

Junos Network Secure

Product Overview

Product Overview. Junos Network Secure delivers stateful firewall services integrated with the MXSeries 3D Universal Edge Routers to provide protection for the service provider and enterprise network, as well as a revenue-generating managed service that protects customer infrastructure.

Product Description

Juniper Networks® Junos® Network Secure provides a per-flow state table and performs packet inspection, dropping packets that do not comply with the protocol state. Junos Network Secure includes attack detection, which provides anomaly-based attack detection and protection.

Juniper Networks MX Series 3D Universal Edge Routers use Junos Network Secure to track and control the flow of traffic. The stateful firewall capabilities of Junos Network Secure provide an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts. Junos Network Secure groups relevant flows into conversations. A flow is identified by the following five properties:

- Source address
- Source port
- Destination address
- Destination port
- Protocol

Architecture and Key Components

The MX Series 3D Universal Edge Routers Portfolio

The MX Series portfolio of Ethernet services routers is the industry leader for carrier Ethernet capacity, density and performance. Optimized for emerging Ethernet network architectures and services, the MX Series is purpose-built for the most demanding carrier and enterprise applications, and it leverages Juniper Networks Junos operating system to enable carriers and enterprises to seamlessly and cost-effectively deploy Ethernet and accelerate their next-generation network deployments. By combining a best-in-class hardware platform with the reliability and service flexibility of Junos OS, the MX Series delivers a combination of features and capabilities previously unattainable in carrier Ethernet deployments.

Multiservices Cards (MS-MPC, MS-MIC)

MS-MPCs and MS-MICs are next-generation, advanced service modules for Juniper Networks® MX Series 3D Universal Edge Routers. They deliver the performance, services, and scalability that are critical to today's advanced Ethernet services edge and broadband edge networks. MS-MPCs are full slot modules that supply hardware acceleration for an array of packet processing-intensive services for the MX2020, MX2010, MX960, MX480, and MX240 3D Universal Edge Routers. The MS-MIC is based on Juniper's MIC card hardware form and can be inserted in the MX5, MX10, MX40, and MX80 3D Universal Edge Routers, as well as the MPC1, MPC2, and MPC3 cards.

These cards offer flexible support for stateful firewall, Network Address Translation (NAT), IPsec, anomaly detection, flow monitoring and accounting, and tunnel services. This wide array of services enables service providers and enterprises to secure their network infrastructure; collect rich statistics for billing, capacity planning, and security purposes; and create new services, all with a single module.

Features and Benefits

Junos Network Secure can be used to provide stateful firewall services integrated with the MX Series 3D Universal Edge Routers to provide protection for the service provider and enterprise network, as well as a revenue-generating managed service that protects customer infrastructure. Traffic from any ingress port can be classified and routed to the stateful firewall and then either dropped or forwarded from the proper egress port. This integration allows customers to eliminate external firewalls that consume router ports and additional management resources. Alternately, the integrated firewall function can be used as a first line of defense in a layered security architecture and can offload bulk stateful filtering from the standalone firewall.

Junos Network Secure evaluates packets in the context of the specific flows to which they belong and performs IP packet integrity checks, enabling the MX Series to identify and isolate malicious payloads slipped into active data streams. It also performs statistical modeling to identify unusual traffic patterns such as denial of service/distributed denial of service (DoS/DDoS), network scanning or probing. This powerful solution identifies and isolates a wide range of attacks including DOS attacks (such as SYN flood); network-level attacks such as IP fragmentation or Internet Control Message Protocol (ICMP) "ping of death" attacks; and transport layer attacks such as port scans or teardrop attacks.

The stateful firewall function also supports ALGs for special handling of unique protocols such as H.323, FTP, Session Initiation Protocol (SIP) and ICMP.

Specifications and Approvals

For a complete list of supported software features, please consult the Junos OS documentation at www.juniper.net/techpubs/software.

Junos Network Secure offers the following firewall services:

- Stateful packet filtering (IPv6)—Maintain per-flow state table, allow packets matching criteria
- Packet inspection for a variety of IP values (for example, length, checksum, fragmentation)

- Higher layer state checks including TCP
- Detection and protection against a variety of types of attacks (see following)
- Tracking of "Top Talkers" based on sessions or bandwidth usage based on particular flows, src/dst IP addresses and endpoint pairs
- Anomaly tables for tracking sites under attack or potential hackers
- Support for application layer gateway (ALG) algorithms

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

Model Number	Description
MS-MIC-16G	MS-MIC with 16 GB of memory, occupies single MIC slot on MX5, MX10, MX40, and MX80 3D Universal Edge Routers, as well as on the MPC1, MPC2, and MPC3 cards for the MX2020, MX2010, MX960, MX480, and MX240 3D Universal Edge Router.
MS-MPC	MS-MPC with 128 GB of memory (32 GB per NPU) occupies a single slot in MX2020, MX2010, MX960, MX480, and MX240 3D Universal Edge Routers
JNSFW	Junos Network Secure [Stateful Firewall]

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

JUNIPER
 NETWORKS