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? 4
TND Detection Flow: Trusted vs. Untrusted Network 4
User on the Internet (Untrusted Network) 4
User in a Trusted Network (e.g., Corporate Branch) 4
Key Benefits 5
Versa TND Scenarios 5
TND Deployment Scenarios 5
TND with Customer Private DNS 5
TND with DNS Proxy on SSE Gateway 9
Verification Steps 18
About Versa 20

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

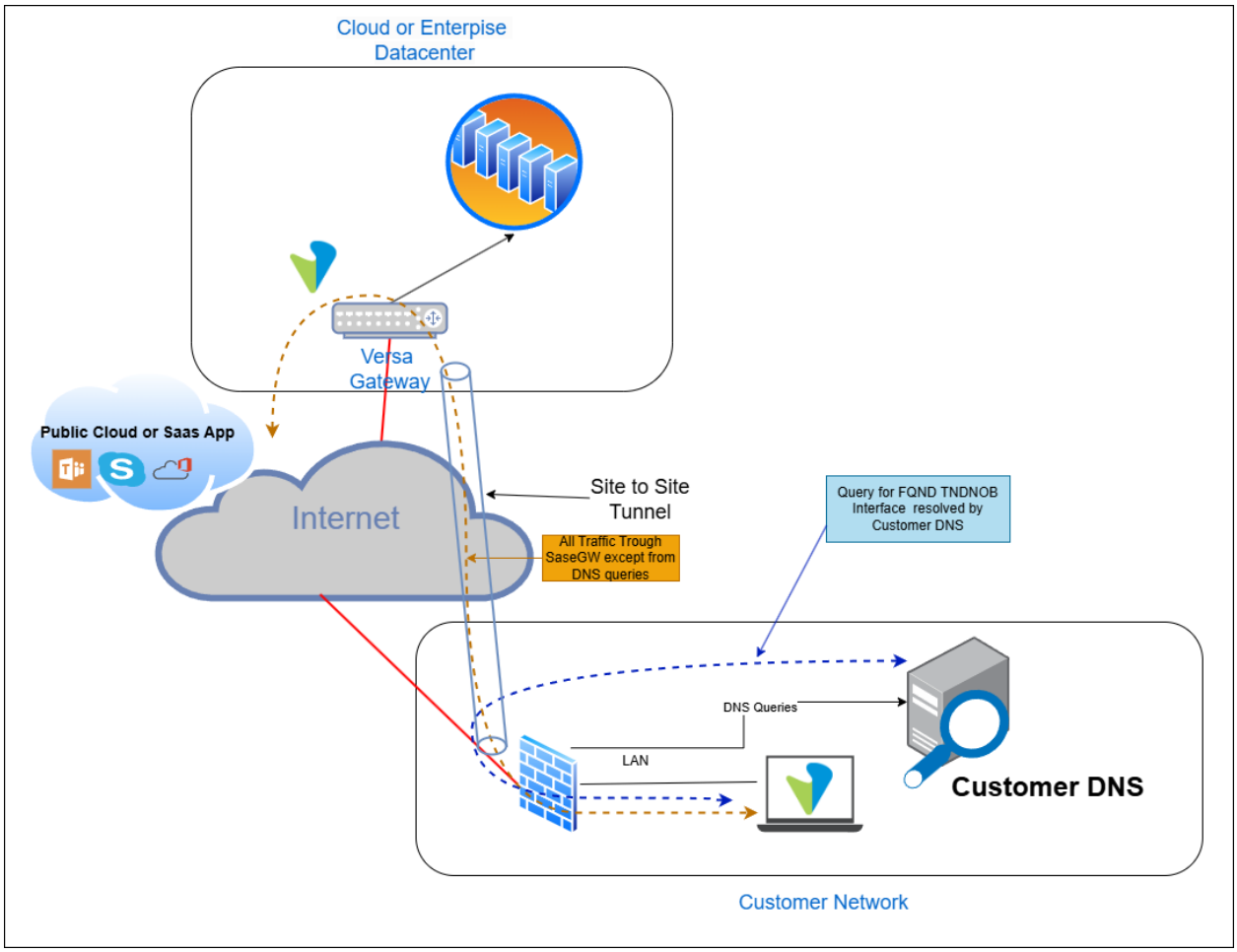
1. The Local DNS servers are configured to resolve the SASE Gateway FQDN to the private IP of the TNDNOB TVI Interface on the Gateway.
2. The SASE Client on the user device attempts to register with the SASE Gateway.
3. The client resolves the SASE Gateway FQDN.
4. The customer's private DNS server resolves 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

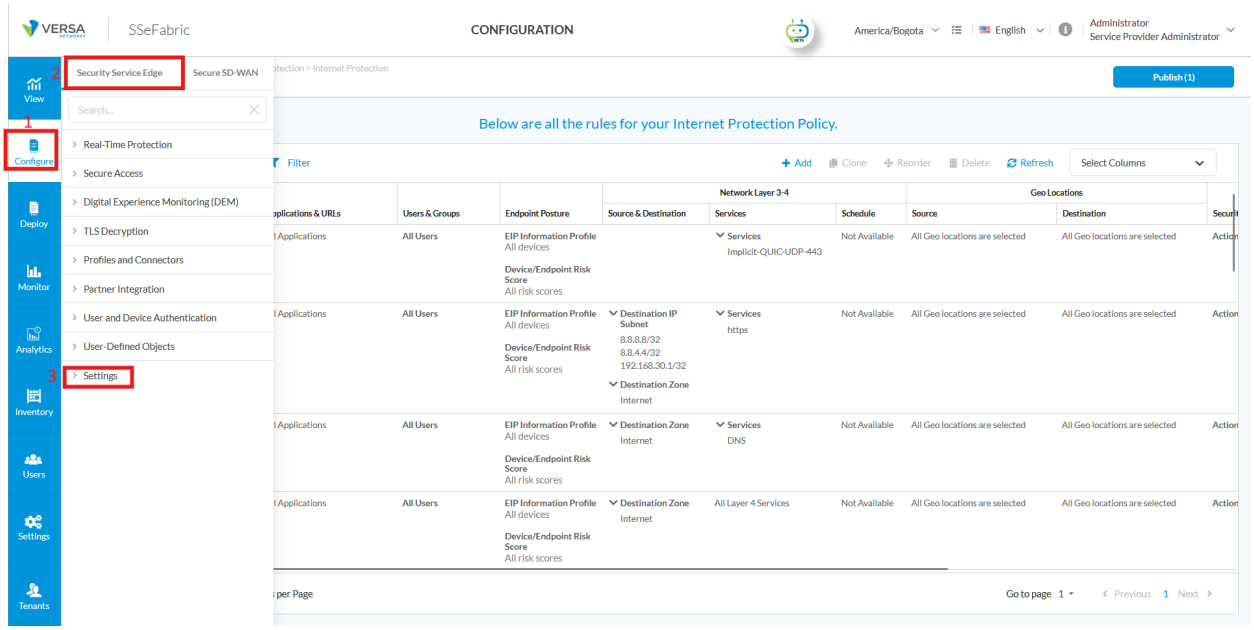
The client's DNS infrastructure must be able to resolve the portal registration domains to the private IP address of the TNDNOB interface.

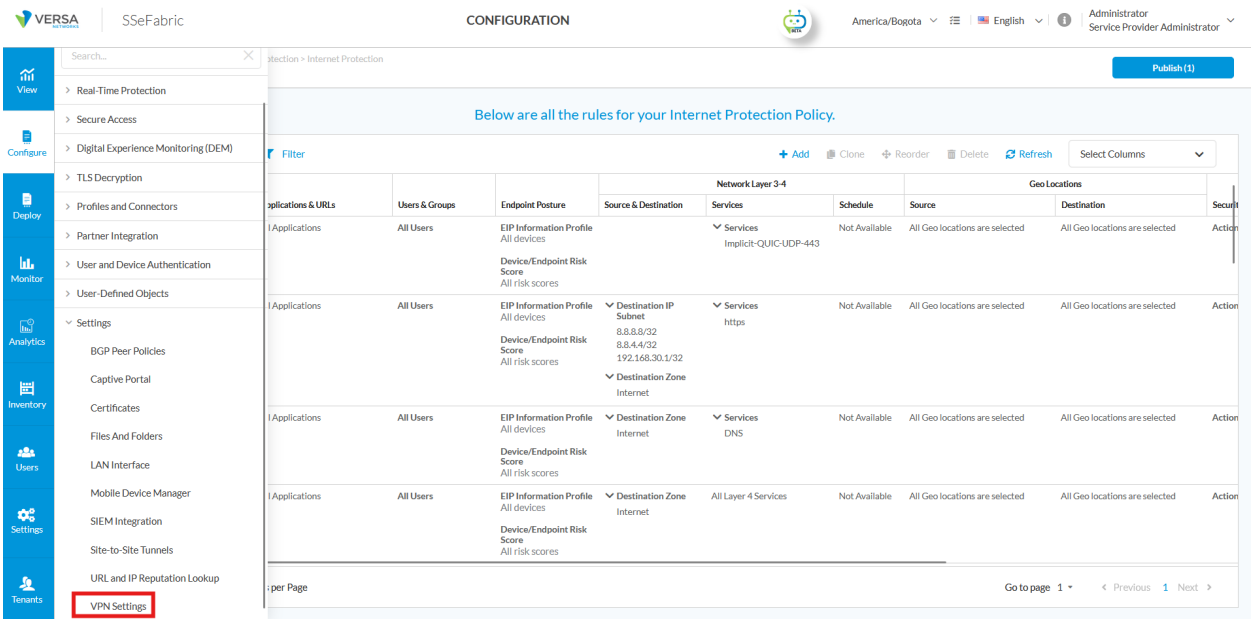
Topology



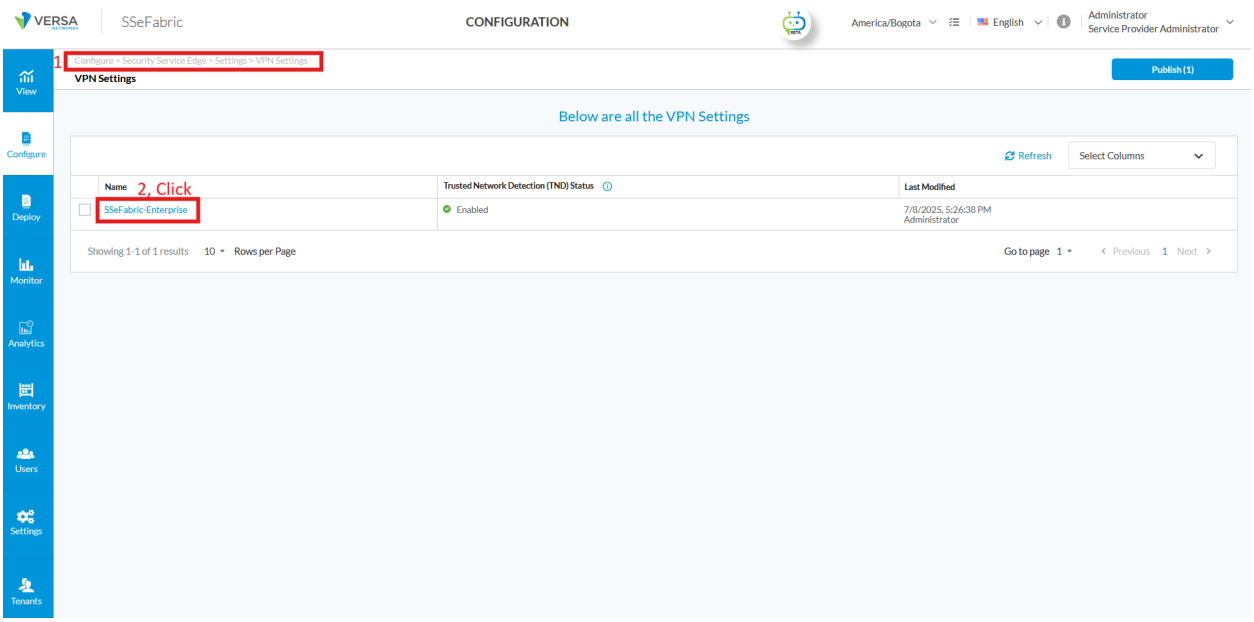
Configuration Steps

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



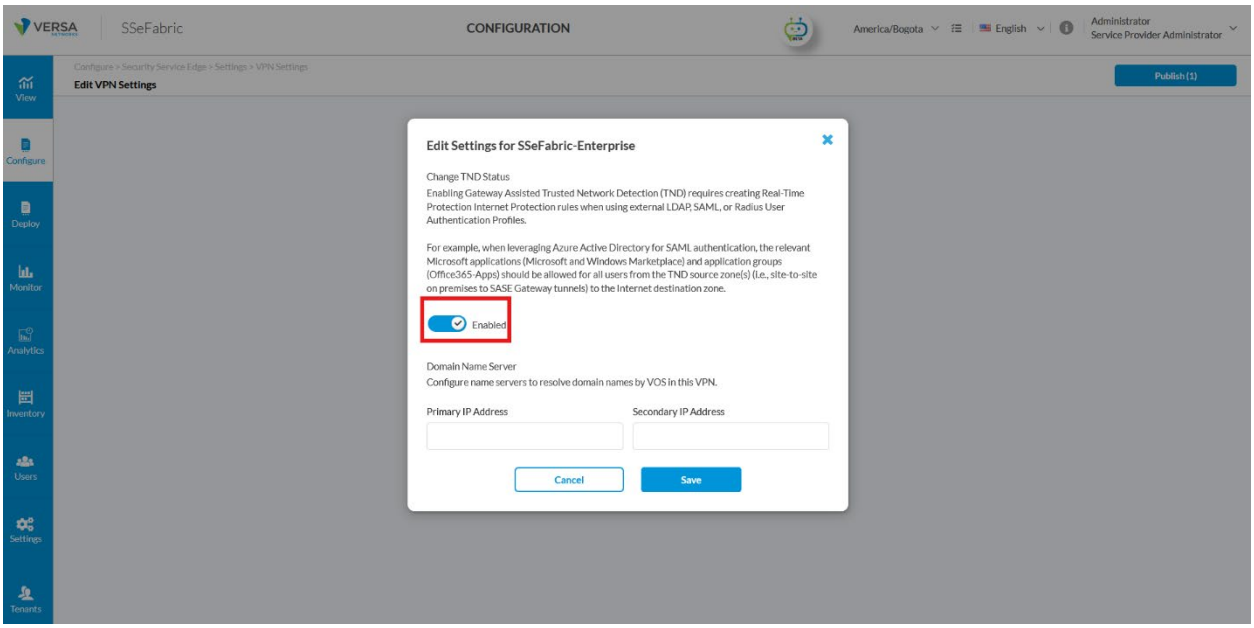


- Select the VPN name



- 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.



- **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
```

- Now, the Customer should create DNS entries for the FQDN portal domains using the TNDNOB 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

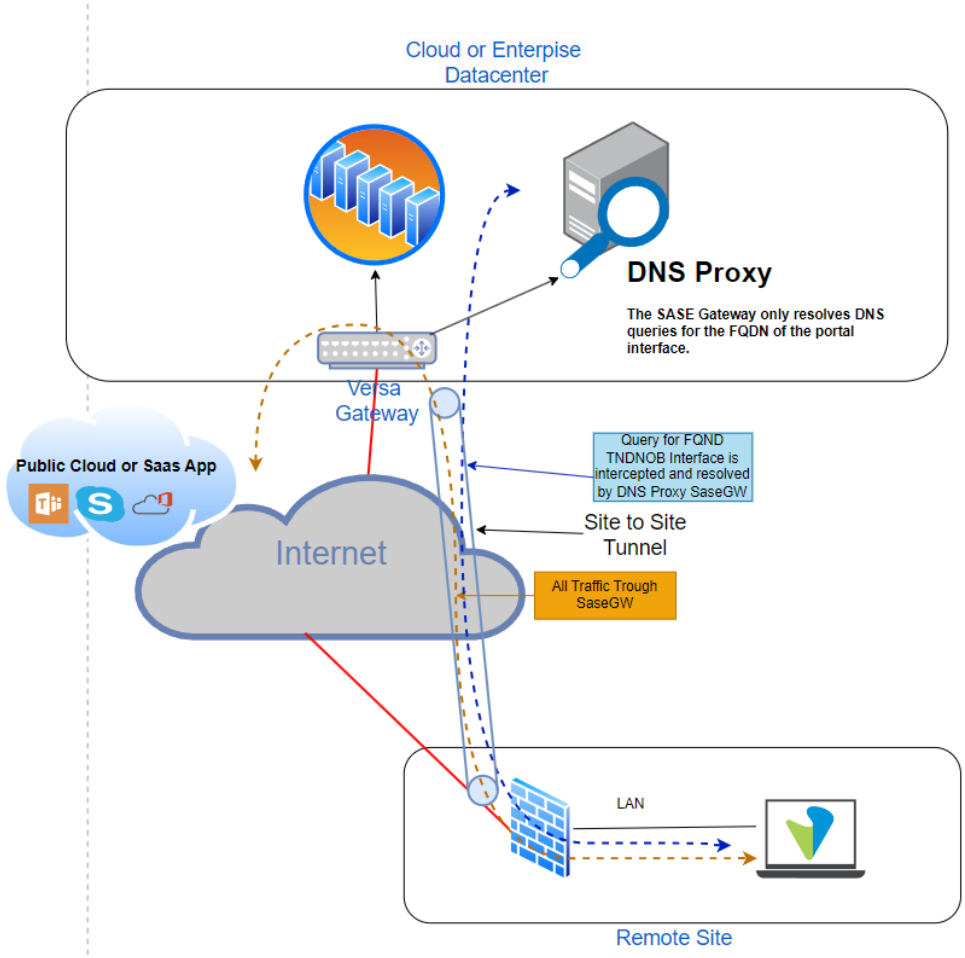
1. The SASE Client on the user device attempts to register with the SASE Gateway.
2. The client resolves the SASE Gateway FQDN. Since all DNS traffic is routed through the SSE Gateway, the gateway intercepts the DNS query.
3. Acting as an DNS proxy, the SASE Gateway resolves the FQDN to a private IP 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

