



SCHÜTZEN SIE IHR UNTERNEHMEN MIT EINER NEXT-GENERATION FIREWALL

Next-Generation Firewalls bieten anwendungssensible und rollenbasierte Sicherheitsmaßnahmen für stärkeren Schutz.

Die Herausforderung

Unternehmen brauchen mehr Kontrolle über die Anwendungen und den Datenverkehr in ihren Netzwerken, um ihre Ressourcen vor Angriffen zu schützen und gleichzeitig die Bandbreitennutzung zu optimieren. Dazu brauchen sie eine effiziente Lösung, die ein sehr großes Maß an Sicherheit bietet.

Die Lösung

Die Gateways der SRX-Serie von Juniper Networks bieten anwendungssensiblen Firewall-Schutz auf dem neuesten Stand der Technik mit integrierter Angriffsprävention, rollenbasierten Zugangskontrollen und branchenführendem Unified Threat Management (UTM) zum Schutz und Management Ihrer Unternehmensressourcen. Die Lösung wird über Junos Space Security Director von Juniper Networks zentral verwaltet.

Vorteile

- Schützt vor in Anwendungen verborgenen Bedrohungen und optimiert die Bandbreitennutzung mit anwendungs-basierten Maßnahmen
- Vereinfacht das Richtlinienmanagement durch nutzer- und rollenbasierte Firewall-Regeln
- Schützt mit IPS (Intrusion Prevention System) und UTM (Unified Threat Management) vor netzwerk-basierten Exploits, Malware und anderen, in legitimen Anwendungen verborgenen Bedrohungen
- Konsolidiert die Administration auf einer zentralen Managementplattform

Unternehmen brauchen Lösungen, mit denen sie ihre Ressourcen effektiv vor der ständig steigenden Zahl gefährlicher neuer Bedrohungen schützen können. Ein Blick auf die aktuellen Schlagzeilen zeigt, warum die Cybersicherheit heute wichtiger ist als je zuvor. Ebenso wichtig sind das effektive Management des Netzwerkverkehrs und die richtige Kombination aus Netzwerk- und Sicherheitsfunktionen. All diese Herausforderungen werden durch die neueste Generation webbasierter Anwendungen und die ständig steigende Anzahl der Mobilgeräte noch verschärft. In einem typischen Unternehmensnetzwerk werden Hunderte und vielleicht sogar Tausende von Anwendungen ausgeführt, von denen einige unternehmenskritisch sind und andere nicht.

Wie prüfen Sie, welche dieser Anwendungen auf das Netzwerk zugreifen dürfen und wie blockieren Sie den Zugriff durch nicht autorisierte Anwendungen? Wie sorgen Sie dafür, dass der Netzwerkverkehr von und zu geschäftskritischen Anwendungen bevorzugt übertragen wird? Wie stärken Sie die Sicherheit, ohne die Effizienz zu beeinträchtigen? Wie verhindern Sie, dass Ihre Sicherheitsmaßnahmen den Geschäftsbetrieb beeinträchtigen? Hier kommen Next-Generation Firewalls ins Spiel.

Die Herausforderung

Da sowohl die Netzwerkinfrastrukturen als auch die Bedrohungen sich ständig weiterentwickeln, dürfen Netzwerksicherheitslösungen nicht still stehen, wenn sie effektiven Schutz bieten sollen. Deshalb brauchen sie eine Architektur, die auch in sich ständig ändernden Netzwerkumgebungen stets die richtige Mischung aus Leistung und Skalierbarkeit bietet. Doch das allein reicht nicht aus. Sie müssen zudem Sicherheitsdienste bereitstellen, mit denen Administratoren alle Anwendungen in ihrem Netzwerk im Blick haben.

Viele Administratoren haben bereits Sicherheitslösungen auf ihre Umgebungen aufgesetzt, um die Herausforderungen der heutigen Geschäftswelt zu bewältigen. Mehrere Sicherheitsappliances und ein oder mehrere Firewalls in ein und demselben Unternehmensnetzwerk sind heute keine Seltenheit mehr. Die zusätzlichen Appliances stärken die Sicherheit, steigern aber auch die Netzwerkkomplexität und den Managementaufwand. In der Regel beeinträchtigen sie somit die Gesamtleistung.

Die Next-Generation Firewalls von Juniper Networks

Die Services Gateways der SRX-Serie von Juniper Networks® schützen Ihre Unternehmensressourcen mit anwendungssensiblen Firewall-Funktionen der nächsten Generation, einem integrierten IPS (Intrusion Prevention System), benutzer- und rollenbasierten Zugangskontrollen und branchenführendem Unified Threat Management (UTM). Next-

Generation Firewalls können alle Datenpakete prüfen und anwendungs- und benutzerspezifische Sicherheitsrichtlinien anwenden. Das bedeutet, dass Sie gezielt Sicherheitsrichtlinien für bestimmte Anwendungen oder Benutzer definieren können, die Daten über das Netzwerk senden oder empfangen. Gleichzeitig können Sie alle Inhalte prüfen, die in Ihrem Netzwerk übertragen werden. So können Sie Ihr Netzwerk vor Bedrohungen schützen, die verfügbare Bandbreite effizient zuweisen und dafür sorgen, dass angemessene Zugriffskontrollen konfiguriert und durchgesetzt werden.

Die Suite Juniper Networks AppSecure enthält eine ganze Reihe von Sicherheitsdiensten für die Lösungen der SRX-Serie, unter anderem zur Klassifizierung von Netzwerkverkehr, zur Verbesserung der Transparenz, zur Durchsetzung von Richtlinien sowie zur Verwaltung der Netzwerksicherheit. AppSecure nutzt eine funktionsreiche Klassifizierungs-Engine, um Anwendungen unabhängig vom Port und Protokoll korrekt zu identifizieren. Diese Klassifizierungs-Engine erkennt auch Anwendungen, die für die Nutzung von Verschleierungstaktiken bekannt sind. So erhalten Sie die Kontextinformationen, die Sie benötigen, um den Datenverkehr in Ihrem Netzwerk unter Kontrolle zu bekommen, anhand genauer Informationen angemessene Richtlinien zu konfigurieren und durchzusetzen und letztendlich die Netzwerkleistung und -skalierbarkeit zu erreichen, die Ihr Unternehmen braucht. Einige Beispiele für die von AppSecure bereitgestellten Services sind AppTrack für einen detaillierten Überblick über den Anwendungsdatenverkehr, AppFW für die granulare Durchsetzung von Richtlinien für diesen Datenverkehr und AppQoS für die Priorisierung und Messung des Anwendungsdatenverkehrs.

Optional können Sie die in den Lösungen der SRX-Serie integrierten IPS- und UTM-Funktionen hinzuziehen, um Ihre Anwendungen noch besser vor Malware, Spam, Phishing und anwendungsspezifischen Exploits zu schützen.

Wir bei Juniper legen großen Wert darauf, dass unsere Lösungen offen und flexibel sind. Im Gegensatz zu manchen anderen Next-Generation-Lösungen unterstützen unsere Sicherheitsdienste nicht nur unser IPS und die von unseren Forscherteams erstellten Anwendungssignaturen, sondern auch das Einfügen benutzerdefinierter Signaturen. So können Sie Ihre Lösung genau an die spezifischen Anforderungen Ihres Unternehmens anpassen.

Darüber hinaus können die Sicherheitsmaßnahmen der SRX-Serie unter Berücksichtigung der Benutzeridentität angewandt werden. Sie können also Sicherheitsrichtlinien für bestimmte Benutzer oder Benutzerarten definieren und direkt in Ihr Netzwerkverzeichnis einspeisen.

Die SRX-Serie besteht aus einer breiten Palette von Modellen, von All-in-One-Sicherheits- und Netzwerk-Appliances für Zweigstellen bis hin zu leistungsstarken, hochgradig skalierbaren Chassis-Lösungen für Datacenter. Alle Modelle unterstützen Next-Generation-Funktionen. Darüber hinaus bietet auch die Plattform Juniper Networks Firefly Perimeter einige Next-Generation-Firewall-Funktionen.

Diese Funktionen können für alle Modelle der SRX-Serie und alle Instanzen von Firefly Perimeter von einer zentralen Managementkonsole aus verwaltet werden. Über diese Konsole, den Juniper Networks Junos® Space Security Director, können Sie sämtliche Sicherheitsdienste verwalten, das Erstellen von Logdateien und Berichten veranlassen, die Verantwortung für verschiedene Aspekte des Managements an Benutzer mit bestimmten Rollen delegieren und diesen Rollen die erforderlichen Zugriffsrechte gewähren. Dieses zentralisierte Management basiert auf dem von allen Juniper-Lösungen genutzten Betriebssystem Junos und profitiert dadurch von demselben hohen Maß an Resilienz und Skalierbarkeit wie die Netzwerklösungen von Juniper Networks, die bei einigen der größten Serviceanbieter weltweit im Einsatz sind.

Das Ergebnis: Eine leistungsstarke Lösung, die Administratoren den klaren Überblick und die Kontextinformationen bietet, die sie brauchen, um Sicherheitsrichtlinien zu formulieren und durchzusetzen, die die neuesten Malwareangriffe stoppen, ohne die Leistung und das Unternehmenswachstum zu drosseln.

Funktionen und Vorteile

- Mit AppSecure schützen Sie Ihre Umgebung vor in Anwendungen verborgenen Bedrohungen und haben zudem mehr Kontrolle über die Anwendungen in Ihrer Umgebung und deren Bandbreitennutzung.
- Durch die Verknüpfung von Lösungen der SRX-Serie mit Ihrem Netzwerkverzeichnis schaffen Sie die Grundlage für datengestützte, benutzer- und rollenbasierte Sicherheitsrichtlinien, die den Zeitaufwand und die Komplexität der Richtlinienverwaltung reduzieren.
- Durch das Einspeisen Ihrer selbst definierten Signaturen in unser IPS schützen Sie Ihr Unternehmen umgehend vor netzwerkbaasierten Exploits, die Schwachstellen in Ihren Anwendungen ausnutzen.
- Mit UTM, das Antiviren- und Antispam-Schutz, Web- und Inhaltsfilterung beinhaltet, schützen Sie Ihr Unternehmen vor Malware, Viren, Spam, Phishing-Angriffen, Einbruchversuchen und anderen Bedrohungen.
- Durch das zentralisierte Management sämtlicher Next-Generation Firewalls über den hochgradig skalierbaren Junos Space Security Director straffen Sie die Verwaltung.

Die Lösung im Detail

AppSecure

Die Suite AppSecure bietet leistungsstarke Sicherheitstools zur Identifizierung von Anwendungen und sorgt so für bessere Transparenz und Kontrolle, die striktere Durchsetzung von Richtlinien sowie stärkere Netzwerksicherheit. AppSecure erkennt das Verhalten und die Schwachstellen von Anwendungen und kann in Anwendungen verborgene Sicherheitsbedrohungen unschädlich machen, auch wenn sie schwer zu erkennen und aufzuhalten sind.

IPS

Das IPS (Intrusion Prevention System) von Juniper schützt Ihr Unternehmen vor netzwerkbasierenden Exploits, die Schwachstellen in Ihren Anwendungen ausnutzen.

UTM

Mit UTM (Unified Threat Management) profitieren die Gateways der SRX-Serie und die virtuelle Firewall Firefly Perimeter von einer branchenführenden UTM-Lösung mit Antivirus- und Antispam-Schutz, Web- und Inhaltsfilter, die Ihre Systeme vor Malware, Viren, Spam, Phishing-Angriffen, Einbruchversuchen und anderen Bedrohungen schützt. UTM kann in der Cloud oder On-Premises bereitgestellt werden.

Benutzer- und rollenbasierte Firewall

Juniper hat mehrere benutzer- und rollenbasierte Firewalls im Angebot, die dynamische Sicherheitsrichtlinien unterstützen. Die branchenüblichen Firewall-Funktionen der nächsten Generation sind in die Gateways der SRX-Serie integriert.

Wenn die Produkte der SRX-Serie mit dem Juniper Identity Management Service (JIMS) verknüpft werden, stehen zusätzliche, skalierbare und feinkörnige Zugriffskontrollen zur Verfügung, die zum Erstellen dynamischer Richtlinien genutzt werden können.

Junos Space Security Director

Security Director bietet umfassende Funktionen für die Skalierung von Sicherheitsmaßnahmen, eine granulare Richtlinienkontrolle und ein breites Spektrum an Richtlinien für das gesamte Netzwerk. Mit Security Director können Administratoren sämtliche Phasen des Lebenszyklus von Sicherheitsrichtlinien für statusbehaftete Firewalls, UTM, IPS, AppSecure, benutzer- und rollendefinierte Firewalls, VPN und NAT mit geringem Zeitaufwand verwalten.

Verwalten und schützen Sie Ihr Netzwerk

Übernehmen Sie die Kontrolle über die Anwendungen und den Datenverkehr in Ihrem Netzwerk, schützen Sie die Ressourcen Ihres

Unternehmens vor Angreifern und optimieren Sie die Zuweisung der verfügbaren Bandbreite. Wenn Sie die Sicherheit stärken müssen, ohne dass der Geschäftsbetrieb komplizierter wird, ist eine Next-Generation Firewall vielleicht genau die richtige Lösung für Sie.

Die Gateways der SRX-Serie schützen Ihre Unternehmensressourcen mit anwendungssensiblen Firewall-Funktionen der nächsten Generation, einem IPS, benutzer- und rollenbasierten Zugangskontrollen und branchenführendem Unified Threat Management (UTM).

Die SRX-Serie besteht aus einer breiten Palette von Modellen, von All-in-One-Sicherheits- und Netzwerk-Appliances bis hin zu leistungsstarken, hochgradig skalierbaren Chassis-Lösungen. Sämtliche Modelle können über den Junos Space Security Director zentral verwaltet werden. Zudem können die Lösungen der SRX-Serie durch andere Sicherheitsdienste ergänzt werden, um eine kosteneffektive Lösung für Ihre spezifischen Anforderungen zu erstellen.

Wenn Sie mehr über die Gateways der SRX-Serie und unsere Next-Generation Firewalls erfahren möchten, schauen Sie unter <https://www.juniper.net/de/de/solutions/security/> vorbei oder wenden Sie sich an Ihren Ansprechpartner bei Juniper.

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 | Engineering
NETWORKS | Simplicity

