

Zero Trust Network Access Overview

- Clientless and universal zero trust network access, on page 1
- Zero trust network access, on page 2
- Comparison of clientless and universal ZTNA, on page 2

Clientless and universal zero trust network access

Zero Trust Access or Zero Trust Network Access (ZTNA) is a security process that protects internal resources using identity-based access, including user trust and posture. The process verifies the user, device, and request context before allowing access to internal resources and applications. It grants the least privilege access only after verifying the user, understanding the request context, and assessing any risks.

ZTNA deployment models

You can choose between two ZTNA deployment models.

- Clientless Zero Trust Network Access
- Universal Zero Trust Network Access

Clientless zero trust network access

Clientless Zero Trust Network Access (Clientless ZTNA) authenticates and authorizes access to protected web-based resources and applications from inside (on-premises) or outside (remote) the network. Clientless ZTNA accomplishes this authentication using an external identity provider (IdP) with Security Assertion Markup Language (SAML) authentication. No client software is needed on the user's device.

Clientless ZTNA is ideal for remote users accessing web applications and unmanaged devices.

Universal zero trust network access

Universal Zero Trust Network Access (Universal ZTNA) is a client-based solution that provides identity-based access to all internal resources regardless of user location. It enforces strong authentication, posture validation, and traffic inspection for each application and user.

Universal ZTNA supports both remote and on-premises users. On-premises users access a trusted network using a Secure Firewall Threat Defense device. Remote users access a trusted network through the cloud-based Secure Access service, which evaluates policies and proxies the user traffic securely in the cloud.

Zero trust network access

Zero Trust Network Access (ZTNA) provides secure, segmented application access by requiring explicit authorization for every connection. This approach reduces the attack surface and simplifies secure migrations without adding devices.

Key characteristics

ZTNA uses your existing Threat Defense deployment as an enforcement point for application access, enabling segmented and per-application authorization. ZTNA establishes individual tunnels for both remote and on-premises users.

ZTNA hides the network from users and ensures that they can only access applications for which they have been explicitly authorized. Authorization for one application does not provide implicit access to other applications, which significantly reduces the attack surface. In other words, every access to an application or a resource must be explicitly authorized.

You can adopt a more secure access model by adding zero trust access functionality to Threat Defense. This eliminates the need to install or manage additional devices in the network.

Comparison of clientless and universal ZTNA

This comparison outlines the key technical and operational differences between clientless ZTNA and universal ZTNA deployment models. Clientless ZTNA uses a browser-based approach, which is ideal for guest users or unmanaged devices that require access to web applications. Universal ZTNA uses an agent-based solution that supports all protocols. It continuously monitors device posture in managed corporate environments. Consider factors such as application support, security inspection capabilities, and licensing requirements to choose the best strategy for securing your remote and on-premises workforce.

Factor	Clientless ZTNA	Universal ZTNA
Client required	No client is required(browser-based)	Yes, Secure Client is required
Application support	Supports HTTPS web applications only	Supports all protocols and applications
Device posture	Device posture monitoring is limited (available through agents such as Duo Desktop)	Provides comprehensive and continuous device posture monitoring
Best for	Guest users, contractors, unmanaged devices	Employees, managed devices
Components involved	Third-party identity provider (IdP) configured with application access using Security Assertion Markup Language (SAML) authentication	• Secure Access • Secure Client software • Identity provider (depending on users' location)
Security policies	Deep inspection (Snort, IPS, File)	Deep inspection (Snort, IPS, File)

Factor	Clientless ZTNA	Universal ZTNA
User location	Remote and on-premises	Remote and on-premises
Licenses	Export-controlled license for Firewall Management Center	Licenses for Secure Access, Secure Client software, and Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator)