

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 *Live!*

#CiscoLiveAPJC



Cisco Webex App

Questions?

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

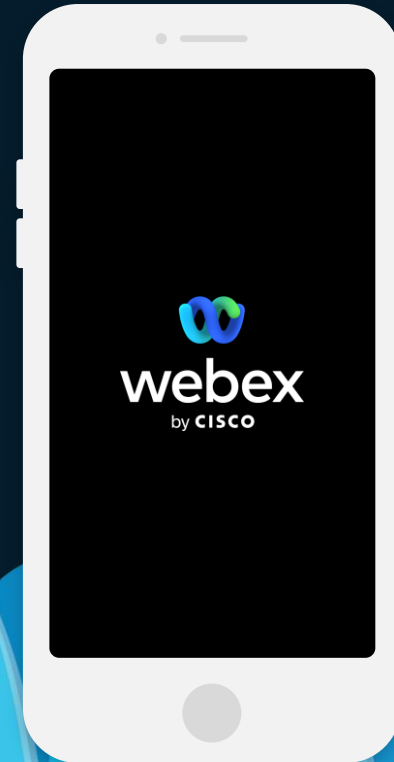
How

- 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 November 15, 2024.



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



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

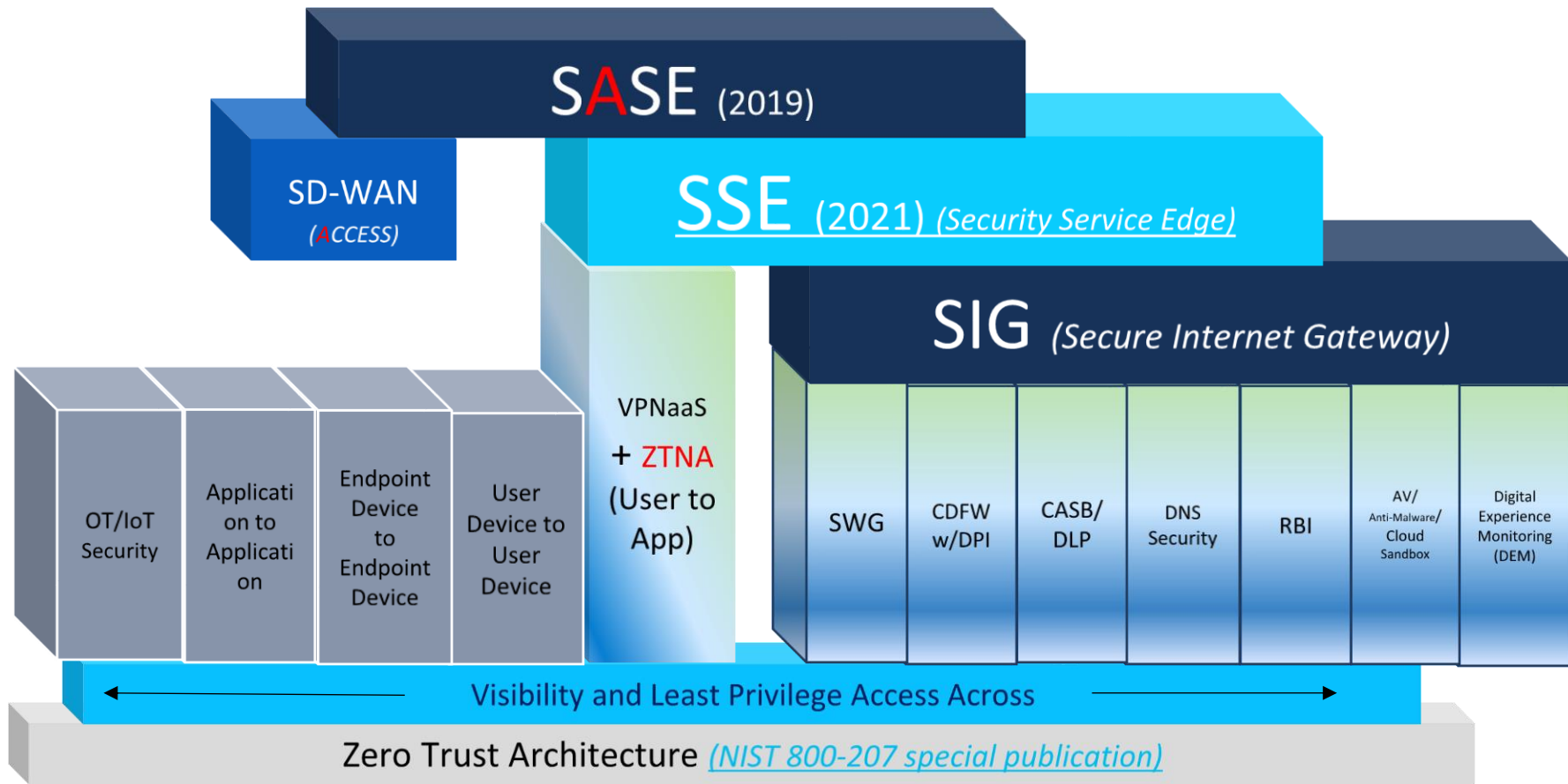


Agenda

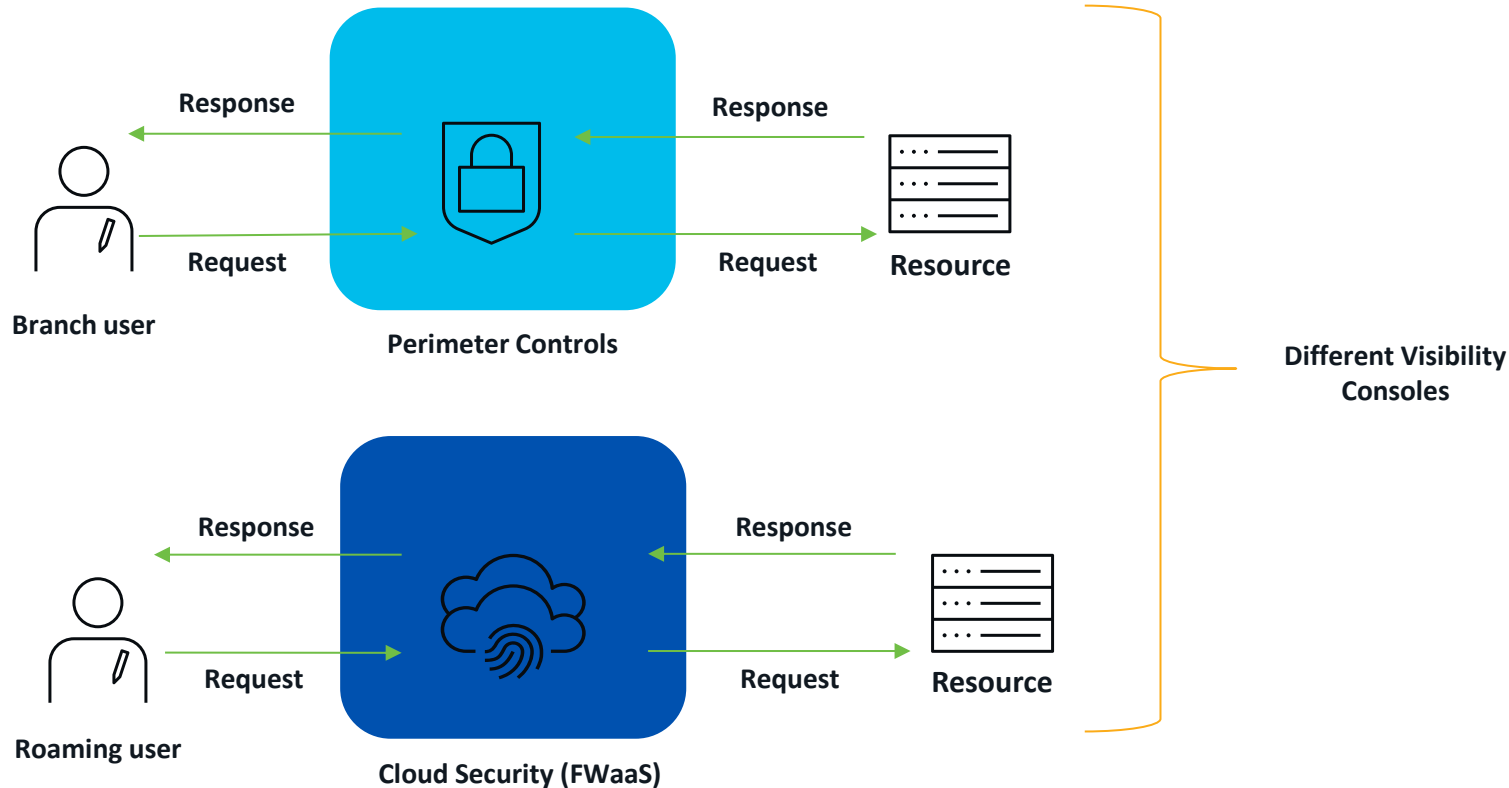
- Introduction – Progressive Buzz
- Audience Poll
- Deployment Plans For Secure Internet Access
- Deployment Plans For Secure Private Access
- Advanced Feature
- Conclusion

Understanding the History

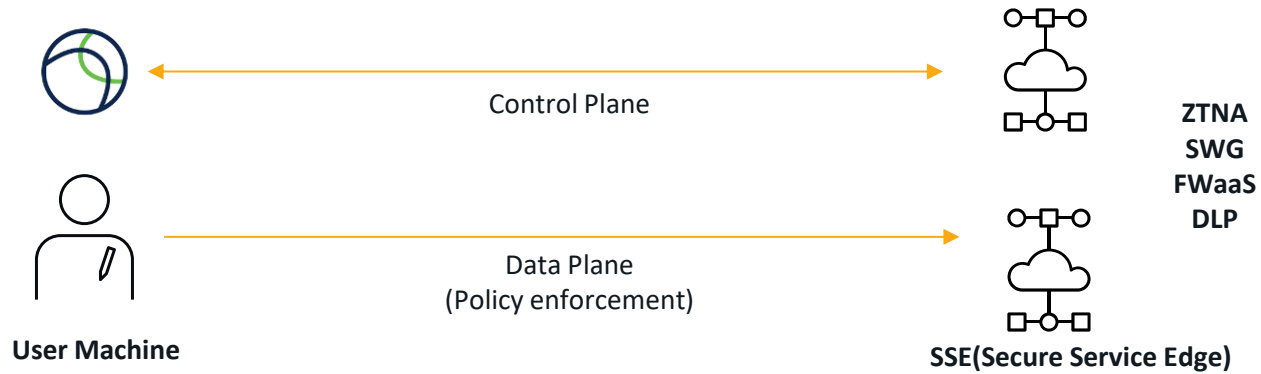




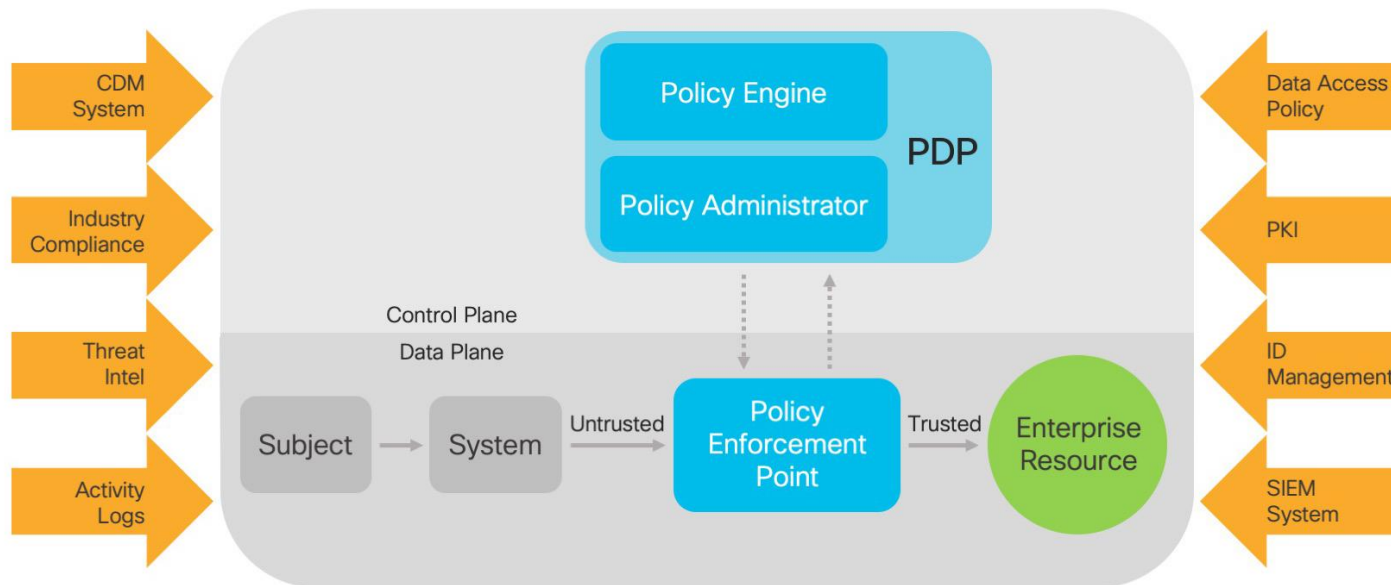
Why Security Service Edge?



