

STÄRKEN SIE TELEARBEIT MIT TUNNELFREIEM SESSION SMART SD-WAN

Telearbeit wird nicht nur immer häufiger, sondern ist für Unternehmen in Krisenzeiten unverzichtbar geworden

Herausforderung

Traditionell basieren VPN-Lösungen auf IPsec- oder SSL-Tunneling. Diese Technologien sind komplex und schwer zu skalieren, da sie auf einem starren Modell beruhen, das die Telearbeit erschwert.

Lösung

Session Smart SD-WAN schafft eine servicezentrierte Fabric, die eine Architektur für standortunabhängiges Arbeiten ermöglicht, die ideal ist, um Agilität, Sicherheit und eine hochwertige Remote-Benutzererfahrung zu bieten.

Vorteile

- Verbesserte Benutzererfahrung und Netzwerkleistung
- Reduzierte Sicherheitsrisiken bei gleichzeitiger Wahrung von Compliance
- Umfassende, fein abgestufte Service- und Netzwerkvisibilität.
- Vereinfachte servicezentrierte und tunnelfreie Architektur

Die COVID-19-Pandemie hat Unternehmen ihre Schwachstellen bei der Bereitstellung flexibler, sicherer und produktiver Arbeitsumgebungen im Homeoffice deutlich vor Augen geführt. Dies gilt insbesondere für VPNs, die für die Arbeit im Homeoffice – oder an anderen Orten außerhalb des Büros – unerlässlich sind. Die Nachfrage nach stark verteilten und sicheren Netzwerklösungen, die die Qualität, Zuverlässigkeit und Agilität bieten, die für die Unterstützung von Telearbeitern erforderlich sind, war noch nie so offensichtlich wie heute. Juniper® Session Smart™ SD-WAN bietet eine Zero-Trust-Struktur, die eine beispiellose Kontrolle und den Zugriff auf die kritischen Ressourcen ermöglicht, die Telearbeitende benötigen – mit einem Routing, das sich nahtlos an die Anforderungen der Anwendungsleistung und des Datenverkehrs anpasst.

Die Herausforderung

Angesichts der gestiegenen Nachfrage nach Telearbeitsplätzen stehen die Verfügbarkeit und die Sicherheit von VPN-Diensten heute im Fokus der IT-Abteilungen von Unternehmen auf der ganzen Welt. VPNs leiten aus Sicherheitsgründen typischerweise den gesamten Datenverkehr durch einen Tunnel in das Netzwerk der Firma. Dazu gehören sichere öffentliche Software-as-a-Service-Anwendungen (SaaS) (z. B. Microsoft Teams, Salesforce und Google Suites), Standard-Internetzugang und am Standort des Kunden gehostete Services.

Traditionell basieren VPN-Lösungen auf der IPsec- oder SSL-Tunneling-Technologie. Diese Arten von VPNs sind komplex und schwer zu skalieren, und sie ermöglichen keine Anwendungskontrolle oder Visibilität. Da Unternehmen die Cloud nutzen, das Internet der Dinge (IoT) sich ausbreitet, Benutzer mobil werden und Anwendungen eine höhere Reaktionsfähigkeit erfordern, macht das starre Routing-Modell dieser Tunneling-Technologien das Arbeiten an Standorten außerhalb des Unternehmens recht schwierig. Aus diesem Grund sind viele Unternehmen durch die hohen VPN/WAN-Kosten frustriert und wollen diese Services erneuern. Durch die gleichzeitige Umstellung ihrer Netzwerke können Unternehmen ihre Investitionen in das WAN maximieren.

