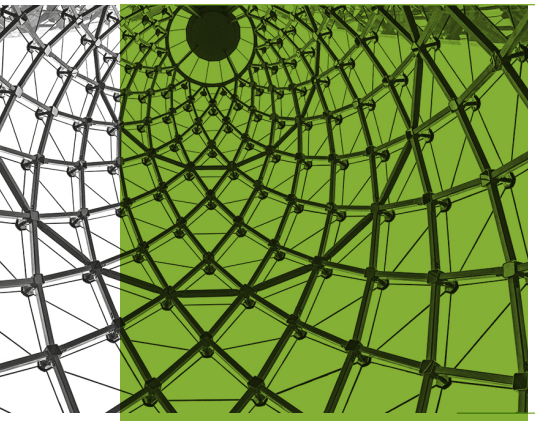

ENTERPRISE@HOME

Volle Sicherheit für mobile Mitarbeiter

Herausforderungen

Organisationen müssen dafür sorgen, dass ihre Remote-Benutzer vernetzt und produktiv bleiben, und gleichzeitig Business Continuity und Sicherheit gewährleisten. Dafür reichen die Endpoint-Absicherung und ein simples VPN zum Unternehmenssitz nicht aus. Es wird eine umfassende und vernetzte Sicherheitsstrategie benötigt.

Lösung

Durch die Kombination aus Mist Wi-Fi und Mist Edge mit Juniper Connected Security können Organisationen das KI-gestützte Unternehmen zum Mitarbeiter nach Hause bringen. Dank Zero Touch-Provisioning können die Juniper Security-Hardware und die Mist Access Points ohne Techniker vor Ort aus der Ferne eingerichtet werden.

Vorteile

- *KI-gestützte Einblicke in das Remote-Benutzererlebnis*
- *Einfache Installation mit Zero-Touch Provisioning*
- *Macht VPN-Technologien überflüssig und bringt das Unternehmensnetzwerk zum Mitarbeiter nach Hause*
- *Überwachung des Unternehmens-Wi-Fi zum Schutz des Business-Datenverkehrs*
- *Mehr Sicherheit und Segmentierung des Business-Datenverkehrs*
- *Hält Bedrohungen mit hochentwickelten Security-Services in Schach*
- *Schaffung eines dynamischen, flexiblen und adaptierbaren Netzwerks*

Die Zeit, in der alle Mitarbeiter persönlich im Büro erscheinen mussten und sämtliche organisatorischen Daten ausschließlich innerhalb der unternehmenseigenen Gebäude existierten, ist vorbei. Es hat sich nicht nur gezeigt, dass das Arbeiten von zu Hause aus möglich ist, sondern auch, dass es in einer Größenordnung funktioniert, die sich keiner vorstellen konnte. Jetzt lautet die wichtigste Herausforderung, die Sicherheit der Remote-Mitarbeiter zu gewährleisten.

Bei den meisten Organisationen ist grundlegende Informationssicherheit an allen Verbindungspunkten ein Muss, zum Beispiel Deep Network Visibility und Umsetzung von Policies. Der Trend zum Home Office macht dieses Modell komplizierter, weil die Mitarbeiter sich nicht mehr im traditionellen, organisatorisch geschützten Zugangsnetzwerk aufhalten. Dadurch ändert sich die Art und Weise, wie wir zwischen unseren Netzwerken agieren. Organisationen jeder Größe brauchen entsprechende Tools, um eine sichere Anpassung an diese neue Landschaft zu gewährleisten.

Die Herausforderung

Überall auf der Welt hatten Organisationen von heute auf morgen plötzlich eine Vielzahl an neuen Remote-Mitarbeitern, was zu einer Überlastung von herkömmlich konfigurierten VPNs führte. Zwar vereinfacht das Routing des gesamten Endpoint-Datenverkehrs über die Kerninfrastruktur des Unternehmensnetzwerks die Sicherheit, indem Abwehrmaßnahmen zentralisiert und konzentriert werden können. Gleichzeitig steigt jedoch das Volumen des Datenverkehrs an, wodurch sich möglicherweise der Zugriff auf Ressourcen verlangsamt und das Remote-Benutzererlebnis beeinträchtigt wird.

