/Restore required to re-sync MnT database

Log Buffering

TCP and Secure Syslog Targets <2.6

- 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.



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6+: Rabbit MQ

A new type of architecture for ISE messaging services

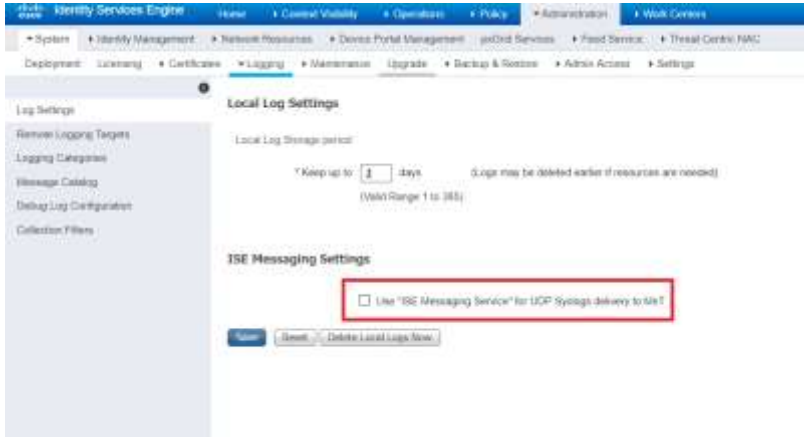
- Move forward in terms of robustness, reliability , Scalability and code quality
- Introduced in 2.6 for Secure Syslog (WAN survivability)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6: Syslogs over ISE Messaging

WAN survivability and securing Syslog using Rabbit MQ

- Syslogs can use secure ISE Messaging instead of UDP
- Messages buffered on PSN while MNT is down
  - Buffer is 4GB otherwise overflow, 200 per/sec 1kb message, 1.5 hrs filled
- DISABLED for Larger systems performance issues needs more hardening before allowed
- Smaller deployments ok ~500tps

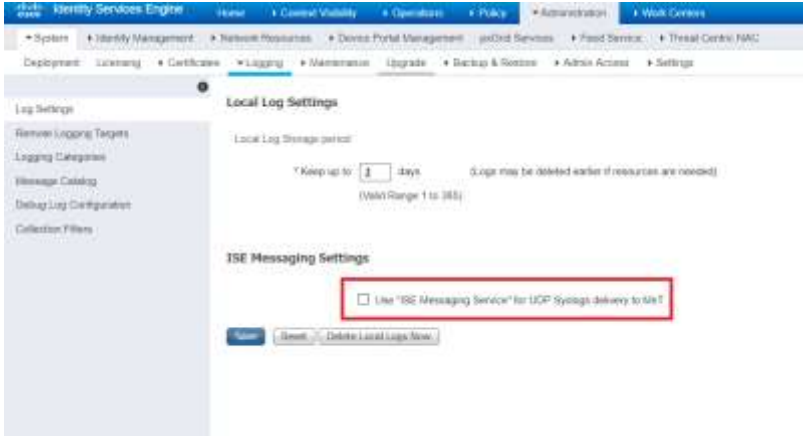


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.7: Syslogs over ISE Messaging

WAN survivability and securing Syslog using Rabbit MQ

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

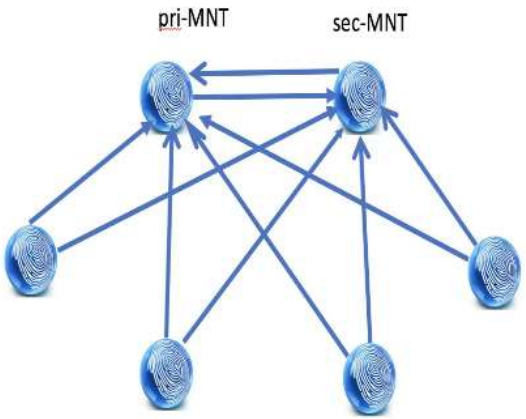


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6: Syslogs over ISE Messaging

RabbitMQ Topology for Syslogs

- Composed of federate links using AMQPS
- Links are unidirectional
- Links from all nodes to pri-MNT
- Links from all nodes to sec-MNT
- Links between the two MNTs

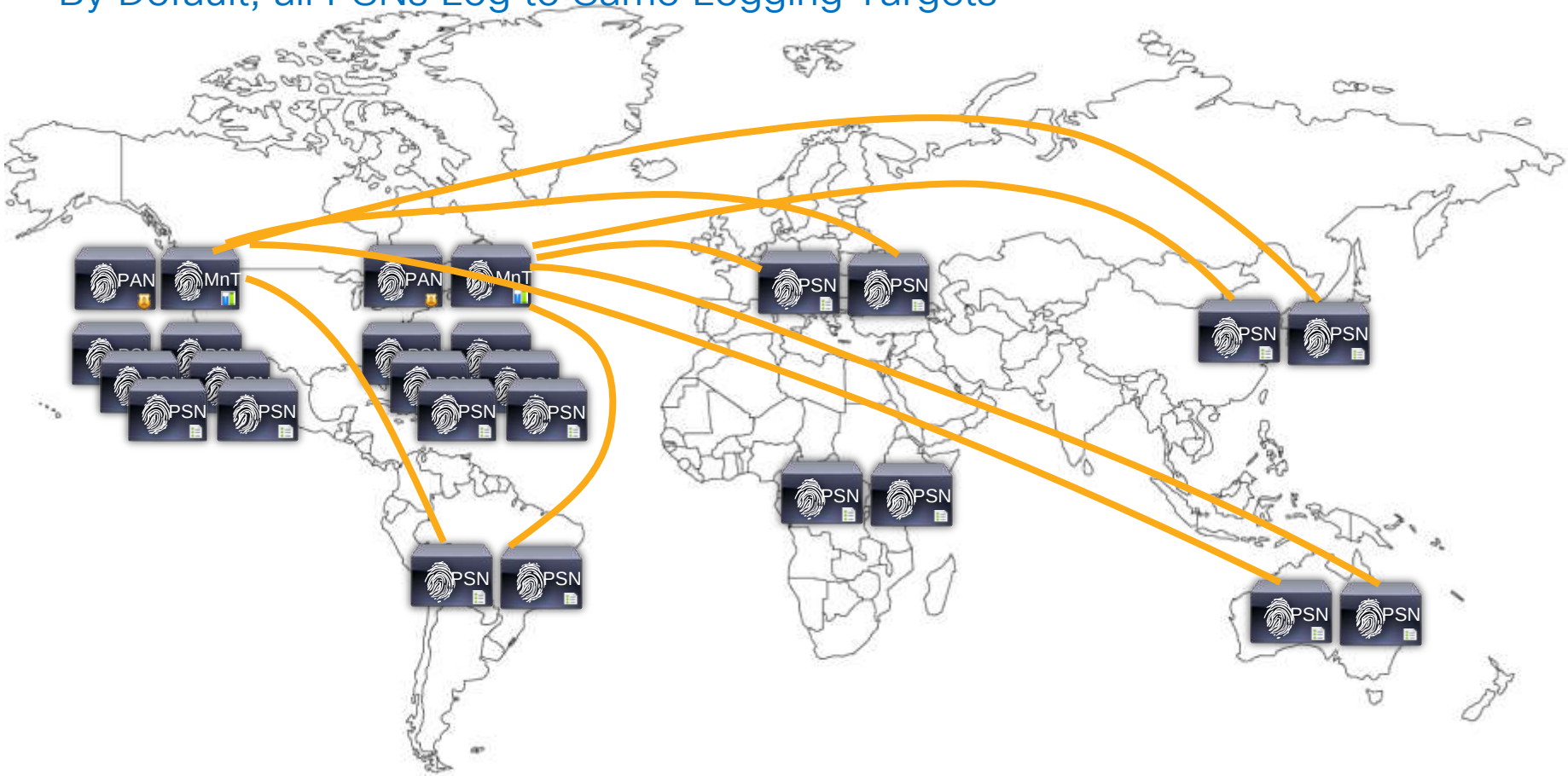


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Custom Logging Targets

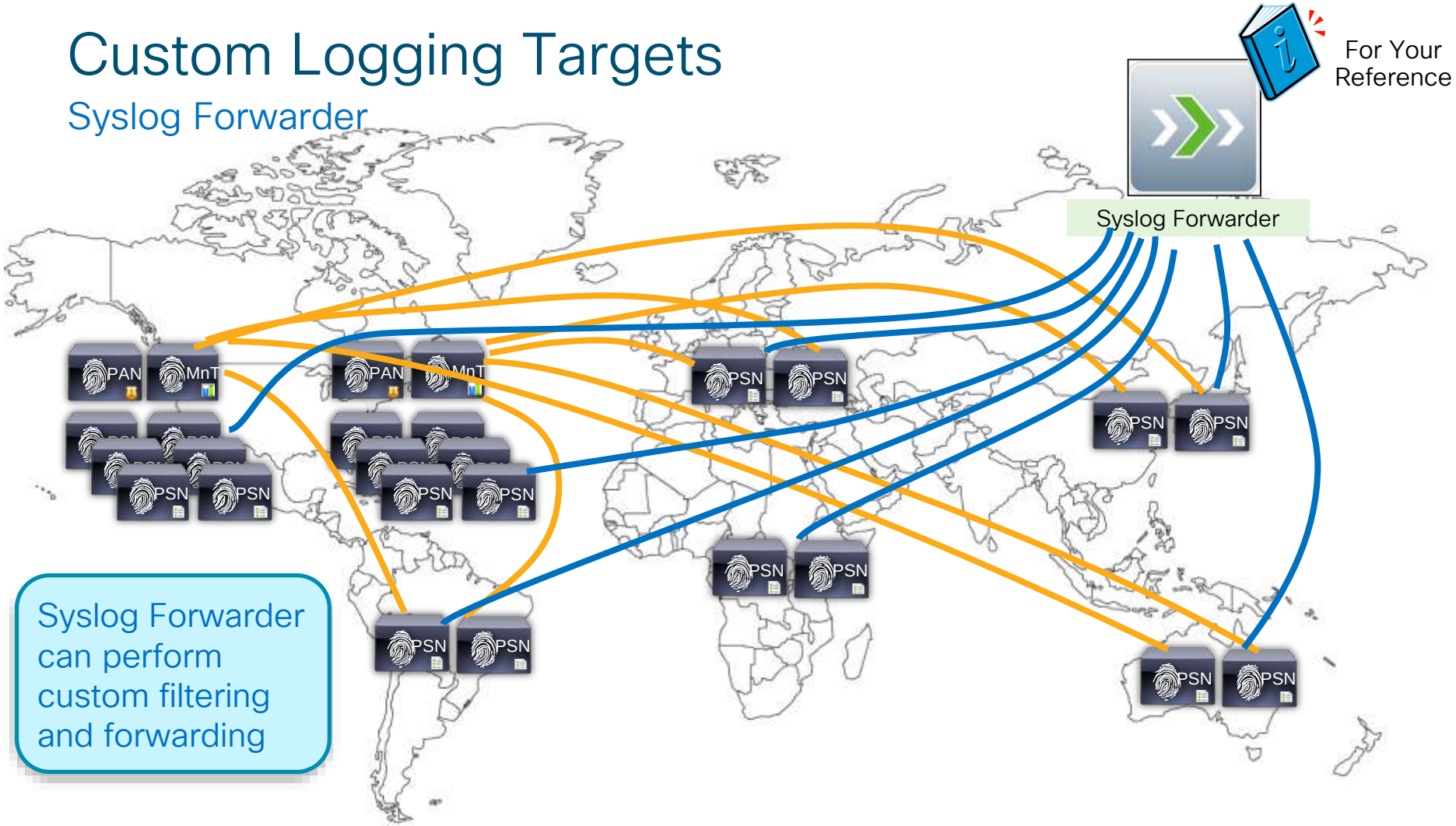
By Default, all PSNs Log to Same Logging Targets

For Your Reference



Custom Logging Targets

Syslog Forwarder



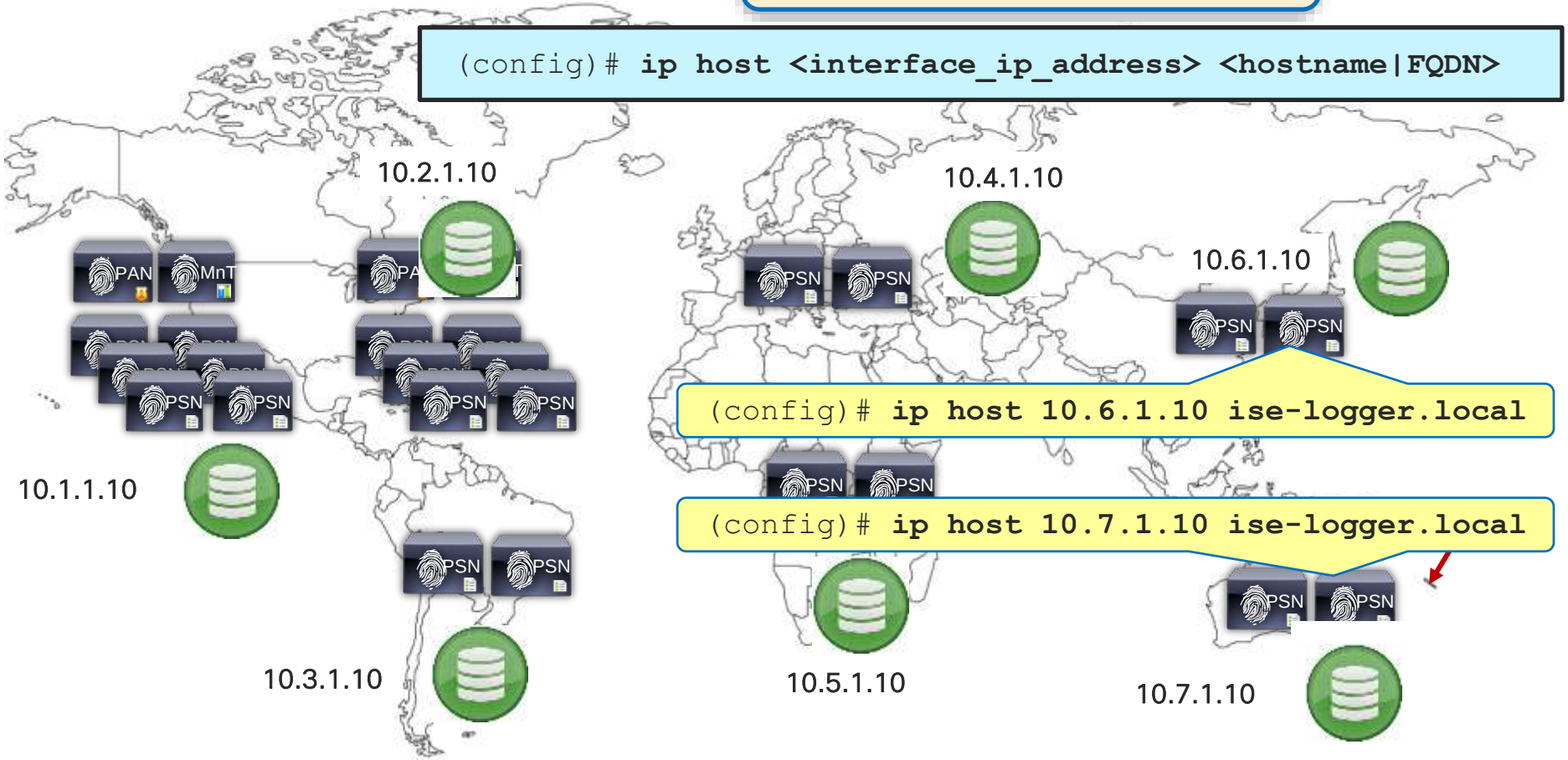
Syslog Forwarder can perform custom filtering and forwarding

Local Logging
Per-PSN Log Targets

Log Target = ise-logger.local

For Your Reference

```
(config)# ip host <interface_ip_address> <hostname|FQDN>
```




```
(config)# ip host 10.6.1.10 ise-logger.local
```

```
(config)# ip host 10.7.1.10 ise-logger.local
```

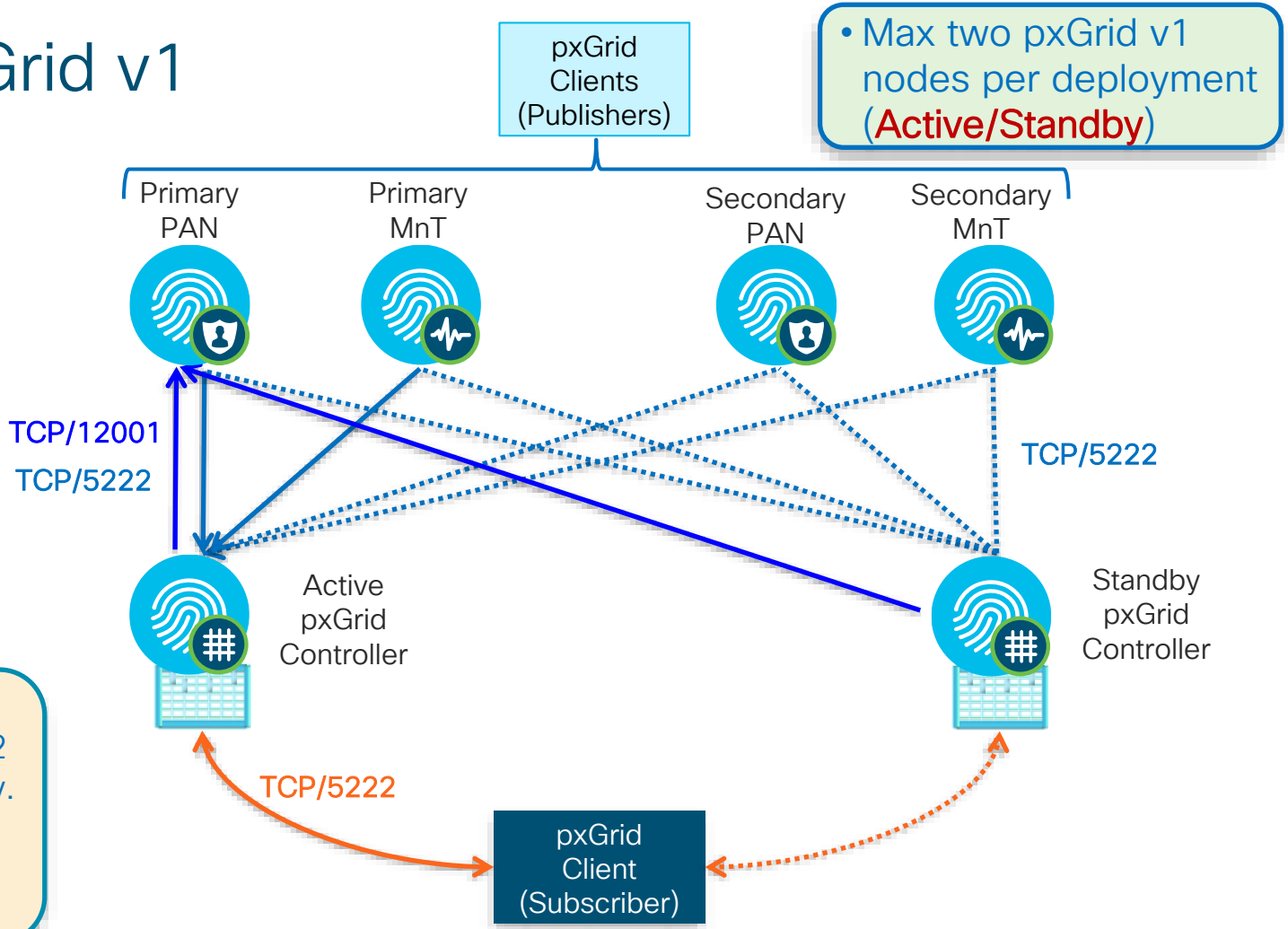
HA for pxGrid v1

Steady State

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

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

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



- Max two pxGrid v1 nodes per deployment (Active/Standby)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

HA for pxGrid v1

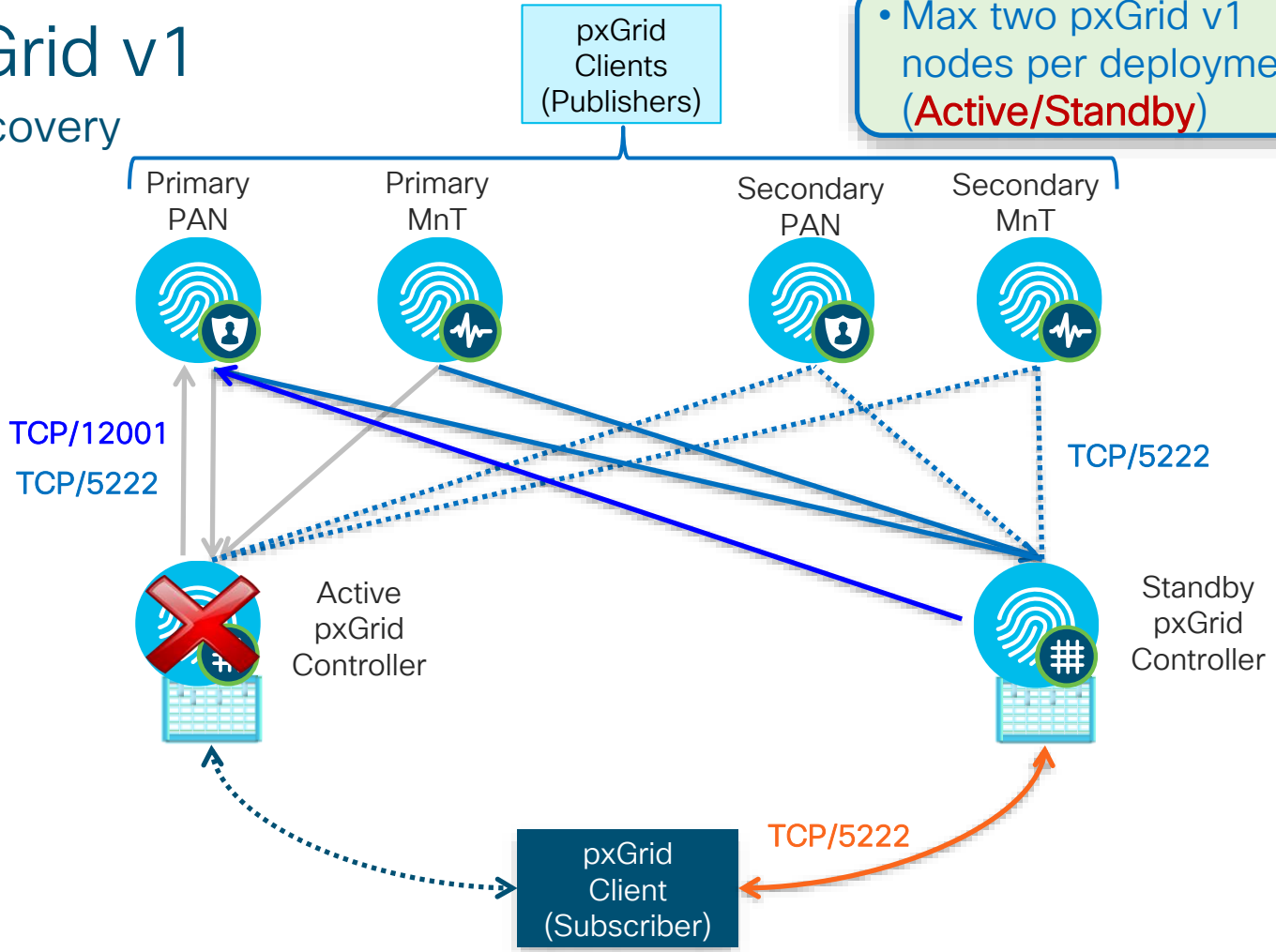
Failover and Recovery

- Max two pxGrid v1 nodes per deployment (Active/Standby)

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.



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

HA for pxGrid v2 (ISE 2.3+)

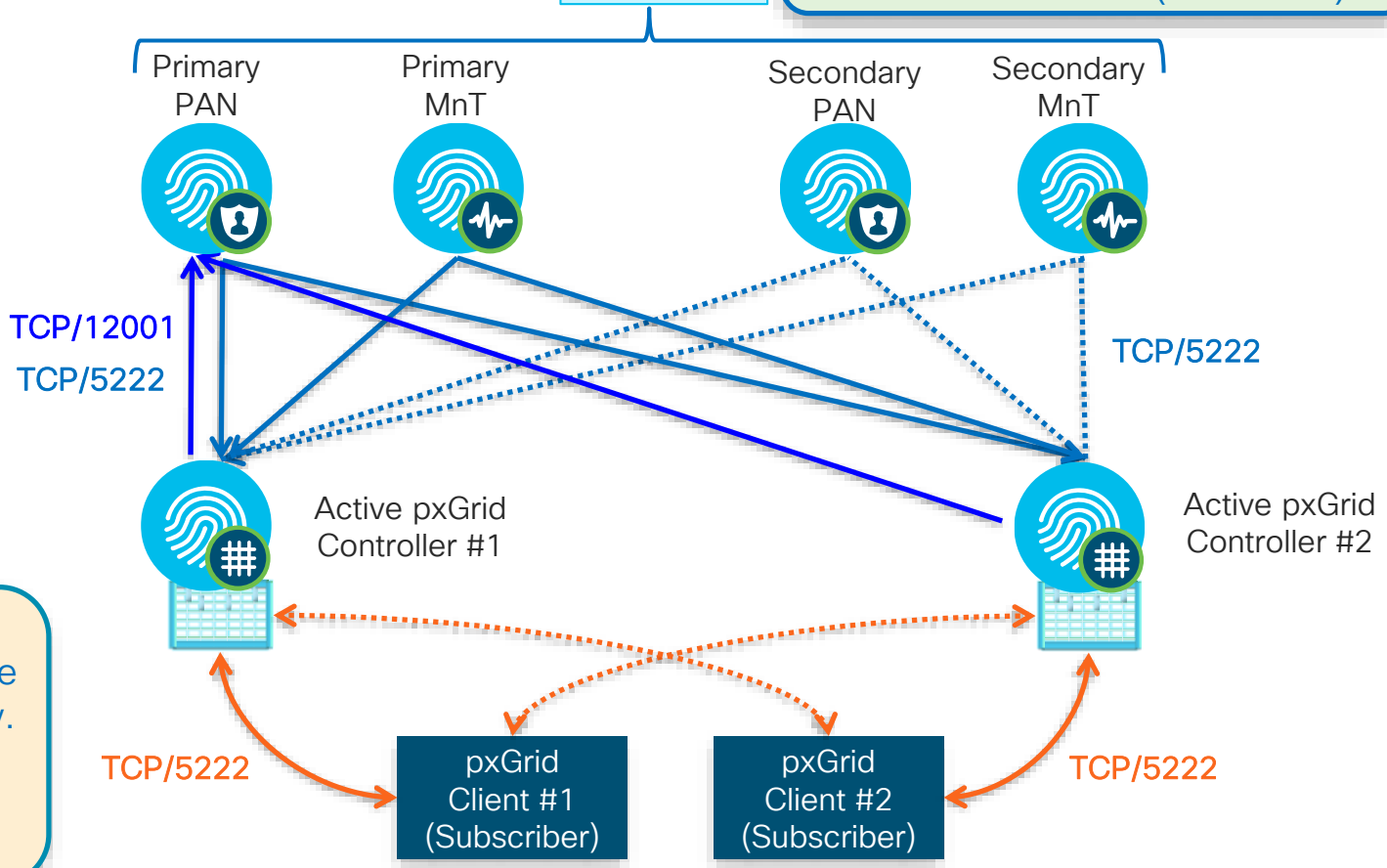
Steady State

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

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

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

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

pxGrid HA

Design Considerations

For Your Reference

- Download pxGrid Identity certs from the Primary and Secondary MnT nodes to pxGrid clients and import both into the Trusted store.
- Specify the hostname of both pxGrid nodes in the pxGrid API.

  Example:
  ./register.sh –keystoreFilename isekeyfile.jks –keystorePassword cisco123 –truststoreFilename rootfile.jks –truststorePassword cisco123 –hostname 10.0.1.33 10.0.2.79
- The pxGrid clients will register to both pxGrid nodes.
- If the pxGrid node registered to the primary goes down, the pxGrid client will continue communication with the pxGrid registered to the secondary node.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

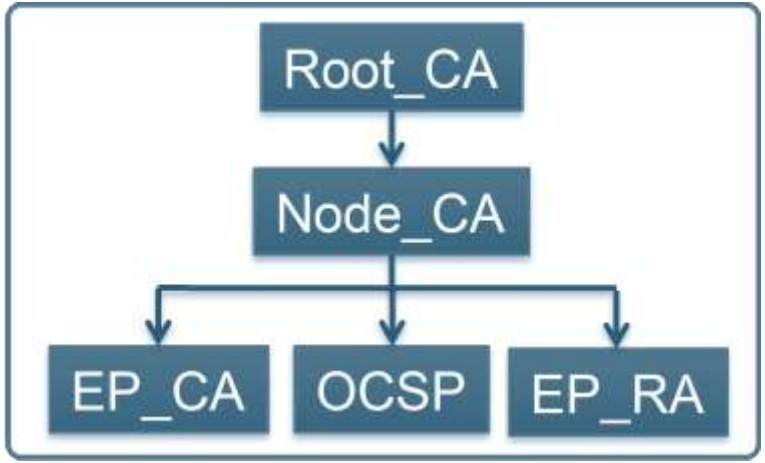
High Availability for Certificate Services

CA Hierarchy

ISE 2.0 Introduced Certificate Type Called NODE_CA

For Your Reference

- ROOT_CA – The Root CA for the entire ISE PKI Hierarchy
- NODE_CA – Responsible for issuing the subordinate EP_CA cert and OCSP cert
- EP_CA – Responsible for issuing Endpoint identity and device certificates
- OCSP – Responsible for signing the OCSP responses
- EP_RA – Registration Authority for SCEP to external CAs

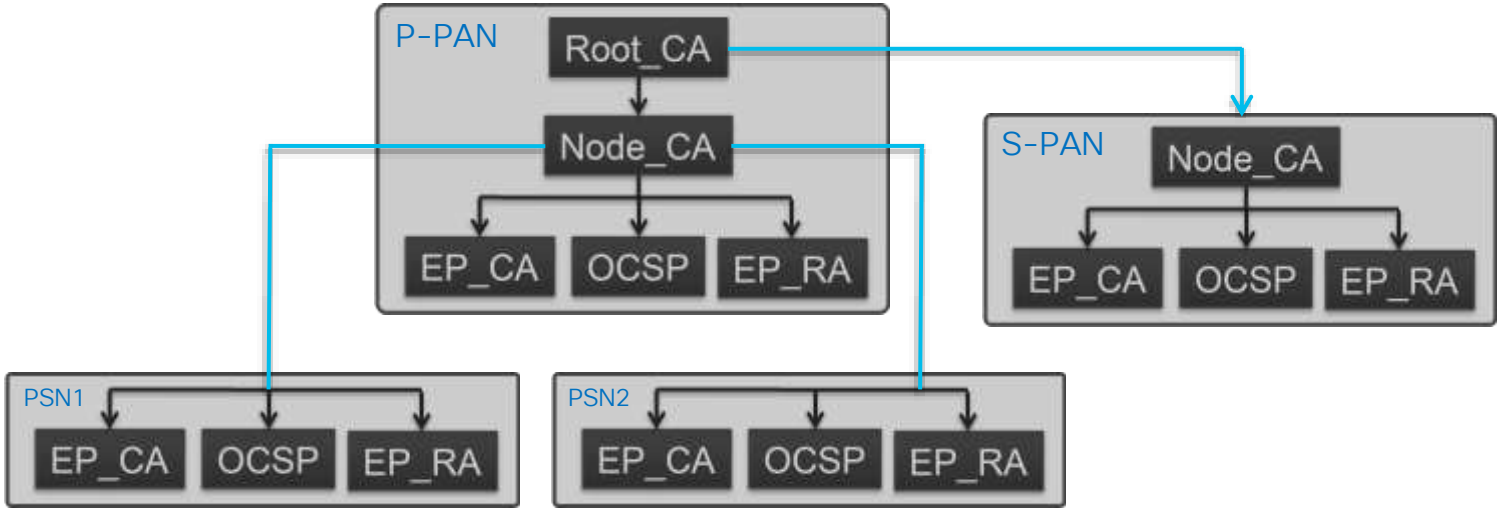


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CA Hierarchy

Multi Node Deployment with 2 PANs and Multiple PSNs

For Your Reference



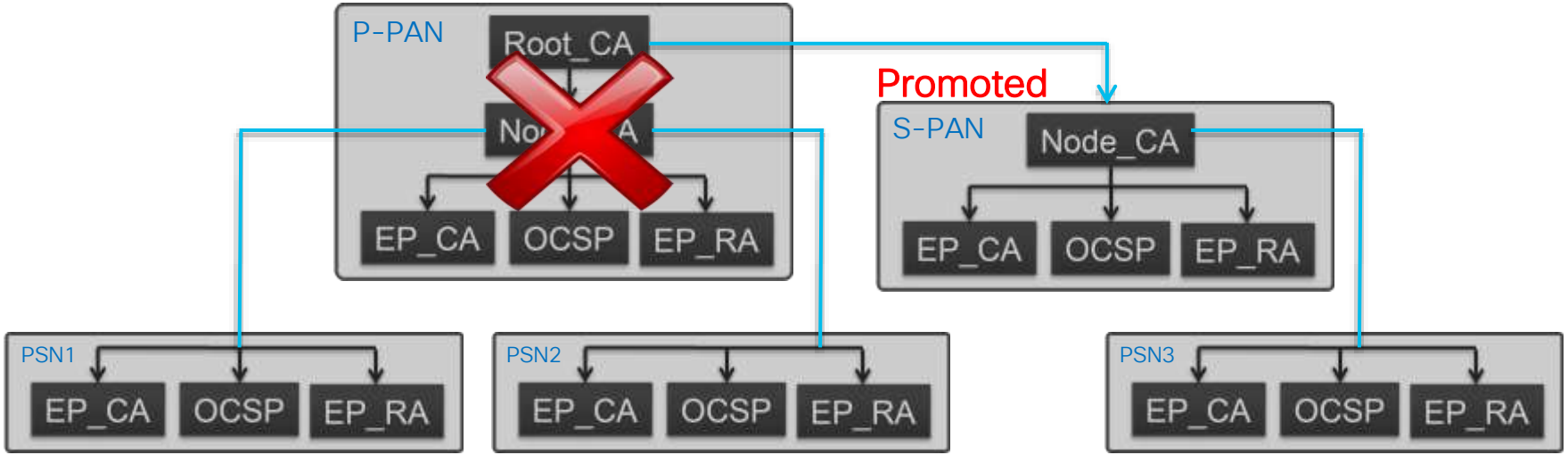
- NODE_CA on Primary and Secondary PAN are signed by ROOT_CA on the Primary PAN
- NODE_CA on Primary PAN is responsible for signing EP_CA and OCSP cert for all PSNs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CA Hierarchy

Multi Node Deployment with 2 PANs and Multiple PSNs

For Your Reference



- NODE_CA on Primary and Secondary PAN are signed by ROOT_CA on the Primary PAN
- NODE_CA on Primary PAN is responsible for signing EP_CA and OCSP cert for all PSNs
- If P-PAN fails and S-PAN promoted, new PSN certs will be signed by S-PAN NODE_CA, but same chain of trust maintained to ROOT_CA

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

When Does CA Hierarchy Switch from 2 Roots to 1 Root?

For Your Reference

- On Fresh Install: YES
  - Single Root Hierarchy for all New Installs.
- On Upgrade: NO
  - No changes on Upgrade – requires manual switch
- To manually switch to a Single Root Hierarchy:
  - Administration > System > Certificate > Certificate Signing Requests > Replace ISE Root CA
  - **Note:** If after an upgrade the administrator does not trigger the "Replace ISE Root CA" operation, then any new PSN registering into the deployment will get its EP_CA and OCSP certificates signed by the ROOT CA on the Primary PAN.
  - This is same behavior as ISE 1.3/1.4.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | pxGrid Identity Mapping

Deployment | Licensing | Certificates | Logging | Maintenance | Backup & Restore | Admin Access | Settings

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

- Overview
- System Certificates
- Endpoint Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- **Certificate Authority**
- Internal CA Settings
- Certificate Templates
- External CA Settings

Disable Certificate Authority

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-pdp

For Your Reference

Export CA Certs from Primary PAN

application configure ise

For Your Reference

- Export the CA Certs to a Repository
- Will be an Encrypted GPG Bundle
- Four Key Pairs

```
cisco-lab-ise/admin# application configure ise

Selection ISE configuration option
    <SNIP>
[7]Export Internal CA Store
[8]Import Internal CA Store
    </SNIP>
[12]Exit
7
Export Repository Name: NAS
Enter encryption-key for export: ##########
Export on progress.............

The following 4 CA key pairs were exported to repository 'NAS' at
'ise_ca_key_pairs_of_cisco-lab-ise':
    Subject:CN=Certificate Services Root CA - cisco-lab-ise
    Issuer:CN=Certificate Services Root CA - cisco-lab-ise
    Serial#:0x6012831a-16794f11-b1248b9b-c7e199ef

    Subject:CN=Certificate Services Endpoint Sub CA - cisco-lab-ise
    Issuer:CN=Certificate Services Root CA - cisco-lab-ise
    Serial#:0x3e4d9644-934843af-b5167e76-cc0256e0

    Subject:CN=Certificate Services Endpoint RA - cisco-lab-ise
    Issuer:CN=Certificate Services Endpoint Sub CA - cisco-lab-ise
    Serial#:0x13511480-9650401a-8461d9d7-5b8dbe17

    Subject:CN=Certificate Services OCSP Responder - cisco-lab-ise
    Issuer:CN=Certificate Services Root CA - cisco-lab-ise
    Serial#:0x10d18efb-92614084-895097f2-9885313b

ISE CA keys export completed successfully
```

Root CA

Sub CA

RA

OCSP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Import CA Certs from Primary to Secondary PAN

- After an upgrade, immediately Export/Import CA certs.
- If want original PPAN to stay Primary *after* upgrade, promote Secondary after CA certs imported.
- Or… Promote Secondary *before* upgrade, upgrade ISE, and then export/import CA certs
- Provides CA redundancy if PPAN fails and Secondary promoted.

```
cisco-lab-ise/admin# application configure ise

Selection ISE configuration option
   <SNIP>
[7]Export Internal CA Store
[8]Import Internal CA Store
   </SNIP>
[12]Exit
8
Import Repository Name: NAS
Enter CA keys file name to import: ise_ca_key_pairs_of_cisco-lab-ise
Enter encryption-key: ########
Import on progress..............

The following 4 CA key pairs were imported:
        Subject:CN=Certificate Services Root CA - cisco-lab-ise
        Issuer:CN=Certificate Services Root CA - cisco-lab-ise
        Serial#:0x6012831a-16794f11-b1248b9b-c7e199ef

        Subject:CN=Certificate Services Endpoint Sub CA - cisco-lab-ise
        Issuer:CN=Certificate Services Root CA - cisco-lab-ise
        Serial#:0x3e4d9644-934843af-b5167e76-cc0256e0

        Subject:CN=Certificate Services Endpoint RA - cisco-lab-ise
        Issuer:CN=Certificate Services Endpoint Sub CA - cisco-lab-ise
        Serial#:0x13511480-9650401a-8461d9d7-5b8dbe17

        Subject:CN=Certificate Services OCSP Responder - cisco-lab-ise
        Issuer:CN=Certificate Services Root CA - cisco-lab-ise
        Serial#:0x10d18efb-92614084-895097f2-9885313b

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

For Your Reference

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example of Exported Keys

ISE 2.0 Example with New Root Hierarchy

For Your Reference

```
The following 5 CA key pairs were exported to repository 'disk' at 'ise_ca_key_pairs_of_ise20-pan1':
    Subject:CN=Certificate Services Root CA - ise20-pan1
    Issuer:CN=Certificate Services Root CA - ise20-pan1
    Serial#:0x06c4fb0a-812b4f07-8fc3361a-2c57ae24

    Subject:CN=Certificate Services Node CA - ise20-pan1
    Issuer:CN=Certificate Services Root CA - ise20-pan1
    Serial#:0x7386ba45-9d754b69-9c82f764-d3263ca7

    Subject:CN=Certificate Services Endpoint Sub CA - ise20-pan1
    Issuer:CN=Certificate Services Node CA - ise20-pan1
    Serial#:0x793e7b17-a0ec40e7-9bfc47f0-974fc909

    Subject:CN=Certificate Services Endpoint RA - ise20-pan1
    Issuer:CN=Certificate Services Endpoint Sub CA - ise20-pan1
    Serial#:0x7e3c09ba-9168441f-a16f219f-6e62cbca

    Subject:CN=Certificate Services OCSP Responder - ise20-pan1
    Issuer:CN=Certificate Services Node CA - ise20-pan1
    Serial#:0x08fcc154-b8414b25-a50ca00d-13994488

