VERSA

IMPLEMENTATION GUIDE

Versa Trusted Network Detection (TND) Gateway Assisted

About This Document

This document outlines the use case, benefits, and deployment considerations for Trusted Network Detection (TND) – Gateway-Assisted, a capability of Versa Secure Access (part of the Versa SASE architecture). It is intended for environments where users connect via the Versa SASE client from trusted enterprise locations—typically corporate branches—where routing traffic through the SASE client tunnel is unnecessary due to existing secure connectivity (via SD-WAN or IPsec) to the Versa cloud gateway

Document Information

Title	**Versa Trusted Network Detection (TND) Gateway Assisted**
Author	Versa Professional Services
Version	V 1.0

Disclaimer

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

What is Trusted Network Detection (TND) Gateway-Assisted?

Trusted Network Detection (TND) Gateway-Assisted enables the Versa SASE client to bypass tunnel creation when operating within a trusted network. This approach is ideal for scenarios where the internal network already has a secure connection to the Versa SASE gateway via SD-WAN or IPsec.

In standard SASE deployments, the Versa client establishes a secure tunnel (typically IPsec) to the SASE gateway to enforce user-specific security policies. However, when the client is behind a trusted network—such as a corporate office with an existing secure connection—this tunnel becomes redundant.

TND Gateway-Assisted ensures:

- A secure control channel is maintained with the SASE gateway.
- Continuous posture evaluation and user identification.
- Policy enforcement based on user and group identity.

This method leverages the existing site-to-site tunnel to the Versa cloud gateway, eliminating the need for additional configuration or tunnel establishment from the client.

TND Detection Flow: Trusted vs. Untrusted Network

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

User on the Internet (Untrusted Network)

- The SASE client resolves the SASE Gateway FQDN to a public IP address.
- The client sends registration data (e.g., MAC address, IP address) to the gateway.
- The SASE Gateway responds with a trusted network = false flag.
- The client proceeds to establish an IPsec tunnel to the gateway.
- Traffic is routed through the tunnel based on the defined routing policies.

User in a Trusted Network (e.g., Corporate Branch)

- The SASE client resolves the SASE Gateway FQDN to a private IP address (via DNS proxy or local DNS).
- The client sends registration data to the gateway.
- The SASE Gateway responds with a trusted network = true flag.
- The client suppresses tunnel creation.
- The gateway continues to enforce user-based policies, session tracking, and posture checks over the control channel (HTTPS).

Key Benefits

- **Tunnel Bypass in Trusted Networks**: Automatically suppresses tunnel creation when the client detects it is within a trusted network.
- **Efficient Policy Enforcement**: Maintains user session tracking, posture validation, and policy enforcement at the SASE gateway without requiring an active tunnel.
- **Reduced Overhead**: Minimizes unnecessary traffic routing and improves performance by avoiding redundant encryption and tunneling.
- **Seamless User Experience**: Simplifies client behavior while preserving security and visibility.

Versa TND Scenarios

1. SD-WAN Branch with Overlay to SSE Gateway

- The branch is part of a Versa SD-WAN fabric with an existing overlay tunnel to the SSE Gateway.
- TND allows the SASE client to bypass tunnel creation while still enabling user identification and policy enforcement at the SSE gateways.
- This ensures complete visibility and control over user traffic from SD-WAN-connected sites to SSE gateways and traffic steering can be applied at SDWAN branches.
- Passive authentication servers are not required, as the gateway receives the user identity directly from the client. (Provided the user identification is not necessary on the SDWAN branch, then VMS becomes mandatory.)

2. Site-to-Site IPsec Tunnel to SSE Gateway (SWG Use Case)

- The customer uses a site-to-site IPsec tunnel from the branch to the SSE Gateway for secure internet access (SWG).
- TND ensures that user identity and posture are enforced at the SSE gateways, even though traffic is routed through the IPsec tunnel.
- Like the SD-WAN case, this approach removes the need for passive authentication, streamlining operations and improving policy accuracy.

TND Deployment Scenarios

In the following sections, we will demonstrate two deployment scenarios:

- **TND with Customer Private DNS**
- **TND with DNS Proxy on SSE Gateway**

These examples illustrate how to configure trusted network detection based on DNS resolution behaviour.

TND with Customer Private DNS

In this use case, a user device located in a branch office connects to the Versa SASE infrastructure through an Overlay or Site-to-Site IPsec tunnel. All traffic, except for DNS queries, is routed through the SASE Gateway (SASEGW) for inspection, control, and identity-based access.

How It Works

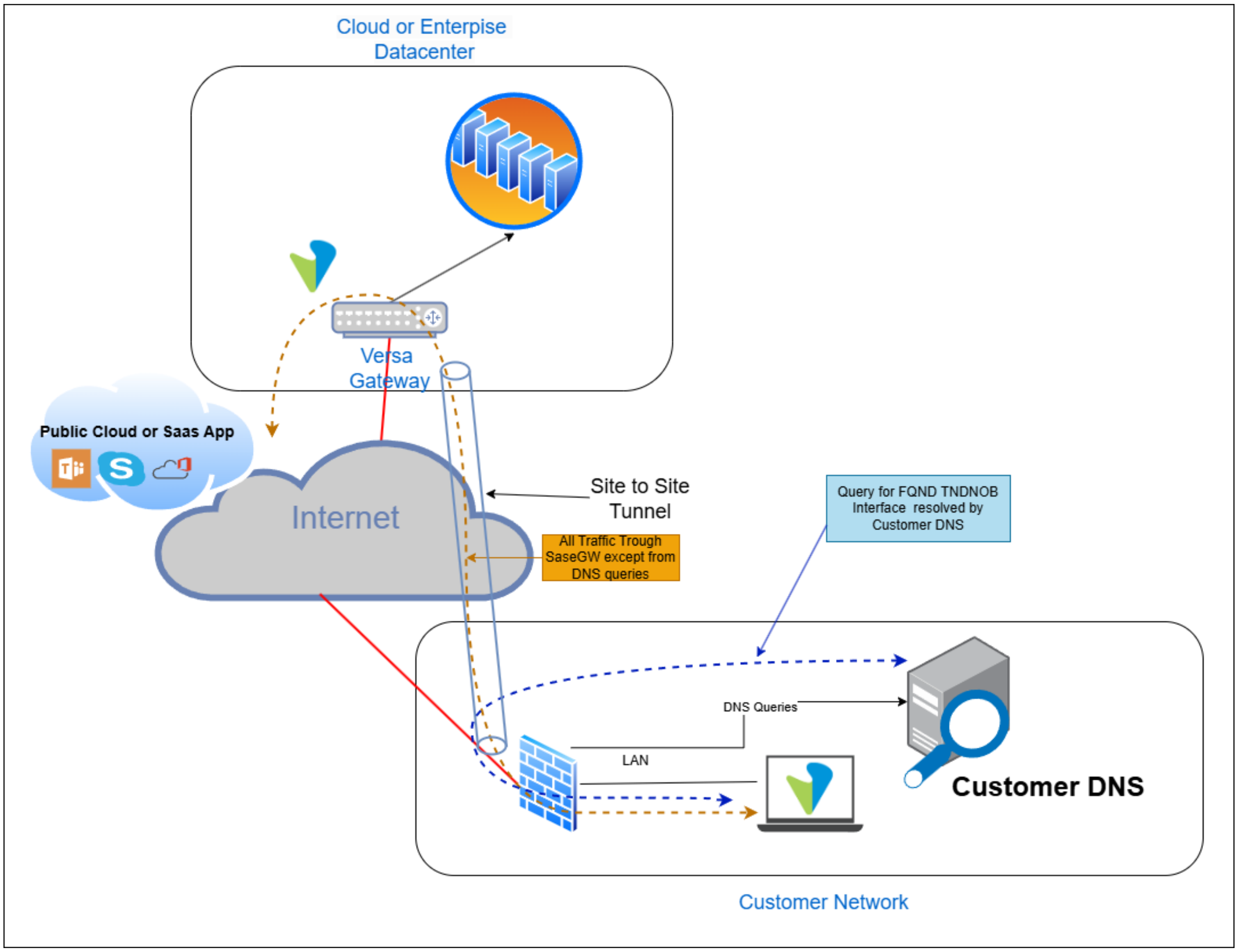
1. The Local DNS servers are configured to resolve the SASE Gateway FQDN to the private IP of the TNDNOB TVI Interface on the Gateway.
2. The SASE Client on the user device attempts to register with the SASE Gateway.
3. The client resolves the SASE Gateway FQDN.
4. The customer's private DNS server resolves the FQDN to a **private IP address**.
5. The client connects to the gateway using this private IP.
6. The gateway responds with a trusted network = true flag, and the client bypasses tunnel creation.
7. Finally, the user can register and connect normally, and the Versa SASE Client should automatically detect the network and display "Trusted Network Identified" and "Tunnel bypassed."
8. Posture validation and policy enforcement continue over the control channel (HTTPS).

NOTE: The internal customer’s DNS infrastructure handles all DNS queries.

Key Requirement

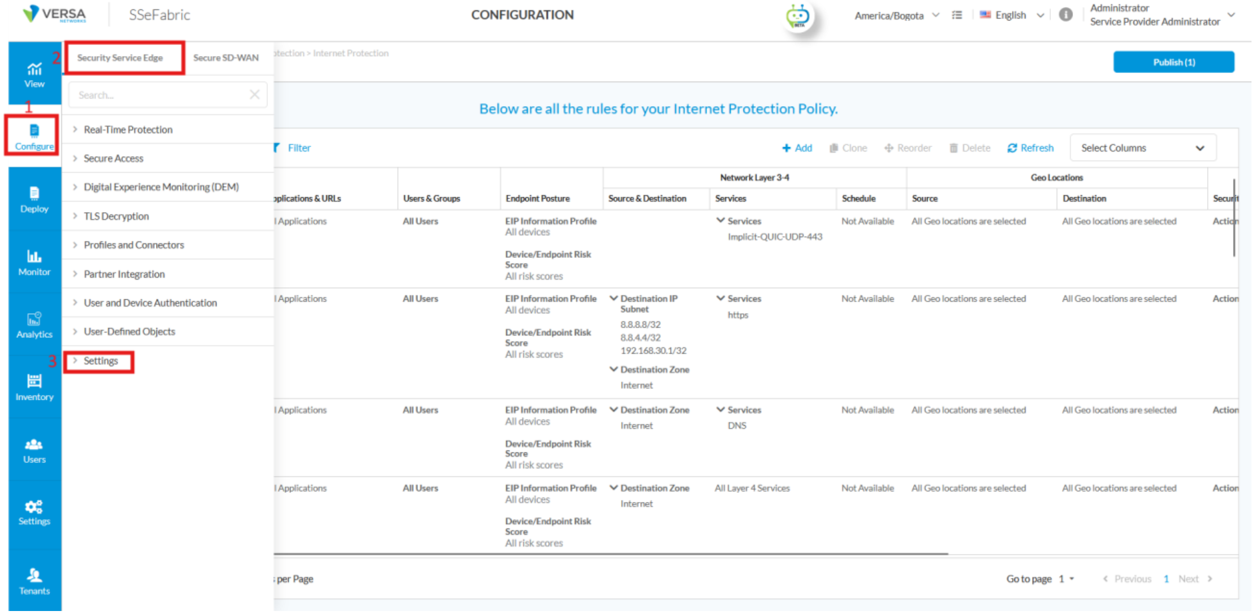
The client's DNS infrastructure must be able to resolve the portal registration domains to the private IP address of the TNDNOB interface.

