SOPHOS

Die sechs wichtigsten Vorteile von ZTNA

Im Vergleich zu Remote Access VPN

Sophos-Whitepaper

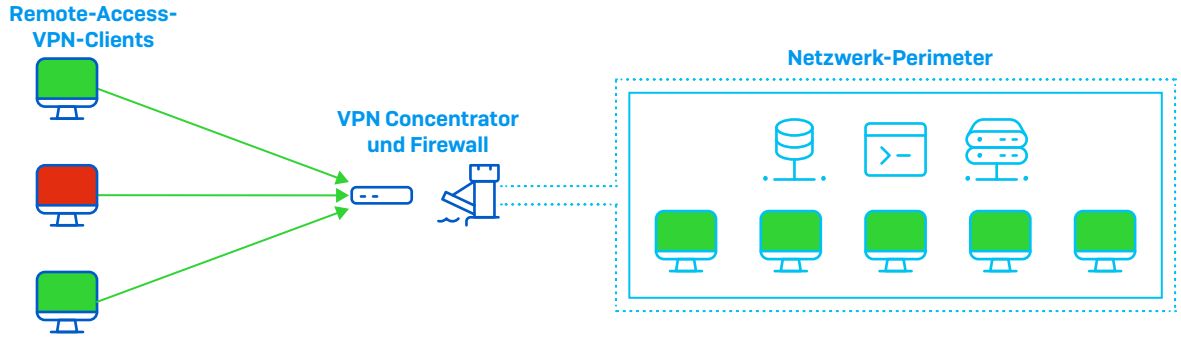
Remote Access VPN hat uns lange Zeit gute Dienste geleistet. Doch der zunehmende Trend zur Remote-Arbeit zeigt nun auch die Grenzen dieses veralteten Konzepts auf. Einige Unternehmen versuchen weiterhin, diese Technologie so lange wie möglich maximal auszureizen. Andere suchen nach besseren Alternativen, die die Probleme von Remote-Access-VPN-Lösungen aus der Welt schaffen. Schon jetzt arbeiten viele Unternehmen erfolgreich mit der nächsten Generation von Remote-Access-Technologien wie ZTNA oder Zero Trust Network Access. Im Vergleich zu Remote Access VPN bietet ZTNA mehr Sicherheit, feinstufigere Kontrollen und ist zugleich für Endbenutzer transparenter.

In unserem ZTNA Buyers Guide gehen wir auf die Einschränkungen und Probleme klassischer Remote-Access-VPN-Lösungen ein und erläutern, welche Vorteile Zero Trust Network Access Unternehmen bietet. Zudem erhalten Sie eine Übersicht über die wichtigsten Funktionen, auf die Sie bei der Wahl Ihrer ZTNA-Lösung achten sollten.

Remote-Access-VPN: Grenzen und Probleme

Remote Access VPN gehört seit Jahrzehnten in praktisch jedem Netzwerk zum Standard und liefert sicheren Zugriff auf Systeme und Ressourcen im Netzwerk. Die Technologie stammt jedoch aus einer Zeit, in der Unternehmensnetzwerke einer mittelalterlichen Festung glichen – mit einem „dicken Schutzwall", dem Perimeter, der sämtliche Ressourcen sicher abschirmte. So gewährt VPN befugten Benutzern zwar sicheren Zugang zum Perimeter. Doch sobald sie im Netzwerk sind, haben sie praktisch uneingeschränkten Zugriff auf Ressourcen.

Herkömmliche Remote-Access-VPN-Lösungen



Netzwerke haben sich kontinuierlich weiterentwickelt und sind heute viel komplexer, verteilter und dynamischer als je zuvor. Anwendungen und Daten befinden sich in der Cloud, Mitarbeiter arbeiten immer öfter mobil. Hinzu kommen die Angriffe der Cyberkriminellen, die beständig auf der Suche nach Schwachstellen im Netzwerk sind.

Eine Remote-Access-Lösung in einer modernen Umgebung auf Basis von VPN (IPsec/SSL) zu verwalten, erweist sich meist als sehr komplex und aufwändig. Sie müssen sich mit IP-Verwaltung, Datenverkehr und Routing, Firewall-Zugriffsregeln sowie der Bereitstellung und Konfiguration von Clients und Zertifikaten abmühen. Bei mehr als einer Handvoll Knoten und Dutzenden Benutzern wird dies schnell zum Vollzeitjob. Auch die Überwachung und Kontrolle der Sicherheit entwickeln sich oft in kürzester Zeit zum Albtraum.