ISE CA keys export completed successfully
```

- Root CA
- Node CA
- Sub CA
- RA
- OCSP

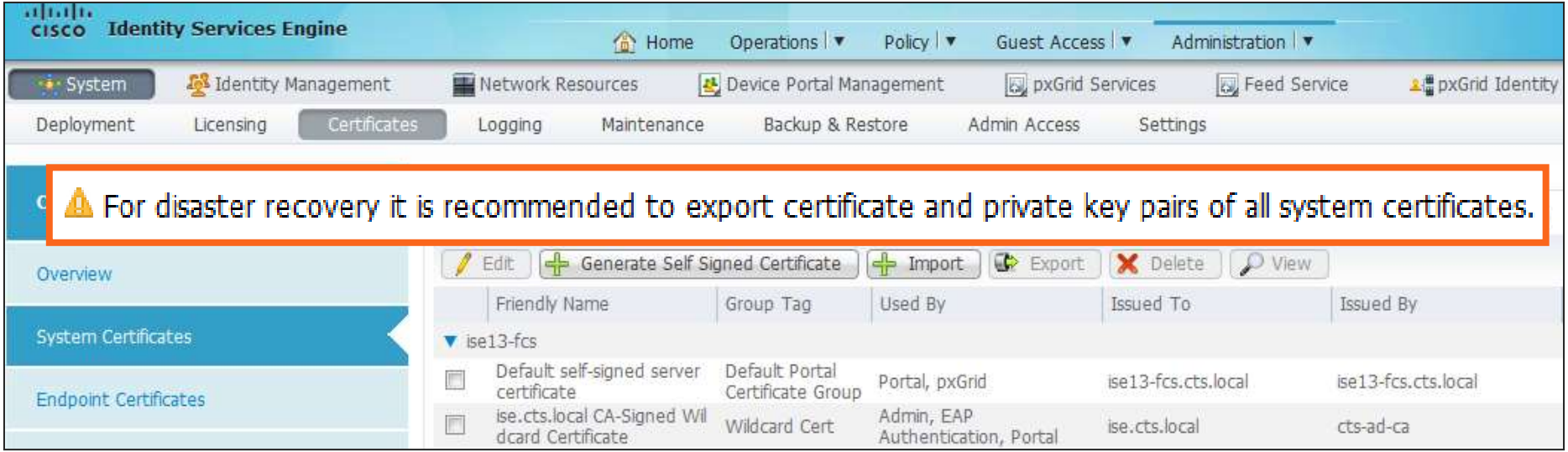
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Certificate Recovery for ISE Nodes

Backup all System (Server) Certificates and Key Pairs

For Your Reference

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

OCSP Responder HA

For Your Reference

- 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).

Disable Certificate Authority

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/

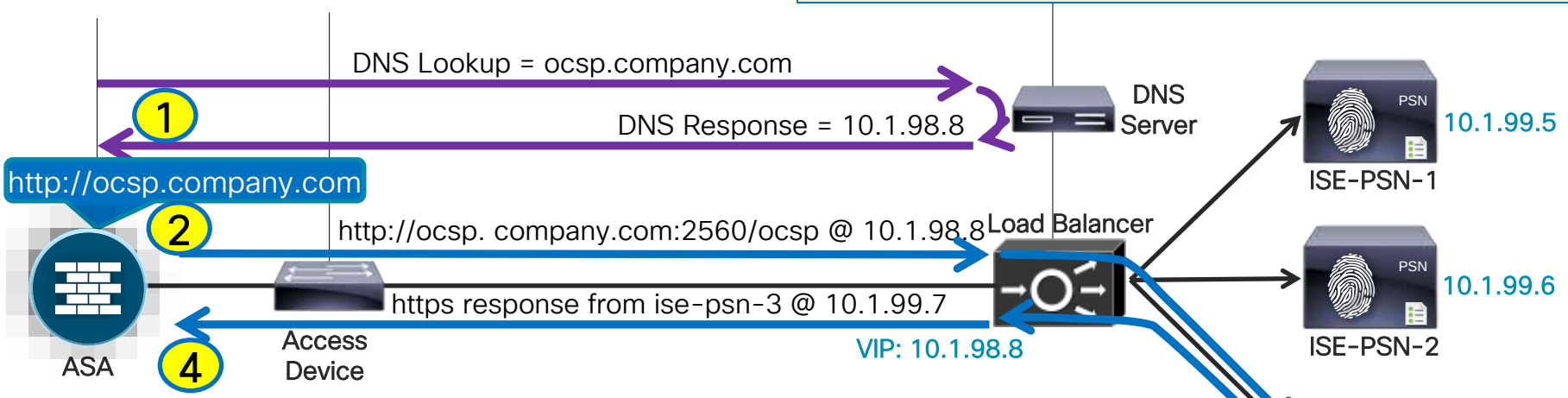
ASA Remote Access VPN Example:

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

For Your Reference

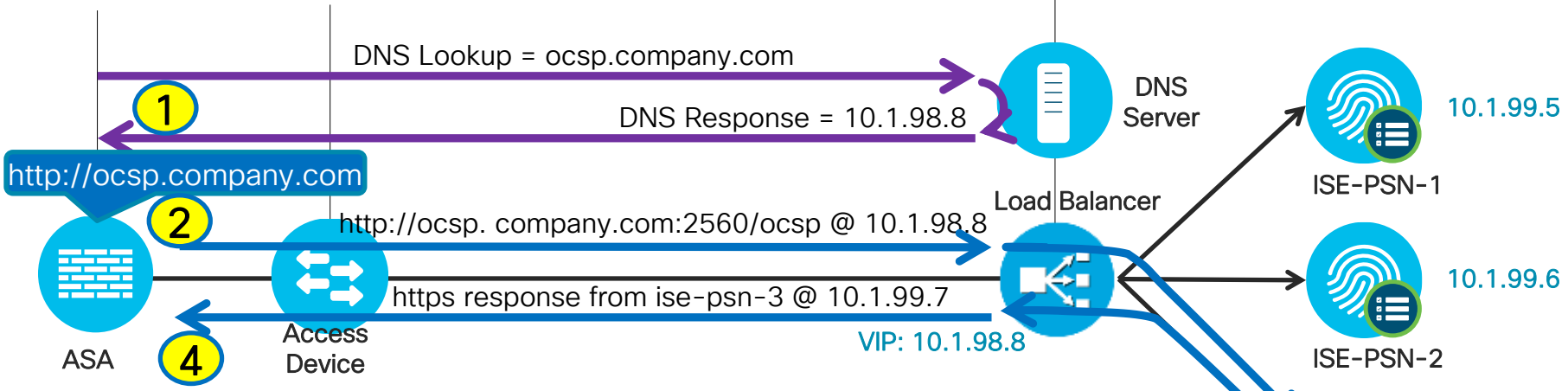
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing OCSP

Sample Flow

Each PSN is a
Database repl
contains same
cates.

Updated Slide with New Icons



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

For Your Reference

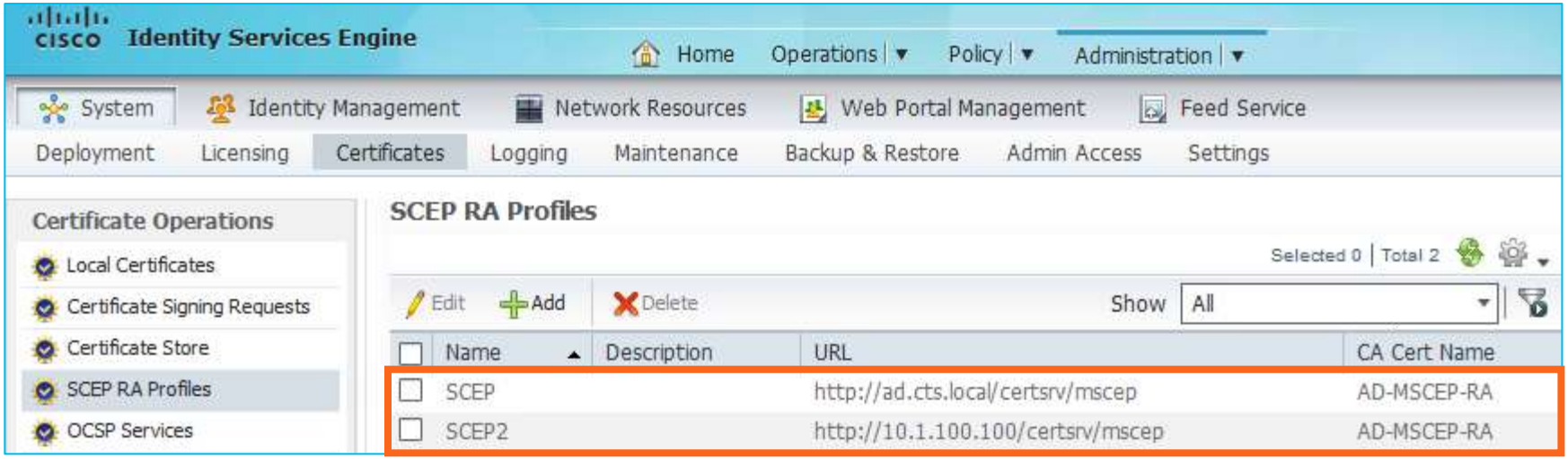
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SCEP Load Balancing for BYOD/NSP (ISE 1.2)

If Multiple SCEP CA Servers Defined…

For Your Reference

- 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.



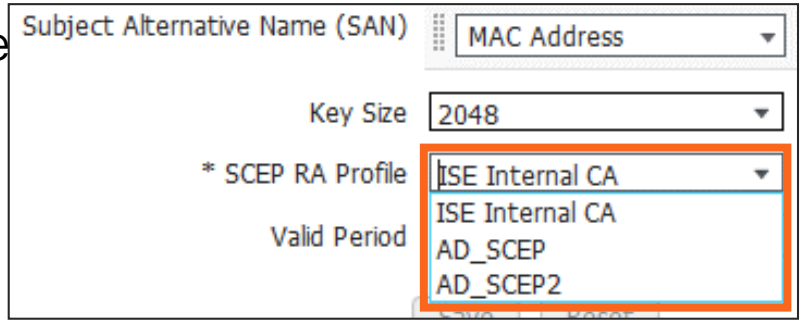
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SCEP Load Balancing (ISE 1.3+)

If Multiple SCEP CA Servers Defined…

For Your Reference

- SCEP Profile defined in Certificate Template –only one can be selected.
- Multiple CA URLs supported in each profile (since ISE 1.3)
- Requests load balanced across CAs



External CA Settings

SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

Edit | Add | Delete

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

High Availability and Scaling for ISE SXP Services

ISE SXP HA

For Your Reference

ISE 2.0 supports up to one pair of SXP PSNs (SXPSNs) where both configured for same mappings and peers.

Each SXPSN in a pair process and “speak” same bindings to same peers.
SXP Listeners receive duplicate bindings (not an issue).

Starting with v2.1, ISE supports two pairs of SXPSNs with bindings to different peers (which can be controlled via SXP Domains).

SXP Domains provides horizontal scaling as well as control which nodes get bindings. If not match specific domain, it hits default. If nodes not mapped to domain, they will be dropped.

Configure SXP under PSN services. Total 4 PSNs can be configured with SXP (two pairs).

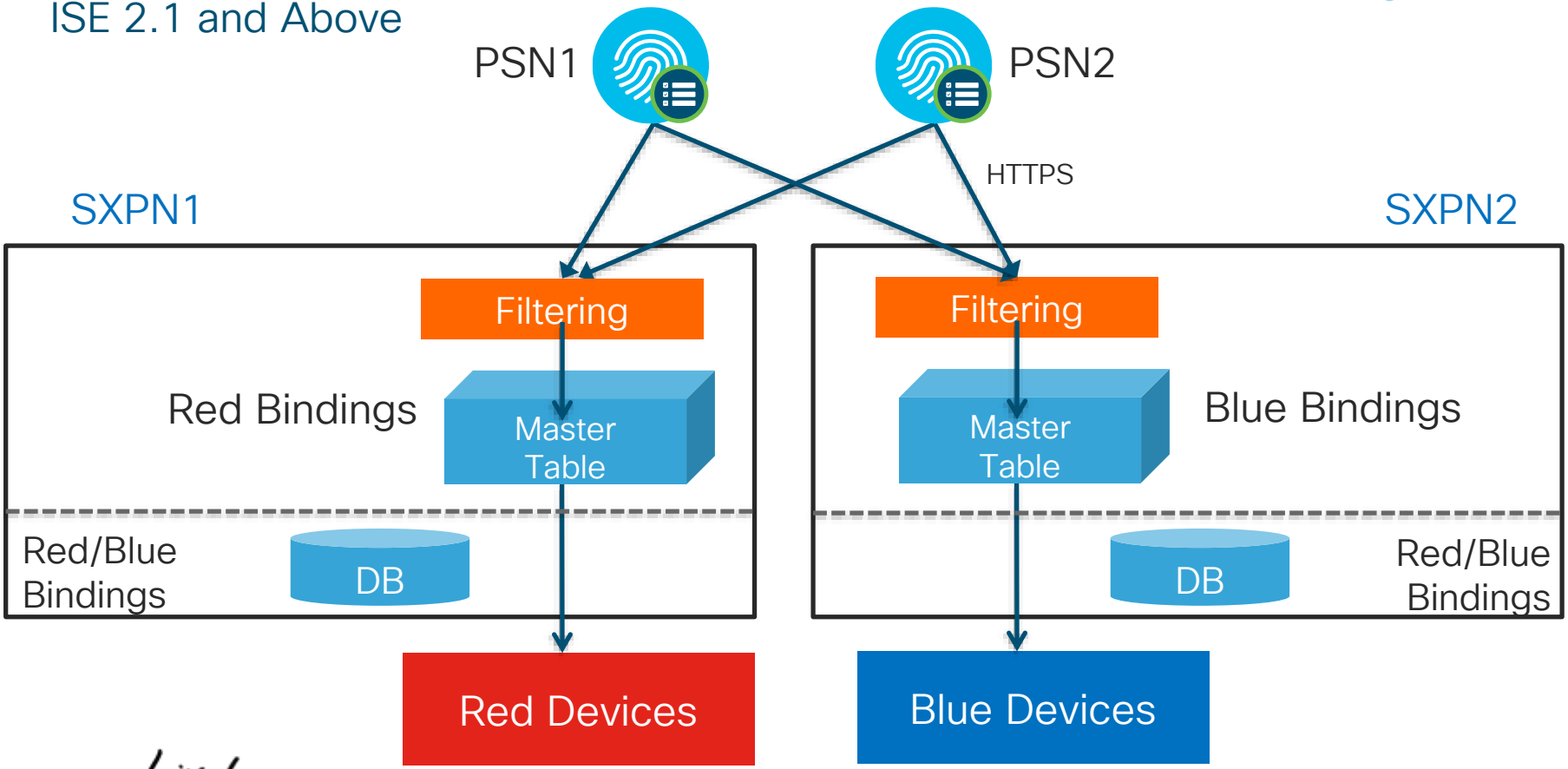
No validation or limit on # PSNs configured for ISE SXP.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE SXP Horizontal Scaling

ISE 2.1 and Above

For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling ISE SXP

For Your Reference

	ISE 2.0	ISE 2.1-2.3	ISE 2.4+
Max ISE SXP nodes / redundant pairs	2 / 1	4 / 2	8 / 4
Max ISE SXP Peers per SXPSN	20	100	200
Max ISE SXP Peers per deployment	20	200	800
Max ISE SXP Bindings per SXP PSN	100k	250k	350k
Max ISE SXP Bindings per deployment	100k	500k	* 1.4M

In ISE 2.1+, SXP Domains allow the splitting of bindings across multiple SXPSNs.

* Max dynamic bindings limited by max RADIUS session scale.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.3 SXP Multi-Service Scaling

For Your Reference

Max SXP Bindings and Peers by Deployment Model and Platform

Deployment Model	Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max ISE SXP Bindings	Max ISE SXP Peers
Standalone: All personas on same node (2 nodes redundant)	3415	0	5,000	2,500	10
	3495	0	10,000	5,000	20
	3515	0	7,500	3,750	15
	3595	0	20,000	10,000	25
Hybrid: PAN + MnT on same node; Dedicated PSN (Minimum 4 nodes redundant)	3415 as PAN+MNT	5 / 3 + 2	5,000	2,500 / 5,000	100
	3495 as PAN+MNT	5 / 3 + 2	10,000	5,000 / 10,000	100
	3515 as PAN+MNT	5 / 3 + 2	7,500	3,750 / 7,500	100
	3595 as PAN+MNT	5 / 3 + 2	20,000	10,000 / 20,000	100
Dedicated PAN and MnT (Minimum 6 nodes redundant)	3495 as PAN and MNT	38 + 2 / 36 + 4	250,000	150,000 / 250,000	100 / 200
	3595 as PAN and MNT	48 + 2 / 46 + 4	500,000	250,000 / 500,000	100 / 200

100 per SXPSN pair

Scaling per SXPSN	Platform		Max RADIUS Sessions per PSN	Max ISE SXP Bindings	Max ISE SXP Peers
Dedicated SXPSN nodes (Gated by Total Deployment Scale)	SNS-3415	1 or 2 SXPSN pairs	5,000	100,000	100
	SNS-3495		20,000	150,000	100
	SNS-3515		7,500	150,000	100
	SNS-3595		40,000	250,000	100

Share PSNs (up to 5) for RADIUS+SXP OR Dedicate PSNs to RADIUS (up to 3) and SXP (2 for HA) Services

ISE 2.4 SXP Multi-Service Scaling

For Your Reference

Max SXP Bindings and Peers by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max ISE SXP Bindings	Max ISE SXP Peers
Standalone	All personas on same node	3515	0	7,500	3,500	20
		3595	0	20,000	10,000	30
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	5 / 3 + 2	7,500	7,500	200
		3595 as PAN+MNT	5 / 3 + 2	20,000	20,000	220
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000	350k / 500k 500k / 500k	150 / 300 450 / 600
		3595 as PAN and Large MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000	350k / 700k 1050k / 1.4M	200 / 400 600 / 800

Share PSNs (up to 5) for RADIUS+SXP OR Dedicate PSNs to RADIUS (up to 3) and SXP (2 for HA) Services

1, 2, 3, or 4 SXPSN pairs

- By Node

Scaling per SXPSN	Platform		Max RADIUS Sessions per PSN	Max ISE SXP Bindings	Max ISE SXP Peers
Dedicated SXPSN nodes (Gated by Total Deployment Size)	SNS-3515		7,500	200,000	200
	SNS-3595		40,000	350,000	220

ISE 2.6 SXP Multi-Service Scaling

For Your Reference

Max SXP Bindings and Peers by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max ISE SXP Bindings	Max ISE SXP Peers
Standalone	All personas on same node	3515	0	7,500	3,500	20
		3595	0	20,000	10,000	30
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT	5 / 3 + 2	10,000	10,000	200
		3655/3695 as PAN+MNT	5 / 3 + 2	25,000/50,000	20,000	220
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000	350k / 500k 500k / 500k	150 / 300 450 / 600
		3695 as PAN and MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000 (2M)	350k / 700k 1050k / 1.4M	200 / 400 600 / 800

Share PSNs (up to 5) for RADIUS+SXP OR Dedicate PSNs to RADIUS (up to 3) and SXP (2 for HA) Services

1, 2, 3, or 4 SXPSN pairs

- By Node

Scaling per SXPSN	Platform		Max RADIUS Sessions per PSN	Max ISE SXP Bindings	Max ISE SXP Peers
Dedicated SXPSN nodes (Gated by Total Deployment Size)	SNS-3615		10,000	200,000	200
	SNS-3655/3695		50,000/100,000	350,000	220

ISE 2.7 SXP Multi-Service Scaling

For Your Reference

Max SXP Bindings and Peers by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max ISE SXP Bindings	Max ISE SXP Peers
Standalone	All personas on same node	3515	0	7,500	3,500	20
		3595	0	20,000	10,000	30
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT	5 / 3 + 2	10,000	10,000	200
		3655/3695 as PAN+MNT	5 / 3 + 2	25,000/50,000	20,000	220
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000	350k / 500k 500k / 500k	150 / 300 450 / 600
		3695 as PAN and MNT	48 + 2 / 46 + 4 44 +6 / 42 + 8	500,000 (2M)	350k / 700k 1050k / 1.4M	200 / 400 600 / 800

Share PSNs (up to 5) for RADIUS+SXP OR Dedicate PSNs to RADIUS (up to 3) and SXP (2 for HA) Services

1, 2, 3, or 4 SXPSN pairs

- By Node

Scaling per SXPSN	Platform		Max RADIUS Sessions per PSN	Max ISE SXP Bindings	Max ISE SXP Peers
Dedicated SXPSN nodes (Gated by Total Deployment Size)	SNS-3615		10,000	200,000	200
	SNS-3655/3695		50,000/100,000	350,000	220

For Your Reference

High Availability and Scaling for TC-NAC Services

For Your Reference

TC-NAC HA

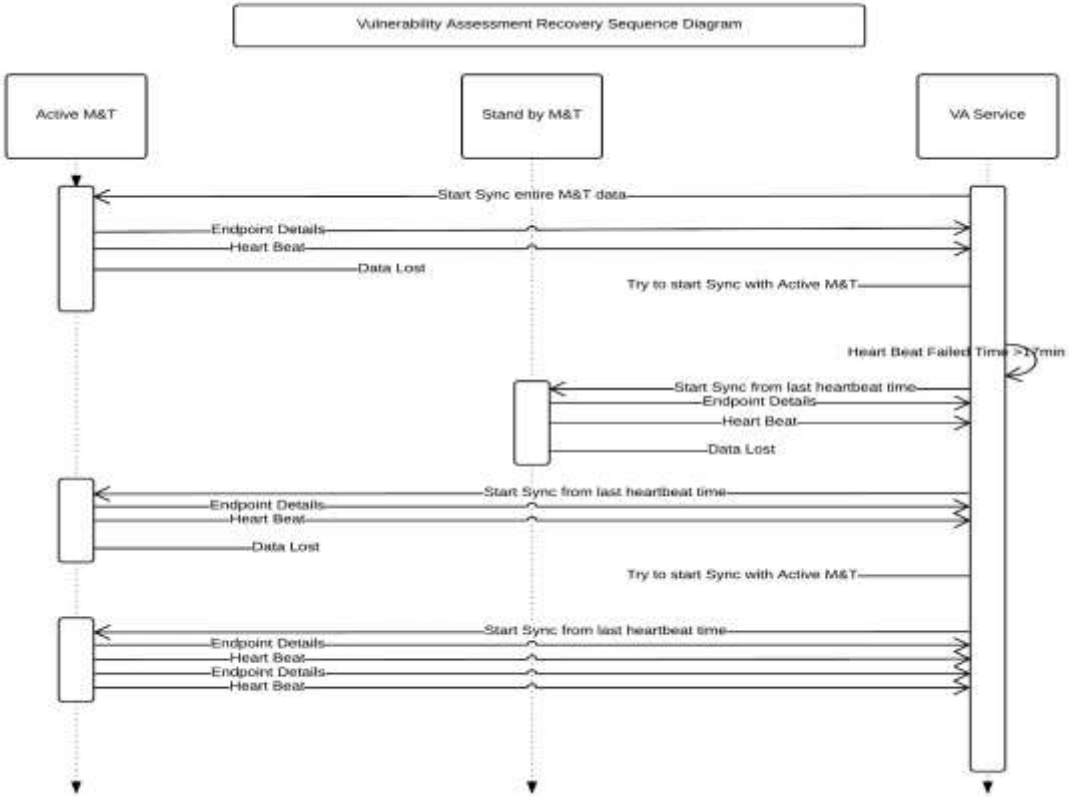
- Currently a limit one PSN to service with no HA.
- If try to enable on another PSN, will get notice that another PSN configured.
- TC-NAC is not installed until enable service under PSN for first time.
  - Takes ~10 minutes when first enabled.
  - Successive changes will simply enable or disable service.
- TC-NAC node always gets info from Active MnT. If Heartbeat fails, then start sync with new Active (Secondary) MnT node. Will try to failback to Primary.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vulnerability Assessment Recovery Sequence

Flow Diagram

For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.4 TC-NAC Multi-Service Scaling

For Your Reference

Max Concurrent TC-NAC Transactions by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max PSNs (dedicated)	Max Sessions per Deployment	Max TC-NAC Adapters	Max VAF TPM	Max IRF TPS
Stand-alone	All personas on same node	3515	0	7,500	1	5	5
		3595	0	20,000	1	5	5
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT+PXG	5 / 4 + 1	7,500	1 / 3	5 / 40	10 / 80
		3595 as PAN+MNT+PXG	5 / 4 + 1	20,000	2 / 5	10 / 40	20 / 80
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	49 + 1	500,000	5	40	80
		3595 as PAN and Large MnT	49 + 1	500,000	5	40	80

In medium deployment, option to share PSN or dedicate PSN; large deployment assume one PSN dedicated to TC=NAC

- By PSN

Scaling per PSN	Platform		Max Sessions per PSN	Max Adapters	Max VAF TPM	Max IRF TPS
Dedicated TC-NAC node	SNS-3515		7,500	3	40	80
	SNS-3595		40,000	5	40	80

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.6 TC-NAC Multi-Service Scaling

For Your Reference

Max Concurrent TC-NAC Transactions by Deployment Model and Platform

Deployment Model		Platform	Max PSNs (dedicated)	Max Sessions per Deployment	Max TC-NAC Adapters	Max VAF TPM	Max IRF TPS
Stand-alone	All personas on same node	3615	0	10,000	1	5	5
		3655	0	25,000	1	5	5
		3655	0	50,000	1	5	5
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3615 as PAN+MNT+PXG	5 / 4 + 1	10,000	1 / 3	5 / 40	10 / 80
		3655 as PAN+MNT+PXG	5 / 4 + 1	25,000	2 / 5	10 / 40	20 / 80
		3655 as PAN+MNT+PXG	5 / 4 + 1	50,000	2 / 5	10 / 40	20 / 80
Dedicated	Each Persona on Dedicated Node	3655 as PAN and MNT	49 + 1	500,000	5	40	80
		3695 as PAN and MnT	49 + 1	500,000 (2M)	5	40	80

In medium deployment, option to share PSN or dedicate PSN; large deployment assume one PSN dedicated to TC=NAC

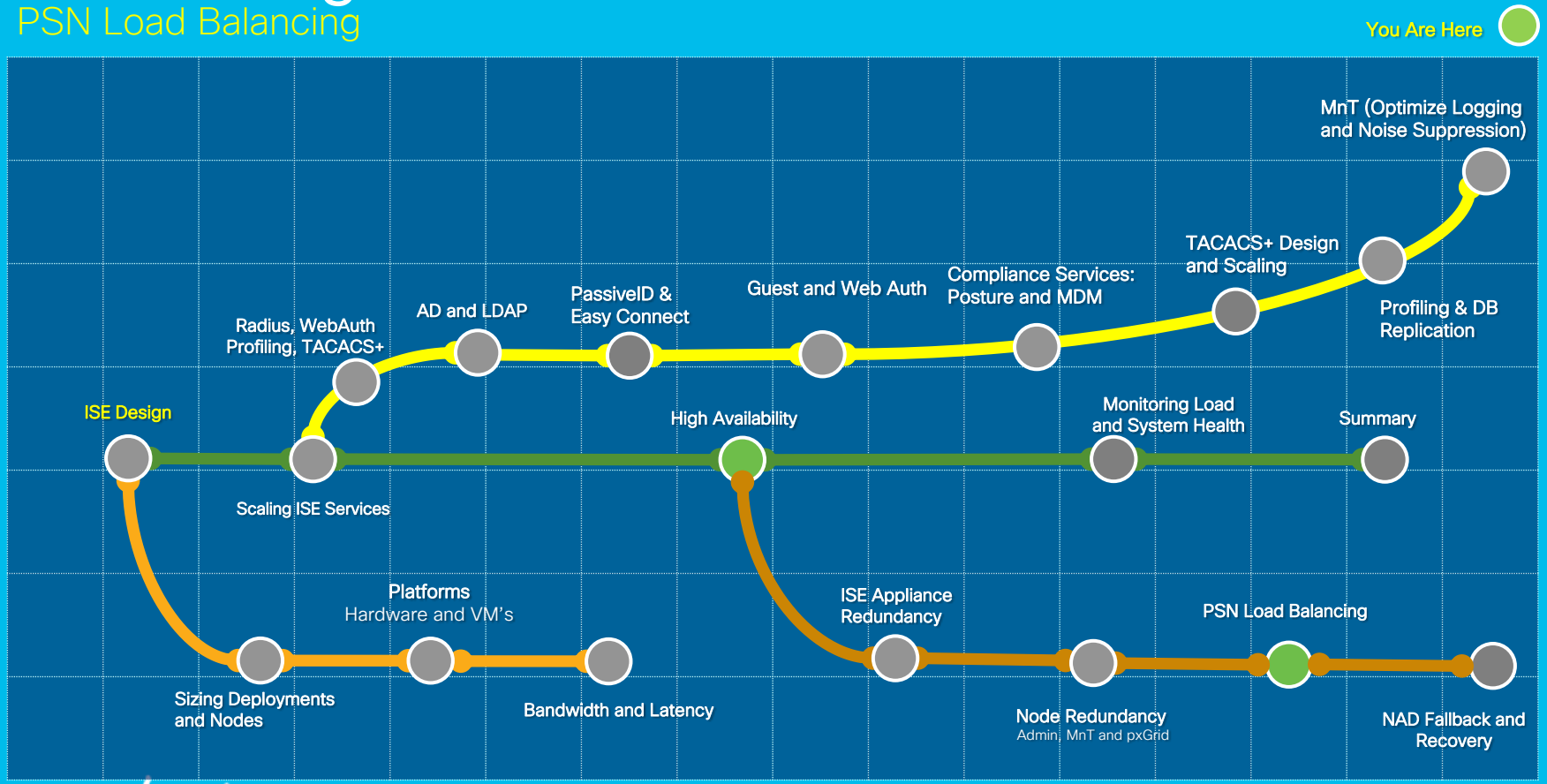
Scaling per PSN	Platform		Max Sessions per PSN	Max Adapters	Max VAF TPM	Max IRF TPS
Dedicated TC-NAC node	SNS-3615		10,000	3	40	80
	SNS-3655		50,000	5	40	80
	SNS-3695		100,000	5	40	80

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Load Balancing

Session Agenda

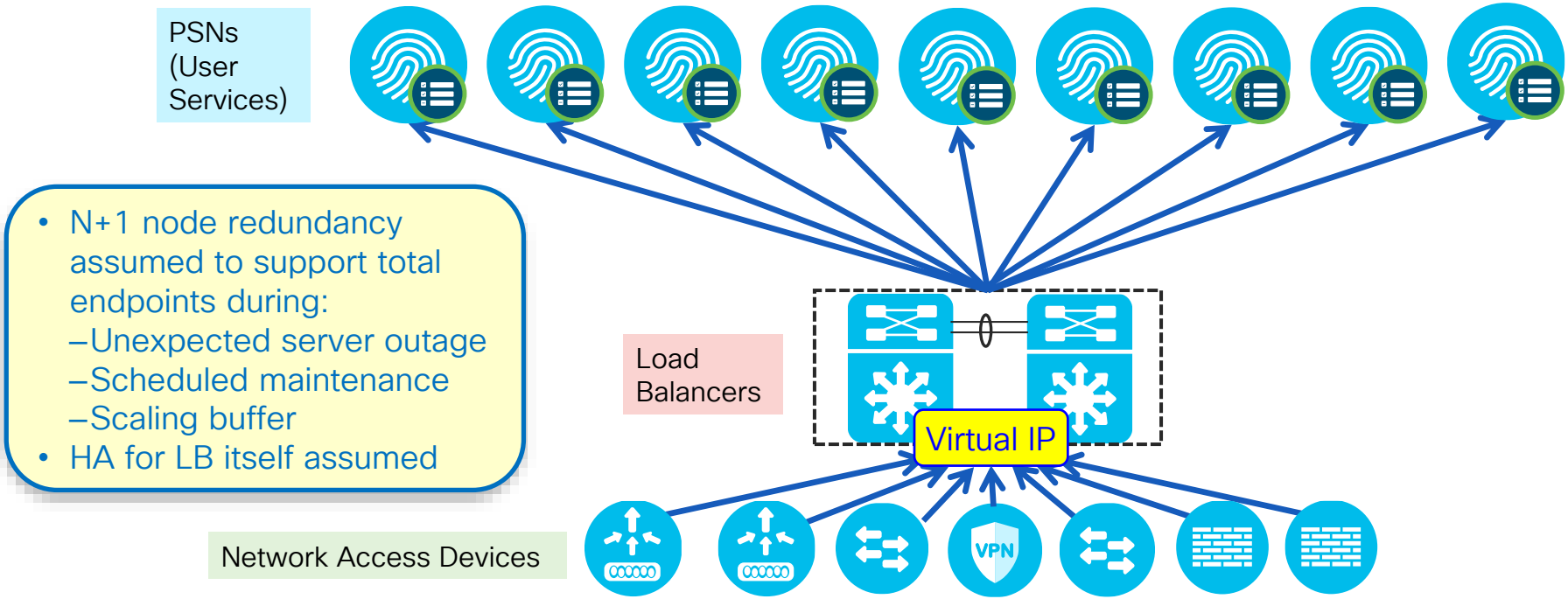
PSN Load Balancing



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing RADIUS, Web, and Profiling Services

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



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

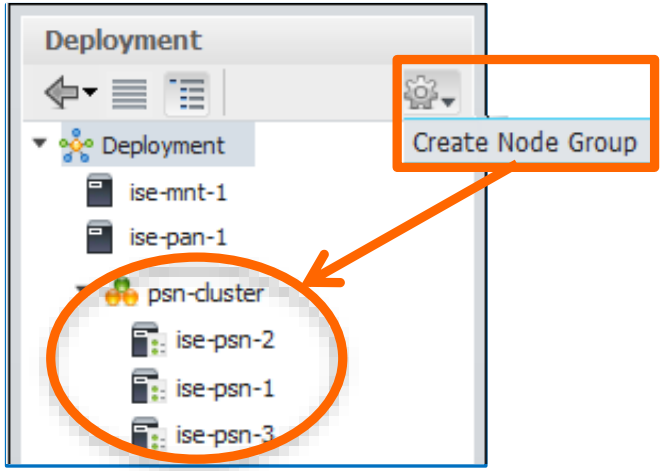
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configure Node Groups for LB Cluster

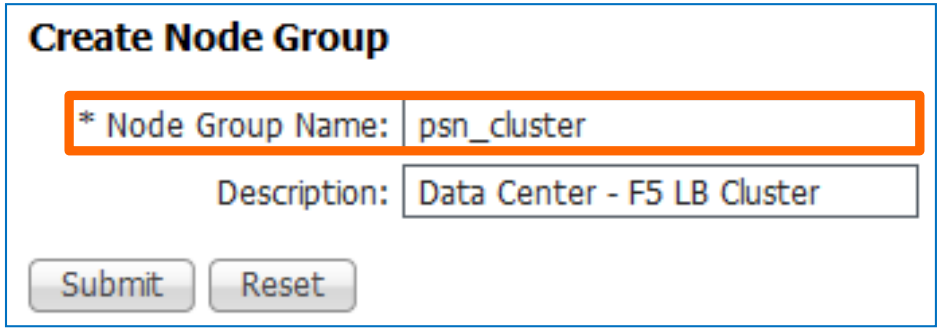
Place all PSNs in LB Cluster in Same Node Group

- Administration > System > Deployment

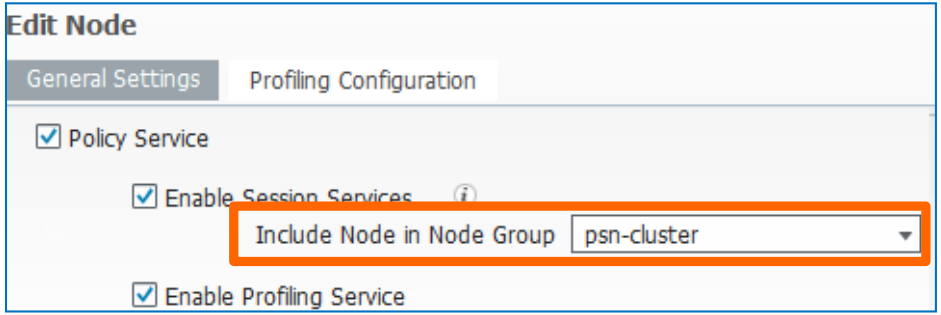
1) Create node group



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



3) Add individual PSNs to node group

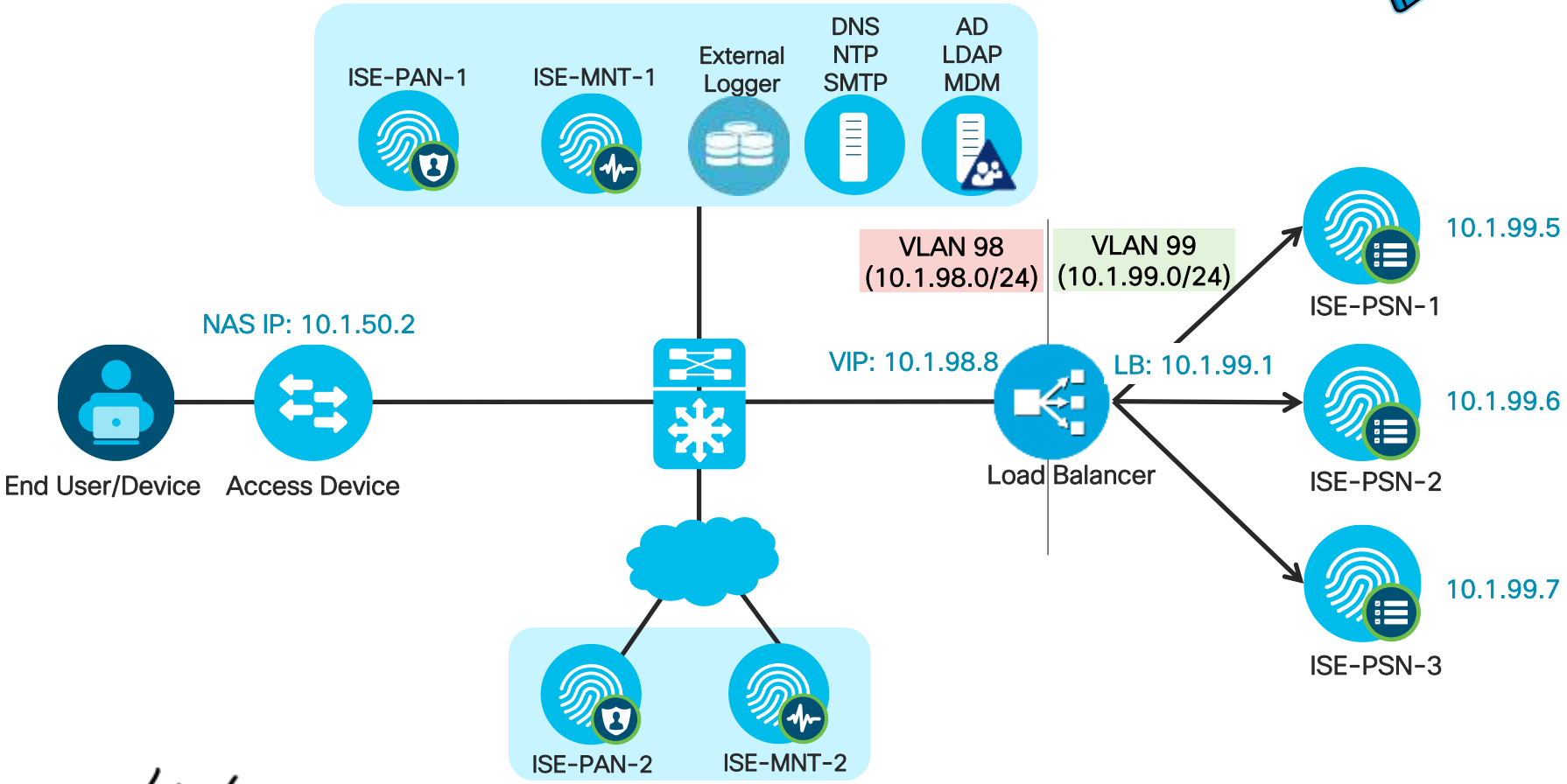


- Node group members can be L2 or L3
- Multicast not required

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

High-Level Load Balancing Diagram

For Your Reference



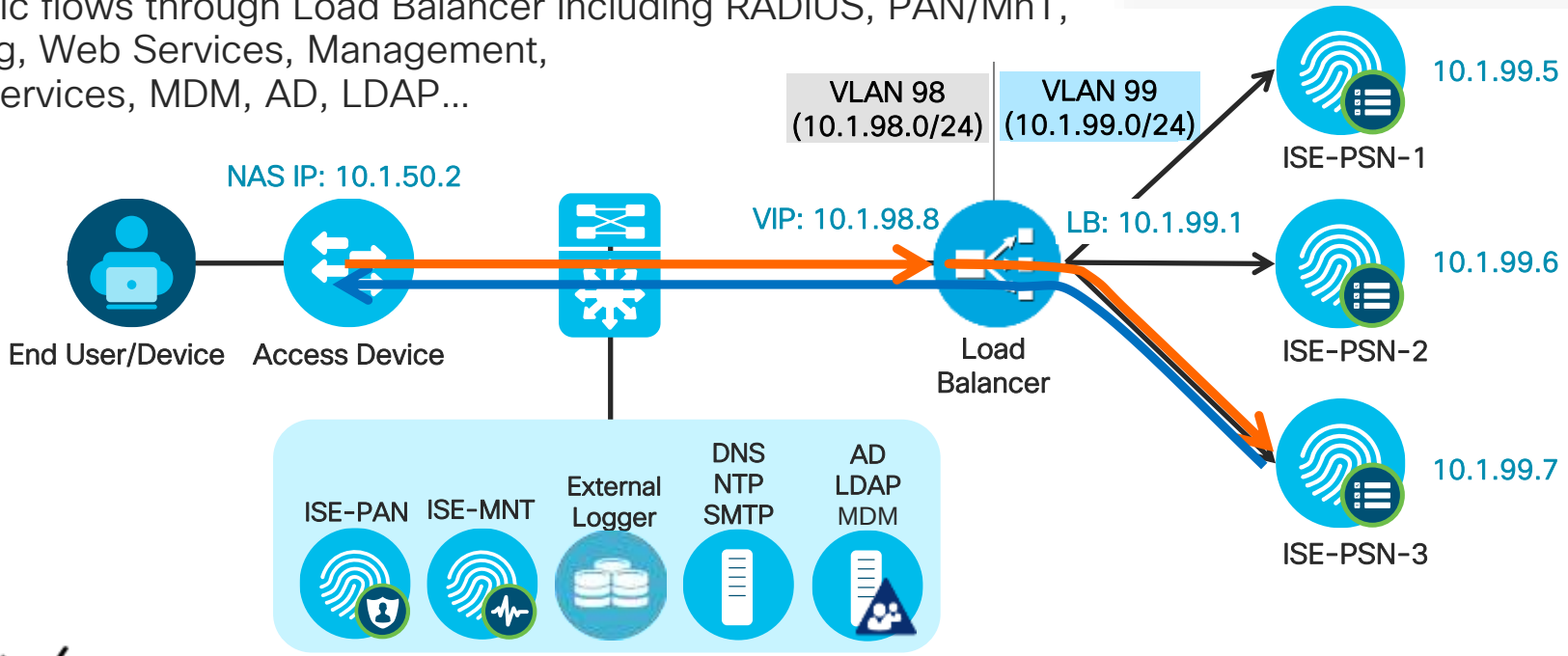
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traffic Flow—Fully Inline: Physical Separation

Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

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

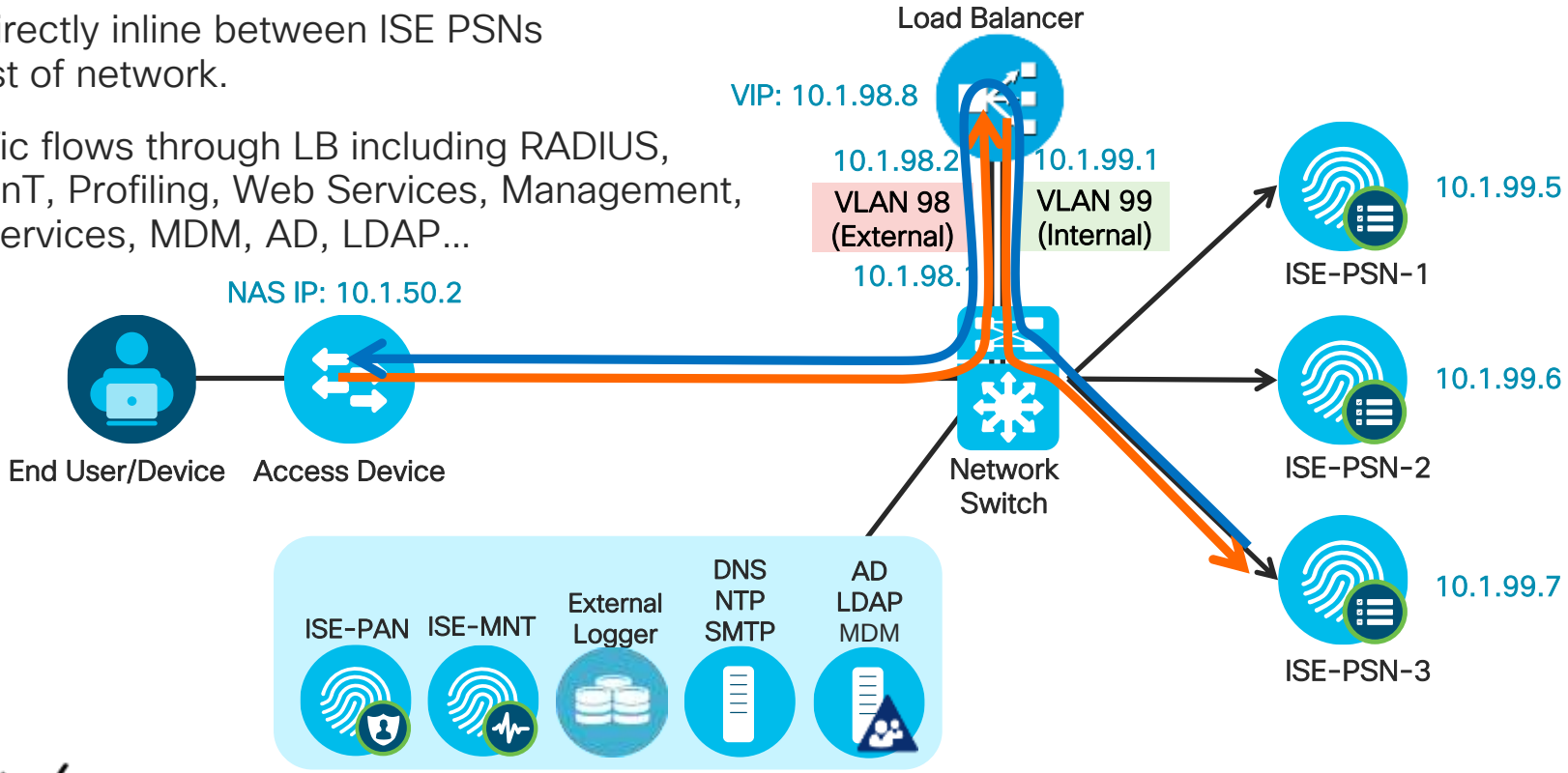


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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…

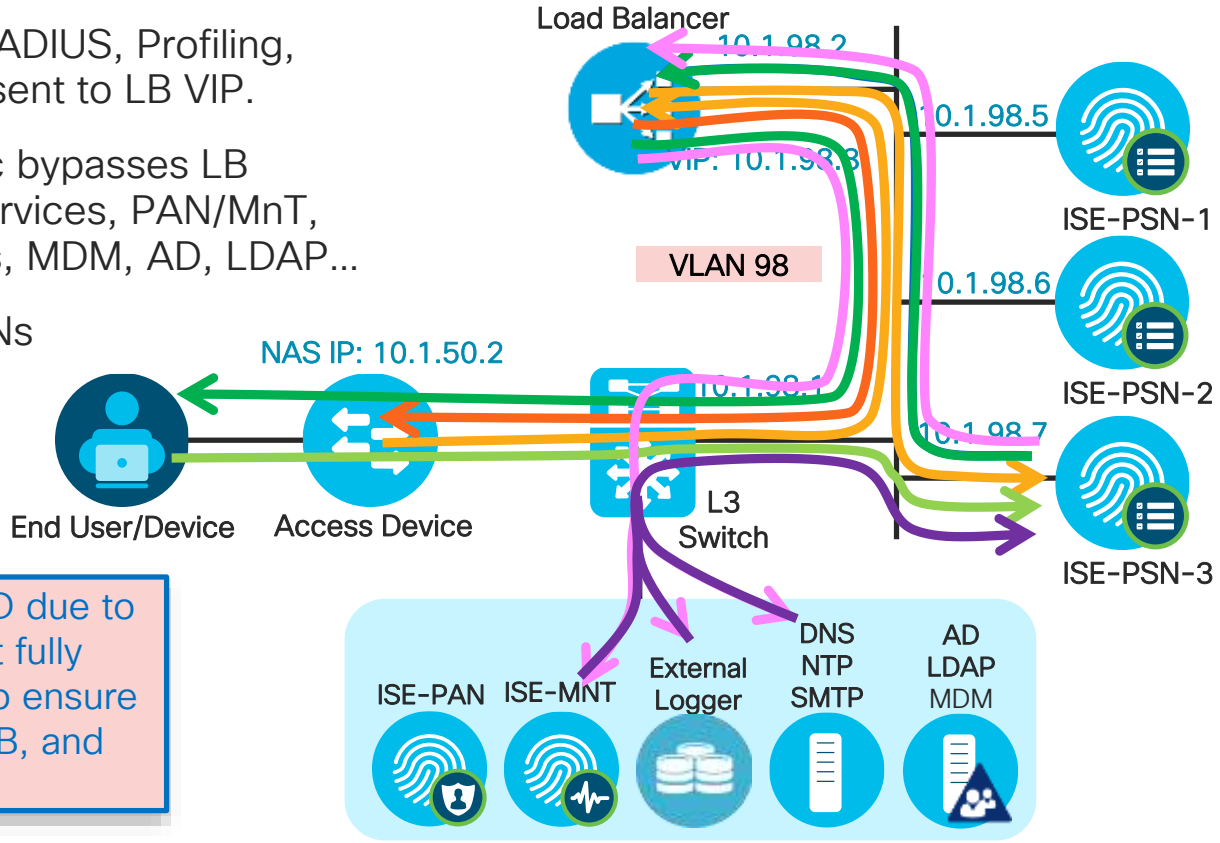


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



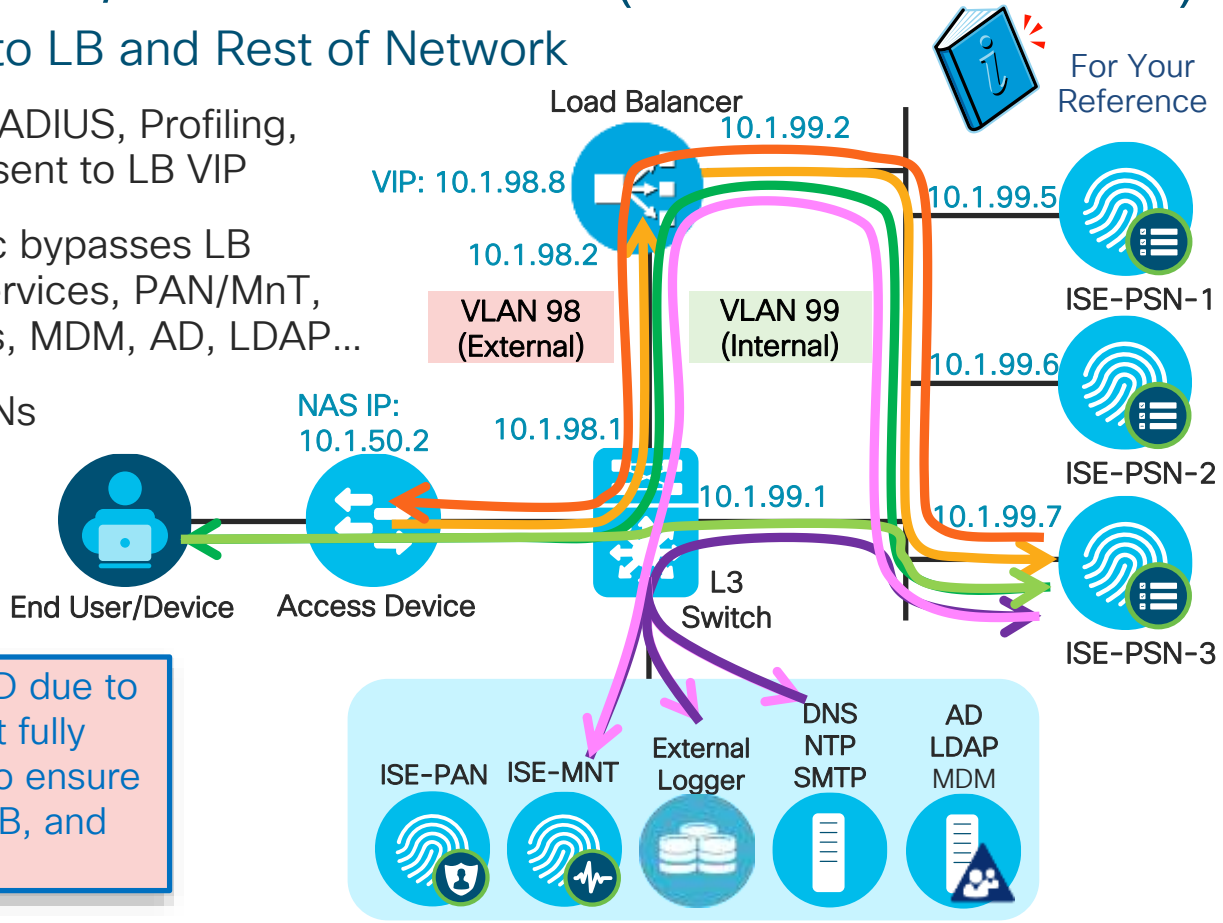
Generally NOT RECOMMENDED due to traffic flow complexity—must fully understand path of each flow to ensure proper handling by routing, LB, and end stations.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Partially Inline: Layer 3/Different VLANs (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



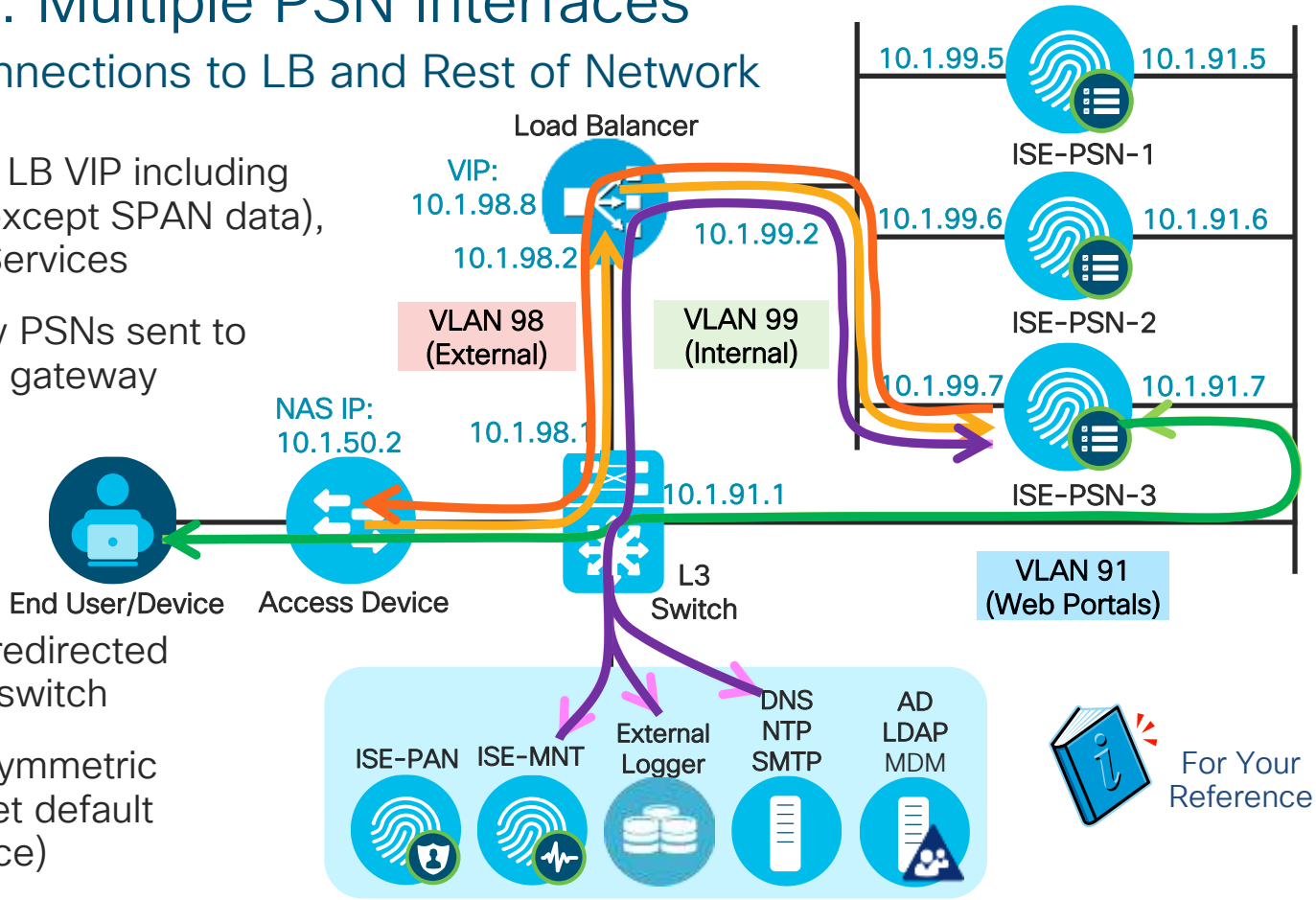
Generally NOT RECOMMENDED due to traffic flow complexity—must fully understand path of each flow to ensure proper handling by routing, LB, and end stations.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Partially Inline: Multiple PSN Interfaces

Separate PSN Connections to LB and Rest of Network

- All LB traffic sent to LB VIP including RADIUS, Profiling (except SPAN data), and directed Web Services
- All traffic initiated by PSNs sent to LB as global default gateway
- Redirected Web Services traffic bypasses LB
- For ISE 1.2, recommend SNAT redirected HTTPS traffic at L3 switch
- ISE 1.3+ supports symmetric traffic responses (set default gateway per interface)

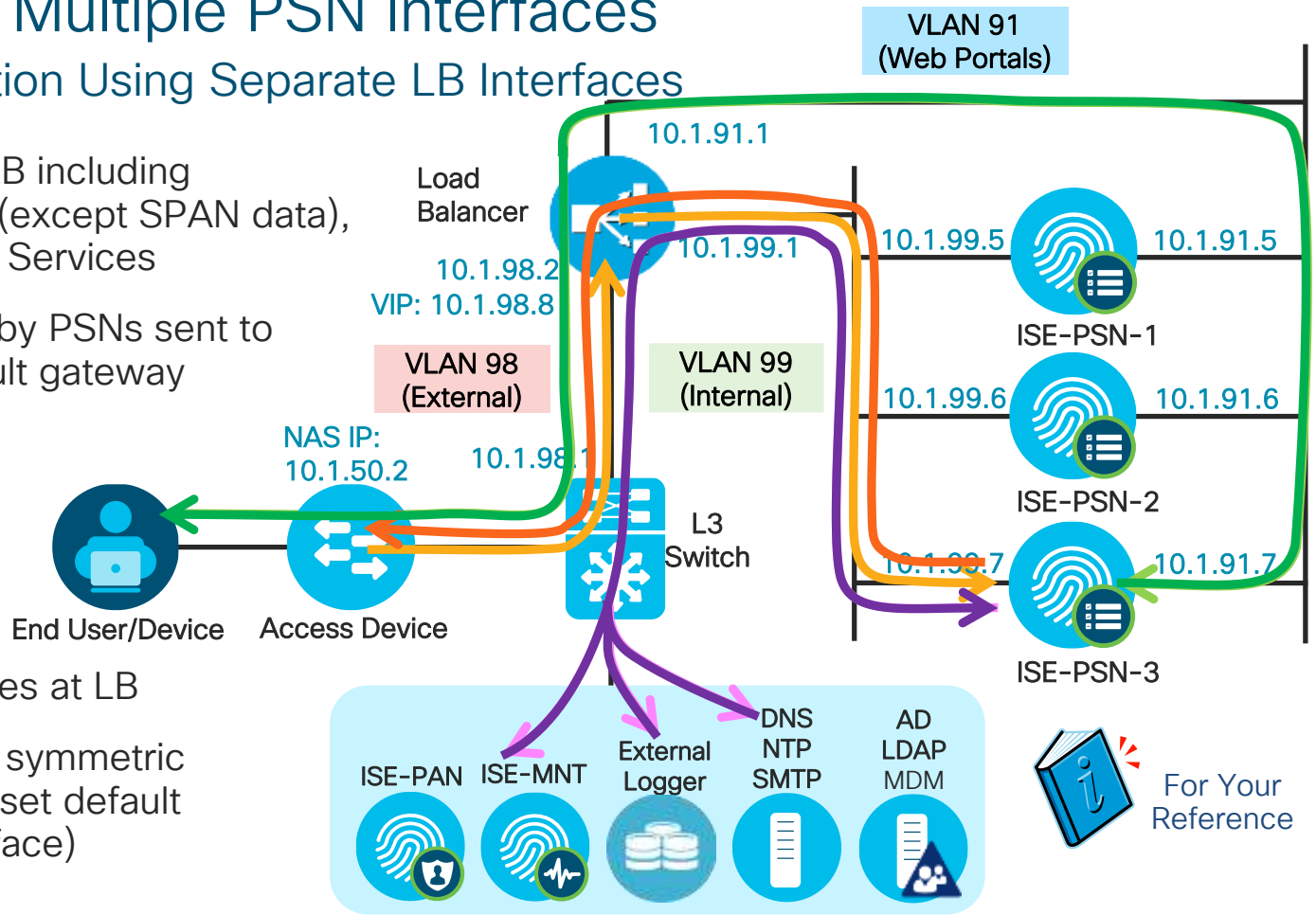


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fully Inline – Multiple PSN Interfaces

Network Separation Using Separate LB Interfaces

- All traffic sent to LB including RADIUS, Profiling (except SPAN data), and directed Web Services
- All traffic initiated by PSNs sent to LB as global default gateway
- LB sends Web Services traffic on separate PSN interface.
- For ISE 1.2, SNAT Web Services at LB
- ISE 1.3+ supports symmetric traffic responses (set default gateway per interface)



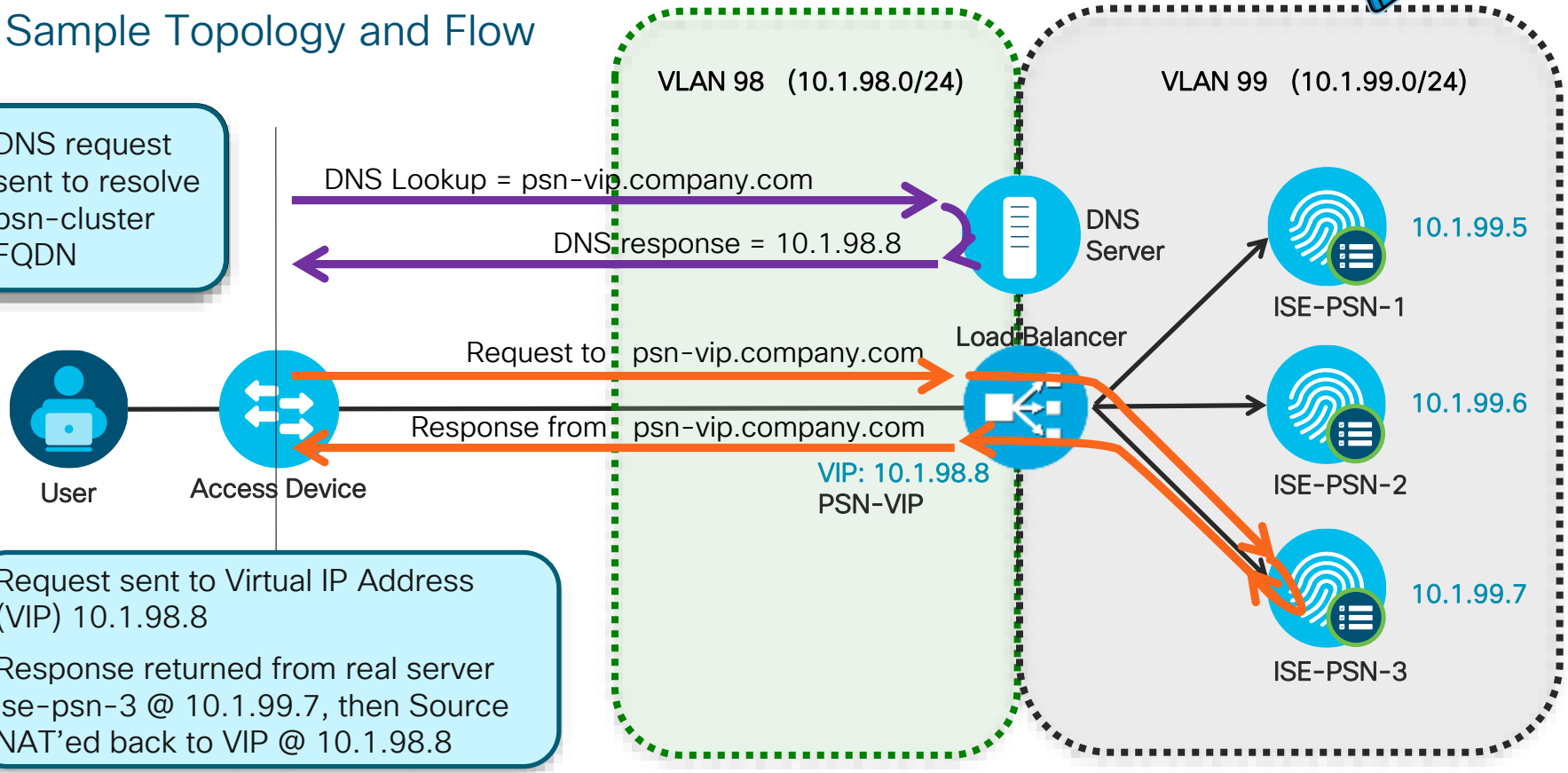
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Load Balancing

Sample Topology and Flow

For Your Reference

DNS request sent to resolve psn-cluster FQDN



Request sent to Virtual IP Address (VIP) 10.1.98.8

Response returned from real server ise-psn-3 @ 10.1.99.7, then Source NAT'ed back to VIP @ 10.1.98.8

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing Policy Services

- **RADIUS AAA Services**

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

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

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

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

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

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

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

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

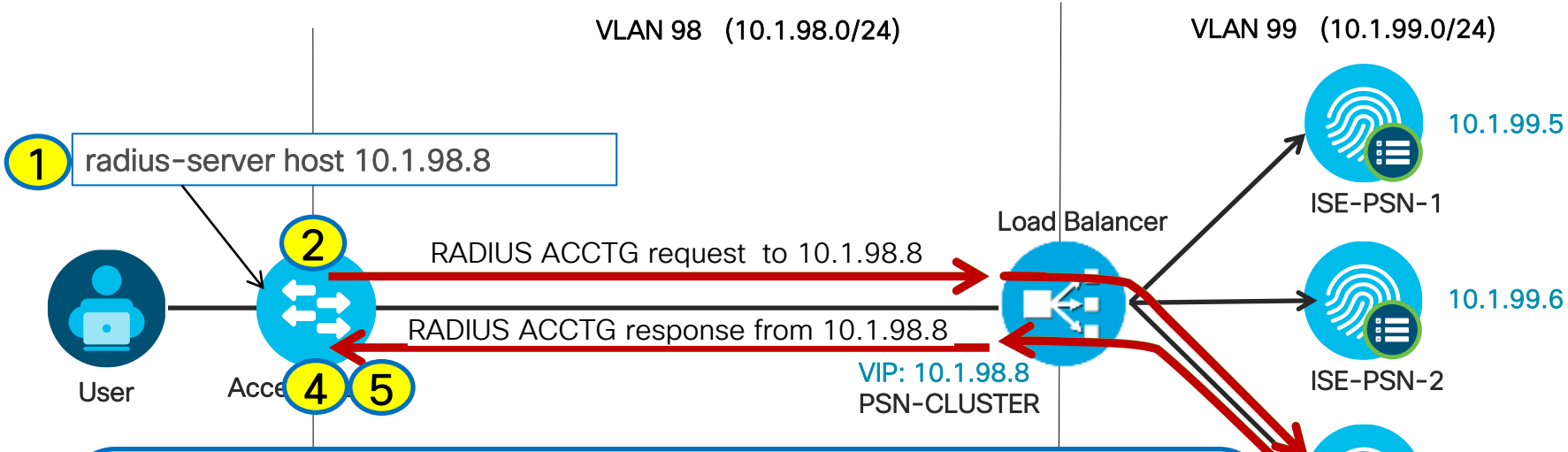
  LB VIP is target for TACACS+ requests. T+ not session based like RADIUS, so not required that requests go to same PSN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing RADIUS

Load Balancing RADIUS

Sample Flow



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancer General RADIUS Guidelines

For Your Reference

RADIUS Servers and Clients – Where Defined

ISE Admin Node > Network Devices

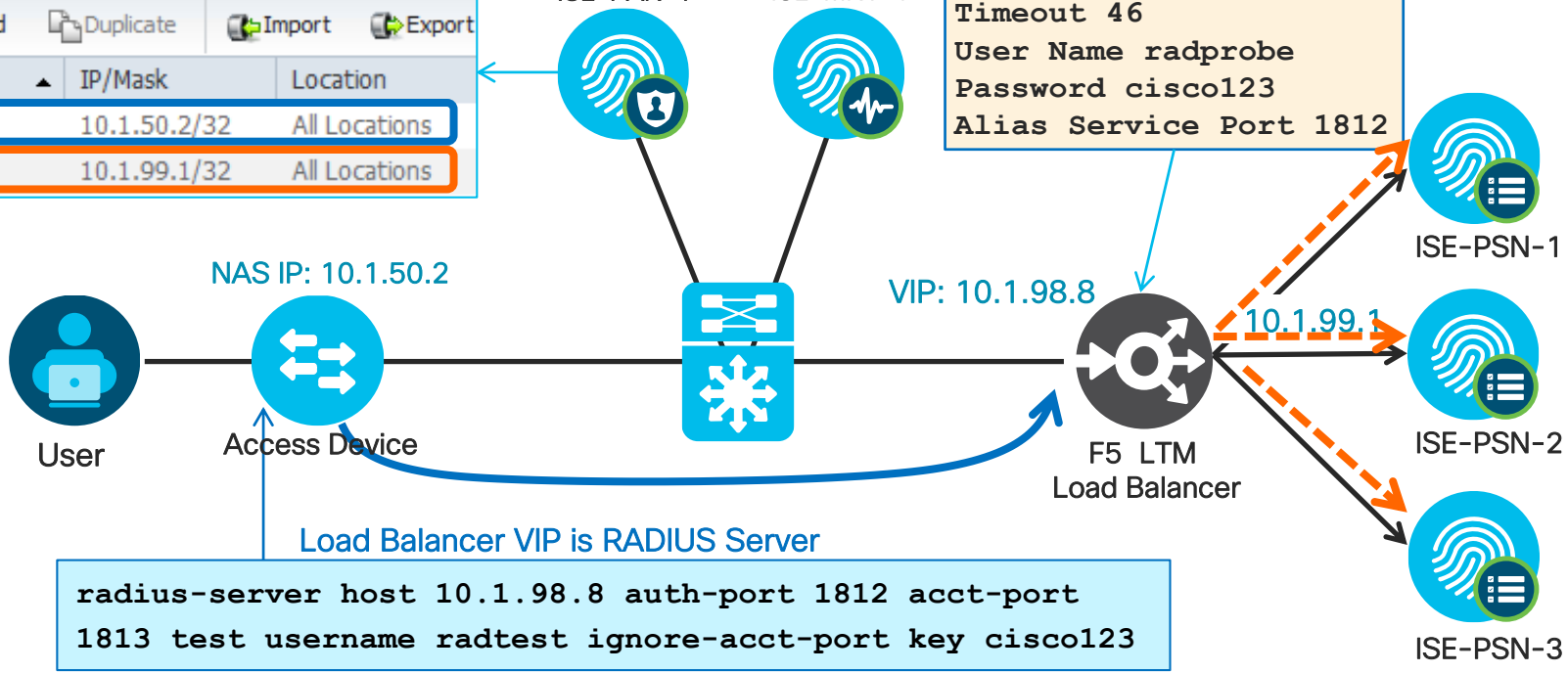
Network Devices (RADIUS Clients)

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

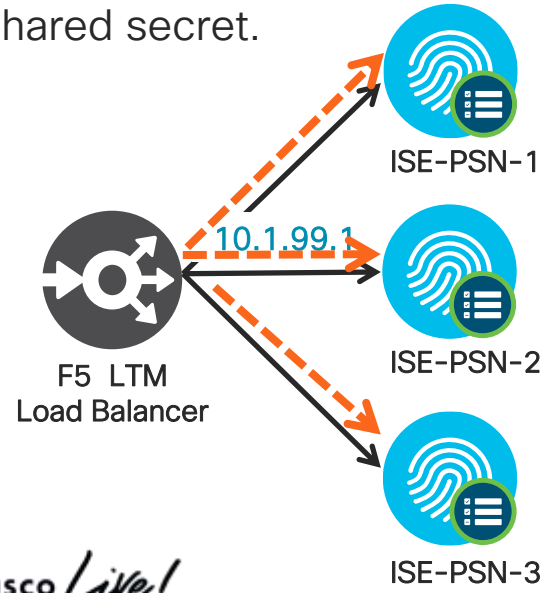
```
radius-server host 10.1.98.8 auth-port 1812 acct-port
1813 test username radtest ignore-acct-port key cisco123
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.



