



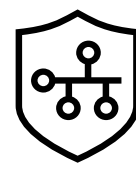
CHECKLISTE: VPN VS. ZTNA

VPNs sind seit Jahrzehnten eine unverrückbare Technologie für den Remote-Zugriff in Unternehmen – eine digitale Zugbrücke zur Unternehmensburg. Angesichts der Verlagerung von Anwendungen in die Cloud und der zunehmenden Mobilität der Benutzer ist die VPN-Technologie jedoch überholt, da sowohl die Sicherheit als auch die Benutzerfreundlichkeit zu wünschen übrig lassen.

Ersetzen Sie Ihr VPN durch eine moderne Technologie: **Zero-Trust-Netzwerkzugriff (ZTNA)**. Erfahren Sie, warum viele Unternehmen ZTNA als VPN-Alternative nutzen.



VPN



ZTNA

Sicherheit

- VPNs verstärken das herkömmliche, auf dem Perimeter basierende Sicherheitsmodell, das jedem Gerät, Benutzer und jeder Anwendung innerhalb der Netzwerkgrenzen bedingungsloses Vertrauen entgegenbringt.
- VPNs geben Ports zum Internet frei, um den Netzwerkzugriff zu ermöglichen, und machen sie so zu einem Ziel für Malware- und Ransomware-Angriffe.
- VPNs bieten Benutzern vollen Zugriff auf die Ressourcen eines Netzwerks und bergen die Gefahr, dass das Netzwerk offengelegt wird.
- VPNs arbeiten auf Netzwerkebene mit Kontrolle und Transparenz über Netzwerkverkehr auf niedriger Ebene.
- VPNs ermöglichen BYOD-Geräten den Zugriff auf das Unternehmensnetzwerk über nicht verwaltete, unternehmens-fremde Endpunkte, über die Malware oder andere Cyberbedrohungen eingeschleust werden können.
- VPNs sind anfällig für DDoS-Angriffe (Distributed Denial of Service), die den VPN-Server überwältigen und den Dienst unterbrechen können.

- ZTNA implementiert das Zero Trust-Sicherheitsmodell, das nach dem Prinzip **„niemals vertrauen, immer überprüfen“** arbeitet und sich nicht auf einen festen Perimeter stützt.
- ZTNA-Lösungen geben keine IPs an das Internet weiter, sodass das Unternehmensnetzwerk für unbefugte Benutzer oder schädliche Akteure unsichtbar ist.
- ZTNA beschränkt laterale Bewegungen und Benutzerverbindungen auf bestimmte Anwendungen und prüft fortlaufend die Vertrauenswürdigkeit von Benutzern und Geräten, um Risiken zu verringern und die Sicherheit zu erhöhen.
- ZTNA arbeitet auf Anwendungsebene und kann granulare Zugriffsrichtlinien auf einer Benutzer-zu-Anwendungs-Basis einrichten. Das Ergebnis ist ein höheres Maß an Kontrolle und eine bessere Transparenz der Aktivitäten.
- ZTNA kann strenge Geräteprüfungen und Richtlinien durchsetzen, bevor der Zugriff auf eine Ressource gewährt wird, sodass nur konforme Geräte eine Verbindung herstellen können.
- ZTNA-Lösungen können DDoS-Angriffe abschwächen, indem sie eine verteilte Cloud-Infrastruktur nutzen, die sich je nach Bedarf vergrößern oder verkleinern lässt. Außerdem können sie Ratenbegrenzungs- und Filtermechanismen anwenden.

Flexibilität

- VPNs sind für den sicheren Remote-Zugriff auf das Unternehmensnetzwerk konzipiert, bieten aber oft nur begrenzte Unterstützung für Cloud-basierte Ressourcen.
- VPNs leiden aufgrund von Bandbreiten-beschränkungen, Netzwerküberlastungen und Latenzzeiten häufig unter Leistungsproblemen.

- ZTNA kann einen sicheren Remote-Zugriff sowohl auf lokale als auch auf Cloud-basierte Ressourcen sowie auf hybride Umgebungen bieten.
- ZTNA-Lösungen können die Leistung optimieren, indem sie eine Cloud-basierte Architektur mit einem möglichst nahen Zugangspfad zum Benutzer und zur Anwendung sowie dank der Cloud eine erhöhte Kapazität nutzen.

Management

- Bei VPNs müssen die Benutzer Client-Software auf ihren Geräten installieren und konfigurieren, was umständlich und fehleranfällig sein kann.
- VPNs lassen sich nur schwer überwachen und überprüfen, da sie keine detaillierten Einblicke in die Benutzeraktivitäten und die Anwendungsnutzung bieten.

- ZTNA-Lösungen bieten einen Zugriff auf Webbrowser ohne Benutzererfahrung vereinfacht und die IT-Supportkosten reduziert.
- ZTNA-Lösungen können detaillierte Protokolle und Berichte über Benutzeridentität, Gerätestatus, Anwendungszugriff und Netzwerkverkehr liefern und ermöglichen so eine bessere Compliance und Sicherheitsanalyse.

Ist es für Sie an der Zeit, sich von VPN zu verabschieden?

Erfahren Sie, wie Sie von VPN zu ZTNA wechseln können.

[E-Book lesen](#)

Weitere Informationen

arubanetworks.com/resource/making-the-switch-from-vpn-to-ztna/

[HPE.com besuchen](#)

[Jetzt chatten](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Die einzigen Garantien für Produkte und Services von Hewlett Packard Enterprise sind in den ausdrücklichen Garantieerklärungen enthalten, die diesen Produkten und Services belegen. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

a00141302DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com

