netskope

Reference Architecture

Steering Traffic through Netskope Security Service Edge

DOCUMENT SCOPE

This document is intended to give an Architecture and Best Practice overview of the Netskope Steering in a single document. This document is intended for:

- Enterprise Architects
- Security and Network Architects
- Solution Architects
- CISO and InfoSec Team
- CIO and CTOs

This reference architecture will demonstrate:

- The different types of steering methods
- Use cases for each method
- The minimum requirements for each steering method
- How to interoperate within an existing proxy environment

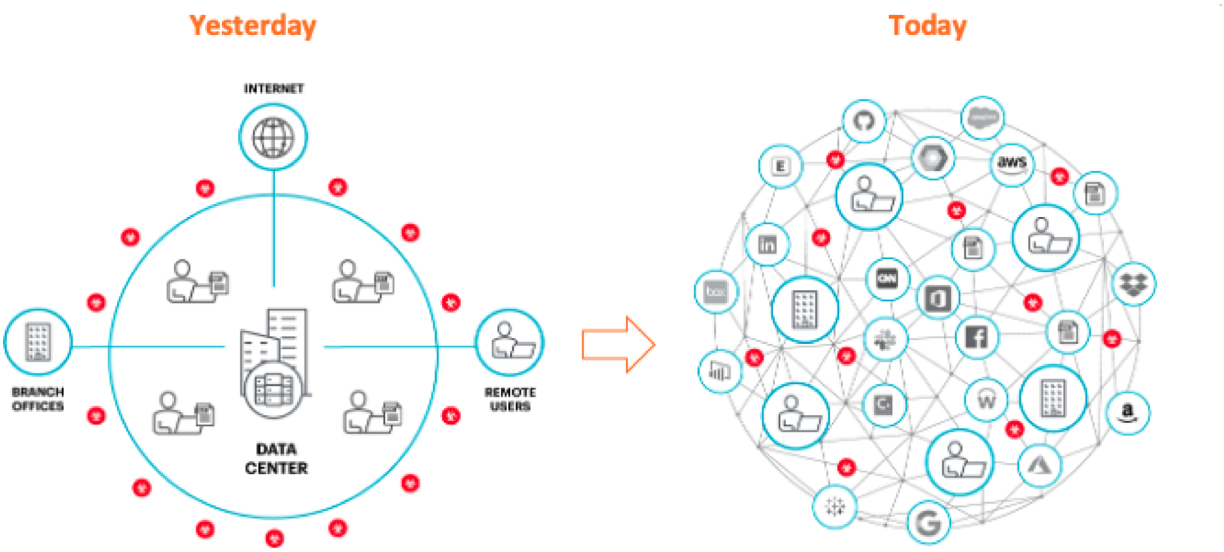
Note: It is not intended to be used as a deployment and troubleshooting guide.

CONTENTS

INTRODUCTION

The ever-changing landscape

All organizations - small, medium and large have witnessed the shift in how their application services were and are being delivered to their users. The shift is happening across all facets - applications, users, user locations, and end points used to access these applications.



Applications that were primarily hosted in the data centers are now spread across - data centers, public clouds and some applications are consumed as Software-as-a-Service.

Users could be employees, contractors, customers, business partners, auditors, etc.

Servers and IoT devices are also endpoints other than users that access application services on the Internet.

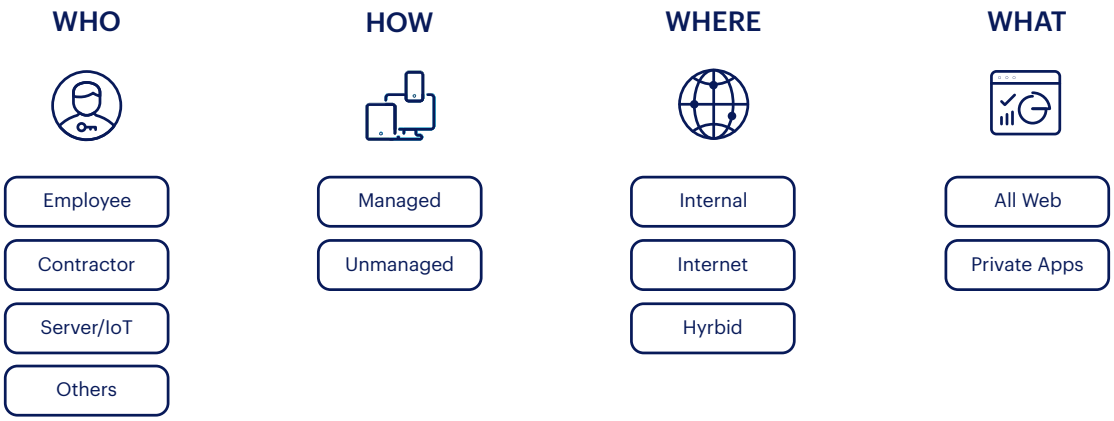
Location and **Endpoints** - Traditionally corporate applications were accessible from internal corporate networks or remotely over a virtual private network from a corporate managed endpoint. However, today's business demands that applications be accessible from anywhere using any device be it a corporate managed device or their personal device.

We are currently experiencing a rapid transformation, anticipating a continuous rise in the number of users operating in a hybrid environment. There is a noticeable trend towards the widespread use of personal or unmanaged devices for accessing corporate applications. Additionally, application services are increasingly proliferating across the cloud and SaaS platforms.

In order to intelligently analyze each user request to an application service, the crucial element we require is "context." Obtaining context is essential in terms of understanding and effectively responding to user interactions, there are four key components that are required to provide context:

- **WHO** - is it an employee or a contractor or is it from another application service or from an IoT device.
- **HOW** - is it a trusted (managed) device or an untrusted (unmanaged) device.
- **WHERE** - is the application services accessed from Public Internet or Internal network

  and finally
- **WHAT** - Determining which specific application service is being accessed and identifying the specific actions being performed — such as View, Create, Edit, Copy, Move, Share, Delete, Comment, etc.— is essential for a comprehensive understanding of the user's interactions.



Note: This reference architecture covers the use cases where traffic is steered to the Internet. Use cases for steering traffic to internal private applications are covered in detail in the ZTNA reference architecture guide here.

The challenge

Organizations have grappled with the myriad challenges posed by legacy on-premises solutions, including issues related to scalability during unexpected peaks or growth, resiliency concerns, increased data center footprint, the burden of hardware and software maintenance, and associated overheads. Notably, these challenges often translate into heightened Total Cost of Ownership (TCO) and occasionally yield suboptimal Return on Investment (ROI).

Moreover, the inflexibility of the architecture in legacy on-premises solutions falls short in meeting evolving security requirements. Any workarounds implemented to address this shortfall typically result in a compromised user experience or, worse, lead to unplanned downtimes.

Recognizing these drawbacks, organizations have come to acknowledge that a cloud-based Secure Services Edge (SSE) represents the optimal solution capable of addressing both current challenges and accommodating future growth seamlessly.

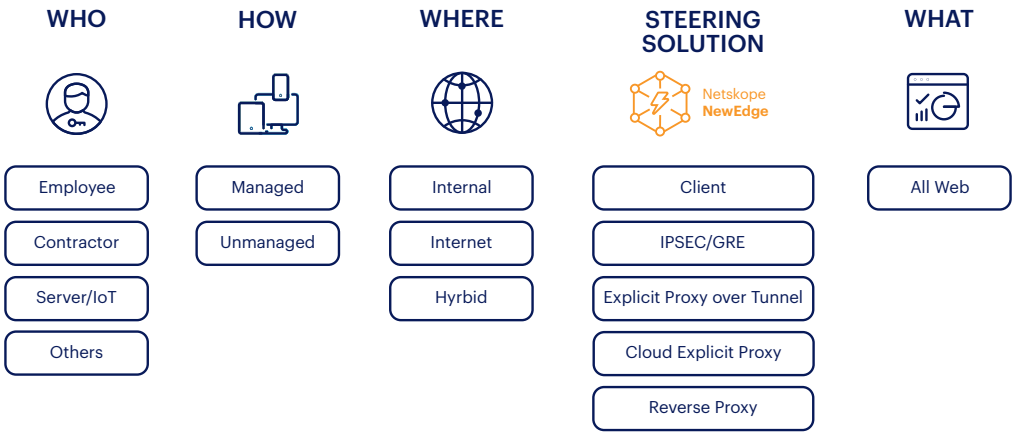
For a seamless integration of a cloud-based SSE solution, it is essential that the solution offers flexible mechanisms for efficiently directing ("steering") traffic to the Secure Services Edge (SSE):

- From any user.
- From wherever the user is.
- From whichever device they use and.
- To whatever application they access.

This is where Netskope, the leader in Gartner's Magic Quadrant for SSE solutions, leads the way in supporting flexible traffic steering methods to meet the different use cases of our customers.

Depending on the use case, customers can choose from a variety of steering solutions, such as:

- **Netskope Steering Client.** The Netskope Steering Client is a lightweight non-intrusive steering client that provides the most comprehensive control and visibility. It steers traffic from the endpoint, to the closest Netskope NewEdge Data Plane, regardless of the device location.
- **Network Tunnel.** When a Netskope Client cannot be installed, steering traffic from on-premises or public cloud endpoints to Netskope NewEdge Data Planes can be achieved with a Network tunnel.
- **Explicit Proxy.** Legacy or regulated environments where an Explicit Proxy needs to be configured, traffic can be steered using Explicit Proxy over Tunnel, Cloud Explicit Proxy or Proxy Chaining options.



In this Reference Architecture Guide, we will comprehensively explore a range of real-world use cases spanning diverse industry verticals. Netskope provides robust traffic steering mechanisms to adeptly handle and navigate through these various scenarios.

We will not cover user access to private applications, this is extensively covered in the ZTNA Next reference architecture guide available here.

USE CASES

In the contemporary hybrid landscape, we can broadly categorize use cases based on whether the user is on-premises or remote, and further, if the user is accessing application services through a device with the Netskope client installed or not. Additionally, there's a potential scenario where the traffic originates from a non-user endpoint, such as a server or an IoT device.

Taking the aforementioned factors into account, the use cases elaborated upon in this reference architecture guide include:

- **Use Case #1** - On-premises or Remote users with Corporate Managed Device.
- **Use Case #2** - On-premises users and devices (servers and IoT) where installation of the Netskope Client is not feasible.
- **Use Case #3** - Remote user utilizing a personal device, including options like Chromebook, where the installation of the Netskope Client is not possible.

In this reference architecture, we are not covering two corner use cases:

1. **Explicit Proxy over Client (EPoC)** - this steering method is used in cases where, in the internal corporate network, there is no default gateway and the endpoint cannot resolve no public FQDNs.
2. **Proxy Chaining (PXC)** - this steering method is considered in cases where users need to egress to the Internet using two or more specific proxies.

Now, let's delve into a detailed exploration of these use cases.

Use Case 1 On-premises or Remote users with Corporate Managed Device

Overview

For this use case as depicted in the diagram above, we consider that:

(Who) Users can be an employee or contractor.

(How) Endpoint used by the user on which Netskope client can be installed. These can be corporate or personal devices managed by an Endpoint Management Solutions.

(Where) Location of the user is on-premises.

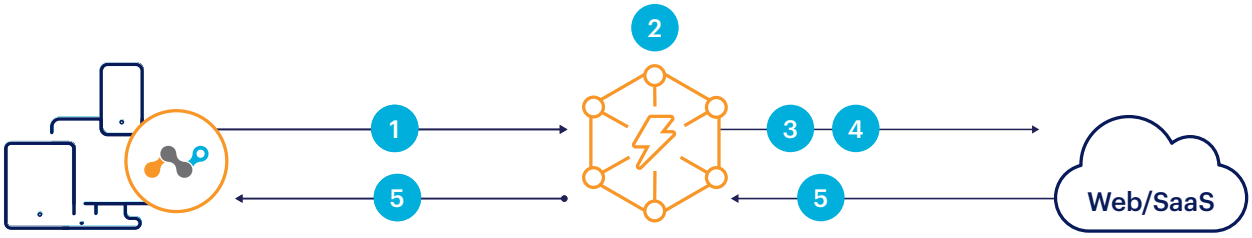
(What) Applications accessed by the user can be any application on the Internet. It could be general web,cloud applications or SaaS.

