

# Step-By-Step Configuration Guide for Versa Secure Private Access (VSPA)

## About This Document

This guide provides a comprehensive, step-by-step configuration process for setting up and preparing your organization's Versa Secure Private Access (VSPA).

Versa Secure Private Access (VSPA) is a software-defined solution that enables secure connectivity for employees working remotely to enterprise applications hosted on-premises or in private clouds.

It is built on a Zero Trust Network Access (ZTNA) framework, ensuring that users and applications are authenticated and authorized before access.

VSPA is part of Versa's Secure Access Service Edge (SASE) offering and integrates:

- Identity management
- Security controls
- Cloud-delivered services
- Software-defined networking

## Document Information

|                |   |
|----------------|---|
| <b>Title</b>   | Step-By-Step Configuration Guide for Versa Secure Private Access (VSPA) |
| <b>Author</b>  | Versa Professional Services   |
| <b>Version</b> | V 1.0   |

## Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

## Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please contact your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

|  |    |
|--|----|
| Scenario .....   | 4  |
| Topology.....  | 5  |
| Configuration steps.....   | 6  |
| <i>Step 1: Set up Site-to-Site Tunnel.....</i>                             | 7  |
| Step 2: Configure Authentication Method .....                              | 14 |
| Step 3: Configure DNS and Private Routes .....                             | 20 |
| Step 4: Configure User-Defined Objects .....                               | 22 |
| Step 5: Secure Client Access Rules.....                                    | 24 |
| Step 6: Configure TLS Decryption Rules and Profiles .....                  | 31 |
| Step 7: Configure Real-Time Protection (Private App Protection) Rules..... | 35 |
| Step 8: Test and Verification.....   | 40 |
| Appendix A – S2S IPsec VPN EBGP Configuration.....                         | 43 |
| BGP Peer Policy Configuration .....  | 43 |
| Configuring BGP Peer Policy .....  | 43 |
| Configuring EBGP in S2S IPsec VPN .....                                    | 46 |
| Appendix B – Authentication Methods Configuration .....                    | 49 |
| Versa Directory .....  | 49 |
| SAML.....  | 49 |
| Device Certificate .....   | 52 |
| User Certificate .....   | 52 |
| Appendix C – User Defined Objects and Endpoint Information Profiles.....   | 55 |
| Appendix D – Secure Access Policies – Key Components .....                 | 61 |
| Appendix E – Real-Time Protection – Key Components.....                    | 69 |
| About Versa.....   | 73 |

# Scenario

## Scenario

ACME-ONE, a global organization, requires secure remote access to internal applications (Active Directory, HR Portal, Financial Apps) hosted in its Data Centre. Connectivity to the Data Centre is established using a route-based IPsec site-to-site tunnel. Remote users must access these applications securely without weakening the organization's security posture.

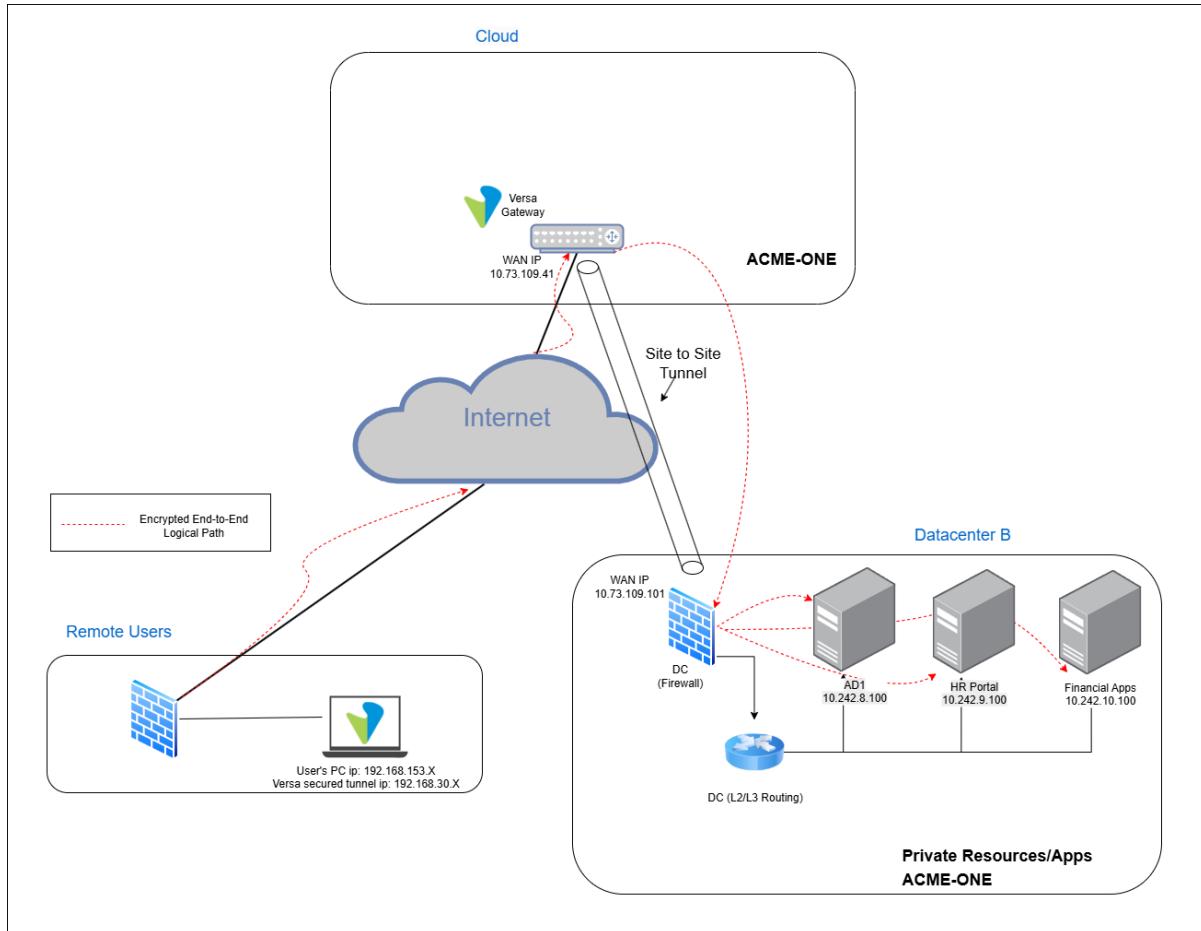
## Customer Requirements

- Strong authentication (Active Directory LDAP)
- Device posture validation
- User-based access controls
- Security enforcement via SSE Gateway: TLS encryption/decryption, Antivirus (AV), Intrusion Prevention System (IPS)
- Policy enforcement based on OS type and user group
- Support for custom applications and URL categories

## Deployment Steps

1. Deploy SSE Gateway with VSPA enabled
2. Establish route-based IPsec site-to-site tunnel to Data Centre
3. Enable access for remote users to private apps (AD, HR Portal, Financial Apps)
4. Configure LDAP authentication with Active Directory
5. Define policies for custom applications and URL categories
6. Apply secure access policies based on OS type and user group
7. Enforce TLS decryption, Antivirus, and IPS inspection through SSE Gateway

# Topology



This topology represents a **secure remote access architecture** where both **Remote Users (working from home)** and Customer **Datacenter B** connect to the cloud-hosted Versa SASE Gateway through **encrypted tunnels**.

- **Cloud**

The cloud hosts a Versa SASE Gateway (**WAN IP: 10.73.109.41**) that terminates remote access and IPsec tunnels. It acts as a bridge between remote users and private resources in Data Centre B, enabling secure access through the Versa Secure Access Client.

- **Datacenter B**

Connects to the Cloud DC via an **IPsec tunnel to the Versa Gateway**.

Firewall WAN IP: 10.73.109.101

Hosts internal services:

- AD1: 10.242.8.100

- HR Portal: 10.242.9.100 (hr-portal.acme-one.com)
- Financial Apps: 10.242.10.100 (financial-apps.acme-one.com)

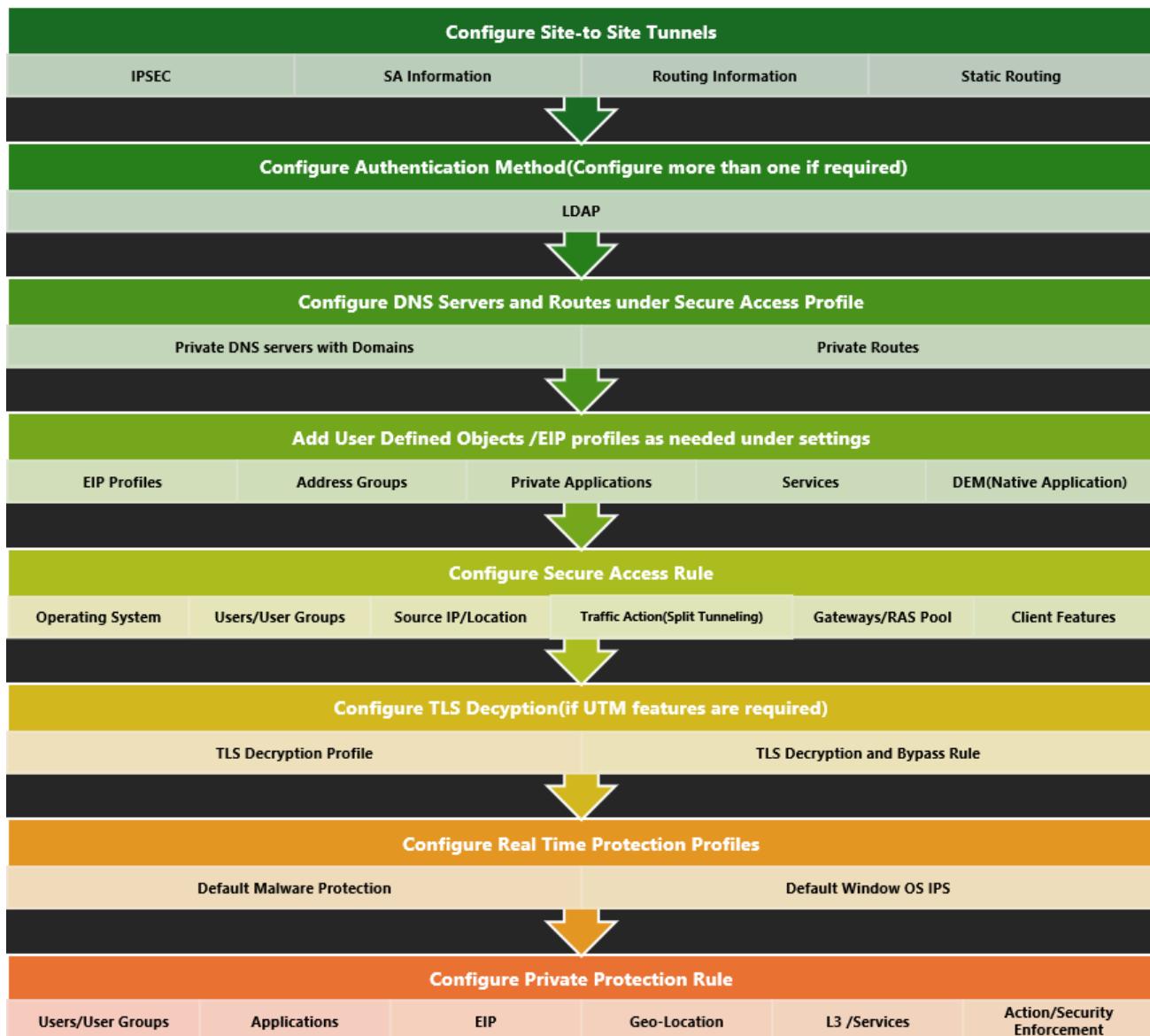
- **Remote Users (Work from Home)**

Located in network **192.168.153.X**, users connect using the **Versa client** and get an IP from the pool **192.160.30.X**. All traffic is securely tunneled to **Cloud DC**, enabling access to corporate resources without back-hauling through Datacenter B.

All communication is **end-to-end encrypted**, and **Cloud DC** acts as the **central access point** for both remote users and Datacenter B.

## Configuration steps

The current VSPA use case and configuration involves the following steps, which will be described in detail in the sections further.



*Step 1: Set up Site-to-Site Tunnel*

An IPSec tunnel facilitates secure remote access to enterprise private applications, DNS servers and Authentication Servers by directing traffic from the Versa gateway to the customer's data center, designated as "Datacenter B" in this case. Versa recommends implementing redundant IPSec tunnels with BGP to ensure high availability.

## Configure Site-to-Site Tunnel

Log in to the Concerto UI using your enterprise administrator credentials (Tenant Admin) to configure a site-to-site tunnel.

Navigate to

**Configure > Security Service Edge > Settings > Site-to-Site Tunnels and click + Add.** This will take you to the new tunnel configuration page.

The tunnel configuration is completed through four wizard screens, as illustrated below. The first section (Enter TYPE) is displayed by default for configuration. Clicking **Next** at each section moves on to the next section of the tunnel configuration.

### IPSec Site-to-Site Tunnel

The default tunnel selection is IPSec. The remaining details, including tunnel type, remote address, and other parameters, should be configured as outlined below.

1. Selecting "Enter TYPE"

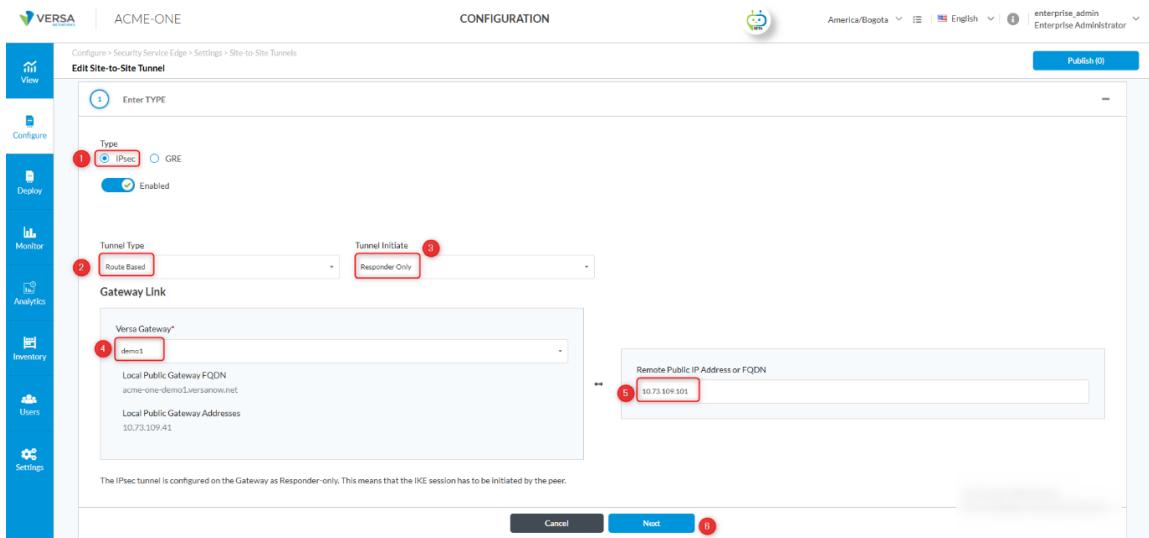
- A. Keep the default selection on **Type** as IPsec, and Tunnel status is default enabled.
- B. Choose the correct **Tunnel Type**. If necessary, use the drop-down menu to change it from the default [Route-Based](#) tunnel to the **Policy-Based** tunnel. This document shows details related to the Route-Based tunnel.
- C. The third step shown in the screenshot is **Tunnel Initiate**, which can be triggered by modes like "Responder Only", "Traffic", or "Automatic". When EBGP is used, "Responder Only" works fine. However, when using a static route, it should be set to "Automatic" or "Traffic". In our use case, we can choose Automatic.

Note that Versa Gateway is set as 'responder only' for the IPsec tunnel. So, the peer must initiate the request for the tunnel for the negotiation to start.

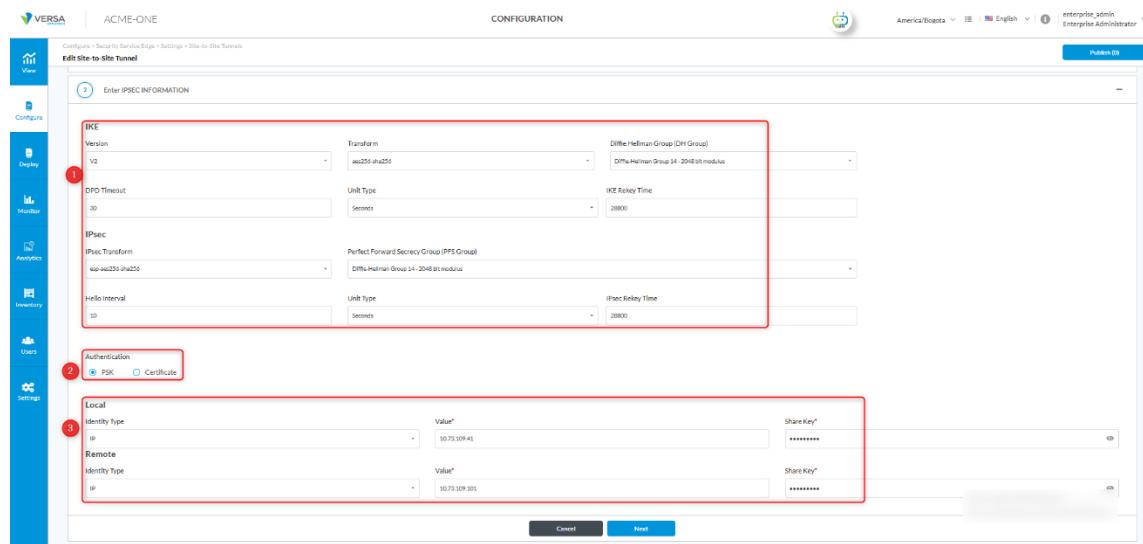
- D. Choose the correct originating Versa SASE gateway from the **Versa Gateway** drop-down menu. Typically, each tenant would be provisioned into multiple gateways for redundancy; this option allows you to choose the appropriate gateway from which you need to build a secure tunnel to your enterprise destination.
- E. Use the **Remote Public IP Address or FQDN** field to enter your enterprise firewall details as the tunnel endpoint.

Note: When configuring Local Identity > Type > FQDN, you must enter the specific FQDN of the SASE Gateway that you want to establish the site-to-site tunnel with from the remote site. This **FQDN** appears below the text "**Local Public Gateway FQDN**" in the image below. In our case, it would be acme-one-demo1.versanow.net.

- F. Click **Next** to proceed to the next section to provide IPSec Parameters



2. Selecting "Enter IPSEC INFORMATION"; Clicking Next in the above section will bring you to this part of the screen, where IPsec-related details are to be provided. Refer to the image below.



A. Provide **IKE** and **IPsec** parameters according to your configuration requirements. The image below shows the default selection; use the drop-down menus to modify as needed. The following table summarizes the recommended settings for both IKE (Phase 1) and IPsec (Phase 2). Note that while some vendors use a shorter lifetime (3600 seconds), we recommend 28800 seconds for consistency and reduced rekeying overhead.

| Phase                  | Parameter          | Value   |
|------------------------|--------------------|---------|
| <b>IKE (Phase 1)</b>   | Encryption         | AES-256 |
|                        | Authentication     | SHA-256 |
|                        | DH Group           | 14      |
|                        | Lifetime (seconds) | 28800   |
| <b>IPsec (Phase 2)</b> | Encryption         | AES-256 |
|                        | Authentication     | SHA-256 |
|                        | PFS (DH Group)     | 14      |
|                        | Lifetime (seconds) | 28800   |

B. Choose the desired Authentication mode. The default selection is a pre-shared key (PSK). If "Certificate" is to be chosen, then Local and remote certificate names and CA chains are to be added.

C. For pre-shared-key based authentication, add Local and Remote identities (Identity Type such as Email, IP, FQDN) and their corresponding Value and Share Key

D. Click **Next**

- Selecting "Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS"

In this section, configure the tunnel interface IP, usually a /30 from your enterprise segment. Select the VPN name assigned to your tenant at the Gateway, the MTU value, and either Static or EBGP as your preferred routing protocol. Refer to the image below.

A. Under "Setup the Versa SASE Gateway routing towards the enterprise VPN" configure the following

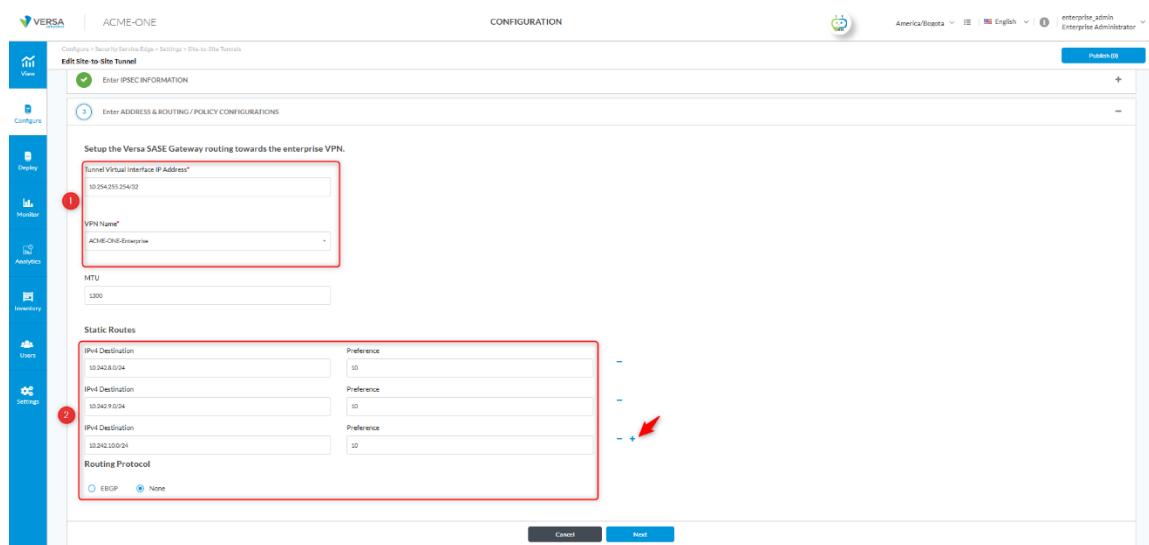
Add a Tunnel Virtual Interface address that is routable within your enterprise network. This typically involves using one IP from a /30 IPv4 address, with the other usable IP from the same /30 to be configured at your enterprise IPSec endpoint.

**VPN Name** to be selected from drop-down, usually the VPN name assigned to your tenant by the service provider, named as <*TenantName-Enterprise*>

Set **MTU**: Versa recommends that the maximum transmission unit be set to 1300 for IPsec-based tunnels

Under Static Routes and Routing Protocols, configure the following

- Click **+ Add** to create a new route.
- Set Routing Protocol to None.
- Enter the destination subnet. (In our case, we need to enter the server subnets one by one: 10.242.8.0/24, 10.242.9.0/24, 10.242.10.0/24).
- Assign a preference value between 1–255 (lower = higher priority).
- Routing Protocol select None.
- Click **Save**.