Topology


Cloud or Enterprise Datacenter
Versa Gateway
Public Cloud or Saas App
Internet
Site to Site Tunnel
All Traffic Trough SaseGW except from DNS queries
Query for FQND TNDNOB Interface resolved by Customer DNS
DNS Queries
LAN
Customer DNS
Customer Network

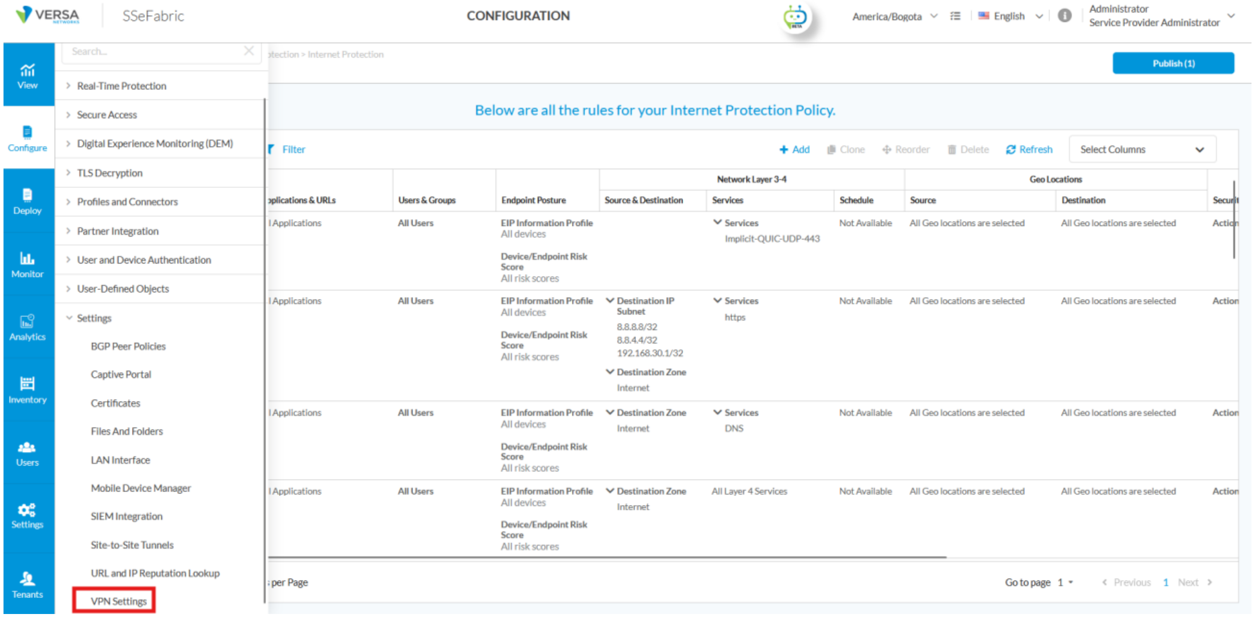
Configuration Steps

1. **Concerto portal:** Configure > Security Service Edge > Settings > VPN Settings >



Below are all the rules for your Internet Protection Policy.

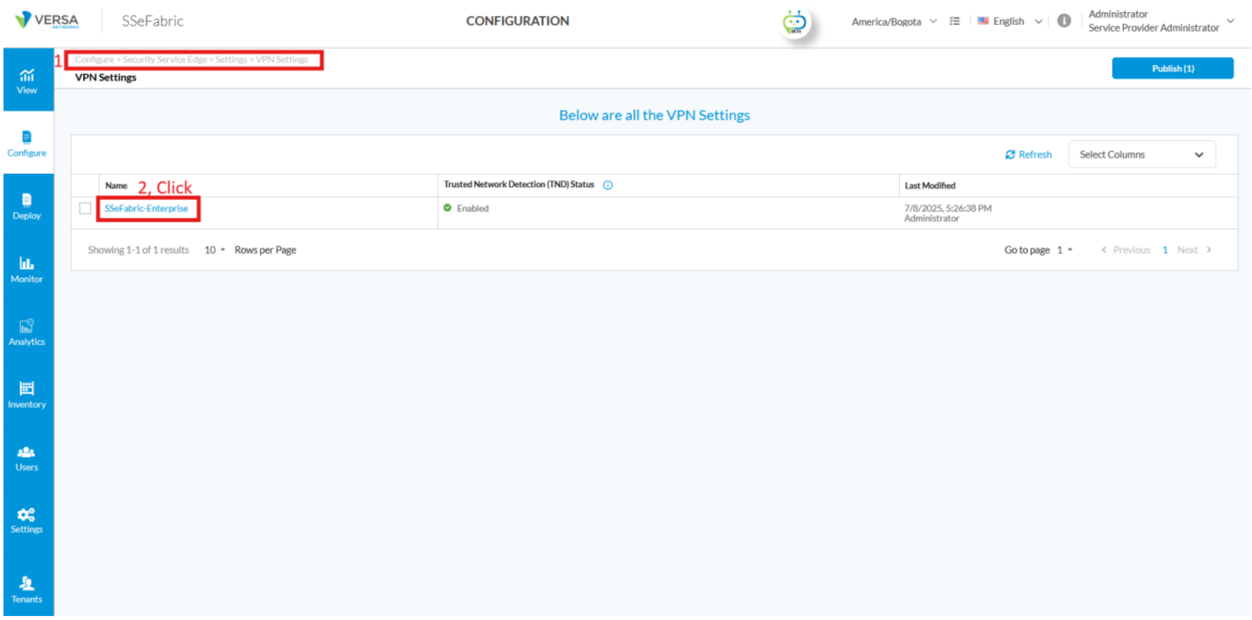
			Network Layer 3-4			Geo Locations		
pplications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Securi
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Actio
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination IP Subnet 8.8.8.8/32 8.8.4.4/32 192.168.30.1/32 Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	Services DNS	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action



Below are all the rules for your Internet Protection Policy.

			Network Layer 3-4			Geo Locations		
pplications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Securi
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Actio
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination IP Subnet 8.8.8.8/32 8.8.4.4/32 192.168.30.1/32 Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	Services DNS	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action

- Select the VPN name



1 Configure > Security Service Edge > Settings > VPN Settings

VPN Settings

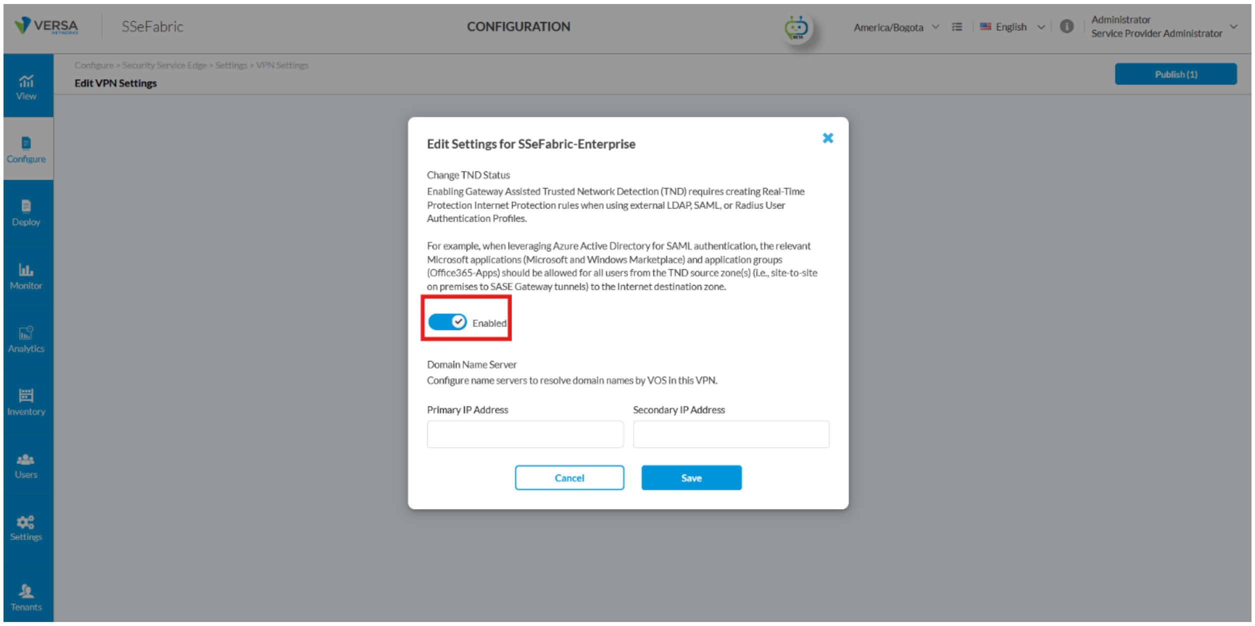
Below are all the VPN Settings

Name 2, Click	Trusted Network Detection (TND) Status	Last Modified
SSeFabric-Enterprise	Enabled	7/8/2025, 5:26:38 PM Administrator

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

- Enable the Knob and Save.

Note: To use TND, it is **not mandatory** to enter the **Primary IP Address** or **Secondary IP Address**. These fields are used when you want to add a **DNS server** to the **system settings** of the SASE Gateway, possibly to use it in **DNS Proxy rules** and enable internal domain resolution using those servers as relays.



Configure > Security Service Edge > Settings > VPN Settings

Edit VPN Settings

Edit Settings for SSeFabric-Enterprise

Change TND Status

Enabling Gateway Assisted Trusted Network Detection (TND) requires creating Real-Time Protection Internet Protection rules when using external LDAP, SAML, or Radius User Authentication Profiles.

For example, when leveraging Azure Active Directory for SAML authentication, the relevant Microsoft applications (Microsoft and Windows Marketplace) and application groups (Office365-Apps) should be allowed for all users from the TND source zone(s) (i.e., site-to-site on premises to SASE Gateway tunnels) to the Internet destination zone.

Enabled

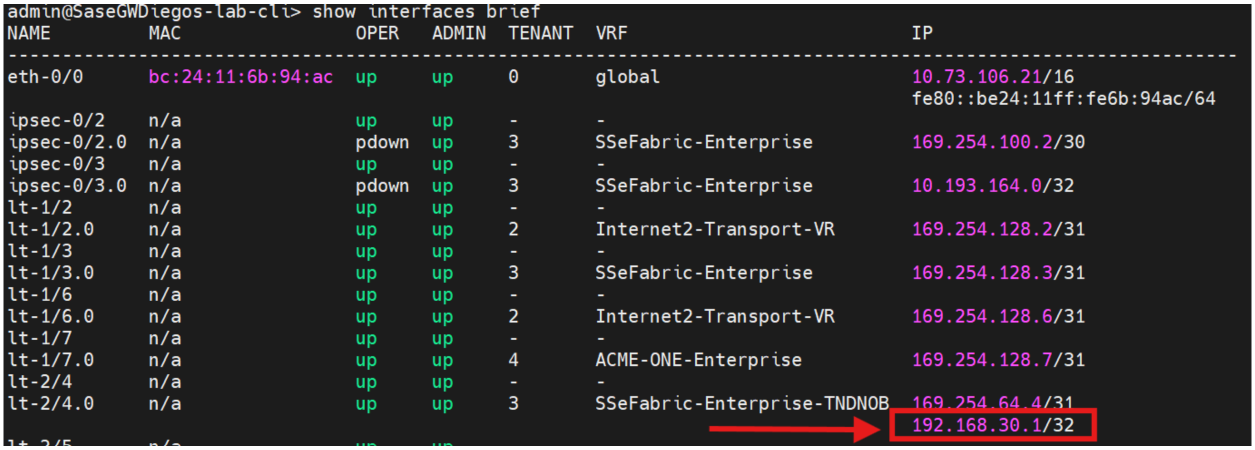
Domain Name Server

Configure name servers to resolve domain names by VOS in this VPN.

Primary IP Address

Secondary IP Address

- **Remarks:** Although you were not explicitly requested to publish the TND status, you must still go to **Publish** and complete the action.
- **Identify TNDNOB TVI IP:** On the SASE Gateway, run the command "*show interfaces brief | tab*"



```
admin@SaseGWDiegos-lab-cli> show interfaces brief
NAME         MAC                OPER   ADMIN  TENANT  VRF                          IP
--------------------------------------------------------------------------------------------------------------------
eth-0/0      bc:24:11:6b:94:ac  up     up     0       global                       10.73.106.21/16
                                                                                   fe80::be24:11ff:fe6b:94ac/64

ipsec-0/2    n/a                up     up     -       -
ipsec-0/2.0  n/a                pdown  up     3       SSeFabric-Enterprise         169.254.100.2/30
ipsec-0/3    n/a                up     up     -       -
ipsec-0/3.0  n/a                pdown  up     3       SSeFabric-Enterprise         10.193.164.0/32
lt-1/2       n/a                up     up     -       -
lt-1/2.0     n/a                up     up     2       Internet2-Transport-VR       169.254.128.2/31
lt-1/3       n/a                up     up     -       -
lt-1/3.0     n/a                up     up     3       SSeFabric-Enterprise         169.254.128.3/31
lt-1/6       n/a                up     up     -       -
lt-1/6.0     n/a                up     up     2       Internet2-Transport-VR       169.254.128.6/31
lt-1/7       n/a                up     up     -       -
lt-1/7.0     n/a                up     up     4       ACME-ONE-Enterprise          169.254.128.7/31
lt-2/4       n/a                up     up     -       -
lt-2/4.0     n/a                up     up     3       SSeFabric-Enterprise-TNDNOB  169.254.64.4/31
                                                                                   192.168.30.1/32
lt-2/5       n/a                up     up
```

- Now, the Customer should create DNS entries for the FQDN portal domains using the TND-NOB interface ip (private ip). (example below).
  DNS A record entry: *sse-demo.versanow.net > 192.168.30.1*

It is important to mention that Versa assigns for TND the first IP address from the ***"Client Address Pool"*** *that was defined during the tenant creation.*

TND with DNS Proxy on SSE Gateway

In this use case, a user device located in a branch office connects to the Versa SASE infrastructure through an Overlay or Site-to-Site IPsec tunnel. All traffic, including DNS queries, is routed through the SASE Gateway (SASEGW) for inspection, control, and identity-based access.

How It Works

1. The SASE Client on the user device attempts to register with the SASE Gateway.

2. The client resolves the SASE Gateway FQDN. Since all DNS traffic is routed through the SSE Gateway, the gateway intercepts the DNS query.

3. Acting as an DNS proxy, the SASE Gateway resolves the FQDN to a private IP address.

4. When TND is enabled, DNS records are automatically created in the DNS Proxy profile on SSE gateways. Therefore, the only requirement is to ensure that user DNS traffic is routed to the SASE Gateway, so it can resolve domains to the IP address of the TNDNOB interface.
5. The client connects to the gateway using this private IP.

6. The gateway responds with a trusted network = true flag and the client bypasses tunnel creation.

7. Finally, the user can register and connect normally, and the Versa SASE Client should automatically detect the network and display "Trusted Network Identified" and "Tunnel bypassed."

8. Posture validation and policy enforcement continue over the control channel (HTTPS).

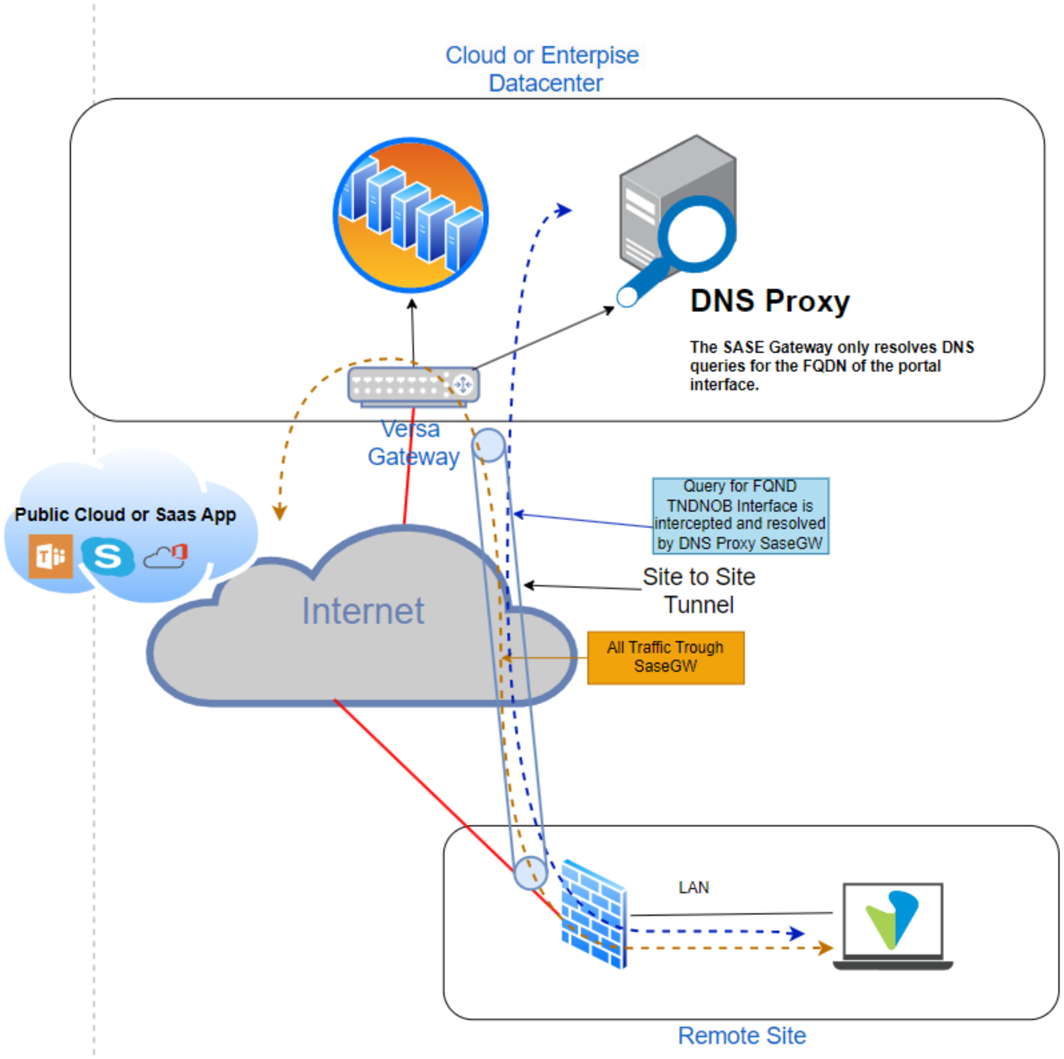
9. Since all DNS queries will come to SSE Gateway, we need to configure DNS proxy to handle private apps and public URL resolution effectively.

   NOTE: In condition where branches are SDWAN, DNS proxy can be applied at each branch level to handle portal fqdn resolution and direct other DNS queries to customer DNS server without the need of sending DNS queries to SSE gateway.

Key Requirement

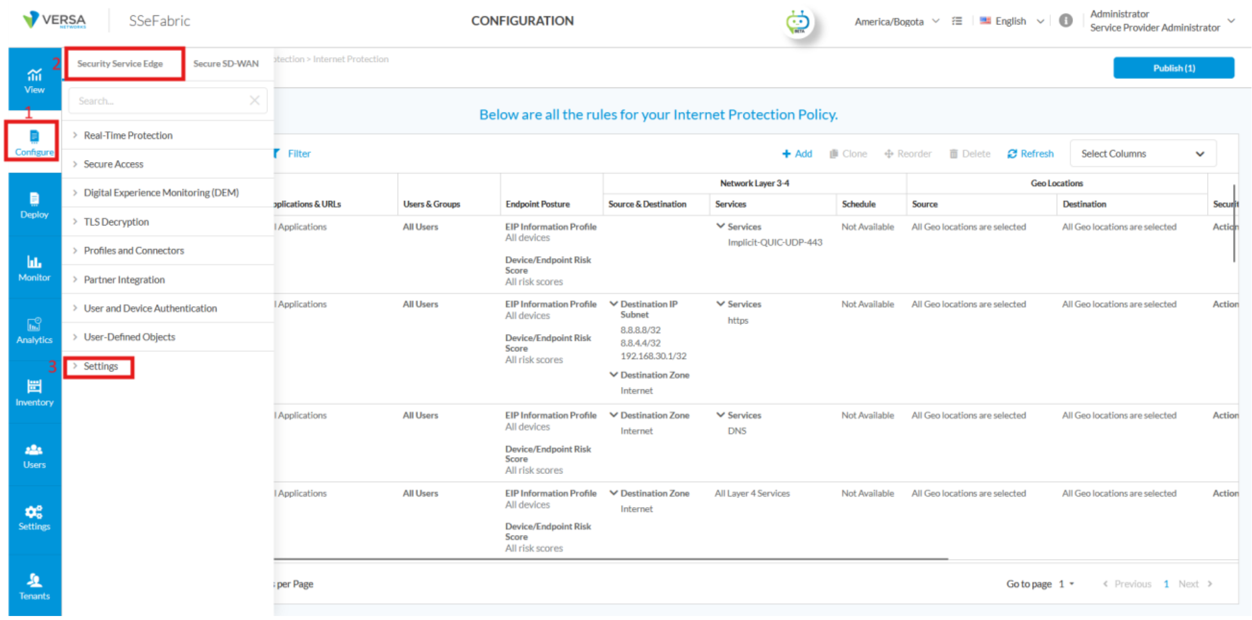
NOTE: All DNS queries from the customer network must be routed through the SSE Gateway to enable DNS interception and trusted network detection.