Recommended Architecture - Netskope Client

For this use case, we recommend "Netskope Client". Details on this architecture, please refer to Chapter Traffic Steering Method with Netskope Client. In this architecture, the endpoint has the Netskope Client installed which connects to the closest Netskope NewEdge Data Plane.

All internet traffic, both web and non-web egressing from the endpoint, and not explicitly bypassed, is steered to Netskope NewEdge Data Plane. On the NewEdge Data Plane, the traffic is inspected based on the real-time security policies defined and the corresponding action is taken.

Traffic Flow to Internet Apps



1. Endpoint with Netskope client connects to the closest Netskope NewEdge Data Plane, for more details on Data Plane selection, please refer to "Automatic Data Plane Selection". All web and non-web traffic to the Internet is steered from the endpoint to the closest Netskope NewEdge Data Plane.
2. Traffic is inspected against the real time security policies defined.
3. Allowed traffic is forwarded from Netskope NewEdge Data Plane to the original destination. on the Internet.
4. Traffic will egress the Netskope NewEdge Data Plane with the shared Netskope IP address range. If the customer desires to egress with a dedicated IP address, then Dedicated Egress IP Address services can be provisioned.
5. Response traffic from the Internet will be destined to Netskope NewEdge Data Plane, which will be inspected before being forwarded to the endpoint.

Pre-requisites

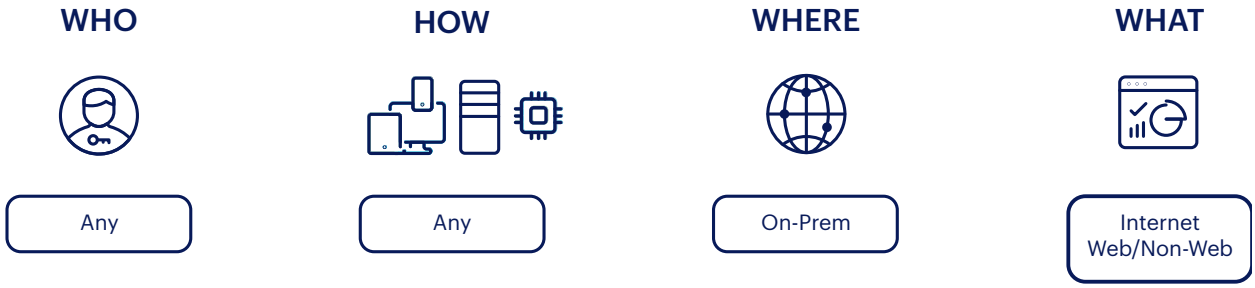
1. Netskope Client installed on the endpoint.
2. Endpoint should be able to resolve `*.goskope.com` FQDNs and have reachability to Netskope IP address ranges.
3. Firewall needs to allow direct access to Netskope domains on protocol HTTPS without SSL interception (authentication should be disabled as well).

Benefits

1. **Simple** architecture.
2. **Consistent security posture** regardless of the user location.
3. **Seamless** deployment and operation.
4. **Comprehensive traffic inspection**, encompassing both web and non-web, directed towards both Internet and Private Applications, originating from the endpoint.
5. **Optimal Performance** facilitated by the Netskope client's connection to the nearest Netskope NewEdge Dataplane.
6. **Unmatched visibility** into all types of traffic—web and non-web, directed to both Internet and Private Applications.
7. **Unified management** through a single pane for all traffic, covering both web and non-web, targeted towards both Internet and Private Applications, departing from the endpoint.

+ Use Case 2 On-premises users and devices (servers and IoT) where installation of the Netskope Client is not feasible

Overview



For this use case as depicted in the diagram above, we consider that:

(Who) User is an employee or contractor.

(How) Endpoint used by the user is a device on which Netskope client **cannot** be installed. Several examples can be provided:

- The organization has embraced Bring Your Own Device (BYOD) strategy.
- User/device connected to the Guest Wifi/Network.
- Server or IoT devices which don't allow Netskope client installation.

(Where) Location of the user is on-prem.

(What) Applications accessed by the user can be any web or non-web application on the Internet.

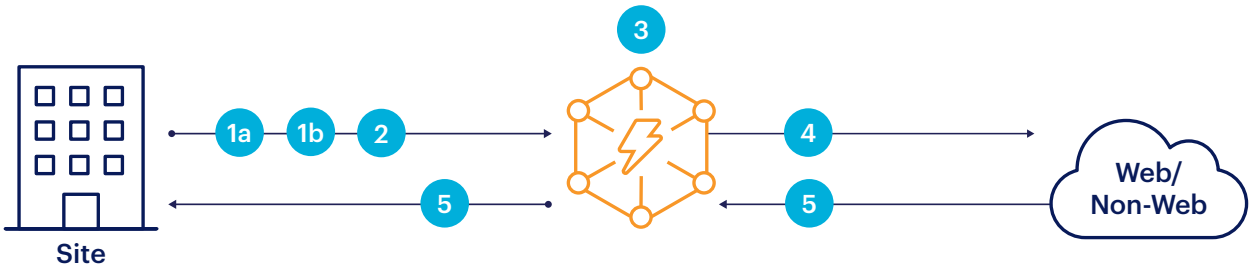
Note: In the scenario where the user is on-premises with an untrusted endpoint, the ideal approach involves blocking access to internal private applications locally. In this specific use case, only traffic directed towards Internet Apps is taken into consideration.

Recommended Architecture - Steering Web and Non-web Apps via IPsec/GRE Tunnel

All traffic, both web and non-web, needs to be steered from the on-premise endpoint to Netskope NewEdge Data Plane. Since the endpoints do not have Netskope Client installed they cannot connect to the Netskope NewEdge Data Plane directly. Hence, we connect the specific network segment or the entire site to the Netskope NewEdge Data Plane via a GRE or IPsec tunnel from any capable customer premise equipment (CPE), more details on Network Tunnel steering can be found in chapter "Traffic Steering Method with Network Tunnels".

In this use case, to steer the traffic from the endpoint to the tunnel, the network administrator needs to configure policy based forwarding/routing techniques, wherein specific routes are defined based on the destination port and destination IP address.

Traffic Flow to Internet Web and Non-web Apps via Tunnel



1. As a prerequisite.
   a. One or more GRE/IPSEC tunnels are configured from each site to Netskope NewEdge Data Plane. We recommend at least two tunnels to different Netskope NewEdge Data Planes for resiliency.
   a. Policy based forwarding/routing policies are defined on the internal network, that route traffic destined to the Internet towards the GRE/IPSEC tunnel established with Netskope NewEdge Data Plane.
2. All web and non-web traffic to the Internet from the endpoint will be steered to Netskope NewEdge Data Plane over the GRE/IPSEC tunnel.

3. Allowed traffic is forwarded from Netskope NewEdge Data Plane to the original destination on the Internet.
4. Traffic will egress the Netskope NewEdge Data Plane with the shared Netskope IP address range. If the customer desires to egress with a dedicated IP address, then Dedicated Egress IP Address services can be provisioned.
5. Response traffic from the Internet will be destined to Netskope NewEdge Data Plane, which will be inspected before being forwarded to the endpoint.

Note: It is possible to enforce User SAML authentication and SSL inspection only if the Netskope Root and Intermediate Certificate bundle can be installed on the endpoints.

Pre-requisites

1. One or more GRE/IPSEC tunnels are configured from each site to Netskope NewEdge Data Plane. We recommend at least two tunnels to different Netskope NewEdge Data Planes for resiliency.
2. Policy based forwarding/routing policies are defined on the internal network, that route traffic destined to the Internet towards the GRE/IPSEC tunnel established with Netskope NewEdge Data Plane.

Benefits

1. Best suited for endpoints on which Netskope Client cannot be installed.
2. **Comprehensive traffic inspection** of all traffic, both web and non-web, and to the Internet.
3. **Visibility** of Private IP of the user, allowing advanced logging and IP-based access policies, in case authentication is not an option.

Recommended Architecture - Steering Web Apps Only via IPsec/GRE Tunnel

When it is not possible to configure policy based forwarding/routing techniques, Explicit Proxy can be defined on the endpoints, and Explicit Proxy over Tunnel (EPoT) steering method can be used for Internet **Web** Apps only.

Also, for large environments that use PAC files deployed on endpoints, and want to continue using it for the large number of exceptions that are already scripted into the PAC file, Explicit Proxy over Tunnel (EPoT) steering method can be used.

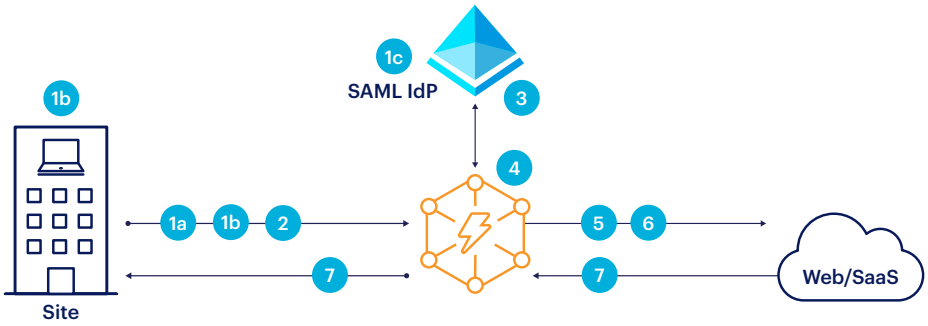
Note: EPoT does not support Internet based non-web applications.

The explicit proxy configuration can point HTTP/HTTPS traffic to one of the reserved IP addresses `163.116.128.80` or `163.116.128.81` on port `8080`, either manually or using a PAC file.

We will need to configure policy based forwarding/routing to route the traffic from the endpoint destined to the EPoT IP addresses over the tunnel.

Note: EPoT only supports ports `80`, `443`, and `8080`.

Traffic Flow to Internet Web Apps via EPoT



1. As a prerequisite.
   a. One or more GRE/IPSEC tunnels are configured from each site to Netskope NewEdge Data Plane. We recommend at least two tunnels to different Netskope NewEdge Data Planes for resiliency.
   b. On the endpoints at the site, traffic needs be steering to Netskope reserved EPoT IP addresses 163.116.128.80 or 163.116.128.81 on port 80. This can be achieved with explicit proxy configured directly on the endpoint or PAC file.
   b. SAML based Identity Provider (IdP) for authenticating the user.
2. All web traffic to the Internet destined on port (80, 443 and 8080) from the endpoint will be steered to the Netskope Proxy over the GRE/IPSEC tunnel which terminates at the Netskope GRE/IPSEC headend.

3. User authentication against the defined SAML IdP.
   Note: There could be scenarios like (server initiated traffic, traffic from IoT devices), where authenticating against SAML IdP might not be feasible. For such scenarios, Netskope provides the option to bypass authentication based on the source IP address, which would be static or from a predefined internal IP range.
4. Netskope Proxy sees the incoming HTTP request on port `8080`. Traffic is inspected against the real time security policies defined.
5. Allowed traffic is forwarded from Netskope NewEdge Data Plane to the original destination on the Internet.
6. Traffic will egress the Netskope NewEdge Data Plane with the shared Netskope IP address range. If the customer desires to egress with a dedicated IP address, then Dedicated Egress IP Address services can be provisioned.
7. Response traffic from the Internet will be destined to Netskope NewEdge Data Plane, which will be inspected before being forwarded to the endpoint.