For Your Reference

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

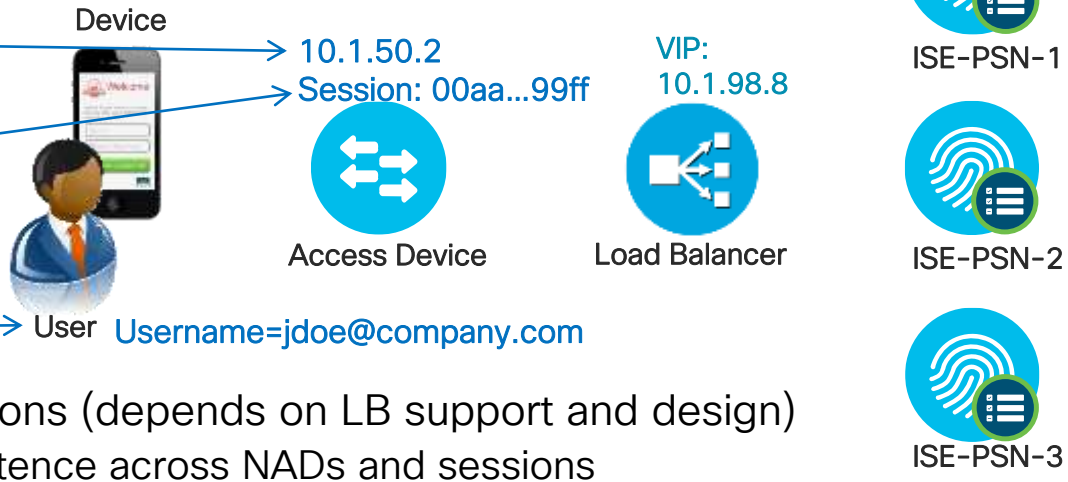
Key Input Format: ASCII / HEXADECIMAL

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancer Persistence (Stickiness) Guidelines

Persistence Attributes

- Common RADIUS Sticky Attributes
  - **Client Address**
    - Calling-Station-ID → MAC Address=00:C0:FF:1A:2B:3C
    - Framed-IP-Address → IP Address=10.1.10.101
  - **NAD Address** → 10.1.50.2
    - NAS-IP-Address
    - Source IP Address
  - **Session ID** → Session: 00aa...99ff
    - RADIUS Session ID
    - Cisco Audit Session ID
  - **Username** → Username=jdoe@company.com



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancer Stickiness Guidelines

Config Examples Based on Calling-Station-ID (MAC Address)

- Cisco ACE Example:

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

- F5 LTM iRule Example:

```
ltm rule RADIUS_iRule {
    when CLIENT_ACCEPTED {
persist uie [RADIUS::avp 31]
}}
```

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

- Citrix NetScaler Example:

```
add lb vserver radius-auth RADIUS 172.16.0.16 1812 -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)" -cltTimeout 120
add lb vserver radius-acct RADIUS 172.16.0.16 1813 -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)" -cltTimeout 120
set lb group RADIUS-Calling-Station-ID -persistenceType RULE -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)
```

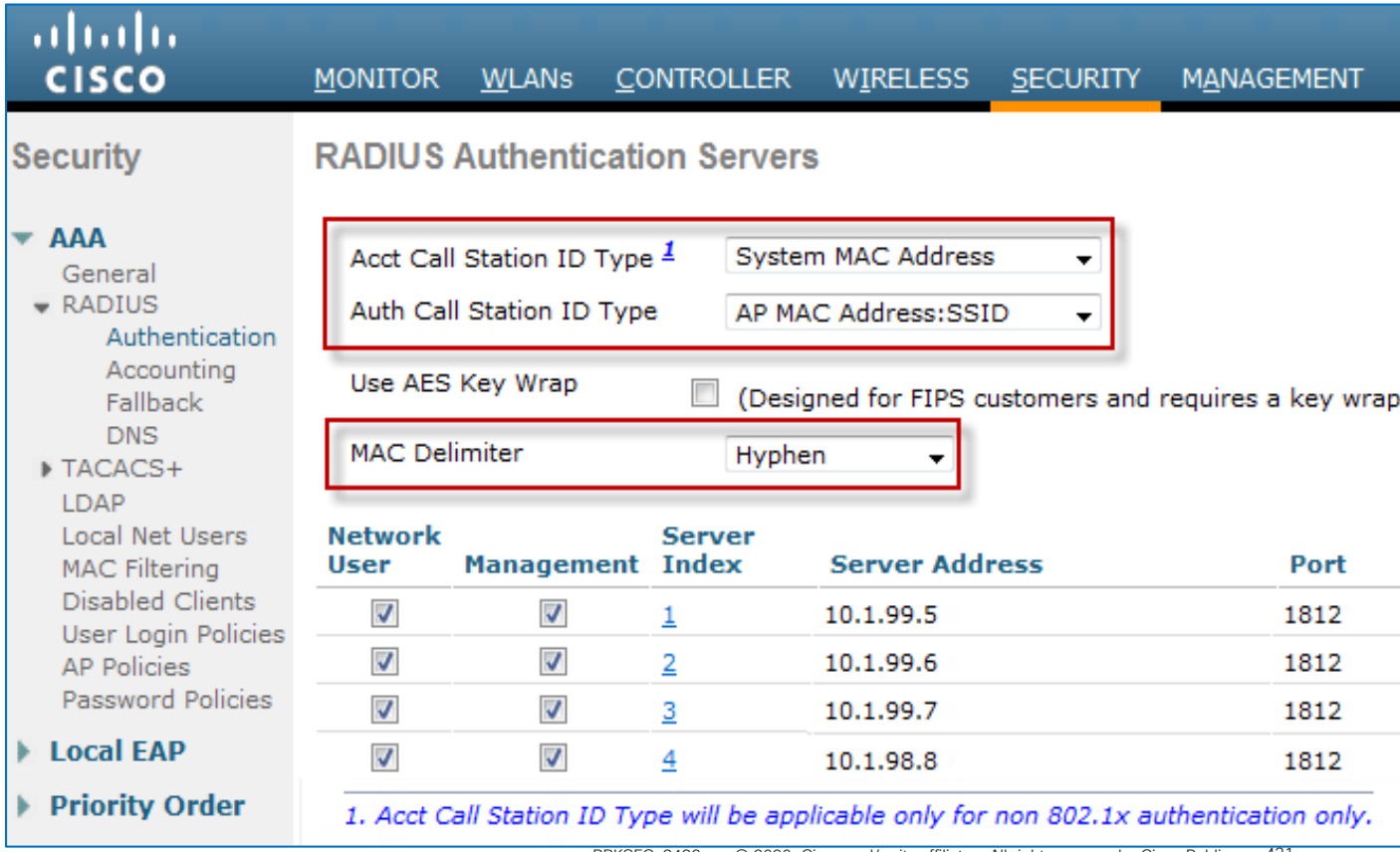

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ensure NAD Populates RADIUS Attributes

For Your Reference

Cisco WLC Example

- WLC sets Calling-Station-ID to MAC Address for RADIUS NAC-enabled WLANs
- General recommendation is to set Acct Call Station ID to **System MAC Address**
- Auth Call Station ID Type may not be present in earlier software versions



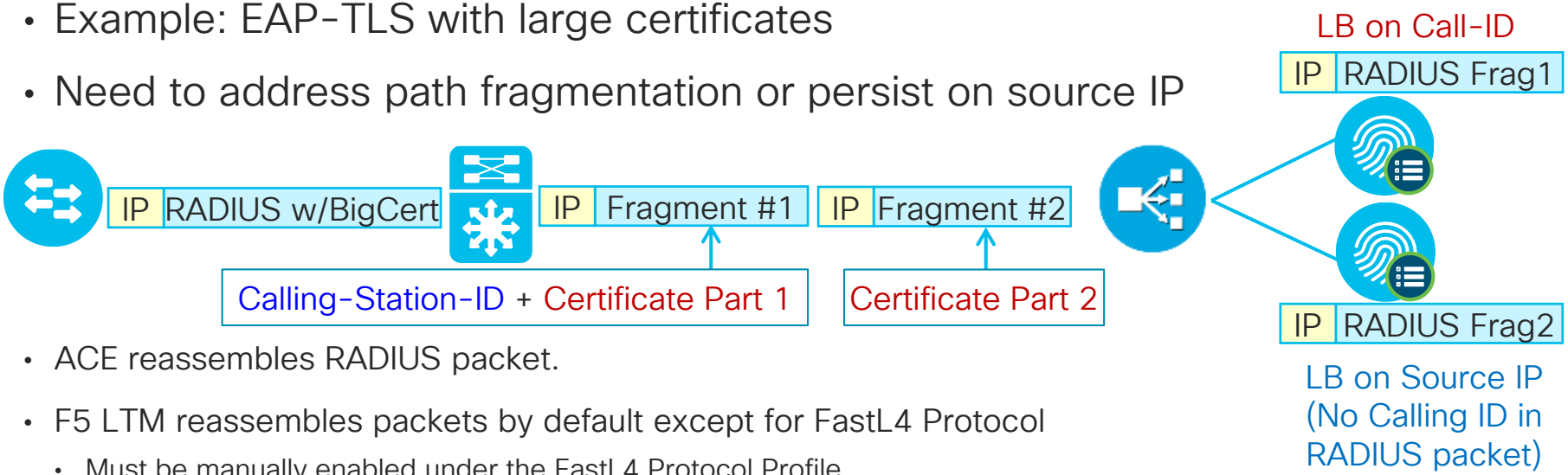
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LB Fragmentation and Reassembly

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

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

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



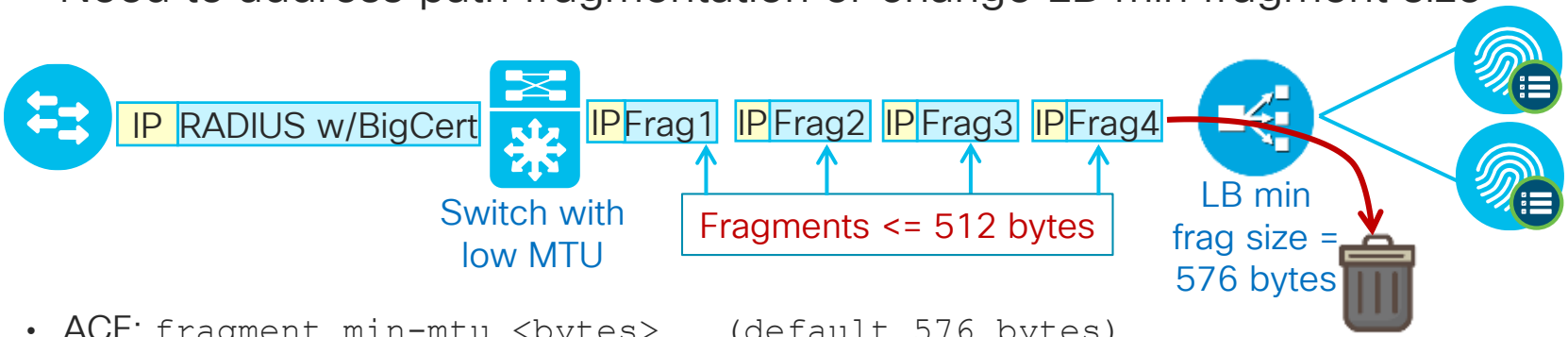
- ACE reassembles RADIUS packet.
- F5 LTM reassembles packets by default except for FastL4 Protocol
  - Must be manually enabled under the FastL4 Protocol Profile
- Citrix NetScaler fragmentation defect—Resolved in NetScaler 10.5 Build 50.10
  - Issue ID 429415 addresses fragmentation and the reassembly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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LB Fragmentation and Reassembly

Watch for packet fragments smaller than LB will accept!

- Example: Intermediate switch/gateway fragments packets below LB minimum
- Need to address path fragmentation or change LB min fragment size



- ACE: `fragment min-mtu <bytes>  (default 576 bytes)`
- F5 LTM: `# tmsh modify sys db tm.minipfragsize value 1`
  - Pre-11.6: Default = 576 bytes
  - 11.6.0+: Default = 566 bytes

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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#Wire
NAS IP Address:	10.1.50.2

Network Device	Server	Authorization Pr...	Identity Group
ace4710	ise-psn-2		
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-I
ace4710	ise-psn-2	Cisco_IP_Phones	Profiled:Cisco-I
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

User Story 8601 : CoA support for NAT'ed load balanced environments

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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	

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Allow Source NAT for PSN CoA Requests

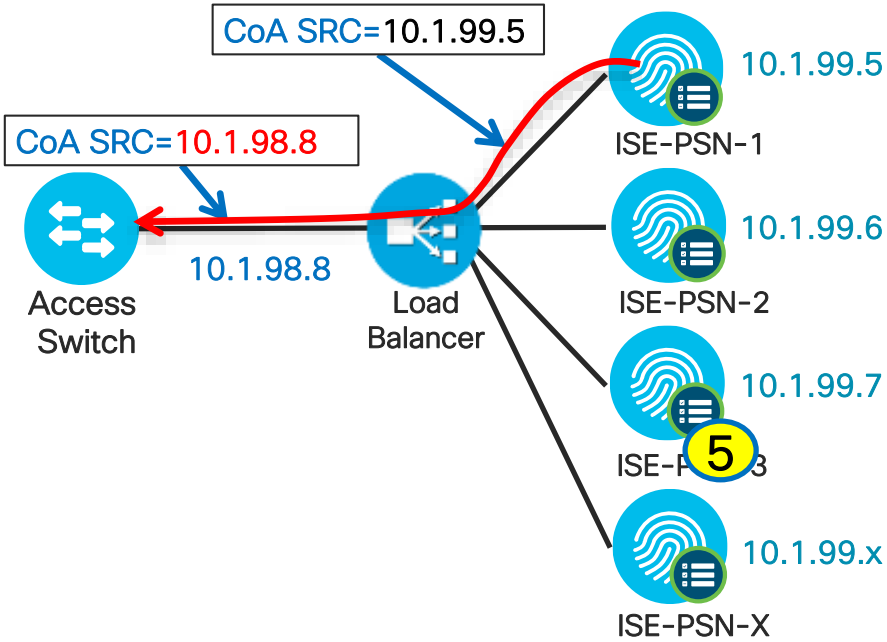
Simplifying Switch CoA Configuration

- Match traffic from PSNs to UDP/1700 or UDP/3799 (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
```



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Allow Source NAT for PSN CoA Requests

For Your Reference

Cisco ACE Load Balancer Example

```
access-list NAT-COA line 5 extended permit udp 10.1.99.0 255.255.255.248 any eq 1700

class-map match-any NAT-CLASS
  2 match access-list NAT-COA

policy-map multi-match NAT-POLICY
  class NAT-CLASS
    nat dynamic 1 vlan 98

interface vlan 98
  description NAD-SIDE
  nat-pool 1 10.1.98.8 10.1.98.8 netmask 255.255.255.255 pat

interface vlan 99
  description PSN-CLUSTER
  service-policy input NAT-POLICY
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Allow Source NAT for PSN CoA Requests

For Your Reference

F5 LTM Load Balancer Example

```
ltm virtual /NAD_ICommon/RADIUS-COA-SNAT {
destination /Common/10.0.0.0:1700
ip-protocol udp
mask 255.0.0.0
profiles {
/Common/udp { }
}
source 10.1.99.0/27
source-address-translation {
pool /Common/radius_coa_snatpool
type snat
}
translate-address disabled
translate-port enabled
```

```
ltm snatpool /Common/radius_coa_snatpool {
members {
/Common/10.1.98.8
}
}
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Allow Source NAT for PSN CoA Requests

For Your Reference

Citrix NetScaler Load Balancer Example

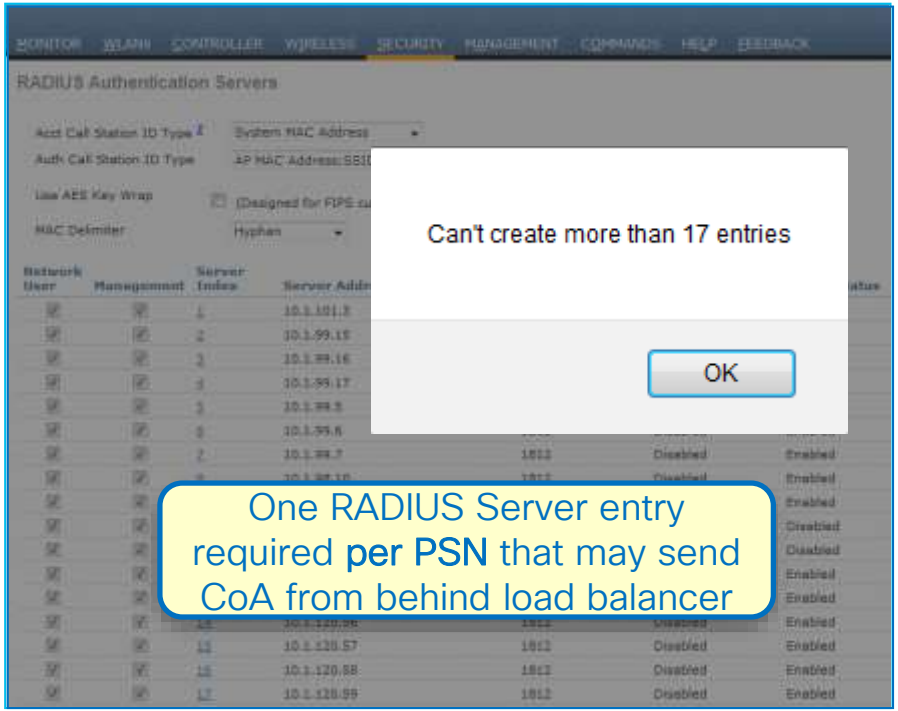
```
add ns acl COA-NAT ALLOW -srcIP = 10.1.99.5-10.1.99.18 -destPort =
1700 -protocol UDP -priority 10

apply ns acls

set rnat COA-NAT -natIP 10.1.98.8
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Allow Source NAT for PSN CoA Requests

Simplifying WLC CoA Configuration

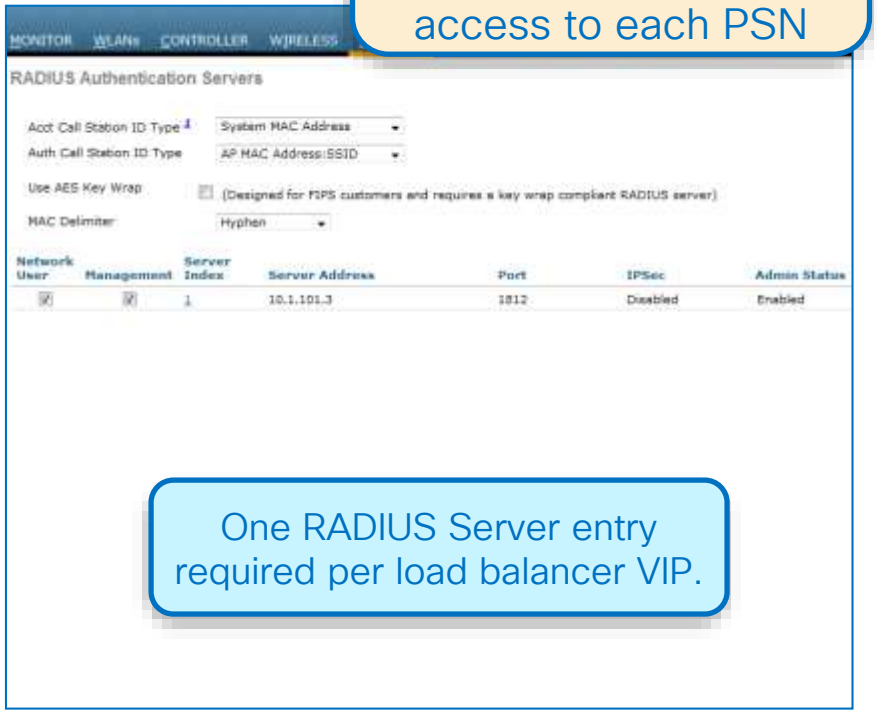
- Before:



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

- After

Simplifies config and reduces # ACL entries required to permit access to each PSN

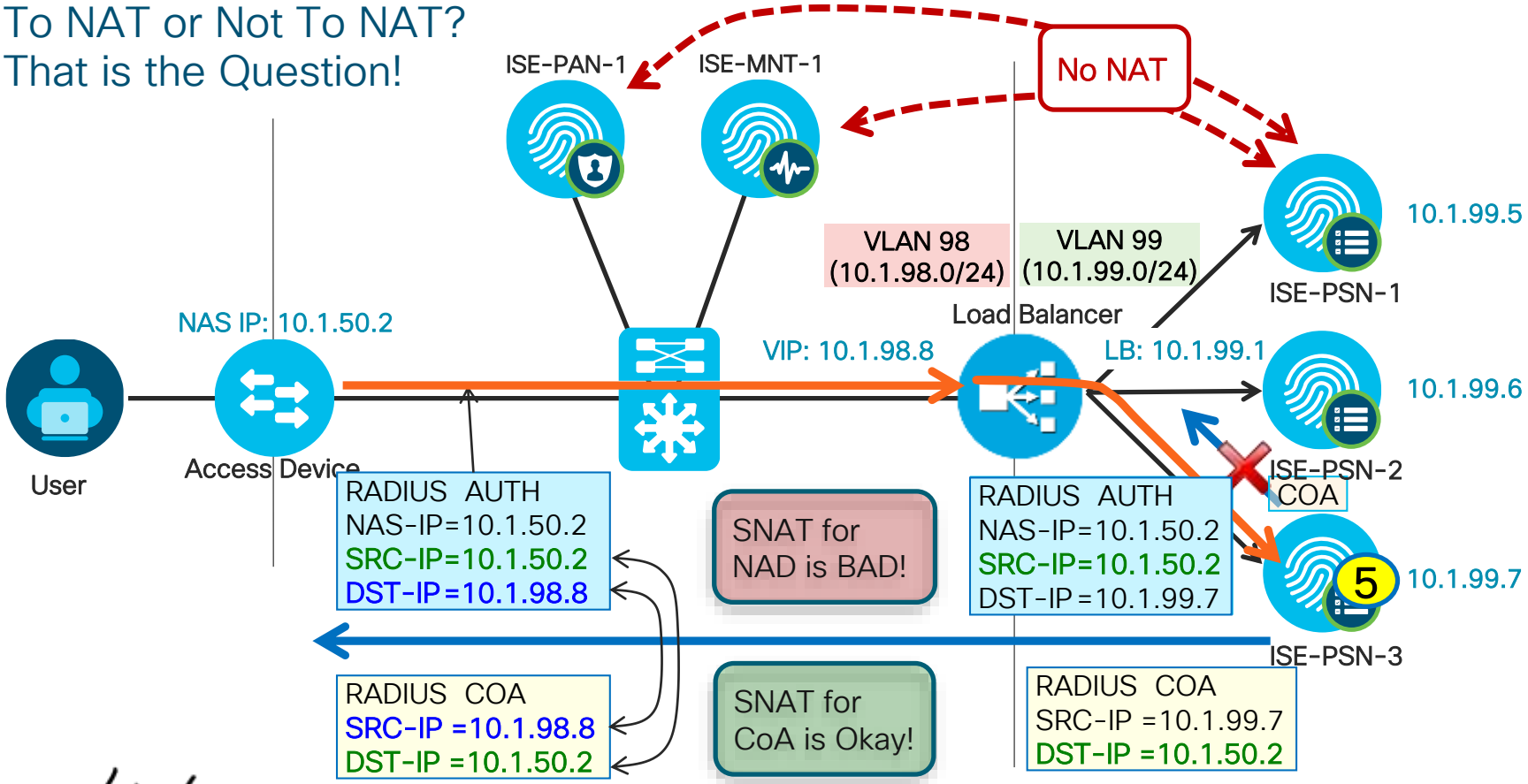


One RADIUS Server entry required per load balancer VIP.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAT Guidelines for ISE RADIUS Load Balancing

To NAT or Not To NAT?
That is the Question!

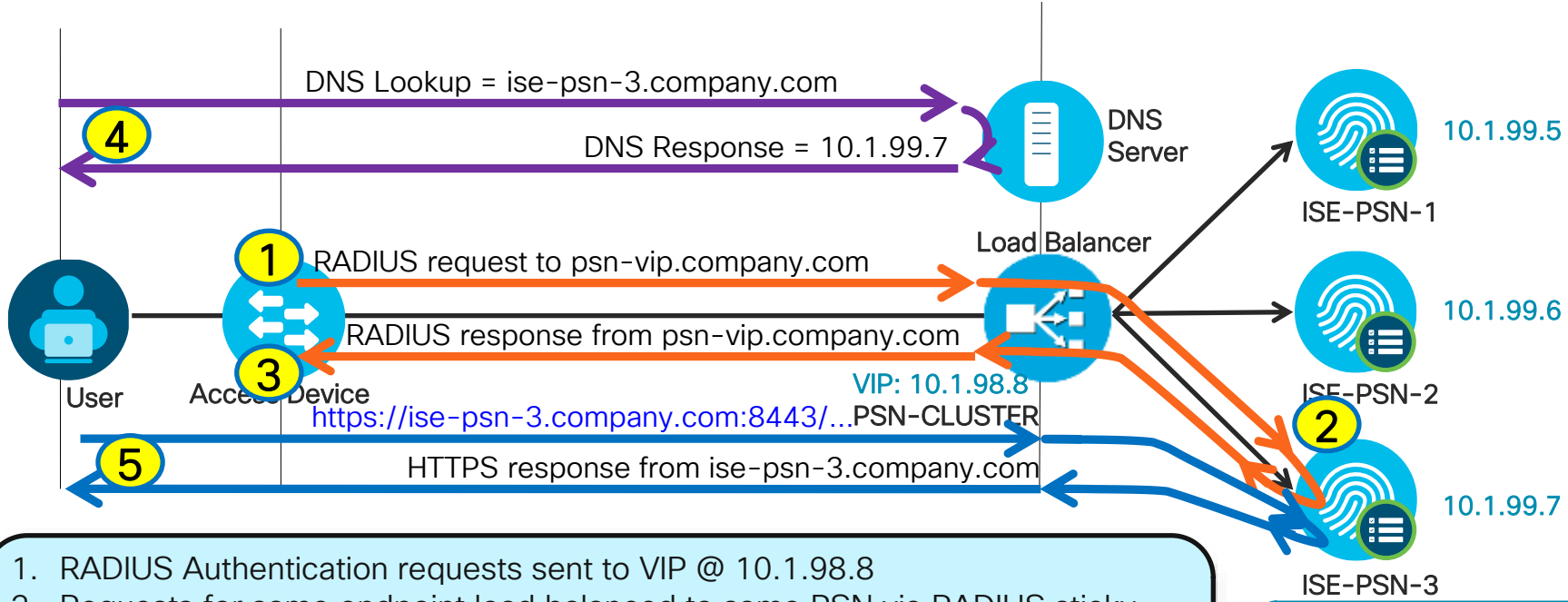


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing ISE Web Services

Load Balancing with URL-Redirection

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



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

ISE Certificate

Subject CN = ise-psn-3.company.com

Load Balancing URL-Redirected Services

When and How to Override Default URL Redirection from Client to PSN

- Use Cases for LB to Terminate redirected HTTPS Requests
  - Obfuscate PSN node names/IP addresses. (Do not want PSN name exposed to browser)
  - Ability to use a different certificate for user facing connection
  - Apply security inspections on web-based requires
  - As a way to secure PSN interfaces in DMZ.
- Requires Authorization Profile be configured with Static Hostname option.
- Load Balancer must be able to persist web request to same PSN that serviced RADIUS session Common methods (else rely on ISE policy logic):
  - LB includes Framed-IP-Address with RADIUS sticky; correlates Framed-IP to HTTPS source IP
  - LB includes BRKSEC3432 with RADIUS sticky; correlates BRKSEC3432 in web request

```
url-redirect=https://<PSN_CN>:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

Note: Since ISE assumes HTTPS for web access, offload cannot be used to increase SSL performance. Load Balancer must reestablish SSL connection to real PSN servers.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

URL Redirection Using Static IP/Hostname

Overriding Automatic Redirection to PSN IP Address/FQDN

- Allows static IP or FQDN value to be returned for CWA or other URL-Redirected Flows
- Common use case: Public DNS or IP address (no DNS available) must be used while preserving variable substitution for *port* and *sessionId* variables.

Common Tasks

Policy > Policy Elements > Results > Authorization > Authorization Profiles

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Centralized Web Auth ▾ ACL ACL-WEBAUTH-REDIRECT

☑ Static IP/Host name public.company.com

DMZ PSN Certificate must match IP/Static FQDN

Specified IP Address/Hostname MUST point to the same PSN that terminates the RADIUS session.

If multiple PSNs, requires LB persistence or AuthZ Policy logic to ensure redirect occurs to correct PSN.

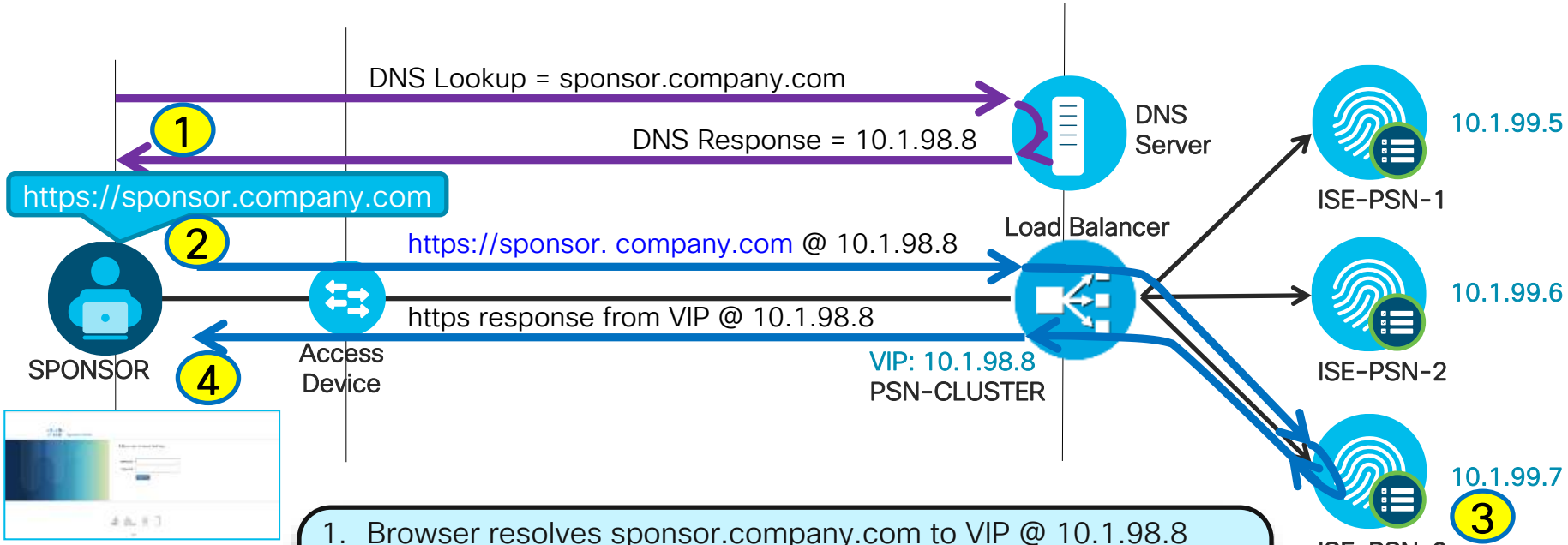
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	DMZ_Guest	if **Select an item** AND Network Access:ISE Host Name EQUALS ise-dmz.cts.local	then Central_Web_Auth_IP
✓	Default	if no matches, then Central_Web_Auth	

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing Non-Redirected Web Servic

For Your Reference

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



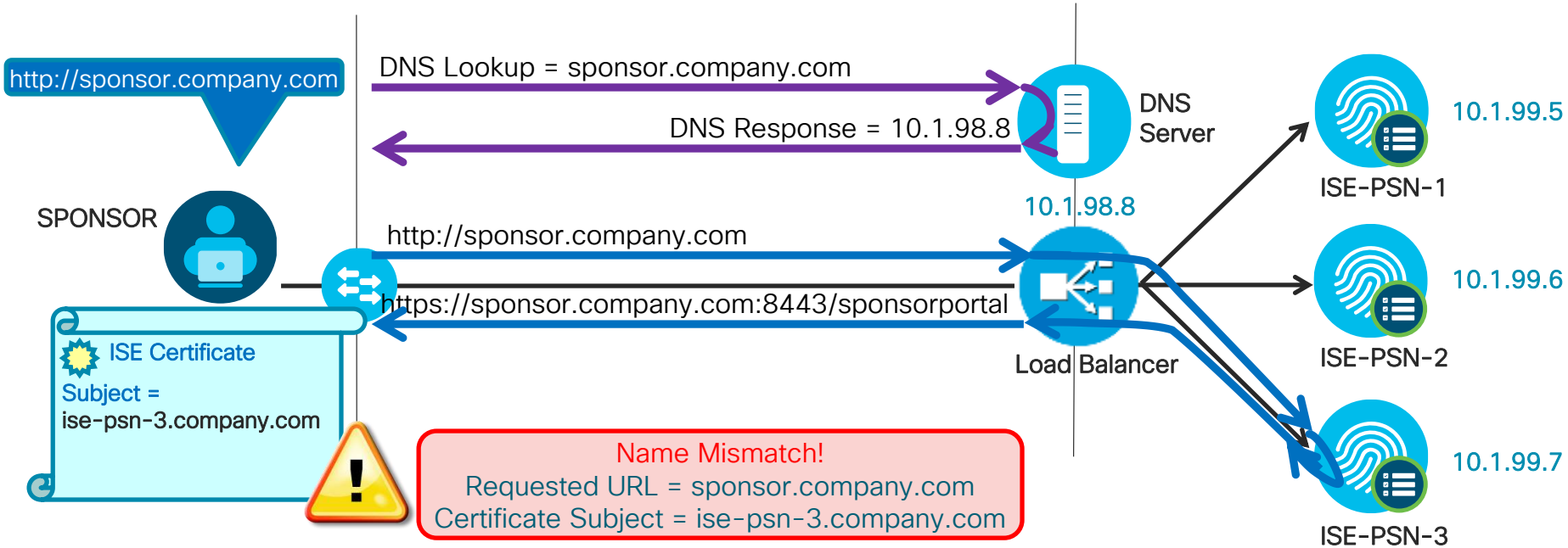
1. Browser resolves sponsor.company.com to VIP @ 10.1.98.8
2. Web request sent to https://sponsor.company.com @ 10.1.98.8
3. ACE load balances request to PSN based on IP or HTTP sticky
4. HTTPS response received from ise-psn-3 @ 10.1.99.7 → translated to VIP @ 10.1.98.8 when passes through LB.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Certificate without SAN

Certificate Warning - Name Mismatch

For Your Reference



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Certificate with SAN

No Certificate Warning

For Your Reference

SPONSOR

DNS Lookup = sponsor.company.com

DNS Response = 10.1.98.8

DNS Server

10.1.98.8

http://sponsor.company.com

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing Preparation

Configure DNS and Certificates

For Your Reference

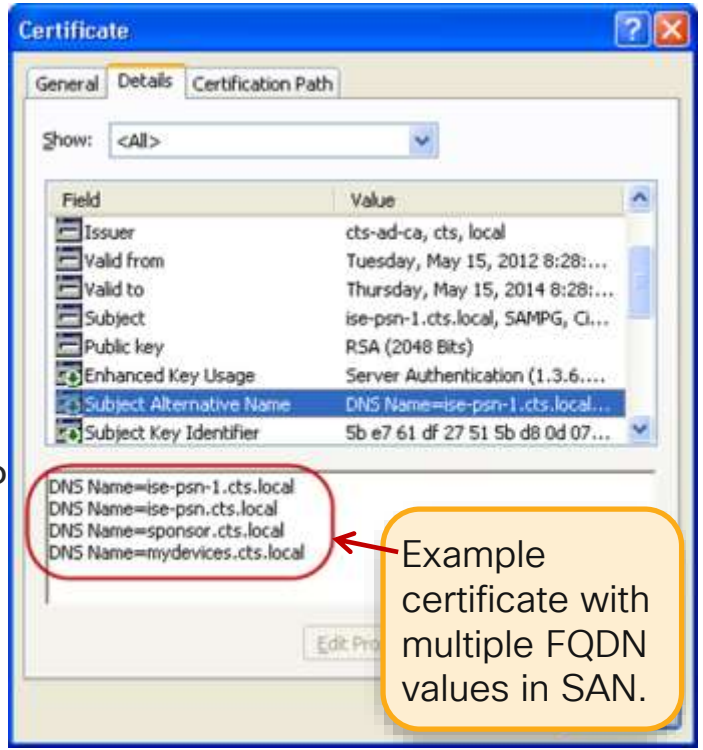
- Configure DNS entry for PSN cluster(s) and assign VIP IP address.

  Example: psn-vip.company.com

DNS SERVER: DOMAIN = COMPANY.COM			
PSN-VIP	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.

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

“Universal Certs”

UCC or Wildcard SAN Certificates

Subject Alternative Name (SAN)

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

Check box to use wildcards

Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

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

Subject

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

Subject Alternative Name (SAN)

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

CN must also exist in SAN

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

Other FQDNs or wildcard as “DNS Names”

IP Address is also option

ISE Certificates

General Best Practices

For Your Reference

- Make sure all certificate CN names can be resolved by DNS
- Use lower case for appliance hostname, DNS name, certificate CN
- ISE cert CSR: Use format “CN=<FQDN>” for subject name
- Ensure time is synced – Use NTP with TZ-UTC for all nodes
- Signed by Trusted CA – required for each node
  - For external users/guests, certs should be signed by 3rd-party CA
- Install entire certificate chains as individual certs into ISE trust store
  - For Web admin, node communications, web portals, PEAP negotiation, select HTTPS option for server certificate—currently limited to one cert
  - For EAP-TLS, enable “Trust for client authentication” for trusted certs
- Use PEM, not DER encoding for import/export operations.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

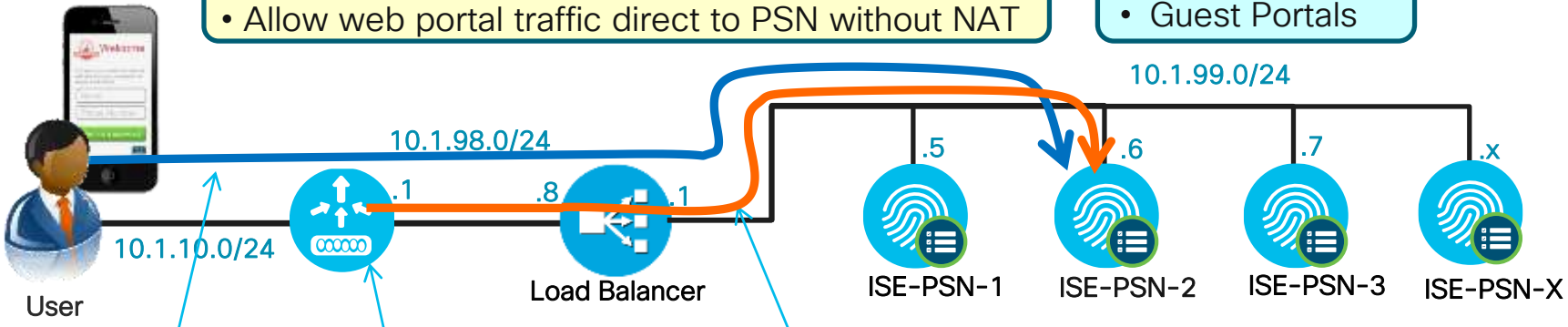
Load Balancer NAT Guidelines for Web Traff

For Your Reference

URL-Redirected Traffic with Single PSN Interface

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

- RADIUS
- Guest Portals



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...

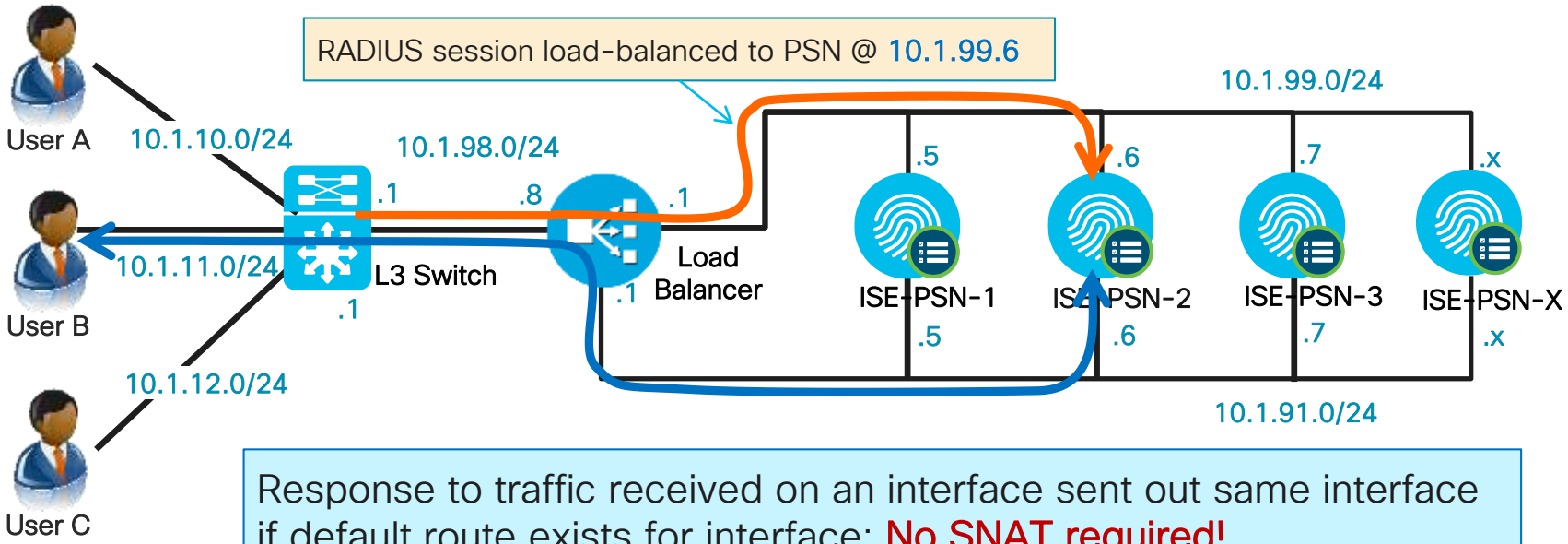
Browser traffic redirected to IP for ise-psn-2.company.com:
https://10.1.99.6:8443/guestportal/Login...

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dedicated Web Interfaces under ISE 1.3+

For Your Reference

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 10.1.99.1eth0
Default route 0.0.0.0/0 10.1.91.1eth1

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dedicated Web Interfaces under ISE 1.3+

For Your Reference

Symmetric Traffic Flows

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

```
ise24-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

```
ise24-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
```

What is default route for outbound connections when multiple default routes configured?

ISE 1.3/1.4: Round-robin
ISE 2.0: ip default-gateway

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SSL Certificates for Internal Server Names

For Your Reference

After November 1, 2015 Certificates for Internal Names Will No Longer Be Trusted

In November 2011, the CA/Browser Forum (CA/B) adopted Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates that took effect on July 1, 2012. These requirements state:

CAs should notify applicants prior to issuance that use of certificates with a Subject Alternative Name (SAN) extension or a Subject Common Name field containing a reserved IP address or internal server name has been deprecated by the CA/B

CAs should not issue a certificate with an expiration date later than November 1, 2015 with a SAN or Subject Common Name field containing a reserved IP address or internal server Name

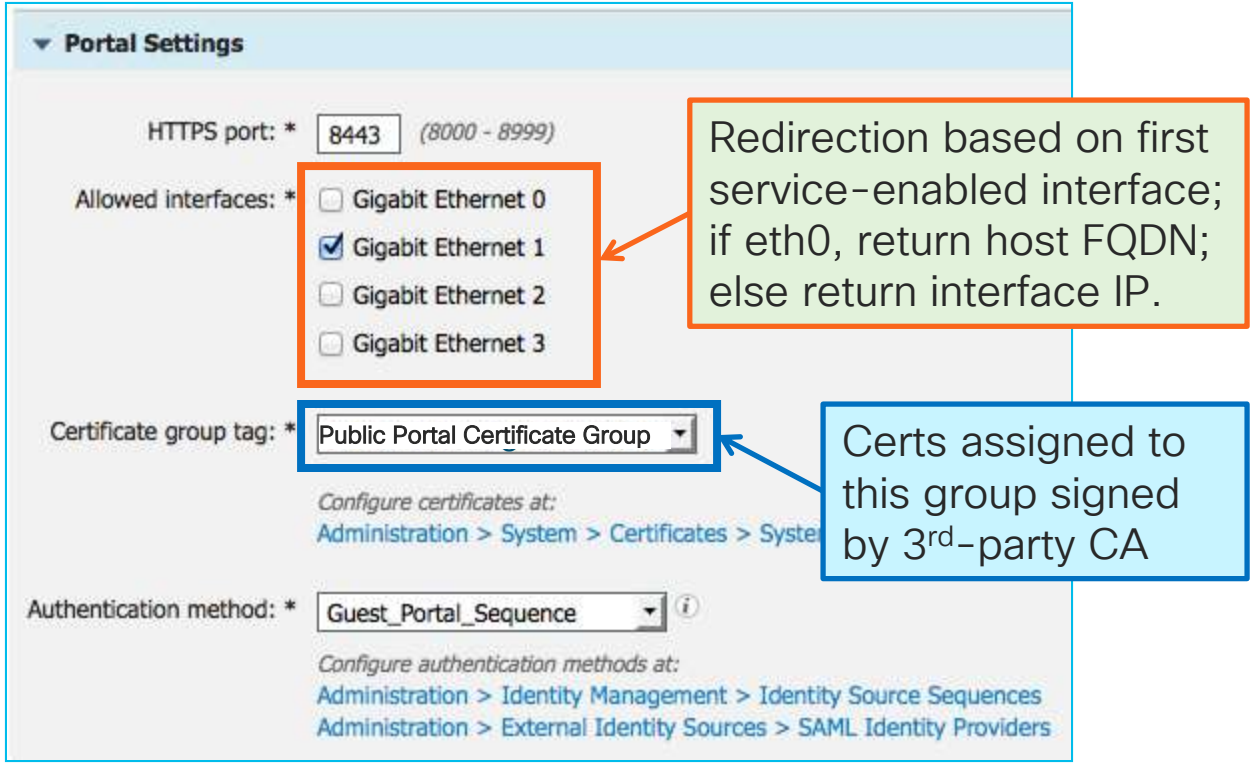
Source: Digicert – https://www.digicert.com/internal-names.htm

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Publicly-Signed Certs for Guest Portals!

For Your Reference

- Starting in ISE 1.3, HTTPS cert for Admin can be different from web portals
- Guest portals can use a different, public certificate
- Admin and internal employee portals (or EAP) can still use certs signed by private CA.



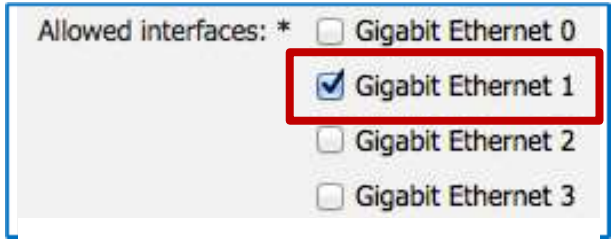
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CWA Example

DNS and Port Settings–Single Interface Enabled for Guest Portal

For Your Reference

- CWA Guest Portal access for ISE-PSN-1 configured for eth1



- IP Address for eth1 on ISE-PSN-1 is 10.1.91.5

ISE Node	IP Address	Interface
ISE-PSN-1	10.1.99.5	# eth0
ISE-PSN-1	10.1.91.5	# eth1
ISE-PSN-1	10.1.92.5	# eth2
ISE-PSN-1	10.1.93.5	# eth3
ISE-PSN-1	10.1.94.5	# eth4
ISE-PSN-1	10.1.95.5	# eth5

- Resulting URL Redirect = https://10.1.91.5:8443/...

I have a feeling this is going to end badly!

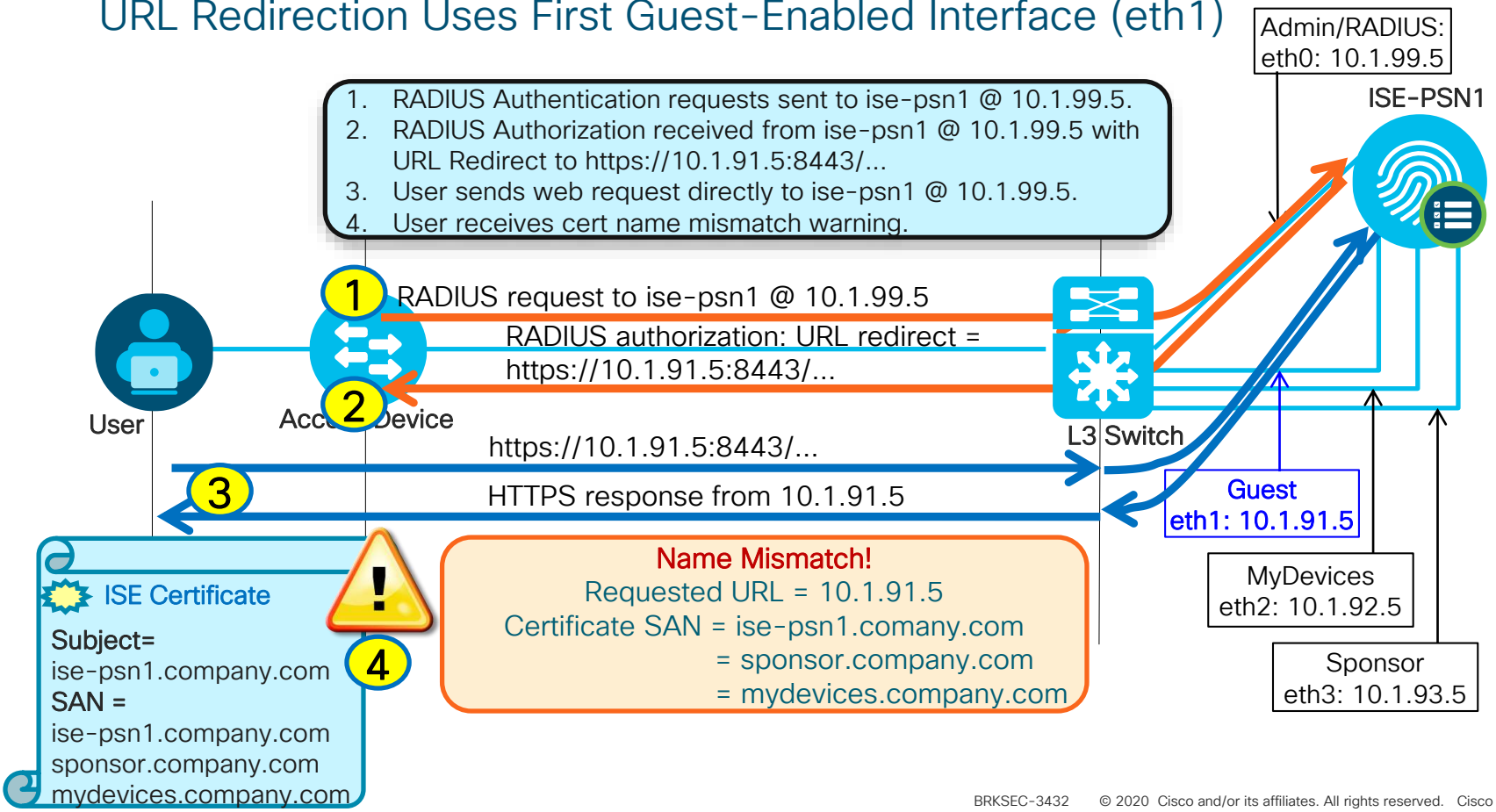
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CWA Example with FQDNs in SAN

URL Redirection Uses First Guest-Enabled Interface (eth1)

For Your Reference

1. RADIUS Authentication requests sent to ise-psn1 @ 10.1.99.5.
2. RADIUS Authorization received from ise-psn1 @ 10.1.99.5 with URL Redirect to https://10.1.91.5:8443/...
3. User sends web request directly to ise-psn1 @ 10.1.99.5.
4. User receives cert name mismatch warning.



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Interface Aliases

Specify alternate hostname/FQDN for URL redirection

For Your Reference

- Aliases assigned to interfaces using **ip host** global config command in ADE-OS:

```
(config)# ip host <interface_ip_address> <hostname|FQDN> <hostname|FQDN>
```

- Up to two values can be specified—hostname and/or FQDN; if specify hostname, then globally configured **ip domain-name** appended for use in URL redirection.

→ FQDN can have different domain than global domain!!!

- GigabitEthernet1 (GE1) Example:

```
ise-psn1/admin(config)#  ip  host  10.1.91.5  ise-psn1-guest  ise-psn1-guest.company.com
```

- Host entry for Gigabit Ethernet 0 (eth0) cannot be modified
- Use **show run** to view entries; Use **no ip host <ip_address>** to remove entry.
- Change in interface IP address or alias requires application server restart.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Interface Alias Example

For Your Reference

DNS and Port Settings – Single Interface Enabled for Guest

- Interface eth1 enabled for Guest Portal
- (config)# ip host 10.1.91.5 ise-psn1-guest.company.com
- URL redirect = https://ise-psn1-guest.company.com:8443/...
- Guest DNS resolves FQDN to correct IP address

FQDN with Publicly-Signed Cert

DNS SERVER
DOMAIN = COMPANY.COM

ISE-PSN1-GUEST	IN	A	10.1.91.5	# eth1
ISE-PSN2-GUEST	IN	A	10.1.91.6	# eth1
ISE-PSN3-GUEST	IN	A	10.1.91.7	# eth1

DNS SERVER
DOMAIN = COMPANY.LOCAL

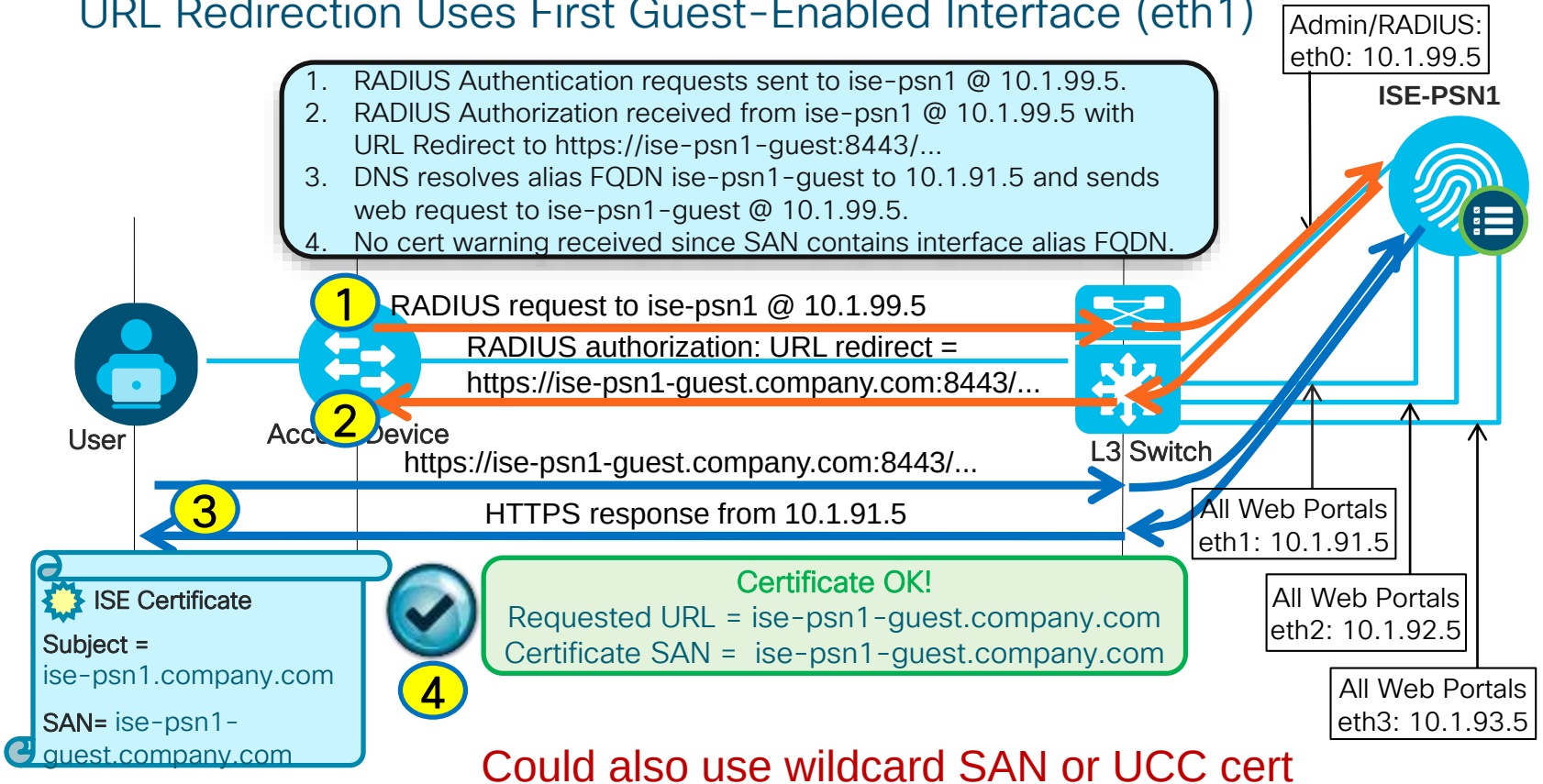
ISE-PSN1	IN	A	10.1.99.5	# eth0
ISE-PSN1-MDP	IN	A	10.1.92.5	# eth2
ISE-PSN1-SPONSOR	IN	A	10.1.93.5	# eth3
ISE-PSN2	IN	A	10.1.99.6	# eth0
ISE-PSN2-MDP	IN	A	10.1.92.6	# eth2
ISE-PSN2-SPONSOR	IN	A	10.1.93.6	# eth3
ISE-PSN3	IN	A	10.1.99.7	# eth0
ISE-PSN3-MDP	IN	A	10.1.92.7	# eth2
ISE-PSN3-SPONSOR	IN	A	10.1.93.7	# eth3

CWA Example using Interface Alias

URL Redirection Uses First Guest-Enabled Interface (eth1)

For Your Reference

1. RADIUS Authentication requests sent to ise-psn1 @ 10.1.99.5.
2. RADIUS Authorization received from ise-psn1 @ 10.1.99.5 with URL Redirect to https://ise-psn1-guest:8443/...
3. DNS resolves alias FQDN ise-psn1-guest to 10.1.91.5 and sends web request to ise-psn1-guest @ 10.1.99.5.
4. No cert warning received since SAN contains interface alias FQDN.



Could also use wildcard SAN or UCC cert

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Load Balancing SAML SSO Logins to ISE Web Services

Load Balancing SAML Requests to ISE PSNs

For Your Reference

SAML SSO for ISE Web Portals

- Advantages:
  - Easy configuration at the Identity Provider side; Ideal for multi-node deployments
  - Only single ‘reply URL’ needed to be configured at the identity provider side

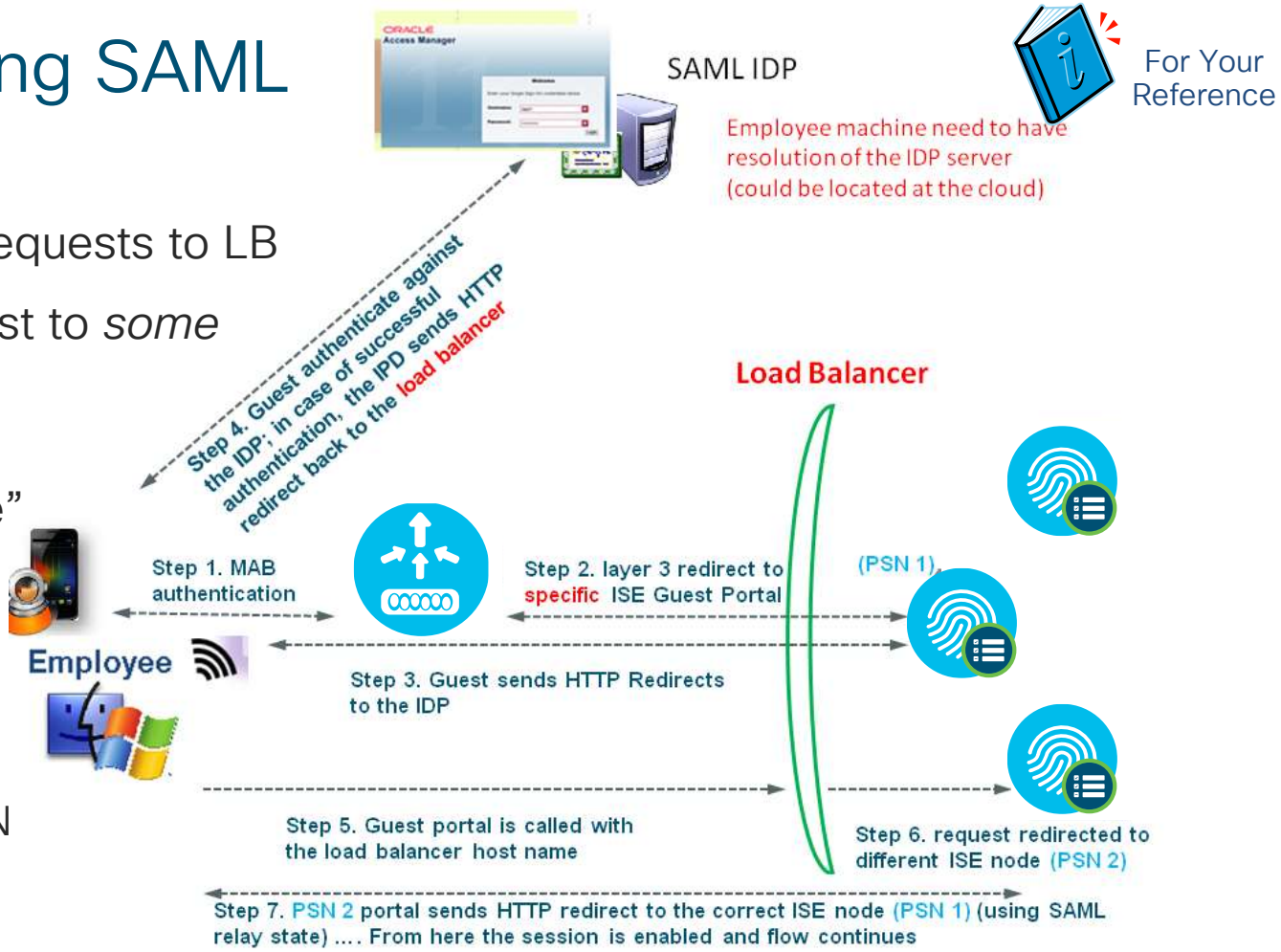
```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameID
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService Location="https://albarak-lnx:8443/mydevicesportal/SSOLoginResponse.action"
/md:SPSSODescriptor>
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

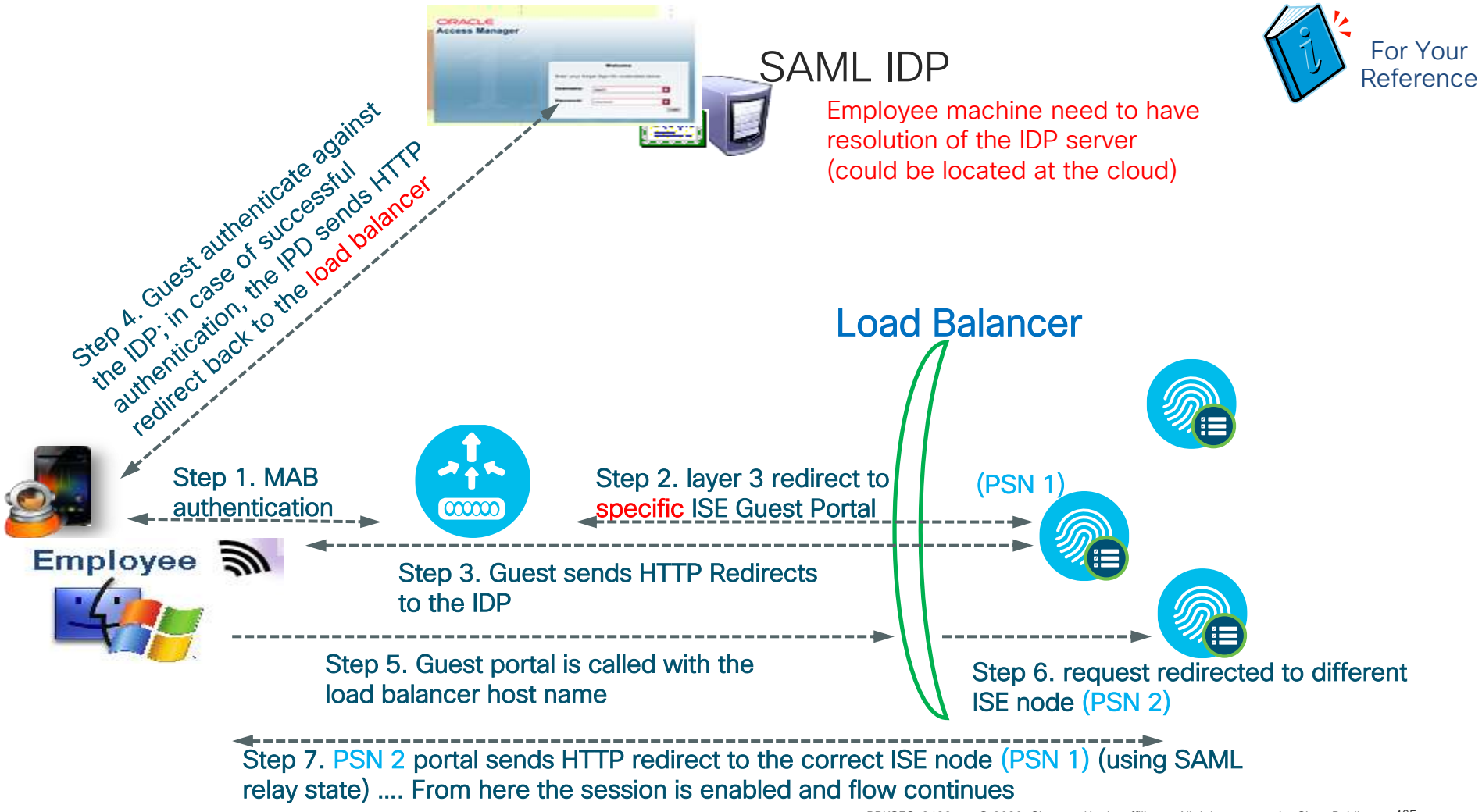
Load Balancing SAML

Flow

- SAML IDP sends requests to LB
- LB forwards request to *some* PSN in LB pool
- PSN reads "SAML Relay State"
  - If intended target, then process request
  - If NOT intended target, redirect user to correct PSN



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

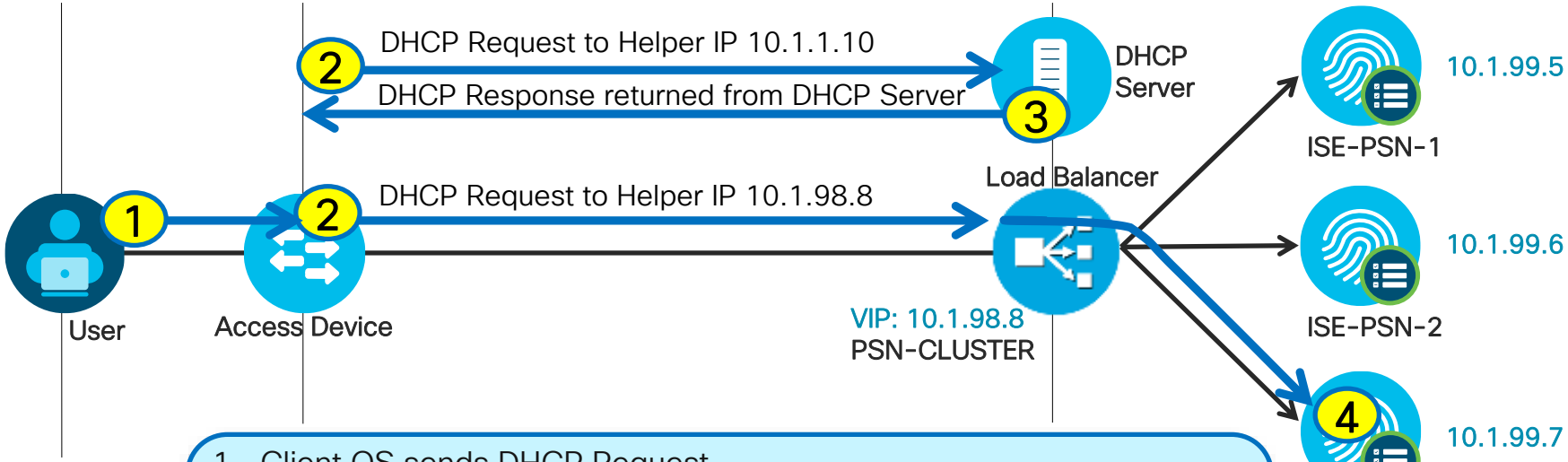


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing Simplifies Device Configurati

For Your Reference

Switch Example for SNMP Traps

- Before

```
!
snmp-server trap-source GigabitEthernet1/0/24
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host 10.1.99.5 version 2c public  mac-notification snmp
snmp-server host 10.1.99.6 version 2c public  mac-notification snmp
snmp-server host 10.1.99.7 version 2c public  mac-notification snmp
!
```

- After

```
!
snmp-server trap-source GigabitEthernet1/0/24
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host 10.1.98.8 version 2c public  mac-notification snmp
!
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling Services using Load Balancers

Which PSN Services Processes Profile Data?

For Your Reference

- **Profiling Probes**
  The following profile data can be load balanced to PSN VIP but may not be processed by same PSN that terminated RADIUS:
  - DHCP IP Helper to DHCP probe
  - NetFlow export to NetFlow Probe
  - SNMP Traps

  Option to leverage Anycast to reduce log targets and facilitate HA

- **SNMP Query Probe (triggered)**
  PSNs configured to send SNMP Queries will send query to NAD that sent RADIUS or SNMP Trap which triggered query. Therefore, SNMP Query data processed by same PSN that terminated RADIUS request for endpoint.

- **SNMP Query Probe (polled)**
  Not impacted by load balancing, although possible that PSN performing polled query is not same PSN that terminates RADIUS for newly discovered endpoints. PSN will sync new endpoint data with Admin. Since poll typically conducted at longer intervals, this should not impact more real-time profiling of endpoints.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Profiling Services using Load Balancers (Cont.)

For Your Reference

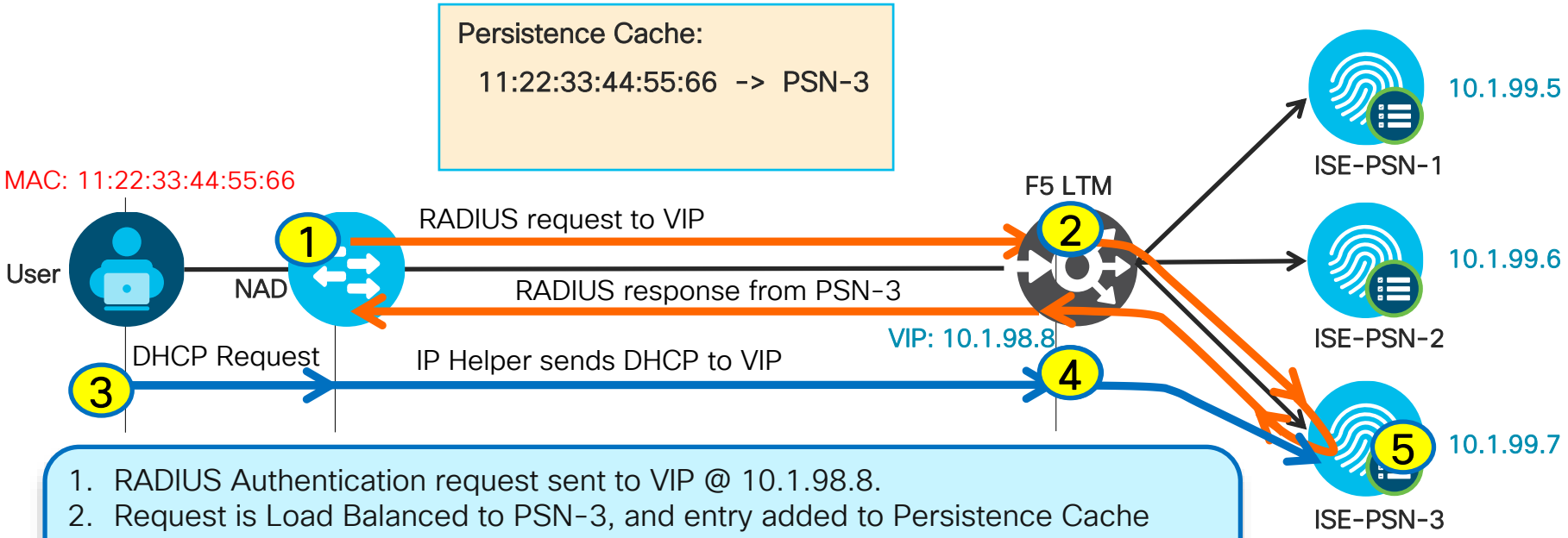
Which PSN Services Process Profile Data?

- **DNS Probe**
  Submitted by same PSN which obtains IP data for endpoint. Typically the same PSN that processes RADIUS, DHCP, or SNMP Query Probe data.
- **NMAP Probe**
  Submitted by same PSN which obtains data which matches profile rule condition.
- **HTTP (via URL redirect)**
  URL redirect will point to PSN that terminates RADIUS auth so HTTP data will be parsed by same PSN.
- **DHCP SPAN or HTTP SPAN**
  Since mirror port is associated to a specific interface on real PSN, cannot provide HA for SPAN data unless configure multiple SPAN destinations to separate PSNs. No guarantee that same PSN that collects SPAN data terminates RADIUS session.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing Sticky Guidelines

Ensure DHCP and RADIUS for a Given Endpoint Use Same PSN



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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Live Log Output for Load Balanced Sessions

Synthetic Transactions

- Batch of test authentications generated from Catalyst switch:

```
# test aaa group radius radtest cisco123 new-code count 100
```

All RADIUS sent to LB VIP @ 10.1.98.8

Requests evenly distributed across real servers:
- ise-psn-1
- ise-psn-2
- ise-psn-3

Time	Status	Details	Identity	Server	Network Device	Authorization Profiles
Oct 13,12 03:50:28.368 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.367 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.366 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.364 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.363 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.322 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.310 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.309 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.293 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.292 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes

Live Log Output for Load Balanced Sessions

For Your Reference

Real Transactions

- All RADIUS sent to LB VIP @ 10.1.98.10
- 1 All phone auth is load balanced from VIP to ise-psn-3 @ 10.1.99.7
- 2 All PC auth is load balanced to ise-psn-1 @ 10.1.99.5; URL Redirect traffic sent to same PSN.
- 3 CoA is sent from same PSN that is handling the auth session.
- 4 dACL downloads are sent from switch itself without a Calling-Station-Id or Framed-IP-Address. Request can be load balanced to any PSN. Not required to pull dACL from same PSN as auth.

Identity	Endpoint ID	IP Address	Server	Authorization Profiles	Identity Group	Posture Status	Event
CTS\employee1	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	Employee,SGT_Employee	Profiled:Workstation:Micr...	Compliant	Authentication succeeded
			ise-psn-1			Compliant	Dynamic Authorization su...
#ACSACL#-IP-POSTL			ise-psn-3				DACL Download Succeedec
CTS\employee1	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	Posture_Remediation	Profiled:Workstation:Micr...	Pending	Authentication succeeded
host/win7-pc.cts.loca	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	AD_Login	Profiled:Workstation:Micr...	NotApplicable	Authentication succeeded
#ACSACL#-IP-AD_LC			ise-psn-1				DACL Download Succeedec
host/win7-pc.cts.loca	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	AD_Login	Profiled:Workstation:Micr...	NotApplicable	Authentication succeeded
00:30:94:C4:52:8A	00:30:94:C4:52:8A	10.1.13.100	ise-psn-3	Cisco_IP_Phones	Profiled:Cisco-IP-Phone	NotApplicable	Authentication succeeded

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE and Load Balancers

For Your Reference

Failure Scenarios

- The VIP is the RADIUS Server, so if the entire VIP is down, then the NAD should fail over to the secondary Data Center VIP (listed as the secondary RADIUS server on the NAD).
- Probes on the load balancers should ensure that RADIUS is responding as well as HTTPS, at a minimum.
  - Validate that RADIUS responds, not just that UDP/1812 & UDP/1813 are open
  - Validate that HTTPS responds, not just that TCP/8443 is open
- Upon detection of failed node using probes (or node taken out of service), new requests will be serviced by remaining nodes→ Minimum N+1 redundancy recommended for node groups.
- Configure LB cluster as a node group.
  - If node group member fails, then another node-group member will issue CoA-reauth for Posture Pending sessions, forcing the sessions to begin again and not be hung.
  - Note: Node groups do not require load balancers

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE and Load Balancers

For Your Reference

General Guidelines

- Do not use Source NAT(SNAT) from access layer for RADIUS; SNAT Optional for HTTP/S:
  - ISE uses Layer 3 address to identify NAD, not NAS-IP-Address in RADIUS packet, so CoA fails.
  - Each PSN <u>must</u> be reachable by the PAN / MNT directly without NAT.
  - Each PSN <u>must</u> be reachable directly from client network for URL redirects (*Note sticky exception)
- Perform sticky (aka: persistence) based on Calling-Station-ID.
  - Some load balancers support RADIUS BRKSEC3432; Others may be limited to Source IP (NAD IP).
- Optional “sticky buddies” (secondary attributes that persist different traffic to same PSN)
  - *Framed-IP-Address if URL redirects must be sent through LB and not bypass LB.
  - DHCP Requested IP Address to ensure DHCP Profile data hits same PSN that terminated RADIUS.
- VIP for PSNs gets listed as the RADIUS server on each NAD for all RADIUS AAA.
- Each PSN gets listed individually in the NAD CoA list by real IP address (not VIP).
  - If source NAT PSN-initiated CoA traffic, then can list single VIP in NAD CoA list.
- Load Balancers get listed as NADs in ISE so their test authentications may be answered.

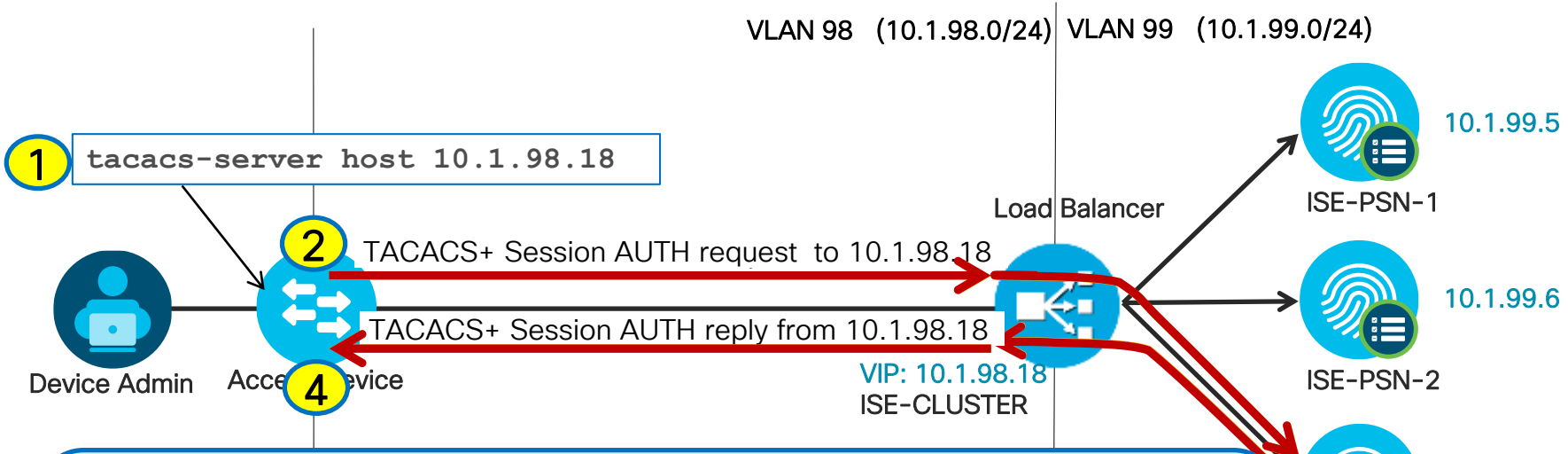
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing TACACS+

Load Balancing TACACS+

Session Authentication, Authorization, and Accounting

- Virtual IP = TACACS+ Server
- VIP listens on TCP/49
- Sticky based on source IP



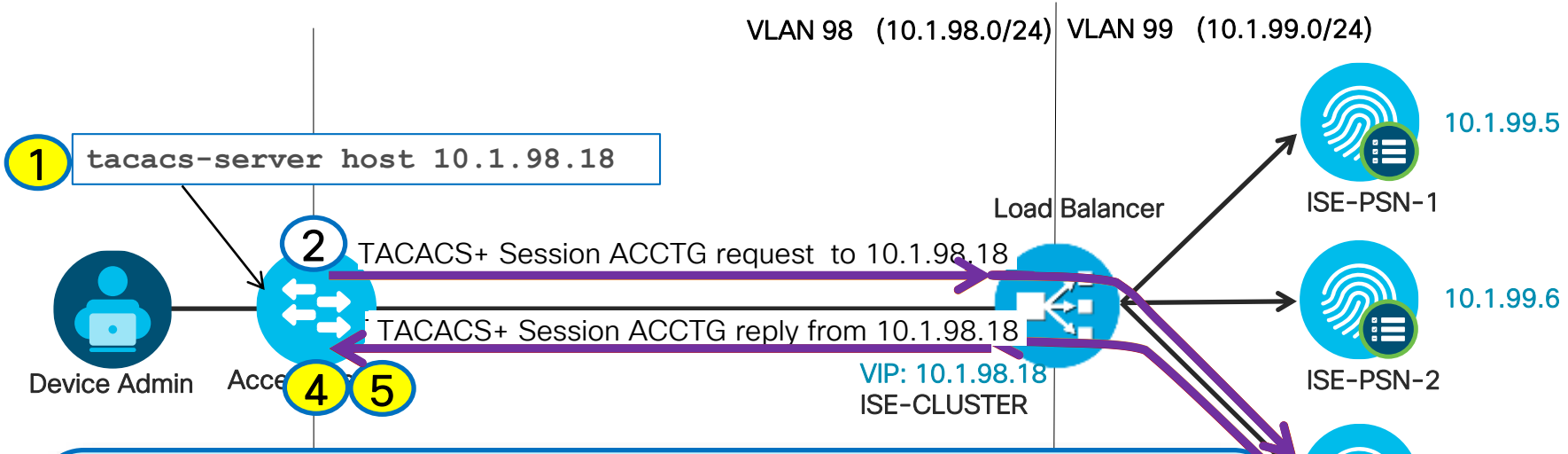
1. NAD has single TACACS+ Server defined (10.1.98.18)
2. TACACS+ Session Authentication requests sent to VIP @ 10.1.98.18
3. Requests from same Admin user load balanced to same PSN via sticky based on Source IP (NAD IP Address)
4. TACACS+ response received from VIP @ 10.1.98.18 (originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing TACACS+

Session Authentication, Authorization, and Accounting

- Virtual IP = TACACS+ Server
- VIP listens on TCP/49
- Sticky based on source IP



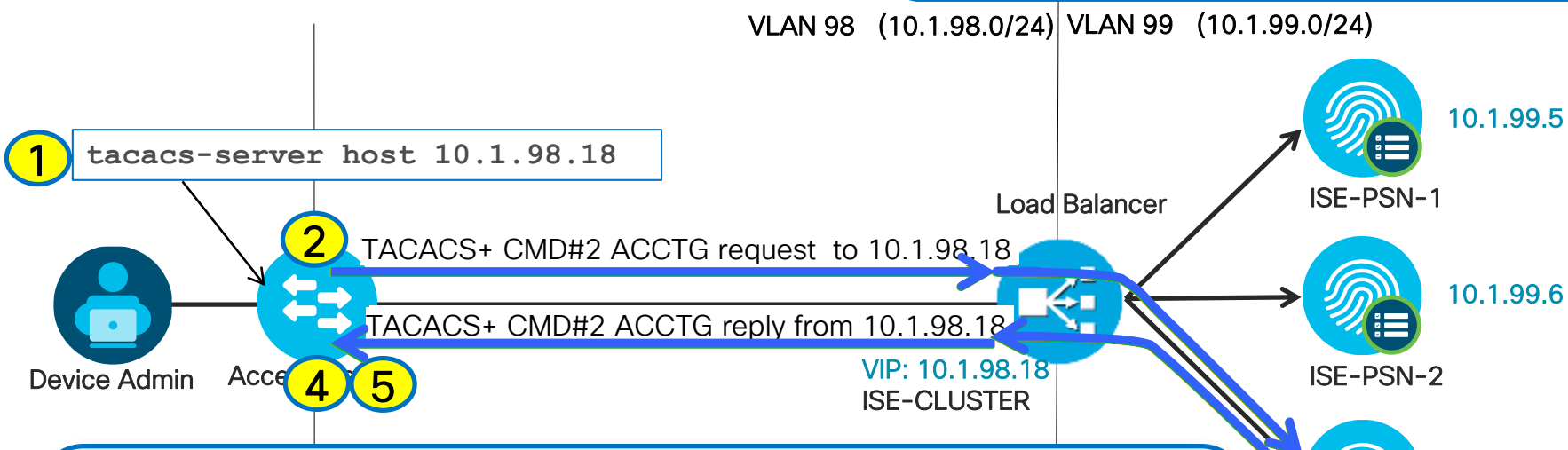
1. NAD has single TACACS+ Server defined (10.1.98.18)
2. TACACS+ Session Authentication requests sent to VIP @ 10.1.98.18
3. Requests from same Admin user load balanced to same PSN via sticky based on Source IP (NAD IP Address)
4. TACACS+ response received from VIP @ 10.1.98.18 (originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. TACACS+ Session Authorization & Accounting sent to/from same PSN per sticky

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing TACACS+

Command Authorization and Accounting

No session like RADIUS, so T+ requests can go to different PSNs, but recommend stick to same PSN for logging/trouble-shooting and for single connect mode.



1. Once **Session** Authenticated, **Command** Authorization/Accounting can begin.
2. TACACS+ Command Authorization request sent to VIP @ 10.1.98.18
3. Requests from same Admin user load balanced to same PSN via sticky based on Source IP (NAD IP Address)
4. TACACS+ response received from VIP @ 10.1.98.18 (originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. TACACS+ Command Accounting sent to/from same PSN per sticky

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing TACACS+

General Recommendations

- Load Balance based on TCP/49.
- Source NAT (SNAT) can be used – No CoA like RADIUS
  - Recommend LB inline with TACACS traffic, else need to address TCP asymmetry.
  - Without SNAT, make sure PSNs set default gateway to LB internal interface IP.
- Persistence – Recommend source IP address
  - Based on assumption that number of T+ clients high and requests per client is low.
- Health Monitoring options:
  - Simple response to TCP/49
  - 3-way handshake expected response
  - Scripts can be used to validate full auth flow.

Packet format: http://www.cisco.com/warp/public/459/tac-rfc.1.76.txt
Packet capture(encrypted):https://www.cloudshark.org/captures/1a9c284c49b0

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing TACACS+

For Your Reference

General Recommendations

1. Configure Virtual Server to LB on tcp/49.
2. SNAT should work as ISE servers do not need to initiate conversation to the TACACS+ clients like RADIUS CoA, but all requests will appear to emanate from LB rather than from the NAD clients. In either case, LB should be physically or logically inline with the TACACS traffic to ensure full processing of the flow and handling of the TCP session. Without SNAT, need to make sure LB internal interface IP is the default gateway for the ISE PSNs (TACACS+ servers).
3. Persistence can be based on simple source IP address based on assumption that the number of T+ clients is high and individual requests per client is relatively low. This should allow for sufficient distribution of requests across ISE PSNs and help ensure Authentication, Authorization, and Accounting requests do not get load balanced between ISE servers. More granular LB based on BRKSEC3432 (or even username) may be possible, but recommend keep it simple to ensure persistence locked to given device. (Initial TCP session establishment will not have TACACS payload. Standard T+ Packet header has Session_ID, but username would be in payload.)
4. Health monitoring can be based on response to tcp/49, or 3-way handshake based expected response, but some customers have used more advanced checks like perl script or scripted tcp to validate full auth process.

Packet format: http://www.cisco.com/warp/public/459/tac-rfc.1.76.txt
Packet capture(encrypted):https://www.cloudshark.org/captures/1a9c284c49b0

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TACACS+ Configuration

Catalyst Switch Example

For Your Reference

Example using **tacacs-server host**

```
tacacs-server host 10.1.98.18 timeout 4 key 0 cisco123 single-connection
tacacs-server host 10.2.98.18 timeout 4 key 0 cisco123 single-connection
tacacs-server retransmit tries
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
ip tacacs source-interface loopback0
```

- Define each PSN (or LB VIP) serving TACACS+
- Single connect reuses single TCP connection; default timeout is 5 seconds; default retransmit is 2 tries
- Enable TACACS+ session authentication
- Enable TACACS+ enable mode authentication
- Enable TACACS+ CLI session authorization
- Enable TACACS+ command authorization (priv 1)
- Enable TACACS+ command authorization (priv 15)
- Enable TACACS+ session accounting
- Enable TACACS+ command accounting (priv 1)
- Enable TACACS+ command accounting (priv 15)
- Configure source interface (IP addr) for TACACS+ Server requests (must match ISE NAD config)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

LDAP Server Load Balancing and Redundancy

Per-PSN LDAP Servers

Added in ISE 2.2!

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

LDAP Identity Sources List > **LDAP1**

LDAP Identity Source

General | Connection | Directory Organization | Groups | Attributes | Advanced Settings

Primary Server

Hostname/IP: ad.cts.local

Port: 389

Secondary Server

☑ Enable Secondary Server

Hostname/IP: ad2.cts.local

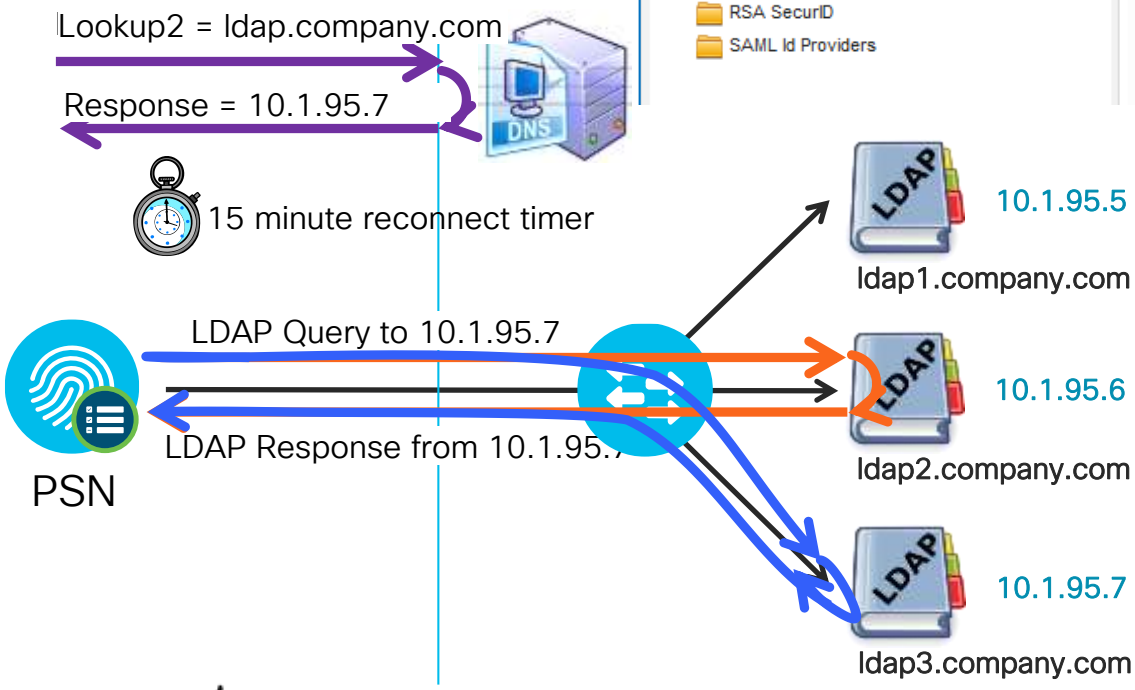
Port: 389

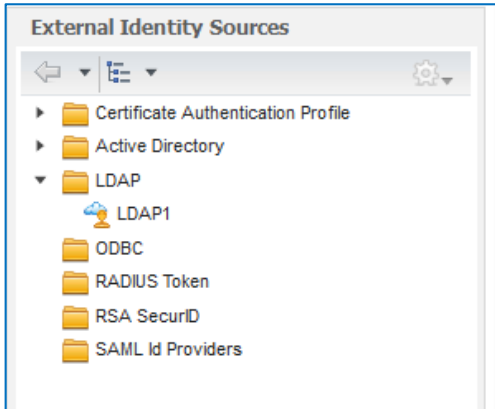
☑ Specify server for each ISE node

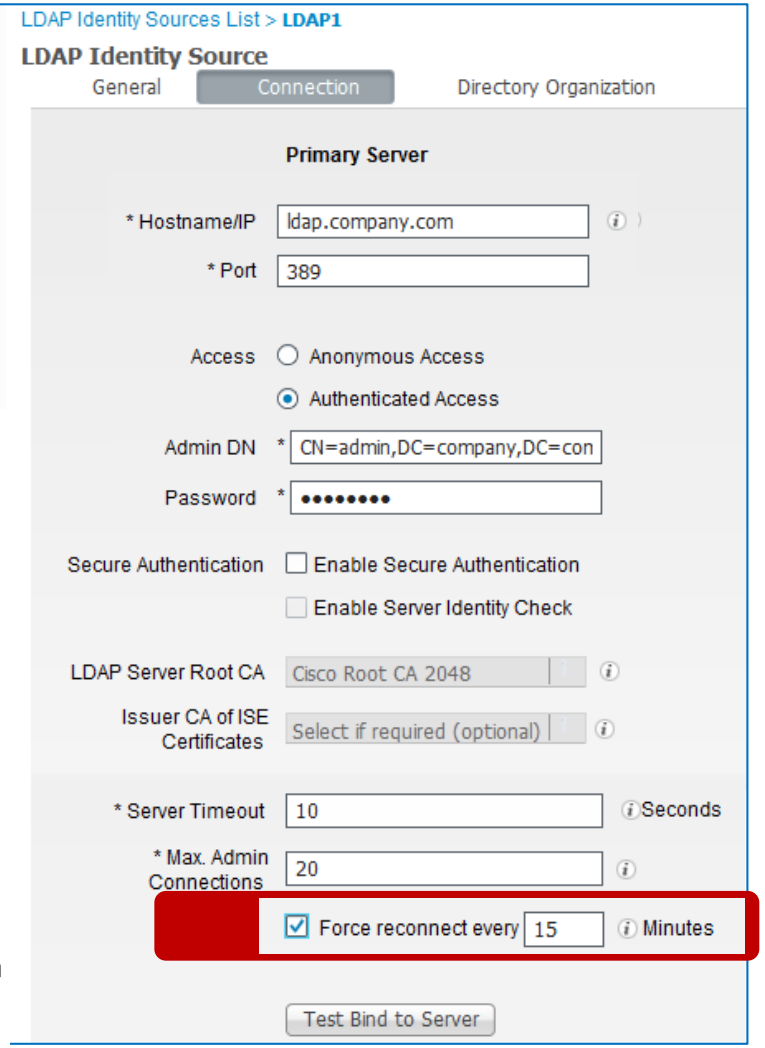
Name	Primary Hostname/IP	Port	Secondary Hostname/IP	Port
ise22-psn1.company.com	ldap1-us-west.company.com	389	ldap2-us-west.company.com	389
ise22-psn2.company.com	ldap1-us-east.company.com	389	ldap2-us-east.company.com	389
ise22-psn3.company.com	ldap1-europe.company.com	389	ldap2-europe.company.com	389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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancing LDAP Servers







Sample Vendor Load Balancer Configurations for Cisco ISE

Vendor-Specific LB Configurations

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

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

F5 LTM

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

For Your Reference

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

Secure Access How -To Guides Series

Author: Craig Hyps, Cisco Systems
Date: December 2014

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Citrix NetScaler

- Cisco Communities > ISE Load Balancing
  - https://community.cisco.com/t5/security-documents/ise-load-balancing/ta-p/3648759
- Citrix NetScaler 1000V Load Balancing Config for ISE
  - https://ciscomarketing.jiveon.com/docs/DOC-64441

- ISE and Citrix NetScaler for LB
  - Detailed discussion on NetScaler Persistence, CoA NAT, etc:
  - https://supportforums.cisco.com/discussion/11949336/ise-and-citrix-netscaler-lb

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

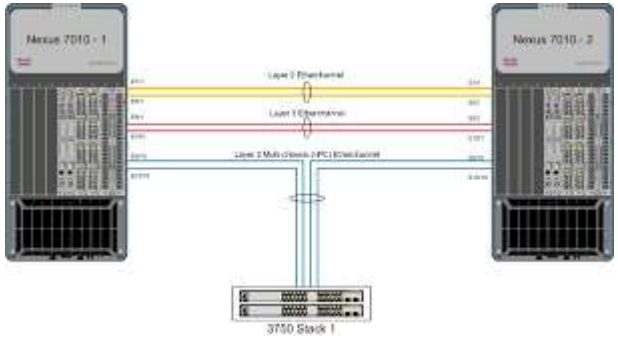
Cisco ACE Load Balancer

- Cisco Communities > ISE Load Balancing
  - https://community.cisco.com/t5/security-documents/ise-load-balancing/ta-p/3648759
- Configuring ACE for Cisco ISE Load Balancing
  - Complete working configuration
  - https://community.cisco.com/t5/security-documents/configuring-ace-for-cisco-ise-load-balancing/ta-p/3642008

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Intelligent Traffic Director (ITD)

Can I Use Cisco ITD to Load Balance ISE Traffic?



- As of June 2020, these are the key considerations and limitations for deploying ISE with ITD for RADIUS LB:
  - Prior to NX-OS 7.2(1), ITD assumes support for Direct Server Return (DSR). ISE does not support this option.
  - ITD added support for non-DSR (destination NAT) in NX-OS Software 7.2(1)D1(1) (also known as Gibraltar MR) on Nexus 7k series of switches only. Destination NAT is necessary to have packets properly forwarded to/from PSNs through ITD.
  - Currently no support for persistence based on Calling-Station-ID, BRKSEC3432, or other RADIUS attributes. Stickiness would need to rely on source IP (NAD IP address) —only feasible if have good distribution of endpoints across NADs of equal capacity.
  - Currently no support for RADIUS health probes; must rely on simple ping/port checks.
  - Currently no support source NAT, so would need extra configuration for CoA to work.

For Your Reference

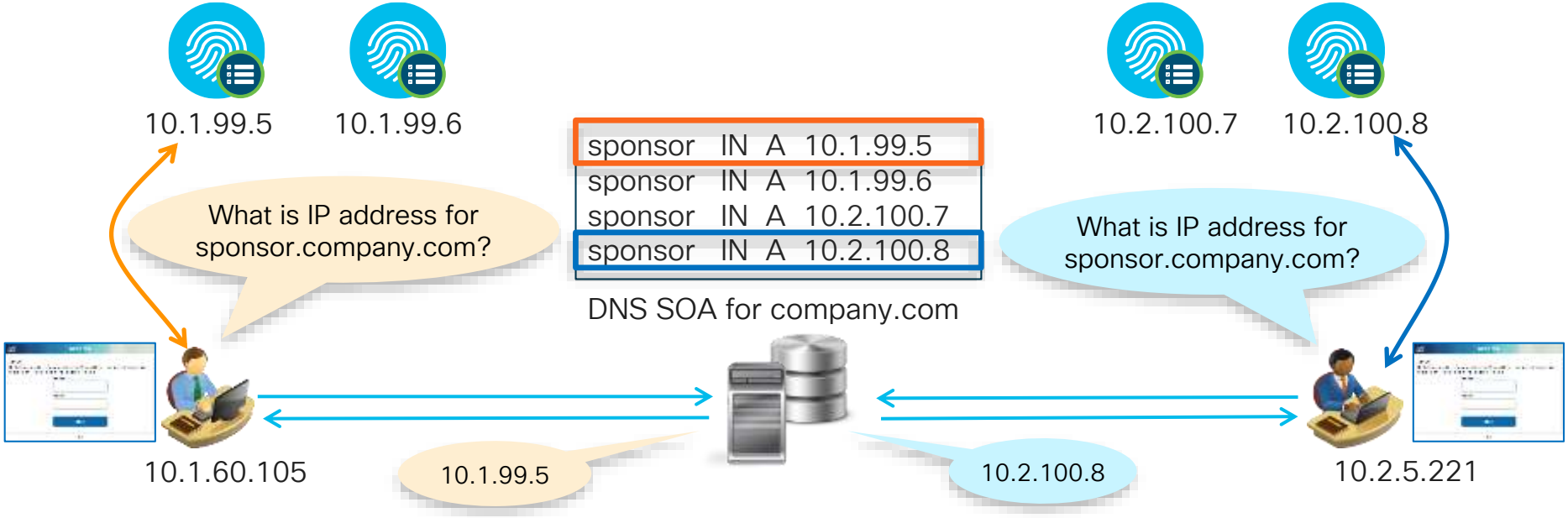
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN HA Without Load Balancers

Load Balancing Web Requests Using DNS

Client-Based Load Balancing/Distribution Based on DNS Response

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

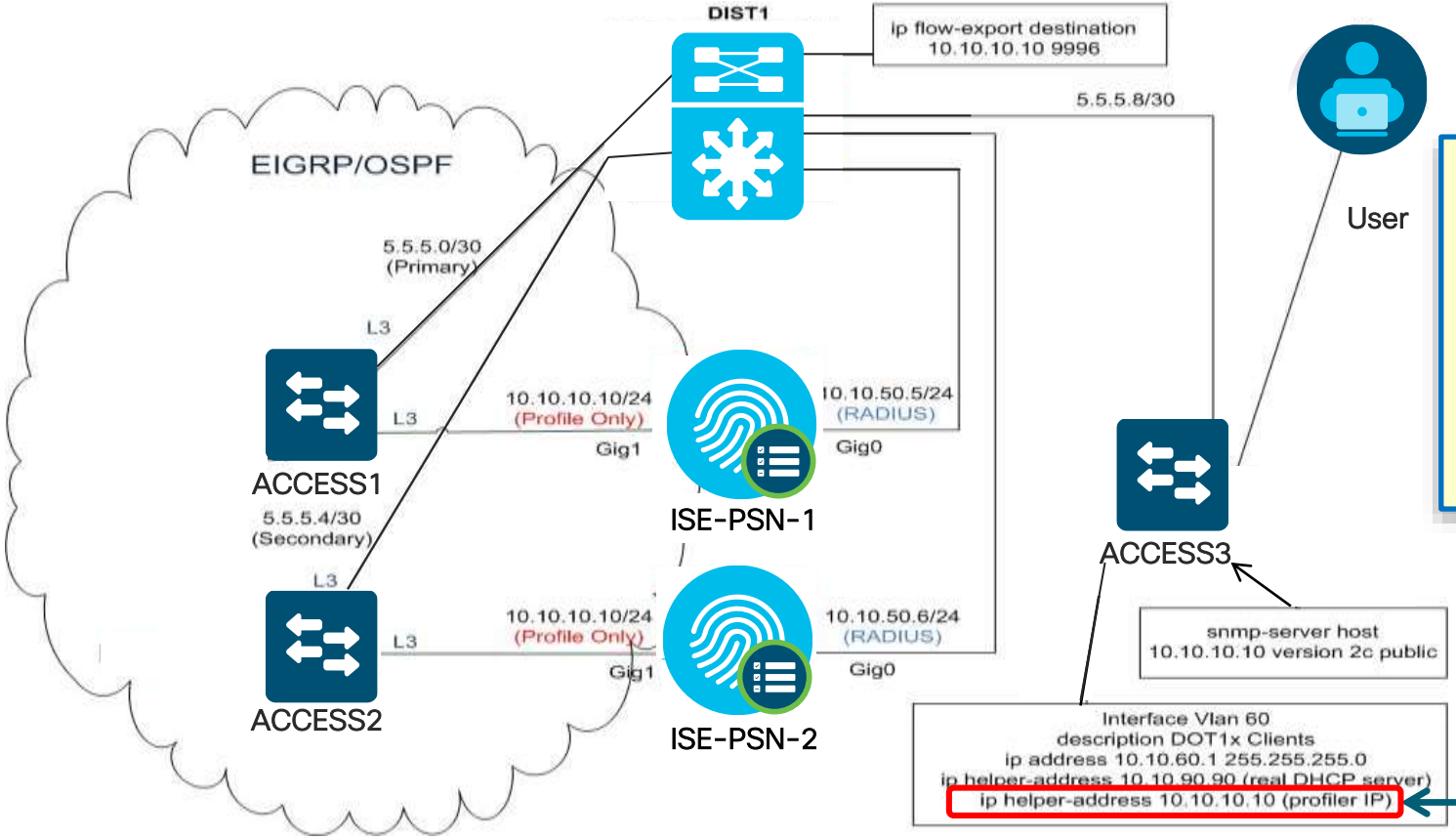


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Anycast for ISE Redundancy

Profiling Example

For Your Reference



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.

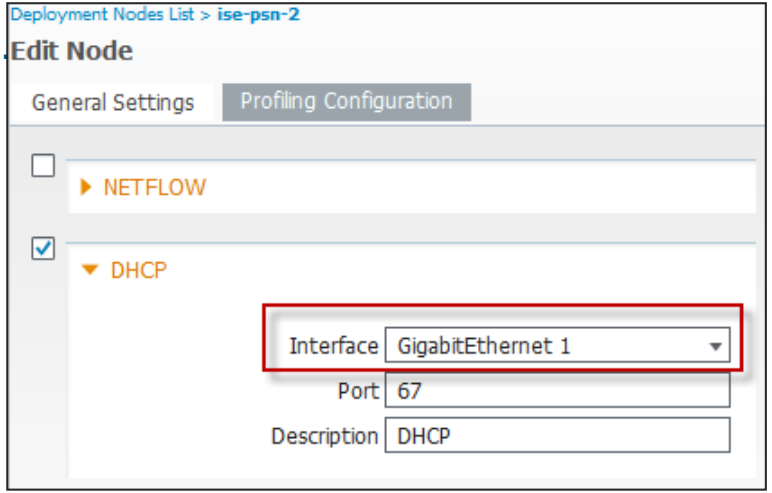
Ex: 10.10.10.10

ISE Configuration for Anycast

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

On each PSN that will participate in Anycast...

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



ISE-PSN-1 Example:

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

ISE-PSN-2 Example:

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


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Routing Configuration for Anycast

Sample Configuration

- Access Switch 1

```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.50 255.255.255
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-
2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 1000 100 255 1 1500
set metric-type internal
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

Both switches advertise same network used for profiling but different metrics

- Access Switch 2

```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.51 255.255.255.0
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-
2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 500 50 255 1 1500
set metric-type external
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

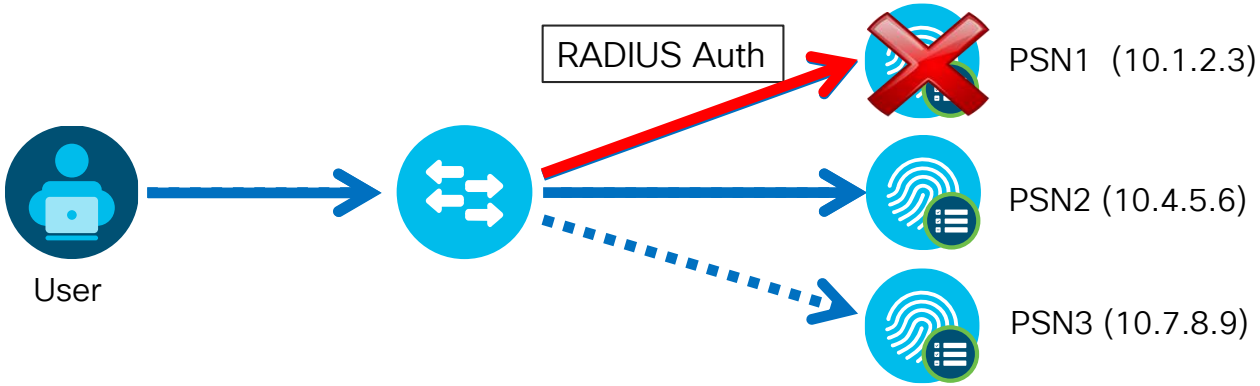
less preferred

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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
```

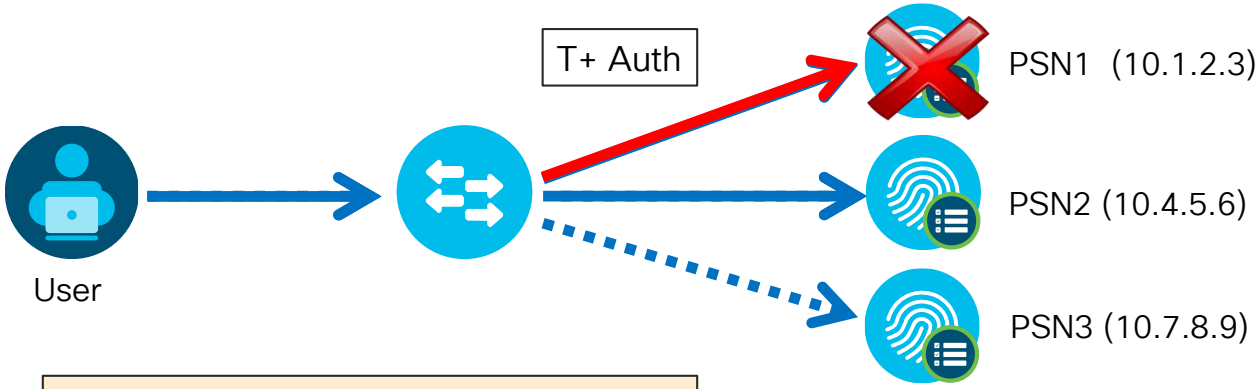

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD-Based TACACS+ Server Redundancy (IOS)

Multiple TACACS+ Servers Defined in Access Device

For Your Reference

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




```
tacacs-server host 10.1.2.3
tacacs-server host 10.4.5.6
tacacs-server host 10.7.8.9
```

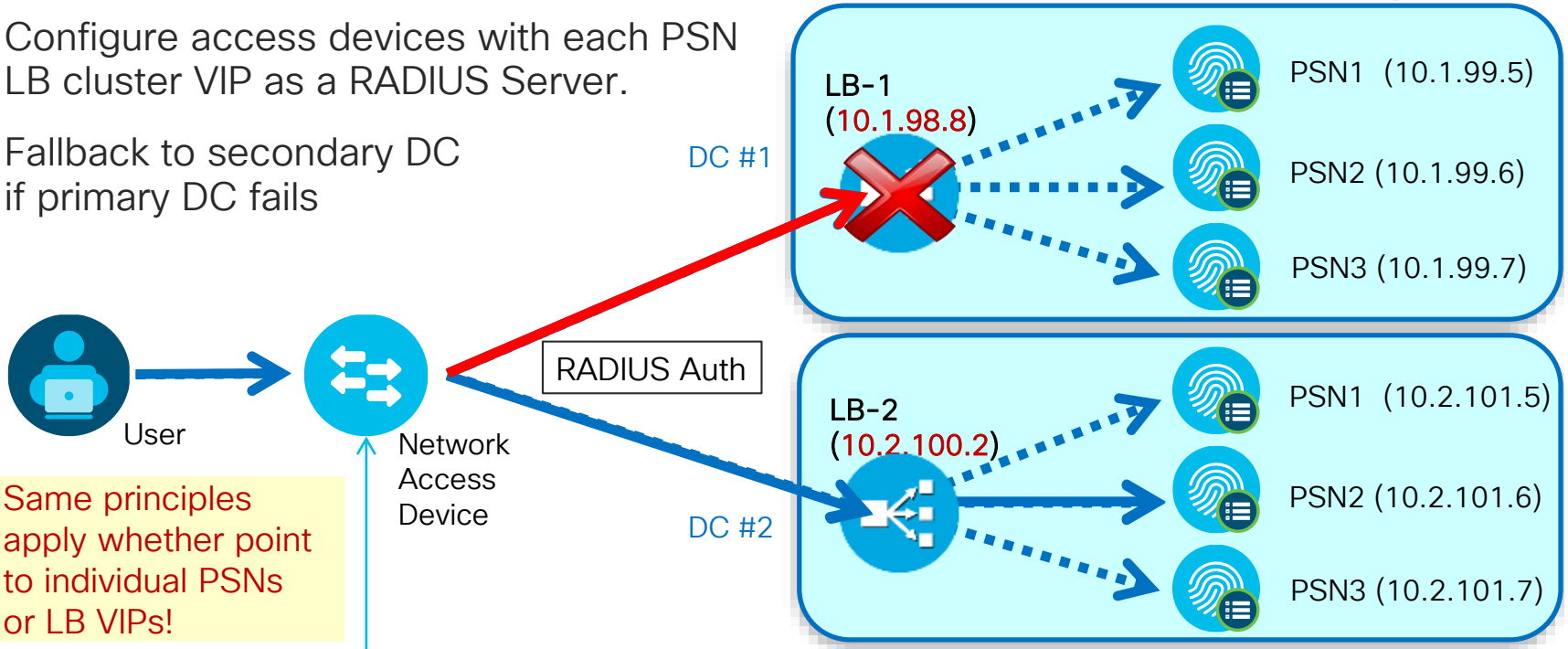

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD-Based Redundancy to Different Data Centers

RADIUS Example – Different RADIUS VIP Addresses

For Your Reference

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



Same principles apply whether point to individual PSNs or LB VIPs!

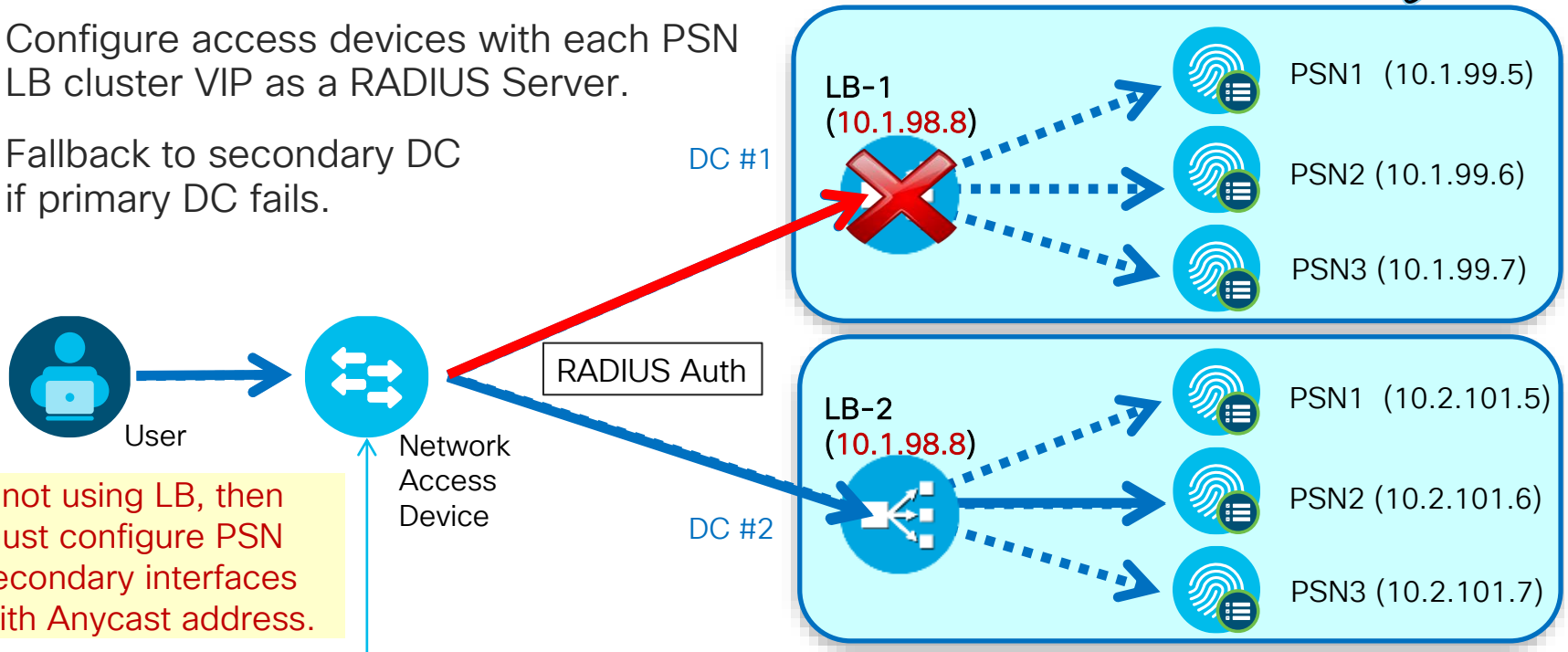
```
radius-server host 10.1.98.8 auth-port 1812 acct-port 1813
radius-server host 10.2.100.2 auth-port 1812 acct-port 1813
```

NAD-Based Redundancy to Different Data Centers

RADIUS Example – Single RADIUS VIP Address using Anycast

For Your Reference

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



If not using LB, then must configure PSN secondary interfaces with Anycast address.

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

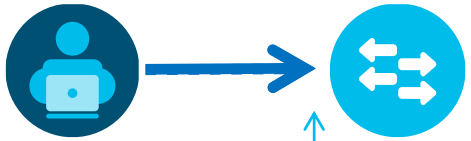
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD-Based Redundancy to Different Data Centers

Profiling Example – Different DHCP VIP Addresses

For Your Reference

- Configure access devices with PSN cluster VIP as an IP Helper.
- Both Data Centers receive copy of DHCP Profiling data
- Same principles apply without LB.



DHCP Relay

DC #1

LB1 (10.1.98.11)

PSN1 (10.1.99.5)

PSN2 (10.1.99.6)

PSN3 (10.1.99.7)

DC #2

LB2 (10.2.100.3)

PSN1 (10.2.101.5)

PSN2 (10.2.101.6)

PSN3 (10.2.101.7)

```
interface VLAN 10
  ip address A.B.C.D 255.255.255.0
  ip helper-address X.X.X.X      # Real
  ip helper-address 10.1.98.11   # LB1
  ip helper-address 10.2.100.3   # LB2
```

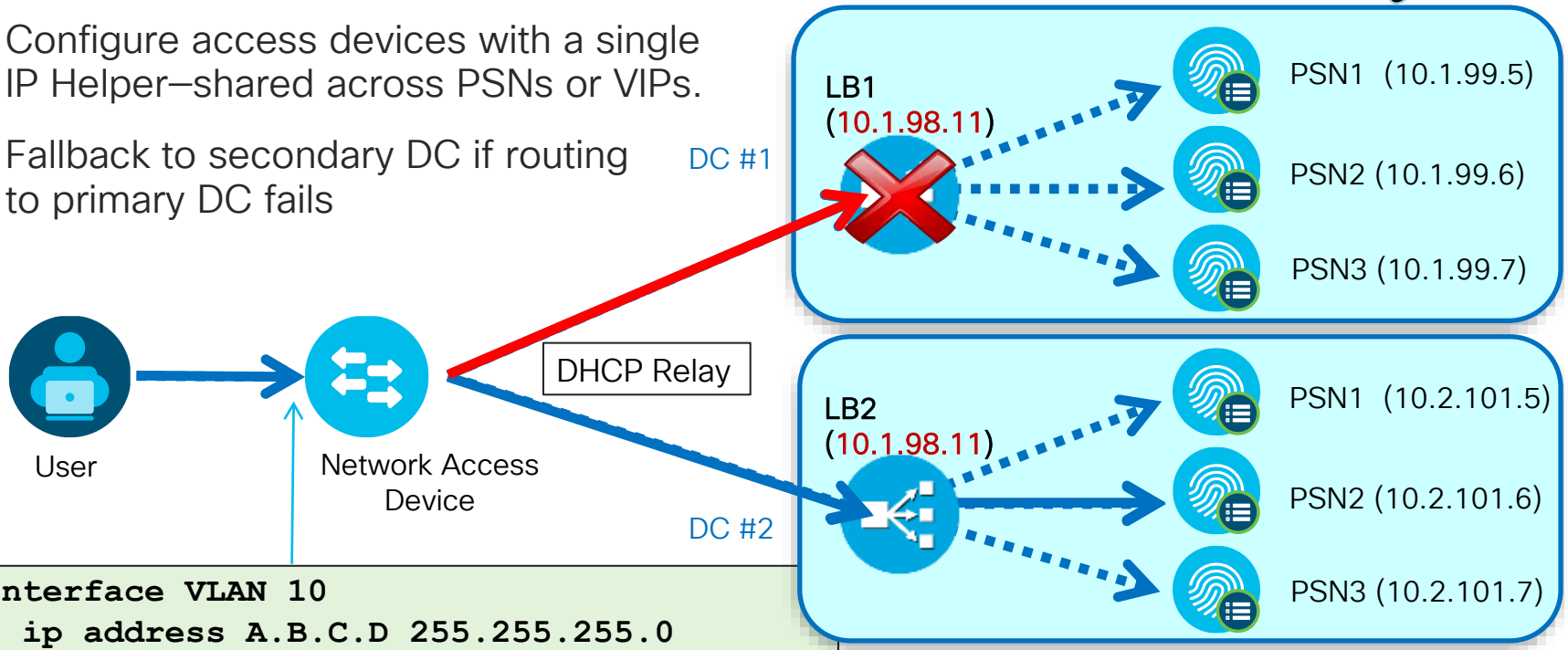
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD-Based Redundancy to Different Data Centers

Profiling Example – Single DHCP VIP Address using Anycast

For Your Reference

- Configure access devices with a single IP Helper–shared across PSNs or VIPs.
- Fallback to secondary DC if routing to primary DC fails




```
interface VLAN 10
  ip address A.B.C.D 255.255.255.0
  ip helper-address X.X.X.X      # Real
  ip helper-address 10.1.98.11   # Anycast
```

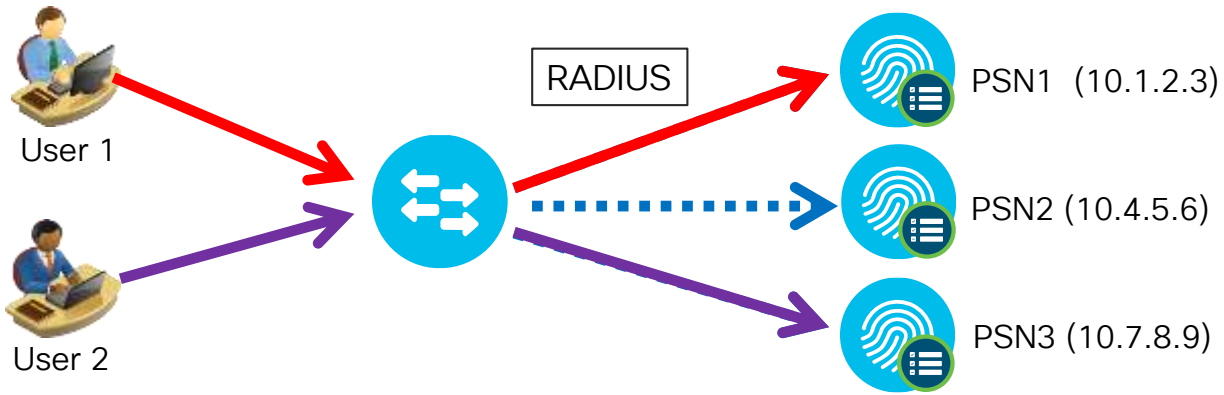
If not using LB, then must configure PSN secondary interfaces with Anycast address.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IOS-Based RADIUS Server Load Balancing

Switch Dynamically Distributes Requests to Multiple RADIUS Servers

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



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

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

IOS-Based RADIUS Server Load Balancing

Sample Live Log

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

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

Reasonable load distribution across all PSNs

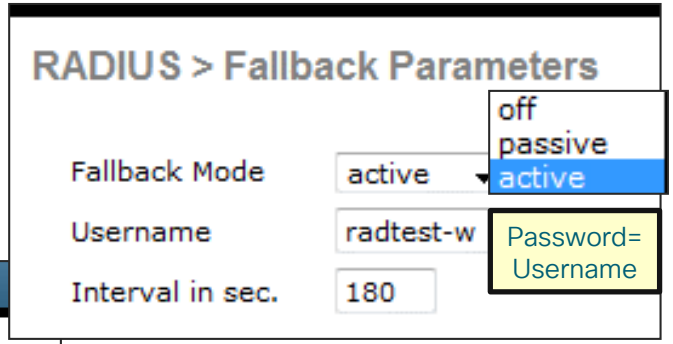
Example shows 3 PSNs in RADIUS group

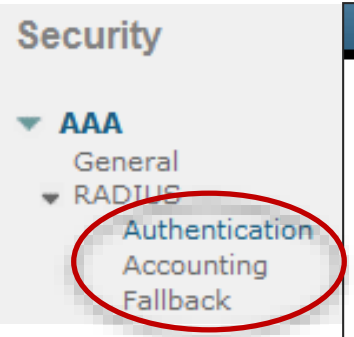
```
cat3750x# test aaa group radius radtest cisco123 new users 4 count 50
AAA/SG/TEST: Sending 50 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
```

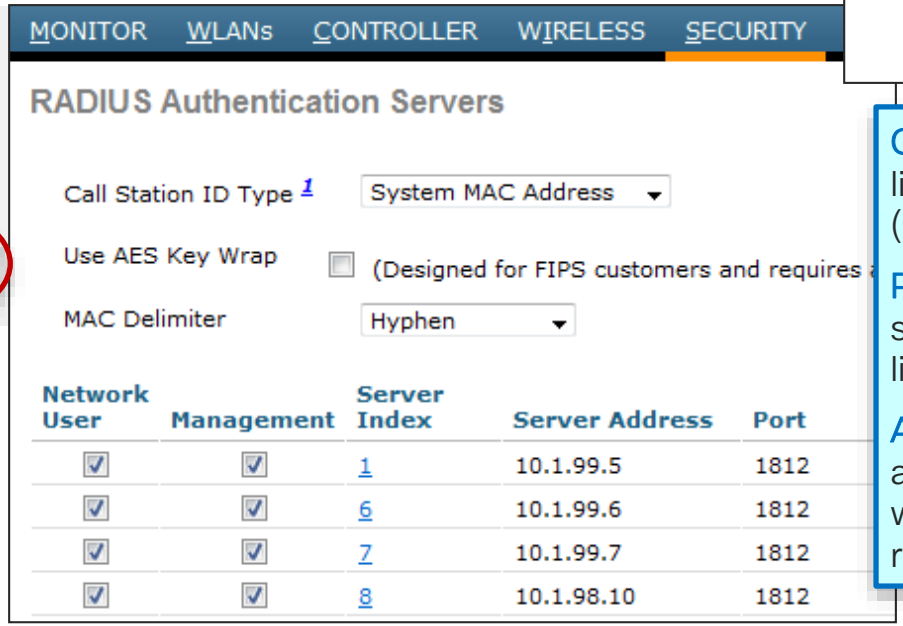
NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

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







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

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

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

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

HA/LB Summary Table

Comparison of Various HA/LB Methods

For Your Reference

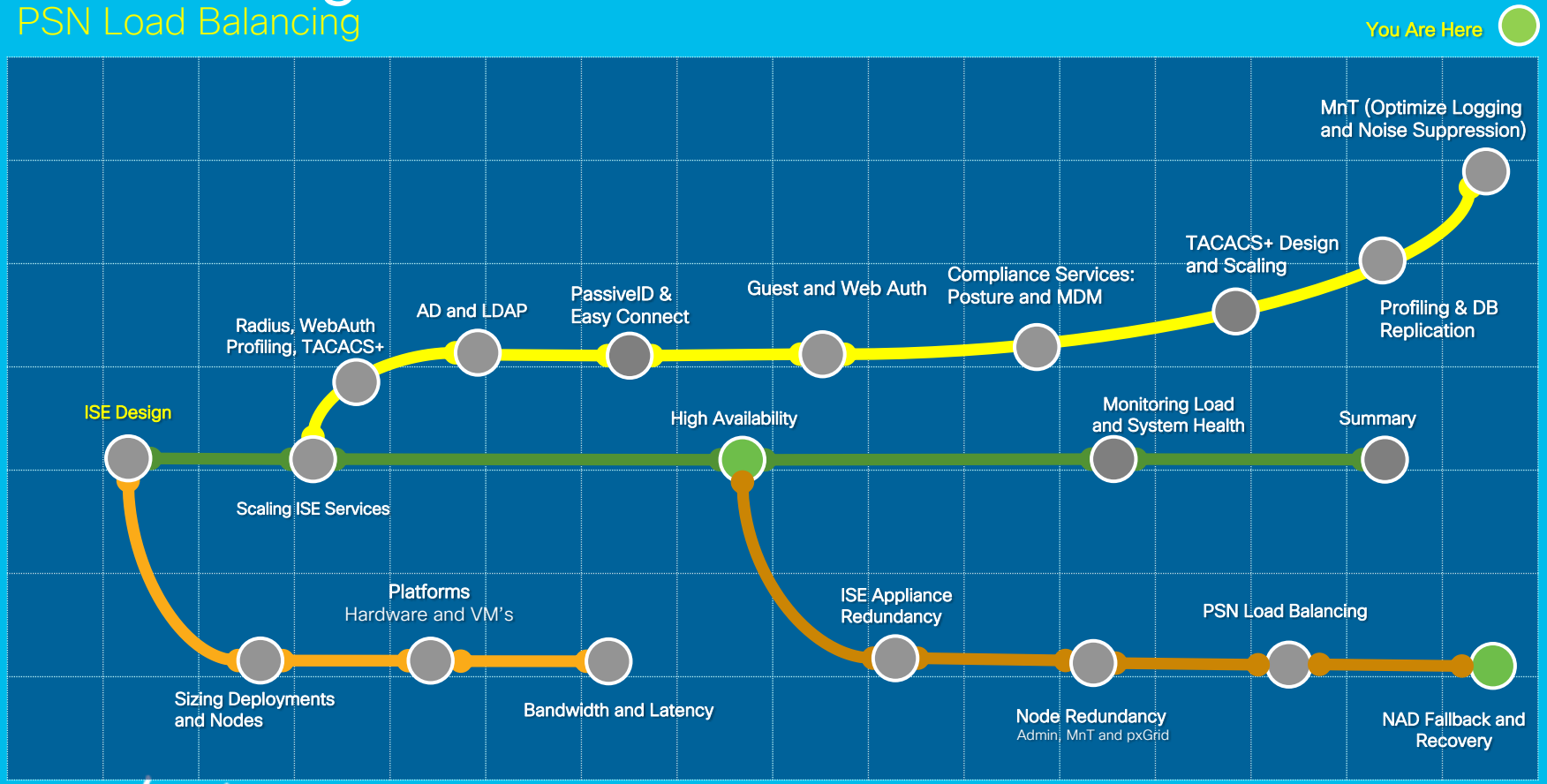
HA/LB Method	Where Configured?	Primary USE Cases	Pros	Cons
Local Load Balancers	Centrally using LB near PSN cluster	RADIUS HTTP/S Profiling	Large scaling, Fast failover, better load distribution, in/out servicing, single IP, adds flexibility, lowers TCO	Higher up-front cost and complexity
DNS/Global LB	Centrally using DNS	LWA / Sponsor / MDP Portals	Large scaling, better load distribution, in/out servicing, single URL	Somewhat higher cost and complexity
Anycast	Centrally using routing	Web Portals, Profiling, RADIUS	Lower cost, supports simple route-based distribution, in/out service, single IP	Higher complexity
NAD RADIUS Server List	Distributed in local NAD config	RADIUS, Profiling (Sensor)	Low cost and complexity, deterministic distribution	Management of distributed lists, poor load distribution
IOS RADIUS LB	Distributed in local NAD config	RADIUS	Low cost and complexity, better per-NAD load distribution	Management of distributed lists

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD Fallback and Recovery

Session Agenda

PSN Load Balancing



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD Fallback and Recovery

Common Questions

Q: How does NAD detect failed RADIUS servers?

A: Test Probes and Test User accounts

Q: What is the default behavior when ALL RADIUS servers down?

A: Unless using ‘authentication open’ no access is granted for unauthorized ports.

Q: Which fallback methods are available?

A: Critical Authentication VLAN for Data and Voice; Critical ACLs; EEM controls

Q: What is the impact of using VLAN-based fallback methods?

A: Users may still be blocked by port ACLs or may not get IP if VLAN changes

Q: Which recovery methods are available?

A: Reinitialize ports when RADIUS server available

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD Fallback and Recovery

Dead RADIUS Server Detection & Recovery

Example using **radius-server host**

For Your Reference

In example, servers are marked “dead” if no response in 60 seconds (1 transmit + 3 retransmits w/15 second timeout).

After 2 minutes, RADIUS test probe will retry server and mark “alive” if response; otherwise recheck every 2 minutes(deadtime).

Some releases may require idle-time to be set lower than dead-time. (CSCtr61120)

```
interface X
  authentication event fail action next-method
  authentication event server dead action reinitialize vlan 11
  authentication event server dead action authorize voice
  authentication event server alive action reinitialize
  authentication violation restrict

radius-server dead-criteria time 30 tries 3
radius-server deadtime 2

authentication critical recovery delay 1000
dot1x critical eapol

epm access-control open

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

radius-server host 10.2.101.3 auth-port 1812 acct-port 1813 test
username radtest ignore-acct-port key cisco123
```

- Move new hosts to specified critical data VLAN
- Authorize new phones to voice VLAN
- Reauthenticate endpoints on port once server “alive”
- Deny access to violating host but do not disable port
- Conditions to mark server as “dead” (Ex: 60 sec.)
- Minutes before retrying server marked as “dead”
- Throttle requests for critical ports once server “alive”
- Send EAPOL-Success when auth critical port
- Permit access if no dACL returned with successful auth
- RADIUS server definition including periodic test to detect server dead/alive:
  - username ‘radtest’: Locally defined test user to auth
  - idle-time: default = 60 = “Send test probe 1 per hour”
  - ignore-acct-port : Test auth-port on
- Fallback RADIUS server if primary server fails

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAD Fallback and Recovery

‘aaa radius group’ Example

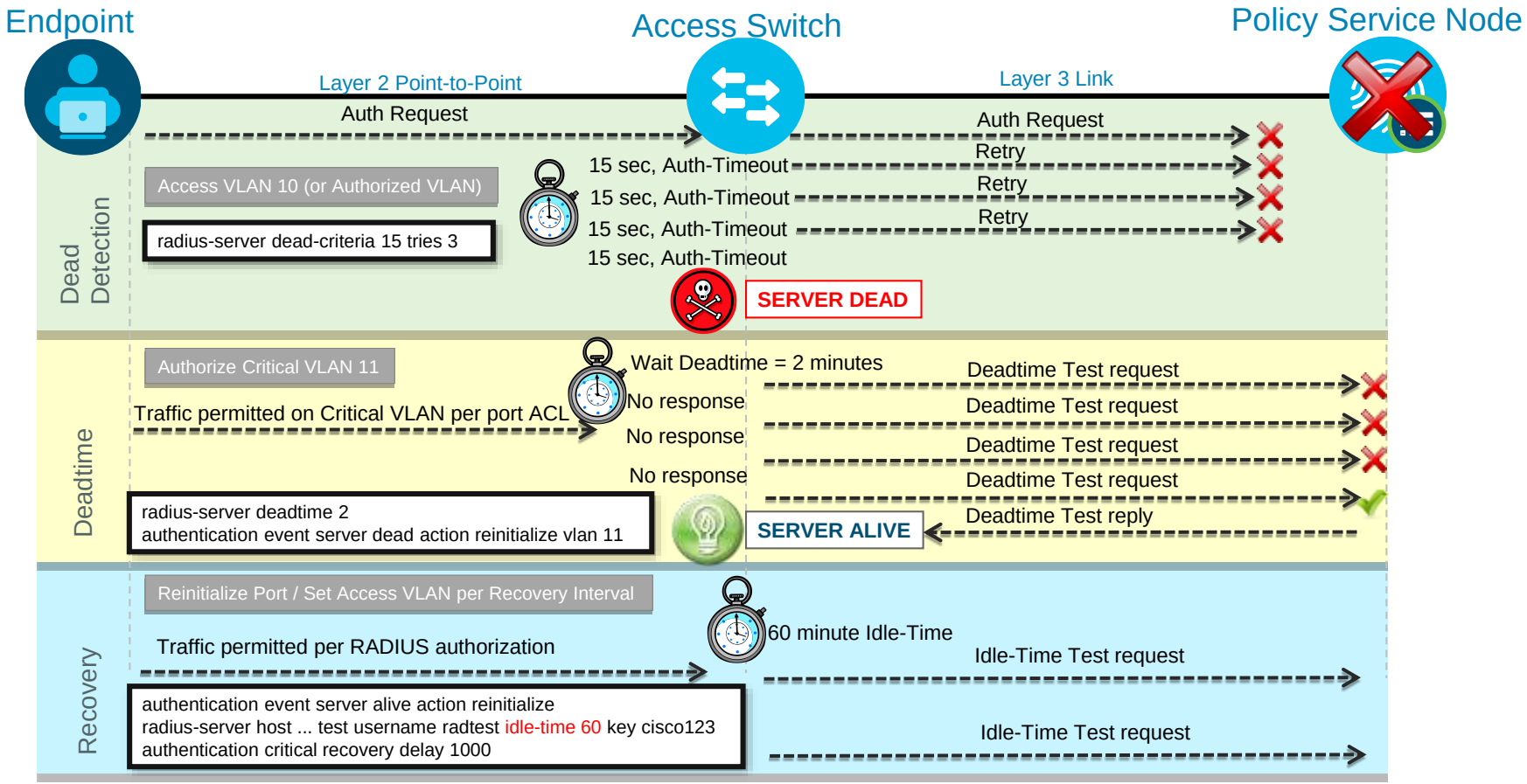
For Your Reference

- Similar configuration as previous example but using **aaa radius group** and **radius server *host*** commands
- **radius server host** defines individual RADIUS servers with separate lines for config parameters
- **aaa radius group** defines RADIUS group with individual server entries listed

```
interface X
  authentication event fail action next-method
  authentication event server dead action reinitialize vlan 11
  authentication event server dead action authorize voice
  authentication event server alive action reinitialize
  authentication violation restrict

authentication critical recovery delay 1000
dot1x critical eapol
epm access-control open
radius-server dead-criteria time 30 tries 3
radius-server deadtime  2

aaa group server radius psn-clusters
  server name psn-cluster1
  server name psn-cluster2

radius server psn-cluster1
  address ipv4 10.1.98.8 auth-port 1812 acct-port 1813
  automate-tester username radtest ignore-acct-port key cisco123

radius server psn-cluster2
  address ipv4 10.2.101.3 auth-port 1812 acct-port 1813
  automate-tester username radtest ignore-acct-port key cisco123
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

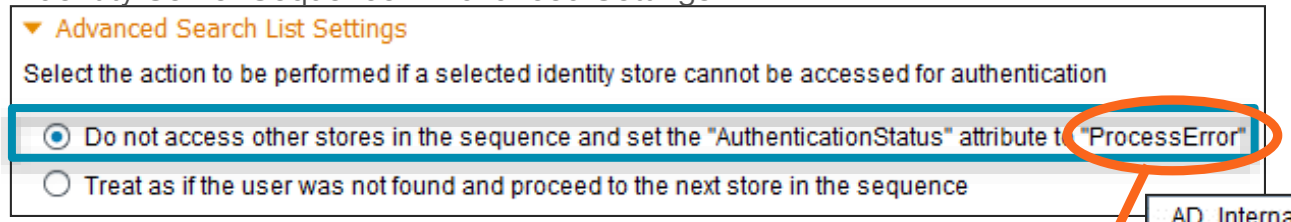
NAD Fallback and Recovery Sequence



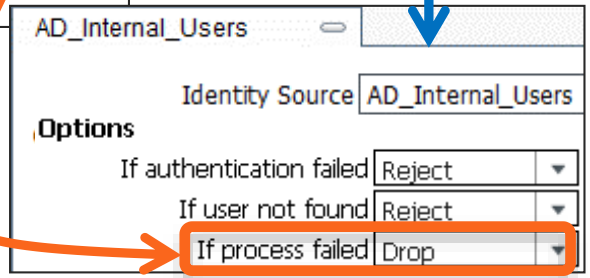
RADIUS Test User Account

Which User Account Should Be Used?

- Does NAD uniformly treat Auth Fail and Success the same for detecting server health?
  IOS treats them the same; ACE RADIUS probe treats Auth Fail= “server down”. Check your LB behavior.
- Do I use an Internal or External ID store account?
  If goal is to validate backend ID store, then Auth Fail may not detect external ID store failure.
- **IOS Example:** Failover on AD failure. **Solution:** Drop auth requests when external ID store is down.
  - Identity Server Sequence > Advanced Settings:



Authentication Policy > ID Source custom processing based on authentication results



- **ACE Example:** If auth fails, then PSN declared down.
  Solution: Create valid user account so ACE test probes return Access-Accept.
  - Could this present a potential security risk?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

RADIUS Test User Account

Access-Accept or Access-Reject?

- If valid user account used, how prevent unauthorized access using probe account?
  If Auth Fail treated as probe failure, then need valid account in ISE db or external store.
  - Match auth from probes to specific source/NDG, Service Type, or User Name.
    Allow AuthN to succeed, but return AuthZ that denies access.

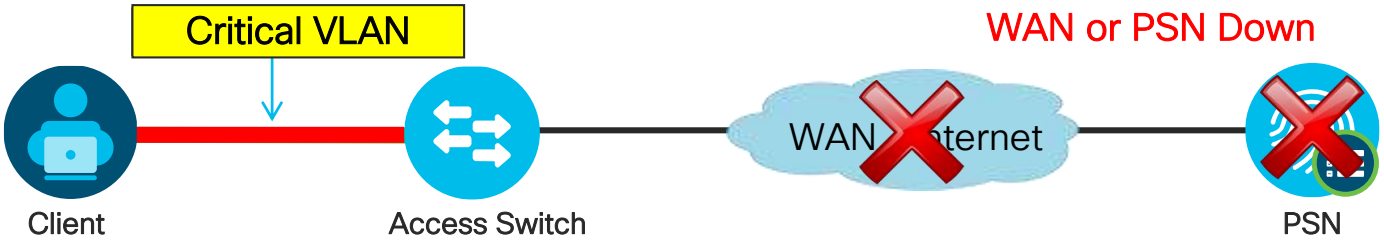
Rule Name		Conditions (identity groups and other conditions)		Permissions
RADIUS Probe	if	(Network Access:NetworkDeviceName EQUALS ace4710 OR Radius:User-Name EQUALS radtest)	then	RADIUS_Probes

Time	Status	Details	Identity	Network Device	Authorization Profiles	Posture Status	Event	Server
Oct 08,12 07:54:25.958 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-3
Oct 08,12 07:54:18.957 PM	✓		radprobe	ace4710	RADIUS_Probes	N		ise-psn-2
Oct 08,12 07:53:43.628 PM	✓		radtest	cat3750x	RADIUS_Probes	N		ise-psn-2
Oct 08,12 07:53:27.044 PM	✓		radtest	cat3750x	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-1
Oct 08,12 07:53:26.960 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-1
Oct 08,12 07:53:25.966 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-3
Oct 08,12 07:53:18.964 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-2

Access-Accept
dACL = deny ip any any

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 authorization status
- Recovery action can re-initialize port when AAA returns

Critical Data 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
authentication event server dead action authorize voice
```

Critical Voice VLAN

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

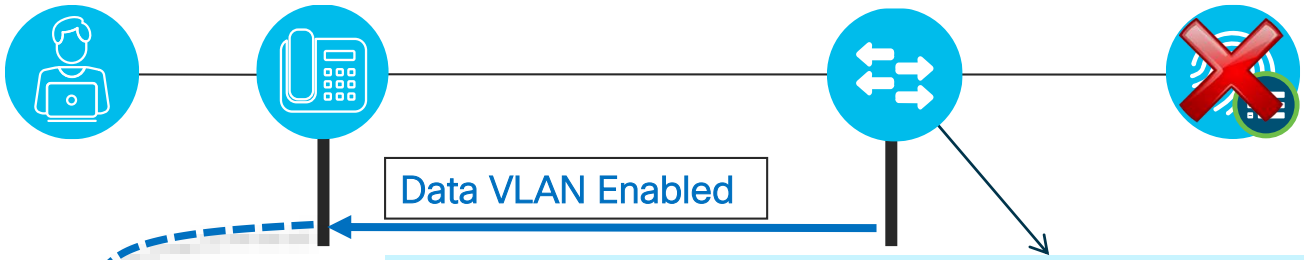
Critical Auth for Data VLAN

Sample Configuration

```
radius-server 10.1.10.50 test username KeepAliveUser key cisco
radius-server dead-criteria time 15 tries 3
radius-server deadtime 1

interface GigabitEthernet1/13
 switchport access vlan 2
 switchport mode access
 switchport voice vlan 200
 authentication event fail action next-method
 authentication event server dead action authorize vlan 100
 authentication event server alive action reinitialize
 authentication order dot1x mab
 dot1x pae authenticator
 authentication port-control auto
 dot1x timeout tx-period 10
 dot1x max-req 2
 mab
 spanning-tree portfast
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

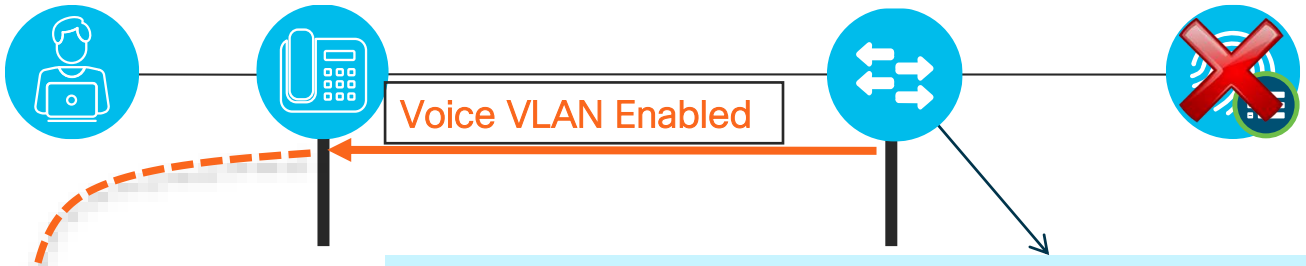
Critical Auth for Data




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


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

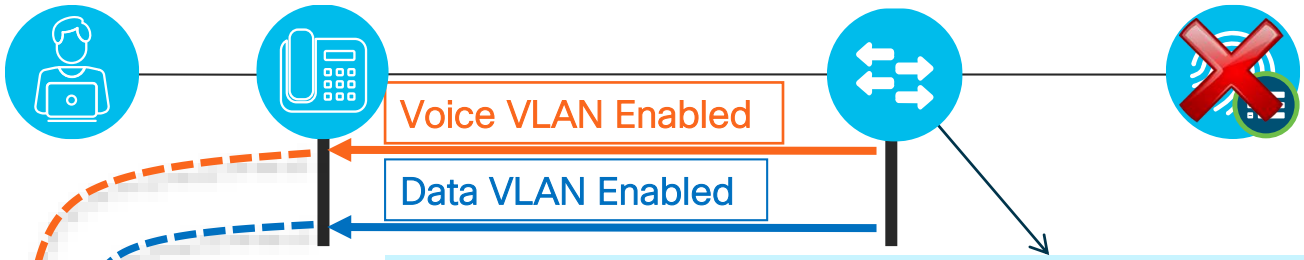
Critical Auth for Voice VLAN (CVV)




```
interface GigabitEthernet 3/48
 dot1x pae authenticator
 authentication port-control auto

 authentication event server dead action authorize voice
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Critical Auth for Data and Voice




```
interface GigabitEthernet 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 Authorization is in effect for domain(s) DATA and VOICE
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multiple Hosts and Critical Auth

Critical Auth for Data and Voice

For Your Reference

- Multi-MDA:

```
Router(config-if)# authentication event server dead action authorize vlan 10
Router(config-if)# authentication event server dead action authorize voice
```

Behavior: Existing data sessions stay authorized in current VLAN; New sessions authorized to VLAN 10

- Multi-Auth:

```
Router(config-if)# authentication event server dead action reinitialize vlan 10
Router(config-if)# authentication event server dead action authorize voice
```

Behavior: All existing data sessions re-authorized to VLAN 10; New sessions are authorized to VLAN 10

- Catalyst Switch Support:

Series	Multi-Auth w/VLAN	Critical Auth for Voice
2k/3k	12.2(55)SE	15.0(1)SE
4k	15.0(2)SG IOS XE 3.2.0SG	15.0(2)SG IOS XE 3.2.0SG
6k	12.2(33)SXJ	12.2(33)SXJ1

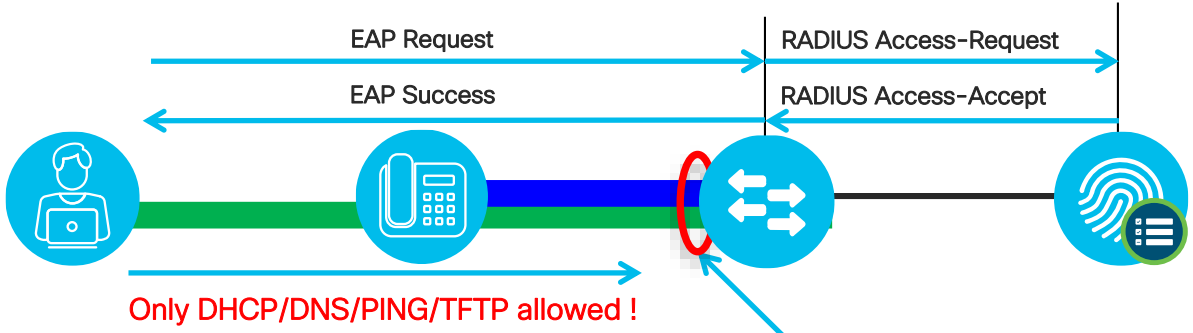
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default Port ACL Issues with No dACL Authorization

Limited Access If ISE Policy Fails to Return dACL!

For Your Reference

- User authentications successful, but authorization profile does not include dACL to permit access, so endpoint access still restricted by existing port ACL!



Auth Success

Authorization Profile = Employee

Access Type = Access-Accept

NO dACL!

```
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
```

```
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
```

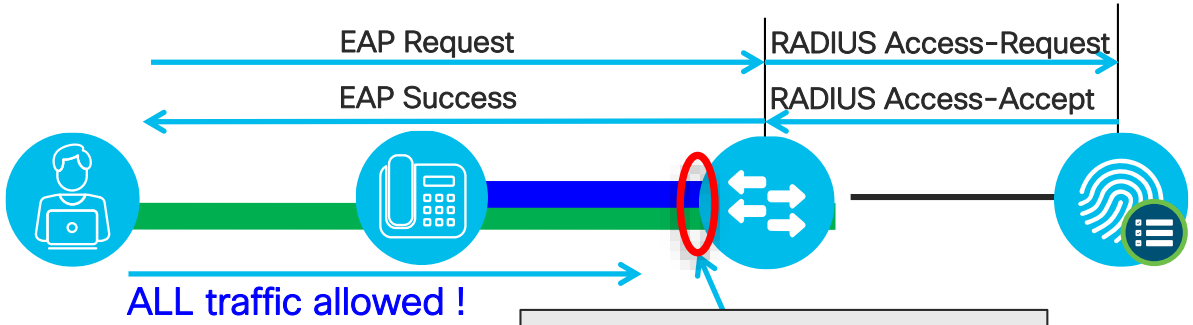

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protecting Against “No dACL” Authorization

For Your Reference

EPM Access Control

- If authentication successful and no dACL returned, a **permit ip host any** entry is created for the host. This entry is created only if no ACLs are downloaded from ISE.



Auth Success

Authorization Profile = Employee

Access Type = Access-Accept

NO dACL!

Insert at top of port ACL:
permit ip any any

```
epm access control open

interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
```

```
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
```

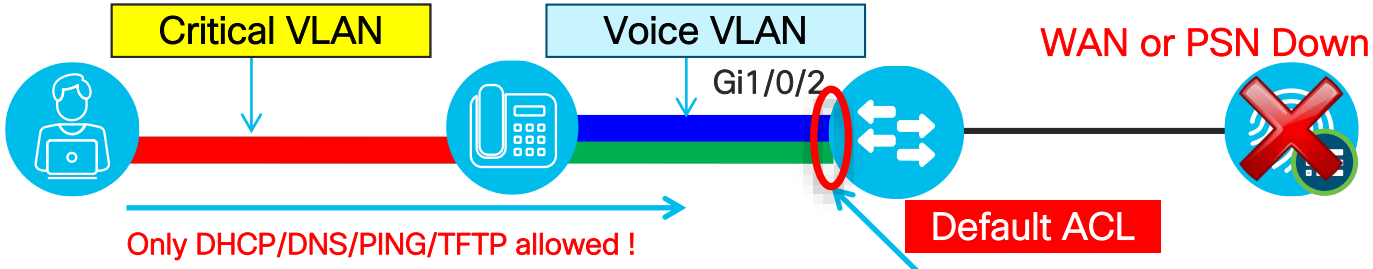
2k/3k: 12.2(55)SE
4k: 12.2(54)G
6k: 15.2(1)SY

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default Port ACL Issues with Critical VLAN

Limited Access Even After Authorization to New VLAN!

- Data VLAN reassigned to critical auth VLAN, but new (or reinitialized) 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
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Critical VLAN w/o Explicit Default Port ACL

For Your Reference

Low Impact versus Closed Mode

- One solution to dACL + Critical Auth VLAN issue is to simply remove the port ACL!
- No static port ACL required for dACLs in current 2k/3k/4k.

2k/3k: 12.2(55)SE
4k: 12.2(54)G
6k: 15.2(1)SY

- Low Impact Mode Use Case:
  - **Initial access permits all traffic**
  - Pro: Immediately allows access to critical services for all endpoints including PXE and WoL devices
  - Con: Temporary window which allows any unauthenticated endpoint to get full access
- Closed Mode User Case
  - **No initial access but default authorization can assign default access policy (typically CWA)**
  - Pro: No access until port authorized
  - Con: Some endpoints may fail due to timing requirements such as PXE or WoL

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Embedded Event Manager with Critical VLAN

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

- EEM available on 3k/4k/6k
- Allows scripted actions to occur based on various conditions and triggers

```
event manager applet default-acl-fallback
 event syslog pattern "%RADIUS-4-RADIUS_DEAD" 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 syslog pattern "%RADIUS-4-RADIUS_ALIVE" 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"
```

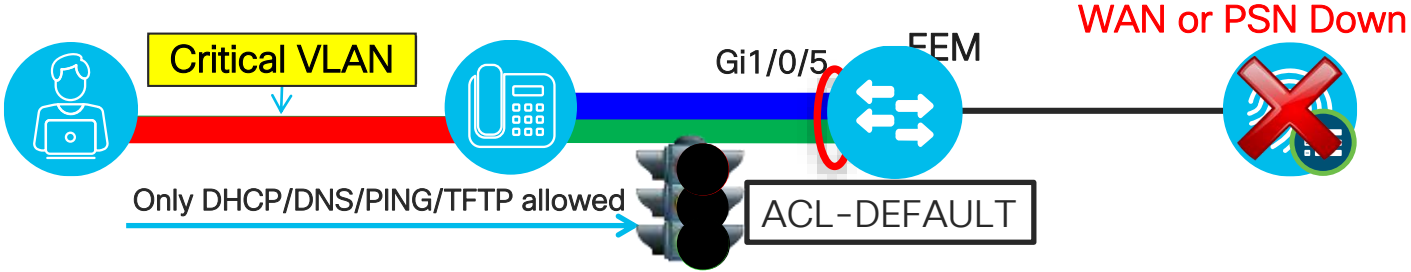
Single RADIUS Server (LB VIP) example shown.

Multi-server option: %RADIUS-3-ALLDEADSERVER

EEM Example

Remove and Add Port ACL on RADIUS Server Status Syslogs

- Port ACLs block new user connections during Critical Auth



- EEM detects syslog message **`%RADIUS-3-ALLDEADSERVER: Group radius: No active radius servers found`** and removes ACL-DEFAULT.

```
event manager applet remove-default-acl
  event syslog pattern "%RADIUS-4-RADIUS_DEAD" maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "interface range gigabitEthernet 1/0/1 - 24"
  action 3.0 cli command "no ip access-group ACL-DEFAULT in"
  action 4.0 cli command "end"
```

- EEM detects syslog message **`%RADIUS-6-SERVERALIVE: Group radius: Radius server 10.1.98.8:1812,1813 is responding again (previously dead)`** and adds ACL-DEFAULT.

```
event manager applet add-default-acl
  event syslog pattern "%RADIUS-4-RADIUS_ALIVE" maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "interface range gigabitEthernet 1/0/1 - 24"
  action 3.0 cli command "ip access-group ACL-DEFAULT in"
  action 4.0 cli command "end"
```

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

EEM Example 2

Modify Port ACL Based on Route Tracking

For Your Reference

```
cat6500(config)# track 1 ip route 10.1.98.0 255.255.255.0 reachability

cat6500(config)# event manager applet default-acl-fallback
cat6500(config-applet)# event track 1 state down maxrun 5
cat6500(config-applet)# action 1.0 cli command "enable"
cat6500(config-applet)# action 1.1 cli command "conf t" pattern "CNTL/Z."
cat6500(config-applet)# action 2.0 cli command "ip access-list extended ACL-DEFAULT"
cat6500(config-applet)# action 3.0 cli command "1 permit ip any any"
cat6500(config-applet)# action 4.0 cli command "end"

cat6500(config)# event manager applet default-acl-recovery
cat6500(config-applet)# event track 1 state up maxrun 5
cat6500(config-applet)# action 1.0 cli command "enable"
cat6500(config-applet)# action 1.1 cli command "conf t" pattern "CNTL/Z."
cat6500(config-applet)# action 2.0 cli command "ip access-list extended ACL-DEFAULT"
cat6500(config-applet)# action 3.0 cli command "no 1 permit ip any any"
cat6500(config-applet)# action 4.0 cli command "end"
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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"
```

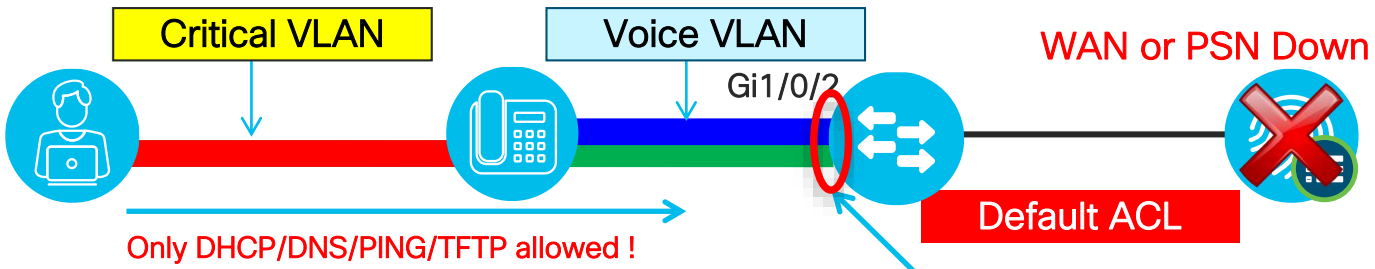
EEM available on Catalyst 3k/4k/6k switches

https://supportforums.cisco.com/document/117596/cisco-eem-basic-overview-and-sample-configurations
https://supportforums.cisco.com/document/48891/cisco-eem-best-practices

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
```

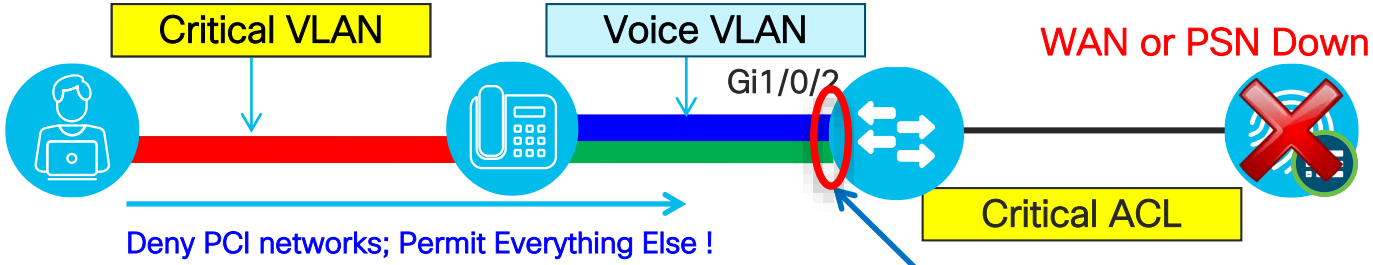
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Critical ACL using Service Policy Template

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

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

- Critical Auth ACL applied on Server Down

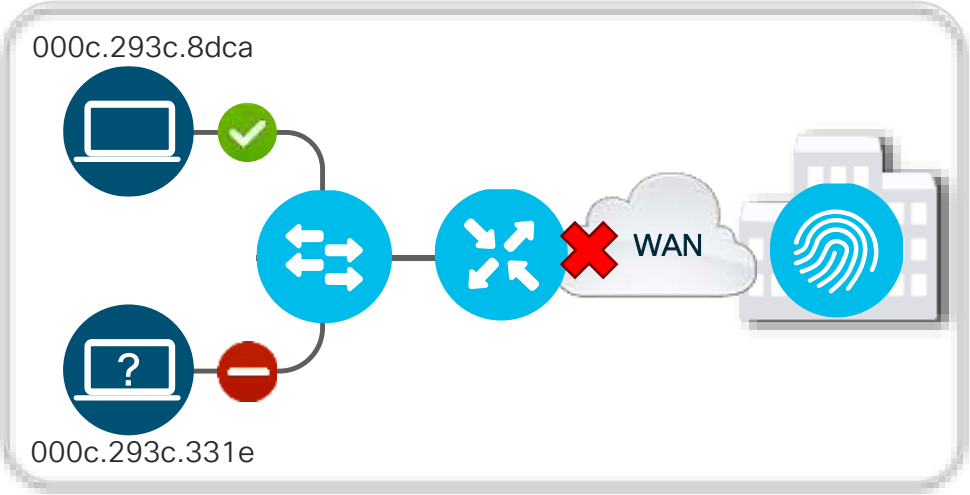



```
policy-map type control subscriber ACCESS-POLICY
  event authentication-failure match-first
    10 class AAA_SVR_DOWN_UNAUTHD do-until-failure
      10 activate service-template CRITICAL_AUTH_VLAN
      20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
      30 activate service-template 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
```

Critical MAB

Local Authentication During Server Failure




```
username 000c293c8dca password 0 000c293c8dca
username 000c293c8dca aaa attribute list mab-local
!
aaa local authentication default authorization mab-local
aaa authorization credential-download mab-local local
!
aaa attribute list mab-local
 attribute type tunnel-medium-type all-802
 attribute type tunnel-private-group-id "150"
 attribute type tunnel-type vlan
 attribute type inacl "CRITICAL-V4"
!
policy-map type control subscriber ACCESS-POL
...
event authentication-failure match-first
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-↵
          until-failure
  10 terminate mab
  20 terminate dot1x
  30 authenticate using mab aaa authc-↵
     list mab-local authz-list mab-local
...
```

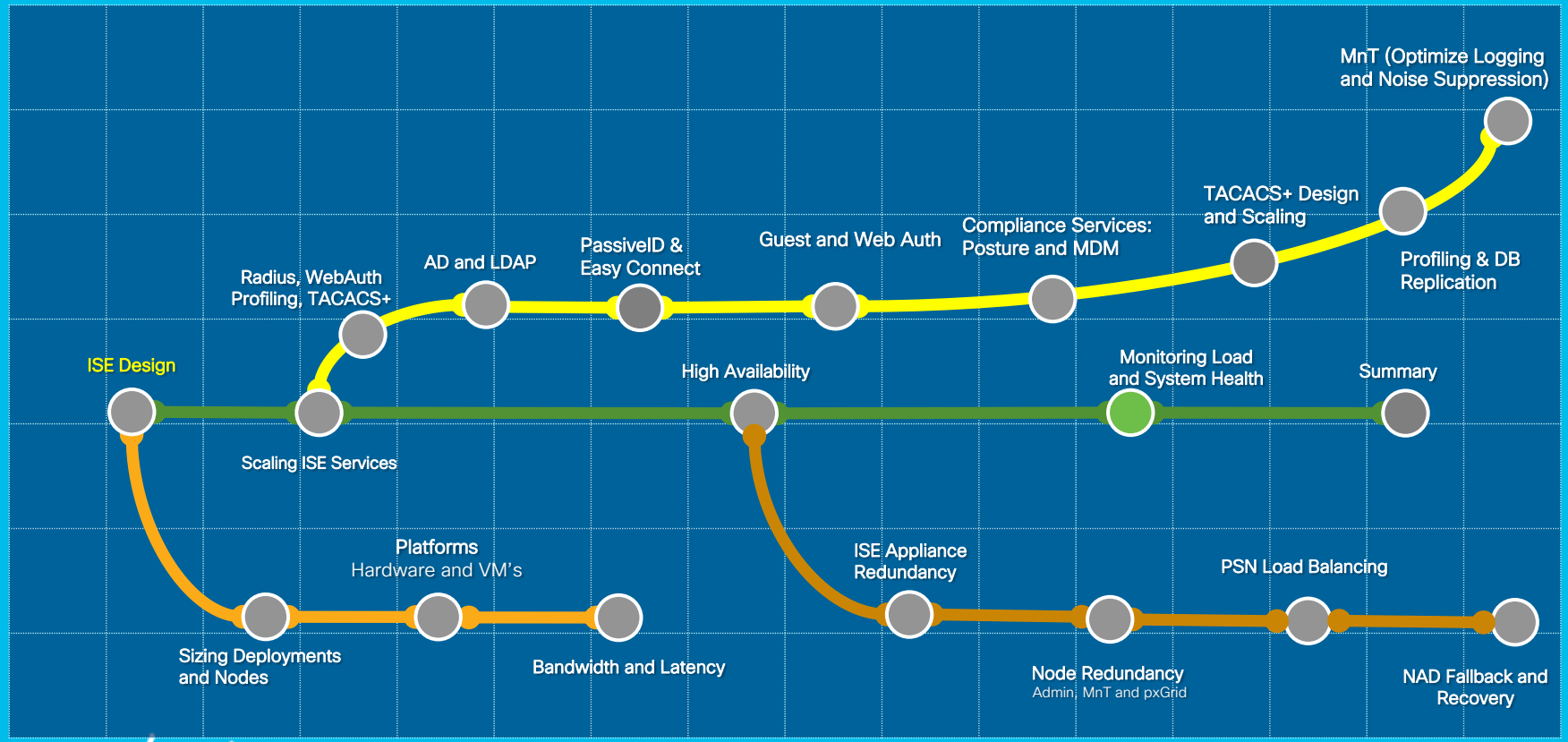
- Additional level of check to authorize hosts during a critical condition.
- EEM Scripts could be used for dynamic update of whitelist MAC addresses
- Sessions re-initialize once the server connectivity resumes.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitoring Load and System Health

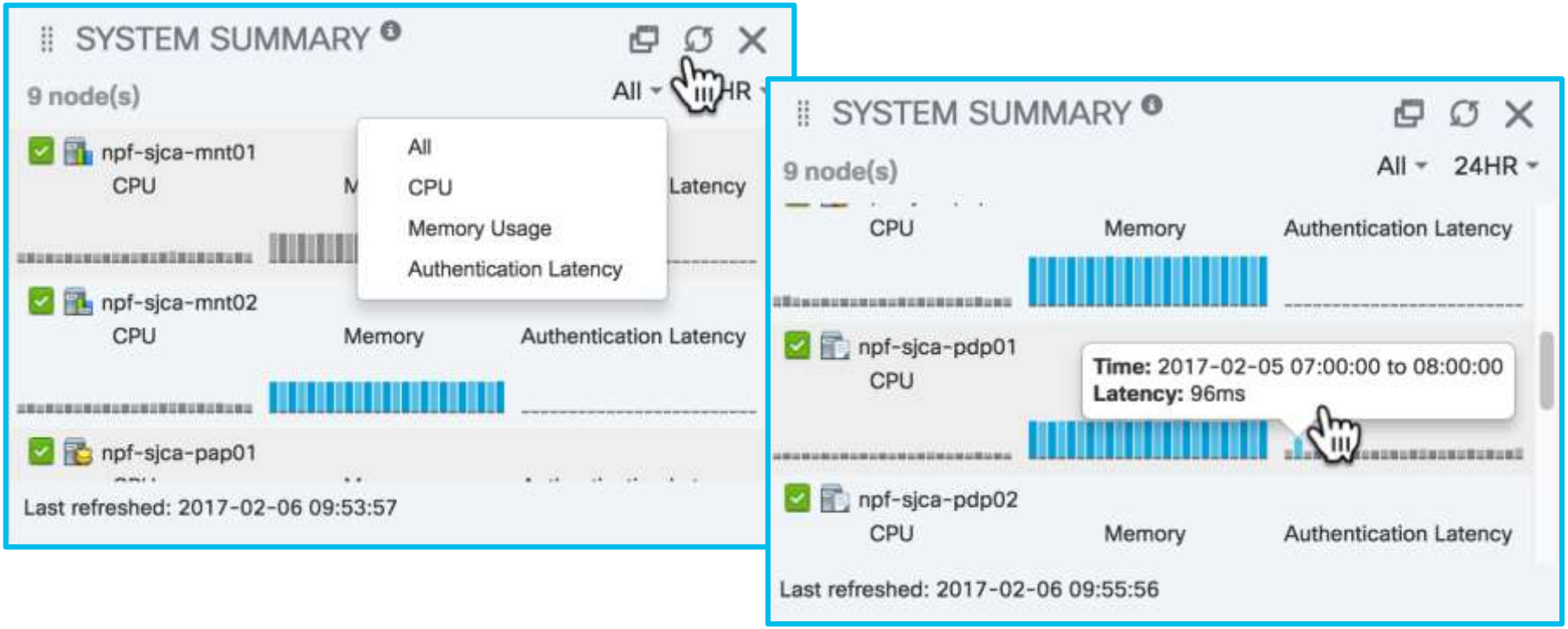
Session Agenda

Monitoring Load and System Health



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Home Dashboard - High-Level Server Health

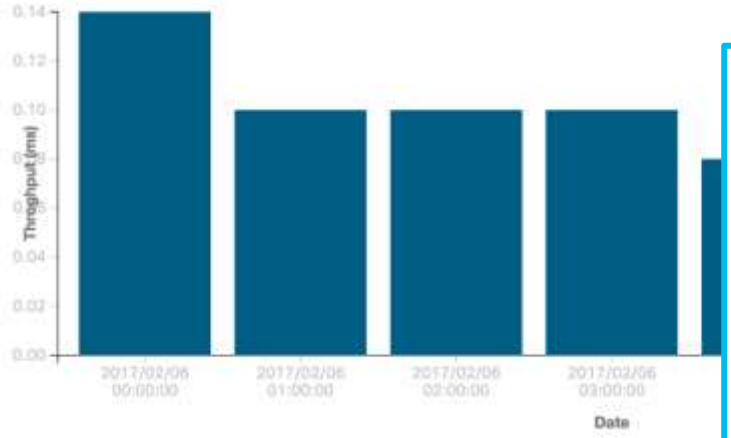


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Server Health/Utilization Reports

Operations > Reports > Diagnostics > Health Summary

Chart: Time Vs Throughput



Health Summary

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

Recent Disk Space Utilization (%)

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

CPU Usage (Updated every 15 min)

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Replication – Message Queue Backlog

Administration > System > Deployment

Deployment Nodes

Edit | Register | Syncup | Deregister

Hostname	Node Type	Personas	Role(s)	Services	Node Status
npf-sjca-mnt01	ISE	Monitoring	PRIMARY(M)	NONE	✓
npf-sjca-mnt02	ISE	Monitoring	SECONDARY(M)	NONE	✓
npf-sjca-pap01	ISE	Administration	SECONDARY(A)	NONE	✓
npf-sjca-pap02	ISE	Administration	PRIMARY(A)	NONE	✓
npf-sjca-pdp01	ISE	Policy Service		IDENTITY MAPPING,TC-NAC,SESSION,PROF...	✓
npf-sjca-pdp02	ISE	Policy Service			
npf-sjca-px01	ISE	Policy Service, pxGrid			
npf-sjca-px02	ISE	Policy Service, pxGrid			
sbg-bgla-pdp01	ISE	Policy Service			

Deployment Status

Registered : Thu Jan 26 2017 23:47:32 GMT-0500 (EST)

Sync Status: 473 messages to be synced.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Application Status (ISE 2.2)

For Your Reference

```
# show application status ise
```

```
ise22-pan1/admin# show application status ise

ISE PROCESS NAME                        STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                       running          3172
Database Server                         running          69 PROCESSES
Application Server                      running          9148
Profiler Database                       running          6239
ISE Indexing Engine                     running          18685
AD Connector                            running          19556
M&T Session Database                    running          6147
M&T Log Collector                       running          9283
M&T Log Processor                       running          9195
Certificate Authority Service           running          15735
EST Service                             running          25380
SXP Engine Service                      running          16549
Docker Daemon                           running          635
TC-NAC MongoDB Container                running          12867
TC-NAC RabbitMQ Container               running          12298
TC-NAC Core Engine Container            running          13617
VA Database                             running          14352
VA Service                              running          14650
Wifi Setup Helper Container             running          15319
 Wifi Setup Helper Vault                running          32
 Wifi Setup Helper MongoDB              running          15
 Wifi Setup Helper Web Server           running          220
 Wifi Setup Helper Auth Service         running          131
 Wifi Setup Helper Main Service         running          166
 Wifi Setup Helper WLC Service          running          283
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID WMI Service                   running          17230
PassiveID Syslog Service                running          17672
PassiveID API Service                   running          18327
PassiveID Agent Service                 running          18628
PassiveID Endpoint Service              running          18986
PassiveID SPAN Service                  running          19384
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled
```

ISE 2.2 adds:

- EST Service
- Wifi Setup Helper details
- Individual Passive ID collection services

ISE Application Status (ISE 2.4)

For Your Reference

```
# show application status ise
```

```
ise22-pan1/admin# show application status ise

ISE PROCESS NAME                        STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                       running          3172
Database Server                         running          69 PROCESSES
Application Server                      running          9148
Profiler Database                       running          6239
ISE Indexing Engine                     running          18685
AD Connector                            running          19556
M&T Session Database                    running          6147
M&T Log Collector                       running          9283
M&T Log Processor                       running          9195
Certificate Authority Service           running          15735
EST Service                             running          25380
SXP Engine Service                      running          16549
Docker Daemon                           running          635
TC-NAC MongoDB Container                running          12867
TC-NAC RabbitMQ Container               running          12298
TC-NAC Core Engine Container            running          13617
VA Database                             running          14352
VA Service                              running          14650
Wifi Setup Helper Container             running          15319
 Wifi Setup Helper Vault                running          32
 Wifi Setup Helper MongoDB              running          15
 Wifi Setup Helper Web Server           running          220
 Wifi Setup Helper Auth Service         running          131
 Wifi Setup Helper Main Service         running          166
 Wifi Setup Helper WLC Service          running          283
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID WMI Service                   running          17230
PassiveID Syslog Service                running          17672
PassiveID API Service                   running          18327
PassiveID Agent Service                 running          18628
PassiveID Endpoint Service              running          18986
PassiveID SPAN Service                  running          19384
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled
```

ISE 2.4 adds:

- ISE RabbitMQ Container

ISE Application Status (ISE 2.6)

For Your Reference

```
# show application status ise
```

```
ise22-pan1/admin# show application status ise

ISE PROCESS NAME                        STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                       running          3172
Database Server                         running          69 PROCESSES
Application Server                      running          9148
Profiler Database                       running          6239
ISE Indexing Engine                     running          18685
AD Connector                            running          19556
M&T Session Database                    running          6147
M&T Log Collector                       running          9283
M&T Log Processor                       running          9195
Certificate Authority Service           running          15735
EST Service                             running          25380
SXP Engine Service                      running          16549
Docker Daemon                           running          635
TC-NAC MongoDB Container                running          12867
TC-NAC RabbitMQ Container               running          12298
TC-NAC Core Engine Container            running          13617
VA Database                             running          14352
VA Service                              running          14650
Wifi Setup Helper Container             running          15319
 Wifi Setup Helper Vault                running          32
 Wifi Setup Helper MongoDB              running          15
 Wifi Setup Helper Web Server           running          220
 Wifi Setup Helper Auth Service         running          131
 Wifi Setup Helper Main Service         running          166
 Wifi Setup Helper WLC Service          running          283
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID WMI Service                   running          17230
PassiveID Syslog Service                running          17672
PassiveID API Service                   running          18327
PassiveID Agent Service                 running          18628
PassiveID Endpoint Service              running          18986
PassiveID SPAN Service                  running          19384
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled
```

ISE 2.6 adds:

- ISE RabbitMQ Container renamed to ISE Messaging Service

KPM in a Nutshell

For Your Reference

- What is KPM?
  - KPM stands for Key Performance Metrics. These are the metrics collected from the MNT nodes about the Endpoints and its artifacts
- Benefits of KPM:
  - **Endpoints Onboarding data:** Measure key performance metrics about Endpoints, like Total, Active, Successful, Failures, Endpoints on-boarded/day
  - **Endpoints Transactional Load data:** # radius requests at a PSN level/hr, Radius requests to # Active EP ratio, How much of these data was persisted in the MNT table and how many of them were suppressed to determine the suppression ratio, what was the Avg and Max load on the PSN during that hour, what was the latency and Avg TPS.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Performance Metrics (KPM)

application configure ise (Options 12 and 13)

CLI added in ISE 1.4
Admin UI Reports added in ISE 2.2

- Generate performance metrics:
  - Endpoints Onboarding
  - Endpoints Transactional Load
- Saves to local disk
  - Can copy to repository for viewing
- Reports are suffixed with date parameter
  - If run in same day, will overwrite
- Can be resource intensive on CPU/Memory, so advised to run during non-peak hours