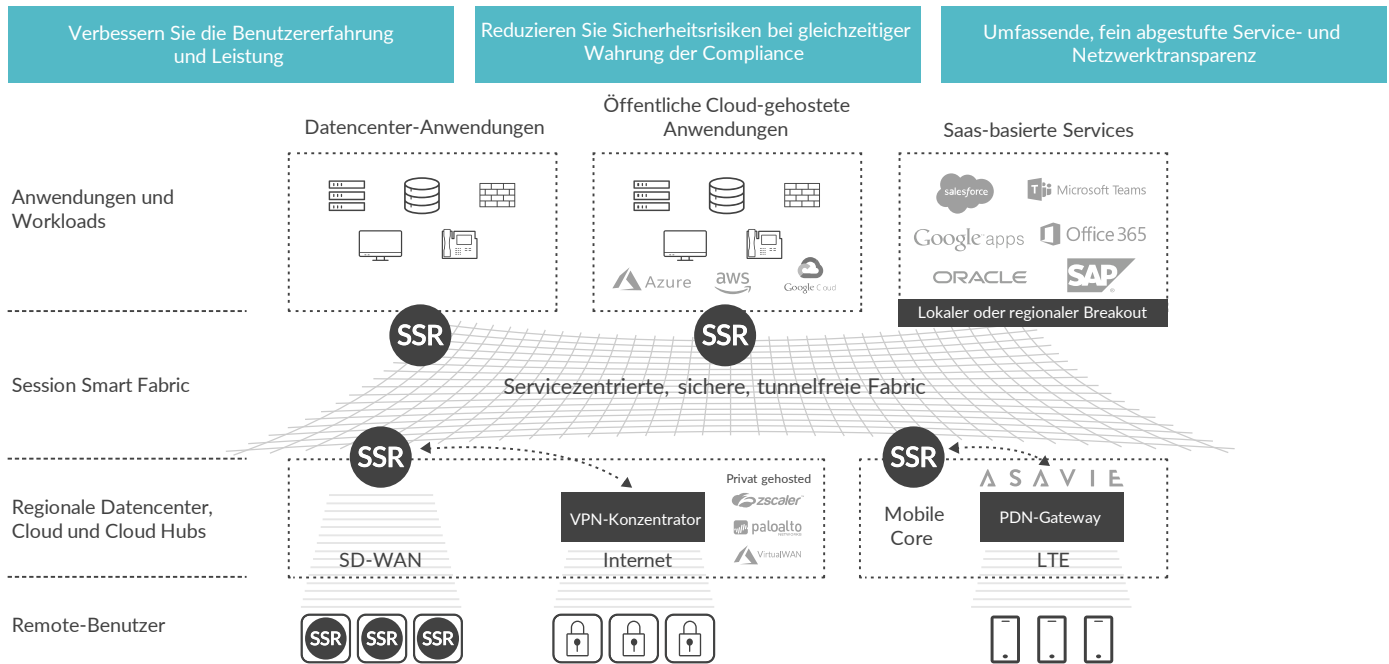


Abbildung 1: Session Smart SD-WAN für Telearbeitende

Die Juniper Session Smart SD-WAN-Lösung

Noch nie zuvor war die Vernetzung so wichtig für unser Leben und unseren Lebensunterhalt. In der Tat war die Nachfrage nach stark verteilten und sicheren Netzlösungen noch nie größer. Die servicezentrierte Fabric der Juniper Session Smart SD-WAN-Lösung vereinfacht die Architektur für standortunabhängiges Arbeiten, die in einzigartiger Weise Agilität, Sicherheit und eine hochwertige Benutzererfahrung bietet.

Als wichtiger Bestandteil der Lösung passt sich der Juniper Session Smart-Router dynamisch an die Leistungsanforderungen der Anwendung an und leitet den Datenverkehr entsprechend weiter. Dieser tunnelfreie Ansatz reduziert die Anwendungslatenz und erhöht gleichzeitig die verfügbare Bandbreite für Video- und andere netzwerkintensive Anwendungen. Die native Sitzungsoptimierung kann verwendet werden, um die Geschwindigkeit und Zuverlässigkeit der Anwendung sowie die Qualität, Sicherheit und Compliance zu verbessern.

Die heutzutage weit verbreitete Telearbeit, die die Arbeit von überall aus ermöglicht, stellt den herkömmlichen perimeterbasierten Sicherheitsansatz infrage und verlangt, dass die Sicherheit in die Netzwerke integriert wird. Session Smart SD-WAN bietet eine Zero-Trust-Fabric, die beispiellose Kontrolle über den Zugriff auf kritische Ressourcen und Daten bietet, die Mitarbeitende benötigen – Routing für den Zugriff zur richtigen Zeit am richtigen Ort.

