HPE aruba networking

Business-Whitepaper

Wechsel von VPN zu ZTNA

Die Vorteile von ZTNA und mögliche Einstiegspunkte

HPE GreenLake

60 %

der Unternehmen werden ihr VPN durch einen ZTNA-Service ersetzen

Die Einführung der Remote-Arbeit war mit neuen Sicherheitsproblemen für Unternehmen verbunden. Mit einer steigenden Anzahl Beschäftigten, die von jedem Ort aus arbeiten, müssen die Unternehmen Möglichkeiten für einen sicheren Remote- und Hybrid-Zugriff auf ihre Netzwerke finden. Eine herkömmliche hierfür genutzte Lösung ist das Virtual Private Network (VPN). Vor dem Hintergrund der Zunahme an Cyber-Bedrohungen jedoch haben sich VPNs als ungeeignet für den Schutz vor modernen Bedrohungen erwiesen. Zero Trust Network Access (ZTNA) ist eine effektivere Lösung für den Schutz des Remote-Zugriffs.

Was ist ZTNA?

Der Begriff Zero Trust Network Access (ZTNA) wurde im April 2019 von Gartner® geprägt und steht für eine Reihe neuer Technologien, die für den sicheren Zugriff auf private Anwendungen entwickelt wurden. ZTNA nutzt granulare Zugriffsrichtlinien für den Zugriff auf bestimmte Anwendungen durch autorisierte Benutzer, ohne dass ein Netzwerkzugriff gewährt wird. Dies ermöglicht einen segmentierten Zugriff basierend auf den geringstmöglichen Rechten, wobei die Speicherorte von Anwendungen niemals über das Internet offengelegt werden, wie dies bei VPNs der Fall ist.

Gartner erwartet ‚dass bis 2023 60 % der Unternehmen ihr VPN durch einen ZTNA-Service ersetzen. Hierdurch wurde ZTNA branchenweit zu dem Zero Trust-Produkt mit dem schnellsten Wachstum, wobei 47 % der IT-Führungskräfte ZTNA als Einstiegspunkt für die Unternehmen gilt, die eine Security Service Edge (SSE)-Plattform im Rahmen eines umfassenderen Secure Access Service Edge (SASE)-Frameworks wünschen.

ZTNA verbessert die Sicherheit

Einer der Hauptgründe, warum Unternehmen ZTNA einführen, ist die hierdurch gebotene bessere Sicherheit. Mit einem VPN gelangen die Benutzer direkt in das Unternehmens-Netzwerk. Sobald ein Benutzer Zugriff auf das Netzwerk erhält, kann er sich lateral bewegen und potenziell auf sensible Daten oder Ressourcen zugreifen. Es überrascht nicht, dass sich „zu viel Vertrauen in die Benutzer“ laut dem SSE Adoption Report 2023 als die größte Herausforderung bestehender Lösungen für einen sicheren Zugriff erwiesen hat. Wenngleich einzuwenden wäre, dass dies für interne Benutzer eine geringere Rolle spielt, ist der Gedanke beängstigend, dass ein Angreifer von einer fehlenden Segmentierung profitieren kann.

Im Gegensatz hierzu erweitert ZTNA niemals den Netzwerkzugriff und gewährt den Zugriff basierend auf Kontext, Benutzeridentität, verwendetem Gerät sowie Anwendungen und Daten, auf die zugegriffen werden soll. Dies bedeutet, dass selbst wenn ein Angreifer versucht, Zugriff auf das Netzwerk zu erlangen, ohne entsprechende Autorisierung nicht nur der Zugriff auf sensible Daten unmöglich ist, sondern der ZTNA-Service ebenfalls die bloße Existenz des Netzwerks verschleiert, sodass es weder sichtbar noch nachverfolgbar ist.

Die Implementierung und Pflege von ZTNA-Lösungen ist üblicherweise kostengünstiger als bei VPN-Lösungen. Die Kosten für VPN gehen weit über die einfachen anfänglichen Kosten hinaus.

ZTNA erhöht die Skalierbarkeit und die Flexibilität

Ein weiterer Grund, warum Unternehmen ZTNA einführen, ist die erhöhte Skalierbarkeit und Flexibilität. Während VPN-Lösungen grundsätzlich hardware- und appliance-basiert sind, werden ZTNA-Lösungen über die Cloud bereitgestellt, sodass der Benutzerzugriff sowie die Verwaltung durch die IT-Abteilung mühelos von jedem Ort aus erfolgen können. Dies ist insbesondere hilfreich für Unternehmen mit Beschäftigten, die hybrid/remote arbeiten oder von unterschiedlichen Orten aus Zugriff auf die Ressourcen benötigen. Wenngleich die Kapazität von VPNs basierend auf der Appliance-Größe eingeschränkt ist, bietet die über die Cloud bereitgestellte Architektur von ZTNA Unternehmen die Möglichkeit einer schnellen Aufwärts- und Abwärts-Skalierung, um die sich verändernden Unternehmensanforderungen zu erfüllen.