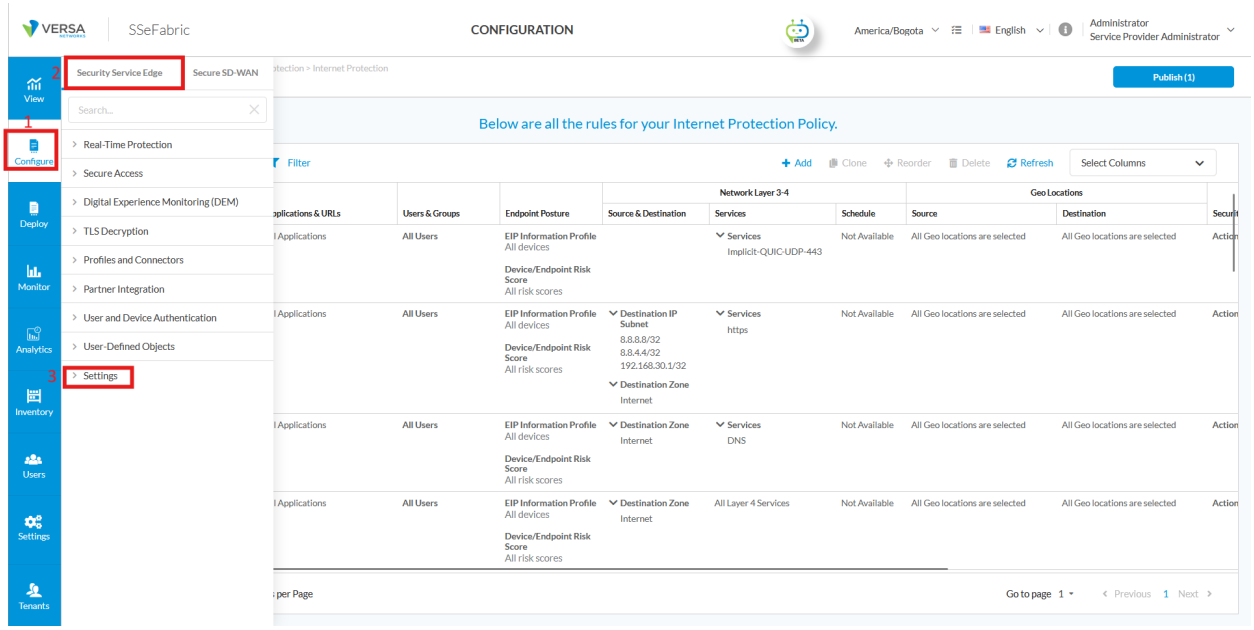
NOTE: All DNS queries from the customer network must be routed through the SSE Gateway to enable DNS interception and trusted network detection.

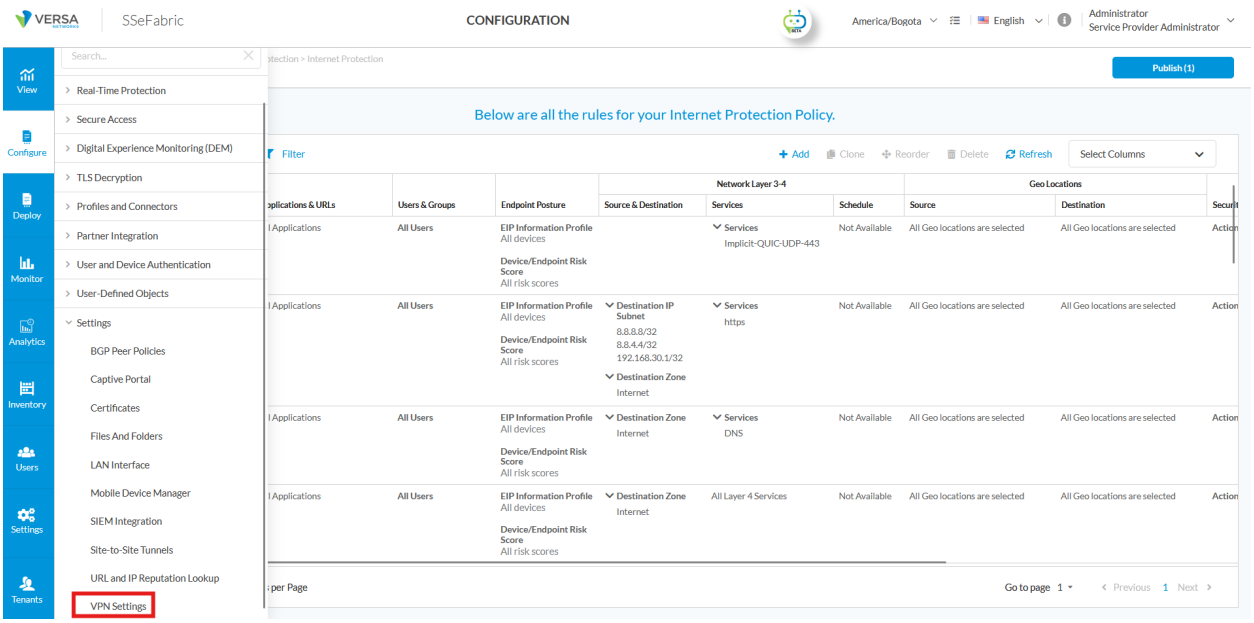
Topology



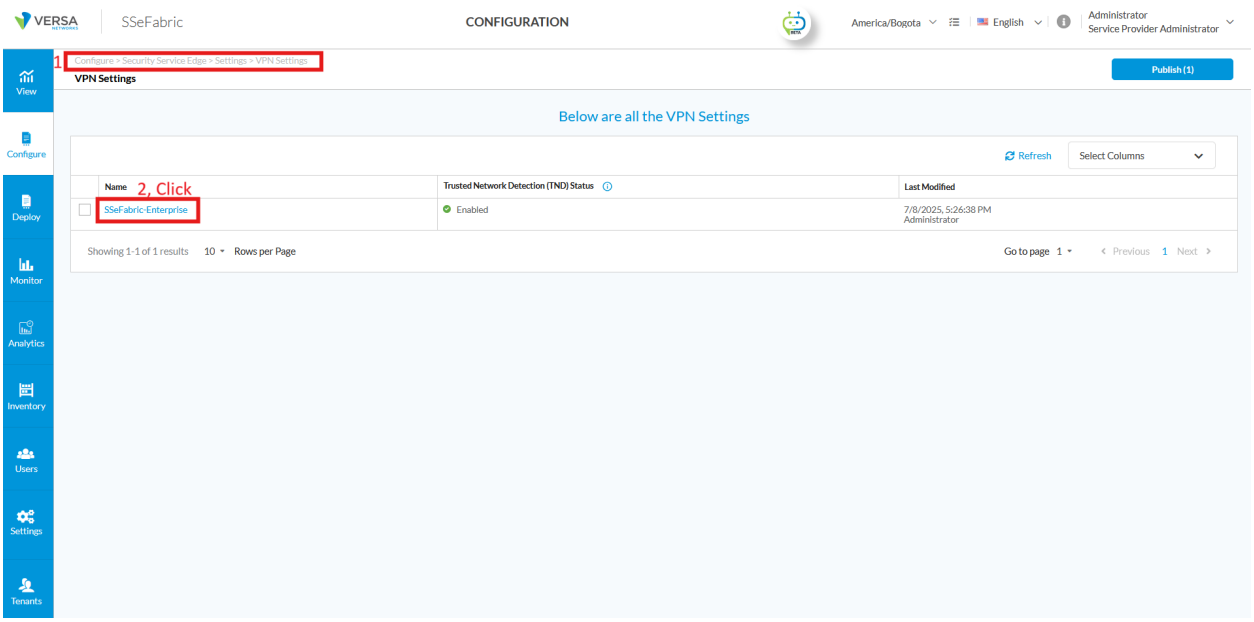
Configuration Steps

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



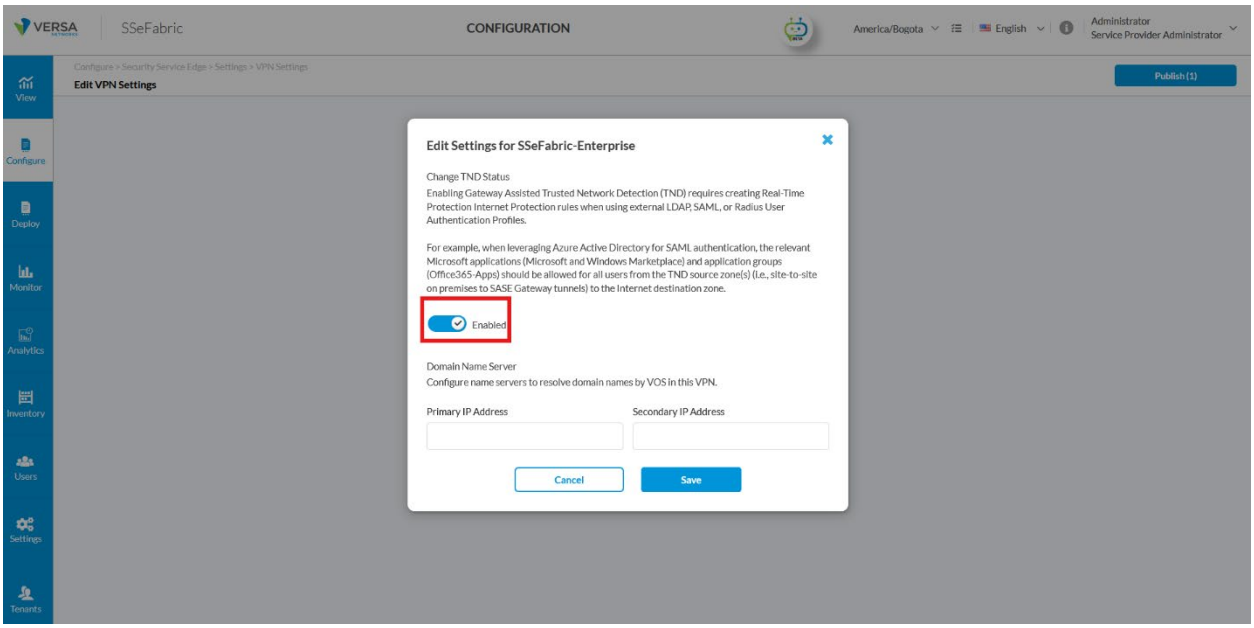


- Select the VPN name

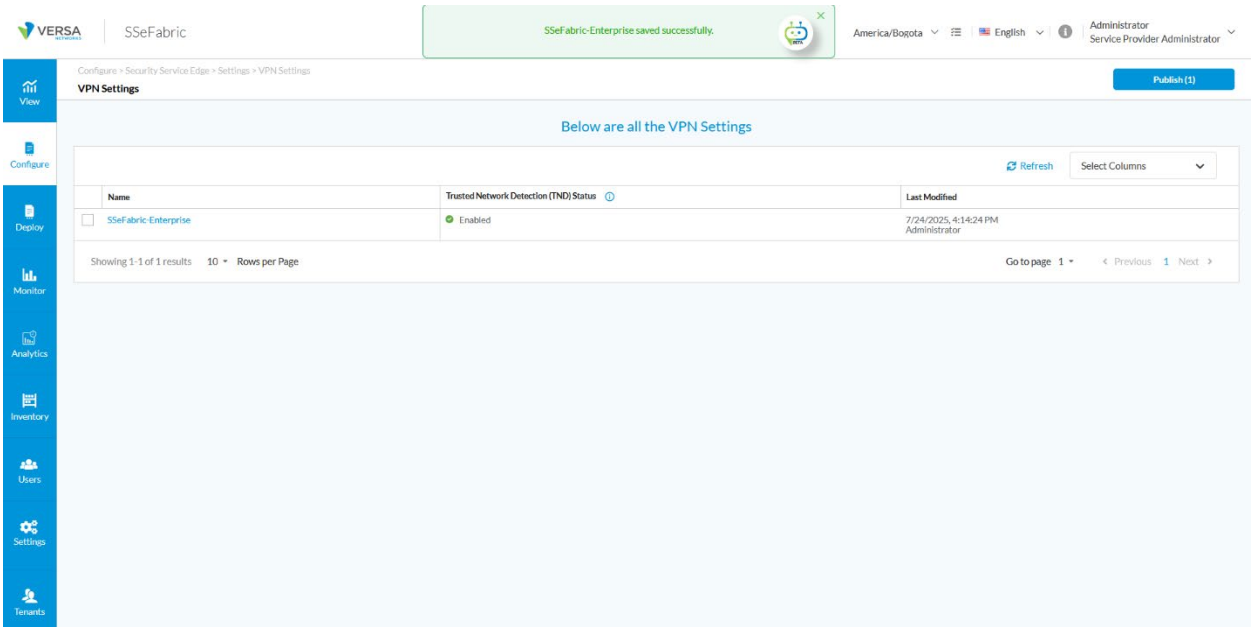


- Enable the Knob and Save.

