Optimizing SSE Connectivity with Trusted Network Detection (TND) and Trusted Network Host (TNH)

Adaptive tunnelling control for consistent SSE policy enforcement and seamless user experience

Executive summary

From a corporate internet breakout perspective, **Security Service Edge (SSE)** Gateways provide centralized and consistent security enforcement across user locations. Compared with traditional local or branch-based breakouts, SSE Gateways simplify policy management, improve compliance, and deliver advanced cloud-native protection.

Enterprises typically adopt one of two primary **architecture models** when connecting end users to SSE Gateways:

1. **Branch to SSE Gateway**
2. **Remote User to SSE Gateway**

Both models utilize identical security capabilities through the SSE Gateway; the key difference is where user traffic originates - either from a fixed branch office or from a remote endpoint. When both models are in use, optimizing how remote users behave on trusted branch networks becomes critical to maintaining performance, visibility, and security alignment.

In many organizations, these architecture models coexist, and remote users frequently connect their devices to trusted branch networks. Without optimization, SASE clients may still build VPN tunnels to the SSE Gateway over an already secured branch path, causing redundant encryption, increased latency, and reduced branch visibility. To address this, Versa provides two mechanisms - Trusted Network Host (TNH) and Trusted Network Detection (TND) - that allow the SASE client to recognize when it is on a trusted enterprise network and suppress unnecessary tunnels.

While both TNH and TND prevent redundant tunnelling at trusted sites, they differ in how deeply they integrate with the SSE Gateway. TNH offers a simple, client-side trusted network check based on reachability to an internal host, improving efficiency but without sharing user identity or posture with the gateway. TND, by contrast, establishes a gateway-assisted trust relationship in which the user is authenticated and the endpoint's security posture is assessed and maintained even when on a trusted network, aligning the optimization with the enterprise's Zero Trust principles.

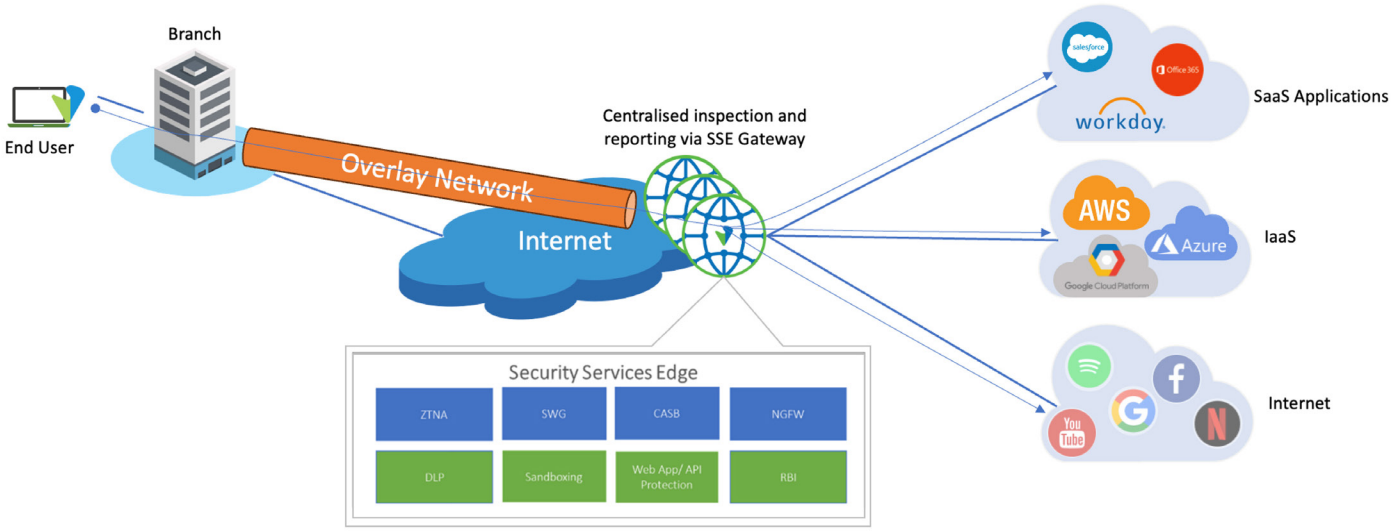
Architecture models

Architecture model 1 - Branch to SSE Gateway

Branch offices connect to SSE Gateways via secure overlay networks, providing centralized inspection and control when accessing SaaS, IaaS, and Internet resources. This model streamlines routing while keeping policies consistent with the enterprise's security framework.

