

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	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.

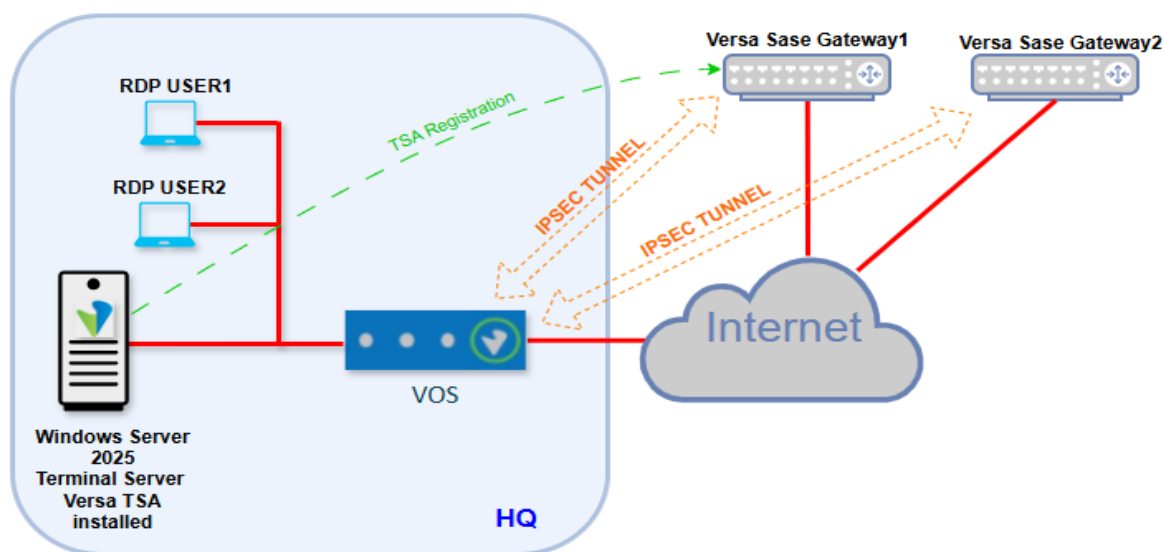
Private Application Access: When multiple users access private applications through a shared environment such as a terminal server, enforcing Zero Trust Network Access (ZTNA) requires identifying users individually, rather than relying on shared attributes like IP addresses. Terminal Server Access (TSA)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

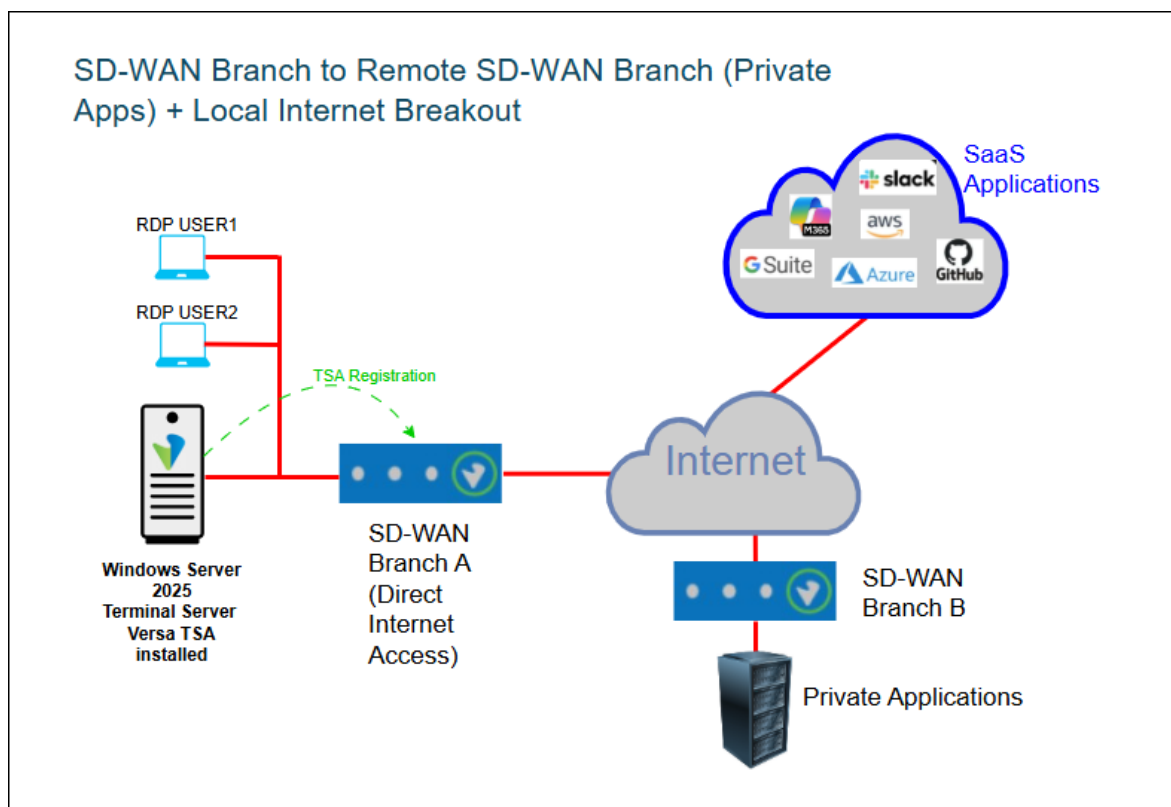
- **Pre-configured SSE Portal URL:** The SSE Gateway is pre-configured with a Portal URL/Captive Portal URL. The TSA agent uses this URL during the registration process.
- **TSA Agent Configuration:** The Versa TSA Agent, installed on the Terminal Server, is configured to communicate with the SSE Gateway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

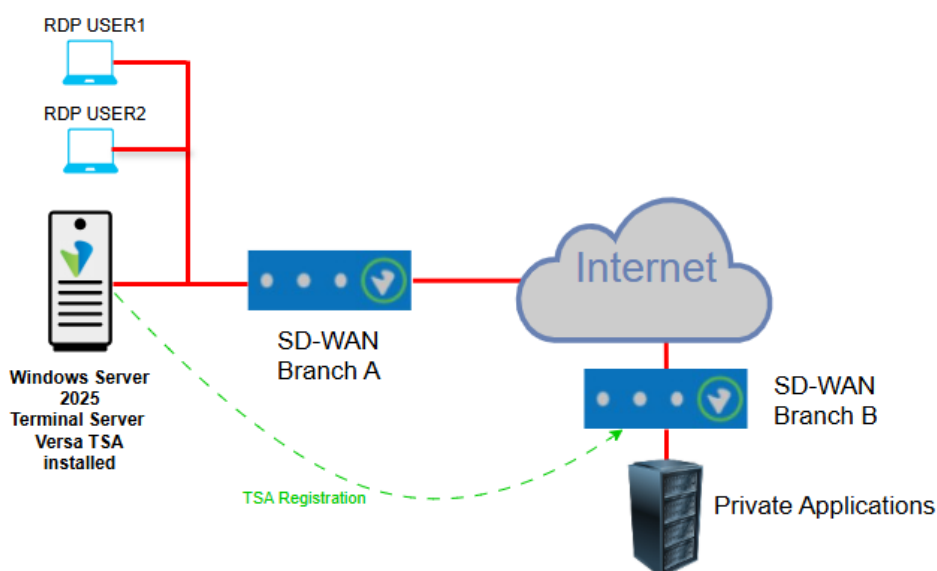
- **Routing-Instance for Captive Portal:** To ensure TSA registration on the captive portal does not break the URLF captive portal action, we will create a separate TSA routing instance, which will be used for registration of TSA agents in Branch A. A paired TVI will be configured between the TSA routing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

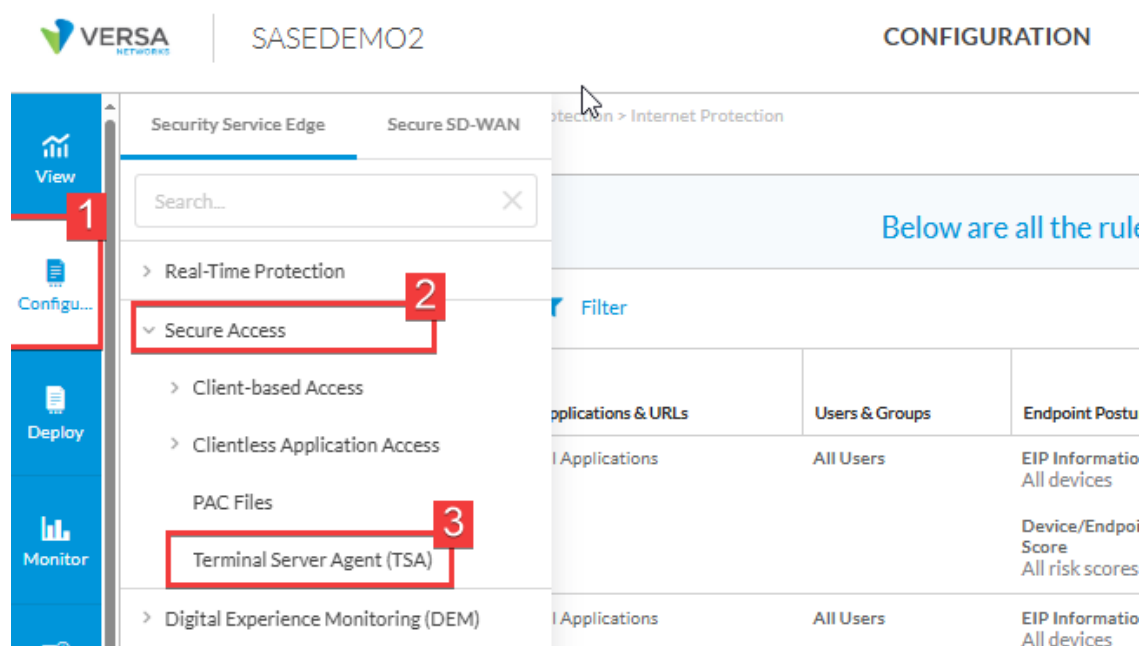
and Enterprise/LAN-VR. A default route will be added in the TSA routing instance pointing to the Enterprise/LAN-VR TVI IP. The TVI IP will be redistributed in SDWAN BGP as all Direct routes are default redistributed.

- **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

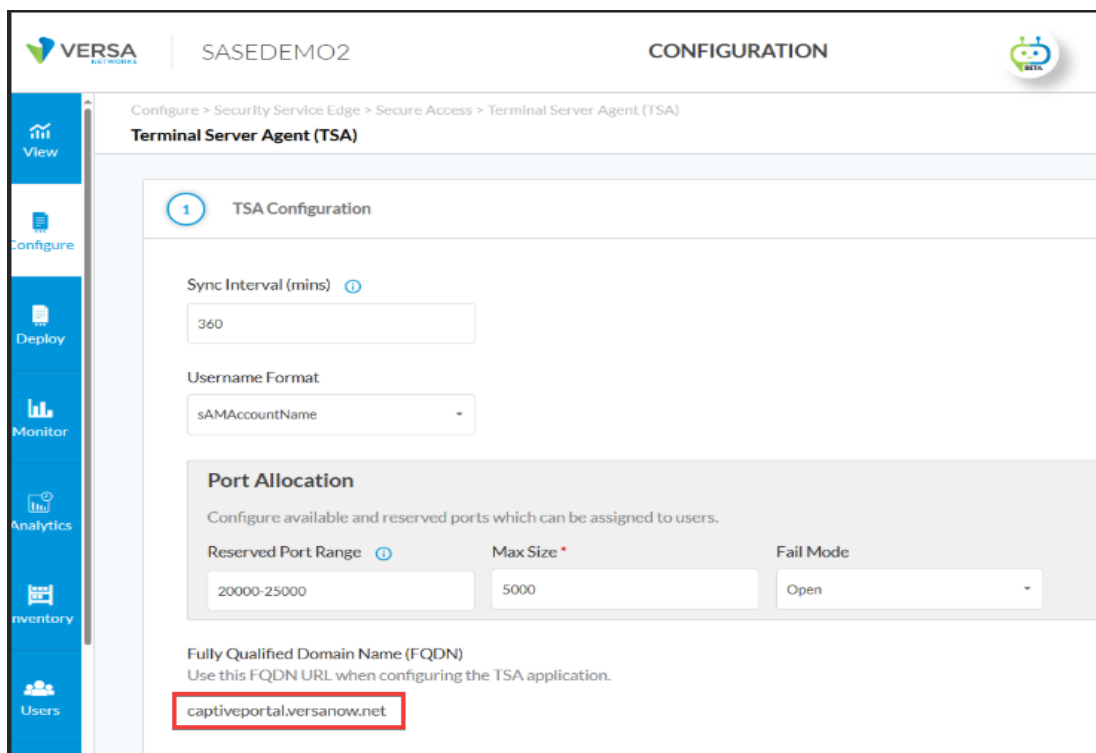
- The first step is to configure the Terminal Server Agent (TSA) in Concerto under the specific tenant (in this case, SASDEMO2).



Below are all the rules

Applications & URLs	Users & Groups	Endpoint Posture
Applications	All Users	EIP Information All devices
Applications	All Users	Device/Endpoint Score All risk scores
Applications	All Users	EIP Information All devices

- 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.



VERSA | SASEDEMO2 | CONFIGURATION

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

Terminal Server Agent (TSA)

1 TSA Configuration

Sync Interval (mins) ⓘ
360

Username Format
sAMAccountName

Port Allocation
Configure available and reserved ports which can be assigned to users.

Reserved Port Range ⓘ Max Size* Fail Mode
20000-25000 5000 Open

Fully Qualified Domain Name (FQDN)
Use this FQDN URL when configuring the TSA application.
captiveportal.versanow.net

- **Port Allocation (Group of Fields)**

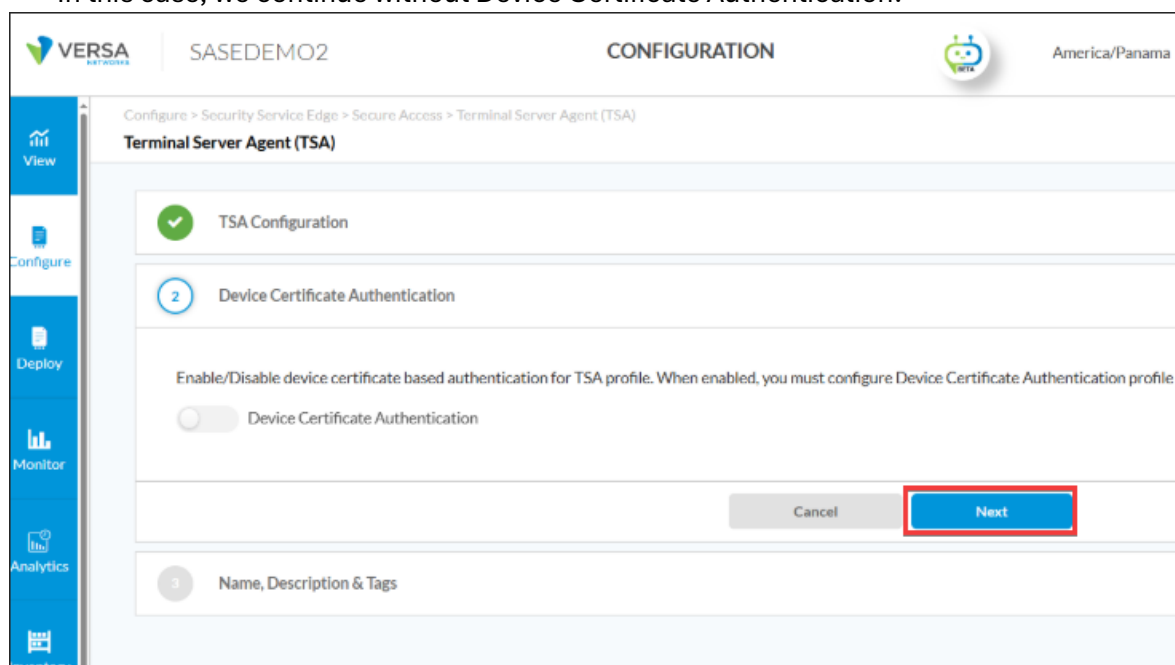
- **Sync Interval:** Enter how often, in minutes, to synchronise the configuration with the TSA.
- **Username Format:** Select the username format to have the TSA recognise
 - **userPrincipalName**—User principal name. A user principal name consists of a prefix (user account name), followed by the @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