Pre-requisites

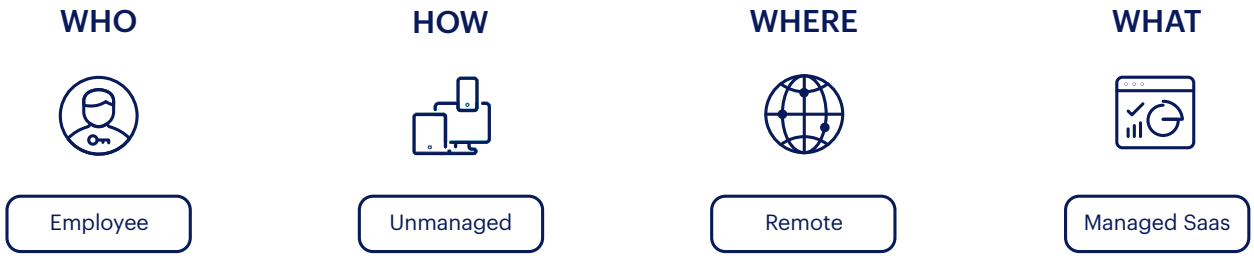
1. One or more GRE/IPSEC tunnels are configured from each site to Netskope NewEdge Data Plane. We recommend at least two tunnels to different Netskope NewEdge Data Planes for resiliency.
2. Policy based forwarding/routing policies are defined on the internal network, that route web traffic destined to the reserved EPoT IP addresses `163.116.128.80` or `163.116.128.81` on port `8080` towards the GRE/IPSEC tunnel established with Netskope NewEdge Data Plane.
3. SAML based Identity Provider (IdP) for authenticating the user.
4. Netskope certificate bundle needs to be trusted on the endpoints.

Benefits

1. Best suited for endpoints on which Netskope Client cannot be installed.
2. EPoT can work with legacy environments using PAC files.
3. **Comprehensive traffic inspection** of all traffic, both web and non-web, and to the Internet using tunnels. Inspection of web traffic to Internet, when using EPoT.
4. **Visibility** of Private IP of the user, allowing advanced logging and IP-based access policies, in case authentication is not an option.

+ Use Case 3 Remote user utilizing a personal device, including options like Chromebook, where the installation of the Netskope Client is not possible

Overview



For this use case as depicted in the diagram above, we consider the:

(Who) Users can be an employee or contractor.

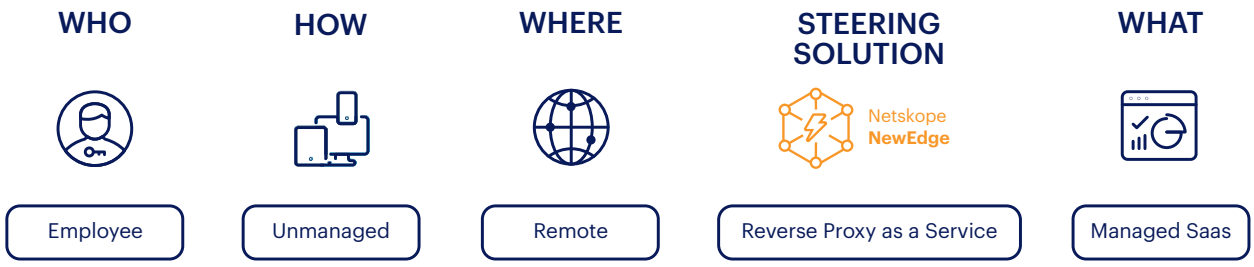
(How) Endpoint used by the user is a device on which Netskope client cannot be installed. For example, it could be an employee working remotely from their personal device, it could be a contractor or auditor or business partner using their organization issued endpoint, and needs access to Internal applications.

(Where) Location of the user is remote.

(What) Applications accessed by the user can be a web based internet application or a SaaS application.

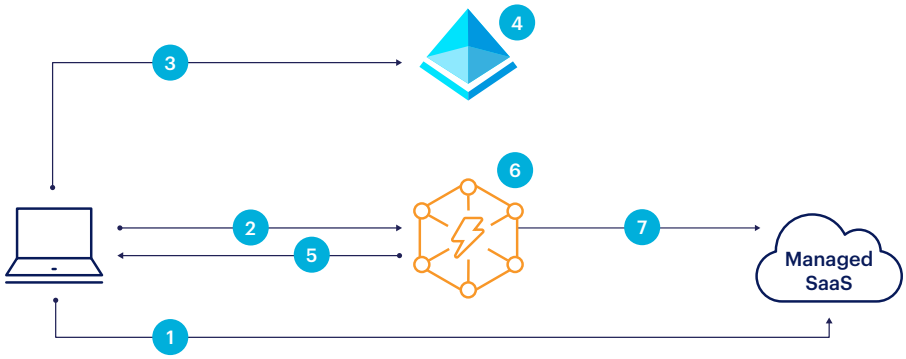
Recommended Architecture for Accessing Managed SaaS Web Apps - Steering with Reverse Proxy as a Service

Today organisations consume many managed SaaS applications that could be accessed from the public Internet. But organisations would like to restrict the access to allow access from only trusted sources (like Netskope IP ranges or Dedicated Egress IP Address services) post authentication.



Netskope provides a reverse proxy deployment mode that steers browser-based cloud traffic from managed cloud apps to the Netskope Security Cloud. This deployment option is required for covering unmanaged devices that are off network accessing managed cloud apps.

Traffic Flow to Managed SaaS Web Apps via Reverse Proxy as a Service



1. User connects to the SaaS application.
2. SaaS application redirects the user to Netskope SAML Proxy.
3. Netskope SAML Proxy redirects the user to the defined SAML IdP.
4. User authenticates against the defined SAML IdP.
5. After successful authentication, user is redirected to Netskope SAML Proxy with the SAML Assertion.
6. Request will be inspected against the real time security policies defined to determine if the traffic needs to be proxied by Netskope Reverse Proxy or bypassed (direct) or blocked to the SaaS application.
7. If the request needs to be proxied, the user will be redirected to rproxy.goskope.com instead of the SaaS application, and Netskope Reverse Proxy will proxy the request to the SaaS application.

Pre-requisites

1. SAML based Identity Provider (IdP) for authenticating the user.
2. Define conditional access in the managed SaaS application to allow access Netskope IP ranges or Dedicated Egress IP Address services.
3. Refer the below knowledge base for respective IdP and SaaS application https://docs.netskope.com/en/netskope-help/proxies/.

Benefits

1. Real-time visibility and control for managed and unmanaged devices accessing managed cloud apps.
2. Only deployment that covers unmanaged devices off network accessing managed cloud apps.
3. Browser traffic only – no native apps or sync clients.

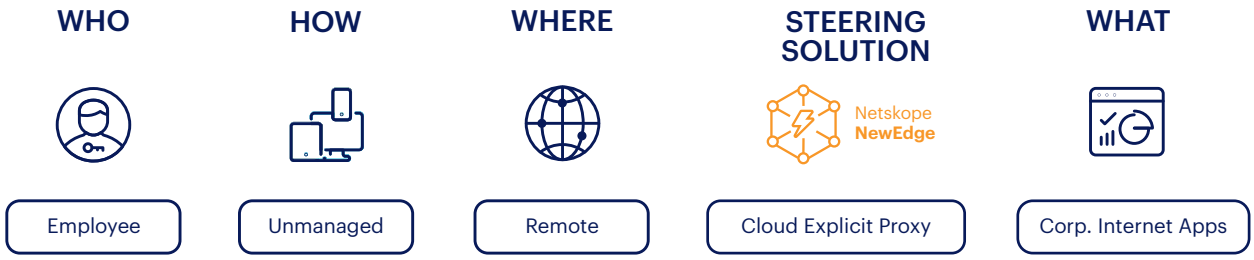
Recommended Architecture for Accessing Corporate Internet Apps - Steering with Cloud Explicit Proxy (CEP)

In a hybrid model, organisations need to expose applications that are hosted in their data centers or on public clouds over the Internet. To reduce the attack surface, organisations would like to allow access from only trusted sources (like Netskope IP ranges or Dedicated Egress IP Address services) post authentication.

For such use cases, where we need to steer the web traffic from the remote endpoint to Netskope NewEdge Data Plane, we recommend Netskope Cloud Explicit Proxy steering method. Please note that this Cloud Explicit Proxy only supports web traffic, and is not supported with desktop or mobile thick/native apps.

Steering of the web traffic is done via PAC file. Once the PAC file is downloaded, the web traffic from the endpoint will be proxied via the cloud proxy service in the Netskope NewEdge Data Plane.

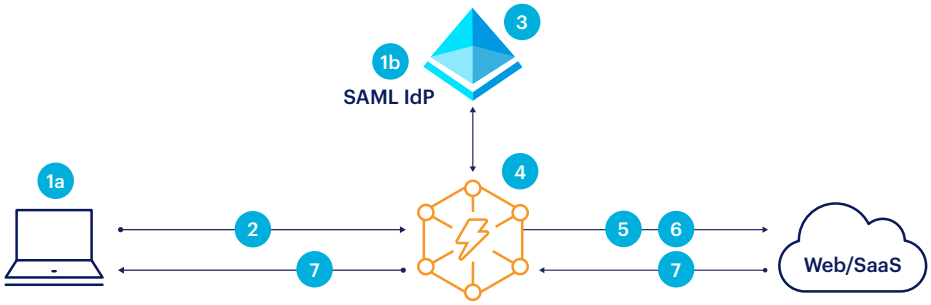
For enterprises that use managed Chromebooks and want these devices to also leverage the Netskope NG-SWG, Netskope provides a Chrome Extension that makes enabling and managing connections to Cloud Explicit Proxy easier.



Currently, Netskope doesn't host PAC files, therefore customers who require to implement this use case need to host the PAC file in their environment.

In case the customer has a need to bypass Netskope security cloud for some type of traffic, traffic exceptions need to be configured at PAC file level.

Traffic Flow to Corporate Internet Apps via CEP



1. As a prerequisite.
   a. PAC file to be hosted externally with destination proxy as `eproxy-<tenant>.goskope.com` on port `8081`
   b. SAML based Identity Provider (IdP) for authenticating the user.
2. All web traffic will hit the cloud forward proxy service at Netskope NewEdge Data Plane.
3. User authentication against the defined SAML IdP.
4. Post successful authentication, traffic will be inspected against the real time security policies defined.
5. Allowed traffic is forwarded from Netskope NewEdge Data Plane to the original destination on the Internet.
6. Traffic will egress the Netskope NewEdge Data Plane with the shared Netskope IP address range. If the customer desires to egress with a dedicated IP address, then Dedicated Egress IP Address services can be provisioned.
7. Response traffic from the Internet will be destined to Netskope NewEdge Data Plane, which will be inspected before being forwarded to the endpoint.

Pre-requisites

1. PAC file to be hosted externally with destination proxy as `eproxy-<tenant>.goskope.com` on port `8081`
2. SAML IdP for user authentication.
3. Cloud Explicit Proxy Root CA has to be deployed and trusted on all devices.

Benefits

1. **Inspection** of traffic to Corporate Internet Apps from remote unmanaged endpoints.
2. **Conditional Access** to Corporate Internet Apps/SaaS is allowed only from Netskope IP ranges or DEIP allotted to the customer tenant.

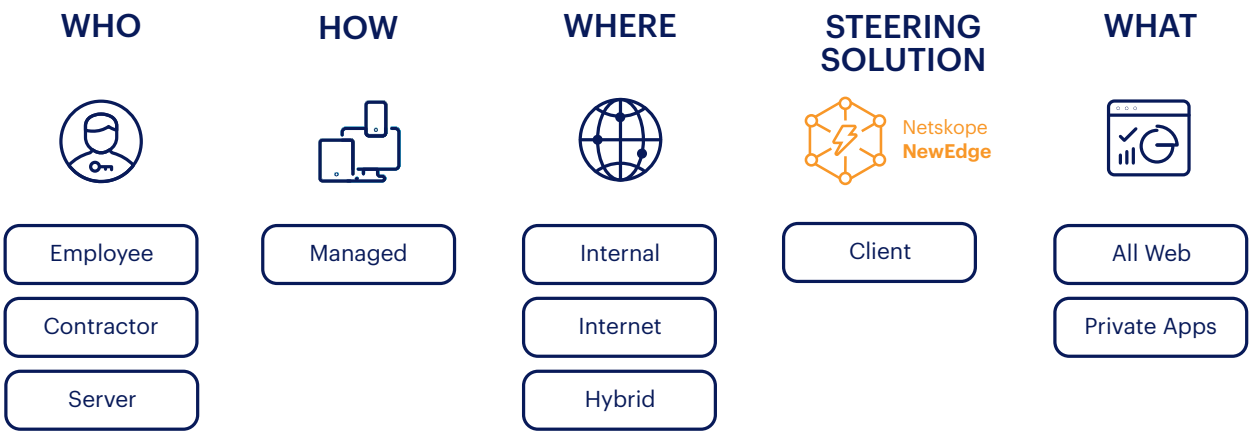
TRAFFIC STEERING METHOD WITH NETSKOPE CLIENT

When to use

- Netskope client can be installed on the endpoint.
- Organizations want inline inspection of all traffic - web or non-web from and to the endpoint to be inspected by the SSE.
- Organizations want a single client for SASE capabilities like Secure Web Gateway, Data Loss Prevention including endpoint Data Loss Prevention, Threat Protection, In-line Cloud Access Security Broker, Cloud Firewall, DNS Security, Remote Browser Isolation & SD-WAN Network Performance.
- Organizations want complete visibility into the user and the endpoint.
- Single client with SSE and SD-WAN capabilities, especially when the user could be using a patchy or lossy network connection.
- Need end-to-end visibility to help proactively detect issues with network, endpoint or application using Netskope Proactive Digital Experience Management (DEM).

This is the Netskope recommended steering method.

As represented in the diagram below, all user traffic to Internet or Internal Private Applications, either web or non-web, will be steered by the Netskope Client to the closest Netskope NewEdge Data Plane (DP) or Point-of-Presence (POP).



Netskope Client

- The Netskope Client is a lightweight steering agent that provides the most comprehensive control and visibility.
- The Netskope Client supports a wide variety of operative systems including Microsoft Windows, Apple macOS, Linux (Ubuntu), Android OS and Apple iOS.
- Netskope Client Agent can be deployed via direct download, email invite, IdP Enrollment, User Endpoint Management (UEM) or Mobile Device Management (MDM) for remote installation without user interaction.
- By default, the Netskope Client is installed in "Single-User" mode. This mode should be used for endpoints that are allocated to an individual user and the device will never be shared. Where multiple users are sharing the same system or device, the Netskope Client must be installed in "Multi-User" mode. Examples where multi-user mode should be considered:
  - Shared Workstations / Laptops.
  - Persistent and Non-persistent VDI.
  - Citrix Virtual Apps with Hosted Shared Desktop .
  - Windows Remote Desktop Services.
  - Floating/Loaner Laptops when loaner PCs that are given to employees on a temporary basis.
  - Kiosk Desktops, such as shared desktops in call centers, conference rooms, front desks, etc.

Netskope Client - Connectivity Requirements

Client Tunnel Establishment

The Netskope Client will always attempt to establish a DTLS (UDP/443) or TLS (TCP/443) tunnel directly with the closest best performing Netskope Data Plane (DP). To allow the Netskope Client to establish a direct connection with the data plane, the Netskope Client must be able to resolve FQDNs within the goskope.com zone. Best practice is to allow DNS resolution of any .goskope.com domain names.

Please refer to: https://docs.netskope.com/en/netskope-client-network-configuration.html for the latest and updated FQDN and IP list.

The minimum requirement for the Netskope Client to work is to have the internal DNS able to resolve the domain `*.goskope.com`. In an environment where internet recursive DNS is disabled, DNS zone forwarding rules for `*.goskope.com` must be created. **If DNS zone forwarding is strictly not possible/permitted, then Netskope Client tunnels can't be used and an alternate steering method must be used, such as Explicit Proxy over IPSec or GRE tunnels (EPoT).**

Netskope Client - Automatic Data Plane Selection

Netskope utilizes multiple methods to select the optimal Netskope Data Plane to connect users to you will not have to do any configuration or assignment for this. The below methods are in order of precedence if they are enabled on your tenant.

Netskope Global Service Load Balancing

Netskope has added a new service to enhance the Automatic Data Plane section process.

- The client will make a REST API call to `gateway.gslb.goskope.com`
- The API provides a list of the top 10 Netskope DP based on the client IP geo-location and the Round-Trip-Time (RTT) for each DP.
- The Netskope Client will then choose a Primary and Backup data plane based on the best RTT.
- The Netskope Client re-evaluates the RTT every 15 minutes and if there is a data plane which has a 25% better RTT than the currently active one, the Netskope Client will switch to the better performing data plane.

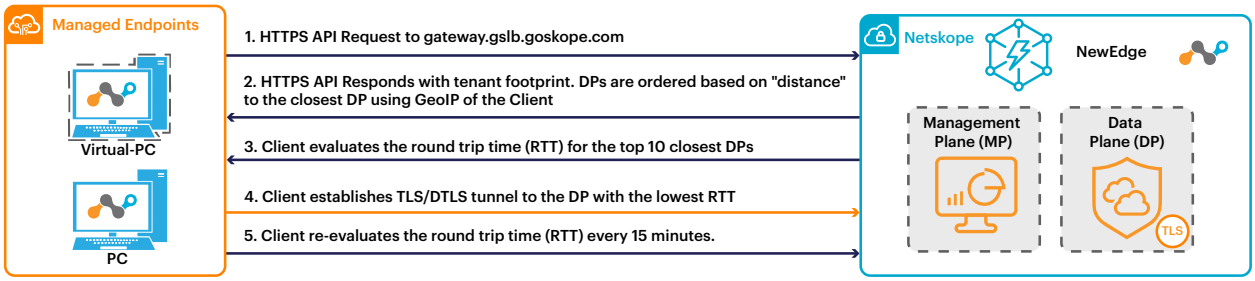


Figure 1: DP selection using Netskope GSLB API

Google DNS

If the Data Plane cannot be determined via GSLB API the Netskope Client will fallback to utilizing a call to Google DNS. In this case:

- The Netskope Client uses Extended Client Subnet (ECS) extension when performing DNS lookups to determine the closest Netskope data plane. ECS provides the Client IP /24 subnet address in the DNS request.
- Netskope Client has been designed to use DNS-over-HTTPS (DoH) protocol which supports ECS as a parameter in the DoH request.
- The Netskope Client is configured to use Google DNS (dns.google) for all DoH (TCP/443) requests which are then forwarded to the Netskope authoritative DNS resolvers. Google DNS (dns.google) is used for the data plane selection only.
- If the Netskope Client can't communicate with Google DNS (8.8.8.8/8.8.4.4), it will fallback to the configured Local DNS (LDNS) obtained by DHCP or configured on the endpoint.

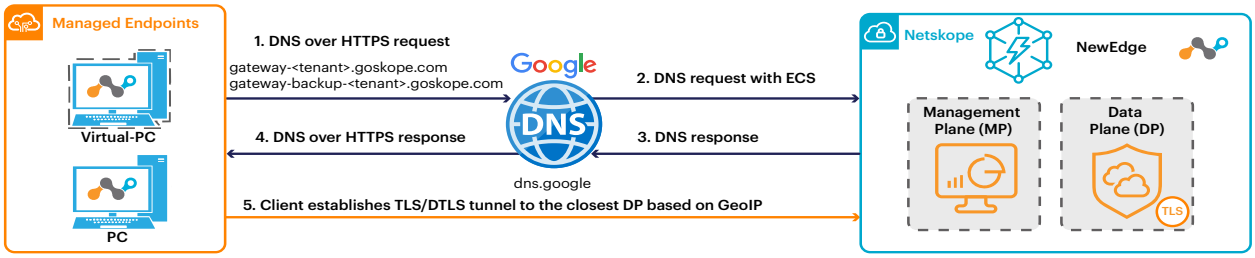


Figure 2: DP selection using Google DNS

Local DNS

The final DNS method is Local DNS (LDNS). In this case the Netskope Client will use the corporate DNS infrastructure to resolve the best Netskope Data Plane.

However, with this method there is a riks, that the user does not get connected to the closest and best Data Plane or Point of Presence (PoP) when the corporate DNS infrastructure is too centralized.

Wrong Nestkope PoP selection with corporate DNS:

1. Client request DNS resolution for gateway-x.goskope.com
2. HQ corporate DNS server is asking Netskope DNS server with the HQ internet breakout address.
3. Netskope DNS responds with a German PoP address.
4. Netskope Client is connecting to the German PoP and to Spain.

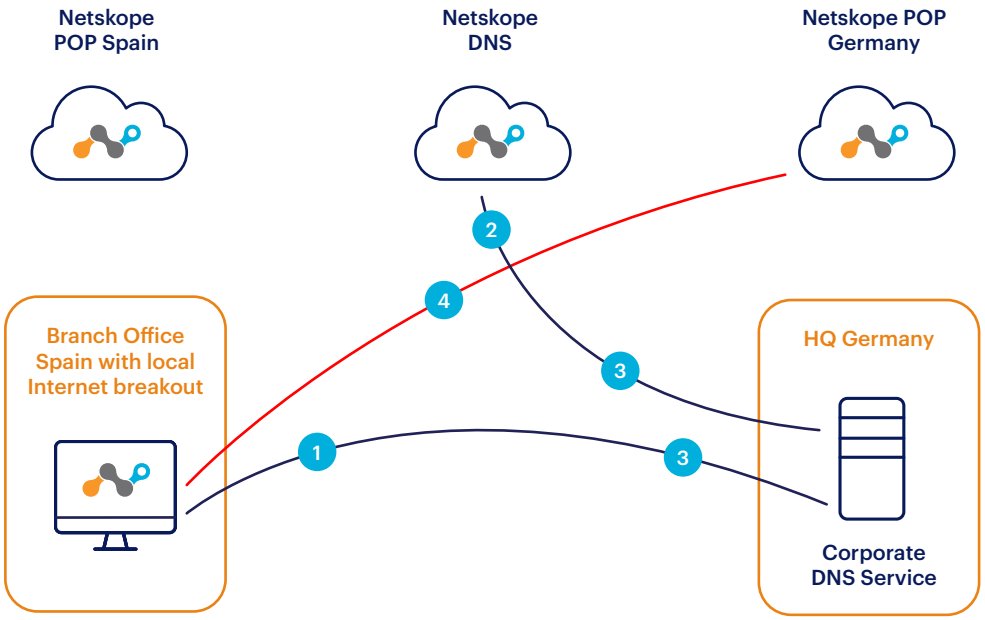


Figure 3: Wrong PoP selection with corporate DNS

Note: Netskope recommends blocking DNS over HTTPS (DoH) via Netskope Real-Time Policy as it forces the browsers to use regular DNS hostname resolution. In this way, Netskope Client continues to monitor the DNS responses and maintain the IP address to hostname mapping, and honor any steering exceptions as needed.

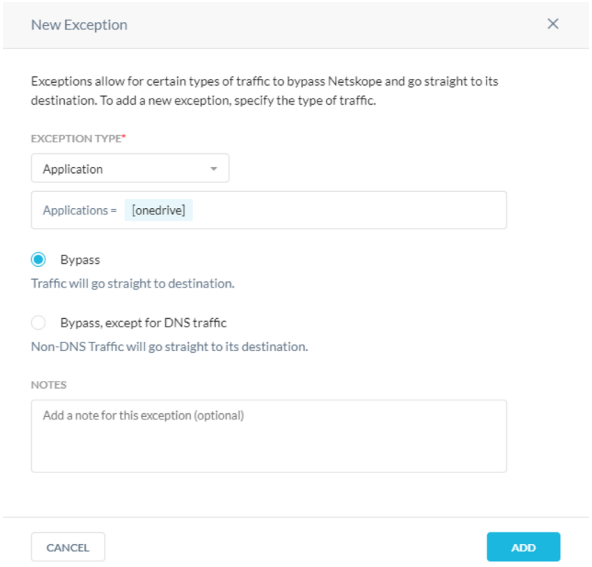
Netskope Client - Steering Configurations

By default the Netskope Client will intercept HTTP/HTTPS (TCP 80 & 443) traffic when enabled for Web/Cloud Apps OR all TCP, UDP and ICMP when the Cloud Firewall module is enabled. Custom ports can be configured to be treated as HTTP/HTTPS traffic and be evaluated against the SWG rules. Traffic is steered to Netskope SSE based on the Steering Configuration.

Steering Exceptions

Steering Exceptions can be configured for the following types of elements:

- Certificate Pinned Applications
- Web Categories
- Domains
- Source/Destination Locations
- Source Countries



When traffic matches a Steering Exception, the Netskope Client will not tunnel the traffic to Netskope SSE and it will be handled by the underlying operating system for processing and routing.

For example, in the picture above, for the specific application of onedrive (Netskope will automatically get the domains) we are setting up a Bypass, this means that the traffic will go straight to its destination, not steered through Netskope.