In einer modernen Umgebung müssen Organisationen schnelle und zuverlässige Verbindungen bereitstellen, welche die Datensicherheit gewährleisten und dynamisch skalierbar sind, um die steigenden Anforderungen an das Unternehmen zu erfüllen.

Die Lösung: Juniper Networks Enterprise@Home

Durch die Kombination aus Mist Wi-Fi und Mist Edge mit Juniper Connected Security können Organisationen das KI-gestützte Enterprise-System zum Nutzer nach Hause zu bringen, und so die erforderliche Sicherheit gewährleisten. Mit Juniper Networks Enterprise@Home lassen sich die Juniper Security-Hardware und Mist Wi-Fi Access Points mit Zero-Touch Provisioning (ZTP) einrichten. So kann ganz ohne Einsatz eines Technikers das entsprechende Managed Networking-Equipment bereitgestellt werden. Die cloudbasierte Managementlösung von Juniper bringt auch für die größten Installationen genügend Skalierbarkeit mit.

Features und Vorteile

- **KI-gestützte Auswertungen für das Benutzererlebnis zu Hause und in Zweigstellen.** Mist ermöglicht den IT-Teams die proaktive Fehlersuche und Problembehebung von überall aus mit Hilfe des virtuellen Assistenten namens Marvis, der proaktiven Erkennung von Auffälligkeiten und Dynamic Packet Capture.
- **Einfachere Installation mit Zero-Touch Provisioning.** Dank ZTP muss kein Techniker mehr vor Ort das Equipment installieren und konfigurieren. Der Benutzer muss lediglich den Mist Access Point und die Juniper Networks SRX Series Services Gateways Firewall an die Stromversorgung anschließen, und schon geht es los – auch zu Hause. Die IT-Abteilung kann das Benutzererlebnis unmittelbar nachvollziehen und dank Cloud-Management auftretende Probleme in den meisten Fällen autonom erkennen und beheben.
- Eliminierung von Overlay VPN-Technologien und Erweiterung des Unternehmensnetzwerks zum Mitarbeiter nach Hause.
- Mit Mist Edge können Unternehmen ihren internen Service Set Identifier (SSID) und die Authentifizierungsservices standortunabhängig auf ihre Remote-Arbeitsplätze übertragen. Durch Installation eines Access Points und den Einsatz von Mist Edge können Organisationen so ihr Netzwerk auf jeden beliebigen Remote-Standort und auf jedes Mitarbeiter-Homeoffice erweitern.
- Einfache Überwachung des Unternehmens-Wi-Fi und Absicherung des Datenverkehrs. Der Einsatz von Mist Wi-Fi zusammen mit Mist Edge stellt eine Erweiterung für den privaten Setup des Benutzers dar, mit der privater und geschäftlicher Datenverkehr effektiv getrennt werden. Aus Sicherheitsperspektive erfolgt damit eine strikte Trennung zwischen geschäftlichen und anderen Benutzern im Haushalt. Lädt ein anderes Haushaltmitglied versehentlich per Phishing eine laterale Bedrohung herunter, bleibt das Unternehmen trotzdem geschützt.
- Mit Juniper Connected Security steigern Sie die Sicherheit, segmentieren den geschäftlichen Datenverkehr und gewährleisten ein qualitativ hochwertiges Erlebnis für ihre Business-Benutzer. Zusätzlich zur Wi-Fi-Anbindung und einem überragenden Benutzererlebnis verfügt Juniper Connected Security über leistungsstarke Tools, die in das Heimnetzwerk des Mitarbeiters integriert werden können. Die SRX Series Services Gateways verfügen über kompakte und robuste Firewalls, mit denen SDWAN, Juniper Advanced Threat Protection und die cloudbasierte Orchestrierung ermöglicht werden. So werden alle Anforderungen an eine Installation optimal erfüllt. Mit Juniper können Organisationen die Heimnetzwerke ihrer Mitarbeiter segmentieren und somit das vom Unternehmen bereitgestellte Equipment strikt von allen persönlichen Geräten im Heimnetzwerk trennen.
- Manchmal ist aufgrund von Compliance-Anforderungen oder der finanziellen Auswirkungen etwaiger Netzwerkausfälle weitere Hardware erforderlich. Juniper sorgt hier für optimale Sicherheit mit seinen SRX Series Firewalls, die für den primären Datenverkehr oder als Ersatzleitung mit herkömmlichen Breitband- bzw. terrestrischen Links verbunden werden können. Optional können die SRX Series Firewalls auch mit Power over Ethernet (PoE) ausgerüstet werden, um zum Beispiel Telefone oder Access Points mit Strom zu versorgen.
- Juniper liefert alle nötigen Tools für die Umsetzung und spart dabei Zeit und Geld. Gleichzeitig werden die Zuverlässigkeit und Sicherheit des Netzwerks weit über das Maß hinaus verbessert, das man normalerweise in privaten Heimnetzwerken vorfindet.
- Halten Sie Bedrohungen in Schach – mit hochentwickelten Security-Services.
- Mehr als je zuvor müssen Security-Geräte heute mit der gestiegenen Netzwerklast zurechtkommen. Die umfänglichen Advanced Threat-Fähigkeiten von Juniper, wie zum Beispiel der Next Generation Firewall Service (NGFW), und das System zum Schutz vor Eindringversuchen (Intrusion Prevention System, IPS) gewährleisten ein sicheres Erlebnis für den Endbenutzer, indem Sicherheitsrichtlinien bedarfsgerecht skaliert werden können und das Netzwerkrisiko miniert wird. Mit den SRX Series Firewalls können die IT-Teams zusätzliche Sicherheitsmaßnahmen vor Ort installieren, um das Netzwerk vor Bedrohungen zu schützen. Diese hochentwickelten Security-Services schützen den Datenverkehr des Unternehmens und sorgen für eine strikte Trennung zwischen beruflichem und privatem Datenverkehr. In manchen Fällen brauchen Unternehmen drahtgebundene Hardware oder nutzen proprietäre Protokolle, die zur ordnungsgemäßen Funktion ein Tunneling benötigen. Das wird durch die robuste Routing-Plattform, die mit der SRX Series erhältliche ist, ermöglicht.
- Schaffen Sie ein dynamisches und flexibles Netzwerk, das sich an neue Anforderungen anpassen kann. Leistungsfähige Lösungen wie SD-WAN und LTE Backup sind optimale Voraussetzungen für eine schnelle und einfache Skalierung, ohne die gesamte Infrastruktur auseinanderzureißen und zu ersetzen. Juniper unterstützt Organisationen bei der Anpassung an neue Muster im Datenverkehr, indem sichergestellt wird, dass jederzeit Konnektivität und Priorisierung für den Business-Datenverkehr bestehen. Alle Maßnahmen hierfür lassen sich mit ZTP einrichten und über die Cloud managen.
- Durch Kombination der Insights-basierten Expertise von Mist mit dem Security- und Datenverkehr-Engineering der SRX Series Firewalls werden Mitarbeiterproduktivität und Sicherheit gesteigert.

