

Zero Trust Network Access Overview

Zero Trust Network Access (ZTNA) secures internal resources by verifying user identity and device posture to grant least-privilege access. Organizations implement either browser-based Clientless ZTNA for web applications or agent-based Universal ZTNA for comprehensive, protocol-wide support using existing threat defense infrastructure.

- 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
- History for zero trust network access, on page 3

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

Factor	Clientless ZTNA	Universal ZTNA
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)
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)

History for zero trust network access

This reference provides the minimum Firewall Management Center and Threat Defense versions needed to support zero trust application policies and monitoring.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Universal Zero Trust Network Access (universal ZTNA).	10.1.0	10.1.0	Universal ZTNA integrates with the Lina datapath, improving performance, scalability, and serviceability without requiring dedicated CPU cores or device reboots. This release supports mixed-mode IPv4 and IPv6 combinations for outer and inner connections, along with IPv6 Source NAT and hardware acceleration for outer tunnels. The system automatically enrolls Secure Access certificates as trustpoints, simplifying deployment. Upgrade Impact: Following a Threat Defense device upgrade, the system automatically reverts the core profile, clears stale certificates, and disables the universal ZTNA feature in the LINA configuration. You must perform a mandatory deployment from the Firewall Management Center to push new trustpoints, re-enable the feature, and restore universal ZTNA traffic handling. Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode. Supported platforms: Secure Firewall 1000 Series, 1100 Series, 1200 Series, 200 Series, 2100 Series, 3100 Series, 4100 Series, 4200 Series, 6100 Series, and 9300 Series and Firewall Threat Defense Virtual.
Universal Zero Trust Network Access (universal ZTNA).	7.7.10	7.7.10	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. It ensures that access to one application does not implicitly grant access to the entire network, as with remote access VPN. New/modified screens: **Policies** > **Security policies** > **Zero Trust Application** Requires Cisco Secure Access and Security Cloud Control. **Note** Due to framework changes, upgrading a universal ZTNA device to Version 10.1+ from older versions disables the feature. Traffic is interrupted until you deploy from the Firewall Management Center. Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode. Supported platforms: Secure Firewall 1150, 3100, 4100, 4200, and Firewall Threat Defense Virtual.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Zero trust access enhancements	7.4.1	7.4.1 with Snort 3	Firewall Management Center now includes the following zero trust access enhancements: • You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. • You can troubleshoot the zero trust configuration issues using the diagnostics tool. New/modified screens: **Policies** > **Access Control** > **Zero Trust Application** New/modified CLI commands: **show running-config zero-trust**, **show zero-trust statistics**
Clientless zero-trust access	7.4.0	7.4.0 with Snort 3	Zero Trust Access allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics**