You make **possible**

cisco

CCIE Security Techtorial

Zia Hussain
Ana Peric
Jay Young
Srilatha Vemula

TECCCIE-3202

cisco Live!

Barcelona | January 27-31, 2020

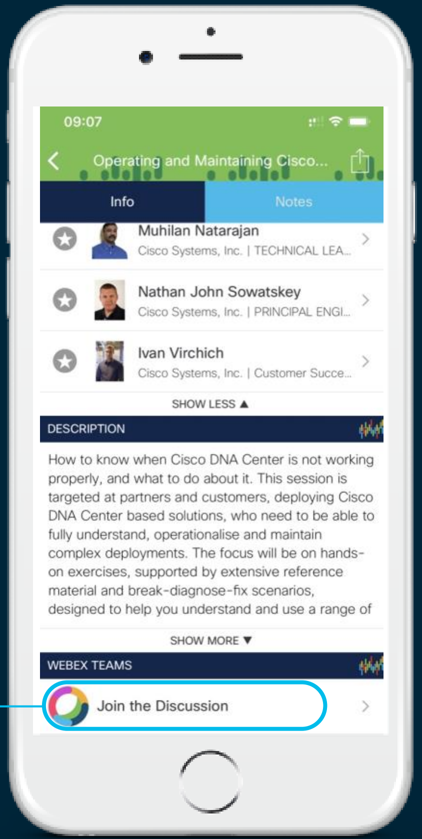
Cisco Webex Teams

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



Agenda

CCIE Certification	CCIE Journey CCIE Security v6 Certification Overview
Exam Preparation	Exam Blueprint Exam Preparation Strategy Exam Tips
Demos	From Blueprint Topics On Configuration and Troubleshooting Live and Recorded

CCIE Journey

Who?

Expert: In 75% topics of Blueprint
Experience: 4-5 years industry experience
Skills: Configure, Optimize and Troubleshoot

Why?

Personal Reasons: Multiple CCIEs, Peer Pressure…
Professional Reasons: Promotion, Job Mandated…

How?

Blueprint
Cisco Configuration Guides
Cisco Press Books
Cisco Live Sessions
Webinars
You Tubes

https://learningnetwork.cisco.com/docs/DOC-36542
https://www.cisco.com/content/dam/en_us/training-events/le31/le46/cln/marketing/learning-matrix/CCIE-Security-v6-Learning-Matrix.xlsx

Lab Exam Blueprint

Domains	Lab Weight Distribution
Perimeter Security and Intrusion Prevention	20 %
Secure Connectivity and Segmentation	20%
Infrastructure Security	15%
Identity Management, Information Exchange and Access Control	25%
Advanced Threat Protection and Content Security	20%

Exam Delivery

Design Module	LDS portal
Deploy-Operate-Optimize Module	LDS portal

Virtual Machines	Physical Devices	Access Types
ISE: 2.4 WSA: 9.2 ESA: 11.1 FMC: 6.2 NGIPS: 6.2 FTD: 6.2 ASA: 9.4(3) CSR1000: 15.5(3), 16.6.3 StealthWatch: 6.10 FireAMP Cloud: 5.3 WLC: 8.3 L2IOSv: 15.2 Win 10 Win Server 2016 Linux 4.17 AnyConnect 4.2	ASA5512: 9.2 ASA5516: 9.8 C3650: 16.6 C3850: 3.7 AP: AP1852: 8.3	Serial Port Terminal Server RDP VNC SSH GUI

Exam Format

Design Module	Deploy-Operate-Optimize Module
3 Hours	5 Hours
Duration not mandated	Duration not mandated
Clocked	Clocked
Backward navigation disabled	Backward navigation enabled
Marked with chapters	No chapters
Question points not shown	Question points shown
Partial scoring	Absolute scoring
Scenario based	Requirements-Symptoms based
Web-based items	Hands-on (majority) + Web-based items

Exam Scoring

Design Module | Minimum Score

DOO Module | Minimum Score

Need To Secure Each Minimum Score

Need To Secure Exam Cut Score

Pass Exam

60 % Deploy (Best effort)

40 % Operate-Optimize (Best effort)

Marks awarded only for working configuration.
Alternate solutions are acceptable if not violating any condition
Single dependency failure may cost multiple tasks.

Lab Tips

- Read lab and task guidelines
- Absorb the topology
- Read all the questions
- Attempt questions in sequence in DOO
- Avoid over verification
- Avoid enabling debugs
- Don’t change device console access
- If cannot solve the task then move on
- Verify all the tasks before you leave

Exam Pass Report

Simple report on meeting the exam cut score with no detail on per module performance.

Security Lab Exam Score Report

Congratulations on passing the CCIE Security Lab Exam!

- Within 12-16 weeks of passing the lab you will receive your CCIE certificate.
- You can download the CCIE logo for personal use by clicking on the CCIE/CCDE Logo Access tab.

- CCIE benefits and other useful information is available here
- If you have had a change of address recently, please update your data on the 'Profile' tab

Lab Score Card: Security

Candidate Name:	abc
Candidate ID:	12345678
Lab Date:	02-28-2020
Lab Site:	Brussels
CCIE Number:	12345

Exam Fail Report

Simple report on meeting modules minimum score but not meeting exam cut score with no detail on per module performance.

Lab Score Card: Security

Candidate Name:	abc
Candidate ID:	12345678
Lab Date:	02-28-2020
Lab Site:	Brussels
CCIE Number:	12345

Your score in all three sections met the respective minimum required score but unfortunately your total score did not meet the necessary overall cutscore. You must meet both conditions to pass the CCIE lab exam.

The report below shows your performance in each section for the CCIE Lab. Note that the performance measure is stated as a percentage of the total number of possible points not as the number of actual points scored.

Design: Met the minimum requirements

DOO: Met the minimum requirements

Overall Lab Requirement: Fail

Exam Fail Report

Lab Score Card: Security

Candidate Name:	abc
Candidate ID:	12345678
Lab Date:	02-20-2020
Lab Site:	San Jose
CCIE Number:	12345

Your score in all three sections met the respective minimum required score but unfortunate
the necessary overall cutscore. You must meet both conditions to pass the CCIE lab exam

The report below shows your performance in each section for the CCIE Lab. Note that the
as a percentage of the total number of possible points not as the number of actual points s

Comprehensive report on not meeting module minimum score with detail on per section performance in that module.

Design: Met the minimum requirements

DOO: FAIL

Section	Section Score
Perimeter Security and Intrusion Prevention	39%
Secure Connectivity and Segmentation	0%
Infrastructure Security	0%
Identity Management, Information Exchange and Access Control	0%
Advanced Threat Protection and Content Security	18%

Overall lab requirement: FAIL

cisco Live!

Introducing Cisco's new certification suite

Cisco Certifications – Announced June 2019

	Associate Level	Specialist Level	Professional Level	Expert Level
Engineering	CISCO CERTIFIED CCNA	CISCO CERTIFIED SPECIALIST	CISCO CERTIFIED CCNP	CISCO CERTIFIED CCIE
Software	CISCO CERTIFIED DEVNET Associate	CISCO CERTIFIED DEVNET SPECIALIST	CISCO CERTIFIED DEVNET Professional	CISCO CERTIFIED DEVNET Expert (Future Offering)

How our program is evolving

Associate Level	**Specialist** Level	**Professional** Level	**Expert** Level
CCNA One Exam	Specialist One Exam: Every written proctored exam (except CCNA) = Cisco Certified Specialist	CCNP Two Exams: 1 concentration exam and 1 technology core in any order, but from the same track	CCIE Lab Exam
DevNet Associate One Exam	DevNet Specialist One Exam: Every DevNet written, proctored exam (except Cisco Certified DevNet Associate) = Cisco Certified DevNet Specialist	DevNet Professional Two Exams: 1 DevNet core and 1 concentration exam in any order, but from the DevNet track	DevNet Expert Future offering

CCNP

Technology Core Exam	Concentration Exam
Enterprise	C C C C C
Security	C C C C C
Service Provider	C C C C C
Collaboration	C C C C C
Data Center	C C C C C

Automation and programmability cross functional course/exam option focused within technology track for CCNP certification

CCIE

Lab Exam
L L
L
L
L
L

1 technology core and 1 CCIE lab in same track

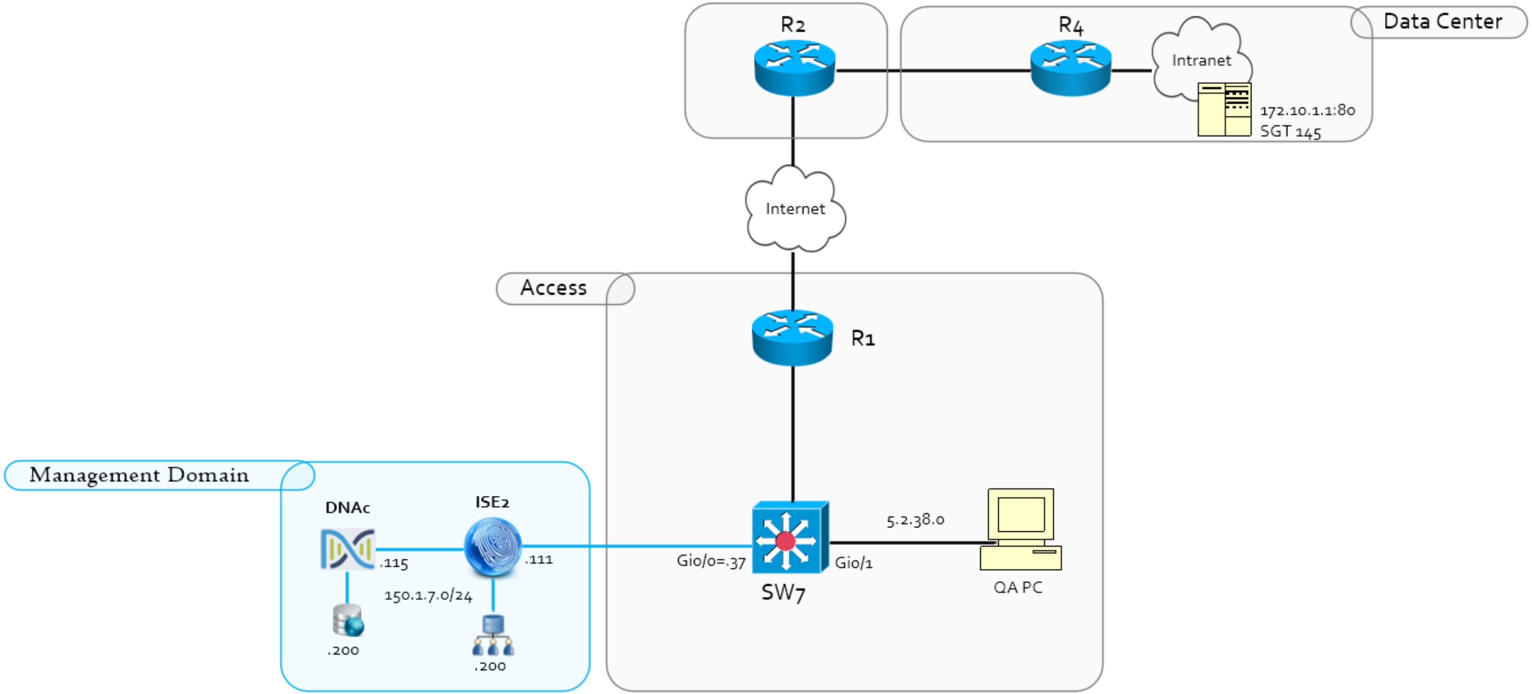
DevNet Professional

Technology Core exam	Concentration exam
DevNet	C C C C C C C C

Future Offering

Demo:
DNAc Policy Orchestration

Topology



R2
R4
Intranet
Data Center
172.10.1.1:80
SGT 145
Internet
Access
R1
Management Domain
DNAc
ISE2
.115
.111
150.1.7.0/24
.200
.200
Gi0/0=.37
Gi0/1
5.2.38.0
SW7
QA PC

Demo

Contact

- Email: zia@cisco.com

Thank you

Cisco Content Security in CCIE Security

Ana Peric, Technical Leader Engineering

TECCCIE-3202

Barcelona | January 27-31, 2020

Agenda

- Blueprint Relevance
- Introduction to Content Security
- Email Security Appliance (ESA) in CCIE Security
- Web Security Appliance (WSA) in CCIE Security
- Security Management Appliance (SMA) in CCIE Security

Introduction – About Me

Ana Perić

- Joined Cisco in 2012
- Based in Munich, Germany
- Technical Leader Engineering in NGENA BU / CPSG
- M.Sc.E.E (Diploma Engineer of Electrical Engineering and Computer Science), CCIE #39884 R&S
- Passionate about Security Automation, Penetration Testing, Sec DevOps, Web/Email Security, Cloud Technologies, and Innovation
- Proud aunt of five-year-old boy

For your reference symbol & Demo Links

- There is a content in your handouts that is not going to be presented in this session, but is important for further reference
- All the slides that are there for your reference are marked with:

- **All Demo Content:** https://cisco.box.com/s/rd3t7jvxsmr6awz7kvhtu8ydmqhr8wwk
- Password for shared content will be shared in **Webex Teams**

Blueprint Relevance

Blueprint Relevance

5.0 Advanced Threat Protection and Content Security	20%	Hide Details

5.1 AMP for networks, AMP for endpoints, and AMP for content security (ESA, and WSA)
5.2 Detect, analyze, and mitigate malware incidents
5.3 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN
5.4 DNS layer security, intelligent proxy, and user identification using Cisco Umbrella
5.5 Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA.
5.6 WCCP redirection on Cisco devices
5.7 Email security features

- 5.7.a Mail policies
- 5.7.b DLP
- 5.7.c Quarantine
- 5.7.d Authentication
- 5.7.e Encryption

5.8 HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella
5.9 SMA for centralized content security management
5.10 Cisco advanced threat solutions and their integration: Stealthwatch, FMC, AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella

Introduction to Content Security

Agenda

Introduction to Content Security

- Email Security Appliance (ESA)
  - Overview & Refresher
  - ESA pipeline
- Web Security Appliance (WSA)
  - Overview & Refresher
  - WSA Policies & Pipeline
- Security Management Appliance (SMA)
  - Overview & Refresher

Cisco Content Security Portfolio

KVM vmware

KVM vmware

Microsoft Hyper-V

KVM vmware

ESA

WSA

SMA

Cisco Content Security Portfolio

Email Security Gateway with variety of features and form-factors:

- **HW Appliances**:
  - C370, C670
  - C380, C680
  - C190,C390,C690
- **Virtual Appliances**: Vmware, KVM

Web Security Appliance (Gateway) with variety of features and form-factors:

- **HW Appliances**:
  - S170, S380, S680
  - S190, S390, S690
- **Virtual Appliances**: Vmware, KVM, Hyper-V

Security Management Appliance for ESA and WSA

- **HW Appliances**:
  - M380, M680
  - M190, M390, M690
- **Virtual Appliances**: Vmware, KVM

ESA

WSA

SMA

Talos - Cisco Threat Research and Intelligence

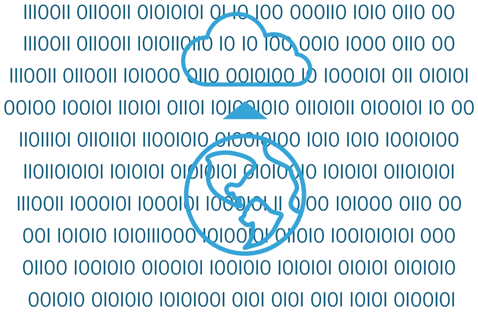
120 TB
Of Data Received Daily

1.5 MILLION
Daily Malware Samples

600 BILLION
Daily Email Messages

16 BILLION
Daily Web Requests

TALOS



24 • 7 • 365 Operations

250+
Full Time Threat Intel Researchers

1.6 MILLION
Telemetry Agents

3-5 minutes
Updates to all security devices

Over 100
Threat Intelligence Partners

Cisco Email Security Appliance (ESA) Overview & Pipeline

Cisco Email Security Appliance - Features

- Global Threat Intelligence (**Talos**)
- Reputation Filtering (by **Talos**)
- Anti-Spam
- Anti-Virus
- Threat Grid & AMP
- Graymail / Global Unsubscribe
- Forged Email Detection (FED)
- Virus Outbreak Filters (VOF)
- Data Loss Prevention (DLP)

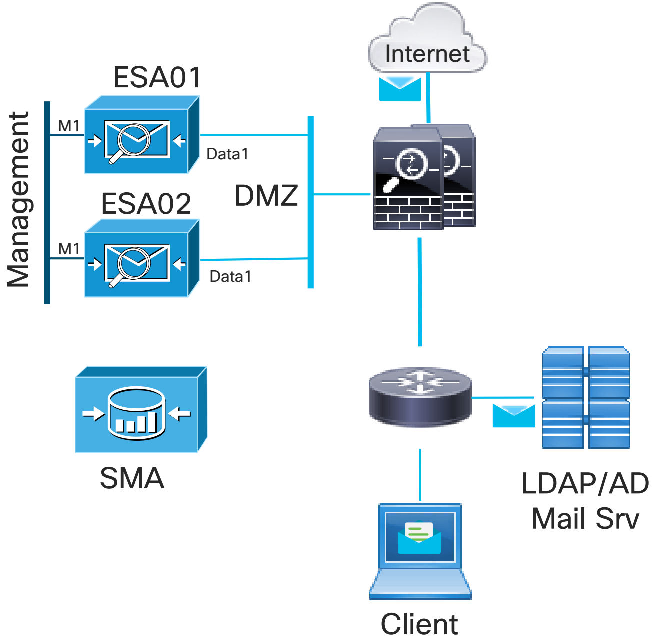
Cisco Email Security Appliance - Features

- Global Threat Intelligence (Talos)
- Reputation Filtering (powered by Cisco Talos Intelligence)
- Anti-Spam Engine
- Anti-Virus Engines (Sophos, McAfee)
- Cisco Threat Grid & Cisco AMP (Anti-Malware Protection)
- Graymail Detection
- Forged Email Detection (FED)
- Virus Outbreak Filters (VOF)
- Data Loss Prevention (DLP)

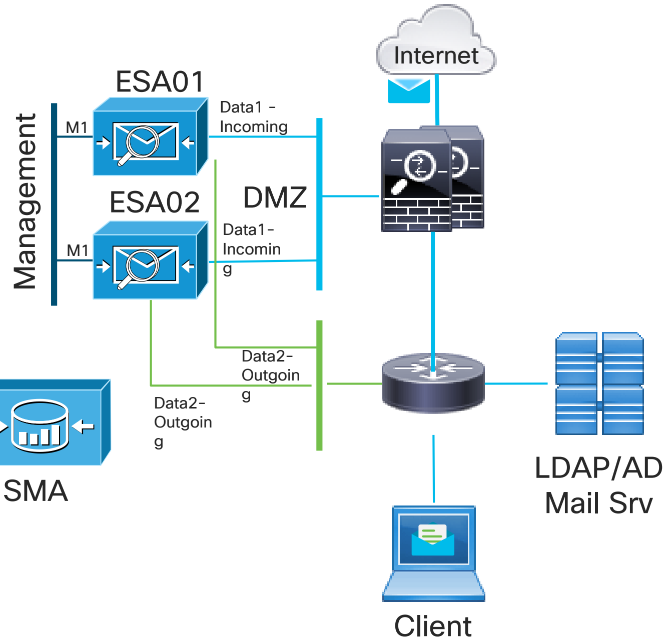
*https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.pdf

Typical ESA Design / Network Placement

Single Listener Design



Two Listeners Design



SMTP Protocol – Simple mail conversation

```
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-a.cisco.com ESMTP
HELO ccietest.com
250 alln-inbound-a.cisco.com
MAIL FROM:<ana@ccietest.com>
250 sender < ana@ccietest.com> ok
RCPT TO:<anperic@cisco.com>
250 recipient < anperic@cisco.com> ok
DATA
354 go ahead
Subject: This is CCIE Sec Test mail
From: Ana Peric <ana@ccietest.com>
To: Ana Peric(anperic) <anperic@cisco.com>

Body of the message, aloha CCIE!
.
250 ok:  Message 424242 accepted
QUIT
221 alln-inbound-a.cisco.com
Connection closed by foreign host.
```

Envelope

Body

Headers

Body

Envelope From, Mail From, RFC5321.MailFrom, Env Sender, etc.

Envelope To, Envelope Recipient, etc.

Header From, RFC5322.From, “Friendly From”, etc

Recipient, Header To, RFC5322.To, etc

Email Security Appliance Pipeline

SMTP SERVER

- Host Access Table (HAT)
- Received Header
- Default Domain
- Domain Map
- Recipient Access Table (RAT)
- Alias Table
- LDAP RCPT Accept
- SMTP Call-Ahead
- DKIM / SPF Verification
- DMARC Verification
- S/MIME Verification

WORKQUEUE

- LDAP RCPT Accept (WQ)
- Masquerading (Table / LDAP)
- LDAP Routing
- Message Filters

Per-Policy Scanning

- Anti-Spam
- Anti-Virus
- Advanced Malware (AMP)
- Graymail, Safe Unsubscribe
- Content Filtering
- Outbreak Filtering
- DLP Filtering (Outbound)

SMTP CLIENT

- Encryption
- Virtual Gateways
- Delivery Limits
- Received: Header
- Domain-Based Limits
- Domain-Based Routing
- Global Unsubscribe
- S/MIME Encryption
- DKIM Signing
- Bounce Profiles
- Message Delivery

ESA Configuration – CCIE Exam – Main Points

What you may be expect to configure?

Initial and Service Config (routing, listeners, DNS, LDAP/AD, LDAP queries	Mail filters & Mail Flow Policies	Outgoing Mail
Host Access Table (HAT) (one per listener)	Sender Groups & SBRS ranges, security (TLS), rate limiting, SPF/DKIM/DMARC verification	Outgoing Mail Policies (AS/AV/AMP/VOF/Content Filters)
Recipient Access Table (RAT) (per listener)	**Incoming Mail Policies** (AS/AV/AMP/Graymail/VOF/ Content Filters)	DLP, Encryption, DKIM Signing, etc.

ESA: Host Access Table Structure

- IPs and Hosts are evaluated in the **HAT/RAT** Top to Down, once there is a match, we break
- **SenderGroups** are containers that define the policy based on match
- Inclusion into a **SenderGroup** is defined by Reputation Score, DNS, or explicit match

Order	Sender Group	SenderBase™ Reputation Score (-10 -8 -6 -4 -2 0 2 4 6 8 +10)	Mail Flow Policy
1	RELAYLIST		RELAYED
2	WHITELIST		TRUSTED
3	BLACKLIST		BLOCKED
4	SUSPECTLIST		HEAVY_THROTTLE
5	GREYLIST		LIGHT_THROTTLE
6	UNKNOWNLIST		ACCEPTED
	ALL		ACCEPTED

Incoming Mail Policies - Example

Incoming Mail Policies

Success — The Advanced Malware Protection settings for policy "mp.vip.incoming" were submitted.

Find Policies

Email Address: [ ] (•) Recipient ( ) Sender [Find Policies]

Policies

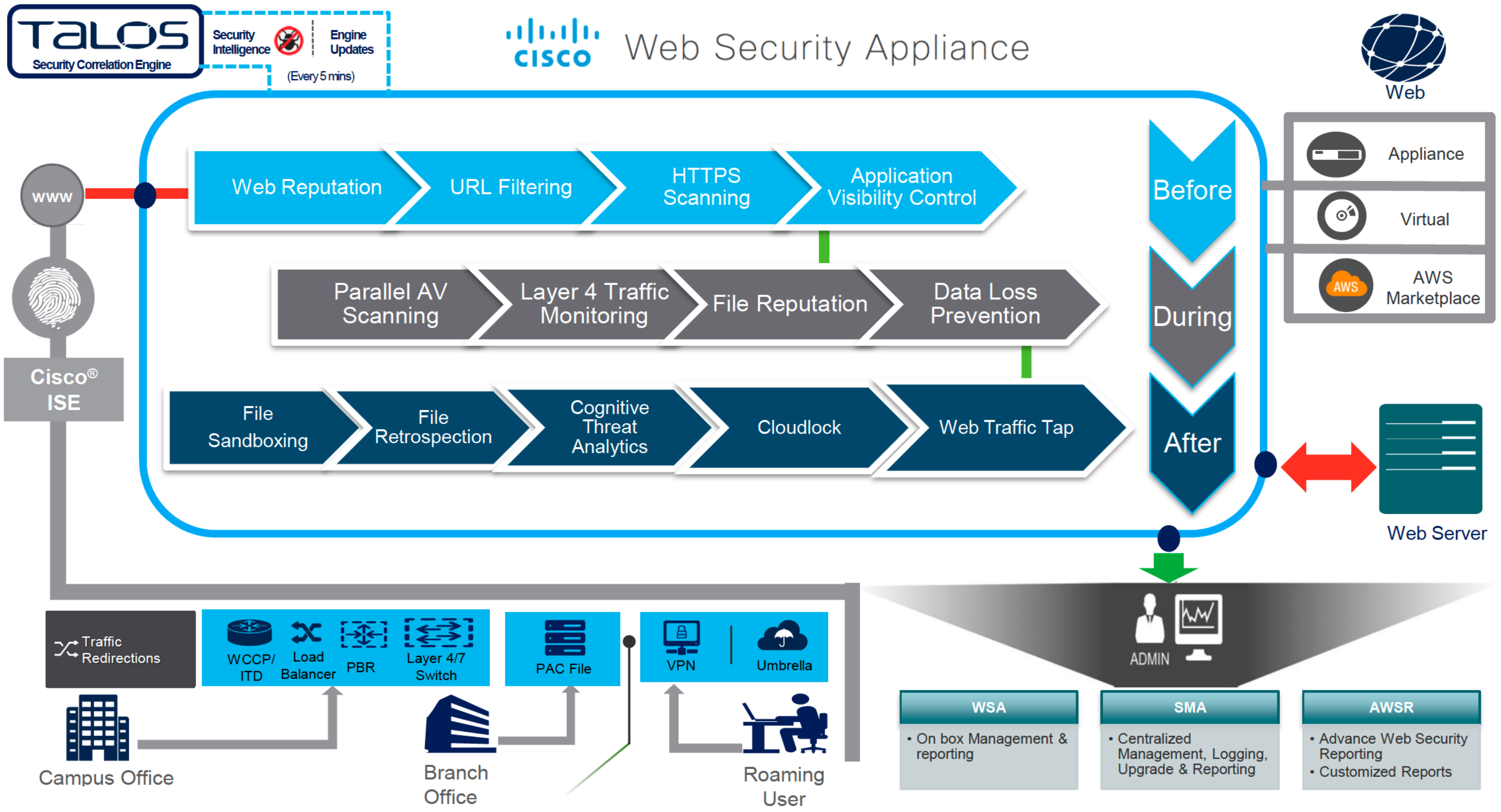
Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	mp.vip.incoming	IronPort Anti-Spam Positive: Quarantine Suspected: Deliver	Sophos Repaired: Deliver Encrypted: Deliver Unscannable: Quarantine Virus Positive: Drop ...	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Disabled	Disabled	Retention Time: Virus: 1 day	

Key: Default Custom Disabled

Cisco Web Security Appliance (WSA) Refresher and Pipeline

Web Security Appliance



Cisco Web Security Appliance – Features

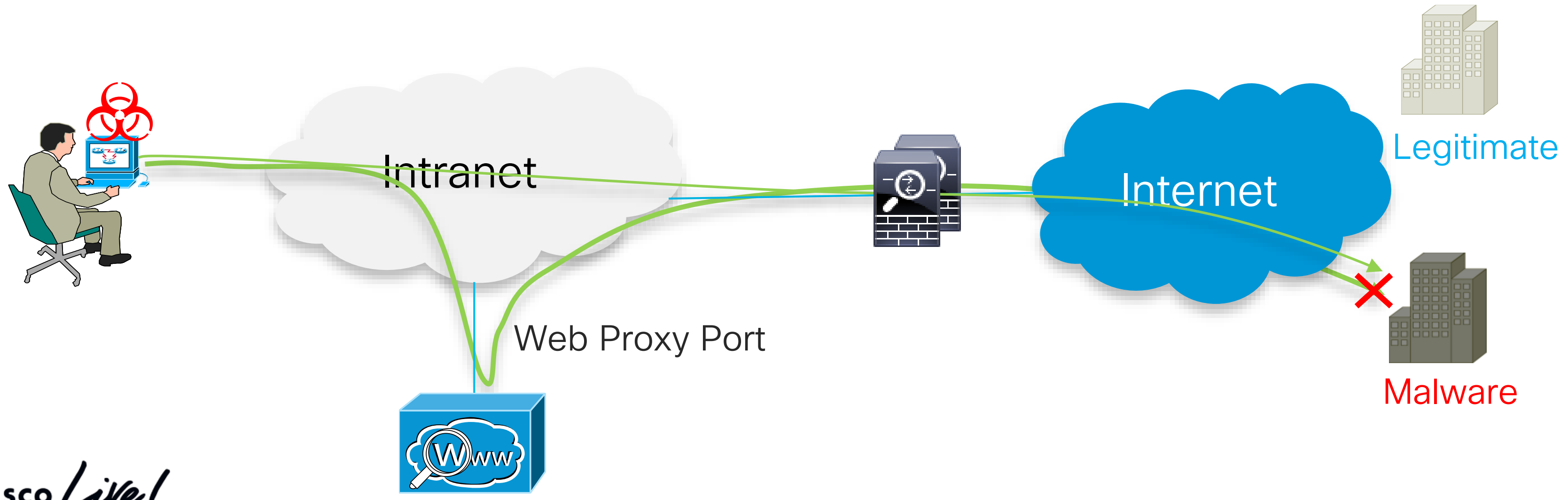
- Web Security Appliance = Web Security Gateway (on-prem, or in AWS)
- High performing HTTP/HTTPS/Native FTP/FTP over HTTP/SOCKS proxy
- Web Based Reputation (WBRS – powered by Talos)
- Anti-Malware
- Anti-Virus
- AMP
- Application Visibility and Control (AVC)
- URL Filtering (End-User Control)

Intercepting Browser Traffic

User browser requests to the internet must be redirected to the WSA web proxy port.

Deployment Methods:

- Explicit Mode
- Transparent Mode



WSA Deployment Options

Explicit Deployment

- Automatically detect settings (WPAD)
- PAC File (hosted on WSA)

Transparent Deployment

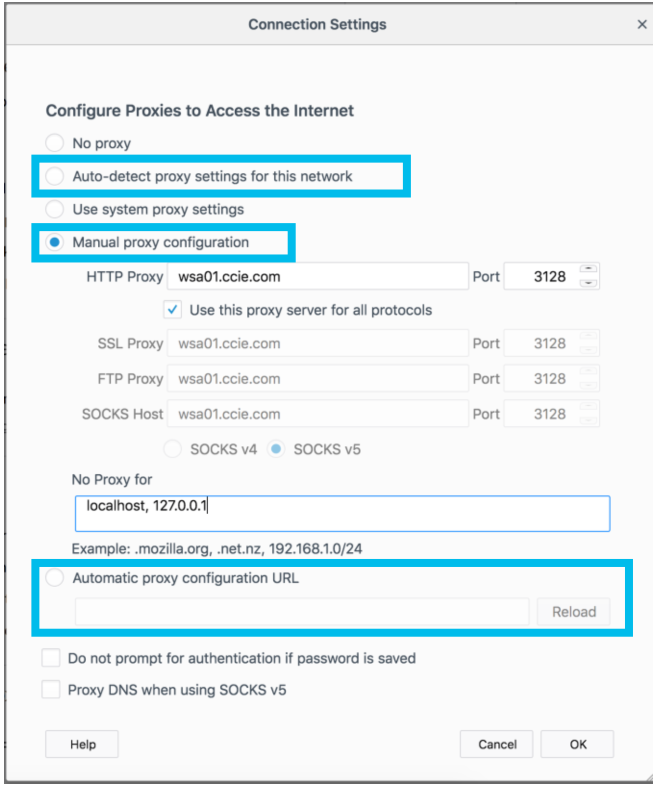
- WCCPv2 (Web Cache Communication Protocol) transparent redirection
- Policy-based Routing (PBR)
- L4/L7 Switch (L4-L7 redirection)

Transparent Mode Traffic Redirection

- Web Cache Control Protocol (WCCP)
  - Available on many switches, routers and firewalls (Cisco and non-Cisco)
  - Will be the redirection mechanism used in this course
  - Provides load-balancing capabilities inside the protocol logic
- Policy Based Routing (PBR)
  - Resource intensive for the router (performed in software)
  - Can be used to redirect to one WSA, or implement active-passive deployment
- Layer 4 Switch
  - Redirects traffic based on port numbers and IP addresses
  - Can do simple load balancing and failover
- Layer 7 Switch
  - Like Layer 4 switch, but can also redirect traffic based on URL
  - Can do sophisticated load balancing and failover

Explicit Forward Mode Configuration

- Three methods to configure a client (Web Browser):
  - Automatically Detect Settings – WPAD Protocol
  - Proxy Auto-Configuration (PAC) Files (host on WSA)
  - Enter the Address of a Proxy Server

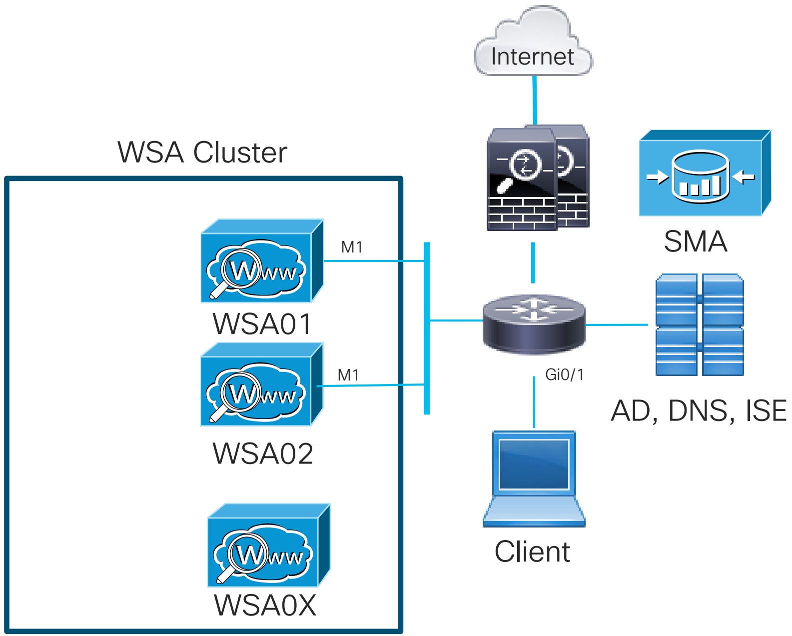


TIP

In Enterprise deployments Use Microsoft Group Policy Objects for central control of these IE settings

Deployment Options – One Interface-only (1)

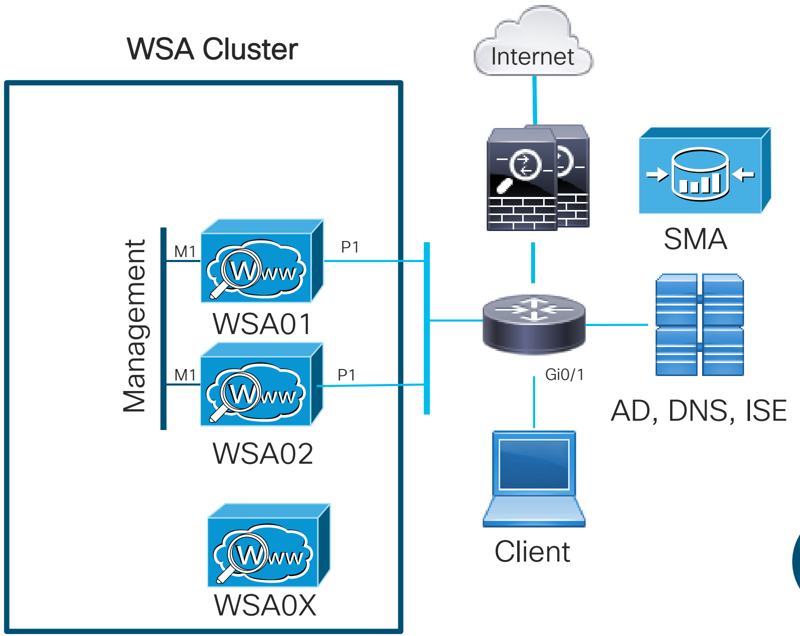
One Interface for both Management and Data traffic



- Applicable to:
    - Any deployment
- All traffic (Management and Proxy) handled via Management interface M1
- Most convenient for explicit deployments
- The easiest to configure and deploy
- **Less secure** (management is not out of bound)

Deployment Options (2)

One Leg Deployment – Separate Management and Data routing tables



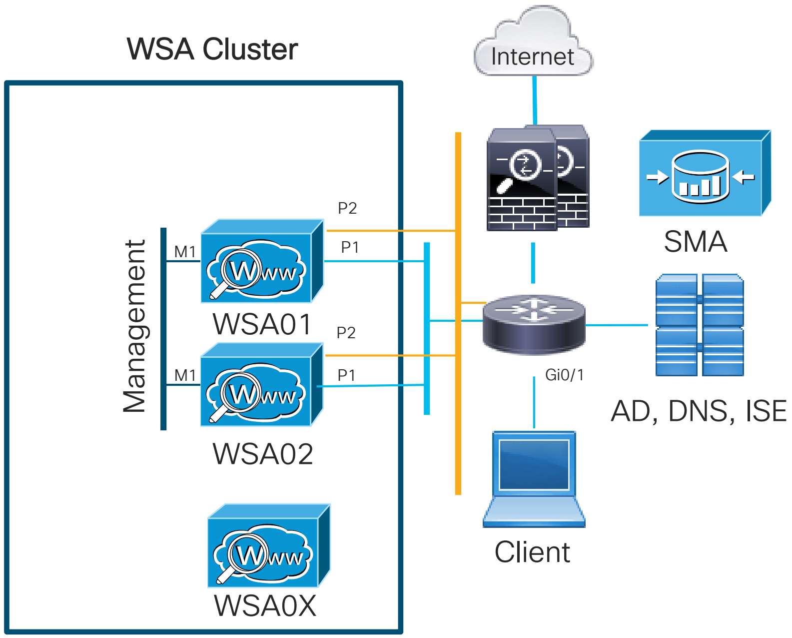
- Applicable to:
    - Any deployment (ex, transparent)
- Proxy traffic handled by P1
- Separated Management on M1
- More secure, clear routing separation

TIP

Services (DNS, updates, auth) by default use M1 routing table if not configured differently

Deployment Options (3)

Two-Leg Deployment – Separate Management and Data routing



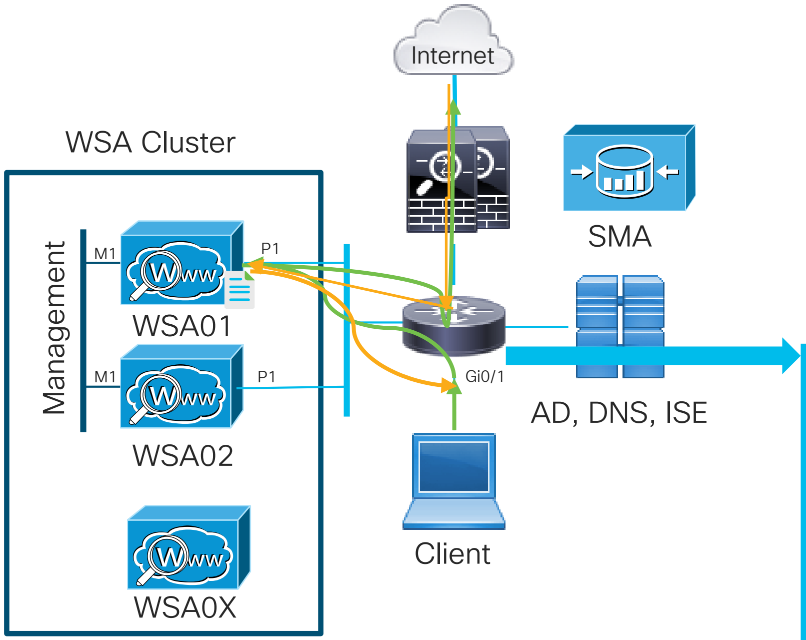
- Applicable to:
  - WCCP, PBR, Explicit
- Incoming traffic to P1 (LAN-facing)
- Outgoing traffic via P2 (Internet-facing)

TIP

P2 doesn't listen on proxy ports by default. If needed enable it via CLI: **`advancedproxyconfig`**

Transparent Deployment Example – WCCPv2

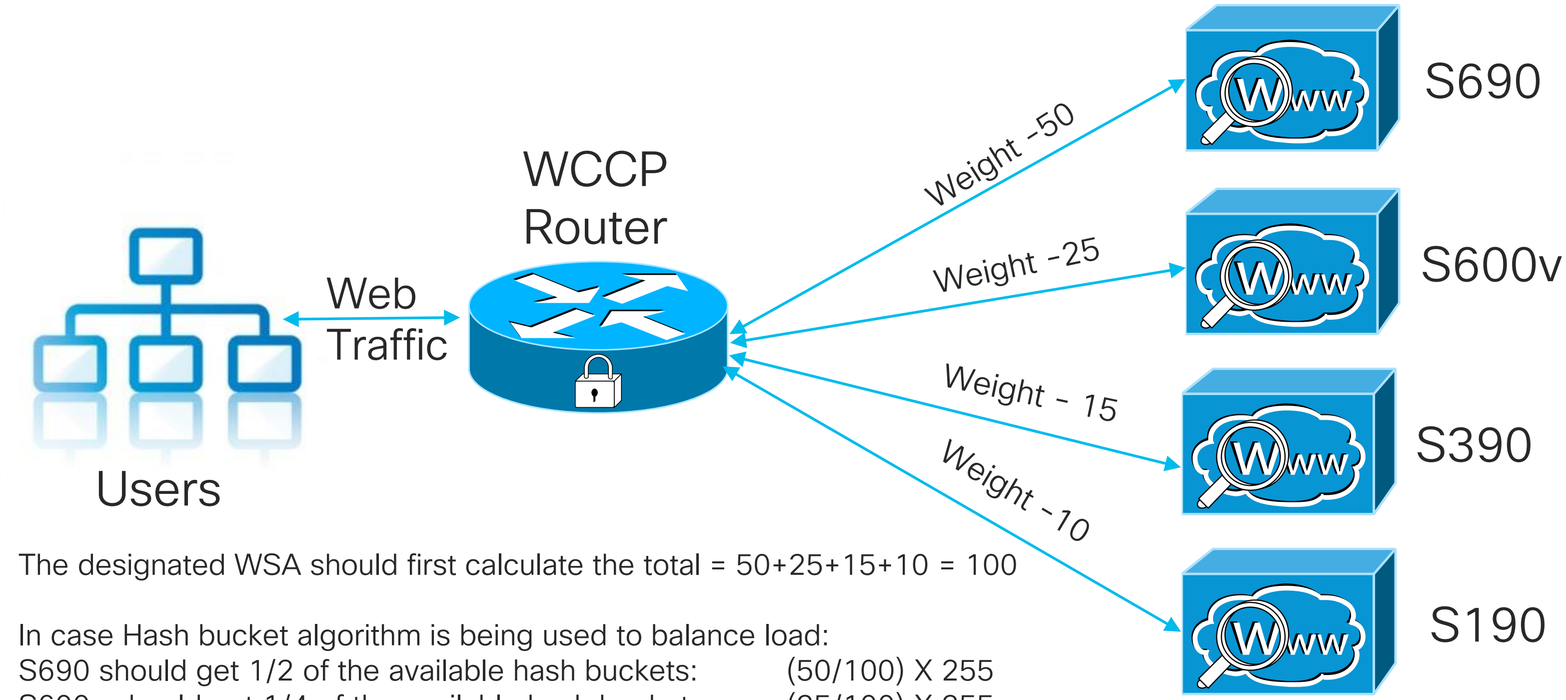
One-Leg Deployment – Separate Management and Data routing



- Design applicable to Explicit, WCCP, PBR, LB
- WCCP redirection & return: **GRE or L2**
- Hash/Mask Assignment

```
ip wccp 91 redirect-group WCCP-REDIRECT

interface gi0/1
ip wccp 91 redirect in
```

WCCP Weighted Load Balancing



The designated WSA should first calculate the total = 50+25+15+10 = 100

In case Hash bucket algorithm is being used to balance load:

S690 should get 1/2 of the available hash buckets:	(50/100) X 255
S600v should get 1/4 of the available hash buckets:	(25/100) X 255
S390 should get 15/100 of the available hash buckets:	(15/100) X 255
S190 should get 1/10 of the available hash buckets:	(10/100) X 255

Explicit Forward Mode vs. Transparent Mode Summary

- Explicit Mode
- Client directs traffic to proxy server
- Requires no network infrastructure to redirect client request
- Proxy resolves hostname of target web server
- Authentication is straight-forward
- Client config must change (several options available)

- Transparent Mode
- Client directs traffic to target web server
- Network infrastructure (such as WCCP) redirects client request to proxy server
- Client resolves hostname of target web-server
- Authentication can be problematic

WSA Policy Types – Refresher

- Identification Policy (Who? / How? / How do we recognize/categorize the end-user?)
- Access Policy (Actions for HTTP / HTTPS decrypted traffic)
- Decryption Policy (HTTPS traffic handling / what do we decrypt?)
- Routing Policy (Upstream Proxy Handling)
- **Outbound Malware Policy** (Do we permit upload of Malware content)
- **Data Security Policy** (What content type can we upload)
- **Other Policy Types**: SaaS/SOCKS Policies/WTT

Web Security Appliance Pipeline for HTTP/S

HTTP Client Request

- Proxy Bypass List
- Identification Profiles (Who?)
- WBRS Score Calculation
- Authentication Authorization Guest Access?

