

Device Management (EDU-200)

Zscaler Client Connector (ZCC): Endpoint application that securely connects users to the Zero Trust Exchange.

Zscaler Internet Access (ZIA): Service that inspects and secures internet-bound traffic.

Zscaler Private Access (ZPA): Service providing secure access to internal private applications.

Proxy Auto-Configuration (PAC): A text file containing JavaScript to guide web browsers on traffic routing to proxies.

Virtual Private Network (VPN): Encrypted connection allowing secure remote access to resources.

Transport Layer Security (TLS): Protocol securing data through encryption during transit.

Datagram Transport Layer Security (DTLS): TLS-based protocol designed for encrypted real-time data transmissions (like voice/video).

Generic Routing Encapsulation (GRE): Cisco-developed protocol for securely encapsulating various data types for transport.

Internet Protocol Security (IPsec): Encrypts and secures communications between networks over the internet.

Network Interface Card (NIC): Hardware component managing access to wireless and wired networks.

Mobile Device Management (MDM): Software enabling organizations to manage and secure mobile devices.

Unified Endpoint Management (UEM): A comprehensive platform managing devices across various operating systems.

Bring Your Own Device (BYOD): Practice allowing employees to use personal devices for work purposes.

Virtual Desktop Infrastructure (VDI): Technology providing virtual workspaces accessible from any device.

Certificate Authority (CA): Entity issuing digital certificates for validating public keys.

Key Terms:

Zero Trust Exchange: Platform ensuring secure end-to-end connectivity based on Zero Trust Architecture principles.

Trusted Network: Network environments defined by criteria ensuring optimized security and data routing.

Device Posture: Represents the security and compliance state of a device in assessing access permissions.

Forwarding Profile: Configuration determining how user traffic is routed securely through Zscaler's cloud services.

App Profile: A set of rules tailored to specific users or groups specifying traffic routing, security policies, and access settings.

Provisioning Key: Tool authenticating App Connectors to ZPA infrastructure.

SSL Inspection: Capability to decrypt and re-encrypt HTTPS traffic for threat detection without causing security errors.

SIPA - Source IP Anchoring: Feature for redirecting specific traffic to bypass proxies based on network trust levels.

Dynamic Location Groups: Automatically updates configurations based on matching attributes like IP or subnet activity.

Posture Control: Mechanism for verifying that devices meet corporate security compliance standards before granting access.

Enrolled Devices: Devices registered within the Zscaler Client Connector for security and policy enforcement.

Z-Tunnel 1.0 vs 2.0: Comparison of Zscaler tunnel versions, where 2.0 provides superior traffic encryption, authentication, and efficiency.

Edge Firewall: Hardware or software solution enforcing security policies at the boundary of a network.



Classification: Process of identifying and categorizing data across environments for enhanced security.

Data Center Location: Physical or virtual network hub facilitating secure and scalable traffic routing.

Sticky NAT: Network Address Translation configuration preserving the association between an IP and a connection.



Experience your world, secured.™

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. Zscaler, Inc. (HQ)

120 Holger Way
San Jose, CA 95134
+1 408.533.0288
zscaler.com