JUNIPER SKY ADVANCED THREAT PREVENTION

Product Overview

Juniper Sky Advanced Threat Prevention is a cloud-based service that provides complete advanced malware protection. Integrated with SRX Series Services Gateways, Sky Advanced Threat Prevention delivers a dynamic anti-malware solution that can adapt to an ever-changing threat landscape.

Product Description

As malware evolves and becomes more sophisticated, it grows more difficult for conventional anti-malware products to effectively defend against these types of attacks. Juniper Networks® Sky Advanced Threat Prevention (ATP) provides advanced anti-malware and anti-ransomware protection against sophisticated "zero-day" and unknown threats by monitoring ingress and egress network traffic looking for malware and other indicators of compromise. Using a pipeline of technologies in the cloud, Juniper Sky ATP delivers progressive verdicts that assess the risk level of each potential attack, providing a higher degree of accuracy in threat prevention. Hosted securely in the cloud, Juniper Sky ATP integrates with Juniper Networks SRX Series Services Gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Juniper Sky ATP's identification technology uses a range of techniques to quickly identify a threat and prevent an impending attack. These range from rapid cache lookups to identify known files to dynamic analysis using unique deception techniques applied in a sandbox environment to trick malware into activating and self-identifying. Patented machine learning algorithms allow Juniper Sky ATP to adapt and identify new malware in the ever-changing threat landscape. Both web- and e-mail-based attacks are defended, protecting the organization from the most prominent threat vectors.

Using evolving techniques that take into account multiple attributes and behaviors of large datasets, Juniper Sky ATP can also identify zero-day attacks and eliminate threats before an attacker infiltrates the network. Once identified, the malware's signature is recorded in the lookup cache and widely propagated to stop similar attacks in the future.

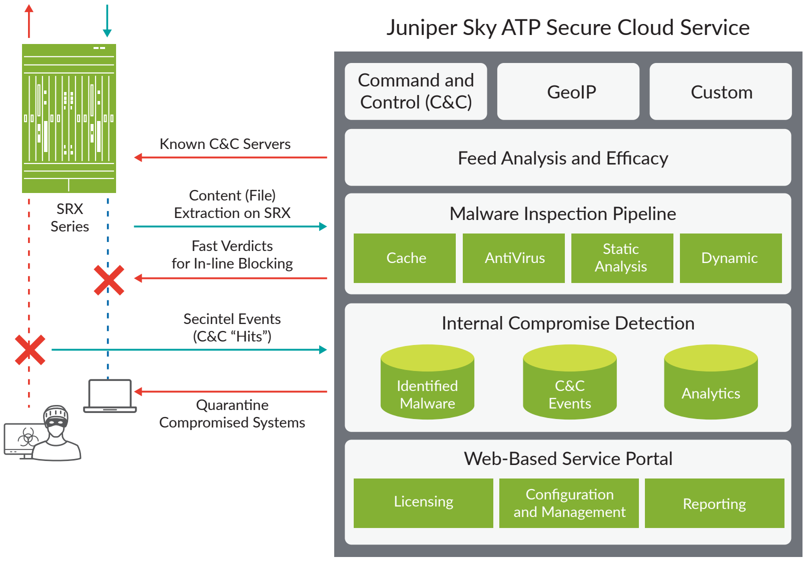
Juniper Sky ATP Secure Cloud Service
Command and Control (C&C)
GeoIP
Custom
Feed Analysis and Efficacy
Malware Inspection Pipeline
Cache
AntiVirus
Static Analysis
Dynamic
Internal Compromise Detection
Identified Malware
C&C Events
Analytics
Web-Based Service Portal
Licensing
Configuration and Management
Reporting
SRX Series
Known C&C Servers
Content (File) Extraction on SRX
Fast Verdicts for In-line Blocking
Secintel Events (C&C "Hits")
Quarantine Compromised Systems

Figure 1: Juniper's Sky Advanced Threat Prevention solution.

Architecture and Key Components

Juniper Sky ATP leverages Juniper's next-generation SRX Series firewall platforms and a cloud-based service component for all management, configuration, and reporting.

Juniper Sky ATP's progressive pipeline analysis engine starts with a cache lookup against a database of known threats. This is accomplished in near real time and facilitates inline blocking of malicious content. Suspicious files are subjected to a series of deeper inspection steps that attempt to positively identify malware. Static analysis combined with processing through multiple antivirus engines attempts to identify the threat; if a file is identified as malware through analysis, its signature is added to the cache to ensure immediate identification of recurring threats in the future.

