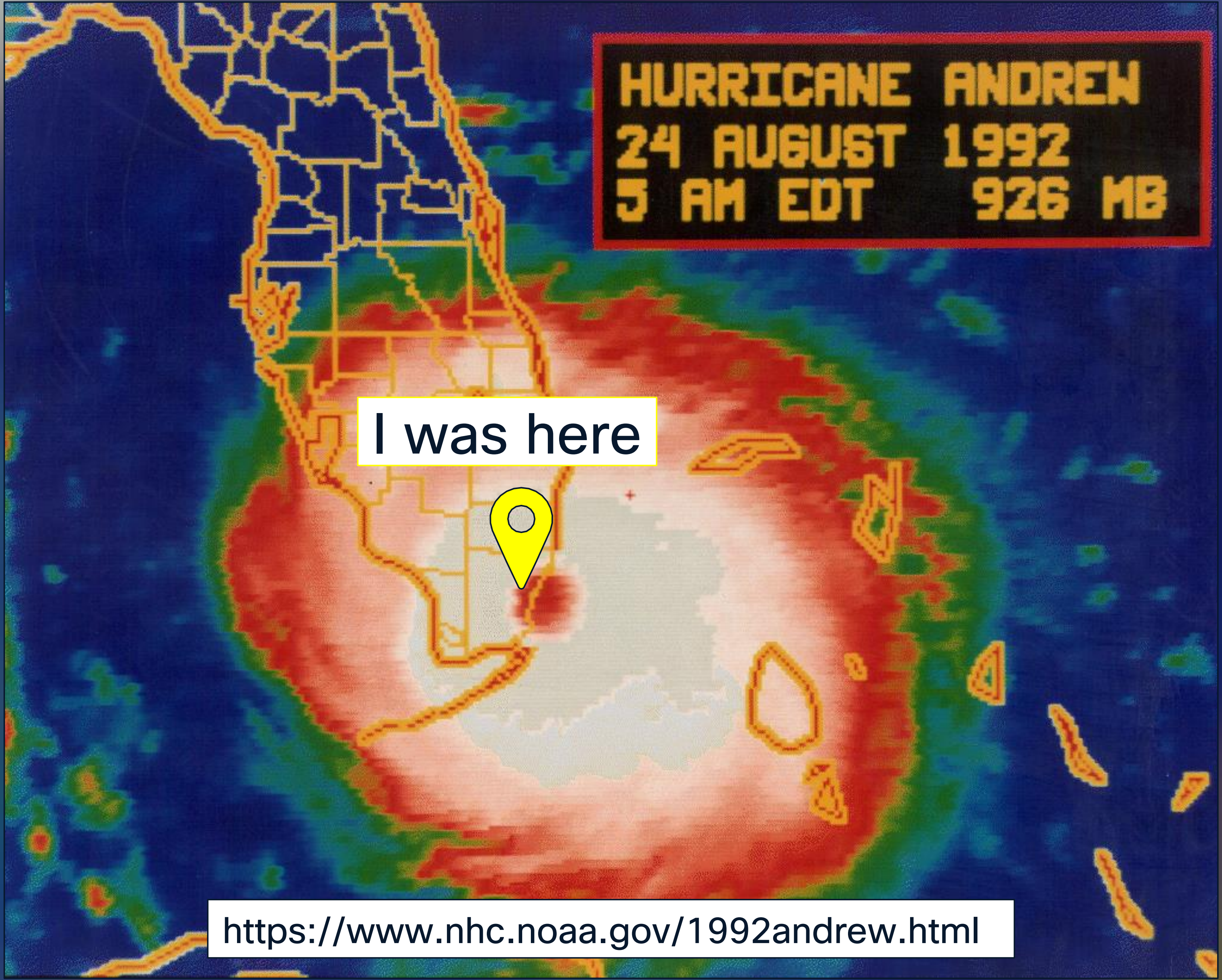
Are You Prepared for the Next Typhoon?

cisco Live!

Paul Giralt
Distinguished Engineer

Steve Nowell
Principal Architect

BRKSEC-2499



I was here

https://www.nhc.noaa.gov/1992andrew.html

Agenda

01 Introduction

02 Salt Typhoon Overview

03 Prevention and Defense

04 Looking to the Future

Cisco Webex App

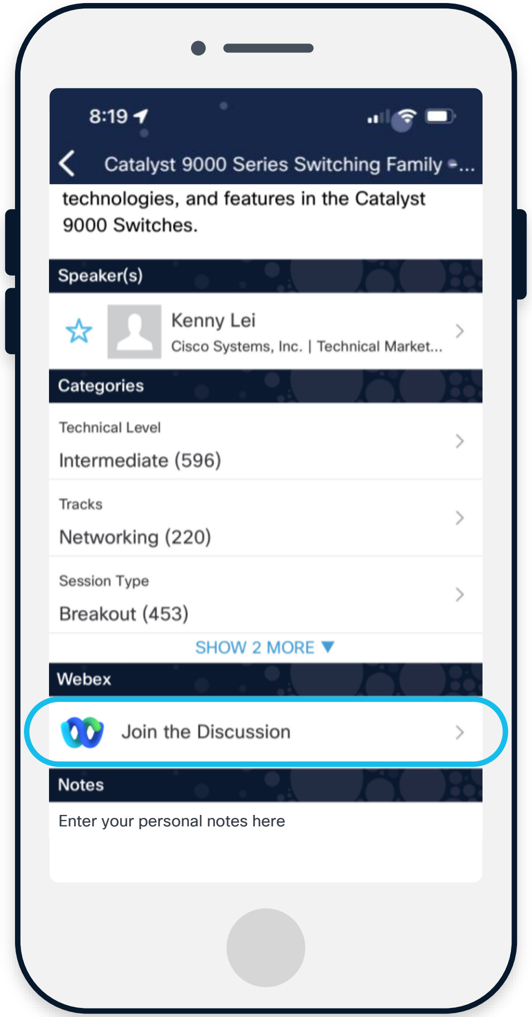
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2025.



8:19

Catalyst 9000 Series Switching Family •...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Do not edit
How to change the design

What best describes the company or partner you work for?

The Slido app must be installed on every computer you’re presenting from

Do not edit
How to change the design

How much do you know about Salt Typhoon?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

> “[Salt Typhoon] represents the most serious and significant cyber threat to our nation, and in particular, U.S. critical infrastructure.”

Jen Easterly

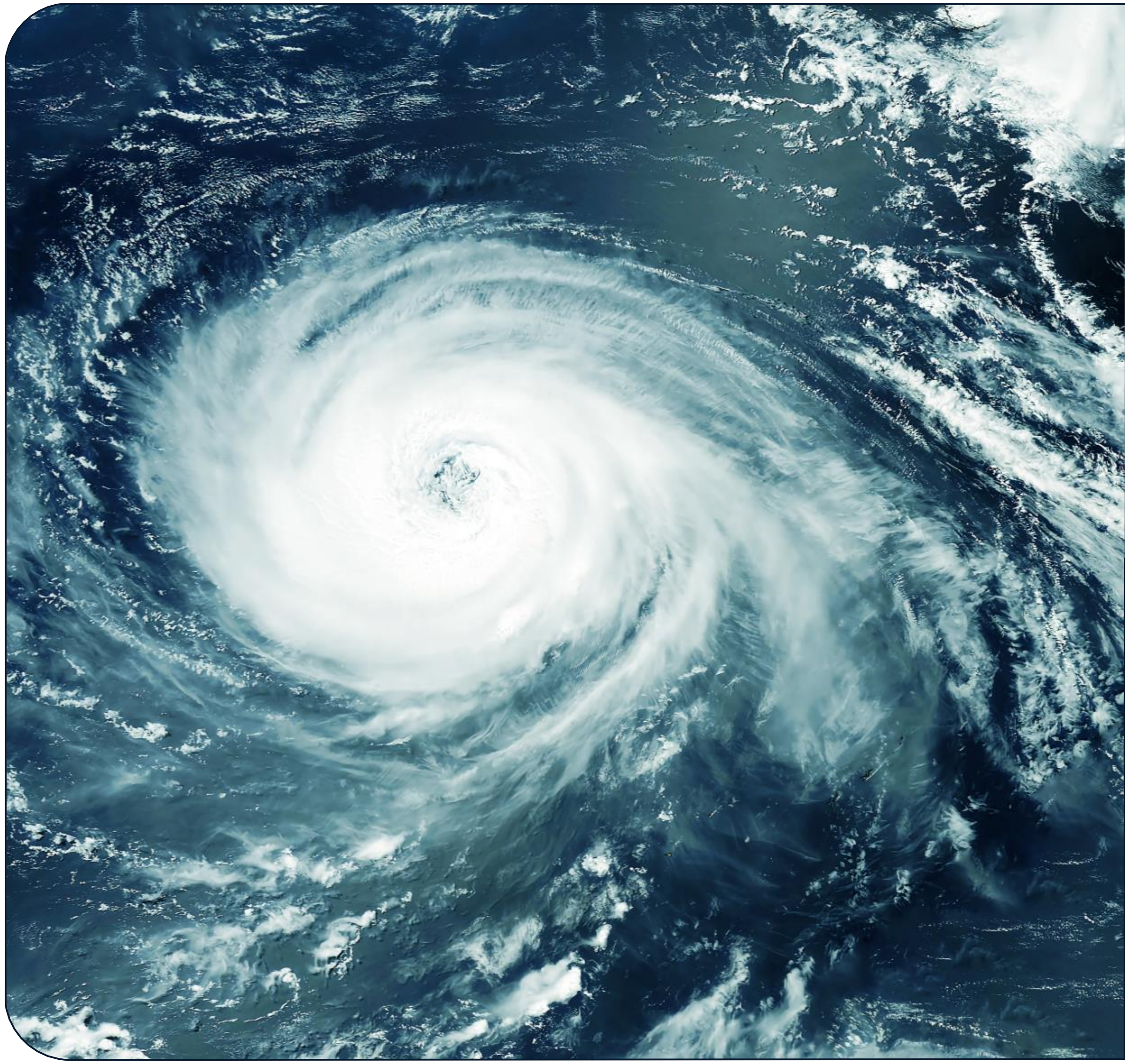
Former Director, US Cybersecurity and Infrastructure Security Agency (CISA)

Source: https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

Salt Typhoon Campaign Overview

Who is Salt Typhoon*?

- State Sponsored Advanced Persistent Threat (APT) actor – name given by Microsoft
- Tenacious, patient, multi-faceted, long dwell time attacks
- US focused but targets in other countries under attack
- Apparent goal of espionage and network reconnaissance
- Heavy use of Living off the Land (LOTL) techniques
- Attacks against products from many different vendors



* The observations in this presentation represent Cisco's understanding of the Salt Typhoon attacks based on available information. The attacks and their impact are still being researched and assessed, and the situation continues to evolve. For the latest, refer to the Cisco Talos blog page: https://blog.talosintelligence.com/author/cisco/

Cisco Talos Report

REFERENCE

https://blog.talosintelligence.com/salt-typhoon-analysis/

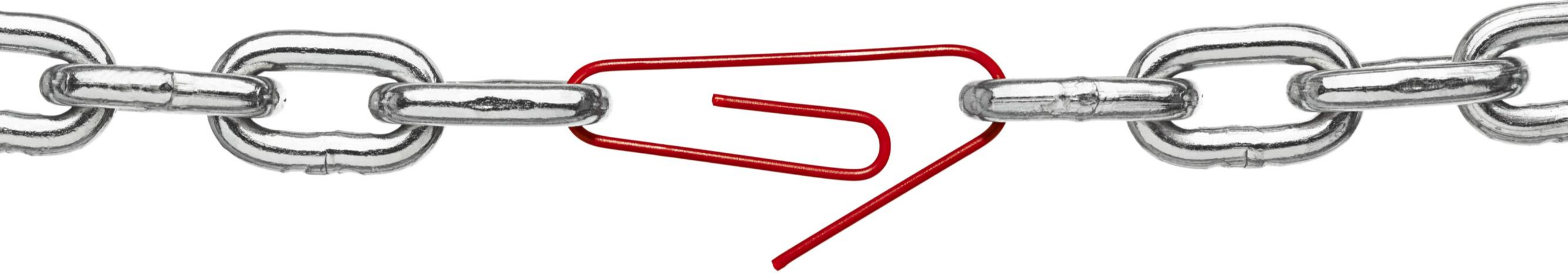
Weathering the storm: In the midst of a Typhoon

By Cisco Talos

THURSDAY, FEBRUARY 20, 2025 08:00

THREAT SPOTLIGHT

How did they get in?



The Weakest Link

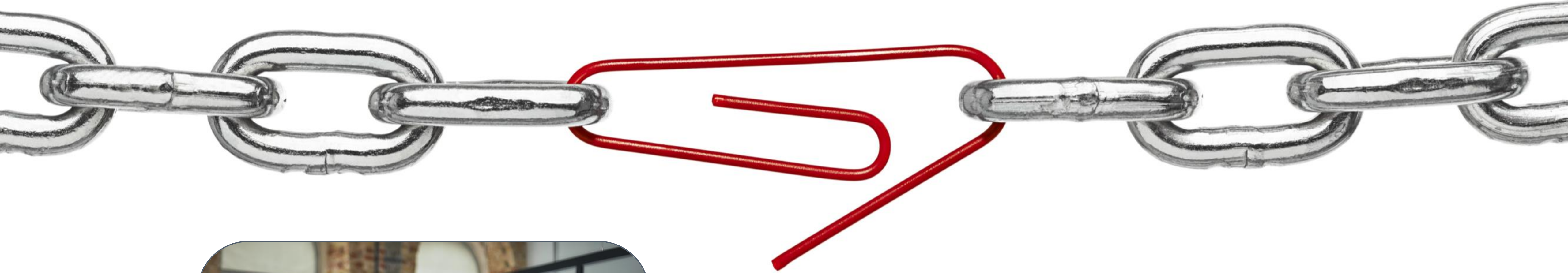
IBM, Stanford University and Verizon all highlight how human behavior, especially around everyday decision-making, is the dominant factor in security breaches. **It was discovered that about 90% of these breaches were sourced by human mistakes**.

https://blogs.cisco.com/security/the-90-5-5-concept-your-key-to-solving-human-risk-in-cybersecurity

How did they get in?

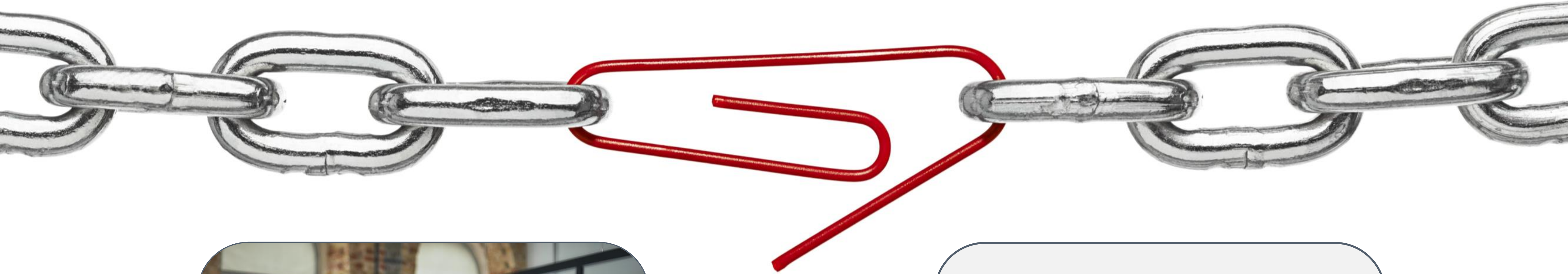
- **Use of valid, stolen credentials**
  - Phishing Attack
  - MFA fatigue attack
  - Data Breach
  - Credential Reuse
  - Brute Force Attack
  - Man in the Middle
  - Malware / Keylogger
  - Insider Threat

How did they get in?



Legitimate User Credentials

How did they get in?



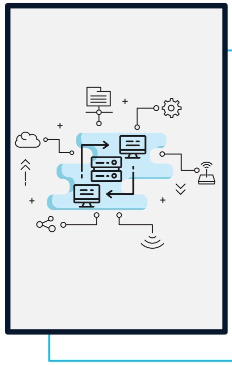
Legitimate User
Credentials

Old, Unpatched Software
(CVE-2018-0171)

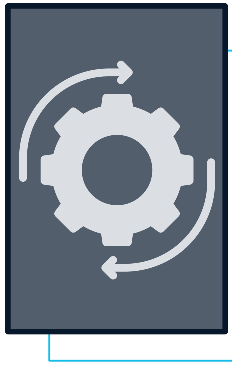
What did they do?

