netskope

Reference Architecture

Netskope Reference Architecture Guide

How to Use Zero Trust Network Access as a Replacement for VPN with Netskope ZTNA Next

CONTENTS

WHO THIS GUIDE IS FOR

This document is intended to provide an overview of the Netskope ZTNA Next solution, answering the questions about why it is important, when it is needed, and how it works at a high level in a single document. It will demonstrate:

- What is ZTNA Next
- The benefits of ZTNA Next
- The use cases for ZTNA Next

Note: This document is not intended to be used as a deployment and troubleshooting guide.

NAMING CONVENTIONS USED IN THIS GUIDE

Netskope Private Access has been renamed to **Netskope ZTNA Next L7**, and Netskope Endpoint SD-WAN is now **Netskope ZTNA Next L3E or Layer 3 Evolution**, aligning with our vision for evolving zero trust application access. Additionally, **Netskope ZTNA Next 360** has been introduced, integrating the capabilities of both ZTNA Next L7 and ZTNA Next L3E into a single, unified Secure Access Service Edge (SASE) offering.

Limitations of Classic ZTNA Architecture

Built with zero trust principles, Zero Trust Network Access (ZTNA) has emerged as a modern alternative to remote access VPN. Using a cloud-hosted broker between users and resources, cloud-delivered ZTNA services authenticate and validate a user's authorization before connectivity. The user and application traffic meets in the middle, creating a secure connection that is an isolated user-to-application segment.

Cloud-delivered ZTNA has many benefits: scalability of the cloud service, simplified network connectivity, and most importantly, enhanced performance and security thanks to direct, logical connectivity and zero trust principles.

However, a key limitation of many cloud-delivered ZTNA solutions is that their architectures only permit client-initiated application traffic. This creates a challenge for critical applications that require server-initiated traffic flow, such as on-premises hosted Voice over Internet Protocol (VoIP). With legacy applications, this limitation creates two challenges:

1. **Traffic direction is client-initiated.** Cloud-delivered ZTNA requires client-initiated application traffic and does not permit server-initiated traffic, which means it cannot serve legacy applications such as:

    - **Legacy Help Desk** solutions that require server-initiated traffic to initiate remote assistance (based on VNC, RDP, or custom protocols).
    - **Legacy Endpoint Management and Patching** solutions that rely on server-initiated traffic to manage and patch endpoints.
    - **Legacy VoIP** solutions that rely on server-to-client and client-to-client communications (Enterprise UC/IP PBX).
    - **Legacy applications and scripts** relying on server-to-client communications (i.e., hard-coded logic with server-initiated traffic to client IP address).

    All the applications above rely on traffic that is initiated by a machine located inside the network and destined to a machine that is located outside the network. Traditionally those communications are enabled through the use of a VPN solution, which makes it possible to route from the internal network to the remote endpoint, through the VPN IP that the Client would be granted inside the network.

2. **Endpoint IP addresses are masked.** This means that ZTNA does not work for applications that require initiating traffic towards the endpoint's IP address, such as legacy forensic tools.

    As a result, many organizations are using ZTNA and VPNs in tandem until they can upgrade their application infrastructure. In effect, this has meant that organizations' legacy applications cannot be free of the security risks and performance challenges associated with VPNs.

Introducing Netskope ZTNA Next

Delivered as a single solution, Netskope ZTNA Next integrates Zero Trust Network Access (ZTNA) and software-defined wide-area networking (SD-WAN) capabilities, enabling the complete retirement — not just partial replacement — of remote access VPNs for all relevant application access use cases, while enhancing security posture and boosting remote worker productivity with secure and seamless connectivity.

The unified Netskope Client sits in front of a converged architecture comprising Netskope ZTNA Next L7 for access to client-initiated applications, and Netskope ZTNA Next L3E to securely connect applications that require bi-directional, server-initiated traffic. The same Netskope Client enables every other client inline Netskope service: NG-SWG, CASB Inline, Cloud Firewall, DNS Security, Endpoint DLP.

The solution utilizes zero trust principles to enhance overall security posture and reduce lateral threat movement, reduce deployment complexity, and optimize performance, and it enables ubiquitous access to corporate resources hosted anywhere through intelligent traffic steering. With ZTNA Next, organizations can avoid maintaining separate ZTNA and VPN clients, and instead provide consistent security for all applications with a unified client deployment.

Key Benefits

Enforces Zero Trust Principles

ZTNA Next incorporates zero trust principles and proposes a shift from traditional network-centric access control to granular application-centric access control on a per-user or user group basis. The solution accelerates the time frame for decommissioning legacy applications and minimises associated security risks, including unauthorized lateral movement. Key benefits include:

- Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers.
- Device Classification options to assess the posture of the client before providing access to private applications hosted in public clouds or on-premises data centers.
- Facilitating the connectivity through the ZTNA broker in Netskope security cloud. The applications are hidden from discovery, and access is restricted only to authenticated and authorised users.
- Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius.
- Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks.

Secures All Enterprise Applications

ZTNA Next also supports server-to-client traffic connectivity, enabling access to both legacy and modern applications through a single client. Key benefits include:

- Eliminating the need to maintain two separate solutions — VPN and ZTNA — for accessing all private applications and achieving greater cost savings by reducing capital and operational expenditure.
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications.

Delivers a Phenomenal User Experience

ZTNA Next provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:

- Automatic traffic steering by the Netskope Client for connecting authorised users directly to specific resources regardless of where it is hosted. Strategically positioned Netskope NewEdge Network point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access.
- Browser (Clientless) access connecting authorised external, third-party users directly to specific resources regardless of where it is hosted. Strategically positioned Netskope NewEdge Network point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access.
- Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.

Provides Full Visibility and Control

ZTNA Next provides real-time visibility into detailed application traffic and user activities across the highly distributed environments, as well as alerting on policy violations, to reduce business risks and protect data. Key benefits include:

- Deep visibility into user access, applications usage, and traffic patterns to detect unusual user activity and prevent threats.
- Enforcing context-aware policies with deep understanding of content and context including user identity, user risk, device identity, device posture, and app risk.
- Simplifying operations with automated troubleshooting, proactive support, and insights into traffic flows and policies.

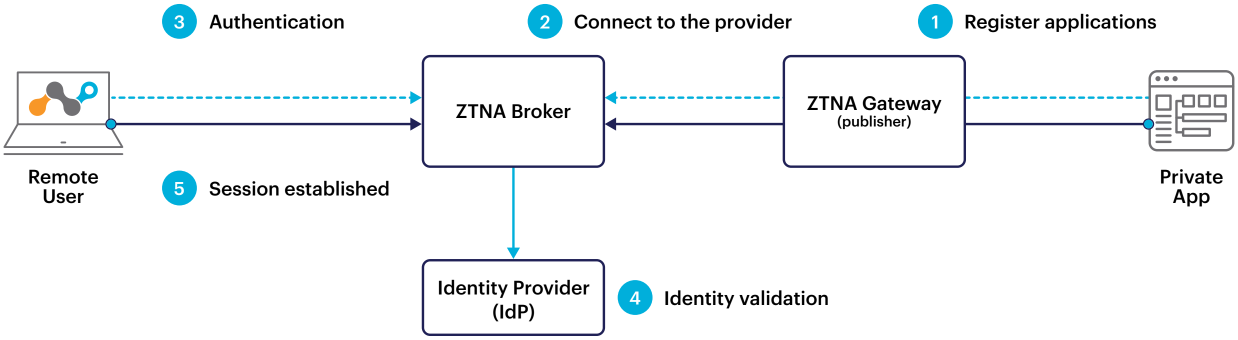
SOLUTION ARCHITECTURE

In this section we'll detail how the components of ZTNA Next work together to address the most common ZTNA use cases, and we'll close by providing an overview of how the two components work together to satisfy all the use cases for a VPN replacement.

Client-Initiated Connectivity: Netskope ZTNA Next L7

Netskope ZTNA Next L7 connects users anywhere to private resources hosted on-premises or in the cloud, ensuring fast and direct application connectivity and superior user experience.

