

# Juniper Networks NetScreen-5GT Series



The Juniper Networks NetScreen-5GT Series is a family of three feature-rich, enterprise-class network security solutions. They are ideally suited for securing remote offices, retail outlets and broadband telecommuter environments, where IT staff support is minimal and ease of configuration and management is crucial. The NetScreen-5GT Series integrates key security applications, routing protocols and resiliency features to provide IT managers a cost effective appliance that is easy to deploy and manage. All NetScreen-5GT Series offerings described below come standard with the following features:

- **Security:** Use the Stateful and Deep Inspection firewall, DoS protection and embedded antivirus to stop network and application level attacks and defend against the propagation of worms and viruses. Prevent users from transmitting private or corporate data, via Phishing and Spyware attacks, with integrated or re-direct web filtering options.
- **Network integration:** Support for key routing protocols, such as BGP, OSPF, RIPv1/2 and ECMP along with NAT, Route and Transparent Layer 2 operation helps facilitate network integration.
- **Resiliency:** Dial-backup or dual Ethernet ports, along with route-based VPNs provide redundancy when network connectivity is business critical. Dual WAN ports can also be used to share traffic load.
- **Port Flexibility:** Almost every network deployment scenario can be accommodated without a hardware upgrade through five configurable Ethernet interfaces. Administrators can enable switching, dual WAN ports, a dedicated DMZ or any combination thereof through a set of six predefined interface layouts called Port Modes.

## Juniper Networks NetScreen-5GT Ethernet

Juniper Networks NetScreen-5GT Ethernet solution is ideal for environments that need hardwired connectivity backed by robust network, application and payload level security. The NetScreen-5GT Ethernet is available with five Ethernet interfaces that can be deployed in a wide variety of configurations.

## Juniper Networks NetScreen-5GT ADSL

The Juniper Networks NetScreen-5GT ADSL adds ADSL connectivity to existing Ethernet connectivity, eliminating the need for an external ADSL modem. It provides a cost effective security and ADSL routing platform, with the same key security applications, routing protocols and resiliency features found in the Ethernet-based platforms, to help ensure network resources are not compromised.

## Juniper Networks NetScreen-5GT Wireless

The Juniper Networks NetScreen-5GT with Wireless brings enterprise-level security applications, routing protocols and resiliency features to help organizations deploy 802.11b/g networks in a secure manner. The NetScreen- 5GT Wireless offers administrators up to four configurable Wireless Security Zones (patent-pending), each with a unique SSID that can be used to provision appropriate levels of security for different types of users. To help ensure wireless security, privacy and interoperability, the NetScreen-5GT Wireless supports a broad set of wireless authentication and privacy mechanisms. The NetScreen-5GT Wireless includes standard Ethernet connectivity with ADSL as a hardware option.

	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
ScreenOS version support	ScreenOS 5.3		
Firewall performance <sup>(1)</sup>	75 Mbps		
3DES VPN performance	20 Mbps		
Deep Inspection (DI) performance	75 Mbps		
Concurrent sessions	2000		
New sessions/second	2000		
Policies	100		
Interfaces	5 10/100 Base-T, 1 Modem, and 1 Console	5 10/100 Base-T + ADSL, 1 Modem, and 1 Console	5 10/100 ports, 1 Wireless port with up to 4 SSIDs, 1 Modem, and 1 Console, 1 ADSL port (optional),
Mode of Operation	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
Layer 2 mode (transparent mode) <sup>(2)</sup>	Yes	Yes	Yes (except with ADSL)
Layer 3 mode (route and/or NAT mode)	Yes	Yes	Yes
NAT (Network Address Translation)	Yes	Yes	Yes
PAT (Port Address Translation)	Yes	Yes	Yes
Configurable port modes	Yes	Yes	Yes
Dual Untrust	Yes	Yes	Yes
Dial back up	Yes	Yes	Yes
Policy-based NAT	Yes	Yes	Yes
Mapped IP	300	300	300
Virtual IP	4	4	4
MIP/VIP Grouping	Yes	Yes	Yes
Users supported	10 or Unrestricted		
IPSec passthru in NAT mode	Yes	Yes	Yes