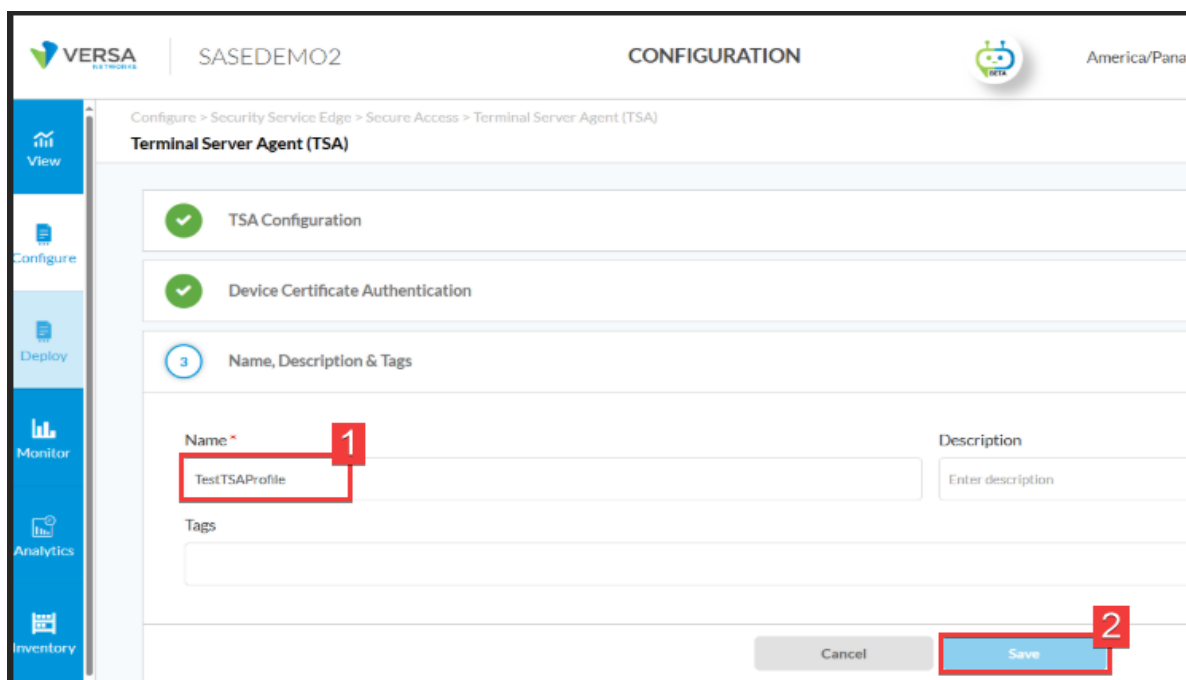
Item	Value
Total Ports Required	4 × 5000 = 20,000
Reserved Port Range	10000-30000
Fail Mode	Close (recommended)

- 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.



The screenshot shows the Versa Configuration interface for the 'Terminal Server Agent (TSA)' configuration. The breadcrumb trail is 'Configure > Security Service Edge > Secure Access > Terminal Server Agent (TSA)'. The main section is titled 'Terminal Server Agent (TSA)'. It contains a progress bar with three steps: 1. TSA Configuration (completed, marked with a green check), 2. Device Certificate Authentication (current step, marked with a blue circle), and 3. Name, Description & Tags (future step, marked with a grey circle). In the 'Device Certificate Authentication' section, there is a text prompt: 'Enable/Disable device certificate based authentication for TSA profile. When enabled, you must configure Device Certificate Authentication profile'. Below this is a toggle switch labeled 'Device Certificate Authentication', which is currently turned off. At the bottom right of the configuration area, there are two buttons: 'Cancel' and 'Next'. The 'Next' button is highlighted with a red rectangle, indicating the next step in the process.

- 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.



VERSA NETWORKS | SASDEMO2 | CONFIGURATION | America/Pana

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

Terminal Server Agent (TSA)

- ✓ TSA Configuration
- ✓ Device Certificate Authentication
- 3 Name, Description & Tags

Name * TestTSAProfile 1


Description: Enter description

Tags

Cancel Save 2

2. Configure the user's authentication profile.

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


SASEDEMO02
CONFIGURATION

View

1
Configure

Deploy

Monitor

Analytics

Inventory

Users

Security Service Edge

Secure SD-WAN

Terminal Server Agent (TSA)

Search...

> Real-Time Protection

> Secure Access

> Digital Experience Monitoring (DEM)

> TLS Decryption

> Profiles and Connectors

> Partner Integration

2
✓ User and Device Authentication

Rules

3
Profiles

SCIM Integration

> User-Defined Objects

> Settings

Sync Interval (Mins)

Username Format

360

sAMAccountName

- Fill in the information of the Active Directory Server

Edit LDAP Authentication Profile: OscarActiveDirectory

1 Settings
 2 User And Group Profile
 3 Review & Submit

Server Type 1

Active Directory

Select either FQDN or IP Address *

☐ FQDN

☒ IP Address 2

10.73.107.18

+ Add Secondary Server

VPN Name * 3

SASEDEMO2-Enterprise

Port * 4

389

Cancel Skip to Review Next

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

Edit LDAP Authentication Profile: OscarActiveDirectory

1 Settings
 2 User And Group Profile
 3 Review & Submit

☐ Enable SSL

SSL Mode

--Select--

CA Certificate

--Select--

+ Add New

Bind DN * 1

CN=admin,CN=Users,DC=canaleros,DC=local

Bind Password * 2

Bind Timeout (sec)

30

Base DN * 3

CN=Users,DC=canaleros,DC=local

Domain Name * 4

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

Settings **2** Review & Submit

Group Object Class * Group Name * Group Member *

User Object Class * User Name *

Refresh Interval (seconds) Password Last Set Password Max Age

- Fill in a name for the authentication profile.

Edit LDAP Authentication Profile: OscarActiveDirectory

Settings **3** Review & Submit

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

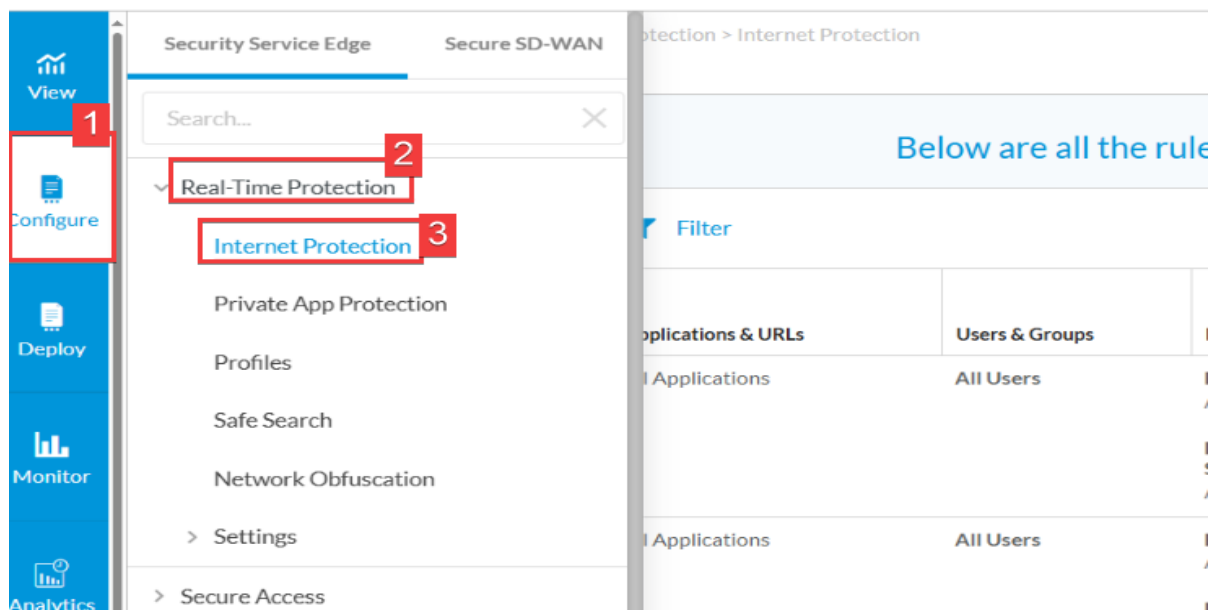
General

Name Description

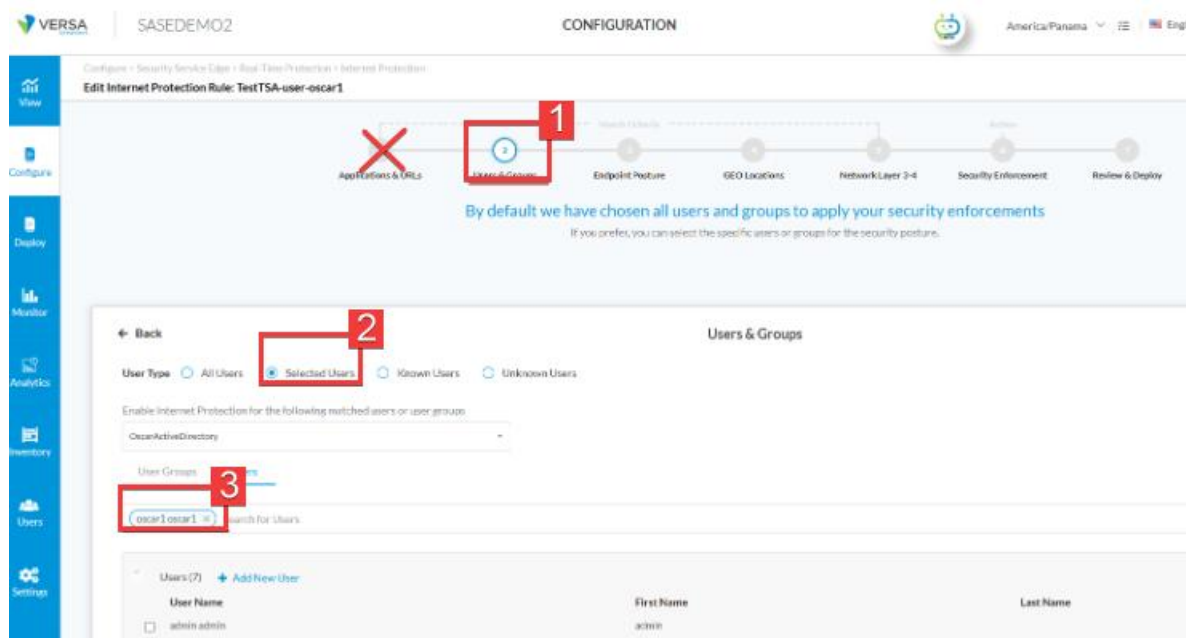
Tags

3. Create Security Policies

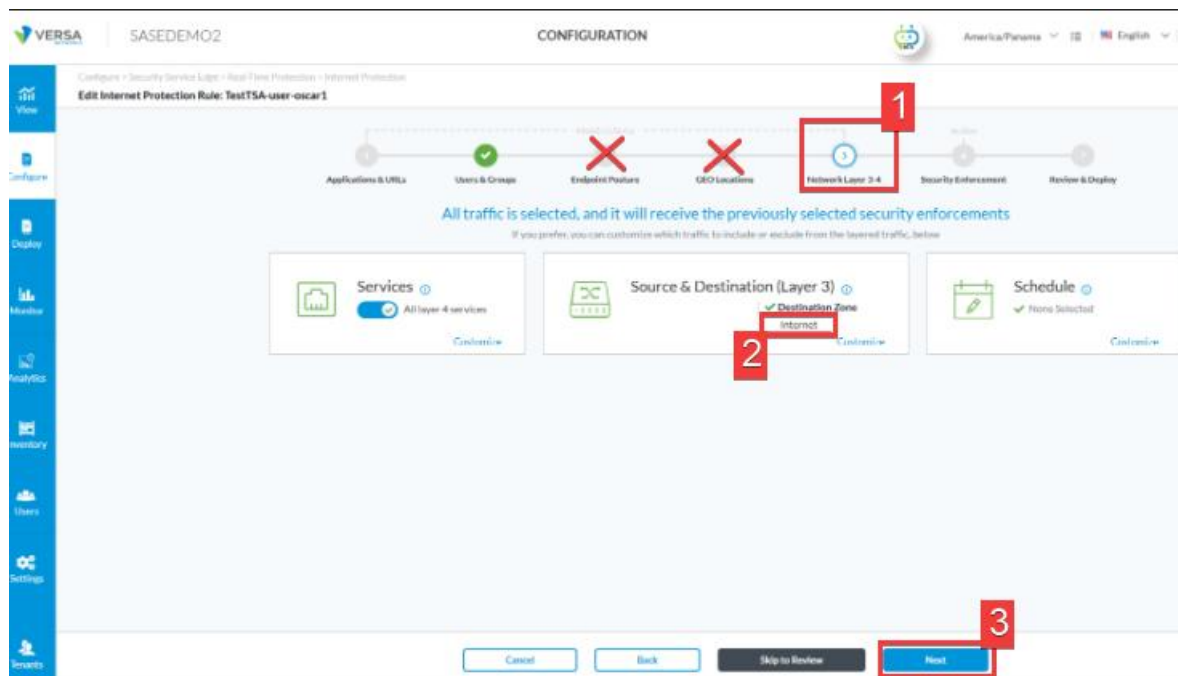
- Add a security rule to filter the required traffic.



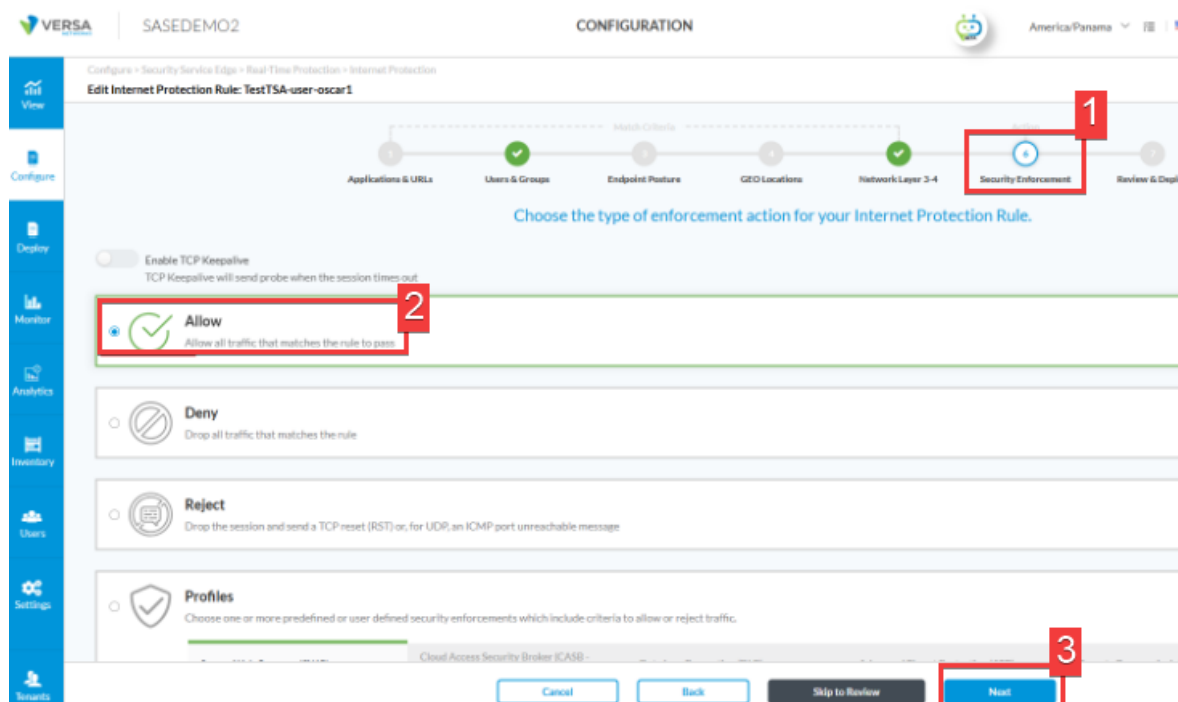
- In this case we selected Active Directory profile and selected user "oscar1"



- Matched all services with Internet as destination.