Der Vorteil des Session Smart-Router

Der Juniper Session Smart Router macht ineffiziente VPN-Tunnel überflüssig und bringt ein kontextbezogenes Bewusstsein in das Netz, indem er transiente Sessions mit den Anwendungen und Services verknüpft, die sie ermöglichen. Diese Technologie vereinfacht die Art und Weise, wie Unternehmen die Anforderungen von Telearbeitern unterstützen: Sie bietet zentralisiertes Management, differenzierte Kontrolle, individualisierte Datenströme und integrierte Funktionen – und alles mit integrierter Sicherheit und dynamischem Datenverkehrsmanagement. Die intelligenten Funktionen der Session Smart SD-WAN-Lösung helfen Unternehmen dabei, unübertroffene Qualität, Zuverlässigkeit und Skalierbarkeit für die Anwendungen und Services bereitzustellen, die für den Erfolg des Unternehmens wichtig sind – selbst bei starker Beanspruchung durch Telearbeitende.

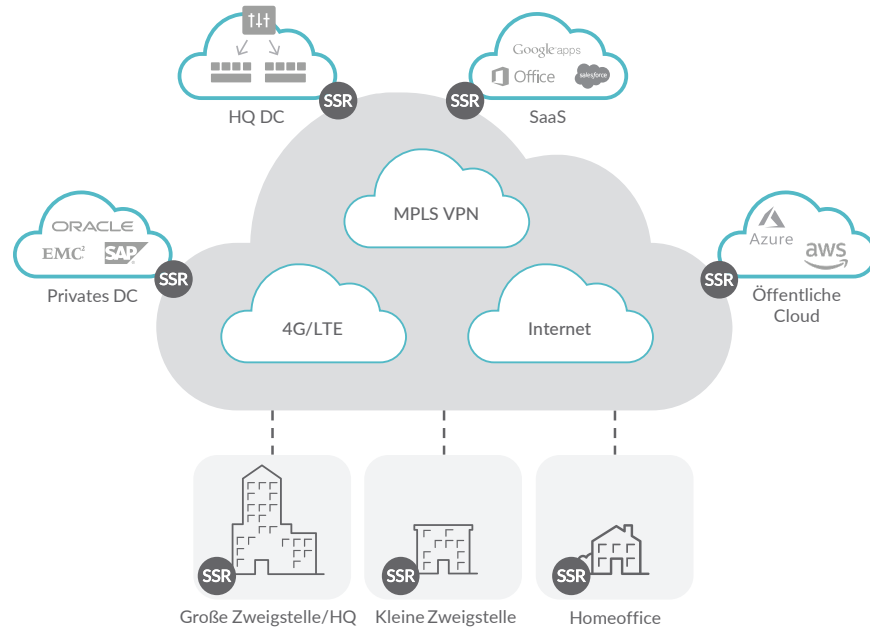


Abbildung 2: Session Smart SD-WAN, tunnelfreie Konnektivität

Die Session Smart SD-WAN-Lösung macht nicht nur Overlays und Tunnel überflüssig, sondern zentralisiert auch die Informationen über Services, Mandanten und Richtlinien. Dadurch entfällt die Notwendigkeit von Automatisierungstools, die Komplexität wird minimiert, die Visibilität verbessert und

Einsparungen maximiert. Darüber hinaus kann dieser kontextorientierte Ansatz die Bedürfnisse von Unternehmen besser unterstützen und zum Erfolg beitragen, insbesondere wenn unerwartete Herausforderungen auftreten und die Fähigkeit zur Unterstützung von Telearbeitenden entscheidend wird.



Abbildung 3: Session Smart SD-WAN ist kontextorientiert

Funktionen und Nutzen

Anwendungsorientiertes Routing

IT-Abteilungen können die Leistung ihrer Netzwerke verbessern, indem sie anwendungsorientiertes Routing bereitstellen. Der Session Smart Router erkennt beispielsweise Anwendungen wie Microsoft Office 365, Google Suites und andere SaaS-Dienste und verlagert diesen Datenverkehr direkt ins WAN. Nur vom Unternehmen gehostete Anwendungen werden an das Datacenter weitergeleitet. Darüber hinaus sorgen dynamische Session- und Anwendungsorientierung für Load Balancing und die Steuerung des Datenverkehrs auf der Grundlage von Session-Richtlinien und dem Status des Netzwerks – Funktionen, die entscheidend sind, wenn Hunderte Mitarbeiter plötzlich nicht mehr an den Unternehmensstandorten arbeiten.

