

# 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

|                |  |
|----------------|--|
| <b>Title</b>   | <b>Versa Terminal Server Agent (TSA) Use Cases</b> |
| <b>Author</b>  | Versa Professional Services                        |
| <b>Version</b> | V 1.0  |

## Disclaimer

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

|   |    |
|---|----|
| 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 .....   | 28 |
| About Versa.....  | 58 |

## 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.

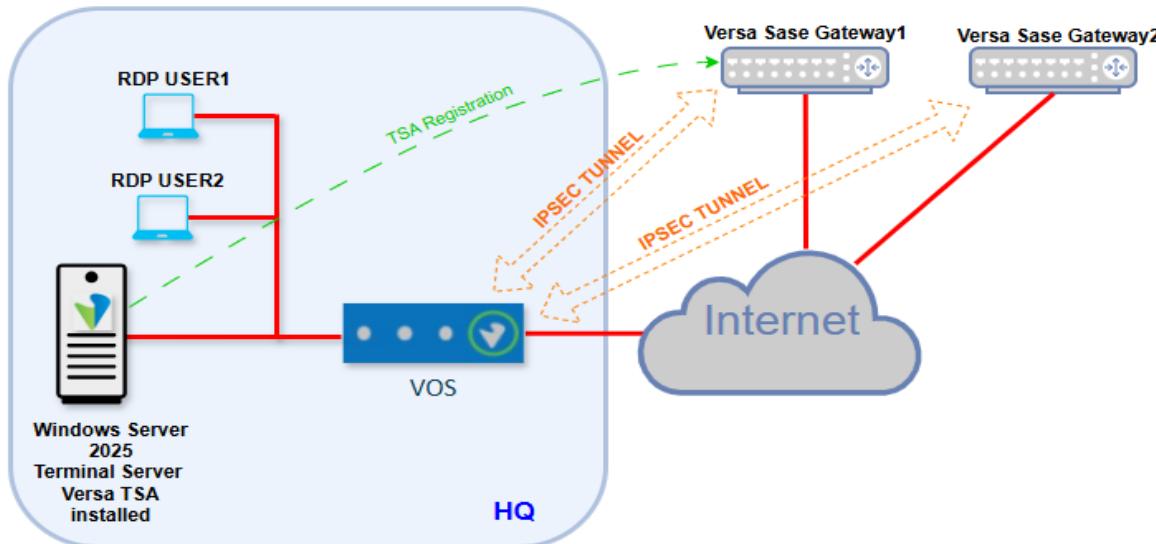
**Private Application Access:** When multiple users access private applications through a shared environment such as a terminal server, enforcing Zero Trust Network Access (ZTNA) requires identifying users individually, rather than relying on shared attributes like IP addresses. Terminal Server Access (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.

### Terminal Server at HQ with Internet via SSE Gateway



## 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:

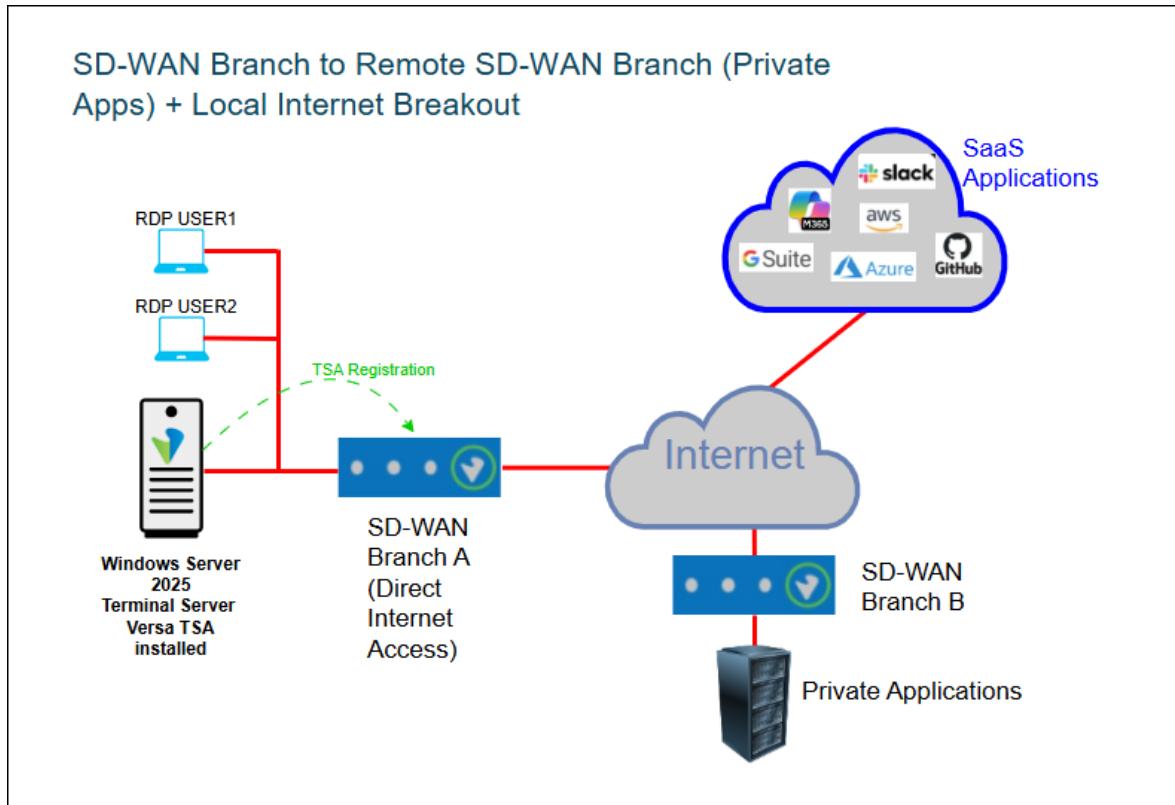
- **Pre-configured SSE Portal URL:** The SSE Gateway is pre-configured with a Portal URL/Captive Portal URL. The TSA agent uses this URL during the registration process.
- **TSA Agent Configuration:** The Versa TSA Agent, installed on the Terminal Server, is configured to communicate with the SSE Gateway 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

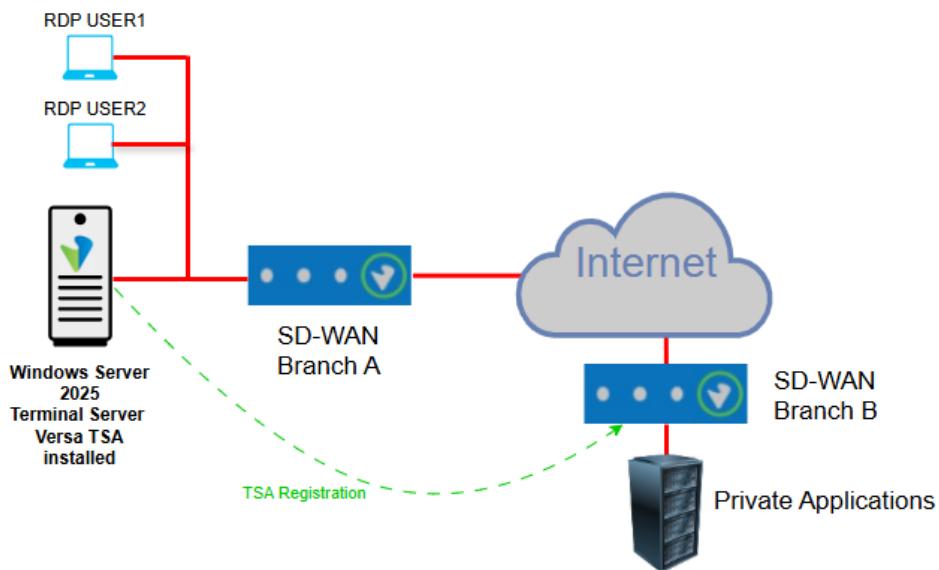
- **Routing-Instance for Captive Portal:** To ensure TSA registration on the captive portal does not break the URLF captive portal action, we will create a separate TSA routing instance, which will be used for registration of TSA agents in Branch A. A paired TVI will be configured between the TSA routing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

### SD-WAN Branch to Remote SD-WAN Branch (Private Apps Only)



### 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).

The screenshot shows the Versa Concerto interface. The left sidebar has 'View' (1) highlighted. The main area shows 'SASEDEMO2' and 'CONFIGURATION'. The 'Secure SD-WAN' tab is selected. Under 'Real-Time Protection', 'Secure Access' (2) is expanded, and 'Terminal Server Agent (TSA)' (3) is selected. A tooltip 'Below are all the rules' is visible above the configuration table.

- 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)**

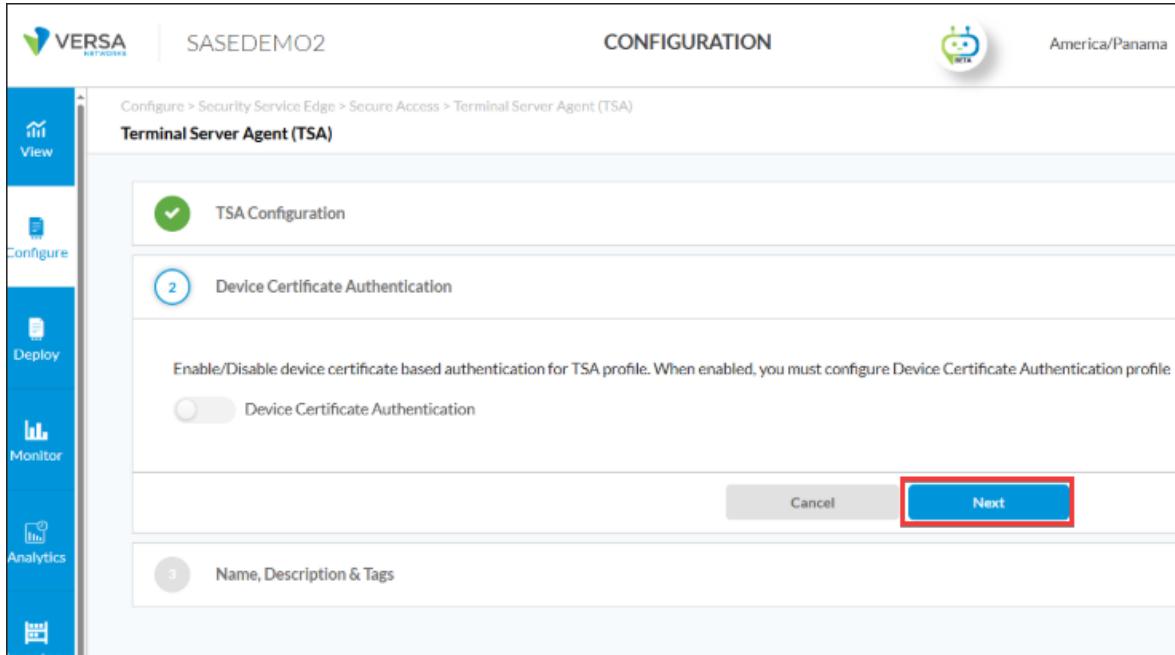
- **Sync Interval:** Enter how often, in minutes, to synchronise the configuration with the TSA.
- **Username Format:** Select the username format to have the TSA recognise
  - **userPrincipalName**—User principal name. A user principal name consists of a prefix (user account name), followed by the @ 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  |

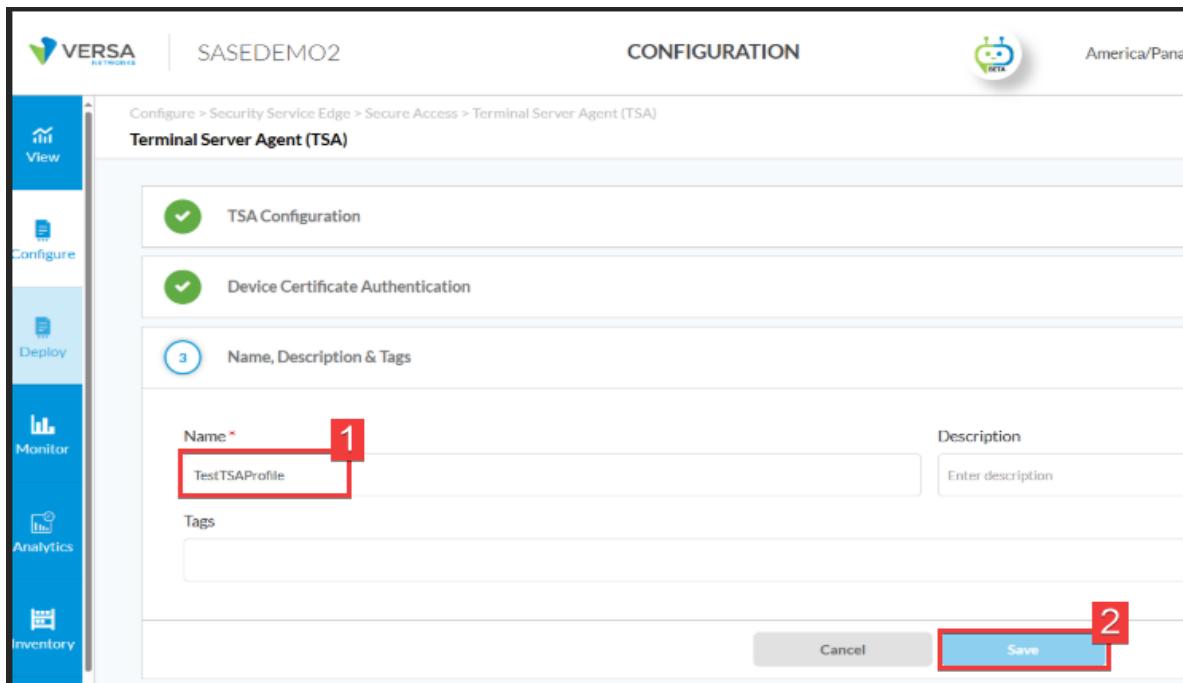
| Item                 | Value                             |
|----------------------|-----------------------------------|
| Total Ports Required | $4 \times 5000 = \mathbf{20,000}$ |
| Reserved Port Range  | <b>10000-30000</b>                |
| Fail Mode            | Close (recommended)               |

- 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.



The screenshot shows the VERSA Network interface for configuring a TSA profile. The left sidebar has buttons for View, Configure, Deploy, Monitor, and Analytics. The main area shows the path: Configure > Security Service Edge > Secure Access > Terminal Server Agent (TSA). The sub-section is 'Terminal Server Agent (TSA)'. Step 1, 'TSA Configuration', is completed. Step 2, 'Device Certificate Authentication', is currently selected. It contains a note: 'Enable/Disable device certificate based authentication for TSA profile. When enabled, you must configure Device Certificate Authentication profile' and a toggle switch that is off. Step 3, 'Name, Description & Tags', is shown but not yet completed. At the bottom are 'Cancel' and 'Next' buttons, with 'Next' being highlighted with a red box.

- 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.*



VERSASEDEMO2 | SASEDEMO2 | CONFIGURATION | America/Pana

Configure > Security Service Edge > Secure Access > Terminal Server Agent (TSA)

**Terminal Server Agent (TSA)**

**TSA Configuration** (checked)

**Device Certificate Authentication** (checked)

**3 Name, Description & Tags**

**Name**  **1**

**Description**

**Tags**

**Save** **2** | Cancel

## 2. Configure the user's authentication profile.

- Create a user authentication profile to match remote desktop users (in this case, Active Directory).

The screenshot shows the VERSA Configuration interface for a device named 'SASEDEMO2'. The left sidebar has a 'Configure' button highlighted with a red box and the number '1'. The main content area shows a table for 'Terminal Server Agent (TSA)' with a sync interval of 360 minutes and a username format of 'sAMAccountName'. The 'User and Device Authentication' section is expanded, with the 'Profiles' item highlighted with a red box and the number '3'. The 'Profiles' section contains a table with one row, showing 'Profile 1' with a 'Sync Interval (Mins)' of 360 and a 'Username Format' of 'sAMAccountName'.

|           | Sync Interval (Mins) | Username Format |
|-----------|----------------------|-----------------|
| Profile 1 | 360                  | sAMAccountName  |

- Fill in the information of the Active Directory Server

## Edit LDAP Authentication Profile: OscarActiveDirectory

1

2

3

4

Cancel Skip to Review Next

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

## Edit LDAP Authentication Profile: OscarActiveDirectory

1

2

3

Bind DN \* CN=admin,CN=Users,DC=canaleros,DC=local

Bind Password \*

Bind Timeout (sec) 30

Base DN \* CN=Users,DC=canaleros,DC=local

Domain Name \* canaleros.local

Base Domain

Search Timeout (sec) 30

Cache Expiry Time (mins) 10

Concurrent Logins 1

Cancel Skip to Review Next

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

Edit LDAP Authentication Profile: OscarActiveDirectory

1. Settings 2. User And Group Profile 3. Review & Submit

|                            |                   |                  |
|----------------------------|-------------------|------------------|
| Group Object Class *       | Group Name *      | Group Member *   |
| group                      | name              | memberOf         |
| User Object Class *        | User Name *       |                  |
| user                       | displayName       |                  |
| Refresh Interval (seconds) | Password Last Set | Password Max Age |
| 180                        | pwdLastSet        | maxPwdAge        |

Cancel Back Skip to Review Next

- Fill in a name for the authentication profile.

Edit LDAP Authentication Profile: OscarActiveDirectory

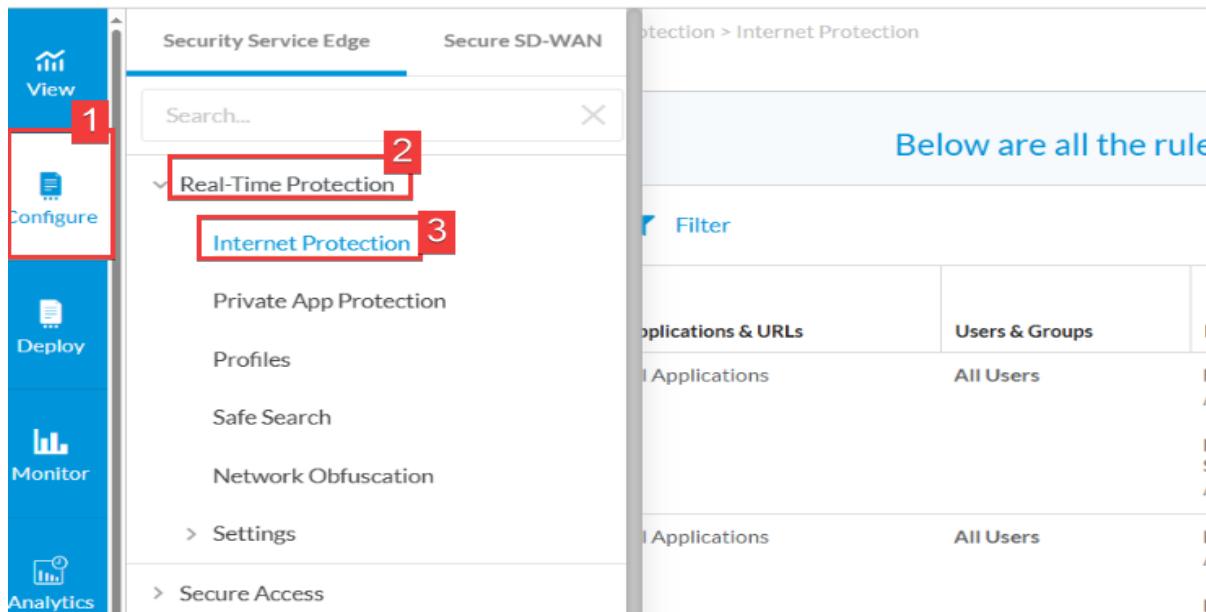
1. Settings 2. User And Group Profile 3. Review & Submit

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

|                      |             |
|----------------------|-------------|
| General              |             |
| Name                 | Description |
| OscarActiveDirectory |             |
| Tags                 |             |

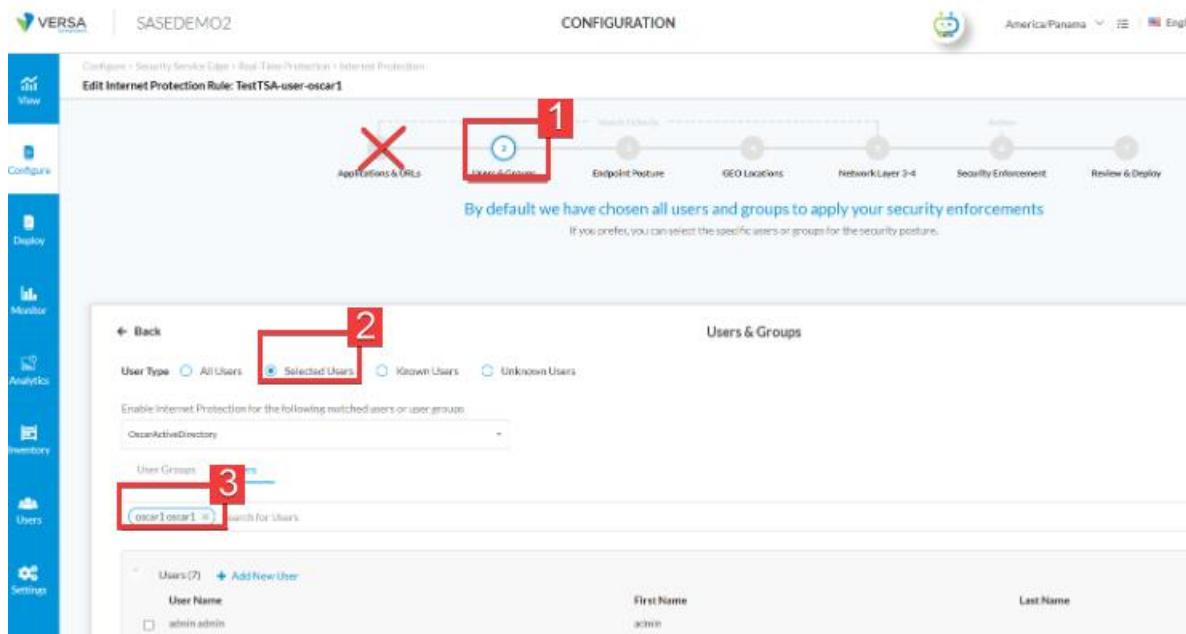
### 3. Create Security Policies

- Add a security rule to filter the required traffic.



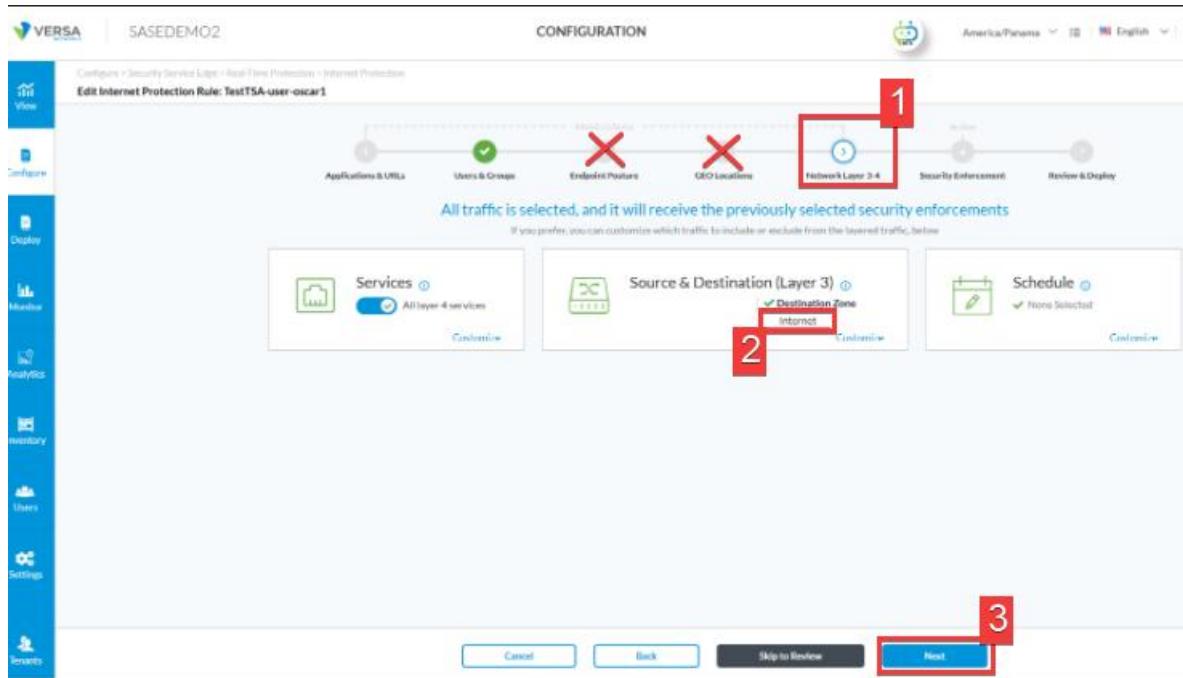
The screenshot shows the VERSA SASEDEMO2 Configuration interface. The left sidebar has a 'Configure' button highlighted with a red box and the number 1. The main menu under 'Real-Time Protection' has 'Internet Protection' highlighted with a red box and the number 3. The right panel displays a list of Internet Protection rules, with the first rule shown in detail. The rule title is 'TestTSA-user-oscar1'. The rule details show 'All Applications' and 'All Users' selected. The rule description states: 'By default we have chosen all users and groups to apply your security enforcements. If you prefer, you can select the specific users or groups for the security posture.'

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

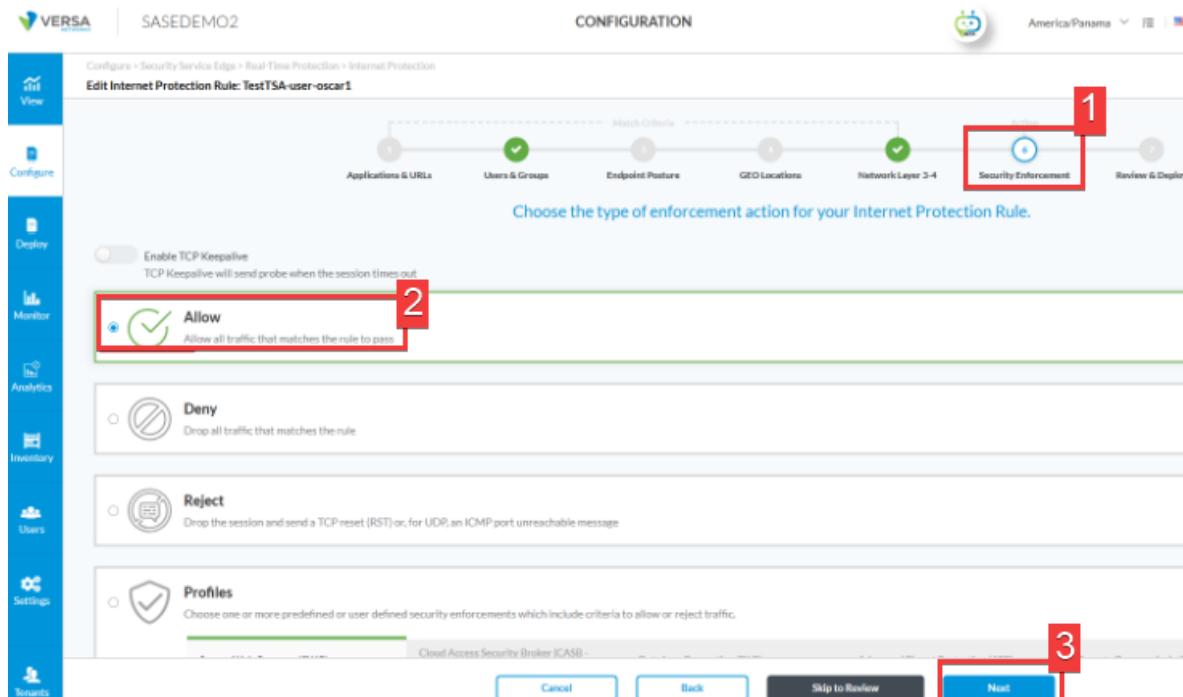


The screenshot shows the 'Edit Internet Protection Rule' configuration page for the rule 'TestTSA-user-oscar1'. The left sidebar has a 'Configure' button highlighted with a red box and the number 1. The main panel shows the 'Users & Groups' section. The 'User Type' is set to 'Selected Users' (highlighted with a red box and the number 2). The 'User Groups' dropdown is set to 'oscar1' (highlighted with a red box and the number 3). The table below shows a single user entry: 'User Name: oscar1', 'First Name: admin', and 'Last Name: '.

- Matched all services with Internet as destination.



- Allow the traffic.



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

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

Edit Internet Protection Rule: TestTSA-user-oscar1

CONFIGURATION

Review your Internet Protection Policy configurations below.

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

General

Name: **TestTSA-user-oscar1** 2

Tags:

Rule Is Enabled:

Applications & URLs 1

Users & Groups 2

Endpoint Posture

GEO Locations

Network Layer 3-4

Security Enforcement

Action:

Review & Deploy 3

- 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.

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

Edit Internet Protection Rule: TestTSA-user-oscar

CONFIGURATION

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

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

Users & Groups 1

User Type:  Selected Users 2

Enable Internet Protection for the following matched users or user groups:

OscarActiveDirectory

User Groups:  Users 3

oscar2

oscar2

Users (7) 3

Add New User

User Name:  admin

First Name:  admin

Last Name:

Cancel Back Skip to Review Next

Configure > Security Service Edge > Real-Time Protection > Internet Protection  
Edit Internet Protection Rule: TestTSA-user-oscar

CONFIGURATION

Match Criteria

1 Applications & URLs 2 Users & Group 3 Endpoint Posture 4 GEO Locations 5 NetworkLayer 3-4 6 Security Enforcement 7 Review & Deploy

Choose the type of enforcement action for your Internet Protection Rule.

Enable TCP Keepalive  
TCP Keepalive will send probe when the session times out

Allow: Allow all traffic that matches the rule to pass

**Deny:** Drop all traffic that matches the rule (highlighted with a red box and labeled '2')

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

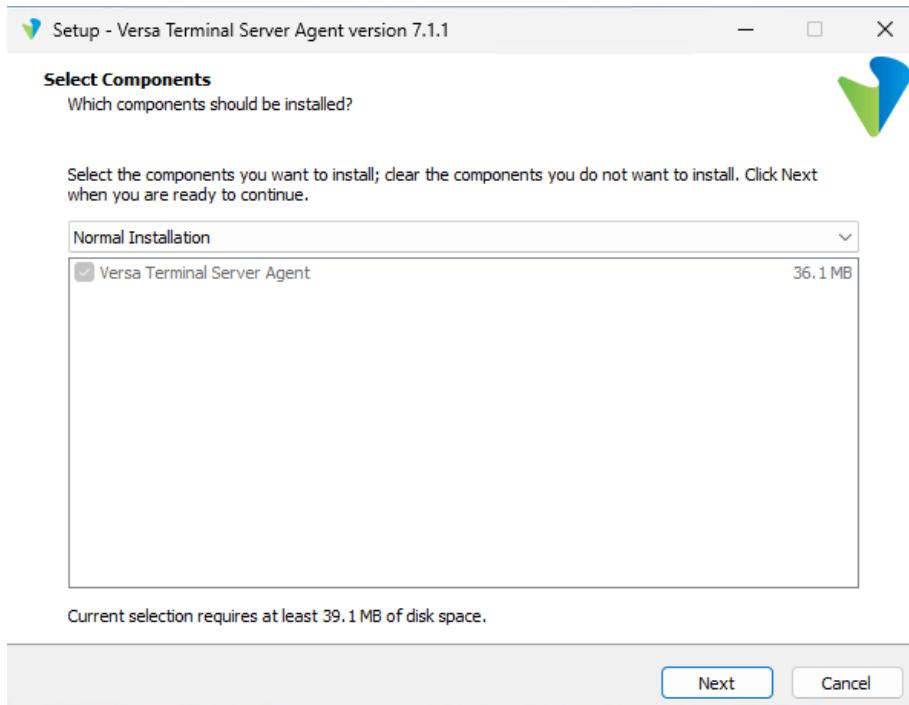
Profiles: Choose one or more predefined or user-defined security enforcements which include criteria to allow or reject traffic.

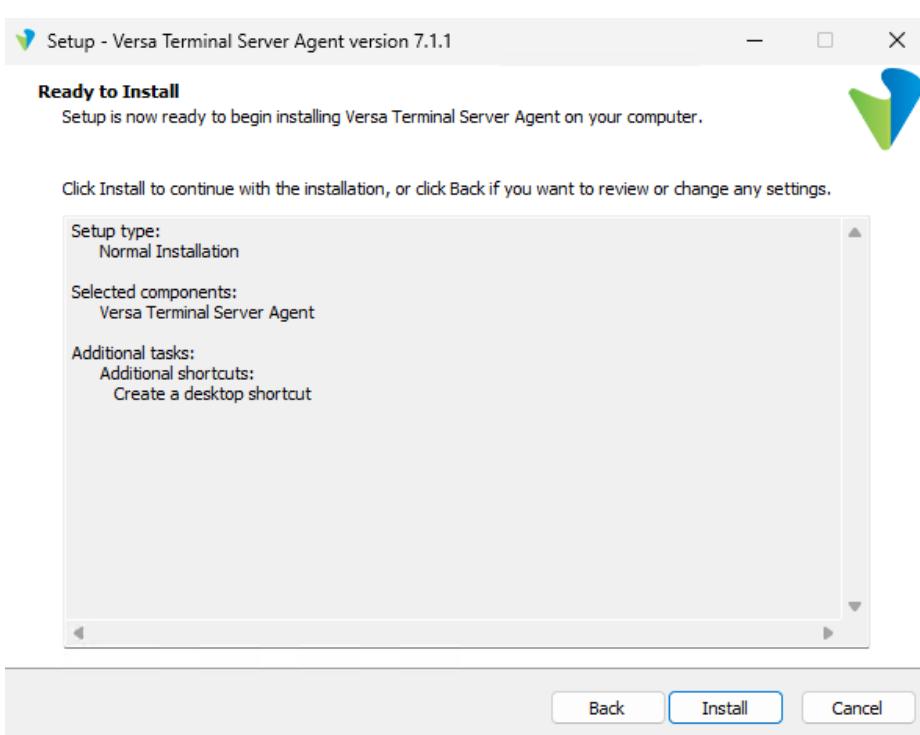
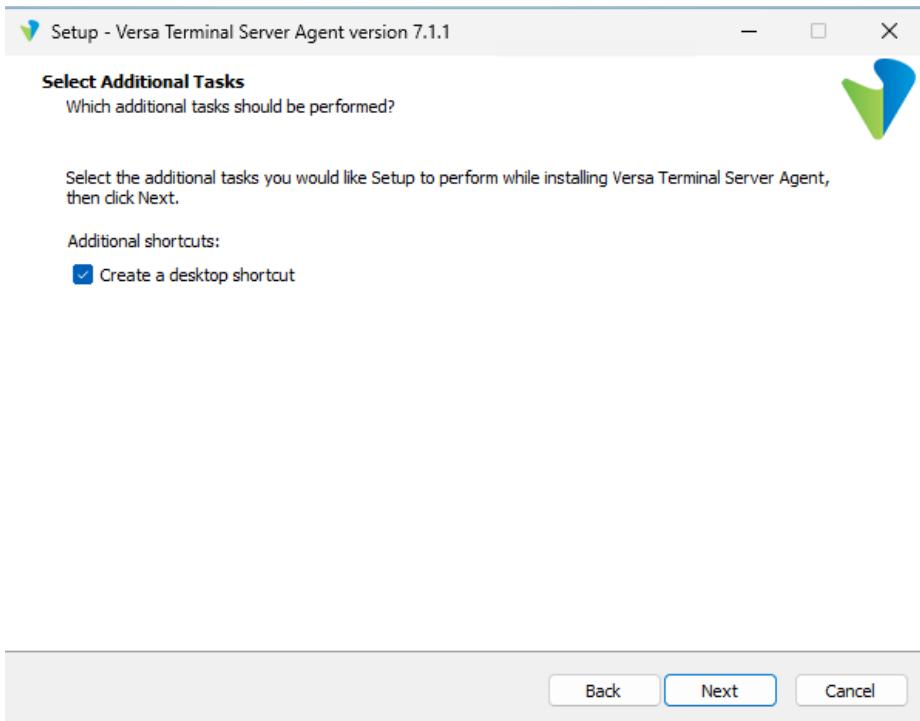
Close Access Security Broker (CASB) -

