VERSA

IMPLEMENTATION GUIDE

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

Title	**Step-By-Step Configuration Guide for Versa Secure Private Access (VSPA)**
Author	Versa Professional Services
Version	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

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.

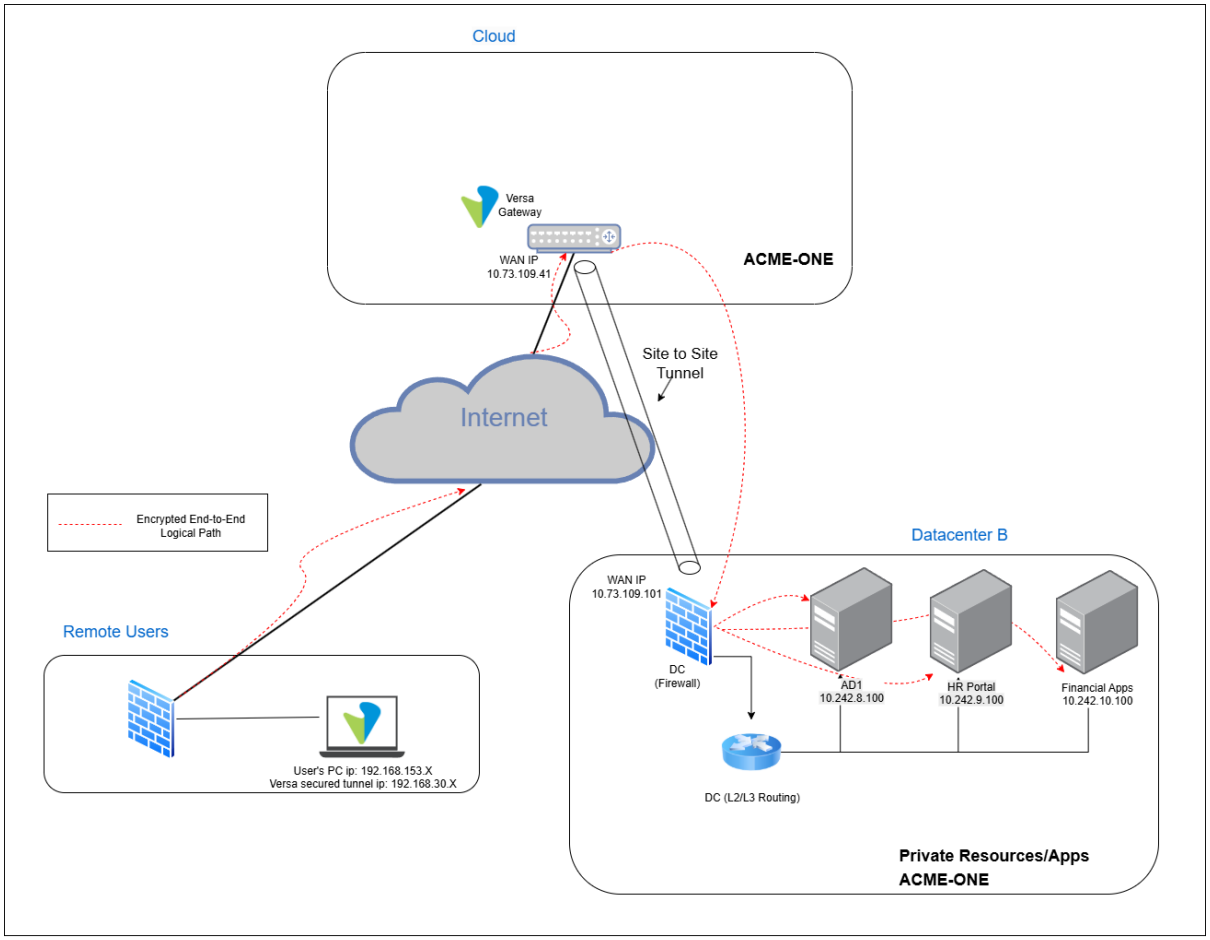
Customer Requirements

- 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)

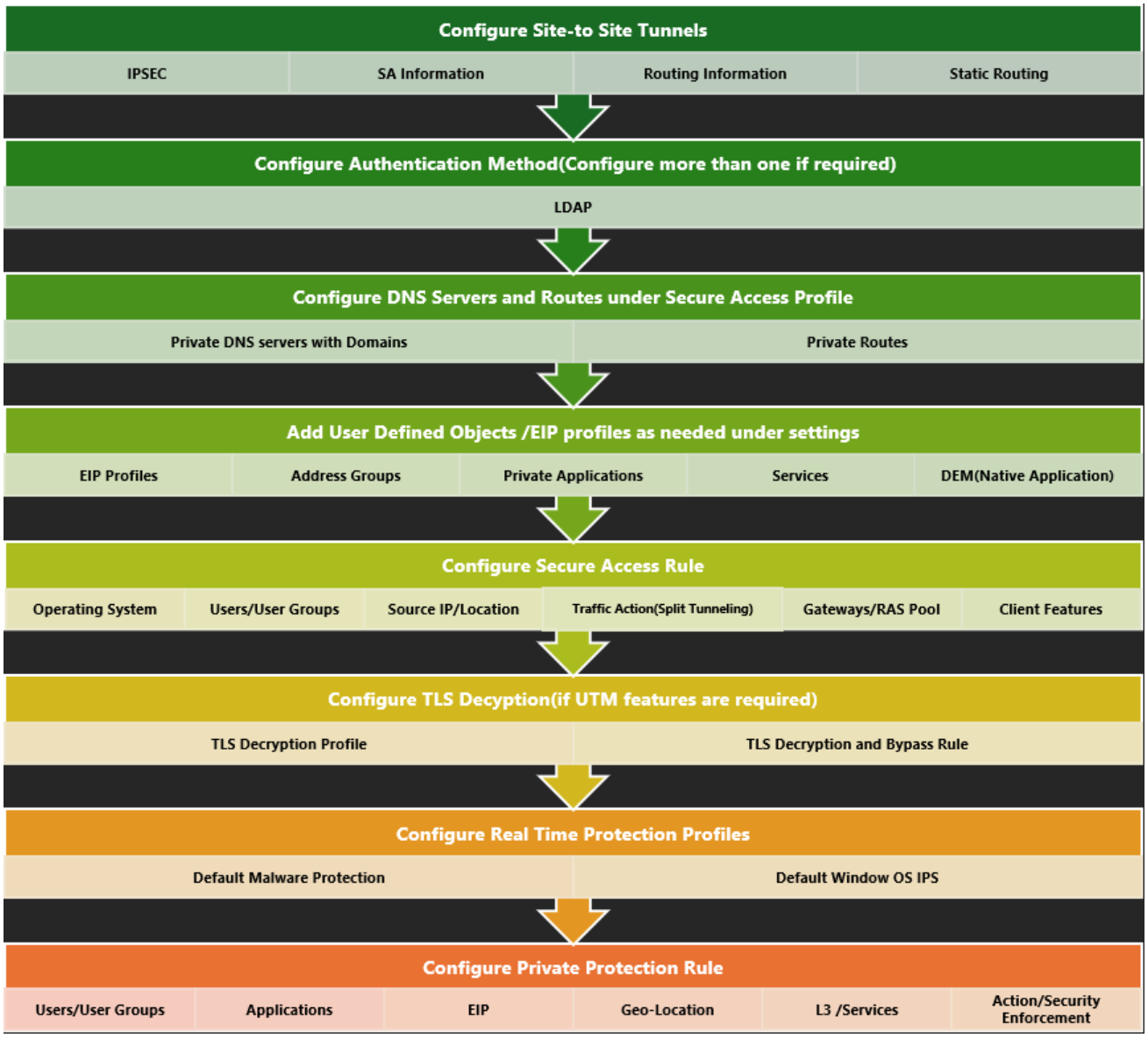
- **Remote Users (Work from Home)**

  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

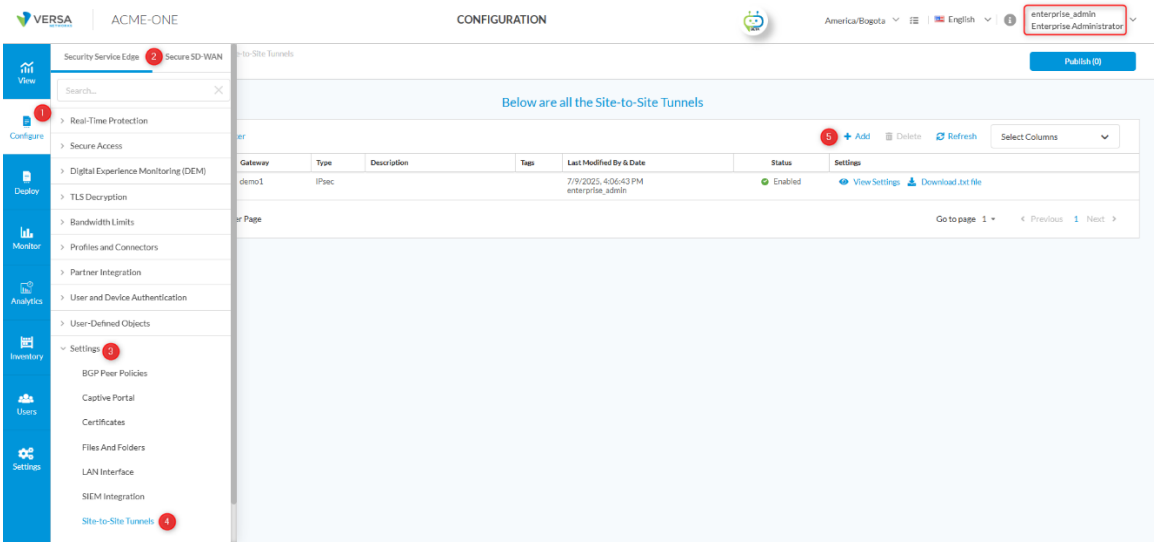
An IPSec tunnel facilitates secure remote access to enterprise private applications, DNS servers and Authentication Servers by directing traffic from the Versa gateway to the customer's data center, designated as "Datacenter B" in this case. Versa recommends implementing redundant IPSec tunnels with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

Configure Site-to-Site Tunnel

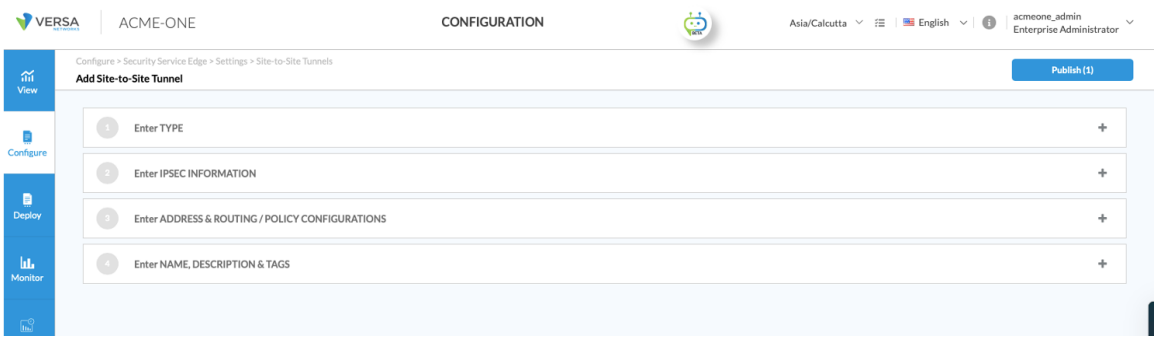
Log in to the Concerto UI using your enterprise administrator credentials (Tenant Admin) to configure a site-to-site tunnel.

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.

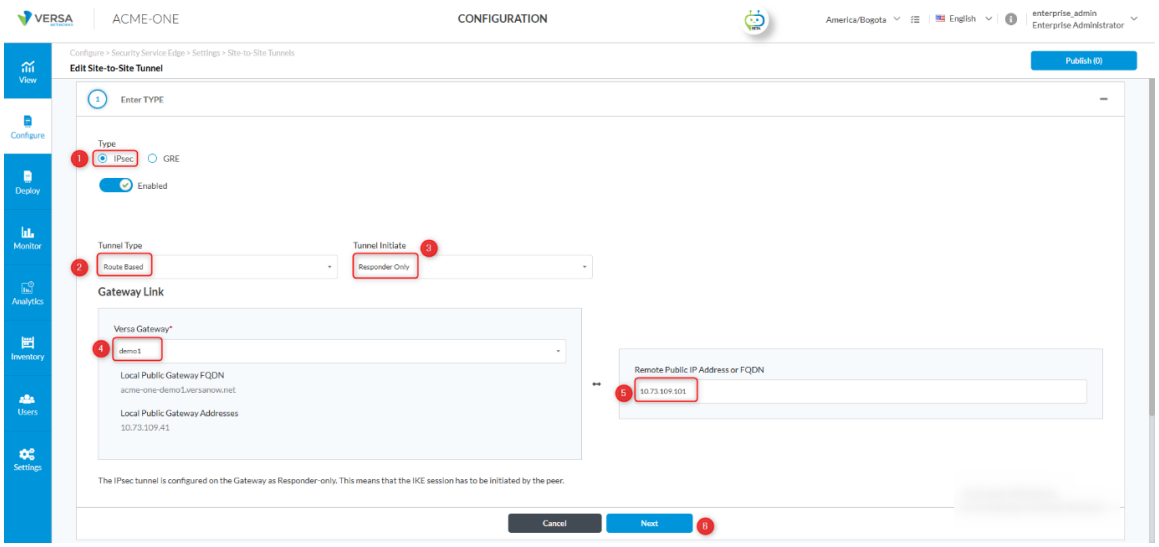
      Note that Versa Gateway is set as ‘responder only’ for the IPsec tunnel. So, the peer must initiate the request for the tunnel for the negotiation to start.

   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.

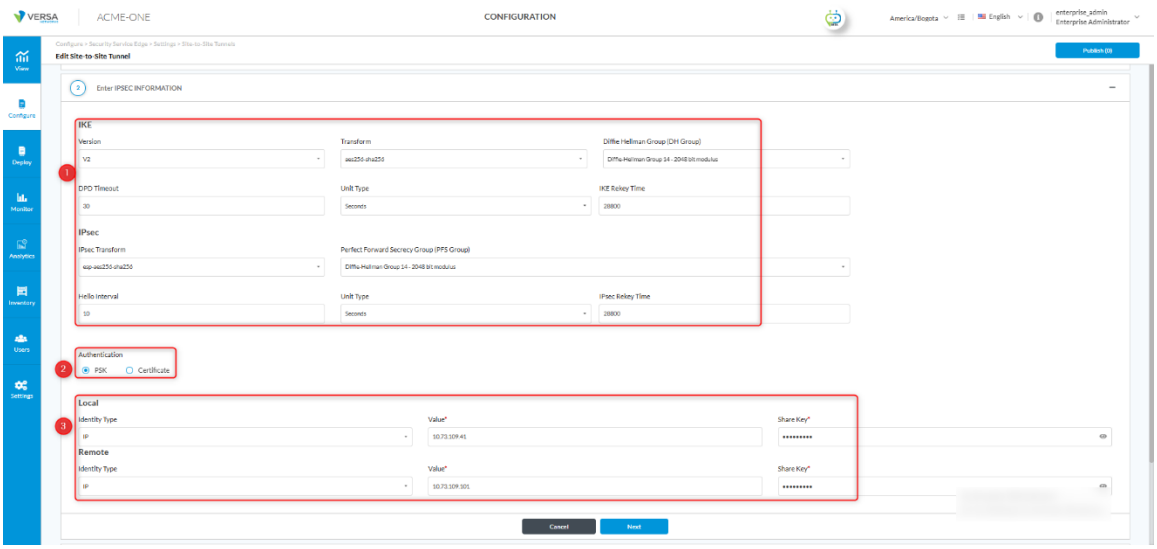
   E. Use the **Remote Public IP Address or FQDN** field to enter your enterprise firewall details as the tunnel endpoint.

      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
IKE (Phase 1)	Encryption	AES-256
	Authentication	SHA-256
	DH Group	14
	Lifetime (seconds)	28800
IPsec (Phase 2)	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

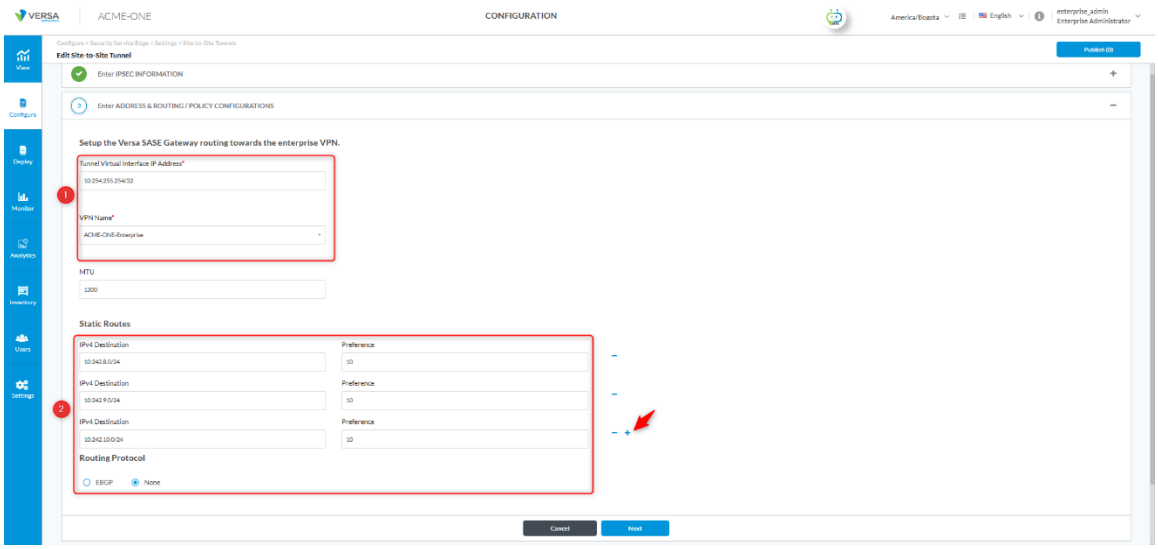
Add a Tunnel Virtual Interface address that is routable within your enterprise network. This typically involves using one IP from a /30 IPv4 address, with the other usable IP from the same /30 to be configured at your enterprise IPSec endpoint.

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

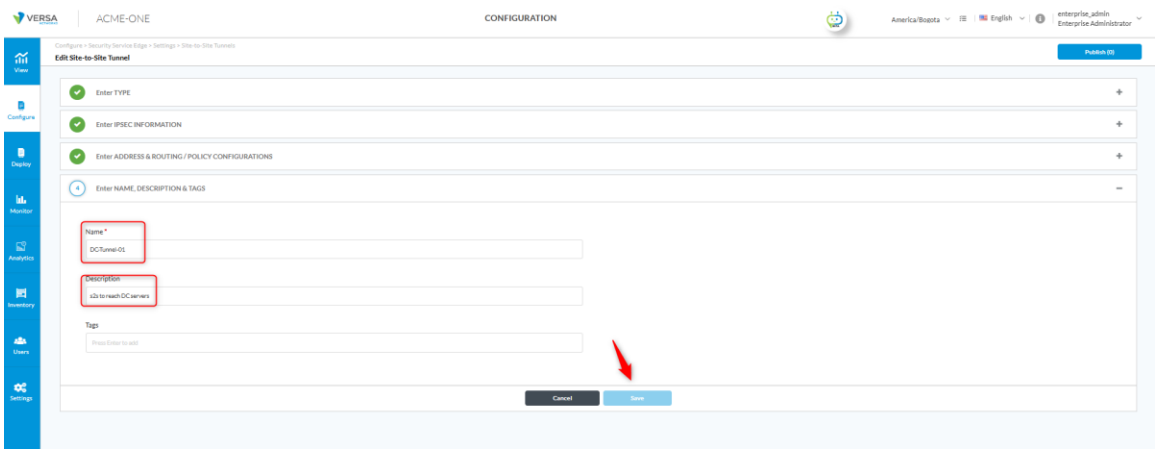
Set **MTU**: Versa recommends that the maximum transmission unit be set to 1300 for IPsec-based tunnels

Under Static Routes and Routing Protocols, configure the following

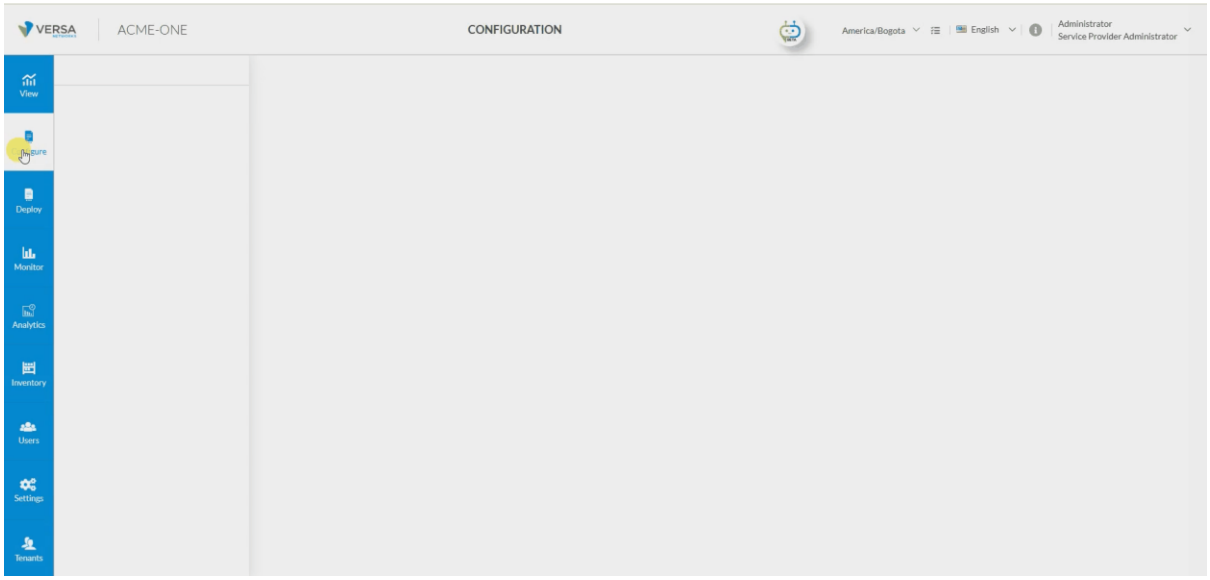
- Click **+ Add** to create a new route.
- Set Routing Protocol to None.
- Enter the destination subnet. (In our case, we need to enter the server subnets one by one: 10.242.8.0/24, 10.242.9.0/24, 10.242.10.0/24).
- Assign a preference value between 1–255 (lower = higher priority).
- Routing Protocol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

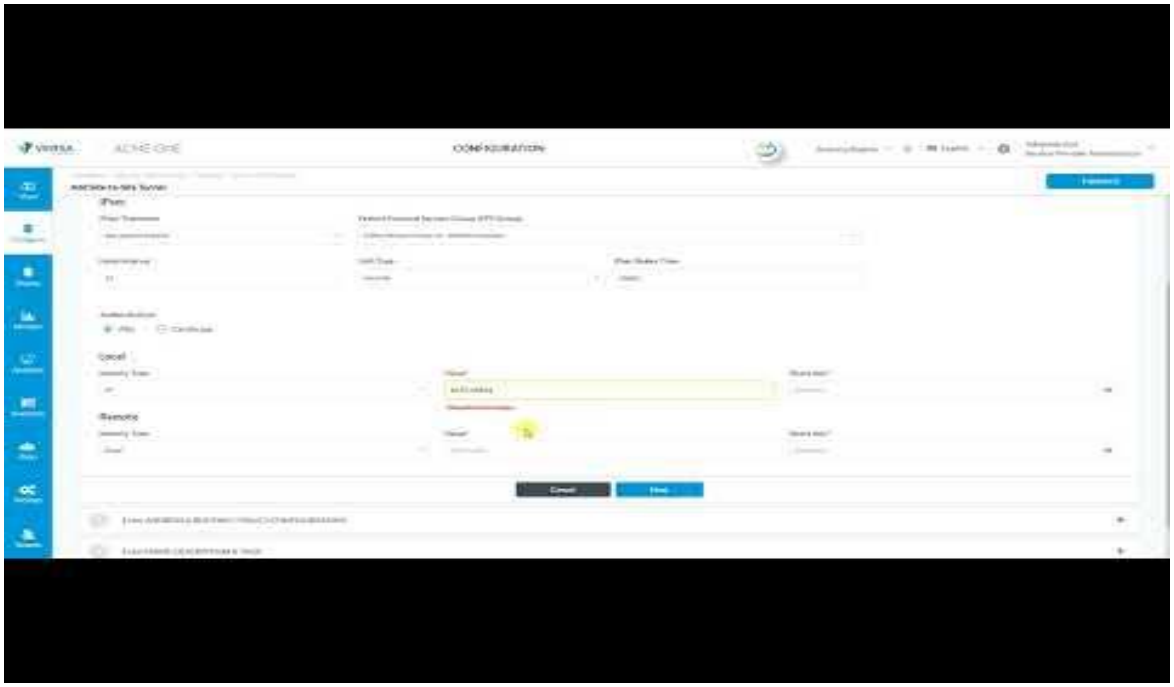


4. Completing section Enter NAME, DESCRIPTION & TAGS



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.

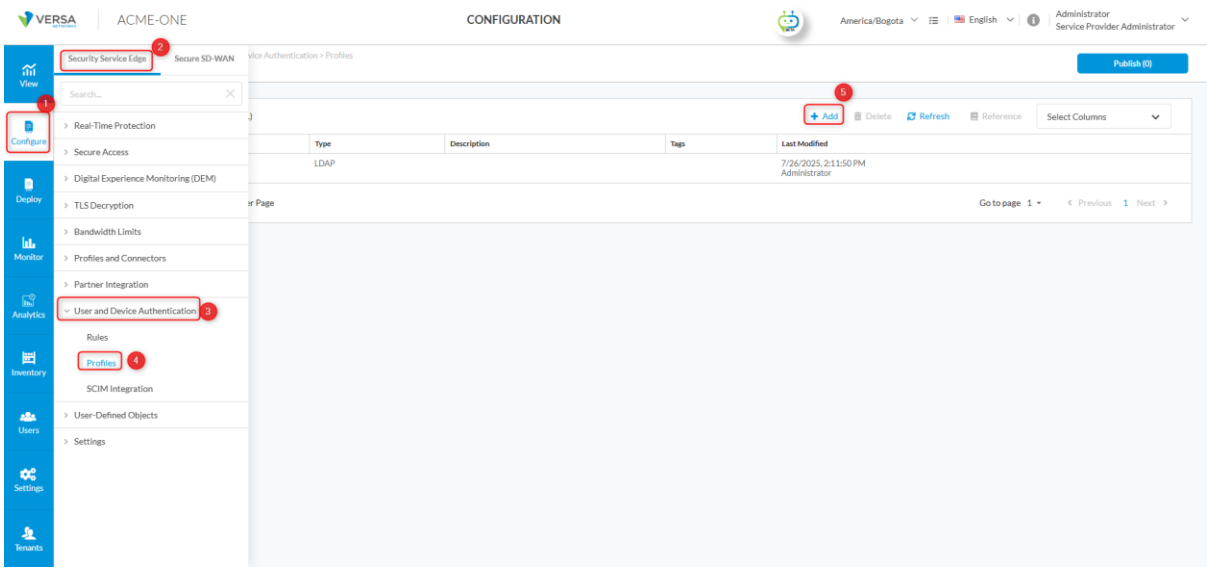
LDAP Active-Directory

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.