Topology

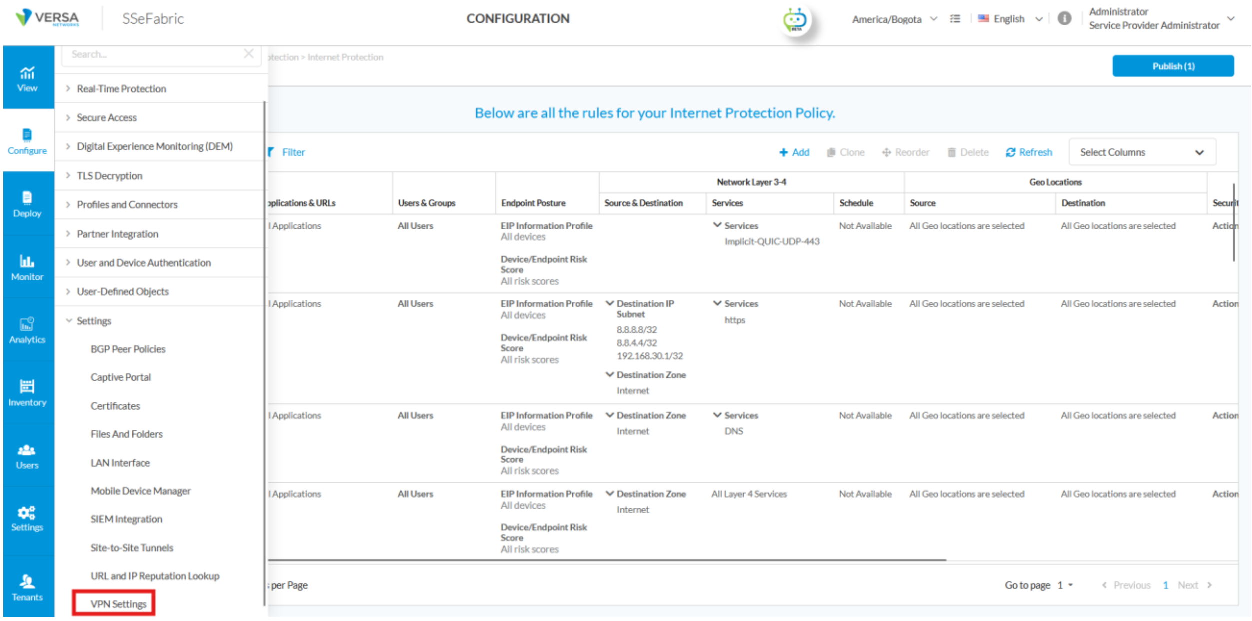

Cloud or Enterprise Datacenter
DNS Proxy
The SASE Gateway only resolves DNS queries for the FQDN of the portal interface.
Versa Gateway
Public Cloud or Saas App
Query for FQND TNDNOB Interface is intercepted and resolved by DNS Proxy SaseGW
Site to Site Tunnel
Internet
All Traffic Trough SaseGW
LAN
Remote Site

Configuration Steps

1. **Concerto portal:** Configure > Security Service Edge > Settings > VPN Settings >

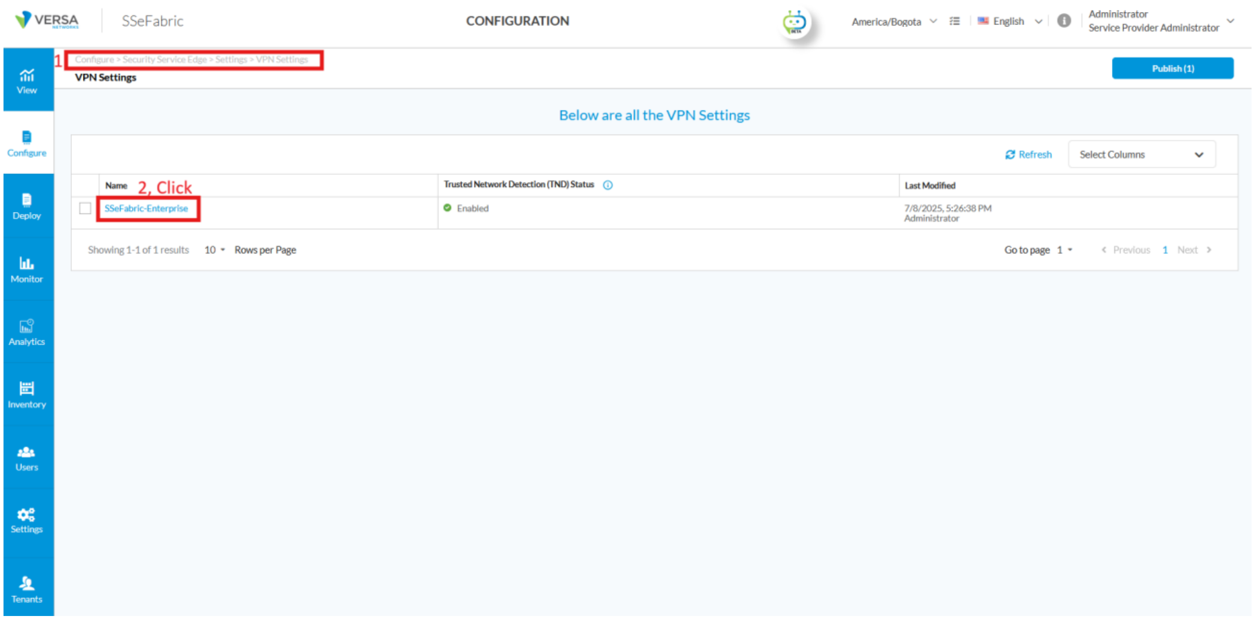


			Network Layer 3-4			Geo Locations		
pplications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Securit
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Actio
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination IP Subnet 8.8.8.8/32 8.8.4.4/32 192.168.30.1/32 Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	Services DNS	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action



			Network Layer 3-4			Geo Locations		
pplications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Securit
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Actio
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination IP Subnet 8.8.8.8/32 8.8.4.4/32 192.168.30.1/32 Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	Services DNS	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action

- Select the VPN name



Configure > Security Service Edge > Settings > VPN Settings

VPN Settings

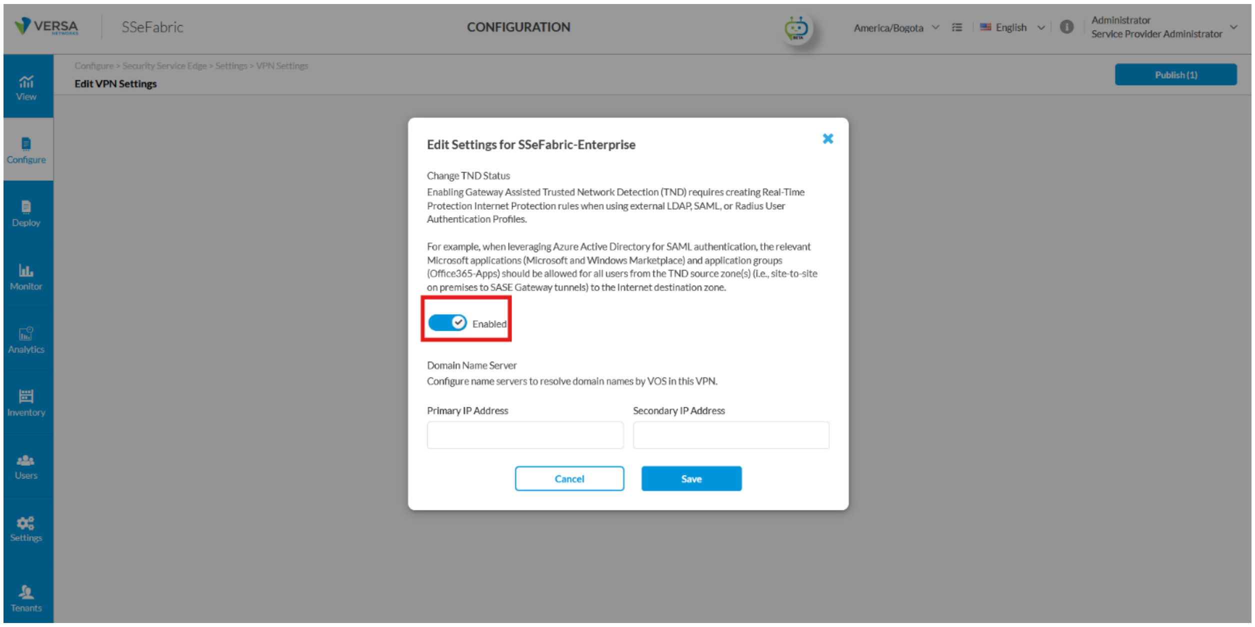
Below are all the VPN Settings

	Name	Trusted Network Detection (TND) Status	Last Modified
□	SSeFabric-Enterprise	Enabled	7/8/2025, 5:26:38 PM Administrator

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

- Enable the Knob and Save.

Note: To use TND, it is **not mandatory** to enter the **Primary IP Address** or **Secondary IP Address**. These fields are used when you want to add a **DNS server** to the **system settings** of the SASE Gateway, possibly to use it in **DNS Proxy rules** and enable internal domain resolution using those servers as relays.



Configure > Security Service Edge > Settings > VPN Settings

Edit VPN Settings

Edit Settings for SSeFabric-Enterprise

Change TND Status

Enabling Gateway Assisted Trusted Network Detection (TND) requires creating Real-Time Protection Internet Protection rules when using external LDAP, SAML, or Radius User Authentication Profiles.

For example, when leveraging Azure Active Directory for SAML authentication, the relevant Microsoft applications (Microsoft and Windows Marketplace) and application groups (Office365-Apps) should be allowed for all users from the TND source zone(s) (i.e., site-to-site on premises to SASE Gateway tunnels) to the Internet destination zone.

Enabled

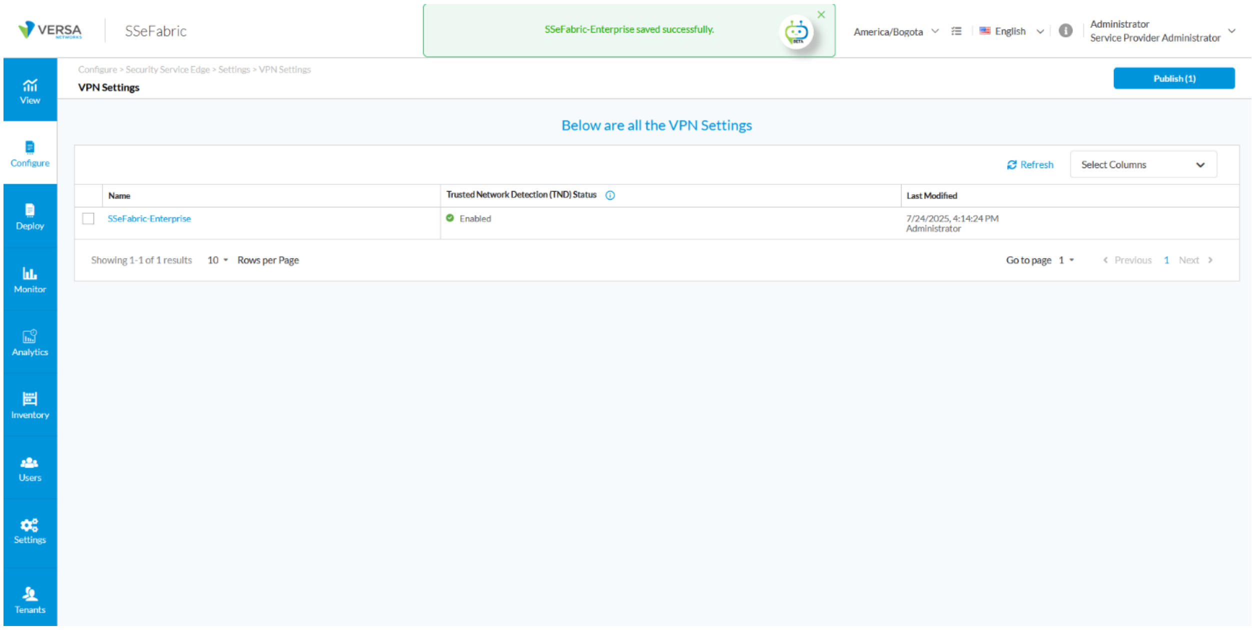
Domain Name Server

Configure name servers to resolve domain names by VOS in this VPN.

Primary IP Address

Secondary IP Address

- **Remarks:** Although you were not explicitly requested to publish the TND status, you must still go to **Publish** and complete the action.



SSeFabric-Enterprise saved successfully.

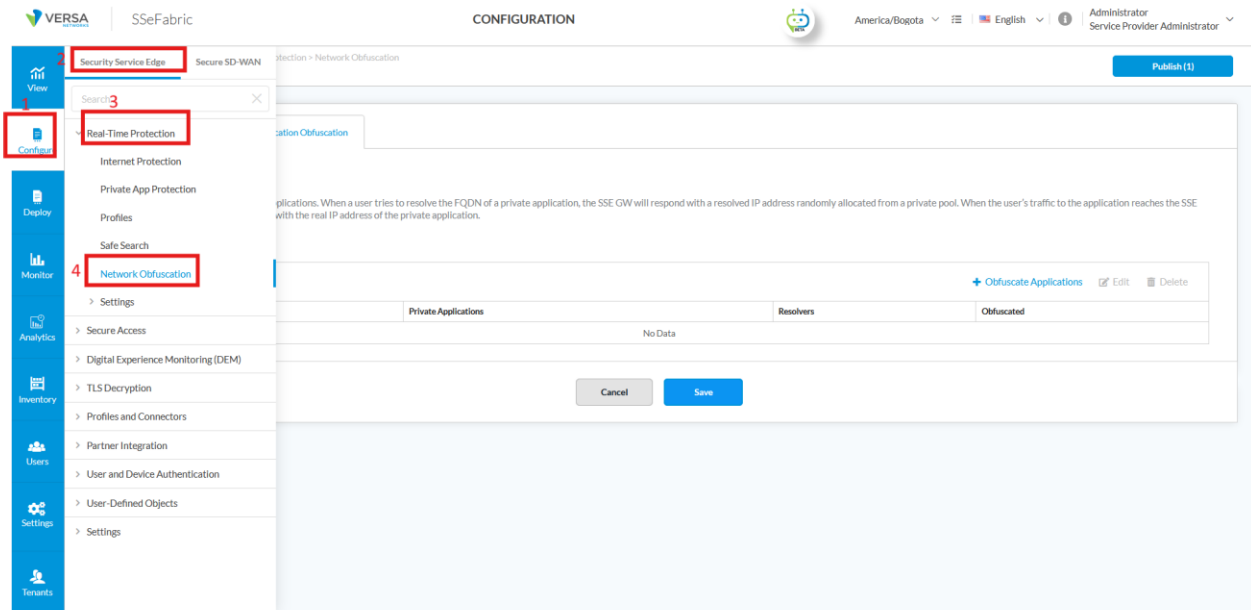
VPN Settings

Below are all the VPN Settings

Name	Trusted Network Detection (TND) Status	Last Modified
SSeFabric-Enterprise	Enabled	7/24/2025, 4:14:24 PM Administrator

2. **DNS Proxy for Private FQDN resolution:** Steps to handle Private apps and Public URL Resolution with DNS Proxy (As required)

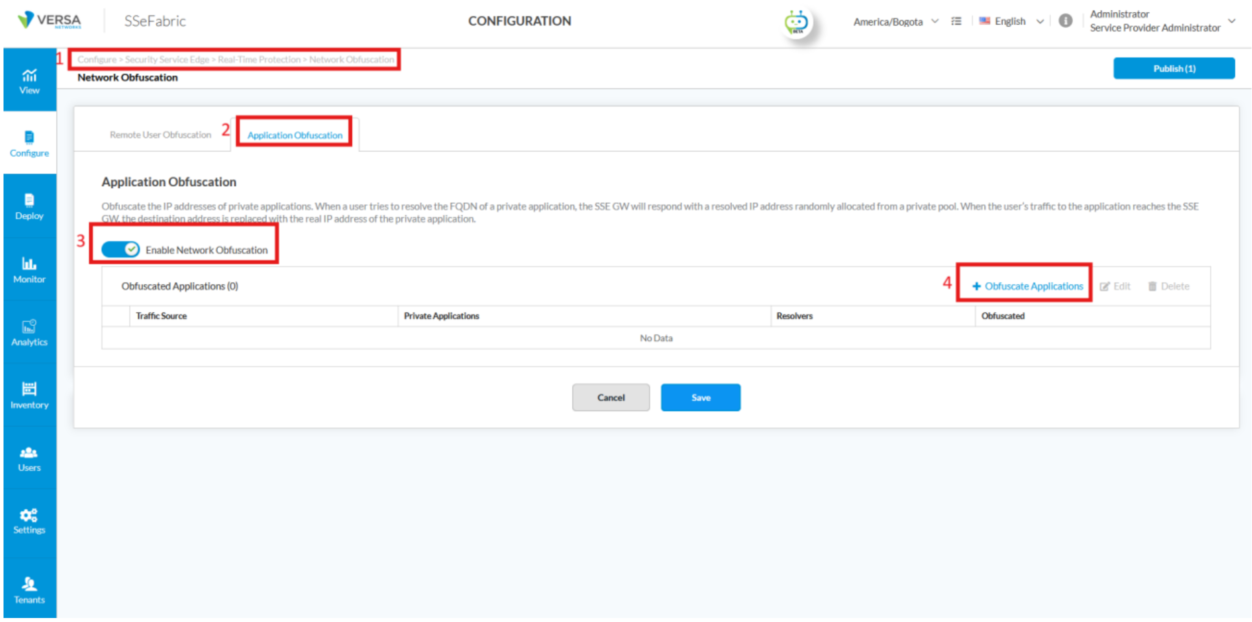
- DNS proxy configuration steps to handle private and public app URL resolution.



plications. When a user tries to resolve the FQDN of a private application, the SSE GW will respond with a resolved IP address randomly allocated from a private pool. When the user's traffic to the application reaches the SSE with the real IP address of the private application.

Private Applications	Resolvers	Obfuscated
No Data		

- Click “+ Obfuscate Applications”



Network Obfuscation

Application Obfuscation

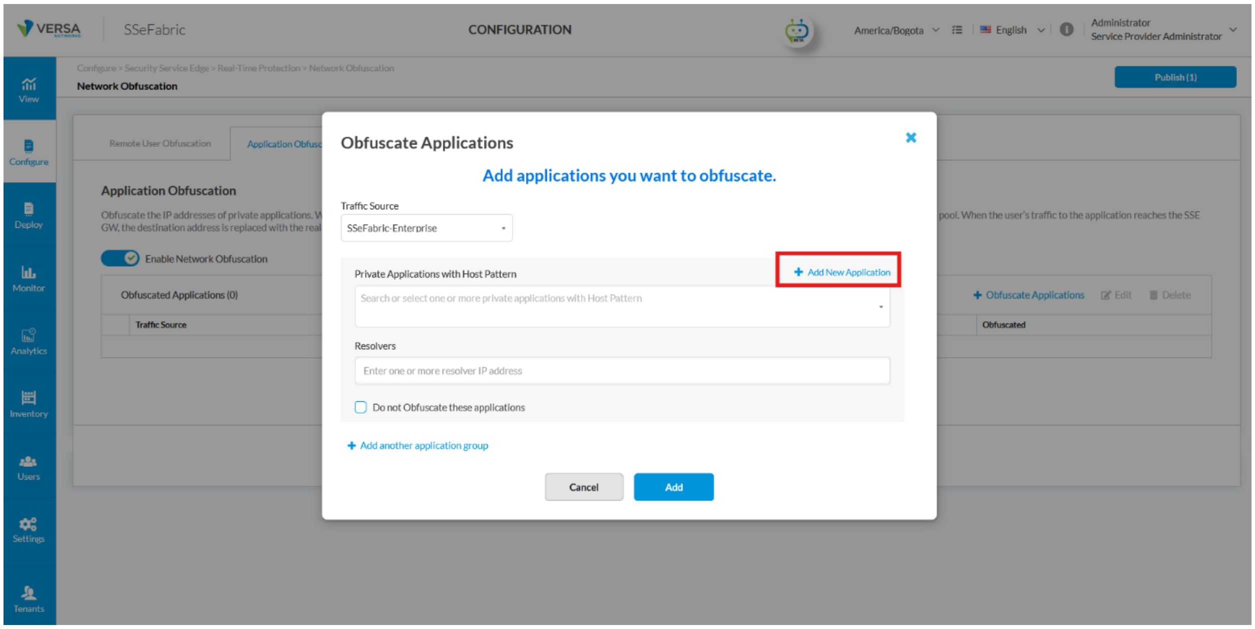
Obfuscate the IP addresses of private applications. When a user tries to resolve the FQDN of a private application, the SSE GW will respond with a resolved IP address randomly allocated from a private pool. When the user's traffic to the application reaches the SSE GW, the destination address is replaced with the real IP address of the private application.

Enable Network Obfuscation

Obfuscated Applications (0)

Traffic Source	Private Applications	Resolvers	Obfuscated
No Data			

- Add Application, you can define a regex pattern for customer private domains/app.



Obfuscate Applications

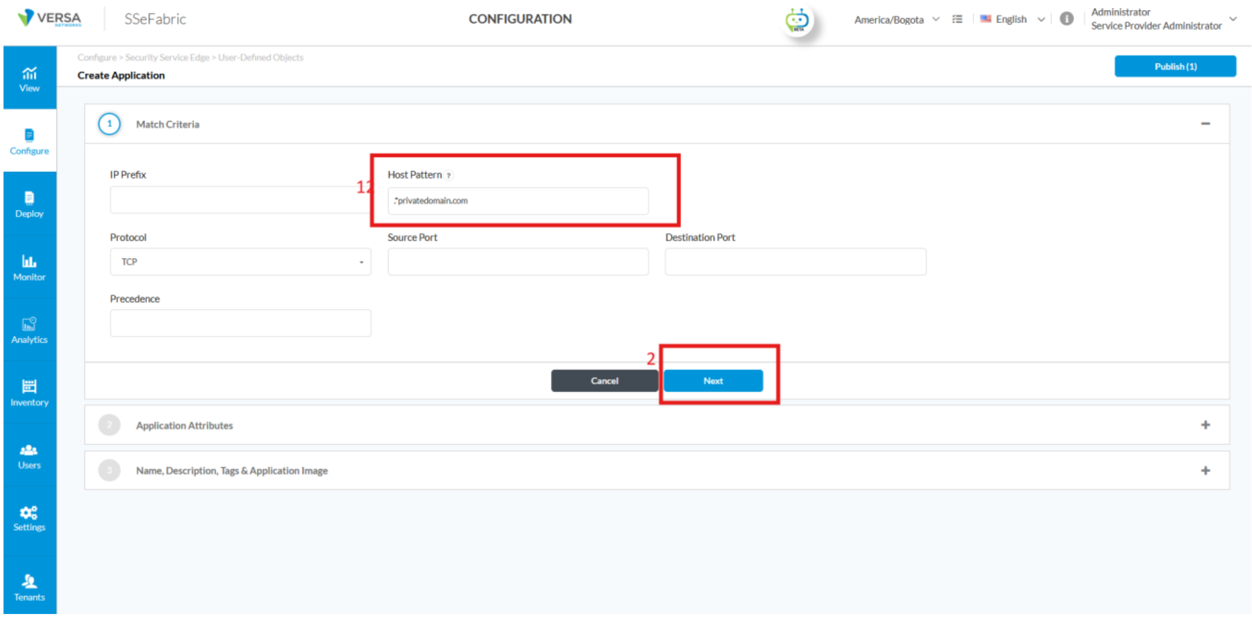
Add applications you want to obfuscate.

Traffic Source: SSeFabric-Enterprise

Private Applications with Host Pattern: Search or select one or more private applications with Host Pattern

Resolvers: Enter one or more resolver IP address

□ Do not Obfuscate these applications



Configure > Security Service Edge > User-Defined Objects

Create Application

1 Match Criteria

IP Prefix:

Host Pattern: .*privatedomain.com

Protocol: TCP

Source Port:

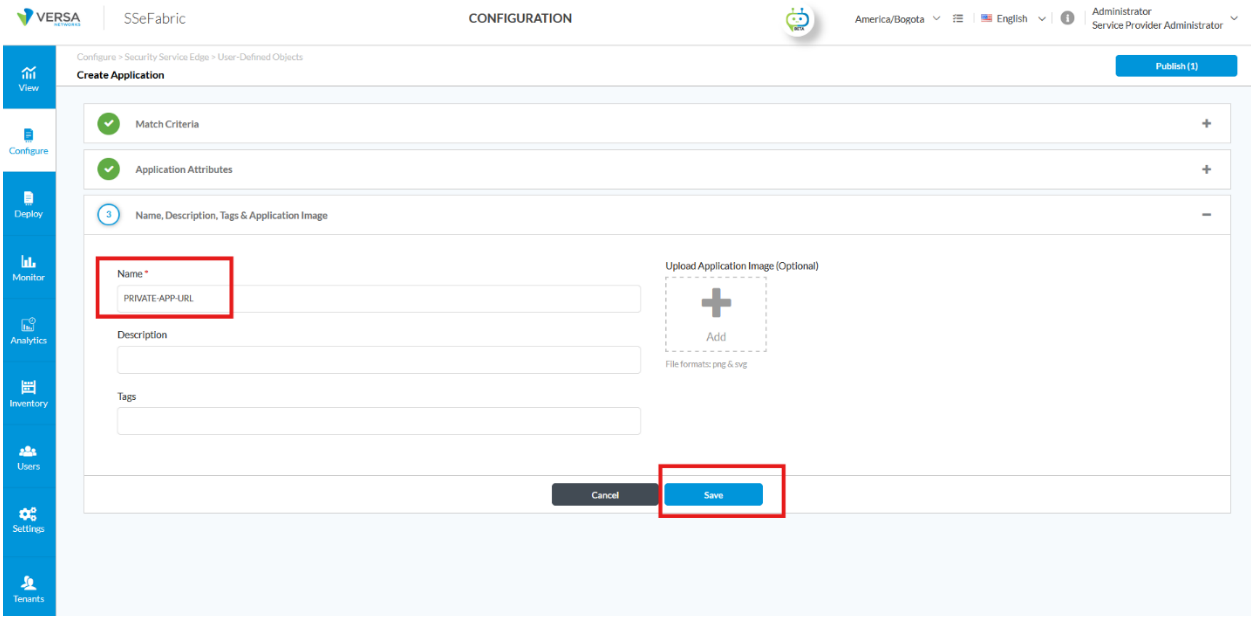
Destination Port:

Precedence:

2 Application Attributes

3 Name, Description, Tags & Application Image

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



Configure > Security Service Edge > User-Defined Objects

Create Application

Match Criteria

Application Attributes

3 Name, Description, Tags & Application Image

Name *: PRIVATE-APP-URL

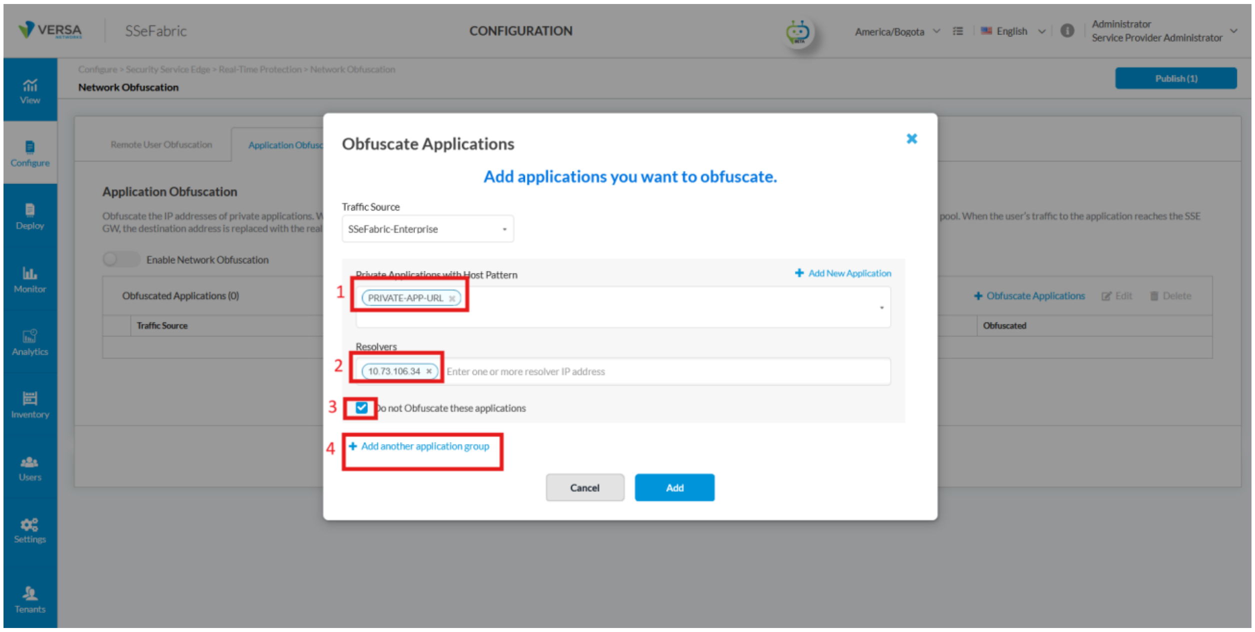
Description:

Tags:

Upload Application Image (Optional)

File formats: png & svg

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


VERSA
SSeFabric
CONFIGURATION
America/Bogota
English
Administrator
Service Provider Administrator
Configure > Security Service Edge > Real-Time Protection > Network Obfuscation
Network Obfuscation
Publish (1)
View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
Tenants
Remote User Obfuscation
Application Obfusc
Application Obfuscation
Obfuscate the IP addresses of private applications. W
GW, the destination address is replaced with the real
pool. When the user's traffic to the application reaches the SSE
Enable Network Obfuscation
Obfuscated Applications (0)
Obfuscate Applications
Edit
Delete
Traffic Source
Obfuscated
1
2
3
4

Obfuscate Applications

Add applications you want to obfuscate.

Traffic Source: SSeFabric-Enterprise

Private Applications with Host Pattern: PRIVATE-APP-URL

+ Add New Application

Resolvers: 10.73.106.34

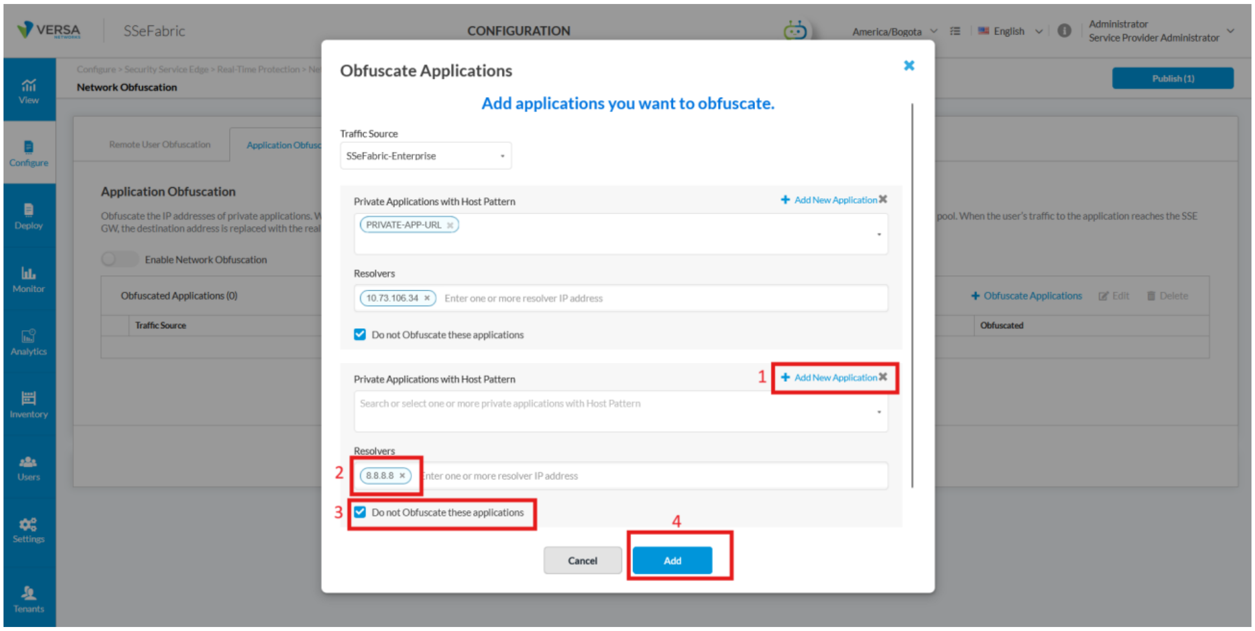
Enter one or more resolver IP address

☑ Do not Obfuscate these applications

+ Add another application group

Cancel | Add

- Do not define any application, so the rest of the domains are matched, and DNS resolvers are defined. It can be either customer-provided or public DNS.


VERSA
SSeFabric
CONFIGURATION
America/Bogota
English
Administrator
Service Provider Administrator
Configure > Security Service Edge > Real-Time Protection > Ne
Network Obfuscation
Publish (1)
View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
Tenants
Remote User Obfuscation
Application Obfusc
Application Obfuscation
Obfuscate the IP addresses of private applications. W
GW, the destination address is replaced with the real
pool. When the user's traffic to the application reaches the SSE
Enable Network Obfuscation
Obfuscated Applications (0)
Obfuscate Applications
Edit
Delete
Traffic Source
Obfuscated
1
2
3
4

Obfuscate Applications

Add applications you want to obfuscate.

Traffic Source: SSeFabric-Enterprise

Private Applications with Host Pattern: PRIVATE-APP-URL

+ Add New Application

Resolvers: 10.73.106.34

☑ Do not Obfuscate these applications

Private Applications with Host Pattern: Search or select one or more private applications with Host Pattern

+ Add New Application

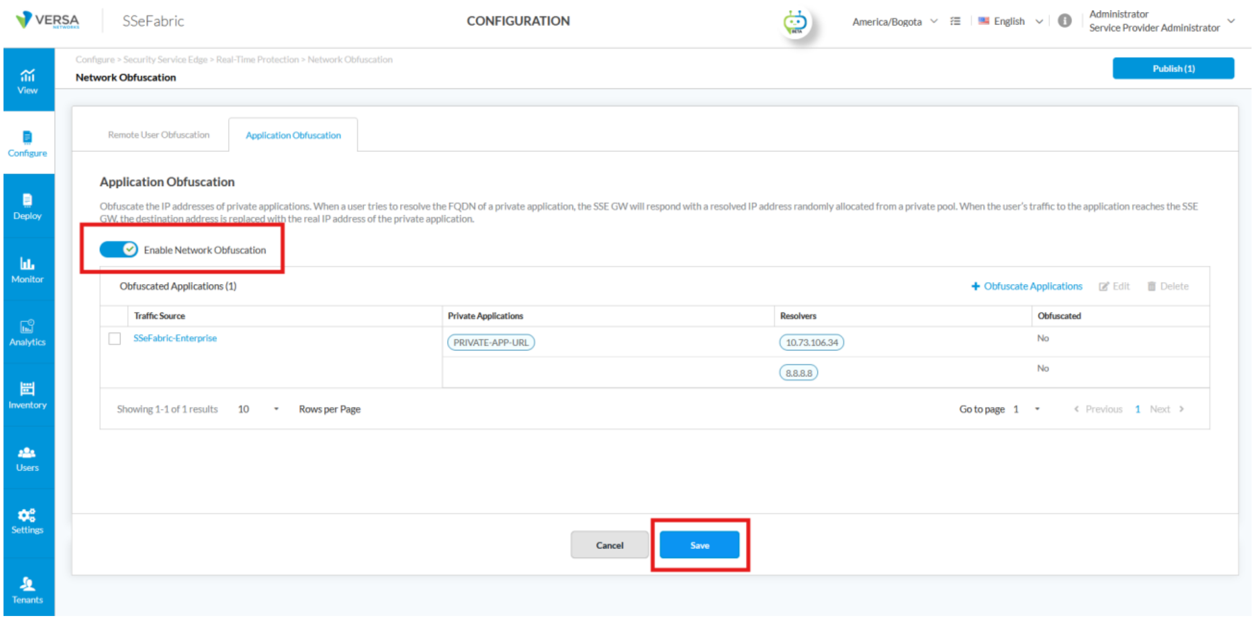
Resolvers: 8.8.8.8

Enter one or more resolver IP address

☑ Do not Obfuscate these applications

Cancel | Add

- Now set Enable Network Obfuscation



Network Obfuscation

Application Obfuscation

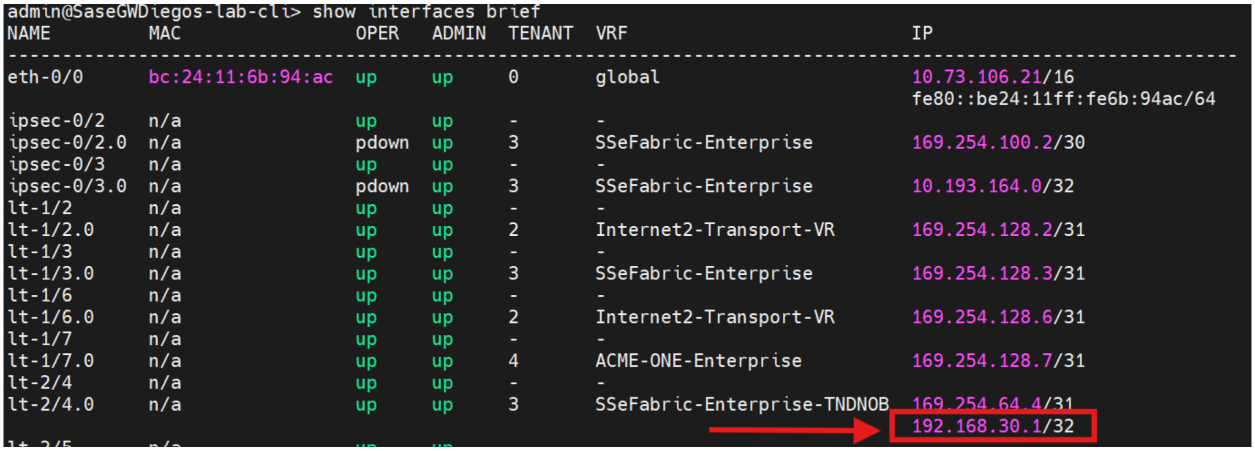
Obfuscate the IP addresses of private applications. When a user tries to resolve the FQDN of a private application, the SSE GW will respond with a resolved IP address randomly allocated from a private pool. When the user's traffic to the application reaches the SSE GW, the destination address is replaced with the real IP address of the private application.

Enable Network Obfuscation

Obfuscated Applications (1)

	Traffic Source	Private Applications	Resolvers	Obfuscated
□	SSeFabric-Enterprise	PRIVATE-APP-URL	10.73.106.34	No
			8.8.8.8	No

3. **Identify TNDNOB TVI IP:** On the SASE Gateway, run the command "*show interfaces brief*"

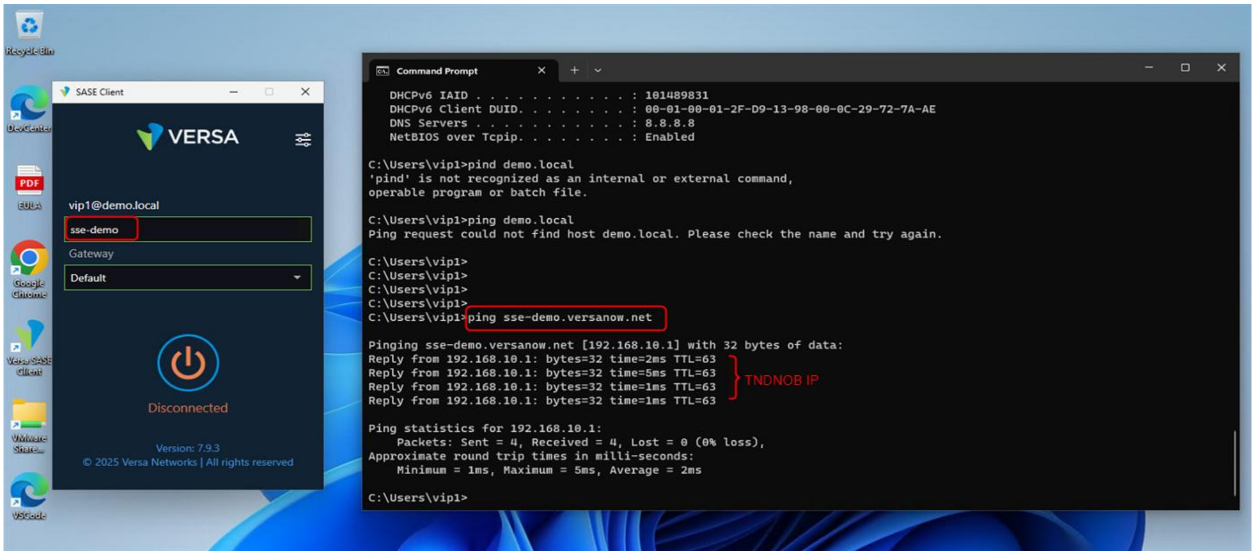


```
admin@SaseGWDiegos-lab-cli> show interfaces brief
NAME         MAC                 OPER   ADMIN  TENANT  VRF                          IP
-------------------------------------------------------------------------------------------------------------------
eth-0/0      bc:24:11:6b:94:ac   up     up     0       global                       10.73.106.21/16
                                                                                    fe80::be24:11ff:fe6b:94ac/64

ipsec-0/2    n/a                 up     up     -       -
ipsec-0/2.0  n/a                 pdown  up     3       SSeFabric-Enterprise         169.254.100.2/30
ipsec-0/3    n/a                 up     up     -       -
ipsec-0/3.0  n/a                 pdown  up     3       SSeFabric-Enterprise         10.193.164.0/32
lt-1/2       n/a                 up     up     -       -
lt-1/2.0     n/a                 up     up     2       Internet2-Transport-VR       169.254.128.2/31
lt-1/3       n/a                 up     up     -       -
lt-1/3.0     n/a                 up     up     3       SSeFabric-Enterprise         169.254.128.3/31
lt-1/6       n/a                 up     up     -       -
lt-1/6.0     n/a                 up     up     2       Internet2-Transport-VR       169.254.128.6/31
lt-1/7       n/a                 up     up     -       -
lt-1/7.0     n/a                 up     up     4       ACME-ONE-Enterprise          169.254.128.7/31
lt-2/4       n/a                 up     up     -       -
lt-2/4.0     n/a                 up     up     3       SSeFabric-Enterprise-TNDNOB  169.254.64.4/31
                                                                                    192.168.30.1/32
lt-2/5       n/a                 up     up
```

It is important to mention that Versa assigns for TND the first IP address from the ***"Client Address Pool"*** *that was defined during the tenant creation.*

Verification Steps

- Make sure DNS resolution for the registration domains is correct: (example below)



vip1@demo.local

sse-demo

Gateway

Default

Disconnected

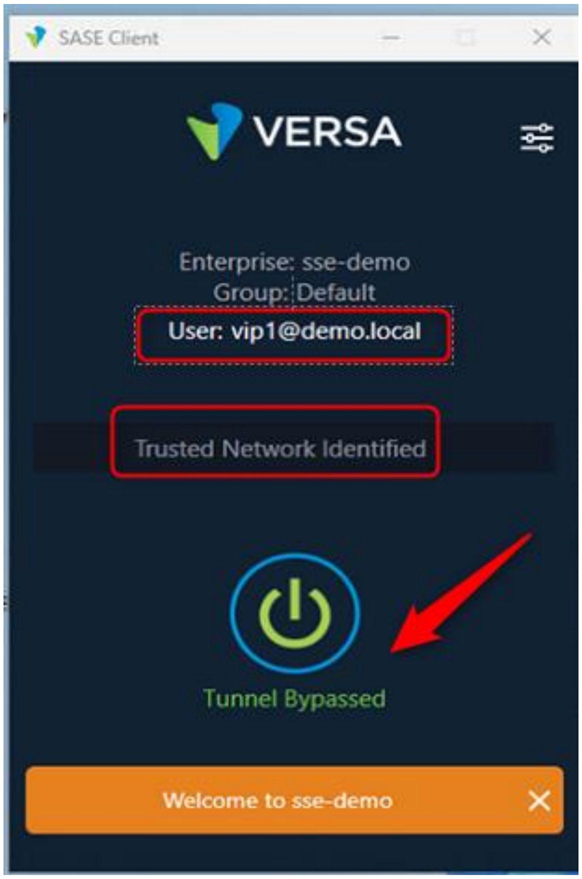
Version: 7.9.3

© 2025 Versa Networks | All rights reserved

```
   DHCPv6 IAID . . . . . . . . . . . : 101489831
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-D9-13-98-00-0C-29-72-7A-AE
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\vip1>pind demo.local
'pind' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vip1>ping demo.local
Ping request could not find host demo.local. Please check the name and try again.

C:\Users\vip1>
C:\Users\vip1>
C:\Users\vip1>
C:\Users\vip1>
C:\Users\vip1>ping sse-demo.versanow.net

Pinging sse-demo.versanow.net [192.168.10.1] with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=2ms TTL=63
Reply from 192.168.10.1: bytes=32 time=5ms TTL=63
Reply from 192.168.10.1: bytes=32 time=1ms TTL=63
Reply from 192.168.10.1: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\Users\vip1>
```

TNDNOB IP

- Register and connect to the SASE portal, then verify the user's identity from Concerto (Analytics).



Enterprise: sse-demo

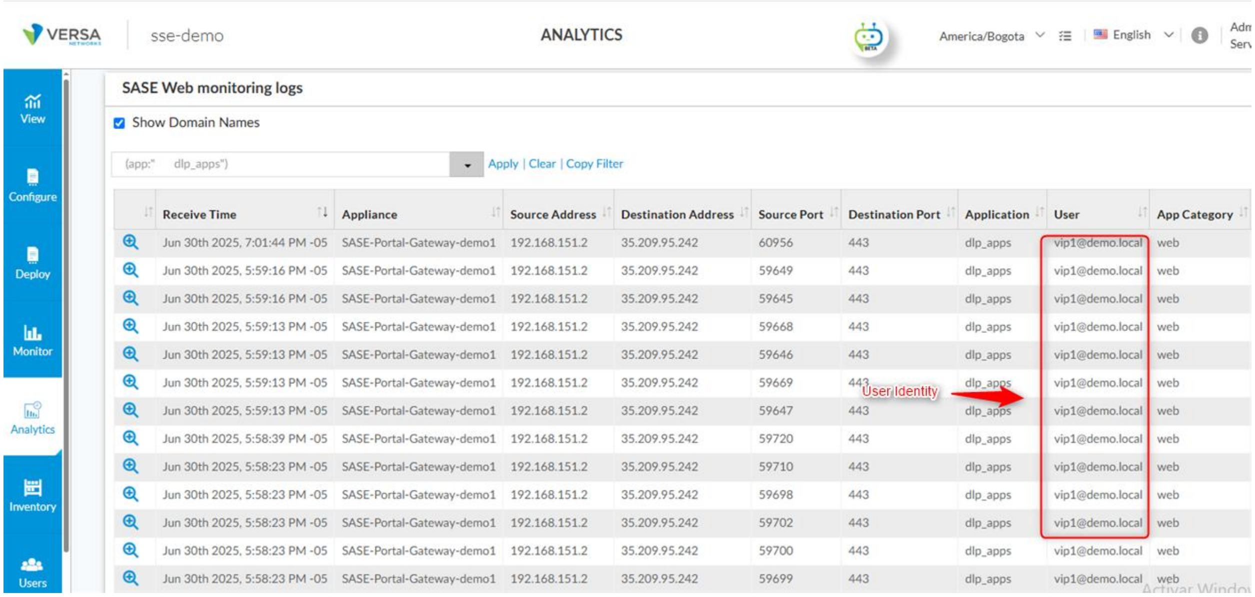
Group: Default

User: vip1@demo.local

Trusted Network Identified

Tunnel Bypassed

Welcome to sse-demo



SASE Web monitoring logs

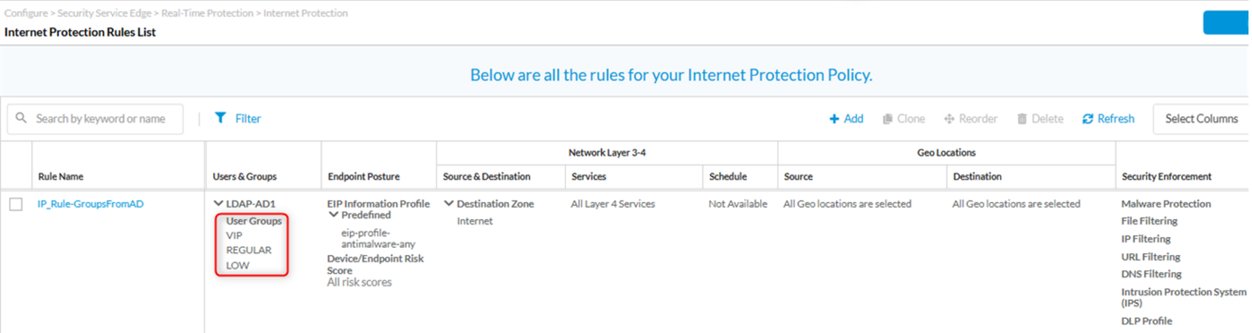
☑ Show Domain Names

(app:" dlp_apps") Apply | Clear | Copy Filter

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	App Category
Jun 30th 2025, 7:01:44 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	60956	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:16 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59649	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:16 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59645	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:13 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59668	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:13 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59646	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:13 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59669	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:59:13 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59647	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:39 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59720	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:23 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59710	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:23 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59698	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:23 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59702	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:23 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59700	443	dlp_apps	vip1@demo.local	web
Jun 30th 2025, 5:58:23 PM -05	SASE-Portal-Gateway-demo1	192.168.151.2	35.209.95.242	59699	443	dlp_apps	vip1@demo.local	web

User Identity

- You can now create real-time protection rules based on user identity, either by using the group or the user as the source.



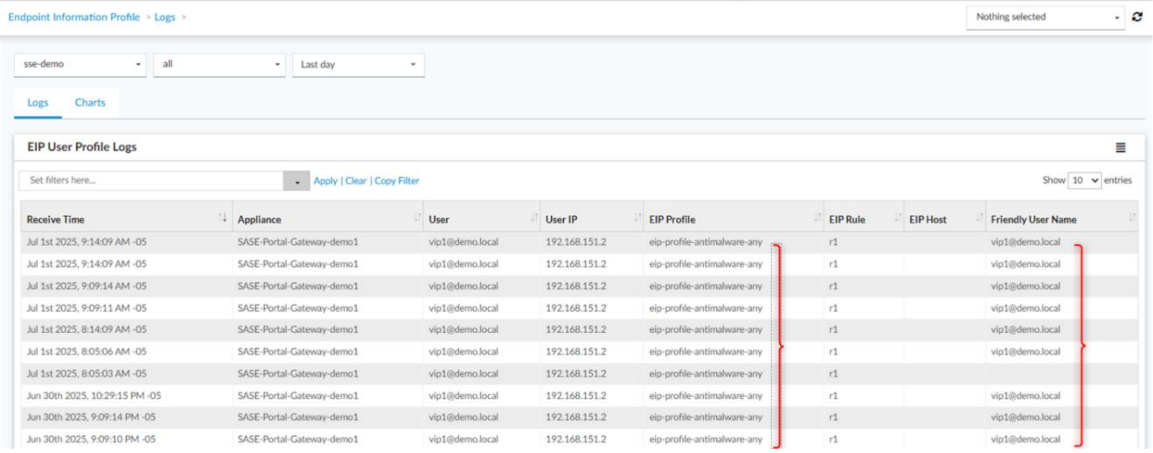
Configure > Security Service Edge > Real-Time Protection > Internet Protection

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

				Network Layer 3-4			Geo Locations		
	Rule Name	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Security Enforcement
□	IP_Rule-GroupsFromAD	LDAP-AD1 User Groups VIP REGULAR LOW	EIP Information Profile Predefined eip-profile-antimalware-any Device/Endpoint Risk Score All risk scores	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Malware Protection File Filtering IP Filtering URL Filtering DNS Filtering Intrusion Protection System (IPS) DLP Profile

- You can validate that EIP information is being collected by the Versa agent and sent periodically via HTTPS (POST) connections to the SASE gateway through the TNDNOB IP. You can also observe other connections made by the agent using ICMP and HTTPS to verify connectivity.



Endpoint Information Profile > Logs >

Nothing selected

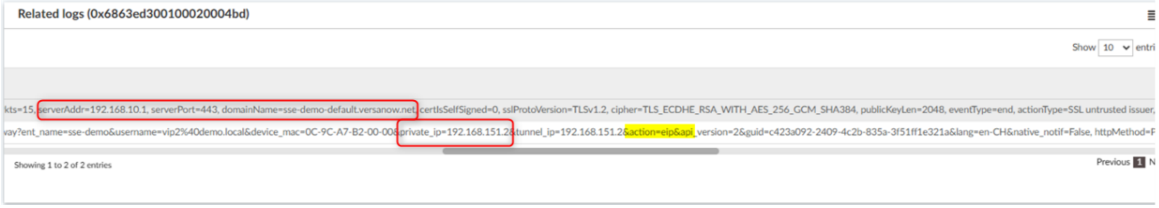
sse-demo | all | Last day

EIP User Profile Logs

Set filters here... Apply | Clear | Copy Filter

Show 10 entries

Receive Time	Appliance	User	User IP	EIP Profile	EIP Rule	EIP Host	Friendly User Name
Jul 1st 2025, 9:14:09 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 9:14:09 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 9:09:14 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 9:09:11 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 8:14:09 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 8:05:06 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jul 1st 2025, 8:05:03 AM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		
Jun 30th 2025, 10:29:15 PM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jun 30th 2025, 9:09:14 PM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local
Jun 30th 2025, 9:09:10 PM -05	SASE-Portal-Gateway-demo1	vip1@demo.local	192.168.151.2	eip-profile-antimalware-any	r1		vip1@demo.local



```
kts=15, serverAddr=192.168.10.1, serverPort=443, domainName=sse-demo-default.versanow.net, certIsSelfSigned=0, sslProtoVersion=TLSv1.2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, publicKeyLen=2048, eventType=end, actionType=SSL untrusted issuer,
vay?ent_name=sse-demo&username=vip2%40demo.local&device_mac=0C-9C-A7-B2-00-00&private_ip=192.168.151.2&tunnel_ip=192.168.151.2&action=eip&api_version=2&guid=c423a092-2409-4c2b-835a-3f51ff1e321a&lang=en-CH&native_notif=False, httpMethod=F
```

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.