

NetScreen ScreenOS 5.0.0 GPRS Reference Guide

ScreenOS 5.0.0 GPRS

P/N 093-1354-000

Rev. A

Copyright Notice

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave. Sunnyvale, CA 95014

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface	iii	IP Fragmentation	30
Conventions	v	GTP-in-GTP Packet Filtering	30
WebUI Navigation Conventions	v	GTP Tunnels	31
CLI Conventions	vi	GTP Tunnel Limiting	31
Juniper Networks NetScreen Documentation	viii	Stateful Inspection	32
New Features in ScreenOS GPRS	1	Tunnel Failover for High Availability	33
New Features and Feature Enhancements	2	Hanging GTP Tunnel Cleanup	34
Features Summary	4	SGSN and GGSN Redirection	35
ScreenOS GPRS Concepts & Examples	7	Overbilling Attack Prevention	36
The NetScreen Device as a GTP Firewall	9	Overbilling Attack Description	36
Gp and Gn Interfaces	10	Overbilling Attack Solution	38
Gi Interface	11	GTP Traffic Monitoring	43
Operational Modes	12	Traffic Logging	43
Virtual System Support	12	Traffic Counting	46
Policy-Based GTP	13	Lawful Interception	47
GTP Inspection Object	17	GPRS CLI Commands	49
GTP Message Filtering	18	Main CLI Prompt	50
Packet Sanity Check	18	GTP Inspection Object Context	59
Message Length Filtering	19	ScreenOS GPRS Troubleshooting	71
Message Type Filtering	20	ScreenOS GPRS Debugging Commands	72
Access Point Name Filtering	23	ScreenOS GPRS Log Messages	73
IMSI Prefix Filtering	26	Glossary	A-I
Messages Rate Limiting	28	Index	IX-I
Sequence Number Validation	29		

Preface

This document aims at GPRS network operators who possess advanced knowledge of GPRS technology.

GPRS networks connect to several external networks including those of roaming partners, corporate customers, GRX (GPRS Roaming Exchange) providers, and the public Internet. GPRS network operators face the challenge of protecting their network while providing and controlling access to and from these external networks. Juniper Networks provides solutions to many of the security problems encumbering GPRS network operators.

In the GPRS architecture, the fundamental reason for security threats to an operator's network is the lack of security inherent in GTP (GPRS tunneling Protocol). GTP is the protocol used between GSNs (GPRS Support Nodes). Communication between different GPRS networks is not secure because GTP does not provide any authentication, data integrity, or confidentiality protection. Implementing IPSec for connections between roaming partners, setting traffic rate limits, and using stateful inspection can eliminate a majority of the security risks that GTP entails.

With ScreenOS GPRS software, Juniper Networks offers a security technology that mitigates a wide variety of attacks on the Gp, Gn, and Gi interfaces. NetScreen ScreenOS GPRS is an enhanced version of the NetScreen ScreenOS firmware and combines most features of ScreenOS in addition to GTP firewall features that address key security issues in mobile operators' networks. Although ScreenOS supports Deep Inspection, Juniper Networks does not recommend that you implement Deep Inspection and GPRS concurrently. Both GPRS and Deep Inspection consume great amounts of system resources and if used concurrently, can cause significant performance degradation.

This manual describes the GTP features of ScreenOS GPRS and demonstrates how to configure GTP functionality on a NetScreen device.

This reference guide is organized into the following chapters:

- [Chapter 1, “New Features in ScreenOS GPRS” on page 1](#)
- [Chapter 2, “ScreenOS GPRS Concepts & Examples” on page 7](#)
- [Chapter 3, “GPRS CLI Commands” on page 49](#)
- [Chapter 4, “ScreenOS GPRS Troubleshooting” on page 71](#)
- [Appendix A, “Glossary” on page A-I](#)

For more information about ScreenOS 5.0.0 features and CLI commands, refer to the following documents:

- *NetScreen Concepts & Examples ScreenOS Reference Guide*, ScreenOS 5.0.0 release
- *NetScreen CLI Reference Guide*, ScreenOS 5.0.0 release

CONVENTIONS

This book presents two management methods for configuring a NetScreen device: the Web user interface (WebUI) and the command line interface (CLI). The conventions used for both are introduced below.

WebUI Navigation Conventions

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links.

Example: **Objects > Addresses > List > New**

To access the new address configuration dialog box, do the following:

1. Click **Objects** in the menu column.
The Objects menu option expands to reveal a subset of options for Objects.
2. (Applet menu) Hover the mouse over **Addresses**.
(DHTML menu) Click **Addresses**.
The Addresses option expands to reveal a subset of options for Addresses.
3. Click **List**.
The address book table appears.
4. Click the **New** link in the upper right corner.
The new address configuration dialog box appears.

CLI Conventions

Each CLI command description in this manual reveals some aspect of command syntax. This syntax may include options, switches, parameters, and other features. To illustrate syntax rules, some command descriptions use *dependency delimiters*. Such delimiters indicate which command features are mandatory, and in which contexts.

Dependency Delimiters

Each syntax description shows the dependencies between command features by using special characters.

- The { and } symbols denote a mandatory feature. Features enclosed by these symbols are essential for execution of the command.
- The [and] symbols denote an optional feature. Features enclosed by these symbols are not essential for execution of the command, although omitting such features might adversely affect the outcome.
- The | symbol denotes an “or” relationship between two features. When this symbol appears between two features on the same line, you can use either feature (but not both). When this symbol appears at the end of a line, you can use the feature on that line, or the one below it.

Nested Dependencies

Many CLI commands have *nested* dependencies, which make features optional in some contexts, and mandatory in others. The three hypothetical features shown below demonstrate this principle.

```
[ feature_1 { feature_2 | feature_3 } ]
```

The delimiters [and] surround the entire clause. Consequently, you can omit **feature_1**, **feature_2**, and **feature_3**, and still execute the command successfully. However, because the { and } delimiters surround **feature_2** and **feature_3**, you must include either **feature_2** or **feature_3** if you include **feature_1**. Otherwise, you cannot successfully execute the command.

The following example shows some of the feature dependencies of the **set interface** command.

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

The { and } brackets indicate that specifying either **flood** or **arp** is mandatory. By contrast, the [and] brackets indicate that the **trace-route** option for **arp** is not mandatory. Thus, the command might take any of the following forms:

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

Availability of CLI Commands and Features

As you execute CLI commands using the syntax descriptions in this manual, you may find that certain commands and command features are unavailable for your NetScreen device model.

Because NetScreen devices treat unavailable command features as improper syntax, attempting to use such a feature usually generates the **unknown keyword** error message. When this message appears, confirm the feature's availability using the ? switch. For example, the following commands list available options for the **set vpn** command:

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```

JUNIPER NETWORKS NETSCREEN DOCUMENTATION

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.juniper.net/techpubs/.

To obtain the latest software version, visit: www.juniper.net/support/. After logging in, select the Download Software option, and then follow the displayed instructions. (You must be a registered user to download Netscreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

New Features in ScreenOS GPRS

This chapter provides an overview of new features and commands added to ScreenOS GPRS since the last release of ScreenOS 4.0.0 GPRS.

- [“New Features and Feature Enhancements”](#) on page 2
- [“Features Summary”](#) on page 4

NEW FEATURES AND FEATURE ENHANCEMENTS

This release of ScreenOS GPRS, version 5.0.0, is based on ScreenOS 5.0.0r6 and supports all of its features. For more information on ScreenOS 5.0.0 features, refer to the *NetScreen ScreenOS Migration Guide* and the *NetScreen Concepts & Examples ScreenOS Reference Guide*, version 5.0.0.

The following table presents an overview of new features and feature enhancements introduced in ScreenOS 5.0.0 GPRS. For conceptual information on these features and to learn how to configure them on a NetScreen device, see the “[ScreenOS GPRS Concepts & Examples](#)” chapter.

Feature	Description
Policy-based GTP	To enable GTP inspection on a NetScreen device, you configure and then apply a GTP Inspection Object to a policy.
GTP IMSI prefix and APN filtering	You can configure up to 1000 IMSI prefixes and up to 2000 APNs. Additionally, a NetScreen device can filter GTP packets based on the combination of an IMSI prefix and an APN.
Overbilling attack prevention	You can configure NetScreen devices to protect subscribers of a PLMN from Overbilling attacks. The solution requires two NetScreen devices and involves the NSGP module and protocol.
GTP sequence number validation	You can configure a NetScreen device to perform Sequence Number Validation.
IP fragmentation of GTP messages	By default, a NetScreen device buffers IP fragments until it receives a complete GTP message, and then performs the inspection of the GTP message.
GGSN & SGSN redirection	NetScreen devices support GTP traffic redirection between SGSNs and GGSNs.

Feature	Description
Detecting GTP-in-GTP packets	You can configure a NetScreen device to detect and drop a GTP packet that contains another GTP packet in its message body.
Unique GTP tunnel index	A NetScreen device assigns a unique index to each GTP tunnel upon its creation. That tunnel index appears for each logged GTP tunnel message.
Virtual system support	NetScreen devices fully support GTP functionality in virtual systems.
GTP lawful interception	You can configure a NetScreen device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification.
GTP traffic counting per bytes of data	You can configure a NetScreen device to count GTP traffic that it processes for the GGSNs and SGSNs that it protects by messages or by bytes of data.
GTP traffic logging	When enabling the logging of GTP packets with a Packet Rate-Limited status, you can specify a logging frequency to control the interval at which the NetScreen device logs these messages.

FEATURES SUMMARY

In addition to the new features and feature enhancements introduced in ScreenOS GPRS 5.0.0 (see [“New Features and Feature Enhancements”](#) on page 2), the following table lists all other features for ScreenOS GPRS.

Feature	Description
GTP Release 1997 and 1999 support	Supports GTP message types for GTP', GTP-U, and GTP-C planes.
Route mode and Transparent mode	Supports the implementation of a NetScreen device in Route mode or in Transparent mode.
GTP Policy Filtering	Instructs the NetScreen device to drop or forward packets based on specified criteria.
GTP Packet Sanity Check	Instructs the NetScreen device to drop or forward packets based on whether or not the GTP message format is valid.
GTP Message Length Filtering	Instructs the NetScreen device to drop or forward packets based on specified GTP message length constraints.
GTP Message Type Screening	Instructs the NetScreen device to drop or forward packets based on the type of message indicated in the GTP header of the packet.
GTP IMSI Prefix Filtering	Instructs the NetScreen device to drop or forward packets based on valid Mobile Country Code (MCC) and Mobile Network Code (MNC) identifiers.
APN Filtering	Instructs the NetScreen device to drop or forward packets based on whether or not the APN and Selection Mode of the GTP packet match specified APN filters.

Feature	Description
Traffic Rate Limiting	Protects GSN resources by limiting the rate of network traffic going to GSNs. You can apply rate limiting separately to GTP-U and GTP-C messages.
GTP Tunnel Limiting	Protects GSN resources by limiting the number of GTP tunnels allowed on each GSN.
GTP Stateful Inspection	Performs numerous verification checks on GTP messages against current tunnel state, including Tunnel Establishment and Teardown and Inter SGSN Routing Area Update.
Hanging GTP Tunnel Cleanup	Identifies and clears hanging tunnels from the NetScreen device state table.
GTP Traffic Logging	Provides basic and extended logging of GTP traffic.
GTP Traffic Counting	Provides information on the number of T-PDU and G-PDU packets the NetScreen device receives and sends.
GTP Tunnel Failover for High Availability	Provides active-passive and active-active high availability (HA) configuration capabilities in Route mode, and active-passive HA in Transparent mode. GTP tunnel failover can only occur between two NetScreen devices.
All Features in ScreenOS 5.0.0	For more information see the <i>NetScreen Concepts & Examples ScreenOS Reference Guide</i> , version 5.0.0.

ScreenOS GPRS Concepts & Examples

This chapter describes new features added to ScreenOS to support GTP (GPRS Tunneling Protocol) functionality. It also describes how you can configure these features on the NetScreen device. This chapter contains the following sections:

- “The NetScreen Device as a GTP Firewall” on page 9
 - “Gp and Gn Interfaces” on page 10
 - “Gi Interface” on page 11
 - “Operational Modes” on page 12
 - “Virtual System Support” on page 12
- “Policy-Based GTP” on page 13
- “GTP Inspection Object” on page 17
- “GTP Message Filtering” on page 18
 - “Packet Sanity Check” on page 18
 - “Message Length Filtering” on page 19
 - “Message Type Filtering” on page 20
 - “Access Point Name Filtering” on page 23
 - “IMSI Prefix Filtering” on page 26
 - “Messages Rate Limiting” on page 28
 - “Sequence Number Validation” on page 29
 - “IP Fragmentation” on page 30
 - “GTP-in-GTP Packet Filtering” on page 30

- “GTP Tunnels” on page 31
 - “GTP Tunnel Limiting” on page 31
 - “Stateful Inspection” on page 32
 - “Tunnel Failover for High Availability” on page 33
- “SGSN and GGSN Redirection” on page 35
- “Overbilling Attack Prevention” on page 36
 - “Overbilling Attack Description” on page 36
 - “Overbilling Attack Solution” on page 38
- “GTP Traffic Monitoring” on page 43
 - “Traffic Logging” on page 43
 - “Traffic Counting” on page 46
 - “Lawful Interception” on page 47

THE NETSCREEN DEVICE AS A GTP FIREWALL

NetScreen ScreenOS GPRS supports GTP, which is the protocol deployed between SGSNs and GGSNs for establishing GTP tunnels for individual mobile stations (MS). A GTP tunnel is a secure channel between GSNs through which two hosts can exchange data. The SGSN receives packets from the MS and encapsulates them within a GTP header before forwarding them to the GGSN through the GTP tunnel. When the GGSN receives the packets, it decapsulates them and forwards them to the external host.