- Allow the traffic.



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

VERSA SASE Demo2 CONFIGURATION

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

Edit Internet Protection Rule: TestTSA-user-oscar1

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

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 Description

Tags

Rule is Enabled

Applications & URLs Edit

✓ All Applications

Users & Groups Edit

Cancel Back Save

- 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.

VERSA SASE Demo2 CONFIGURATION

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

Edit Internet Protection Rule: TestTSA-user-oscar2

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

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

Users & Groups

User Type All Users Selected Users Known Users Unknown Users

Enable Internet Protection for the following matched users or user groups

OscarActiveDirectory

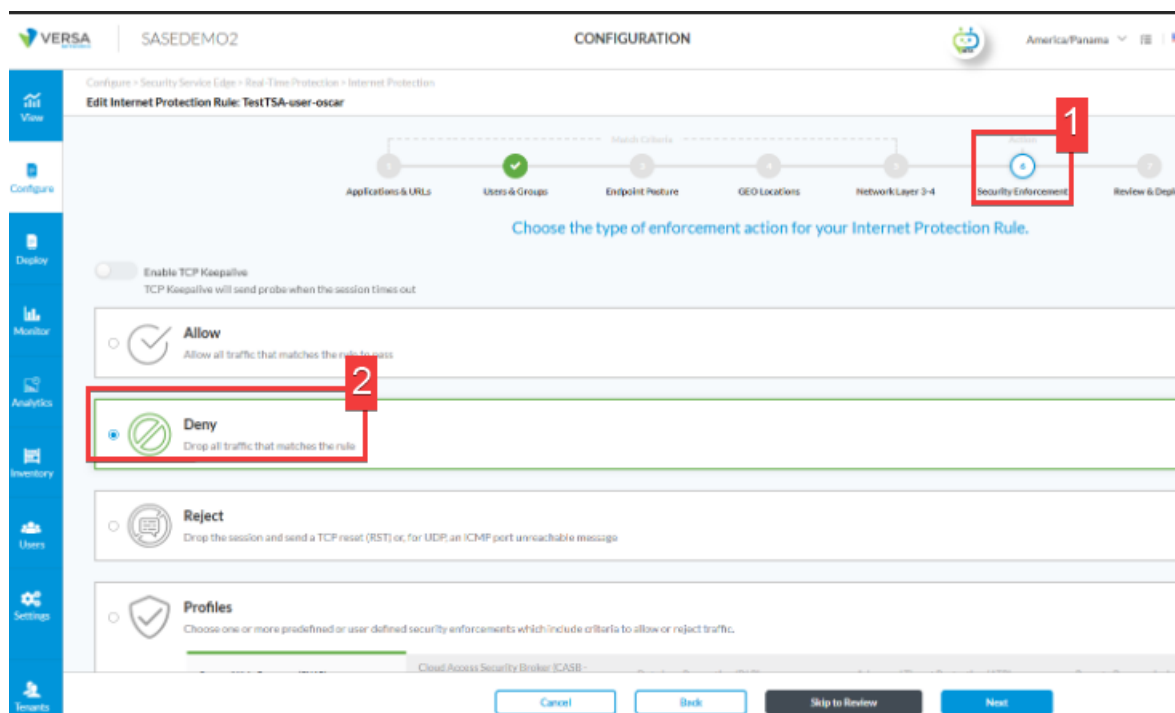
User Groups

oscar2 oscar2 Match for Users

Users (7) Add New User

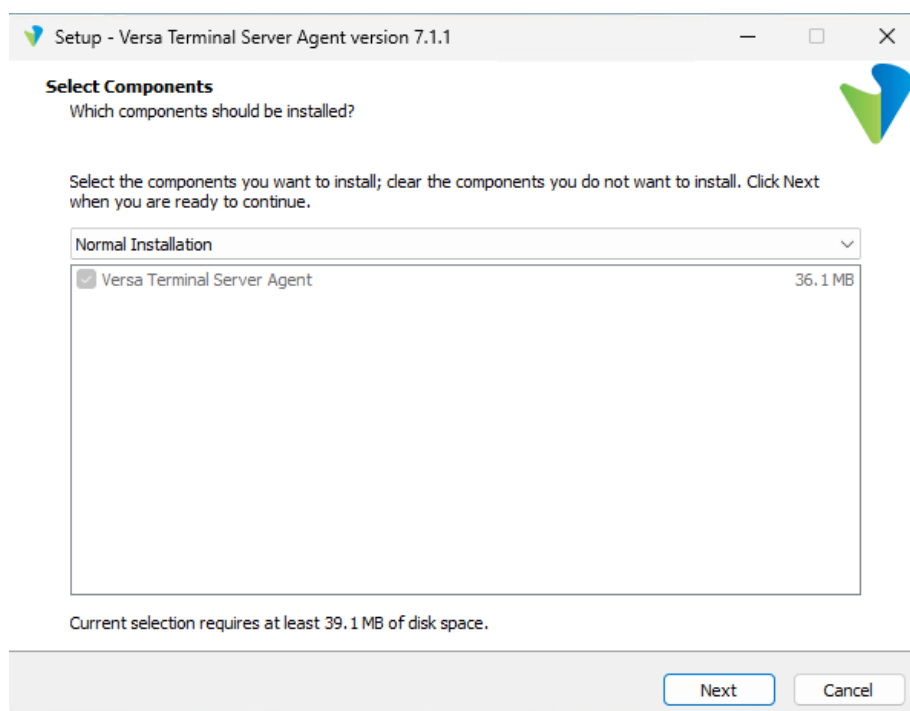
User Name	First Name	Last Name
admin admin	admin	

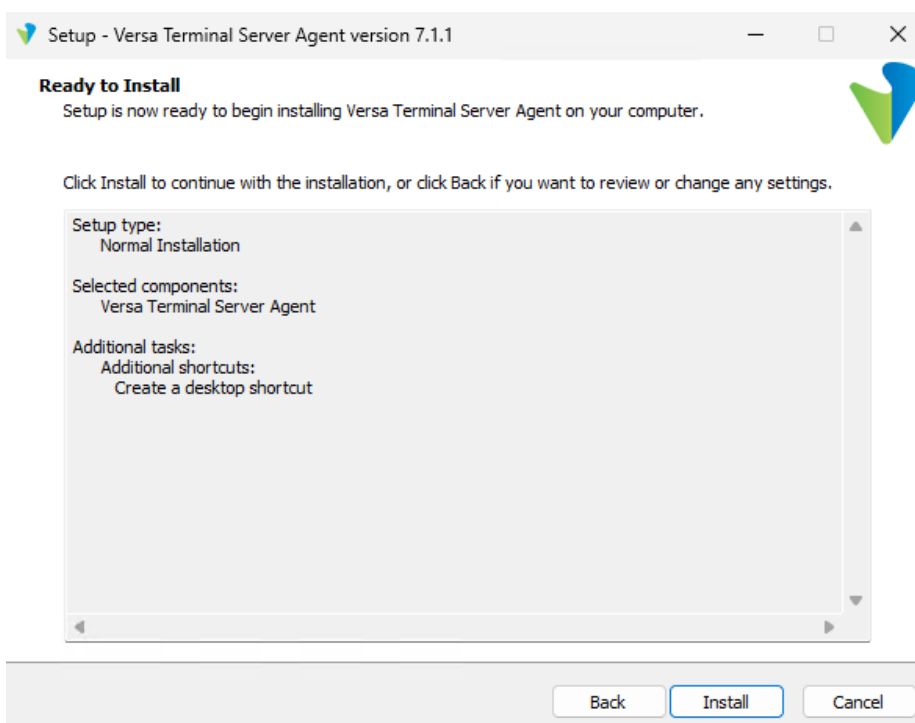
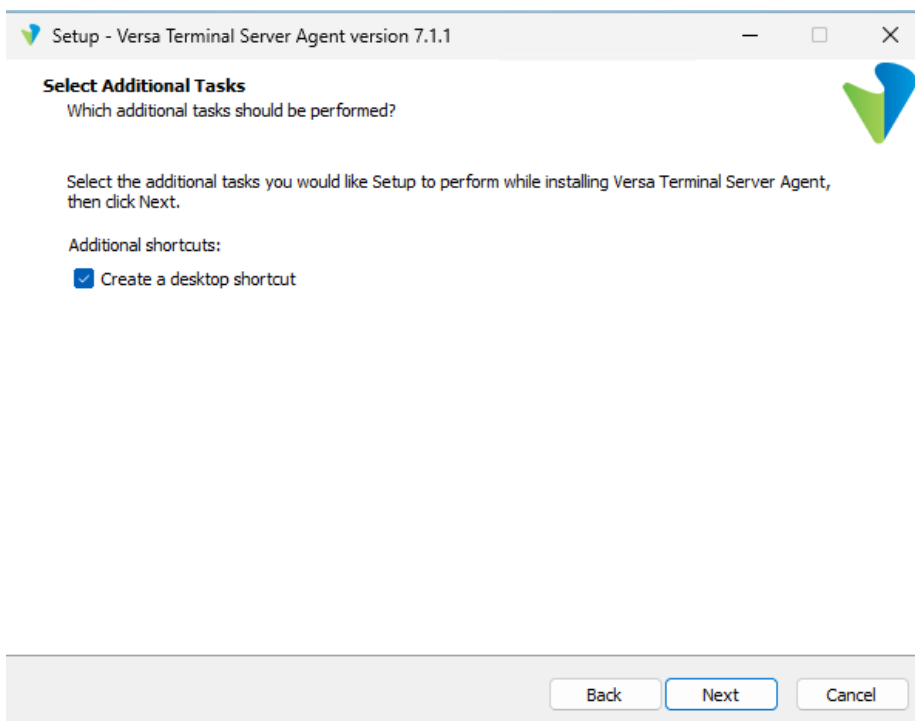
Cancel Back Skip to Review Next



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.





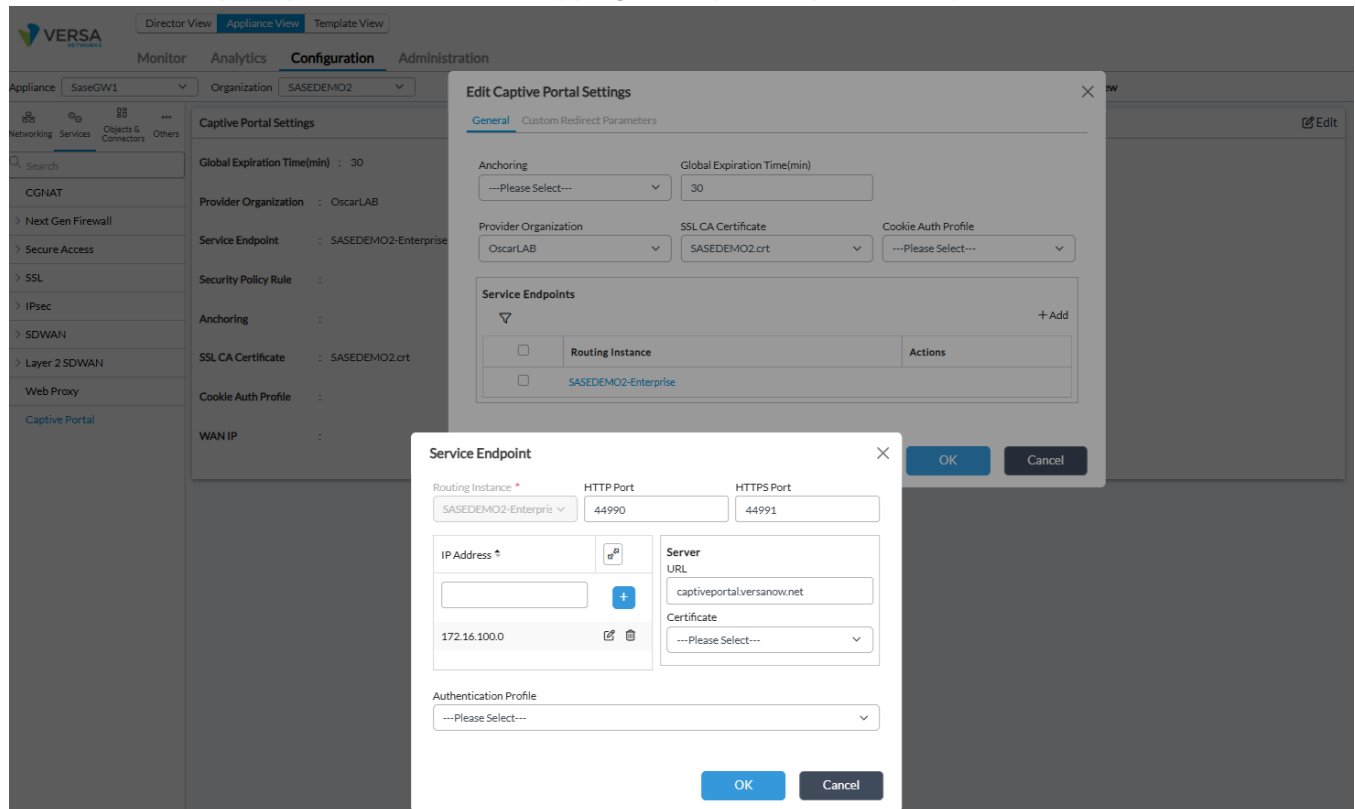
5. FQDN for TSA Agent.

We propose two options here.

- 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
eth-0/1    52:0a:49:6b:07:02  down  up      0      global   fe80::500a:49ff:fe6b:701/64
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      SASEDEM02-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      SASEDEM02-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      SASEDEM02-Control-VR  10.30.0.4/32
tvi-0/23   n/a      up    up      -      -        -
tvi-0/23.0 n/a      up    up      4      SASEDEM02-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      SASEDEM02-Enterprise  172.16.100.0/32
vni-0/0    52:0a:49:6b:07:02  up    up      2      INET-Transport-VR  10.73.107.12/16
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>
```

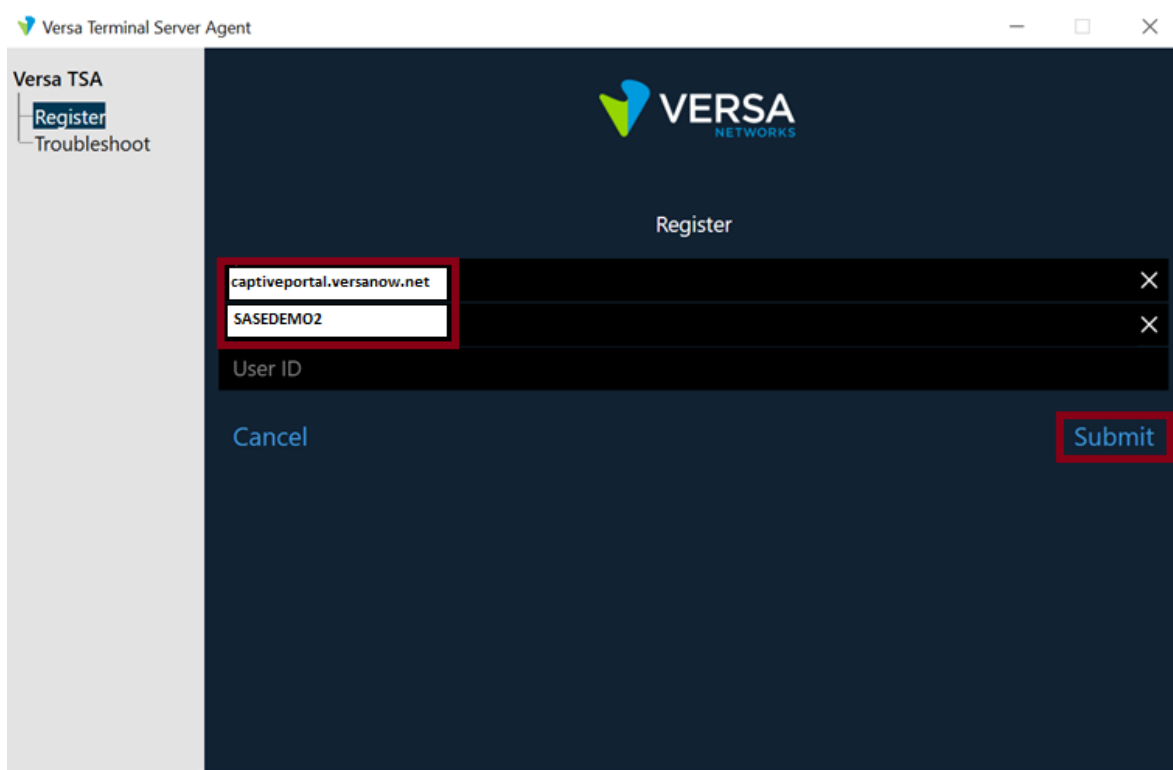
```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# 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
```

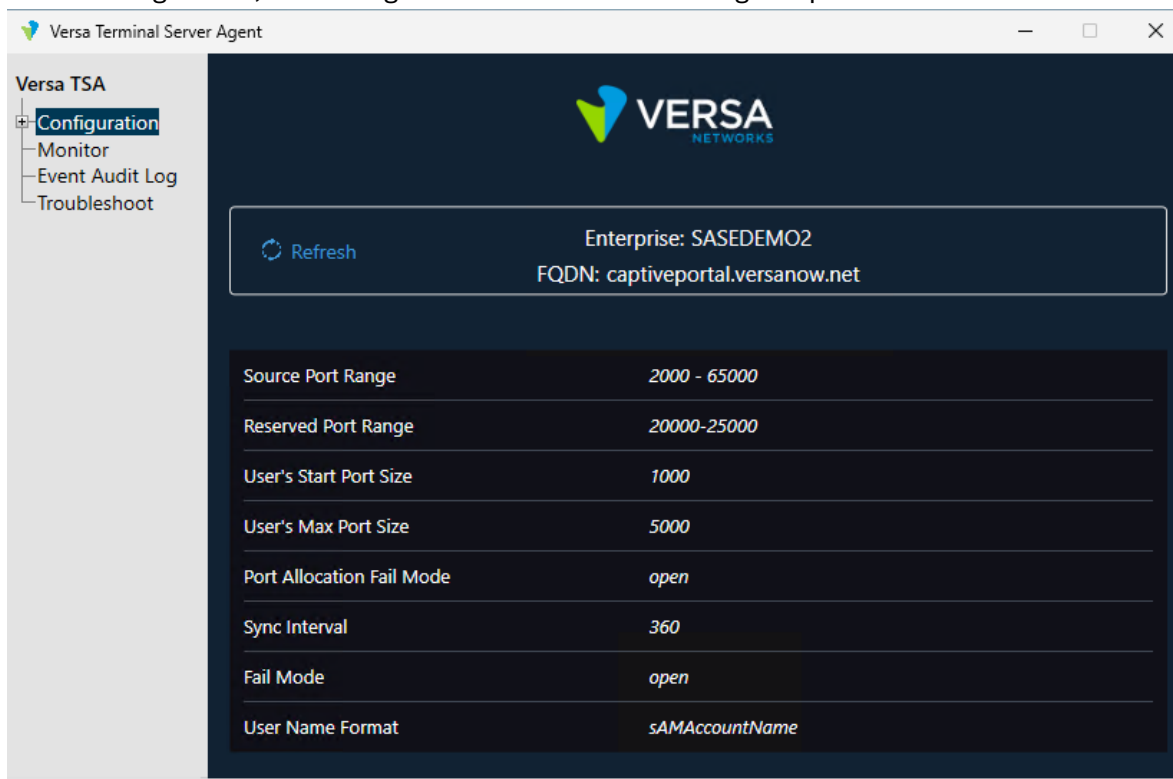
The image shows the Versa SASEDEM02 Configuration interface. The left sidebar contains navigation icons for View, Configure, Deploy, Monitor, Analytics, Inventory, and Users. The main panel is titled 'Terminal Server Agent (TSA)' and shows the 'TSA Configuration' section. It includes fields for 'Sync Interval (mins)' (360), 'Username Format' (sAMAccountName), and 'Port Allocation' (Reserved Port Range: 20000-25000, Max Size: 5000, Fail Mode: Open). The 'Fully Qualified Domain Name (FQDN)' field is set to 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

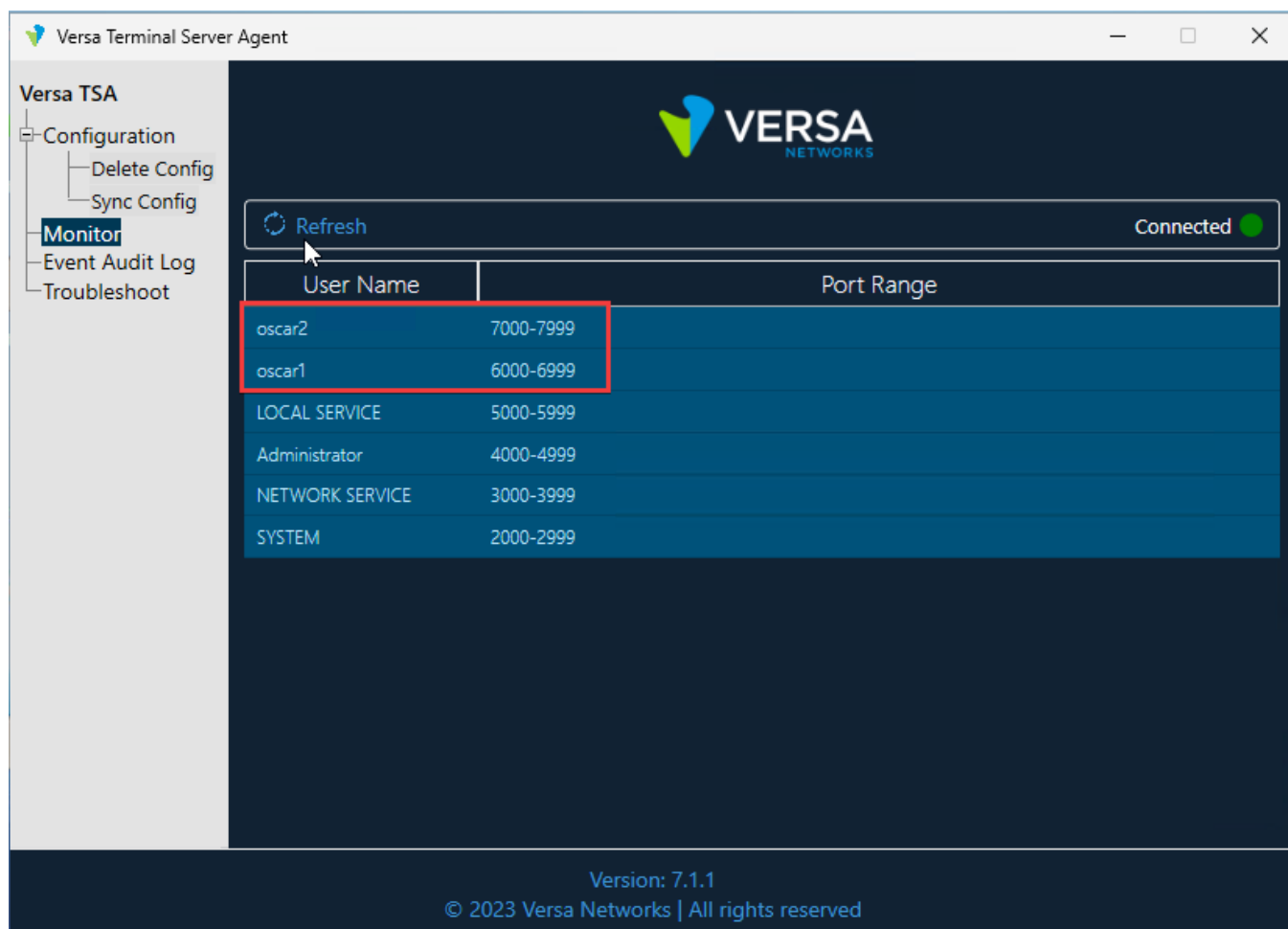


- Once registered, the Configuration tab will show settings acquired from the TSA Profile.



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.



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**

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

Summary **Services** Networking System Tools

Configuration Shell Config

SDWAN **INGPW** CGNAT Secure Access SDLAN IPsec Sessions SCI APM VMS

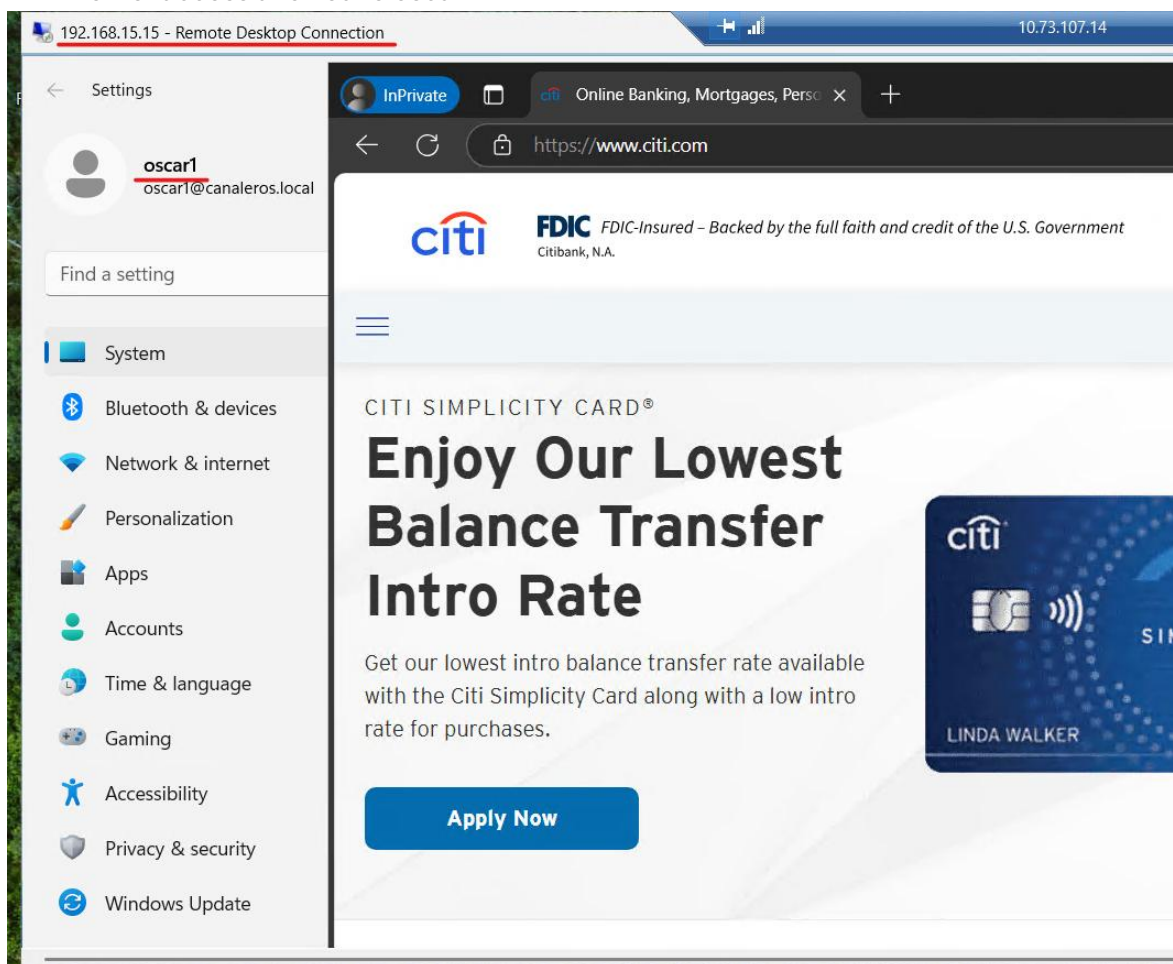
DOS Policies Entity Risk Score File Filtering IP Filtering Microsegmentation Policies Microsegmentation Statistics Persistent Action Policies Security Packages Sessions SNAT SSL Cloud URL Filtering **User Identification** User Risk So

Live Users **Detail**

Search

	IP Address	Name	Status	Session Hits	Time To Expiry	Expiration Mode	Information Source	Internal ID	Time Stamp	Login Time Sta
✓	192.168.15.15	tsa-multuser	Live	93147	60	inactivity	n/a	0	2025-07-22 15:29:08	2025-05-27 06
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”

VERSA

NETWORKS

Director View

Appliance View

Template View

Monitor

Analytics

Configuration

Administration

Organization

SASEDEMO2

You are currently in Appliance View

Summary

Devices

Cloud Workflow

Total Appliances

6

SaseGW1

SaseGW1 | FL US

Inband Management Address: 10.30.0.5

Out of band Management Address: 10.73.107.7/16

System Bridge Address: 0A:49:4B:07:01:00

Reachable

SYN: IN SYN

Up since: Tue May 13 08:19:30 2025

Summary

Services

Networking

System

Tools

Configuration

Shell

Config Status

Upgrade

Subscription

SDWAN

NGFW

CGNAT

Secure Access

SDLAN

IPsec

Sessions

SCI

APM

VMS

Extensive

Back

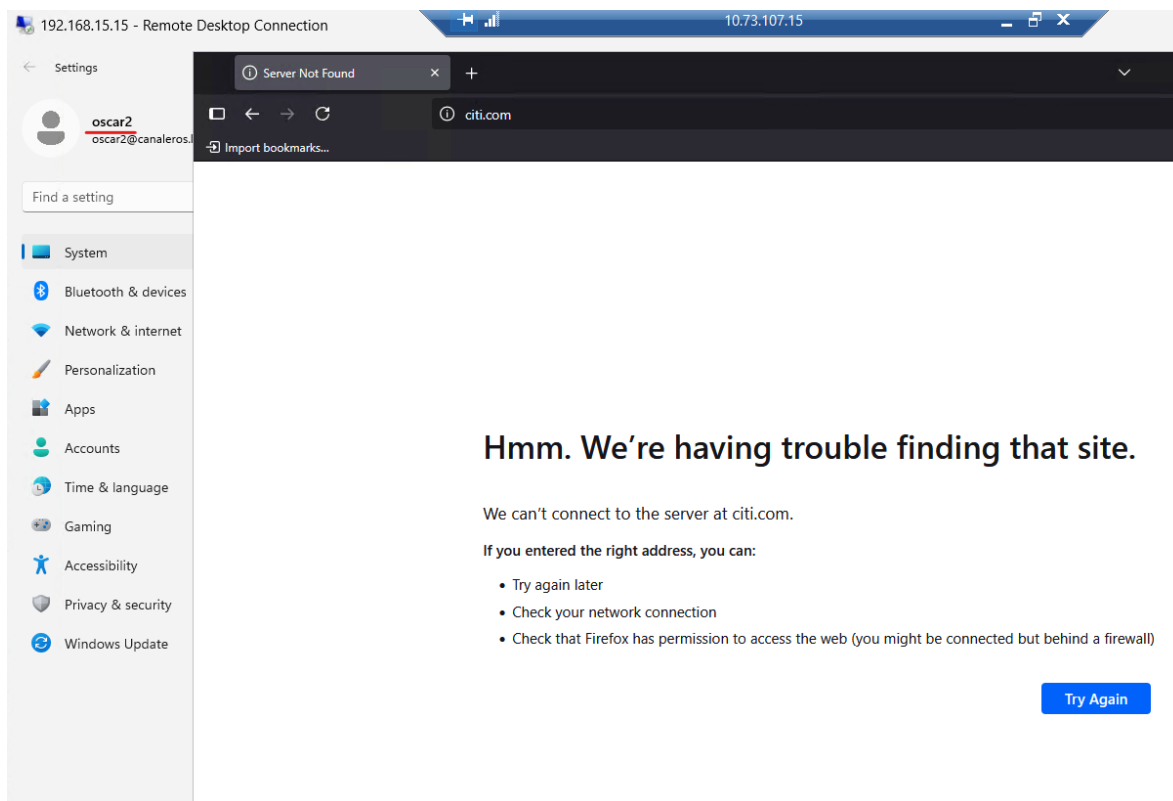
Search

1

25

Application	Source IP	Destination IP	Protocol	Source Port	Destination P...	SDWAN	Natted	Reverse Egres...	Nsh Peer Dest...	Reverse Packe...	NAT Source IP	Reverse Rel...	Reverse SDW...	Reverse Egres...	Nsh Peer Sour...	Parent Sessio...	External Serv...	Is Child
>		10.30.0.5	TCP	1356	1234	No	No			23397						0	false	No
>		192.168.15.15	TCP	2002	443	Yes	No	Branch-1-VOS		667			2899235639...	INET/INET		0	false	No
>	citi_bank(predef)	192.168.15.15	TCP	6024	443	Yes	Yes	Branch-1-VOS		73	10.73.107.12		2899235639...	INET/INET		0	false	No
>	citi_bank(predef)	192.168.15.15	TCP	6012	443	Yes	Yes	Branch-1-VOS		176	10.73.107.12		2899235639...	INET/INET		0	false	No
>	dns(predef)	192.168.15.15	TCP	6098	443	Yes	Yes	Branch-1-VOS		80	10.73.107.12		2899235639...	INET/INET		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.

Organization: SASEDEMO2 You are currently in Appliance View Build

Summary Devices Cloud Workload

Total Appliances: 6 SaseGW1

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_SYNC Up since: Tue May 13 08:19:30 2022

Summary Services Networking System Tools Configuration Shell Config Status Upgrade Subscription

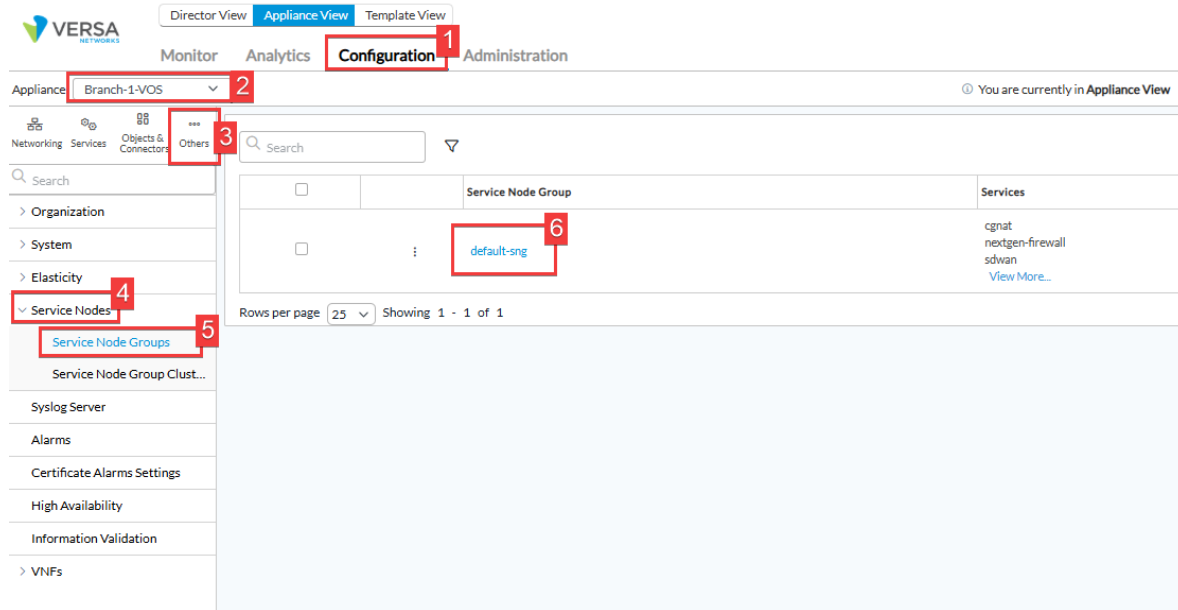
Application	Source IP	Destination IP	Protocol	Source Port	Destination P...	Reverse Egres...	Nsh Peer Dest...	Reverse Packe...	NAT Source IP	Reverse Relea...	Reverse Egres...	Nsh Peer Sour...	Parent Sessio...	External Servi...	Is Child	RX WAN Ckt	Forward FEC ...	Forward St
> [img]	192.168.15.15	146.75.93.91	TCP	7105	443			0	10.73.107.12	-		0	0	false	No	INET:INET		
> [img]	192.168.15.15	199.232.211.52	TCP	7033	443			0	10.73.107.12	-		0	0	false	No	INET:INET		
> [img] dns/(predef)	192.168.15.15	8.8.8.8	UDP	63910	53	Branch-1-VOS		1	10.73.107.12	INET:INET		0	0	false	No	INET:INET		
> [img]	192.168.15.15	172.64.155.119	TCP	7017	443			0	10.73.107.12	-		0	0	false	No	INET:INET		
> [img] dns/(predef)	192.168.15.15	8.8.8.8	UDP	59433	53	Branch-1-VOS		1	10.73.107.12	INET:INET		0	0	false	No	INET:INET		
> [img]	192.168.15.15	104.18.32.137	TCP	7096	443			0	10.73.107.12	-		0	0	false	No	INET:INET		
> [img]	192.168.15.15	151.101.41.60	TCP	7019	443			0	10.73.107.12	-		0	0	false	No	INET:INET		
> [img] dns/(predef)	192.168.15.15	8.8.8.8	UDP	57401	53	Branch-1-VOS		1	10.73.107.12	INET:INET		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 Director Configuration page. The interface includes a top navigation bar with tabs for Director View, Appliance View, and Template View. Below this is a secondary navigation bar with Monitor, Analytics, Configuration (highlighted with a red box and callout 1), and Administration. The main content area is divided into a left sidebar and a central table.

Callout 1: Points to the 'Configuration' tab in the top navigation bar.

Callout 2: Points to the 'Appliance' dropdown menu in the top left, which is currently set to 'Branch-1-VOS'.

Callout 3: Points to the 'Others' icon in the left sidebar navigation menu.

Callout 4: Points to the 'Service Nodes' dropdown menu in the left sidebar navigation menu.

Callout 5: Points to the 'Service Node Groups' option in the expanded 'Service Nodes' dropdown menu.

Callout 6: Points to the 'default-sng' link in the 'Service Node Group' column of the table.

	Service Node Group	Services
<input type="checkbox"/>	default-sng	cgnat nextgen-firewall sdwan View More...

At the bottom of the table, it says 'Rows per page: 25 Showing 1 - 1 of 1'.

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

×

Edit Service Node Group - default-sng

Name *

default-sng

Service Node Group ID *

0

Description

Tags

Type

Internal

Elastic Policy

--Select--

Egress Interface

--Select--

Ingress Interface

--Select--

Service Function Egress Address

Service Function Ingress Address

Services *

Available Services

Add All

Search

Q

adc

>

stateful-firewall

>

ipsec

>

secure-access

>

tdf

>

iot-security

>

Selected Services

Remove All

Search

Q

cgnat

×

nextgen-firewall

×

sdwan

×

1

→

2

OK

Cancel

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

The screenshot shows the Versa Director interface in the Appliance View Configuration tab. The left sidebar shows the 'Organization' menu item highlighted with a red box and a red '1'. The main table lists organizations with columns: Organization Name, Appliance Owner, Enterprise Names, Services, Service Node Groups, Service Node Group Cluster, and Peak Rate (pps). The 'SASEDEMO2' organization is highlighted with a red box and a red '2'. Below the table, the 'Edit Organization Limit - SASEDEMO2' dialog is open. The 'Services' tab is selected, and the 'SASEDEMO2' service is highlighted with a red box and a red '3'. The 'OK' button is highlighted with a red box and a red '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 Director interface in the Appliance View Configuration tab. The left sidebar shows the 'TSA' menu item highlighted with a red box and a red '1'. The main table lists TSA profiles with columns: Name, Description, Sync Interval, Fail Mode, Username Format, and Actions. The 'TSAprofile-1' profile is highlighted with a red box and a red '2'. Below the table, the 'TSA Profile' configuration page is open. The 'General' tab is selected, and the 'TSA Profile' is highlighted with a red box and a red '3'. The 'OK' button is highlighted with a red box and a red '4'.

- Type in the Name (Required).

Edit TSA Profiles

×

Name *

TSAprofile-1

Description

Sync Interval(mins)

360

Fail Mode

Open

▼

Username Format

userPrincipalName

▼

Port Allocation

Source Range *

10000-20000

Reserved Range

Start Size *

100

Max Size *

1000

Fail Mode

Close

▼

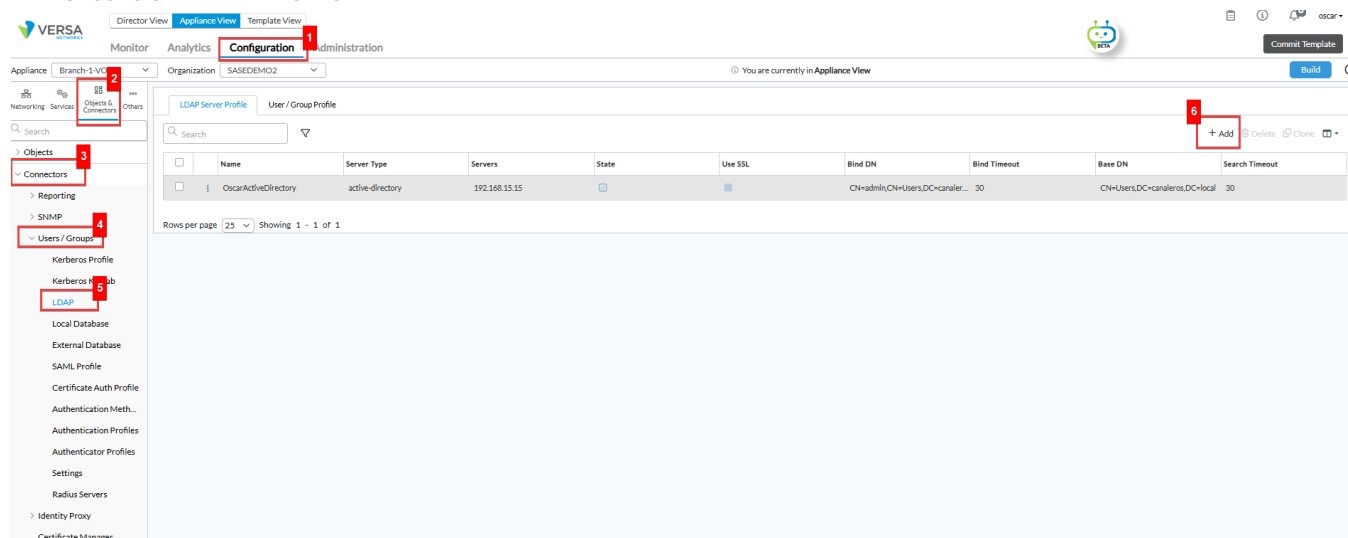
OK

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	$4 \times 5000 = 20,000$
Reserved Port Range	10000-30000
Fail Mode	Close (recommended)

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



The screenshot shows the Versa configuration interface. The left sidebar contains a navigation menu with the following items: Appliance, Networking, Services, Objects & Connectors, Reporting, SNMP, Users / Groups, Kerberos Profile, Kerberos H...ab, LDAP, Local Database, External Database, SAML Profile, Certificate Auth Profile, Authentication Meth..., Authentication Profiles, Authenticator Profiles, Settings, Radius Servers, Identity Proxy, and Certificate Manager. The main area displays the 'LDAP Server Profile' configuration page. A table lists the LDAP servers, with one entry for 'OscarActiveDirectory' on '192.168.15.15'. The table has columns for Name, Server Type, Servers, State, Use SSL, Bind DN, Bind Timeout, Base DN, and Search Timeout. The 'Bind DN' is 'CN=admin,CN=Users,DC=canaler...' and the 'Base DN' is 'CN=Users,DC=canaleros,DC=local'. The 'Search Timeout' is '30'. The bottom of the table shows 'Rows per page: 25' and 'Showing 1 - 1 of 1'.

- 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 *
Active Directory

Domain Base
Domain Name *
canaleros.local

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

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

Bind Password *
.....

Bind Timeout *
30

Search Timeout *
30

Use SSL
☐ Enable ☒ Disable

State
☒ Enable ☐ Disable

SSL Mode
LDAPS

CA Certificate
--Select--

OK Cancel

- Fill in the information of the Active Directory server.

Edit LDAP Server Profile - OscarActiveDirectory

General **Servers**

Servers

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

OK Cancel

Edit Servers

Name *
192.168.15.15

IP Address
192.168.20.15

Port *
389

Routing Instance
SASEDEMO2-Enterprise

FQDN

OK Cancel

• Create an Authentication Method

VERSA Configuration page showing the 'Authentication Methods' section in the left sidebar. The main table displays the following data:

Name	Description	Method	Profile	Actions
ldap-auth		LDAP	OscarActiveDirectory	

Rows per page: 25 | Showing 1 - 1 of 1

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

Edit Authentication Methods

Name *

ldap-auth

Description

Authentication Method

Method

LDAP Profile

LDAP Profile

OscarActiveDirectory

OK

Cancel

- Create an authentication profile.

The screenshot shows the VERSA Configuration page. The left sidebar contains a navigation menu with the following items: Reporting, SHMP, Users / Groups, Kerberos Profile, Kerberos Keytab, LDAP, Local Database, External Database, SAML Profile, Certificate Auth Profile, Authentication Meth..., Authentication Profiles, Authenticator Profiles, Settings, and Radius Servers. The 'Authentication Profiles' item is highlighted with a red box and a red number 5. The main content area shows a table with columns: Name, Default Authenticator, Default Authentication Method, Caching Mode, Cache Expiration (mins), Cookie Expiration (mins), LEF Profile, and Routing Instance. The table contains one row with the name 'Idap-auth'. A red box with a red number 6 highlights the '+ Add' button in the top right corner of the table.

- Note that the caching mode must be hybrid

The screenshot shows the 'Edit Authentication Profile - Idap-auth' form. The form has two tabs: 'General' and 'Rules'. The 'General' tab is active. The form contains the following fields and controls:

- Name:** A text field containing 'Idap-auth', highlighted with a red box.
- Description:** A text field.
- Authentication Type:** A dropdown menu with 'Active' selected.
- Caching Mode:** A dropdown menu with 'Hybrid' selected, highlighted with a red box.
- Cookie Name:** A text field.
- Cache Expiration (mins):** A text field containing '10'.
- Cookie Expiration (mins):** A text field.
- Concurrent Login:** A text field containing '1'.
- Expiration Mode:** A dropdown menu with '--Select--' selected.
- Default Authenticator:** A dropdown menu with '--Select--' selected.
- Proactive-Reauth:** A checkbox.
- Default Authentication Method:** A list of methods with checkboxes. The 'Idap-auth' method is selected and highlighted with a red box.
- LEF Profile:** A dropdown menu with '--Select--' selected.
- Default Profile:** A checkbox that is checked.

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

- Set the TSA profile along with the authentication method

Director View | **Appliance View** | Template View

Monitor | Analytics | **Configuration** | Administration

Appliance | Branch VCS | Organization | SASEDEMO2

You are currently in Appliance View

Build | Edit

General

URI	:	TSA
Service Type	:	TSA
Authentication	:	ldap-auth
LEF Profile	:	-
Default LEF Profile	:	enabled
Device Authentication Profile	:	-
TSA Profile	:	TSAprofile-1

Add Services [X]

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.

The screenshot shows the Versa SD-WAN configuration interface. The 'Configuration' tab is active, and the 'Virtual Routers' section is highlighted in the left sidebar (labeled 2). In the top right corner, the 'Build' button is highlighted (labeled 1). Below the sidebar, a table lists existing Virtual Routers:

Name	View	Interfaces	Networks	Static Routes	OSPF	OSPFv3	BGP	PIM	IGMP	RIP	Router Advertisement	Redistribution Policies
INET-Transport-VR		tv-0/602.0	INET	0.0.0.0/0			3000					ST-Policy
OscarLAB-Control-VR		phv1025 tv-0/2.0 tv-0/3.0					1					Control-VR-Policy
OscarLAB-LAN-VR												
SASEDEMO2-Control-VR		phv1025 tv-0/22.0 tv-0/23.0					11					Control-VR-Policy
SASEDEMO2-Enterprise		tv-0/603.0 tv-0/772.0	LAN1				3115					Default-Policy-To-BGP
SASEDEMO2-Enterprise-TSA		tv-0/771.0		0.0.0.0/0								

An '+ Add' button is highlighted (labeled 3) above the table.

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

The screenshot shows the 'Configure Virtual Router' dialog box. The 'Virtual Router Details' tab is selected (labeled 1). The 'Instance Name' field is highlighted (labeled 2) and contains the text 'SASEDEMO2-Enterprise-TSA'. The 'Instance type' is set to 'Virtual routing instance'. The 'Global VRF ID' field is empty. Below these fields, there are sections for 'MPLS VPN Core' and 'EVPN Core', each with fields for 'Local Router Address' and 'Local Router Interface'. The 'Interfaces/Networks' section is currently empty, showing 'Interfaces/Networks Not Configured'. At the bottom right, the 'OK' button is highlighted (labeled 3).

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

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Administration

Appliance | Branch-1-VOS (South)

© You are currently in Appliance View

Commit Template | Commit | Discard

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

Search

Name	Description	IP Address/Mask	MTU	Type	Pseudo Tunnel	Pseudo Tunnel Remote Address
ptv1025					tv1-0/3.0	10.30.0.0
ptv1035					tv1-0/23.0	10.30.0.2
tv1-0/2	VXLAN Tunnel Interface for OscarLAB Cont...	10.30.0.8/32		p2mp-vlan		
tv1-0/22	VXLAN Tunnel Interface for SASEDEMO2 C...	10.30.0.8/32		p2mp-vlan		
tv1-0/23	ESP Tunnel Interface for SASEDEMO2 Cont...	10.30.0.9/32		p2mp-esp		
tv1-0/3	ESP Tunnel Interface for OscarLAB Control...	10.30.0.9/32		p2mp-esp		
