

# Juniper Networks NetScreen-500 GPRS



## • Comprehensive GPRS security solution

The NetScreen-500 GPRS security solution protects operators' infrastructure on roaming connections, subscribers from Internet-based attacks, and mobile access corporate connections

## • High-performance, scalable operation

Multiple gigabit network interfaces, multiple virtual routers, ASIC-accelerated performance, and VLAN (virtual LAN) support enable GPRS operators to scale their security solutions along with subscriber growth

## • Flexible network connectivity

Routing support for OSPF, BGP, or Layer 2 transparent bridge mode ensures seamless integration into existing GPRS data networks

## • Built-in Operations and Maintenance (O&M) features

A wide range of management features such as sub-second failover High Availability, redundant load-sharing power supplies, management by NetScreen-Security Manager, and out-of-band management network interfaces, ensures the NetScreen-500 GPRS can be effectively managed with minimal downtime

## Product overview

Mobile operators that are adding General Packet Radio Service (GPRS) to their customer offerings, must take appropriate measures to protect their network infrastructure and subscribers, due to the inherent lack of security in the GPRS Tunneling Protocol (GTP). The NetScreen-500 GPRS combines the hardware-accelerated firewall, VPN and traffic management capabilities of the NetScreen-500 with enhanced features designed to provide mobile operators with a purpose built, high performance, scalable security solution to protect their GPRS data networks.

The NetScreen-500 GPRS solution secures roaming connections using a combination of stateful inspection, traffic rate limiting, traffic sanity checks, traffic logging, and traffic accounting. These features allow mobile operators to protect their network infrastructure from Denial of Service (DoS) attacks and subscriber hijacking attacks. The NetScreen-500 GPRS features can also be used to control roaming partner network access, in addition to controlling which external networks subscribers may access (through APN Filtering). Both GTP Releases 1997 and 1999 are fully supported, including charging gateway traffic (GTP). The NetScreen-500 GPRS provides secure scalable Internet and corporate Intranet connectivity from a mobile operator's network. VPN technologies including IPSec, L2TP, and 802.1q VLANs logically separate the connections from the mobile operator's network to the external networks and enable the application of security policies even when the destination networks are using the same network address space. This enables mobile operators to cost-effectively offer subscribers a secure connection to the Internet and offer corporate customers secure Intranet access.

## Flexible roaming security features

Traffic filtering features in the NetScreen-500 GPRS allow mobile operators to specify which versions of GTP are allowed on their network and which GTP messages are permitted. Traffic logging and debugging features log GTP traffic for traffic analysis and debugging purposes, and IPSec VPNs can ensure the integrity of GTP traffic between operators. GTP security features include:

- Policy based GTP enforcement for all GPRS features
- Full support at all GPRS interfaces
- Ability to combine multiple interfaces in single device (Gn, Gp, Ga, Gi)
- Per direction traffic filtering
- Zone to Zone filtering
- Packet sanity checks enforce legal packet length, mandatory Information Elements (IEs), and mandatory field settings
- Message length checking ensures GTP traffic meets the maximum and minimum length as set by the operator
- Message type filtering checks the GTP protocol version as well as the message type against filters specified by the operator
- APN and selection mode filtering check GTP protocol messages to determine if a roaming subscriber is allowed to access a specified external network
- IMSI-prefix filtering ensures only traffic from valid roaming partners is allowed by checking the GTP message Mobile Country Code (MCC) and Mobile Network Code (MNC)
- Enhanced Traffic logging selectively logs all GTP traffic including GSN IP addresses, tunnel endpoint ID, Message Type, IMSI, MSISDN, APN, and Selection Mode. Extended logging can also be enabled by GPRS operators
- Traffic accounting creates log entries for every PDP context, including the elapsed time of the session and the number of T-PDUs (user data in GTP packets) sent
- Rate limiting controls the rate of GTP signaling and user plane messages so that GSNs are protected from being overwhelmed in a DoS attack
- IPSec VPN ensures the confidentiality and integrity of GTP traffic between operators or over an operator's WAN. IPSec VPNs can be implemented in combination with the GTP features above to ensure roaming traffic comes from legitimate roaming partners and is not malicious
- Malicious attack prevention, such as overbilling prevention
- GGSN and SGSN proxy redirection, for load balancing and redundancy

### Secure, scalable Internet/Intranet connectivity (Gi interface)

The NetScreen-500 GPRS includes VPN, packet filtering and traffic management features to help protect GPRS networks from Internet borne attacks such as DoS.

- Virtual routers support up to 250 routing domains and 250 zones, which are used to logically separate traffic to or from different APNs
- BGP and OSPF routing protocols enable flexible deployment within your network or WAN environment
- APN logical connection mapping uses IPSec, L2TP, and 802.1q VLANs to separate traffic from the GGSN to the NetScreen Virtual Router and then to the destination network
- APN security policies control the network traffic that is permitted to or from the APN destination network

High Availability: Active/Active, Active/Passive, Full Mesh  
Throughput: 700 Mbps Firewall, 600 Mbps GTP, 250 Mbps VPN

### NetScreen-Security Manager Support

Mobile operators deploying the NetScreen ScreenOS 5.0 GPRS security solution can now use NetScreen-Security Manager to control and monitor the solution.

- Configure, control and monitor GPRS GTP deployments
- Configure, control and monitor NSGP for over-billing attack prevention
- Use Statistical Report Server for historical reporting and SLA verification

### Technical Specification (Gn/Gp/Ga)

- 3GPP technical specification 09.60 GTP release 1997
- 3GPP technical specification 29.060 GTP release 1999
- GTP over UDP and TCP
- GTP<sup>1</sup> (GTP Prime) for charging gateway traffic
- 150,000 GTP tunnels
- 250 virtual routers
- 250 zones
- 10,000 VPN tunnels
- 20,000 policies
- Virtual Systems (VSYS) support for GTP (up to 10 vsys)
- Lawful Interception functionality\*  
\* Only for logging certain information to an external lawful intercept server.

### Technical Specification (Gi)\*

- 250 virtual routers (routing domains)
- 10,000 VPN tunnels
- 20,000 policies  
\* The NS S200 (which does not run GPRS Software) may be deployed at Gi interface in combination with NetScreen 500 GPRS at Gn/GP interface(s)



**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 2004, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen Global 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, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSE, MS, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, 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, NMO-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.