
cisco Live!
GO BEYOND
#CiscoLiveAPJC

From Fish to Shark: 8 Stepping Stones in Cisco Secure Access (Secure Service Edge) Journey

Bhavik Shah: Solutions Engineer, Cybersecurity
Sandeep Yadav: Solutions Engineer, Cybersecurity

BRKSEC-2482

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2482

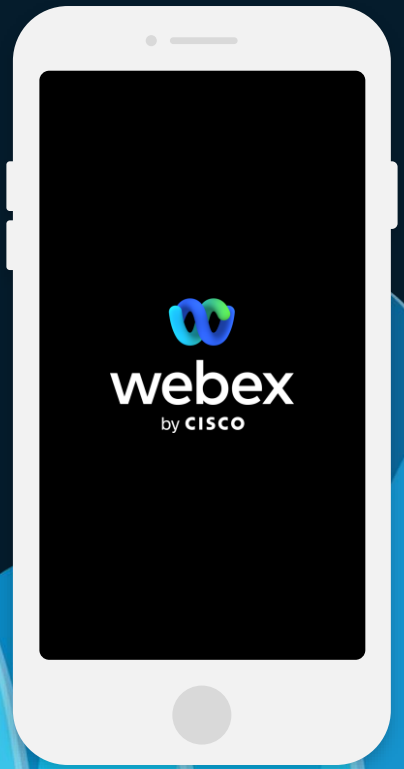
Questions?

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 November 15, 2024.



cisco Live!

Abstract

With the rapid cloud adoption and hybrid work for users, security is no longer confined to the enterprise network perimeter. Thus, it becomes of paramount importance to provide an integrated Security Service Edge (SSE) architecture which unifies security of web, private and SaaS applications from evolving threats. This unified architecture helps in providing seamless control and security in accessing applications remotely to different personas like employees, trusted partners and contractors. How do you maximize benefit and minimize risk when adopting Cisco Secure Access? This session gives phased approach to achieve success while implementing Cisco Secure Access.

- **Deployment Plan**: The deployment plan includes phases for private apps connectivity, remote access, on-network users, and advanced features
- **Deployment Methods**: Deployment methods include Secure Private Access, ZTA Client-Based, RA VPN, ZTNA Clientless, and Branch IPsec Tunnel
- **Advanced Features**: Advanced features include Duo Passport, CII, reporting and analysis, DEM integration, decryption, and IPS enforcement
- **Automating the migration** from Umbrella Roaming agent to Secure client with a PowerShell script
- **Deployment Plan:** The deployment plan includes phases for Internet connectivity, remote access, on-network users, and advanced features
- **Deployment Methods:** Deployment methods include Secure Internet Access, Certificate, PAC URL for Servers and Branch IPsec Tunnel - with Cisco and 3rd Party.
- **Advanced Features**: Advanced features include Duo Passport, CII, reporting and analysis, DEM integration, Selective decryption, DLP, RBI and SIEM Integration
- Explore **policy creation with AI/ML**

Bhavik Shah

Solutions Engineer, Cybersecurity

Cisco Systems, Inc.

- Fun fact:
  - Loves running and fitness freak
  - Marathon runner with 2 10K finish and 1 21K Finish
  - Learning new stuff and exploring unknown territories.
- Work:
  - 15+ years of experience in Cybersecurity
  - Problem Solver, Innovator, Good Listener
  - CCIE Security #59125
  - GIAC Cloud Penetration Tester (GCPN)
- Family:
  - 1 daughter, 3 years old.

Sandeep Yadav

Solutions Engineer, Cybersecurity

Cisco Systems, Inc.

- CCIE Security#42053
- 10 Years + in the Cybersecurity Industry
- Cisco System Certified Instructor (CCSI#35384)
- CCIE Security -2014 | CCSI#35348 | GIAC – GCIH, GDSA | PCNSE
- Co-Author for Security Experience Center (SEC)

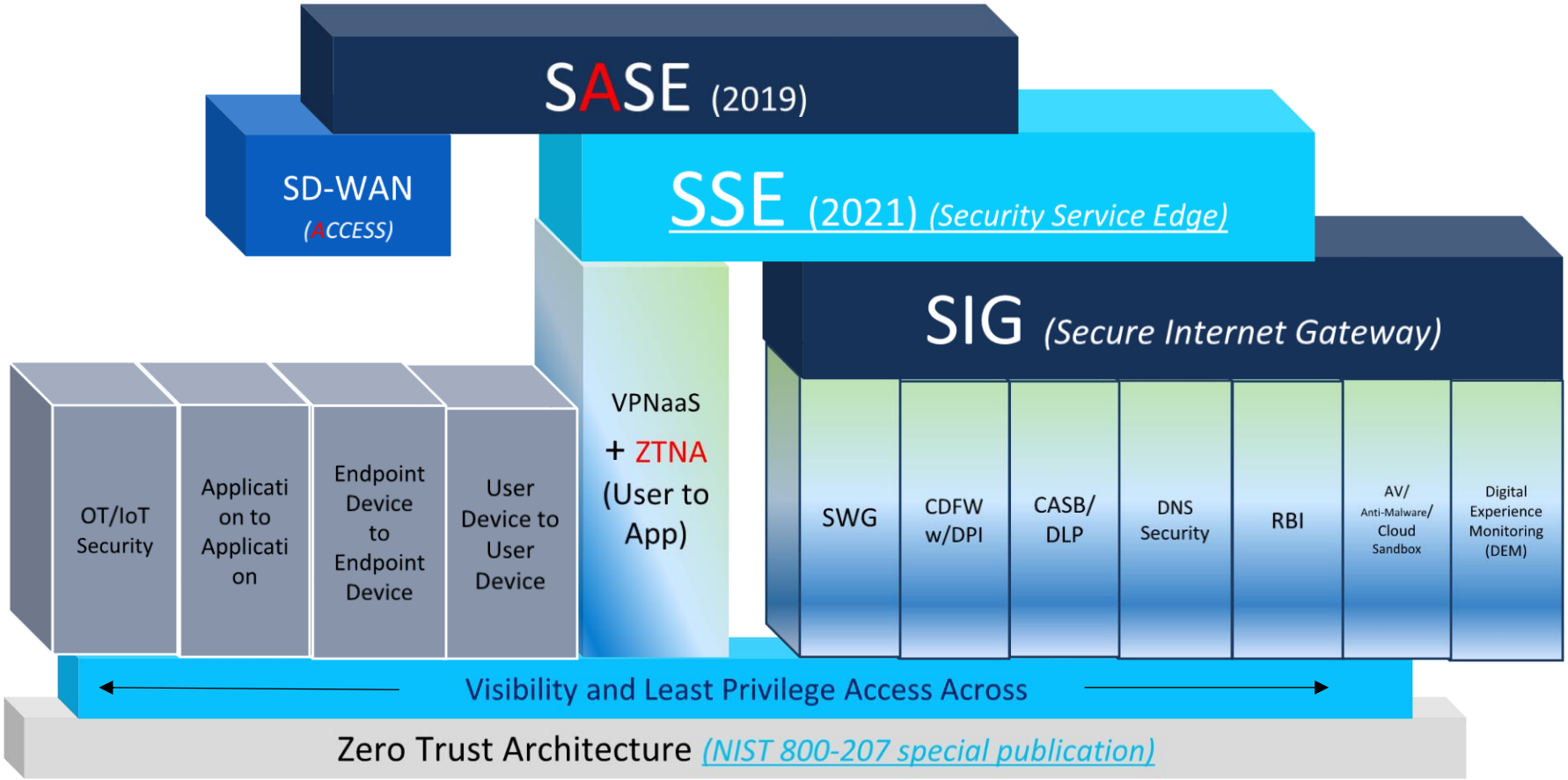
- Family – Father (6 yrs and 4 Months old daughters)

- Now: Busy building Security Experience Center For ASEAN Countries

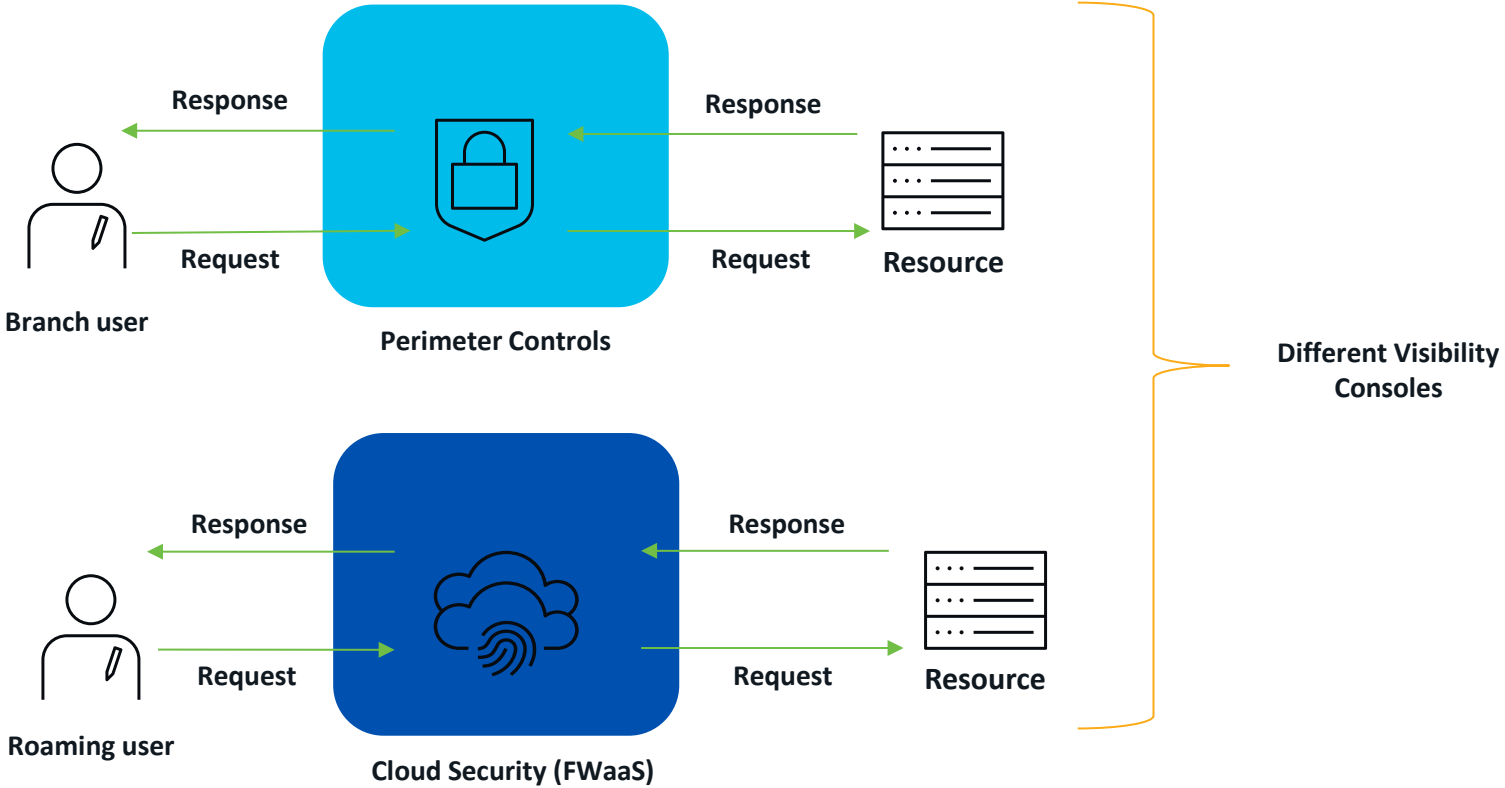
Agenda

- Introduction – Progressive Buzz
- Audience Poll
- Deployment Plans For Secure Internet Access
- Deployment Plans For Secure Private Access
- Advanced Feature
- Conclusion

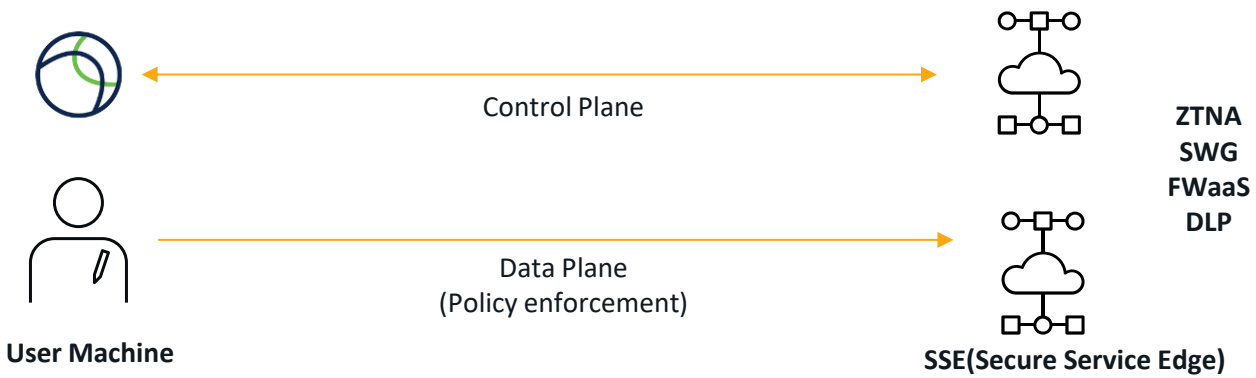
Understanding the History



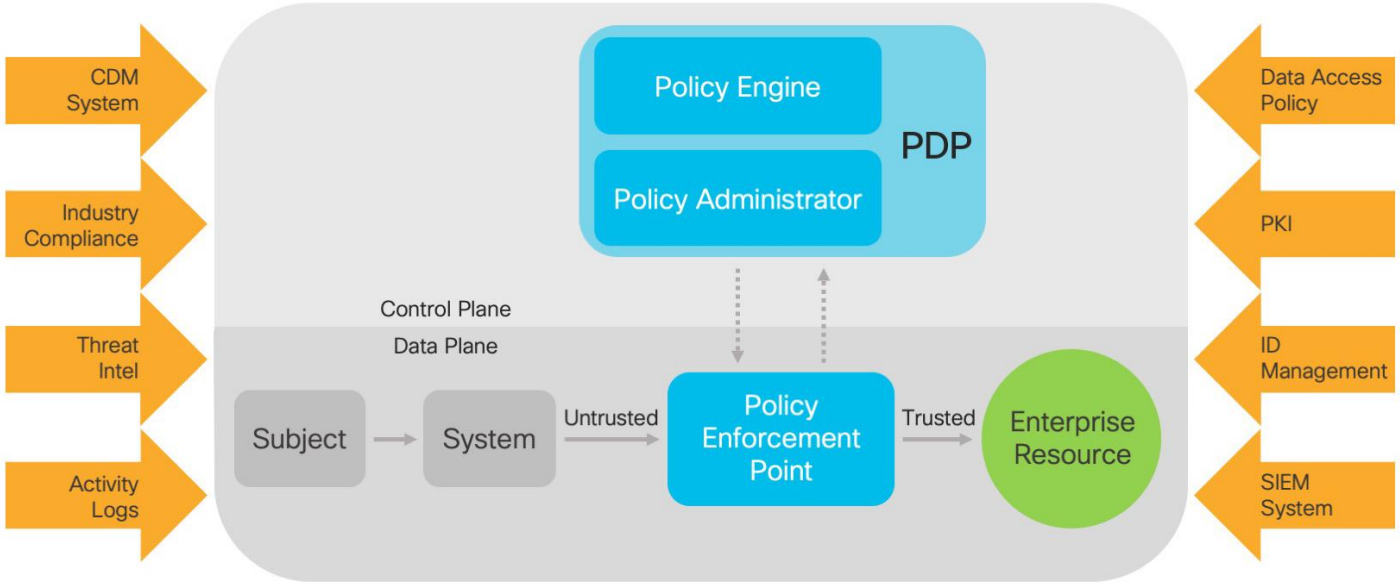
Why Security Service Edge?



Uncovering SSE



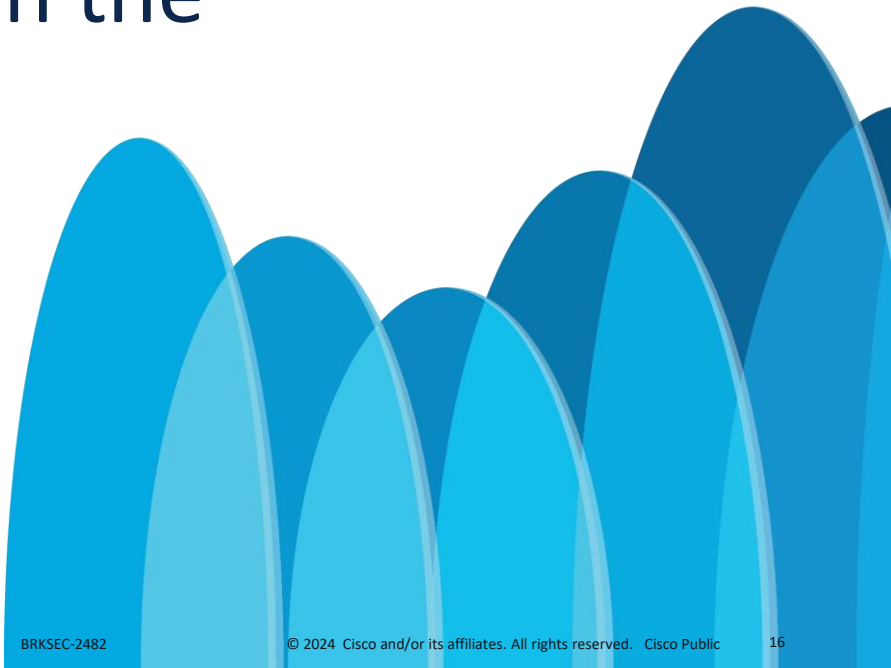
NIST 800-207: Zero Trust Architecture



Source: https://csrc.nist.gov/publications/detail/sp/800-207/final

Here is where you are on the Zero Trust Journey

Map the Phases according to your environment



Gartner: Secure Access Service Edge (SASE)

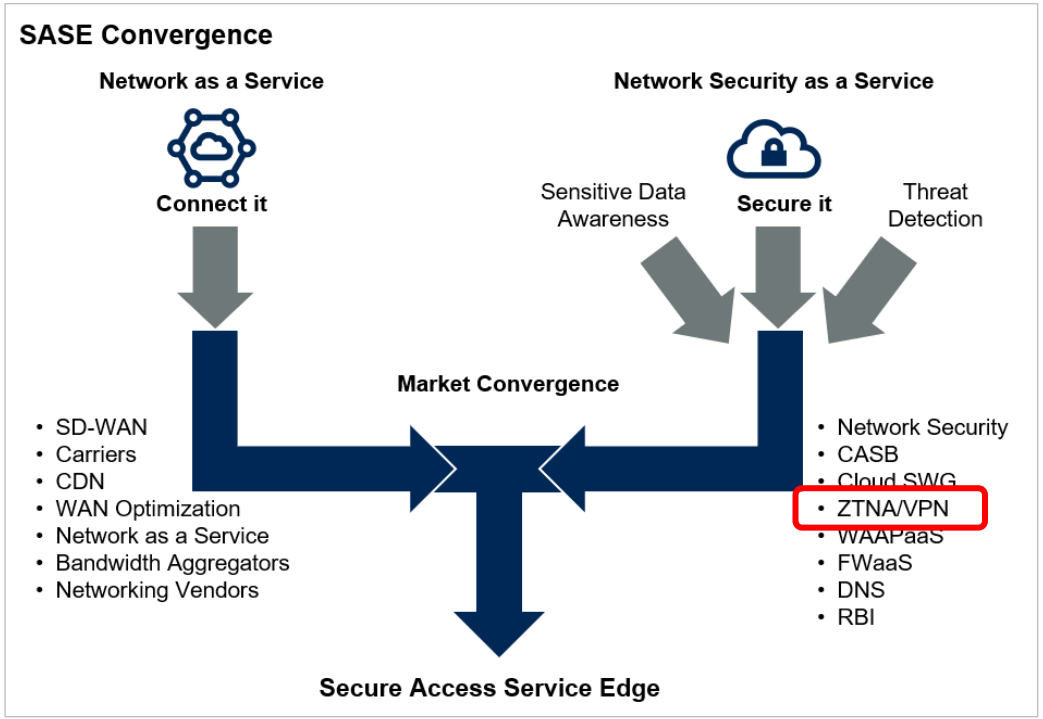
Convergence of networking and security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

Benefit rating:
Transformational

Market penetration:
Less than 1% of target audience

Maturity:
Emerging

Gartner, The Future of Network Security Is in the Cloud, Neil MacDonald, Aug 30, 2019



Gartner. Licensed for Distribution

Market Guide for Zero Trust Network Access

Published 8 June 2020 - ID G00726817 - 27 min read

By Analysts Steve Riley, Lawrence Orans, Neil MacDonald

ZTNA augments traditional VPN technologies for application access, and removes the excessive trust once required to allow employees and partners to connect and collaborate. Security and risk management leaders should pilot ZTNA projects as part of a SASE strategy or to rapidly expand remote access.

