PRISMA ACCESS
BY PALO ALTO NETWORKS

Sichere Transformation: Fernzugriff mit Prisma Access statt VPNs

Überblick

VPNs sind so sehr zur Standardlösung für den sicheren Fernzugriff auf Unternehmensnetzwerke geworden, dass viele von uns die Begriffe „Fernzugriff“ und „VPN“ als Synonyme verwenden. Doch mit der zunehmenden Nutzung von Cloud-Anwendungen ändern sich die Anforderungen an Netzwerke und die Netzwerk-Sicherheit. Netzwerk- und Sicherheitsteams müssen sich nun mit der Frage beschäftigen, wie sie für sicheren Zugang zu allen in ihrem Unternehmen genutzten Anwendungen sorgen können – sowohl innerhalb als auch außerhalb der eigenen Rechenzentren.

Lassen diese neuen Anforderungen sich mit VPNs erfüllen oder ist es an der Zeit, den Fernzugriff völlig neu zu durchdenken und zu einer moderneren Lösung zu wechseln?

Die Grenzen des Fernzugriffs

VPNs wurden für einen ganz bestimmten Zweck entwickelt: als Gateway für legitime Nutzer, die sich außerhalb des Firewall-Perimeters befinden und Zugang zu den Ressourcen im Rechenzentrum benötigen.

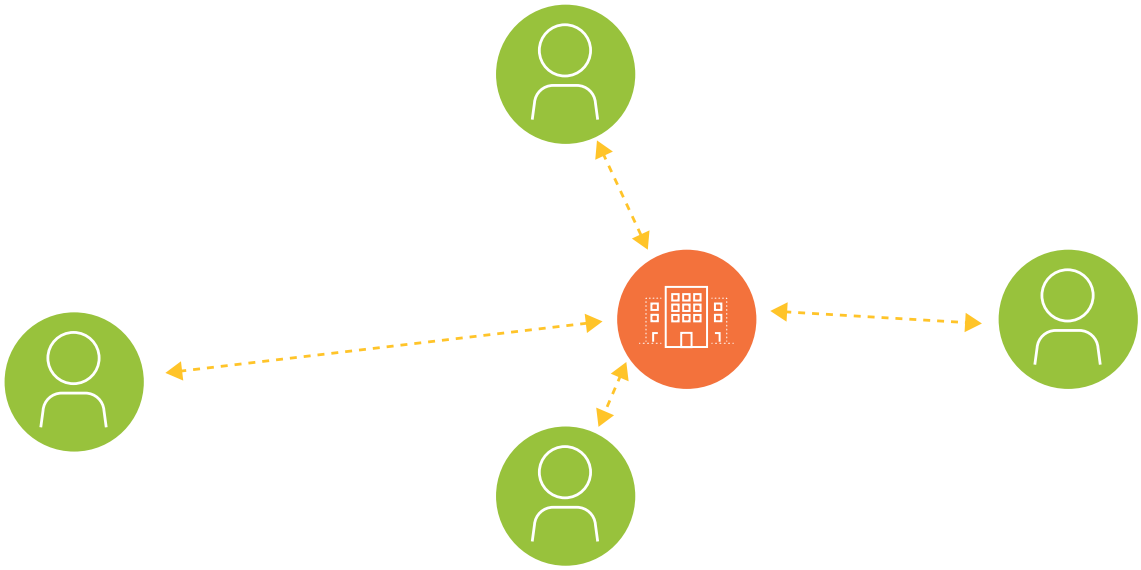

Abbildung 1: Konventionelle VPN-Architektur für den Fernzugriff

Architektonisch betrachtet ist ein solches VPN eine Sterntopologie, bei der die Nutzer (bzw. ihre Endgeräte) über verschieden lange „Strahlen“ mit dem zentralen Knoten – dem unternehmensinternen Rechenzentrum – verbunden sind. Mit zunehmender Entfernung vom Rechenzentrum sinkt die Leistung, während Probleme wie die Latenz zunehmen. Dennoch ist dies die bestmögliche Architektur für den Zugriff auf Anwendungen im Rechenzentrum, da dies auf direktem Weg erreicht wird.

Die Situation ändert sich jedoch, sobald auch Cloud-Anwendungen Teil der Infrastruktur sind. Der Datenverkehr in einem VPN wird immer zuerst an das VPN-Gateway geleitet, auch wenn er für eine in der Cloud gehostete Anwendung bestimmt ist. Der Datenverkehr geht also zuerst zum VPN-Gateway in der Firmenzentrale und dann über eine Firewall am Netzwerkrand ins Internet. Die Antwort der Anwendung nimmt denselben Weg, in umgekehrter Richtung. Die Daten nehmen also sowohl auf dem Hin- als auch auf dem Rückweg

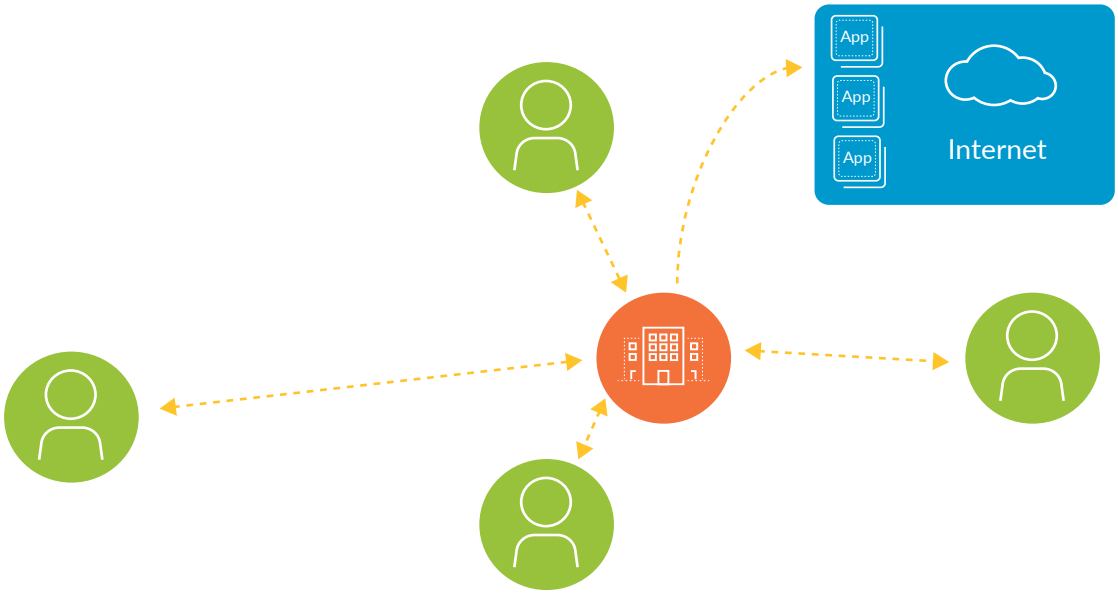

Abbildung 2: Konventionelle VPN-Architektur, bei der der Datenverkehr von und zu Cloud-Umgebungen über die Firmenzentrale läuft

einen langen Umweg über die Firmenzentrale, obwohl ihr Zielort über das Internet erreichbar ist. Aus der Sicherheitsperspektive ist das sinnvoll (da die meisten Sicherheitsvorrichtungen sich am Rand des Unternehmensnetzwerks befinden), doch aus dem Blickwinkel der Netzwerkoptimierung ist es nicht zielführend.

Im Gegenteil: Der Umweg über ein VPN kann die Nutzererfahrung von Cloud-Anwendungen so stark beeinträchtigen, dass viele Nutzer VPNs nur verwenden, wenn das unbedingt erforderlich ist. Sie melden sich also über das VPN an, wenn sie Zugang zum unternehmensinternen Rechenzentrum benötigen, und dann wieder ab, wenn das nicht mehr der Fall ist. Das ist ein Problem für das Sicherheitsteam, denn wenn die Nutzer nicht über das VPN angemeldet sind, hat es keinen Überblick über die Anwendungen, die sie nutzen. Infolgedessen kann es weder den Zugriff auf nicht genehmigte Anwendungen unterbinden noch sonstige Sicherheitsrichtlinien konsequent durchsetzen.

Diese Herausforderung lässt sich nicht mit zusätzlichen VPN-Gateways bewältigen, denn ein VPN-Gateway ist nur der Endpunkt eines VPN-Tunnels. Es analysiert den Netzwerkverkehr nicht. Daran ändern auch zusätzliche VPN-Gateways nichts – zumindest nicht, solange keine zusätzlichen Sicherheitsmaßnahmen implementiert werden.

Unbefriedigende Kompromisse

Um die mit VPN verbundenen Netzwerkprobleme zu umgehen, nutzen Unternehmen oft Kompromisslösungen mit negativen Auswirkungen auf die Sicherheit.

- **Nutzerinitiierte Tunnel:** In einem gängigen Modell können die Nutzer den Aufbau eines VPN-Tunnels veranlassen, wenn sie Zugang zum unternehmensinternen Rechenzentrum benötigen. In diesem Modell sind Nutzer gewöhnlich nur für kurze Zeit per VPN verbunden. Sobald sie die Anwendungen im Rechenzentrum nicht mehr benötigen, melden sie sich wieder ab. Wenn sie nicht mit dem VPN verbunden sind, greifen sie direkt auf das Internet zu, ohne dass der Datenverkehr überprüft wird.
- **Getrennte Tunnel:** Eine weitere gängige, aber unsichere Methode sind getrennte Tunnel. Bei diesem Modell wird nur der Netzwerkverkehr vom und zum Unternehmensnetzwerk über das VPN übertragen. Für alles andere wird der Direktzugang zum Internet genutzt. Dadurch wird möglicherweise die Latenz des Internetdatenverkehrs reduziert, doch der Datenaustausch mit dem Internet und mit öffentlichen Clouds kann nicht kontrolliert werden.
- **Web-Proxys:** Als Ausgleich für die Zeit, in der ein Nutzer nicht mit dem VPN verbunden ist, wurden in vielen Unternehmen alternative Sicherheitsmaßnahmen implementiert. Ein Beispiel hierfür sind Web-Proxys. Web-Proxys wurden jedoch nicht für die umfassende Prüfung des Netzwerkverkehrs konzipiert. Noch bedenklicher ist, dass der Verkehr, den ein solcher Proxy analysiert, sich grundlegend von dem in der Firmenzentrale inspizierten Netzwerkverkehr unterscheidet. Die Ergebnisse hängen also vom Nutzerstandort ab und sind daher nicht ohne Weiteres vergleichbar.

Zusammenfassend lässt sich sagen, dass viele Sicherheitsverantwortliche angesichts der steigenden Zahl der mobilen Mitarbeiter und der cloudbasierten Anwendungen zu der Schlussfolgerung gelangen, dass die vorhandenen Lösungen für den Fernzugriff weder Schritt halten noch das erforderliche Maß an Sicherheit bieten können. Deshalb ist ein neuer Ansatz erforderlich.

Eine moderne Architektur für mobile Mitarbeiter

Mobile Mitarbeiter benötigen Zugang zum Rechenzentrum, zum Internet und zu Anwendungen in öffentlichen, privaten und Hybrid-Clouds. Mit anderen Worten: Der neue Ansatz sollte den Benutzern an allen Standorten stets optimalen Zugang zu sämtlichen Anwendungen bieten. Prisma™ Access stellt eine cloudbasierte Sicherheitsinfrastruktur bereit, über die Nutzer sicher mit einem nahegelegenen Cloud-Gateway verbunden werden können. Damit unterstützt dieser Cloud-Service nicht nur den sicheren Zugriff auf alle Anwendungen, sondern auch die Überprüfung und Überwachung des gesamten Datenverkehrs, unabhängig vom genutzten Port und Protokoll.

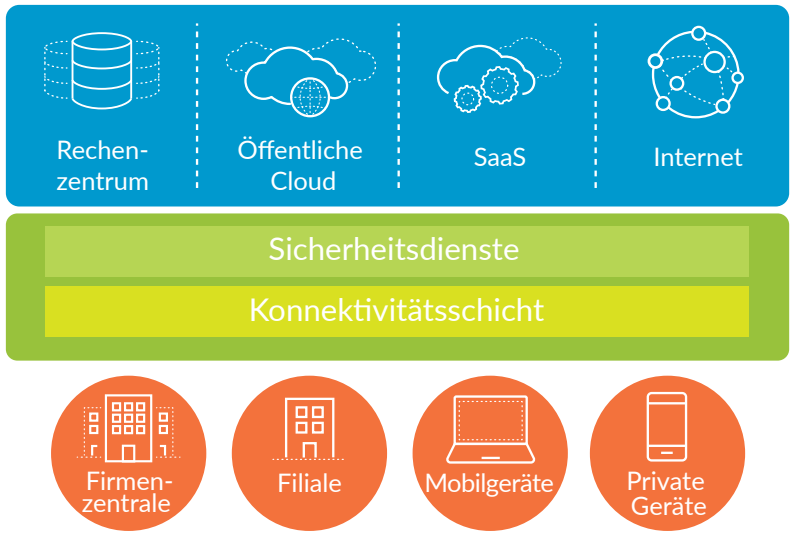

Abbildung 3: Cloudbasierter Schutz für alle Nutzer, unabhängig vom Standort

Für verwaltete Mobilgeräte

Auf den verwalteten Geräten dieser Nutzer (Laptops, Handys oder Tablets) ist die App GlobalProtect installiert. Diese App stellt automatisch (ohne Zutun des Nutzers) eine Verbindung zu Prisma Access her, sobald das Gerät mit dem Internet verbunden ist.

Prisma Access verbindet Anwendungen an verschiedenen Standorten über seine Konnektivitätsschicht miteinander, sodass Nutzer Zugang zu allen Anwendungen haben, unabhängig davon, ob diese in der Cloud oder im Rechenzentrum gehostet werden. Die Konnektivitätsschicht nutzt App-ID™, User-ID™ und die entsprechenden Richtlinien, um den sicheren Zugriff auf Anwendungen in öffentlichen Clouds, Software-as-a-Service-Umgebungen und Rechenzentren zu unterstützen.

Auf der Schicht der Sicherheitsdienste stellt Prisma Access die erforderlichen Sicherheitsmaßnahmen bereit. Dazu gehören alle Sicherheitsmaßnahmen, die Sie von der Palo Alto Networks Security Operating Platform® gewohnt sind, darunter das Erkennen von bekannter und neuer Malware, Exploits, Kommunikation mit Command-and-Control-Servern und Angriffen mit gestohlenen Anmeldedaten.

Für nicht verwaltete/BYOD-Geräte

In Kombination mit der MDM-Integration (Mobile Device Management) kann Prisma Access zur Durchsetzung von BYOD-Richtlinien eingesetzt werden. Dabei werden durch die Integration Funktionen wie anwendungsspezifische VPNs verfügbar. Beschäftigte von Auftragnehmern und Vertragspartnern, andere Nutzer mit nicht verwalteten Geräten sowie Mitarbeiter mit BYOD-Geräten erhalten über clientloses VPN Fernzugriff zum Rechenzentrum. Mit diesem Ansatz kann die SAML-Proxy-Integration genutzt werden, um Nutzern nicht verwalteter Geräte mit Inline-Sicherheitsmaßnahmen sicheren Zugang zu SaaS-Anwendungen zu bieten.

Zukunftssicher

Wenn Sie prüfen, ob Ihre vorhandene VPN-Architektur den Anforderungen Ihres Unternehmens noch gewachsen ist, sollten Sie auch den Wechsel zu einer völlig neuen Architektur in Erwägung ziehen, mit der Sie Ihren Nutzern sicheren Zugang zu sämtlichen Anwendungen gewähren und Ihr Unternehmen gleichzeitig effektiv vor Cyberangriffen schützen können. Mit Prisma Access befreien Sie Ihr Unternehmen von den Einschränkungen, die mit VPN-basiertem Fernzugriff einhergehen, und bieten Ihren Nutzern sicheren Zugang zu allen Anwendungen, die sie benötigen.

Weitere Informationen finden Sie unter www.paloaltonetworks.com/cloud-security/prisma-access.

PRISMA ACCESS
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam,
Niederlande

Telefon: +31 20 888 1883
Vertrieb: 0800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

secure-transformation-replacing-remote-access-vpn-with-prisma-accesssb-