Juniper Networks | Engineering Simplicity

TechTarget | Custom Media White Paper

Fünf unverzichtbare Merkmale zukunftsfähiger SD-WAN-Lösungen

©2021, Juniper Networks, Inc.

KURZFASSUNG

Obwohl jedes Unternehmen auf das Internet angewiesen ist, wurden konventionelle Unternehmensnetzwerke nicht für den sicheren Zugriff auf die erfahrungsintensiven Anwendungsumgebungen von heute konzipiert. Die ursprünglichen Internet-Host-Systeme haben bereitwillig Dateien und Informationen mit allen angeschlossenen Geräten ausgetauscht und es gab so gut wie keine Sicherheitsprotokolle.

Das blieb natürlich auch Cyberkriminellen nicht verborgen und sie suchten eifrig nach immer neuen Methoden, um in geschützte Systeme einzudringen, an vertrauliche Daten zu kommen und fremde Systeme mit Malware oder Ransomware zu infizieren, was verheerende Folgen für die betroffenen Unternehmen haben kann.

Dieses Whitepaper befasst sich mit der Entwicklung von softwaredefinierten Wide-Area-Netzwerken (SD-WANs) der ersten Generation und mit der Frage, was bei der Bewertung von Lösungen der nächsten Generation zu beachten ist.

©2021, Juniper Networks, Inc.

Herausforderungen rund um SD-WANs

SD-WANs wurden seit ihren Anfängen zu Beginn des 21. Jahrhunderts stark weiterentwickelt. Daher sollten insbesondere zwei Nutzergruppen jetzt ein Upgrade erwägen. Das sind zum einen diejenigen, die SD-WANs von Anfang an genutzt haben. Sie haben von deren Vorteilen profitiert, stoßen nun aber an die Leistungsgrenzen der ersten, inzwischen veralteten, Produktgeneration. Und zum anderen sind es die großen Unternehmen, die den Sprung in eine SD-WAN-Umgebung noch vor sich haben und weiterhin herkömmliche WAN-Modelle nutzen.

Im Laufe der Zeit haben diese Unternehmen die Komplexität ihrer Netzwerksicherheitsinfrastruktur durch ständige Anbauten und Umbauten erhöht. Vielerorts werden mehrere verschiedene Tunnel und virtuelle private Netzwerke (VPNs) sowie eine Vielzahl von Einzellösungen für bestimmte Sicherheitskomponenten und spezifische Bedrohungen genutzt. Infolgedessen müssen die IT-Abteilung und das Network Operations Center (NOC) mehrere verschiedene Produkte und Konsolen nutzen, um die Sicherheitsmaßnahmen für LAN-, WAN- und Cloud-Workloads zu verwalten. Und da diese Sicherheitsmaßnahmen oft erst nachträglich aufgesetzt wurden, beeinträchtigen sie die Anwendungsleistung und die Benutzererfahrung. Noch schlimmer ist jedoch, dass Unternehmen immer noch mit einer wachsenden Zahl von Sicherheitsverletzungen und Malware-Angriffen konfrontiert sind, die ihr Geschäft – und sogar die ganze Volkswirtschaft – zum Stillstand bringen können.

Netzwerk-Routing muss weiterentwickelt werden

Die meisten derzeit genutzten Routing-Protokolle und -Methoden beruhen auf jahrzehntealter Technologie, deren Nachteile nun immer deutlicher werden. Zum Beispiel:

- Traditionelle Hub-and-Spoke-Topologien können die neuen dynamischen Workflows und die unzähligen Datenflüsse, die durch SaaS- und Cloud-Anwendungen entstehen, nicht mehr bewältigen.
- Netzwerkarchitekten tun sich schwer damit, anwendungsorientierte Service Level Agreements (SLAs) zu unterstützen, die den heutigen Anforderungen der Anwender entsprechen.
- Viele Unternehmen müssen mit einer bunten Mischung aus für jeweils nur einen Zweck geeigneten Geräten und Sicherheitsprodukten wie Routern, Firewalls, IPS-Geräten, VPN-Appliances usw. jonglieren, was die betrieblichen und logistischen Herausforderungen nur noch verstärkt.

> Es wird immer deutlicher, dass herkömmliche SD-WANs ineffizient und kostspielig geworden sind.

Es wird immer deutlicher, dass herkömmliche SD-WANs ineffizient und kostspielig geworden sind. Sie tragen zwar zur Bewältigung einiger Managementherausforderungen bei, haben aber mehrere Schwächen, darunter die fehlende Servicegarantie für einzelne Datenströme, die mangelnde Transparenz von Netzwerksitzungen und Anwendungsdaten und den hohen Ressourcen- und Bandbreitebedarf von VPN-Tunneln und IPsec.

Obwohl das Routing von Grund auf geändert werden muss, schrecken Unternehmen vor dem Gedanken zurück, ganze Infrastrukturen komplett auszutauschen, um von den Vorteilen der neuesten SD-WAN-Lösungen zu profitieren.

©2021, Juniper Networks, Inc.

Viele Risiken bei Inaktivität

Sich ständig ändernde Anforderungen setzen die IT-Abteilung jeden Tag aufs Neue unter Druck. Einige der Herausforderungen:

- Initiativen zur digitalen Transformation erhöhen die Zahl der Nutzer und die Datenmenge im Netz.
- Die wachsende Anzahl an Geräten für den Zugriff auf Unternehmensressourcen und Cloud-Anwendungen vergrößert die Angriffsfläche.
- Der Mangel an Fachkräften mit den erforderlich Spezialkenntnissen setzt die bestehenden Teams noch mehr unter Druck, mit weniger mehr zu erreichen.

Diese steigenden Anforderungen machen sich in allen Branchen bemerkbar. Und wenn das Netzwerk nicht mithalten kann, leidet die Kundenerfahrung. Bei WANs geht es nicht mehr nur um Konnektivität und das Versenden von Paketen – vom WAN hängt ab, wer eine positive Nutzererfahrung genießt. Standort und Gerät spielen dabei eine untergeordnete Rolle.

Wenn das Netzwerk nicht in der Lage ist, Probleme selbst zu beheben oder zumindest selbst zu diagnostizieren, werden die Mitarbeiter in der IT-Abteilung und im NOC immer zwischen mehreren Konsolen hin- und herwechseln müssen, um alles im Griff zu behalten. Und wenn es zu Problemen – oder Sicherheitsverstößen – kommt, weisen sie sich schnell gegenseitig die Schuld zu.

Das heißt ganz klar: Ein veraltetes WAN kann für ein Unternehmen ein Wettbewerbsnachteil sein.

Zukunftsfähiges SD-WAN: Was sich Unternehmen wünschen

Der Weg zur Lösung dieser Herausforderungen führt über die Einführung zukunftsfähiger SD-WAN-Lösungen, die einen Großteil der veralteten Einzelprodukte ablösen und die Skalierbarkeit und Flexibilität bieten, die selbst große Unternehmen benötigen.

Bei der Wahl einer zukunftsfähigen SD-WAN-Lösung sollten Sie auf diese fünf ausschlaggebenden Komponenten achten und auf den Einsatz der entsprechenden Funktionen bestehen::

1. Sitzungsbasierte Architektur: Sie sorgt dafür, dass für jede Sitzung eine intelligente Routing-Fabric erzeugt wird, die genau auf die Anforderungen dieser Sitzung abgestimmt ist und Ihnen eine bessere Übersicht über die Benutzererfahrung und die Netzwerkleistung bietet.
2. Zero-Trust-Netzwerkzugriff: Unternehmen sollten heutzutage nicht mehr jedem, sondern nichts und niemandem vertrauen.
3. AIOps: Die Fähigkeit, das Netzwerk zu automatisieren und zu orchestrieren, hilft Unternehmen, Probleme zu lösen, bevor sie sich auf den laufenden Betrieb auswirken oder zu Datenverlusten führen.
4. Tunnelfreier Netzwerkzugriff: Damit entfällt die Notwendigkeit von VPNs und IPsec-basierten Tunnels, die sehr ressourcenintensiv sind.
5. Secure Access Service Edge (SASE): SASE-basierte Kriterien tragen dazu dabei, einer zunehmend mobilen Belegschaft maximale Performance und Sicherheit zu bieten – unter anderem durch zentralisierte, einfache Sicherheitsrichtlinien und -verwaltung sowie rollenbasierten Zugriff.

Mit dem Session Smart™ SD-WAN von Juniper lässt sich dies relativ einfach erreichen.

©2021, Juniper Networks, Inc.

Die Vorteile von Session Smart™

Was spricht für Session Smart™? Wer im Geschäftsleben erfolgreich sein will, muss die bestmögliche Benutzererfahrung bieten. Nur ein Session Smart™-Netzwerk ist in der Lage, die zukunftsweisende Kombination aus Intelligenz, Visibilität und Simplizität zu bieten, die erforderlich ist, um die strengen Anforderungen an die Netzwerkleistung und -sicherheit von heute und morgen zu erfüllen. Session Smart™-Netzwerke sind benutzerbasiert und kontextbezogen und bieten eine fein abgestufte Kontrolle über Sicherheits- und Leistungs-SLAs.

Session Smart™-Netzwerke basieren vollständig auf einem Zero-Trust-Modell, um ein Höchstmaß an Sicherheit zu gewährleisten. Sie nutzen Secure Vector Routing (SVR), was Administratoren die Eigenschaften bietet, die sie von einem IPsec-Tunnel erwarten – jedoch ohne Paket-Overhead und andere Nachteile. So werden nicht nur Netzwerkstaus vermieden und die verfügbare Bandbreite erweitert, sondern Administratoren haben auch einen besseren Einblick in den Verkehrsfluss und können die Qualität jeder Verbindung von einem Ende bis zum anderen überwachen. Sicherheit und Performance werden durch adaptive Verschlüsselung weiter verbessert – eine intelligentere Methode, für Sicherheit zu sorgen und gleichzeitig die Benutzererfahrung zu verbessern. Schließlich ist 90 % allen Datenverkehrs bereits verschlüsselt und muss nicht noch einmal verschlüsselt werden.

Da diese Innovationen eine hochwertige Benutzererfahrung gewährleisten und globale Compliance-Standards erfüllen, ist diese Lösung ideal für Kunden, die ein SD-WAN suchen, das die SASE-Kriterien erfüllt. (SASE ist eine moderne Cybersicherheitsarchitektur, die darauf abzielt, Sicherheit und Nutzer näher zueinander zu bringen und Nutzern je nach aktuellem Risikoniveau angemessene Zugangsrechte zuzuweisen.)

Session Smart™-SD-WAN ist vollständig softwarebasiert und kompatibel mit den bereits implementierten Lösungen der Kunden., die Kunden bereits haben. Für Unternehmen bedeutet das einen reibungslosen Umstieg ohne radikalen Systemaustausch. Ein sitzungs- und softwarebasierter Ansatz reduziert zudem die Komplexität am Netzwerk-Edge, da weniger Middleboxen wie Load Balancer, Router, DDoS-Schutz und so weiter benötigt werden. Stattdessen sind diese Funktionen in einem einzigen Session Smart™-Router zusammengefasst und werden als Teil des SD-WAN auf einer beliebigen branchenüblichen Hardwareplattform ausgeführt. Das gewährleistet optimale Performance ganz unabhängig davon, ob die Lösung auf einer virtuellen Maschine, einem virtuellen oder handelsüblichen physischen Server oder in der Cloud auf Azure oder Amazon Web Services bereitgestellt wird.

In vielen Fällen ist ein Session Smart™-Router am Netzwerk-Edge – mit Layer-3- und 4-Firewall-Fähigkeit und Zero Trust – vom Sicherheitsstandpunkt aus mehr als ausreichend und macht kostspielige und möglicherweise leistungsmindernde Next-Generation-Firewalls an allen Standorten überflüssig.

©2021, Juniper Networks, Inc.

Session Smart™-SD-WAN bietet folgende Vorteile:

- eine Verbesserung der Bandbreitennutzung um 50 %
- enorme Skalierbarkeit auf 10.000 Standorte und mehr
- Layer-3- und 4-Firewall-Funktionen, einschließlich Paketfilterung, IDS/IPS, DoS-Schutz, DPI, URL-Filterung und mehr
- Zero-Trust-Modell mit standardmäßiger Zugriffsverweigerung
- Möglichkeit der ständigen Überwachung der Pfade zur Nutzung der besten verfügbaren Routen, um eine optimale Benutzererfahrung zu gewährleisten
- Möglichkeit, Benutzer und Anwendungen im Netzwerk zu erkennen und zu verstehen und Sitzungen gemäß einfach konfigurierbaren Leistungs- und Sicherheits-SLAs intelligent weiterzuleiten
- Beseitigung der Umwege, die dadurch entstehen, dass der gesamte Datenverkehr über das Datencenter geroutet wird, was die Leistung drosseln und die Benutzerfreundlichkeit beeinträchtigen kann

IPsec und VPNs können nicht unbegrenzt skaliert werden und versagen oft, wenn die Anforderungen steigen. Session Smart™-SD-WAN ist ein kosteneffizienter, einfacher Ansatz zur Skalierung von Netzwerken und Sicherheit selbst für große Unternehmen, mit einer tunnelfreien Architektur, die weder in der Größe noch im Umfang für LAN, WAN, Cloud und IoT begrenzt ist.

Anpassbare Servicelevel ermöglichen es IT-Teams, die Auswirkungen des WAN auf die Endbenutzererfahrung sofort zu verstehen.

Benutzererfahrung ist heute das Maß der Dinge

Session Smart™-SD-WAN reiht sich in ein wachsendes und umfassendes Portfolio ein, das in letzter Zeit bereits durch die Übernahmen von 128 Technology, Apstra und Netrounds erweitert wurde. So wird die Vision einer vollständigen End-to-End- und Client-to-Cloud-Vision von Juniper Wirklichkeit. Die Strategie ist klar: Die Benutzererfahrung ist so wichtig wie die Verfügbarkeit.

Die umfangreichen Telemetriedaten, die der Session Smart™-Router auf Benutzer- und Anwendungsebene erfasst, werden an Juniper WAN Assurance und Marvis, einen KI-basierten virtuellen Netzwerkassistenten, weitergeleitet. Dadurch erhalten IT-Teams Einblicke und die Möglichkeit, Probleme proaktiv zu lösen. Anpassbare Servicelevel ermöglichen es IT-Teams, die Auswirkungen des WAN auf die Endbenutzererfahrung sofort zu verstehen. Letztlich setzen Juniper Mist AI und Marvis die Daten aus drahtlosen, kabelgebundenen und WAN-Netzwerksegmenten zu einem Gesamtbild zusammen, um ein einziges, unterbrechungsfreies und optimiertes Erlebnis im gesamten Unternehmen für Nutzer und Betreiber zu schaffen.

Nächste Schritte

Der Session Smart-Router von Juniper ist eine fortschrittliche, servicezentrierte Netzwerklösung, die das softwaredefinierte Routing auf eine neue Ebene hebt. Der Session Smart™-Router eignet sich perfekt für die moderne digitale Geschäftswelt und ermöglicht eine agile, sichere und belastbare WAN-Konnektivität mit bahnbrechenden Kostenvorteilen und bestechender Einfachheit. Weitere Informationen finden Sie unter https://www.juniper.net

©2021, Juniper Networks, Inc.

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 Vertriebshauptsitz

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Telefon: +1-888-JUNIPER (+1-888-586-4737)

oder +1-408-745-2000

Fax: +1-408-745-2100

www.juniper.net

Hauptniederlassung für die Regionen APAC und EMEA

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, Niederlande

Telefon: +31-0-207-125-700

Fax: +31-0-207-125-701

Copyright 2021 Juniper Networks, Inc. Alle Rechte vorbehalten. Juniper Networks, das Juniper Networks Logo, Juniper, Junos und andere Marken sind eingetragene Marken von Juniper Networks, Inc. und/oder seinen angeschlossenen Unternehmen in den USA und anderen Ländern. Andere Namen sind möglicherweise Marken ihrer jeweiligen Eigentümer. Eine Haftung durch Juniper Networks für fehlerhafte Angaben in diesem Dokument wird ausgeschlossen. Juniper Networks behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu übertragen oder anderweitig zu überarbeiten.

Diese Inhalte wurden von Juniper Networks in Auftrag gegeben und von TechTarget Inc. produziert.