VERSA

IMPLEMENTATION GUIDE

Versa Terminal Server Agent (TSA) Use Cases

About This Document

This document is intended to help customers understand the use case, benefits, and deployment considerations for the Versa Terminal Server Agent (TSA) in Secure Access and Zero-Trust architecture. It is specifically tailored for environments where multiple users access shared desktop systems such as Windows-based Terminal Servers.

Document Information

Title	**Versa Terminal Server Agent (TSA) Use Cases**
Author	Versa Professional Services
Version	V 1.0

Disclaimer

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

What is TSA? 4
Versa TSA Use Cases 5
Scenario 1: Terminal Server at HQ with Internet via SSE Gateway 5
Connectivity Options 5
TSA Integration with SSE 6
Scenario 2: SD-WAN Branch to Remote SD-WAN Branch (Private Apps) + Local Internet Breakout (LBO) 6
Why TSA Registration is Needed at Branch A 7
TSA Integration with Versa SD-WAN Branch 7
Scenario 3: SD-WAN Branch to Remote SD-WAN Branch (Private App Access Only) 8
Why TSA Registration is Needed at Branch B 8
TSA Integration with Versa SD-WAN Branch 8
Configuration Steps: Scenario 1 9
Configuration Steps: Scenario 2 & 3 27
About Versa 57

What is TSA?

In modern enterprise environments, users often access business-critical applications or the internet via shared Windows Terminal Servers, particularly in branch locations connected through Versa SD-WAN or IPsec-based SASE architectures. However, this shared infrastructure masks individual user identities, presenting a significant challenge for enforcing Zero Trust security. Enforcing user-specific security policies becomes challenging in multi-user environments such as Windows Terminal Servers, especially when multiple users share a single IP address. That's where **TSA** steps in.

By default, when multiple users connect through the same Windows Terminal Server host, VOS Appliance (SDWAN or SSE gateway) cannot distinguish one user from another, making user-based access control impossible.

Versa TSA Solves This By:

- Allocating a unique port range for each user session on Windows Terminal Server.
- Communicating this user-port mapping to the connected VOS Appliance.
- Letting the firewall track individual users, even if they share the same IP address.

This enables precise, per-user or per-group policy enforcement, just like in a typical single-user environment.

How It Works

1. TSA is installed and configured on the Windows terminal server.
2. TSA assigns users a dedicated port range as users log in.
3. TSA sends these mappings (user ↔ port range) to the Versa OS (VOS) devices using a Control Channel it maintains to the VOS Appliance.
4. The VOS Appliance creates a mapping table between IP, port, and user.
5. Security policies based on user identity or group membership are enforced, even for shared IP sessions.

Why It Matters

- You can enforce Zero Trust policies in shared desktop environments.
- Get clear visibility into who's doing what, even when using the same terminal server.

Why It Doesn't DO

- The TSA agent does not build any tunnel from Windows Server to the VOS Appliance
- The TSA agent does not control how user traffic is routed from Windows Server to VOS Appliance.

Versa TSA Use Cases

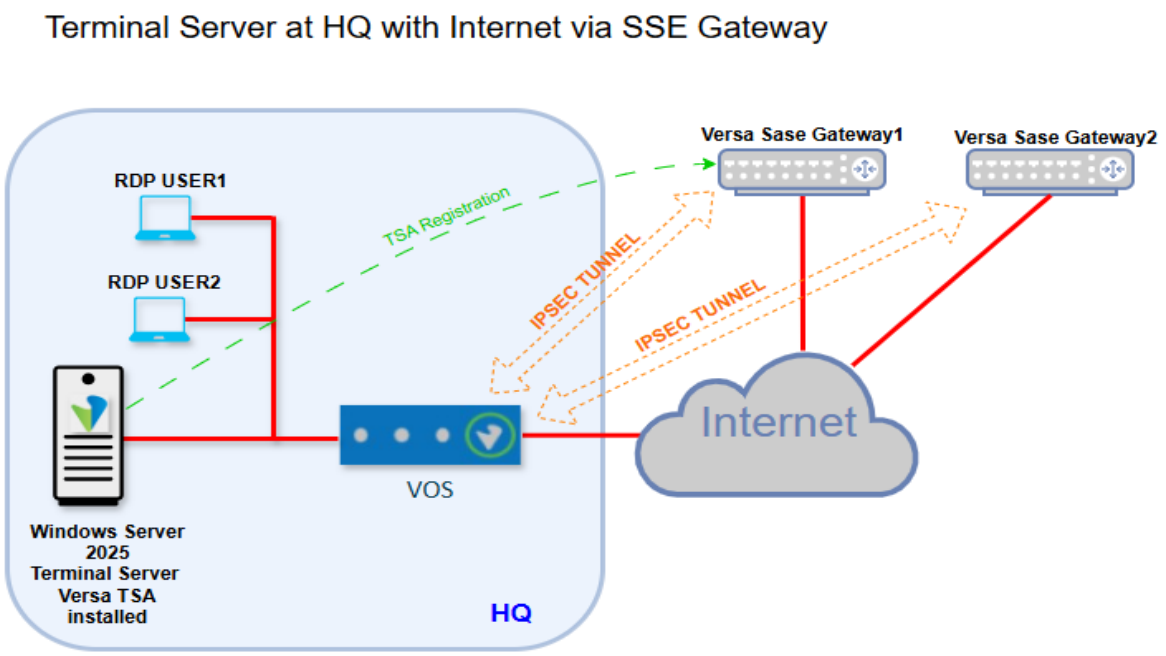
Internal Application Access: When multiple users connect to internal apps from a shared terminal server, all traffic appears to come from the same IP address. This makes enforcing access policies such as URL filtering, DLP, or CASB controls based on user identity or role impossible. Without that visibility, organizations can't reliably control access to sensitive systems, enforce segmentation, or track individual user activity.

Private Application Access: When multiple users access private applications through a shared environment such as a terminal server, enforcing Zero Trust Network Access (ZTNA) requires identifying users individually, rather than relying on shared attributes like IP addresses. Terminal Server Access (TSA) helps address this challenge by enabling user-level visibility and the ability to apply access control policies. For example, users with different access privileges can RDP into the same terminal server but receive access to private applications based on their identities.

We can also have a mixed case of Internet and Private applications access.

Scenario 1: Terminal Server at HQ with Internet via SSE Gateway

In this scenario, the Terminal Server is hosted at the customer's headquarters (HQ), data centre (DC), or branch office. Users connect remotely to this Terminal Server, and all internet-bound traffic is routed through a Secure Service Edge (SSE) Gateway for inspection and policy enforcement.



Connectivity Options

Traffic from the Terminal Server is routed to the SSE Gateway through the local branch using one of the following methods:

- Versa SD-WAN overlay
- Traditional site-to-site IPsec tunnel

The choice depends on the customer's existing network architecture. This connection provides a secure path for forwarding internet-bound traffic from the Terminal Server to the SSE infrastructure.

TSA Integration with SSE

To enable integration between the Terminal Server Agent (TSA) and the SSE Gateway, the following setup is required:

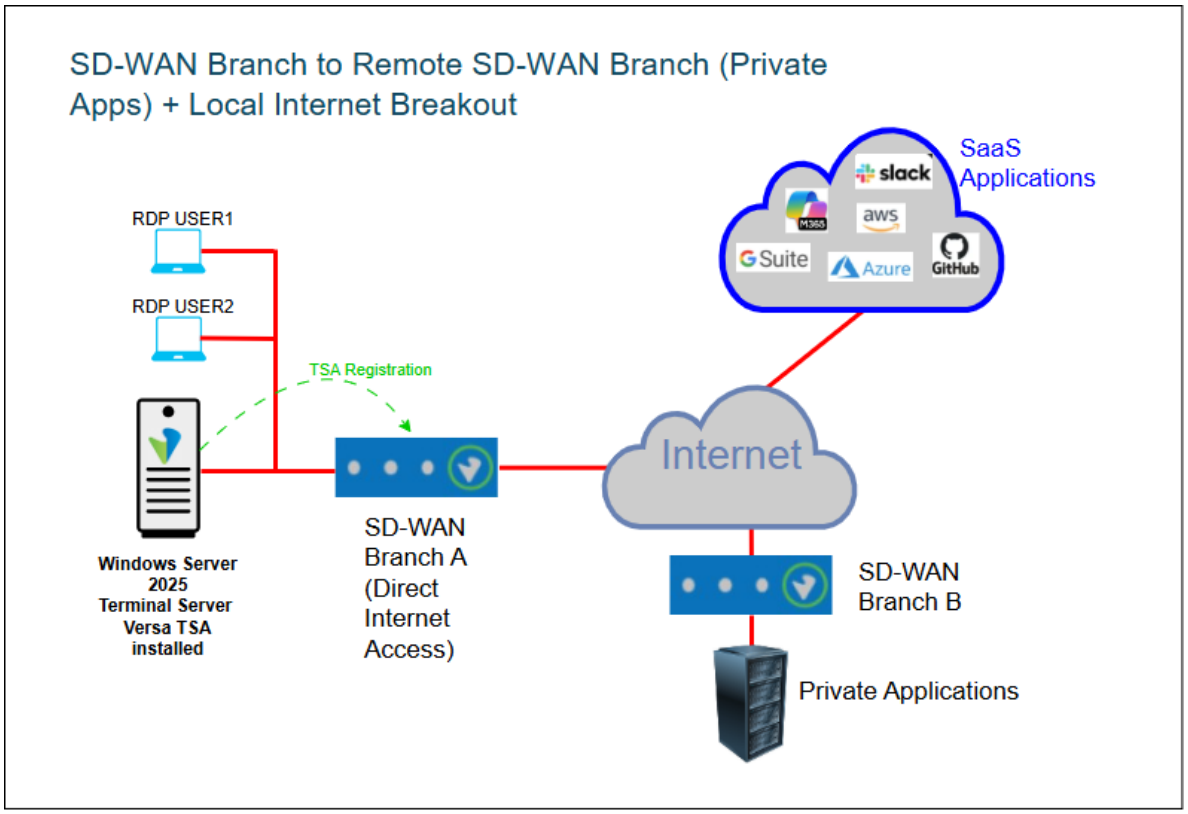
- **Pre-configured SSE Portal URL:** The SSE Gateway is pre-configured with a Portal URL/Captive Portal URL. The TSA agent uses this URL during the registration process.
- **TSA Agent Configuration:** The Versa TSA Agent, installed on the Terminal Server, is configured to communicate with the SSE Gateway using an SSE Portal URL.
- **Private IP Resolution:** The Captive portal URL or SSE Portal URL should resolve to the private IP address of the SSE Gateway. This ensures direct communication for user registration and updates over the SD-WAN overlay or IPsec tunnel to the SSE gateway.
- **Note**: The Portal URL can also resolve to a public IP and still support registration over TLS. However, resolving to a private IP is recommended for environments that require fully private communication.
- **Traffic Path Requirement**: Regardless of how the Portal URL resolves, a secure tunnel (SD-WAN or IPsec) to the SSE Gateway is still required to carry TSA client control traffic and user data traffic.
- **High Availability Support**: If multiple SSE Gateways are deployed for redundancy, the Portal URL's FQDN should resolve to both private IP addresses. This enables automatic failover and load balancing between gateways.

Scenario 2: SD-WAN Branch to Remote SD-WAN Branch (Private Apps) + Local Internet Breakout (LBO)

In this scenario, the Terminal Server is located at SD-WAN Branch A, where users connect remotely. These users access:

- Private applications hosted behind remote SD-WAN Branch B via Terminal Server
- The internet via Local Internet Breakout (LBO) at Branch A.

Connectivity between Branch A and Branch B is established through an SD-WAN overlay tunnel.



Why TSA Registration is Needed at Branch A

To accurately identify users accessing both private and public applications, TSA registration must occur at Branch A. This ensures that user identity is captured at the point where both types of traffic originate.

If the customer has multiple sites with local Terminal Servers and LBO, this setup should be replicated at each site to maintain consistent user identification and policy enforcement.

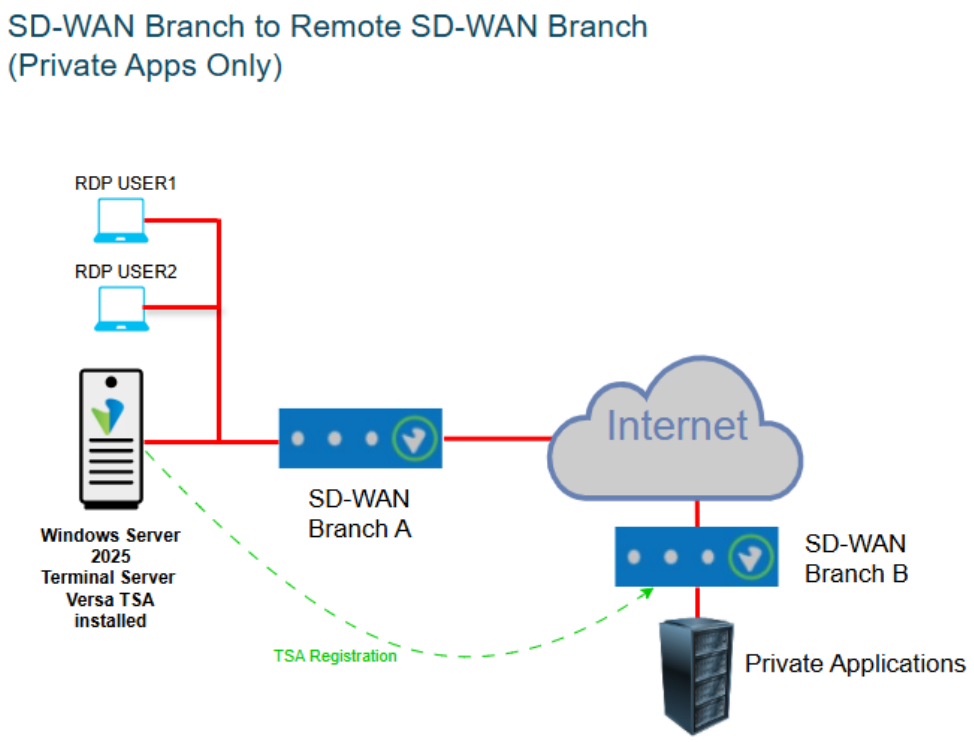
TSA Integration with Versa SD-WAN Branch

- **Routing-Instance for Captive Portal:** To ensure TSA registration on the captive portal does not break the URLF captive portal action, we will create a separate TSA routing instance, which will be used for registration of TSA agents in Branch A. A paired TVI will be configured between the TSA routing instance and Enterprise/LAN-VR. A default route will be added in the TSA routing instance pointing to the Enterprise/LAN-VR TVI IP.
- **TSA Captive Portal Configuration:** SD-WAN Branch A must be configured with a Captive Portal for TSA registration in the TSA routing instance, and the FQDN will be mapped to the TVI IP in the TSA routing instance.
- **TSA Agent Setup:** The Versa TSA Agent, installed on the Terminal Server at Branch A, is configured to communicate with the local SD-WAN branch using a Captive Portal URL.
- **Private IP Resolution:** The Captive Portal URL should resolve to the private TVI IP address of the TSA routing-instance Branch A.

Scenario 3: SD-WAN Branch to Remote SD-WAN Branch (Private App Access Only)

In this scenario, the Terminal Server is located at SD-WAN Branch A, where users connect remotely via Remote Desktop. These users access private applications hosted behind remote SD-WAN Branch B. No internet access is allowed through Branch A.

Connectivity between Branch A and Branch B is established via an SD-WAN overlay tunnel.



Why TSA Registration is Needed at Branch B

Since the requirement is to identify users only for private application access, TSA registration should be performed at Branch B. This ensures that user identity is captured at the point where private applications are hosted and accessed.

If the customer has multiple sites with local Terminal Servers, all of them can register to Branch B for consistent user identification and access control.

Note: If Local Internet Breakout (LBO) is also configured at Branch B, access control policies for internet-bound traffic can be enforced there as well for all remote branches.

TSA Integration with Versa SD-WAN Branch

To enable TSA integration at Branch B, the following configuration is required:

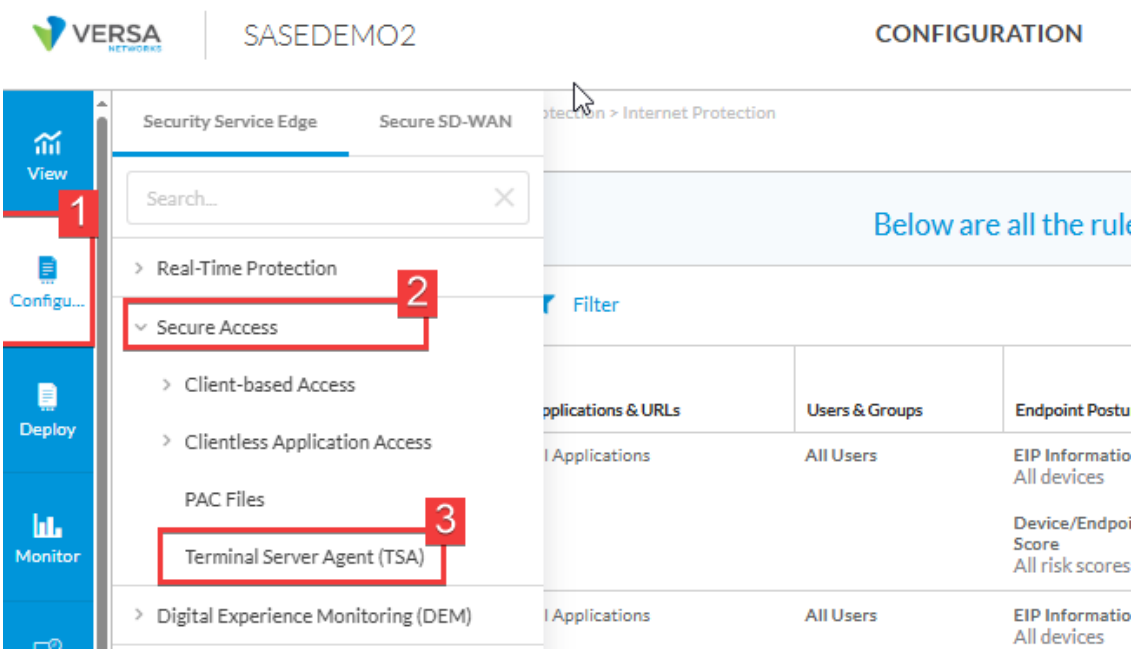
- **Routing-Instance for Captive Portal:** To ensure TSA registration on the captive portal does not break the URLF captive portal action, we will create a separate TSA routing instance, which will be used for registration of TSA agents in Branch B. A paired TVI will be configured between the TSA routing instance and Enterprise/LAN-VR. A default route will be added in the TSA routing instance

pointing to the Enterprise/LAN-VR TVI IP. The TVI IP will be redistributed in SDWAN BGP as all Direct routes are default redistributed.

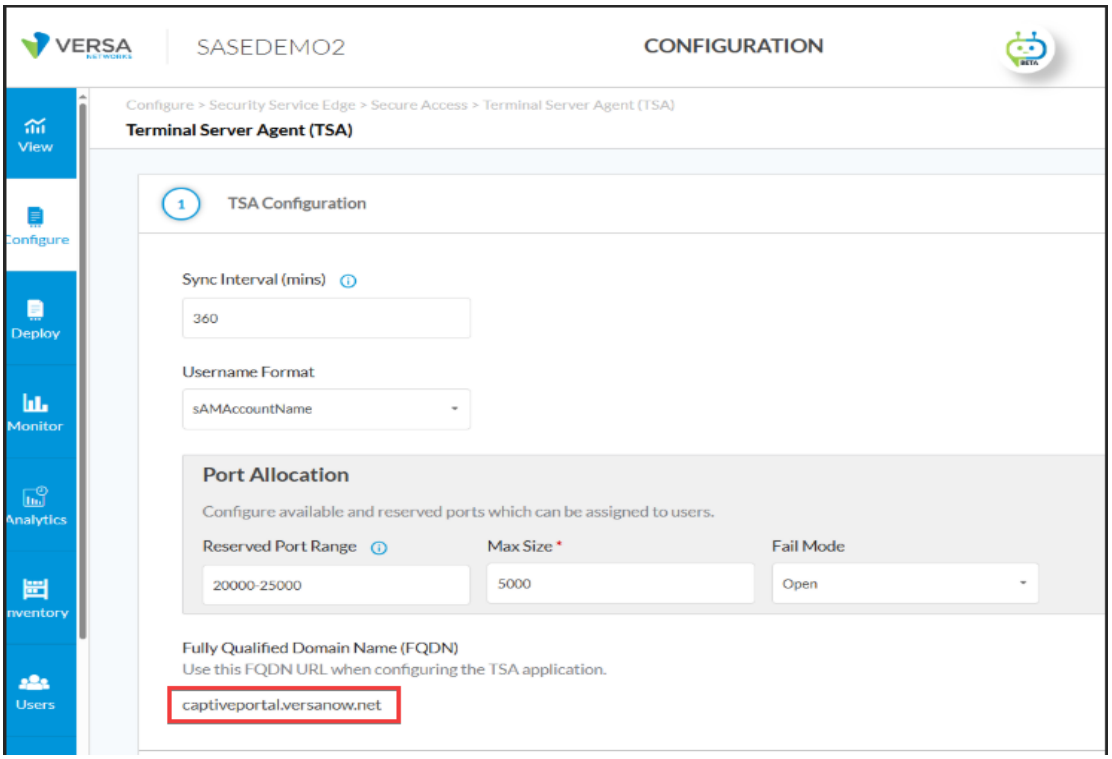
- **Captive Portal Configuration**: SD-WAN Branch B must be configured with a Captive Portal for TSA registration in the TSA routing instance, and the FQDN will be mapped to the TVI IP in the TSA routing instance.
- **TSA Agent Setup**: The Versa TSA Agent, installed on the Terminal Server at Branch A, is configured to communicate with SD-WAN Branch B using a **Captive Portal URL**.
- **Private IP Resolution**: The Captive Portal URL should resolve to the **private LAN IP address** of the Versa Operating System (VOS) at SD-WAN Branch B.

Configuration Steps: Scenario 1

1. **Configure the TSA profile in Concerto**
   - The first step is to configure the Terminal Server Agent (TSA) in Concerto under the specific tenant (in this case, SASEDEMO2).



   - FQDN highlighted here can either be used for TSA agent registration or the SSE portal FQDN can also be used, explained further in Step 4.

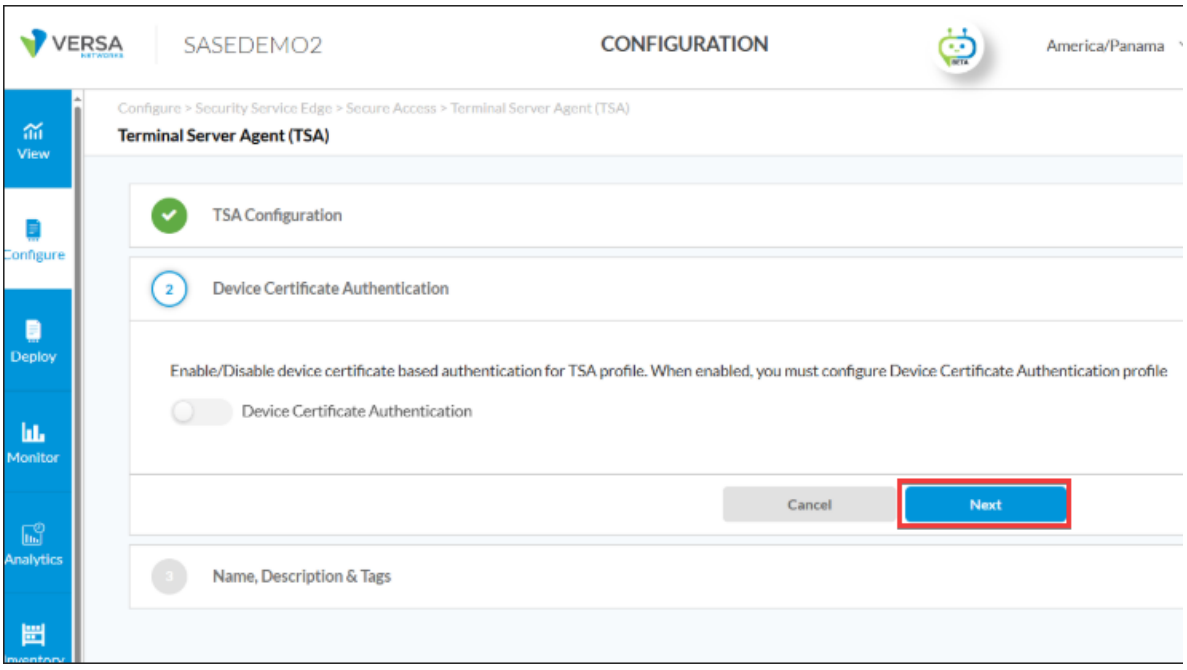


- Port Allocation (Group of Fields)
  - **Sync Interval**: Enter how often, in minutes, to synchronise the configuration with the TSA.
  - **Username Format**: Select the username format to have the TSA recognise
    - **userPrincipleName**—User principal name. A user principal name consists of a prefix (user account name), followed by the @ symbol and a suffix (DNS domain name). For example, someone@my-company.com.
    - **sAMAccountName**—The sAMAccountName attribute is a login name that supports clients and servers from previous Windows versions, for backwards compatibility, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.
  - **Reserved Port Range:** Enter the reserved port allocation range for user sessions. The value must be entered into the Port-Start - Port-End format, and the port range must have a minimum of 10000 ports. For example, enter 1024-10000 to start port 1024 and end port 10000. Range: 1024 through 65535
  - **Maximum Size (Required):** Enter the maximum port allocation size for each user. The maximum size must be a multiple of the start size. Range: 0 through 65535. Default: 5000
  - **Fail Mode:** Select the traffic mode if the TSA server connection fails,
    - **Close**—Deny traffic if the TSA server connection fails. This is the default state.
    - **Open**—Allow traffic if the TSA server connection fails.
  - **Fully Qualified Domain Name (FQDN):** Use this FQDN URL when configuring the TSA application

- Example Scenario

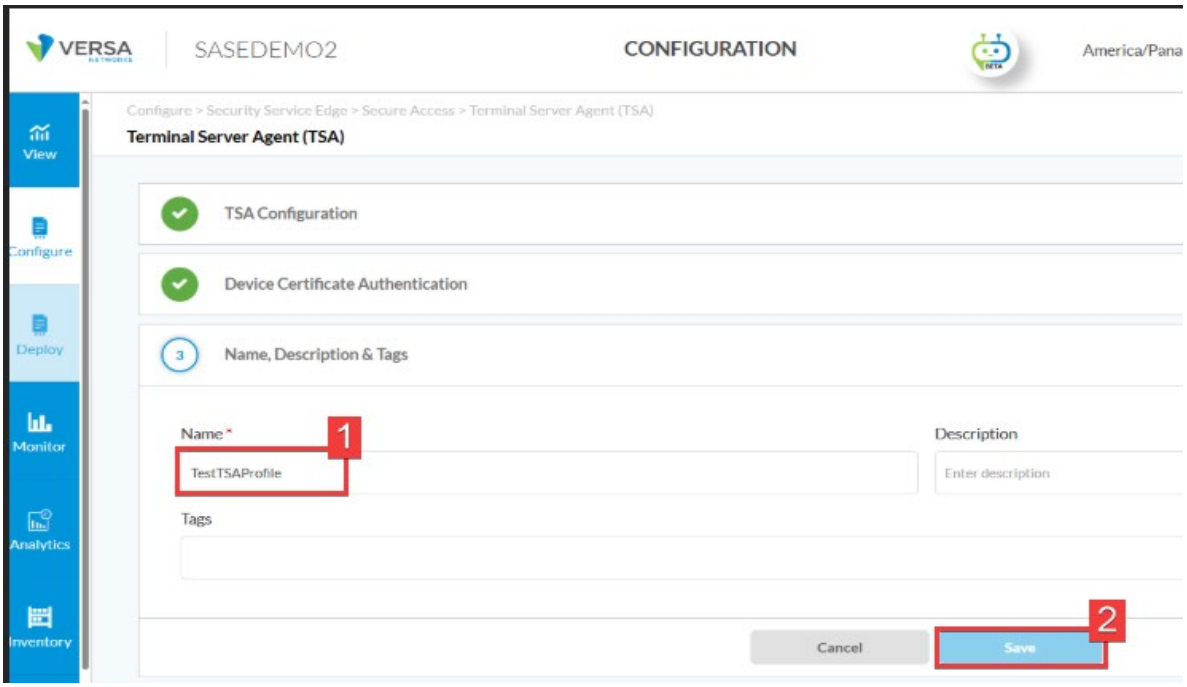
Item	Value
Total Users	4
Max Ports per User	5000
Total Ports Required	4 × 5000 = **20,000**
Reserved Port Range	**10000-30000**
Fail Mode	Close (recommended)

- In the Device Certificate Authentication section, select the toggle to enable or disable device certificate-based authentication for the TSA profile. When enabled, you must configure a device certificate authentication profile.
- In this case, we continue without Device Certificate Authentication.

