VERSA

IMPLEMENTATION GUIDE

Step-By-Step Configuration Guide for Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA)

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) and Versa Secure Internet Access (VSIA).

Versa Secure Access Solutions deliver comprehensive, software-defined connectivity and security for today's hybrid workforce. Built on Versa's industry-leading Secure Access Service Edge (SASE) framework, these solutions ensure secure, reliable access to both enterprise and internet resources — anywhere, anytime.

Versa Secure Private Access (VSPA) enables employees to securely connect to enterprise applications hosted in on-premises data centers, private clouds, or public clouds. Leveraging the Zero Trust Network Access (ZTNA) framework, VSPA safeguards users and applications through identity-driven, policy-based access control, seamlessly integrating networking, security, and cloud-delivered services.

Versa Secure Internet Access (VSIA) provides secure and optimized internet connectivity from any location. It protects users, devices, and data through advanced security capabilities — including Secure Web Gateway (SWG), Next-Generation Firewall-as-a-Service (NGFWaaS), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP). VSIA extends protection to headquarters, branches, home offices, remote workers, travelers.

Together, Versa Secure Private Access and Versa Secure Internet Access offer a unified approach to Zero Trust and SASE — empowering enterprises with secure, seamless access to both private and public resources.

Document Information

Title	**Config Guide for Versa Secure Private Access (VSPA) & Versa Secure Internet Access**
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 get in touch with 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.

Contents

Scenario

ACME-ONE, a global enterprise, needs two things at the same time:

- **Secure remote access** for users working outside the office who need to reach private applications in their datacenters.
- **Secure internet access** for users inside branches and campuses—without wrecking performance or user experience.

To deliver this, ACME-ONE uses **Versa Secure Private Access (VSPA)** and **Versa Secure Internet Access (VSIA)** together as a unified Zero Trust framework.

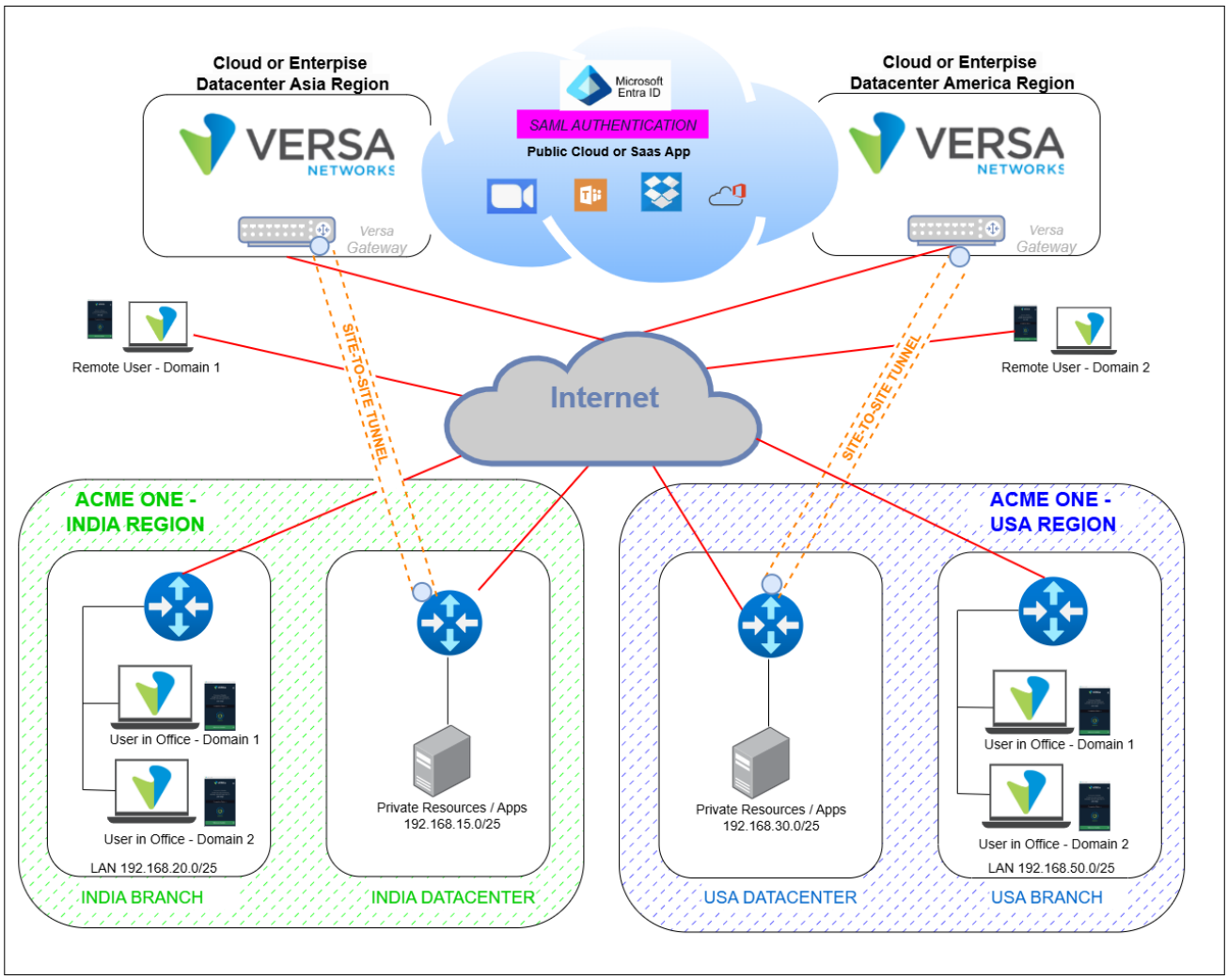
- **VSPA** brokers least-privilege access from remote endpoints to private applications through the SSE gateway.
- **VSIA** secures web traffic for branch/campus users, optimizes SaaS performance, and applies policy enforcement for all outbound internet use.

Identity services come from **Microsoft Entra ID**, which also handles user and group lifecycle automation using **SCIM**.

Customer Requirements

- Strong authentication (Microsoft Entra ID).
- Policy enforcement is based on users or groups.
- Local Breakout of approved application´s traffic (conferencing apps).
- Security enforcement via SSE Gateway: TLS encryption/decryption, Antivirus (AV), Intrusion Prevention System (IPS), URL Filtering.
- Exclude approved URL categories from TLS inspection and enforcement.
- Avoid access to personal and/or external Saas Tenant**.**

Topology



Topology Overview

This topology represents ACME-ONE solution with 2 regions (India and USA) datacenters and branches. The datacenters of each region connect to the nearest cloud-hosted Versa SASE gateways through encrypted tunnels. The organization also has remote users connecting directly to the internet from outside the branches.

1. **Remote Users (Work from Home)**

   - Endpoints run the Versa SASE Client
   - Authentication via Entra ID (SAML/OIDC, MFA enforced)
   - Remote access to private apps is routed through datacenter IPsec tunnels and into the SSE gateways

- SSE gateways provide a DNS proxy with Split-DNS for internal zone resolution
- Local breakout is allowed for trusted Conferencing Apps (Zoom)
- Remaining internet traffic goes through the SSE Gateway
- TLS decryption is applied to all internet traffic except regulated financial/medical categories
- High/medium risk + unknown/undefined traffic is fully inspected (AV + IPS)
- URL filtering blocks high-risk and reputation-based threats; uncategorized/undefined URLs should be blocked.

2. Branch & Campus Topology

- Branch users run the Versa SASE Client for user identification, but with the Trusted Network Detection (TND) Gateway Assisted feature, it creates only a control channel to the Gateways without any tunneling. This will bypass all traffic, including local private traffic. Internet traffic should be routed to the SSE gateway using the site-to-site tunnels, except for the conference application (Zoom).
- Authentication is performed via Entra ID (SAML/OIDC + MFA).
- Internet traffic is decrypted, inspected, and enforced with AV/IPS, except for regulated categories (finance and health)/sites (Do-Not-Decrypt policies).

Key Steps

- **Establish SASE–Datacenter Site-to-Site Tunnels**
  - Build IPsec tunnels from global SASE gateways to each datacenter region.
- **Integrate Microsoft Entra ID (SAML)**
  - Configure identity provider settings on the Versa gateways
  - Enable MFA and SCIM-based user/group sync
- **Secure Access Profiles**
  - Define DNS servers (no domains)
- **Secure Access Rules (VSIA + VSPA)**
  - Create SA rules for VSIA+VSPA

- Add exceptions for trusted applications (Zoom)
- Enforce identity-based policies

- **TLS Decryption Policies**
  - Add URL category-based bypass rules first
  - Then Apply decryptions for all traffic.
- **Trusted Network Detection**
  - Detect when users are on campus and auto-switch private app flows to LAN
- **SaaS Tenant Control**
  - Enforce corporate-only access to O365 and sanctioned SaaS tenants
- **Apply SSE Security Controls**
  - AV, IPS, DLP as required
  - Web filtering based on group, app, and security posture
- **Real-Time Protection**
  - Block high-risk URL categories and reputation-based threats
  - Enforce controls for uncategorized traffic

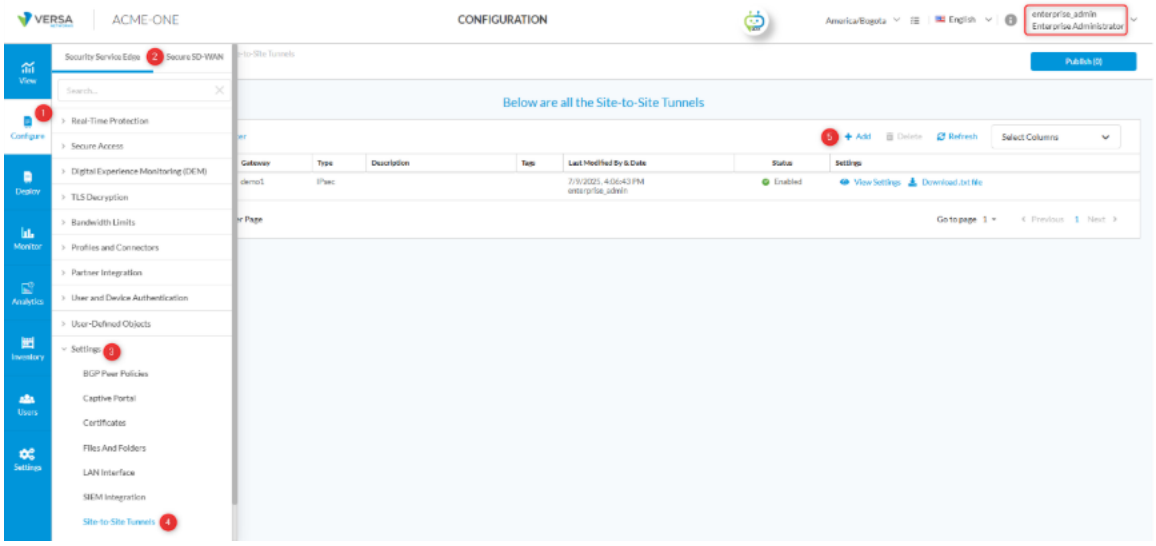
Configuration Steps

Step 1: Set Up Site-to-Site Tunnel

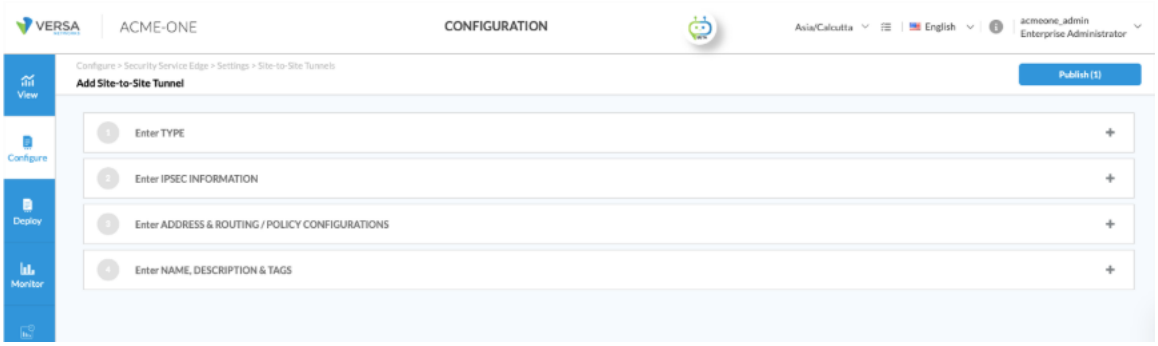
The site-to-site tunnel is essential for allowing remote users connected to the gateway to access enterprise-hosted private applications. The Versa gateway and the customer data center (DC) firewall (or any other device behind which enterprise applications are hosted) establish a tunnel the gateway uses to route remote user traffic to the enterprise's private applications.

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.



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.

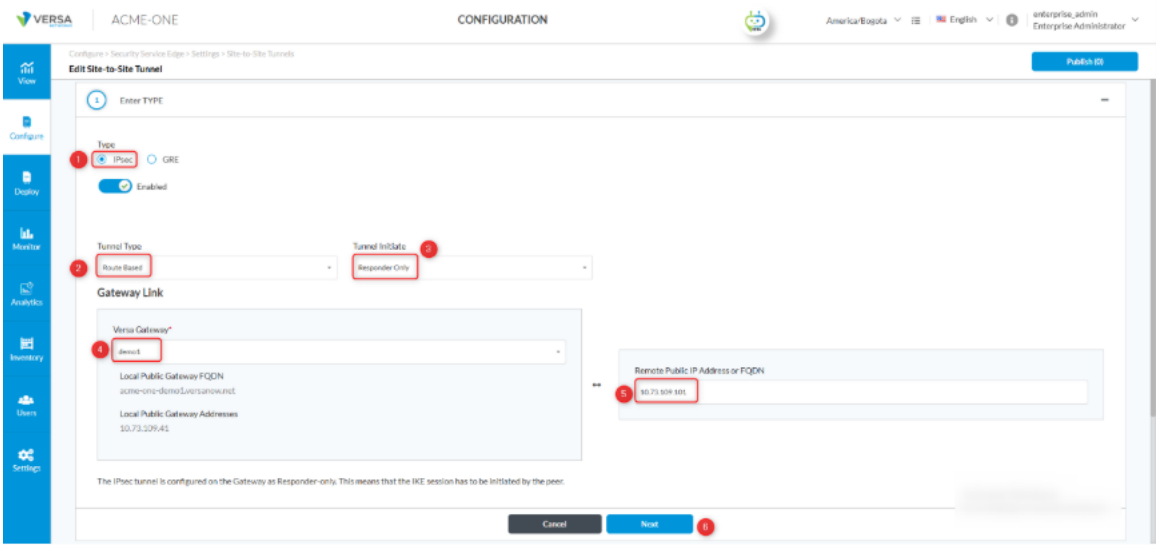
   Note that Versa Gateway is set as ‘responder only’ for the IPsec tunnel. So, the peer must initiate the request for the tunnel for the negotiation to start.

   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.

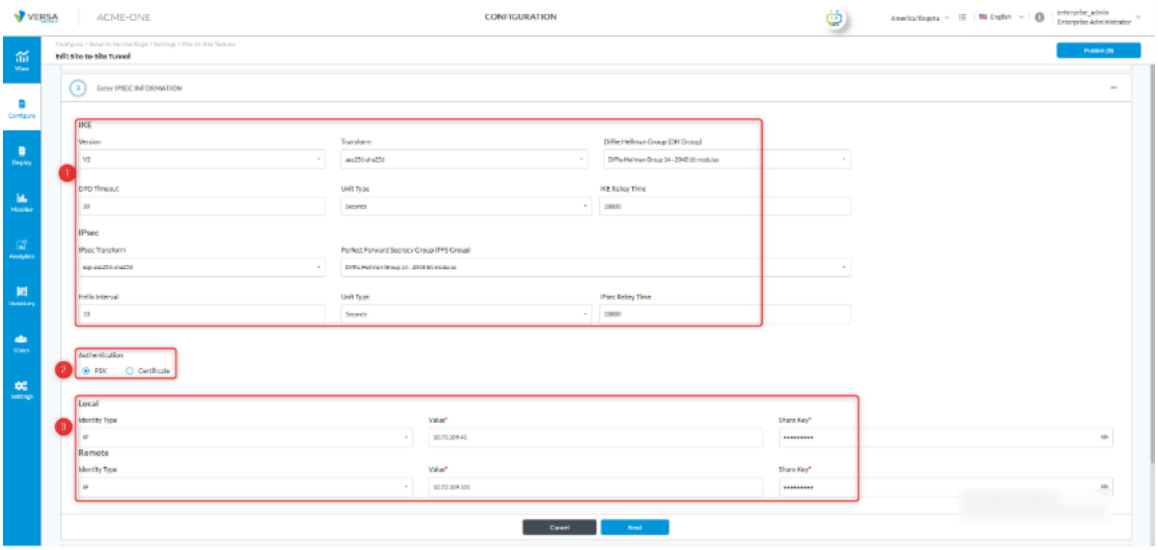
   E. Use the **Remote Public IP Address or FQDN** field to enter your enterprise firewall details as the tunnel endpoint.

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.**

3. 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.

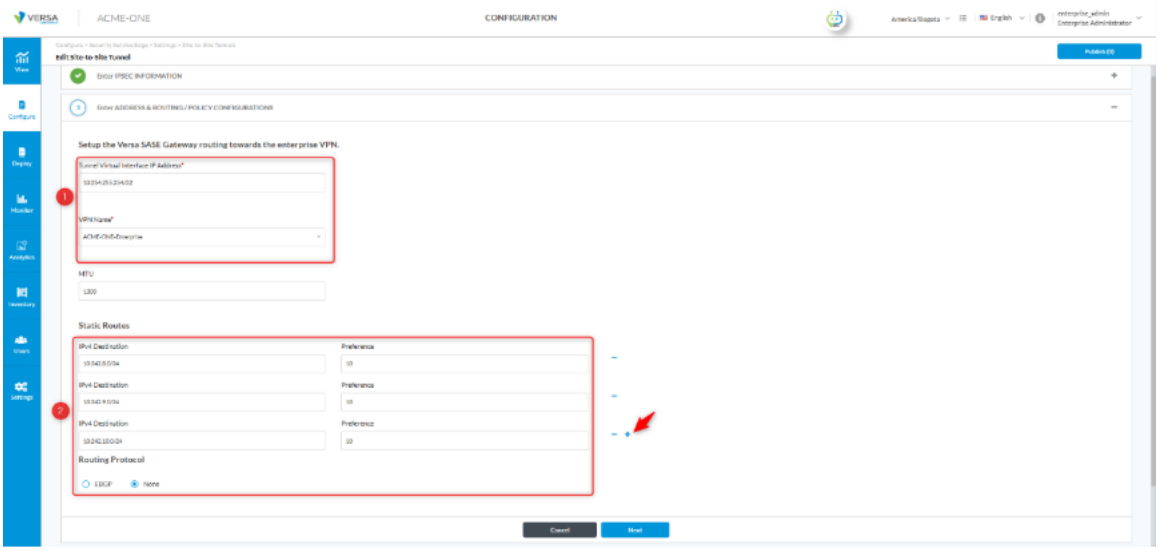
A. Under "Setup the Versa SASE Gateway routing towards the enterprise VPN" configure the following

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.

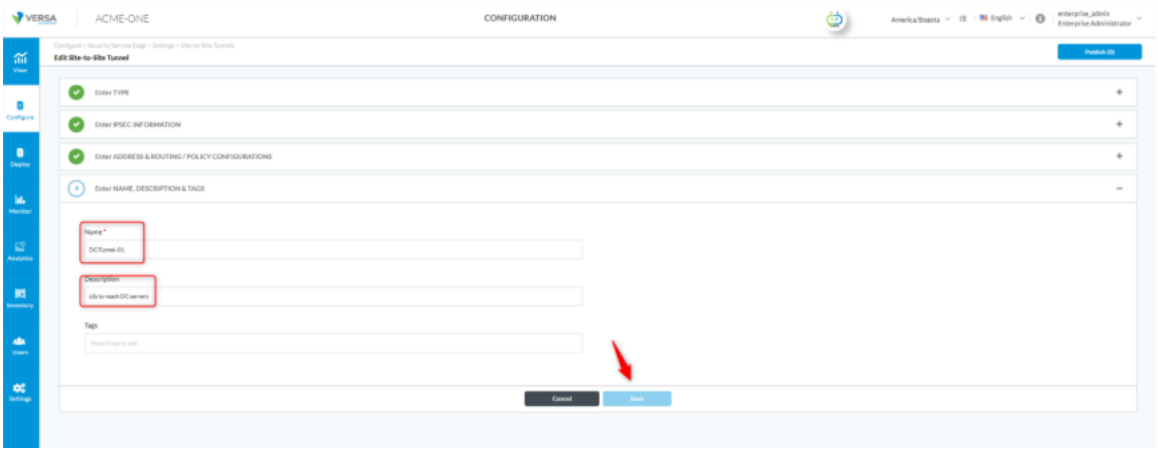
VPN Name to be selected from drop-down, usually the VPN name assigned to your tenant by the service provider, named as <*TenantName-Enterprise*>

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: 192.168.15.0/25, 192.168.20.0/25, 192.168.30.0/25, 192.168.50.0/25).
- Assign a preference value between 1–255 (lower = higher priority).
- Routing Protocol select None.
- Click **Save**.



4. Completing section Enter NAME, DESCRIPTION & TAGS



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.

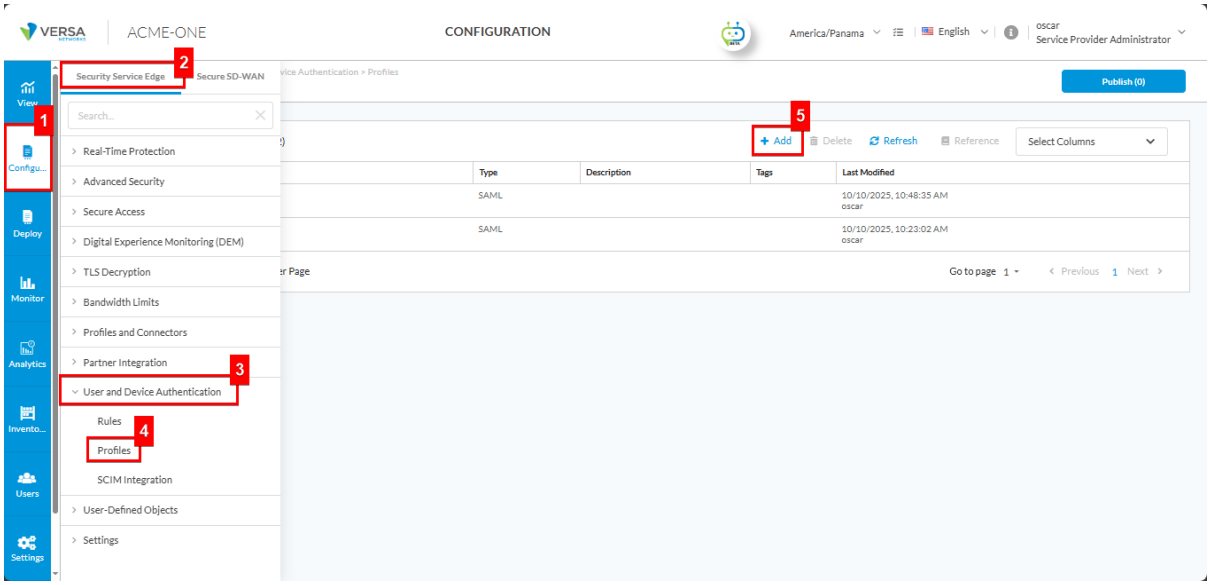
Step 2: Configure Authentication Method

Versa SASE supports various authentication methods, including LDAP and SAML. This example utilizes Microsoft Entra ID with SCIM for users' authentication when connecting via the SASE client.

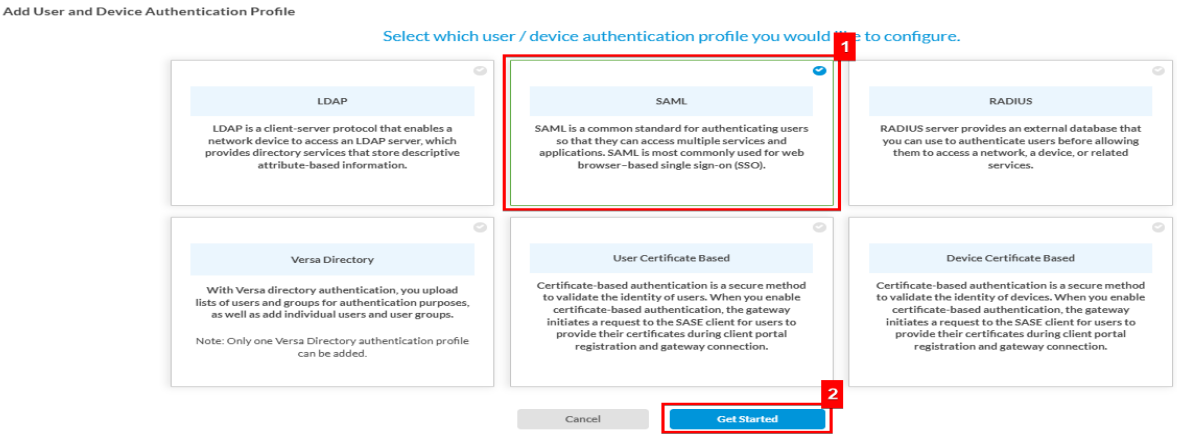
See **Appendix A** for other authentication methods, configurations and options available on the Microsoft Entra ID portal.

For the configurations needed on the Concerto, navigate to:

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

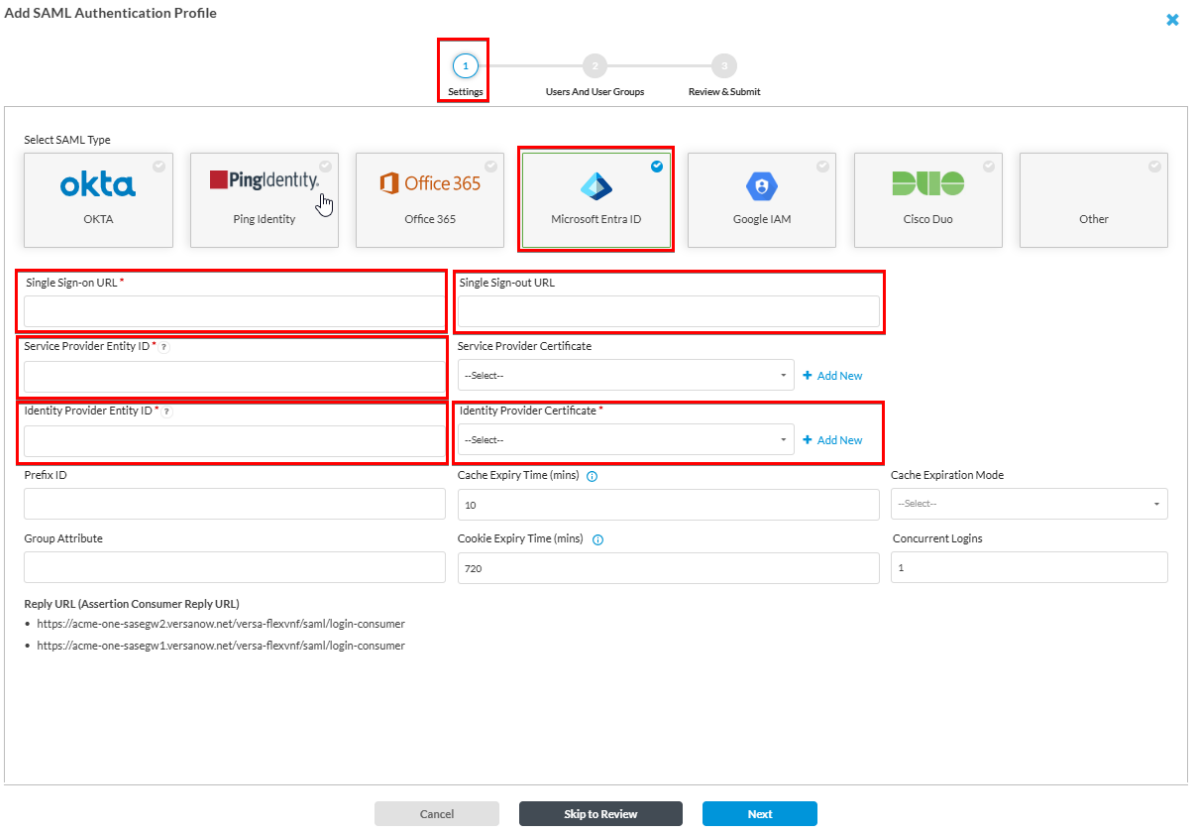


Select **SAML** as Authentication Method then Click **Get Started**



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

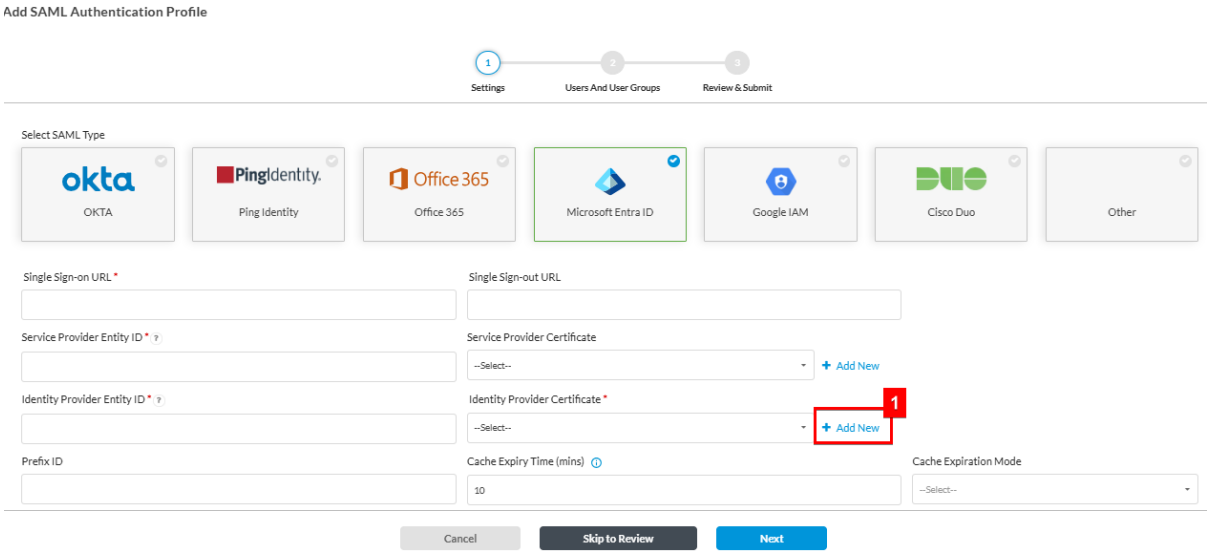
Single Sign-on URL, **Service Provider Entity ID** and **Identity Provider Entity ID** are mandatory fields to be configured, and you must upload a certificate issued by MICROSOFT ENTRA ID.



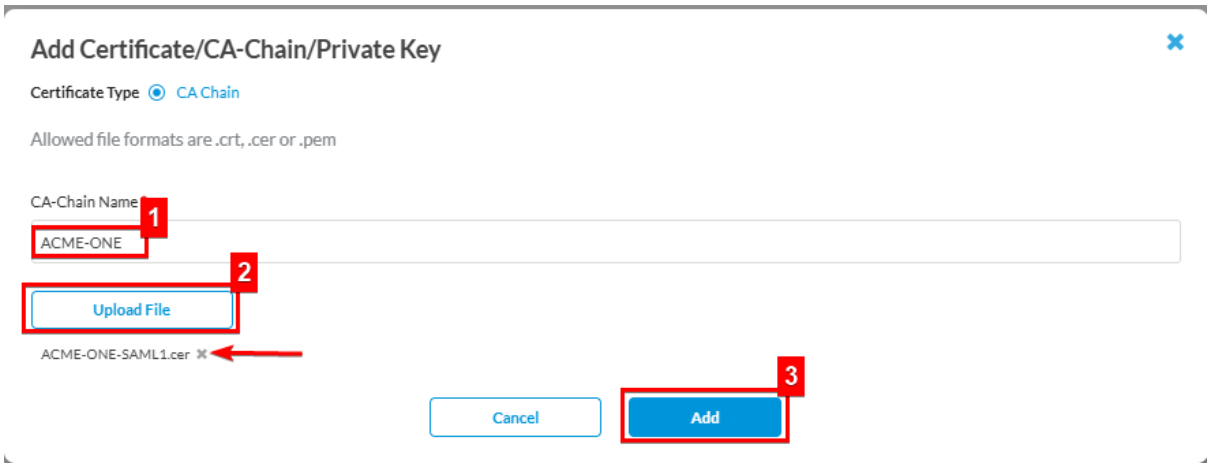
Example:

- **Single Sign-on URL:** https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2
- **Single Sign-out URL:** https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2
- **Service Provider Entity ID:** https://acme-one-sasegw1.versanow.net/metadata
- **Identity Provider Issuer**: https://sts.windows.net/900afbfd-92ce-441a-abc6-ad81e25b7711/

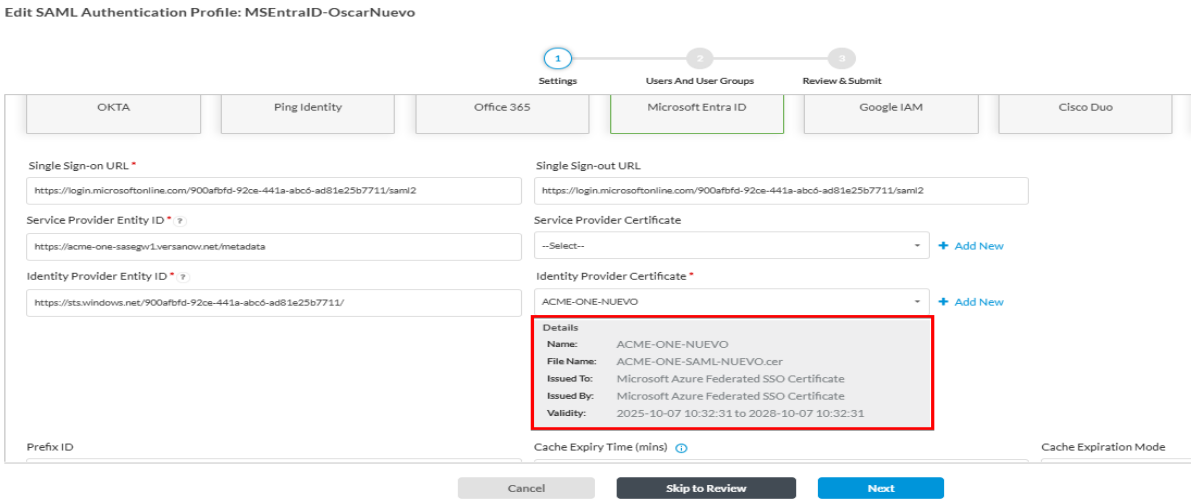
Then, upload the **Identity Provider Certificate** by clicking on the **Add** New button. Rename the downloaded certificate file from .cert to .crt before use on concerto.



Assign a descriptive name for **CA-Chain Name,** then upload certificate by clicking on the **Upload File**. Locate the certificate and click **Add**



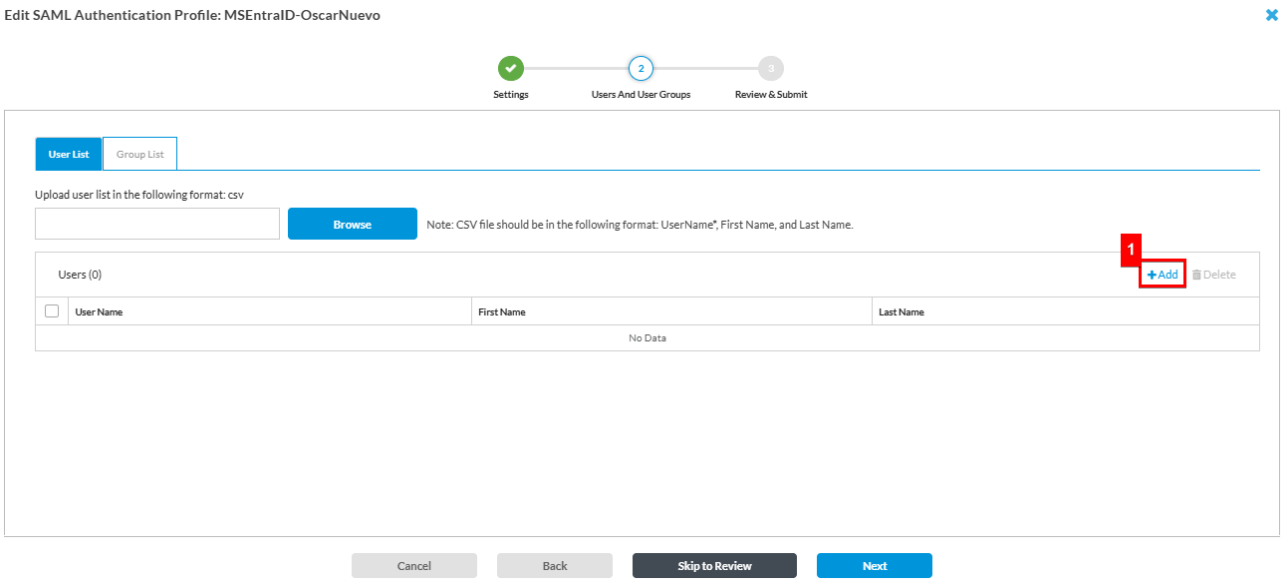
If the certificate was uploaded successfully, the certificate details will be displayed.



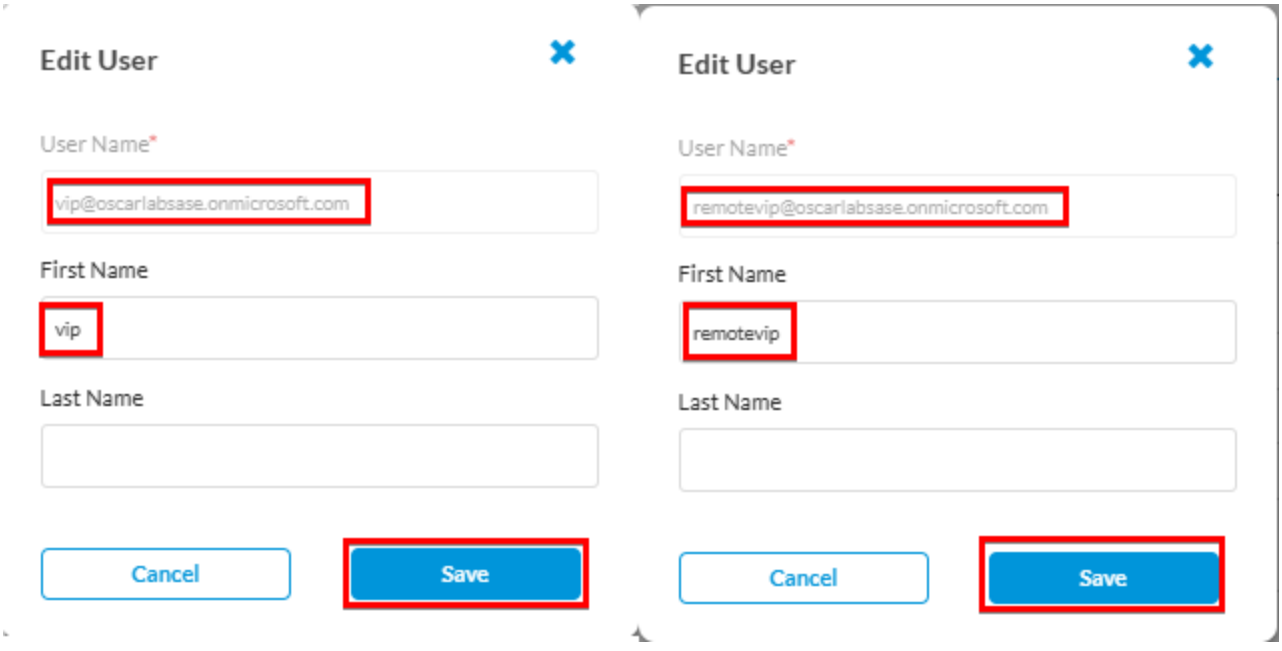
Then **Next**

On the **Users and User Groups** page, you can add either individual users or entire groups. Unlike LDAP, SAML-based users and groups do not auto-populate; they must be created manually. These users or groups can then be referenced when configuring Secure Access Rules and Real-Time Protection Rules.

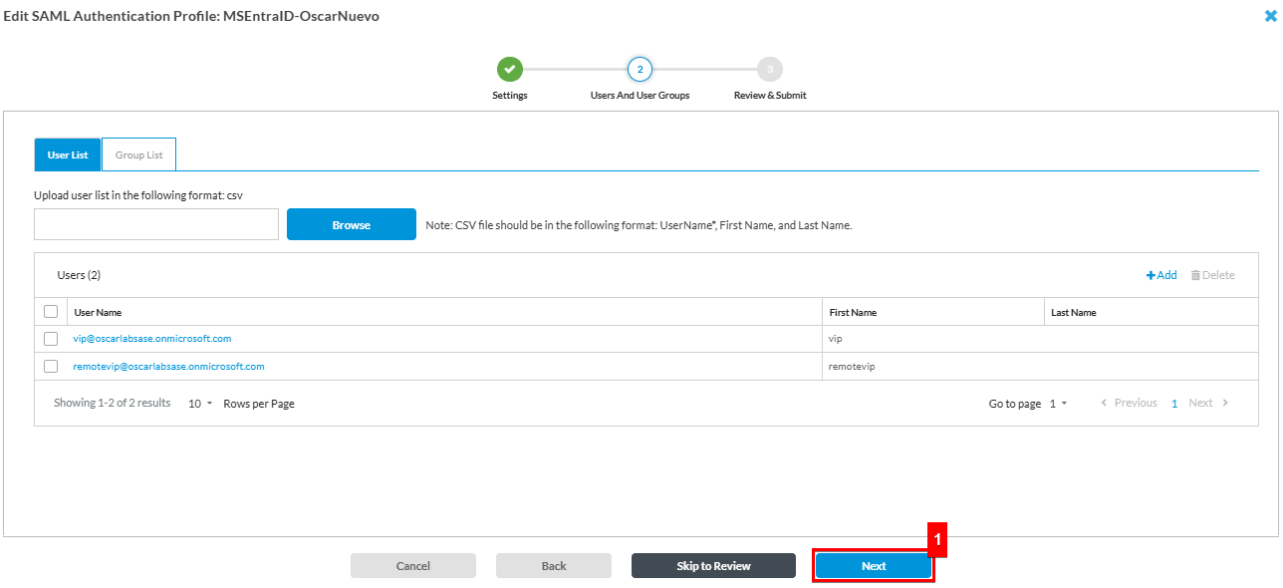
In this case we will add manually 2 users (vip@oscarlabsase.onmicrosoft.com and remotevip@oscarlabsase.onmicrosoft.com) for testing purposes. Click ***+Add***.



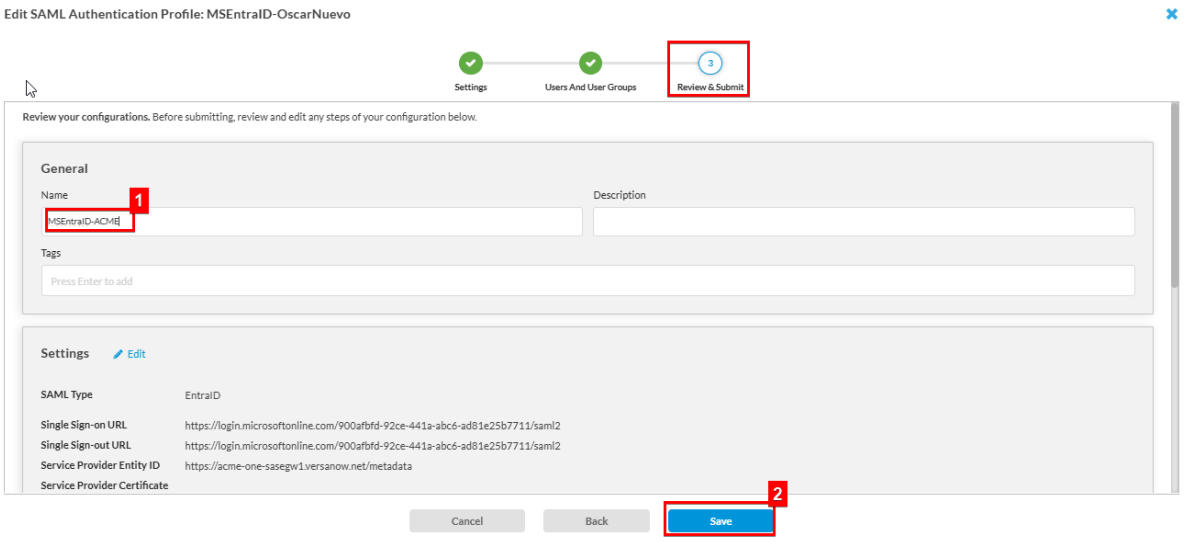
Add the ***Username, First Name*** and click ***Save*** for both users.



Click ***Next*** to proceed.



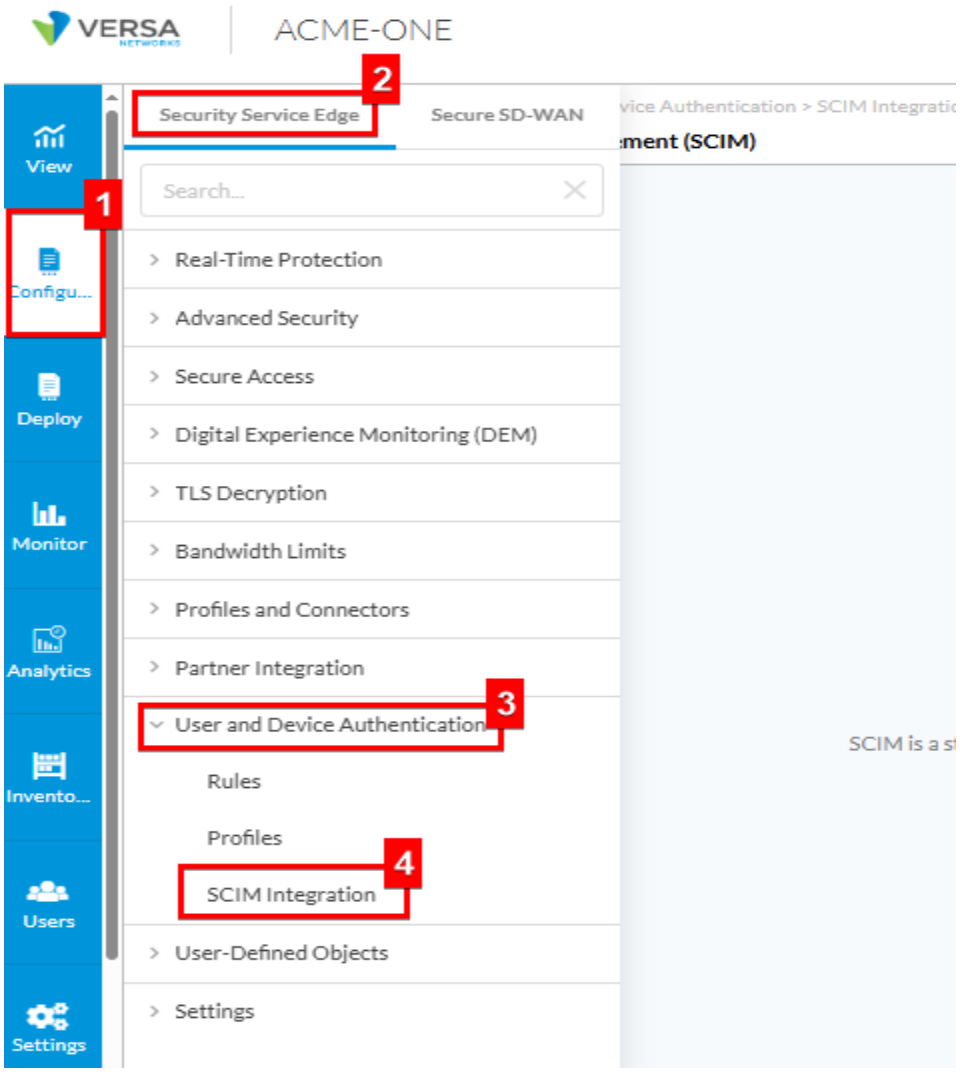
On the **Review & Submit** page, enter a **Name** and **Description** for the profile, then review all configuration details including general information, SAML settings, and assigned users or groups. Once confirmed, click **Save** to complete the profile creation.

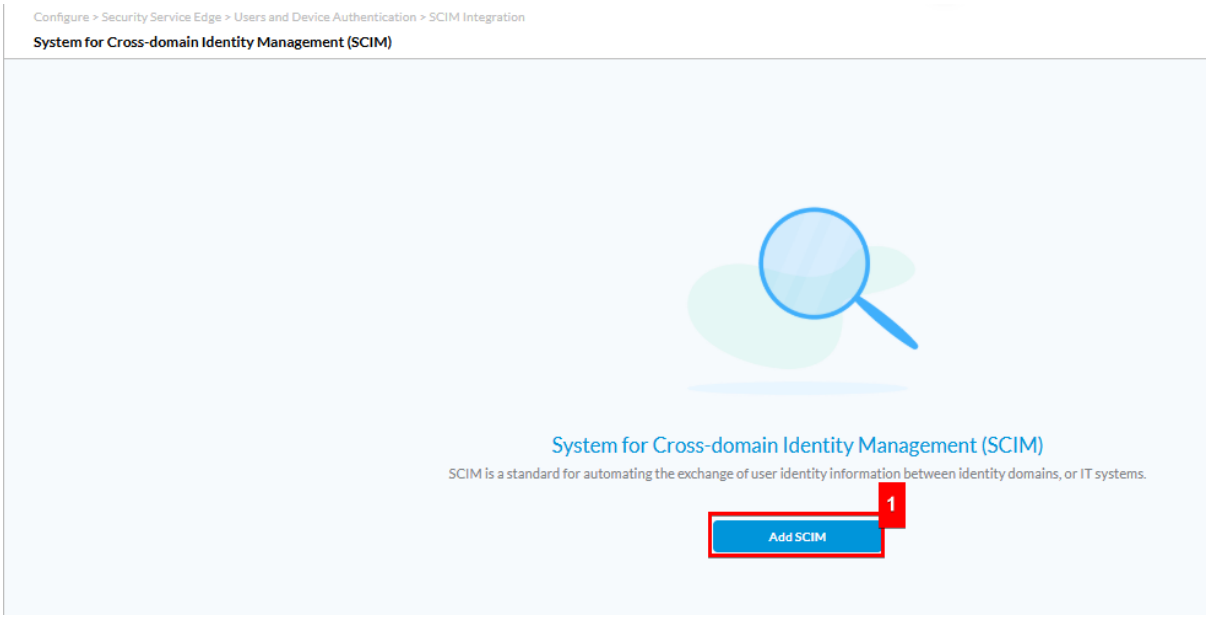


NOTE: As an alternative; to avoid adding the users manually, there is the option to enable **SCIM** integration to automate user and group provisioning. SCIM service can be leveraged as another method for managing users and groups. Unlike LDAP-based authentication profiles, SCIM operates as part of a separate identity provisioning setup outside of the profile configuration workflow. The SCIM provisioning steps are mentioned below.

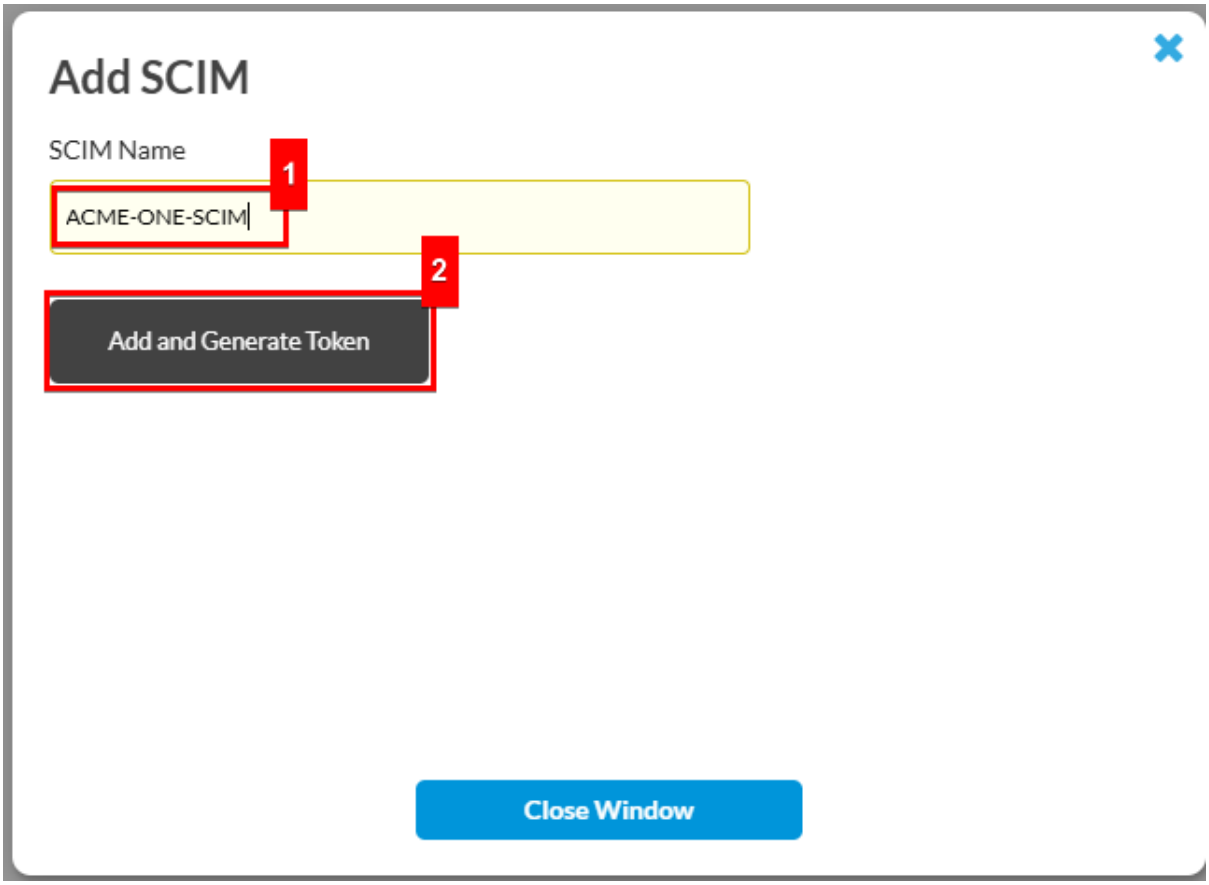
Provision SCIM Service

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



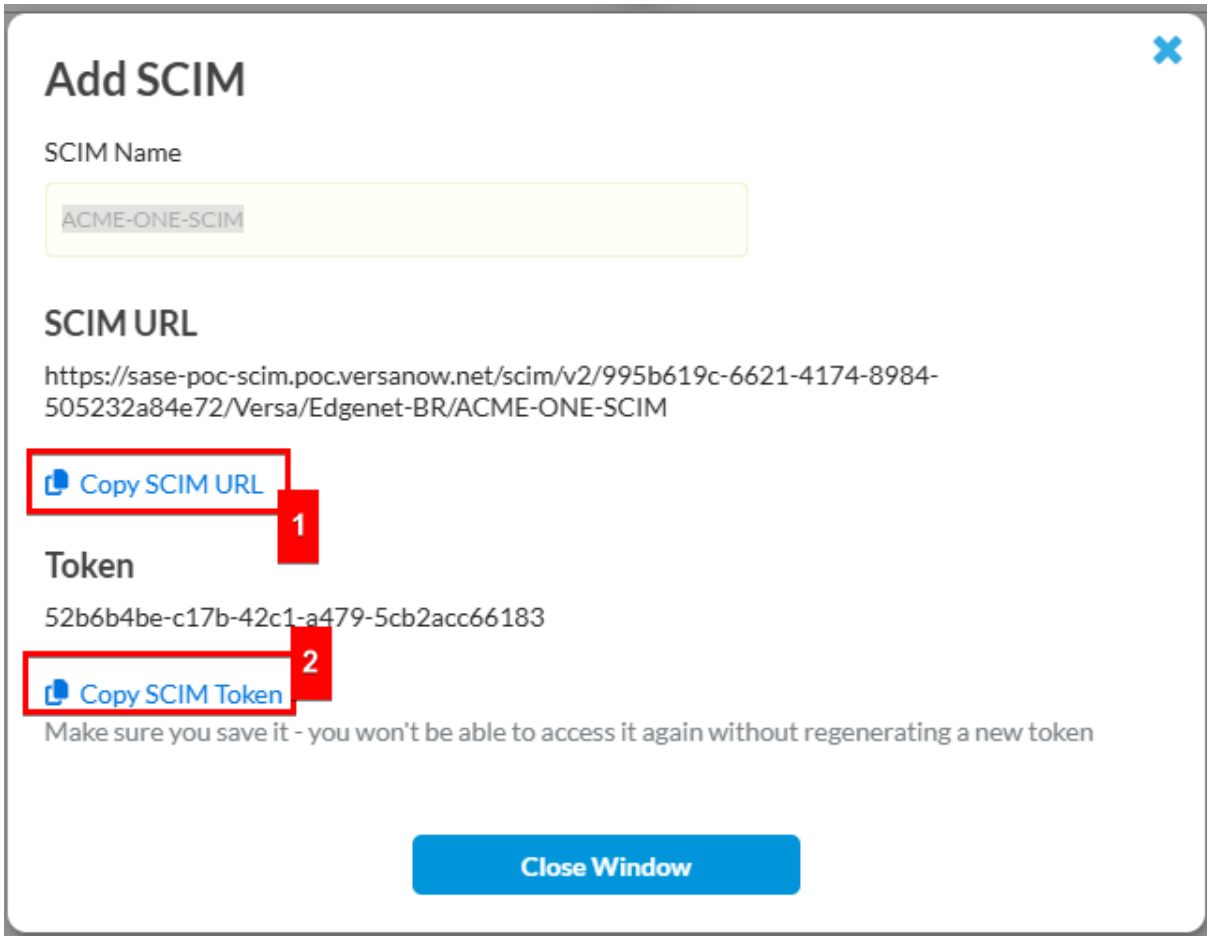


When the Add SCIM popup window displays. enter a ***name*** in the SCIM Name field. Ensure that you use a unique name to identify the IdP from which users or user groups are provisioned and click on ***Add and Generate Token***



The following window displays. Copy the SCIM URL and token and save them.

The URL includes the tenant's name, VMS ID, SCIM cloud server FQDN, and the SCIM name that you provide in the Add SCIM screen. You use this URL and token when you provision SCIM using Microsoft Entra ID. Entering these details in Entra creates a channel between the IdP and SCIM cloud server.



Step 3: Configure User-Defined Object

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 will create a couple of **Private Applications** to be used in our **Private Protection Policies**. The following section outlines the steps to create a Private Application.

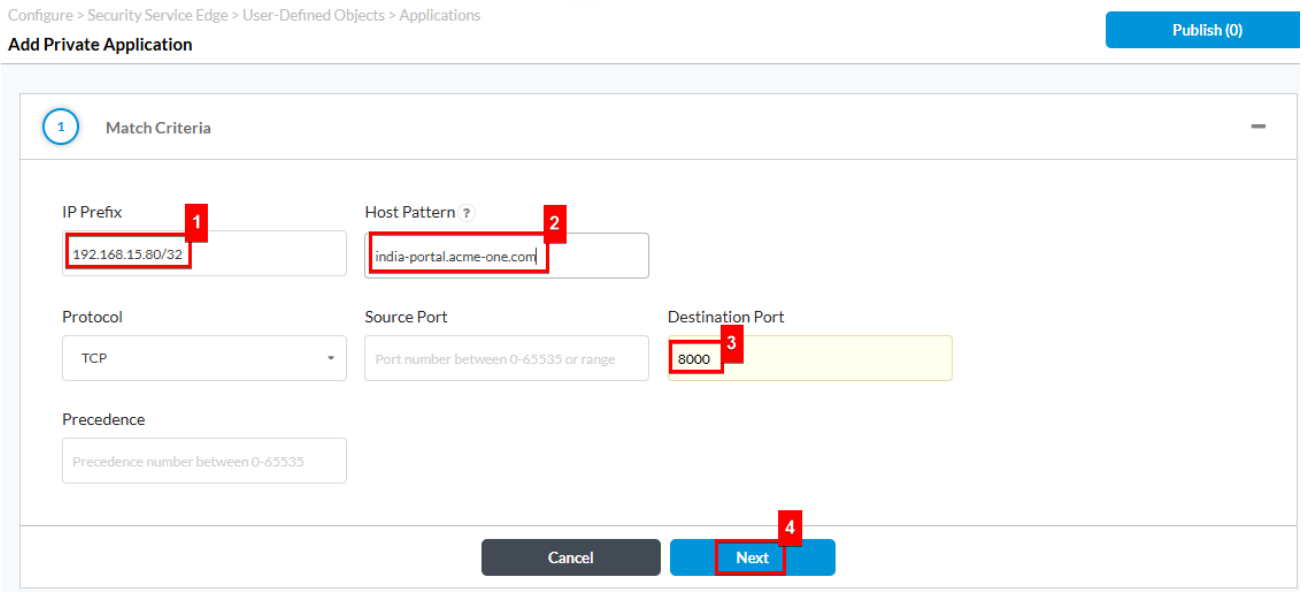
To create a **Private Application**, navigate to

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

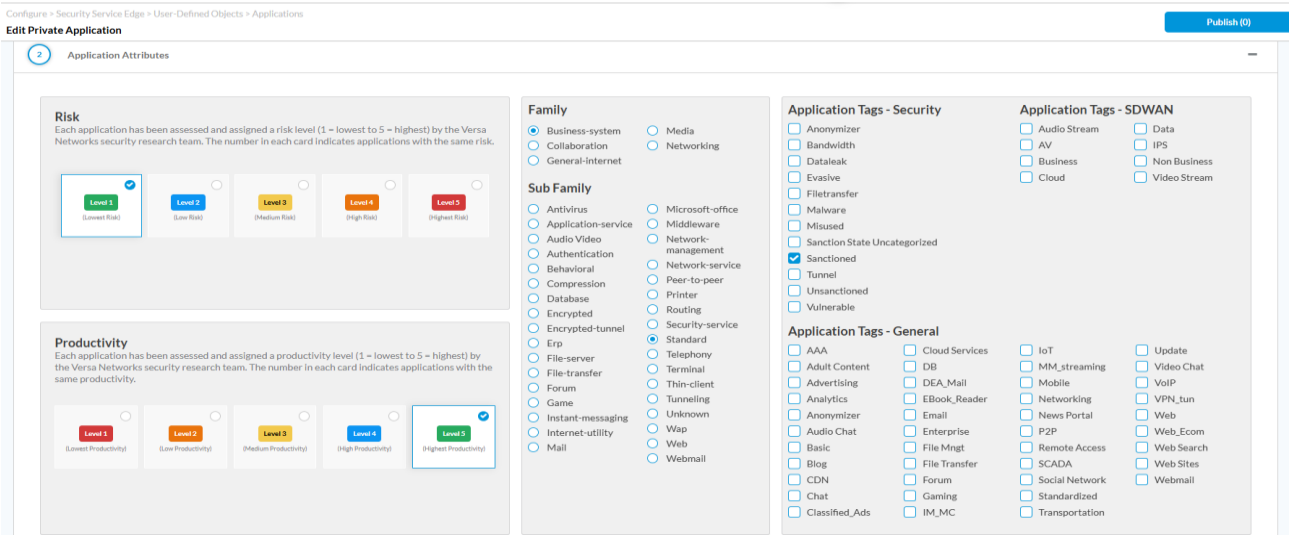
Then, create the test apps **india-portal.acme-one.com** and **usa-apps.acme-one.com** as follows:

india-portal.acme-one.com:

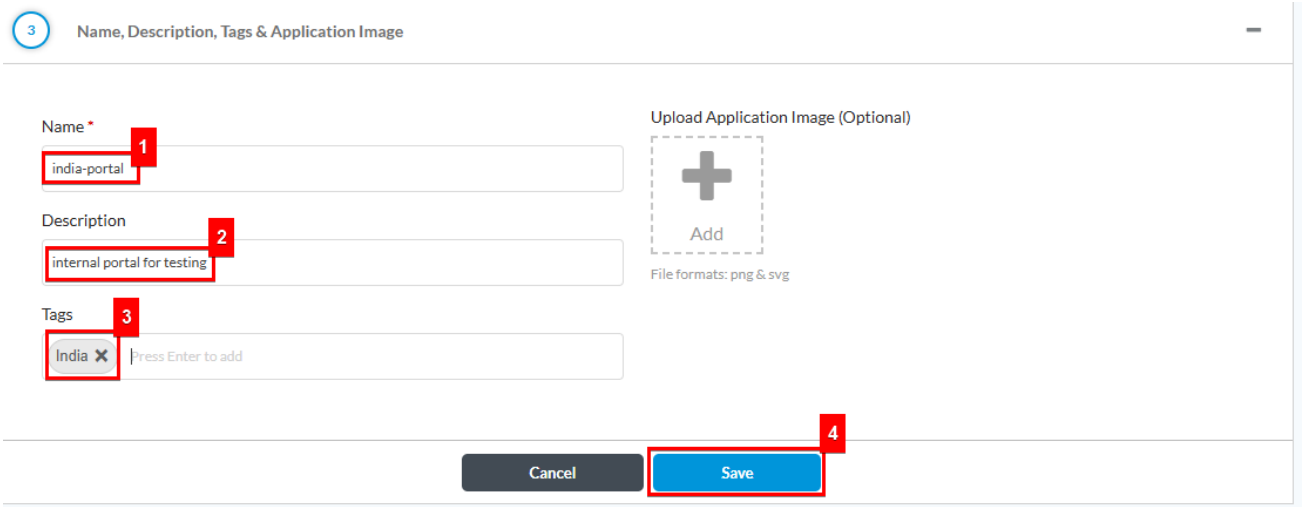
Match Criteria



Application Attributes

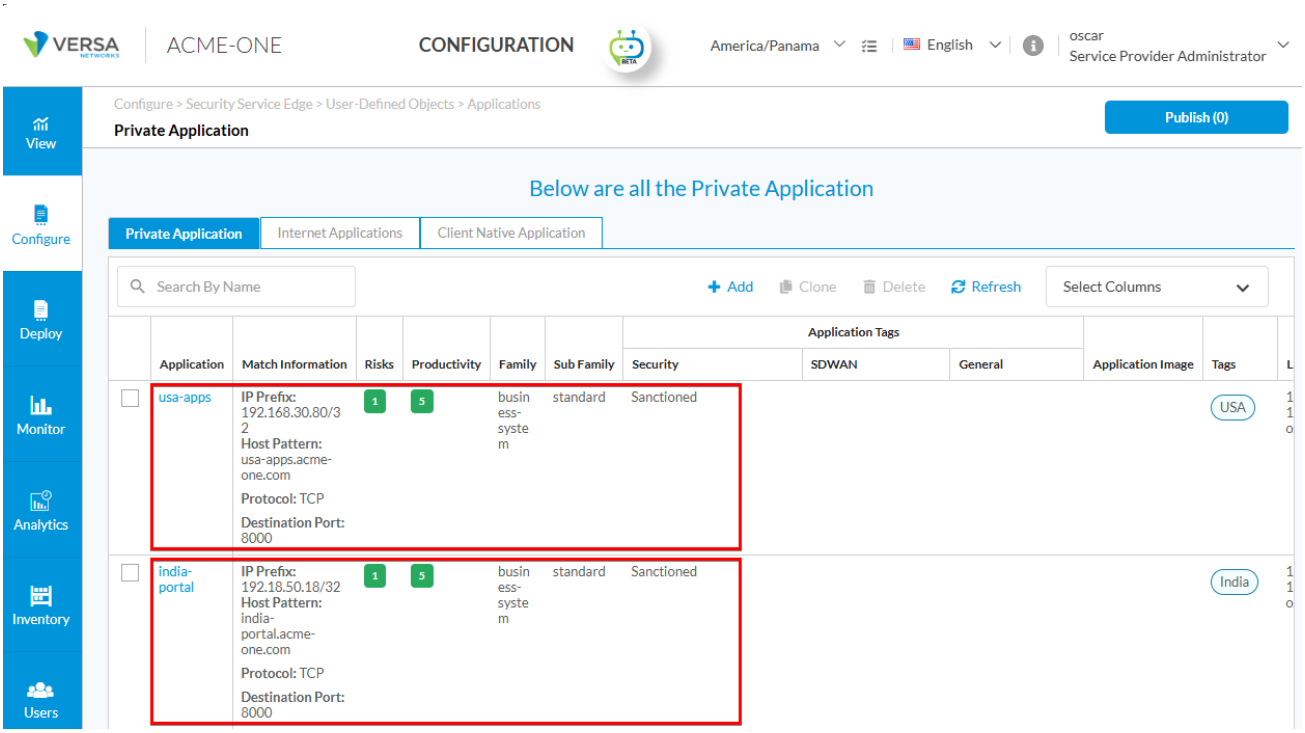


Name, Description, Tags & Application Image.



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

The private app definitions should resemble the image below.



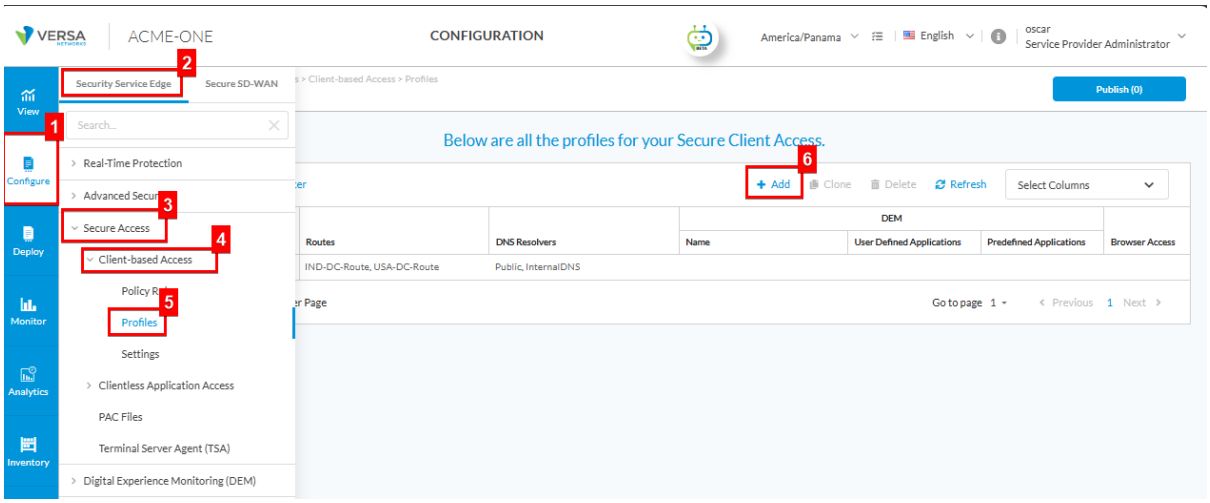
Step 4: Secure Access Profile: Configure DNS Server

For the VSIA & VSPA setup, we need to configure the DNS server IP address without Domains. In this case, ACME-ONE uses public DNS server 8.8.8.8.

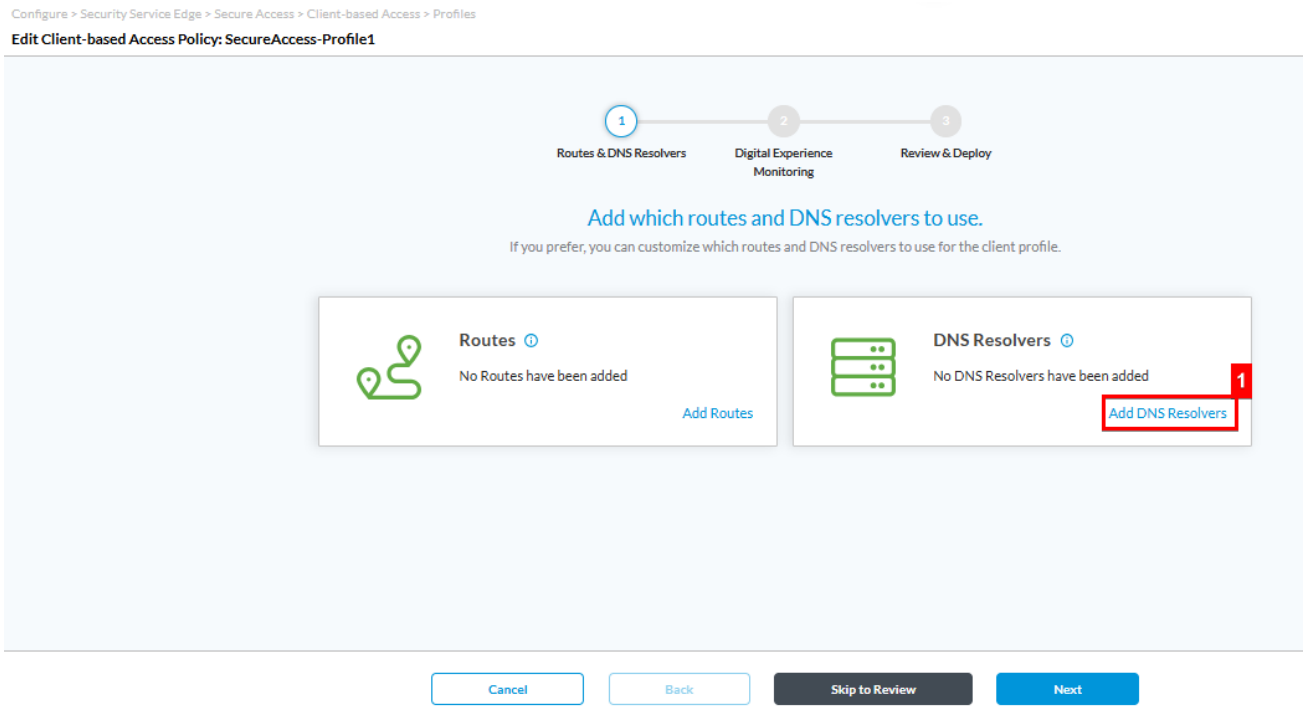
Note: **Secondary DNS Server** – It is recommended to configure one or more redundant DNS servers to ensure name resolution continuity in the event of a primary DNS server failure. In this configuration, a secondary DNS server is not defined because it is optional for this deployment scenario.