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)

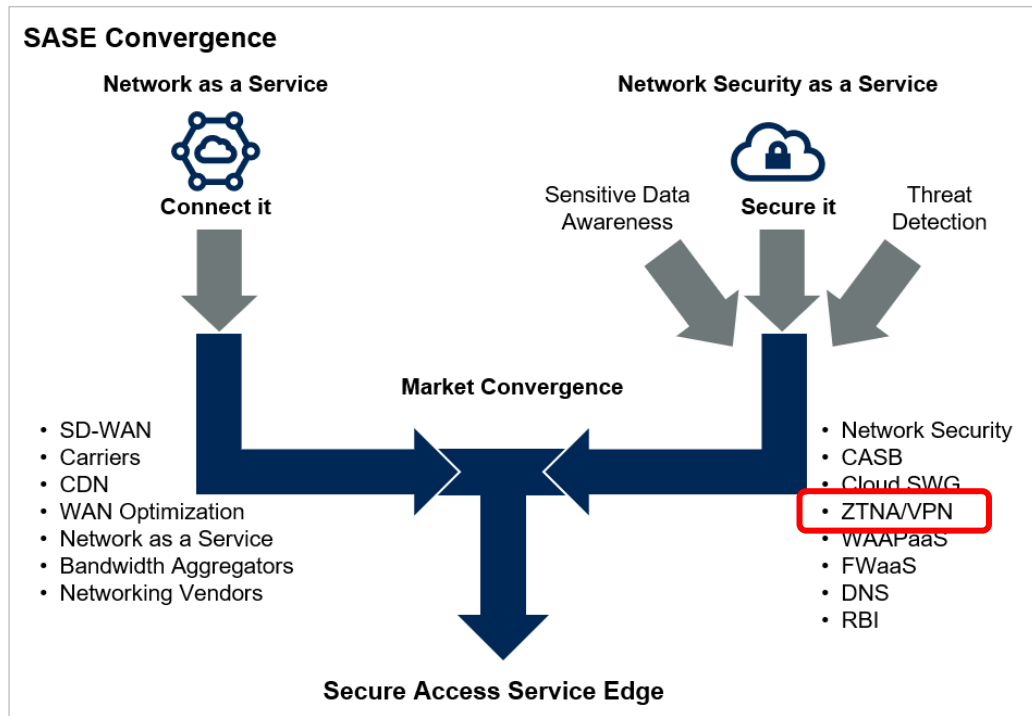
Convergence of networking and security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

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



Market Guide for Zero Trust Network Access

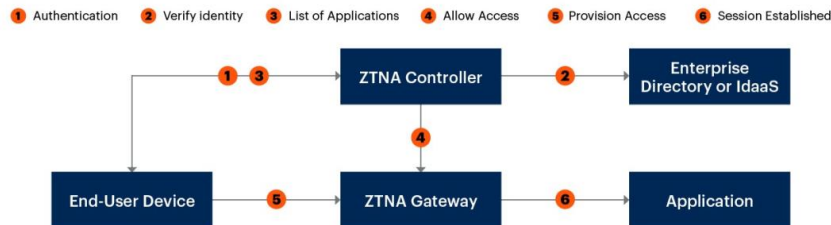
Published 8 June 2020 - ID G00726817 - 27 min read

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

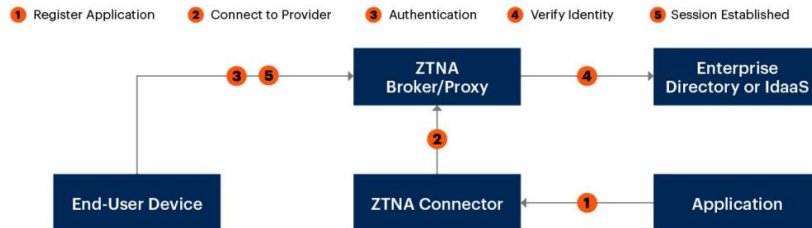
Conceptual Model of Endpoint-Initiated ZTNA