Firewall	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
Number of network attacks detected	31	31	31
Network attack detection	Yes	Yes	Yes
DoS and DDoS protections	Yes	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes	Yes
Malformed packet protections	Yes	Yes	Yes
Deep Inspection (DI) firewall <sup>(3)</sup>	Yes	Yes	Yes
Protocol anomaly detection	Yes	Yes	Yes
Stateful protocol signatures	Yes	Yes	Yes
Deep Inspection (DI) signature packs (see table on page 4)	Yes	Yes	Yes
Content Inspection	Yes	Yes	Yes
Malicious Web filtering	Up to 48 URLs		
External Web Filtering (Websense)	Yes	Yes	Yes
External Web Filtering (SurfControl)	Yes	Yes	Yes
Brute force attack mitigation	Yes	Yes	Yes
Syn cookie protection	Yes	Yes	Yes
DI attack pattern obfuscation	Yes	Yes	Yes
Zone-based IP spoofing	Yes	Yes	Yes
Integrated Web filtering	Yes	Yes	Yes
<b>VPN</b>			
Concurrent VPN tunnels	Up to 10		
Tunnel interfaces	Up to 10		
DES (56 bit), 3DES (168-bit) and AES encryption	Yes	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes	Yes
Manual Key, IKE, PKI (X.509)	Yes	Yes	Yes
Perfect forward secrecy (DH Groups)	1, 2, 5	1, 2, 5	1, 2, 5
Prevent replay attack	Yes	Yes	Yes
Remote access VPN	Yes	Yes	Yes
L2TP within IPSec	Yes	Yes	Yes
Dead Peer Detection	Yes	Yes	Yes
IPSec NAT traversal	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes
VPN tunnel monitor	Yes	Yes	Yes
<b>Antivirus/Anti-Spam<sup>(4)</sup></b>			
Embedded Scan Engine	Yes	Yes	Yes
Antivirus signatures	> 80,000	> 80,000	> 80,000
Protocols	POP3, SMTP, HTTP, IMAP, FTP	POP3, SMTP, HTTP, IMAP, FTP	POP3, SMTP, HTTP, IMAP, FTP
HTTP Webmail only	Yes	Yes	Yes
Automated Pattern file updates	Yes	Yes	Yes
Maximum AV Users <sup>(5)</sup>	10 or 25 depending on user license		
Embedded Anti-Spam	Yes	Yes	Yes
Anti phishing <sup>(6)</sup>	Yes	Yes	Yes
Spyware / Adware / Keylogger Protection	Yes	Yes	Yes
<b>Firewall and VPN User Authentication</b>			
Built-in (internal) database - user limit	up to 100	up to 100	up to 100
3rd Party user authentication	RADIUS, RSA, SecurID, and LDAP		
XAUTH VPN authentication	Yes	Yes	Yes
Web-based authentication	Yes	Yes	Yes

Logging/Monitoring	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
Syslog (multiple servers)	External, up to 4 servers		
E-mail (2 addresses)	Yes	Yes	Yes
NetIQ WebTrends	External	External	External
SNMP (v1, v2)	Yes	Yes	Yes
Standard and custom MIB	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes
At session start and end	Yes	Yes	Yes
<b>Virtualization</b>			
Virtual routers (VRs)	3	3	3
802.1Q VLAN Tagging	Yes	Yes	Yes
<b>Routing</b>			
OSPF/BGP/RIPv1/v2 dynamic routing	3 instances each		
Static routes	1024	1024	1024
Source Based Routing, Source Interface Based Routing	Yes	Yes	Yes
Equal cost multi-path routing	Yes	Yes	Yes
IGMP groups	2400	2400	2400
<b>High Availability (HA)</b>			
HA Lite	Yes - with Extended License Key		
Dial Backup <sup>(6)</sup>	Yes	Yes	Yes
Dual Untrust	Yes	Yes	Yes
<b>VoIP</b>			
H.323 ALG	Yes	Yes	Yes
SIP ALG	Yes	Yes	Yes
MGCP ALG	Yes	Yes	Yes
NAT for H.323/SIP	Yes/Yes	Yes/Yes	Yes/Yes
<b>IP Address Assignment</b>			
Static	Yes	Yes	Yes
DHCP/PPPoE/PPPOA client	Yes/Yes/No	Yes/Yes/Yes	Yes/Yes/Yes (w/ADSL)
Internal DHCP server	Yes	Yes	Yes
DHCP relay	Yes	Yes	Yes
<b>PKI Support</b>			
PKI certificate requests (PKCS 7 and PKCS 10)	Yes	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes	Yes
Online Certificate Status Protocol (OCSP)	Yes	Yes	Yes
Self Signed Certificates	Yes	Yes	Yes
Certificate Authorities Supported	Verisign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape), DOD PKI, Baltimore		
<b>RADIUS Accounting</b>			
RADIUS Start/Stop	Yes	Yes	Yes
<b>System Management</b>			
WebUI (HTTP and HTTPS)	Yes	Yes	Yes
Command Line Interface (console)	Yes	Yes	Yes
Command Line Interface (telnet)	Yes	Yes	Yes
Command Line Interface (SSH)	Yes, v1.5 and v2.0 compatible		
NetScreen-Security Manager	Yes	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes	Yes
Rapid deployment	Yes	Yes	Yes

Administration	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
Local administrators database	20	20	20
External administrator database	RADIUS/LDAP/SecurID		
Restricted administrative networks	6	6	6
Root Admin, Admin, and Read Only use	Yes	Yes	Yes
Software upgrades	TFTP/WebUI/SCP/NSM		
Configuration Roll-back	Yes	Yes	Yes
<b>Traffic Management</b>			
Guaranteed bandwidth	Yes	Yes	Yes
Maximum bandwidth	Yes	Yes	Yes
Ingress Traffic Policing	Yes	Yes	Yes
Priority-bandwidth utilization	Yes	Yes	Yes
DiffServ stamp	Yes	Yes	Yes
<b>ADSL Support</b>			
ADSL over POTS	N/A	Yes	Yes (optional)
ADSL over ISDN	N/A	Yes	Yes (optional)
ADSL DMT issue 2	N/A	Yes	Yes (optional)
ADSL G lite Yes No	N/A	Yes	Yes (optional)
Dying Gasp Support	N/A	Yes	Yes (optional)
Deutsche Telecom Support	N/A	Yes	Yes (optional)
<b>ADSL Layer 2 and encapsulations</b>			
PPPoE/PPPoA	N/A	Yes	Yes (optional)
2684/1483 (Bridge and Routed Mode)	N/A	Yes	Yes (optional)
ATM AAL5/ATM PVCs	N/A	Yes/10	Yes/10 (optional)
<b>Wireless Radio</b>			
Transmit Power	N/A	N/A	Up to 200 mW
Wireless Standards supported	N/A	N/A	802.11b/g
Access Point Survey	N/A	N/A	Yes
Maximum Configured SSIDs	N/A	N/A	8
Maximum Active SSIDs	N/A	N/A	4
<b>Wireless Security</b>			
Wireless Privacy	N/A	N/A	WPA (AES or TKIP), IPSec VPN, WEP
Wireless Authentication	N/A	N/A	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x
Additional Dial-up VPN Tunnels	N/A	N/A	20 for 10-user and Plus, 40 for Extended
MAC Access Controls	N/A	N/A	Permit or Deny
Client Isolation	N/A	N/A	Yes
<b>Antennae options</b>			
Diversity Antenna	N/A	N/A	Included
Directional Antenna	N/A	N/A	Optional
Omni-directional Antenna	N/A	N/A	Optional

Dimensions and Power	5GT 10 user or plus	5GT ADSL 10 user or plus	5GT Wireless 10 user or plus
Dimensions (H/W/L)	1/8.25/5 inches	1/8.25/7.25 inches	1/8.25/7.25 inches
Power Supply (DC)	No	No	No
Weight	1.5 lbs	2 lbs.	2.5 lbs.
Rack mountable	Yes, w/separate kit		
Power Supply (AC)	9-12VDC 12W	12VDC 18W	
<b>Environment</b>			
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		
MTBF (Telecordia standard)	32.2 Years	26.7 Years	23.9 Years
<b>Certifications</b>			
Safety Certifications	UL, CUL, CB, TUV		
EMC Certifications	FCC class B, CE class B, C-Tick, VCCI class B		
Common Criteria EAL4 Certification	Yes	No	No
FIPS 140-2, Level 2 Certification	Yes	No	No
ICSA Firewall and VPN	Yes	Yes	Yes
Wi-Fi Alliance 802.11 Certification	No	No	Yes
Wi-Fi Alliance Enterprise Certification	No	No	Yes

(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. Layer 2 mode is only supported in Trust/Untrust port mode.  
(3) Updates to Deep Inspection signatures requires signature service which is available for additional purchase  
(4) Requires additional purchase of antivirus signature and antispam detection subscriptions.  
(5) Recommended number of users  
(6) Tested with 3COM 5686 56K modem and ZyXel omni.net

LCD ISDN modem  
(7) Can be done through "site blocking" via URL filtering - whether integrated or redirect, and "inbound email blocking" via anti-spam and/or Juniper-Kaspersky embedded AV for those platforms which support it.  
(8) Juniper-Kaspersky engine only.

### License Options

The NetScreen-5GT Series is available in licensing options to support different numbers of users.

Licensing Options	Description
10 user Product license	Limits capacity to 10 concurrent users
Plus Product license	Increases capacity to an unlimited number of users
Extended Product license	Increases sessions and VPN tunnel capacities to 4000 and 25 respectively. Adds a DMZ zone and HA lite (no session synchronization)

### Port Modes

Port Modes provide configuration flexibility to the interface options on each of the NetScreen-5GT Series platforms. The tables below depict the different Port Mode and Tunnel zone options. A tunnel zone is an extra zone for terminating tunnel interfaces.

### NetScreen-5GT Ethernet Port Mode Options

Interfaces 5 10/100 ports, 1 Modem and 1 Console, Current ScreenOS version 5.1

Port Mode	Availability	Trusted Wired Security Zones	Tunnel Zones
Trust-Untrust	All Licenses	1	1
Dual-Untrust	All Licenses	1	1
Home-Work	All Licenses	2*	1
TrustUntrustDMZ	Extended Only	2	1
DMZDual Untrust	Extended Only	2	1
Combined	All Licenses	2*	1
Dual-Untrust-DMZ	Extended Only	2	1
Dual-DMZ	Extended Only	2	1

\* Home Zone Cannot Access Work Zone in Home-Work and Combined Port Modes.

**NetScreen-5GT ADSL and NetScreen-5GT Wireless/ADSL Port Mode Options**

Interfaces 5 10/100 ports, 1 ADSL port 1 Modem and 1 Console, Current ScreenOS version 5.3

	Availability	Trusted Wired and Wireless** Zones	Tunnel Zones	Additional Wireless Security Zones**
Trust-Untrust	All Licenses	1	1	1
Home-Work	All Licenses	2*	1	1
Extended	Extended Only	2	1	2

\*Home Zone Cannot Access Work Zone in Home-Work and Combined Port Modes.

\*\* Wireless security product only

**NetScreen-5GT Wireless Port Mode Options**

5 10/100 ports, 1 Wireless radio, 1 Modem, and 1 Console, 1 ADSL port (optional), Current ScreenOS version 5.3

	Availability	Trusted Wired and Wireless** Zones	Tunnel Zones	Additional Wireless Security Zones**
Trust-Untrust	All Licenses	1	1	1
Dual-Untrust**	All Licenses	1	1	1
Home-Work	All Licenses	2*	1	1
Combined**	All Licenses	2*	1	1
Extended	Extended Only	2	1	2

\*Home Zone Cannot Access Work Zone in Home-Work and Combined Port Modes.

\*\* These Port modes are not available in the ADSL version of the NetScreen-5GT ADSL

Product	Part Number
<b>Juniper Networks-5GT Ethernet</b>	
<b>Juniper Networks NetScreen-5GT 10 User</b>	
NetScreen-5GT US power supply	NS-5GT-001
NetScreen-5GT UK power supply	NS-5GT-003
NetScreen-5GT Europe power supply	NS-5GT-005
NetScreen-5GT Japan power supply	NS-5GT-007-nn
<b>NetScreen-5GT ADSL</b>	
<b>Juniper Networks NetScreen-5GT ADSL 10 User*</b>	
NetScreen-5GT ADSL US power supply	NS-5GT-011-x
NetScreen-5GT ADSL UK power supply	NS-5GT-013-x
NetScreen-5GT ADSL Europe power supply	NS-5GT-015-A

Product	Part Number
<b>NetScreen-5GT Wireless</b>	
<b>Juniper Networks NetScreen-5GT Wireless 10 User</b>	
NetScreen-5GT Wireless US Only - US power supply	NS-5GT-021
NetScreen-5GT Wireless World* - UK power supply	NS-5GT-023
NetScreen-5GT Wireless World* - Europe power supply	NS-5GT-025
NetScreen-5GT Wireless Japan Only* - Japan power supply	NS-5GT-027-nn
NetScreen-5GT Wireless World* - US power supply	NS-5GT-028
<b>NetScreen-5GT Wireless ADSL</b>	
<b>Juniper Networks NetScreen-5GT Wireless ADSL 10 User</b>	
NetScreen-5GT Wireless ADSL US Only - US power supply	NS-5GT-031-x
NetScreen-5GT Wireless ADSL World* - UK power supply	NS-5GT-033-x
NetScreen-5GT Wireless ADSL World* - Europe power supply	NS-5GT-035-x
NetScreen-5GT Wireless ADSL World* - US power supply	NS-5GT-038-x
<b>NetScreen-5GT Upgrades</b>	
Anti-Virus, Deep Inspection, Web Filtering, and Anti-Spam can be purchased via subscription licenses.	
NetScreen-5GT Upgrade from 10-User to NetScreen-5GT Plus (Unrestricted user)	NS-5GT-PLU
NetScreen-5GT Upgrade from 10-User to NetScreen-5GT Extended	NS-5GT-ETU
NetScreen-5GT Upgrade from Plus to Extended	NS-5GT-EPU
<b>Accessories</b>	
Rack mount kit for 2 NetScreen-5GTs	NS-5GT-RMK

\* World units may not be purchased in Japan or the US due to regulatory restrictions.

To order ADSL Annex A or Annex B units, replace the -x at the end of the sku with an A or B.

Please check ISP and DSLAM compatibility for the ADSL connections at [www.juniper.net/products/integrated/5GT-ADSL/](http://www.juniper.net/products/integrated/5GT-ADSL/)

**Deep Inspection (DI) Signature Packs**

This feature enhancement allows ScreenOS to support targeted DI signature pack optimized for your specific network deployment. You can now select the DI signature pack that improves threat prevention for your network environment to ensure detection accuracy and coverage.

Protection Type*	Deployment Type	Defense type	Attack Type
Base	Branch Offices Small/Medium Businesses	Client/Server and worm protection	Selected set of critical signatures
Client	Remote/Branch Offices	Perimeter defense, compliance for hosts (desktops, etc)	Attacks in the server- to-client direction
Server	Small/Medium Businesses	Perimeter defense, compliance for server infrastructure	Attacks in the client-to- server direction
Worm Mitigation	Remote/Branch Offices of Large Enterprises	Most comprehen- sive defense against worm attacks	Worms, Trojans, back- door attacks



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](http://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 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.