Concepts & Examples
ScreenOS Reference Guide

Volume 13:
General Packet Radio Service

Release 5.4.0, Rev. A

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-015780-01, Revision A

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 Juniper Networks' 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 JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

Chapter 1 Continued

About This Volume

Volume 13: General Packet Radio Service is for GPRS network operators who possess advanced knowledge of GPRS technology.

This volume describes the GTP features in ScreenOS and demonstrates how to configure GTP functionality on a Juniper Networks security device. It contains the following chapter:

- Chapter 1, "GPRS," describes the GPRS Tunneling Protocol (GTP) features in ScreenOS and demonstrates how to configure GTP functionality on a Juniper Networks security device.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces **{ }** is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example:

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

  means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface."

- Variables are in *italic* type:

  set admin user *name1* password *xyz*

In text:

- Commands are in **boldface** type.
- Variables are in *italic* type.

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 1: Images in Manual Illustrations

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

  set address trust “local LAN” 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **“ local LAN ”** becomes **“local LAN”**.

- Multiple consecutive spaces are treated as a single space.

- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, **“local LAN”** is different from **“local lan”**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

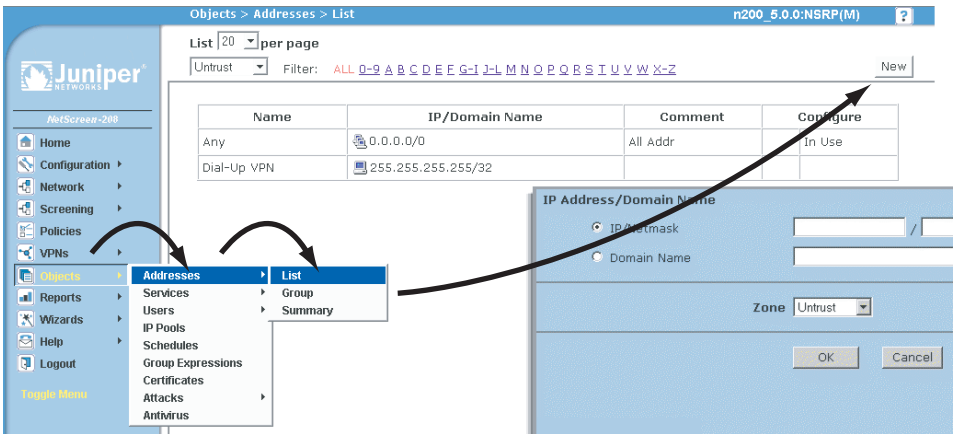
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes (“), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 2: WebUI Navigation



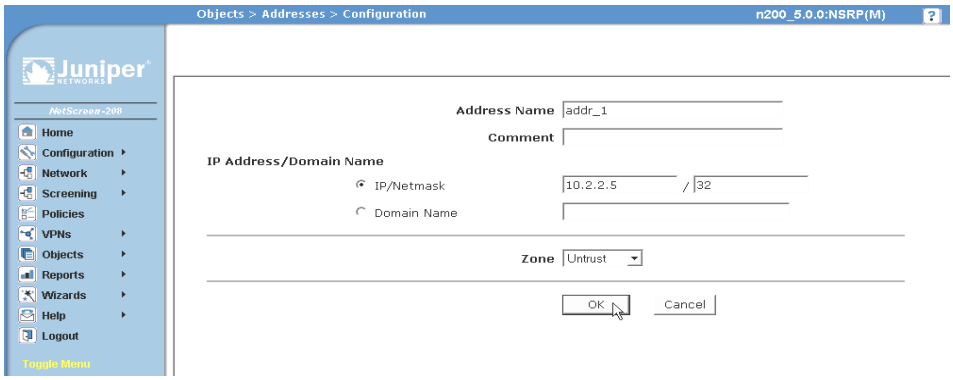
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

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

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

Figure 3: Navigational Path and Configuration Settings



Juniper Networks Documentation

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

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Chapter 1

GPRS

General Packet Radio Service (GPRS) networks connect to several external networks including those of roaming partners, corporate customers, GPRS Roaming Exchange (GRX) 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 plaguing GPRS network operators.

In the GPRS architecture, the fundamental cause of security threats to an operator's network is the inherent lack of security in GPRS Tunneling Protocol (GTP). GTP is the protocol used between GPRS Support Nodes (GSNs). Communication between different GPRS networks is not secure because GTP does not provide any authentication, data integrity, or confidentiality protection. Implementing Internet Protocol Security (IPSec) for connections between roaming partners, setting traffic rate limits, and using stateful inspection can eliminate a majority of the GTP's security risks. Juniper Networks security devices mitigate a wide variety of attacks on the Gp, Gn, and Gi interfaces. The GTP firewall features in ScreenOS address key security issues in mobile operators' networks.

NOTE: Only ISG 2000 devices support GTP functionality.

This chapter describes the GTP features that ScreenOS supports and explains how you can configure them on a Juniper Networks security device. This chapter contains the following sections:

The Security Device as a GPRS Tunneling Protocol Firewall

The GPRS Tunneling Protocol (GTP) is used to establish a GTP tunnel, for individual mobile stations (MS), between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN). A GTP tunnel is a channel between GSNs through which two hosts 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 Juniper Networks GTP-licensed security device provides firewall protection for the following types of GPRS interfaces:

- Gn—The Gn interface is the connection between an SGSN and a GGSN within the same Public Land Mobile Network (PLMN).
- Gp—The Gp interface is the connection between two Public Land Mobile Network 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 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.

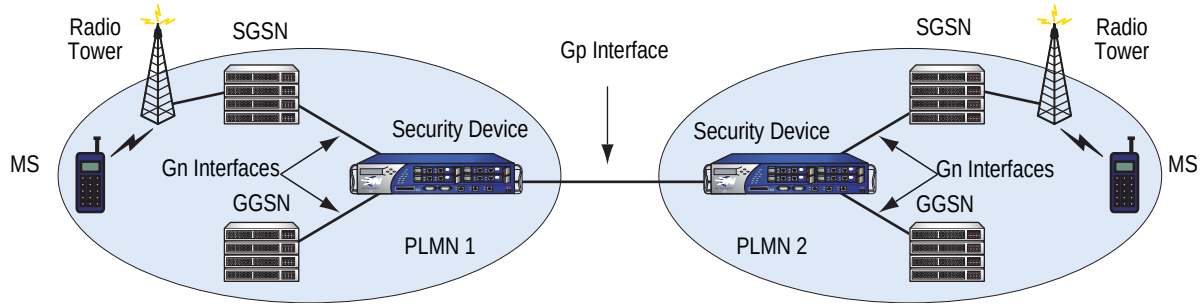
Gp and Gn Interfaces

You implement a security device on the Gn interface to protect core network assets such as the SGSN and GGSN. To secure GTP tunnels on the Gn interface, you place the security device between SGSNs and GGSNs within a common PLMN.

When you implement a security device to 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 the security device so that all traffic, incoming and outgoing, goes through the firewall.

Figure 1 illustrates the placement of Juniper Networks security devices to protect PLMNs on the Gp and Gn interfaces.

Figure 1: Gp and Gn Interfaces



Gi Interface

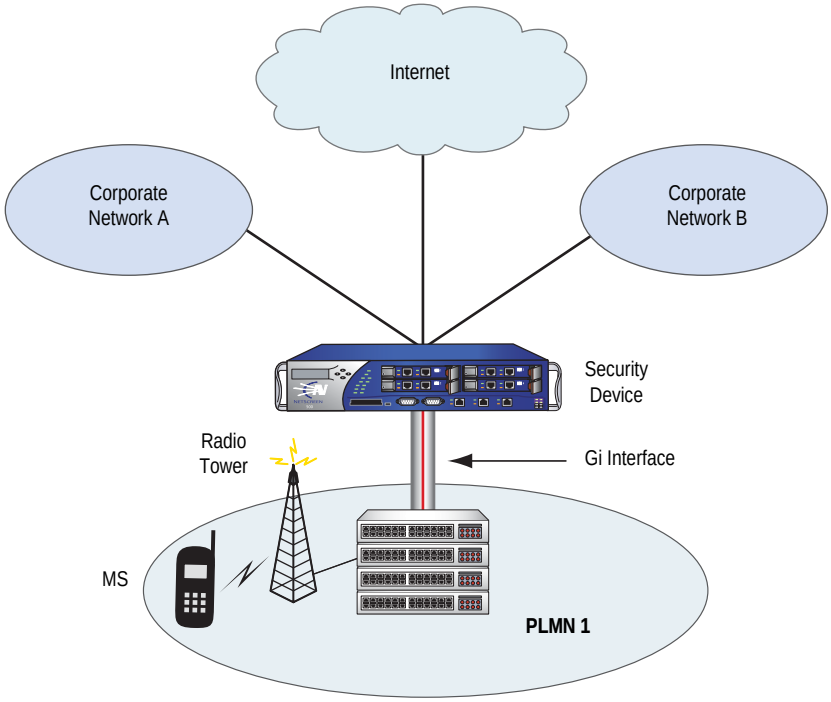
When you implement a security device on the Gi interface, you can simultaneously control traffic for multiple networks, protect a PLMN against the Internet and external networks, and protect mobile users from the Internet and other networks. ScreenOS provides a great number of virtual routers, making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

The security device can securely forward packets to the Internet or destination networks using the Layer 2 Tunneling Protocol (L2TP) for IPSec virtual private network (VPN) tunnels. (Note, however, that Juniper Networks security devices do not support full L2TP.)

For more information about the features and capabilities of virtual routers, see *Volume 7: Routing*.

Figure 2 illustrates the implementation of a security device to protect a PLMN on the Gi interface.

Figure 2: Gi Interface



Operational Modes

ScreenOS supports two interface operational modes with GTP: Transparent mode and Route mode. If you want the security device to participate in the routing infrastructure of your network, you can run it in Route mode. This requires a certain amount of network redesign. Alternatively, you can implement the security device into your existing network in Transparent mode without having to reconfigure the entire network. In Transparent mode, the security device functions as a Layer 2 switch or bridge, and the IP addresses of interfaces are set at 0.0.0.0, making the presence of the security device invisible, or *transparent*, to users.

ScreenOS supports Network Address Translation (NAT) on interfaces and policies that do not have GTP inspection enabled.

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

For more information about operational modes and high availability, see *Volume 2: Fundamentals* and *Volume 11: High Availability*, respectively.

Virtual System Support

Juniper Networks security devices fully support GTP functionality in virtual systems (vsys). To conserve resources, however, we recommend that you use no more than 10 vsys.

Policy-Based GPRS Tunneling Protocol

By default, the PLMN that the security device protects is in the Trust zone. The security 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 security zone 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 security 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 security device to permit, deny, or tunnel GTP traffic. However, this does not enable the device to inspect GTP traffic. In order for the security 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 must first create a GTP inspection object (see “GPRS Tunneling Protocol Inspection Object” on page 7). 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 zone), and you can configure policies that specify multiple source and destination addresses.

In policies, you can enable features such as traffic logging and traffic counting. For more information about policies, see *Volume 2: Fundamentals*.

Example: Configuring Policies to Enable GTP Inspection

In this example, you configure interfaces and 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, then click **Apply**.

   GTP Name: GPRS1

2. **Interfaces**
   Network > Interfaces > Edit (for ethernet1/1): Enter the following, then click **Apply**:

   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24

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

   Zone Name: Untrust
   IP Address/Netmask: 1.1.1.1/24

3. **Addresses**
   Objects > Addresses > List > New: Enter the following, 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, 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, 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, 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**
   set gtp configuration gprs1
   (gtp:gprs1)-> exit
   save

2. **Interfaces**
   set interface ethernet1/1 zone trust
   set interface ethernet1/1 ip 10.1.1.1/24
   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ip 1.1.1.1/24

3. **Addresses**
   set address trust local-ggsn 10.1.1.0/32
   set address untrust remote-sgsn 2.2.2.5/32

4. **Policies**
   set policy from trust to untrust local-ggsn remote-sgsn gtp permit
   The system returns a policy ID, for example: policy id = 4.

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

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

   set policy id 5 gtp gprs1
   save

GPRS Tunneling Protocol Inspection Object

To enable the security device to perform the inspection of GPRS Tunneling Protocol (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 that enforce different GTP configurations. You can configure the security device to control GTP traffic differently based on source and destination zones and addresses, action, and so on.

To configure GTP features, you must enter the context of a GTP configuration. To save your settings in the CLI, you must first exit the GTP configuration, then enter the **save** command.

Example: Creating a GTP Inspection Object

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

WebUI

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

GTP Name: LA-NY
Sequence Number Validation: (select)
GTP-in-GTP Denied: (select)

CLI

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

GTP Message Filtering

When a security device receives a GTP packet, it checks the packet against policies configured on the device. If the packet matches a policy, the device 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 device drops the packet.

This section describes features that constitute a GTP configuration, which the security device uses to perform GTP traffic inspection. It includes the following sections:

- Packet Sanity Check
- Message-Length Filtering
- Message-Type Filtering
- Message-Rate Limiting
- Sequence Number Validation
- IP Fragmentation
- GTP-in-GTP Packet Filtering
- Deep Inspection

Packet Sanity Check

The security device performs a GTP sanity check on each packet to determine if it is a valid UDP and GTP packet. The sanity check protects GPRS Support Node (GSN) resources by preventing them from trying to process malformed GTP packets.

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

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

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

NOTE: Juniper Networks complies with GTP standards established by the 3rd Generation Partnership Project (3GPP). For more information about 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 security device to drop packets that do not meet your specified minimum or maximum message lengths. 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 GPRS GTP inspection object.

WebUI

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

Minimum Message Length: 8
Maximum Message Length: 1200

CLI

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

Message-Type Filtering

You can configure the security device to filter GTP packets and permit or deny them based on their message type. By default, the security 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 about message types, see "Supported Message Types" on page 10.

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 security device to drop the error-indication and failure-report message types for version 1.

WebUI

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

Tunnel Management:
    Error Indication: (select)
Location Management:
    Failure Report Request/Response: (select)

CLI

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

Supported Message Types

Table 1 lists the GPRS Tunneling Protocol (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.

Table 1: GPRS Tunneling Protocol (GTP) Messages

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	✓	✓

Message	Message Type	Version 0	Version 1
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		✓
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	✓	✓

Message	Message Type	Version 0	Version 1
sgsn context response	sgsn-context	✓	✓
sgsn context acknowledge	sgsn-context	✓	✓
supported extension headers notification	supported-extension		✓
g-pdu	gtp-pdu	✓	✓
update pdp context request	update-pdp	✓	✓
updated pdp context response	update-pdp	✓	✓
version not supported	version-not-supported	✓	✓

Message-Rate Limiting

You can configure the security 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. Because GTP-C messages require processing and replies, they can potentially overwhelm a GSN. By setting a rate limit on GTP-C messages, you can protect your GSNs from possible Denial of Service (DoS) attacks such as the following:

- **Border gateway bandwidth saturation:** A malicious operator connected to the same GRX as your PLMN can direct so much network traffic at your Border Gateway that legitimate traffic is starved for bandwidth in or out of your PLMN, thus denying roaming access to or from your network.

- **GTP flood:** 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, and can prevent a GPRS from attaching to the network.

This feature limits the rate of traffic sent to each GSN from the Juniper Networks 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, then click **Apply**:

Control Plane Traffic Rate Limit: 300

CLI

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

Sequence Number Validation

You can configure a security 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 Packet Data Protocol (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 security device between the GGSNs, the device can perform this validation for the GGSN and drop packets that arrive out of sequence. 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**, then click **Apply**.

CLI

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

IP Fragmentation

A GTP packet consists of the message body and three headers: GTP, UDP and IP. If the resulting IP packet is larger than the message transmission unit (MTU) on the transferring link, the sending SGSN or GGSN performs an IP fragmentation.

By default, a security device buffers IP fragments until it receives a complete GTP message, and then inspects the GTP message.

GTP-in-GTP Packet Filtering

You can configure a security 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 security 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**, then click **Apply**.

CLI

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

Deep Inspection

You can configure the security device to perform deep inspection (Deep Inspection) on the tunnel endpoint ID (TEID) in G-PDU data messages.

Example: Enabling GTP-in-GTP Packet Filtering

In this example, you enable the security device to perform DI of G-PDU data messages on the TEID. You can configure DI only from the CLI.

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set teid-di
(gtp:gprs1)-> exit
save
```

GTP Information Elements

Information Elements (IEs) are included in all GTP control message packets. IEs provide information about GTP tunnels, such as creation, modification, deletion, and status. ScreenOS supports IEs consistent with 3GPP Release 6. If you are running an earlier release, or have contractual agreements with operators running earlier releases of 3GPP, you can reduce network overhead by restricting control messages containing unsupported IEs.

This section describes IEs contained in control messages you can configure the security device to screen based on IEs. It includes the following sections:

- Access Point Name Filtering
- IMSI Prefix Filtering
- Radio Access Technology
- Routing Area Identity and User Location Information
- APN Restriction
- IMEI-SV
- Protocol and Signaling Requirements
- Supported R6 Information Elements
- 3GPP R6 IE Removal

Access Point Name Filtering

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

- **Network ID**—Identifies the name of an external network such as "mobiphone.com"

- **Operator ID**—which uniquely identifies the operators' PLMN such as "mnc123.mcc456"

By default, the security 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 2,000 APNs.

To enable APN filtering, you must specify one or more APNs. To specify an APN, you need to know the domain name of the network (for example, mobiphone.com) and, optionally, 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 wildcard 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 Home Location Register (HLR) has verified the user subscription. You set the selection mode according to the security needs of your network. Possible selection modes include the following:

- **Mobile Station—**Mobile station-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 security device inspects GTP packets to ----look for APNs that match APNs that you set. If the APN of a GTP packet matches an APN that you specified, the security 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 security device automatically denies all other APNs that do not match.

Additionally, a security device can filter GTP packets based on the combination of an International Mobile Subscriber Identity (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 use the wildcard "*". You also set **Network** as the selection mode.

WebUI

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

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs
Selection Mode: Network (select)

CLI

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

IMSI Prefix Filtering

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

By setting IMSI prefixes, you can configure the security device to deny GTP traffic coming from nonroaming partners. By default, a security device does not perform IMSI prefix filtering on GTP packets. By setting IMSI prefixes, you configure the security device to filter **create pdp request** messages and only permit GTP packets with IMSI prefixes that match the ones you set. The security device allows GTP packets with IMSI prefixes that do not match any of the IMSI prefixes that you set. To block GTP packets with IMSI prefixes that do not match any of the IMSI prefixes set, use an explicit wildcard for the IMSI filter, and the action: **drop** should be the last IMSI prefix filtering policy. You can set up to 1,000 IMSI prefixes.

When you filter GTP packets based on an IMSI prefix, yo must also specify an APN. See "Example: Setting a Combined IMSI Prefix and APN Filter."

Example: Setting a Combined IMSI Prefix and APN Filter

In this example, you set **mobiphone.com.mnc123.mcc456.gprs** as an APN and use the wildcard "*". You permit all selection modes for this APN. You also set the IMSI prefix for a known PLMN, which is 246565. The MCC-MNC pair can be five or six digits.

WebUI

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

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs
Mobile Country-Network Code: 246565
Selection Mode: Mobile Station, Network, Verified (select)

CLI

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

NOTE: Selecting the variable **pass** in the CLI is equal to selecting all three selection modes in the WebUI. Using this variable permits traffic from all selection modes for the specified APN.

Radio Access Technology

The Radio Access Technology (RAT) information element provides ways to stimulate Wideband Code Division Multiple Access (WCDMA), and to perform reporting via billing information systems.

Previously, the SGSN IP address was used to distinguish between 3rd Generation Wireless Mobile Communication Technology (3G) systems and 2nd Generation Wireless Mobile Communication Technology (2G) systems. With the introduction of combined 2G/3G SGSNs, however, you must configure the RAT Information Element to enable the security device to make this distinction. When you set a RAT IE, you must also specify an APN. See "Example: Setting an RAT and APN Filter."

Example: Setting an RAT and APN Filter

In this example, you set **mobiphone.com.mnc123.mcc456.gprs** as an APN and use the wildcard "*". You permit all selection modes for this APN. You configure the security device to drop the GTP message if the value of the RAT IE matches the string value 123

WebUI

Currently you can set an RAT and APN combination only from the Command Line Interface (CLI).

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set rat 123 apn *mobiphone.com drop
(gtp:gprs1)-> exit
save
```

Routing Area Identity and User Location Information

Some countries restrict subscriber access to certain types of network content. To comply with these regulatory demands, network operators need to be able to police subscriber's requested content before allowing a content download. ScreenOS gives network operators the ability to screen content based on the Routing Area Identity (RAI) and User Location Information (ULI) IEs. Because the current 3GPP Call Detail Record (CDR) formats and realtime charging interfaces lack these attributes, billing and charging systems are required to look up SGSN IP addresses to determine roaming partners for settlement and end-user charging. ScreenOS gives network operators the ability to screen control messages based on RAI and ULI. When you set a RAI or ULI IE, you must also specify an APN. See "Example: Setting an RAI and APN Filter" and "Example: Setting a ULI and APN Filter." and

Example: Setting an RAI and APN Filter

In this example, you set **mobiphone.com** as an APN and use the wildcard "*". You permit all selection modes for this APN. And you configure the security device to drop GTP messages if the RAI IE matches the string value: 12345*.

WebUI

Currently you can set an RAI and APN combination only from the Command Line Interface (CLI).

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set rai 12345* *mobiphone.com drop
(gtp:gprs1)-> exit
save
```

Example: Setting a ULI and APN Filter

In this example, you set **mobiphone.com** as an APN and use the wildcard "*". You permit all selection modes for this APN. And you configure the security device to drop GTP messages if the ULI IE matches the string value 123456.

WebUI

Currently you can set a ULI and APN combination only from the Command Line Interface (CLI).

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set uli 123456 apn mobiphone.com drop
(gtp:gprs1)-> exit
save
```

APN Restriction

Multiple concurrent primary Packet Data Protocol (PDP) contexts, and an MS/UE capable of routing between these two access points, can put IP security at risk for corporate users who have both private and a public APN.s The APN Restriction IE, added to the GTP **create PDP context** response message, ensures the mutual exclusivity of a PDP context if requested by a GGSN (or rejected if this condition cannot be met), and thus avoids the security threat.

IMEI-SV

The International Mobile Equipment Identity-Software Version (IMEI-SV) IE provides ways to adapt content to the terminal type and client application whenever a proxy server for this purpose is not present. This IE is also useful in reports generated from the GGSN, AAA and/or Wireless Application Protocol Gateway (WAP GW). The GTP-aware security device supports the RAT, RAI, ULI, APN Restriction and IMEI-SV in GTP attributes to avoid treatment or categorization as unambiguous traffic, which can be harmful to GPRS traffic or GPRS roaming traffic. These attributes are included in the set of useful filter attributes used to block specific GPRS traffic and or GPRS roaming traffic. When you set an IMEI-SV IE, you must also specify an APN. See "Example: Setting an IMEI-SV and APN Filter."

Example: Setting an IMEI-SV and APN Filter

In this example, you set **mobiphone.com** as an APN and use the wildcard "*". You permit all selection modes for this APN. And you configure the security device to pass the GTP message if the IMEI-SV IE matches the string: 87652.

WebUI

Currently you can set an RAI and APN combination only from the Command Line Interface (CLI).

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set imei-sv 87652* apn mobiphone.com pass
(gtp:gprs1)-> exit
save
```

Protocol and Signaling Requirements

The security device supports the following attributes in the GTP **Create PDP Context Request** message:

- RAT
- RAI
- ULI
- APN Restriction
- IMEI-SV

The security device supports the following attributes in the GTP **Update PDP Context Request** message:

- RAT
- RAI
- ULI

The security device supports the APN Restriction attribute in the GTP **Update PDP Context Response** message.

You can configure the above GTP signaling messages on the security device as follows:

- Transparently pass
- Block based on (individually)
  - RAT
  - RAI (with ranges such as 123*)
  - ULI (with ranges)
  - IMEI-SV (with ranges)

Combined Support

For concurrent support of IMSI and APN filtering, as well as the IEs defined above, the following precedence order is required:

1. Individual R6 filtering in decreasing order of priority (RAT, RAI, ULI, IMEI-SV) is applied first. The algorithm used is as follows:
   a. In case of a match, the appropriate policy is applied.
   b. If there is no match, the next lower priority order filter is applied, and so on.
2. IMSI range and APN or APN wildcard filtering is applied next.

Supported R6 Information Elements

ScreenOS supports all 3GPP R6 IEs for GTP, as listed in Table 2.

Table 2: Supported Information Elements

IE Type Value	Information Element
1	Cause
2	International Mobile Subscriber Identity (IMSI)
3	Routing Area Identity (REI)
4	Temporary Logical Link Identity (TLLI)
5	Packet TMSI (P-TMSI)
8	Reordering Required
9	Authentication Triplet
11	MAP Cause
12	P-TMSI Signature
13	MS Validated
14	Recovery

IE Type Value	Information Element
15	Selection Mode
16	Tunnel Endpoint Identifier Data I
17	Tunnel Endpoint Identifier Control Plane
18	Tunnel Endpoint Identifier Data II
19	Teardown ID
20	NSAPI
21	RANAP Cause
22	RAB Context
23	Radio Priority SMS
24	Radio Priority
25	Packet Flow ID
26	Charging Characteristics
27	Trace Reference
28	Trace Type
29	MS Not Reachable Reason
127	Charging ID
128	End User Address
129	MM Context
130	PDP Context
131	Access Point Name
132	Protocol Configuration Options
133	GSN Address
134	MS International PSTN/ISDN Number (MSISDN)
135	Quality of Service Profile
136	Authentication Quintuplet
137	Traffic Flow Template
138	Target Identification
139	UTRAN Transparent Container
140	RAB Setup Information
141	Extension Header Type List
142	Trigger Id
143	OMC Identity
144	RAN Transparent Container
145	PDP Context Prioritization
146	Additional RAB Setup Information
147	SGSN Number
148	Common Flags
149	APN Restriction
150	Radio Priority LCS

IE Type Value	Information Element
151	RAT Type
152	User Location Information
153	MS Time Zone
154	IMEI-SV
155	CAMEL Charging Information Container
156	MBMS UE Context
157	Temporary Mobile Group Identity (TMGI)
158	RIM Routing Address
159	MBMS Protocol Configuration Options
160	MBMS Service Area
161	Source TNC PDCP context Information
162	Additional Trace Information
163	Hop Counter
164	Selected PLMN ID
165	MBMS Session Identifier
166	MBMS2G/3G Indicator
167	Enhanced NSAPI
168	MBMS Session Duration
169	Additional MBMS Trace Information
251	Charging Gateway Address
255	Private Extension

3GPP R6 IE Removal

The 3GPP R6 IE Removal feature allows you to retain interoperability in roaming between 2GPP and 3GPP networks. You can configure the GTP-aware security device, residing on the border of a PLMN and a GRX and acting as a Gp firewall, to remove 3GPP-specific attributes from the GTP packet header when the packet passes into a 2GPP network. You can configure the security device to remove the RAT, RAI, ULI, IMEI-SV, and APN Restriction IEs from GTP messages prior to forwarding these messages to the GGSN.

Example: R6 Removal

In this example, you configure the Gp interface of the security device to remove newly added R6 IEs (RAT, ULI, IMEI-SV and APN Restriction) from the GTP message.

WebUI

Objects > GTP > New: Select the following, then click **Apply**:

Remove R6 EI: (Select)

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set  remove-r6
(gtp:gprs1)-> exit
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: one for GTP-U (user data) messages and one for GTP-C (signaling and control) messages.

GTP Tunnel Limiting

You can configure the security 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, then click **Apply**:

```
Maximum Number of Tunnels
    Limited to tunnels: (select), 800
```

CLI

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

Stateful Inspection

Following a series of GTP packet verifications (see "GTP Message Filtering" on page 8), the security device then verifies the GTP packet against the current GTP tunnel state. The security 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 security device receives a "create pdp context response" message when it did not previously receive a "create pdp context request" message, the security device drops the response message.

Basically, if it receives a GTP packet that does not belong in the current GTP state model, the security 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 is able to successfully accept the connection (authentication if any, resource allocation, Quality of Service (QoS) guarantees), 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 security 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 security 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 security 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 security device.

Tunnel Failover for High Availability

ScreenOS supports two HA (high availability) modes: active-active when the security device is in Route mode and active-passive when the security device is in either Route or Transparent mode. In essence, two security 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 security 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 security device to remove hanging GTP tunnels. For more information, see "Hanging GTP Tunnel Cleanup" on page 25.

For more information about HA and to learn how to configure security devices for high availability, see *Volume 11: High Availability*.

Hanging GTP Tunnel Cleanup

This feature removes hanging GTP tunnels on the security 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 security device to detect and remove hanging GTP tunnels automatically.

When you set a GTP tunnel timeout value, the security 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, then click **Apply**:

Tunnel Inactivity Timeout: 12

CLI

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

SGSN and GGSN Redirection

Juniper Networks security 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 security devices to prevent GPRS Overbilling attacks. The following section describes the Overbilling attack and then explains the solution.

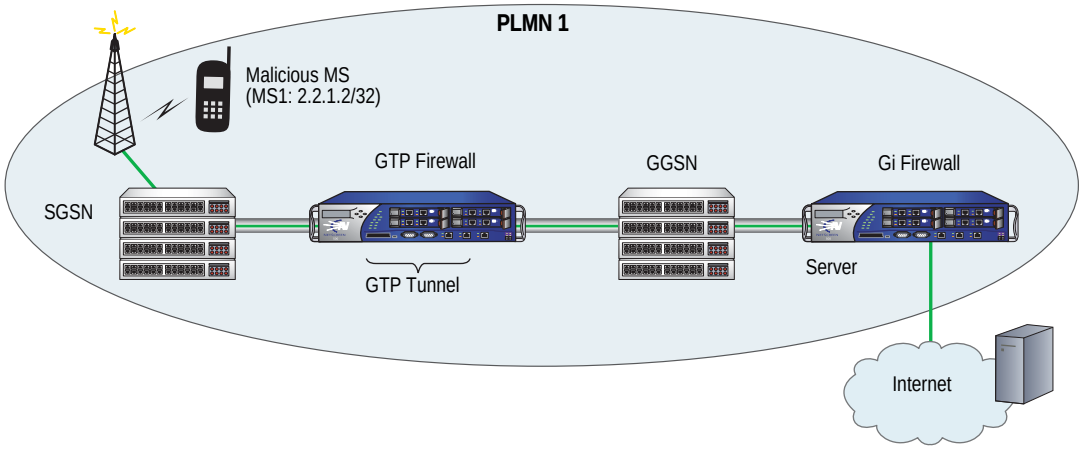
Overbilling-Attack Description

In order to understand an Overbilling attack, it is important to know that a mobile station (MS) gets its 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, causing the new MS to be billed for unsolicited traffic. Figure 3, Figure 4, and Figure 5 illustrate this scenario in detail.

In Figure 3, the 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.

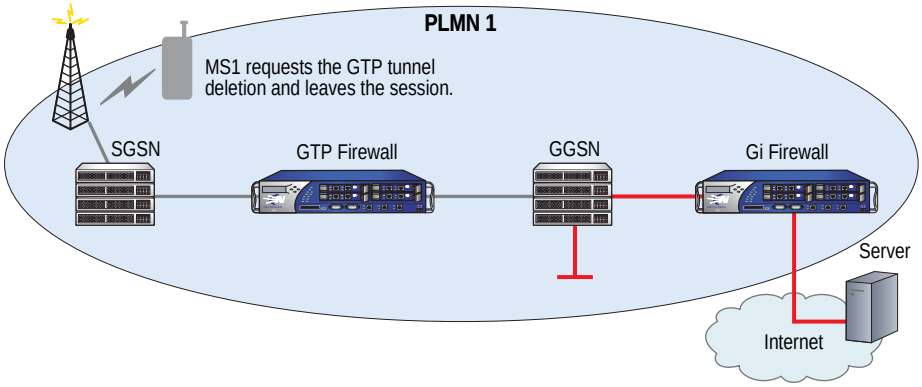
Figure 3: Starting a Session



In Figure 4, 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.

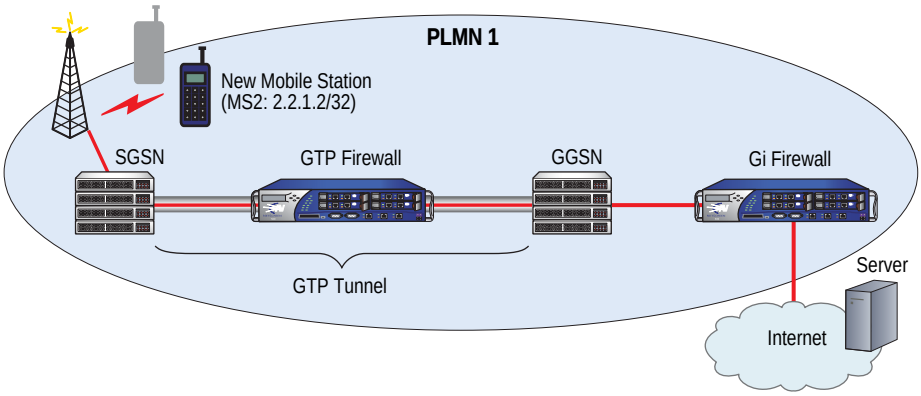
Figure 4: Deleting a GTP Tunnel



In Figure 5, 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.

Figure 5: Receiving Unsolicited Data



Overbilling-Attack Solution

To protect subscribers of a PLMN from Overbilling attacks requires two security devices and involves NetScreen Gatekeeper Protocol (NSGP) 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 devices. 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 security 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 ScreenOS 5.0.0 or ScreenOS 5.1.0 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.

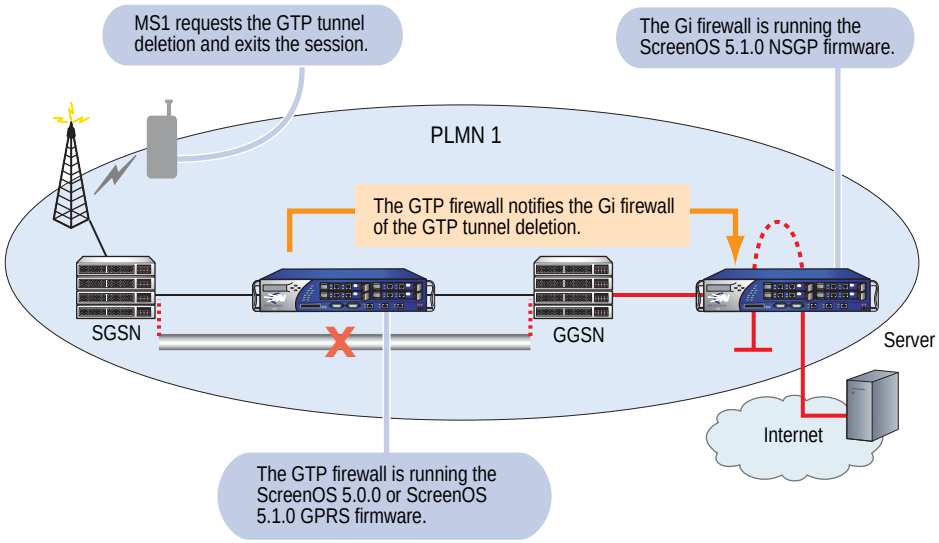
After initiating a session with the server and as the server begins to send packets to MS1, MS1 sends a request to the SGSN to delete the GTP tunnel and exits the session.

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.

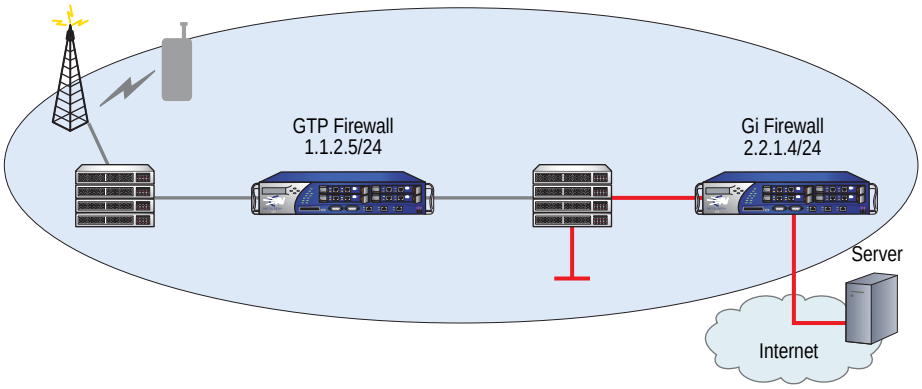
Figure 6: GTP Tunnel Deletion Notification



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.

Figure 7: GTP and Gi Firewall Setup



GTP Firewall (Client)

WebUI

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

Overbilling Notify: (select)
Destination IP: 2.2.1.4
Source Interface: ethernet1/2
Destination Context: 2

Policies > (From: Untrust, To: Trust) New: Enter the following, 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

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

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

```
set policy id 2 gtp gprs1
save
```

Gi Firewall (Server)

WebUI

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

Context ID: 2
Zone: Untrust

CLI

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

GTP Traffic Monitoring

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

NOTE: By default, traffic logging is disabled on a Juniper Networks security device.

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

- Timestamp
- Source IP address
- Destination IP address
- Tunnel Identifier (TID) or Tunnel Endpoint Identifier (TEID)
- Message type

- Packet status: forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited
- Interface, vsys, or vrouter name (if applicable)
- Public Land Mobile Network (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 about monitoring features, see "Monitoring Security Devices" on page **3-**53.

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 security device logs these messages. For example, if you set the frequency value to 10, the security 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 security 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 security 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, 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

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

Traffic Counting

With the GTP traffic counting feature, you can configure the security 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 security device counts traffic for each GTP tunnel separately and differentiates GTP-User and GTP-Control messages. When a tunnel is deleted, the security 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 Juniper Networks security devices.

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, then click **Apply**:

Traffic Counters: Count by Message (select)

CLI

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

Lawful Interception

You can configure a security 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 security device can actively trace concurrently. The default number of simultaneous active traces is three. 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 security device does not log any of the content from a GTP-U packet.

The security 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 security 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, then click **Apply**:

Maximum Simultaneous Active Trace: 2
Trace Message: 1064
Subscribers identified by: Select **IMSI**, enter 12**3456789012345**, then click **Add**.

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set trace imsi 123456789012345
(gtp:gprs1)-> set trace max-active 2 save-length 1064
(gtp:gprs1)-> exit
save
```

Index

T

V

W