Credential Use and Expansion

Configuration Exfiltration



Infrastructure Pivoting



Configuration Modification

Do not edit
How to change the design

What is the password for this user?

username admin password 7 0104030550

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Salt Typhoon – Credential Use and Expansion

Credential Use and Expansion

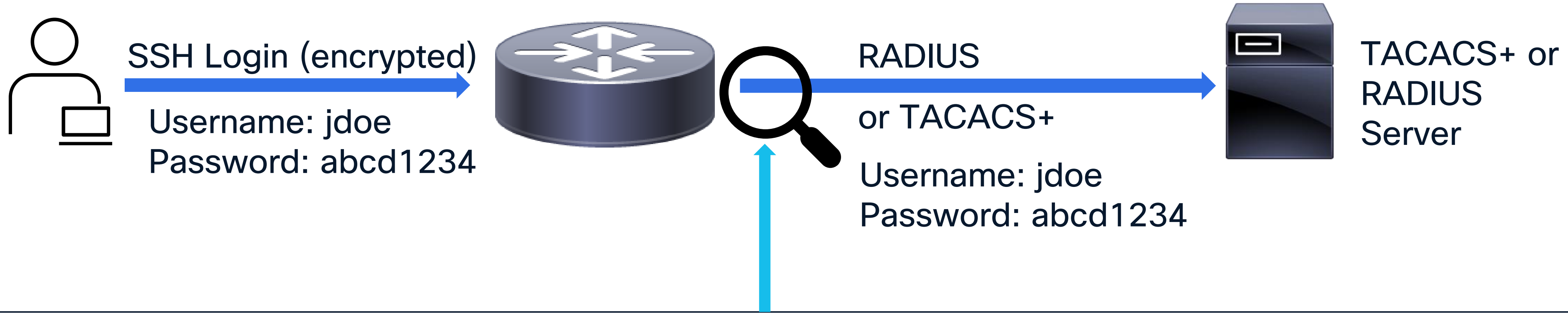
- Acquisition of additional credentials
  - Deciphering local accounts / keys with weak password types

```
radius server test
 address ipv4 10.1.2.3 auth-port 1812 acct-port 1813
 key 7 15060E1F10

tacacs server test
 address ipv4 10.1.2.3
 key 7 15060E1F10

username ciscolive password 7 10590C180E

snmp-server community DONTDOTHIS RW
```

Salt Typhoon – Credential Use and Expansion

Credential Use and Expansion

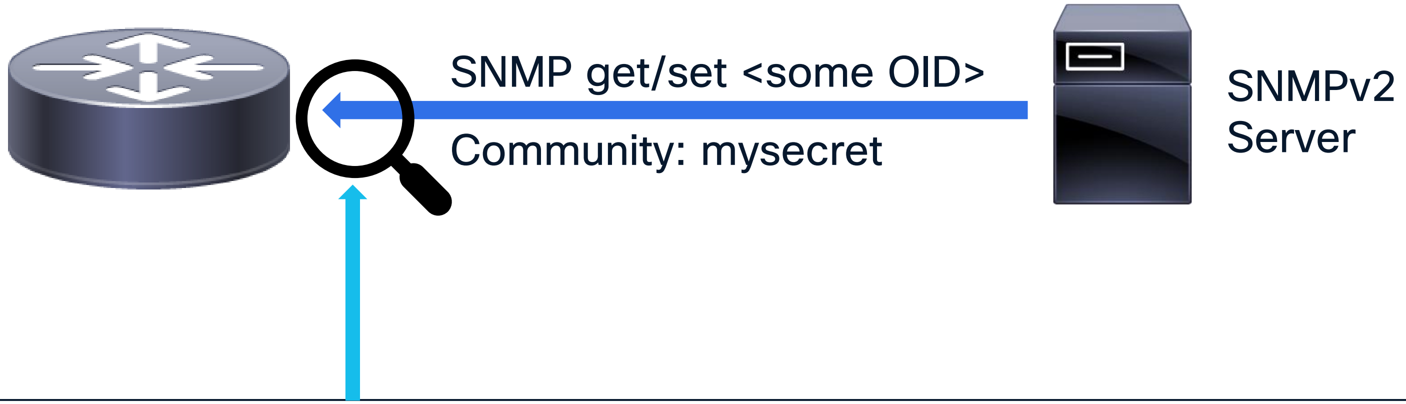
- Acquisition of additional credentials
  - Deciphering local accounts / keys with weak password types
  - Capture of unencrypted / weakly encrypted SNMP, TACACS+, and RADIUS traffic



```
Router#monitor capture badguy interface g1 both match ipv4 protocol tcp any any eq 49
```

Salt Typhoon – Credential Use and Expansion

- Acquisition of additional credentials
  - Deciphering local accounts / keys with weak password types
  - Capture of unencrypted / weakly encrypted SNMP, TACACS+, and RADIUS traffic



```
Router#monitor capture badguy interface g1 both match ipv4 protocol udp any any eq 161
```

Salt Typhoon – Configuration Exfiltration

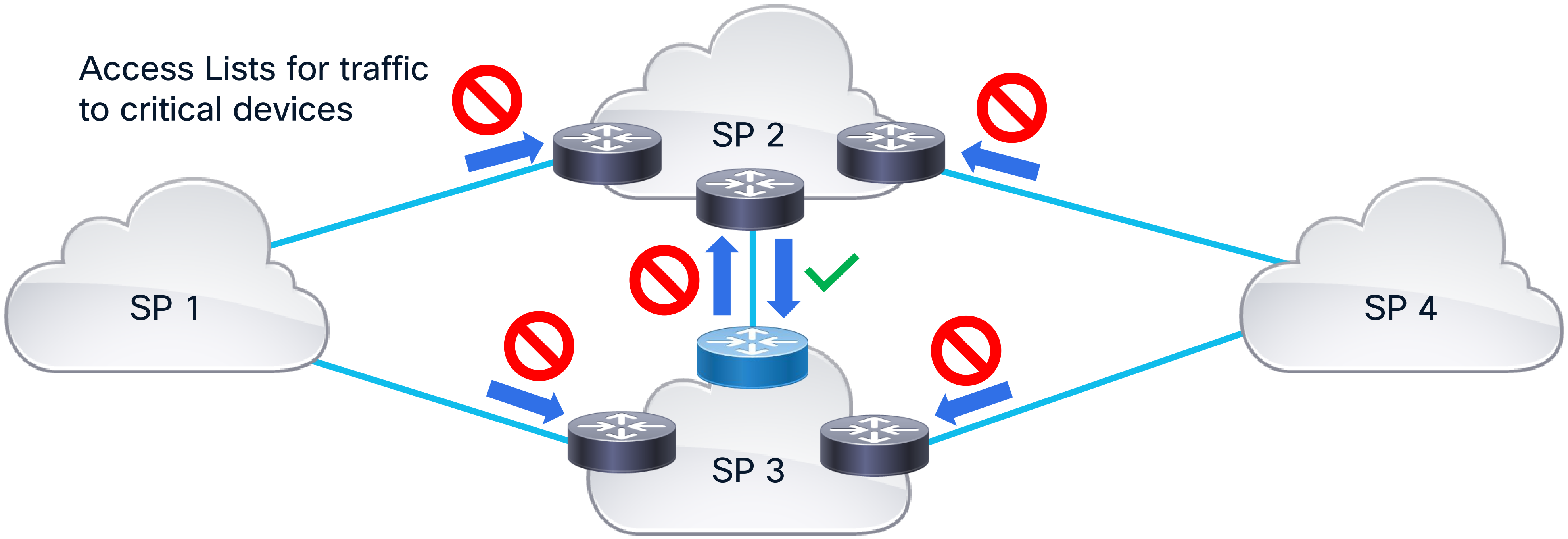
Configuration Exfiltration

- **What does a configuration tell you?**
  - Credentials
  - Device IP Addresses
  - Server Addresses (TACACS+, RADIUS, Logging, NTP, etc...)
  - Access Lists (e.g. what traffic is allowed to management interfaces)
  - Routing Protocol Configuration
  - Neighbor / Peering Connections
  - Interface Descriptions (what is this device connected to)

Salt Typhoon – Infrastructure Pivoting

Infrastructure Pivoting

- Movement within trusted infrastructure
- Originating traffic from trusted sources
- Exploit trusted connections between providers



Access Lists for traffic to critical devices

Salt Typhoon – Configuration Modification

Configuration Modification

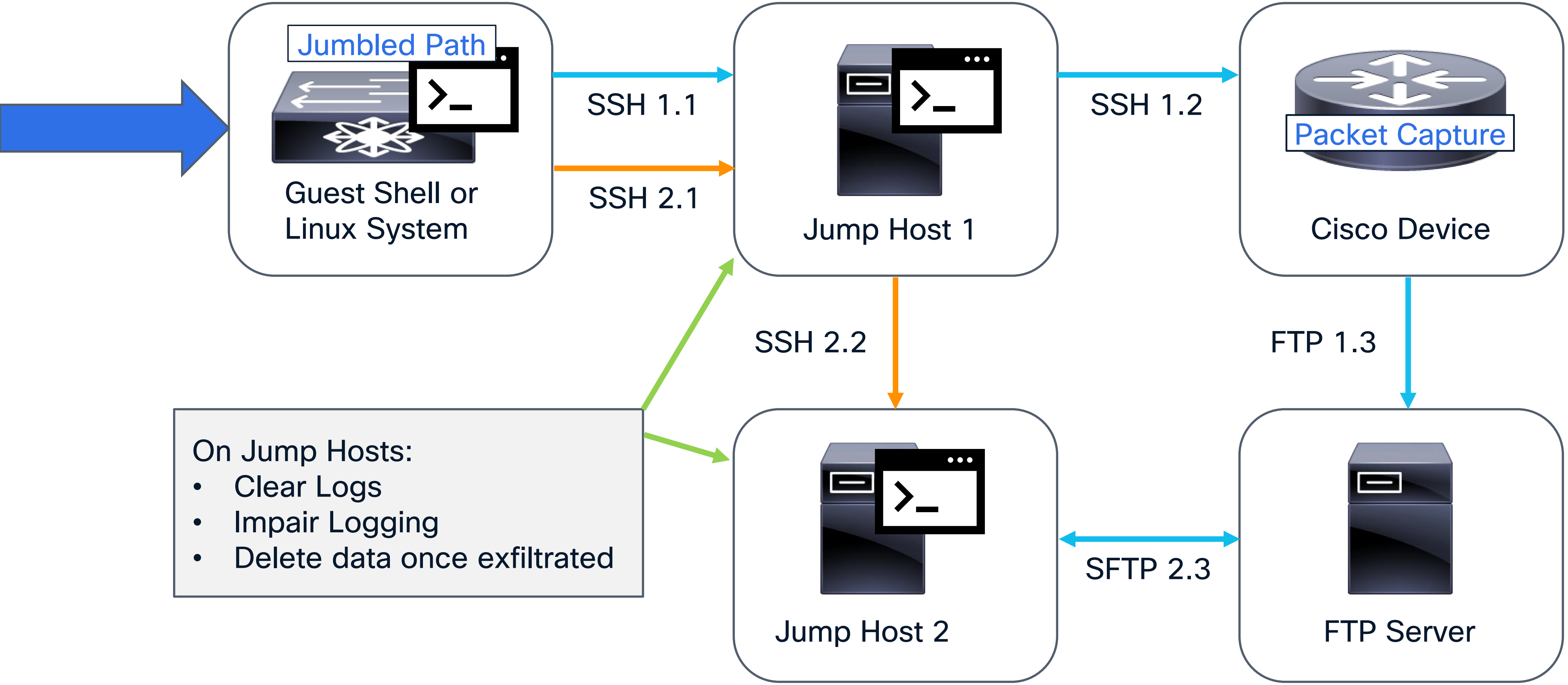
- Modification of device configurations to expand access to network and elevate privileges
  - Creation of unexpected local accounts
  - AAA/TACACS+ server IP address config modification
  - Loopback interface IP address modifications
  - GRE tunnel creation and use
  - ACL modifications
  - SNMP community string modifications
  - HTTP/HTTPS server modifications

Salt Typhoon – Configuration Modification

Configuration Modification

- Modification of configuration to gain a persistent presence and undetected access in the network
  - Strategically enabling and disabling of guest shell environments (Linux shell)
  - Creation of SSH processes in guest shells on high port numbers
  - Creation of Linux-level users (modification of “/etc/shadow” and “/etc/passwd”) in shells
  - Added SSH “authorized_keys” under root or other users at Linux level

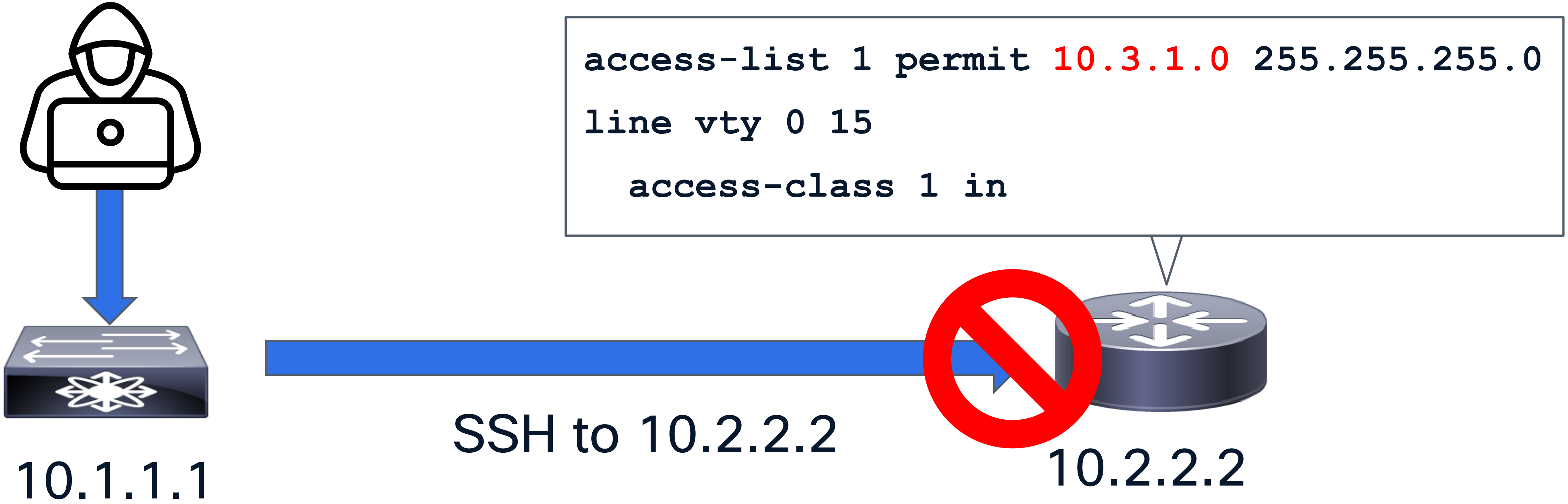
Salt Typhoon – Jumbled Path



On Jump Hosts:

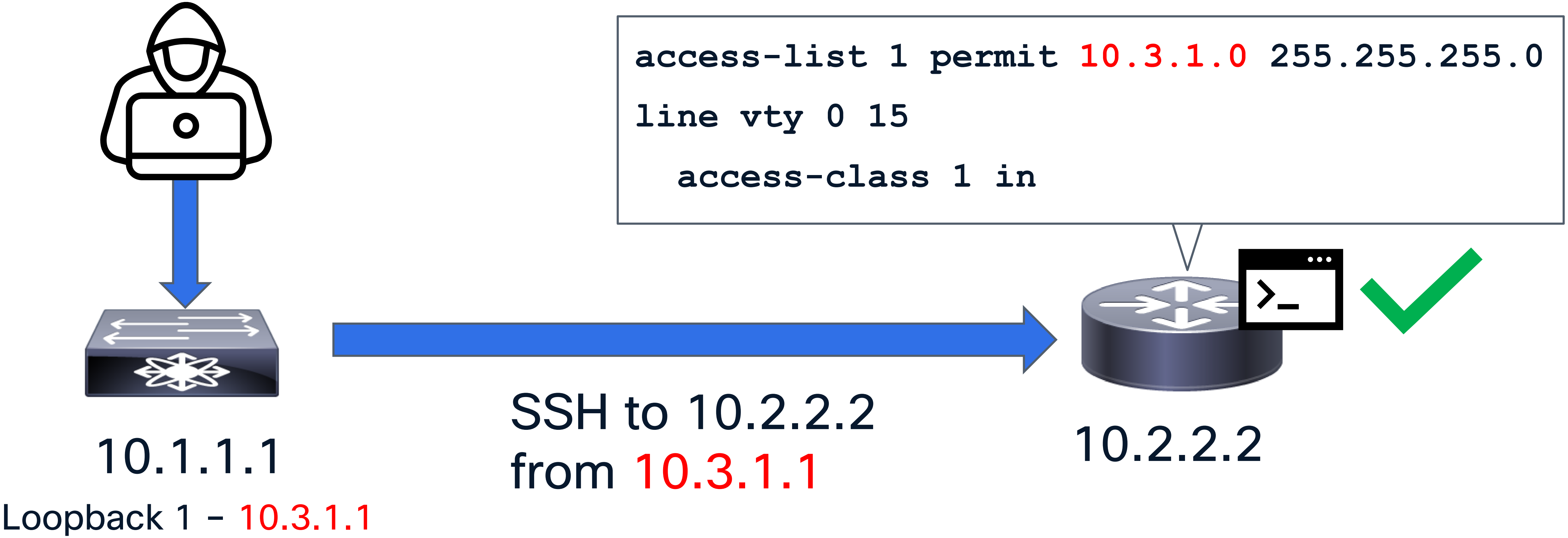
- Clear Logs
- Impair Logging
- Delete data once exfiltrated

Salt Typhoon – Defense Evasion



```
access-list 1 permit 10.3.1.0 255.255.255.0
line vty 0 15
  access-class 1 in
```

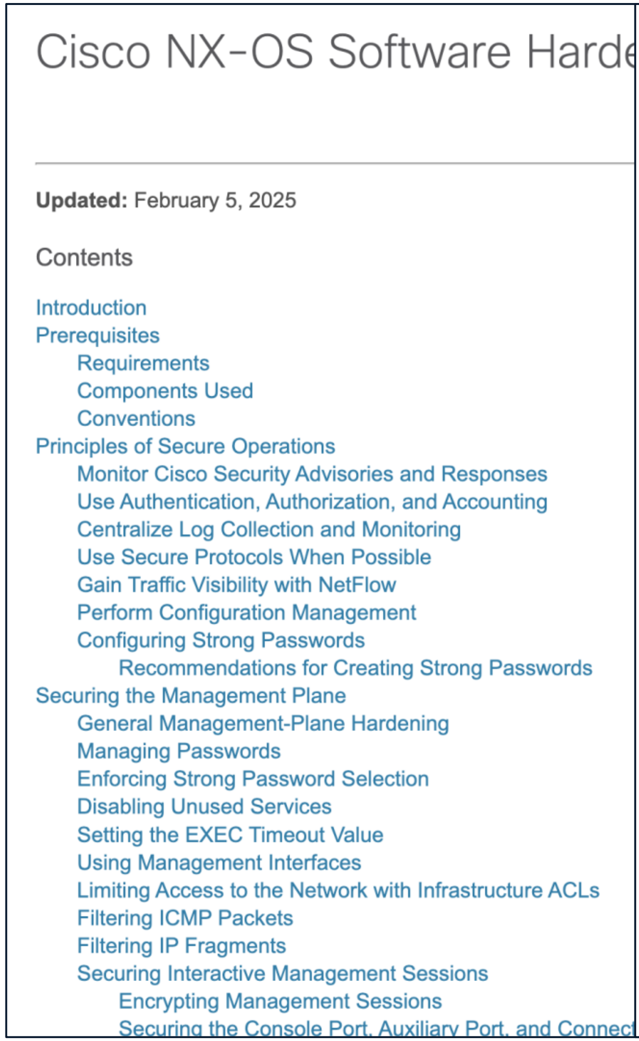
Salt Typhoon – Defense Evasion



```
access-list 1 permit 10.3.1.0 255.255.255.0
line vty 0 15
  access-class 1 in
```

Prevention and Defense

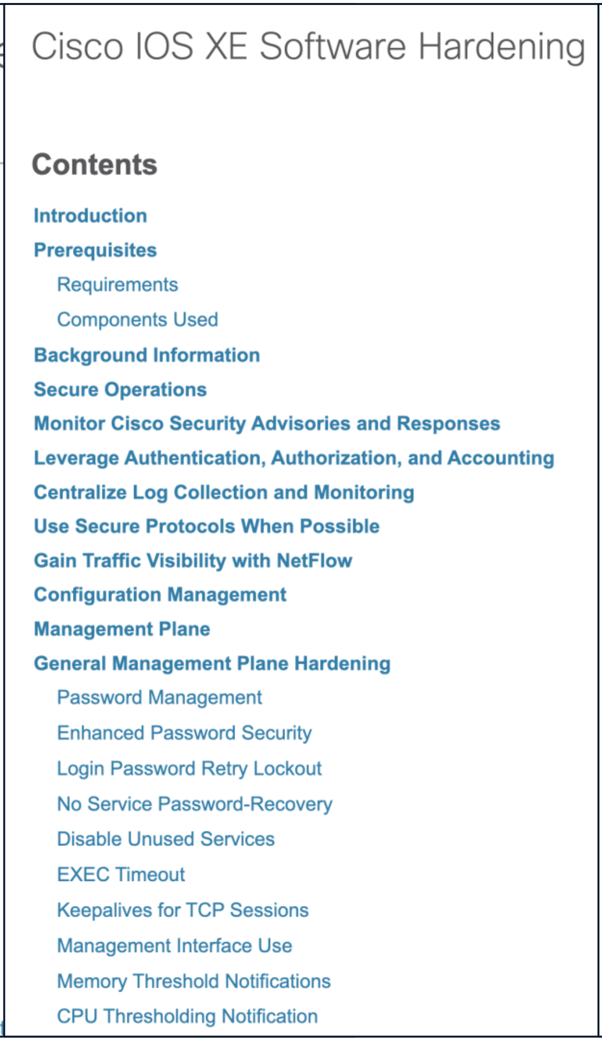
Network Device Hardening Guides



Cisco NX-OS Software Harde

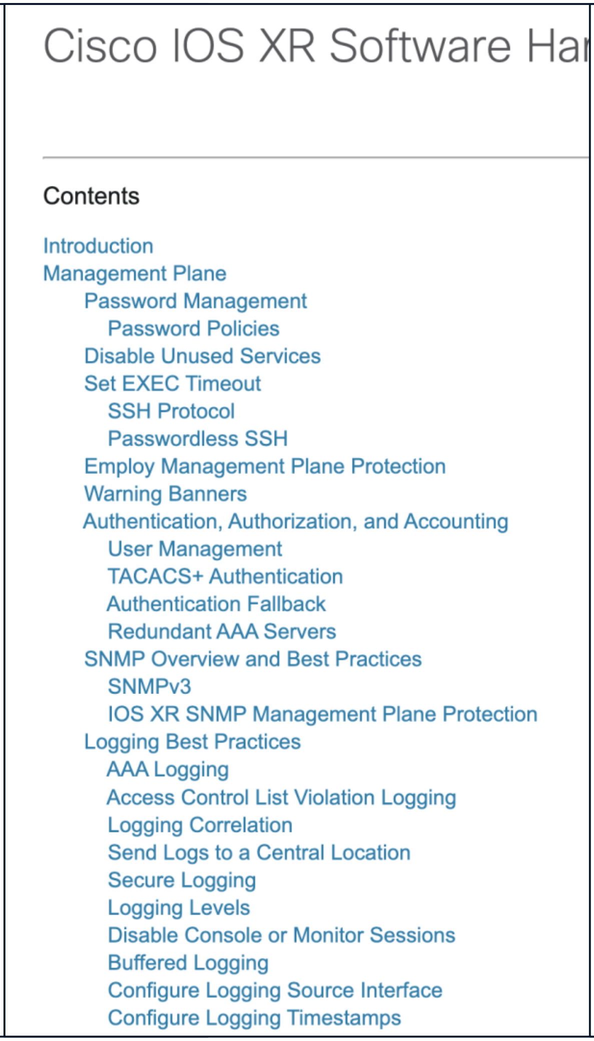
Updated: February 5, 2025

Contents



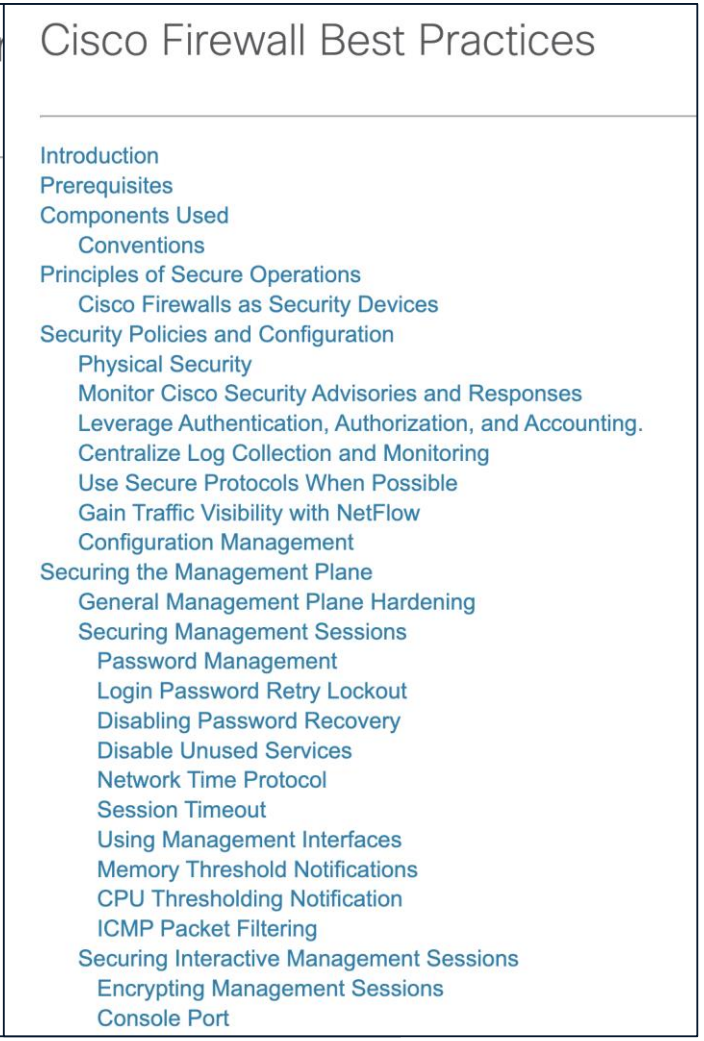
Cisco IOS XE Software Hardening

Contents



Cisco IOS XR Software Har

Contents



Cisco Firewall Best Practices

Network Device Hardening Guides

REFERENCE

NXOS:
https://sec.cloudapps.cisco.com/security/center/resources/securing_nx_os.html

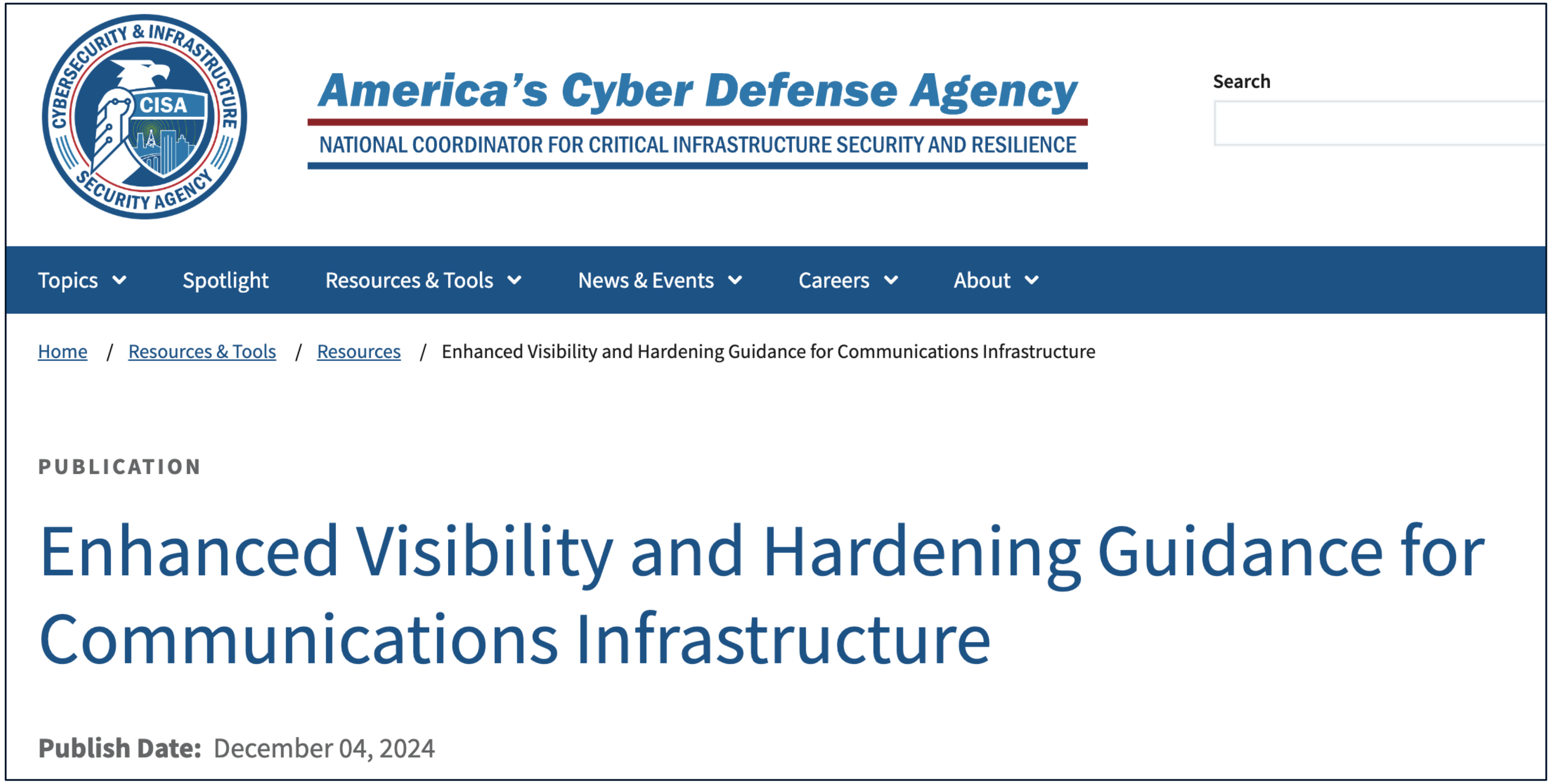
IOS XE:
https://sec.cloudapps.cisco.com/security/center/resources/IOS_XE_hardening

IOS XR:
https://sec.cloudapps.cisco.com/security/center/resources/Cisco-IOS-XR-HardeningGuide

ASA:
https://sec.cloudapps.cisco.com/security/center/resources/firewall_best_practices

Network Device Hardening Guides

REFERENCE



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Home / Resources & Tools / Resources / Enhanced Visibility and Hardening Guidance for Communications Infrastructure