.

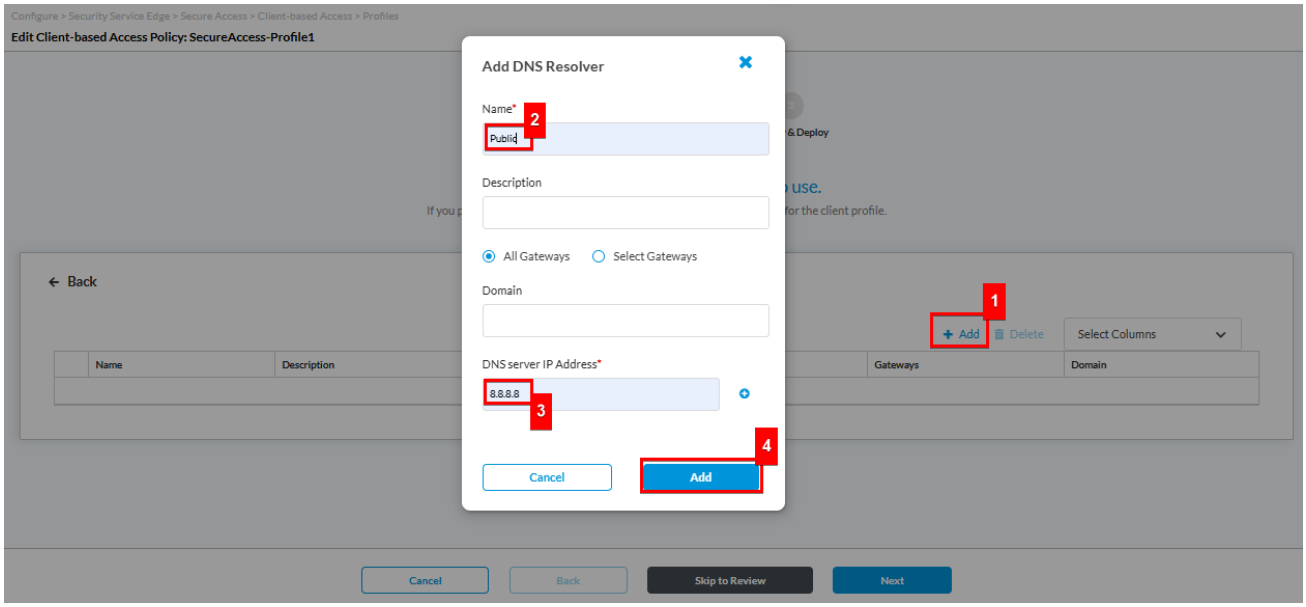
To create a Secure Access profile, navigate to ***Configure > Security Service Edge > Secure Access > Client-based Access > Profiles*** and click on ***+Add*** as shown in the figure below.



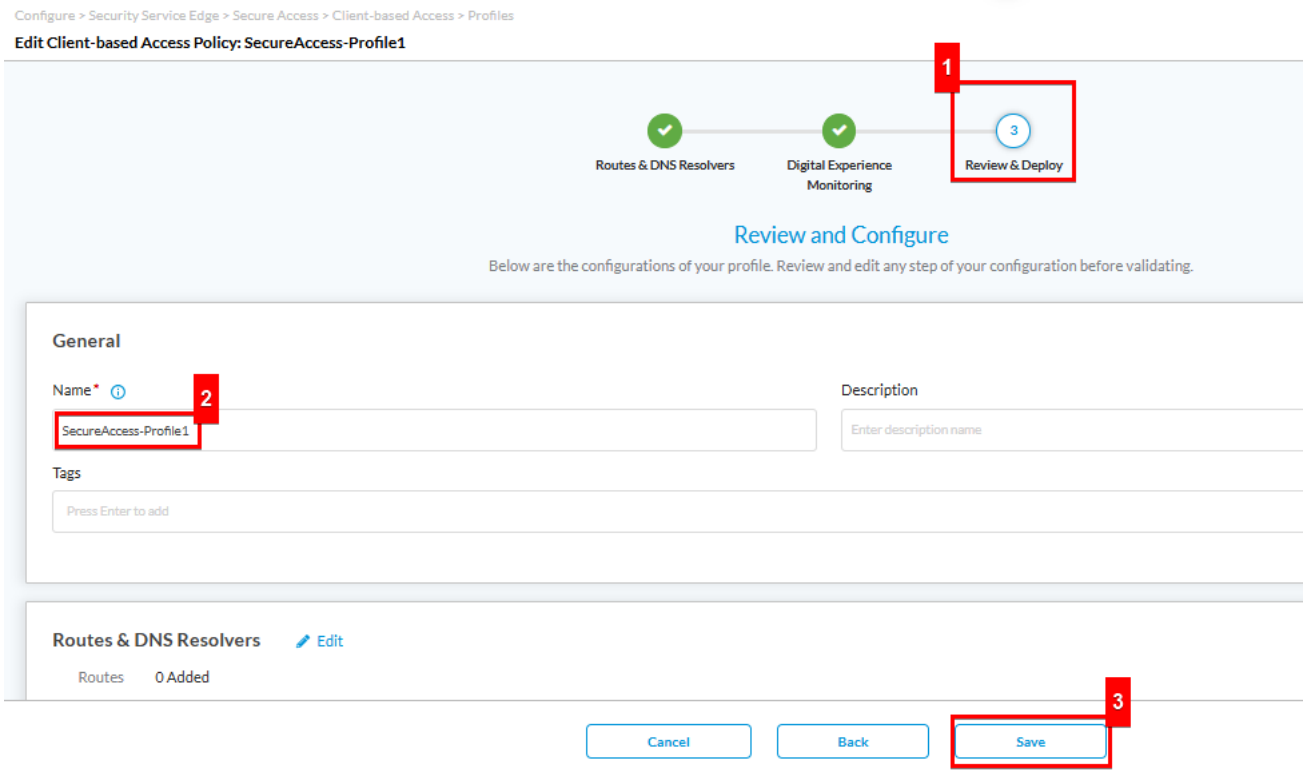
Click on ***Add DNS Resolvers***



Insert the DNS information and click ***Add***. Then click ***Next*** until Review & Deploy section.



Then click ***Next*** until ***Review & Deploy*** section. Add a descriptive ***Name*** and click ***Save.***



Step 5: Define Secure Access rules

In VSPA + VSIA setup, the SSE Gateway is the default gateway for private and public traffic.

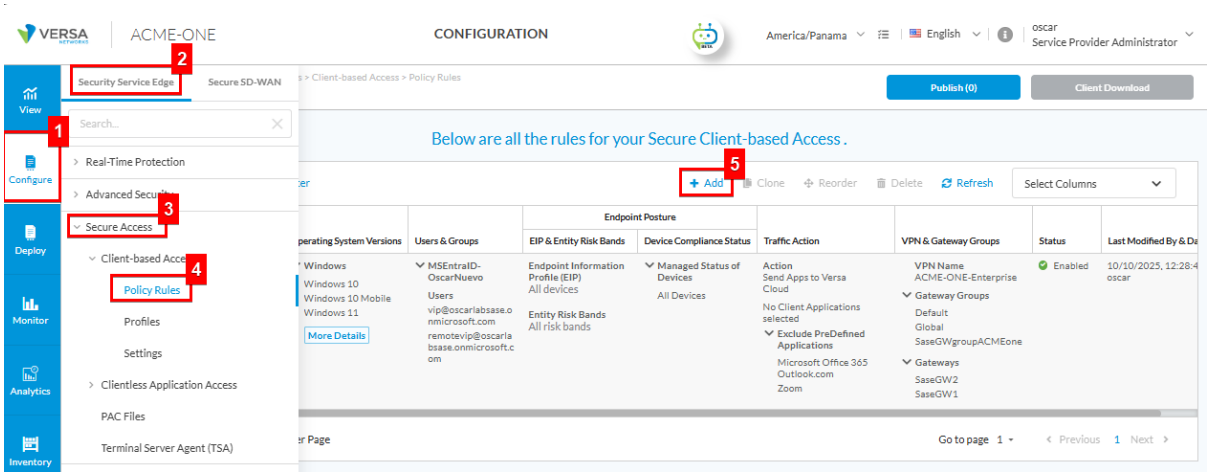
When the users are working from home, all traffic is routed through the SSE Gateway but to meet the requirements of this case, the only exception will be conferencing applications traffic, which will be configured to break out locally.

When users are in the office, the Trusted Network Detection (TND) Gateway Assisted feature will be used to bypass private traffic locally and the remaining internet traffic will continue to be routed via the SSE gateway, including the same exception of conferencing application (Zoom).

The TND feature will be configured in the next step of this document.

To meet the requirements of this case; since only one level of users is being used for testing purposes, only one secure client access rule is needed to enable local breakout for conferencing application (Zoom), so that these applications are sent directly to the Internet without passing through the SASE gateways.

To configure navigate to ***Configure*** > ***Security Service Edge*** > ***Secure Access*** > ***Client-based Access*** > ***Policy Rules*** and click on ***+Add***.

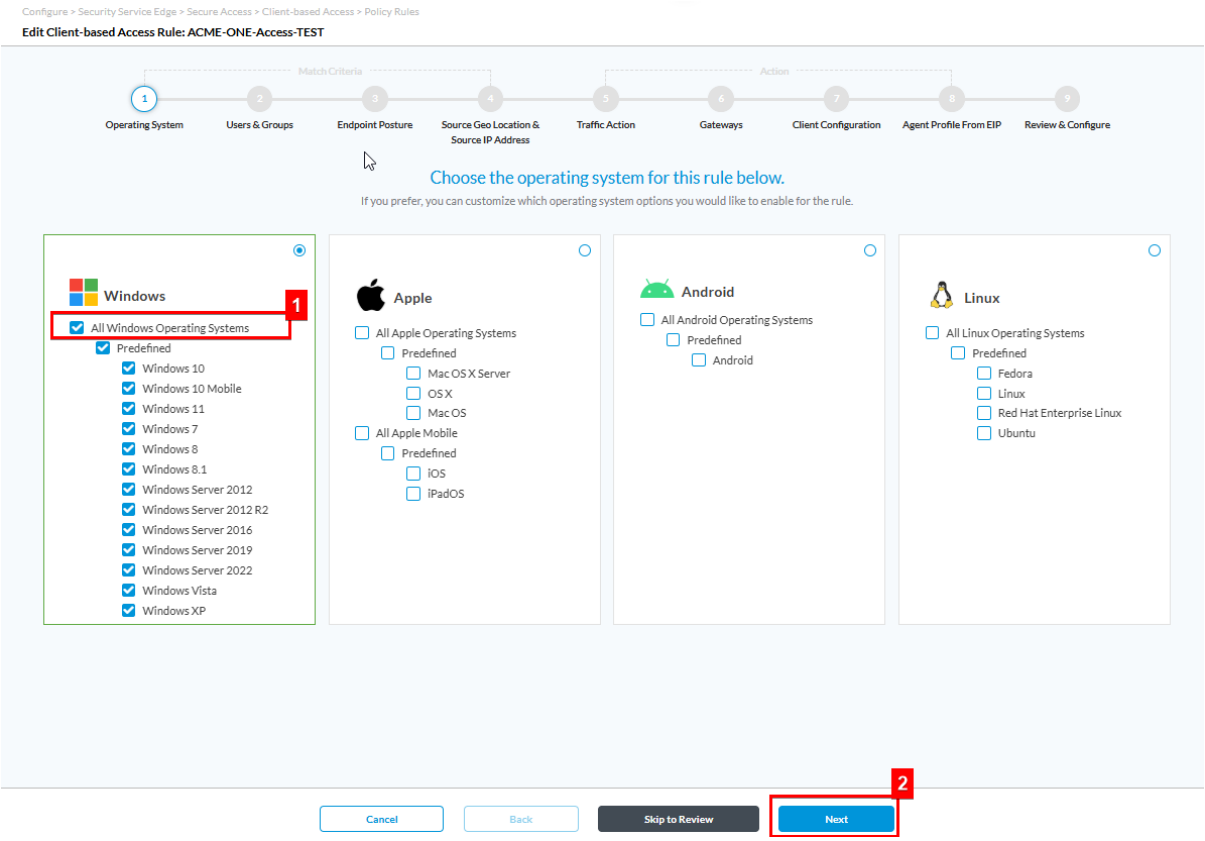


For this example, we are setting up the secure access rule according to these requirements:

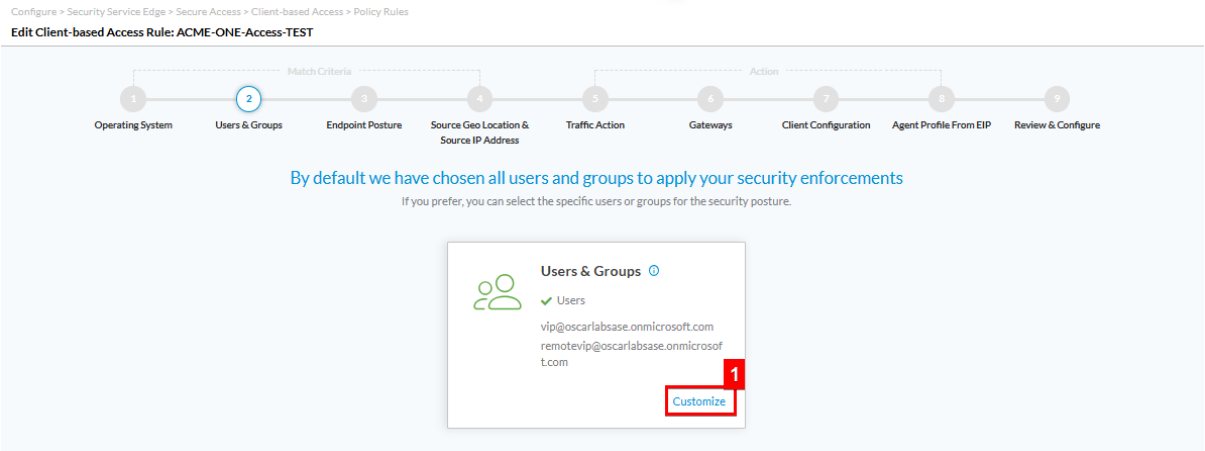
Knob	Current Use Case	Reason	Best Practice (Production)
Operating Systems	All Windows versions	Ensures compatibility with all Windows OS versions in the enterprise.	Limit to *supported/managed OS versions only* (e.g., Win11). Block EOL OS (Win7) to reduce risk.
Users & Groups	All required user or groups (vip and remotevip)	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: no eip profile	No Enforcement required from the users devices.	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 all users need this breakout	We can define an IP address to enforce the user connection from a specific location and a WAN circuit.
Traffic Action	Subscription: VSPA (Versa Secure Private Access) & VSIA (Versa Secure Internet Access)	Secure access to internal applications and secure internet traffic	Same as lab.
Traffic Action	Allow – Send Apps to Versa Cloud Gateway. Add Zoom to the applications	All traffic will go the gateways, but the applications added will bypass the tunnels.	Select approved applications that are trusted and need no enforcement to optimize their performance sending the traffic directly to the internet
Gateways	Select the gateways available for this tenant	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	Select the Secure Client Access Profile: SecureAccess-Profile1	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	IPsec	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	Optional in the lab.	**To** enforce real-time posture evaluation with EIP. Continuous evaluation is key for Zero Trust.

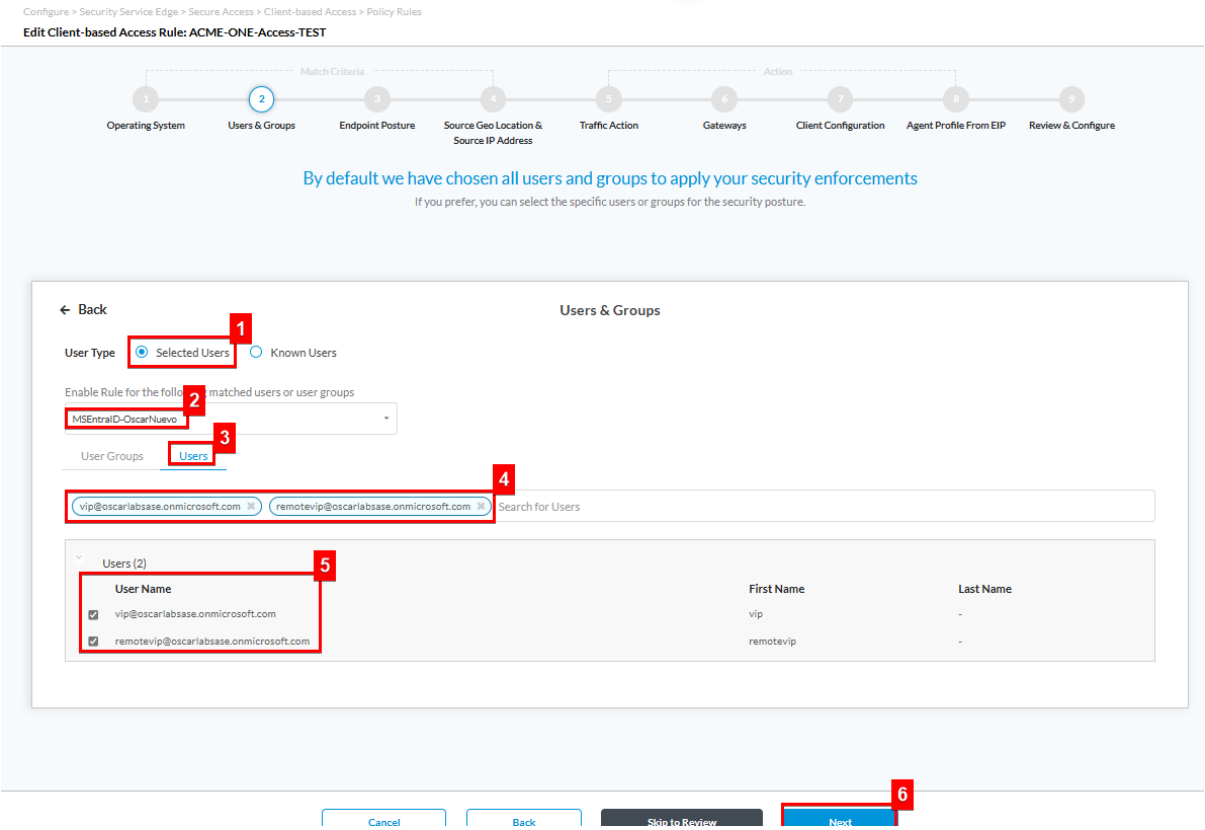
For this use case, select **All Windows** versions and then click ***Next***.



In the users and group section click in ***Customize***.

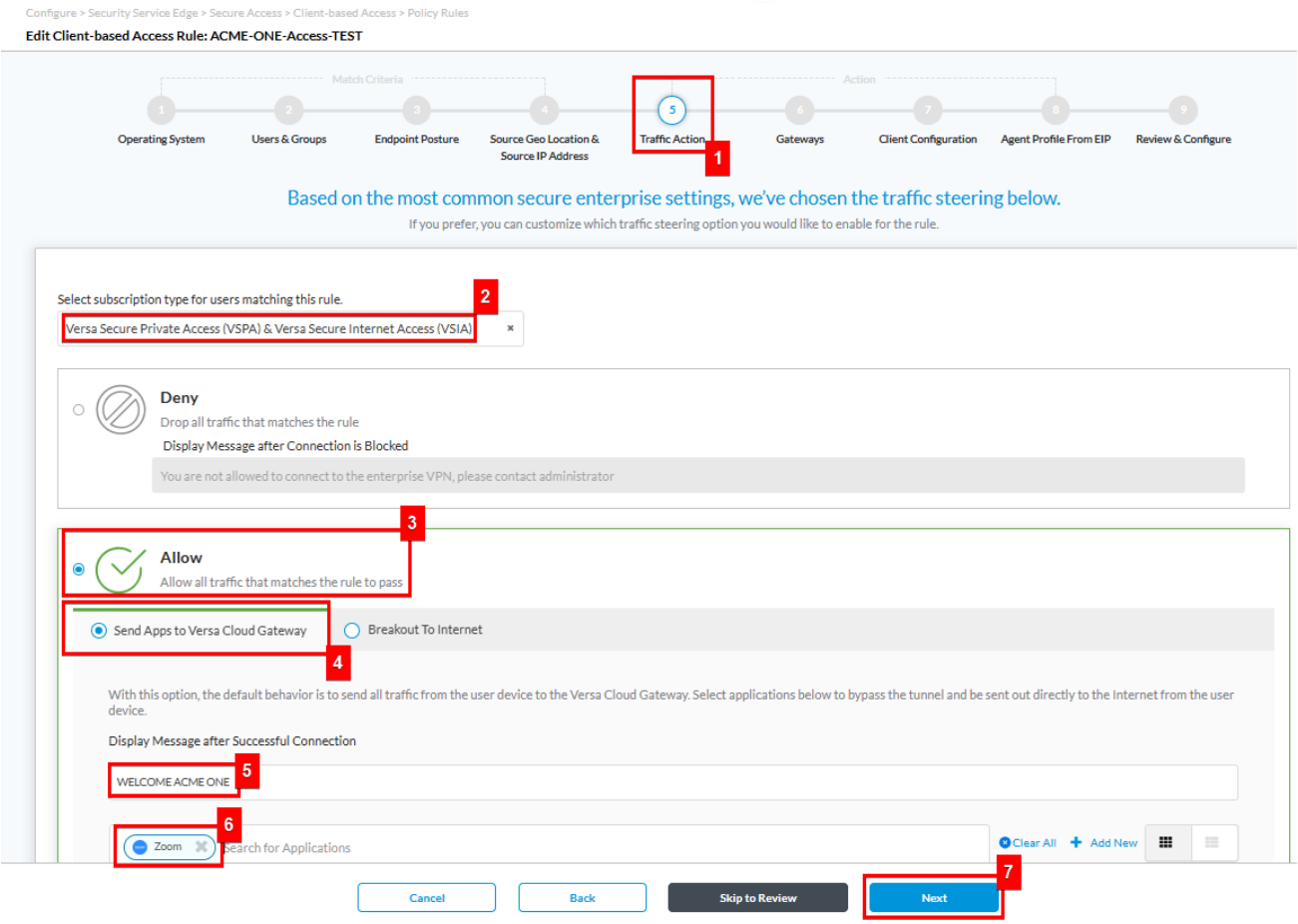


In the users and groups configuration, select the SAML authentication profile created before in step 2, Fill the name of users that need to use these specific applications, and then click Next. In this case, as an example we only used 2 users.

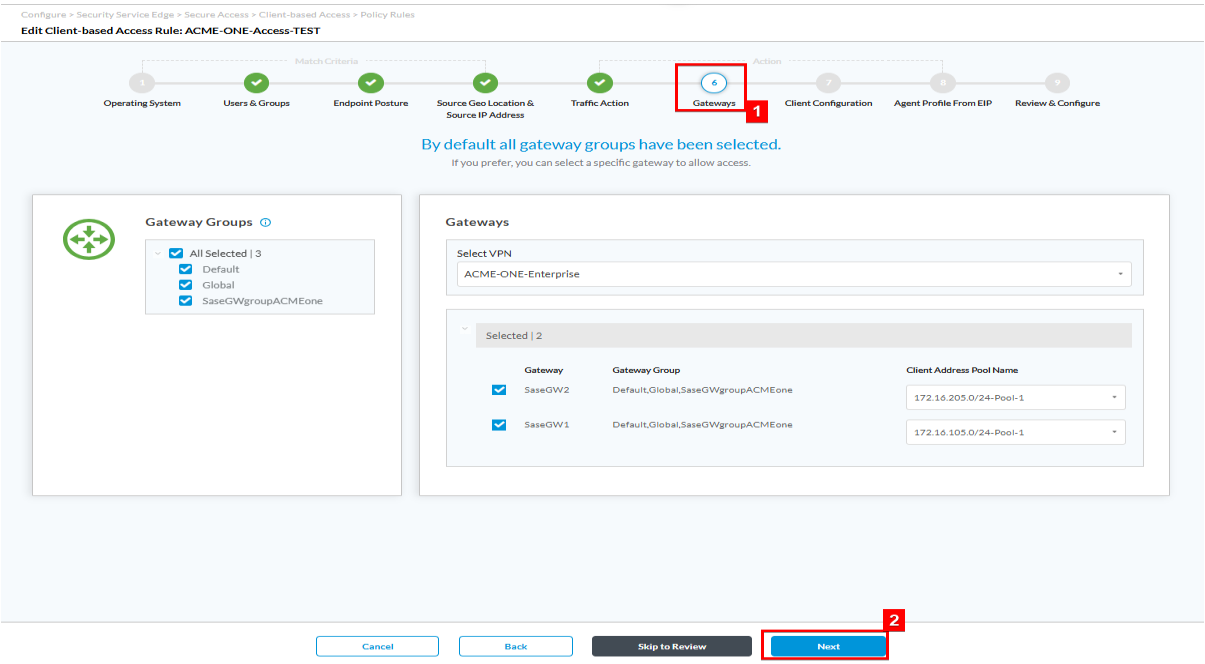


Then click Next until the ***Traffic Action*** section

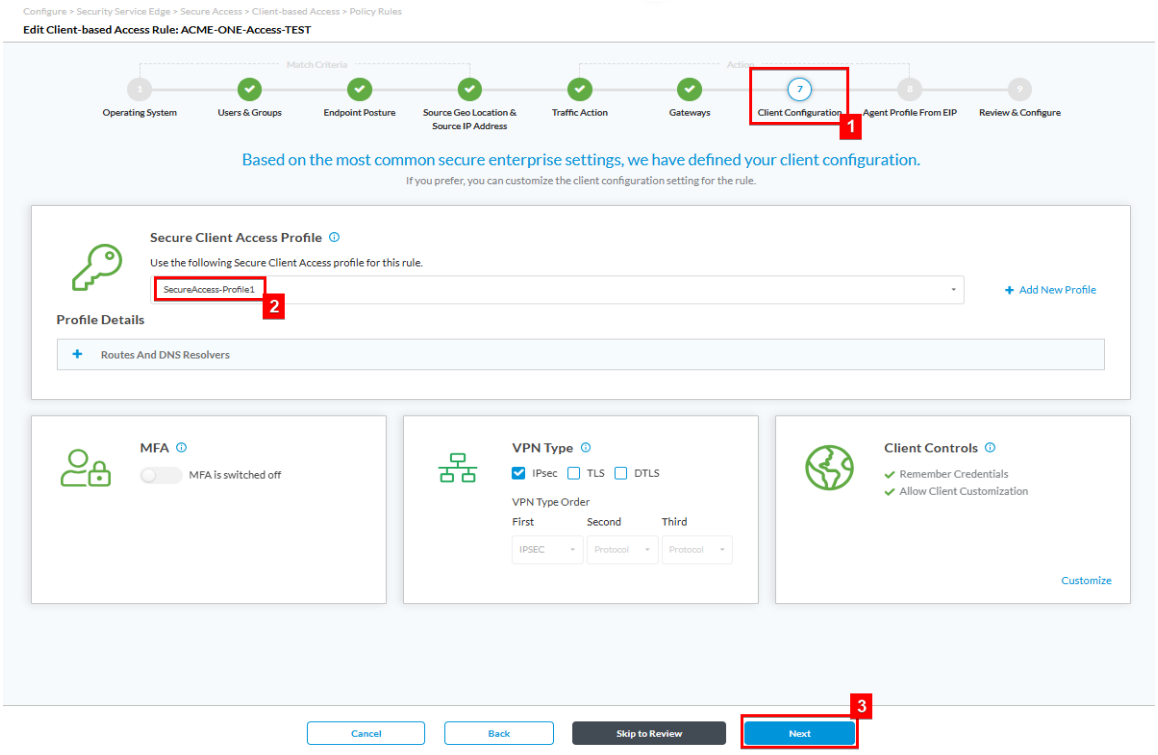
For the traffic action configuration first select the Subscription type corresponding to your License, in this case ***VSPA & VSIA***. Select ***allow***, this action will send the matching traffic to the gateway, but the applications selected in the list bellow will be sent out directly to the internet. In this case ***Zoom.*** Then click ***next***.



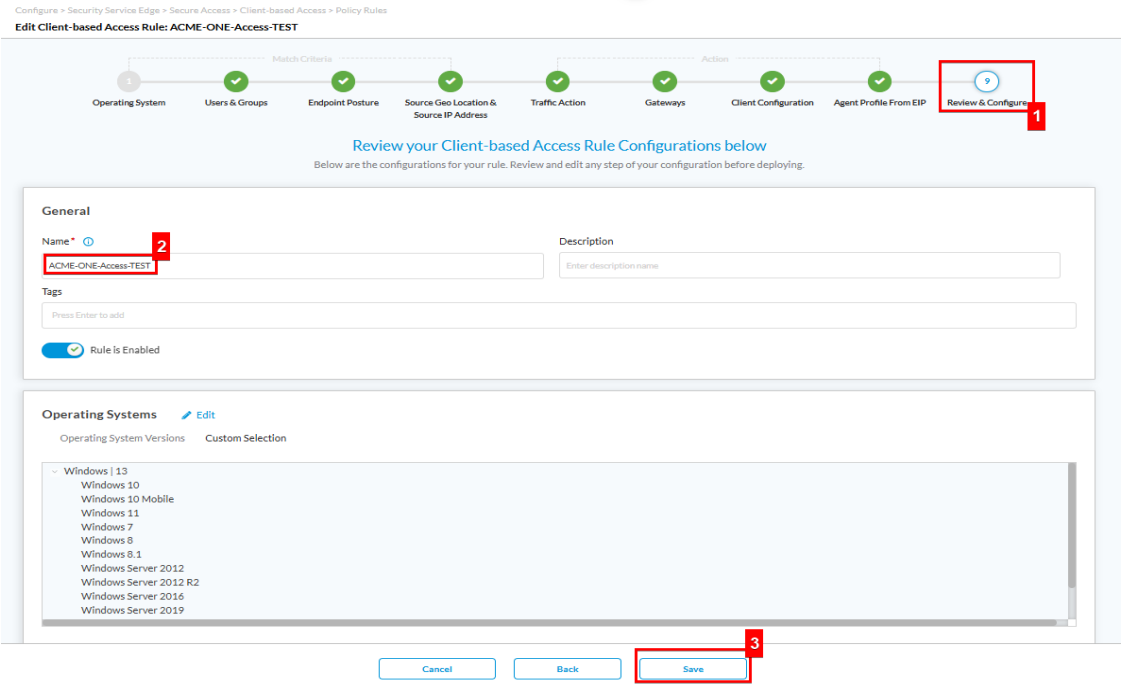
Let the default gateways configuration and click ***next***.



Select the ***Secure Client Access Profile*** to be used with this rule the click ***Next***.



Then click ***Next*** until ***Review & Configuration*** section and assign a descriptive ***Name*** for the Access Rule, if you need to verify you can scroll down and check the configuration. If it's required, you can edit the configuration again. Now click **Save**.



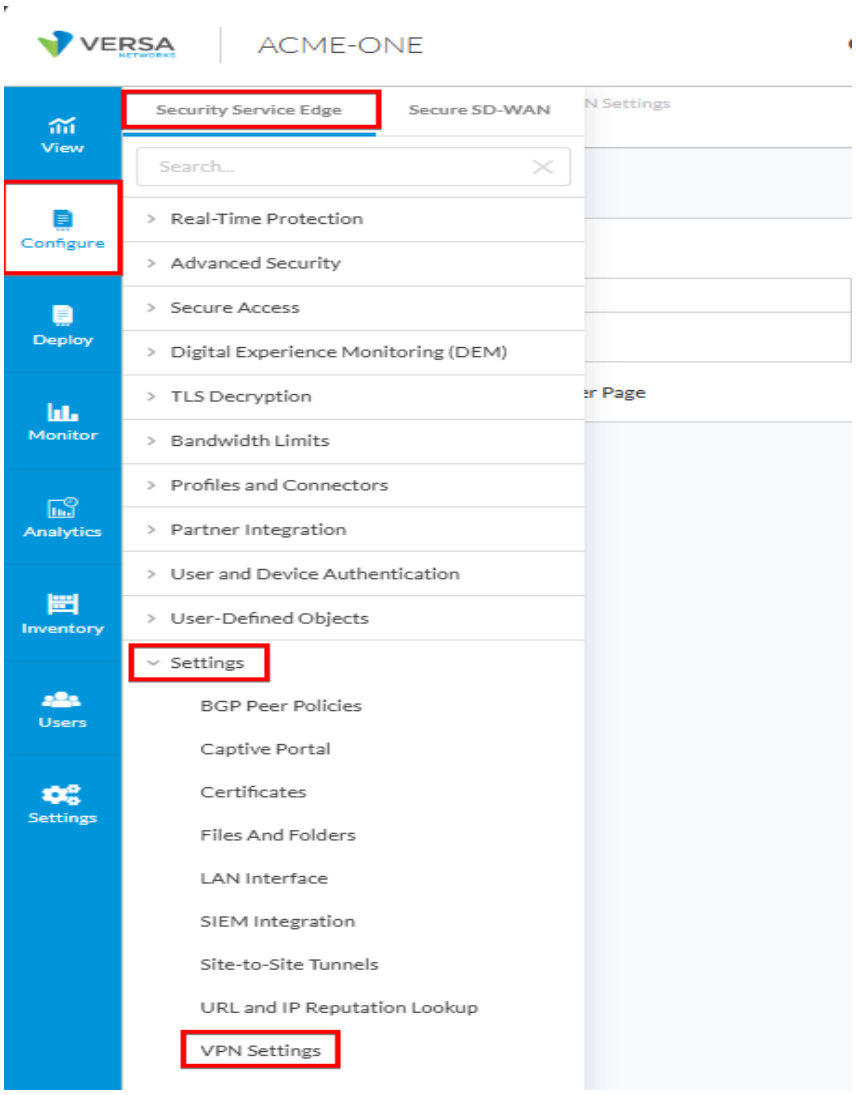
Define the rule to be evaluated first and click Save.

Step 6: Trusted Network Detection: When the user is in the office

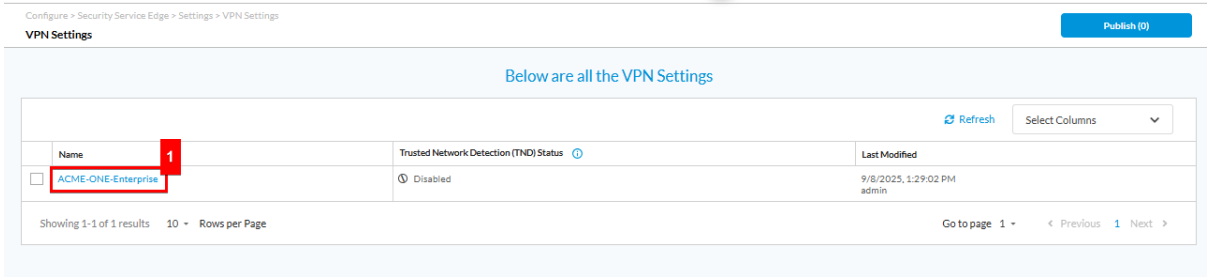
ACME-ONE can use this feature to bypass the SASE gateway when the SASE client is located behind their trusted network/corporate office. In this mode, the secure tunnel to the SASE gateway will not be formed when the SASE client is already behind a trusted network and instead uses the site-to-site connection to the Versa SASE gateways.

When the Versa SASE client initiates registration with the SASE Gateway, the gateway determines whether the client is in a trusted or untrusted network based on the IP address used to connect (private vs. public) and responds accordingly.

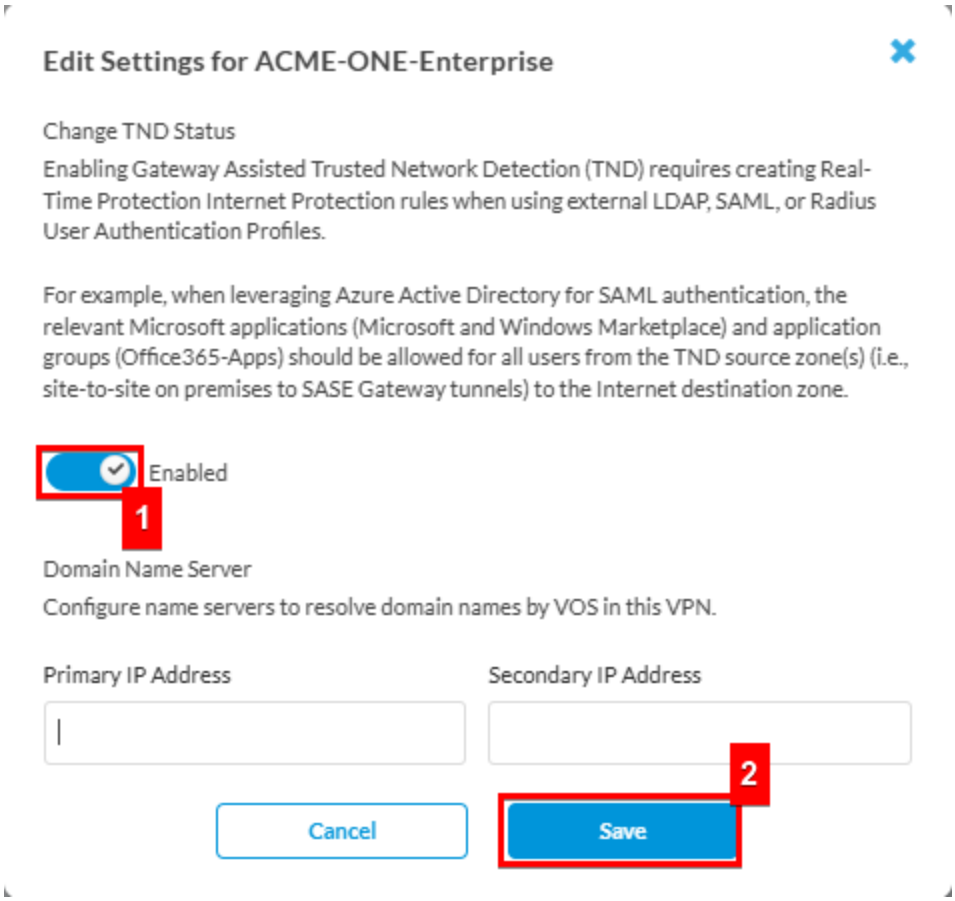
To Configure Trusted Network Detection – Gateway-Assisted, edit the already created VPN in ***Configure*** > ***Security Service Edge*** > ***VPN Settings***.



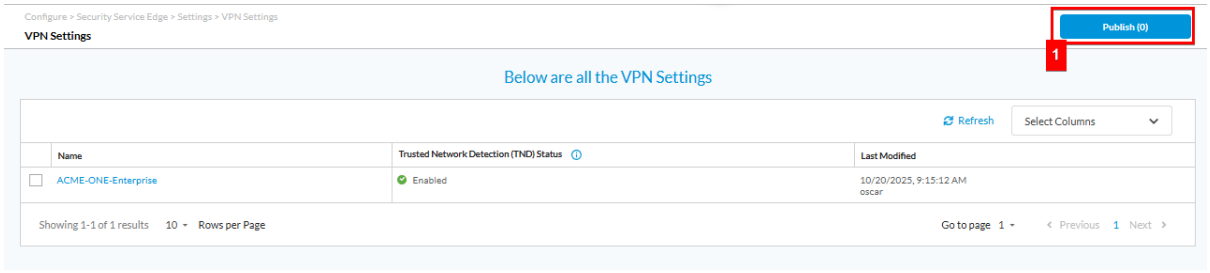
Click on the VPN name to open and edit the settings



Enable the Trusted mode with DNS Configuration. There is no need to add Domain Name Servers as these fields are used to add a DNS server to the SASE Gateways. Then click ***Save***.



Once the above configuration is saved, we need to Publish the configurations so that concerto derives the configuration to the SASE Gateways. The concerto portal ***will not*** request to publish.



Captive portal VR and Interface IP addresses are automatically populated with pre-defined configuration.

Now a DNS entry should be created for the FQDN portal domain to resolve the TNDNOB private ip. In this case,

1

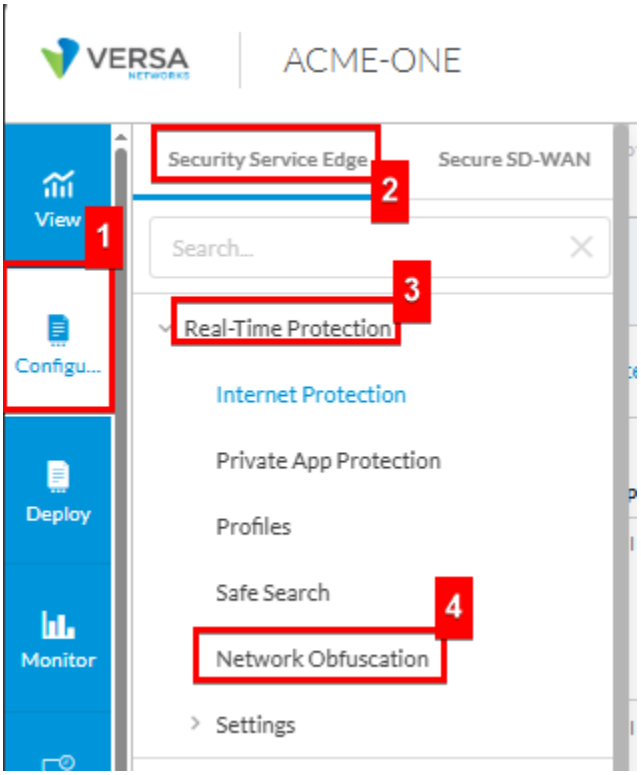
Domain Name	FQDN	IP Address
Portal	acme-one.versanow.net	172.16.105.1
Group	acme-one-sasegwgroupacmeone.versanow.net	172.16.105.1
Gateway	acme-one-sasegw1.versanow.net	172.16.105.1

Step 7: DNS Proxy for Private Domain Resolution

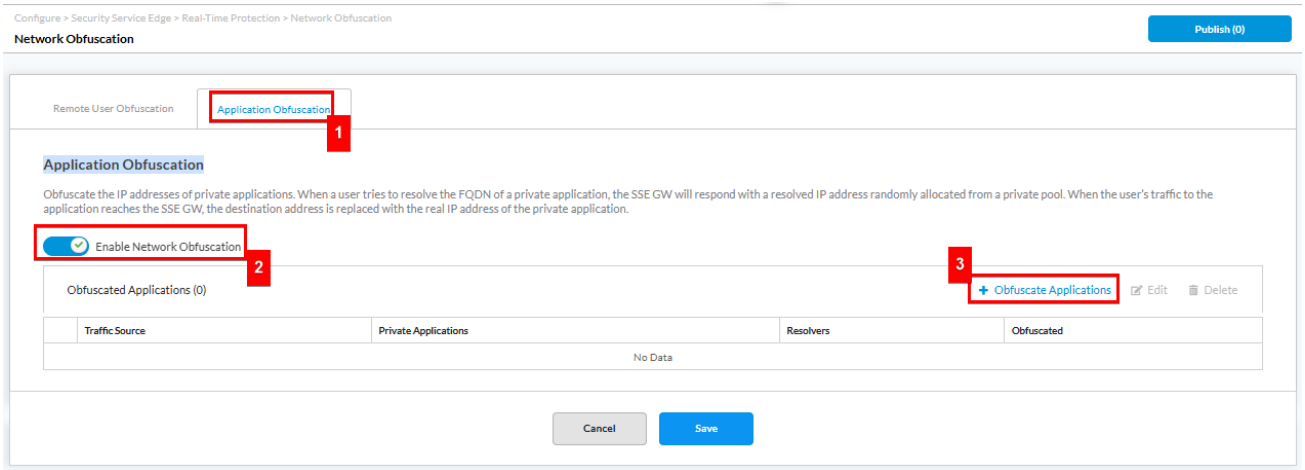
When users are working from home with VSIA+VSPA, client DNS routes point to the SASE Gateways. This organization has internal applications and services that require customized DNS handling. To meet the requirements of this scenario, we need to configure selective DNS requests to be forwarded through a DNS proxy to the corporate DNS. All other external DNS queries, such as those for websites or cloud services, can be sent to the global DNS server for standard resolution.

This example explains how to configure a DNS proxy with network obfuscation for Versa SASE client.

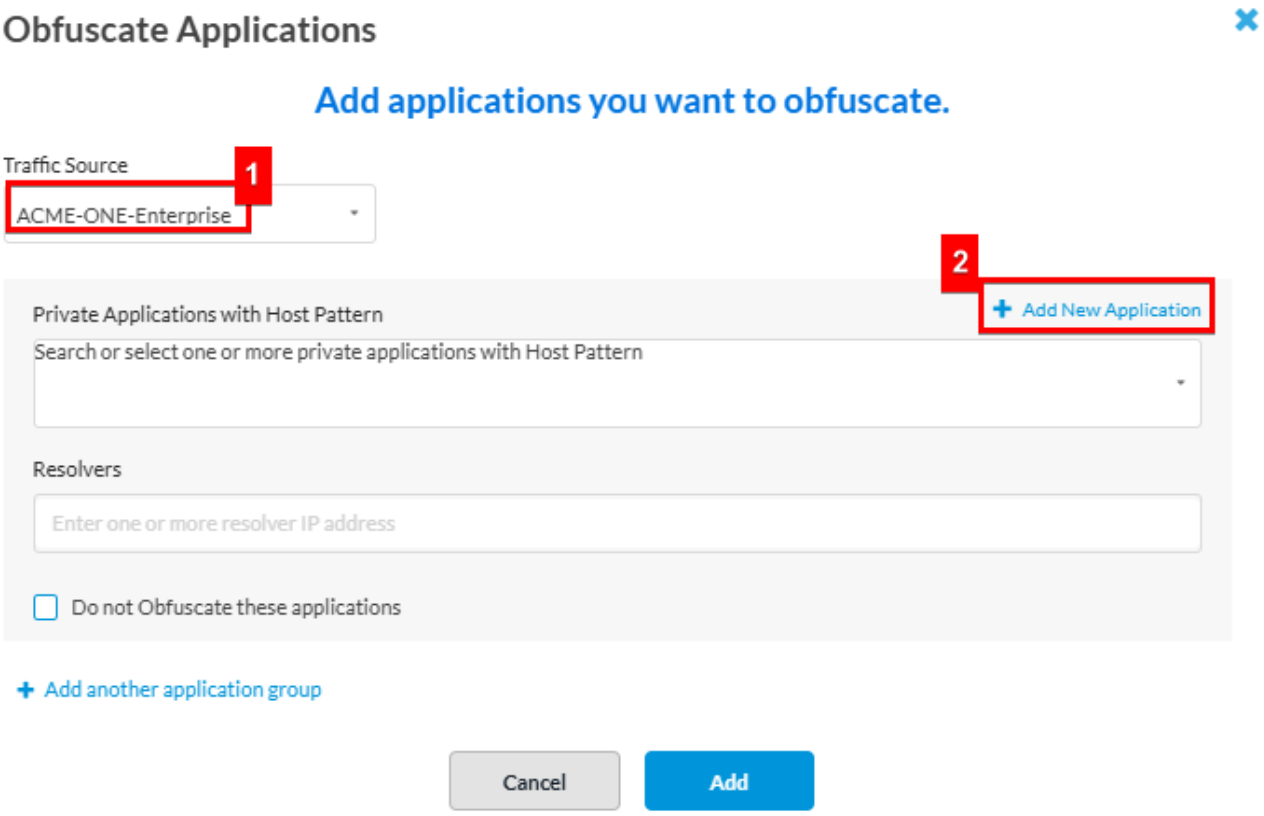
Go to ***Configure*** > ***Security Service Edge*** > ***Real-Time Protection*** > ***Network Obfuscation***.



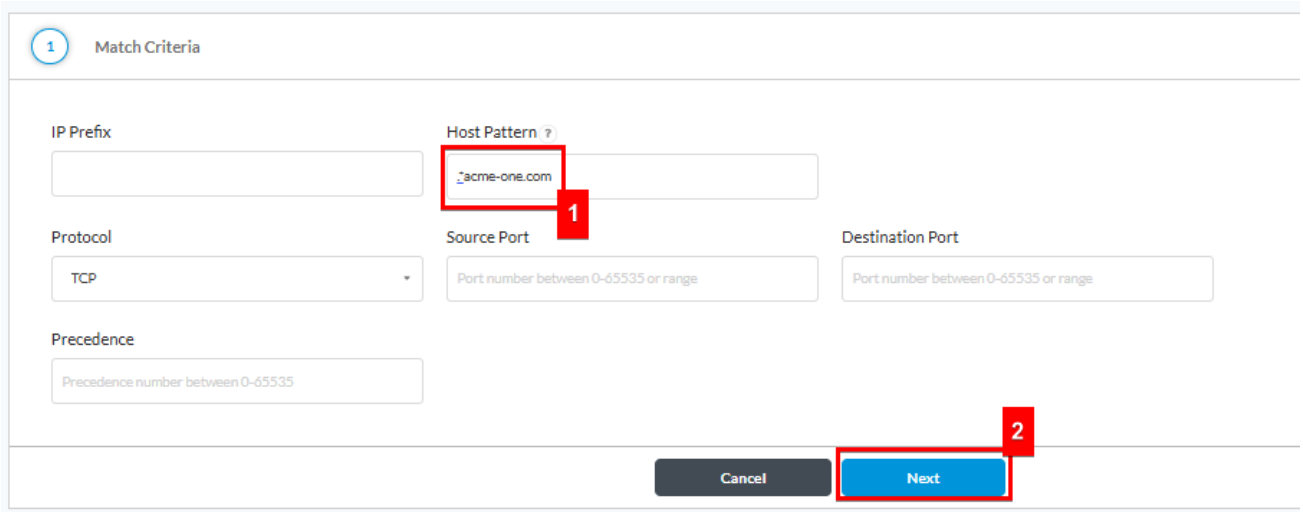
Go to ***Application Obfuscation*** tab and then slide the toggle to Enabled. Then click ***+ Obfuscation Applications***.



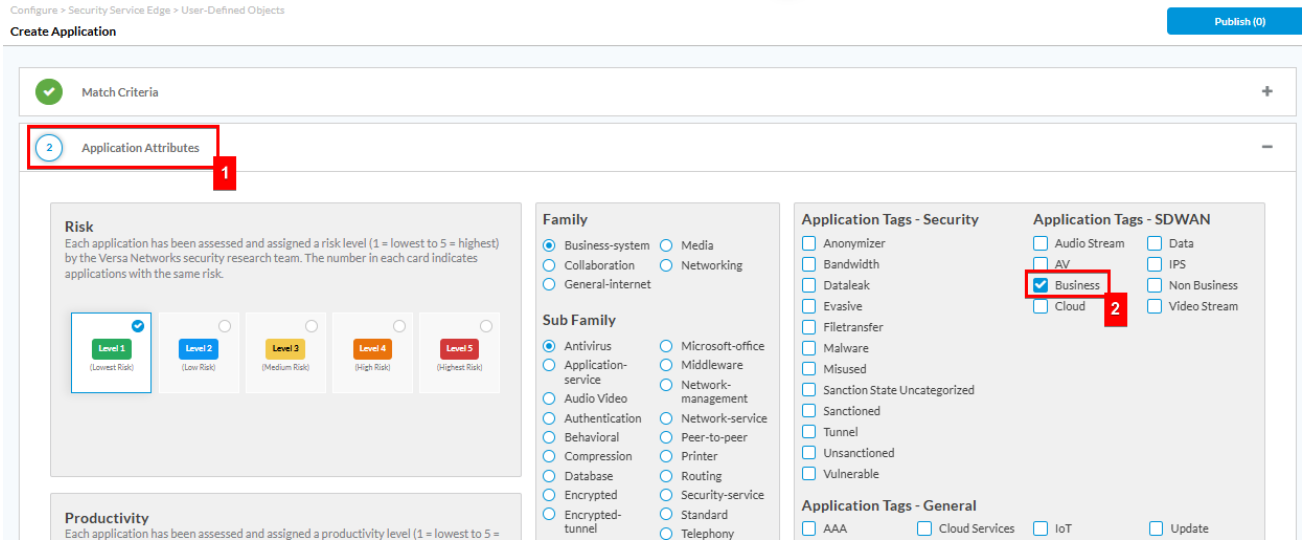
In the Obfuscate Applications screen, make sure the tenant is selected and enter a regex pattern for customer private domains/app in ***+Add New Application***.



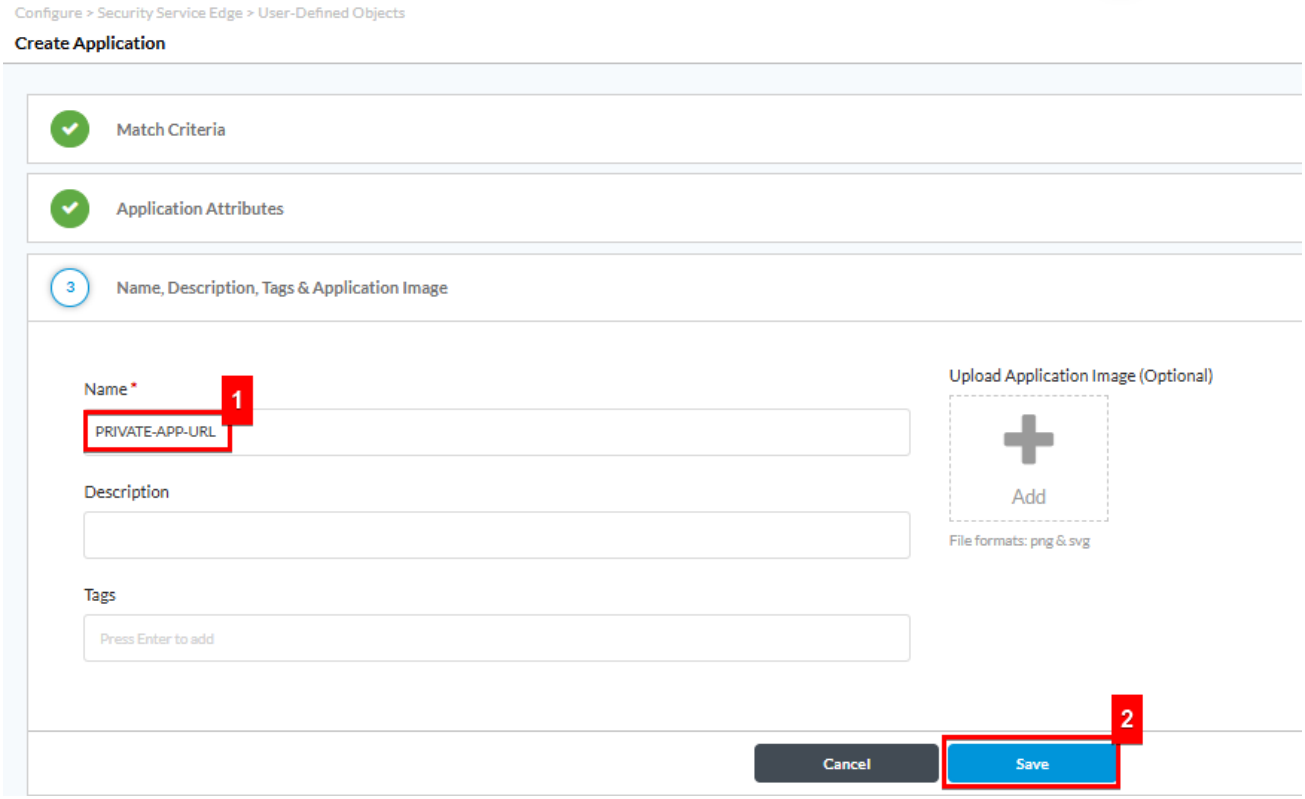
We will add the pattern of the private domain ***.*acme-one.com*** and then click ***Next***.



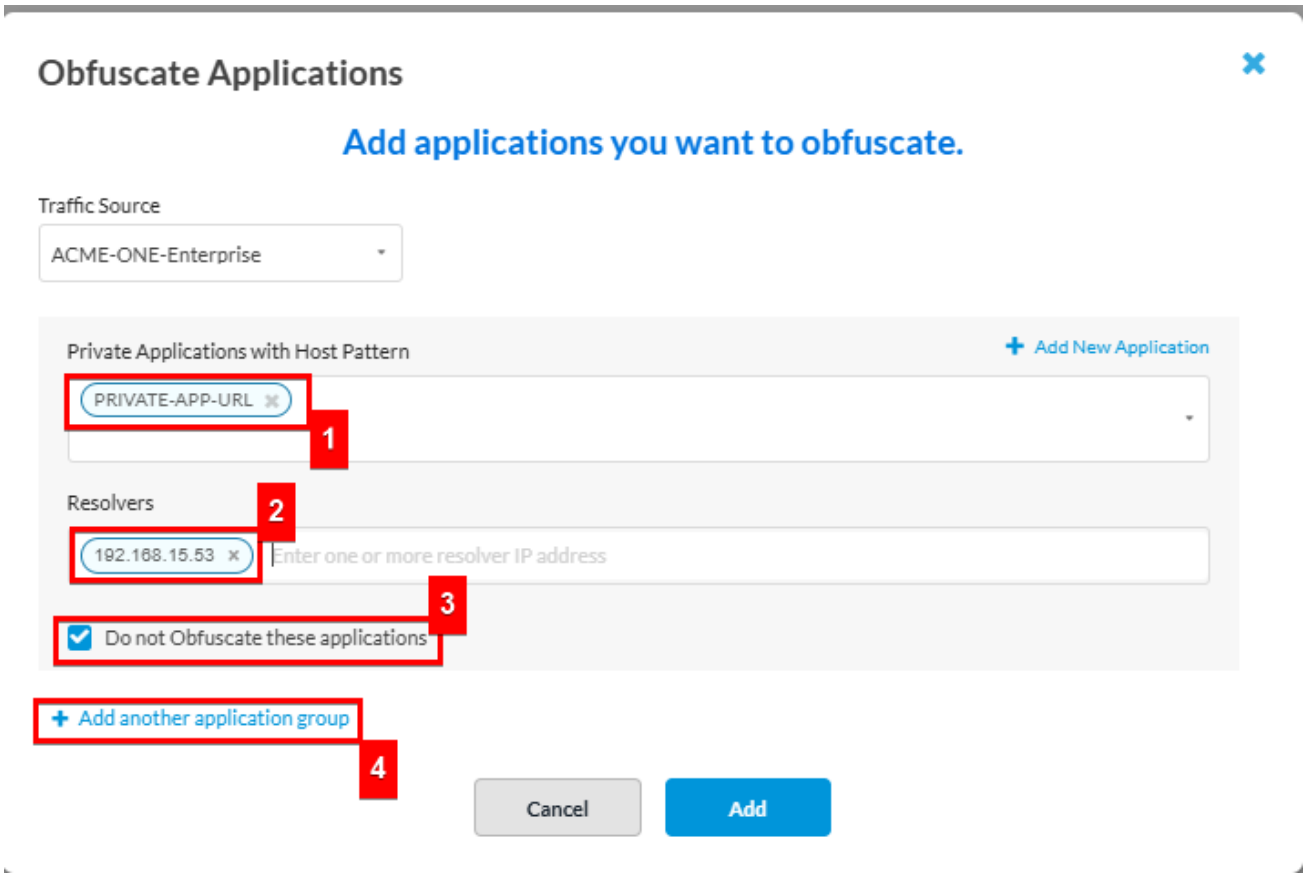
In ***Application Attributes*** a tag is necessary, we used Business and click ***Next***.



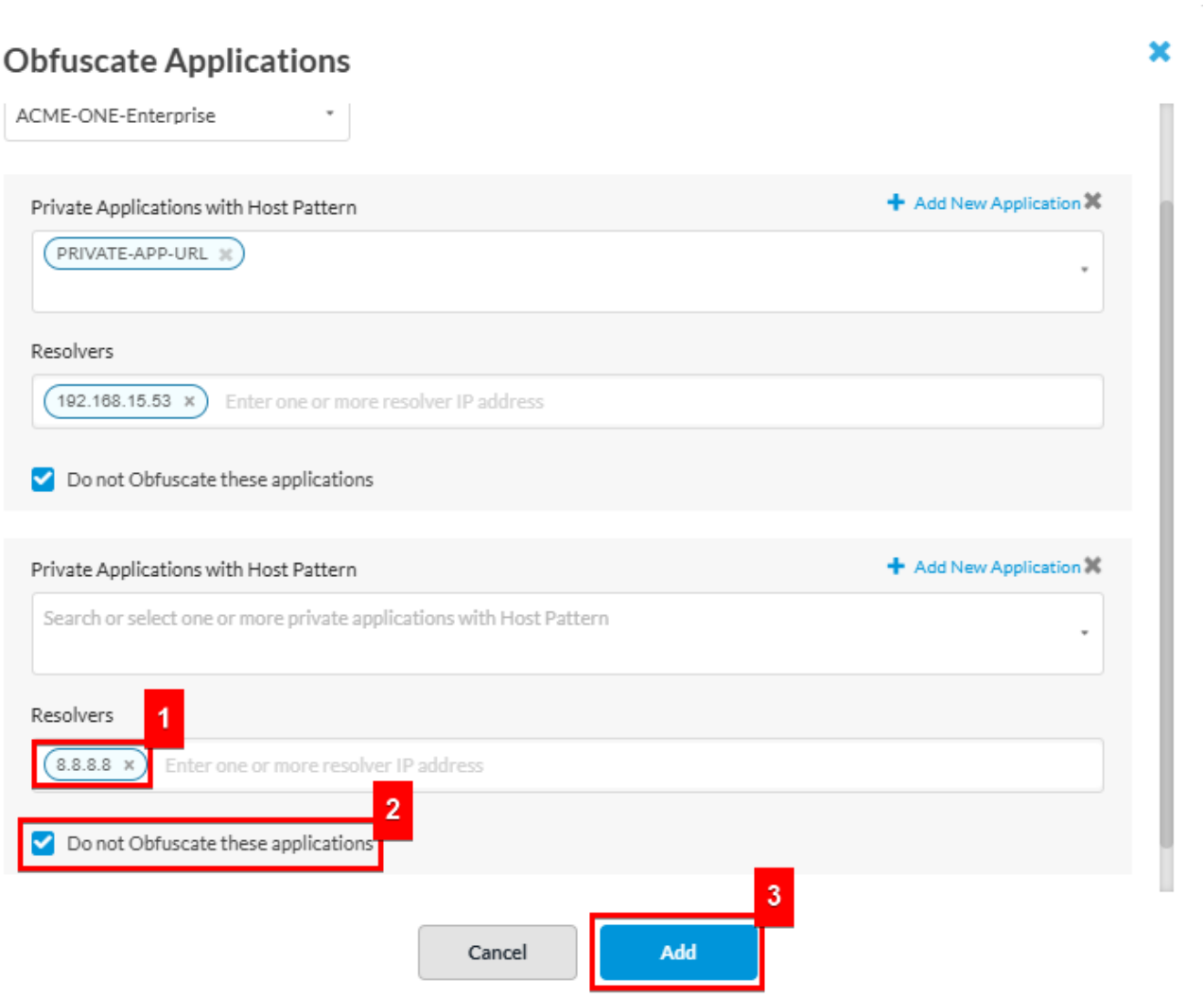
Define the ***Name*** for the added application domains/URL.



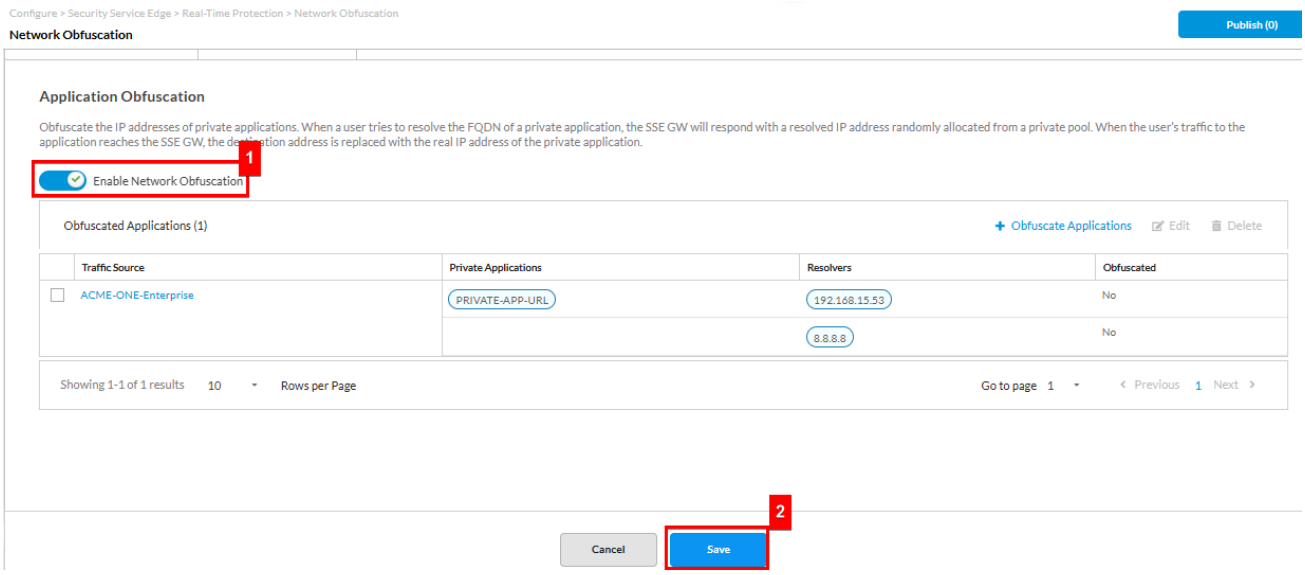
Select the created Application. The resolver would be the internal DNS server that can resolve private domains. Set “Do not obfuscate’ and “add another application group”



Do not define any application, so the rest of the domains are matched, and DNS resolver is defined as the public DNS. Then click ***Add***.



Now set Enable Network Obfuscation and click Save



Step 8: Enforce TLS Policies: Do-Not-Decrypt for Health/Finance | Decrypt the rest.

In this scenario to maintain user privacy and comply with regulations:

- Financial services and healthcare-related websites should be explicitly excluded from decryption.
- All other traffic will be decrypted, allowing sensitive flows to be inspected and protected by Versa's security stack.

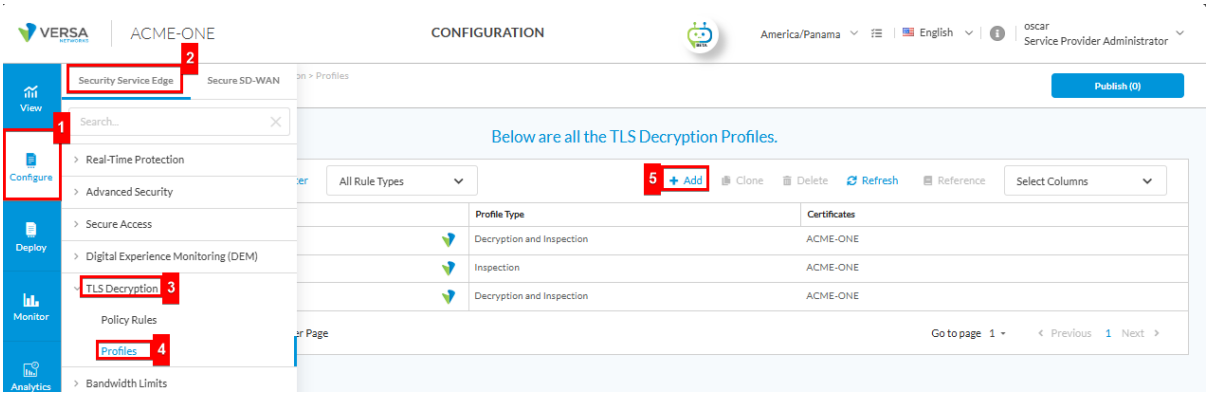
The required information to complete the configuration is in the next list.

Parameter	**Description**
Profiles Name	Name for Decryption Profiles
Certificate	Certificate to be used for TLS Decryption
Key Exchange Algorithms	Key Exchange Algorithms allowed to be used for TLS
Encryption Algorithms	Encryption Algorithms allowed to be used for TLS
Authentication Algorithms	Authentication Algorithms allowed to be used for TLS
TLS Cipher Suites	TLS Cipher Suites allowed to be used for TLS

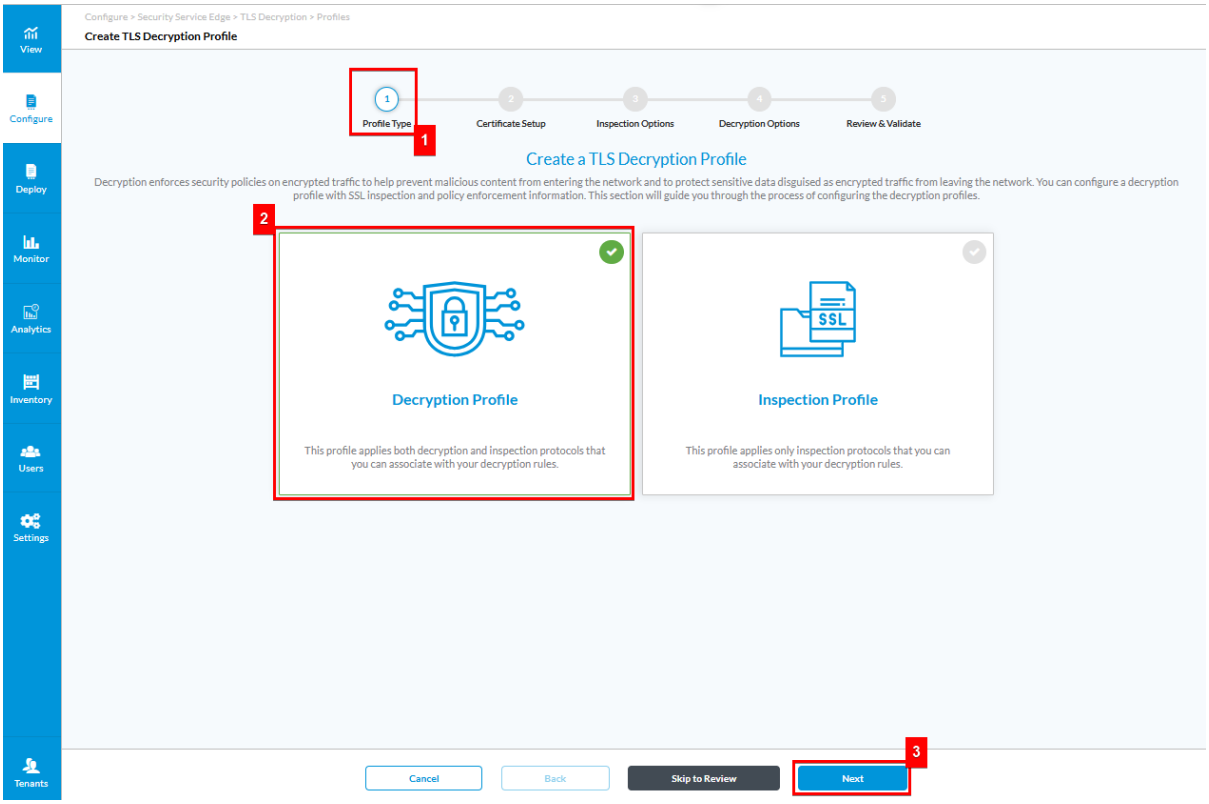
Versa includes some predefined profiles you can use, but if some specific/custom profile is required, please follow the steps listed below to create a new one.

To meet the requirements on this scenario we will need to configure

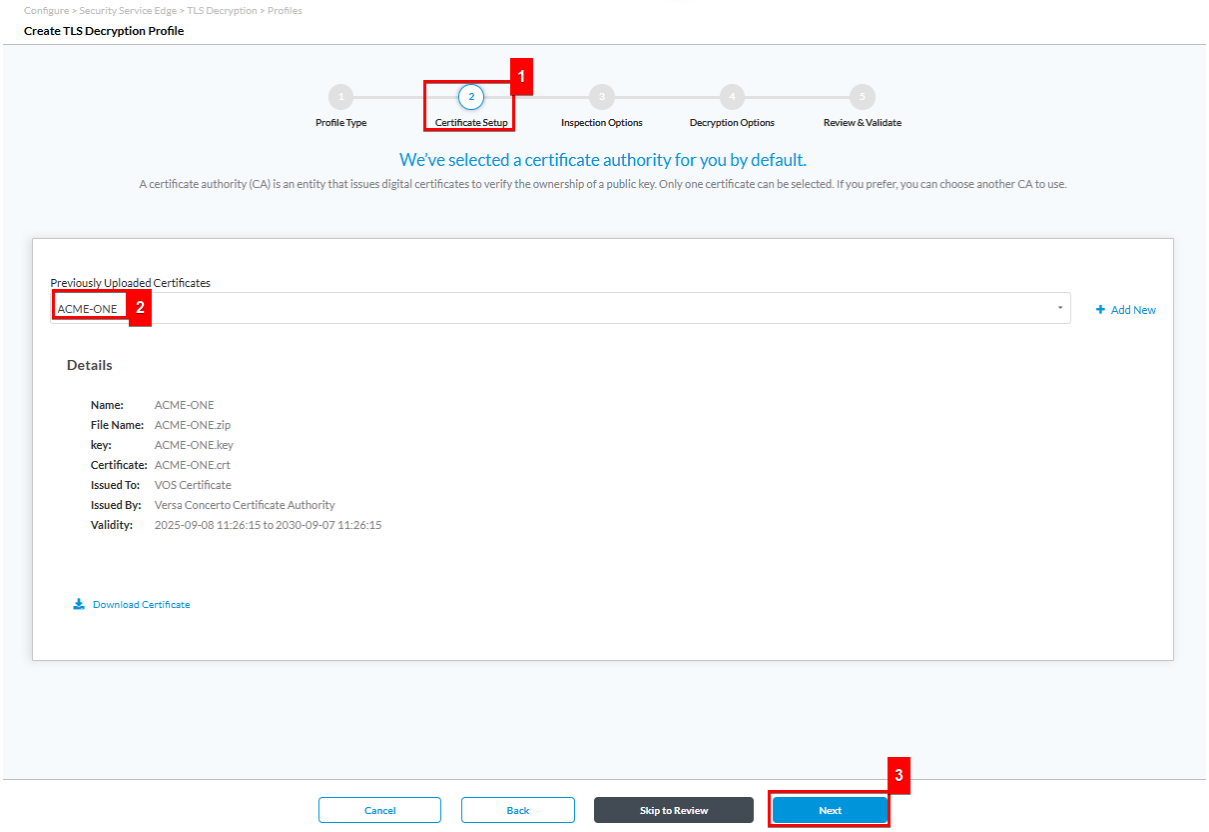
Configure TLS decryption, first create a decryption profile in ***Configure*** > ***Security Service Edge*** > ***TLS Decryption*** > ***Profiles*** > ***+Add***.



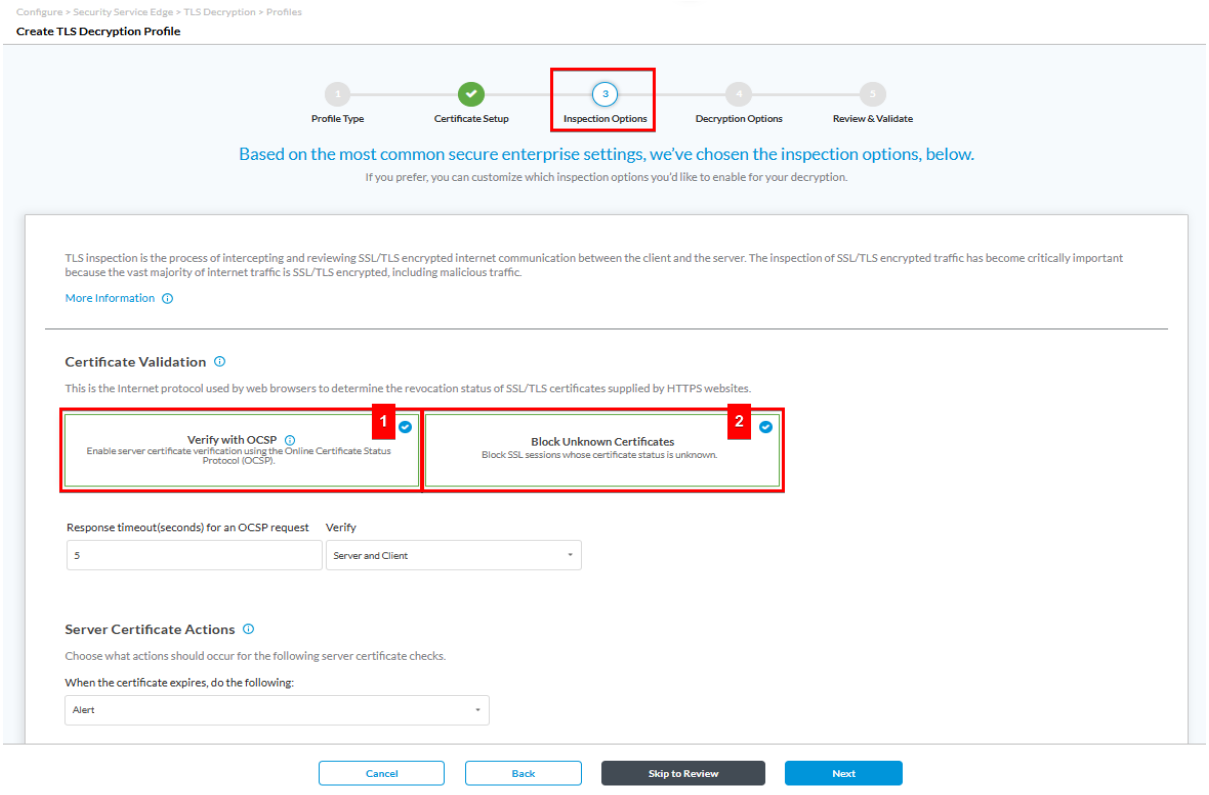
For this case choose ***Decryption Profile***



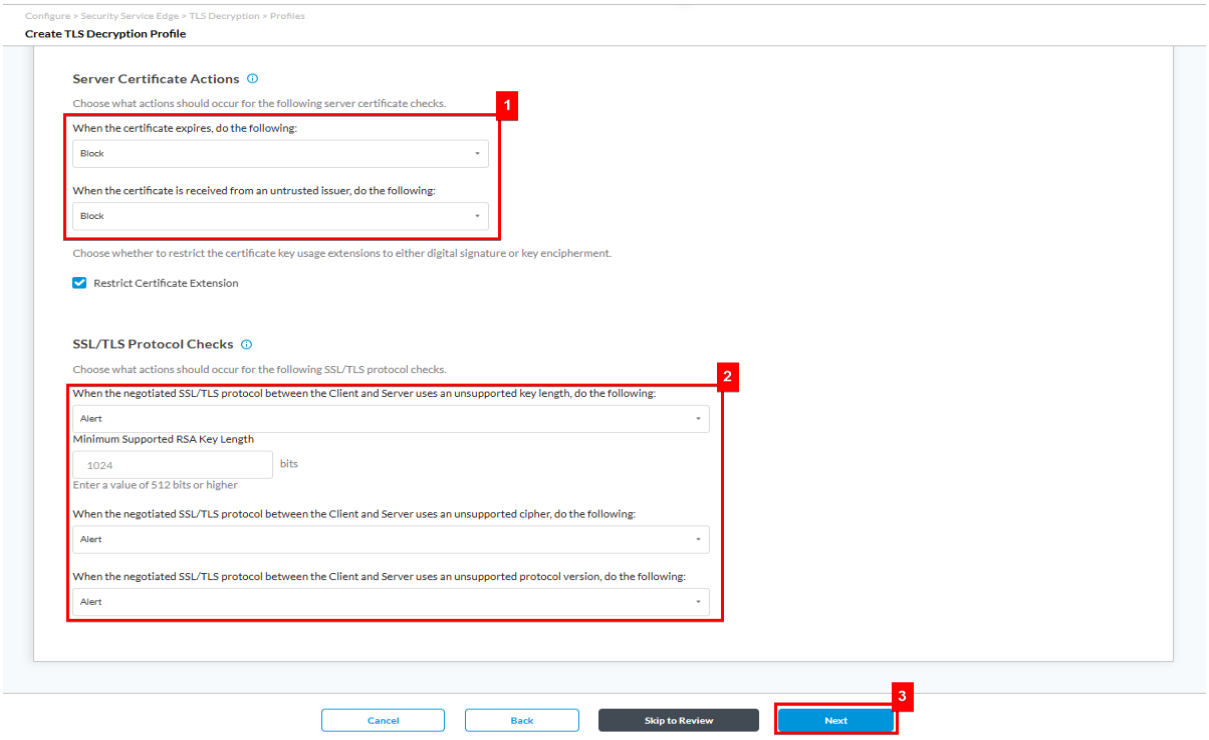
Choose the ***Certificate***, then click ***Next***.



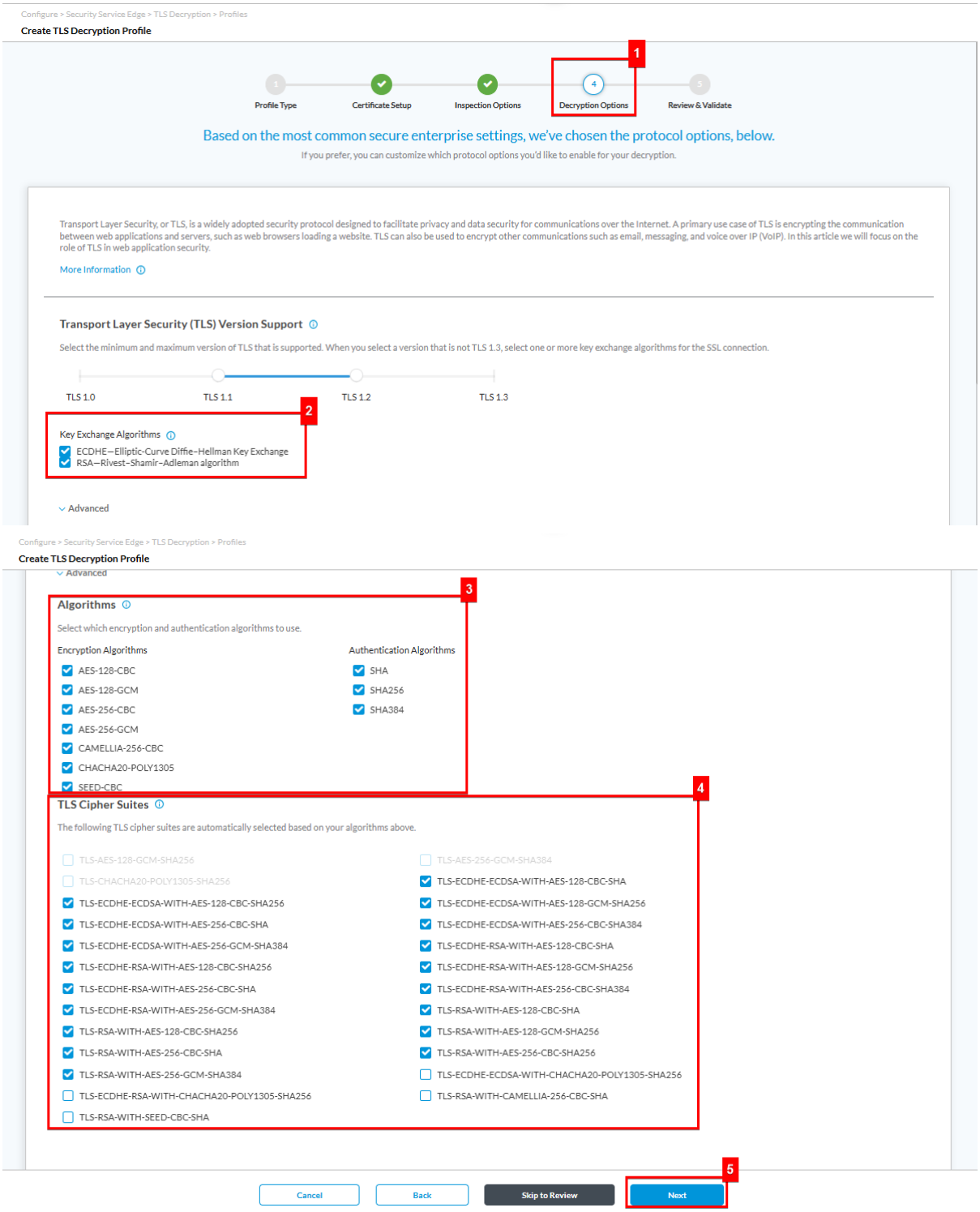
Enable OSCP Verification and blocking Unknown Certificates, now scroll down.



Block Expired and Unknown Certificates and Alert Unsupported Key Lengths, Unsupported Cipher and Unsupported Protocol Version. Then click Next.

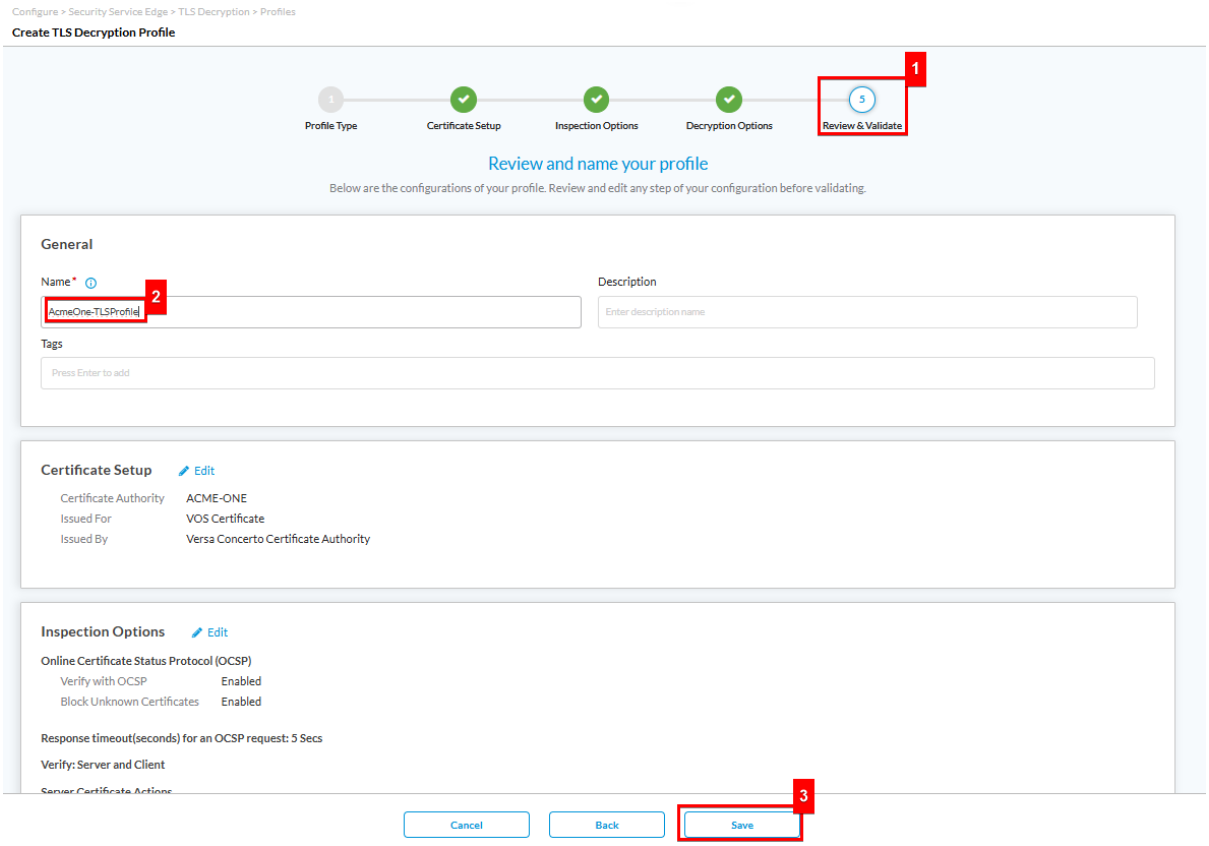


Select Key Exchange Algorithms, choose Encryption and Authentication Algorithms, now scroll down.

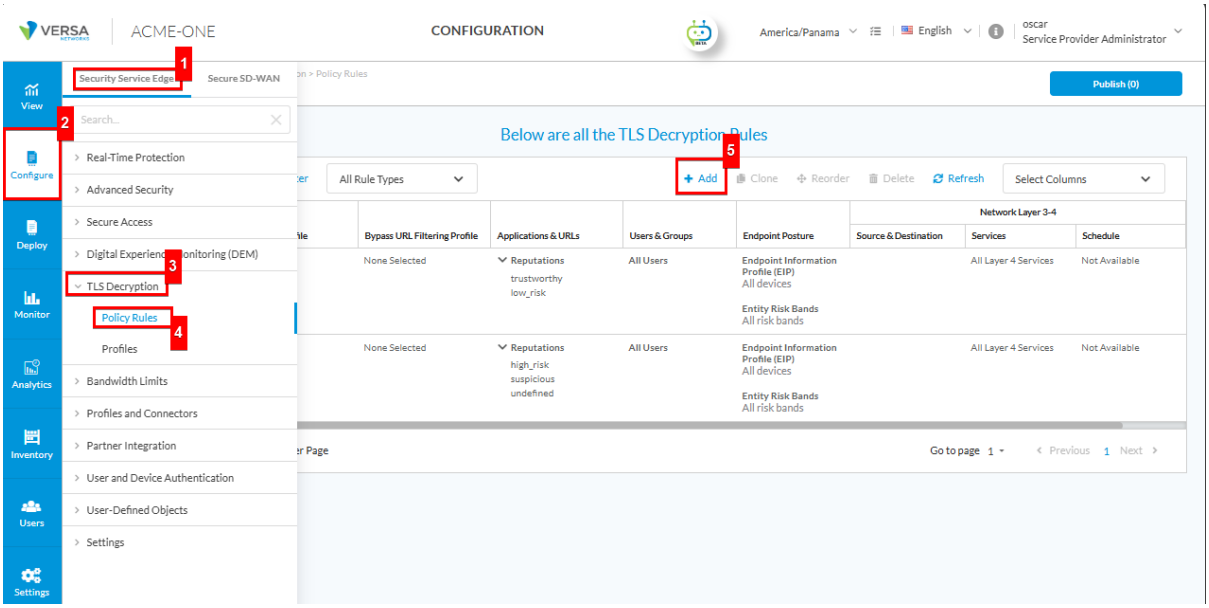

Configure > Security Service Edge > TLS Decryption > Profiles
Create TLS Decryption Profile
1
Profile Type
Certificate Setup
Inspection Options
4
Decryption Options
5
Review & Validate
Based on the most common secure enterprise settings, we've chosen the protocol options, below.
If you prefer, you can customize which protocol options you'd like to enable for your decryption.
Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.
More Information
Transport Layer Security (TLS) Version Support
Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.
TLS 1.0
TLS 1.1
TLS 1.2
TLS 1.3
2
Key Exchange Algorithms
ECDHE—Elliptic-Curve Diffie–Hellman Key Exchange
RSA—Rivest–Shamir–Adleman algorithm
Advanced

Configure > Security Service Edge > TLS Decryption > Profiles
Create TLS Decryption Profile
Advanced
3
Algorithms
Select which encryption and authentication algorithms to use.
Encryption Algorithms
AES-128-CBC
AES-128-GCM
AES-256-CBC
AES-256-GCM
CAMELLIA-256-CBC
CHACHA20-POLY1305
SEED-CBC
Authentication Algorithms
SHA
SHA256
SHA384
4
TLS Cipher Suites
The following TLS cipher suites are automatically selected based on your algorithms above.
TLS-AES-128-GCM-SHA256
TLS-CHACHA20-POLY1305-SHA256
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
TLS-RSA-WITH-AES-128-CBC-SHA256
TLS-RSA-WITH-AES-256-CBC-SHA
TLS-RSA-WITH-AES-256-GCM-SHA384
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
TLS-RSA-WITH-SEED-CBC-SHA
TLS-AES-256-GCM-SHA384
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384
TLS-RSA-WITH-AES-128-CBC-SHA
TLS-RSA-WITH-AES-128-GCM-SHA256
TLS-RSA-WITH-AES-256-CBC-SHA256
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA
5
Cancel
Back
Skip to Review
Next

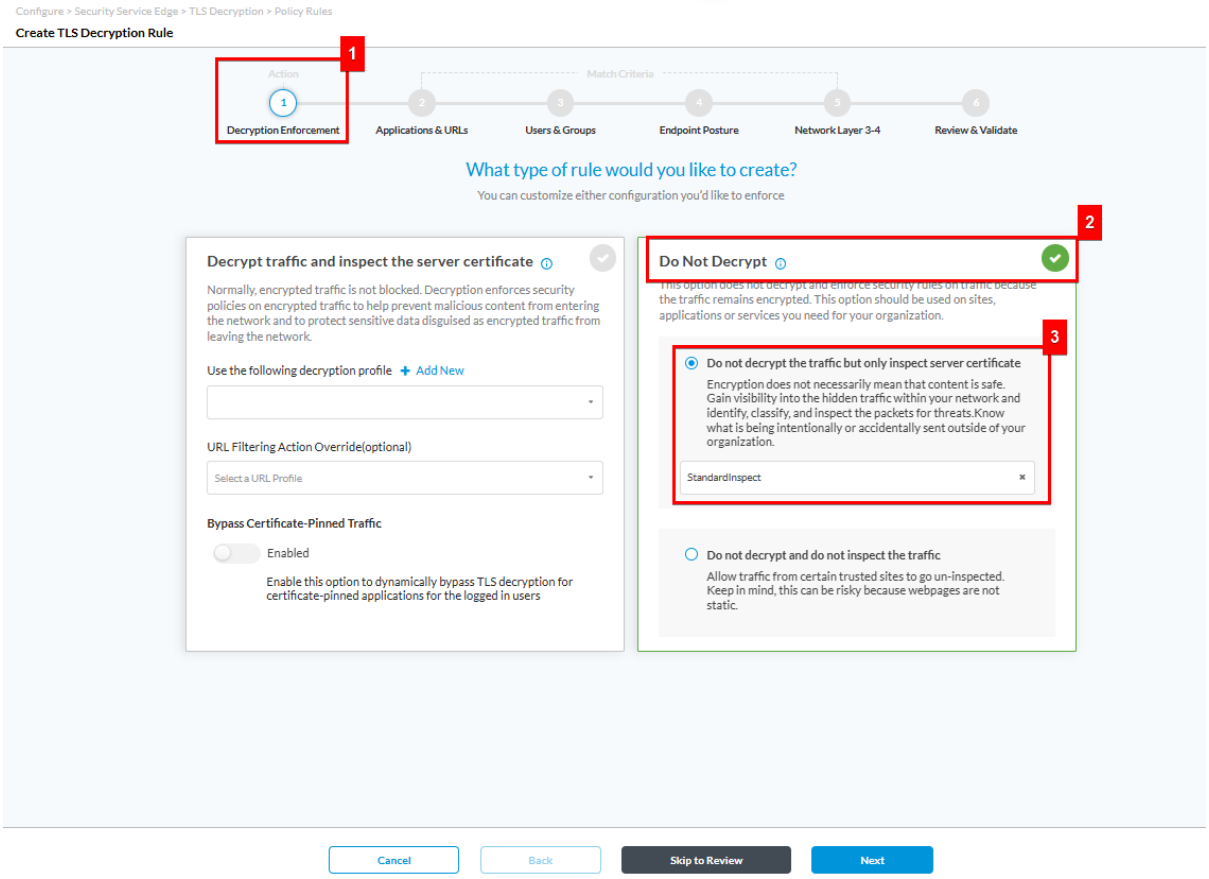
Assign a descriptive ***Name*** then click ***Save***.



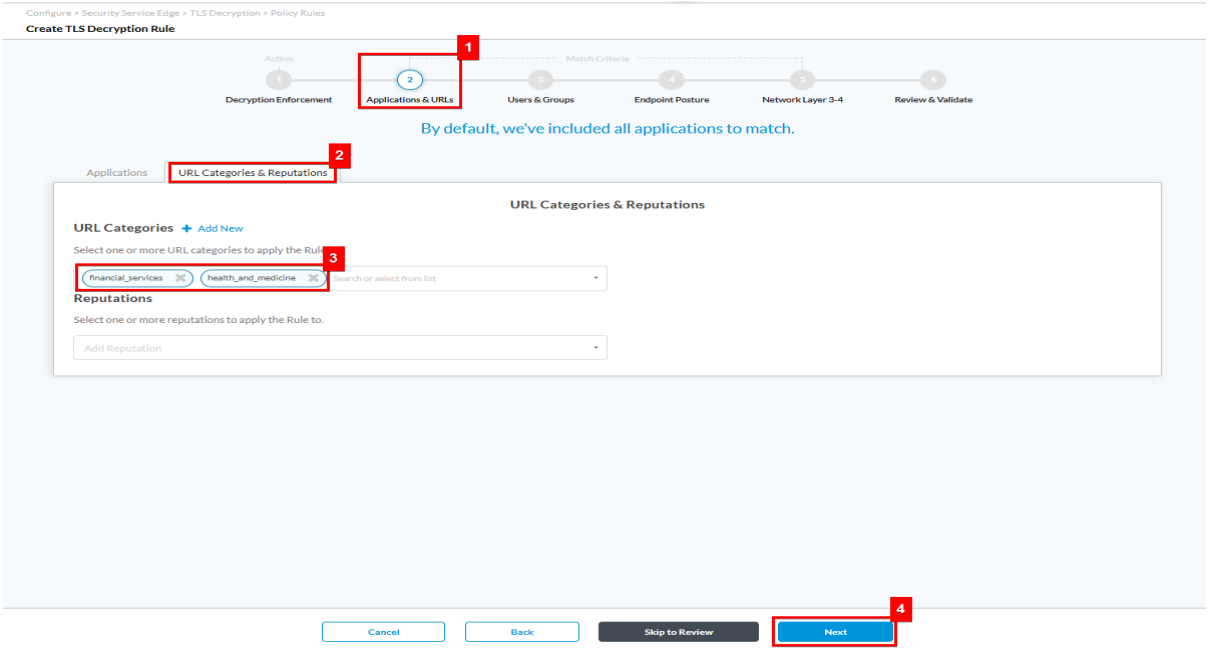
Now, to create the 2nd rule to avoid Health and Financial URLs to be decrypted, go to ***Configure*** > ***Security Service Edge*** > ***TLS Decryption***_> ***Policy Rules***, Then Click ***Add*** to create a new TLS Decryption Policy Rule.



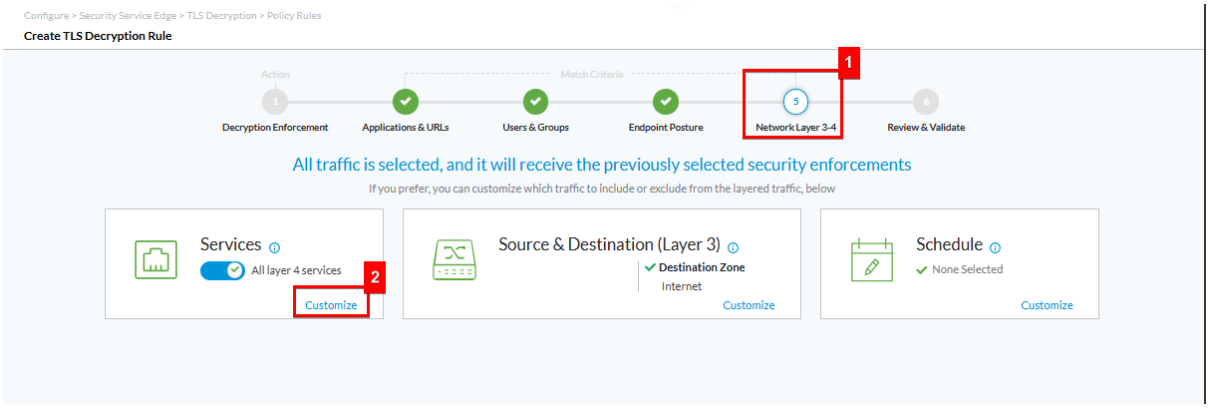
Select ***Do Not Decrypt*** Option and the option to Inspect Certificates with the ***Standard Inspect*** Profile, Then Click ***Next***.



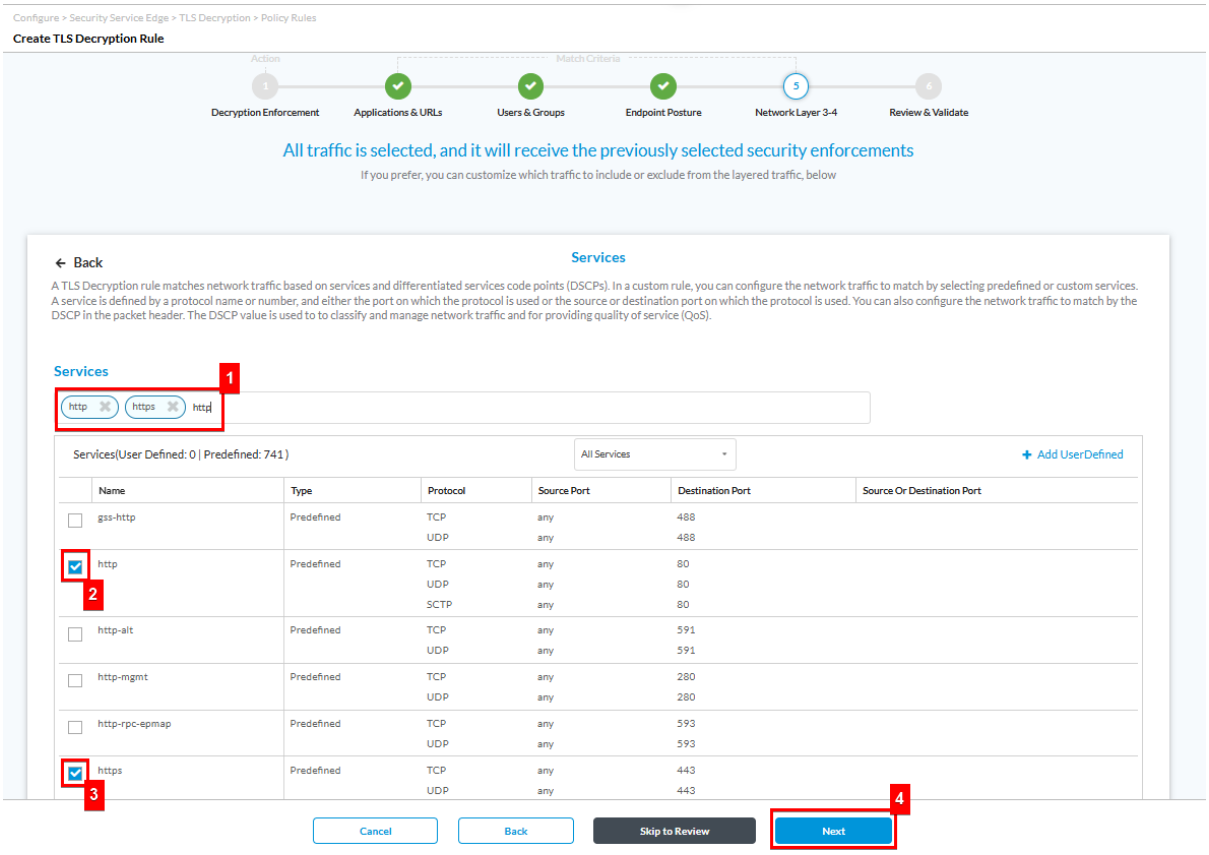
From ***URLs Categories and Reputations***, search for ***financial_services*** and ***health_and_medicine*** categories, then Click ***Next***.



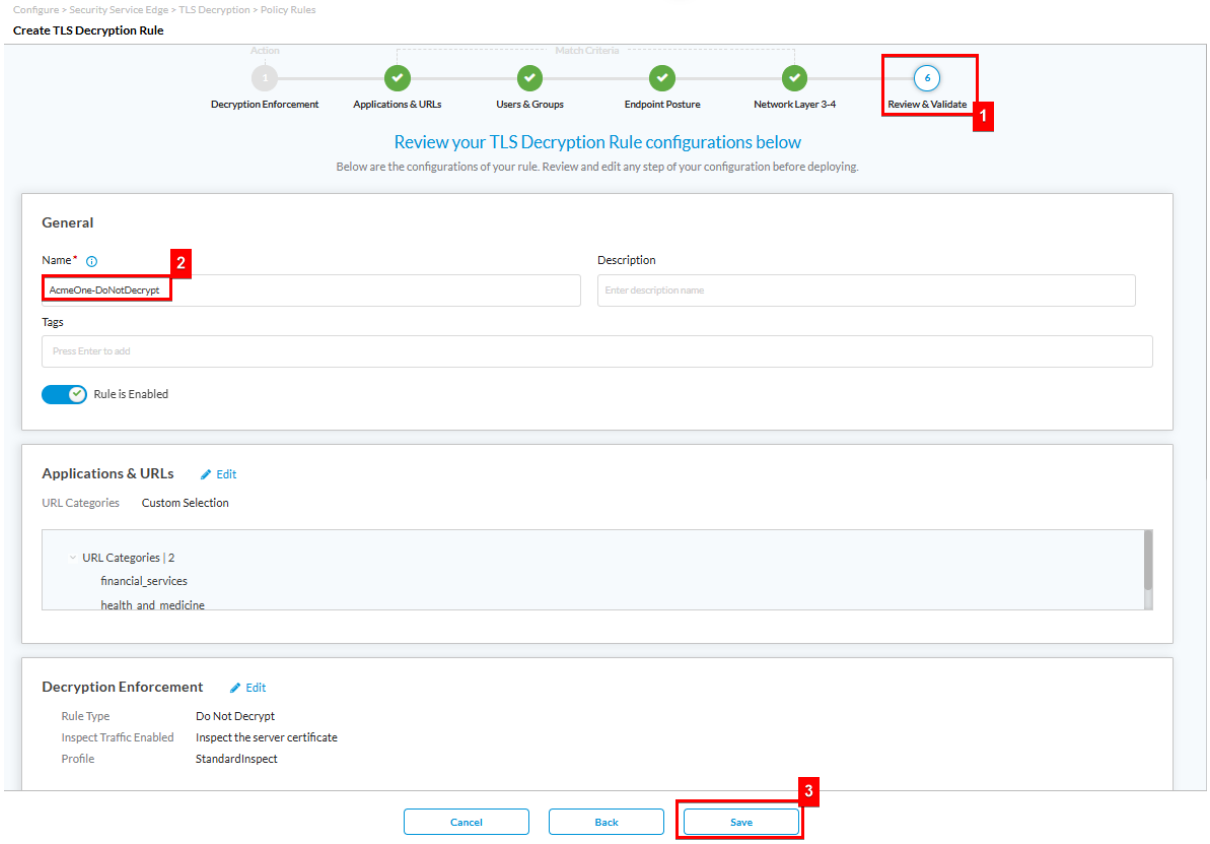
Click ***Next*** in ***Users & Groups*** and in ***Endpoint Posture***, until you reach ***Network Layer 3-4***. Click on ***Customize*** in section ***Services***.

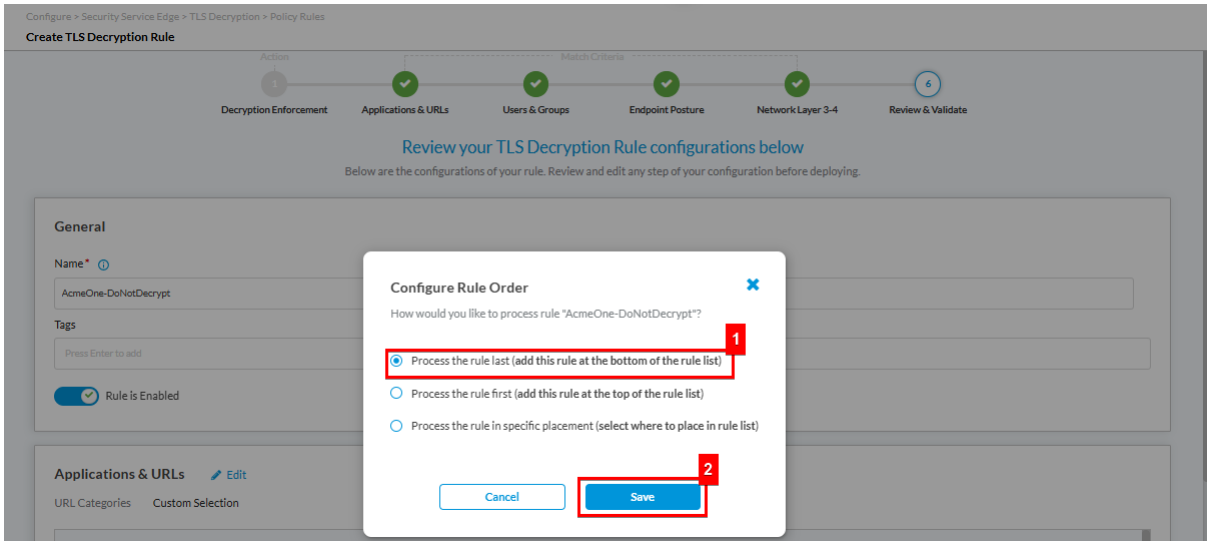


Look for http and add services ***http*** and ***https*** to avoid resources consumption looking for other services. Then Click ***Next***.

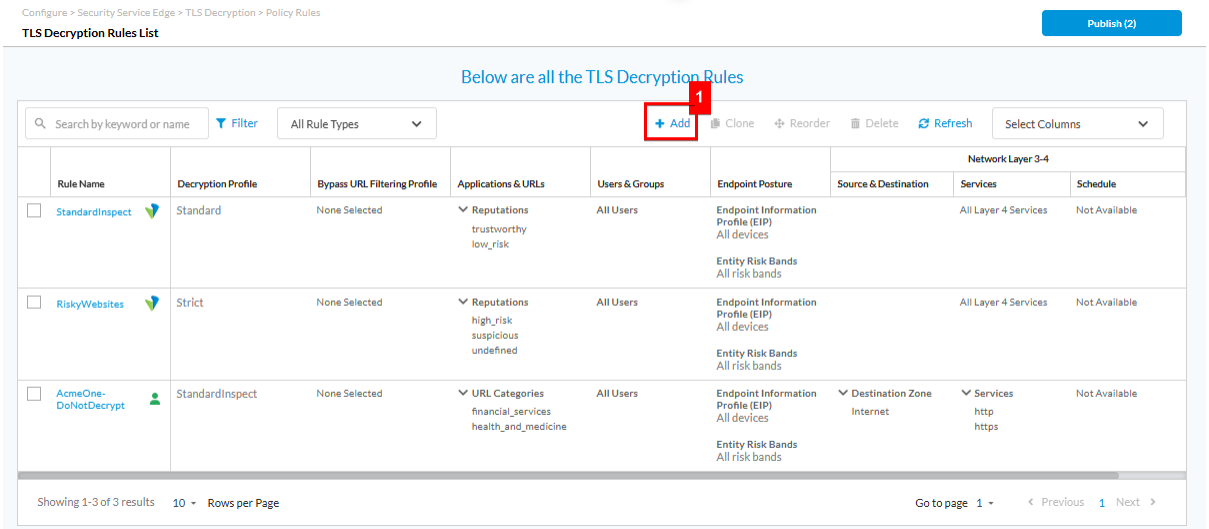


Add descriptive ***Name***, click ***Save*** to finish, Configure Rule order window will be deployed. Select Process Rule First option and then click Save again.

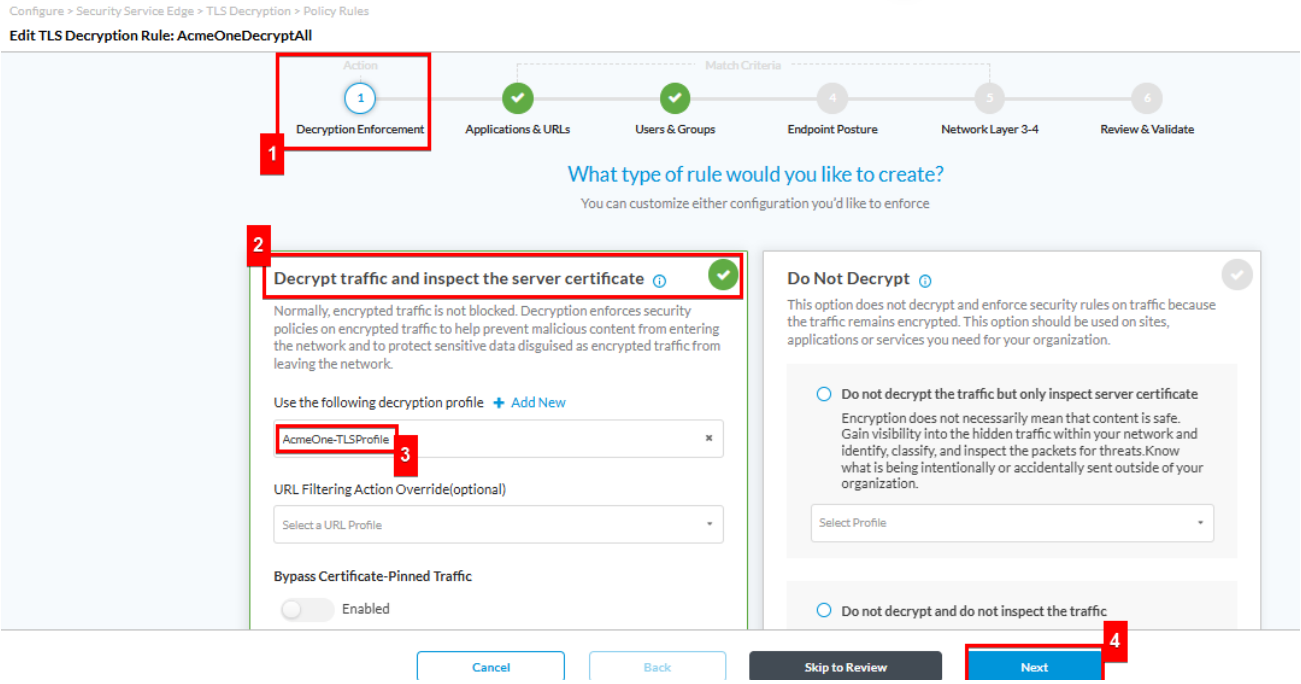

Configure > Security Service Edge > TLS Decryption > Policy Rules
Create TLS Decryption Rule
Action
Match Criteria
Decryption Enforcement
Applications & URLs
Users & Groups
Endpoint Posture
Network Layer 3-4
6
Review & Validate
1
Review your TLS Decryption Rule configurations below
Below are the configurations of your rule. Review and edit any step of your configuration before deploying.
General
Name*
2
AcmeOne-DoNotDecrypt
Description
Enter description name
Tags
Press Enter to add
Rule is Enabled
Applications & URLs
Edit
URL Categories
Custom Selection
URL Categories | 2
financial_services
health_and_medicine
Decryption Enforcement
Edit
Rule Type
Do Not Decrypt
Inspect Traffic Enabled
Inspect the server certificate
Profile
StandardInspect
3
Cancel
Back
Save


Configure > Security Service Edge > TLS Decryption > Policy Rules
Create TLS Decryption Rule
Decryption Enforcement
Applications & URLs
Users & Groups
Endpoint Posture
Network Layer 3-4
Review & Validate
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*
AcmeOne-DoNotDecrypt
Tags
Press Enter to add
Rule is Enabled
Applications & URLs
Edit
URL Categories
Custom Selection
Configure Rule Order
How would you like to process rule "AcmeOne-DoNotDecrypt"?
1
Process the rule last (add this rule at the bottom of the rule list)
Process the rule first (add this rule at the top of the rule list)
Process the rule in specific placement (select where to place in rule list)
2
Cancel
Save

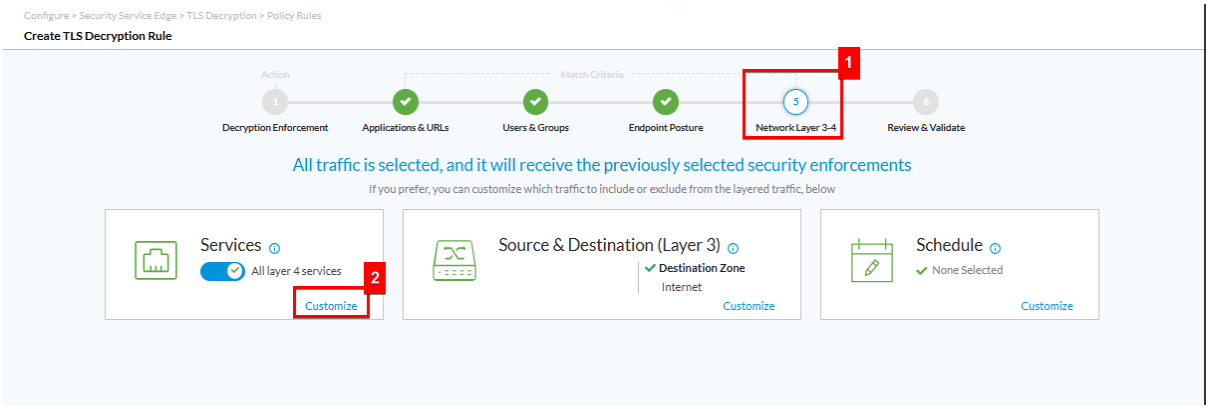
To create the rule allowing to decrypt all traffic, click ***Add***.



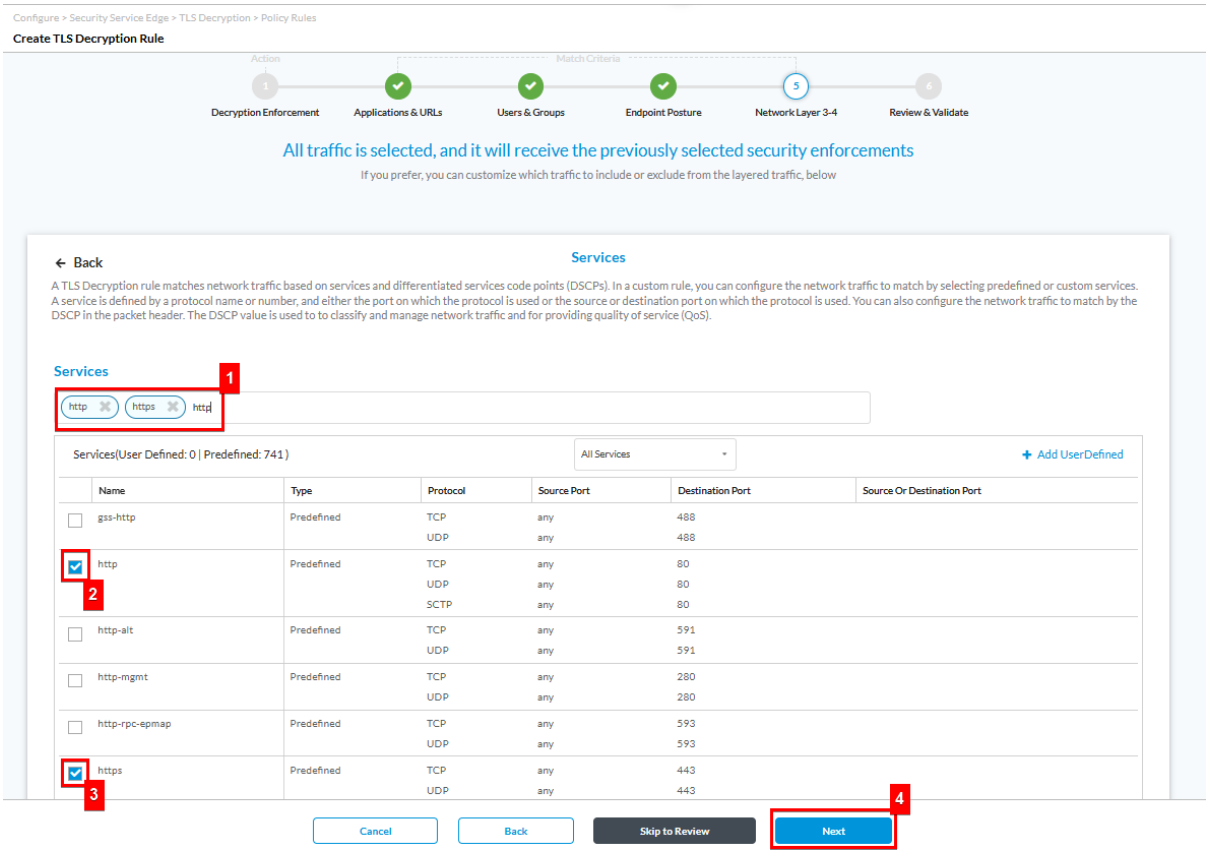
Select ***Decrypt Traffic and Inspect server Certificate***, Select the ***Decryption Profile*** and ***URL Filtering Action Override***, then click Next.



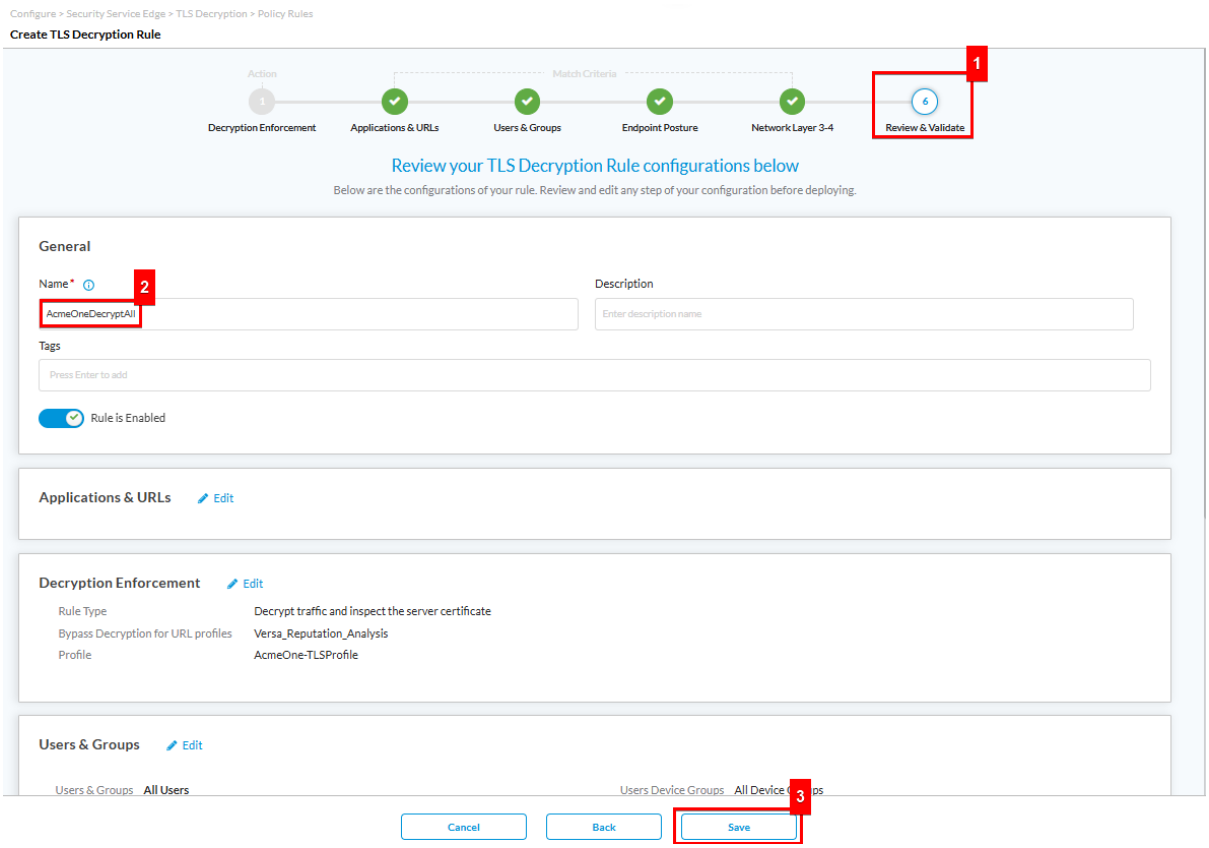
Click ***Next*** in ***Applications and URLs***, ***Users & Groups*** and in ***Endpoint Posture***, until you reach ***Network Layer 3-4***. Click on ***Customize*** in section ***Services***.

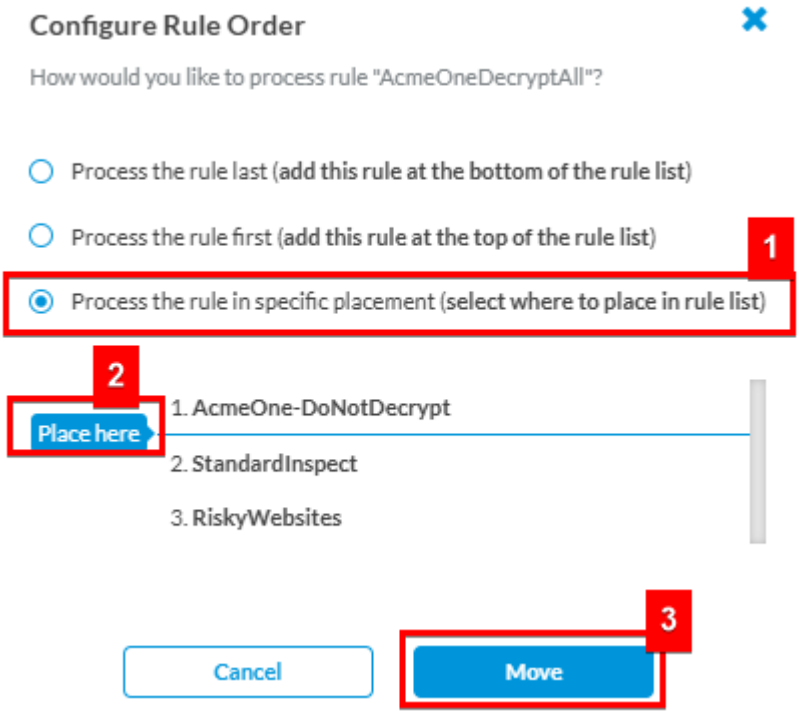


Look for http and add services ***http*** and ***https*** to avoid resources consumption looking for other services. Then Click ***Next***.



Add descriptive ***Name***, click ***Save*** to finish, Configure Rule order window will be deployed. Select Process the Rule in specific placement, place it in the second position and then click Save again.





Place the rule in the second position, after the ***DoNotDecrypt*** rule.

Step 9: Configure Real-Time Protection Profiles and Rules

- First, create different profiles to ensure secure access in accordance with the organization's requirements. For this case, two profiles will be used: a custom profile for URL Filtering and a predefined profile for Malware protection.

- Once all profiles are created or selected from predefined options, proceed to configure the protection policies.

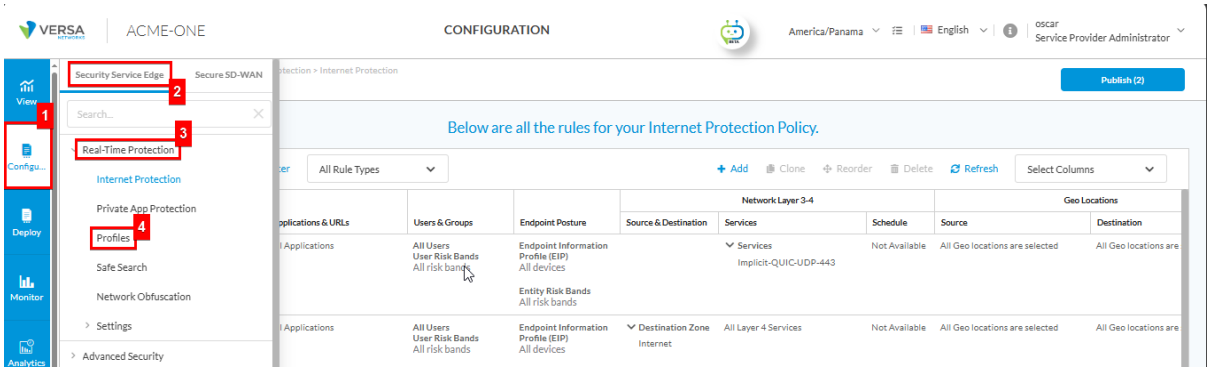
- Next, configure SaaS Tenant Control to ensure users access O365 only with corporate domain accounts. This prevents logins with personal or third-party accounts, reducing the risk of data leakage or use of unmanaged, non-compliant environments.

Custom URL Filtering Profile

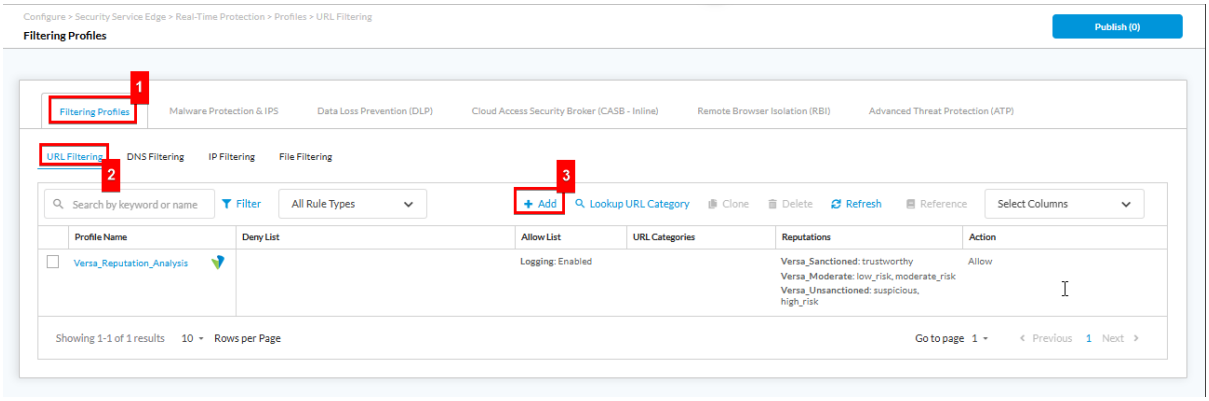
In this use case, all the users will be enforced by one URL filtering profile that blocks the following categories of sites: malware, phishing, botnet, adult, and illegal. Also, URL filtering blocks high-risk and uncategorized/undefined URLs reputation-based threats. The others reputations will be allowed.

To meet these requirements, we will need to create a custom URL Filtering Profile as follows:

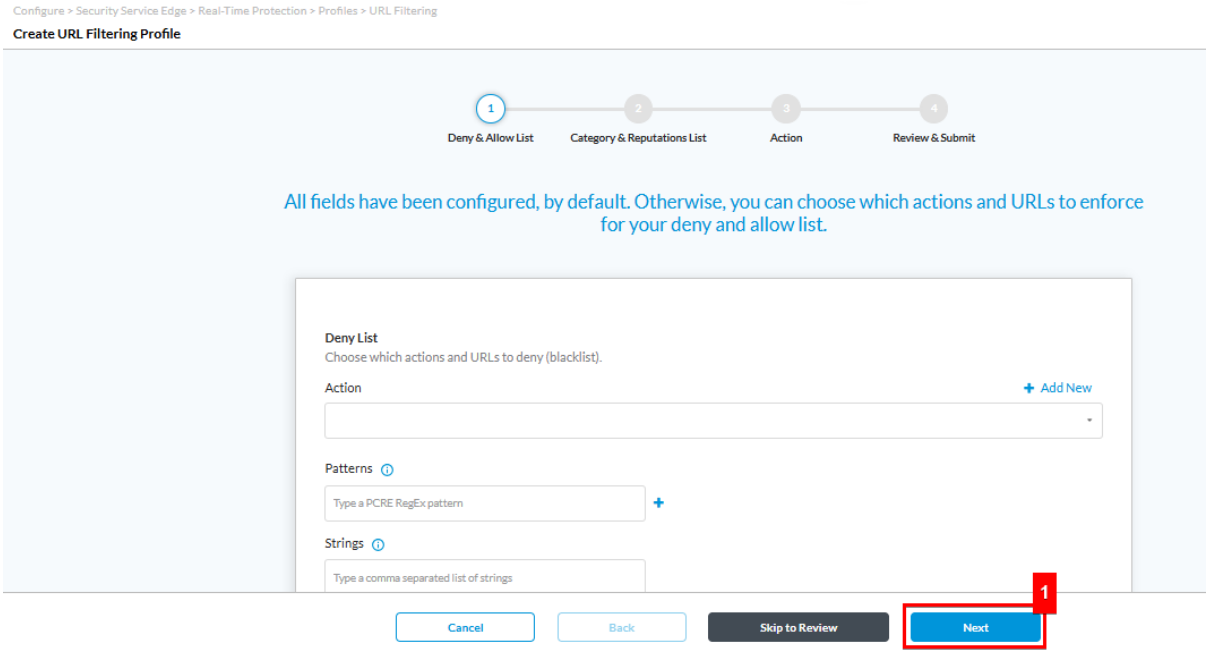
Go to ***Configure*** > ***Security Service Edge*** > ***Real Time Protection*** > ***Profiles***.



Go to ***Filtering Profiles***, select ***URL Filtering***, then click ***+Add*** to create the profile.

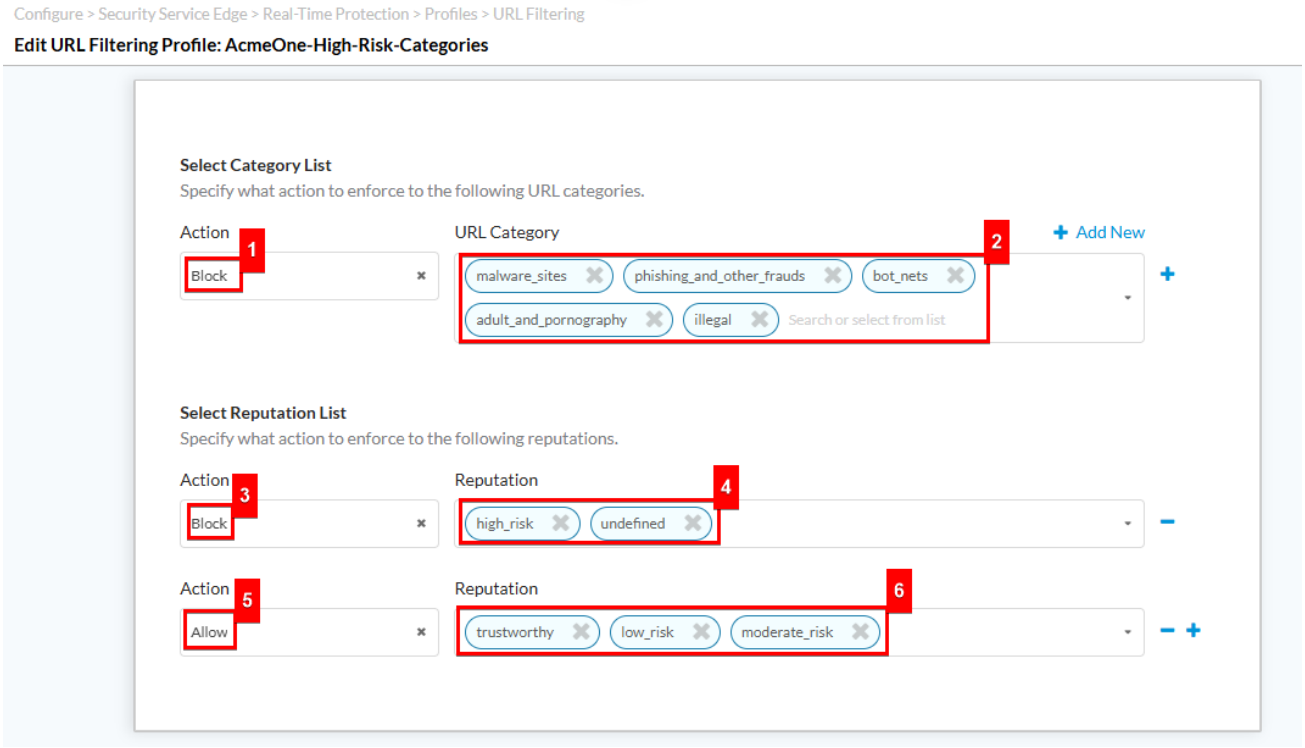


There is no specific URLS to allow or deny, so click Next in Deny/Allow List Action without making any changes.

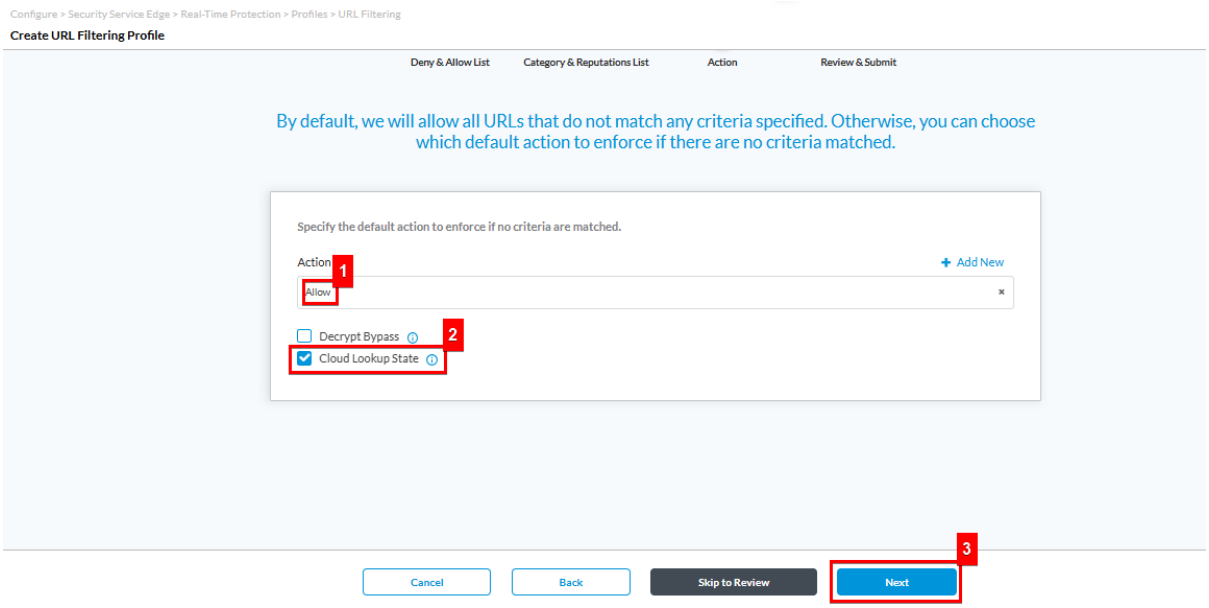


Select Block in the ***Action*** field for Category List section, search and select the ***URL Categories*** malware, phishing, botnet, adult, illegal.

Then select Block in the first ***Action*** field for Reputation List section, search and select ***Reputation*** high_risk and undefined. Click on the **+** to add a second **Action** field, select Allow then search and select ***Reputation*** trustworthy, low_risk and moderate_risk. Then click ***Next*** to continue.



Select Allow as default ***Action*** if the URL does not match any URL category nor reputation. Enabled ***Cloud lookup State***. This helps provide visibility into millions of URLs and categories beyond what can be stored locally. Click ***Next*** to continue.



Add a descriptive ***Name*** for the profile and then click on ***Save***.

Malware Protection & IPS Profile (Predefined)

ACME-ONE requires the enablement of Antivirus and Intrusion Prevention System (IPS) for safeguarding internet traffic to detect, block, and neutralize malicious threats before they can compromise your devices or data.

By default, Versa SASE provides predefined security profiles to protect against malware and IPS. In this scenario, we will use those predefined profiles available because they both meet the requirements for these threats. Therefore, there is no need to create customs profiles in this section.

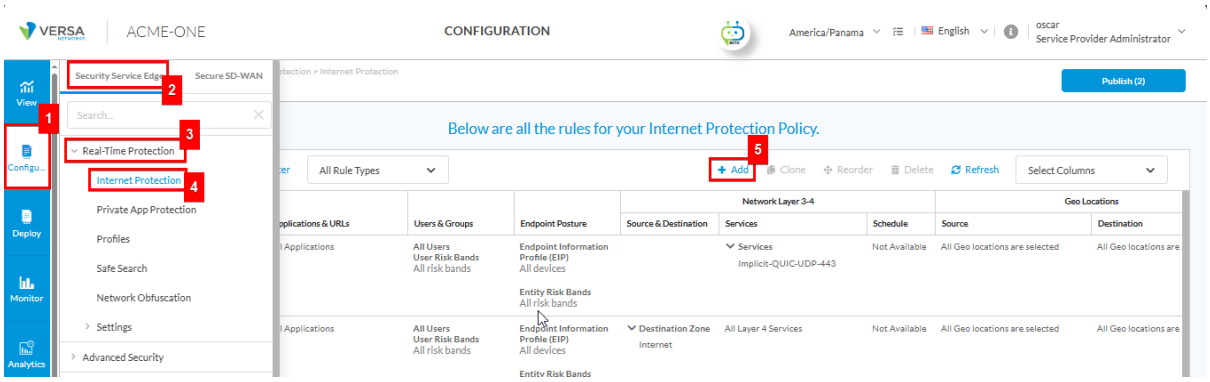
Internet Protection Rules

Now that all the profiles required to enforce the security of the use case are ready to be used, we will proceed with the internet protection rules configuration. For this case, all users; with no exception, need to be secured with these profiles therefore we will create one Real-time Protection rule for all users accessing the Internet, as follows:

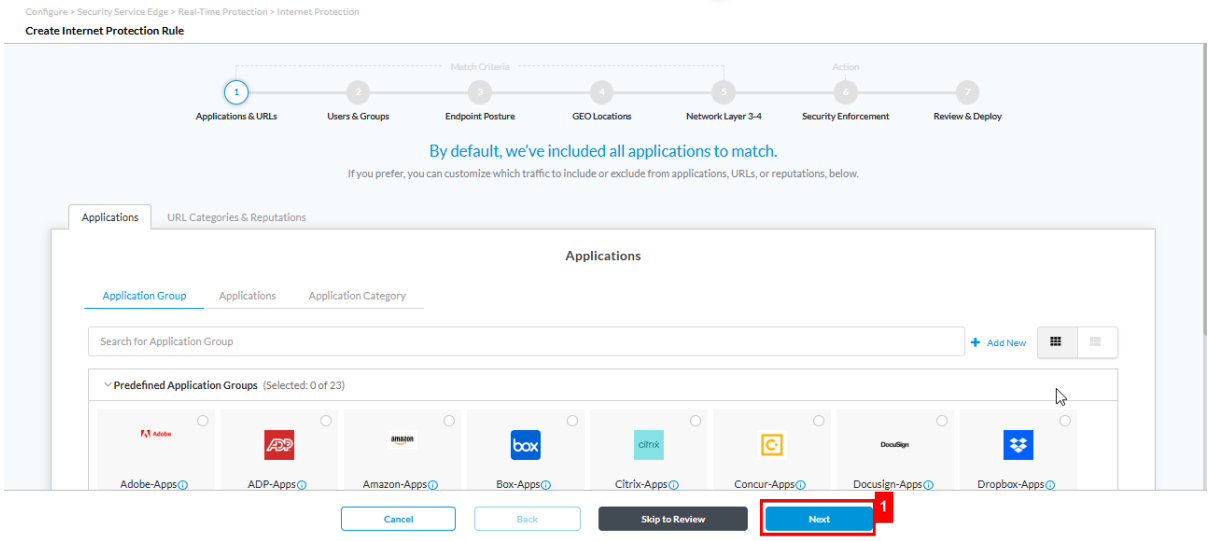
Navigate to

Configure > ***Security Service Edge*** > ***Real-Time Protection*** > ***Internet Protection***,

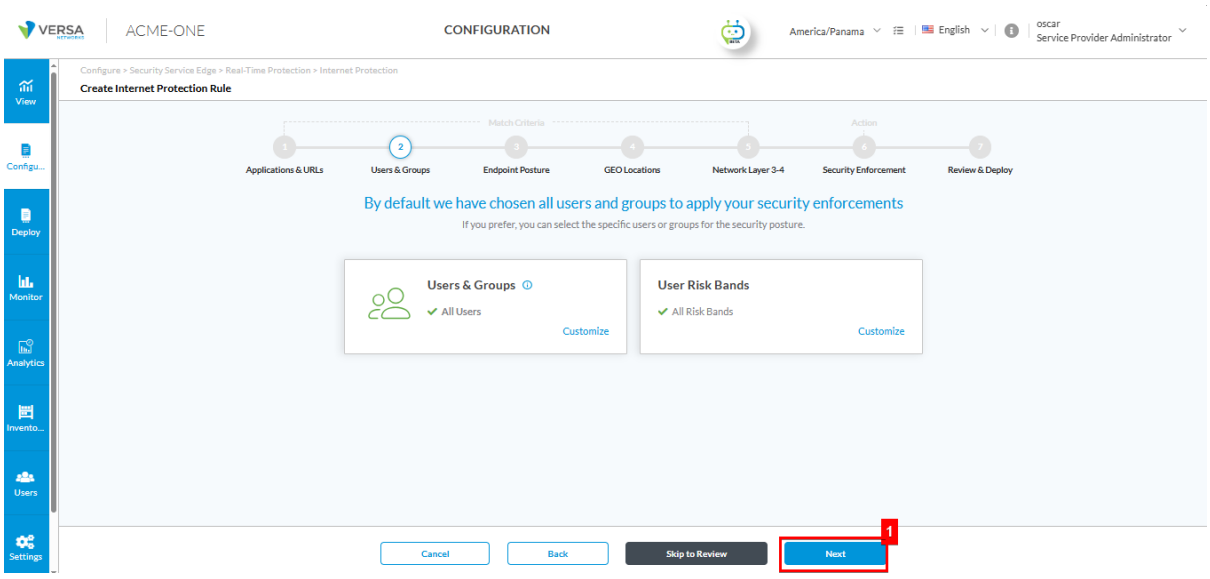
Click on ***+Add***. Each Internet Protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR 'ed and on different tabs is 'AND'.