ACME-ONE

CONFIGURATION

Edit Site-to-Site Tunnel

Enter IPSEC INFORMATION

Enter ADDRESS & ROUTING/ POLICY CONFIGURATIONS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address: 10.254.253.254/32

VPN Name: ACME-Child-Enterprise

MTU: 1300

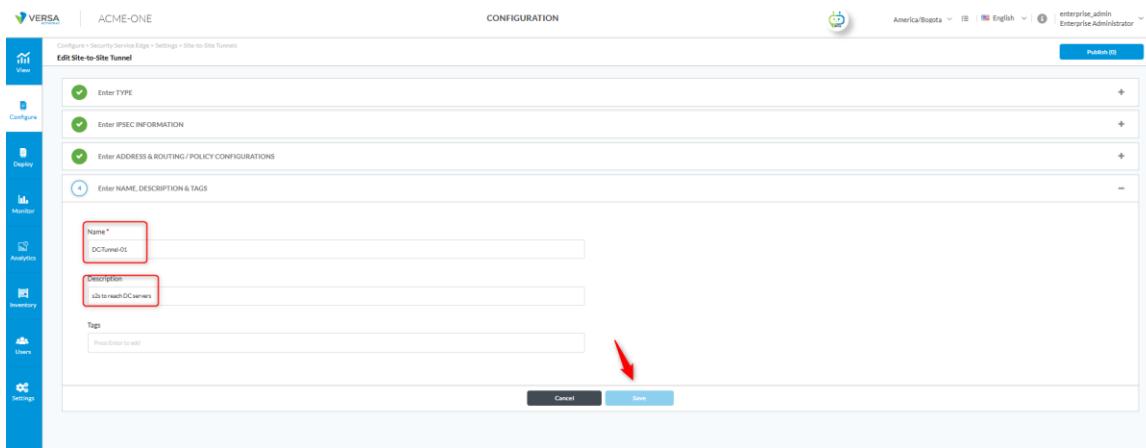
Static Routes

|                                  |                |
|----------------------------------|----------------|
| IPv4 Destination: 10.242.8.0/24  | Preference: 10 |
| IPv4 Destination: 10.242.9.0/24  | Preference: 10 |
| IPv4 Destination: 10.242.10.0/24 | Preference: 10 |

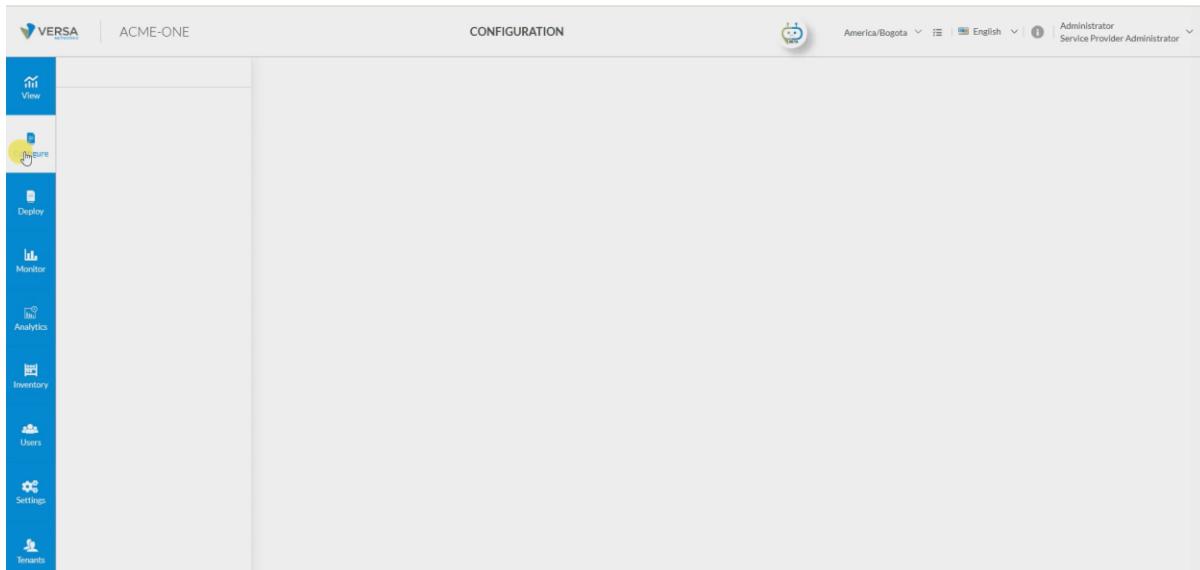
Routing Protocol: EBGP

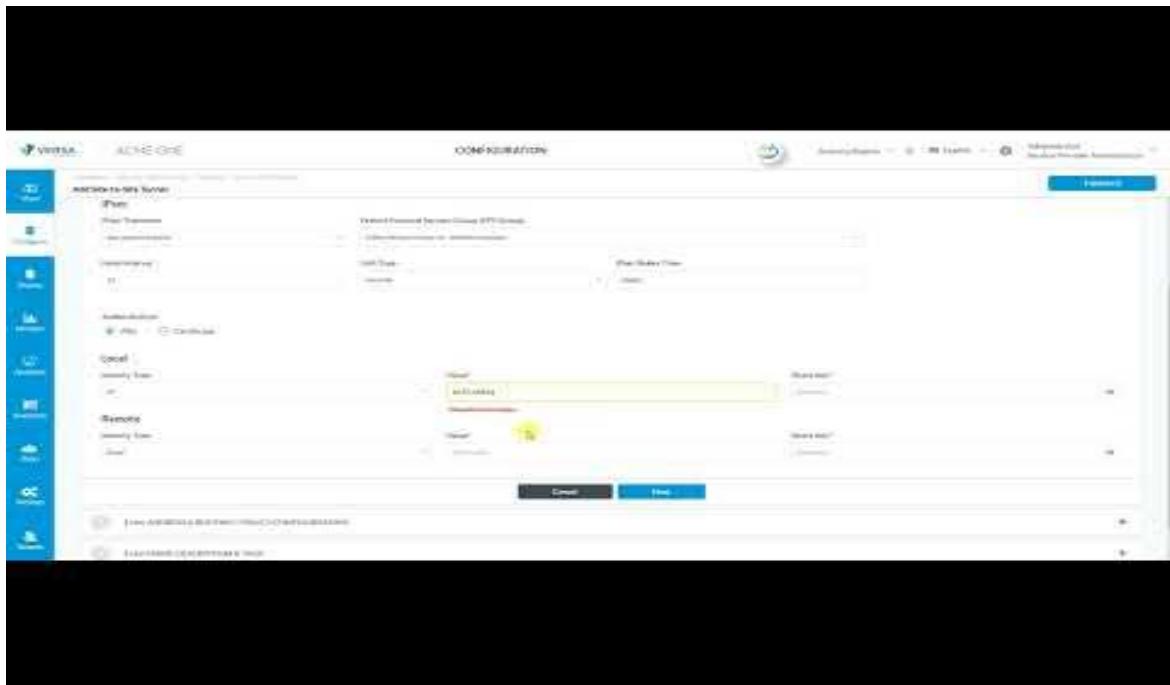
Cancel Next

#### 4. Completing section Enter NAME, DESCRIPTION & TAGS



An embedded video showing the full procedure is included below.





Notes: Ensure that the IPSec tunnel on the peer firewall is configured using the same parameters described in this guide.

NOTE: For high availability and dynamic routing across multiple tunnels, EBGP is

recommended. See Appendix A for configuration details.

## Step 2: Configure Authentication Method

Versa SASE supports various authentication methods, including LDAP and SAML. It's recommended to use your enterprise's existing system. This example utilizes LDAP with Active Directory for remote user authentication when connecting via the SASE client. See Appendix B for other authentication method configuration options.

### LDAP Active-Directory

LDAP allows Versa OS to authenticate users by querying a directory server. Users can be validated individually or in groups. Configuration involves specifying the server, VR, SSL settings, and profile details, then saving the setup.

- [SSL Enabled](#) – To ensure secure communication to the LDAP server. (In our case, we are using SSL disabled)
- [Add secondary Server](#) – To ensure redundancy in case of failure of the Primary server.

Navigate to

**Configure > Security Service Edge > User and Device Authentication > Profiles and click + Add** and follow these steps. Refer to the image below.

ACME-ONE

CONFIGURATION

Secure SD WAN

Service Authentication > Profiles

Administrator

America/Bogota | English | Service Provider Administrator

Secure SD WAN

Real-Time Protection

Secure Access

Digital Experience Monitoring (DEM)

TLS Decryption

Bandwidth Limits

Profiles and Connectors

Partner Integration

User and Device Authentication

Rules

Profiles

SCIM Integration

User-Defined Objects

Settings

Tenants

+ Add

Go to page 1 | < Previous | Next >

Click **+ Add**

ACME-ONE

CONFIGURATION

Configure > Security Service Edge > Users and Device Authentication > Profiles

User and Device Authentication Profile

Administrator

America/Bogota | English | Service Provider Administrator

User and Device Authentication Profiles (0)

+ Add

Name

Type

Description

Tags

Last Modified

No Data

Profile

SCIM Integration

User-Defined Objects

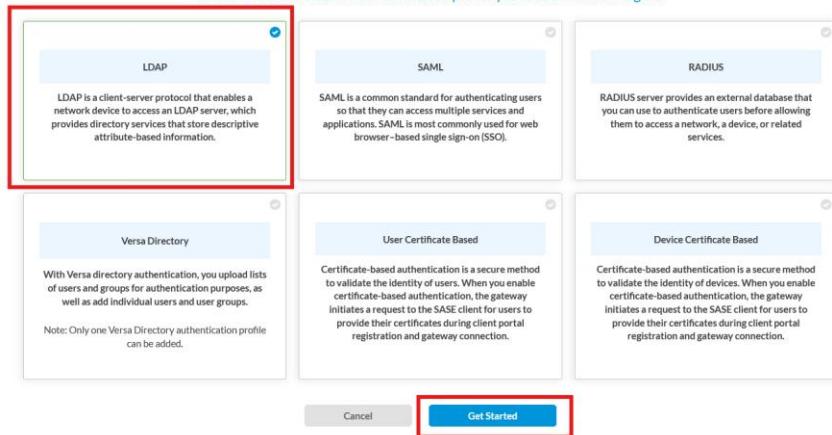
Settings

Tenants

Select **LDAP** as Authentication Method then Click **Get Started**

#### Add User and Device Authentication Profile

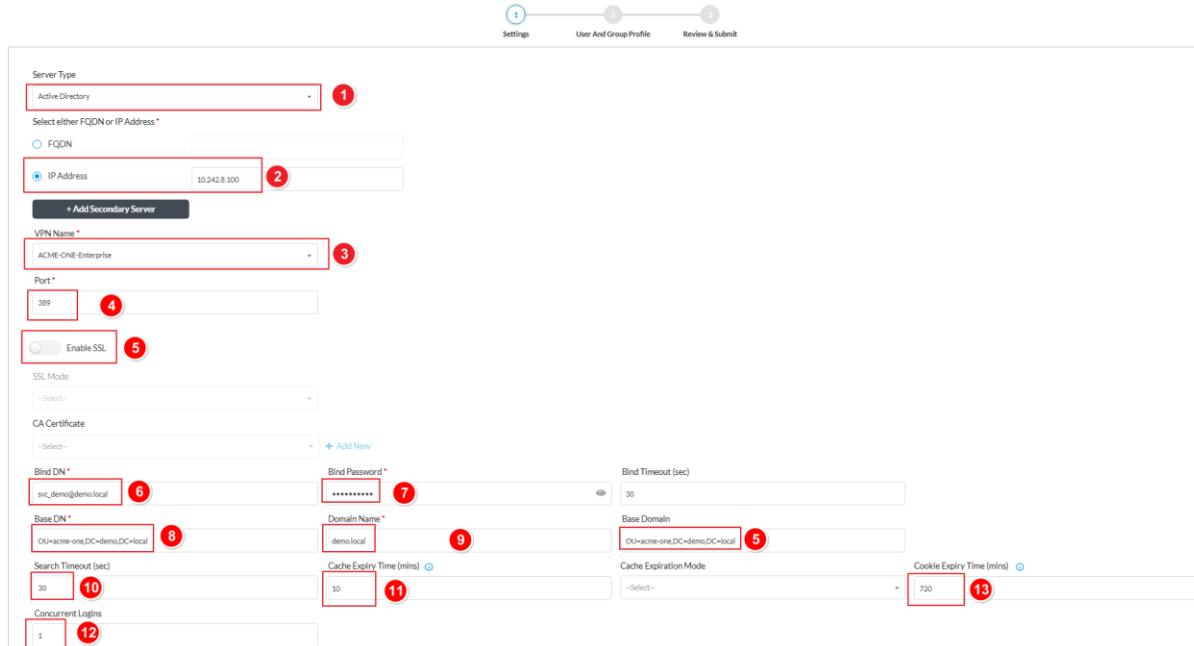
Select which user / device authentication profile you would like to configure.



Now, we need to complete the 3 steps as follows: (**Settings, User and Group Profile, Review & Submit**)

#### Settings:

We must complete the information as shown in the image below. Each highlighted field is explained in the following table, which provides its corresponding value and technical definition.



| Parameter                       | Description   | Current Use Case                      |
|---------------------------------|---|---------------------------------------|
| <b>1. Server Type</b>           | Indicates if the authentication source is Microsoft Active Directory or Open-LDAP.  | Active Directory                      |
| <b>2. FQDN or IP Address</b>    | Fully Qualified Domain Name (FQDN) or IP address of the AD/LDAP server.   | 10.242.8.100                          |
| <b>3. VPN Name</b>              | Defines which VPN instance or network segment this authentication profile applies to.   | ACME-ONE-Enterprise                   |
| <b>4. Port</b>                  | Port used for LDAP/AD communication. - 389: Default LDAP port<br>- 636: Default LDAPS (LDAP over SSL)   | 389 TCP                               |
| <b>5. SSL Status</b>            | Enabled/Disabled: Determines if the connection uses SSL/TLS. If enabled, you must also specify the CA certificate for TLS verification.   | Disabled                              |
| <b>6. Bind DN</b>               | The Distinguished Name (DN) of the service account that Versa uses to connect and query the directory.<br><br>This DN allows Versa to authenticate to the AD/LDAP server and perform user and group searches. | svc_demo@demo.local                   |
| <b>7. Bind Password</b>         | Password for the Bind DN account.   | Service account password              |
| <b>8. Base DN</b>               | Starting point in the LDAP directory tree for searches. Defines the organizational scope.   | Example: OU=acme-one,DC=demo,DC=local |
| <b>9. Domain Name</b>           | The name of the AD domain.  | demo.local                            |
| <b>10. Search Timeout (sec)</b> | Maximum wait time (in seconds) for an LDAP query response.  | 30                                    |

|                               |  |     |
|-------------------------------|--|-----|
| 11. Cache Expiry Time (mins)  | Time (in minutes) that LDAP user/group data will be cached before refreshing.  | 10  |
| 12. Concurrent Logins         | Maximum number of concurrent sessions allowed per user.  | 3   |
| 13. Cookie Expiry Time (mins) | Specifies the validity period of the authentication cookie. When the cookie expires, it becomes invalid, requiring the user to log in again for the next connection request. | 720 |

Once all values are filled in, click Next to proceed with the step 2 (*User and Group Profile*).

**User and Group Profile:** We must complete the information as shown in the image below. Each highlighted field is explained in the following table, which provides its corresponding value and technical definition.

| Parameter | Value / Default | Description |
|-----------|-----------------|-------------|
|           |                 |             |

|                                  |   |  |
|----------------------------------|---|--|
| 1. <b>Group Object Class</b>     | group   | Standard AD object class for security and distribution groups. Required for identifying groups in the directory.                             |
| 2. <b>Group Name</b>             | name  | Attribute that defines the display name of a group. Used by Versa to match groups during policy evaluation.                                  |
| 3. <b>Group Member</b>           | memberOf  | Attribute that lists group memberships for a user object. Ensures Versa can apply policies based on AD group membership.                     |
| 4. <b>User Object Class</b>      | user  | Standard AD object class for user accounts. Required for identifying users in the directory.   |
| 5. <b>User Name</b>              | userPrincipalName (recommended) or sAMAccountName | Attribute used for login. userPrincipalName (e.g., vip1@acme-one.com) is modern and preferred. sAMAccountName is legacy but still supported. |
| 6. <b>Password Last Set</b>      | pwdLastSet  | Attribute indicating when a user's password was last changed. Useful for enforcing password expiration policies.                             |
| 7. <b>Password Max Age</b>       | maxPwdAge   | Attribute defining the maximum password lifetime. Derived from the AD domain password policy.  |
| 8. <b>Refresh Interval (sec)</b> | 21600 (default = 6 hours)                         | Determines how often Versa refreshes user and group information from LDAP. Can be tuned based on how frequently the directory changes.       |

Once all values are filled in, click Next to proceed with the step 3 (*Review & Submit*).

#### **Review & Submit:**

Enter a descriptive value in the Name field (for example: AD-DC1).

Then, review all parameters to confirm they are configured correctly before submitting and then click on Save.

Review your configurations. Before submitting, review and edit any steps of your configuration below.

Settings
User And Group Profile
Review & Submit 3

**General**

|      |                    |             |
|------|--------------------|-------------|
| Name | AD-DC1             | Description |
| Tags | Press Enter to add |             |

**Settings** Edit

|                    |                     |
|--------------------|---------------------|
| Server Type        | active-directory    |
| FQDN or IP Address | 10.242.8.100        |
| VPN Name           | ACME-ONE-Enterprise |
| Port               | 389                 |
| SSL Status         | Disabled            |
| SSL Mode           |                     |
| CA Certificate     |                     |
| File Name          |                     |
| Installed To       |                     |

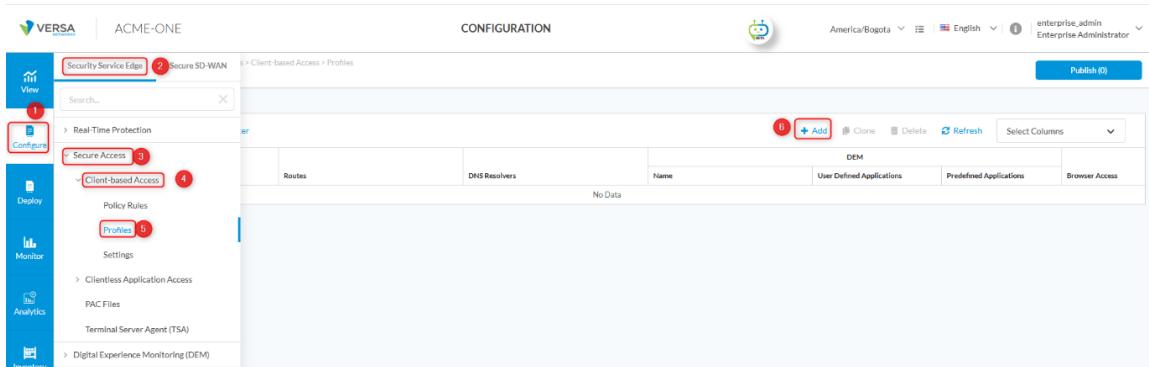
Cancel
Back
Save

Note: - The scope of Active Directory read access depends on the AD administrator. In our case, access has been granted to the **OU=ACME-ONE** within the global domain **demo.local**, using the designated service account.

### Step 3: Configure DNS and Private Routes

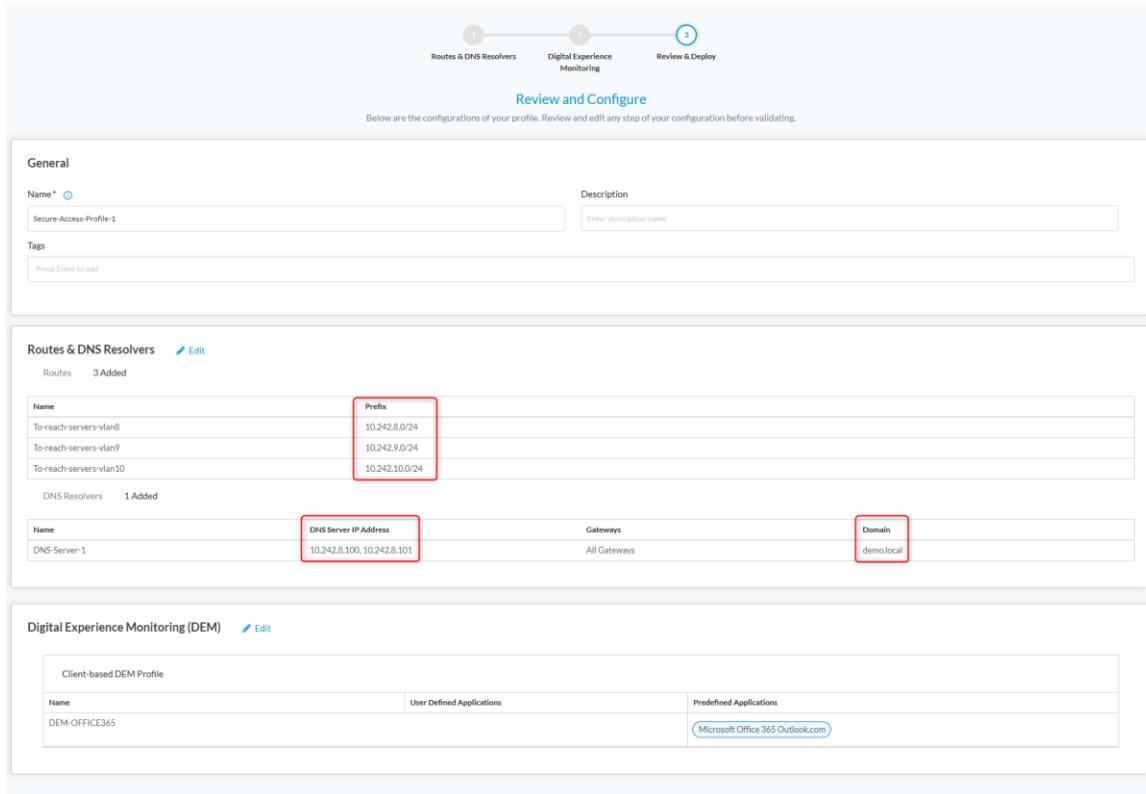
In the VSPA use case, to facilitate the resolution of private applications when a user connects remotely and to route all private application traffic from the SASE client, Secure Access Profiles are employed to define DNS Resolvers, Private Routes and DEM (application performance monitoring).

Navigate to **Configure > Security Service Edge > Secure Access > Client-based Access > Profiles** and click on **+Add** as shown in the figure below.



Configure the IPs and domain(s) of your internal DNS servers under DNS resolvers, private routes under the routes section and any private applications that you would want to monitor from the client under Digital Experience Monitor.

- Secondary DNS server - It is recommended to configure redundant DNS server(s) to take over in case of failure.



**Review and Configure**  
Below are the configurations of your profile. Review and edit any step of your configuration before validating.

**General**

|        |                         |             |                        |
|--------|-------------------------|-------------|------------------------|
| Name * | Secure-Access-Profile-1 | Description | Enter description name |
| Tags   | Press Enter to add      |             |                        |

**Routes & DNS Resolvers** [Edit](#)

| Routes                  |                | 3 Added |
|-------------------------|----------------|---------|
| Name                    | Prefix         |         |
| To-reach-servers-vlan8  | 10.242.8.0/24  |         |
| To-reach-servers-vlan9  | 10.242.9.0/24  |         |
| To-reach-servers-vlan10 | 10.242.10.0/24 |         |

| DNS Resolvers |                            | 1 Added      |            |
|---------------|----------------------------|--------------|------------|
| Name          | DNS Server IP Address      | Gateways     | Domain     |
| DNS-Server-1  | 10.242.8.100, 10.242.8.101 | All Gateways | demo.local |

**Digital Experience Monitoring (DEM)** [Edit](#)

| Client-based DEM Profile |                           |                                  |  |
|--------------------------|---------------------------|----------------------------------|--|
| Name                     | User Defined Applications | Predefined Applications          |  |
| DEM-OFFICE365            |                           | Microsoft Office 365 Outlook.com |  |

## Step 4: Configure User-Defined Objects

Versa supports a variety of user-defined objects (Example, Applications, services). When a particular object is not listed under pre-defined objects, we can define the object using the User-defined (Custom) Object.

Custom applications can be classified as:

- Any application that needs to interact with the **client** or be referenced in a **Secure Access Rule** must be defined as a **Client Native Application**. For split tunnelling or DEM use case.
- Applications that interact with the **gateway** or are referenced in **Real-Time Protection Rules** must be defined as **Private Applications**. To allow or block a private application.

In our case, we defined a **Client Native Application** (<http://dem-monitoring.demo.local:8000>) for use with the **DEM module**, enabling the collection of performance statistics. We also created a couple of **Private Applications** to be used in our **Real-Time Protection Policies**. The following section outlines the steps to create both a Client Native Application and a Private Application.

To create a **Client Native Application**, navigate to

**Configure > Security Service Edge > Secure Access > User-Defined Objects > Applications.**

The Client Native Application configuration should resemble the example shown in the image below.

| Application             | File Path/FQDN                    | Host                        | Protocol | Custom Port | URI Path    | App Protocol | Ignore SSL Warning | Application Image | Tags | Last Modified                             |
|-------------------------|-----------------------------------|-----------------------------|----------|-------------|-------------|--------------|--------------------|-------------------|------|---|
| DEM-Monitoring Internal | FQDN: dem-monitoring.acme-one.com | dem-monitoring.acme-one.com | TCP      | 8000        | monitoring1 | HTTP         | Disabled           |                   |      | 7/28/2025, 9:48:28 AM<br>enterprise_admin |

Now, we can adjust the Secure Access Profile DEM profile created in the last section by changing the DEM accordingly.

**Routes & DNS Resolvers** [Edit](#)

Routes 3 Added

| Name                    | Prefix         |
|-------------------------|----------------|
| To-reach-servers-vlan8  | 10.242.8.0/24  |
| To-reach-servers-vlan9  | 10.242.9.0/24  |
| To-reach-servers-vlan10 | 10.242.10.0/24 |

DNS Resolvers 1 Added

| Name         | DNS Server IP Address      | Gateways     | Domain     |
|--------------|----------------------------|--------------|------------|
| DNS-Server-1 | 10.242.8.100, 10.242.8.101 | All Gateways | demo.local |

**Digital Experience Monitoring (DEM)** [Edit](#)

Client-based DEM Profile

| Name                    | User Defined Applications | Predefined Applications |
|-------------------------|---------------------------|-------------------------|
| DEM-Monitoring-Internal | (DEM-Monitoring-Internal) |                         |

[Cancel](#) [Back](#) [Save](#)

To create a **Private Application**, navigate to

**Configure > Security Service Edge > User-Defined Objects > Applications > Private Application**

Then, create the test apps **hr-portal.acme-one.com** and **financial-apps.acme-one.com** as follows:

**hr-portal.acme-one.com:**

- Step 1: Match Criteria

**1 Match Criteria**

|                 |                                      |                  |
|-----------------|--------------------------------------|------------------|
| IP Prefix       | Host Pattern ?                       |                  |
| 10.242.9.100/32 | hr-portal.acme-one.com               |                  |
| Protocol        | Source Port                          | Destination Port |
| TCP             | Port number between 0-65535 or range | 8000             |
| Precedence      | Precedence number between 0-65535    |                  |

[Cancel](#) [Next](#)

- Step 2: Application Attributes

Configure > Security Service Edge > User-Defined Objects > Applications

Edit Private Application

2 Application Attributes

**Risk**  
Each application has been assessed and assigned a risk level (1 = lowest to 5 = highest) by the Versa Networks security research team. The number in each card indicates applications with the same risk.

**Productivity**  
Each application has been assessed and assigned a productivity level (1 = lowest to 5 = highest) by the Versa Networks security research team. The number in each card indicates applications with the same productivity.

**Family**

- Business-system
- Collaboration
- General-Internet
- Media
- Networking

**Sub Family**

- Antivirus
- Application-service
- Audio-Video
- Authentication
- Behavioral
- Compression
- Database
- Encrypted
- Encrypted-tunnel
- Erp
- File-server
- File-transfer
- Forum
- Game
- Instant-messaging
- Internet-utility
- Mail
- Microsoft-office
- Middleware
- Network-management
- Network-service
- Peer-to-peer
- Printer
- Routing
- Security-service
- Standard
- Telephony
- Terminal
- Thin-client
- Tunneling
- Unknown
- Wap
- Web
- Webmail

**Application Tags - Security**

- Anonymizer
- Bandwidth
- Dataleak
- Evasive
- Filetransfer
- Malware
- Misused
- Sanction State Uncategorized
- Sanctioned
- Tunnel
- Unsanctioned
- Vulnerable

**Application Tags - SDWAN**

- Audio Stream
- Data
- AV
- IPS
- Business
- Non Business
- Cloud
- Video Stream

**Application Tags - General**

- AAA
- Adult Content
- Advertising
- Analytics
- Anonymizer
- Audio Chat
- Basic
- Blog
- CDN
- Chat
- Classified\_Ads
- Cloud Services
- DB
- DEA\_Mall
- Ebook\_Reader
- Email
- Enterprise
- File Mgt
- File Transfer
- Forum
- Gaming
- IM\_MC
- IoT
- MM\_streaming
- Mobile
- Networking
- News Portal
- P2P
- Remote Access
- SCADA
- Social Network
- Standardized
- Update
- VoIP
- VPN\_tun
- Web
- Web\_Ecom
- Web Search
- Web Site
- Webmail
- Transportation

**Publish (0)**

- Step 3: Name, Description, Tags & Application Image

Configure > Security Service Edge > User-Defined Objects > Applications

Edit Private Application

Match Criteria

Application Attributes

3 Name, Description, Tags & Application Image

**Name \***  
hr-portal

**Description**  
internal HR Portal for testing

**Tags**  
HR

**Upload Application Image (Optional)**  
Add

**Cancel** **Save**

**Publish (0)**

Do the same for the other application ([financial-apps.acme-one.com](http://financial-apps.acme-one.com)) or any other one you want to test.

The private app definitions should resemble the image below.

ACME-ONE

Configure > Security Service Edge > User-Defined Objects > Applications

Private Application

Below are all the Private Application

1 hr-portal

IP Prefix: 10.242.9.100/32  
Host Pattern: hr-portal.acme-one.com  
Protocol: TCP  
Destination Port: 8000

2 ICMP-ServerVlan9

IP Prefix: 10.242.9.0/24  
Protocol: ICMP

3 financial-apps

IP Prefix: 10.242.10.100/32  
Host Pattern: financial-apps.acme-one.com  
Protocol: TCP  
Destination Port: 8000

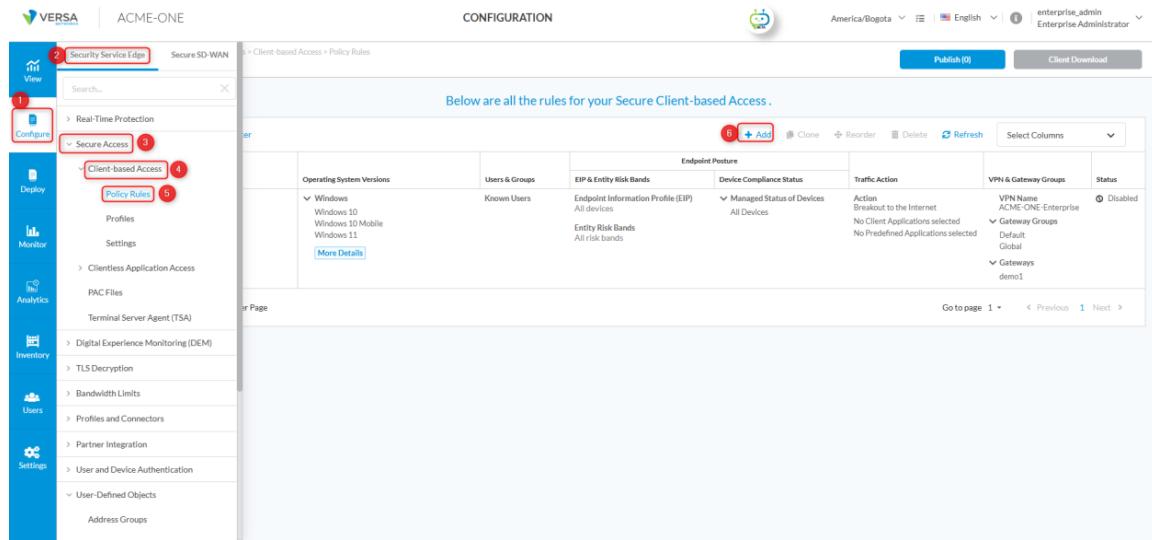
**Publish (0)**

## Step 5: Secure Client Access Rules

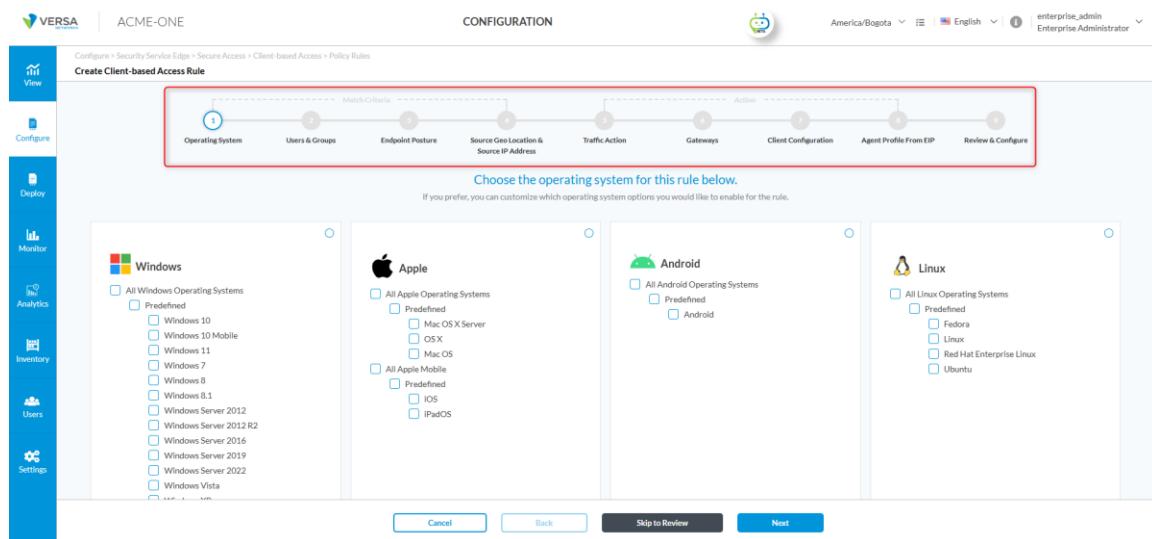
Secure Access rules define the connection between the end user machine (that is installed with Versa SASE Client) and the SASE gateway. Secure Client Access defines who, how, and under what conditions a user can connect to the gateway, including SASE client features and the type of traffic sent to the gateway. Before configuring the Secure Access Client-based Rule, ensure that the connectivity between the gateway and your authentication server is established.

To configure a secure client access rule, navigate to

**Configure > Security Service Edge > Secure Access > Client-based Access > Rules and click on +Add.**



Next, we must complete several steps by selecting all the corresponding modules we want to configure for the target users or groups (see image below).



For this example, we are setting up the secure access rule according to these requirements:

| Knob | Current Use Case | Reason | Best Practice (Production) |
|------|------------------|--------|----------------------------|
|------|------------------|--------|----------------------------|

|                                     |  |   |  |
|-------------------------------------|--|---|--|
| <b>Operating Systems</b>            | Windows 7, 10, 11  | Ensures compatibility with supported Windows OS versions in the enterprise. | Limit to <i>supported/managed OS versions only</i> (e.g., Win10/11). Block EOL OS (Win7) to reduce risk.   |
| <b>Users &amp; Groups</b>           | All required user groups (Contractors, Finance, HR, IT, VIP, etc.)         | Broad inclusion for testing.  | Apply <b>least-privilege access</b> : segment users by role and sensitivity (e.g., Finance vs. Contractors). Specific rules for each user can also be considered if each user group has different access requirements, location etc. |
| <b>Endpoint Posture</b>             | Management Status: All devices<br>EIP Profile: eip-profile-antimalware-any | Enforces the presence of anti-malware.                                      | Require managed devices and endpoint compliance where possible. Strengthens endpoint hygiene   |
| <b>Source Geo Location</b>          | All  | No geo-restriction defined.   | Restrict access to <b>approved geographies</b> where the company operates. Deny or challenge high-risk regions.  |
| <b>Source IP Address</b>            | None   | As users are remote   | We can define an IP address to enforce the user connection from a specific location and a WAN circuit.   |
| <b>Traffic Action</b>               | VSPA (Secure Private Access)   | Secure access to internal applications.                                     | Same as lab.   |
| <b>Gateways</b>                     | Single gateway in the lab  | Select the gateway that we want the user to connect to                      | Select gateways according to the type of user and the regional gateways that will serve them, ensuring that a redundant gateway is always included in the rule to guarantee high availability and low latency.                       |
| <b>Client Configuration</b>         | Define routes and DNS resolvers  | Ensures reachability of internal resources and split-DNS.                   | Same as lab. Add redundancy with <b>multiple DNS resolvers</b> .   |
| <b>Secure Client Access Profile</b> | Secure-Access-Profile-1  | Select the profile created in step 3  | Same as lab  |
| <b>MFA</b>                          | Disabled   | Not required in the lab.  | <b>Enable MFA</b> (Email or TOTP as per the requirement). Critical for Zero Trust.   |
| <b>VPN Type</b>                     | All (IPsec, TLS, DTLS)   | Flexibility during lab testing.   | Define the order of preference (Recommended: DTLS > IPsec > TLS).  |
| <b>Client Controls</b>              | Default values   | Defaults are sufficient for the lab use case.                               | Harden controls (Tamper Protection, Tunnel Monitoring, Always-   |

|                          |   |                      |  |
|--------------------------|---|----------------------|--|
|                          |   |                      | On with Trusted Network Detection).  |
| <b>EIP Agent Profile</b> | Blank (example: AntiMalware_category_all) | Optional in the lab. | To enforce real-time posture evaluation with EIP. Continuous evaluation is key for Zero Trust. |

Now, we need to complete the 9 steps as follows:

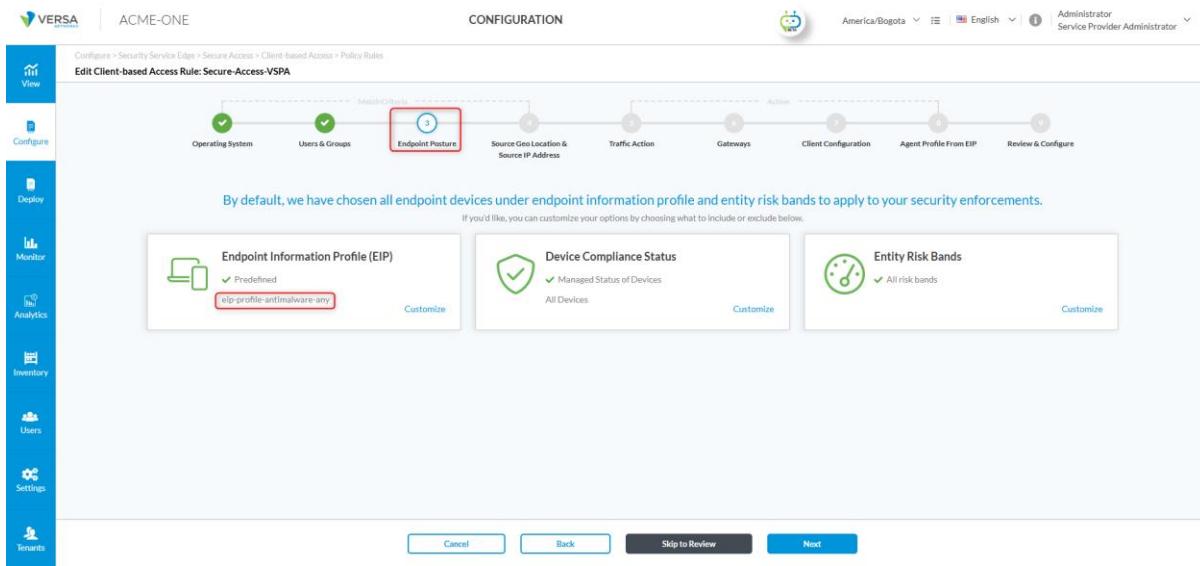
- 1. Operating System:** Select Windows and choose the versions to be tested: **Windows OS** (7, 10, and 11).

The screenshot shows the 'Edit Client-based Access Rule: Secure-Access-VSPA' configuration process. The 'Operating System' step is highlighted with a red box. A red arrow points to the 'Windows' section, which is selected. The interface shows checkboxes for various Windows and Apple operating systems.

- 2. Users & Groups:** Select the groups (**contractors, finance, general, hr, it, low, and vip**).

The screenshot shows the 'Edit Client-based Access Rule: Secure-Access-VSPA' configuration process. The 'Users & Groups' step is highlighted with a red box. A red arrow points to the 'User Groups' list, which includes 'contractors', 'finance', 'general', 'hr', 'it', 'low', 'regular', and 'vip'.

**3. Endpoint Posture:** The predetermined profile eip-profile-antimalware-any has been selected. This profile is characterized by a rule that incorporates two objects (eip-object-antimalware-any-installed and eip-object-antimalware-any-running), which are assessed using an AND condition. During the pre-registration process, information gathered from the client is validated against this EIP profile to decide whether access is permitted or denied based on the results. For more details about EIP profiles, refer to **Appendix C – User Defined Objects and Endpoint Information Profiles**.



ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure-Access-VSPA

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements. If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

✓ Predefined

eip-profile-antimalware-any

Customize

Device Compliance Status

✓ Managed Status of Devices

All Devices

Customize

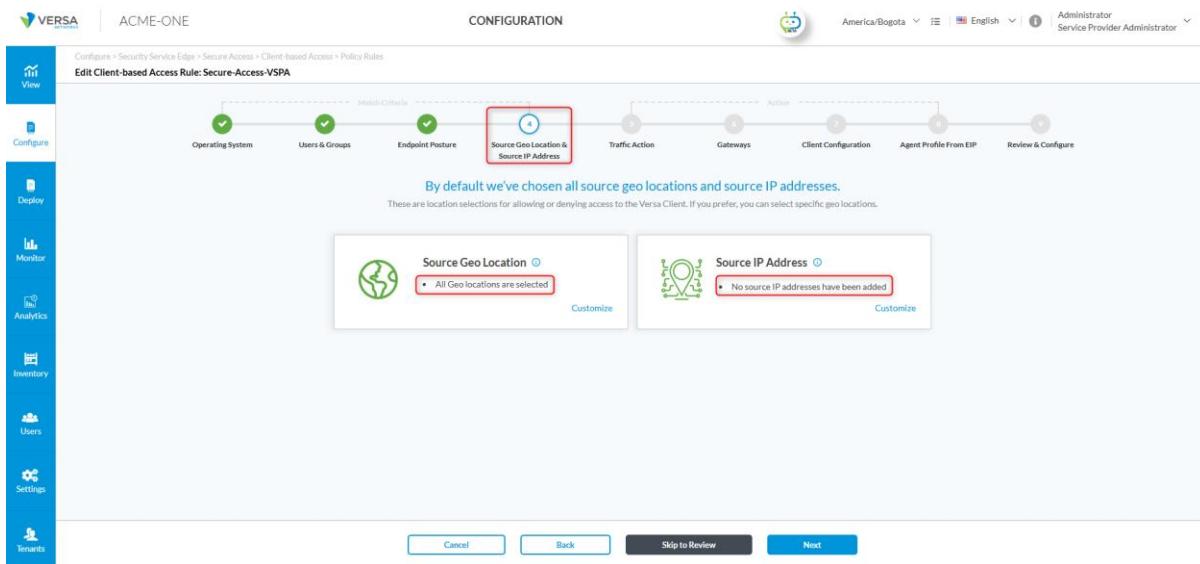
Entity Risk Bands

✓ All risk bands

Customize

Cancel | Back | Skip to Review | Next

**4. Source Geo Location & Source:** Default values are used since the use case is LAB



ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure-Access-VSPA

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

By default we've chosen all source geo locations and source IP addresses. These are location selections for allowing or denying access to the Versa Client. If you prefer, you can select specific geo locations.

Source Geo Location

All Geo locations are selected

Customize

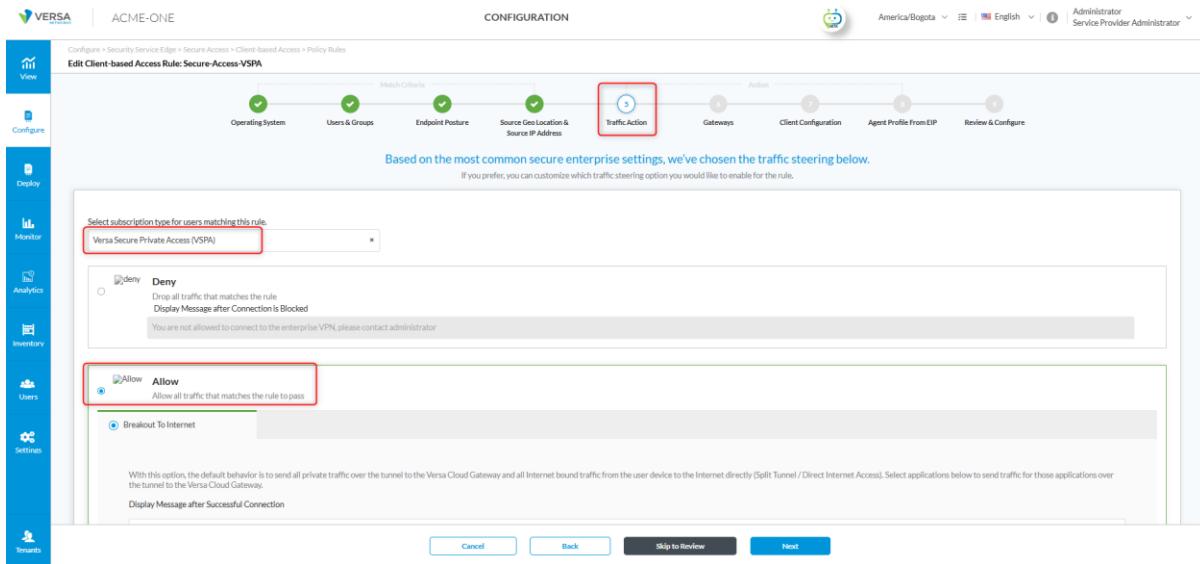
Source IP Address

No source IP addresses have been added

Customize

Cancel | Back | Skip to Review | Next

**5. Traffic Action:** The subscription type selected is **Versa Secure Private Access (VSPA)**.



ACME-ONE

CONFIGURATION

Edit Client-based Access Rule: Secure-Access-VSPA

Based on the most common secure enterprise settings, we've chosen the traffic steering below.

Select subscription type for users matching this rule: Versa Secure Private Access (VSPA)

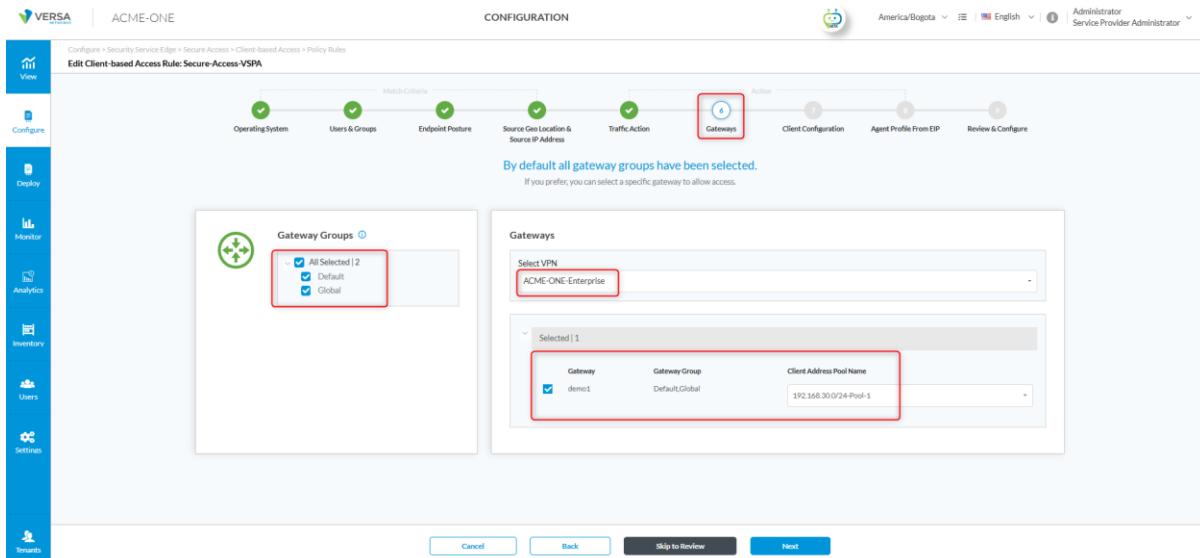
Deny: Drop all traffic that matches the rule. Display Message after Connection Is Blocked: You are not allowed to connect to the enterprise VPN, please contact administrator.

Allow: Allow all traffic that matches the rule to pass.

Breakout To Internet: With this option, the default behavior is to send all private traffic over the tunnel to the Versa Cloud Gateway and all Internet bound traffic from the user device to the Internet directly (Split Tunnel / Direct Internet Access). Select applications below to send traffic for those applications over the tunnel to the Versa Cloud Gateway. Display Message after Successful Connection:

Cancel Back Skip to Review Next

**6. Gateways:** Select the gateway groups and mark the gateways to be associated with the rule. Since there is only one gateway in our case, we selected it only.



ACME-ONE

CONFIGURATION

Edit Client-based Access Rule: Secure-Access-VSPA

By default all gateway groups have been selected. If you prefer, you can select a specific gateway to allow access.

Gateway Groups:  All Selected | 2  Default  Global

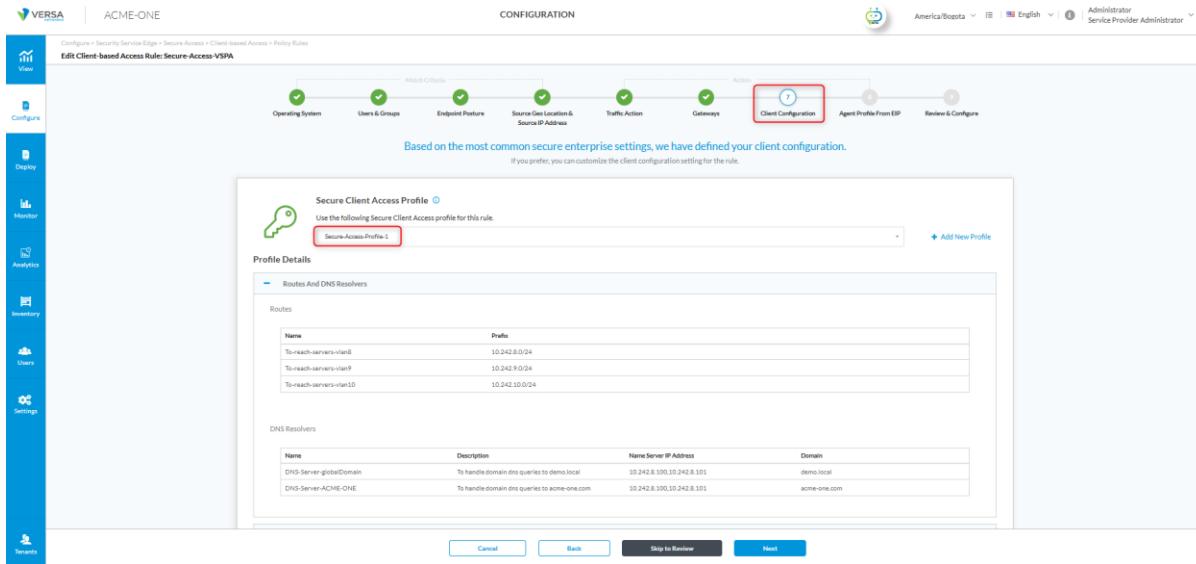
Gateways: Select VPN: ACME-ONE-Enterprise

Selected | 1: 

| Gateway | Gateway Group  | Client Address Pool Name |
|---------|----------------|--------------------------|
| demo1   | Default,Global | 192.168.30.0/24-Pool-1   |

Cancel Back Skip to Review Next

**7. Client Configuration:** Select the previously created Secure Client Access profile (Secure-Access-Profile-1).



Based on the most common secure enterprise settings, we have defined your client configuration. If you prefer, you can customize the client configuration setting for the rule.

**Secure Client Access Profile**

Use the following Secure Client Access profile for this rule.

**Secure-Access-Profile-1**

**Profile Details**

**Routes And DNS Resolvers**

**Routes**

| Name                    | Prefix         |
|-------------------------|----------------|
| To-reach-servers-vlan8  | 10.242.8.0/24  |
| To-reach-servers-vlan9  | 10.242.9.0/24  |
| To-reach-servers-vlan10 | 10.242.10.0/24 |

**DNS Resolvers**

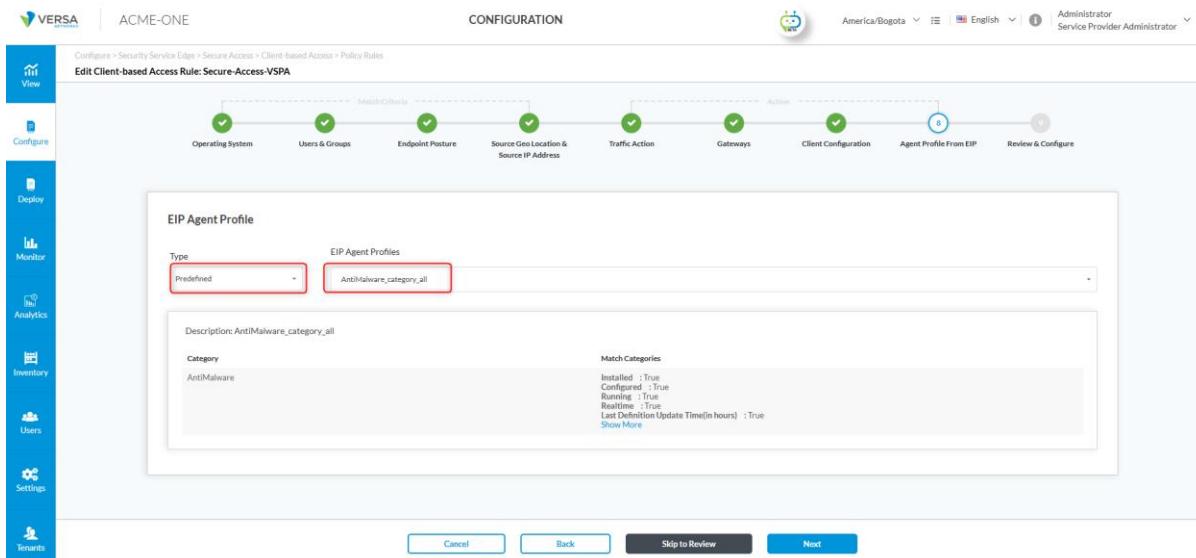
| Name                    | Description                                  | Name Server IP Address    | Domain       |
|-------------------------|--|---------------------------|--------------|
| DNS-server-globalDomain | To handle domain dns queries to demo-local   | 10.242.8.100,10.242.8.101 | demo-local   |
| DNS-Server-ACME-ONE     | To handle domain dns queries to acme-one.com | 10.242.8.100,10.242.8.101 | acme-one.com |

**Client Configuration**

**Agent Profile From EIP**

**Review & Configure**

**8. Agent Profile From EIP:** Select the predefined type, and in EIP Agent Profile, choose Antimalware\_category\_all.



**EIP Agent Profile**

**Type**

Predefined

**EIP Agent Profiles**

AntMalware\_category\_all

**Description:** AntiMalware\_category\_all

**Category**

AntiMalware

**Match Categories**

- Installed : True
- Configured : True
- Running : True
- Realtime : True
- Last Scan Update Time(in hours) : True
- Show More

**Client Configuration**

**Agent Profile From EIP**

**Review & Configure**

**9. Review & Configure:** Once the configuration is complete, it should resemble the example shown in the image below.

**Edit Client-based Access Rule: Secure Access Policy 1**



**Review your Client-based Access Rule Configurations below**  
Below are the configurations for your rule. Review and edit any step of your configuration before deploying.

**General**

Name:  Description:

Tags:  Rule is Enabled:

**Operating Systems** [Edit](#)

Operating System Versions: [Custom Selection](#)

- Windows 14
- Windows 10
- Windows 10 Mobile
- Windows 11
- Windows 7

**Users & Groups** [Edit](#)

Users & Groups: AD-DC1

User Groups: 8

- contractors
- finance
- general
- hr
- it
- law
- regular
- vo

**Endpoint Posture** [Edit](#)

Device Compliance Status: All Devices

Endpoint Information Profile (EIP): Preferred: 1

| Name                         | Description                  | Rule |
|------------------------------|------------------------------|------|
| eip-profile-anti-malware-any | eip-profile-anti-malware-any |      |

Entity Risk Bands: All risk bands

**Source Geo Location and Source IP Address** [Edit](#)

Source:  All source Geo locations are selected

**Traffic Action** [Edit](#)

Action Selected: split tunnel

Subscription: Versa Secure Private Access (VSPA)

Custom Applications: [Custom Selection](#)

Custom Applications: 1

- DEM Monitoring Interface

**Gateways** [Edit](#)

Selected VPN: ACME ONE Enterprise

Gateways:  All Gateways selected

Gateway Groups:  All Gateway Groups selected

**Client Configuration** [Edit](#)

Profile Name: Secure Access Profile 1

| VPN Type | Type    | Status | Order |
|----------|---------|--------|-------|
| IPsec    | Enabled | 3      |       |
| TLS      | Enabled | 1      |       |
| DTLS     | Enabled | 2      |       |

Client Controls:  Allow Client Customization

MFA Authenticator Service: Not Selected

**EIP Agent Profile** [Edit](#)

Prediction: AntiMalware\_category\_all

## Step 6: Configure TLS Decryption Rules and Profiles

TLS Decryption facilitates the inspection of encrypted HTTPS traffic routed to Versa via the SASE client. This capability enables administrators to specify which websites should undergo decryption, thereby providing visibility into the payload and supporting advanced security functionalities such as Intrusion Prevention Systems (IPS), anti-malware, and Data Loss Prevention (DLP). Decryption profiles further allow the specification of certificates, the enforcement of TLS

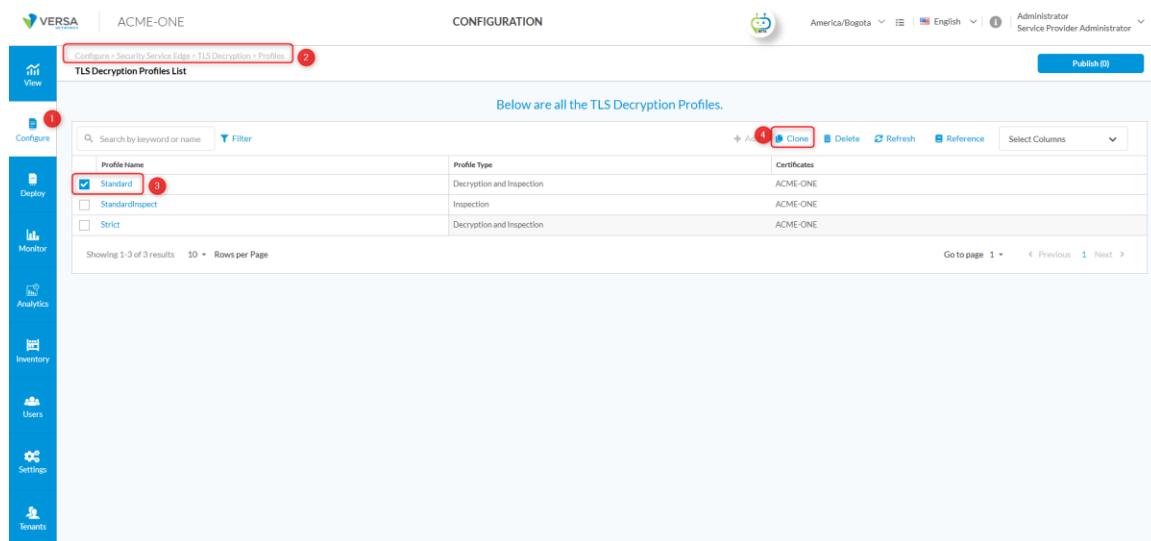
version restrictions, the activation of OCSP verification, and the customization of additional settings to ensure secure traffic inspection.

In our scenario, we will create a decryption profile that conducts standard inspection without OCSP verification, as this pertains solely to VSPA where OCSP verification may not be necessary. This can be accomplished by cloning the Standard profile and disabling the OCSP verification option. Moreover, we will establish two TLS decryption rules: one to decrypt traffic to hr-portal.acme-one.com, and another to bypass decryption (i.e., "Do Not Decrypt") for traffic directed to financial-apps.acme-one.com.

Navigate to the following path and configure the appropriate decryption profile:

### Configure > Security Service Edge > TLS Decryption > Profiles

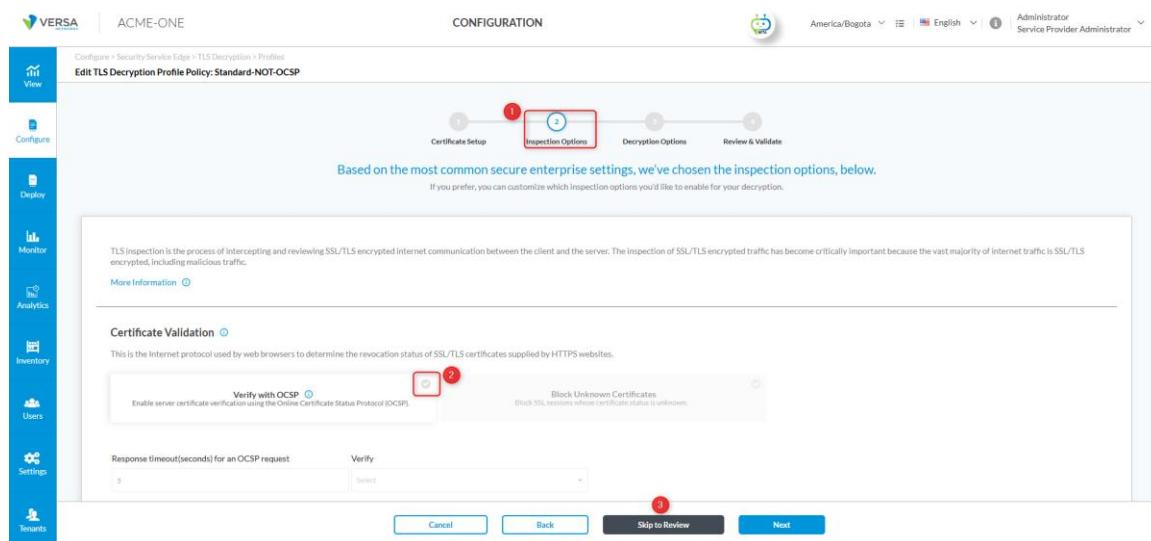
Select the *Standard* profile, then click **Clone** to create a copy. Modify the cloned profile by disabling **OCSP verification**, as it will not be used with self-signed certificates in this lab environment.



The screenshot shows the 'TLS Decryption Profiles List' page. On the left, a sidebar lists 'View', 'Configure' (which is selected and highlighted in blue), 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants'. The main content area has a header 'CONFIGURATION' and a sub-header 'TLS Decryption Profiles List'. It displays a table with three rows:

| Profile Name                                 | Profile Type              | Certificates |
|--|---------------------------|--------------|
| <input checked="" type="checkbox"/> Standard | Decryption and Inspection | ACME-ONE     |
| <input type="checkbox"/> StandardInspect     | Inspection                | ACME-ONE     |
| <input type="checkbox"/> Strict              | Decryption and Inspection | ACME-ONE     |

Below the table, there are buttons for 'Add', 'Clone' (highlighted with a red box), 'Delete', 'Refresh', 'Reference', and 'Select Columns'. At the bottom, there are links for 'Go to page 1', 'Previous', 'Next', and 'Rows per Page' (set to 10).



The screenshot shows the 'Edit TLS Decryption Profile Policy: Standard-NOT-OCSP' page. The left sidebar is identical to the previous screenshot. The main content area has a header 'CONFIGURATION' and a sub-header 'Edit TLS Decryption Profile Policy: Standard-NOT-OCSP'. It shows a progress bar with four steps: 'Certificate Setup' (1), 'Inspection Options' (2, highlighted with a red box), 'Decryption Options' (3), and 'Review & Validate' (4). A message says 'Based on the most common secure enterprise settings, we've chosen the inspection options, below.' Below this, a note says 'TLS inspection is the process of intercepting and reviewing SSL/TLS encrypted internet communication between the client and the server. The inspection of SSL/TLS encrypted traffic has become critically important because the vast majority of internet traffic is SSL/TLS encrypted, including malicious traffic.' There is a 'More Information' link. The 'Inspection Options' step shows a 'Certificate Validation' section with a note about OCSP. A checkbox 'Verify with OCSP' (highlighted with a red box) is checked, and a sub-note says 'Enable server certificate verification using the Online Certificate Status Protocol (OCSP)'. Below this, there is a 'Response timeout(seconds) for an OCSP request' input field with a value of 5, and a 'Verify' button. At the bottom, there are 'Cancel', 'Back', 'Skip to Review' (highlighted with a red box), and 'Next' buttons.

Now we can create our TLS Decryption rules — one to inspect traffic to hr-portal.acme-one.com and another to bypass decryption for financial-apps.acme-one.com.

## TLS Decryption Rule 1:

Navigate to the following path to create the rule:

**Configure > Security Service Edge > TLS Decryption > Policy Rules**

**Click + Add**, then complete the six configuration steps and save the rule. The final configuration should resemble the image below.

Review your TLS Decryption Rule configurations below  
Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

### General

Name\*  Description

Tags

Rule is Enabled

### Applications & URLs

[Edit](#)

Applications Custom Selection

Applications | 1  
hr-portal

### Decryption Enforcement

[Edit](#)

Rule Type: Decrypt traffic and inspect the server certificate  
Bypass Decryption for URL profiles: None Selected  
Profile: Standard-NOT-OCSP

### Users & Groups

[Edit](#)

Users & Groups All Users Users Device Groups All Device Groups

### Endpoint Posture

[Edit](#)

### Network Layer 3-4

[Edit](#)

Services  All Services

destination

Zones | 3  
DC-Tunnel-01  
Internet  
SD-WAN Zone

## TLS Decryption Rule 2:

Navigate to the following path to create the rule:

**Configure > Security Service Edge > TLS Decryption > Policy Rules**

**Click + Add**, then complete the six configuration steps and save the rule. The final configuration should resemble the image below.

Review your TLS Decryption Rule configurations below  
Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

**General**

|  |  |
|--|--|
| Name* <input type="text" value="Do-Not-Decrypt-Financial-Apps"/> | Description <input type="text" value="to ssl bypass financial-apps.acme-one.com"/> |
| Tags <input type="text" value="Press Enter to add"/>             |  |
| <input checked="" type="checkbox"/> Rule Is Enabled              |  |

**Applications & URLs** [Edit](#)

Applications Custom Selection

- Applications | 1  
financial-apps

**Decryption Enforcement** [Edit](#)

|                         |                            |
|-------------------------|----------------------------|
| Rule Type               | Do Not Decrypt             |
| Inspect Traffic Enabled | Do not Inspect the Traffic |

**Users & Groups** [Edit](#)

Users & Groups **All Users** Users Device Groups **All Device Groups**

**Endpoint Posture** [Edit](#)

**Network Layer 3-4** [Edit](#)

Services  All Services

**destination**

- Zones | 3  
DC-Tunnel-01  
Internet  
SD-WAN Zone

Finally, configure the TLS Decryption Rules stack as shown in the image below.

ACME-ONE CONFIGURATION

Configure > Security Service Edge > TLS Decryption > Policy Rules

**TLS Decryption Rules List**

Below are all the TLS Decryption Rules

| Rule Name  | Decryption Profile                             | Bypass URL Filtering Profile | Applications & URLs                                   | Users & Groups | Endpoint Posture                                  | Source & Destination  | Services             | Schedule      | Status                                       |
|--|--|------------------------------|---|----------------|---|---|----------------------|---------------|--|
| <input type="checkbox"/> Do-Not-Decrypt-Financial-Apps | Do not decrypt and do not inspect the traffic. | None Selected                | ▼ Application<br>financial-apps                       | All Users      | Endpoint Information Profile (EIP)<br>All devices | ▼ Destination Zone<br>DC-Tunnel-01<br>Internet<br>SD-WAN Zone | All Layer 4 Services | Not Available | <span style="color: green;">● Enabled</span> |
| <input type="checkbox"/> Decrypt-HR-Portal             | Standard-NOT-OCSP                              | None Selected                | ▼ Application<br>hr-portal                            | All Users      | Endpoint Information Profile (EIP)<br>All devices | ▼ Destination Zone<br>DC-Tunnel-01<br>Internet<br>SD-WAN Zone | All Layer 4 Services | Not Available | <span style="color: green;">● Enabled</span> |
| <input type="checkbox"/> decrypt_all                   | Standard                                       | None Selected                | All Applications                                      | All Users      | Endpoint Information Profile (EIP)<br>All devices | ▼ Destination Zone<br>Internet                                | All Layer 4 Services | Not Available | <span style="color: green;">● Enabled</span> |
| <input type="checkbox"/> StandardInspect               | Standard                                       | None Selected                | ▼ Reputations<br>trustworthy<br>low_risk              | All Users      | Endpoint Information Profile (EIP)<br>All devices |   | All Layer 4 Services | Not Available | <span style="color: gray;">● Disabled</span> |
| <input type="checkbox"/> RiskyWebsites                 | Strict   | None Selected                | ▼ Reputations<br>high_risk<br>suspicious<br>undefined | All Users      | Endpoint Information Profile (EIP)<br>All devices |   | All Layer 4 Services | Not Available | <span style="color: gray;">● Disabled</span> |

Showing 1-5 of 5 results Rows per Page

Go to page 1 < Previous 1 Next >

## Step 7: Configure Real-Time Protection (Private App Protection) Rules

To begin, make sure that the Private Applications from Step 4 have been configured. For this example, we will use the test applications hr-portal.acme-one.com and financial-apps.acme-one.com.

Next, we need to create Real-time Private Protection policies for our test users accessing the previously defined private apps, as follows:

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Private App Protection,**

**click on +Add** (Click on Let's Go, if this is your first Private App Rule). Each private protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR 'ed and on different tabs is 'AND'.

- For this example, we are setting up the rule according to these requirements:
- Applications: (financial apps and hr-portal)
- Users & Groups: vip from (AD-DC1)
- Endpoint Posture: default (All Devices)
- Source & Destination: default (DC-Tunnel-01 and SD-WAN Zone)
- Services: default (All layer 4 Services)
- Schedule: default (Not available – meaning no restrictions)
- Geo locations: default (all Source and Destinations)
- Security Enforcement:
  - Malware Protection: predefined (Easy Malware Protection)
  - IPS: predefined (Windows OS Protection)

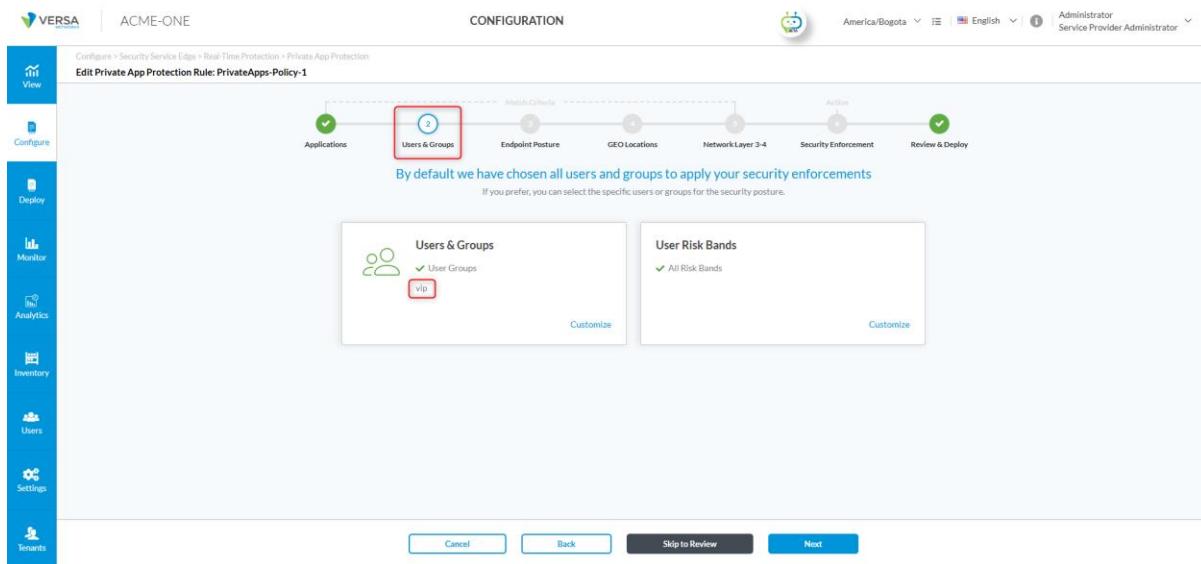
| Knob | Required Setting<br>(Lab Example) | Reason / Rationale | Best Practice (Production) |
|------|-----------------------------------|--------------------|----------------------------|
|------|-----------------------------------|--------------------|----------------------------|

|                                 |  |  |   |
|---------------------------------|--|--|---|
| <b>Applications</b>             | Financial Apps, HR-Portal              | Focuses on protecting sensitive business apps.         | Expand to <b>all critical private apps</b> . Use app tags/groups for scalability.                                     |
| <b>Users &amp; Groups</b>       | vip (from AD-DC1)                      | Targets high-value users (execs/VIPs).                 | Apply <b>role-based segmentation</b> (e.g., Finance group → Finance apps). Enforce least privilege across all groups. |
| <b>Endpoint Posture</b>         | Default (All Devices)                  | Ensures the rule applies to any device in lab testing. | Require <b>managed devices</b> and enforce <b>anti-malware, patch, and disk encryption posture</b> .                  |
| <b>Source &amp; Destination</b> | Default (DC-Tunnel-01 and SD-WAN Zone) | Matches common DC/branch paths.                        | Narrow to <b>specific zones/tunnels</b> for critical apps. Apply segmentation to reduce lateral movement.             |
| <b>Services</b>                 | Default (All Layer 4 Services)         | Simplifies setup; covers all protocols.                | Restrict to <b>specific ports/protocols</b> used by the protected apps.   |
| <b>Schedule</b>                 | Default (Always active)                | Keeps enforcement continuous and straightforward.      | Optionally apply <b>time-based restrictions</b> for contractor access or as required.                                 |
| <b>Geo Locations</b>            | Default (All Source & Destinations)    | No geo-restriction in the lab.                         | Restrict to <b>approved operating regions</b> . Block or challenge high-risk geos.                                    |
| <b>Malware Protection</b>       | Predefined: Easy-Malware Protection    | Provides baseline anti-malware scanning.               | Predefined is recommended for most production cases.  |
| <b>IPS</b>                      | Predefined: Windows OS Protection      | Applies IPS tuned for Windows OS threats.              | Use predefined IPS profiles based on the requirement and environment. Use "Versa-Recommended" if unsure.              |

Now, we need to complete the 7 steps as follows:

## 1. Applications: Select the previously created applications: **Financial-apps** and **HR-Portal**.

## 2. Users & Groups: Select the vip group for our example.



Configure > Security Service Edge > Real-Time Protection > Private App Protection

Edit Private App Protection Rule: PrivateApps-Policy-1

CONFIGURATION

Administrator Service Provider Administrator

Applications

Users & Groups

Endpoint Posture

GEO Locations

Network Layer 3-4

Security Enforcement

Action

Review & Deploy

By default we have chosen all users and groups to apply your security enforcements

If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

User Groups

vip

User Risk Bands

All Risk Bands

Customize

Customize

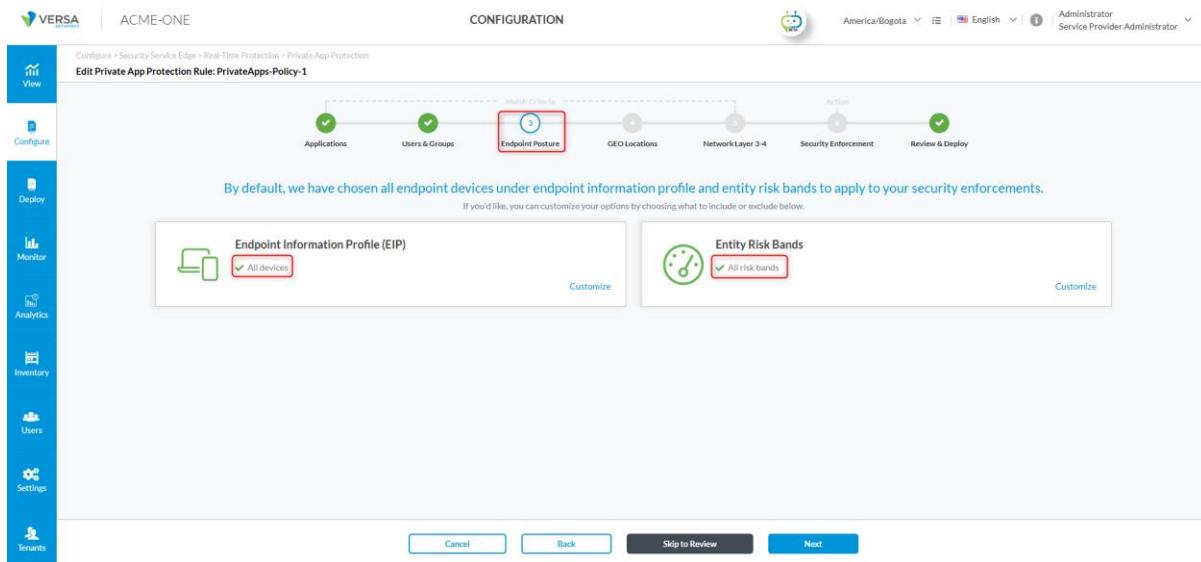
Cancel

Back

Skip to Review

Next

## 3. Endpoint Posture: Default values are used.



Configure > Security Service Edge > Real-Time Protection > Private App Protection

Edit Private App Protection Rule: PrivateApps-Policy-1

CONFIGURATION

Administrator Service Provider Administrator

Applications

Users & Groups

Endpoint Posture

GEO Locations

Network Layer 3-4

Security Enforcement

Action

Review & Deploy

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

All devices

Entity Risk Bands

All risk bands

Customize

Customize

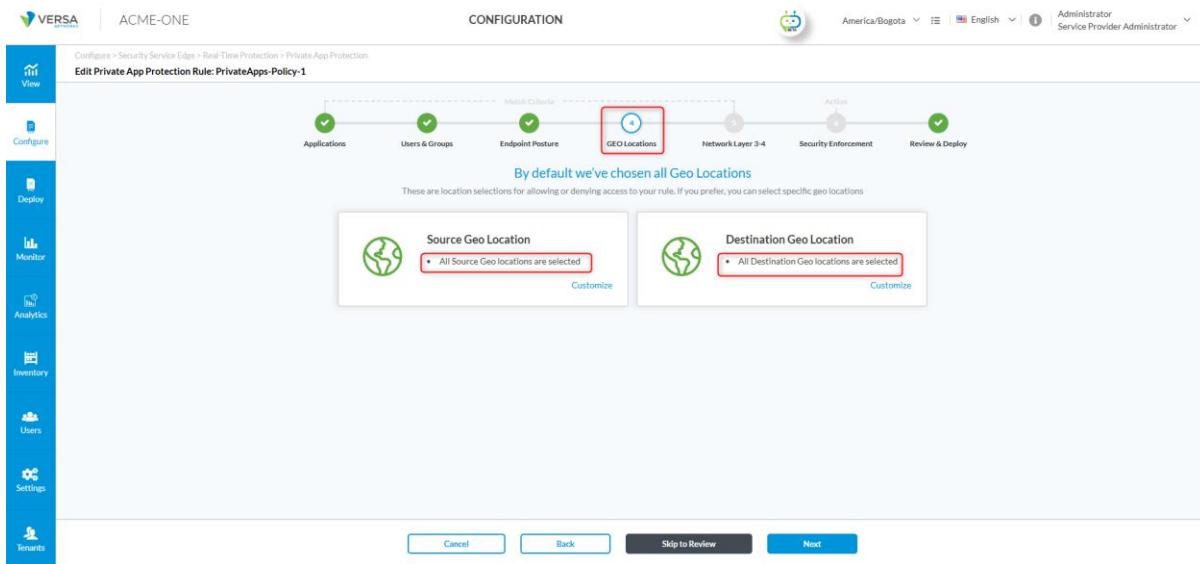
Cancel

Back

Skip to Review

Next

## 4. Geo Locations: Default values are used.



ACME-ONE

CONFIGURATION

Edit Private App Protection Rule: PrivateApps-Policy-1

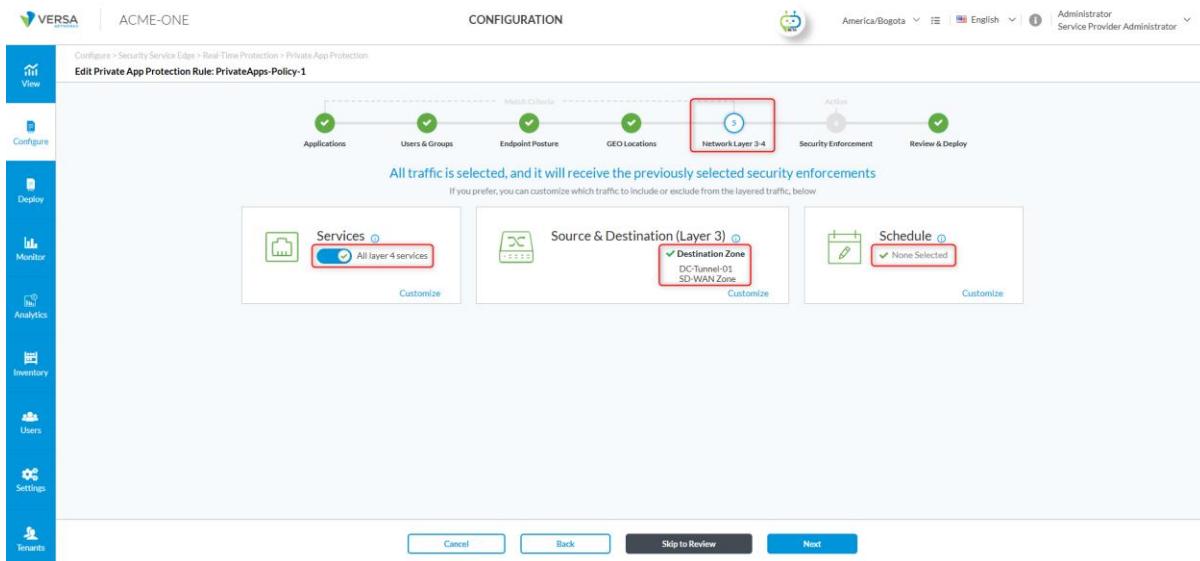
Applications    Users & Groups    Endpoint Posture    **GEO Locations**    Network Layer 3-4    Security Enforcement    Review & Deploy

By default we've chosen all Geo Locations  
These are location selections for allowing or denying access to your rule. If you prefer, you can select specific geo locations

Source Geo Location: All Source Geo locations are selected  
Destination Geo Location: All Destination Geo locations are selected

Cancel    Back    Skip to Review    Next

## 5. Network Layer 3-4: Default values are used.



ACME-ONE

CONFIGURATION

Edit Private App Protection Rule: PrivateApps-Policy-1

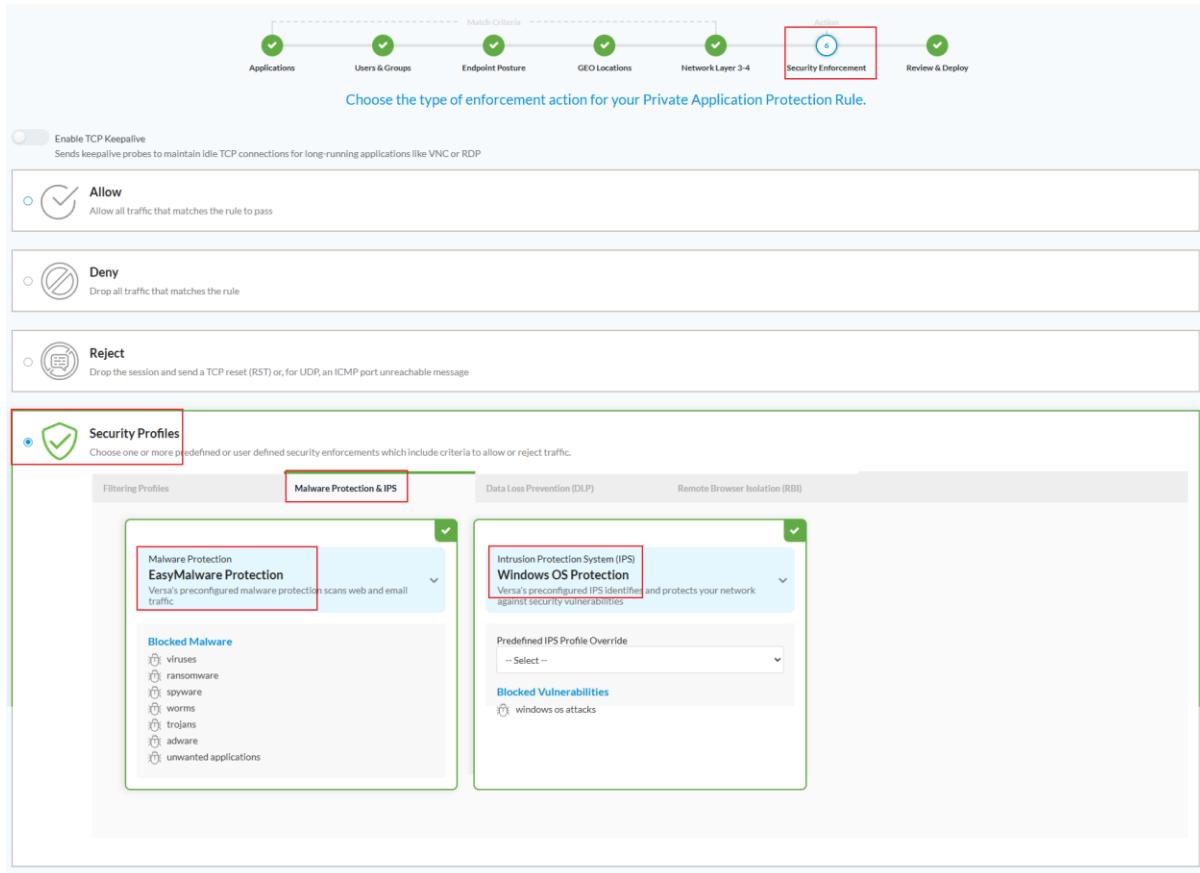
Applications    Users & Groups    Endpoint Posture    GEO Locations    **Network Layer 3-4**    Security Enforcement    Review & Deploy

All traffic is selected, and it will receive the previously selected security enforcements  
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services: All layer 4 services  
Source & Destination (Layer 3): Destination Zone: DC-Tunnel-01, SD-WAN Zone  
Schedule: None Selected

Cancel    Back    Skip to Review    Next

## 6. Security Enforcement: Select the checkbox (Security Profiles). Then, click on the second tab Malware Protection & IPS and select Malware Protection: **EasyMalware Protection** and Intrusion Protection System (IPS): **Windows OS Protection**.



Choose the type of enforcement action for your Private Application Protection Rule.

Enable TCP Keepalive  
Sends keepalive probes to maintain idle TCP connections for long-running applications like VNC or RDP

Allow  
Allow all traffic that matches the rule to pass

Deny  
Drop all traffic that matches the rule

Reject  
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

Security Profiles  
Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Filtering Profiles      Malware Protection & IPS      Data Loss Prevention (DLP)      Remote Browser Isolation (RBI)

**Malware Protection & IPS**

- EasyMalware Protection**  
Versa's preconfigured malware protection scans web and email traffic.
- Windows OS Protection**  
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities.

**Blocked Malware**

- viruses
- ransomware
- spyware
- worms
- trojans
- adware
- unwanted applications

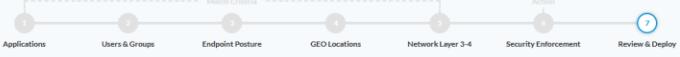
**Blocked Vulnerabilities**

- windows os attacks

**7. Review & Deploy:** Once the configuration is complete, it should resemble the example shown in the image below.

Configure > Security Service Edge > Real-Time Protection > Private App Protection

Edit Private App Protection Rule: PrivateApps-Policy-1



Review your Private App Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

**General**

Name\*  Description

Tags

Rule is Enabled

**Applications**

Applications Custom Selection

Applications 1 2  financial-apps  hr-portal

**Users & Groups**

Users & Groups AD-DC1

User Risk Bands All Risk Bands

User Group | 1  Name  vip

**Endpoint Posture**

**GEO Locations**

Source  All source Geo locations are selected

Destination  All destination Geo locations are selected

**Network Layer 3-4**

Services  All Services

destination  DC-Tunnel-01

zones  SD-WAN Zone

**Security Enforcement**

Enforcements  EasyURLFiltering

EasyMalware Protection

Windows OS Protection

Versa's preconfigured URL filters controls all web-browsing activity

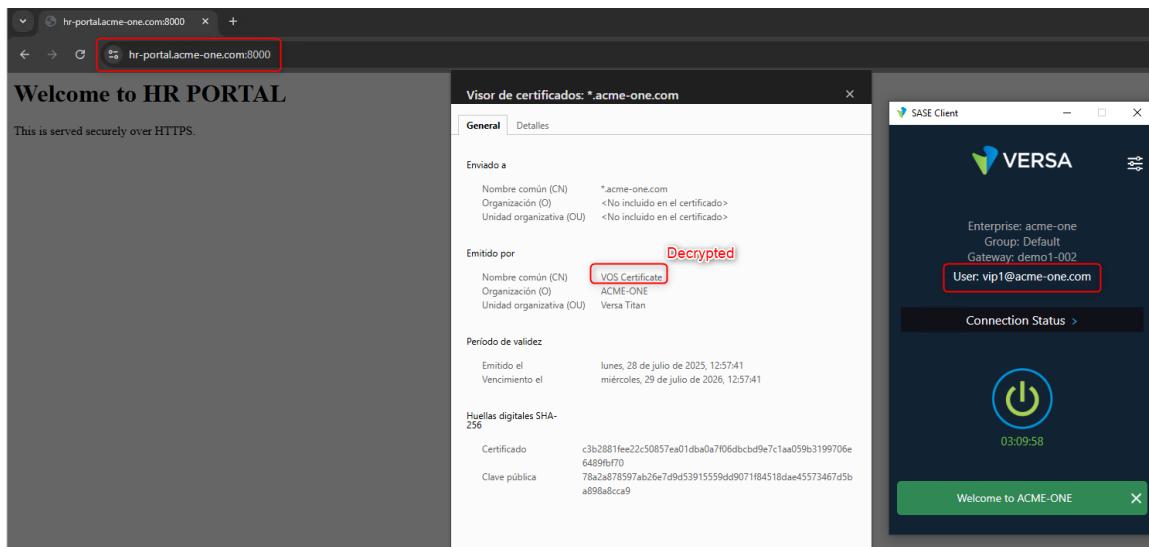
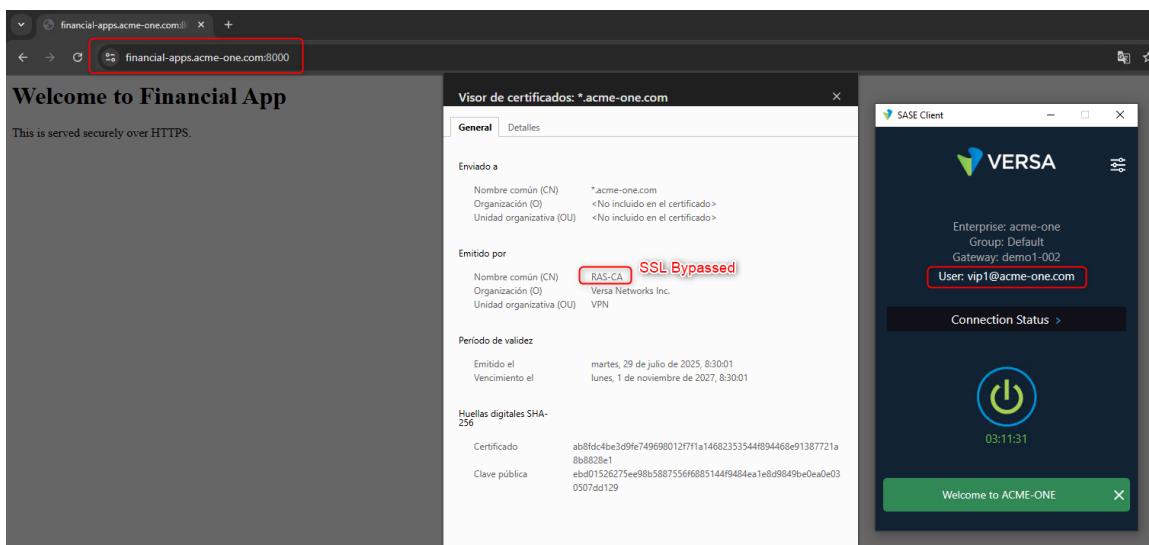
Versa's preconfigured malware protection scans web and email traffic

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

## Step 8: Test and Verification

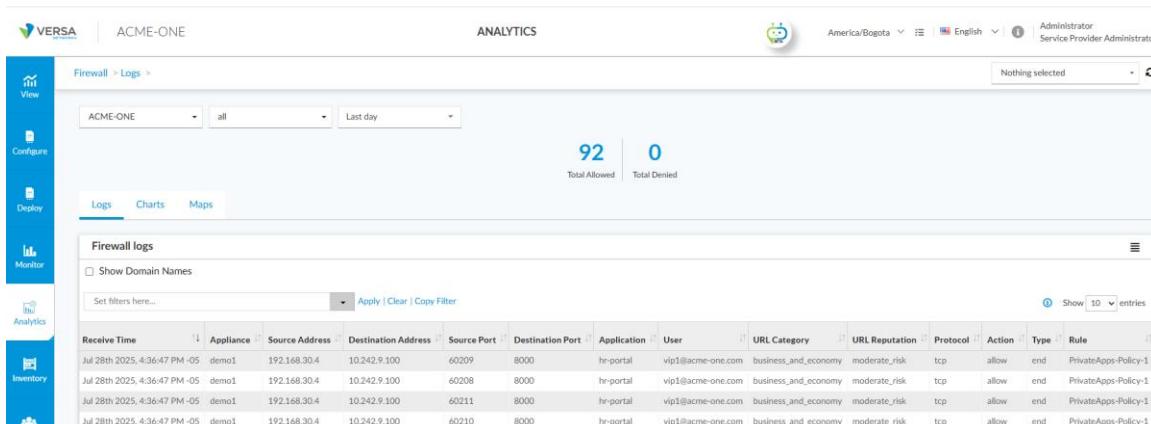
**Important:** All the changes made in the previous steps must be **published from Concerto** in order for the Gateway to apply the configuration.

User connected to ACME-ONE PORTAL and can access the private apps.

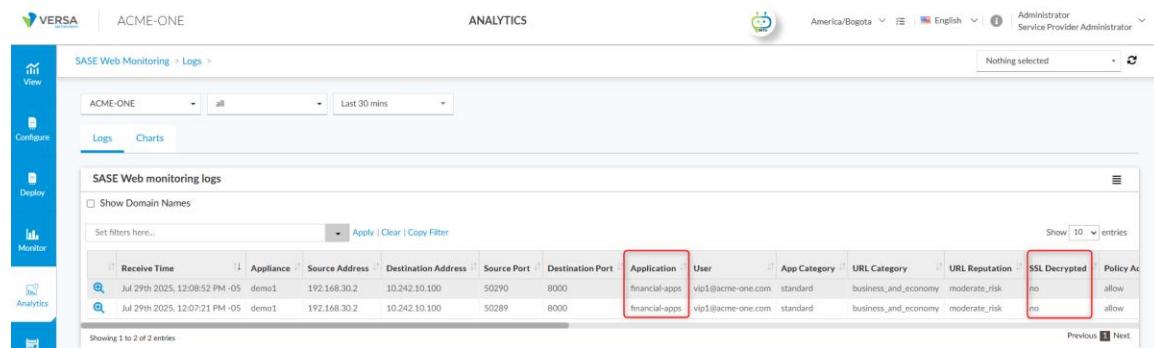



Logs from Analytics:

HR-PORTAL.ACME-ONE.COM



## FINANCIAL-APPS.ACME-ONE.COM (SSL Bypassed)



The screenshot shows the VERSA Analytics interface with the following details:

**Header:** ACME-ONE, ANALYTICS, America/Bogota, English, Administrator, Service Provider Administrator

**Left Sidebar:** View, Configure, Deploy, Monitor, Analytics

**Page Title:** SASE Web Monitoring > Logs

**Filter Bar:** ACME-ONE, all, Last 30 mins

**Log Types:** Logs (selected), Charts

**Table Headers:** Receive Time, Appliance, Source Address, Destination Address, Source Port, Destination Port, Application, User, App Category, URL Category, URL Reputation, SSL Decrypted, Policy Action

**Table Data:**

| Receive Time                   | Appliance | Source Address | Destination Address | Source Port | Destination Port | Application    | User              | App Category | URL Category         | URL Reputation | SSL Decrypted | Policy Action |
|--------------------------------|-----------|----------------|---------------------|-------------|------------------|----------------|-------------------|--------------|----------------------|----------------|---------------|---------------|
| Jul 29th 2025, 12:08:52 PM -05 | demo1     | 192.168.30.2   | 10.242.10.100       | 50290       | 8000             | financial-apps | vip1@acme-one.com | standard     | business_and_economy | moderate_risk  | No            | allow         |
| Jul 29th 2025, 12:07:21 PM -05 | demo1     | 192.168.30.2   | 10.242.10.100       | 50289       | 8000             | financial-apps | vip1@acme-one.com | standard     | business_and_economy | moderate_risk  | No            | allow         |

**Table Footer:** Showing 1 to 2 of 2 entries, Previous, Next

# Appendix A – S2S IPsec VPN EBGP Configuration

## Overview

When multiple tunnels exist between your enterprise and the SASE gateways, you should leverage a dynamic routing protocol to provide redundancies and path preferences. Versa SASE gateways support EBGP protocol as the dynamic routing protocol for this purpose.

For optimal routing control and security, it is recommended that both export and import policies be utilized to limit routing table entries to only those required.

## BGP Peer Policy Configuration

BGP peer policies consist of one or more terms for filtering BGP routes received from remote BGP peers or those advertised to them. You can configure import policies to modify or reject routes coming from remote BGP peers and export policies to apply regulations to routes advertised to BGP peers. Once you configure BGP peer policies, you will use them when setting up site-to-site tunnels.

## Configuring BGP Peer Policy

Refer to the following Versa Docs for BGP Peer Policy Configuration:-

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_BGP\\_Peer\\_Policies](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_BGP_Peer_Policies)

Navigate to

Configure > Security Service Edge > Settings > BGP Peer Policies and click Add BGP Policy. This will take you to the new BGP policy configuration page, as shown below.

ACME-ONE

CONFIGURATION

BGP Peer Policies

Below are all the BGP Peer Policies

| Policy Terms | Last Modified                          |
|--------------|--|
| Term1        | 3/12/2025, 7:24:25 PM<br>acmeone_admin |
| Term1        | 3/12/2025, 7:18:51 PM<br>acmeone_admin |

Add BGP Policy

1. Configure

2. Security Service Edge

3. Settings

4. BGP Peer Policies

5. Add BGP Policy

*Note: The BGP policy configuration is completed through two wizard steps: Enter Policy Term, followed by Enter Name, Description & Tags as illustrated below. The first section (Enter Policy Term) is displayed by default for configuration. Clicking Next will take you to the next section.*

ACME-ONE

CONFIGURATION

Add BGP Peer Policy

Enter Policy Term

Enter Name, Description & Tags

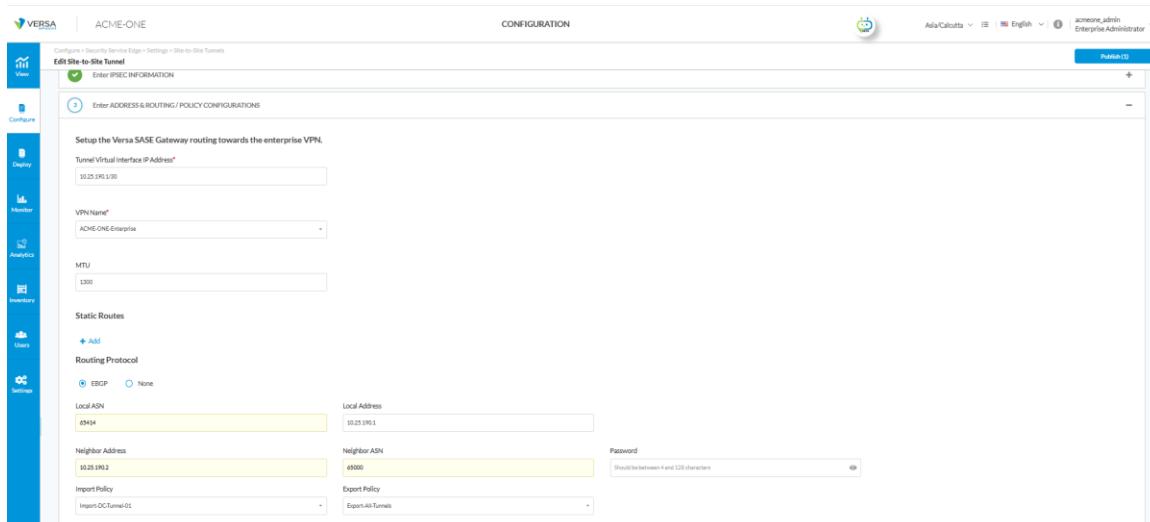
*We are now required to establish at least one policy term by adhering to these procedural steps.*

#### Step 1: Completing Section Enter Policy Term

1. Click on Add.
2. The 'Add Policy Term' wizard appears.
3. Under the Criteria section, specify the match criteria. You can select one (can also be left to none) or more of the following match criteria available and then set an action to it:
  - a. Community
  - b. Extended Community

- c. AS Path
- d. Metric
- e. NLRI
  - i. IPv4 Prefixes (Use + button to add as many as required)
  - ii. Min Length (Default: None, Range (24-32))
  - iii. Max Length (Default: None, Range (0-32))
  - iv. IPv6 Prefixes (Use + button to add as many as required)
  - v. Min Length (Default: None, Range (0-128))
  - vi. Max Length (Default: None, Range (0-128))
  - vii. Action (Permit/Deny)

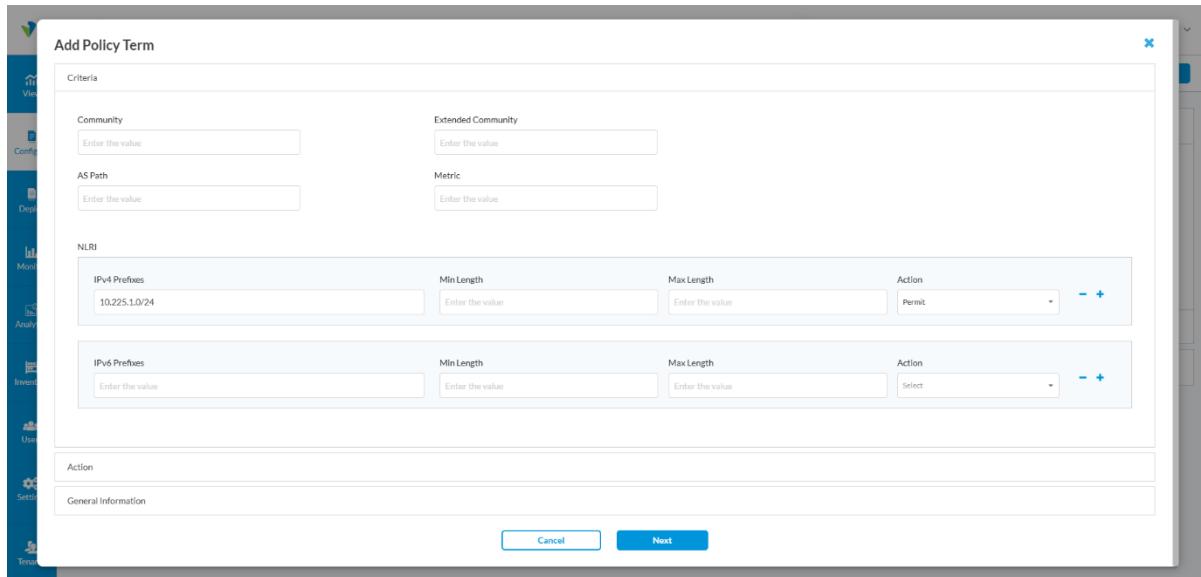
Note: IPv4 Prefix based match is shown in this document.



- 4. Name the policy term and click on 'Save'.

## Step 2: Multiple Policy Terms

You can add multiple terms to a single policy by clicking on + Add BGP Policy. This allows for complex routing policies with multiple match criteria.



Add Policy Term

Criteria

Community  
Enter the value

Extended Community  
Enter the value

AS Path  
Enter the value

Metric  
Enter the value

NLRI

IPv4 Prefixes  
10.225.1.0/24  
Min Length  
Enter the value  
Max Length  
Enter the value  
Action  
Permit

IPv6 Prefixes  
Enter the value  
Min Length  
Enter the value  
Max Length  
Enter the value  
Action  
Select

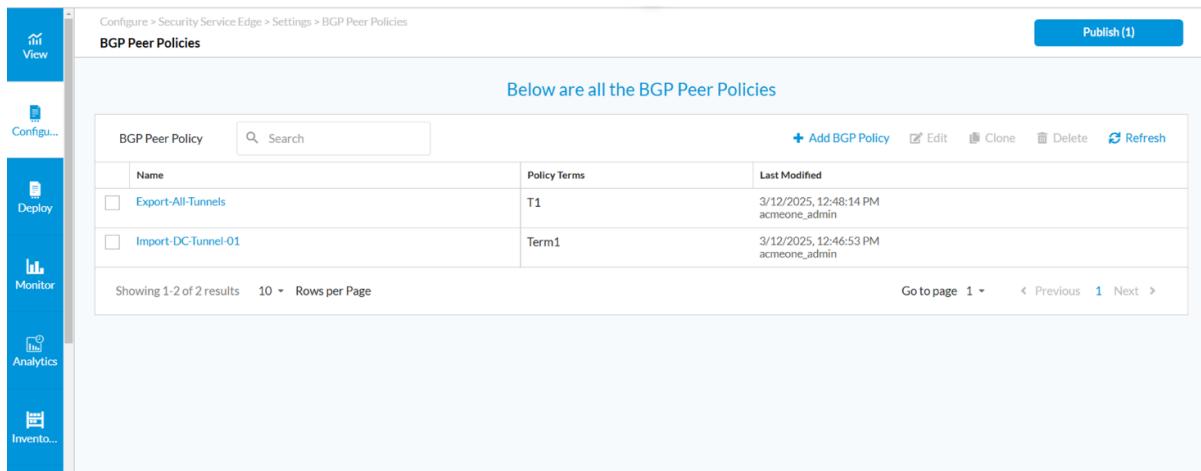
Action

General Information

Cancel Next

### Step 3: Final Policy Configuration

Fill in the required field under match criteria. Then, select the action for enforcement. Name the policy and click on 'Save'.



Configure > Security Service Edge > Settings > BGP Peer Policies

**BGP Peer Policies**

Below are all the BGP Peer Policies

Add BGP Policy Edit Clone Delete Refresh

| Name                | Policy Terms | Last Modified                           |
|---------------------|--------------|---|
| Export-All-Tunnels  | T1           | 3/12/2025, 12:48:14 PM<br>acmeone_admin |
| Import-DC-Tunnel-01 | Term1        | 3/12/2025, 12:46:53 PM<br>acmeone_admin |

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 < Previous 1 Next >

### Configuring EBGP in S2S IPsec VPN

- Selecting "Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS"

In this section, configure the tunnel interface IP, usually a /30 from your enterprise segment. Select the VPN name assigned to your tenant at the Gateway, the MTU value, and either Static or EBGP as your preferred routing protocol. Refer to the image below.

- i. Under "Setup the Versa SASE Gateway routing towards the enterprise VPN" configure the following

Add a Tunnel Virtual Interface address that is routable within your enterprise network. This typically involves using one IP from a /30 IPv4 address, with the other usable IP from the same /30 to be configured at your enterprise IPsec endpoint.

**VPN Name** to be selected from drop-down, usually the VPN name assigned to your tenant by the service provider, named as *<TenantName-Enterprise>*

Set **MTU**: Versa recommends that the maximum transmission unit be set to 1300 for IPsec-based tunnels

Under Routing Protocols, select EBGP and update the following information.

- Local AS number: Private AS number the customer wants to use.
- Local IP address: This will be the IPsec tunnel interface IP defined in the above step.
- Import and Export Policies: This BGP Peer Policy created in early will appear in the dropdown and can be attached here. The import policy is intended to influence what we learn from the peer, while the export policy is designed to control which routes we advertise to the peer.
- Set Routing Protocol to None.
- Enter the destination subnet. (In our case, we need to enter the server subnets one by one: 10.242.8.0/24, 10.242.9.0/24, 10.242.10.0/24).
- Assign a preference value between 1–255 (lower = higher priority).
- Routing Protocol select None.
- Click Save.

ACME-ONE

CONFIGURATION

America/Bogota | English | enterprise\_admin

VPN Name: ACME-ONE-Enterprise

MTU: 1300

Static Routes

Import Policy: Import-DC-Tunnel-01

Export Policy: Export-DC-Tunnel-01

Cancel | Next

Name the tunnel and click on 'save'.

ACME-ONE

CONFIGURATION

Asia/Calcutta | English | acmeone\_admin

Site-to-Site Tunnels

Below are all the Site-to-Site Tunnels

|                          | Name         | Gateway | Type  | Description | Tags | Last Modified                         | Status  | Settings                          |
|--------------------------|--------------|---------|-------|-------------|------|---------------------------------------|---------|-----------------------------------|
| <input type="checkbox"/> | DC-Tunnel-01 | SASE-GW | IPsec |             |      | 3/4/2025, 2:25:07 PM<br>Administrator | Enabled | <a href="#">Download.txt file</a> |
| <input type="checkbox"/> | DC-Tunnel-02 | SASE-GW | IPsec |             |      | 3/4/2025, 2:25:25 PM<br>Administrator | Enabled | <a href="#">Download.txt file</a> |

Showing 1-2 of 2 results | 10 Rows per Page | Go to page 1 | < Previous | Next >

After creating the tunnel, we have an option to download the tunnel configuration as a .txt file, that can be used to configure the tunnel on the remote end.

## Appendix B – Authentication Methods Configuration

### Versa Directory

Add the users/user groups information one by one or upload a CSV file containing this information in the following format. Other fields are filled by default. You can edit the default value if required. logins refer to the number of devices logged in with the same user username, allowed to be connected to the gateway at any given point in time. 'Cache interval' refers to how long the user authentication information is cached on the gateway.

For Users:

Username (Email)\*, First Name, Last Name, Phone, Description, and Group Name.

For User Groups:

Group Name\* and Description.

Note that \* indicates a mandatory field.

Add Versa Directory Authentication Profile

Review your configurations. Before submitting, review and edit any steps of your configuration below.

**General**

Name: Versa-Directory-Profile

Description:

Tags:

**Settings**

Cache Expiry Time (mins): 10

Concurrent Logins: 1

**Users & User Groups**

Users(3): Engguser1@acme.com, Engguser2@acme.com, AccUser1@acme.com

User Groups(2): Engineering, Accounts

Cancel Back Save

Before you do the above configuration, ensure that the IAM server details are configured by your Service Provider.

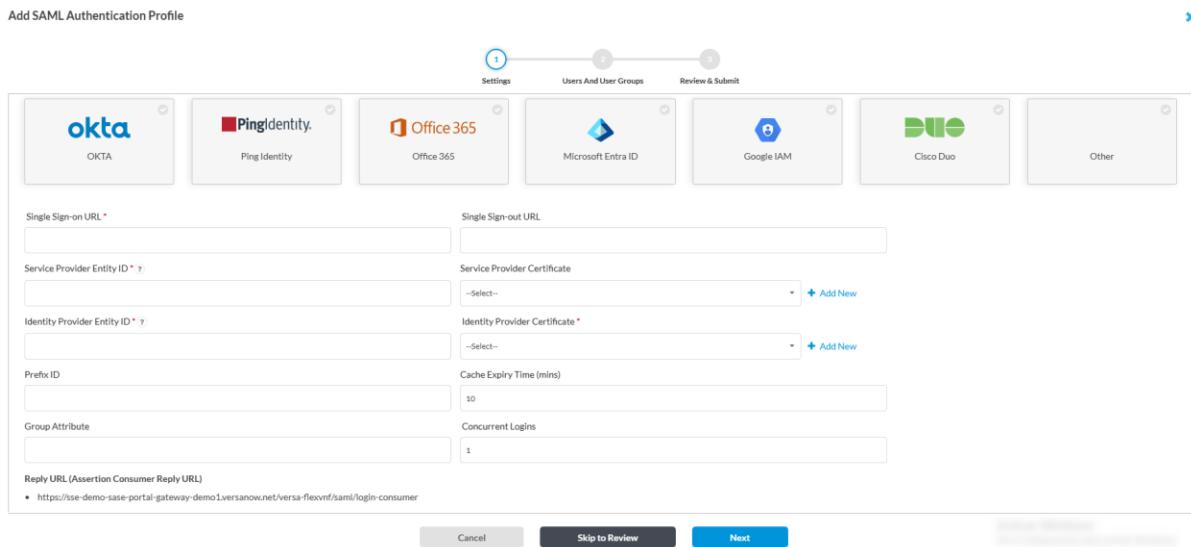
Log in to the email account that was referenced in the Versa Directory. Your email should have a message from Versa Networks letting you know a new account has been created. Click SET PASSWORD to create a new password. You can use the username received on the mail and the password you set to login to the Versa Secure Access Client.

### SAML

SAML authenticates users so that they can access multiple services and applications. SAML is useful when you want to access multiple services or applications and have authentication for each service or application, for example, Google and its related services. SAML is a common standard for exchanging authentication between parties and is most used for web browser-based single sign-on (SSO).

To begin with, Select the SAML type.

Add SAML Authentication Profile



Single Sign-on URL \*:

Single Sign-out URL:

Service Provider Entity ID \*:

Service Provider Certificate:

Identity Provider Entity ID \*:

Identity Provider Certificate \*:

Prefix ID:

Cache Expiry Time (mins):

Group Attribute:

Concurrent Logins:

Reply URL (Assertion Consumer Reply URL):

- https://sse-demo-sase-portal-gateway-demo1.versanow.net/versa-flexvnf/saml/login-consumer

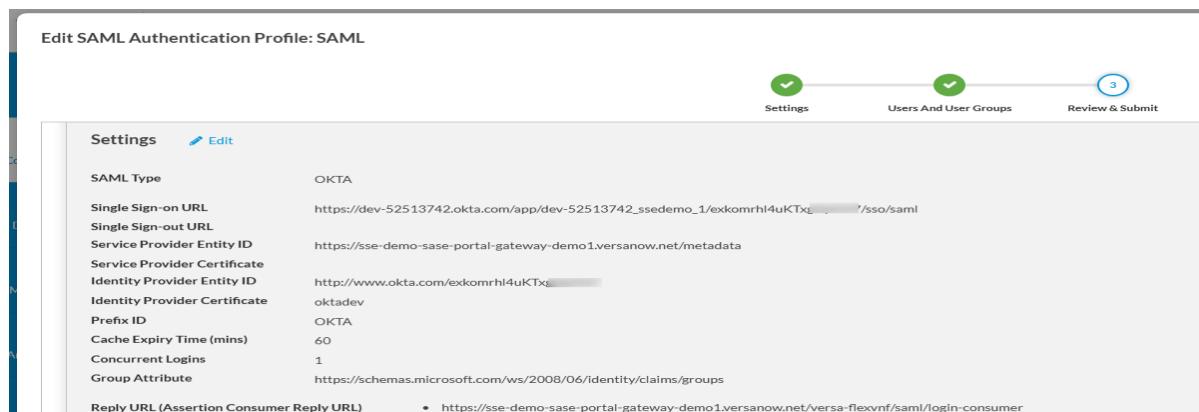
Cancel Skip to Review Next

Then, select the Identity Provider to configure and please refer to the following link for more information: [LINK TO BE ADDED](#)

Example for Okta

Concerto Configuration:

Edit SAML Authentication Profile: SAML



Settings Edit

SAML Type: OKTA

Single Sign-on URL: https://dev-52513742.okta.com/app/dev-52513742\_ssedemo\_1/exkomrhl4uKTxL.../sso/saml

Single Sign-out URL: https://sse-demo-sase-portal-gateway-demo1.versanow.net/metadata

Service Provider Entity ID: https://www.okta.com/exkomrhl4uKTxL...

Identity Provider Entity ID: oktadev

Identity Provider Certificate: http://www.okta.com/exkomrhl4uKTxL...

Prefix ID: OKTA

Cache Expiry Time (mins): 60

Concurrent Logins: 1

Group Attribute: https://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Reply URL (Assertion Consumer Reply URL):

- https://sse-demo-sase-portal-gateway-demo1.versanow.net/versa-flexvnf/saml/login-consumer

Settings Users And User Groups Review & Submit

## Okta Configurations:

- Create a new app integration (SAML 2.0).
- Edit the general settings (see the image below for reference). Make sure the Group Attribute is the same in both places (Concerto SAML Configuration and Okta).
- Download the Okta certificate and upload it to Concerto in the Identity Provider Certificate field.
- Assign users or groups to the application.

**SAML Settings** [Edit](#)

**GENERAL**

|                      |   |
|----------------------|---|
| Single Sign On URL   | https://sse-demo-sase-portal-gateway-demo1.versanow.net/versa-flexvnf/saml/login-consumer |
| Recipient URL        | https://sse-demo-sase-portal-gateway-demo1.versanow.net/versa-flexvnf/saml/login-consumer |
| Destination URL      | https://sse-demo-sase-portal-gateway-demo1.versanow.net/versa-flexvnf/saml/login-consumer |
| Audience Restriction | https://sse-demo-sase-portal-gateway-demo1.versanow.net/metadata                          |

**Default Relay State**

|                      |              |
|----------------------|--------------|
| Name ID Format       | EmailAddress |
| Response             | Signed       |
| Assertion Signature  | Signed       |
| Signature Algorithm  | RSA_SHA256   |
| Digest Algorithm     | SHA256       |
| Assertion Encryption | Unencrypted  |
| SAML Single Logout   | Disabled     |
| SAML Signed Request  | Disabled     |

**authnContextClassRef**

|                      |                            |
|----------------------|----------------------------|
| authnContextClassRef | PasswordProtectedTransport |
|----------------------|----------------------------|

**Honor Force Authentication**

|                            |     |
|----------------------------|-----|
| Honor Force Authentication | Yes |
|----------------------------|-----|

**Assertion Inline Hook**

|                       |                 |
|-----------------------|-----------------|
| Assertion Inline Hook | None (disabled) |
|-----------------------|-----------------|

**SAML Issuer ID**

|                |   |
|----------------|---|
| SAML Issuer ID | http://www.okta.com/\${org.externalKey} |
|----------------|---|

**Maximum app session lifetime**

**ATTRIBUTE STATEMENTS**

| Name   | Name Format | Value             |
|--|-------------|-------------------|
| <b>GROUP ATTRIBUTE STATEMENTS</b>                              |             |                   |
| Name   | Name Format | Filter            |
| https://schemas.microsoft.com/microsoft.identity.claims/groups | Unspecified | Matches regex: .* |

## Device Certificate

Device Certificate-based authentication is a secure method to validate the identity of devices.

Start by uploading the CA Chain. Select the username identifying field in the certificate. Enable Verify with OSCP and select the source VR (optional). Select whether to use device certificate-based authentication in the pre-logon stage (toggle the enable button, if needed). In case of using user-certificate-authentication along with device-certificate-authentication, select the order of authentication. Finally, name the profile and click on 'save'.

Edit Device Certificate Authentication Profile: Auth\_Profile-Cert-Based

Review your configurations. Before submitting, review and edit any steps of your configuration below.

**General**

Name: Auth\_Profile-Device\_Cert-Based

Tags:

**Settings**

Client CA Chain: CA-CHAIN

Username Identifying Field in Certificate: subject

Verify with OCSP: Disabled

Is CA Server on Internet?:

VPN Name:

Cache Expiry Time (mins): 10

Concurrent Logins:

**Authentication Order**

Prelogon: Disabled

Profile to authenticate first: User

Cancel Back Save

## User Certificate

User Certificate-based authentication is a secure method to validate the identity of users.

The steps to configure are similar to device certificate (Refer to the section before this one). We also have option here to use LDAP/SAML profile along with the user certificate authentication. We need to select the order of authentication. Finally, name the profile and click on 'save'.

Edit User Certificate Authentication Profile: Auth\_Profile\_User\_cert

Review your configurations. Before submitting, review and edit any steps of your configuration below.

General

|                        |             |
|------------------------|-------------|
| Name                   | Description |
| Auth_Profile_User_cert |             |
| Tags                   |             |

Settings [Edit](#)

|                               |          |
|-------------------------------|----------|
| Client CA Chain               | CA-CHAIN |
| Username Identifying Field in | subject  |
| Verify with OCSP              | Disabled |
| Is CA Server on Internet?     |          |
| VPN Name                      |          |
| Cache Expiry Time (mins)      | 10       |
| Concurrent Logins             |          |

Additional Authentication Method [Edit](#)

|                               |              |
|-------------------------------|--------------|
| Multi-factor Authentication   | Enabled      |
| Profile to authenticate first | LDAP Profile |
| Cache Expiry Time (mins)      | 10           |

Users [Edit](#)

|          |
|----------|
| Users(0) |
| No users |

Cancel Back Save

Edit User Certificate Authentication Profile: Auth\_Profile\_User\_cert

Review your configurations. Before submitting, review and edit any steps of your configuration below.

General

|                        |             |
|------------------------|-------------|
| Name                   | Description |
| Auth_Profile_User_cert |             |
| Tags                   |             |

Settings [Edit](#)

|                               |          |
|-------------------------------|----------|
| Client CA Chain               | CA-CHAIN |
| Username Identifying Field in | subject  |
| Verify with OCSP              | Disabled |
| Is CA Server on Internet?     |          |
| VPN Name                      |          |
| Cache Expiry Time (mins)      | 10       |
| Concurrent Logins             |          |

Additional Authentication Method [Edit](#)

|                               |              |
|-------------------------------|--------------|
| Multi-factor Authentication   | Enabled      |
| Profile to authenticate first | LDAP Profile |
| Cache Expiry Time (mins)      | 10           |

Users [Edit](#)

|          |
|----------|
| Users(0) |
| No users |

Cancel Back Save

## Appendix C – User Defined Objects and Endpoint Information Profiles

Versa supports a variety of user-defined objects (Example: Applications, services). When a particular object is not listed under pre-defined objects, we can define the object using the User-defined (Custom) Object.

To configure a user-defined object, navigate to

**Configure > Security Service Edge > Secure Access > User-Defined Objects.**

### User-Defined Application

To create a Custom Application, Navigate to

**Configure > Security Service Edge > Secure Access > User-Defined Objects > Applications.**

For a VSPA use case, we either define a Private Application or a client Native Application. Any Application that needs to interact with the client (or needs to be referenced under Secure Access Rule) must be defined under Client Native Application. Other Custom Applications, which need to be referenced under Real-Time Protection Rules (or needs to interact with the gateway), must be defined under Private Application.

### Client Native Application

Enter either the FQDN or File Path (the full path to the Application executable file) of the Application, provide a name to the Application and optionally an application logo can be uploaded, click on save.

## Private Application

A Private application can be defined using one or more of the following match conditions IP Prefix, FQDN, Source/Destination Port and Protocol. The application can also be tagged as per the nature of the Application. After filling in the required details, provide a name to the application, optionally upload a log of the Application and click on save.

- Configuring **Application Tags** help classify the Application based on risk and Productivity and can be useful for monitoring purposes on Analytics.
- Do not create Private Applications for a condition that requires only an L3/L4 match (Ex. IP or Port). Use Applications only for FQDN based or a combination of multiple L3/L4 parameters (Ex. IP and Port combination).

## Address Groups

An Address Group is a group of IPs (or FQDNs) that can be used as match criteria for L3 based Source/Destination Address match in policies.

To configure Address Groups, Navigate to

**Configure > Security Service Edge > Secure Access > User-Defined Objects > Address Groups. Click on +Add.**

An address Group may be defined as a Subnet, IP Range, Wildcard IP, FQDN or an address file (needs to be uploaded). We can add multiple Addresses of each type. Press 'Enter' after adding each address. We can have multiple types of Address under a single address group. Provide a name for the Address group and click on 'Save'.

## Services

Services are used to define ports numbers that can be used as match criteria in policies under L3/L4 match. Versa has already defined a lot of well-known services such as HTTP (Port 80), HTTPS (Port 443), etc. If the service that your organization is using needs a custom port to be defined, it can be done under User-defined Services.

To configure a user-defined service, Navigate to

***Configure > Security Service Edge > User-Defined Objects > Services. Click on + Add User Defined.***

Fill in the Protocol and Port details, provide a name and click on 'save'.

## End-point Information Profiles

Endpoint Inspection Policies (EIPs) provide a robust mechanism for assessing the security posture of endpoint devices attempting to connect to the Gateway. By collecting information such as the presence of the latest security patches, up-to-date antivirus definitions, and other critical indicators, EIPs enable you to enforce granular access controls based on device compliance.

To configure EIP, Navigate to

**Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles.**

There are three building blocks of EIP. They are

- EIP Objects

EIP objects define the various match criteria to check the security status of a particular category. Select all the required match conditions. Go through the fields below to understand how to construct an EIP object.

- Disabled—Perform no validation. This is the default.
- False—Perform validation, and if the endpoint reports the status as False, the match is successful.
- True—Perform validation, and if the endpoint reports the status as True, the match is successful.

- EIP Profiles

EIP profile is a collection of various EIP objects (either predefined or user-defined), that are used as match criteria in various access policies on the gateway. Select the category of EIP, the EIP objects under that category get listed. Select the required objects under each category. Name the profile and click on 'Save'.

- EIP Agents

EIP Agents define all information to collect from the endpoint for a particular category. This information is then used by the gateway to validate the match criteria for an EIP object. For each item, select one of the following options:

- Disabled—The item is disabled.
- True—Click to extract the information for this category.
- False—Click to not extract the information for this category.

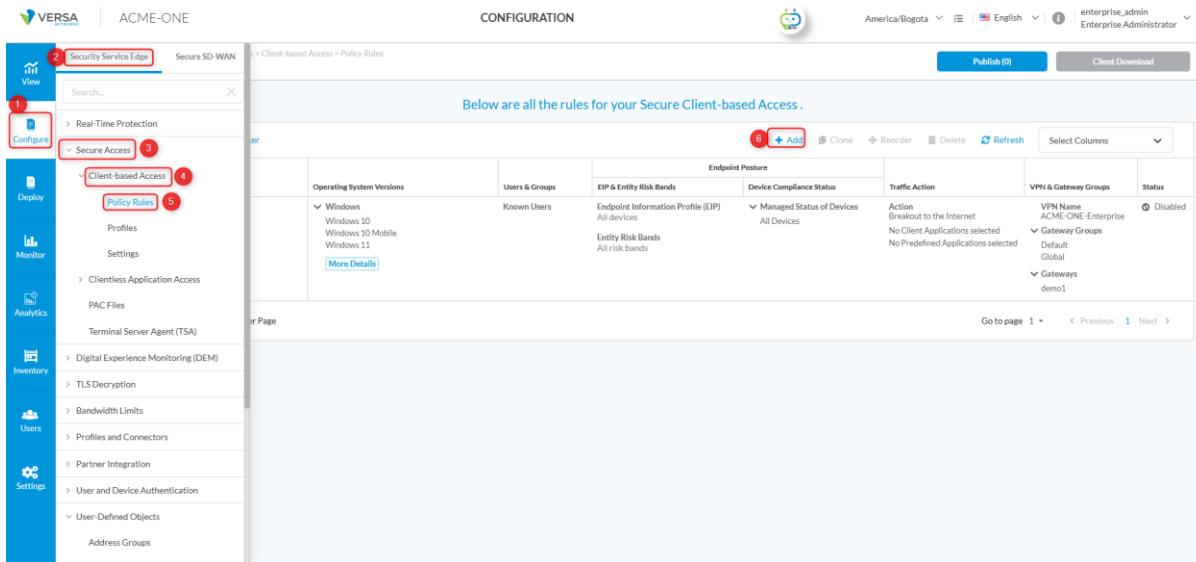
We can define multiple categories under the same Agent profile.

## Appendix D – Secure Access Policies – Key Components

Secure Access rules define the connection between the end user machine (that are installed with Versa SASE Client) and the SASE gateway. Secure Client Access defines who, how and under what conditions a user can connect to the gateway, client-features and what all traffic is sent to the gateway. Before configuring the Secure Access Client-based Rule, ensure that the connectivity between the gateway and your authentication server is established.

To configure secure client access rule, Navigate to

**Configure > Security Service Edge > Secure Access > Client-based Access > Rules and click on +Add.**



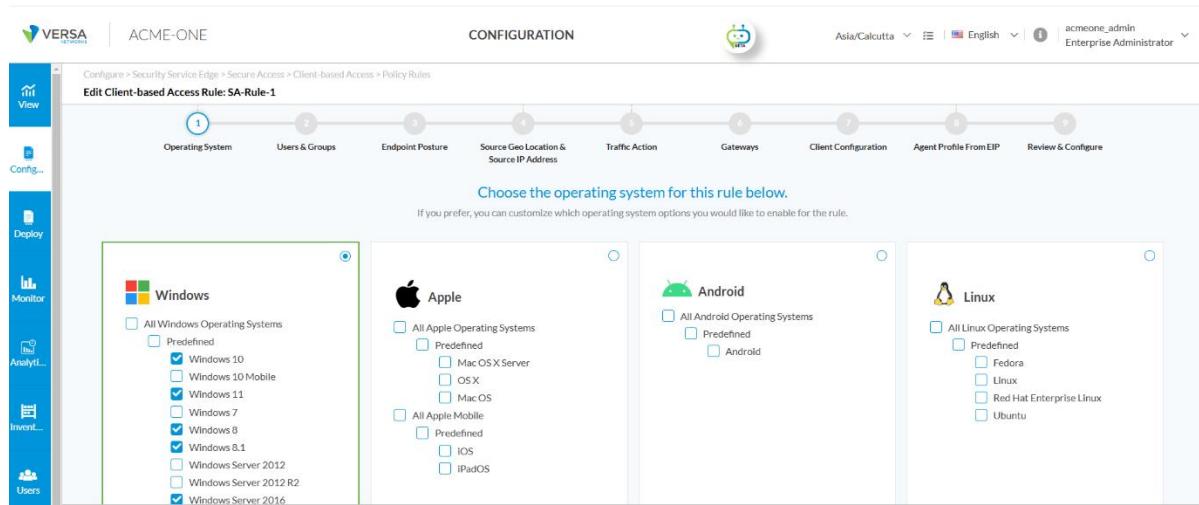
The following are the match conditions for secure access rules:

- Operating System
- Users/User Groups
- Endpoint Information Profile (Posture Checks)
- Source Address/Geo-location

Note that all the above match criteria are 'AND' and within the same tab, it is 'OR'.

## Operating system

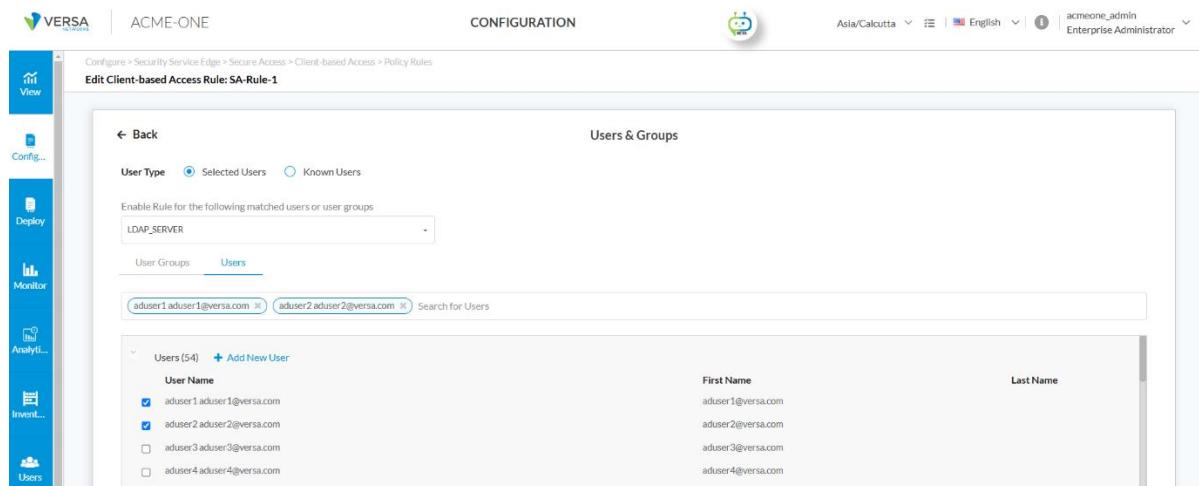
Operating systems are used to define end user machine operating systems. We can match only one operating system (Ex. Windows) with one rule. However, in the same rule we can match multiple flavors (or versions) of that operating system (Ex. Windows Professional, Windows Vista etc..). We also have an option to match a custom operating system (defined under User-defined objects). Select the Operating system. By default, when you select an operating system, all versions under that operating system will get selected. We can customize this as desired.



- It is recommended to select only the versions of operating systems used in your organization and not leave them to default, which reduces the chance of an unauthorized user connecting to the gateway.

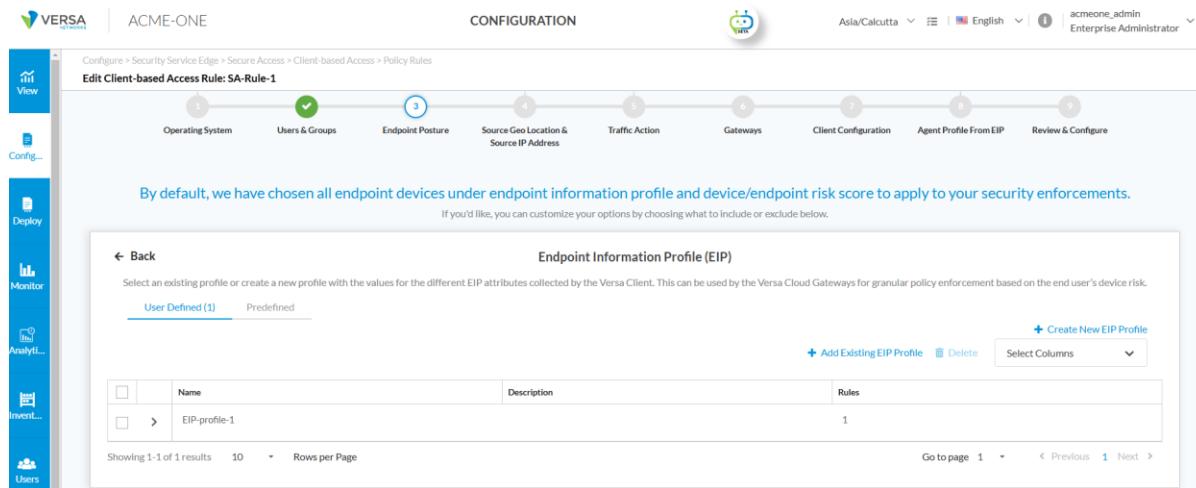
## Users/User Groups

This section defines which users/user groups will use this rule to connect to the gateway. Under the Authentication-profile, select the type of Authentication profile. Under 'Selected Users', select the users/user groups. By default, user match criteria are set to 'Any'.



## Endpoint Information Profile (EIP)

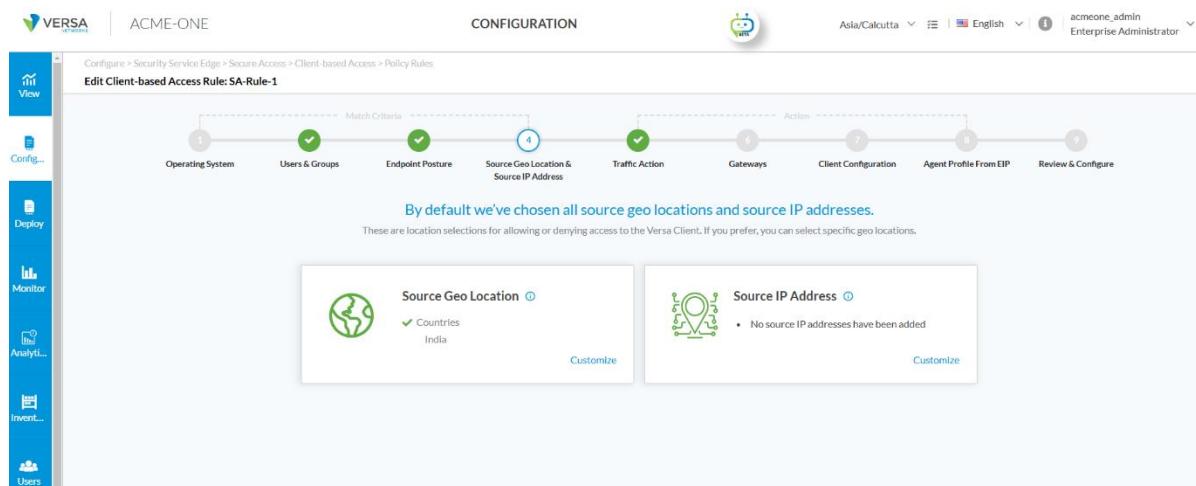
Device-Risk Info helps to define what all software/applications need to be present on the user machine for it to be able to connect to the gateway. More granular details like the version of the software, status etc. can also be defined. Versa has a set of pre-defined EIPs. We can also use the user-defined EIP profiles defined in the previous sections as match criteria. Choose the EIP profile created in the previous section or else select the predefined EIP profile.



| Name          | Description | Rules |
|---------------|-------------|-------|
| EIP-profile-1 |             | 1     |

## Source Address/Geo-location

This criterion helps restrict the Source Address or Geo-location to selective locations/Addresses. We have granular options like country, state and city while defining the location. By default, Source Geo-location is set to all, and Source IP address is set to Any.



Based on the match criteria defined above, the following actions can be enforced on the traffic and the client.

- Traffic Action
- Gateways

- Client Configuration
- Agent Profile from EIP

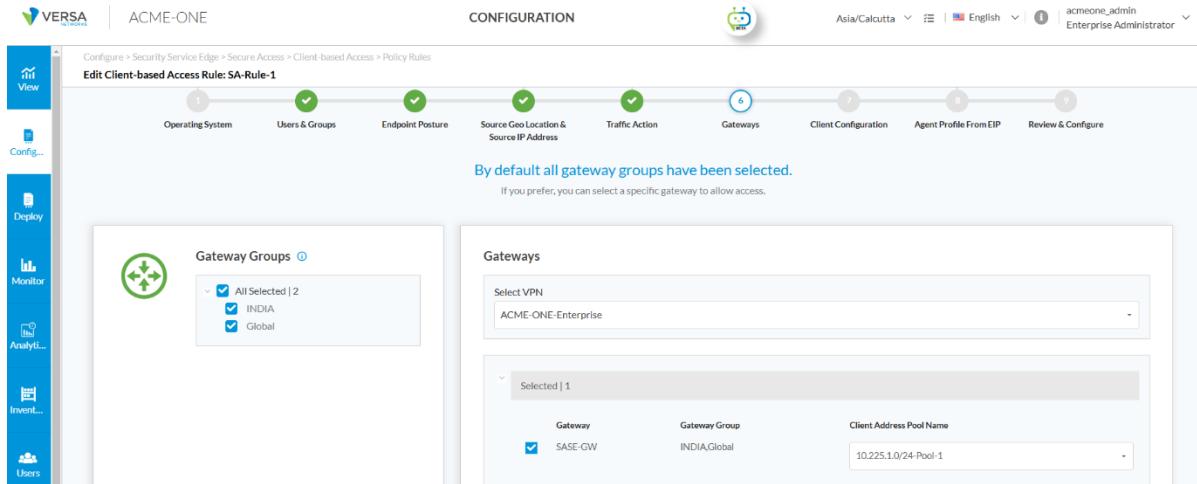
## Traffic Action

For VSPA only, there are two possible traffic actions. One is to deny the traffic, and the other one is to allow the traffic (where all private Application traffic is directed to the versa gateway, and the Internet bound traffic breaks out locally).

If you want to send any application to the gateway, they can be selected under the applications section. We have the option to either select an application from the list of pre-defined or custom (defined in the above sections) applications. This option can be useful in cases where certain source IPs are whitelisted on the destination server. Thus, the traffic is sent to the destination server via the enterprise network (which in turn is via the SSE gateway for a remote user).

## Gateways

This section lists the gateways (and the gateway groups) to which the end-user will connect to. If an enterprise has subscribed to multiple gateways, then this section helps define which set of users will connect to which gateways. We also configure the IP pool of the end-user machines, while connected to the gateway for each selected gateway under this section. This IP is nothing but the tunnel IP address of the end user machine while connected to the gateway. The IP pool that is configured here must be whitelisted on the enterprise firewalls for a remote user to be able to access the enterprise applications. We can define multiple IP pools for an enterprise on a gateway (each pool mapped to a set of users), which can then be used for monitoring, auditing or access restriction purpose inside the enterprise network.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: SA-Rule-1

Operating System ✓

Users & Groups ✓

Endpoint Posture ✓

Source Geo Location & Source IP Address ✓

Traffic Action ✓

Gateways 6 ✓

Client Configuration ✓

Agent Profile From EIP ✓

Review & Configure ✓

By default all gateway groups have been selected.  
If you prefer, you can select a specific gateway to allow access.

Gateway Groups ○

- All Selected | 2
- INDIA
- Global

Gateways

Select VPN

ACME-ONE-Enterprise

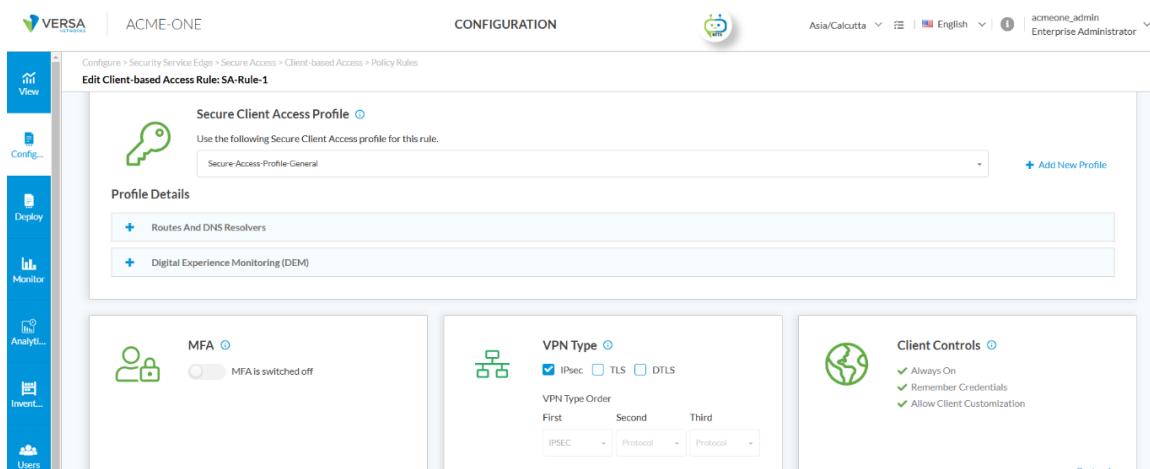
Selected | 1

| Gateway | Gateway Group | Client Address Pool Name |
|---------|---------------|--------------------------|
| SASE-GW | INDIA/Global  | 10.225.1.0/24 Pool-1     |

## Client Configuration

The following configurations are covered under this section:

- Secure Client Access Profile
- MFA
- VPN Type
- Client Controls



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: SA-Rule-1

Secure Client Access Profile ○

Use the following Secure Client Access profile for this rule.

Secure-Access-Profile-General

[+ Add New Profile](#)

Profile Details

- [+ Routes And DNS Resolvers](#)
- [+ Digital Experience Monitoring \(DEM\)](#)

MFA ○

MFA is switched off

VPN Type ○

IPsec  TLS  DTLS

VPN Type Order

| First | Second   | Third    |
|-------|----------|----------|
| IPSEC | Protocol | Protocol |

Client Controls ○

- Always On
- Remember Credentials
- Allow Client Customization

[Customize](#)

## Secure Client Access Profile

Select the required secure client access profile from the list of profiles created in the previous sections.

## MFA

In addition to the authentication done via the authentication profile, we can also authenticate the users based on Email OTP/Time-based OTP. This is a useful feature, when an enterprise does not have multiple factors of authentication in the authentication profile. To enable, turn on the MFA button. On the following tab, select one of the above options and fill in the required details.

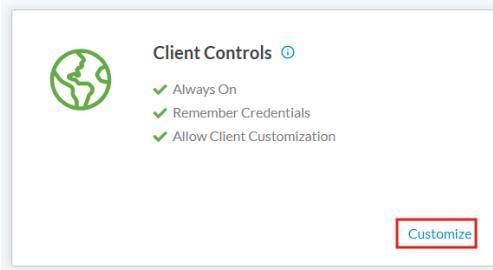
## VPN Type

Versa supports IPSEC, TLS and DTLS for connectivity between the end-user machine and the gateway via the Versa Secure Access Client. We can configure one or more of the VPN types. Also, the order in which they need to take over in case of failure of primary VPN type.

- It is recommended to configure IPSEC as backup VPN type, when TLS/DTLS is configured as primary.

## Client Controls

The Versa Secure Access Client offers a range of client control options for enterprise customization. To configure client options, click on customize. Some of the widely used client control options include:



### *Always On*

The end-user will not be able to disconnect the VPN. There are options to re-connect automatically and a few other customizations available, which are Disconnect- Never (meaning you will not be able to disconnect the client at all), while if you configure something in interval you can disconnect the client, but it gets automatically reconnected in that stipulated time again.

### *Client Logo*

It is used for Client white labeling. You can upload your Enterprise logo to be instead of Versa logo on the client screen.

### *Fail-open/Close*

*Fail-open indicates that the end-user will be able to connect to the internet, even if not connected to the gateway (Default). Fail-close indicates that the end-user will not be able to access the internet, if not connected to the VPN.*

### *Allow Client customization*

*If disabled, end-user will not be able to make any changes with respect to the gateway from the client.*

### *Tamper-Protection*

*If enabled, the end-user will not be able to delete the account or uninstall the client without the Administrator tamper protection password.*

### *Portal Lifetime*

*It is time in minutes that the configuration sync happens between the gateway and the client automatically. In case of any configuration change to take immediate effect, we need to re-register the client.*

### *Trusted Network Hostname*

*This is the FQDN of the host that is accessible only from within your enterprise. If enabled, the tunnel to the gateway is bypassed when the user connects from the office (from within your enterprise domain). The traffic is sent to the gateway only in case of a remote user.*

*While this is enabled, there is an option to specify trusted routes. Only the trusted networks are bypassed from the gateway, and all the other traffic is still sent to the gateway. This is called the semi-trusted mode.*

### *End-point DLP*

*With endpoint DLP, we can control Copy, Paste, screenshot and USB options on the end-user machine.*

### *EIP Agent Profile*

EIP Agent profile refers to the profiles containing the list of endpoint information that needs to be collected from the user machine. This information can be used while connecting to the gateway in secure access profile or in Real-time Protection Policies, while connecting to the Internet/Private Apps. Select the type of EIP Agent Profile (Pre-defined/user-defined). Then, select the corresponding agent profile from the dropdown.

## Appendix E – Real-Time Protection – Key Components

### Private App Protection

Private Protection rules are firewall rules used to define protection for the custom applications in your enterprise. Note that you will not be able to configure protection for any pre-defined applications under private App protection.

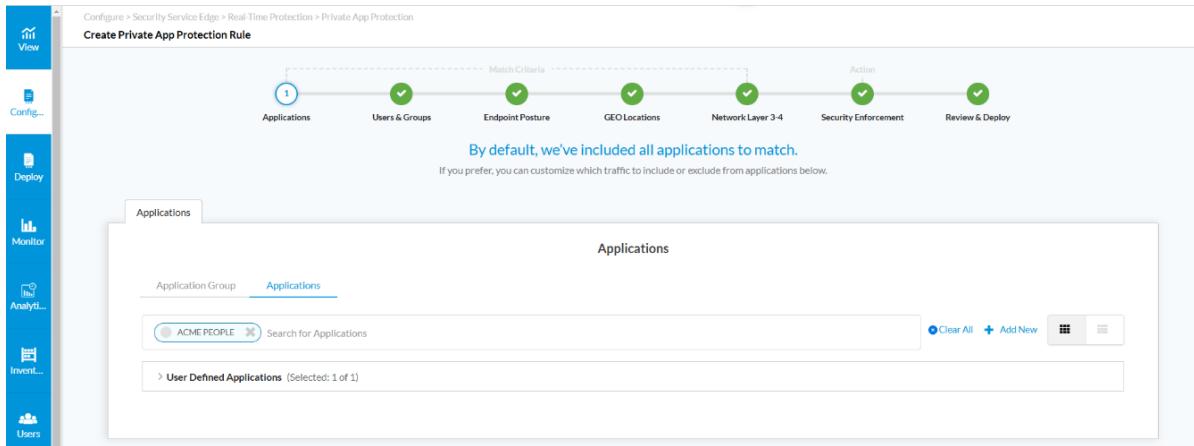
To configure Private App Protection, navigate to

**Configure > Security Service Edge > Real-Time Protection > Private App Protection and click on +Add**

(Click on Let's Go, if this is your first Private App Rule). Each private protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR 'ed and on different tabs is 'AND'.

The match criteria are as follows:

- Applications—Individual applications, groups of applications, categories of applications, predefined URL categories (created in previous steps). Select one or more Applications/Groups.



Configure > Security Service Edge > Real-Time Protection > Private App Protection  
Create Private App Protection Rule

Match Criteria

Applications

Users & Groups

Endpoint Posture

GEO Locations

Network Layer 3-4

Action

Review & Deploy

By default, we've included all applications to match.  
If you prefer, you can customize which traffic to include or exclude from applications below.

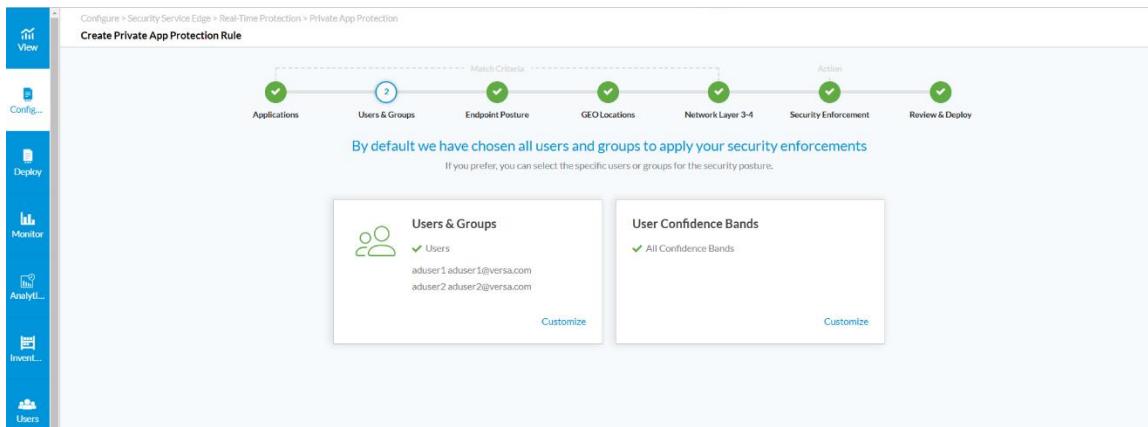
Applications

Application Group Applications

ACME PEOPLE Search for Applications

User Defined Applications (Selected: 1 of 1)

- User groups—Individual users or groups of users. Select users/user groups.



Configure > Security Service Edge > Real-Time Protection > Private App Protection  
Create Private App Protection Rule

Match Criteria

Applications

Users & Groups

Endpoint Posture

GEO Locations

Network Layer 3-4

Action

Review & Deploy

By default we have chosen all users and groups to apply your security enforcements  
If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

Customize

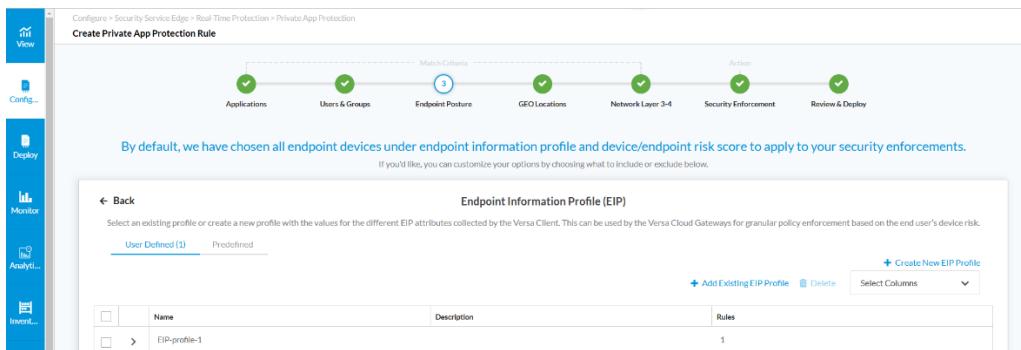
User Confidence Bands

Customize

Users

aduser1 aduser1@versa.com  
aduser2 aduser2@versa.com

- Endpoint Posture- Predefined and user-defined Endpoint Information Profiles (EIP). Select the EIP Profiles needed to restrict access based on end-device posture.



Configure > Security Service Edge > Real-Time Protection > Private App Protection  
Create Private App Protection Rule

Match Criteria

Applications

Users & Groups

Endpoint Posture

GEO Locations

Network Layer 3-4

Action

Review & Deploy

By default, we have chosen all endpoint devices under endpoint information profile and device/endpoint risk score to apply to your security enforcements.  
If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

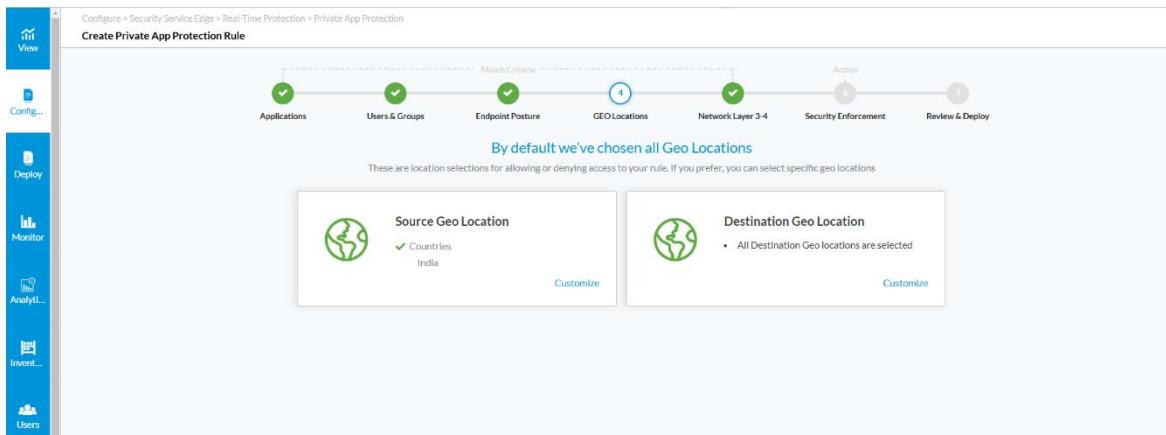
User Defined (1) Predefined

Create New EIP Profile

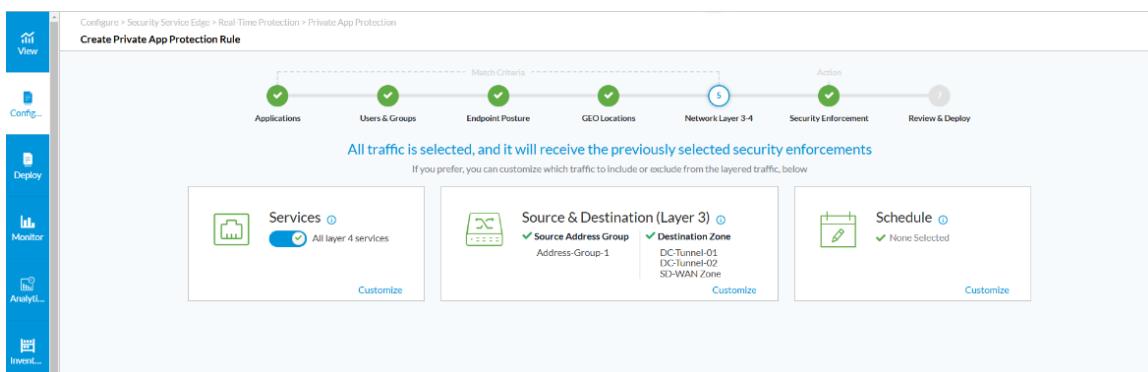
Add Existing EIP Profile Delete Select Columns

|  | Name          | Description | Rules |
|--|---------------|-------------|-------|
|  | EIP-profile-1 |             | 1     |

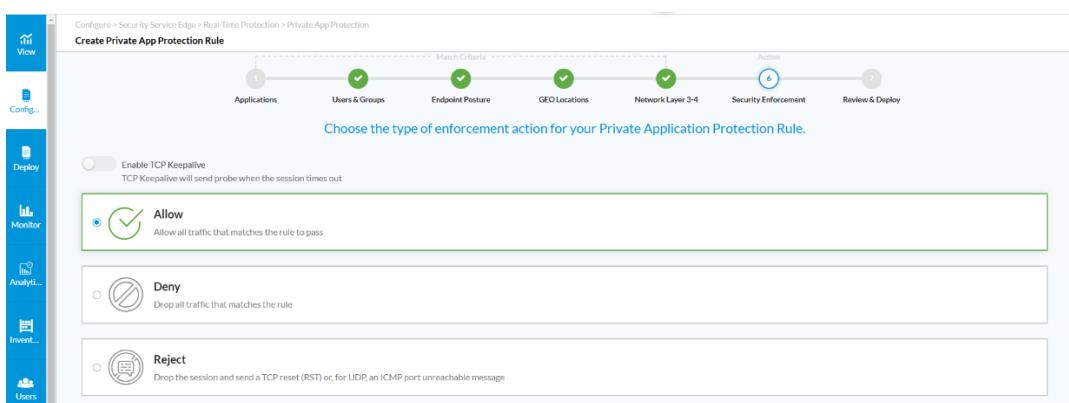
- Geolocation—Geographic location of the source or the destination. You can choose country, state and city.



- Network Layer 3 and Layer 4— IP address of the source/destination & Custom or predefined protocol-based services. The Address groups already created are listed here. You can either use them or add new address group by clicking on + Add Address Group. After creating, select the check box against the address groups to select them. Similarly, select the source/destination zones as needed. Each of the tunnel toward the DC, gets created as a zone. So, you can control what resources are allowed to access for a user based on zones.



The enforcement actions are Allow, deny or reject. Select any of the actions to enforce to the traffic.



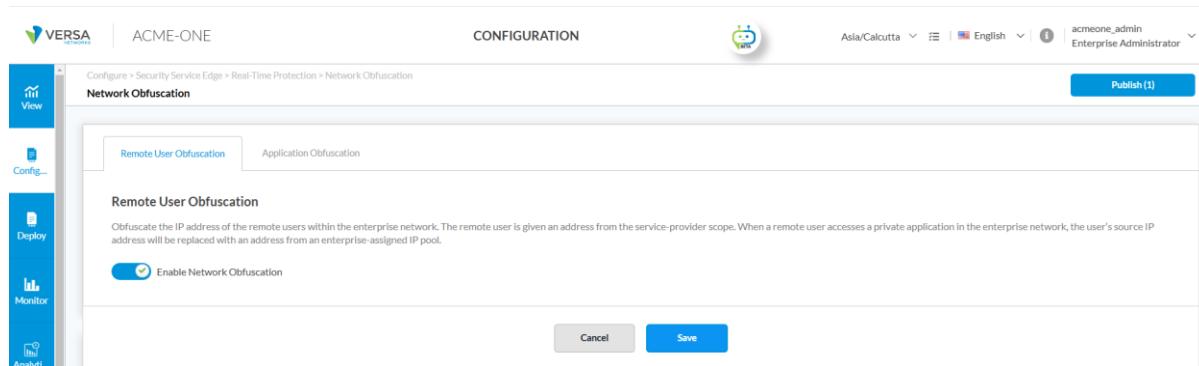
## Network Obfuscation

Network Obfuscation when enabled is used to protect the identity of the user or the end application. There are two types of Network Obfuscation, which are explained below. To configure network obfuscation, Navigate to

**Configure > Security Service Edge > Real-Time Protection > Network Obfuscation**

### Remote User Obfuscation

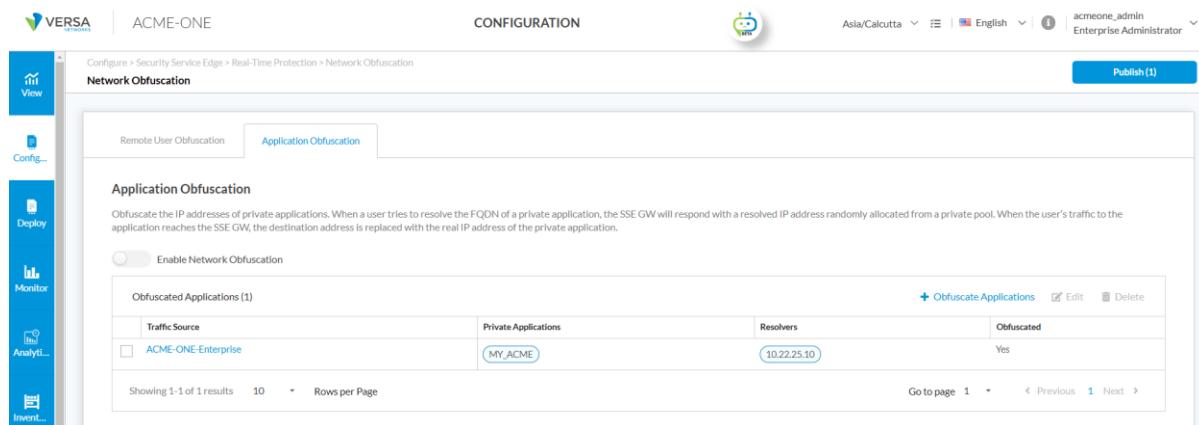
When enabled, is used to hide the IP address of the end user inside the enterprise network. Just toggle the "Enable Network Obfuscation" to enable remote user obfuscation.



The screenshot shows the 'Network Obfuscation' configuration page. On the left, there is a vertical sidebar with icons for View, Config..., Deploy, Monitor, and Analytic. The main header is 'ACME-ONE' and 'CONFIGURATION'. The sub-header is 'Configure > Security Service Edge > Real-Time Protection > Network Obfuscation'. The sub-sub-header is 'Network Obfuscation'. There are two tabs: 'Remote User Obfuscation' (selected) and 'Application Obfuscation'. The 'Remote User Obfuscation' section contains the following text: 'Obfuscate the IP address of the remote users within the enterprise network. The remote user is given an address from the service-provider scope. When a remote user accesses a private application in the enterprise network, the user's source IP address will be replaced with an address from an enterprise-assigned IP pool.' Below this is a toggle switch labeled 'Enable Network Obfuscation' which is checked. At the bottom are 'Cancel' and 'Save' buttons.

### Application Obfuscation

When enabled, it is used to hide the identity of the private application from the end user. The IP of the private application is randomly chosen on the gateway from a pool. The IP of the same private application seen by two different users is different and keeps changing even within the same session and hence prevents lateral movement inside the enterprise network. To enable, click on +Obfuscate Application. Select the Private Application (defined by a host pattern) or add a new application. Add the DNS resolver.



The screenshot shows the 'Network Obfuscation' configuration page. The sidebar and header are the same as the previous screenshot. The sub-sub-header is 'Network Obfuscation'. There are two tabs: 'Remote User Obfuscation' (selected) and 'Application Obfuscation'. The 'Application Obfuscation' section contains the following text: 'Obfuscate the IP addresses of private applications. When a user tries to resolve the FQDN of a private application, the SSE GW will respond with a resolved IP address randomly allocated from a private pool. When the user's traffic to the application reaches the SSE GW, the destination address is replaced with the real IP address of the private application.' Below this is a toggle switch labeled 'Enable Network Obfuscation' which is unchecked. At the bottom are 'Cancel' and 'Save' buttons. Below the tabs is a table titled 'Obfuscated Applications (1)'. It has columns: 'Traffic Source', 'Private Applications', 'Resolvers', and 'Obfuscated'. There is one row with 'ACME-ONE-Enterprise' in 'Traffic Source', 'MY.ACME' in 'Private Applications', '10.22.25.10' in 'Resolvers', and 'Yes' in 'Obfuscated'. At the bottom of the table are buttons for '+ Obfuscate Applications', 'Edit', and 'Delete'. Below the table are pagination controls: 'Showing 1-1 of 1 results', '10 Rows per Page', 'Go to page 1', 'Previous 1 Next', and 'Next'.

## About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the [VersaONE Universal SASE Platform](#) delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit <https://www.versa-networks.com> and follow Versa on [LinkedIn](#) and X (Twitter) [@versanetworks](#).