Figure 1: Conceptual Model of Endpoint-Initiated ZTNA

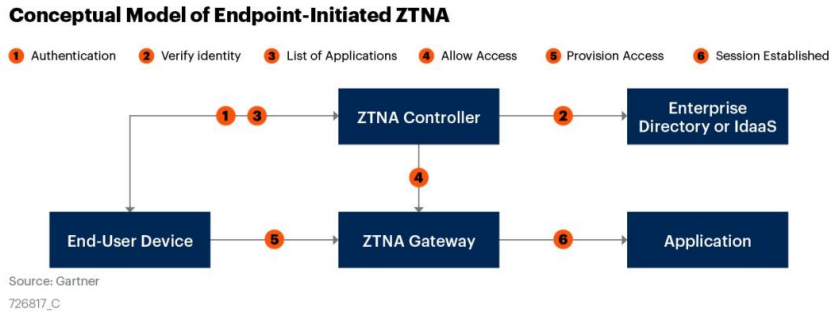
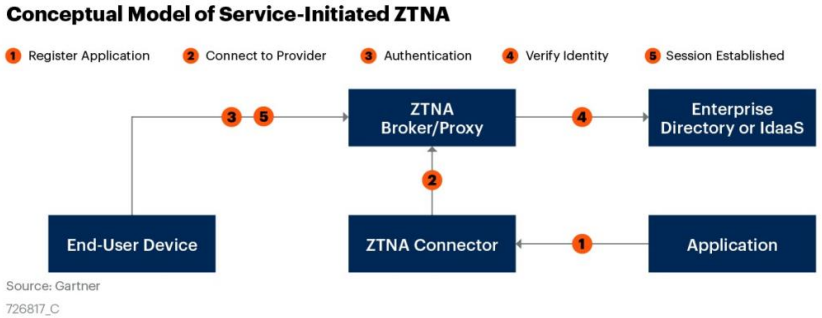


Figure 2: Conceptual Model of Service-Initiated ZTNA

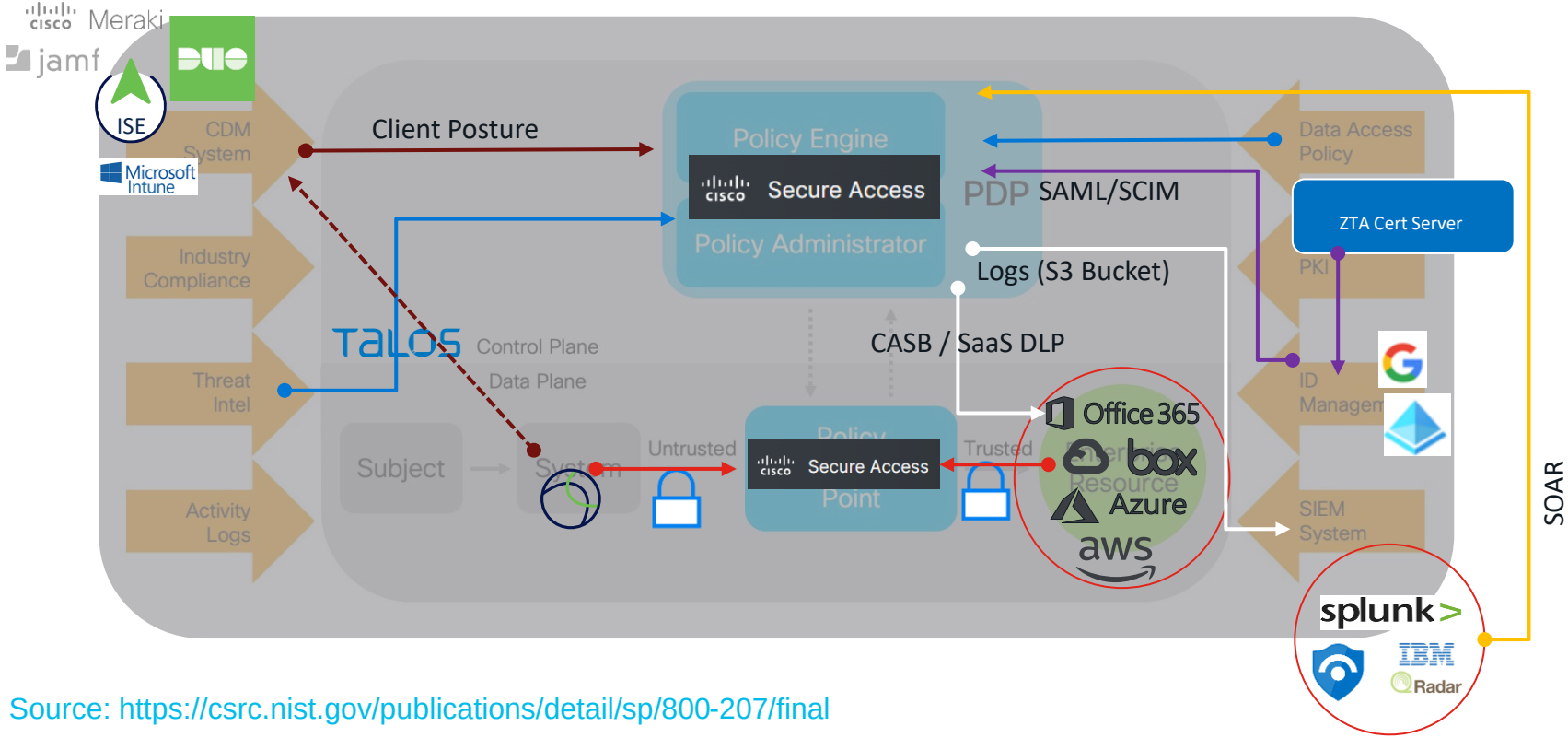


ZTNA Alternatives

Several alternative approaches to ZTNA for making applications are available to communities of internal and external users:

- Legacy VPNs remain popular, but they might not provide sufficient risk management for exposed services and can be more difficult to manage, given the dynamic nature of digital business. Legacy VPNs may also create scale and bandwidth issues for mostly mobile workforces. Always-on VPNs that require device and user authentication provide similar outcomes as ZTNA; however, basic network-access VPNs do not. Factor security requirements into VPN models and user satisfaction expectations. For third-party privileged access into enterprise systems, a PAM tool can be a useful alternative to a VPN.
- Exposing web applications through a reverse-proxy-based web application firewall (WAF) is another option. With WAF as a service (i.e., cloud WAF), traffic passes through the provider's WAF service for inspection before delivery to its destination. To avoid false positives or potential application malfunctions, cloud WAFs, like any other WAF, typically require some time

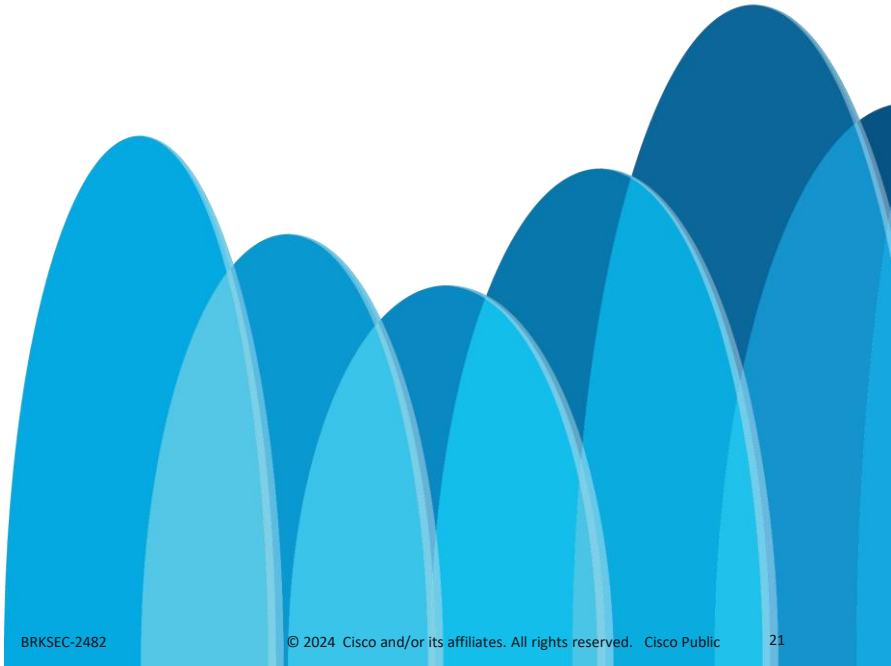
NIST 800-207: Zero Trust Architecture



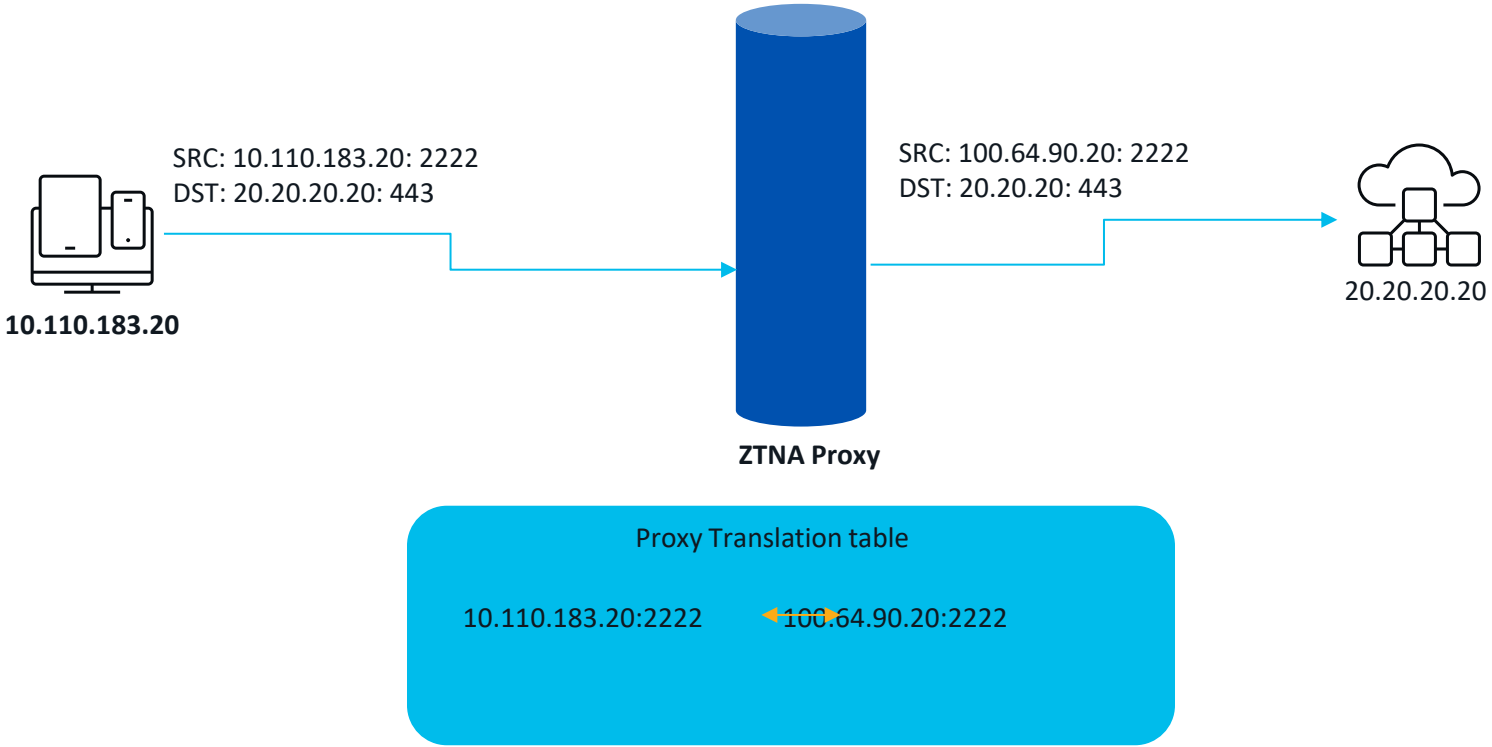
Source: https://csrc.nist.gov/publications/detail/sp/800-207/final

We have a Remote Access VPN Solution and wish to replace it with modern access method such as SDP or ZTNA?

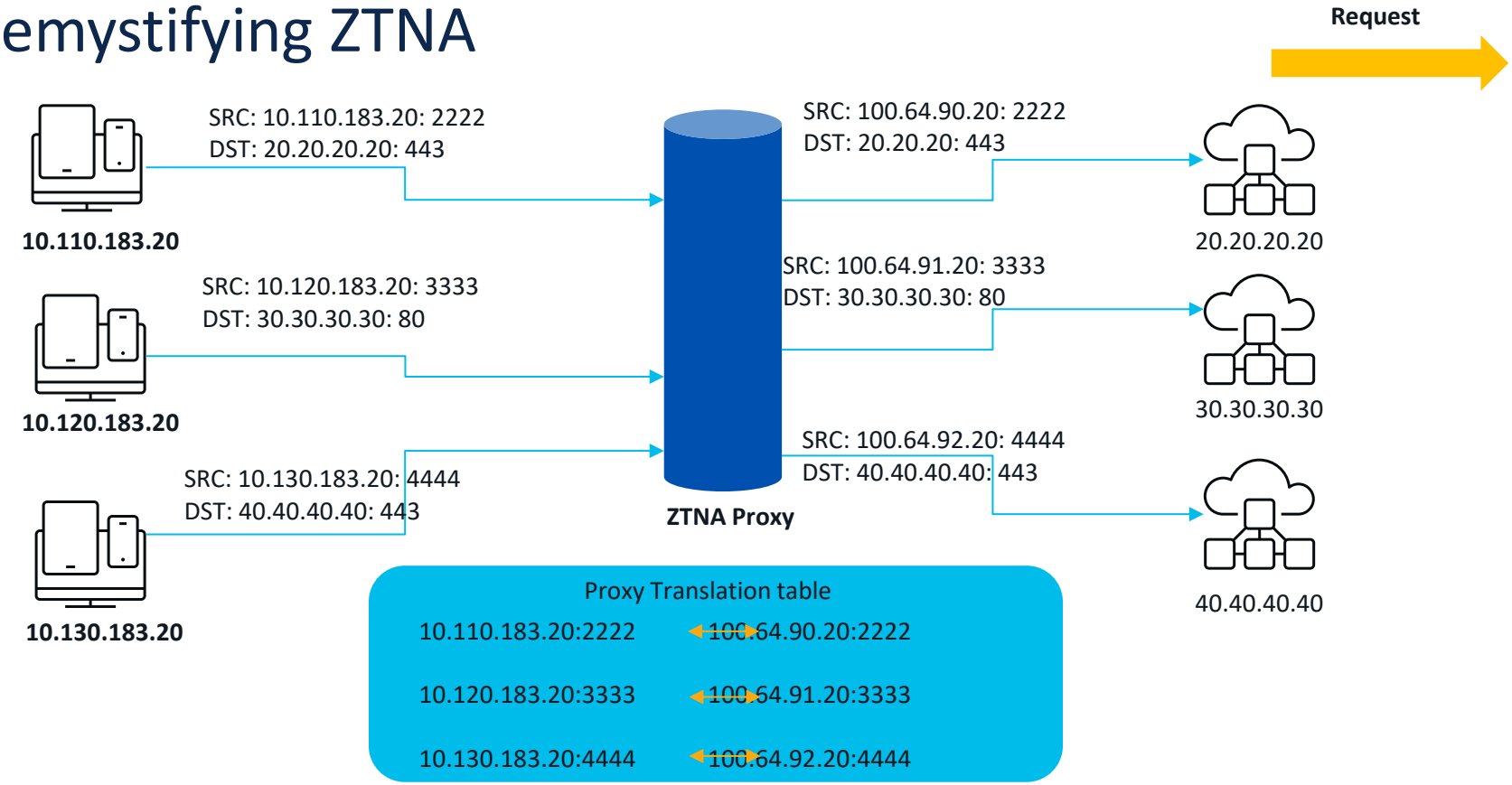
Here is what you need to know.