Source: Gartner
726817_C

Figure 2: Conceptual Model of Service-Initiated ZTNA

Conceptual Model of Service-Initiated ZTNA



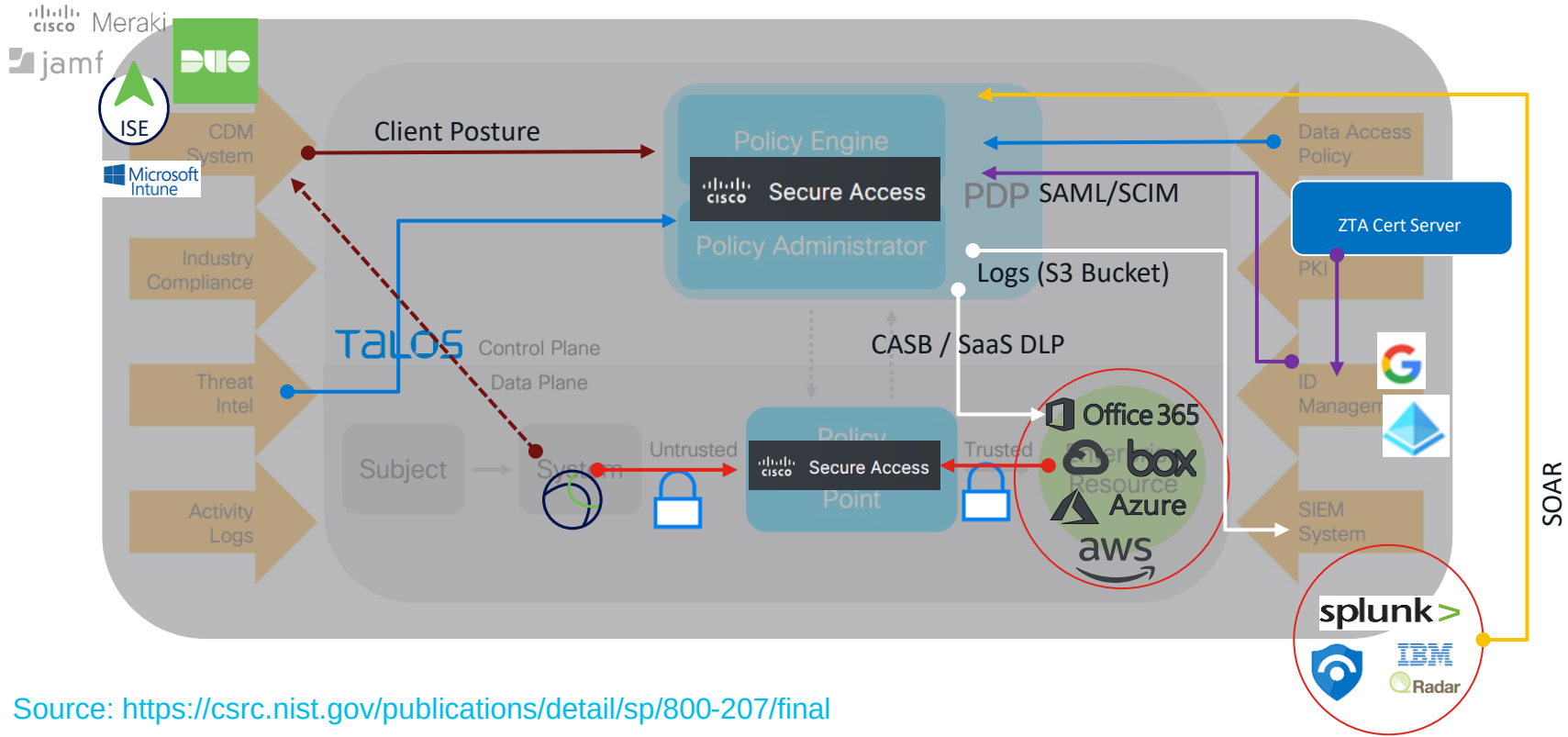
Source: Gartner
726817_C

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

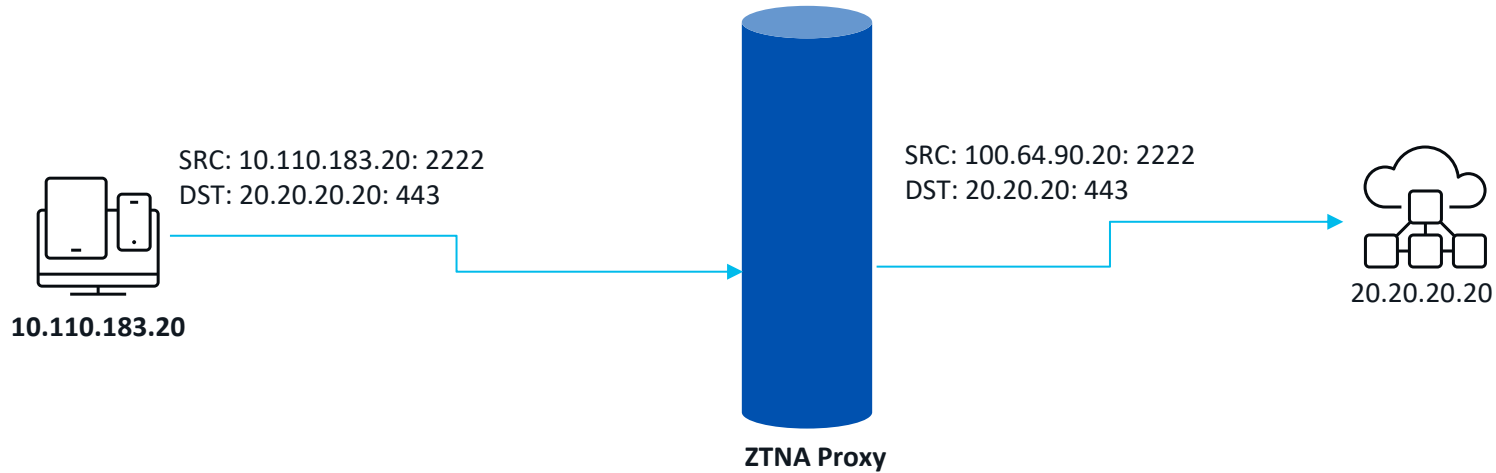
NIST 800-207: Zero Trust Architecture



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

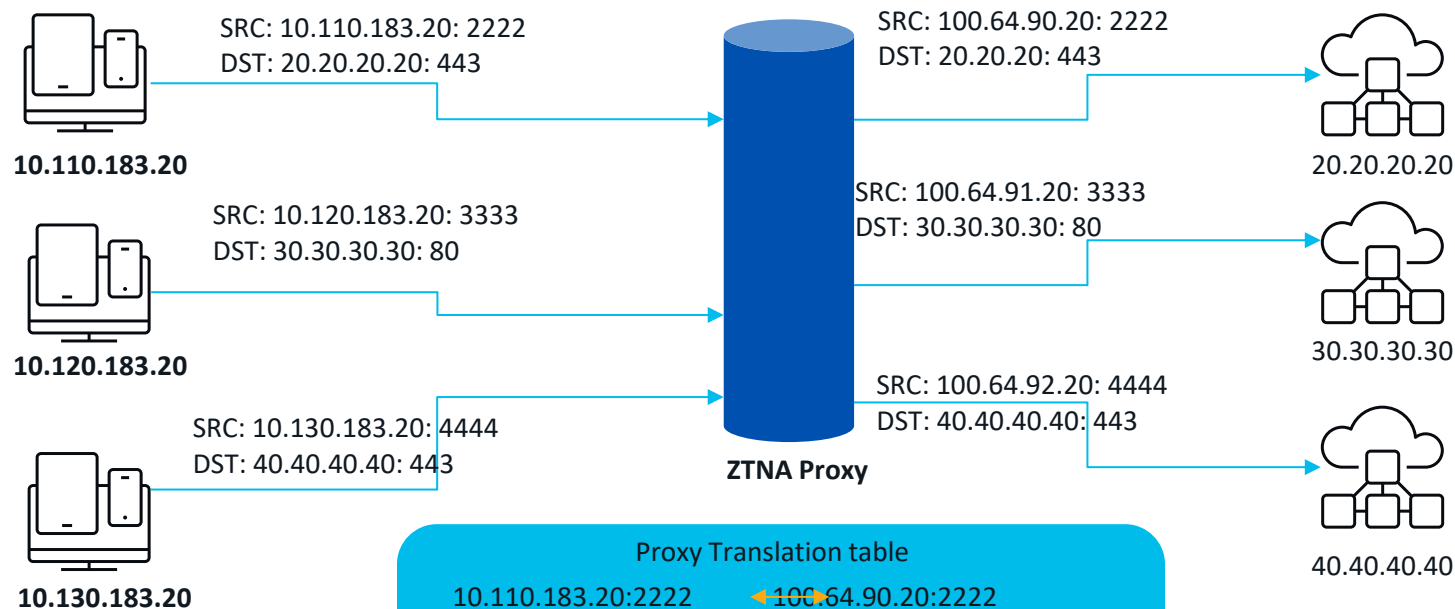


Proxy Translation table

10.110.183.20:2222 ← 100.64.90.20:2222

Demystifying ZTNA

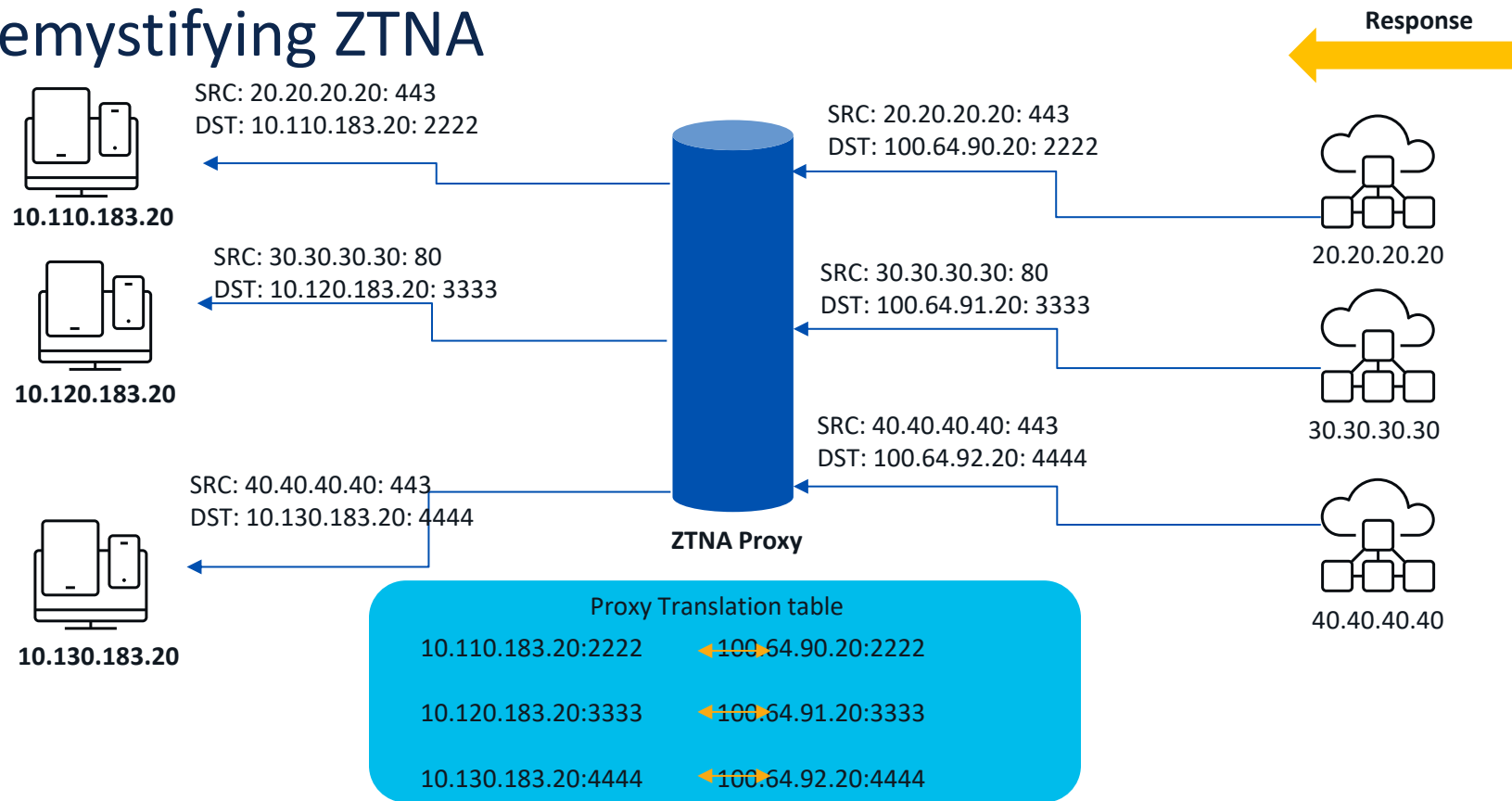
Request



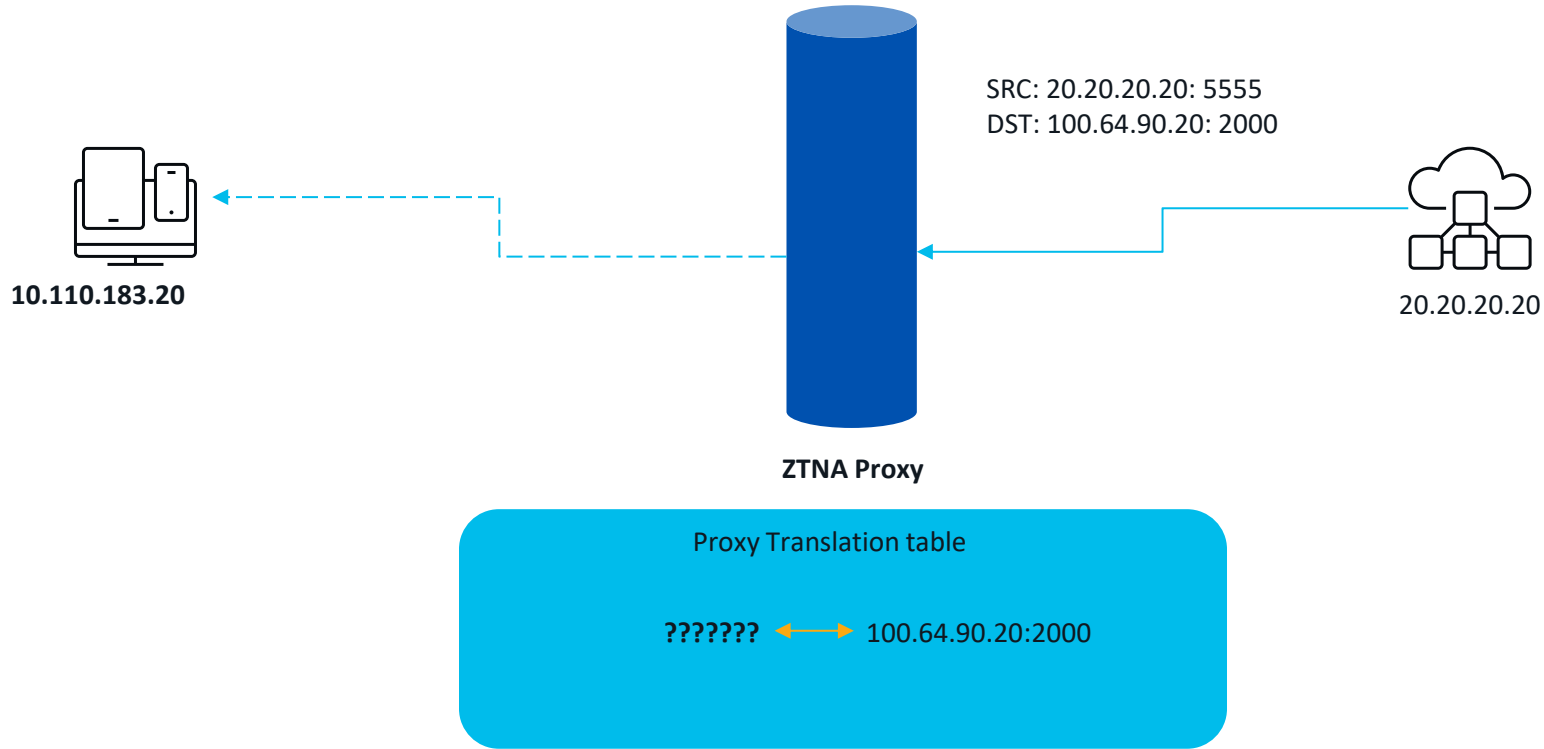
Proxy Translation table

10.110.183.20:2222	← 100.64.90.20:2222
10.120.183.20:3333	← 100.64.91.20:3333
10.130.183.20:4444	← 100.64.92.20:4444

Demystifying ZTNA

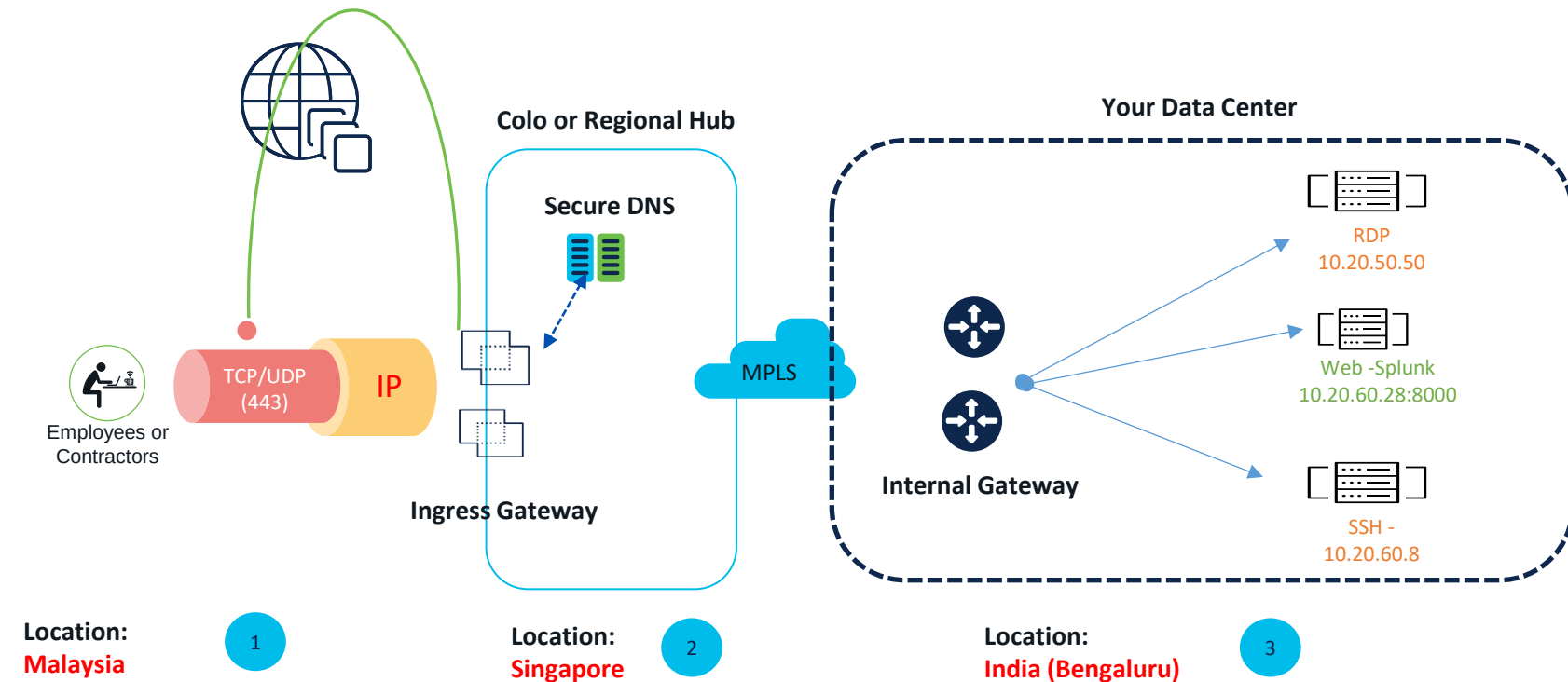


Demystifying ZTNA



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

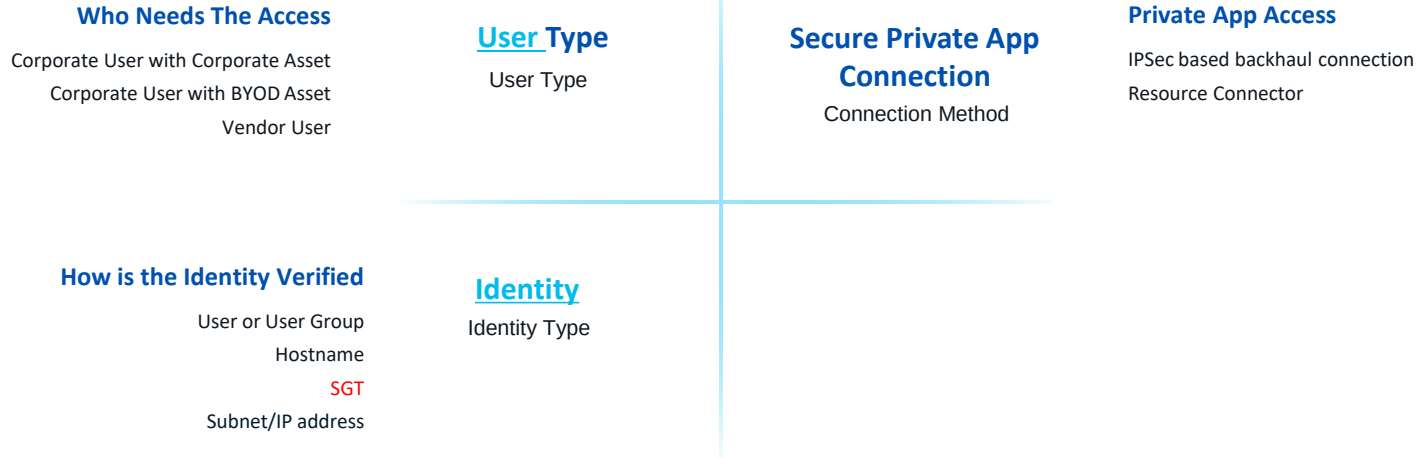
How is the Identity Verified

User or User Group
Hostname
SGT
Subnet/IP address

Identity

Identity Type

Building Blocks For Private Access



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

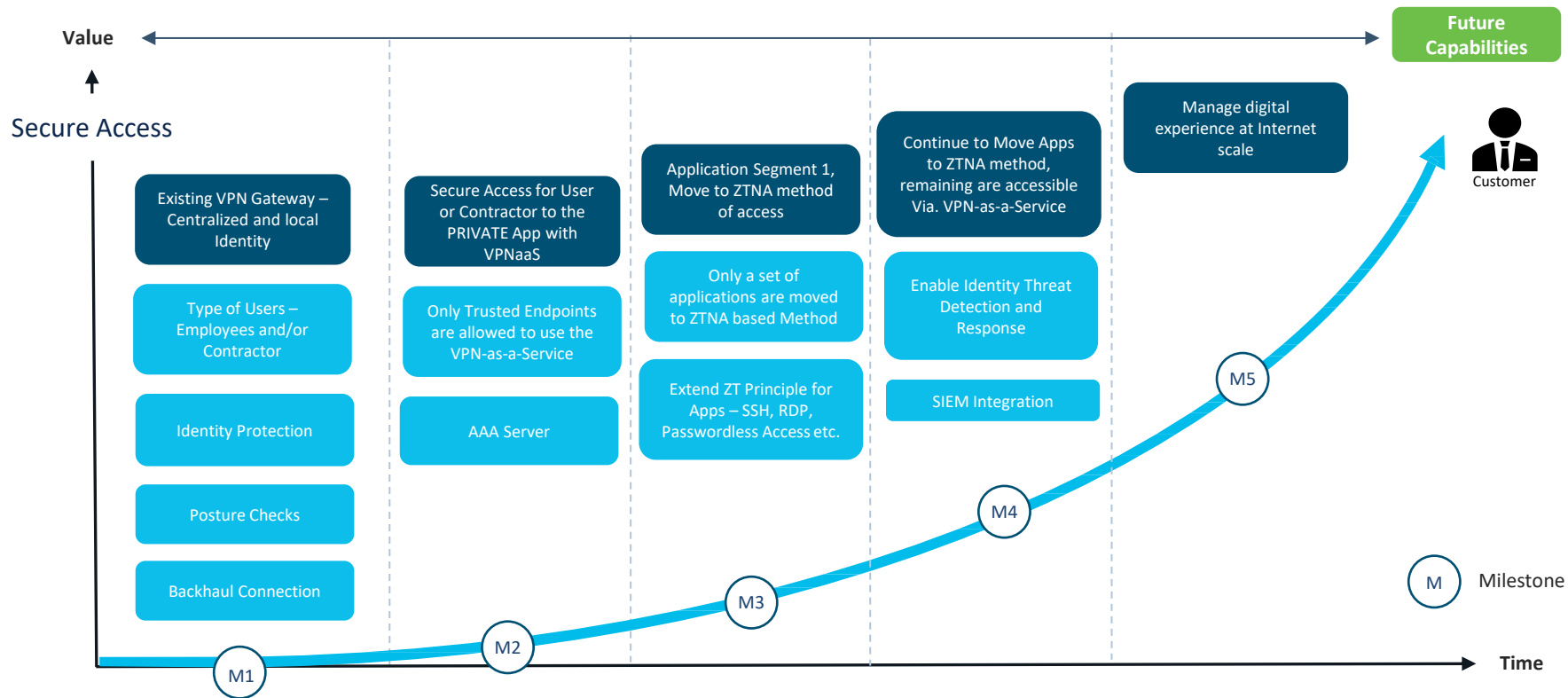
Using Remote Access VPN method
Using ZTNA Agent Method
Using Browser (Clientless)Method

Deployment

Secure Private Access (Branch / DC / Roaming User)

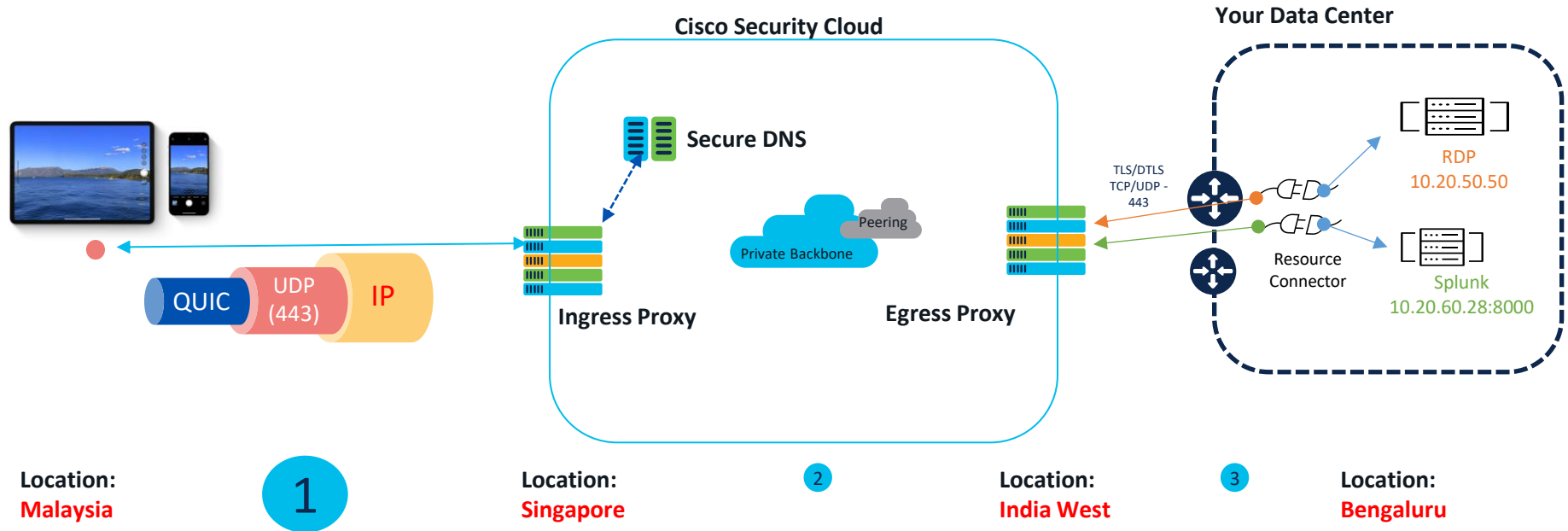
- RA VPN (Secure Client – VPN Module)
- Client-Based ZTNA (Secure Client – ZTNA Module)
- ZTNA Clientless (Browser-Based)
- Branch and DC (IPsec Tunnel and/or Resource connector)

Phased Execution - VPN -> VPNaaS -> ZTNA



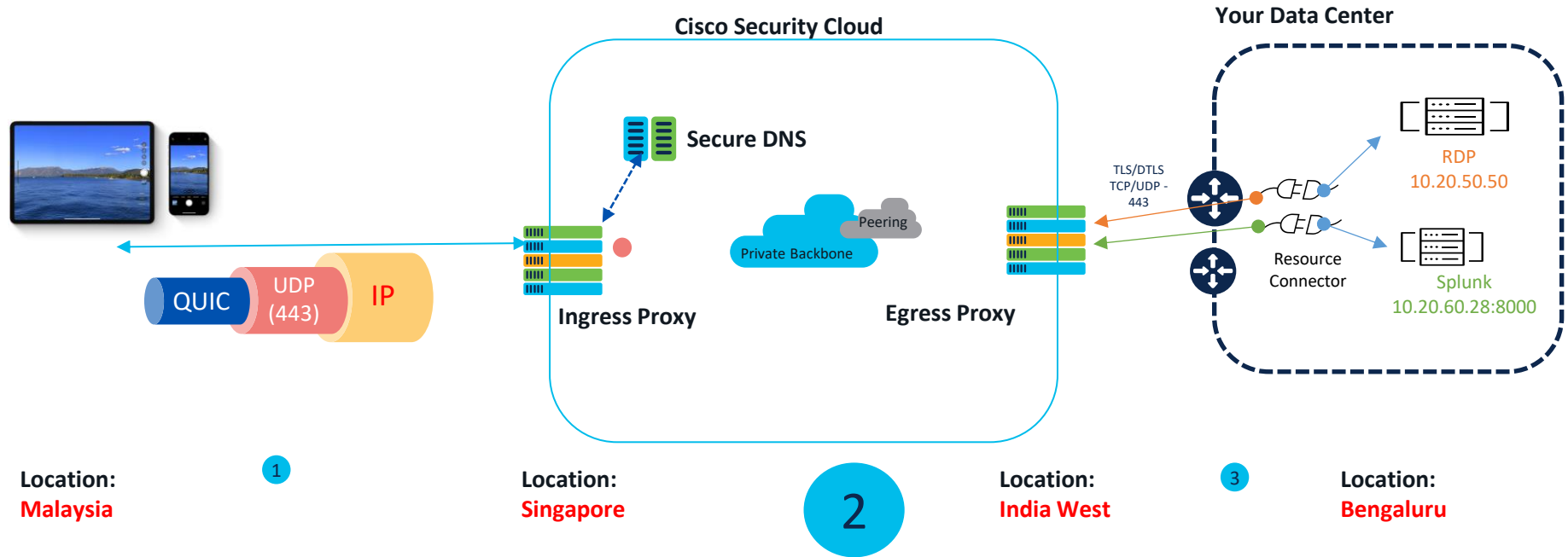
Lab Topology

ZTNA in Secure Private Access-Cisco Secure Access



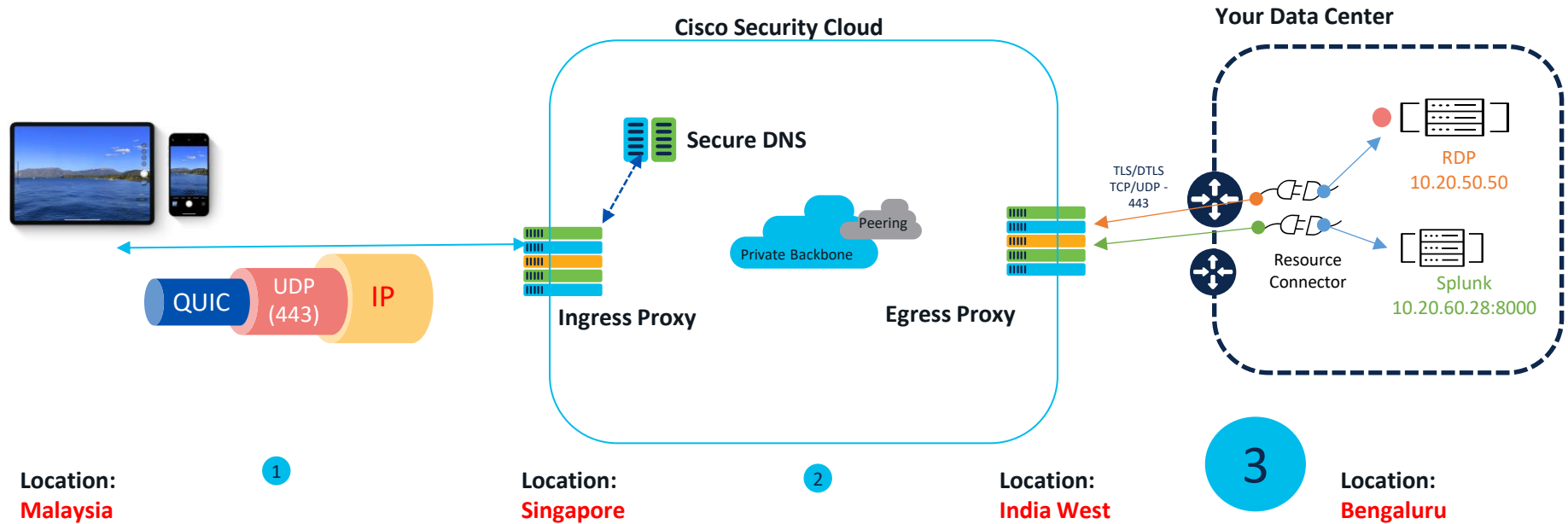
Lab Topology

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 (<i>Manual, AD, IdP</i>)
Deploy Secure Access Root CA (<i>if not deployed already</i>)
Configure Endpoint Posture Profile (<i>if not deployed already</i>)
Configure RA VPN Settings • Configure DNS Servers (<i>*If local DNS server, create Private Access Resource and Private Access Policy to allow access to it</i>) • IP Pool dedicated for RA VPN
Configure RA VPN Profile • Configure General Settings (<i>Endpoint Posture Profile *optional</i>) • Define Authentication Method (<i>SAML Cert MultiCert SAML+Cert</i>) • 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

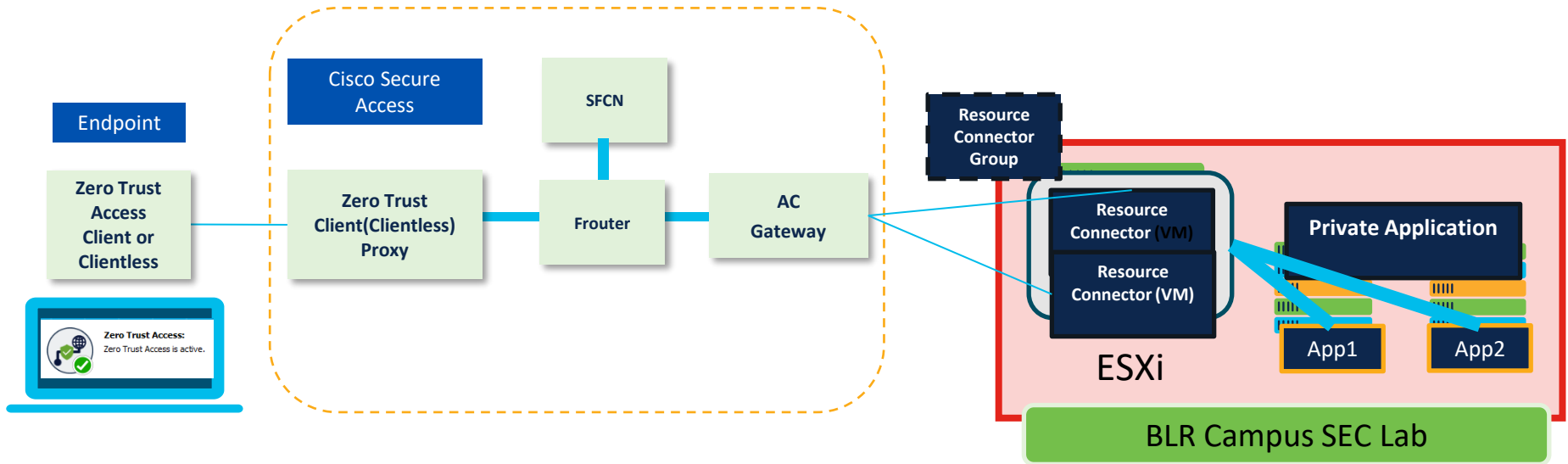
Reporting Review

User Access

Connection Method – Clientless ZTNA

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

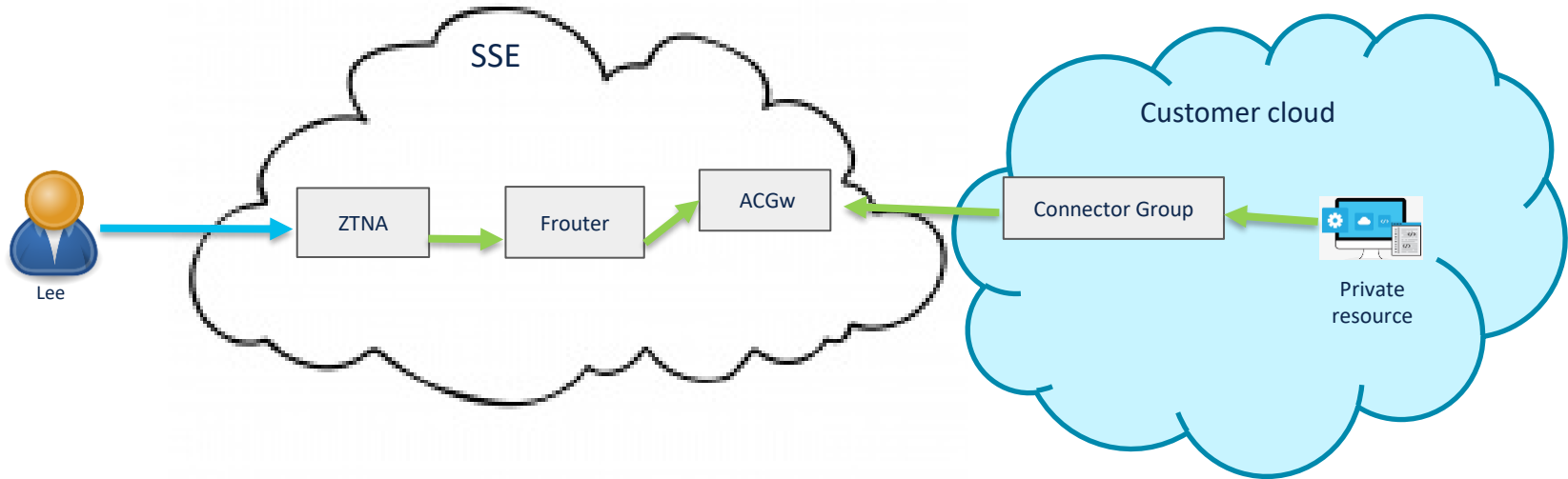
Topology



Resource Connector and No IPSec

Scenario:

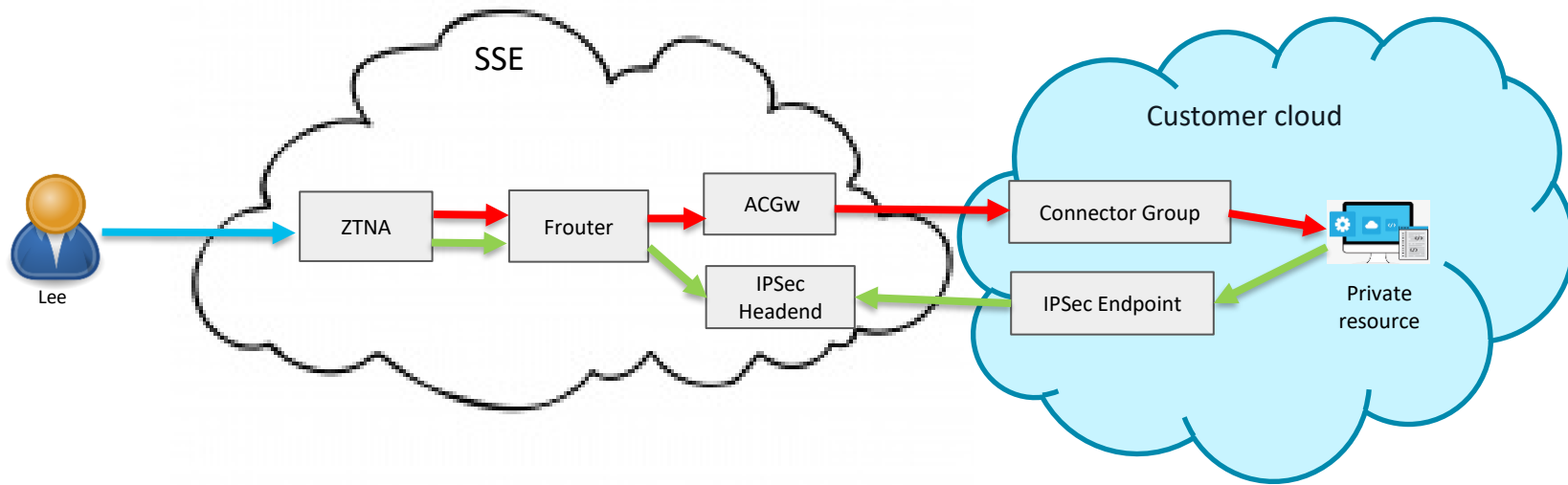
- Resource Connector is preferred path
- No IPSec Tunnel possible in SEC due to InfoSec Compliance.



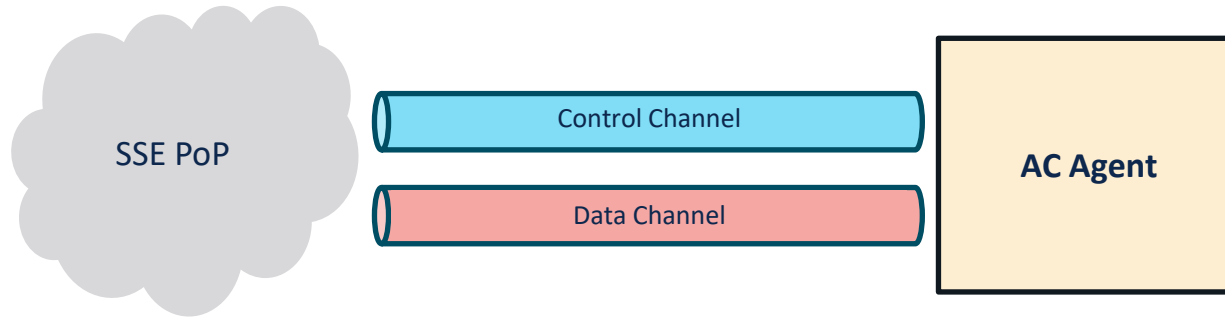
Failover between Resource Connector and IPSec

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

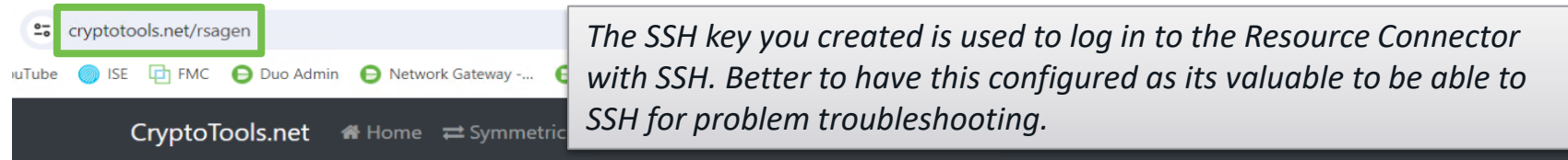
Item No.	Operational Locations	Implementation details
0	Any device	(Optional) Create an SSH key
1	Secure Access console	Defining Connector Groups
2	Secure Access console	Download the resource connector image
3	VMware ESXi – 7.0.3	Deploy a resource connector
4	Secure Access console	Add a resource connector 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



The screenshot shows the website cryptotools.net/rsagen. The page title is "RSA Key Generator". Below the title, there is a text box that says: "You may generate an RSA private key with the help of this tool. Additionally, it will display the public key of a generated or pasted private key." There is a form with a "Key Length" dropdown menu set to "4096" and a "Generate key pair" button. Below the form, there are two text areas labeled "Private key" and "Public key".

The SSH key you created is used to log in to the Resource Connector with SSH. Better to have this configured as its valuable to be able to SSH for problem troubleshooting.

RSA Key Generator

You may generate an RSA private key with the help of this tool. Additionally, it will display the public key of a generated or pasted private key.

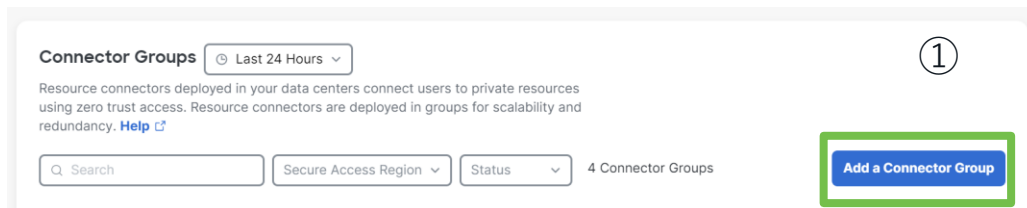
Key Length 4096 Generate key pair	
Private key	Public key

Private key
Public key

The generated SSH key will be used in a later step. At this time, please create an SSH key

1. Define connector groups

Secure access
console

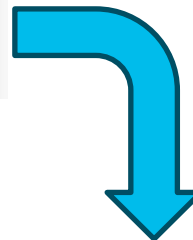


Connector Groups Last 24 Hours ▾

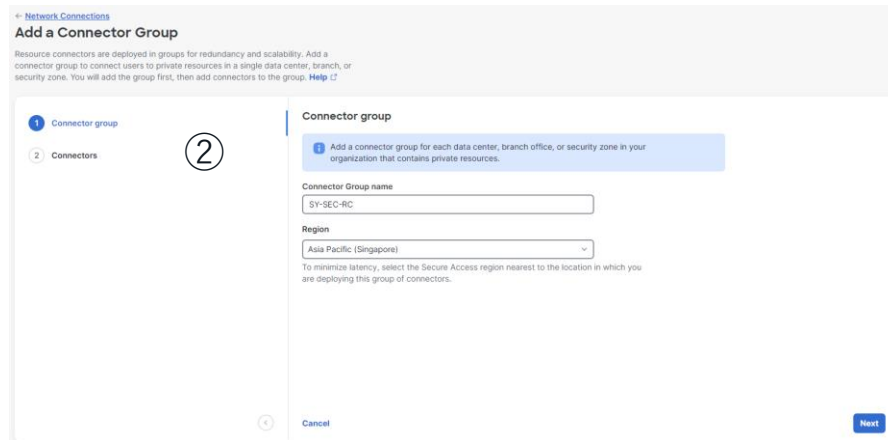
Resource connectors deployed in your data centers connect users to private resources using zero trust access. Resource connectors are deployed in groups for scalability and redundancy. [Help](#)

Q Search Secure Access Region ▾ Status ▾ 4 Connector Groups

Add a Connector Group



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.)



Network Connections

Add a Connector Group

Resource connectors are deployed in groups for redundancy and scalability. Add a connector group to connect users to private resources in a single data center, branch, or security zone. You will add the group first, then add connectors to the group. [Help](#)

Connector group

1 Add a connector group for each data center, branch office, or security zone in your organization that contains private resources.

Connector Group name
SY-SEC-RC

Region
Asia Pacific (Singapore)

To minimize latency, select the Secure Access region nearest to the location in which you are deploying this group of connectors.

Cancel Next

1. Define connector groups

Secure access
console

[VMware ESXi] Select Create

Add a Connector Group

Resource connectors are deployed in groups for redundancy and scalability. Add a connector group to connect users to private resources in a single data center, branch, or security zone. You will add the group first, then add connectors to the group. [Help](#)

1 Connector group
SY-SEC-RC, Asia Pacific (Singapore)

2 Connectors

Connectors

You will deploy connector instances for this group using a resource connector image provided by Cisco. Choose a virtual environment and review the information on this page, then follow the steps on the next page. [Help](#)

Amazon Web Services

VMware ESXi

Scaling calculator

For planning purposes, estimate the maximum volume of traffic that connectors in this group must handle:



Throughput in Gbps

Estimated number of connectors to deploy in this connector group:

11 x instances (each with 2 CPU's and 4 GB RAM)

Note: This recommendation is based on 75% CPU load, includes 1 connector for redundancy, and assumes adequate network capacity.

You can deploy additional connectors at any time.

Cancel

Back

Save

2. Download the resource connector image

Next steps

Resource connectors deployed in a connector group will connect user traffic to all private resources assigned to the group. After one or more connector groups is configured, take the following steps to deploy connectors in the connector groups and assign private resources to groups. [Help](#)

Secure access
console

1 Deploy your Connectors

Create connectors using the image provided by Cisco.

 [Download Connector Image for VMware](#) 

①

- Each connector in a group must be able to connect to all of the resources assigned to the group.
- All connectors in a group must use the same virtual environment, for example AWS or VMware.
- Deploy at least two connectors in each connector group for redundancy during connector upgrades.
- The downloaded image can be used for all connector groups.
- When you create each connector, you will associate it with a connector group using the connector group's provisioning key from the table below.