A NetScreen device can provide security for the following types of GPRS interfaces:

- Gn – The Gn interface is the connection between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) within the same Private Land Mobile Network (PLMN).
- Gp – The Gp interface is the connection between two PLMNs.
- Gi – The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN

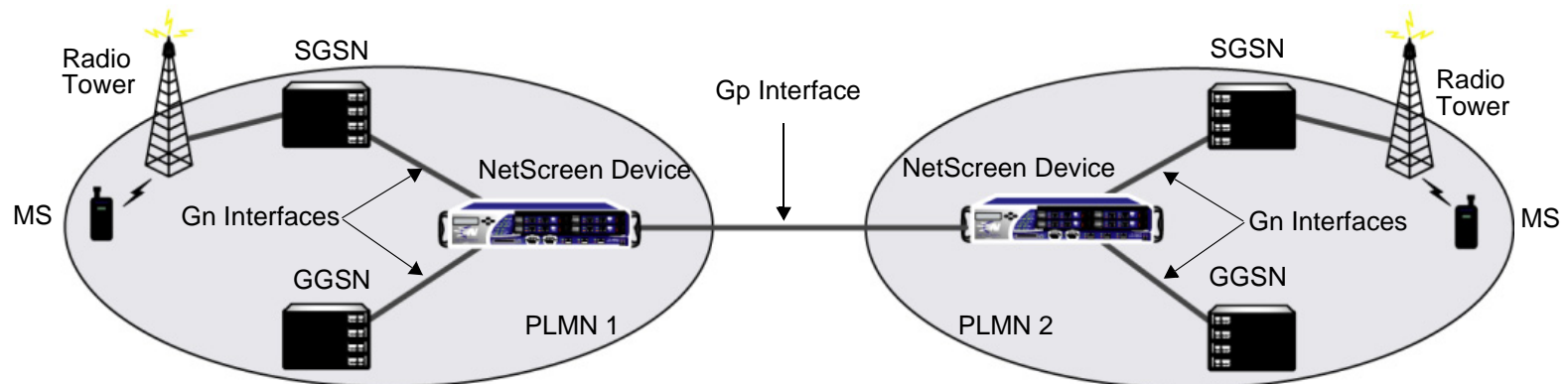
Note: The term “interface” has two different meanings in ScreenOS and in GPRS technology. In ScreenOS, an interface is like a doorway to a security zone and allows traffic to enter and exit the zone. In GPRS, an interface is a connection, or a reference point, between two components of a GPRS infrastructure, for example an SGSN and a GGSN.

Gp and Gn Interfaces

When you implement a NetScreen device on the Gn interface, you protect mobile users from other users in the same PLMN. To secure GTP tunnels on the Gn interface, you place the NetScreen device between SGSNs and GGSNs within a common PLMN.

When you implement a NetScreen device on the Gp interface, you protect a PLMN against another PLMN. To secure GTP tunnels on the Gp interface, you place the SGSNs and GGSNs of a PLMN behind a NetScreen device therefore having all incoming and outgoing traffic go through the NetScreen device.

The following illustrates the implementation of NetScreen devices to protect a PLMNs on the Gp and Gn interfaces.



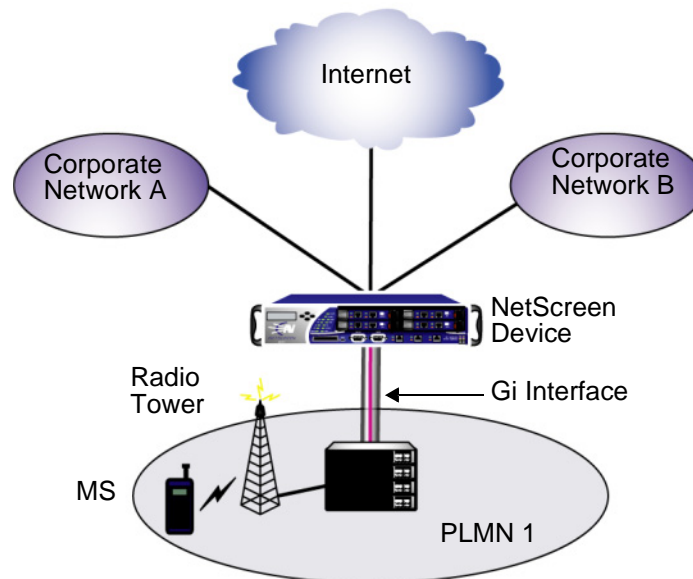
Gi Interface

When you implement a NetScreen device on the Gi interface, you can simultaneously control traffic for multiple networks, protect a PLMN against the Internet and external networks, and protect mobile users from the Internet and other networks. ScreenOS provides a great number of virtual routers making it possible for you to use one virtual router per customer network, therefore allowing the separation of traffic for each customer network.

The NetScreen device can securely forward packets to the Internet or destination networks using L2TP for IPSec VPN tunnels. (Note that NetScreen devices do not support full L2TP.)

For more information on features and capabilities of virtual routers, refer to the *NetScreen Concept & Examples ScreenOS Reference Guide*.

The following illustrates the implementation of a NetScreen device to protect a PLMN on the Gi interface.



Operational Modes

ScreenOS GPRS supports two interface operational modes with GTP: Transparent mode and Route mode. Operators can implement a NetScreen device in Route mode if they want the device to participate in the routing infrastructure of their network. This requires a certain amount of network redesigning. Alternatively, operators can implement a NetScreen device in Transparent mode into their existing network without having to reconfigure their entire network. In Transparent mode, the NetScreen device acts like a Layer 2 switch or bridge and the IP addresses of interfaces are set at 0.0.0.0, making the presence of the NetScreen device invisible, or “transparent”, to users.

ScreenOS GPRS supports NAT on interfaces and policies that do not have GTP inspection enabled.

Currently in ScreenOS, Transparent mode only supports active-passive HA (high availability), unlike Route mode which supports both active-passive and active-active HA.

For more information on operational modes and high availability, refer to the *NetScreen Concepts & Examples ScreenOS Reference Guide*—Volume 2, “Fundamentals” and Volume 8, “High Availability” respectively.

Virtual System Support

NetScreen devices fully support GTP functionality in virtual systems. To conserve resources, however, NetScreen recommends that you use no more than 10 virtual systems.

POLICY-BASED GTP

By default, the PLMN that the NetScreen device protects is in the Trust zone. The NetScreen device protects the PLMN in the Trust zone against other PLMNs in other zones. You can place all the PLMNs against which you are protecting your PLMN in the Untrust zone or you can create user-defined zones for each PLMN. A PLMN can occupy one or multiple security zones.

You must create policies to enable traffic to flow between zones and PLMNs. Policies contain rules that permit, deny or tunnel traffic. A NetScreen device performs GTP policy filtering by checking every GTP packet against policies that regulate GTP traffic and by then forwarding, dropping or tunneling the packet based on these policies.

By selecting the GTP service in a policy, you enable the NetScreen device to permit, deny or tunnel GTP traffic. However, this does not enable the device to inspect GTP traffic. In order for the NetScreen device to inspect GTP traffic, you must apply a GTP configuration, also referred to as a GTP Inspection Object, to a policy.

Before you can apply a GTP configuration to a policy, you first have to create a GTP Inspection Object (see [“GTP Inspection Object” on page 17](#)). You can apply only one GTP Inspection Object per policy, but you can apply a GTP Inspection Object to multiple policies. Using policies, you can permit or deny the establishment of GTP tunnels from certain peers such as an SGSN.

You can configure policies that specify “Any” as the source or destination zone (thereby including all hosts in the source or destination zone). You can also configure policies that specify multiple source and destination addresses.

You can enable features such as traffic logging and counting in policies. For more information on policies, see the *NetScreen Concept & Examples ScreenOS Reference Guide*.

Example: Configuring Policies to Enable GTP Inspection

In this example, you configure interfaces, create addresses and two policies to allow bidirectional traffic between two networks within the same PLMN. You also apply a GTP Inspection Object to the policies.

WebUI

1. GTP Inspection Object

Objects > GTP > New: Enter the following, and then click **Apply**.

GTP Name: GPRS1

2. Interfaces

Network > Interfaces > Edit (for ethernet3/2): Enter the following, and then click **Apply**:

Zone Name: Trust

IP Address/Netmask: 10.1.1.1/24

Network > Interfaces > Edit (for ethernet1/2): Enter the following, and then click **OK**:

Zone Name: Untrust

IP Address/Netmask: 1.1.1.1/24

3. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: local-GGSN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: remote-SGSN

IP Address/Domain Name:

IP/Netmask: (select), 1.2.2.5/32

Zone: Untrust

4. Policies

Policies > (From: Trust, To: Untrust) > New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), local-GGSN

Destination Address:

Address Book Entry: (select), remote-SGSN

Service: GTP

GTP Inspection Object: GPRS1 (select)

Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), remote-SGSN

Destination Address:

Address Book Entry: (select), local-GGSN

Service: GTP

GTP Inspection Object: GPRS1 (select)

Action: Permit

CLI

1. GTP Inspection Object

```
ns500-> set gtp configuration gprs1
ns500(gtp:gprs1)-> exit
ns500-> save
```

2. Interfaces

```
ns500-> set interface ethernet3/2 zone trust
ns500-> set interface ethernet3/2 ip 10.1.1.1/24
ns500-> set interface ethernet1/2 zone untrust
ns500-> set interface ethernet1/2 ip 1.1.1.1/24
```

3. Addresses

```
ns500-> set address trust local-ggsn 10.1.1.0/32
ns500-> set address untrust remote-sgsn 2.2.2.5/32
```

4. Policies

```
ns500-> set policy from trust to untrust local-ggsn remote-sgsn gtp permit
```

The system returns a policy ID, for example: policy id = 4

```
ns500-> set policy id 4 gtp gprs1
ns500-> set policy from untrust to trust remote-sgsn local-ggsn gtp permit
```

The system returns a policy ID, for example: policy id = 5

```
ns500-> set policy id 5 gtp gprs1
ns500-> save
```

GTP INSPECTION OBJECT

To enable the NetScreen device to perform the inspection of GTP traffic, you must create a GTP Inspection Object and then apply it to a policy. GTP Inspection Objects provide more flexibility in that they allow you to configure multiple policies each enforcing different GTP configurations. You can configure the NetScreen device to control GTP traffic differently based on source and destination zones and addresses, action, and so on.

Note that to configure GTP features, you must enter the context of a GTP configuration. Furthermore, in the CLI, to save your settings, you must first exit the GTP configuration, and then enter the save command.

Example: Creating a GTP Inspection Object

In this example you create a GTP Inspection Object named LA-NY where you preserve most of the default values, but enable the Sequence Number Validation and GTP-in-GTP Denied features.

WebUI

Objects > GTP > New: Enter the following, and then click **Apply**.

GTP Name: LA-NY

Sequence Number Validation: (select)

GTP-in-GTP Denied: (select)

CLI

```
ns500-> set gtp configuration la-ny
ns500(gtp:la-ny)-> set seq-number-validated
ns500(gtp:la-ny)-> set gtp-in-gtp-denied
ns500(gtp:la-ny)-> exit
ns500-> save
```

GTP MESSAGE FILTERING

When a NetScreen device receives a GTP packet, it checks the packet against policies configured on the device. If the packet matches a policy, the NetScreen device then inspects the packet according to the GTP configuration applied to the policy. If the packet fails to meet any of the GTP configuration parameters, the NetScreen device drops the packet.

This section describes features that constitute a GTP configuration and by which the NetScreen device performs GTP traffic inspection.

Packet Sanity Check

The NetScreen device performs a GTP packet sanity check to determine if a packet is a valid UDP and GTP packet. By performing a sanity check, the NetScreen device protects its GSN resources by preventing them from trying to process malformed GTP packets.

When performing the GTP packet sanity check, the NetScreen device examines the header of each GTP packet for the following:

- GTP release version number—ScreenOS GPRS supports versions 0 and 1 (including GTP')
- Appropriate setting of predefined bits—which predefined bits depends on the GTP release version number
- Protocol type—for version 1 (including GTP')
- UDP/TCP packet length

If the packet does not conform to UDP and GTP standards, the NetScreen device drops the packet. This prevents the NetScreen device from forwarding malformed or forged traffic. The NetScreen device performs GTP packet sanity checking automatically; there is no need to configure this feature.

Note: NetScreen complies to GTP standards established by the 3GPP (3rd Generation Partnership Project). For more information on these standards, refer to the following technical specification documents:

- 3GPP TS 09.60 v6.9.0 (2000-09)
- 3GPP TS 29.060 v3.8.0 (2001-03)
- 3GPP TS 32.015 v3.9.0 (2002-03)

Message Length Filtering

You can configure the NetScreen device to drop packets that do not meet the minimum or maximum message lengths that you specify. In the GTP header, the message length field indicates the length, in octets, of the GTP payload. It does not include the length of the GTP header itself, the UDP header, or the IP header. The default minimum and maximum GTP message lengths are 0 and 1452, respectively.

Example: Setting GTP message lengths

In this example, you configure the minimum GTP message length to be 8 octets and the maximum GTP message length to be 1200 octets for the “GPRS1” GTP Inspection Object.

WebUI

Objects > GTP > Edit (GPRS1): Enter the following, and then click **Apply**:

Minimum Message Length: 8

Maximum Message Length: 1200

CLI

```
ns500-> set gtp configuration gprs1
ns500(gtp:gprs1)-> set min-message-length 8
ns500(gtp:gprs1)-> set max-message-length 1200
ns500(gtp:gprs1)-> exit
ns500-> save
```

Message Type Filtering

You can configure the NetScreen device to filter GTP packets and permit or deny them based on their message type. By default, the NetScreen device permits all GTP message types.

A GTP message type includes one or many messages. When you permit or deny a message type, you automatically permit or deny all messages of the specified type. For example, if you select to drop the **sgsn-context** message type, you thereby drop “sgsn context request”, “sgsn context response”, and “sgsn context acknowledge” messages. For more information on message types, see [“Supported Message Types” on page 21](#).

You permit and deny message types based on the GTP version number. For example, you can deny message types for one version while you permit them for the other version.

Example: Permitting and Denying Message Types

In this example, for the “GPRS1” GTP configuration, you configure the NetScreen device to drop the error-indication and failure-report message types—both for version 1.

WebUI

Objects > GTP > Edit (GPRS1) > Message Drop: Select the following in the Version 1 column, and then click **Apply**:

Error Indication: (select)

Failure Report Request/Response: (select)

CLI

```
ns500-> set gtp configuration gprs1
ns500(gtp:gprs1)-> set drop error-indication
ns500(gtp:gprs1)-> set drop failure-report
ns500(gtp:gprs1)-> exit
ns500-> save
```

Supported Message Types

The following table lists the GTP messages supported in GTP Releases 1997 and 1999 (including charging messages for GTP') and the message types that you can use to configure GTP message type filtering.

Message	Message Type	Version 0	Version 1
create AA pdp context request	create-aa-pdp	✓	
create AA pdp context response	create-aa-pdp	✓	
create pdp context request	create-pdp	✓	✓
create pdp context response	create-pdp	✓	✓
Data record request	data-record	✓	✓
Data record response	data-record	✓	✓
delete AA pdp context request	delete-aa-pdp	✓	
delete AA pdp context response	delete-aa-pdp	✓	
delete pdp context request	delete-pdp	✓	✓
delete pdp context response	delete-pdp	✓	✓
echo request	echo	✓	✓
echo response	echo	✓	✓
error indication	error-indication	✓	✓
failure report request	failure-report	✓	✓
failure report response	failure-report	✓	✓
forward relocation request	fwd-relocation		✓
forward relocation response	fwd-relocation		✓
forward relocation complete	fwd-relocation		✓
forward relocation complete acknowledge	fwd-relocation		✓
forward SRNS context	fwd-srns-context		✓

Message	Message Type	Version 0	Version 1
forward SRNS context acknowledge	fwd-srns-context		✓
identification request	identification	✓	✓
identification response	identification	✓	✓
node alive request	node-alive	✓	✓
node alive response	node-alive	✓	✓
note MS GPRS present request	note-ms-present	✓	✓
note MS GPRS present response	note-ms-present	✓	✓
pdu notification request	pdu-notification	✓	✓
pdu notification response	pdu-notification	✓	✓
pdu notification reject request	pdu-notification	✓	✓
pdu notification reject response	pdu-notification	✓	✓
RAN info relay	ran-info		✓
redirection request	redirection	✓	✓
redirection response	redirection	✓	✓
relocation cancel request	relocation-cancel		✓
relocation cancel response	relocation-cancel		✓
send route info request	send-route	✓	✓
send route info response	send-route	✓	✓
sgsn context request	sgsn-context	✓	✓
sgsn context response	sgsn-context	✓	✓
sgsn context acknowledge	sgsn-context	✓	✓
supported extension headers notification	supported-extension		✓
g-pdu	gtp-pdu	✓	✓

Message	Message Type	Version 0	Version 1
update pdp context request	update-pdp	✓	✓
updated pdp context response	update-pdp	✓	✓
version not supported	version-not-supported	✓	✓

Access Point Name Filtering

An Access Point Name (APN) is an Information Element (IE) included in the header of a GTP packet that provides information on how to reach a network. An APN is composed of two elements:

- A network ID, which identifies the name of an external network such as “mobiphone.com”
- An operator ID, which uniquely identifies the operators’ PLMN such as “mnc123.mcc456”

By default, the NetScreen device permits all APNs. However, you can configure the device to perform APN filtering to restrict roaming subscribers’ access to external networks. You can configure up to 2000 APNs.

To enable APN filtering, you must specify one or more APNs. To set an APN, you need to know the domain name of the network (for example, “mobiphone.com”), and the operator ID. Because the domain name (network ID) portion of an APN can potentially be very long and contain many characters, you can use the wildcard “*” as the first character of the APN. The wild card indicates that the APN is not limited only to “mobiphone.com”, but also includes all the characters that might precede it.

You must also set a Selection Mode for the APN. The Selection Mode indicates the origin of the APN and whether or not the HLR (Home Location Register) verified the user-subscription. You set the Selection Mode according to the security needs of your network. The possible Selection Modes are the following:

- **Mobile Station** – MS-provided APN, subscription not verified
This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user’s subscription to the network.
- **Network** – Network-provided APN, subscription not verified
This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user’s subscription to the network.

- **Verified** – MS or Network-provided APN, subscription verified

This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.

APN filtering applies only to “create pdp request” messages. When performing APN filtering, the NetScreen device inspects GTP packets looking for APNs that match APNs that you set. If the APN of a GTP packet matches an APN that you specified, the NetScreen device then verifies the Selection Mode and only forwards the GTP packet if both the APN and the Selection Mode match the APN and the Selection Mode that you specified. Because APN filtering is based on perfect matches, using the wildcard “*” when setting an APN suffix can prevent the inadvertent exclusion of APNs that you would otherwise authorize. The NetScreen device automatically denies all other APNs that do not match.

Additionally, a NetScreen device can filter GTP packets based on the combination of an IMSI prefix and an APN.

Example: Setting an APN and a Selection Mode

In this example, you set “mobiphone.com.mnc123.mcc456.gprs” as an APN, and you use the wildcard “*”. You also set Network as the Selection Mode.

WebUI

Objects > GTP > Edit (GPRS1) > APN > New: Enter the following, and then click **OK**:

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs

Selection Mode: Network (select)

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set apn *mobiphone.com.mnc123.mcc456.gprs selection net
ns500(gtp:gprs1)-> exit
ns500-> save
```

Example: Setting a combined IMSI prefix and APN filter

In this example, you set “mobiphone.com.mnc123.mcc456.gprs” as an APN using the wildcard “*” and permit all Selection Modes for this APN. You also set the IMSI prefix for a known PLMN, which is 246565¹.

WebUI

Objects > GTP > Edit (GPRS1) > APN: Enter the following, and then click **OK**:

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs

Mobile Country-Network Code: 246565

Selection Mode: Mobile Station, Network, Verified (select)

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set mcc-mnc 246565 apn *mobiphone.com.mnc123.mcc456.gprs
    pass2
ns500(gtp:gprs1)-> exit
ns500-> save
```

-
1. The MCC-MNC pair can be five or six digits.
 2. The variable “pass” in the CLI is equal to selecting all three Selection Modes in the WebUI as it permits traffic from all Selection Modes for the specified APN.

IMSI Prefix Filtering

A GSN (GPRS Support Node) identifies a mobile station by its IMSI (International Mobile Station Identity). An IMSI is composed of three elements: the MCC (Mobile Country Code), the MNC (Mobile Network Code), and MSIN (Mobile Subscriber Identification Number). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or PLMN.

You can configure the NetScreen device to deny GTP traffic coming from non-roaming partners by setting IMSI prefixes. By default, a NetScreen device does not perform IMSI prefix filtering on GTP packets. By setting IMSI prefixes, you configure the NetScreen device to filter "create pdp request" messages and only permit GTP packets with IMSI prefixes that match the ones you set. The NetScreen device drops GTP packets with IMSI prefixes that do not match any of the IMSI prefixes that you set. You can set up to 1000 IMSI prefixes.

Additionally, you can filter GTP packets based on the combination of an IMSI prefix and an APN, see ["Example: Setting a combined IMSI prefix and APN filter"](#) on page 25.

Example: Setting an IMSI Prefix

In this example, you enable IMSI prefix filtering in the "GPRS1" GTP Inspection Object by setting an IMSI prefix: 246565³.

WebUI

Objects > GTP > Edit (GPRS1) > APN+IMSI: Enter the following, and then click **OK**:
Mobile Country-Network Code: 246565

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set mcc-mnc 246565
ns500(gtp:gprs1)-> exit
ns500-> save
```

3. The MCC-MNC pair can be five or six digits.

Disabling IMSI Prefix Filtering

You can disable IMSI prefix filtering by removing all MCC-MNC pairs set on the NetScreen device. Once you remove all the IMSI prefixes, the NetScreen device no longer inspects “create pdp request” messages for valid IMSI prefixes and permits all MCC-MNC pairs.

Example: Disabling IMSI Prefix Filtering

In this example, you remove the IMSI prefix you previously set for the “GPRS1” GTP Inspection Object, which is 246565.

Note: This example assumes that there is only one IMSI prefix configured in the GTP Inspection Object. To disable IMSI prefix filtering, you must remove all IMSI prefixes set in a GTP configuration.

WebUI

Objects > GTP > Edit (GPRS1) > APN+IMSI: Click **Remove** for the 246565 Mobile Country Network Code, and then answer **OK** to the prompt asking you to confirm the removal.

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> unset mcc-mnc 246565
ns500(gtp:gprs1)-> exit
ns500-> save
```

Messages Rate Limiting

You can configure the NetScreen device to limit the rate of network traffic going to a GSN. You can set separate thresholds, in packets per second, for GTP-Control (GTP-C) messages. GTP-C messages can potentially overwhelm a GSN as they require processing and replying. By setting a rate limit on GTP-C messages, you can protect your GSNs from possible Denial of Service (DoS) attacks such as Border Gateway bandwidth saturation⁴ and GTP flood⁵.

This feature limits the rate of traffic sent to each GSN from the NetScreen firewall. The default rate is “unlimited”.

Example: Setting a Rate Limit

In the following example, you limit the rate of incoming GTP-C messages to 300 packets per second.

WebUI

Objects > GTP > Edit (GPRS1): Enter the following, and then click **Apply**:

Control Plane Traffic Rate Limit: 300

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set limit rate 300
ns500(gtp:gprs1)-> exit
ns500-> save
```

-
4. A malicious operator connected to the same GRX as your PLMN can generate enough network traffic directed at your Border Gateway, so that legitimate traffic is starved for bandwidth in or out of your PLMN, thus denying roaming access to or from your network.
 5. GTP traffic can flood a GSN, forcing it to spend its CPU cycles processing illegitimate data. This can prevent subscribers from roaming, forwarding data to external networks, or preventing a GPRS attach to the network.

Sequence Number Validation

You can configure a NetScreen device to perform Sequence Number Validation.

The header of a GTP packet contains a Sequence Number field. This number indicates to the GGSN receiving the GTP packets the order of the packets. During the PDP context activation stage, a sending GGSN uses zero (0) as the Sequence Number value for the first G-PDU it sends through a tunnel to another GGSN. The sending GGSN increments the Sequence Number value for each following G-PDU it sends. The value resets to zero when it reaches 65535.

During the PDP context activation stage, the receiving GGSN sets its counter to zero. Subsequently, whenever the receiving GGSN receives a valid G-PDU, the GGSN increments its counter by one. The counter resets to zero when it reaches 65535.

Normally, the receiving GGSN compares the Sequence Number in the packets it received with the sequence number from its counter. If the numbers correspond, the GGSN forwards the packet, if they differ, the GGSN drops the packet. By implementing a NetScreen device between the GGSNs, the device can perform this validation for the GGSN and drop “out-of-sequence” packets. This feature helps conserve GGSN resources by preventing the unnecessary processing of invalid packets.

Example: Enabling Sequence Number Validation

In this example, you enable the Sequence Number Validation feature.

WebUI

Objects > GTP > Edit (GPRS1): Select **Sequence Number Validation**, and then click **Apply**.

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set seq-number-validated
ns500(gtp:gprs1)-> exit
ns500-> save
```

IP Fragmentation

A GTP packet consists of the message body, GTP header, and UDP and IP header. If the resulting IP packet is larger than the MTU on the transferring link, the sending SGSN or GGSN performs an IP fragmentation.

By default, a NetScreen device buffers IP fragments until it receives a complete GTP message, and then performs the inspection of the GTP message.

GTP-in-GTP Packet Filtering

You can configure a NetScreen device to detect and drop a GTP packet that contains another GTP packet in its message body.

Example: Enabling GTP-in-GTP Packet filtering

In this example, you enable the NetScreen device to detect and drop GTP packets that contain a GTP packet in the message body.

WebUI

Objects > GTP > Edit (GPRS1): Select **GTP-in-GTP Denied**, and then click **Apply**.

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set gtp-in-gtp-denied
ns500(gtp:gprs1)-> exit
ns500-> save
```

GTP TUNNELS

A GTP tunnel enables the transmission of GTP traffic between GSNs using the GPRS Tunneling Protocol (GTP). There are two types of tunnels: a tunnel for GTP-U messages (user data) and a tunnel for GTP-C (signaling and control) messages.

The following section provides information on GTP tunnels and describes how you can configure the NetScreen device to manage them.

GTP Tunnel Limiting

You can configure the NetScreen device to limit the number of GTP tunnels. The GSNs to which this limit applies is specified in the policy to which you append the GTP Inspection Object. This feature prevents from exceeding the capacity of the GSNs.

Example: Setting GTP Tunnel Limits

In the following example, you limit the number of roaming GTP tunnels to 800 for the “GPRS1” GTP Inspection Object.

WebUI

Objects > GTP > Edit (GPRS1): Enter the following, and then click **Apply**:

Maximum Number of Tunnels

Limited to tunnels: (select), 800

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set limit tunnel 800
ns500(gtp:gprs1)-> exit
ns500-> save
```

Stateful Inspection

Following a series of GTP packet verifications (see [“GTP Message Filtering” on page 18](#)), the NetScreen device then verifies the GTP packet against the current GTP tunnel state. The NetScreen device bases its action of forwarding or dropping a GTP packet on previous GTP packets it received. For example, a request message precedes a response message, so if the NetScreen device receives a “create pdp context response” message when it did not previously receive a “create pdp context request” message, the NetScreen device drops the response message.

Basically, if it receives a GTP packet that does not belong in the current GTP state model, the NetScreen device drops the packet. The following are simplified examples of GTP state models.

GTP Tunnel Establishment and Teardown

A mobile station wants to reach an external network “www.buygadgets.com” and performs a GPRS attach with an SGSN to initiate a GTP tunnel establishment. The SGSN sends a “create pdp context request” message to a GGSN. If the GGSN finds “www.buygadgets.com” in its records, it replies with a “create pdp context response” message. This exchange of messages between the SGSN and the GGSN establishes a GTP tunnel through which the MS can send GTP User messages to the external network.

To terminate the communication, the MS performs a GPRS detach with the SGSN to initiate the GTP tunnel teardown. The SGSN sends a “delete pdp context request” message to the GGSN. The GGSN replies with a “delete pdp context response” message and deletes the GTP tunnel from its records. When the SGSN receives the response, it also removes the GTP tunnel from its records.

A NetScreen device can receive multiple requests to establish GTP tunnels for different GSNs simultaneously. To help keep track of all tunnels (tunnel status and log messages for the different tunnels), a NetScreen device assigns a unique index to each tunnel upon its creation. That tunnel index appears for each logged GTP tunnel message.

Inter SGSN Routing Area Update

When an MS moves out of the range of the current SGSN and enters a new SGSN area, the new SGSN sends a “sgsn context request” to the old SGSN asking it to transfer all information it has on the MS. The old SGSN responds with a “sgsn context response” message and sends the new SGSN all the information it has on the MS. Upon receiving the response and information, the new SGSN confirms reception by sending a “sgsn context acknowledge” message to the old SGSN.

From this point on, the old SGSN forwards to the new SGSN any new T-PDUs it receives for the MS. To complete this “hand over” procedure, the new SGSN must send an “update pdp context request” message to the GGSN to which the GGSN replies with a “update pdp context response” message.

In the case where the SGSNs are located in different PLMNs, all the GTP messages go through the NetScreen device. In the case where the two SGSNs are in the same PLMN and the GGSN is in a different PLMN, only the “update pdp context request/response” messages go through the NetScreen device.

Tunnel Failover for High Availability

ScreenOS supports two HA (high availability) modes: active-active when the NetScreen device is in Route mode and active-passive when the NetScreen device is in either Route or Transparent mode. In essence, two NetScreen devices in an HA configuration act as master and backup devices. The backup device mirrors the master’s configuration, including existing GTP tunnels, and is ready to take over the duties of the master device if the master fails. The failover between master and backup is rapid and invisible to the user.

During failover, established GTP tunnels remain active and intact, but GTP tunnels in the process of establishment are lost. For these, you have to re-initiate GTP tunnel establishment after a failover. It is also possible that GTP tunnels in the process of teardown (or termination) miss the confirmation message and are left hanging on the NetScreen device. Hanging GTP tunnels can occur for various reasons. With regards to HA, a hanging GTP tunnel occurs when the GSN at one end of a tunnel sends the GSN at the other end of the tunnel a “delete pdp context request” message, and while it is waiting for the response, a failure occurs disrupting the communication and preventing the GSN from receiving the “delete pdp context response” message (confirming the deletion) from the other GSN. The GSN that sent the confirmation message simultaneously deleted its pdp context while the GSN at the other end of the GTP tunnel is left hanging, still waiting for the deletion confirmation.

You can configure the NetScreen device to remove hanging GTP tunnels. For more information, see [“Hanging GTP Tunnel Cleanup” on page 34](#).

For more information on HA and to learn how to configure NetScreen devices for high availability, refer to Volume 8, “High Availability”, in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Hanging GTP Tunnel Cleanup

This feature removes hanging GTP tunnels on the NetScreen device. GTP tunnels may hang for a number of reasons, for instance, “delete pdp context response” messages might get lost on a network or a GSN might not get properly shut down. You can configure the NetScreen device to detect and remove hanging GTP tunnels automatically.

When you set a GTP tunnel timeout value, the NetScreen device automatically identifies as “hanging” any GTP tunnel that is idle for the period of time specified by the timeout value and removes it. The default GTP tunnel timeout value is 24 hours.

Example: Setting the Timeout for GTP Tunnels

In this example, you set the GTP tunnel timeout for the “GPRS1” GTP Inspection Object to 12 hours.

WebUI

Objects > GTP > Edit (GPRS1): Enter the following, and then click **Apply**:

Tunnel Inactivity Timeout: 12

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set timeout 12
ns500(gtp:gprs1)-> exit
ns500-> save
```

SGSN AND GGSN REDIRECTION

NetScreen devices support GTP traffic redirection between SGSNs and GGSNs.

- **SGSN Redirection** – An SGSN (A) can send create-pdp-context requests in which it can specify different SGSN IP addresses (SGSN B and SGSN C) for subsequent GTP-C and GTP-U messages. Consequently, the GGSN sends the subsequent GTP-C and GTP-U messages to SGSNs B and C, instead of A.
- **GGSN Redirection** – A GGSN (X) can send create-pdp-context responses in which it can specify different GGSN IP addresses (GGSN Y and GGSN Z) for subsequent GTP-C and GTP-U messages. Consequently, the SGSN sends the subsequent GTP-C and GTP-U messages to GGSNs Y and Z, instead of X.

OVERBILLING ATTACK PREVENTION

You can configure NetScreen devices to prevent GPRS Overbilling attacks. The following section describes the Overbilling attack and then explains the solution.

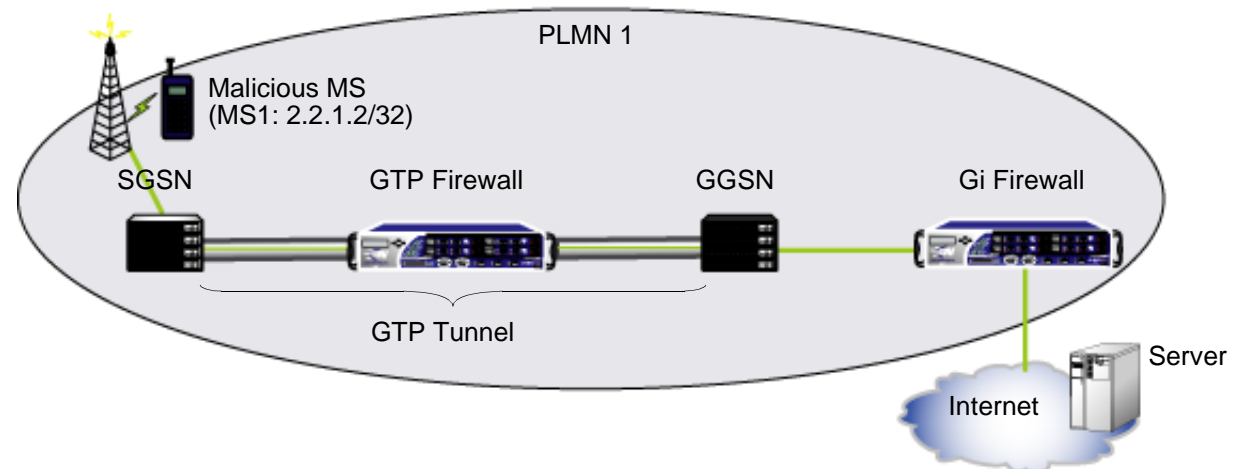
Overbilling Attack Description

Before explaining what an Overbilling attack is, it is important to know that mobile stations get their IP address from an IP pool. This said, an Overbilling attack can occur in various ways. Namely, it can occur when a legitimate subscriber returns his IP address to the IP pool, at which point an attacker can hijack the IP address, which is vulnerable because the session is still open. When the attacker takes control of the IP address, without being detected and reported, the attacker can download data for free (or more accurately, at the expense of the legitimate subscriber) or send data to other subscribers.

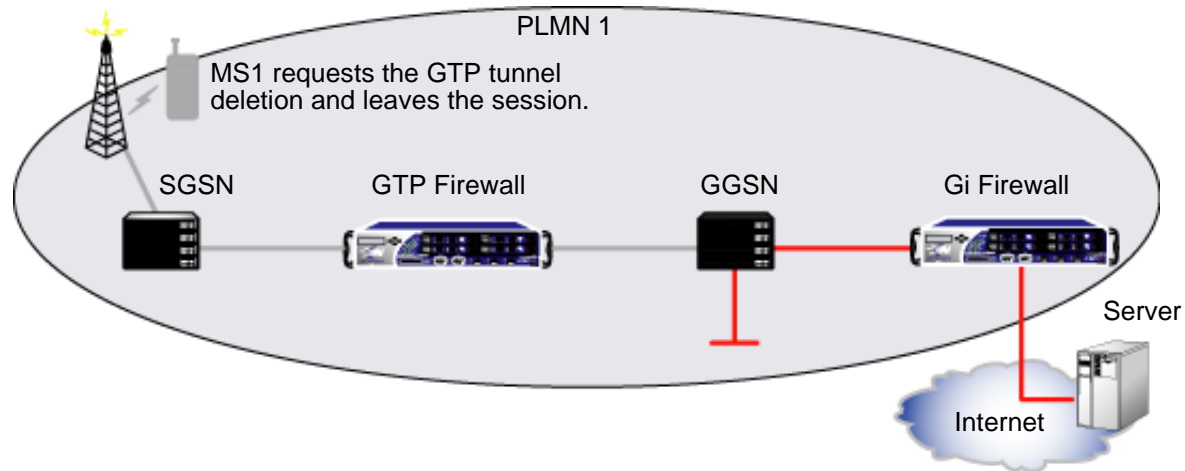
An Overbilling attack can also occur when an IP address becomes available and gets reassigned to another MS. Traffic initiated by the previous MS might be forwarded to the new MS, therefore causing the new MS to be billed for unsolicited traffic. The following illustrations explain this scenario in detail.

The following illustrations describe an Overbilling attack.

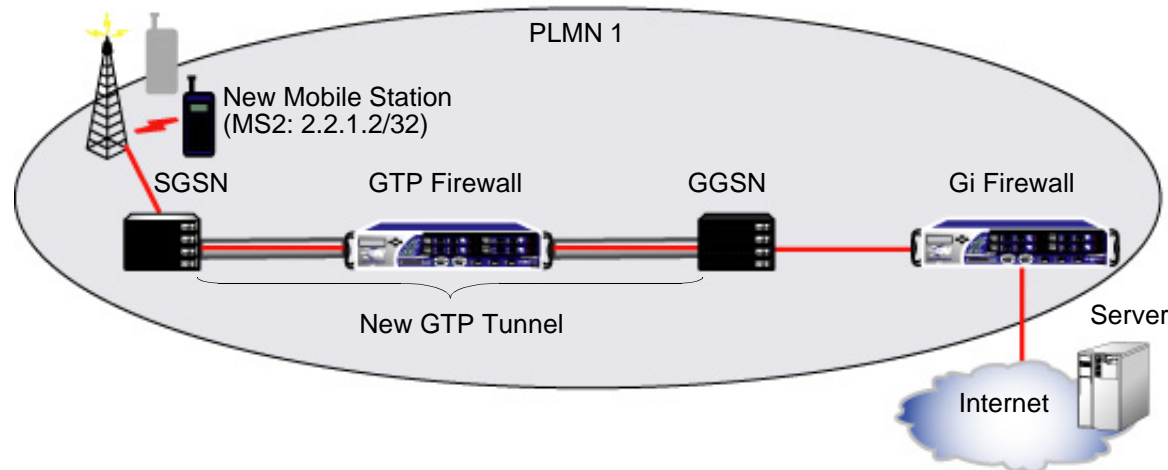
MS1 gets an IP address and requests a GTP tunnel to the GGSN. The SGSN builds a GTP tunnel per MS1's request. MS1 initiates a session with the server.



As the server begins to send packets to MS1, MS1 simultaneously sends a request to the SGSN to delete the GTP tunnel, but leaves open the session to the server. The server continues to send packets to the GGSN. The Gi firewall, not aware that the GTP tunnel was deleted, forwards the packets to the GGSN. The GGSN drops the packets because the GTP tunnel no longer exists.



A new mobile station, MS2 (the victim), sends a request to the SGSN for a GTP tunnel to the GGSN and receives the IP address of 2.2.1.2/32 (the same IP address used by MS1). The SGSN creates a new GTP tunnel to the GGSN. Upon detecting the new GTP tunnel for destination IP address 2.2.1.2, the GGSN, which kept receiving packets for the old session with the same destination IP address, but different MS (MS1), now forwards these packets to MS2. Although MS2 did not solicit this traffic intended for MS1, MS2 gets billed for it.



Overbilling Attack Solution

To protect subscribers of a PLMN from Overbilling attacks requires two NetScreen devices and involves NSGP (NetScreen Gatekeeper Protocol) and the NSGP module.

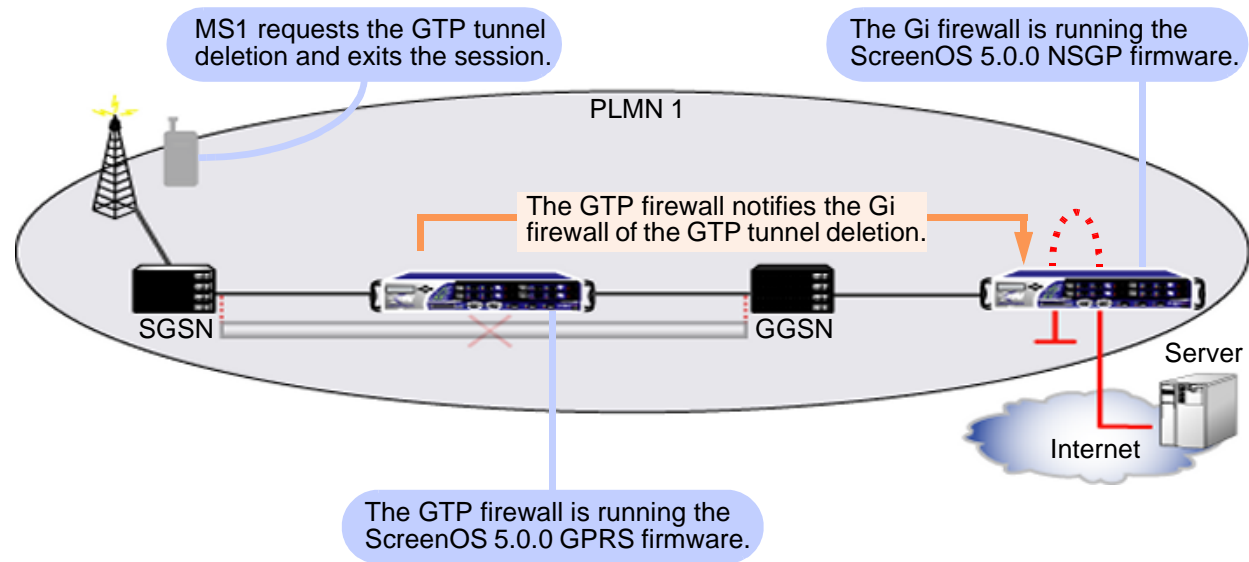
The NSGP module includes two components: the client and the server. The client connects to the server and sends requests, which the server processes. Both client and server support multiple connections to each other and to others simultaneously.

NSGP uses the Transmission Control Protocol (TCP) and monitors the connectivity between client and server by sending Hello messages at set intervals. NSGP currently only supports the “session” type of context, which is a space that holds user-session information, is bound to a security zone, and is identified by a unique number (context ID).

When configuring NSGP on the client and server devices, you must use the same context ID on each device. When the client sends a “clear session” request to the server, the request must include the context ID and IP address of the server. Upon receiving the “clear session” message, the server matches the context ID and then clears the session from its table.

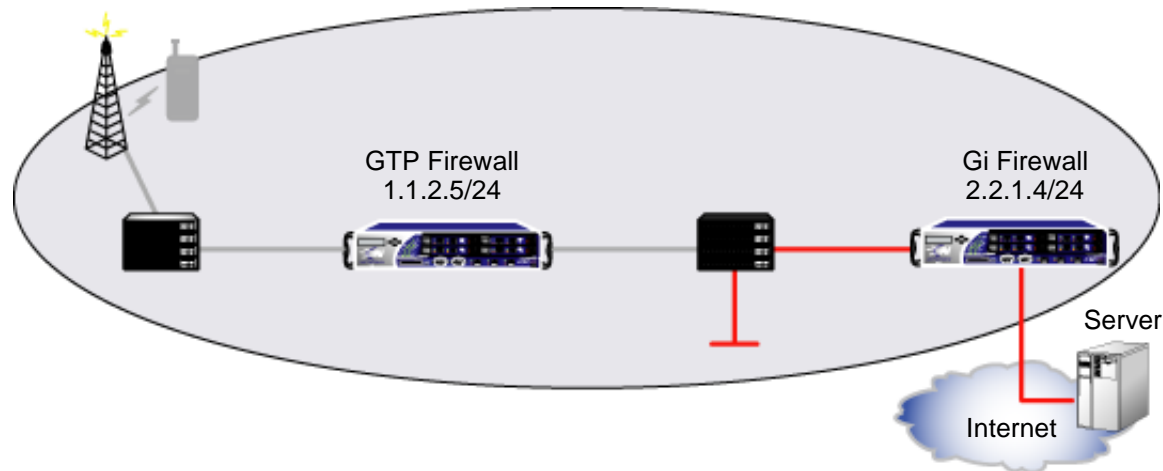
The NetScreen device acting as the Gi firewall (the server) must run the ScreenOS 5.0.0 NSGP firmware, and the other device acting as the GTP firewall (the client) must run the ScreenOS 5.0.0 GPRS firmware. You configure NSGP on the GTP firewall to enable it to notify the Gi firewall when a GTP tunnel is deleted and you configure NSGP on the Gi firewall to enable it to automatically clear sessions whenever the Gi firewall gets a notification from the GTP firewall that a GTP tunnel was deleted. By clearing the sessions, the Gi firewall stops the unsolicited traffic.

After initiating a session with the server and as the server begins to send packets to MS1, MS1 sends a request to the SGSN to delete the GTP tunnel and exits the session. Upon the tunnel deletion, the GTP firewall immediately notifies the Gi firewall of the GTP tunnel deletion. The Gi firewall removes the session from its table. Subsequently, when the server attempts to send packets to the GGSN, the Gi firewall intercepts and drops them. As a result, a new MS, even if using the same IP address as a previous MS, cannot receive and be charged for traffic it did not initiate itself.



Example: Configuring the Overbilling Attack Prevention Feature

In this example you configure NSGP on both the GTP firewall (client) and Gi firewall (server). This example assumes that you configured the “GPRS1” GTP Inspection Object on both the GTP and Gi firewalls.



GTP Firewall (client)

WebUI

Network > Interface > Edit (ethernet1/2): Enter the following, and then click **Apply**:

Zone Name: Untrust (select)

IP Address/Netmask: 1.1.2.5/24

Management Services: Telnet (select)

Objects > GTP > Edit (GPRS1) > Overbilling: Enter the following, and then click **Apply**:

Destination IP: 2.2.1.4

Source Interface: ethernet1/2

Destination Context: 2

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: Any

GTP Inspection Object: GPRS1

Action: Permit

CLI

```
ns500-> set interface ethernet1/2 zone Untrust
ns500-> set interface ethernet1/2 ip 1.1.2.5/24
ns500-> set interface ethernet1/2 manage telnet
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set notify 2.2.1.4 src-interface ethernet1/2 context 2
ns500(gtp:gprs1)-> exit
ns500-> save
ns500-> set policy from untrust to trust any any any permit
```

The system returns a policy ID, for example: policy id = 2

```
ns500-> set policy id 2 gtp gprs1
ns500-> save
```

Gi Firewall (server)

WebUI

Network > Interface > Edit (ethernet1/2): Enter the following, and then click **Apply**:

Zone Name: Untrust (select)

IP Address/Netmask: 2.2.1.4/24

Management Services: Telnet (select)

Other Services: Overbilling (select)

NSGP: Enter the following, click **Add**, and then click **OK**:

Context ID: 2

Zone: Untrust

CLI

```
ns500-> set interface ethernet1/2 zone Untrust
ns500-> set interface ethernet1/2 ip 2.2.1.4/24
ns500-> set interface ethernet1/2 manage telnet
ns500-> set interface ethernet1/2 nsgp
ns500-> set nsgp context 2 type session zone untrust
ns500-> save
```

GTP TRAFFIC MONITORING

NetScreen devices provide comprehensive tools for monitoring traffic flow in real-time. For GTP traffic, you can monitor traffic using the GTP traffic logging and the GTP traffic counting features.

Traffic Logging

With the GTP traffic logging feature, you can configure the NetScreen device to log GTP packets based on their status. You can also specify how much information, basic or extended, you want about each packet. You can use the console, syslog, and the WebUI to view traffic logs.

The status of a GTP packet can be any of the following:

- Forwarded – A packet that the NetScreen device transmits because the GTP policy allows it.
- Prohibited – A packet that the NetScreen device drops because the GTP policy denies it.
- Rate-limited – A packet that the NetScreen device drops because it exceeds the maximum rate limit of the destination GSN.
- State-invalid – A packet that the NetScreen device drops because it failed stateful inspection.
- Tunnel-limited – A packet that the NetScreen device drops because the maximum limit of GTP tunnels for the destination GSN is reached.

Note: By default, traffic logging is disabled on the NetScreen device.

Each log entry in its basic form contains the following information:

- Timestamp
- Source IP address
- Destination IP address
- TID (Tunnel Identifier) or TEID (Tunnel Endpoint Identifier)
- Message type
- Packet status: forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited
- Interface, vsys, or vrouter name (if applicable)
- PLMN or zone name

Each log entry in its extended form contains the following information in addition to the “basic” information:

- IMSI
- MSISDN
- APN
- Selection Mode
- SGSN address for signaling
- SGSN address for user data
- GGSN address for signaling
- GGSN address for user data

Note: For more information on NetScreen monitoring features, refer to the “Monitoring NetScreen Devices” section in Volume 2 of the NetScreen Concepts & Examples ScreenOS Reference Guide.

When enabling the logging of GTP packets with a Packet Rate-Limited status, you can also specify a logging frequency to control the interval at which the NetScreen device logs these messages. For example, if you set the frequency value to 10, the NetScreen device only logs every tenth message above the set rate limit.

By setting a logging frequency, you help conserve resources on the syslog server and on the NetScreen device and can avoid a logging overflow of messages.

Example: Enabling GTP Packet Logging

In this example, for the “GPRS1” GTP Object Inspection, you configure the NetScreen device to log prohibited, rate-limited and state-invalid GTP packets. You opt for basic logging of prohibited and rate-limited packets, with a frequency value of 10 for the rate-limited packets, and extended logging for state-invalid packets.

WebUI

Objects > GTP > Edit (GPRS1) > Log: Enter the following, and then click **Apply**:

Packet Prohibited: Basic (select)

Packet State-invalid: Extended (select)

Packet Rate-Limited: Basic (select)

When Packet Rate Limit is exceeded, log every other messages: 10

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set prohibited basic
ns500(gtp:gprs1)-> set state-invalid extended
ns500(gtp:gprs1)-> set rate-limited basic 10
ns500(gtp:gprs1)-> exit
ns500-> save
```

Traffic Counting

With the GTP traffic counting feature, you can configure the NetScreen device to tally the number of user data and control messages (or bytes of data), received from and forwarded to the GGSNs and SGSNs that it protects. The NetScreen device counts traffic for each GTP tunnel separately and differentiates GTP-User and GTP-Control messages. When a tunnel is deleted, the NetScreen device counts and logs the total number of messages or bytes of data that it received from and forwarded to the SGSN or GGSN.

The log entry for the deletion of a tunnel contains the following information:

- Timestamp
- Interface name (if applicable)
- SGSN IP address
- GGSN IP address
- TID
- Tunnel duration time in seconds
- Number of messages sent to the SGSN
- Number of messages sent to the GGSN

Note: By default, traffic logging is disabled on the NetScreen device.

Example: Enabling GTP Traffic Counting

In this example, you enable GTP traffic counting by messages in the “GPRS1” GTP Inspection Object.

WebUI

Objects > GTP > Edit (GPRS1) > Log: Enter the following, and then click **Apply**:

Traffic Counters: Count by Messages (select)

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> log traffic-counters
ns500(gtp:gprs1)-> exit
ns500-> save
```

Lawful Interception

You can configure a NetScreen device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification. You can identify subscribers by their IMSI or MS-ISDN and log the content of user data and control messages going to and from the subscriber.

You can configure the number of subscribers that the NetScreen device can actively trace concurrently. The default number of simultaneous active traces is three (3). For GTP packets containing user data, you can specify the number of bytes of data to log. You can log partial or complete packets. The default value is zero, which means that the NetScreen device does not log any of the content from a GTP-U packet.

The NetScreen device sends the logged packets to an external server (such as Syslog) dedicated to Lawful Interception operations.

Example: Enabling Lawful Interception

In this example, you enable the NetScreen device to trace a subscriber with 345678 as an IMSI prefix in the “GPRS1” GTP Inspection Object. You also set the number of active traces to 2 and the number of bytes to log to 1064.

WebUI

Objects > GTP > Edit (GPRS1) > Subscriber Trace: Enter the following, and then click **Apply**:

Maximum Simultaneous Active Trace: 2

Trace Message: 1064

Subscribers identified by: Select **IMSI**, enter **345678**, and then click **Add**.

CLI

```
ns500-> set gtp config gprs1
ns500(gtp:gprs1)-> set trace imsi 345678
ns500(gtp:gprs1)-> set trace max-active 2 save-length 1064
ns500(gtp:gprs1)-> exit
ns500-> save
```

GPRS CLI Commands

This chapter covers the NetScreen Command Line Interface (CLI) commands that you can use to configure GTP functionality on the NetScreen device.

Note: You can also configure GTP functionality using the WebUI. For more information, see the [ScreenOS GPRS Concepts & Examples](#) chapter.

This chapter is divided into two sections:

Commands in the main CLI prompt which contain the following CLI commands:

- [“Main CLI Prompt” on page 50](#)
 - [config on page 50](#)
 - [gtp on page 51](#)
 - [interface on page 53](#)
 - [nsgp on page 55](#)
 - [policy on page 58](#)

Commands within a GTP Inspection Object context, which contain the following keywords:

- [“GTP Inspection Object Context” on page 59](#)
 - [apn on page 64](#)
 - [configuration on page 64](#)
 - [drop on page 65](#)
 - [gtp-in-gtp-denied on page 66](#)
 - [limit on page 66](#)
 - [log on page 67](#)
 - [max-message-length on page 67](#)
 - [mcc-mnc on page 68](#)
 - [min-message-length on page 68](#)
 - [notify on page 69](#)
 - [seq-number-validated on page 69](#)
 - [timeout on page 69](#)
 - [trace on page 70](#)
 - [tunnel on page 70](#)

MAIN CLI PROMPT

Execute the commands in this section from the main CLI command prompt.

config

Description: Use the **config** command to display the configuration settings for a NetScreen device. The output of this command includes information on GTP functionality configured on the device.

Syntax

get

`get config`

Keywords and Variables

config

`get config`

config

Displays all configuration information including configured GTP Inspection Objects and their respective GTP parameters. To obtain information about a specific GTP Inspection Object only, enter the **get config** command while you are in the context of that GTP Inspection Object.

gtp

Description: Use the **gtp** commands to obtain information about or remove GTP Inspection Object configurations, and also delete existing GTP tunnels on the NetScreen device.

Note: To configure a GTP Inspection Object, enter the context of that object. The **set** and **unset** commands then become available enabling you to set GTP parameters.

Syntax

clear

```
clear gtp tunnel { number | all }
```

get

```
get gtp configuration [ name_str ]
```

set

```
set gtp configuration name_str
```

Keywords and Variables

gtp

```
clear gtp tunnel { number | all }  
get gtp configuration [ name_str ]  
set gtp configuration name_str
```

gtp

The **clear** command deletes tunnels, thus terminating the connection between the communicating parties. The following specifies which tunnels are deleted:

- *number* Tunnel index (or tunnel ID number)—specifies which tunnel to delete. The NetScreen device assigns an index to each tunnel and uses this number internally.
- **all** Specifies to delete all tunnels on the NetScreen device.

The **get** command displays the GTP Inspection Objects configured on the NetScreen device. If you enter the **get** command while you are in the context of a GTP Inspection Object, you obtain information on the GTP configuration such as tunnel timeout, message length, and APNs.

The **set** command creates a GTP Inspection Object and enters the context of that object.

- **configuration** *name_str* Creates a GTP Inspection Object by assigning it a name or enters the context of an existing GTP Inspection Object.

The **unset** command deletes the specified GTP Inspection Object.

interface

Description: Use the **interface** command to enable or disable an interface on the Gi firewall (the server) for Overbilling Attack notification. To view the complete syntax, keywords and variables for the **interface** command, refer to the *NetScreen CLI Reference Guide Version 5.0.0*.

Syntax

get

```
get interface
```

set

```
set interface interface nsgp [ enforce-ipsec ]
```

unset

```
unset interface interface nsgp
```

Keywords and Variables

interface

```
get interface
set interface interface nsgp [ enforce-ipsec ]
unset interface interface nsgp
```

interface The **get** command displays the configuration and status of NSGP on the NetScreen device. The **set** or **unset** commands enables or disables the exchange of Overbilling Attack information through the specified interface on the NetScreen device. You must set an interface on both NetScreen devices: the GTP firewall (client) and the Gi firewall (server). The interface for the client and server must have different IP addresses. Also, you can enable nsgp on a physical Ethernet interface only.

- **enforce-ipsec** Sets the interface to only accept incoming connections from an IPSec tunnel.

nsgp

Description: Use the **nsgp** command to configure the Overbilling Attack notification feature on the Gi firewall (the server).

Syntax

clear

```
clear nsgp { ip_addr | all }
```

get

```
get nsgp [ detail ]
```

set

```
set nsgp  
{  
  context id_num type session zone zone |  
  md5-authentication password |  
  port port_num  
}
```

unset

```
unset nsgp [ context id_num | md5-authentication | port ]
```

Keywords and Variables

all

```
clear nsgp all
```

all Closes all active connections on the NetScreen device. You can also close active connections on a per IP address basis by entering a specific IP address instead of the keyword “all”.

context

```
set nsgp context id_num type string zone zone  
unset nsgp context id_num
```

context Creates or deletes a context of a specific type for the specified zone.

- **type** *string* Identifies the type of context. Currently NetScreen devices only supports the “session” type.
- **zone** *name* Identifies the zone for which you are creating the context.

Note that the same context must exist on both the client and the server.

detail

```
get nsgp [ detail ]
```

detail Displays NSGP settings and status of contexts within the current root or virtual system. At the root level, this command also displays information for all virtual systems.

md5-authentication

```
set nsgp md5-authentication password  
unset nsgp md5-authentication
```

md5-authentication Directs the Gi firewall to enforce the MD5 auth option specified in the TCP header. You can only specify one MD5 authentication password per NetScreen device.

Note: This command is only available at the root level and not at the vsys level.

port

```
set nsgp port port_num  
unset nsgp port
```

port Identifies the port number used by the Gi firewall to receive Overbilling Attack notifications. The default port number is 12521.

Note: This command is only available at the root level and not at the vsys level.

policy

Description: Use the **policy** command to assign a GTP Inspection Object to a specific policy. To view the complete syntax, keywords and variables for the **policy** command, refer to the *NetScreen CLI Reference Guide Version 5.0.0*.

Syntax

set

```
set policy id id_num gtp name_str
```

unset

```
unset policy id id_num gtp name_str
```

Keywords and Variables

policy

```
set policy id id_num gtp name_str
```

```
unset policy id id_num gtp name_str
```

policy

Enables or disables a GTP Inspection Object on the specified policy.

- **id** *id_num* Identifies the policy to which you are assigning a GTP Inspection Object.
- **gtp** *name_str* Identifies the name of the GTP Inspection Object you are assigning to the policy. Before you can assign a GTP Inspection Object to a policy, you must first create the GTP configuration. For more information, see the **set gtp configuration** command on [page 50](#).

GTP INSPECTION OBJECT CONTEXT

Executing the **set gtp configuration** *name_str* command places the CLI in the specified GTP Inspection Object context. For example, the following command places the CLI in the London-NY GTP Inspection Object context:

```
set gtp configuration london-ny
```

Once you initiate the GTP Inspection Object context, all subsequent command executions apply to the specified GTP Inspection Object configuration (London-NY in this example).

Syntax

get

```
get configuration
```

set

```
set
```

```
{
  apn
  {
    string1 { drop | pass / selection [ ms | net | vrf ] } |
    any
  } |
  gtp-in-gtp-denied |
  limit { rate number | tunnel number } |
  log
  {
    traffic-counters [ byte-counts ] |
    forwarded { basic | extended } |
    prohibited { basic | extended } |
    rate-limited { basic | extended } [ frequency-number ] |

```

1. You can use the “*” wildcard as the first character in the APN, for example, “*.netscreen.com”.

```

    state-invalid { basic | extended } |
    tunnel-limited { basic | extended }
  } |
max-message-length number |
mcc-mnc number apn string { drop | pass | selection [ ms | net | vrf ] |
min-message-length number |
notify ip_addr
  {
  [ port port_num ]
  src-interface interface context id_num [ md5-authentication password ]
  } |
seq-number-validated |
timeout number /
trace
  {
  imsi number |
  max-active number [ save-length number ] |
  msisdn number
  }
}

```

set (drop)

```

set drop
  {
  {
  create-pdp |
  crt-aa-pdp |
  data-record |
  del-aa-pdp |
  delete-pdp |
  echo |
  error-indication |
  failure-report |
  fwd-relocation |

```

```

fwd-srns-context |
g-pdu |
identification |
node-alive |
note-ms-present |
pdu-notification |
ran-info |
redirection |
relocation-cancel |
send-route |
sgsn-context |
supported-extension |
update-pdp |
ver-not-supported
}
[ number ]
}

```

unset

```

unset
{
  apn string |
  gtp-in-gtp-denied |
  limit { rate [ control | user ] | tunnel } |
  log
  {
    traffic-counters [ byte-counts ] |
    forwarded |
    prohibited |
    rate-limited |
    state-invalid |

```

```

    tunnel-limited
    } |
max-message-length |
mcc-mnc number apn string |
min-message-length |
notify |
seq-number-validated |
timeout |
trace
  {
    imsi number |
    max-active |
    msisdn number
  }
}

```

unset (drop)

```

unset drop
{
create-pdp |
crt-aa-pdp |
data-record |
del-aa-pdp |
delete-pdp |
echo |
error-indication |
failure-report |
fwd-relocation |
fwd-srns-context |
g-pdu |
identification |
node-alive |
note-ms-present |

```

```
pdu-notification |
ran-info |
redirection |
relocation-cancel |
send-route |
sgsn-context |
supported-extension |
update-pdp |
ver-not-supported
}
[ number ]
}
```

Keywords and Variables

apn

```
set apn string { drop | pass / selection }  
unset apn string
```

apn

The **set** and **unset** commands allow access or deny access to specific Access Point Names (APNs).

- *string* Sets an APN suffix such as “netscreen.com.mcc123.mnc456.gprs”.
- **drop** Specifies to deny GTP packets from all Selection Modes for this APN.
- **pass** Specifies to permit GTP packets from all Selection Modes for this APN.
- **selection** Specifies one of the following Selection Modes for the APN:
 - **ms** The APN is provided by a mobile station (MS) and the user-subscription is not verified.
 - **net** The APN is provided by a network and the user-subscription is not verified.
 - **vrf** The APN is provided by a network or an MS and the user-subscription is verified.

Note: Because APN filtering is based on perfect match, using the wildcard “*” when setting an APN suffix may prevent the inadvertent exclusion of APNs that you would otherwise authorize. The NetScreen device automatically permits all other APNs that do not match.

configuration

```
get configuration
```

configuration Displays information on the configuration of the current GTP Inspection Object.

drop

```
set drop message_type [ version number ]  
unset drop message_type [ version number ]
```

drop

Enables the NetScreen device to permit or deny messages based on the message type and GTP release version number.

- *number* Specifies the GTP release version number for the specified message type. The possible versions are **0** (for GTP 97) or **1** (GTP 99). If you do not set a version number, the device drops all packets of the specified message type for both GTP release versions.

The following lists CLI keywords that each represent a GTP message type. A GTP message type includes one or many messages. When you set or unset a message type, you automatically permit or deny access to all messages of the specified type.

- **create-pdp** Represents Create PDP Context Request and Create PDP Context Response messages.
- **crt-aa-pdp** Represents Create AA PDP Context Request and Create AA PDP Context Response messages.
- **del-aa-pdp** Represents Delete AA PDP Context Request and Delete AA PDP Context Response messages.
- **delete-pdp** Represents Delete PDP Context Request and Delete PDP Context Response messages.
- **echo** Represents Echo Request and Echo Response messages.
- **error-indication** Represents Error Indication messages.
- **failure-report** Represents Failure Report Request and Failure Report Response messages.
- **fwd-relocation** Represents Forward Relocation Request, Forward Relocation Response, Forward Relocation Complete, and Forward Relocation Complete Acknowledge messages.
- **fwd-srns-context** Represents Forward SRNS Context Request and Forward SRNS Context Response messages.
- **g-pdu** Represents G-PDU and T-PDU messages.
- **identification** Represents Identification Request and Identification Response messages.
- **node-alive** Represents Node Alive Request and Node Alive Response messages.
- **note-ms-present** Represents Note MS GPRS Present Request and Note MS GPRS Present Response messages.

gtp-in-gtp-denied

```
set gtp-in-gtp-denied
unset gtp-in-gtp-denied
```

gtp-in-gtp-denied Enables the NetScreen device to detect and drop GTP packets that contain another GTP packet in its message body.

limit

```
set limit { rate number | tunnel number }
unset limit { rate | tunnel }
```

limit The **set** or **unset** command configures or removes the following types of limits:

- **rate** *number* Specifies a limit in packets per second for GTP-C messages.
- **tunnel** *number* Specifies a limit in the number of GTP tunnels that can be created in the current GTP Inspection Object per GSN.

log

```
set log { ... }
unset log { ... }
```

log

Instructs the NetScreen device to log or cease logging the following information:

- **traffic-counters** The number of user data and control messages the NetScreen device received from and forwarded to the GGSNs and SGSNs it protects.
 - **byte-counts** The number of bytes the NetScreen device received from and forwarded to the GGSNs and SGSNs it protects instead of the number of messages.
- **forwarded** A packet that the NetScreen device transmitted because it was valid.
- **prohibited** A packet that the NetScreen device dropped because it was invalid.
- **rate-limited** A packet that the NetScreen device dropped because it exceeded the maximum rate limit of the destination GSN.
 - **frequency-number** Specifies a logging frequency to control the interval at which the NetScreen device logs messages that it drops because they exceed the set rate limit.
- **state-invalid** A packet that the NetScreen device dropped because it failed stateful inspection.
- **tunnel-limited** A packet that the NetScreen device dropped because the maximum limit of tunnels for the destination GSN was reached, thus a tunnel could not be established.

The following options apply to all the **set log** commands listed above except for **traffic-counters**:

- **basic** Specifies to log the basic Information Elements (IEs) of the GTP message.
- **extended** Specifies to log other IEs in addition to the basic IEs of the GTP message.

For more information on basic and extended logging, see [“Traffic Logging” on page 43](#).

max-message-length

```
set max-message-length number
unset max-message-length
```

max-message-length

Sets the maximum message payload length (in bytes) the NetScreen device accepts for a GTP message. The default maximum message length is 65535 bytes.

mcc-mnc

```
set mcc-mnc number apn string { ... }  
unset mcc-mnc number apn string
```

mcc-mnc

By default, the NetScreen device grants access to any International Mobile Station Identity (IMSI) prefix. An IMSI prefix consists of a Mobile Country Code (MCC) and a Mobile Network Code (MNC). The **set** and **unset** commands allow or deny specific IMSI prefixes. These commands only apply to create pdp context request GTP messages. The MCC-MNC pair can be five or six digits. You can filter GTP packets based on the combination of an IMSI prefix and an APN.

- *number* Specifies an IMSI prefix.
- *string* Specifies an APN.
- **pass** Enables the NetScreen device to permit GTP packets from all Selection Modes for the specified APN.
- **drop** Enables the NetScreen device to deny GTP packets from all Selection Modes for the specified APN.
- **selection** Specifies one of the following Selection Modes for the APN:
 - **ms** The APN is provided by a mobile station (MS) and the user-subscription is not verified.
 - **net** The APN is provided by a network and the user-subscription is not verified.
 - **vrf** The APN is provided by a network or an MS and the user-subscription is verified.

min-message-length

```
set min-message-length number  
unset min-message-length
```

min-message-length

Sets the minimum message payload length (in bytes) the NetScreen device accepts for a GTP message. The default minimum message length is 0 bytes.

notify

```
set notify ip_addr { ... }  
unset notify
```

- notify** The **set** command enables the GTP firewall (the client) to notify the Gi firewall (the server) of the overbilling attack. Such notification directs the server to drop the unwanted traffic. The **unset** command disables the notification feature on the GTP firewall.
- **ip_addr** The IP address of the Gi firewall (server).
 - **port port_num** The port number on which the Gi firewall receives notification messages.
 - **src-interface interface** The interface from which the GTP firewall sends Overbilling Attack notification to the Gi firewall.
 - **context id_num** The number that identifies the context. Note that the same context must exist on the Gi firewall.
 - **md5-authentication password** The MD5 authentication password.

seq-number-validated

```
set seq-number-validated  
unset seq-number-validated
```

- seq-number-validated** Enables or disables the GTP Sequence Number Validation feature. For more information on this feature, see [“Sequence Number Validation” on page 29](#).

timeout

```
set timeout number  
unset timeout
```

- timeout** Sets the tunnel timeout value in hours. The default is 24 hours. Via the process of stateful inspection, if a NetScreen device detects no activity in a tunnel for a specified period of time (timeout), it removes the tunnel from the state table.

trace

```
set trace { ... }  
unset trace { ... }
```

- trace** Enables the NetScreen device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification.
- **imsi number** Indicates the IMSI prefix for which you want the NetScreen device to trace GTP packets.
 - **max-active number** Specifies the maximum number of subscribers that the NetScreen device can trace concurrently for the current GTP Inspection Object. The default value is 3 and the range is 1 to 20.
 - **save-length number** Specifies the number of bytes of data to log for GTP packets containing user data. You can log partial or complete packets. The default value is 0, which means that the NetScreen device does not log any of the content from a GTP-U packet.
 - **msisdn number** Indicates the MS-ISDN for which you want the NetScreen device to trace GTP packets.

tunnel

```
clear gtp tunnel { number | all }  
get gtp tunnel
```

- tunnel** The **get** command displays information on active tunnels on the NetScreen device. The **clear** command deletes tunnels, thus terminating the connection between the communicating parties. The following specifies which tunnels are deleted:
- **number** Tunnel index (or tunnel ID number)—specifies which tunnel to delete. The NetScreen device assigns an index to each tunnel and uses this number internally.
 - **all** Specifies to delete all tunnels on the NetScreen device.

ScreenOS GPRS Troubleshooting

This chapter covers log messages that pertain specifically to ScreenOS GPRS and its purpose is to help you troubleshoot problems that you may encounter in your GPRS network. The chapter presents each log message, explains its meaning, and provides a recommended administrative action.

For information on log messages that relate to ScreenOS, refer to the *NetScreen Message Log Reference Guide* for a complete list of log messages.

SCREENOS GPRS DEBUGGING COMMANDS

Use the following command to collect information that can help you determine the nature of the problem:

```
debug gtp { all | basic | cfg | ext | ha | info | msg | task }
```

Use the following command to view the information resulting from executing a debug command:

```
get dbuf stream
```

SCREENOS GPRS LOG MESSAGES

The following messages appear both in the NetScreen device log and in the debugging information.

Message GTP-DROP <message>: bad EndUserAddr IE

Meaning The NetScreen device dropped the specified message because the address in the EndUserAddr IE was a network address (0.0.0.0) or netmask (255.255.255.255).

Action If you generated the GTP packet, fix the EndUserAddr IE in the GTP packet header. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the EndUserAddr IE in the GTP packet header.

Message GTP-DROP <message>: bad GSNaddr IE

Meaning The NetScreen device dropped the specified message because the address in the GSNaddr IE was a network address (0.0.0.0) or netmask (255.255.255.255).

Action If you generated the GTP packet, fix the GSNaddr IE in the GTP packet header. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GSNaddr IE in the GTP packet header.

Message GTP-DROP <message>: bad GGSNaddr in PDPcontext IE

Meaning The NetScreen device dropped the specified message because the GGSN address in the PDPcontext IE was a network address (0.0.0.0) or netmask (255.255.255.255).

Action If you generated the GTP packet, fix the GGSNaddr in the PDPContext IE in the GTP packet header. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GGSNaddr in the PDPContext IE in the GTP packet header.

- Message** GTP-DROP <message>: bad GTP header
- Meaning** The NetScreen device dropped the specified message because it failed the GTP header sanity check. Possible causes are wrong GTP version number, incorrect number of preset bits, incorrect Protocol Type (PT) bit, and wrong packet length.
- Action** If you generated the GTP packet, fix the GTP packet header. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GTP packet header.
-
- Message** GTP-DROP <message>: bad GTP version for port 2123/2152
- Meaning** The NetScreen device dropped the specified message because it received the message on ports reserved for GTP version 1 messages, but the GTP version of the message was not version 1.
- Action** If you generated the GTP packet, fix its GTP version. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GTP version of the packet.
-
- Message** GTP-DROP <message>: bad GTP version for port 3386
- Meaning** The NetScreen device dropped the specified message because it received the message on ports reserved for GTP version 0 messages, but the GTP version of the message was not version 0.
- Action** If you generated the GTP packet, fix its GTP version. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GTP version of the packet.

- Message** GTP-DROP <message>: bad GTP' version
- Meaning** The NetScreen device dropped the specified message because the message version was not GTP' version 0 or 1.
- Action** If you generated the GTP packet, fix its GTP' version. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to fix the GTP' version of the packet.
-
- Message** GTP-DROP <message>: bad message type for GTP plane/version
- Meaning** The NetScreen device dropped the specified message because its message type was incorrect for the specified GTP plane (GTP-C, GTP-U or GTP') or GTP version number.
- Action** If you generated the GTP packet, change the GTP message type or change the GTP plane. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to change the GTP message type or change the GTP plane.
-
- Message** GTP-DROP <message>: bad state (direction)
- Meaning** The NetScreen device dropped the specified response message because it was going in the wrong direction. For example, a response message must go in the opposite direction of a request message.
- Action** Investigate possible network problems such as routing or layer 2 loops. GSNs that are communicating with each other should not be sending GTP messages through the same path through the NetScreen device.

- Message** GTP-DROP <message>: bad state (GSN)
- Meaning** The NetScreen device dropped the specified message because there was no preceding request message for the current GSN.
- Action** Investigate possible network problems such as packet loss or asymmetric routing, which might have resulted in the NetScreen device not seeing the initial request message. Another possible reason for this invalid packet might be that someone is spoofing response packets. It may also be that this invalid packet is the result of a GSN changing its IP address in the period of time between when a request is sent and a response is received.
-
- Message** GTP-DROP <message>: bad state (message)
- Meaning** The NetScreen device dropped the specified message because this message was not expected in the current state.
- Action** Investigate possible network problems such as packet loss or asymmetric routing, which might have caused the loss of GTP messages during transmission. This invalid packet may also be the result of errors in the GSN or an attacker spoofing GTP messages.
-
- Message** GTP-DROP <message>: bad state (path)
- Meaning** The NetScreen device dropped the specified message because there was no preceding request message for the current path.
- Action** Investigate possible network problems such as packet loss or asymmetric routing, which might have resulted in the NetScreen device not seeing the initial request message. Another possible reason for this invalid packet might be that someone is spoofing response packets.

- Message** GTP-DROP <message>: bad state (tunnel)
- Meaning** The NetScreen device dropped the specified message because there was no preceding request message for the current TID or TEID and GSN.
- Action** Investigate possible network problems such as packet loss or asymmetric routing, which might have resulted in the NetScreen device not seeing the initial request message. Another possible reason for this invalid packet might be that someone is spoofing response packets.
-
- Message** GTP-DROP <message>: bad state (update tunnel)
- Meaning** The NetScreen device dropped the specified message because there was no such tunnel to update.
- Action** Investigate possible network problems such as packet loss or asymmetric routing, which might have resulted in the NetScreen device not seeing the initial request message. Another possible reason for this invalid packet might be that someone is spoofing response packets.
-
- Message** GTP-DROP <message>: chargID IE is zero
- Meaning** The NetScreen device dropped the specified message because the value of its ChargingID IE should not be zero.
- Action** If you generated the GTP packet, modify the ChargeID IE. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the ChargeID IE.

- Message** GTP-DROP <message>: disallowed V0 message
- Meaning** The NetScreen device dropped the specified message because this message type was not permitted by GTP version 0.
- Action** Verify the configuration for message type filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“Message Type Filtering” on page 20](#).
-
- Message** GTP-DROP <message>: disallowed V1 message
- Meaning** The NetScreen device dropped the specified message because this message type was not permitted by GTP version 1.
- Action** Verify the configuration for message type filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“Message Type Filtering” on page 20](#).
-
- Message** GTP-DROP <message>: disallowed IMSI/TID prefix
- Meaning** The NetScreen device dropped the specified message because the IMSI or TID prefix of the message was not permitted.
- Action** Verify the configuration for IMSI prefix filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“IMSI Prefix Filtering” on page 26](#).

- Message** GTP-DROP <message>: disallowed APN with SelectionMode
- Meaning** The NetScreen device dropped the specified message because the APN IE of the message combined with the value of the Selection Mode IE was not permitted.
- Action** Verify the configuration for APN filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“Access Point Name Filtering” on page 23](#).
-
- Message** GTP-DROP <message>: duplicate IE <name_str>
- Meaning** The NetScreen device dropped the specified message because the specified IE was repeated too many times in the message.
- Action** If you generated the GTP packet, correct the duplicate IE. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the duplicate IE.
-
- Message** GTP-DROP <message>: IMSI IE is zero
- Meaning** The NetScreen device dropped the specified message because the value of its IMSI IE should not be zero.
- Action** If you generated the GTP packet, correct the IMSI IE. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the IMSI IE.

- Message** GTP-DROP <message>: inconsistent message length
- Meaning** The NetScreen device dropped the specified message because its GTP length field was inconsistent with the UDP/TCP length standard.
- Action** If you generated the GTP packet, correct the GTP message length. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the GTP message length.
-
- Message** GTP-DROP <message>: sourceIP inconsistent with GSNaddr IE
- Meaning** The NetScreen device dropped the specified message because the address in its GSNaddr IE was different from the source IP address in the UDP/TCP header.
- Action** If you generated the GTP packet, correct the GSNaddr IE. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the GSNaddr IE.
-
- Message** GTP-DROP <message>: missing IE <name_str>
- Meaning** The NetScreen device dropped the specified message because the required specified IE for that message type was missing.
- Action** If you generated the GTP packet, add the missing IE in the GTP header. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to add the missing IE in the GTP header.

- Message** GTP-DROP <message>: non-ascending order IEs
- Meaning** The NetScreen device dropped the specified message because the IEs were not in ascending order.
- Action** If you generated the GTP packet, rearrange the IEs in ascending order. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to rearrange the IEs in ascending order.
-
- Message** GTP-DROP <message>: non-digit TID
- Meaning** The NetScreen device dropped the specified message because the TID was not a digit. The TID may contain an octet, which was neither a digit nor “f” for padding. The TID can only contain digits from 0 to 9 and the letter “f”.
- Action** If you generated the GTP packet, correct the TID. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the TID.
-
- Message** GTP-DROP <message>: non-zero TID/TEID
- Meaning** The NetScreen device dropped the specified message because the TID or TEID should not be 0 (zero).
- Action** If you generated the GTP packet, modify the TID or TEID to not be 0 (zero). If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the TID or TEID to not be 0 (zero).

- Message** GTP-DROP <message>: NSAPI is not 'f' in TID
- Meaning** The NetScreen device dropped the specified message because the NSAPI in the TID was not "f" for padding in this pdu-notification message.
- Action** If you generated the GTP packet, correct the NSAPI in the TID. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to correct the NSAPI in the TID of the GTP packet.
-
- Message** GTP-DROP <message>: rate limit
- Meaning** The NetScreen device dropped the specified message because the rate limit configured on the NetScreen device for GTP-C (GTP-Control) messages was exceeded.
- Action** You can verify the GTP-C messages rate limit configured on the NetScreen device and if you determine that it is too low, you can opt to increase it.
-
- Message** GTP-DROP <message>: rate limit for T-PDU
- Meaning** The NetScreen device dropped the specified message because the rate limit for T-PDU (or GTP-User) messages was exceeded.
- Action** You can verify the GTP-U messages rate limit configured on the NetScreen device and if you determine that it is too low, you can opt to increase it.

Message GTP-DROP <message>: TEIDcontrol IE is zero

Meaning The NetScreen device dropped the specified message because the value of its TEIDcontrol IE should not be zero.

Action If you generated the GTP packet, modify the TEIDcontrol IE to not be zero. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the TEIDcontrol IE in the GTP packet header to not be zero.

Message GTP-DROP <message>: TEIDdata IE is zero

Meaning The NetScreen device dropped the specified message because the value of its TEIDdata IE should not be zero.

Action If you generated the GTP packet, modify the TEIDdata IE to not be zero. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the TEIDdata IE in the GTP packet header to not be zero.

Message GTP-DROP <message>: TEID/TID/IMSI is zero

Meaning The NetScreen device dropped the specified message because the value of its TID—the IMSI part of it—or TEID should not be zero.

Action If you generated the GTP packet, modify the TID (IMSI) or TEID to not be zero. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the TID (IMSI) or TEID of the GTP packet to not be zero.

Message GTP-DROP <message>: too short

Meaning The NetScreen device dropped the specified message because it was too short.

Action Verify the configuration for GTP message length filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“Message Length Filtering” on page 19](#).

Message GTP-DROP <message>: too long

Meaning The NetScreen device dropped the specified message because it was too long.

Action Verify the configuration for GTP message length filtering on the NetScreen device and modify it if need be. For more information on how to do this, see [“Message Length Filtering” on page 19](#).

Message GTP-DROP <message>: tunnel limit

Meaning The NetScreen device dropped the specified message because the GTP tunnel limit on the GSN was exceeded.

Action You can verify the GTP tunnel limit configured on the NetScreen device and if you determine that it is too low, you can opt to increase it.

Message GTP-DROP <message>: unknown IE <name>

Meaning The NetScreen device dropped the specified message because the specified IE was undefined.

Action Verify the configuration of the current GSN for errors or malfunctions.

- Message** GTP-DROP <message>: wrong destination port
- Meaning** The NetScreen device dropped the specified message because the message was received on the wrong port. For example, maybe a GTP-C message was received on a port reserved for GTP-U messages only or a T-PDU message was received on a port reserved for GTP-C messages only.
- Action** Verify the configuration of the current GSN for errors or malfunctions.
-
- Message** GTP-DROP <message>: long extension header
- Meaning** The NetScreen device dropped the specified message because its extension header was too long.
- Action** If you generated the GTP packet, modify the extension header to an acceptable length. If the GTP packet came from an outside source, research who generated the GTP packet and if the source is not malicious, instruct them to modify the extension header to an acceptable length.
-
- Message** GTP-DROP <message>: bad new GSN
- Meaning** The NetScreen device dropped the specified message because the system does not have enough memory to allocate a new GSN.
- Action** No recommended action
-
- Message** GTP-DROP <message>: out of new GSNs
- Meaning** The NetScreen device dropped the specified message because the system does not have enough memory to allocate a new GSN.
- Action** No recommended action

Message GTP-DROP <message>: bad new path

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new path.

Action No recommended action

Message GTP-DROP <message>: out of new paths

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new path.

Action No recommended action

Message GTP-DROP <message>: out of new path requests

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new path.

Action No recommended action

Message GTP-DROP <message>: bad new tunnel

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new tunnel.

Action No recommended action

Message GTP-DROP <message>: out of new tunnel

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new tunnel.

Action No recommended action

Message GTP-DROP <message>: out of second tunnel

Meaning The NetScreen device dropped the specified message because the device does not have enough memory to allocate a new tunnel for the secondary PDP activation.

Action No recommended action

Message GTP-DROP <message>: unknown IE (name_str)

Meaning The NetScreen device dropped the specified message because the specified IE Type is undefined. There might be a compatibility issue with other GSNs.

Action Contact Juniper Networks technical support by visiting www.netscreen.com/cso. (Note: You must be a registered Juniper Networks customer.)



Glossary

APN

Access Point Name. An APN is an IE included in the header of a GTP packet that provides information on how to reach a network. It is composed of two elements: a network ID and an operator ID.

G-PDU

A G-PDU is a user data message. It consists of a T-PDU plus a GTP header.

GGSN

Gateway GPRS Support Node.

Gi interface

The interface between a GSN and an external network or the Internet.

Gn interface

The interface between two GSNs within the same PLMN.

Gp interface

The interface between two GSNs located in different PLMNs.

GPRS

General Packet Radio Service. A packet-based technology that enables high-speed wireless Internet and other data communications. GPRS provides more than three to four times greater speed than conventional GSM systems. Using a packet data service, subscribers are always connected and always online so services are easy and quick to access.

GTP

GPRS Tunneling Protocol.

GTP-C Message

GTP-Control Message. Control plane messages are exchanged between GSN pairs in a path. The control plane messages are used to transfer GSN capability information between GSN pairs, to create, update and delete GTP tunnels and for path management.

GTP-PDU

A GTP Protocol Data Unit is either a GTP-C message or a GTP-U message.

GTP Tunnel

GTP Tunnel. A GTP tunnel in the GTP-U plane is defined for each PDP Context in the GSNs. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and APN (for Tunnel Management messages) or for each MS (for messages not related to Tunnel Management). A GTP tunnel is identified in each node with a TEID, an IP address and a UDP port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.

GTP-U Message

GTP-User Message. User plane messages are exchanged between GSN pairs or GSN/RNC pairs in a path. The user plane messages are used to carry user data packets, and signalling messages for path management and error indication.

GRX

GPRS Roaming Exchange.

GSM

Global System for Mobile Communications.

HLR

Home Location Register.

IE

Information Element.

IMSI

International Mobile Station Identity.

MCC

Mobile Country Code.

MNC

Mobile Network Code.

MSIN

Mobile Subscriber Identification Number.

MS

Mobile Station.

NSAPI

Network Service Access Point Identifier.

PDP

Packet Data Protocol.

PDP Context

A user session on a GPRS network.

PDU

Protocol Data Unit.

PLMN

Public Land Mobile Network. A public network dedicated to the operation of mobile radio communications.

PT

Protocol Type.

SGSN

Serving GPRS Support Node.

Signalling Message

Any GTP-PDU except the G-PDU. GTP signalling messages are exchanged between GSN pairs in a path. The signalling messages are used to transfer GSN capability information between GSN pairs and to create, update and delete GTP tunnels.

T-PDU

A T-PDU is the payload that is tunnelled in the GTP tunnel.

TID

Tunnel Identifier.

TEID

Tunnel Endpoint Identifier. The TEID uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C messages.

UDP

User Datagram Protocol.

Index

A

- active-active HA 5
- active-passive HA 5
- APN 64
 - filtering 4, 23, 24
 - selection mode 23

C

- CLI
 - GTP commands 49
- CLI command
 - all 56
 - apn 64
 - config 50
 - configuration 50, 64
 - context 56
 - drop 65
 - gtp 52
 - interface 54
 - limit 66
 - log 67
 - max-message-length 67
 - mcc-mnc 68
 - min-message-length 68
 - notify 69
 - seq-number-validated 69
 - set (message) 60
 - timeout 69
 - trace 70
 - tunnel 70
 - unset 61
 - unset (message) 62
- conventions v
 - CLI vi
 - WebUI v
- counting 13

G

- GGSN redirection 2
- GTP
 - Access Point Name (APN) filtering 23
 - CLI commands 49
 - commands 51
 - GTP-in-GTP packet filtering 30
 - GTP-in-GTP packets 3
 - IMSI prefix filtering 4, 26
 - IP fragmentation 30
 - message 21
 - message length filtering 4, 19
 - message type 20, 21, 65
 - message type filtering 4, 20
 - messages rate limiting 28
 - packet sanity check 4, 18
 - policy filtering 4
 - policy-based 13
 - protocol 9
 - release 1997 4
 - standards 18
 - stateful inspection 5, 32
 - traffic counting 3, 5, 46
 - traffic logging 3, 5, 43
 - tunnel failover 5, 33
 - tunnel index 3
 - tunnel limiting 5, 31
 - tunnel timeout 34
- GTP inspection object 2, 13, 17
- GTP message
 - version 0 21
 - version 1 21

H

- HA 12, 33
 - active-active 5
 - active-passive 5
- hanging GTP tunnel 5, 33, 34

I

- IMSI prefix filtering 26, 27
- interface
 - Gi 9, 11
 - Gn 9, 10
 - Gp 9, 10
- IP fragmentation 2

L

- L2TP 11
- lawful interception 3, 47
- logging 13

M

- MNC 4
- Mobile Network Code (MNC) 4
- mode
 - NAT 12
 - route 4, 5, 12
 - transparent 4, 5, 12

N

- NAT mode 12

O

- operational modes 12
- overbilling attack
 - description 36
 - solution 38
- overbilling attack prevention 2, 36–42
 - configuring 40

P

- policy 13
- policy, configuring 14

R

rate limiting
 GTP-C messages 28
route mode 4, 5, 12

S

selection mode
 APN 23
 MS 23
 network 23
 verified 24

sequence number validation 2, 29
SGSN redirection 2
stateful inspection 5

T

timeout 34
traffic
 counting 5
 logging 5
 rate limiting 5

transparent mode 4, 5, 12
tunnel failover 5

V

virtual system support 12

W

WebUI 49
 conventions v
wildcard 23, 24, 64