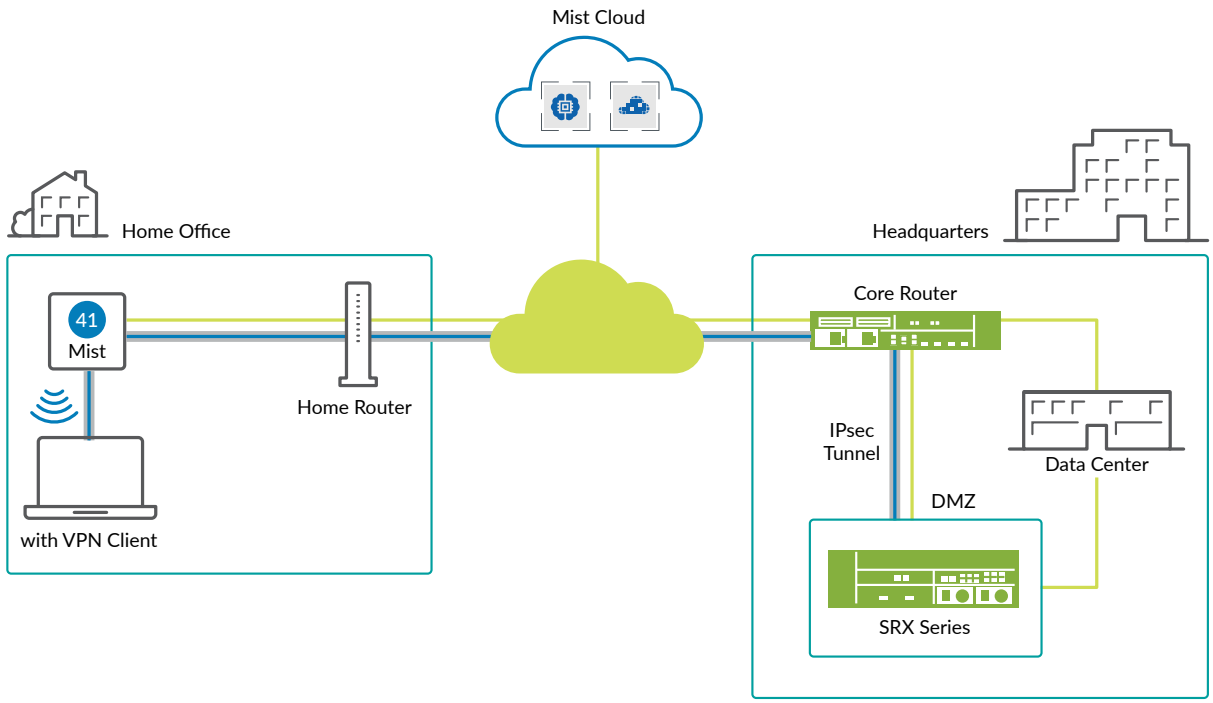

Abbildung 1: Die Mist Wi-Fi-Lösung für Remote-Arbeitsplätze

Lösungskomponenten

Mist Wi-Fi für Remote-Arbeitsplätze

Der Einsatz eines Mist Wi-Fi Access Points in einem Remote-Office oder in der Privatwohnung eines Mitarbeiters hilft Organisationen dabei, KI-gestützte Erkenntnisse zur Steigerung der Produktivität zu nutzen. Mit der KI-Engine namens Marvin können Probleme mit Benutzererlebnis oder Netzwerk proaktiv identifiziert sowie die Ursachen ermittelt und behoben werden. Das geschieht entweder automatisch oder durch Aktionen des Benutzers. Das steigert die Netzwerkeffizienz und ermöglicht den IT-Teams die einfache Fehlersuche im Heimnetz aus der Ferne.

Mist ermöglicht es Organisationen, ihr verteiltes Zugangsnetzwerk abzusichern, inklusive der Mitarbeiter, die von zu Hause aus arbeiten. Und weil die Skalierung so agil erfolgt wie bei einer Microservice-Cloud, sorgt Mist Wi-Fi dafür, dass auch die größten Heimarbeitsumgebungen effizient gemanagt werden können.

Die folgende Tabelle zeigt beispielhaft die Hardware- und Softwarespezifikationen zur Mist Wi-Fi-Lösung für Remote-Arbeitsplätze.

Produktcode	Lösungsbeschreibung
APBRU	Premium Performance Gigabit Wi-Fi Wave 2 Access Point (4x4:4) mit adaptivem Bluetooth Low Energy Array für moderne standortbasierte Services und eingebauter Antenne
	Universeller AP-Halter für T-Schiene und Trockenbaumontage für Indoor Access Points (im Lieferumfang enthalten).

Erweiterung des Unternehmens mit Mist Edge

Die Mist Edge Microservice-Plattform hilft dabei, kostspielige und komplexe Overlay VPN-Technologien zu eliminieren und das Unternehmensnetzwerk in die Privatwohnung des Mitarbeiters zu erweitern. Zusammen mit den Mist Wi-Fi Access Points unterstützt Mist Edge Organisationen dabei, ihre Wireless- und Authentifizierungsservices auf Remote-Standorte weltweit zu erweitern.

Durch das Management der Netzwerkgrenze beim Mitarbeiter maximieren Organisationen die Sicherheit des Datenverkehrs und sorgen gleichzeitig für eine bestmögliche Erlebnisqualität (Quality of Experience, QoE) beim Mitarbeiter. Mist Edge verfügt über die Fähigkeit zum Traffic Shaping. So wird gewährleistet, dass der Datenverkehr rationell gehandhabt wird, der Betrieb unterbrechungsfrei weiterläuft und gleichzeitig der Datenschutz sichergestellt ist.