Key characteristics (as depicted by the diagram below):

- Branch edge devices form an overlay tunnel (e.g. SDWAN, IPsec or GRE) to the SSE Gateway
- All outbound traffic (including Internet and cloud apps) passes through centralized inspection
- Policies and reporting remain uniform for all branch users

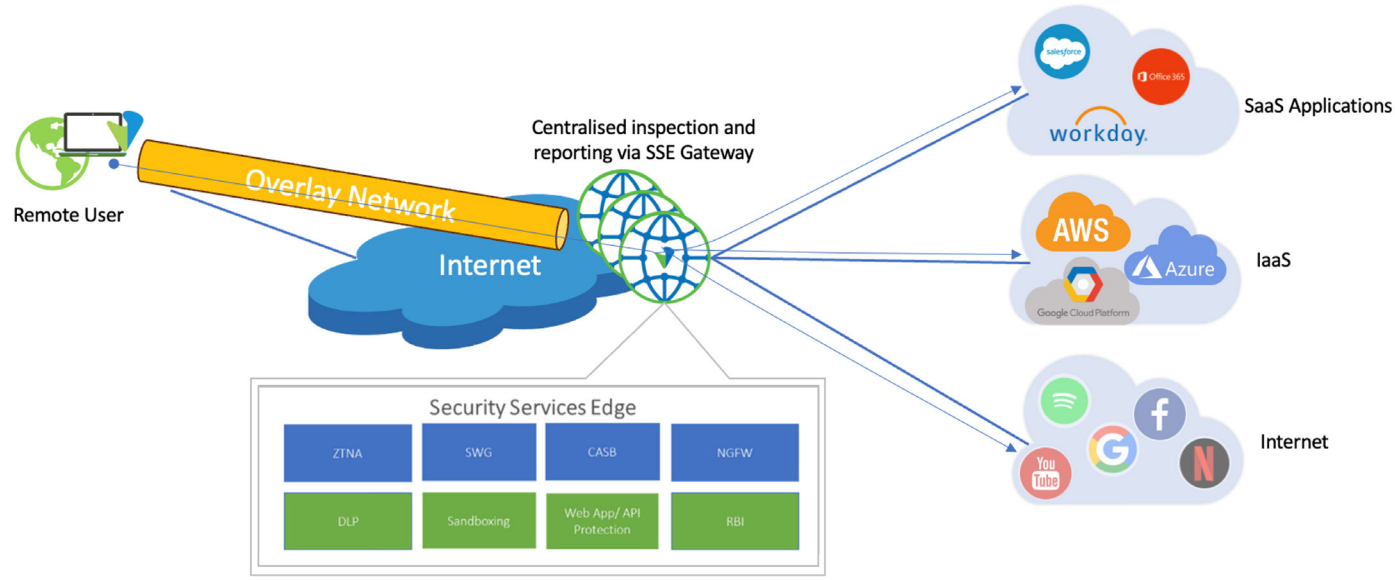


Architecture model 2 - Remote User to SSE Gateway

Remote Users rely on the **SASE client** installed on their endpoints (e.g., Windows, macOS, iOS, Linux) to create a secure VPN tunnel directly to the SSE Gateway. This approach ensures that remote users receive the same policy enforcement as those in branch offices.