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

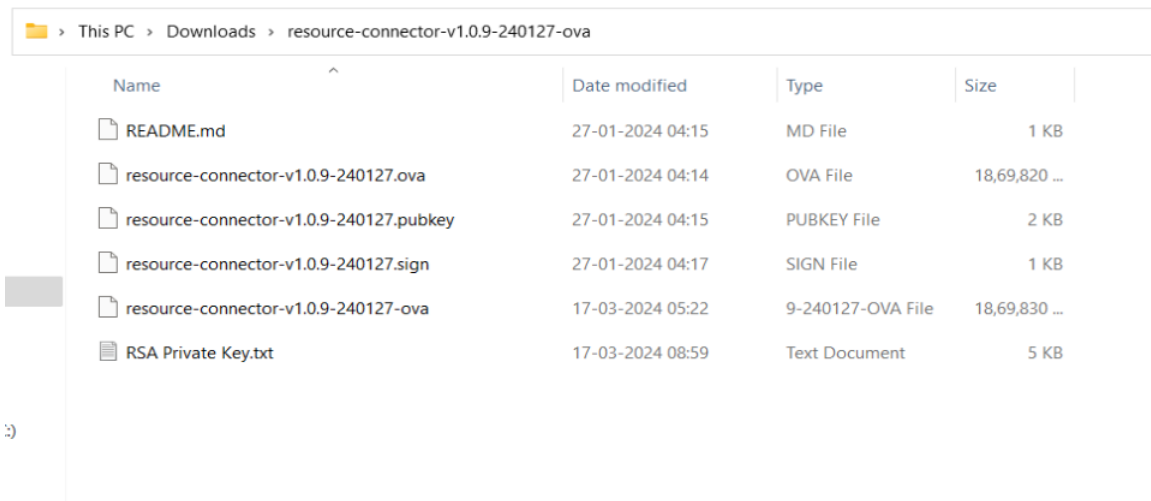
(2) You will need to enter the Provisioning Key in a later step, so copy it and keep it handy.

Connector Group	Environment	Provisioning Key	
Incedo - Testing	AWS		 Copy  Regenerate  Key expired
SECApplsInfoSecLab	VMware ESXi		 Copy  Regenerate Key expires on Apr 1, 2024 5:30 AM IST

②

2. Download the resource connector image

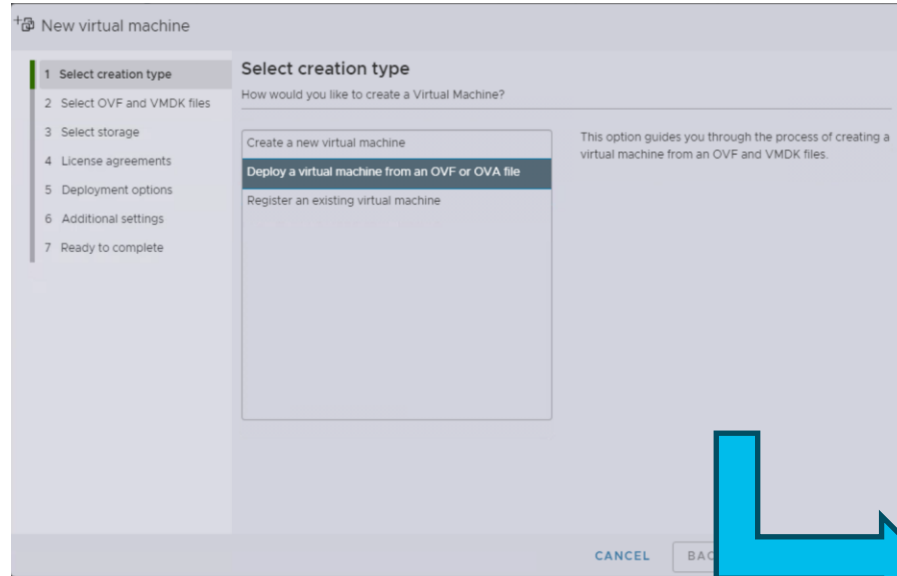
Untar the file and then use this ova file



> This PC > Downloads > resource-connector-v1.0.9-240127-ova				
Name	Date modified	Type	Size	
README.md	27-01-2024 04:15	MD File	1 KB	
resource-connector-v1.0.9-240127.ova	27-01-2024 04:14	OVA File	18,69,820 ...	
resource-connector-v1.0.9-240127.pubkey	27-01-2024 04:15	PUBKEY File	2 KB	
resource-connector-v1.0.9-240127.sign	27-01-2024 04:17	SIGN File	1 KB	
resource-connector-v1.0.9-240127-ova	17-03-2024 05:22	9-240127-OVA File	18,69,830 ...	
RSA Private Key.txt	17-03-2024 08:59	Text Document	5 KB	

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.

This PC > Downloads > resource-connector-v1.0.9-240127-ova

Name	Date modified	Type	Size
README.md	27-01-2024 04:15	MD File	1 KB
resource-connector-v1.0.9-240127.ova	27-01-2024 04:14	OVA File	18,69,820 ...
resource-connector-v1.0.9-240127.pubkey	27-01-2024 04:15	PUBKEY File	2 KB
resource-connector-v1.0.9-240127.sign	27-01-2024 04:17	SIGN File	1 KB
resource-connector-v1.0.9-240127-ova	17-03-2024 05:22	9-240127-OVA File	18,69,830 ...
RSA Private Key.txt	17-03-2024 08:59	Text Document	5 KB

3. Deploy the resource connector

VMware ESXi

New virtual machine - M_MGMT_RC2

- 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 Deployment options
- 5 Additional settings
- 6 Ready to complete

Additional settings

Additional properties for the VM

VM boot time setup

Provisioning key	NjAXyZyWODM4Yzc5NGMxNjkyNjRjMDMxOWM3Z
IP Address/Mask	10.20.50.69/24
Gateway IP Address	10.20.50.1
DNS server list	10.20.50.13
NTP server list	ntp.mango.local
SSH public key	fgzhYz8wVIMvECU18n2IoRpGK/XI1CmHIQIDAQAB
SSH public key type	

Enter the Key that you copied in the Secure Access console

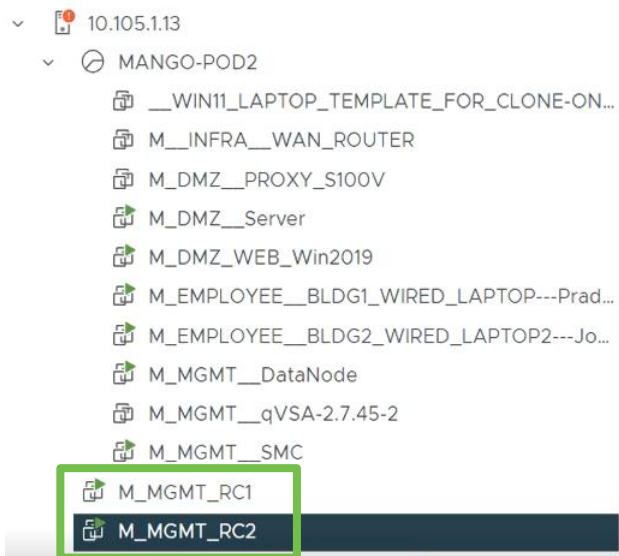
Enter any IP/Gateway/DNS/NTP Server
➤Note, It's a Private Resource connector, use RFC1918 address and make sure the private IP can reach the Private Resources/ Apps

Item 2 to 4 click next and proceed to item 5 Additional Settings.

Enter the SSH Public key contained in the id_rsa.pub obtained in step 0 (Optional)

3. Deploy the resource connector

VMware ESXi



3. “Confirm” the resource connector

Secure access
console

2 Confirm Connectors

Deployed connectors will appear in this list when they contact Secure Access. confirm that each connector is expected before it can transmit traffic.

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

Connectors to confirm

#	Connector ID	Connector Group	Secure Access Region	Origin IP Address	Announced time	Enable	Revoke
1	esx-75e737eede2b456	SECApplsInfoSecLab	India (West)	10.20.50.68	Mar 18, 2024 3:25 PM IST	☒	× Revoke

Confirm connectors

Connector Groups Last 24 Hours

Resource connectors deployed in your data centers connect users to private resources using zero trust access. Resource connectors are deployed in groups for scalability and redundancy. [Help](#)

Search

Secure Access Region

Status

Environment

3 Connector Groups

Add a Connector Group

Connector Group	Secure Access Region	Status	Connectors	Resources	Requests	Average CPU Load
SECApplsInfoSecLab VMware ESXI	India (West)	Connected	1	0	0	N/A

4. Assign private resource to a resource connector group

Secure access
console

Secure Access

In the Resource Connector Group that you created, add the(Created) Select and assign a Private Resource

Private Resources

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure a private resource if you plan to allow end users to connect to the resource using zero-trust access. [Help](#)

Private Resources

Search by resource name: SY-SEC-App

Private Resource

- SEC-FTP-10×20×50×14
- SEC-ISE-10×20×60×8
- SEC-Jumphost-RDP-10×20×50×50
- SEC-PAN-GUI-10×20×60×29

Choose Private Resources

Copy from existing private resource group: Private Resource Group

Choose Private Resources

16 available

- ☐ asdad
- ☐ bhavik-ubuntu-private
- ☐ bhavik-ubuntu-ztna
- ☐ bhavik-windows-private
- ☐ LabTest
- ☐ MM-e-mechanic
- ☐ MM-FileServer
- ☐ MM-Priv-DNS
- ☐ MM-Priv-VPN

Private Resource >[Save]

8 selected

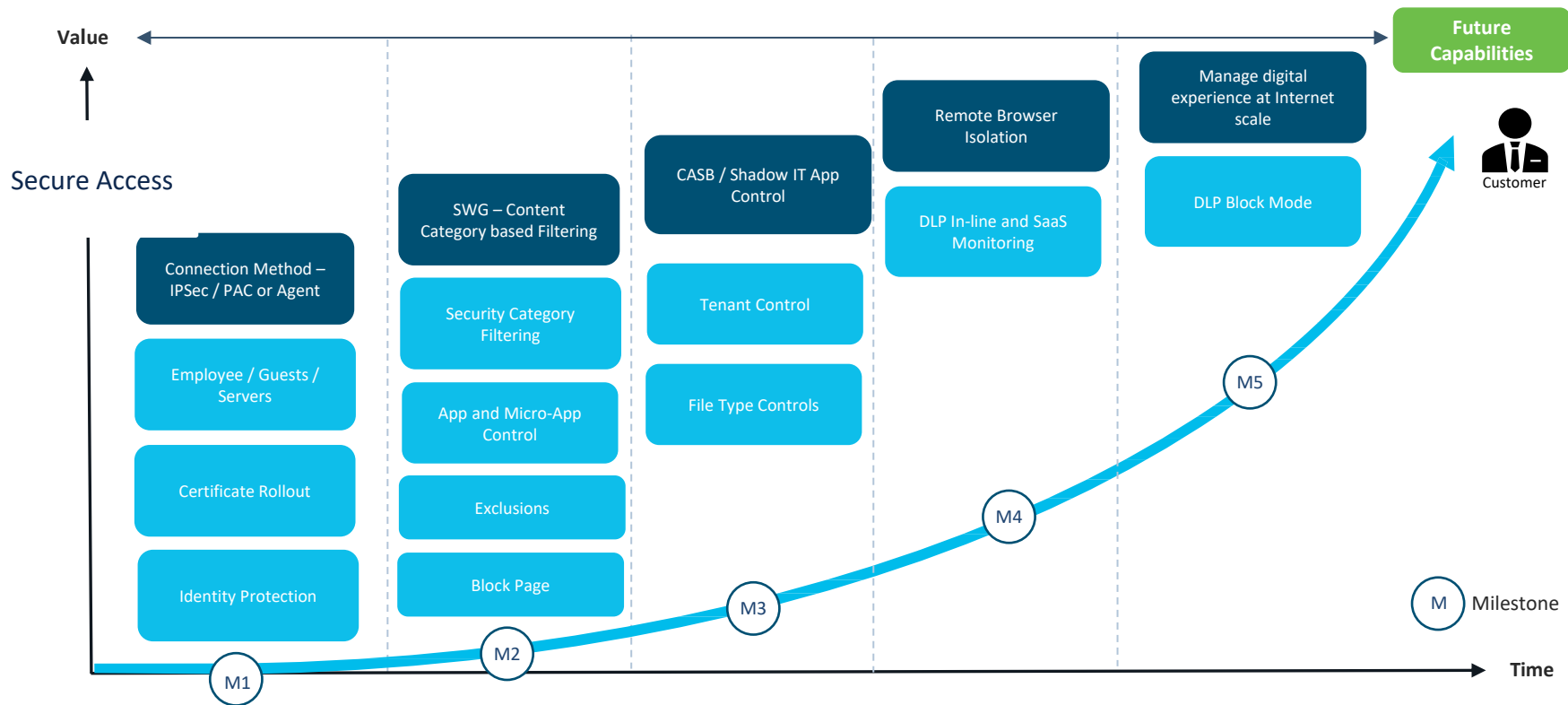
- ☐ SEC-FTP-10×20×50×14
- ☐ SEC-ISE-10×20×60×8
- ☐ SEC-Jumphost-RDP-10×20×50×50
- ☐ SEC-PAN-GUI-10×20×60×29
- ☐ SEC-Rook-Server-10×20×50×200
- ☐ SEC-SNA-Dashboard-10×20×60×15
- ☐ SEC-Splunk-SIEM-10×20×60×28
- ☐ SEC-WEB-App-10×20×50×11