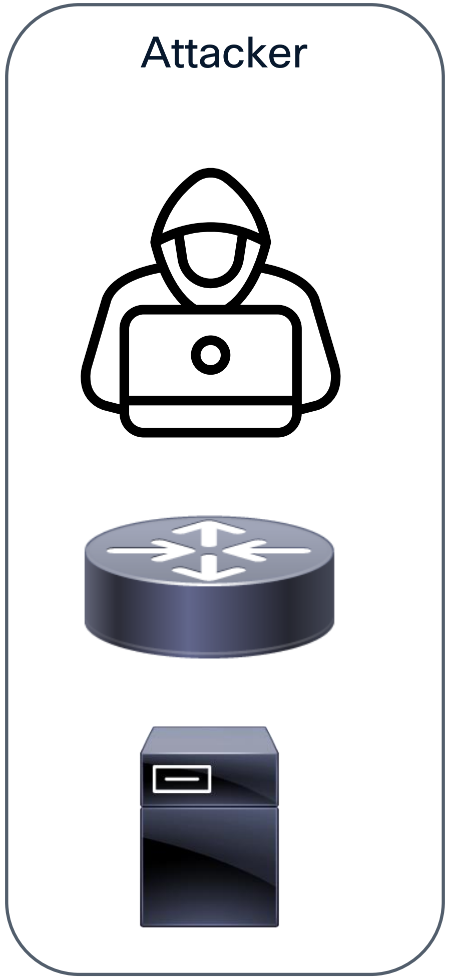
PUBLICATION

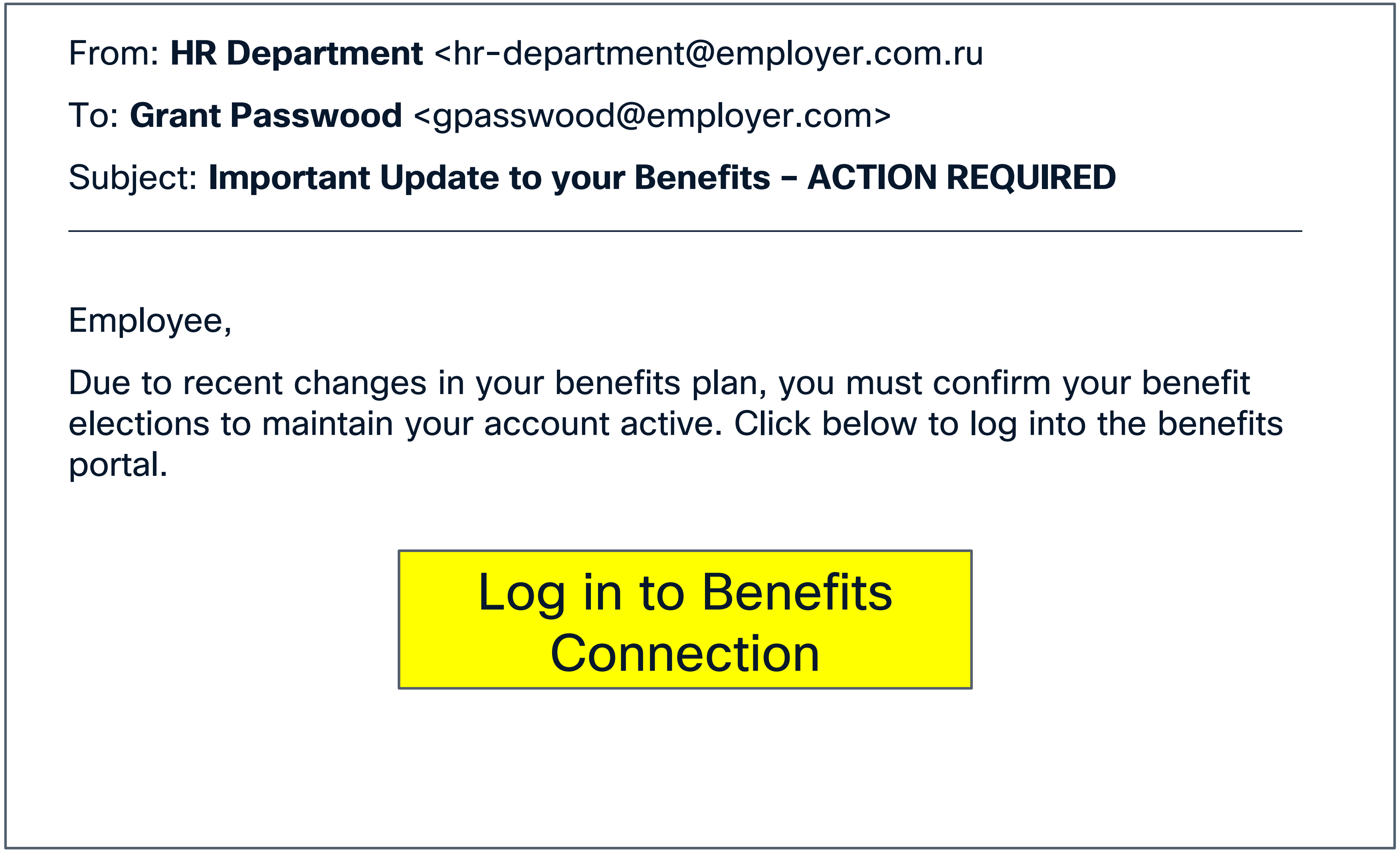
Enhanced Visibility and Hardening Guidance for Communications Infrastructure

Publish Date: December 04, 2024

https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

Protecting from an Attack





From: **HR Department** <hr-department@employer.com.ru

To: **Grant Passwood** <gpasswood@employer.com>

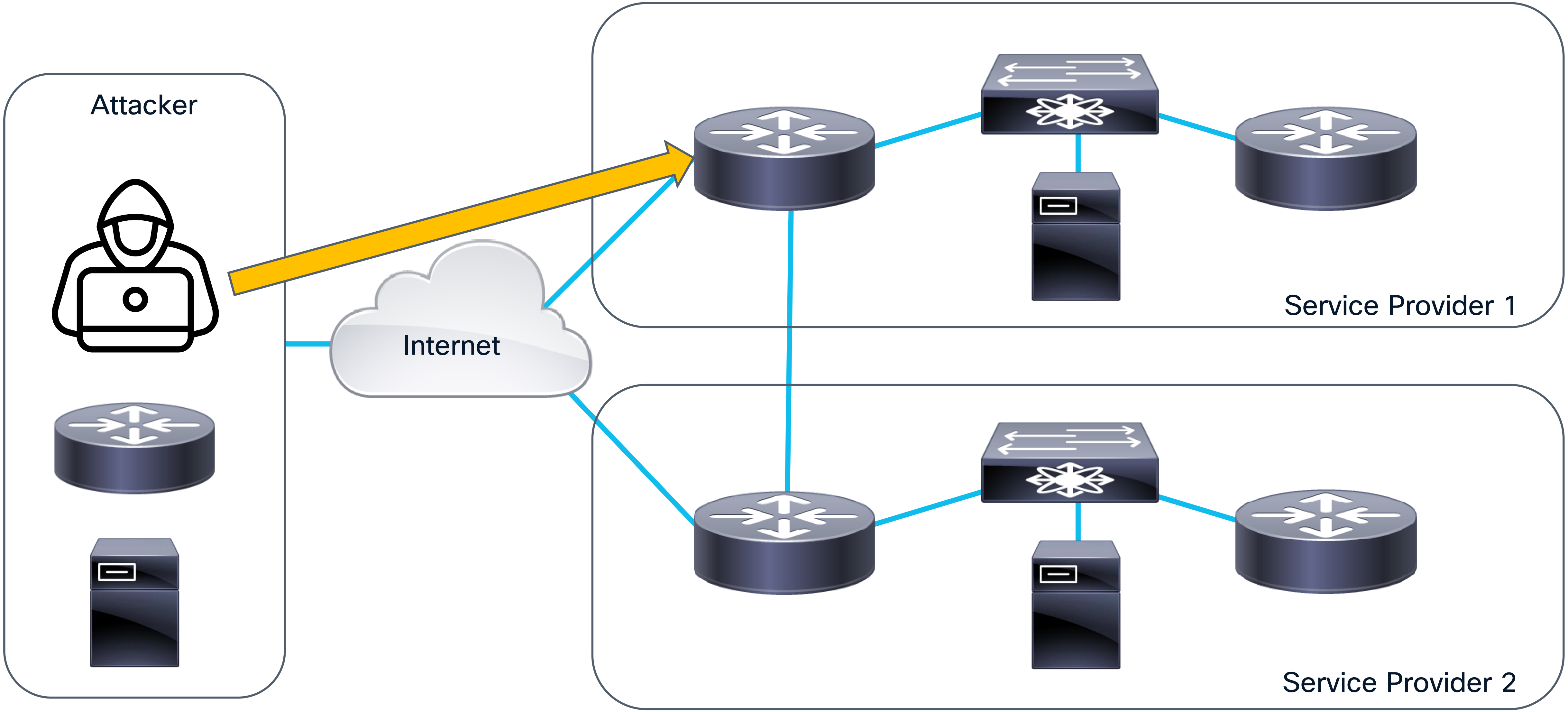
Subject: **Important Update to your Benefits – ACTION REQUIRED**

Employee,

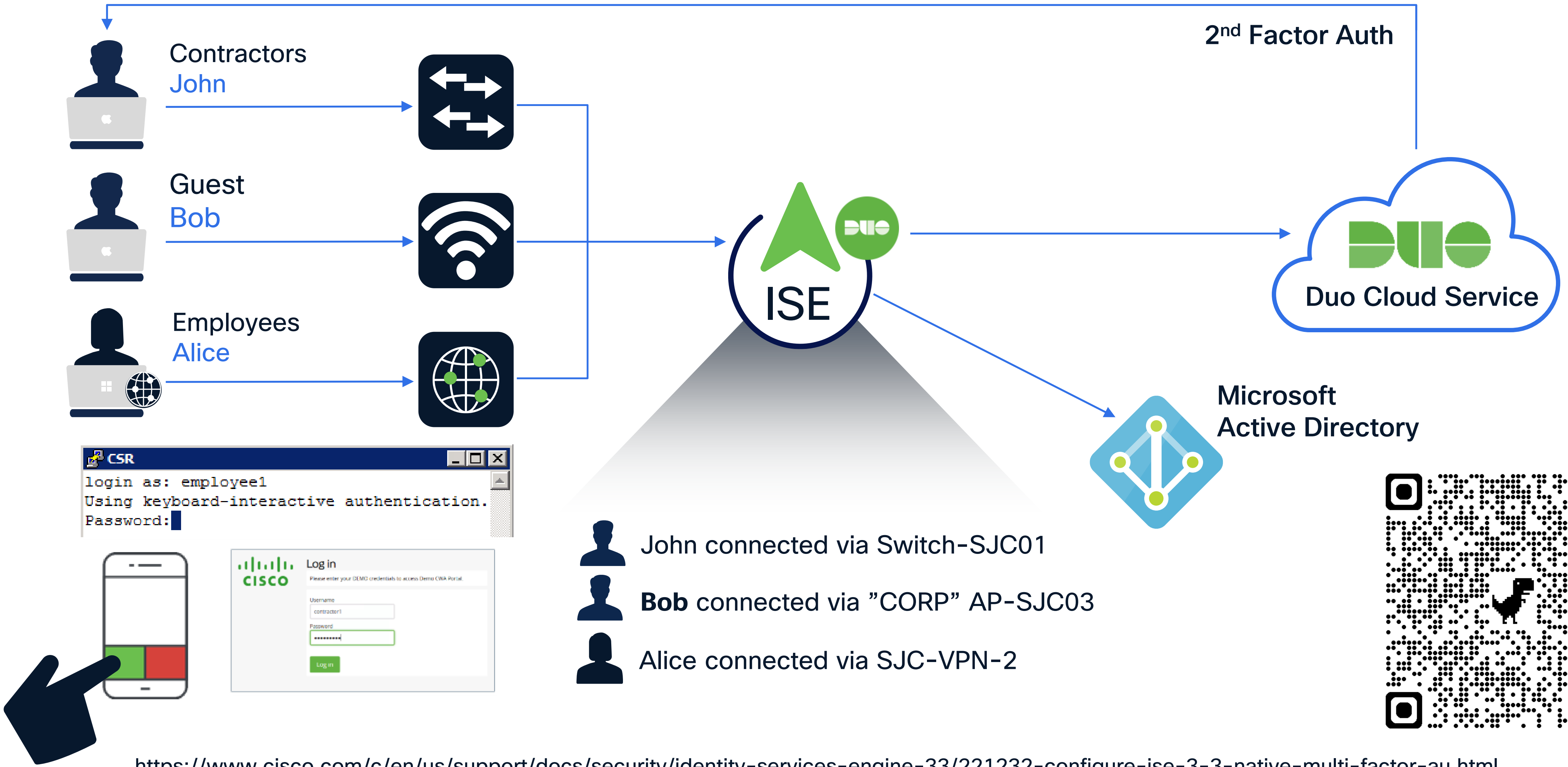
Due to recent changes in your benefits plan, you must confirm your benefit elections to maintain your account active. Click below to log into the benefits portal.

Log in to Benefits Connection

Attack Example Topology



Enable MFA for SSH Logins



```
login as: employee1
Using keyboard-interactive authentication.
Password:
```

Please enter your DEMO credentials to access Demo CWA Portal.

Username: contractor1

Password: ••••••••

John connected via Switch-SJC01

Bob connected via ”CORP” AP-SJC03

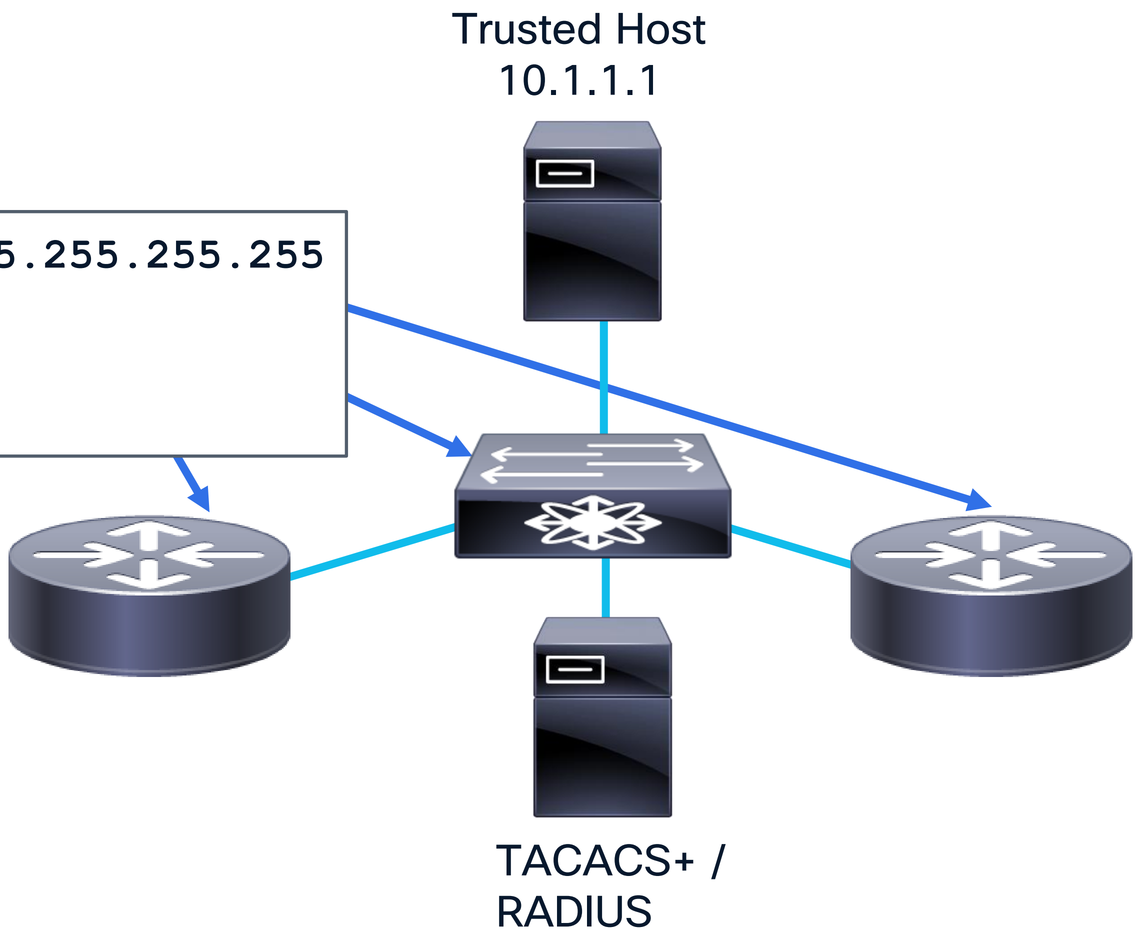
Alice connected via SJC-VPN-2

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-33/221232-configure-ise-3-3-native-multi-factor-au.html

Restricting Management Access

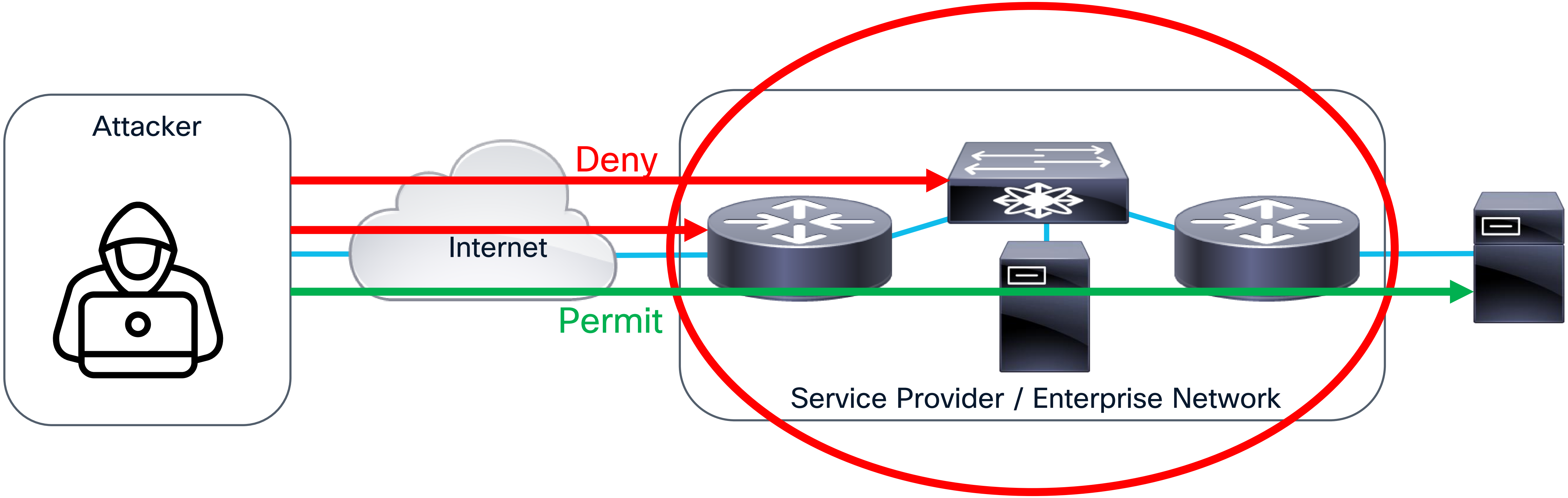
- Management Interface Access Lists
- Trusted Management Hosts
- Infrastructure Access Lists (iACL)

```
access-list 1 permit 10.1.1.1 255.255.255.255
line vty 0 15
  access-class 1 in
```