Finally, dynamic analysis is applied in a sandbox environment, where the threat is "detonated" and observed. Unique deception techniques are employed to elicit malware response and self-identification. Threats that slip by during the more extensive analysis stage are identified, logged, reported, and can be easily mitigated by security operations staff. Infected hosts are automatically isolated and blocked from outbound network access by delivering an "infected host" feed to the SRX Series device.

Juniper Sky ATP supports both web-based and e-mail-borne threats. With the SSL decryption capabilities of the SRX Series firewalls, any malware transmitted in encrypted sessions can also be easily identified. Support for the SMTP and IMAP e-mail protocols allows Juniper Sky ATP to examine e-mails for malicious attachments and even quarantine e-mails that might pose a threat to the end user.

Juniper Sky ATP utilizes public cloud infrastructure to deliver a flexible and scalable solution. All communications between the SRX Series device and the cloud are secure, conducted over encrypted connections on both sides. Files uploaded to the cloud for processing are destroyed afterward to ensure privacy. A detailed description of the Juniper Sky ATP privacy policy, as well as the broader Juniper Networks privacy policy, can be found on the product web portal at https://sky.junipersecurity.net/.

Juniper Sky ATP is available globally with the service delivered from data centers in North America (U.S. and Canada), EMEA, and APAC. This allows customers in these regions to benefit from the Juniper Sky ATP threat prevention and intelligence services while addressing customers' data localization and data privacy concerns. Data submitted in a particular region will be processed in that region, and will not leave the geographic boundaries of the region. Customers have greater control and certainty over the location of the data in order to comply with regulatory and privacy requirements.

Features and Benefits

Integrating with next-generation SRX Series firewalls for detection and enforcement allows Juniper Sky ATP to provide dynamic, automated protection against known malware and advanced zero-day threats, resulting in nearly instantaneous threat responses.

Features and capabilities include:

- Windows 7, Windows 10, and Android operating system support
- Deep analysis and sandboxing support for multiple file types including executables, PDFs, MS Office files, archives, and Flash
- Support for HTTP, HTTPs, SMTP(s), and IMAP(s) protocols
- Comprehensive logging and integration with Juniper Secure Analytics (JSA) and IBM QRadar SIEMs allows rapid threat analysis and incident response
- Integration with Junos Space Security Director (Version 16.1 or later) simplifies security policy management and monitoring using an intuitive centralized interface
- Fast verdict capability that enables the SRX Series firewall to block malicious traffic in inline blocking mode
- Scalable secure cloud infrastructure that, when a threat is discovered, shares updates globally among customers in near real time to block additional attacks
- Patented pipeline of technologies to analyze sophisticated malware, "detonate" files in a controlled sandboxing environment, and identify zero day threats
- Comprehensive API support to programmatically deliver dynamic threat intelligence feeds , upload files for analysis, and manage compromised hosts, enabling easy integration with the larger threat ecosystem
- STIX and TAXII support enable threat intelligence sharing in a standard format
- Integration with endpoint solutions from Carbon Black to consume and share threat intelligence, expanding threat identification and remediation capabilities to endpoints
- Integration with Cloud Access Security Brokers (CASBs) Netskope and CipherCloud to enable advanced threat protection for SaaS applications
- Rich set of curated threat feeds to proactively block outbound command and control (C&C) communication
- Full-featured, web-based portal to provision, monitor, and manage services, as well as a rich set of reports and analytics to provide customers with deep visibility into threats and potentially compromised hosts
- Ability to upload suspicious files through the Web UI for processing

- Deep analytics that identify compromised systems; this information is propagated to SRX Series firewalls via infected host feeds to quarantine compromised systems in near-real time
- Inspection of all e-mail attachments for malware; Sky Advanced Threat Prevention supports the SMTP and IMAP* e-mail protocols and offers flexible policy enforcement options including quarantine and Tag-and-Deliver, while admin and end-user notifications ensure a full lifecycle workflow and superior user experience
- Ability to whitelist/blacklist specific file hashes
- Easy one-click integration of third-party feed sources such as Office 365, Tor, etc.; enable new use cases by referencing these feeds in firewall policies
- Ability to track infected endpoints by MAC address and account for changing IP addresses using the Juniper Networks Policy Enforcer component (for more information, please read the Policy Enforcer data sheet)

* Note: E-mail (IMAP) scanning is only supported on the SRX1500, SRX5000 line, and SRX4000 line of Services Gateways at this time.

Product Options

Juniper Sky ATP is available in two forms: Premium, which offers full advanced malware protection; and Basic, which provides threat feeds only. Customers who do not require full file-based advanced malware protection can purchase the Basic version to protect their organizations from botnets, command and control, phishing, and other attacks that can be addressed using threat intelligence feeds. Customers who want full protection from sophisticated malware, which requires content inspection, should purchase the Premium offering. The two versions are described in Table 1.

A free version of Juniper Sky ATP is also available for existing customers of supported SRX Series devices with a valid software support contract. The free download supports executable processing and infected host feeds. To obtain the free Juniper Sky ATP download, visit https://www.juniper.net/us/en/dm/free-sky-atp/.

Table 1: Juniper Sky Advanced Threat Prevention versions

	Basic (threat feeds only)	Premium
Core functionality	Command and Control, GeoIP, and custom feeds; no file processing or advanced malware protection	Full functionality including advanced file processing for HTTP, HTTPs, and SMTP (e-mail) protocols; includes Command and Control, GeoIP, and custom feeds
APIs	Threat Intelligence APIs only	All APIs including File/Hash
Infected host feed/endpoint quarantine	Not available	Included
Monitoring and management	Juniper Sky ATP web portal and Junos Space Security Director	Juniper Sky ATP web portal and Junos Space Security Director
Supported platforms	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4000 line, SRX5000 line, vSRX	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4000 line, SRX5000 line, vSRX
Licensing	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year
Sample SKU naming convention	SRX1500-THRTFEED-1	SRX1500-ATP-1

Ordering Information

Basic Sky Advanced Threat Prevention (Threat Feeds Only)

Product Number	Description
SRX300-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX300
SRX300-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX300
SRX300-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX300
SRX320-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX320
SRX320-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX320
SRX320-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX320
SRX340-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX340
SRX340-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX340
SRX340-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX340
SRX345-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX345
SRX345-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX345
SRX345-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX345
SRX550-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX550M
SRX550-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX550M
SRX550-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX550M
SRX1500-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX1500
SRX1500-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX1500
SRX1500-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX1500
SRX4100-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4100
SRX4100-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4100
SRX4100-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4100
SRX4200-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4200
SRX4200-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4200
SRX4600-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4600
SRX4600-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4600
SRX4600-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX4600
SRX5400-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5400
SRX5400-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5400
SRX5400-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5400
SRX5600-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5600
SRX5600-THRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5600
SRX5600-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5600
SRX5800-THRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5800
SRX5800-THRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on SRX5800
VSRX10MTHRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 10Mbps
VSRX10MTHRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 10Mbps
VSRX10MTHRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 10Mbps
VSRX100MTHRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 100Mbps
VSRX100MTHRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 100Mbps
VSRX100MTHRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 100Mbps
VSRX1GTHRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 1Gbps
VSRX1GTHRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 1Gbps

Product Number	Description
VSRX1GTHRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 1Gbps
VSRX2GTHRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 2Gbps
VSRX2GTHRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 2Gbps
VSRX2GTHRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 2Gbps
VSRX4GTHRTFEED-1	One Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 4Gbps
VSRX4GTHRTFEED-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 4Gbps
VSRX4GTHRTFEED-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention Threat Intelligence Feeds only (no file processing) on vSRX 4Gbps

Premium Sky Advanced Threat Prevention

Product Number	Description
SRX300-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX300
SRX300-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX300
SRX320-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX320
SRX320-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX320
SRX340-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX340
SRX340-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX340
SRX340-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX340
SRX345-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX345
SRX345-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX345
SRX345-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX345
SRX550-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX550M
SRX550-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX550M
SRX550-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX550M
SRX1500-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX1500
SRX1500-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX1500
SRX1500-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX1500
SRX4100-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4100
SRX4100-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4100
SRX4100-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4100
SRX4200-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4200
SRX4200-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4200
SRX4200-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4200
SRX4600-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4600
SRX4600-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4600
SRX4600-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX4600
SRX5400-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5400
SRX5400-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5400
SRX5600-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5600
SRX5600-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5600
SRX5600-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5600
SRX5800-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5800
SRX5800-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5800
SRX5800-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on SRX5800
VSRX-10M-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-10M-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-10M-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-100M-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on 100Mbps vSRX
VSRX-100M-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on 100Mbps vSRX
VSRX-1G-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-1G-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-1G-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-2G-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-2G-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-2G-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-4G-ATP-1	One Year Subscription for Juniper Sky Advanced Threat Prevention on 4Gbps vSRX
VSRX-4G-ATP-3	Three Year Subscription for Juniper Sky Advanced Threat Prevention on 4Gbps vSRX
VSRX-4G-ATP-5	Five Year Subscription for Juniper Sky Advanced Threat Prevention on 4Gbps vSRX

Note: AppSecure functionality on SRX Series devices is a prerequisite for the Juniper Sky ATP feature. Depending on the SRX Series platform, a separate license may be required to enable AppSecure. Please consult the specific SRX Series platform datasheet for the most accurate information.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700

JUNIPER NETWORKS | **Engineering** Simplicity