```
ise22-b368/admin# app config ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Exit
12
You are about to generate Daily KPM (Key Performance Metrics).
  % Warning  Generating KPM stats may impact ISE performance during the gener
on of the report.It is suggested to run this report during non-peak hours and
en not conflicting with other scheduled operations of ISE.
Are you sure you want to proceed? y/n [n]: y
Starting to generate Daily KPM stats
Copying files to /localdisk
Completed generating daily KPM stats. You can find details in following file
cated under /localdisk
KPM_onboarding_results_01_MAY_2015.xls
KPM_trx_load_01_MAY_2015.xls
```

For Your Reference

Options 12 and 13

cisco Live!

KPM Attributes

For Your Reference

- KPM OnBoarding Results:
  - Total Endpoints : Total number of endpoints in the deployment
  - Successful Endpoints : How many of them were on boarded successfully
  - Failed Endpoints : How many failed to on board
  - New EP/day : New endpoints seen in the deployment for a given day
  - Total Onboarded/day : Total endpoints on-boarded for a given day
- KPM Trx Load
  - Timestamp: Date/Time, This is an hourly window, extrapolated from the syslogs sent by the PSNs
  - PSN name : Hostname of the PSN sending syslogs to the MNT collector
  - Total Endpoints: Total number of endpoints in the deployment
  - Active Endpoints: Active number of endpoints in the deployment for that hour.
- KPM Trx Load (cont)
  - Radius Requests : Number of Radius requests sent by the PSNs for that hour.
  - RR_AEP_ratio : Ratio of Radius Requests to the number of Active endpoints on an hourly basis. This will give the number of radius request an Active EP makes on an average.
  - Logged_to_MNT/hr : Number of Radius Request persisted in the DB
  - Noise/hr : Number of Radius Request suppressed, only the counter increases but the data is not persisted in the DB.
  - Supression_hr % : % of suppression
  - Avg_Load (avg) : Average load of the PSNs during that hourly window
  - Max Load (avg): Max load of the PSNs during that hourly window
  - Latency_per_request: Latency per radius request (average)
  - Avg TPS : Average number of transactions per second on that PSN.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Raw Sample of KPM Stats Output

For Your Reference

- KPM_TRX_LOAD_<DATE>.xls

TIMESTAMP	PSN NAME	TOTAL ENDP	ACTIVE ENDF	RADIUS REQUESTS	RR_AEP_RATIO	LOGGED TO MNT/HR	NOISE/HR	SUPPRESSION_HR%	AVG LOAD Avg	MAX LOAD Avg	Latency Per Request	AVG TPS
7/31/13 23:00	ise-4	7148	496	1569					1.36	2.5	0.05	
8/1/13 1:00	ise-4	7151	490	924	1.89	335	589	63.74	1.04	2.5	0.09	0.26
8/1/13 2:00	ise-4	7151	488	519	1.06	150	369	71.1	1.04	2.5	0.28	0.14
8/1/13 3:00	ise-4	7151	485	599	1.24	183	416	69.45	0.83	2.5	0.21	0.17
8/1/13 5:00	ise-4	7152	482	458	0.95	153	305	66.59	0.63	2.5	0.5	0.13
8/1/13 6:00	ise-4	7152	492	960	1.95	297	663	69.06	1.88	2.5	0.08	0.27
8/1/13 7:00	ise-4	7154	500	2272	4.54	749	1523	67.03	1.25	2.5	0.04	0.63
8/1/13 9:00	ise-4	7161	592	3558	6.01	1174	2384	67	3.13	5	0.06	0.99
8/1/13 10:00	ise-4	7167	618	3551	5.75	1086	2465	69.42	2.08	5	0.05	0.99
8/1/13 11:00	ise-4	7169	628	3910	6.23	1333	2577	65.91	13.13	82.5	0.07	1.09
8/1/13 13:00	ise-4	7185	577	4055	7.03	1244	2811	69.32	3.13	5	0.04	1.13
8/1/13 14:00	ise-4	7193	588	3079	5.24	1037	2042	66.32	2.73	5	0.06	0.86
8/1/13 15:00	ise-4	7197	578	4086	7.07	1212	2874	70.34	4.17	7.5	0.04	1.14
8/1/13 17:00	ise-4	7206	519	2856	5.5	1134	1722	60.29	2.71	5	0.07	0.79
8/1/13 18:00	ise-4	7213	504	2307	4.58	753	1554	67.36	3.75	7.5	0.19	0.64
8/1/13 19:00	ise-4	7215	482	1711	3.55	456	1255	73.35	3.13	7.5	0.12	0.48
8/1/13 21:00	ise-4	7217	491	1664	3.39	433	1231	73.98	3.13	5	0.07	0.46
8/1/13 22:00	ise-4	7217	484	1391	2.87	377	1014	72.9	2.29	5	0.07	0.39
8/1/13 23:00	ise-4	7217	476	913	1.92	279	634	69.44	2.73	5	0.1	0.25

- KPM_ONBOARDING_RESULTS_<DATE>.xls

TOTAL ENDPOINTS	SUCCESSFUL ENDPOINTS	FAILED ENDPOINTS	NEW EP/Day	TOTAL ONBOARDED/Day
7217	6931	286	7	0

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Performance Metrics (KPM)

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

Also available from CLI (# application configure ise)

Provide RADIUS Load, Latency, and Suppression Stats

Key Performance Metrics

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

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

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Serviceability Counter Framework

For Your Reference

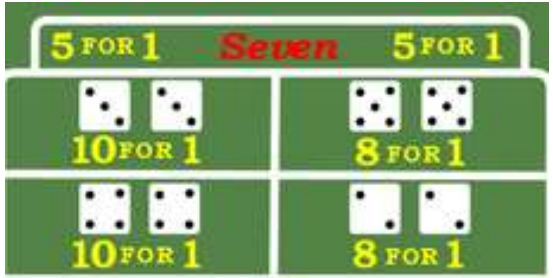
Overview

- Counter Framework (CF) is a library to periodically collect different ISE attributes.
- Modules like profiler, network access, etc configured few critical attributes in CF.
- CF periodically collects all these attributes in each node and persists in MnT via syslog.
- “ISE Counters” report (Operations → Reports → Diagnostics) lists the attribute values per node.
- All counter attributes are enabled by default. To disable/enable use “application configure ise” admin command with option number 14 ([14]Enable/Disable Counter Attribute Collection).
- Support bundle of MnT node (if “Include monitoring and reporting logs” is checked) will have the counter attribute database table dump in csv format.
- Similar to admin “show cpu usage” command, cpu usage are displayed in “Health Summary” report (Operations → Reports → Diagnostics).

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Displaying Profiler Statistics

The Hard Way




```
ise21-pan1/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Exit
```

6 <Enter>

Create an RMI connector client and connect it to the RMI connector server

Get an MBeanServerConnectionRetrieve MXBean

Press <Enter> to continue...

Timestamp,Elapsed,EHQDroppedEvents,LocalEndPointReads,EndpointsOwnerChanged,ProbeDummyEndpointsDetected,ProbeSnmpQueryEndpointsDetected,RadiusPacketsReceived,CoAHandledEvents,RemoteUpdateAverted,ProbeDhcpEndpointsDetected,IosSensorDhcpDetected,HttpPacketsNonAdjacentDropped,NACReSyncNotify,EndpointsDropped,RemoteUpdate,ProbeNmapSnmpQueryTriggered,HttpPacketsAdjacent,IosSensorCdpDetected,EndpointsProfiled,HttpPacketsReceived,EndpointsReProfiled,FeedPolicyCreate,DhcpSkipProfiling,EndpointsUpdated,ProbeRadiusEndpointsDetected,IosSensorMdnsDetected,ProbeDnsEndpointLookupAvert,ProfilerCacheMisses,ProbeSnmpTrapEndpointsDetected,ARPSave,IosSensorH323Detected,ARPUpdate,CoADroppedEvents,ARPMiss,ProbeDnsEndpointsDetected,ProbeNetflowEndpointsDetected,ProbeSpanEndpointsDetected,ARPHit,EndpointsRetrievedFromOwner,IosSensorLldpDetected,ARPRetrieve,EndpointsSaved,ProfilerCacheHits,FeedPolicyUpdate,SnmpTrapsReceived,IosSensorHttpDetected,FeedEndpointsReProfiled,RemoteSave,SnmpQueriesPerformed,NACEndpointNotify,EndpointsDeleted,IosSensorMDMDetected,DhcpPacketsReceived,NmapSubnetScanEndpointsDiscovered,ProbeHttpEndpointsDetected,ProbeDnsEndpointLookup,EndpointsCached,IosSensorSipDetected,NetflowPacketsReceived,ProbeNmapScannedEndpoints,EndpointsDetected

1493585875206,1000,0,193,0,0,0,18,0,7,0,0,0,0,0,0,0,0,0,7,0,0,0,0,22,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,7,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8

1493585876233,2027,0,193,0,0,0,18,0,7,0,0,0,0,0,0,0,0,0,7,0,0,0,0,22,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,7,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8

1493585877258,3052,0,193,0,0,0,18,0,7,0,0,0,0,0,0,0,0,0,7,0,0,0,0,22,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,7,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8

1493585878288,4082,0,193,0,0,0,18,0,7,0,0,0,0,0,0,0,0,0,7,0,0,0,0,22,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,7,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8

1493585879325,5119,0,193,0,0,0,18,0,7,0,0,0,0,0,0,0,0,0,7,0,0,0,0,22,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,7,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8

Serviceability Counter Framework (CF)

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

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

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

- Audit
- Device Administration
- Diagnostics
  - AAA Diagnostics
  - AD Connector Operations
  - Endpoint Profile Changes
  - Health Summary
  - ISE Counters
  - Key Performance Metrics
  - Misconfigured NAS
  - Misconfigured Supplicants
  - Network Device Session ...
  - OCSP Monitoring
  - RADIUS Errors

ISE Counters

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

Node specific report

Filters

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

Thresholds

Counter Attribute Threshold

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

Detected platform size

Disable/Enable Counter Attribute Collection

For Your Reference

```
pmbudev-vm75/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Exit

14
Do you want to Enable(e) or Disable(d) counter attribute collection? [e/d]d
Completed disabling counter attributes. It will take at the most 30 minute to get effected.
no crontab for oracle

Selection ISE configuration option
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Counters

5-Minute and > 5-Minute Collection Results

Threshold Counter Trends (attributes collected every 5 min)

Collected At	IO Wait	Protocol...	Probe R...	Probe R...	ARP Ca...	Hostna...	NMAP S...	Endpoin...	TC-NAC...
2017-04-30 12:10:35.122	.35	42718	0	0	64550	64	72	284	NA
2017-04-30 12:05:35.119	.35	42711	0	0					
2017-04-30 12:00:35.117	.35	42704	0	0					
2017-04-30 11:55:35.115	.35	42695	0	0					
2017-04-30 11:50:33.958	.35	42687	0	0					
2017-04-30 11:45:33.956	.35	42681	0	0					
2017-04-30 11:40:33.954	.35	42672	0	0					
2017-04-30 11:35:33.952	.35	42664	0	0					
2017-04-30 11:30:33.95	.35	42658	0	0					
2017-04-3									
2017-04-3									
2017-04-3									
2017-04-3									
2017-04-3									

Threshold Counter Trends (attributes collected more than 5 min)

Collected At	Endpoint Ownership Change	Endpo...	Endpo...	Http E...	SNMP...	DNS ...	DNS ...	SNMP...	DHCP...
2017-04-30 12:10:...	52126	117870	119439	NA	NA	NA	NA	NA	NA
2017-04-30 11:50:...	52121	117843	119412	0	8698	2733	309139	0	2600521
2017-04-30 11:30:...	52115	117						NA	NA
2017-04-30 11:20:...	NA	NA							2598673
2017-04-30 11:10:...	52108	1178						NA	NA
2017-04-30 10:50:...	52102	1177							2596835
2017-04-30 10:30:...	52096	1177						NA	NA
2017-04-30 10:20:...	NA	NA							2594996
2017-04-30 10:10:...	52089	117745	119314	NA	NA	NA	NA	NA	NA
2017-04-30 09:50:...	52086	117720	119289	0	8670	2723	307252	0	2593164
2017-04-30 09:30:...	52086	117708	119277	NA	NA	NA	NA	NA	NA
2017-04-30 09:20:...	NA	NA	NA	0	8670	2720	306878	0	2591329
2017-04-30 09:10:...	52086	117699	119268	NA	NA	NA	NA	NA	NA
2017-04-30 08:50:...	52080	117671	119240	0	8656	2717	306312	0	2589471
2017-04-30 08:30:...	52074	117653	119222	NA	NA	NA	NA	NA	NA

Example:
Endpoint Ownership Changes per interval (20 min for this metric; threshold = 5k events)

Example:
Delta in this interval = 6 ownership changes (over 20 minutes)

Note: Counters are cumulative so need to take deltas to determine events per interval

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

`show cpu` CLI and in Health Summary Report

For Your Reference

```
ise22-pan1/admin# sh cpu usage

ISE Function                          % CPU Usage          CPU Time      Number of threads
-----------------------------------------------------------------------------------------------
Threat Centric NAC MongoDB Container      0.10             93:08.35              22
Database Server                           0.05             51:51.94              81 processes
ISE Indexing Engine                       0.03             33:18.51             101
Identity Mapping Service                  0.03             30:33.69              40
M&T Log Collector
Vulnerability Asse
M&T Log Processor
Admin Process JVM
Docker Daemon
Admin Webapp
Certificate Author
Profiler Database
Quartz Scheduler
M&T Session Databa
Vulnerability Asse
NSF Persistence La
Database Listener
Message Queue
WIFI Setup
Profiler
RMI Services
Syslog Processor
Guest Services
Threat Centric NAC
Threat Centric NAC
BYOD Services
```

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

- My Reports
- Reports
  - Audit
  - Device Administration
  - Diagnostics
    - AAA Diagnostics
    - AD Connector Operations
    - Endpoint Profile Changes
    - Health Summary
    - ISE Counters

Rows/Page 1 | 1 / 1

CPU Usage (Updated every 15 min)

ISE Function	% CPU Usage	CPU Time	Number of Threads
Threat Centric NAC MongoDB Container	0.10	92:44.51	22
Database Server	0.05	51:28.31	78 processes
ISE Indexing Engine	0.03	33:08.88	99
Identity Mapping Service	0.03	30:21.67	40
M&T Log Collector	0.02	18:57.98	7
Vulnerability Assessment Service	0.02	14:59.23	45
M&T Log Processor	0.01	14:05.91	64
Admin Process JVM Threads	0.01	11:33.92	12

Summary of Reports Enhancements in ISE 2.2

For Your Reference

Revamp of the Report framework

Changed the flex pages to html pages
(Technology used – HTML, JS, Backbone, Bootstrap for frontend)

Merged Saved report and Favorite report to one bucket ‘My Report’

Local csv export limit has been increased to 5000 records

Local pdf export limit is 1000 records.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary of Reports Enhancements in ISE 2.2

Continued

For Your Reference

- Clicking on the report will generate the the report for last 7 days.
- In multi section report (e.g. -Authentication Summary)the pagination is supported at each and every grid section(e.g – Authentications by Failure reason) i.e navigation to next set of records for each section can be done individually.
- Added Custom time range filter and Advance filter in all the reports
- Regex can be used for server, identity and mac address column. The supported regex are :- (*abc -> ends with, abc* -> starts with and abc* or *abc -> ‘OR’ condition)
- Scheduled and saved reports will save the details of definition

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Scalability and High Availability

For Your Reference

Summary Review

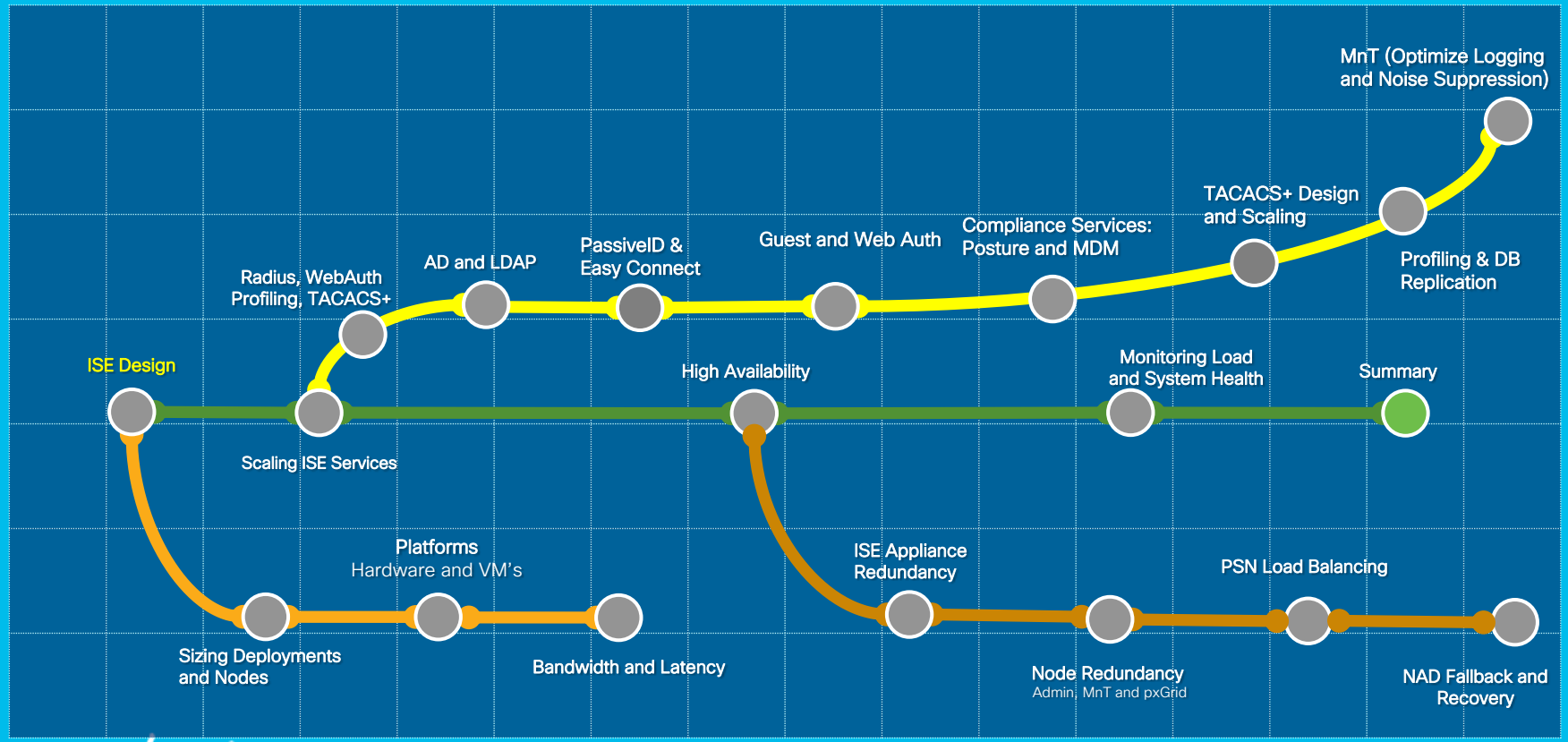
- Appliance selection and persona allocation impacts deployment size.
- VM appliances need to be configured per physical appliance sizing specs.
- Profiling scalability tied to DB replication—deploy node groups and optimize PSN collection.
- Leverage noise suppression to increase auth capacity and reduce storage reqs.
- ISE enhances scalability with multi-AD and auto-device registration & purge.
- Admin, MnT, and pxGrid 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.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Closing Comments

Session Agenda

Monitoring Load and System Health



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Community Page on Sizing and Scalability

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

cisco Communities

Cisco Communities > Technology > Security > Policy and Access > Identity Services Engine (ISE) > Documents

ISE Performance & Scale

- ISE 2.4 Deployment Scale and Limits
- ISE 2.2+ Deployment Scale and Limits
- ISE Hardware Platforms
- ISE PSN Performance
  - ISE TACACS+ Performance
  - ISE 2.3 RADIUS Performance
  - ISE 2.2 RADIUS Performance
  - ISE 2.0 Scenario-Based Performance
  - ISE 2.2 Passive Identity (Passive ID) and Easy Connect Scaling
    - Passive ID / EZC Scaling Per Deployment
    - Passive ID / Easy Connect Scaling per PSN dedicated to Passive ID Servic
    - Passive ID - Provider and Consumer Scaling
  - ISE 2.2 Platform Exchange Grid (pxGrid) Scaling
    - pxGrid Scaling per Deployment
    - pxGrid Scaling per Dedicated pxGrid Node
  - ISE 2.2 SXP Scaling
    - ISE SXP Scaling per Deployment
    - ISE SXP Scaling per SXPSN
  - ISE 2.2 Threat-Centric NAC (TC-NAC) Scaling
    - TC-NAC Scaling per Deployment
    - TC-NAC Scaling per PSN
- ISE Storage Requirements
  - VM Disk Size Minimum Requirement
  - MnT Persona Log Storage Requirements
    - RADIUS Log Retention (Days):
    - TACACS+ log retention(Days)
      - Scripted device admin model:
      - Human admin - Device admin model
- ISE Latency & Bandwidth
  - ISE 2.0 Latency
  - ISE 2.1 Latency
  - WAN Bandwidth Calculator
- Sources

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Performance & Scale Resources

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

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

ISE Deployment Sizing and Scalability

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

ISE Install Guide on Deployment Sizing

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

Includes Working Configs for ACE and F5

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

ISE Load Balancing

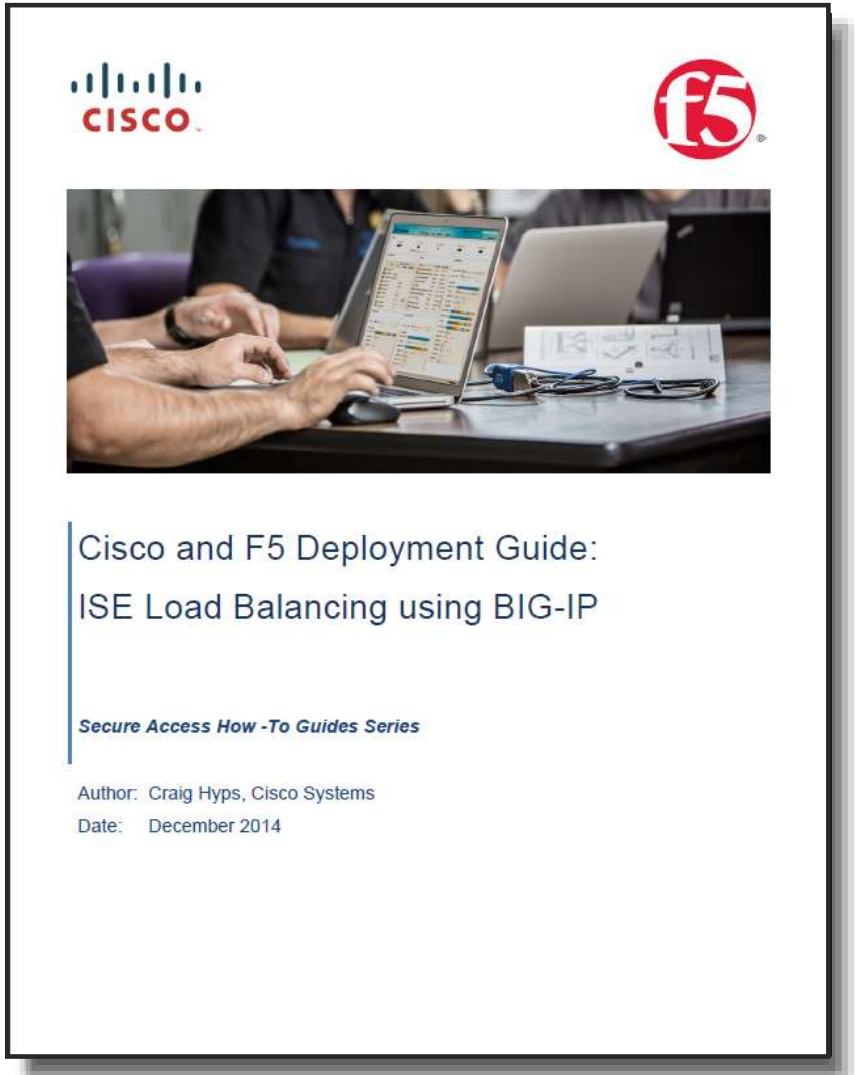
ISE Latency and Bandwidth Calculators

ISE MnT Log sizing calculator for TACACS+ and RADIUS

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

cisco Live!

For Your Reference



Cisco and F5 Deployment Guide:

ISE Load Balancing using BIG-IP

Secure Access How -To Guides Series

Author: Craig Hyps, Cisco Systems

Date: December 2014

- Cisco Communities
  https://community.cisco.com/t5/security-documents/ise-load-balancing/ta-p/3648759
  Includes Sample Working Configs, Videos, and update notes on LB Guide.
- Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP:
  https://community.cisco.com/t5/security-documents/how-to-cisco-amp-f5-deployment-guide-ise-load-balancing-using/ta-p/3631159
- Linked from F5 website under Cisco Alliance page > White Papers:
  https://f5.com/solutions/technology-alliances/cisco

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Additional Resources

Public Resources

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Additional Resources

Public Resources

ISE Licensing & Ordering	http://cs.co/ise-license
ISE Training	http://cs.co/ise-training
ISE Portal Builder	http://isepb.cisco.com
Trustsec Compatibility	http://cs.co/trustsec-compatibility
Trustsec Resources	http://cs.co/trustsec-resources

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Your Reference

Additional Resources

Sales Resources (Cisco & Partners)

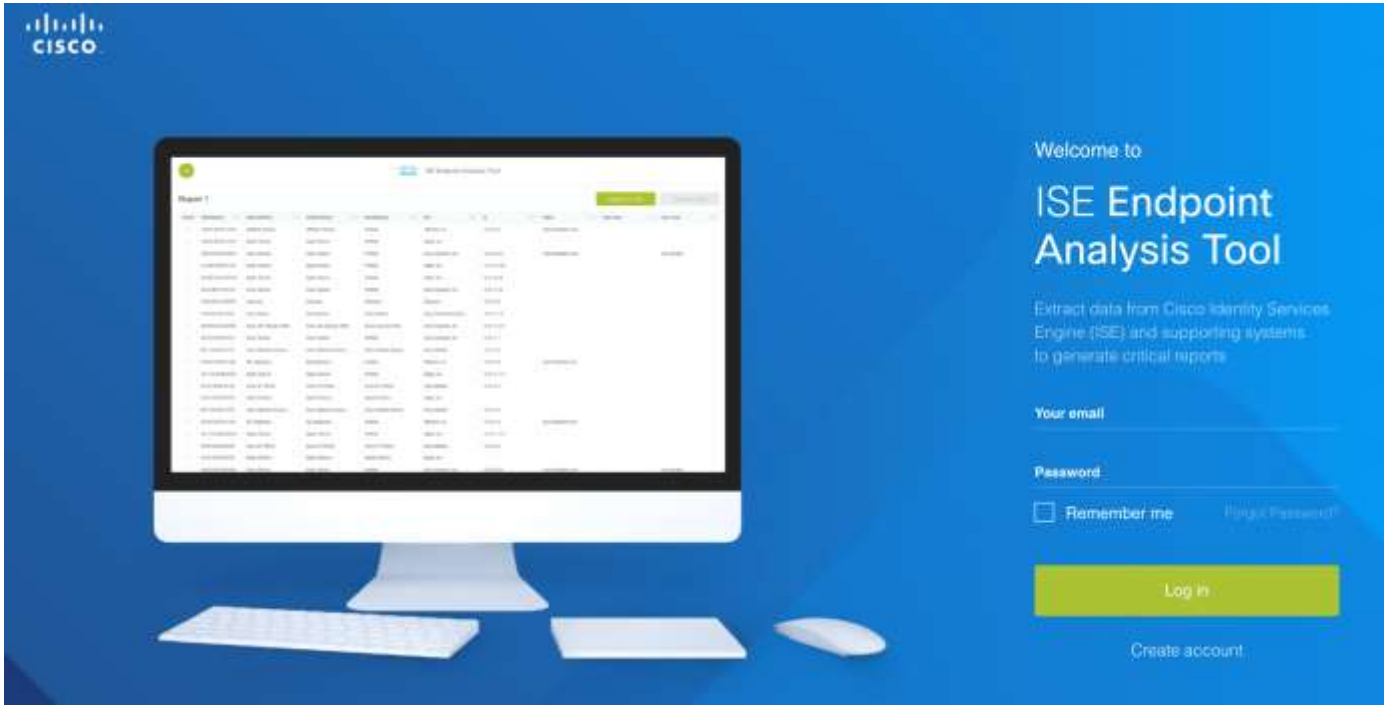
Selling ISE @ Training	http://cs.co/selling-ise-training
Selling ISE Demos	http://cs.co/selling-ise-demos
ISE Instant Demo	http://cs.co/ise-instant-demo
ISE Proof Of Value Kit	http://cs.co/ise-pov
ISE Bill Of Materials Tool	http://ise-bom.cisco.com

How to Find ISE Customer References

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Endpoint Analysis Tool

http://iseeat.cisco.com



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Portal Builder

http://isepb.cisco.com

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

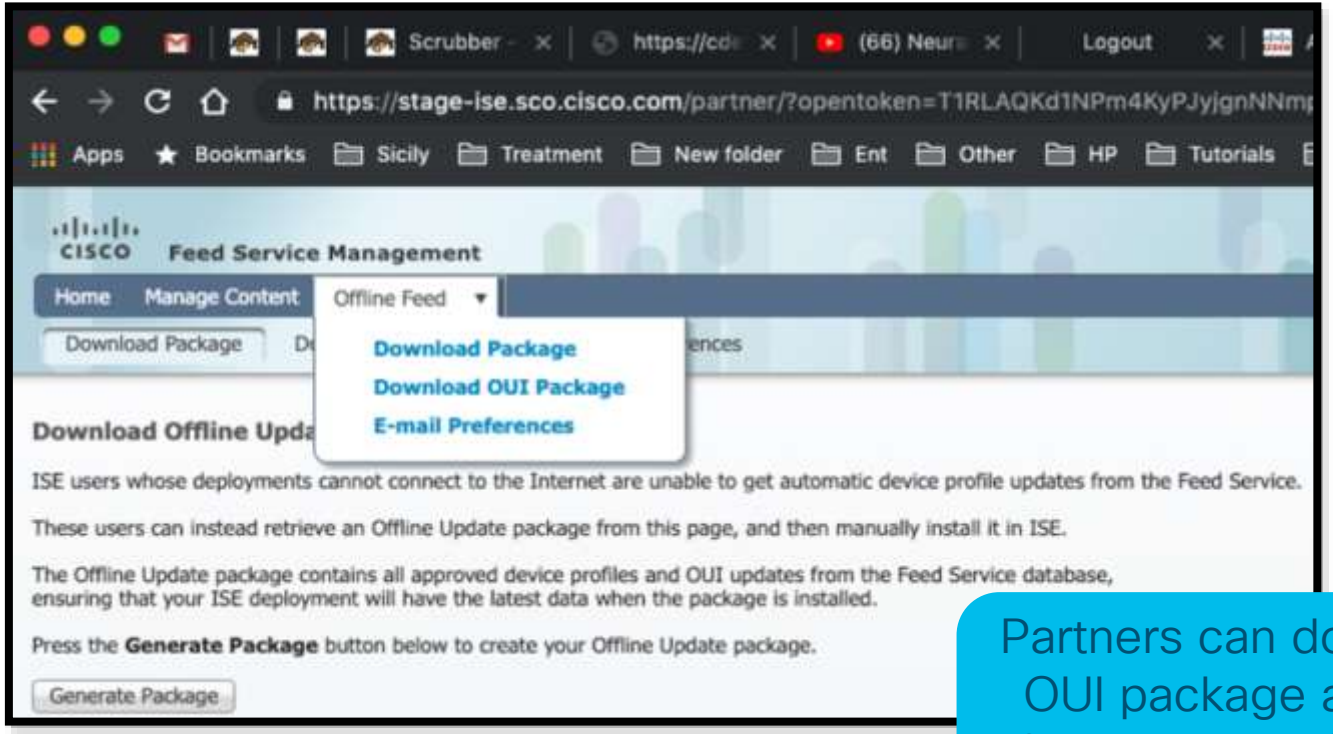
ISE Bill Of Materials Tool

http://ise-bom.cisco.com

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 2.7 Update

New Partner Portal- 2.7



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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplified Guest User Experience with 2.7

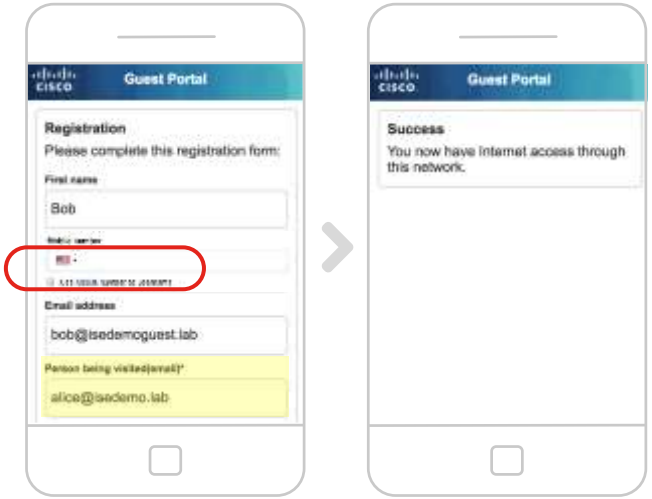
Auto-login on sponsor approval | Phone number as username

Problem

After self-registration, guest users need to wait for sponsor approval and credentials to be shared for gaining network access

Solution

Guest Auto Login feature in ISE 2.7 provides the ability for guests to log in automatically without credentials after sponsor approval.



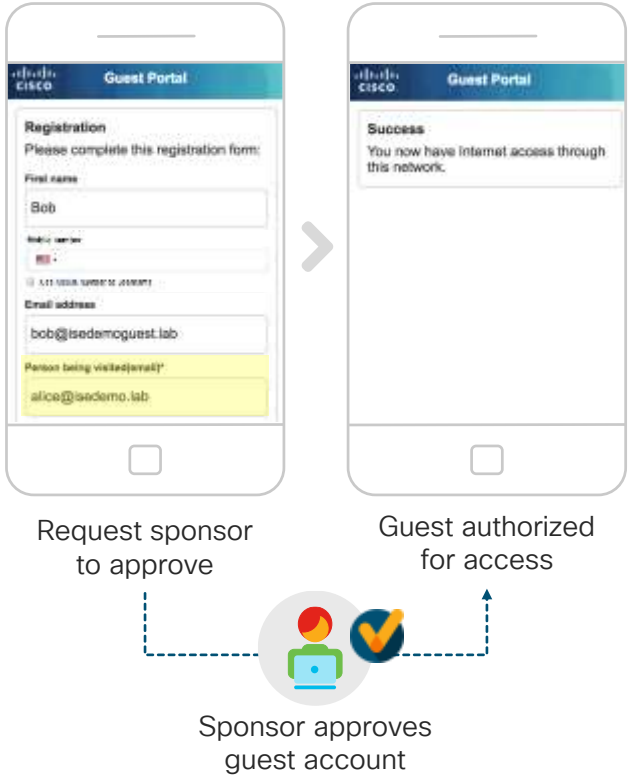
Request sponsor to approve

Guest authorized for access

Sponsor approves guest account

Simplified Guest User Experience with 2.7

- **Grace Access**
  You can grant 5 to 30 minutes of internet access to self-registered guests who are waiting for sponsor approval to your corporate network.
- **Guest Password Recovery**
  You can now enable the Reset Password option in the Guest portal for self-registered guests. Self-registered guests with valid guest account can use this option when they forget their password.
- **Phone Number as the Guest User Identifier**
  In addition to email address or username, guest users can now use their phone numbers as their user ID for guest access.
- **Secure SMTP**
  Guest email notifications can now be sent through a secure SMTP server



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TEAP Support

TEAP RFC 7170 is a standard for tunnelled EAP authentication method. It allows the following functionality:

- Performs a full TLS handshake to build the tunnel
- User/machine authentication during tunnel building or inside the tunnel via client certificate without running an inner method
- User/machine authentication in the inner method via username/password or certificate
- Supported inner methods are EAP-MSCHAPv2, EAP-TLS and Basic Password Authentication
- Multiple inner methods invocation (EAP Chaining)
- Crypto-Binding
- Channel-Binding
- Server-side state session resume
- Client-side state session resume (PAC)
- Transition from short handshake using PAC to full handshake in case of PAC is not valid
- Generating and providing user/machine certificate to the client
- Providing the list of trusted roots to the client

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TEAP Support –ISE Configuration

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Dictionaries | Conditions | Results

- Authentication
  - Allowed Protocols
- Authorization
- Profiling
- Posture
- Client Provisioning

EAP-TTLS Inner Methods

- [x] Allow PAP/ASCII
- [x] Allow CHAP
- [x] Allow MS-CHAPv1
- [x] Allow MS-CHAPv2
- [x] Allow EAP-MD5
- [x] Allow EAP-MS-CHAPv2
  - [x] Allow Password Change Retries 1 (Valid Range 0 to 3)
- [x] Allow TEAP

TEAP Inner Methods

- [x] Allow EAP-MS-CHAPv2
  - [x] Allow Password Change Retries 3 (Valid Range 0 to 3)
- [x] Allow EAP-TLS
  - [ ] Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- [x] Accept client certificate during tunnel establishment
- [ ] Request Basic Password Authentication
- [ ] Enable EAP Chaining

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

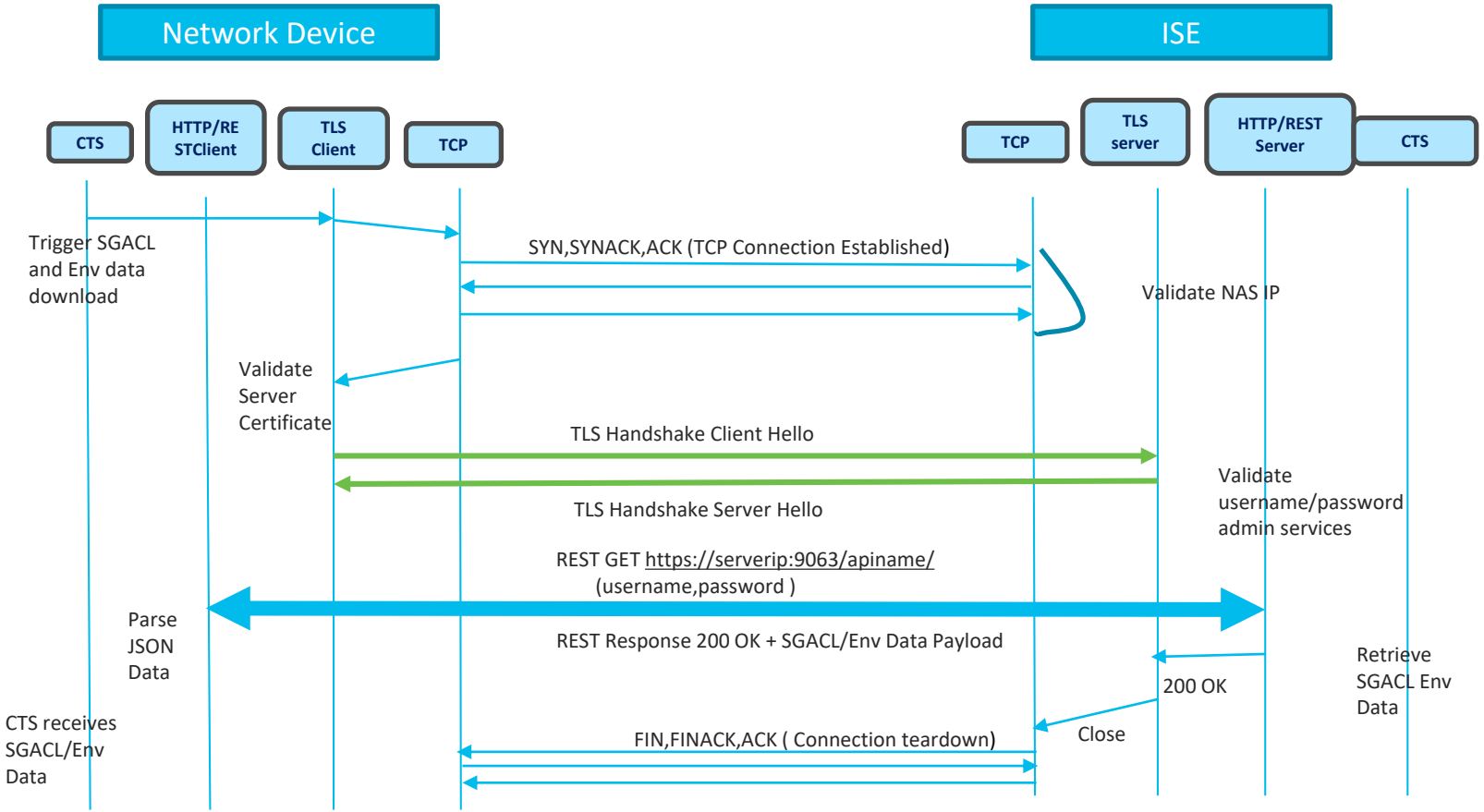
Streamlining Policy Downloads

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Streamlining Policy Downloads

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaway Points

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Please fill out the survey

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

CISCO

You make **possible**