Per Policy Matching

- Protocols/User-Agent
- Custom URL Category Match
- Pre-Defined URL Category
- AVC
- Objects
- MIME File-Type Filter
- Anti-Virus/Anti-Malware Scanning

HTTPS Client Request

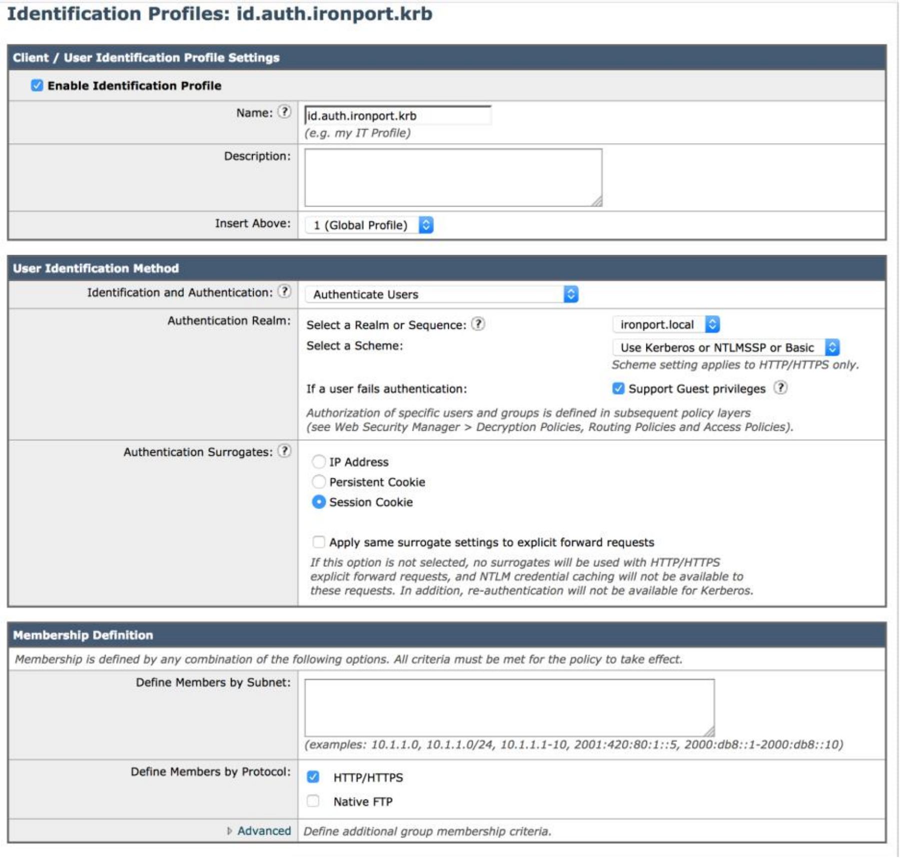
- Proxy Bypass List
- Identification Profiles (Who?)
- Custom URL Category Match
- WBRS Score Calculation
- Authentication Authorization Guest Access?

Per Policy Matching

- Decryption
- Pre-Defined URL Category
- AVC
- Objects
- MIME File-Type Filter
- Anti-Virus/Anti-Malware Scanning
- Encryption

Identification Policy - Refresher

- Answers the question: “WHO”
- Matches Source traffic by different criteria:
  - IP/Subnet/IPv6, or protocol/port
  - Custom/Pre-defined URL cat
  - User-Agent
  - Authentication Method (enforces authentication)



Access Policy - Refresher

Defines & Enforces Corporate Web Security Policy for **HTTP** and **Decrypted HTTPS traffic**

Access Policies

Policies							
Add Policy...							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	**ap.auth.ironport** Identification Profile: id.auth.ironport.krb All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 86	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	
Edit Policy Order...							

HTTPS Decryption – Refresher (1)

- WSA can decrypt HTTPS traffic by acting like “Man-in-the-Middle”
- For security reasons, try to use SSL key size that is > 1024 bits
- HTTPS decryption is controlled in:
  - **Global Setting**: HTTPS Proxy Configuration (Security Services -> HTTPS Proxy)
  - **Per-Policy configuration**: Web Security Manager -> Decryption Policies

Decryption Policies

Policies

Add Policy...

Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	**dp.subnet10** Identification Profile: id.subnet10 All identified users	Pass Through: 1 Monitor: 61 Decrypt: 4 Drop: 13	(global policy)	(global policy)	
	Global Policy Identification Profile: All	Monitor: 79	Enabled	Decrypt	

HTTPS Proxy

HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Generated Certificate: Common name: heka.ironport.local Organization: CC Organizational Unit: IronPort Country: DE Expiration Date: Nov 19 21:20:36 2020 GMT Basic Constraints: Not Critical
Decryption Options	
Decrypt for Authentication:	Enabled
Decrypt for End-User Notification:	Enabled
Decrypt for End-User Acknowledgement:	Enabled
Decrypt for Application Detection:	Disabled
Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Monitor Mismatched Hostname: Monitor Unrecognized Root Authority / Issuer Drop Invalid Signing Certificate Drop Invalid Leaf Certificate Drop All other error types: Drop
Online Certificate Status Protocol Options	
OCSP Result Handling:	Revoked Certificate: Drop Unknown Certificate: Monitor OCSP Error: Monitor

HTTPS Decryption – Refresher (2)

Decryption Policy Actions

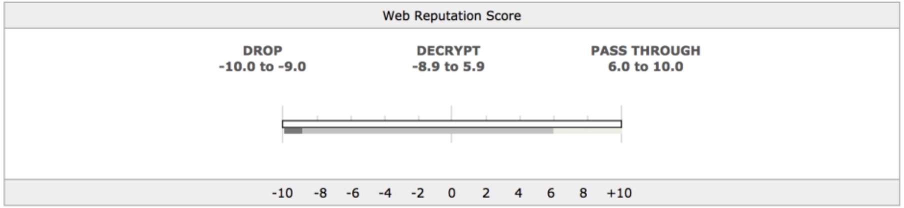
- Drop – traffic is dropped / HTTPS connection Terminated
  - Note: In transparent deployment NO End-User Notification is displayed for dropped connection
- Decrypt: Traffic is decrypted, and further matching access policy is used to determine further behavior
- Pass-Through: HTTPS connection will not be intercepted – end-user communicates with destination HTTPS server directly w/o additional scanning
- Monitor – this is NOT an final action, means that we only continue further checks down the pipeline

Decryption Policy Considerations – in more details

- Decrypt only traffic needed by Company Security Policy & Rely on WBRS!
- What do I need to decrypt, and what not?
  - Decrypt only categories that would need further fine-grained control / access policy processing / Referrer Exemption & AV/AM scanning
  - Decrypt for:
    - Authentication
    - End-User-Notification display
    - End-User-Acknowledgements display
  - Pass-through traffic that might be confidential (i.e Financial / Banking sites)
  - Drop the traffic that would have action Block by the corresponding Access Policy
  - Drop Categories matching: Illegal, forbidden, and business inappropriate content

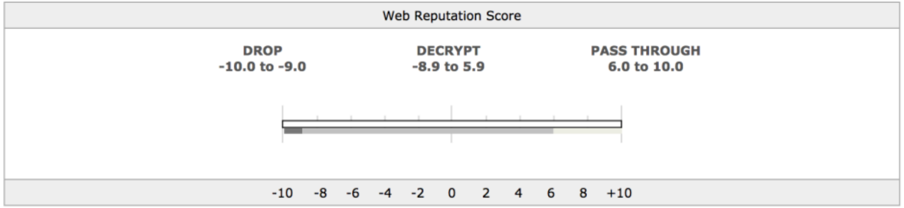
HTTPS & WBRS – How do dots connect?

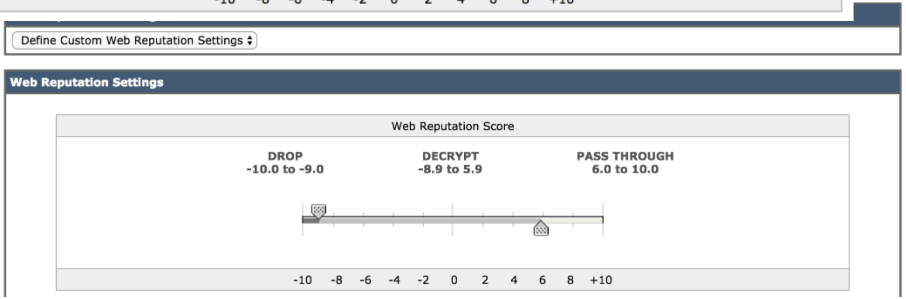
- Unless explicitly specified by Custom or Pre-defined URL category, action will be determined by WBRS score (if WBRS is enabled)



HTTPS & WBRS – How do dots connect?

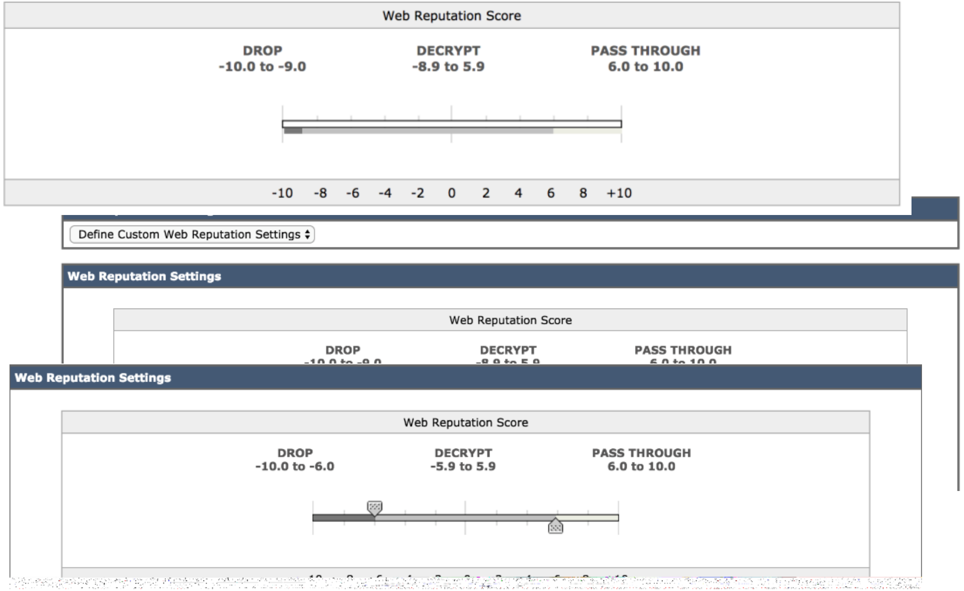
- Unless explicitly specified by Custom or Pre-defined URL category, action will be determined by WBRS score (if WBRS is enabled)
- One can choose default (less aggressive)





HTTPS & WBRS – How do dots connect?

- Unless explicitly specified by Custom or Pre-defined URL category, action will be determined by WBRS score (if WBRS is enabled)
- One can choose default (less aggressive)
- Custom WBRS decryption – more aggressive values setup



WSA Configuration – CCIE Exam – Main Points

What you may be expect to configure?

Different deployment methods: explicit, transparent mode / one-leg / two-leg / unified/separate routing

Initial Setup

- Networking / Routing
- DNS, alerts, logging, default policy setup
- Enabled Services (Web Usage Control, Anti-Virus/Malware Scannaers, AMP, etc)

Custom URL Category creation (local/remote)

Identification & Access Policies – URL filtering, AVC, Objects, AV/AM

HTTPS Decryption & Policies

Advanced topics

Upstream proxies, routing, outbound malware policies, Secure mobility, etc.

Cisco Security Management Appliance (SMA) Refresher

Security Management Appliance (SMA)

- SMA for Web Security
- Centralized Configuration Management
- Centralized Web Tracking
- Centralized Web Reporting

- SMA for Email Security
- Centralized Spam Quarantine
- Centralized Message Tracking
- Centralized Email Reporting

SMA Configuration – CCIE Exam – Main Points

What you may be expect to configure?

- Initial SMA Configuration: Networking, DNS, interfaces, routing
- Configure WSA centralized Services
- Configure ESA centralized Services
- Add ESA/WSA devices to SMA configuration
- Initialize Web Configuration Managers / Deploy WSA configuration to multiple WSA devices
- Configure Centralized SPAM Quarantine

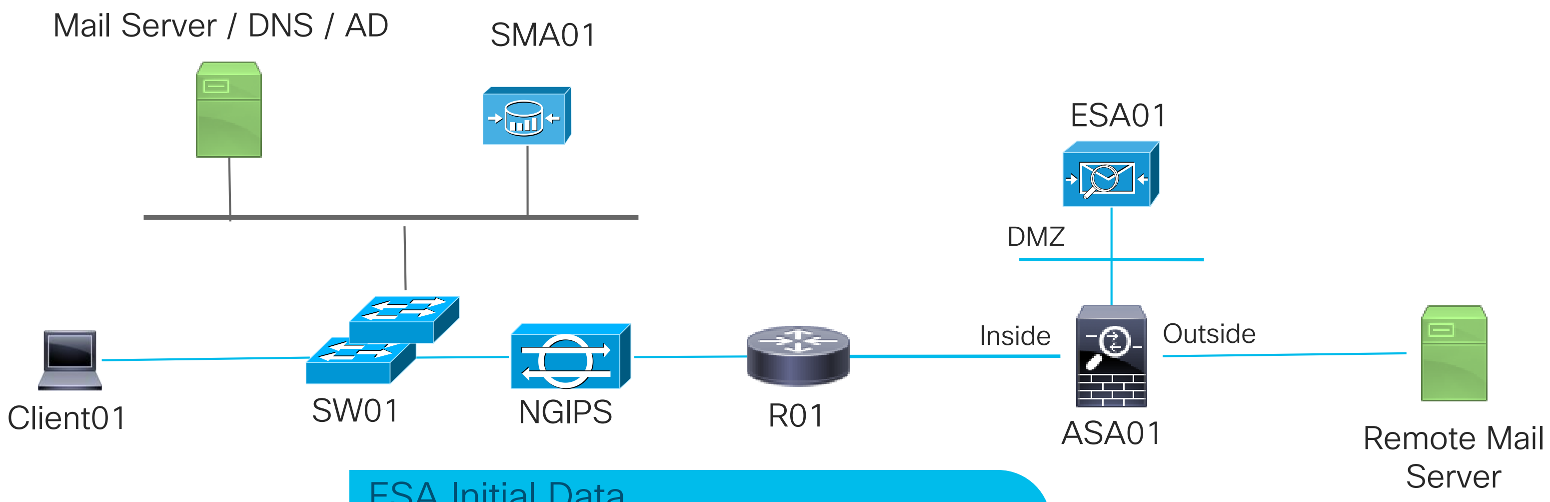
Email Security Appliance (ESA) in CCIE Security

Configuration and Troubleshooting Case Study

cisco Live!

ESA Configuration Case Study

ESA Configuration Topology



ESA Initial Data

Initial Credentials: admin/ironport
Hostname: esa01.ironport.local
Management: 10.48.63.21/26
DG: 10.48.63.1
DNS/AD/MailServer: 10.48.78.19
Domain: ironport.local
SMA IP: 10.48.78.56

ESA Configuration Task 1/2

- Perform Initial Configuration of **ESA01** device on Topology Diagram
  - All the relevant details are on diagram
  - Use credentials admin/CiscoCCIE2018!
- Configure Incoming Mail Listener with name: **IncomingMailListener**
- Configure ESA01 to accept emails for domain: @ironport.local
- Make sure ESA01 is not configured as an **Open Relay**
- Perform **TCP Reset** on connections with known bad reputation score
- Limit number of recipients to 10 per email message for all the messages that are hitting **ACCEPTED** Mail Flow Policy in Host Access Table

Configuration Steps 1/2

- 1. Run Setup Wizard with given parameters (Initial Setup):
  GUI > System Administration > System Setup Wizard
- 2. Configure Listener using default Values and name IncomingMailListener
  GUI > Network > Listeners
- 3-4. RAT Configuration - Allowed domain ironport.local
  GUI > Mail Policies > Recipient Access Table (RAT)
- 5. HAT Configuration - Modify BLOCKED Mail Flow Policy behavior
  GUI > Mail Policies > Mail Flow Policies > BLOCKED
- 6. HAT Configuration – Modify ACCEPTED Mail Flow Policy
  GUI > Mail Policies > Mail Flow Policies > ACCEPTED

ESA Configuration Task 2/2 (Bonus)

Incoming Mail Policy Configuration

- If recipient of email is ccie@ironport.local override default incoming mail settings in such a way that:
  - All SPAM messages are Dropped
  - All **Suspected SPAM** Messages are delivered with special subject prepended to the message [SUSPECTED SPAM - CCIE], and with additional custom header X-MaybeSpam-MaybeNot
  - **Drop** all Positive Virus detections
  - If message can't be scanned by Anti Virus scanner, send it to quarantine
  - All other incoming email policy for this user should be the same as in Default Policy

Configuration Steps 2/2

- Create new Incoming Mail Flow Policy
  - UI > Mail Policies > Incoming Mail Policies > Add Policy
- Add User:
  - Sender: Any
  - Recipients: ccie@ironport.local
- Modify Anti Spam settings of new Incoming Mail Policy
- Modify Anti Virus settings of new Incoming Mail Policy
- Commit the changes

Verification

- SSH to CLI of ESA01 using admin account
- Send mail using telnet to IncomingMail listener's IP address

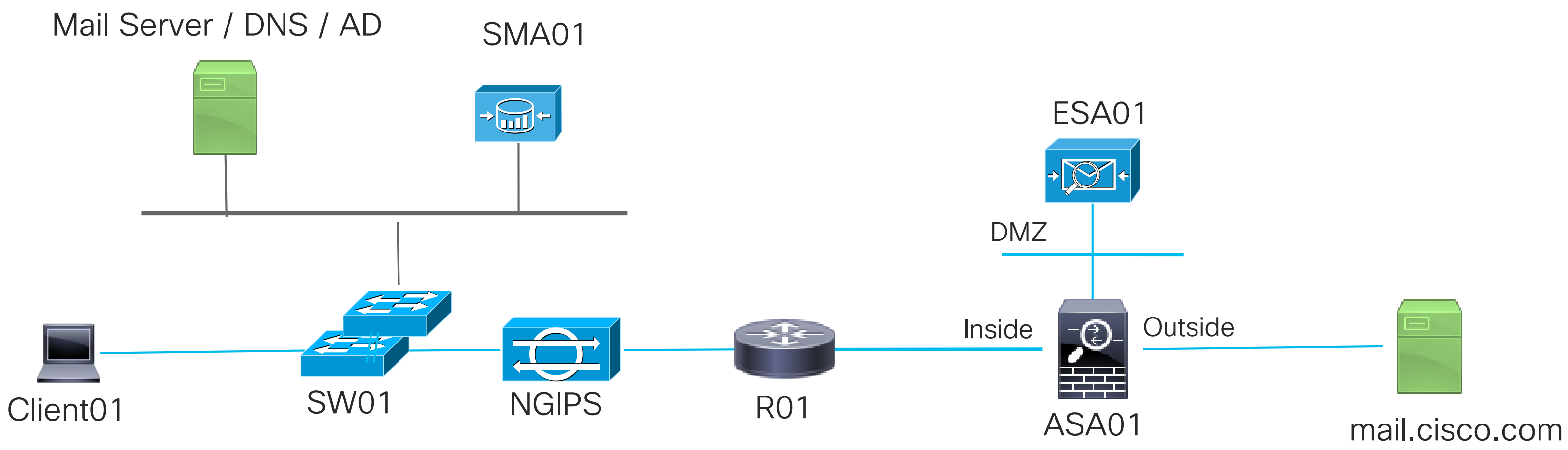
```
mail from:<anperic@cisco.com>
rcpt to: ccie@ironport.local
DATA
  Whatever you want to send is fine, hello Barcelona!
  .
```

  - Check the MID (Message ID) in ESA01's mail_logs to verify you hit the correct Incoming Mail Policy

ESA Configuration Case Study Demo

ESA Troubleshooting Case Study

ESA Troubleshooting Topology



ESA Initial Data

Initial Credentials: admin/ironport
Data1: 10.48.63.21/26
DG: 10.48.63.1
DNS/AD/MailServer: 10.48.78.19
Domain: ironport.local
SMA IP: 10.48.78.56

ESA Troubleshooting Task (2 Issues)

- Client01 opened a ticket that email sent to him on his email address ccie@ironport.local from email address test@cisco.com was sent by the sender, but never received by Client01 user
- Please resolve the ticket, and verify the solution by imitating outside connection to ESA01 by using ESA01 SSH access and telnet command
- Note:
  - *If configuration changes are needed on ESA, make those changes in the later stages of the email pipeline.
  - No new policies should be added

Checks

- Always check mail_logs – the most important logs on ESA!
- Verify email ever came from the sender:

```
grep test@cisco.com mail_logs
```

- Did mail come from that email?
- What happened with a connection (grep ICID in mail_logs)
- What happened with destination connection (grep DCID in mail_logs)
- If the mail didn't even come to ESA01, is it blocked by some other device (FW/IPS)?

Verification

- SSH to CLI of ESA01 using admin account
- Send mail using telnet to **IncomingMail** listener's IP address

```
mail from:<test@cisco.com>
rcpt to:<ccie@ironport.local>
DATA
Yet another email for testing.
.
```

- Check the MID (Message ID) in ESA01's mail_logs to verify you hit the correct Incoming Mail Policy, and verify it's not blocked any more

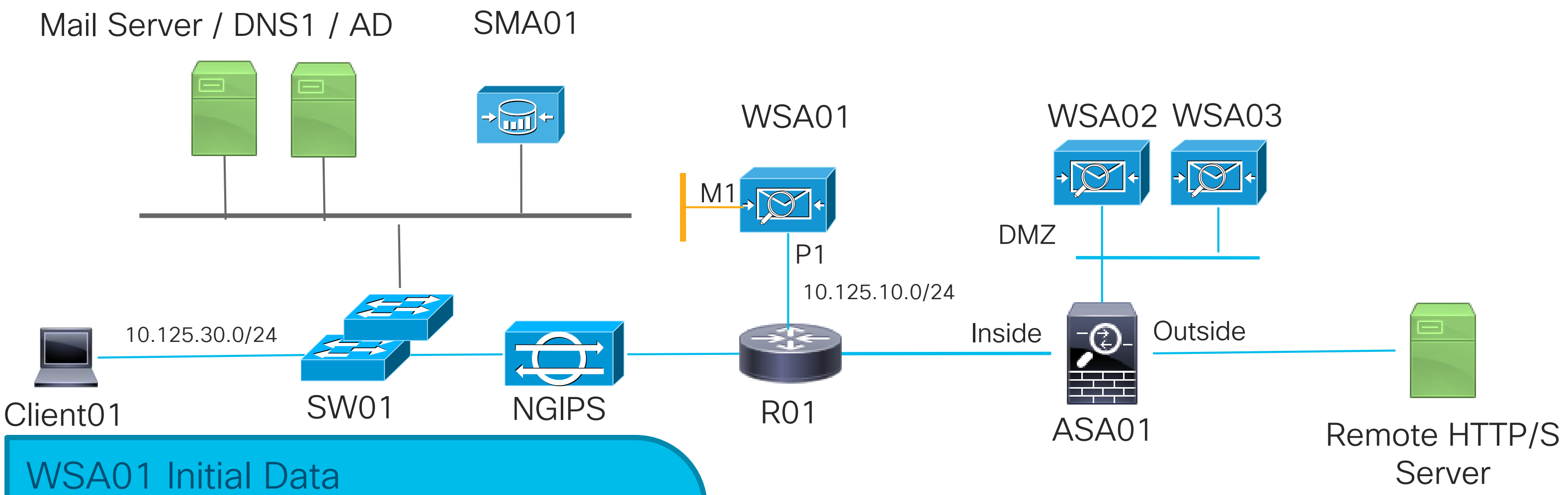
ESA Troubleshooting Case Study Demo

Web Security Appliance (WSA) in CCIE Security

Configuration and Troubleshooting Case Study

WSA Configuration Case Study

WSA Configuration Topology



WSA01 Initial Data
Hostname: **wsa01.ironport.local**
Initial Credentials: admin/ironport
M1: 10.255.0.42/24, DG: 10.255.0.1/24
P1: 10.125.10.10/24, DG: 10.125.10.1/24
DNS1/AD: 10.48.78.19
DNS2: 10.48.78.31
Domain: ironport.local
SMA IP: 10.48.78.56
Client: 10.125.30.30

Topology Considerations

DMZ WSA02 and WSA03 are already pre-configured
Authentication realm ironport.local is already created and functional on WSA01

WSA Configuration Task 1 – Initial Setup

- Initialize WSA01 in such a way that it has out-of-band-management, IP addressing as shown in topology diagram
- Configure transparent redirection on WSA01 and R01
  - Service Group 91
  - HTTP / HTTPS interesting traffic
  - GRE redirection & return method
- Configure DNS1 and DNS2 in such a way that request will be sent in round-robin fashion

WSA Configuration Steps – Task1

- Run Setup Wizard with given parameters (Initial Setup):
  - GUI > System Administration > System Setup Wizard
- Configure WCCP Service on WSA01 & R01
  - GUI > Network > Transparent Redirection
  - R01 CLI WCCP config
- DNS Configuration
  - GUI > Network > DNS (configure same DNS weights for 2 servers)
- commit the changes

WSA Configuration Task 2 – Policy Configuration

- All the users in subnet 10.0.0.0/8 should be authenticated, except destinations to cisco.com and all subdomains of cisco.com domain (where no authentication will be used).

- Insecure proxy authentication methods should not be allowed

- HTTP and decrypted HTTPS policy should be blocking Social Media categories for traffic in default case

WSA Configuration Steps – Task 2

- Create Identity id.auth, that will match:
  - Subnet 10.0.0.0/8
  - Enforce Authentication: NTLMSSP only (not using fallback to Basic Auth)
  - GUI > Web Security Manager > Identification Profiles
- Create custom URL category cat.noauth to match:
  - cisco.com & .cisco.com
- Create Identity id.no.auth that will be exemption from authentication based on category cat.noauth avoid authentication
  - Place id.noauth ABOVE id.auth
- Create Access Policy ap.noauth to match id.noauth
- Create Access Policy ap.auth to match id.auth & commit the changes

Verification - Task 2

- Generate HTTP request to www.ciscolive.com from subnet 10.0.0.0/8, authenticate using credentials ccie/CCIECLEUR2019!
- Verify accesslogs on WSA, and that access was granted
- Verify that request matched **id.auth** and **ap.auth**
- Generate HTTP request to www.cisco.com using computer from subnet 10.0.0.0/8.
  - Accesslogs should show that there is no authentication and we are using **id.noauth** & ap.noauth

WSA Configuration Task 3
Bonus Upstream Proxy Configuration

- Users from subnet **10.125.30.0/24** should be using upstream proxy farm called "**upstreamccie01**", with following details:
  1. Upstream proxies IPs are on the diagram (WSA02, WSA03)
  2. Failover method to be used: active/passive
  3. Failover from primary WSA02 to secondary WSA03 should happen only after 3 unsuccessful reconnection attempts

WSA Configuration Steps – Task 3

1. Create upstream proxy group upstreamccie01
   - GUI > Network > Upstream Proxy > Add a Group
   - Add WSA02, WSA03 into Upstream Prox Group
   - For WSA02, configure “Reconnection Attempts”: 3
   - Load Balancing: None (Failover)
2. Configure Routing Policy

- GUI > Web Security Manager > Routing Policies
- Match 10.125.30.0/24 (directly or by identity) and use upstreamccie01 upstream proxy group

3. commit the changes

Verification – Task 3

- Generate HTTP request to www.ciscolive.com from subnet 10.125.30.0/24 using curl
- Verify accesslogs on WSA, and that access was granted
- Verify using accesslogs that request matched routing policy and was sent to upstream proxy

WSA Configuration Case Study Demo

R01 WCCP configuration (1)

Step1: WCCP Interest list WCCP-REDIRECT

TIP

If you use authentication & transparent WCCP redirection, make sure to have first **DENY** statements to the destination of WSA proxy IP, to prevent authentication loop

```
ip access-list extended WCCP-REDIRECT

! Exclude traffic to WSAs IP from redirection

deny ip 10.125.30.0 0.0.0.255 host 10.125.10.10

deny ip 10.125.30.0 0.0.0.255 host 10.125.10.11

! Specify interesting traffic (ports are not needed explicitly, as they are negotiated on WCCP Control Level already by the client)

permit tcp 10.125.30.0 0.0.0.255 any eq www

permit tcp 10.125.30.0 0.0.0.255 any eq 443
```


R01 WCCP configuration (2)

- Step2: WCCP Service Group Configuration to use previously configured WCCP-REDIRECT ACL
- Step 3: Apply WCCP redirection on incoming (LAN facing) interface

```
ip wccp 91 redirect-list WCCP-
REDIRECT
```

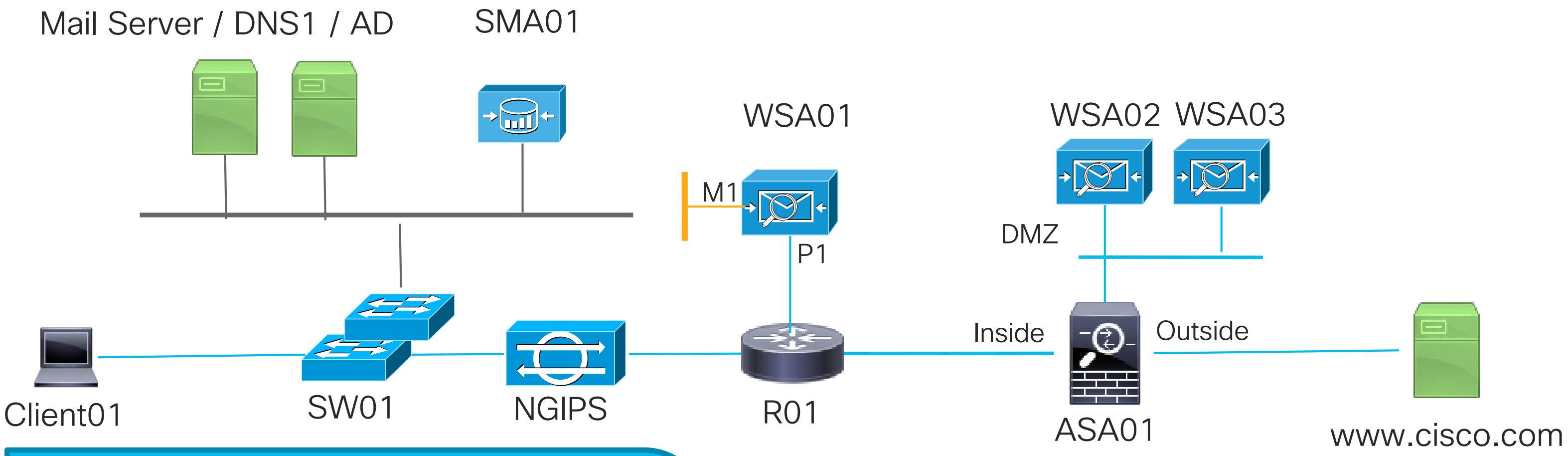
```
interface Gi0/1

 ip wccp 91 redirect in
```

Useful WCCP troubleshooting commands

```
! Show commands
show ip wccp 91
show ip wccp 91 detail
show ip wccp 91 client
show ip wccp 91 service
! Restarting the session
clear ip wccp 91
! Debug
debug ip wccp (packets|events|sub-blocks)
```

WSA Troubleshooting Case Study

WSA Troubleshooting Topology



WSA01 Initial Data
Initial Credentials: admin/ironport
M1: 10.255.0.42/24, DG: 10.255.0.1/24
P1: 10.125.10.10/24, DG: 10.125.10./24
DNS1/AD: 10.48.78.19
DNS2: 10.48.78.31
Domain: ironport.local
SMA IP: 10.48.78.56
Client IP: 10.125.30.30/24

Topology Considerations

DMZ WSA02 and WSA03 are already pre-configured
Authentication realm **ironport.local** is already created and functional on WSA01

WSA Troubleshooting Task (2 Issues)

- Site https://www.cisco.com is not reachable from the client Client01
- Please resolve the issue.
- Client IP: 10.125.30.30/24

WSA Checks

- Always check accesslogs for IP 10.125.30.30 towards www.cisco.com (use grep)
- Verify if the request was allowed/blocked, or did it reach WSA01 in the first place
- Verify connectivity from WSA01 (telnet, curl)
- Use a packet capture tool on WSA01
- Re-configure WSA01 if needed, and issues detected in configuration

WSA Verification

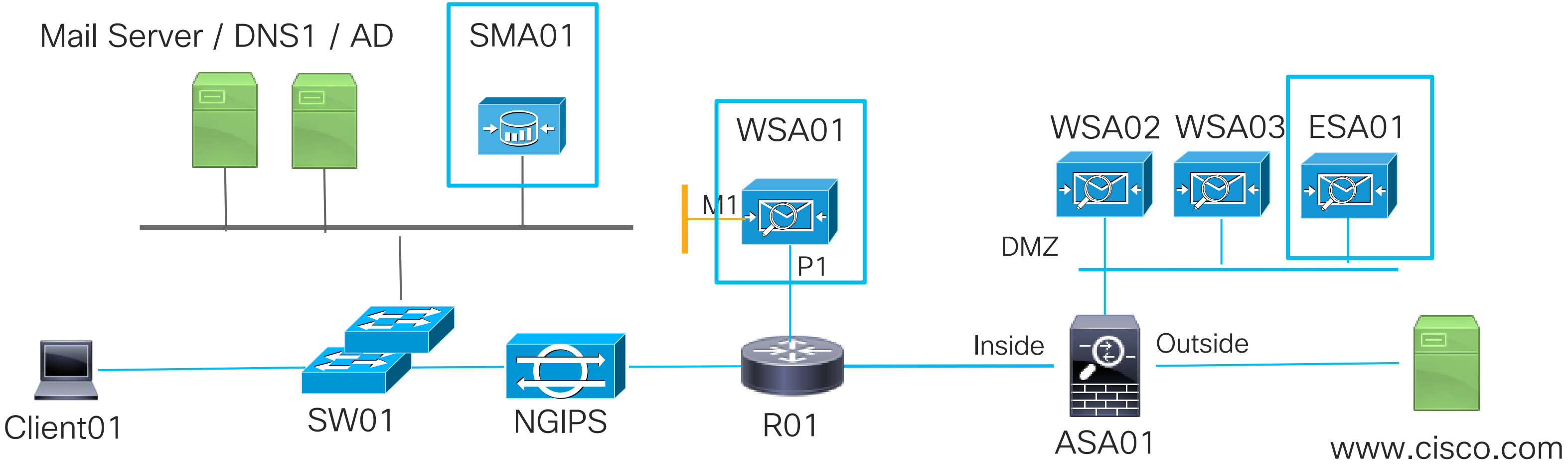
- Successful verification will show 200 HTTP response code when test client tries to visit www.cisco.com
  - User either curl tool on client, or a Web Browser
- Client should be able to see the Web page

WSA Troubleshooting Case Study Demo

Security Management Appliance (SMA) in CCIE Security

Configuration and Troubleshooting Case Study

SMA Configuration Topology



SMA Configuration Task

- Configure SMA01 so it offers:
  - Centralized SPAM quarantine to ESA01
  - Make sure ESA01 sends SPAM messages to SMA01
  - Centralized Reporting and Web tracking for WSA01
  - Credentials for all three devices are: admin/CiscoCCIE2019!

SMA Configuration Steps

- Enable Centralized SPAM quarantine on SMA
- Add WSA01 & ESA01 appliances to SMA configuration
- Enable external SPAM quarantine on ESA01
- Enable external Web Tracking and Reporting on WSA01
- Commit the changes

SMA Configuration Case Study Demo

Cisco Live References – Content Security

- ESA: BRKSEC-3540: I Wonder Where That Phish Has Gone, Hrvoje Dogan, Cisco Live Berlin 2017.
- ESA: BRKSEC-3008: “Extreme Filtering”, Hrvoje Dogan, Cisco Live Berlin 2016.
- ESA: BRKSEC-3127: Advanced - Cisco's E-mail Encryption Capabilities, Hrvoje Dogan, Cisco Live 2015.
- ESA: BRKSEC-2131: Cisco Email Security Deep Dive & Best Practices, Usman Din, Cisco Live Las Vegas 2016.
- WSA: BRKSEC-3006: The Trip to TLS Land using the WSA, Tobias Mayer, Cisco Live Berlin 2016.
- WSA: BRKSEC-3303: Cisco Web Security Appliance Configuration Best Practices & Performance Troubleshooting, Ana Peric, Cisco Live Barcelona 2018.

Thank you

Identity Services Engine

ISE in the CCIE lab

Srilatha Vemula (CCIE#33670), Technical Solutions Architect

TECCCIE-3202

Barcelona | January 27-31, 2020

About me

- 11 years with Cisco
- CCIE Security # 33670
- Technical Solutions Architect
- Scuba diving, hiking, canoeing

Agenda

- ISE Persona Overview
- Network access with ISE
- Policy set model
- Device administration with ISE
    - RADIUS
    - TACACS
- Case-Studies
- Troubleshooting

Blueprint v6.0 - ISE

4.0 Identity Management, Information Exchange, and Access Control	**25%**	Hide Details

4.1 ISE scalability using multiple nodes and personas.
4.2 Cisco switches and Cisco Wireless LAN Controllers for network access AAA with ISE.
4.3 Cisco devices for administrative access with ISE
4.4 AAA for network access with 802.1X and MAB using ISE.
4.5 Guest lifecycle management using ISE and Cisco Wireless LAN controllers
4.6 BYOD on-boarding and network access flows
4.7 ISE integration with external identity sources

- 4.7.a LDAP
- 4.7.b AD
- 4.7.c External RADIUS

4.8 Provisioning of AnyConnect with ISE and ASA
4.9 Posture assessment with ISE
4.10 Endpoint profiling using ISE and Cisco network infrastructure including device sensor
4.11 Integration of MDM with ISE
4.12 Certificate-based authentication using ISE
4.13 Authentication methods

- 4.13.a EAP Chaining
- 4.13.b Machine Access Restriction (MAR)

4.14 Identity mapping on ASA, ISE, WSA, and FTD
4.15 pxGrid integration between security devices WSA, ISE, and Cisco FMC
4.16 Integration of ISE with multi-factor authentication
4.17 Access control and single sign-on using Cisco DUO security technology

Caution .....