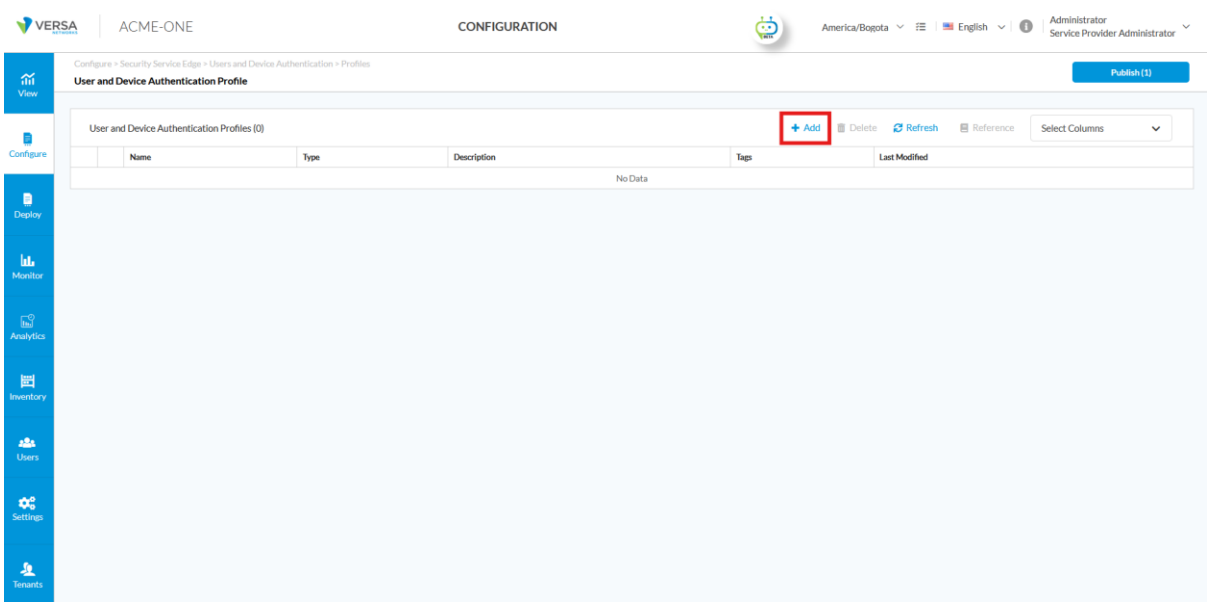
- SSL Enabled – To ensure secure communication to the LDAP server. (In our case, we are using SSL disabled)
- Add secondary Server – To ensure redundancy in case of failure of the Primary server.

Navigate to

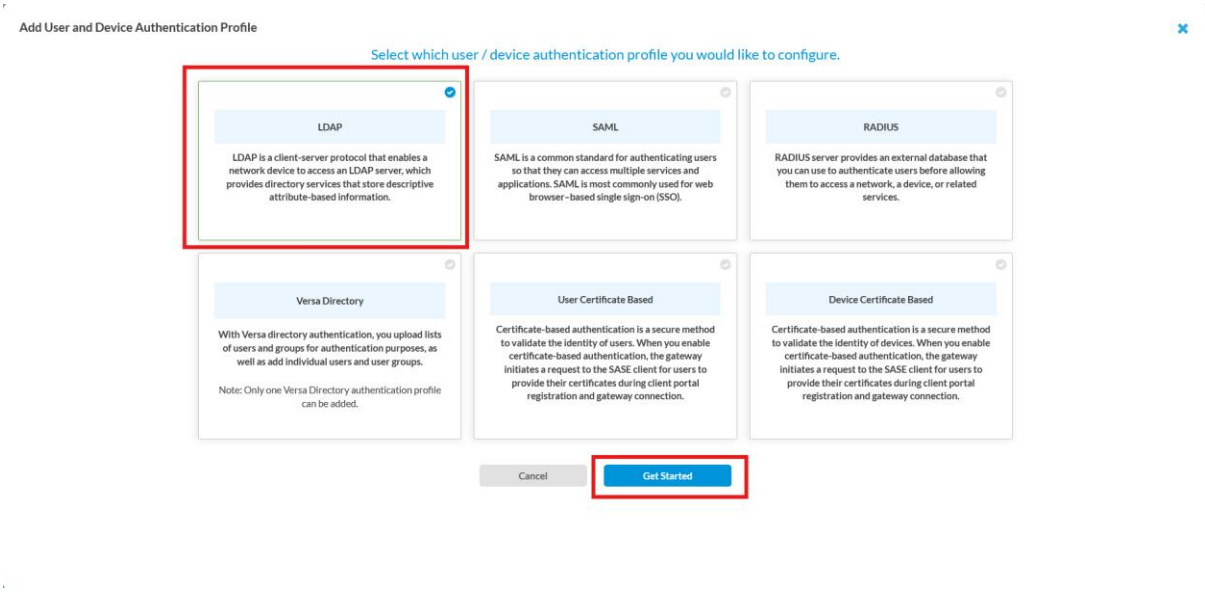
Configure > Security Service Edge > User and Device Authentication > Profiles and click **+ Add** and follow these steps. Refer to the image below.



Click **+ *Add***



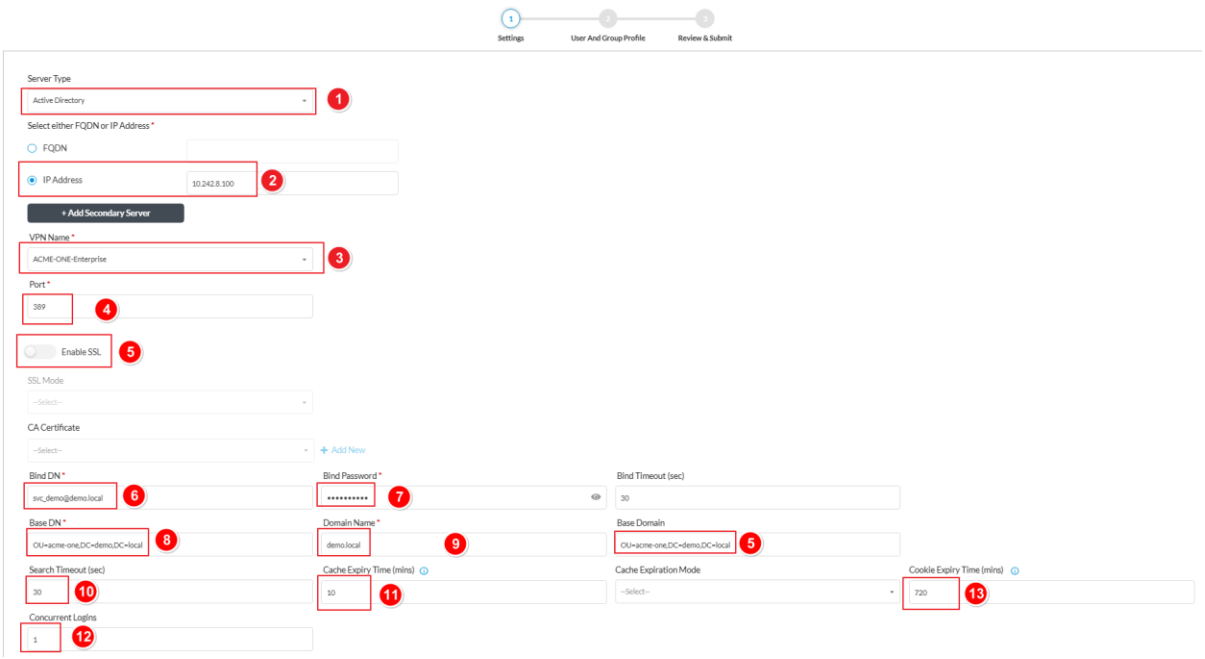
Select **LDAP** as Authentication Method then Click **Get Started**



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.

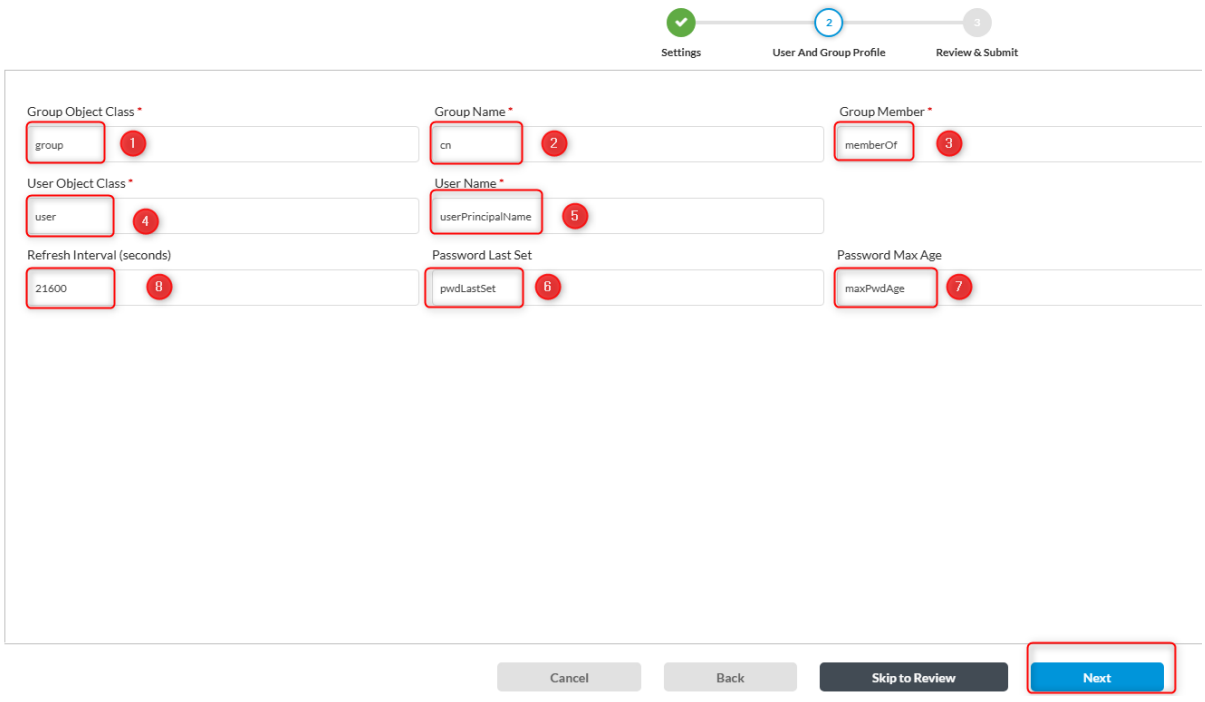


Parameter	Description	Current Use Case
1. **Server Type**	Indicates if the authentication source is Microsoft Active Directory or Open-LDAP.	Active Directory
2. **FQDN or IP Address**	Fully Qualified Domain Name (FQDN) or IP address of the AD/LDAP server.	10.242.8.100
3. **VPN Name**	Defines which VPN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

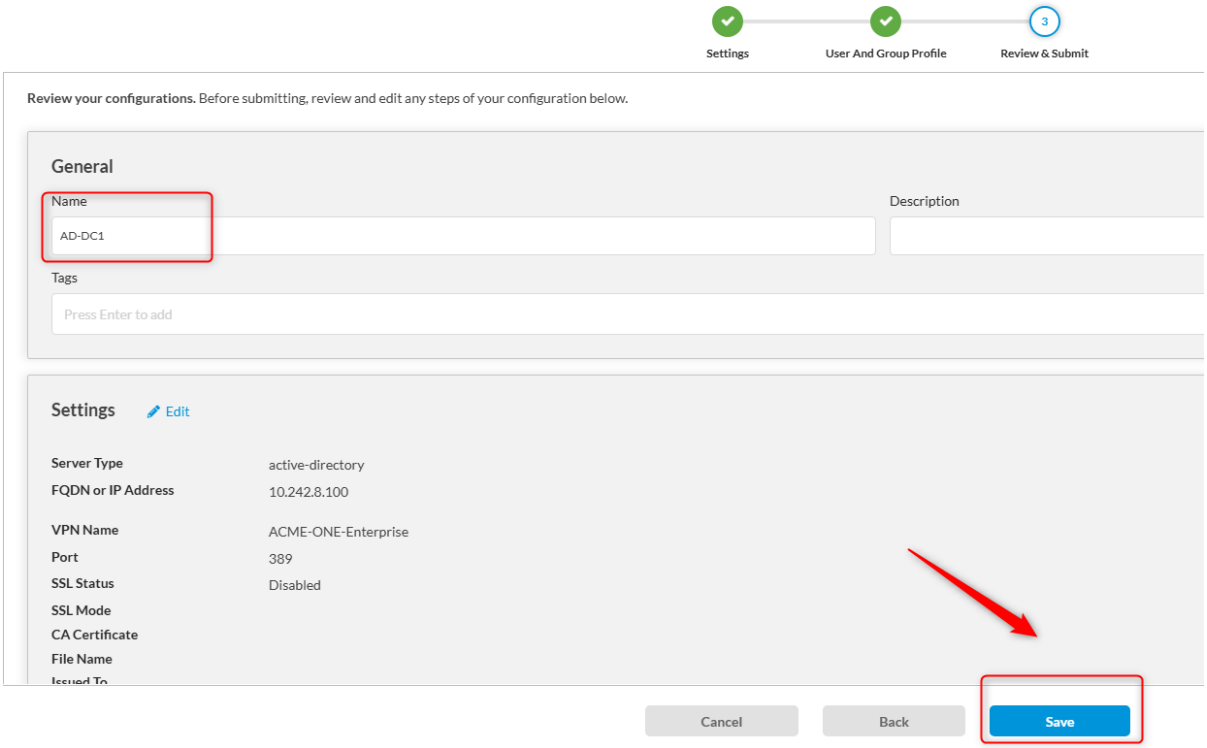
1. **Group Object Class**	group	Standard AD object class for security and distribution groups. Required for identifying groups in the directory.
2. **Group Name**	name	Attribute that defines the display name of a group. Used by Versa to match groups during policy evaluation.
3. **Group Member**	memberOf	Attribute that lists group memberships for a user object. Ensures Versa can apply policies based on AD group membership.
4. **User Object Class**	user	Standard AD object class for user accounts. Required for identifying users in the directory.
5. **User Name**	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. **Password Last Set**	pwdLastSet	Attribute indicating when a user's password was last changed. Useful for enforcing password expiration policies.
7. **Password Max Age**	maxPwdAge	Attribute defining the maximum password lifetime. Derived from the AD domain password policy.
8. **Refresh Interval (sec)**	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.

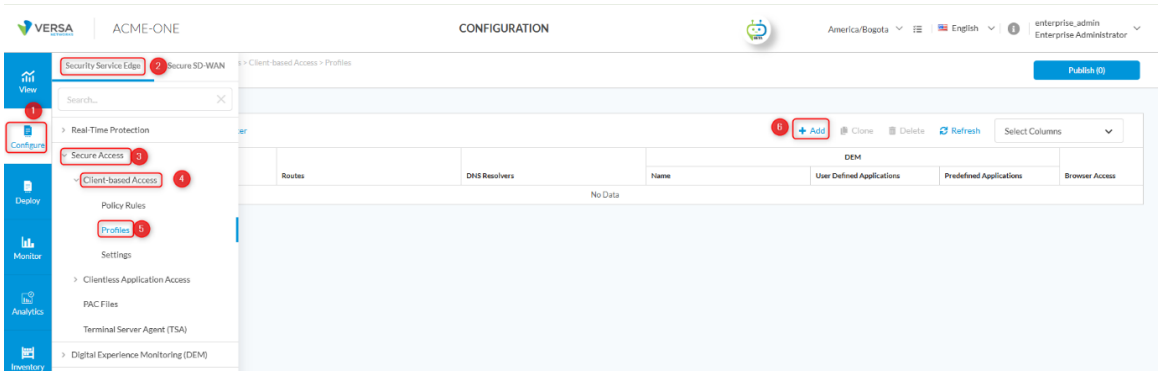


Note: - The scope of Active Directory read access depends on the AD administrator. In our case, access has been granted to the **OU=ACME-ONE** within the global domain **demo.local**, using the designated service account.

Step 3: Configure DNS and Private Routes

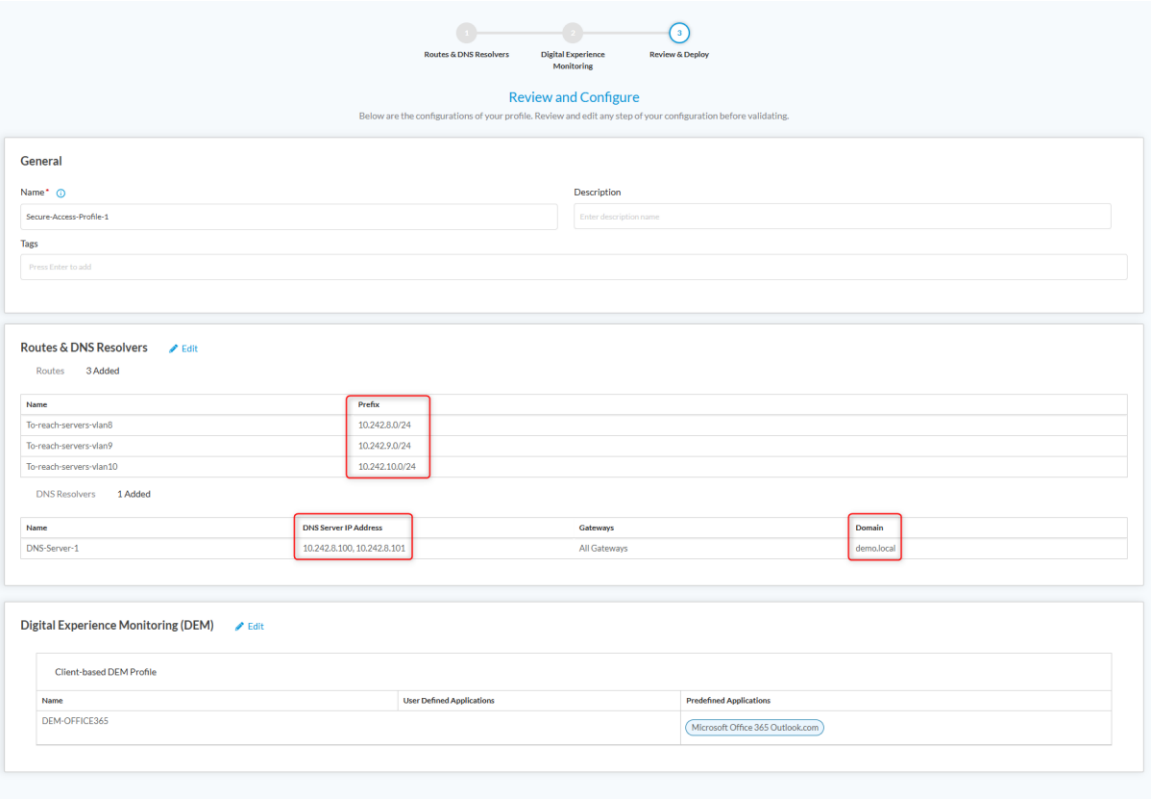
In the VSPA use case, to facilitate the resolution of private applications when a user connects remotely and to route all private application traffic from the SASE client, Secure Access Profiles are employed to define DNS Resolvers, Private Routes and DEM (application performance monitoring).

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.



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:

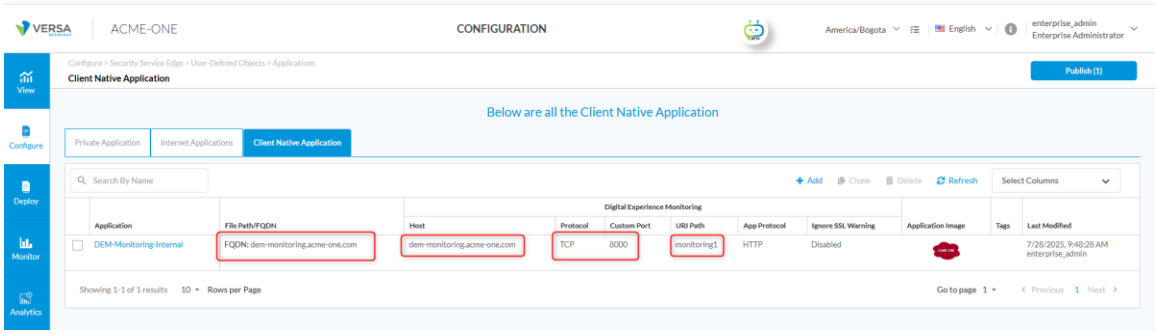
- Any application that needs to interact with the **client** or be referenced in a **Secure Access Rule** must be defined as a **Client Native Application**. For split tunnelling or DEM use case.
- Applications that interact with the **gateway** or are referenced in **Real-Time Protection Rules** must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

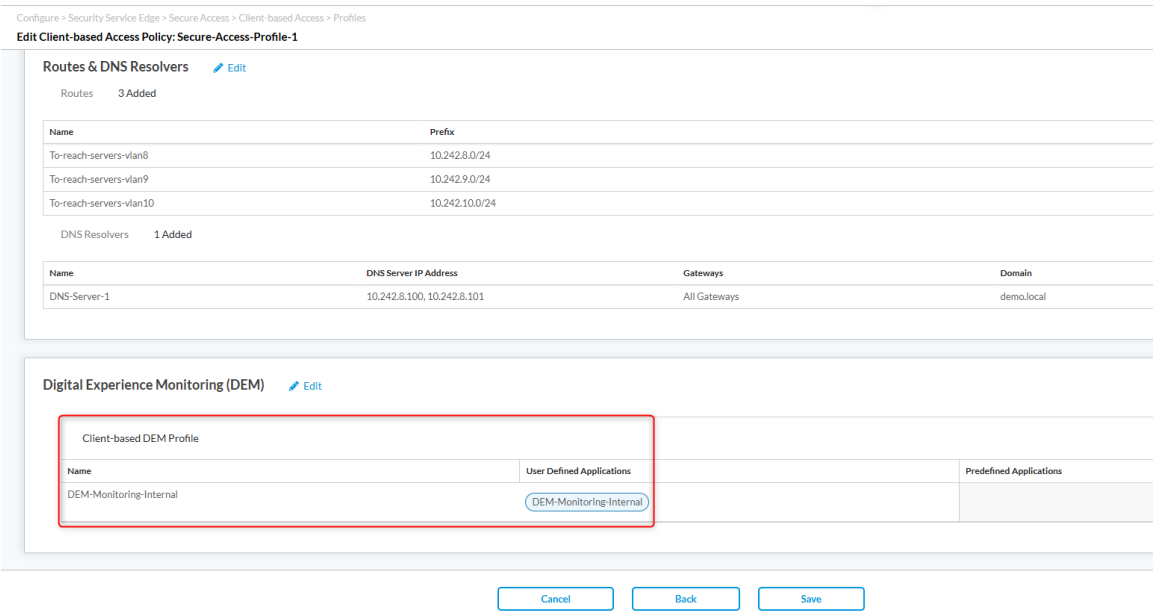
To create a **Client Native Application**, navigate to

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

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



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



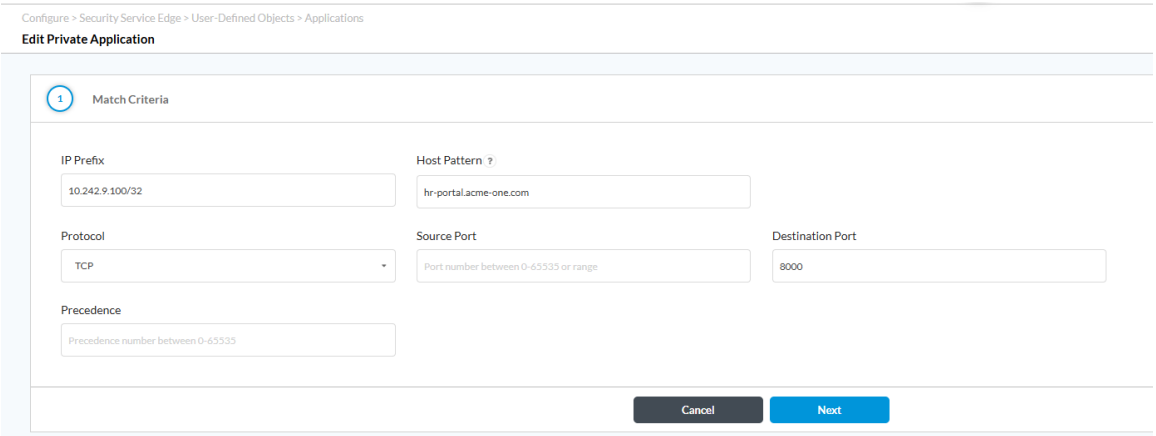
To create a **Private Application**, navigate to