Produktcode	Lösungsbeschreibung
AP41-WW	Premium Performance Gigabit Wi-Fi Wave 2 Access Point (4x4:4) mit adaptivem Bluetooth Low Energy Array für moderne standortbasierte Services und eingebauter Antenne
APBRU	Universeller AP-Halter für T-Schiene und Trockenbaumontage für Indoor Access Points (im Lieferumfang enthalten)
SUB-ME-1S-1Y	Mist Edge-Abonnement für ein Jahr und einen Access Point (Data Tunneling-Service)

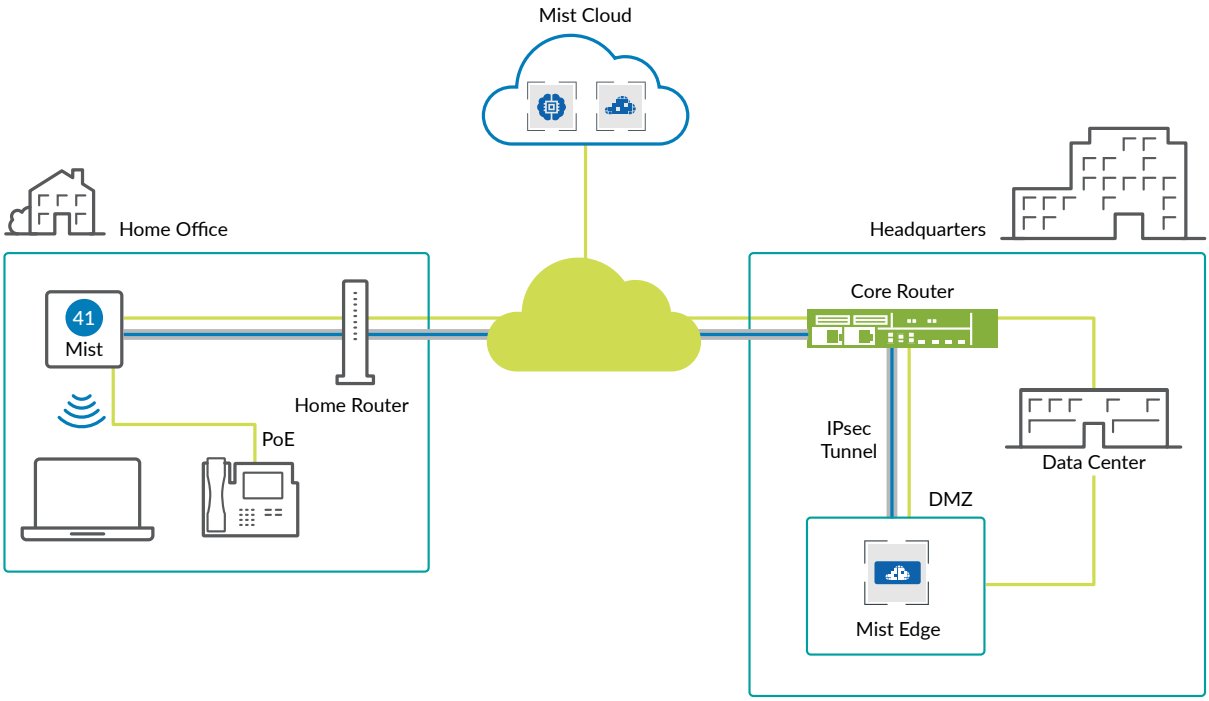

Abbildung 2: Erweitertes Unternehmen mit der Mist Edge-Lösung

Juniper Connected Security mit Mist

Juniper Connected Security mit Mist hilft dabei, das Unternehmens-Wi-Fi zu überwachen und den dienstlichen Datenverkehr abzusichern. Durch die strikte Trennung von privaten und dienstlichen Daten wird ein qualitativ hochwertiges Erlebnis gewährleistet. Zusätzlich zum zuverlässigen Wi-Fi-Benutzererlebnis mit den Mist Access Points verfügt Juniper Connected Security auch über leistungsfähige Tools, die im Heimnetzwerk des Mitarbeiters eingesetzt werden können. Die kompakten und robusten SRX Series Firewalls ermöglichen SD-WAN, Juniper Advanced Threat Protection, cloudbasierte Orchestrierung, und sogar ein LTE-Backup, um alle Einsatzanforderungen abzudecken. Optional kann auch Mist Edge hinzugefügt werden, um das organisatorische SSID und die Authentifizierungsservices auf die externen Standorte zu erweitern.