- **CCIE Lab != Production**
- Some of the suggestions here go against best practices for an ISE production deployment
- Slides will call out production friendly or CCIE lab-only recommendations.
- Speaker not responsible for Melted ISE in production ;)

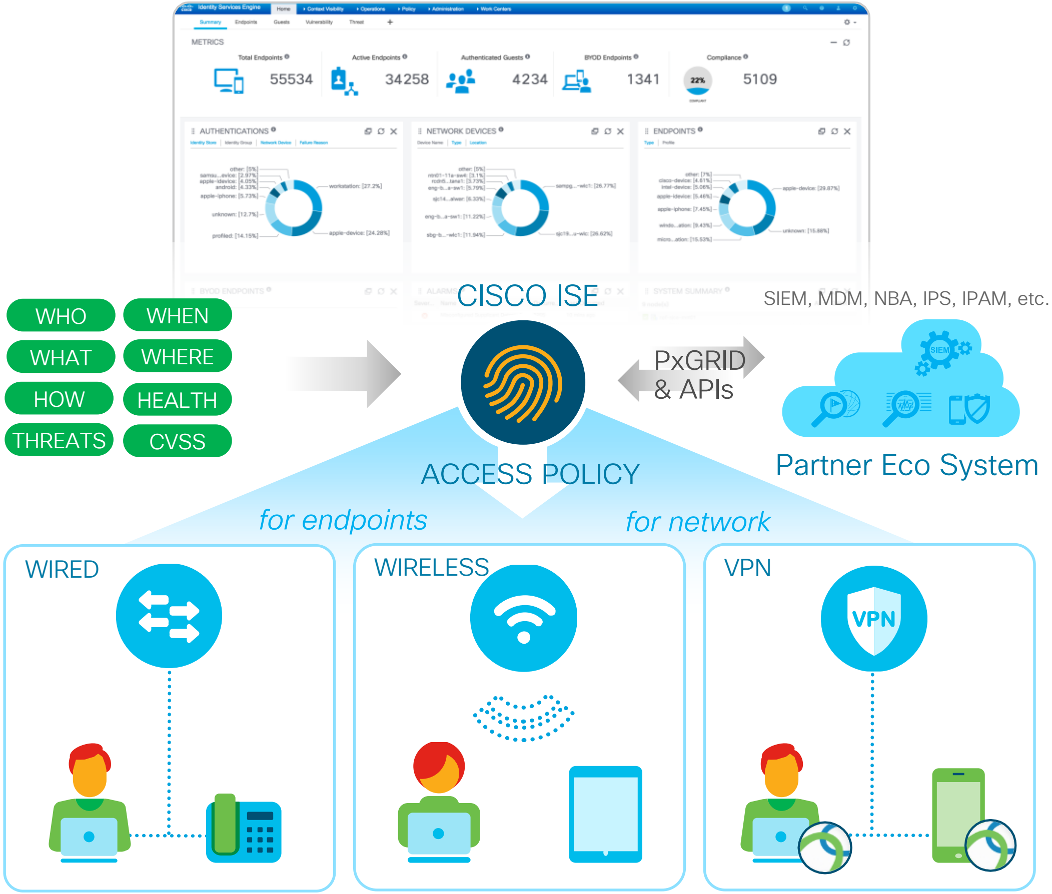
Cisco ISE overview

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform, that lets you,

See
Users, endpoints and applications

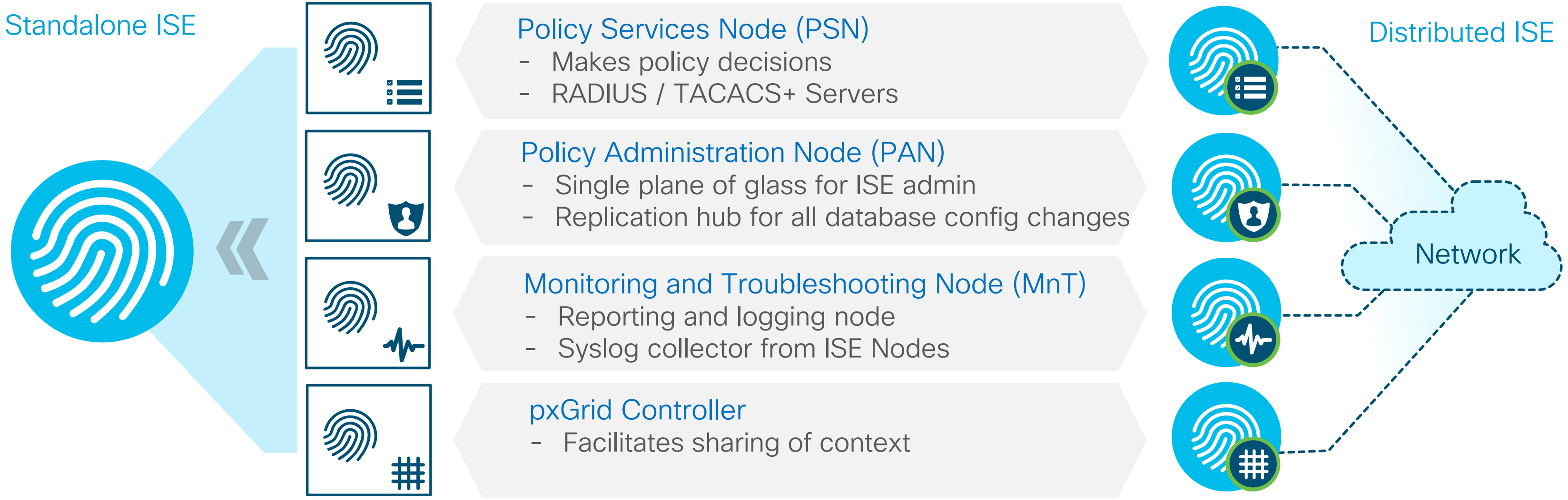
Secure
By controlling network access and segmentation

Share
Context with partners for enhanced operations



Role-based Access Control | Guest Access | BYOD | Secure Access

ISE Architecture

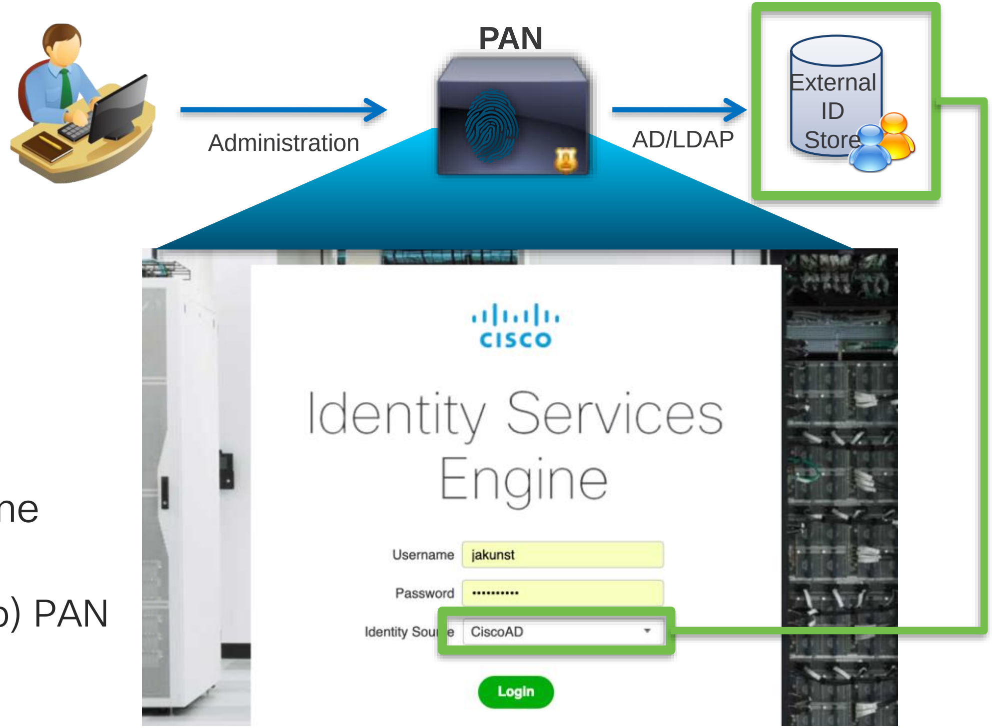


Policy Administration Node (PAN)

Writeable Access to the Database

For your reference

- 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



Policy Service Node (PSN)

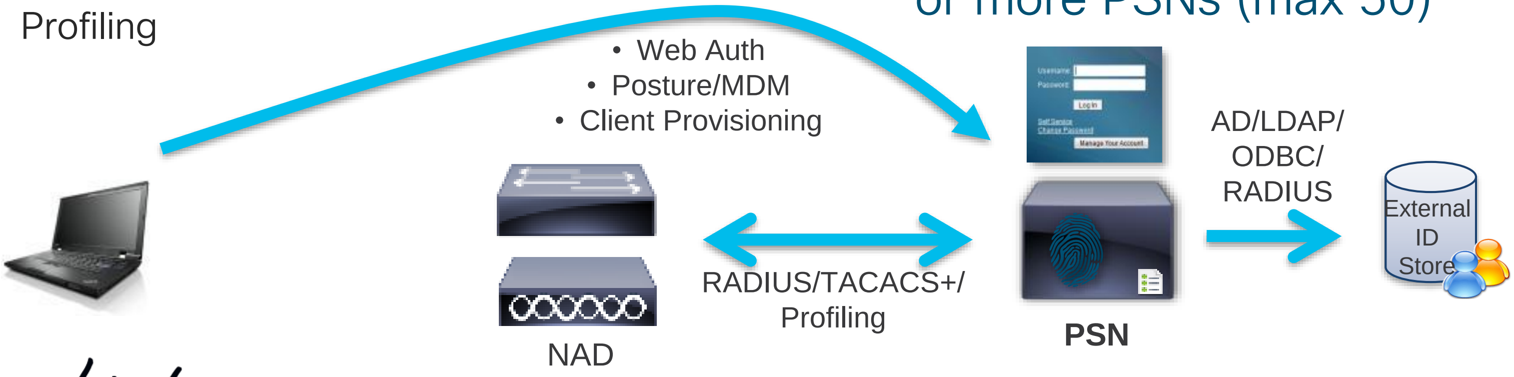
RADIUS/TACACS+ Server for the Network Devices

- 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

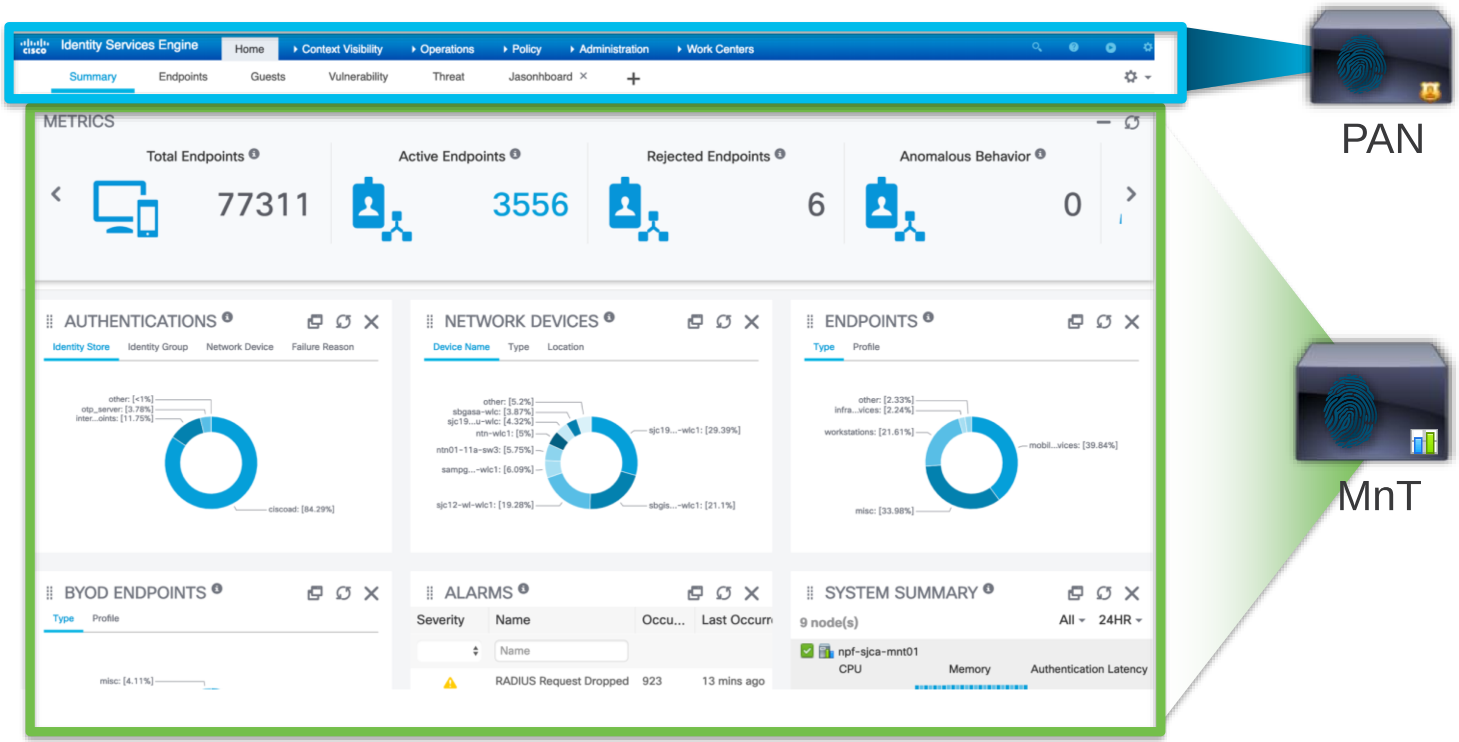
Each ISE deployment must have one or more PSNs (max 50)



Monitoring and Troubleshooting Node (MNT)

Dashboard

For your reference

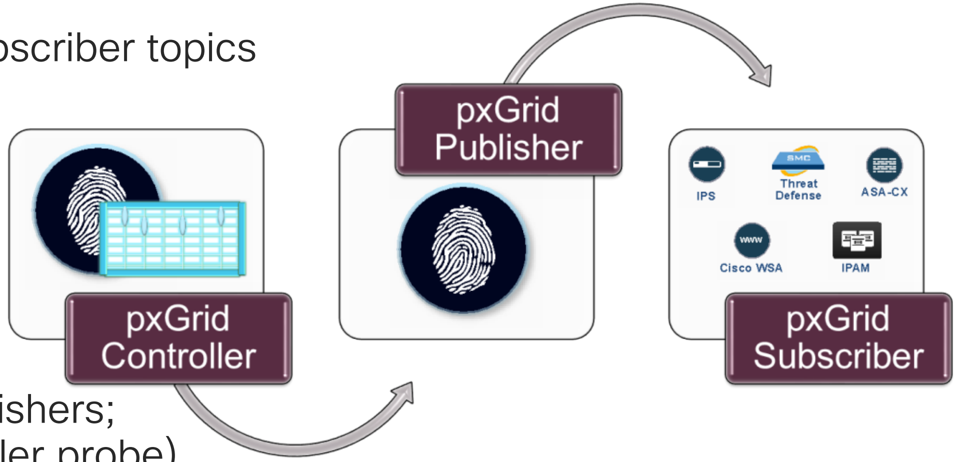


pxGrid Controller (PXG)

Context Data Sharing

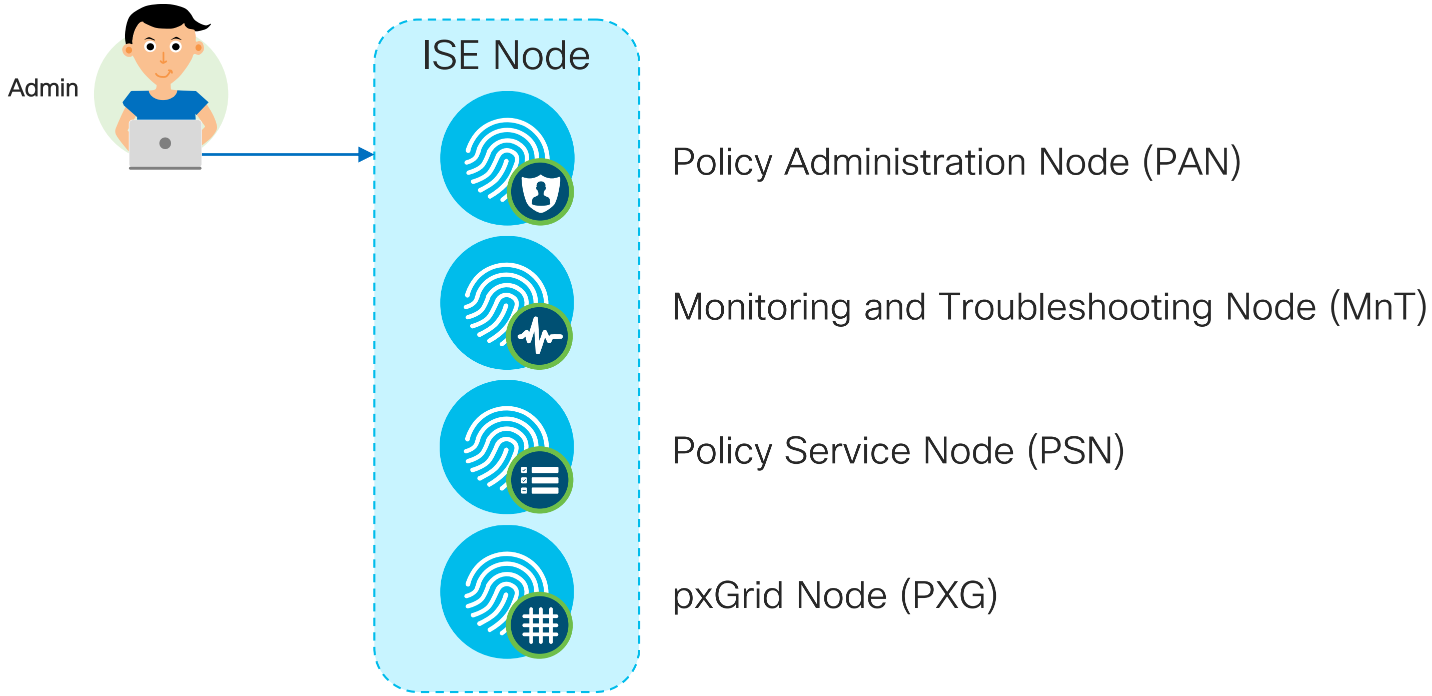
For your reference

- Enabled as pxGrid persona
  - Max 4 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

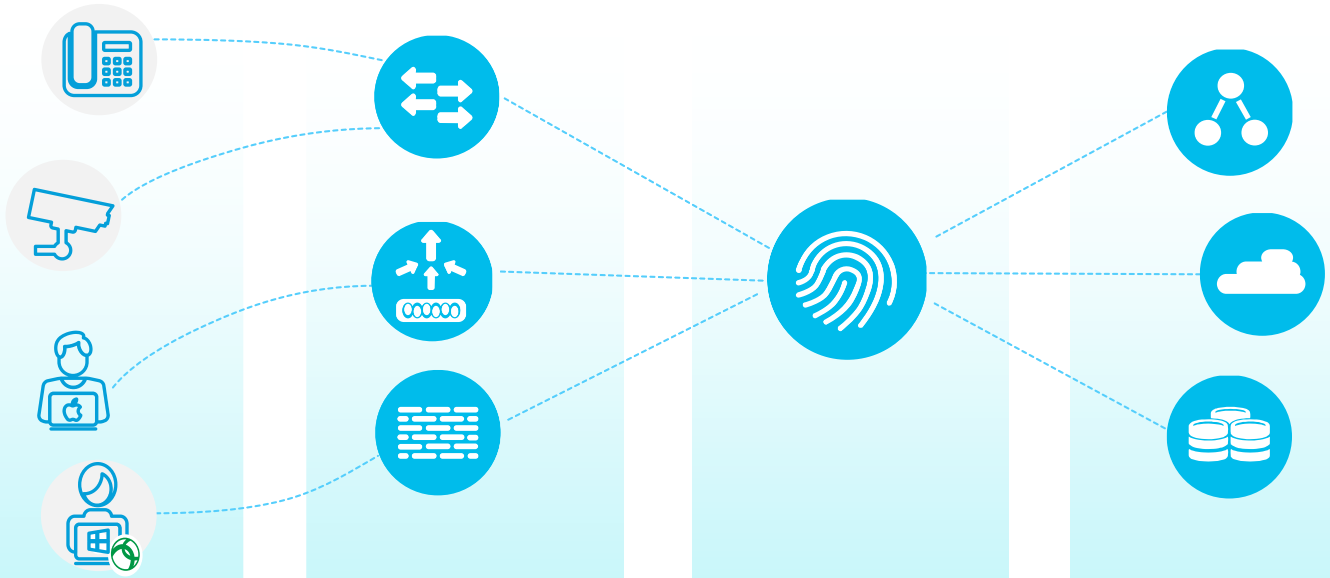


Standalone Deployment (CCIE Lab)

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



Network Access Deployment Components



Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- VPN gateways
- Wireless LAN Controllers

Cisco ISE

- Standalone ISE
- Multi-node ISE
- VM/Appliance

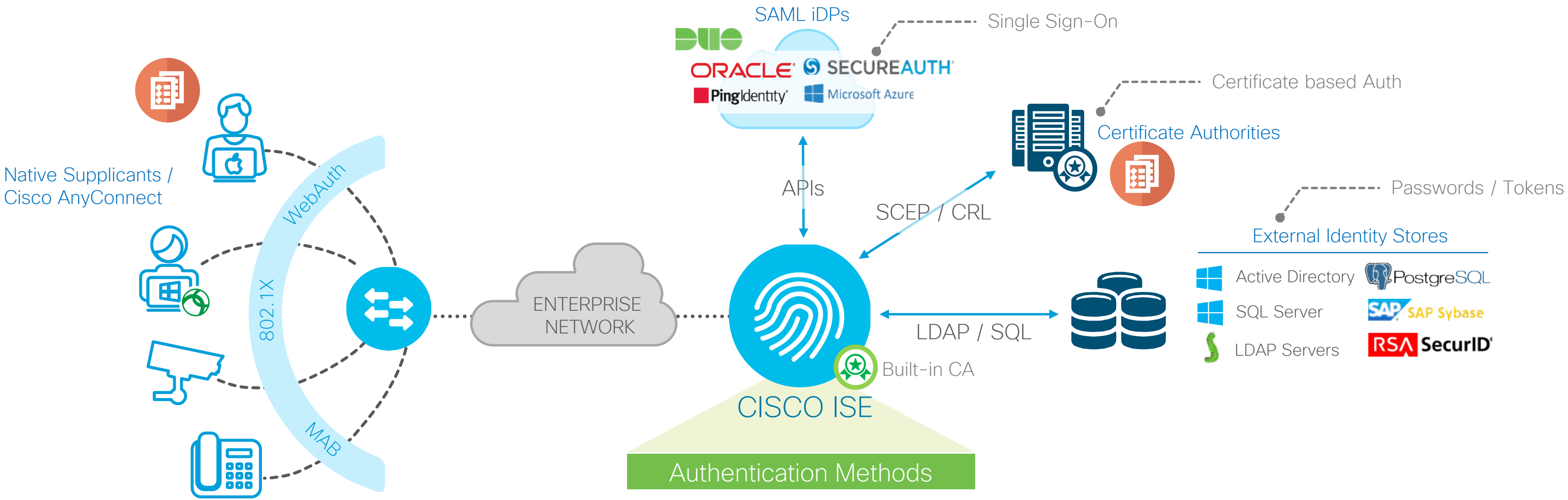
External Services

- AD/LDAP
- MDM
- Security services

RADIUS

- RFC 2865, Accounting RFC 2866
- UDP Ports: Authentication 1812, Accounting 1813
  - Cisco Legacy 1645/1646
- Information transmitted via Attribute/Value Pairs

Authentication Methods



Authentication Methods

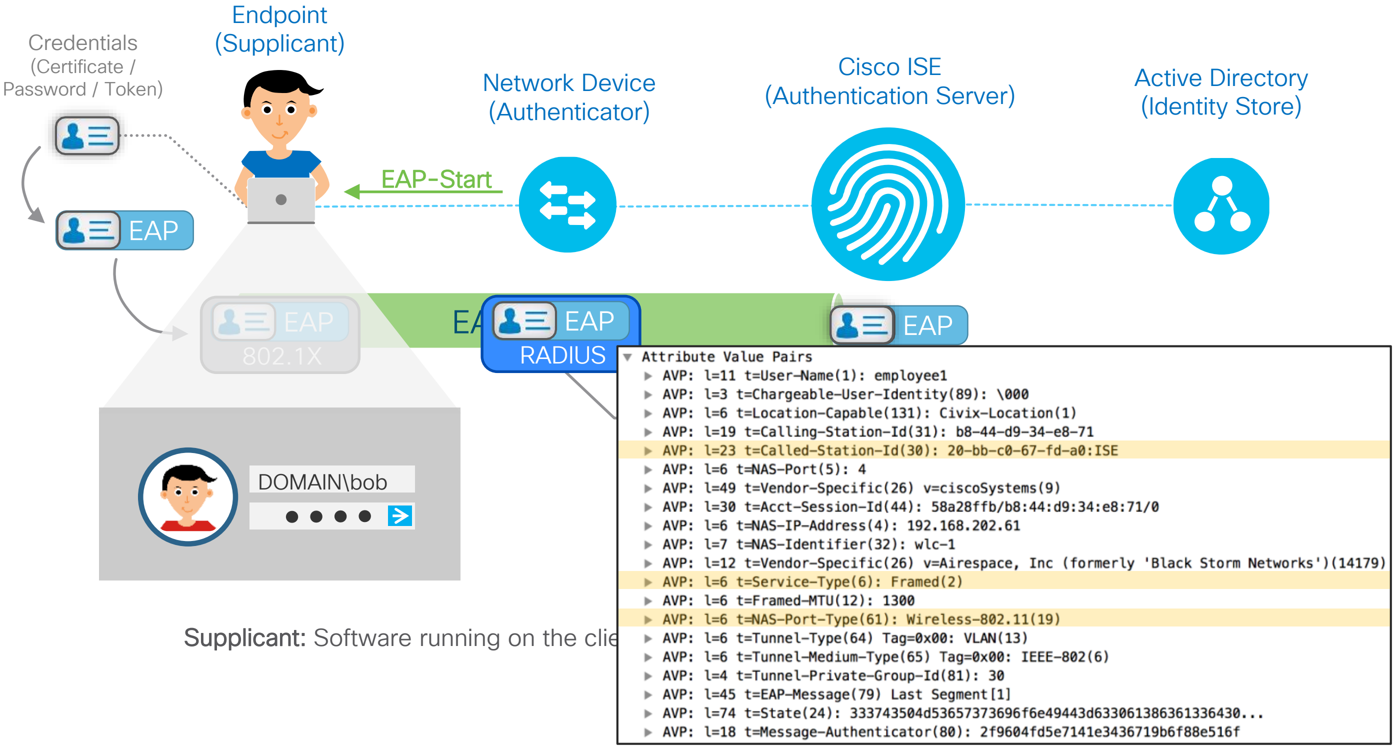
ACTIVE IDENTITY

- IEEE 802.1X
  - 802.1X PEAP-MSCHAPv2
  - **802.1X EAP-TLS**
- Web Authentication
  - Central WebAuth
  - Local WebAuth

PASSIVE IDENTITY

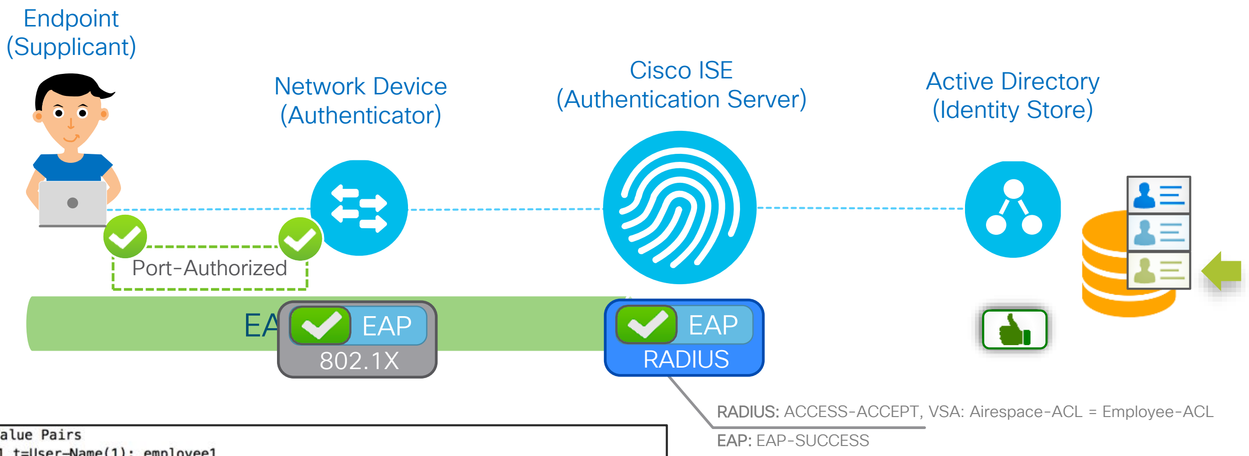
- MAC Authentication Bypass
- Easy Connect ®

Fundamentals of 802.1X



Supplicant: Software running on the clie

Fundamentals of 802.1X




```
▼ Attribute Value Pairs
  ▶ AVP: l=11 t=User-Name(1): employee1
  ▶ AVP: l=40 t=State(24): 526561757468536573736f6e3a63306138636133643030...
  ▶ AVP: l=51 t=Class(25): 434143533a633061386361336430303030303033353861...
  ▶ AVP: l=6 t=EAP-Message(79) Last Segment[1]
  ▶ AVP: l=18 t=Message-Authenticator(80): ea8102e64735fe4037e02bc3d3a720f4
  ▼ AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
      AVP Type: 26
      AVP Length: 37
    ▶ VSA: l=31 t=Cisco-AVPair(1): cts:security-group-tag=0004-0
  ▶ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
  ▼ AVP: l=20 t=Vendor-Specific(26) v=Airespace, Inc (formerly 'Black Storm Networks')(14179)
      AVP Type: 26
      AVP Length: 20
    ▶ VSA: l=14 t=Airespace-ACL-Name(6): Employee-ACL
```

thentication Protocol

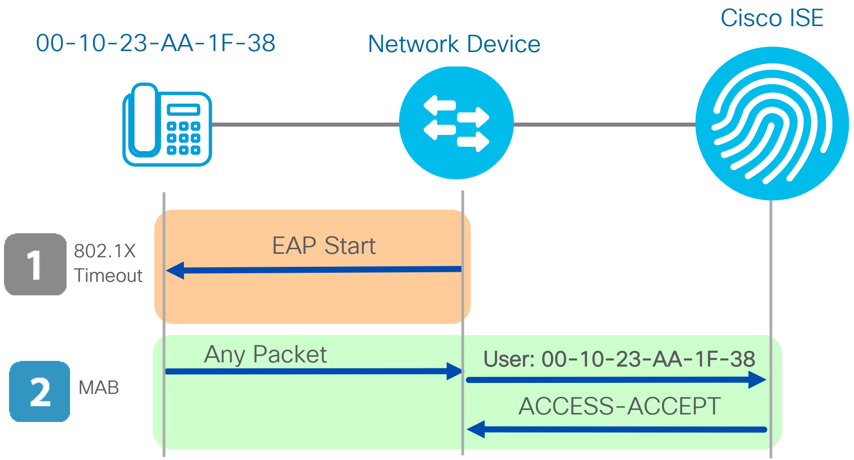
tials to the authenticator (Network Device).

MAC Authentication Bypass (MAB)

Endpoints without supplicant will fail 802.1X authentication!

```
▼ Attribute Value Pairs
  ▶ AVP: l=14 t=User-Name(1): b844d934e871
  ▶ AVP: l=24 t=Called-Station-Id(30): 20-bb-c0-67-fd-a0:OPEN
  ▶ AVP: l=19 t=Calling-Station-Id(31): b8-44-d9-34-e8-71
  ▶ AVP: l=6 t=NAS-Port(5): 4
  ▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.202.61
  ▶ AVP: l=7 t=NAS-Identifier(32): wlc-1
  ▶ AVP: l=12 t=Vendor-Specific(26) v=Airespace, Inc (formerly 'Black Storm Networks')(14179)
  ▶ AVP: l=18 t=User-Password(2): Encrypted
  ▶ AVP: l=6 t=Service-Type(6): Call-Check(10)
  ▶ AVP: l=6 t=Framed-MTU(12): 1300
  ▶ AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
  ▶ AVP: l=6 t=Tunnel-Type(64) Tag=0x00: VLAN(13)
  ▶ AVP: l=6 t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
  ▶ AVP: l=4 t=Tunnel-Private-Group-Id(81): 30
  ▼ AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
      AVP Type: 26
      AVP Length: 49
    ▶ VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8ca3d0000000058a28e54
  ▶ AVP: l=30 t=Acct-Session-Id(44): 58a28e54/b8:44:d9:34:e8:71/1
```

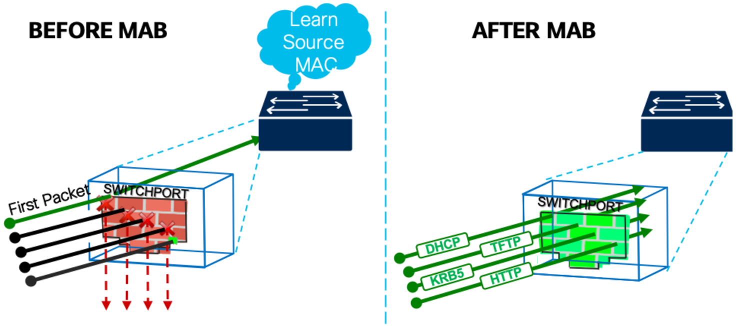
Bypassing "Known" MAC Addresses



MAB requires a MAC address database | ISE can build this database dynamically with profiling

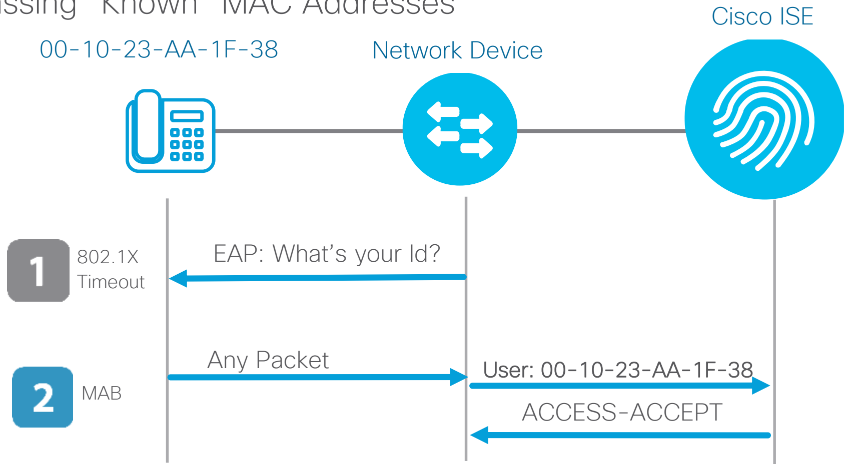
MAC Authentication Bypass(MAB)

For your reference



Functional Overview

Bypassing "Known" MAC Addresses



MAC Address Discovery

- MAC Address Inventories
- MAB in Monitor-Mode
- MAB address prefixes(OUI)

MAB requires a MAC address database

- Internal Database
- External LDAP
- Microsoft Active Directory

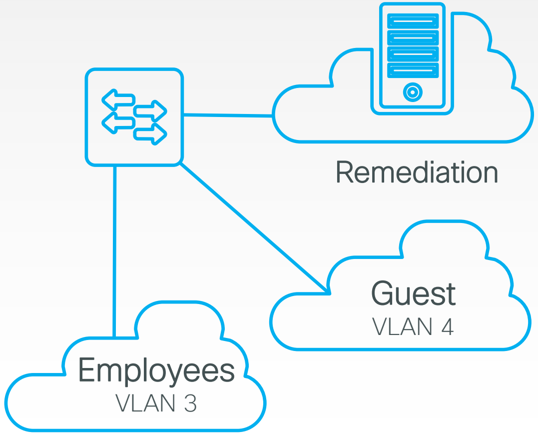
** Introduction to Device Sensor and Profiling topics are covered later in the course*

Authorization

3 Major Authorization Options for Access Control

VLANs

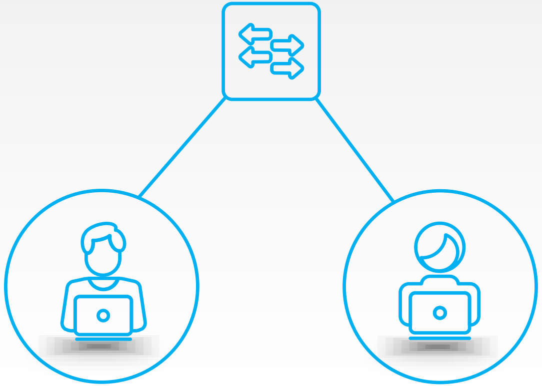
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

DACL or Named ACL

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)

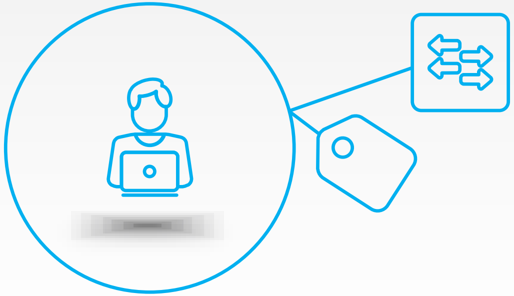


Employee
permit ip any any

Contractor
deny ip host <critical>
permit ip any any

Scalable Group Tags

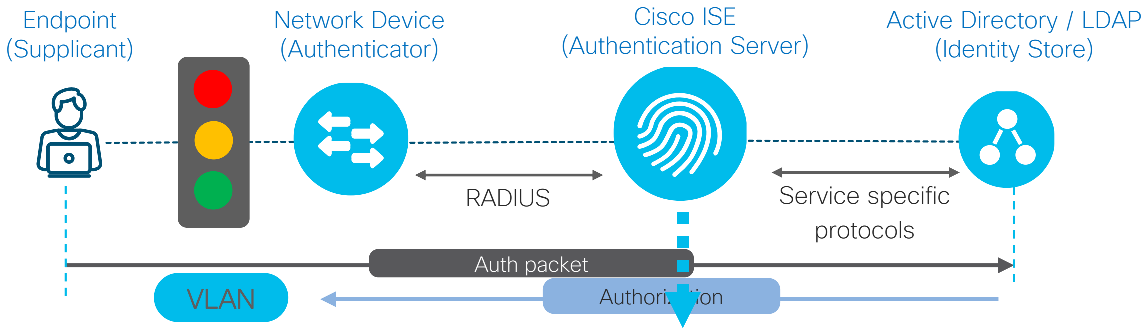
Cisco TrustSec



16 bit SGT assignment and SGT based Access Control

Authorization Options

Dynamic VLAN



Authorization Profiles > **Employees-Demo.local**

Authorization Profile

* Name: Employees-Demo.local

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

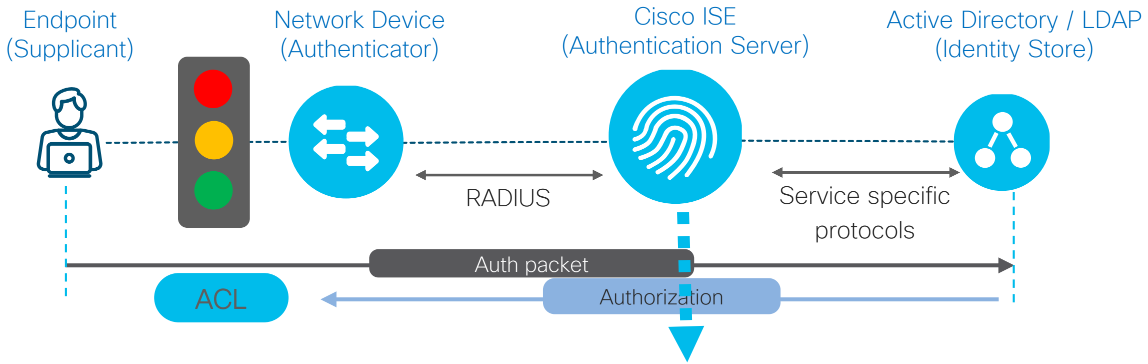
- [ ] DACL Name
- [ ] ACL (Filter-ID)
- [ ] Security Group
- [x] VLAN — Tag ID 1 — Edit Tag — ID/Name 192_168_6_0-SJC15_VN

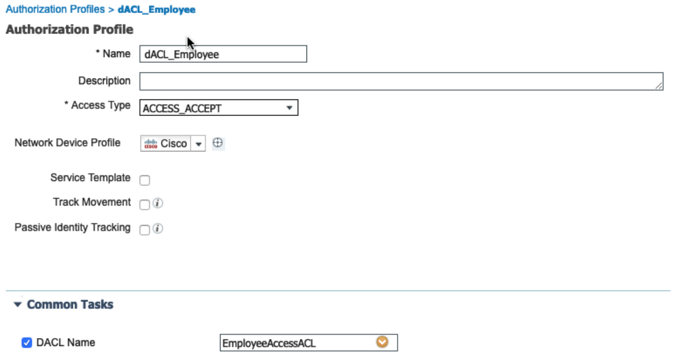
Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:192_168_6_0-SJC15_VN
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Authorization Options

Downloadable ACLs





Policy Set Overview

ISE policy fundamentals

Policy | Administration | Work Centers

Policy Sets **Profiling**
Posture **Client Provisioning**
Policy Elements
Dictionaries
Conditions
Results

If CONDITION = True, Then RESULT

Based on DICTIONARY attributes

Common Principle for

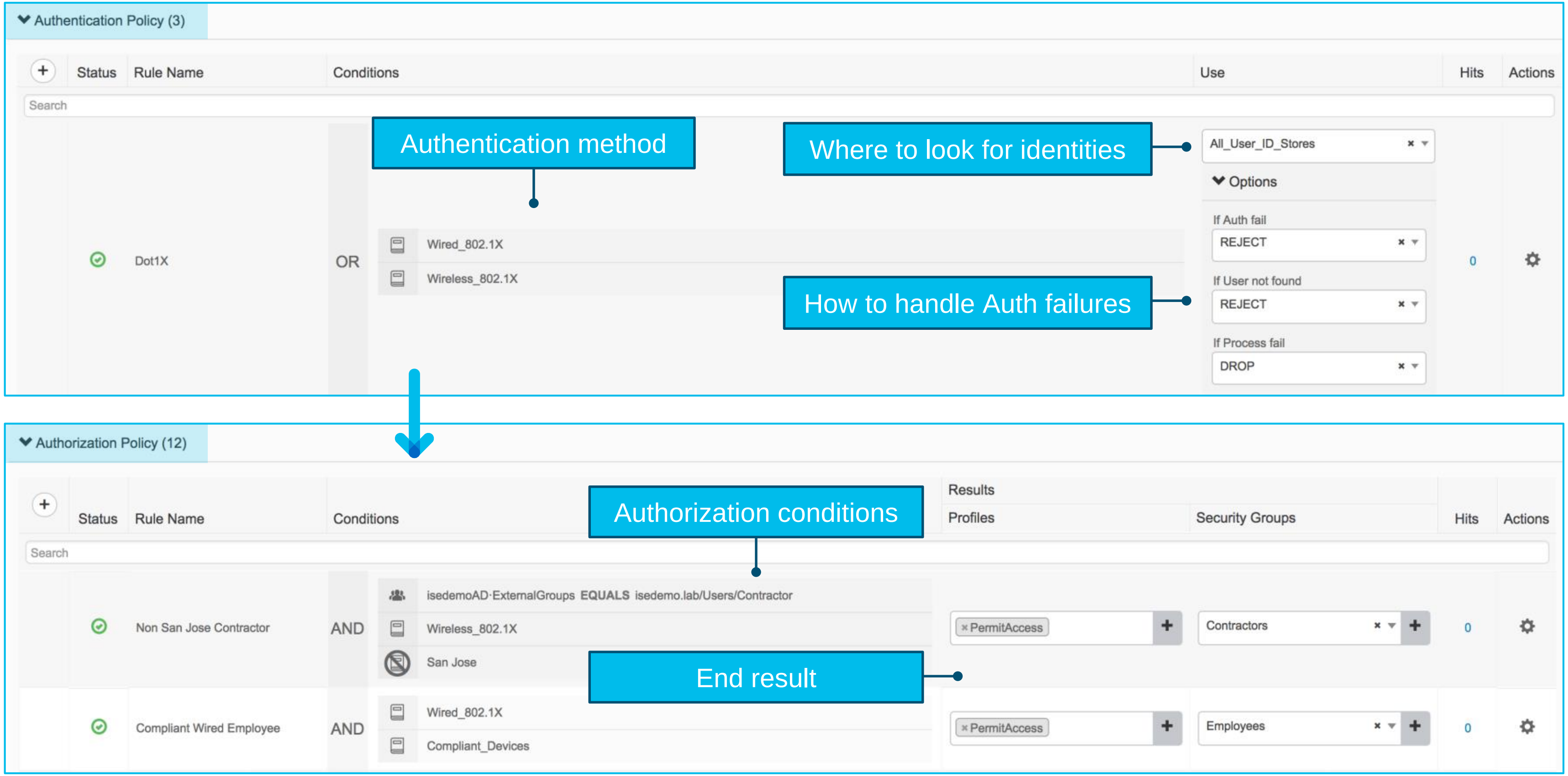
- Authentication policy
- Authorization Policy
- Profiler policy
- Posture policy
- Client provisioning policy

E.g. Authorization Policy:

If IP Phones = True, Then Voice VLAN

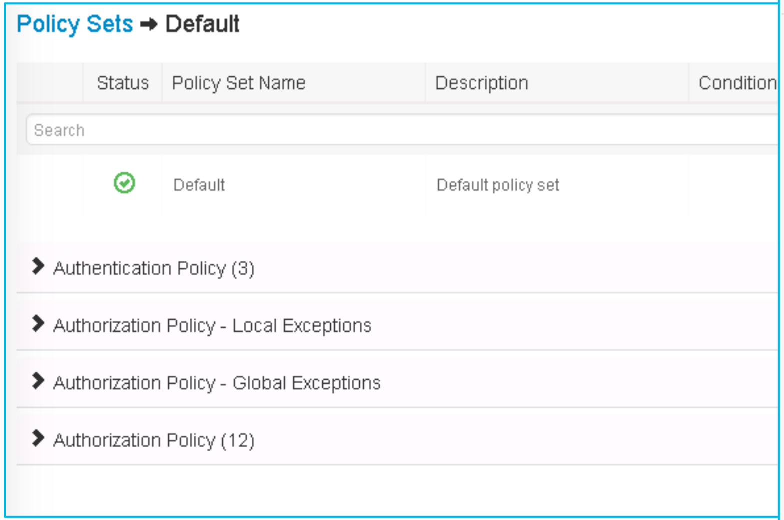
Endpoint Identity Group = IP Phones

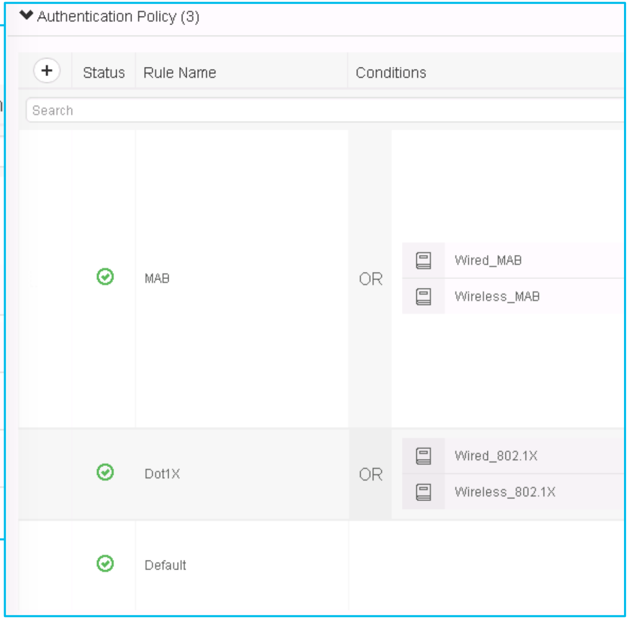
ISE Authentication and Authorization policy

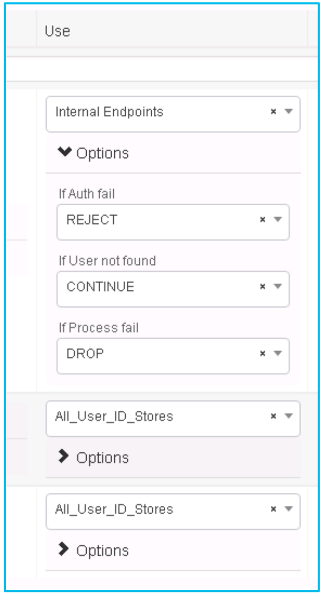


Default Policies

Before we get into any policy configuration, there are some default policies in ISE 2.4 that are important to understand.







Default Policies

Default enabled Authorization rules

Authorization Policy (12)

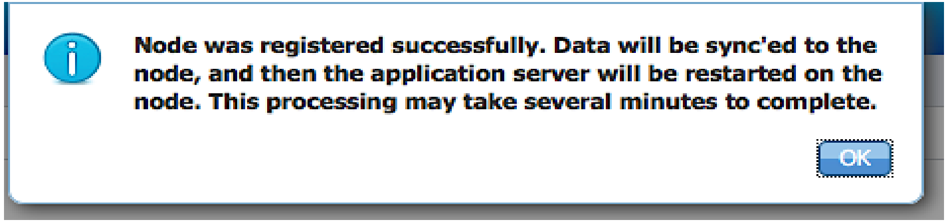
Status	Rule Name	Conditions	Results: Profiles
✓	Wireless Black List Default	AND: Wireless_Access; IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Blacklist	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones
✓	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess
✓	Default		DenyAccess

ISE Time Save

General time saving tips for CCIE Lab

ISE restart duration

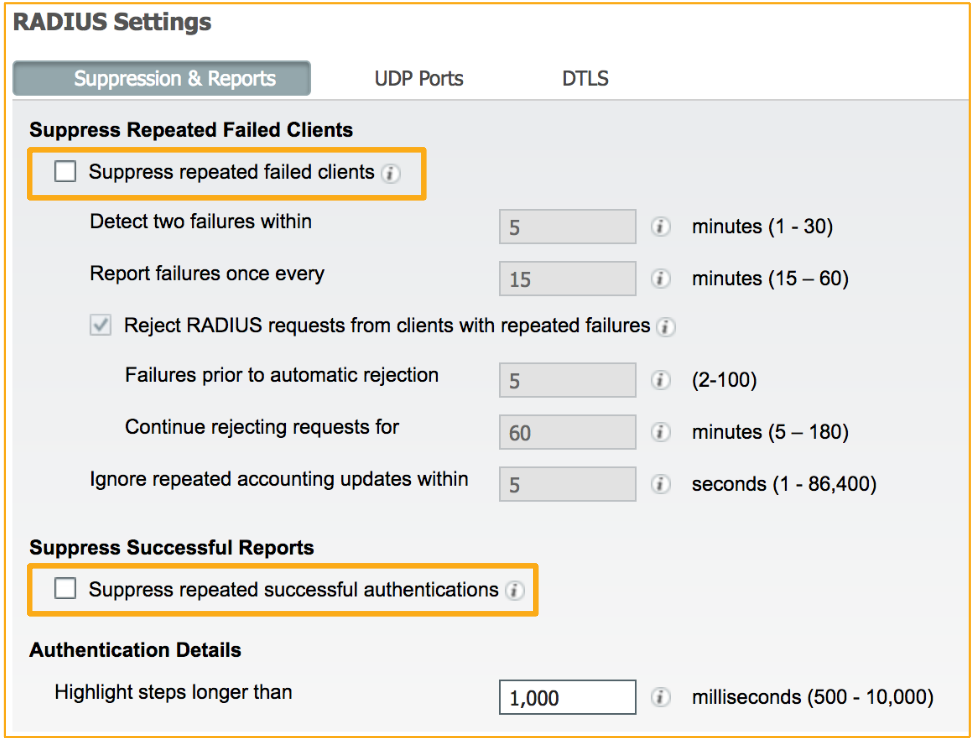
- ISE services can take up to 30 minutes to stop and start
- Initial setup, adding nodes to deployment or changing persona restarts services
- Strategize restart period in lab
- Best time to complete restart requiring changes is right at the start of the configuration section.



CCIE Lab-only

Disable all suppression

- ISE has two suppression mechanism enabled by default:
  - Logging of repeated successful authentication
  - Authentication of endpoints that fail repeatedly
- Both suppressions will cause difficulties in testing and troubleshooting in lab.
- Uncheck everything at Administration > System > Settings > Protocols > RADIUS



Default Policy Sets

CCIE Lab-only

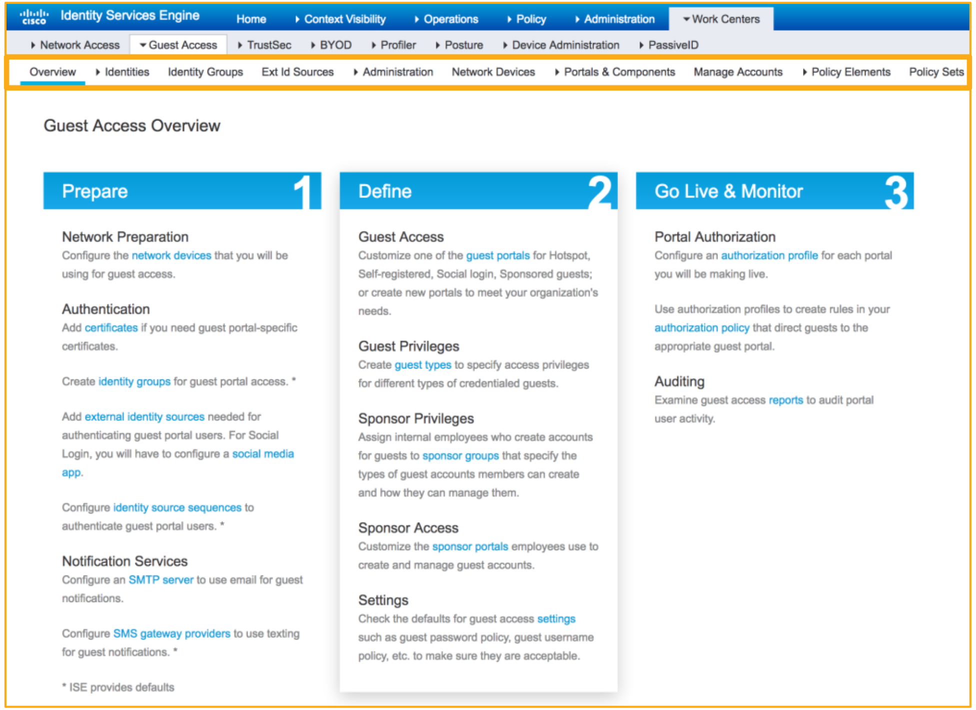
- ISE policy engine will attempt to match every session to every rule in sequence
- Sequence of rules is important
- May match wrong session to wrong rule or wrong DB
- Create specific rules in lab

Wireless MAB	Wireless_MAB	PermitAccess
Wired MAB	Wired_MAB	PermitAccess
Wireless 802.1x	Wireless_802.1X	PermitAccess
802.1x	Wired_802.1X	PermitAccess
Default		DenyAccess

Production Best Practice

Workflows

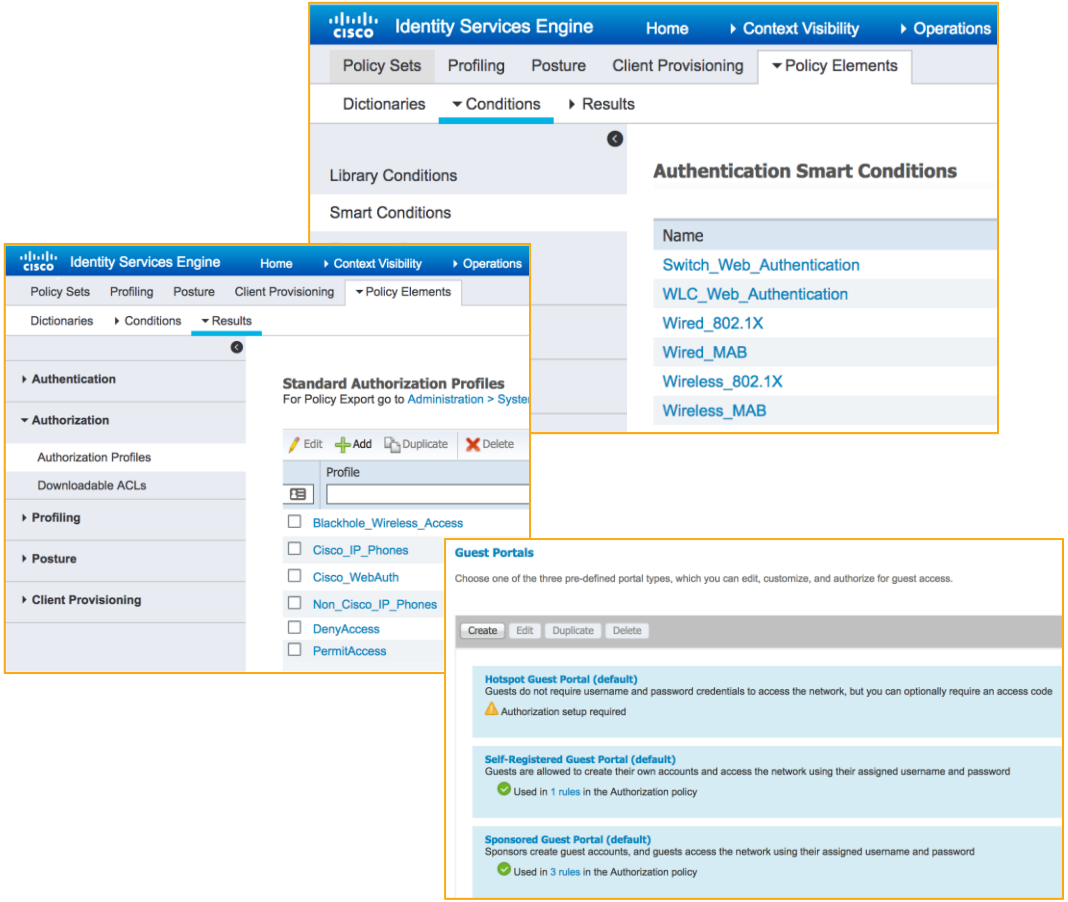
- Every flow in ISE requires multiple elements to be configured and tied together
- Elements are created or configured in different places in the GUI
- Workflows make it simple to configure flows.
- Start with Overview and work your way right in the sub-menu



Pre-Built Elements

CCIE Lab-only

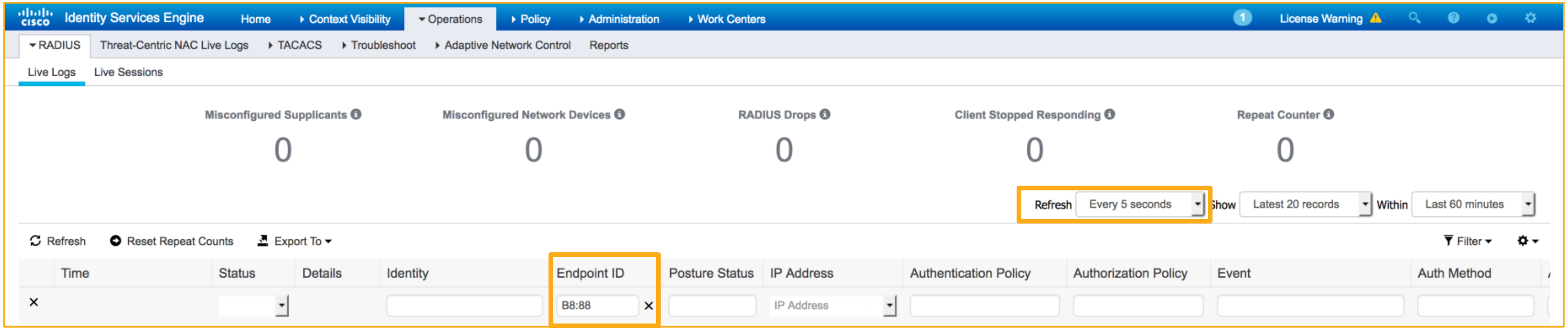
- ISE has a lot of pre-built elements for every flow.
- Use pre-built elements where possible
- Authentication, Authorization, Guest and Posture flows have good pre-built conditions and results you can use.
- Pre-built portal pages can be modified as required to suit lab needs.



Live Logs – Your best friend

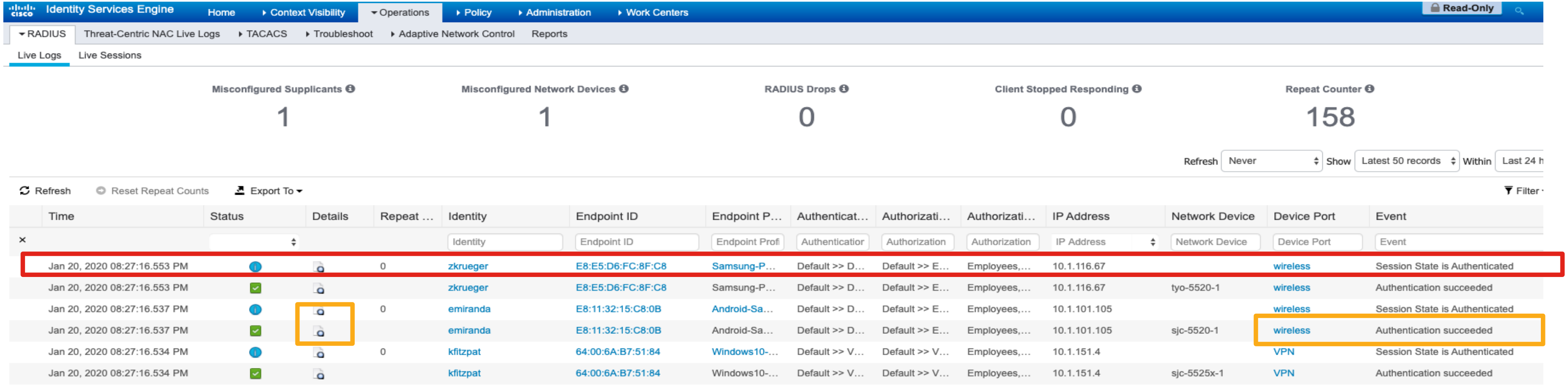
Production Best Practice

- Understand and use live logs.
- For CCIE lab, they provide the only troubleshooting tools you should need.
- ISE debug logs are time consuming. Avoid them in the lab.
- Set refresh timer to 5 seconds on Live logs
- Use filters, especially Endpoint ID, to filter out noise



Live Logs – Your best friend

- Ignore the lines that have a blue icon on the Status column
- Understand sequence of logs that will be seen for a flow.
- Pay particular attention to dynamic authorization logs.
- The details icon will open detailed logs of the session in a different tab/page.
- Look for explanation of failure in the detailed logs page.



Case Study 1

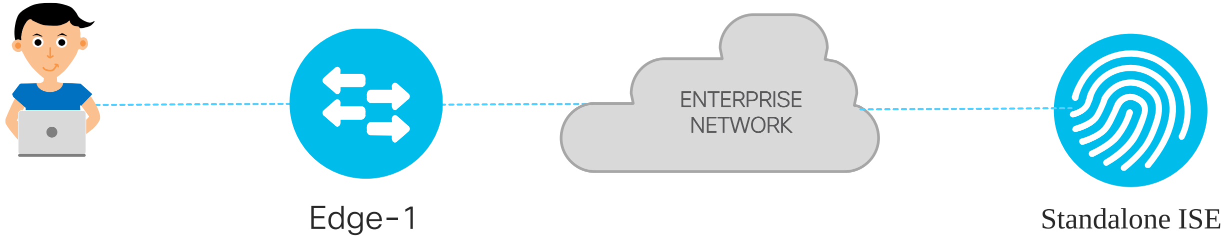
Configuration Task

Configure 802.1x for the wired client using ISE.

User is on Edge-1 port Gi1/0/10

User should use the credentials hr1/C1sco12345 to connect to the network

ISE should dynamically place in vlan 1021



Steps:

1) NAD (Network access device) Configuration

2) ISE configuration
    - Add NAD on ISE
    - ID Store
    - Authorization Profile (Elements)
    - Authentication Policy
    - Authorization Policy

3) Configure the 802.1x supplicant

4) Verification

CCIE Lab-only

Step 1
Switch configuration – AAA + RADIUS

- Enabling AAA will change device login method. Ensure you and proctor can login to device.
- Declares RADIUS server, Dynamic authorization server and AAA.
- Some IOS versions require RADIUS server to be declared with a name, as shown
- Accounting configuration is very important and should allow **newinfo** updates

```
radius server ise
 address ipv4 <ise-psn-ip> auth-port 1645 acct-port 1646
 pac key <shared-key>
!
aaa group server radius ise-group
 server name ise
!
aaa authentication dot1x default group ise-group
aaa authorization network default group ise-group
aaa accounting update newinfo periodic 600
aaa accounting dot1x default start-stop group ise-group
!

ip device tracking // MUST
dot1x system-auth-control // MUST

aaa server radius dynamic-author
 client <ise-psn-ip> server-key <shared-key>
  auth-type any
!
radius-server vsa send authentication
radius-server vsa send accounting
```

CCIE Lab-only

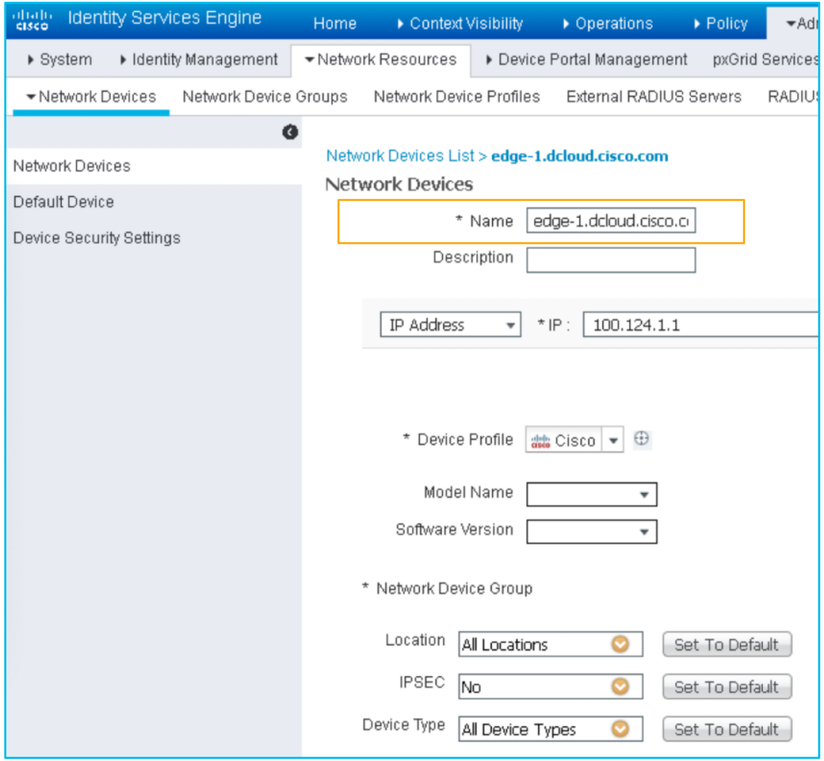
Step 1(b)
Switch configuration – Interface

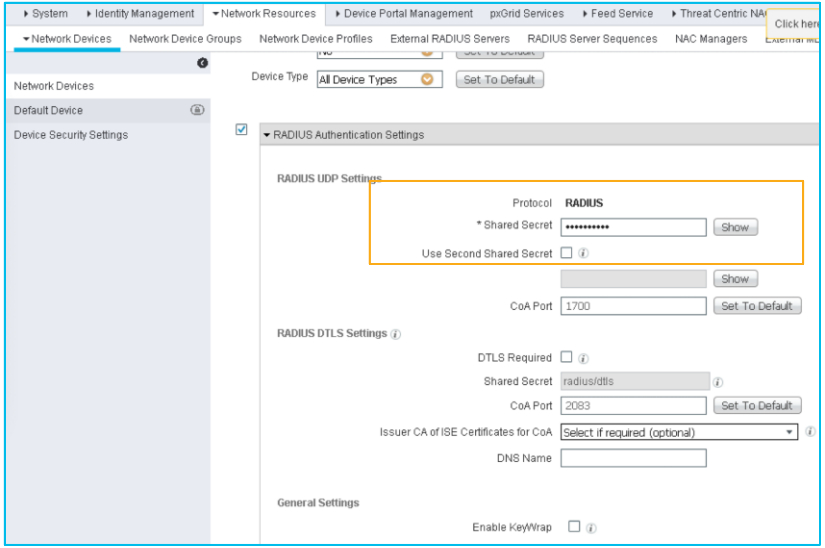
- These commands enable and enforce 802.1x and MAB on the interface.
- Timers should be left at default for the lab, unless specifically required by a question
- These should only be applied to the interface that connects to the test machine.
- Authentication can quickly be disabled on the interface with the command - **authentication port-control force-authorized**

```
interface GigabitEthernet1/0/x
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
```

Step 2 – ISE Configuration

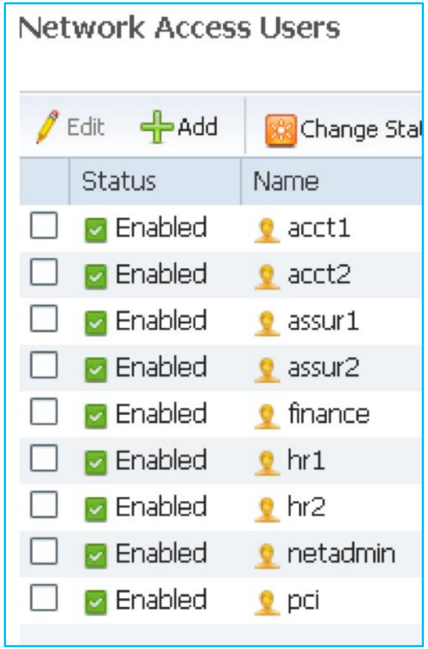
Add switch as NAD on ISE (Administration – Network Resources – Network Devices)



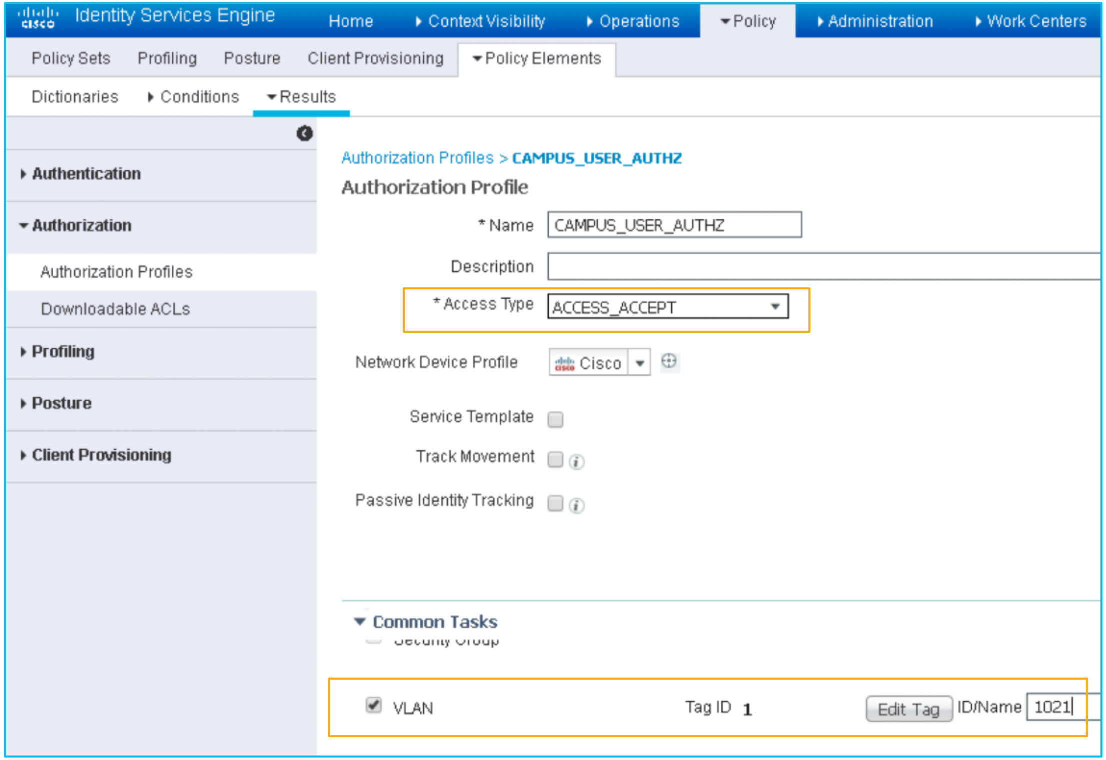


Step 2 - ISE Configuration

User account to be present in the ID Store. Internal Users for this task. Validate if **hr1** user is in the ISE internal database

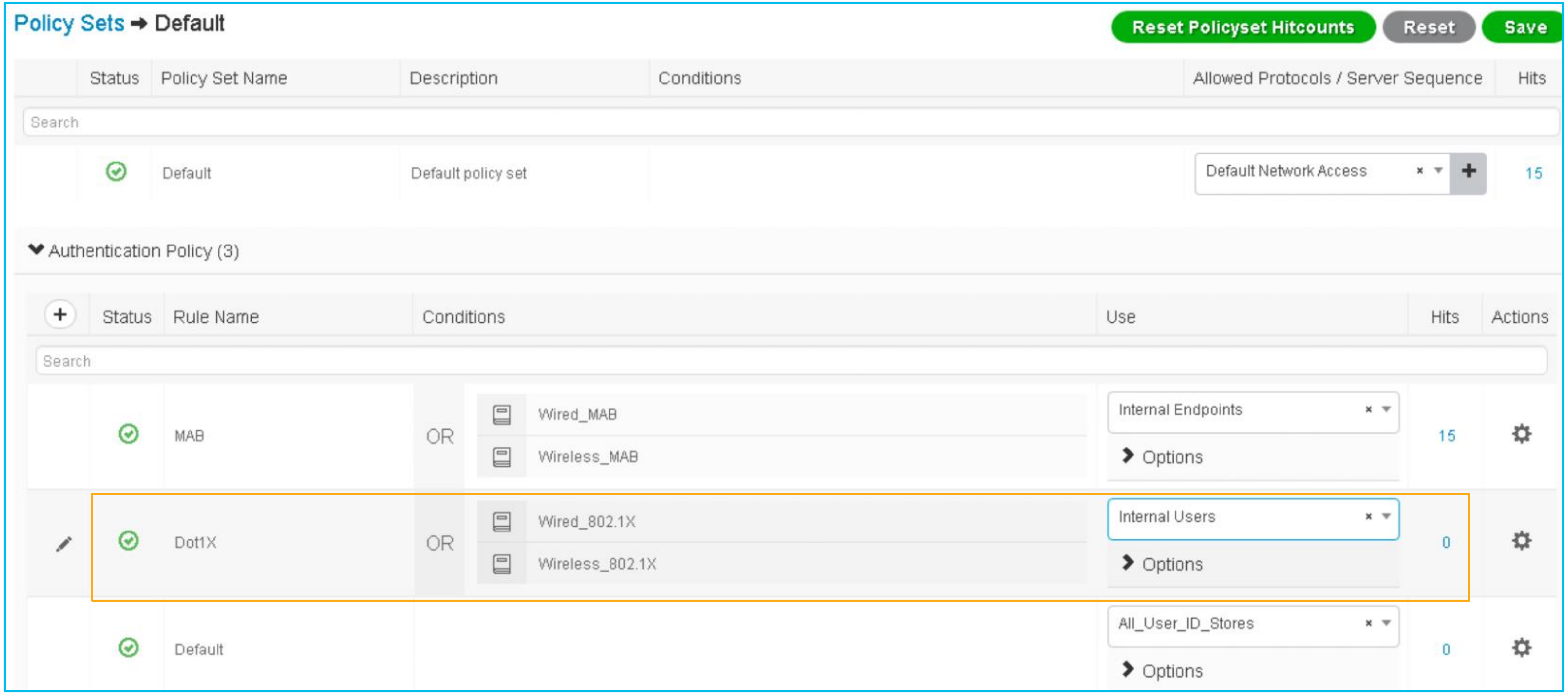


Authorization profile for the user to send an **access-accept and VLAN 1021**



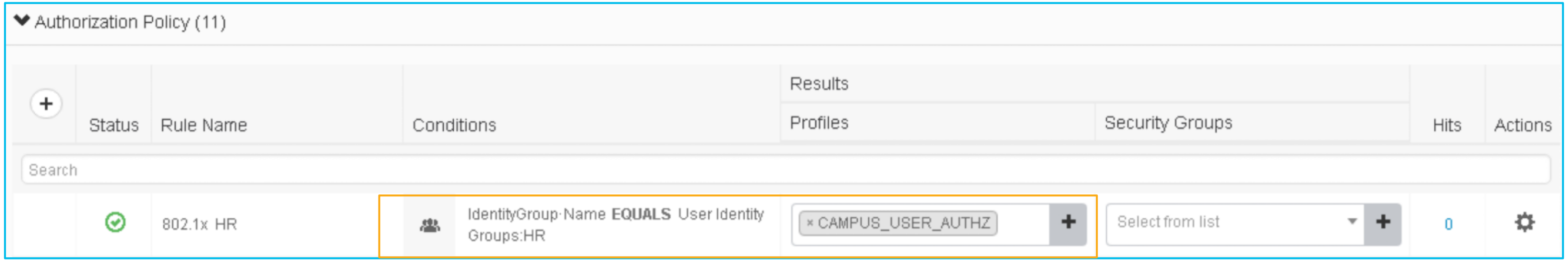
Step 2 - ISE Policy Configuration

Leverage Default Policy set on ISE



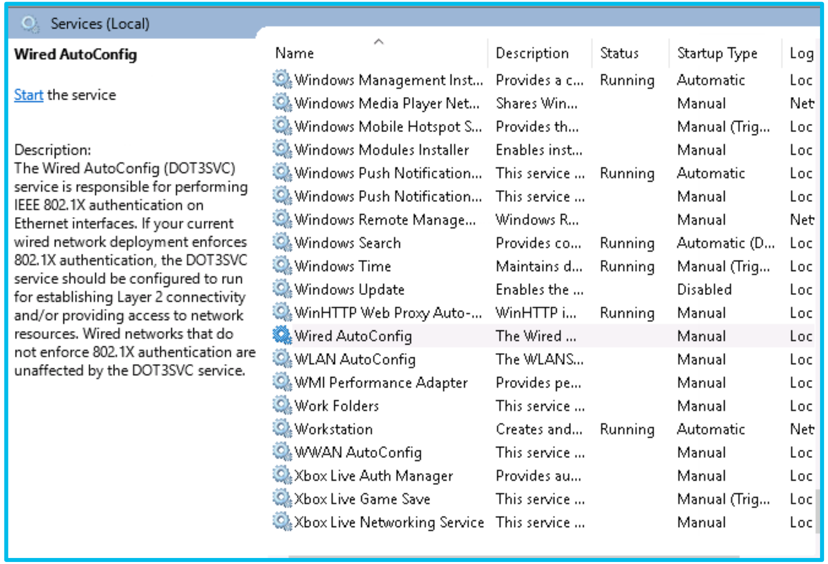
Step 2 - ISE Policy Configuration

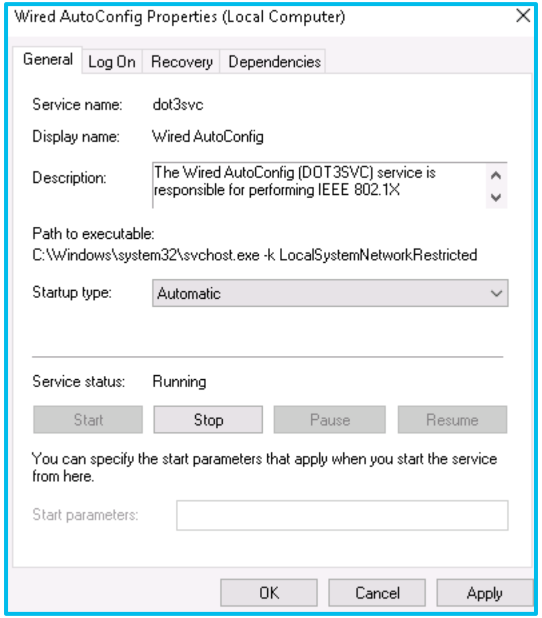
Authorization Policy to match on HR group and push the authorization result previously configured

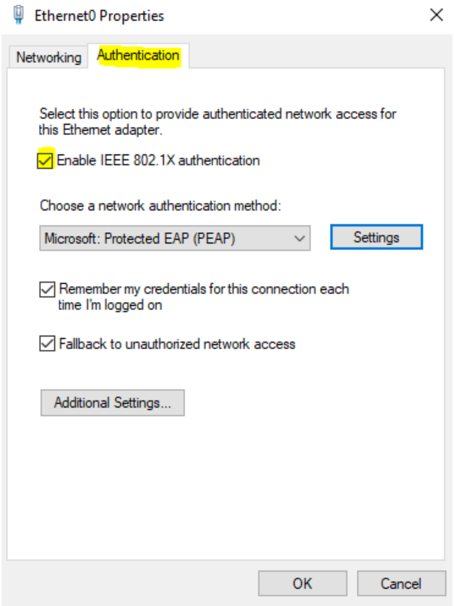


Step 3 – Client 802.1x Configuration

The WiredAutoconfig service enables the 802.1X supplicant on Windows.
It is set to manual startup by default.







Step 4 – Verification

Connect the client and verify – ISE and Switch

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Endpoint ID	Identity	Authenticat...	Authorization Policy	Authorization Pr...	IP Address	Network Devi
				hr1				IP Address	
Jan 25, 2020 03:19:08.011 PM			00:0C:BD:06:3...	hr1	Default >> D...	Default >> 802.1x HR	CAMPUS_USER_...	100.100.0.21,fe...	
Jan 25, 2020 03:19:05.145 PM			00:0C:BD:06:3...	hr1	Default >> D...	Default >> 802.1x HR	CAMPUS_USER_...	100.100.0.21,fe...	edge-1.dcloud.
Jan 25, 2020 03:18:54.284 PM			00:0C:BD:06:3...	hr1	Default >> D...	Default >> 802.1x HR	CAMPUS_USER_...		edge-1.dcloud.

Overview

Event	5200 Authentication succeeded
Username	hr1
Endpoint Id	00:0C:BD:06:3E:DA
Endpoint Profile	Microsoft-Workstation
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> 802.1x HR
Authorization Result	CAMPUS_USER_AUTHZ

Result

Class	CACS:1A007D6400000025DD48B016:Cisco-ISE/369344377/981
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 1021

Step 4 - Verification

show authentication sessions interface <no> details

```
edge-1#sh auth sessions  int gi1/0/10 det
            Interface:  GigabitEthernet1/0/10
               IIF-ID:  0x17A0B7CA
          MAC Address:  000c.bd06.3eda
         IPv6 Address:  fe80::1937:68ed:a3bd:1843
         IPv4 Address:  100.100.0.21
            User-Name:  hr1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  1A007D6400000025DD48B016
      Acct Session ID:  0x00000001
               Handle:  0x6b000002
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Local Policies:

Server Policies:
           Vlan Group:  Vlan: 1021


Method status list:
       Method           State
        dot1x           Authc Success
```


ISE – Active Directory Integration & Demo

ISE – AD PreRequisities

- Active Directory ports open between ISE and AD (LDAP: TCP/389, 3268, UDP/389 ▪ SMB: TCP/445 ▪ KDC: TCP/88 ▪ KPASS: TCP/464)
- Time sync between ISE and AD (Max ~5 min difference)
- ISE to resolve AD FQDN
- Active Directory Admin credentials to create computer accounts to join ISE

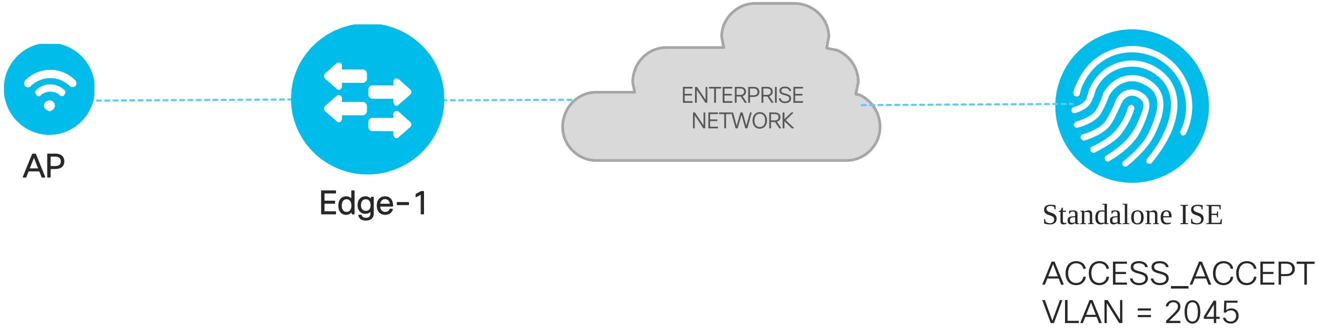
Case Study 2

Configuration Task

Access-point connected to Edge-1 port Gi1/0/1

Configure ISE to dynamically assign the access-points to AP vlan 2045.

