

Juniper Networks NetScreen-ScreenOS 4.0 MCAST

- **Policy-based control and protection for multicast transmissions for both firewall and VPN environments**
- **Maintains dynamic nature of multicast delivery across administrative boundaries and network domains with support for IGMP, PIM-SM and PIM Rendezvous Point Proxy**
- **IGMP and PIM are University of New Hampshire (UNH) certified to help ensure that NetScreen devices will interoperate with existing networking components**

Product overview

Delivering multimedia content across today's busy networks presents IT departments with a unique set of security and traffic management challenges: how to deliver rich, multimedia content to the target audience without overloading the network with unnecessary traffic while maintaining tight network security. Juniper Network's high performance security solutions are able to satisfy these critical requirements through support for industry standard multicast routing protocols and technologies.

Juniper combines policy-based security management with support for multicast to provide organizations such as the financial services industry, universities and government agencies with the ability to maintain their global security policies while delivering rich, multimedia content to a targeted group of individuals. Juniper Network's granular policy-based security allows an IT department to manage network security while adding yet another layer of control over who can or cannot receive multicast transmissions.

Unlike some security solutions that either require multiple components to perform multicast delivery or circumvent network security by re-routing multicast deliveries around the firewall, Juniper combines powerful multicast routing capabilities with world class security to provide a one-box solution that meets the needs of today's demanding networking environments.

Policy-based control

Using Juniper's policy-based management capabilities, IT departments can tightly control the networking and security in a single interface, thereby minimizing the number of configuration errors that may lead to security holes. Juniper's policy-based management capabilities include:

- Grant or deny which data streams can traverse the network and/or which hosts can join specific multicast groups
- IP address conflict avoidance through group address translations that allow internal and external streaming applications to use the same group address without conflict

- Delivery of multicast transmissions across IP networks that do not support multicast
- The ability to encapsulate, encrypt and non-repudiate multicast transmissions
- Traffic management with guaranteed bandwidth, maximum bandwidth and prioritization capabilities

High Availability

Juniper Network's NetScreen ScreenOS Multicast is fully compatible with the Juniper Network's NetScreen High Availability (HA), one of the most comprehensive HA security solutions today. With the NetScreen HA, multicast networks can be deployed in Active/Passive, Active/Active or Active/Active Full Mesh modes – all with Stateful firewall and VPN fail-over. NetScreen HA functionality provides sub-second fail-over between interfaces or devices while maintaining session/connection state information, security associations, configuration changes and more for both firewall and VPN.

Multicast platform support

Juniper Networks NetScreen ScreenOS 4.0-MCAST is currently available on the following platforms:

- NetScreen-5200 8G
- NetScreen-204/208
- NetScreen-50
- NetScreen-5XT

For platform ordering data, dimensions and other specifications, please contact your local sales representative or review the respective Juniper product datasheets.

