Overview of Universal Zero Trust Network Access

This section provides an overview of Universal Zero Trust Network Access (universal ZTNA) including its components, benefits, and prerequisites.

Universal Zero Trust Network Access

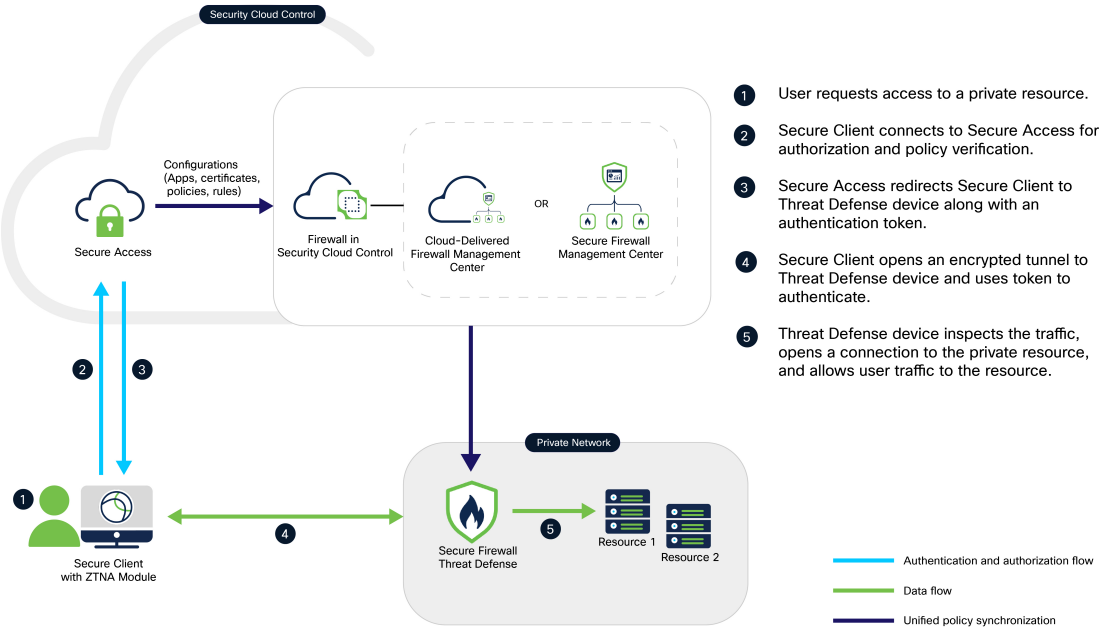
Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. Unlike traditional remote access VPNs, universal ZTNA ensures that access to one application does not implicitly grant access to others, thereby reducing the network attack surface.

Components of Universal ZTNA Solution

A new configuration of universal ZTNA consists of Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator), and Secure Access, both provisioned on the Security Cloud Control platform. Security Cloud Control Firewall Management uses a Firewall Management Center to manage the Firewall Threat Defense devices.

Universal ZTNA supports both on-premises Firewall Management Center, and Cloud-Delivered Firewall Management Center.

Figure 1: Components of Universal ZTNA Solution



- **Security Cloud Control Firewall Management**: Manages the configuration and deployment of universal ZTNA policies to the Firewall Threat Defense devices. The Threat Defense devices protect on-premises resources by enforcing universal ZTNA policies. A Threat Defense device inspects traffic and enforces intrusion prevention system (IPS), file, and malware policies.
- **Secure Access**: Defines the access policies, posture, and security profiles for the user. It enforces the policies for user traffic through the cloud.
- **Security Cloud Control platform**: Provides a unified secure management plane for both Secure Access and Secure Firewall, simplifying the administration of universal ZTNA policies across them.
- **Secure Client**: The Secure Client is installed on the end user's device. It acts as the enforcement point that intercepts connection requests to protected internal resources, enabling secure, identity-based access.

Benefits of Universal ZTNA

Universal ZTNA addresses the evolving network security challenges and operational complexities. Here is how deploying a universal ZTNA solution helps the administrators:

- Granular Access Control: Access is granted based on user identity and posture, ensuring secure access for both remote and on-premises users.
- Reduced Attack Surface: Access to one application does not imply access to others, minimizing potential vulnerabilities.
- Consistent Policy Enforcement: Policies are evaluated and managed in the Secure Access Cloud, while traffic proxying and enforcement (such IPS, malware) occur on Firewall Threat Defense devices.
- Dynamic Traffic Steering: Traffic is routed to the nearest enforcement point, optimizing connectivity and reducing latency for on-premises users.

- Simplified Policy Management: Policy enforcement is centralized across cloud and on-premises environments, allowing unified and granular control over application access based on identity and device compliance.
- Reduced Network Complexity: By intercepting and managing application access at the endpoint with the Secure Client, universal ZTNA eliminates the need for traditional VPNs and complex network segmentation, simplifying network design and management.

Prerequisites for Universal ZTNA

Secure Firewall Management Center and the Threat Defense devices

- The devices must run version 7.7.10.
- The devices must have a minimum of 16 cores.
- The devices must be configured for routed mode.
- Secure Firewall must be configured with a DNS server to resolve the private resource FQDNs.

Security Cloud Control

- Requires an enterprise account in either the United States or Europe region.
- Requires a Subscription for Secure Access and Secure Firewall.

Secure Client

- The client must run version 5.1.10 or later.
- ZTNA module must be enabled on the Secure Client.
- The client must run on a platform that supports Trusted Platform Module (TPM), such as Windows 11.

Licenses

- Secure Firewall Management Center requires a smart license account with export-controlled features. It does not function in universal ZTNA when operating in evaluation mode.

  Secure Firewall Threat Defense devices require Threat and Malware licenses if Intrusion Policy or File/Malware Policies are configured.
- Secure Access requires a subscription of Cisco Secure Private Access Essentials or Advantage.

Certificates

These certificates are required for the universal ZTNA solution.

- Client Device Identity Certificate:

  Secure Client presents the user identity certificate during the Mutual Transport Layer Security (mTLS) session with Secure Access and Firewall Threat Defense to request access to private resources. The client certificate is enrolled and managed as part of the Zero Trust Network Access module (ZTNA) on the Secure Client.
- Firewall Threat Defense Device Certificate:

Threat Defense devices that are enabled for universal ZTNA use the device certificates to establish secure mTLS connections with the Secure Client and Secure Access. Ensure that the device identity certificate is of type PKCS12.

- (Optional) Decryption Certificate:

  To decrypt traffic sent to private resources, enable decryption for those resources in Secure Access and provide the server certificate and key. We recommend using a certificate signed by a publicly recognized certificate authority (CA).