JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Securing GTP and SCTP Traffic User Guide for Security Devices

Published
2023-12-14

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Securing GTP and SCTP Traffic User Guide for Security Devices

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to configure General Packet Radio Switching (GPRS) Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP) in Junos OS on the SRX Series Firewalls to secure GTP and SCTP traffic flow to external networks. The GTP firewall features such as policy-based GTP, GTP inspection, and GTP handover techniques address key security issues in mobile operators networks.

1
CHAPTER

General Packet Radio Service (GPRS) Overview

Introduction to GPRS

IN THIS SECTION

GPRS Overview

IN THIS SECTION

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 the GPRS tunneling protocol (GTP). GTP is the protocol used between GPRS support nodes (GSNs). GTP is used to establish a GTP tunnel for individual user endpoints (UEs) and between a Service Gateway (S-GW) and a PDN Gateway (P-GW) in 4G. A GTP tunnel is a channel between GSNs through which two hosts exchange data. The SGSN (S-GW) receives packets from the user endpoints 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.

Communication between different GPRS networks is not secure because GTP does not provide any authentication, data integrity, or confidentiality protection. Implementing IP 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. The GTP firewall features in Junos OS address key security issues in mobile operators' networks.

Juniper Networks security devices mitigate a wide variety of attacks on the following types of GPRS interfaces:

- Gn—The Gn interface is the connection between an SGSN (S-GW) and a GGSN within the same public land mobile network (PLMN).

  S5 - The S5 interface is the connection between a S-GW and P-GW within the PLMN in 4G networks.

- Gp—The Gp interface is the connection between two PLMNs.

  S8 -The S8 interface is the bearer plane connection between home and visited PLMNs in 4G networks.

- Gi—The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN.

  SGi - The SGi interface is the connection between a P-GW and the Internet or destination networks connected to a PLMN in 4G networks.

The term *interface* has different meanings in Junos OS and in GPRS technology. In Junos OS, an interface is a doorway to a security zone that 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 (S-GW) and a GGSN (P-GW).

Starting in Junos OS Release 18.4R1, GPRS tunneling protocol (GTP) traffic security inspection is supported on IPv6 addresses along with existing IPv4 support. With this enhancement, a GTP tunnel using either IPv4 and IPv6 addresses is established for individual user endpoints (UEs) between a Serving GPRS Support Node (SGSN) in 3G or a Service Gateway (S-GW) and a Gateway GPRS Support Node (GGSN) in 3G or a PDN Gateway (P-GW) in 4G. With IPv6 support, GTP Application Layer Gateway (ALG) inspects or ignores IPv6 GTP sessions according to the policy configurations. All ALG functions on IPv4 are supported on IPv6. You can Inspect GTP signaling or data messages transmitted over IPv6 based on the policy configurations.

This topic contains the following sections:

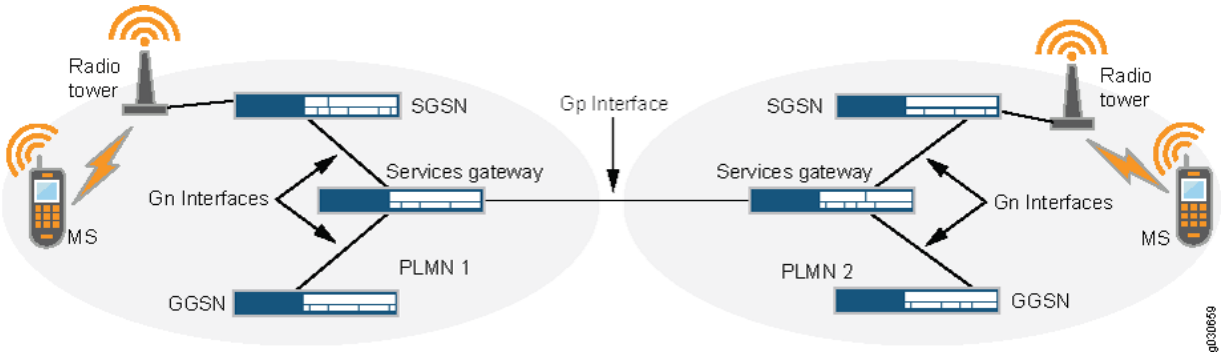
Gp and Gn Interfaces

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

When you implement a security device to the Gp interface, you protect a PLMN from another PLMN. To secure GTP tunnels on the Gp interface, you place the SGSNs (S-GW) and GGSNs(P-GW) of a PLMN behind the security device so that all traffic, incoming and outgoing, goes through the firewall.

Figure 1 on page 4 illustrates the placement of Juniper Networks SRX Series Firewalls used to protect PLMNs on the Gp and Gn interfaces.

Figure 1: Gp and Gn Interfaces



Gi Interface

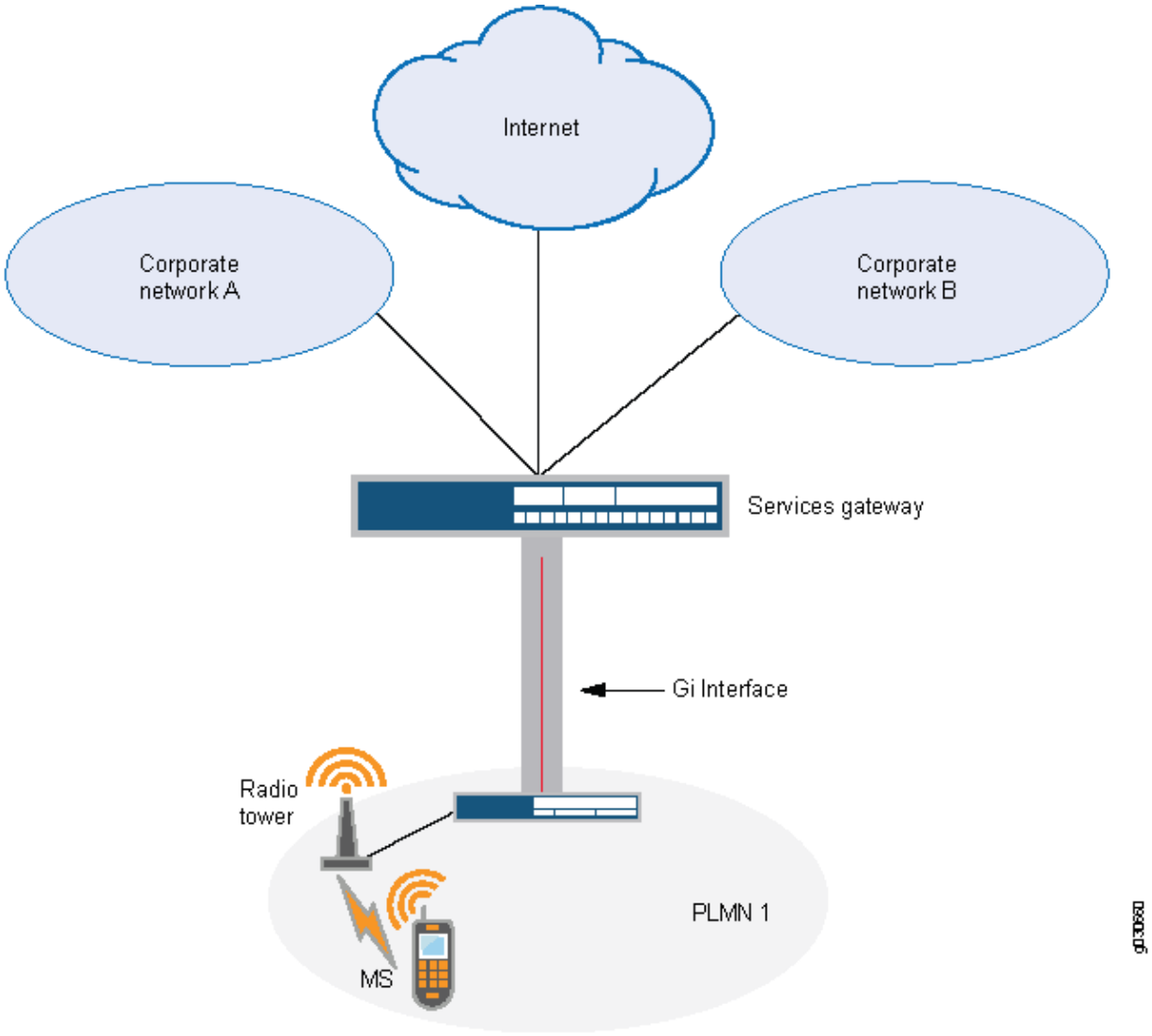
When you implement a security device on the Gi interface, you can simultaneously control traffic for multiple networks, protect a PLMN against the Internet and external networks, and protect mobile users from the Internet and other networks. Junos OS provides a great number of virtual routers, making 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.

SRX Series Firewalls do not support full L2TP.

Figure 2 on page 5 illustrates the implementation of a security device to protect a PLMN on the Gi interface.

Figure 2: Gi Interface



Operational Modes

Junos OS 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.

Junos OS supports NAT on interfaces and policies that do not have GTP inspection enabled.

Currently in Junos OS, route mode supports active/passive, and active/active *chassis cluster*. Transparent mode supports active/passive only.

GTP In-Service Software Upgrade

GTP supports unified in-service software upgrade (ISSU) between two SRX Series Firewalls running two different Junos OS releases. Unified ISSU is performed on a chassis cluster, enabling a software upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

On SRX5400, SRX5600, and SRX5800 devices, ISSU is supported from Junos OS Release 12.1X45 through Junos OS Release 12.1X46 and from Junos OS Release 12.1X46 through Junos OS Release 12.3X48-D10. ISSU is not supported from Junos OS Release 12.1X45 through Junos OS Release 12.3X48-D10.

Understanding GTP Support for Central Point Architecture

IN THIS SECTION

User equipment (for example, a cellphone) attaches to a Serving GPRS Support Node (SGSN) or S-GW (Serving Gateway) for General Packet Radio Service (GPRS) data service. The SGSN (S-GW) connects to a gateway GPRS support node to access the Internet. The user equipment requests the SGSN to create one or multiple GPRS tunneling protocol (GTP) tunnels to the GGSN or P-GW (PDN Gateway) for Internet access. In situations where the user equipment moves to a new location, the user equipment has to attach to another SGSN. The new SGSN notifies the GGSN to update the new SGSN information in the original tunnel.

The GTP Application Layer Gateway (ALG) maintains the status of the tunnels and permits tunnel update request packets only for the existing tunnels. When the user equipment moves to a new location and attaches to another SGSN, the new SGSN information must be updated in the original tunnel. Because few GTP-C messages are bidirectional, and messages can be sent either sent by the SGSN or the GGSN, correct session distribution is not guaranteed. That is, the GTP ALG stops creating a session

if the first packet originates from an unknown direction. In this case, the first packet and the other pending packets are dropped.

To prevent GTP-C packets from being dropped, a new flow session is created and the GTP-C traffic is allowed to pass even if the GGSN or SGSN direction is not determined. Later, the GGSN IP is determined using the correct SPU to create the flow session; otherwise, the session is migrated to the designated SPU.

Starting from Junos OS Release 18.4R1, the GTP-C tunnel is enhanced to support the tunnel-based session distribution to speed up the tunnel set up process and load balance the sessions between the SPUs. The tunnel-based session guarantees that the GTP-C tunnel messages reach the control tunnel and finish the stateful inspection. If the GTP-C distribution is enabled, the GTP-C tunnels and the GTP-C tunnel sessions are distributed by the SGSN tunnel endpoint identifier (TEID) of the tunnel. Use the `set security forwarding-process application-services enable-gtpu-distribution` command to enable the tunnel-based session distribution where the GTP-C traffic of different tunnels are spread across different SPUs. This command is mandatory. If it's missing from the configuration, the GTP ALG will stop working and will not inspect GTP packets.

Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, the central point architecture is enhanced. Enhancements are as follows:

- Prevent GTP-C packet drop issues during the SGSN handover.
- Support the GTP-C message rate-limiting to protect the GGSN from flooding of GTP-C messages.
- Distribute GTP-C and GTP-U traffic handled by a GGSN and SGSN pair on all SPUs by switching to tunnel-based session distribution in which the GTP-C and GTP-U traffic of different tunnels is spread across different SPUs. Use the `enable-gtpu-distribution` command to enable GTP-C or GTP-U session distribution.

GTP Tunnel Management

GTP is used to establish a GTP tunnel for individual user endpoints (UEs) and 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 user endpoints (UEs) 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.

Tunnel Object: The Client endpoints contain information for downstream GSN (SGSN), the Server endpoints hold information for upstream GSN (GGSN). Each tunnel endpoint reserves the fields one for IPv4 address and one for IPv6 address. The tunnel endpoint saves the addresses learned in the tunnel creation or update messages.

Redirect Entry: Redirect entries (also called redirect tunnels) are installed to help finding the anchor SPU. Redirect endpoints are created by means of the creation of normal GTP tunnels. A redirect entry is mapped to one tunnel endpoint and it copies IP address(es), TEID value, and the anchor SPU ID from the tunnel. With IPv6 tunnel support, redirect entry is expanded like tunnel object.

GSN

The gateway GPRS support node (GGSN) or P-GW (PDN Gateway) converts the incoming data traffic coming from the mobile users through the Service gateway GPRS support node (SGSN) and forwards it to the relevant network, and vice versa. The GGSN and the SGSN together form the GPRS support nodes (GSN).

GSN Object: The GTP ALG maintains a GSN table. Each GSN node in a GSN table will record one GSN IP address, (IPv4 or IPv6), GSN restart counter, and GSN-based rate-limiting counter, and so on. If a GSN node has both IPv4 and IPv6 address, The GTP ALG will generate two GSN entries, one for IPv4 address and the other for IPv6 address and the two GSN entries in the same GSN node counts the rate-limit signaling messages independently, and ages out separately.

GSN Reboot: If a GSN reboots, the restart counter changes and the related tunnels will get deleted. For example, if a GSN node is enabled with two IP addresses on tunnels. then the GSN restart is found by only one IP address (IPv4 or IPv6). The tunnels with both IP addresses are removed, and vice versa.

Path Object Management

A path object contains two GSN address and it supports both IPv4 and IPv6 addresses. A path object records the information between the GSN addresses such as message counter, the last time, and so on. For a GSN that has both IPv4 and IPv6 address, the two addresses have their separated paths. Each path performs its own rate-limitation, and ages out separately.

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1, GPRS tunneling protocol (GTP) traffic security inspection is supported on IPv6 addresses along with existing IPv4 support. With this enhancement, a GTP tunnel using either IPv4 and IPv6 addresses is established for individual user endpoints (UEs) between a Serving GPRS Support Node (SGSN) in 3G or a Service Gateway (S-GW) and a Gateway GPRS Support Node (GGSN) in 3G or a PDN Gateway (P-GW) in 4G. With IPv6 support, GTP Application Layer Gateway (ALG) inspects or ignores IPv6 GTP sessions according to the policy configurations. All ALG functions on IPv4 are supported on IPv6. You can Inspect GTP signaling or data messages transmitted over IPv6 based on the policy configurations.
15.1X49-D40	Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, the central point architecture is enhanced.

RELATED DOCUMENTATION

- Chassis Cluster Overview
- Day One: SRX Series Up and Running with Advanced Security Services

CHAPTER 2

Securing GTP Traffic

Policy-Based GTP

IN THIS SECTION

The GPRS tunneling protocol (GTP) policies contain rules that permit, deny, or tunnel traffic. The 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.

Understanding Policy-Based GTP

By default, the public land mobile network (PLMN) that the Juniper Networks device protects is in the Trust zone. The 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. The device performs GPRS tunneling protocol (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 device to permit, deny, or tunnel GTP traffic. However, this does not enable the device to inspect GTP traffic. For the device to inspect GTP traffic, you must apply a GTP configuration, also referred to as a *GTP inspection object*, to a policy.

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 a Serving GPRS Support Node (SGSN).

Starting in Junos OS Release 19.4R1, to accommodate IoT (Internet of Things) and roaming firewall use cases, the GTP tunnel scale per SPU is increased for the following SRX5000 (SRX5400, SRX5600, SRX5800), and SRX4600 devices:

Table 1:

Platform	SRX5000 SPC2	SRX5000 SPC3	SRX4600
Pre 19.4 Tunnel Scale per SPU	600K	1.2M	400K
Pre 19.4 Tunnel Scale per SPC	600K * 4	1.2M * 2	400k
19.4 onwards Tunnel Scale per SPU	3M	12M	4M
19.4 onwards Tunnel Scale per SPC	3M * 4	12M * 2	4M

Starting in Junos OS Release 20.1R1, to enable IoT (Internet of Things) and roaming firewall use cases, the GTP tunnel scale is increased for the following SRX Series Firewalls:

Table 2:

Platform	SRX1500	SRX4100	SRX4200
Pre 20.1 Tunnel Scale per system	204800	409600	819200
20.1 onwards Tunnel Scale per system	1024000	4096000	4096000

For vSRX Virtual Firewall instances, the number of tunnels supported depends on the available system memory.

Table 3:

Platform	Memory	Tunnel Number
vSRX Virtual Firewall	4G/6G	40K
	8G/10G/12G/14G	200K
	16G/20G/24G/28G	400K
	32G/40G/48G	800K
	56G/64G	1600K (1.6M)

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 traffic logging.

Example: Enabling GTP Inspection in Policies

IN THIS SECTION

This example shows how to enable GTP inspection in policies.

Requirements

Before you begin, the device must be restarted after GTP is enabled. By default, GTP is disabled on the device.

Overview

In this example, you configure interfaces as ge-0/0/1 and ge-0/0/2, the addresses are 2.0.0.254/8 and 3.0.0.254/8. You then configure the security zone and specify address as 2.0.0.5/32 and 3.0.0.6/32. You enable the GTP service in the security policies to allow bidirectional traffic between two networks within the same PLMN.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp profile gtp1
set interfaces ge-0/0/1 unit 0 family inet address 2.0.0.254/8
set interfaces ge-0/0/2 unit 0 family inet address 3.0.0.254/8
set security zones security-zone sgsn interfaces ge-0/0/1.0 host-inbound-traffic system-services
all
set security zones security-zone sgsn host-inbound-traffic protocols all
set security zones security-zone ggsn interfaces ge-0/0/2.0 host-inbound-traffic system-services
all
set security zones security-zone ggsn host-inbound-traffic protocols all
set security address-book global address local-sgsn 2.0.0.5/32
set security address-book global address remote-ggsn 3.0.0.6/32
set security policies from-zone sgsn to-zone ggsn policy sgsn_to_ggsn match source-address local-
sgsn destination-address remote-ggsn application junos-gprs-gtp
set security policies from-zone sgsn to-zone ggsn policy sgsn_to_ggsn then permit application-
services gprs-gtp-profile gtp1
set security policies from-zone ggsn to-zone sgsn policy ggsn_to_sgsn match source-address
remote-ggsn destination-address local-sgsn application junos-gprs-gtp
```

```
set security policies from-zone ggsn to-zone sgsn policy ggsn_to_sgsn then permit application-
services gprs-gtp-profile gtp1
```

Step-by-Step Procedure

To configure GTP inspection in policies:

1. Create the GTP inspection object.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Configure interfaces.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 2.0.0.254/8
user@host# set ge-0/0/2 unit 0 family inet address 3.0.0.254/8
```

3. Configure security zones.

```
[edit security zones]
user@host# set security-zone sgsn interfaces ge-0/0/1.0
user@host# set security-zone sgsn host-inbound-traffic system-services all
user@host# set security-zone sgsn host-inbound-traffic protocols all
user@host# set security-zone ggsn interfaces ge-0/0/2.0
user@host# set security-zone ggsn host-inbound-traffic system-services all
user@host# set security-zone ggsn host-inbound-traffic protocols all
```

4. Specify addresses.

```
[edit security address-book global]
user@host# set address local-sgsn 2.0.0.5/32
user@host# set address remote-ggsn 3.0.0.6/32
```

5. Enable the GTP service in the security policies.

```
[edit security policies]
user@host# set from-zone sgsn to-zone ggsn policy sgsn_to_ggsn match source-address local-
```

```
sgsn destination-address remote-ggsn application junos-gprs-gtp
user@host# set from-zone sgsn to-zone ggsn policy sgsn_to_ggsn then permit application-
services gprs-gtp-profile gtp1
user@host# set from-zone ggsn to-zone sgsn policy ggsn_to_sgsn match source-address remote-
ggsn destination-address local-sgsn application junos-gprs-gtp
user@host# set from-zone ggsn to-zone sgsn policy ggsn_to_sgsn then permit application-
services gprs-gtp-profile gtp1
```

Results

From configuration mode, confirm your configuration by entering the `show security` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this `show` output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]

user@host# show security
...
gprs {
gtp {
profile gtp1;
  }
}
zones {
security-zone Trust {
host-inbound-traffic {
system-services {
all;
}
protocols {
all;
  }
}
interfaces {
ge-0/0/1.0;
  }
}
...
```

```
host-inbound-traffic {
system-services {
all;
}
protocols {
all;
  }
}
interfaces {
ge-0/0/1.0;
  }
}
host-inbound-traffic {
system-services {
all;
}
protocols {
all;
  }
}
interfaces {
ge-0/0/2.0;
   }
}
}
address-book {
global {
address local-sgsn 2.0.0.5/32;
address remote-ggsn 3.0.0.6/32;
   }
}
policies {
from-zone sgsn to-zone ggsn {
policy sgsn_to_ggsn {
match {
source-address local-sgsn;
destination-address remote-ggsn;
application junos-gprs-gtp;
}
then {
permit {
application-services {
gprs-gtp-profile gtp1;
```

```
    }
    }
   }
   }
}
from-zone ggsn to-zone sgsn {
policy ggsn_to_sgsn {
match {
source-address remote-ggsn;
destination-address local-sgsn;
application junos-gprs-gtp;
}
}
then {
permit {
application-services {
gprs-gtp-profile gtp1;
     }
     }
  }
  }
default-policy {
permit-all;
}
}
...
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying GTP Inspection in Policies | 19

Confirm that the configuration is working properly.

Verifying GTP Inspection in Policies

Purpose

Verify that GTP inspection is enabled.

Action

From operational mode, enter the `show security` command.

Understanding GTP Inspection Objects

For the 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. Use the following command to create a GTP inspection object named `la-ny`: `set security gprs gtp profile la-ny`. GTP inspection objects provide more flexibility in that they allow you to configure multiple policies that enforce different GTP configurations. You can configure the 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 `commit` command.

Example: Creating a GTP Inspection Object

IN THIS SECTION

This example shows how to create a GTP inspection object.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you create a GTP inspection object named LA-NY. You preserve most of the default values, and enable the sequence number validation feature.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure a GTP inspection object:

1. Create a GTP inspection object.

```
[edit]
user@host# set security gprs gtp profile la-ny
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying GTP Inspection Object

Purpose

Verify that GTP inspection object is enabled.

Action

From operational mode, enter the `show security gprs` command.

Understanding GTPv2

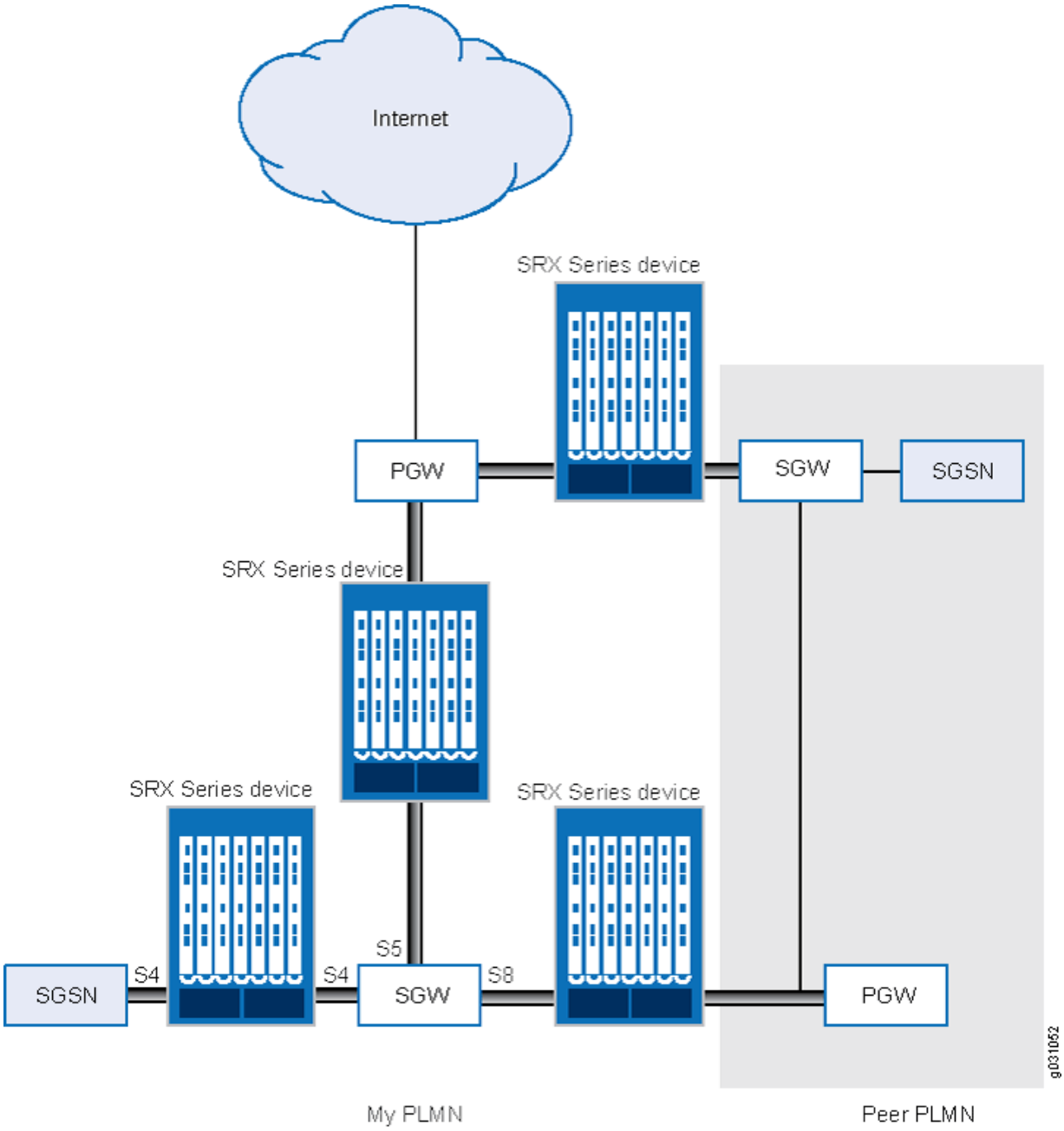
The GPRS tunneling protocol (GTP) establishes a GTP tunnel between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) for individual Mobile Stations (MS). GTP version 2 (GTPv2) is supported from Junos OS Release 11.4.

GTPv2 is part of Long Term Evolution (LTE), a fourth generation (4G) wireless broadband technology developed by Third-Generation Partnership Project (3GPP). 3GPP is the standard body for developing GPRS standards. LTE is designed to increase the capacity and speed of mobile telephone networks. GTPv2 is a protocol designed for LTE networks. An LTE network comprises network elements, LTE interfaces, and protocols.

GTPv0 and GTPv1 are implemented using SGSNs and GGSNs. However, in GTPv2, the traditional SGSNs and GGSNs are replaced by three logical nodes—a serving gateway (SGW), a packet data network gateway (PGW), and a mobility management entity (MME).

Figure 3 on page 22 shows the following LTE interfaces where SRX Series Firewalls are deployed in the public land mobile network (PLMN).

Figure 3: LTE Interfaces



- S5—This interface connects an SGW and a PGW. It provides user plane tunneling and tunnel management capability between the SGW and the PGW. It is also used for SGW relocation that happens because of user equipment mobility or SGW connection to a non-collocated PGW. The S5 interface is equivalent to the Gn interface in a Third Generation (3G) mobile network.
- S8—This interface connects an SGW in a visited PLMN (VPLM) and a PGW in a home PLMN (HPLMN). S8 is the inter-PLMN variant of S5. The S8 interface is equivalent to the Gp interface in a 3G mobile network.

- S4—This interface connects an S4 SGSN and an SGW. It provides related control and mobility support between GPRS core network and 3GPP Anchor function. It also provides user plane tunneling if direct tunneling is not established. The S4 interface does not have any equivalent interface in the 3G mobile network, because it provides interoperability between 3G and 4G networks.

Understanding Policy-Based GTPv2

GPRS tunneling protocol version 2 (GTPv2) implements a policy mechanism that checks every GTPv2 packet against security policies that regulate GTPv2 traffic. Based on the security policy, the packet is then forwarded, dropped, or tunneled.

A GTPv2 security policy allows you to forward, deny, or tunnel GTPv2 traffic. However, the security policy does not enable GTPv2 traffic inspection on the device. To enable traffic inspection, you must apply a GTPv2 inspection object to a security policy. A GTPv2 inspection object is a set of configuration parameters for processing GTPv2 traffic.

You can apply only one GTPv2 inspection object per security policy. However, you can apply an inspection object to multiple security policies.

By default, a GTPv2 inspection object is not applied to a security policy. You need to explicitly apply an inspection object to a security policy.

Using GTPv2 security policies, you can permit or deny GTPv2 tunnel establishment from certain peers, such as a serving gateway (SGW). You can configure GTPv2 security policies that specify multiple source and destination addresses, address groups, or an entire zone.

Example: Enabling GTPv2 Inspection in Policies

IN THIS SECTION

This example shows how to enable GTPv2 inspection in policies.

Requirements

Before you begin, the device must be restarted after GTPv2 is enabled. By default, GTPv2 is disabled on the device.

Overview

In this example, you configure interfaces as ge-0/0/1 and ge-0/0/2, and assign them the interface addresses 4.0.0.254/8 and 5.0.0.254/8, respectively. You then configure the security zones and specify the global addresses as 4.0.0.5/32 and 5.0.0.6/32, respectively. You enable GTPv2 inspection in security policies to allow bidirectional traffic between two networks within the same public land mobile network (PLMN).

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
 set security gprs gtp profile gtp2
set interfaces ge-0/0/1 unit 0 family inet address 4.0.0.254/8
set interfaces ge-0/0/2 unit 0 family inet address 5.0.0.254/8
set security zones security-zone sgw1 interfaces ge-0/0/1.0 host-inbound-traffic system-services
all
set security zones security-zone sgw1 host-inbound-traffic protocols all
set security zones security-zone pgw1 interfaces ge-0/0/2.0 host-inbound-traffic system-services
all
set security zones security-zone pgw1 host-inbound-traffic protocols all
set security address-book global address local-sgw1 4.0.0.5/32
set security address-book global address remote-pgw1 5.0.0.6/32
```

```
set security policies from-zone sgw1 to-zone pgw1 policy sgw1_to_pgw1 match source-address local-
sgw1 destination-address remote-pgw1 application junos-gprs-gtp
set security policies from-zone sgw1 to-zone pgw1 policy sgw1_to_pgw1 then permit application-
services gprs-gtp-profile gtp2
set security policies from-zone pgw1 to-zone sgw1 policy pgw1_to_sgw1 match source-address
remote-pgw1 destination-address local-sgw1 application junos-gprs-gtp
set security policies from-zone pgw1 to-zone sgw1 policy pgw1_to_sgw1 then permit application-
services gprs-gtp-profile gtp2
```

Step-by-Step Procedure

To configure GTPv2 inspection in policies:

1. Create the GTPv2 inspection object.

```
[edit]
user@host# set security gprs gtp profile gtp2
```

2. Configure the interfaces.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 4.0.0.254/8
user@host# set ge-0/0/2 unit 0 family inet address 5.0.0.254/8
```

3. Configure the security zones.

```
[edit security zones]
user@host# set security-zone sgw1 interfaces ge-0/0/1.0
user@host# set security-zone sgw1 host-inbound-traffic system-services all
user@host# set security-zone sgw1 host-inbound-traffic protocols all
user@host# set security-zone pgw1 interfaces ge-0/0/2.0
user@host# set security-zone pgw1 host-inbound-traffic system-services all
user@host# set security-zone pgw1 host-inbound-traffic protocols all
```

4. Specify the addresses.

```
[edit security address-book global]
user@host# set address local-sgw1 4.0.0.5/32
user@host# set address remote-pgw1 5.0.0.6/32
```

5. Enable GTPv2 inspection in the security policies.

```
[edit security policies]
user@host# set from-zone sgw1 to-zone pgw1 policy sgw1_to_pgw1 match source-address local-
sgw1 destination-address remote-pgw1 application junos-gprs-gtp
user@host# set from-zone sgw1 to-zone pgw1 policy sgw1_to_pgw1 then permit application-
services gprs-gtp-profile gtp2
user@host# set from-zone pgw1 to-zone sgw1 policy pgw1_to_sgw1 match source-address remote-
pgw1 destination-address local-sgw1 application junos-gprs-gtp
user@host# set from-zone pgw1 to-zone sgw1 policy pgw1_to_sgw1 then permit application-
services gprs-gtp-profile gtp2
```

Results

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone sgw1 to-zone pgw1 {
    policy sgw1_to_pgw1 {
    match {
    source-address local-sgw1;
        destination-address remote-pgw1;
        application junos-gprs-gtp;
        }
        then {
            permit {
            application-services {
            gprs-gtp-profile gtp2;
        }
        }
    }
```

```
    }
}
from-zone pgw1 to-zone sgw1 {
    policy pgw1_to_sgw1 {
    match {
    source-address remote-pgw1;
        destination-address local-sgw1;
        application junos-gprs-gtp;
    }
        then {
            permit {
            application-services {
            gprs-gtp-profile gtp2;
        }
    }
    }
    }
}
default-policy {
    permit-all;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying GTPv2 Inspection in Policies

Purpose

Verify that GTPv2 inspection is enabled.

Action

From operational mode, enter the `show security policies` command.

Understanding GTP Path Restart

Restarting a GPRS tunneling protocol (GTP) path terminates all GTP tunnels between two devices. Each GTP gateway is associated with a restart number. You can obtain a restart number from the Recovery information element (IE) of a GTP message.

You can detect a restart by comparing the locally stored restart number with the newly obtained one. The locally stored restart number is a nonzero value and does not match with the new restart number.

You can use the `set security gprs gtp profile` **`name`** `restart-path (echo | create | all)` *configuration statement* to restart a GTP path.

After you configure this command, the device detects the changed restart number obtained from the Recovery IE in the messages. You can use the `echo` option to obtain a new restart number from echo messages, the `create` option to obtain a restart number from create-session messages, or the `all` option to obtain a new restart number from all types of GTP messages.

Example: Restarting a GTPv2 Path

IN THIS SECTION

This example shows how to restart a GTPv2 path.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

For brevity, this example uses GTPv2.

In this example, you restart the GTPv2 path for the GTPv2 inspection object named gtp2. You obtain a new restart number from the Recovery information element (IE) in an echo message.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To restart the GTPv2 path:

1. Specify the GTPv2 profile.

```
[edit]
user@host# set security gprs gtp profile gtp2
```

2. Restart the path.

```
[edit]
user@host# set security gprs gtp profile gtp2 restart-path echo
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

IN THIS SECTION

To verify the configuration is working properly, enter the `show security gprs` command.

Purpose

Action

Understanding GTPv2 Tunnel Cleanup

A GPRS tunneling protocol version 2 (GTPv2) tunnel enables transmission of GTPv2 traffic between GPRS support nodes (GSNs).

While transmitting traffic, GTPv2 tunnels might hang for a number of reasons. For example, delete-pdp-request messages might get lost in the network, or a GSN might not shut down properly. In such a case, you can remove hanging GTPv2 tunnels either automatically or manually.

To remove a hanging GTPv2 tunnel automatically, you need to set a GTPv2 tunnel timeout value on the device. The device automatically identifies and removes a tunnel that is idle for the period specified by the timeout value. The default GTPv2 tunnel timeout value is 36 hours.

You can use the `set security gprs gtp profile` **`name`** `timeout` *configuration statement* to configure this value on the device. The timeout range is 1 through 1000 hours.

To remove a hanging GTPv2 tunnel manually, you need to use the `clear security gprs gtp tunnel` *operational mode command*.

Example: Setting the Timeout Value for GTPv2 Tunnels

IN THIS SECTION

This example shows how to set the timeout value for GTPv2 tunnels.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you set the tunnel timeout value to 40 hours for the GTPv2 inspection object named gtp2.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure the GTPv2 tunnel timeout value:

1. Specify the GTPv2 profile.

```
[edit]
user@host# set security gprs gtp profile gtp2
```

2. Specify the timeout value.

```
[edit]
user@host# set security gprs gtp profile gtp2 timeout 40
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying GTPv2 Tunnel Timeout Value

Purpose

Verify that GTPv2 tunnel timeout value.

Action

From operational mode, enter the `show security gprs` command.

Understanding GTPv2 Traffic Logging

You can use the console or syslog to view GPRS tunneling protocol version 2 (GTPv2) traffic logs. You can configure the device to log GTPv2 packets based on their status. GTPv2 packet status can be any of the following:

- Forwarded—GTPv2 packet was forwarded because it was valid.
- State-invalid—GTPv2 packet was dropped because it failed stateful inspection or a sanity check. In case of a sanity check failure, the packet is marked as sanity.
- Prohibited—GTPv2 packet was dropped because it failed message length, message type, or International Mobile Subscriber Identity (IMSI) prefix checks.
- Rate-limited—GTPv2 packet was dropped because it exceeded the maximum rate limit of the destination GPRS support node (GSN).

By default, GTPv2 logging is disabled on the device. You can use the `set security gprs gtp profile` **`name`** `log` *configuration statement* to enable GTPv2 logging on the device.

Example: Enabling GTPv2 Traffic Logging

IN THIS SECTION

This example shows how to enable GTPv2 traffic logging on a device.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable GTPv2 traffic logging for forwarded GTPv2 packets.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To enable GTPv2 traffic logging for forwarded GTPv2 packets:

1. Specify the GTPv2 profile.

```
[edit]
user@host# set security gprs gtp profile gtp2
```

2. Enable logging for GTPv2 forwarded packets.

```
[edit]
user@host# set security gprs gtp profile gtp2 log forwarded basic
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

RELATED DOCUMENTATION

Monitoring GTP Traffic | 96

GTPv1 Message Filtering

IN THIS SECTION

A GTP packet contains a message body and the GTP, UDP, and the IP headers. A GTP packet is passed or dropped based on the GTP message filters. The GTP messages are filtered based on the message-length and message-type.

Understanding GTP Message Filtering

IN THIS SECTION

When the device receives a GPRS tunneling protocol (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 will pass or drop the packets based on the configuration of the GTP inspection object.

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

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

Understanding GTP Message-Length Filtering

You can configure the device to drop packets that do not meet your specified minimum or maximum message lengths. In the GPRS tunneling protocol (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 65,535 bytes, respectively.

Understanding GTP Message-Type Filtering

You can configure the device to filter GPRS tunneling protocol (GTP) packets and permit or deny them based on their message type. By default, the 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.

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: Setting the GTP Message-Length Filtering

IN THIS SECTION

This example shows how to set the GTP message lengths.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you configure the minimum GTP message length to 8 octets and the maximum GTP message length to 1200 octets for the GTP inspection object.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure the GTP message lengths:

1. Specify the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Specify the minimum message length.

```
[edit]
user@host# set security gprs gtp profile gtp1 min-message-length 8
```

3. Specify the maximum message length.

```
[edit]
user@host# set security gprs gtp profile gtp1 max-message-length 1200
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Supported GTP Message Types

Table 4 on page 38 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.

Table 4: GTP Messages

Message	Message Type	Version 0	Version 1
create AA pdp context request	create-aa-pdp	b	
create AA pdp context response	create-aa-pdp	b	
create pdp context request	create-pdp	b	b
create pdp context response	create-pdp	b	b
data record request	data-record	b	b
data record response	data-record	b	b
delete AA pdp context request	delete-aa-pdp	b	
delete AA pdp context response	delete-aa-pdp	b	

Table 4: GTP Messages *(Continued)*

Message	Message Type	Version 0	Version 1
delete pdp context request	delete-pdp	b	b
delete pdp context response	delete-pdp	b	b
echo request	echo	b	b
echo response	echo	b	b
error indication	error-indication	b	b
failure report request	failure-report	b	b
failure report response	failure-report	b	b
forward relocation request	fwd-relocation	b	b
forward relocation response	fwd-relocation	b	b
forward relocation complete	fwd-relocation	b	b
forward relocation complete acknowledge	fwd-relocation	b	b
forward SRNS context	fwd-srns-context	b	b
forward SRNS context acknowledge	fwd-srns-context	b	b
identification request	identification	b	b
identification response	identification	b	b

Table 4: GTP Messages *(Continued)*

Message	Message Type	Version 0	Version 1
node alive request	node-alive	b	b
node alive response	node-alive	b	b
note MS GPRS present request	note-ms-present	b	b
note MS GPRS present response	note-ms-present	b	b
pdu notification request	pdu-notification	b	b
pdu notification response	pdu-notification	b	b
pdu notification reject request	pdu-notification	b	b
pdu notification reject response	pdu-notification	b	b
RAN info relay	ran-info	b	b
redirection request	redirection	b	b
redirection response	redirection	b	b
relocation cancel request	relocation-cancel	b	b
relocation cancel response	relocation-cancel	b	b
send route info request	send-route	b	b
send route info response	send-route	b	b

Table 4: GTP Messages *(Continued)*

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

Example: Filtering GTP Message Types

IN THIS SECTION

This example shows how to permit and deny GTP message types.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, for the gtp1 profile, you configure the device to drop the error-indication and failure-report message types for version 1.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To permit and deny GTP message types:

1. Configure the device.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Drop the error indication.

```
[edit]
user@host# set security gprs gtp profile gtp1 drop error-indication 1
```

3. Drop the failure report messages.

```
[edit]
user@host# set security gprs gtp profile gtp1 drop failure-report 1
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Understanding Rate Limiting for GTP Control Messages

You can configure the device to limit the rate of network traffic going to a GPRS support node (GSN). You can set separate thresholds, in packets per second, for GGSN tunneling protocol, 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 GPRS Roaming Exchange (GRX) as your public land mobile network (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—GPRS tunneling protocol (GTP) traffic can flood a GSN, forcing it to spend its CPU cycles processing illegitimate data. This can prevent subscribers from roaming and forwarding data to external networks, and it can prevent a General Packet Radio Service (GPRS) from attaching to the network.

This feature limits the rate of traffic sent to each GSN from the Juniper Networks device. The default rate is unlimited.

Understanding Path Rate Limiting for GTP Control Messages

You can restrict the maximum packets per second for specific control messages on a path on SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices. These GPRS tunneling protocol (GTP) messages include `create-req`, `delete-req`, and other GTP messages. However, you can restrict the maximum packets per minute for an `echo-req` GTP message.

The `path-rate-limit` function controls specific GTP messages in both the forward and reverse directions. A drop threshold and an alarm threshold can be configured for each control message in the forward and

reverse direction for one path. If the control messages on one path reach the alarm threshold, an alarm log is generated. If the number of control messages received reaches the drop threshold, a packet drop log is generated and all other control messages of this type received later are dropped.

To control message traffic in the forward and reverse directions, configure a policy on the device such that the direction that is consistent with the configured policy is defined as forward, and the opposite direction is defined as reverse. Use the `set security gprs gtp profile <profile-name> path-rate-limit` statement to restrict the maximum packets per second for specific control messages on a path.

You can configure both the `rate-limit` and the `path-rate-limit` options at the same time.

Example: Limiting the Message Rate and Path Rate for GTP Control Messages

IN THIS SECTION

This example shows how to limit the message rate and the path rate for GTP control messages. The `rate-limit` option limits the GTP messages per second and the `path-rate-limit` option controls specific GTP messages in both the forward and reverse directions.

Requirements

This example uses the following hardware and software components:

- SRX5400 device
- Junos OS Release 12.1X45-D10

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you limit the rate of incoming GTP messages to 300 packets per second and you limit the path rate for GTP control messages in both the forward and reverse directions. You configure the

device to limit the rate of network traffic going to a GPRS support node (GSN), and you restrict the maximum packets per second or per minute for specific control messages on a path. For `create-req`, `delete-req`, and `other` GTP messages you restrict the maximum packets per second. However, for an `echo-req` GTP message, you restrict the maximum packets per minute.

The `path-rate-limit` function controls specific GTP messages in both the forward and reverse directions. Configure the `alarm-threshold` parameter to configure the device to raise an alarm when the GTP control messages on a path have reached the configured limit. Configure the `drop-threshold` to drop traffic when the number of packets per second or per minute exceeds the configured limit.

Configuration

IN THIS SECTION

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp profile gtp1 rate-limit 300
set security gprs gtp profile gtp1 path-rate-limit message-type create-req alarm-threshold
forward 50 reverse 50
set security gprs gtp profile gtp1 path-rate-limit message-type delete-req alarm-threshold
forward 50 reverse 50
set security gprs gtp profile gtp1 path-rate-limit message-type echo-req alarm-threshold forward
50 reverse 50
set security gprs gtp profile gtp1 path-rate-limit message-type other alarm-threshold forward 50
reverse 50
set security gprs gtp profile gtp1 path-rate-limit message-type create-req drop-threshold
forward 80 reverse 80
set security gprs gtp profile gtp1 path-rate-limit message-type delete-req drop-threshold
forward 80 reverse 80
set security gprs gtp profile gtp1 path-rate-limit message-type echo-req drop-threshold forward
```

```
80 reverse 80
set security gprs gtp profile gtp1 path-rate-limit message-type other drop-threshold forward 80
reverse 80
```

Procedure

Step-by-Step Procedure

To configure the GTP message rate and path rate limit:

1. Specify the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Set the GTP message rate limit.

```
[edit security gprs gtp profile gtp1]
user@host# set rate-limit 300
```

3. Specify the message type to set the path rate limit for GTP control messages.

```
[edit security gprs gtp profile gtp1]
user@host# set path-rate-limit message-type
```

4. Select GTP control message types.

```
[edit security gprs gtp profile gtp1]
user@host# set path-rate-limit message-type create-req
user@host# set path-rate-limit message-type delete-req
user@host# set path-rate-limit message-type echo-req
user@host# set path-rate-limit message-type other
```

5. Set the alarm threshold for the GTP control message types.

```
[edit security gprs gtp profile gtp1 path-rate-limit]
user@host# set message-type create-req alarm threshold
```

```
user@host# set message-type delete-req alarm threshold
user@host# set message-type echo-req alarm threshold
user@host# set message-type other alarm threshold
```

6. Limit the control messages in the forward direction.

```
[edit security gprs gtp profile gtp1 path-rate-limit message-type]
user@host# set create-req alarm threshold forward 50
user@host# set delete-req alarm threshold forward 50
user@host# set echo-req alarm threshold forward 50
user@host# set other alarm threshold forward 50
```

7. Limit the control messages in the reverse direction.

```
[edit security gprs gtp profile gtp1 path-rate-limit message-type]
user@host# set create-req alarm threshold reverse 50
user@host# set delete-req alarm threshold reverse 50
user@host# set echo-req alarm threshold reverse 50
user@host# set other alarm threshold reverse 50
```

8. Set the drop threshold for the GTP control message types.

```
[edit security gprs gtp profile gtp1 path-rate-limit]
user@host# set message-type create-req drop threshold
user@host# set message-type delete-req drop threshold
user@host# set message-type echo-req drop threshold
user@host# set message-type other drop threshold
```

9. Limit the control messages in the forward direction.

```
[edit security gprs gtp profile gtp1 path-rate-limit message-type]
user@host# set create-req drop threshold forward 80
user@host# set delete-req drop threshold forward 80
user@host# set echo-req drop threshold forward 80
user@host# set other drop threshold forward 80
```

10. Limit the control messages in the reverse direction.

```
[edit security gprs gtp profile gtp1 path-rate-limit message-type]
user@host# set create-req drop threshold reverse 80
user@host# set delete-req drop threshold reverse 80
user@host# set echo-req drop threshold reverse 80
user@host# set other drop threshold reverse 80
```

Results

From configuration mode, confirm your configuration by entering the `show security gprs gtp profile` *`profile-name`* command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security gprs gtp profile p1
        rate-limit 300;
        path-rate-limit {
            message-type create-req {
                drop-threshold {
                    forward 80;
                    reverse 80;
                }
                alarm-threshold {
                    forward 50;
                    reverse 50;
                }
            }
            message-type delete-req {
                drop-threshold {
                    forward 80;
                    reverse 80;
                }
                alarm-threshold {
                    forward 50;
                    reverse 50;
                }
            }
            message-type echo-req {
                drop-threshold {
                    forward 80;
```

```
                    reverse 80;
                }
                alarm-threshold {
                    forward 50;
                    reverse 50;
                }
            }
            message-type other {
                drop-threshold {
                    forward 80;
                    reverse 80;
                }
                alarm-threshold {
                    forward 50;
                    reverse 50;
                }
            }
    }
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose

Verify that the GTP message rate and path rate limit configuration is correct.

Action

From operational mode, enter the `show security gprs gtp counters path-rate-limit` command.

```
Path-rate-limit counters:
                                  Drop                      Alarm
Create Request                     20                        50
Delete Request                     20                        50
Echo Request                       20                        50
Others                             20                        50
```

Meaning

The `show security gprs gtp counters path-rate-limit` command displays the number of packets received since the alarm threshold or the drop threshold value was reached. If you configure the `alarm-threshold` value as 50 and the `drop-threshold` value as 80 for the Create Request message, and if the device receives 100 packets in a second or minute, then the Drop number will be 20 and the Alarm number will be 50.

Example: Enabling GTP Sequence Number Validation

IN THIS SECTION

This example shows how to enable GTP sequence number validation feature.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you set the gtp profile as gtp1 and you also enable the sequence number validation feature.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To enable GTP sequence number validation feature:

1. Set the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Enable the sequence number validation.

```
[edit]
user@host# set security gprs gtp profile gtp1 seq-number-validated
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Configuring GTP Handover Group

IN THIS SECTION

A GPRS tunneling protocol (GTP) handover group is a set of SGSNs or serving gateway (SGW) with a common address-book library.

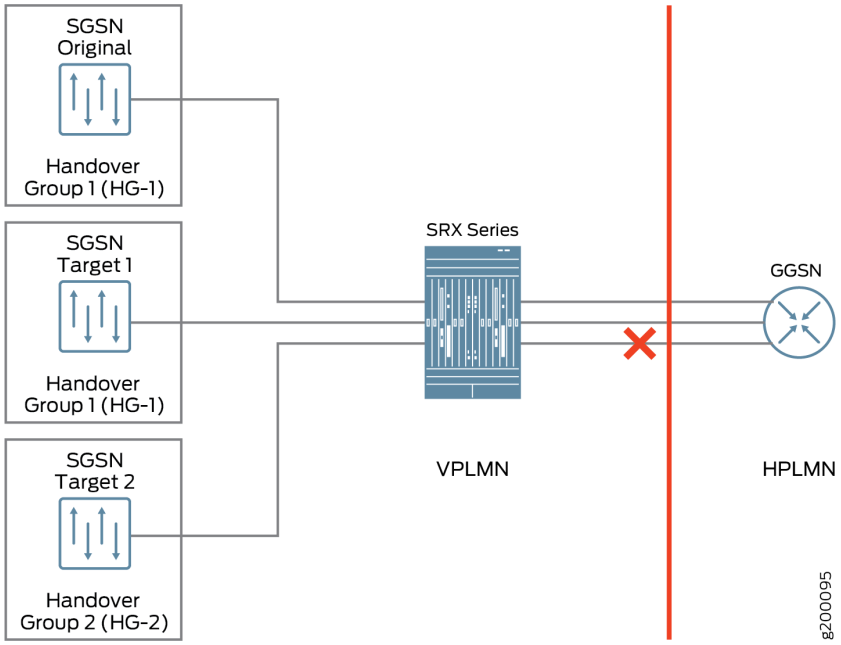
GTP Handover Group Overview

A GPRS tunneling protocol (GTP) handover group is a set of SGSNs or serving gateway (SGW) with a common address-book library. An administrator can configure a GTP profile and associate an GTP handover group to the GTP profile. When a GTP handover group name is referenced by a GTP profile, the device checks to see if the current SGSN/SGW address and the proposed SGSN/SGW address are both contained within the same GTP handover group. If both SGSN/SGW addresses are contained within the same GTP handover group, then the handover is allowed. If both the current and proposed SGSN/SGW addresses are not within the same GTP handover group, then the profile for the default handover group is used.

GTP handover across different GTP handover groups is not allowed.

You can configure the handover group using the `set security gprs gtp profile profile-name handover-group` command. If there is no handover group defined in the GTP profile, and if the traffic reaches the policy configured with this profile, handover between all GTPs matching this policy is permitted by default. Handover is denied if the configuration command is set using the `set security gprs gtp handover-default deny` command.

Figure 4: GTP Handover Group



For example, the user equipment accesses the Internet through the GTP tunnels built over the SGSN and the gateway GPRS support node (GGSN). The SGSN builds GTP tunnels to the GGSN to transfer the user equipment data, which attaches to the SGSN. In a home-routed roaming architecture, a roaming user equipment device roams back to the GGSN of a home PLMN (HPLMN) through a visited SGSN (VSGSN) of a visited PLMN (VPLMN). If the original SGSN and the SGSN target 1 as shown in Figure 4 on page 53 belong to the same handover group (HG-1), then handover occurs. If the SGSN original seeks to handover to SGSN target 2, which is in a different handover group (HG-2), then handover is denied.

Understanding GTP Handover Messages

Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, support for GTP handover messages is provided. During handover procedures, Serving GPRS Support Node (SGSN) context messages (request, response, and acknowledge) or forward relocation messages are sent between the new and the old mobility management entity (MME) and SGSN. For GPRS tunneling protocol (GTP) version 2, the messages should be context messages or forward relocation messages. For simplicity, these types of messages are uniformly referred as handover messages. The packet data protocol (PDP) context information is acquired from these messages. The PDP context is set up on the SRX Series Firewall when these messages are received, and then subsequent GTP messages can be normally inspected according to the new PDP context.

Use the `set security gprs gtp profile <profile-name> handover-on-roaming-intf` command to enable PDP context setup by handover messages. Use the `delete security gprs gtp profile <profile-name> handover-on-roaming-intf` command to disable PDP context setup by handover messages.

The addresses and tunnel endpoint identifiers (TEIDs) for forwarding data traffic are also acquired from handover messages. In addition, the forward tunnel can be set up on SRX Series Firewalls for forwarding GPRS tunneling protocol, user plane (GTP-U) stateful check.

Handover between different GTP versions is supported.

Key features of GTP handover are:

- Support for GTP inter-MME/SGSN handover messages for GTPv0, v1, and v2
- Inter-MME/SGSN handover messages inspection
- GTP PDP context and forwarding tunnel setup according to the information in handover messages
- GTP-U inspection for forwarding data traffic
- Support for PDP context update by updating and modifying messages with different versions
- System log and counter for handover messages

Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, the Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) of the GTPv1 or GTPv2 nodes cannot communicate with the GTPv0 node. If a device sends a GTPv1 or GTPv2 message to update the tunnels created by GTPv0, these messages are dropped and the GTPv0 tunnel will not be updated.

Example: Configuring Handover Groups

IN THIS SECTION

This example shows how to configure GTP handover groups on GTP profiles.

Requirements

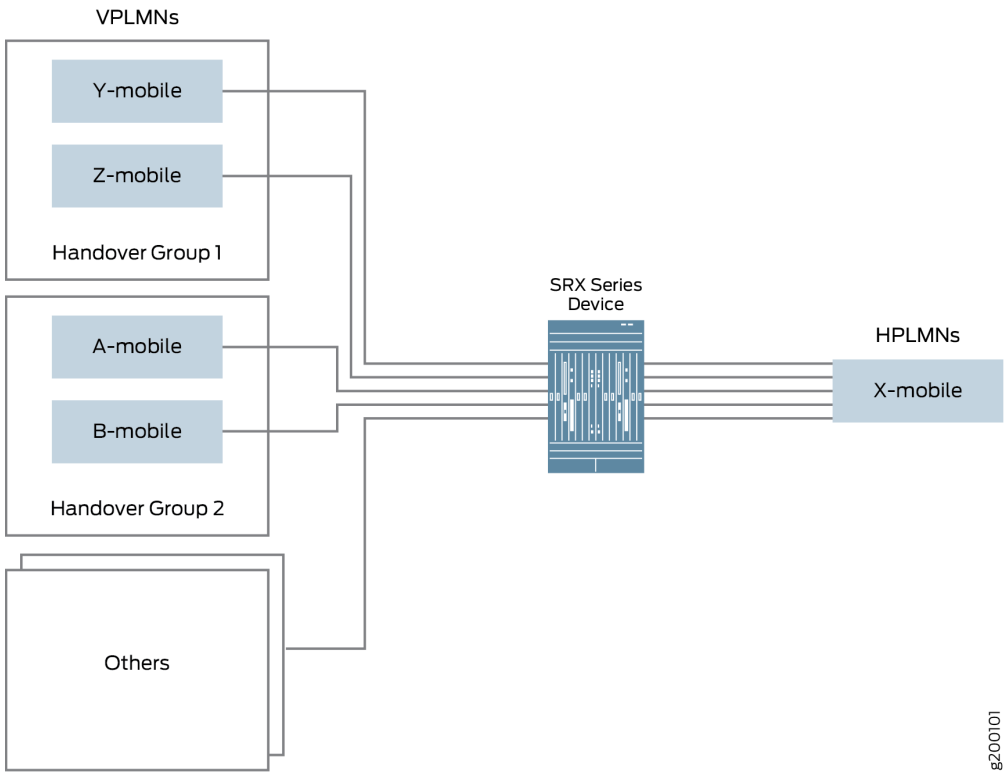
Before you begin, you need an SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, or SRX5800 device or a vSRX Virtual Firewall instance and user equipment that needs to connect to the Internet. You will also need a 3G or 4G mobile core network and a home and visited network.

Overview

A user equipment accesses the Internet through SGSN or Serving Gateway (SGW) and GGSN or packet data network gateway (PGW) in a 3G or 4G core network. The SGSN/SGW builds GTP tunnels to the GGSN/PGW to transfer the user equipment data, which attaches to the SGSN/SGW. In a home-routed roaming architecture, a roaming user equipment roams back to its GGSN of home PLMN (HPLMN) through a visited SGSN (VSGSN) of a visited PLMN (VPLMN). If the user equipment device moves out of the coverage area of the visited SGSN/SGW, it is handed over to another visited SGSN/SGW.

In this example, see Figure 5 on page 55 X-mobile is the home PLMN and the visited PLMN is the Y-mobile and the Z-mobile. You can configure GTP handover groups for the X-mobile and perform the handover within the same handover group.

Figure 5: Handover Group Configuration



Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security address-book global address X-mobile-hMME 10.10.10.1/32
set security address-book global address X-mobile-hPGW 10.10.10.2/32
set security address-book global address-set X-mobile address X-mobile-hMME
set security address-book global address-set X-mobile address X-mobile-hPGW
set security address-book global address-set X-mobile description hPLMN
set security address-book global address Y-mobile-vMME-2a 20.20.20.1/32
set security address-book global address Y-mobile-vMME-2b 20.20.20.2/32
set security address-book global address Y-mobile-vSGW-2a 20.20.20.10/32
set security address-book global address Y-mobile-vSGW-2b 20.20.20.11/32
set security address-book global address-set Y-mobile address Y-mobile-vMME-2a
set security address-book global address-set Y-mobile address Y-mobile-vMME-2b
set security address-book global address-set Y-mobile address Y-mobile-vSGW-2a
set security address-book global address-set Y-mobile address Y-mobile-vSGW-2b
set security address-book global address-set Y-mobile description vPLMN2
set security address-book global address Z-mobile-vMME-3a 30.30.30.1/32
set security address-book global address Z-mobile-vMME-3b 30.30.30.2/32
set security address-book global address Z-mobile-vSGW-3a 30.30.30.10/32
set security address-book global address Z-mobile-vSGW-3b 30.30.30.11/32
set security address-book global address-set Z-mobile address Z-mobile-vMME-3a
set security address-book global address-set Z-mobile address Z-mobile-vMME-3b
set security address-book global address-set Z-mobile address Z-mobile-vSGW-3a
set security address-book global address-set Z-mobile address Z-mobile-vSGW-3b
set security address-book global address-set Z-mobile description vPLMN3
set security address-book global address-set as-AT address-set Z-mobile
```

```
set security address-book global address-set as-AT address-set Y-mobile
set security address-book global address-set as-AT address-set X-mobile
set security gprs gtp handover-group hg-AT address-book global address-set as-AT
set security gprs gtp profile Scenario-1 handover-on-roaming-intf
set security gprs gtp profile Scenario-1 handover-group hg-AT
set security zones security-zone vplmn
set security zones security-zone hplmn
set security policies from-zone vplmn to-zone hplmn policy ply-vh1 match source-address Y-mobile
set security policies from-zone vplmn to-zone hplmn policy ply-vh2 match source-address Z-mobile
set security policies from-zone vplmn to-zone hplmn policy ply-vh match destination-address X-
mobile
set security policies from-zone vplmn to-zone hplmn policy ply-vh match application junos-gprs-
gtp
set security policies from-zone vplmn to-zone hplmn policy ply-vh then permit application-
services gprs-gtp-profile Scenario-1
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match source-address X-mobile
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match destination-address Y-
mobile
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match destination-address Z-
mobile
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match application junos-gprs-
gtp
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r then permit application-
services gprs-gtp-profile Scenario-1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration mode* in the *Junos OS CLI User Guide*.

To configure GTP handover group in a GTP profile:

1. Specify the addresses in the address book.

```
[edit]
user@host# set security address-book global address X-mobile-hMME 10.10.10.1/32
user@host# set security address-book global address X-mobile-hPGW 10.10.10.2/32
user@host# set security address-book global address-set X-mobile address X-mobile-hMME
user@host# set security address-book global address-set X-mobile address X-mobile-hPGW
user@host# set security address-book global address-set X-mobile description hPLMN
user@host# set security address-book global address Y-mobile-vMME-2a 20.20.20.1/32
```

```
user@host# set security address-book global address Y-mobile-vMME-2b 20.20.20.2/32
user@host# set security address-book global address Y-mobile-vSGW-2a 20.20.20.10/32
user@host# set security address-book global address Y-mobile-vSGW-2b 20.20.20.11/32
user@host# set security address-book global address-set Y-mobile address Y-mobile-vMME-2a
user@host# set security address-book global address-set Y-mobile address Y-mobile-vMME-2b
user@host# set security address-book global address-set Y-mobile address Y-mobile-vSGW-2a
user@host# set security address-book global address-set Y-mobile address Y-mobile-vSGW-2b
user@host# set security address-book global address-set Y-mobile description vPLMN2
user@host# set security address-book global address Z-mobile-vMME-3a 30.30.30.1/32
user@host# set security address-book global address Z-mobile-vMME-3b 30.30.30.2/32
user@host# set security address-book global address Z-mobile-vSGW-3a 30.30.30.10/32
user@host# set security address-book global address Z-mobile-vSGW-3b 30.30.30.11/32
user@host# set security address-book global address-set Z-mobile address Z-mobile-vMME-3a
user@host# set security address-book global address-set Z-mobile address Z-mobile-vMME-3b
user@host# set security address-book global address-set Z-mobile address Z-mobile-vSGW-3a
user@host# set security address-book global address-set Z-mobile address Z-mobile-vSGW-3b
user@host# set security address-book global address-set Z-mobile description vPLMN3
user@host# set security address-book global address-set as-AT address-set X-mobile
user@host# set security address-book global address-set as-AT address-set Y-mobile
user@host# set security address-book global address-set as-AT address-set Z-mobile
```

2. Specify the handover group.

```
user@host# set security gprs gtp handover-group hg-AT address-book global address-set as-AT
```

3. Configure the handover groups on the GTP profile.

```
user@host# set security gprs gtp profile Scenario-1 handover-on-roaming-intf
user@host# set security gprs gtp profile Scenario-1 handover-group hg-AT
```

4. Configure security zones for the GTP profile.

```
user@host# set security zones security-zone vplmn
user@host# set security zones security-zone hplmn
```

5. Define security policies for the GTP profile.

```
set security policies from-zone vplmn to-zone hplmn policy ply-vh1 match source-address Y-
mobile
```

```
set security policies from-zone vplmn to-zone hplmn policy ply-vh2 match source-address Z-
mobile
user@host# set security policies from-zone vplmn to-zone hplmn policy ply-vh match
destination-address X-mobile
user@host# set security policies from-zone vplmn to-zone hplmn policy ply-vh then permit
application-services gprs-gtp-profile Scenario-1
user@host# set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match source-
address X-mobile
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match destination-address
Y-mobile
set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match destination-address
Z-mobile
user@host# set security policies from-zone hplmn to-zone vplmn policy ply-vh-r match
application junos-gprs-gtp
user@host# set security policies from-zone hplmn to-zone vplmn policy ply-vh-r then permit
application-services gprs-gtp-profile Scenario-1
```

Results

From configuration mode, confirm your configuration by entering the `show security gprs gtp profile`, `show security address-book`, and `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]

user@host# show security gprs gtp
profile Scenario-1 {
    handover-on-roaming-intf;
    handover-group {
        hg-AT;
    }
}
handover-group hg-AT {
    address-book global {
        address-set {
            as-AT;
        }
```

```
    }
}
```

```
[edit]

user@host# show security address-book
global {
    address X-mobile-hMME 10.10.10.1/32;
    address X-mobile-hPGW 10.10.10.2/32;
    address Y-mobile-vMME-2a 20.20.20.1/32;
    address Y-mobile-vMME-2b 20.20.20.2/32;
    address Y-mobile-vSGW-2a 20.20.20.10/32;
    address Y-mobile-vSGW-2b 20.20.20.11/32;
    address Z-mobile-vMME-3a 30.30.30.1/32;
    address Z-mobile-vMME-3b 30.30.30.2/32;
    address Z-mobile-vSGW-3a 30.30.30.10/32;
    address Z-mobile-vSGW-3b 30.30.30.11/32;
    address-set X-mobile {
        description hPLMN;
        address X-mobile-hMME;
        address X-mobile-hPGW;
    }
    address-set Y-mobile {
        description vPLMN2;
        address Y-mobile-vMME-2a;
        address Y-mobile-vMME-2b;
        address Y-mobile-vSGW-2a;
        address Y-mobile-vSGW-2b;
    }
    address-set Z-mobile {
        description vPLMN3;
        address Z-mobile-vMME-3a;
        address Z-mobile-vMME-3b;
        address Z-mobile-vSGW-3a;
        address Z-mobile-vSGW-3b;
    }
    address-set as-AT {
        address-set Z-mobile;
        address-set Y-mobile;
        address-set X-mobile;
```

```
    }
}
```

```
[edit]

user@host# show security policies
from-zone vplmn to-zone hplmn {
    policy ply-vh {
        match {
            source-address [ Y-mobile Z-mobile ];
            destination-address X-mobile;
            application junos-gprs-gtp;
        }
        then {
            permit {
                application-services {
                    gprs-gtp-profile Scenario-1;
                }
            }
        }
    }
}
from-zone hplmn to-zone vplmn {
    policy ply-vh-r {
        match {
            source-address X-mobile;
            destination-address [ Y-mobile Z-mobile ];
            application junos-gprs-gtp;
        }
        then {
            permit {
                application-services {
                    gprs-gtp-profile Scenario-1;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

Confirm that the configuration is working properly. The `show security gprs gtp` command displays all the handover groups configured for the GTP profile Scenario-1.

Release History Table

Release	Description
15.1X49-D70	Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, the Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) of the GTPv1 or GTPv2 nodes cannot communicate with the GTPv0 node.
15.1X49-D40	Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, support for GTP handover messages is provided.

Enabling GTP Interoperability between 2G and 3G Networks

IN THIS SECTION

The GPRS Tunneling Protocol (GTP) is defined by the third-generation partnership project (3GPP) standards to carry General Packet Radio Service (GPRS) within third generation (3G) or fourth generation (4G) networks. The information elements (IEs) provide information about GPRS tunneling protocol (GTP) tunnels, such as creation, modification, deletion, and status. The IEs are included in all GTP control message packets.

Understanding GTP Information Elements

Information elements (IEs) are included in all GPRS tunneling protocol (GTP) control message packets. IEs provide information about GTP tunnels, such as creation, modification, deletion, and status. Junos OS supports IEs consistent with Third–Generation Partnership Project (3GPP) Release 6, Release 7, Release 8, and Release 9. If you have contractual agreements with operators running earlier releases of 3GPP, you can reduce network overhead by restricting control messages containing unsupported IEs.

If a new information element (IE) is introduced, there will be no drop in GTP messages because GTP passes the messages even if it encounters unknown new IEs.

Understanding R6, R7, R8, and R9 Information Elements Removal

The Third-Generation Partnership Project (3GPP) R6, R7, R8, and R9 information elements (IEs) removal feature allows you to retain interoperability in roaming between Second-Generation Partnership Project (2GPP) and 3GPP networks. You can configure the GPRS tunneling protocol (GTP)-aware Juniper Networks device, residing on the border of a public land mobile network (PLMN) and a GPRS Roaming Exchange (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 device to remove the RAT, RAI, Common Flags, ULI, MS Time Zone, IMEI-SV, and access point name (APN) restriction IEs from GTP messages prior to forwarding these messages to the gateway GPRS support node (GGSN).

Supported R6, R7, R8, and R9 Information Elements

Junos OS supports all 3GPP R6 IEs for GTP), as listed in Table 5 on page 64.

Table 5: 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
15	Selection Mode
16	Tunnel Endpoint Identifier Data I
17	Tunnel Endpoint Identifier Control Plane
18	Tunnel Endpoint Identifier Data II

Table 5: Supported Information Elements *(Continued)*

IE Type Value	Information Element
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

Table 5: Supported Information Elements *(Continued)*

IE Type Value	Information Element
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

Table 5: Supported Information Elements *(Continued)*

IE Type Value	Information Element
146	Additional RAB Setup Information
147	SGSN Number
148	Common Flags
149	APN Restriction
150	Radio Priority LCS
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

Table 5: Supported Information Elements *(Continued)*

IE Type Value	Information Element
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
173	BSS Container
174	Cell Identification
175	PDU Numbers
176	BSSGP Cause
178	RIM Routing Address Discriminator
179	List of setup PFCS

Table 5: Supported Information Elements *(Continued)*

IE Type Value	Information Element
180	PS Hand-over XID Parameters
188	Reliable INTER RAT HANDOVER INFO
251	Charging Gateway Address
255	Private Extension

Junos OS supports all 3GPP R7 IEs for GTP, as listed in Table 6 on page 69.

Table 6: Supported Information Elements

IE Type Value	Information Element
172	PS Handover Request Context
181	MS Info Change Reporting Action
182	Direct Tunnel Flags
183	Correlation-ID
184	Bearer Control Mode

Junos OS supports all 3GPP R8 IEs for GTP, as listed in Table 7 on page 69.

Table 7: Supported Information Elements

IE Type Value	Information Element
189	RFSP Index

Junos OS supports all 3GPP R9 IEs for GTP, as listed in Table 8 on page 70.

Table 8: Supported Information Elements

IE Type Value	Information Element
190	Fully Qualified Domain Name (FQDN)
191	Evolved Allocation/Retention Priority 1
192	Evolved Allocation/Retention Priority 2
193	Extended Common Flags
194	User CSG Information (UCI)
195	CSG Information Reporting Action
196	CSG ID
197	CSG Membership Indication (CMI)
198	Aggregate Maximum Bit Rate (AMBR)

Example: Removing R6, R7, R8, and R9 Information Elements from GTP Messages

IN THIS SECTION

This example shows how to remove R6 information elements from GTP messages.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

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

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To remove R6 information elements from GTP messages:

1. Specify the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Specify the information element.

```
[edit]
user@host# set security gprs gtp profile gtp1 remove-ie version v1 release R6
user@host# set security gprs gtp profile gtp1 remove-ie version v1 release R7
user@host# set security gprs gtp profile gtp1 remove-ie version v1 release R8
user@host# set security gprs gtp profile gtp1 remove-ie version v1 release R9
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Understanding GTPv1 Information Element Removal

The number of network elements in a mobile network is expanding with the introduction of multiple releases of 3GPP specifications. Every release introduces newer information elements (IEs) that are not defined in the prior releases. Therefore mobile networks have diverse set of network elements creating inter operability problems between different releases of the devices. You can configure the GPRS tunneling protocol (GTP) firewall to remove information elements (IE) by release with the following command.

`set security gprs gtp profile` *gtp1* `remove-ie`.

However newer IEs that will be introduced in the future releases might also cause inter operability problems. Each information element has a unique ID, the IE number. IE numbers range from 1 to 255. You can configure the GTP firewall to remove specific IEs using the user-configured IE number.

When you configure the IE removal, the GTP firewall deletes the corresponding IEs of the GTPv1 messages; updates the length of the GTP, the UDP, and the IP; and then passes the GTPv1 message. The GTP firewall also updates the cyclic redundancy check (CRC) code. IE removal by IE number supports all IEs, ranging from 1 to 255.

You can remove the IE removal configuration with the following commands:

`delete security gprs gtp profile` *gtp1* `remove-ie`—Deletes the IE removal configuration for the GTP profile GTP1.

`delete security gprs gtp profile` *gtp1* `remove-ie version` *v1* `number` *4*—Deletes the IE removal configuration for GTP profile with version v1 and IE number 4.

Starting from Release 20.2R1, Junos OS supports IE removal feature for both GTPv1-C and GTPv2-C.

SEE ALSO

Example: Configure IE removal for GTPV1 and GTPv2 | 85

Example: Removing GTPv1 Information Elements Using IE Number

IN THIS SECTION

This example shows how to configure the GPRS tunelling protocol (GTP) interface of the security device to remove user-configured IEs from GTP messages.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you configure IE removal for the GTP profile called gtp1. The IEs are removed using the user-configured IE number 4.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy

and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp profile gtp1
set security gprs gtp profile gtp1 remove-ie version v1 number 4
```

Step-by-Step Procedure

To configure the GTP interface of the security device to remove user-configured IEs from the GTP message:

1. Specify the GTP profile.

   [edit]

   user@host# `set security gprs gtp profile gtp1`

2. Specify the IE number.

   [edit security gprs gtp profile gtp1]

   user@host# `set remove-ie version v1 number 4`

Results

From configuration mode, confirm your configuration by entering the `show security gprs` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
gtp {
    profile gtp1 {
        remove-ie {
            version v1 {
                number 4;
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Understanding GTPv2 Information Elements

Information elements (IEs) are included in all GPRS tunneling protocol version 2 (GTPv2) control message packets. IEs provide information about GTPv2 tunnels, such as creation, modification, deletion, and status. The Junos operating system (Junos OS) supports IEs consistent with the Third-Generation Partnership Project (3GPP) Release 8.

Starting from Junos OS Release 20.2R1, a new IE enforcement function, Must-IE check is supported to check the presence of IEs that should be contained in a GTP message. Support for an existing feature IE removal is extended from GTPv1-C to both GTPv1-C and GTPv2-C.

Must-IE check—You can use this function to check the presence of IEs that should be contained in a GTP message. It is a function to verify the GTP message integrity. Must-IEs are not limited to the Mandatory IEs in 3GPP TS. You can define any IE as a Must-IE in a message in accordance with your GTPv1 or GTPv2 versions and GTPv1 or GTPv2 interfaces. The device checks the presence of Must-IEs of specific GTP messages and forwards the messages only if Must-IEs are present. We've implemented Must-IE check with flexible message profile configurations, which helps you to define must IEs of interested messages. Along with appropriate message profile configurations, Must-IE check can easily accommodate any GTP releases, message format, or IE status.

IE removal—You can use this functionality to retain interoperability between Second-Generation Partnership Project (2GPP) and Third-Generation Partnership Project (3GPP) networks. You can remove IEs of specific types from all messages for GTPv1 and GTPv2. Each information element has a unique ID, the IE number. IE numbers range from 1 to 255. You can use the IE removal to configure the GTP firewall to remove specific IEs using the user-configured IE number. It enables the communication between GTP entities whose GTP protocols are of different releases. IE removal helps to remove all instances of specified IEs such as supporting IE, Grouped IE, Embedded IE, or embedded grouped IE.

SEE ALSO

Example: Configure Must-IE check for GTPv1 and GTPv2 | **76**

Example: Configure IE removal for GTPV1 and GTPv2 | **85**

Example: Configure Must-IE check for GTPv1 and GTPv2

SUMMARY

You can enable this function to verify the presence of IEs in GTPv1 and GTPv2 message. This helps to verify message integrity. You can define any IE as a Must-IE in a message in accordance with your GTPv1 or GTPv2 versions and GTPv1 or GTPv2 interfaces. The device checks the presence of Must-IEs of specific GTP messages and forwards the messages only if Must-IEs are present.

IN THIS SECTION

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall.
- Junos OS Release 20.2R1.

Overview

Information elements (IEs) are included in all GPRS tunnelling protocol (GTP) control message packets. Every GTP-C message is constructed by a GTP header and multiple GTP Information Elements (IE). Each IE type is identified by a number between 1 – 255. Third-Generation Partnership Project (3GPP) TS defines an IE list, for every GTP message, some of them are mandatory, others are optional or conditional.

IEs of GTPv1 are encoded in TV or TLV format. Therefore, GTPv1 use IE number to identify IEs. IEs of GTPv2 are encoded in TLIV format. Therefore, GTPv2 use IE number and instance number to identify IEs.

Must-IE check is a function to check the presence of IEs that should be contained in a GTP message, which helps to verify the GTP message integrity. Must-IEs are not limited to the Mandatory IEs in 3GPP TS. You can define any IE as a Must-IE in a message in accordance with your GTPv1 or GTPv2 versions and GTPv1 or GTPv2 interfaces. The device checks the presence of Must-IEs of specific GTP messages and forwards the messages only if Must-IEs are present.

We've implemented Must-IE check with flexible message profile configurations, which helps you to define must IEs of interested messages. We call it as interested messages because IEs are not defined as mandatory in TS. Along with appropriate message profile configurations, Must-IE check can easily accommodate any GTP releases, message format, or IE status.

Configuration

IN THIS SECTION

Configure Must-IE check for GTPv1

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp message-ie-profile-v1 msgie-v1 message 2 ie 14
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 2
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 3
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 16
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 17
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 20
set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 133
set security gprs gtp profile GTP must-ie-v1 msgie-v1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. If you need help, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Configure a GTPv1 message-ie profile msgie-v1. In this example, we have created a profile named msgie-v1.

```
[edit]
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1
```

2. Create a message-ie-profile-v1 and add interested messages and IEs in message-ie-profile-v1. GTPv1 use IE number to identify IEs. In this example, in 3GPP TS 29.060, message type 2 is an Echo response and message type 16 is a Create PDP Context request. For message type 2, IE 14 is a recovery IE, which is mandatory in Echo response. For message type 16, the IEs provided are mandatory IEs in Create PDP Context request.

```
[edit]
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 2 ie 14
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 2
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 3
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 16
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 17
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 20
user@host# set security gprs gtp message-ie-profile-v1 msgie-v1 message 16 ie 133
```

3. Bind the message-ie profile to GTP profile as Must-IE. Must-IE check is implemented with message profile configurations, which helps you to define must IEs of interested messages.

```
[edit]
user@host#  set security gprs gtp profile GTP must-ie-v1 msgie-v1
```

Configure Must-IE check for GTPv2

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 73
set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 80
set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 87
set security gprs gtp grouped-ie-profile Bearer-ctxt-rmv ie 73
set security gprs gtp message-ie-profile-v2 msgie-v2 message 2 ie 3
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 1
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 71
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 82
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 87 instance 0
```

```
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 87 instance 1
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 93  instance 0 grouped-ie-profile Bearer-ctxt-crt
set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 93 instance 1 grouped-ie-profile Bearer-ctxt-rmv
set security gprs gtp profile GTP must-ie-v2 msgie-v2
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

1. Configure a GTPv2 message-ie profile msgie-v2. In this example, we have created a profile named msgie-v2.

```
[edit]
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2
```

2. Define a grouped-ie-profile and link to the IEs. A grouped IE is a group of IEs, or a group of grouped IEs. For example, Bearer Context is a grouped IE containing multiple IEs. PDN Connection is another grouped IE containing multiple instances of Bearer Context and other IEs. You must link a grouped-ie-profile only to a grouped IE, otherwise you will receive an error: “Error: IE %d is not a grouped-ie”.

```
[edit]
user@host# set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 73
user@host# set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 80
user@host# set security gprs gtp grouped-ie-profile Bearer-ctxt-crt ie 87
user@host# set security gprs gtp grouped-ie-profile Bearer-ctxt-rmv ie 73
```

3. Create a message-ie-profile-v2 and add interested messages and IEs in message-ie-profile-v2. We call the messages as interested messages because IEs are not defined as mandatory in TS. GTPv2 use IE number and instance number to identify IEs. Instance is defined in 3GPP TS 29.274 for only GTPv2. If more than one IEs of the same type are sent with a message for different purpose, these IEs will have different instance values. If you do not specify the instance value, the device will automatically take the default value as 0.

```
[edit]
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 2 ie 3
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 1
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 71
```

```
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 82
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 87 instance 0
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 87 instance 1
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 93 instance 0
grouped-ie-profile Bearer-ctxt-crt
user@host# set security gprs gtp message-ie-profile-v2 msgie-v2 message 32 ie 93 instance 1
grouped-ie-profile Bearer-ctxt-rmv
```

4. Bind the message-ie profile to GTP profile as Must-IE. Must-IE check is implemented with message profile configurations, which helps you to define must IEs of interested messages.

```
[edit]
user@host# set security gprs gtp profile GTP must-ie-v2 msgie-v2
```

Results

From configuration mode, confirm your configuration by entering the `show security gprs gtp` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security gprs gtp
profile GTP {
    must-ie-v1 {
        msgie-v1;
    }
}
message-ie-profile-v1 msgie-v1 {
    message 2 {
        ie 14;
    }
    message 16 {
        ie 2;
        ie 3;
        ie 16;
        ie 17;
        ie 20;
        ie 133;
```

```
    }
}
```

```
[edit]
user@host# show security gprs gtp
profile GTP {
    must-ie-v2 {
        msgie-v2;
    }
}
grouped-ie-profile Bearer-ctxt-crt {
    ie 73;
    ie 80;
    ie 87;
}
grouped-ie-profile Bearer-ctxt-rmv {
    ie 73;
}
message-ie-profile-v2 msgie-v2 {
    message 2 {
        ie 3;
    }
    message 32 {
        ie 1;
        ie 71;
        ie 82;
        ie 87 {
            instance 0;
            instance 1;
        }
        ie 93 {
            instance 0 {
                grouped-ie-profile {
                    Bearer-ctxt-crt;
                }
            }
            instance 1 {
                grouped-ie-profile {
                    Bearer-ctxt-rmv;
                }
            }
```

```
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verify the GTPv1 Message-IE Profile

Purpose

To verify GTPv1 Message-IE profile.

Action

From operational mode, enter the `show security gprs gtp message-ie-profile-v1 (all | <msgie-prf-v1-name>)` command.

```
user@host> show security gprs gtp message-ie-profile-v1 all
GTP Profile List (id, name):
            1 msgie-v1

user@host> show security gprs gtp message-ie-profile-v1 msgie-v1
Profile msgie-v1, uid 1

Message Number 2
IE numbers:
14

Message Number 16
```

```
IE numbers:
2, 3, 16, 17, 20, 133
```

Meaning

The output displays the details of GTPv1 Message-IE profile.

Verify the GTPv2 Message-IE Profile

Purpose

To verify the GTPv2 Message-IE profile.

Action

From operational mode, enter the `show security gprs gtp message-ie-profile-v2 (all | <msgie-prf-v2-name>)` command.

```
user@host> show security gprs gtp message-ie-profile-v2 all
GTP Profile List (id, name):
            1 msgie-v2

user@host> show security gprs gtp message-ie-profile-v2 msgie-v2

Profile msgie-v2, uid 1

Message Number   IE number/Grouped-IE   Instance numbers
2
                 3                      0

32
                 1                      0
                 71                     0
                 82                     0
                 87                     0
                 87                     1
                 Bearer-ctxt-crt        0
                 Bearer-ctxt-rmv        1
```

Meaning

The output displays the details of GTPv2 Message-IE profile.

Verify the grouped-ie profile

Purpose

To verify grouped-ie profile.

Action

From operational mode, enter the `show security gprs gtp grouped-ie-profile (all | <grpie-prf-name>)` command.

```
user@host> show security gprs gtp grouped-ie-profile all
GTP Profile List (id, name):
            1 Bearer-ctxt-crt
            2 Bearer-ctxt-rmv

user@host> show security gprs gtp grouped-ie-profile Bearer-ctxt-crt
Profile Bearer-ctxt-crt, uid 1
Grouped-IE Number   IE number/Grouped-IE   Instance numbers
93                  73                      0
                    80                      0
                    87                      0


user@host> show security gprs gtp grouped-ie-profile Bearer-ctxt-rmv
Profile Bearer-ctxt-rmv, uid 2
Grouped-IE Number   IE number/Grouped-IE   Instance numbers
93                   73                     0
```

Meaning

The output displays the details of grouped-IE profile.

SEE ALSO

Understanding GTPv2 Information Elements | 75

Example: Configure IE removal for GTPV1 and GTPv2

SUMMARY

You can enable this function to remove IEs of specific types from all messages for GTPv1 and GTPv2. This helps to retain interoperability between Second-Generation Partnership Project (2GPP) and Third-Generation Partnership Project (3GPP) networks.

IN THIS SECTION

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall.
- Junos OS Release 20.2R1.

Overview

The number of network elements in a mobile network is expanding with the introduction of multiple releases of 3GPP specifications. Every release introduces newer information elements (IEs) that are not defined in the prior releases. Therefore, mobile networks have diverse set of network elements creating interoperability problems between different releases of the devices. .

Each information element has a unique ID, the IE number. IE numbers range from 1 to 255. You can configure the GTP firewall to remove specific IEs using the user-configured IE number.

In this example, you can remove IEs of specific types from all messages for GTPv1 and GTPv2. It enables the communication between GTP entities whose GTP protocols are of different releases. This configurations helps to remove all instances of specified IEs such as supporting IE, Grouped IE, Embedded IE, or embedded grouped IE.

The IE removal support is already available for GTPv1-C. Starting in Junos OS Release 20.2R1, IE removal function is extending support for both GTPv1-C and GTPv2-C. You can use this functionality to retain interoperability between Second-Generation Partnership Project (2GPP) and Third-Generation Partnership Project (3GPP) networks.

Configuration

IN THIS SECTION

Configure IE removal for GTPv1

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp ie-set ieset-v1-r7 ie 172
set security gprs gtp ie-set ieset-v1-r7 ie 180
set security gprs gtp ie-set ieset-v1-r7 ie 181
set security gprs gtp ie-set ieset-v1-r7 ie 182
set security gprs gtp ie-set ieset-v1-r7 ie 183
set security gprs gtp ie-set ieset-v1-r7 ie 184
set security gprs gtp ie-set ieset-v1-r7 ie 199
set security gprs gtp profile GTP remove-ie-v1 ieset-v1-r7
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Configure an ieset for GTPv1. In this example, we have created an ieset named ieset-v1-r7.

```
[edit]
user@host# set security gprs gtp ie-set ieset-v1-r7
```

2. Add interested IEs in the ieset-v1-r7.

```
[edit]
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 172
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 180
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 181
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 182
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 183
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 184
user@host# set security gprs gtp ie-set ieset-v1-r7 ie 199
```

3. Bind the ieset to GTP profile as remove-ie. In this example, bind ieset-v1 as remove-ie-v1.

```
[edit]
user@host# set security gprs gtp profile GTP remove-ie-v1 ieset-v1-r7
```

Configure IE removal for GTPv2

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs gtp ie-set ieset-v2 ie 255
set security gprs gtp profile GTP remove-ie-v2 ieset-v2
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Configure an ieset for GTPv2. In this example, we have created an ieset named ieset-v2.

```
[edit]
user@host# set security gprs gtp ie-set ieset-v2
```

2. Add interested IEs in the ieset-v2.

```
[edit]
user@host# set security gprs gtp ie-set ieset-v2 ie 255
```

3. Bind the ieset to GTP profile as remove-ie. In this example, bind ieset-v2 as remove-ie-v2.

```
[edit]
user@host# set security gprs gtp profile GTP remove-ie-v2 ieset-v2
```

Results

From configuration mode, confirm your configuration by entering the `show security gprs gtp` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security gprs gtp
profile GTP {
    remove-ie-v1 {
        ieset-v1-r7;
    }
    remove-ie-v2 {
        ieset-v2;
    }
}
ie-set ieset-v1-r7 {
    ie 172;
    ie 180;
    ie 181;
    ie 182;
    ie 183;
    ie 184;
    ie 199;
}
ie-set ieset-v2 {
    ie 255;
}
```

Verification

IN THIS SECTION

Verify GTPv1 and GTPv2 IE removal Profile

Purpose

To verify GTPv1 and GTPv2 IE removal profile.

Action

From operational mode, enter the `show security gprs gtp ie-set (all | <ieset-name>)` command.

```
user@host> show security gprs gtp ie-set all
GTP Profile List (id, name):
            1 ieset-v1-r7
            2 ieset-v2

user@host> show security gprs gtp ie-set ieset-v1-r7
Profile ieset-v1-r7, uid 1
IE numbers:
172, 180, 181, 182, 183, 184, 199

user@host> show security gprs gtp ie-set ieset-v2
Profile ieset-v2, uid 2
IE numbers:
255
```

Meaning

The output displays the details of GTPv1 and GTPv2 IE removal profile.

SEE ALSO

Understanding GTPv1 Information Element Removal | 72

Understanding GTP APN Filtering

An access point name (APN) is an information element (IE) included in the header of a GPRS tunneling protocol (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 example.com.
- Operator ID—Uniquely identifies the operators' public land mobile network (PLMN) such as mnc123.mcc456.

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

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, example.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 example.com but also includes all the characters that might precede it.

You may 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 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 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.

Additionally, the device can filter GTP packets based on the combination of an International Mobile Subscriber Identity (IMSI) prefix and an APN. When you filter GTP packets based on an IMSI prefix, you must also specify an APN.

An APN string is case-insensitive. For instance, in the following example you set two APN strings, WWW.EXAMPLE.COM and www.example.com, with the same IMSI prefix value. In this configuration, the lowercase string will display after the uppercase string, and the packet will be dropped.

user@host# show configuration security gprs gtp | display set

set security gprs gtp profile test apn WWW.EXAMPLE.COM imsi-prefix * action pass

set security gprs gtp profile test apn www.example.com imsi-prefix * action drop

If an APN is configured with two IMSI prefix entries, then the IMSI prefix with the longest match takes priority. For example, see the following configuration:

user@host# show configuration security gprs gtp | display set

set security gprs gtp profile test apn WWW.EXAMPLE.COM imsi-prefix 12345678 action pass

set security gprs gtp profile test apn www.example.com imsi-prefix 12345 action drop

If an incoming packet value matches the IMSI prefix value 12345678, then the packet will pass. The IMSI prefix value 12345678 takes precedence over the IMSI prefix value 12345, as the longest matched IMSI prefix takes priority.

Example: Setting a GTP APN and a Selection Mode

IN THIS SECTION

This example shows how to set a GTP APN and a selection mode.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you set a GTP APN as example.com.mnc123.mcc456.gprs and use the wildcard (*) character. You also set the IMSI prefix and set the selection mode as network.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure a GTP APN and a selection mode:

1. Specify the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Set a selection mode for the APN.

```
[edit]
user@host# set security gprs gtp profile gtp1 apn *example.com.mnc123.mcc456.gprs imsi-prefix
* action selection net
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Understanding IMSI Prefix Filtering of GTP Packets

A GPRS support node (GSN) identifies a mobile station (MS) by its International Mobile Station Identity (IMSI). An IMSI consists of 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 device to deny GPRS tunneling protocol (GTP) traffic coming from nonroaming partners. By default, a device does not perform IMSI prefix filtering on GTP packets. By setting IMSI prefixes, you configure the device to filter create-pdp-request messages and permit only GTP packets with IMSI prefixes that match the ones you set. The 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 drop action should be the last IMSI prefix filtering policy.

When you filter GTP packets based on an IMSI prefix, you must also specify an APN.

Example: Setting a Combined IMSI Prefix and APN Filter

IN THIS SECTION

This example shows how to set and combine IMSI prefix and APN filter.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you set example.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.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To set and combine IMSI prefix and APN filter:

1. Set the GTP profile.

```
[edit]
user@host# set security gprs gtp profile gtp1
```

2. Set the selection mode for APN.

```
[edit]
user@host# set security gprs gtp profile gtp1 apn *example.com.mnc123.mcc456.gprs imsi-prefix
246565* action pass
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the `show security gprs` command.

Understanding GTPv2 IMSI Prefix and APN Filtering

A GPRS support node (GSN) identifies a Mobile Station (MS) by its International Mobile Subscriber 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 is a three-digit number, and the MNC is a two-digit or three-digit number. The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network or public land mobile network (PLMN). Therefore, the IMSI prefix acts as the PLMN identifier and is used to identify valid roaming partners.

By default, a device does not perform IMSI prefix filtering on GPRS tunneling protocol version 2 (GTPv2) packets. By setting IMSI prefixes, you configure the device to filter create-session-request messages and permit only GTPv2 packets with IMSI prefixes that match the ones you set.

When you filter GTPv2 packets based on an IMSI prefix, you must also specify an access point name (APN).

An APN is an information element (IE) included in the header of a GTPv2 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 example.com.
- Operator ID—Uniquely identifies the operators' PLMN, such as mnc123.mcc789.gprs.

For example, example.com.mnc123.mcc789.gprs is an APN for reaching the example.com network through the mnc123.mcc789.gprs operator.

By default, a device does not perform APN filtering on GTPv2 packets. However, you can configure the device to perform APN filtering to restrict access to roaming subscribers to external networks.

You can use the `set security gprs gtp profile` **`profile name`** `apn` **`pattern-string`** `imsi-prefix` **`imsi-prefix-digits`** `action (pass |drop |selection)` *configuration statement* to filter packets based on the combination of an IMSI prefix and an APN.

To specify an APN, you need to know the network ID or the domain name of the network (for example, example.com) and, optionally, the operator ID. Because the network ID portion of an APN can be very long, you can use the wildcard (*) as the first character of the APN string. For example, if you use *.example.com as the network ID, the wildcard indicates that the APN is not limited only to example.com but also includes all the characters that might precede it.

You can use the `selection` option to 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:

- ms—MS-provided APN, subscription is not verified.
- net—Network-provided APN, subscription is not verified.

- vrf—MS-provided or network-provided APN, subscription is verified.

You can use the `drop` option to drop all APNs and the `pass` option to pass all APNs for any selection mode.

When performing APN filtering, the device inspects packets to look for APNs that match APNs that you set. If the APN of a packet matches an APN that you specified, then the device verifies the selection mode and forwards the GTPv2 packet.

The device only forwards the GTPv2 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.

IMSI prefix and APN filtering apply to create-session-request messages only.

RELATED DOCUMENTATION

Policy-Based GTP | 11

Monitoring GTP Traffic

IN THIS SECTION

The GPRS Tunneling Protocol (GTP) establishes a GTP tunnel for a user equipment, between a Service gateway GPRS support node (SGSN) and gateway GPRS support node (GGSN), and an SGSN and mobility management entity (MME). The SGSN receives packets from the user equipment 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 the packets and forwards the packets to the external host.

Understanding GTP-U Inspection

The GPRS tunneling protocol user plane (GTP-U) inspection performs security checks on GTP-U packets. When GTP-U inspection is enabled, the invalid GTP-U packets are blocked and the GPRS support node (GSN) is protected from a GTP-U attack.

Once GTP-U inspection is enabled and depending on the device configuration, GTP-U inspection might include checks on GTP-in-GTP packets, end-user authorization, packet sequence validity, and tunnel validity. If any configured check fails, the GTP-U packet is dropped.

If the GTP-U inspection is enabled while the GTP-U distribution is disabled then the following message is displayed: `GTP-U inspection is enabled, please enable GTP-U distribution to ensure that GTP-U packets are inspected by the proper inspectors, and avoid dropping GTP-U packets wrongly. Execute CLI “set security forwarding-process application-services enable-gtpu-distribution" to enable GTP-U distribution.` It is strongly recommended that when you enable GTP-U inspection, GTP-U distribution should also be enabled.

Starting in Junos OS Release 15.1X49-D100 and Junos OS Release 17.3R1, on SRX5400, SRX5600, and SRX5800 devices, if the GTP profile is configured then the GTP module will select the anchor SPU for distributing the UDP traffic coming on port 2123 and 2152. If you do not configure the GTP profile, then the GTP module will not work and it will not select the anchor SPU for the UDP traffic on port 2123 and 2152.

The following list describes the various types of GTP-U inspections that are performed on the traffic:

- **GTP-U tunnel check**—The GTP-U module checks that the GTP-U packet matches a GTP tunnel. If no tunnel matches the GTP-U packet, then the GTP-U packet is dropped.
- **GTP-in-GTP check**—In the SPU, the GTP module checks to ensure that the GTP-U payload is not a GTP packet. If the payload is a GTP packet, then the GTP packet is dropped.
- **End-user address check**—If the user tunnel is found for the GTP-U packet, then the GTP-U module checks for the end-user address. If the GTP-U payload address does not match the end-user address, then the GTP-U packet is dropped.

  Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, the end-user address in certain scenarios is not carried in GTP create messages. For example, if DHCPv4 is used for IPv4 address allocation, the IPv4 address field in the GTP create message will be set to `0.0.0.0`. The user equipment and GGSN/PGW get the address from the DHCP server. In this scenario, the GTP module cannot get the address for the end-user address check. Subsequently, if this configuration is enabled, the GTP create message will be dropped.
- **Sequence number check**—The GTP-U module compares the GTP-U packet sequence number with the sequence number stored in the GTP-U tunnel. If it is not in the specified range, then the GTP-U packet is dropped. If it is in the range, then the GTP-U tunnel refreshes the sequence number and allows the GTP-U packet to pass.

At the end of the GTP-U inspection, the GTP-U tunnel refreshes the timers and counters.

Understanding GTP Tunnel Enhancements

A GPRS tunneling protocol (GTP) tunnel is a channel between two GPRS support nodes through which two hosts exchange data. The GTP tunnel consists of the GTP control plane (GTP-C) and GTP user plane (GTP-U). GTP-C is used to signaling between the gateway GPRS support node (GGSN) and the serving GPRS support node (SGSN), while the GTP-U tunnel is used to encapsulate and route the user plane traffic across multiple signaling interfaces.

GTP handling is enhanced to update the GTP tunnel and session lifetime to avoid GTP tunnel timeout issues. The GTP tunnel timeout value is configured in the GTP profile and bound to the GTP user plane (GTP-U) tunnel. The timer value is refreshed when the data traffic reaches the GTP-U tunnel and the timer value decreases when the GTP-U tunnel is in idle state. The GTP-U tunnel is deleted when the timer value decreases to zero and the corresponding GTP-C tunnel is also deleted when all GTP-U tunnels bound to the GTP-C tunnels are deleted.

When GTP-U inspection is disabled, data traffic is unable to refresh the GTP-U tunnel after the timer value expires and all GTP tunnels timeout even though data traffic flows across the tunnels. In this scenario, since the GTP tunnels need to be updated, the device drops the update request as the GTP-U tunnel is not present.

To avoid GTP tunnel timeout issues, even if the GTP user validation is disabled, the GTP-U traffic can refresh the GTP tunnel. GTP-U traffic can refresh only GTPv1 and GTPv2 tunnels, and not GTPv0 tunnels. You need to configure the `set security forwarding-process application-services enable-gtpu-distribution` command to avoid aging of or expiry of the GTP tunnels.

The GTP-U tunnel has a session attach flag that is checked when scanning the GTP-U tunnels. If the session attach flag is present in the tunnel, the timer value does not decrease and prevents the tunnel from being deleted while the tunnel is in service.

On SRX5400, SRX5600, and SRX5800 devices, the number of GTP tunnels supported per SPU is increased from 200,000 tunnels to 600,000 tunnels per SPU, for a total of 2,400,000 tunnels per SPC2 card.

Understand Validation of IP Address in GTP Messages

IN THIS SECTION

IP addresses in GPRS tunneling protocol (GTP) message on Gp or the S8 interface are validated with the configured IP group list to prevent attacks. IP group list is a list of IP addresses that belongs to all kinds of network equipment. You must configure the IP addresses that belongs to network equipment in the IP group list.

S8 - This interface connects an SGW in a visited PLMN (VPLM) and a PGW in a home PLMN (HPLMN). S8 is the inter-PLMN variant of S5. The S8 interface is equivalent to the Gp interface in a 3G mobile network.

The GTP firewall determines if the IP addresses in GTP messages and matches with the configured IP group list, and following action takes place-

- If the IP addresses are found in the IP group list, the GTP messages are considered valid and forwarded to Packet and Forwarding Engine.
- If the IP addresses are not found in the IP group list, the GTP messages are dropped.

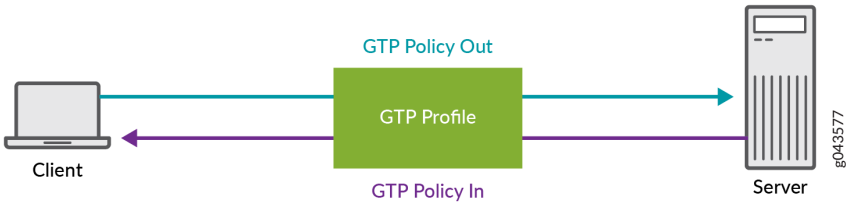
IP Group Setup in GTP Message

IP group is a list of IP addresses that belongs to all kinds of network equipment. IP group name(s) are referenced in GTP profiles. The GTP firewall applies configured policies in incoming and outgoing IP addresses in GPRS tunneling protocol (GTP) message mentioned in Table 10 on page 101 and Table 11 on page 101.

For example, the traffic between client and server in Figure 6 on page 100, there are two policies configured.

- *GTP Policy Out* is for the traffic from client to server.
- *GTP Policy In* is for the traffic from server to client.

Figure 6: GTP Profile for incoming and outgoing GTP messages



All the IP addresses of client and server must be configured in the IP group list and bound to the *GTP Policy Out* and *GTP Policy In* policies.

There are two different types of groups are introduced for different IP addresses. One is for NE IP addresses group, and the other is for User Equipment (UE) IP addresses group listed as in Table 9 on page 100.

Table 9: Network Equipment and User Equipment IP Address Support on Various Networks

Network Types	Network Equipment IP Address	User Equipment IP Address
2G(GPRS) and 3G(UMTS)	RNC, SGSN and GGSN	End User Address
4G(LTE)	eNodeB, MME, SGW and PGW	PDN Address Allocation (PAA)

When GTP messages comes to message handler stage, network equipment IP addresses group and user equipment IP addresses group are validated respectively based on the parsed information elements and IP address header information.

- Network equipment IP addresses group: IP address header and information element IP address in GTP message are compared against the configured network equipment IP addresses group list (if exist). If the NE IP address is found in the configured NE IP addresses group, pass the data packet to UE IP addresses group else drop the packet.
- User equipment IP addresses group: All end user IP addresses are validated against the configured user equipment IP addresses group list. If the user equipment IP address is found in the configured user equipment IP addresses group, pass the data packet else drop the packet.

Supported GTP messages

There are many types of messages pass through Gp or S8 interfaces, some of the supported GTP messages are following.

Table 10: GTPv0 Messages

Message Type	GTP Message	Reference in TS 29.060
1	Echo Request	7.4.1
2	Echo Response	7.4.2
16	Create PDP Context Request	7.5.1
17	Create PDP Context Response	7.5.2
18	Update PDP Context Request	7.5.3
19	Update PDP Context Response	7.5.4
20	Delete PDP Context Request	7.5.5
21	Delete PDP Context Response	7.5.6
22	Create AA PDP Context Request	7.5.7
23	Create AA PDP Context Response	7.5.8
24	Delete AA PDP Context Request	7.5.9
25	Delete AA PDP Context Response	7.5.10

Table 11: GTPv1 Messages

Message Type	GTP Message	Reference in TS 29.060
1	Echo Request	7.2.1
2	Echo Response	7.2.2

Table 11: GTPv1 Messages *(Continued)*

Message Type	GTP Message	Reference in TS 29.060
16	Create PDP Context Request	7.3.1
17	Create PDP Context Response	7.3.2
18	Update PDP Context Request	7.3.3
19	Update PDP Context Response	7.3.4
20	Delete PDP Context Request	7.3.5
21	Delete PDP Context Response	7.3.6

Table 12: GTPv2 Messages

Message Type	GTP Message	Reference 3GPP TS 29.274
1	Echo Request	23.007
2	Echo Response	23.007
32	Create Session Request	29.274
33	Create Session Response	29.274
36	Delete Session Request	29.274
37	Delete Session Response	29.274
34	Modify Bearer Request	29.274
35	Modify Bearer Response	29.274

Table 12: GTPv2 Messages *(Continued)*

Message Type	GTP Message	Reference 3GPP TS 29.274
95	Create Bearer Request	29.274
96	Create Bearer Response	29.274
97	Update Bearer Request	29.274
98	Update Bearer Response	29.274
99	Delete Bearer Request	29.274
100	Delete Bearer Response	29.274

IEs involved in IP validity

The following are the information elements (IE) messages belonging to 3GPP Gp or S8 interface.

IEs are configured on Gp or the S8 interface, if an unexpected IE appears in the message, it might be ignored and not be checked even if it is an NE IP address.

Table 13: IEs in GTPv0 messages

GTP Message	Address Type	IE Type
Create PDP Context Request Create AA PDP Context Request	End User Address SGSN Address for signalling SGSN Address for user traffic	End User Address GSN Address GSN Address
Create PDP Context Response Create AA PDP Context Response	End user address GGSN Address for signalling GGSN Address for user traffic	End User Address GSN Address GSN Address
Update PDP Context Request	SGSN Address for signalling SGSN Address for user traffic	GSN Address GSN Address

Table 13: IEs in GTPv0 messages *(Continued)*

GTP Message	Address Type	IE Type
Update PDP Context Response	GGSN Address for signalling GGSN Address for user traffic	GSN Address GSN Address

Table 14: GTPv1 messages

GTP Message	Address Type	IE Type
Create PDP Context Request	End User Address SGSN Address for signalling SGSN Address for user traffic	End User Address GSN Address GSN Address
Create PDP Context Response	End user address GGSN Address for signalling GGSN Address for user traffic Alternative GGSN Address for Control Plane Alternative GGSN Address for user traffic	End User Address GSN Address GSN Address GSN Address GSN Address
Update PDP Context Request (SGSN-initiated)	SGSN Address for signalling SGSN Address for user traffic Alternative SGSN Address for Control Plane Alternative SGSN Address for user traffic	GSN Address GSN Address GSN Address GSN Address
Update PDP Context Request (GGSN-initiated)	End User Address	End User Address
Update PDP Context Response (by GGSN)	GGSN Address for signalling GGSN Address for user traffic Alternative GGSN Address for Control Plane Alternative GGSN Address for user traffic	GSN Address GSN Address GSN Address GSN Address
Update PDP Context Response (by SGSN)	SGSN Address for User Traffic	GSN Address

Table 15: GTPv2 messages

GTP Message/Bearer Context	Address Type	IE Type
Create Session Request	Sender Address for Control Plane PDN Address Allocation H(e)NB Local IP Address MME/S4-SGSN Identifier	F-TEID PAA IP Address IP Address
Create Session Request (Bearer context to be created)	S5/S8-U SGW F-TEID	F-TEID
Create Session Response	PGW S5/S8 F-TEID for Control Plane interface PDN Address Allocation	F-TEID PAA
Create Session Response (Bearer context to be created)	S5/S8-U PGW F-TEID	F-TEID
Create Bearer Request (Bearer context)	S5/8-U PGW F-TEID	F-TEID
Create Bearer Response	MME/S4-SGSN Identifier	IP Address
Create Bearer Response (Bearer context)	S5/8-U SGW F-TEID S5/8-U PGW F-TEID	F-TEID F-TEID
Modify Bearer Request	Sender Address for Control Plane H(e)NB Local IP Address MME/S4-SGSN Identifier	F-TEID IP Address IP Address
Modify Bearer Request (Bearer context)	S5/8-U SGW F-TEID	F-TEID
Delete Session Request	Sender Address for Control Plane	F-TEID
Delete Bearer Response	MME/S4-SGSN Identifier	IP Address
Update Bearer Response	MME/S4-SGSN Identifier	IP Address

Example: Configure the Validity of IP Address in GTP Messages

IN THIS SECTION

This example shows how you configure IP address validity in GPRS tunneling protocol (GTP) message.

Requirements

SRX Series Firewall with Junos OS Release 19.3R1 or later. This configuration example is tested on Junos OS Release 19.3R1.

This example uses the following hardware and software components:

- You need any one of the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, and vSRX Virtual Firewall instance.
- User equipment that needs to connect to the Internet. You will also need a 3G or 4G mobile core network and a home and visited network.

Overview

In this example, you configure the validity of the IP address in GPRS tunneling protocol (GTP) message.

You can prevent a variety of attacks by validating the IP addresses of incoming and outgoing packets in GTP messages against the IP addresses configured in the IP group list. IP group is a list of IP addresses that belongs to all kinds of network equipment. IP group name(s) are referenced in GTP profiles. The GTP firewall applies configured policies in incoming and outgoing IP addresses in GPRS tunneling protocol (GTP) messages.

Configure IP Address in GTP Messages

IN THIS SECTION

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Procedure

CLI Quick Configuration

```
set security gprs gtp profile gtp1 timeout 1
set security gprs gtp profile gtp1 log forwarded detail
set security gprs gtp profile gtp1 log state-invalid detail
set security gprs gtp profile gtp1 log prohibited detail
set security gprs gtp profile gtp1 log gtp-u all
set security gprs gtp profile gtp1 log gtp-u dropped
set security gprs gtp profile gtp1 restart-path echo
set security gprs gtp profile gtp1 req-timeout 30
set security gprs gtp traceoptions file debug_gtp
set security gprs gtp traceoptions file size 1000m
security gprs gtp traceoptions flag all
set security gprs gtp gsn timeout 1
set security zones security-zone SGSN_1
set security zones security-zone SGSN_0
set security zones security-zone SGSN_2
set security address-book global address att-mme 192.0.2.0/24
set security address-book global address att-sgw 192.51.100.0/24
set security address-book global address china-mobile-pgw 203.0.113.0/24
set security address-book global address ue-mobile 203.0.113.1/24
set security address-book global address-set ne-group-as address china-mobile-pgw
set security address-book global address-set ne-group-as address att-mme
set security address-book global address-set ne-group-as address att-sgw
set security address-book global address-set ue-group-as address ue-mobile
```

```
set security gprs gtp ip-group ng1 address-book global address-set ne-group-as
set security gprs gtp ip-group ug1 address-book global address-set ue-group-as
set security gprs gtp profile gtp1 ne-group ng1
set security gprs gtp profile gtp1 ue-group ug1
set security policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match source-address
any
set security policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match destination-
address any
set security policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match application any
set security policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 then permit
application-services gprs-gtp-profile gtp1
set security policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match source-address
any
set security policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match destination-
address any
set security policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match application any
set security policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN then permit
application-services gprs-gtp-profile gtp1
set security policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match source-address
any
set security policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match destination-
address any
set security policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match application any
set security policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 then permit
application-services gprs-gtp-profile gtp1
```

To configure IP address in the GTP messages:

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

Step-by-Step Procedure

1. Configure a GTP profile to process the traffic that goes to the GTP firewall.

```
[edit security gprs]
user@host# set gtp profile gtp1 timeout 1
user@host# set gtp profile gtp1 log forwarded detail
user@host# set gtp profile gtp1 log state-invalid detail
user@host# set gtp profile gtp1 log prohibited detail
user@host# set gtp profile gtp1 log gtp-u all
```

```
user@host# set gtp profile gtp1 log gtp-u dropped
user@host# set gtp profile gtp1 restart-path echo
user@host# set gtp profile gtp1 req-timeout 30
user@host# set gtp traceoptions file debug_gtp
user@host# set gtp traceoptions file size 1000m
user@host# set gtp traceoptions flag all
user@host# set gtp gsn timeout 1
```

2. Configure the security zone to support inbound and outbound traffic for all system services for all interfaces connected.

```
[edit security zones]
user@host# set security-zone SGSN_1
user@host# set security-zone SGSN_0
user@host# set security-zone SGSN_2
```

3. Specify the IP address in the global address book, these IP addresses are used for validating IP addresses in incoming or outgoing GTP messages.

```
[edit security address-book global]
user@host# set address att-mme 192.0.2.0/24
user@host# set address att-sgw 192.51.100.0/24
user@host# set address china-mobile-pgw 203.0.113.0/24
user@host# set address ue-mobile 203.0.113.1/24
user@host# set address-set ne-group-as address china-mobile-pgw
user@host# set address-set ne-group-as address att-mme
user@host# set address-set ne-group-as address att-sgw
user@host# set ddress-set ue-group-as address ue-mobile
```

4. Configure the defined network equipment and user equipment IP address group to IP group list, this IP group list is used in GTP messages.

```
[edit security gprs]
user@host# set gtp ip-group ng1 address-book global address-set ne-group-as
user@host# set gtp ip-group ug1 address-book global address-set ue-group-as
```

5. Apply GTP profile to network equipment and user equipment groups.

```
[edit security gprs]
user@host# set gtp profile gtp1 ne-group ng1
user@host# set gtp profile gtp1 ue-group ug1
```

6. Enable the GTP service in the security policies.

```
[edit security]
user@host# set policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match source-
address any
user@host# set policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match destination-
address any
user@host# set policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 match application
any
user@host# set policies from-zone SGSN_1 to-zone SGSN_0 policy HSGSN_VSGSN1 then permit
application-services gprs-gtp-profile gtp1
user@host# set policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match source-
address any
user@host# set policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match destination-
address any
user@host# set policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN match application
any
user@host# set policies from-zone SGSN_2 to-zone SGSN_0 policy VSGSN1_HSGSN then permit
application-services gprs-gtp-profile gtp1
user@host# set policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match source-
address any
user@host# set policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match destination-
address any
user@host# set policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 match application
any
user@host# set policies from-zone SGSN_2 to-zone SGSN_1 policy HSGSN_VSGSN2 then permit
application-services gprs-gtp-profile gtp1
```

Results

From configuration mode, confirm your configuration by entering the `show security gprs` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security gprs
gtp {
    profile GTP {
        timeout 1;
        log {
            forwarded detail;
            state-invalid detail;
            prohibited detail;
            gtp-u all;
            gtp-u dropped;
        }
        restart-path echo;
        req-timeout 30;
    }
    profile gtp1 {
        ne-group {
            ng1;
        }
        ue-group {
            ug1;
        }
    }
    traceoptions {
        file debug_gtp size 1000m;
        flag all;
    }
    gsn {
        timeout 1;
    }
    ip-group ng1 {
        address-book global {
            address-set {
                ne-group-as;
            }
        }
```

```
    }
    ip-group ug1 {
        address-book global {
            address-set {
                ue-group-as;
            }
        }
    }
}
```

From configuration mode, confirm your configuration by entering the `show security zones` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security zones
security-zone SGSN_1;
security-zone SGSN_0;
security-zone SGSN_2;
```

From configuration mode, confirm your configuration by entering the `show security address-book` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security address-book
global {
    address att-mme 192.0.2.0/24;
    address att-sgw 192.51.100.0/24;
    address china-mobile-pgw 192.51.100.0/24;
    address ue-mobile 203.0.113.1/24;
    address-set ne-group-as {
        address china-mobile-pgw;
        address att-mme;
        address att-sgw;
    }
    address-set ue-group-as {
        address ue-mobile;
    }
}
```

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone SGSN_1 to-zone SGSN_0 {
    policy HSGSN_VSGSN1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    gprs-gtp-profile GTP;
                }
            }
        }
    }
}
from-zone SGSN_2 to-zone SGSN_0 {
    policy VSGSN1_HSGSN {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    gprs-gtp-profile GTP;
                }
            }
        }
    }
}
from-zone SGSN_2 to-zone SGSN_1 {
    policy HSGSN_VSGSN2 {
        match {
            source-address any;
```

```
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    gprs-gtp-profile GTP;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verify the IP Group

Purpose

Verify the IP Group is configured.

Action

Use the `show security gprs gtp ip-group` command to get the details of the configured IP group.

```
All configured IP group:
    Group name              Address book name       Address set name
    ng1                     global                  ne-group-as
    ug1                     global                  ue-group-as
```

Verify the GTP profile

Purpose

Verify the GTP profile is configured.

Action

Use the `show security gprs gtp configuration 1` command to get the details of the configured IP group.

```
Profile Details:

      Index                       : 2
      Min Message Length          : 0
      Max Message Length          : 65535
      Timeout                     : 24
      Rate Limit                  : 0
      Request Timeout             : 5
      Remove R6                   : 0
      Remove R7                   : 0
      Remove R8                   : 0
      Remove R9                   : 0
      Deny Nested GTP             : 0
      Validated                   : 0
      Passive learning enable     : 0
      Restart Path                : 0
      Log Forwarded               : 0
      Log State Invalid           : 0
      Log Prohibited              : 0
      Log Ratelimited             : 0
      Frequency Number            : 0
      Drop AA Create PDU          : 0
      Drop AA Delete PDU          : 0
      Drop Bearer Resource        : 0
      Drop Change Notification    : 0
      Drop Config Transfer        : 0
      Drop Context                : 0
      Drop Create Bear            : 0
      Drop Create Data Forwarding : 0
      Drop Create PDU             : 0
      Drop Create Session         : 0
      Drop Create Forwarding Tnl  : 0
```

```
        Drop CS Paging              : 0
        Drop Data Record            : 0
        Drop Delete Bearer          : 0
        Drop Delete Command         : 0
        Drop Delete Data Forwarding : 0
        Drop Delete PDN             : 0
        Drop Delete PDP             : 0
        Drop Delete Session         : 0
        Drop Detach                 : 0
        Drop Downlink Notification  : 0
        Drop Echo                   : 0
        Drop Error Indication       : 0
        Drop Failure Report         : 0
        Drop FWD Access             : 0
        Drop FWD Relocation         : 0
        Drop FWD SRNS Context       : 0
        Drop G-PDU                  : 0
        Drop Identification         : 0
        Drop MBMS Sess Start        : 0
        Drop MBMS Sess Stop         : 0
        Drop MBMS Sess Update       : 0
        Drop Modify Bearer          : 0
        Drop Modify Command         : 0
        Drop Node Alive             : 0
        Drop Note MS Present        : 0
        Drop PDU Notification       : 0
        Drop Ran Info               : 0
        Drop Redirection            : 0
        Drop Release Access         : 0
        Drop Relocation Cancel      : 0
        Drop Resume                 : 0
        Drop Send Route             : 0
        Drop SGSN Context           : 0
        Drop Stop Paging            : 0
        Drop Supported Extension    : 0
        Drop Suspend                : 0
        Drop Trace Session          : 0
        Drop Update Bearer          : 0
        Drop Update PDN             : 0
        Drop Update PDP             : 0
        Drop Ver Not Supported      : 0
        Handover group name         : N/A
```

```
        NE group name               : ng1
        UE group name               : ug1
```

Release History Table

Release	Description
15.1X49-D40	Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, the end-user address in certain scenarios is not carried in GTP create messages.
15.1X49-D100	Starting in Junos OS Release 15.1X49-D100 and Junos OS Release 17.3R1, on SRX5400, SRX5600, and SRX5800 devices, if the GTP profile is configured then the GTP module will select the anchor SPU for distributing the UDP traffic coming on port 2123 and 2152. If you do not configure the GTP profile, then the GTP module will not work and it will not select the anchor SPU for the UDP traffic on port 2123 and 2152.

RELATED DOCUMENTATION

Policy-Based GTP | 11

GTP traffic logs

IN THIS SECTION

You can use the console or syslog to view GPRS Tunneling Protocol (GTP) version traffic logs.

Understanding GTP traffic logs

To help you troubleshoot issues, the GTP logs include messages indicating the type of problem that occurred. GTP packets are dropped because of the following reasons:

- GTP header sanity check failure

- GTP payload sanity check failure
- Disallowed by configuration
- System resource failure
- System internal failure

Table 16 on page 118 lists the reasons and explanations for GTP packet drop due to GTP header sanity check failure.

Table 16: Reasons for GTP Packet Drop Due to GTP Header Sanity Check Failure

GTP Packet Drop Reason	Explanation
Invalid GTP header	The GTP header is malformed because of the following reasons: • Invalid length • Unexpected messages For example, GTP protocol data unit (GTP-PDU) or GTP user plane (GTP-U) messages are received on the GTP control (GTP-C) port.
Inconsistent length between UDP and GTP headers	The length of the UDP payload differs from the length of the GTP message. For example, the length of the UDP payload is smaller than the minimum length of the GTP header.
Long extension header (GTPv1)	The total length of extension headers exceeds the UDP length (GTPv1 only).
Invalid GTPv0 TID	The GTPv0 tunnel identifier (TID) format is incorrect.
Invalid piggyback flag (GTPv2)	There is a piggyback flag in the piggyback packet header. The piggyback packet header should not include a piggyback flag.

Table 17 on page 119 lists the reasons and explanations for GTP packet drop due to GTP payload sanity check failure.

Table 17: Reasons for GTP Packet Drop Due to GTP Payload Sanity Check Failure

GTP Packet Drop Reason	Explanation
Invalid IMSI	The International Mobile Subscriber Identity (IMSI) format is incorrect.
Zero chargID	The information element (IE) of the charging ID carries zero value.
Req Rsp context not match	The response message matches the request, but some content information does not match the request.
Bad retransmit response	The retransmitted response has the same content as the original one. So, if the original response is invalid, the retransmit ones will be dropped without check.
Missing IE	GTP-C messages are missing mandatory IEs.
IE unexpected	Unexpected IEs are present in the GTP message. For example, the Packet Data Protocol (PDP) context IE number exceeds the maximum context number supported in the SGSN context message.
Unknown IE type	Unknown IE types are present. Valid IE values range from 1–255. Unknown IE types are either zero or not supported.
Non-ascending order IEs	IEs are incorrectly ordered in the GTPv0 and GTPv1 messages.
Bad IE length	The IE length is incorrect. For example, the IE length is zero, but the IE should have data content.
Duplicate IE	Some IEs are repeated in a message. Packets are dropped because duplicate IEs should not be repeated in a message.
Non-zero TID/TEID	The header contains a nonzero tunnel endpoint identifier (TEID) (GTPv1/GTPv2) or TID (GTPv0). The value must be zero, such as in an Echo Request.

Table 17: Reasons for GTP Packet Drop Due to GTP Payload Sanity Check Failure *(Continued)*

GTP Packet Drop Reason	Explanation
Zero TID/TEID	Zero TEID or TID is used for tunnel messages. The value must be nonzero, such as in the GTP-PDU transmitted on a tunnel (TEID).
TEIDcontrol IE is zero or incorrect	TEID IE for GTP-C tunnel is incorrect. For example, the TEID carried in the Update PDP Response message varies from the TEID of the GTP-C tunnel's uplink endpoint.
TEIDdata IE is zero	The TEID IE for the GTP-U tunnel is zero. For example, the TEID of the GTP-U tunnel carried in the Create PDP Request message is zero.
Bad control GSNaddr IE	The GPRS support node (GSN) address for the GTP-C tunnel is incorrect or an invalid IP address.
Bad user GSNaddr IE	The GSN address for the GTP-U tunnel is incorrect or an invalid IP address.
Bad EndUserAddr IE	This type of error occurs because of the following reasons: • The end-user address is invalid. • The end-user address validation is enabled, and the Create message does not include the end-user address IE.
C-tunnel not found	The GTP-C tunnel is not found when the device receives a message to modify or delete the GTP-U tunnel or to create a secondary GTP-U tunnel of the GTP-C tunnel.
U-tunnel not found	The GTP-U tunnel is not found when the device receives a message to modify or delete the GTP-U tunnel or to send the GTP-PDU through the GTP-U tunnel.
Invalid GTP control tunnel	The GTP-C tunnel is invalid when the device receives messages to modify or delete the GTP-U tunnel or to create a secondary GTP-U tunnel of the GTP-C tunnel. For example, the tunnel is deleted by CLI command or by another Delete message and becomes invalid during message processing.

Table 17: Reasons for GTP Packet Drop Due to GTP Payload Sanity Check Failure *(Continued)*

GTP Packet Drop Reason	Explanation
Invalid GTP user tunnel	The GTP-U tunnel is invalid when the device receives messages to modify or delete the GTP-U tunnel or to send the GTP-PDU through the GTP-U tunnel. For example, the tunnel is deleted by CLI command or by another Delete message and becomes invalid during message processing.
No request for match	A response message does not match a request because of the following reasons: • An unexpected response • A late response after request timeout For example, you can see a Delete PDP Response, but you did not see the matching Delete PDP Request.
EBI not found (GTPv2)	The Evolved Packet System (EPS) bearer ID (EBI) IE is not found in GTP-C messages. For example, if the EBI IE is not carried in the Delete Bearer Request message, the message is dropped.
IE context error (GTPv2)	Errors exist in the bearer context IE. For example, the IP address in the bearer context IE is an invalid IP address.
Wrong source IP	The source IP address of a GTP message is incorrect. For example, when you receive a Delete PDP Request message, you use the destination IP address to find a GTP-C tunnel. The destination IP address is the same as one endpoint of the GTP-C tunnel. If the source IP address varies from the other endpoint of the GTP-C tunnel, the message is dropped.
Wrong destination IP	The destination IP address of a GTP message is incorrect. For example, a GTPv0 tunnel is found by a GTPv0 TID. When you receive a Delete PDP Request message, if the source IP address matches one endpoint of the tunnel, but the destination IP address varies from the other endpoint of the tunnel, the message is dropped.

Table 17: Reasons for GTP Packet Drop Due to GTP Payload Sanity Check Failure *(Continued)*

GTP Packet Drop Reason	Explanation
Invalid EBI (GTPv2)	Packets are dropped because an invalid EBI value is used in the GTPv2 message. The value of EBI should be in range from 5–15.
Not supported GTPv2 interface type	Incorrect interface type in F-TEID IE. For example, in the Create Session Response message, if the Packet Data Network Gateway (PGW) F-TEID is included and the interface type is not S5/8 PGW, the message is dropped.
Bad NSAPI	The Network Service Access Point Identifier (NSAPI) is incorrect for the following reasons: • NSAPI range must be 5–15. • The GTP-U tunnel with an NSAPI cannot be created, modified, or deleted, because the tunnel does not exist or it was created, modified, or deleted by another message process of the same type.
Bad primary utnl not exist	The primary GTP-U tunnel does not exist when a secondary tunnel is created.
Too many same type IE	The number of IEs of the same type exceeds the maximum allowed. For example, the maximum IE number for bearer context is 11.
Bad V2 LBI	The GTP-C message carries invalid linked bearer ID (LBI) IE. For example, the GTP-U tunnel with the bearer ID in the LBI IE does not exist or is not a primary GTP-U tunnel.
Bad conflict with primary utnl	The newly created GTP-U tunnel conflicts with the other tunnel, and the conflicting tunnel is the primary tunnel of the newly created one.
Bad ctnl endpoint restarted	The Create PDP Context message for secondary context includes a recovery IE to change the restart counter of GSN.

Table 17: Reasons for GTP Packet Drop Due to GTP Payload Sanity Check Failure *(Continued)*

GTP Packet Drop Reason	Explanation
Bad V0 GGSN IP	The IP address of GSN address IE is different from the GGSN IP address of the tunnel in the GTPv0 Update PDP Context Response message.
Not support Bi-NAT	When static NAT is configured in both forward and reverse directions, the packet is dropped. We support static NAT in only one direction.
Illegal retransmit request	The content of a retransmit request message is different from the original request message. The error check is for security consideration to drop the malformed messages.
Over PDP connection max number	The number of PDP connection IEs exceeds the maximum tunnel number range for one user equipment (UE) device.

Table 18 on page 123 lists the reasons and explanations for GTP packet drop that occurs because an action is disallowed by configuration.

Table 18: Reasons for GTP Packet Drop Because Action Is Disallowed by Configuration

GTP Packet Drop Reason	Explanation
Too short	The length of the GTP packet payload is less than the minimum length configured. The minimum length is configured by the user.
Too long	The length of the GTP packet payload is greater than the maximum length configured. The maximum length is configured by the user.
Filtered by IMSI/APN filter	The APN/IMSI IE in the GTP-C packet matches the filter for the APN/IMSI that is configured to be denied.
Over GSN packet rate limit	The traffic sent to the GSN exceeds the GSN aggregate rate limit.

Table 18: Reasons for GTP Packet Drop Because Action Is Disallowed by Configuration *(Continued)*

GTP Packet Drop Reason	Explanation
Bad message type for GTP version	This type of error occurs because of the following reasons: • A GTP message with message type is configured as to be dropped. When you drop a message type, you drop all messages of the specified type. • An incorrect message type is used. For example, a GTP-C message carries an **error indication** message type.
Over path rate limit	The packets have reached the path rate limit (drop-threshold value).
Cross group handover deny	The handover message is dropped because the old and new nodes are in different GTP handover groups, which are configured by the user.
Default handover group deny	The handover message is dropped after you configure a default handover option as deny.
NE group check failure	The IP address of the GSN in the message is not included in the network equipment (NE) group.
UE group check failure	The IP address of the end user in the message is not included in the UE group.
Bad sequence number	In GTP-U inspection, the GTP FW compares the received GTP-U packet sequence number with the sequence number stored in the GTP-U tunnel. If they are not in the specified range, then the GTP packet is dropped.
GTP-in-GTP	In GTP-in-GTP checks, if the received GTP-U packet's payload is an IP packet with a GTP well-known port, then the GTP packet is dropped.
Bad end user address	In GTP-U inspection, if the user tunnel is found for the GTP-U packet, then the GTP FW checks for the end-user address. If the received GTP-U payload address does not match the end-user address assigned at the creation of the tunnel, then the GTP packet is dropped.

Table 19 on page 125 lists the reasons and explanations for GTP packet drop due to system resource failure.

Table 19: Reasons for GTP Packet Drop Due to System Resource Failure

GTP Packet Drop Reason	Explanation
Out of new GSN	The GSN number exceeds the maximum allowed number.
Duplicate JBUF failed	This error indicates a memory allocation failure.
New GTP JMPI cookie	This error indicates a memory allocation failure.
Bad new rt_cookie	This error indicates a memory allocation failure.
Out of new path	The number of path objects for the path rate limit exceeds the maximum number.
Bad new sync action	This error indicates a memory allocation failure.
Bad new redirect utnl	This error indicates a memory allocation failure.
Out of request	This error indicates a memory allocation failure.
Out of action	This error indicates a memory allocation failure.
New create C-tunnel	Creation of GTP-C tunnel fails because the tunnel limit is exceeded or because of a failed memory allocation.
New create U-tunnel	Creation of GTP-U tunnel fails because the tunnel limit is exceeded or because of a failed memory allocation.

Table 20 on page 126 lists the reasons and explanations for GTP packet drop due to system internal failure.

Table 20: Reasons for GTP Packet Drop Due to System Internal Failure

GTP Packet Drop Reason	Explanation
Send JMPI failed	Juniper Message Passing Interface (JMPI) request fails on the SRX5000 line of devices with SPC2/SPC3.
JMPI remote process failed	JMPI remote process fails on the SRX5000 line of devices with SPC2/SPC3.
Bad reinject	Internal failure is caused by invalid reinjection of packets on the SRX5000 line of devices with SPC2/SPC3.
Wrong SPU	Internal failure is caused by incorrect Services Processing Units (SPUs) on the on SRX5000 line of devices with SPC2/SPC3.
Unknown action type	Internal failure is caused by unexpected data in memory. For example, memory is overwritten due to software or hardware bugs.
IP group not found	Internal failure is caused by unexpected data in memory.
No action for request	Internal failure is caused by unexpected data in memory.
System under resetting	Tunnel cleanup is not yet complete when you run the `clear security gprs gtp tunnel all` command, and the packets are dropped.

SEE ALSO

Understanding GTPv2 Traffic Logging | 33

Example: Enabling GTPv2 Traffic Logging | 33

NAT for GTP

IN THIS SECTION

The Network Address Translation (NAT) protocol is used to inspect the GTP traffic between the internal GPRS network and the Internet (external network) and vice versa.

Understanding NAT for GTP

A General Packet Radio Service (GPRS) interface supports both GPRS tunneling protocol (GTP) inspection and Network Address Translation (NAT) simultaneously in the same routing instance. When GTP packets configured with static NAT are inspected in a network, only addresses within IP headers are translated. The addresses within their payloads are not translated. For each endpoint, the related GTP session must belong to the same zone and virtual router. This means the header source IP, C-tunnel IP, and U-tunnel IP in the payload are defined in the same scope for a packet.

When you enable NAT, only the outer IP packet has to be translated. The embedded IP addresses are not translated.

During a GTP packet flow, the source IP address and destination IP address cannot be translated to NAT simultaneously. When you delete or deactivate NAT rule configuration on a device, the NAT rule related GSN and GTP tunnels are deleted. If the NAT rule related GSN number and tunnel number are huge, this deleting process will take several minutes.

Example: Configuring GTP Inspection in NAT

IN THIS SECTION

This example shows how to configure a NAT rule to map a private IP (one that is inside the network and not routable) to a public IP (one that is outside of the network and is routable). It also shows how to inspect GTP traffic between an internal and external network.

Requirements

Before you begin, the device must be restarted after GTP is enabled. By default, GTP is disabled on the device.

Overview

In this example, you configure interfaces as ge-0/0/0 and ge-0/0/1, with addresses 10.0.0.254/8 and 123.0.0.254/8. You then configure the security zone and static NAT. You enable the GTP service in the security policies to allow bidirectional traffic between two networks, and you check the traffic between the internal and external network.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
 set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.254/8
set interfaces ge-0/0/1 unit 0 family inet address 123.0.0.254/8
set security zones security-zone zone1 interfaces ge-0/0/0.0 host-inbound-traffic system-
services all
set security zones security-zone zone1 host-inbound-traffic protocols all
set security zones security-zone other-zone interfaces ge-0/0/1.0 host-inbound-traffic system-
services all
set security zones security-zone other-zone host-inbound-traffic protocols all
set security address-book global address gsn1 10.0.0.1/8
set security address-book global address other-gsn 20.0.0.1/8
set security nat static rule-set rs1 from zone other-zone
set security nat static rule-set rs1 rule r1 match destination-address 123.0.0.1/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 10.0.0.1/32
set security nat proxy-arp interface ge-0/0/0.0 address 123.0.0.1/32
set security gprs gtp profile gtp1
set security gprs gtp profile gtp1 timeout 1
set security gprs gtp profile gtp1 seq-number-validated
set security policies from-zone zone1 to-zone other-zone policy out-gtp match source-address gsn1
set security policies from-zone zone1 to-zone other-zone policy out-gtp match destination-
address other-gsn
set security policies from-zone zone1 to-zone other-zone policy out-gtp match application junos-
gprs-gtp
set security policies from-zone zone1 to-zone other-zone policy out-gtp then permit application-
services gprs-gtp-profile gtp1
set security policies from-zone other-zone to-zone zone1 policy in-gtp match source-address
other-gsn
set security policies from-zone other-zone to-zone zone1 policy in-gtp match destination-address
gsn1
set security policies from-zone other-zone to-zone zone1 policy in-gtp match application junos-
gprs-gtp
set security policies from-zone other-zone to-zone zone1 policy in-gtp then permit application-
services gprs-gtp-profile gtp1
```

Step-by-Step Procedure

To configure GTP inspection in NAT:

1. Configure interfaces.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.254/8
user@host# set interfaces ge-0/0/1 unit 0 family inet address 123.0.0.254/8
```

2. Configure and security zones

```
[edit security]
user@host# set zones security-zone zone1 interfaces ge-0/0/0.0 host-inbound-traffic system-
services all
user@host# set zones security-zone zone1 host-inbound-traffic protocols all
user@host# set zones security-zone other-zone interfaces ge-0/0/1.0 host-inbound-traffic
system-services all
user@host# set zones security-zone other-zone host-inbound-traffic protocols all
```

3. Define the address book.

```
[edit security]
user@host# set address-book global address gsn1 10.0.0.1/8
user@host# set address-book global address other-gsn 20.0.0.1/8
```

4. Define NAT rule.

```
[edit security nat]
user@host# set static rule-set rs1 from zone other-zone
user@host# set static rule-set rs1 rule r1 match destination-address 123.0.0.1/32
user@host# set static rule-set rs1 rule r1 then static-nat prefix 10.0.0.1/32
user@host# set proxy-arp interface ge-0/0/0.0 address 123.0.0.1/32
```

5. Enable GTP profile.

```
[edit security gprs gtp]
user@host# set profile gtp1
```

```
user@host# set profile gtp1 timeout 1
user@host# set profile gtp1 seq-number-validated
```

6. Check GTP traffic.

```
[edit security policies]
user@host# set from-zone zone1 to-zone other-zone policy out-gtp match source-address gsn1
user@host# set from-zone zone1 to-zone other-zone policy out-gtp match destination-address
other-gsn
user@host# set from-zone zone1 to-zone other-zone policy out-gtp match application junos-gprs-
gtp
user@host# set from-zone zone1 to-zone other-zone policy out-gtp then permit application-
services gprs-gtp-profile gtp1
user@host# set from-zone other-zone to-zone zone1 policy in-gtp match source-address other-gsn
user@host# set from-zone other-zone to-zone zone1 policy in-gtp match destination-address gsn1
user@host# set from-zone other-zone to-zone zone1 policy in-gtp match application junos-gprs-
gtp
user@host# set from-zone other-zone to-zone zone1 policy in-gtp then permit application-
services gprs-gtp-profile gtp1
```

Results

From configuration mode, confirm your configuration by entering the `show security` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
gprs {
    gtp {
        profile gtp1 {
            timeout 1;
            seq-number-validated;
        }
    }
}
address-book {
    global {
        address gsn1 10.0.0.1/8;
```

```
        address other-gsn 20.0.0.1/8;
    }
}
nat {
    static {
        rule-set rs1 {
            from zone other-zone;
            rule r1 {
                match {
                    destination-address 123.0.0.1/32;
                }
                then {
                    static-nat {
                        prefix {
                            10.0.0.1/32;
                        }
                    }
                }
            }
        }
    }
    proxy-arp {
        interface ge-0/0/0.0 {
            address {
                123.0.0.1/32;
            }
        }
    }
}
policies {
    from-zone zone1 to-zone other-zone {
        policy out-gtp {
            match {
                source-address gsn1;
                destination-address other-gsn;
                application junos-gprs-gtp;
            }
            then {
                permit {
                    application-services {
                        gprs-gtp-profile gtp1;
                    }
                }
```

```
            }
        }
    }
    from-zone other-zone to-zone zone1 {
        policy in-gtp {
            match {
                source-address other-gsn;
                destination-address gsn1;
                application junos-gprs-gtp;
            }
            then {
                permit {
                    application-services {
                        gprs-gtp-profile gtp1;
                    }
                }
            }
        }
    }
}
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone zone1 {
        host-inbound-traffic {
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
```

```
    }
    security-zone other-zone {
        host-inbound-traffic {
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/1.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying GTP Inspection on NAT | 134

Confirm that the configuration is working properly.

Verifying GTP Inspection on NAT

Purpose

Verify the GTP traffic between the internal network and the external network.

Action

From operational mode, enter the `show security` command.

Understanding Network Address Translation-Protocol Translation

Network Address Translation-Protocol Translation (NAT-PT) is a protocol translation mechanism that can be done in two directions, from IPv4 address format to IPv6 address format and vice versa. NAT-PT binds the addresses in the IPv6 network with addresses in the IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms.

In each direction, the static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes a destination IP address translation in one direction and a source IP address translation in the opposite direction.

The main advantage of NAT-PT is that the end devices and networks can run either IPv4 addresses or IPv6 addresses and traffic can be started from any side.

Example: Enhancing Traffic Engineering by Configuring NAT-PT Between an IPv4 and an IPv6 Endpoint with SCTP Multihoming

IN THIS SECTION

This example shows how to enhance traffic engineering by configuring NAT-PT between an IPv4 endpoint and an IPv6 endpoint. NAT-PT is a protocol translation mechanism that allows communication between IPv6-only and IPv4-only nodes through protocol-independent translation of IPv4 and IPv6 datagrams, requiring no state information for the session. NAT-PT binds the addresses in the IPv6 network with addresses in the IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms. The main advantage of NAT-PT is that the end devices and networks can run either IPv4 addresses or IPv6 addresses and traffic can be started from any side.

Requirements

This example uses the following hardware and software components:

- SRX5400 device

- Endpoint A connected to an SRX5400 device using two IPv6 addresses
- Endpoint B connected to an SRX5400 device using two IPv4 addresses

Overview

IN THIS SECTION

- Topology | 136

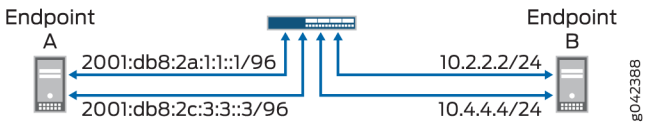
In this example, you configure NAT-PT between an IPv4 endpoint and an IPv6 endpoint. Endpoint A is connected to the SRX5400 device using two IPv6 addresses and endpoint B is connected to the SRX5400 device using two IPv4 addresses.

You can configure the SRX5400 device to translate the IP header and IP address list (located in the INIT/INT-ACK message) between an IPv4 address format and an IPv6 address format. In each direction, static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the opposite direction.

Figure 7 on page 136 illustrates the network topology used in this example.

Topology

Figure 7: NAT-PT Between an IPv4 Endpoint and an IPv6 Endpoint



For configuring NAT-PT details between IPv4 and IPv6 endpoints, seeTable 21 on page 136.

Table 21: Configuring NAT-PT Details Between IPv4 and IPv6 Endpoints

Endpoints	Address One	Address Two
A (IPv6)	2001:db8:2a:1:1::1/96	2001:db8:2c:3:3::3/96

Table 21: Configuring NAT-PT Details Between IPv4 and IPv6 Endpoints *(Continued)*

Endpoints	Address One	Address Two
B (IPv4)	10.2.2.2/24	10.4.4.4/34

Configuration

IN THIS SECTION

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-4/0/0 unit 0 family inet address 10.1.1.100/24
set interfaces ge-4/0/0 unit 0 family inet6 address 2001:db8:2a:1:1::100/96
set interfaces ge-4/0/1 unit 0 family inet address 10.2.2.100/24
set interfaces ge-4/0/1 unit 0 family inet6 address 2001:db8:2b:2:2::100/96
set interfaces ge-4/0/2 unit 0 family inet address 10.3.3.100/24
set interfaces ge-4/0/2 unit 0 family inet6 address 2001:db8:2c:3:3::100/96
set interfaces ge-4/0/3 unit 0 family inet address 10.4.4.100/24
set interfaces ge-4/0/3 unit 0 family inet6 address 2001:db8:2d:4:4::100/96
set security zones security-zone sctp_zone1 host-inbound-traffic system-services all
set security zones security-zone sctp_zone1 host-inbound-traffic protocols all
set security zones security-zone sctp_zone1 interfaces ge-4/0/0.0
set security zones security-zone sctp_zone1 interfaces ge-4/0/2.0
set security zones security-zone sctp_zone2 host-inbound-traffic system-services all
set security zones security-zone sctp_zone2 host-inbound-traffic protocols all
set security zones security-zone sctp_zone2 interfaces ge-4/0/1.0
set security zones security-zone sctp_zone2 interfaces ge-4/0/3.0
set security nat static rule-set sctp-natpt-from-zone1 from zone sctp_zone1
set security nat static rule-set sctp-natpt-from-zone1 rule r1-dst match destination-address
```

```
2001:db8:2b:2:2::2/96
set security nat static rule-set sctp-natpt-from-zone1 rule r1-dst then static-nat prefix
10.2.2.2/32
set security nat static rule-set sctp-natpt-from-zone1 rule r3-dst match destination-address
2001:db8:2d:4:4::4/96
set security nat static rule-set sctp-natpt-from-zone1 rule r3-dst then static-nat prefix
10.4.4.4/32
set security nat static rule-set sctp-natpt-from-zone2 from zone sctp_zone2
set security nat static rule-set sctp-natpt-from-zone2 rule r2-dst match destination-address
10.1.1.1/32
set security nat static rule-set sctp-natpt-from-zone2 rule r2-dst then static-nat prefix
2001:db8:2a:1:1::1/96
set security nat static rule-set sctp-natpt-from-zone2 rule r4-dst match destination-address
10.3.3.3/32
set security nat static rule-set sctp-natpt-from-zone2 rule r4-dst then static-nat prefix
2001:db8:2c:3:3::3/96
```

Procedure

Step-by-Step Procedure

To configure NAT-PT between an IPv4 endpoint and an IPv6 endpoint:

1. Configure interfaces.

```
[edit interfaces]
user@host# set ge-4/0/0 unit 0 family inet address 10.1.1.100/24
user@host# set ge-4/0/0 unit 0 family inet6 address 2001:db8:2a:1:1::100/96
user@host# set ge-4/0/1 unit 0 family inet address 10.2.2.100/24
user@host# set ge-4/0/1 unit 0 family inet6 address 2001:db8:2b:2:2::100/96
user@host# set ge-4/0/2 unit 0 family inet address 10.3.3.100/24
user@host# set ge-4/0/2 unit 0 family inet6 address 2001:db8:2c:3:3::100/96
user@host# set ge-4/0/3 unit 0 family inet address 10.4.4.100/24
user@host# set ge-4/0/3 unit 0 family inet6 address 2001:db8:2d:4:4::100/96
```

2. Configure zones.

```
[edit security zones]
user@host# set security-zone sctp_zone1 host-inbound-traffic system-services all
user@host# set security-zone sctp_zone1 host-inbound-traffic protocols all
```

```
user@host# set security-zone sctp_zone1 interfaces ge-4/0/0.0
user@host# set security-zone sctp_zone1 interfaces ge-4/0/2.0
user@host# set security-zone sctp_zone2 host-inbound-traffic system-services all
user@host# set security-zone sctp_zone2 host-inbound-traffic protocols all
user@host# set security-zone sctp_zone2 interfaces ge-4/0/1.0
user@host# set security-zone sctp_zone2 interfaces ge-4/0/3.0
```

3. Configure rules for the first static NAT zone.

```
[edit security nat]
user@host# set static rule-set sctp-natpt-from-zone1 from zone sctp_zone1
```

4. Specify the static NAT rule match criteria for the traffic coming from zone 1.

```
[edit security nat]
user@host# set static rule-set sctp-natpt-from-zone1 rule r1-dst match destination-address
2001:db8:2b:2:2::2/128
user@host# set static rule-set sctp-natpt-from-zone1 rule r1-dst then static-nat prefix
10.2.2.2/32
user@host# set static rule-set sctp-natpt-from-zone1 rule r3-dst match destination-address
2001:db8:2d:4:4::4/128
user@host# set static rule-set sctp-natpt-from-zone1 rule r3-dst then static-nat prefix
10.4.4.4/32
```

5. Configure rules for the second static NAT zone.

```
[edit security nat]
user@host# set static rule-set sctp-natpt-from-zone2 from zone sctp_zone2
```

6. Specify the static NAT rule match criteria for the traffic coming from zone 2.

```
[edit security nat]
user@host# set static rule-set sctp-natpt-from-zone2 rule r2-dst match destination-address
10.1.1.1/32
user@host# set static rule-set sctp-natpt-from-zone2 rule r2-dst then static-nat prefix
2001:db8:2a:1:1::1/128
user@host# set static rule-set sctp-natpt-from-zone2 rule r4-dst match destination-address
10.3.3.3/32
```

```
user@host# set static rule-set sctp-natpt-from-zone2 rule r4-dst then static-nat prefix
2001:db8:2a:3:3::3/128
```

Results

From configuration mode, confirm your configuration by entering the `show interfaces`, `show security zones`, and `show security nat static` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
    user@host# show interfaces
    ge-4/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.100/24;
        }
        family inet6 {
            address 2001:db8:2a:1:1::100/96;
        }
    }
}
ge-4/0/1 {
    unit 0 {
        family inet {
            address 10.2.2.100/24;
        }
        family inet6 {
            address 2001:db8:2b:2:2::100/96;
        }
    }
}
ge-4/0/2 {
    unit 0 {
        family inet {
            address 10.3.3.100/24;
        }
        family inet6 {
            address 2001:db8:2c:3:3::100/96;
        }
    }
}
```

```
ge-4/0/3 {
    unit 0 {
        family inet {
            address 10.4.4.100/24;
        }
        family inet6 {
            address 2001:db8:2d:4:4::100/96;
        }
    }
}
```

```
[edit]
user@host# show security zones
security-zone sctp_zone1 {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-4/0/0.0;
        ge-4/0/2.0;
    }
}
security-zone sctp_zone2 {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-4/0/1.0;
        ge-4/0/3.0;
```

```
    }
}
```

```
[edit]
user@host# show security nat static
rule-set sctp-natpt-from-zone1 {
    from zone sctp_zone1;
    rule r1-dst {
        match {
            destination-address 2001:db8:2b:2:2::2/128;
        }
        then {
            static-nat {
                prefix {
                    10.2.2.2/32;
                }
            }
        }
    }
    rule r3-dst {
        match {
            destination-address 2001:db8:2d:4:4::4/128;
        }
        then {
            static-nat {
                prefix {
                    10.4.4.4/32;
                }
            }
        }
    }
}
rule-set sctp-natpt-from-zone2 {
    from zone sctp_zone2;
    rule r2-dst {
        match {
            destination-address 10.1.1.1/32;
        }
        then {
            static-nat {
                prefix {
```

```
                    2001:db8:2a:1:1::1/128;
                }
            }
        }
    }
    rule r4-dst {
        match {
            destination-address 10.3.3.3/32;
        }
        then {
            static-nat {
                prefix {
                    2001:db8:2c:3:3::3/128;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the Configuration | 143

Verifying the Configuration

Purpose

Verify that the NAT-PT configuration between an IPv4 endpoint and an IPv6 endpoint is correct.

Action

From operational mode, enter the `show security zones` and `show security nat static rule all` commands.

```
user@host> show security zones
```

```
Security zone: sctp_zone1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 2
  Interfaces:
    ge-4/0/0.0
    ge-4/0/2.0

Security zone: sctp_zone2
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 2
  Interfaces:
    ge-4/0/1.0
    ge-4/0/3.0
```

```
user@host> show  security nat static rule all
Total static-nat rules: 4
Total referenced IPv4/IPv6 ip-prefixes: 4/4

Static NAT rule: r1-dst               Rule-set: sctp-natpt-from-zone1
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : sctp_zone1
  Destination addresses     : 2001:db8:2b:2:2::2
  Host addresses            : 10.2.2.2
  Netmask                   : 128
  Host routing-instance     : N/A
  Translation hits          : 0
    Successful sessions     : 0
    Failed sessions         : 0
  Number of sessions        : 0

Static NAT rule: r3-dst               Rule-set: sctp-natpt-from-zone1
  Rule-Id                   : 2
  Rule position             : 2
  From zone                 : sctp_zone1
  Destination addresses     : 2001:db8:2d:4:4::4
  Host addresses            : 10.4.4.4
  Netmask                   : 128
  Host routing-instance     : N/A
```

```
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0

Static NAT rule: r2-dst               Rule-set: sctp-natpt-from-zone2
  Rule-Id                    : 3
  Rule position              : 3
  From zone                  : sctp_zone2
  Destination addresses      : 10.1.1.1
  Host addresses             : 2001:db8:2a:1:1::1
  Netmask                    : 32
  Host routing-instance      : N/A
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0

Static NAT rule: r4-dst               Rule-set: sctp-natpt-from-zone2
  Rule-Id                    : 4
  Rule position              : 4
  From zone                  : sctp_zone2
  Destination addresses      : 10.3.3.3
  Host addresses             : 2001:db8:2c:3:3::3
  Netmask                    : 32
  Host routing-instance      : N/A
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

Meaning

The `show security zones` command displays all the zones configured and the interfaces associated with the zone. The `show security nat static rule all` command displays all the static NAT rules configured.

RELATED DOCUMENTATION

NAT Overview

PMI Flow Based CoS functions for GTP-U

IN THIS SECTION

Power-Mode IPsec (PMI) is a new mode of operation that provides IPsec performance improvements.

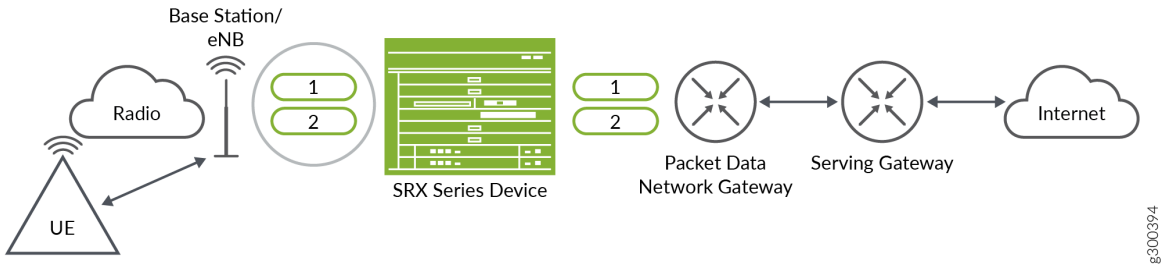
PMI Flow Based CoS functions for GTP-U scenario with TEID Distribution and Asymmetric Fat Tunnel Solution

With non-GTP traffic, the per-flow CoS solution assumes that all the packets of the same session should have same DSCP value. This won't work for GTP -U because it carries different user data. Therefore, there will be different DSCP code points for the same 5-tuple GTP session. If you combine the GTP-U session distribution solution together with per-flow CoS solution, you can provide a per-flow CoS solution for GTP-U scenario even if it carries multiple streams with different DSCP code inside one GTP tunnel.

The following information gives an overview on TEID based hash distributions and asymmetric fat tunnel solution.

TEID based hash distributions: GTP-U uses a fixed UDP port-2152 as its source port and destination port. There may be data streams from different users multiplexed within a single flow session, so 5-tuple is not enough to separate these data streams. There is a 4-byte field inside GTP payload called tunnel endpoint identifier (TEID), which is used to identify different connections in the same GTP tunnel. In order to migrate the GTP sessions to the anchor PIC, you need IPsec session affinity. Hence, a 6-tuple (including TEID) hash distribution is introduced for creating GTP-U sessions to different cores on anchor PIC, instead of creating GTP-U sessions only on the Anchor PIC.

Figure 8: LTE Networking Architecture



The Figure 8 on page 147 shows a typical LTE network architecture where an SRX Series Firewall is deployed as security gateway. A fat GTP tunnel carries data from different users. IPsec tunnels on the security gateway could be a fat tunnel due to the fat GTP tunnel. The SRX Series Firewall can create one GTP session with a high-bandwidth of GTP traffic. However, the throughput is limited to one core processor's performance.

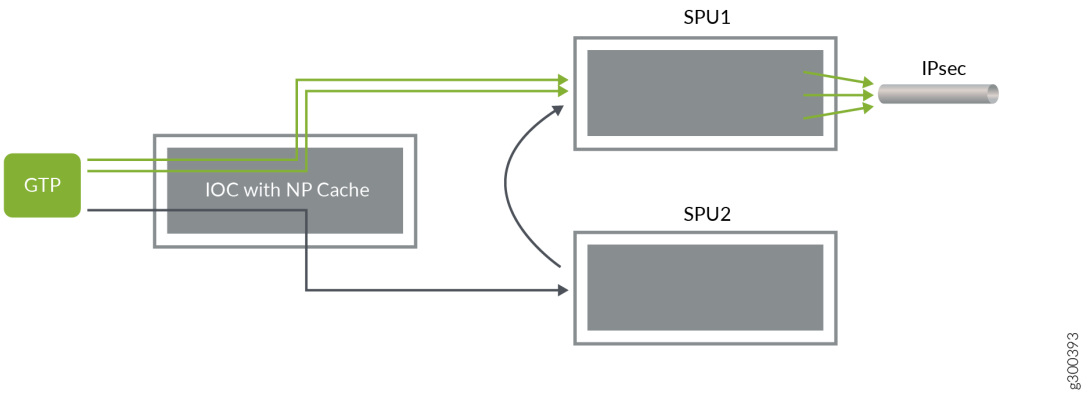
If you use TEID-based hash distribution for creating GTP-U sessions when PMI and IPsec session affinity are enabled, following events take place:

You can an enable SRX Series Firewall to process asymmetric fat tunnels (Example: 30Gbps on encryption direction / 3 Gbps on decryption direction) because PMI provides parallel encryption on multiple cores for one tunnel.

You can split a fat GTP session to multiple sessions and distribute them to different cores. This helps to increase the bandwidth for fat GTP tunnel on the SRX Series Firewalls.

Asymmetric fat tunnel solution: An SRX Series Firewalls support asymmetric fat tunnels because PMI provides parallel encryption on multiple cores for one tunnel. The TEID based hash distribution is introduced for creating GTP-U sessions to multiple cores on anchor PIC. When both PMI and IPsec session affinity are enabled, the clear-txt traffic acts as a fat GTP tunnel. This helps a fat GTP session to split into multiple slim GTP sessions and handle them on multiple cores simultaneously.

Figure 9: Fat GTP Tunnel Processing



The Figure 9 on page 148 shows how a fat tunnel processed when TEID-based hash distribution for creating GTP-U sessions.

On the encryption path, when one GTP tunnel with the 5-tuple enters, the Input/Output card (IOC) distributes the traffic into different cores according to 6-tuple including TEID hash. If the traffic is destined for the same IPsec tunnel, flow creates multiple GTP sessions on different cores of the anchor SPU.

The flow installs multiple NP caches on the IOC and when subsequent packets hit the NP cache, they are distributed to different cores on the anchor SPU.

Configurations to enable PMI and GTP

The following configuration helps to enable PMI and GTP.

Before you begin determine the following:

Understand how to establish PMI and GTP. Per-flow CoS functions for GTP-U traffic in PMI mode is available. TEID-based hash distribution for creating GTP-U sessions to multiple cores on anchor PIC when both PMI and IPsec session affinity are enabled. TEID-based hash distribution can help split a fat GTP session to multiple slim GTP sessions and process them on multiple cores in parallel. With this enhancement, per-flow CoS for GTP-U traffic is enabled even when the traffic carries multiple streams with different DSCP code within one GTP tunnel.

The following steps explain how to enable PMI and GTP sessions:

1. Set NP cache mode.

```
[edit]
user@host# set chassis fpc 1 np-cache
```

2. Configure power-mode IPsec. When IPsec is enabled, the IPSec tunnel could be a fat tunnel due to the fat flow session.

```
[edit security]
user@host# set flow power-mode-ipsec
```

3. Configure GTP-U session distribution.

```
[edit security]
user@host# set forwarding-process application-services enable-gtpu-distribution
```

4. Enable IPsec session-affinity.

```
[edit security]
user@host# set flow load-distribution session-affinity ipsec
```

5. From the configuration mode, confirm your configuration by entering the `show` command.

```
[edit security]
user@host# show
flow {
    load-distribution {
        session-affinity {
            ipsec;
        }
    }
    power-mode-ipsec;
}
forwarding-process {
    application-services {
        enable-gtpu-distribution;
    }
}
```

6. Commit the configuration.

```
[edit security]
user@host# commit
```

7. Reboot the device as NP cache requires reboot to take effect.

GGSN Overview

IN THIS SECTION

The gateway GPRS support node (GGSN) converts the incoming data traffic coming from the mobile users through the Service gateway GPRS support node (SGSN) and forwards it to the relevant network, and vice versa. The GGSN and the SGSN together form the GPRS support nodes (GSN).

Understanding GGSN Redirection

Junos OS supports GPRS tunneling protocol (GTP) traffic and gateway GPRS support node (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 GGSN tunneling protocol, control (GTP-C) and GGSN tunneling protocol, user plane (GTP-U) messages to GGSNs Y and Z, instead of X.

GGSN Pooling Scenarios Overview

IN THIS SECTION

The General Packet Radio Service (GPRS) tunneling protocol (GTP) supports different Gateway GPRS Support Node (GGSN) IP addresses during a tunnel creation procedure. There are two GGSN pooling scenarios that support Serving GPRS Support Node (SGSN) roaming.

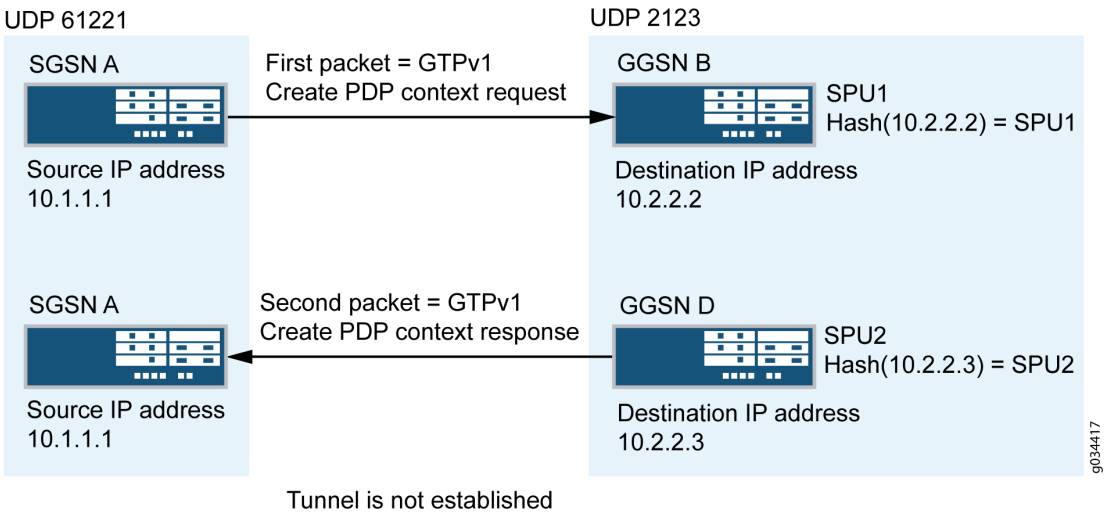
Understanding GGSN Pooling for Scenario 1

In Figure 10 on page 152, a packet data protocol (PDP) context request is sent from SGSN A to GGSN B during a GTP tunnel creation procedure. After sending the PDP context request message, GGSN D records the request information and it uses a different destination IP address from the request packet's destination IP address to send the response message to SGSN A.

In this scenario, two GTP packet messages are sent to Services Processing Unit 1 (SPU1) and SPU2 by the central point, and the messages are processed by SPU1 and SPU2 individually. The session is created on SPU1 and SPU 2 for each GTP packet. SPU1 records the request packet information and SPU2 records the response packet information.

The PDP response message sent from GGSN D to SGSN A is dropped because of a lack of request information. Thus the GTP tunnel is not established.

Figure 10: GGSN Pooling Scenario 1



NOTE: SPU2 cannot retrieve request information from SPU1.

Install Request Information to Remote SPU

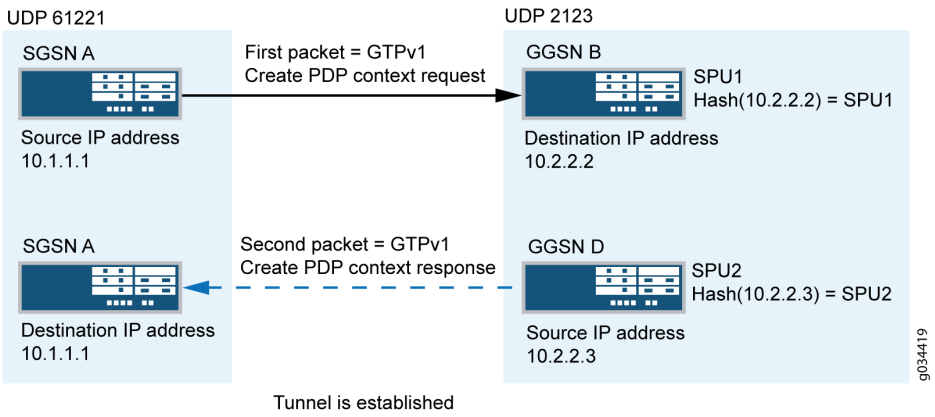
In this scenario, the PDP response packet was dropped because of a lack of request information, and the GTP tunnel was not established. This can be resolved by installing the request information on the correct SPU.

In Figure 11 on page 153, when creating a tunnel, the response packet's GGSN IP address changes, triggering a new session, and the central point distributes the message to another SPU.

The response packet always sends to the request packet's source address to the SPU. This helps to install the request information to the remote SPU for the next response packet.

Install the request information into the predictable SPU, HASH (req-src-ip) function while processing the request packet. After the expected SPU number (Hash (10.1.1.1) = SPU2) is calculated by the source IP address of the PDP request message, the request information is installed in the remote SPU2 through the Juniper Message Passing Interface (JMPI).

Figure 11: Functionality : GGSN Pooling Scenario 1



Now the request information is installed on local SPU1 and remote SPU2, so the PDP response message is allowed.

Workarounds for Scenario 1

In scenario 1, the PDP context request message sent from SGSN A reached the Junos OS default application `junos-gprs-gtp` and the GTP inspection was enabled for PDP context request message. However, the PDP context response message sent from GGSN D cannot reach the Junos OS default application `junos-gprs-gtp`. Thus the packet will not be inspected by the GTP module.

As a workaround, you need to enable GTP inspection for the PDP context response message by configuring the custom policy and applications. Refer to Configuring a GGSN Custom Policy/Application.

Understanding GGSN Pooling for Scenario 2

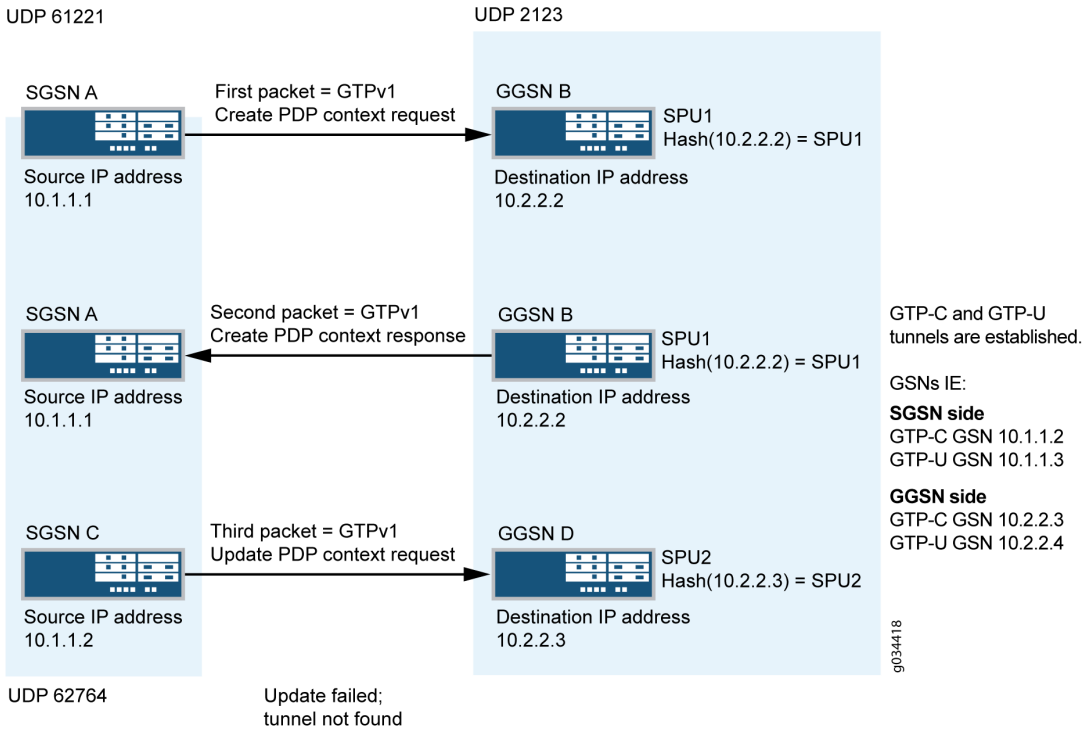
In Figure 12 on page 155, a packet data protocol (PDP) context request is sent from SGSN A to GGSN B during a GTP tunnel creation procedure. After receiving the PDP context request message, GGSN B sends the PDP context response message to SGSN A. After receiving the PDP context response message, the GTP-C tunnel is created between SGSN C and GGSN D. Then SGSN C sends an update PDP context request message to GGSN D using different source and destination IP addresses from the request packet's IP header.

In scenario 2, the SGSN A creates the first GTP context request and sends it to the SPU by the central point. The session is created for the request packet on SPU1. The response packet sent from GGSN B to SGSN A reaches the session correctly.

The request packet sent from SGSN A indicates that GTP-C is established on control IP 10.1.1.2 and the GTP-U is established on data IP 10.1.1.3. Likewise, the response message sent from GGSN indicates that GTP-C is established on control IP 10.2.2.3 and GTP-U is established on data IP 10.2.2.4.

The GTP-C and GTP-U tunnels are created on local SPU1 after all the endpoints are established. However, the tunnel is not established on SPU 2, so the PDP update request message received from SPU2 is dropped.

Figure 12: GGSN Pooling Scenario 2



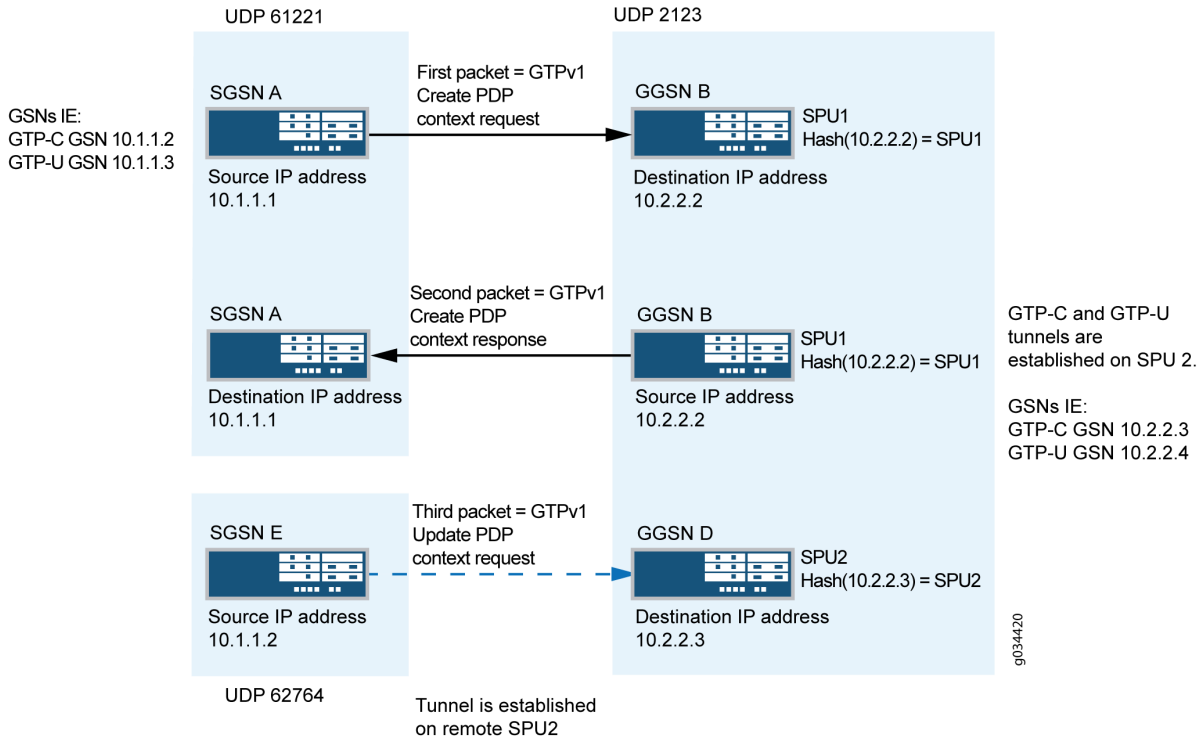
Install Tunnel Information to Remote SPU

In scenario 2, the update request packet is dropped because of a lack of tunnel information. This can be resolved by installing the tunnel information to the correct SPU after the request and response packets are processed. The SPU that receives the response packet installs the tunnel information on the local or remote SPU.

In Figure 13 on page 156, after the tunnel is established, the control messages are sent to the control tunnel endpoint. The destination IP address of all the control messages should be the control tunnel's GGSN endpoint IP address. This helps to calculate the remote SPU number in advance for the subsequent control message.

Install the tunnel information into the predictable SPU. After the SPU number is calculated by the control tunnel GGSN endpoint IP, the tunnel information is installed in the remote SPU through JMPI.

Figure 13: Functionality : GGSN Pooling Scenario 2



Now the tunnel information is installed on remote SPU2, so the PDP update response message is allowed.

Example: Configuring a GGSN Custom Policy and Application

IN THIS SECTION

This example shows how to configure a Gateway GPRS Support Node (GGSN) custom policy and application to support GGSN pooling scenario 1.

Requirements

This example uses the following hardware and software components:

- SRX5400 device
- A PC
- Junos OS Release 12.1X44-D10

Configuration

IN THIS SECTION

Configuring a GGSN Custom Policy

Overview

This example shows how to configure Security policies for GTP traffic which will make traffic work in case GTP Pooling occurs. This same example will also make GTP traffic flow correctly when the GTP Distribution feature is enabled, with or without GTP inspection. What we do here is configure the security policies in both directions, mirrored. In both directions we use the same address objects and the same applications. Besides the regular GTP application junos-gprs-gtp, we create a custom reverse GTP application, named reverse-junos-gprs-gtp. This reverse GTP application will make GTP packets match the security policy, even when only their source UDP port is a well-known GTP port. This way, all GTP traffic will be matched by the policies and handled correctly as GTP traffic.

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

In case when the GTP Distribution feature is used without GTP inspection, do not create the GTP profile and do not apply the application-services gtp-profile to the security policies.

```
set security address-book global address local_GSN_range 10.1.1.0/24
set security address-book global address remote_GSN_range 10.2.2.0/24
set security gtp profile GTP-Profile
set security policies from-zone trust to-zone untrust policy t-u match source-address
local_GSN_range
set security policies from-zone trust to-zone untrust policy t-u match destination-address
remote_GSN_range
set security policies from-zone trust to-zone untrust policy t-u match application junos-gprs-gtp
set security policies from-zone trust to-zone untrust policy t-u match application reverse-junos-
gprs-gtp
set security policies from-zone trust to-zone untrust policy t-u then permit application-
services gtp-profile GTP-Profile
set security policies from-zone untrust to-zone trust policy u-t match source-address
remote_GSN_range
set security policies from-zone untrust to-zone trust policy u-t match destination-address
local_GSN_range
set security policies from-zone untrust to-zone trust policy u-t match application reverse-junos-
gprs-gtp
set security policies from-zone untrust to-zone trust policy u-t match application junos-gprs-gtp
set security policies from-zone untrust to-zone trust policy u-t then permit application-
services gtp-profile GTP-Profile
```

Step-by-Step Procedure

To configure a GGSN custom policy:

1. Configure the source address.

```
[edit security] user@host#  set security policies from-zone trust to-zone untrust policy t-u
match source-address local_GSN_range
```

2. Configure the destination address.

```
[edit security]
user@host#  set security policies from-zone trust to-zone untrust policy t-u match
destination-address remote_GSN_range
```

3. Configure the policy applications.

```
[edit security]
user@host#set security policies from-zone trust to-zone untrust policy t-u match application
junos-gprs-gtp
user@host#set security policies from-zone trust to-zone untrust policy t-u match application
reverse-junos-gprs-gtp
```

4. Configure the activity type and specify the GTP profile name.

```
[edit security]user@host# set security policies from-zone trust to-zone untrust policy t-u
then permit application-services gtp-profile GTP-Profile
```

In case when the GTP Distribution feature is used without GTP inspection:

```
[edit security] user@host# set security policies from-zone trust to-zone untrust policy t-u
then permit
```

5. Configure the same again, with the security zones trust and untrust reversed.

Results

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy t-u {
        match {
            source-address local_GSN_range;
            destination-address remote_GSN_range;
            application [ junos-gprs-gtp reverse-junos-gprs-gtp ];
        }
        then {
            permit {
                application-services {
                    gtp-profile GTP-Profile;
```

```
                }
            }
        }
    }
}
from-zone untrust to-zone trust {
    policy u-t {
        match {
            source-address remote_GSN_range;
            destination-address local_GSN_range;
            application [ reverse-junos-gprs-gtp junos-gprs-gtp ];
        }
        then {
            permit {
                application-services {
                    gtp-profile GTP-Profile;
                }
            }
        }
    }
}
```

Before we can commit the configuration, we need to configure the reverse GTP application.

Configuring Reverse GTP Application

When using the GTP Distribution feature, the flow sessions will be set as uni-directional. This action to set them as uni-directional is performed by the GTP ALG (even when not using GTP Inspection). For this reason it is needed that the GTP ALG gets applied to all GTP traffic.

The predefined application junos-gprs-gtp is configured with the GTP ALG. However in some cases GTP traffic may not match this application, which will be the case for the return traffic when a different source port was used than the standard GTP UDP ports. In that case the reverse session wing can have a random destination port and the standard GTP port as source port. In order to make sure that the GTP ALG is applied to this reverse GTP traffic in this case, it is needed to add the following 'reverse' GTP application to all the GTP security policies.

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set applications application reverse-junos-gprs-gtp-c term t1 alg gprs-gtp-c
set applications application reverse-junos-gprs-gtp-c term t1 protocol udp
set applications application reverse-junos-gprs-gtp-c term t1 source-port 2123
set applications application reverse-junos-gprs-gtp-c term t1 destination-port 0-65535
set applications application reverse-junos-gprs-gtp-u term t1 alg gprs-gtp-u
set applications application reverse-junos-gprs-gtp-u term t1 protocol udp
set applications application reverse-junos-gprs-gtp-u term t1 source-port 2152
set applications application reverse-junos-gprs-gtp-u term t1 destination-port 0-65535
set applications application reverse-junos-gprs-gtp-v0 term t1 alg gprs-gtp-v0
set applications application reverse-junos-gprs-gtp-v0 term t1 protocol udp
set applications application reverse-junos-gprs-gtp-v0 term t1 source-port 3386
set applications application reverse-junos-gprs-gtp-v0 term t1 destination-port 0-65535
set applications application-set reverse-junos-gprs-gtp application reverse-junos-gprs-gtp-c
set applications application-set reverse-junos-gprs-gtp application reverse-junos-gprs-gtp-u
set applications application-set reverse-junos-gprs-gtp application reverse-junos-gprs-gtp-v0
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose

Verify that the GGSN custom policy configuration is correct.

Action

Commit the configuration and exit. From operational mode, enter the `show security policies` command.

Sample Output

command-name

```
[edit]
user@host# show applications
application reverse-junos-gprs-gtp-c {
    term t1 alg gprs-gtp-c protocol udp source-port 2123 destination-port 0-65535;
}
application reverse-junos-gprs-gtp-u {
    term t1 alg gprs-gtp-u protocol udp source-port 2152 destination-port 0-65535;
}
application reverse-junos-gprs-gtp-v0 {
    term t1 alg gprs-gtp-v0 protocol udp source-port 3386 destination-port 0-65535;
}
application-set reverse-junos-gprs-gtp {
    application reverse-junos-gprs-gtp-c;
    application reverse-junos-gprs-gtp-u;
    application reverse-junos-gprs-gtp-v0;
}

[edit]
user@host# commit and-quit
commit complete
Exiting configuration mode

user@host> show security policies
Default policy: deny-all
Default policy log Profile ID: 0
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
  Policy: t-u, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: local_GSN_range
    Destination addresses: remote_GSN_range
    Applications: junos-gprs-gtp, reverse-junos-gprs-gtp
    Source identity feeds: any
```

```
    Destination identity feeds: any
    Action: permit, application services
From zone: untrust, To zone: trust
  Policy: u-t, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: remote_GSN_range
    Destination addresses: local_GSN_range
    Applications: reverse-junos-gprs-gtp, junos-gprs-gtp
    Source identity feeds: any
    Destination identity feeds: any
    Action: permit, application services
```

This output shows a summary of policy configuration.

3

CHAPTER

Securing Stream Control Transmission Protocol (SCTP) Traffic

SCTP Overview

IN THIS SECTION

Stream Control Transmission Protocol (SCTP) is a transport-layer protocol that ensures reliable, in-sequence transport of data. SCTP provides multihoming support where one or both endpoints of a connection can consist of more than one IP address. This enables transparent failover between redundant network paths.

Understanding Stream Control Transmission Protocol

IN THIS SECTION

Stream Control Transmission Protocol (SCTP) is an IP Transport Layer protocol. SCTP exists at an equivalent level with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), which provides transport layer functions to many Internet applications. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP and supports data transfer across the network in single IP or multi-IP cases.

SCTP can transport signaling messages to and from Signaling System 7 (SS7) for 3G mobile networks through M3UA, M2UA, or SUA. SCTP is a packet-based transport protocol. SCTP provide reliable and secure transport, minimized end-to-end delay, short failover time in case of network failures and both sequence and no-sequence transport.

SCTP is optimized to:

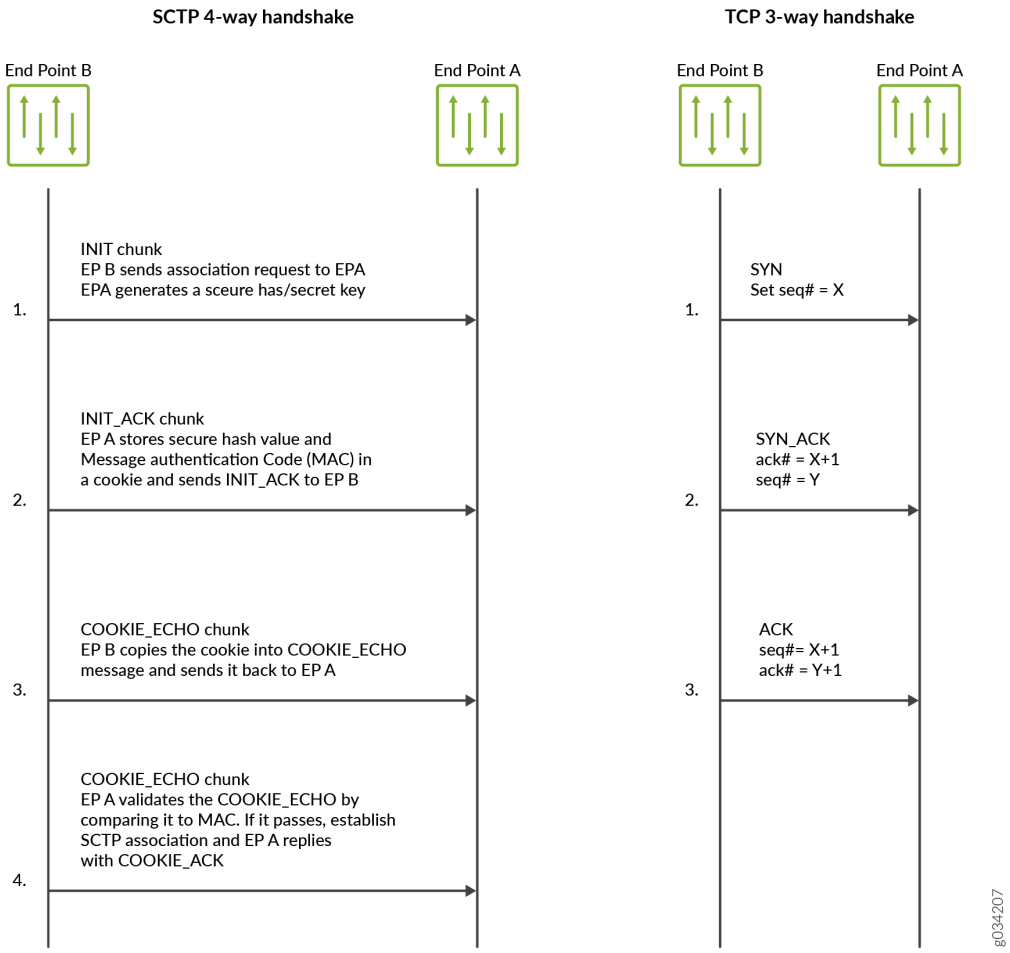
- Avoid the multithread infrastructure problems, when the traffic is high
- Improve the SCTP association searching rate (association lookup process speed is increased) by SCTP hash table optimization on the SPU
- Improve FSM for retransmission cases

Starting in Junos OS Release 12.3X48-D10 and Junos OS Release 17.3R1, the SCTP module inspects IPv4 and IPv6 traffic and checks all segments of the SCTP packet. (In previous releases the module inspected only IPv4 traffic and checked only the first segment of the SCTP packet.) The packet is then permitted or dropped based on the policy. For IPv6 traffic, the SCTP module inspects every extension header until it finds the SCTP header, and then only the SCTP header is processed and all the other headers are ignored.

SCTP is used for applications where monitoring and detection of loss of session is required. The SCTP path or session failure detection mechanism, for example, the heartbeat, monitors the connectivity of the session.

Figure 14 on page 167 illustrates the SCTP 4-way handshake and TCP 3-way handshake.

Figure 14: SCTP 4-way Handshake and TCP 3-way Handshake



SCTP Services

SCTP provides the following services:

- Aggregate Server Access Protocol (ASAP)
- Bearer-independent Call Control (BICC)
- Direct Data Placement Segment chunk (DDP-segment)
- Direct Data Placement Stream session control (DDP-stream)
- Diameter in a DTLS/SCTP DATA chunk (Diameter-DTLS)
- Diameter in a SCTP DATA chunk (Diameter-SCTP)

- DPNSS/DASS 2 extensions to IUA Protocol (DUA)
- Endpoint Handlescape Redundancy Protocol (ENRP)
- H.248 Protocol (H248)
- H.323 Protocol (H323)
- ISDN User Adaptation Layer (IUA)
- MTP2 User Peer-to-Peer Adaptation Layer (M2PA)
- MTP2 User Adaptation Layer (M2UA)
- MTP3 User Adaptation Layer (M3UA)
- Other unspecified-configured SCTP payload protocols (Others)
- Q.IPC
- Reserved
- S1 Application Protocol (S1AP)
- Simple Middlebox Configuration (SIMCO)
- SCCP User Adaptation Layer (SUA)
- Transport Adapter Layer Interface (TALI)
- V5.2 User Adaptation Layer (V5UA)
- X2 Application Protocol (X2AP)

SCTP Limitations and Constraints

SCTP has the following limitations and constraints:

- IP Addresses
  - A maximum of eight source IP addresses and eight destination IP addresses are allowed in an SCTP communication.
  - Only static IP NAT is supported; the interface packets (from one side: client or server) coming in must belong to the same zone.
- Policies
  - Dynamic policy is not supported. You must configure all policies for SCTP sessions.

- When policies are deleted, the related sessions and associations are cleared.
- You configure one policy to permit SCTP traffic from all client IPs to all server IPs, and another policy to permit SCTP traffic from server IPs to client IPs. If one policy has an SCTP profile, then the same SCTP profile is needed for the reverse policy.
- If you configure different policies for each session belonging to one association, there will be multiple policies related to one association, and the SCTP packet management (drop, rate-limit, and so on) uses the profile attached to the handling SCTP session's policy.
- The applications used in the security policies to permit the SCTP ALG traffic cannot be configured using the `application-protocol ignore` option. This condition is applicable even if the SCTP ALG inspection is not configured.

- SCTP enable/disable is controlled by whether there is a SCTP profile configured.
  - If no profile is attached to a policy, SCTP packets are forwarded without inspection.
  - If a profile with the `nat-only` option is attached to a policy, then only NAT translation is done on the SCTP packets matching the policy. If a profile does not have the `nat-only` option set, then both NAT translation and SCTP inspection are done on each SCTP packet matching the policy.
  - If you disable SCTP, all associations are deleted, and subsequent SCTP packets are passed or dropped according to the policy.
  - If you enable SCTP, all existing SCTP sessions must be cleared or the traffic matching old sessions will be forwarded without any inspection from the SCTP module.

    If you want to enable SCTP again, all the running SCTP communications will be dropped, because no associations exist. New SCTP communications can establish an association and perform the inspections.

    > **NOTE**: Clear old SCTP sessions when SCTP is reenabled; doing this will avoid any impact caused by the old SCTP sessions on the new SCTP communications.

  - If you add an SCTP profile to an existing policy, you must do one of the following: clear related sessions or remove the old policy and create a new policy.
  - If you change the timeout value in the SCTP profile, the configured handshake and the timeout value in existing associations will not change.

- SCTP Rate Limiting
  - Any change in the rate-limiting configuration will not affect the subsequent traffic of existing associations. It will apply to the newly established associations.

  - The supported protocol decimal value is from 0 to 63. This value includes 48 IANA assigned protocols and 16 unassigned protocols.
  - A maximum of 80 addresses are rate limited in one profile.
  - A maximum of 10 protocols are rate limited for one address in one profile.
  - The supported rate limit value is from 1 to 12000.
- SCTP Payload Protocol Blocking
  - Any change in the protocol-blocking configuration immediately impacts the subsequent traffic of existing associations.
  - The supported protocol decimal value is from 0 to 63. This value includes 48 IANA assigned protocols and 16 unassigned protocols.
- An SCTP endpoint can be a multihomed host with either all IPv4 addresses or all IPv6 addresses. An SCTP endpoint also supports NAT-PT in two directions, from an IPv4 address format to an IPv6 address format, and vice versa. SCTP module does not support IPv4 or IPv6 mixed-up multihoming and IPv4 or IPv6 mixed-up NAT-PT.
- For static NAT to work, the interfaces packets (from one side: client or server side) coming in must belong to the same zone.
- For multihome cases, only IPv4 address parameter or IPv6 address parameter in INIT or INI-ACK is supported.
- Only static NAT is supported for SCTP.
- Only established SCTP associations are synchronized to peer sessions.
- SCTP sessions are not deleted with associations; they time out in 30 minutes, which is the default value. The timeout value is configurable and can be changed.
- If the 4-way handshake process is not handled on one node, and is handled instead on two nodes (for example, two sessions on two nodes in active/active mode) or if the cluster is in failover before the 4-way handshake is completed, the association will not be established successfully.
- One SPU supports a maximum of 20,000 associations and a maximum of 1,280,000 SCTP sessions.

  In some cases, the associations might not be distributed to SPUs very evenly because the ports' hash result on the central point is uneven. For example, this event can occur when only two peers of ports are used, and one peer has 100 associations, but another peer has only one association. In this case, the associations cannot be distributed evenly on the firewall with more than one SPU.
- Unified in-service software upgrade (ISSU) to earlier Junos OS releases is not supported.

- The M3UA/SCCP message parsing is checked , but the M3UA/SCCP stateful inspection is not checked.
- Only ITU-T Rec. Q.711-Q.714 (07/96) standard is supported. ANSI, ETSI, China, and other standards are not supported.
- Only RFC 4960 is supported.
- VPN session affinity does not support GPRS tunneling protocol (GTP) and Stream Control Transmission Protocol (SCTP).

SCTP Features Overview

The following are the important features of SCTP:

- Multihoming support where one or both endpoints of a connection can consist of more than one IP address. This enables transparent failover between redundant network paths.
- Delivery of data in chunks within an independent stream eliminates unnecessary head-of-line blocking.
- Path selection and monitoring functionality to select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.
- Improved error detection suitable for jumbo Ethernet frames.

Understanding Central Point Architecture Support for SCTP

A Stream Control Transmission Protocol (SCTP) association is a connection between two SCTP endpoints. Each SCTP endpoint identifies the association with a tag. During an SCTP association setup, two SCTP endpoints exchange their own tags for receiving packets. During the exchange of packets between two SCTP endpoints, both the source address and the destination address can change in the association life cycle.

Prior to Junos OS Release 15.1X49-D40, all sessions of a given SCTP association are hashed to the same Services Processing Unit (SPU) by the fixed per-association SCTP port pair. However, in some cases, multiple SCTP associations share the same port pair, resulting in a bad load-balancing situation with all traffic being handled by a single SPU. Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, to handle the load-balancing issue, tag-based hash distribution is used to ensure even distribution of SCTP traffic from different associations among all SPUs. A 32-bit connection tag is introduced that uniquely identifies the SCTP sessions. The connection tag for SCTP is the vTag and the connection ID remains 0 if the connection tag is not used by the sessions.

The SCTP flow session utilizes a connection tag to more finely distribute SCTP traffic across SPUs on SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices that support the SCTP ALG. The connection tag is decoded from the SCTP vtag. A separate SCTP session will be created for each of the first three packets—that is, one session for INIT, INIT-ACK, and COOKIE-ECHO, respectively. Because, the reverse-direction traffic has its own session, the session can no longer match the existing forward-direction session and pass through automatically. Therefore, similar to the forward-direction policy, an explicit policy is needed for approving the reverse-direction SCTP traffic. In this scenario, the SCTP flow session requires a bidirectional policy configuration to be established for even a basic connection.

SEE ALSO

Understanding Enhancements to Central Point Architecture for the SRX5000 Line

SCTP Packet Structure Overview

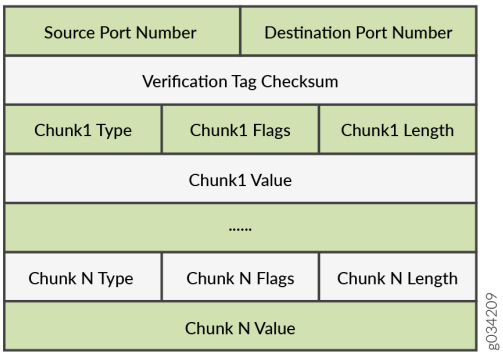
IN THIS SECTION

An SCTP packet consists of the following sections:

- "Common Header Section" on page 173
- "Data Chunk Section" on page 173

Figure 15 on page 173 illustrates the structure of the SCTP packet.

Figure 15: SCTP Packet Structure



Common Header Section

All SCTP packets require a common header section. This section occupies the first 12 bytes of the packet. Table 22 on page 173 describes the fields in the common header section:

Table 22: Common Header Fields

Field	Description
Source port number	Identifies the sending port.
Destination port number	Identifies the receiving port. The hosts use the destination port number to route the packet to the appropriate destination or an application.
Verification tag	Distinguishes stale packets from a previous connection. This is a 32-bit random value created during initialization.
Checksum	Uses the cyclic redundancy check (CRC32) algorithm to detect errors that might have been introduced during data transmission.

Data Chunk Section

Data chunk section—This section occupies the remaining portion of the packet. Table 23 on page 174 describes the fields in the data chunk section:

Table 23: Data Chunk Fields

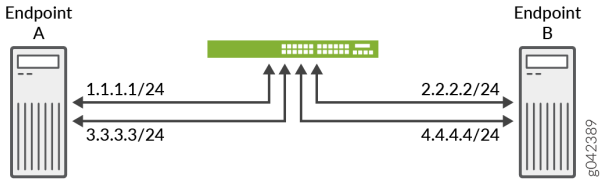
Field	Description
Chunk Type	Identifies the contents of the chunk value field. This is 1- byte long.
Chunk Flags	Consists of 8 flag-bits whose definition varies with the chunk type. The default value is zero. This indicates that no application identifier is specified by the upper layer for the data.
Chunk Length	Specifies the total length of the chunk in bytes. This field is 2 - bytes long. If the chunk does not form a multiple of 4 bytes (that is, the length is not a multiple of 4) it is implicitly padded with zeros which are not included in the chunk length.
Chunk Value	A general purpose data field.

The resource manager (RM) allows 8 source IP addresses and 8 destination IP addresses during an SCTP communication.

Understanding SCTP Multihoming

A Stream Control Transmission Protocol (SCTP) endpoint can be a *multihomed* host with either all IPv4 addresses or all IPv6 addresses. In Figure 16 on page 174, endpoint A is connected to an SRX Series Firewall with two IPv4 addresses, and endpoint B is connected to an SRX Series Firewall with two IPv4 addresses. Therefore, endpoint A and endpoint B can set up an association using four different pairs of IP addresses, resulting in four valid paths for communication.

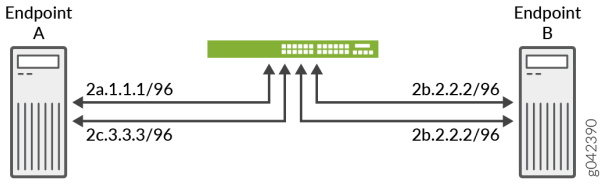
Figure 16: SCTP Multihoming with Two IPv4 Endpoints



In Figure 17 on page 175, endpoint A is connected to an SRX Series Firewall with two IPv6 addresses, and endpoint B is connected to an SRX Series Firewall with two IPv6 addresses. Therefore, endpoint A

and endpoint B can set up an association using four different pairs of IP addresses, resulting in four valid paths for communication.

Figure 17: SCTP Multihoming with Two IPv6 Endpoints



Understanding SCTP Multichunk Inspection

The Stream Control Transmission Protocol (SCTP) firewall checks all chunks in a message and then permits or drops the packet based on the policy. Use the `set security gprs sctp multichunk-inspection enable` command to enable SCTP multichunk inspection to check all chunks in a message. Use the `delete security gprs sctp multichunk-inspection enable` or `set security gprs sctp multichunk-inspection disable` command to disable SCTP multichunk inspection to check only the first chunk.

After enabling SCTP multichunk inspection, the SCTP firewall checks all chunks in a message and permits or drops the packet. The SCTP firewall drops the packet in the following cases:

- The layout of the SCTP chunks do not follow RFC 4960.
- A control chunk cannot pass the inspection of the SCTP finite state machine (FSM) or sanity checks.
- A data chunk is not allowed to pass the SCTP profile because of the SCTP FSM or sanity checks.
- A data chunk is not allowed to pass through the SCTP profile because of protocol blocking or rate limiting. The SCTP firewall resets this chunk to a null protocol data unit (PDU) and continues to check the next chunk. A data chunk is set to a null PDU based on the following rules:
  - When you set the null PDU value to `0xFFFF` using the `set security gprs sctp nullpdu protocol ID-0xFFFF` command, then the payload protocol identifier value is replaced with `0xFFFF` and the user data field is not modified.
  - When you set the null PDU value to `0x0000` using the `set security gprs sctp nullpdu protocol ID-0x0000` command, then the payload protocol identifier value is replaced with `0x0000` and the first four bytes of the user data field is replaced with zeroes.

  If all chunks in a packet are null PDUs, the SCTP firewall drops the packet.

Understanding SCTP Behavior in Chassis Cluster

In a *chassis cluster* configuration mode, the SCTP configuration and the established SCTP association is synced with the peer device. The SCTP module supports both active-active and active-passive modes.

The established SCTP association sends a creation or deletion message to the peer whenever an association is created or deleted on the active device. The secondary device adds or deletes an association respectively upon receiving the message from the established SCTP association. SCTP module then registers the corresponding callback function to receive and handle this message. There is no continuous timer sync between the two associations.

SCTP module will register a cold start sync function when a secondary device joins the cluster or reboots. The SCTP cold start function is called to sync all SCTP associations with the peer devices at the same time.

After the switchover, the established SCTP associations will remain functioning, but the associations in the progress of establishment will be lost and the establishment procedure needs to be re-initiated. It is also possible that the associations in the progress of teardown miss the ack message and leaves unestablished SCTP associations in the firewall. These associations will be cleaned up when the timer expires (5 hours by default) due to no activity in the association.

- You should configure all policies for your required SCTP sessions.
  For example, suppose you have endpoints A and B. Endpoint A has one SCTP association with x number of IPs (IP_a1, IP_a2, IP_a3...IP_ax). Endpoint B has one SCTP association with y number of IPs (IP_b1, IP_b2, IP_b3...IP_by.) The policy on the security device should permit all possible x*y paths in both directions.
- When an SCTP association is removed, the related SCTP sessions still exist and time out by themselves.

Release History Table

Release	Description
15.1X49-D40	Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, to handle the load-balancing issue, tag-based hash distribution is used to ensure even distribution of SCTP traffic from different associations among all SPUs.
12.3X48-D10	Starting in Junos OS Release 12.3X48-D10 and Junos OS Release 17.3R1, the SCTP module inspects IPv4 and IPv6 traffic and checks all segments of the SCTP packet.

RELATED DOCUMENTATION

Chassis Cluster Overview

SCTP Configuration

IN THIS SECTION

Stream Control Transmission Protocol (SCTP) can be configured to perform stateful inspection on all SCTP traffic.

SCTP Configuration Overview

You must configure at least one SCTP profile to enable the security device to perform stateful inspection on all SCTP traffic. The stateful inspection of SCTP traffic will drop some anomalous SCTP packets.

The SCTP firewall supports deeper inspection of the profiles:

- Packet filtering—The profile configuration of drop packets for special SCTP payload protocol and M3UA service enables packet filtering.
- Limit-rate—Controls the M3UA and SCCP packets rate per association.

The SCTP deeper inspection requires the following settings:

- Creating a SCTP profile
- Configuring the filtering and limit parameters
- Binding the SCTP profile to a policy

Example: Configuring a Security Policy to Permit or Deny SCTP Traffic

IN THIS SECTION

This example shows how to configure a security policy to permit or deny SCTP traffic.

Requirements

Before you begin:

- Create zones. See Example: Creating Security Zones.
- Configure an address book and create addresses for use in the policy. See Example: Configuring Address Books and Address Sets.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See Example: Configuring Security Policy Applications and Application Sets.
- Configure a GPRS SCTP profile. See "Example: Configuring a GPRS SCTP Profile for Policy-Based Inspection to Reduce Security Risks" on page 184.

Overview

The SCTP firewall implements a policy mechanism that is administratively used to determine the packets that can be passed or dropped. Policies can be configured for multiple addresses, address groups, or the entire zone.

In situations where only a few ports are used for SCTP traffic, the SCTP associations are not evenly distributed to Services Processing Units (SPUs). This occurs in the following cases:

- Uneven hash results on the association ports pairs.
- The number of port pairs is less than, or not much greater than, the number of SPUs.

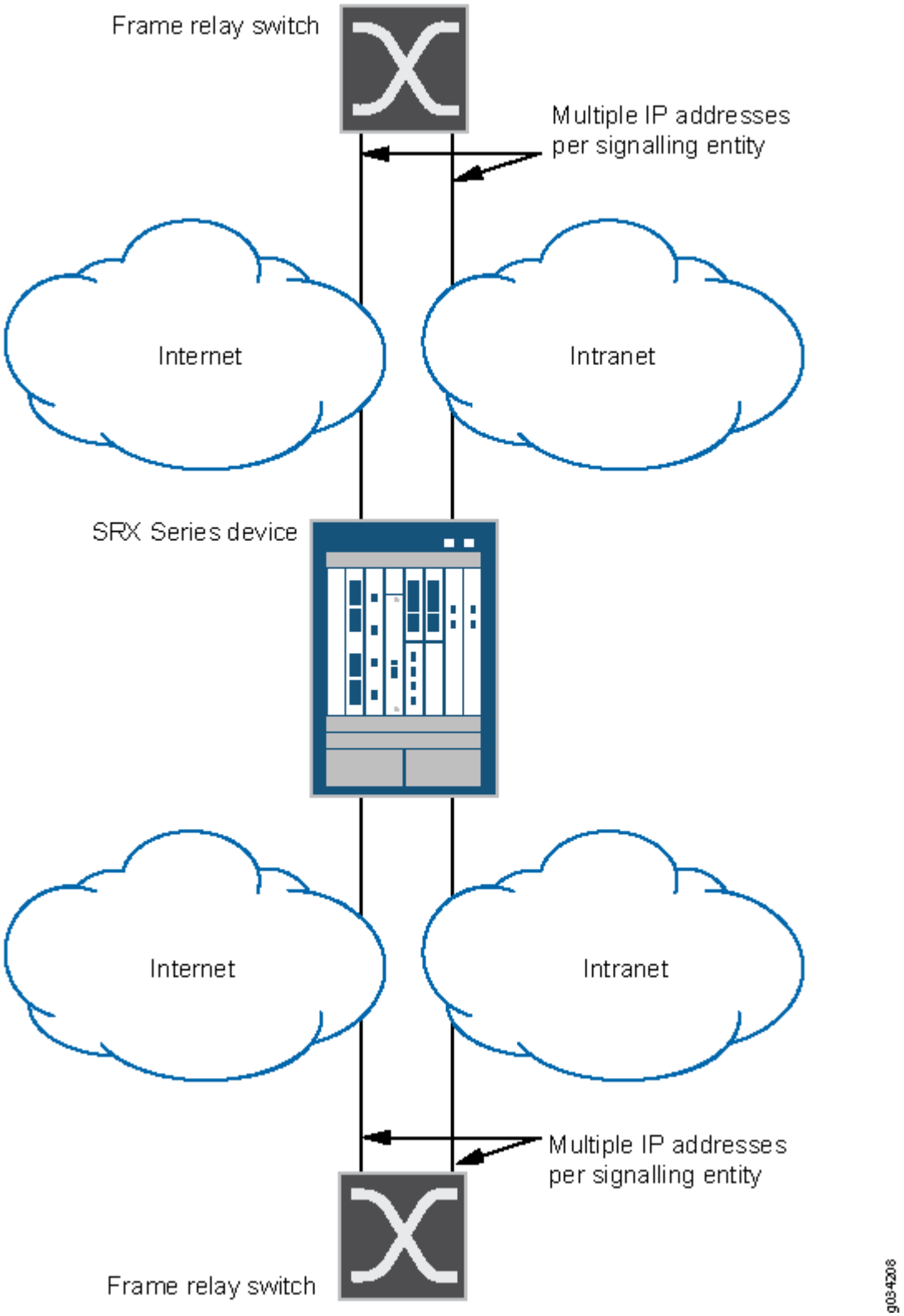
This configuration example shows how to:

- Deny SCTP traffic from the trust zone to the IP address 10.1.1.0/24 in the untrust zone.

- Permit SCTP traffic from an IP address 10.1.2.0/24 in the trust zone to the untrust zone with the SCTP configuration specified in the roam2att profile.

Figure 18 on page 180 shows the SCTP firewall implementation.

Figure 18: SCTP Firewall Implementation



Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone trust interfaces ge-0/0/2
set security zones security-zone untrust interfaces ge-0/0/1
set security policies from-zone trust to-zone untrust policy deny-all match source-address any
set security policies policy from-zone trust to-zone untrust policy deny-all match destination-
address 10.1.1.0/24
set security policies policy from-zone trust to-zone untrust policy deny-all match application
junos-gprs-sctp
set security policies from-zone trust to-zone untrust policy deny-all then deny
set security policies from-zone trust to-zone untrust policy allow-att-roaming match source-
address 10.1.2.0/24
set security policies from-zone trust to-zone untrust policy allow-att-roaming match destination-
address any
set security policies policy from-zone trust to-zone untrust policy allow-att-roaming match
application junos-gprs-sctp
set security policies from-zone trust to-zone untrust policy allow-att-roaming then permit
application-services gprs-sctp-profile roam2att
```

Step-by-Step Procedure

To configure a security policy to permit or deny SCTP traffic:

1. Configure the interfaces and security zones.

```
[edit security zones]
user@host# set security-zone trust interfaces ge-0/0/2
user@host# set security-zone untrust interfaces ge-0/0/1
```

2. Create the security policy to permit traffic from the trust zone to the untrust zone.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy allow-att-roaming match source-address 10.1.2.0/24
user@host# set policy allow-att-roaming match destination-address any
user@host# set policy allow-att-roaming match application junos-gprs-sctp
user@host# set policy allow-att-roaming then permit application-services gprs-sctp-profile
roam2att
```

3. Create the security policy to deny traffic from the trust zone to the untrust zone.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy deny-all match source-address any
user@host# set policy deny-all match destination-address 10.1.1.0/24
user@host# set policy deny-all match application junos-gprs-sctp
user@host# set policy deny-all then deny
```

Results

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy deny-all {
        match {
            source-address any;
            destination-address 10.1.1.0/24;
            application junos-gprs-sctp;
        }
        then {
```

```
            deny;
        }
    }
    policy allow-att-roaming {
        match {
            source-address 10.1.2.0/24;
            destination-address any;
            application junos-gprs-sctp;
        }
        then {
            permit {
                application-services {
                    gprs-sctp-profile roam2att;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying SCTP Configuration | 183

Confirm that the configuration is working properly.

Verifying SCTP Configuration

Purpose

Verify the policy inspection configuration.

Action

From operational mode, enter `show configuration |display set |match profile`

Example: Configuring a GPRS SCTP Profile for Policy-Based Inspection to Reduce Security Risks

IN THIS SECTION

In the GPRS architecture, the fundamental cause of security threats to an operator's network is the inherent lack of security in the GPRS tunneling protocol (GTP). This example shows how to configure a GPRS SCTP profile for policy-based inspection to reduce the GTP's security risks.

Requirements

Before you begin, understand the GPRS SCTP hierarchy and its options.

Overview

In this example, you configure a GPRS SCTP profile by setting the limit rate parameter and the payload protocol parameter for SCTP inspection. If your policy includes the `nat-only` option, the payload IP addresses are translated, but they are not inspected.

The SCTP commands can be applied only to the policy configured with an SCTP profile.

If you remove the SCTP profile from the policy, the packets are forwarded without any inspection, and the IP address list in the packet payload will not be translated, even if the related static NAT is configured.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter **commit** from configuration mode.

```
set security gprs sctp profile roam2att limit rate address 10.1.1.0 sccp 100
set security gprs sctp profile roam2att limit rate address 10.1.1.0 ssp 10
set security gprs sctp profile roam2att limit rate address 10.1.1.0 sst 50
set security gprs sctp profile roam2att drop payload-protocol all
set security gprs sctp profile roam2att permit payload-protocol dua
```

Step-by-Step Procedure

To configure a GPRS SCTP profile:

1. Configure the limit rate parameter.

   The limit rate is per association.

   ```
   [edit security gprs sctp profile roam2att]
   user@host# set limit rate address 10.1.1.0 sccp 100
   user@host# set limit rate address 10.1.1.0 ssp 10
   user@host# set limit rate address 10.1.1.0 sst 50
   ```

2. Configure the payload protocol to drop all SCTP payload messages.

   ```
   [edit security gprs sctp profile roam2att]
   user@host# set drop payload-protocol all
   ```

3. Configure the payload protocol to allow certain SCTP payload messages.

   ```
   [edit security gprs sctp profile roam2att]
   user@host# set permit payload-protocol dua
   ```

Results

From configuration mode, confirm your configuration by entering the **show security gprs** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security gprs
sctp {
    profile roam2att {
        drop {
            payload-protocol all;
        }
        permit {
            payload-protocol dua;
        }
        limit {
            rate {
                address 10.1.1.0 {
                    sccp 100;
                    ssp 10;
                    sst 50;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying SCTP Profile Configuration | 187

Confirm that the configuration is working properly.

Verifying SCTP Profile Configuration

Purpose

Verify the SCTP profile configuration.

Action

From configuration mode, enter the **show configuration security gprs sctp profile roam2att** command.

```
user@host> show configuration security gprs sctp profile roam2att
drop {
    payload-protocol all;
}
permit {
    payload-protocol dua;
}
limit {
    rate {
        address 10.1.1.0 {
            sccp 100;
            ssp 10;
            sst 50;
        }
    }
}
```

Meaning

The output displays information about the SCTP payload messages allowed and SCTP payload messages that are dropped. Verify the following information:

- Dropped SCTP payload messages
- Allowed SCTP payload messages

4

CHAPTER

Configuration Statements and Operational Commands

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- *Junos CLI Reference*

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- *Configuration Statements*
- *CLI Commands*