However, Certificate Pinned Applications have the option to Bypass Netskope Proxy + Tunnel, which will tunnel the traffic to Netskope and egress via Netskope Data Plane, but it will bypass SSL decryption and policy enforcement. This provides additional visibility and it's recommended to enable Bypass + Tunnel for Certificate Pinned Applications as it prevents the need to open and manage firewall rules for these applications.

Netskope Client - Interoperability with 3rd party VPN clients

When working remotely, many customers configure their VPN clients in “Full” tunnel mode to steer all network traffic from the endpoint to the data center. This is typically done as a security best practice to ensure no traffic from the managed endpoint can evade inspection of the enterprise network security controls. When the Netskope Client is deployed, it establishes a TLS and DTLS tunnel to the Netskope Security Service Edge (SSE), and steers web/cloud traffic to the Netskope SSE applying security functions such as DLP, threat protection, access control, etc.

If the VPN tunnel is established in full tunnel mode, the Netskope Client (TLS and DTLS) tunnels will be routed over the VPN tunnel. This presents the following suboptimal outcomes:

- Traffic to the Netskope SSE will take a suboptimal route, especially in a distributed environment where remote users are geographically distant from the enterprise network. Such routing defeats many benefits of Netskope's distributed SSE network.
- Internal security infrastructure is blind to the Netskope bound traffic, due to the requirement to disable SSL Decryption - it has no visibility into TLS/ DTLS tunnels and thus provides no additional security value.
- Customers don’t realize the full benefit of leveraging SSE for offloading security processing from their on-premises infrastructure, such as SSL/TLS decryption.

For the Netskope Client to interoperate with 3rd party VPN clients, the VPN client should be configured in Split tunnel mode to allow Netskope tunnel to egress directly via Internet to the closest Netskope data plane location.

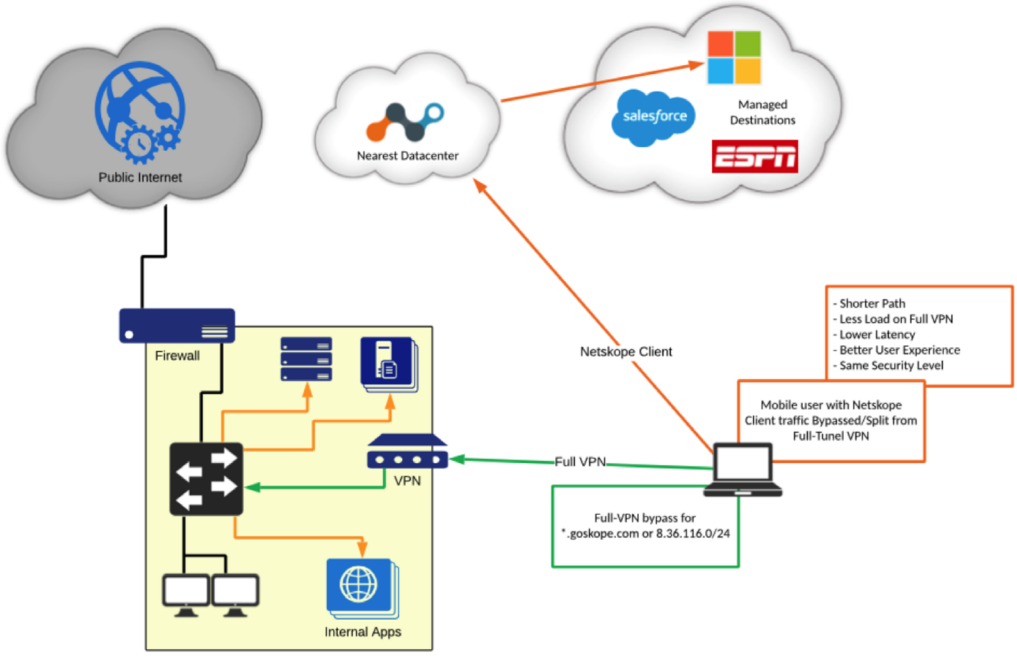


Figure 4: Tunnel with Exception VPN (Recommended)

Additional reading Don't Strangle your SASE article

In addition to configuring Split tunnel mode, you will need to add Steering Exceptions for the Netskope Client to bypass the VPN concentrator gateway IP addresses to prevent SSL VPN traffic being steered to Netskope SSE. Steering exceptions need to be configured in the Netskope Tenant User Interface (UI). Please refer to Exception Configuration for VPN Applications: https://docs.netskope.com/en/exception-configuration-for-vpn-applications.html

For more recommendations and pros/cons of Split vs Full VPN tunnels refer to this blog post from the Netskope portal: https://www.netskope.com/blog/dont-strangle-your-sase

Benefit of deploying Netskope Client

- Netskope Client is the preferred steering method and customers are always advised to deploy whenever possible. It facilitates universal connectivity to the Netskope Security Cloud regardless of the user and endpoint location.
- These benefits are a solution for common issues of the past such as lack of security if the user is outside of the organization, lack of Zero Trust approach to the access to company resources and no integration with the identity and the security stack. This causes companies to have a highly complex operation with a lot of blind spots that put the organization at risk.
- In the context of discussing how Netskope addresses challenges with legacy architecture, the following sections highlight the benefits for organizations looking to enhance their network security, user experience, and operational efficiency:
    - Remote worker support
        - Network based architecture usually relies on backhauling the traffic to a datacenter to apply network based security. This generates higher latency and capacity issues.
        - Netskope Client can redirect dynamically to the closest datacenter and leverage New Edge peering to provide the best user experience.
    - Authentication
        - Authentication has always been a challenge with proxies, which rely on HTTP authentication mechanisms to authenticate/identify the user. But it is not transparent for the browser or the application that needs to support it and generates a dependency on the directory/IDP. As a consequence it can generate performance and availability issues while not accurate (IP based authentication is weak). Moreover, customers need to manage complex exception lists for applications like office applications which don't support HTTP authentications.
        - Netskope Client solves those issues by performing client certificate based authentication at the network level (SSL session to connect to the Data Plane), which means:
            - It's only done once, not for each domain/session.
            - It's invisible for the browser or the app, it cannot fail, therefore no exception to manage.
            - It's not based on the IP but on the SSL session, therefore more secure, no problem to share the same IP.
            - It doesn't need any interactive validation with any IDP, so even if the IDP or AD is down the authentication is still working.

- **Easier to deploy**
  - Network based deployment requires architecture design, build, validation which takes months to complete and requires additional work on the authentication integration, PAC hosting and Root CA deployment.
  - Netskope Client can be easily deployed with SCCM (System Center Configuration Manager) or any EDM (Enterprise Device Management), the authentication and SSL CA are automatically and transparently deployed.

- **Flexible steering**
  - Network based steering relies mainly on PAC files which are complex to manage. Don't forget that if the PAC distribution is not properly working, the internet access will be broken. Internet outages - because of PAC mistakes - are common. Dynamic proxy distributions are often very complex to set and operate. The other issue with PAC files is that it doesn't guarantee that the flow will go through the proxy. An application may not support the PAC file or a malware can just ignore it.
  - Netskope client allows to configure steering centrally and provide smarter decisions like dynamic steering or SNI based steering. It's even possible to provide fail close mechanisms. Finally, there is no risk of syntax errors or PAC availability with Netskope Client steering.
  - In environments without a default route to the Internet, and or no public DNS resolution, Netskope Client can be deployed in Explicit Proxy mode.

- **Better Security**
  - When PAC file are used, applications can ignore or bypass explicit proxy.
  - Netskope Client cannot be disabled (unless admin allows it) and can leverage additional security features like fail close and device classification.
  - The root certificate for SSL inspection are automatically installed with the Netskope Client.

- **Enhanced user experience**
  - With network based deployment, it is impossible to display user notification / error messages inside native apps. It is also challenging to insert interactive messages inside complex SaaS services like O365 or G Suite. Therefore users won't be aware of what's wrong in the application, resulting in a bad user experience.
  - With Netskope Client, we can leverage popups to display notifications when we cannot display them in the browser: for native apps, for complex SaaS applications in the browser. Moreover, we can leverage the notification to request end user feedback (justification) which legacy solutions cannot provide. In these cases, the users are aware of what's wrong with the application, resulting in a better user experience.

- Simple management
  - Troubleshooting network based deployment is often complex because the user activity is mixed with all users and on the device there are no embedded troubleshooting tools. Packet capture is often the only way to troubleshoot but requires additional software and rights to be performed.
  - Netskope Client is extremely simple to troubleshoot.
  - The debug log is providing details about steering decisions, configuration updates, behavior of the client in general.
  - Debug log level can be controlled remotely.
  - Logs can be retrieved centrally, without any user action.
  - Packet capture and speed test can be performed directly from the client.
  - Netskope Client also provide remote control (enable/disable/fail close) and granular upgrade control (latest version, specific golden release).

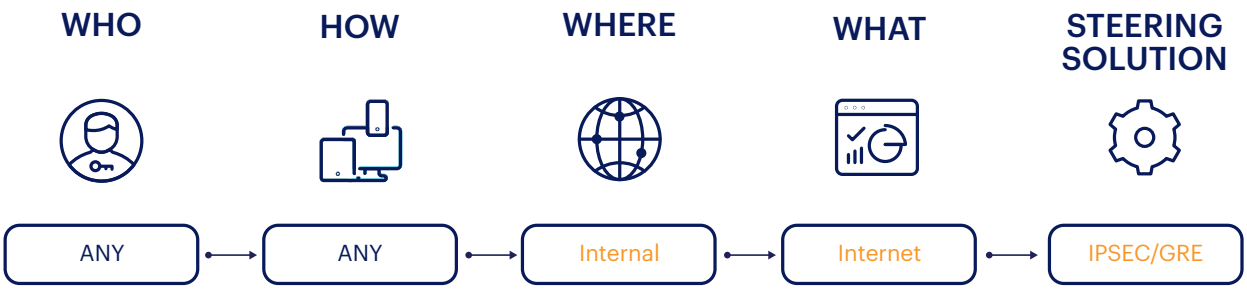
- Operational Cost Reduction
  - No on-premises proxy software/hardware, decryption hardware, management tools and load balancers required.
  - Zero Trust: User Identity and Endpoint Identity is available for granular policy-based decisions.
  - Zero Trust: Device Classification / Device Posture.
  - Operation simplified: Unified SWG, CASB, CFW, ZTNA and Endpoint DLP using a single client.
  - Although compatible, No on-premises proxy software/hardware, decryption hardware, management tools and load balancers required for this deployment.
  - Always ON.

More information about the Netskope Client can be reviewed on the Netskope Documentation site (https://docs.netskope.com/en/netskope-help/traffic-steering/netskope-client/).

TRAFFIC STEERING METHOD WITH NETWORK TUNNELS

When to use

- When it is not possible to install Netskope client on the endpoint. In this scenario, it is recommended to steer the traffic from the endpoint to Netskope NewEdge DP over a network tunnel.
- Netskope supports IPSec or GRE tunnels from a capable device, such as a router, firewall, SD-WAN appliance, or public cloud platform such as AWS, Azure and GCP.
- Scenarios where network tunnels should be used/considered:
  - Server that run without an explicit user login.
  - Unmanaged devices on a managed network, for example, Guest Wifi.
  - Devices that don't support Netskope Client, for example, IoT/Smart devices.



Traffic can be steered from the endpoints over the Network Tunnels to Netskope NewEdge DP using either:

- Transparent Policy Based Forwarding/Routing (PBF/PBR) or
- Configuring an Explicit Proxy, better known as Explicit Proxy over Tunnel (EPoT).
- Netskope Borderless SD-WAN offering can also be considered, which provides orchestration for tunnels and can automatically set up tunnels to Netskope NewEdge DP from its HW-based or virtual edge devices. This provides a seamless way to steer traffic to Netskope using network tunnels.
- Integrations with other SD-WAN vendors are also available and are documented here https://docs.netskope.com/en/netskope-help/integrations-439794/ipsec-and-gre/.

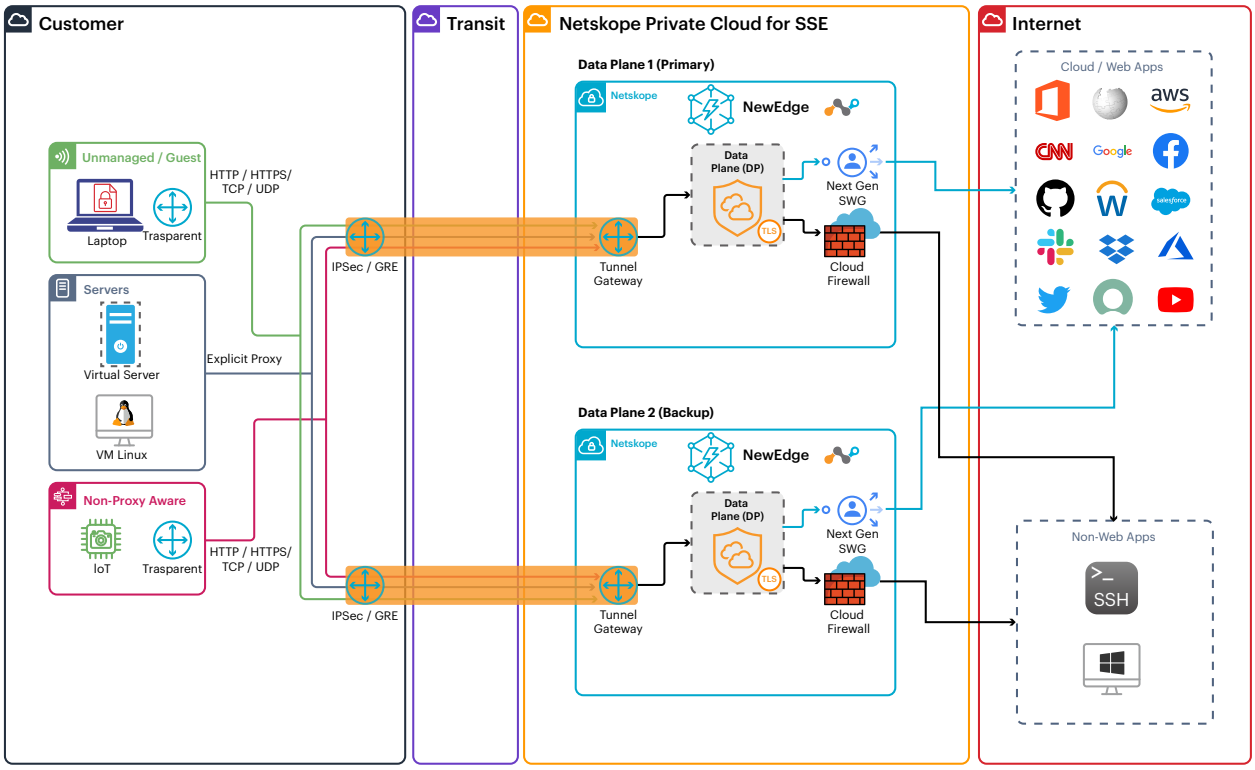


Figure 5: Tunnel Steering Example

Prerequisites

- Install the Netskope Root and Intermediate CA certificate on all devices where SSL decryption is required.
- SAML IdP to authenticate users.
- Ensure that **Many-to-One NAT** is not enabled on the network device that is initiating a tunnel to Netskope so that the real endpoint device IP is used for identity and policy-based decisions.
- For resiliency, create at least two tunnels to different Netskope NewEdge DPs from each site.

IPSec Tunnels

Internet Protocol Security (IPSec) is a secure network protocol that authenticates and encrypts the packets of data to provide secure encrypted communication between two endpoints.

Supported features and limitations:

- Maximum of 16,000 hosts per IPSec tunnel.
- The maximum number of tunnels (SAs) per IKE connection at one time is 10.
- 500 Mbps throughput limit per tunnel. 1Gbps is available with Netskope approval and is an add-on SKU available for purchase.
- NAT-T traversal must be enabled.

- IKEv2 only.
- Multiple tunnels can be created per source peer IP, using different source identities.
- Authentication: Pre-Shared Key.
- Traffic from the same user or endpoint must go through the same tunnel. Load balancing is supported using Source IP persistence.

Supported IKEv2 Parameters

- Phase 1 Parameters
  - Encryption algorithms: AES128-CBC, AES192-CBC, AES256-CBC
  - Integrity algorithms: SHA256, SHA384, SHA512
  - DH Group: 14, 15, 16, 18
  - SA lifetime: 24 hours
  - Dead Peer Detection (DPD)
- Phase 2 Parameters
  - Encryption algorithms: AES128-CBC, AES256-CBC, AES128-GCM, AES192-GCM, AES256-GCM, Null
  - Integrity algorithms: SHA256, SHA384, SHA512
  - DH Group: 14, 15, 16, 18
  - PFS: Supported
  - SA lifetime: 2 hours

GRE Tunnels

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links. GRE uses logical tunnel interfaces that terminate to a Netskope NewEdge DP. The NewEdge GRE gateway validates the source peer (router/firewall) IP of the tunnel against the configured source peer in the Netskope User Interface (UI).

Supported features and limitations:

- Maximum of 64,000 hosts per GRE tunnel.
- 1 Gbps throughput limit per tunnel.
- Maximum of one (1) tunnel per source peer IP for each Netskope data plane.
- ICMP keep-alive must be sent to the probe IP only.

Despite the fact that the GRE tunnel is not encrypted, web traffic traversing the GRE tunnel is encrypted using HTTPS for the vast majority of traffic. The small remaining percentage of traffic sent with HTTP which is not encrypted and usually accounts for less than 5% of traffic, will be sent in the clear.

Policy Based Forwarding/Routing

Policy Based Forwarding/Routing (PBF or PBR) is transparent to the endpoint and should be configured to steer TCP/80 (HTTP) and TCP/443 (HTTPS) by default. Non-standard web ports are also supported but must be configured in the tenant steering configuration for the traffic to be accepted. If Cloud Firewall has been enabled, you can steer all Internet bound TCP, UDP and ICMP traffic over the tunnel.

PBF has the advantage of not requiring any specific configuration on the end point to steer traffic to Netskope, therefore can support applications that are not “proxy aware”. PBF supports Authentication using SAML or can be disabled based on Domain, Web Categories, User Source IP Address and Egress (ISP) Source IP Address.

Important: Only steer traffic that is configured to be accepted over the network tunnel. All other traffic will be dropped.

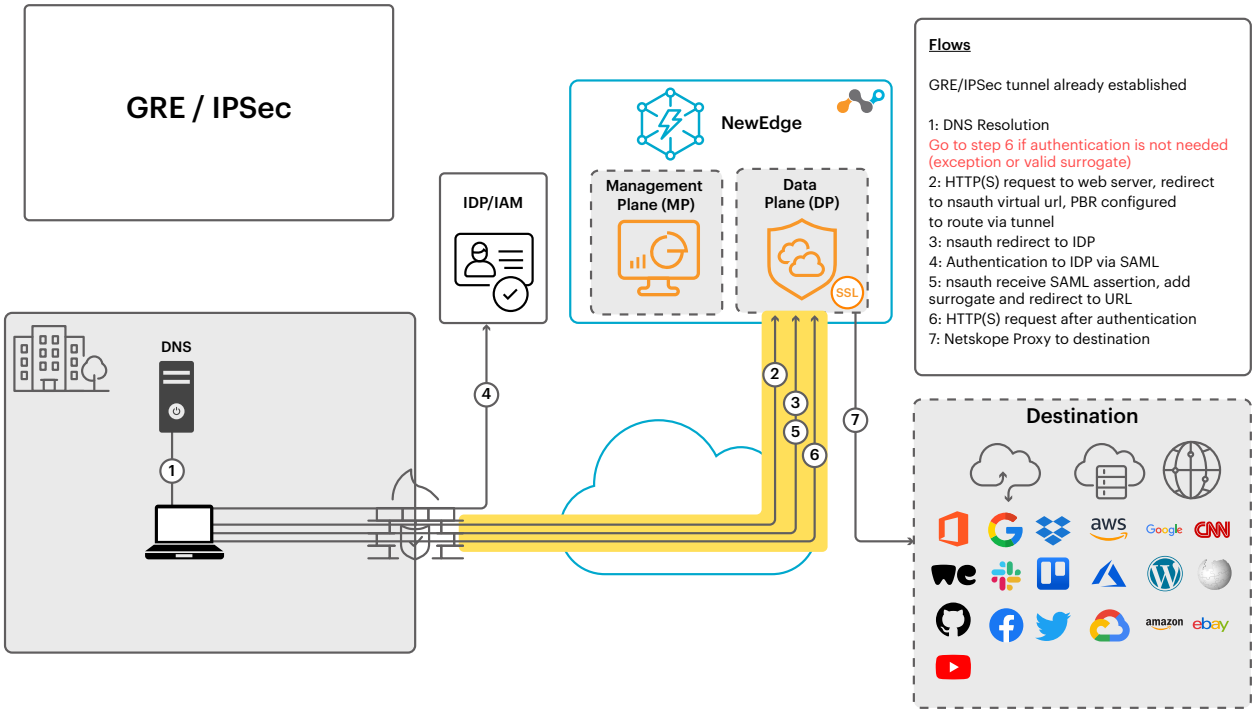
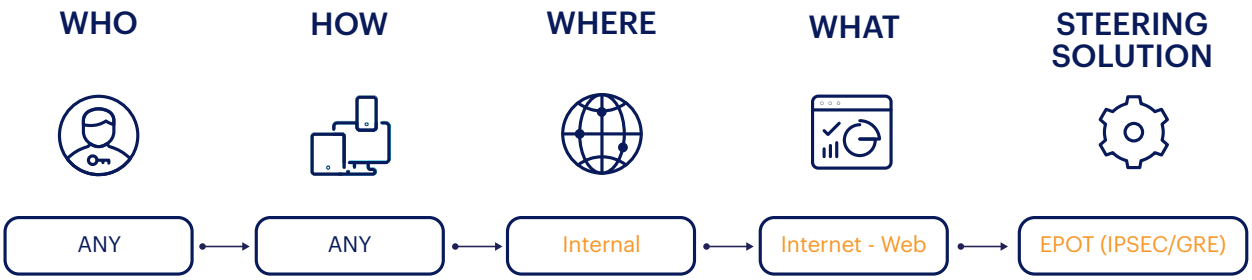


Figure 6: IPSec / GRE – Policy Based Forwarding

TRAFFIC STEERING METHOD WITH EXPLICIT PROXY OVER TUNNEL (EPOT)

When to use

- When it is not possible to install Netskope client on the endpoint, but it is possible to configure an Explicit Proxy on the endpoint.
- When tunnels can be setup from the site to Netskope NewEdge DP, but it is not possible to define Policy Based Forwarding to steer traffic from the endpoint to the tunnel.



EPoT is like any other explicit proxy configuration, but the explicit proxy endpoint is only available when an IPSec or GRE tunnel is established. You can steer clients to use the explicit proxy by using a Proxy Auto-Configuration (PAC) file or setting the explicit proxy IP and port manually within the client.

Note: The dedicated Explicit Proxy IP is `163.116.128.80/163.116.128.81`, port `80`. This IP address is accessible from any Netskope DP and terminates locally.

Prerequisites

- IPSec/GRE Tunnels from the site to Netskope NewEdge DP.
- Explicit Proxy to be defined using a Proxy Auto-Configuration (PAC) file or setting the Explicit Proxy IP and Port manually on the endpoint.
- SAML IdP to authenticate users.
- Add a /32 route for the dedicated Explicit Proxy IP addresses `163.116.128.80/163.116.128.81`, port `80` to be routed over the network tunnel.

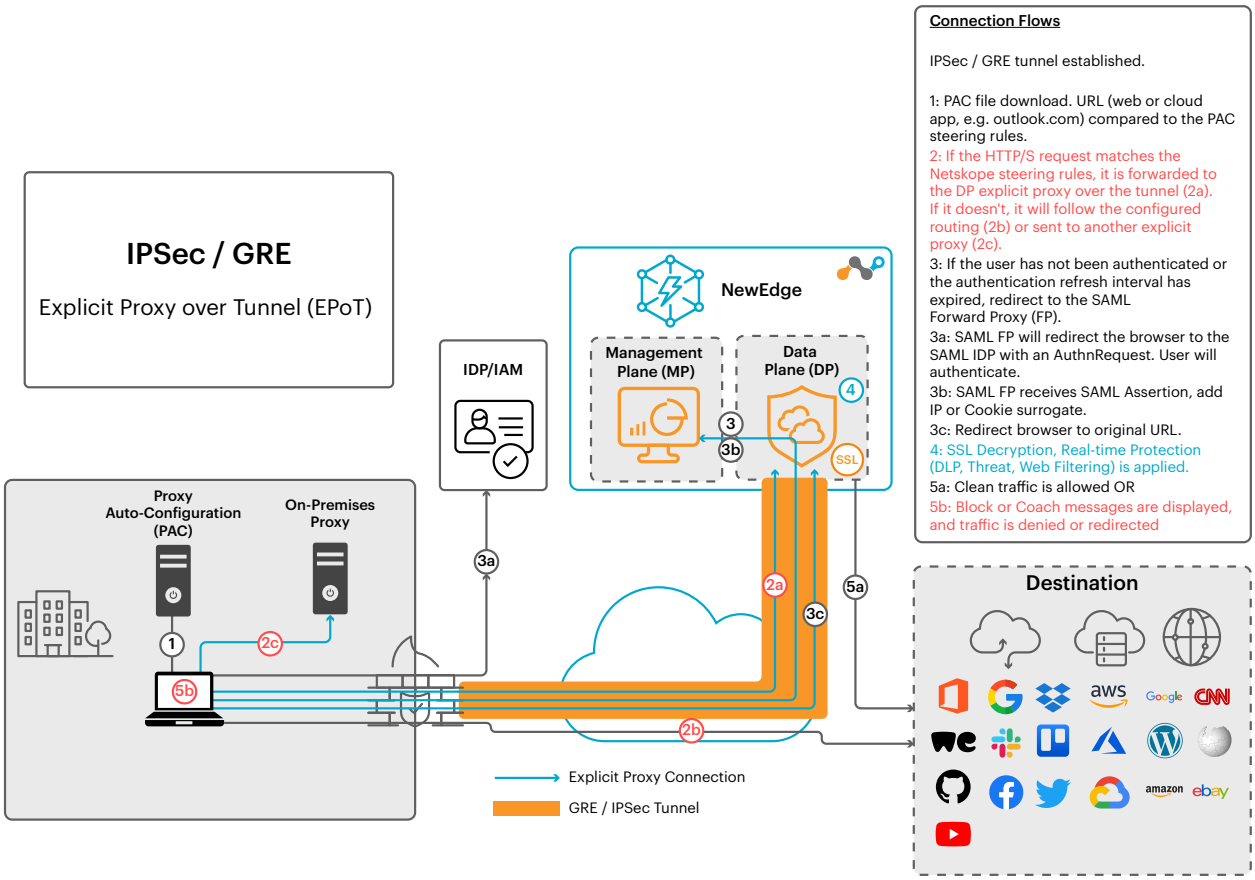


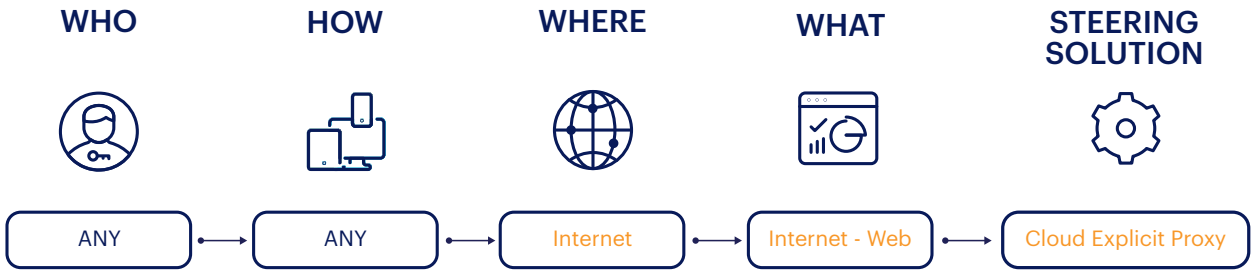
Figure 7: IPSec / GRE – Explicit Proxy over Tunnel

TRAFFIC STEERING METHOD WITH CLOUD EXPLICIT PROXY

When to use

Another way to steer traffic inline to Netskope SSE is via Cloud Explicit Proxy (CEP). This method can be leveraged when a Netskope Client cannot be installed or if there is a preference for Explicit Proxy architecture, for example when the network is a highly secure environment that doesn't have a default gateway. Additionally, Cloud Explicit Proxy does not require an IPSEC or GRE tunnel and can be reached from the Internet.

Please note that this Cloud Explicit Proxy only supports browser-originated traffic, and is not supported with desktop or mobile thick/native apps.



Prerequisites

1. The Operational System or Browser explicit proxy settings should be changed to use a PAC file or point directly to the Netskope explicit proxy FQDN.
2. The Certificate Authority for SSL decryption should be manually installed.
   a. For roaming users leveraging this architecture, an additional CA has to be installed for the Captive Portal (CN: `eproxy.caadmin.netskope.com`).
2. The local network firewall should allow connections to port 8081 on the designated explicit proxy FQDN, for example `eproxy-<tenant_name>.goskope.com`
3. Users can be identified by your identity provider (IdP) with Single-Sign on or the source IP's can be added to the Allowlist and bypassed from authentication.
4. When using your IdP for Single-Sign On the IdP portal domain(s) should be bypassed from authentication to guarantee that the page successfully loads.

The architectures below demonstrates how CEP works on the Netskope SSE Platform when a user is roaming:

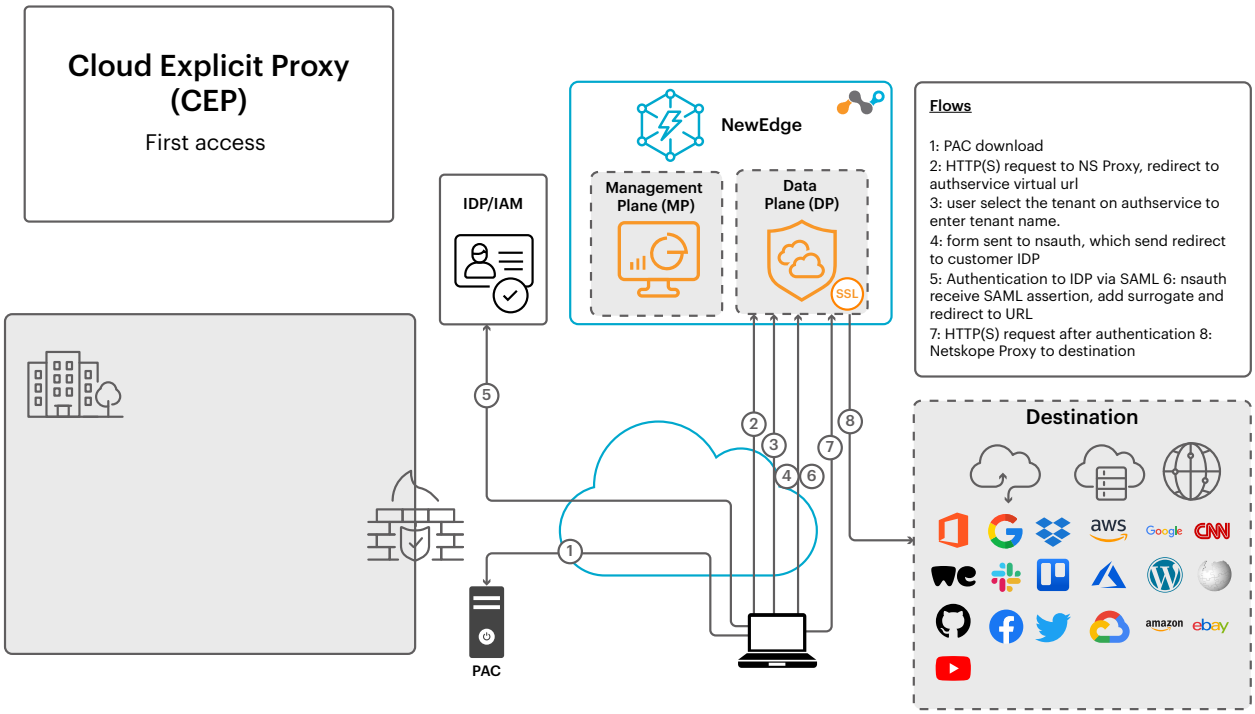


Figure 8: CEP - First Access (before authentication)

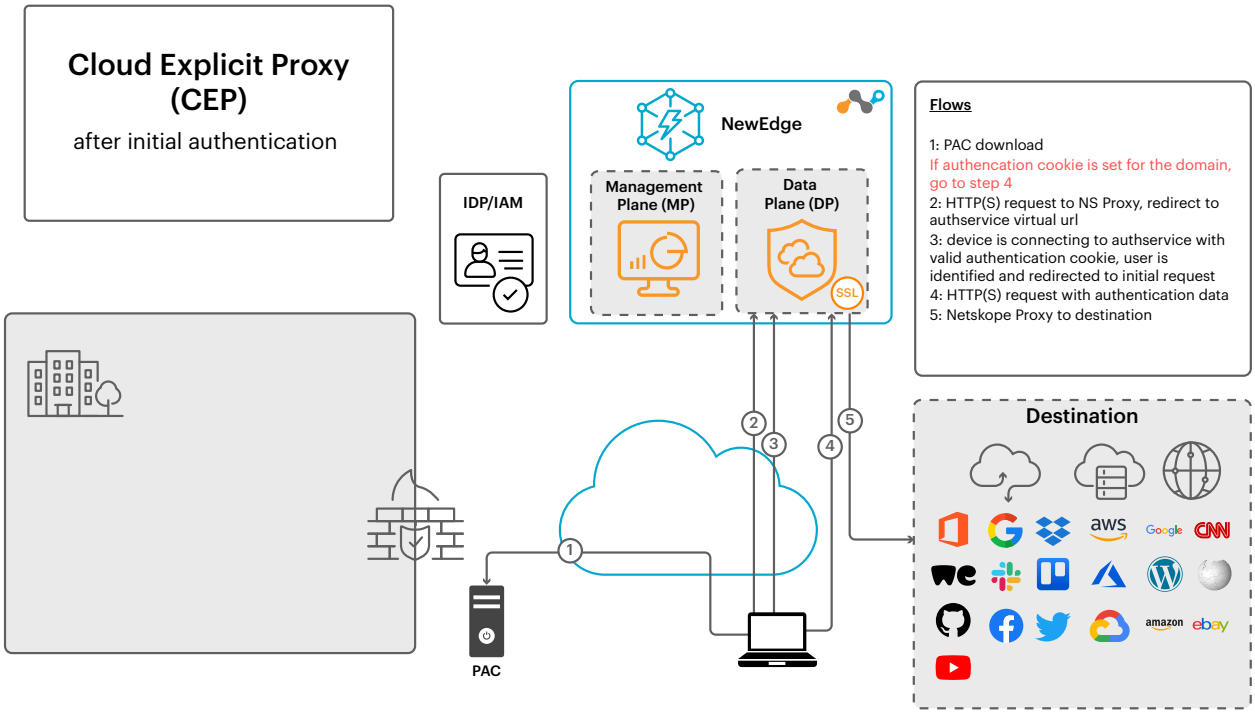


Figure 9: CEP after initial authentication

Support for ChromeOS devices

For enterprises that use managed Chromebooks and want these devices to also leverage the Netskope NG-SWG, Netskope provides a Chrome Extension that makes enabling and managing connections to Cloud Explicit Proxy easier.