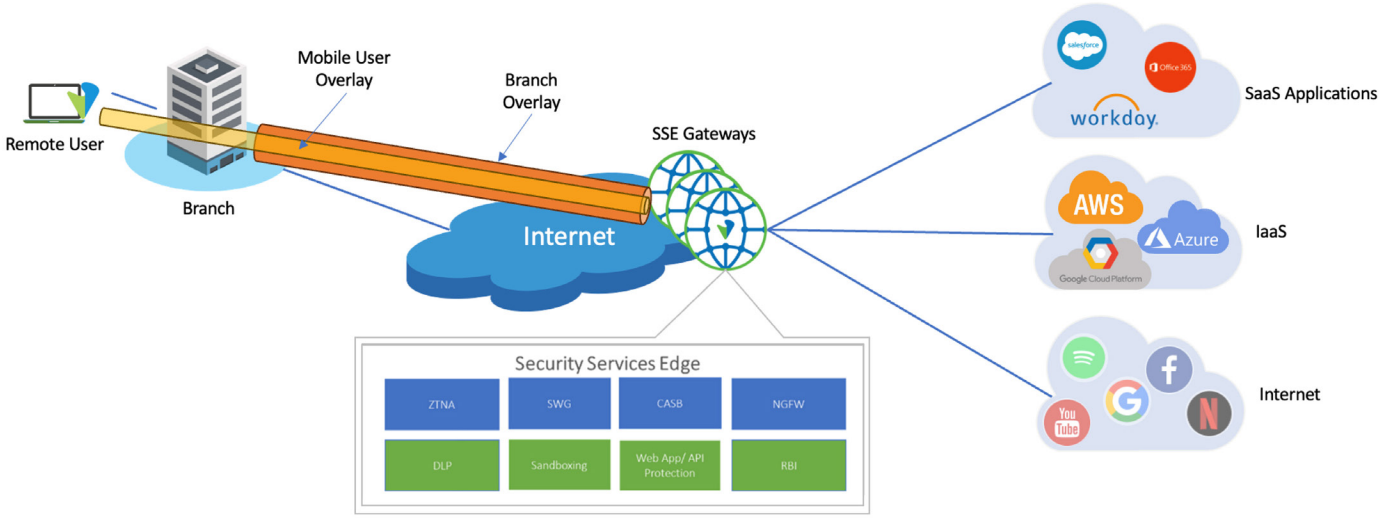
Key characteristics (as depicted by the diagram below):

- The SASE client builds a tunnel (e.g. IPSEC, DTLS or TLS) to the nearest SSE Gateway
- All outbound traffic passes through the Gateway for inspection and enforcement
- Consistent user identity and posture validation are maintained across any network



The hybrid challenge: Remote users at branch locations

In many enterprises, Remote Users frequently connect their portable devices to trusted branch networks. Without optimization, these users' SASE clients still attempt to create a tunnel to the SSE Gateway, even when already inside a trusted site. For example, in the following diagram, the Remote User builds an overlay network which is transported over the branch overlay network to reach the SSE Gateways:



This behaviour introduces **performance inefficiencies and visibility challenges**, such as:

- **Redundant tunnelling** causing unnecessary encryption and double encapsulation
- **Increased latency**, especially for locally hosted or branch-optimized applications
- **Obscured visibility**, since traffic inside a Remote User tunnel is opaque to branch monitoring systems
- **Higher bandwidth consumption**, impacting branch WAN utilization
- **Increased device resource usage**, reducing mobile device battery life

To mitigate these effects, the SASE client can automatically determine whether it is connected to a trusted network and adapt its behaviour accordingly. Versa Networks provides two mechanisms to achieve this: **Trusted Network Host** and **Trusted Network Detection**.

Trusted Network Host (TNH)

TNH is a lightweight 'client-side' mechanism that allows the SASE client to decide whether it is connected to a trusted network by verifying reachability to a specific **internal host**.

How TNH works

1. The administrator configures an internal-only FQDN or IP address as the Trusted Host
2. Before attempting to connect to the SSE Gateway, the SASE client pings this Host
3. If the Host responds successfully, the client assumes the network is trusted and suppresses tunnel creation
4. If the Host does not respond, the network is considered untrusted, and the client proceeds to create a VPN tunnel to the SSE Gateway

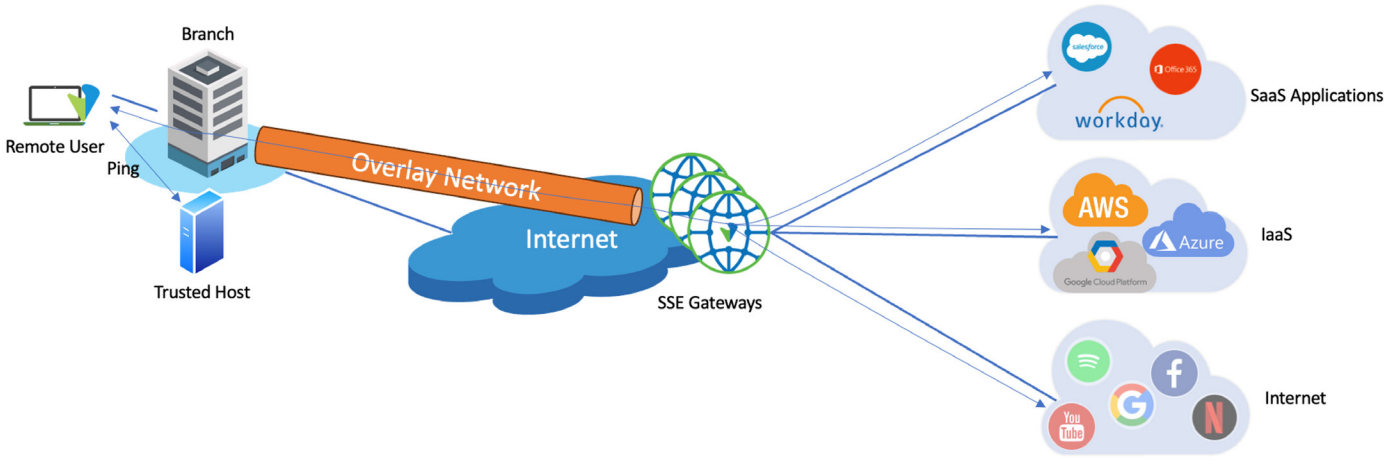
Best practice: Mitigating single endpoint risk in TNH