Kurz: Konventionelle Remote-Access-VPN-Lösungen bringen unnötige Einschränkungen und Probleme:

1. **Implizites Vertrauen** – Remote Access VPN leistet gute Arbeit dabei, Benutzer so durch den Perimeter ins Unternehmensnetzwerk zu bringen, als würden sie sich direkt anmelden. Im Netzwerk genießen sie jedoch bedingungsloses Vertrauen und umfassenden Zugriff auf Ressourcen – ein erhebliches und unnötiges Sicherheitsrisiko.
2. **Potenzieller Bedrohungsvektor** – Remote Access VPN erkennt nicht den Status des Geräts, mit dem die Verbindung zum Unternehmensnetzwerk hergestellt wird. So entsteht ein möglicher Infektionsvektor für Bedrohungen auf kompromittierten Geräten.
3. **Ineffizientes Backhauling** – Remote Access VPN stellt einen einzigen Point of Presence im Netzwerk bereit, was wiederum zu Backhauling von Datenverkehr von mehreren Standorten, Rechenzentren oder Anwendungen über den Remote-Access-VPN-Tunnel führen kann.
4. **Mangelnde Transparenz** – Remote Access VPN erkennt verarbeiteten Datenverkehr bzw. Nutzungsmuster nicht, sodass sich Benutzeraktivitäten und Anwendungsnutzung nur schwer überwachen lassen.
5. **Geringe Benutzerfreundlichkeit** – Dass VPN-Clients nicht besonders benutzerfreundlich sind, ist altbekannt. Dazu gehören erhöhte Latenz, eingeschränkte Performance, Verbindungsprobleme und ein Mehraufwand für das Helpdesk.
6. **Hoher Verwaltungsaufwand** – Remote Access VPN-Clients einzurichten, bereitzustellen und Benutzer an- und abzumelden, ist mit enormen Aufwand verbunden. Darüber hinaus gestaltet sich die Verwaltung von VPN im Firewall- und Gateway-Bereich schwierig – insbesondere bei einer Vielzahl an Knoten, Firewall-Zugriffsregeln, Datenverkehr und Routing und umfangreicher IP-Verwaltung. Da entwickelt sich das Ganze schnell zum Vollzeitjob.

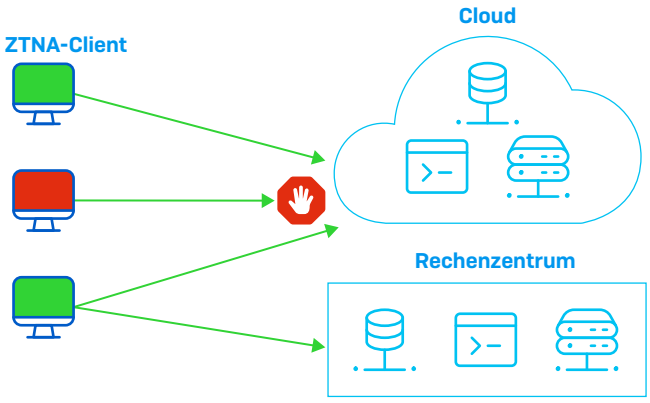
ZTNA: Begriffserklärung und Funktionsweise

ZTNA oder auch Zero Trust Network Access wurde vor allem dazu konzipiert, die Einschränkungen und Probleme von Remote Access VPN aus der Welt zu schaffen. Mit ZTNA können Benutzer sicher und von jedem Standort aus auf genau die Daten und Anwendungen zugreifen, die sie für ihre Arbeit benötigen – nicht mehr und nicht weniger. Es gibt mehrere grundlegende Unterschiede zwischen ZTNA und Remote Access VPN.

Wie aus dem Namen Zero Trust (Null Vertrauen) hervorgeht, basiert ZTNA auf dem Prinzip „Nichts und niemandem vertrauen, alles überprüfen". Das Zero-Trust-Prinzip löst das Konzept einer einzigen Firewall ab, die das Netzwerk wie ein „mittelalterlicher Schutzwall" abschirmt. So bilden bei ZTNA jeder Benutzer, jedes Gerät und jede Netzwerkanwendung einen eigenen Perimeter. Dabei werden Verbindungen nur nach Prüfung von Zugangsdaten, Gerätestatus und Zugriffsrichtlinien zugelassen. Das Ergebnis: weitaus bessere Sicherheit, Segmentierung und Kontrolle.

Ein weiterer wesentlicher Unterschied in der Funktionsweise von ZTNA besteht darin, dass sich Benutzer nicht einfach uneingeschränkt im Netzwerk bewegen können. Vielmehr werden sichere Tunnel zwischen einem Benutzer und dem spezifischen Gateway der Anwendung erstellt, auf die der Benutzer zugreifen darf – und nur darauf. Dies sorgt für eine bedeutend sicherere Mikro-Segmentierung und bringt damit eine Reihe von Vorteilen für die Sicherheit, Kontrolle, Transparenz, Effizienz und Performance. So ist bei Remote Access VPN beispielsweise nicht ersichtlich, auf welche Anwendungen Ihre Benutzer zugreifen. ZTNA zeigt dagegen Status und Aktivitäten aller Anwendungen in Echtzeit an und liefert damit wertvolle Informationen, mit Hilfe derer Sie potenzielle Probleme rechtzeitig erkennen und Lizenz-Audits durchführen können. Dank zusätzlicher Mikro-Segmentierung verhindert ZTNA laterale Bewegungen von Geräten oder Benutzerzugriffe zwischen Ressourcen im Netzwerk. Jeder Benutzer, jedes Gerät und jede Anwendung oder Ressource sind ein eigener Sicherheits-Perimeter. Das Konzept des impliziten Vertrauens fällt weg.

Zero Trust Network Access



Zudem ist ZTNA insgesamt dynamischer und transparenter, läuft im Hintergrund und erfordert – von der ersten Identitätsprüfung abgesehen – keinerlei Benutzerzugriff. Ihre Benutzer bemerken meist nicht einmal, dass sie sich über sichere, verschlüsselte Tunnel mit Anwendungen verbinden.

Vorteile von ZTNA

Zero Trust Network Access bietet zahlreiche Vorteile und wird häufig aus folgenden Gründen eingesetzt:

- **Arbeit im Homeoffice:** Mit ZTNA-Lösungen lässt sich der Remote-Zugriff von mobilen Mitarbeitern viel einfacher verwalten. Dank komfortabler, flexibler Bereitstellung und Benutzerregistrierung sparen Sie wertvolle Zeit und Ressourcen gegenüber VPN. Für Ihre Mitarbeiter im Homeoffice ist die Handhabung zudem transparenter und benutzerfreundlicher.
- **Mikro-Segmentierung von Anwendungen:** ZTNA-Lösungen bieten weitaus mehr Anwendungssicherheit dank Mikro-Segmentierung, Integration des Gerätestatus in Zugriffsrichtlinien und kontinuierlicher Authentifizierungsprüfung. Außerdem gibt es bei Zero Trust kein implizites Vertrauen und das bei VPN gängige Risiko lateraler Bewegungen wird minimiert.
- **Abwehr von Ransomware:** ZTNA-Lösungen beseitigen einen gängigen Angriffsvektor für Ransomware und andere Angriffsarten, die darauf abzielen, das Netzwerk zu infiltrieren. Da sich ZTNA-Benutzer nicht mehr „im Netzwerk" befinden, haben Bedrohungen, die bei VPN im Netzwerk möglicherweise Fuß fassen, mit ZTNA keine Chance.
- **Schnelles Onboarding neuer Anwendungen und Benutzer:** ZTNA ist sicherer und agiler, insbesondere in sich schnell wandelnden Umgebungen mit einer hohen Benutzerfluktuation. So richten Sie neue Anwendungen schnell und sicher ein, melden Geräte und Benutzer einfach an und ab und erhalten dabei Informationen über Anwendungsstatus und -nutzung.

Alle Vorteile von ZTNA im Vergleich zu herkömmlichen Remote-Access-VPN-Lösungen im Überblick:

1. **Zero Trust** – ZTNA basiert auf dem Zero-Trust-Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Dieser Ansatz bietet erheblich mehr Sicherheit und bessere Mikro-Segmentierung: Alle Benutzer und Geräte bilden ihren eigenen Perimeter. Identität und Integrität werden beim Zugriff auf Unternehmensdaten und -anwendungen immer überprüft. Benutzer dürfen nur auf Anwendungen und Daten zugreifen, die explizit in den entsprechenden Richtlinien definiert sind. Dies minimiert laterale Bewegungen sowie damit verbundene Risiken.
2. **Geräte-Integrität** – ZTNA integriert den Sicherheitsstatus und die Compliance von Geräten in Zugriffsrichtlinien. So können Sie Zugriffe nicht richtlinienkonformer, infizierter oder kompromittierter Systeme auf Unternehmensdaten und -anwendungen unterbinden und das Risiko von Datenpannen und Datenverlusten minimieren.
3. **Standortunabhängiger Zugriff** – ZTNA ist netzwerkunabhängig und funktioniert daher in jedem Netzwerk gleich gut und sicher: zu Hause, im Hotel, im Café oder im Büro. Für maximalen Benutzerkomfort lassen sich Verbindungen unabhängig vom Benutzer- und Gerätestandort sicher und transparent verwalten.
4. **Benutzerfreundlichkeit** – ZTNA baut sichere Verbindungen bei Bedarf im Hintergrund auf und sorgt so für maximale Benutzerfreundlichkeit. In der Regel bemerken Benutzer nicht einmal, dass eine ZTNA-Lösung ihre Daten schützt.
5. **Mehr Transparenz** – ZTNA bietet mehr Einblick in die Anwendungsaktivitäten, was insbesondere bei der Überwachung des Anwendungsstatus, bei Kapazitätenplanung, Lizenzverwaltung und bei Audits eine wichtige Rolle spielt.
6. **Einfachere Verwaltung** – ZTNA-Lösungen sind meist effizienter und ressourcenschonender und lassen sich daher ganz einfach bereitstellen und verwalten. Darüber hinaus sind ZTNA-Lösungen agiler und damit insbesondere für sich schnell wandelnde Umgebungen mit einer hohen Benutzerfluktuation perfekt geeignet. So lässt sich die tägliche Verwaltungsroutine problemlos und zeitsparend bewältigen.

Buyers Guide: Worauf es bei einer ZTNA-Lösung ankommt

Achten Sie beim Vergleich der ZTNA-Lösungen neben unterstützten Plattformen, Gateways und Identitätsanbietern auch auf folgende Aspekte:

Bereitstellung und Verwaltung in der Cloud

Cloud-Management bietet zahlreiche Vorteile: sofortige Inbetriebnahme, reduzierte Management-Infrastruktur, schnelle Bereitstellung und Registrierung sowie standortunabhängiger Zugriff. So können sich Ihre Benutzer sofort anmelden und produktiv arbeiten, ohne dass Sie in zusätzliche Management-Server oder -Infrastruktur investieren müssen. Cloud-Management sorgt außerdem für sofortigen, sicheren Zugriff von überall, auf allen Geräten und unterstützt so Ihre gewünschte Arbeitsweise. Zudem lassen sich neue Benutzer schnell und einfach registrieren – ganz unabhängig davon, wo sie sich gerade befinden.

Integration mit anderen Cybersecurity-Lösungen

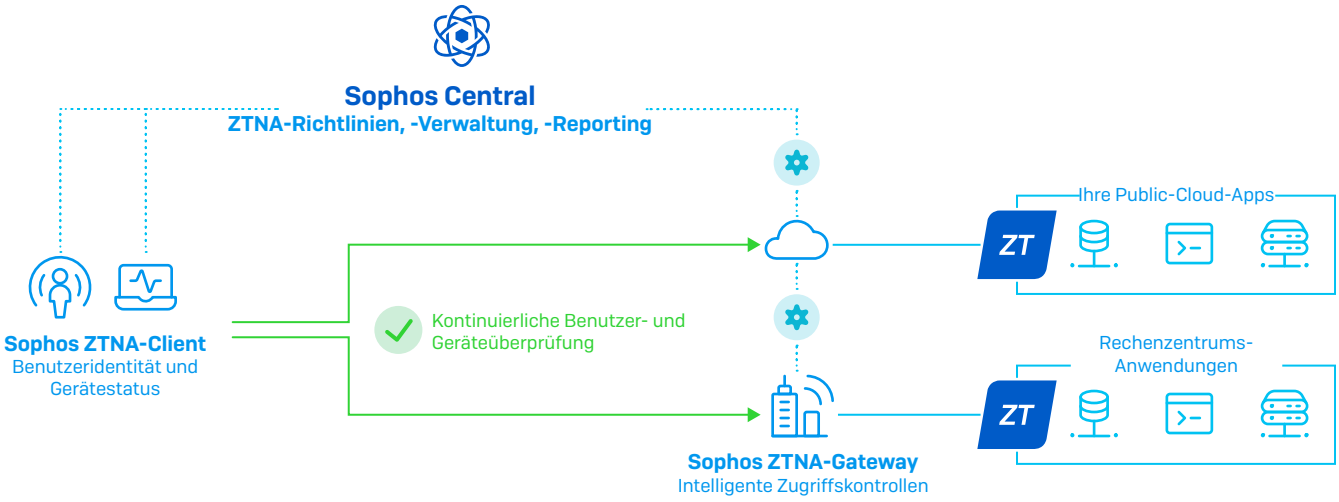
ZTNA-Lösungen lassen sich in der Regel gut als Standalone-Produkte nutzen. Eine enge Integration mit Ihren anderen Cybersecurity-Produkten, wie etwa Ihrer Firewall oder Endpoint Protection, bietet jedoch enorme Vorteile. Mit einer integrierten Cloud-Management-Konsole können Sie die Arbeitsleistung Ihres Teams einfach und effizient erweitern. Indem Sie ZTNA gemeinsam mit allen anderen IT-Security-Produkten über eine zentrale Konsole verwalten, können Sie Kosten für die Systemverwaltung sparen und benötigen weniger Zeit für die Schulung Ihrer Mitarbeiter. Außerdem sorgt dies für eine umfassende Transparenz über Ihre IT-Security-Produkte, insbesondere wenn diese Telemetriedaten austauschen. Sie profitieren von wesentlich mehr Sicherheit und einer Reaktion in Echtzeit, wenn kompromittierte Geräte oder Bedrohungen ins Netzwerk gelangen. Ihre Produkte arbeiten perfekt zusammen, stoppen Angriffe und Bedrohungen sofort und verhindern laterale Bewegungen, eine weitere Ausbreitung sowie Datendiebstahl.

