DER KI-GESTÜTZTE CAMPUS

Künstliche Intelligenz für die Campus-Netzwerke des kommenden Jahrzehnts

Whitepaper

INHALTSVERZEICHNIS

KURZFASSUNG

In den nächsten zehn Jahren werden voraussichtlich die Verbesserung der Benutzererfahrung und die Simplifizierung des IT-Betriebs im Mittelpunkt des Netzwerks stehen. Herkömmliche kabelgebundene und WLAN-Lösungen sind oft nicht ausreichend skalierbar, zuverlässig, sicher, leistungsstark oder ausreichend flexibel, um den heutigen Herausforderungen und vielfältigen Unternehmensanforderungen gerecht zu werden.

Im Gegensatz dazu nutzt der KI-gestützte Campus das Potenzial der künstlichen Intelligenz (KI) im Zeitalter von Cloud, mobiler Arbeit und IoT. Die Campus-Lösung von Juniper kombiniert ein robustes Hardwareportfolio mit der Leistungsfähigkeit von Mist AI™, um den Netzwerkbetrieb zu straffen, die Benutzererfahrung zu verbessern und IT-Teams in die Lage zu versetzen, sich auf strategische Initiativen zu konzentrieren. In diesem Whitepaper besprechen wir die Komponenten eines umfassenden, KI-gestützten Campus-Netzwerks mit Mist AI.

Einführung

Unternehmensnetzwerke machen derzeit einen massiven Wandel durch, um den wachsenden Anforderungen von Cloud-fähigen Netzwerken sowie einer Vielzahl an mobilen und IoT-Geräten gerecht zu werden. Allerdings steigt mit der Anzahl der Geräte auch die Komplexität. Cloud-basierte Anwendungen ermöglichen neue Geschäftsmodelle, steigern die geschäftliche Agilität und unterstützen die Nutzung von Schlüsseltechnologien wie Unified Communications, Videokonferenzen und andere latenzempfindliche Anwendungen. Darüber hinaus können die technologischen Fortschritte und die weit verbreitete Einführung von maschinellem Lernen (ML) und KI die Abläufe und Erfahrungen sowohl für IT-Teams als auch für Endbenutzer erheblich verbessern.

Netzwerkarchitekten gestalten ihre Netzwerke neu, um den heutigen Geschäftsanforderungen Cloud-fähiger Anwendungen an Daten, Sprache und Video gerecht zu werden, indem sie offene Standards und softwaregestützte Managementplattformen nutzen und so die Betriebskosten senken. Dabei geht es letztendlich um den Einsatz einfacherer Automatisierungs-, Telemetrie- und KI-Funktionen zum Aufbau von Netzwerken, die den Ansprüchen der nächsten zehn Jahre gewachsen sind.

Das KI-gestützte Campus-Netzwerk von Juniper

Das Portfolio an Cloud-Services, Software- und Hardwareprodukten von Juniper Networks bietet End-to-End-Lösungen für Campus-Netzwerke, die sich über die Bereiche WAN, LAN, WLAN und Sicherheit erstrecken. Dabei werden offene Standards wie Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) unterstützt, um eine simplifizierte Architektur, Skalierbarkeit und höhere Leistung zu erreichen.

Der KI-gestützte Campus von Juniper besteht aus den folgenden Komponenten:

- Eine moderne, auf Microservices basierte AIOps-Plattform für die Cloud
- KI-gestütztes WLAN und kabelgebundenes Switching
- Campus-Fabrics mit EVPN-VXLAN
- Cloud-fähige Campus-Ethernet-Switches
- Access Points der Enterprise-Klasse für WLAN, Bluetooth LE und IoT
- Juniper Connected Security und Netzwerksegmentierung
- Betriebssystem Junos®
- Junos Telemetry

Eine moderne, auf Microservices basierte AIOps-Plattform für die Cloud

Die Juniper® Mist-Cloud-Architektur basiert auf Microservices, die beispiellose Agilität, Skalierbarkeit und Ausfallsicherheit bieten. Cloud-Services können bei Bedarf elastisch skaliert werden und machen die Kosten und die Komplexität monolitischer Hardware obsolet. Aktuelle Erweiterungen und Bugfixes können nahezu wöchentlich und ohne Unterbrechung des Netzwerkbetriebs installiert werden. Die Plattform bietet hundertprozentige Programmierbarkeit über offene APIs. Das ermöglicht einen komplett automatisierten Betrieb und eine nahtlose Integration in ergänzende Drittanbieter-Produkte. Die Juniper Mist Cloud-Architektur bietet einen innovativen Ansatz für Unternehmensnetzwerke, bei dem KI, ML und Data Science mit der neuesten Microservices-Technologie kombiniert werden, um eine einzigartige Lösung bereitzustellen.

KI-gestütztes WLAN und kabelgebundenes Switching

Juniper setzt Mist AI in Campus-Netzwerken ein, um die Benutzererfahrung zu optimieren und den IT-Betrieb über eine einheitliche kabelgebundene und drahtlose Lösung zu simplifizieren. Herkömmliche Lösungen sind mehr als 15 Jahre alt und nutzen monolithisch aufgebauten Quellcode, der nur mit großem Ressourcenaufwand skalierbar, fehleranfällig und schwer zu verwalten ist. Damit sind diese Lösungen schlicht nicht mehr zeitgemäß, da die Qualität einer Netzwerkinfrastruktur heutzutage an der Benutzererfahrung – und nicht mehr an der Verfügbarkeit – gemessen wird. Was ist das Geheimnis von Juniper?

Juniper Wi-Fi Assurance ersetzt manuelle Schritte zur Fehlerbehebung durch automatisierte, drahtlose Abläufe. Dadurch wird das WLAN vorhersehbar, zuverlässig und messbar, mit transparenten Servicelevels für die Benutzer. Die Erkennung von Anomalien automatisiert Auslöser, um Pakete zum Abgleich von Ereignissen zu erfassen und Netzwerkintelligenz mit Radio Resource Management (RRM) auf Client-Ebene aufzubauen, um einen beispiellosen Einblick in die Benutzererfahrung des drahtlosen Netzwerks zu erhalten.

Juniper Wired Assurance (siehe Abbildung 1) weitet KI-gestützte Automatisierung auf kabelgebundene Geräte aus.

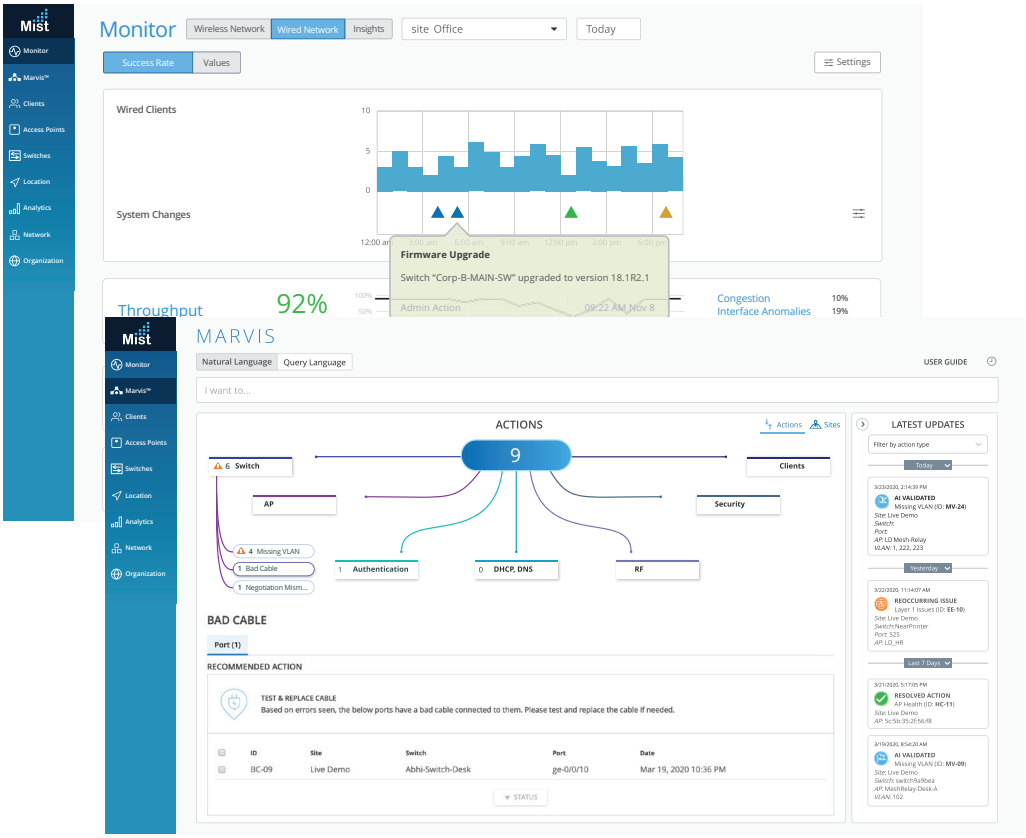

Abbildung 1: Wired Assurance und der virtuelle Netzwerkassistent Marvis

Die Lösung nutzt die reichhaltigen Telemetriedaten, die das Betriebssystem Junos auf den Ethernet-Switches der EX-Serie von Juniper Networks® erfasst, um die Betriebsabläufe zu simplifizieren, die mittlere Reparaturzeit (MTTR) zu verkürzen und eine bessere Übersicht über die Endbenutzererfahrung mit IoT-Geräten, Servern, Druckern usw. zu bieten. Juniper Wired Assurance simplifiziert alle Aspekte der Switches der EX-Serie – vom Onboarding über die Bereitstellung bis hin zur Verwaltung über die Juniper Mist Cloud-Architektur.

Der virtuelle Netzwerkassistent Marvis (Abbildung 1) wurde mit Mist AI speziell für WLAN-, LAN- und WAN-Netzwerke in Unternehmen entwickelt. Natürliche Sprachverarbeitung gestattet es den Benutzern, direkt mit der Mist AI-Engine zu interagieren: Der Netzwerkbetrieb wird so von der reaktiven Fehlersuche zur proaktiven Problembehebung mithilfe selbstgesteuerter Aktionen transformiert. Marvis erhöht die IT-Effizienz, minimiert die Anzahl von Support-Tickets und reduziert die Dauer bis zur Lösung. Vor dem Hintergrund der rasant zunehmenden Nutzung von KI im IT-Betrieb (AIOps) unterstützt Marvis Unternehmen bei der effizienten und bedarfsgerechten Skalierung ihrer IT-Prozesse.

Campus-Fabrics

Die steigende Anzahl an IoT-Geräten in Campus-Umgebungen kann nur mit Netzwerken unterstützt werden, die schnell und ohne Anstieg der Komplexität skaliert werden. Da viele dieser Geräte nur über begrenzte Netzwerkfähigkeiten verfügen, benötigen sie eine gebäude- oder campusübergreifende L2-Bindung. Das beeinträchtigt die Optionen für die Netzwerksegmentierung und führt zu Schleifen, langsamer Konvergenz bei Fehlern und Sicherheitsproblemen aufgrund von Data Plane Flooding. Das Sicherheitsproblem wurde traditionell durch proprietäre private VLANs gelöst, doch die anderen Probleme wie Schleifen und langsame Konvergenz blieben bei L2-Netzwerken bestehen. Dieser Ansatz ist ineffizient und mühsam in Bezug auf die Verwaltung – ineffizient aufgrund des übermäßigen Verbrauchs von Netzwerkbandbreite und mühsam in der Verwaltung, da VLANs auf neue Netzwerk-Ports erweitert werden müssen.

EVPN-VXLAN

Die KI-gestützte Campus-Architektur entkoppelt das Overlay-Netzwerk vom Underlay mit Technologien wie Open-Standard-Ethernet-VPN (EVPN) und Virtual Extensible LAN (VXLAN). Dies sorgt für ein Netzwerk ohne Schleifen mit schnellerer Konvergenz und entspricht den Anforderungen moderner Unternehmensnetzwerke, da Netzwerkadministratoren logische L2-Netzwerke über verschiedene L3-Netzwerke hinweg erstellen können. Ein EVPN-VXLAN unterstützt auch die Mikrosegmentierung, indem es den Datenverkehr zwischen IoT-Geräten trennt und so zusätzliche Sicherheit bietet. Juniper unterstützt die folgenden validierten EVPN-VXLAN-Campus-Fabrics:

- **EVPN-Multihoming (auf zusammengelegten Core- oder Verteilungsschichten)**: EVPN-Multihoming an der Netzwerkverteilung ermöglicht es Access-Switches, LAGs über ein Gerätepaar in der Verteilung zu bilden. Dadurch wird das Spanning Tree Protocol (STP) in den Netzwerken auf dem Campus überflüssig, indem Multihoming-Funktionen von der Zugangsebene bis zur Verteilungsschicht zur Verfügung stehen. Auf diese Weise lassen sich auch die Verteilungs- und Core-Schichten zusammenlegen.
- **Core und Distribution von Campus-Fabrics**: Ein Paar miteinander verbundener Core- oder Distribution-Switches der EX-Serie bietet L2 EVPN- und L3 VXLAN-Gateway-Unterstützung. Das IP Clos-Netzwerk zwischen der Verteilungs- und der Core-Schicht stellt zwei Modi bereit: zentral oder über den Edge geroutetes Bridging-Overlay.
- **Campus Fabric IP Clos:** Die Campus Fabric IP Clos-Architektur verlagert die Funktionalität des VXLAN L2-Gateways auf die Zugangsschicht, was eine Mikrosegmentierung mit standardbasierten, gruppenbasierten Richtlinien ermöglicht.

Mit einer End-to-End-EVPN-VXLAN-Architektur können Sie Ihren Campus und Ihr Datencenter als eine einzige IP-Fabric verwalten, wobei die OTT-Richtlinien und -Kontrolle durch Juniper erfolgen. Dies simplifiziert auch die Durchsetzung von Richtlinien durch gruppenbasierte Richtlinien im gesamten Netzwerk. In einem Clos-Netzwerk oder einer IP-Fabric können beliebig viele Switches miteinander verbunden und EVPN-VLAN genutzt werden, um die Fabric zu erweitern, mehrere Unternehmensgebäude zu verbinden und L2 mit VXLAN über das Netzwerk auszudehnen.

Weitere Informationen finden Sie unter www.juniper.net/assets/de/de/local/pdf/solutionbriefs/3510643-en.pdf.

Neben EVPN-VXLAN-basierten Architekturen unterstützt Juniper auch die Virtual Chassis-Technologie, mit der bis zu 10 miteinander verbundene Switches als ein einziges, logisches Gerät mit einer IP-Adresse betrieben werden können. Virtual Chassis-Technologie ermöglicht es Unternehmen, die physische Topologie von logischen Gruppierungen von Endgeräten zu trennen und so eine effiziente Ressourcennutzung zu ermöglichen.

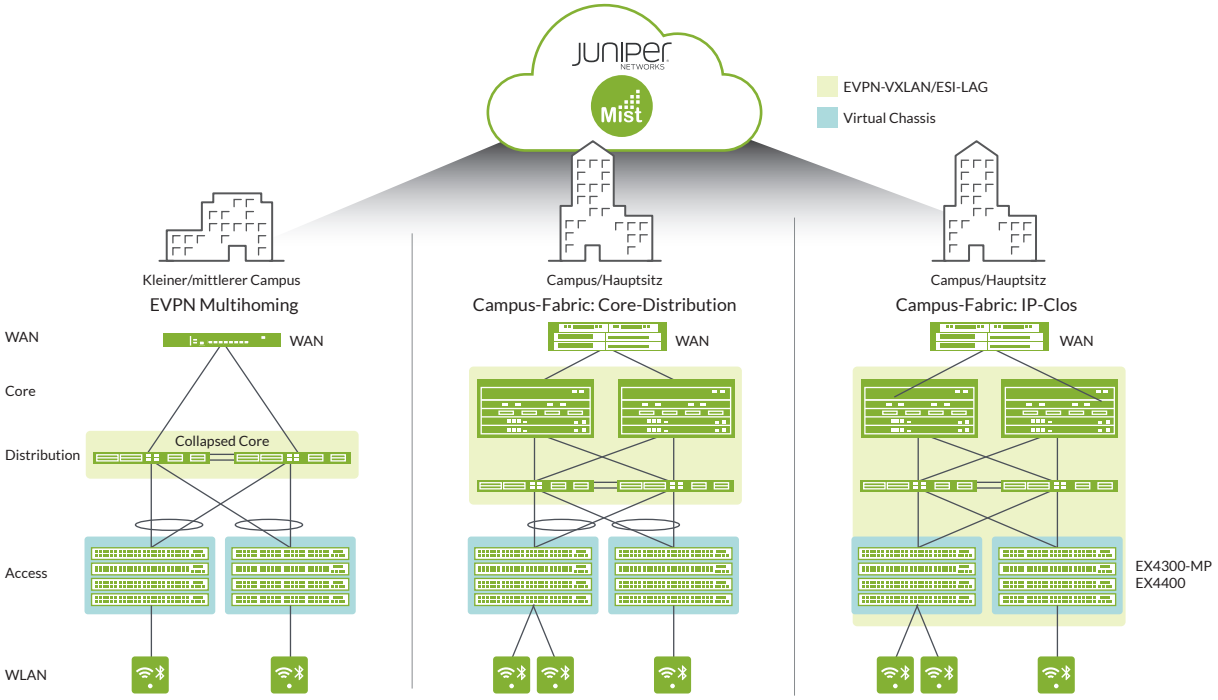

Abbildung 2: Campus-Fabrics mit Virtual Chassis- und EVPN-VXLAN-basierten Architekturen

Cloud-fähige Campus-Ethernet-Switches

Juniper bietet ein KI-gestütztes, programmierbares und offenes Portfolio an Access- und Core-/Distribution-Switches für Campus-Netzwerke der Enterprise-Klasse. Die Access-Switches sind Cloud-fähig und unterstützen Juniper Wired Assurance, wodurch AIOps für Zugangsebenen-Switching möglich wird. Die Switches erfüllen eine Reihe von Campus-Anforderungen, wie z. B.:

- Cloud-fähig und von der Juniper Mist Cloud-Architektur verwaltet
- Multigigabit-Unterstützung
- Media Access Control Security (MACsec) AES256
- Power over Ethernet (PoE/PoE+/PoE++)
- Skalierbare Fabric-Architekturen (Virtual Chassis und EVPN-VXLAN)
- Anbieterübergreifender Support
- Standardbasierte Mikrosegmentierung mit gruppenbasierten Richtlinien (GBP)
- Ablaufbasierte Telemetrie