Relying on a single Trusted Network Host creates a single point of failure - if the host is offline, under maintenance, or unreachable, the SASE client incorrectly classifies the trusted branch as untrusted and builds unnecessary VPN tunnels.

Recommended mitigations:

- Use a highly available FQDN resolving to a Virtual IP (VIP) for critical services like internal DNS
  - (DNS is an ideal candidate for TNH due to its 99.9% uptime, universal reachability, and native redundancy across enterprise networks).
- Alternatively, DNS Anycast can be used as the TNH
- Temporary FQDN changes should be considered during trusted host maintenance (NOTE – this requires SASE client re-registration to the SSE Gateway to download the amended TNH configuration. Re-registration is automatically performed by default every 24 hours although configurable)

Example scenario



As shown in the figure above, a Remote User connects to a corporate branch Wi-Fi network. The SASE client pings an internal server configured as the Trusted Host. The ping succeeds, so the client concludes the branch network is trusted and bypasses tunnel creation. All traffic continues to route through the branch overlay toward the SSE Gateway, maintaining enterprise-wide policy consistency.

Benefits of TNH

- Eliminates unnecessary VPN tunnels and double encryption
- Reduces latency and improves user performance
- Preserves visibility and policy enforcement at the branch
- Saves WAN bandwidth and device battery life

Limitations of TNH

While TNH provides a basic and effective method of trusted network identification, it has limited integration with ZTNA-based features on the SSE Gateway:

- Users appear as unknown in policy and reporting dashboards
- No authentication or posture data is shared with the SSE Gateway
- Additional configuration would be required to correlate Remote User identity

Trusted Network Detection (TND)

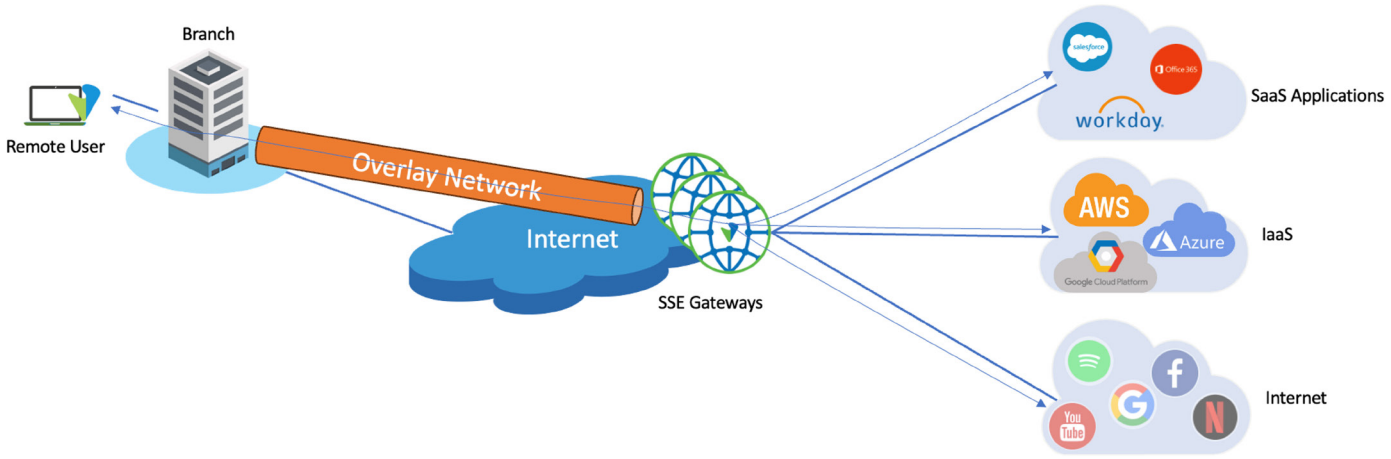
TND provides an advanced, integrated mechanism for trusted network identification. Unlike TNH - which performs simple client-side connectivity tests to a local host - TND establishes bidirectional awareness between the **SASE client**