Use MAB as the access-point is not capable of 802.1x



CCIE Lab-only

Steps:

1) NAD (Network access device) Configuration

2) ISE configuration

- Add NAD on ISE
- ID Store
- Authorization Profile (Elements)
- Authentication Policy
- Authorization Policy

3) Verification

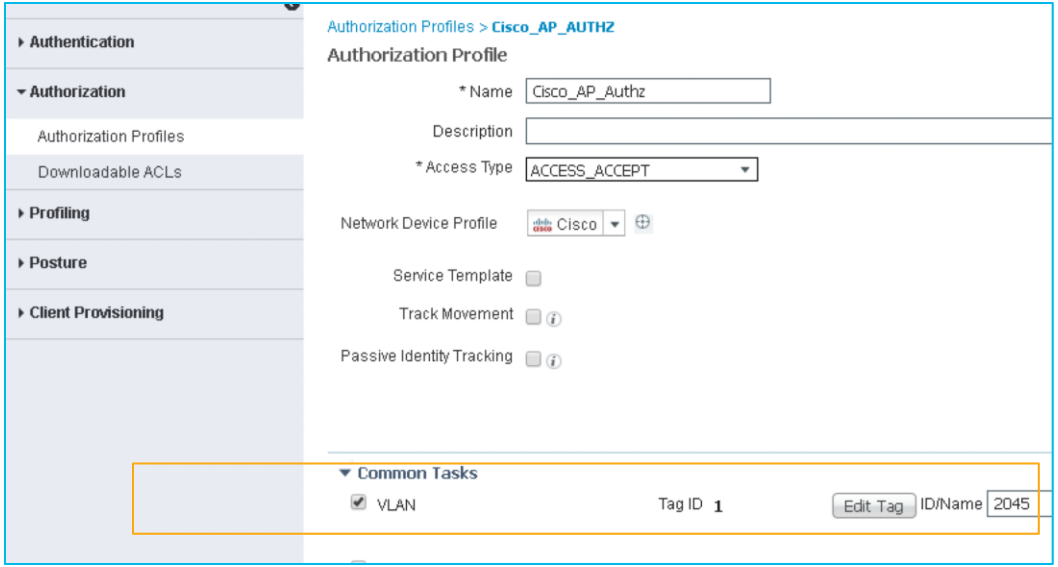
CCIE Lab-only

Switch configuration – Interface

```
interface GigabitEthernet1/0/1
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab**
authentication priority dot1x mab**
authentication port-control auto
mab
dot1x pae authenticator**
```

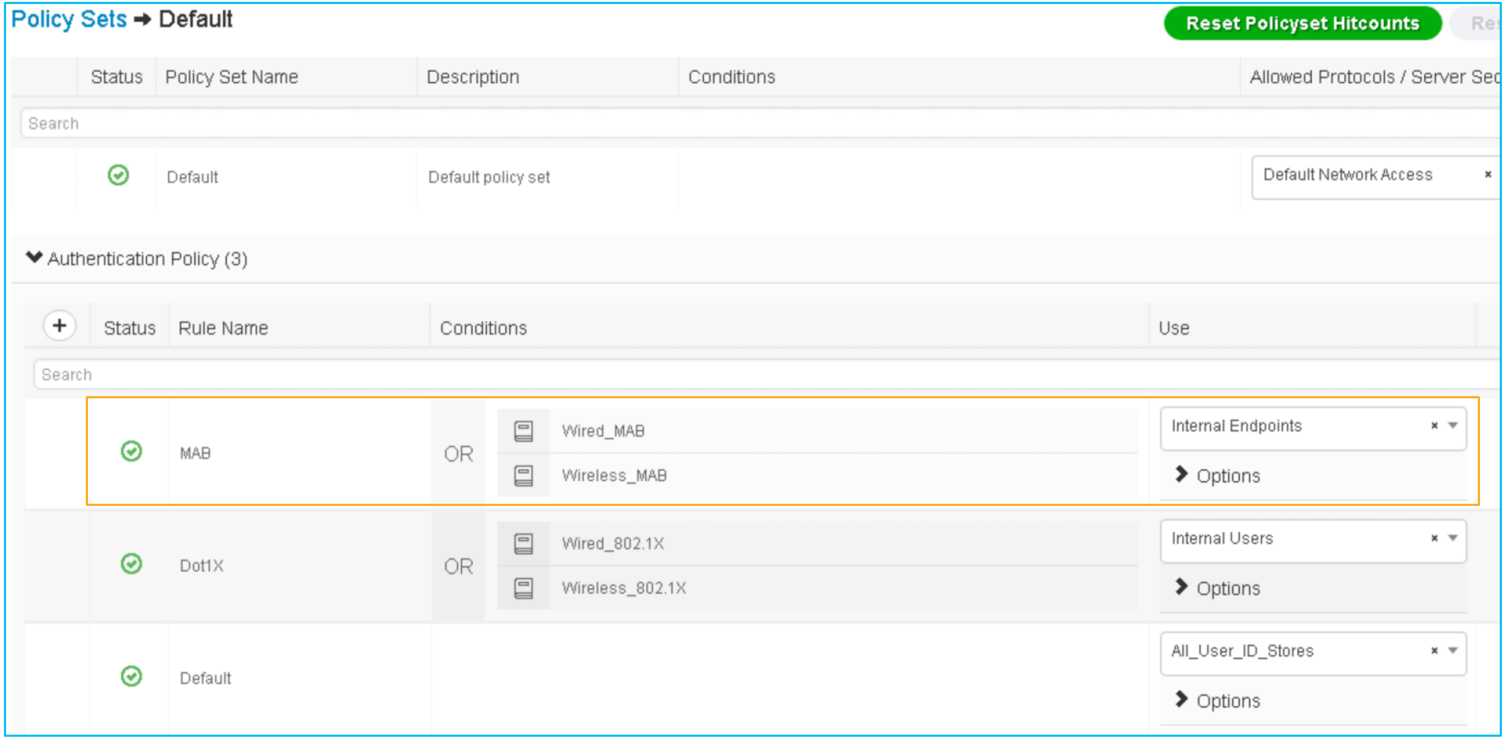
***Optional*

ISE authorization profile



Step 2 - ISE Policy Configuration

Leverage Default Policy set on ISE



Step 2 - ISE Policy Configuration

Authorization Policy to match on the access-point endpoint policy

Authorization Policy (5)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
	802.1x HR	IdentityGroup·Name **EQUALS** User Identity Groups:HR	CAMPUS_USER_AUTHZ	Select from list	2	
	Profiled Cisco IP Phones	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones	Select from list	0	
	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0	
	Profiled Cisco APs	EndPoints·EndPointPolicy **EQUALS** Cisco-Device:Cisco-Access-Point	Cisco_AP_Authz	Select from list	0	
	Default		DenyAccess	Select from list	87	

Verification

	Time	Status	Details	Endpoint ID	Identity	Endpoint P...	Authenticat...	Authorization Policy	Authorization Pr...
×				Endpoint ID	Identity	Endpoint Prof	Authenticatior	Authorization Policy	Authorization Profile
	Jan 25, 2020 05:17:06.773 PM			78:72:5D:3F:A1...	78:72:5D:3F:A1:FA	Cisco-AP-Air...	Default >> M...	Default >> Profiled Ci...	Cisco_AP_Authz
	Jan 25, 2020 05:16:48.730 PM			78:72:5D:3F:A1...	78:72:5D:3F:A1:FA	Cisco-AP-Air...	Default >> M...	Default >> Profiled Ci...	Cisco_AP_Authz

```
edge-1#show authentication sessions int gi1/0/1 details
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x1D3C810E
          MAC Address:  7872.5d3f.a1fa
         IPv6 Address:  fe80::7a72:5dff:fe3f:a1fa
         IPv4 Address:  192.168.0.101
            User-Name:  78-72-5D-3F-A1-FA
          Device-type:  Cisco-AIR-LAP
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  1A007D6400000067DDB4523B
      Acct Session ID:  0x00000004
               Handle:  0x5a000008
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Local Policies:

Server Policies:
           Vlan Group:  Vlan: 2045


Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

CCIE Lab-only

Steps:

1) Device Configuration
2) ISE configuration
    - Authorization Profile (Elements)
    - Add NAD on ISE
    - Authentication Policy
    - Authorization Policy
3) Configure the 802.1x supplicant
4) Verification

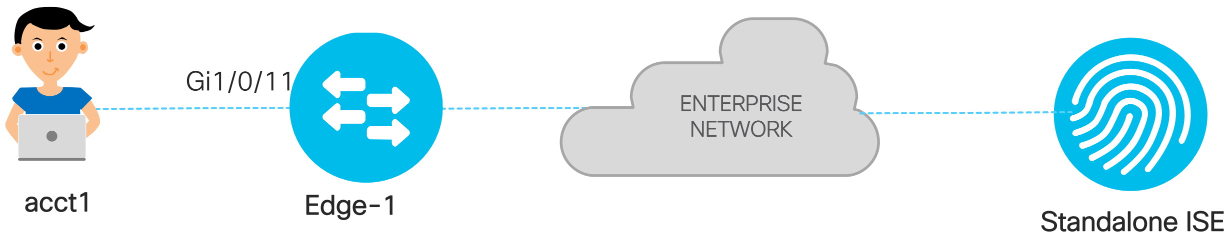
Case Study 3

Troubleshooting Task

“acct1” user is connecting to Edge-1 port Gi1/0/11

After implementing 802.1x on the switch, the “acct” user is not able to ping public DNS server 8.8.8.8

Your goal is to troubleshoot the issue on ISE and switch to make sure acct1 can ping the server 8.8.8.8



Troubleshooting Methodology:

1) Connect the client to replicate the issue

2) ISE Live Logs. Check the policy matched on the user and the attributes pushed by ISE

3) Switch **“show authentication session int gi1/0/11 details”** to view the server attributes. Check if any of the dynamic attributes pushed by ISE or configuration on the switch is blocking the server connection.

4) **“terminal monitor”** on the switch if necessary.

5) **“debug icmp trace”** if necessary, on the switch

6) Remove dot1x on the port to validate if dot1x is causing the issue – Issue Isolation

Case Study 3

ISE Logs

Refresh | Reset Repeat Counts | Export To | Filter

	Time	Status	Details	Endpoint ID	Identity	Endpoint P...	Authenticat...	Authorization Policy	Authorization Pr...
×				Endpoint ID	Identity	Endpoint Prof	Authenticatior	Authorization Policy	Authorization Profile
	Jan 25, 2020 08:51:48.662 PM			00:0C:BD:06:3...	acct1		Default >> D...	Default >> 802.1x AC...	ACCT_USER_AU...
	Jan 25, 2020 08:51:47.293 PM				#ACSACL#-IP-DE...				
	Jan 25, 2020 08:51:47.288 PM			00:0C:BD:06:3...	acct1		Default >> D...	Default >> 802.1x AC...	ACCT_USER_AU...

Overview

Event	5200 Authentication succeeded
Username	acct1
Endpoint Id	00:0C:BD:06:3E:DB
Endpoint Profile	
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> 802.1x ACCT
Authorization Result	ACCT_USER_AUTHZ

Result

Class	CACS:1A007D6400000068DE796EA6:Cisco-ISE/369344377/3222
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 1021
EAP-Key-Name	19:5e:2c:ae:ee:74:e0:ac:35:7e:dc:53:bc:27:8d:a0:d4:4a:ad:55:96:04:50:3a:d0:bd:a1:bf:0c:65:f6:9b:29:5f:59:31:12:b3:b9:7d:7c:18:39:d8:e2:5b:aa:34:8b:77:06:66:33:0b:f5:a1:39:0c:cf:a1:51:40:45:a0:10
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-DENY_ALL_TRAFFIC-57f6b0d3
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Case Study 3

Switch output

```
edge-1#sh authentication sessions int gi1/0/11 details
            Interface:  GigabitEthernet1/0/11
               IIF-ID:  0x17CA5D7F
          MAC Address:  000c.bd06.3edb
         IPv6 Address:  fe80::e0da:d97b:5c0:d6d4
         IPv4 Address:  169.254.214.212
            User-Name:  acct1
          Device-type:  Un-Classified Device
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  1A007D6400000068DE796EA6
      Acct Session ID:  0x00000005
               Handle:  0x50000009
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Server Policies:
           Vlan Group:  Vlan: 1021
              ACS ACL: xACSACLx-IP-DENY_ALL_TRAFFIC-57f6b0d3


Method status list:
       Method           State
        dot1x           Authc Success
```

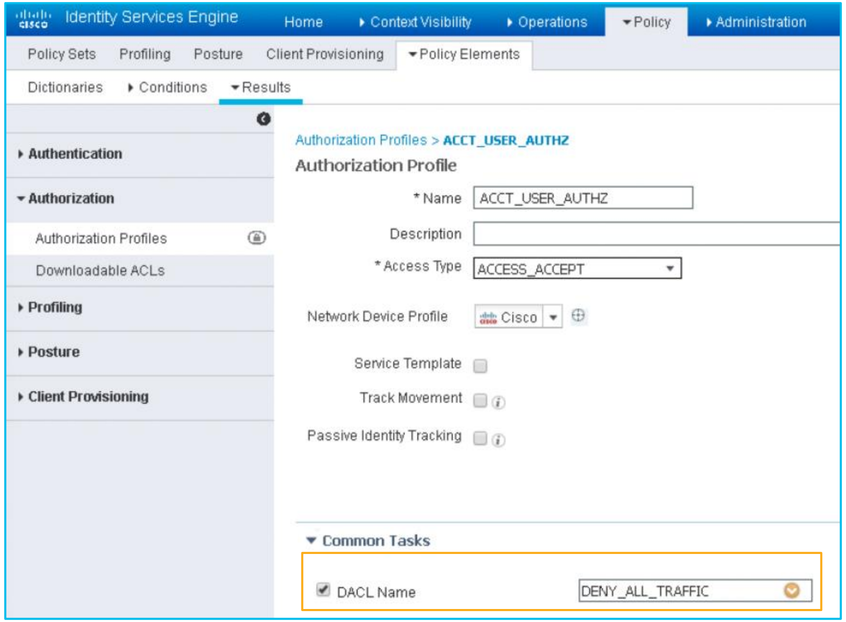
```
edge-1#show ip access-lists xACSACLx-IP-DENY_ALL_TRAFFIC-57f6b0d3
Extended IP access list xACSACLx-IP-DENY_ALL_TRAFFIC-57f6b0d3
    1 deny ip any any
edge-1#
```

Case Study 3

Solution

Issue: ISE pushing DACL – **deny ip any any**

Fix – Remove the DACL from the authorization result or push **“permit ip any any”**



NAD Device configuration - WLC

CCIE Lab-only

For your reference

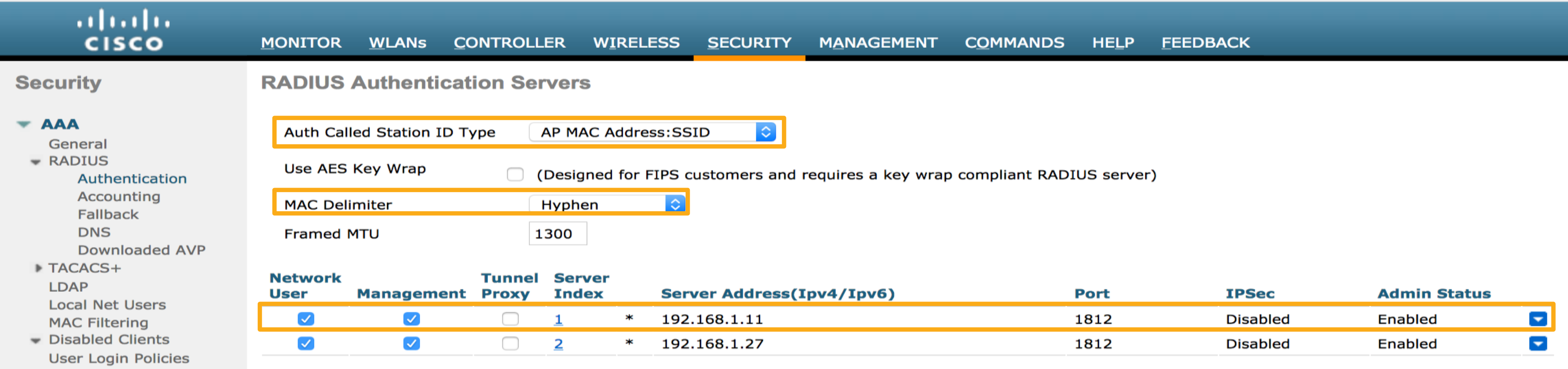
- Every ISE flow can be accomplished with one fixed set of WLC configuration
- They can be broken into:
  - AAA server config
  - SSID Authentication config
  - SSID Advanced config

Production Best Practice

WLC configuration – AAA Server config

For your reference

- Define the ISE PSN in the Authentication and Accounting section under Security>AAA > RADIUS
- Set "Support for CoA" to Enabled in server definition
- Set "Called Station ID type to AP MAC Address:SSID in both sections
- Set MAC Delimiter to "Hyphen" in both sections

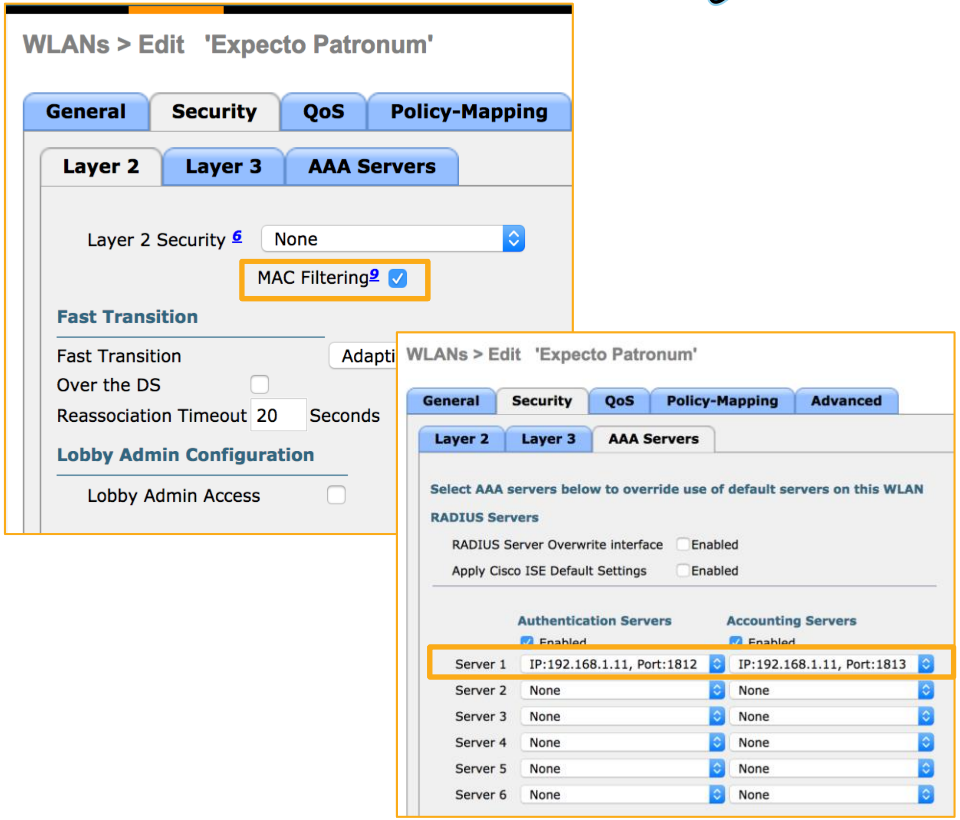


WLC configuration – SSID Authentication

Production Best Practice

For your reference

- Configure Layer 2 authentication as per the question.
- Enable “MAC filtering” if Guest flow is required.
- Select ISE PSN for authentication and account under the “AAA Server” tab

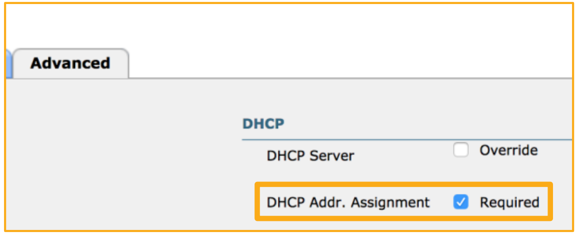


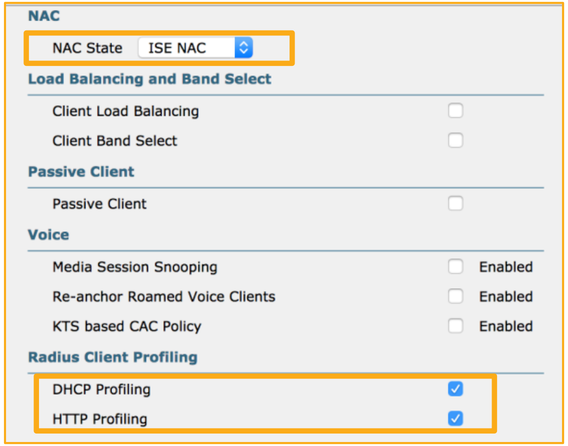
WLC configuration – SSID Advanced

Production Best Practice

For your reference

- Enable “DHCP Addr. Assignment”
- Set “NAC State” to ”ISE NAC”
- Enable DHCP Profiling and HTTP profiling





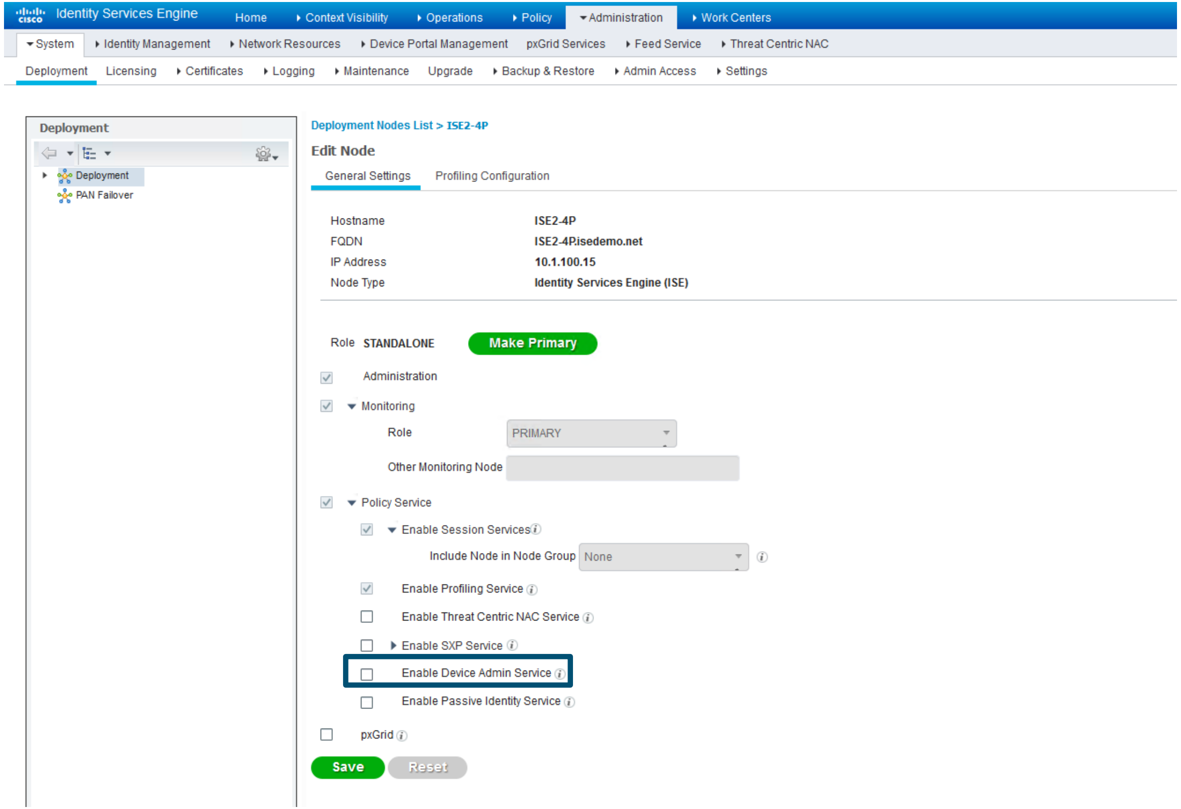
TACACS
Device Administration

Comparison: TACACS+ and RADIUS

	TACACS+	RADIUS
Transmission Protocol	TCP	UDP
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813
Intended Purpose	Device management	User access control
Encryption	Full packet encryption	Encrypts only passwords up to 16 bytes
AAA Architecture	Separate control of each service: authentication, authorization, and accounting	Authentication and authorization combined as one service

TACACS+ Configuration steps

- Enable TACACS+ services
- Determine ID Store
- Register NAD with ISE
- Policy Elements
  - TACACS Profiles
  - Command Sets
- Policy Set Configuration
- Configure NAD



TACACS Profile Example

Task Type

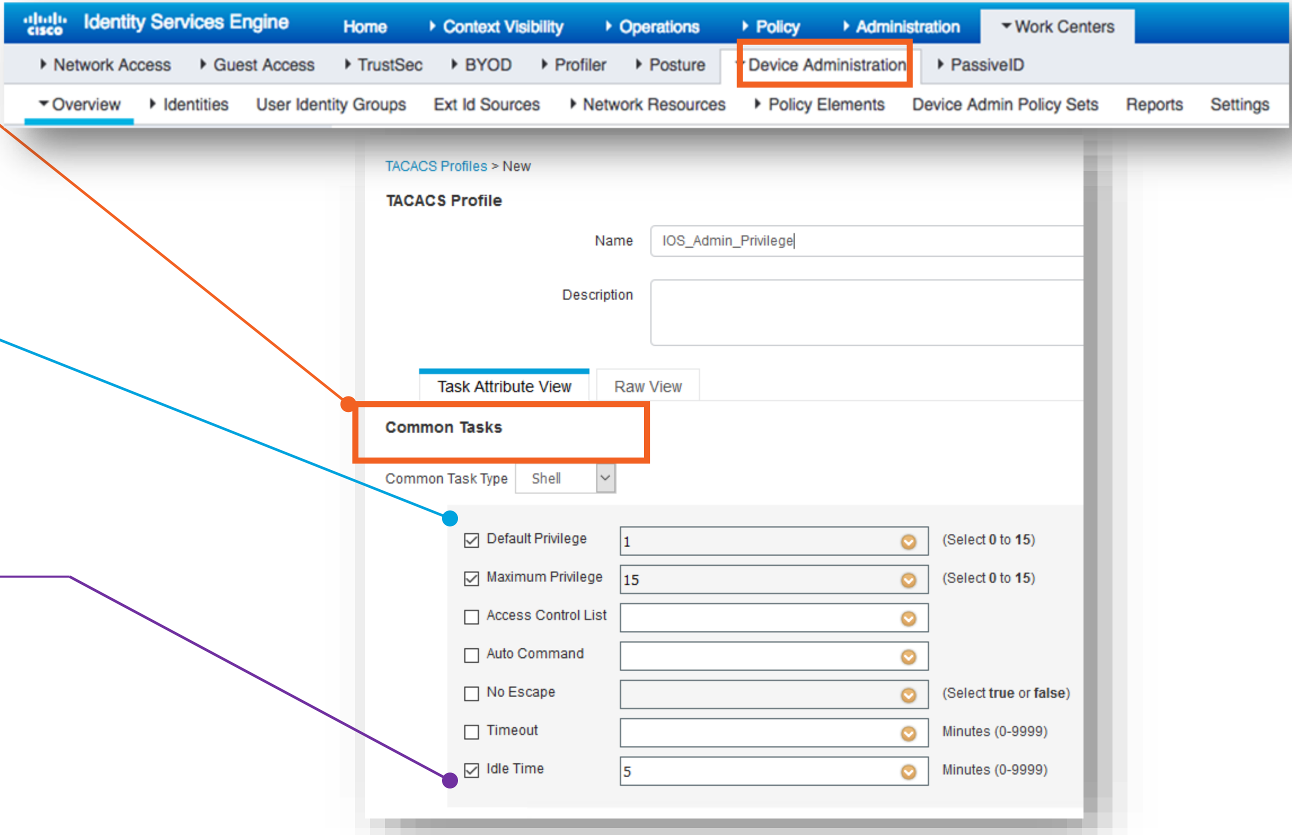
Specific for the Device Is a nice UI feature, to provide specific UI per device type

IOS Privilege Level

Default = Assigned at Login
Max = Limit with "enable" command

Idle Time

For High-Powered Access, Limit the session time when no activity



Command Set

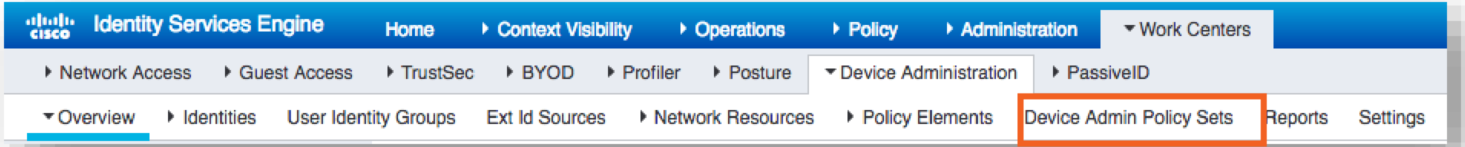
Commands

Permit any command that is not listed below ☐

Add | Trash | Edit | Move Up | Move Down

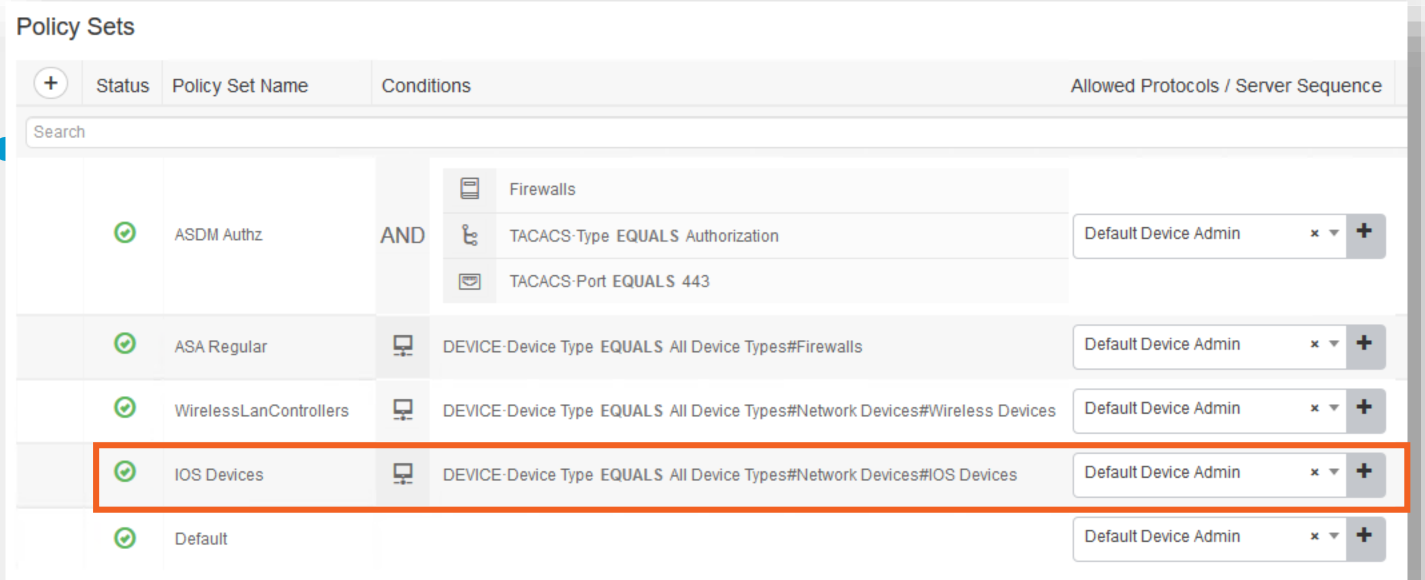
Grant	Command	Arguments
PERMIT	show	running-config
PERMIT	show	interface
PERMIT	configure	terminal
PERMIT	interface	
PERMIT	no	authentication port-control
PERMIT	exit	

Device Admin Policy Sets (TACACS+)



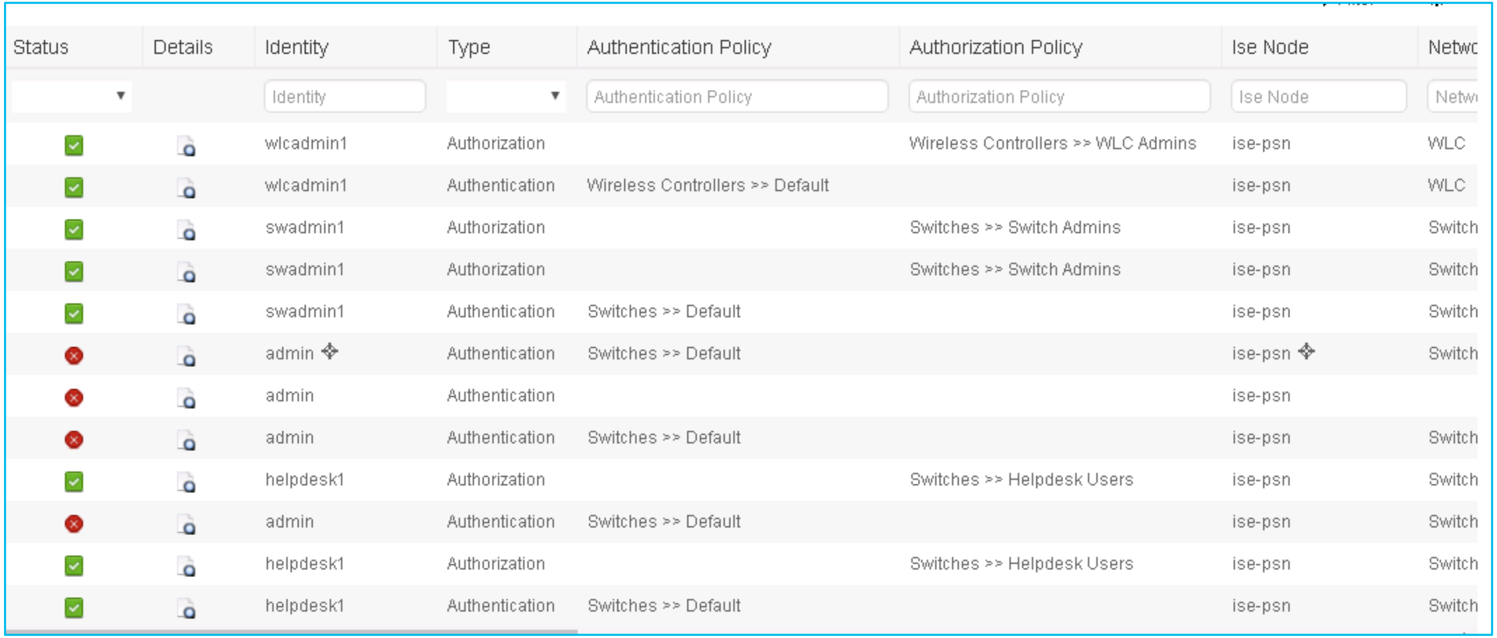
Policy Set Ordered List

Provides both Management AND Execution order



TACACS Monitoring

TACACS Device Admin is monitored through a separate Live Log



Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Netwo
		Identity		Authentication Policy	Authorization Policy	Ise Node	Netw
		wlcadmin1	Authorization		Wireless Controllers >> WLC Admins	ise-psn	WLC
		wlcadmin1	Authentication	Wireless Controllers >> Default		ise-psn	WLC
		swadmin1	Authorization		Switches >> Switch Admins	ise-psn	Switch
		swadmin1	Authorization		Switches >> Switch Admins	ise-psn	Switch
		swadmin1	Authentication	Switches >> Default		ise-psn	Switch
		admin	Authentication	Switches >> Default		ise-psn	Switch
		admin	Authentication			ise-psn	
		admin	Authentication	Switches >> Default		ise-psn	Switch
		helpdesk1	Authorization		Switches >> Helpdesk Users	ise-psn	Switch
		admin	Authentication	Switches >> Default		ise-psn	Switch
		helpdesk1	Authorization		Switches >> Helpdesk Users	ise-psn	Switch
		helpdesk1	Authentication	Switches >> Default		ise-psn	Switch

Case Study 5

Configuration Task 1

Local login has been used to login to the devices so far.

Your goal is to configure device administration on Edge-1.

Helpdesk user (helpdesk/C1sco12345) should be able to receive privilege 15 but only able to permit “show” commands.

Network admin (netadmin/C1sco12345) should be able to execute all commands and have highest privilege.

Task 2

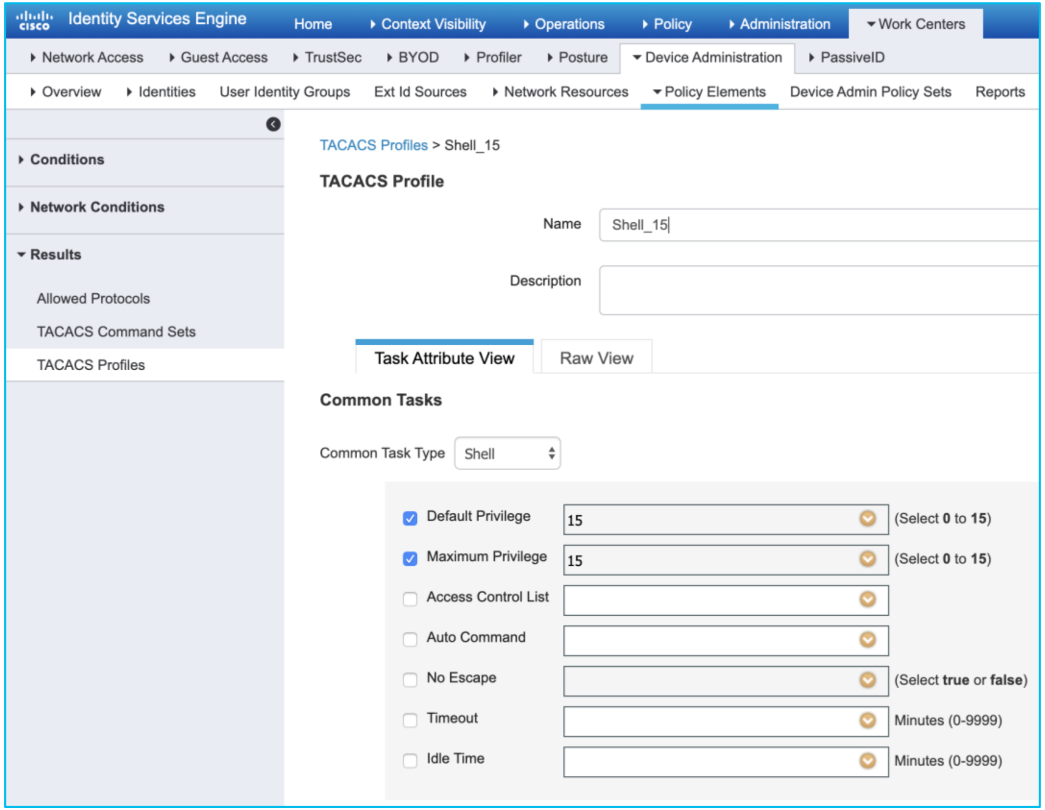
All commands executed need to be accounted for future audits.

Switch Configuration

```
! Configure TACACS server and server group on Edge-1

tacacs server tacacs_100.64.0.100
 address ipv4 100.64.0.100
 key 7 15315A1F07257A767B6760
 timeout 4

aaa group server tacacs+ tacacs-group
 server name tacacs_100.64.0.100

! TACACS for login, shell and command authorization

aaa authentication login VTY_authen group tacacs-group local
aaa authorization exec VTY_author group tacacs-group none
aaa authorization commands 0 VTY_cmd group tacacs-group none
aaa authorization commands 1 VTY_cmd group tacacs-group none
aaa authorization commands 15 VTY_cmd group tacacs-group none