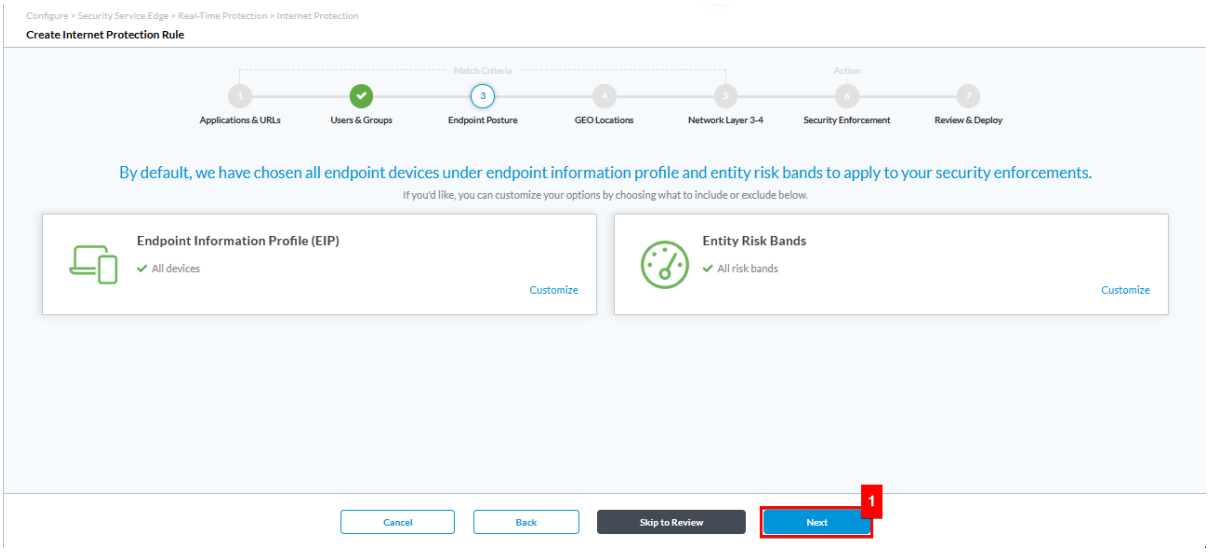
URL Filtering, Antivirus, and IPS will be performed using a profile, so no matching applications or URL is required, just click ***Next*** without making any changes.



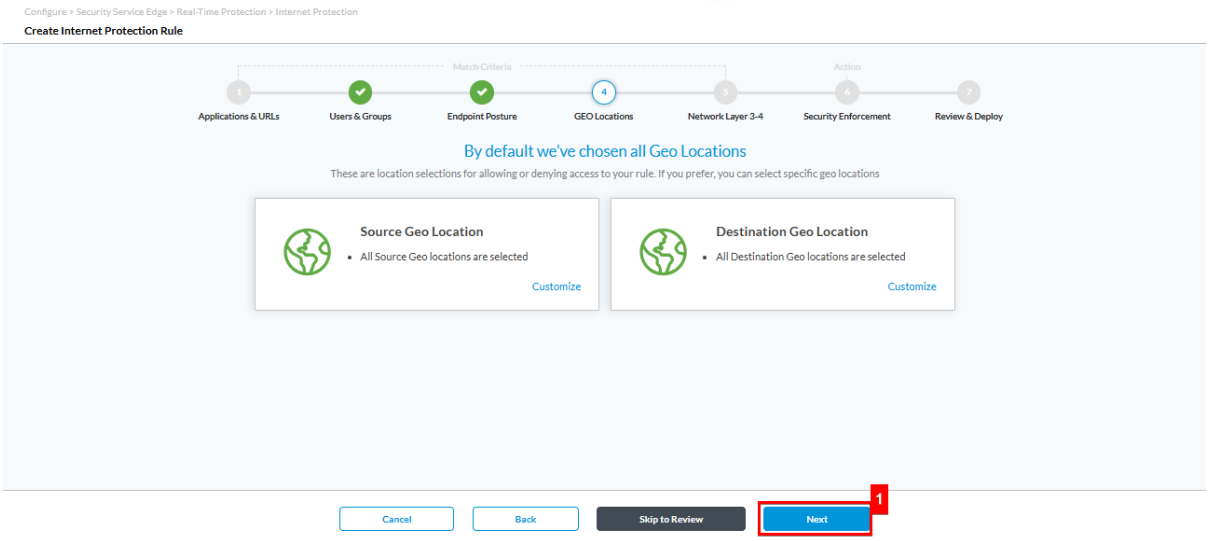
In the Users & Groups section you can customize and select the users or groups to match this protection. In this case the protection will be enabled for all users so there is no need to apply any change and just click ***Next***.



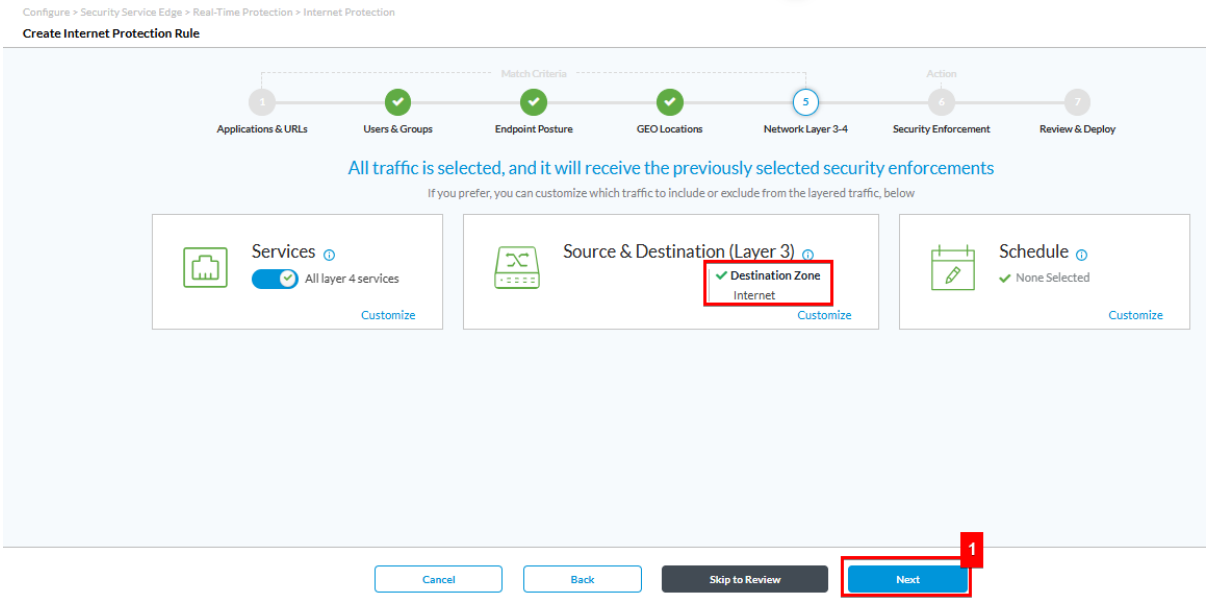
No EIP or Entity Risk criteria will be used as match criteria so Click ***Next*** in Endpoint Posture section.



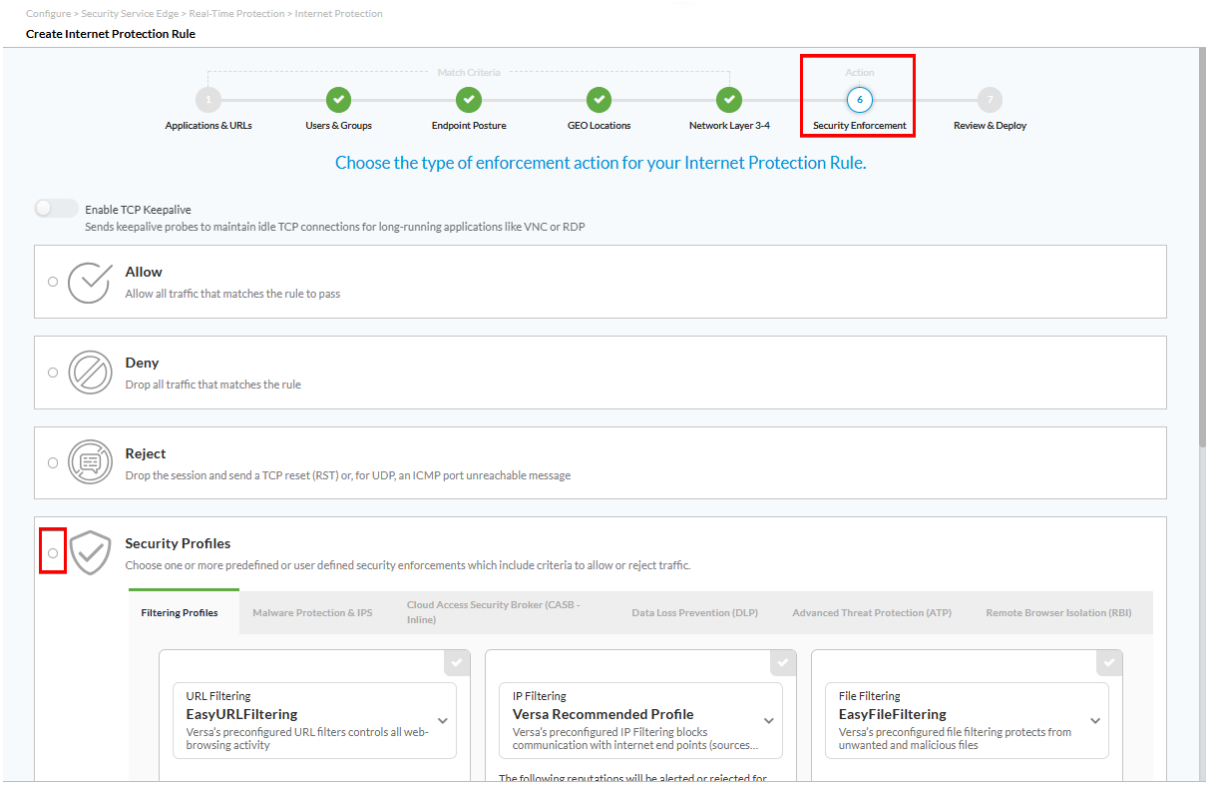
Click ***Next*** in Geo Posture section, no match criteria for geo location for traffic.



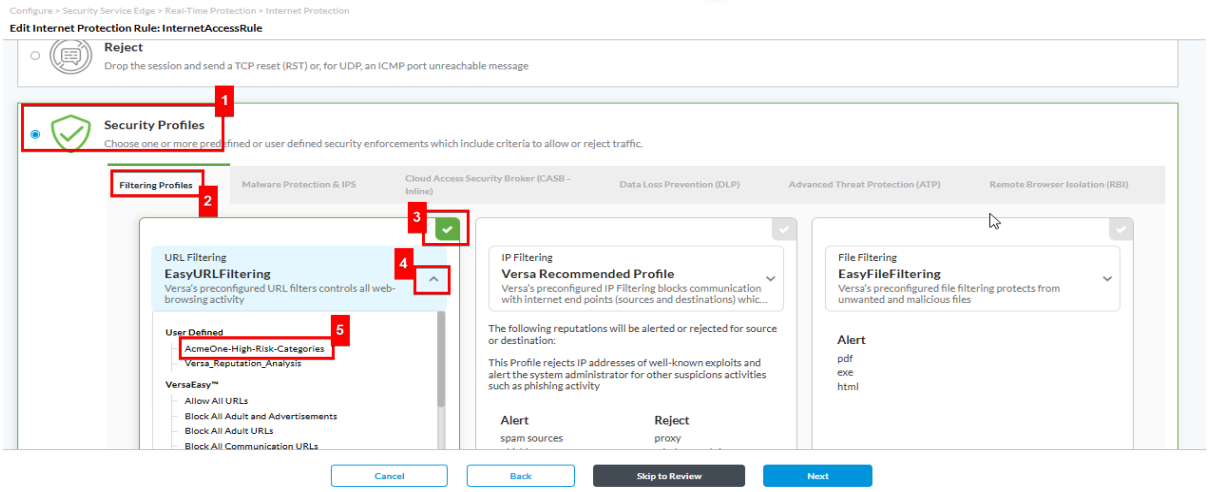
In the Network Layer section, keep the Internet as the Destination Zone for this rule and click ***Next***.



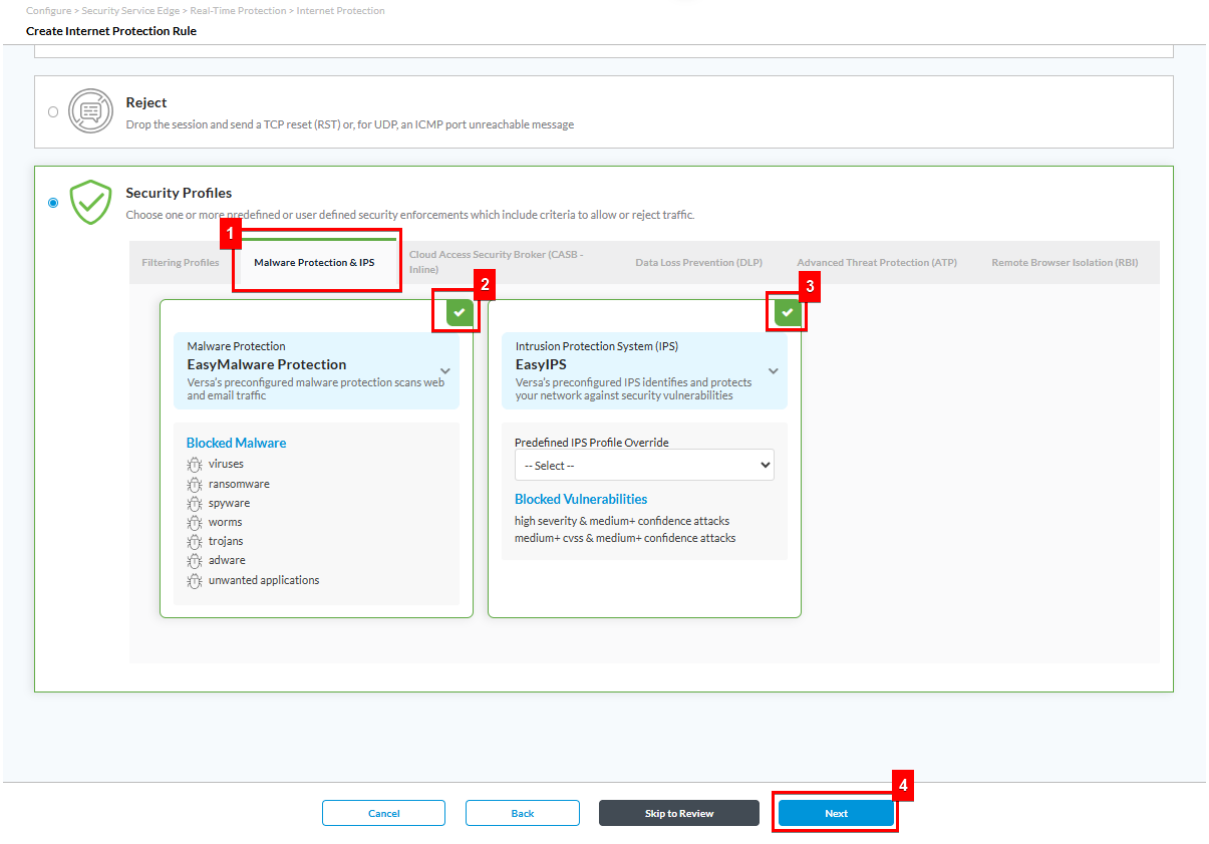
In the ***Security Enforcement*** section scroll down and Select ***Security Profiles***



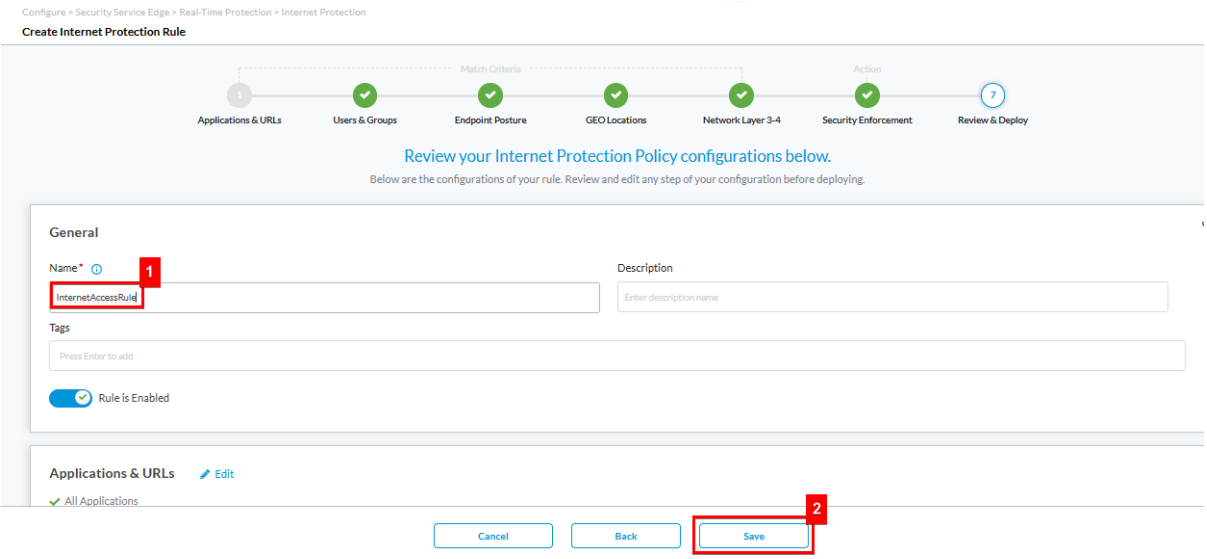
In section ***Filtering Profiles*** enable ***URL Filtering*** and select the User Defined ***AcmeOne-High Risk-Categories*** profile that was created before.

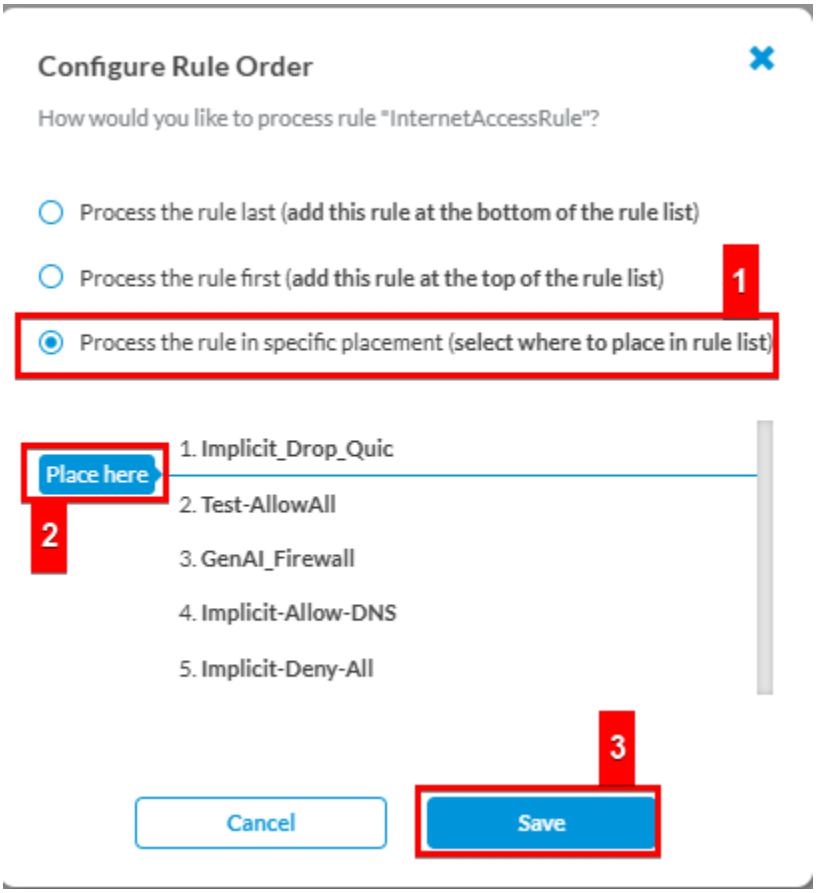


Then click on the section ***Malware Protection & IPS*** and enable the Malware protection check mark, select the Versa´s preconfigured ***EasyMalware Protection*** and the Intrusion Protection System (IPS) check mark with the Versa´s preconfigured ***EasyIPS*** protection and click ***Next***.



Use a descriptive ***Name*** and Click ***Save*** to create this rule. Save the rule after implicit ***Implicit_Drop_Quic*** rule





Private Protection Rules

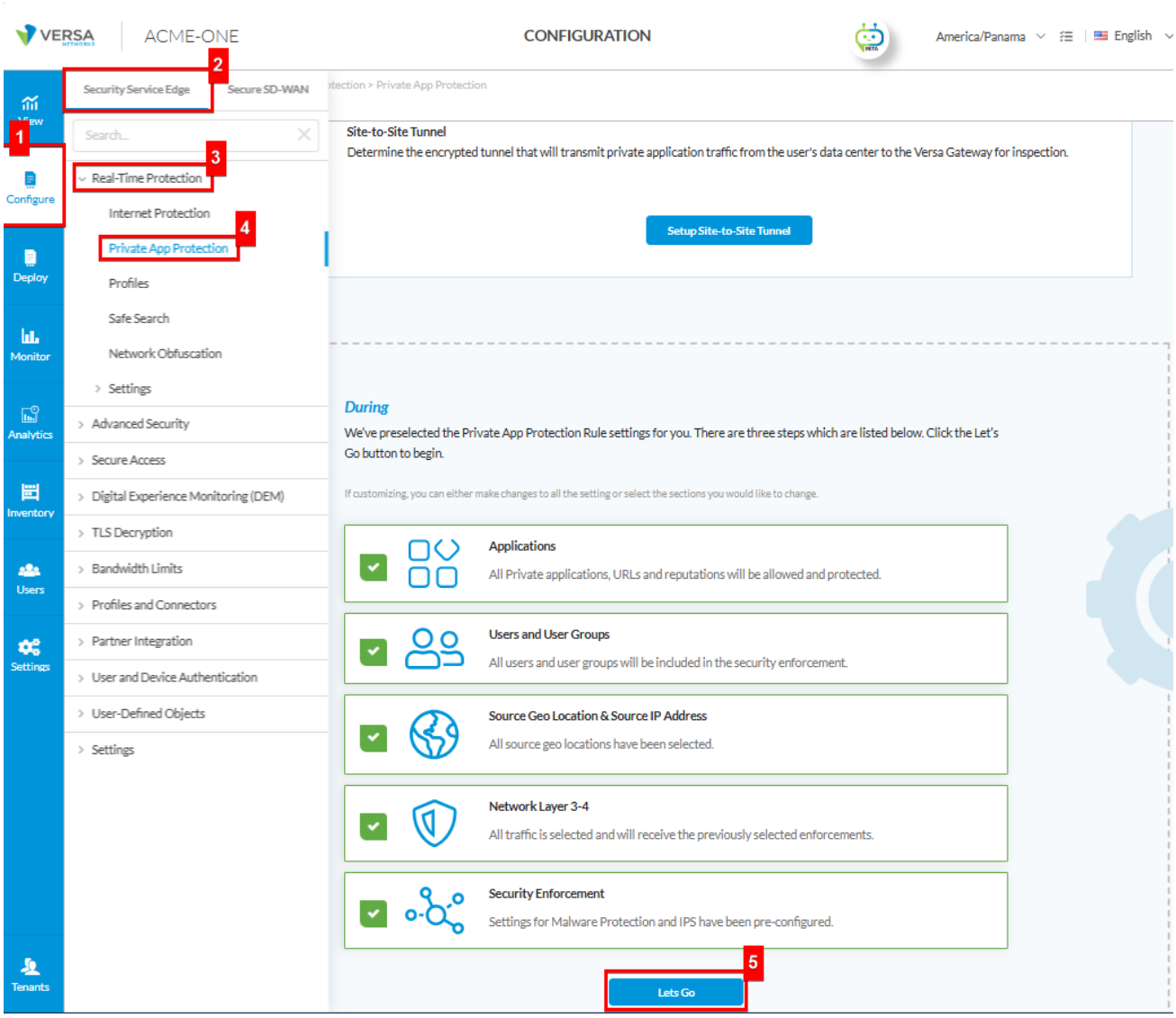
Next, we create a Real-Time Private App Protection policy to secure traffic from remote users accessing internal applications hosted in the datacenters. To begin, make sure that the Private Applications from Step 3 have been configured.

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

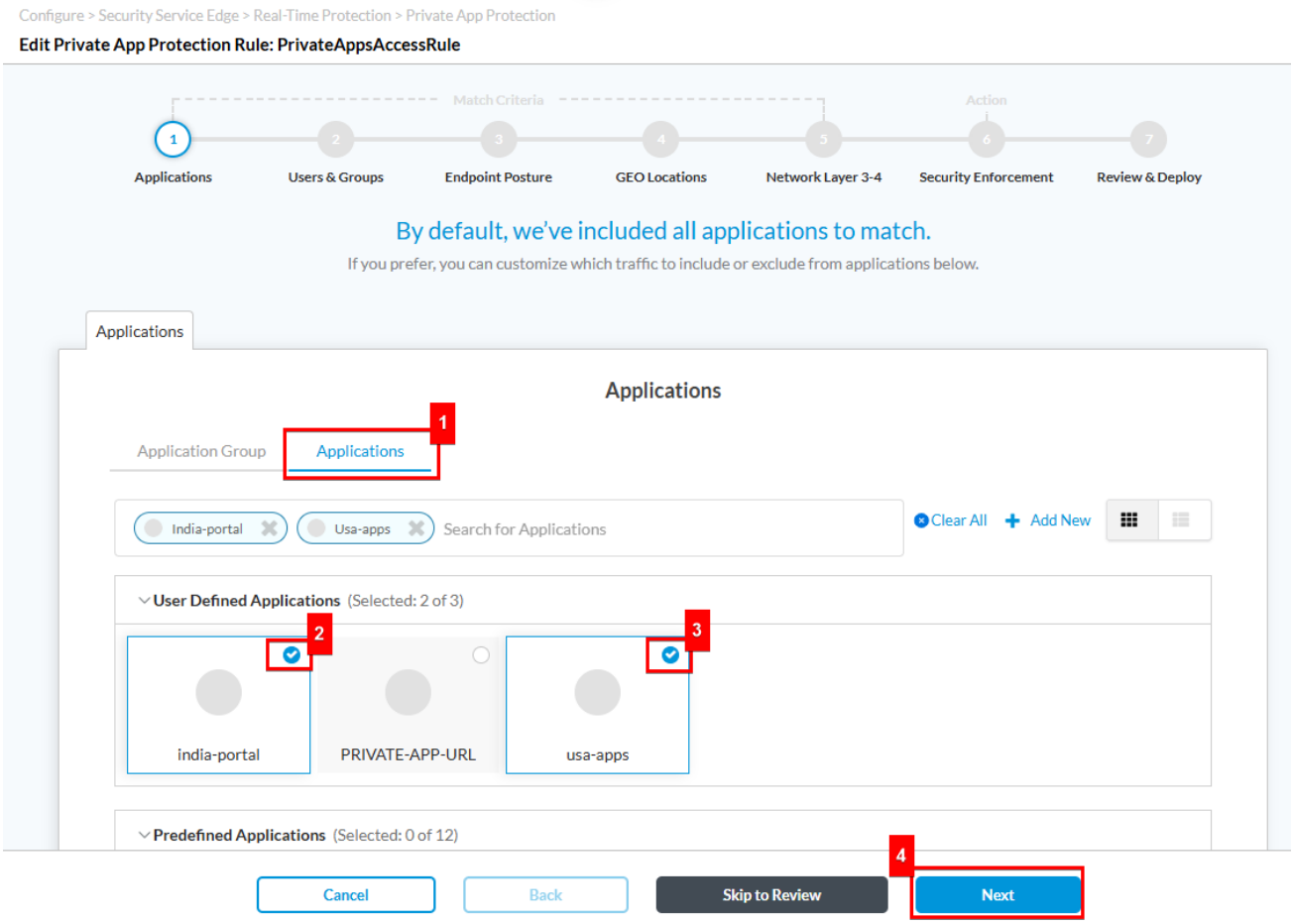
Navigate to

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

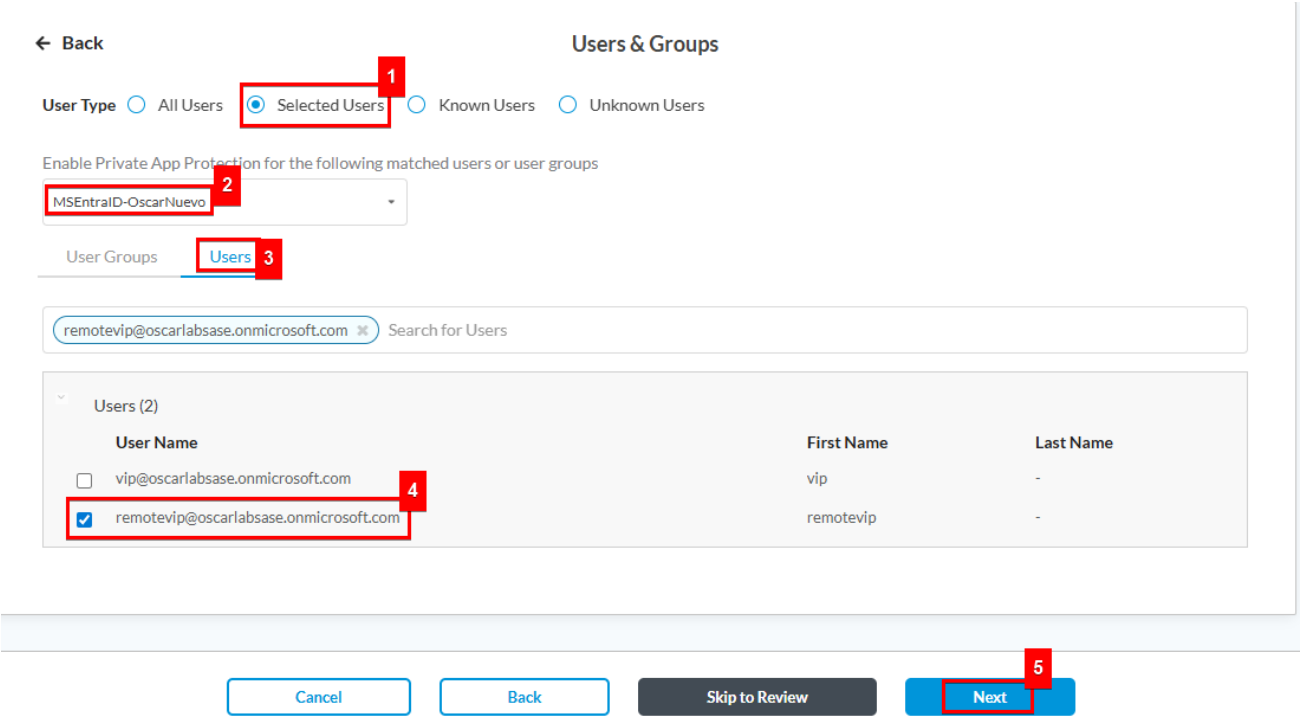
Click on **+Add** (Click on Let's Go, if this is your first Private App Rule). Each private protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR 'ed and on different tabs is 'AND'.



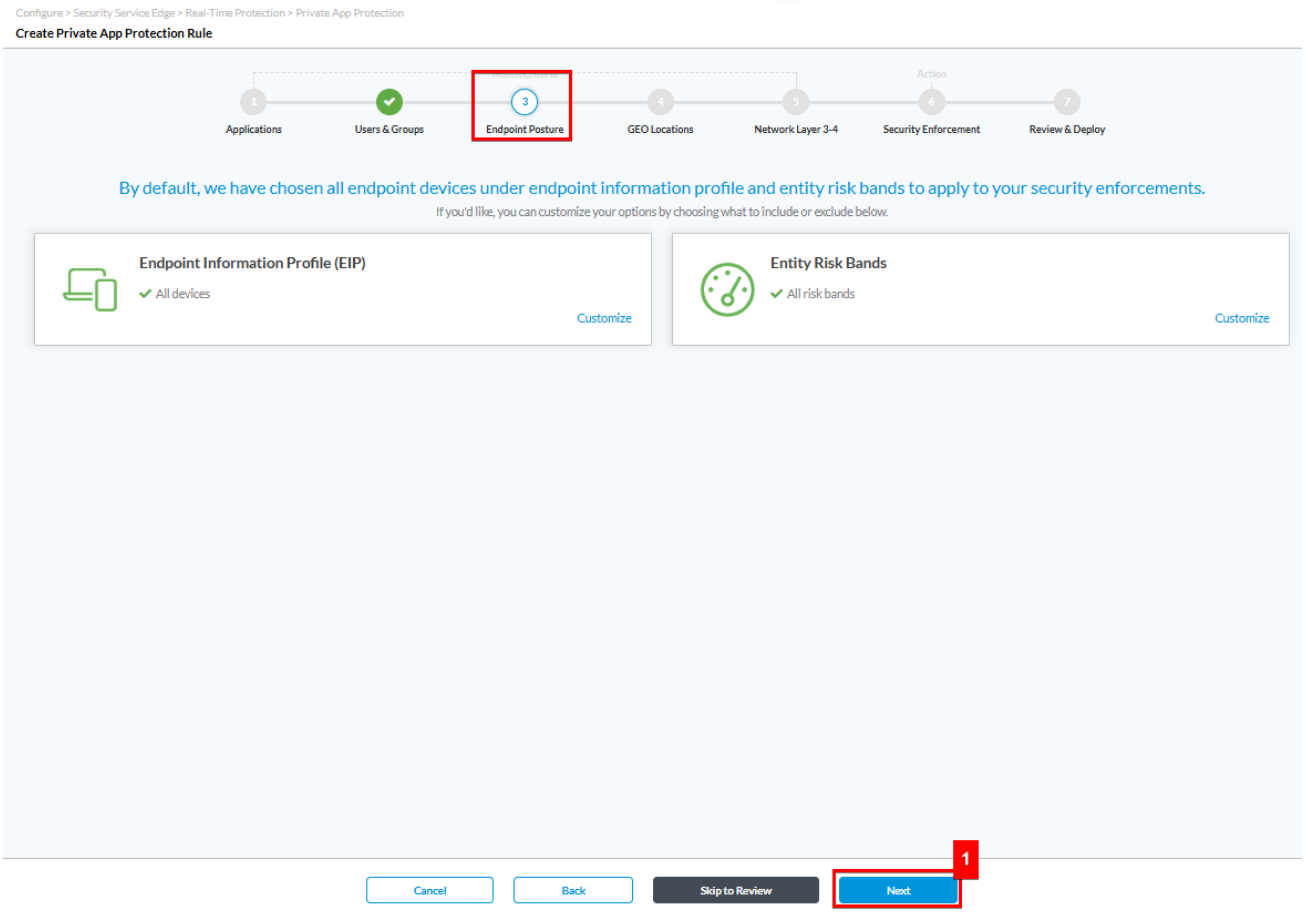
Select the previously created applications (**India-portal** and **Usa-apps**) and click ***Next***.