+ Add

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

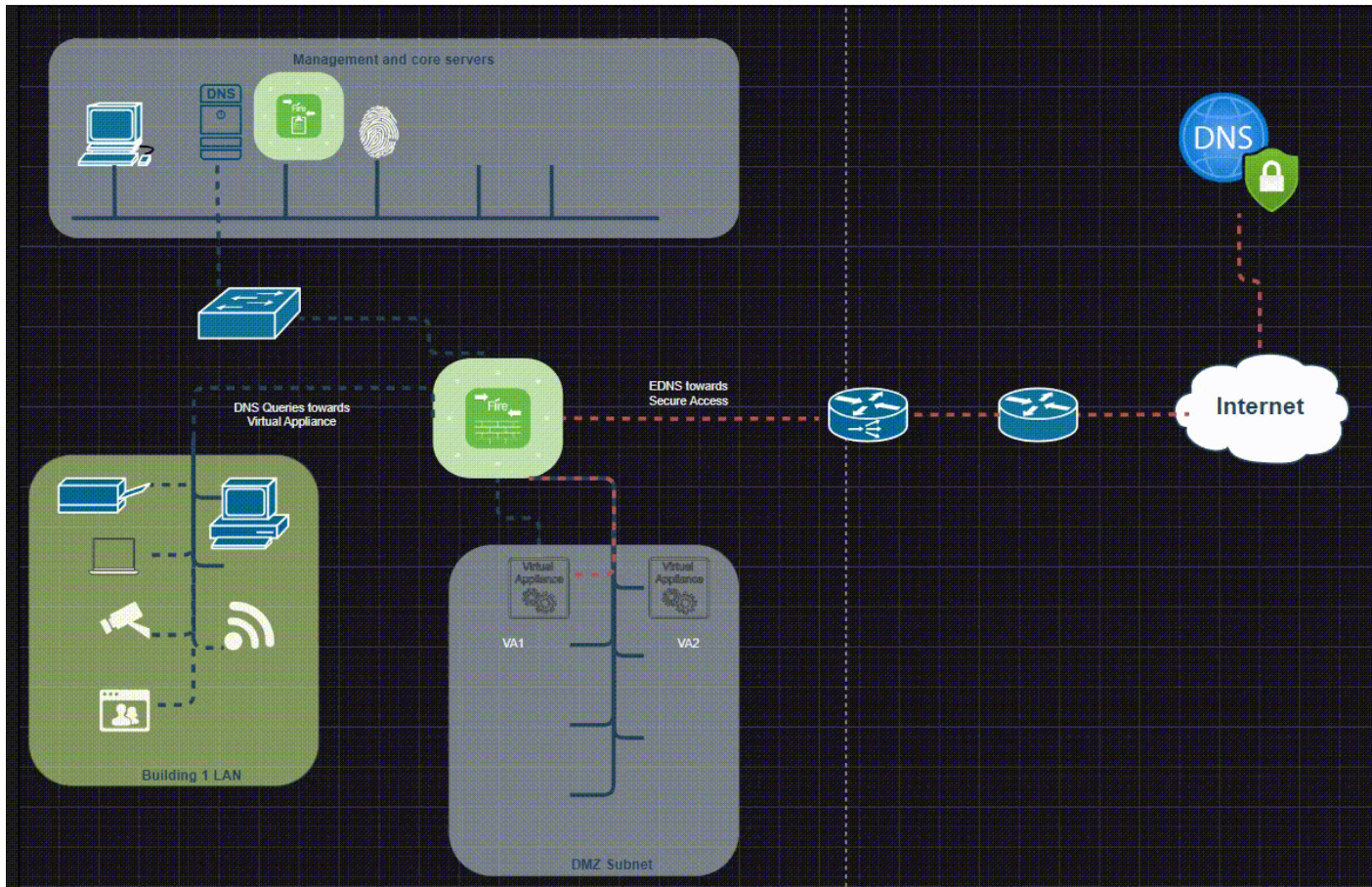
Secure

- 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 (<i>208.67.222.222 & 208.67.220.220</i>)
Deploy Secure Access Root CA
Reporting Review
Configure Internet Access Rule to enforce required protection and access controls (<i>optional</i>)



DNS VA Deployment and Configuration



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 (<i>Manual, AD, IdP</i>) (<i>optional</i>)
Enable SAML Authentication (<i>*requires decryption enablement</i>) (<i>optional</i>)
Configure Internet Access Rule to enforce required protection and access controls (<i>optional</i>)

SWG Layer PAC URL Configuration



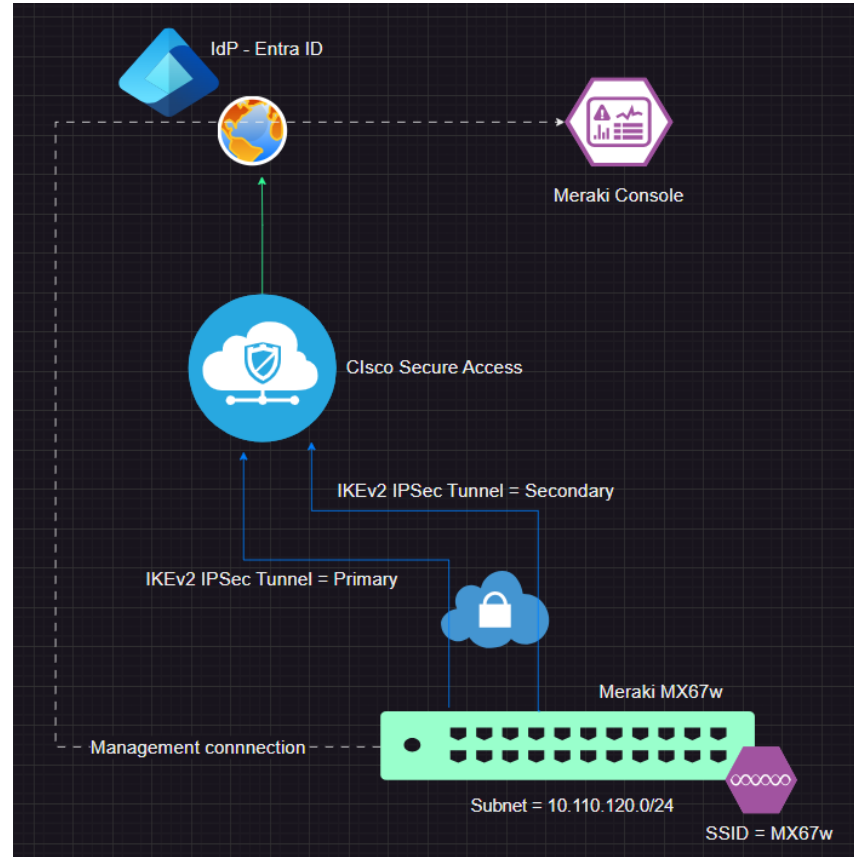
Secure SWG Traffic

Method: IPSec Tunnel

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

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

MX67W in this Example



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

Secure
Access

Network Connections
Manage the connections that allow users to access resources

Network Tunnel Groups
Manage connections between your data centers and SSE

Connector Groups → **Network Tunnel Groups**

General Settings
Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name Enter a Tunnel Group Name
SY-MX1

Region Select the Region or Data Center Location
India (West)

Device Type Set Device Type to Meraki MX
Meraki MX

Next

1. Connect
2. Network Connections
3. Network Tunnel Groups
4. Next

Configure Parameters for IPSec Tunnel

Secure
Access

| Sandeep Yadav

[← Network Tunnel Groups](#)
Add a Network Tunnel Group
Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase
Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID

SY-mx67w @<org><hub>.sse.cisco.com

Passphrase

ThisIsCiscoSecureAccess [Hide](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

..... [Show](#)

Cancel

Back

Next

Configure Parameters for IPSec Tunnel

Secure
Access

- General Settings
- Tunnel ID and Passphrase
- Routing
- 4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network subnet overlap

☐ Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

Routing option

☒ Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24

Add

192.168.128.0/24 X

10.110.120.0/24 X

☐ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Cancel

Back

Save

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.

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

✓ Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	SY-mx67w@8206398-625301437-sse.cisco.com
Primary Data Center IP Address:	3.111.63.143
Secondary Tunnel ID:	SY-mx67w@8206398-625301439-sse.cisco.com
Secondary Data Center IP Address:	13.233.35.114
Passphrase:	ThisIsCiscoSecureAccess

[Download CSV](#)

Done

Configure Site-to-Site VPN

Meraki

Site-to-site VPN

Type ⓘ

☐ Off
Do not participate in site-to-site

☒ Hub (Mesh)

Monitor

Appliance status

Security center

VPN status

Rogue APs

Route table

Configure

Addressing & VLANs

Wireless settings

DHCP

Firewall

Site-to-site VPN ✓

Routing

Client VPN

VPN settings

Local networks

Name	VPN mode	Subnet	Uplink
Default	Disabled	192.168.128.0/24	Any
Test_Subnet	Enabled	10.110.120.0/24	Any

NAT traversal

☒ Automatic
Connections to remote peers are arranged by the Meraki cloud.

☐ Manual: Port forwarding
Remote peers contact the WAN appliance using a public IP and port that you specify. Use this if your WAN appliance is behind another NAT and "Automatic" traversal does not work.

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

Non-Meraki VPN peers ⓘ

Name	IKE Version	IPsec policies	Public IP / Hostname	Local ID	Remote ID ⓘ	Private subnets	Preshared secret	Availability ⓘ
SSE-India-West	IKEv2 ▾	Umbrella	3.111.63.143	SY-mx67w@8206398-6253C		0.0.0.0/0	*****	All networks
SSE-India-West-Secondary	IKEv2 ▾	Umbrella	13.233.35.114	SY-mx67w@8206398-6253C		0.0.0.0/0	*****	All networks

[Add a peer](#)

Choose a Preset

- Umbrella
- Default
- AWS
- Azure
- Umbrella**
- Umbrella (Deprecated)
- Zscaler
- Custom

Phase 1

Encryption: ▾

Authentication: ▾

Pseudo-random Function: ▾

Diffie-Hellman group: 14 ▾

Lifetime (seconds): 14400

Phase 2

Encryption: AES 256

Authentication: SHA1

PFS group: Off ▾

Lifetime (seconds): 3600

[Cancel](#) [Update](#)

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

The screenshot shows the Meraki dashboard interface. The top navigation bar is green with the Cisco Meraki logo. The left sidebar contains navigation links: Network (Home Network), Network-wide, Security & SD-WAN (selected), Cameras, Insight, and Organization. The main content area shows the VPN Status for Home Network, with a sub-menu on the left containing Monitor (Appliance status, Security center, VPN status (checked), Rogue APs, Route table) and Configure (Addressing & VLANs, Wireless settings, DHCP, Firewall, Site-to-site VPN, Routing). A blue banner at the top of the main content area reads: "Read the [blog post](#) to find out everything this page has to offer."

VPN Status › **Home Network** for the last day ▼

[Overview](#) [VPN participants](#)

No data available for this VPN network during this time period.

0 site-to-site peers 1 exported subnet 2 Non-Meraki peers

Status ▲	Name	Public IP	Subnets	+
●	SSE-India-West	3.111.63.143	0.0.0.0/0	
●	SSE-India-West-Secondary	13.233.35.114	0.0.0.0/0	
2 total				

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

← Network Tunnel Groups

SY-MX 

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#) 

Summary

 Warning

Primary and secondary hubs mismatch in number of tunnels.

Region	India (West)
Device Type	Meraki MX
Routing Type	Static Routing
IP Address Range	192.168.128.0/24, 10.110.120.0/24
Last Status Update	Apr 10, 2024 4:53 PM

Primary Hub

 Hub Down

0

Active Tunnels

Tunnel Group ID	SY-mx67w@8206398-625301437-sse.cisco.com
Data Center	sse-aps-1-1-0
IP Address	3.111.63.143

Secondary Hub

 Hub Up

1

Active Tunnels 

Tunnel Group ID	SY-mx67w@8206398-625301439-sse.cisco.com
Data Center	sse-aps-1-1-1
IP Address	13.233.35.114

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

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#) 

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Secondary 1	131074	113.211.211.4	sse-aps-1-1-1	13.233.35.114	 Connected	Apr 10, 2024 4:53 PM

Setup Access Policy For Internet Access

Secure
Access

Access Policy

[Rule Defaults and Global Settings](#)

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Q SY-SEC-MX

Filters 1 Reset all

Add Rule

3 Results

Customize view

	☐	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
	☐	9	SY-SEC-MX-SIA-Allow-Rule	Internet	Allow	SY-MX	Arts +53		76.6k		
	☐	10	SY-SEC-MX-SIA-Block-Rule	Internet	Block	SY-MX	Illegal Down... +6		845		
	☐	54	SY-SEC-MX-SIA-Isolate	Internet	Isolate	SY-MX	SY-SEC-RBI +1		22		

Rows per page 100 < 1 >

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
0x120x0	SY-MX	https://acronis-detection-test.com/acronis-test-file-macOS	16.24.40.177	10.110.120.1		Allowed — Isolated	Uncategorized	
0x120x0	SY-MX	https://acronis-detection-test.com/acronis-test-file-macOS	16.24.40.177	10.110.120.1		Allowed — Isolated	Uncategorized	
0x120x0	SY-MX	https://acronis-detection-test.com/acronis-test-file.exe	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0x120x0	SY-MX	https://acronis-detection-test.com/acronis-test-file.exe	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0x120x0	SY-MX	http://theguardian.com/	15.184.45.91	10.110.120.1		Allowed — Isolated	Uncategorized	
0x120x0	SY-MX	http://theguardian.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 < >