Benutzer- und Verwaltungskomfort

Die ideale Lösung sollte ein überzeugendes Benutzererlebnis bieten und sich einfach verwalten lassen. Insbesondere in Zeiten zunehmender Remote-Arbeit spielen eine effiziente Benutzerregistrierung und Geräteeinrichtung eine wesentliche Rolle. Nur so können Sie dafür sorgen, dass neue Benutzer so schnell wie möglich produktiv arbeiten können. Achten Sie darauf, wie der ZTNA-Agent bereitgestellt wird und wie einfach sich Benutzer und Richtlinien hinzufügen lassen. Ihre Lösung sollte maximalen Komfort für Ihre Endbenutzer sowie ein hohes Maß an Transparenz bieten. Dazu gehören beispielsweise Echtzeit-Informationen über Anwendungsaktivitäten, um Auslastungsspitzen proaktiv zu bestimmen, sowie Einblick in Kapazitäten, Lizenznutzung und Anwendungsprobleme.

Sophos ZTNA

Sophos ZTNA basiert auf dem Zero-Trust-Prinzip und sorgt für einfachen, integrierten und sicheren Netzwerkzugriff. Unsere ZTNA-Lösung wird in der Cloud bereitgestellt und verwaltet und ist in Sophos Central integriert – unsere Cloud-Security-Plattform, der weltweit die meisten Kunden vertrauen. In Sophos Central verwalten Sie nicht nur ZTNA, sondern auch Ihre Sophos Firewalls, Endpoints, Mobilgeräte, Cloud-Security, Ihren Server- und E-Mail-Schutz und vieles mehr.



Sophos ZTNA zeichnet sich auch durch eine enge Integration mit der Sophos Firewall und unserer Endpoint Protection Intercept X aus. Dabei profitieren Sie von Synchronized Security sowie dem Security Heartbeat, der Statusdaten zwischen der Firewall, Ihren Geräten, ZTNA und Sophos Central austauscht, um automatisch auf Bedrohungen oder nicht konforme Geräte zu reagieren. Kompromittierte Systeme werden automatisch isoliert, bis eine vollständige Bereinigung erfolgt ist.

Unsere Kunden bestätigen uns: Eine integrierte Cybersecurity-Lösung von Sophos spart enorm viel Zeit. Kunden, die alle ihre Sophos-Produkte über Sophos Central verwalten und die automatische Bedrohungssuche und Reaktion von Synchronized Security nutzen, geben an, dass sie so die Arbeitsleistung ihres IT-Teams effektiv verdoppeln konnten. Natürlich ist Sophos ZTNA auch mit Sicherheitsprodukten anderer Anbieter kompatibel. Unsere Lösung ist jedoch perfekt auf die Komponenten des Sophos-Ökosystems abgestimmt und bietet in Kombination mit anderen Sophos-Produkten einzigartige Transparenz, Sicherheit und Reaktion.

Mehr erfahren unter

www.sophos.de/ztna

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

21-08-09 DE (DD)

SOPHOS