tv1-0/602	WAN side Split Tunnel Interface between IN...	169.254.0.2/31		paired		
tv1-0/603	LAN side Split Tunnel Interface between IN...	169.254.0.3/31		paired		
tv1-0/771		10.10.10.1/30	1400	paired		
tv1-0/772		10.10.10.2/30	1400	paired		

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

© 2025 Versa Networks | All Rights Reserved | 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 - tv1-0/771

Tunnel | Pseudo Tunnel | PPPoE

Interface * | tv1 | 0 / 771 | Disable | Mirror Interface

Description

MTU | 1400 | Mode | IPsec

Tunnel Type | Paired | Paired Interface * | tv1 | 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				

OK | Cancel

- 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.

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Admin

Appliance | Branch-1-VOS (South)

Networking | Services | Objects & Connectors | Others

Search

Interfaces

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

> VRRP

VNI | AE | ENet | IRB | T1/E1

Search

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

Edit Tunnel Interface - tvi-0/771

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

+ 1

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

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Admin

Appliance | Branch-1-VOS (South)

Networking | Services | Objects & Connectors | Others

Search

Interfaces

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

> VRRP

Zones

VNI | AE | ENet | IRB | T1/E1

Search

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

Rows per page 25 Showing 1 - 10 of 10

Edit Tunnel Interface - tvi-0/771

tvi - 0 / 771

☐ Disable ☐ Mirror Interface

Description

MTU 1400 Mode IPsec

Edit Subinterface

General IPv4 IPv6 Bridge

Unit 0 Description

VLAN ID 0 ☐ Disable

Bandwidth

Uplink (Kbps) 1..100000000 Downlink (Kbps) 1..100000000

OK Cancel

Edit Subinterface

General **IPv4** Bridge

Static Address

☐ IP Address/Mask

☐ 10.10.10.1/30

OK Cancel

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

VERSA

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Admin

Appliance Branch-1-VOS (South)

Networking Services Objects & Connectors Others

Search

Interfaces

WLAN

T1/E1 Auth

Networks

Virtual Wires

Global Routers

Virtual Routers

Virtual Switches

> IP-SLA

> TWAMP

SaaS App Monitor

> VRRP

Zones

> DNS

LLDP

Zone Protection Profiles

VNI AE ENet IRB T1/E1

Search

☐ Name

☐ pti1025

☐ pti1035

☐ tvi-0/2

☐ tvi-0/22

☐ tvi-0/23

☐ tvi-0/3

☐ tvi-0/602

☐ tvi-0/603

☐ tvi-0/771

☐ **tvi-0/772**

Rows per page 25 Showing 1 - 10 of 10

Edit Tunnel Interface - tvi-0/772

tvi 0 / 772

☐ Disable ☐ Mirror Interface

Description

MTU 1400 Mode IPsec

Tunnel Type Paired Paired Interface * tvi 0 / 771

☐ Next Round Trip Time

Multihoming

Active Mode --Select--

Subinterface

☐ Unit

☐ 0

Edit Subinterface

General **IPv4** IPv6 Bridge

Static Address

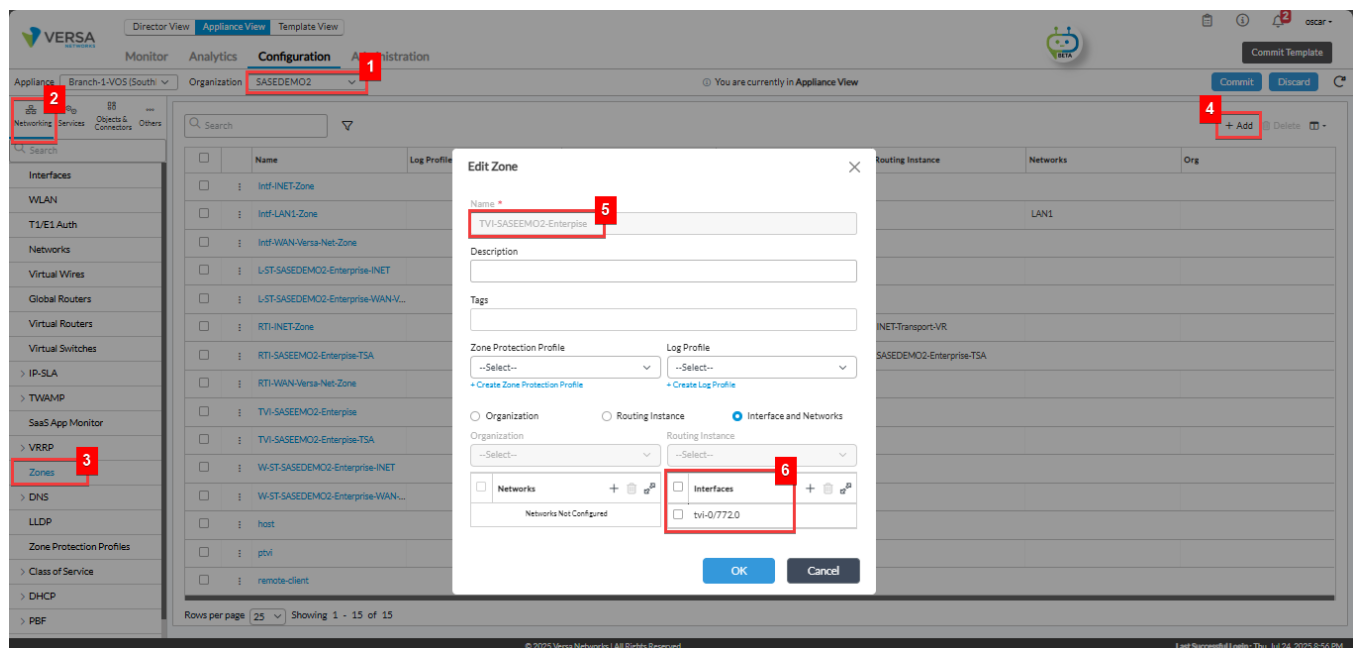
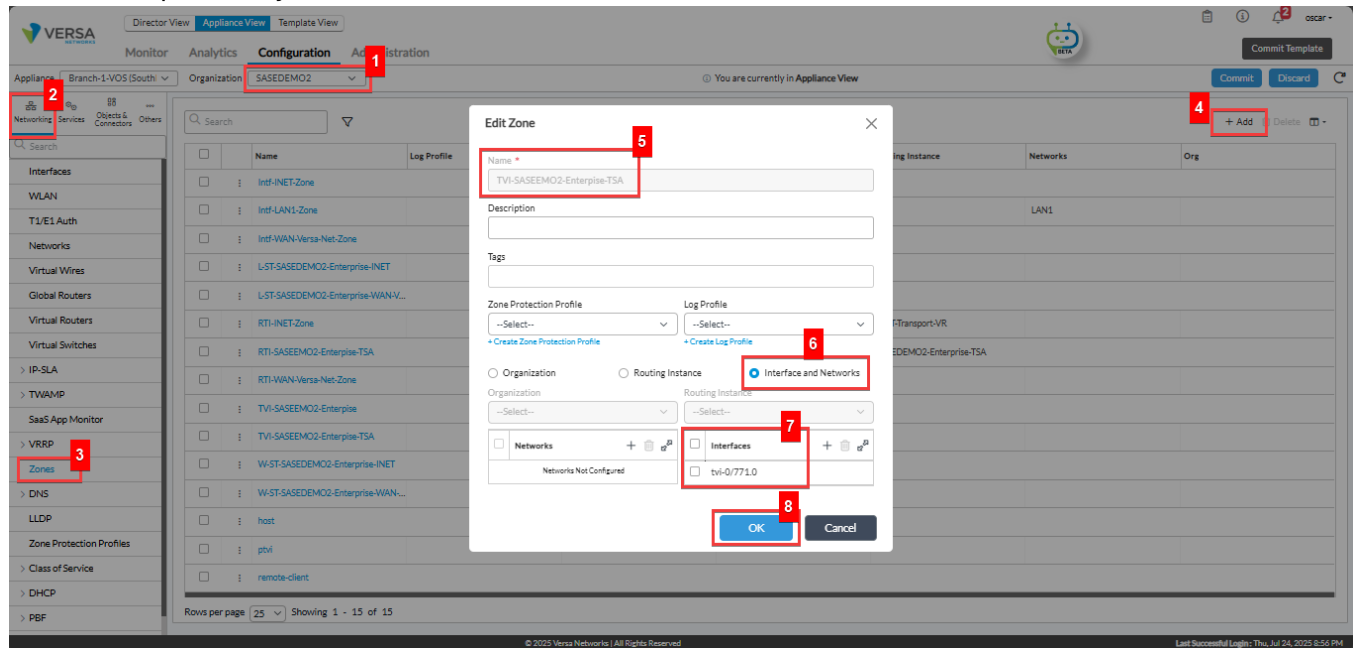
☐ IP Address/Mask

☐ 10.10.10.2/30

OK Cancel

OK Cancel

- 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.

The screenshot shows the Versa Networks Configuration page. The left sidebar contains a navigation menu with categories like Networking, Services, and System. The main content area is titled 'Configuration' and shows a table of Organization Limits. The table has columns for Organization Name, Appliance Owner, Enterprise Names, Services, Service Node Groups, Service Node Group Clusters, QoS, Session, and DHCP. The table lists two organizations: OscarLAB and SASEDEMO2. The SASEDEMO2 row is highlighted, and the 'Limits' option is selected in the left sidebar. The table shows that SASEDEMO2 has a session limit of 1000000 and a DHCP limit of 1000000. The table also shows that SASEDEMO2 has a service node group cluster of 'default-ong' and a service node group of 'default-ong'.

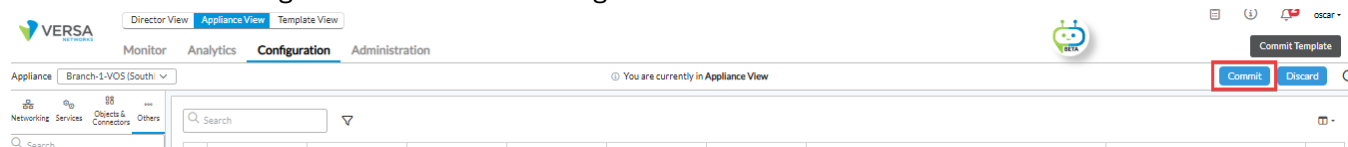
- Add the TVI interfaces in the Traffic Identification tab.

The screenshot shows the 'Edit Organization Limit - SASEDEMO2' dialog box. The 'Traffic Identification' tab is selected. The dialog box contains a table of TVI interfaces. The table has columns for TVI ID, TVI Name, and TVI Description. The table lists four TVI interfaces: tv-0/1035, tv-0/22.0, tv-0/23.0, and tv-0/603.0. The tv-0/771.0 and tv-0/772.0 rows are highlighted. The 'Add' button is visible in the top right corner of the table. The 'OK' and 'Cancel' buttons are at the bottom right of the dialog box.

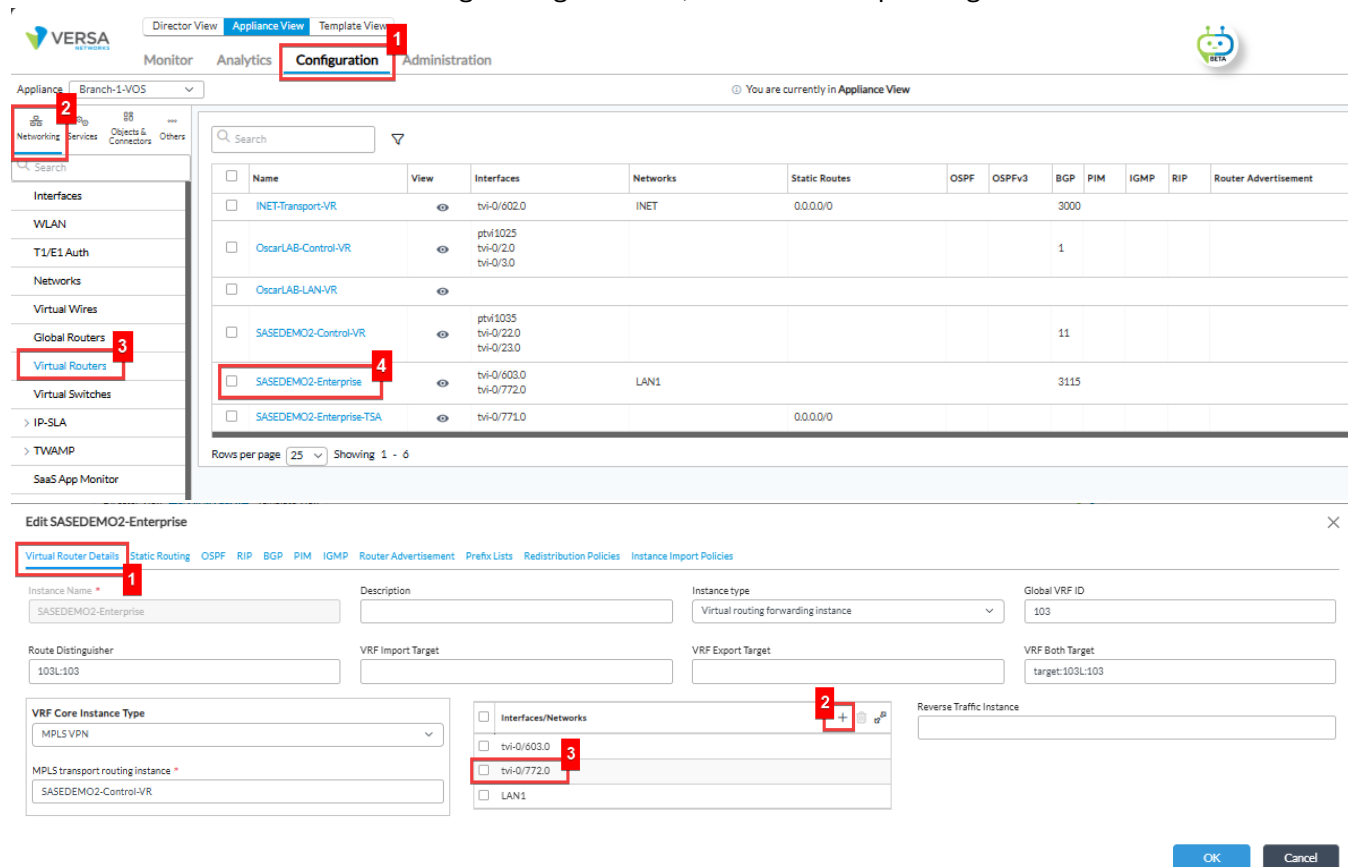
- Add the new Routing Instance “SASEDEMO2-Enterprise-TSA” to the Available and then Owned section in the Resources tab.

The screenshot shows the 'Edit Organization Limit - SASEDEMO2' dialog box. The 'Resources' tab is selected. The dialog box contains several sections: Available Routing Instances, Owned Routing Instances, Available Provider Organizations, Available Networks, Available URL Categories, and Available Address Groups. The 'Available Routing Instances' section lists four routing instances: INET-Transport-VR, OscarLAB-Control-VR, SASEDEMO2-Control-VR, and SASEDEMO2-Enterprise. The 'Owned Routing Instances' section lists three routing instances: SASEDEMO2-Control-VR, SASEDEMO2-Enterprise, and SASEDEMO2-Enterprise-TSA. The 'Available Provider Organizations' section lists one provider organization: OscarLAB. The 'Available Networks' section lists three networks: INET, LAN1, and WAN-Versa-Net. The 'Available URL Categories' section is empty. The 'Available Address Groups' section is empty. The 'SASEDEMO2-Enterprise-TSA' routing instance is highlighted in the 'Owned Routing Instances' section. The 'OK' and 'Cancel' buttons are at the bottom right of the dialog box.

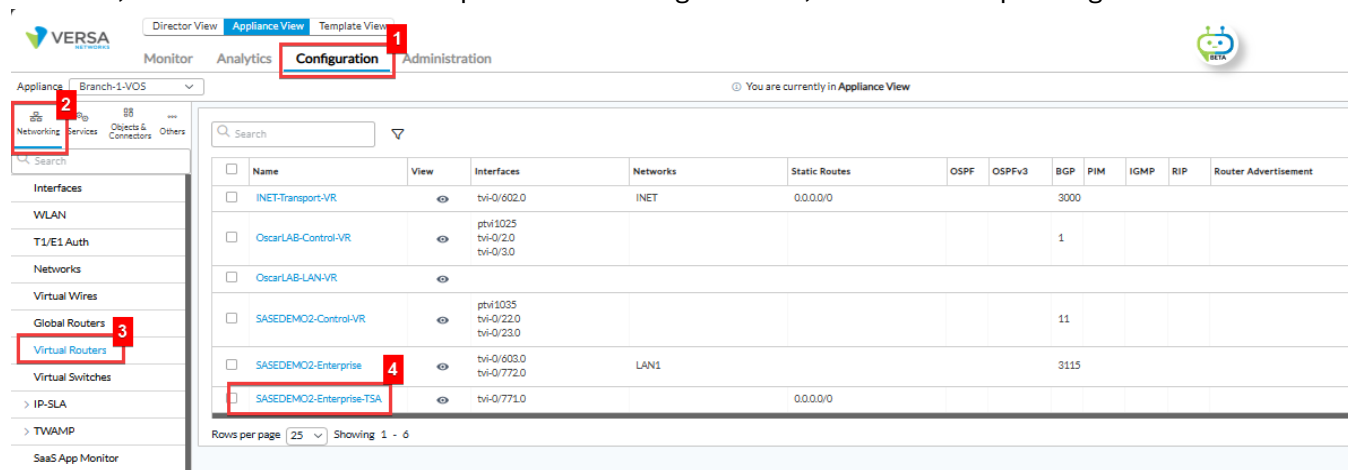
- Commit the changes to save the new configurations.



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



- Next, in the “SASEMO2-Enterprise-TSA” routing instance, add the corresponding new TVI interface



Edit SASEMO2-Enterprise-TSA

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

Instance Name: SASEMO2-Enterprise-TSA | Description: | Instance type: Virtual routing instance | Global VRF ID: |

☐ MPLS VPN Core

Local Router Address: IPv4 Or IPv6 Address | Local Router Interface: --Select-- | Family: --Select--

☐ EVPN Core

Local Router Address: IPv4 Address | Local Router Interface: --Select-- | Family: --Select--

☐ Cloud Export Instance | ☐ Intelligent Traffic Director

☐ Interfaces/Networks | tvl-0/771.0

OK Cancel

- Add a default route in “SASEMO2-Enterprise-TSA” with next-hop as TVI IP in “SASEMO2-Enterprise”

Edit SASEMO2-Enterprise-TSA

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

IPv4/v6 Unicast | IPv4 Multicast | IPv6 Multicast

Edit IPv4/v6 Unicast

Destination: 0.0.0.0/0 | Monitor: --Select-- | Monitor Group: --Select--

Metric: Allowed Range is 1 - 4294967295 | Preference: 1 | Tag: |

Action

Interface: tvl-0/771.0 | Next Hop IP Address: 10.10.10.2 | Next Routing Instance: --Select-- | Discard: ☐ | Reject: ☐ | No Install: ☐

☐ Enable ICMP | Interval: Allowed Range is 1 - 60 | Threshold: Allowed Range is 1 - 60

☐ Enable BFD (Bidirectional Forwarding Detection) | Minimum Receive Interval (msec): Allowed Range is 1 - 235000 | Minimum Transmit Interval (msec): Allowed Range is 1 - 235000 | Multiplier: Allowed Range is 1 - 255

OK Cancel

- Now, create a new security policy to allow traffic towards “SASEMO2-Enterprise-TSA” routing instance.

VERSA | Director View | Appliance View | Template View

Monitor | Analytics | **Configuration** | Administration

Appliance: SASEMO2 | Organization: SASEMO2

Access Policies | Rules

Default-Policy | Search: | + Add | Delete | Clone | Move

Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	Source
1	AccessRule-Oscar1	False							User Defined Devices
2	Allow_From_That	False		Intf-LAN1-Zone					Discovered Devices
3	Allow_From_SOWAN	False		ptvl					User Defined Devices
4	To-TSA	False							
5	From-TSA	False		TVI-SASEMO2-Enter...					
6	DenyRule-Oscar2	False							

- Name the policy

Edit Rule - To-TSA ✕

General 1 Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

Name 2 To-TSA

Description

Tags Alias Name

☐ Disable Rule

OK Cancel

- In the Destination tab, select the “TVI-SASEMO2-Enterprise” zone assigned TVI in SASEMO2-Enterprise routing instance.

Edit Rule - To-TSA ✕

General Source **Destination** 1 Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

☐ Destination Zone 2 + New Zone + ⌵ ⌶

☐ TVI-SASEMO2-Enterprise

☐ Destination Address Negate

☐ Region + ⌵ ⌶

☐ Destination Location Negate

☐ Custom Geo Circle + ⌵ ⌶

☐ Destination Address + New Address + New Address Group + ⌵ ⌶

Destination Address Not Configured

☐ Destination Address Anycast

☐ State + ⌵ ⌶

State Not Configured

☐ Destination Site Name + ⌵ ⌶

Destination Site Name Not Configured

☐ City + ⌵ ⌶

City 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: --Select-- Session Timeout (secs): ☐ Send TCP Keep Alive at Session Timeout

Profiles ☐ Profile Groups

☐ IP Filtering: --Select-- ☐ Antivirus: --Select-- ☐ File Filtering: --Select--

☐ Vulnerability: --Select-- ☐ URL Filtering: --Select-- ☐ DNS Filtering: --Select--

☐ Predefined Vulnerability Profile Override: --Select-- ☐ CASB Profile: --Select-- ☐ DLP Profile: --Select--

☐ ATP Profile: --Select-- ☐ RBI Profile: --Select--

OK **Cancel**

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

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Appliance: Branch-1-VOS Organization: SASEDEMO2

Access Policies **Rules**

Default-Policy Search

+ Add **Delete** **Clone** **Move**

Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	Source	User Defined Devices	Discovered Devices	User Defined Devices Fil
1	AccessRule-Oscar1	False										
2	Allow_From_Trust	False		Intf-LAN1-Zone								
3	Allow_From_SOWMAN	False		ptv1								
4	To-TSA	False										
5	From-TSA	False		TV1-SASEDEMO2-Enter...								
6	DenyRule-Oscar2	False										

- Name the policy

Edit Rule - From-TSA

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

Name:

Description:

Tags: Alias Name:

☐ Disable Rule

OK **Cancel**

- In the Source tab, select the “TVI-SASEMO2-Enterprise-TSA” zone assigned to TVI in SASEMO2-Enterprise-TSA routing instance.

Edit Rule - From-TSA

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

Source Zone **TVI-SASEMO2-Enterprise-TSA**

Source Address Source Address Not Configured

Source Site Name Source Site Name Not Configured

Source Address Negate

Region Region Not Configured

City City Not Configured

State State Not Configured

Source Location Negate

Custom Geo Circle Custom Geo Circle Not Configured

Scalable Group Tag Scalable Group Tag Not Configured

EIP Profiles EIP Profiles Not Configured

Managed Device ☒ Not Configured ☐ True ☐ False

Ingress Routing Instance --Select--

Egress Routing Instance --Select--

OK **Cancel**

- Allow the traffic

Edit Rule - From-TSA

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

Actions **Log**

Actions ☒ Allow ☐ Deny ☐ Reject ☐ Apply Security Profile

Synced Flow --Select-- **Session Timeout (secs)** ☐ Send TCP Keep Alive at Session Timeout

Profiles ☒ Profile Groups

☐ IP Filtering --Select-- ☐ Antivirus --Select-- ☐ File Filtering --Select--

☐ Vulnerability --Select-- ☐ URL Filtering --Select-- ☐ DNS Filtering --Select--

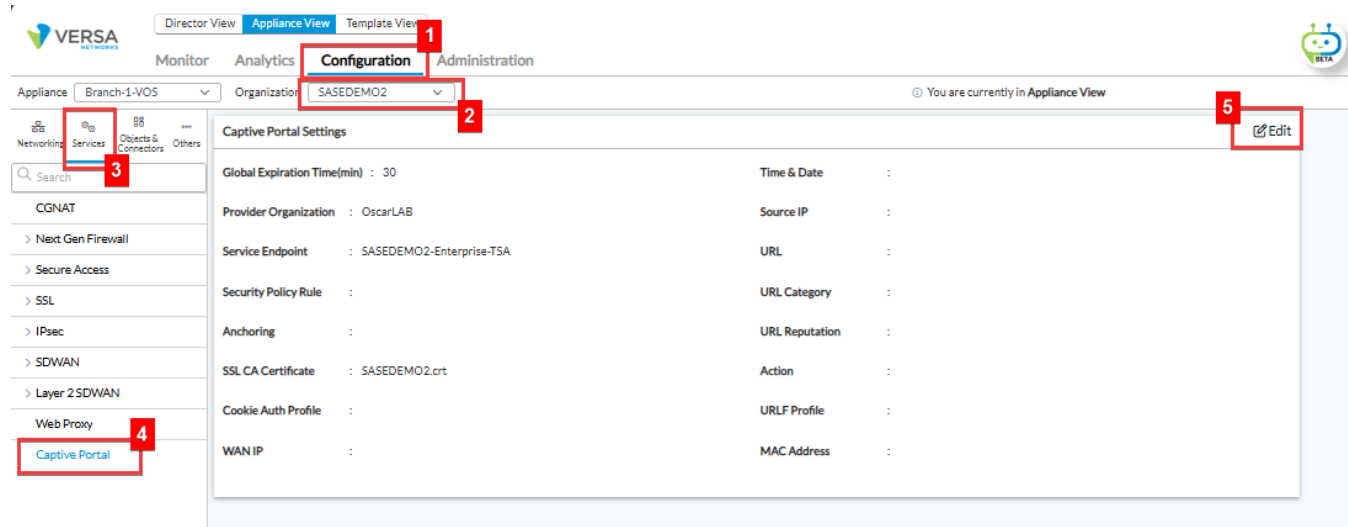
☐ Predefined Vulnerability Profile Override --Select-- ☐ CASB Profile --Select-- ☐ DLP Profile --Select--

☐ ATP Profile --Select-- ☐ RBI Profile --Select--

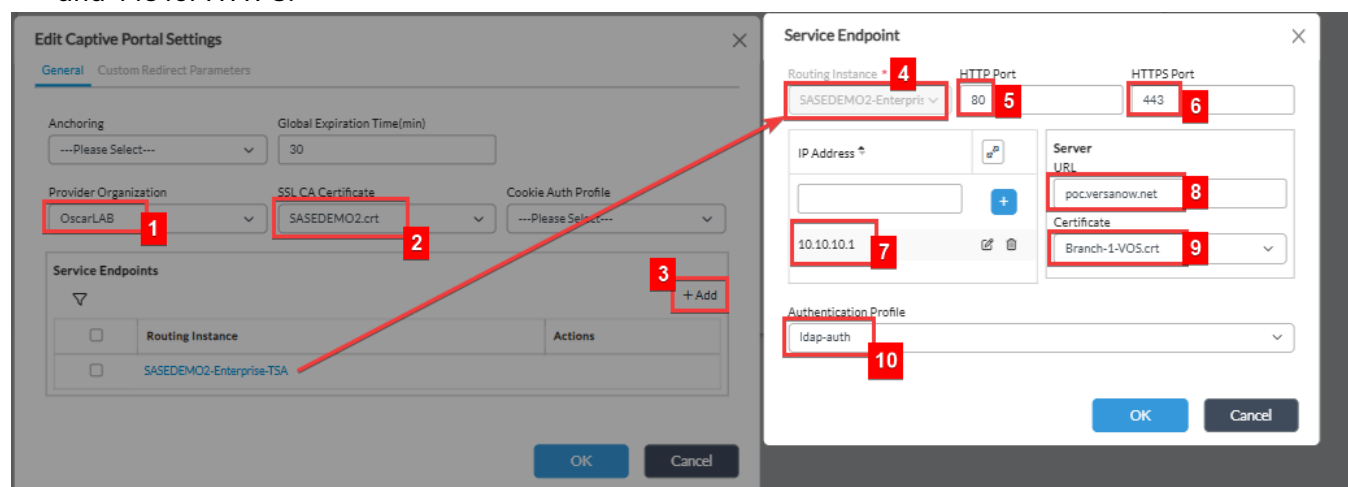
OK **Cancel**

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.

Edit Captive Portal Settings

General Custom Redirect Parameters

Anchoring: ---Please Select--- Global Expiration Time(min): 30

Provider Organization: OscarLAB SSL CA Certificate: SASEDEMO2.crt Cookie Auth Profile: ---Please Select---

Service Endpoints

Routing Instance	Actions
SASEDEMO2-Enterprise	
SASEDEMO2-Enterprise-TSA	

Service Endpoint

Routing Instance: SASEDEMO2-Enterprise

HTTP Port: 44990

HTTPS Port: 44991

IP Address: [Empty]

Server URL: [Empty]

Certificate: ---Please Select---

Authentication Profile: ---Please Select---

OK **Cancel**

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

- Add a security rule to filter the required traffic.

VERSA Director View Appliance View Template View

Monitor Analytics **Configuration** Administration

Appliance: Branch-1-VDS Organization: SASEDEMO2

Access Policies **Rules**

Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	Source	User Defined Devices	Discovered Devices	User Defined Devices Filter
1	AccessRule-Oscar1	False										
2	DenyRule-Oscar2	False										
3	Allow_From_Trust	False		Intf-LAN1-Zone								
4	Allow_From_SWAN	False		pub								

Rows per page: 25 Showing 1 - 4 of 4

- Name the rule.

Edit Rule - AccessRule-Oscar1

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

Name: AccessRule-Oscar1

Description: [Empty]

Tags: [Empty]

☐ Disable 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

<input type="checkbox"/> Destination Zone	+ New Zone +	<input type="checkbox"/> Destination Address
<input type="checkbox"/> RTI-INET-Zone		
<input type="checkbox"/> Destination Address Negate		<input type="checkbox"/> Destination Address Ar
<input type="checkbox"/> Region	+ -	<input type="checkbox"/> State
Region Not Configured		
<input type="checkbox"/> Destination Location Negate		<input type="checkbox"/> Scalable Group Tag
<input type="checkbox"/> Custom Geo Circle	+ -	
Custom Geo Circle Not Configured		

- 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

Match Users **User Group Profile**

☐ Local Database ☐ External Database

☐ Users ☐ Groups

☐ oscar1

+ New Custom User

Add Custom User

Name *
oscar1

User Principle Name *
oscar1@canaleros.local

OK Cancel

- 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 | Log

Actions 1

☒ Allow ☐ Deny ☐ Reject ☐ Apply Security Profile

Synced Flow: --Select-- Session Timeout (secs): --Select-- ☐ Send TCP Keep Alive at Session Timeout

Profiles ☐ Profile Groups

☐ IP Filtering --Select-- ☐ Antivirus --Select-- ☐ File Filtering --Select--

☐ Vulnerability --Select-- ☐ URL Filtering --Select-- ☐ DNS Filtering --Select--

☐ Preddefined Vulnerability Profile Override --Select-- ☐ CASB Profile --Select-- ☐ DLP Profile --Select--

☐ ATP Profile --Select-- ☐ RBI Profile --Select--

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: Selected Users Groups User Group Profile: ActiveDirectory

☐ Local Database

☐ Users **+ New Custom User** +

☐ oscar2

Add Custom User X

Name *
oscar2

User Principle Name *
oscar2@canaleros.local

OK **Cancel**

Policies

Profiles

Profile Groups

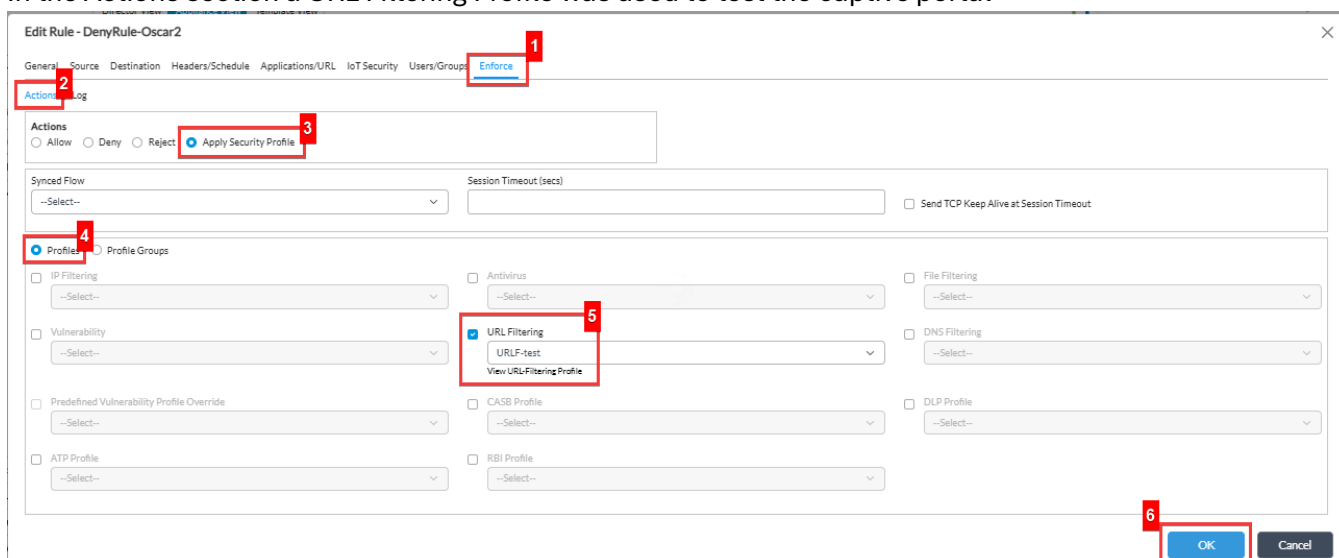
CASB Constraint

Security Settings

Microsegmentation

Rows per page: 25 Showing 1 - 4 of 4

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



Edit Rule - DenyRule-Oscar2

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

Actions Log

☐ Allow
 ☐ Deny
 ☐ Reject
 ☒ **Apply Security Profile**

Synced Flow: --Select--
 Session Timeout (secs):
 ☐ Send TCP Keep Alive at Session Timeout

Profiles Profile Groups

<input type="checkbox"/> IP Filtering --Select--	<input type="checkbox"/> Antivirus --Select--	<input type="checkbox"/> File Filtering --Select--
<input type="checkbox"/> Vulnerability --Select--	<input checked="" type="checkbox"/> URL Filtering URLF-test View URL Filtering Profile	<input type="checkbox"/> DNS Filtering --Select--
<input type="checkbox"/> Predefined Vulnerability Profile Override --Select--	<input type="checkbox"/> CASB Profile --Select--	<input type="checkbox"/> DLP Profile --Select--
<input type="checkbox"/> ATP Profile --Select--	<input type="checkbox"/> RBI Profile --Select--	

OK Cancel

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.

The screenshot shows a Notepad window with the hosts file content and a Service Endpoint configuration window. A red arrow points from the IP address 10.10.10.1 in the hosts file to the IP Address field in the Service Endpoint configuration window.

hosts - Notepad