	Juniper Networks NetScreen-5200 8G ⁽¹⁾	Juniper Networks NetScreen-500 ⁽¹⁾	Juniper Networks NetScreen-200 Series ⁽¹⁾	Juniper Networks NetScreen-50 ⁽¹⁾	Juniper Networks NetScreen-5XT ⁽¹⁾
Maximum Performance and Capacity					
Concurrent sessions	1,000,000	250,000	128,000	32,000	2,000
New sessions/second	25,000	17,000	13,000	7,000	2,000
Firewall performance	4 Gbps	700 Mbps	400 or 550 Mbps	170 Mbps	70 Mbps
3DES (168 bit)	2 Gbps	250 Mbps	200 Mbps	50 Mbps	20 Mbps
Policies	40,000	20,000	4,000	1,000	100
Interfaces	8 mini-GBIC (SX or LX)	Up to 8 10/100 or Mini-GBIC (SX or LX), up to 4 GBIC (SX or LX)	4 or 8 10/100 Base-T	4 10/100 Base-T	5 10/100 Base-T
Virtualization					
Maximum number of Virtual Systems	500	25	N/A	N/A	N/A
Maximum number of security zones	1000	8 default, up to 50 custom	8 default, 18 maximum with virtualization key	4 user definable	2
Maximum number of virtual routers	500	2 default, up to 25 custom	2 default, 7 maximum with virtualization key	2	2
Maximum number of VLANs	4000	100	0 default, up to 32 with virtualization key	0	0
Mode of Operation					
Transparent mode (all interfaces)	Yes	Yes	Yes	Yes	Yes
Route mode (all interfaces)	Yes	Yes	Yes	Yes	Yes
NAT (Network Address Translation)	Yes	Yes	Yes	Yes	Yes
Home/work zones	No	No	No	No	Yes
Policy-based NAT	Yes	Yes	Yes	Yes	Yes
PAT (Port Address Translation)	Yes	Yes	Yes	Yes	Yes
Virtual IP	8	4	4	2	1
Mapped IP	10,000 – 1,000 per virtual system	4,000 - 256 per virtual system	4,000	1,000	100
Users per port, Trusted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	10 or Unrestricted
Routing					
RIPv2/OSPF/BGP dynamic routing	Yes, up to 8 instances ea.	Yes, up to 8 instances ea.	Yes, up to 2 instances ea.	Yes, up to 2 instances ea.	Yes, up to 2 instances ea.
Routes	20,000	8,192	4,000	2,000	1,000
IGMP (v1, v2)	Yes	Yes	Yes	Yes	Yes
IGMP Proxy	Yes	Yes	Yes	Yes	Yes
PIM-SM	Yes	Yes	Yes	Yes	Yes
Group Address Translation	Yes	Yes	Yes	Yes	Yes
Multicast inside IPSec VPN	Yes	Yes	Yes	Yes	Yes
Max. IGMP Groups	4,000	1,000	600	300	50
Max. MROUTES	8,192	4,096	4,096	2,048	1,024
IP Address Assignment					
Static	Yes	Yes	Yes	Yes	Yes
DHCP client	No	No	Untrusted interface	Untrusted interface	Untrusted interface
PPPoE client	No	No	Untrusted interface	Untrusted interface	Untrusted interface
Internal DHCP server	Interfaces in Trust Zone	Interfaces in Trust Zone	Interfaces in Trust Zone	Interfaces in Trust Zone	All zones but Untrusted
DHCP relay	Yes	Yes	Yes	Yes	Yes
Network Attack Protections					
Number of attacks detected	31	31	31	31	31
DoS and DDoS protections	Yes	Yes	Yes	Yes	Yes
TCP reassembly for fragmented attack protection	Yes	Yes	Yes	Yes	Yes
Malformed packet protections	Yes	Yes	Yes	Yes	Yes
Malicious URL protections	Yes	Yes	Yes	Yes	Yes
Network attack protections configurable per zone	Yes	Yes	Yes	Yes	Yes
VPN					
IPSec VPN tunnels	up to 25,000	up to 10,000	up to 1,000	up to 100	up to 10
Manual Key, IKE, PKI (X.509)	Yes	Yes	Yes	Yes	Yes
DES (56 bit), 3DES (168 bit) and AES encryption	Yes	Yes	Yes	Yes	Yes
MD-5, SHA-1 authentication	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy (DH Groups)	1,2,5	1,2,5	1,2,5	1,2,5	1,2,5
Prevent replay attack	Yes	Yes	Yes	Yes	Yes
L2TP within IPSec	Yes	Yes	Yes	Yes	Yes
Star (hub and spoke) VPN network topology	Yes	Yes	Yes	Yes	Yes
IPSec NAT traversal	Yes	Yes	Yes	Yes	Yes
Tunnel interfaces	1,024	1,024	256	50	10
Redundant VPN gateway	Yes	Yes	Yes	Yes	Yes

	Juniper Networks NetScreen-5200 8G ⁽¹⁾	Juniper Networks NetScreen-500 ⁽¹⁾	Juniper Networks NetScreen-200 Series ⁽¹⁾	Juniper Networks NetScreen-50 ⁽¹⁾	Juniper Networks NetScreen-5XT ⁽¹⁾
PKI Support					
PKI certificate requests (PKCS 7 and PKCS 10)	Yes	Yes	Yes	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes	Yes	Yes	Yes
Online Certificate Status Protocol (OCSP)	Yes	Yes	Yes	Yes	Yes
Firewall and VPN User Authentication					
Built-in (internal) database - user limit	25,000	15,000	1,500	500	100
RADIUS (external) database	Yes	Yes	Yes	Yes	Yes
RSA SecurID (external) database	Yes	Yes	Yes	Yes	Yes
LDAP (external) database	Yes	Yes	Yes	Yes	Yes
RADIUS authentication accounting	Yes	Yes	Yes	Yes	Yes
XAUTH VPN authentication	Yes	Yes	Yes	Yes	Yes
Web-based authentication	Yes	Yes	Yes	Yes	Yes
Traffic Management					
Guaranteed bandwidth	No	Yes	Yes	Yes	Yes
Maximum bandwidth	Yes	Yes	Yes	Yes	Yes
Priority bandwidth utilization	No	Yes	Yes	Yes	Yes
DiffServ stamp	No	Yes	Yes	Yes	Yes
High Availability (HA)					
Active/Active or Active/Passive HA with NSRPv2	Yes	Yes	Yes	Active/Passive only	No
Redundant interfaces	Yes	Yes	Yes	No	No
Session synchronization for firewall and VPN	Yes	Yes	Yes	Yes	No
Device failure detection	Yes	Yes	Yes	Yes	No
Link failure detection	Yes	Yes	Yes	Yes	Yes
Network notification on fail-over	Yes	Yes	Yes	Yes	No
Authentication for new HA members	Yes	Yes	Yes	Yes	No
Encryption of HA traffic	Yes	Yes	Yes	Yes	No
System Management					
Juniper Networks NetScreen-Global PRO	No	No	No	No	No
Juniper Networks NetScreen-Global PRO Express	No	No	No	No	No
WebUI (HTTP and HTTPS)	Yes	Yes	Yes	Yes	Yes
Command Line Interface (console)	Yes	Yes	Yes	Yes	Yes
Command Line Interface (telnet)	Yes	Yes	Yes	Yes	Yes
Secure Command Shell (SSH v1.5 compatible)	Yes	Yes	Yes	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes	Yes	Yes	Yes
SNMP custom MIB	Yes	Yes	Yes	Yes	Yes
Administration					
Local administrator database	20	20	20	20	20
External administrator database	RADIUS/LDAP/SecurID	RADIUS/LDAP/SecurID	RADIUS/LDAP/SecurID	RADIUS/LDAP/SecurID	RADIUS/LDAP/SecurID
Restricted administrative networks	6	6	6	6	6
Root admin, admin, and read only user levels	Yes	Yes	Yes	Yes	Yes
Software upgrades and config changes	TFTP/WebUI	TFTP/WebUI	TFTP/WebUI	TFTP/WebUI	TFTP/WebUI
Schedules	256	256	256	256	256
Logging/Monitoring					
Syslog	External	External	External	External	External
E-mail (2 addresses)	Yes	Yes	Yes	Yes	Yes
NetQ WebTrends	External	External	External	External	External
SNMP	Yes	Yes	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes	Yes	Yes
VPN tunnel monitor	Yes	Yes	Yes	Yes	Yes
Websense URL filtering (external)	Yes	Yes	Yes	Yes	Yes

Certificate Authorities Supported: VeriSign, Entrust, Microsoft, RSAKeon, iPlanet (Juniper Networks), Baltimore, DODPKI

(1) Performance, capacity and features listed are based upon NetScreen ScreenOS 4.0.1 Multicast and may vary with other NetScreen ScreenOS releases. Actual throughput may vary based upon packet size and enabled features.

Flexibility

NetScreen ScreenOS Multicast leverages dynamic routing and standards support to deliver rich multimedia applications and content to subscribers that reside anywhere on the network, even on different domains or subnets. Alternatively, administrators can use built-in support for OSPF, BGP and RIPv2 to define static multicast routes that help the network operate more efficiently and allows administrators to deploy a solution that fits their routing and security requirements.

Additional multicast protocol support includes:

- Internet Group Membership Protocol (IGMP v2 & v1) support extends the edge of the multicast delivery domain to facilitate the delivery of content between routers and subscribers
- IGMP proxy support allows a Juniper Networks NetScreen device to act as a host to upstream routers or as a router to downstream hosts even if chosen multicast routing protocols are not supported by NetScreen
- Static MROUTES provides the ability to define fixed multicast routes to help lower network traffic activity (no advertising or learning) and accelerate the data forwarding process
- PIM-SM (Sparse Mode) support enables multicast support where senders/subscribers are not directly attached to a Juniper Networks NetScreen device by automatically finding the optimal delivery route
- PIM-SM Rendezvous Point proxy acts as traffic cop for PIM routers to permit transmission delivery across NAT boundaries and segmented networks

Standards Supported

ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, LDAP, SecurID, IPSec (ESP, AH), MD5, SHA-1, AES, DES, 3DES, L2TP, IKE (ISAKMP), TFTP (client), SNMP, X.509 v3, DHCP, PPPoE, SCEP, OCSP, 802.1q

Software pricing and availability

NetScreen ScreenOS 4.0-MCAST is a limited release. It is available by request to customers with current and valid support contracts that entitle them to NetScreen ScreenOS 4.0 or later.

