Device Management (EDU-200)

Tunnelling

In networking, tunnelling is a way of securely moving data between networks without being detected. Tunnelling encapsulates the data inside a secure wrapper, keeping it safe from outside threats.

IPSec Tunnel

An IPsec tunnel is a secure, encrypted network connection established between two endpoints (usually firewalls or routers) over a public network like the internet, commonly used for Site-to-Site or Remote Access VPNs. It encrypts the entire original IP packet (header and payload) and encapsulates it in a new IP packet to protect data integrity and confidentiality.

GRE Tunnel

A Generic Routing Encapsulation (GRE) tunnel is ideal for forwarding internet-bound traffic from your corporate network to the Zscaler service. GRE is a tunneling protocol for encapsulating packets inside a transport protocol. A GRE-capable router encapsulates a payload packet inside a GRE packet.

Z-Tunnel

The Zscaler service uses a lightweight, HTTP tunnel called the Zscaler Tunnel (Z-Tunnel) to forward traffic to the ZIA Public Service Edges. When a user connects to the web, Zscaler Client Connector establishes the Z-Tunnel to the closest ZIA Public Service Edge, and forwards the web traffic through the tunnel so that the ZIA Public Service Edge can apply the appropriate security and access policies.

Z-Tunnel 1.0

Z-Tunnel 1.0 forwards traffic to the Zscaler cloud via CONNECT requests, much like a traditional proxy. Version 1.0 sends all proxy-aware traffic or port 80/443 traffic to the Zscaler service, depending on the forwarding profile configuration.

Z-Tunnel 2.0

Z-Tunnel 2.0 has a tunnelling architecture that uses DTLS or TLS to send packets to the Zscaler service. Because of this, Z-Tunnel 2.0 is capable of sending all ports and protocols.

Z-Tunnel Best Practices

- Zscaler recommends Z-Tunnel 2.0 for remote and on-premises users.
- Z-Tunnel traffic should always be exempt from SSL Inspection on third-party proxies and edge firewalls.
- Z-Tunnel 2.0 traffic from endpoints should always be exempted from IPsec/GRE tunnels.
- All Z-Tunnel 2.0 traffic must be set up with "sticky NAT" when NAT Pool is on the edge firewall/router.
- All Z-Tunnel 1.0 traffic from endpoints can be forwarded using existing IPsec/GRE tunnels.

Zscaler Client Connector

Zscaler Client Connector, a lightweight software agent installed on user devices (laptops, phones, etc.) that securely tunnels all their traffic through the Zscaler cloud (Zero Trust Exchange) for security, policy enforcement, and performance monitoring, providing secure remote access to internet, cloud, and private apps without needing traditional VPNs.

Proxy Auto Configuration (PAC) File

The PAC file is embedded as part of the Forwarding Profile configuration to provide granular control over how traffic is forwarded to or bypasses Zscaler's security cloud.

- A PAC (Proxy Auto-Configuration) file is a text file that contains JavaScript code designed to guide web browsers and applications on how to route internet traffic.
- The primary function of a PAC file is to determine whether web requests should be sent directly to the destination server or through a proxy server based on predefined rules.

Types of PAC Files

1. Forwarding Profile PAC Files: Used to bypass web traffic (processed by proxy-aware apps).App Profile PAC Files

2. App Profile PAC Files: Used to define how Client Connector should forward traffic (processed by Client Connector)

Forwarding Profile

The Forwarding Profile plays an integral role in managing Zscaler Client Connector by determining how user traffic is routed, secured, and inspected through the Zscaler cloud. Forwarding Profiles instruct Zscaler Client Connector how to forward a user's traffic to the Zscaler cloud depending on the user's current network environment.

Benefits of Forwarding Profile

Following are the benefits of Forwarding Profile:

- Control how traffic flows from user devices in various network environments.
- Configure different Forwarding Profiles with different network settings within multiple locations.
- Save time locating a profile using the Search feature.
- Easily manage existing profiles using view, edit, copy, and delete features.

App Profiles

Configuring App Profiles in Zscaler Client Connector ensures that the connector operates according to your organization's unique needs. This enables consistent security enforcement, dynamic traffic routing, seamless user experience, and ease of management.

- An App Profile in Zscaler Client Connector is a set of policy rules that determines how the Client Connector app behaves for different users or groups.
- App Profiles allow administrators to tailor security and connectivity settings based on user identity, device type, network, and other criteria.