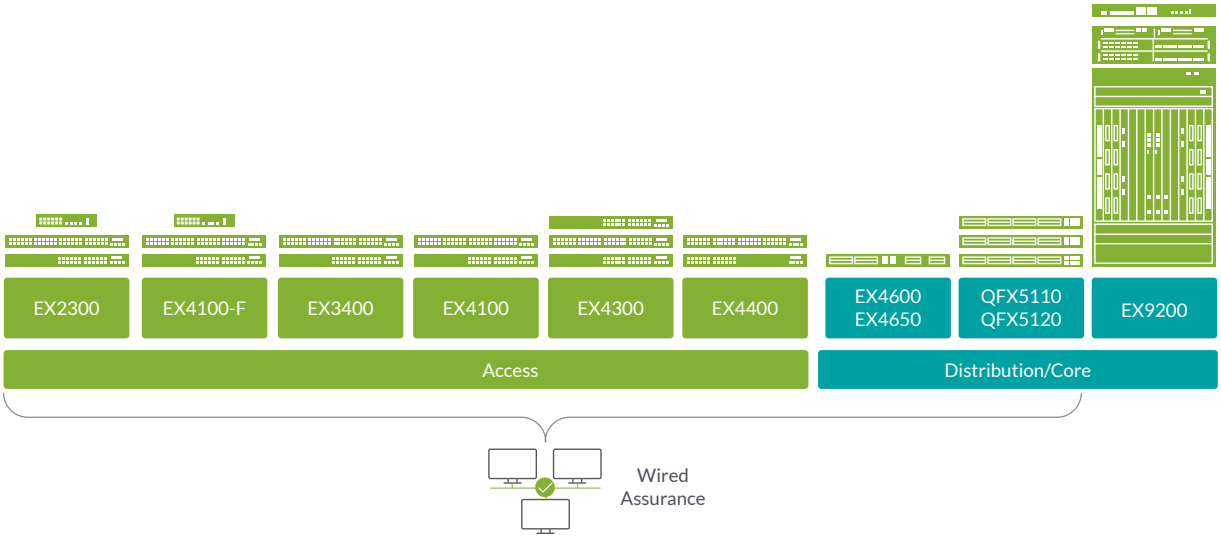

Abbildung 3: Das Campus-Portfolio mit Switches der EX- und QFX-Serie

Bereitstellung einer KI-gestützten Campus-Fabric

Die manuelle Konfiguration von Campus-Fabrics kann zu Inkonsistenzen und vermeidbaren Fehlern bei der Bereitstellung führen. Juniper löst diesen operativen Aufwand, indem EVPN-VXLAN-Campus-Fabrics einfach über die Juniper Mist Cloud verwaltet werden können. Genauer gesagt, können Administratoren eine Topologie auswählen (EVPN Multihoming, Distribution-Core oder IP CLOS) und die Software den Rest erledigen lassen (siehe Abbildung 4). Dieser KI-gestützte Ansatz vereinheitlicht das Management der LAN-, WLAN- und WAN-Umgebungen auf dem Campus und in Zweigstellen und sorgt für eine hervorragende Benutzererfahrung in kabelgebundenen und drahtlosen Netzwerken.

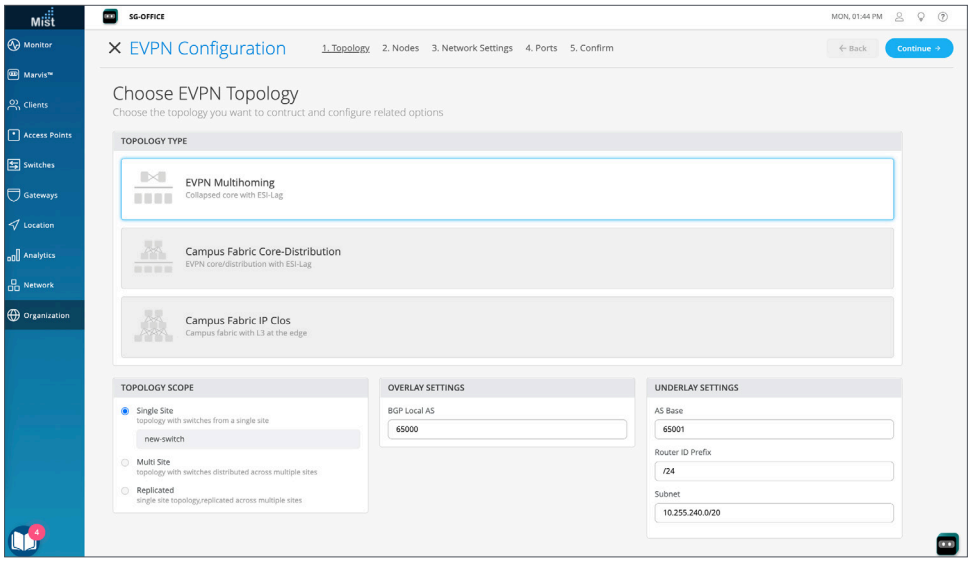

Abbildung 4: Entwurf einer Juniper Wired Assurance-Campus-Fabric

* Anfänglich wird EVPN-Multihoming unterstützt, die Unterstützung weiterer Architekturen ist für zukünftige Versionen vorgesehen.

Betrieb einer KI-gesteuerten Campus-Fabric

Juniper Wired Assurance übernimmt, konfiguriert und verwaltet die Cloud-verwalteten Ethernet-Switches der EX-Series und diagnostiziert und behebt etwaige Probleme. Der Cloud-basierte Service bietet KI-gestützte Automatisierung und Servicelevels, um eine bessere Benutzererfahrung für verbundene Geräte zu gewährleisten. Juniper Wired Assurance nutzt die umfangreichen Telemetriedaten des Junos® Betriebssystems für Switches, um die Betriebsabläufe zu simplifizieren, die mittlere Reparaturzeit zu verkürzen und die Visibilität zu verbessern. Die wichtigsten Merkmale für den Day 0- bis Day 2-Betrieb:

- **Day 0-Betrieb:** Nahtlose Integration von Switches durch Übernahme eines Greenfield-Switches oder Übernahme eines Brownfield-Switches mit einem einzigen Aktivierungscode für echte Plug-and-Play-Simplizität.
- **Day 1-Betrieb:** Implementierung eines vorlagenbasierten Konfigurationsmodells für Massen-Roll-outs von traditionellen und Campus-Fabric-Bereitstellungen bei gleichzeitiger Beibehaltung der Flexibilität und Kontrolle, die für die Anwendung benutzerdefinierter standort- oder switch-spezifischer Attribute erforderlich ist. Automatisierte Bereitstellung von Ports über dynamische Port-Profile.
- **Day 2-Betrieb:** Nutzung der KI in Juniper Wired Assurance, um Servicelevel-Erwartungen wie Durchsatz, erfolgreiche Verbindungen und Switch-Integrität mit wichtigen Metriken vor und nach der Verbindung zu erfüllen (siehe Abbildung 5). Zusätzlich erkennen selbststeuernde Funktionen in Marvis Actions Schleifen, fügen fehlende VLANs ein, korrigieren falsch konfigurierte Ports und identifizieren defekte Kabel, Port-Flapping sowie wiederholt ausfallende Clients (siehe Abbildung 6). Zudem können Software-Upgrades ganz einfach über die Juniper Mist Cloud vorgenommen werden.

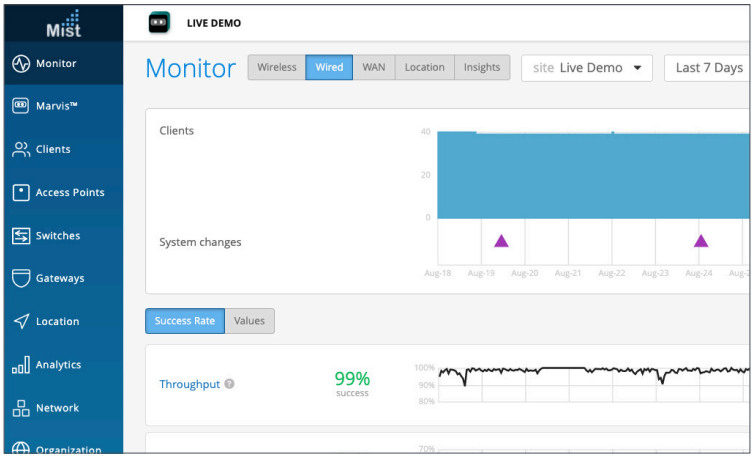

Abbildung 5: Juniper Wired Assurance SLEs (Service Level Expectations)

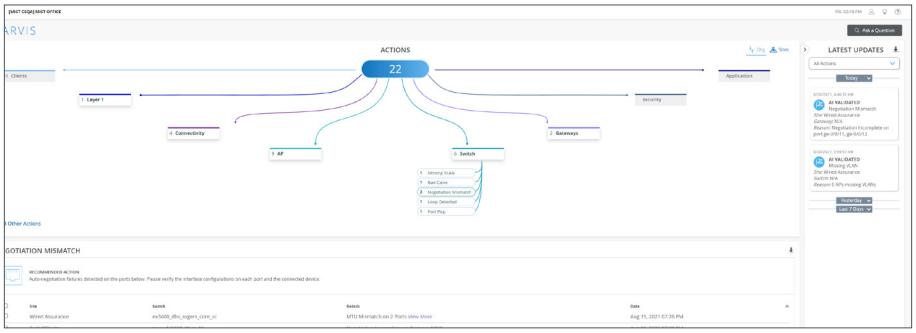

Abbildung 6: Marvis Actions für kabelgebundene Switches

Weitere Informationen zu Juniper Wired Assurance

WLAN-Access Points der Enterprise-Klasse

Juniper gehört zu den Vorreitern, wenn es um die Konvergenz von WLAN, Bluetooth Low Energy (BLE) und IoT mit Access Points der Enterprise-Klasse geht. Diese Produkte nutzen maschinelles Lernen und den Abgleich von Ereignissen, um Funktionen zur Datenerfassung, Analyse und Durchsetzung von Richtlinien bereitzustellen. Die leistungsstarken Access Points der Serien AP 43 und AP 45 von Juniper verfügen über ein patentiertes dynamisches vBLE-Antennen-Array mit 16 Elementen und bieten Ortungsdienste mit branchenführender Präzision und Skalierbarkeit. Juniper Access Points sind speziell dafür ausgelegt, Metadaten für mehr als 150 Zustände zu sammeln, die in die Mist AI-Engine einfließen.

Funktion	AP45	AP34	AP43	AP63	AP33	AP32	AP12
WLAN-Standard	Wi-Fi 6E 802.11ax (Wi-Fi 6) 4x4: 4SS	Wi-Fi 6E 802.11ax (Wi-Fi 6) 2x2: 2SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 5 GHz: 4x4: 4SS 2,4 GHz: 2x2: 2SS	802.11ax (Wi-Fi 6) 5 GHz: 4x4: 4SS 2,4 GHz: 2x2: 2SS	802.11ax (Wi-Fi 6) 2x2: 2SS
Antennenoptionen	Intern/extern	Intern	Intern/extern	Intern/extern	Intern	Intern/extern	Intern
Virtual BLE	✓	–	✓	✓	✓	–	–

Juniper Connected Security

Im Jahr 2020 berichtete ZDNet, dass die Anzahl der an das FBI gemeldeten Cyberangriffe um 69 % pro Jahr steigt. Vor diesem Hintergrund benötigt selbst die kleinste Organisation eine effektive Cybersicherheitsstrategie für ihr Netzwerk. Dazu muss zunächst ein Gesamtbild der zu schützenden Infrastruktur und der drohenden Gefahren erstellt werden, das keine großen Lücken aufweisen darf. Bislang ist es der Industrie für Netzwerksicherheit allerdings trotz der zahlreichen Innovationen der letzten 10 Jahre nicht gelungen, die Anzahl der erfolgreichen Cyberangriffe zu reduzieren. Unbestritten ist jedoch, dass Sicherheitsmaßnahmen in Campus-Netzwerken an jedem Verbindungspunkt installiert werden müssen. Auf diese Weise kann das Netzwerk mithlfe von KI eine erfolgreiche Verteidigung aufbauen und sich schneller und erfolgreicher schützen.

Juniper® Connected Security dehnt Visibilität, Threat Intelligence und Richtliniendurchsetzung auf jeden Verbindungspunkt im Netzwerk aus, vom Client bis zur Workload. Durch die Nutzung aller Verbindungspunkte zur Erstellung einer umfassenden Übersicht über sämtliche Benutzer und Komponenten eines Campus-Netzwerks und den Einsatz von KI zur Risikobewertung in Echtzeit können Netzwerksicherheitsteams das Risiko reduzieren und ihr Campus-Netzwerk schützen, ohne den Zugriff auf die Campus-Ressourcen zu beeinträchtigen.