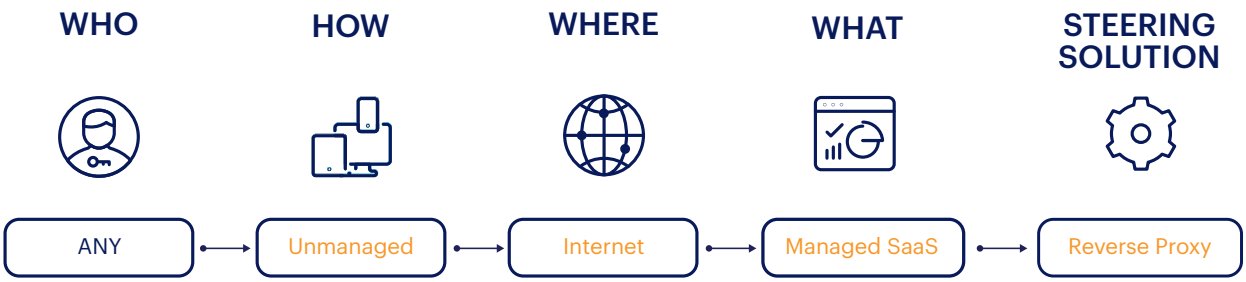
This method makes use of the Explicit Proxy steering, but with help of the extension, tenant information that users typically have to enter on each new session are suppressed and uninterrupted smooth experience for the users is achieved. Netskope official documentation provides detailed information on how to install and manage the extension and SSL certificates using the Google Admin Console.

The extension can be downloaded from the Chrome WebStore here.

TRAFFIC STEERING METHOD WITH REVERSE PROXY

When to use

- When the employee or a contractor with an unmanaged endpoint needs to access managed SaaS applications



Internal Private Web Applications can be securely accessed over the Internet from remote endpoints without Netskope client via Netskope Reverse Proxy steering method.

Non-web Private Applications can be published via Apache Guacamole like service, which can then be accessed using Netskope Reverse Proxy solution. For example, RDP over HTTPS or SSH over HTTPS.

Prerequisites

1. Internal Web applications need to be defined as Private Apps with Browser Access enabled in the customer tenant.
2. Remote users need to access the Internal Private Web Application from the browser via the unique URL (ending with `goskope.com`) provided in the respective Browser Access configuration. CNAME DNS record will need to be made if a customised friendly FQDN is desired.
3. SAML IdP for user authentication.

CONCLUSION

At Netskope, our primary objective is to assist our customers in staying ahead of the various security challenges related to cloud, data, and network systems. Our customers exhibit diverse needs and environments; some prioritize user experience, while others emphasize strict regulatory compliance. Nevertheless, they all share a common concern: the need for robust security against continually evolving cyber threats.

At Netskope, we are dedicated to ensuring that our solution deployments are entirely customer-centric, encompassing a wide range of deployment options without compromising on security features. Our multi-model deployment approach includes:

- Netskope Steering Client (Netskope Client)
- Network Tunnels: Utilizing IPSec or GRE
- Tunnelled Explicit Proxy: Implemented over Network Tunnels (EPoT)
- Explicit Proxy: Leveraging Cloud Explicit Proxy (CEP)

What sets Netskope apart is that our solutions are adaptable to environments of all sizes and scales.

APPENDIX 1 - DEDICATED EGRESS IP ADDRESS (SOURCE IP ADDRESS PINNING)

Requirement

It is very common to see cloud architectures that rely on IP pinning as a way to prevent unauthorized access to cloud services. This is when an Access Control List (ACL) is configured in the Cloud Service only allowing access to the application from IP addresses which are owned by the organization. One very common application to make use of this technique is Azure AD with Conditional Access Policies, which can be based off of incoming IP, as one of its evaluation criteria.

Challenge

This method tends to create challenges for roaming users due to the use of dynamic IP's and when a company adopts any kind of multi-tenant Cloud Proxy technology once the egress IP's are usually shared.

Solution

Netskope SSE solves this problem by also offering Dedicated IP addresses to egress traffic, guaranteeing that all traffic from a particular tenant egress the platform from an IP that is only used by the organization. Once licensed, customers are given a list of IP's in each Netskope DP that are exclusive to their tenant. Dedicated IP's work with all available steering methods.

Overview of Dedicated Egress IP (DEIP)

Netskope can optionally offer Dedicated IP addresses per customer tenant. This is a licensable feature and available on all NewEdge data planes. The solution allocates a minimum of 2x IP addresses from Netskope owned IP ranges per data plane per tenant and these IP ranges are completely separate to the shared pool range.

All traffic (SWG, Cloud Firewall) from the customer tenant will use these IP addresses. Netskope also has the ability of setting up policies to steer only certain traffic via Dedicated Egress IPs.

A maximum of 8 IP addresses per data plane can be made available depending on the customers traffic requirements and port exhaustion is actively monitored.

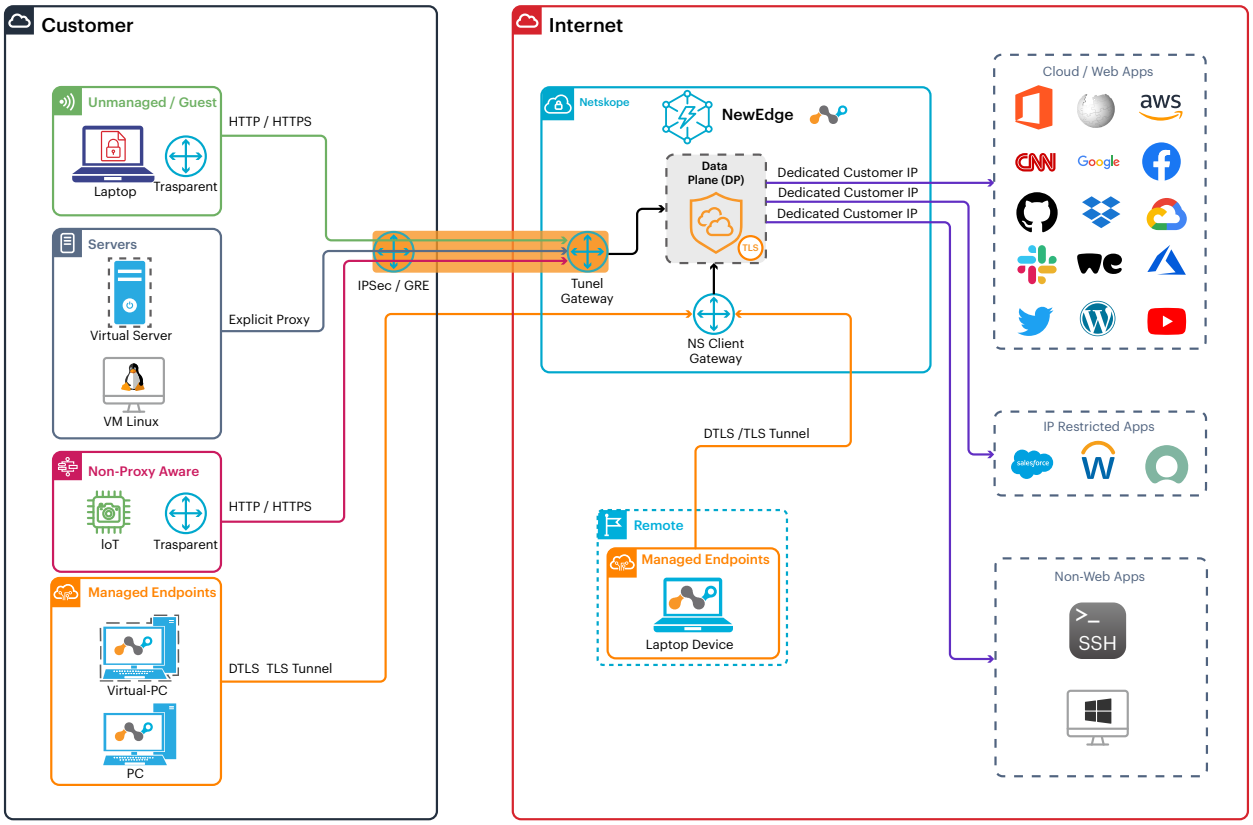


Figure 10: Netskope Dedicated IP Range

Benefits of DEIP

This option has the following benefits::

- It can be used as a broad security control to prevent users from accessing public Web and Cloud applications when not traversing the Netskope SSE platform.
- It can be used in access control policies like Microsoft AzureAD (Entra AD) Conditional Access Policies as an additional trust criteria for access of cloud apps or even specific riskier operations..
- It forces users to enable/install the Netskope Client to access the application when roaming.
- Remove the need to backhaul application access to private datacenter just to leverage allowed egress IPs, which can severely impact performance.
- Traffic traverses the Netskope SSE platform, therefore security controls are applied - Malware/ Threat, DLP, RBI.
- Netskope Cloud Firewall will use the same dedicated IP addresses for accessing Non-Web (TCP/ UDP) applications and ports.
- IP addresses are dedicated to the customer tenant for the life of the contract.

ADDITIONAL RESOURCES

Videos

- **Netskope: Flexible Deployment Options** (5 minutes and 42 seconds)
  https://www.youtube.com/watch?v=obRTgR8t6zk
- **Netskope Location Awareness and Steering** (3 minutes and 43 seconds)
  https://www.youtube.com/watch?v=946KK43hzjE

Training

- **Netskope Security Cloud Introductory Online Technical Training** (4 hours, divided into 10 courses ~ average time to completion: 25 minutes)
  https://www.netskope.com/training/netskope-security-cloud-introductory-online-technical-training
- **Steering related Courses:**
  - Course 8: Introductory Technical Training: Deployment Options Overview—15 min
  - Course 9: Introductory Technical Training: Netskope Out-of-Band Deployment Options—30 min
  - Course 10: Introductory Technical Training: Netskope Inline Deployment Option—25 min
- To request an account, please email: training@netskope.com. Include the following: first name, last name, business email address, and business name.

Lab

- **Self paced Hands on Lab** (client steering method, 2-4 hours with 48 hour access)
  https://www.netskope.com/company/events/intelligent-sse-hands-on-lab

Addendum

- **Firewall Rules / Network ACLs**
  The Netskope Client requires direct connectivity to the Netskope Security Service Edge (SSE) for the best possible performance. To allow the Netskope Client to connect directly to the Netskope SSE, TCP & UDP 443 must be allowed through the firewall to the SSE network IP ranges referred below. The Netskope Client uses HTTPS, TLS and DTLS protocols. Below are the IP ranges for the Netskope SSE Global network.

  Please refer to:
  https://support.netskope.com/s/article/NewEdge-Consolidated-List-of-IP-Range-for-Allowlisting
  for the consolidated list of IP ranges of all NewEdge DCs.

- **Disable SSL Decryption/Inspection on Network Devices**
  SSL Decryption must be disabled on all firewalls or inspection devices for theNetskope Client to connect to the Netskope Security Service Edge. **The payload of Netskope Client tunnel uses a proprietary framing protocol which other security tools would not be able to parse and inspect.**

  For additional security, Netskope Client also pins itself to Netskope-issued SSL certificates to ensure that security of the tunnel is not compromised or intercepted in any way.

- **Endpoint Antivirus / Malware**
  A number of Netskope Client Folders, Files and Processes need to be added to endpoint antivirus/ malware applications to allow the Netskope Client to run and connect to Netskope SSE.

  Please follow the best practice recommendations from:
  https://docs.netskope.com/en/exceptions-for-anti-virus-applications.html

- **Security Enforcements**
  Password protection for uninstallation is supported on Windows, macOS and Linux. Preventing service stop using this password is only supported on Windows.

  Protect Client configuration and resources is Windows only - Prevent users from tampering with the Netskope Client process, configuration files, registry, and directory location.

- **Network Detection**
  Dynamic steering enables location-based steering capabilities via on-premises or off-premises. Depending on the location, you can set up the steering configuration to steer or bypass configured traffic. When a managed device is detected to be on-premises, only cloud applications are steered and when the device is detected to be off-premises, all web traffic is steered. Dynamic steering also extends the capability to steer traffic from all or specific private applications.

  More information here:
  https://docs.netskope.com/en/netskope-help/traffic-steering/steering-configuration/enabling-dynamic-steering

- **Fail Close**
  Activating the "Fail Close" setting will concurrently activate "Password protection for client uninstallation and service stop." Additionally, it will deactivate the options for "Allow disabling of Private Apps Access" and "Allow disabling of clients."

  In simpler terms, turning on "Fail Close" not only secures the uninstallation and service stop processes with a password but also prevents the disabling of Private Apps Access and clients.

- **SSL TLS Inspection**
  SSL decryption policies are applied right after the traffic is steered to Netskope. By default, all traffic steered to Netskope will be decrypted, then further analyzed via Real-time Protection policies.

  If there is any traffic that you would like to leave encrypted, such as anonymous guest traffic and private financial/medical traffic, you can specify them in the Management UI, SSL Decryption Policies.

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivalled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.