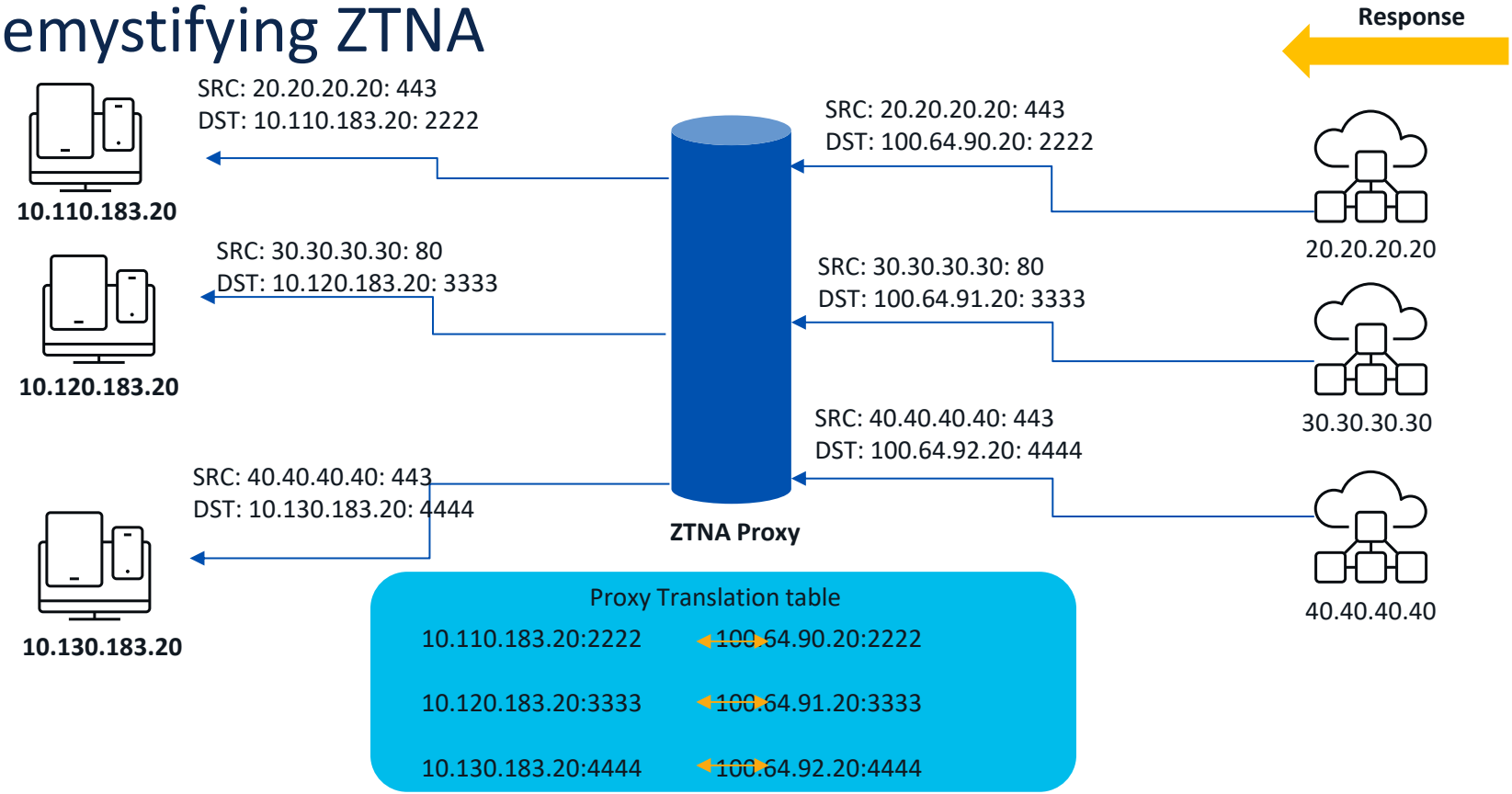
Demystifying ZTNA



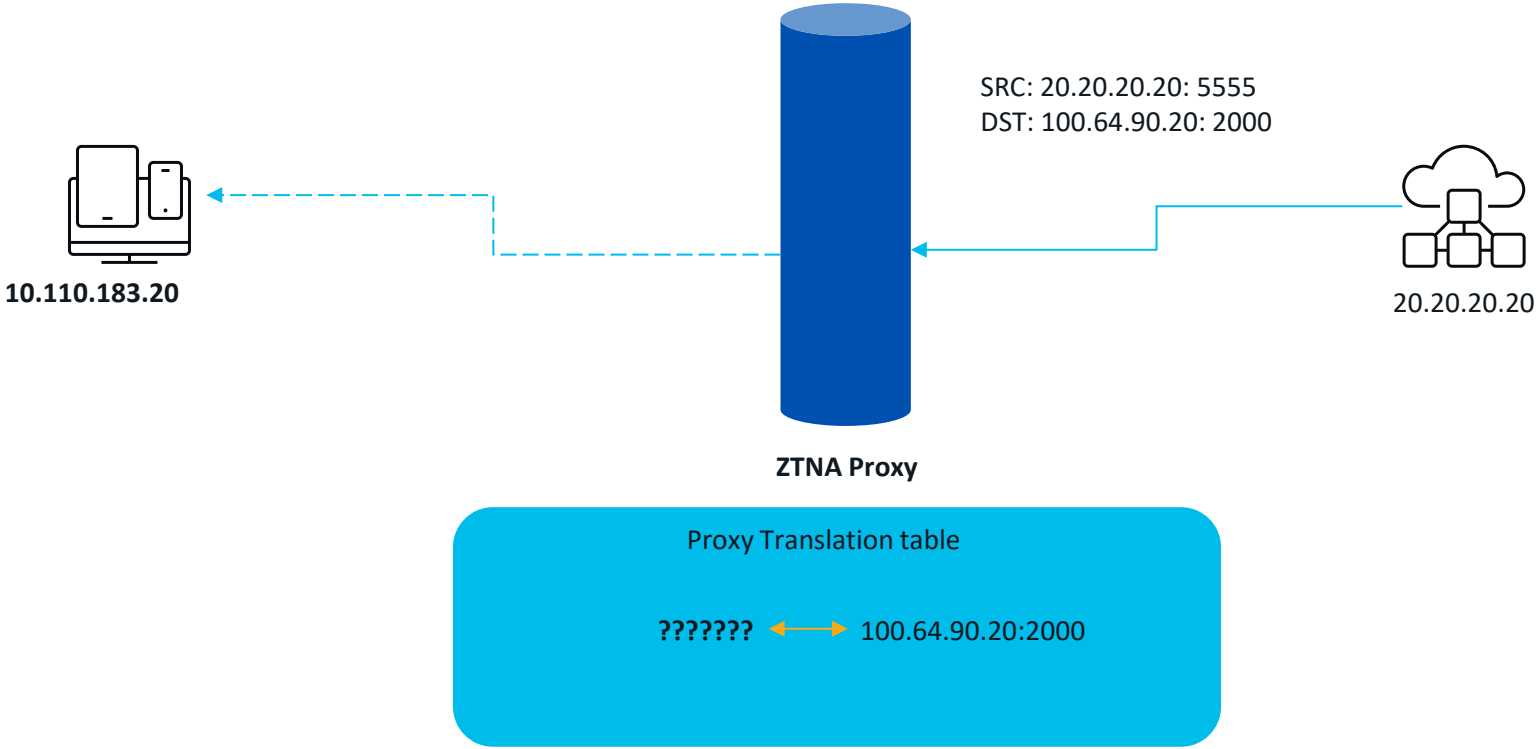
Demystifying ZTNA



Demystifying ZTNA

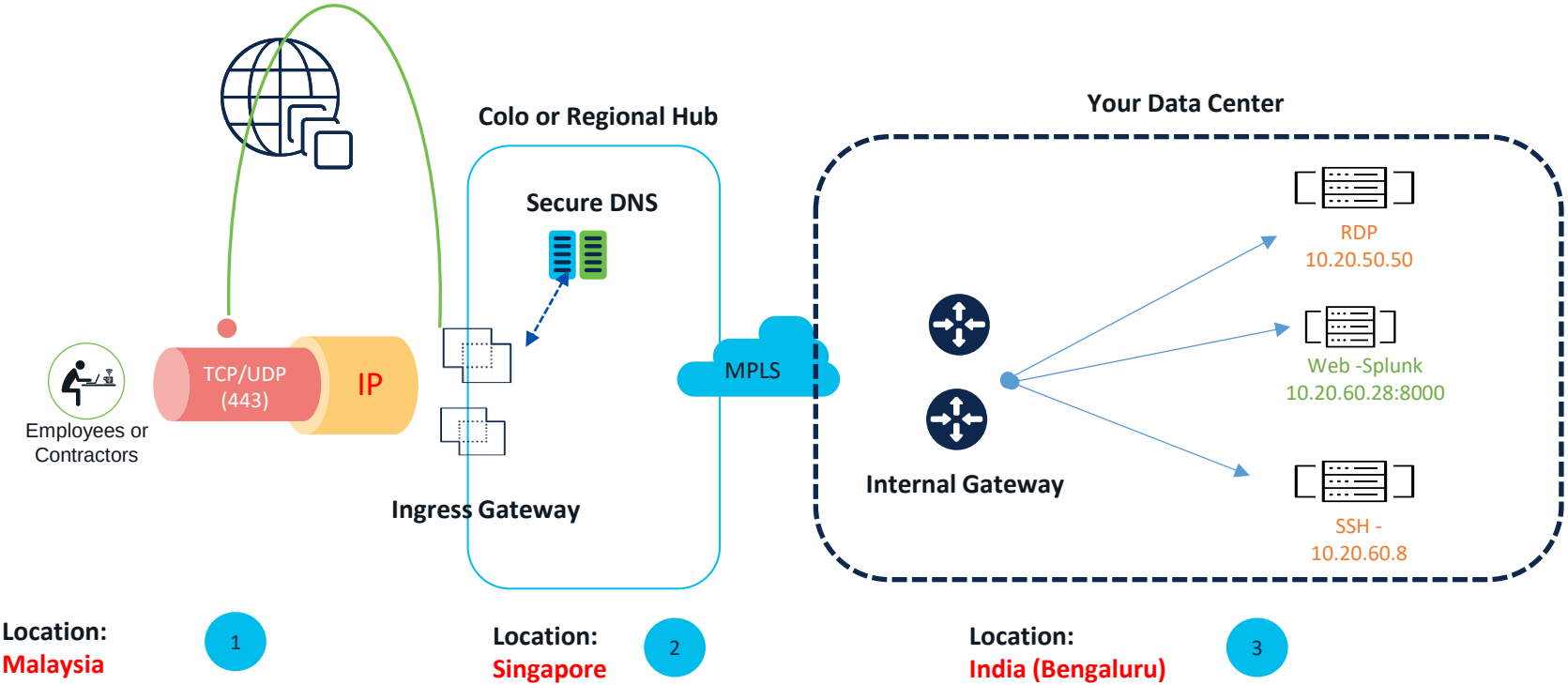


Demystifying ZTNA



Lab Topology – Secure Private Access

Existing Setup



Building Blocks For Private Access

Who Needs The Access

Corporate User with Corporate Asset
Corporate User with BYOD Asset
Vendor User with BYOD Asset

User Type

User Type

Building Blocks For Private Access

Who Needs The Access

Corporate User with Corporate Asset
Corporate User with BYOD Asset
Vendor User

User Type

User Type

How is the Identity Verified

User or User Group
Hostname
SGT
Subnet/IP address

Identity

Identity Type

Building Blocks For Private Access

Who Needs The Access

Corporate User with Corporate Asset
Corporate User with BYOD Asset
Vendor User

User Type

User Type

Secure Private App Connection

Connection Method

Private App Access

IPSec based backhaul connection
Resource Connector

How is the Identity Verified

User or User Group
Hostname
SGT
Subnet/IP address

Identity

Identity Type

Building Blocks For Private Access

Who Needs The Access

Corporate User with Corporate Asset

Corporate User with BYOD Asset

Vendor User

User Type

User Type

Secure Private App Connection

Connection Method

Private App Access

IPSec based backhaul connection

Resource Connector

How is the Identity Verified

User or User Group

Hostname

SGT

Subnet/IP address

Identity

Identity Type

User Access

Connection Method

How the user connect to SSE

Using Remote Access VPN method

Using ZTNA Agent Method

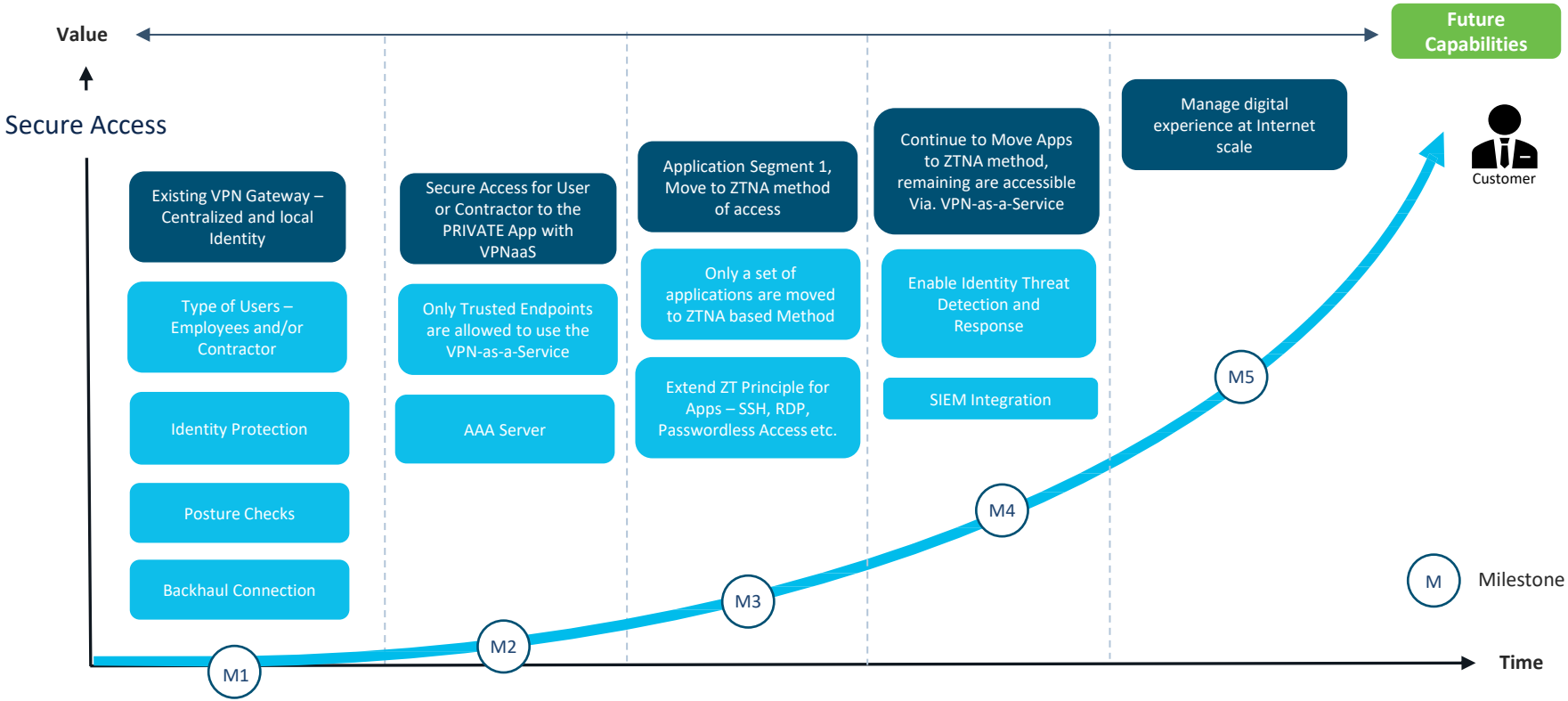
Using Browser (Clientless)Method

Deployment

Secure Private Access (Branch / DC / Roaming User)

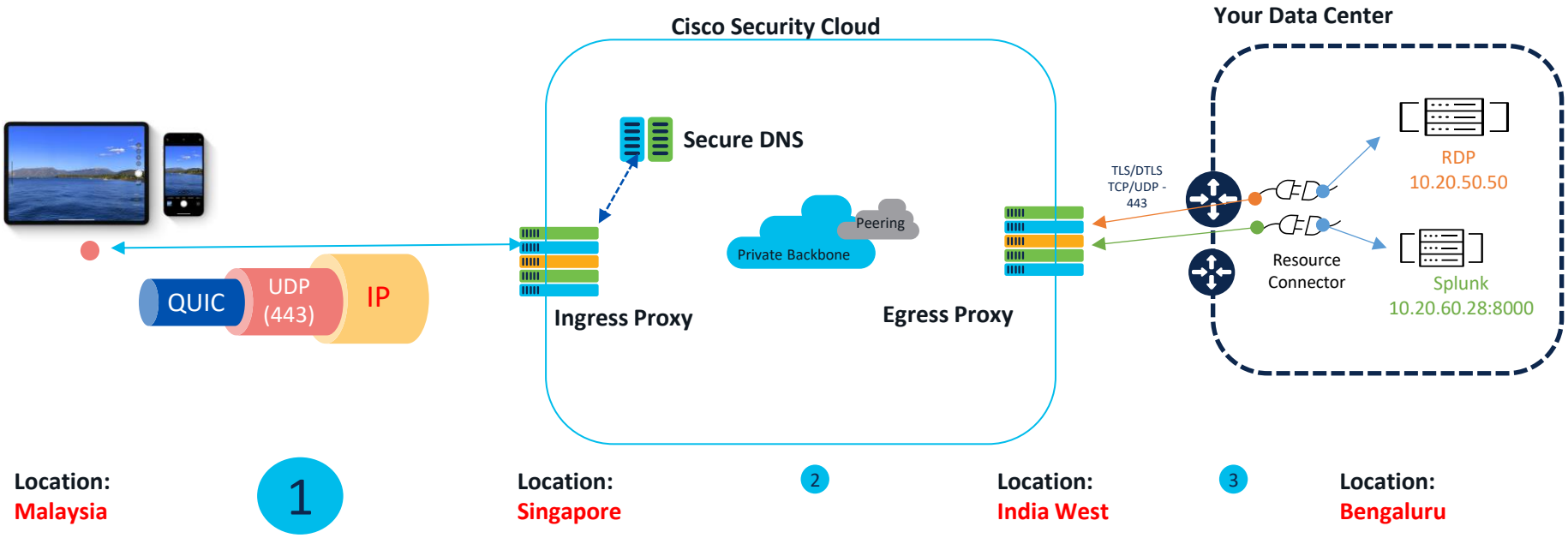
- RA VPN (Secure Client – VPN Module)
- Client-Based ZTNA (Secure Client – ZTNA Module)
- ZTNA Clientless (Browser-Based)
- Branch and DC (IPsec Tunnel and/or Resource connector)

Phased Execution - VPN -> VPNaaS -> ZTNA



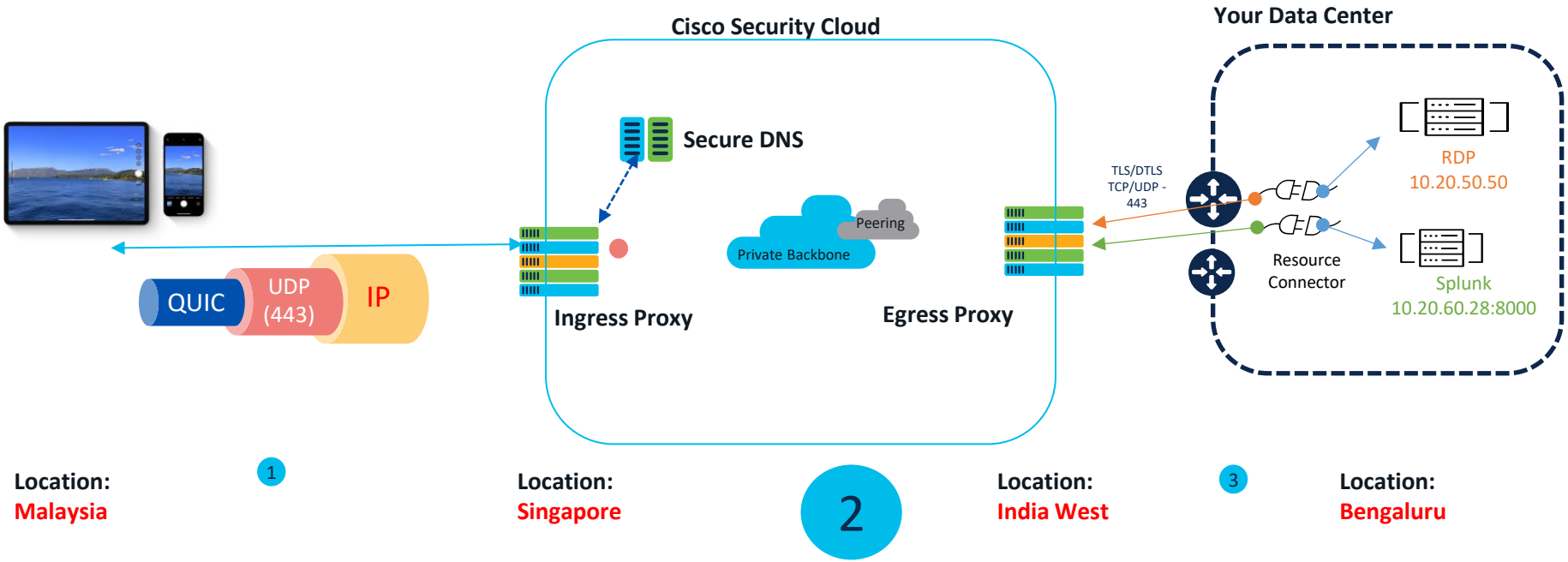
Lab Topology

ZTNA in Secure Private Access-Cisco Secure Access



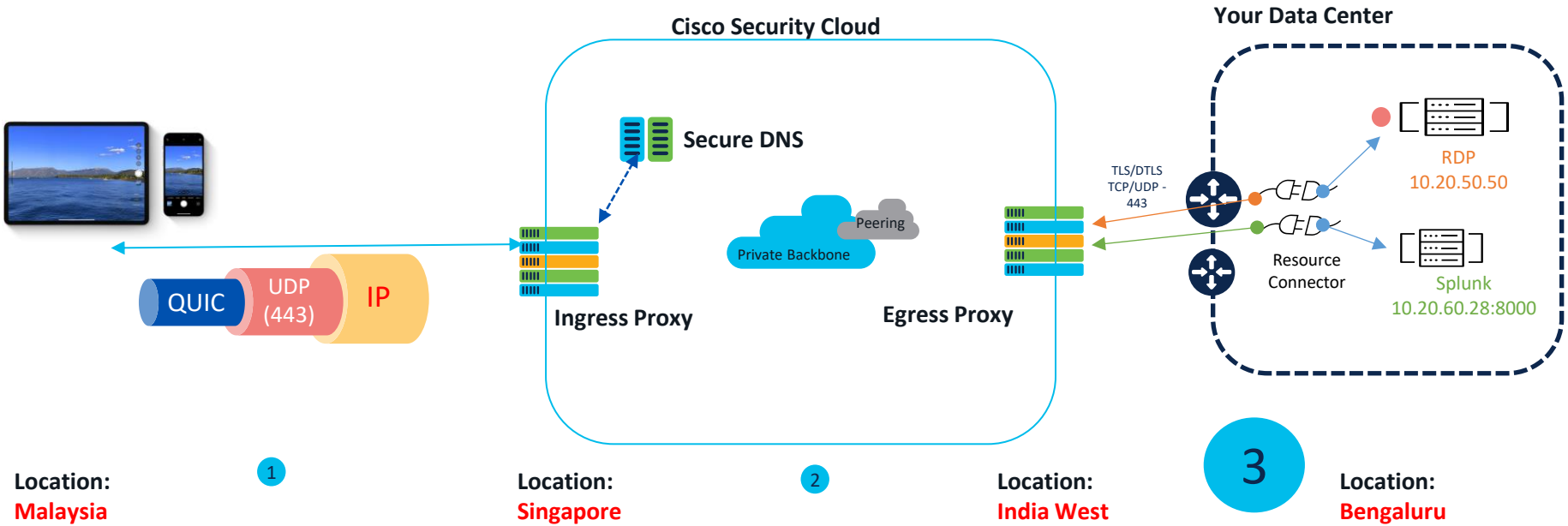
Lab Topology

ZTNA in Secure Private Access-Cisco Secure Access



Lab Topology

ZTNA in Secure Private Access-Cisco Secure Access



Private App Connection Method

IPSec Tunnel / Resource Connector

Private Applications

Pre-requisites/Deployment Steps
Setup IPsec Tunnel/App Connector (if IPsec, configure traffic selection for RAVPN IP pool/ZTNA subnet (100.64.0.0/10) and Branch private subnets)
Network config to forward RAVPN IP pool/ZTNA subnet (100.64.0.0/10) through the tunnel
Configure Private Resources/Groups on Secure Access dashboard
*Configure Private Access Policy to allow access to Private Resources
Reporting review

**Requires identity sources to be provisioned prior this task*

User Access

Connection Method – Remote Access VPN

Pre-requisites/Deployment Steps
User Provisioning *(Manual, AD, IdP)*
Deploy Secure Access Root CA *(if not deployed already)*
Configure Endpoint Posture Profile *(if not deployed already)*
Configure RA VPN Settings • Configure DNS Servers *(*If local DNS server, create Private Access Resource and Private Access Policy to allow access to it)* • IP Pool dedicated for RA VPN
Configure RA VPN Profile • Configure General Settings *(Endpoint Posture Profile *optional)* • Define Authentication Method *(SAML | Cert | MultiCert | SAML+Cert)* • Define Traffic Steering • Define Endpoint Settings
Provision the Secure Client VPN Module & .xml profile
Configure Private Access Policy to allow access to Private Resources
Reporting Review

User Access

Connection Method – Client Based ZTNA

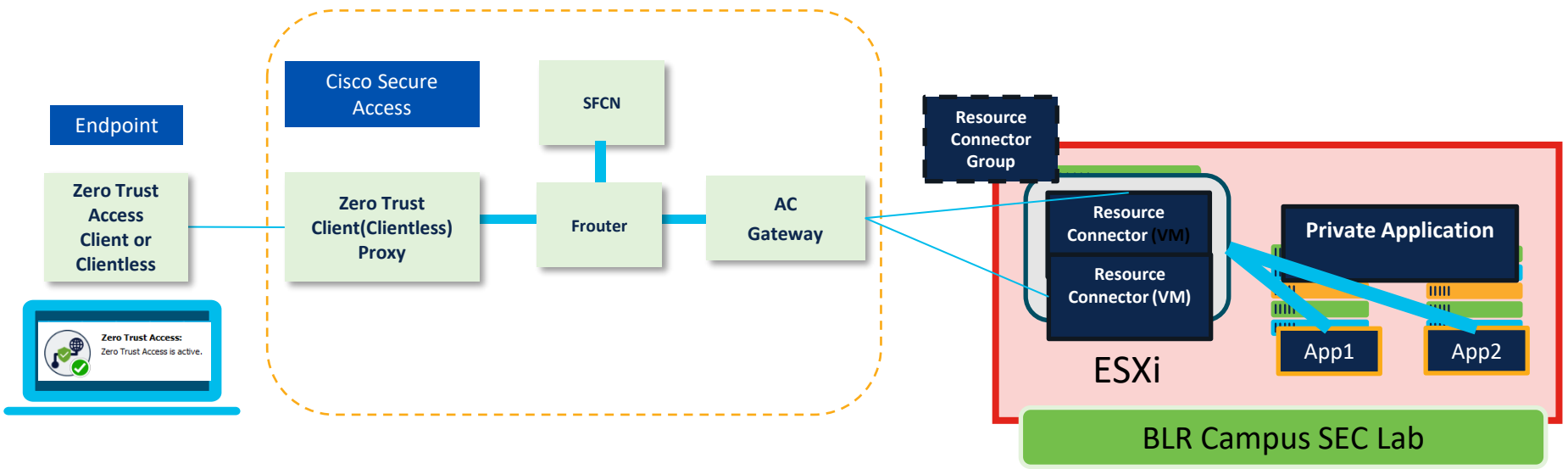
Pre-requisites/Deployment Steps
User Provisioning *(Manual, AD, IdP)*
Setup SAML authentication with your preferred IdP
Deploy Secure Access Root CA *(if not deployed already)*
Configure Endpoint Posture Profile *(optional)*
Provision the Secure Client ZTNA Module & Enrollment Process
Configure Private Access Policy to allow access to Private Resources
Reporting Review

User Access

Connection Method – Clientless ZTNA

Pre-requisites/Deployment Steps
User Provisioning *(Manual, AD, IdP)*
SAML Authentication
Deploy Secure Access Root CA *(if not deployed already)*
Configure Posture Profile *(optional)*
Determine Private Resource provisioning method for initial Resources *(Public URL for Private Resources)*
Configure Private Access Policy to allow access to Private Resources
Reporting Review

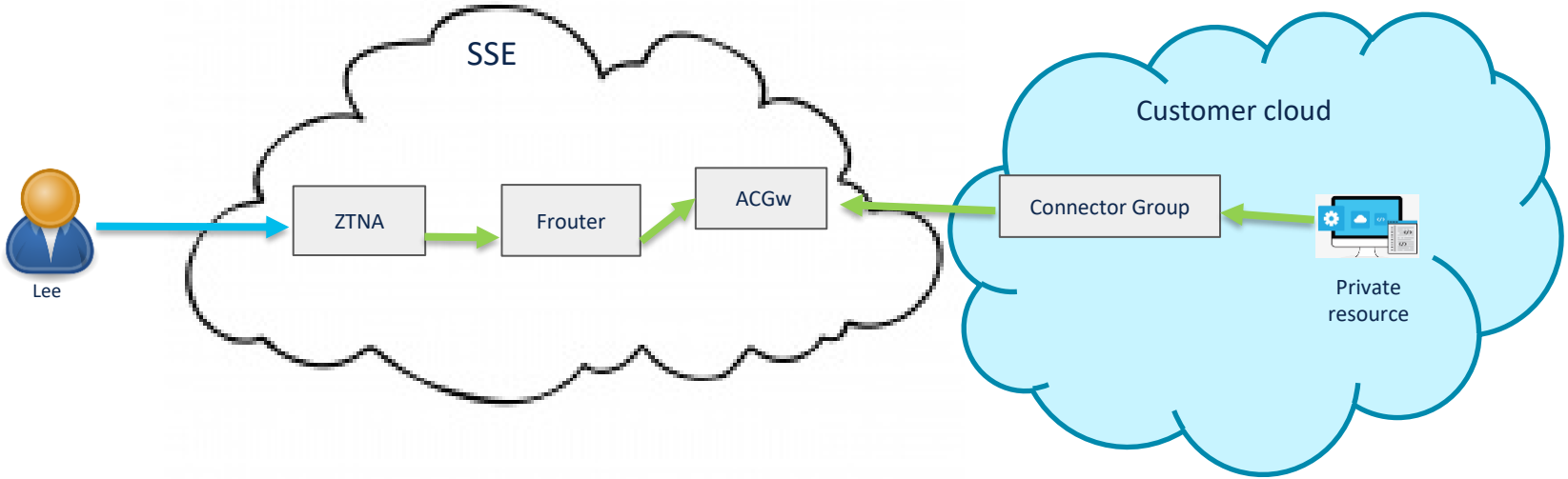
Topology



Resource Connector and No IPSec

Scenario:

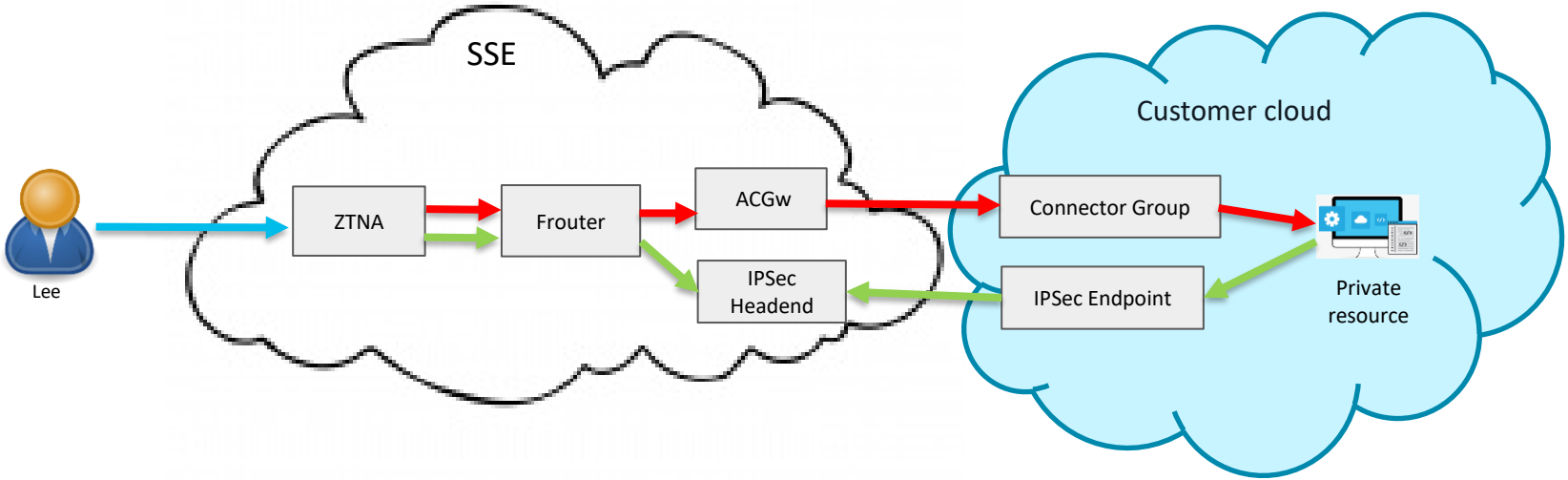
- Resource Connector is preferred path
- No IPSec Tunnel possible in SEC due to InfoSec Compliance.



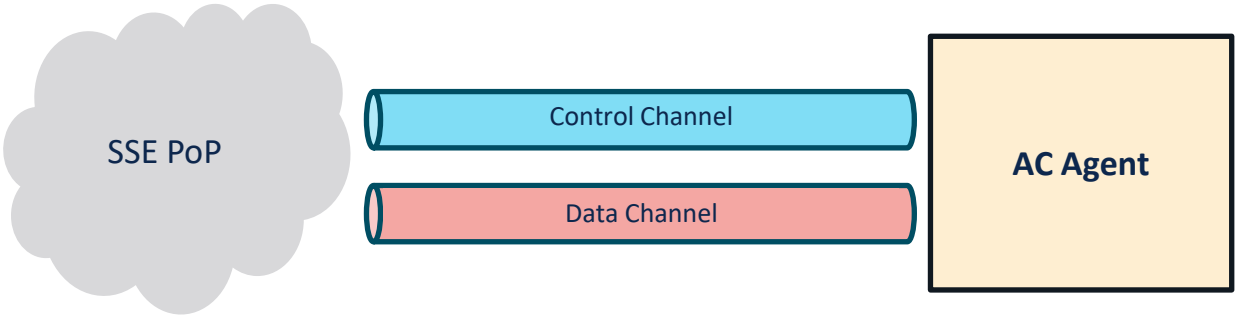
Failover between Resource Connector and IPSec

Scenario:

- Resource Connector is preferred path
- If IPSec exists, then ZTNA fails over to IPSec on ACGw API returning *not-found* or error



Communication Channel for App Connectors



Firewall access rules for App Connectors

SSE Services	FQDN/IPs for Whitelisting	Port/Protocol
Gateway	Cisco IP Space	TCP/UDP 443
Controller	us.controller.acgw.sse.cisco.com eu.controller.acgw.sse.cisco.com Ap.controller.acgw.sse.cisco.com Will resolve to AWS Static IPs	TCP/443
Repo (Auto upgrades)	us.repo.acgw.sse.cisco.com eu.repo.acgw.sse.cisco.com Ap.repo.acgw.sse.cisco.com Will resolve to AWS Static IPs	TCP/443
ACME	prod.acme.sse.cisco.com	TCP/443
SSE API Gateway	api.sse.cisco.com	TCP/443
SSE PKI	Ssepki.cryptosvcs.cisco.com	TCP/80

- Customer edge firewall rules (FQDNs/IPs)

Resource connector deployment steps

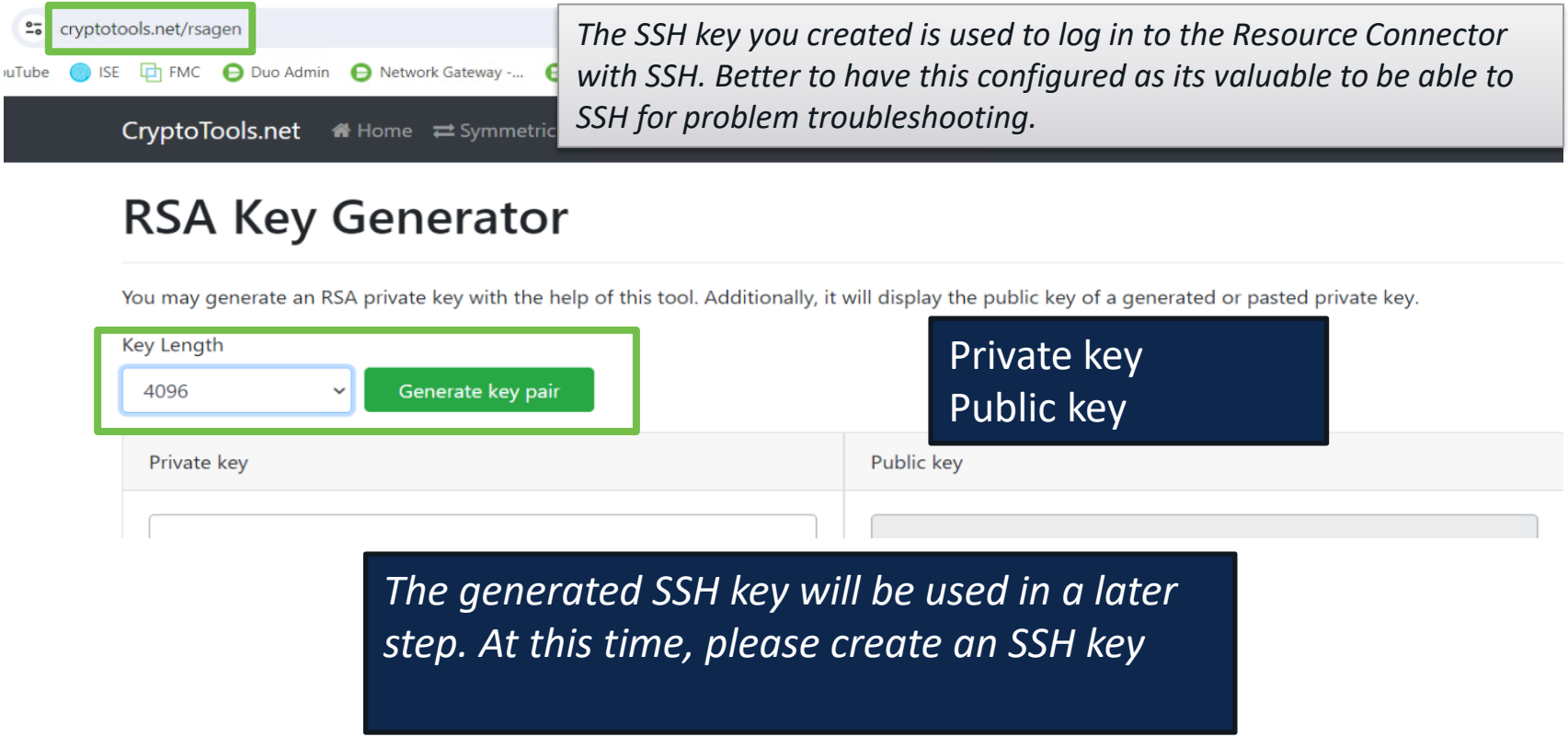
Item No.	Operational Locations	Implementation details
0	Any device	(Optional) Create an SSH key
1	Secure Access console	Defining Connector Groups
2	Secure Access console	Download the resource connector image
3	VMware ESXi – 7.0.3	Deploy a resource connector
4	Secure Access console	Add a resource connector to the “Confirm”
5	Secure Access console	Assigning Private Resources to a Resource Connector Group
6	ZTA Terminals with module installation	Make sure you have access to private resources
7	Any device	(Optional) SSH to the Resource Connector

<After work>

- If necessary, you can add more resource connectors to increase throughput capacity
- If necessary, assign the newly added private resources to the connector group

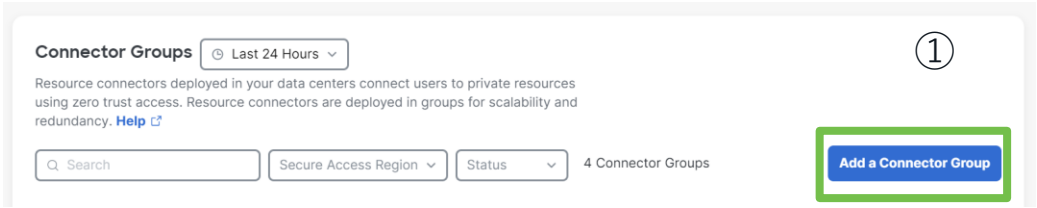
0. (Optional) Create an SSH key

Any device

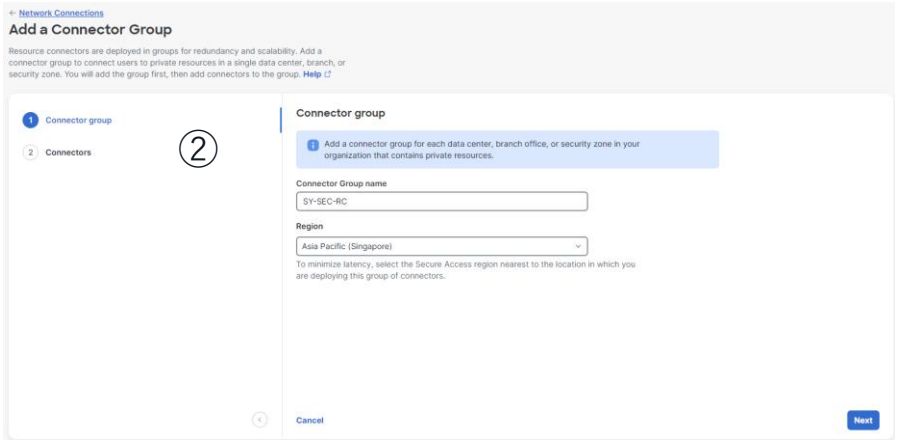


1. Define connector groups

Secure access console



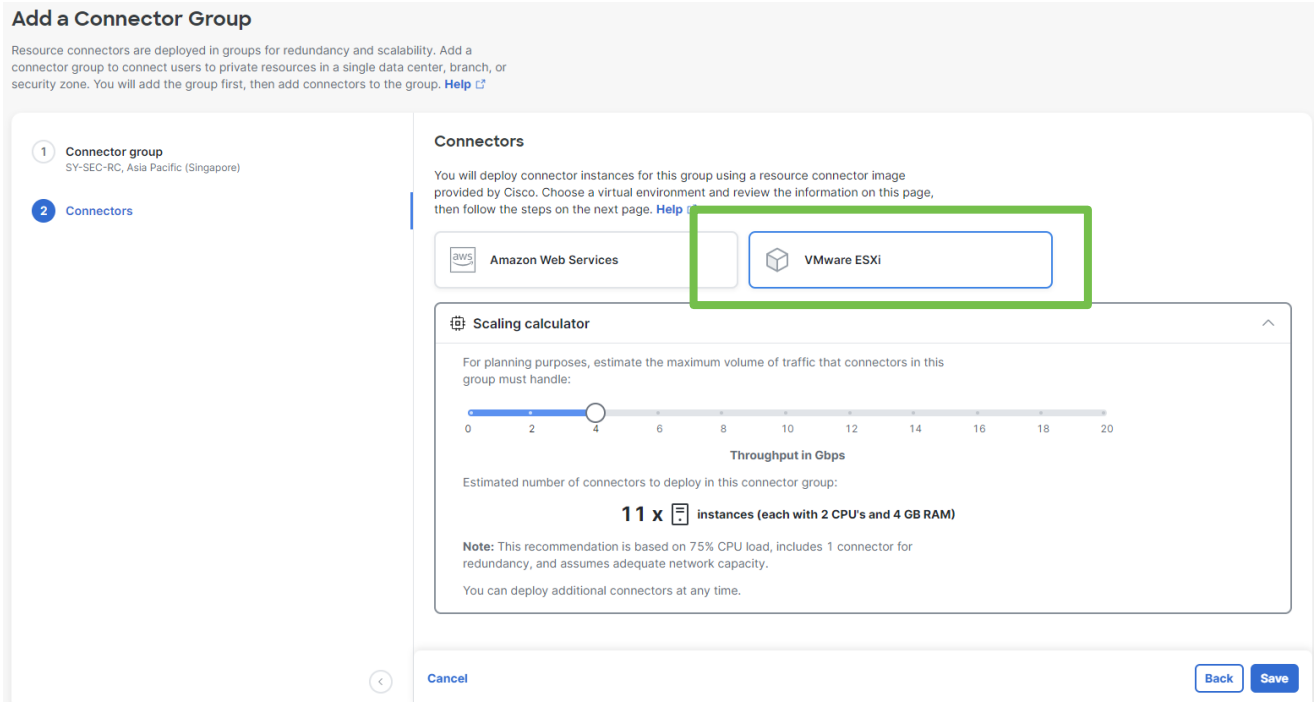
② Enter a name of your choice, Connector Select the region where you want to install it. Choose a region that is close to the private resources you want to access. (Region can only be set on this screen.)



1. Define connector groups

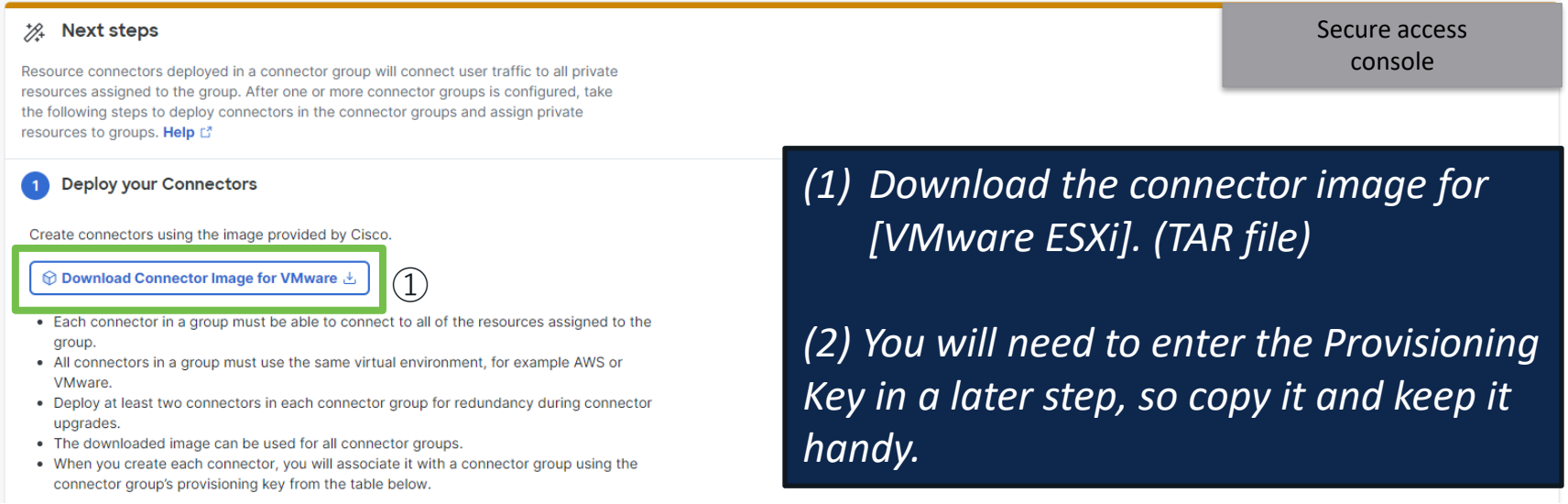
Secure access console

[VMware ESXi] Select Create



2. Download the resource connector image

Secure access console

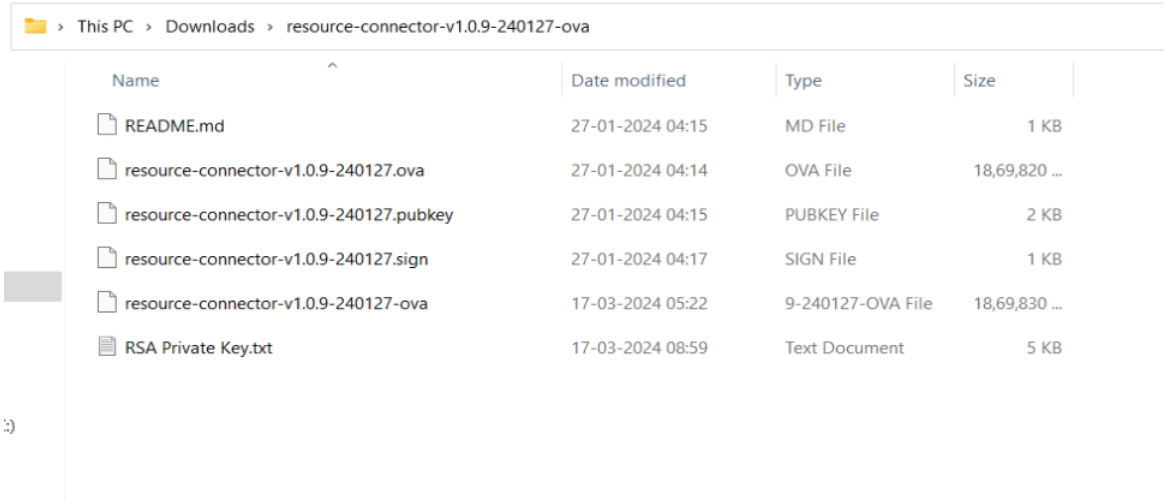


(1) Download the connector image for [VMware ESXi]. (TAR file)

(2) You will need to enter the Provisioning Key in a later step, so copy it and keep it handy.