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

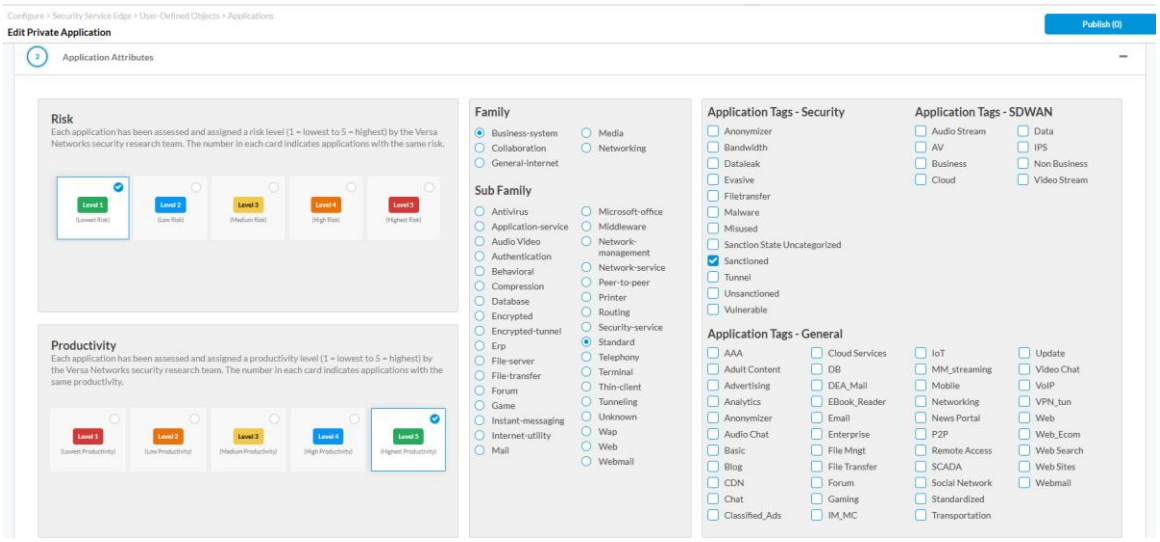
Then, create the test apps **hr-portal.acme-one.com** and **financial-apps.acme-one.com** as follows:

hr-portal.acme-one.com:

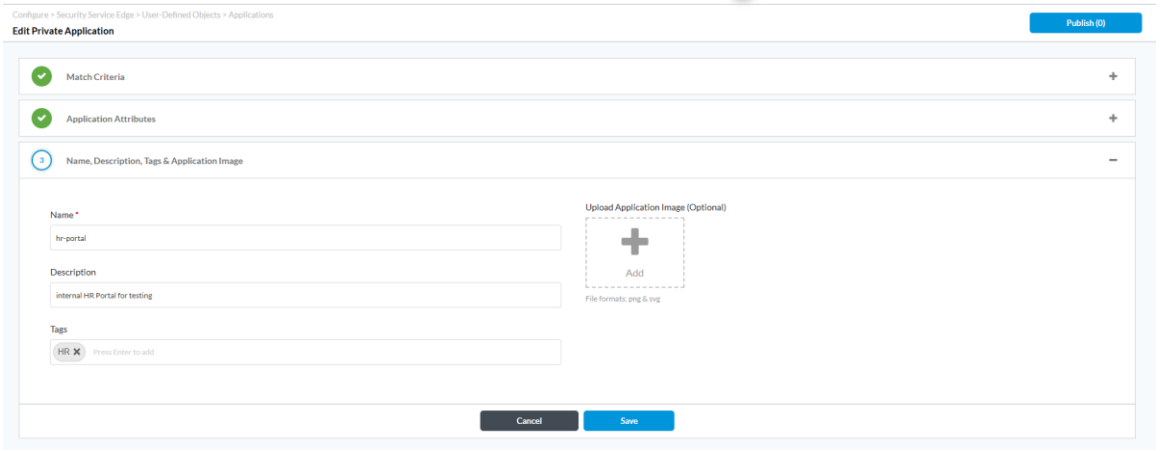
- Step 1: Match Criteria



- Step 2: Application Attributes

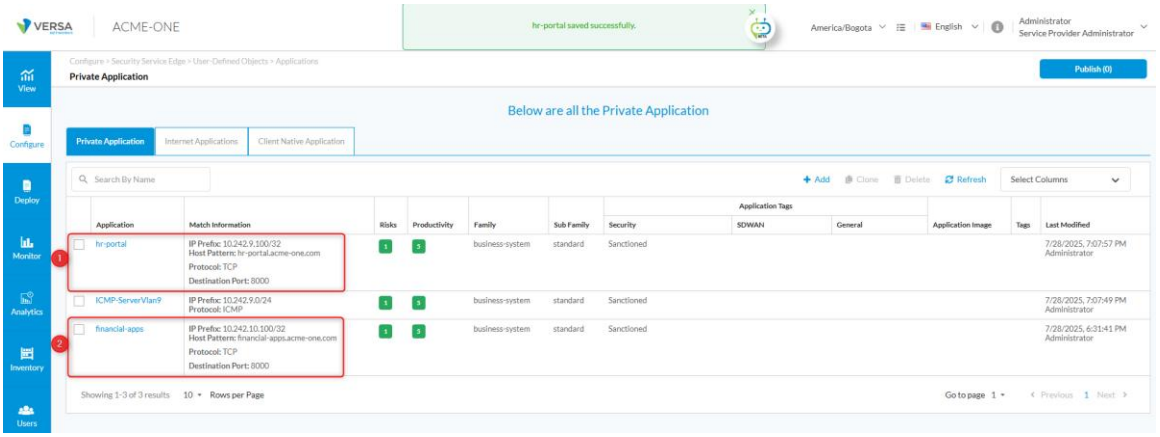


- Step 3: Name, Description, Tags & Application Image



Do the same for the other application (**financial-apps.acme-one.com**) or any other one you want to test.

The private app definitions should resemble the image below.

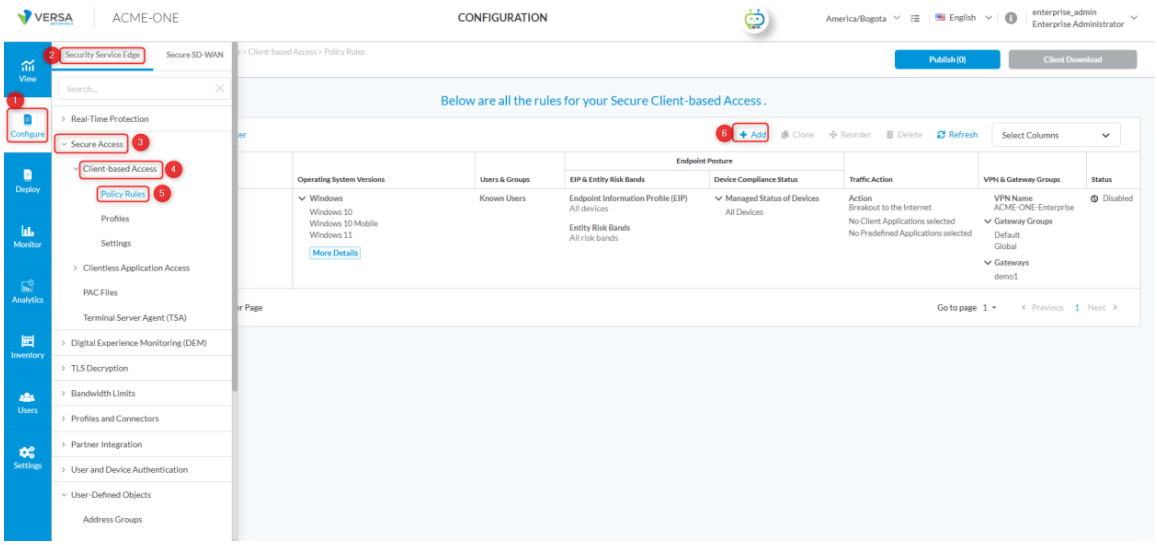


Step 5: Secure Client Access Rules

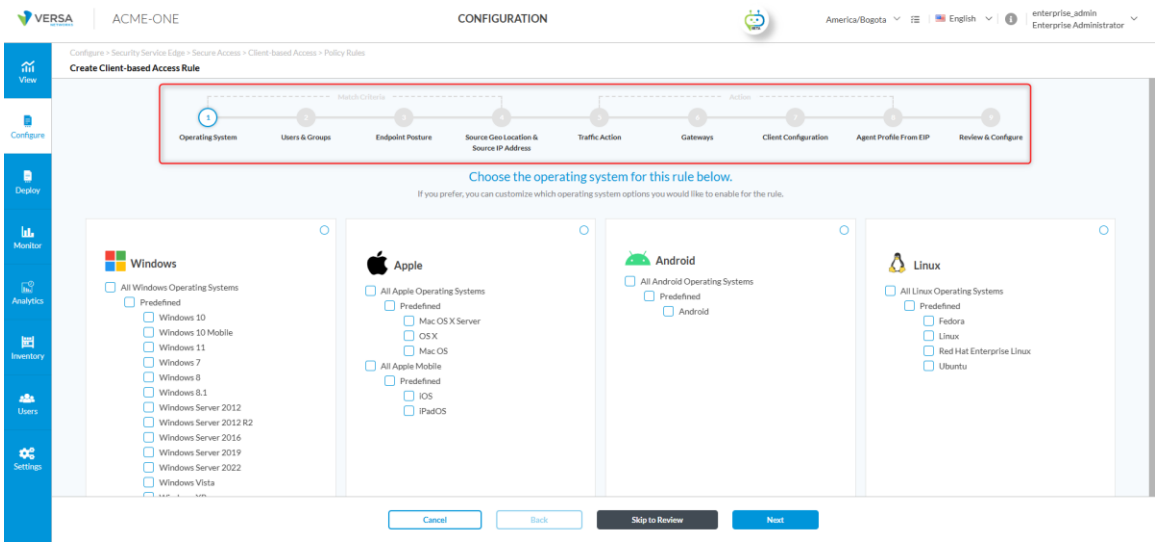
Secure Access rules define the connection between the end user machine (that is installed with Versa SASE Client) and the SASE gateway. Secure Client Access defines who, how, and under what conditions a user can connect to the gateway, including SASE client features and the type of traffic sent to the 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:

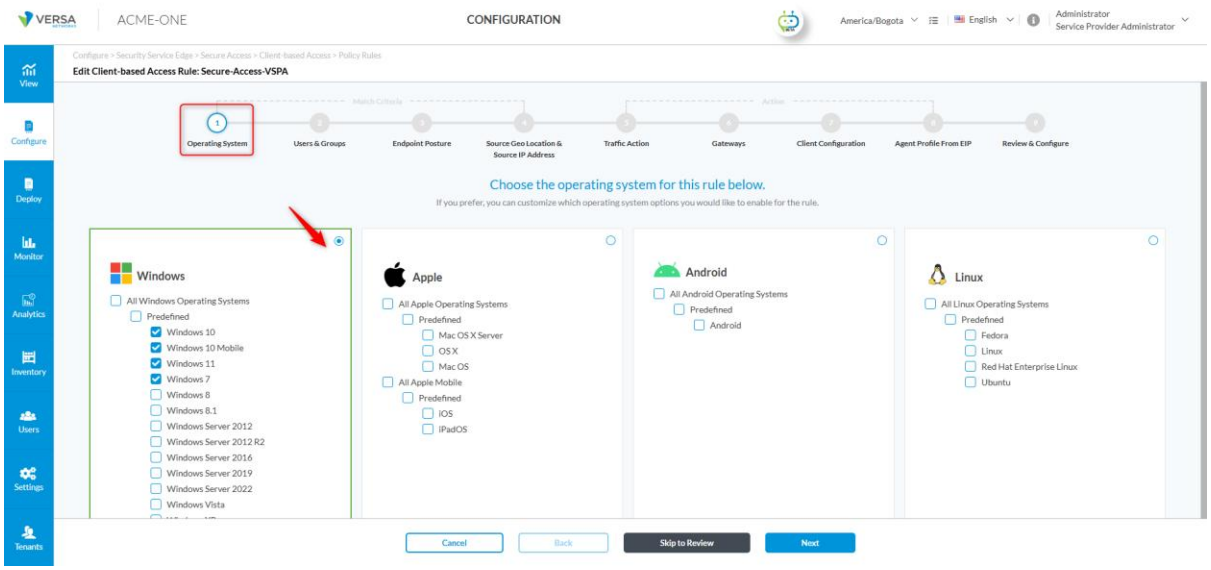
Knob	Current Use Case	Reason	Best Practice (Production)

Operating Systems	Windows 7, 10, 11	Ensures compatibility with supported Windows OS versions in the enterprise.	Limit to *supported/managed OS versions only* (e.g., Win10/11). Block EOL OS (Win7) to reduce risk.
Users & Groups	All required user groups (Contractors, Finance, HR, IT, VIP, etc.)	Broad inclusion for testing.	Apply **least-privilege access**: 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.
Endpoint Posture	Management Status: All devices EIP Profile: eip-profile-antimalware-any	Enforces the presence of anti-malware.	Require managed devices and endpoint compliance where possible. Strengthens endpoint hygiene
Source Geo Location	All	No geo-restriction defined.	Restrict access to **approved geographies** where the company operates. Deny or challenge high-risk regions.
Source IP Address	None	As users are remote	We can define an IP address to enforce the user connection from a specific location and a WAN circuit.
Traffic Action	VSPA (Secure Private Access)	Secure access to internal applications.	Same as lab.
Gateways	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.
Client Configuration	Define routes and DNS resolvers	Ensures reachability of internal resources and split-DNS.	Same as lab. Add redundancy with **multiple DNS resolvers**.
Secure Client Access Profile	Secure-Access-Profile-1	Select the profile created in step 3	Same as lab
MFA	Disabled	Not required in the lab.	**Enable MFA** (Email or TOTP as per the requirement). Critical for Zero Trust.
VPN Type	All (IPsec, TLS, DTLS)	Flexibility during lab testing.	Define the order of preference (Recommended: DTLS > IPsec > TLS).
Client Controls	Default values	Defaults are sufficient for the lab use case.	Harden controls (Tamper Protection, Tunnel Monitoring, Always-

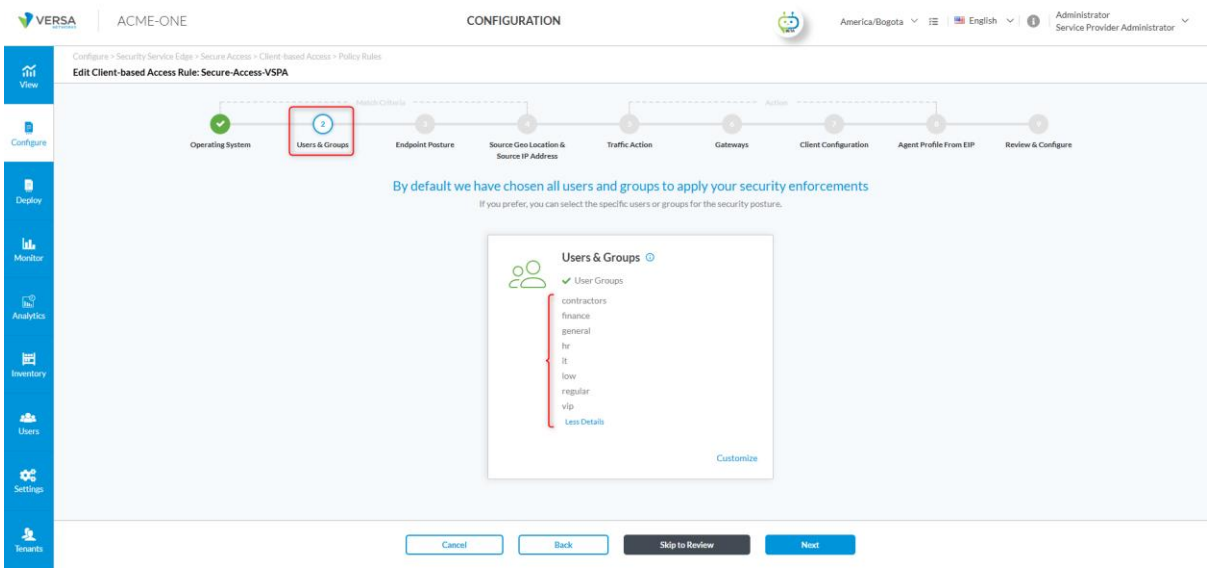
			On with Trusted Network Detection).
EIP Agent Profile	Blank (example: AntiMalware_category_all)	Optional in the lab.	**To** enforce real-time posture evaluation with EIP. Continuous evaluation is key for Zero Trust.

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

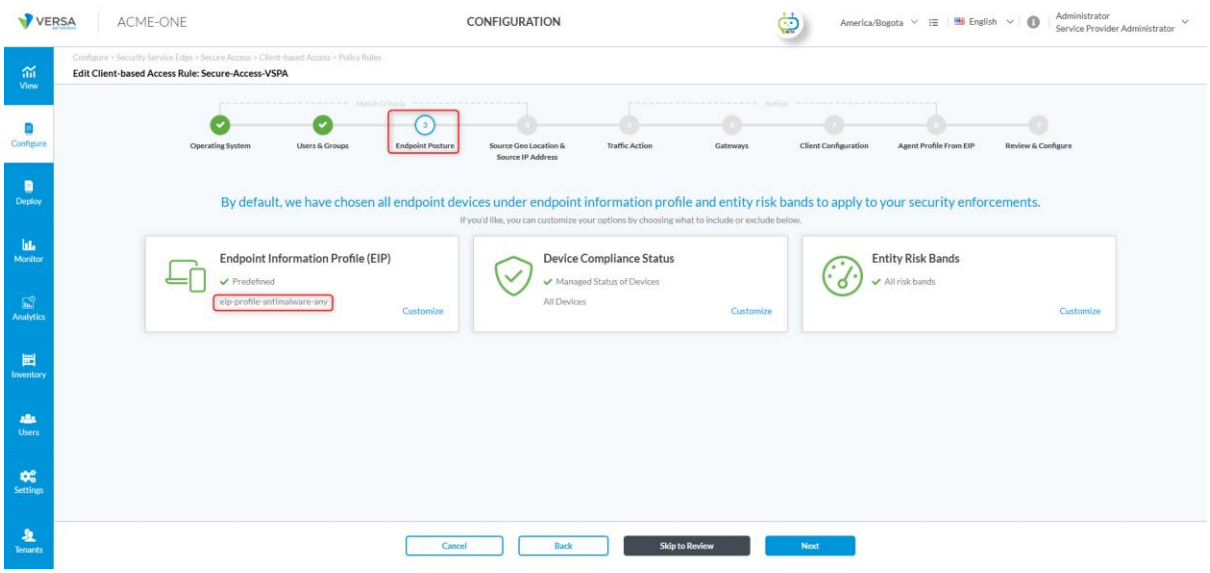
1. **Operating System:** Select Windows and choose the versions to be tested: **Windows OS** (7, 10, and 11).



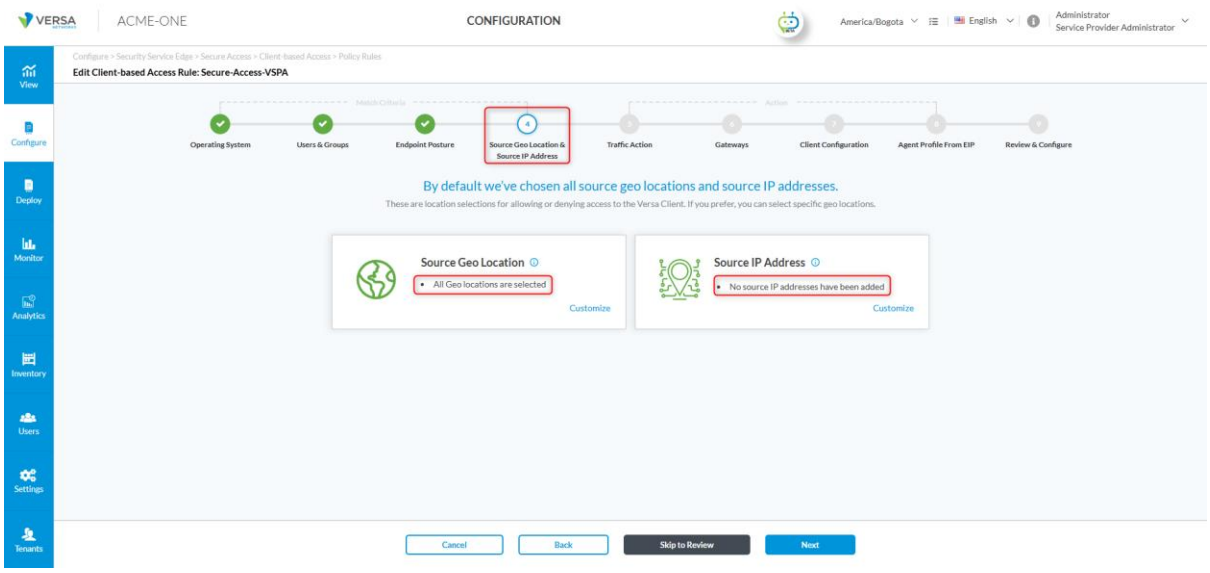
2. **Users & Groups:** Select the groups (**contractors, finance, general, hr, it, low, and vip).**



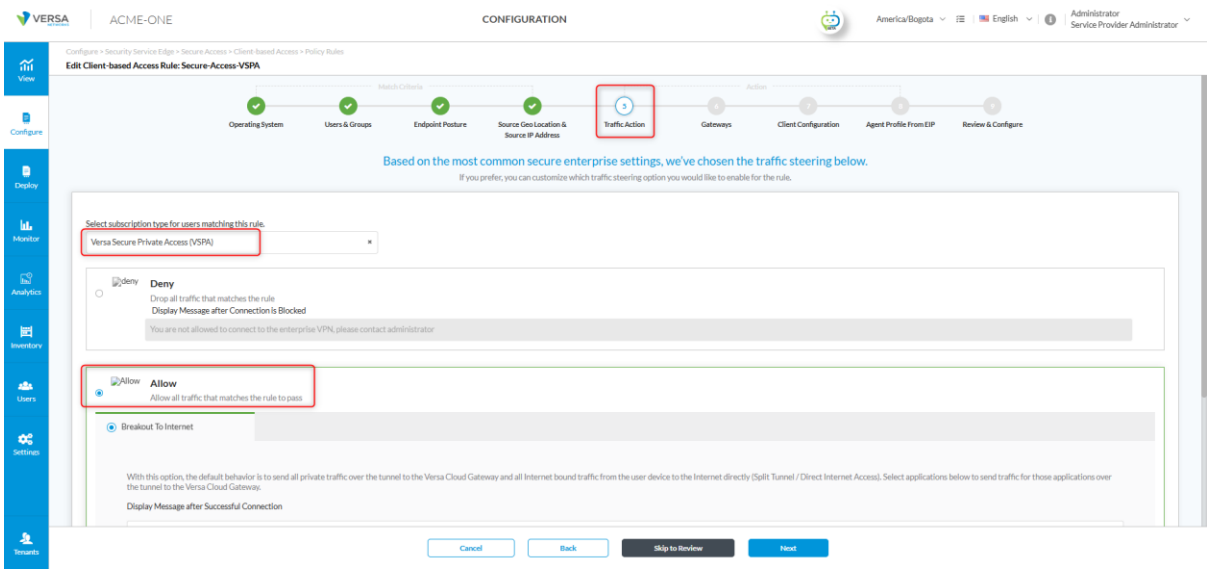
3. **Endpoint Posture:** The predetermined profile eip-profile-antimalware-any has been selected. This profile is characterized by a rule that incorporates two objects (eip-object-antimalware-any-installed and eip-object-antimalware-any-running), which are assessed using an AND condition. During the 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.**



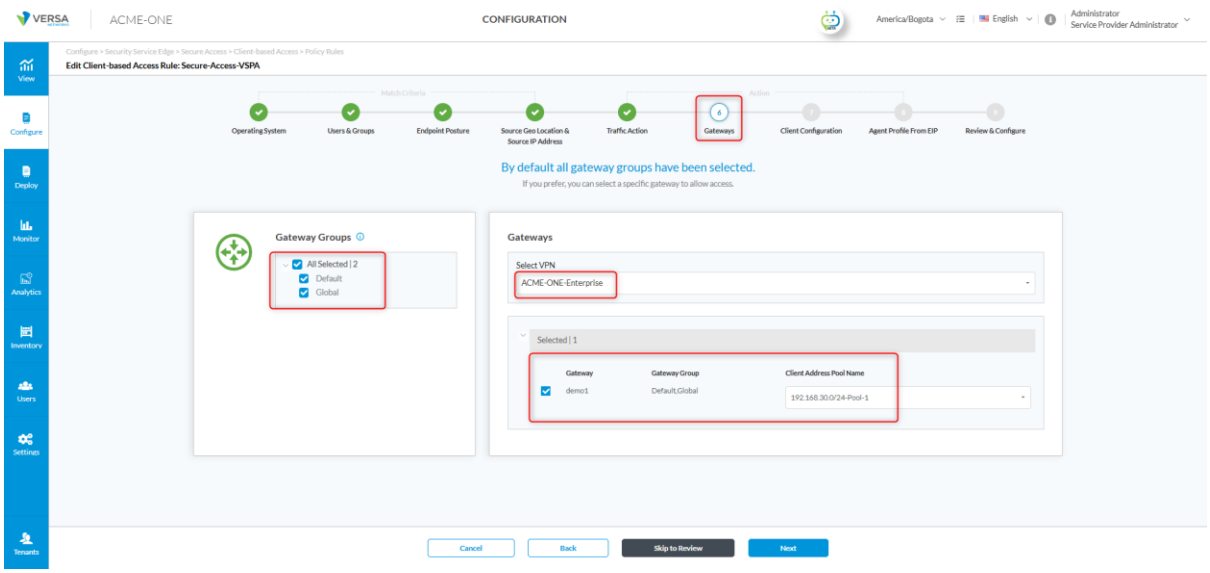
4. **Source Geo Location & Source:** Default values are used since the use case is LAB



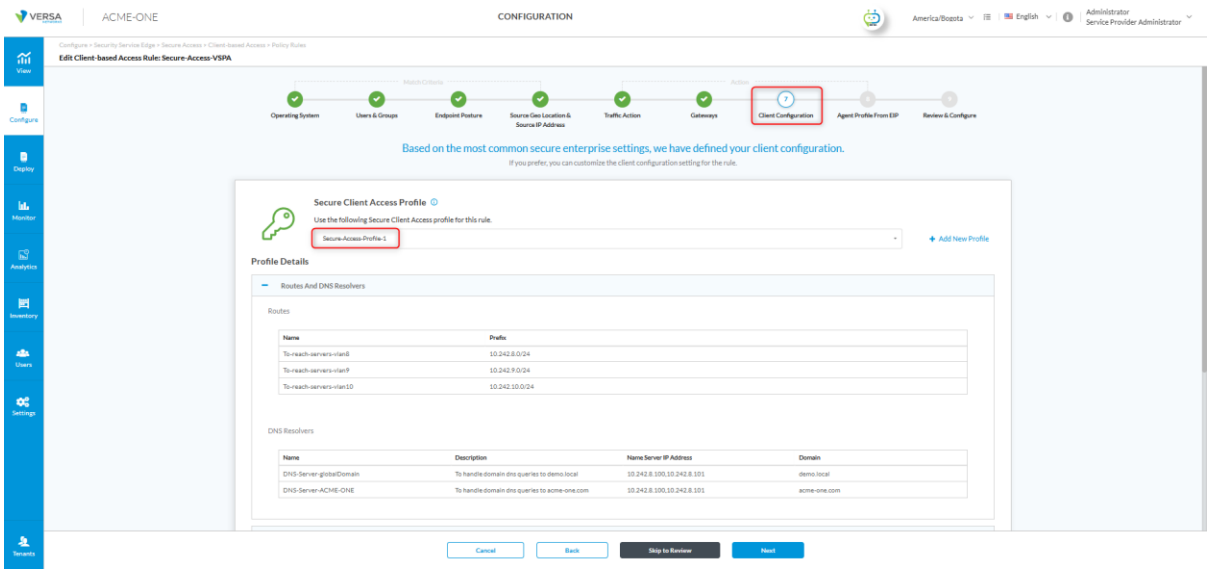
5. **Traffic Action:** The subscription type selected is **Versa Secure Private Access (VSPA)**.