Daten: Die Datensicherheit muss zwei Bereiche schützen: Die Daten im Datencenter und den Zugriff auf diese Daten am Netzwerk-Edge. Daher dienen sämtliche Komponenten einer Zero-Trust-Architektur dem Schutz von Daten und Datenzugriffen. Das erfordert die Verschlüsselung der Daten, sowohl zur Übertragung als auch zur Speicherung, und sichere Verbindungen.

- Secure Vector Routing ermöglicht eine auf Routing-Vektoren basierte Segmentierung und erschwert Angreifern damit das Abfangen von Daten während der Übertragung erheblich.
- Secure Connect bietet Zero Trust Network Access (ZTNA, Zero-Trust-Netzwerkzugang) für alle Netzwerkverbindungen, unabhängig vom Ausgangspunkt, und bettet sie in einen privaten Tunnel ein.
- Absichtsbasierte Sicherheitsmaßnahmen nutzen die Automatisierungsfunktionen von Junos zur automatisierten Durchsetzung von Sicherheitsrichtlinien in öffentlichen Clouds. Beispielsweise werden alle Daten in neu erstellten Buckets in Amazon S3 verschlüsselt gespeichert und auch ohne manuell konfigurierte Regeln sind nur autorisierte Zugriffe möglich.

Das Netzwerk

Alle Datenpakete in einem Netzwerk sollten legitim sein, weder Exploits noch Malware enthalten und für den Transfer von Punkt A zu Punkt B autorisiert sein. Um dies zu gewährleisten, muss der Netzwerkverkehr inspiziert und nach schädlichen Inhalten durchsucht werden.

Next-Generation Firewalls (NGFW) wurden für genau diesen Zweck entwickelt. Normalerweise werden sowohl Paket-Header und -Inhalte als auch Paketgruppen mit Signaturen verglichen, um schädlichen Datenverkehr zu erkennen. Mithilfe von KI lässt sich zudem ermitteln, ob noch unbekannte Dateien, Systemverhalten und Verkehrsmuster auf einen Angriffsversuch hindeuten.

Die Services-Gateways der SRX-Series von Juniper Networks bieten Visibilität im und Kontrolle über den Netzwerkverkehr sowie zusätzliche Sicherheitsfunktionen zur Bekämpfung bekannter und neuer Bedrohungen mit KI-basierten Sicherheitsservices wie:

- Bedrohungsprävention zur Abwehr neuer Malware: Juniper ATP-Cloud nutzt maschinelles Lernen, um neue Dateien und ihr Laufzeitverhalten rasch zu beurteilen und zu ermitteln, ob sie Malware oder Grayware enthalten.
- Visibilität und Kontrolle ohne Entschlüsselung: ATP Cloud beurteilt zudem das mit verschlüsseltem Netzwerkverkehr und verbundenen IoT- und anderen Geräten einhergehende Risiko. Dies geschieht anhand wichtiger Komponenten der genutzten Zertifikate und des Datenverkehrsverhaltens.

Menschen/Benutzer

Campus-Benutzer greifen auf interne und über das Internet erreichbare Ressourcen zu. Gleichzeitig gelten Benutzer jedoch auch als potenzielle Angriffsvektoren, weswegen sie und ihre Zugriffsanforderungen authentifiziert und kontrolliert werden müssen, um das Risiko zu minimieren.

Die Gateways der SRX-Series unterstützen benutzerbasierte Richtlinien und damit eine nuancierte Zugangskontrolle für interne und externe Ressourcen. Sie sind mit allen gängigen Identitätsmanagementsystemen kompatibel und unterstützen die Durchsetzung konsistenter Zugriffskontrollen und Sicherheitsrichtlinien – unabhängig davon, wo ein Benutzer Zugriff verlangt. Darüber hinaus prüft ATP Cloud, ob ein Benutzerkonto geknackt wurde, passt die Sicherheitsrichtlinien und/oder das VLAN entsprechend an und aktiviert gegebenenfalls zusätzliche Authentifizierungsebenen.

Workloads

Workloads sind – mitunter vergängliche – Komponenten einer Anwendung. Der Schutz von Workloads vor Anwendungs-Exploits und die Trennung verschiedener Workloads und Anwendungen durch Segmentierung sind gute Methoden, um die wertvollsten Ressourcen in einem Datencenter vor Angreifern zu schützen, die sich dort bereits Zugang verschafft haben.

- Cloud Workload Protection schützt Anwendungs-Workloads in jeder Cloud- und lokalen Umgebung automatisch vor Zero-Day-Exploits, sobald sie erfolgen. Der Schutz stellt sicher, dass Produktionsanwendungen stets über ein Sicherheitsnetz gegen auf Schwachstellen abzielende Angriffe verfügen, damit geschäftskritische Services weiterhin zugänglich und ausfallsicher sind. Cloud Workload Protection wendet selbstständig (und ohne manuelle Eingriffe) Mikrosegmentierung an, um individuelle Datenbanken, Datensammler, laufende Anwendungen und alle anderen Ressourcen zu schützen.
- Die Juniper Networks cSRX Container Firewall schützt Anwendungen mit einer containerisierten Firewall, die den Datenverkehr von und zu einer einzelnen Anwendung segmentiert und kontrolliert.

Geräte

Die Erstellung einer Übersicht über alle mit einem Campus-Netzwerk verbundenen Geräte ist nicht trivial, da es sich um Benutzer- oder IoT-Geräte und gelegentlich sogar Server handeln kann. IoT-Geräte können sich überall auf dem Campus befinden und sehr vielfältige Funktionen haben, von Verkaufsautomaten über Kaffeemaschinen bis hin zu Druckern. Im Gegensatz zu Benutzergeräten sind nicht alle IoT-Geräte mit Endpunkt-Agenten ausgestattet. Daher lässt sich oft nicht eindeutig ermitteln, welches Maß an Netzwerkzugang sie erhalten sollten und was ihr aktueller Sicherheitsstatus ist.

- ATP Cloud fungiert als Junipers Threat-Intelligence-Zentrale für das Netzwerk, unter anderem zur Beurteilung des mit verbundenen Geräten einhergehenden Risikos, zur Identifizierung verschiedener Gerätetypen (auch für IoT-Geräte) und zur Koordinierung geeigneter Maßnahmen, wenn ein mit dem Netzwerk verbundenes Gerät kompromittiert wird.