Cancel Back Skip to Review Next

#### 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.





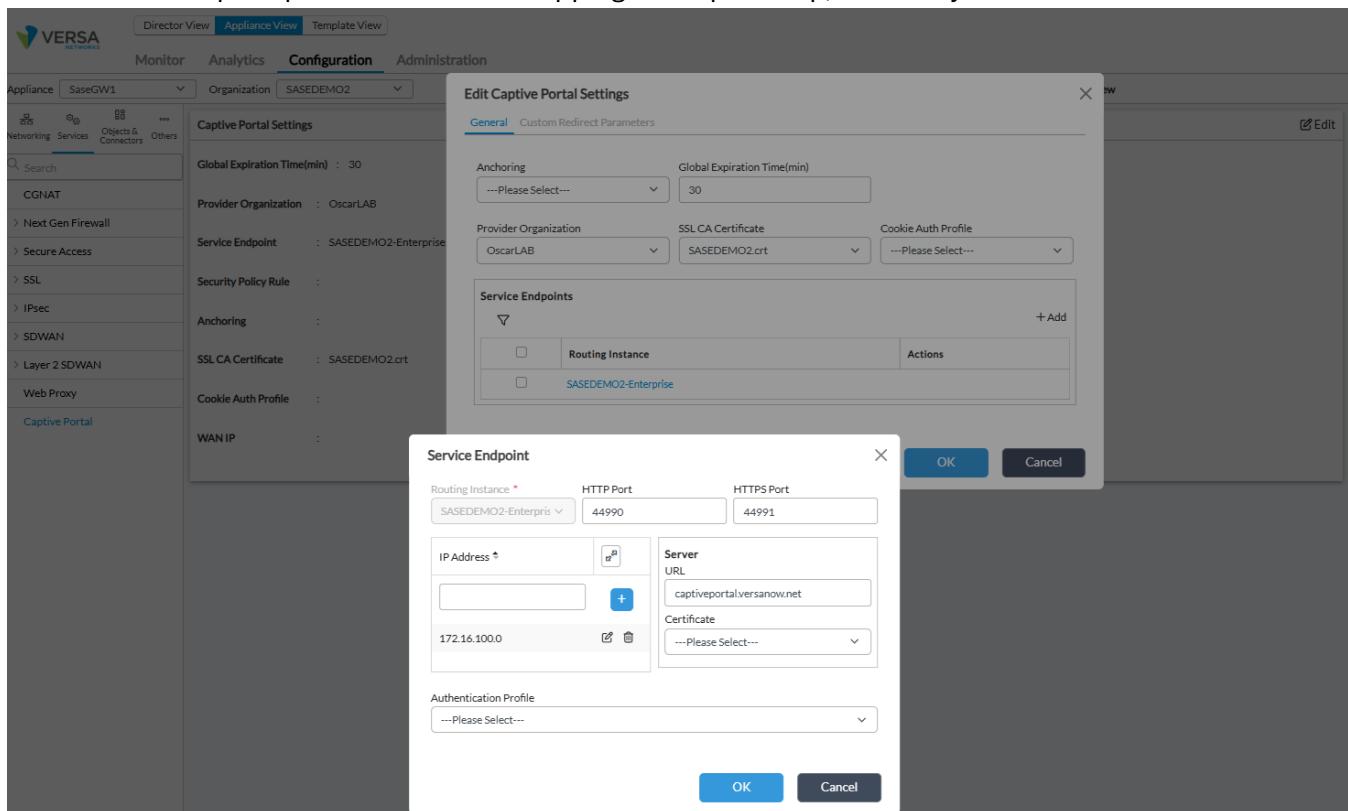
## 5. FQDN for TSA Agent.

We propose two options here.

- a) 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)
- b) 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.

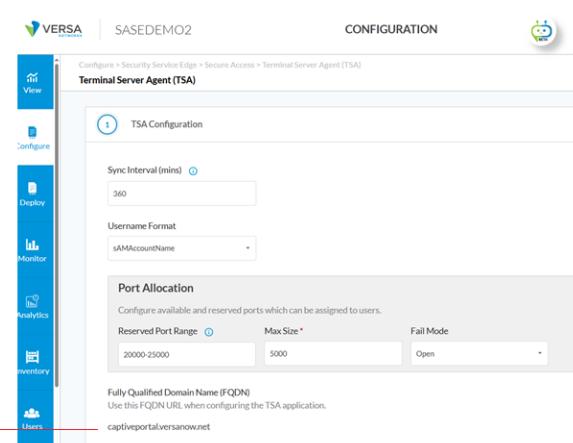


The screenshot shows the VERSA Director UI with the 'Configuration' tab selected. A modal dialog titled 'Edit Captive Portal Settings' is open. The 'General' tab is selected, showing fields for 'Global Expiration Time(min)' (set to 30), 'Provider Organization' (set to OscarLAB), and 'Service Endpoint' (set to SASEDEMO2-Enterprise). Below these are sections for 'Service Endpoints' and 'Cookie Auth Profile'. A sub-dialog titled 'Service Endpoint' is also open, showing a table with a single entry for 'SASEDEMO2-Enterprise'. The sub-dialog includes fields for 'Routing Instance' (set to SASEDEMO2-Enterprise), 'HTTP Port' (set to 44990), 'HTTPS Port' (set to 44991), 'IP Address' (set to 172.16.100.0), 'Server URL' (set to captiveportal.versanow.net), and 'Certificate' (a dropdown menu). The sub-dialog has 'OK' and 'Cancel' buttons.

```
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
          |          |       |       |       |          |
          |          down  up    0    global  fe80::500a:49ff:fe6b:701/64
eth-0/1   n/a          up    up    -    -        -          -
lt-1/2    n/a          up    up    2    INET-Transport-VR  169.254.128.2/31
lt-1/2.0  n/a          up    up    2    -        -          -
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
tv1-0/2   n/a          up    up    -    -        -          -
tv1-0/2.0 n/a          up    up    2    OscarLAB-Control-VR  10.30.0.4/32
tv1-0/22  n/a          up    up    -    -        -          -
tv1-0/22.0 n/a          up    up    4    SASEDEMO2-Control-VR  10.30.0.4/32
tv1-0/23  n/a          up    up    -    -        -          -
tv1-0/23.0 n/a          up    up    4    SASEDEMO2-Control-VR  10.30.0.5/32
tv1-0/3   n/a          up    up    -    -        -          -
tv1-0/3.0 n/a          up    up    2    OscarLAB-Control-VR  10.30.0.5/32
tv1-0/602 n/a          up    up    -    -        -          -
tv1-0/602.0 n/a          up    up    2    INET-Transport-VR  169.254.0.2/31
tv1-0/603 n/a          up    up    -    -        -          -
tv1-0/603.0 n/a          up    up    2    OscarLAB-LAN-VR  169.254.0.3/31
tv1-1/103 n/a          up    up    -    -        -          -
tv1-1/103.0 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> █
```

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10    x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1    localhost
#      ::1          localhost
172.16.100.0    captiveportal.versanow.net
```



VERSATSA Configuration

Configure > Security Service Edge > Secure Access > Terminal Server Agent (TSA)

Terminal Server Agent (TSA)

TSA Configuration

Sync Interval (min): 360

Username Format: sAMAccountName

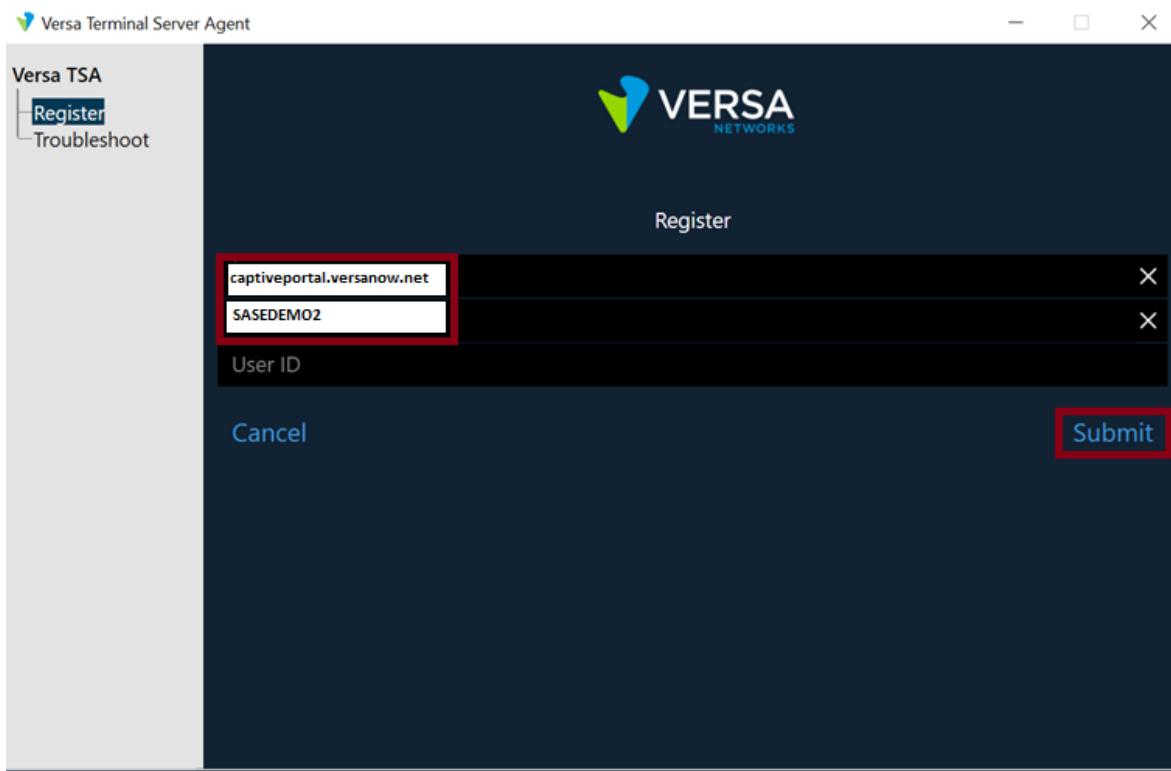
Port Allocation

Resered Port Range: 20000-25000, Max Size: 5000, Fail Mode: Open

Fully Qualified Domain Name (FQDN): captiveportal.versanow.net

## 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

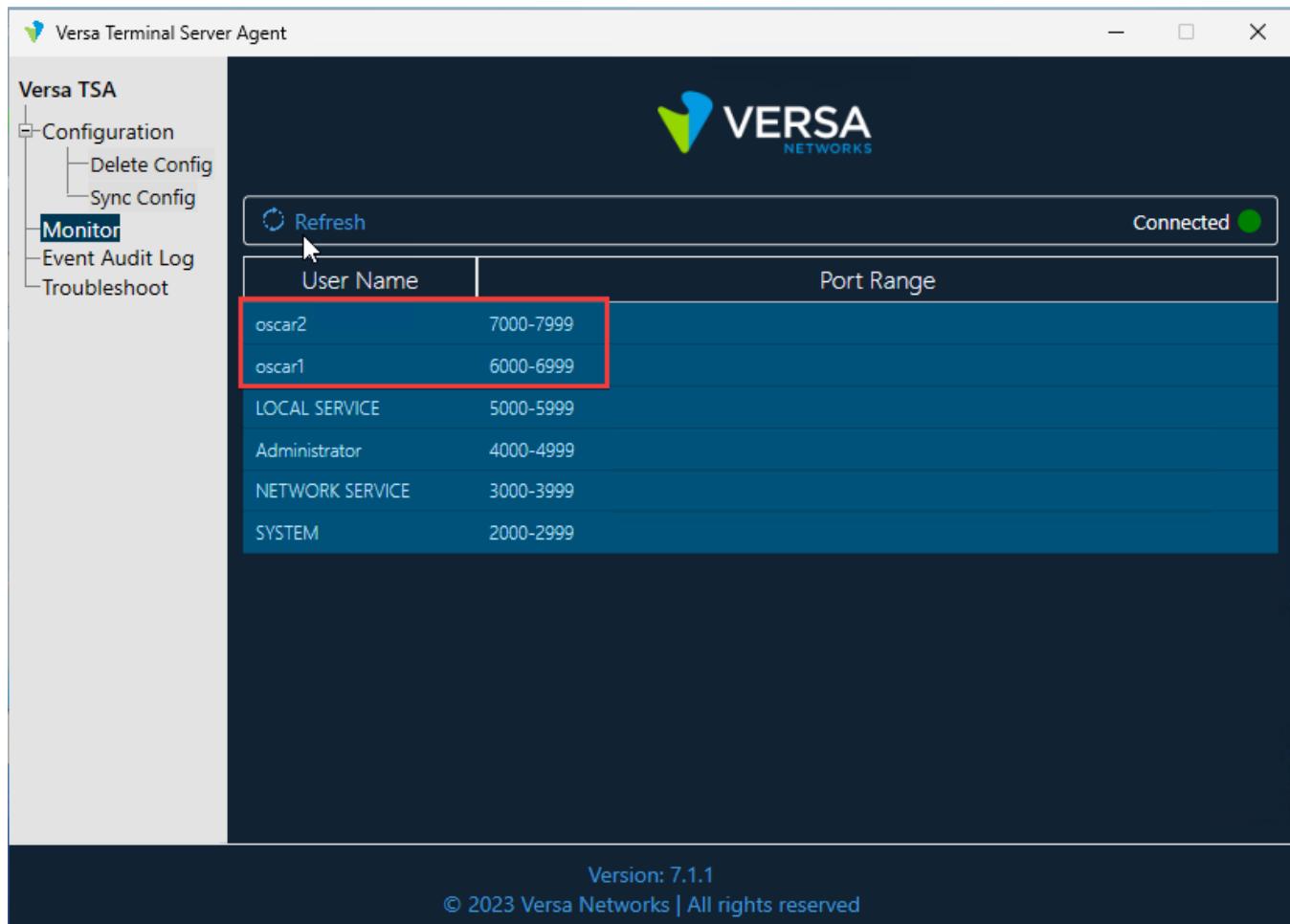


- Once registered, the Configuration tab will show settings acquired from the TSA Profile.



## 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.

VERSA NETWORKS

Director View Appliance View Template View

Monitor Analytics Configuration Administration

Organization: SASEDEMO2 You are currently in Appliance View

Summary Devices Cloud Workload

Total Appliances: 6 SaseGW1 X

SaseGW1 FL, US  
Inband Management Address: 10.30.0.5  
Out of band Management Address: 10.73.107.7/16  
System Bridge Address: 0A:49:6B:07:01:00

Reachable SYNC: IN

Configuration Shell Config

Summary Services Networking System Tools

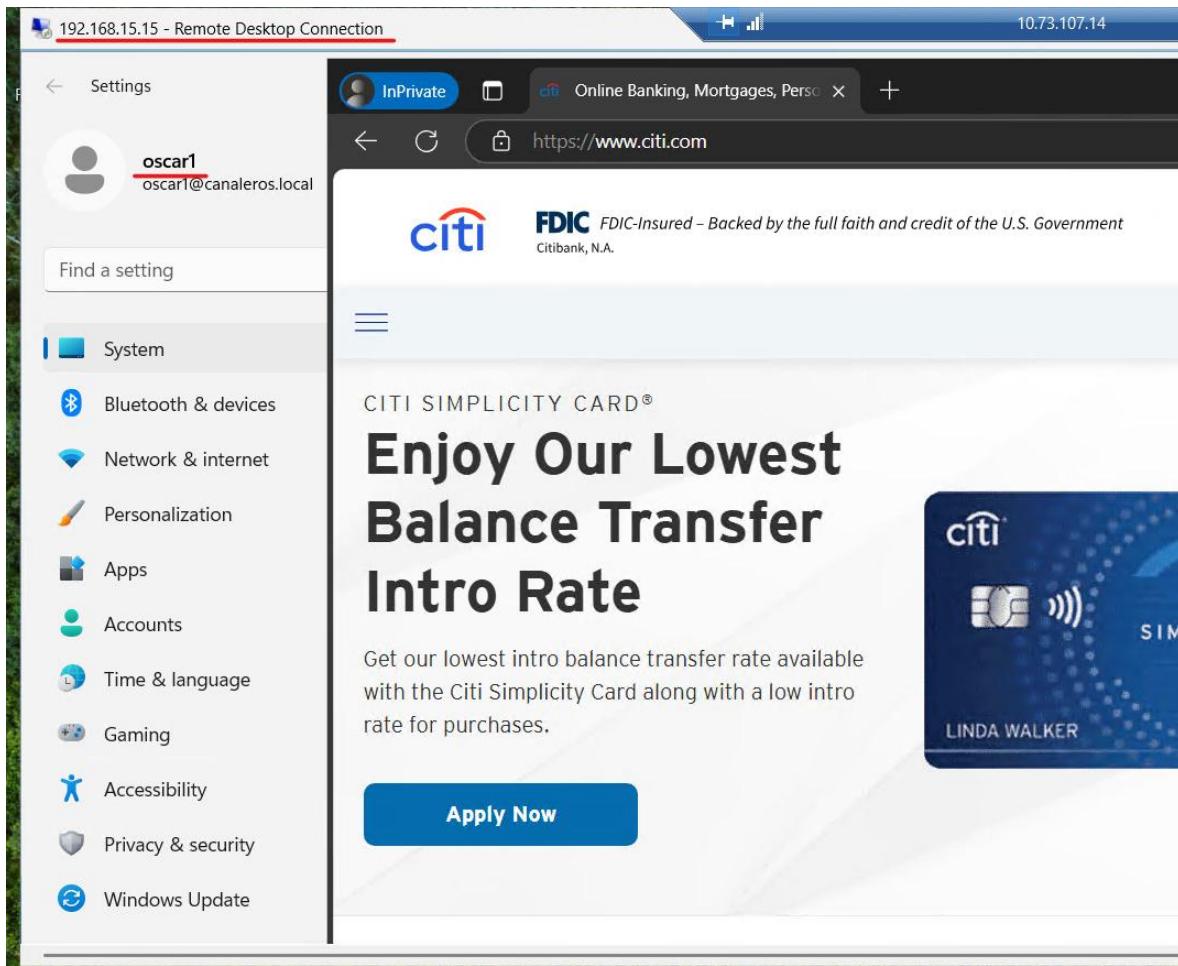
SDWAN NGFW CGNAT Secure Access SDLAN IPsec Sessions SCI APM VMS

DoS Policies Entity Risk Score File Filtering IP Filtering Microsegmentation Policies Microsegmentation Statistics Persistent Action Policies Security Packages Sessions SNAT SSL Cloud URL Filtering User Identification User Risk Sc

Live Users Detail Search

| Username        | User ID | Group ID | Port Range | Login Timestamp     |
|-----------------|---------|----------|------------|---------------------|
| administrator   | 0       |          | 4000-4999  | 2025-07-22 15:21:39 |
| local service   | 0       |          | 5000-5999  | 2025-07-22 15:21:39 |
| network service | 0       |          | 3000-3999  | 2025-07-22 15:21:39 |
| oscar1          | 8194    |          | 6000-6999  | 2025-07-22 15:21:39 |
| oscar2          | 8193    |          | 7000-7999  | 2025-07-22 15:21:39 |
| system          | 0       |          | 2000-2999  | 2025-07-22 15:21:39 |

- 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"

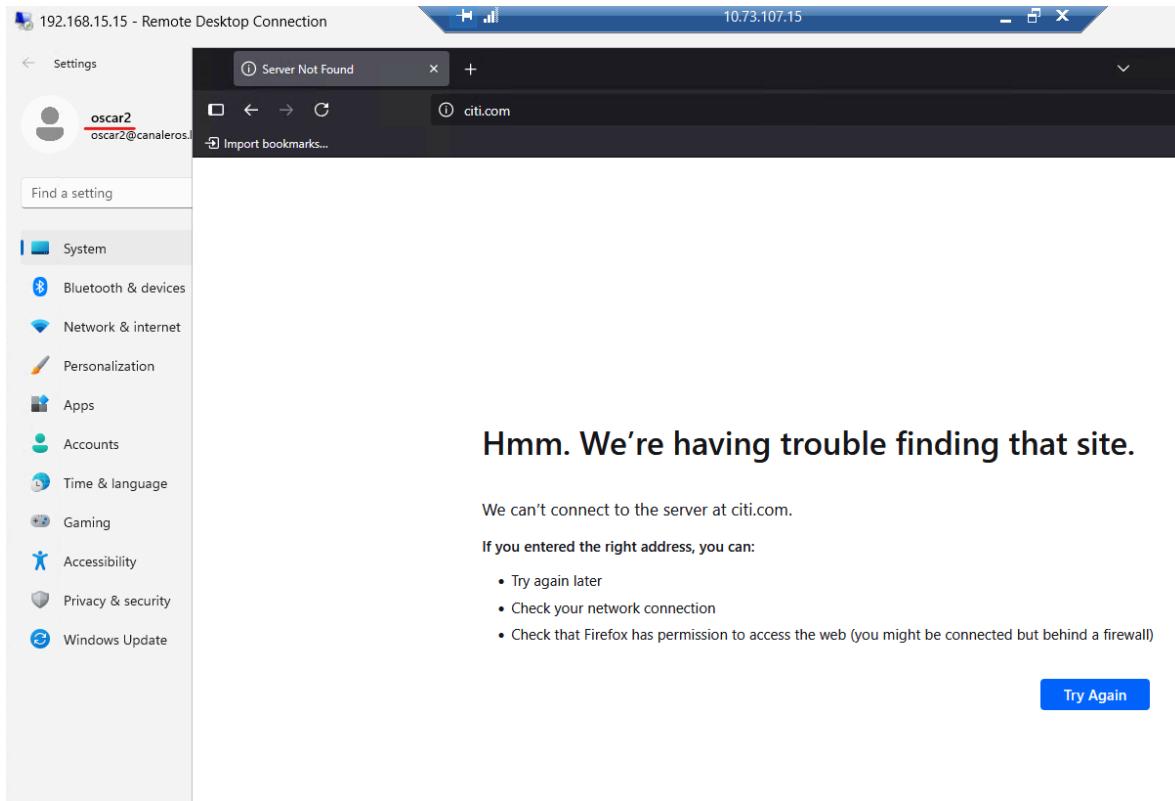
The screenshot shows the SSE Gateway interface in Appliance View. The top navigation bar includes 'Director View', 'Appliance View' (selected), 'Template View', 'Monitor', 'Analytics', 'Configuration', and 'Administration'. The top right shows a user icon and the text 'oscar1'. The main content area shows a summary of 'Total Appliances' (6) and a specific session for 'SaseGW1'. The session details are as follows:

- Inband Management Address: 10.0.0.5
- Out of band Management Address: 10.73.107.7/16
- System Bridge Address: 0A:49:6B:07:01:00

The session table is titled 'Extensive' and includes columns for Application, Source IP, Destination IP, Protocol, Source Port, Destination Port, SDWAN, Natted, Reverse Egress, Nsh Peer Dest, Reverse Packe, NAT Source IP, Reverse Releas, Reverse SDW, Reverse Egress, Nsh Peer Sour, Parent Sessio, External Servi, and Is Child. The table lists several entries, with the last four entries (related to citi\_bank) highlighted with a red box:

| Application           | Source IP     | Destination IP | Protocol | Source Port | Destination Port | SDWAN | Natted       | Reverse Egress | Nsh Peer Dest | Reverse Packe | NAT Source IP | Reverse Releas | Reverse SDW | Reverse Egress | Nsh Peer Sour | Parent Sessio | External Servi | Is Child |
|-----------------------|---------------|----------------|----------|-------------|------------------|-------|--------------|----------------|---------------|---------------|---------------|----------------|-------------|----------------|---------------|---------------|----------------|----------|
| > 10.30.0.5           | 10.30.0.0     | TCP            | 1356     | 1234        | No               | No    | No           | 23397          |               |               |               |                |             | 0              | false         | No            |                |          |
| > 192.168.15.15       | 172.16.100.0  | TCP            | 2002     | 443         | Yes              | No    | Branch-1-VOS | 667            |               |               | 2899235693... | INETINET       | 0           | false          | No            |               |                |          |
| > citi_bank/(prefdef) | 192.168.15.15 | 23.59.206.93   | TCP      | 6024        | 443              | Yes   | Yes          | Branch-1-VOS   | 73            | 10.73.107.12  | 2899235693... | INETINET       | 0           | false          | No            |               |                |          |
| > citi_bank/(prefdef) | 192.168.15.15 | 23.59.206.93   | TCP      | 6012        | 443              | Yes   | Yes          | Branch-1-VOS   | 176           | 10.73.107.12  | 2899235693... | INETINET       | 0           | false          | No            |               |                |          |
| > dns/(prefdef)       | 192.168.15.15 | 172.64.41.4    | TCP      | 6098        | 443              | Yes   | Yes          | Branch-1-VOS   | 80            | 10.73.107.12  | 2899235693... | INETINET       | 0           | false          | No            |               |                |          |

- 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.

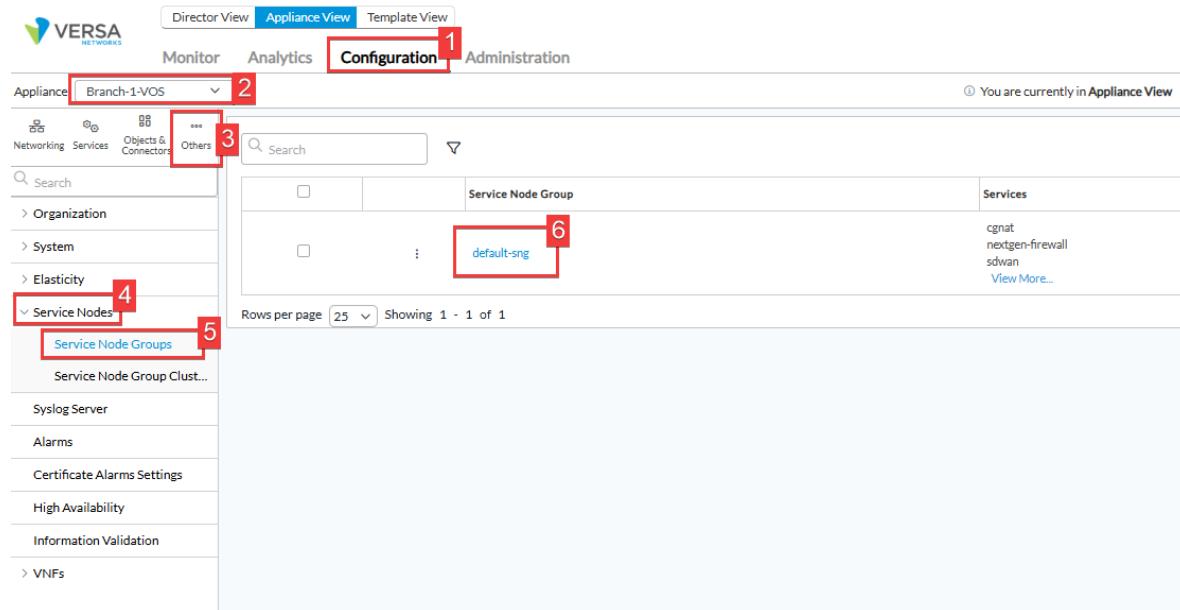
| Application   | Source IP     | Destination IP | Protocol | Source Port | Destination Port | Reverse Egress... | Nsh Peer Dest... | Reverse Packe... | NAT Source IP | Reverse Relea... | Reverse Egres... | Nsh Peer Sour... | Parent Sessio... | External Servi... | Is Child | RX WAN Ckt | Forward FEC ... | Forward St |
|---------------|---------------|----------------|----------|-------------|------------------|-------------------|------------------|------------------|---------------|------------------|------------------|------------------|------------------|-------------------|----------|------------|-----------------|------------|
| dns/(prefdef) | 192.168.15.15 | 104.18.32.137  | TCP      | 7096        | 443              | 0                 | 10.73.107.12     | -                | -             | 0                | 0                | 0                | 0                | 0                 | false    | No         | INET:INET       |            |
| dns/(prefdef) | 192.168.15.15 | 151.101.41.60  | TCP      | 7019        | 443              | 0                 | 10.73.107.12     | -                | -             | 0                | 0                | 0                | 0                | 0                 | false    | No         | INET:INET       |            |

## Configuration Steps: Scenario 2 & 3

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

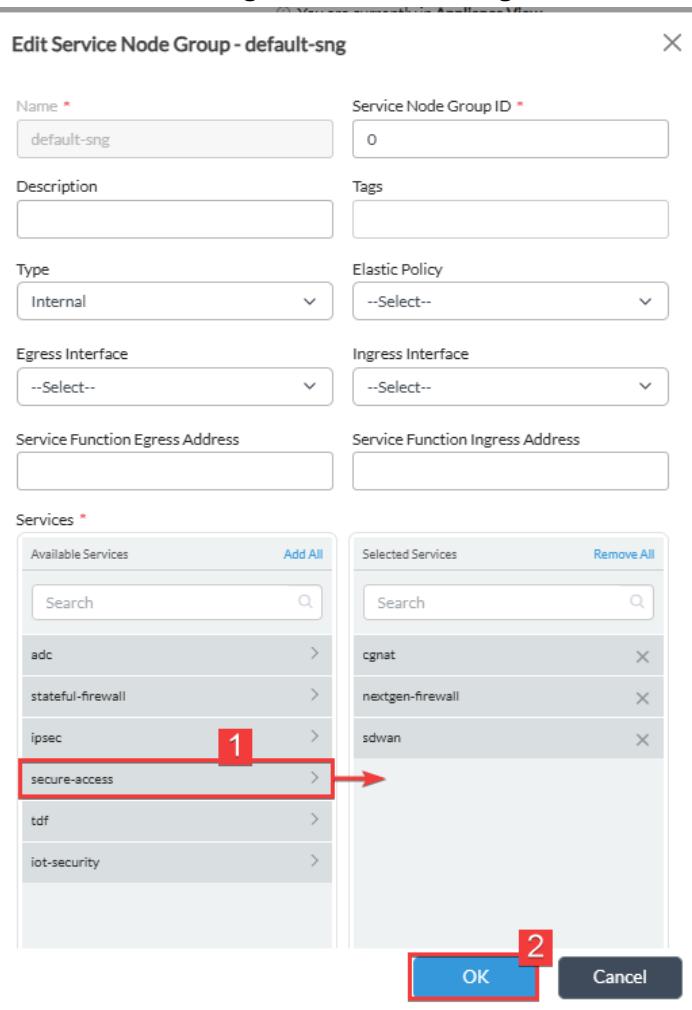
### 1. Edit the default-sng adding the secure-access feature in Director.

- Secure-Access feature needs to be added to the SD-WAN device (if not added before).

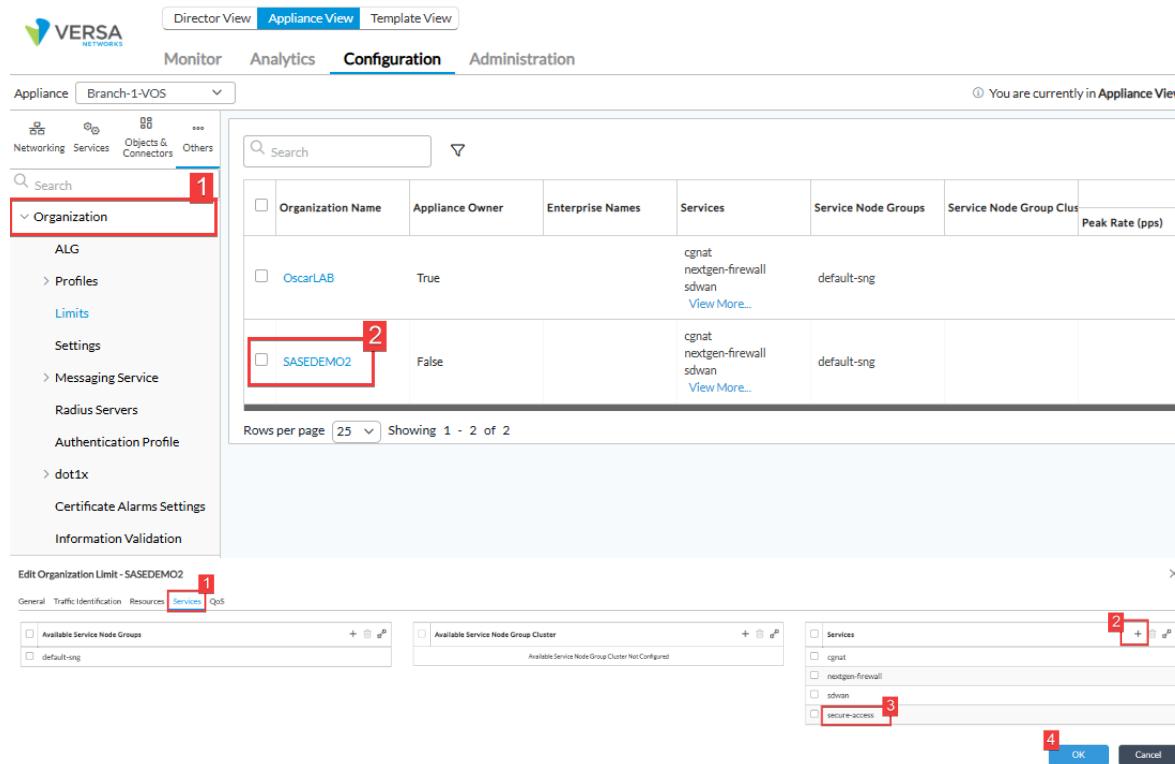


The screenshot shows the VERSA Network Director interface in Appliance View. The top navigation bar includes Director View, Appliance View (selected), and Template View. Below the navigation is a menu bar with Monitor, Analytics, Configuration (selected and highlighted with a red box and a red '1'), and Administration. The main content area shows an Appliance dropdown set to 'Branch-1-VOS' (highlighted with a red box and a red '2'). On the left, a sidebar lists various sections: Networking, Services, Objects & Connectors, and Others (highlighted with a red box and a red '3'). The 'Service Nodes' section is expanded (highlighted with a red box and a red '4'), showing 'Service Node Groups' (highlighted with a red box and a red '5'). The main pane displays a table for 'Service Node Group' with one entry: 'default-sng' (highlighted with a red box and a red '6'). The table has columns for 'Service Node Group' and 'Services', with 'cgnat', 'nextgen-firewall', and 'sdwan' listed under 'Services'. A 'View More...' link is also present. The bottom of the main pane shows 'Rows per page' set to 25 and 'Showing 1 - 1 of 1'.

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



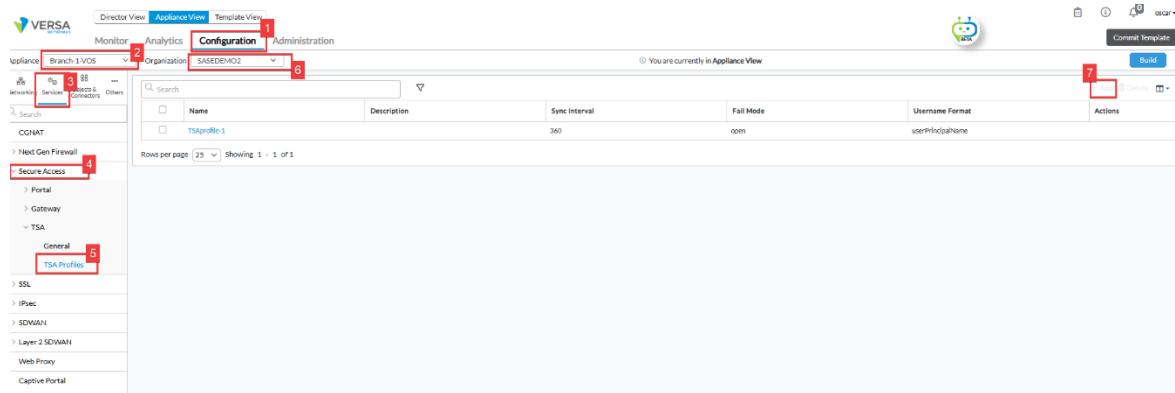
- Also add the feature to the Organization Limits in the Services tab.



The screenshot shows the VERSA Configuration interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Analytics, Configuration (selected), and Administration. A message indicates "You are currently in Appliance View". The left sidebar shows a tree structure with "Organization" selected (marked with a red box 1). The main content area displays a table for "Organization Limits". The table has columns: Organization Name, Appliance Owner, Enterprise Names, Services, Service Node Groups, Service Node Group Clus, and Peak Rate (pps). Two rows are present: "OscarLAB" (Appliance Owner: True) and "SASEDEMO2" (Appliance Owner: False). The "SASEDEMO2" row is highlighted with a red box 2. The "Services" column for "SASEDEMO2" lists "cgnat", "nextgen-firewall", and "sdwan", with a "View More..." link. The "Service Node Groups" column shows "default-sng". The "Edit Organization Limit - SASEDEMO2" dialog is open (marked with a red box 4). It has tabs for General, Traffic Identification, Resources, Services (selected), and QoS. The "Services" list on the right includes checkboxes for "cgnat", "nextgen-firewall", "sdwan", and "secure-access" (marked with a red box 3). The "OK" button is highlighted with a red box 4.

## 2. Configure TSA profile in Director

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



The screenshot shows the VERSA Configuration interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Analytics, Configuration (selected), and Administration. A message indicates "You are currently in Appliance View". The left sidebar shows a tree structure with "Secure Access" selected (marked with a red box 4). Under "Secure Access", "TSA Profiles" is selected (marked with a red box 5). The "Organization" dropdown is set to "SASEDEMO2" (marked with a red box 6). The main content area displays a table for "TSA Profiles". The table has columns: Name, Description, Sync Interval, Fail Mode, Username Format, and Actions. One row is present: "TSAprofile-1". The "Actions" column for "TSAprofile-1" is highlighted with a red box 7.

- Type in the Name (Required).

**Edit TSA Profiles** X

Name \*

Description

Sync Interval(mins)

Fail Mode

Open

Username Format

userPrincipalName

**Port Allocation**

Source Range \*

Reserved Range

Start Size \*

Max Size \*

Fail Mode

Close

OK

Cancel

- **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
    - **userPrincipalName**—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 | $4 \times 5000 = \mathbf{20,000}$ |
| Reserved Port Range  | <b>10000-30000</b>                |
| Fail Mode            | Close (recommended)               |

- Configure the Active Directory authentication for TSA, please refer [Configure-LDAP](#)
- Create an LDAP Profile

The screenshot shows the VERSA NSA Configuration interface. The left sidebar has a tree structure with 'Objects' (3), 'Connectors' (3), and 'Users / Groups' (4) expanded. Under 'Users / Groups', 'Kerberos Profile' and 'LDAP' are listed. The main panel shows the 'Configuration' tab selected. In the center, the 'LDAP Server Profile' sub-tab is active. A table lists an existing LDAP server profile named 'OscarActiveDirectory'. The table has columns for Name, Server Type, Servers, State, Use SSL, Bind DN, Bind Timeout, Base DN, and Search Timeout. A red box highlights the '+ Add' button in the top right corner of the table header.

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

Edit LDAP Server Profile - OscarActiveDirectory

**General** Servers

|   |   |                 |                         |
|---|---|-----------------|-------------------------|
| Name *  | OscarActiveDirectory  |                 |                         |
| Description   | Tags  |                 |                         |
| Server Type *   | Domain Base   | Domain Name *   | Base DN *               |
| Active Directory  |   | canaleros.local | CN=Users,DC=canaleros,I |
| Bind DN *   | Bind Password *   | Bind Timeout *  | Search Timeout *        |
| CN=admin,CN=Users,DC=   | *****   | 30              | 30                      |
| Use SSL   | State   | SSL Mode        | CA Certificate          |
| <input type="radio"/> Enable <input checked="" type="radio"/> Disable | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | LDAPS           | --Select--              |

OK Cancel

- Fill in the information of the Active Directory server.

Edit LDAP Server Profile - OscarActiveDirectory

**General** **Servers**

| <input type="checkbox"/> Name          | IP Address    | Port | Routing Instance     |
|--|---------------|------|----------------------|
| <input type="checkbox"/> 192.168.15.15 | 192.168.20.15 | 389  | SASEDEMO2-Enterprise |

OK Cancel

**Edit Servers**

|               |                      |
|---------------|----------------------|
| Name *        | IP Address           |
| 192.168.15.15 | 192.168.20.15        |
| Port *        | Routing Instance     |
| 389           | SASEDEMO2-Enterprise |
| FQDN          |                      |

OK Cancel

- Create an Authentication Method

Appliance View   Appliance View   Template View

Monitor   Analytics   Configuration **1**   Administration

Appliance   Branch-1-VOS   Objects **2**   Connectors **3**   Others

Organization   SASEDEMO2

You are currently in Appliance View

Search:

| Name      | Description | Method | Profile              | Actions                |
|-----------|-------------|--------|----------------------|------------------------|
| ldap-auth |             | LDAP   | OscarActiveDirectory | <input type="button"/> |

Rows per page: 25 Showing 1 - 1 of 1

Object Types: Networking Services, Objects & Connectors, Others

Search:

Objects:   
 Connectors **3**   
 Reporting   
 SNMP **4**   
 Users / Groups **5**   
 Kerberos Profile   
 Kerberos Keytab   
 LDAP   
 Local Database   
 External Database   
 SAML Profile   
 Certificate Auth Profile **6**   
 Authentication Methods   
 Authentication Profiles   
 Authenticator Profiles   
 Settings   
 Radius Servers   
 Identity Proxy   
 Certificate Manager

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

Edit Authentication Methods

Name **\***  
ldap-auth

Description

Authentication Method

Method: LDAP Profile **7**   LDAP Profile: OscarActiveDirectory **8**

OK   Cancel

- Create an authentication profile.

- Note that the caching mode must be hybrid

**Edit Authentication Profile - ldap-auth**

**General** Rules

|                                 |                         |
|---------------------------------|-------------------------|
| Name *                          | ldap-auth               |
| Description                     | Active                  |
| Cookie Name                     | Cache Expiration (mins) |
| Expiration Mode                 | Default Authenticator   |
| Default Authentication Method * |                         |
| LEF Profile                     |                         |

**Caching Mode** Hybrid

**Cookie Expiration (mins)** 10

**Concurrent Login** 1

**Proactive-Reauth**

**Default Authenticator**  Idp-auth

**LEF Profile**  Default Profile

**OK** **Cancel**

- Set the TSA profile along with the authentication method

VERSA Director View Appliance View Template View

Monitor Analytics Configuration Administration

Appliance Brain VOS Organization SASEDEMO2

Networking Services Objects & Others

Search CGNAT

Next Gen Firewall

Secure Access

Portal

Gateway

2

3

General

URI : TSA

Service Type : TSA

Authentication : ldap-auth

LEF Profile : -

Default LEF Profile : enabled

Device Authentication Profile : -

TSA Profile : TSAprofile-1

You are currently in Appliance View

Commit Template

Build

For edit

Add Services

URI \* tsa

Service Type : TSA

TSA Profile : TSAprofile-1

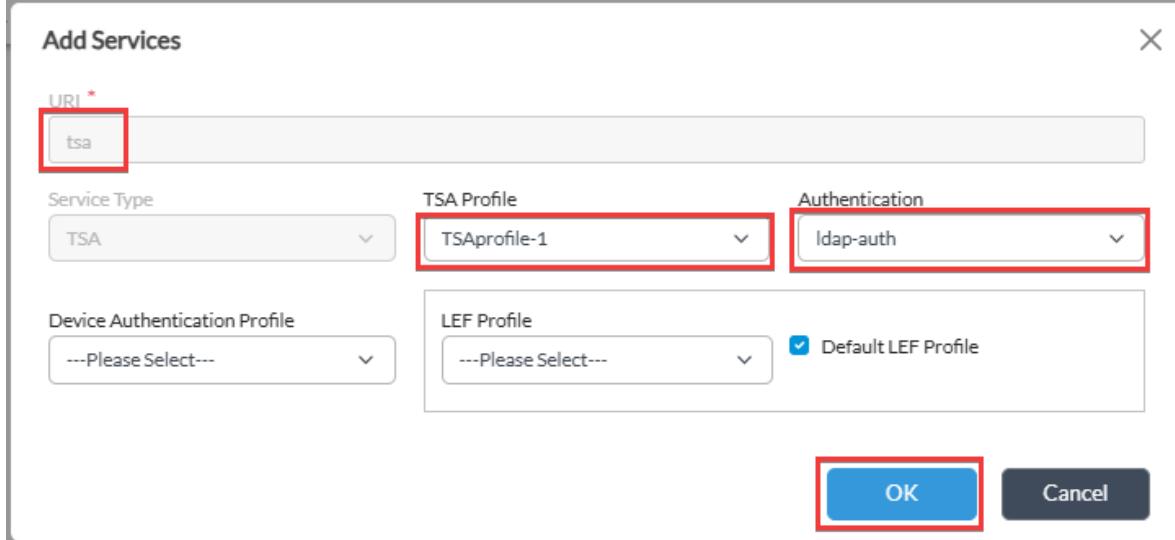
Authentication : ldap-auth

Device Authentication Profile : ---Please Select---

LEF Profile : ---Please Select---

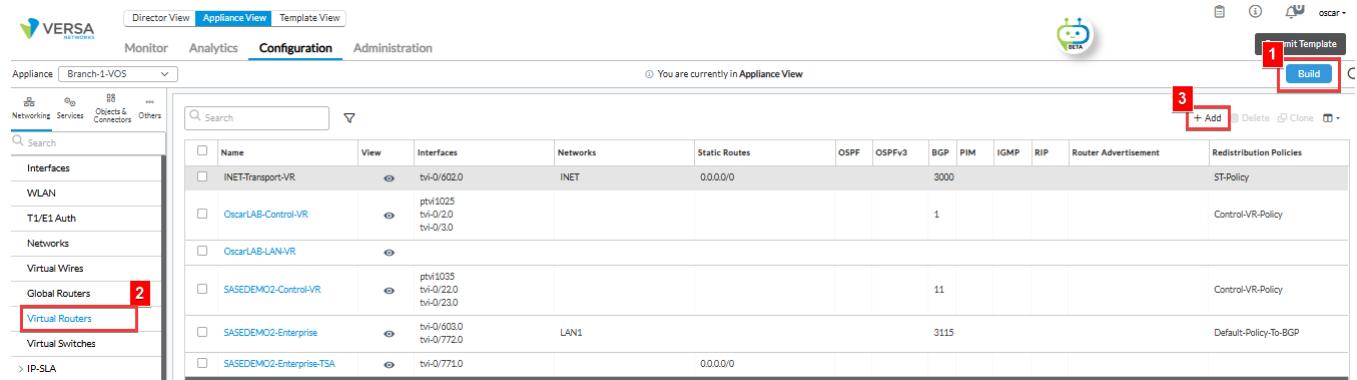
Default LEF Profile

OK Cancel



### 3. Create a new routing instance for TSA registration

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



Appliance Branch-1-VOS

Director View Appliance View Template View

Monitor Analytics Configuration Administration

You are currently in Appliance View

Search

Virtual Routers 2

INET-Transport-VR

OscarLAB-Control-VR

OscarLAB-LAN-VR

SASEDEMO2-Control-VR

SASEDEMO2-Enterprise

SASEDEMO2-Enterprise-TSA

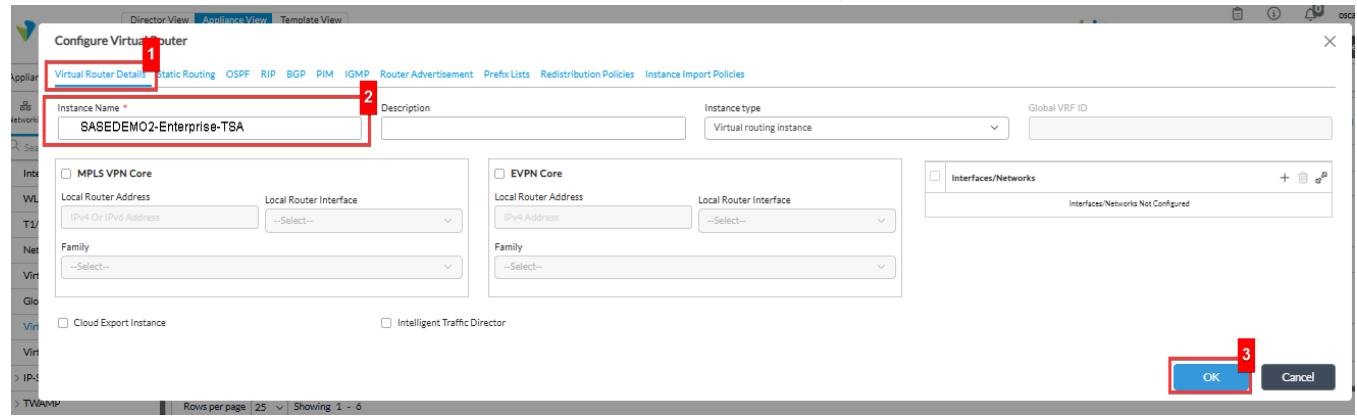
3 3

+ Add Delete Clone

Build 1

Redistribution Policies

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



Configure Virtual Router 1

Virtual Router Details 2 Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

Instance Name 2 Description Instance type Global VRF ID

SASEDEMO2-Enterprise-TSA

Virtual routing instance

MPLS VPN Core

EVPN Core

Interfaces/Networks

Cloud Export Instance Intelligent Traffic Director

OK 3 Cancel

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

VERSAsight Director View Appliance View Template View

Monitor Analytics Configuration Administration

Appliance Branch-1-VOS (South)

You are currently in Appliance View

Commit Template

Networking Services Objects & Connectors Others

Search  ▼

**Interfaces** 2

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

> VRP

Zones

> DNS

LLDP

Zone Protection Profiles

> Class of Service

> DHCP

> PBF

VNI AE ENet IRB T1/E1 **Tunnel** 2 DSL WWAN Wi-Fi uCPE Loopback Fabric Management

+ Add 3 delete edit ...

| <input type="checkbox"/> | Name      | Description                                   | IP Address/Mask | MTU  | Type | Pseudo Tunnel | Pseudo Tunnel Remote Address |
|--------------------------|-----------|---|-----------------|------|------|---------------|------------------------------|
| <input type="checkbox"/> | pvif1025  |   |                 |      |      | tvf-0/3.0     | 10.30.0.0                    |
| <input type="checkbox"/> | pvif1035  |   |                 |      |      | tvf-0/23.0    | 10.30.0.2                    |
| <input type="checkbox"/> | tvf-0/2   | VXLAN Tunnel Interface for OscarLAB Cont...   | 10.30.0.8/32    |      |      | p2mp-vxlan    |                              |
| <input type="checkbox"/> | tvf-0/22  | VXLAN Tunnel Interface for SASEDEMO2 C...     | 10.30.0.8/32    |      |      | p2mp-vxlan    |                              |
| <input type="checkbox"/> | tvf-0/23  | ESP Tunnel Interface for SASEDEMO2 Cont...    | 10.30.0.9/32    |      |      | p2mp-esp      |                              |
| <input type="checkbox"/> | tvf-0/3   | ESP Tunnel Interface for OscarLAB Control...  | 10.30.0.9/32    |      |      | p2mp-esp      |                              |
| <input type="checkbox"/> | tvf-0/602 | WAN side Split Tunnel Interface between IN... | 169.254.0.2/31  |      |      | paired        |                              |
| <input type="checkbox"/> | tvf-0/603 | LAN side Split Tunnel Interface between IN... | 169.254.0.3/31  |      |      | paired        |                              |
| <input type="checkbox"/> | tvf-0/771 |   | 10.10.10.1/30   | 1400 |      | paired        |                              |
| <input type="checkbox"/> | tvf-0/772 |   | 10.10.10.2/30   | 1400 |      | paired        |                              |

Rows per page **25** Showing 1 - 10 of 10

Last Successful Login: Thu, Jul 24, 2025 8:56 PM

- 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 Tunnel Interface - tvi-0/771**

**Tunnel** **1** **2** **3** **4** **5** **6** **Cancel**

**Interface \*** **tvi** **0** **/ 771** **Disable** **Mirror Interface**

**Description**

**MTU** **1400** **Mode** **IPsec**

**Tunnel Type** **Paired** **Paired Interface \*** **tvi** **0** **/ 772**

**Next Routing Instance Nexthop**

**Multihoming**  
**Active Mode** **--Select--** **ESI**

**Subinterfaces**

|                          | <b>Unit</b> | <b>IP Address/Mask</b> | <b>DHCPv6</b> | <b>Interface Mode</b> | <b>ID</b> | <b>VLAN ID List</b> |
|--------------------------|-------------|------------------------|---------------|-----------------------|-----------|---------------------|
| <input type="checkbox"/> | <b>IPv4</b> | <b>IPv6</b>            |               |                       |           |                     |

**OK**

- 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.

Appliance View Configuration

Monitor Analytics Admin

Appliance Branch-1-VOS (South)

Networking Services Objects & Connectors Others

Interfaces WLAN T1/E1 Auth Networks Virtual Wires Global Routers Virtual Routers Virtual Switches IP-SLA TWAMP SaaS App Monitor VRRP

Search

Name

ptvi1025 ptvi1035 tvi-0/2 tvi-0/22 tvi-0/23 tvi-0/3 tvi-0/602 tvi-0/603 tvi-0/771 tvi-0/772

0 / 771

Disable Mirror Interface

Description

MTU 1400 Mode IPsec

Tunnel Type Paired Paired Interface \* tvi 0 / 772

Next Routing Instance Nexthop

Multihoming Active Mode --Select-- ESI

Subinterfaces

| Unit | IP Address/Mask | DHCPv6 | Interface Mode | VLAN ID | VLAN ID List |
|------|-----------------|--------|----------------|---------|--------------|
| IPv4 | IPv6            |        |                |         |              |
|      |                 |        |                |         |              |

+ 1 2

Appliance View Configuration

Monitor Analytics Admin

Appliance Branch-1-VOS (South)

Networking Services Objects & Connectors Others

Interfaces WLAN T1/E1 Auth Networks Virtual Wires Global Routers Virtual Routers Virtual Switches IP-SLA TWAMP SaaS App Monitor VRRP Zones

Search

Name

ptvi1025 ptvi1035 tvi-0/2 tvi-0/22 tvi-0/23 tvi-0/3 tvi-0/602 tvi-0/603 tvi-0/771 tvi-0/772

0 / 771

Disable Mirror Interface

Description

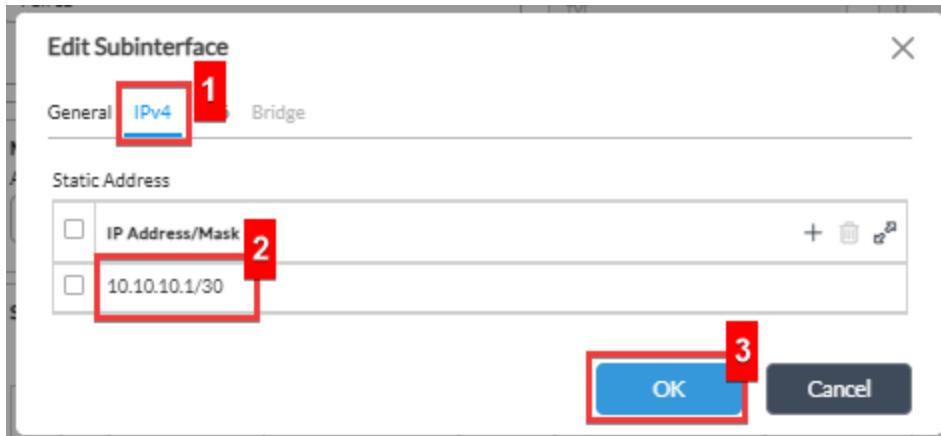
MTU 1400 Mode IPsec

Unit 0

VLAN ID 0

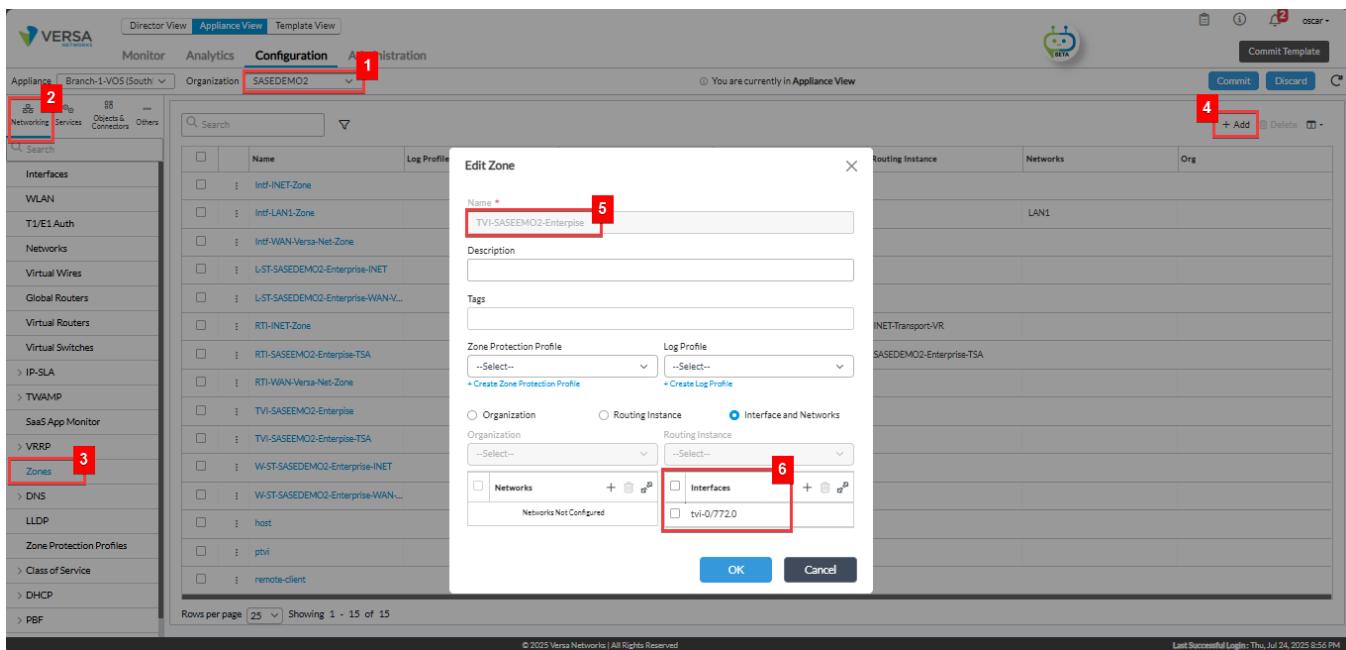
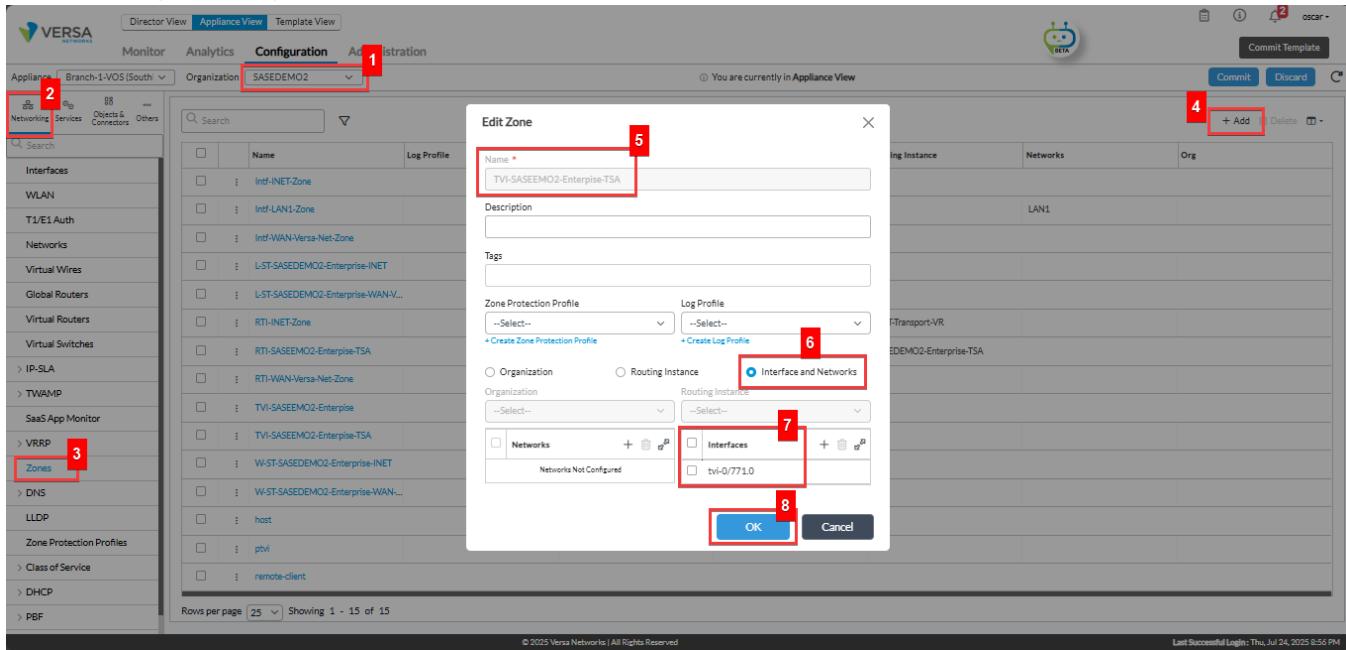
Bandwidth Uplink (Kbps) 1...10000000 Downlink (Kbps) 1...10000000

OK Cancel

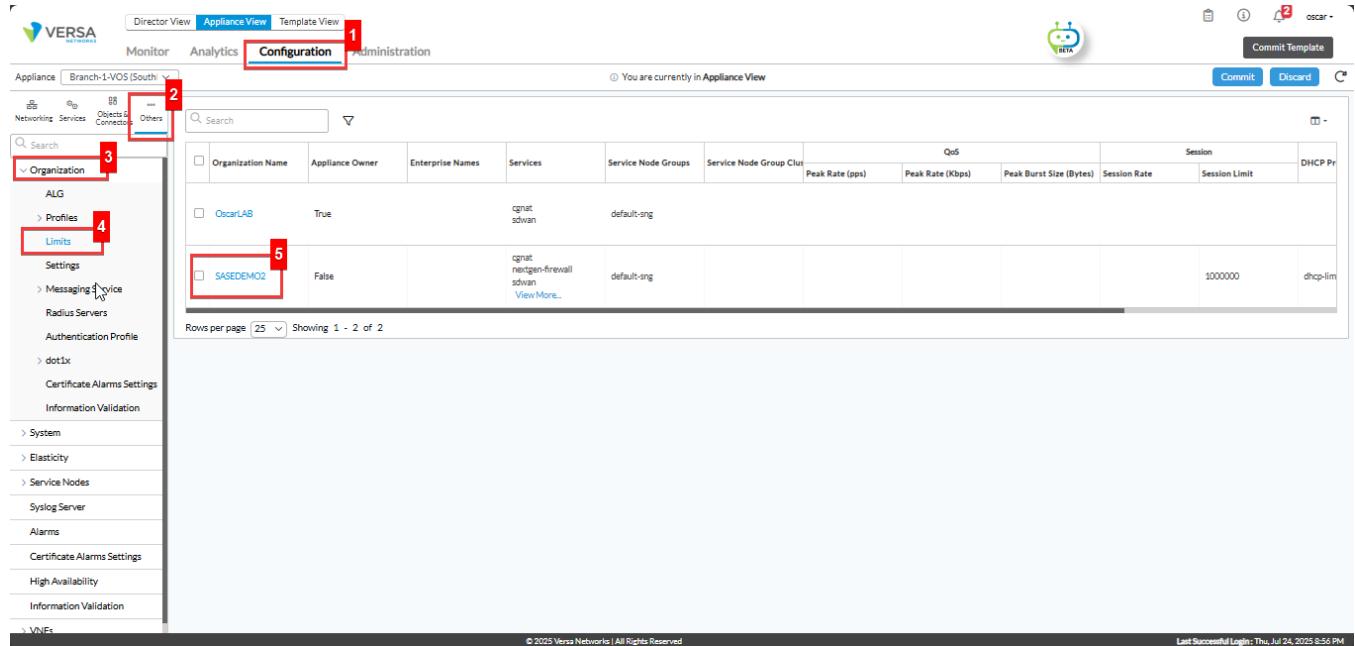


- Edit the interface tvi-0/772 with the same previous steps with the corresponding IP address in the same subnet.

- 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.

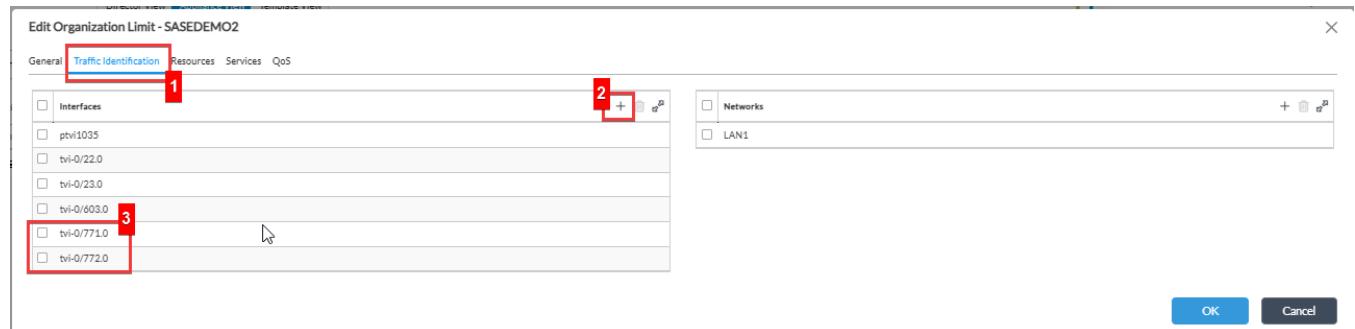


Appliance Branch-1-VOS (South) Configuration

Organization: SASEDEMO2

| Organization Name | Appliance Owner | Enterprise Names                                  | Services    | Service Node Groups | Service Node Group Clus | QoS | Session | DHCP Pr          |
|-------------------|-----------------|---|-------------|---------------------|-------------------------|-----|---------|------------------|
| OscarLAB          | True            | cgnat<br>sdwan                                    | default-sng |                     |                         |     |         |                  |
| SASEDEMO2         | False           | cgnat<br>nextgen-firewall<br>sdwan<br>ViewMore... |             | default-sng         |                         |     |         | 1000000 dhcp-lim |

- Add the TVI interfaces in the Traffic Identification tab.



Edit Organization Limit - SASEDEMO2

General Traffic Identification Resources Services QoS

Interfaces

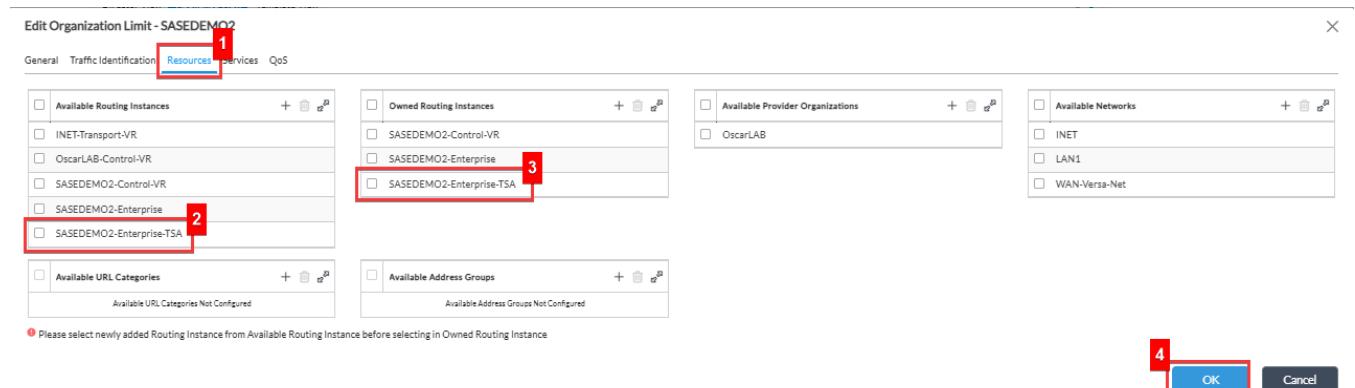
tvI-0/1035  
tvI-0/22.0  
tvI-0/23.0  
tvI-0/603.0  
tvI-0/771.0  
tvI-0/772.0

Networks

LAN1

OK Cancel

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



Edit Organization Limit - SASEDEMO2

General Traffic Identification Resources Services QoS

Available Routing Instances

INET-Transport-VR  
OscarLAB-Control-VR  
SASEDEMO2-Control-VR  
SASEDEMO2-Enterprise  
SASEDEMO2-Enterprise-TSA

Owned Routing Instances

SASEDEMO2-Control-VR  
SASEDEMO2-Enterprise  
SASEDEMO2-Enterprise-TSA

Available Provider Organizations

OscarLAB

Available Networks

INET  
LAN1  
WAN-Versa-Net

Available URL Categories

Available Address Groups

Available URL Categories Not Configured  
Available Address Groups Not Configured

● Please select newly added Routing Instance from Available Routing Instance before selecting in Owned Routing Instance

OK Cancel

- Commit the changes to save the new configurations.

Appliance Branch-1-VOS (South) ▾

Director View Appliance View Template View

Monitor Analytics Configuration Administration

Commit Template

Commit

Discard

Appliance View

Networking Services Objects & Connectors Others

Search

Search

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

Appliance Branch-1-VOS ▾

Director View Appliance View Template View

Monitor Analytics Configuration Administration

Appliance View

Networking Services Objects & Connectors Others

Interfaces

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers 3

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

1

2

3

4

Virtual Router Details Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

1

Instance Name \* SASEDEMO2-Enterprise

Description

Instance type Virtual routing forwarding instance

Global VRF ID 103

Route Distinguisher 103L:103

VRF Import Target

VRF Export Target

VRF Both Target target:103L:103

VRF Core Instance Type MPLS VPN

MPLS transport routing instance \* SASEDEMO2-Control-VR

2

3

4

Interfaces/Networks

tvi-0/603.0

tvi-0/772.0

LAN1

Reverse Traffic Instance

OK Cancel

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

Appliance Branch-1-VOS ▾

Director View Appliance View Template View

Monitor Analytics Configuration Administration

Appliance View

Networking Services Objects & Connectors Others

Interfaces

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers 3

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

1

2

3

4

Virtual Router Details Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

1

Instance Name \* SASEDEMO2-Enterprise-TSA

Description

Instance type Virtual routing forwarding instance

Global VRF ID 103

Route Distinguisher 103L:103

VRF Import Target

VRF Export Target

VRF Both Target target:103L:103

VRF Core Instance Type MPLS VPN

MPLS transport routing instance \* SASEDEMO2-Enterprise

2

3

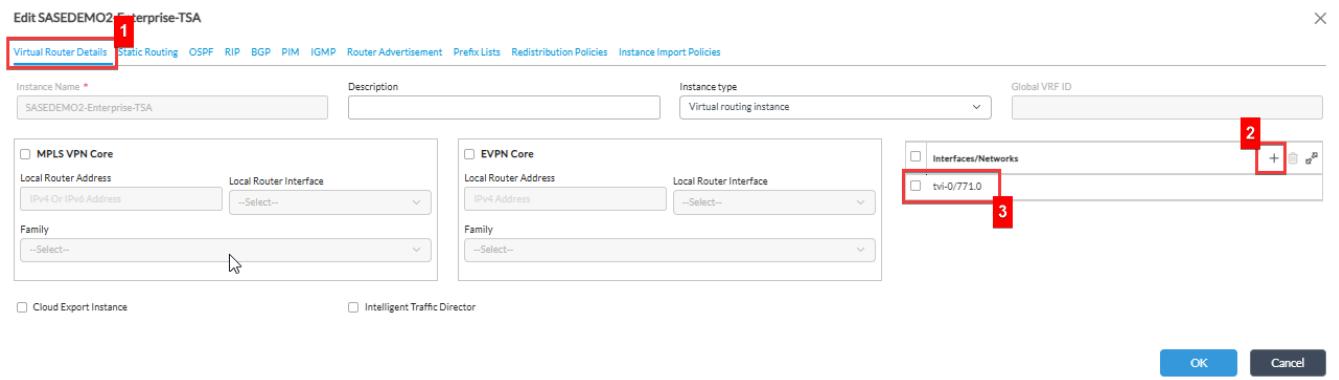
4

Interfaces/Networks

tvi-0/771.0

Reverse Traffic Instance

OK Cancel



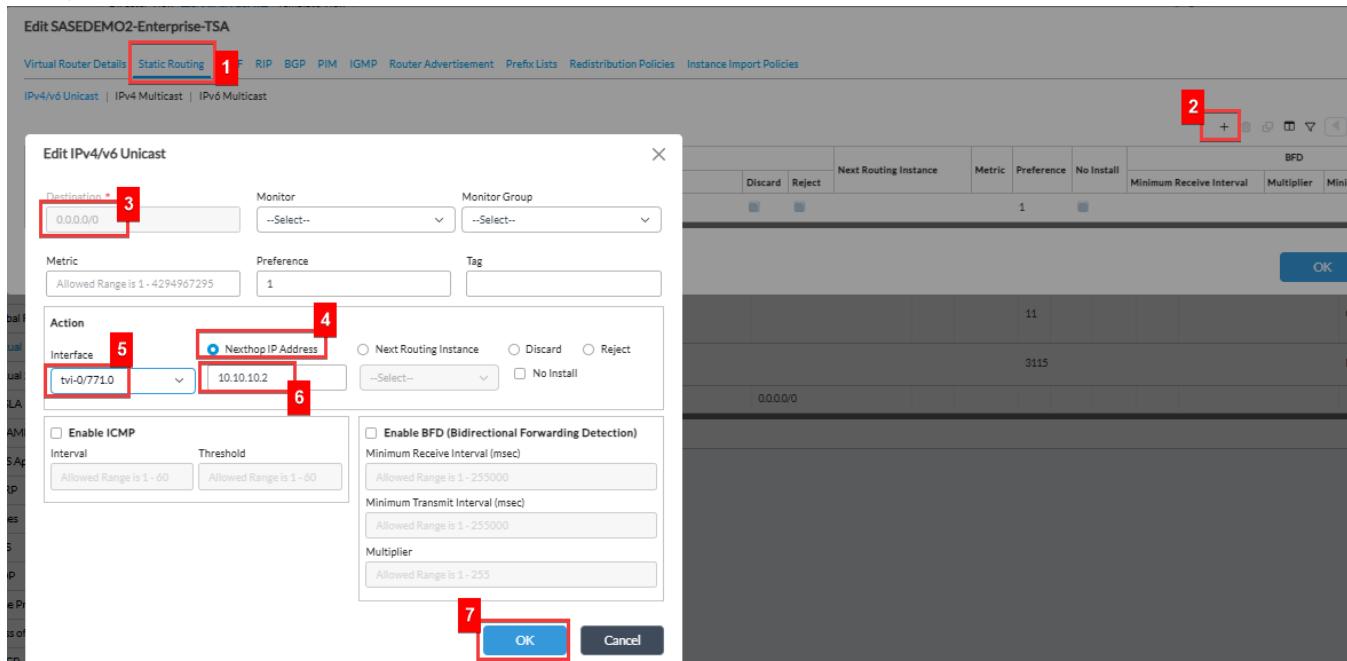
Virtual Router Details **1**

Static Routing **2**

tv1-0/771.0 **3**

OK Cancel

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



Static Routing **1**

OK **2**

0.0.0.0/0 **3**

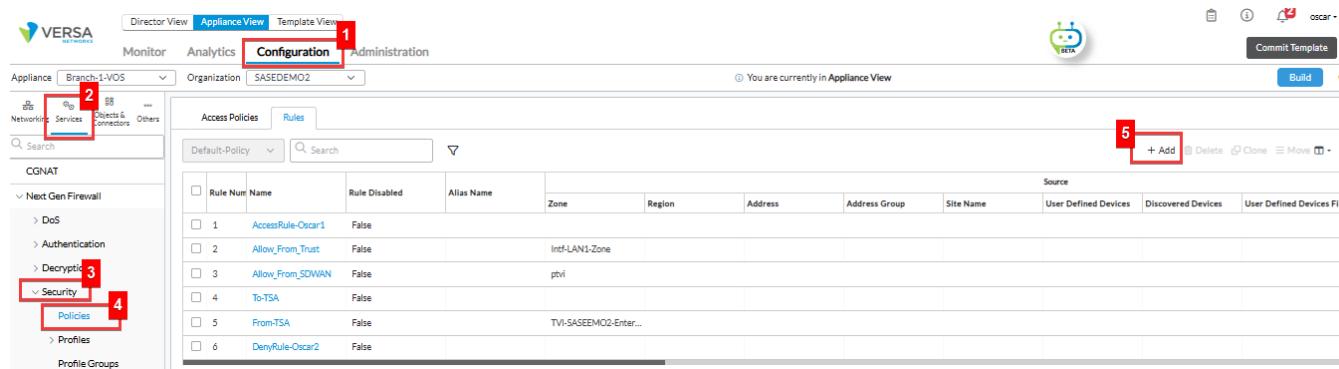
Nexthop IP Address **4**

tv1-0/771.0 **5**

OK **6**

OK **7**

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



Configuration **1**

Access Policies **2**

Policies **3**

+ Add **4**

+ Add **5**

- Name the policy

1

2

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

Name:  2

Description:

Tags:

Alias Name:

Disable Rule

OK Cancel

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

1

2

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

Destination Zone + New Zone

TVI-SASEDEMO2-Enterprise

Destination Address + New Address + New Address Group

Destination Address Anycast

Destination Site Name

Destination Site Name Not Configured

Region +

Region Not Configured

State +

State Not Configured

City +

City Not Configured

Destination Location Negate

Custom Geo Circle +

Custom Geo Circle Not Configured

Scalable Group Tag +

Scalable Group Tag Not Configured

OK Cancel

- Allow the traffic

Edit Rule - To-TSA

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups **Enforce**

**Actions** Log

**Actions**  Allow  Deny  Reject  Apply Security Profile

Synced Flow  Session Timeout (secs)  Send TCP Keep Alive at Session Timeout

Profiles  Profile Groups

IP Filtering  Antivirus  File Filtering  
 Vulnerability  URL Filtering  DNS Filtering  
 Predefined Vulnerability Profile Override  CASB Profile  DLP Profile  
 ATP Profile  RBI Profile

**OK** **Cancel**

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

VERSA Network **Appliance View** **Configuration** Administration

Appliance Branch-1-VOS Organization SASEDEMO2

Network Services Policies & Connectors Others

Search CGNAT

Next Gen Firewall > DoS > Authentication > Decryption > Security > Policies

**1** **2** **3** **4** **5**

Access Policies Rules

Default-Policy  Search

| Rule Num | Name              | Rule Disabled | Alias Name            | Zone | Region | Address | Address Group | Site Name | User Defined Devices | Discovered Devices | User Defined Devices Fil |
|----------|-------------------|---------------|-----------------------|------|--------|---------|---------------|-----------|----------------------|--------------------|--------------------------|
| 1        | AccessRule-Oscar1 | False         |                       |      |        |         |               |           |                      |                    |                          |
| 2        | Allow_From_Trust  | False         | Intf-LAN1-Zone        |      |        |         |               |           |                      |                    |                          |
| 3        | Allow_From_SDWAN  | False         | ptvi                  |      |        |         |               |           |                      |                    |                          |
| 4        | To-TSA            | False         |                       |      |        |         |               |           |                      |                    |                          |
| 5        | From-TSA          | False         | TV-SASEDEMO2-Enter... |      |        |         |               |           |                      |                    |                          |
| 6        | DenyRule-Oscar2   | False         |                       |      |        |         |               |           |                      |                    |                          |

- Name the policy

Edit Rule - From-TSA

**1** **2**

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

Name \* **From-TSA**

Description

Tags

Alias Name

Disable Rule

**OK** **Cancel**

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

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

8010

8011

8012

8013

8014

8015

8016

8017

8018

8019

8020

8021

8022

8023

8024

8025

8026

8027

8028

8029

8030

8031

8032

8033

8034

8035

8036

8037

8038

8039

8040

8041

8042

8043

8044

8045

8046

8047

8048

8049

8050

8051

8052

8053

8054

8055

8056

8057

8058

8059

8060

8061

8062

8063

8064

8065

8066

8067

8068

8069

8070

8071

8072

8073

8074

8075

8076

8077

8078

8079

8080

8081

8082

8083

8084

8085

8086

8087

8088

8089

8090

8091

8092

8093

8094

8095

8096

8097

8098

8099

80100

80101

80102

80103

80104

80105

80106

80107

80108

80109

80110

80111

80112

80113

80114

80115

80116

80117

80118

80119

80120

80121

80122

80123

80124

80125

80126

80127

80128

80129

80130

80131

80132

80133

80134

80135

80136

80137

80138

80139

80140

80141

80142

80143

80144

80145

80146

80147

80148

80149

80150

80151

80152

80153

80154

80155

80156

80157

80158

80159

80160

80161

80162

80163

80164

80165

80166

80167

80168

80169

80170

80171

80172

80173

80174

80175

80176

80177

80178

80179

80180

80181

80182

80183

80184

80185

80186

80187

80188

80189

80190

80191

80192

80193

80194

80195

80196

80197

80198

80199

80200

80201

80202

80203

80204

80205

80206

80207

80208

80209

80210

80211

80212

80213

80214

80215

80216

80217

80218

80219

80220

80221

80222

80223

80224

80225

80226

80227

80228

80229

80230

80231

80232

80233

80234

80235

80236

80237

80238

80239

80240

80241

80242

80243

80244

80245

80246

80247

80248

80249

80250

80251

80252

80253

80254

80255

80256

80257

80258

80259

80260

80261

80262

80263

80264

80265

80266

80267

80268

80269

80270

80271

80272

80273

80274

80275

80276

80277

80278

80279

80280

80281

80282

80283

80284

80285

80286

80287

80288

80289

80290

80291

80292

80293

80294

80295

80296

80297

80298

80299

80300

80301

80302

80303

80304

80305

80306

80307

80308

80309

80310

80311

80312

80313

80314

80315

80316

80317

80318

80319

80320

80321

80322

80323

80324

80325

80326

80327

80328

80329

80330

80331

80332

80333

80334

80335

80336

80337

80338

80339

80340

80341

80342

80343

80344

80345

80346

80347

80348

80349

80350

80351

80352

80353

80354

80355

80356

80357

80358

80359

80360

80361

80362

80363

80364

80365

80366

80367

80368

80369

80370

80371

80372

80373

80374

80375

80376

80377

80378

80379

80380

80381

80382

80383

80384

80385

80386

80387

80388

80389

80390

80391

80392

80393

80394

80395

80396

80397

80398

80399

80400

80401

80402

80403

80404

80405

80406

80407

80408

80409

80410

80411

80412

80413

80414

80415

80416

80417

80418

80419

80420

80421

80422

80423

80424

80425

80426

80427

80428

80429

80430

80431

80432

80433

80434

80435

80436

80437

80438

80439

80440

80441

80442

80443

80444

80445

80446

80447

80448

80449

80450

80451

80452

80453

80454

80455

80456

80457

80458

80459

80460

80461

80462

80463

80464

80465

80466

80467

80468

80469

80470

80471

80472

80473

80474

80475

80476

80477

80478

80479

80480

80481

80482

80483

80484

80485

80486

80487

80488

80489

80490

80491

80492

80493

80494

80495

80496

80497

80498

80499

80500

80501

80502

80503

80504

80505</

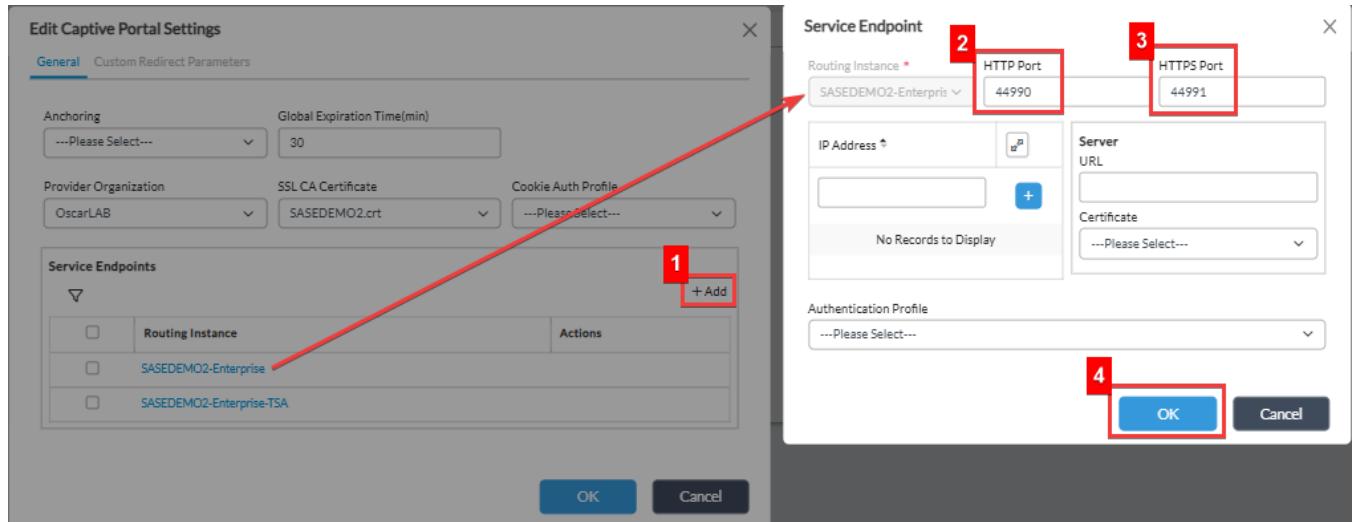
#### 4. Configure captive portal

- 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.

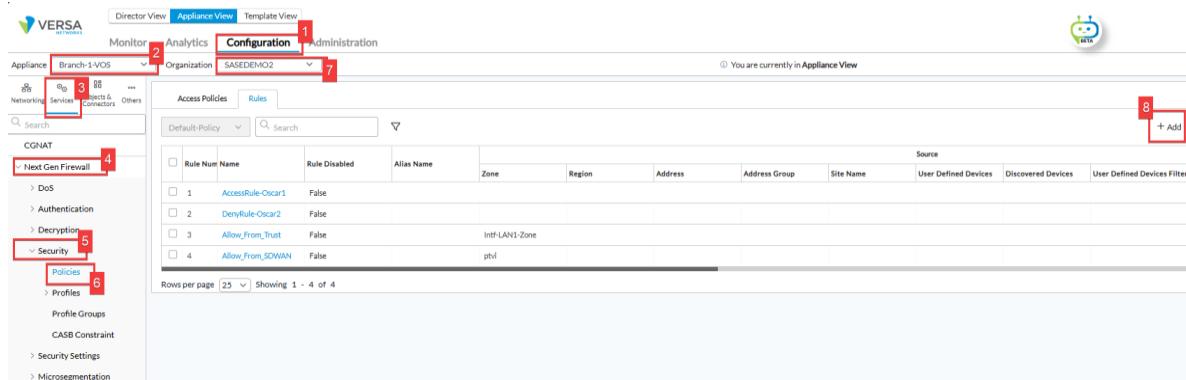
Add the TSA routing instance TVI interface IP, type the captive portal URL and select the endpoint Certificate created for the captive portal URL. Select the Authentication method and click OK. Set 80 for HTTP and 443 for HTTPS.

- 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.

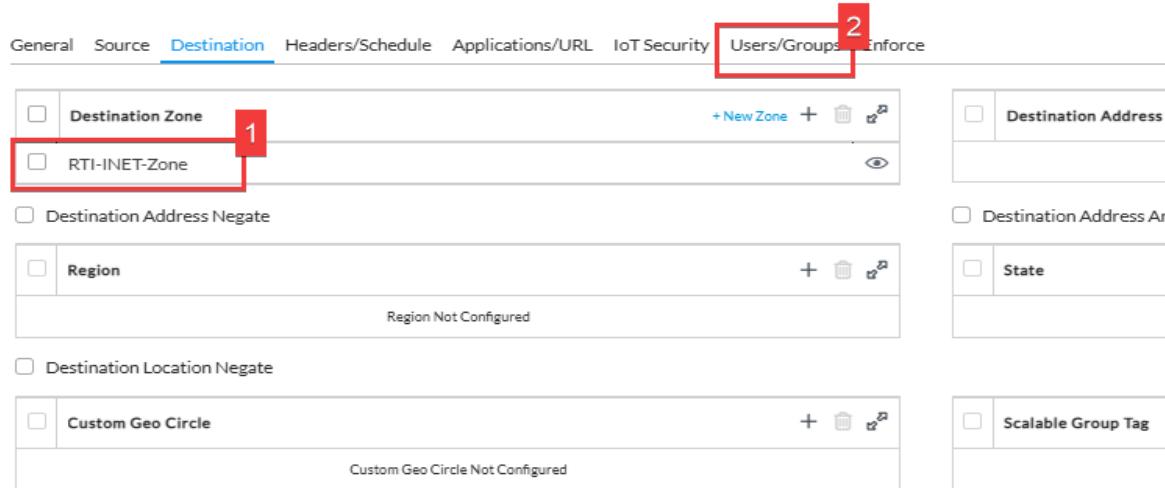


- Name the rule.



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

### Edit Rule - AccessRule-Oscar1



General   Source   **Destination**   Headers/Schedule   Applications/URL   IoT Security   **Users/Groups**   Enforce

Destination Zone **1**

RTI-INET-Zone

Destination Address Negate

Region

Region Not Configured

Destination Location Negate

Custom Geo Circle

Custom Geo Circle Not Configured

Destination Address

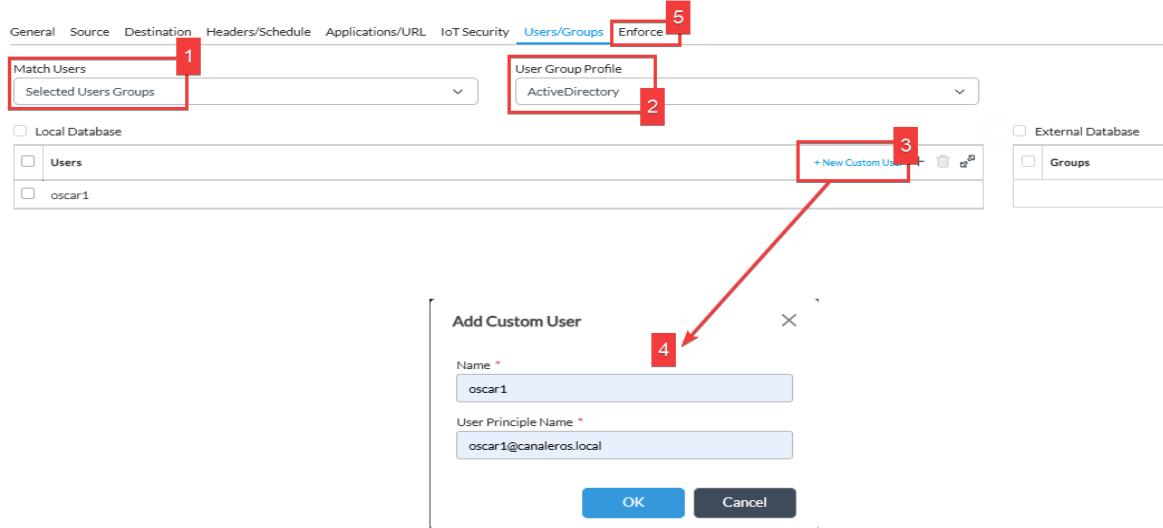
Destination Address Ar

State

Scalable Group Tag

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

### Edit Rule - AccessRule-Oscar1



General   Source   Destination   Headers/Schedule   Applications/URL   IoT Security   **Users/Groups**   **Enforce** **5**

**1** Match Users

**2** User Group Profile

**3** + New Custom User

**4** Add Custom User

Local Database

Users

oscar1

External Database

Groups

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

Edit Rule - AccessRule-Oscar1

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups **Enforce**

**Actions** 1

Allow  Deny  Reject  Apply Security Profile

Syncd Flow  Session Timeout (secs)  Send TCP Keep Alive at Session Timeout

Profiles  Profile Groups

IP Filtering  Antivirus  File Filtering  
 Vulnerability  URL Filtering  DNS Filtering  
 Predefined Vulnerability Profile Override  CASB Profile  DLP Profile  
 ATP Profile  RBI Profile

2 **OK**

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

Edit Rule - DenyRule-Oscar2

General Source Destination Headers/Schedule Applications/URL IoT Security **Users/Groups** Enforce

Match Users  Local Database

Selected Users Groups  ActiveDirectory

Users  oscar2

+ New Custom User

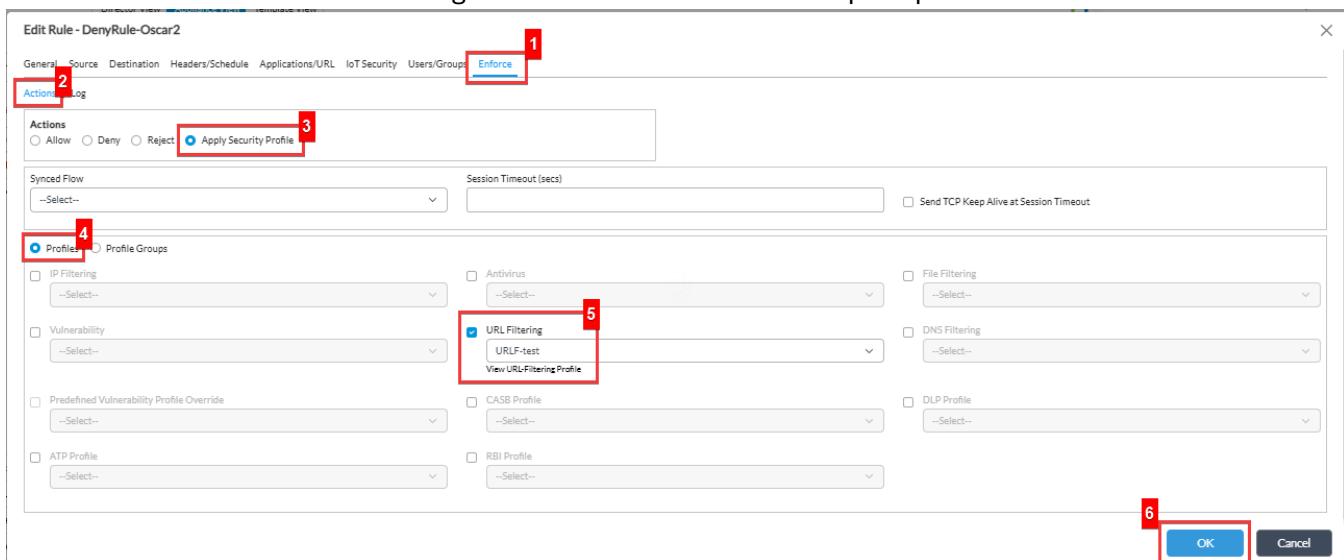
**Add Custom User**

Name \* oscar2

User Principle Name \* oscar2@canaleros.local

OK Cancel

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 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.

hosts - Notepad

```

hosts - Notepad
File Edit Format View Help
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost
172.16.100.0      captiveportal.versanow.net
10.10.10.1      poc.versanow.net

```

Service Endpoint

Routing Instance: SASEDEMO2-Enterprise

HTTP Port: 80

HTTPS Port: 443

IP Address: 10.10.10.1

Server URL: poc.versanow.net

Certificate: Branch-1-VOS.crt

Authentication Profile: IdpAuth

OK Cancel

VERSA

Director View Appliance View Template View

Monitor Analytics Configuration Administration

Organization: SASEDEMO2

Summary Devices Cloud Workload

You are currently in Appliance View

Branch-1-VOS | MA, US

Inband Management Address: 10.30.0.9

Out of band Management Address: 10.73.107.19/16

System Bridge Address: 0A:49:6B:13:01:00

Summary Services Networking System Tools

Interfaces Routes BGP OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP 802.1X RIP Switching LLDP TWAMP

All Interfaces

|   | Interface    | Oper Status | Admin Status | VRF                       | Address       | MAC | Tenant ID | Interface ID |
|---|--------------|-------------|--------------|---------------------------|---------------|-----|-----------|--------------|
| □ | > tvi-0/771  | up          | up           | SASEDEMO2-Enterprise-T... | N/A           | n/a | 3         | -            |
| □ | > tvi-0/7710 | up          | up           | SASEDEMO2-Enterprise-T... | 10.10.10.1/30 | n/a | 3         | -            |

## 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.

Versa Terminal Server Agent

Versa TSA

- Configuration
- Monitor**
- Event Audit Log
- Troubleshoot

VERSA NETWORKS

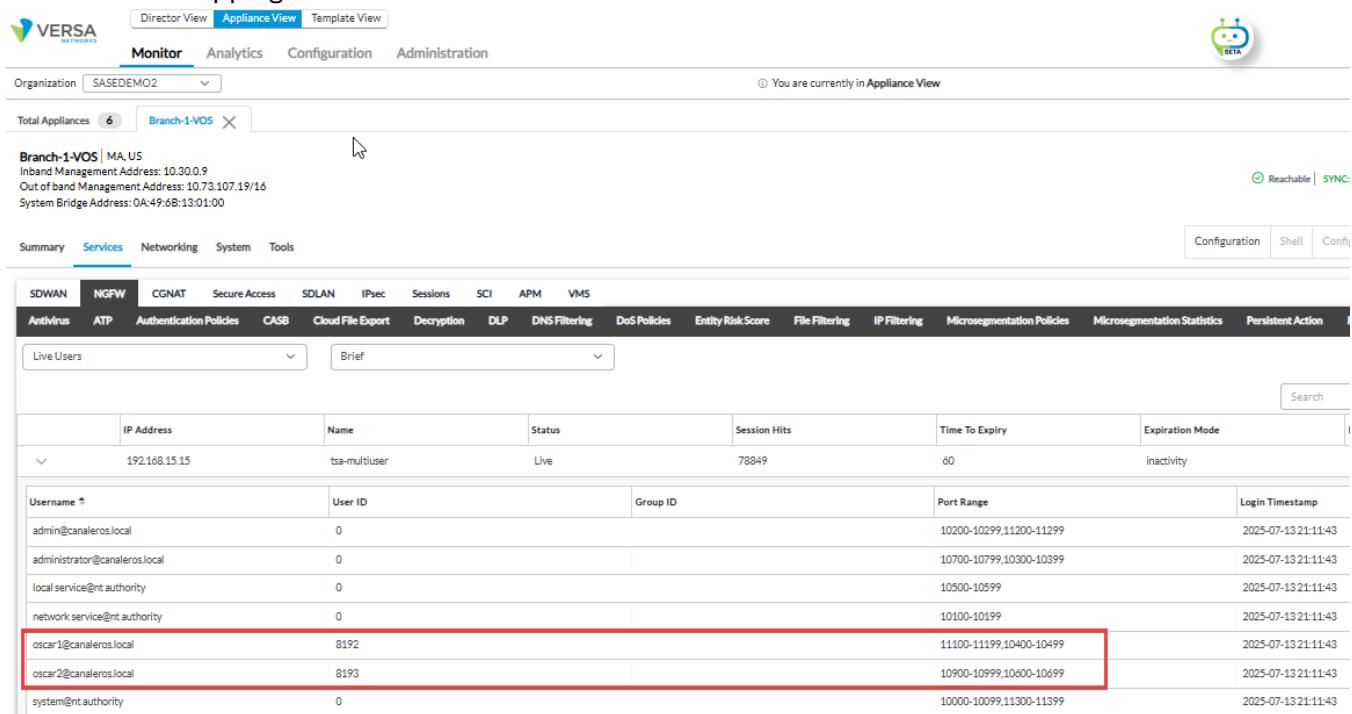
Connected

Refresh

| User Name                           | Port Range              |
|-------------------------------------|-------------------------|
| oscar2@canaleros.local              | 10900-10999,10600-10699 |
| LOCAL SERVICE@NT AUTHORITY\SYSTEM   | 10500-10599             |
| oscar1@canaleros.local              | 11100-11199,10400-10499 |
| Administrator@canaleros.local       | 10700-10799,10300-10399 |
| admin@canaleros.local               | 10200-10299             |
| NETWORK SERVICE@NT AUTHORITY\SYSTEM | 10100-10199             |
| SYSTEM@NT AUTHORITY\SYSTEM          | 10000-10099             |

Version: 7.1.1  
© 2023 Versa Networks | All rights reserved

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



Organization: SASEDEMO2

Branch-1-VOS | MA, US

Inband Management Address: 10.30.0.9  
Out of band Management Address: 10.73.107.19/16  
System Bridge Address: 0A:49:6B:13:01:00

reachable | SYNC

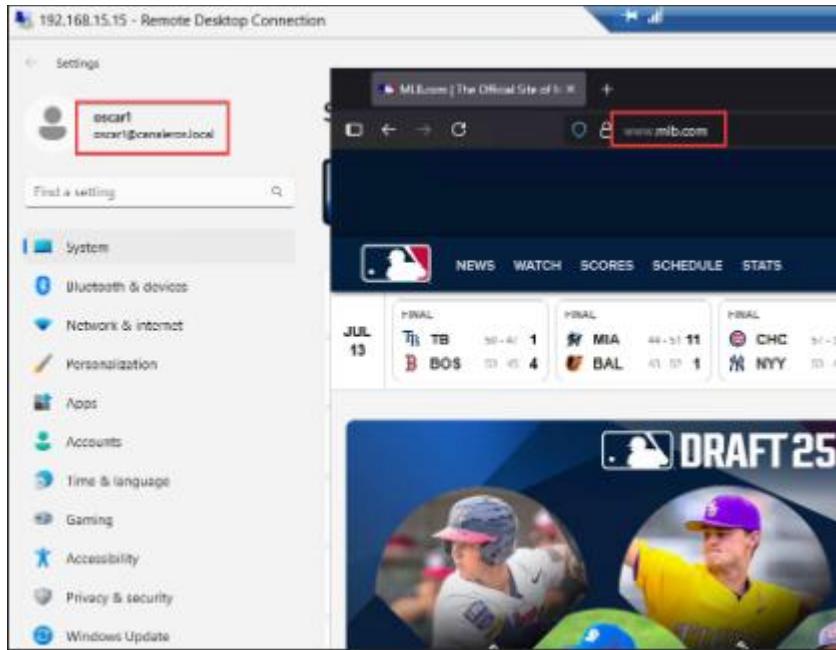
Summary Services Networking System Tools

Configuration Shell Config

| IP Address             | Name          | Status | Session Hits | Time To Expiry          | Expiration Mode     |
|------------------------|---------------|--------|--------------|-------------------------|---------------------|
| 192.168.15.15          | tsa-multouser | Live   | 78849        | 60                      | inactivity          |
| oscar1@canaleros.local | 8192          |        |              | 11100-11199,10400-10499 | 2025-07-13 21:11:43 |
| oscar2@canaleros.local | 8193          |        |              | 10900-10999,10600-10699 | 2025-07-13 21:11:43 |
| system@nt authority    | 0             |        |              | 10000-10099,11300-11399 | 2025-07-13 21:11:43 |

## 8. Tests Results

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

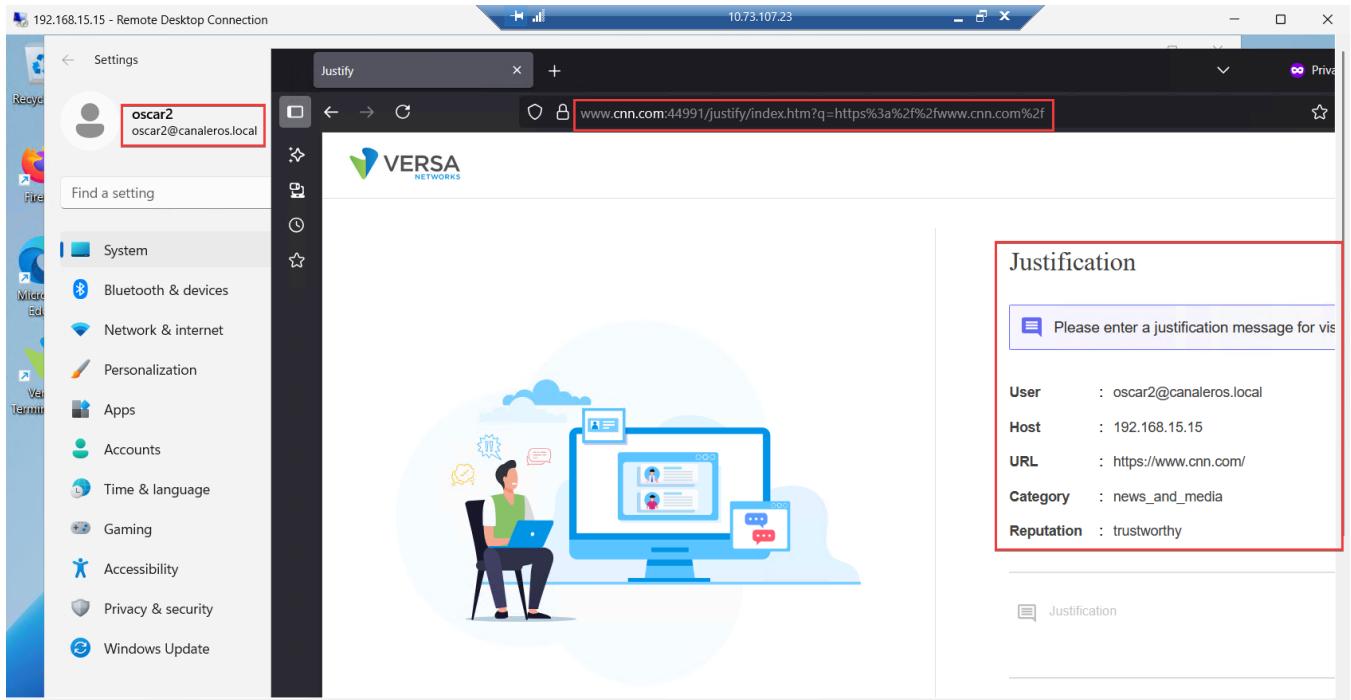


- In this output from the SD-WAN branch device, we can see the session of the internet webpage tested and the traffic being allowed by the policy created for user "oscar1"

| Session Count | Session Created | Session Closed | NAT Session Count |
|---------------|-----------------|----------------|-------------------|
| 58            | 176563          | 176505         | 56                |

| Application         | Rule              | Source IP     | Destination IP | Protocol | Source Port | Destination Port | Forward Byte Count | Reverse Byte Count |
|---------------------|-------------------|---------------|----------------|----------|-------------|------------------|--------------------|--------------------|
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 151.101.41.91  | TCP      | 10492       | 443              | 3.968              | 4.128              |
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 151.101.41.91  | TCP      | 10408       | 443              | 4.933              | 3.784              |
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 151.101.41.91  | TCP      | 10427       | 443              | 4.943              | 3.792              |
| > adobe/(prefdef)   | AccessRule-Oscar1 | 192.168.15.15 | 23.44.73.62    | TCP      | 10420       | 443              | 3.518              | 6.111              |
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 151.101.41.60  | TCP      | 10476       | 443              | 5.451              | 16.788             |
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 151.101.41.91  | TCP      | 11140       | 443              | 25.125             | 2651.826           |
| > mlb.com/(prefdef) | AccessRule-Oscar1 | 192.168.15.15 | 104.18.33.10   | TCP      | 10482       | 443              | 3.184              | 10.031             |

- 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.

The screenshot shows the VERSA Networks SD-WAN interface. The 'Monitor' tab is selected. A 'Session Filter' dialog is open, showing session search criteria. The main area displays a table of session details, with two rows highlighted with a red box:

| Extensive                           | Application            | Rule             | Source IP     | Destination IP  | Protocol | Source Port | Destination Port | Forward Byte Count | Reverse Byte Count |
|-------------------------------------|------------------------|------------------|---------------|-----------------|----------|-------------|------------------|--------------------|--------------------|
| <input type="checkbox"/>            | > Unknown              |                  | 10.30.0.9     | 10.30.0.0       | TCP      | 1226        | 1234             | 0                  | 9630.18            |
| <input checked="" type="checkbox"/> | > msnp/(predef)        | Allow_From_Trust | 192.168.15.10 | 20.59.87.226    | TCP      | 65304       | 443              | 10.775             | 13.892             |
| <input checked="" type="checkbox"/> | > unknown_tcp/(predef) |                  | 192.168.15.15 | 192.168.20.10   | TCP      | 3389        | 53518            | 349.781            | 53.211             |
| <input checked="" type="checkbox"/> | > msnp/(predef)        | Allow_From_Trust | 192.168.15.15 | 20.59.87.225    | TCP      | 10126       | 443              | 10.817             | 13.894             |
| <input checked="" type="checkbox"/> | > websocket/(predef)   | Allow_From_Trust | 192.168.15.15 | 10.10.10.1      | TCP      | 10124       | 443              | 4.346              | 6.502              |
| <input checked="" type="checkbox"/> | > Unknown              | From-TSA         | 192.168.15.15 | 10.10.10.1      | TCP      | 10124       | 443              | 0.55               | 1.666              |
| <input checked="" type="checkbox"/> | > mozilla/(predef)     | DenyRule-Oscar2  | 192.168.15.15 | 34.107.243.93   | TCP      | 10028       | 443              | 7.924              | 2.542              |
| <input checked="" type="checkbox"/> | > mozilla/(predef)     | DenyRule-Oscar2  | 192.168.15.15 | 34.149.100.2... | TCP      | 10076       | 443              | 5.207              | 8.806              |

## 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](#).