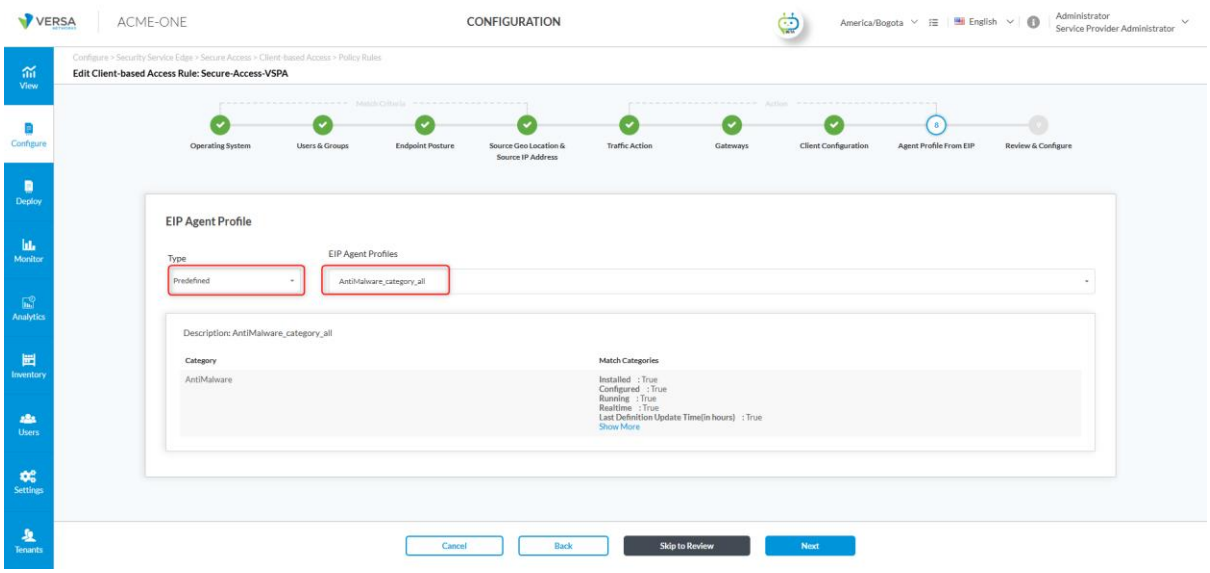
6. **Gateways:** Select the gateway groups and mark the gateways to be associated with the rule. Since there is only one gateway in our case, we selected it only.



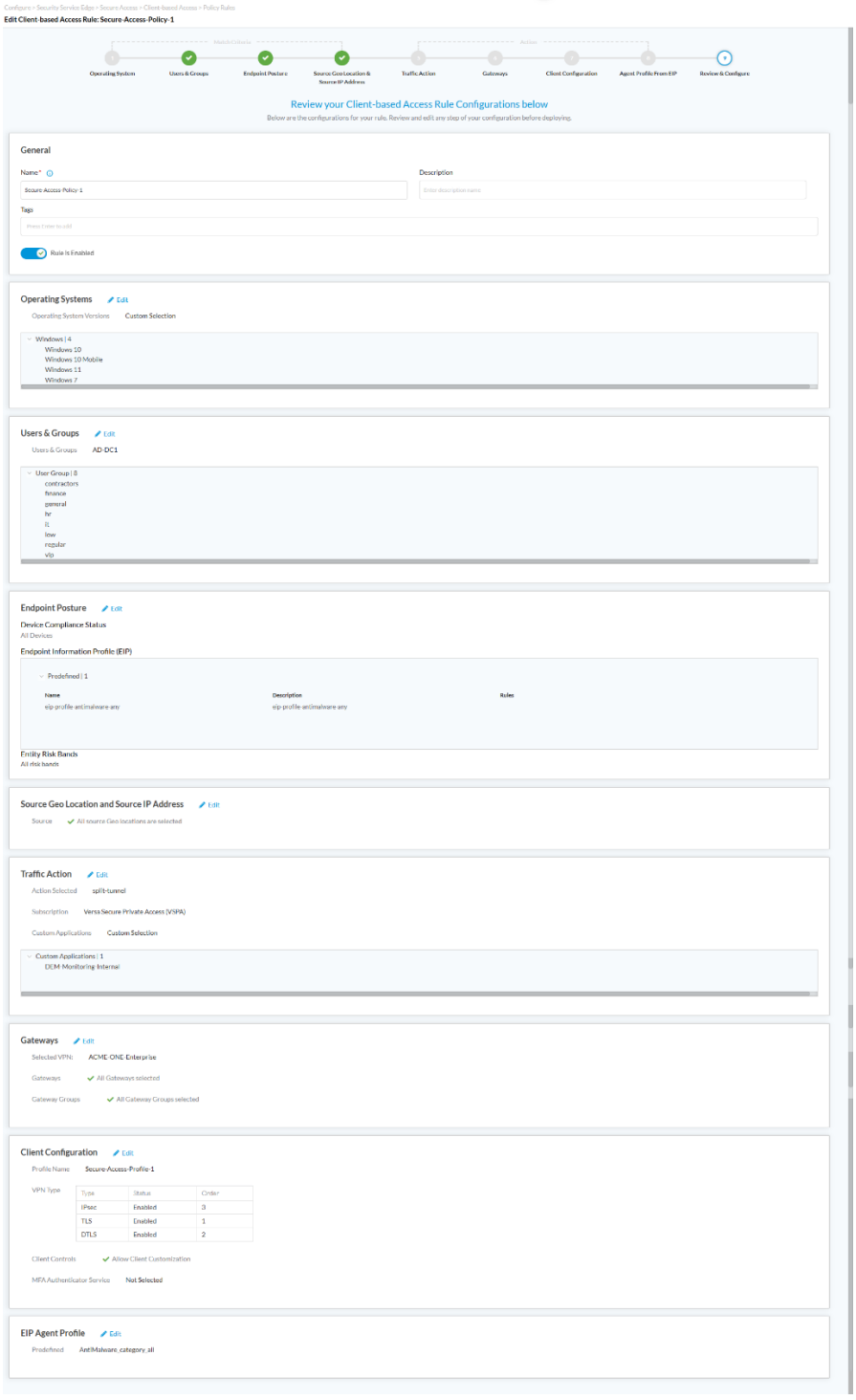
7. **Client Configuration:** Select the previously created Secure Client Access profile (Secure-Access-Profile-1).



8. **Agent Profile From EIP:** Select the predefined type, and in EIP Agent Profile, choose Antimal-ware_category_all.



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



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

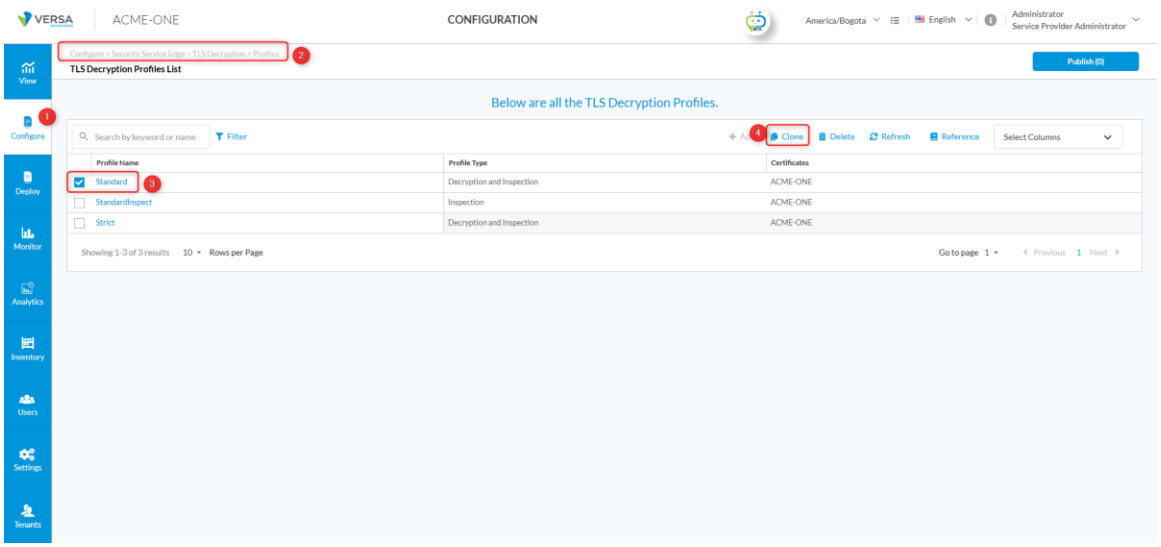
version restrictions, the activation of OCSP verification, and the customization of additional settings to ensure secure traffic inspection.

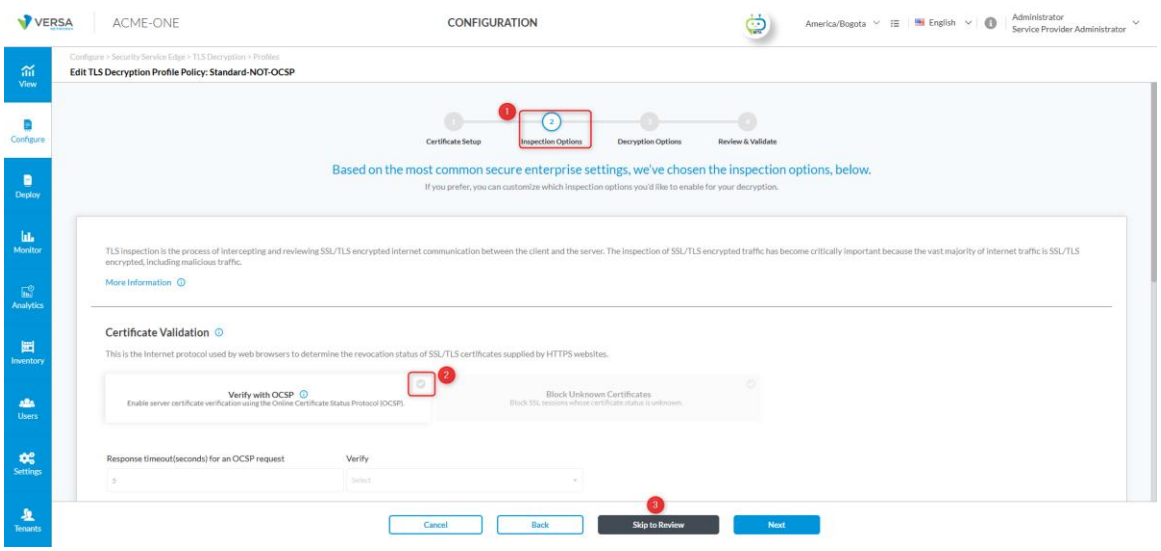
In our scenario, we will create a decryption profile that conducts standard inspection without OCSP verification, as this pertains solely to VSPA where OCSP verification may not be necessary. This can be accomplished by cloning the Standard profile and disabling the OCSP verification option. Moreover, 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.





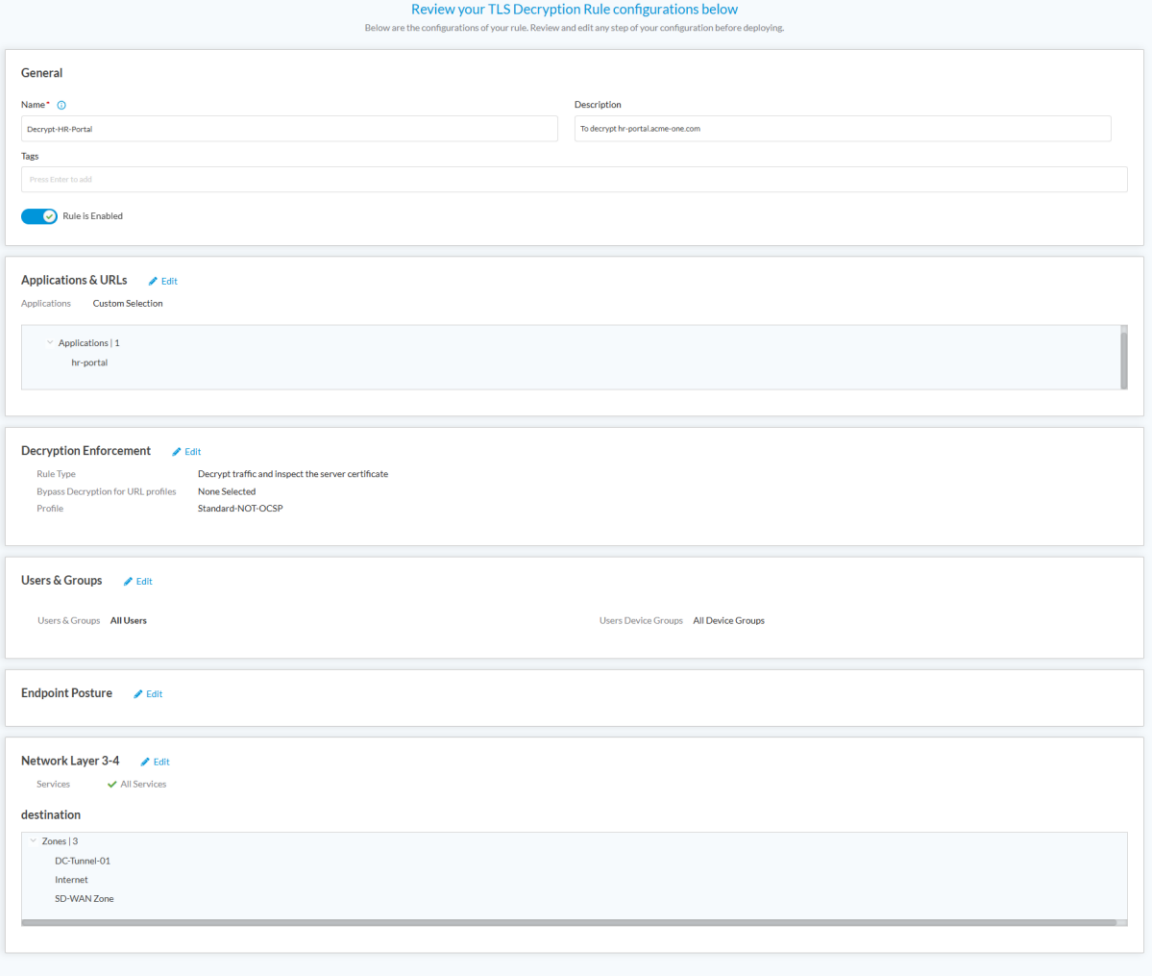
Now we can create our TLS Decryption rules — one to inspect traffic to hr-portal.acme-one.com and another to bypass decryption for financial-apps.acme-one.com.

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.

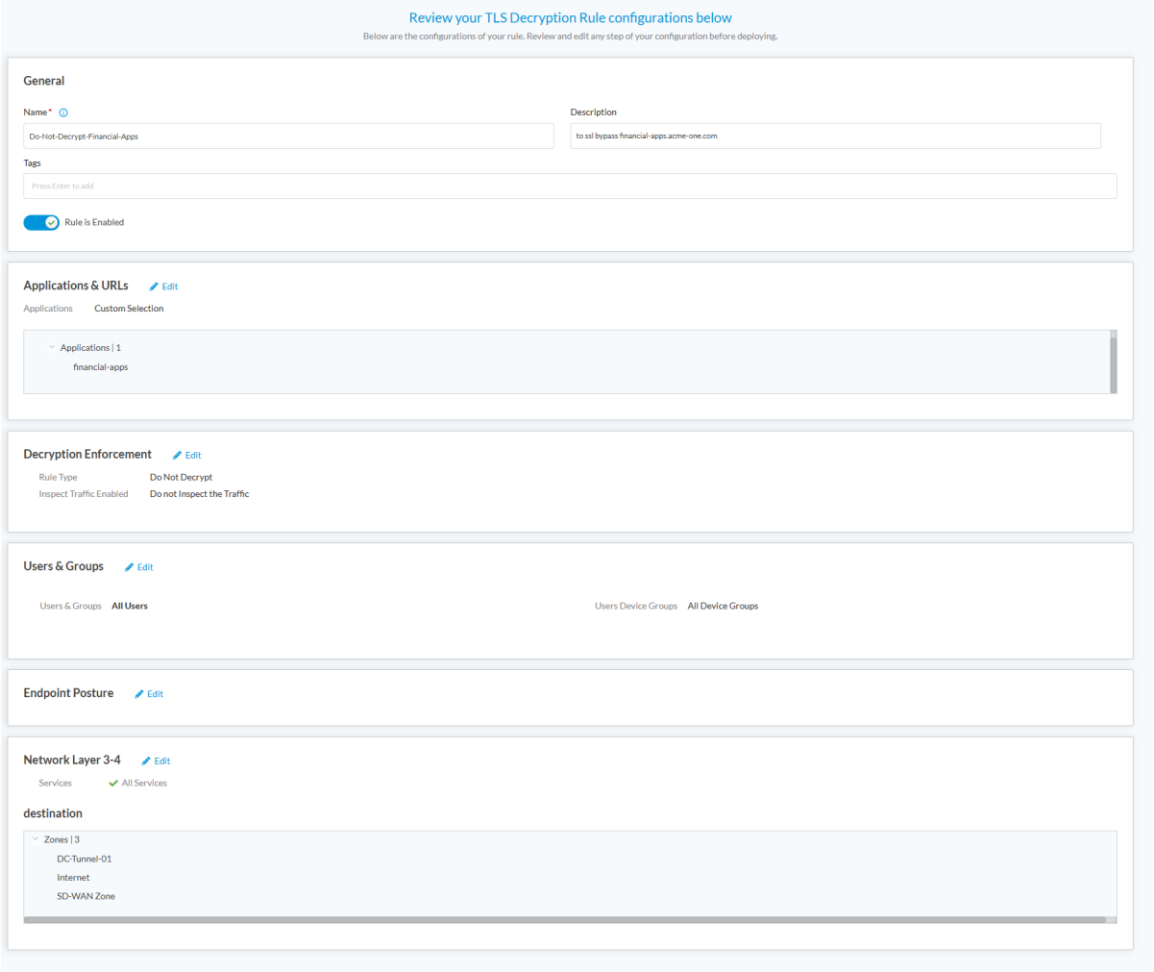


TLS Decryption Rule 2:

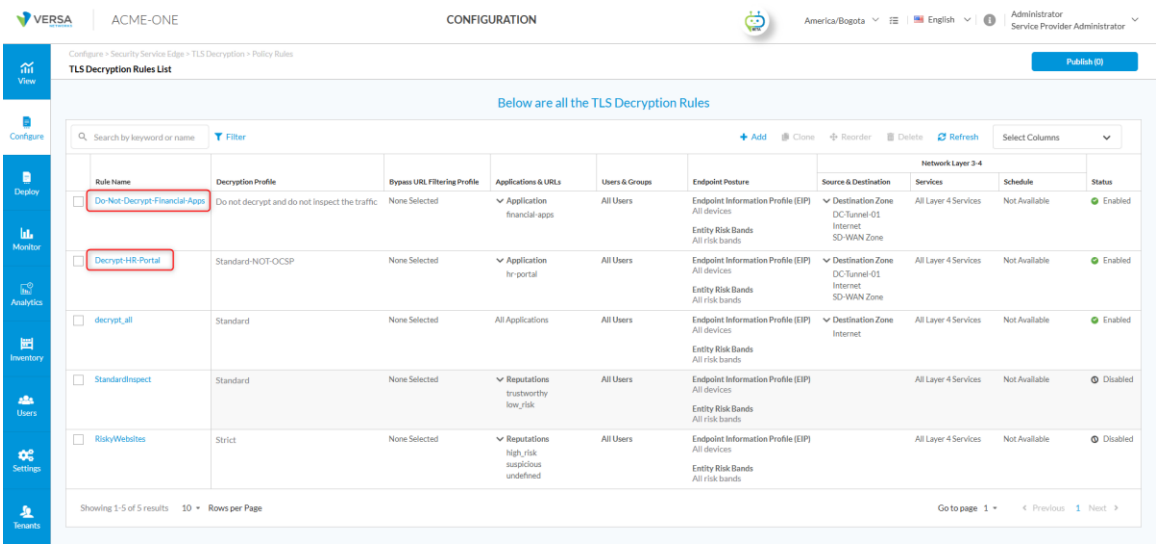
Navigate to the following path to create the rule:

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.



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



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'.

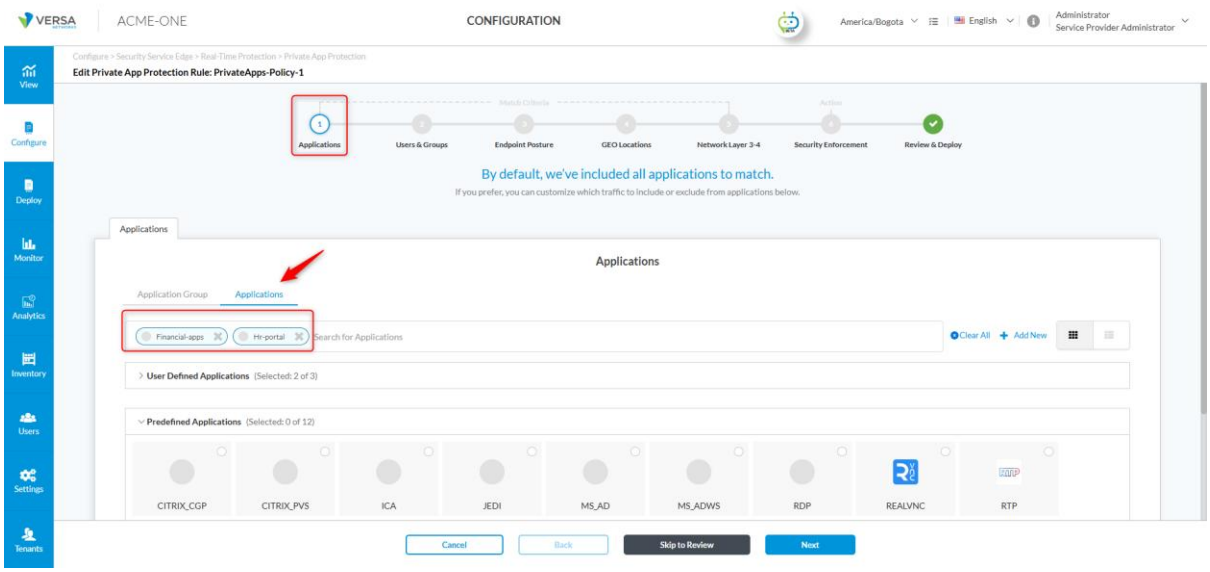
- For this example, we are setting up the rule according to these requirements:
- Applications: (financial apps and hr-portal)
- Users & Groups: vip from (AD-DC1)
- Endpoint Posture: default (All Devices)
- Source & Destination: default (DC-Tunnel-01 and SD-WAN Zone)
- Services: default (All layer 4 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 (Lab Example)	Reason / Rationale	Best Practice (Production)

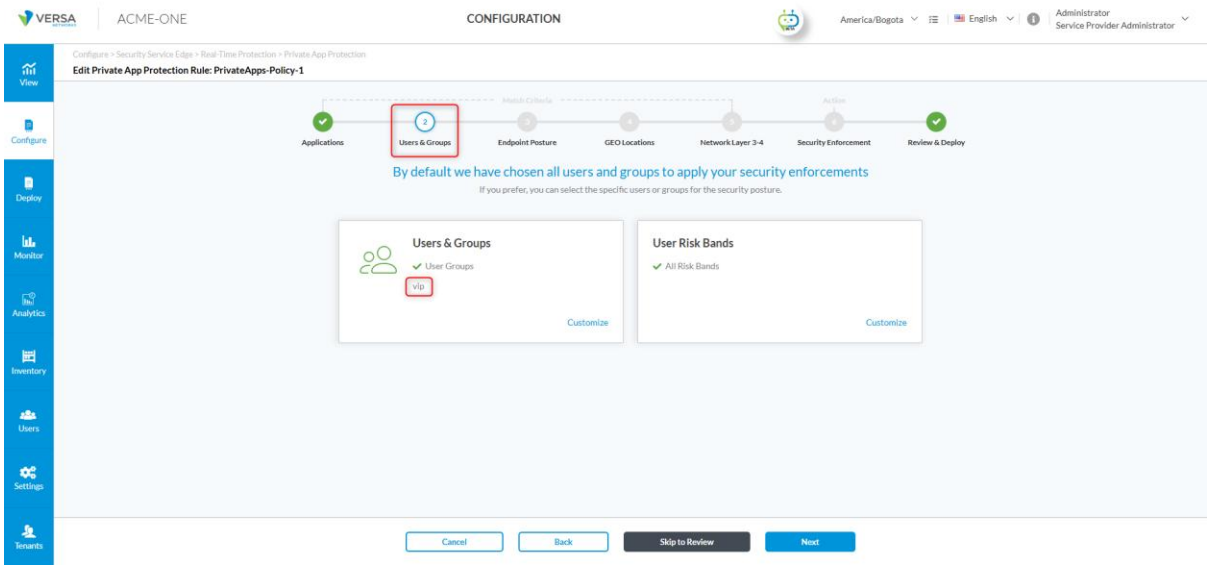
Applications	Financial Apps, HR-Portal	Focuses on protecting sensitive business apps.	Expand to **all critical private apps**. Use app tags/groups for scalability.
Users & Groups	vip (from AD-DC1)	Targets high-value users (execs/VIPs).	Apply **role-based segmentation** (e.g., Finance group → Finance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

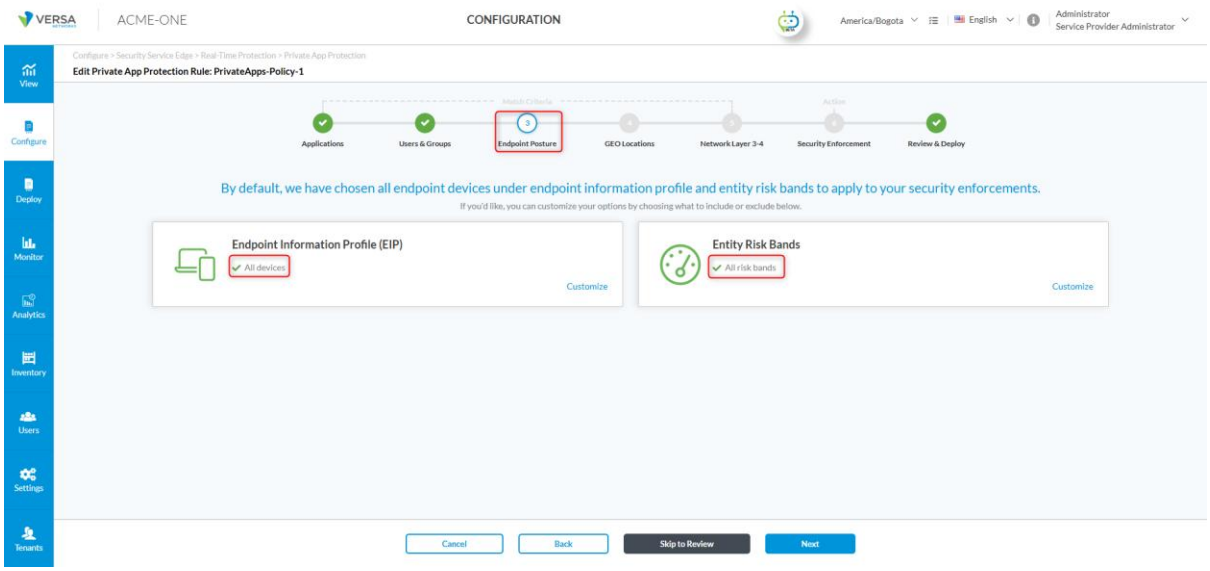
1. **Applications:** Select the previously created applications: **Financial-apps** and **HR-Portal**.



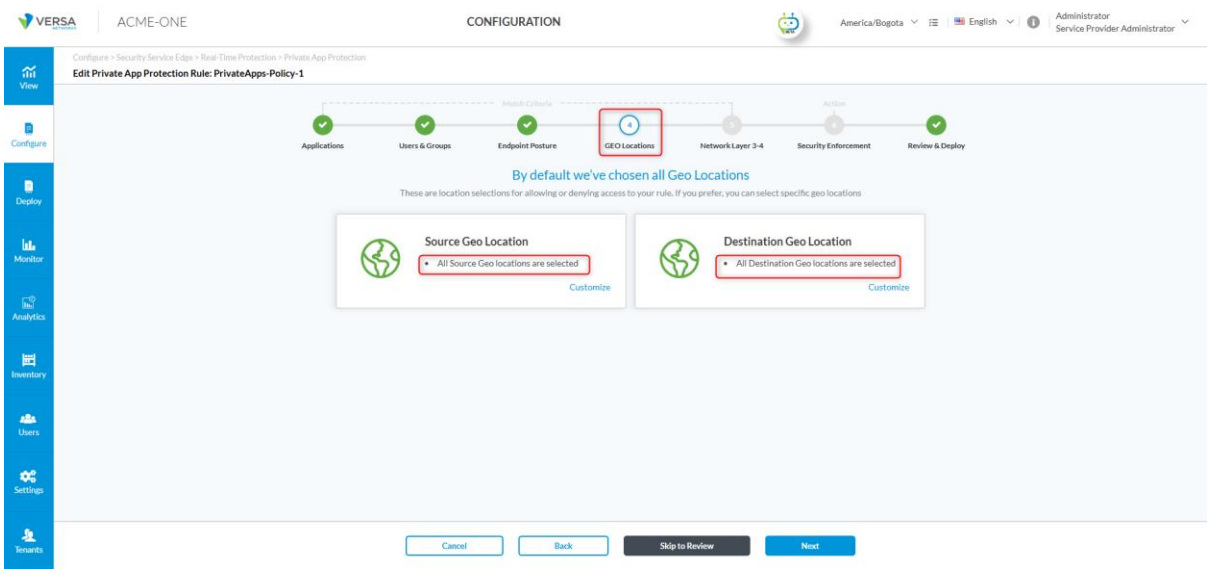
2. **Users & Groups:** Select the vip group for our example.



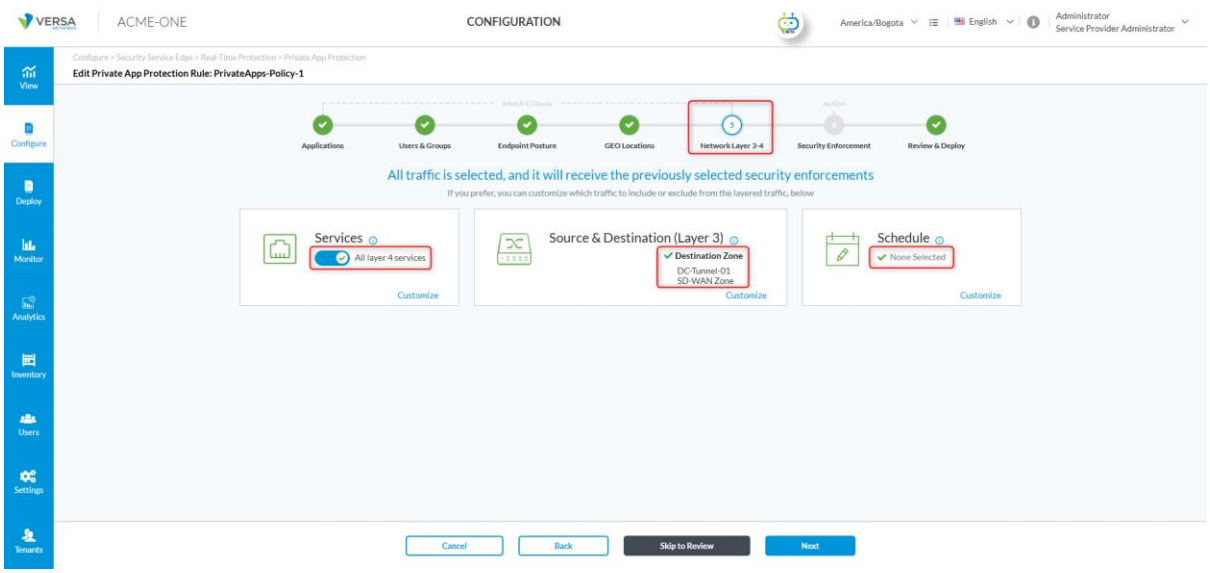
3. **Endpoint Posture:** Default values are used.



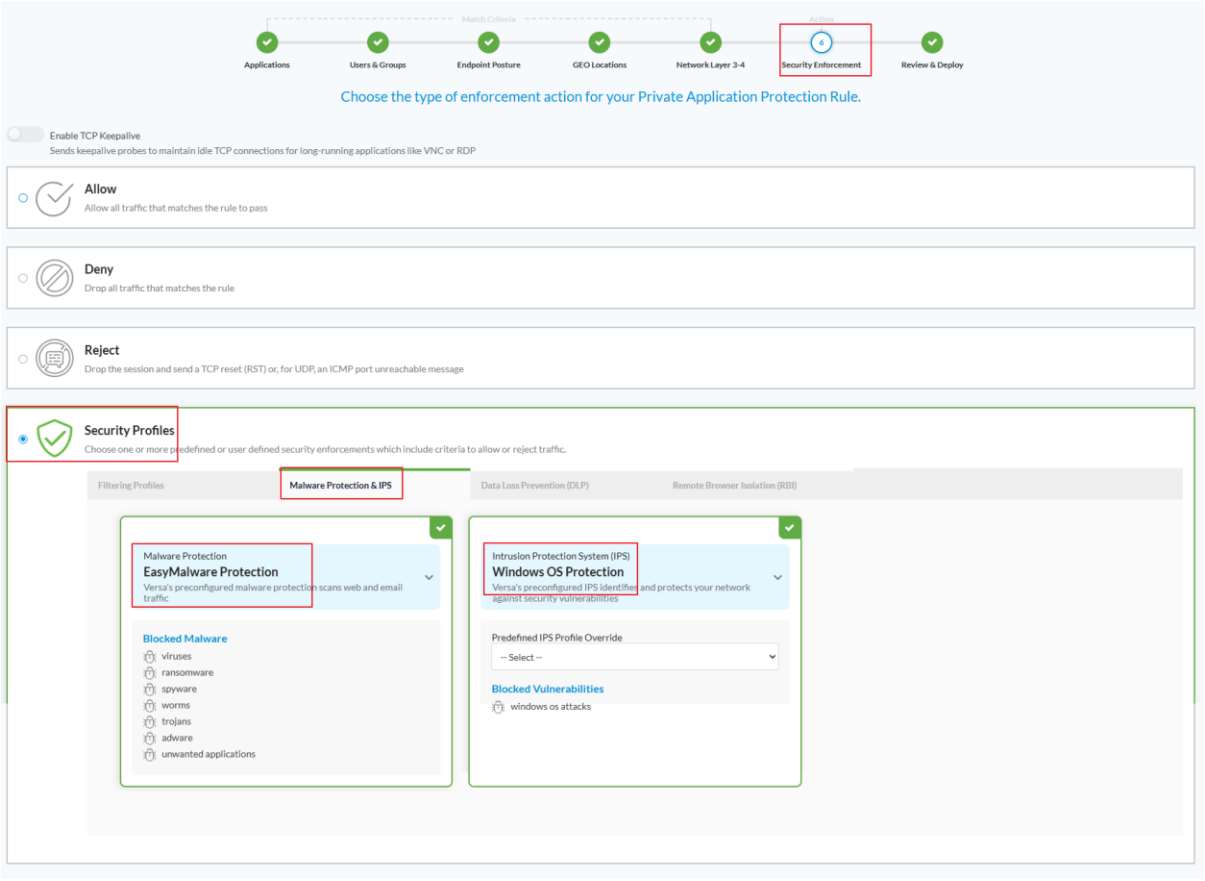
4. **Geo Locations:** Default values are used.



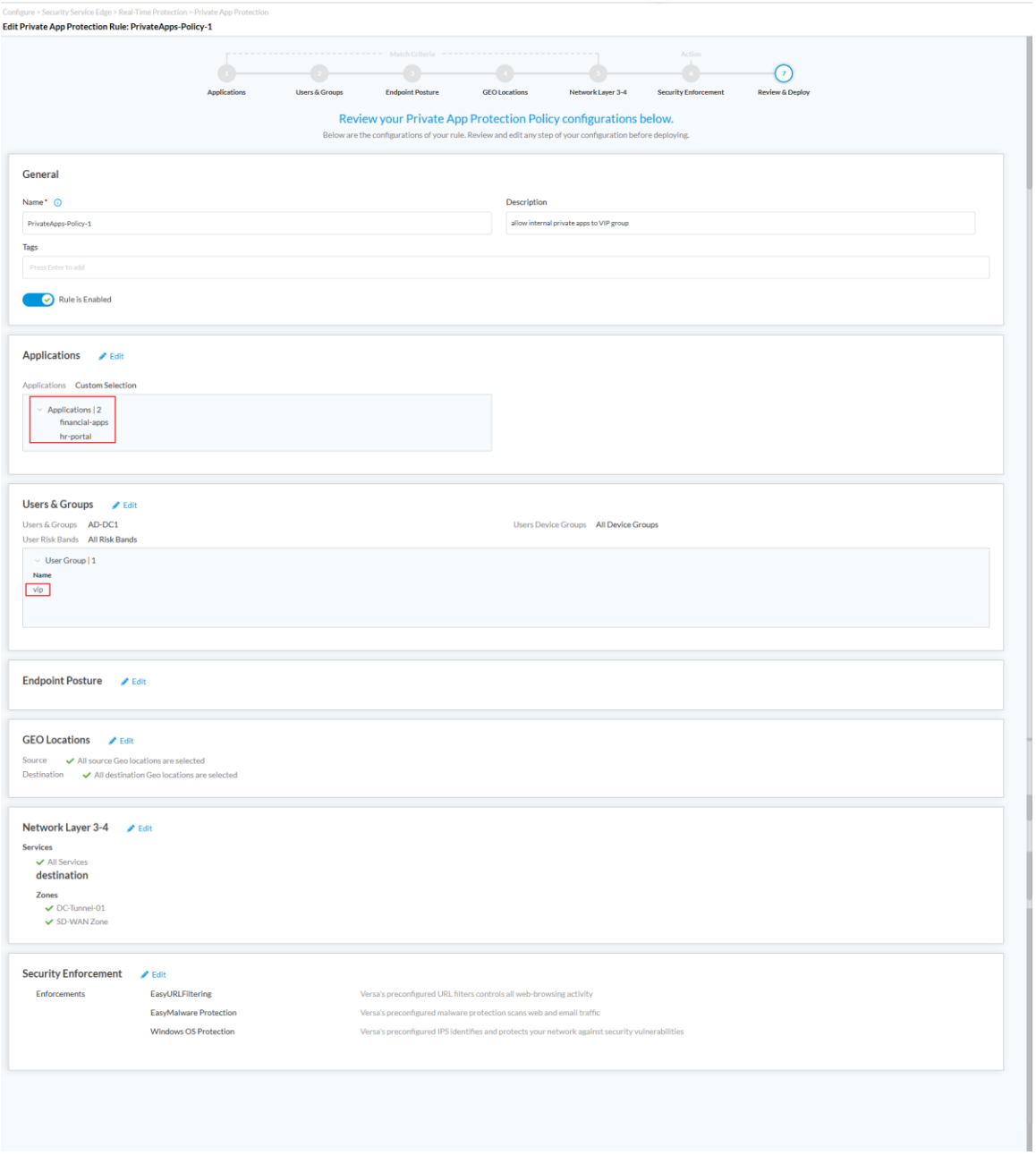
5. **Network Layer 3-4:** Default values are used.



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**.



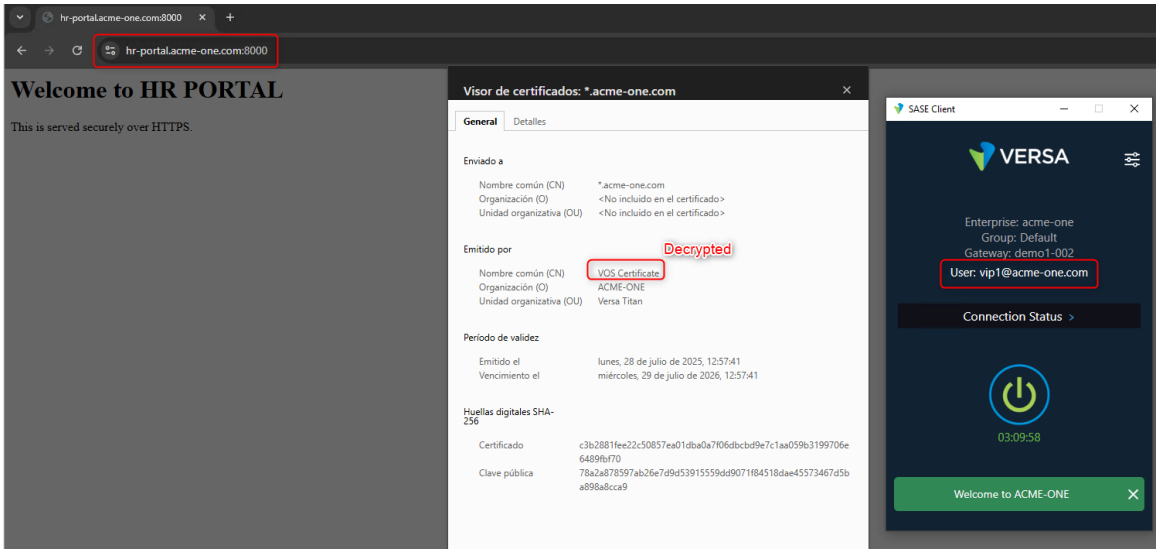
7. **Review & Deploy:** Once the configuration is complete, it should resemble the example shown in the image below.

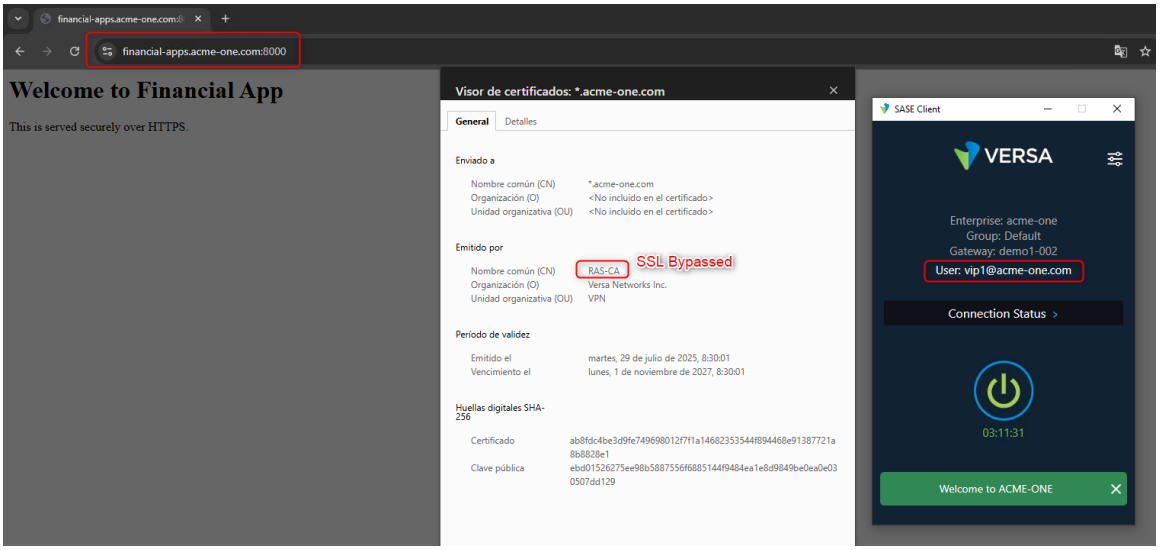


Step 8: Test and Verification

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

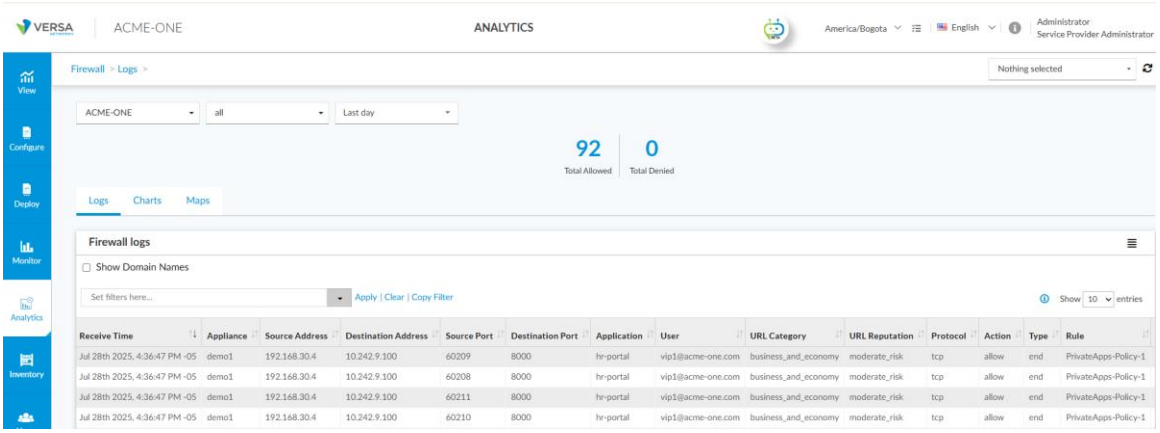
User connected to ACME-ONE PORTAL and can access the private apps.



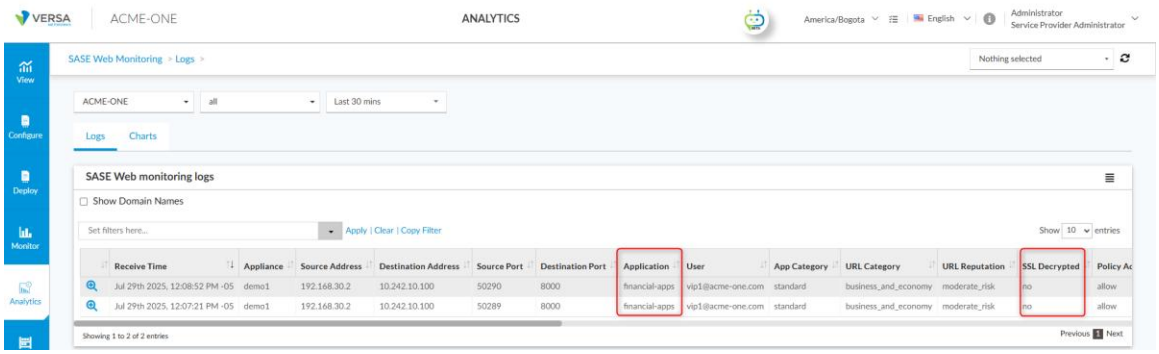


Logs from Analytics:

HR-PORTAL.ACME-ONE.COM



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



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.

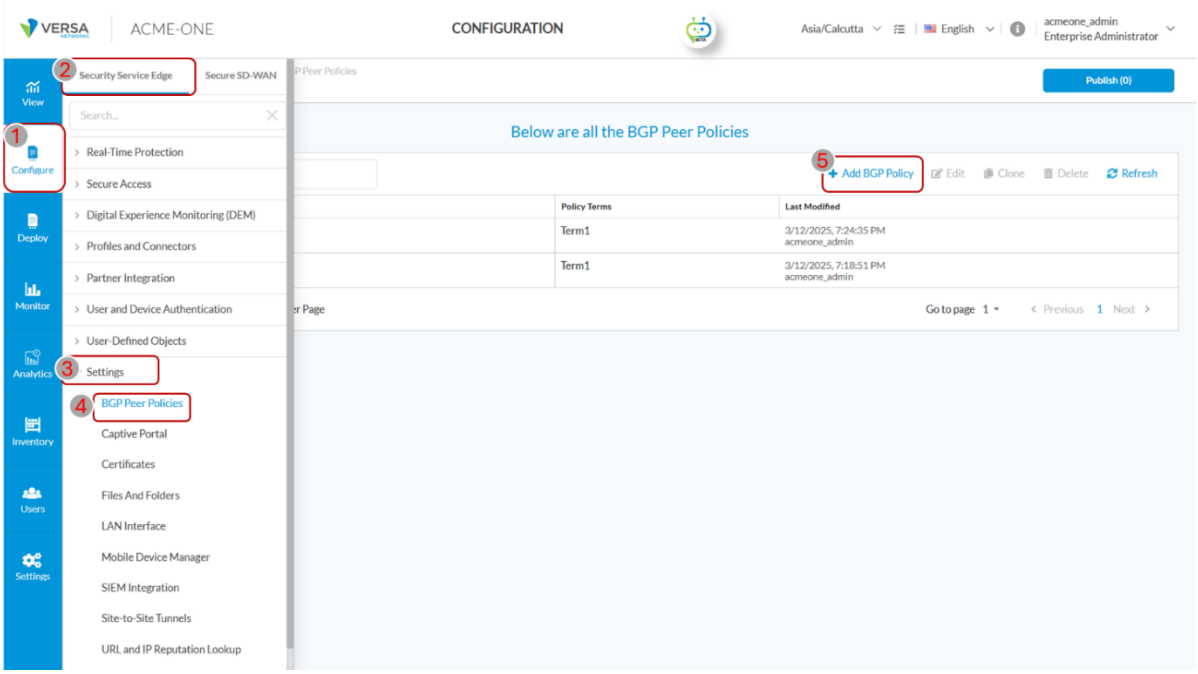
Configuring BGP Peer Policy

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

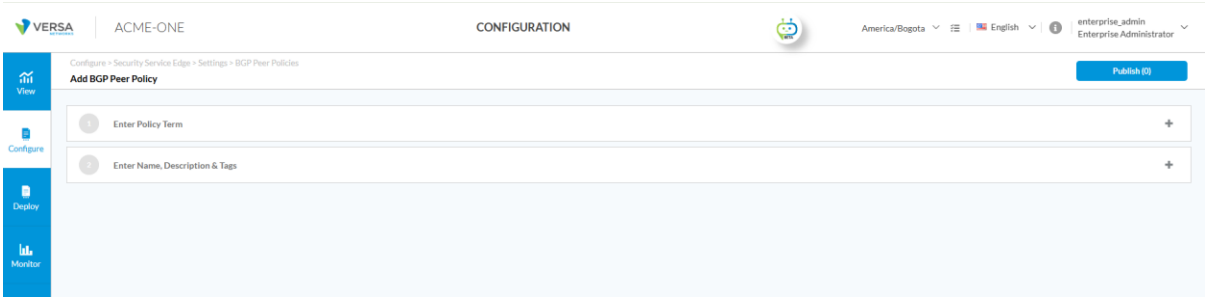
https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_BGP_Peer_Policies

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.