FIPS 140-2 Zertifizierung

Der Computersicherheitsstandard der US-Regierung, FIPS-140-2, wird zur Genehmigung von kryptografischen Modulen und zur Wahrung der Geheimhaltung verwendet. Session Smart SD-WAN erfüllt diese Zertifizierung und ermöglicht es Unternehmen, ein Netz aufzubauen, das den Anforderungen der Payment Card Industry (PCI) und des Health Insurance Portability and Accountability Act (HIPAA) entspricht. Darüber hinaus ist der Session Smart Router nach ICSA Labs Network Firewall zertifiziert und hat die PCI-Bescheinigung erhalten. Unternehmen können sich sicher sein, dass ihre Netzwerke – und ihre Daten – sicher sind, ganz gleich, wo sich die Mitarbeiter befinden.



Abbildung 4: Zertifiziert nach FIPS-140-2 und ICSA Labs Network Firewall

Zero-Trust-Sicherheit

Mit Session Smart SD-WAN können Unternehmen ein Netzwerk aufbauen, das auf Zero-Trust-Sicherheit basiert und dafür sorgt, dass jeder Datenstrom verschlüsselt und auf der Grundlage der zugehörigen Sicherheitsrichtlinien authentifiziert wird. So können Unternehmensverantwortliche sicher sein, dass sie selbst bei Mitarbeitern, die von zu Hause aus arbeiten, sicher mikrosegmentierte Verbindungen oder individualisierte VPNs für verschiedene Geschäftsbereiche innerhalb einer großen Organisation anbieten können.



Abbildung 5: Leistungsmerkmale der Session Smart SD-WAN-Lösung

Erhöhte Visibilität

Der Juniper Session Smart Conductor bietet eine zentrale Orchestrierung, Verwaltung, Zero-Touch-Bereitstellung, Überwachung und Analyse für verteilte Session Smart Router. Diese Tools bieten eine einheitliche Ansicht des gesamten Netzwerks und erweiterte Session-Statistiken, was in Homeoffice-Umgebungen immer mehr an Bedeutung gewinnt. Mit ihnen können Administratoren benutzerdefinierte Diagramme auf Basis ausgewählter wichtiger Leistungsindikatoren (KPIs) und detaillierte Berichte über Sicherheits- und Verkehrsereignisse erstellen. Dies ermöglicht es Unternehmen, Angriffe auf das Netzwerk zu erkennen und zu verhindern, selbst wenn die Mitarbeiter über mehrere Standorte verteilt sind, und gleichzeitig die Compliance-Anforderungen des Unternehmens zu erfüllen.



Session Smart SD-WAN – Anwendungsfälle

Session Smart SD-WAN zu Hause

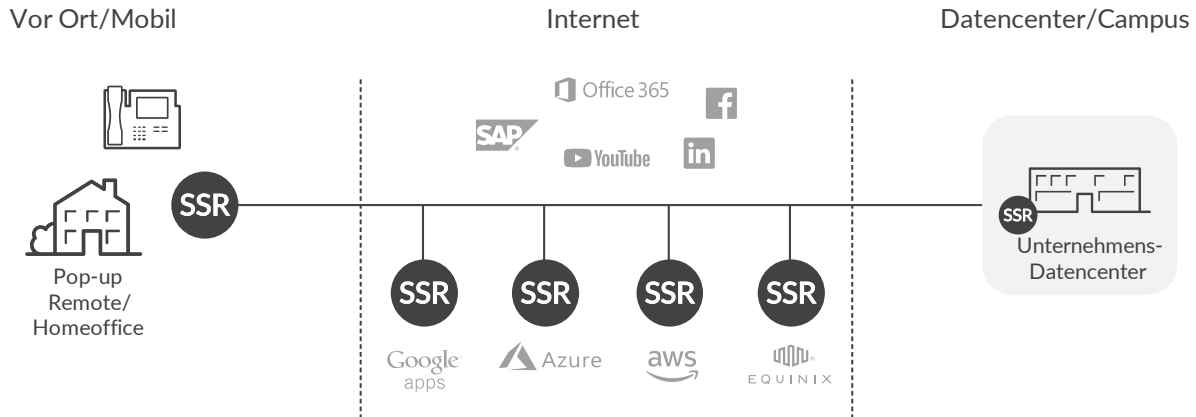


Abbildung 6: Session Smart SD-WAN zu Hause

Kundennutzen

| Benutzererfahrung | Sicherheit und Compliance | Visibilität |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> Einfache Verbindung zum Gerät | <ul style="list-style-type: none"> FIPS 140-2 | <ul style="list-style-type: none"> Überprüfung pro Sitzung |
| <ul style="list-style-type: none"> Geringe Latenz und hoher Durchsatz | <ul style="list-style-type: none"> Konnektivität von innen nach außen | <ul style="list-style-type: none"> Mandanten- und Serviceleistungen |
| <ul style="list-style-type: none"> Vollständig automatisierte Bereitstellung | <ul style="list-style-type: none"> Mikrosegmentierter Zugang | <ul style="list-style-type: none"> Vollständig verteilte Analytik |