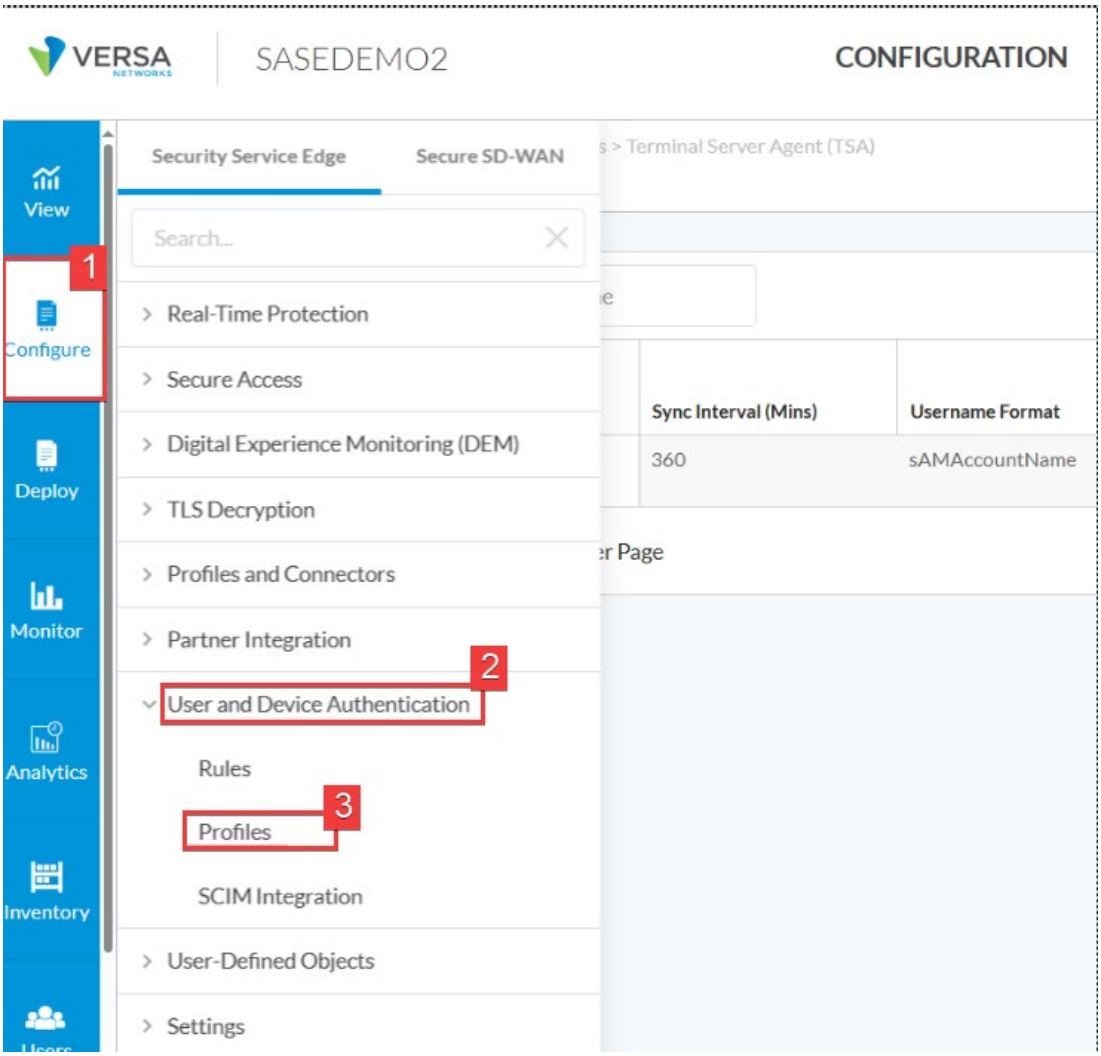


- Type in the Name (Required), Description & Tags section for the profile and save it.

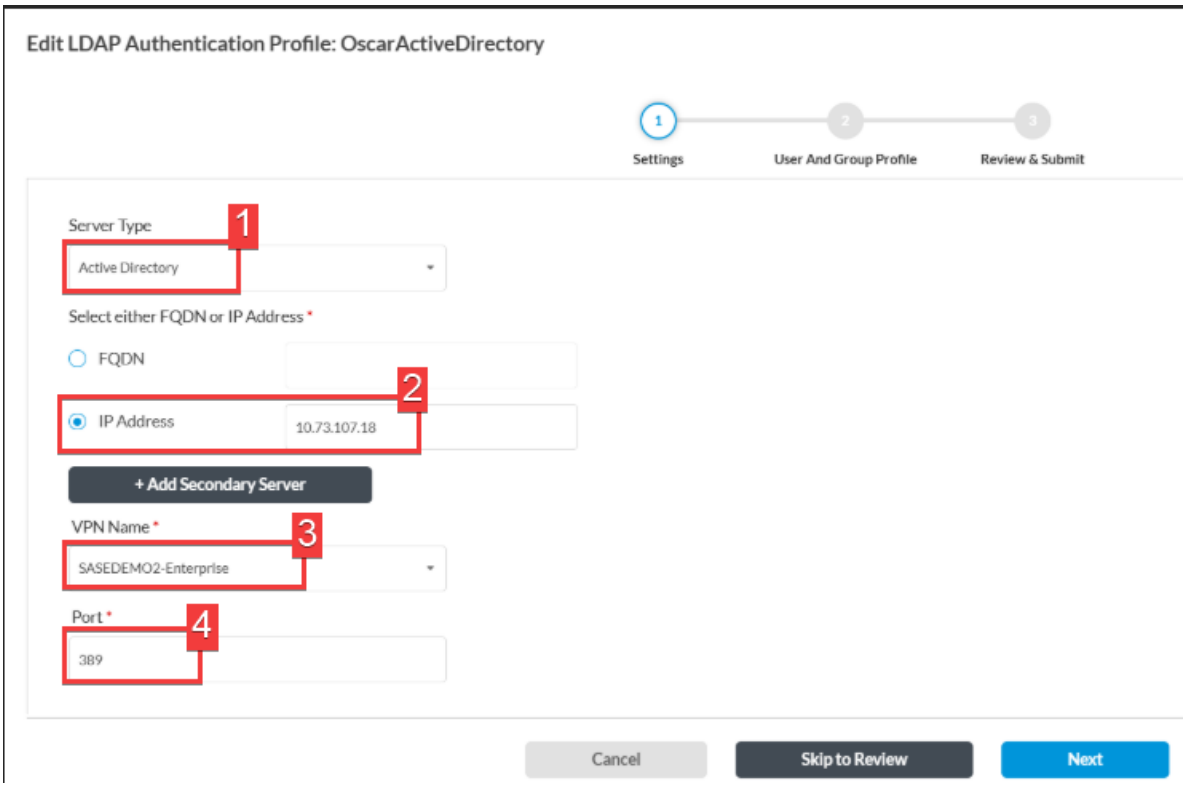
NOTE: *Only one TSA profile can be configured in the Concerto per tenant.*



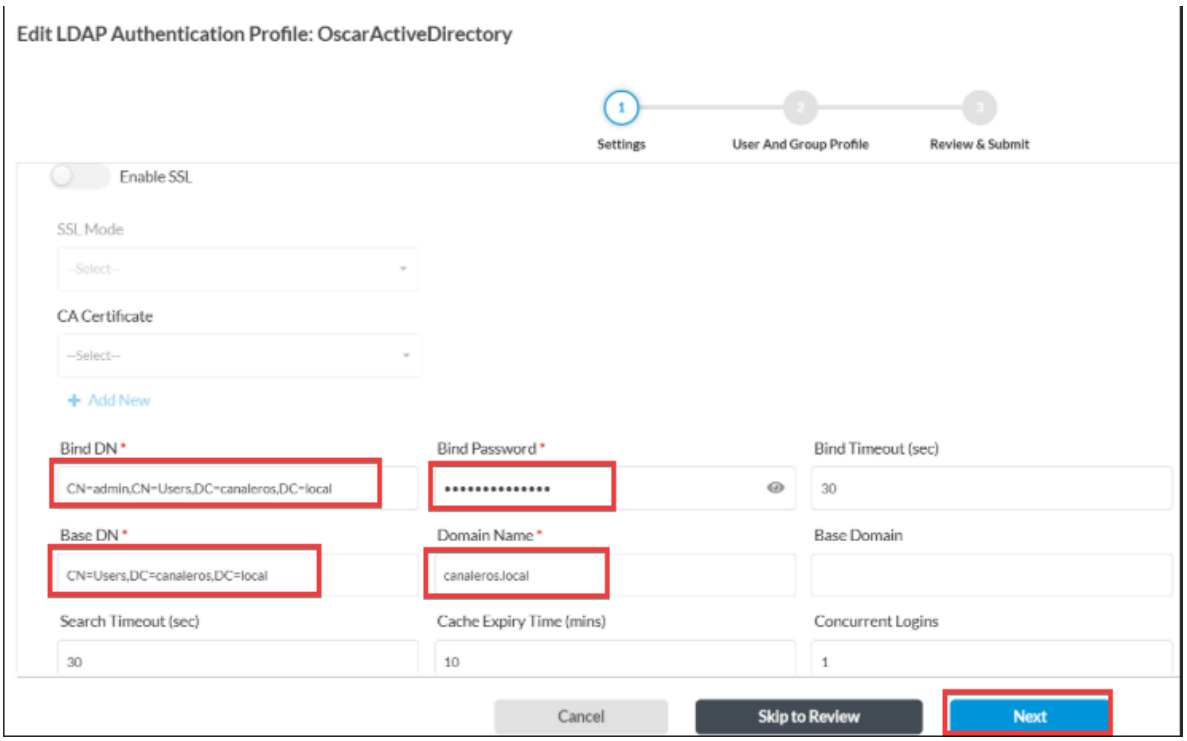
2. **Configure the user's authentication profile.**
    - Create a user authentication profile to match remote desktop users (in this case, Active Directory).



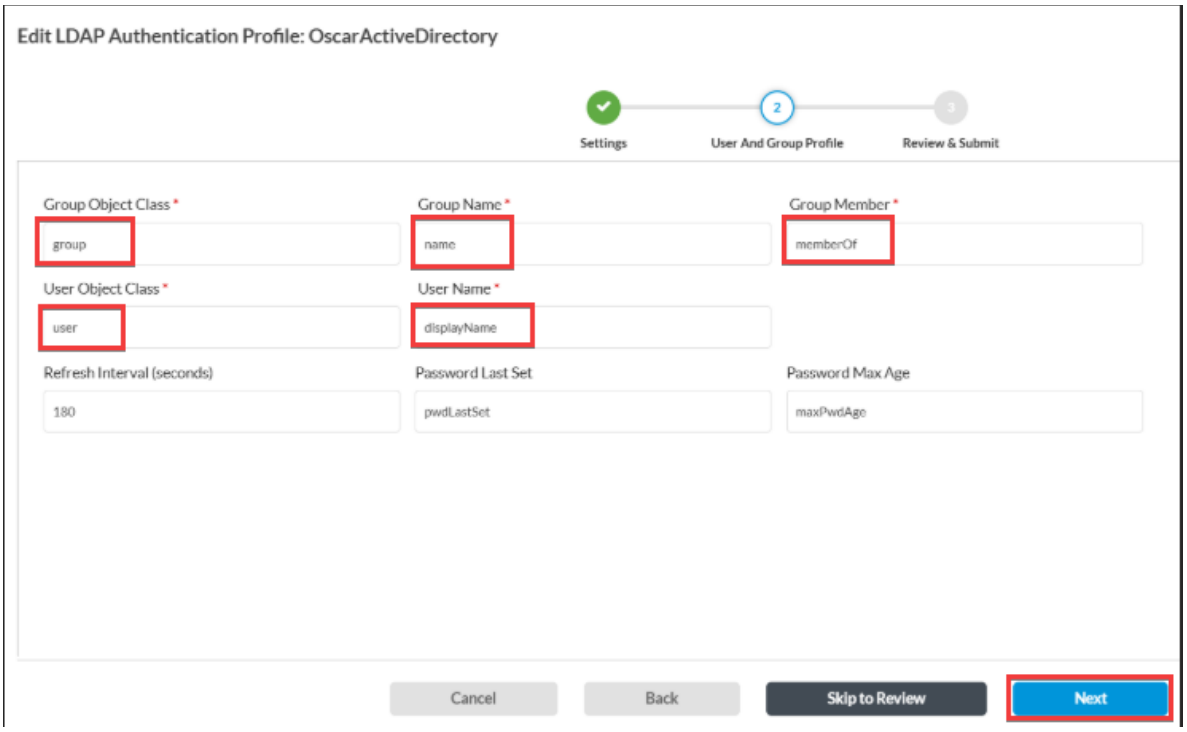
- Fill in the information of the Active Directory Server



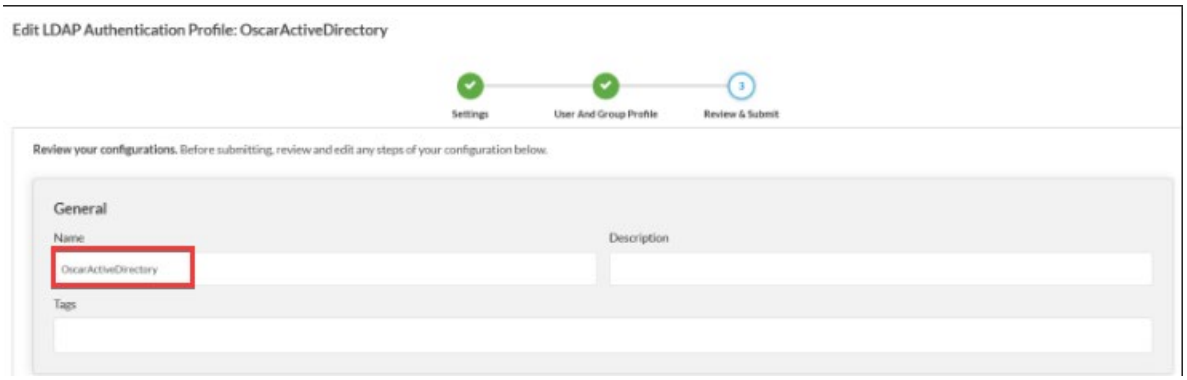
- Continue with the bind data information to log in to the Active Directory



- Add the groups and usernames information of the users from Active Directory

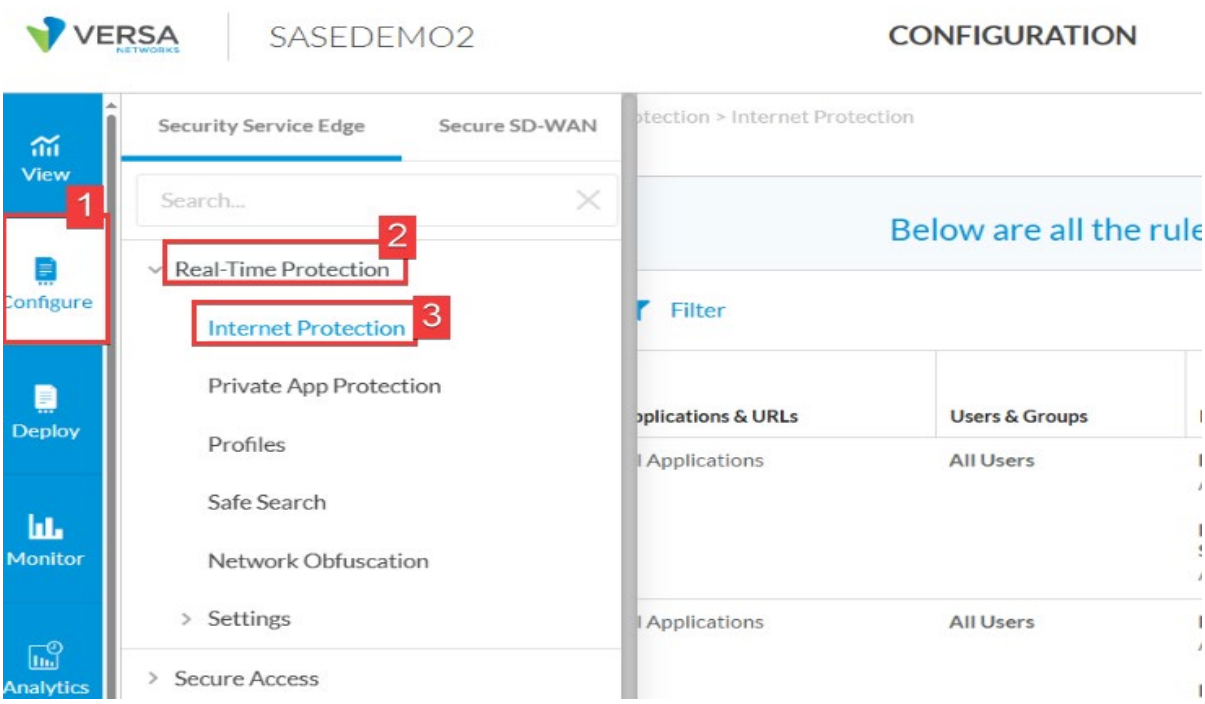


- Fill in a name for the authentication profile.

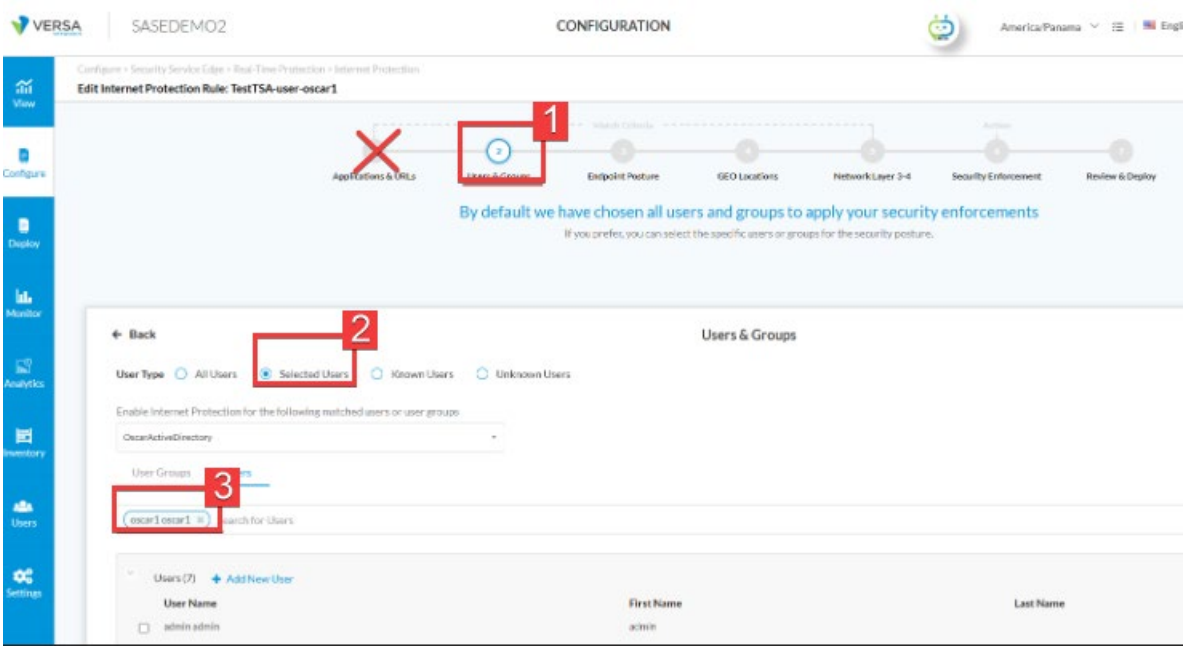


3. Create Security Policies

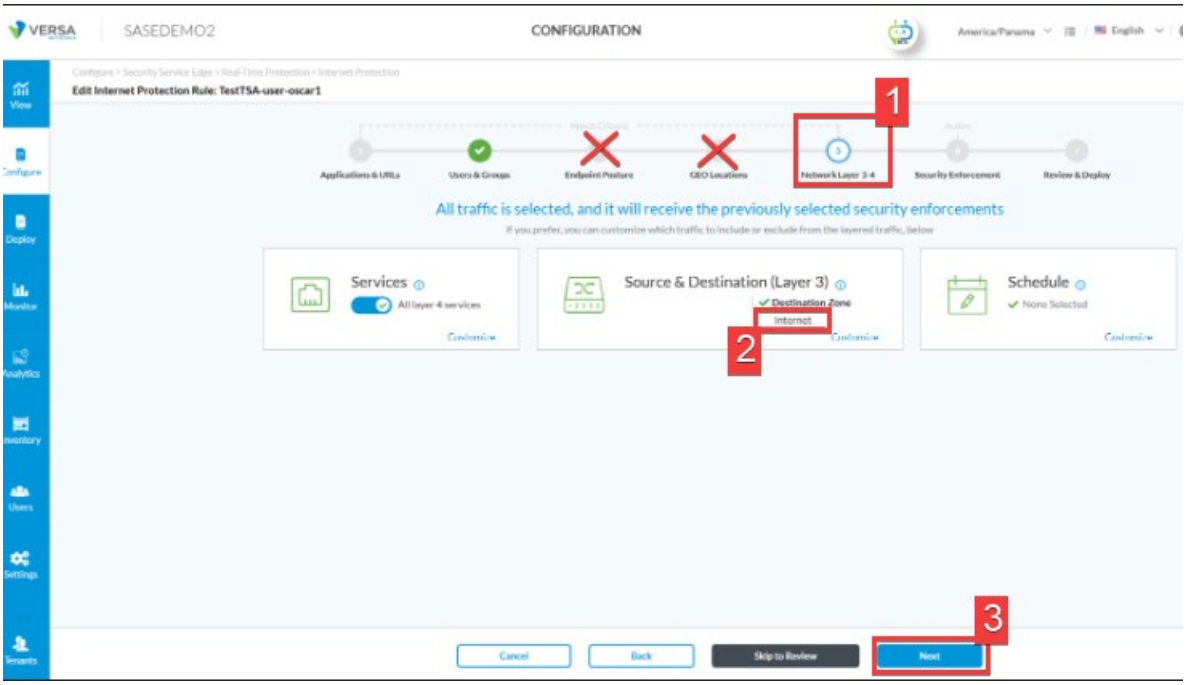
- Add a security rule to filter the required traffic.



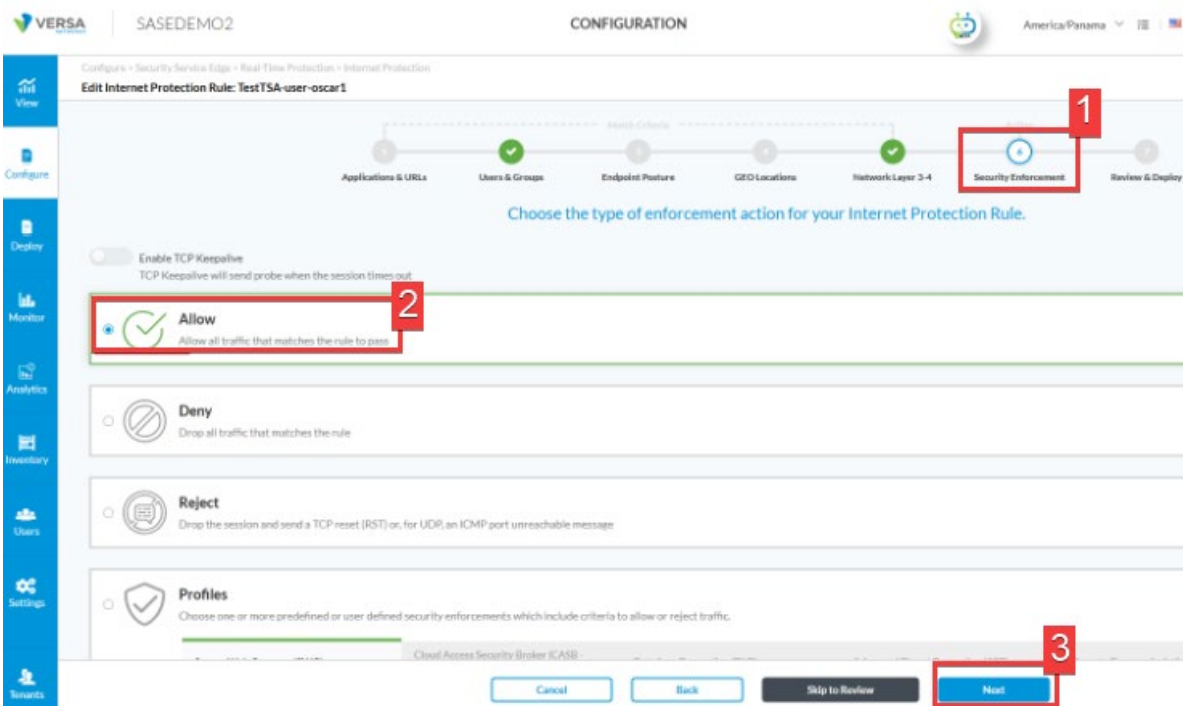
- In this case we selected Active Directory profile and selected user ”oscar1”



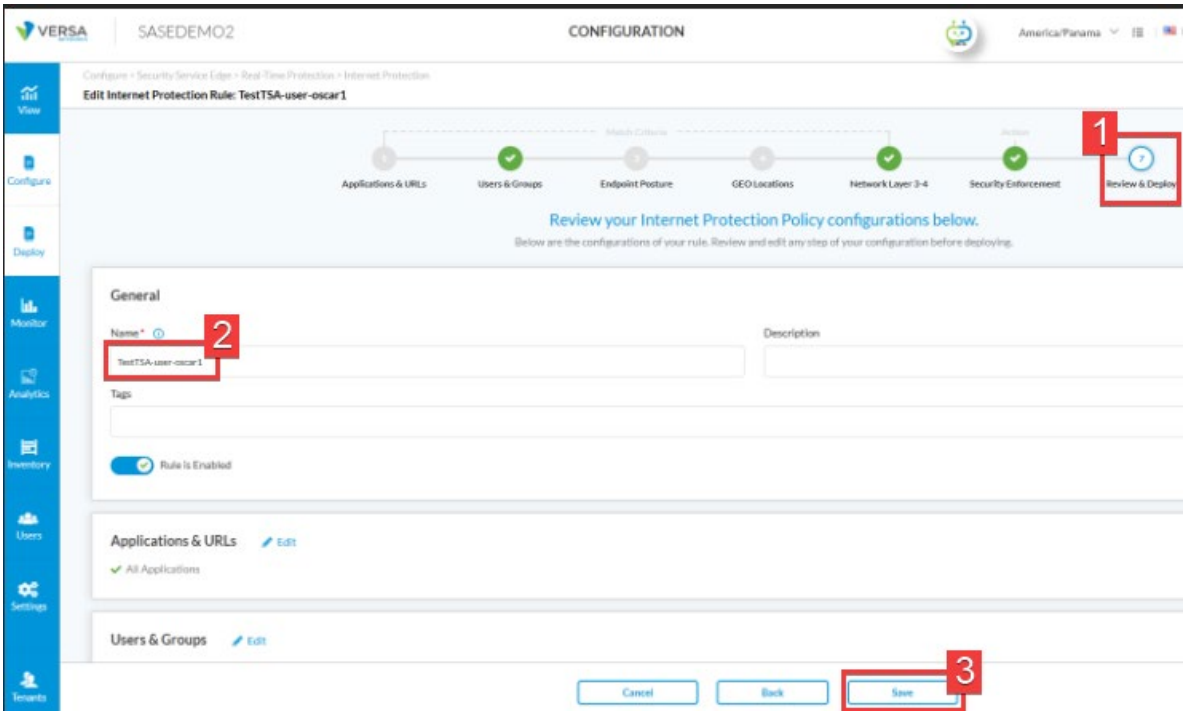
- Matched all services with Internet as destination.



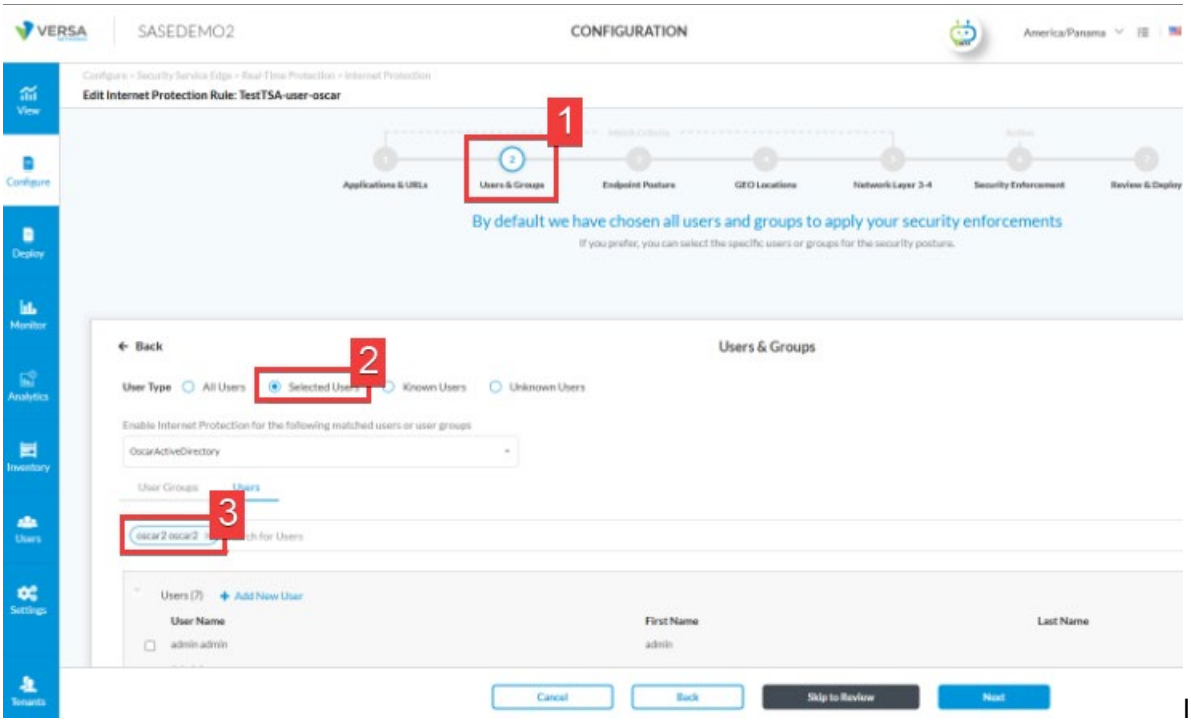
- Allow the traffic.

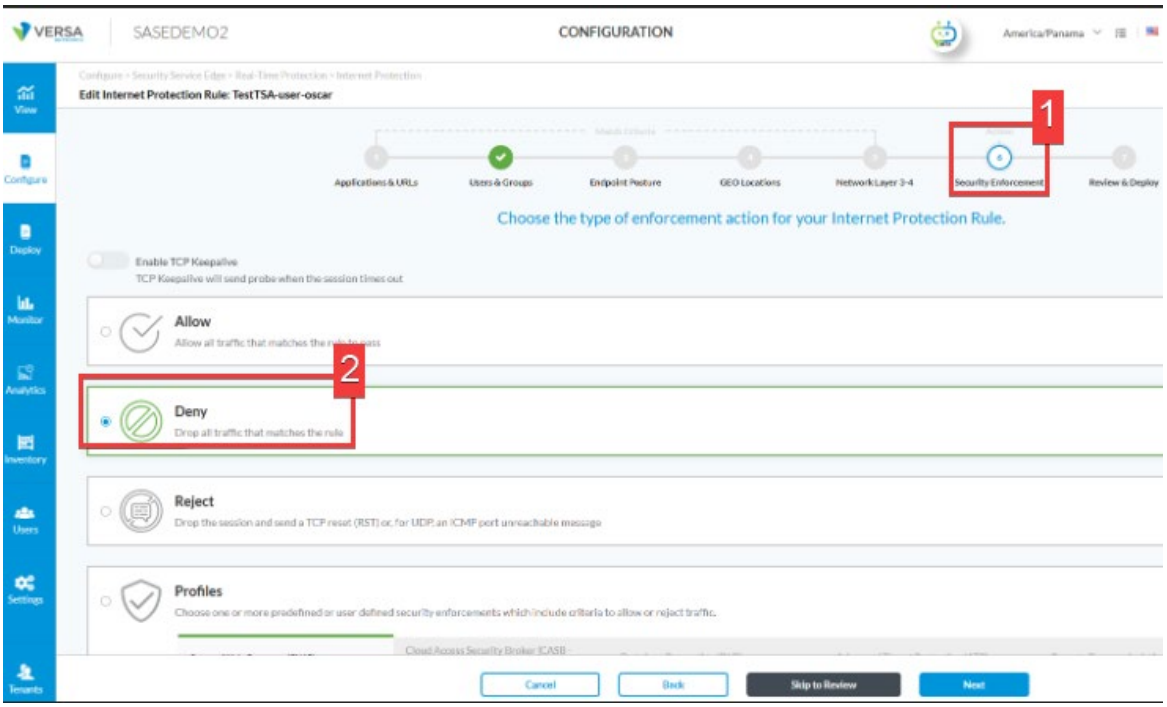


- Name the rule, save the configuration, and publish it to the SSE gateways.

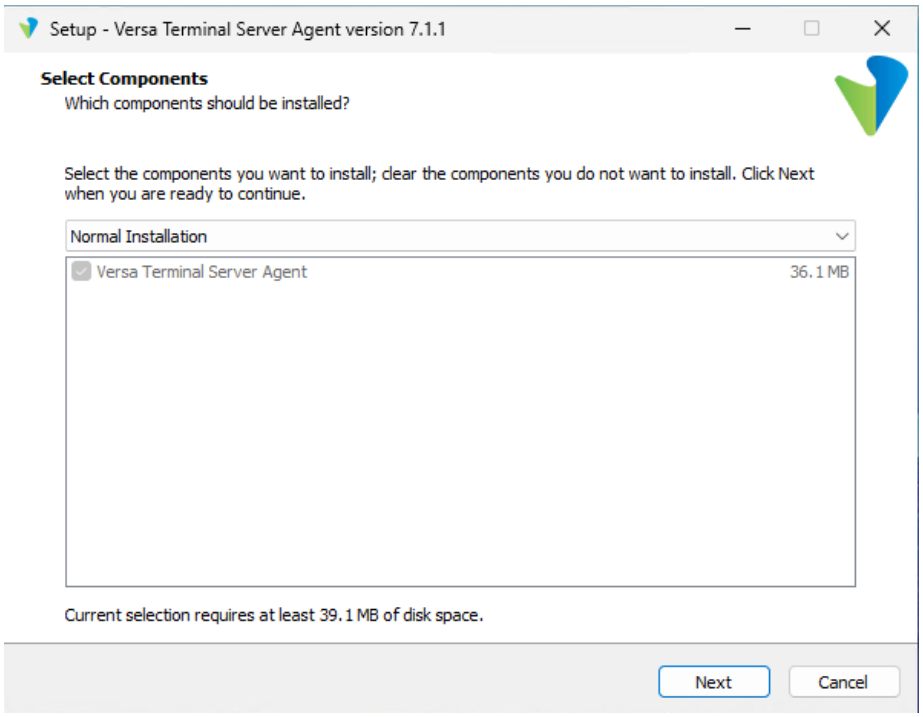


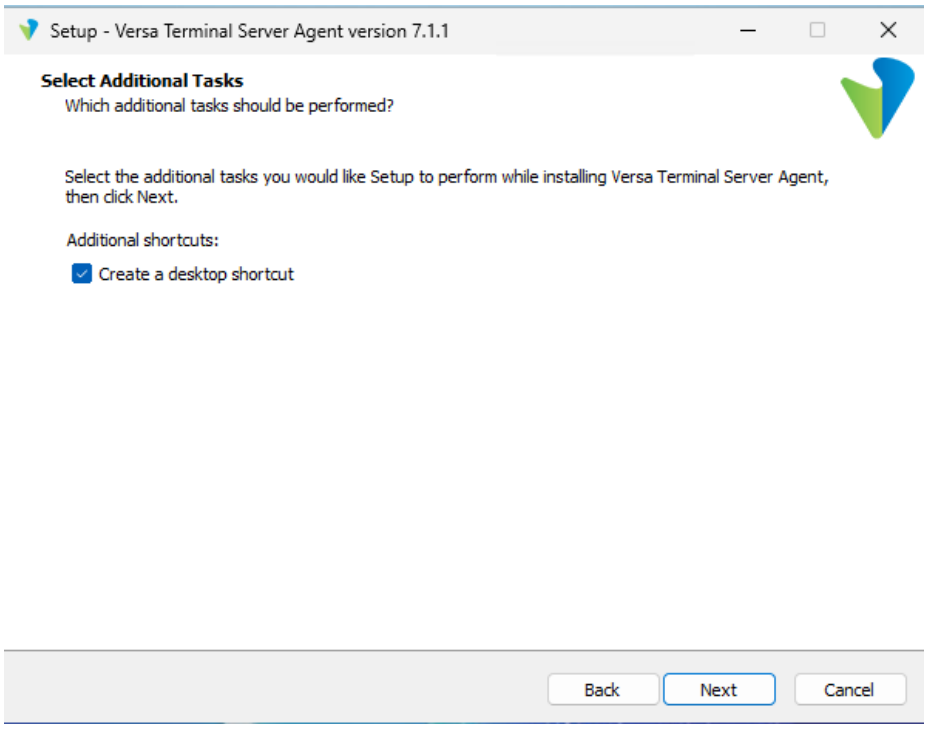
- Similarly, you can create a policy for other user connectivity via Terminal Server. Example this policy is for user" oscar2". The enforcement is to deny traffic.

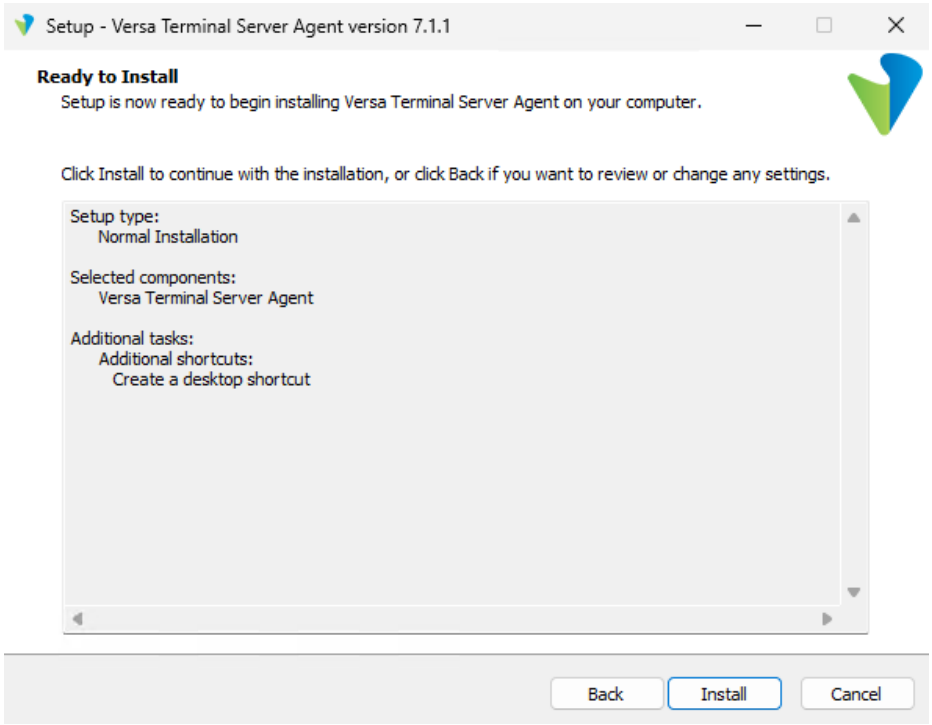




4. **TSA Agent Installation and Configuration Steps**
   - Generate a self-signed End Entity certificate from the SASE gateway, using the CA that´s already generate while setting up the SASE gateway.
   - Export the SASE Gateways or SDWAN device CA certificate and install it in the Windows Terminal Server in Trusted Root Certificate Authorities, reference Steps: Link
   - Install the Versa TS Agent in the Windows Terminal Server.







5. **FQDN for TSA Agent.**

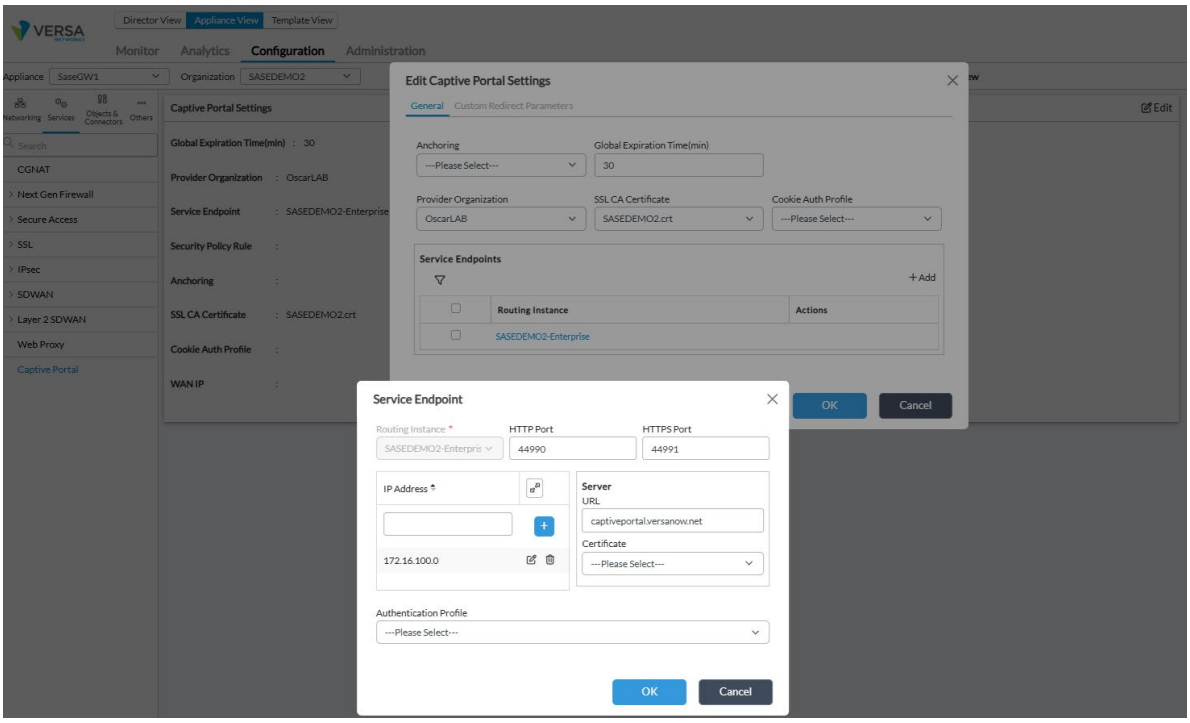
   We propose two options here.

   - Use FQDN displayed in SSE Portal during TSA profile creation and create a entry in your local network DNS server to resolve private TVI (usually the first IP of SASE client IP pool). This IP address will be reachable over the SDWAN Overlay tunnel or IPsec tunnel (in case of non-sdwan site)

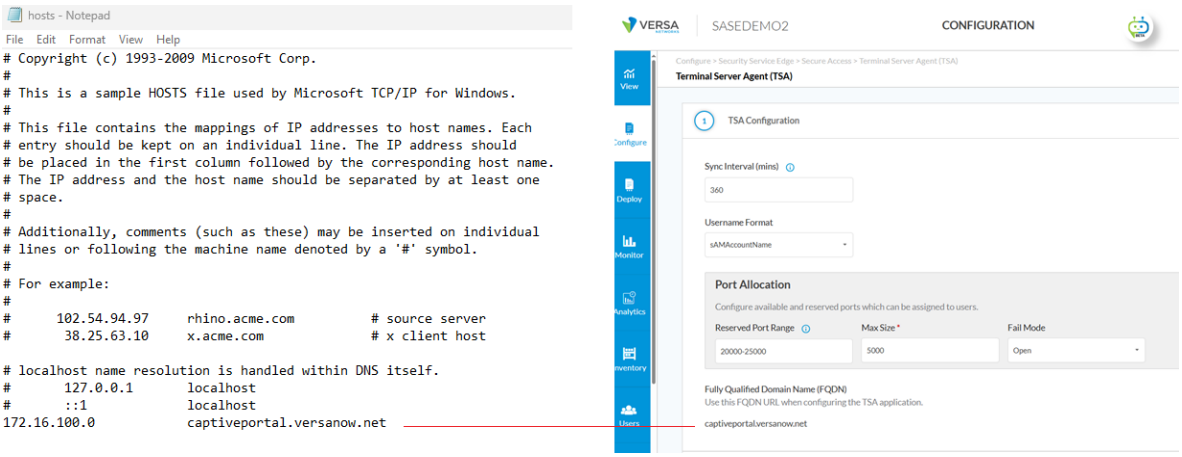
- Use SSE Portal FQDN (same as used by SASE client), this will default resolve to public IP of SASE gateways. TSA client will connect to SSE gateways via Internet.

Make sure the Terminal Server can resolve the FQDN URL with the TVI interface assigned to the SSE Gateway VPN pool either by a DNS server or with a manual local host entry. In this case, a local host entry was used to resolve the URL with the TVI interface IP address shown in the next Image.

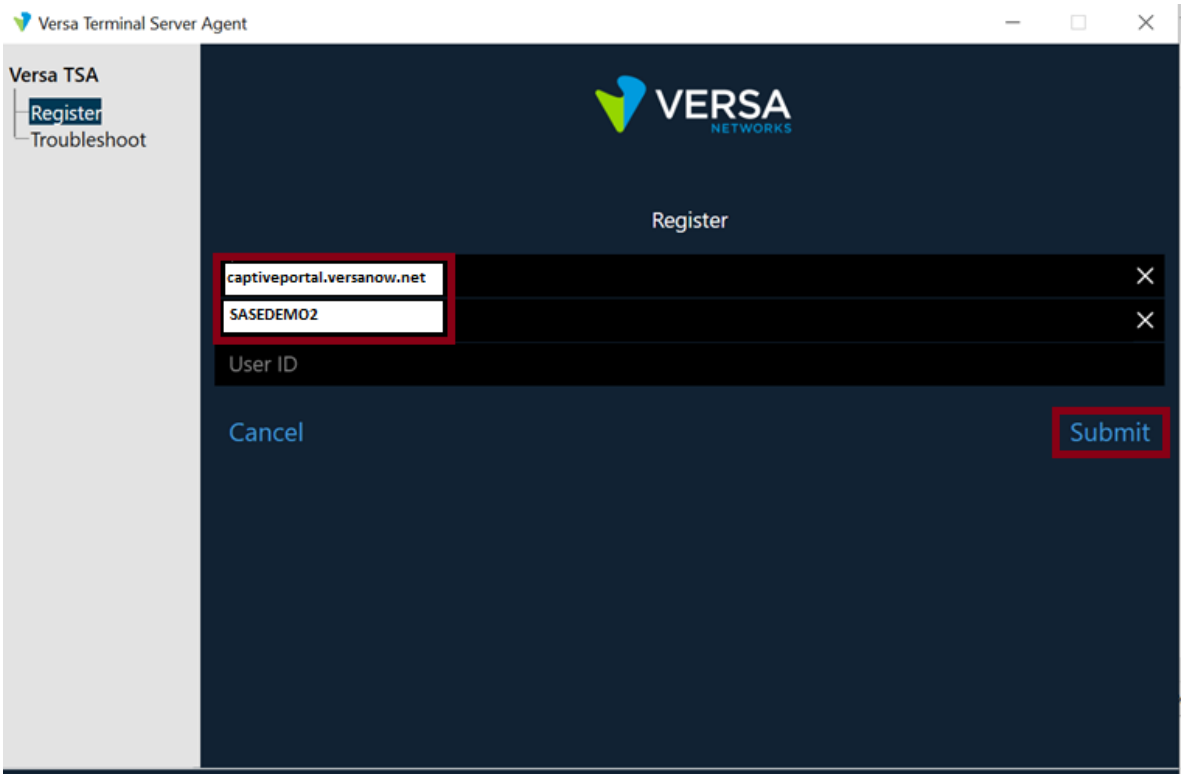
Below are the captive portal URL and its mapping to the private ip, viewed by the Director.



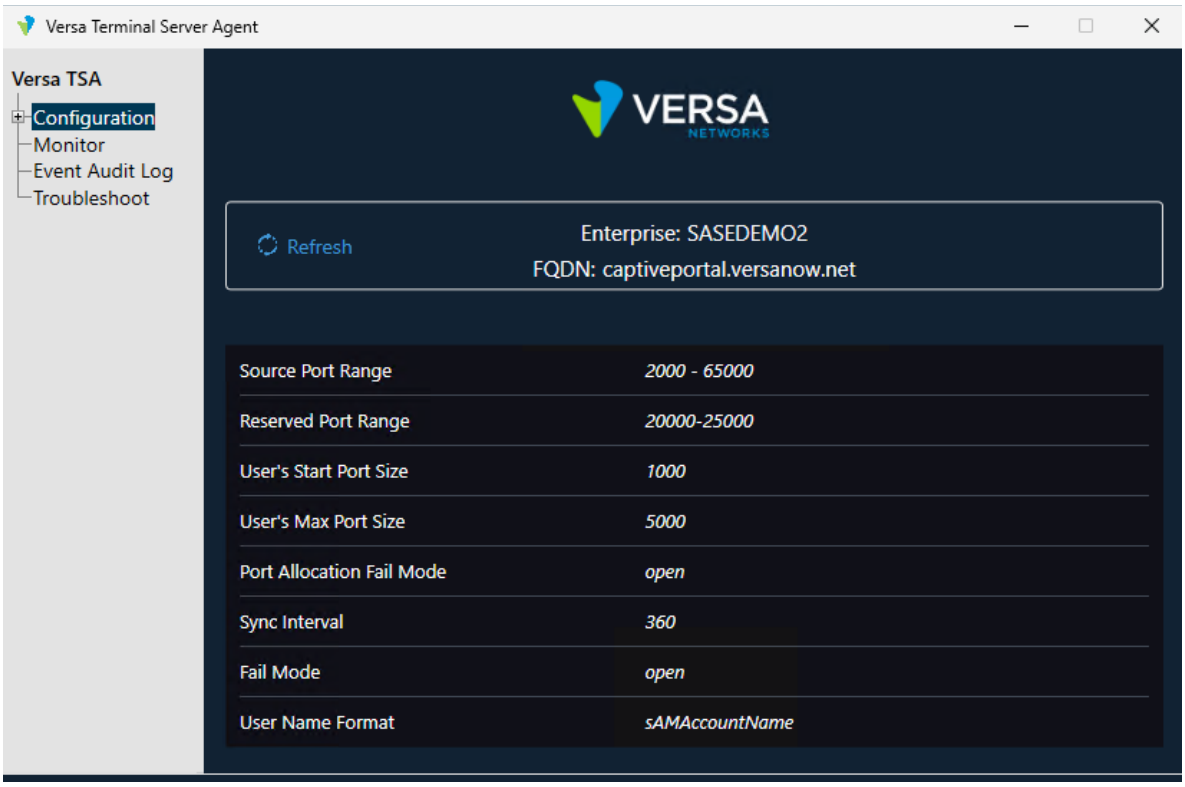

```
admin@SaseGW1-cli> show interfaces brief | tab
NAME          MAC                OPER  ADMIN  TENANT  VRF                 IP
-------------------------------------------------------------------------------------------
eth-0/0       52:0a:49:6b:07:01  up    up     0       global              10.73.107.7/16
                                                                         fe80::500a:49ff:fe6b:701/64
eth-0/1                          down  up     0       global
lt-1/2        n/a                up    up     -       -
lt-1/2.0      n/a                up    up     2       INET-Transport-VR   169.254.128.2/31
lt-1/3        n/a                up    up     -       -
lt-1/3.0      n/a                up    up     4       SASEDEMO2-Enterprise 169.254.128.3/31
ptvi1025      n/a                up    up     2       OscarLAB-Control-VR 10.30.0.0/32
ptvi1035      n/a                up    up     4       SASEDEMO2-Control-VR 10.30.0.2/32
tvi-0/2       n/a                up    up     -       -
tvi-0/2.0     n/a                up    up     2       OscarLAB-Control-VR 10.30.0.4/32
tvi-0/22      n/a                up    up     -       -
tvi-0/22.0    n/a                up    up     4       SASEDEMO2-Control-VR 10.30.0.4/32
tvi-0/23      n/a                up    up     -       -
tvi-0/23.0    n/a                up    up     4       SASEDEMO2-Control-VR 10.30.0.5/32
tvi-0/3       n/a                up    up     -       -
tvi-0/3.0     n/a                up    up     2       OscarLAB-Control-VR 10.30.0.5/32
tvi-0/602     n/a                up    up     -       -
tvi-0/602.0   n/a                up    up     2       INET-Transport-VR   169.254.0.2/31
tvi-0/603     n/a                up    up     -       -
tvi-0/603.0   n/a                up    up     2       OscarLAB-LAN-VR     169.254.0.3/31
tvi-1/103     n/a                up    up     -       -
tvi-1/103.0   n/a                up    up     4       SASEDEMO2-Enterprise 172.16.100.0/32
vni-0/0       52:0a:49:6b:07:02  up    up     -       -
vni-0/0.0     52:0a:49:6b:07:02  up    up     2       INET-Transport-VR   10.73.107.12/16

[ok][2025-08-06 11:35:17]
admin@SaseGW1-cli>
```



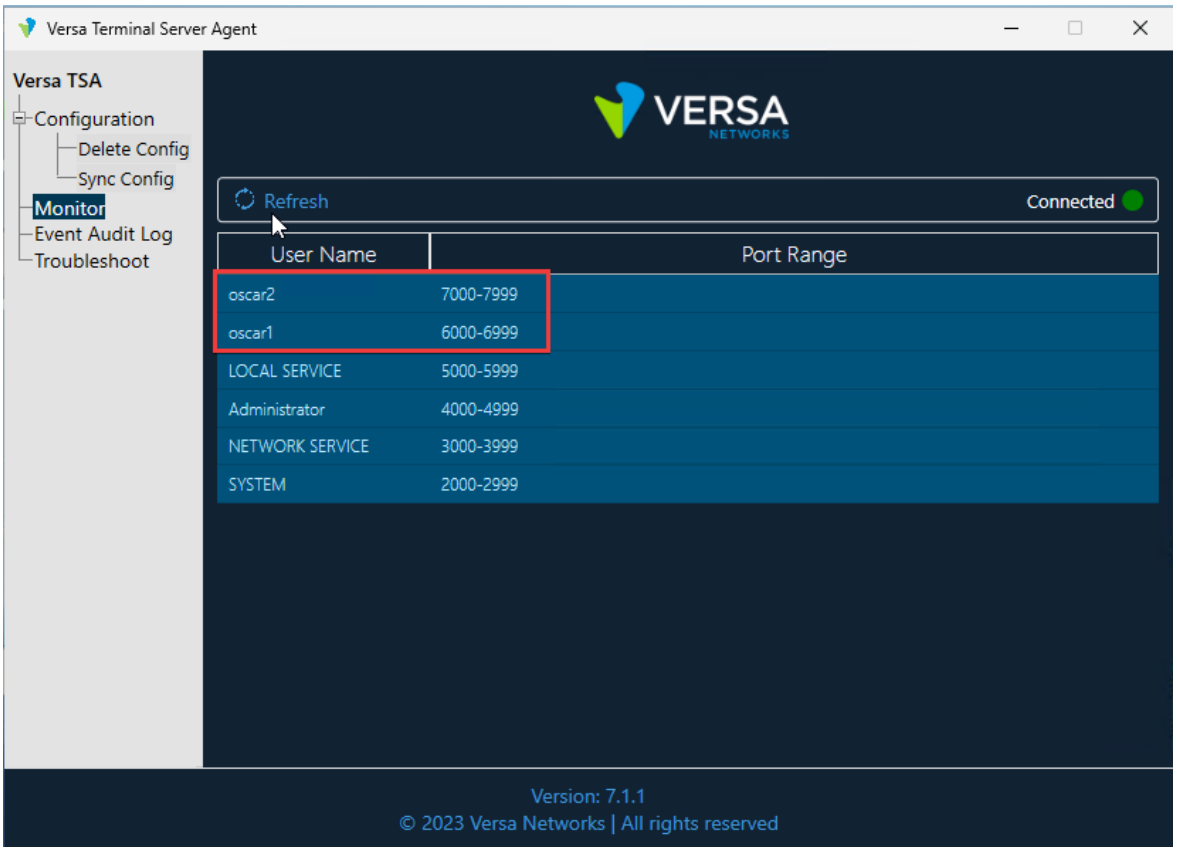
6. **Register the TS Agent to the SASE Gateway:**
   - Open the Versa TSA software installed in the Remote Desktop server and select Register. Fill in the captive portal URL, the Tenant, and the Username from the active directory that will be used to register to the SSE Gateway



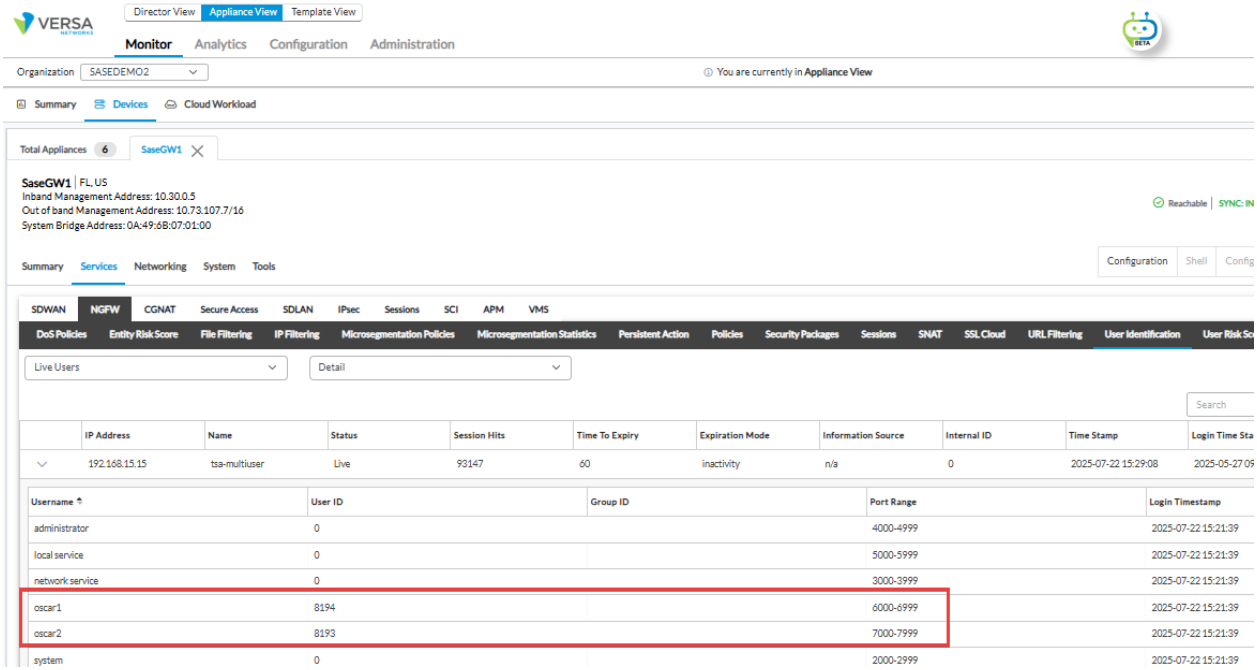
   - Once registered, the Configuration tab will show settings acquired from the TSA Profile.



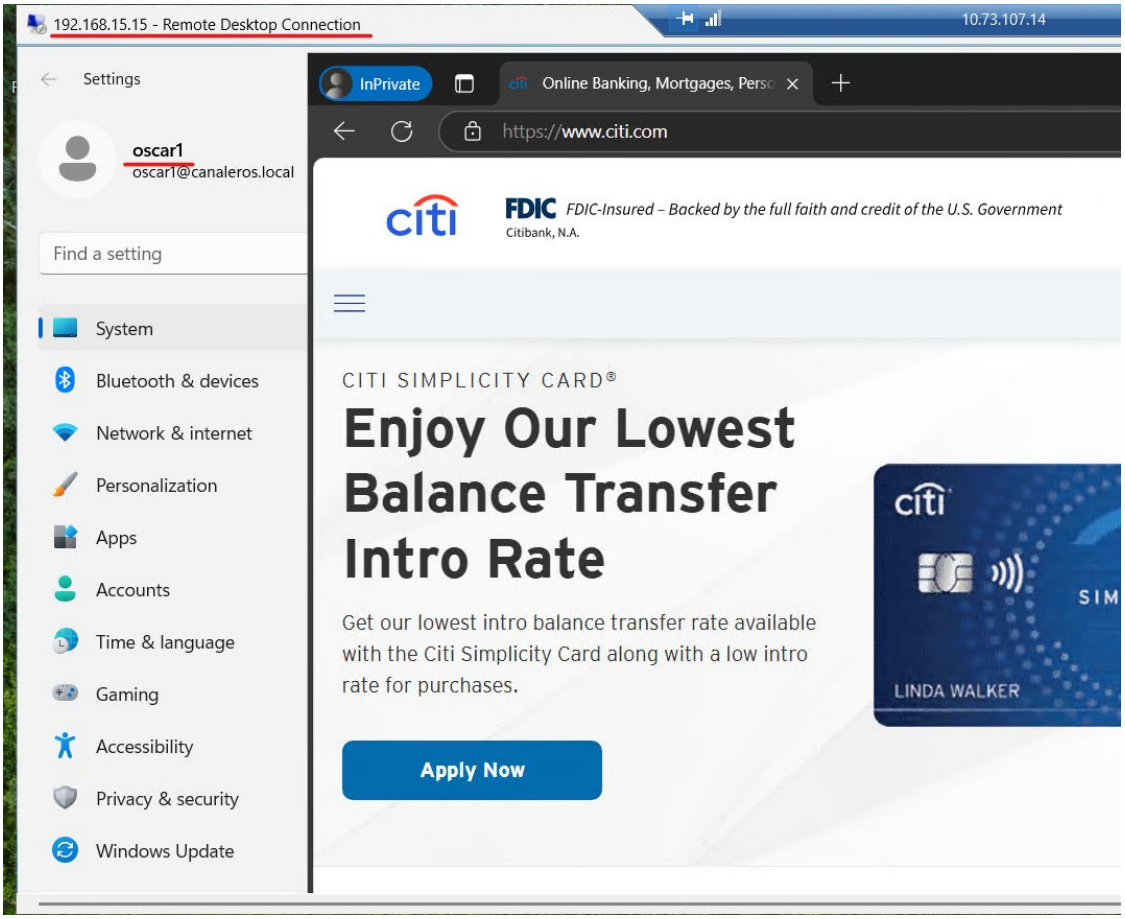
7. **Testing TSA connection**
   - In this case, there are two users (oscar1 and oscar2) connected to Terminal Server. Notice that the TSA monitor tab can identify both users, and it shows the port range allocated to each user.



