# SCHUTZ TRADITIONELLER UND CLOUD-RECHENZENTREN MIT INTELLIGENTER SICHERHEIT

## Verbesserte Sicherheitseffizienz durch dynamische Intelligenz

### Herausforderung

Immer komplexere Bedrohungen können Clouds lahmlegen, Abläufe im Rechenzentrum zum Erliegen bringen und zum Diebstahl wichtiger Daten führen. Obwohl bereits viele intelligente Sicherheitslösungen auf dem Markt sind, die Bedrohungen in Echtzeit transparent machen, war es bisher einfach zu schwierig, diese Daten in nutzbare Lösungen zu verwandeln, das über Firewall-Richtlinien ausgeführt werden können.

### Lösung

Die Services-Gateways der SRX-Serie bieten adaptive Security Intelligence Services, die Ihnen dabei helfen, Sicherheitsrichtlinien zu optimieren und Cyber-Angriffe abzuwehren. Diese Firewalls sorgen dafür, dass Ihre Sicherheitsumgebung genau auf die Bedrohungen abgestimmt ist, die eine aktive Gefahr darstellen.

### Vorteile

- Wirkungsvoller intelligenter und zeitnaher Schutz vor aktuellen Bedrohungen
- Flexibilität und individuell anpassbare Firewall-Richtlinien durch Anwendung von Feeds mit Bedrohungsinformationen
- Reduzierung der operativen Last durch dynamisches Einbeziehen von Sicherheitsanalysedaten in Firewall-Richtlinien
- Hohe Perfromance und skalierbarer Rechenzentrumsschutz durch intelligente Serviceverkettung

Der Schutz Ihrer Rechenzentren, des Netzwerk-Edges und der Cloud-Umgebungen ist eine ständige Herausforderung. Ihre Gegner sind Cyberkriminelle, Cyberterroristen oder Hacktivisten, die mit immer ausgeklügelteren Angriffstechniken eine sich ständig verändernde Bedrohungslandschaft schaffen. Traditionelle Firewalls, die sich auf eine Überwachung von Schicht 3 und 4 konzentrieren, sind für die heutigen Bedrohungsumgebung nicht mehr ausreichend. Die Next-Generation-Firewalls sind zwar leistungsstark, aber nicht für den Schutz vor der Schnelligkeit und Vielfältigkeit neuer Bedrohungen ausgelegt. Heutzutage muss Ihre Firewall in der Lage sein, direkt auf bekannte oder neue, erkenntnisgestützte Daten zu Bedrohungen zu reagieren. Sie muss Angriffe genau identifizieren und eine schnelle Reaktion ermöglichen.

Durch den Wechsel hin zu Cloud-Architekturen wird die traditionelle Firewall-Administration schon allein aufgrund der Komplexität der verteilten Sicherheit beschwerlich und anfällig für menschliche Fehler. Benötigt wird eine Firewall, die sich an neue Bedrohungen nahezu in Echtzeit und auf automatisierte und dynamische Weise anpassen kann.

## Die Herausforderung

Beim Aufbau und bei der Verwaltung eines herkömmlichen oder Cloud-Rechenzentrums ist Sicherheit ein grundlegendes Element. Es ist keine einfache Aufgabe, ein Gleichgewicht hinsichtlich des Benutzerzugriffs auf Anwendungen und des Schutzes digitaler Assets zu finden. Im Folgenden finden Sie einige der wichtigsten Herausforderungen:

- **Proprietäre und unflexible Sicherheitsplattformen:** Einige Firewall-Lösungen nutzen zwar eine cloudbasierte Bedrohungserkennung[1], die beteiligten Daten sind jedoch häufig proprietär, auf der Firewall vorkonfiguriert und unflexibel, sodass eine Auswahl oder Kontrolle der bereitgestellten Informationen nicht möglich ist.
- **Unwirksamkeit der Sicherheitslösung:** Der Markt quillt über vor Anbietern, die behaupten, Lösungen zur Bedrohungserkennung im Angebot zu haben. Die meisten der verfügbaren Daten-Feeds ermöglichen jedoch keine unmittelbare Umsetzung. Ihre Firewall kann diese Daten-Feeds daher nicht direkt in die Firewall-Richtlinien integrieren, sodass kein optimaler Schutz möglich ist.
- **Statische Adressgruppen:** Administratoren sind in der Regel bei der Überwachung oder Blockierung auf statische Adresslisten angewiesen und müssen die Firewall-Richtlinie bei jeder Änderung der Listen manuell anpassen. Das ist umständlich und schwierig zu handhaben.
- **Firewall-Performance:** Firewall-Dienste wie IPS und Anwendungsüberwachung wirken sich häufig negativ auf die Firewall-Performance aus. Insbesondere Einträge von Feeds mit Bedrohungsinformationen können schnell auf einem einzelnen Firewall-Gerät in die Tausende (wenn nicht mehr) gehen, sodass sich Performance-Probleme ergeben, die unnötige Upgrades erforderlich machen. Darüber hinaus wird die Bedrohungserkennung auf der Firewall möglicherweise nicht so eingesetzt, dass eine maximale Nutzung ihrer Ressourcen ermöglicht wird.
- **Keine zentrale Richtlinienverwaltung:** Eine zuverlässige und zentrale webbasierte Verwaltungslösung ist wichtig, wenn die Anzahl der Firewalls in Ihrem Netzwerk zunimmt und einheitliche Richtlinien in der Firewall-Umgebung umgesetzt werden müssen.

[1] In diesem Dokument werden die Begriffe „Bedrohungserkennung“ und „Sicherheit“ synonym verwendet, außer wenn auf GeoIP (Adressgruppe) Bezug genommen wird.

## Die Firewall der SRX-Serie von Juniper Networks mit Security Intelligence

Juniper bietet ein vollständiges Portfolio skalierbarer Sicherheitslösungen, die Kunden basierend auf den Services Gateways der SRX-Serie von Juniper vor den größten Bedrohungen schützen. Die SRX-Serie bildet die Grundlage für eine Vielzahl an Services, einschließlich UTM-Services, Firewall-Services der nächsten Generation und dynamischen Analyse-Services, die von Unternehmen und Service Providern als weitere Bausteine hinzugefügt werden können.

Diese dynamischen Analysedienste (Dynamic Intelligence Services) stellen zahlreiche Feeds mit Bedrohungsinformationen (sowohl im Roh- als auch im bearbeiteten Datenzustand) bereit, die aggregiert, normiert, analysiert und dynamisch an Sicherheitsrichtlinien verteilt werden können, die am Firewall-Enforcement-Point angewendet werden. Diese Dienste werden über ein offenes, skalierbares Framework ermöglicht, das ein integraler Bestandteil der SRX-Umgebung ist. Das offene Framework-Design basiert auf der Annahme, dass Bedrohungen weiter zunehmen und neue Intelligence-Feeds hinzukommen werden und Sicherheitsadministratoren bei ihrem Streben nach der Umsetzung eines zuverlässigen Sicherheitsansatzes Big Data nutzen möchten.

**Juniper SRX mit Security Intelligence-Lösung: ein Konzept in drei Schritten**

1. **Erkenntnisgestützte Sicherheitsdaten werden über Spotlight Secure Connector freigegeben.**
   a. Spotlight Secure erfasst erkenntnisgestützte Daten-Feeds, optimiert sie und sendet die aktualisierten Daten-Feeds zurück an Spotlight Secure Connector. Derzeit sind die folgenden Feeds verfügbar: Command and Control (C&C) und Identifizierung von Adressen über GeoIP.
   b. Analysedaten zu lokalen Bedrohungen (von Kunden oder Drittanbietern bereitgestellt Feeds) werden an Spotlight Secure Connector gesendet.
2. **Spotlight Secure Connector aggregiert die Security Intelligence-Daten dynamisch und sorgt dafür, dass nur die aktuellsten Daten an die Gateways der SRX-Serie verteilt werden.** Da die Aggregation der Bedrohungserkennungsdaten vor Ort erfolgt, ist die Integration von Analysedaten aus zahlreichen Quellen wie Spotlight Secure, eigene lokale Feeds, Drittanbieter-Feeds usw. möglich. Diese Daten werden anschließend für die Richtliniendurchsetzung auf den Geräten der SRX-Serie verfügbar gemacht. Im Unterschied zu anderen Angeboten auf dem Markt ist nicht die Firewall selbst dafür verantwortlich, Daten-Feeds von einem Cloud-Service abzurufen, noch ist der Firewall-Administrator verantwortlich, der sich um die Konfiguration jeder Firewall, auf der die Analysedaten verfügbar sein sollen, kümmern muss. Darüber hinaus übernehmen Junos Space Security Director und Log Director die zentrale Verwaltung der Bedrohungserkennungsrichtlinien sowie die Protokollerfassung zu Sicherheitsereignissen für die Geräte der SRX-Serie.
3. **Die Gateways der SRX-Serie nutzen Security Intelligence als Teil ihrer Sicherheitsrichtlinie.** Die SRX-Serie ist in der Lage, auf der Grundlage der Daten-Feeds Richtlinien für bestimmte Anwendungsfälle durchzusetzen. So können beispielsweise Verbindungen von beschädigten Systemen zu C&C-Diensten unterbunden werden. Die beträchtliche operative Effizienz und Schnelligkeit des Schutzes sind dadurch möglich, dass die SRX-Serie Adressgruppen nutzt, die dynamisch mithilfe von benutzerdefinierten Feeds aktualisiert werden, die entweder vom Administrator oder von GeoIP-Daten aus Spotlight Secure bereitgestellt werden. Die Aktualisierung der Adressgruppe erfolgt dynamisch: Da keinerlei Commits oder Konfigurationsänderungen erforderlich sind, können die für die Anwendung von Sicherheitsrichtlinien in der SRX Serie eingesetzten Adressen ohne zusätzliches Wartungsfenster geändert werden.

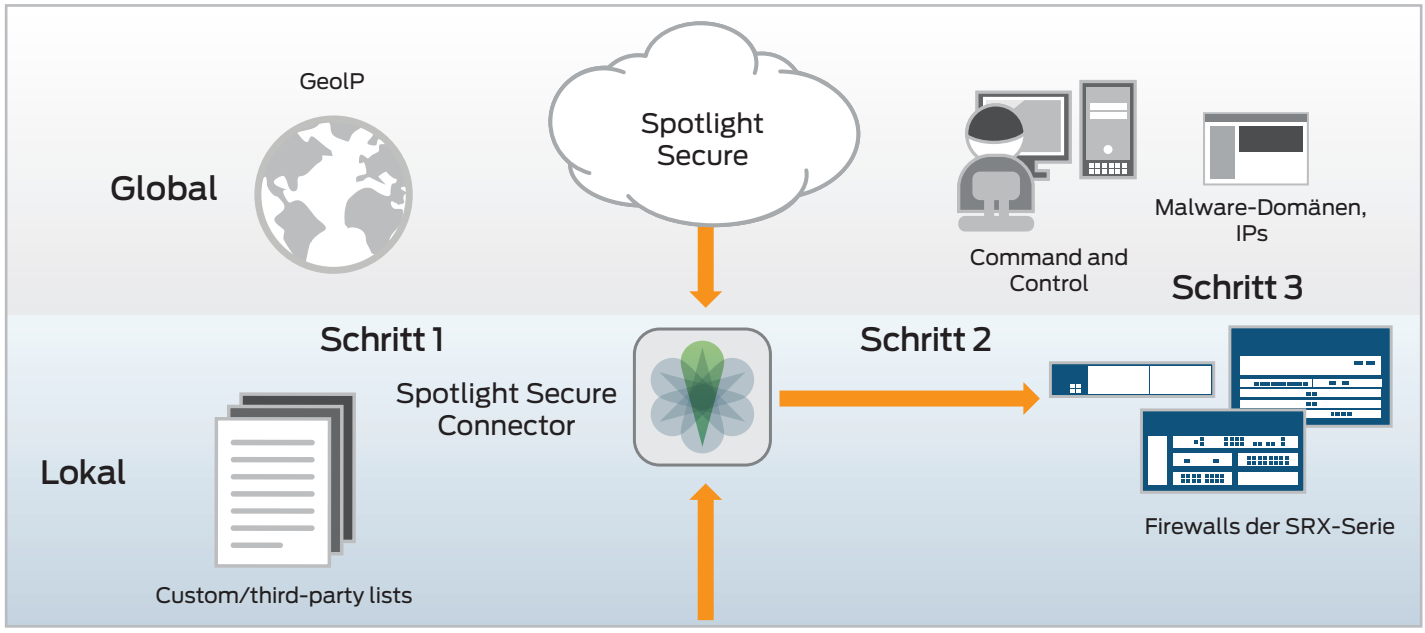


Abbildung 1: Die SRX-Serie mit Security Intelligence basiert auf der Integration mit Spotlight Secure und Spotlight Secure Connector

## Funktionen und Vorteile der Juniper Lösung

| Funktion der Security Intelligence-Lösung von Juniper | Beschreibung | Vorteile |
|---|---|---|
| Skalierbares und offenes Security Intelligence-Framework | • Aggregation und Steuerung der Bedrohungserkennungsdaten vor Ort.<br>• Möglichkeit zum Hinzufügen neuer Feeds mit Bedrohungsdaten, einschließlich benutzerdefinierter Feeds und anderer Datenarten, für einen höheren Schutz vor neuen Bedrohungen dank des erweiterbaren Frameworks.<br>• Kontrolle über die Aktualisierungsraten von Daten-Feeds beim Kunden.<br>• Zukunftssicheres Design dank der Erweiterbarkeit mit neuen Technologien. | • Bedarfs- und anwendungsfallgerechte Anpassungsfähigkeit für mehr Sicherheit und operative Flexibilität<br>• Einfache und flexible Anwendung von Data-Feeds für bedarfsorientierte Richtlinien |
| Umsetzbare erkenntnisgestützte Sicherheitsdaten, die dynamisch in Firewall-Richtlinien der SRX-Serie integriert werden können | • Feeds mit Bedrohungserkennungsdaten, die durch Aggregation der Daten auf Appliances der SRX-Serie schnell einsetzbar sind.<br>• Höhere Zuverlässigkeit im Vergleich zu anderen Lösungen auf dem Markt aufgrund weniger falsch positiver Alarme.<br>• Umsetzbare Erkenntnisse aufgrund der Schweregradbewertung von Bedrohungen.<br>• Optimiert für den Einsatz auf Firewall-Geräten der SRX-Serie. | • Eliminierung der Notwendigkeit einer manuellen Aggregation und Bereinigung von Bedrohungserkennungsdaten durch den Kunden vor der Nutzbarkeit der Daten<br>• Effektiver und zeitnaher Schutz vor neuen Bedrohungen unter Berücksichtigung der Netzwerkumgebung und Ihrer individuellen Anforderungen |
| Dynamische Aktualisierung von Adressgruppen | • Kein Angewiesensein auf statische Adresslisten für die Überwachung oder Blockierung.<br>• Die SRX-Serie nutzt eine dynamische Aktualisierung von Adressgruppen anhand von benutzerdefinierten Feeds, die entweder vom Administrator oder von GeoIP-Daten stammen, die über Spotlight Secure bereitgestellt werden. | • Reduziert den operativen Aufwand für Sicherheitsadministratoren<br>• Erhöht die betriebliche Effizienz |
| Optimierte Implementierung sorgt für bestmögliche Ressourcennutzung und echten Mehrwert für den Kunden | • Die SRX-Serie bietet Unterstützung für ein hohes Volumen an Daten-Feed-Einträgen (bis zu 1 Million Einträge von Daten-Feeds auf einer einzelnen Firewall).<br>• Kunden haben die Möglichkeit, Bedrohungen Prioritäten zuzuweisen, um so die maximale Nutzung von Firewall-Ressourcen mithilfe von Spotlight Secure Connector sicherzustellen. | • Bietet die für den heutigen Bedrohungsschutz erforderliche Leistung |
| Flexible, zentrale Richtlinienkonfiguration und Verwaltung der Firewall-Richtlinien | • Einfache zentrale Verwaltung von Juniper Firewall, IPsec VPN, IPS, UTM, NAT und Bedrohungserkennungsrichtlinien über Junos Space Security Director. | • Ermöglicht Support und Verwaltung auch bei Bereitstellungen im großen Maßstab<br>• Einheitliche Richtlinien auf allen Firewalls der SRX-Serie |

### Effektive Sicherheitsmaßnahmen sind für die Cloud und das Rechenzentrum von entscheidender Bedeutung

Damit Sie über neue Bedrohungen immer rechtzeitig informiert sind, bietet Juniper für die verteilten Feeds mit Bedrohungsinformationen einen wichtigen kontinuierlichen Mehrwert. Der Feed mit Bedrohungsinformationen von Juniper zeichnet sich insbesondere durch die folgenden Merkmale aus:

- Starke Konzentration auf Command and Control-Datenverkehr (C&C), der mit Malware und Botnets in Zusammenhang steht, und Bedrohungserkennung in Form von IP-Adressen, Domänen und URLs
- Basiert auf zahlreichen Drittanbieter-Datenquellen und Bedrohungsinformationen aus der eigenen Malware-Forschungsabteilung von Juniper
- Stündliche Aktualisierung von Spotlight Secure hält die Daten auf dem neuesten Stand und sorgt dafür, dass die neuesten Bedrohungen blockiert werden
- Die enthaltene Bewertung des Bedrohungsschweregrads für jeden Feed-Eintrag gewährleistet, dass Richtlinien auf der Basis des Schweregrads erstellt und die Lösung für Ihre eigenen Bereitstellungen angepasst werden kann. Dies führt zu einer Reduzierung von falsch positiven Alarmen und höherer Wirksamkeit.

Unsere integrierte Lösung ermöglicht es jedem Gerät der SRX-Serie, auf der Grundlage von verfügbarem Speicher und Ressourcen zu bestimmen, wie viele Daten aufgenommen werden können. Die aktivsten und gefährlichsten Bedrohungen werden von Spotlight Secure Connector priorisiert, sodass eine optimale Nutzung der Firewall-Ressourcen und damit die bestmögliche Bedrohungserkennung erreicht wird.

## Lösungskomponenten

**Services Gateways der SRX-Serie:** Firewalls von Juniper Networks, die Firewall-, IPsec- VPN-, IPS-, AppSecure-, UTM-, NAT- und Bedrohungserkennungsrichtlinien durchsetzen, die auf Spotlight Secure basieren (z. B. C&C, GeoIP) und/oder über Spotlight Secure Connector-Feeds (z. B. von Kunden oder Drittanbietern) bereitgestellt werden. Der wichtigste Punkt: Diese Funktionen arbeiten in Verbindung miteinander und ermöglichen Ihnen, die Sicherheitsdienste auszuwählen, die für Ihre Geschäftsanforderungen entscheidend sind, und diese als Bestandteil eines mehrschichtigen Sicherheitskonzepts anzuwenden.

**Junos Space Security Director:** Die zentrale Verwaltungsplattform für die Verwaltung von Richtlinien der SRX-Serie.

**Hinweis:** Für die Nutzung von Security Director zur Verwaltung der Sicherheitsrichtlinien ist der Einsatz der Junos Space Network Management-Plattform erforderlich.

**Junos Spotlight Secure:** Um mit der sich ständig verändernden Bedrohungslandschaft Schritt halten zu können, sind dynamische Bedrohungserkennungssysteme unerlässlich. Derzeit bietet Juniper über Spotlight Secure, einen Cloud-basierten Dienst zur Bedrohungserkennung, und verwandte Bedrohungserkennungssysteme Feeds mit Bedrohungsinformationen zum Schutz vor zahlreichen Bedrohungen:

- Command and Control-Feeds (C&C): zum Schutz des Netzwerks vor Botnets

- GeoIP-Daten (IP-Adressen, die mit einem geographischen Standort in Verbindung gebracht werden können): zur Beschränkung oder Unterbindung des Datenverkehr mit diesen Standorten aus Geschäftsgründen
- Benutzerdefinierte Feeds mit Bedrohungsdaten (von Kunden oder Drittanbietern stammend): zum spezifischen Schutz vor Bedrohungen für ein spezielles Kunden-/Anwendungsfallszenario. Es kann z. B. eine Liste von IPs/URLs als Teil der Firewall-Richtlinie der SRX-Serie in Form von Blacklists/Whitelists verwendet werden.

**Dynamische Adressgruppen:** Eine IP-Liste, die entweder für „Quell-" oder „Zielobjekte" in einer Regel für die SRX-Serie eingesetzt werden kann. Die Aktualisierung der Adressengruppe erfolgt dynamisch: Da keinerlei Commits oder Konfigurationsänderungen erforderlich sind, können die für die Anwendung von Sicherheitsrichtlinien eingesetzten Adressen ohne zusätzliches Wartungsfenster geändert werden. Für dynamische Adressgruppen werden die folgenden Feeds unterstützt:

- Feeds mit benutzerdefinierten IP-Listen
- GeoIP-Feeds (von Spotlight Secure)

**Spotlight Secure Connector:** Als Erweiterung von Spotlight Secure hin zu Ihrem Standort nimmt Spotlight Secure Connector Feeds von Spotlight Secure und lokalen Quellen auf, die dann an Gateways der SRX-Serie weitergegeben werden, und dient somit als Konsolidierungspunkt, der die Lösung mit Daten versorgt. Die Feeds mit Sicherheitsinformationen, die über Spotlight Secure verfügbar sind, umfassen:

- IPs, Domänen und URLs, die für bösartige C&C- oder Botnet-Aktivitäten bekannt sind: Wenn ein infiziertes Gerät versucht, eine Verbindung zu einen C&C-Server über das Internet aufzubauen, kann die SRX-Serie den Verkehr auf der Grundlage eines Echtzeit-Feeds mit C&C-Zielen, die über Spotlight Secure bereitgestellt werden, unterbinden. Die Feed-Daten werden häufig aktualisiert, dynamisch geladen und erfordern weder Commits noch Konfigurationsänderungen.
- GeoIP-Daten (länderspezifische Zuordnung von IPs)

Spotlight Secure Connector sammelt die folgenden standortspezifischen Sicherheitsinformationen:

- Feeds mit benutzerdefinierten IP-Listen von Kunden oder Dritten (z. B. Konsortien): können aus einer benutzerdefinierten Datei manuell hochgeladen oder über regelmäßige Updates per Webserver konfiguriert werden

## Zusammenfassung: Effektiver Netzwerkschutz ermöglicht ein besseres Kundenerlebnis

Alle Unternehmen dürften übereinstimmend der Meinung sein, dass ein positives Kundenerlebnis eine der wichtigsten geschäftlichen Notwendigkeiten ist und Sicherheit „einfach funktionieren muss", auch wenn neue Bedrohungen auftauchen und der Datenverkehr zunimmt.

Die Sicherheitslösungen für die Services Gateways der SRX-Serie von Juniper wurden von Grund auf mit dem Gedanken konzipiert, für die sich rasch verändernde Bedrohungslandschaft gerüstet und reaktionsfähig zu sein. Darüber hinaus sorgt Juniper durch die zentrale Verwaltung aller Richtlinien der SRX-Serie über die Junos Space Network Management-Plattform für geringeren Zeitaufwand und weniger Komplexität.

Im Endeffekt stellen wir Ihnen eine offene, erkenntnisbasierte Sicherheitslösung bereit, die Sie nach eigenem Bedarf ausbauen und basierend auf Ihren Geschäftsanforderungen erweitern können. Spotlight Secure liefert umsetzbare erkenntnisgestützte Sicherheitsdaten, die direkt für Richtlinien nutzbar sind. Sie können jedoch auch Ihre eigenen Quellen zur Bedrohungserkennung hinzufügen, um flexibel auf sich ändernde Erfordernisse zu reagieren.

### Nächste Schritte

Besuchen Sie www.juniper.net/security, oder wenden Sie sich an einen Vertriebsmitarbeiter von Juniper, um mehr über die Service Gateways der SRX-Serie und die integrierten Security Intelligence-Lösungen zu erfahren.

## Über Juniper Networks

Juniper Networks spezialisiert sich auf Innovationen im Netzwerkbereich. Von Geräten bis hin zu Rechenzentren, von Verbrauchern bis hin zu Cloud-Providern: Die Software, Siliziumtechnologie und Systeme von Juniper Networks eröffnen dem Netzwerk neue Dimensionen. Das Unternehmen ist für Kunden und Partner in aller Welt tätig. Weitere Informationen finden Sie unter **www.juniper.net**.


Unternehmens- und Vertriebshauptsitz

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

Hauptsitz 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


Wenn Sie sich für den Kauf einer Lösung von Juniper Networks interessieren, wenden Sie sich an einen Vertriebsmitarbeiter von Juniper Networks (unter +1-866-298-6428) oder an einen autorisierten Vertriebspartner.




3510517-002-DE Okt. 2014