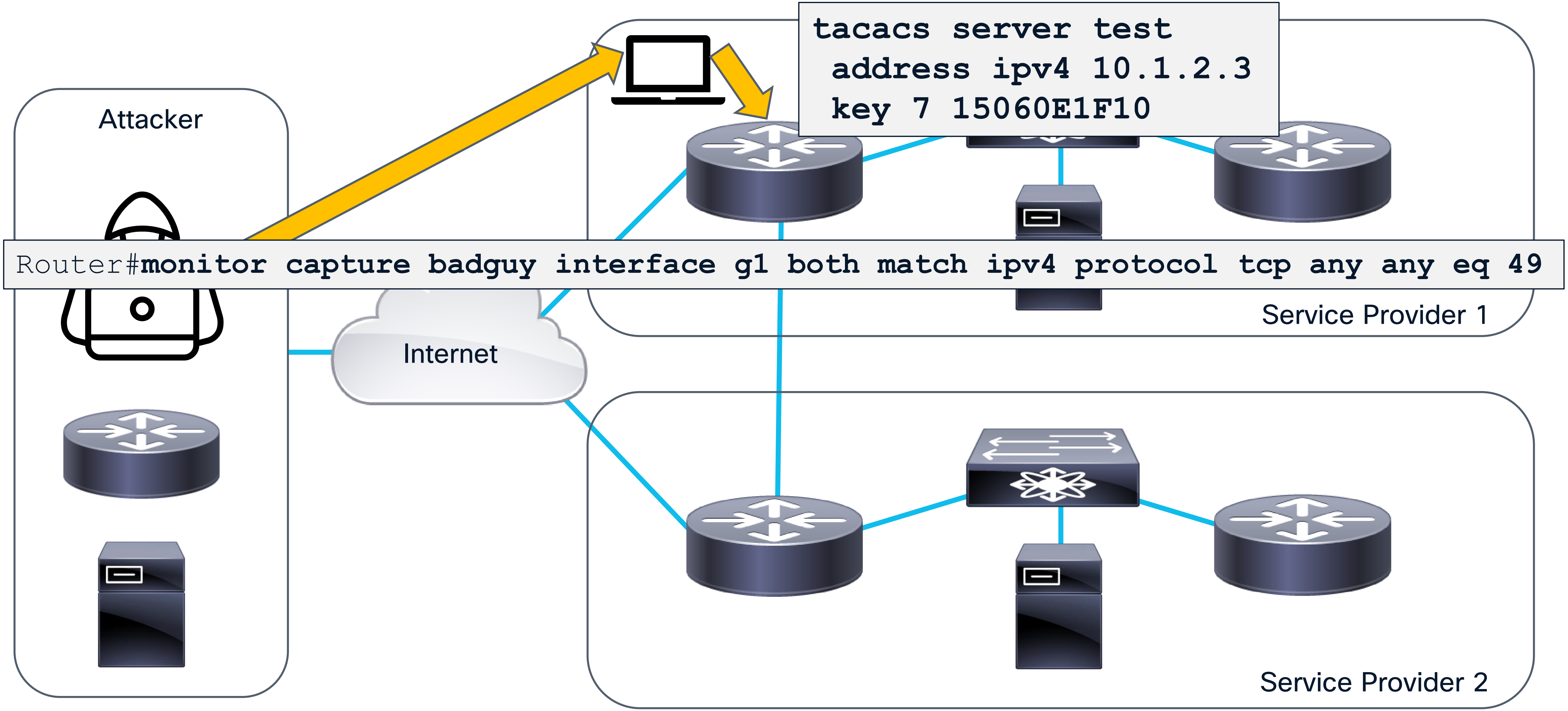


Infrastructure Access Lists (iACLs)

- Inbound filters configured at the routed edge of the network domain
- Logic: traffic *sourced from untrusted network *destined to infrastructure *DENY*
- Logic: transit traffic *PERMIT*



Gathering Additional Credentials

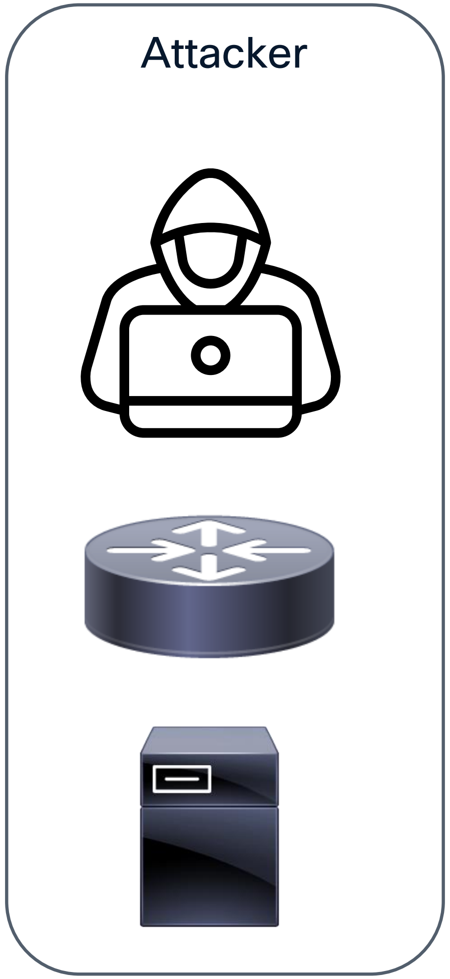


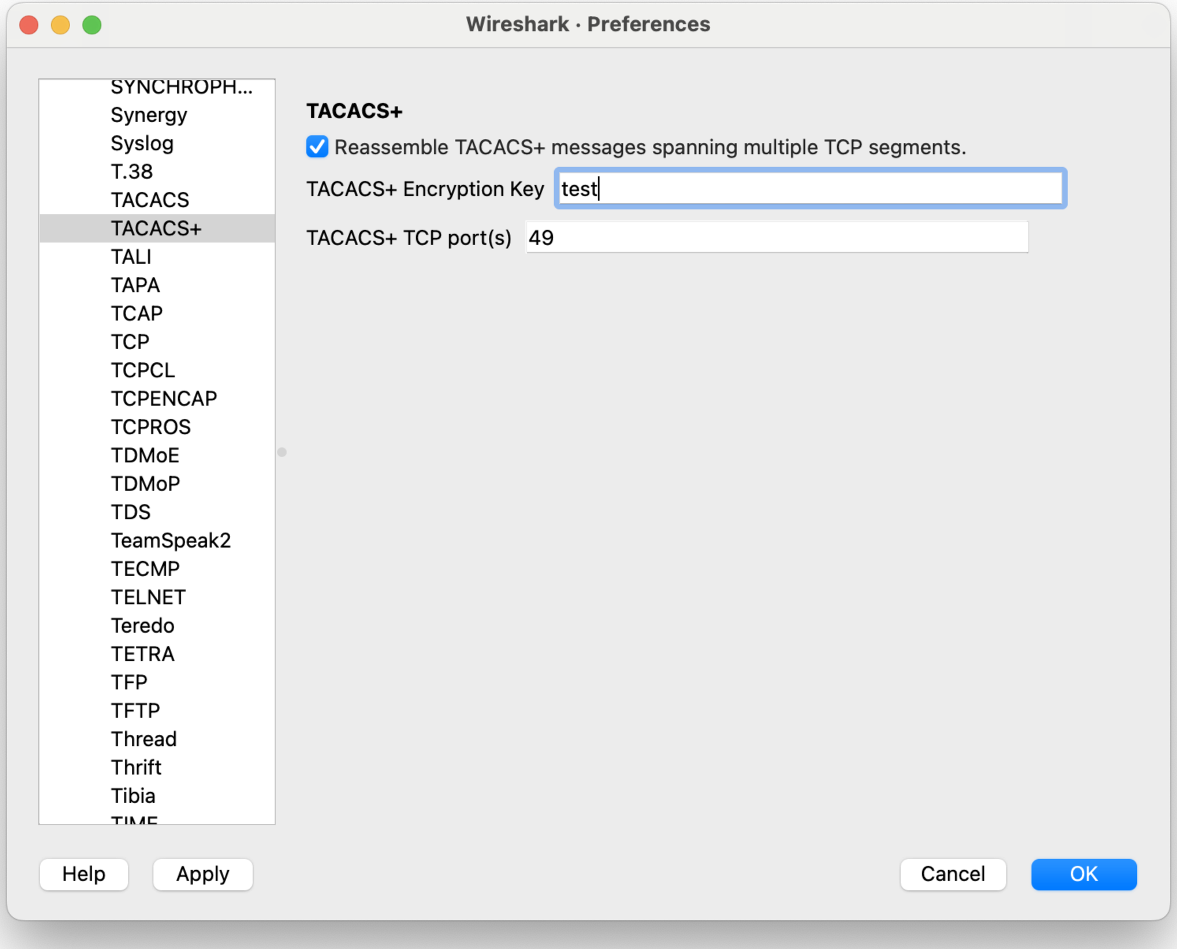
```
tacacs server test
 address ipv4 10.1.2.3
 key 7 15060E1F10
```

```
Router#monitor capture badguy interface g1 both match ipv4 protocol tcp any any eq 49
```

Gathering Additional Credentials

`key 7 15060E1F10` ⟹ "test"





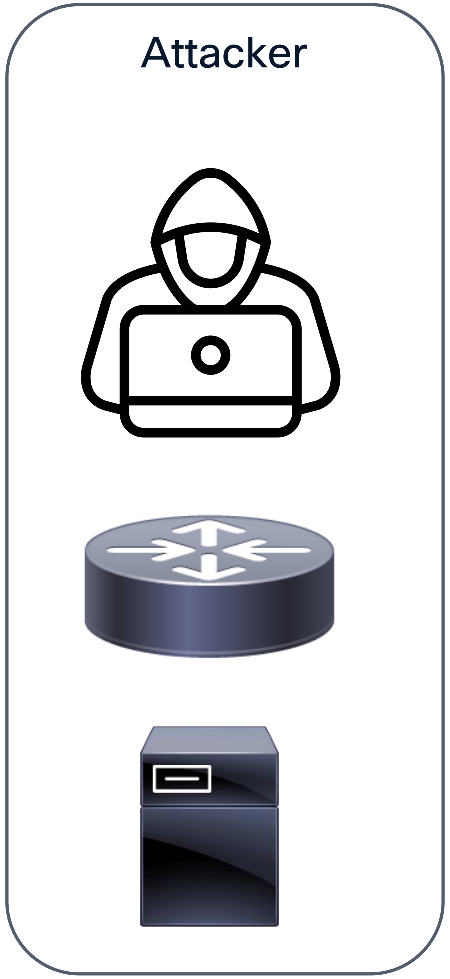
TACACS+

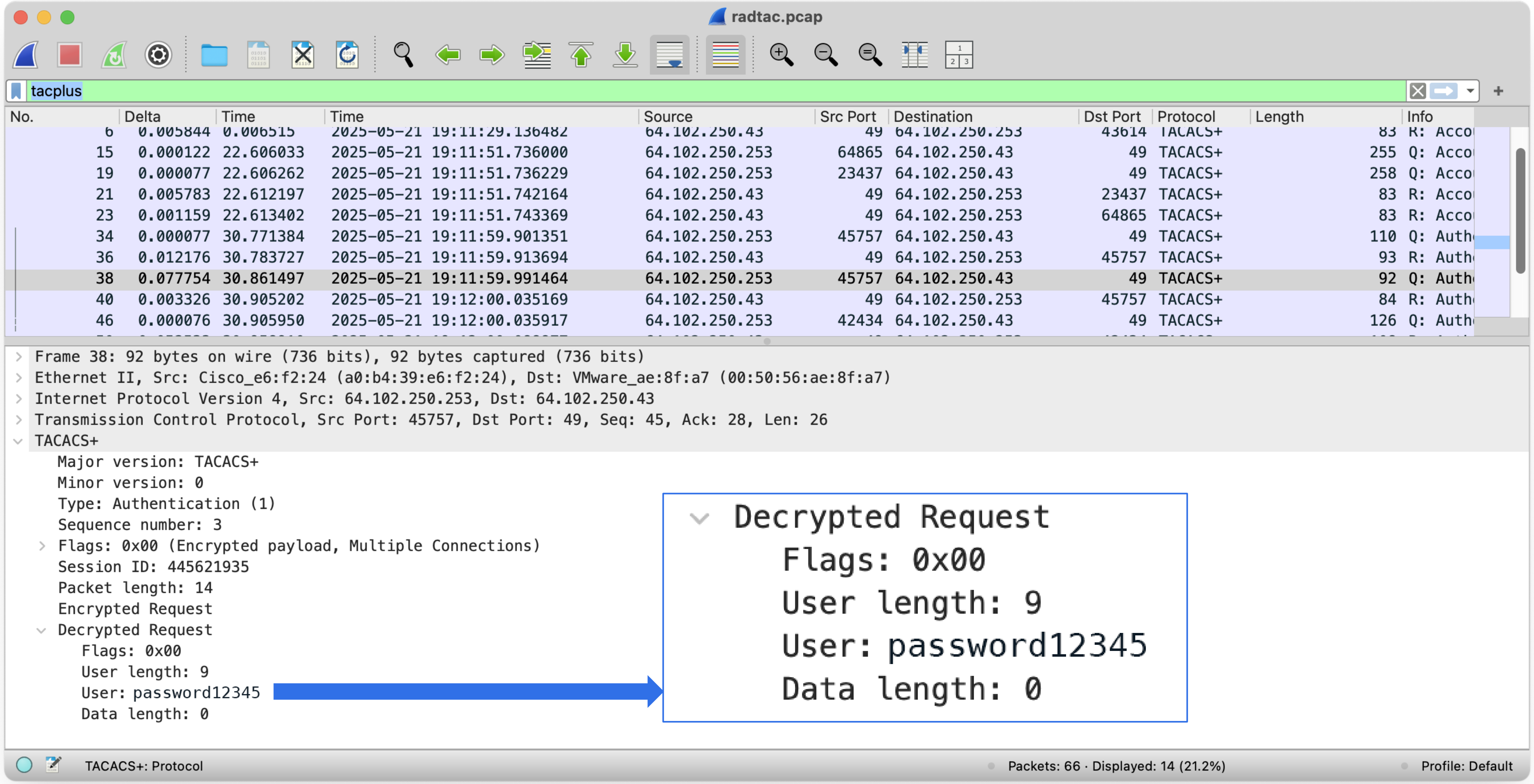
☑ Reassemble TACACS+ messages spanning multiple TCP segments.