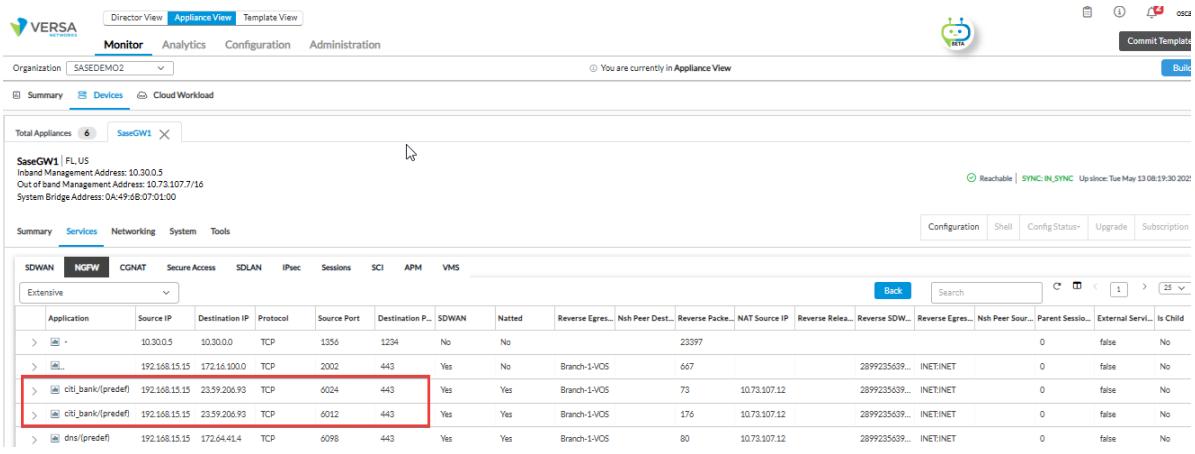
- TSA user-mapping in the SASE gateway. The users are visible through the GUI of the SSE Gateway monitor tab in Director.



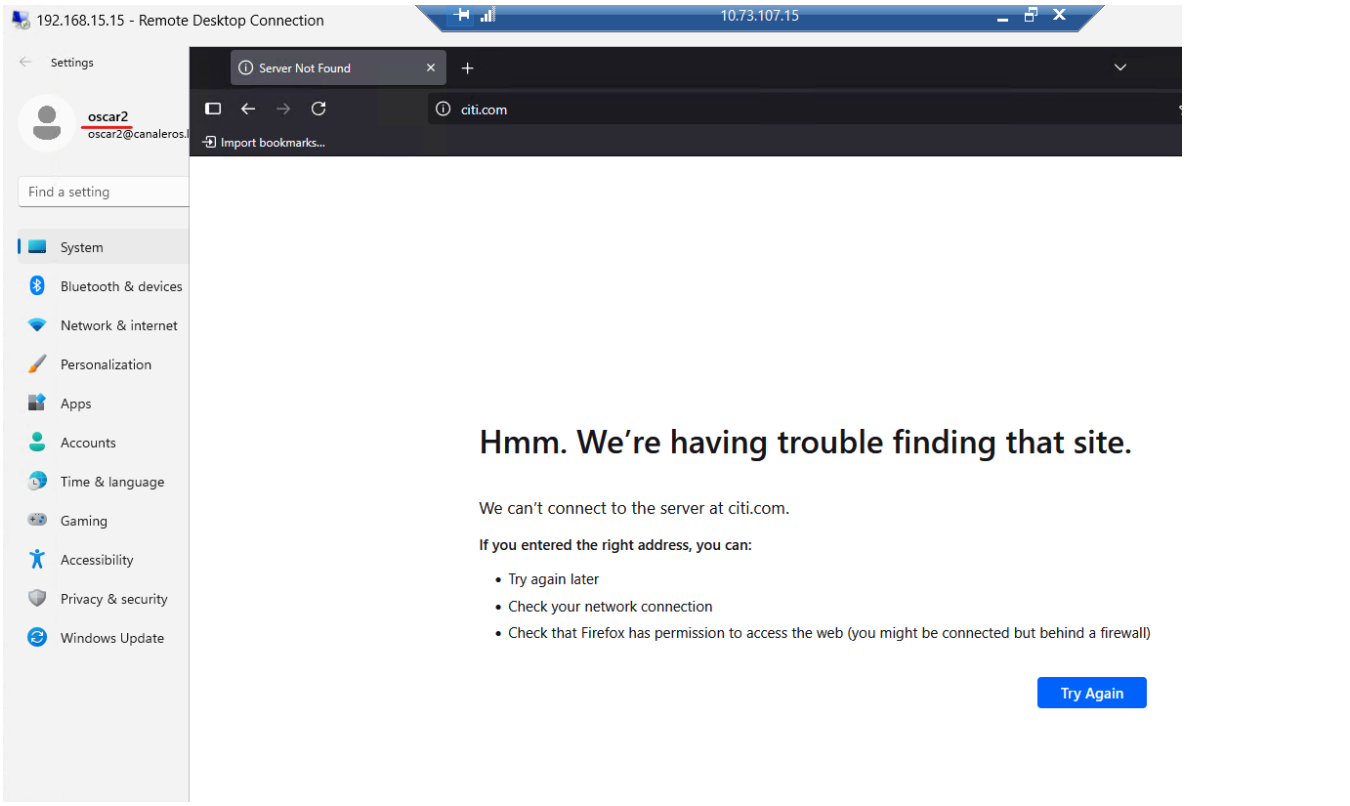
- Internet access allowed to oscar1



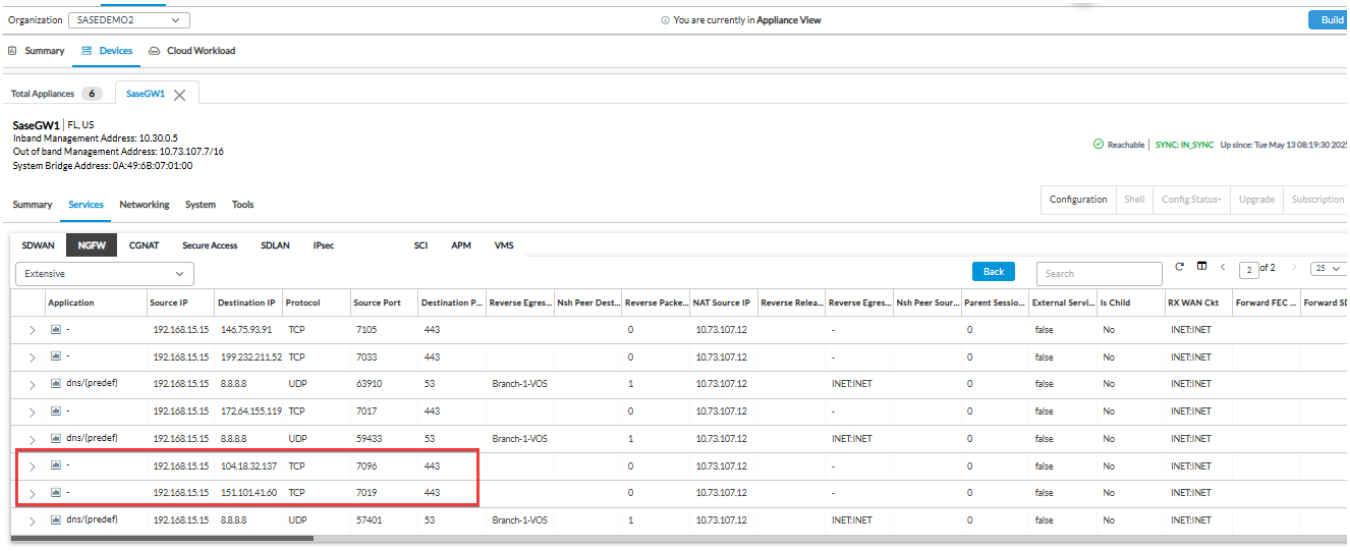
- In this output from the SSE Gateway, we can see the session of the internet webpage tested and the traffic being allowed by the policy created for user “oscar1”



- Internet access denied to oscar2



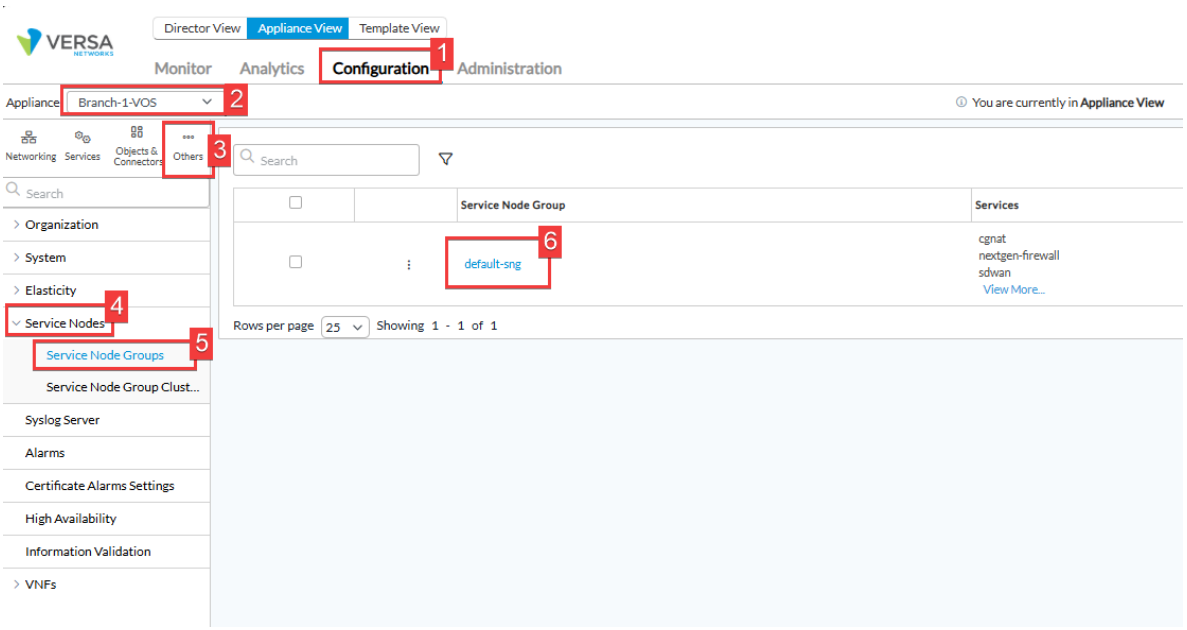
- Capture of the remote desktop connection of user "oscar2" and testing internet browsing. In this output from the SSE Gateway, we can see the session of the internet webpage tested and the traffic being denied by the policy module.



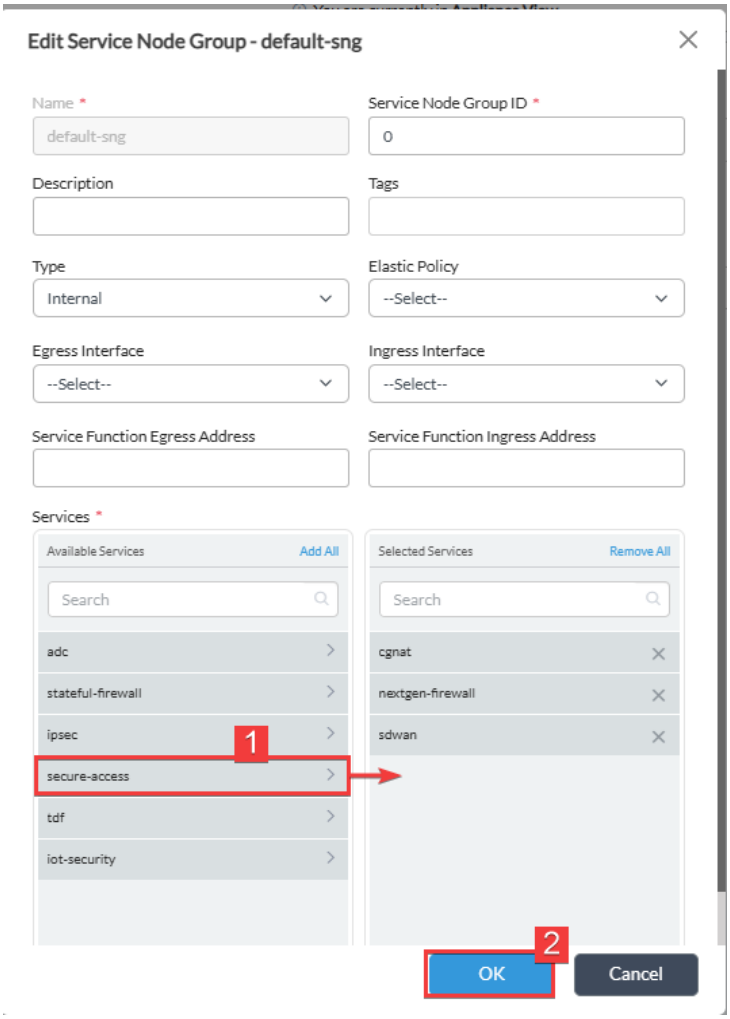
Configuration Steps: Scenario 2 & 3

NOTE: All changes suggested below should either be done in the Device Template or a “General” Service Template

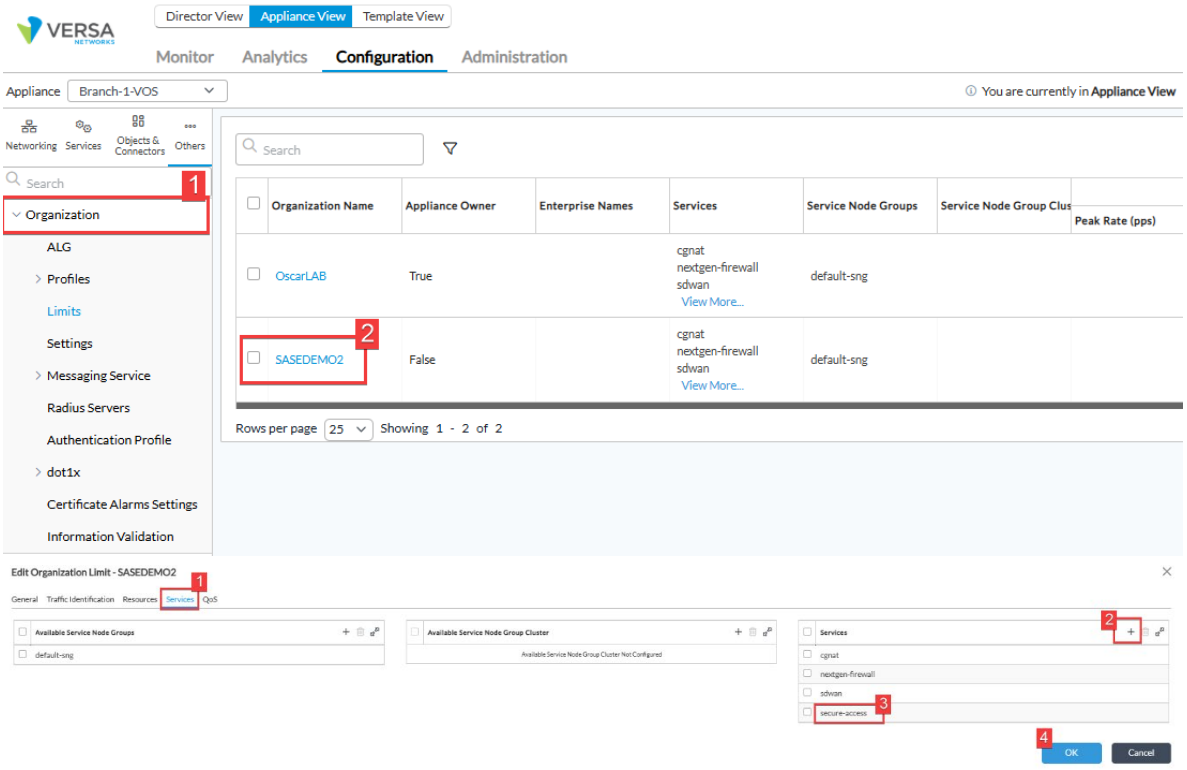
1. Edit the default-sng adding the secure-access feature in Director.
   - Secure-Access feature needs to be added to the SD-WAN device (if not added before).



- Make sure the setting is selected in the right section and click OK.

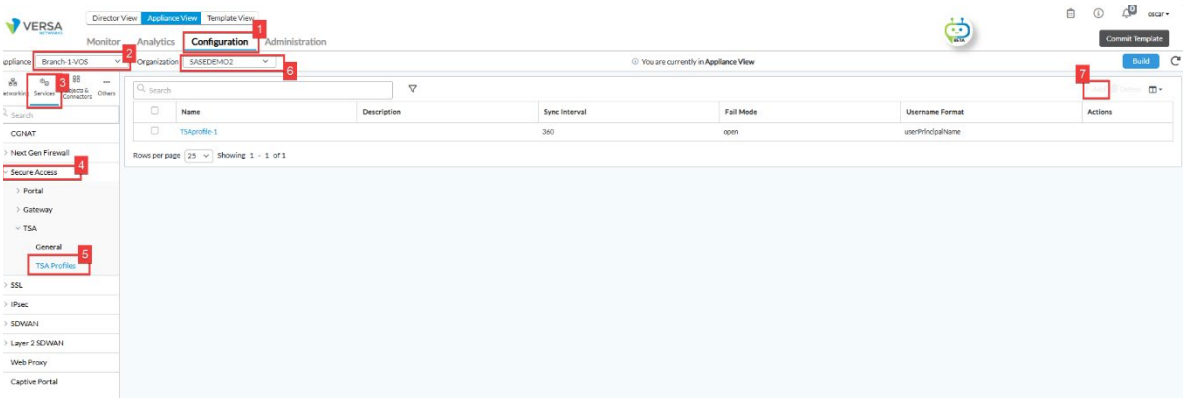


- Also add the feature to the Organization Limits in the Services tab.

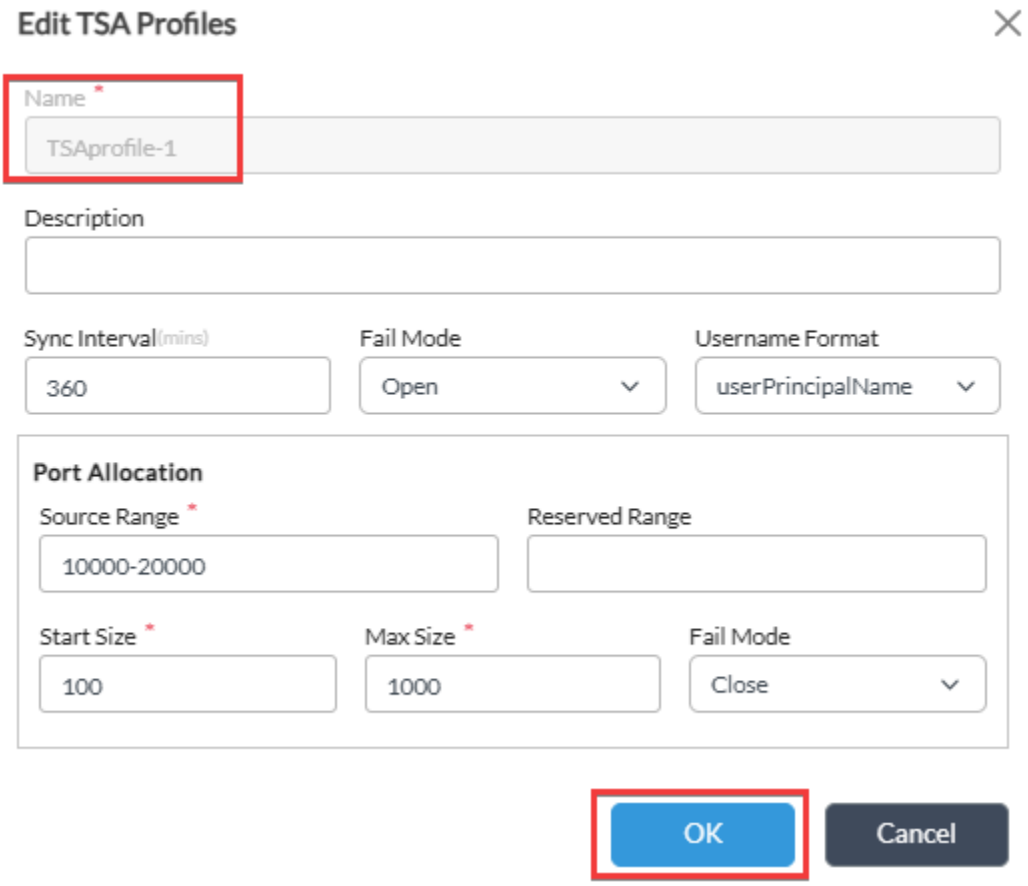


2. Configure TSA profile in Director

- Configure the Terminal Server Agent (TSA) in Director under the specific organization (in this case SASEDEMO2).



- Type in the Name (Required).



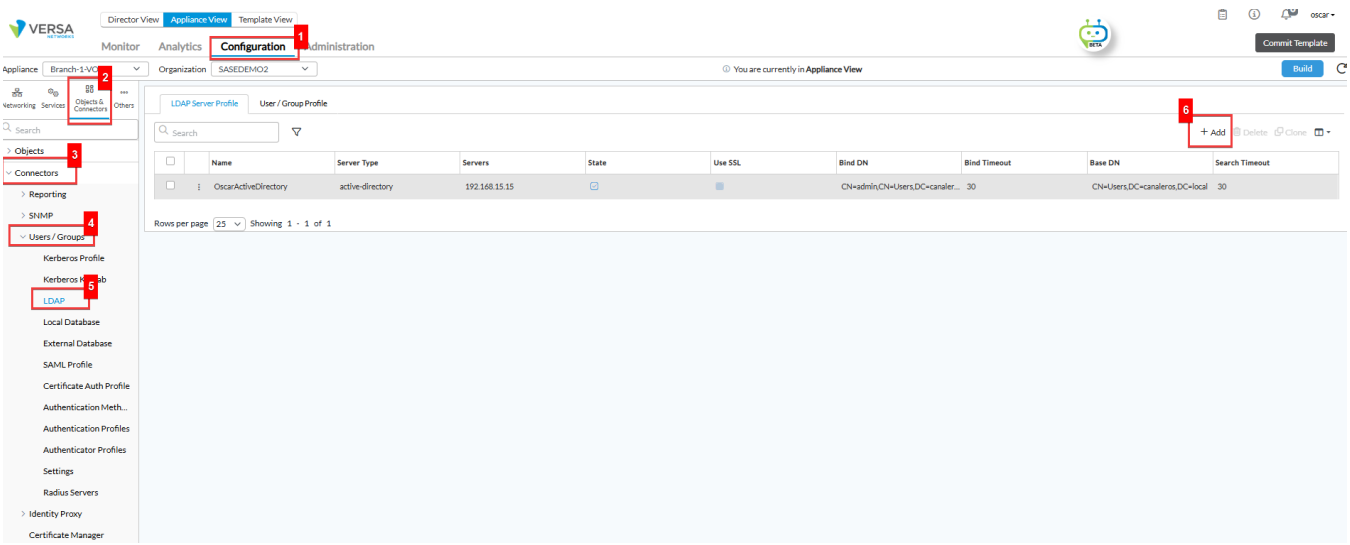
- **Port Allocation (Group of Fields)**
  - **Sync Interval:** Enter how often, in minutes, to synchronise the configuration with the TSA.
  - **Username Format:** Select the username format to have the TSA recognise
    - **userPrincipleName**—User principal name. A user principal name consists of a prefix (user account name), followed by the @ symbol and a suffix (DNS domain name). For example, someone@my-company.com.
    - **sAMAccountName**—The sAMAccountName attribute is a login name that supports clients and servers from previous Windows versions, for backwards compatibility, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.
  - **Reserved Port Range:** Enter the reserved port allocation range for user sessions. The value must be entered into the Port-Start - Port-End format, and the port range must have a minimum of 10000 ports. For example, enter 0-10000 to start port 0 and end port 10000. Range: 0 through 65535

- **Maximum Size (Required):** Enter the maximum port allocation size for each user. The maximum size must be a multiple of the start size. Range: 0 through 65535. Default: 5000
- **Fail Mode:** Select the traffic mode if the TSA server connection fails,
  - **Close**—Deny traffic if the TSA server connection fails. This is the default state.
  - **Open**—Allow traffic if the TSA server connection fails.
- **Fully Qualified Domain Name (FQDN):** Use this FQDN URL when configuring the TSA application

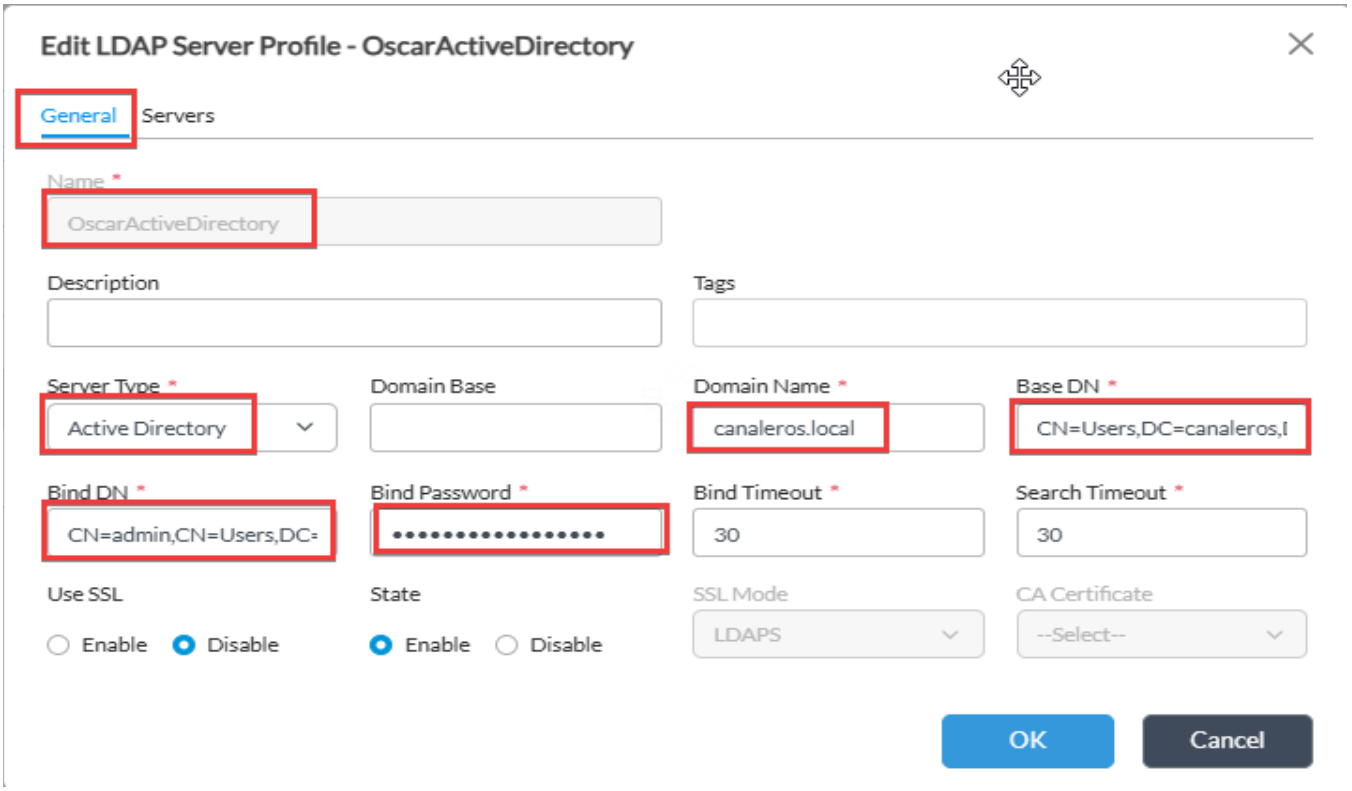
- **Example Scenario**

Item	Value
Total Users	4
Max Ports per User	5000
Total Ports Required	4 × 5000 = **20,000**
Reserved Port Range	**10000-30000**
Fail Mode	Close (recommended)

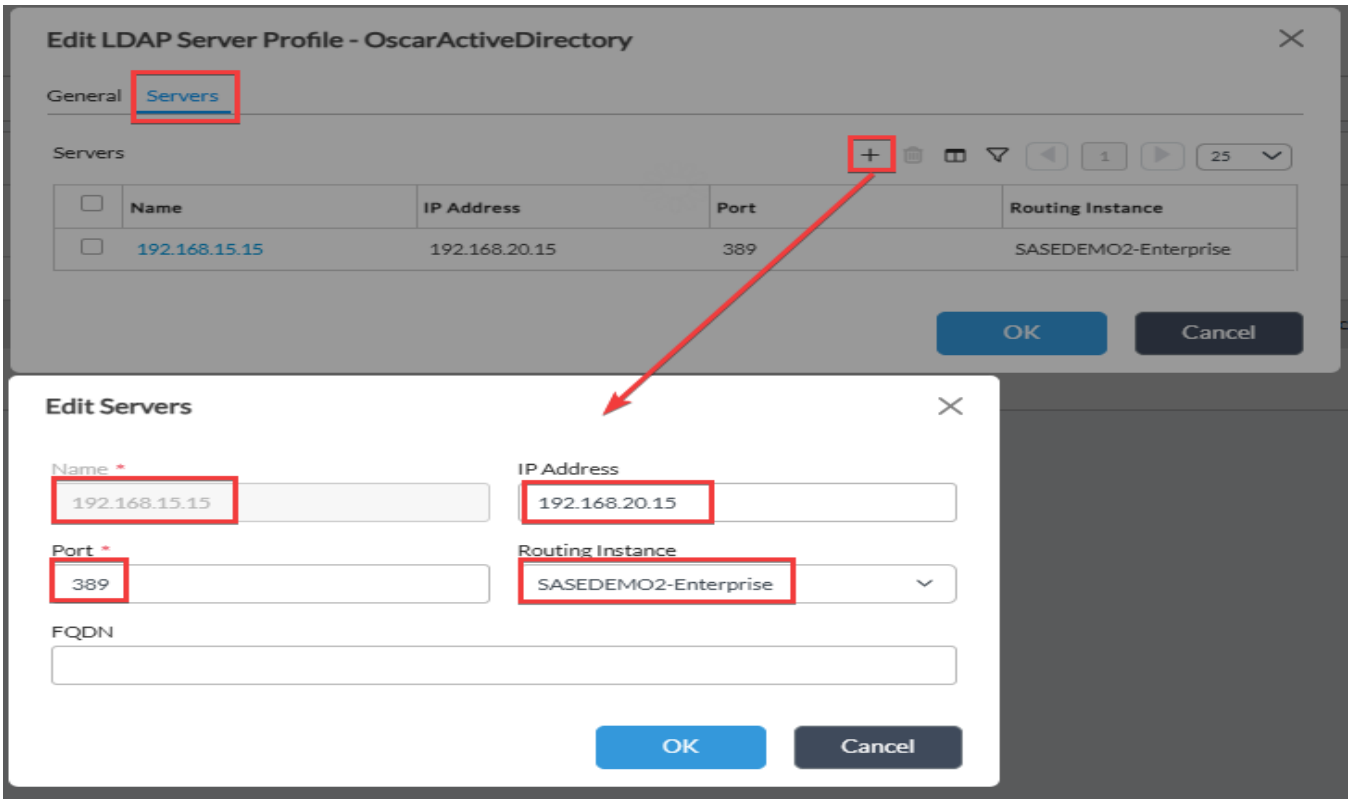
- Configure the Active Directory authentication for TSA, please refer Configure-LDAP
- Create an LDAP Profile



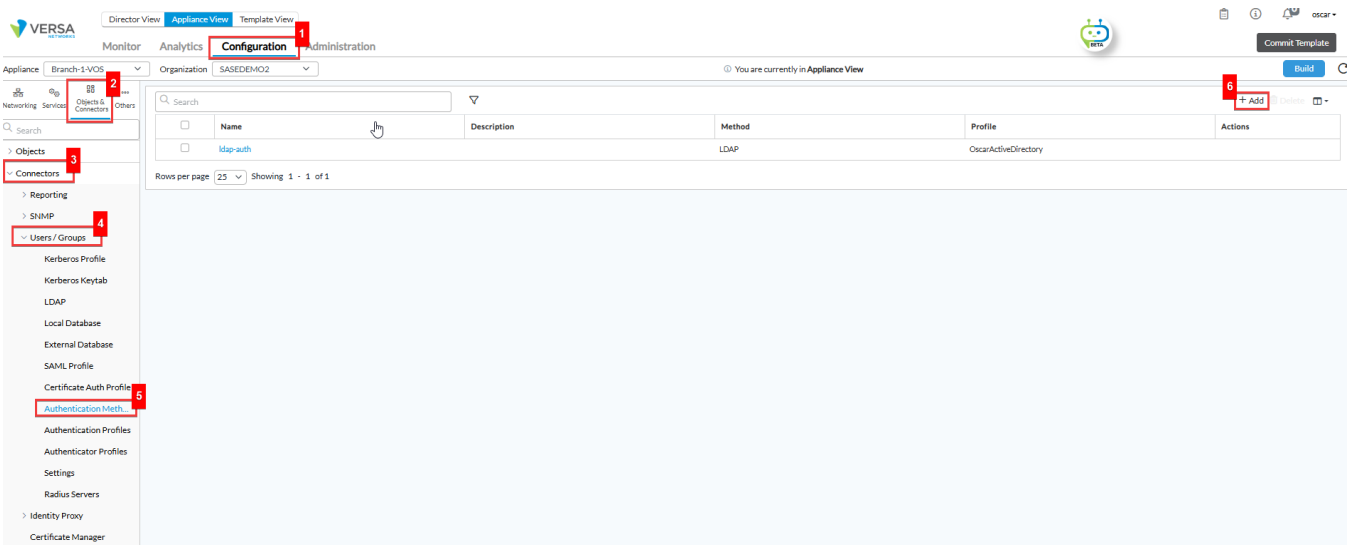
- Fill in the bind data information to log in to the Active Directory.



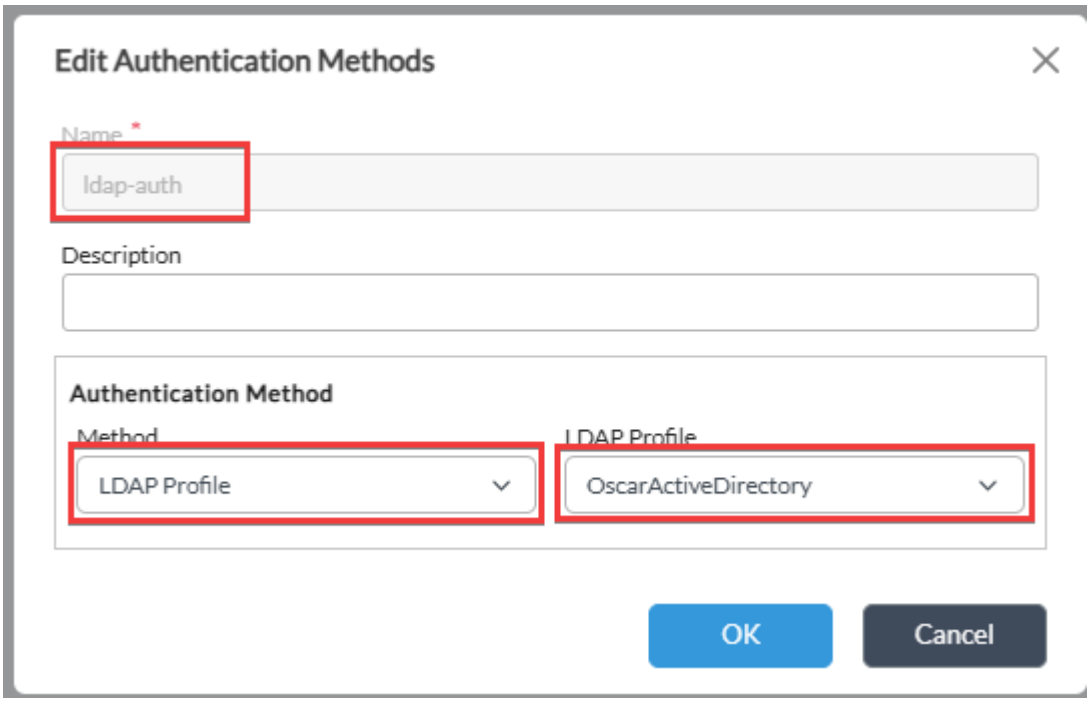
- Fill in the information of the Active Directory server.



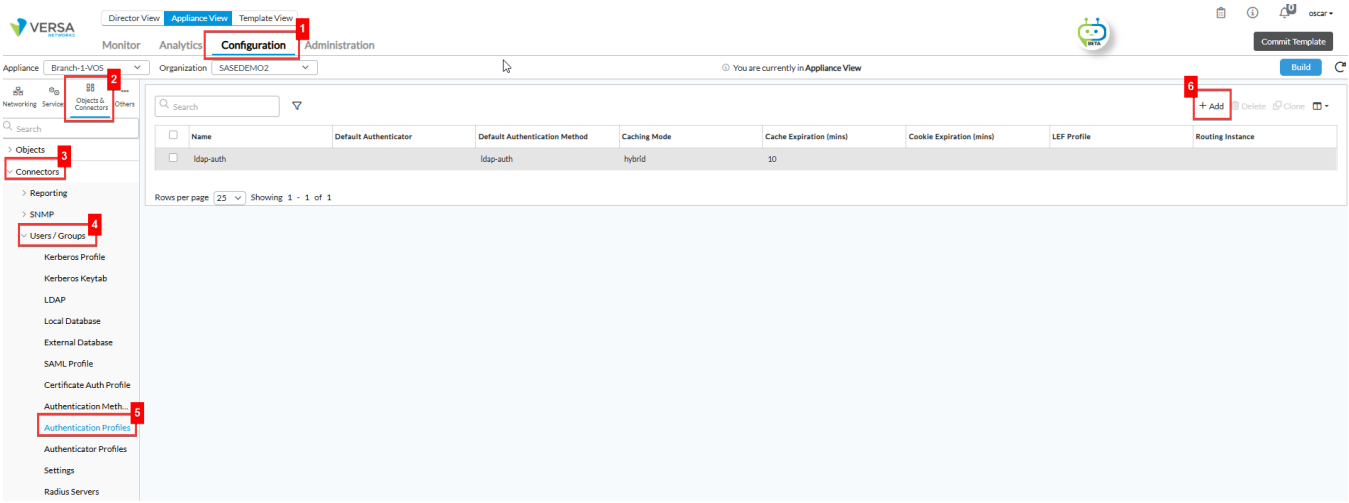
- Create an Authentication Method



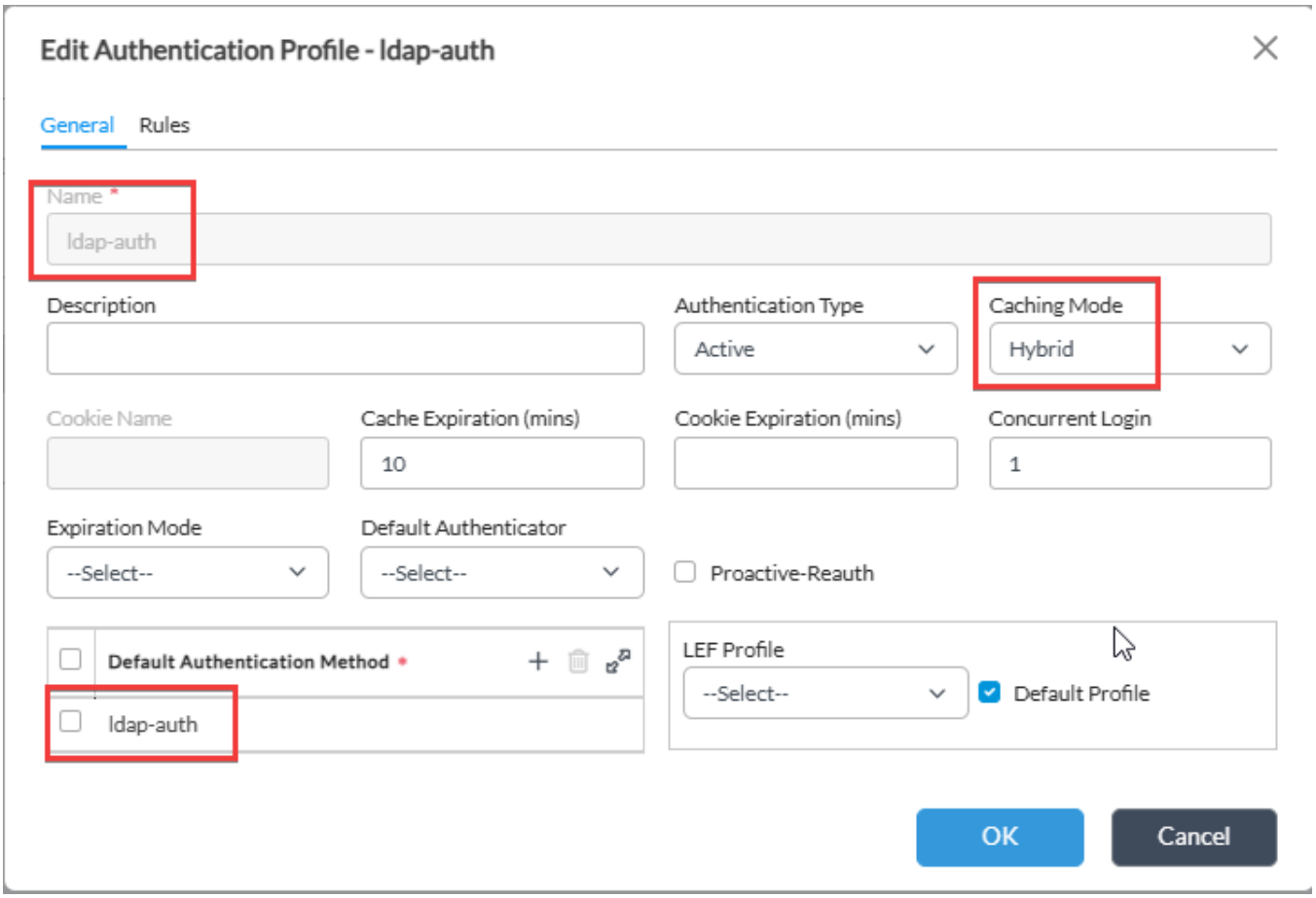
- Name de method, select the method and LDAP profile from the dropdown menus.



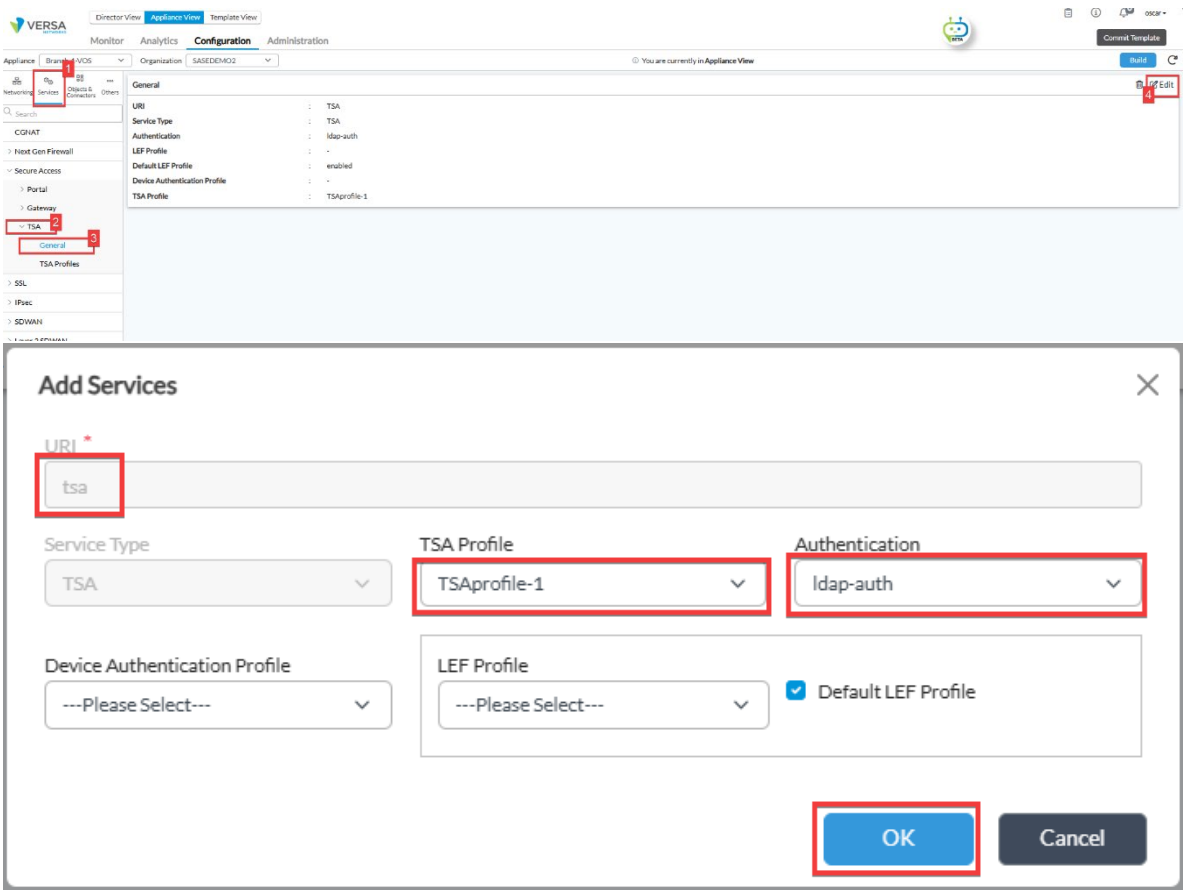
- Create an authentication profile.



- Note that the caching mode must be hybrid

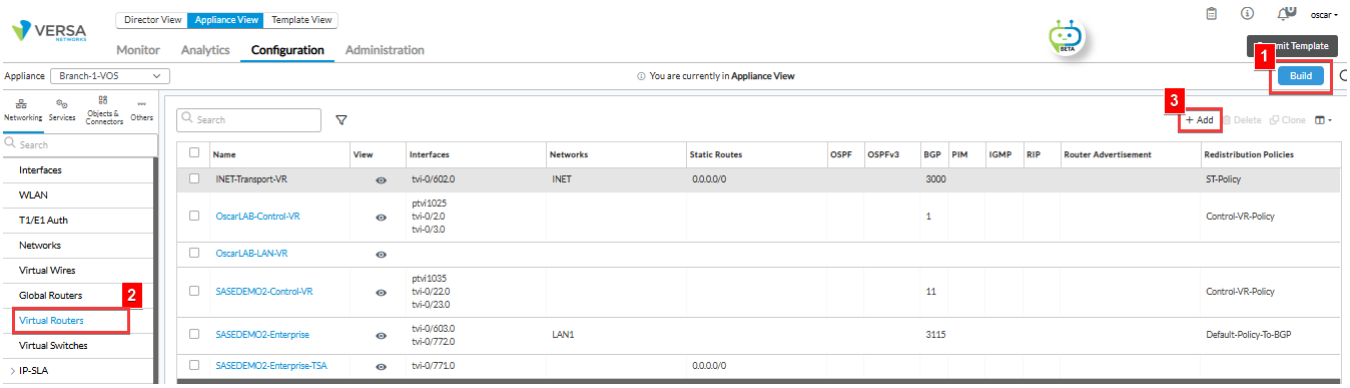


- Set the TSA profile along with the authentication method

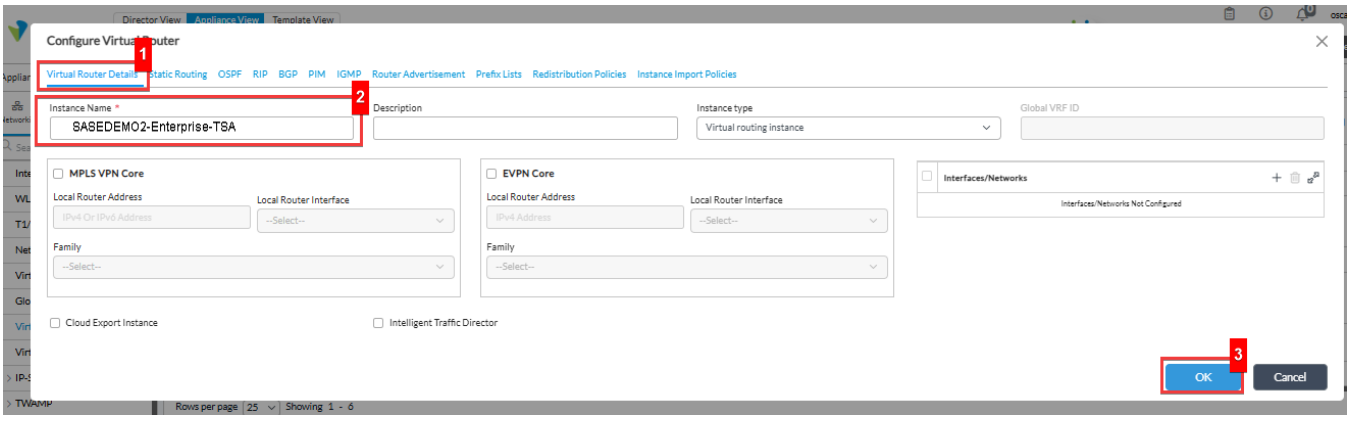


3. Create a new routing instance for TSA registration

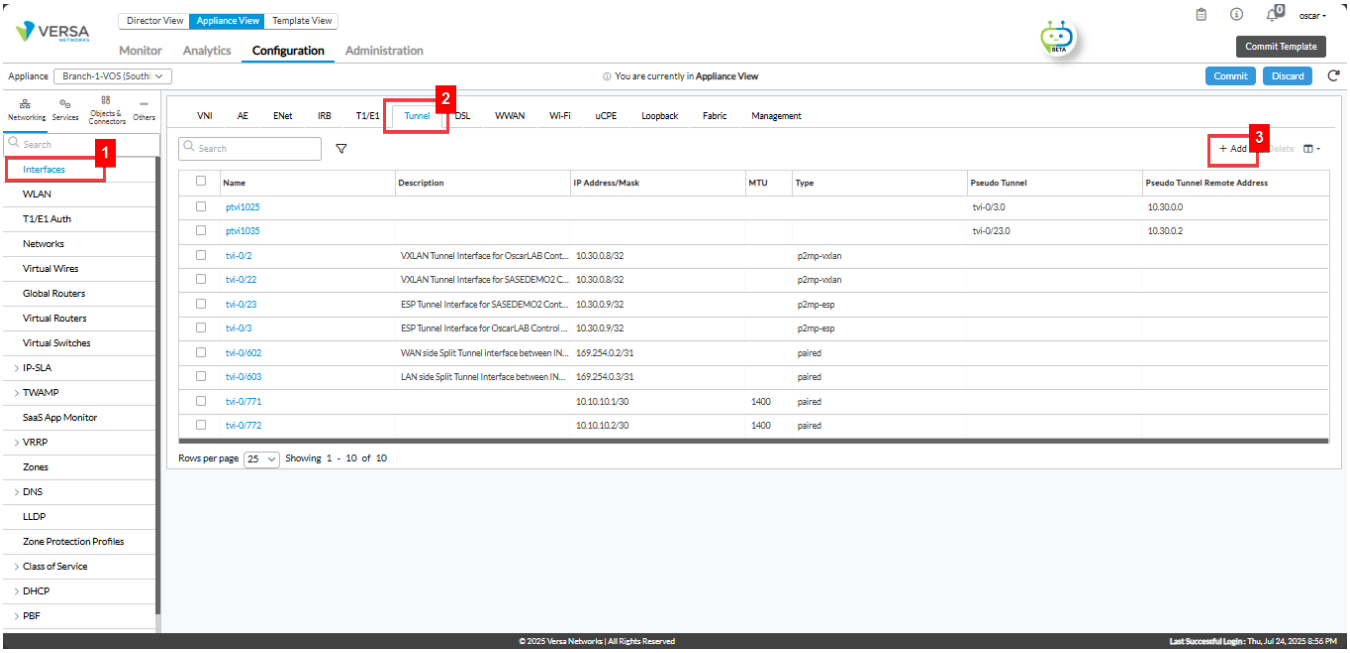
- Enable the build mode for the SD-WAN device and add a new Virtual Router.



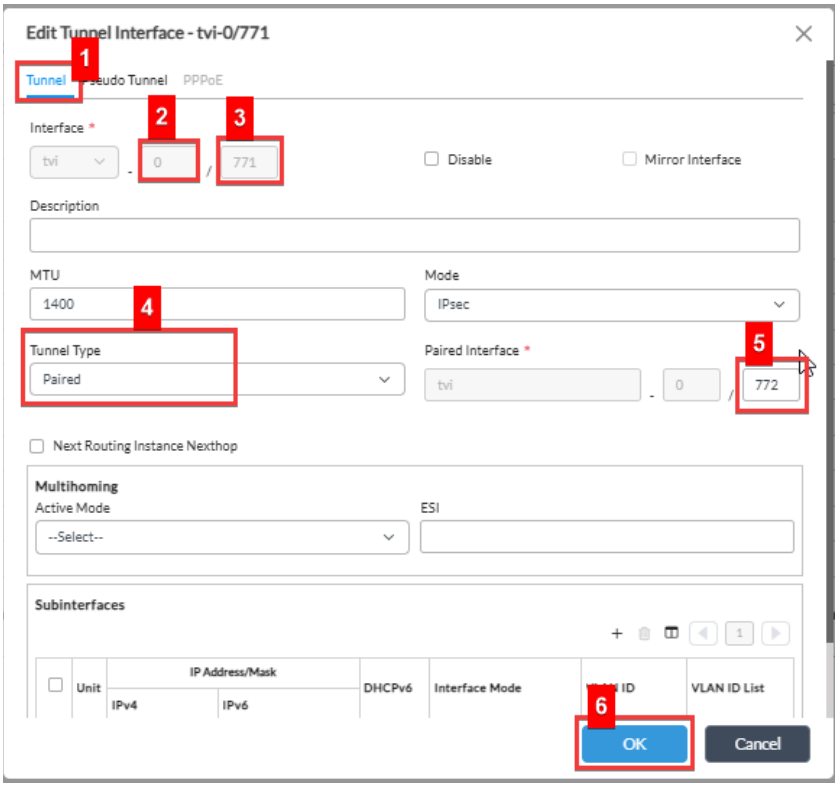
- Name the new Virtual-Router, in this case “SASEDEMO2-Enterprise-TSA”



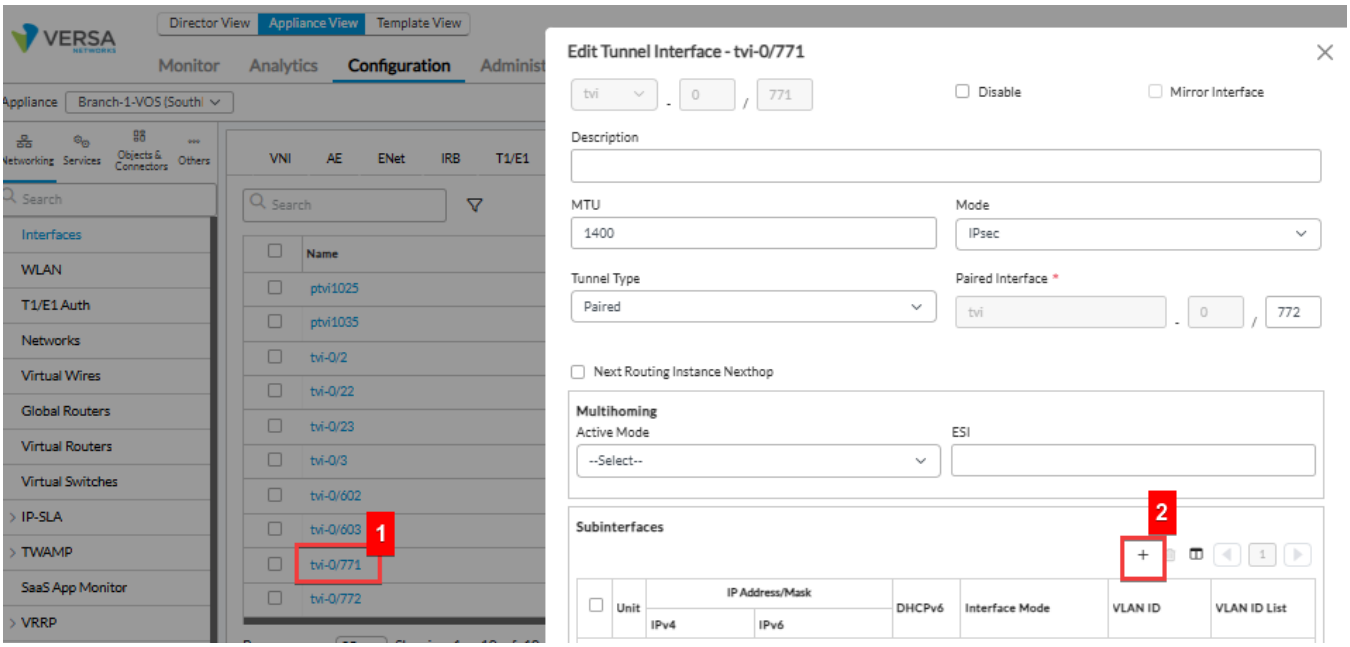
- Create a paired TVI interface to leak routes between the “SASEDEMO2-Enterprise-TSA’ routing instance and the existing Enterprise-VR routing instance.

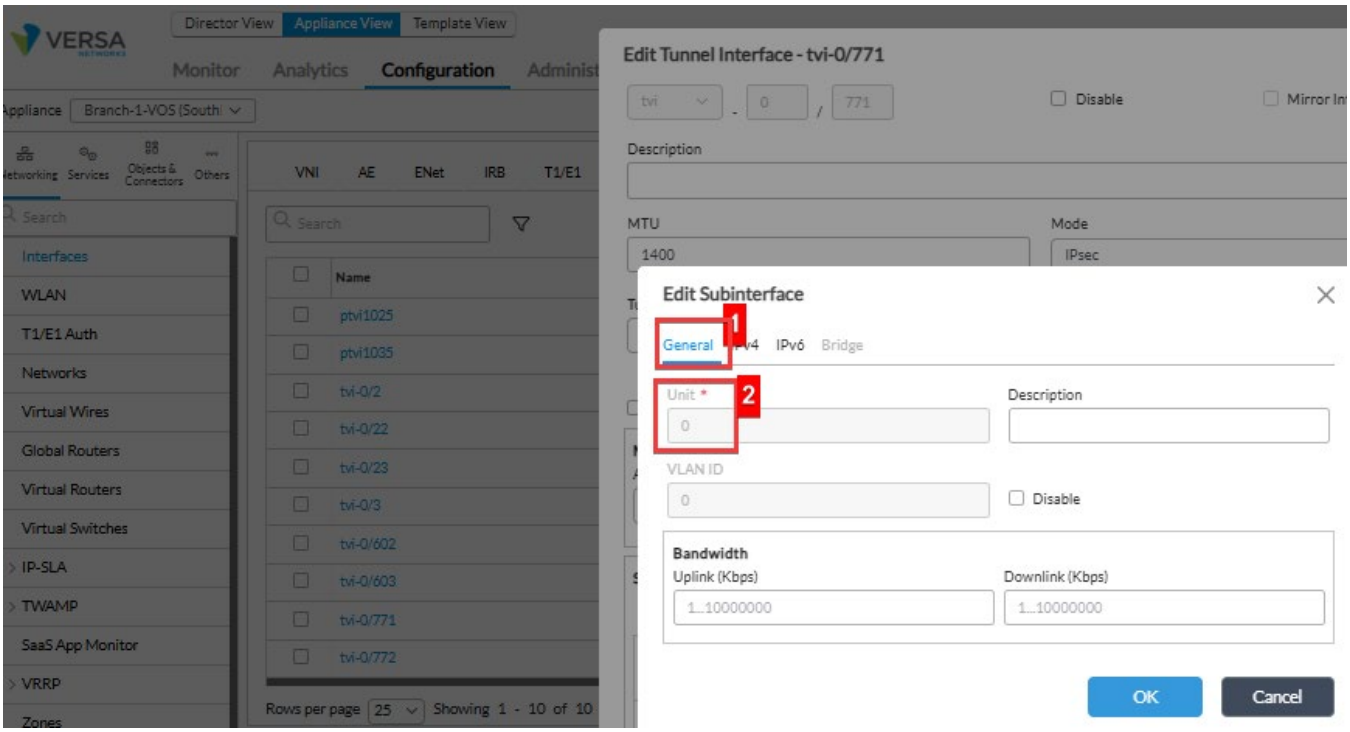


- Tvi-0/771 was created with Paired Tunnel Type and paired interface Tvi-0/772. This will create both interfaces. Ensure the numbers defined are not already in use

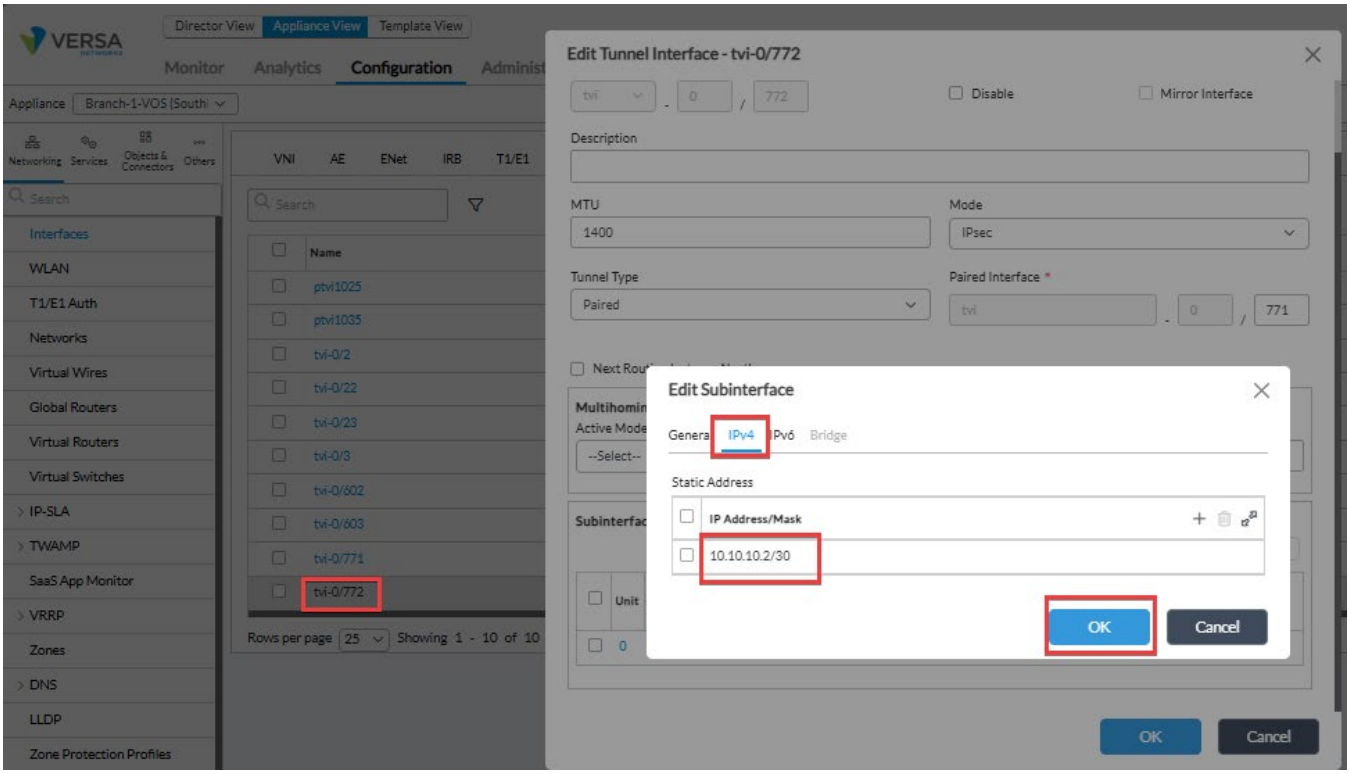


- Edit each interface to assign the IP address. Two IP addresses are required, so a /31 or /30 subnet is required. It should not be part of the overlay pool or used in customer existing network.

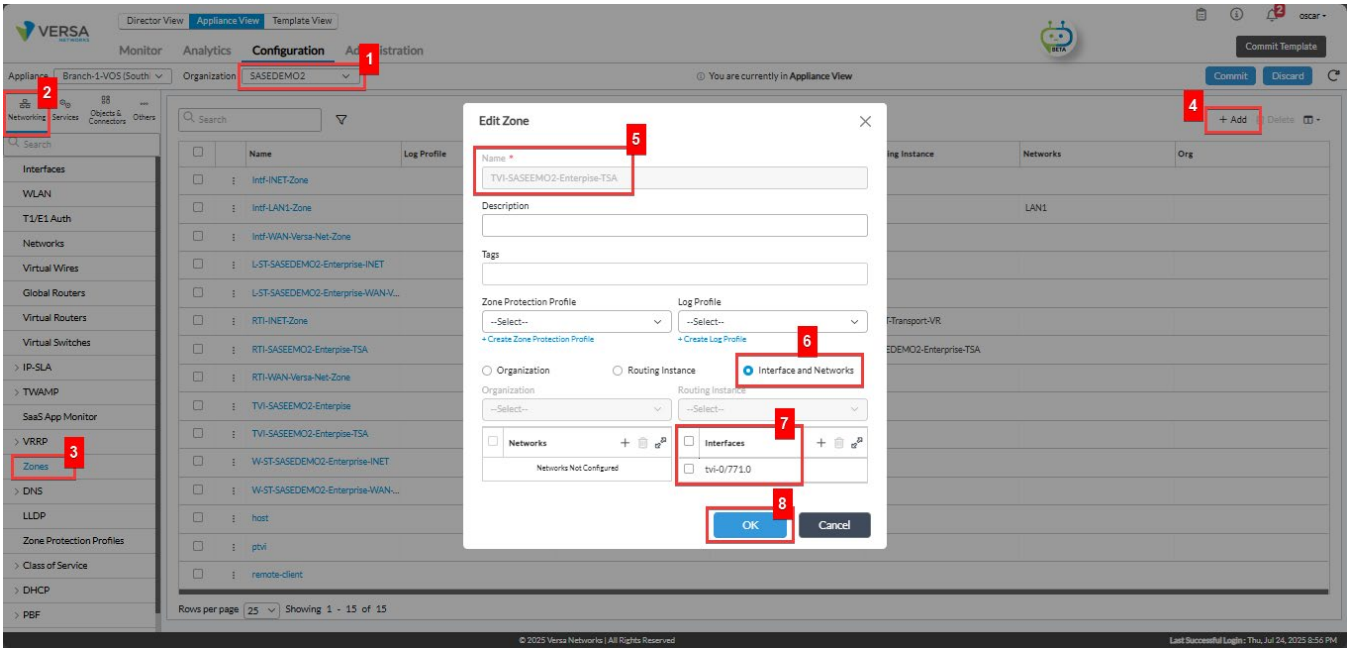


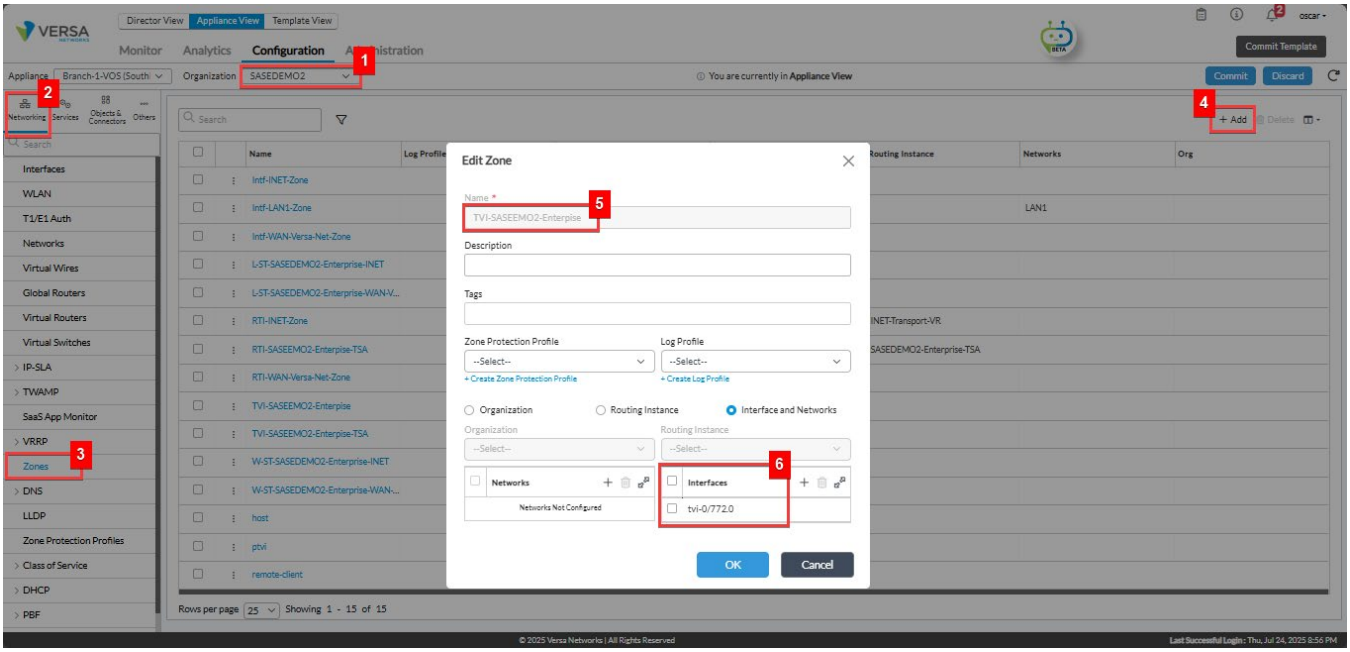


- Edit the interface tvi-0/772 with the same previous steps with the corresponding IP address in the same subnet.

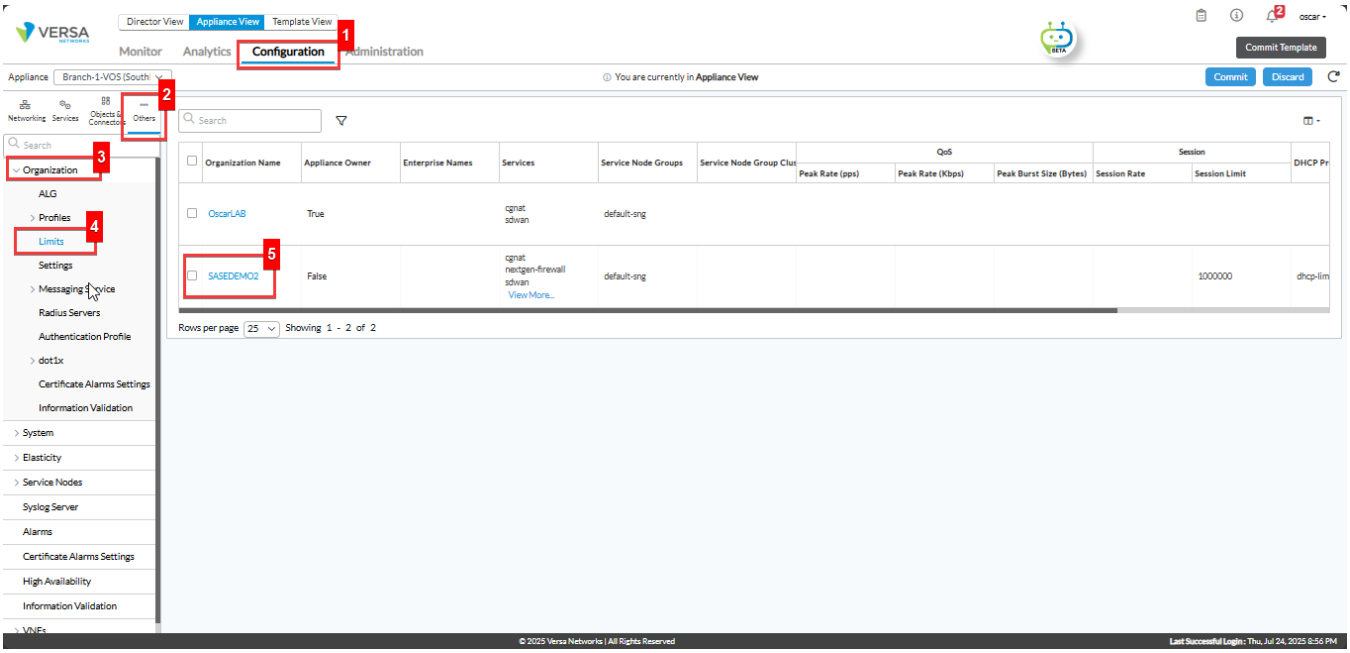


- Create two new zones “TVI-SASEDEMO2-Enterprise-TSA” and “TVI-SASEDEMO2-Enterprise”, (we used the routing instance name to represent the TVI is part of which VR) to assign the respective tvi interface created previously

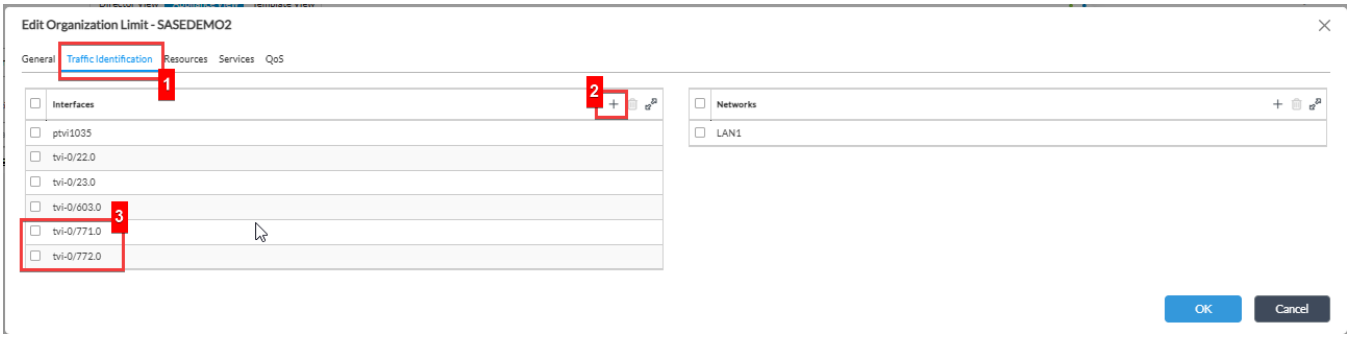




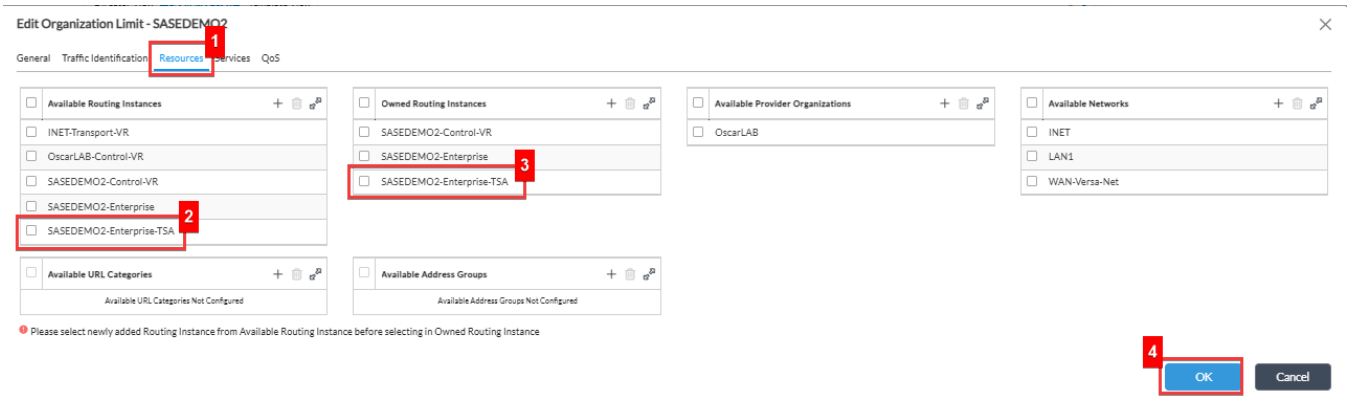
- Edit the Limits option of the organization's tenant to add newly created interfaces and routing instances.



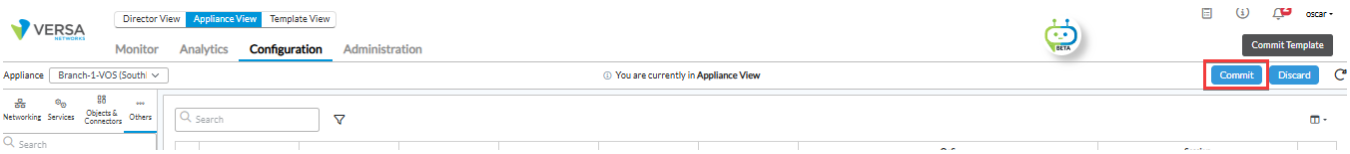
- Add the TVI interfaces in the Traffic Identification tab.



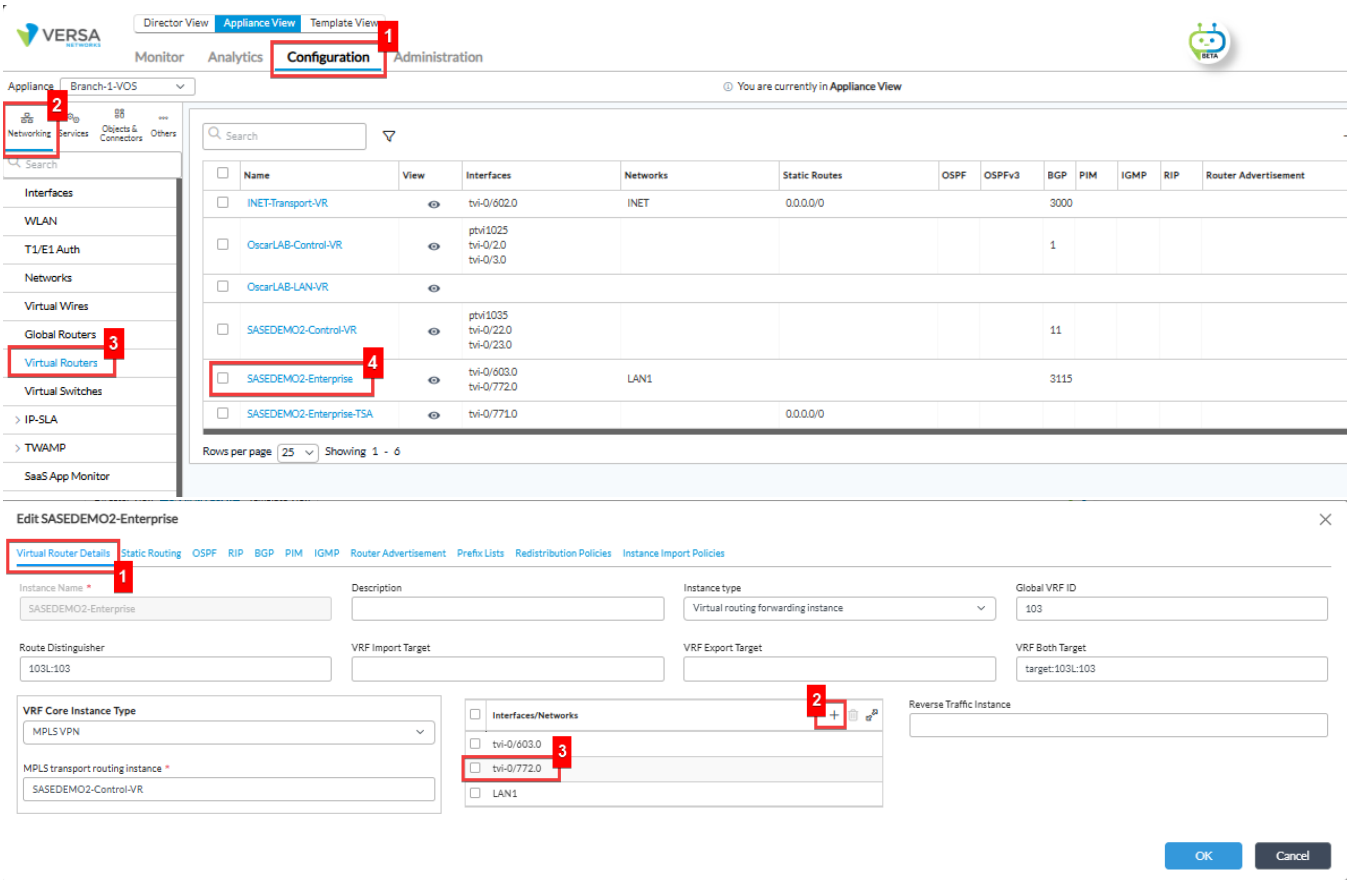
- Add the new Routing Instance "SASEDEMO2-Enterprise-TSA" to the Available and then Owned section in the Resources tab.



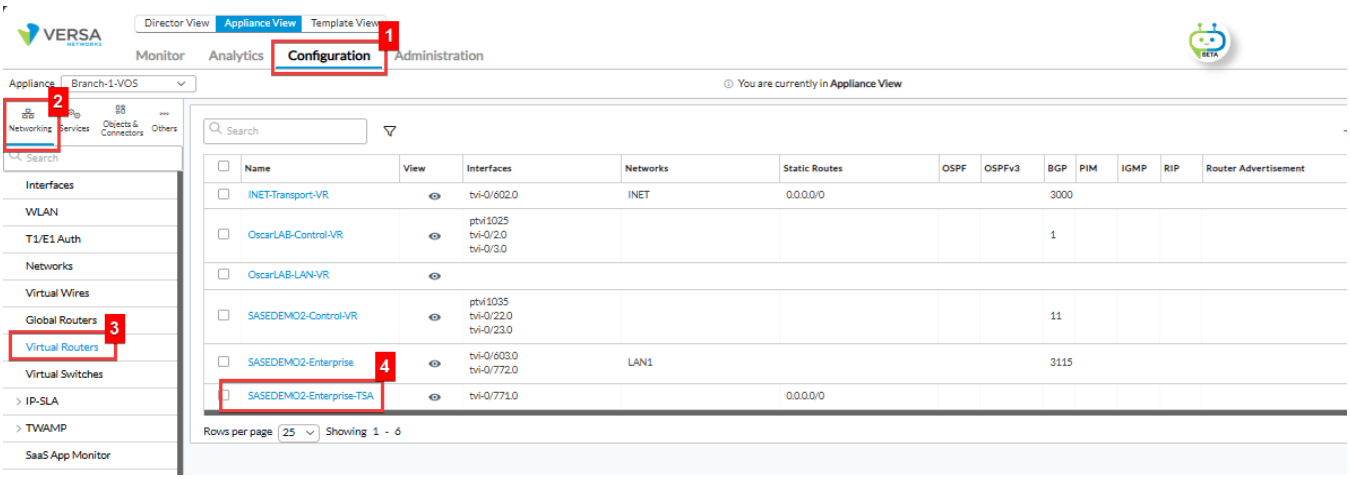
- Commit the changes to save the new configurations.

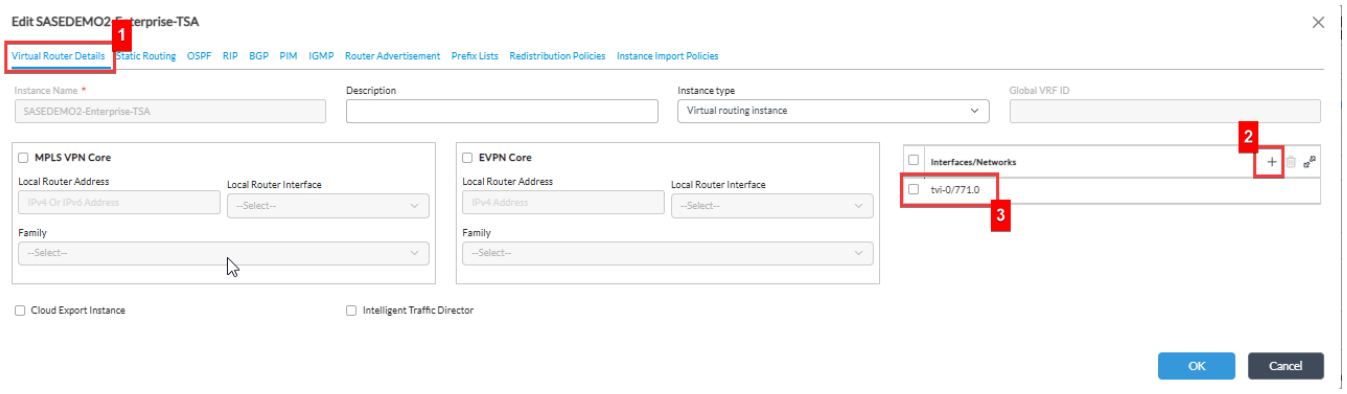


- Edit Virtual Routers. First existing routing instance, add the corresponding TVI interface

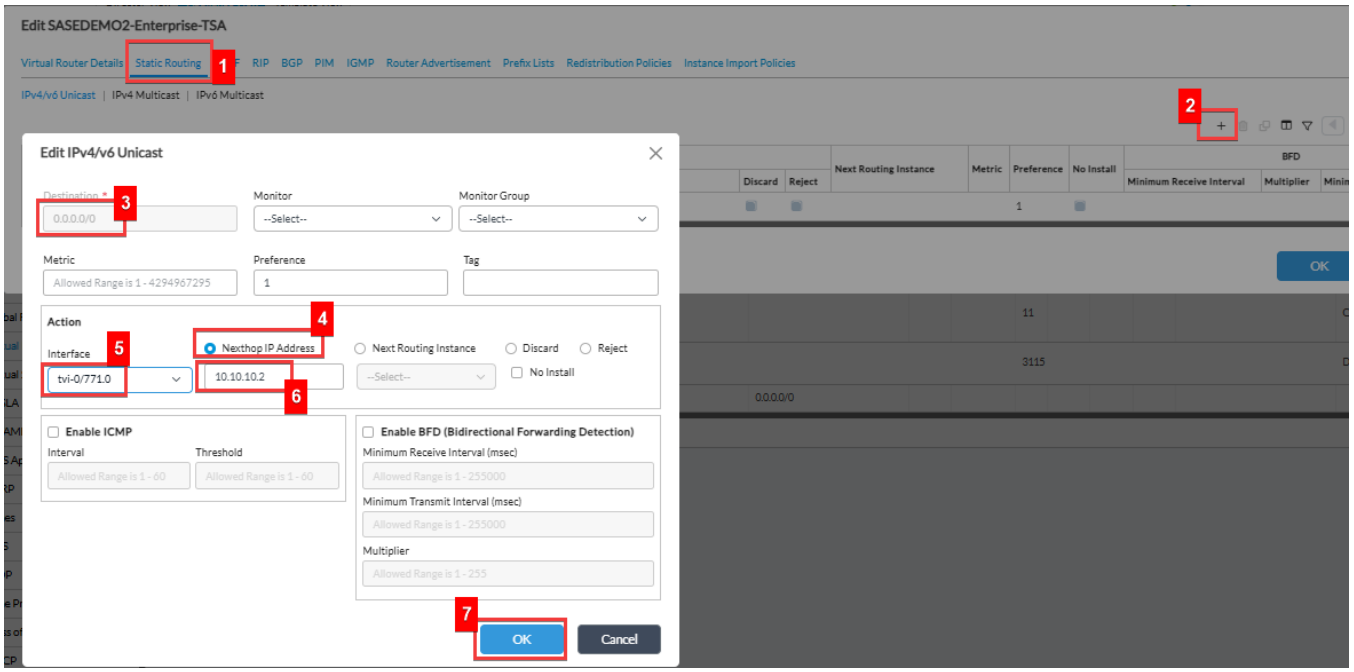


- Next, in the “SASEDEMO2-Enterprise-TSA” routing instance, add the corresponding new TVI interface

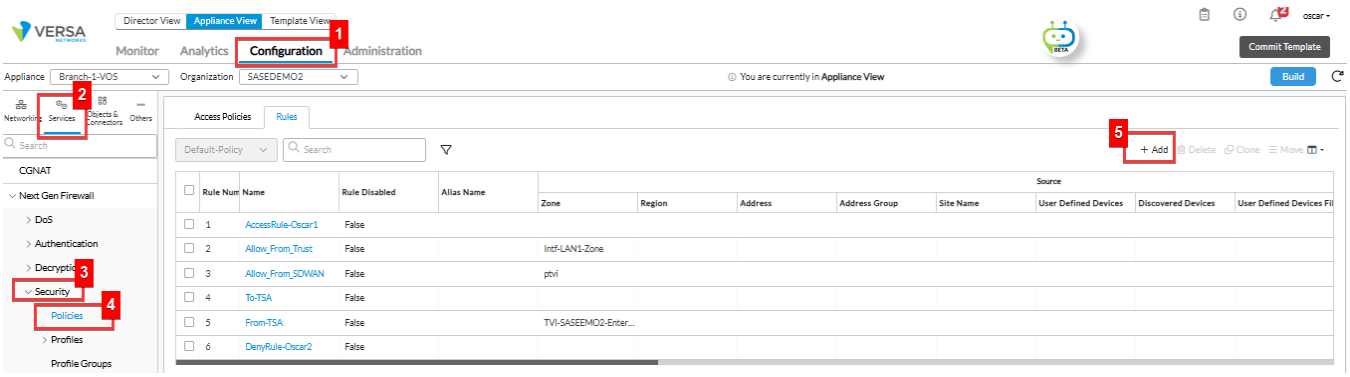




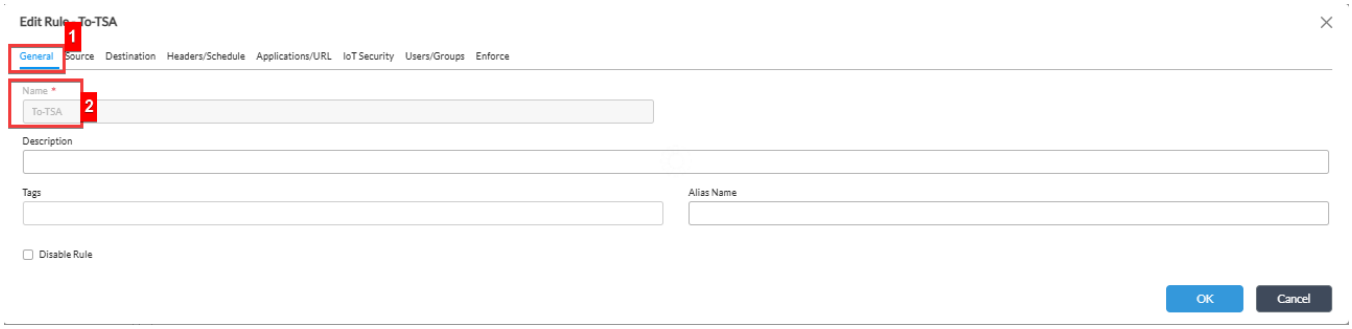
- Add a default route in “SASEDEMO2-Enterprise-TSA” with next-hop as TVI IP in “SASEDEMO2-Enterprise”



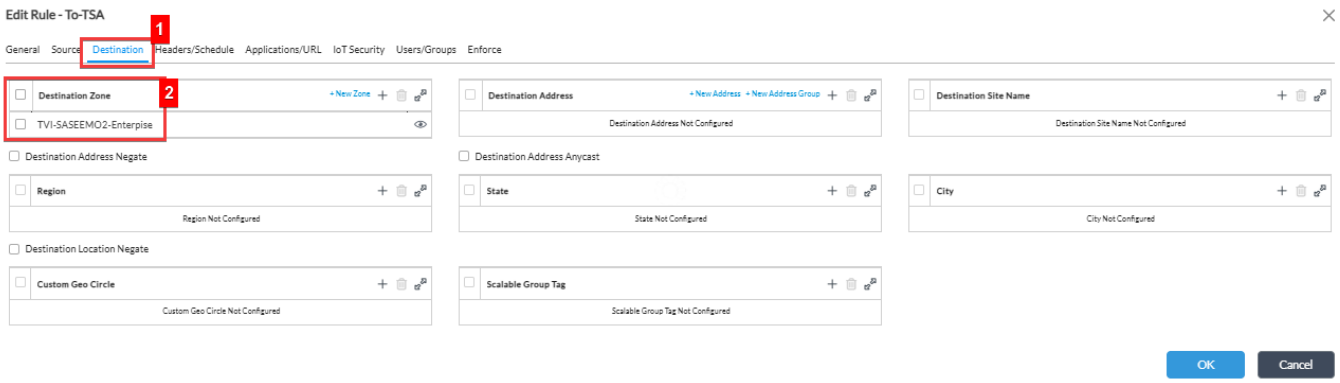
- Now, create a new security policy to allow traffic towards “SASEDEMO2-Enterprise-TSA” routing instance.



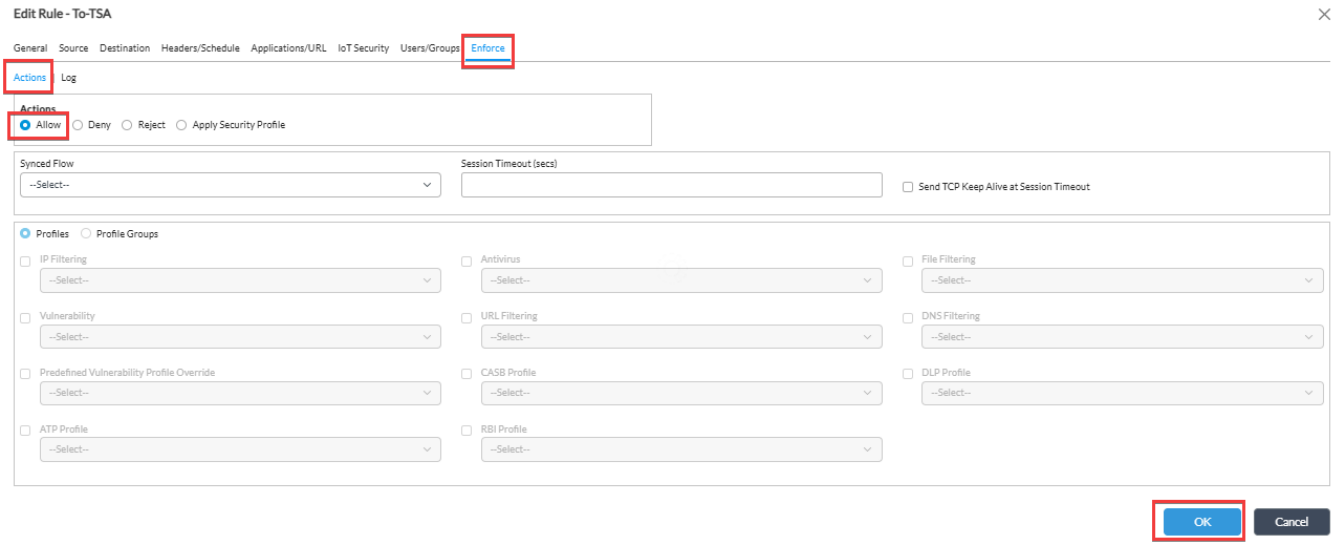
- Name the policy



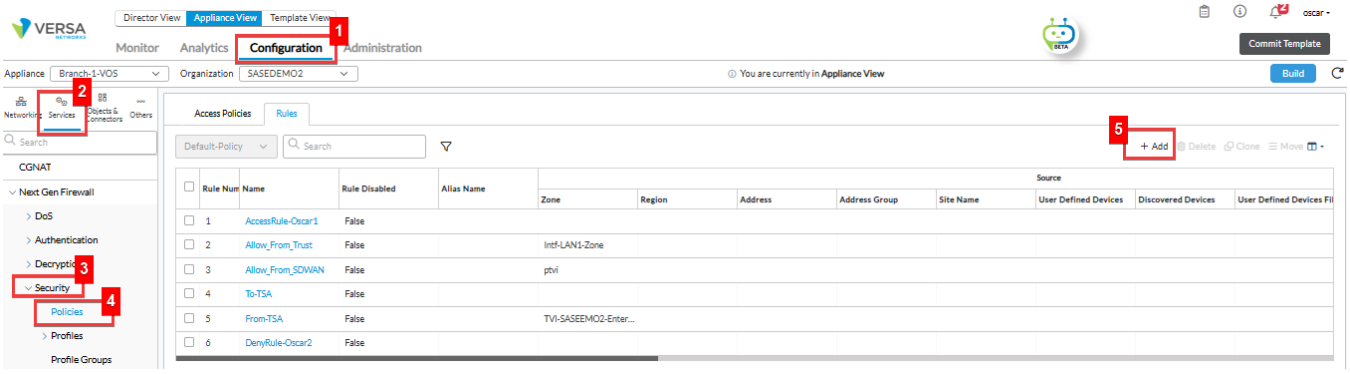
- In the Destination tab, select the “TVI-SASEDEMO2-Enterprise” zone assigned TVI in SASEDEMO2-Enterprise routing instance.



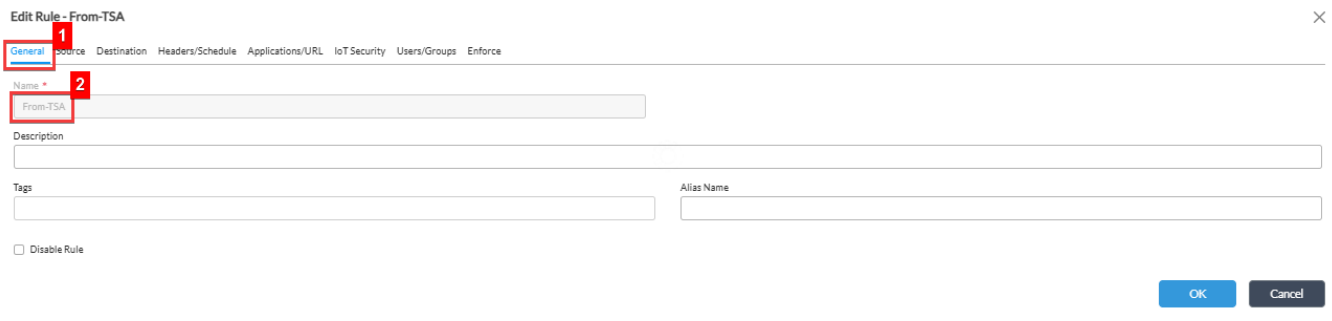
- Allow the traffic



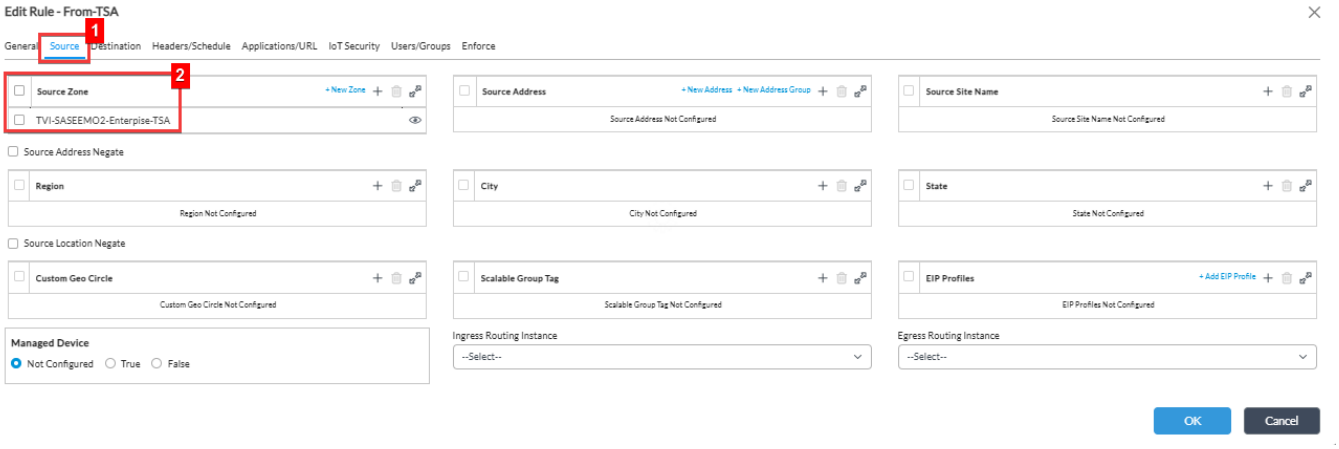
- Next, create a new security policy to allow traffic from “SASEDEMO2-Enterprise-TSA” routing-instance.



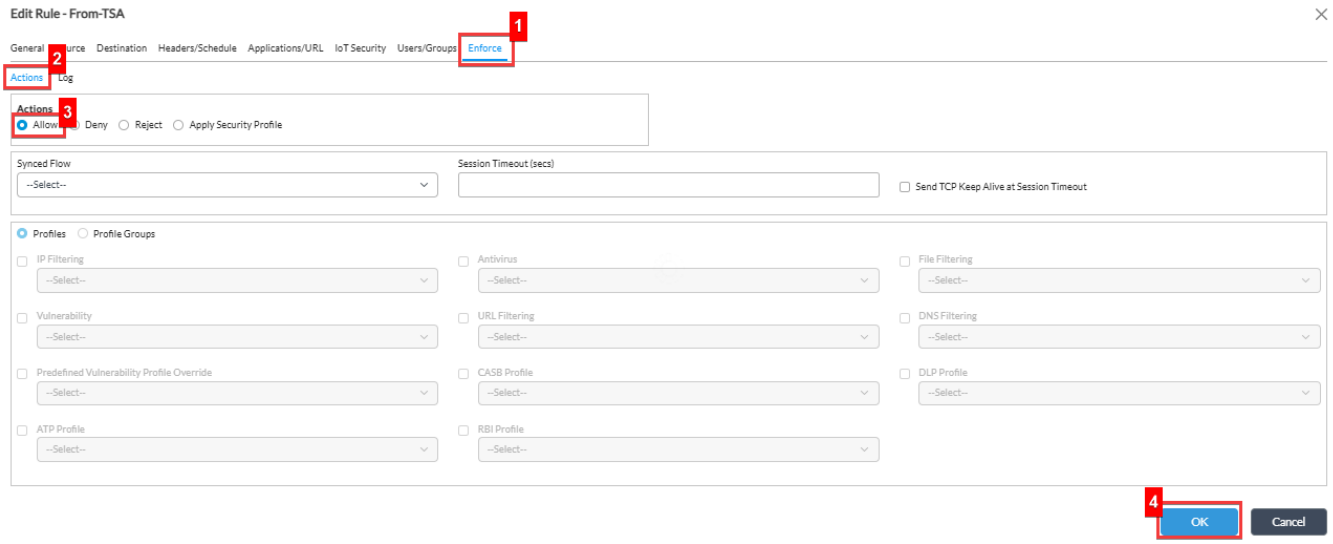
- Name the policy



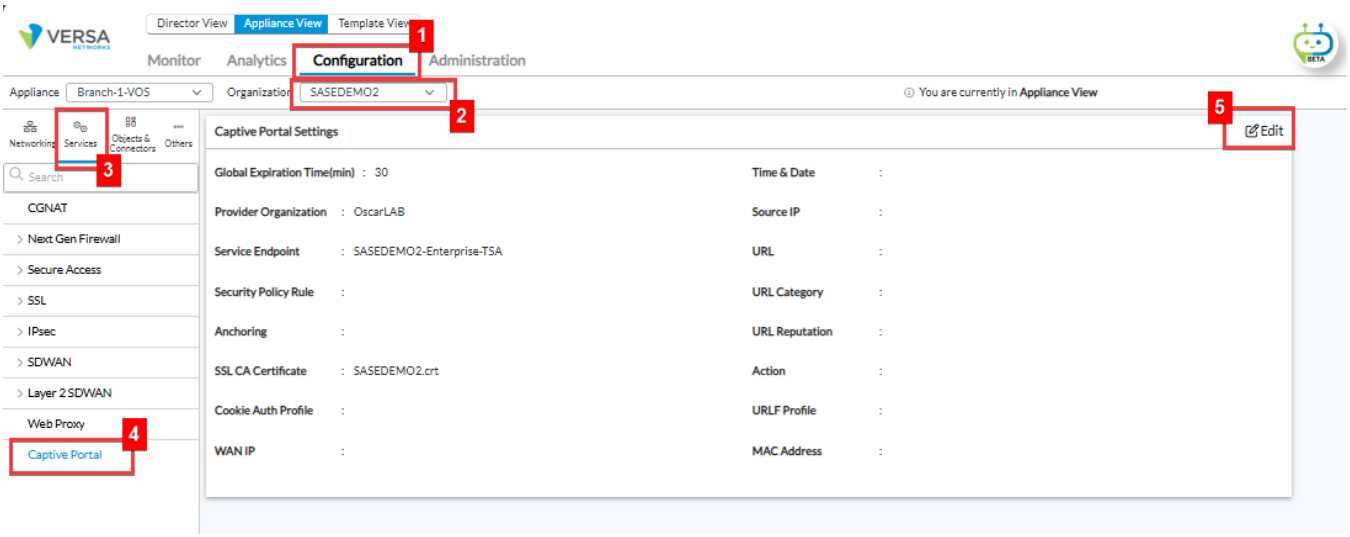
- In the Source tab, select the “TVI-SASEDEMO2-Enterprise-TSA” zone assigned to TVI in SASEDEMO2-Enterprise-TSA routing instance.



- Allow the traffic

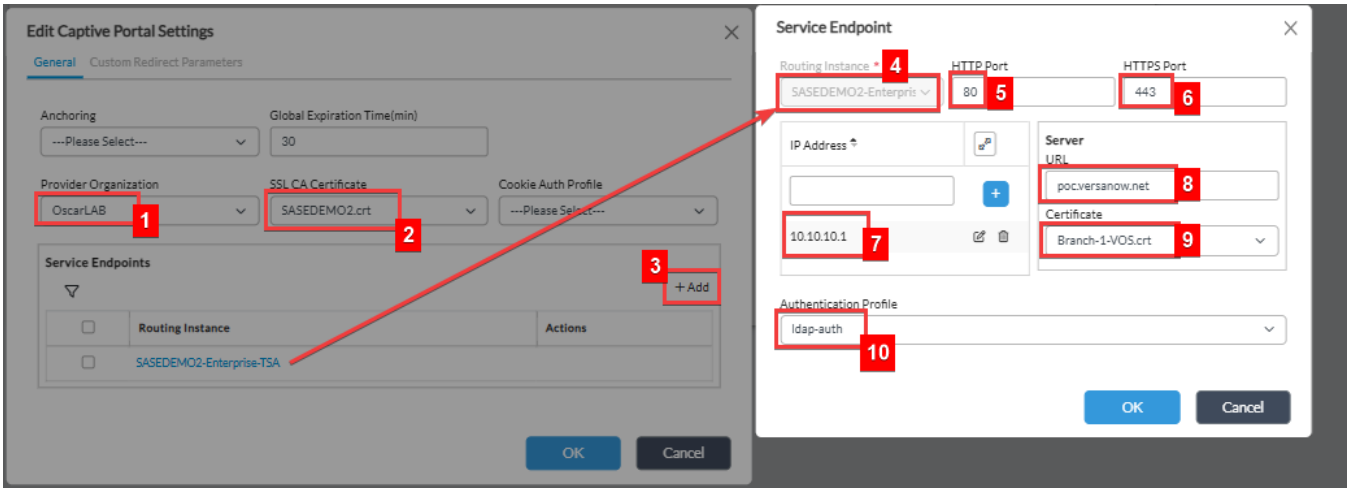


4. **Configure captive portal**
   - The following are the prerequisites to configure Captive Portal for TSA:
     - Generated Endpoint certificate for VOS with CN as captive portal URL.
     - Upload the Endpoint certificate, its private key and CA certificate from the Director or CLI to VOS.
   - Select the Captive Portal in the required organisation and edit.

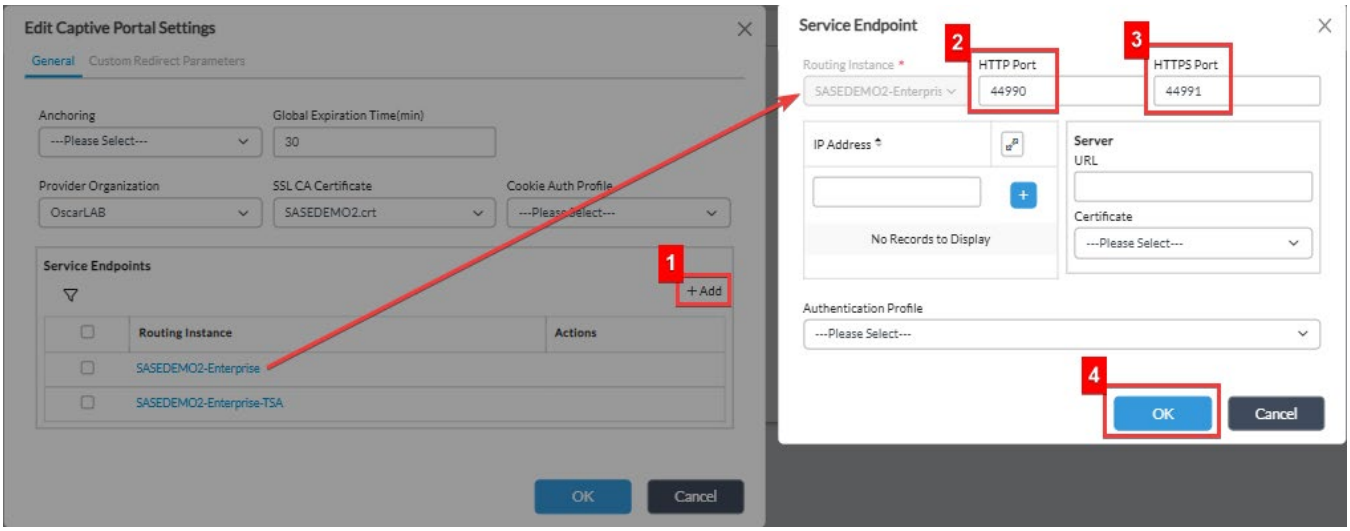


- In the captive portal, select the provider Org and the CA Certificate, then add the Service Endpoint with the new TSA routing instance.

  Add the TSA routing instance TVI interface IP, type the captive portal URL and select the endpoint Certificate created for the captive portal URL. Select the Authentication method and click OK. Set 80 for HTTP and 443 for HTTPS.

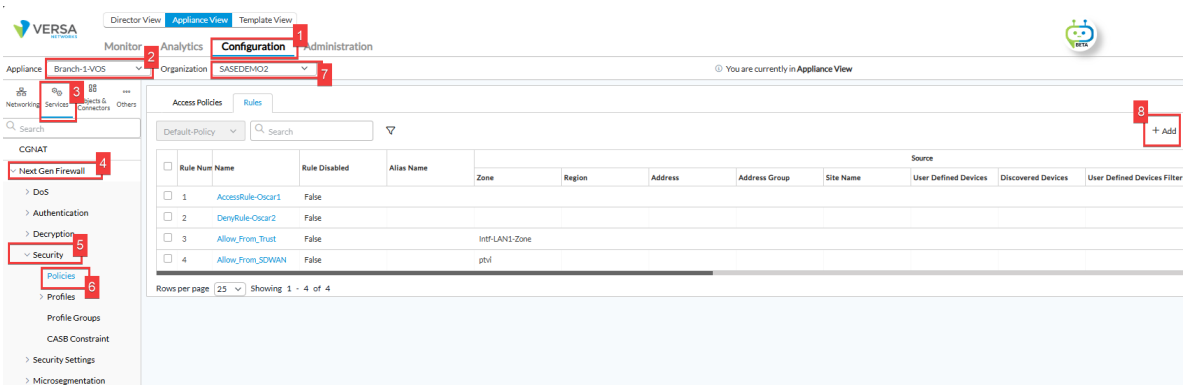


- Optional: Next, add the captive portal settings related to the Enterprise routing instance. And keep the random HTTP and HTTPS ports that will be used to display the captive portal.

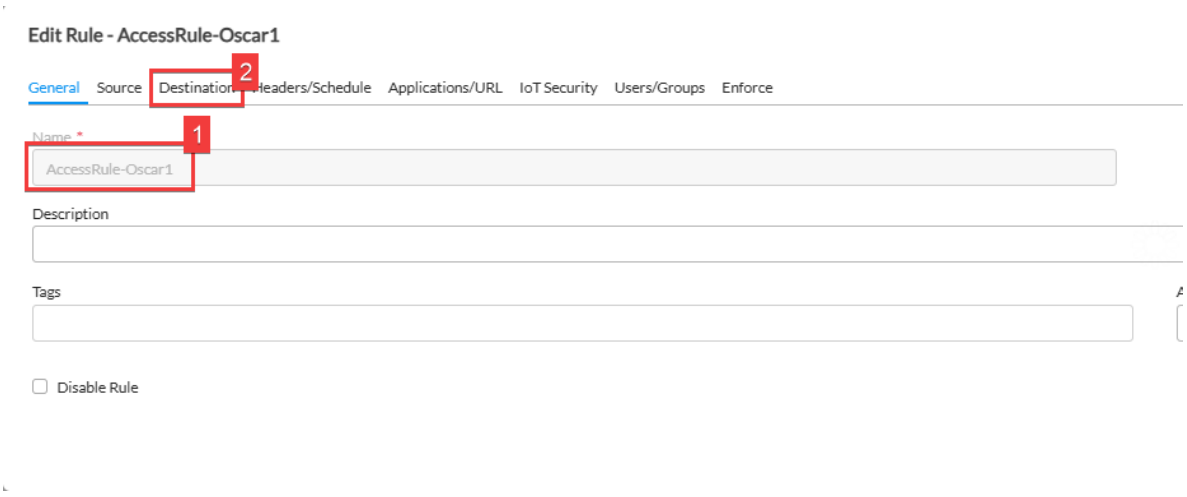


5. Create security policies with the Windows Remote Desktop server for users.

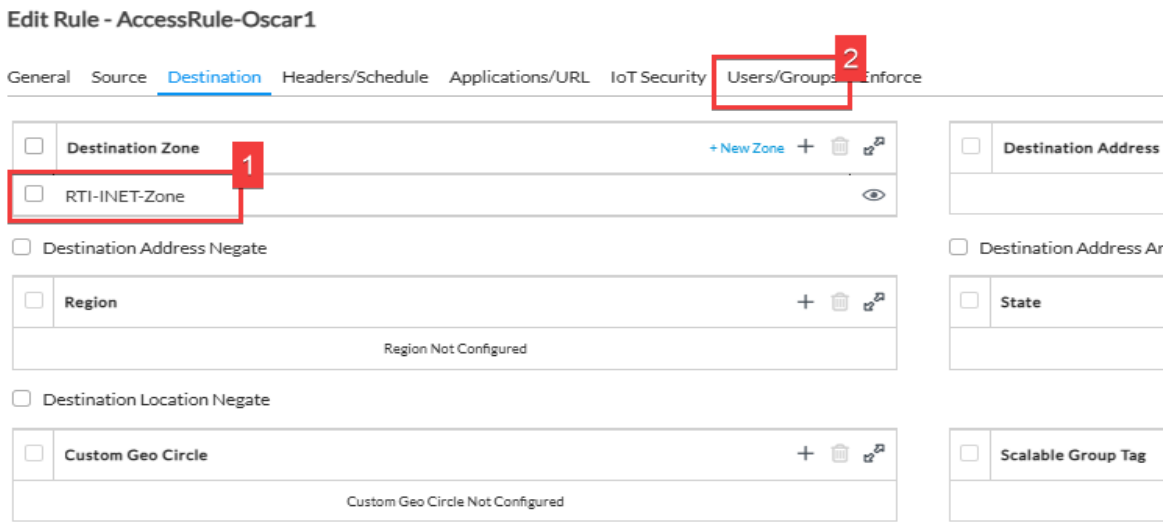
- Add a security rule to filter the required traffic.



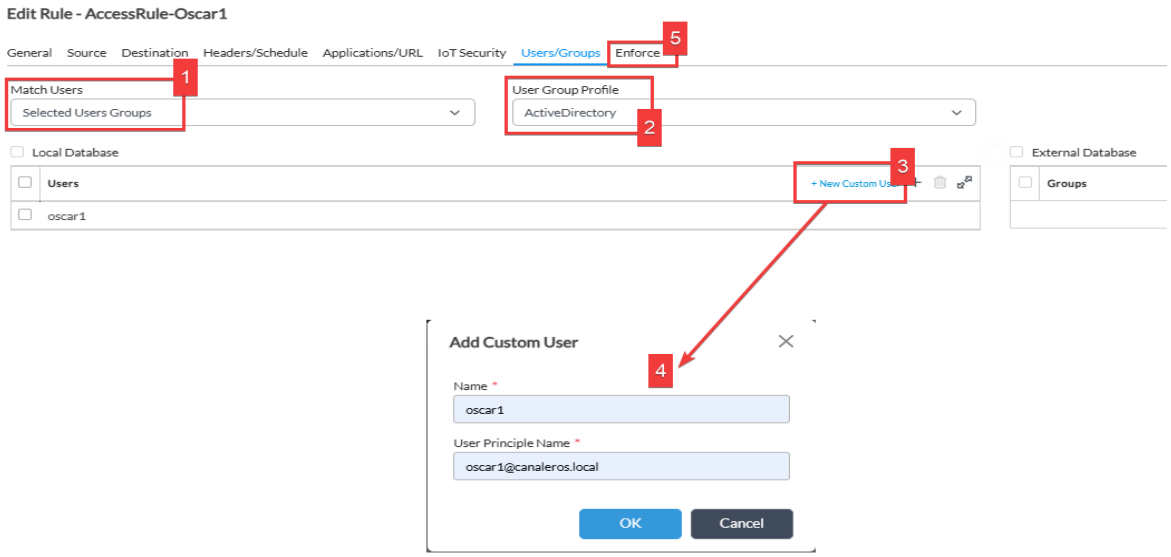
- Name the rule.



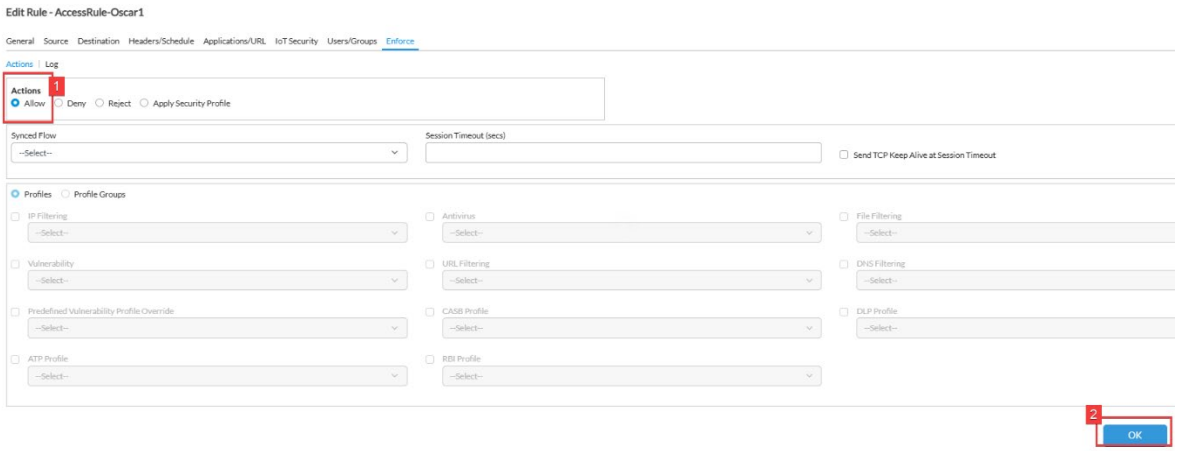
- Select INET as destination zone to match all traffic heading to the Internet.



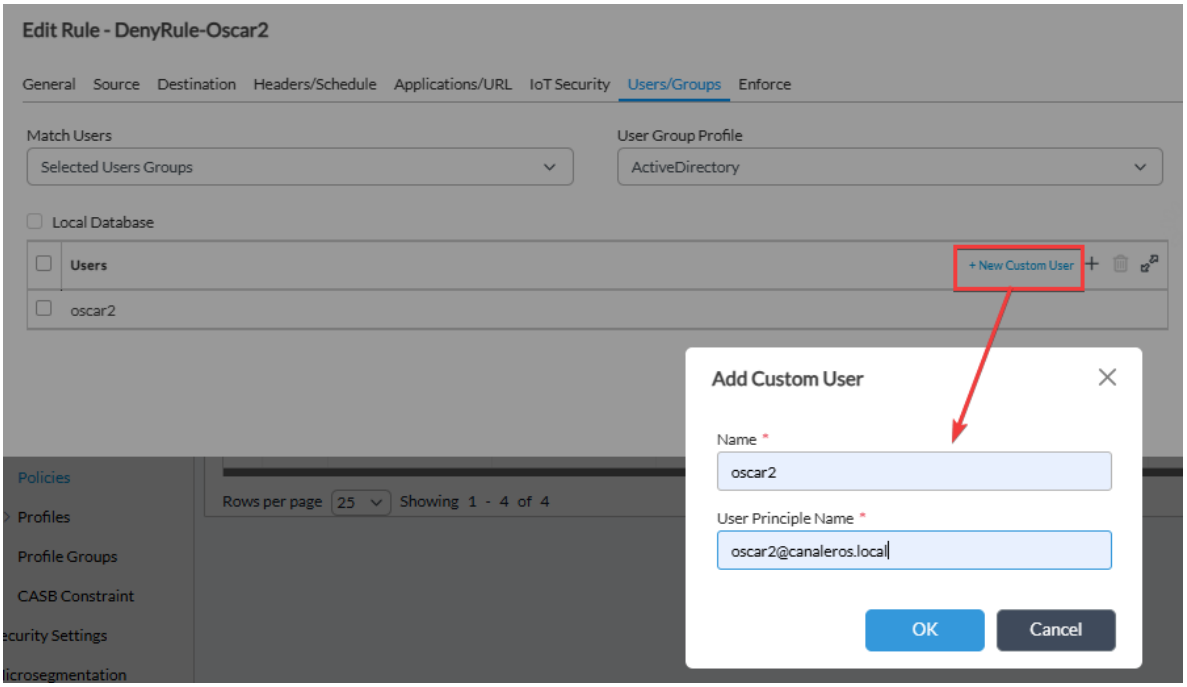
- Add custom user ”oscar1” matching the Active Directory data.



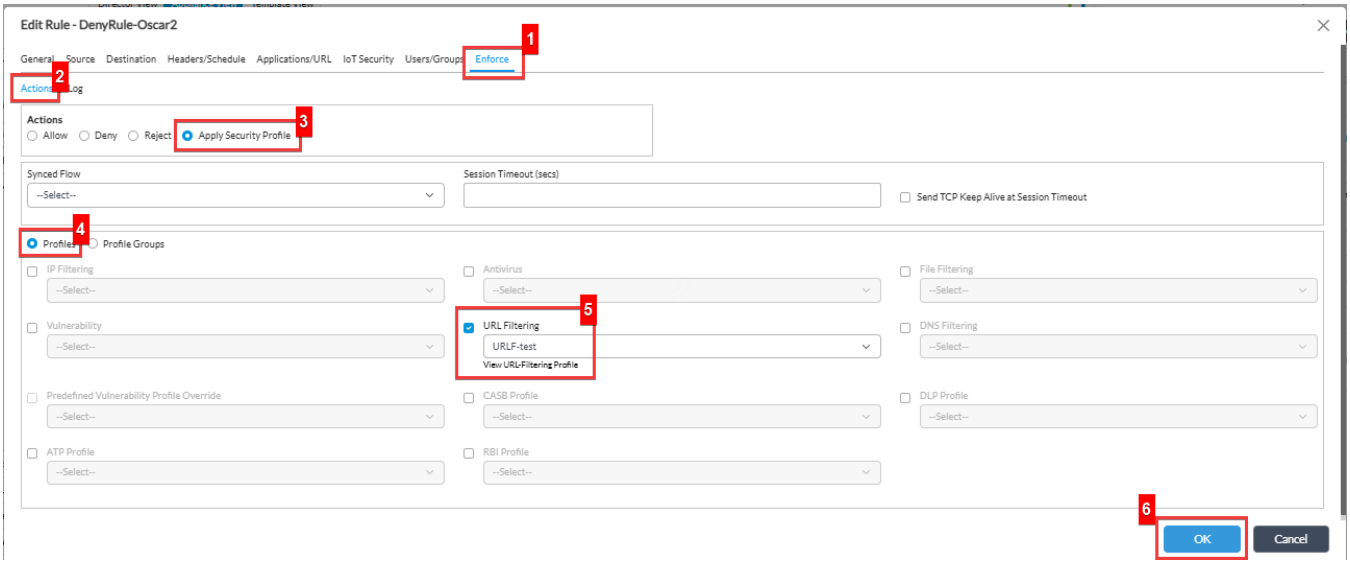
- Next policy will be the same just changing the following options (User and Action)



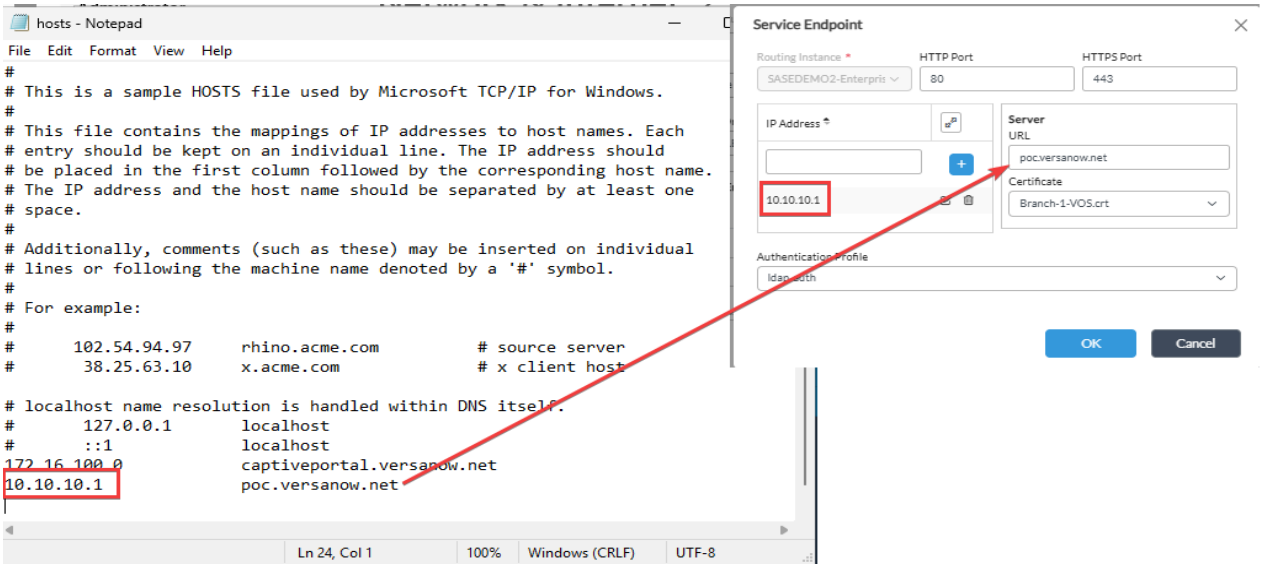
- Add custom user ”oscar2” matching the Active Directory data.

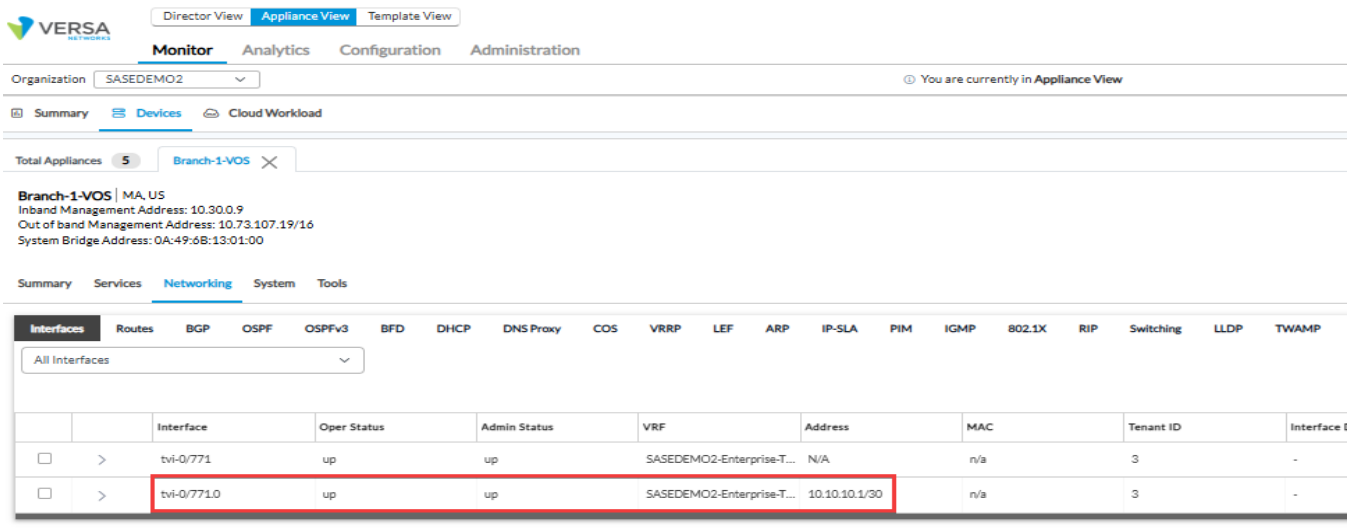


- In the Actions section a URL Filtering Profile was used to test the captive portal



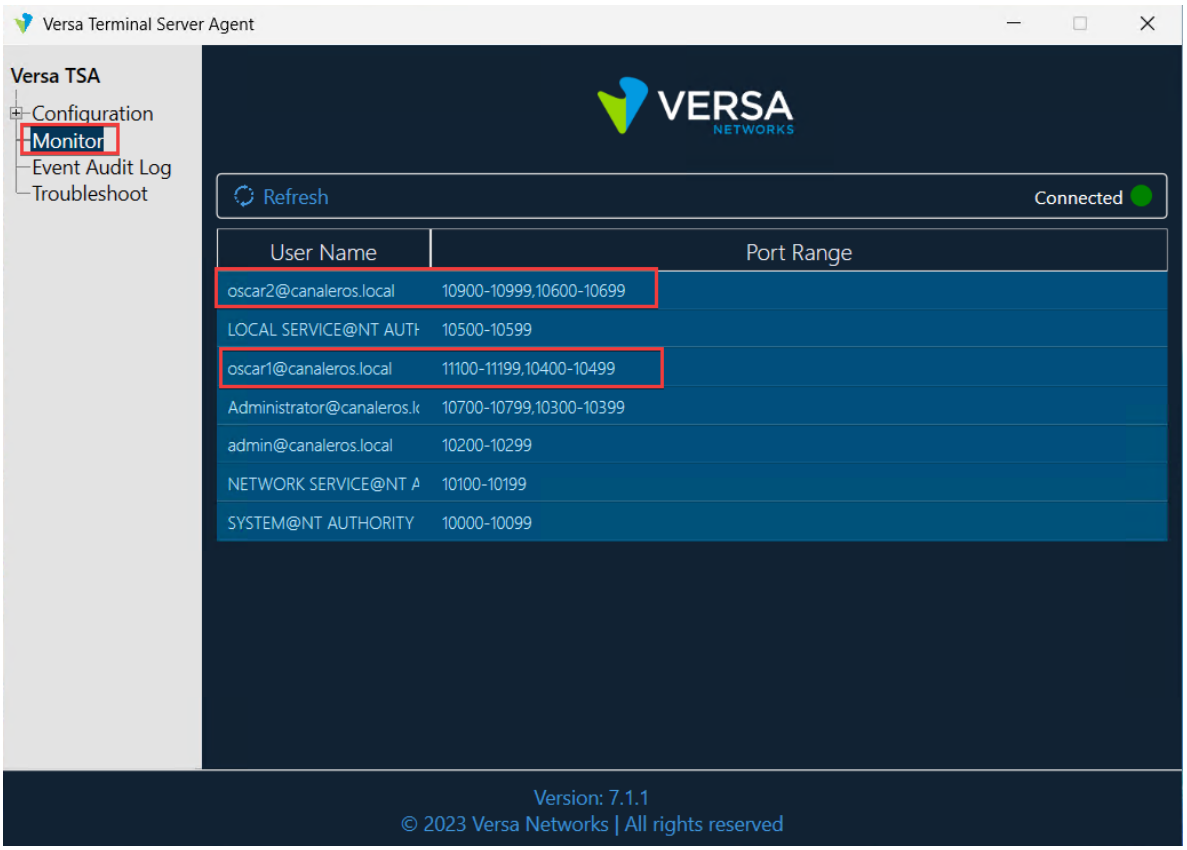
6. **Install the Versa TS Agent**
    - Follow the steps 4 “TSA Agent Installation and Configuration Steps” of “Scenario 1: Configuration Steps”. The only exception being FQDN (defined in in above steps 3), Enterprise-Name and User details
7. **FQDN for TSA Agent.**
    - Follow the steps 5 “FQDN for TSA Agent” of “Scenario 1: Configuration Steps”. The only exception is FQDN (defined in above steps 3) and tvi IP address.
    - Make sure the remote desktop server can resolve the FQDN URL with the LAN IP assigned to the SD-WAN branch device either by a DNS server or with a manual local host entry.
    - In this example, the local host file in the server was used to resolve the tvi Interface for the new Enterprise routing instance of the tenant in the SD-WAN Branch Device.



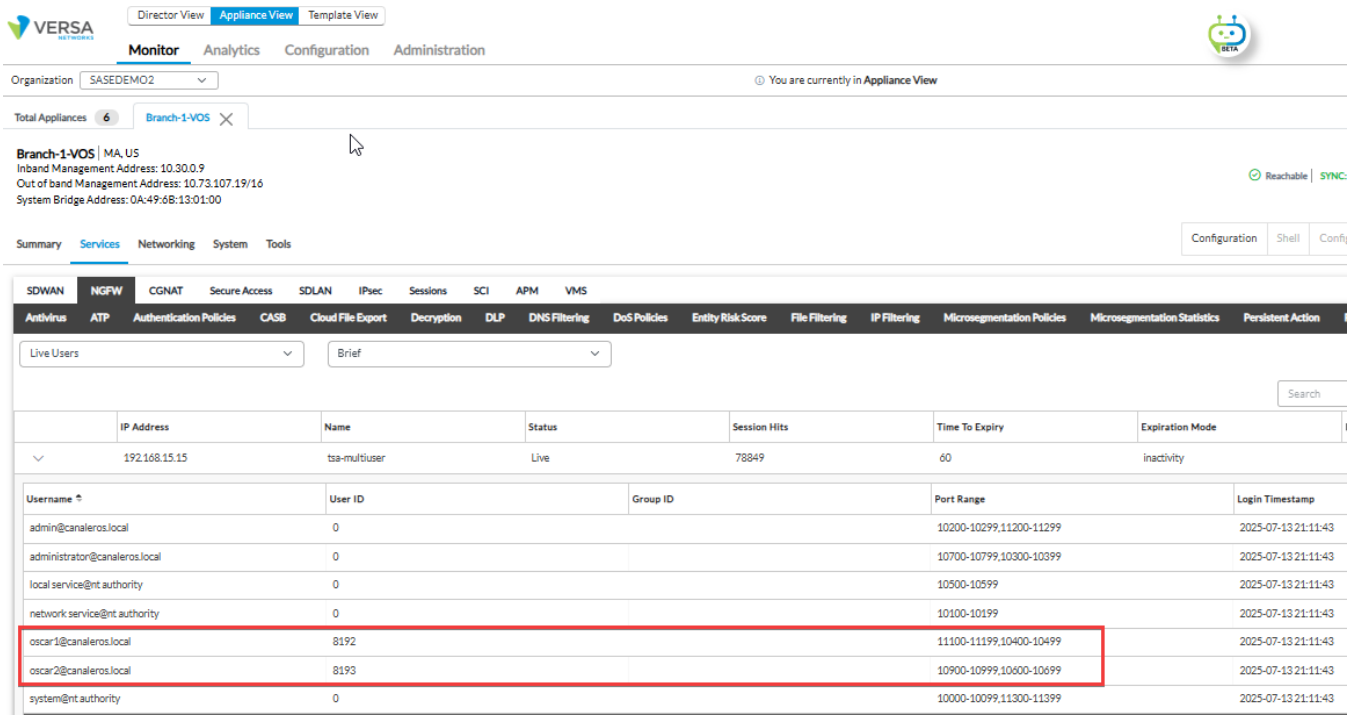


8. **Testing TSA connection**

- In this case, there are two users (oscar1 and oscar2) connected via Remote Desktop to the server. Notice that the TSA monitor tab is able to identify both users, and it shows the port range allocated to each user.

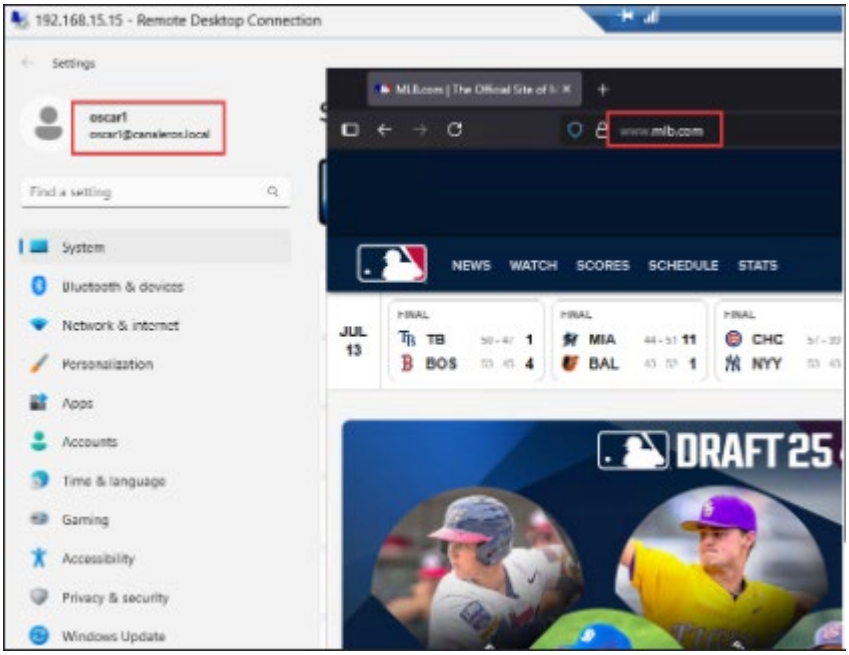


- TSA user-mapping in the Versa SD-WAN Branch device

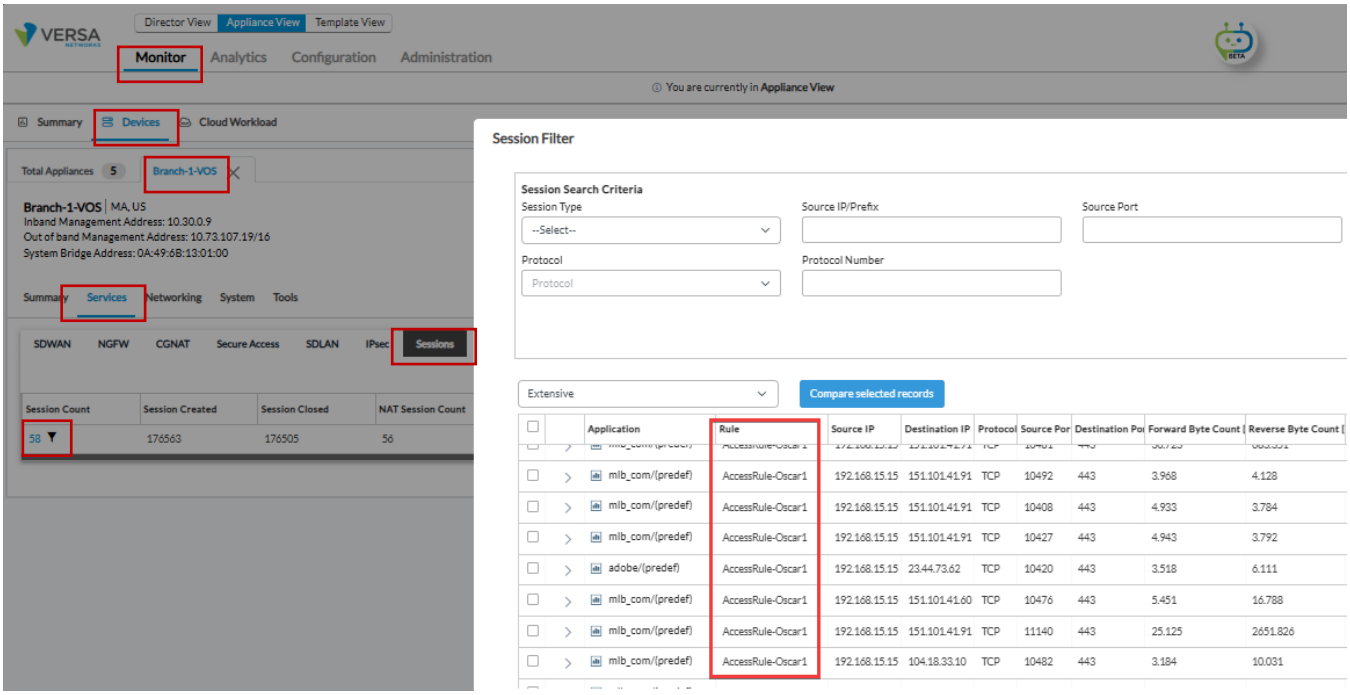


9. Tests Results

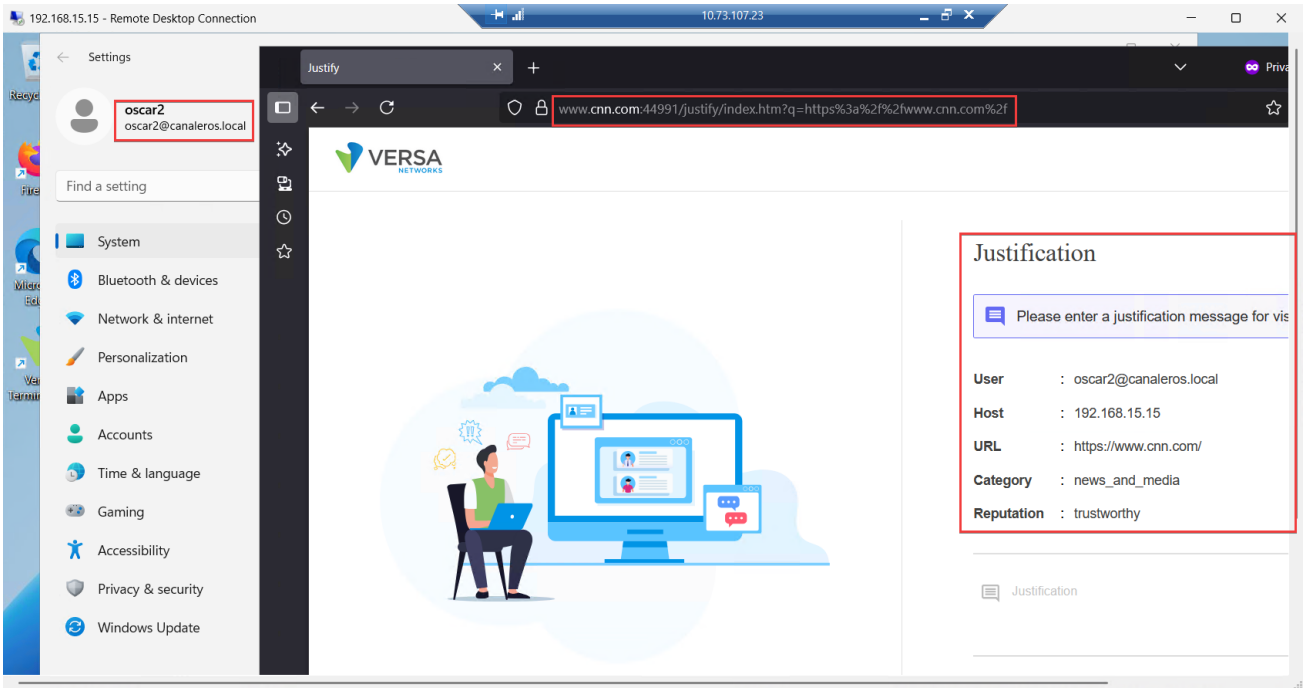
- Internet access is allowed to oscar1. Capture of the remote desktop connection of user" oscar1" and testing internet browsing.



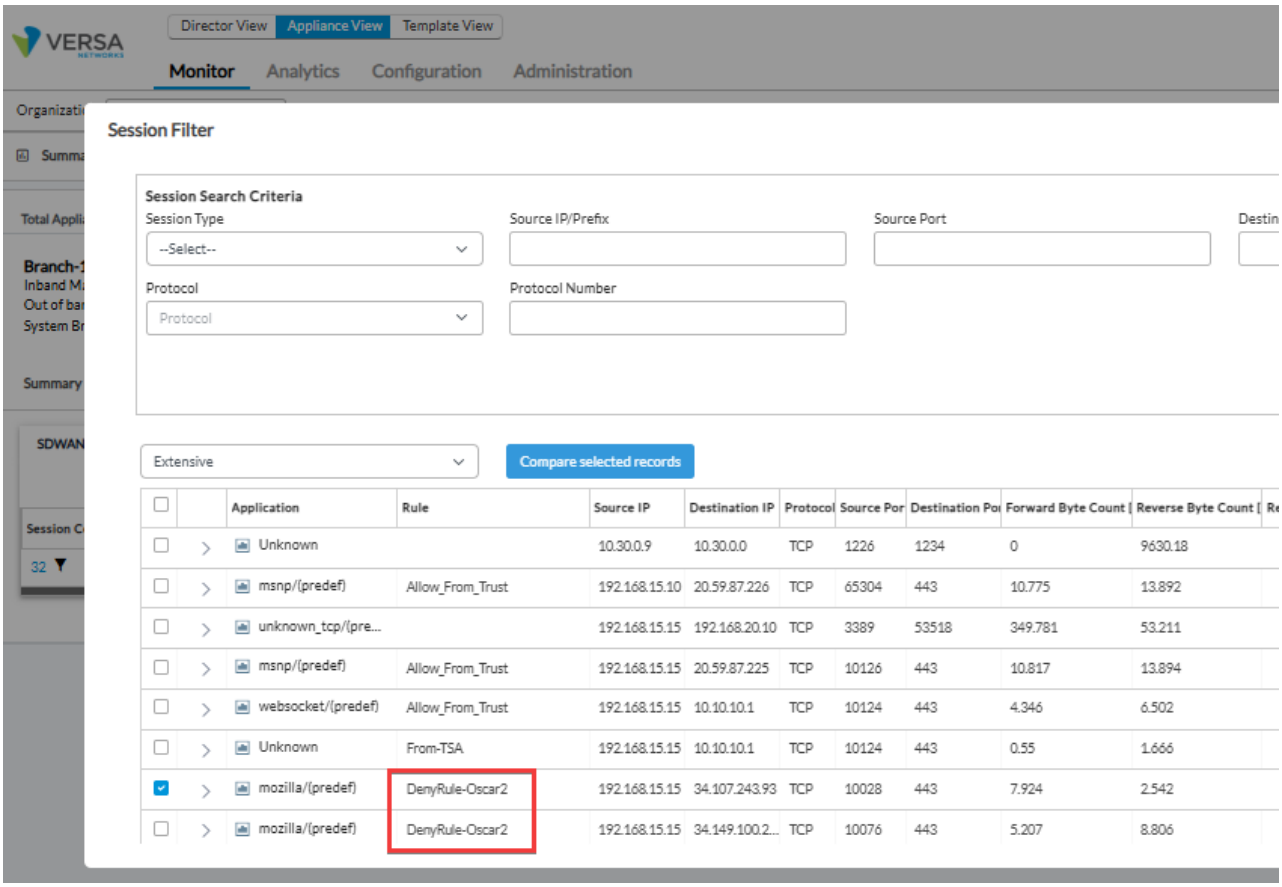
- In this output from the SD-WAN branch device, we can see the session of the internet webpage tested and the traffic being allowed by the policy created for user "oscar1"



- Internet access filtered to oscar2 (using captive portal with action justify)



- Capture of the remote desktop connection of user “oscar2” and testing internet browsing. In this output from the SD-WAN branch device, we can see the session of the internet webpage tested and the same number of bytes received being dropped.



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.