Junos® OS

General Packet Radio Service Feature Guide for Security Devices

Modified: 2017-08-09

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

Junos® OS General Packet Radio Service Feature 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 http://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- SRX4100
- SRX4200
- SRX5400
- SRX5600
- SRX5800
- vSRX
- SRX1500

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xvi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Introduction to General Packet Radio Service

GPRS Overview

Supported Platforms SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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 mobile stations (MSs) 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 MS and encapsulates them within a GTP header before forwarding them to the GGSN through the GTP tunnel. When the GGSN receives the packets, it decapsulates them and forwards them to the external host.

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 and a GGSN within the same public land mobile network (PLMN).
- Gp—The Gp interface is the connection between two PLMNs.
- Gi—The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN.

NOTE: The term *interface* has 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 and a GGSN.

This topic contains the following sections:

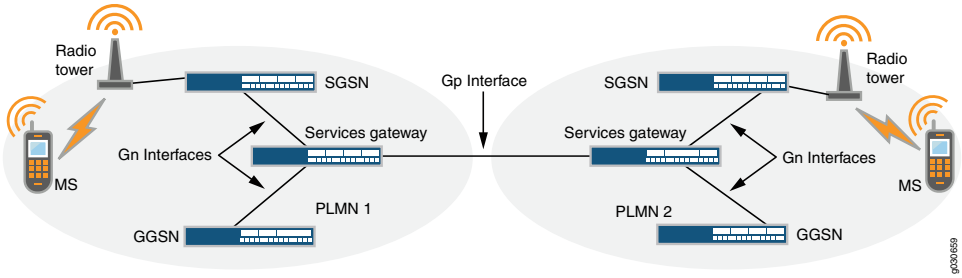
Gp and Gn Interfaces

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

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

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

Figure 1: Gp and Gn Interfaces



Gi Interface

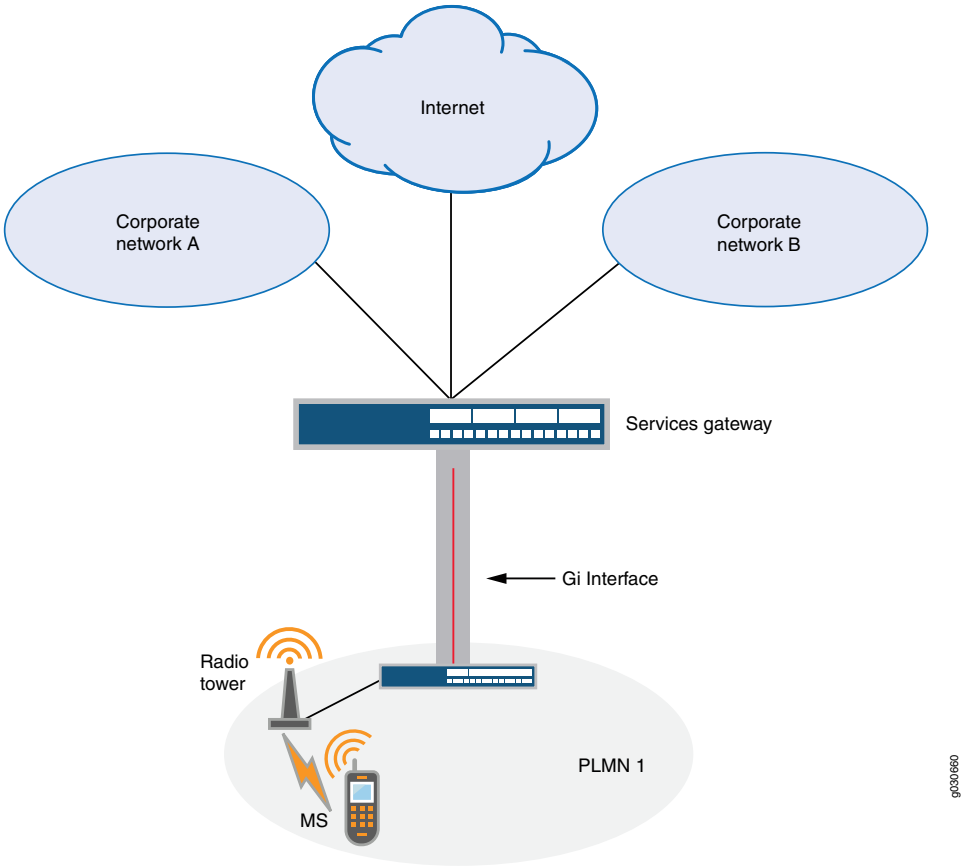
When you implement a security device on the Gi interface, you can simultaneously control traffic for multiple networks, protect a PLMN against the Internet and external networks, and protect mobile users from the Internet and other networks. Junos OS provides a great number of virtual routers, making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

NOTE: SRX Series devices 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 Network Address Translation (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 devices 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.