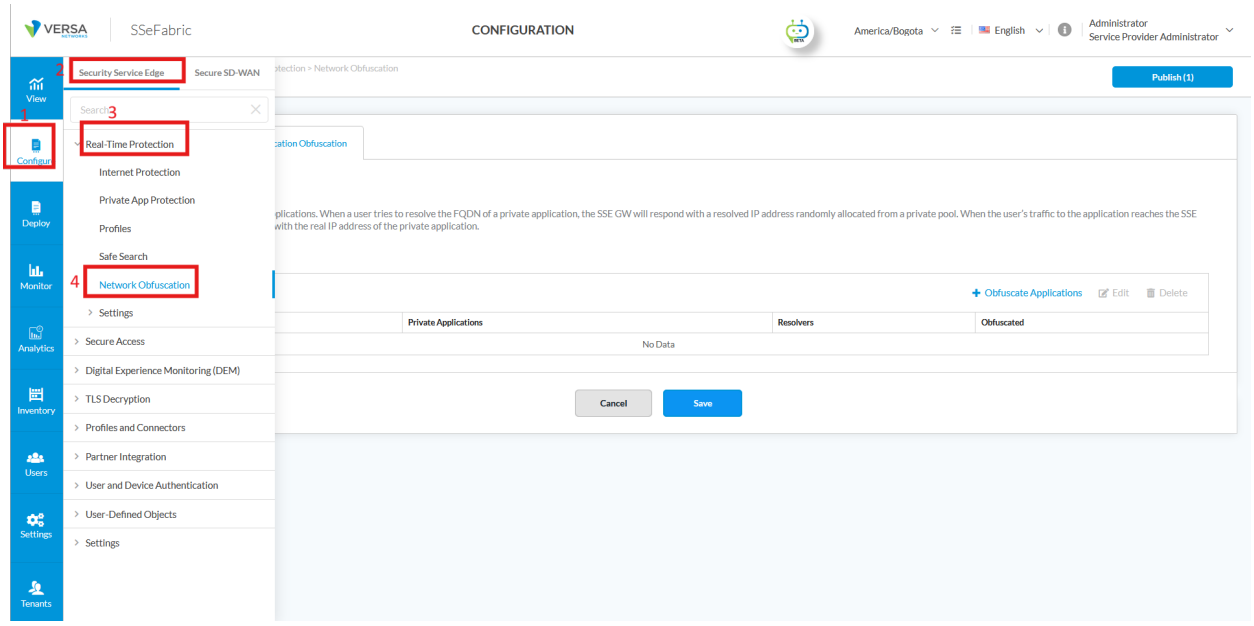
Note: To use TND, it is **not mandatory** to enter the **Primary IP Address** or **Secondary IP Address**. These fields are used when you want to add a **DNS server** to the **system settings** of the SASE Gateway, possibly to use it in **DNS Proxy rules** and enable internal domain resolution using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



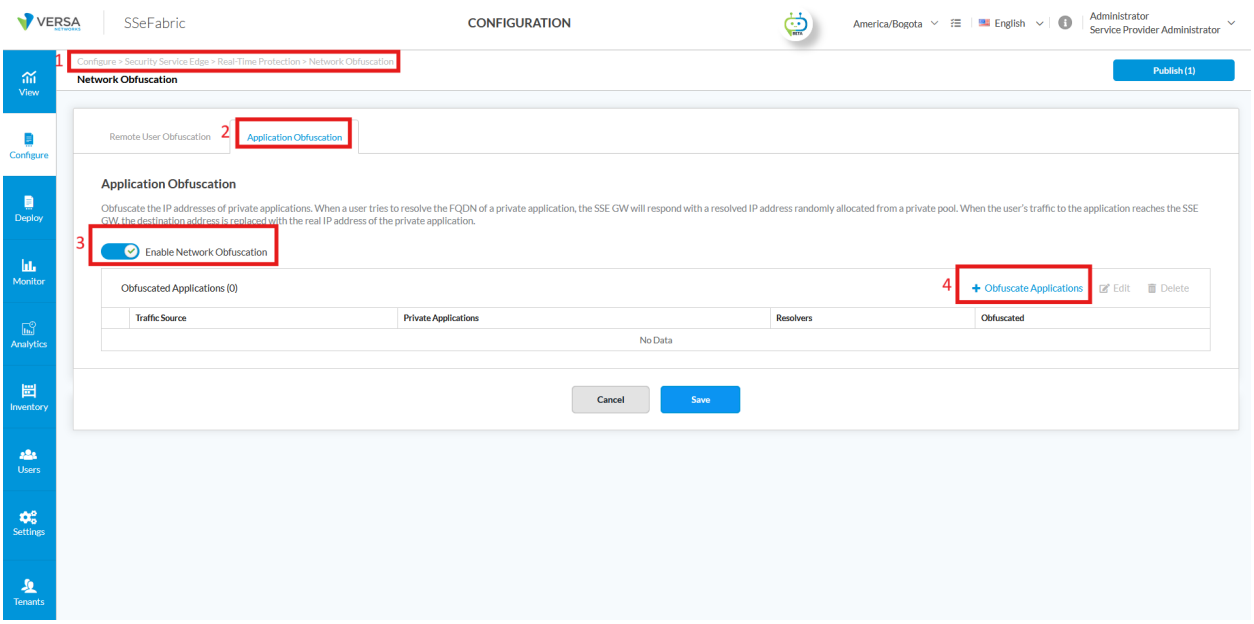
- **Remarks:** Although you were not explicitly requested to publish the TND status, you must still go to **Publish** and complete the action.



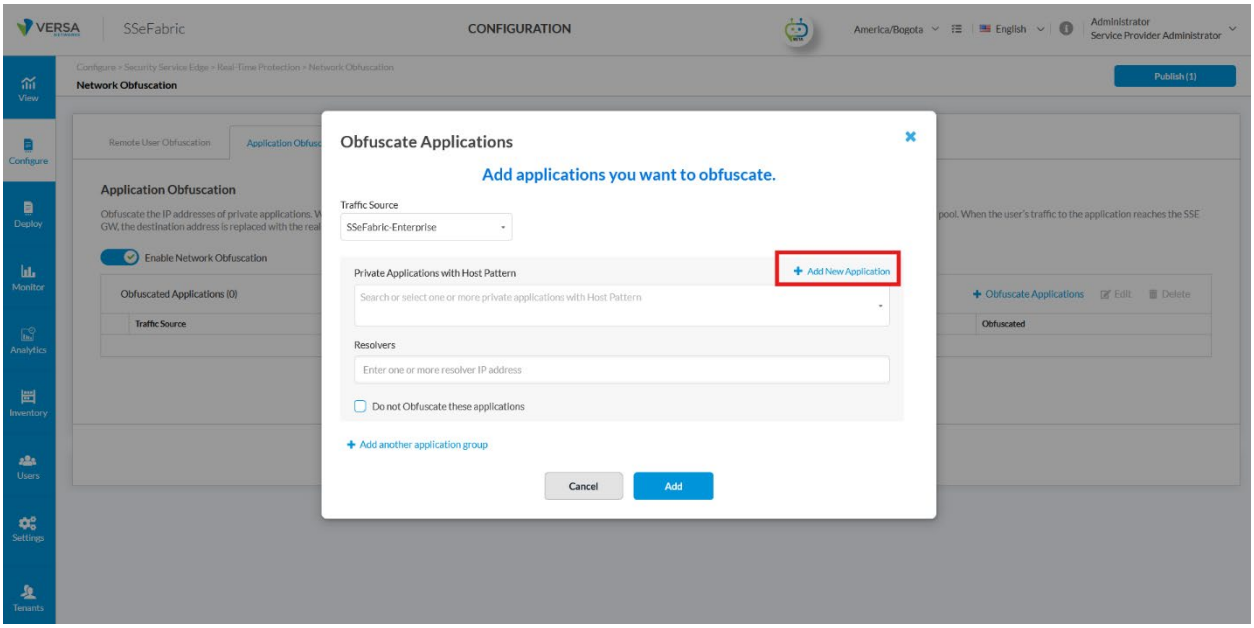
2. **DNS Proxy for Private FQDN resolution:** Steps to handle Private apps and Public URL Resolution with DNS Proxy (As required)
    - DNS proxy configuration steps to handle private and public app URL resolution.

