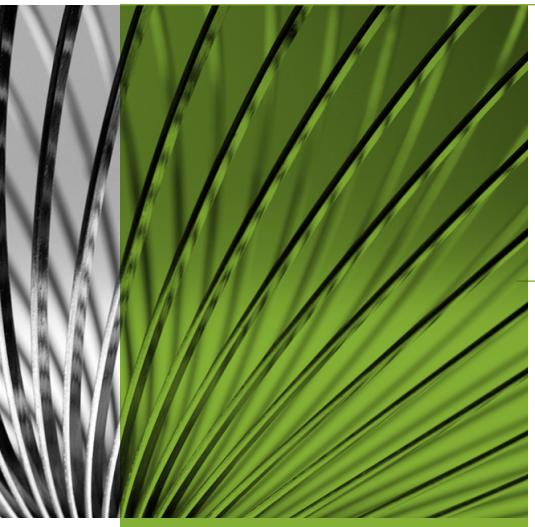

POLICY ENFORCER

Product Overview

Juniper Connected Security 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 ATP Cloud'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

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 entirely vulnerable to insider attacks. Malware-infected endpoints are best isolated at the network connectivity source 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, security teams can't effectively secure the network.

Juniper Networks® Connected Security offers a comprehensive approach that addresses these security concerns. Specifically, Juniper Connected Security delivers:

- **Pervasive Security:** Juniper's Connected Security enables pervasive security across the entire network, supporting both physical and virtual switches, routers, and security devices 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), and Microsoft Azure. Each network element can also act as a security sensor, providing visibility into and intelligence about intra- and inter-network communications.
- **Policy Orchestration:** 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.
- **SecIntel:** Juniper Connected Security provides the ability to aggregate threat information from multiple local (such as security information and event management), cloud-based (such as Juniper ATP Cloud), and even third-party threat detection solutions.

As a component of Junos® Space Security Director, Policy Enforcer provides a more straightforward, user intent-based threat management policy modification and distribution tool. It 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

With Policy Enforcer, information security is controlled and managed by security software. New devices are automatically covered by security policies instead of identifying their IP address as with other solutions. These software-defined, environments can be moved without affecting security policies and controls already in place. Other advantages include:

- **Better and more detailed security.** By providing better visibility into network activity, you can detect and respond faster to cyber threats and other security incidents by leveraging threat intelligence from multiple sources.
- **Scalability and cost savings.** A software-based model allows you to quickly and easily scale security up or down based on your immediate needs, all without having to add or subtract hardware that is expensive to buy and maintain.
- **Simpler solution**. Hardware security architectures can be complex due to the servers and specialized physical devices required. In a software model, security is based on policies. Policy Enforcer protects information anywhere it resides without depending on its physical location.

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 ATP Cloud through SecIntel	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 Connected Security 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 a 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, Google Cloud, Microsoft Azure, VMware, KVM, Hyper-V, 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 see the threats entering their network, as well as infected endpoints, at any time.
RESTful APIs for Automation	Provides RESTful APIs to use 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 Juniper SecIntel threat feeds provided through Juniper ATP Cloud and supported on different Juniper SRX Series Services Gateways in the latest release of Policy Enforcer.

Table 2. Supported Juniper SecIntel Threat Feeds on SRX Series Devices

Models/Platform	Supported Threat Feeds
vSRX: 2 VCPUs, 4 GB RAM (server requirements)	CC, AntiMalware, Infected Hosts, GEO IP
SRX4100, SRX4200	
SRX4600	
SRX340, SRX345, SRX380, SRX550M, SRX1500	
SRX5400, SRX5600, SRX5800	
SRX300, SRX320	CC, GEO IP

Similarly, different Policy Enforcer deployments are supported on other 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	Supported Policy Enforcer Modes
EX2200, EX3300, EX4200, EX4300, EX9200, EX2300, EX3400, QFX5100, QFX5200, vQFX	Juniper ATP Cloud 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	Supported Policy Enforcer Modes
Cisco ISE	ATP Cloud with PE (part of Secure Fabric)
HP Aruba Clearpass	
Forescout CounterAct	

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

Policy Enforcer integration with VMware NSX requires the following components, detailed in Table 5.

Table 5. VMware NSX Support

Models	Supported Policy Enforcer Modes
VMware NSX	Microsegmentation and threat remediation with vSRX
VMware vCenter and ESXi	
vSRX version	

Policy Enforcer integration with Juniper Contrail requires the following components, detailed in Table 6.

Table 6. Juniper Contrail Support

Models	Supported Policy Enforcer Modes
Juniper Contrail	Microsegmentation and threat remediation with vSRX
vSRX version	

Policy Enforcer for public cloud requires the following components detailed in Table 7.

Table 7. AWS Support

Models	Supported Policy Enforcer Modes
vSRX version	vSRX policy based on workload discovery

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 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/product/en_US/security-director. For ordering information, please contact your Juniper sales representative.

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 manage up to 20 SRX Series firewalls and 80 EX Series switches, 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 to address the threat remediation and workload discovery scenarios.

Note: You do not need to purchase a separate license for high availability (HA). For ordering information, please contact your Juniper sales representative.

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: +31.207.125.700