```
#
# 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.
#
#       ::1               localhost
#       172.16.100.0      captiveportal.versaow.net
#       10.10.10.1        poc.versaow.net
```

Service Endpoint

Routing Instance: SASEMO2-Enterprise

HTTP Port: 80

HTTPS Port: 443

IP Address: 10.10.10.1

Server URL: poc.versaow.net

Certificate: Branch-1-VOS.crt

Authentication Profile: ldap-auth

OK Cancel

The screenshot shows the Versa Director Appliance View. The configuration of the tvI-0/771.0 interface is highlighted in red.

VERSA

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Administration

Organization: SASEMO2

Summary | Devices | Cloud Workload

Total Appliances: 5 | Branch-1-VOS

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 t
<input type="checkbox"/>	tvI-0/771	up	up	SASEMO2-Enterprise-T...	N/A	n/a	3	-
<input type="checkbox"/>	tvI-0/771.0	up	up	SASEMO2-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



Refresh

Connected

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

Version: 7.1.1

© 2023 Versa Networks | All rights reserved

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

Director View
Appliance View
Template View

Monitor
Analytics
Configuration
Administration

Organization: SASEDEMO2
You are currently in Appliance View

Total Appliances: 6
Branch-1-VOS

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
Conf

SDWAN
NGFW
CGNAT
Secure Access
SDLAN
IPsec
Sessions
SCI
APM
VMS

Antivirus
ATP
Authentication Policies
CASB
Cloud File Export
Decryption
DLP
DNS Filtering
DoS Policies
Entity Risk Score
File Filtering
IP Filtering
Microsegmentation Policies
Microsegmentation Statistics
Persistent Action

Live Users
Brief

IP Address

Name

Status

Session Hits

Time To Expiry

Expiration Mode

192.168.15.15
tsa-multiuser
Live
78849
60
inactivity

Username

User ID

Group ID

Port Range

Login Timestamp

admin@canaleros.local
0
10200-10299,11200-11299
2025-07-13 21:11:43

administrator@canaleros.local
0
10700-10799,10300-10399
2025-07-13 21:11:43

local.service@nt.authority
0
10500-10599
2025-07-13 21:11:43

network.service@nt.authority
0
10100-10199
2025-07-13 21:11:43

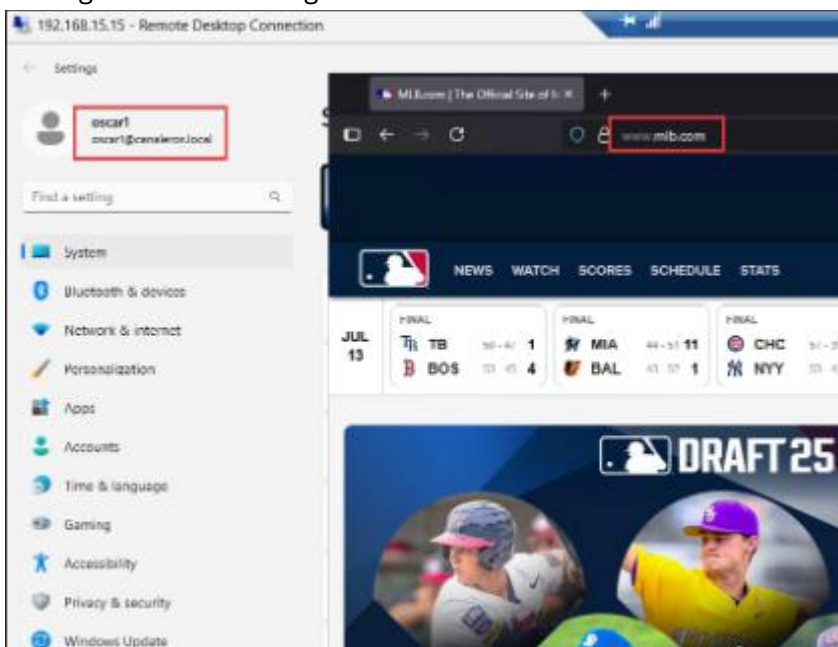
oscar1@canaleros.local
8192
11100-11199,10400-10499
2025-07-13 21:11:43

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.

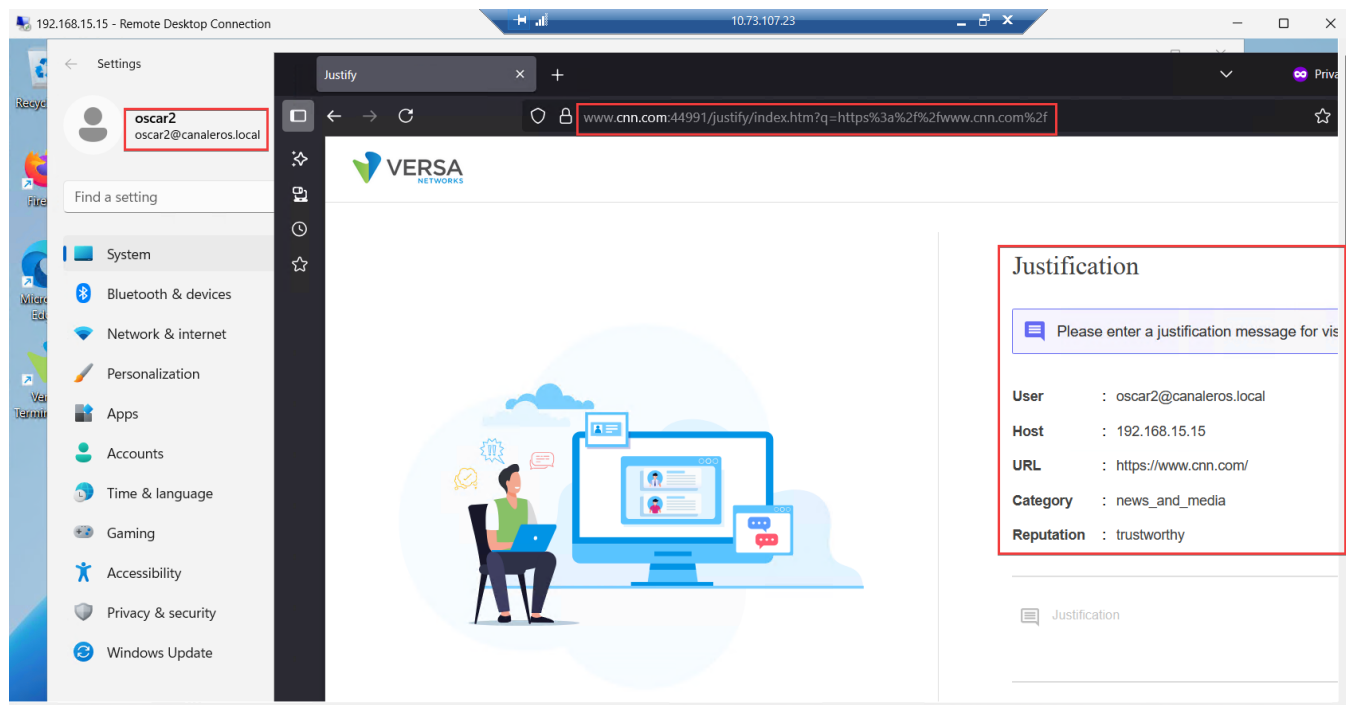


- In this output from the SD-WAN branch device, we can see the session of the internet webpage tested and the traffic being allowed by the policy created for user “oscar1”

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/(predef)	AccessRule-Oscar1	192.168.15.15	151.101.41.91	TCP	10492	443	3.968	4.128
mlb_com/(predef)	AccessRule-Oscar1	192.168.15.15	151.101.41.91	TCP	10408	443	4.933	3.784
mlb_com/(predef)	AccessRule-Oscar1	192.168.15.15	151.101.41.91	TCP	10427	443	4.943	3.792
adobe/(predef)	AccessRule-Oscar1	192.168.15.15	23.44.73.62	TCP	10420	443	3.518	6.111
mlb_com/(predef)	AccessRule-Oscar1	192.168.15.15	151.101.41.60	TCP	10476	443	5.451	16.788
mlb_com/(predef)	AccessRule-Oscar1	192.168.15.15	151.101.41.91	TCP	11140	443	25.125	2651.826
mlb_com/(predef)	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.

VERSA NETWORKS

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Administration

Session Filter

Session Search Criteria

Session Type: --Select-- | Source IP/Prefix: | Source Port: | Destin: |

Protocol: Protocol | Protocol Number: |

Extensive | Compare selected records

	Application	Rule	Source IP	Destination IP	Protocol	Source Port	Destination Port	Forward Byte Count	Reverse Byte Count	Re
<input type="checkbox"/>	> Unknown		10.30.0.9	10.30.0.0	TCP	1226	1234	0	9630.18	
<input type="checkbox"/>	> msnp/(predef)	Allow_From_Trust	192.168.15.10	20.59.87.226	TCP	65304	443	10.775	13.892	
<input type="checkbox"/>	> unknown_tcp/pre...		192.168.15.15	192.168.20.10	TCP	3389	53518	349.781	53.211	
<input type="checkbox"/>	> msnp/(predef)	Allow_From_Trust	192.168.15.15	20.59.87.225	TCP	10126	443	10.817	13.894	
<input type="checkbox"/>	> websocket/(predef)	Allow_From_Trust	192.168.15.15	10.10.10.1	TCP	10124	443	4.346	6.502	
<input 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 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](#).