With the ZTNA Next L7 architecture, private resources remain invisible to discovery and attacks. Authenticated users gain secure direct access to authorized applications over application tunnels that are encrypted using TLS.



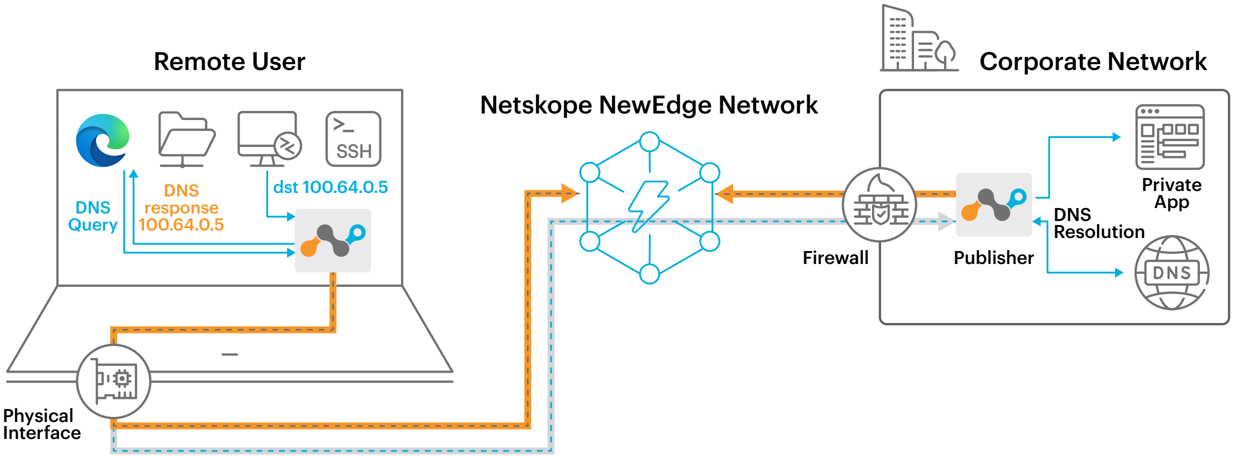
Terms and Definitions

- **Netskope Client:** The Netskope Client is a simple lightweight application that steers traffic from the end-user device to Netskope Cloud. It provides real-time visibility of the managed devices accessing the Web, SaaS applications, Private Applications, and SD-WAN destinations from any location.
- **Netskope Publisher:** The Netskope ZTNA Next L7 Publisher is a software package that is deployed in the Customer's premises (aka "border"), whether in an on-premises network, a Data Center, or Public Cloud. The Publisher enables private application connectivity between the Customer's premises and the Netskope cloud. The Netskope Publisher has both connectivity toward the Private Application (whatever protocol and port) and connectivity toward the Netskope NewEdge Network PoPs to establish the ZTNA Next L7 TLS tunnel toward the closest Netskope PoP.

- **Private Application:** The Netskope ZTNA Next L7 Private Application is an application that resides inside the Customer's premises (aka "border"), whether in an on-premises network, a Data Center, or Public Cloud. A Private Application is configured defining the following parameters:
  - **Name:** Private Application name
  - **Host:** FQDN(s), Wildcard Domains and Subdomains, IP addresses, IP Ranges, CIDR(s) of the application(s) to publish
  - **Protocol & Port:** TCP and/or UDP ports and/or ranges used by the application(s) to publish
  - **Publisher:** List of ZTNA Next L7 Publishers that will serve the Private Application
  - **Stub IP:** IP address that belongs to the CGNAT-reserved IP range 100.64.0.0/10, arbitrarily assigned to a configured Private Application when not configured to use the "Publisher DNS" option
  - **Private Application Tag:** Tag(s) associated to the Private Applications that will be used in Real-Time Protection policies to manage user's access to the Private Application
- **Steering Configuration:** A steering configuration controls what kind of traffic gets steered to Netskope for real-time deep analysis and what kind of traffic gets bypassed. It's for endpoints using the Netskope Client and directs traffic from end-users to the Netskope Cloud.
- **Real-Time Protection Policy:** Connections to Private Applications are not allowed by default, so a user is not notified when that private app is inaccessible. Real-Time Protection policies, an essential component of the Netskope Zero Trust Engine, are required to enable access to Users, Groups, or Organizational Units (OUs) and to log the events. Real-time Protection policies are used to:
  - Grant access to a private app for users, groups, or OUs
  - Block access and notify the user(s) why access is denied
  - Block access but provide instructions to gain access, such as contacting IT or upgrading a device
  - Use a DLP profile to get Page Events, Alerts, and DLP Incidents data for private apps
- **Netskope PoP:** A Netskope Data Center part of the Netskope NewEdge Network.

+ Use Case 1 Client Access to Applications Requiring DNS Resolution Masquerading the Application IP Address

In this use case, remote endpoints need to access a Private Application via its FQDN. This is the default Netskope ZTNA Next L7 application configuration for what concerns FQDN resolution and it involves the use of a Stub IP. The advantages of this configuration are that there is no need to configure any IP address of the target application, greatly simplifying the configuration and the management of Private Applications, and it also allows configuring Private Applications that reside in different networks with overlapping IP addresses. Supported features and limitations:



+ The flow of the connection will be:

1. A Netskope Publisher (more than one as per best practices) has been deployed on the network where the Private Application resides, whether in the same subnet or a different one, depending on the micro-segmentation requirements of the customer.
2. A Private Application defined by FQDN (wildcard of domains/subdomains are also allowed) has been configured and associated to the Netskope Publisher(s) that will be used to connect to the Private Application.
3. The Private Application has been included on the Steering Configuration that applies to the user.
4. The Private Application has been explicitly allowed on the Netskope Zero Trust Engine through a Real-Time Protection policy for the users/groups that are authorized to access it, provided they comply with other zero trust criteria, such as Endpoint Posture Check, Operating System, etc.
5. The user logs into the remote endpoint and the Netskope Client synchronises the Steering Configuration and the Private Applications definitions, then it establishes the ZTNA Next L7 TLS tunnel toward the closest Netskope PoP.

+ The flow of the connection will be (cont.):

6 The Netskope Client measures with a cadence of 5 minutes the RTT toward all the Publishers serving all the Private Applications synchronised, selecting for each Private Application only the Publishers that are in the lowest "bucket" of RTT times, hence closer. The Netskope Client then synchronises the selected Publisher list to the ZTNA Next L7 service in the Netskope PoP, so the latter will know what is the group of Publishers it must use to connect the Client to every defined Private Application.

7 The user initiates a connection to the Private Application using the FQDN of the Application.

8 The remote endpoint initiates a DNS request for the FQDN requested.

9 The Netskope Client filters the DNS requests, and if it matches the FQDN requested with the one specified on a Private Application assigned to the user via the Steering Configuration, it resolves the DNS query with a Stub IP address associated to the Private Application.

10 The remote endpoint initiates the application traffic toward the resolved Stub IP address.

11 The Netskope Client matches the Stub IP, the protocol, and port, and if they match the ones specified on a Private Application assigned to the user via the Steering Configuration, it encapsulates (steers) the traffic inside the ZTNA Next L7 TLS tunnel alongside other info such as the original FQDN requested by the client.

12 The Private Application traffic reaches the Netskope PoP, where the ZTNA Next L7 service applies the Real-Time Protection policies based on the contextual info. If the conditions don't satisfy the policy, the connection is dropped on the Netskope PoP (and it never reaches the internal network).

13 If the conditions satisfy the policy, the packet must be routed to the destination. The ZTNA Next L7 service is aware of what is (are) the Publisher(s) serving the specific Private Application:

a. If the Netskope Client and the Publisher(s) serving the Private Application are connected to the same Netskope PoP, ZTNA Next L7 will choose the Publisher to use based in a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, and it will "stitch" the Client and Publisher TLS tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the Private Application traffic to the selected Publisher.

b. If the Publisher(s) serving the Application are connected to a different Netskope PoP than the Netskope Client, the ZTNA Next L7 service will choose the Publisher to use based on a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, it will create a third TLS tunnel between the Netskope PoPs where the Client and the Publisher are connected, it will "stitch" the three tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the Private Application traffic to the selected Publisher.

14 The Netskope Publisher that receives the Private Application traffic performs a DNS resolution for the FQDN passed by the Netskope Client the corporate DNS server(s) configured and resolves the real local IP of the Private Application.

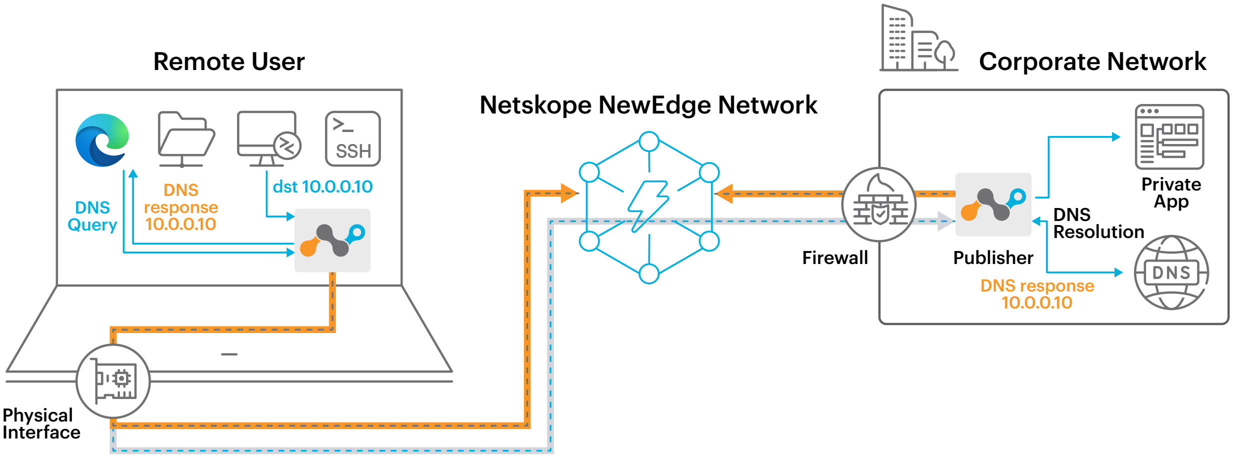
15 The Netskope Publisher then performs a Source and Destination NAT and sends the Private Application traffic to the IP of the Private Application using its local IP address.

16 The Private Application will respond to the Netskope Publisher, which in turn performs a Source and Destination NAT and forwards the response to the remote endpoint through the end-to-end encrypted tunnel.

17 The remote endpoint and the Application are able to communicate with each other.

+ Use Case 2 Client-based Access to Applications Requiring DNS Resolution Using the Application IP Address

In this use case, remote endpoints need to access a Private Application via its FQDN. With this configuration the FQDN requested by the remote endpoint will be resolved with the real local IP address of the Private Application. Some Private Applications don't work properly when there is a NAT and/or they rely on specific DNS resolutions that must provide specific IP addresses (for instance, Active Directory Domain Services). With this configuration we are able to support such Private Applications. However, this use case requires additional configuration steps, namely the need to specify both the FQDN and the real IP address of the Application. Moreover, as we must configure the real IP of the application, this use case doesn't support overlapping networks addressing.



+ The flow of the connection will be:

1. A Netskope Publisher (more than one as per best practices) has been deployed on the network where the Private Application resides, whether in the same subnet or a different one, depending on the micro-segmentation requirements of the customer.

2. A Private Application defined by FQDN (wildcard of domains/subdomains are also allowed) and the respective real IP addresses of the Private Application have been configured and associated to the Netskope Publisher(s) that will be used to connect to the Private Application.

3. The Private Application has been included on the Steering Configuration that applies to the user.

4. The Private Application has been explicitly allowed on the Netskope Zero Trust Engine through a Real-Time Protection policy for the users/groups that are authorized to access it, provided they comply with other zero trust criteria, such as Endpoint Posture Check, Operating System, etc.

5. The user logs into the remote endpoint and the Netskope Client synchronises the Steering Configuration and the Private Applications definitions, then it establishes the ZTNA Next L7 TLS tunnel toward the closest Netskope PoP.

+ The flow of the connection will be (cont.):

6 The Netskope Client measures with a cadence of 5 minutes the RTT toward all the Publishers serving all the Private Applications synchronised, selecting for each Private Application only the Publishers that are in the lowest "bucket" of RTT times, hence closer. The Netskope Client then synchronises the selected Publisher list to the ZTNA Next L7 service in the Netskope PoP, so the latter will know what is the group of Publishers it must use to connect the Client to every defined Private Application.

7 The user initiates a connection to the Private Application using the FQDN of the Application.

8 The remote endpoint initiates a DNS request for the FQDN requested.

9 The Netskope Client filters the DNS requests, and if it matches the FQDN requested with the one specified on a Private Application assigned to the user via the Steering Configuration, it encapsulates (steers) the DNS request to the ZTNA Next L7 TLS tunnel.

10 The ZTNA Next L7 service on the Netskope PoP sends the DNS request to the chosen Publisher:

a. If the Netskope Client and the Publisher(s) serving the Private Application are connected to the same Netskope PoP, ZTNA Next L7 will choose the Publisher to use based in a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, and it will "stitch" the Client and Publisher TLS tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the DNS request to the selected Publisher.

b. If the Publisher(s) serving the Application are connected to a different Netskope PoP than the Netskope Client, the ZTNA Next L7 service will choose the Publisher to use based on a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, it will create a third TLS tunnel between the Netskope PoPs where the Client and the Publisher are connected, it will "stitch" the three tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the DNS request to the selected Publisher.

11 The Publisher will forward the DNS query to the corporate DNS server(s) configured and resolves the real local IP of the Private Application.

12 The DNS resolution is forwarded to the remote endpoint via the ZTNA Next L7 TLS tunnel, so the remote endpoint resolves the FQDN of the application with the real IP address of the Private Application.

13 The remote endpoint initiates the application traffic toward the resolved IP address.

14 The Netskope Client matches the IP, the protocol, and port defined on the Private Application, and if they match the ones specified on a Private Application assigned to the user via the Steering Configuration, it encapsulates (steers) the traffic inside the ZTNA Next L7 TLS tunnel alongside other info such as the original FQDN requested by the client.

15 The Private Application traffic reaches the Netskope PoP, where the ZTNA Next L7 service applies the Real-Time Protection policies based on the contextual info. If the conditions don't satisfy the policy, the connection is dropped on the Netskope PoP (and it never reaches the internal network).

16 If the conditions satisfy the policy, the packet must be routed to the destination. The ZTNA Next L7 service sends the Private Application traffic on the same end-to-end tunnel to the same Publisher used for the DNS resolution.

17 The Netskope Publisher then performs a Source NAT and sends the Private Application traffic to the IP of the Private Application using its local IP address.