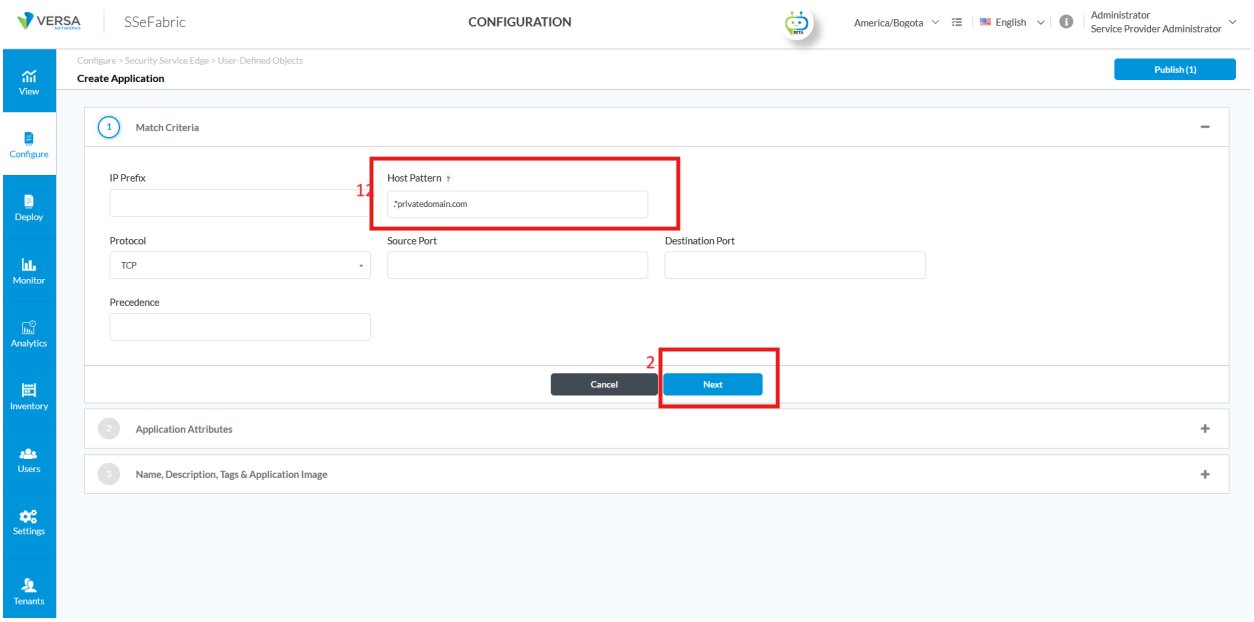


    - Click "**+ Obfuscate Applications**"

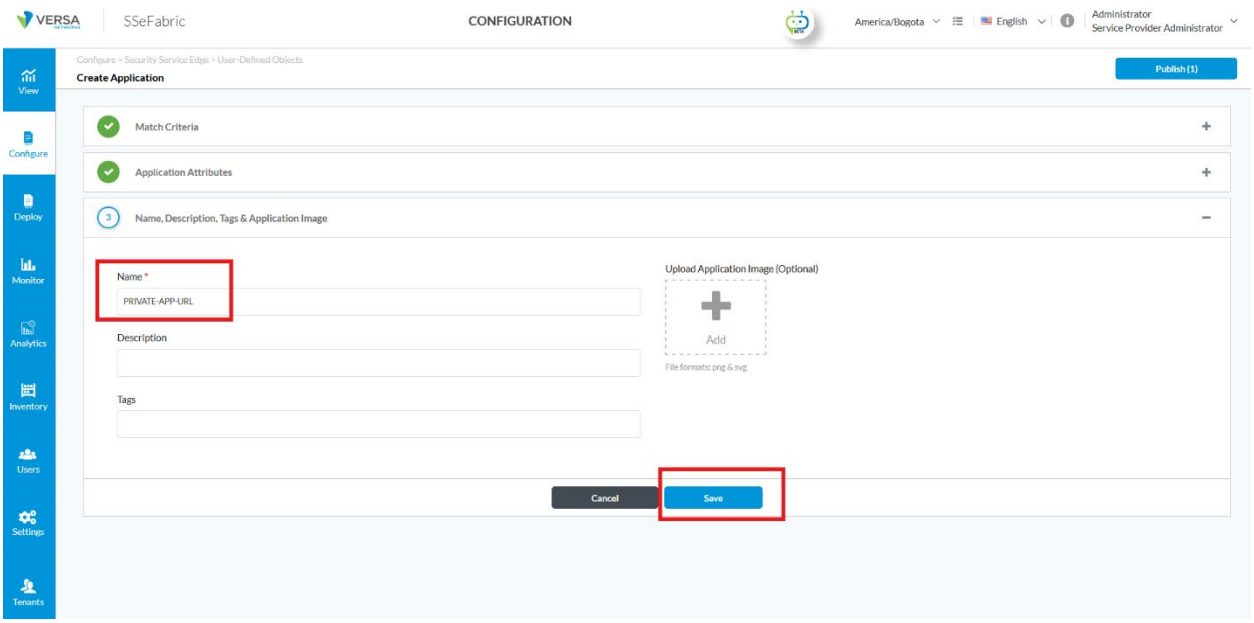


- Add Application, you can define a regex pattern for customer private domains/app.

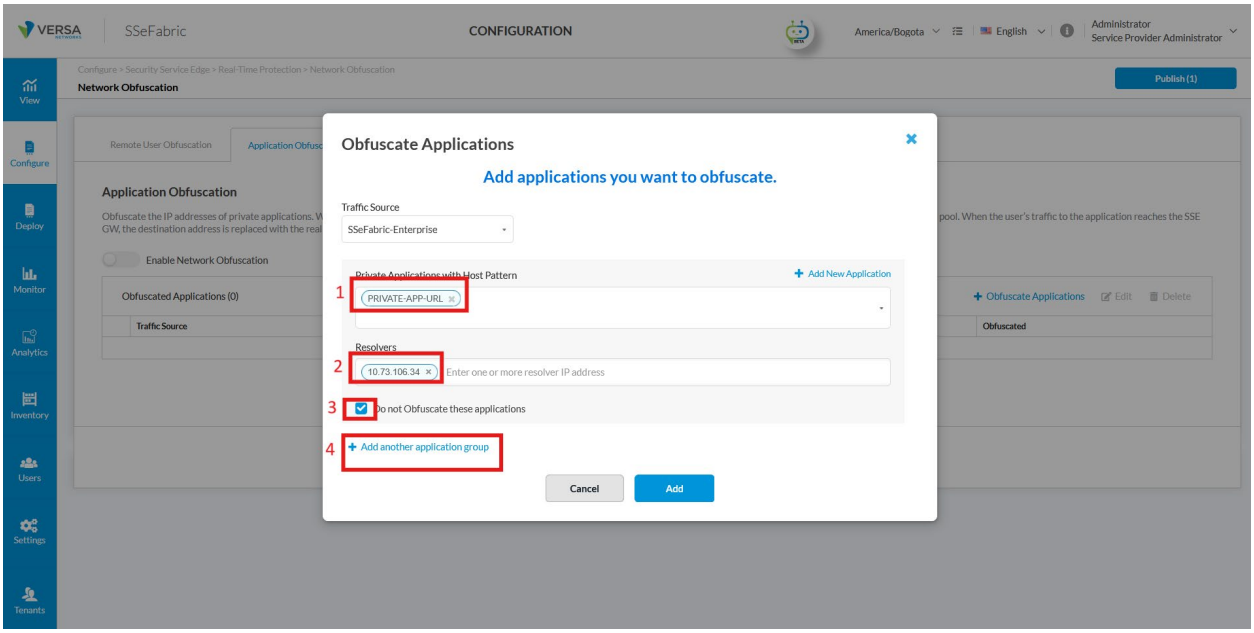




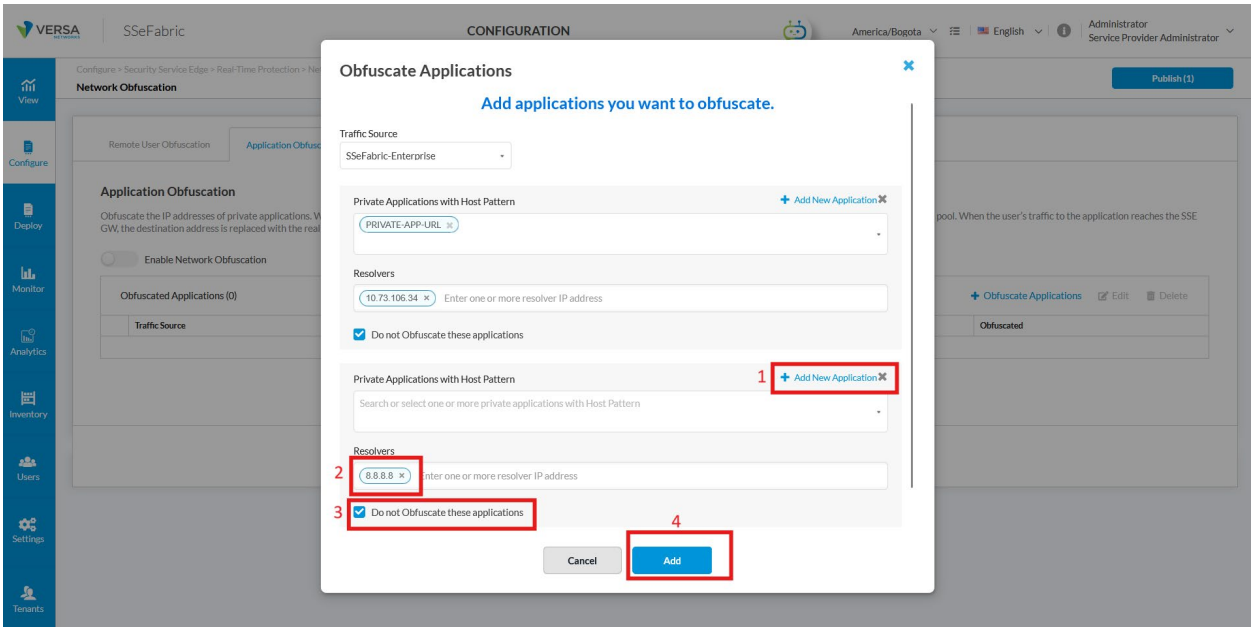
- Define the Name for the added application domains/URL.



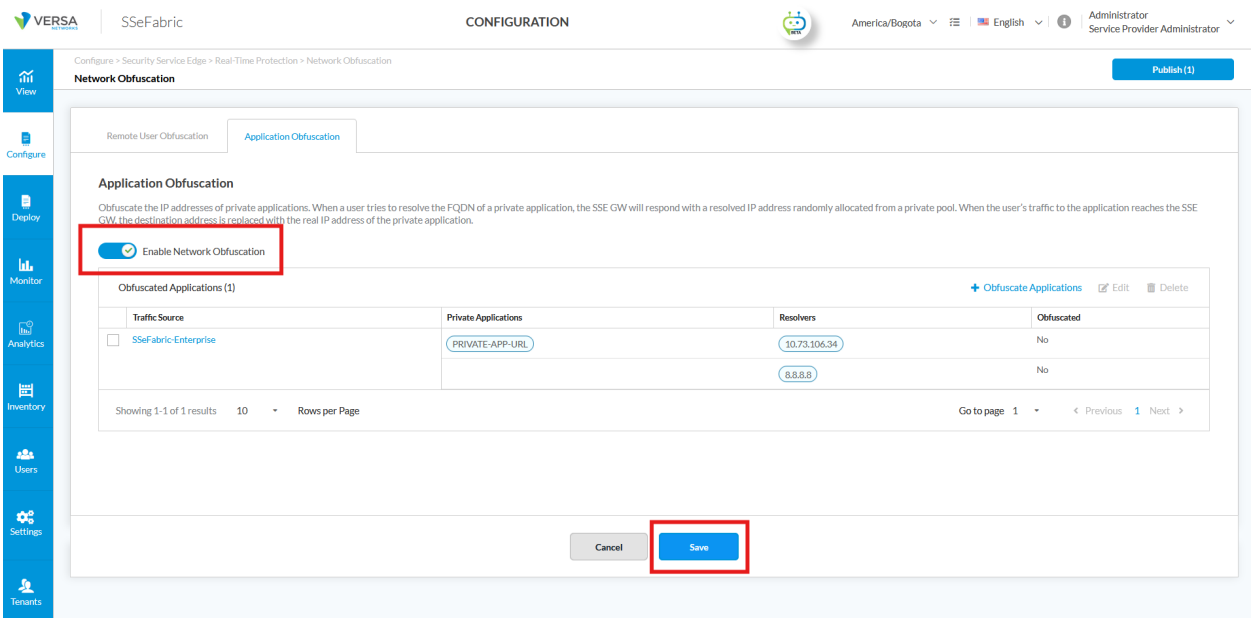
- Select the created Application. The resolver would be the customer's DNS server that can resolve private domains. Set “Do not obfuscate’ and “add another application group”.



- 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.



- Now set Enable Network Obfuscation



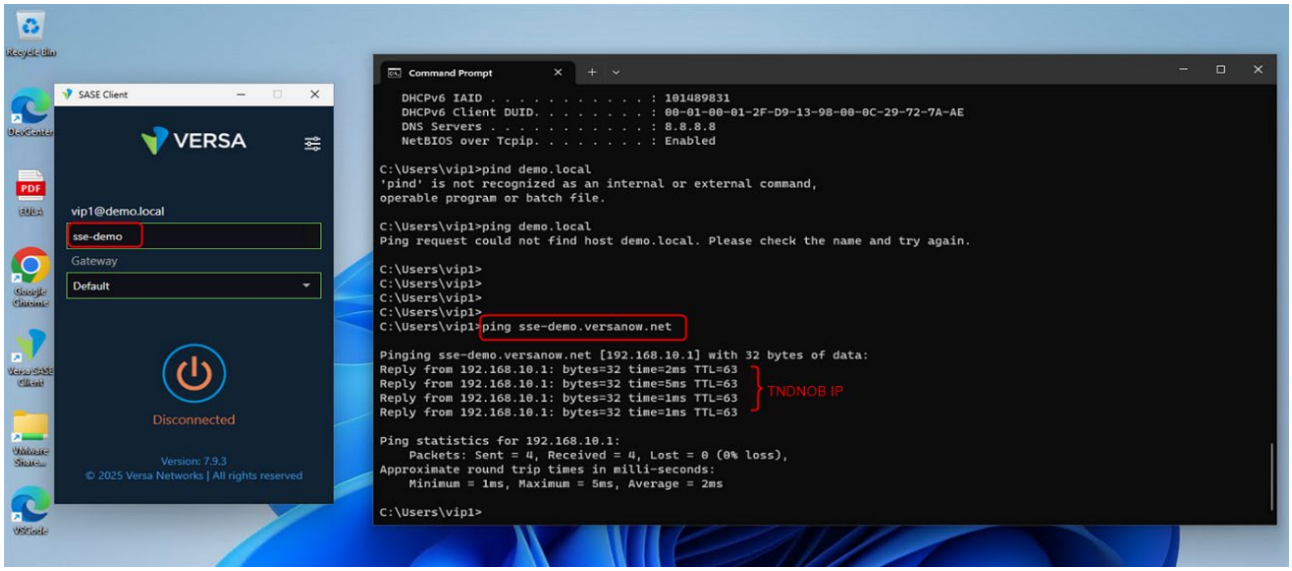
3. **Identify TNDNOB TVI IP:** On the SASE Gateway, run the command "*show interfaces brief*"

```
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
```

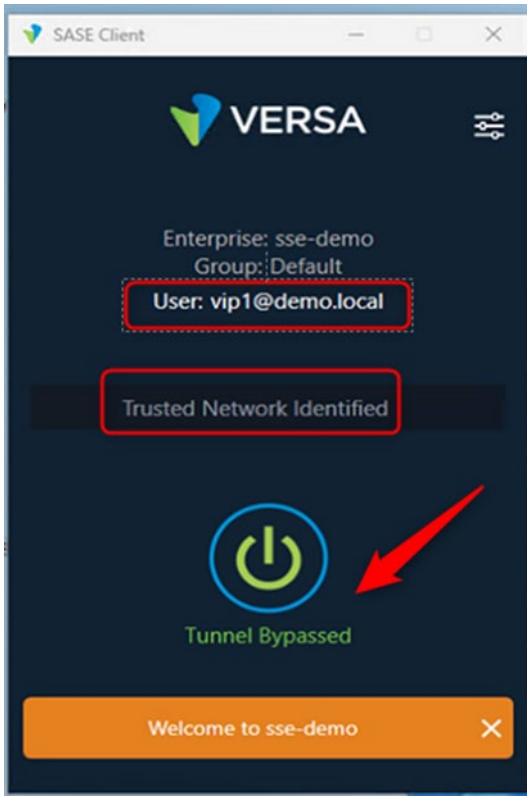
*It is important to mention that Versa assigns for TND the first IP address from the **"Client Address Pool"** that was defined during the tenant creation.*

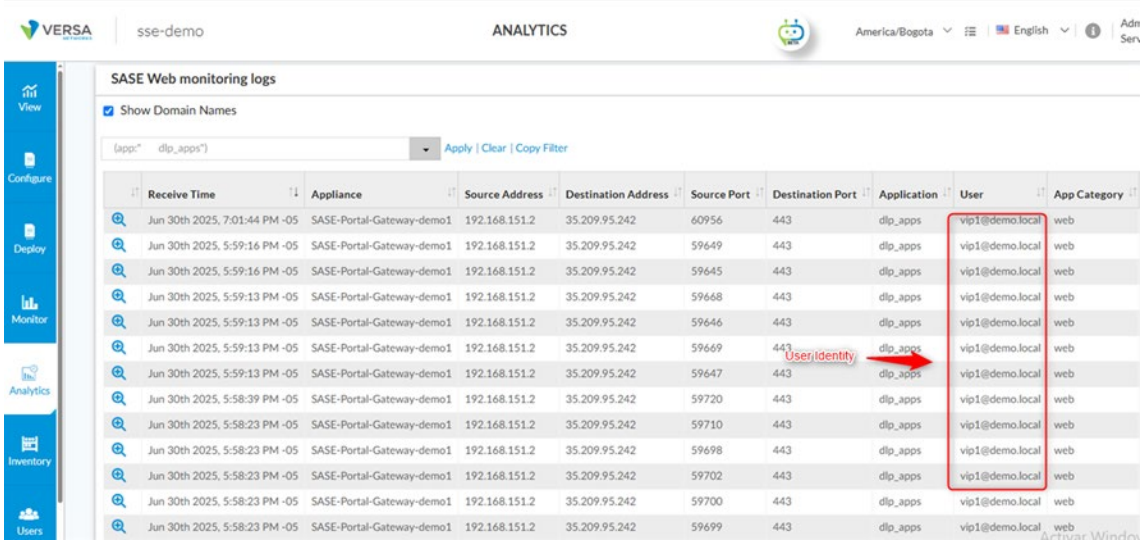
Verification Steps

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

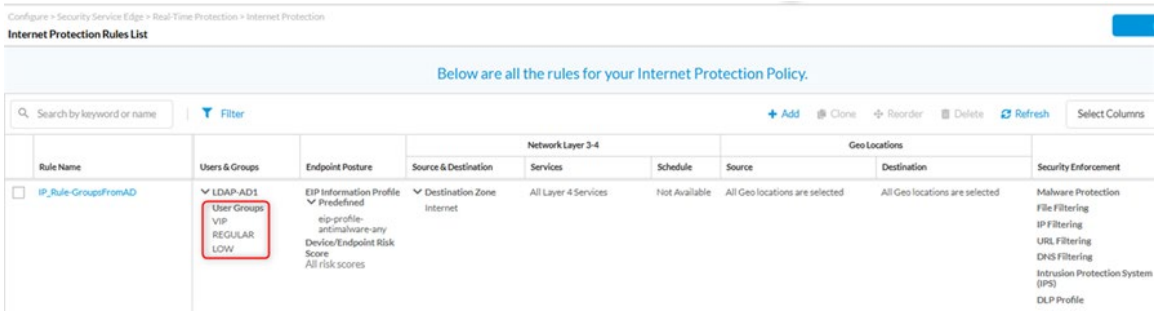


- Register and connect to the SASE portal, then verify the user's identity from Concerto (Analytics).

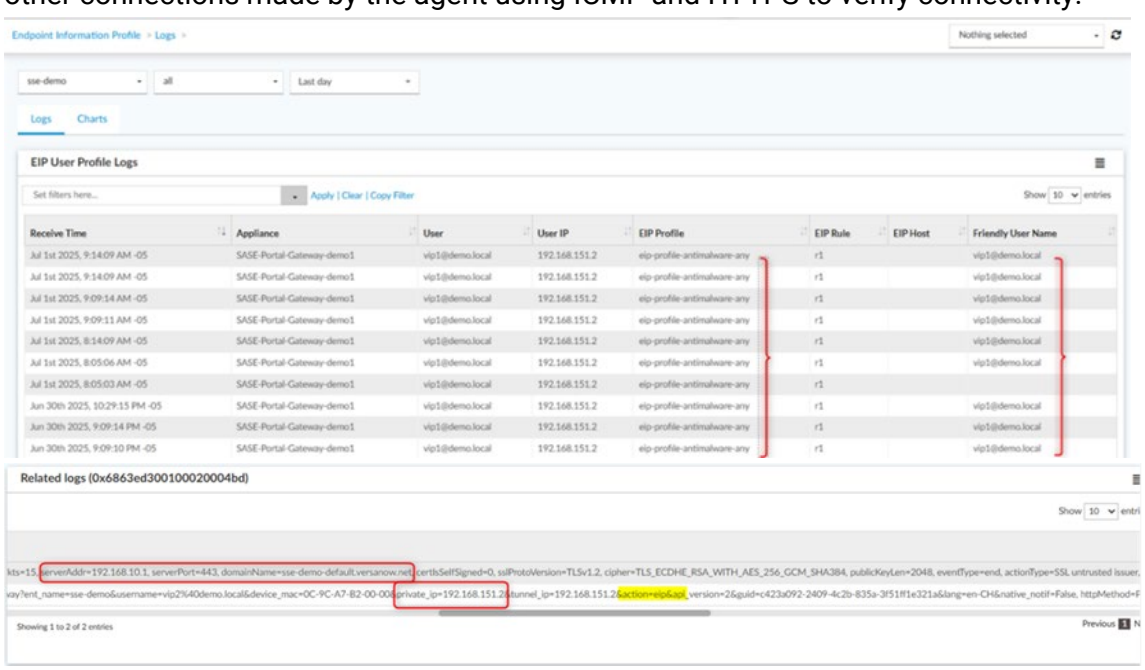




- You can now create real-time protection rules based on user identity, either by using the group or the user as the source.



- 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.



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.