TACACS+ Encryption Key: test

TACACS+ TCP port(s): 49

Gathering Additional Credentials





tacplus

No.	Delta	Time	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
6	0.005844	0.006515	2025-05-21 19:11:29.136482	64.102.250.43	49	64.102.250.253	43614	TACACS+	83	R: Acco
15	0.000122	22.606033	2025-05-21 19:11:51.736000	64.102.250.253	64865	64.102.250.43	49	TACACS+	255	Q: Acco
19	0.000077	22.606262	2025-05-21 19:11:51.736229	64.102.250.253	23437	64.102.250.43	49	TACACS+	258	Q: Acco
21	0.005783	22.612197	2025-05-21 19:11:51.742164	64.102.250.43	49	64.102.250.253	23437	TACACS+	83	R: Acco
23	0.001159	22.613402	2025-05-21 19:11:51.743369	64.102.250.43	49	64.102.250.253	64865	TACACS+	83	R: Acco
34	0.000077	30.771384	2025-05-21 19:11:59.901351	64.102.250.253	45757	64.102.250.43	49	TACACS+	110	Q: Auth
36	0.012176	30.783727	2025-05-21 19:11:59.913694	64.102.250.43	49	64.102.250.253	45757	TACACS+	93	R: Auth
38	0.077754	30.861497	2025-05-21 19:11:59.991464	64.102.250.253	45757	64.102.250.43	49	TACACS+	92	Q: Auth
40	0.003326	30.905202	2025-05-21 19:12:00.035169	64.102.250.43	49	64.102.250.253	45757	TACACS+	84	R: Auth
46	0.000076	30.905950	2025-05-21 19:12:00.035917	64.102.250.253	42434	64.102.250.43	49	TACACS+	126	Q: Auth

```
> Frame 38: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Cisco_e6:f2:24 (a0:b4:39:e6:f2:24), Dst: VMware_ae:8f:a7 (00:50:56:ae:8f:a7)
> Internet Protocol Version 4, Src: 64.102.250.253, Dst: 64.102.250.43
> Transmission Control Protocol, Src Port: 45757, Dst Port: 49, Seq: 45, Ack: 28, Len: 26
v TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 3
  > Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 445621935
    Packet length: 14
    Encrypted Request
  v Decrypted Request
      Flags: 0x00
      User length: 9
      User: password12345
      Data length: 0
```

```
v Decrypted Request
    Flags: 0x00
    User length: 9
    User: password12345
    Data length: 0
```

TACACS+: Protocol

Packets: 66 · Displayed: 14 (21.2%)

Profile: Default

Protecting Credentials - Cisco Password Types

Type	Reversibility	Definition	Secure
0	n/a	Unencrypted	🚫
4	Non-reversible	Weak Hash - Removed in 2013	🚫
5	Non-reversible	MD5	🚫
6	Reversible	128 bit AES Encrypted	✓
7	Reversible	Vigenere Cipher (very weak)	🚫
8	Non-reversible	SHA256	✓
9	Non-reversible	SCRYPT	✓
10	Non-reversible	SHA512 (IOS XR Only)	✓

Protecting Credentials

REFERENCE

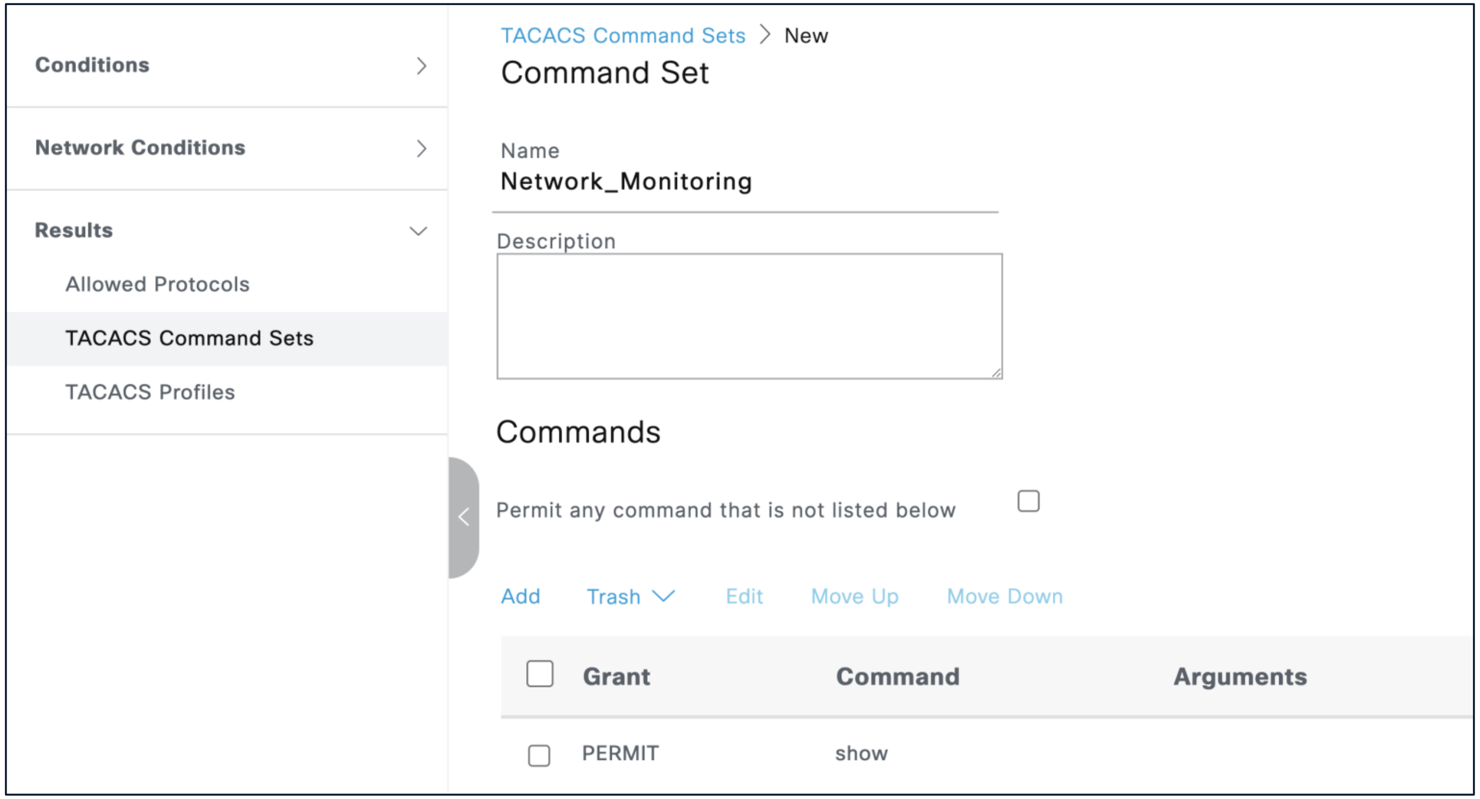
```
RP/0/RP0/CPU0:ios(config)#tacacs-server host 10.1.1.1
RP/0/RP0/CPU0:ios(config-tacacs-host)#key encrypt6 cisco
RP/0/RP0/CPU0:May 20 04:00:25.682 UTC: parser[287]:
%MGBL-SYS-3-TYPE6_AES_ENCR_NOT_CONFIGURED : Type6 aes encryption is not configured
RP/0/RP0/CPU0:May 20 04:00:25.682 UTC: parser[287]:
%MGBL-PARSER-3-ERR_GENERAL_ERR : Type 6 password/'password encryption aes' requires
:  a valid masterkey to be configured
RP/0/RP0/CPU0:ios(config)#password6 encryption aes

RP/0/RP0/CPU0:ios#key config-key password-encryption
New password Requirements: Min-length 6, Max-length 64
Enter new key :
Enter confirm key :

RP/0/RP0/CPU0:ios(config)#tacacs-server host 10.1.1.1
RP/0/RP0/CPU0:ios(config-tacacs-host)#key encrypt6 cisco

RP/0/RP0/CPU0:ios#sh run tacacs-server
tacacs-server host 10.1.1.1 port 49
 key 6 58454460654a46465253615c4a5146415e594d61484a6046664756
```

Type 6 Credential Considerations

- Config Key is used to encrypt credentials – should be unique per device
- Config Key is *only* needed to copy the configuration file from one device to another without re-entering credentials
- Securely store the key in a password vault *if* you want the ability to copy a configuration to another device without having to re-enter credentials

Using TACACS+ for Command Authorization

- Use TACACS+ Command Authorization (e.g. Command Sets) to enforce least privilege for users
- Consider using time-based policies
- Don't forget to restrict service / automation / machine accounts
- "Explicit Permit" vs. "Explicit Deny + permit remaining commands"



Command Set

Name
Network_Monitoring

Description

Commands

Permit any command that is not listed below □

□	Grant	Command	Arguments
□	PERMIT	show	

Command Authorization Policy Recommendations

REFERENCE

- Deny use of the 'clear log' & 'clear command history' commands
- Deny use of packet capture
- Baseline all M2M 'service account' command requirements – only allow necessary commands
- Deny instantiation of guest shell, bash shell & XR third-party applications
- Deny most users ability to alter AAA configuration commands
- Only allow specific aaa-server addresses to be configured
- Deny the creation of tunnels for all accounts that don't strictly need that capability
- Enforce logging at 'Informational' level. Lower levels logging configurations are denied
- Only allow specific external logging destinations – restrict ability to change the destination
- Limit who is allowed to create local users on devices
- Only allow the configuration of network standard tacacs-source interfaces
- Analyze all identity-groups to ensure least privilege policy is consistent with their device administration duties

Protecting AAA Protocols

- Legacy RADIUS and TACACS+ use MD5 for “encryption”
  - Many flaws making it unsuitable for modern encryption

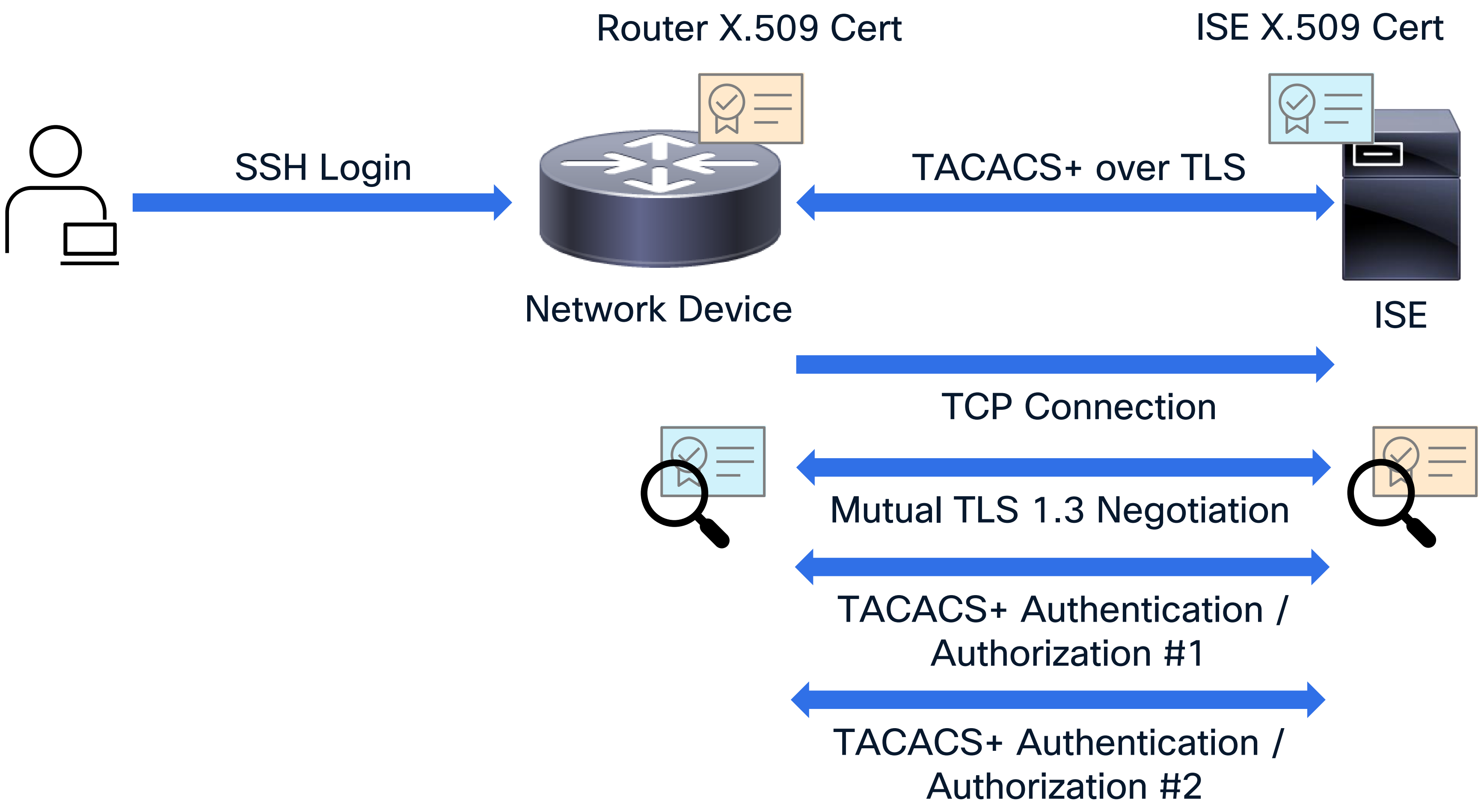
- Use RadSec with Certificates for RADIUS Traffic
- Use TACACS+ over TLS

TACACS+ over TLS1.3

- New RFC adds support for TLS1.3 to TACACS+ (currently in draft form – soon to be ratified - draft-ietf-opsawg-tacacs-tls13-21)

Platform	Release(s)
ISE	3.4 Patch 2 and 3.5
IOS XE	17.15.4 and 17.18.1
IOS XR	25.2.1 + SMU
NX OS	10.6.1
ACI	6.1.4
MDS	9.4(3b)

TACACS+ over TLS1.3



Router X.509 Cert

ISE X.509 Cert

SSH Login

TACACS+ over TLS

Network Device

ISE

TCP Connection

Mutual TLS 1.3 Negotiation

TACACS+ Authentication / Authorization #1

TACACS+ Authentication / Authorization #2

Do not edit
How to change the design

Do you have CA-signed (either private or public) certificates on your network devices?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Do not edit
How to change the design

How hard would it be to get CA-signed certificates on your devices?

ⓘ The Slido app must be installed on every computer you’re presenting from

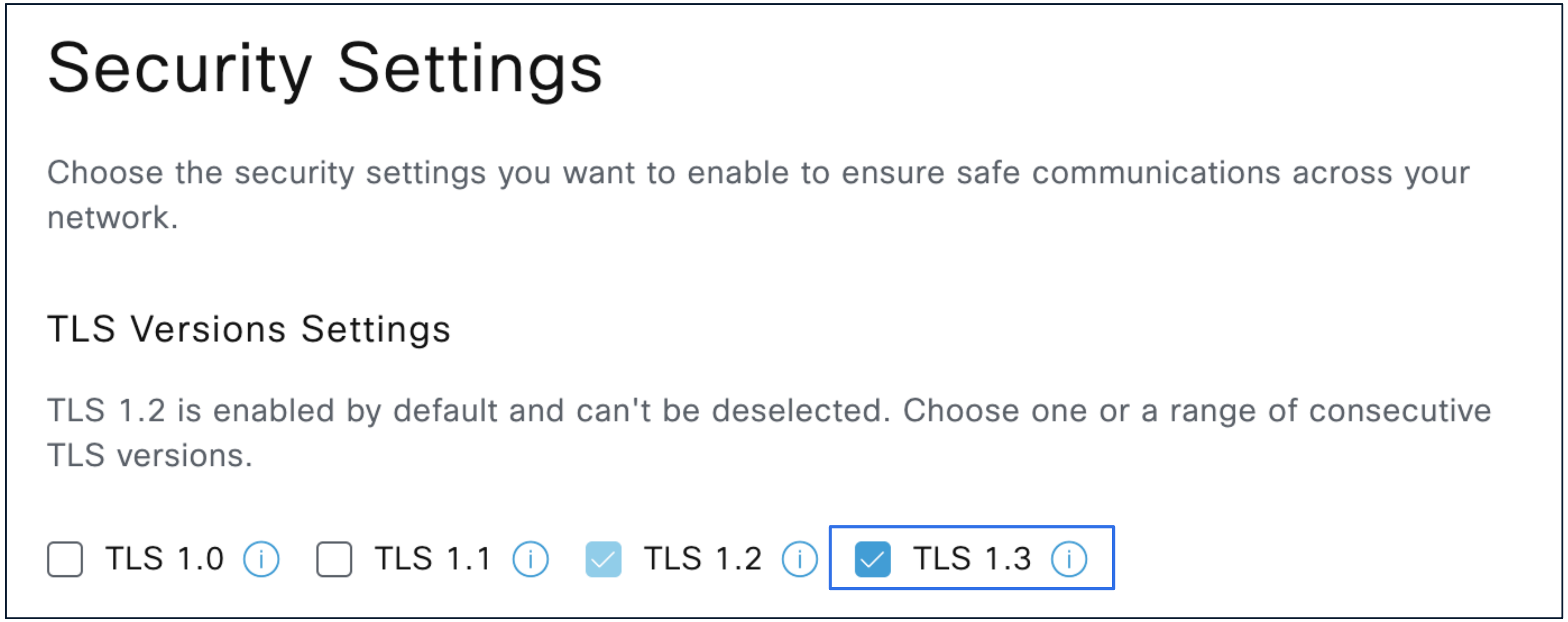
slido

TACACS+ over TLS1.3 – ISE Configuration

REFERENCE

Administration > Settings > Security Settings

- TACACS+ over TLS requires TLS 1.3 to be enabled



Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

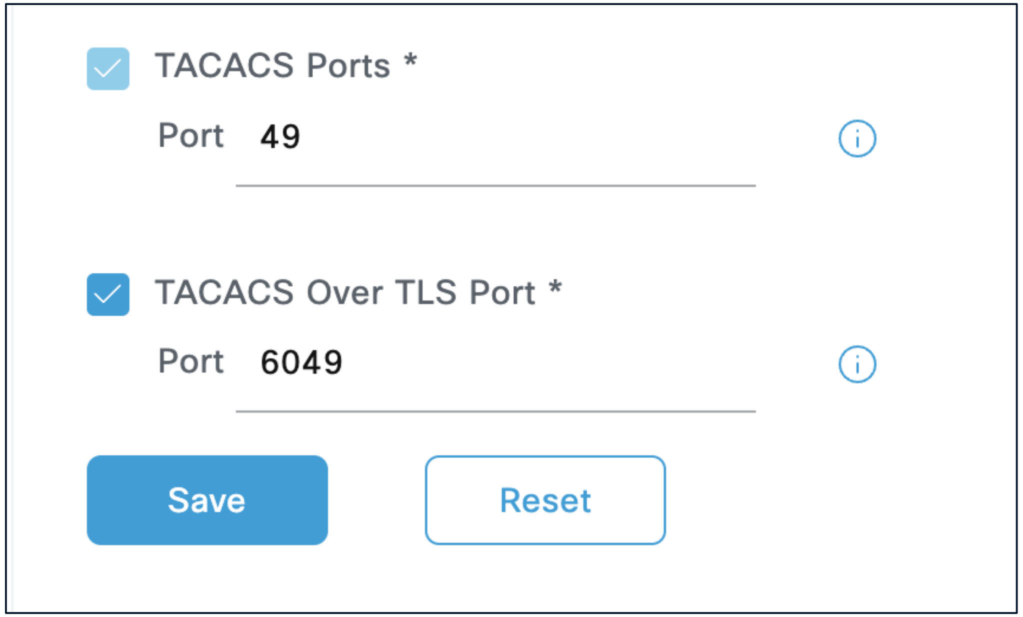
□ TLS 1.0 ⓘ □ TLS 1.1 ⓘ ☑ TLS 1.2 ⓘ ☑ TLS 1.3 ⓘ

TACACS+ over TLS1.3 – ISE Configuration

REFERENCE

Work Centers > Overview > Deployment

Configure TACACS+ over TLS port



☑ TACACS Ports *

Port 49

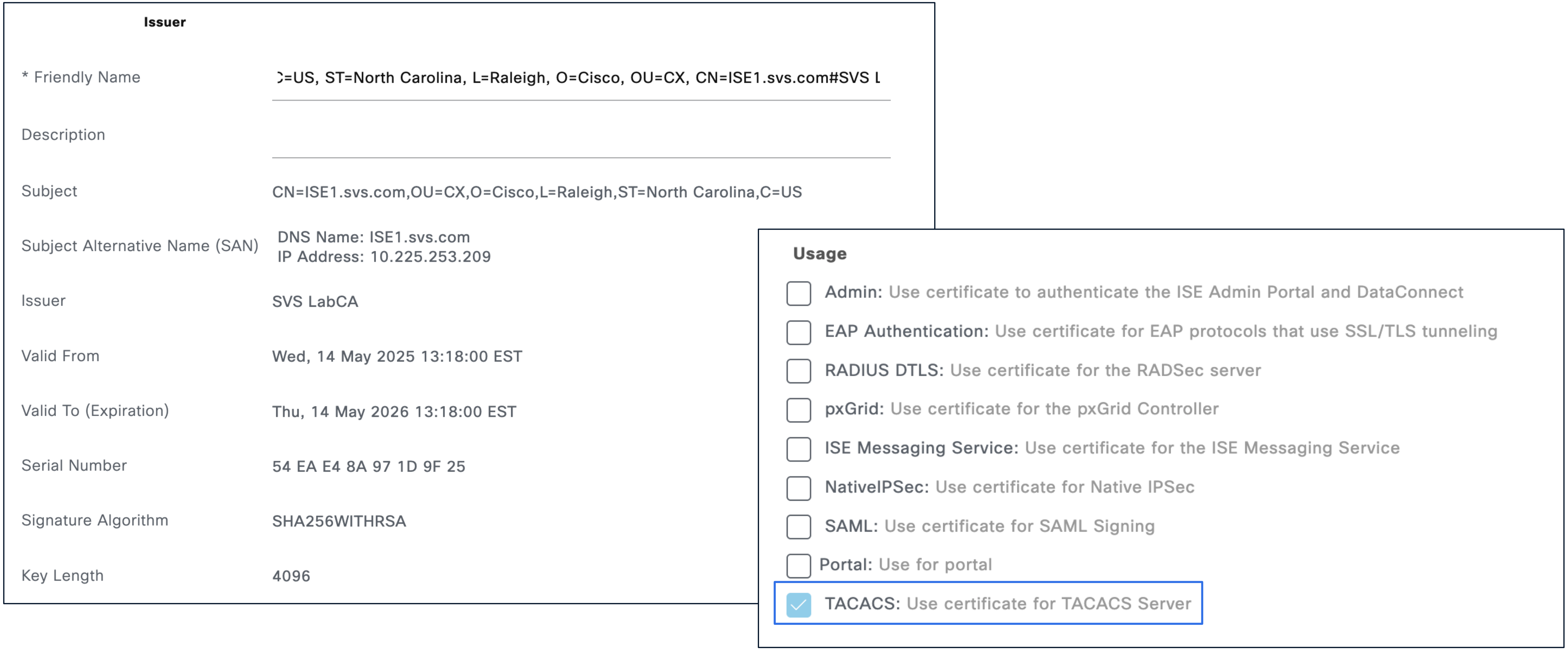
☑ TACACS Over TLS Port *

Port 6049

TACACS+ over TLS1.3 – ISE Configuration

REFERENCE

Administration > Certificates > System Certificates



Issuer

* Friendly Name	C=US, ST=North Carolina, L=Raleigh, O=Cisco, OU=CX, CN=ISE1.svs.com#SVS L
Description	
Subject	CN=ISE1.svs.com,OU=CX,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Subject Alternative Name (SAN)	DNS Name: ISE1.svs.com IP Address: 10.225.253.209
Issuer	SVS LabCA
Valid From	Wed, 14 May 2025 13:18:00 EST
Valid To (Expiration)	Thu, 14 May 2026 13:18:00 EST
Serial Number	54 EA E4 8A 97 1D 9F 25
Signature Algorithm	SHA256WITHRSA
Key Length	4096

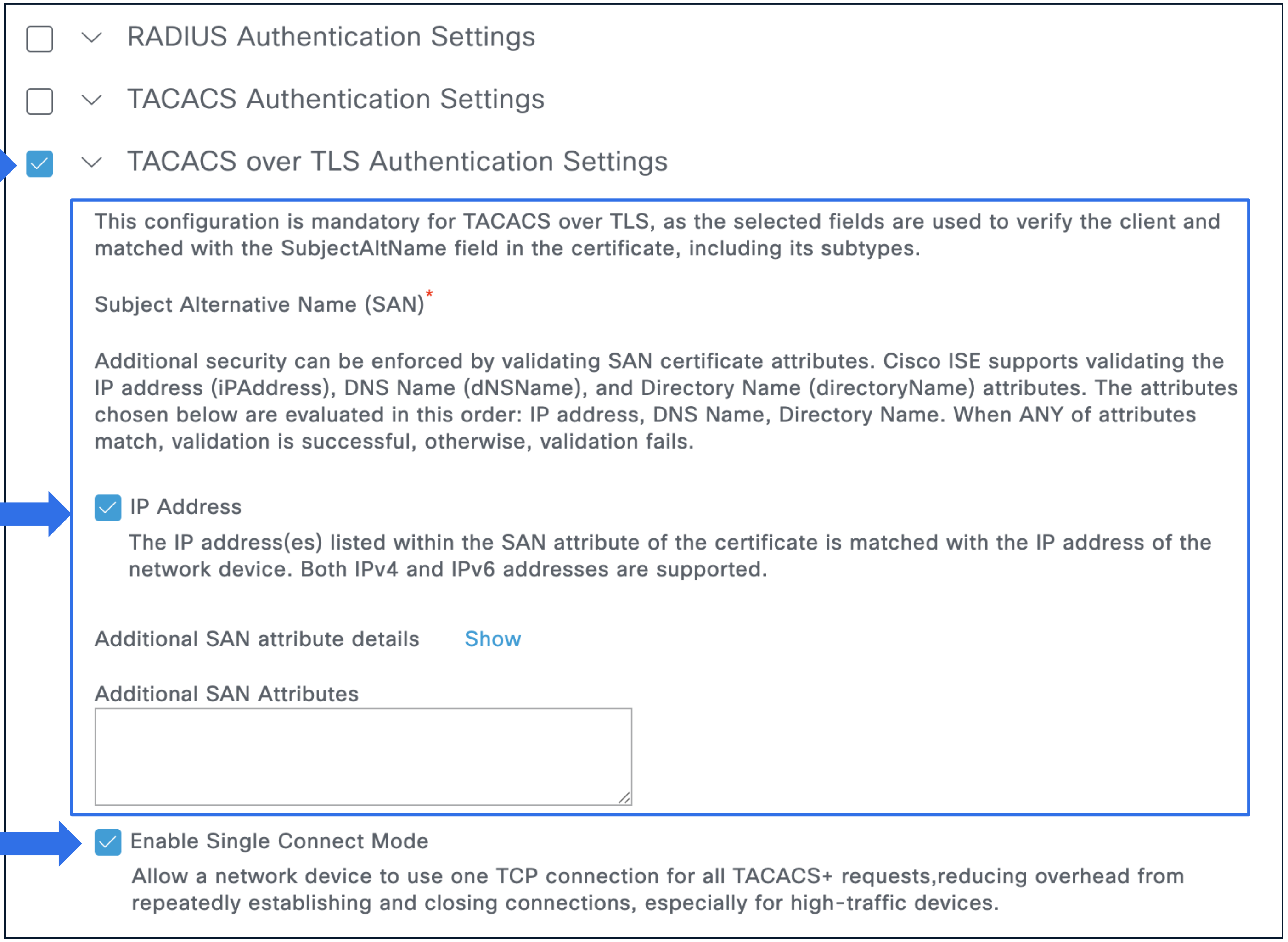
Usage

- □ **Admin:** Use certificate to authenticate the ISE Admin Portal and DataConnect
- □ **EAP Authentication:** Use certificate for EAP protocols that use SSL/TLS tunneling
- □ **RADIUS DTLS:** Use certificate for the RADSec server
- □ **pxGrid:** Use certificate for the pxGrid Controller
- □ **ISE Messaging Service:** Use certificate for the ISE Messaging Service
- □ **NativeIPSec:** Use certificate for Native IPSec
- □ **SAML:** Use certificate for SAML Signing
- □ **Portal:** Use for portal
- ☑ **TACACS:** Use certificate for TACACS Server

TACACS+ over TLS1.3 – ISE Configuration

REFERENCE

Administration > Network Devices



Enable TACACS+ over TLS

Configure SAN Attributes to validate device certificate

Configure Single Connect Mode

□ RADIUS Authentication Settings

□ TACACS Authentication Settings

☑ TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN)*

Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (iPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☑ IP Address

The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details Show

Additional SAN Attributes

☑ Enable Single Connect Mode

Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

TACACS+ over TLS1.3 - IOS XR

REFERENCE

```
crypto ca trustpoint svs-new
 crl optional
 subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.com
 subject-alternative-name IP:10.225.253.167
 enrollment url terminal

aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 2
  tls
   trustpoint svs-new
  !
  single-connection
  single-connection-idle-timeout 5
 !
```

TACACS+ over TLS1.3 - IOS XR

REFERENCE

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Fri May 23 19:25:00.713 UTC

Trustpoint       : svs-new
==================================================
CA certificate
  Serial Number  : 20:CD:74:02:C4:DA:37:F5
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
```

TACACS+ over TLS1.3 - IOS XR

REFERENCE

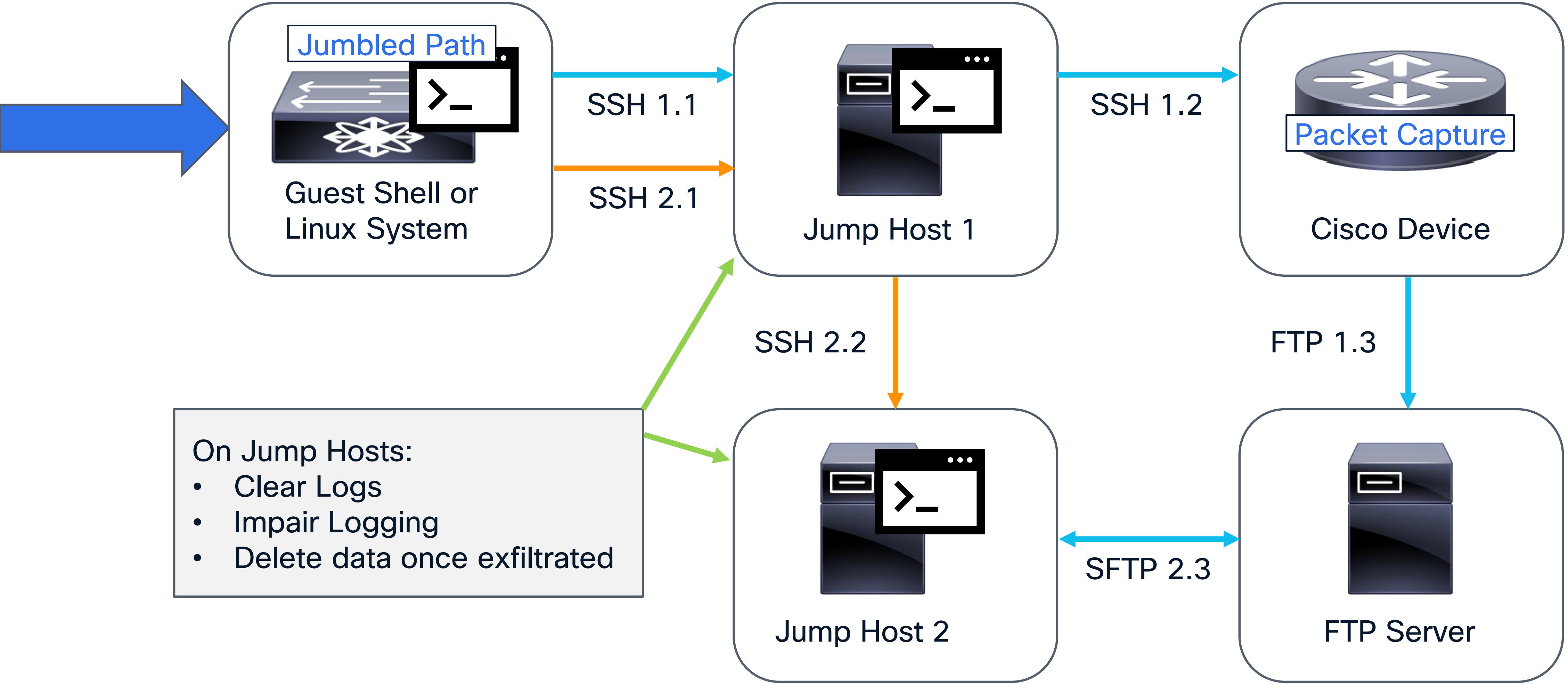
```
Router certificate
  Key usage          : General Purpose
  Status             : Available
  Serial Number      : 09:4C:69:B0:66:93:74:EF
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.com,OU=SVS,O=Cisco,L=RTP,…
  Issued By          :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs-new
```

TACACS+ over TLS1.3 - IOS XE

REFERENCE

