

Juniper Networks NetScreen-Hardware Security Client



The Juniper Networks NetScreen-Hardware Security Client, combined with NetScreen-Security Manager, is Juniper's most cost effective security solution for the fixed telecommuter and small remote office. It can easily be deployed and managed in large deployments with Juniper Network's Rapid Deployment capabilities, eliminating expensive staging steps. Using the same operating system as all NetScreen firewall and VPN solutions, the NetScreen-Hardware Security Client is able to provide the same level of protection as is found at the central sites.

Juniper Networks NetScreen-Hardware Security Client 5 User or Plus

Maximum Performance and Capacity⁽¹⁾

ScreenOS version support	ScreenOS 5.2
Firewall performance	50 Mbps
3DES performance	10 Mbps
Deep Inspection performance	50 Mbps
Concurrent sessions	1,000
New sessions/second	1,000
Policies	50
Interfaces	5 10/100 Base-T
Number of supported users	5 or unrestricted

Mode of Operation

Layer 2 mode (transparent mode) ⁽²⁾	No
Layer 3 mode (route and/or NAT mode)	Yes
NAT (Network Address Translation)	Yes
PAT (Port Address Translation)	Yes
Home/work zones	Yes
Dual Untrust	No
Dial backup	No
Policy-based NAT	Yes
Users supported	5 or unrestricted
IPSec pass thru in NAT mode	5 or unrestricted

Firewall

Number of network attacks detected	31
Network attack detection	Yes
DoS and DDoS protections	Yes
TCP reassembly for fragmented packet protection	Yes
Malformed packet protections	Yes
Deep Inspection firewall	Yes
Protocol anomaly	Yes
Stateful protocol signatures	Yes
DI Protocols supported	HTTP, FTP, SMTP, POP, IMAP, DNS NetBIOS/SMB, MS-RPC, P2P, IM
Number of application attacks detected w/DI	over 650
Content Inspection	Yes
Embedded antivirus	Yes
Malicious Web filtering	Up to 48 URLs
External Web filtering (Websense or SurfControl)	Yes
Integrated Web filtering	Yes
Brute force attack mitigation	Yes
DI attack pattern obfuscation	Yes
SYN cookie	Yes
Zone-based IP spoofing	Yes

VPN

Concurrent VPN tunnels	2
Tunnel interfaces	3
DES (56-bit), 3DES (168-bit) and AES encryption	Yes
MD-5 and SHA-1 authentication	Yes
Manual Key, IKE, PKI (X.509)	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes

Juniper Networks NetScreen-Hardware Security Client 5 User or Plus

VPN

L2TP within IPSec	Yes
IPSec NAT traversal	Yes
Redundant VPN gateways	Yes
VPN tunnel monitor	Yes

Antivirus

Embedded Scan Engine	Yes (5 user) Future (Plus)
Antivirus signatures	> 80,000
Protocols (POP3,SMTP,HTTP, IMAP, FTP)	Yes
HTTP Webmail only	Yes
Maximum AV Users	5
Automated Pattern file updates	Yes

Firewall and VPN User Authentication

Built-in (internal) database - user limit	up to 100
3rd Party user authentication	RADIUS, RSA SecurID, and LDAP
XAUTH VPN authentication	Yes
Web-based authentication	Yes

Logging/Monitoring

Syslog (multiple servers)	External, up to 4 servers
E-mail (2 addresses)	Yes
NetIQ WebTrends	External
SNMP (v1, v2)	Yes
Standard and custom MIB	Yes
Traceroute	Yes
At session start and end	Yes

Virtualization

Virtual Routers (VRs)	2
-----------------------	---

Routing

OSPF/BGP dynamic routing	No
RIPv1/v2 dynamic routing	2 instances
Static routes	1,024
Source-based routing	Yes
Equal cost multi-path routing	Yes

High Availability (HA)

Dial backup	No
Dual Untrust	No
LDAP and RADIUS server failover	Yes

VoIP

H.323 ALG	Yes
SIP ALG	Yes
NAT for H.323/SIP	Yes

IP Address Assignment

Static	Yes
DHCP, PPPoE client	Yes
Internal DHCP server	Yes
DHCP relay	Yes

Juniper Networks NetScreen-Hardware Security Client 5 User or Plus

PKI Support

PKI certificate requests (PKCS 7 and PKCS 10)	Yes
Automated certificate enrollment (SCEP)	Yes
Online Certificate Status Protocol (OCSP)	Yes
Self Signed Certificates	Yes
Certificate Authorities Supported	
Verisign	Yes
Entrust	Yes
Microsoft	Yes
RSA Keon	Yes
iPlanet (Netscape)	Yes
Baltimore	Yes
DOD PKI	Yes

Authentication

RADIUS Start/Stop	Yes
-------------------	-----

System Management

WebUI (HTTP and HTTPS)	Yes
Command Line Interface (console)	No
Command Line Interface (telnet)	Yes
Command Line Interface (SSH)	Yes, v1.5 and v2.0 compatible
NetScreen-Security Manager	Yes
All management via VPN tunnel on any interface	Yes
Rapid deployment	Yes

Administration

Local administrators database	20
External administrator database	RADIUS/LDAP/SecurID
Restricted administrative networks	6
Root Admin, Admin, and Read Only user levels	Yes
Software upgrades	TFTP/WebUI/SCP/NSM
Configuration Roll-back	Yes

Traffic Management

Guaranteed bandwidth	Yes
Maximum bandwidth	Yes
Priority-bandwidth utilization	Yes
DiffServ stamp	Yes

Dimensions and Power

Dimensions (H/W/L)	1/8.25/5 inches
Weight	1.3 lbs.
Rack mountable	Yes, with separate kit
Power Supply (AC)	12 VDC, 12 W
90 to 264 VAC to power supply with regional linear supply	12 VDC, 12 W
Power Supply (DC)	No

Certifications

Safety Certifications
UL, CUL, CSA (5XT only), CB
EMC Certifications
FCC class B, BSMI Class A, CE class B, C-Tick, VCCI class B

Environment

Operational temperature: 23° to 122° F, -5° to 50° C
Non-operational temperature: -4° to 158° F, -20° to 70° C
Humidity: 10 to 90 % non-condensing
NetScreen-HSC: 8.5 years

MTBF (Belcore model)

NetScreen-HSC: 8.5 years

Ordering Information

Product	Part Number	
Juniper Networks NetScreen-HSC (5 user) – The NetScreen-HSC 5 user comes standard with embedded AV engine.		
NetScreen-HSC	US power supply	NS-HSC-001-AV
NetScreen-HSC	UK power supply	NS-HSC-003-AV
NetScreen-HSC	Europe power supply	NS-HSC-005-AV
NetScreen-HSC	Japan power supply	NS-HSC-007-AV

Juniper Networks NetScreen-HSC (Plus) – The NetScreen-HSC Plus will support an embedded AV engine at a future date.

NetScreen-HSC Plus	US power supply	NS-HSC-101
NetScreen-HSC Plus	UK power supply	NS-HSC-103
NetScreen-HSC Plus	Europe power supply	NS-HSC-105
NetScreen-HSC Plus	Japan power supply	NS-HSC-107-NN

(1) Performance and capacity provided are the measured maximums under ideal testing conditions. May vary by deployment and features enabled.

(2) The following features are not supported in Layer 2 (transparent mode): NAT, PAT, policy based NAT, virtual IP, mapped IP, OSPF, BGP, RIPv2, and IP address assignment. Transparent mode only works in trust/untrust mode.



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

Copyright 2005, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Globel Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESR E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOS, M5, M7, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-50T, NetScreen-SXP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.