Policy Enforcer

Product Overview

Juniper's Software-Defined Secure Network (SDSN) platform leverages the entire network, not just perimeter firewalls, as a threat detection and security enforcement domain. Policy Enforcer, a component of Junos Space Security Director, enforces threat remediation and microsegmentation policies on Juniper virtual and physical SRX Series firewalls, EX Series and QFX Series switches, MX Series routers, third-party switch and wireless networks, private cloud/SDN solutions like Contrail and VMware NSX, and public cloud deployments. Juniper Sky ATP's cloud-based malware detection, Command and Control, and GeoIP identification feeds, along with trusted custom feeds, act as threat detection mechanisms for Policy Enforcer to orchestrate remediation workflows.

Product Description

Recent attacks on corporate networks have exposed the shortcomings of traditional "perimeter only" security architectures, proving that they are insufficient for providing complete and holistic protection. There are several key reasons why perimeter only solutions are inadequate:

- A single application or endpoint breach inside the perimeter leaves the entire network vulnerable because attacks inside the perimeter cannot be blocked.
- Networks are completely vulnerable to insider attacks. Malware-infected endpoints are best isolated at the source of network connectivity to limit the possibility of lateral attack propagation.
- When an internal attack moves laterally inside an organization, visibility and intelligence from perimeter devices show no evidence of malicious activity. Without this visibility, it is impossible for security teams to effectively secure the network.

Juniper Networks® Software-Defined Secure Network (SDSN) offers a holistic approach that addresses these security concerns. Specifically, Juniper's SDSN delivers:

- **Pervasive Security:** Juniper's SDSN enables pervasive security across the entire network using switches, routers, and security devices—physical and virtual—for on-premise scenarios, leveraging SDN solutions such as Juniper Networks Contrail and VMware NSX to orchestrate networking functionality where needed, along with applications hosted in public cloud platforms such as Amazon Web Services (AWS). Each network element can also act as a security sensor, providing visibility into and intelligence about intra- and inter-network communications.
- **User Intent-Based Policy**: A simplified policy framework based on business-oriented items such as users, user groups, geographic locations, devices, sites, tenants, applications, and threats, this solution allows switches, routers, firewalls, and other network devices to work in concert by sharing data and resources, orchestrating remediation actions within the network.
- **Threat Intelligence Aggregation:** Juniper's SDSN provides the ability to aggregate threat information from multiple local (such as security information and event management), cloud-based (such as Sky Advanced Threat Prevention), and even third-party threat detection solutions.

Policy Enforcer, a component of Junos® Space Security Director, provides a simpler user intent-based threat management policy modification and distribution tool that allows updated policies to be deployed on Juniper Networks EX Series Ethernet Switches and QFX Series switches, as well Juniper virtual and physical SRX Series Services Gateways.

Architecture and Key Components

Secure Network

Policy Enforcer provides an abstraction called the Secure Network that includes perimeter firewalls as well as switches that connect applications and users. The Secure Network acts as a coherent system representing a specific location, such as a branch office, and the security and networking devices deployed at that location, detecting network activity and enforcing specified policies. In public cloud scenarios, a secure network represents a Virtual Private Cloud (VPC). An additional abstraction called Policy Enforcement Groups, representing business entities such as users and applications, support network-independent user intent-oriented policies.

Advanced Threat Prevention

Juniper's cloud-based Sky Advanced Threat Prevention (ATP) solution provides multiple threat feeds, including:

- Command and Control (C&C), which identifies known malicious command and control sites
- Geo IP, which identifies the geographical locations of different entities on the Internet
- Malware, which identifies known malware threats
- Infected host, which provides a list of infected internal hosts based on advanced machine learning techniques

The Policy Enforcer natively integrates with Sky Advanced Threat Prevention, orchestrating security workflows to protect both perimeter-oriented traffic as well as lateral threat propagation within the network. It also supports a custom feeds option, allowing users to leverage solutions other than Juniper Sky ATP as their trusted threat feed source. Multiple types of custom feeds are supported for granular threat remediation purposes, including:

- Dynamic Address: A dynamic group of IP addresses that can be used in security policies.
- Whitelist: Known and trusted IP addresses, URLs, and domains.
- Blacklist: Known, untrusted IP addresses, URLs, and domains.
- Infected Host: Hosts that are known to be infected and compromised.
- DDoS: Lists of known attacking hosts as well as their internal targets.

It also provides security operators with the granular control required to take automated remediation actions depending upon the severity of the threat. These can include perimeter firewall-related actions like deny or log traffic, network switch-related actions like quarantine of infected hosts, router-related actions like updates to BGP Flowspec, SDN-related actions like dynamic security service chaining, or public cloud-related actions like updates to security groups.

Infected Host Tracking

The mobility of infected endpoints and the resulting change in network IP addresses can easily circumvent security in perimeter-only protection architectures. When an endpoint IP address gets reassigned due to user mobility, Policy Enforcer keeps track of infected host movement and enforces consistent security both pre- and post-mobility, delivering a coherent system that makes it difficult to circumvent security policies.

Custom Threat Feed Management

Federal, financial, retail, and other security-sensitive customers subscribe to custom threat feeds from different sources to keep up with the ever-changing threat landscape. In addition, Security Information and Event Management (SIEM), honeypots, and other security analytics solutions provide threat feeds to the security teams. Policy Enforcer exposes a RESTful API that these custom feeds can leverage when enforcing relevant controls across the secure network.

VMware NSX Support

Security Director Policy Enforcer integrates with VMware NSX for microsegmentation use cases, allowing enterprises to configure a single policy covering both physical and virtual SRX Series firewalls deployed on the perimeter, as well as vSRX virtual firewalls natively integrated with NSX for east-west traffic inside the data center. In addition, Policy Enforcer applies NSX security tags to virtual machines identified as infected with malware or Command and Control activity, enabling NSX to trigger host-based security controls such as dynamic virus scans, network security controls like enabling IPS, or both.

Juniper Contrail Support

Security Director Policy Enforcer integrates with Juniper Contrail for microsegmentation, allowing enterprises to configure a single policy covering both physical and virtual SRX Series firewalls deployed on the perimeter, as well as vSRX virtual firewalls natively integrated with Contrail for east-west traffic inside the data center. In addition, Policy Enforcer can quarantine end points identified as infected with malware or Command and Control activity, mitigating lateral threats inside the network.

Amazon Web Services Support

Security Director Policy Enforcer integrates with AWS for workload discovery, allowing enterprises to configure a dynamic workload metadata-based policy that is always kept up-to-date without requiring security administrators to manually update the VM inventory in Security Director. In addition, Policy Enforcer updates AWS Security Groups for the VMs identified as infected with malware or command and control activity, mitigating lateral threats inside the network.

Extensible SDSN Ecosystem

Policy Enforcer supports an extensible framework whereby third party security vendors can integrate and deliver advanced security capabilities. Scenarios include integration with third-party NAC vendors for threat remediation on endpoints connected to non-Juniper networking equipment and integration with endpoint security vendors for threat remediation directly at the infected endpoint level, among others.

Features and Benefits

Table 1: Policy Enforcer Features and Benefits

Feature	Description	Benefits
Infected Host Blocking	Blocks traffic based on threat information provided by Juniper Sky Advanced Threat Prevention	In addition to blocking traffic from infected entities on the perimeter firewalls, customers can take network-oriented actions like quarantining to contain lateral threat movement inside the network.
Infected Host Tracking	Addresses change of common network identity-related issues due to user and application mobility	Enforces consistent security policies for the entities even when the underlying network identity (such as IP address) changes for the infected hosts. The secure network tracks infected host movement across the network to identify attempts to circumvent security controls.
Custom Threat Feed	Integrates custom/third-party threat feeds into the SDSN framework for automated incident response	Leverages existing customer investments in trusted third-party threat feeds to enforce controls using Juniper solutions.
Metadata-Based Dynamic Access Control Policies	Provides cloud-ready policy model enabling agile workloads common in private and public cloud deployments	Implements consistent security policy model that supports on-premises as well as different cloud deployments, reducing the operational costs of maintaining different rule sets for different domains.
Microsegmentation for Private Cloud Deployments	Integrates with VMware NSX and Juniper Contrail SDN platforms for private cloud workload segmentation	Provides advanced security with granular segmentation for application workloads in private clouds, leveraging integration with Juniper Contrail and VMware NSX platforms.
Public and Private Cloud Workload and Metadata Discovery	Discovers dynamic cloud workloads, including cloud-specific metadata	Delivers up-to-date policies on firewalls, even for agile and dynamic workloads, reducing the time required to support security for cloud workloads.
Threat Mitigation for Private and Public Cloud Deployments	Integrates with AWS, VMware NSX, and Juniper Contrail Cloud platforms for multicloud threat remediation	Identifies infected application components wherever the application may be running, mitigating lateral threat propagation inside the network.
DDoS Mitigation	Integrates with Juniper MX Series routers	Updates BGP Flowspec on MX Series routers to mitigate active DDoS attacks forwarding traffic to scrubbing centers or blocking traffic from reaching victim hosts inside the network.
Monitoring Dashboards	Offers threat-related dashboards for easy identification of the entire network's threat posture	Allows customers to clearly see the threats entering their network, as well as infected endpoints, at any time.
RESTful APIs for Automation	Provides RESTful APIs that can be used in conjunction with automation tools	Automates configuration and management of physical, logical, or virtual SRX Series devices, and the security features on EX Series and QFX Series switches.