```
crypto pki trustpoint svs_cat9k
 enrollment terminal pem
 subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.com
 subject-alt-name cat9k.svs.com
 revocation-check none
 eckeypair svs-256ec-key
 hash sha512

tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 180
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip vrf forwarding Mgmt-vrf
 tls ip tacacs source-interface GigabitEthernet0/0
```

Preventing APT Activities



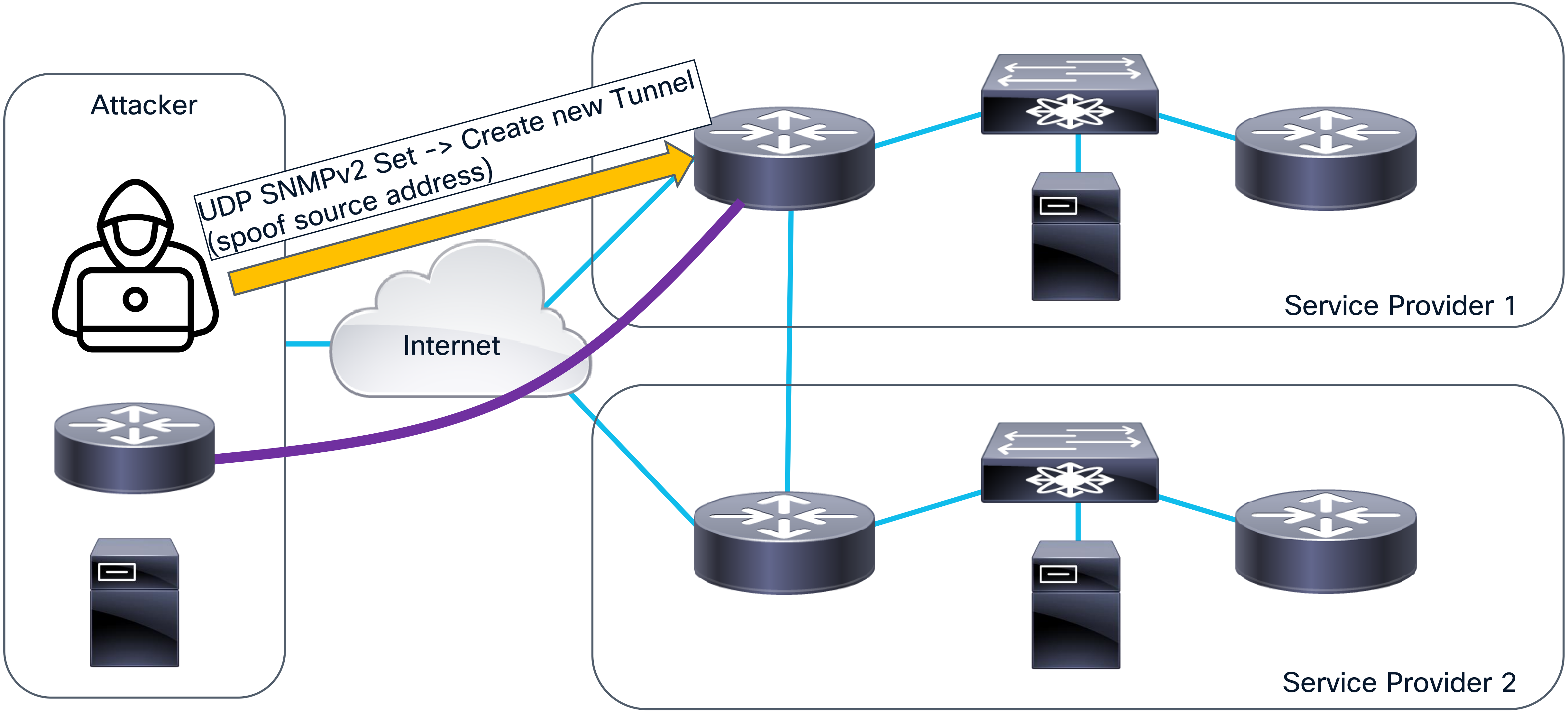
On Jump Hosts:

- Clear Logs
- Impair Logging
- Delete data once exfiltrated

Stopping Lateral Movement

- Create segmented network for management traffic
- Maintain tight management access lists / audit existing filters
- Create Infrastructure access lists (iACLs) on the edge
- Restrict use of Guest Shell / bash shells / XR 3rd Party Applications
- Pay attention to connections to trusted parties

Attack Example Topology



Attack Example Topology

Attacker
UDP
(sp
...t -> Create new Tunnel
Provider 1
Service Provider 2

Stop using SNMPv2!
(Especially with RW Privileges)

Logging and Monitoring

- Monitor for suspicious activities
  - Unexpected configuration changes (especially anything related to AAA or logging)
  - Clearing of log files on devices (clear log)
  - Monitor AAA accounting logs – are high risk commands being used (e.g. packet capture, guest shell)
  - Monitor for unusual network traffic originating / terminating on network devices (e.g. traffic on unexpected port numbers)

- Coming Soon: auditd support to monitor guest shells and bash shell activity

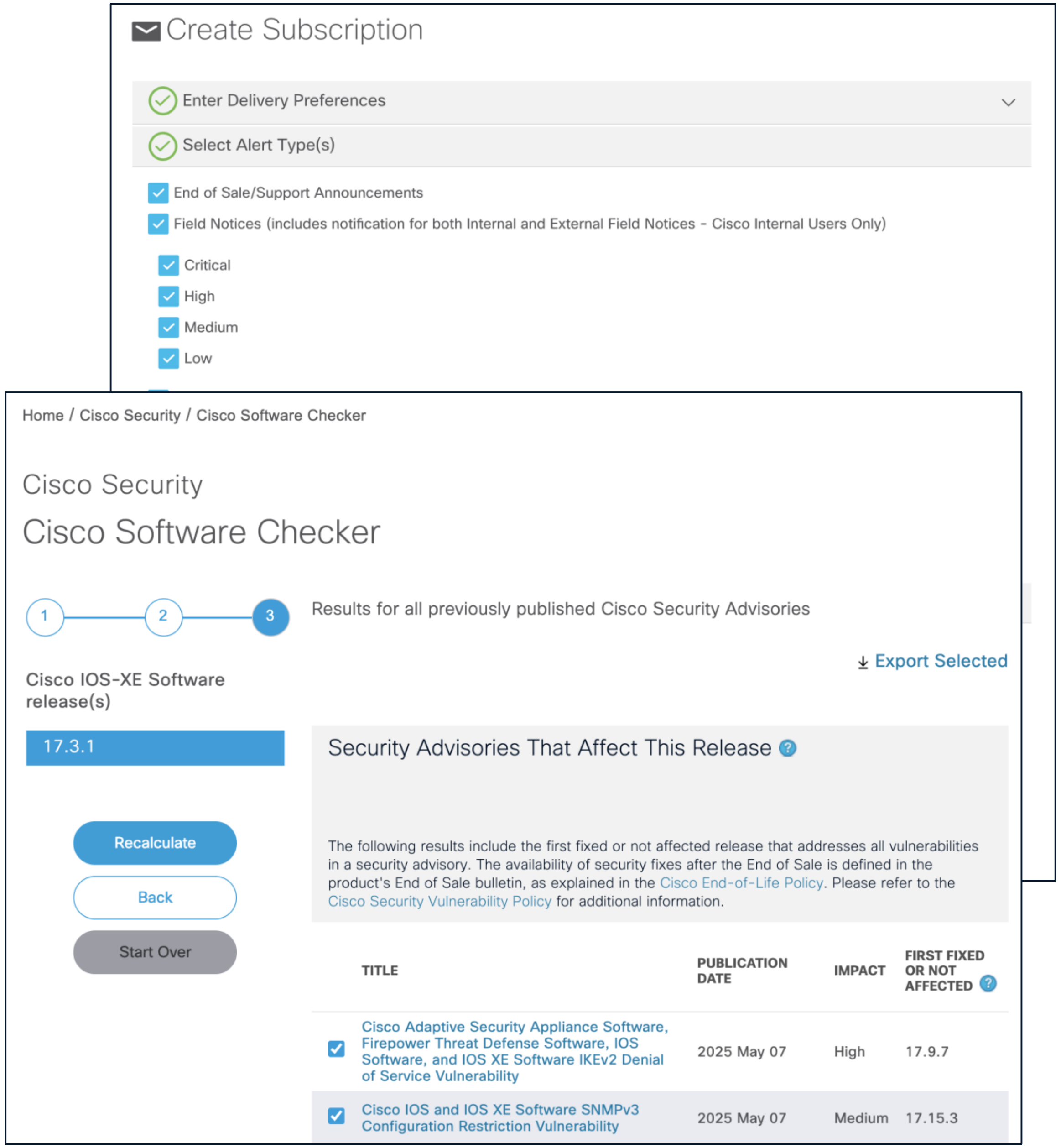
Keeping Software Updated

https://cway.cisco.com/mynotifications

- Subscribe to Security Advisory, Field Notice, and End of Life Notifications

https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

- Check for advisories for a given platform and version
- Can upload a ‘show ver’



Create Subscription

Enter Delivery Preferences

Select Alert Type(s)

☑ End of Sale/Support Announcements

☑ Field Notices (includes notification for both Internal and External Field Notices - Cisco Internal Users Only)

☑ Critical
☑ High
☑ Medium
☑ Low

Home / Cisco Security / Cisco Software Checker

Cisco Security

Cisco Software Checker

Results for all previously published Cisco Security Advisories

Export Selected

Cisco IOS-XE Software release(s)

17.3.1

Security Advisories That Affect This Release

The following results include the first fixed or not affected release that addresses all vulnerabilities in a security advisory. The availability of security fixes after the End of Sale is defined in the product's End of Sale bulletin, as explained in the Cisco End-of-Life Policy. Please refer to the Cisco Security Vulnerability Policy for additional information.

	TITLE	PUBLICATION DATE	IMPACT	FIRST FIXED OR NOT AFFECTED
☑	Cisco Adaptive Security Appliance Software, Firepower Threat Defense Software, IOS Software, and IOS XE Software IKEv2 Denial of Service Vulnerability	2025 May 07	High	17.9.7
☑	Cisco IOS and IOS XE Software SNMPv3 Configuration Restriction Vulnerability	2025 May 07	Medium	17.15.3

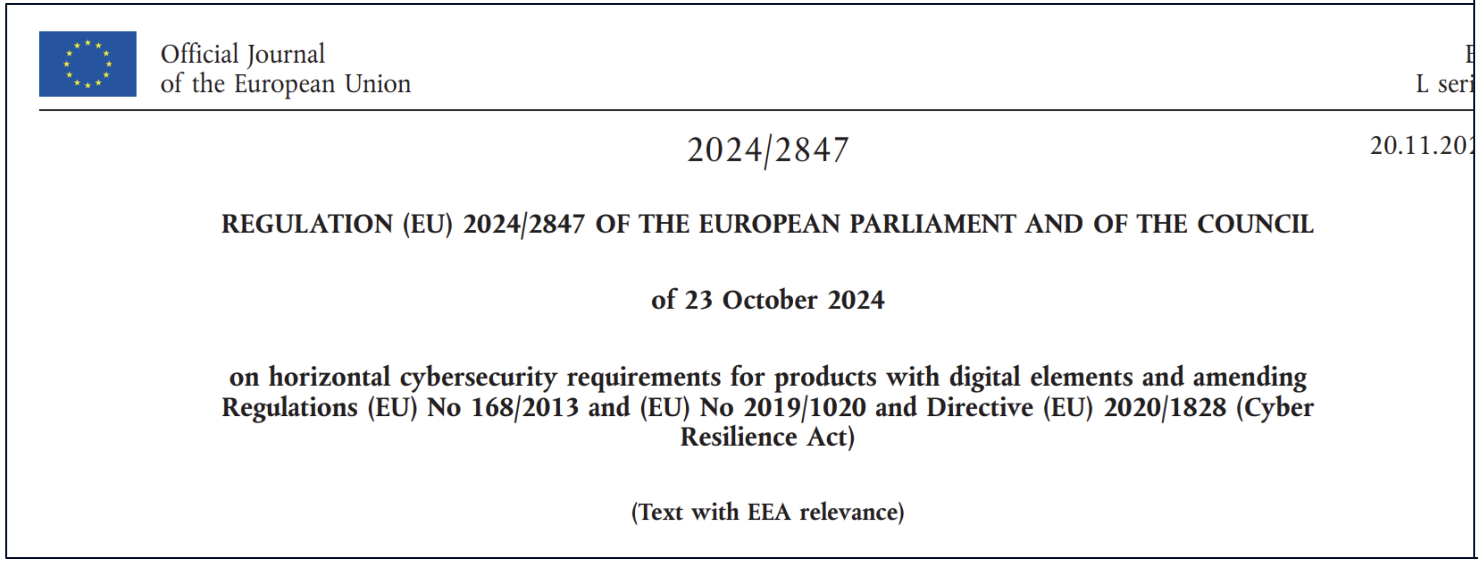
Looking to the Future

What is in store for the future?

Hardening Guides → Secure by Default

Moving to more Secure by Default / Secure by Design

- Why change? Why now?
  - Threat Actor Sophistication is increasing
  - Increasing government regulations
  - Lower customer friction for secure configuration



Official Journal
of the European Union

E
L seri

2024/2847

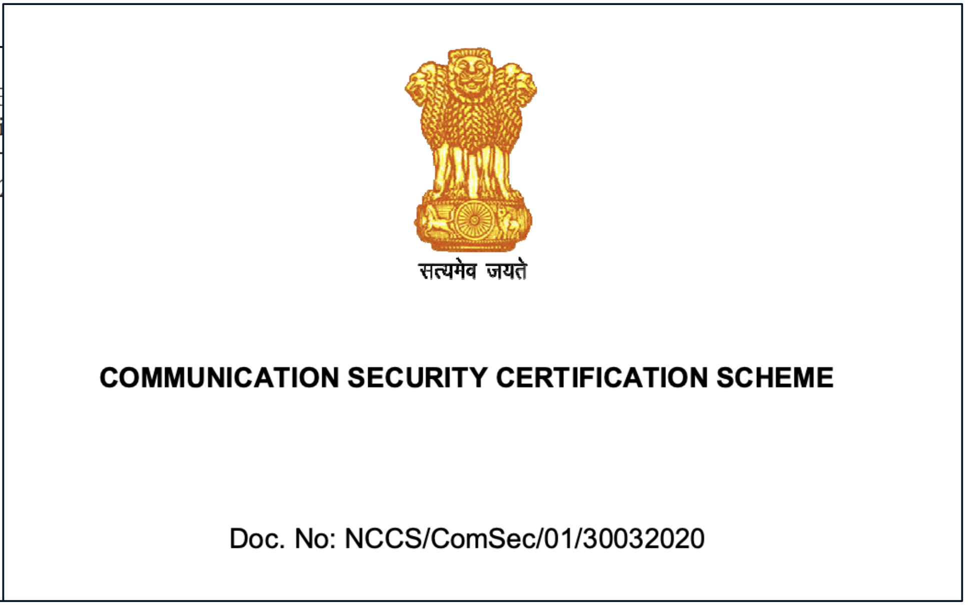
20.11.202

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)



सत्यमेव जयते

COMMUNICATION SECURITY CERTIFICATION SCHEME

Doc. No: NCCS/ComSec/01/30032020

Do not edit
How to change the design

How do you authenticate administrators on network devices?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

Do not edit

How to change the design

Which versions of SNMP do you use in your network?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

Do not edit
How to change the design

Which of these protocols do you use?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

Do not edit
How to change the design

How often do you upgrade to a new software release?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Do you use Type 6 (AES) to store credentials on your devices?

Moving to more Secure by Default / Secure by Design

- Deprecation and Removal of Insecure Protocols
  - Telnet
  - TFTP
  - FTP
  - HTTP
  - SSHv1
  - SNMPv1
  - SNMPv2c
  - SNMPv3 without auth / encryption
  - TLS1.0 / TLS1.1

Moving to more Secure by Default / Secure by Design

- All credentials and keys can only be stored with strong encryption (type 6) or strong hashes (type 8/9/10) automatically
- Management Interfaces must be explicitly configured
- Warnings if secure best practices are not followed
- Changes to defaults to secure choices

New Capabilities on the Horizon

- TACACS+ over TLS
- auditd support for monitoring shell environments
- FIDO2 support over SSH
- Scalability of SSH public keys (useful for machine accounts)
- tetragon support on network operating systems

The products and features described in this document are shared for informational purposes only and are subject to change at Cisco’s sole discretion; are in varying stages of development, to be offered on a when-and-if-available basis; and are not contractual commitments. Customers should not rely on the availability of any future product or feature in executing any agreements or placing any orders related to specified projects.

Do not edit
How to change the design

What changes are you planning on implementing?

ARE YOU PREPARED?

- Follow Hardening Guides
- Use MFA for SSH / Management
- Restrict Management Planes
- Encrypt Device Credentials
- Secure Authentication Protocols
- Use Command Authorization
- Disable Insecure Features

Cisco Customer Experience is here to help

Lifecycle Services

Solution Consulting

Coming Soon:
Cisco Support Assistant
AI-enabled Hardening Audit and Report

https://www.cisco.com/site/us/en/services/index.html

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at: pgiralt@cisco.com, snowell@cisco.com

Thank you

CISCO Live!