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.*



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))*

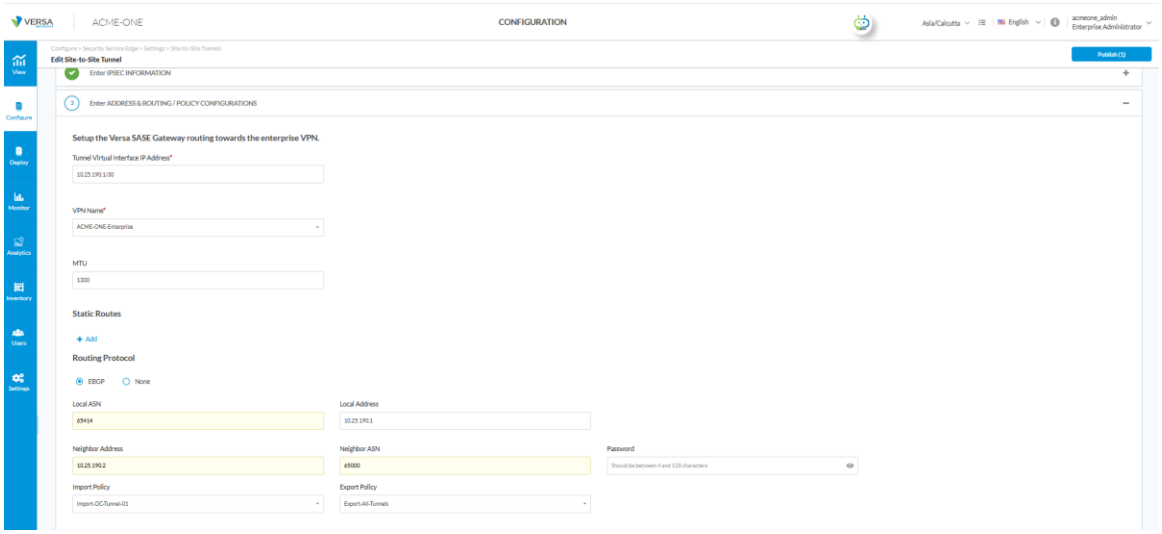
iv. *IPv6 Prefixes (Use + button to add as many as required)*

v. *Min Length (Default: None, Range (0-128))*

vi. *Max Length (Default: None, Range (0-128))*

vii. *Action (Permit/Deny)*

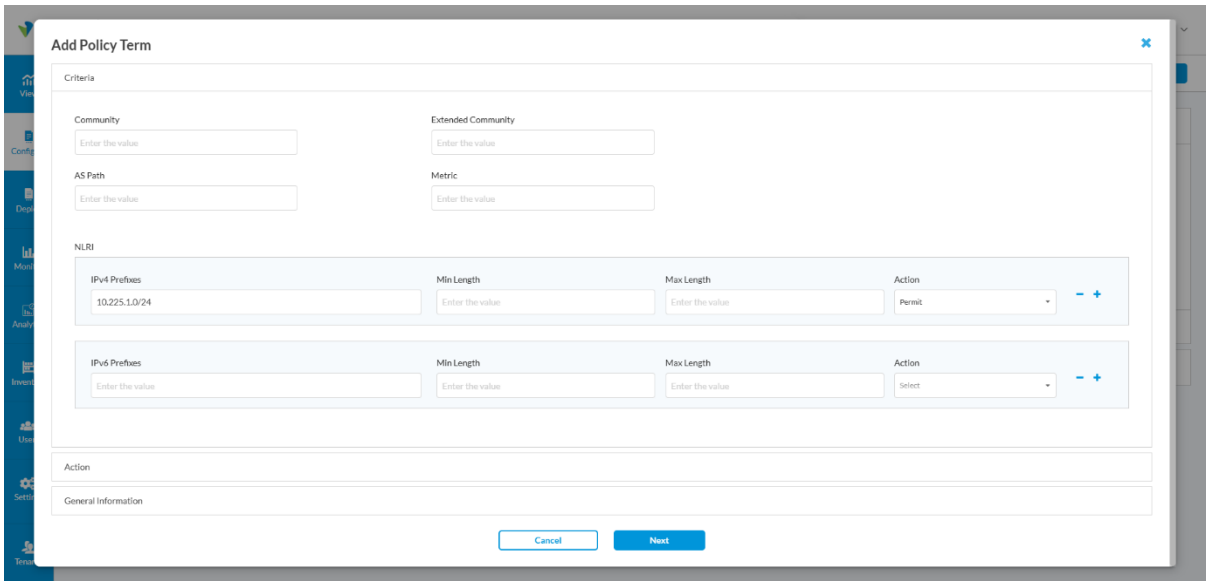
Note: IPv4 Prefix based match is shown in this document.



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

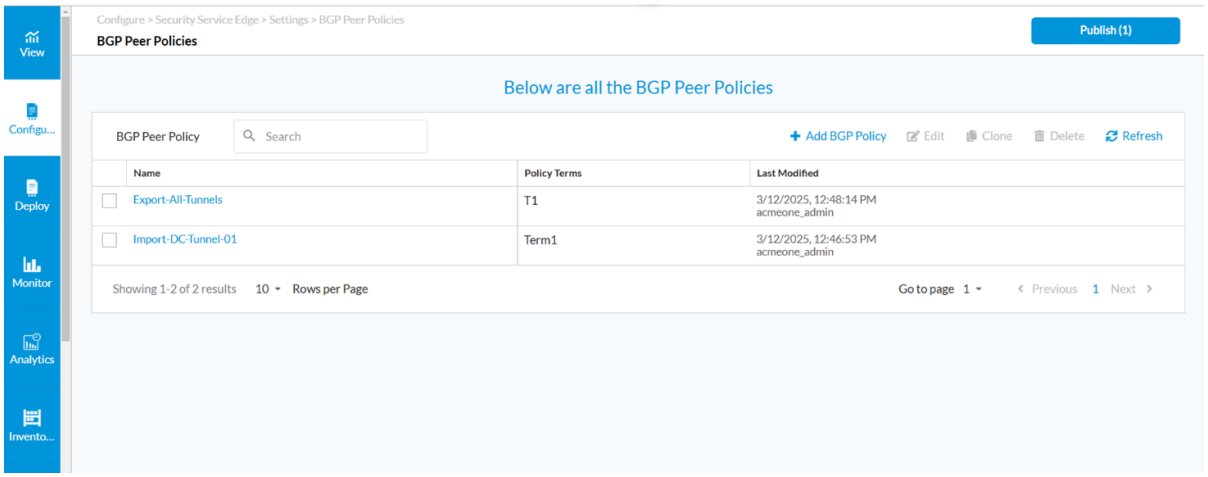
Step 2: Multiple Policy Terms

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.



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'.



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

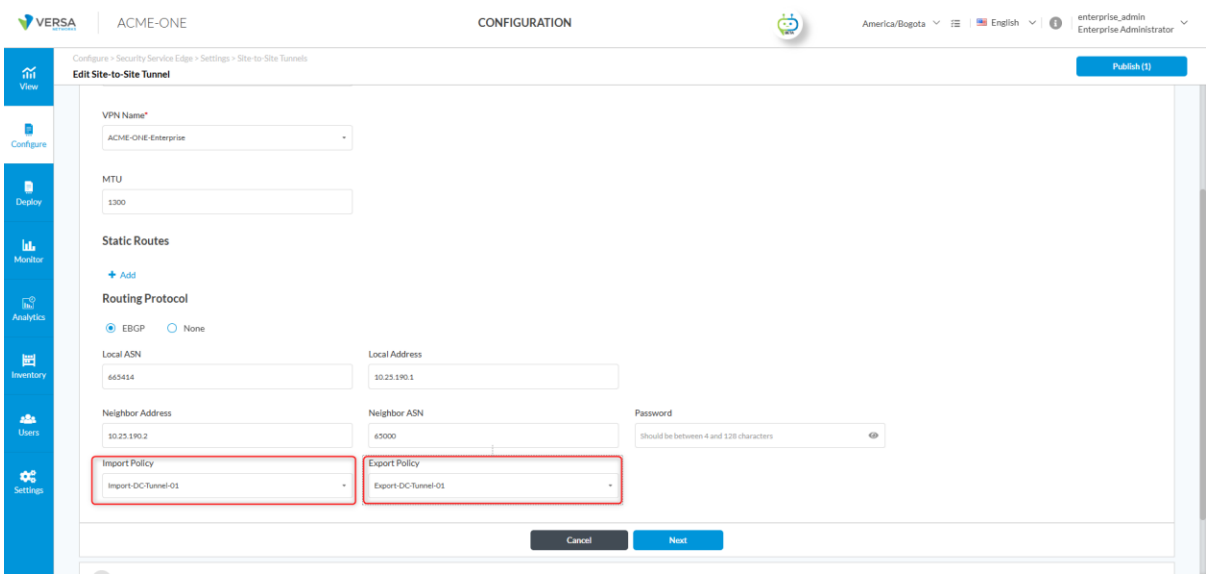
Add a Tunnel Virtual Interface address that is routable within your enterprise network. This typically involves using one IP from a /30 IPv4 address, with the other usable IP from the same /30 to be configured at your enterprise IPSec endpoint.

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

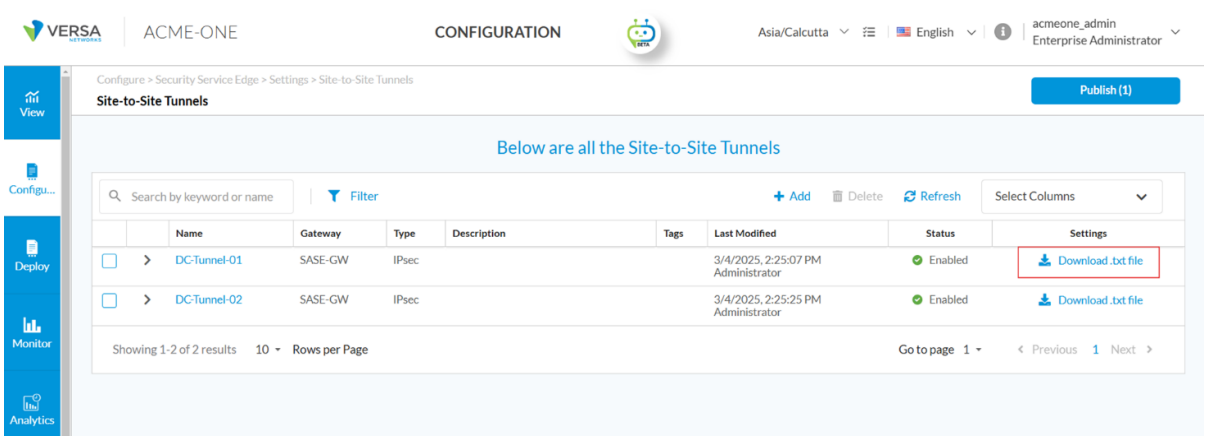
Set MTU: Versa recommends that the maximum transmission unit be set to 1300 for IPsec-based tunnels

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.



Name the tunnel and click on 'save'.



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.

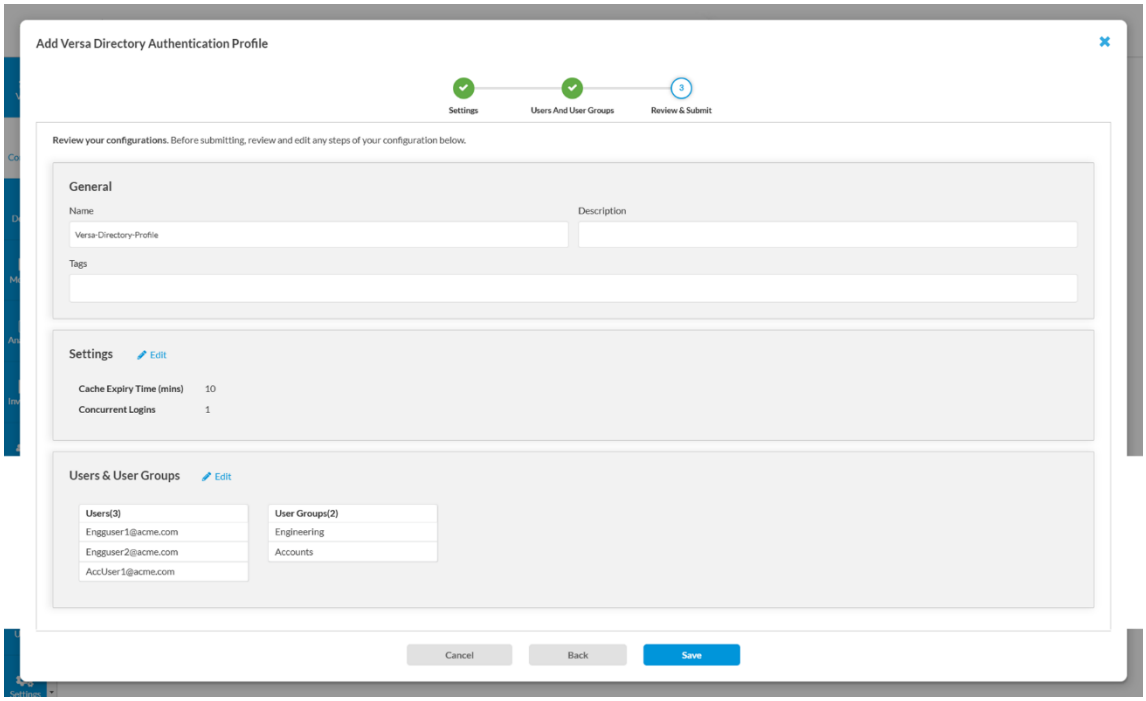
For Users:

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

For User Groups:

Group Name* and Description.

Note that * indicates a mandatory field.



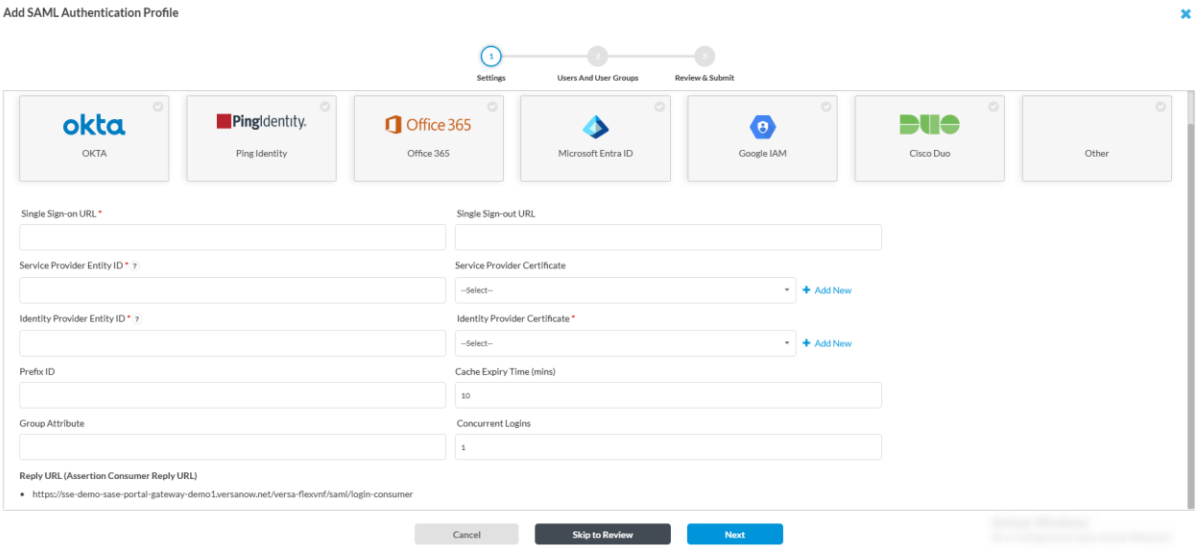
Before you do the above configuration, ensure that the IAM server details are configured by your Service Provider.

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).

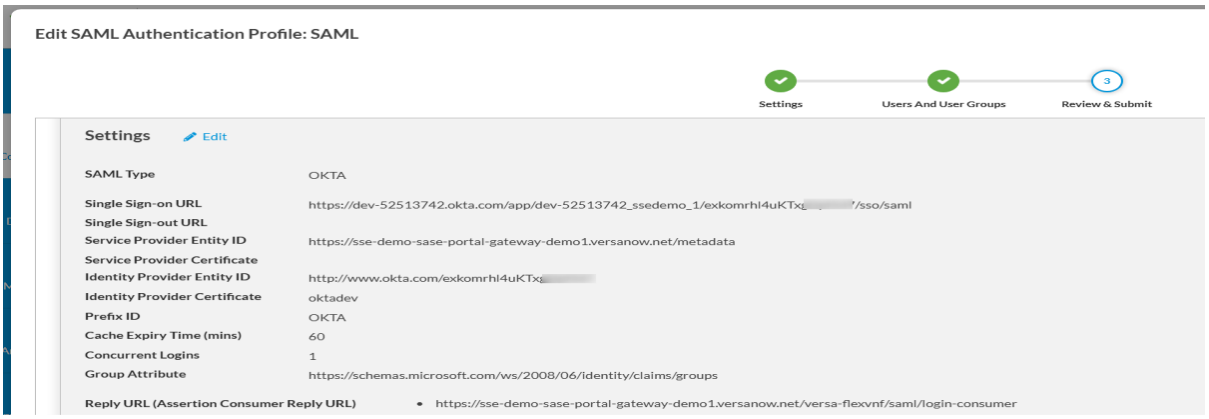
To begin with, Select the SAML type.



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

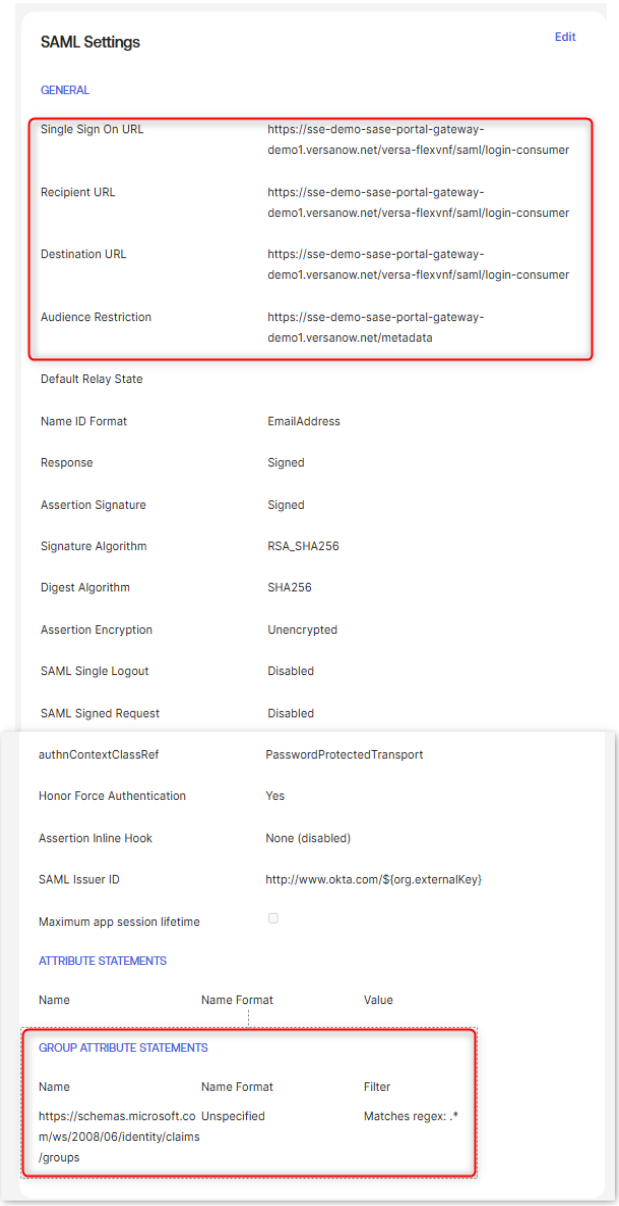
Example for Okta

Concerto Configuration:



Okta Configurations:

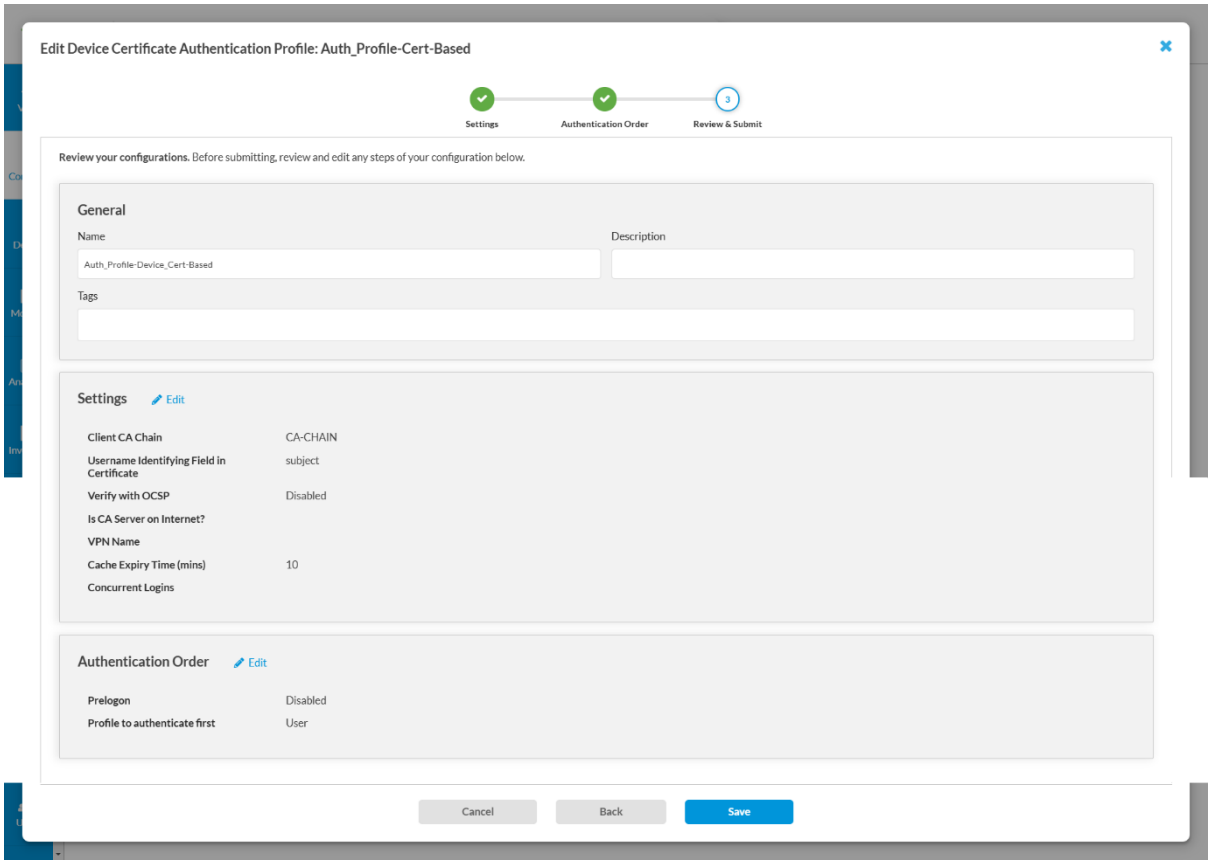
- Create a new app integration (SAML 2.0).
- Edit the general settings (see the image below for reference). Make sure the Group Attribute is the same in both places (Concerto SAML Configuration and Okta).
- Download the Okta certificate and upload it to Concerto in the Identity Provider Certificate field.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



Device Certificate

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

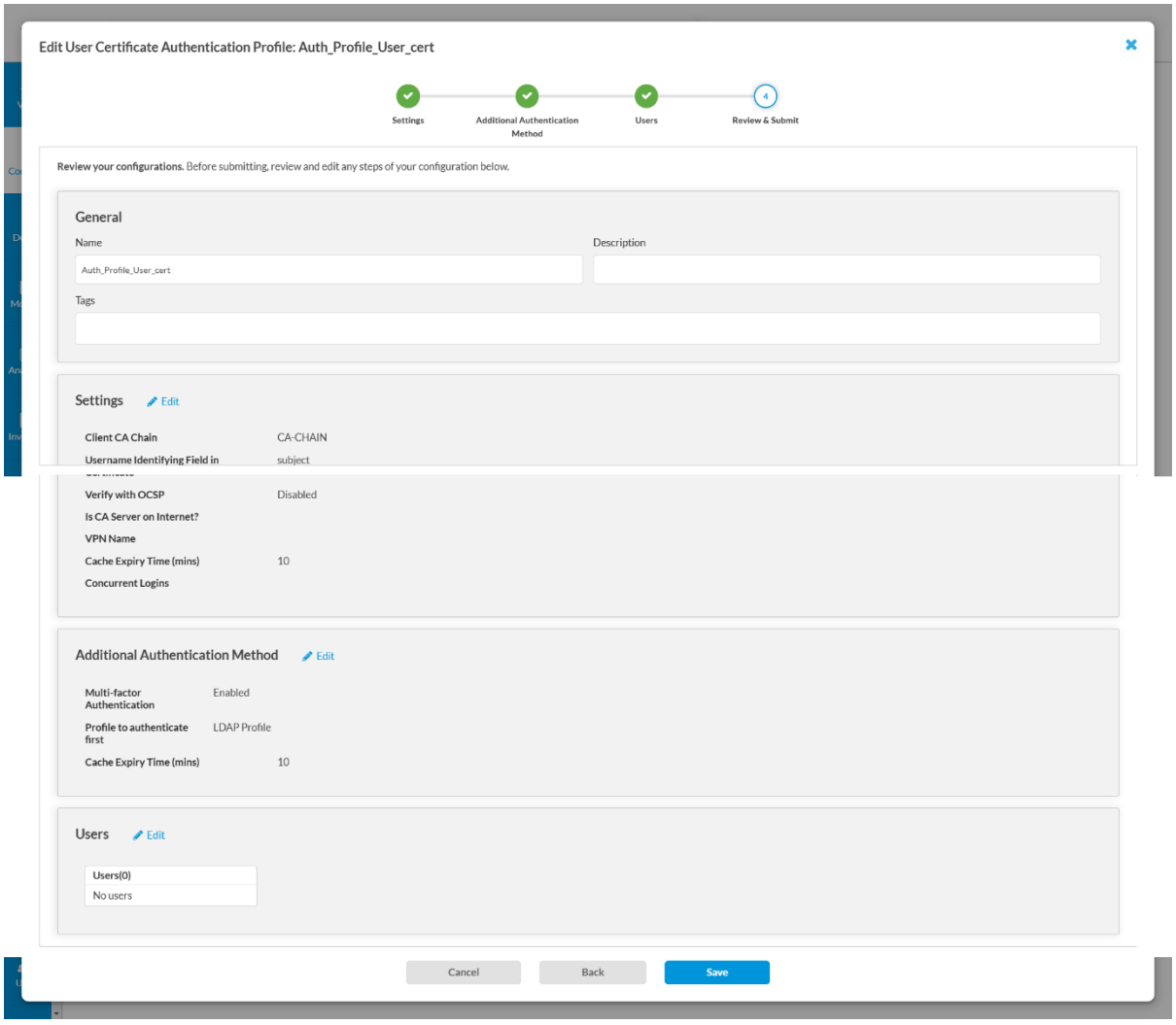
Start by uploading the CA Chain. Select the username identifying field in the certificate. Enable Verify with OSCP and select the source VR (optional). Select whether to use device certificate-based authentication in the pre-logon stage (toggle the enable button, if needed). In case of using user-certificate-authentication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

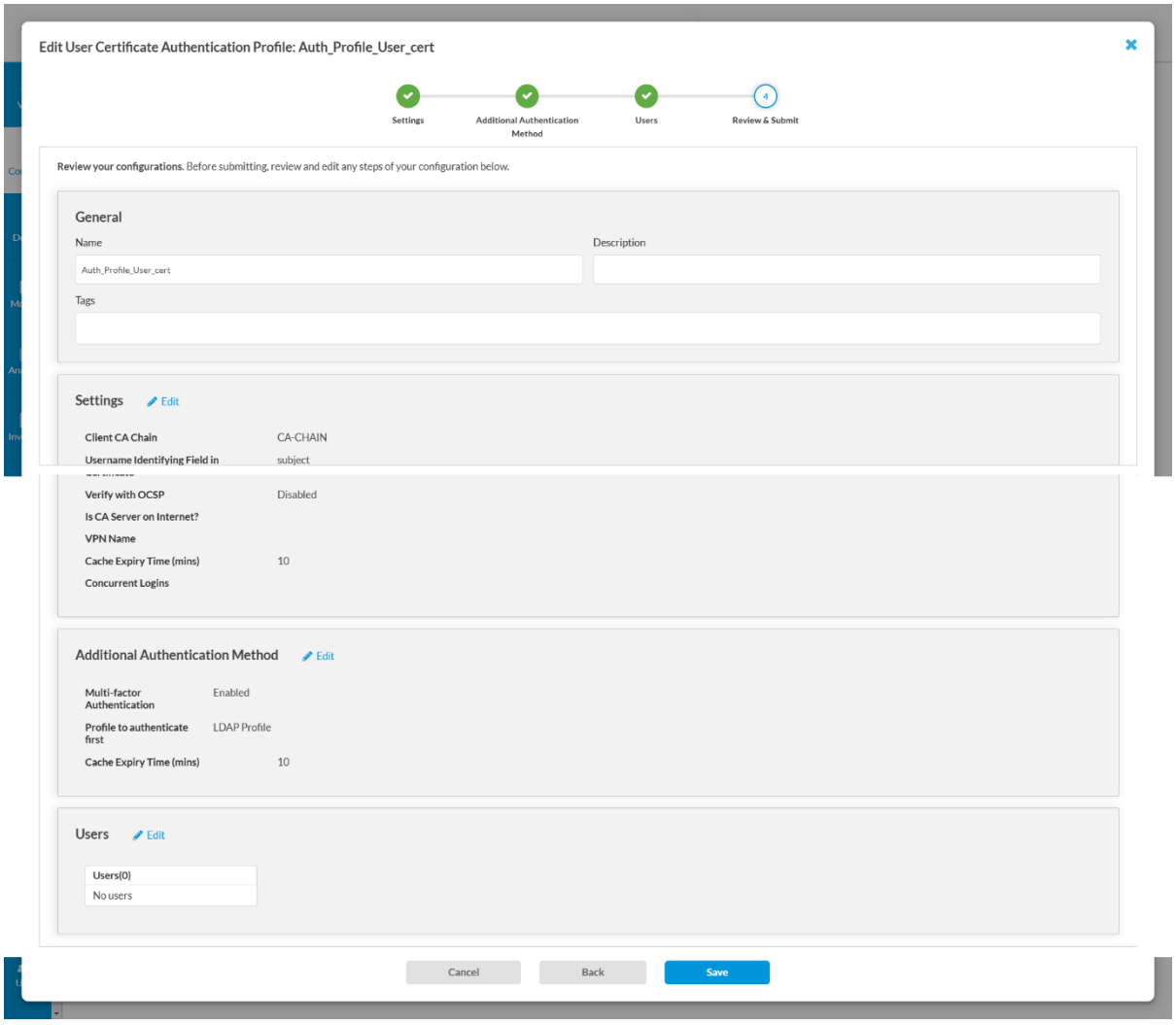


User Certificate

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
Settings
Additional Authentication Method
Users
4
Review & Submit
Review your configurations. Before submitting, review and edit any steps of your configuration below.
General
Name
Auth_Profile_User_cert
Description
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
Settings
Additional Authentication Method
Users
4
Review & Submit
Review your configurations. Before submitting, review and edit any steps of your configuration below.
General
Name
Auth_Profile_User_cert
Description
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

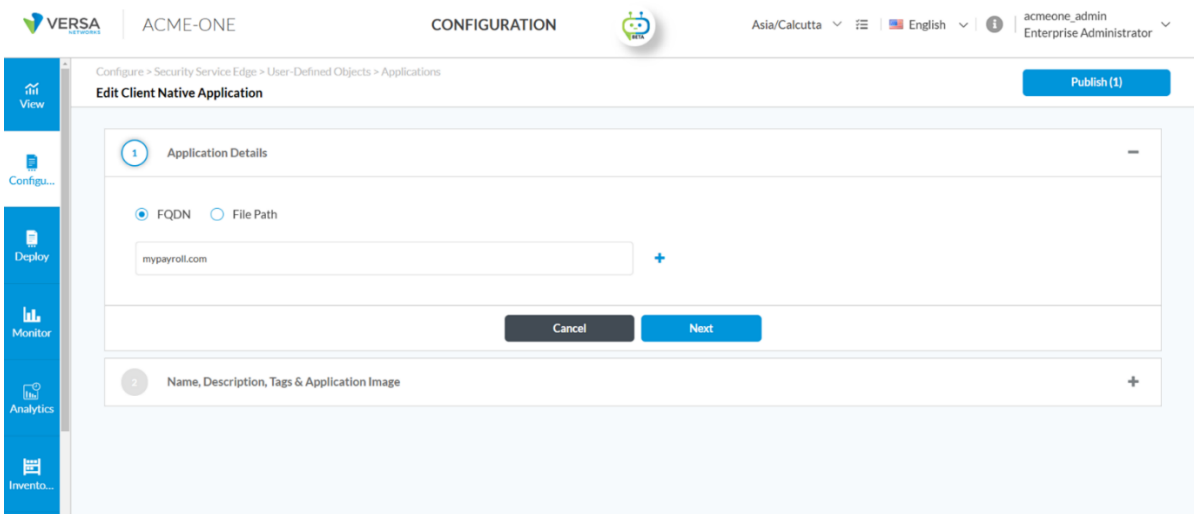
To create a Custom Application, Navigate to

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.

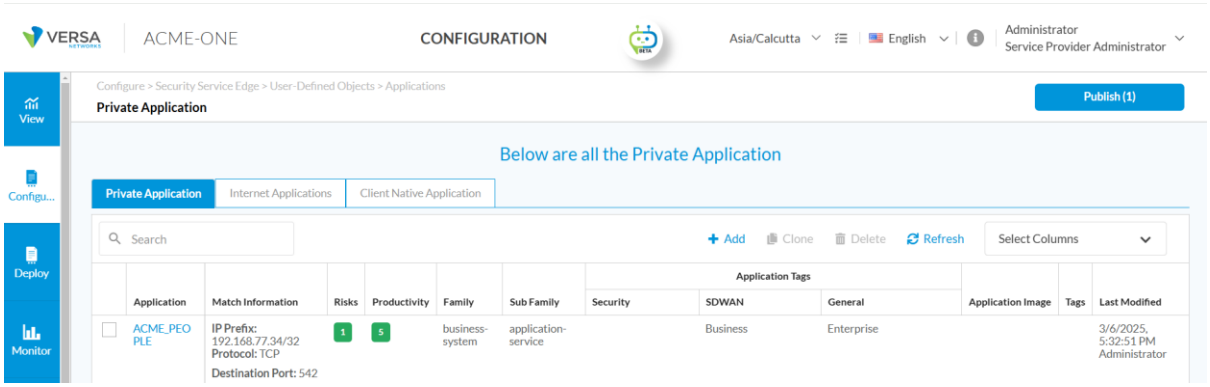
Client Native Application

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).

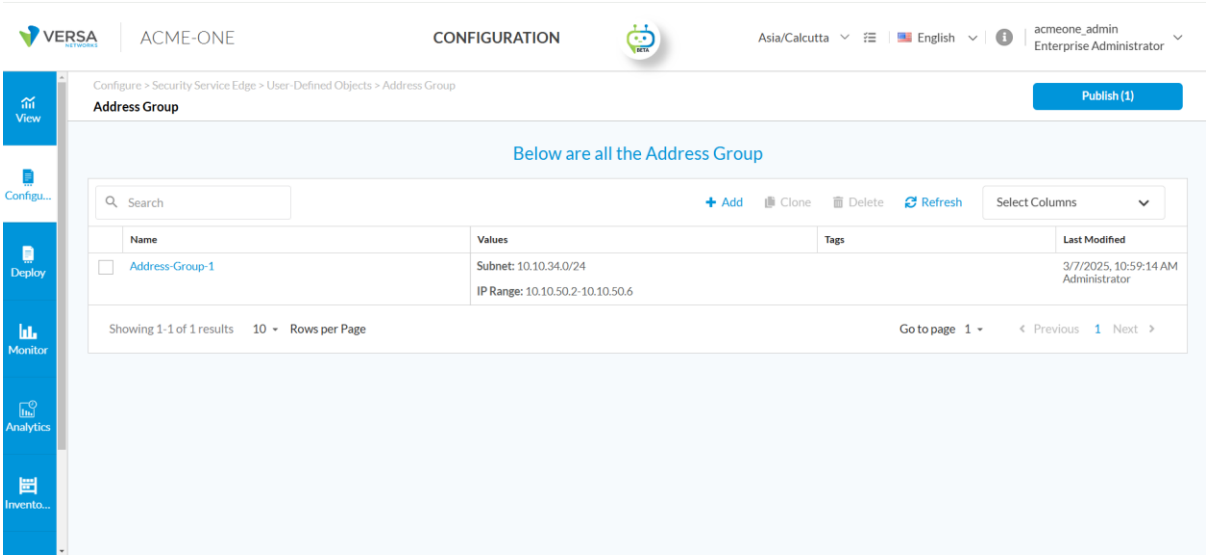
Address Groups

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'.



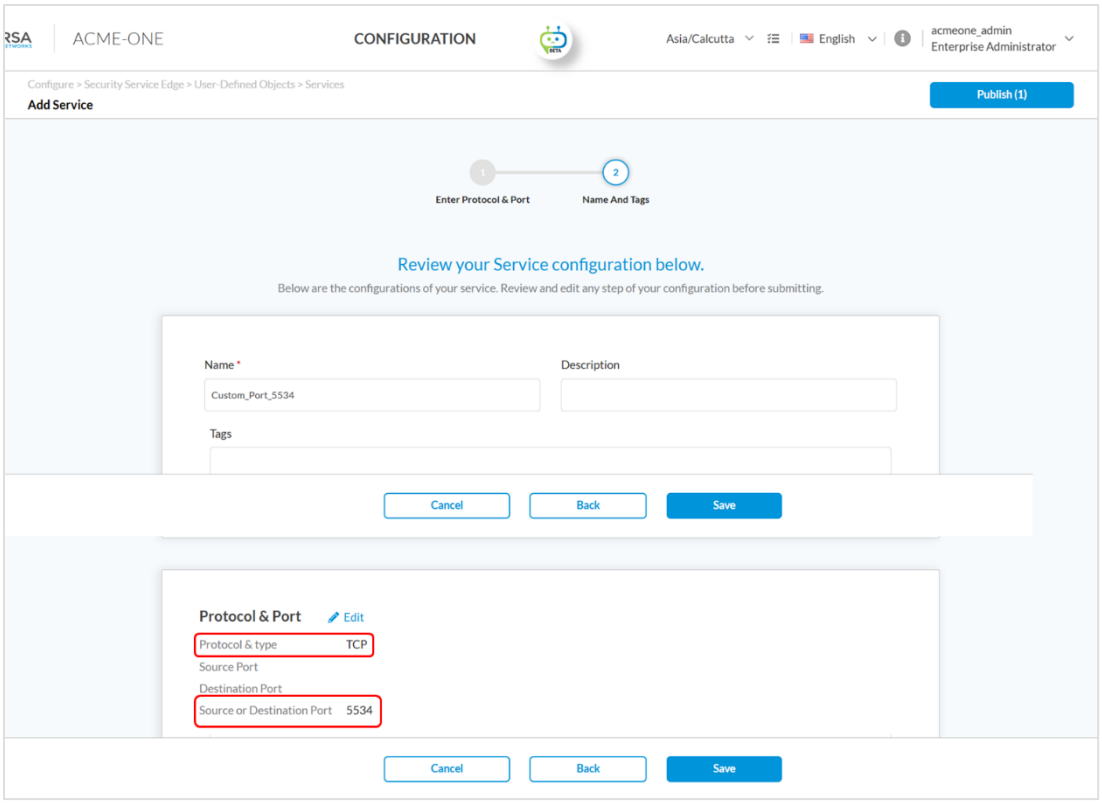
Services

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'.

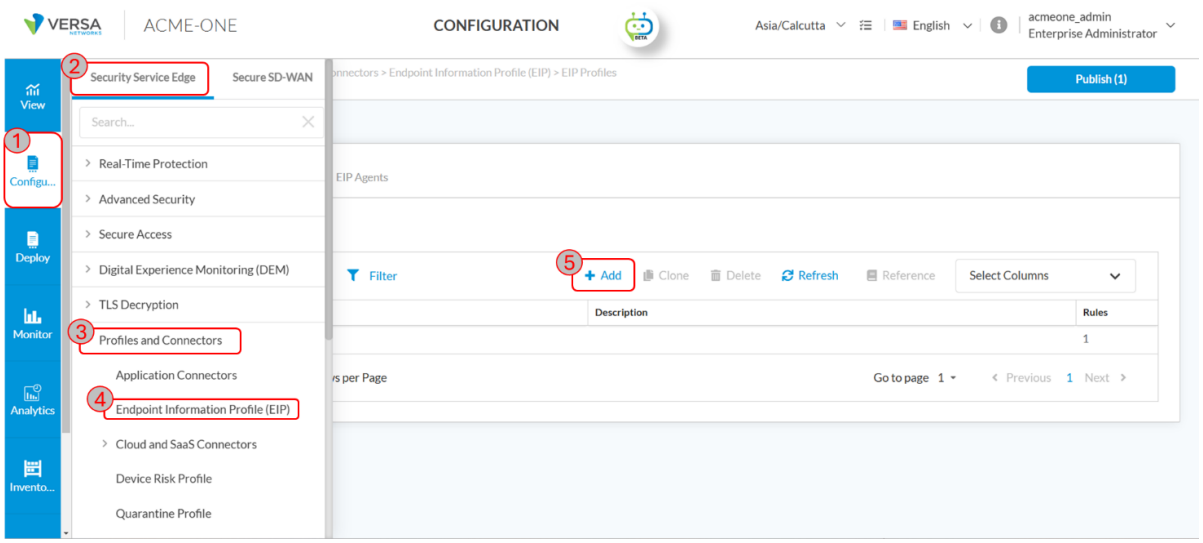


End-point Information Profiles

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.***

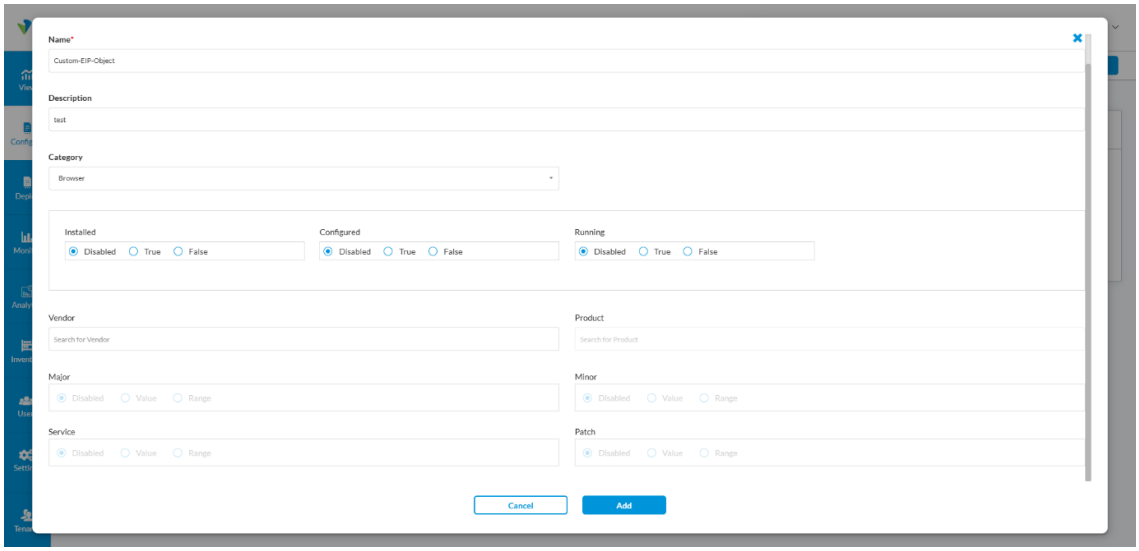


There are three buildings blocks of EIP. They are

- EIP Objects

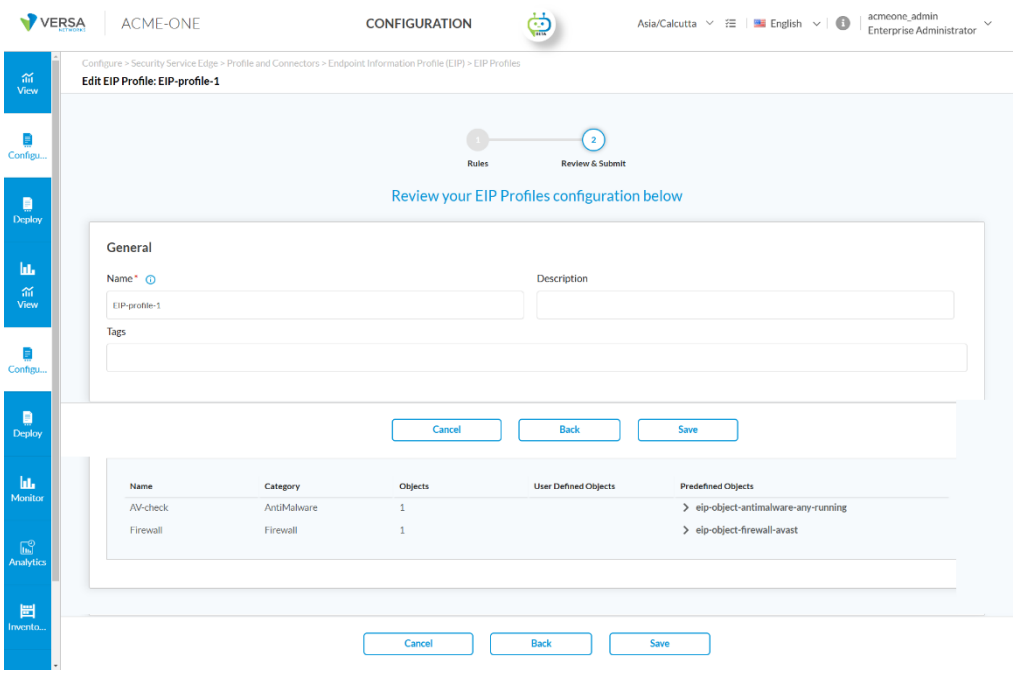
EIP objects define the various match criteria to check the security status of a particular category. Select all the required match conditions. Go through the fields below to understand how to construct an EIP object.

- 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'.

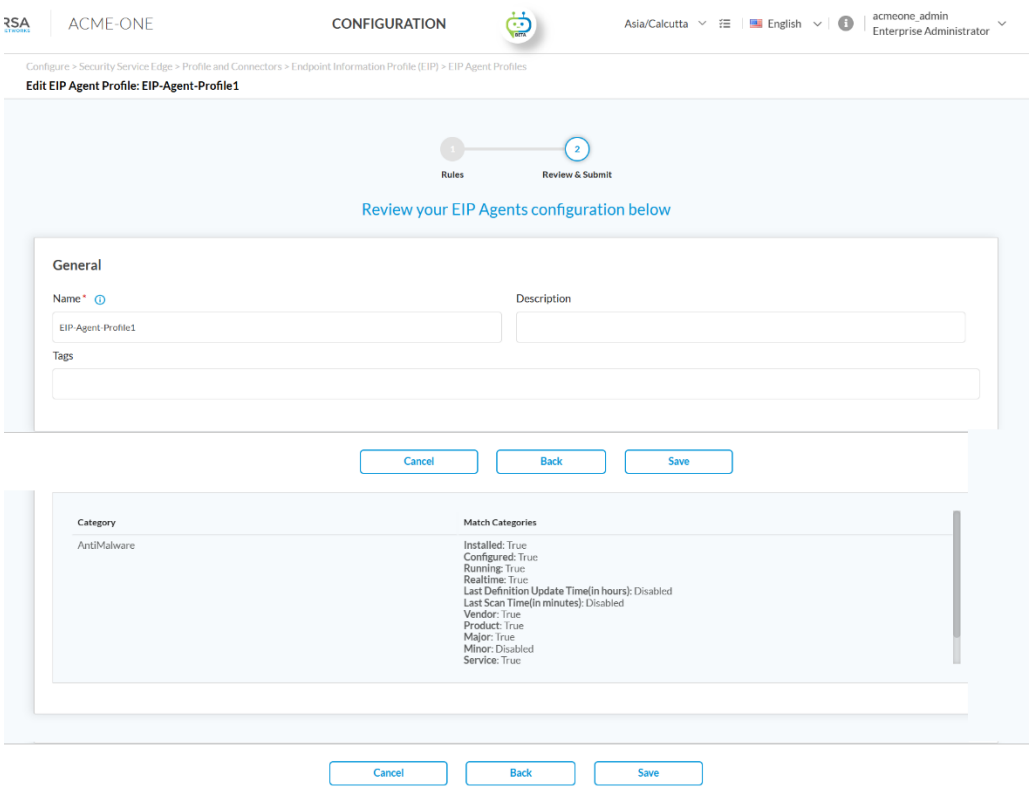


- EIP Agents

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.

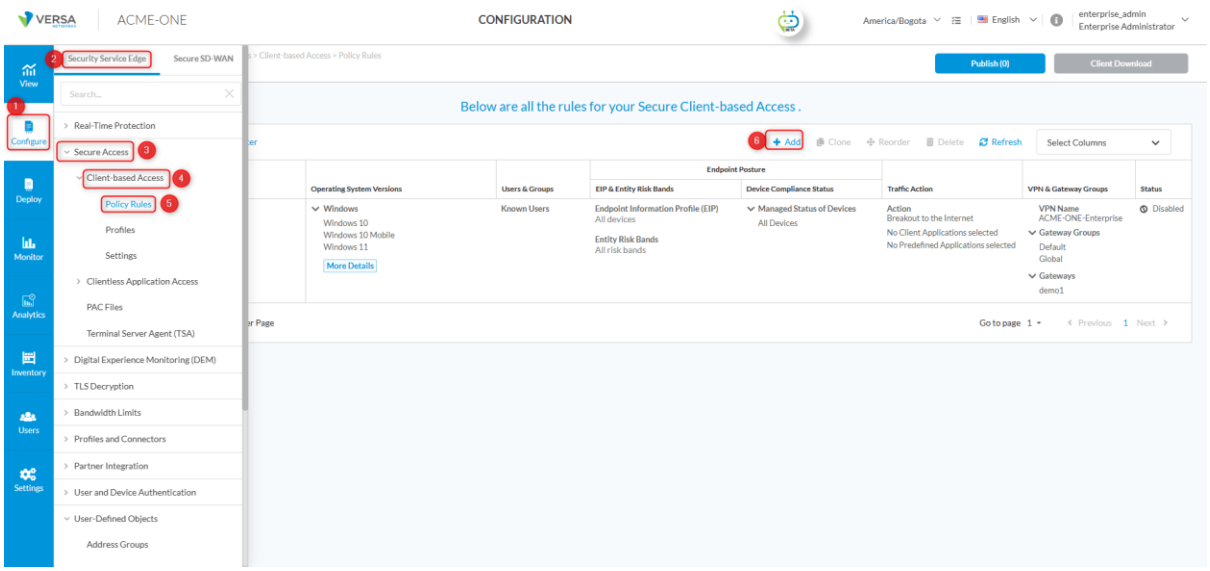


Appendix D – Secure Access Policies – Key Components

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.***



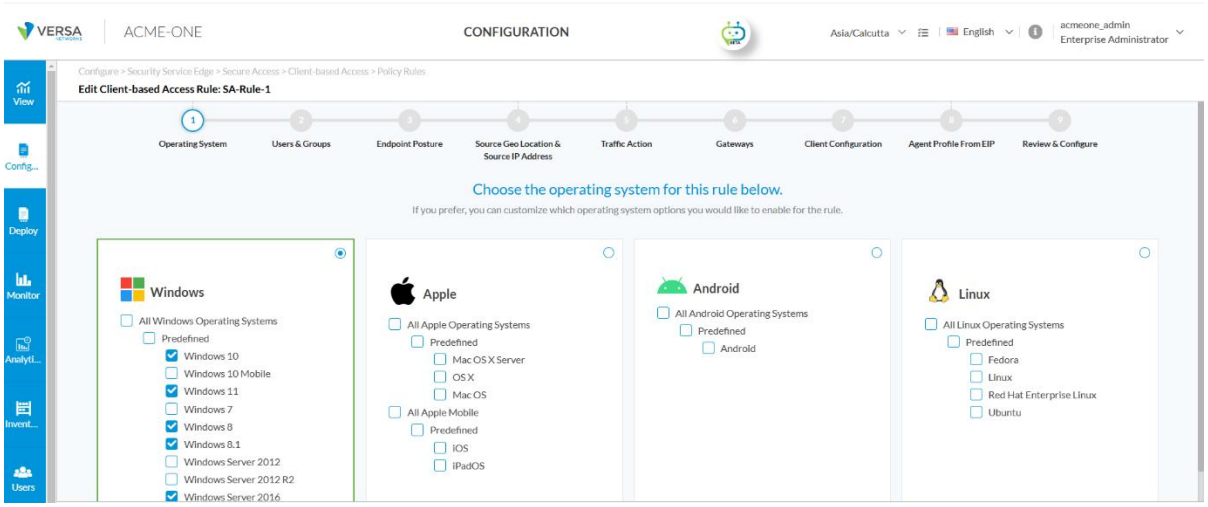
The following are the match conditions for secure access rules:

- 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

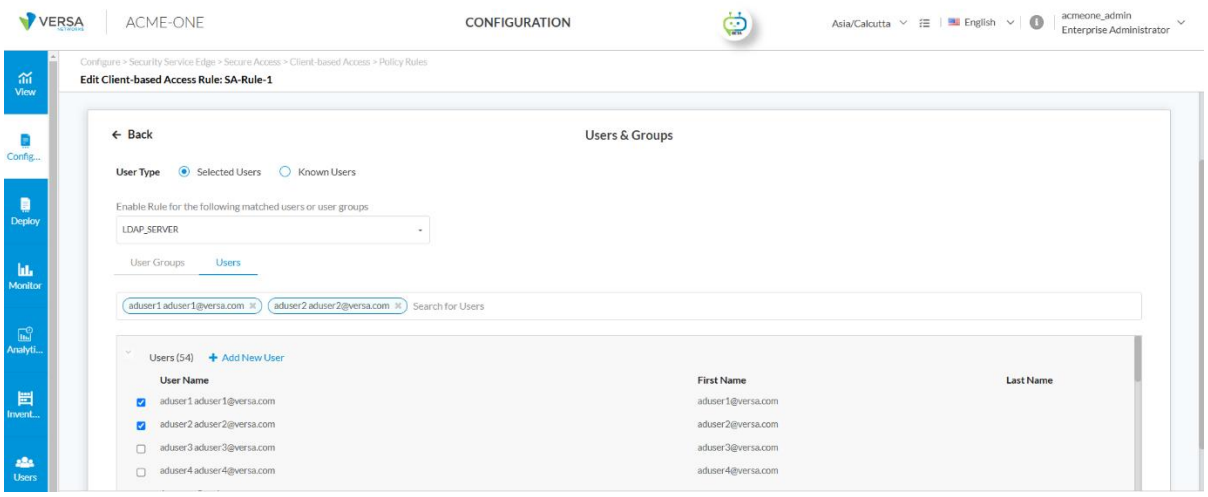
Operating systems are used to define end user machine operating systems. We can match only one operating system (Ex. Windows) with one rule. However, in the same rule we can match multiple flavors (or versions) of that operating system (Ex. Windows Professional, Windows Vista etc..). We also have an 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.

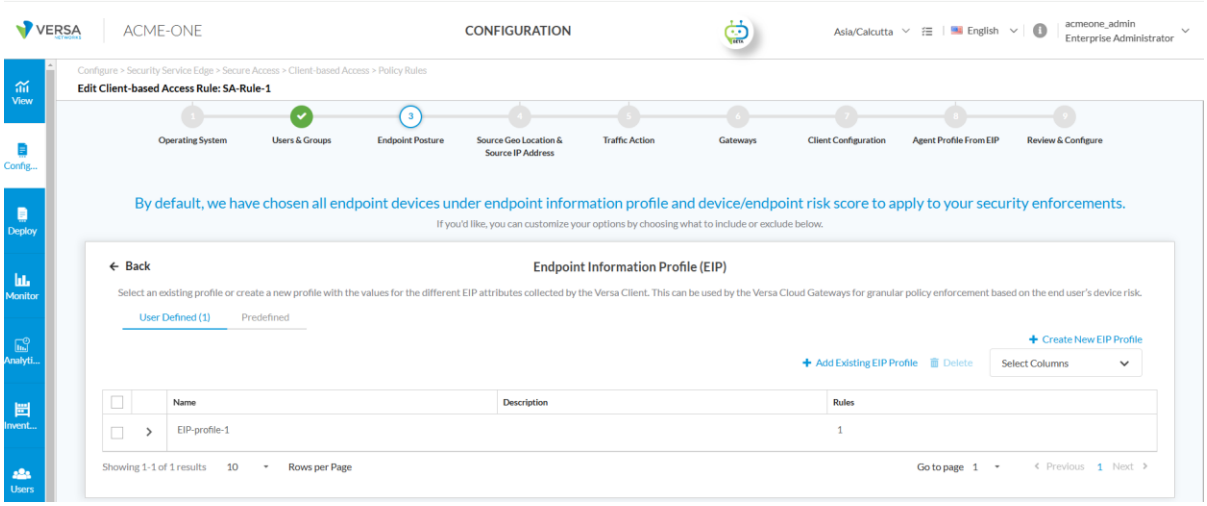
Users/User Groups

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'.



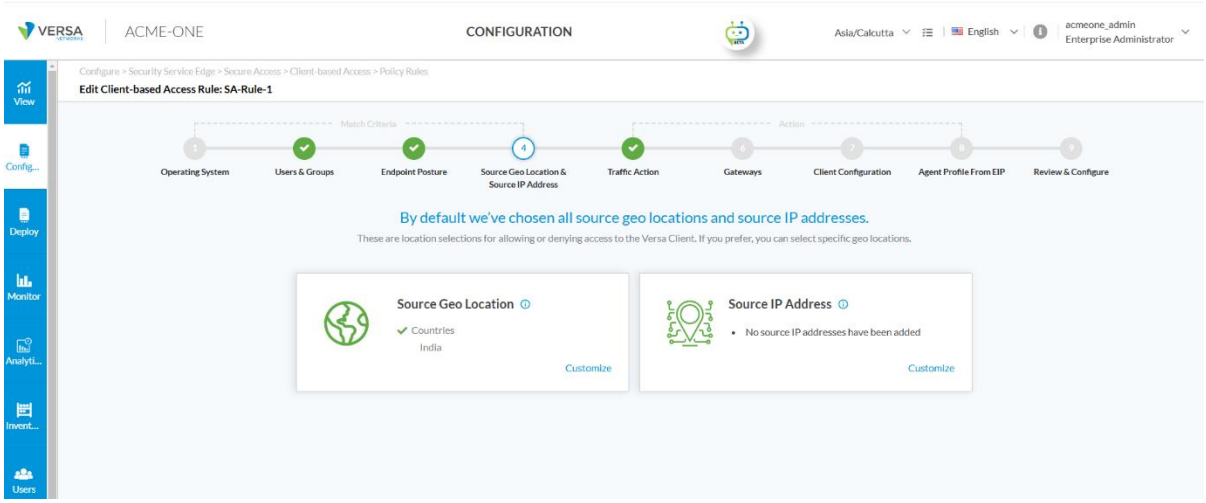
Endpoint Information Profile (EIP)

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.



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.

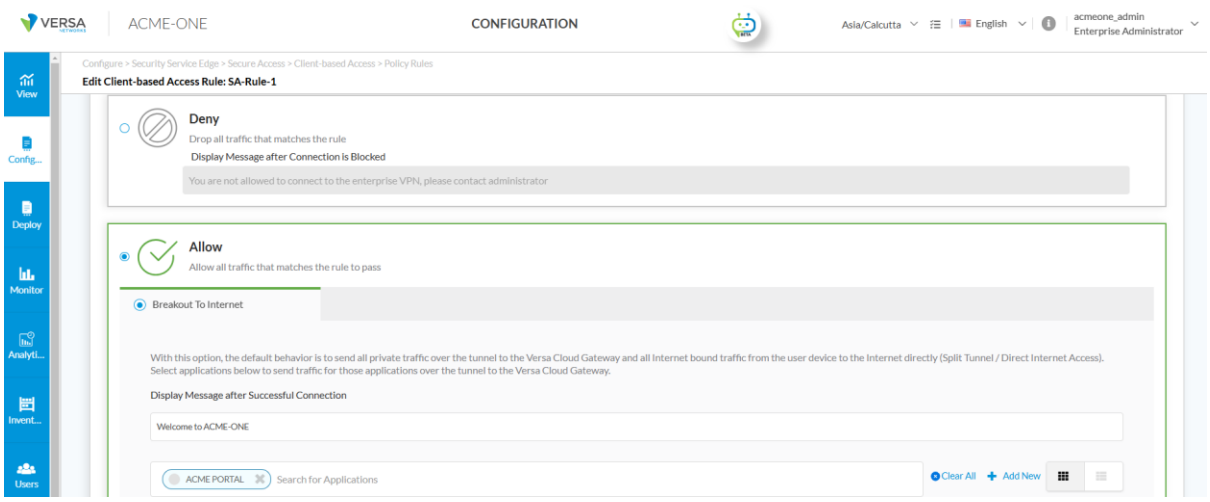
- Traffic Action
- Gateways

- Client Configuration
- Agent Profile from EIP

Traffic Action

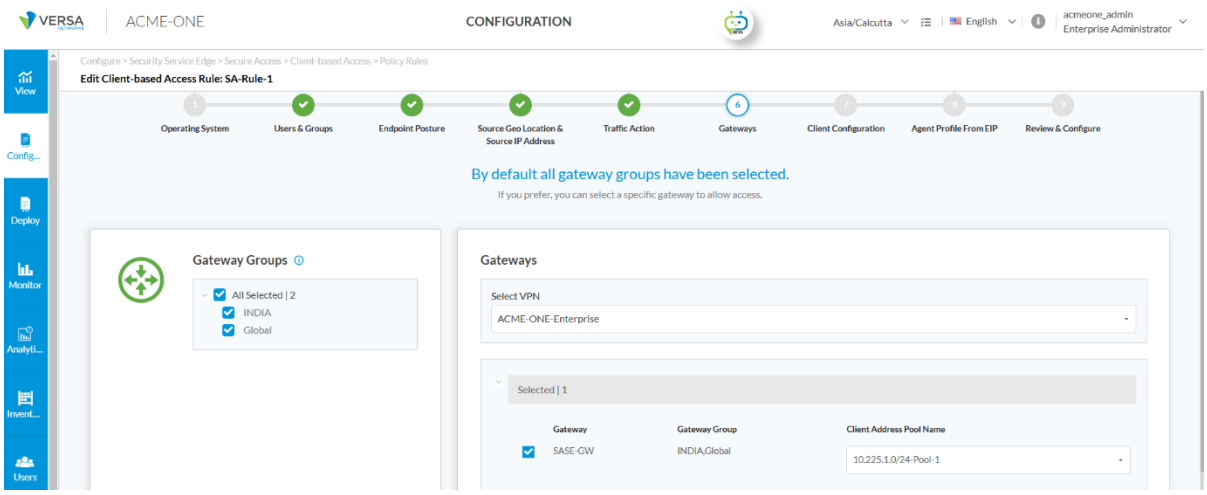
For VSPA only, there are two possible traffic actions. One is to deny the traffic, and the other one is to allow the traffic (where all private Application traffic is directed to the versa gateway, and the Internet bound traffic breaks out locally).

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

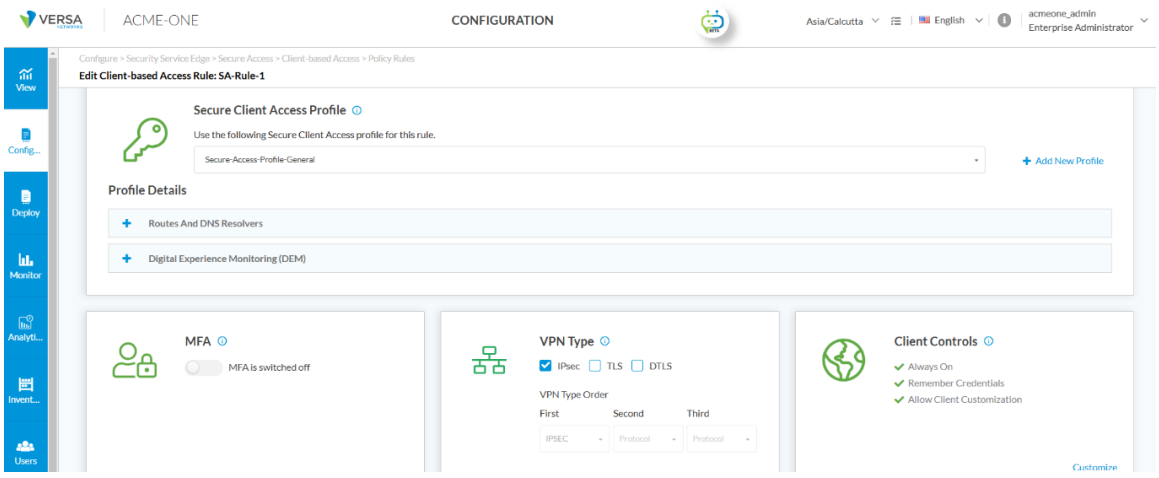
This section lists the gateways (and the gateway groups) to which the end-user will connect to. If an enterprise has subscribed to multiple gateways, then this section helps define which set of users will connect to which gateways. We also configure the IP pool of the end-user machines, while connected 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.



Client Configuration

The following configurations are covered under this section:

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



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.

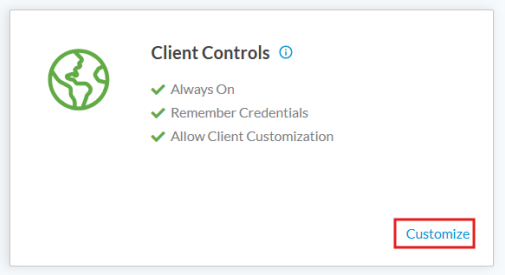
VPN Type

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.

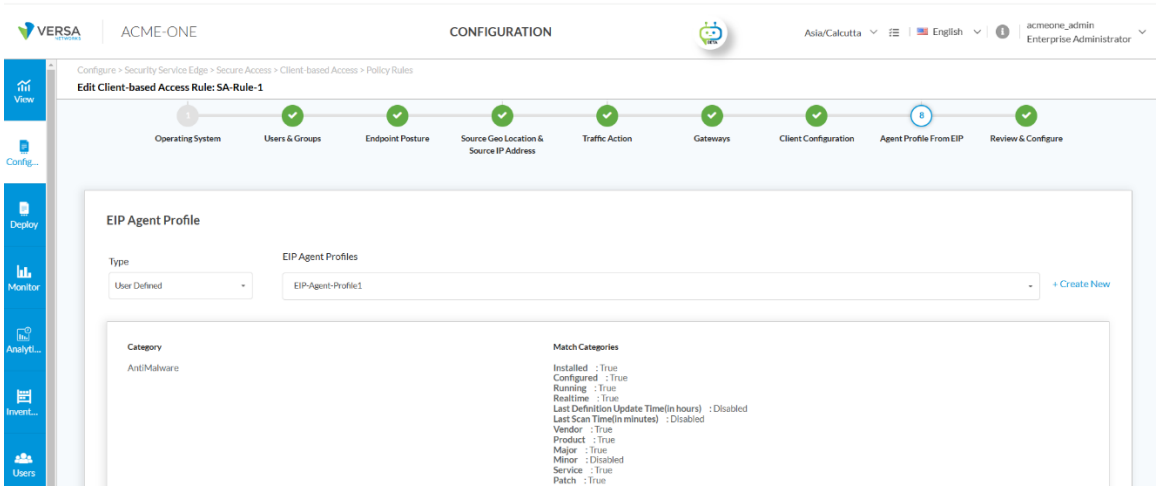
While this is enabled, there is an option to specify trusted routes. Only the trusted networks are bypassed from the gateway, and all the other traffic is still sent to the gateway. This is called the semi-trusted mode.

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.

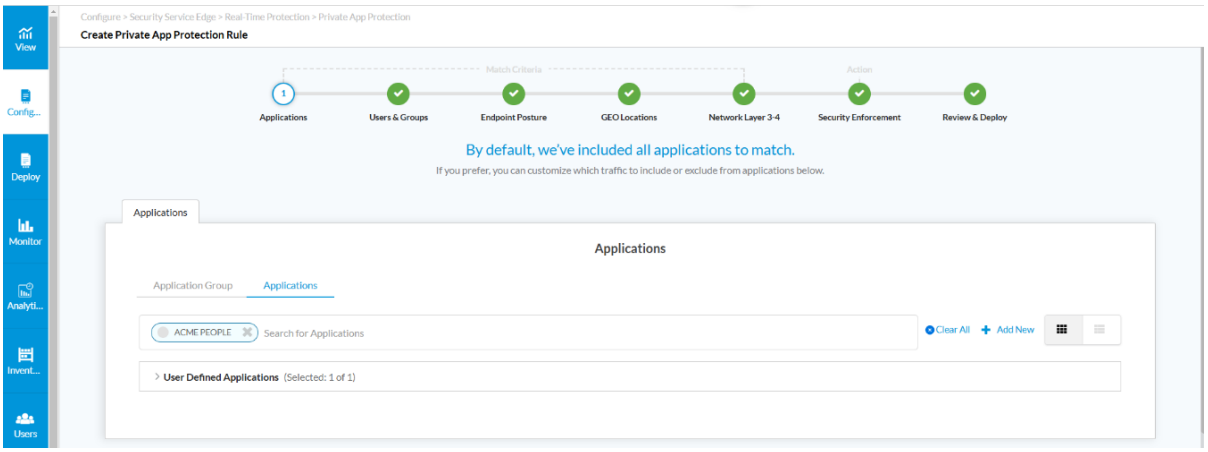
To configure Private App Protection, navigate to

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

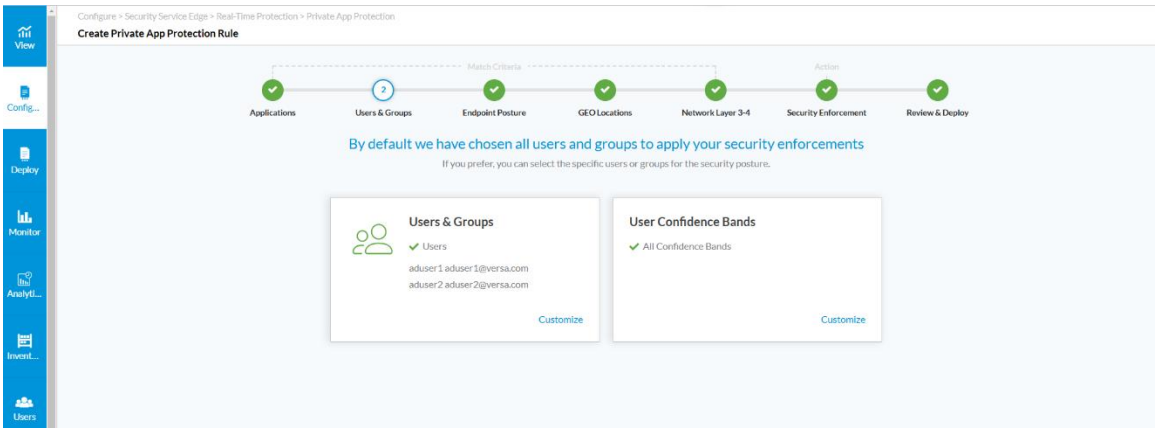
(Click on Let's Go, if this is your first Private App Rule). Each private protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR 'ed and on different tabs is 'AND'.

The match criteria are as follows:

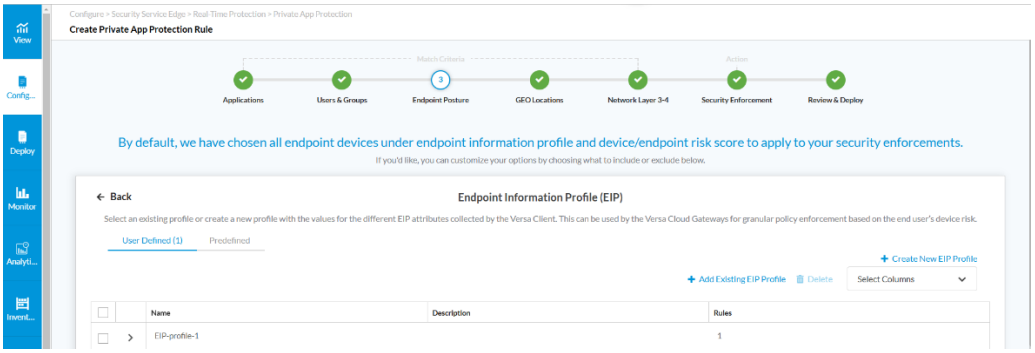
- Applications—Individual applications, groups of applications, categories of applications, predefined URL categories (created in previous steps). Select one or more Applications/Groups.



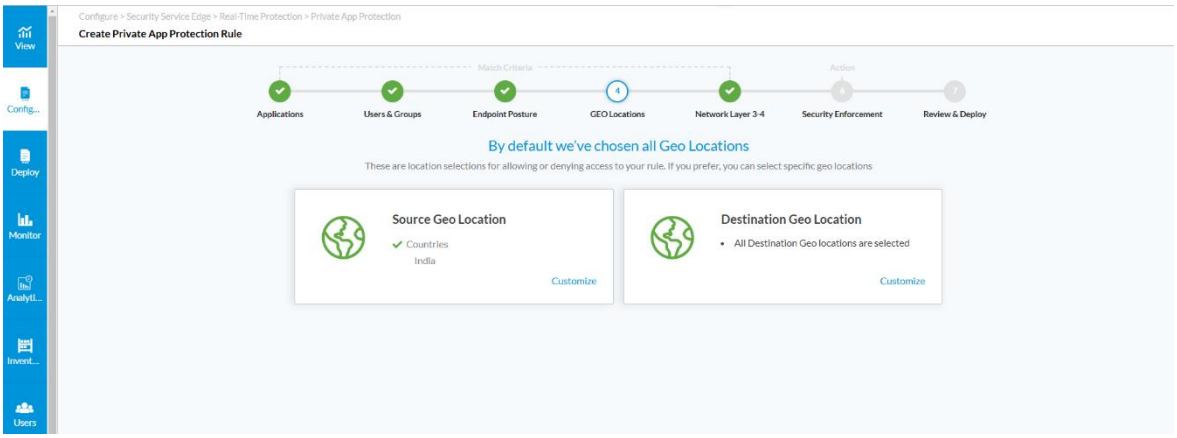
- User groups—Individual users or groups of users. Select users/user groups.



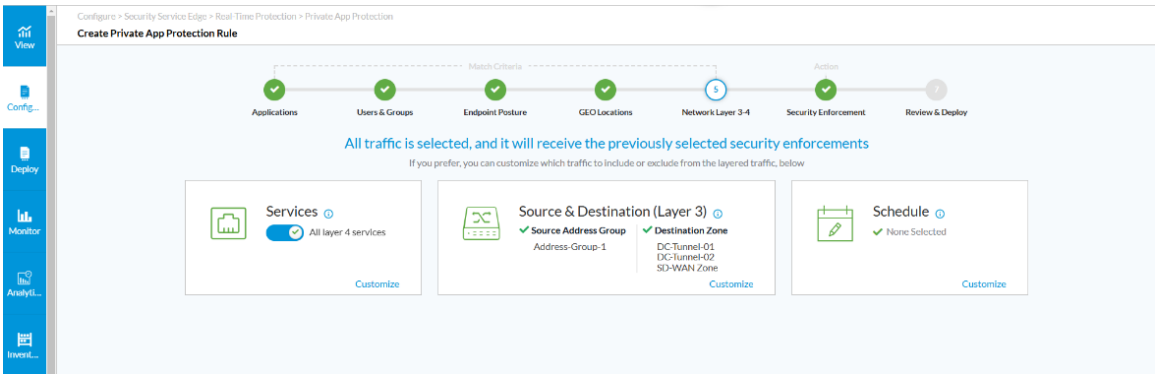
- Endpoint Posture- Predefined and user-defined Endpoint Information Profiles (EIP). Select the EIP Profiles needed to restrict access based on end-device posture.



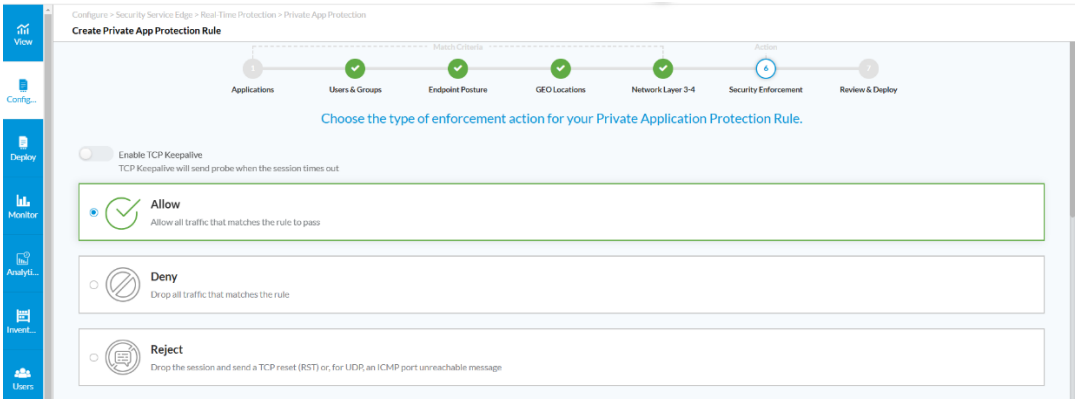
- Geolocation—Geographic location of the source or the destination. You can choose country, state and city.



- 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.



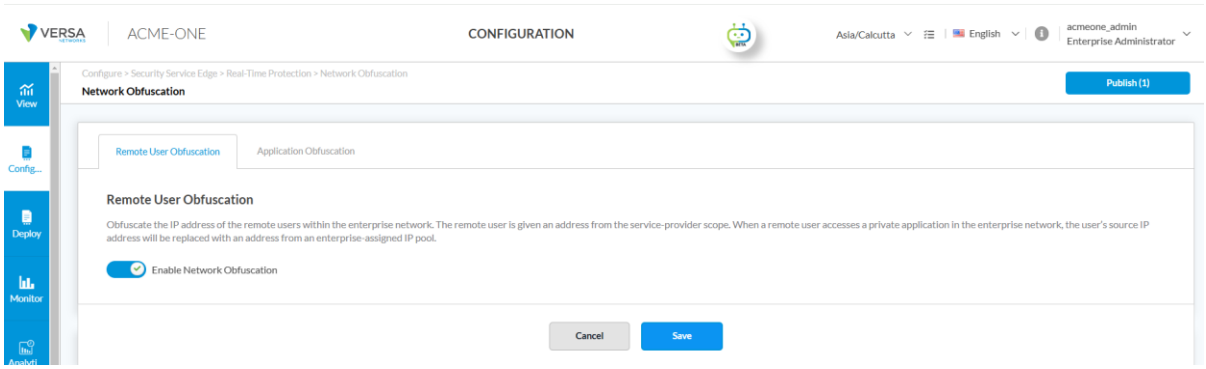
Network Obfuscation

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***

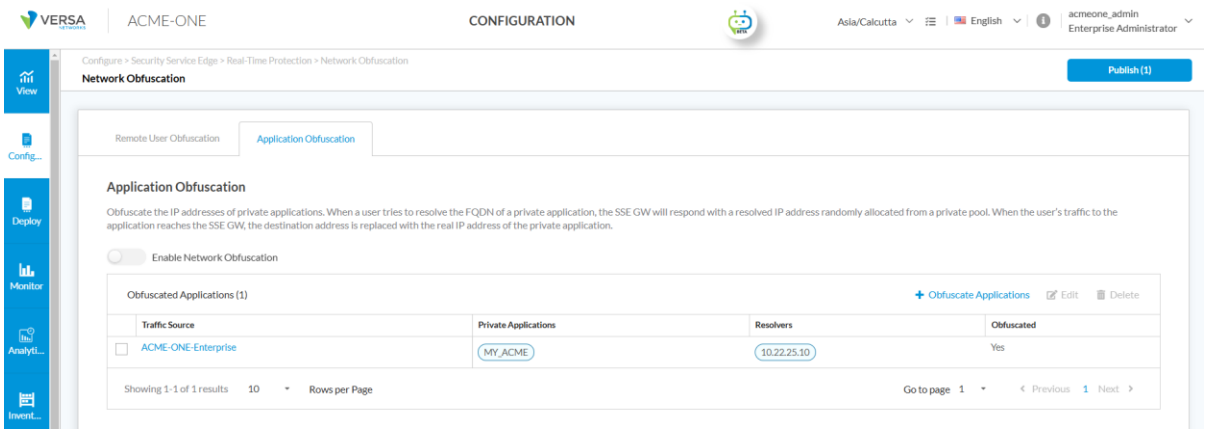
Remote User Obfuscation

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.



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.



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.