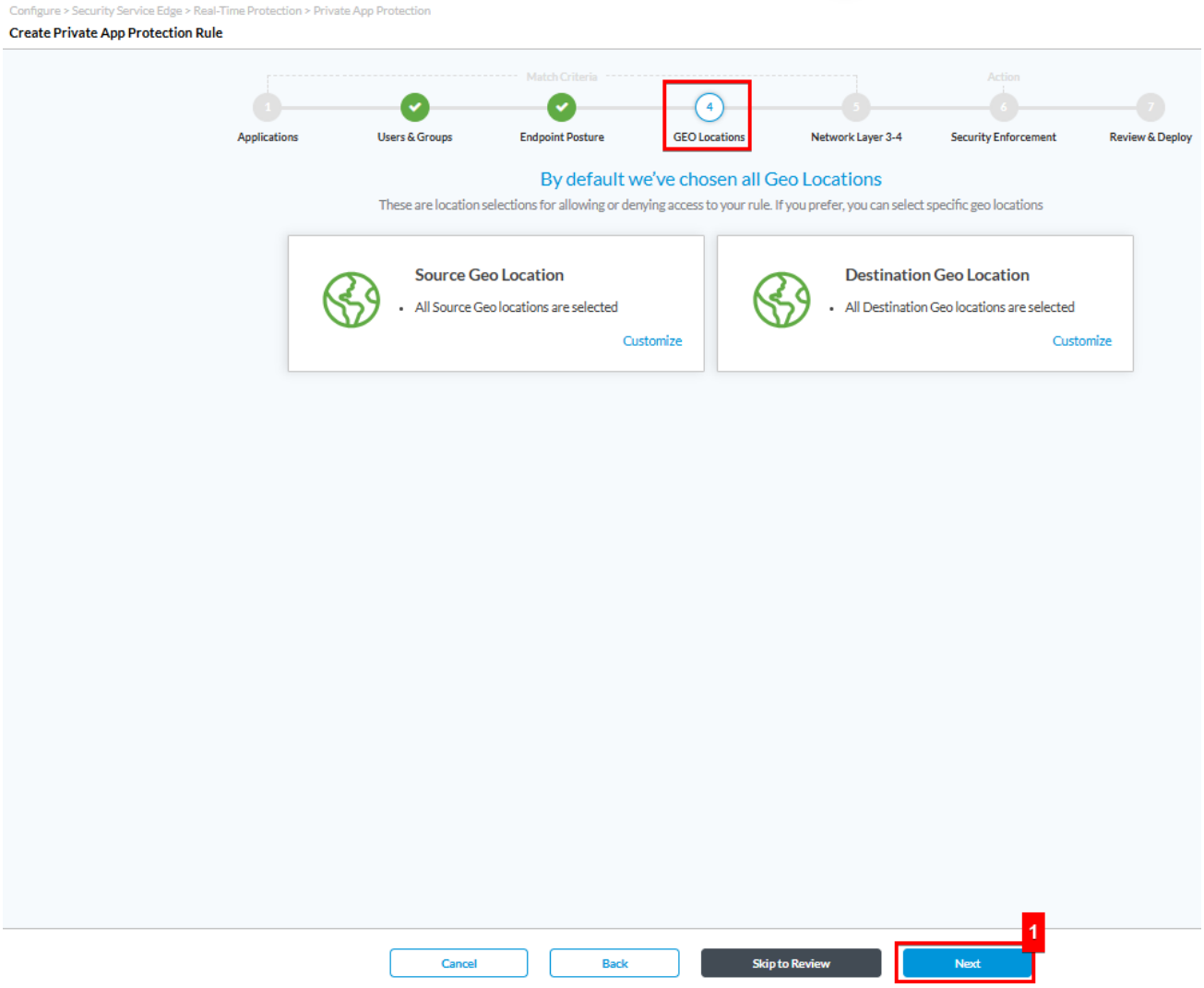
In the Users & Groups section you can customize and select the users or groups to match this protection. In this case the protection will be enabled for ***remotevip*** test users and click ***Next***.



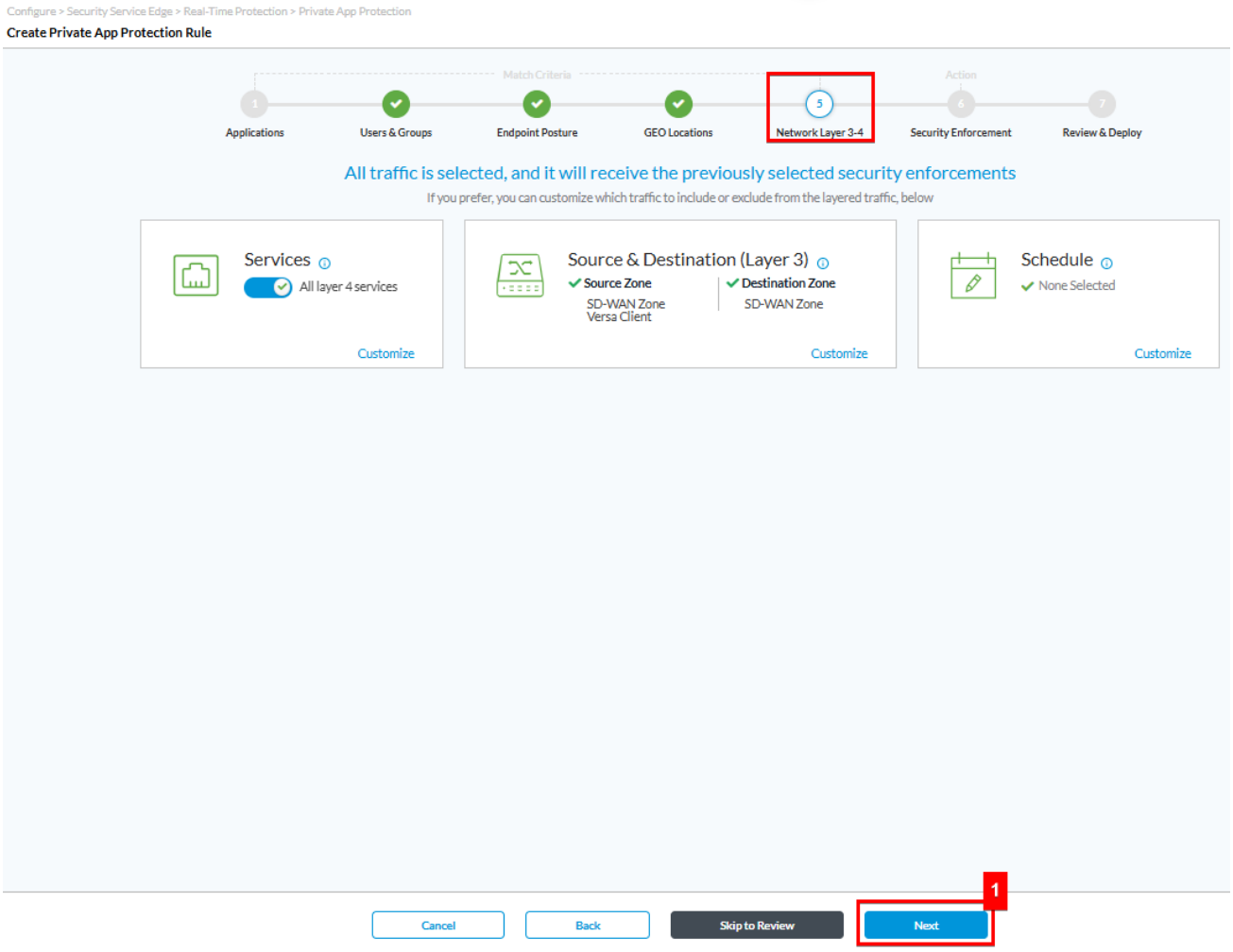
No EIP or Entity Risk criteria will be used as match criteria so Click ***Next*** in Endpoint Posture section.



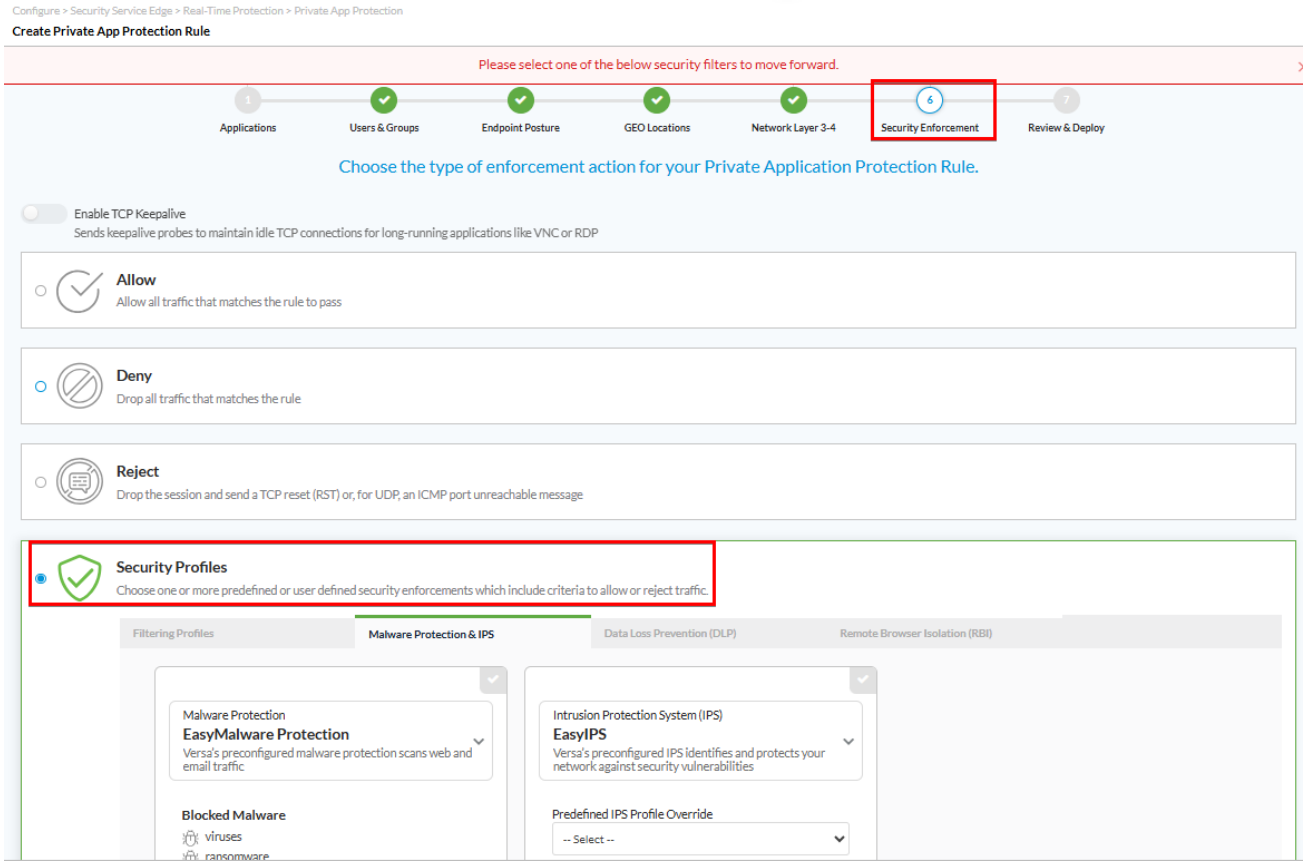
Click ***Next*** in Geo Posture section, no match criteria for geo location for traffic.



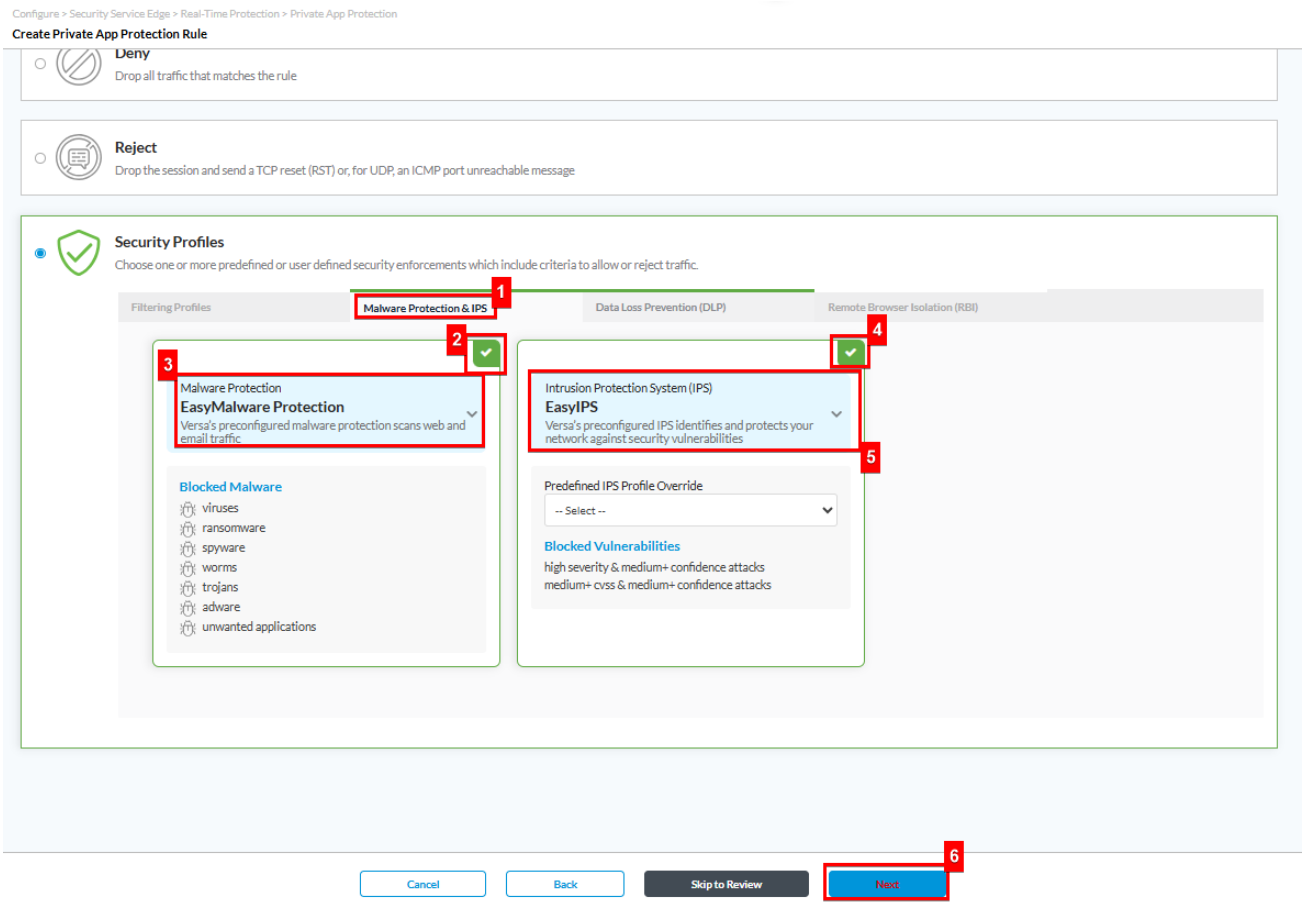
In ***Network Layer 3-4*** section, keep the default values to match all traffic from remote users to internal applications. Click ***Next***.



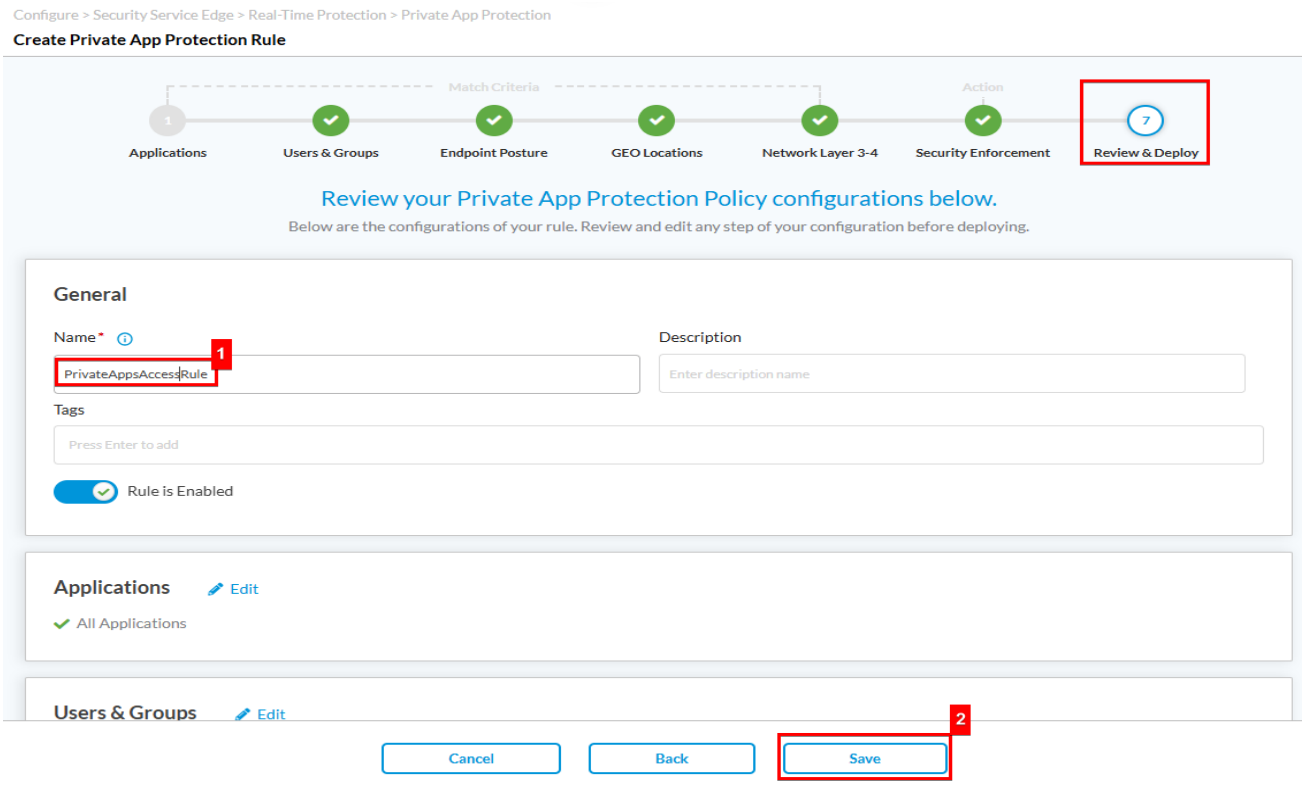
In the ***Security Enforcement*** section scroll down and Select ***Security Profiles***



Then click on the section ***Malware Protection & IPS*** and enable the Malware protection check mark, select the Versa´s preconfigured ***EasyMalware Protection*** and the Intrusion Protection System (IPS) check mark with the Versa´s preconfigured ***EasyIPS*** protection and click ***Next***.



Use a descriptive ***Name*** and Click ***Save*** to create this rule.



Saas Tenant Control

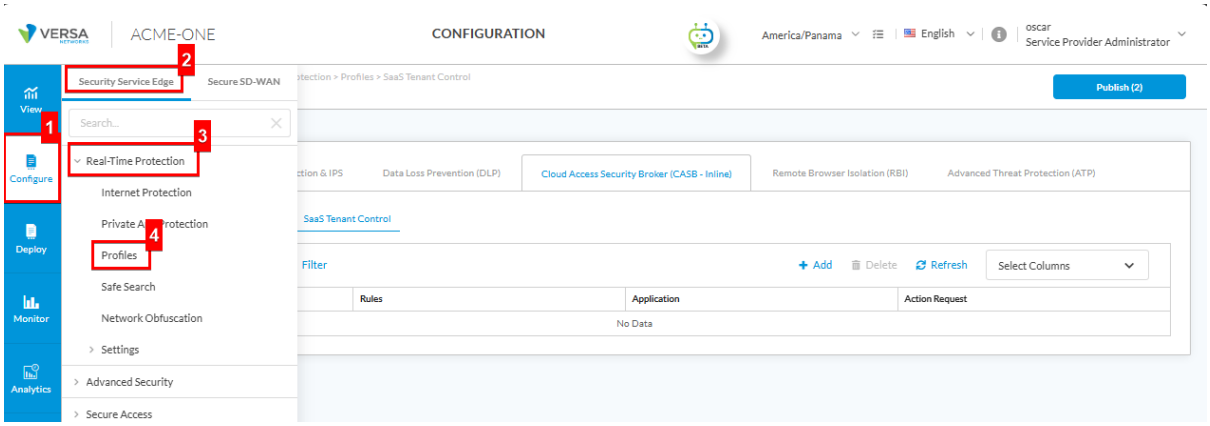
In this scenario, users cannot use personal accounts for Office 365, users cannot use other organizations' tenants and only the corporate Office 365 tenant is accessible. To ensure these restrictions, two controls are required.

Why Are Two Controls Required?

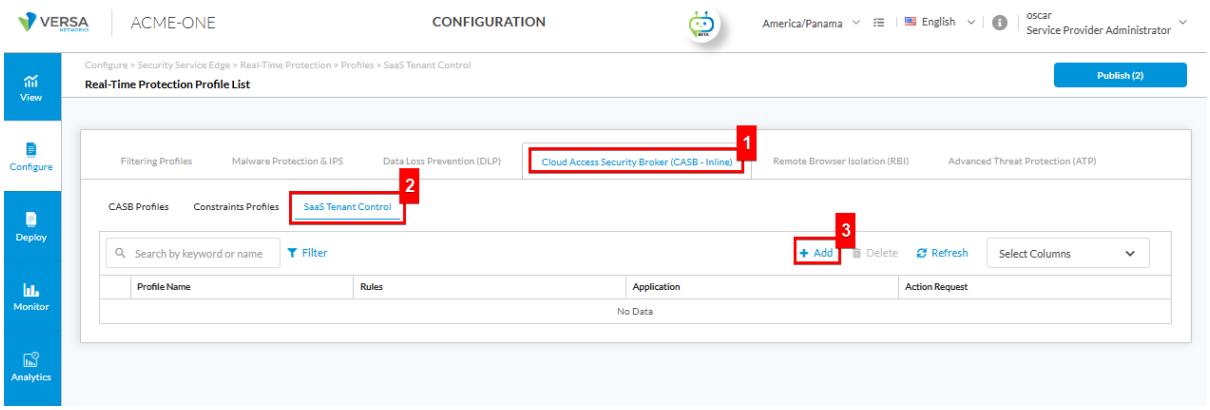
Office 365 Block Consumer Account: This control prevents users from signing in with personal Microsoft accounts (e.g., @outlook.com, @hotmail.com, @live.com). Without this restriction, users could bypass corporate monitoring and store or share sensitive data in unmanaged personal accounts.

Microsoft-Office365-Tenant-Restrictions: This control enforces access to a specific corporate tenant (e.g., oscarlabsase.onmicrosoft.com). Even if a user tries to log in with another company's Office 365 tenant or a third-party organizational account, the connection will be blocked. This ensures all traffic is tied to the customer's authorized tenant only.

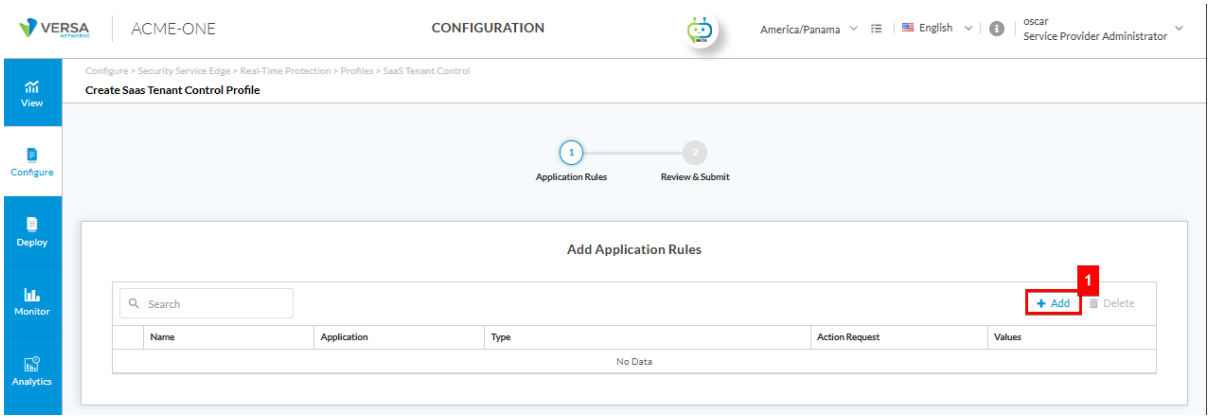
To configure SaaS Tenant Control, go to ***Configure*** > ***Security Service Edge*** > ***Real Time Protection*** > ***Profiles***.



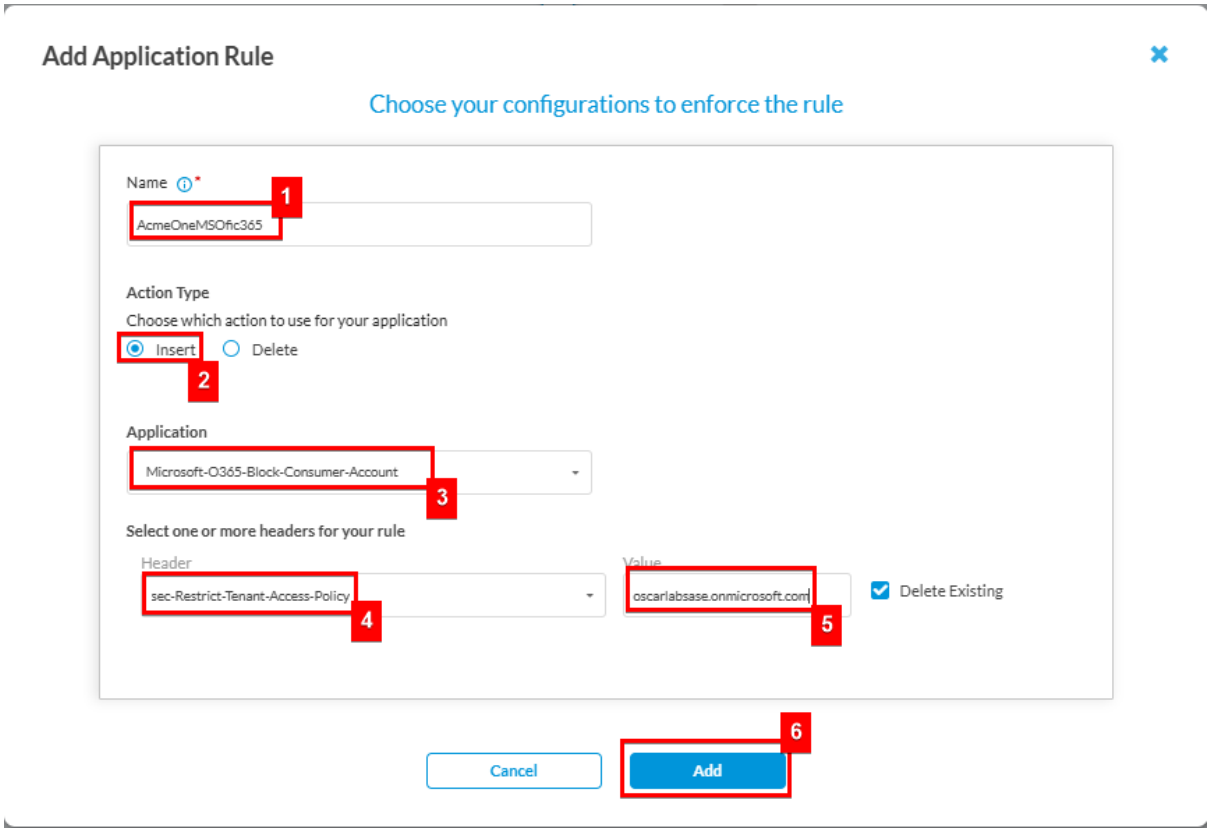
Next, go to ***Cloud Access Security Broker CASB*** > ***SaaS Tenant Control*** > ***Add***.



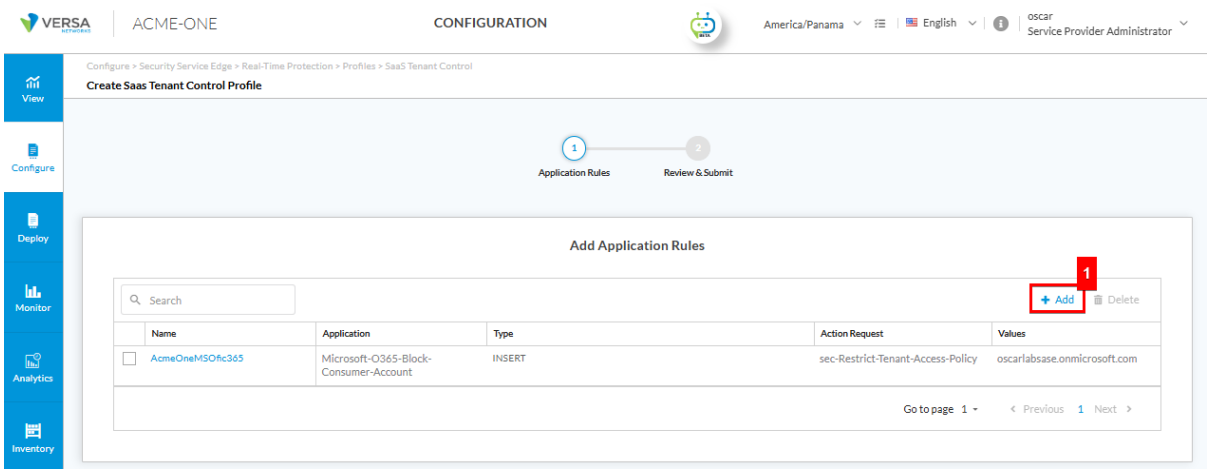
Click on ***Add*** to create a Rule.



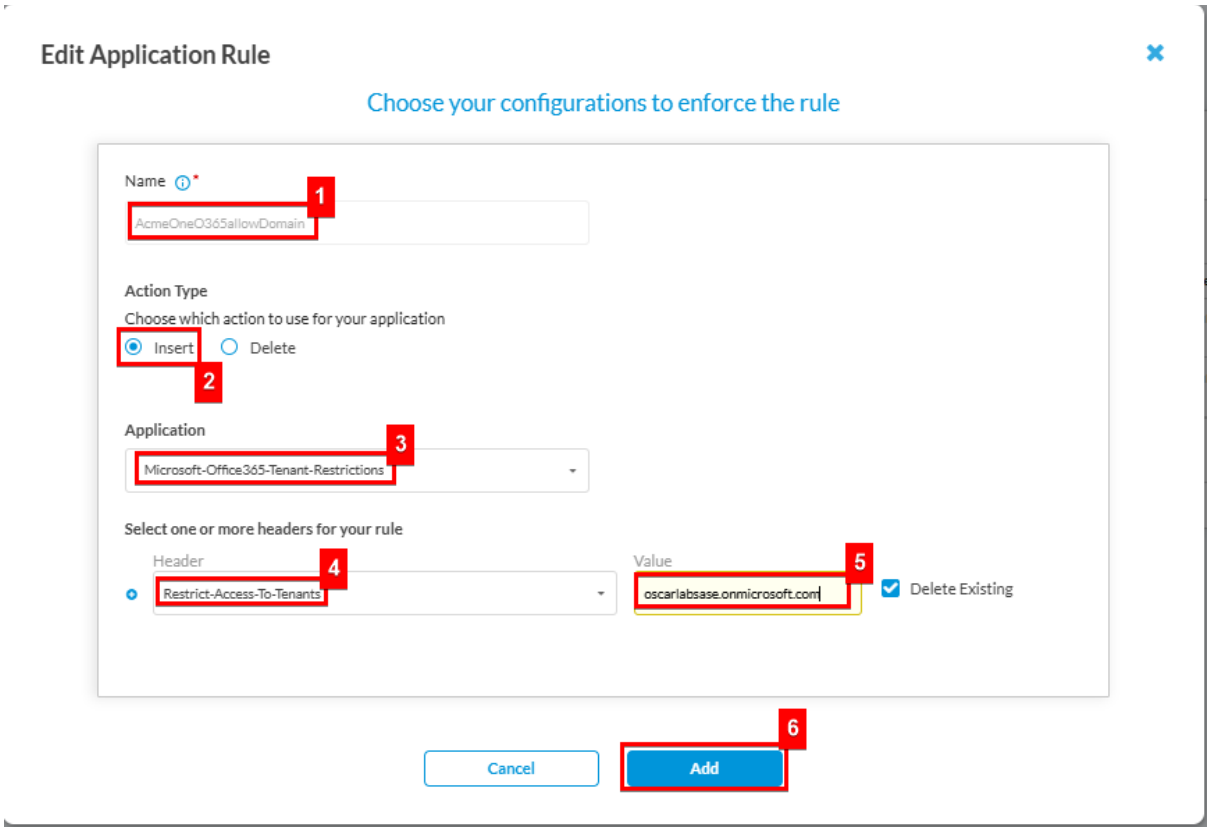
Assign a Descriptive ***Name***, select the ***Insert*** Option, In the ***Application*** Menu look for Microsoft-O365-Block-Consumer-Account to filter consumer/public domains, for ***Header*** option use Sec-Restrict-Tenant-Access-policy with the ***Value*** oscarlabsase.onmicrosoft.com. Then Click ***Add***.



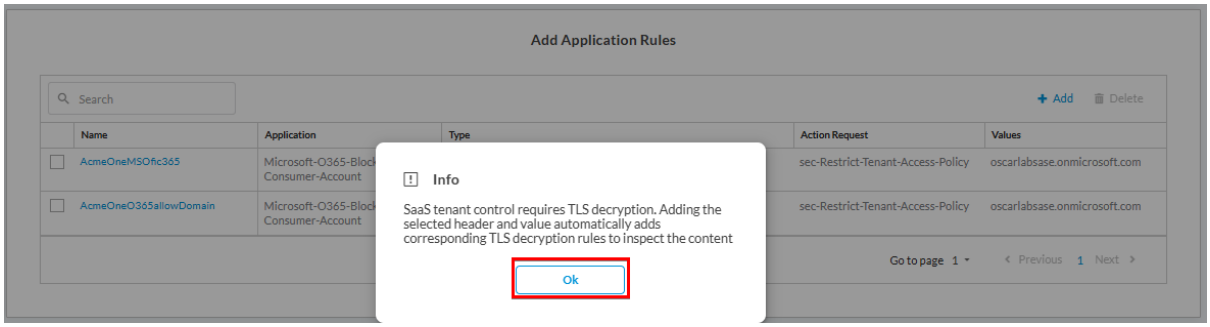
Select ***Add*** again to create a restriction for corporate domains different to acme-one.com



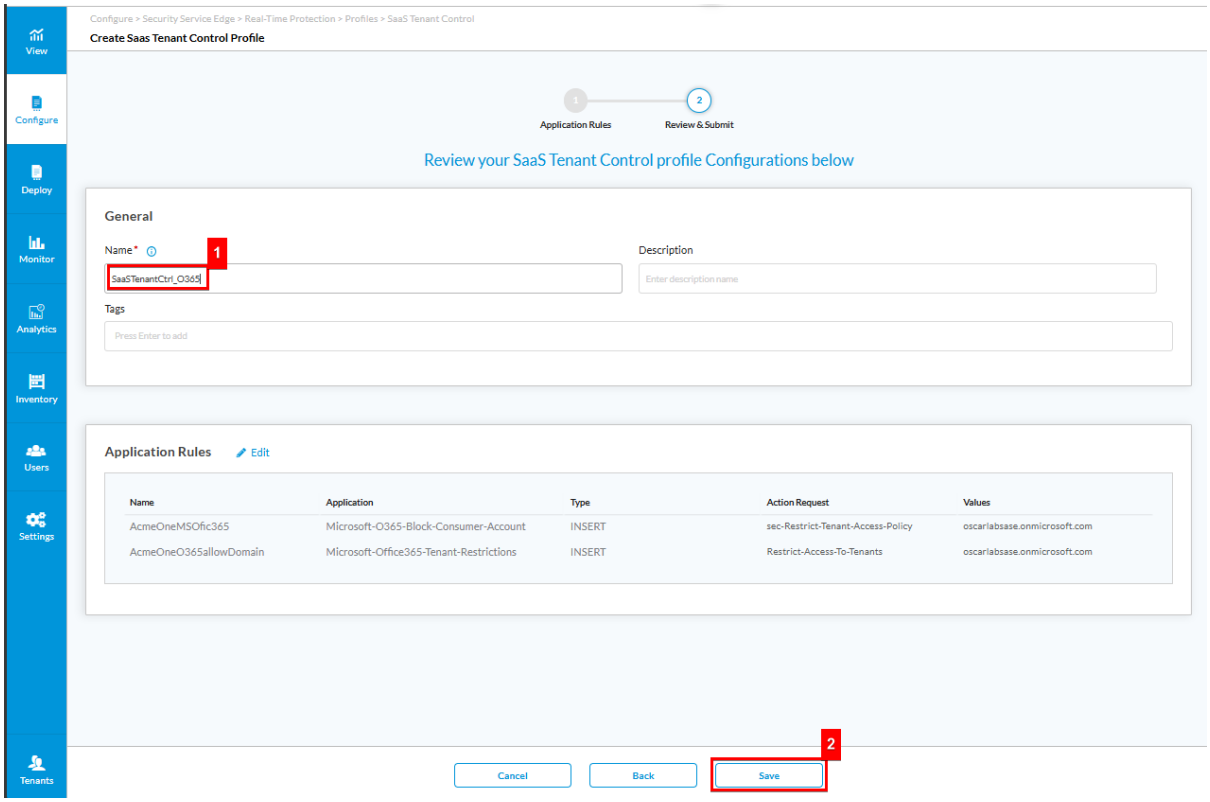
Assign a Descriptive ***Name***, select the ***Insert*** Option, In the ***Application*** Menu look for Microsoft-Office365-Tenant-Restrictions to filter corporate domains, for ***Header*** option use Restrict-Access-To-Tenants with the ***Value*** oscarlabsase.onmicrosoft.com. Then Click ***Add*** and then ***Next***.



Click ***Ok*** in the information window reporting the TLS decryption rule creation, Then Click ***Next***.



To complete the configuration, assign a descriptive ***Name*** and click ***Save***.



Appendix A - Authentication Method - Microsoft Entra ID

Microsoft Entra ID is a cloud-based identity and access management service that provides secure single sign-on (SSO) to Microsoft 365, SaaS apps, and on-premises resources using standards like SAML, OAuth, and OpenID Connect. For this and other authentication methods configuration please refer to document [Step-By-Step-Authentication-Methods-Configuration.docx]

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.