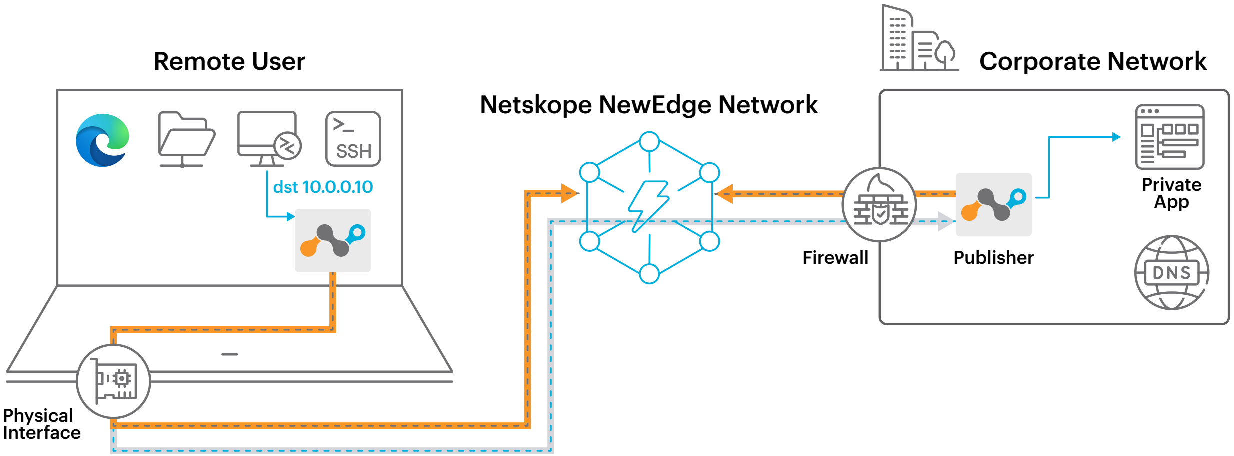
18 The Private Application will respond to the Netskope Publisher, which in turn performs a Destination NAT and forwards the response to the remote endpoint through the end-to-end encrypted tunnel.

19 The remote endpoint and the Private Application are able to communicate with each other.

+ Use Case 3

Client-based Access to Applications without DNS Resolution

Although in modern environments Applications are accessed by users via their FQDN, there are still circumstances where users need to access Applications using an IP address, whether for habit or due to simplicity of the implementation. In this use case, remote endpoints need to access a Private Application via its internal IP address.



+ The flow of the connection will be:

1. A Netskope Publisher (more than one as per best practices) has been deployed on the network where the Private Application resides, whether in the same subnet or a different one, depending on the micro-segmentation requirements of the customer.

2. A Private Application defined by IP address (CIDR, ranges are also allowed) has been configured and associated to the Netskope Publisher(s) that will be used to connect to the Private Application.

3. The Private Application has been included on the Steering Configuration that applies to the user.

4. The Private Application has been explicitly allowed on the Netskope Zero Trust Engine through a Real-Time Protection policy for the users/groups that are authorized to access it, provided they comply with other zero trust criteria, such as Endpoint Posture Check, Operating System, etc.

5. The user logs into the remote endpoint and the Netskope Client synchronises the Steering Configuration and the Private Applications definitions, then it establishes the ZTNA Next L7 TLS tunnel toward the closest Netskope PoP.

6. The Netskope Client measures with a cadence of 5 minutes the RTT toward all the Publishers serving all the Private Applications synchronised, selecting for each Private Application only the Publishers that are in the lowest "bucket" of RTT times, hence closer. The Netskope Client then synchronises the selected Publisher list to the ZTNA Next L7 service in the Netskope PoP, so the latter will know what is the group of Publishers it must use to connect the Client to every defined Private Application.

7. The user initiates a connection to the Private Application using the internal IP address of the Application.

+ The flow of the connection will be (cont.):

8 The Netskope Client matches the IP, protocol, and port defined on the Private Application, and if they match the ones specified on a Private Application assigned to the user via the Steering Configuration, it encapsulates (steers) the traffic inside the ZTNA Next L7 TLS tunnel.

9 The Private Application traffic reaches the Netskope PoP, where the ZTNA Next L7 service applies the Real-Time Protection policies based on the contextual info.
If the conditions don't satisfy the policy, the connection is dropped on the Netskope PoP (and it never reaches the internal network).

10 If the conditions satisfy the policy, the packet must be routed to the destination:

a. If the Netskope Client and the Publisher(s) serving the Private Application are connected to the same Netskope PoP, ZTNA Next L7 will choose the Publisher to use based in a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, and it will "stitch" the Client and Publisher TLS tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the Private Application traffic to the selected Publisher.

b. If the Publisher(s) serving the Application are connected to a different Netskope PoP than the Netskope Client, the ZTNA Next L7 service will choose the Publisher to use based on a round-robin strategy (if more than one are configured and available) among the Publishers selected as faster and closer on point 6, it will create a third TLS tunnel between the Netskope PoPs where the Client and the Publisher are connected, it will "stitch" the three tunnels together, creating a logical encrypted tunnel between the Client and the Publisher, and it will send the Private Application traffic to the selected Publisher.

11 The Netskope Publisher that receives the Private Application traffic performs a Source NAT and sends the Private Application traffic to the IP of the Application using its local IP address.

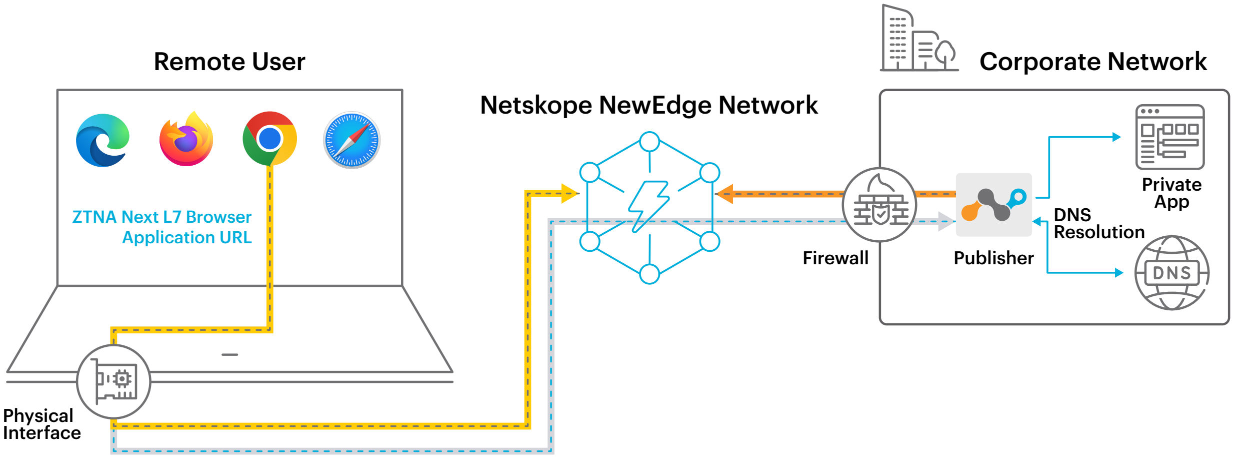
12 The Private Application will respond to the Netskope Publisher, which in turn will perform a Destination NAT and forward the response to the remote endpoint through the end-to-end encrypted tunnel.

13 The remote endpoint and the Application are able to communicate with each other.

+ Use Case 4 Clientless Access to Web Applications for Unmanaged Devices

Companies need to give external third parties and employees with personal devices access to web-based private applications. With the clientless deployment of ZTNA Next L7, known as Browser Access, Netskope provides secure connectivity for unmanaged devices. Using their existing web browser, users can safely access private apps without installing an agent, which may not be possible.

Additionally, as Netskope ZTNA Next L7 Browser Access supports Websocket, it can be used to publish clientless HTML5 remote desktop applications such as Apache Guacamole and its derived solutions too (such as Microsoft RDS Web Service, VMware Horizon “HTML Access,” CyberArk PSM Gateways and similar), to provide RDP/SSH/VNC access to local resources.



+ The flow of the connection will be:

1. A Netskope Publisher (more than one as per best practices) has been deployed on the network where the Private Application resides, whether in the same subnet or a different one, depending on the micro-segmentation requirements of the customer.

2. A Netskope Clientless Private Application defined by IP or FQDN has been configured and associated with the Netskope Publisher(s) that will be used to connect to the Private Application, and is enabled for “Browser Access.” The Netskope Clientless Private Application returns a specific Reverse Proxy HTTPS URL that will be used by the users to initiate the traffic toward the Private Application.

3. As per best practices, a customer-specific “Custom URL” has been configured for the Private Application.

4. Netskope Clientless Private Application SAML authentication has been configured on the Netskope tenant, under the Reverse Proxy SAML authentication settings, toward the desired IdP.

5. The Private Application has been explicitly allowed on the Netskope Zero Trust Engine through a Real-Time Protection policy for the users/groups that are authorized to access it.

+ The flow of the connection will be (cont.):

6 The user logs into the remote endpoint where there is no Netskope Client installed.

7 The user initiates a connection from a Browser to the Private Application using the configured "Custom URL".

8 The remote endpoint resolves the "Custom URL" with an IP address that belongs to the Netskope Reverse Proxy architecture and it begins an HTTPS connection toward it.

9 The HTTPS traffic reaches the Netskope PoP, where the Reverse Proxy initiates an SAML authentication against the configured IdP.

10 If the user completes the SAML authentication and if the Private Application has been allowed for the authenticated user, the ZTNA Next L7 service is aware of what is (are) the Publisher(s) serving the specific Private Application:

a. If the Publisher(s) serving the Application is (are) connected to the same Netskope PoP, ZTNA Next L7 will choose the Publisher to use based on a round-robin strategy if more then one, and it will "stitch" the HTTPS connection and Publisher TLS tunnels together, creating a single end-to-end encrypted connection between the remote endpoint and the Publisher, and it will send the Application traffic to the selected Publisher.

b. If the Publisher(s) serving the Application is (are) connected to a different Netskope PoP, ZTNA Next L7 will choose the Publisher to use based on a round-robin strategy if more then one, it will create a TLS tunnel between the ZTNA Next L7 services in the Reverse Proxy and Publisher PoPs, it will "stitch" the tunnels together creating a single end-to-end encrypted connection between the remote endpoint and the Publisher, and it will send the Application traffic to the selected Publisher.

11 If the Private Application is defined on an FQDN, the Netskope Publisher that receives the Private Application traffic performs a DNS resolution for the FQDN configured, and resolves the real local IP of the Private Application.

12 The Netskope Publisher then performs a Source and Destination NAT and sends the Private Application traffic to the IP of the Private Application using its local IP address.

13 The Private Application will respond to the Netskope Publisher, which in turn performs a Source and Destination NAT and forwards the response to the remote endpoint through the end-to-end encrypted tunnel.

14 The remote endpoint and the Application are able to communicate with each other.

15 It's also possible to apply DLP controls on upload/download activities through the configuration of a DLP Real-Time Protection policy that applies to a Private Application. This will ensure that the user accessing the Private Application, which can be third-party users who cannot be protected by the Netskope Client, will not be able to upload/download sensitive data to/from the Private Application.

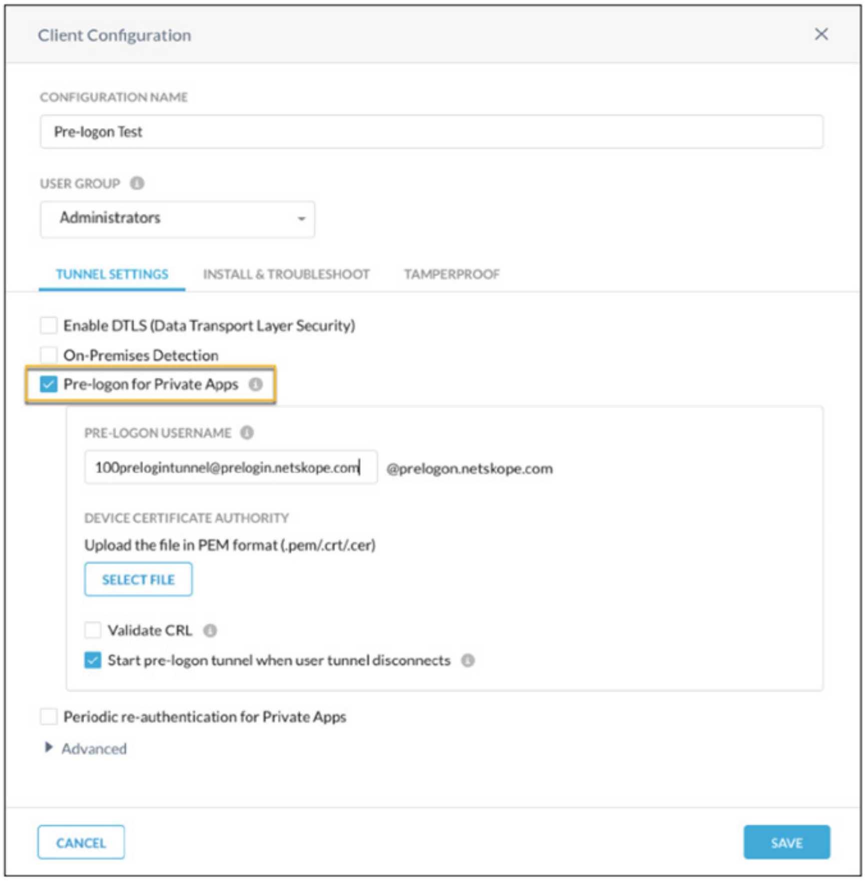
Optional Configurations

Client Pre-Logon Connectivity

By default, ZTNA Next L7 tunnels are established when the user has logged in and the user session starts, but there are some use cases that require a machine to connect to Private Applications before the user logs in. Some examples of use cases that require Pre-Logon Connectivity are Windows Autopilot deployment or password-reset capabilities for Active Directory joined machines, where the machines need to access on-premises resources like Domain Controllers before the user logs in.

When the ZTNA Next L7 Pre-Logon feature is enabled, this is the flow:

1. ZTNA Next L7 Pre-Logon functionality has been configured and enabled on the Default Client Configuration and on any other Client Configuration assigned to specific groups.
2. A Netskope Publisher (more than one as per best practices) has been deployed on the network where the Private Application resides, whether in the same subnet or a different one, depending on the micro-segmentation requirements of the customer.
3. A Private Application has been configured and associated to the Netskope Publisher(s) that will be used to connect to the Private Application (with any of the three methods described above).
4. The Private Application has been included on the Default Steering Configuration, which applies to the configured Pre-Logon user(s) configured.
5. The Private Application has been explicitly allowed on the Netskope Zero Trust Engine through a Real-Time Protection policy for the Pre-Logon user(s), provided they comply with other zero trust criteria, such as Endpoint Posture Check, Operating System, etc.
6. The machine boots and the Netskope Client service starts. The Netskope Client synchronises the Private Application definitions for the Pre-Logon user, then it establishes the ZTNA Next L7 TLS tunnel toward the closest Netskope PoP.
7. Any request for a Private Application defined for the Pre-Logon user in the three possible ways detailed above will be managed via the Pre-Logon ZTNA Next L7 tunnel.
8. When a user logs in, the Pre-Logon ZTNA Next L7 tunnel is terminated and the user ZTNA Next L7 tunnel is established.
9. When a user logs off, the user ZTNA Next L7 tunnel is closed and (optionally, depending on the Client Configuration) the Pre-Logon tunnel is established.



Client Configuration

CONFIGURATION NAME

Pre-logon Test

USER GROUP

Administrators

□ Enable DTLS (Data Transport Layer Security)

□ On-Premises Detection

☑ Pre-logon for Private Apps

PRE-LOGON USERNAME

100prelogintunnel@prelogin.netskope.com @prelogon.netskope.com

DEVICE CERTIFICATE AUTHORITY

Upload the file in PEM format (.pem/.crt/.cer)

□ Validate CRL

☑ Start pre-logon tunnel when user tunnel disconnects

□ Periodic re-authentication for Private Apps

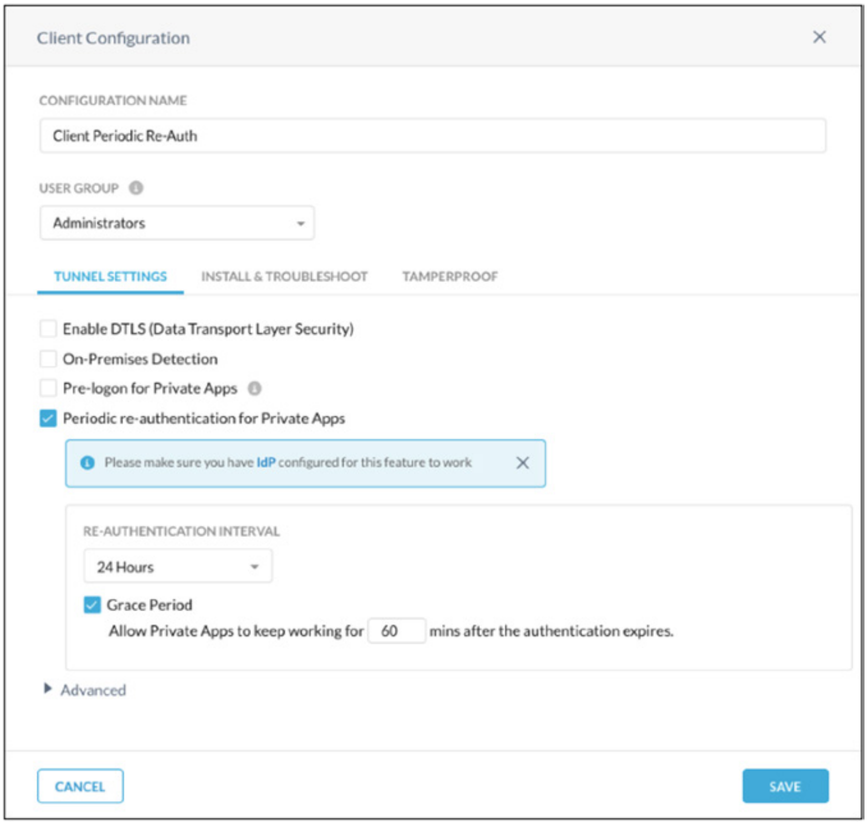
Periodic Client Re-Authentication

By default, ZTNA Next L7 tunnels are established automatically without forcing the user to perform an explicit authentication. There are circumstances where a company may want to force user authentication before establishing the ZTNA Next L7 tunnel, and possibly to initiate a user re-authentication at scheduled intervals.

When the ZTNA Next L7 Periodic Re-Authentication feature is enabled, this is the flow:

1. ZTNA Next L7 Periodic Re-Authentication functionality has been configured and enabled on Client Configuration assigned to specific groups.
2. IdP “Forward Proxy” SAML authentication has been configured for “Client Enrollment”.
3. The user logs into the remote endpoint and the Netskope Client synchronises the Private Application definitions, then:
   a. If the tenant backend flag “Re-auth on Logon” has not been enabled, the Netskope Client will establish the ZTNA Next L7 tunnel.
   b. If the tenant backend flag “Re-auth on Logon” has been enabled, the Netskope Client will prompt the user for IdP SAML authentication and establish the ZTNA Next L7 tunnel only if the user successfully completes the authentication.

4. Based on the “Re-Authentication Interval” and “Grace Period” settings, the user is prompted to re-authenticate at the end of the re-authentication interval and the ZTNA Next L7 tunnel is terminated if the user doesn’t re-authenticate for the duration of the “Grace Period.” In case the “Grace Period” is not enabled, the ZTNA Next L7 tunnel terminates automatically at the end of the re-authentication interval.



Client Configuration

CONFIGURATION NAME

Client Periodic Re-Auth

USER GROUP

Administrators

□ Enable DTLS (Data Transport Layer Security)

□ On-Premises Detection

□ Pre-logon for Private Apps

☑ Periodic re-authentication for Private Apps

Please make sure you have IdP configured for this feature to work

RE-AUTHENTICATION INTERVAL

24 Hours

☑ Grace Period

Allow Private Apps to keep working for 60 mins after the authentication expires.

It’s important to note that as we enforce a user authentication using SAML authentication with an IdP, it’s also possible to define Conditional Access policies on the IdP that would look at other contextual info regarding the SAML authentication attempt, such as source (network/country) conditional access, Intune posture conditional access, MFA enforcement, etc.

Server-Initiated Connectivity: Netskope ZTNA Next L3E

Netskope ZTNA Next L3E leverages the industry's first software-based unified SASE client to deliver granular and dynamic network performance, visibility, and security capabilities.

Below are examples of the Netskope ZTNA Next L3E connectivity flow for the 3 main use cases related to remote access. Netskope ZTNA Next L3E can cover other SD-WAN specific use cases, like QoS, Application Assurance, and others we'll not cover in this guide.

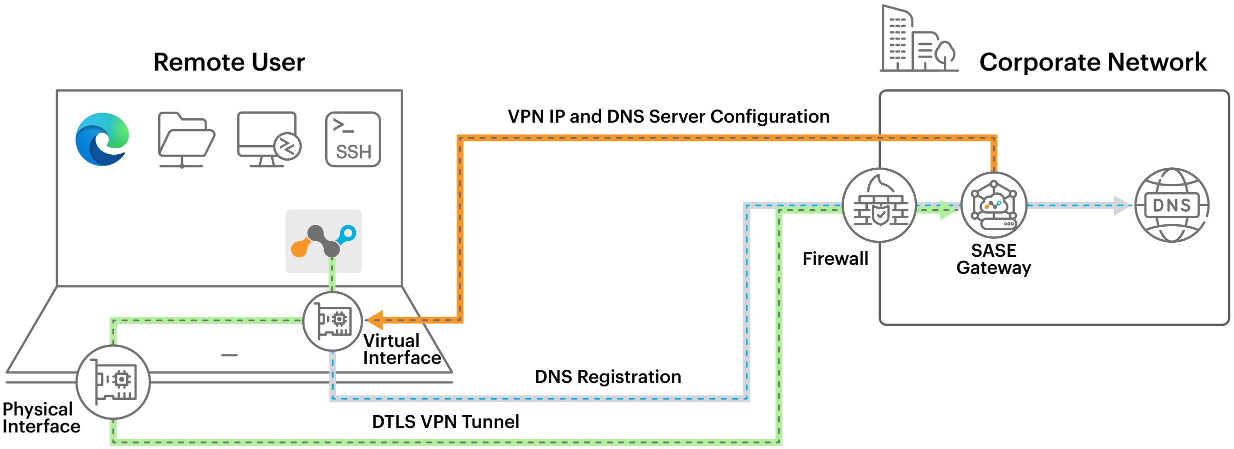
Terms and Definitions

- **Netskope Client:** The Netskope Client is a simple lightweight application that steers traffic from the end-user device to Netskope Cloud. It provides real-time visibility of the managed devices accessing the Web, SaaS applications, Private Applications, and SD-WAN destinations from any location.
- **Netskope ZTNA Next L3E:** The Netskope ZTNA Next L3E is a component of the Netskope Client that manages SD-WAN connections and routing to SD-WAN destinations on the end-user device.
- **Netskope SASE Gateway:** The Netskope SASE Gateway is a software that provides transport-agnostic connectivity, offering zero trust security regardless of the network medium, such as LTE, Ethernet, or Wi-Fi. With the SASE GW, organizations can establish secure overlay networks, end-to-end encryption, and enjoy robust network security. The SASE Gateway is deployed in the Customer's premises (aka "border"), whether in an on-premises network, a Data Center, or Public Cloud, and it can be deployed as a virtual machine or using Netskope SASE Gateway Appliances.
- **AppX:** AppX is a concept used in Netskope Borderless SD-WAN to identify Applications. In our context we use the Custom Applications AppX type, which can be used to classify the traffic based on a custom configuration. This configuration helps in identifying the specific traffic in the monitoring page, and Policies based on the AppX can also be created to allow and route users' traffic. An AppX is configured defining the following parameters (one or more traffic type can be classified under a single custom app):
  - **Name:** The name for the AppX
  - **Description:** The description for the AppX
  - **Category:** The category to which the AppX will belong
  - **Protocol:** The protocol used by the application
  - **CIDR Host:** The destination IP or hostname used by the application
  - **Port Range:** The Destination port number(s) used by the application
  - **Web Access:** In case the application is a webpage
- **Client Template:** The Client Templates enables administrators to streamline and simplify the configuration of ZTNA Next L3E at scale. Templates are used by administrators to deploy any number of ZTNA Next L3E that have multiple configuration parameters in common to users and groups.
- **SD-WAN Policies:** SD-WAN Policies are a set of rules that apply to specific traffic, and they are applied to users and groups via the Client Templates. SD-WAN Policies are defined based on:
  - The Topology
  - The AppX
  - The Security
  - The Services
  - Other General Settings (SNMP, Syslog, NetFlow)

Use Cases

+ Use Case 1 Remote Endpoint DNS Registration

Many Server-to-Client or Client–to-Client applications rely on DNS to resolve the IP addresses of the Clients, and if the Clients are remote, they rely on DNS registrations of the VPN address of the remote endpoint on the DNS Servers. In this use case, the objective is to register the remote endpoint's VPN IP to a corporate DNS, in order for local Servers/Clients/Applications to be able to correctly resolve the FQDN of the remote endpoint.



+ The flow of the connection will be:

1. A Netskope SASE Gateway is configured to allow ZTNA Next L3E tunnels and to allow an SD-WAN Application (AppX) for the corporate DNS Server(s) using Client Templates and Policies.

2. On the remote endpoint, a virtual interface and local routes are used by Netskope ZTNA Next L3E to establish the ZTNA Next L3E tunnel and to encapsulate the traffic for the configured SD-WAN Applications (AppX).

3. ZTNA Next L3E establishes a DTLS (UDP 443) VPN tunnel with the SASE Gateway.

4. The ZTNA Next L3E virtual interface gets a VPN IP address and subnet mask, the corporate DNS server(s) and DNS suffix as per the assigned ZTNA Next L3E Configuration Template.

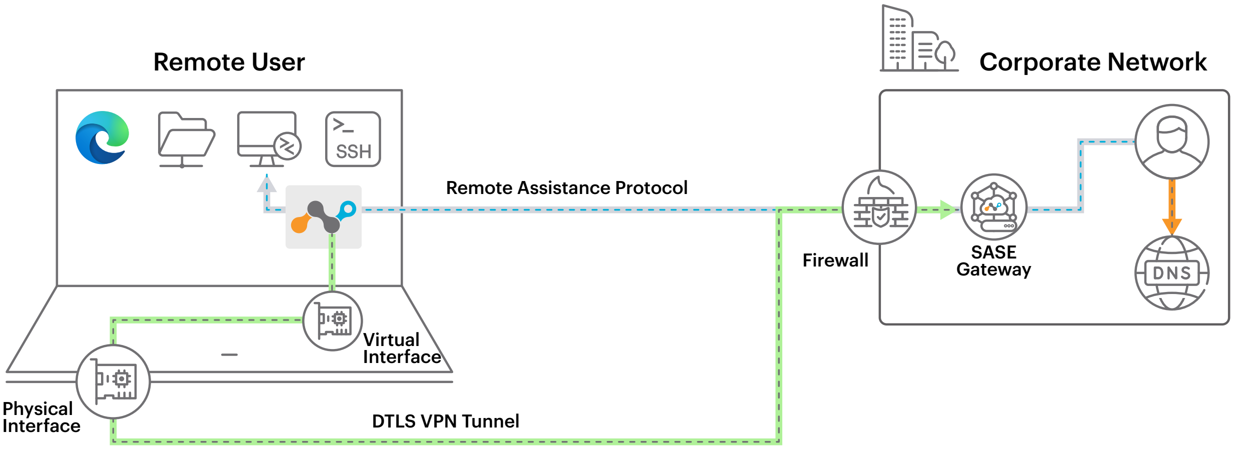
5. ZTNA Next L3E receives the SD-WAN Applications (AppX) definitions that are allowed in the ZTNA Next L3E tunnel as per the assigned Client Policy, and configures the routes tables accordingly.

6. As the corporate DNS Server is configured on the virtual VPN interface and the DNS traffic for the corporate DNS Server is allowed by the Client Policy, the remote endpoint OS registers itself with the corporate DNS server (i.e., Active Directory DNS) via Dynamic DNS registration, updating the corporate DNS record for client hostname with the VPN virtual interface's IP address via the ZTNA Next L3E tunnel.

7. All the Servers and Clients that rely on the corporate DNS for DNS resolution will be able to resolve the FQDN of the remote endpoint with the VPN virtual interface's IP.

+ Use Case 2 Server-to-Client Application Access (Legacy Help Desk Remote Assistance, Update/Patching Solutions)

Some legacy applications, such as legacy help desk Remote Assistance platforms, rely on Server-to-Client communications to work. The same concepts can be applied for legacy on-premises Update/Patching solutions. In this case, a legacy help desk platform wants to initiate a Remote Assistance connection (RDP, VNC, etc.) to the remote endpoint.



+ The flow of the connection will be:

1. A Netskope SASE Gateway is configured to allow ZTNA Next L3E tunnels and is configured to allow SD-WAN Applications (AppX) for the corporate DNS Server(s) and the Remote Assistance protocol (RDP, VNC, etc.) using Client Templates and Policies.

2. On the remote endpoint, a virtual interface and local routes are used by Netskope ZTNA Next L3E to establish the ZTNA Next L3E tunnel and to encapsulate the traffic for the configured SD-WAN Applications (AppX).

3. ZTNA Next L3E establishes a DTLS (UDP 443) VPN tunnel with the SASE Gateway.

4. The ZTNA Next L3E virtual interface gets a VPN IP address and subnet mask, the corporate DNS server(s) and DNS suffix as per the assigned ZTNA Next L3E Configuration Template.

5. ZTNA Next L3E receives the SD-WAN Applications (AppX) definitions that are allowed in the ZTNA Next L3E tunnel as per the assigned Client Policy, and configures the routes tables accordingly.

6. The remote endpoint performs a Dynamic DNS registration as per previous use case.

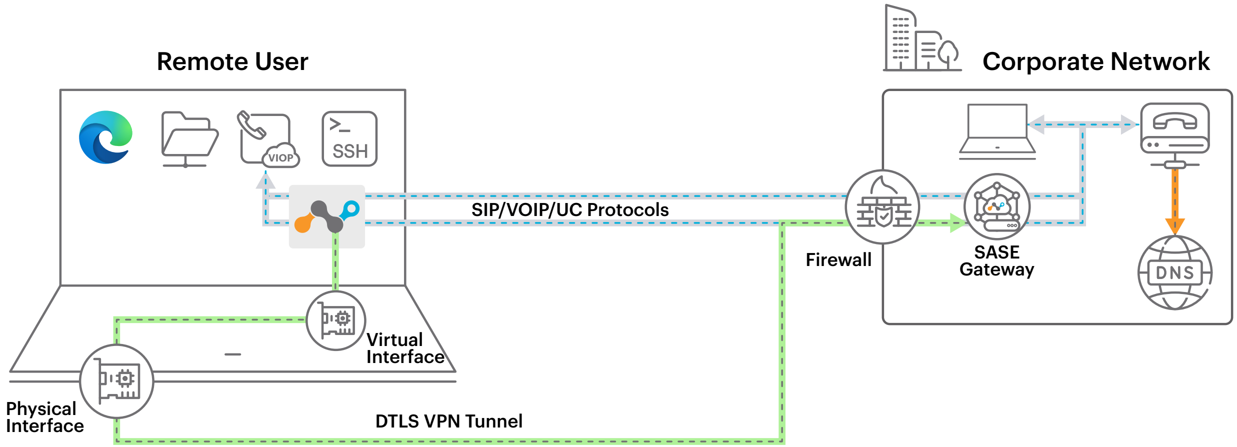
7. The help desk solution initiates a Remote Assistance connection (RDP, VNC, etc.), first resolving the FQDN of the remote endpoint machine, which will match the VPN IP address.

8. The help desk solution initiates a Remote Assistance connection (RDP, VNC, etc.) toward the remote endpoint's VPN IP.

9. The SASE Gateway and ZTNA Next L3E will ensure the Remote Assistance connection (RDP, VNC, etc.) traffic is encapsulated in the DTLS VPN, ensuring a bi-directional route between the help desk solution and the remote endpoint.

+ Use Case 3 Server-to-Client and Client-to-Client Applications Access (Legacy VoIP Solutions)

Legacy SIP/VoIP and Unified Communications (UC) solutions (Cisco UC/PBX, Avaya, Microsoft Lync, Mitel, etc.) rely on Server-to-Client and also Client-to-Client connections to ensure the routing of the calls. In this case, a remote endpoint using a legacy SIP/VoIP/UC solution needs to route the traffic to the SIP/VoIP/UC Server and other endpoints, and it needs to be reachable from the SIP/VoIP/UC Server and other endpoints in order to make and receive audio/video communications.



+ The flow of the connection will be:

1. A Netskope SASE Gateway is configured to allow ZTNA Next L3E tunnels and is configured to allow SD-WAN Applications (AppX) for the corporate DNS Server(s) and the SIP/VoIP/UC protocols (RTP, SIP, Stun, etc.) using Client Templates and Policies.

2. On the remote endpoint, a virtual interface and local routes are used by ZTNA Next L3E to establish the ZTNA Next L3E tunnel and to encapsulate the traffic for the configured SD-WAN Applications (AppX).

3. ZTNA Next L3E closes a DTLS (UDP 443) VPN tunnel with the SASE Gateway.

4. The ZTNA Next L3E virtual interface gets a VPN IP address and subnet mask, the corporate DNS server(s) and DNS suffix as per the assigned ZTNA Next L3E Configuration Template.

5. ZTNA Next L3E receives the SD-WAN Applications (AppX) definitions that are allowed in the ZTNA Next L3E tunnel as per the assigned Client Policy, and configures the routes tables accordingly.

6. The remote endpoint performs a Dynamic DNS registration as per previous use case.

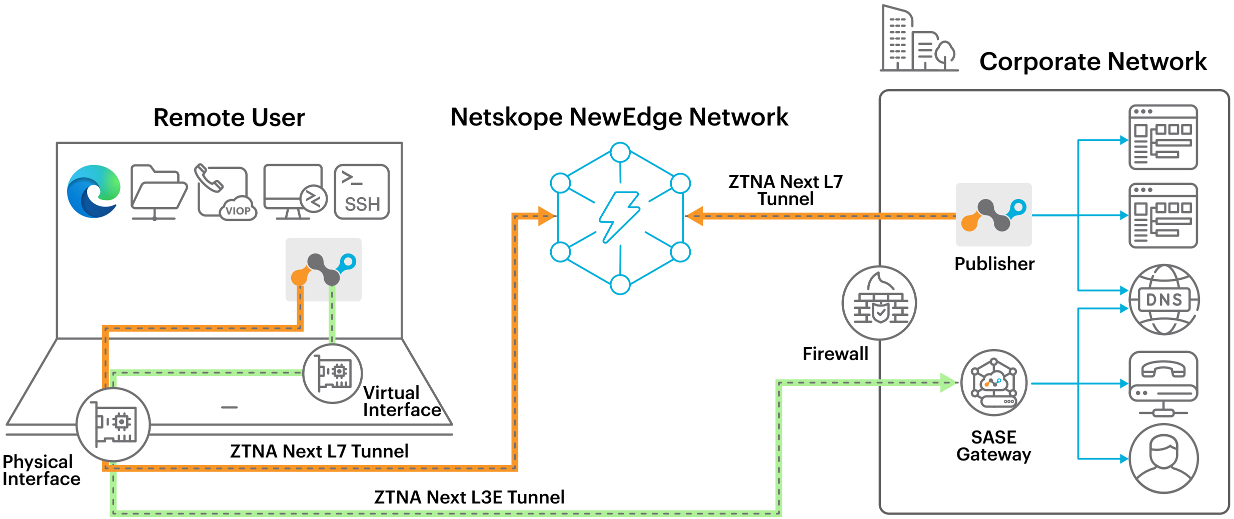
7. The remote endpoint’s SIP/VoIP/UC software initiates a connection to the SIP/VoIP/UC Server.

8. If the remote user initiates an audio/video communication with another Client or externally, the SIP/VoIP/UC traffic will be sent via the ZTNA Next L3E tunnel and it will reach the destination accordingly.

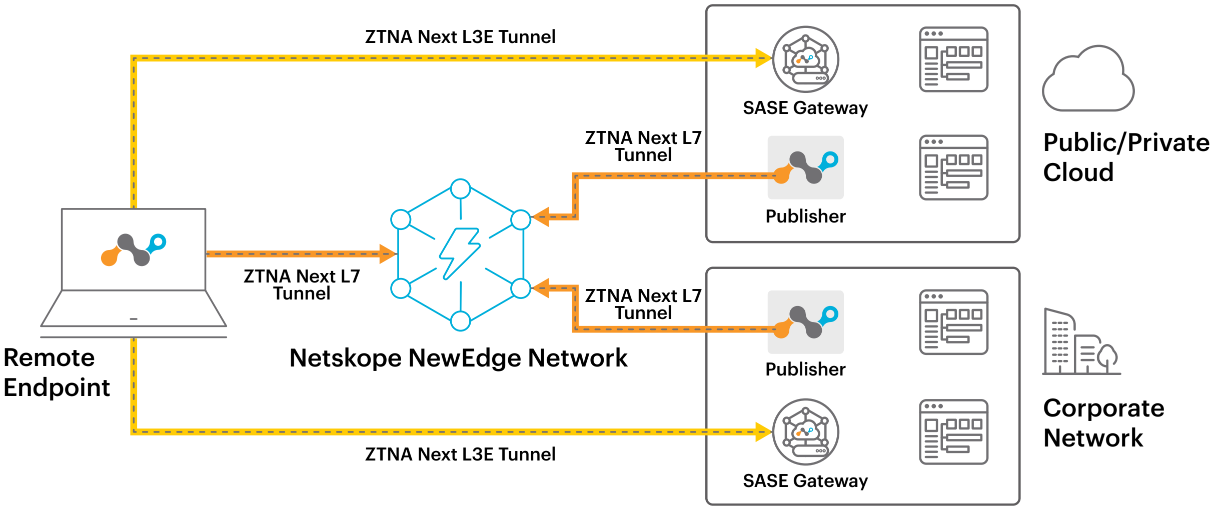
9. If another endpoint, whether remote or local, initiates an audio/video communication with the remote endpoint, the local infrastructure of DNS and SASE Gateway and ZTNA Next L3E running on the remote endpoint will ensure the Server-to-Client and Client-to-Client communications will reach the remote endpoint.

Full Zero Trust Application Access: Netskope ZTNA Next 360

Combining ZTNA Next L7 and ZTNA Next L3E capabilities on the same Endpoint, Netskope enables organisations to apply granular zero trust access to all Internal Applications, and support all use cases for a VPN replacement.



ZTNA Next 360 vastly improves the user experience by supporting multiple ZTNA Next L7 applications through a single connection to the NewEdge Network. Additionally, it supports multiple ZTNA Next L3E tunnels to multiple SASE Gateways, whether they're located in private Data Centers or Private/Public Clouds. This enables customers to not only streamline access and improve performance for all types of private applications, but also ensure granular zero trust-based access.



RELATED DOCUMENTATION

Solution

Website: Replace VPNs with ZTNA Next

eBook: 6 Most Compelling Use Cases for Complete Legacy VPN Replacement

Solution Brief: Netskope ZTNA Next

White Paper: Delivering on the Promise of 100% Legacy VPN Retirement

How To’s

How to Configure Client Prelogon Connectivity

How to Configure Client Re-authentication

How to Configure Private Applications for Microsoft Active Directory Domain Services

How to Configure Private Applications with Microsoft’s System Center Configuration Manager (SCCM)

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.