< Destination	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, Co	...
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	96.126.103.196	10.110.120.1		Blocked — Potentially Unwanted Applications (Protected File)	Malware, Software/Technology, Co	...
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 (<i>if planning Roaming Module to remain "active" while on-network</i>)
Deploy Secure Access Root CA (<i>if not deployed already</i>)
Provision Secure Client Roaming Module & <i>Orginfo.json</i> (<i>same folder location as Umbrella</i>)
Define TND configuration (<i>if needed</i>)
User Visibility – User Provisioning (<i>Manual, AD, IdP</i>) (<i>optional</i>)
Configure Internet Access Rule to enforce required protection and access controls (<i>optional</i>)
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 (<i>Manual, AD, IdP</i>)
Deploy Secure Access Root CA (<i>if not deployed already</i>)
Configure Endpoint Posture Profile (<i>optional</i>)
Configure RA VPN Settings • Configure DNS Servers • IP Pool dedicated for RA VPN
Configure RA VPN Profile • Configure General Settings • Define Authentication Method (<i>SAML/Cert/MultiCert/SAML+Cert/MultiCert</i>) • 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 (<i>optional</i>)

SWG -Secure Client with Full Tunnel



Advanced Feature

SIA—Advanced Features

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

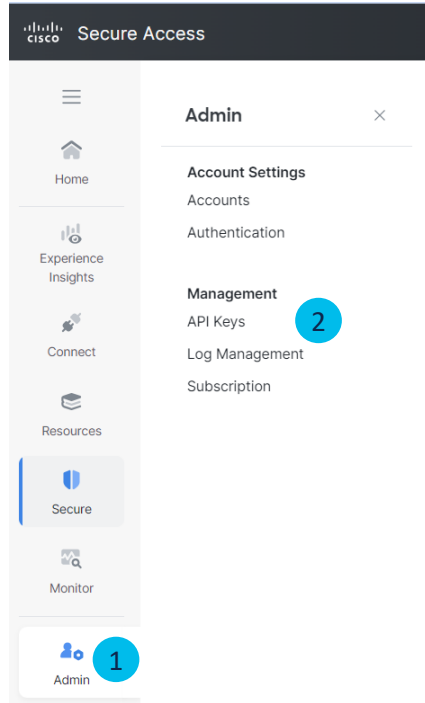
Cisco Secure Access SIEM Integration

Splunk Enterprise Security

CISCO *Live!*



Manage Event and Audit Logs



The image shows the Amazon S3 configuration screen. The screen has a title bar with "Amazon S3", "Status" (Not Configured), and "Last Sync" (Never). The main content area has two radio buttons: "Use your company-managed Amazon S3 bucket" and "Use Cisco-managed Amazon S3 storage" (3). Below the second radio button is a link: "Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#)." Below this is a "Select a Region" dropdown menu with "US West (N. California)" selected. Below that is a "Select a Retention Duration" dropdown menu with "30 days" selected. At the bottom right are "CANCEL" and "SAVE" buttons. Below the main content area is a large box with a cloud icon and the text: "We're activating AWS S3 export now... Once activation is complete, we'll provide you with keys to access your new S3 storage."

Select Data Warehouse Location

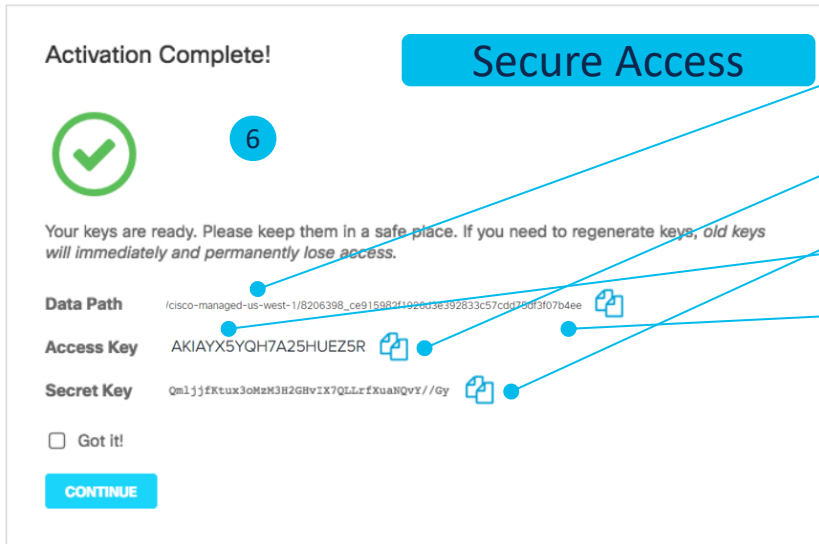
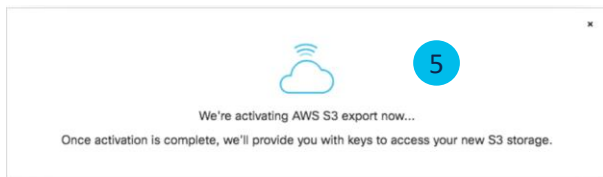
The location options listed here are the choices you have as to where Cisco Secure Access will save all reporting data. For more information, see [Log Management](#).

- ☒ **North America - California, US (Current)**
Physical location of the North American data warehouse. (4)
- ☐ **Europe - Frankfurt, DE**
Physical location of the European data warehouse.

[CANCEL](#) [NEXT](#)

SIEM Integration

Splunk App



7

Name:
Enter a unique name for the data input

Interval:
Time interval of input in seconds, 600 is the recommended value.

Index:

AWS Region:
AWS Region

AWS Access Key Id:
AWS Access Key Id

AWS Secret Access Key:
AWS Secret Access Key

AWS S3 Bucket Name:
AWS S3 Bucket Name

AWS S3 Directory Prefix:
AWS S3 Directory Prefix

Default Start Date:
Event Processor uses this date if there are no events updated

Event Type:
Event Type

Log Retention Duration

Amazon S3

6

Status

Active (Managed)

Last Sync

Sep 24, 2024 at 7:52 AM

✔ We're sending data to your Cisco-managed S3 storage.

Storage Region

US West (N. California)

Retention Duration

7 days [Edit](#)

Admin Audit Log

Include Admin Audit Log in S3

☐

Log Https Query

Log Query Parameters for HTTPS transaction

☒

Data Path

s3://cisco-managed-us-west-1/8206398_ce915982f1926d3e392833c57cdd75df3f07b4ee

Last Sync

Sep 24, 2024 at 7:52 AM

Schema Version

v9 [View Details](#)

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Forget your keys?

You can regenerate them below. Note that this will invalidate any existing keys.

STOP LOGGING

REGENERATE KEYS

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

Amazon S3

6

Status
● Active (Managed)

Last Sync
Sep 24, 2024 at 7:52 AM

✓ We're sending data to your Cisco-managed S3 storage.

Storage Region

US West (N. California)

Retention Duration

7 days [Edit](#)

Admin Audit Log

Include Admin Audit Log in S3
☐

Log Https Query

Log Query Parameters for HTTPS transaction
☒

Data Path

s3://cisco-managed-us-west-1/8206398_ce915982f1926d3e392833c57cdd75df3f07b4ee

Last Sync

Sep 24, 2024 at 7:52 AM

Schema Version

v9 [View Details](#)

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Forget your keys?

You can regenerate them below. Note that this will invalidate any existing keys.

STOP LOGGING

REGENERATE KEYS

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

cisco *Live!*

#CiscoLiveAPJC

BRKSEC-2482

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

92

Log Schema Version

Amazon S3

6

Status
● Active (Managed)

Last Sync
Sep 24, 2024 at 7:52 AM

✓ We're sending data to your Cisco-managed S3 storage.

Storage Region

US West (N. California)

Retention Duration

7 days [Edit](#)

Admin Audit Log

Include Admin Audit Log in S3
☐

Log Https Query

Log Query Parameters for HTTPS transaction
☒

Data Path

s3://cisco-managed-us-west-1/8206398_ce915982f1926d3e392833c57cdd75df3f07b4ee

Last Sync

Sep 24, 2024 at 7:52 AM

Schema Version

v9 [View Details](#)

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Forget your keys?

You can regenerate them below. Note that this will invalidate any existing keys.

STOP LOGGING

REGENERATE KEYS

- 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

Secure

Policy

Access Policy

Data Loss Prevention Policy

Profiles

Endpoint Posture Profiles

IPS Profiles

Security Profiles

Settings

Threat Categories

Notification Pages

Do Not Decrypt Lists

Certificates

Data Classification

public internet sites from devices that are on your network or that your
rules apply to users and devices accessing applications and other resources on
applies the first rule in the list that matches traffic. [Help](#)

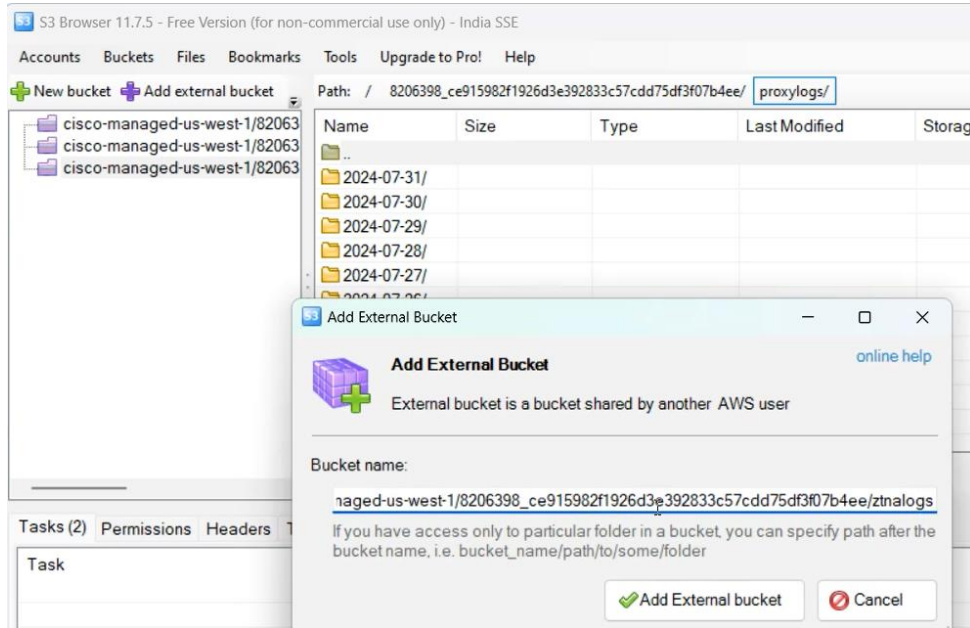
Filters Reset all

Add Rule

Customize view

	Access	Action	Sources	Destinations	Security	Logging	Hits	Status	
ZTNA_Access	Private	Allow	Bhavik Shah ... +2	SY-SEC-App	Security	Enabled	1.1k	✓	...
ZTNA_Access_O...	Private	Allow	Bhavik Shah ... +2	SY-SEC-App	Security	Enabled	-	✓	...
	Private	Allow	Sandeep Yada...	10.20.50.14 +1	-	Enabled	-	✓	...
lock	Internet	Block	Sandeep Yada...	SY-SEC-Block... +2	Security	Enabled	-	✓	...

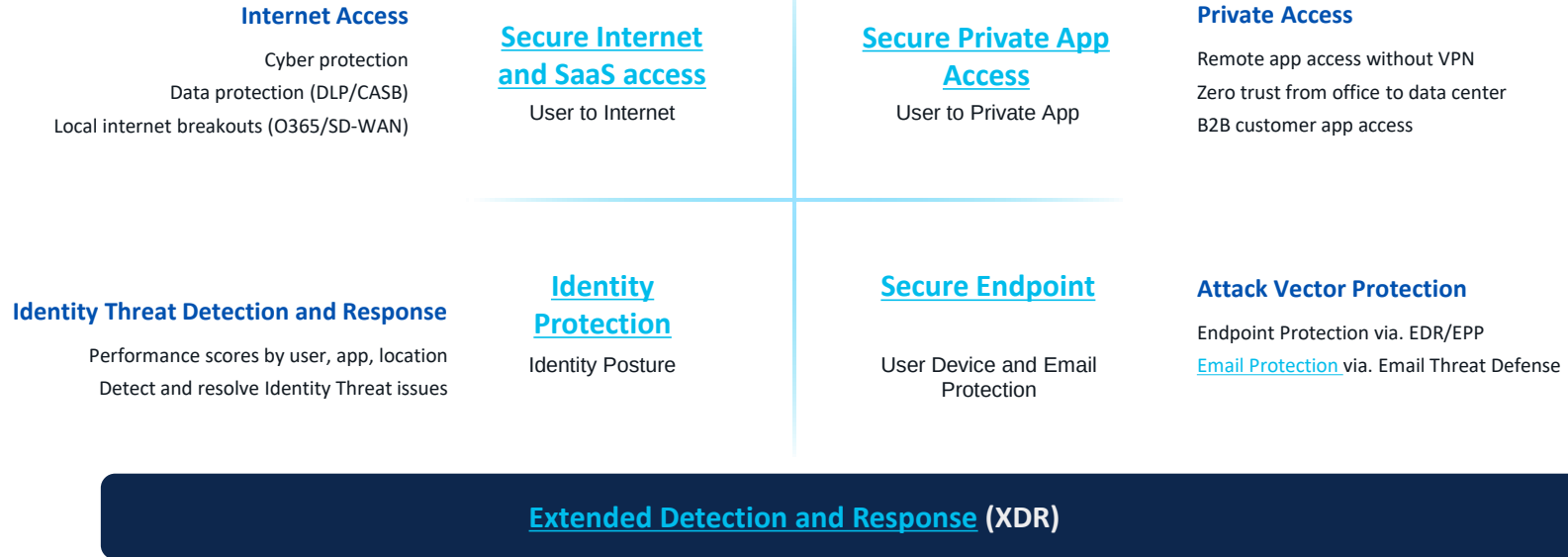
Verify Logs are uploaded to S3 bucket



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



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

CISCO *Live!*

- 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!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC