FÜNF GRÜNDE FÜR DEN UMSTIEG AUF DIE SRX300-FIREWALLS DER NÄCHSTEN GENERATION

Erweiterter Schutz im gesamten Netzwerk zur Absicherung der Benutzer, Anwendungen und Infrastruktur

Die Herausforderung

IT-Teams, die sich mit veralteten Firewalls ohne Produktsupport zufrieden geben, setzen ihr Netzwerk dem Risiko von Cyberangriffen aus und bringen damit das gesamte Unternehmen in Gefahr.

Die Lösung

Der Umstieg auf die neuesten Services Gateways der SRX300-Modellreihe von Juniper bietet wirksamen Schutz – selbst vor extrem raffinierten Bedrohungen.

Vorteile

- *Bedrohungserkennung und -abwehr in Echtzeit mit ausgereiften Sicherheitsfunktionen*
- *Konsolidierung von Sicherheits- und Netzwerkmanagement auf einer zentralen Plattform*
- *Schnellere Reaktion auf erkannte Bedrohungen dank vereinfachter Sicherheitsprozesse*
- *Minimierung von Unterbrechungen der Sicherheitsprozesse*

Angesichts immer neuer Medienberichte über Sicherheitsverletzungen ist das Thema Cybersicherheit in aller Munde. Das Weltwirtschaftsforum sieht Cyberangriffe als Begleiterscheinung der zunehmenden Unverzichtbarkeit des Internets und zählt das Risiko von Datenverlusten und -diebstählen zu den fünf zentralen Herausforderungen unserer Zeit.[1] Daher müssen moderne Unternehmen geeignete Maßnahmen ergreifen, um Cyberbedrohungen rasch erkennen, eindämmen und abwehren zu können und zu verhindern, dass der geschäftliche Erfolg durch kostspielige Datenlecks und Compliance-Verstöße gefährdet wird.

Die Herausforderung

Im Zeitalter der Mobilgeräte, der Cloud und des Internets der Dinge (IoT) bietet das altbewährte Konzept der Absicherung des Perimeters keinen ausreichenden Schutz mehr. Zum einen werden Cyberbedrohungen immer komplexer, zum anderen ist die Angriffsfläche moderner Unternehmen wesentlich größer. Darüber hinaus sind konventionelle Sicherheitsinfrastrukturen den heutigen Netzwerkgeschwindigkeiten und getarnten Bedrohungen nicht gewachsen. Diese alternden Lösungen sind meist so komplex und mit derart zeitaufwendigen Wartungsprozessen verbunden, dass Sicherheitsteams nicht effizient arbeiten können, weil sie vorwiegend mit der Pflege des Systems beschäftigt sind. So entstehen Sicherheitslücken, die dann möglicherweise von finanziell motivierten Cyberkriminellen und staatlich gesponsorten Hackern ausgenutzt werden.

Der Migrationspfad von Juniper Networks zur Ersetzung alter Firewalls

Unternehmen mit veralteten Firewalls können auf denkbar einfache Weise auf die Services Gateways der SRX300-Modellreihe von Juniper Networks® umstellen, um ihre Sicherheitsinfrastruktur zu stärken und zu vereinfachen. Die Modelle SRX300, SRX320, SRX340 und SRX345 bieten ausgereifte Sicherheits-, Netzwerk-, SD-WAN- und LTE-Backup-Funktionen auf einer zentralen Plattform. Dank des unkomplizierten Migrationspfads sind die Services Gateways der SRX-Serie die ideale Wahl für Unternehmen mit mehreren Filialen und verteilten Standorten. Zudem profitieren Kunden von schnellen, einfachen Netzwerkupgrades, ausgereiften Firewall-Funktionen zur Abwehr komplexer Bedrohungen sowie den Sicherheitsprozessen und dem umfassenden Know-how der Juniper-Sicherheitsexperten.

Fünf Gründe für den Umstieg auf die SRX300-Firewalls der nächsten Generation

Veraltete Firewalls sind ein Sicherheitsrisiko. Doch mit einem Upgrade auf ein neues SRX300-Services-Gateway können Unternehmen mit mehreren Niederlassungen oder verteilten Standorten ihr Sicherheitsniveau heben und ihre Betriebsprozesse wirkungsvoll schützen. Dieser Schritt bringt fünf wichtige Vorteile.

[1]Global Risks Report 2018 des Weltwirtschaftsforums (in englischer Sprache): http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

1. **Vereinfachte Infrastruktur für moderne Cybersicherheit:** Die SRX300-Produkte dienen der Juniper-Plattform Connected Security als strategische Netzwerkkomponenten zur Durchsetzung von Richtlinien. Dadurch werden die Sicherheitsprozesse in Ihrem Unternehmen vereinfacht und Benutzer, Anwendungen und Infrastrukturen besser geschützt. Außerdem spürt die SRX300 im Zusammenspiel mit Juniper Sky™ Advanced Threat Prevention schwer zu erfassende Malware wie Ransomware auf und stellt sicher, dass Ihre Maßnahmen zur Cyberabwehr kontinuierlich auf neue Bedrohungen und Risiken abgestimmt werden. Dies ermöglicht die automatisierte Verwaltung und Durchsetzung von Sicherheitsrichtlinien in Ihrer gesamten Unternehmensinfrastruktur, basierend auf aktuellen Netzwerk- und Bedrohungsdaten.
2. **Bedrohungsabwehr in Echtzeit:** Die Integration der SRX300-Services-Gateways mit Juniper Sky ATP erweitert Ihre Sicherheitsinfrastruktur um eine zusätzliche Schicht, sodass nun auch vollkommen unbekannte Malware erkannt und abgewehrt wird, bevor sie ihr Ziel erreicht. Juniper Sky ATP nutzt maschinelle Lernalgorithmen, um mithilfe cloudbasierter Echtzeitdaten über das Internet und per E-Mail übertragene Dateien kontinuierlich auf Ransomware und andere getarnte Bedrohungen zu überprüfen. Durch die Kombination mit dieser Lösung können die SRX300-Firewalls gründliche Überprüfungen, Inline-Blocking und aussagekräftige Warnmeldungen bieten.
3. **Stärkere Sicherheit bei optimaler Nutzung vorhandener Kenntnisse:** Die SRX300-Modellreihe bietet stärksten Schutz für Unternehmensinfrastrukturen, die sich über mehrere Standorte erstrecken. Nach der Umstellung profitiert Ihr Unternehmen von den noch effektiveren Funktionen der aktuellen Version von Juniper Networks Junos®. Gleichzeitig bleibt Ihren Sicherheits- und Netzwerkteams die Einarbeitung in ein neues Betriebssystem für die Konfiguration und Administration neuer Netzwerke erspart, da die betreffenden Mitarbeiter auf ihre vorhandenen Juniper-Kenntnisse zurückgreifen können. Das bedeutet Effizienzsteigerungen in der IT und damit zusätzliche Zeit und Ressourcen für geschäftliche Innovationen.
4. **Bereitstellungsmodelle für verteilte Enterprise-Infrastrukturen:** Moderne Unternehmen mit verteilten Infrastrukturen und mehreren Filialen benötigen eine zentrale Plattform mit Sicherheits- und SD-WAN-Funktionen, die automatische Bereitstellungsprozesse (Zero Touch Provisioning), anwendungsbasiertes Routing und die Sicherstellung einer erstklassigen Servicequalität ermöglichen.
5. **Sicheres Routing:** Die Services Gateways der SRX300-Modellreihe bieten ein breites Spektrum an WAN-Konnektivitätsoptionen für Filialen und verteilte Standorte, da sie MACsec-Ports und integrierte Glasfaserports sowie LTE-Backups für Drahtlosnetzwerke unterstützen.

So wählen Sie die richtige SRX300-Firewall für Ihr Unternehmen

Die SRX300-Produkte wurden speziell für die Anforderungen von Unternehmen mit verteilten Standorten entwickelt. Dabei können die Nutzer älterer Juniper-Firewalls auf das jeweils entsprechende SRX300-Nachfolgemodell umsteigen und so ihre Sicherheitsinfrastruktur mit innovativer Technologie der nächsten Generation modernisieren. Möglich sind beispielsweise folgende Migrationspfade:

- Wenn Sie derzeit ein SSG-5- oder SRX100-Modell verwenden, bietet sich ein Upgrade auf das Services Gateway SRX300 an.
- Wenn Sie derzeit ein SSG-20- oder SRX210/SRX220-Modell verwenden, bietet sich ein Upgrade auf das Services Gateway SRX320 an.
- Wenn Sie derzeit ein SSG-140- oder SRX240-Modell verwenden, bietet sich ein Upgrade auf das Services Gateway SRX340 oder SRX345 an.

Das Modell SRX300 eignet sich perfekt für die Absicherung kleiner Zweigstellen und Ladengeschäfte, da es Sicherheits-, Routing-, SD-WAN- und WAN-Funktionen in einem kompakten Desktopformat vereint. Zusätzlich zu diesen Features bietet das ebenfalls für die sichere Anbindung kleinerer Niederlassungen ausgelegte Modell SRX320 optionale PoE+-Ports. Dagegen wurde das Modell SRX340 speziell für die sichere Anbindung mittelgroßer Filialinfrastrukturen konzipiert: Hier erhalten Sie neben konsolidierten Sicherheits-, Routing- und SD-WAN-Funktionen im 1U-Format auch WAN-Konnektivität zur Anbindung von Remote-Standorten sowie optionale UTM-Funktionen (Unified Threat Management) und LTE-Backups für Drahtlosnetzwerke. Und für die Absicherung mittelgroßer bis großer Filialumgebungen gibt es das Services Gateway SRX345, das zusätzlich zu den bereits genannten Vorteilen Firewall-Durchsatzraten von bis zu 5 Gbit/s und einen IPsec-VPN-Durchsatz von 800 Mbit/s bietet.

SRX300

SRX320

SRX340

SRX345

Fazit: Starke Cybersicherheit kann ganz einfach sein

Das Thema Cybersicherheit wird von Tag zu Tag komplexer. Klar ist jedoch, dass es sich kein Unternehmen leisten kann, seine Daten mit veralteten Firewalls zu schützen. Mit der „Connected Security"-Plattform von Juniper und den Services-Gateways der SRX300-Modellreihe lässt sich die Cyberabwehr Ihres Unternehmens sowohl stärken als auch vereinfachen. Zugleich können Sie die für Ihre Anforderungen optimalen Schutzmaßnahmen effizient in Ihre Infrastruktur einbinden.

Nächste Schritte

Weitere Informationen über die SRX300-Firewalls der nächsten Generation finden Sie unter www.juniper.net/us/en/products-services/security/srx-series/srx300/.

Wenn Sie mehr über die Migrationsoptionen der SRX300-Modellreihe erfahren möchten, wenden Sie sich bitte an Ihren Ansprechpartner bei Juniper Networks.

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 Überwindung ihrer größten Herausforderungen. Wir bei Juniper Networks sind überzeugt, dass Netzwerke ein Medium für den weltweiten Wissensaustausch und den 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.

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