Die folgenden Funktionen von ATP Cloud tragen zum Schutz von Geräten in einem Zero-Trust-Netzwerk bei:

Risiko-Profiling, Driven by Mist AI

Die Risikoprofilerstellung, gesteuert von Juniper Mist AI, bringt Netzwerksicherheit zum Edge des verteilten Zugangsnetzes. Durch Erstellung von Risikoprofilen können IT-Teams ihre Infrastruktur schützen, indem sie für umfassende Netzwerkvisibilität und Richtliniendurchsetzung an jedem Verbindungspunkt im Netzwerk sorgen. Dadurch werden Campus-Netzwerke bedrohungssensibel und spielen eine aktive Rolle bei der Bedrohungsabwehr.

Security Intelligence für Mist Systems

Wenn ATP Cloud oder die Geräte der SRX-Serie durch Warnmeldungen auf Bedrohungen hingewiesen werden, beurteilen sie umgehend das Risiko, das durch die Verbindung von Benutzern oder Geräten mit drahtlosen Netzwerken entsteht, und ergreifen geeignete Maßnahmen. Das kann beispielsweise eine Quarantäne oder die Durchsetzung bestimmter Richtlinien sein.

Security Intelligence für die EX-Serie

ATP Cloud informiert die Switches der EX-Serie über kompromittierte Geräte, sodass diese die betroffenen Geräte blockieren oder isolieren und somit auch für Geräte ohne Endpunkt-Agent eine effektive Gerätekontrolle bereitstellen können.

Analysen und Automatisierung

Eine umfassende Übersicht über die Geschehnisse in einem Netzwerk ist ein guter erster Schritt, reicht aber allein nicht aus. Visibilität und Threat Intelligence müssen zur Durchsetzung von Zero-Trust-Richtlinien genutzt werden, um das Risiko zu mindern und die Abläufe in den Netzwerk- und Sicherheitsteams skalierbar zu gestalten. Organisationen erzielen erhöhte Visibilität mit:

- Security Director Cloud. Eine Benutzeroberfläche zur Verwaltung von On-Premises- und Cloud-basierten sowie aus der Cloud bereitgestellten Sicherheitssteuerungen. Mit Security Director Cloud können Kunden sicherstellen, dass ihre Sicherheitsrichtlinien den Benutzern, Geräten und Anwendungen folgen, wenn diese den Standort wechseln, ohne dass die Visibilität oder die Richtlinien zum Schutz vor Bedrohungen beeinträchtigt werden. Sicherheitsrichtlinien können einmal erstellt und unabhängig von Standortänderungen auf jeden Benutzer, jedes Gerät und jede Anwendung ausgeweitet werden.
- Security Director Insights. Diese Funktion von Security Director importiert Threat Intelligence und erkannte Bedrohungen aus beliebigen Sicherheitstools anderer Anbieter, hebt laufende Angriffe hervor und ordnet sie in das Mitre ATT&CK-Framework ein. Anschließend kann Security Director entweder direkt oder über Ansible-Automatisierung geeignete Maßnahmen identifizieren und andere Tools im Netzwerk zu deren Umsetzung orchestrieren.
- Automatisierung mit Junos. Das Betriebssystem Junos von Juniper stellt eine robuste API-Suite und andere native Automatisierungsfunktionen bereit, mit denen nahezu alle Prozesse und Ressourcen auf den Plattformen von Juniper konfiguriert, gesteuert und ihre Leistung protokolliert werden können. Die Option, aus Programmen heraus auf Junos-Funktionen zuzugreifen, kann beispielsweise genutzt werden, um Support-Tickets und Änderungsanträge automatisch zu bearbeiten und dabei darauf zu achten, dass der Gesamtzustand der Architektur nicht beeinträchtigt wird. Eine solche Prozessautomatisierung trägt zur Senkung der Investitions- und Betriebskosten bei.

Segmentierung in Campus-Netzwerken

Netzwerkarchitekten können eine Kombination aus mehreren Techniken (wie Mikro- und Makrosegmentierung) einsetzen, um Daten und Ressourcen zu schützen. Eine universelle EVPN-VXLAN-Architektur kann sich über

Campus und Datencenter erstrecken und ermöglicht eine einheitliche End-to-End-Segmentierung von Endgeräten und Anwendungen. Darüber hinaus hilft sie, Layer 2-Flooding zu minimieren, um Sicherheitsbedrohungen zu reduzieren und das Netzwerk zu simplifizieren.

- Makrosegmentierung ist eine logische Trennung des Netzwerks innerhalb gemeinsam genutzter Netzwerkgeräte und über gemeinsam genutzte Verbindungen hinweg. Dies wird in einem EVPN-VXLAN Netzwerk durch die Verwendung von VLANs auf Layer 2 und virtuellem Routing und Forwarding (VRF) auf Layer 3 erreicht. VRF sorgt für Isolierung, indem es den IP-Datenverkehr zwischen zwei VRF-Geräten voneinander trennt.
- Mikrosegmentierung trägt durch Risikominderung und die dynamische Anpassung an neue Sicherheitsanforderungen ebenfalls zu wichtigen Aspekten der Netzwerksicherung bei. Juniper hilft bei der Implementierung von Mikrosegmentierung auf Grundlage von Zugriffskontrolllisten (ACLs) oder Firewall-Filtern, um den Datenverkehr innerhalb des virtuellen Netzwerks zu kontrollieren.

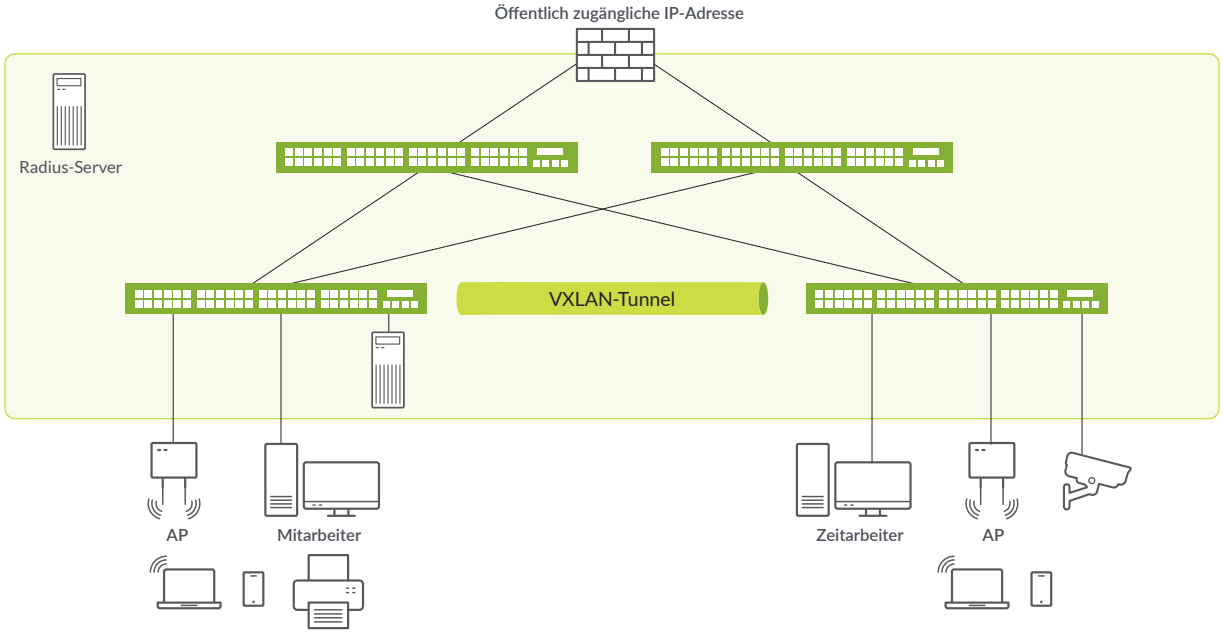

Abbildung 7: Netzwerksegmentierung nach Mitarbeitenden oder IoT-Geräten

Junos OS: Die Grundlage für Hochleistungsnetzwerke

Junos® OS bietet eine gemeinsame Sprache für die Routing-, Switching- und Sicherheitsgeräte von Juniper. Die Leistungsfähigkeit eines einzigen Junos OS reduziert die Komplexität in Hochleistungsnetzwerken, um die Verfügbarkeit zu erhöhen und Services bei geringeren Gesamtbetriebskosten schneller bereitzustellen. Die einheitliche Benutzererfahrung und die automatisierten Tools von Junos erleichtern die Planung und Schulung, straffen den Routinebetrieb und ermöglichen eine schnellere Implementierung von Änderungen im gesamten Netzwerk.

Was Junos OS von anderen Netzwerkbetriebssystemen unterscheidet, ist die Art und Weise, wie es aufgebaut ist: ein einziges Betriebssystem, das in einem Software-Release-Track und mit einer modularen Architektur bereitgestellt wird. Die wichtigsten Vorteile sind folgende:

- Ein einziges Betriebssystem für alle Arten und Größen von Plattformen reduziert den Zeit- und Arbeitsaufwand für die Planung, die Bereitstellung und den Betrieb von Netzwerk- und Sicherheitsinfrastrukturen.
- Ein Release-Track erfüllt die sich ändernden Anforderungen an Software durch die zuverlässige Bereitstellung neuer Funktionen in regelmäßigen, bewährten Intervallen.
- Eine modulare Softwarearchitektur bietet hochverfügbare, sichere und skalierbare Software, die offen für Automatisierung und Innovationen durch Partner ist.

Junos Telemetry

Herkömmliche Datenmodelle zur Erfassung von Betriebsdaten über den Systemzustand lassen sich angesichts der Größe heutiger Netzwerke nicht mehr effizient skalieren. Die Telemetrieschnittstelle von Junos umgeht dieses Problem mit einem Push-Modell, das Daten asynchron liefert und Polling überflüssig macht. Daher ist die Junos Telemetrieschnittstelle hoch skalierbar und kann Tausende von Objekten in einem Netzwerk überwachen.

Junos Telemetry Interface: Die Telemetrieschnittstelle von Junos unterstützt die Implementierung von Sensoren zum Erfassen und Exportieren von Daten für verschiedene Systemressourcen, wie physische Schnittstellen und Firewall-Filter. Es werden zwei Datenmodelle unterstützt:

- Ein von Juniper Networks definiertes, offenes und erweiterbares Datenmodell, das eine verteilte Architektur nutzt und daher problemlos skalierbar ist.
- Ein OpenConfig-Datenmodell, das Daten in Form von strukturierten Google-Protokollpuffer-Nachrichten (gpb) in einem universellen Schlüssel-/Wert-Format generiert. Da gRPC-Remote-Prozessaufrufe auf TCP basieren und die SSL-Verschlüsselung unterstützen, gilt dieses Modell als sicher und zuverlässig.

Fazit

Der KI-gestützte Campus von Juniper wurde entwickelt, um Kunden eine flexible, standardbasierte und moderne Architektur für eine Cloud-fähige Zukunft zu bieten. Er erfüllt die heutigen strengen Anforderungen, ohne Kompromisse bei der Zuverlässigkeit, Sicherheit und Agilität einzugehen. Oft verwendete Bausteine, vorgefertigte Automatisierungs-Workflows und benutzerdefinierte Automatisierungs-Toolkits erweitern die Vorteile vorausschauender Analyse vom Datencenter bis zum Campus und darüber hinaus.

Weitere Ressourcen

- Campus Design Center
- Webseite der EX-Serie
- Juniper Mist Cloud Services
- Juniper Connected Security
- Live-Demo: Wired and Wireless Wednesday
- Live-Demo: Das KI-gestützte Unternehmen
- Juniper Connected Security

Über Juniper Networks

Juniper Networks hat es sich zur Aufgabe gemacht, den Netzwerkbetrieb drastisch zu simplifizieren und für eine erstklassige Endbenutzererfahrung zu sorgen. Unsere Lösungen bieten Automatisierung, Sicherheit und KI, damit Sie von branchenführenden Einblicken und messbaren Ergebnissen profitieren. Wir sind davon überzeugt, dass zuverlässige Verbindungen uns einander näherbringen und uns alle in die Lage versetzen, die größten Herausforderungen der Welt in Bezug auf Wohlstand, Nachhaltigkeit und Gleichheit zu bewältigen.

JUNIPER NETWORKS | Driven by Experience™

Hauptniederlassung für die Regionen APAC und EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 207 125 700
Fax: +31 207 125 701

Hauptsitz und Sitz des Vertriebs
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

2000752-006-DE Juli 2022