Specifications

Table 2 captures the Sky Advanced Threat Prevention threat feeds supported on different versions of Juniper SRX Series Services Gateways in the latest release of Policy Enforcer.

Table 2: Supported Sky Advanced Threat Prevention Threat Feeds on SRX Series Devices

Models/Platform	Junos Software Version	Supported Threat Feeds
vSRX: 2 VCPUs, 4 GB RAM (server requirements)	Junos 15.1X49-D60 and above	CC, AntiMalware, Infected Hosts, GEO IP
SRX4100, SRX4200	Junos 15.1X49-D65 and above	CC, AntiMalware, Infected Hosts, GEO IP
SRX4600	Junos 15.1X49-D110 and above	CC, AntiMalware, Infected Hosts, GEO IP
SRX340, SRX345, SRX550M, SRX1500	Junos 15.1X49-D60 and above	CC, AntiMalware, Infected Hosts, GEO IP
SRX5400, SRX5600, SRX5800	Junos 15.1X49-D62 and above	CC, AntiMalware, Infected Hosts, GEO IP
SRX550, SRX650, SRX1400	Junos 12.1X46-D25 and above	CC, GEO IP
SRX300, SRX320	Junos 15.1X49-D90 and above	CC, GEO IP

Similarly, different modes of Policy Enforcer deployments are supported on different Juniper EX Series and QFX Series switch platforms as shown in Table 3.

Table 3: Supported Policy Enforcer Deployment Modes on EX Series and QFX Series Devices

Models	Junos Software Version	Supported Policy Enforcer Modes
EX2200, EX3300, EX4200	Junos 15.1R1.5 and above	Juniper Sky ATP with PE (part of Secure Fabric)
EX4300, EX9200	Junos 14.1X53-D30 and above	Juniper Sky ATP with PE (part of Secure Fabric)
EX2300, EX3400	Junos 15.1X53-D50 and above	Juniper Sky ATP with PE (part of Secure Fabric)
QFX5100, QFX5200, vQFX	Junos 14.1X53-D40 and above	Juniper Sky ATP with PE (part of Secure Fabric)

Policy Enforcer supports threat remediation for end points connected to third-party switch platforms as shown in Table 4.

Table 4: Supported Third-Party Switch Platforms*

Models	Software Version	Supported Policy Enforcer Modes
Cisco ISE	2.1 and above	Sky ATP with PE (part of Secure Fabric)
HP Aruba Clearpass	6.0 and above	Sky ATP with PE (part of Secure Fabric)
Forescout CounterAct	7.0 and above	Sky ATP with PE (part of Secure Fabric)

* Specific switch and wireless devices is based on the NAC solution capabilities.

Policy Enforcer integration with MX Series routers requires the following components detailed in Table 5.

Table 5: MX Series Support for DDoS

Models	Software Version	Supported Policy Enforcer Modes
Juniper MX Series physical and vMX virtual routers	Junos 14.2R1 and above	DDoS mitigation with BGP Flowspec

Policy Enforcer integration with VMware NSX requires the following components, detailed in Table 6.

Table 6: VMware NSX Support

Models	Software Version	Supported Policy Enforcer Modes
VMware NSX	6.3.1	Microsegmentation and threat remediation with vSRX
VMware vCenter and ESXi	6.0.0	Microsegmentation and threat remediation with vSRX
vSRX version	15.1X49-D100	Microsegmentation and threat remediation with vSRX

Policy Enforcer integration with Juniper Contrail requires the following components, detailed in Table 7.

Table 7: Juniper Contrail Support

Models	Software Version	Supported Policy Enforcer Modes
Juniper Contrail	5.0	Microsegmentation and threat remediation with vSRX
vSRX version	15.1X49-D100	Microsegmentation and threat remediation with vSRX

Policy Enforcer for public cloud requires the following components detailed in Table 8.

Table 8: AWS Support

Models	Software Version	Supported Policy Enforcer Modes
vSRX version	15.1X49-D100	vSRX policy based on workload discovery

Client Browser Support

Security Director and Policy Enforcer are best viewed on the following browsers:

- Google Chrome v.54x and above
- Internet Explorer v.11 on Windows 7
- Firefox v.46 and above

VMware Version

Junos Space works with VMware vSphere 4.0 and above.

Junos Operating System Software

The SRX Series Services Gateways run Junos OS software. Junos Space Security Director runs on Juniper devices running Junos OS 10.3 and later releases.

Junos Space Network Management Platform

Junos Space Security Director 16.1 runs on Junos Space 16.1.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

Junos Space Appliance

Junos Space Virtual Appliance includes the complete Junos Space software package as well as the Junos OS operating system. It requires users to create a virtual machine in order to deploy the appliance. The recommended specifications for the virtual machine are identical to the specifications of the physical appliance. See www.juniper.net/documentation/en_US/junos-space14.1/topics/concept/junos-space-virtual-appliance-overview.html.

Product Number	Description
JA2500-A-BSE	Base Appliance

Policy Enforcer

The Policy Enforcer software is licensed based on the number of networking and security devices you will manage in the Secure Network. For example, if you will be managing up to 20 SRX Series firewalls and 80 EX Series switches, then you would purchase a single license for SDSN-PE-100. In the case of AWS, each VPC that leverages vSRX as the gateway will use two device units—one for the vSRX and one for the VPC itself—in order to address the threat remediation and workload discovery scenarios.

Note: You do not need to purchase a separate license for high availability (HA).

The following licenses enable customers to procure both Policy Enforcer as well as Security Director. These licenses are for customers who do not have Security Director.

Product Number	Description
SDSN-PE-50	Policy Enforcer for 50 networking and security devices. Includes Security Director entitlement.
SDSN-PE-100	Policy Enforcer for 100 networking and security devices. Includes Security Director entitlement.
SDSN-PE-500	Policy Enforcer for 500 networking and security devices. Includes Security Director entitlement.
SDSN-PE-1000	Policy Enforcer for 1000 networking and security devices. Includes Security Director entitlement.

Existing Security Director customers interested in Policy Enforcer as an add-on should use the following licenses:

Product Number	Description
SDSN-PE-ADD-ON-50	Policy Enforcer add-on license for 50 networking and security devices for existing Security Director deployments
SDSN-PE-ADD-ON-100	Policy Enforcer add-on license for 100 networking and security devices for existing Security Director deployments
SDSN-PE-ADD-ON-500	Policy Enforcer add-on license for 500 networking and security devices for existing Security Director deployments
SDSN-PE-ADD-ON-1K	Policy Enforcer add-on license for 1000 networking and security devices for existing Security Director deployments

For private cloud scenarios (VMware NSX and Juniper Contrail), Policy Enforcer is provided as a bundle that includes a vSRX Virtual Firewall, an Advanced Security subscription, and management components.

The following table lists the licenses needed for VMware NSX integration.

Product Number	Description
JNSX-ADS-1-1Y	Juniper SDSN for NSX Advanced Security with vSRX for 1 physical CPU socket—1 year subscription. License includes support for Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with AppSecure and IDP feature support.
JNSX-ADS-1-3Y	Juniper SDSN for NSX Advanced Security with vSRX for 1 physical CPU socket—3 year subscription. License includes support for Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with AppSecure and IDP feature support.
JNSX-ADS-1-5Y	Juniper SDSN for NSX Advanced Security with vSRX for 1 physical CPU socket—5 year subscription. License includes support for Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with AppSecure and IDP feature support.

The following table lists the licenses needed for Contrail integration:

Product Number	Description
JCNTR-ADS-1-1Y	Juniper SDSN for Contrail Advanced Security with vSRX for 1 physical CPU socket—1 Year subscription. Includes Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with ASEC and IPS.
JCNTR-ADS-1-3Y	Juniper SDSN for Contrail Advanced Security with vSRX for 1 physical CPU socket—3 Year subscription. Includes Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with ASEC and IPS.
JCNTR-ADS-1-5Y	Juniper SDSN for Contrail Advanced Security with vSRX for 1 physical CPU socket—5 Year subscription. Includes Security Director, Policy Enforcer, 1 vSRX entitlement for 1 physical CPU socket protection with ASEC and IPS.

Policy Enforcer in non-SDSN mode can also function as a threat intelligence platform that aggregates and distributes Command and Control (CC) feeds, GeoIP feeds, and custom feeds. In this mode, the advanced user intent-based policy is not applicable. Similar functionality was first introduced by the Juniper Networks Spotlight Secure product; Policy Enforcer will support such functionality moving forward. Additional information can be found on the Spotlight Secure data sheet.

Existing Spotlight Secure customers using Security Director 15.1 or earlier, and new customers who want to use the “feed-only” functionality, will need to install the Policy Enforcer virtual machine (a free download) and Security Director 16.1. Currently available Spotlight Secure licenses will be valid for such deployments and can be purchased separately. Existing Spotlight Secure customers can reuse the licenses at no additional cost and without requiring any licensing-related procedures.

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
Fax: +1.408.745.2100
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
Fax: +31.0.207.125.701

1000602-005-EN Mar 2018