and **SSE Gateway** through private IP resolution and trust metadata exchange. While TNH operates purely at the client level, TND leverages **gateway-assisted validation**.

How TND works

1. The SASE Client resolves the SSE Gateway FQDN to a **private IP address** that is accessible only through the enterprise network (for example, via internal DNS resolution or a DNS proxy on the SSE Gateway)
2. This private IP address is the **first address in the tenant's SASE Client pool** and is **unique to each SSE Gateway**
3. Because routing between the enterprise network and the SSE Gateway is already established, **no additional routing configuration** is required to advertise this private IP address internally
4. The SASE Client then sends registration data to the SSE Gateway
5. The SSE Gateway validates the connection and marks the network as trusted
6. The SASE Client suppresses tunnel creation while maintaining a secure control channel (HTTPS) with the SSE Gateway
7. User authentication, posture verification, and reporting continue seamlessly over this control channel

Example scenario



As shown in the figure above, a Remote User connects to a corporate branch LAN where, in this example, internal DNS resolution returns a private IP address for the SSE Gateway. The client communicates successfully with this address, receives the trusted network flag, and suppresses the tunnel. The user remains authenticated, and the SSE Gateway continues posture checks and policy enforcement based on control-plane data.

Benefits of TND over TNH

- Users remain authenticated on the SSE Gateway as known users
- Full user reporting and policy tracking remain intact
- Endpoint posture information is shared for Zero Trust compliance enforcement

NOTE - Additional configuration requirements for TND

When implementing TND, the enterprise administrator must configure Internet Protection Rules on the SSE Gateway to explicitly allow communication between Remote Users and the enterprise's authentication servers. By default, this traffic may be blocked by the Gateway's security policies. For example, if users authenticate via Microsoft Entra ID using SAML, rules must be defined to permit traffic between the user and Entra ID through the Gateway's ingress and egress zones.

Feature comparison

Advantage	Trusted Network Host (TNH)	Trusted Network Detection (TND)
Overlay tunnel suppression at trusted sites	✓	✓
Improved performance/reduced latency	✓	✓
Bandwidth efficiency (no double encapsulation)	✓	✓
Branch level visibility preserved	✓	✓
Remote User authentication on SSE Gateway[1]	✗	✓
User posture and compliance shared - aligning with Zero Trust	✗	✓
Users appear as 'known' in logs and reporting	✗	✓
Supported OS platforms	Android, ChromeOS, Linux; macOS, Windows	Android, ChromeOS, Linux; macOS, Windows
Configuration Complexity	Low – simple host reachability check configuration	Moderate – requires additional SSE Gateway policy adjustments to permit authentication flows
Best Suited for	Simple trusted branch detection	Integrated authentication and policy frameworks

[1] optionally, user authentication may be configured for traffic from branches. This would include Remote Users using the TNH feature (Configure User and Device Authentication)

Summary and recommendations

For enterprises adopting SSE and SASE architectures, optimizing how mobile and branch traffic is categorized and routed can significantly improve user experience and operational efficiency.

- **TNH** is best suited for simpler environments or as an initial deployment phase where trusted branch network identification is sufficient. It requires minimal configuration and effectively prevents redundant tunnels
- **TND** is a more advanced and integrated approach ideal for organizations requiring user identity continuity, posture enforcement, and unified analytics whether users are remote or on site.

Both methods contribute to seamless secure access by ensuring the SASE client only establishes tunnels when needed. By implementing either mechanism - or combining both where applicable -organizations can achieve a balance of **security, performance, and visibility** across fixed and mobile network environments.

Further references

For detailed configuration guidance and integration examples, refer to:

- Versa Gateway Assisted Trusted Network Detection (TND)
- Configure Detection of Trusted Networks for SASE Gateways

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, a 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.

Part# TB_SSECNCT-TND-TNH-01.0