Noch wichtiger: ZTNA-Services bieten Richtlinien für eine ausgesprochen granulare und flexible Zugriffssteuerung, die bis zur Benutzer- und Anwendungsebene angewendet werden können. Die Zugriffs-Segmentierung mithilfe von VPN bedeutet eine komplexe Netzwerk-Segmentierung, doch mit ZTNA ist die Implementierung des Zugriffs mit geringstmöglichen Rechten so einfach wie das Anpassen einer Richtlinie.

ZTNA ermöglicht eine Steigerung der Produktivität

ZTNA-Lösungen bieten ein besseres Zugriffserlebnis als VPNs. VPNs beeinträchtigen die geschäftliche Produktivität, da die Benutzer mit langsamen Verbindungsgeschwindigkeiten (durch VPN-Backhauls), unkomfortablen und konstanten Trennungen sowie komplexen und wiederkehrenden Anmeldungen konfrontiert sind. All dies beeinträchtigt die Arbeit der Benutzer und führt zu Frustration.

ZTNA hingegen bietet ein benutzerfreundlicheres Erlebnis. Er ermöglicht Endbenutzern den einfachen Zugriff auf private Anwendungen durch Beseitigen des Datenverkehrs-Backhauls, unterbrechungsfreie Verfügbarkeit, selbst bei Netzwerkänderungen und einen reibungslosen Anmeldevorgang mit umfassender Integration von SSO- sowie anderen Lösungen für das Identitäts-Management.

ZTNA ist kosteneffizienter

Die Implementierung und Pflege von ZTNA-Lösungen ist üblicherweise kostengünstiger als bei VPN-Lösungen. Die Kosten für VPN gehen weit über die anfänglichen Kosten hinaus … Neben VPN-Konzentratoren erfordern VPNs kostspielige lokale Hardware, wie beispielsweise einen DDoS-Schutz, interne und externe Firewalls, Lastverteiler usw. All dies ist für einen einzelnen eingehenden Sicherheits-Stack vorgesehen (Unternehmen verfügen durchschnittlich über 3 – 5). Außerdem benötigen Sicherheits-Teams üblicherweise eine(n) oder mehrere Mitarbeitende für die Überwachung und Verwaltung des VPN. Hierdurch stehen die Mitarbeitenden nicht für dringendere und wichtigere Projekte zur Verfügung. Ein solcher perimeter-zentrierter Ansatz für einen sicheren Zugriff ist kostenintensiv.

Im Gegensatz hierzu erfordern ZTNA-Lösungen keine kostspielige Hardware oder Software, die lokal installiert und gewartet werden muss. Außerdem möchten die Unternehmen mithilfe von SSE-Plattformen die Notwendigkeit von VPN-Konzentratoren (63 %), SSL-Überprüfungen (50 %) und DDoS-Schutz (44 %) beseitigen. Tatsächlich bieten die besten SSE-Plattformen ZTNA-Technologien, durch die VPNs und der Sicherheits-Stack für eingehende Verbindungen überflüssig werden, was zu erheblichen Kosteneinsparungen führt. ZTNA ist darüber hinaus intuitiv und einfach zu verwalten und bietet Unternehmen die Möglichkeit, die Anzahl der Ressourcen und Team-Mitglieder zur Verwaltung des sicheren Zugriffs deutlich zu reduzieren. Und ZTNA-Lösungen nutzen ein abonnement-basiertes Preismodell, das Kostentransparenz bietet und zu hohe Lizenzausgaben verhindert.

Lassen Sie sich nicht von VPN zurückhalten

Die Anzahl der remote und hybrid arbeitenden Beschäftigten nimmt stetig weiter zu. Daher ist für Unternehmen entscheidend, über eine moderne Lösung für sicheren Zugriff zu verfügen. Als moderne Lösung bewältigt ZTNA die Einschränkungen von VPNs und bietet mehr Sicherheit, Flexibilität, Skalierbarkeit, Leistung und Kosteneffizienz für den Remote-Zugriff.

Das Beste an ZTNA ist, dass er Bestandteil einer größeren Sicherheits-Strategie ist. Wir beobachten, dass bei der Einführung einer Security Services Edge (SSE)-Plattform nahezu 50 % der Unternehmen mit der Einführung von ZTNA beginnen. Wo starten Sie?

Vollständiger Umstieg von VPN auf HPE Aruba Networking ZTNA

Erfahren Sie mehr über den Einsatz von HPE Aruba Networking ZTNA als Alternative zu VPN

Entdecken Sie die HPE Aruba Networking SSE-Plattform

arubanetworks.com/products/sse

Besuchen Sie **ArubaNetworks.com**

Entscheiden Sie sich für das richtige Produkt. Kontaktieren Sie unsere Presales-Experten.

Kontakt

BWP_Switch-to-ZTNA_A4_RB_022224 a00136655dee

Hewlett Packard Enterprise