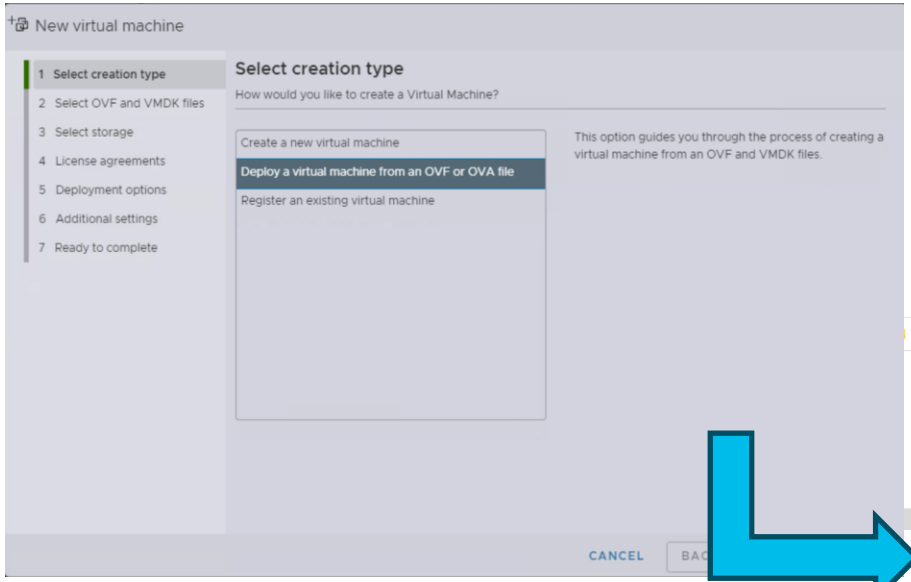
2. Download the resource connector image

Untar the file and then use this ova file

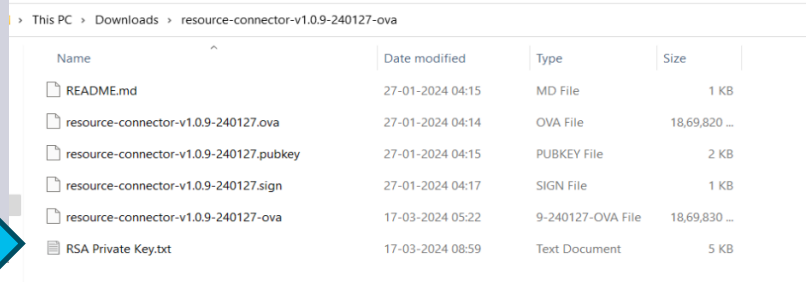


3. Deploy the resource connector

VMware ESXi

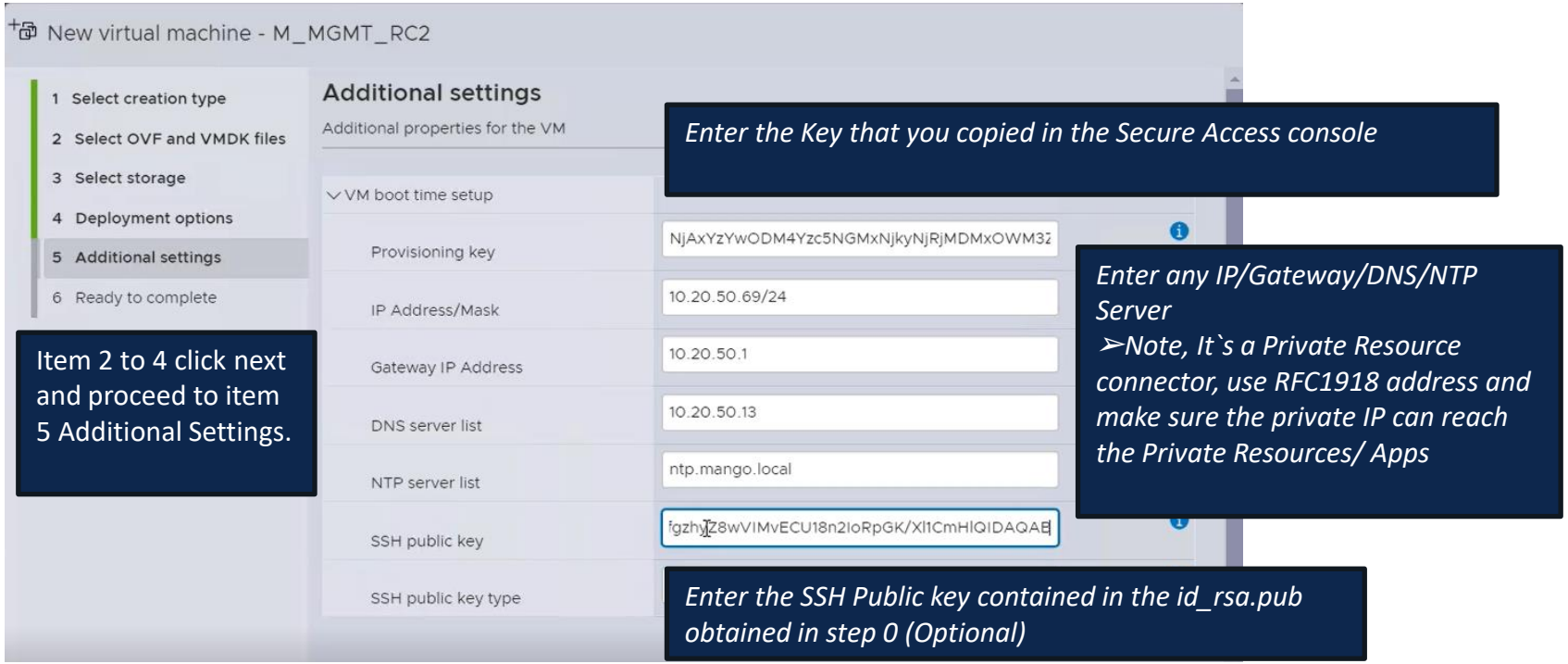


In the VMware ESXi console, specify the ova file that you unzipped in the previous page to deploy the resource connector.



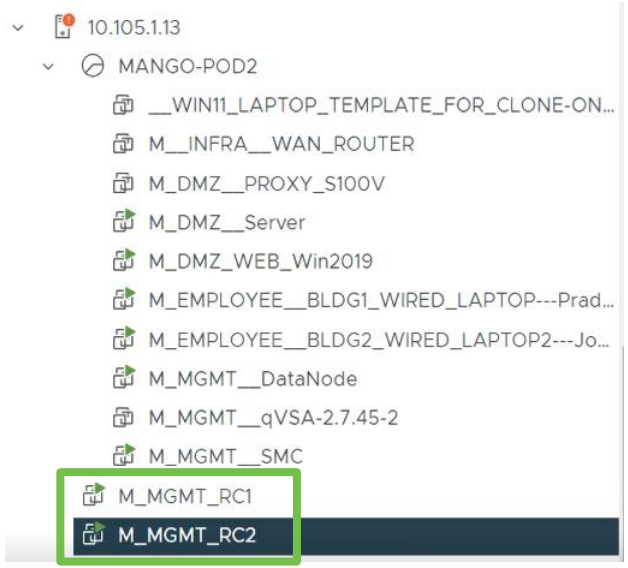
3. Deploy the resource connector

VMware ESXi



3. Deploy the resource connector

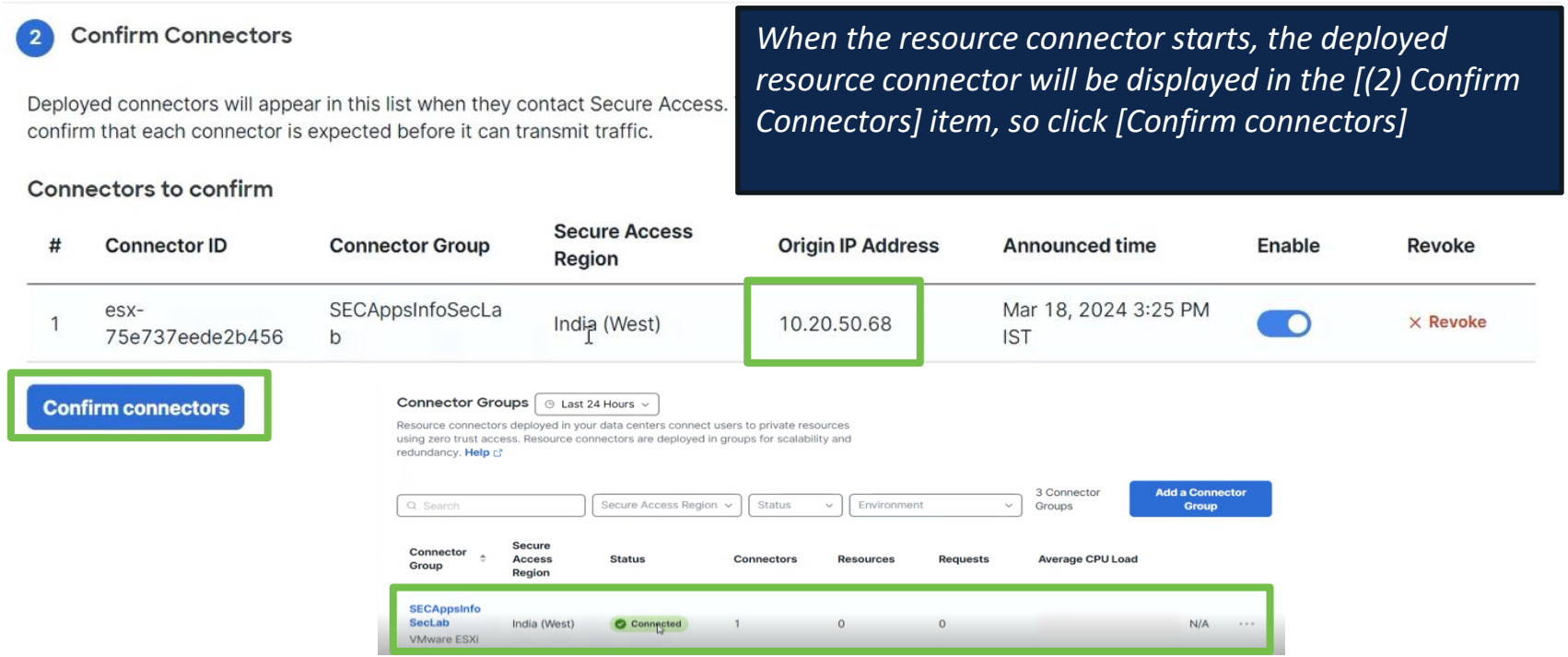
VMware ESXi



3. “Confirm” the resource connector

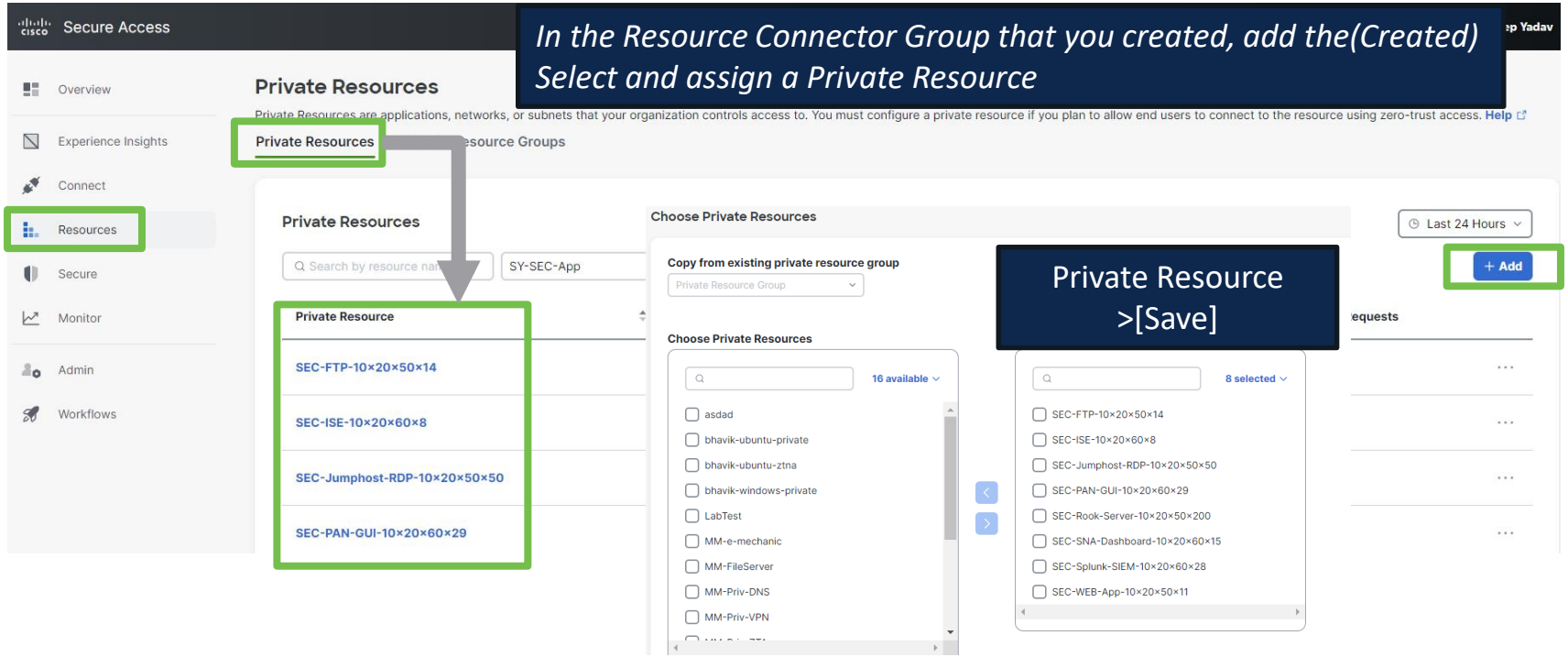
Secure access console

When the resource connector starts, the deployed resource connector will be displayed in the [(2) Confirm Connectors] item, so click [Confirm connectors]



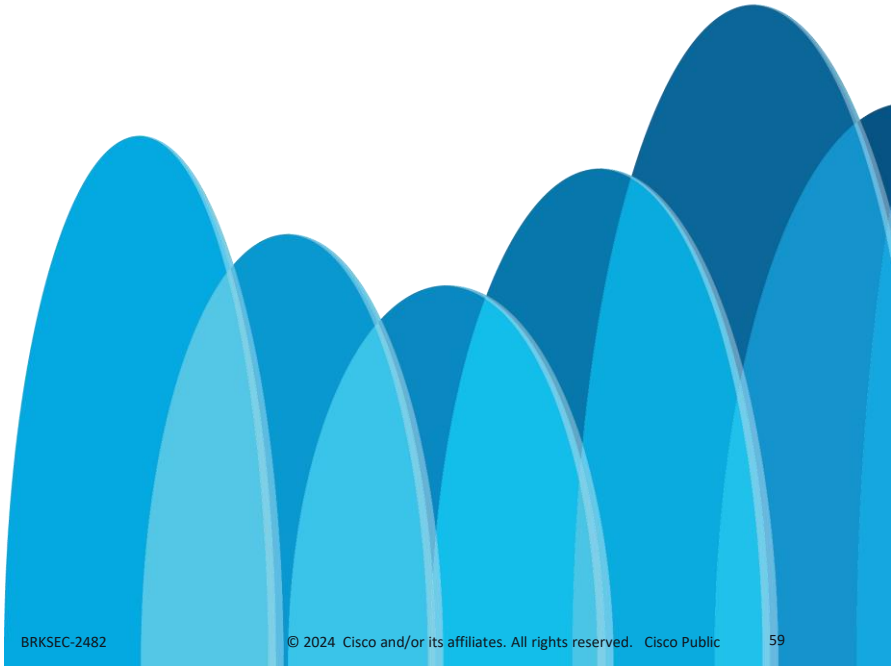
4. Assign private resource to a resource connector group

Secure access console

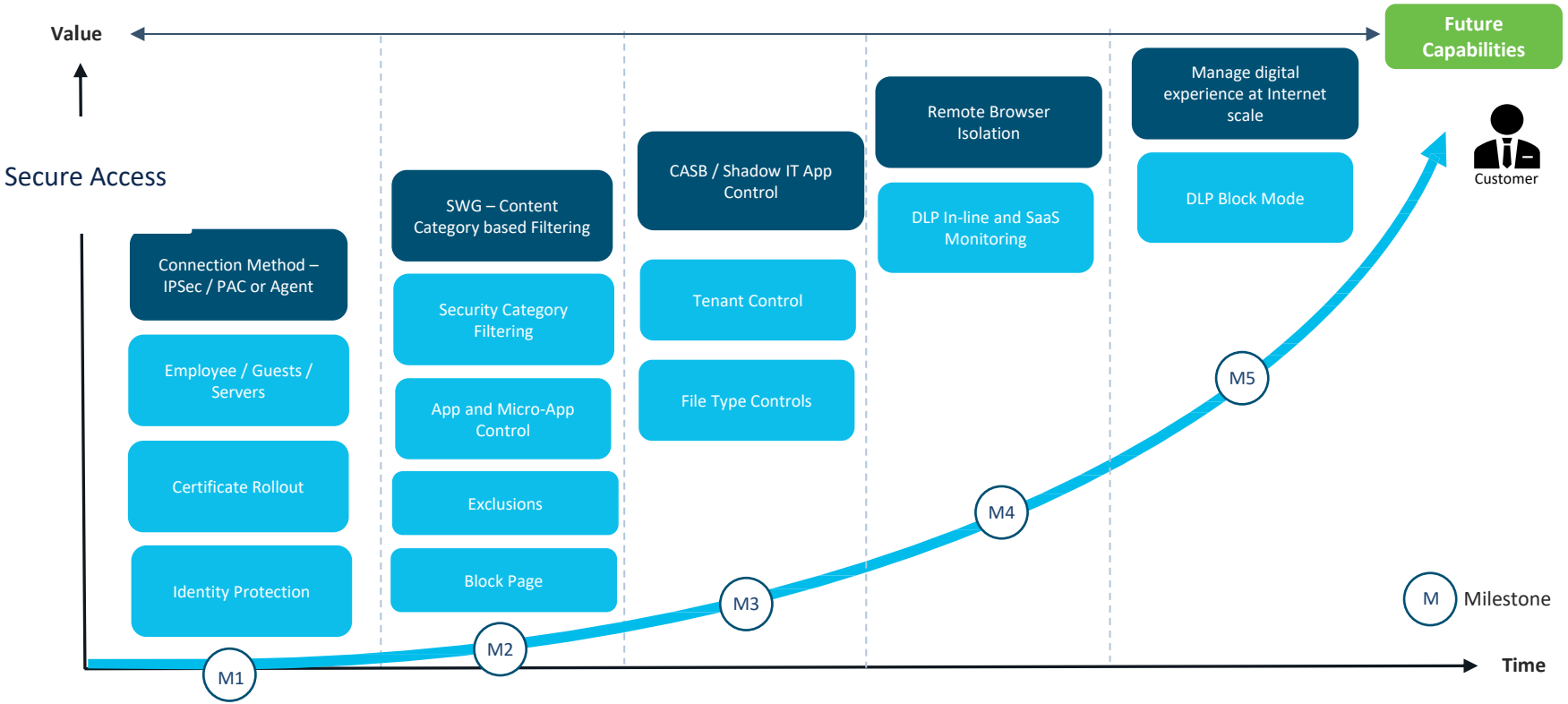


We have a Proxy Appliance and wish to replace it with a Cloud Proxy

Here is what you need to know.



Phased Capability Execution



Deployments

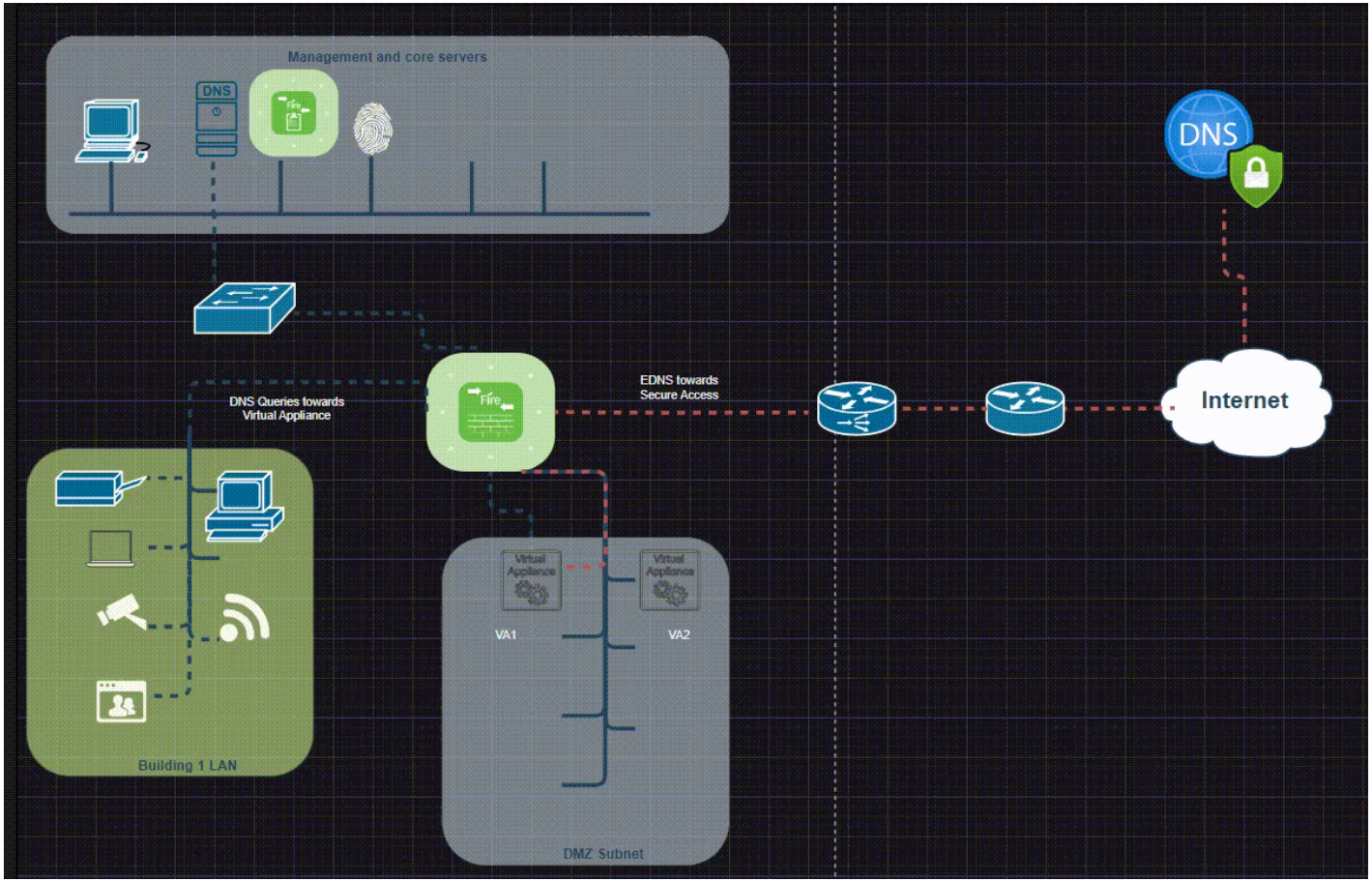
Secure

- Network Protection
- PAC File
- Branch (IPsec Tunnel)
- Roaming Module
- RA VPN (Secure Client – VPN Module)

Secure DNS Traffic

Layer 1

Pre-requisites/Deployment Steps
Register your public IP address
Point local DNS forwarders to Secure Access Resolvers *(208.67.222.222 & 208.67.220.220)*
Deploy Secure Access Root CA
Reporting Review
Configure Internet Access Rule to enforce required protection and access controls *(optional)*



DNS VA Deployment and Configuration

cisco Live!

Secure SWG Traffic

Method: PAC URL

Pre-requisites/Deployment Steps
Configure Domains to be bypassed from Secure Access
Review Network Requirements
Register your public IP address
Deploy Secure Access Root CA
Configure the Secure Access hosted PAC file on endpoints
Reporting Review
User Visibility – User Provisioning *(Manual, AD, IdP) (optional)*
Enable SAML Authentication *(*requires decryption enablement) (optional)*
Configure Internet Access Rule to enforce required protection and access controls *(optional)*

SWG Layer PAC URL Configuration

cisco Live!

Secure SWG Traffic

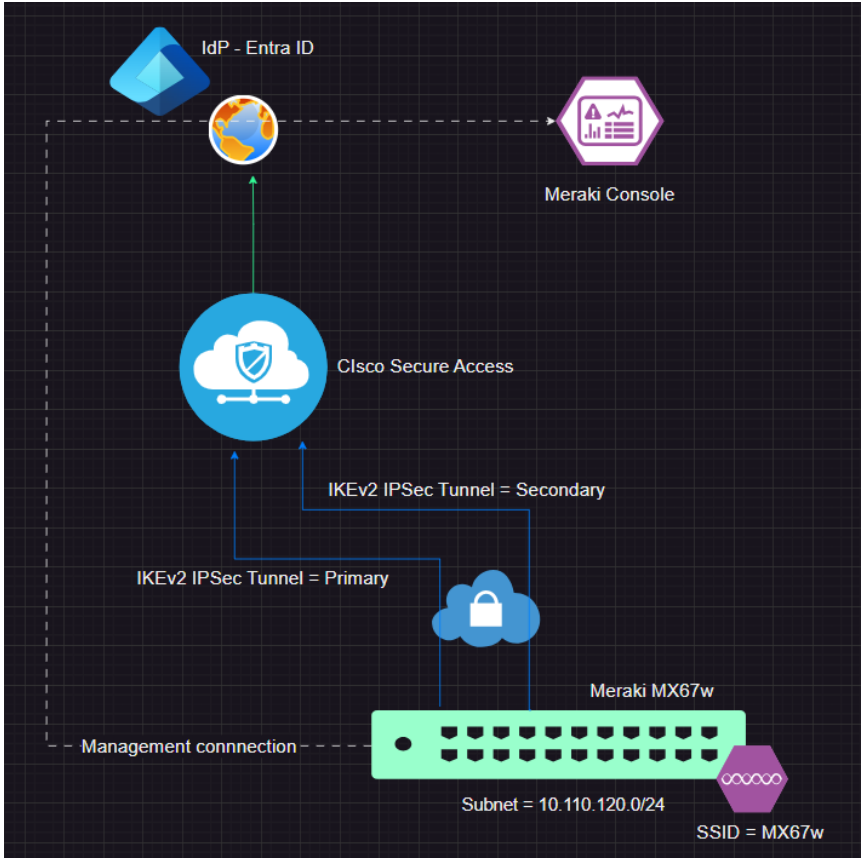
Method: IPSec Tunnel

Pre-requisites/Deployment Steps
Deploy Secure Access Root CA *(if not deployed already)*
Identify location, edge devices, existing tunnels and subnets
Setup IPsec Tunnel & Traffic Selection to be routed to Secure Access
User Visibility – User Provisioning *(Manual, AD, IdP) (optional)*
Enable SAML Authentication *(*requires decryption enablement) (optional)*
Reporting Review
Configure Internet Access Rule to enforce required protection and access controls *(optional)*

Example of Connecting Meraki MX to Cisco Secure Access with IKEv2 IPSec Tunnel

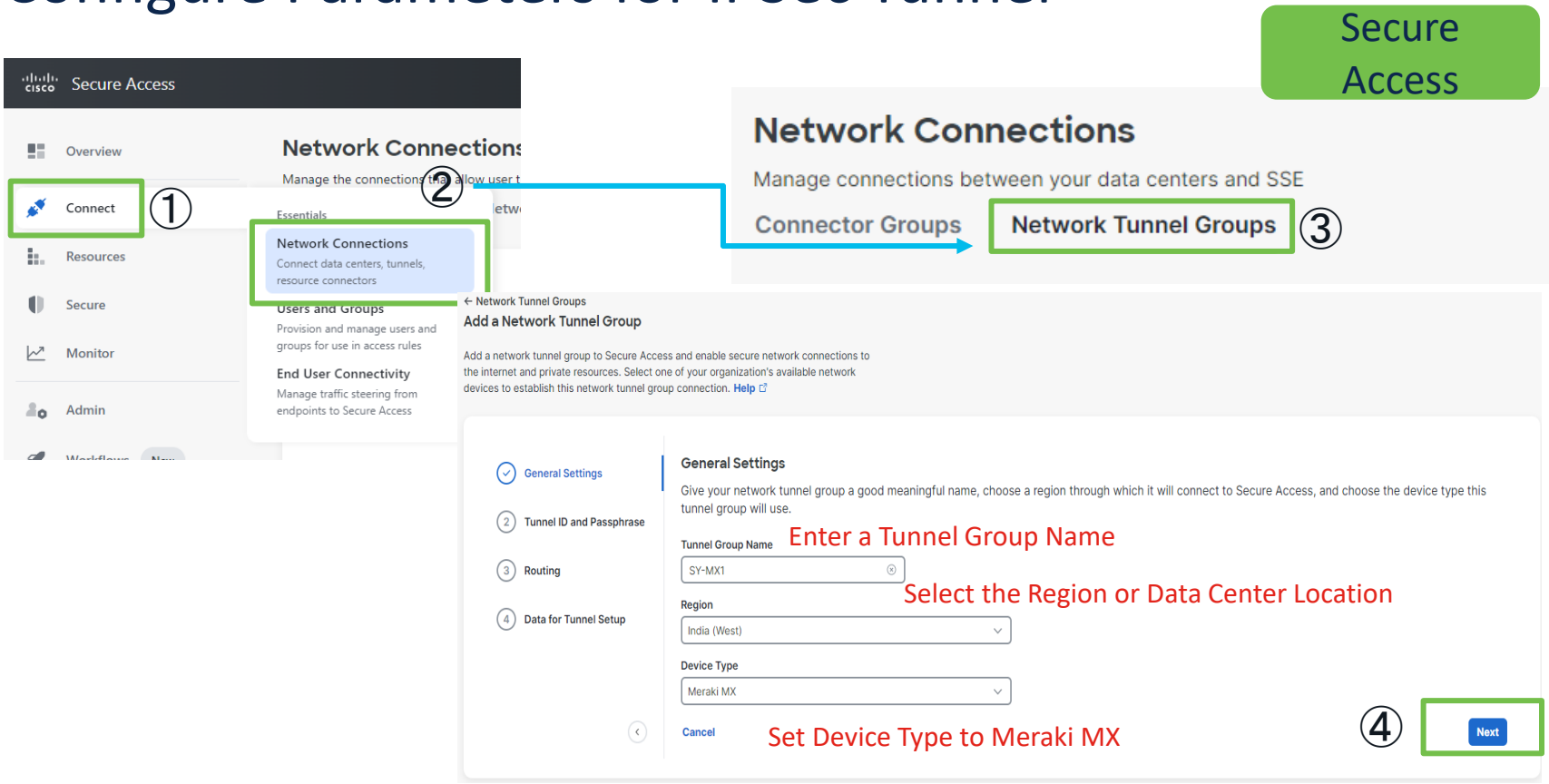
MX67W in this Example

cisco Live!



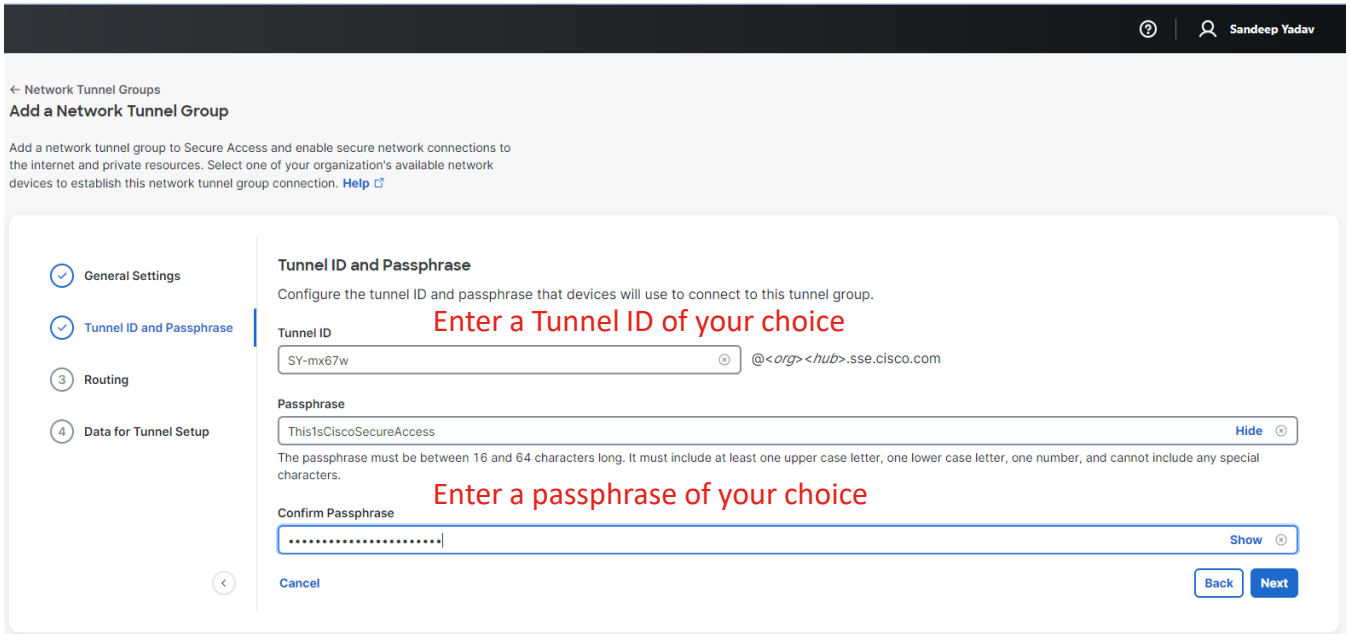
Item No.		Configuration Console	Task
1	**Configuring Parameters for IPSec Tunnel Connections**		
	1	Cisco Secure Access	Tunnel Group, Data Center Location, Tunnel ID, Tunnel Passphrase and routing information.
2	**Creating and Connecting IPSec Tunnels**		
	1	Meraki Console	Configuring an IPSec Tunnel in Site-to-site VPN
3	**Verification**		
	1	Meraki Console	Confirmation of the VPN Status
	2	Cisco Secure Access	Confirmation of the Tunnel Status
4	Verification of Access Policy and Reporting		

Configure Parameters for IPSec Tunnel



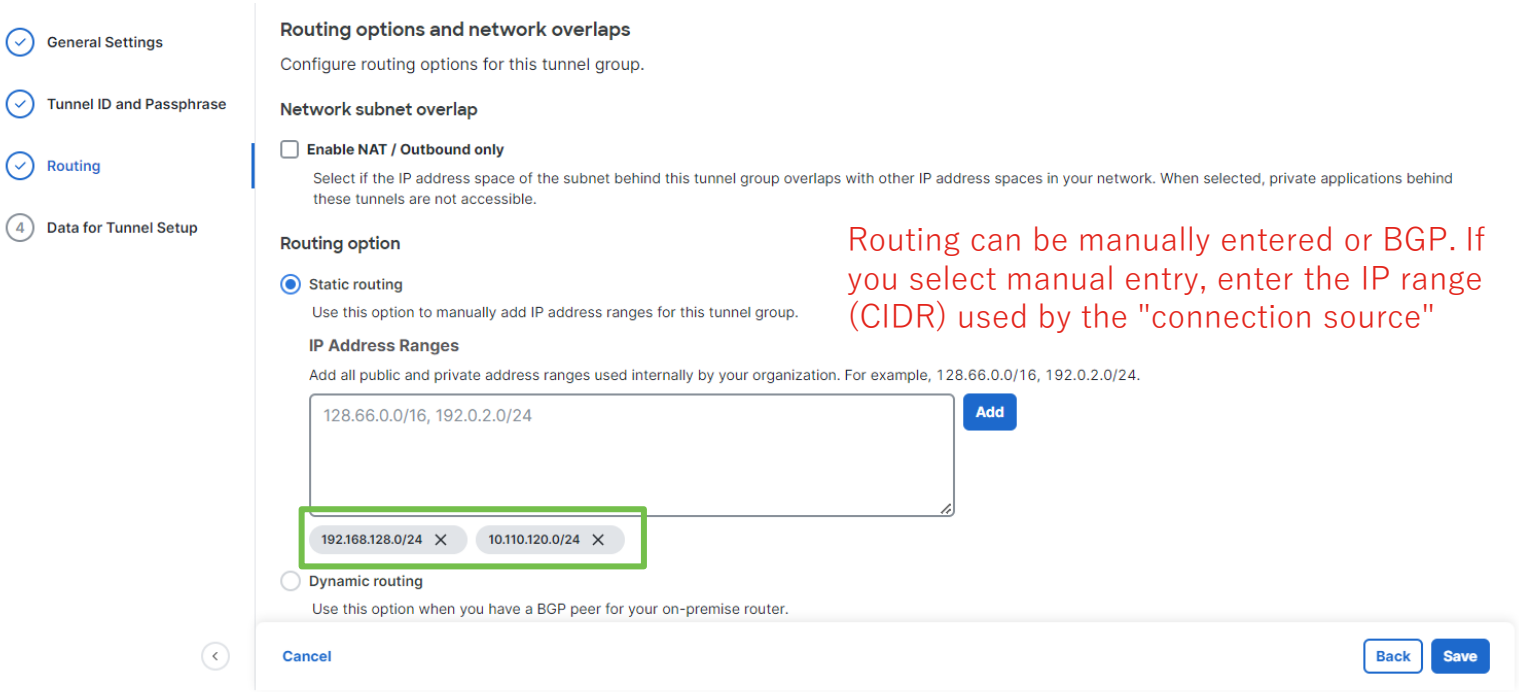
Configure Parameters for IPSec Tunnel

Secure Access



Configure Parameters for IPSec Tunnel

Secure Access



Routing can be manually entered or BGP. If you select manual entry, enter the IP range (CIDR) used by the "connection source"

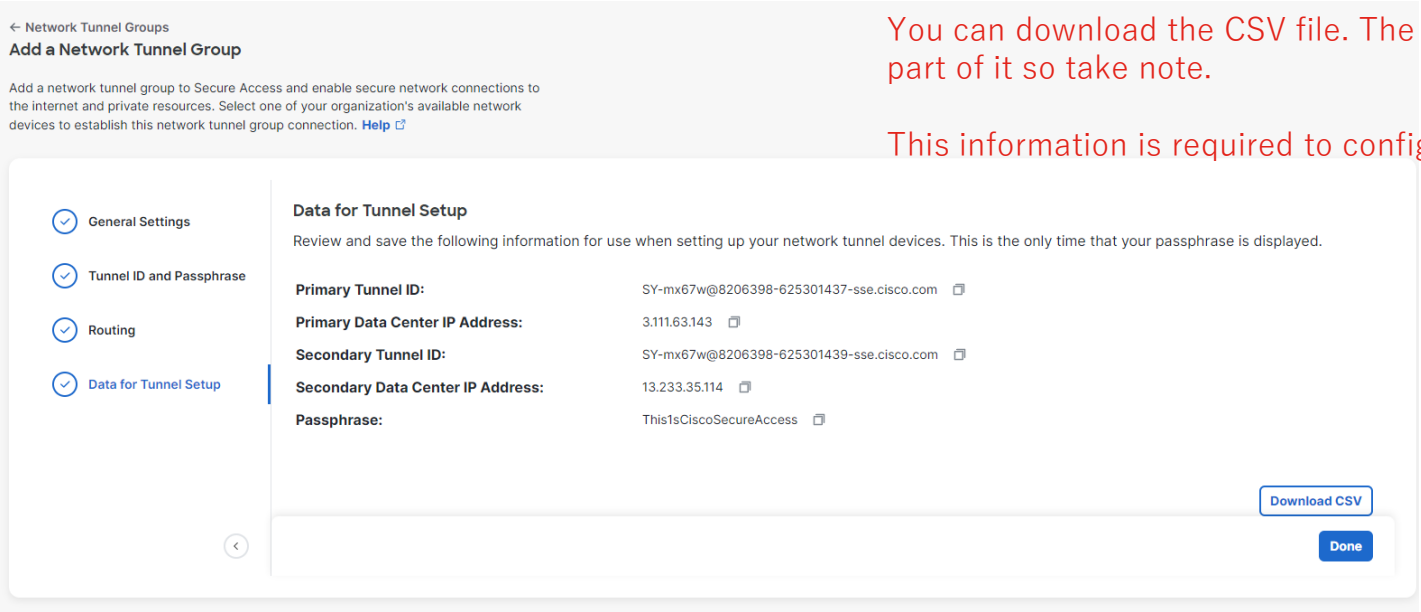
Configure Parameters for IPSec Tunnel

Secure Access

In the Final Step, Tunnel Setup parameters with Data Center IP address are displayed.

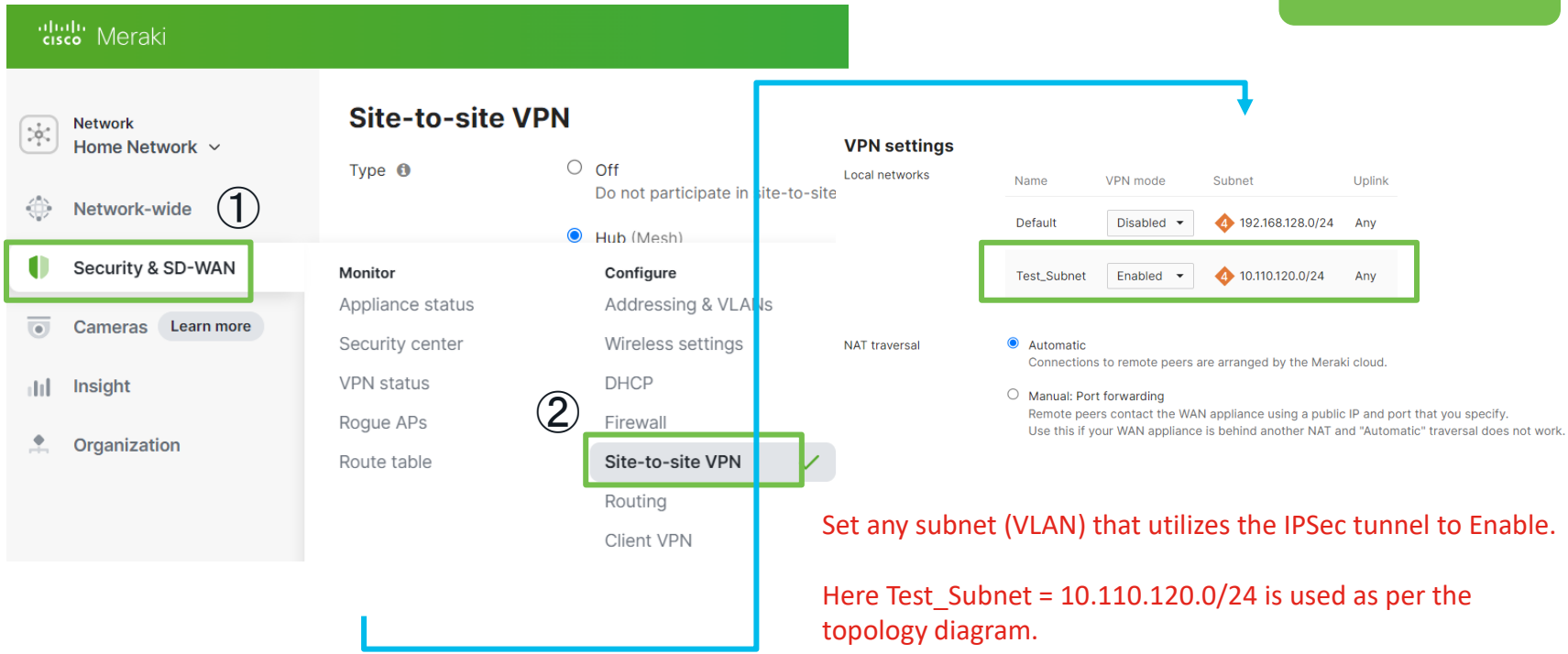
You can download the CSV file. The passphrase is not part of it so take note.

This information is required to configure Meraki MX.



Configure Site-to-Site VPN

Meraki

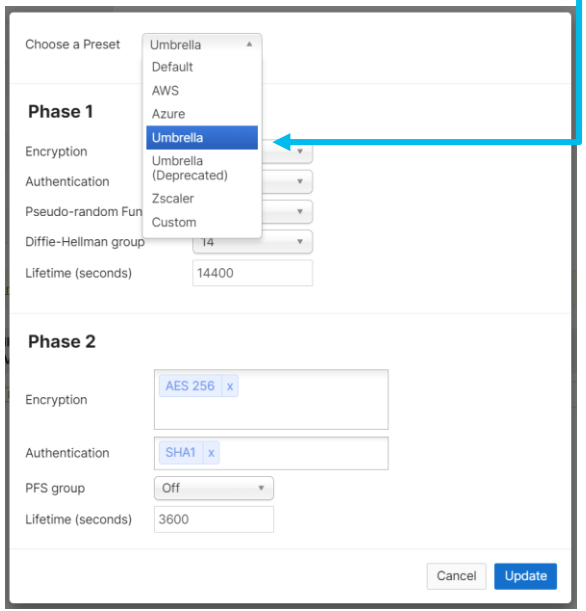


Set any subnet (VLAN) that utilizes the IPSec tunnel to Enable.

Here Test_Subnet = 10.110.120.0/24 is used as per the topology diagram.

Configure Site-to-Site VPN

Meraki

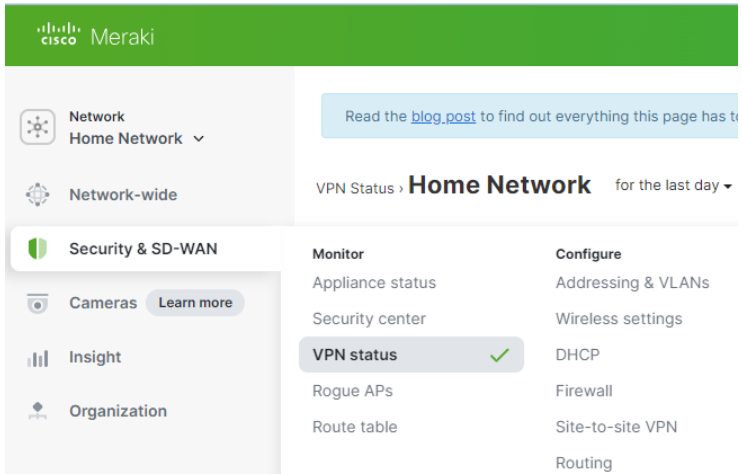


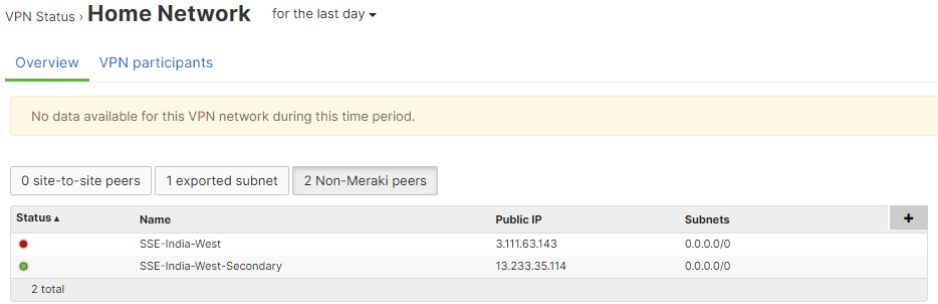
Name: Enter a name of your choice
IKE version: *Select IKEv2*
IPSec Policies: Click and Choose “Umbrella” from the Choose a Preset option of IPsec Profile. Next, click "Update
Public IP/Hostname: Enter the IP address of the data center you got from the SSE console.
User FQDN (or Local ID): Enter the Tunnel ID that you have from the SSE console.
Remote ID: Leave blank
Private subnets: Type "0.0.0.0/0“
PreShared secret: Enter the Passphrase you configured on the SSE console.
Availability: Select any network

Lastly, click "Save Changes" at the bottom of the screen at the end.

Verification of Site-To-Site IPSec Tunnel

Meraki

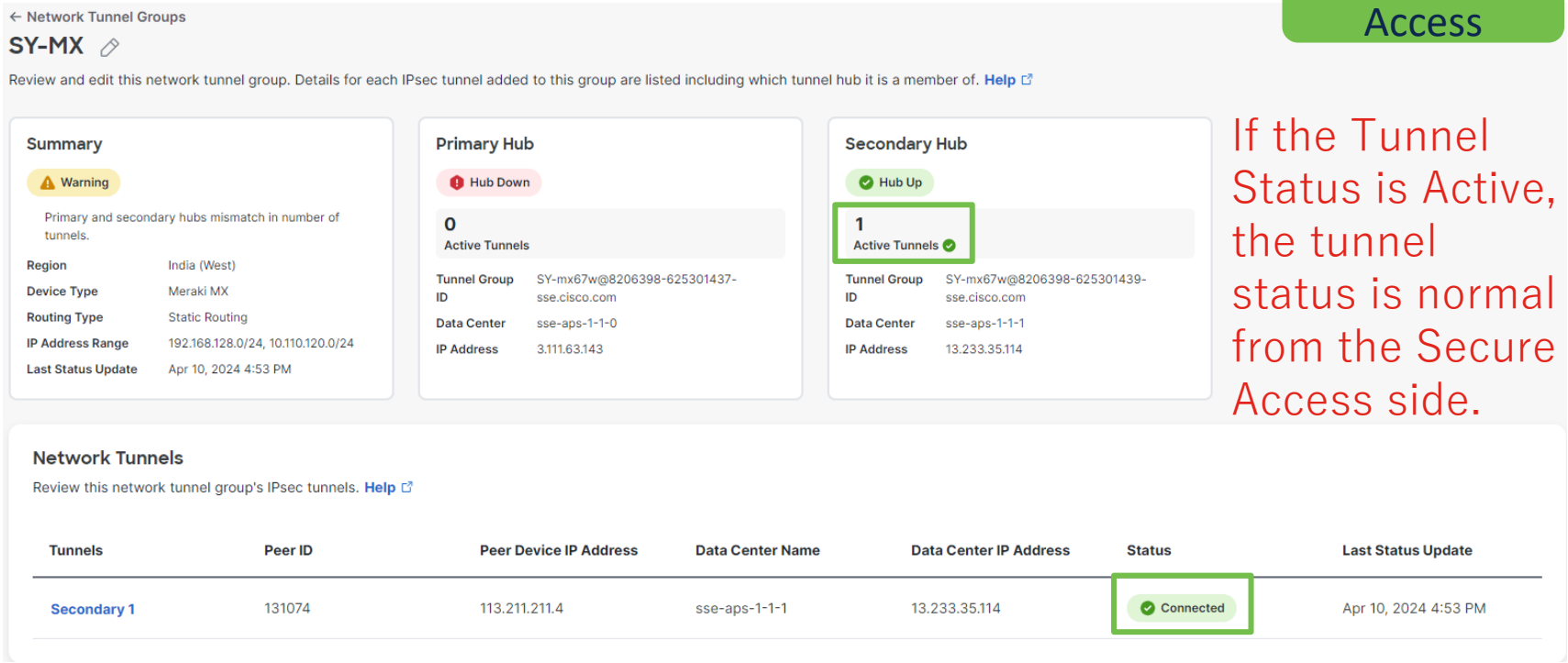




If Status is a green light, it is a normal tunnel status from the Meraki side.

Verification of Site-To-Site IPSec Tunnel

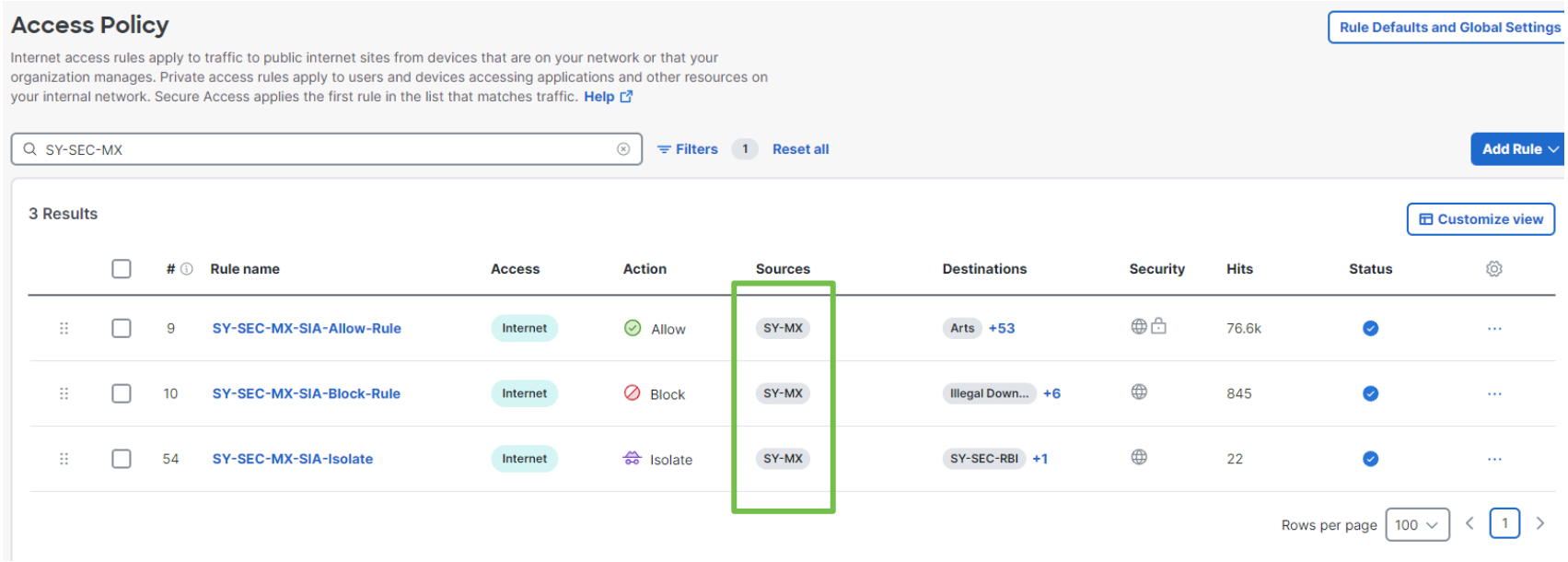
Secure Access



If the Tunnel Status is Active, the tunnel status is normal from the Secure Access side.

Setup Access Policy For Internet Access

Secure Access



Verify Reporting

Secure Access

12 Total Viewing activity from Apr 9, 2024 5:01 PM to Apr 10, 2024 5:01 PM Page: 1

	Rule Identity	Destination	Destination IP	Internal IP	External IP	Action	Categories	Resc
0×120×0	SY-MX	https://acronis-detection-test.com/acronis-test-file-macOS	16.24.40.177	10.110.120.1		Allowed — Isolated	Uncategorized	
0×120×0	SY-MX	https://acronis-detection-test.com/acronis-test-file-macOS	16.24.40.177	10.110.120.1		Allowed — Isolated	Uncategorized	
0×120×0	SY-MX	https://acronis-detection-test.com/acronis-test-file.exe	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0×120×0	SY-MX	https://acronis-detection-test.com/acronis-test-file.exe	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0×120×0	SY-MX	http://thegurdian.com/	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0×120×0	SY-MX	http://thegurdian.com/	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	

8 Total Viewing activity from Apr 9, 2024 5:01 PM to Apr 10, 2024 5:01 PM Page: 1 Results per page: 50 1 - 8 of 8

stination	Destination IP	Internal IP	External IP	Action	Categories
https://www.grc.com/files/LeakTest.exe	4.79.142.202	10.110.120.1		Blocked — Cisco AMP Disposition is Malicious (PUA.Win.Trojan.Leaktest::1201)	**Malware,** Software/Technology, Cc
https://filestore.fortinet.com/fortiguard/test-files/ml/ai_sample1	154.52.16.195	10.110.120.1		Blocked — Cisco AMP Disposition is Malicious (W32.Auto:7057e3.in03.Talos)	**Malware,** Computer Security
https://filegen.fortinet.com/v1/sandbox-file	154.52.16.216	10.110.120.1		Blocked — Antivirus Disposition is Malicious (Dropped:Trojan.Eicartest.G)	**Malware,** Computer Security
https://wildfire.paloaltonetworks.com/publicapi/test/macos	35.247.145.23	10.110.120.1		Blocked — Antivirus Disposition is Malicious (OSX/Agent.AGA)	**Malware,** Computer Security
http://malware.wicar.org/data/ms09_072_style_object.html	208.94.116.24	10.110.120.1		Blocked — Antivirus Disposition is Malicious (JS:Exploit.JS.Agent.LW)	**Malware,** Software/Technology, Po
http://malware.wicar.org/data/js_crypto_miner.html	208.94.116.24	10.110.120.1		Blocked — Antivirus Disposition is Malicious (JS/Cryptominer.G4)	**Malware,** Software/Technology, Po
https://didierstevens.com/files/data/pdf-doc-vba-eicar-dropper.zip	96.126.103.19	10.110.120.1		Blocked — Potentially Unwanted Applications (Protected File)	**Malware,** Software/Technology, Cc
https://rbi.demo.checkumbrella.com/SPECIAL-REPORT.docx	54.68.212.177	10.110.120.1		Blocked — Potentially Unwanted Applications (Protected File)	**Malware,** Computer Security

Secure SWG Traffic

Method: Client Based SWG Traffic

Pre-requisites/Deployment Steps
Configure Domains/IPs to be resolved by local DNS server or bypass from the web proxy
Download the Orginfo.json file from Secure Access Dashboard
Network requirements *(if planning Roaming Module to remain "active" while on-network)*
Deploy Secure Access Root CA *(if not deployed already)*
Provision Secure Client Roaming Module & *Orginfo.json (same folder location as Umbrella)*
Define TND configuration *(if needed)*
User Visibility – User Provisioning *(Manual, AD, IdP) (optional)*
Configure Internet Access Rule to enforce required protection and access controls *(optional)*
Enable Web Security Setting (phase1: individually/ phase2: globally)
Reporting Review

SWG –Secure Client Configuration

Secure SWG Traffic

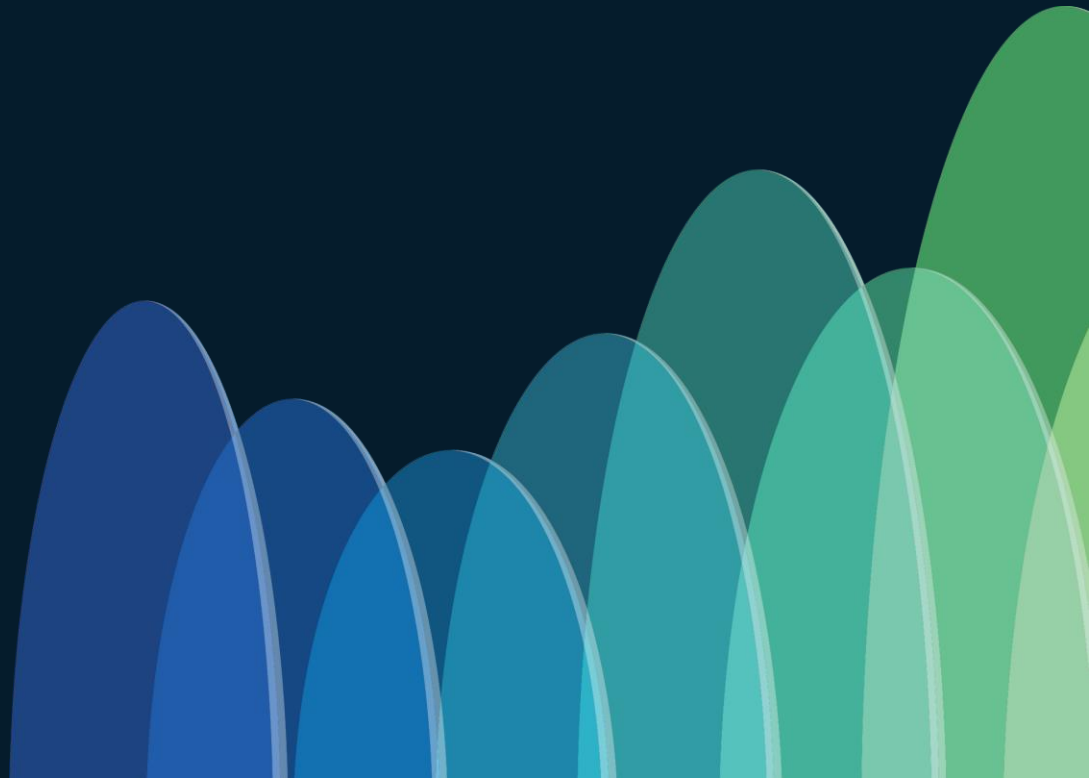
Method: Remote Access VPN Full Tunnel

Pre-requisites/Deployment Steps
User Provisioning *(Manual, AD, IdP)*
Deploy Secure Access Root CA *(if not deployed already)*
Configure Endpoint Posture Profile *(optional)*
Configure RA VPN Settings • Configure DNS Servers • IP Pool dedicated for RA VPN
Configure RA VPN Profile • Configure General Settings • Define Authentication Method *(SAML|Cert|MultiCert|SAML+Cert|MultiCert)* • Define Traffic Steering • Define Endpoint Settings
Provision the Secure Client VPN Module & .xml profile
Reporting Review
Configure Internet Access Rule to enforce required protection and access controls *(optional)*

SWG -Secure Client with Full Tunnel

cisco Live!

Advanced Feature



SIA–Advanced Features

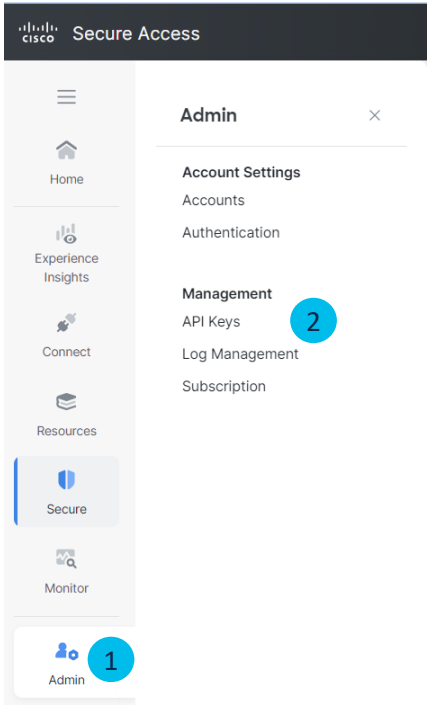
- RBI
- DLP
- DEM
- Block Page Customization
- Dispute Category

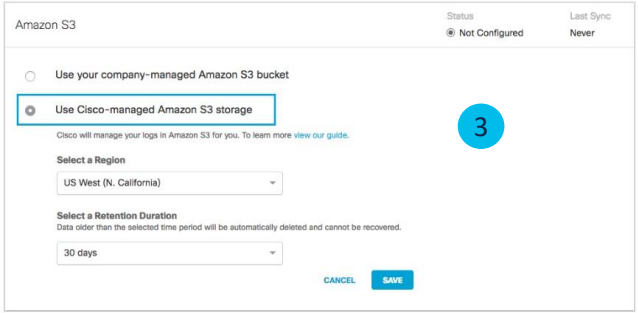
Cisco Secure Access SIEM Integration

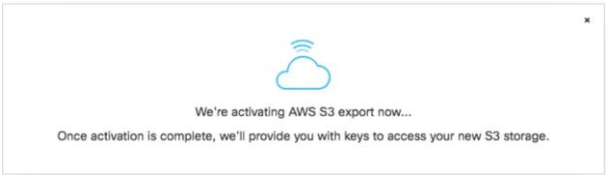
Splunk Enterprise Security

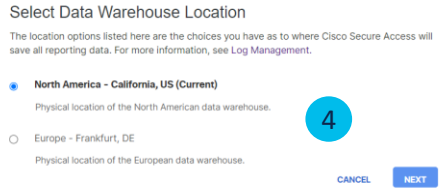
cisco Live!

Manage Event and Audit Logs

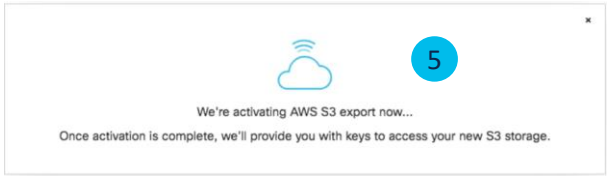


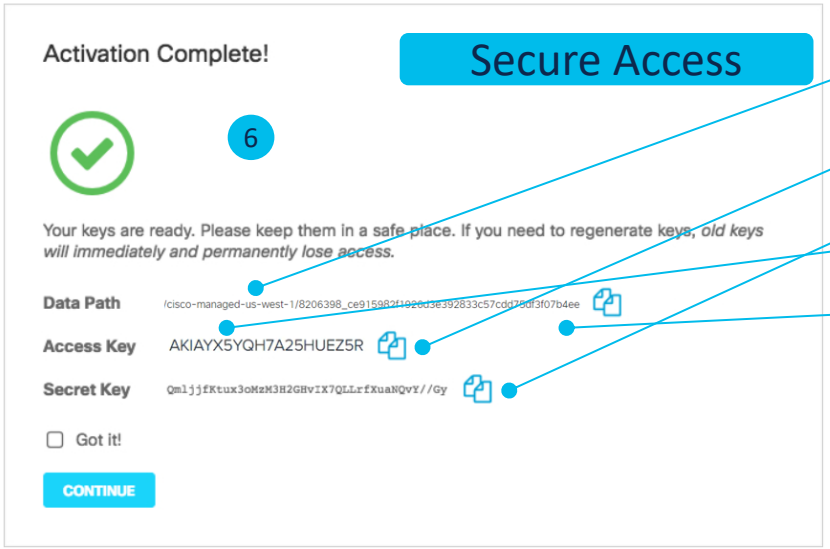




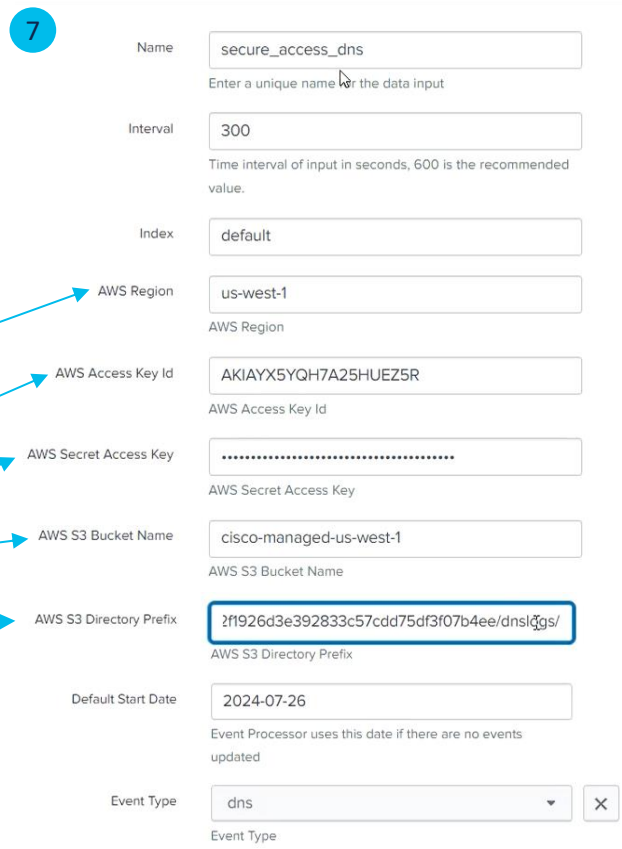


SIEM Integration

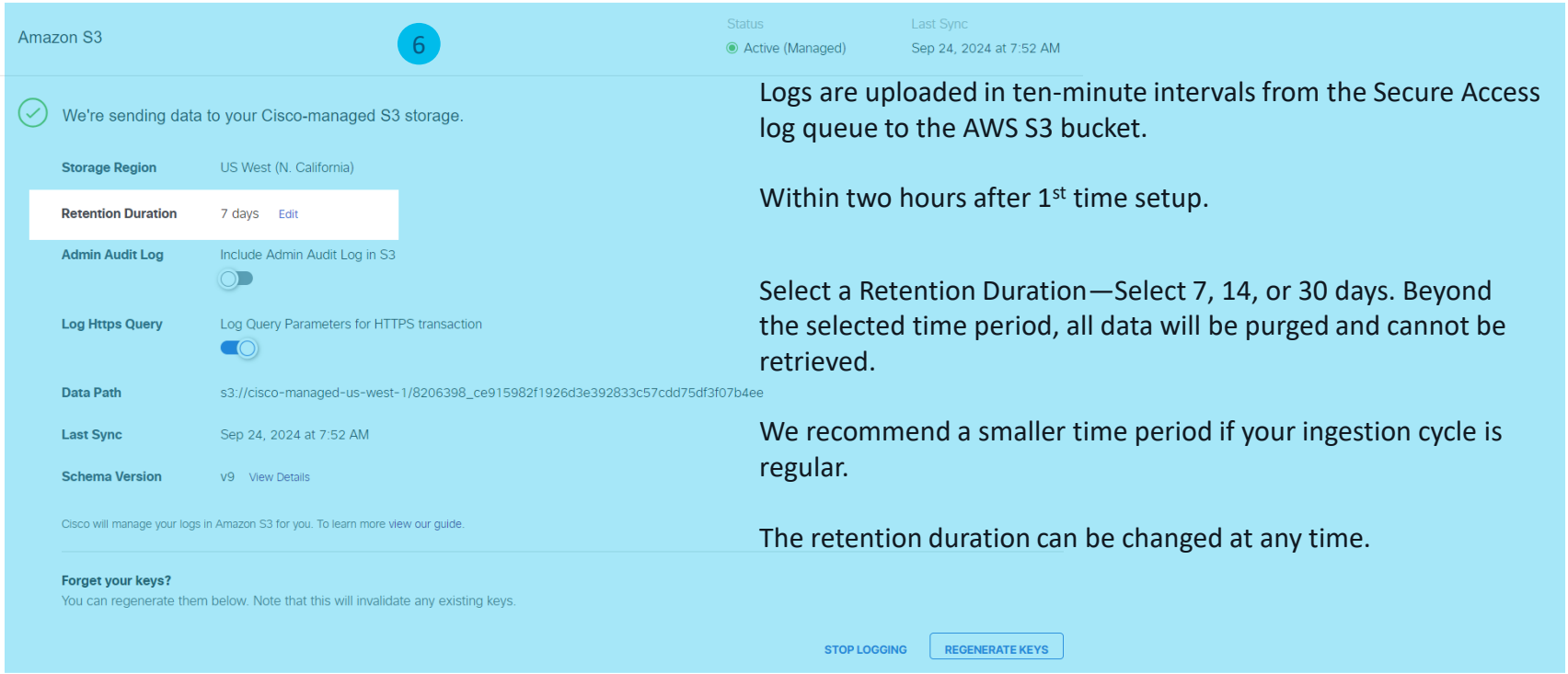




Splunk App



Log Retention Duration



Logs are uploaded in ten-minute intervals from the Secure Access log queue to the AWS S3 bucket.

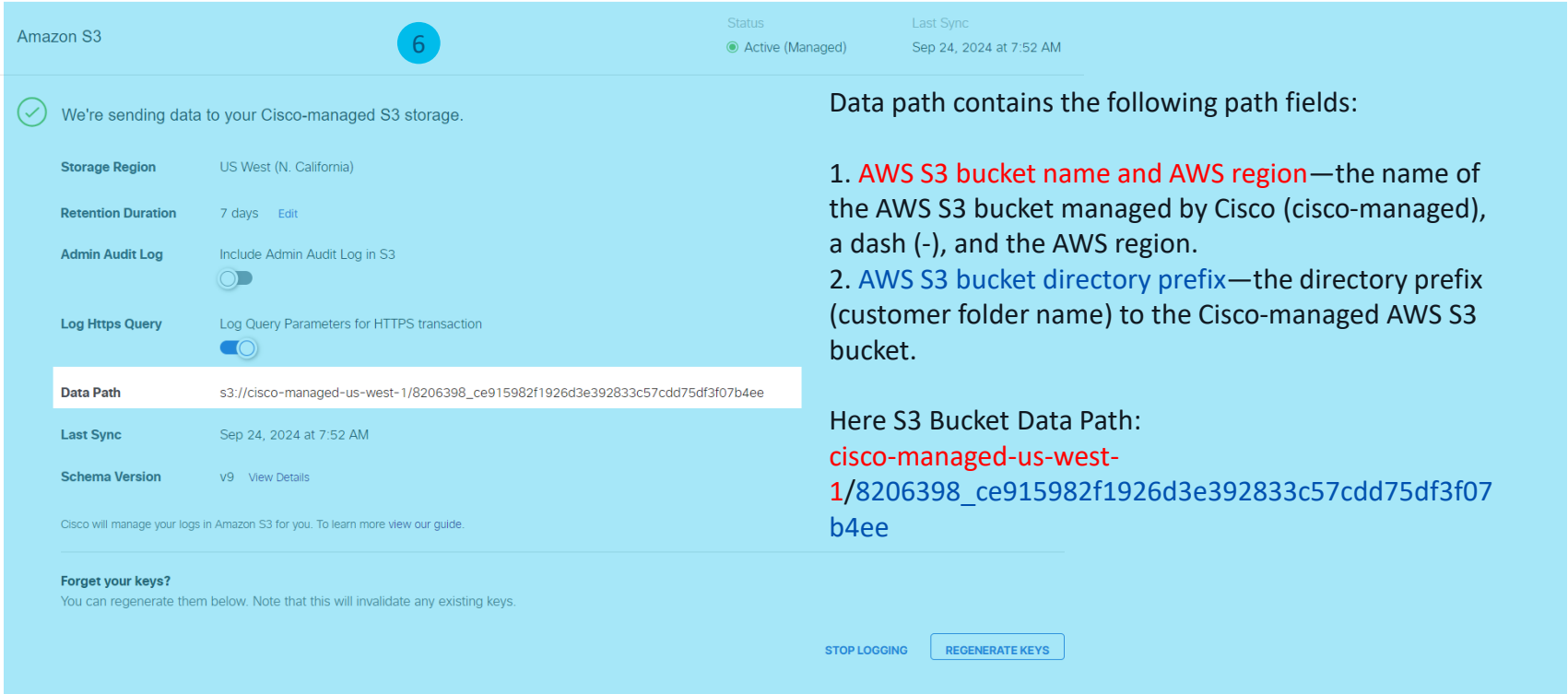
Within two hours after 1st time setup.

Select a Retention Duration—Select 7, 14, or 30 days. Beyond the selected time period, all data will be purged and cannot be retrieved.

We recommend a smaller time period if your ingestion cycle is regular.

The retention duration can be changed at any time.

S3 Bucket Data Path

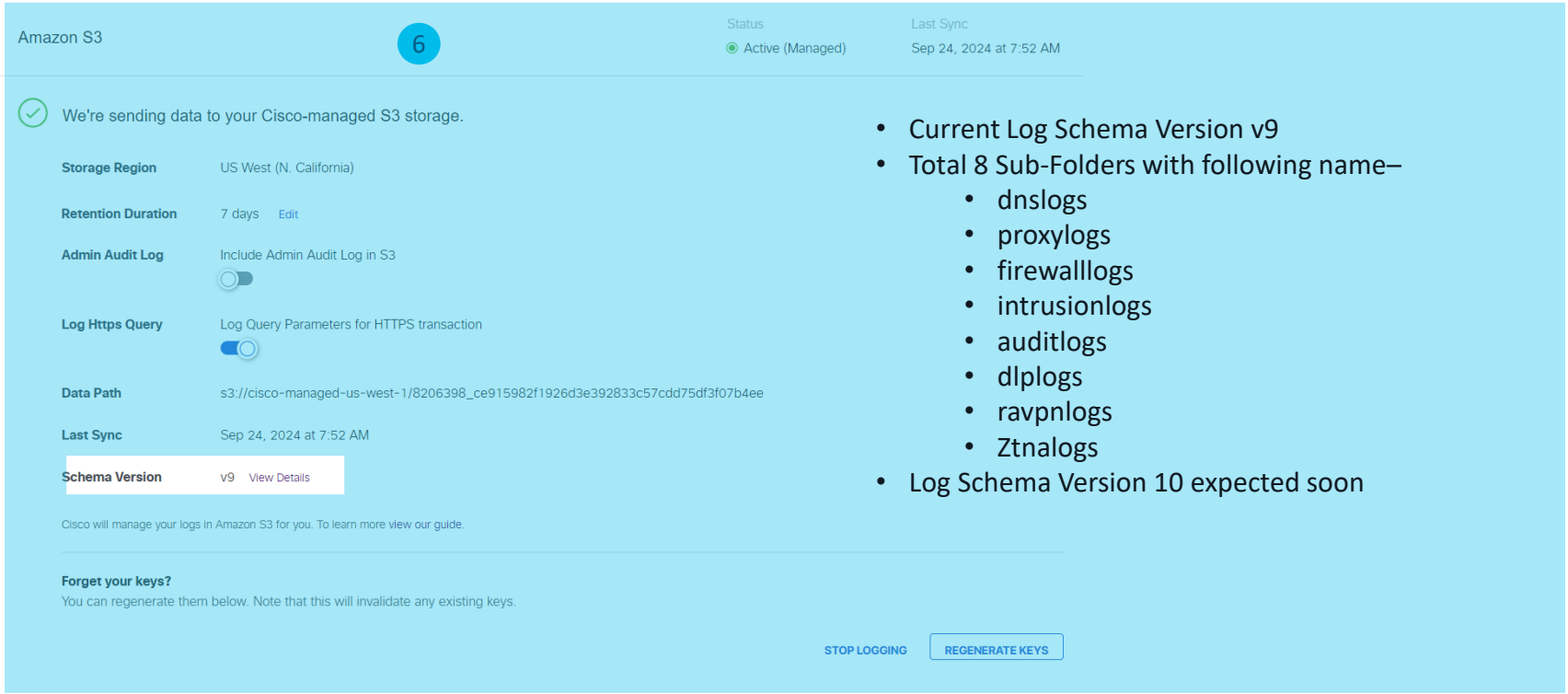


Data path contains the following path fields:

1. AWS S3 bucket name and AWS region—the name of the AWS S3 bucket managed by Cisco (cisco-managed), a dash (-), and the AWS region.
2. AWS S3 bucket directory prefix—the directory prefix (customer folder name) to the Cisco-managed AWS S3 bucket.

Here S3 Bucket Data Path:
cisco-managed-us-west-1/8206398_ce915982f1926d3e392833c57cdd75df3f07b4ee

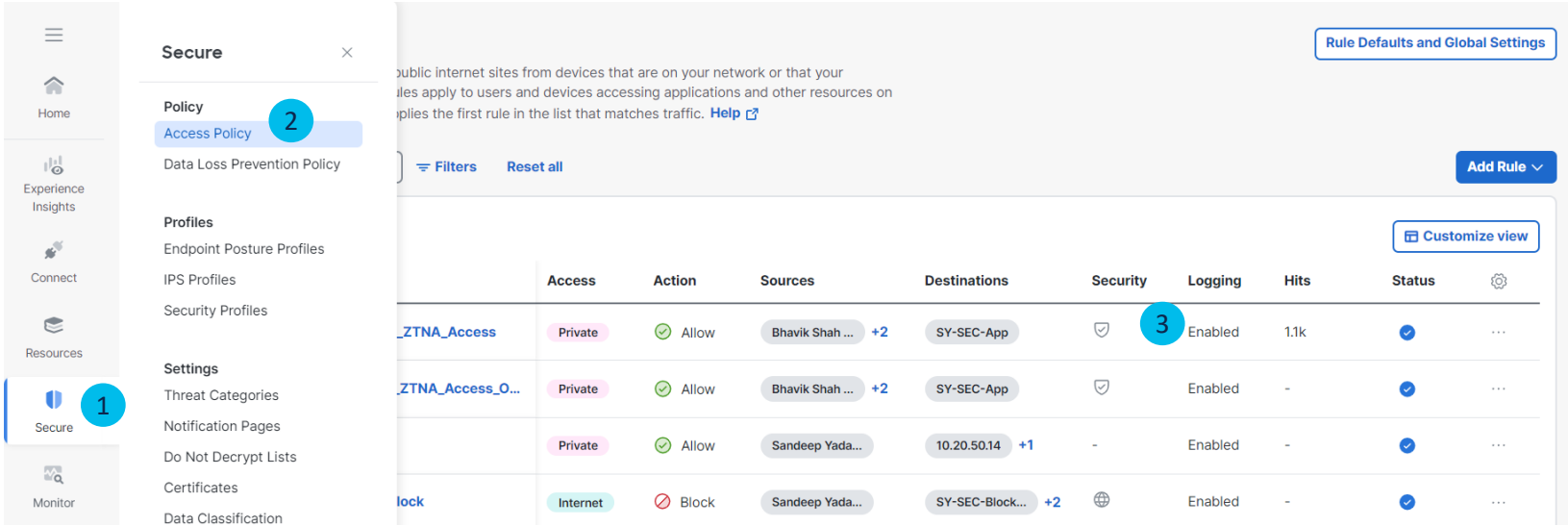
Log Schema Version



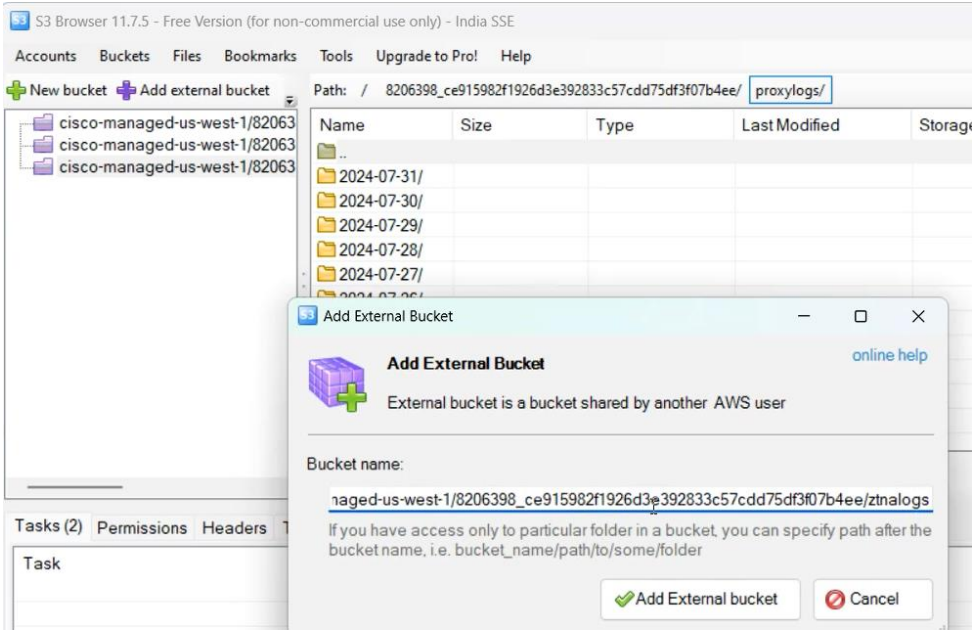
- Current Log Schema Version v9
- Total 8 Sub-Folders with following name–
  - dnslogs
  - proxylogs
  - firewalllogs
  - intrusionlogs
  - auditlogs
  - dlplogs
  - ravpnlogs
  - Ztnalogs
- Log Schema Version 10 expected soon

https://docs.sse.cisco.com/sse-user-guide/docs/log-formats-and-versioning

Enable Access Rule For Logging



Verify Logs are uploaded to S3 bucket



You can use S3 Browser Application to verify that event logs are uploaded to the S3 bucket and download it offline..

In this example adding ztnalogs folder.

Summary: Building Blocks Discussed

Internet Access

Cyber protection
Data protection (DLP/CASB)
Local internet breakouts (O365/SD-WAN)

Secure Internet and SaaS access

User to Internet

Secure Private App Access

User to Private App

Private Access

Remote app access without VPN
Zero trust from office to data center
B2B customer app access

Identity Threat Detection and Response

Performance scores by user, app, location
Detect and resolve Identity Threat issues

Identity Protection

Identity Posture

Secure Endpoint

User Device and Email Protection

Attack Vector Protection

Endpoint Protection via. EDR/EPP
Email Protection via. Email Threat Defense

Extended Detection and Response (XDR)

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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:
bhavsha2@cisco.com | syadav2@cisco.com

Thank you


cisco Live!
GO BEYOND
#CiscoLiveAPJC