Juniper ermöglicht Organisationen die Segmentierung der Heimnetzwerke ihrer Mitarbeiter. Dabei wird das gesamte dienstlich zur Verfügung gestellte Equipment strikt von privaten Geräten getrennt. Gleichzeitig schafft die Organisation mit Hilfe von Traffic Shaping ein qualitativ hochwertiges Benutzererlebnis. Außerdem wird sichergestellt, dass der Datenverkehr rationell gehandhabt wird. Damit wird ein unterbrechungsfreier Geschäftsbetrieb ebenso gewährleistet wie der Datenschutz.

Die folgende Tabelle enthält Beispielspezifikationen für Hardware und Software für die Lösung Juniper Connected Security mit Mist.

Produktcode	Lösungsbeschreibung
AP41-WW	Premium Performance Gigabit Wi-Fi Wave 2 Access Point (4x4:4) mit adaptivem Bluetooth Low Energy Array für moderne standortbasierte Services und eingebauter Antenne
APBRU	Universeller AP-Halter für T-Schiene und Trockenbaumontage für Indoor Access Points (im Lieferumfang enthalten
SRX340-SYS-JB	SRX340 Services Gateway mit Hardware (16GbE, 4x MPIM Slots, 4GB RAM, 8GB Flash, Stromversorgung, Kabel und RMK) und Junos Betriebssystem-Softwarebasis (Firewall, NAT, IPSec, Routing, MPLS und Switching).

Juniper deckt sämtliche Einsatzanforderungen ab und gewährleistet so einen unterbrechungsfreien Geschäftsbetrieb, Sicherheit und Datenschutz. Wir von Juniper Networks unterstützen unsere Kunden dabei, heute und in Zukunft ein sicheres und zuverlässiges Benutzererlebnis zu garantieren.

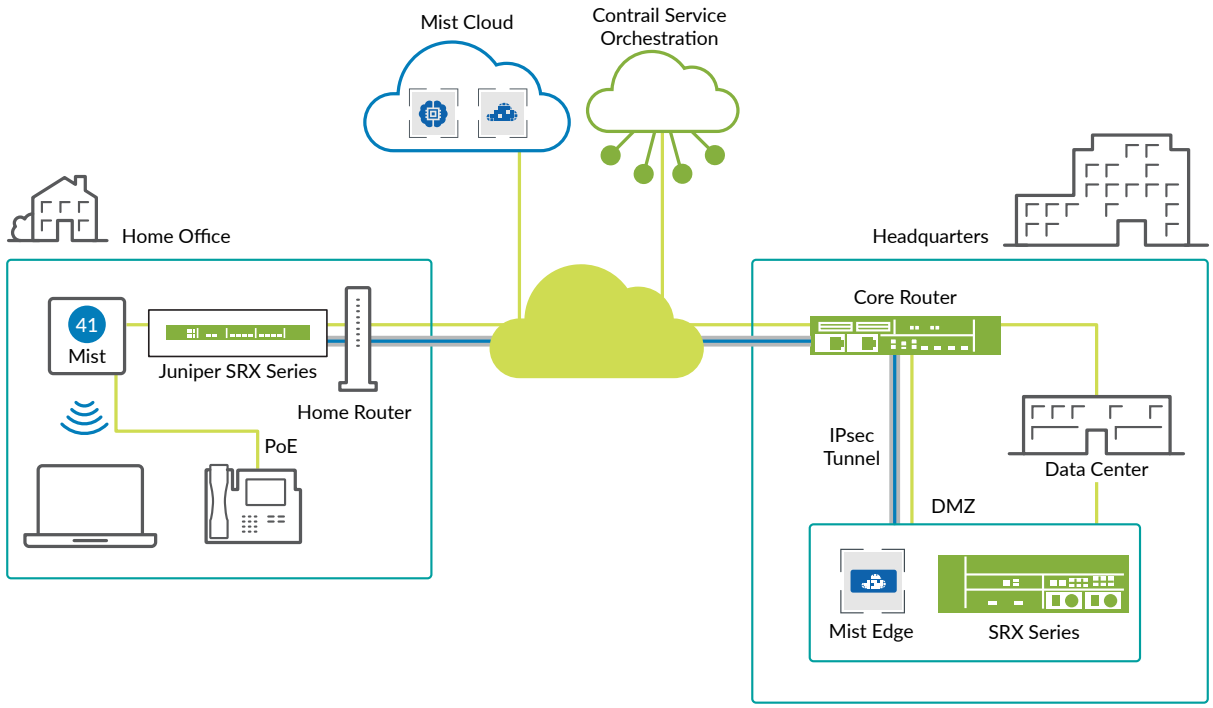

Abbildung 3: Juniper Connected Security mit Mist

Fazit – So sind Remote-Arbeitsplätze überall sicher

Juniper steht bereit, damit Organisationen Einblicke in ihr Remotebenutzer-Erlebnis erhalten und dieses Erlebnis mit Automatisierung verbessern und absichern können. Mit Mist, Juniper Connected Security, den SRX Series Firewalls und Juniper Advanced Threat Protection bietet Juniper die erforderlichen Tools für die Unterstützung von Remote-Arbeitsplätzen, egal, wo diese sich befinden. Mit den leistungsfähigen Lösungen sparen Organisationen Zeit und Geld und steigern zugleich die Zuverlässigkeit und Sicherheit des Netzwerks weit über das Maß hinaus, das mit herkömmlichen Wi-Fi-Lösungen im typischen Heimnetzwerk möglich ist..

Die nächsten Schritte

Für weitere Informationen wenden Sie sich bitte an Ihren Juniper Networks-Vertreter.

Über Juniper Networks

Juniper Networks sorgt mit Produkten, Lösungen und Services, die die Welt vernetzen, für mehr Einfachheit im Netzwerk. Mit speziell entwickelten Innovationen beseitigen wir die Barrieren und Komplexitäten beim Networking im Zeitalter der Cloud und lösen so die schwierigsten Herausforderungen unserer Kunden und Partner – Tag für Tag. Wir bei Juniper Networks glauben, dass das Netzwerk eine Ressource für den Austausch von Wissen und menschlichem Fortschritt ist, die die Welt verändert. Unser Anspruch ist es, völlig neue Wege zu finden, um automatisierte, skalierbare und sichere Netzwerke zu schaffen, die mit der Geschäftswelt Schritt halten können.

Über Aeroaccess

Aeroaccess wurde 2008 mit dem Ziel gegründet, als mittelständisches Systemhaus Anwender mit Mobiler Indoor und Outdoor Kommunikation, auch weltweit, zu versorgen. Durch die Spezialisierung auf neue und zukunftsorientierte Technologien fordert der Kunde von uns verstärkt Full-Service Modelle. Dem entsprechen wir durch unsere Angebotspalette, die von der Planung, über weltweite Logistik, die Implementierung, das Management bis zu Vor-Ort Wartung und Betrieb, auch als Solution-Provider oder Leasingpartner, reicht. Insgesamt werden von aeroaccess derzeit mehr als 300.000 User in mehr als 170 Ländern bei der Arbeit mit mobilen Lösungen unterstützt.

In der zweiten Generation, verbunden mit dem Umzug nach München / Unterföhring, wird nun der Ausbau von durchgreifenden Endanwendungen verstärkt vorangetrieben, um unseren Kunden für die Betreiber- aber auch für die Anwender-Ebene weitere Ausbaustufen bei gleichzeitiger personeller Entlastung anbieten zu können.

aeroaccess mobile communication

Aeroaccess GmbH
Feringastr. 13
-D- 85774 Unterföhring

Mail: info@aeroaccess.de
Tel: 089 700 743 540

JUNIPER NETWORKS | Mist A Juniper Company

nuvias

3510666-001-EN Apr 2020