In diesem Anwendungsfall wird ein Session Smart Router zu Hause und ein anderer im Datencenter oder in der Cloud eingesetzt. Die Anwendungen werden dann auf der Grundlage ihres Ziels intelligent geroutet. Während SaaS-Anwendungen beispielsweise direkt in das WAN verlagert werden, können Unternehmensanwendungen, die eine erweiterte Unified Threat Management (UTM)-Behandlung erfordern, in das Datencenter des Unternehmens geroutet werden.

Session Smart SD-WAN in der Cloud

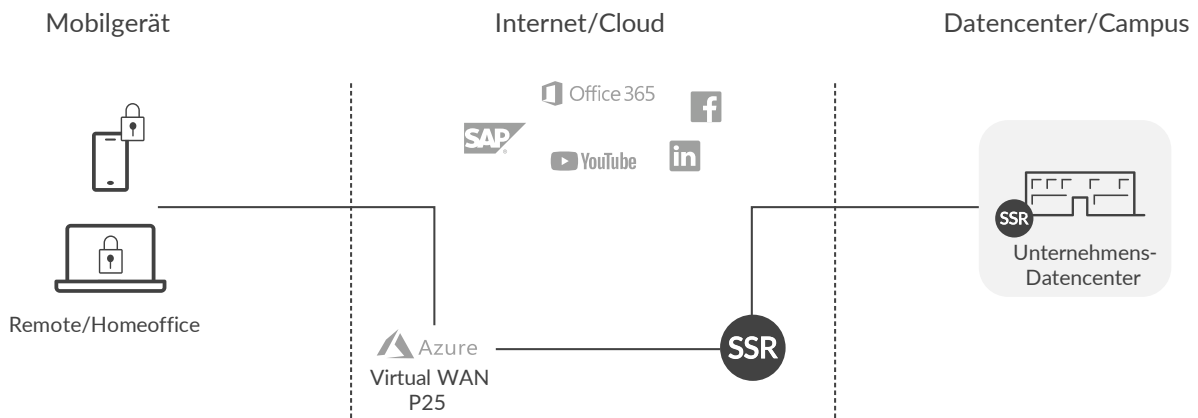


Abbildung 7: Session Smart SD-WAN in der Cloud

Kundennutzen

| Benutzererfahrung | Sicherheit und Compliance | Visibilität |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • VPN-Client-Erfahrung (Portal/Login) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Überprüfung pro Sitzung |
| <ul style="list-style-type: none"> • Cloud-basiertes Skalieren | <ul style="list-style-type: none"> • Konnektivität von innen nach außen | <ul style="list-style-type: none"> • Mandanten- und Serviceleistungen |
| <ul style="list-style-type: none"> • Nahtlose Konnektivität | <ul style="list-style-type: none"> • Mikrosegmentierter Zugang | <ul style="list-style-type: none"> • Vollständig verteilte Analytik |

In diesem Anwendungsfall verbindet sich ein Telearbeiter über Standardtechnologie mit dem Cloud-VPN-Gateway, das dann den Datenverkehr an den Session Smart Router übergibt, der die Pakete intelligent an das richtige Ziel routet. Der Session Smart Router kann unterscheiden zwischen RFC1918-Netzwerken, die in das Firmennetz geroutet werden, und allem anderen Verkehr, einschließlich Cloud-Services, die entweder direkt zu den Services oder durch eine UTM-Lösung geroutet werden.

Session Smart SD-WAN im Datacenter mit privatem LTE-Zugang

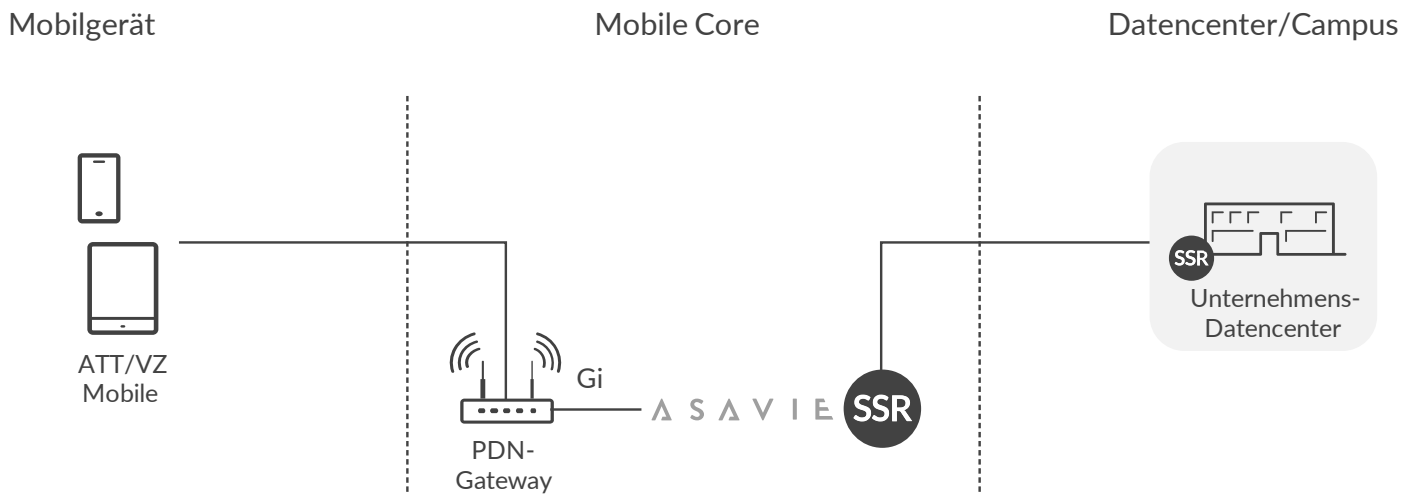


Abbildung 8: Session Smart SD-WAN im Datacenter mit privatem LTE-Zugang

Kundennutzen

| Benutzererfahrung | Sicherheit und Compliance | Visibilität |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Client-basierte Erfahrung (Portal/Login) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Überprüfung pro Sitzung |
| <ul style="list-style-type: none"> • Cloud-basiertes Skalieren | <ul style="list-style-type: none"> • Konnektivität von innen nach außen | <ul style="list-style-type: none"> • Mandanten- und Serviceleistungen |
| <ul style="list-style-type: none"> • Nahtlose Konnektivität | <ul style="list-style-type: none"> • Mikrosegmentierter Zugang | <ul style="list-style-type: none"> • Vollständig verteilte Analytik |

Dieser Anwendungsfall profitiert von einer Partnerschaft mit Asavie, die flächendeckende sichere private LTE-Verbindungen anbietet, um die Arbeit von zu Hause aus zu erleichtern. Das Session Smart SD-WAN wird im LTE-Core und im Datacenter des Unternehmens eingesetzt und bietet Netzsicherheit, Netzwerkzugangskontrolle, anwendungsorientiertes Routing und Compliance.

Session Smart SD-WAN mit Wireguard

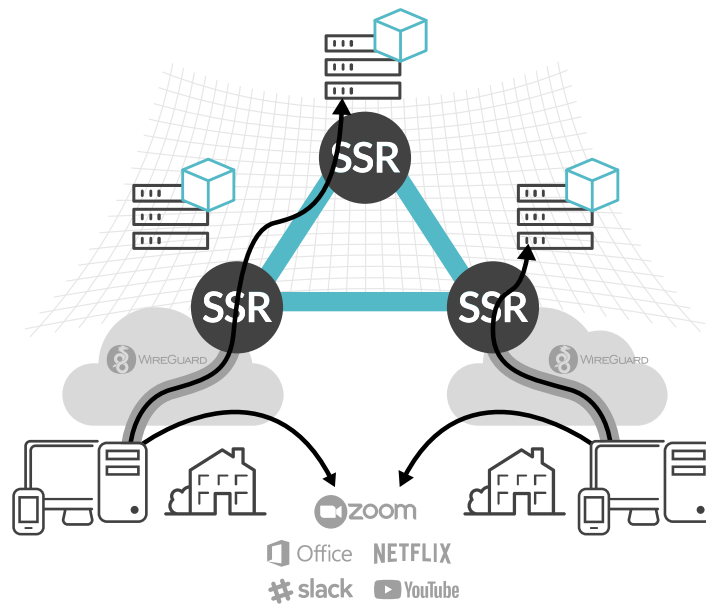


Abbildung 9: Session Smart SD-WAN mit Wireguard

Kundennutzen

| Benutzererfahrung | Sicherheit und Compliance | Visibilität |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Zero-Touch-Erfahrung (Wi-Fi-Verbindung) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Überprüfung pro Sitzung |
| <ul style="list-style-type: none"> • Cloud-basiertes Skalieren | <ul style="list-style-type: none"> • Konnektivität von innen nach außen | <ul style="list-style-type: none"> • Mandanten- und Serviceleistungen |
| <ul style="list-style-type: none"> • Vollständig automatisierte Bereitstellung | <ul style="list-style-type: none"> • Mikrosegmentierter Zugang | <ul style="list-style-type: none"> • Vollständig verteilte Analytik |

In diesem letzten Einsatzszenario werden Unternehmensgeräte, die für die Arbeit außerhalb des Büros vorgesehen sind, mit einem leichtgewichtigen Wireguard – einer kostenlosen und quelloffenen VPN – Lösung – eingerichtet, der ein Peering mit einem (oder mehreren) Session Smart Routern in der Topologie des Unternehmens durchführt. Es sendet selektiv und intelligent sichere Sessions an die Session Smart Router-Peers, wo Services abgerufen werden können, und verlagert sichere SaaS- und Benutzerdienste direkt in das Breitbandnetz. Wireguard, kombiniert mit dem Session Smart-Router, erweitert den Zugang zum Netzwerk des Unternehmens auf Benutzer, die sich außerhalb des Büros befinden.

Zusammenfassung – Session Smart SD-WAN stellt alles für den Erfolg von Telearbeitenden bereit

Die Juniper Session Smart SD-WAN-Lösung bietet eine zentrale Steuerung, eine vereinfachte Bereitstellung kontextbezogener Netzwerke, intelligentes Service-Routing mit In-Band-Signalen, fein abgestufte Mikrosegmentierung und integrierte Sicherheit auf der Basis eines Zero-Trust-Modells. Diese Kombination aus Funktionen und Fähigkeiten geht über herkömmliche Router-Angebote hinaus, indem sie mehrere zugrunde liegende Netzwerkprobleme löst, die sonst dem Erfolg von Telearbeit im Weg stünden.

Das Ergebnis ist ein kontextbezogenes Netzwerk, das sich einfach, dynamisch und sicher über Grenzen hinweg ausdehnen kann und es Unternehmen ermöglicht, anwendungsfreundliche Infrastrukturen aufzubauen, die flexibel genug sind, um den Anforderungen einer verteilten Belegschaft gerecht zu werden.

Nächste Schritte

Um zu erfahren, wie Session Smart SD-WAN Ihrem Unternehmen helfen kann, Telearbeitende zu unterstützen, wenden Sie sich bitte an Ihren Juniper Kundenbetreuer oder besuchen Sie www.juniper.net.

Über Juniper Networks

Juniper Networks vereinfacht mit seinen Produkten, Lösungen und Services die Netzwerke, die unsere Welt umspannen. Durch kontinuierliche Innovation überwinden wir die Einschränkungen und die Komplexität, mit der Netzwerkadministratoren in der Cloud-Ära zu kämpfen haben, und unterstützen unsere Kunden und Partner bei der Bewältigung ihrer größten Herausforderungen. Wir bei Juniper Networks sind überzeugt, dass Netzwerke ein Medium für den weltweiten Wissensaustausch und den die Welt verändernden Fortschritt der Menschheit sind. Deshalb haben wir uns das Ziel gesetzt, bahnbrechende Lösungen für automatisierte, skalierbare und sichere Netzwerke zu entwickeln, die mit dem Tempo unserer schnelllebigen Geschäftswelt Schritt halten.

Unternehmens- und Vertriebs Hauptsitz

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Telefon: +1 888 586 4737
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net/de

Hauptniederlassung für die Regionen APAC und EMEA

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 0207 125 700
Fax: +31 0207 125 701

JUNIPER NETWORKS | Engineering Simplicity