! TACACS command accounting

aaa accounting exec default start-stop group tacacs-group
aaa accounting commands 0 default start-stop group tacacs-group
aaa accounting commands 1 default start-stop group tacacs-group
aaa accounting commands 15 default start-stop group tacacs-group
```

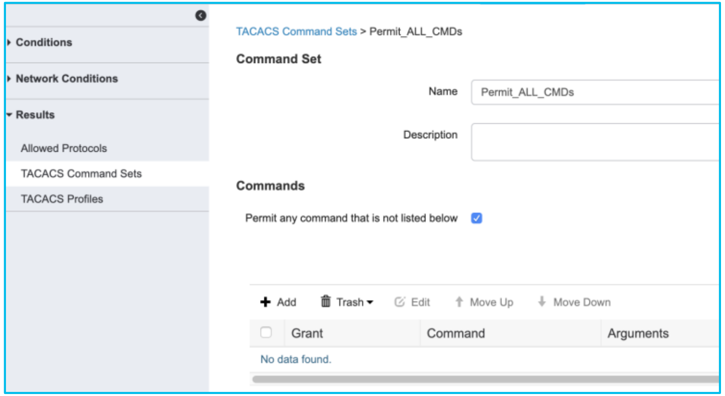
```
! Calling the TACACS method lists in line VTY

line vty 0 15
 authorization commands 0 VTY_cmd
 authorization commands 1 VTY_cmd
 authorization commands 15 VTY_cmd
 authorization exec VTY_author
 login authentication VTY_authen
 transport input all
```

ISE Configuration

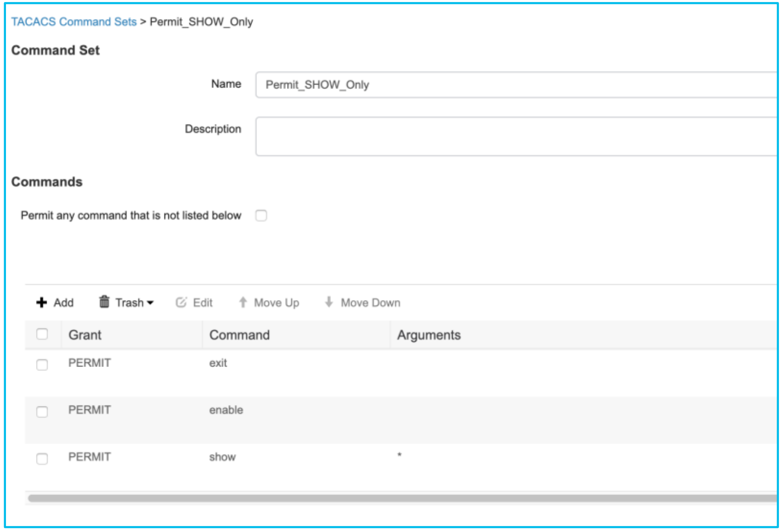


ISE Configuration

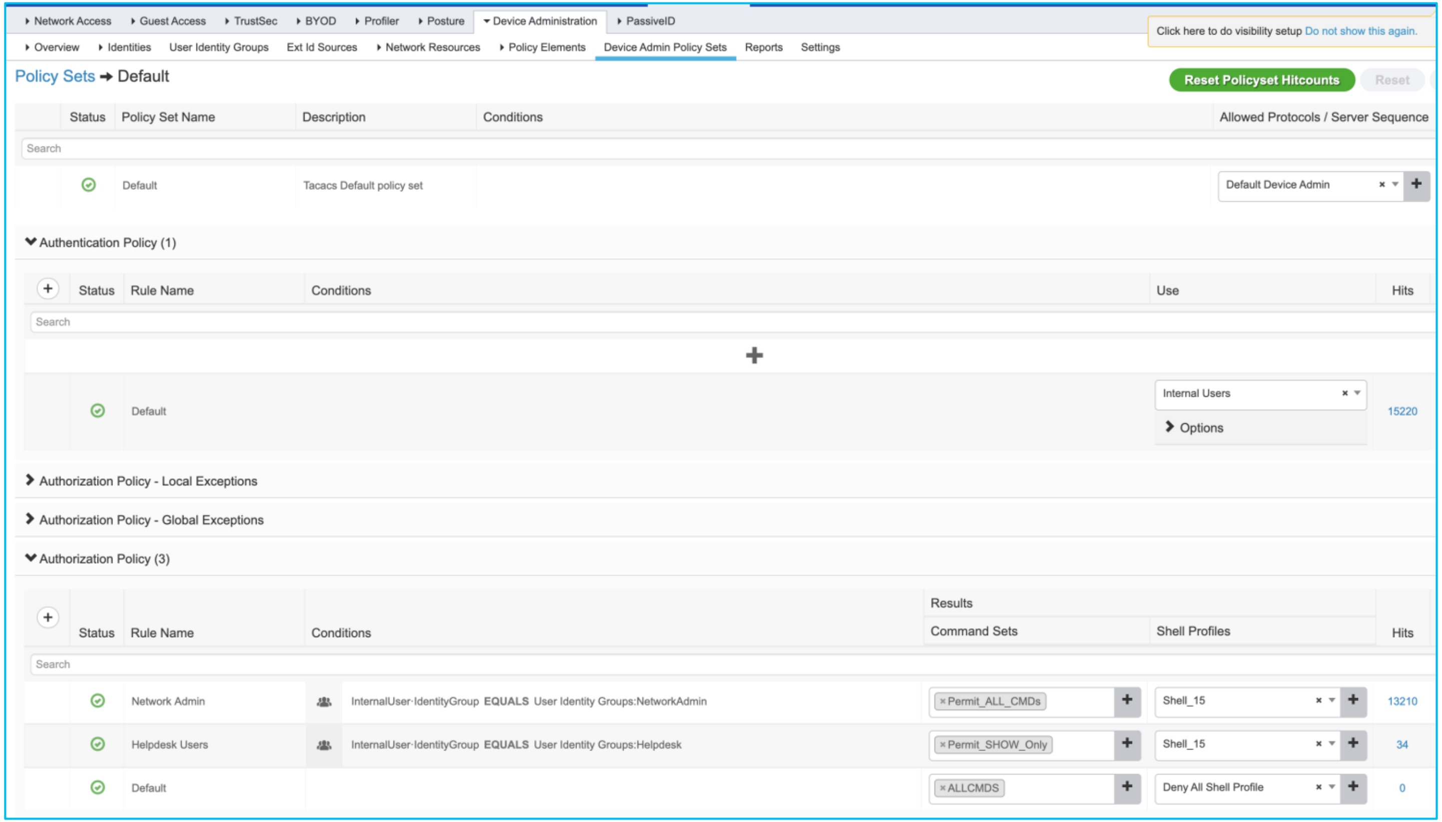
Permit All Command set



Read-Only Command set



ISE Configuration



Verification

netadmin

```
$ ssh netadmin@100.124.1.1
Password:


edge-1>
edge-1>en
Password:
edge-1#show priv
Current privilege level is 15
edge-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
edge-1(config)#int gi1/0/5
edge-1(config-if)#shut
edge-1(config-if)#no shut
edge-1(config-if)#end
edge-1#
edge-1#
```

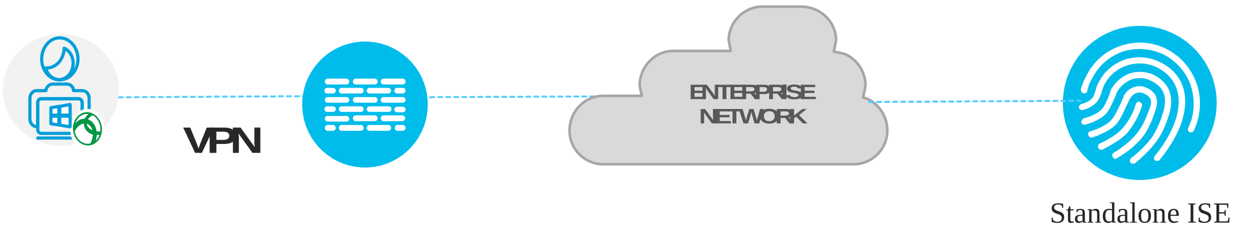
helpdesk

```
$ ssh helpdesk@100.124.1.1
Password:
edge-1#
edge-1#
edge-1#
edge-1#conf t
Command authorization failed.

edge-1#exit
Connection to 100.124.1.1 closed by remote host.
Connection to 100.124.1.1 closed.

[Sun Jan 26 10:08:54 UTC] maglev@100.64.0.101 (maglev-master-100-64-0-101) ~
$
```


Case Study 4

VPN user is authenticating with ISE but unable to connect to the network

Troubleshoot the issue and make sure the VPN user is able to connect

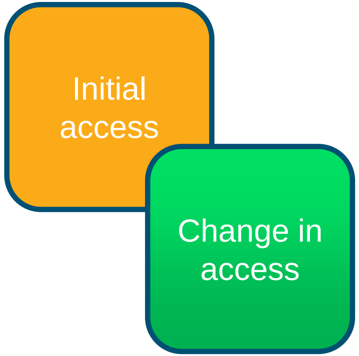


Troubleshooting Methodology:

1. Check configuration on ASA
2. Syslogs on ASA
3. ISE Live logs to see the policy match and the failure message
4. **“user is disabled”? – Enable the User on ISE**
5. **No debugs on ISE – too risky**

Change of Authorization (CoA)

RFC 5176



RADIUS CoA (Change of Authorization) is a feature that allows ISE to adjust an active client session.

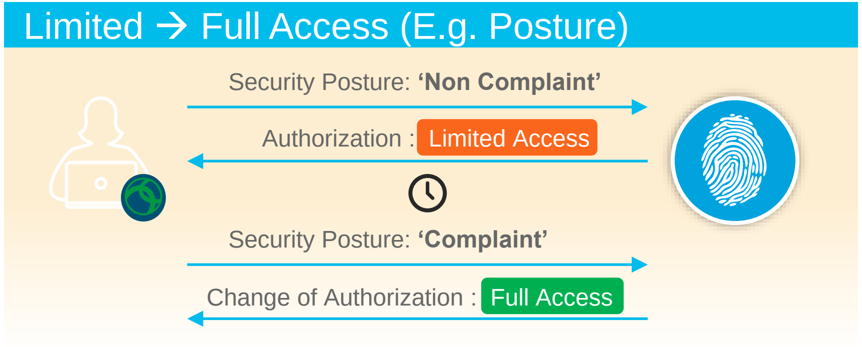
Requires endpoint's 'active session' on ISE

Automatic / Manual initiation of CoA

Use cases:
- Central Web Authentication (CWA)
- Device Profiling
- Posture assessment
- Threat Centric NAC
- Adaptive Network Control and more

Change of Authorization (CoA)

- Central Web Authentication
  - Guest Access
  - Bring your Own device flows
  - Web notifications
- Posture Assessment
- Threat Centric NAC
- Adaptive Network Control
- Device Profiling
- Easy Connect



URL Re-direction ACL – Switch vs WLC

CCIE Lab-only

For your reference

- URL redirection is required for most advanced ISE flows
- Requires static ACL on network device
  - Defines what traffic should or should not be redirected.
- For lab, allow all traffic to ISE PSN
- Permit and Deny statements are switched (no pun intended) on a switch vs WLC

```
ip access-list extended redirect
 deny   ip any host 192.168.1.11
 deny   udp any any eq domain
 permit ip any any
```

Access List Name: redirect

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.11 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	192.168.1.11 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any
5	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

Ice see devices with Profiling

Understanding Profiling and configuring it quickly in the lab

What is profiling?

Collection

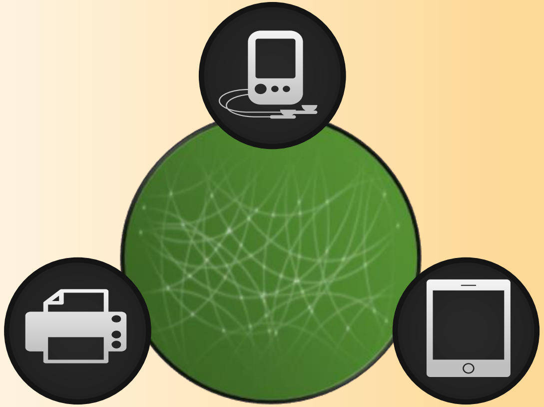
NMAP | Active Directory | NetFlow

HTTP | LLDP/CDP

Radius | SNMP | DHCP

- Process of collecting data to be used for identifying devices
- Uses Probes for collecting device attributes

Classification



Classifies based on Device fingerprint

Profiling Implementation

Profiling Services Configuration Flow

Probes Selection	Some probes are better suited to classify certain device types
↓	
Profiling Policies	Unknown devices policies creation or existing policies customization
↓	
Probes Activation and Configuration	Per PSN probe activation and network devices configuration (both ISE and NAD)
↓	
Authorization Policies	Authorization policies using profiling results as conditions

Probe Selection

Summary of Probe Usage

RADIUS	Useful to collect MAC (Vendor ID)/IP address and for Device Sensor
DHCP	One of the best Probe to collect Device/OS type information
SNMP	To collect CDP/LLDP information via MIBS (when device uses CDP/LLDP) Useful to build MAC/IP mapping table (ARP table) Useful to collect MAC/Port binding (SNMP-Traps)
HTTP	Best method to collect 'User agent' : OS version, Browser, ...
NMAP	Help to collect more information on the device, useful for OS identification (OS version, SNMP system description, ...) (ISE 2.1 Added SMB Discovery to NMAP Scanning)

Summary of Probe Usage (cont.)

DNS	Used to collect FQDN from IP address (reverse DNS lookup)
NETFLOW	Complementary profiling method for collecting traffic (Analysis of flow protocol or destination)
Active Directory	Gathers OS information from Active Directory, when hostname is available

Profiling Policies

Profiling Services Configuration Flow

Probes Selection	Some probes are better suited to classify certain device types
Profiling Policies	Unknown devices policies creation or existing policies customization
Probes Activation and Configuration	Per PSN probe activation and network devices configuration (both ISE and NAD)
Authorization Policies	Authorization policies using profiling results as conditions

Profiling Policy Terminology

Profiling Policy

Profiling Conditions

Dictionary Attribute = Value

Increase "Certainty Factor (CF)" & check next condition

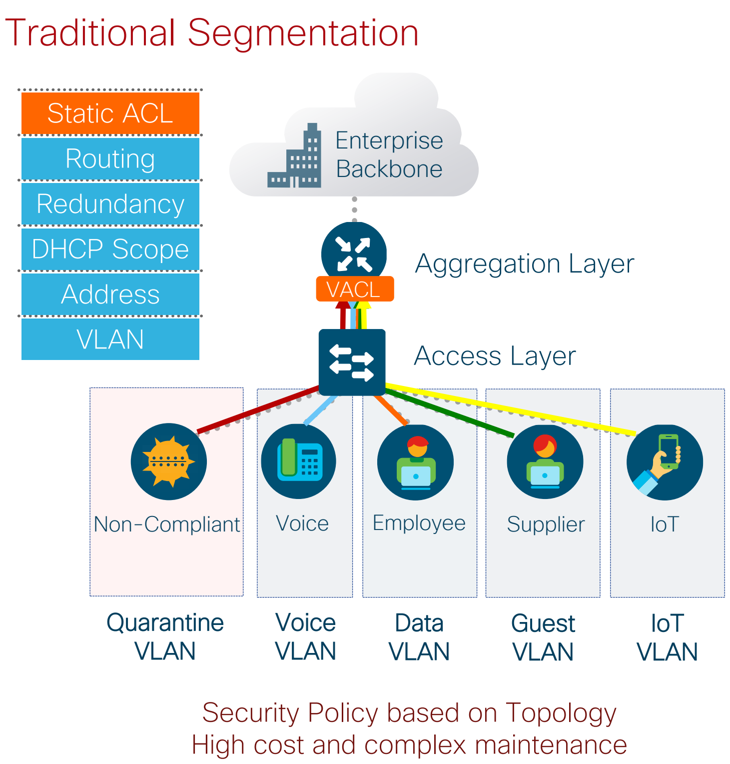
If "CF" > Threshold, Apply Profile & Optionally Assign Endpoint to Group

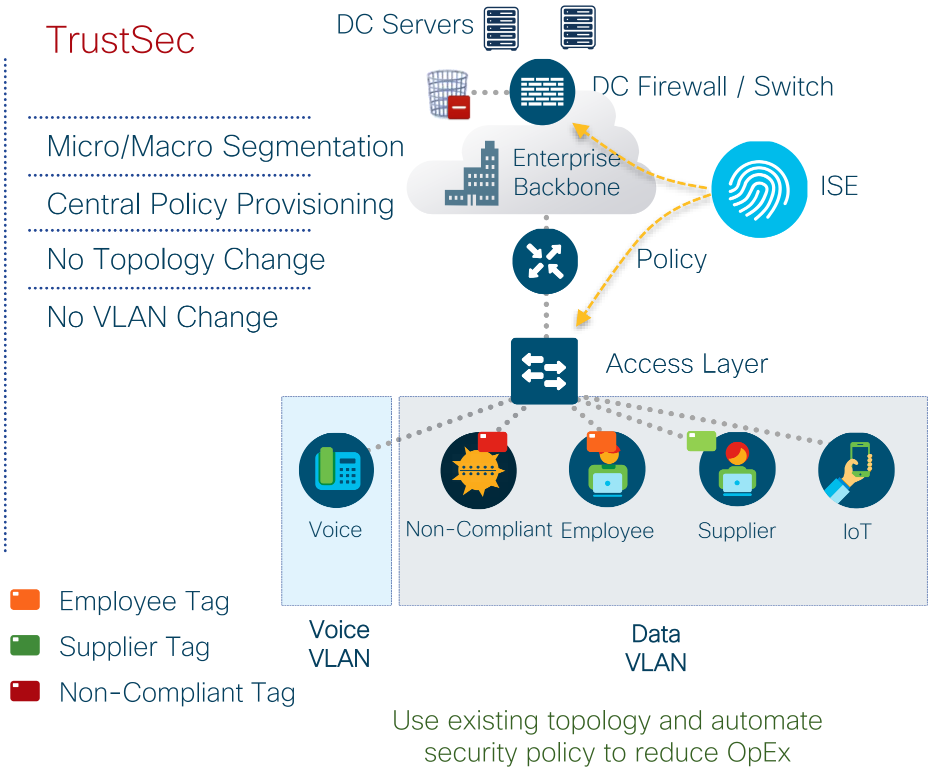
Profiling Policy Terminology

- Dictionary Attributes – attributes that can be collected by probes (e.g. MAC OUI, RADIUS Calling-station-id, IP User-Agent…)
- Profiling Conditions – matches a collected value against a dictionary attribute (e.g. User-Agent CONTAINS Android, OUI CONTAINS Apple, dhcp-class-identifier CONTAINS CP-9971…). You can use the existing ones or create your own.
- Profiling Policy – defines a set of rules for an endpoint to be considered a match. It is possible for the same device to match rules on multiple profiling policies.
- Certainty Factor (CF) – each rule within a profiling policy results in a CF assignment, a minimum cumulative CF is required in order to match a device into a profiling policy. Highest CF will determine which profile a device will match.
- Exception Action – used to statically assign an endpoint to a policy when a profiling condition is met

Cisco TrustSec

SGTs simplifies segmentation and access control



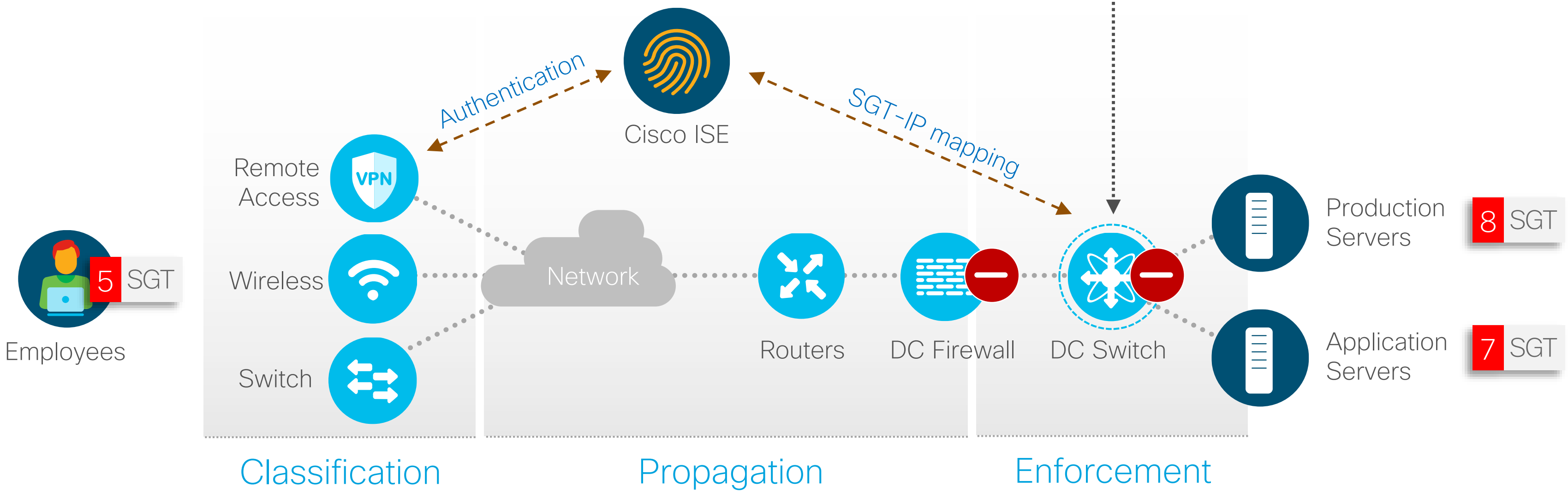


Segmenting with Security Group Tags (SGTs)

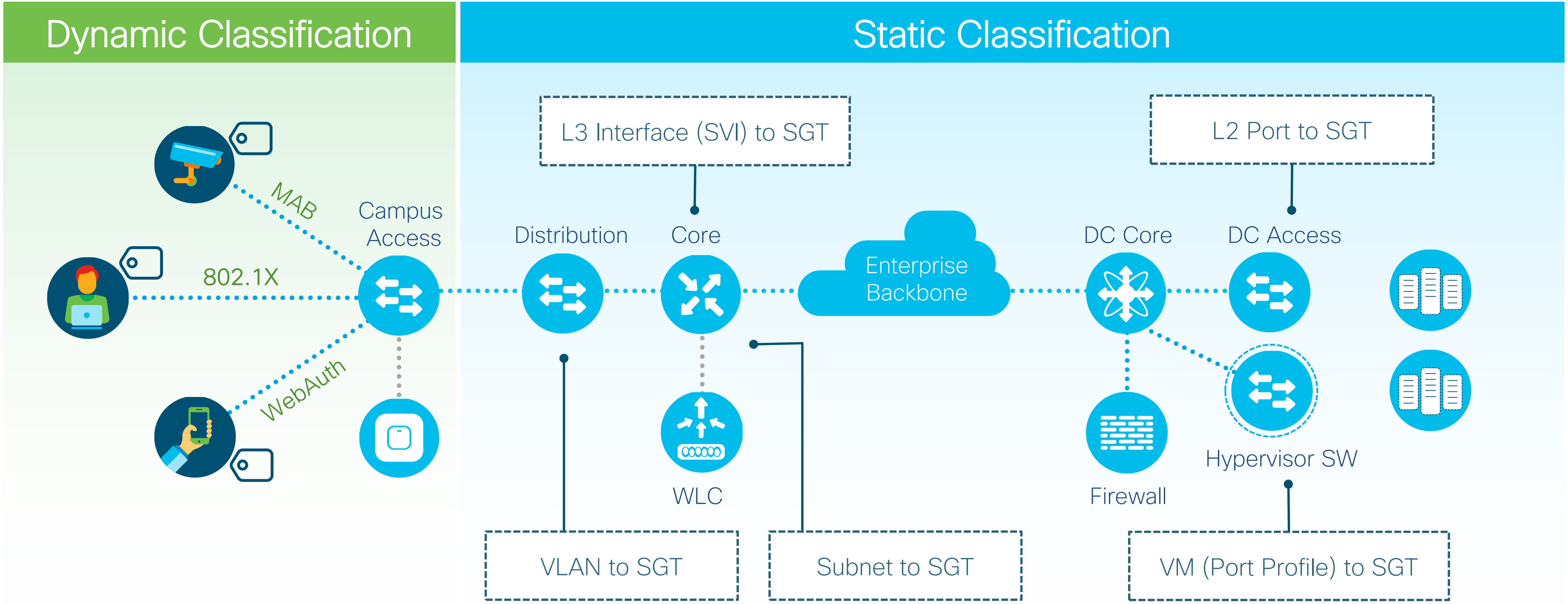
Destination

Egress Policy	App_Serv	Prod_Serv
Employee	Permit All	Deny All
App_Serv	Permit All	Deny All
Prod_Serv	Deny All	Permit All

Source

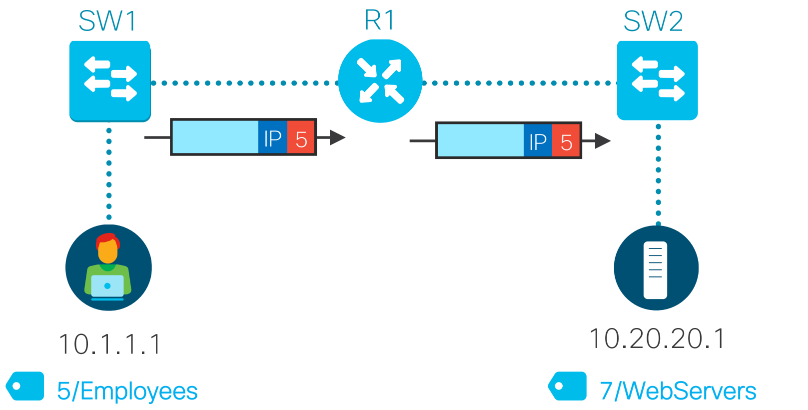


Classification



Two ways to propagate

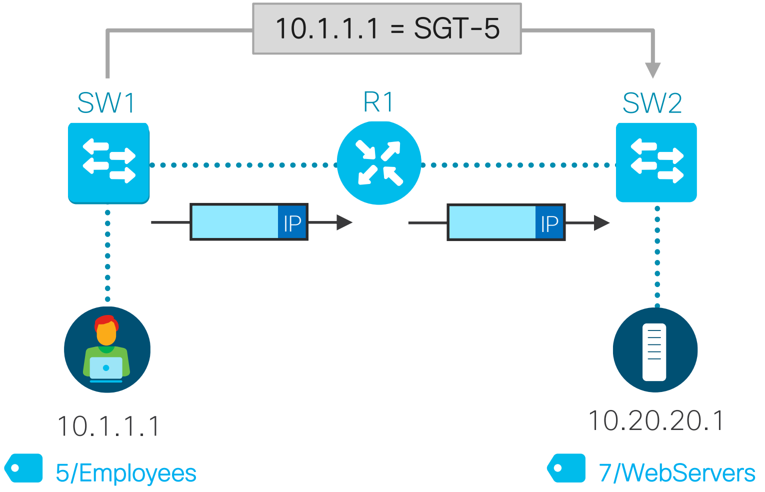
DATA PLANE PROPOGATION



SGT carried inline in the data traffic. Methods include, SGT over:

- Ethernet
- MACSec
- LISP/VxLAN
- IPSec
- DMVPN
- GETVPN

CONTROL PLANE PROPOGATION



IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over:

- SXP
- pxGrid

Summary

- Disable features that can cause problems with troubleshooting
- Use pre-built elements to your advantage
- Keep device config simple
- Understand what probes are required for profiling but enable all probes in the lab.
- Keep it simple ! ISE is easy and will save you a lot of time in the lab.

Thank you

TECCCIE-3202

PKI based IPsec Authentication

Jay Young – Technical Leader.Customer Delivery

Barcelona | January 27-31, 2020

Agenda

- What is PKI
- Configure PKI
- IKEv1/2
- Configuration DMVPN

What is PKI

Breaking down the AAA

- AAA is a combination of the following three concepts
  - Authentication (AuthC) – Who somebody is
  - Authorization (AuthZ) – What is that person allowed to do
  - Accounting - Recording what that person did and when

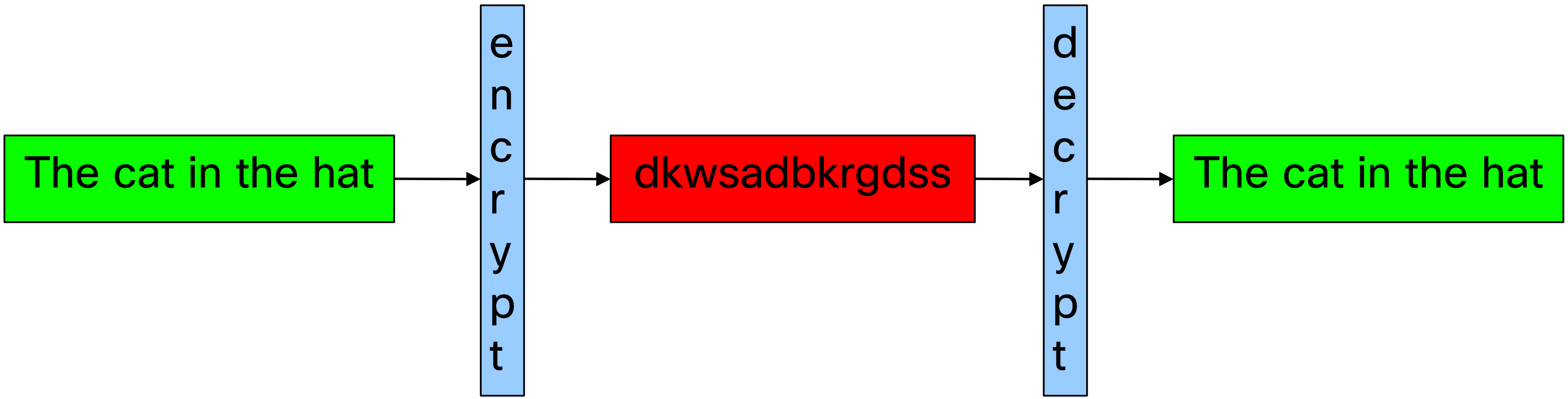
- PKI (Public Key Infrastructure) is only used to authenticate (AuthC)!
  - PKI is simply a mechanism to confirm that a public key belongs to a specific person. Protocols like IKE, SSL and email leverage this assertion to perform the authentication.

Cryptography concepts

- Confidentiality – Doesn't allow original message to be read
  - Cipher – A method that provides confidentiality
- Integrity – Confirms that this message hasn't been altered in transit
  - Hash – A method that verifies originality
- Non-repudiation – Confirms that the message was sent by only the sender
  - Digital Signature – A method that provides non-repudiation

Confidentiality

- Cryptography at it's base is a process that you apply to a message so that it can provide confidentiality.
- In most cases it will be a message transferring from person A to person B and it needs to be guaranteed that no other person can read the message even if it was intercepted.

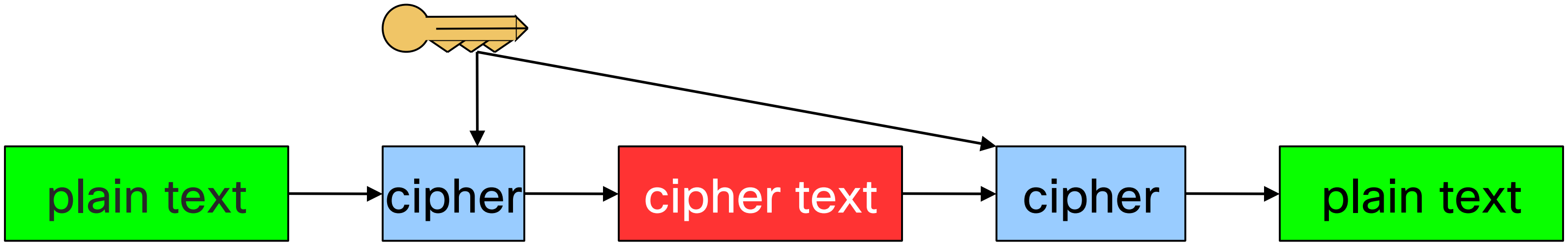


Encryption

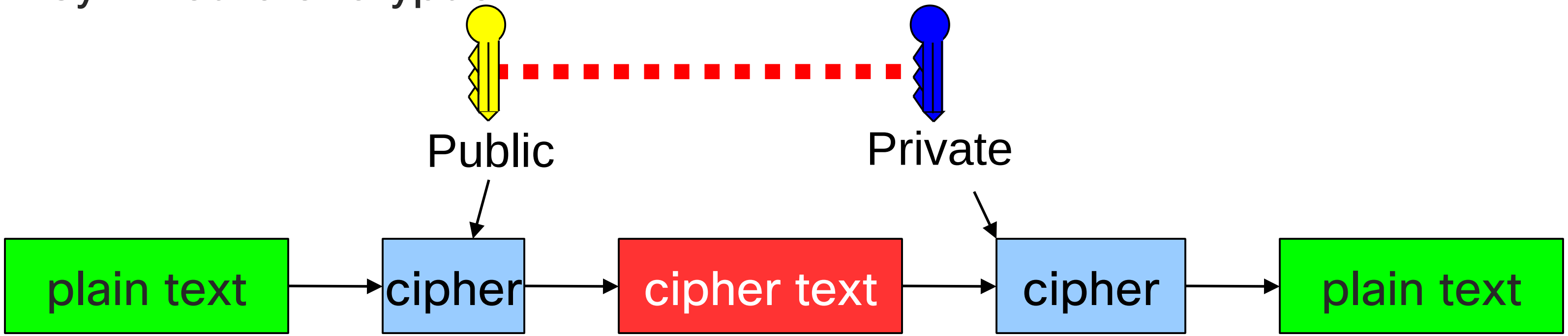
- There are two ways to encrypt data: symmetrically or asymmetrically
- Symmetric encryption - the same key is used for encryption as is used for decryption.
  - Example ciphers: RC4, DES, 3DES, AES
- Asymmetric encryption – a different key is used for encryption as decryption.
  - Examples ciphers: RSA, DSA, ECDSA

Encryption

Symmetric encryption



Asymmetric encryption



Integrity

- Integrity is a way of detecting that a message has not been tampered with, altered, or corrupted during its transmission from A to B. Please note that this provides no confidentially
- Commonly uses for integrity:
  - Plastic rings on caps of soda bottles.
  - Foil covering of medicine bottles
  - CRC checks of Ethernet frames
- In terms of computer data integrity we use a process called hashing to detect if even one single bit of a file or packet has been changed.

Hashing

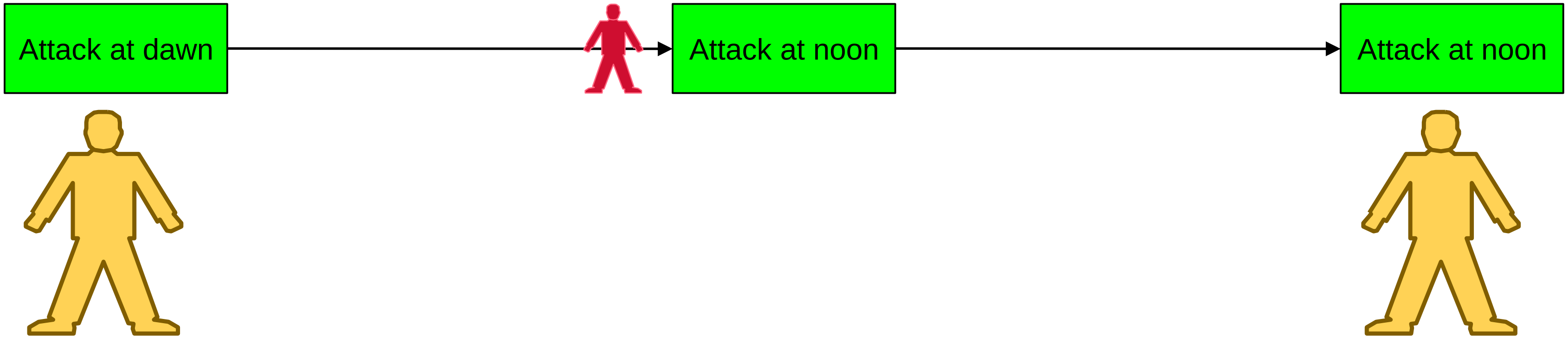
- To determine whether or not the data has changed we need a process that will take, as input, an arbitrary amount of data and generate a fixed length value. It also needs to meet these four requirements:
    - it is easy to compute the hash value for any given message
    - it is infeasible to find a message that has a given hash,
    - it is infeasible to modify a message without changing its hash,
    - it is infeasible to find two different messages with the same hash.
- "infeasible" means that it would take all the computers in the world a couple thousand years

Hashing

- A few examples of hashing algorithms include:
- MD4/5 – Message Digest Algorithm
- SHA-1/2/3 – Secure Hashing Algorithm
- RIPEMD – RACE Integrity Primitives Evaluation Message Digest
- Whirlpool

Non-repudiation

- Non-repudiation is confirmation that the sender of the message did indeed send it and the messages content has not been altered in transit.
- If an attacker intercepts the message he/she can alter the message. The receiver will not know that the message has been changed without non-repudiation.



Digital Signature (creation)

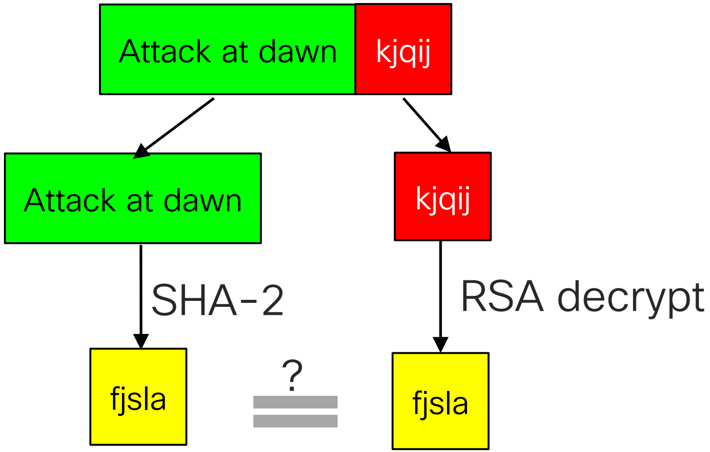
- Using a combination of hashing and asymmetric encryption we can receive a message, verify that it was sent by the sender and it hasn't be altered in transit.
- Sender Step 1) Generate a hash of the message

- Sender Step 2) Encrypt the hash with sender’s private key

- Sender Step 3) Append the signature to the message and transmit

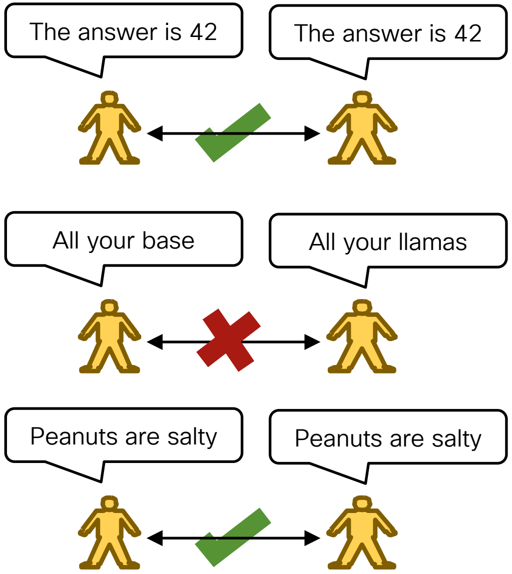
Digital Signature (validation)

- Receiver steps:
- Separate message from signature
- Compute hash on message
- Decrypt the signature with the senders public key
- Compare decrypted fingerprint against computed hash

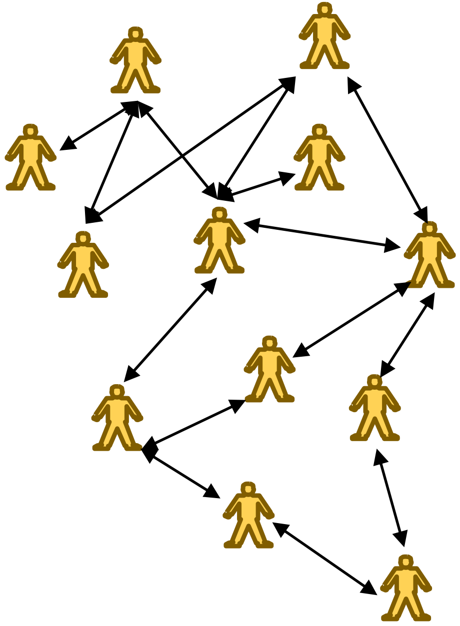


Trust models

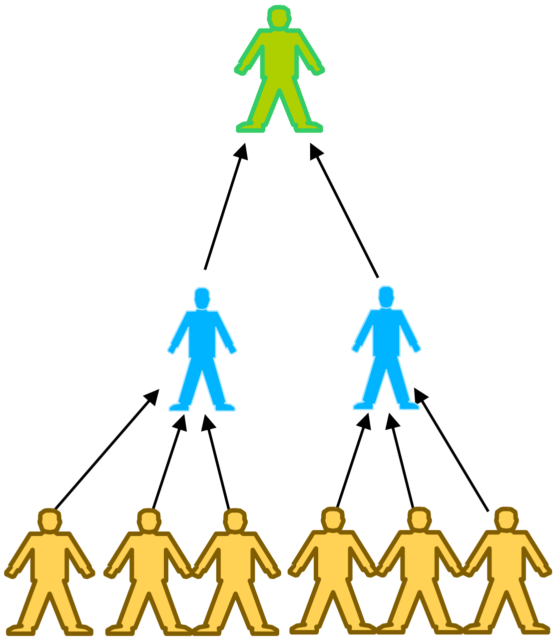
- Peer to Peer (PSK)



- Web-of-Trust (PGP)



- Hierarchical (PKI)



Building a Public Key Infrastructure (PKI)

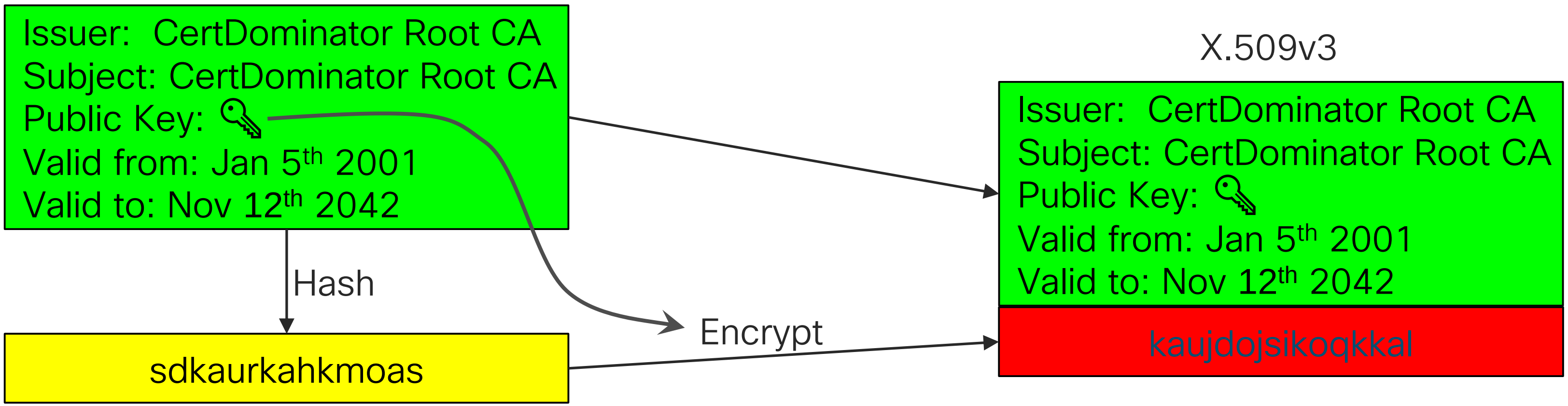
- Since we know that PKI has a root of trust, we need to build a certificate authority (CA) that is self-signed.

- Root CA generates an RSA key pair
- Creates a cleartext box with all of it's information in it like:
  - Common Name, Company Name, Organizational Unit
  - City, State, Country
  - A copy of its RSA Public Key
  - Validity Dates

Issuer: CertDominator Root CA
Subject: CertDominator Root CA
Public Key: 🔑
Valid from: Jan 5th 2001
Valid to: Nov 12th 2042

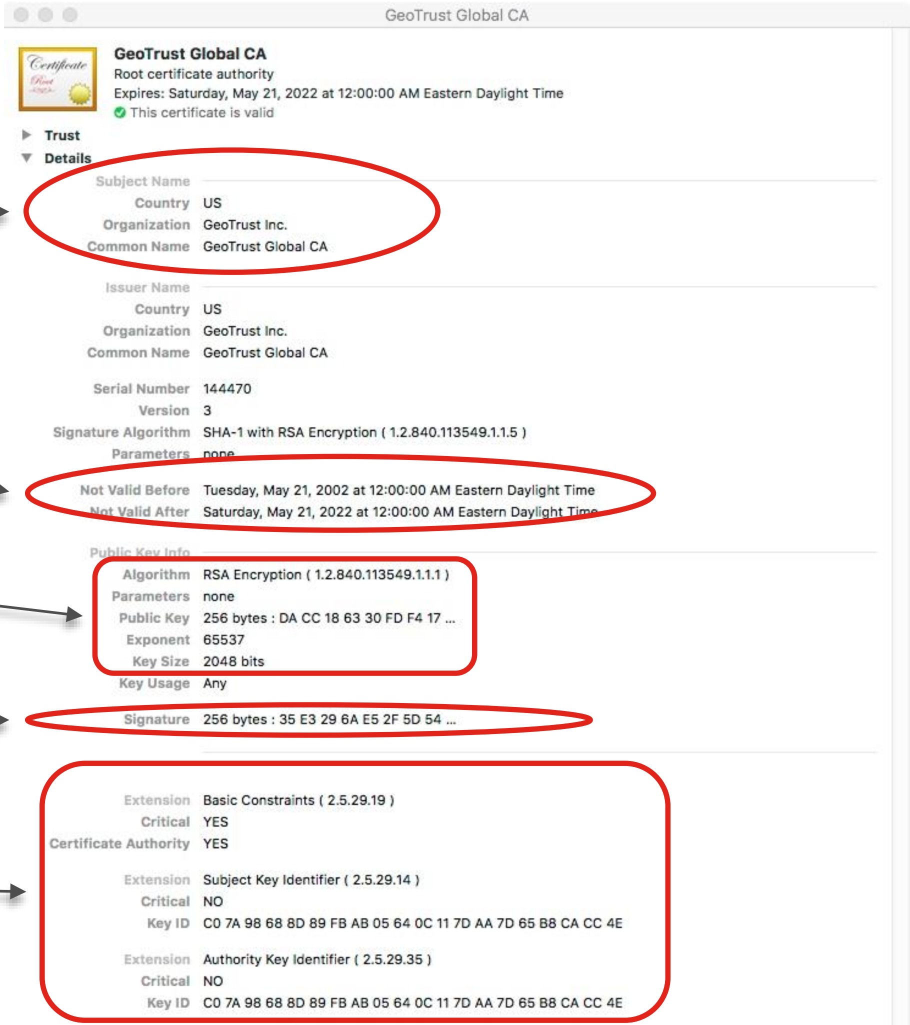
Building a Public Key Infrastructure (PKI)

- Generate a hash of cleartext box
- Encrypt hash with Root CA's private key
- Append encrypted hash (fingerprint/signature) to cleartext box
- Voila! You now have a self-signed Root CA certificate



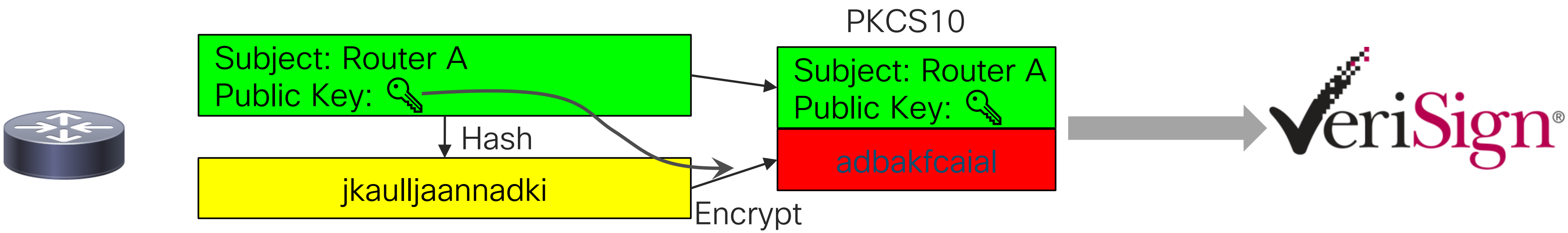
A Root CA in real life

1. Name
2. Validity Dates
3. RSA Public Key
4. Signature
5. Additional Info



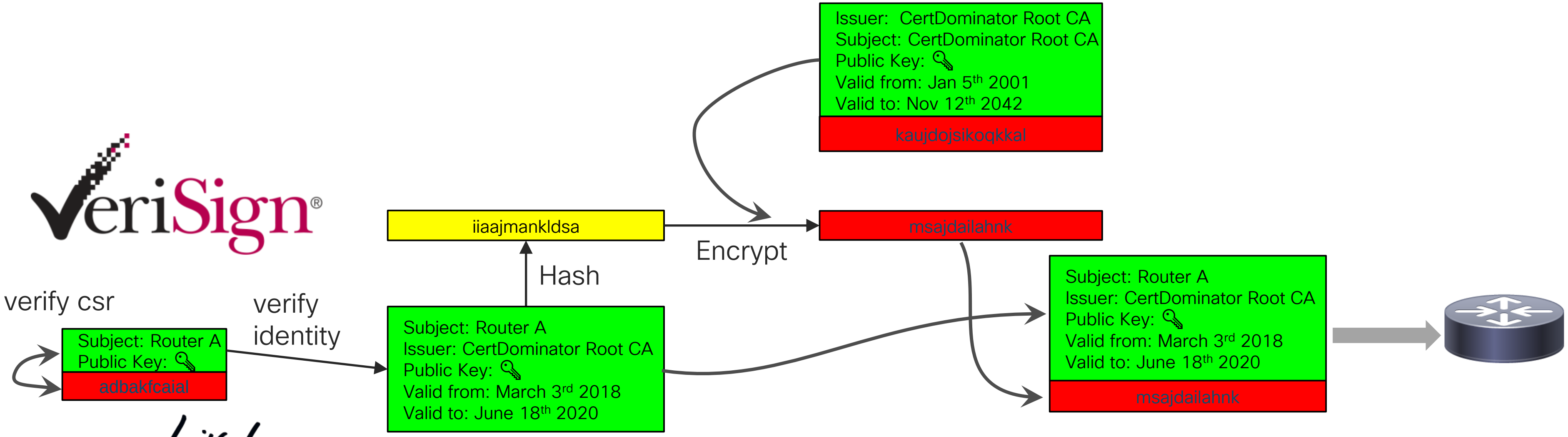
Enrolling into a Public Key Infrastructure (PKI)

- Router generates a RSA keypair
- Create a cleartext box with it's information in it
- Digitally sign the cleartext with Router's private key. This is now called a certificate signing request (CSR) or PKCS10
- Append encrypted hash (fingerprint/signature) to cleartext box
- Send to Certificate Authority



Enrolling into a Public Key Infrastructure (PKI)

- Root CA verifies the identity of the requestor and csr
- Takes cleartext info and adds some additional data to it
- Signs the new cleartext info with the Root CA private key
- Appends signature to cleartext.
- Send back certificate to router



Configure PKI - CA

Building a IOS CA Server

- Step 1

  - Manually set the time on the router:

```
RootCA#config terminal
RootCA(config)#clock timezone EST -5
RootCA(config)#clock summertime EDT recurring
RootCA(config)#exit
RootCA#clock set 22:300:00 22 Feb 2018
```

  - Or use NTP

```
RootCA#config terminal
RootCA(config)#clock timezone EST -5
RootCA(config)#clock summertime EDT recurring
RootCA(config)#ntp server 192.168.1.1
```

Building a IOS CA Server

- Step 2

  - Generate an RSA keypair and enable HTTP server

```
RootCA#config terminal
Router(config)#crypto key generate rsa label CA modulus 2048 exportable
The name for the keys will be: CA


% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 12 seconds)

RootCA(config)#ip http server
```

Building a IOS CA Server

- Step 3

  - Configure the CA Server

```
RootCA#config terminal
RootCA(config)#crypto pki server CA
RootCA(cs-server)# database level complete
RootCA(cs-server)# database archive pkcs12 password Cisco123
RootCA(cs-server)# issuer-name CN=RootCA
RootCA(cs-server)# hash sha256
RootCA(cs-server)# lifetime crl 10
RootCA(cs-server)# lifetime certificate 365
RootCA(cs-server)# lifetime ca-certificate 3650
RootCA(cs-server)# auto-rollover 60
```

Building a IOS CA Server

- Step 4

  - Turn on the CA

```
RootCA(cs-server)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
RootCA(cs-server)#
```


Building a IOS CA Server

- Step 5

  - Validate the CA is operational

```
RootCA#show crypto pki server
Certificate Server CA:
   Status: enabled
   State: enabled
   Server's configuration is locked (enter "shut" to unlock it)
   Issuer name: CN=RootCA
   CA cert fingerprint: AB615ECA FE55B934 7353FF78 D7AFE7E1
   Granting mode is: manual
   Last certificate issued serial number (hex): 1
   CA certificate expiration timer: 01:32:36 UTC May 13 2028
   CRL NextUpdate timer: 11:32:45 UTC May 16 2018
   Current primary storage dir: nvram:
   Database Level: Complete - all issued certs written as<serialnum>.cer
   Auto-Rollover configured, overlap period 60 days
   Autorollover timer: 01:32:36 UTC Mar 14 2028
```


Building a IOS CA Server

- Final Step

  - Export the RootCA certificate (save to notepad for later)

```
RootCA(config)#crypto pki export CA pem terminal
% The specified trustpoint is not enrolled (CA).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIDADCCAeigAwIBAgIBATANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDEwZSb290
Q0EwHhcNMTgwNTE2MDEzMjM2WhcNMjgwNTEzMDEzMjM2WjARMQ8wDQYDVQQDEwZS
b290Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDgMinBhBjoIQTk
+UHeHnN1jyh3eE567dDfSO0es+xWAXPOKFgslA+8A3TR+6Dk9cgDft3WynElr7mQ
...<output omitted for brevity>...
Ph6NVjfk0BJCfcKiadS6woQiUuft4hqSlF4TtYnNMgyx9hflgNoWNLZ+ULUv2laF
E+jdu6i75IYqm8ptmifT9UDNE8VhuTnaF3oZIAcaoU67Ga+3A4Nwe+9r0jRQw2Uy
D/CY5Q==
-----END CERTIFICATE-----

RootCA(config)#
```

Configure PKI - Client

Enrolling into a PKI with IOS as a client

- Trustpoints
    - A trustpoint is a container that can hold up to two certificates. It can hold either:
        - Just a CA certificate
        - Two certificates
            - One identity certificate (a cert you own the private key for)
            - The CA certificate that issued the identity certificate above

Enrolling into a PKI with IOS as a client

- Step 1

  - Manually set the time on the router:

```
Router#config terminal
Router(config)#clock timezone EST -5
Router(config)#clock summertime EDT recurring
Router(config)#exit
Router#clock set 22:300:00 22 Feb 2018
```

  - Or use NTP

```
Router#config terminal
Router(config)#clock timezone EST -5
Router(config)#clock summertime EDT recurring
Router(config)#ntp server 192.168.1.1
```


Enrolling into a PKI with IOS as a client

- Step 2

  - Generate an RSA key pair

```
Router#config terminal
Router(config)#hostname R1
R1(config)#ip domain-name example.com
R1(config)#crypto key generate rsa label MYKEY1 modulus 2048
exportable
The name for the keys will be: MYKEY1

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...[OK]
```

Enrolling into a PKI with IOS as a client

- Step 3

  - Create a trustpoint and enter info about the router

```
R1#config terminal
R1(config)#crypto pki trustpoint MYTP1
R1(config)#enrollment terminal
R1(config)#rsakeypair MYKEY1
R1(config)#subject-name cn=r1.example.com,o=Widget LTD
R1(config)#fqdn r1.example.com
R1(config)#serial-number none
R1(config)#ip-address none
R1(config)#revocation-check none
R1(config)#exit
```

Enrolling into a PKI with IOS as a client

- Step 4a
  - Authenticate the RootCA into this router

```
R1(config)#crypto pki authenticate MYTP1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDADCCAeigAwIBAgIBATANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDEwZSb290
Q0EwHhcNMTgwNTE2MDEzMjM2WhcNMjgwNTEzMDEzMjM2WjARMQ8wDQYDVQQDEwZS
b290Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDgMinBhBjoIQTk
...<input omitted for brevity>...
FpEOcjBdnzGM8GyrlKJNJNm78HHdLX2faWQvI2nf9ujgfO09HRvd22gQi6yxro7W
c0BHJ546Hb80O3GzNGxekxUc+KmpCNh2lHe3S73eJjkxYkSGIzy+G2FpbhLOIAHa
v4MzDekkWTroFsKMPJo6dYgBFPUbGzXM3RmsPKQV0nhUiD3cRWukLsP0AhJGVHgp
Ph6NVjfk0BJCfcKiadS6woQiUuft4hqSlF4TtYnNMgyx9hflgNoWNLZ+ULUv2laF
E+jdu6i75IYqm8ptmifT9UDNE8VhuTnaF3oZIAcaoU67Ga+3A4Nwe+9r0jRQw2Uy
D/CY5Q==
-----END CERTIFICATE-----
quit
```

cisco Live!

Enrolling into a PKI with IOS as a client

- Step 4b

  - Authenticate the RootCA into this router

```
Certificate has the following attributes:
  Fingerprint MD5: AB615ECA FE55B934 7353FF78 D7AFE7E1
  Fingerprint SHA1: 89979D02 A5DEF64D 4EE9C825 885129C4 02F32400

  % Do you accept this certificate? [yes/no]: yes
  Trustpoint CA certificate accepted.
  % Certificate successfully imported
  R1(config)#
```


Enrolling into a PKI with IOS as a client

- Step 5
  - Verify the RootCA was installed properly

```
R1#show crypto pki certificates MYTP1
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
 Subject:
   cn=RootCA
 Validity Date:
   start date: 01:32:36 UTC May 16 2018
   end date: 01:32:36 UTC May 13 2028
 Associated Trustpoints: MYTP1
```

Enrolling into a PKI with IOS as a client

- Step 6

  - Generate a Certificate Signing Request (CSR)

```
R1(config)#crypto pki enroll MYTP1
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=r1.example.com,o=Widget LTD
% The subject name in the certificate will include: r1.example.com
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIICszCCAZsCAQAwTTETMBEGA1UEChMKV2lkZ2V0IExURDEXMBUGA1UEAxMOcjEu
ZXhhbXBsZS5jb20xHTAbBgkqhkiG9w0BCQIWDnIxLmV4YW1wbGUuY29tMIIBIjAN
<output omitted for brevity>
zCJlE6v78udsaGFgpDy20k++co4xhxygbay5b7iVKiv9kHRLPezWOxvsox9PGqiV
tA9qVyq08jjzoBJJKWxS/8opjty3xt1zXOyWw601bDuj9ucRnG7bSwseeqb9NlbZ
L83ODrmQrLaoxkW+V6ELCTKRPAHDfpk=
---End - This line not part of the certificate request---
```


Enrolling into a PKI with IOS as a client

- Step 7

    - On the CA Server submit the CSR

```
RootCA#crypto pki server CA request pkcs10 terminal
PKCS10 request in base64 or pem
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
MIICszCCAZsCAQAwTTETMBEGA1UEChMKV21kZ2V0IExURDEXMBUGA1UEAxMOcjEu
ZXhhbXBsZS5jb20xHTAbBgkqhkiG9w0BCQIWDnIxLmV4YW1wbGUuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxTuU1jW/9kx5IlTjB3owJYNJBqCx
...<input omitted for brevity>...
hIDQ24U7gXuOGMU21aPtuQ/LZxmEBwZYHdPRePc0kzcocpNTalNf4IKx35zxXOQf
v4NxVHA2ZIInq4ojedF0EsrfL1ddXhUdgyek+KW4tZR9udlRdLGY/6AtH1dvwpxA
zCJlE6v78udsaGFgpDy20k++co4xhxygbay5b7iVKiv9kHRLPezWOxvsox9PGqiV
tA9qVyq08jjzoBJJKWxS/8opjty3xt1zXOyWw601bDuj9ucRnG7bSwseeqb9NlbZ
L83ODrmQrLaoxkW+V6ELCTKRPAHDfpk=
quit
% Enrollment request pending, reqId=1
```


Enrolling into a PKI with IOS as a client

- Step 8

  - On the CA Server view the requests

```
RootCA#show crypto pki server CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID State     Fingerprint                         SubjectName
--------------------------------------------------------------
RA certificate requests:
ReqID State     Fingerprint                         SubjectName
--------------------------------------------------------------
Router certificates requests:
ReqID State     Fingerprint                         SubjectName
--------------------------------------------------------------
1     pending   009C4CCEBE7DB60AC9F1E271E1FBAF8E
hostname=r1.example.com,cn=r1.example.com,o=Widget LTD
```

Enrolling into a PKI with IOS as a client

- Step 9

    - On the CA Server grant the request

```
RootCA#crypto pki server CA grant 1
% Granted certificate:
```


```
MIIDKzCCAhOgAwIBAgIBAjANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDEwZSb290
Q0EwHhcNMTgwNTE2MDE1NjMyWhcNMTkwNTE2MDE1NjMyWjBNMRMwEQYDVQQKEwpX
aWRnZXQgTFREMRcwFQYDVQQDEw5yMS5leGFtcGxlLmNvbTEdMBsGCSqGSIb3DQEJ
AhYOcjEuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDFO5TWNb/2THkiVOMHejAlg0kGoLGdZS8Pf6X2/Z8g4abNqXLtKzWcm+caal0A
ofP9xDTU3CftofYvQZIGprukUgKnhP+EgNDbhTuBe44YxTbVo+25D8tnGYQHBlgd
09F49zSTNyhyk1NqU1/ggrHfnPFc5B+/g3FUcDZkgieriiN50XQSyt8vV11eFR2D
J6T4pbi1lH252VF0sZj/oC0fV2/CnED/xAMkR7VHJ1YDpMPcGUMfdvnsIJq3Sgxg
e3jYukzSG5/UzGsXBS9+VWnSPqEyrfOhdn2TOIj+mzhEhNoDknOrGAYJasA+b55e
3w+lCiXL4spm8uPzBz48njtBAgMBAAGjUjBQMA4GA1UdDwEB/wQEAwIFoDAfBgNV
HSMEGDAWgBTpAMxawXGZhTkWz+joSyU4hsORizAdBgNVHQ4EFgQUnylsS5Nlr5yv
d62+urQ25+ybG9owDQYJKoZIhvcNAQELBQADggEBADmVZ857UkmdylmA7G3TLqCY
GtEgn4eGpHzMYehuCJL1qHmic5tdELV3u1FF6K7oSFnAchjL/PQYyZXhWfwkPbCQ
VeJoiO6EyDe2ZMA/uOuhprpW2mH9OLo1+TFBhGwtEl1VgZVasFLm9Dpb6WkeE28x
9FumMC4e5IfGGlkXbTtuGbqyrOkSV7JH1+l7cvbX6juY5yjJ389N2C7pnzDd7U5F
eO4QD4SD8kjlURHeKHEbjZHasL0payuQ8IaMrFPonX1WXll0T86LX6v7EQ8A3g8m
FUYOnvFvw+Ws58F743J00ODMWY6L8lURvory455FEQLSSQ37WpC8BzukLVfDaBY=
```


Enrolling into a PKI with IOS as a client

- Step 10

  - On the router import the certificate

```
R1(config)#crypto pki import MYTP1 certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
MIIDKzCCAhOgAwIBAgIBAjANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDEwZSb290
Q0EwHhcNMTgwNTE2MDE1NjMyWhcNMTkwNTE2MDE1NjMyWjBNMRMwEQYDVQQKEwpX
aWRnZXQgTFREMRcwFQYDVQQDEw5yMS5leGFtcGxlLmNvbTEdMBsGCSqGSIb3DQEJ
AhYOcjEuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
...<input omitted for brevity>...
GtEgn4eGpHzMYehuCJL1qHmic5tdELV3u1FF6K7oSFnAchjL/PQYyZXhWfwkPbCQ
VeJoiO6EyDe2ZMA/uOuhprpW2mH9OLo1+TFBhGwtEl1VgZVasFLm9Dpb6WkeE28x
9FumMC4e5IfGGlkXbTtuGbqyrOkSV7JH1+l7cvbX6juY5yjJ389N2C7pnzDd7U5F
eO4QD4SD8kjlURHeKHEbjZHasL0payuQ8IaMrFPonX1WXl10T86LX6v7EQ8A3g8m
FUYOnvFvw+Ws58F743J00ODMWY6L8lURvory455FEQLSSQ37WpC8BzukLVfDaBY=
quit
% Router Certificate successfully imported


R1(config)#
```

Enrolling into a PKI with IOS as a client

- Final Step

  - Verify the certificate was imported properly

```
R1#show crypto pki certificates MYTP1
Certificate
 Status: Available
 Certificate Serial Number (hex): 02
 Certificate Usage: General Purpose
 Issuer:
   cn=RootCA
 Subject:
   Name: r1.example.com
   hostname=r1.example.com
   cn=r1.example.com
   o=Widget LTD
 Validity Date:
   start date: 01:56:32 UTC May 16 2018
   end date: 01:56:32 UTC May 16 2019
 Associated Trustpoints: MYTP1
```

Configure PKI - Client (the easy way)

cisco Live!

Enrolling into a PKI with IOS as a client

- Step 1

  - Change RootCA to auto-grant certificates

```
RootCA(config)#crypto pki server CA
RootCA(cs-server)#shut
Certificate server 'shut' event has been queued for processing.
RootCA(cs-server)#grant auto
RootCA(cs-server)#no shut
Certificate server 'no shut' event has been queued for processing.
RootCA(cs-server)#
```

Enrolling into a PKI with IOS as a client

- Step 2

  - Set time and configure trustpoint the same as before but instead change the **enrollment** command to point to IOS CA.

```
R1(config)#crypto pki trustpoint MYTP1
R1(ca-trustpoint)#enrollment url http://10.7.7.81
```

  - Then authenticate the RootCA certificate

```
R1(config)#crypto pki authenticate MYTP1
Certificate has the following attributes:
      Fingerprint MD5: AB615ECA FE55B934 7353FF78 D7AFE7E1
     Fingerprint SHA1: 89979D02 A5DEF64D 4EE9C825 885129C4 02F32400

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Enrolling into a PKI with IOS as a client

- Step 3

  - Enroll with the CA Server

```
R1(config)#crypto pki enroll MYTP1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
Password:<blank>
Re-enter password:<blank>

% The subject name in the certificate will include: cn=r1.example.com,o=Widget LTD
% The subject name in the certificate will include: r1.example.com
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose MYTP1' command will show the
fingerprint.
```


Enrolling into a PKI with IOS as a client

- Step 4

  - Verify the RootCA cert and identity cert are installed

```
R1(config)#do show crypto pki certificates MYTP1
Certificate
 Status: Available
 Certificate Serial Number (hex): 03
 Certificate Usage: General Purpose
 Issuer:
   cn=RootCA
 Subject:
   Name: r1.example.com
   hostname=r1.example.com
   cn=r1.example.com
   o=Widget LTD
 Validity Date:
   start date: 02:44:00 UTC May 16 2018
   end date: 02:44:00 UTC May 16 2019
 Associated Trustpoints: MYTP1
```

```
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
 Subject:
   cn=RootCA
 Validity Date:
   start date: 01:32:36 UTC May 16 2018
   end date: 01:32:36 UTC May 13 2028
 Associated Trustpoints: MYTP1
```

Troubleshooting

- Verify time is correct and authoritative

```
show clock detail
```

- Verify IP/TCP connectivity to CA server for SCEP to work

```
telnet <ip of CA> 80
```

- Debug commands

```
debug crypto pki api
debug crypto pki callback
debug crypto pki scep
debug crypto pki server
debug crypto pki transactions
debug crypto pki validation
```

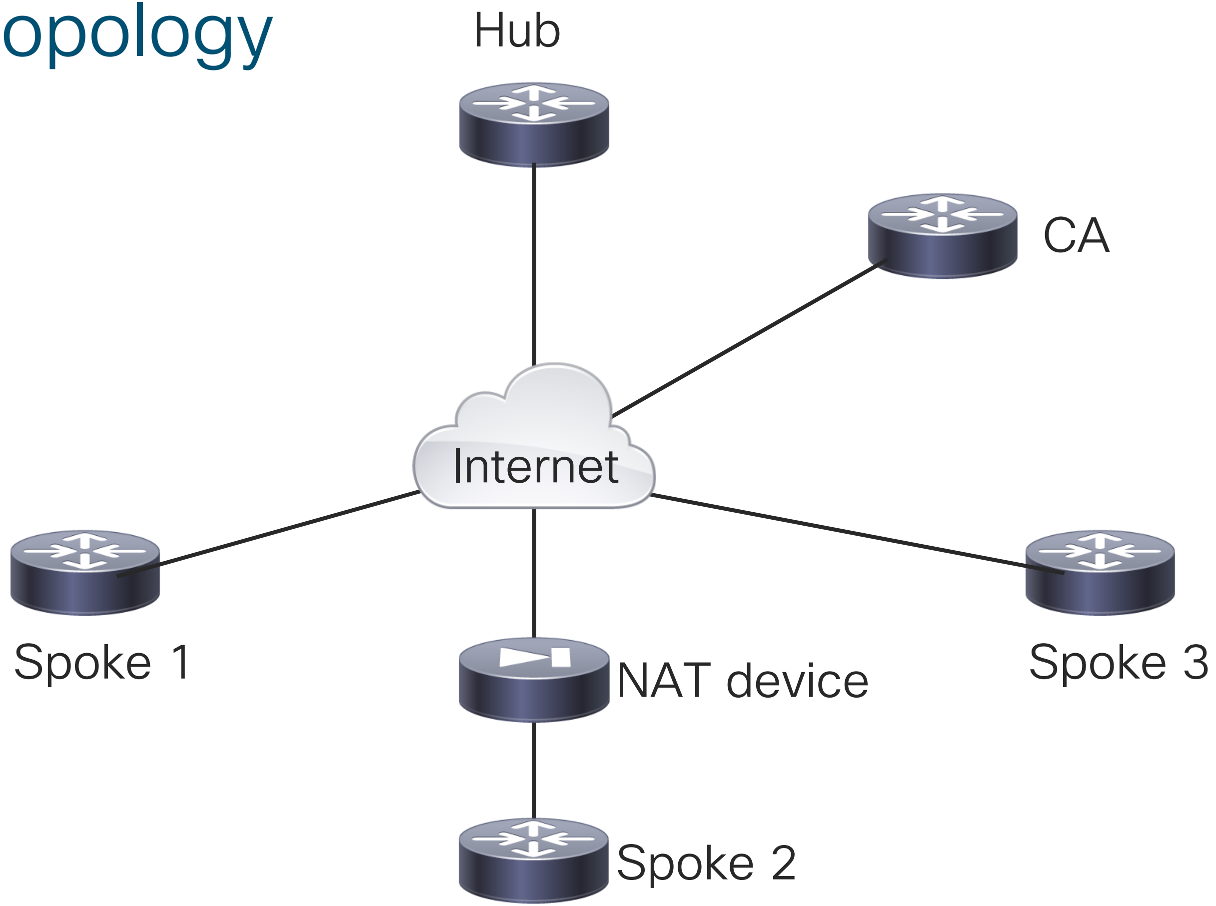

Demo Time!!!!!

VIRL Topology File (Take home lab)

- Will require Virtual Internet Routing Lab (VIRL)
- Check it out here: http://virl.cisco.com/

- Topology file:
- https://cisco.box.com/s/rd3t7jvxsmr6awz7kvhtu8ydmqhr8wwk
- Password will be shared in **Webex Teams**

Lab Topology



Troubleshooting Solutions

- Time on Spoke 2 was incorrect.
  - Used "`debug crypto pki X`" commands to determine the reason
  - Use SNTP/NTP or manually set it.
  - The following command should not have a "`.`" or "`*`" in front of the time
    - `show clock detail`

- HTTP traffic was blocked on CA's WAN interface by ACL
  - Use telnet to test TCP 3-way handshake
  - Then simulate a basic HTTP request by typing the following command

```
telnet <ip of CA> 80
GET / HTTP/1.0
```

IKEv1/IKEv2

ISAKMP

- ISAKMP defines two phases:
- Phase 1
  - Used for control plane
  - Establish secure channel between peers
  - Prove identities
  - Negotiate data plane security settings
- Phase 2
  - Used for data plane
  - Transports the protected data

IKEv1 Main Mode

IKEv1- Main Mode (message 1 and 2)

- The first two messages are used to negotiate the following cryptographic attributes:
  - Authentication method*
  - Encryption cipher*
  - Integrity hash*
  - Lifetime of Security Association
  - Diffie-Hellman Key Exchange Group *
- Initiator proposes a list of combinations of the starred (*) above
- Responder picks one of the combinations proposed
- Lifetime is MIN(initiator, responder)
- NOT encrypted – Peer NOT authenticated yet

IKEv1- Main Mode (MM1)

Initiator

Responder

HDR

cookie:

- initiator = X (randomly generated number per session)
- responder = 00000000,

SA (multiple crypto policies),

Vendor IDs – String or hash value. Used to advertise support for capabilities not defined in standard (i.e. NAT-T)

MM1

Unencrypted – Unauthenticated

Reference

cisco Live!

IKEv1- Main Mode (MM2)

Initiator

Responder

HDR

cookie:

- initiator = X (retained)
- responder = Y (randomly generated per session),

SA (the selected crypto policy),

Vendor IDs – String or hash value. Used to advertise support for capabilities not defined in standard (i.e. NAT-T)

MM2

Unencrypted – Unauthenticated

Reference

IKEv1- Main Mode (message 3 and 4)

- Exchange Diffie-Hellman key values
- Exchange Nonce values
- Detect if NAT is used between peers
- Suggest trusted certificate authorities (CA)
- After this exchange, further communication is encrypted and secure.
- Peer NOT authenticated yet.

IKEv1- Main Mode (MM3)

Initiator

Responder

HDR (cookie i=X,r=Y)

Diffie-Hellman Key Exchange material (g^xi)

Nonce from initiator (random data [entropy + anti-replay])

Additional Vendor IDs

NAT-Discovery Payloads

MM3

Unencrypted – Unauthenticated

Reference

IKEv1- Main Mode (MM4)

Initiator

Responder

HDR (cookie i=X,r=Y)

Diffie-Hellman Key Exchange material (g^xr)

Nonce from responder (random data [entropy + anti-replay])

Additional Vendor IDs

NAT-Discovery Payloads

[Certificate Request] – Hints of which CAs the responder trusts

MM2

Unencrypted – Unauthenticated

Reference

Diffie-Hellman Groups

Number	Name
1	Group 1 - 768-bit MODP Group
2	Group 2 - 1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
17	6144-bit MODP Group
18	8192-bit MODP Group
19	256-bit random ECP group
20	384-bit random ECP group
21	521-bit random ECP group
22	1024-bit MODP Group with 160-bit Prime Order Subgroup
23	2048-bit MODP Group with 224-bit Prime Order Subgroup
24	2048-bit MODP Group with 256-bit Prime Order Subgroup
25	192-bit Random ECP Group
26	224-bit Random ECP Group

Reference

Diffie-Hellman Primer

p=23   g=5   p and g are constants defined by DH Group

Alice

a=6

$g^a \bmod p = A = 5^6 \bmod 23 = 15{,}625 \bmod 23 = 8$

$g^b \bmod p = A = 5^{15} \bmod 23 = 30{,}517{,}578{,}125 \bmod 23 = 19$

$s = B^a \bmod p$

$s = 19^6 \bmod 23$

$s = 47{,}045{,}881 \bmod 23$

$s = 2$

Alice

b=15

$A^b \bmod p = s$

$8^{15} \bmod 23 = s$

$35{,}184{,}372{,}088{,}832 \bmod 23 = s$

$2 = s$

Reference

IKEv1- KEYS

- From the derived secret value a SKEYID is created using values from the ISAKMP exchange.
- Provides protection against replay attacks using the same DH values.
- Different SKEYID generation based on authentication type:
  - Pre-shared-key: SKEYID = prf(pre-shared-key, Ni_b | Nr_b)
  - Signatures (Certs): SKEYID = prf(Ni_b | Nr_b, g^xy)
- Then from that SKEYID three sub-keys are created:
  - SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0) - For further keying material derivation
  - SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1) - Authentication Key
  - SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2) - Encryption Key

Reference

IKEv1- Main Mode (message 5 and 6)

- Exchange certificate
- Prove identity using Pre-Shared Key or Certificate
- Cryptographically validate previous messages – prevents session hijack
- Switched to UDP/4500 if NAT had been detected in MM3+4
- Encrypted – Peer is proving identity.

IKEv1- Main Mode (MM5)

Initiator | Responder

HDR (cookie i=X,r=Y)

Identity (a string value representing who I am)

Auth payload (cryptographic proof-of-possession built from pre-shared-key or digital signature)

[Initial Connect] – Optional payload to help synchronize SAs

[Certificate] – Copy of initiator's ID cert + chain

[Certificate Request] – Hints of which CAs the initiator trusts

MM5

Encrypted

Initiator: Proving identity

Responder: Unauthenticated

Reference

IKEv1- Main Mode (MM6)

Initiator

Responder

HDR (cookie i=X,r=Y)

Identity (a string value representing who I am)

Auth payload (cryptographic proof-of-posession built from preshared-key or digital signature)

[Certificate] – Copy of responder’s ID cert + chain

MM6

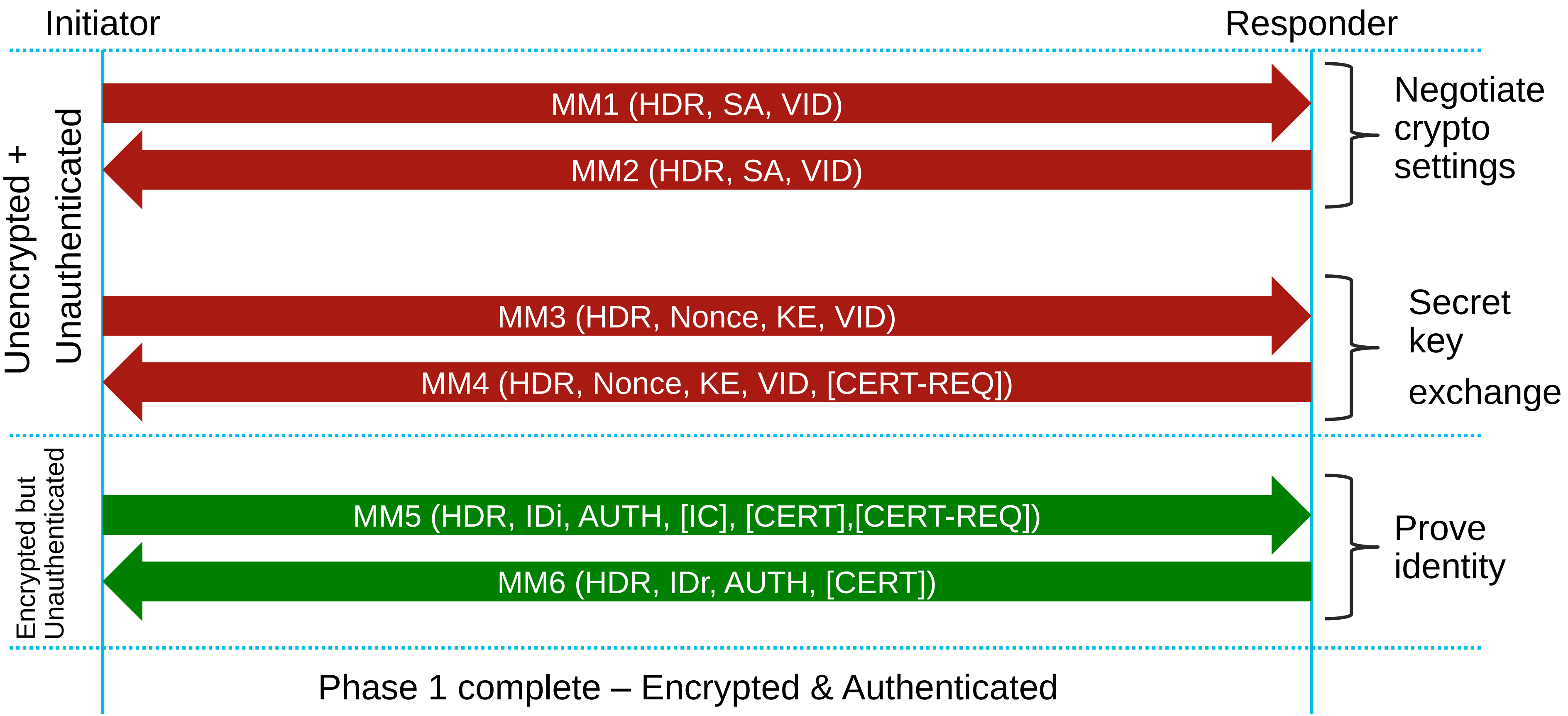
Encrypted

Initiator: Authenticated

Responder: Proving identity

Reference

IKEv1 – Main Mode Summary



IKEv1 – Quick Mode Phase 2

- Quick mode allows the establishment of an IPsec SA in three messages
- Things negotiated:
  - Traffic to be protected
  - How to be encapsulated
  - How to be encrypted
  - How to provide integrity
  - How long the SA is valid for in time and volume of data
  - If Perfect Forward Secrecy (PFS) is required

IKEv1- Quick Mode (QM1)

Initiator

Responder

HASH(1)

SA (Transform sets, SPI)

Nonce (for replay protection)

[Key Exchange] (if PFS is desired)

Proposed Traffic Selectors

NAT address information

QM1

Reference

IKEv1- Quick Mode (QM2)

Initiator

Responder

HASH(2)

SA (Transform set, SPI)

Nonce (for replay protection)

[Key Exchange] (if PFS is desired)

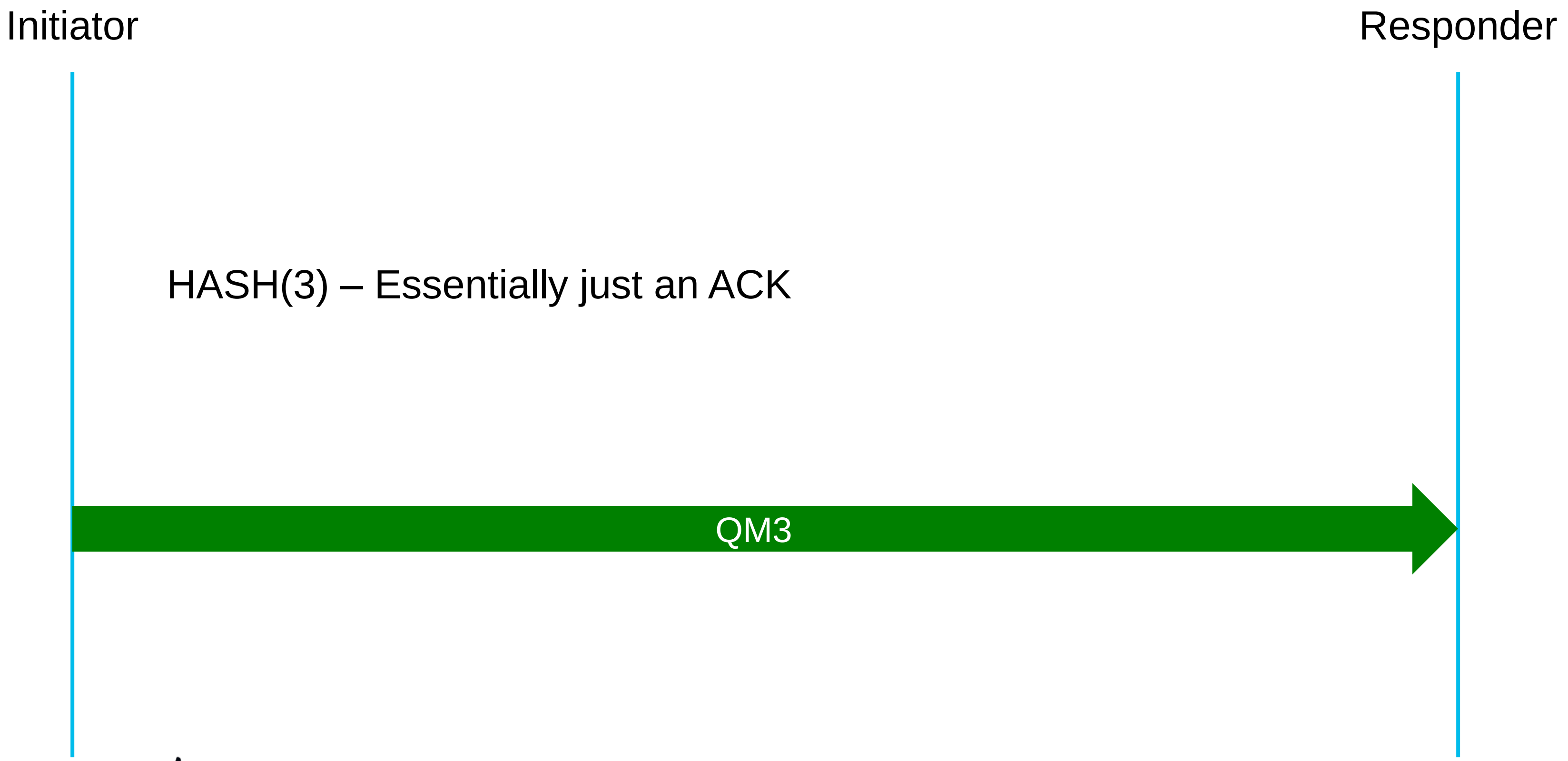
Selected Traffic Selectors

NAT address information

QM2

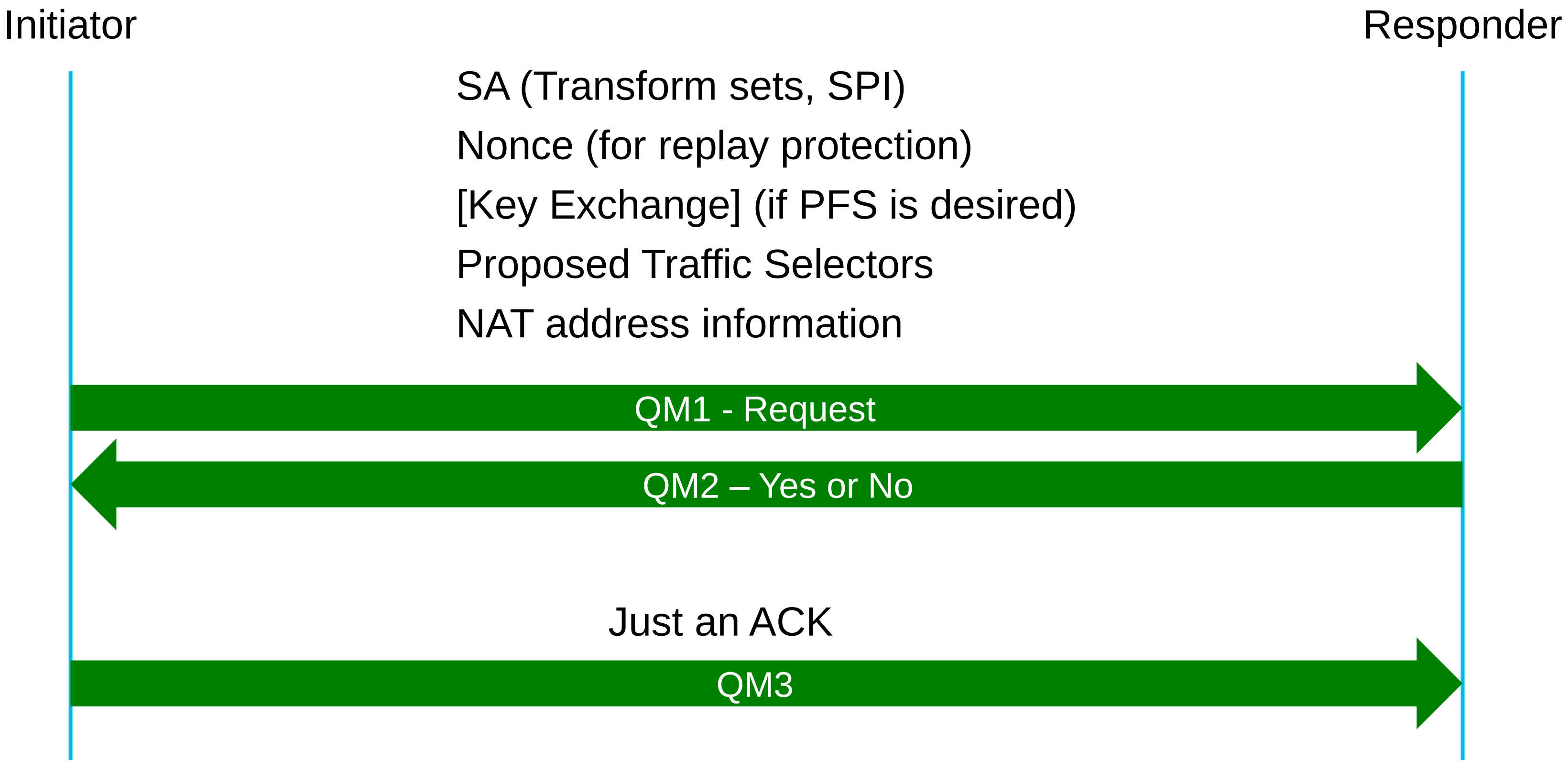
Reference

IKEv1- Quick Mode (QM3)



Reference

IKEv1- Quick Mode Summary



cisco Live!

IKEv1 Add-ons

IKEv1 – NAT breaks things™

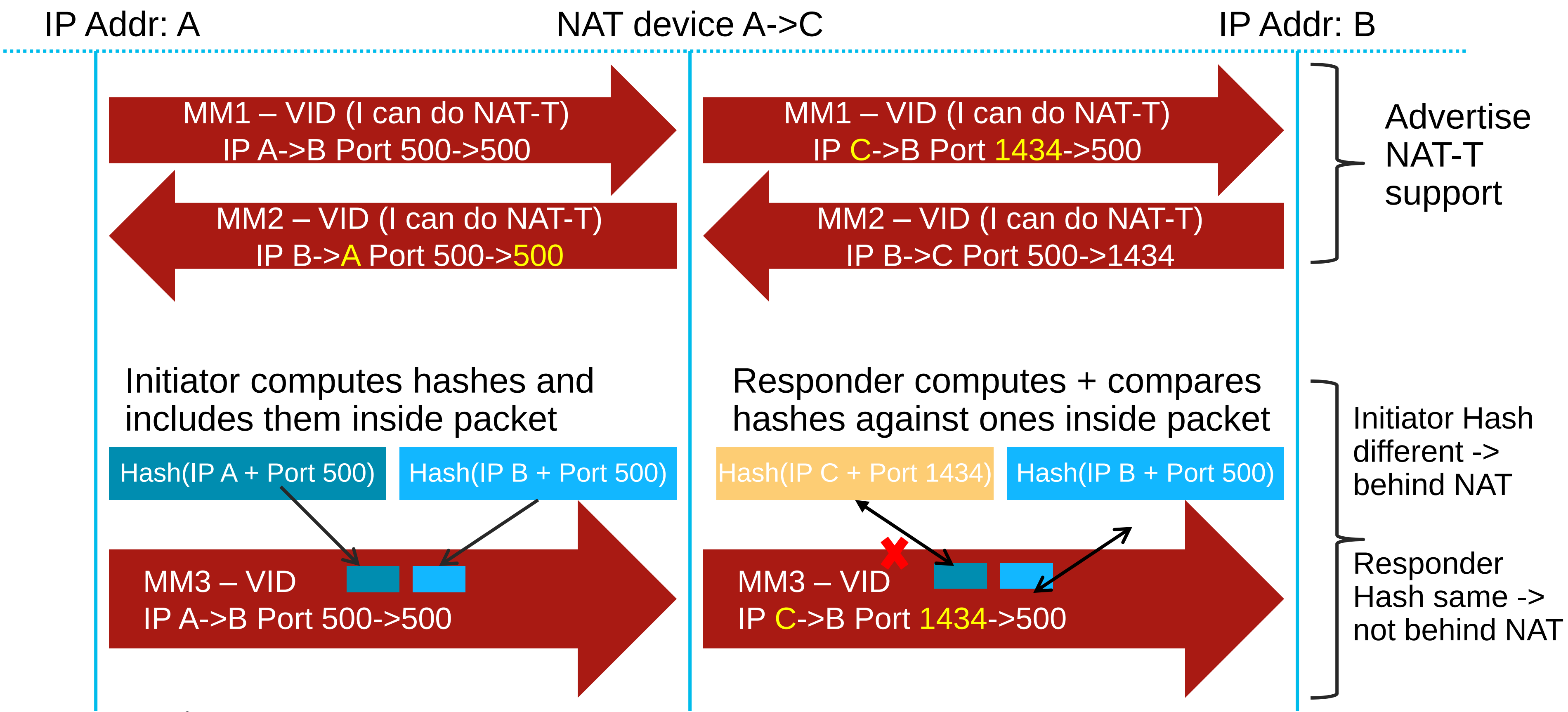
- IPsec uses IP protocol 50 (ESP) and 51 (AH)
- 1:1 NAT
  - AH can't work – Integrity check performed over IP address fields + payload
  - ESP can work – Integrity check performed only over payload
- N:1 Port Address Translation (PAT)
  - Rule of Thumb – Only TCP and UDP can reliably be NATted
- ESP doesn't have ports ∴ ESP can't work through PAT

- Solution: Encapsulate ESP packets within UDP

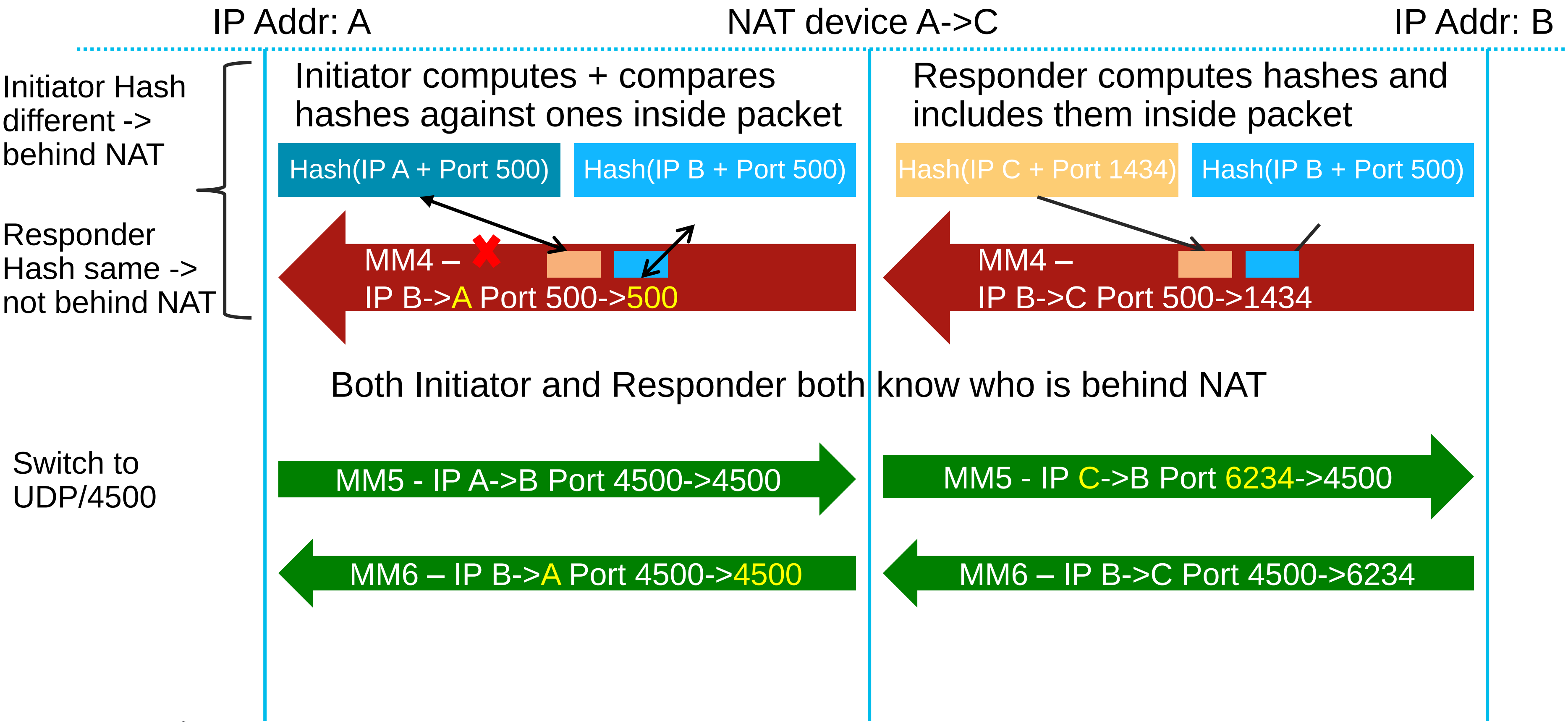
IKEv1 – NAT-T

- Solution: Encapsulate ESP packets within UDP when going through NAT
- NAT/PAT devices only see UDP packets.
- Port 4500 is reserved for IPsec over UDP
- Support for NAT-T was added with RFC 3947 and 3948

IKEv1 – Determine if NAT is in path



IKEv1 – Determine if NAT is in path



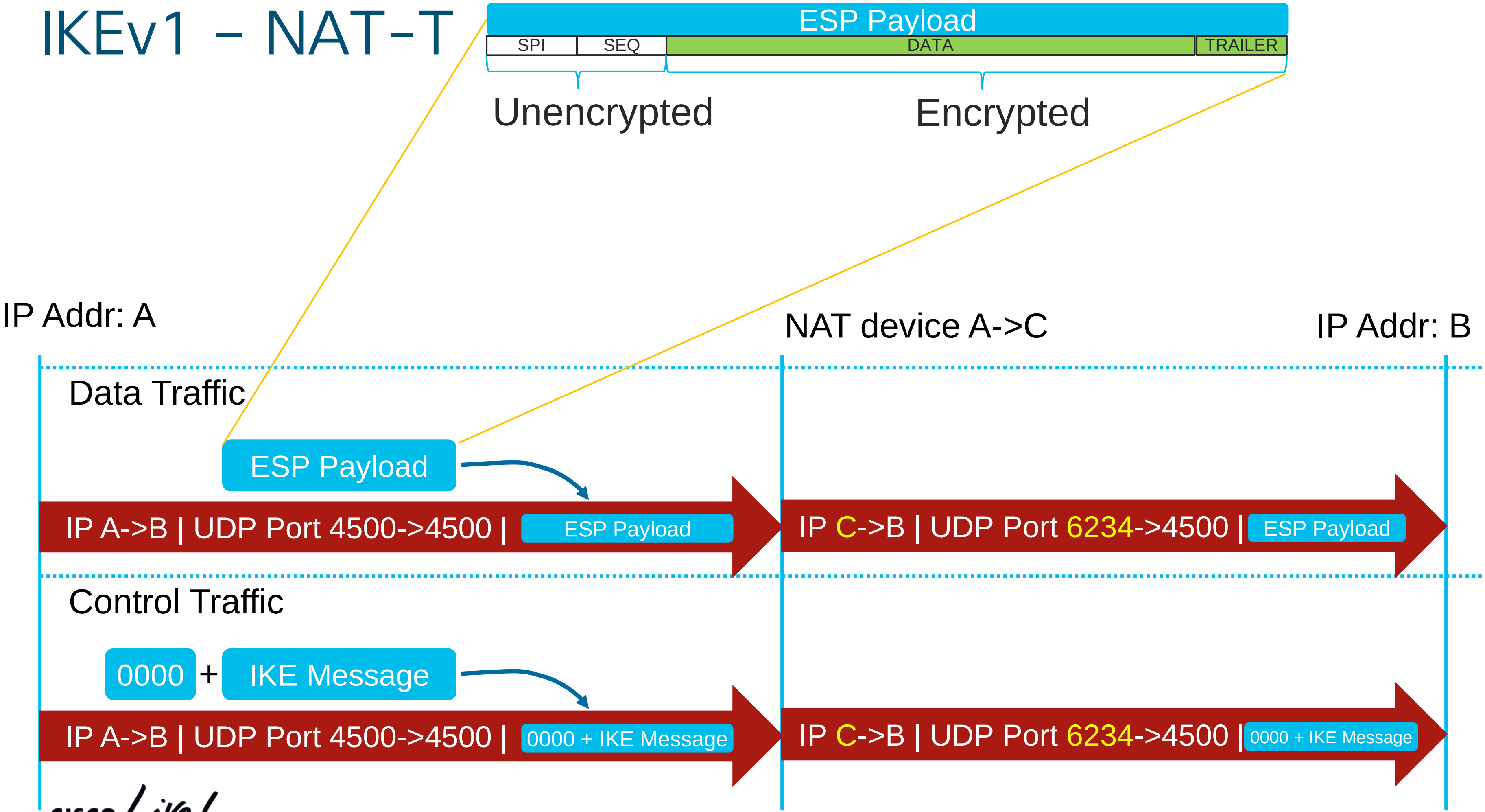
IKEv1 – NAT-T

- Normal Case:
  - UDP/500 for control channel
  - ESP or AH for data channel

- Problem: Stateful firewalls (NAT devices) can prevent the control channel communication due to inactivity even when data channel is actively used.

- NAT Case:
  - Send both control channel and data channel over UDP/4500

IKEv1 – NAT-T



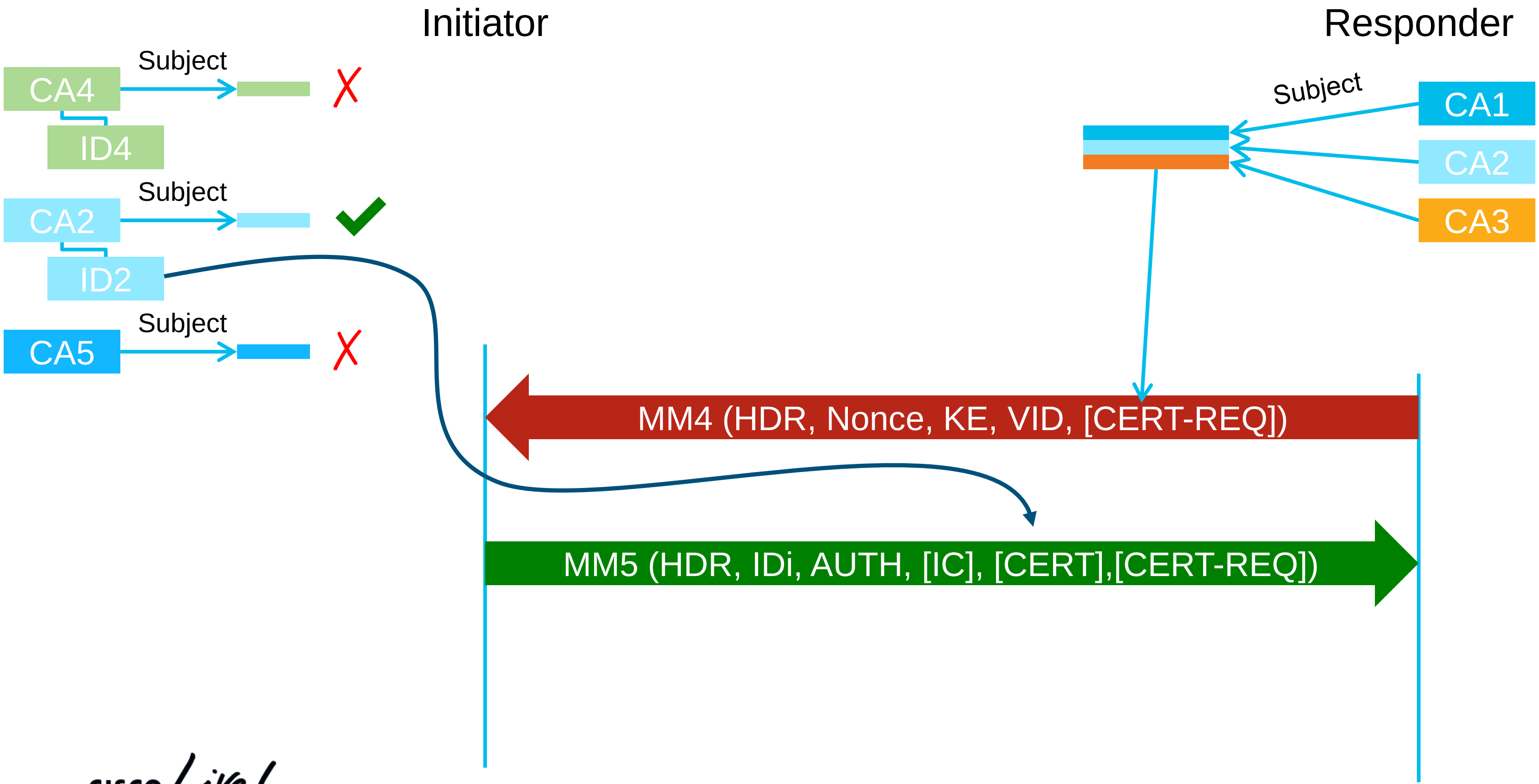
ESP Payload
SPI
SEQ
DATA
TRAILER
Unencrypted
Encrypted
IP Addr: A
NAT device A->C
IP Addr: B
Data Traffic
ESP Payload
IP A->B | UDP Port 4500->4500 |
ESP Payload
IP C->B | UDP Port 6234->4500 |
ESP Payload
Control Traffic
0000
+
IKE Message
IP A->B | UDP Port 4500->4500 |
0000 + IKE Message
IP C->B | UDP Port 6234->4500 |
0000 + IKE Message

IKEv1 – Certificates

- Authentication can use certificates
- Problem 1: Peer must know which CAs are trusted by peer
- Explicit configuration doesn't scale

- Solution 1: RFC4945 – Prior to AUTH provide a list of trusted CAs to peer
  - In MM4 – Responder sends list of CA he trusts
  - In MM5 – Initiator sends list of CA he trusts.

IKEv1 – Certificates



ISAKMP Fragmentation

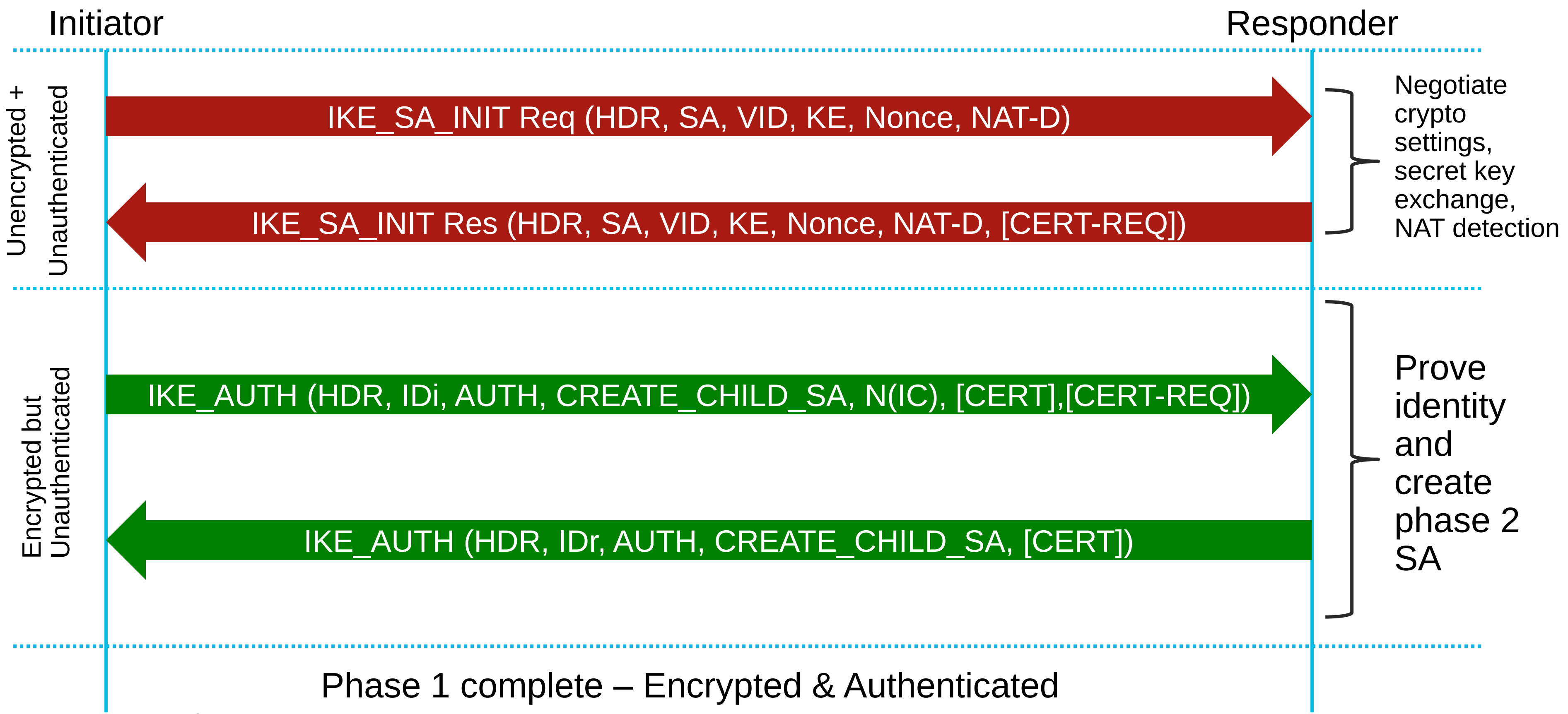
- Large IKE messages make large UDP datagrams
- Packets get fragmented at IP layer
- Filtering/Blocking of fragments causes protocol failure
- Solution: Fragment at Application layer
- IKEv1 – Proprietary
  - Encrypt then segment across multiple UDP packets
- IKEv2 – Standard, RFC7383
  - Segment then encrypt

IKEv2

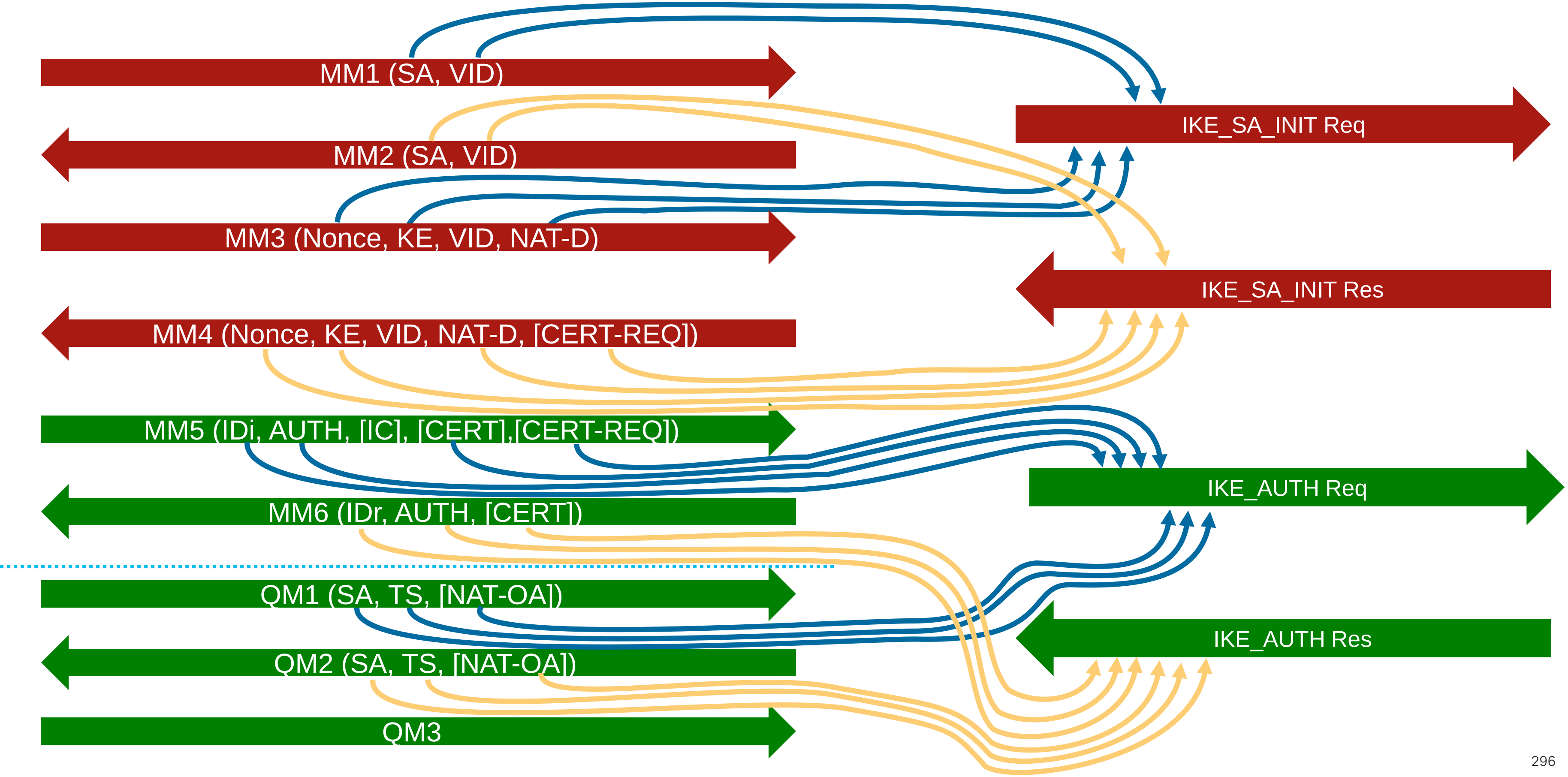
IKEv2 – Goals (What did we learn)

- Define IKEv2 in one document rather than a combination of many
- Reduce setup latency by reducing number of messages
- More secure
- Always provide identity protection (No Aggressive mode)
- PSK is not used in crypto key generation*
- Provide additional authentication mechanisms (EAP)
- Allow more flexible authentication choices (asymmetrical)
- Exchange of routes and attributes
- Reduce number of options/methods – simplify implementations

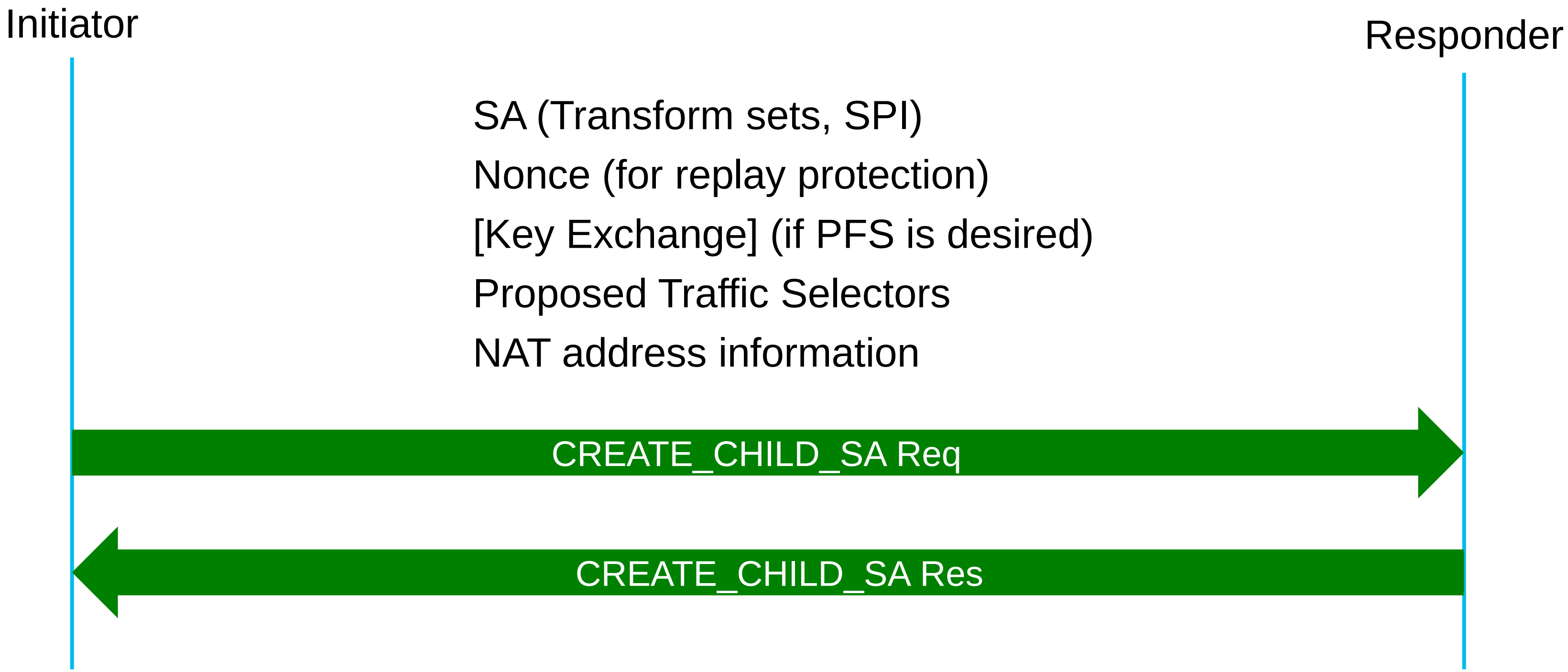
IKEv2 – Session Establishment Overview



IKEv1 vs IKEv2 – Session Establishment Overview



IKEv2 – 2nd Child SA Establishment



Configure DMVPN w/ PKI

cisco Live!

Configure Hub

- Step 1

  - Configure a certificate map to match certificates based on their information

```
HUB(config)#crypto pki certificate map MYMAP1 10
HUB(ca-certificate-map)#issuer-name eq cn=RootCA
```


Configure Hub

- Step 2

  - Configure an IKEv2 profile to match the incoming connections

```
HUB(config)#crypto ikev2 profile DMVPN
HUB(config-ikev2-profile)#match certificate MYMAP1
HUB(config-ikev2-profile)#authentication local rsa-sig
HUB(config-ikev2-profile)#authentication remote rsa-sig
HUB(config-ikev2-profile)#pki trustpoint MYTP1
```


Configure Hub

- Step 3

  - Configure an ipsec profile to link to the IKEv2 profile

```
HUB(config)#crypto ipsec profile DMVPN
HUB(ipsec-profile)#set ikev2-profile DMVPN
```


Configure Hub

- Step 4

  - Configure the DMVPN hub tunnel

```
HUB(config)#int tunnel 100
HUB(config-if)#ip address 172.16.1.254 255.255.255.0
HUB(config-if)#no ip split-horizon eigrp 100
HUB(config-if)#ip nhrp network-id 100
HUB(config-if)#ip nhrp map multicast dynamic
HUB(config-if)#tunnel source gigabitEthernet 0/1
HUB(config-if)#tunnel mode gre multipoint
HUB(config-if)#tunnel protection ipsec profile DMVPN
```


Configure Spoke

- Step 1 – Repeat step 1-3 from Hub
-

```
Spoke1(config)#crypto pki certificate map MYMAP 10
Spoke1(ca-certificate-map)#issuer-name eq cn=RootCA
Spoke1(config)#crypto ikev2 profile DMVPN
Spoke1(config-ikev2-profile)#match certificate MYMAP
Spoke1(config-ikev2-profile)#authentication local rsa-sig
Spoke1(config-ikev2-profile)#authentication remote rsa-sig
Spoke1(config-ikev2-profile)#pki trustpoint MYTP1
Spoke1(config-ikev2-profile)#crypto ipsec profile DMVPN
Spoke1(ipsec-profile)#set ikev2-profile DMVPN
```


Configure Spoke

- Step 2

  - Configure the tunnel interface

```
Spoke1(config)#interface Tunnel100
Spoke1(config-if)#ip address 172.16.1.1 255.255.255.0
Spoke1(config-if)#ip nhrp network-id 100
Spoke1(config-if)#ip nhrp nhs 172.16.1.254 nbma 192.0.2.2 multicast
Spoke1(config-if)#tunnel source GigabitEthernet0/1
Spoke1(config-if)#tunnel mode gre multipoint
Spoke1(config-if)#tunnel protection ipsec profile DMVPN
```


Verify the tunnel

- On spoke
  - VPN Tunnel establishment (Phase 1)

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.0.2.10/500        192.0.2.2/500         none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify: RSA
      Life/Active Time: 86400/36791 sec
 IPv6 Crypto IKEv2 SA
```


Verify the tunnel

- On spoke

  - VPN Tunnel establishment (Phase 2)

```
Spoke1#show crypto ipsec sa
interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 192.0.2.10
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.0.2.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.2/255.255.255.255/47/0)
   current_peer 192.0.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28824, #pkts encrypt: 28824, #pkts digest: 28824
    #pkts decaps: 28814, #pkts decrypt: 28814, #pkts verify: 28814
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.10, remote crypto endpt.: 192.0.2.2
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x2339D26(36936998)
     PFS (Y/N): N, DH group: none
```


Verify the tunnel

- On spoke

  - VPN Tunnel establishment (Phase 2)

```
local crypto endpt.: 192.0.2.10, remote crypto endpt.: 192.0.2.2
plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x2339D26(36936998)
PFS (Y/N): N, DH group: none

inbound esp sas:
 spi: 0x25AD872B(632129323)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Transport, }
   conn id: 78, flow_id: SW:78, sibling_flags 80000000, crypto map: Tunnel100-head-0
   sa timing: remaining key lifetime (k/sec): (4317636/2552)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

outbound esp sas:
 spi: 0x2339D26(36936998)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Transport, }
   conn id: 77, flow_id: SW:77, sibling_flags 80000000, crypto map: Tunnel100-head-0
   sa timing: remaining key lifetime (k/sec): (4317635/2552)
```


Verify the tunnel

- On spoke

  - NHRP registration

```
Spoke1#show ip nhrp nhs
Legend:E=Expecting replies, R=Responding, W=Waiting
Tunnel100:
172.16.1.254 RE NBMA Address: 192.0.2.2 priority = 0 cluster = 0
```

  - Ping the Hub’s tunnel address

```
Spoke1#ping 172.16.1.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/9/15 ms
```


Verify the tunnel

- On spoke

  - Verify EIGRP came up and exchanged routes

```
Spoke1#show ip route
<output omitted>
S*    0.0.0.0/0 [1/0] via 192.0.2.9
      10.0.0.0/32 is subnetted, 2 subnets
C        10.255.255.1 is directly connected, Loopback100
D        10.255.255.255 [90/27008000] via 172.16.1.254, 01:07:33, Tunnel100
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Tunnel100
L        172.16.1.1/32 is directly connected, Tunnel100
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.8/30 is directly connected, GigabitEthernet0/1
L        192.0.2.10/32 is directly connected, GigabitEthernet0/1
```

Troubleshooting

- ISAKMP establishment

  - IKEv1 uses 6 packets with Main Mode (MM1-MM6). Use debug to determine which packets make it across the network

    ```
    debug crypto isakmp
    debug crypto ipsec
    ```

  - IKEv2 uses 2 messages (IKE-INIT and IKE-AUTH). Use debugs to determine which packets make it across the network. Each message has a request and a corresponding response.

    ```
    debug crypto ikev2
    debug crypto ikev2 packet
    debug crypto ipsec
    ```

Troubleshooting

- ISAKMP establishment

  - IKEv1/IKEv2 and IPsec use the following protocols. Ensure connectivity across network for each protocol:

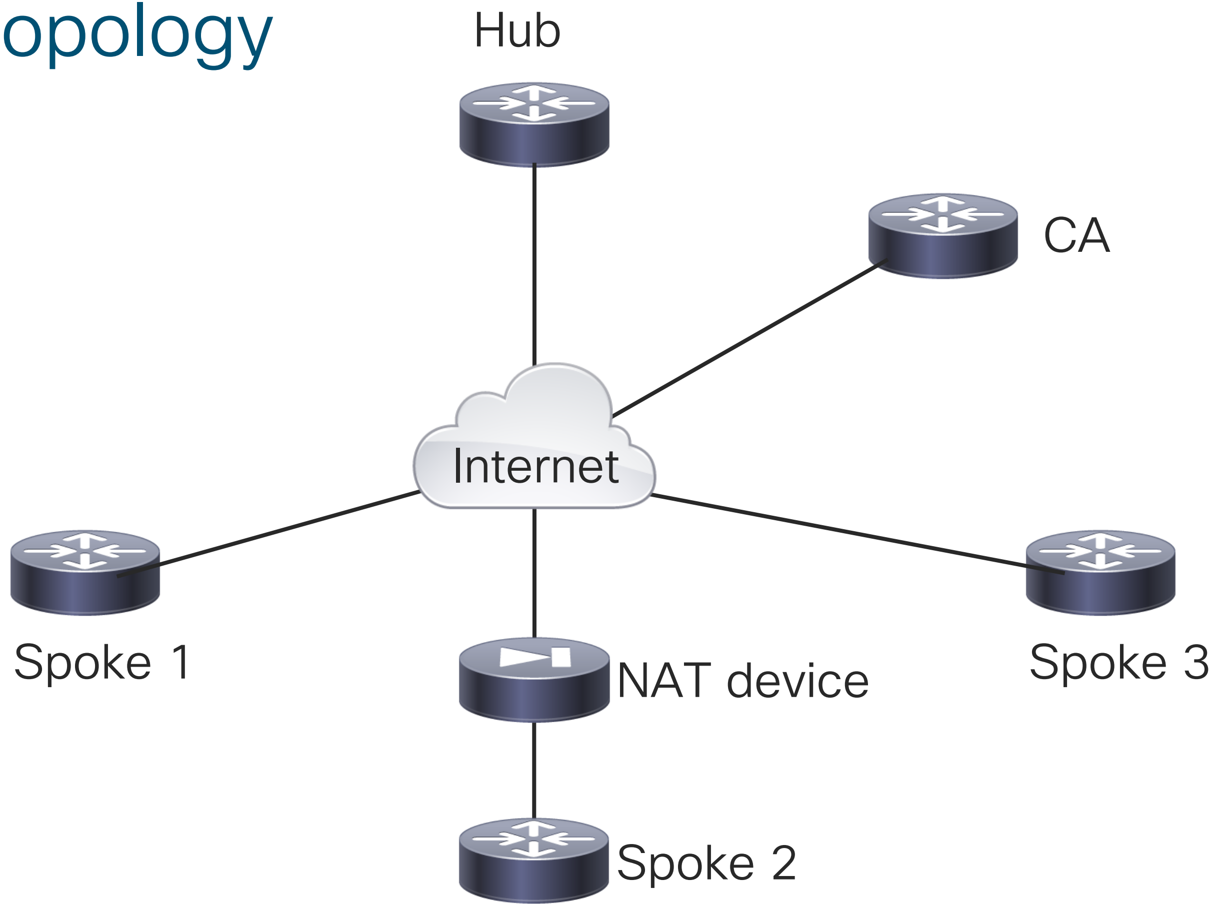
```
UDP/500 – Normal case
ESP - IP protocol 50
UDP/4500 - If NAT is detected in path
```

  - Certificates are large and will make the authentication part of the ISAKMP exchanges large too. This will generate large UDP packet that will need to be fragmented. Ensure path can handle fragmented packet or use IKEv2 fragmentation.

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ipsec
```

Demo Time!!!!!

Lab Topology



Troubleshooting Solutions

- Spoke 2's BIG packets never made it to the Hub
  - Used "`debug crypto ikev2`" and "`debug crypto ikev2 packet`" to see the IKE-AUTH Request wasn't getting there.
  - Tested with pings and large pings. Large packets wouldn't make it
  - Instead of fragmenting at Layer-3 (IP) move up the stack and fragment at Layer-7 (IKE Fragmentation) with "`crypto ikev2 fragmentation mtu <x>`" command

- Spoke 2's IKE-AUTH Request still never made it to the Hub
  - Saw the drops on ACL/saw the packet in packet capture
  - But didn't see the packet in IKEv2 debugs

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.

Continue your education

- Demos in the Cisco campus
- Walk-in self-paced labs
- Meet the engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**