Related Documentation

- *Ethernet Switching and Layer 2 Transparent Mode Feature Guide for Security Devices*
- *Chassis Cluster Overview*
- Understanding Policy-Based GTP on page 11
- Understanding GTP Inspection Objects on page 17
- Understanding GTP Message Filtering on page 21
- Supported GTP Message Types on page 24

Understanding Central Point Architecture Support for GTP

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

User equipment (for example, a cellphone) attaches to a Serving GPRS Support Node (SGSN) for General Packet Radio Service (GPRS) data service. The SGSN 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 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 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-U traffic handled by a GGSN and SGSN pair on all SPUs by switching to tunnel-based session distribution in which the GTP-U traffic of different tunnels is spread across different SPUs. Use the **enable-gtpu-distribution** command to enable GTP-U session distribution.

Release History Table

Release	Description
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

- enable-gtpu-distribution on page 147

Understanding GTP Handover Messages

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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 device 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 devices for forwarding GPRS tunneling protocol, user plane (GTP-U) stateful check.

NOTE: **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.

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.

Related Documentation

- Understanding GTP Message Filtering on page 21

PART 2

Configuring GPRS Tunnel Protocol v1

CHAPTER 2

Configuring Policy-Based GTP

Understanding Policy-Based GTP

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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).

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.

Related Documentation

- GPRS Overview on page 3
- Understanding GTP Inspection Objects on page 17

Example: Enabling GTP Inspection in Policies

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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

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

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.

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message Filtering on page 21
- Supported GTP Message Types on page 24

CHAPTER 3

Configuring GTP Inspection Objects

Understanding GTP Inspection Objects

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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. 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.

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message Filtering on page 21
- Supported GTP Message Types on page 24
- Example: Creating a GTP Inspection Object on page 17

Example: Creating a GTP Inspection Object

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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

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

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message Filtering on page 21
- Supported GTP Message Types on page 24

Understanding IP Address Validation on GTP

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800

The user equipment (for example, a cellphone) accesses data through the mobile core network, and information is carried in the GTP tunnel by GTP-U packets. The IP address of the user equipment is allocated during the GTP-U tunnel creation. User equipment can support both IPv4 and IPv6 address types. The address allocated to the user equipment is recognized by the GTP-U tunnel.

During the GTP-U security check procedure, IPv4 and IPv6 addresses for user equipment will be checked against the end-user address stored in the user tunnel. Once the GTP-U

packet is determined to match the user equipment address, the packet data unit (PDU) is parsed to obtain the user equipment address. To validate the IP address, use the following command:
user@host# set security gprs gtp profile *profile-name* end-user-address-validated

If the user equipment address is IPv4, it will be compared with the IPv4 address stored in the user tunnel. If the user equipment address is IPv6, it will be compared with the IPv6 address stored in the user tunnel. If the result of the comparison is the same, the data packet will pass; otherwise, the packet will be dropped.

Related Documentation
- end-user-address-validated (GTP) on page 147

Understanding GTP-U Inspection

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: 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.

NOTE: 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.

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

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

- GPRS Overview on page 3

CHAPTER 4

Configuring GTP Message Filtering

Understanding GTP Message Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message-Length Filtering on page 22
- Supported GTP Message Types on page 24

Understanding GTP Message-Length Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Example: Setting the GTP Message Lengths on page 22
- Supported GTP Message Types on page 24

Example: Setting the GTP Message Lengths

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message-Length Filtering on page 22
- Supported GTP Message Types on page 24

Understanding GTP Message-Type Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Example: Permitting and Denying GTP Message Types on page 26
- Supported GTP Message Types on page 24

Supported GTP Message Types

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Table 3 on page 24 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 3: 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	
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

Table 3: GTP Messages *(continued)*

Message	Message Type	Version 0	Version 1
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
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
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

Table 3: GTP Messages *(continued)*

Message	Message Type	Version 0	Version 1
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

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message-Type Filtering on page 23
- Example: Setting the GTP Message Lengths on page 22

Example: Permitting and Denying GTP Message Types

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

- Requirements on page 26
- Overview on page 26
- Configuration on page 26
- Verification on page 27

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

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message-Type Filtering on page 23
- Supported GTP Message Types on page 24

Understanding GTP Message-Rate Limiting

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Example: Limiting the Message Rate and Path Rate for GTP Control Messages on page 28
- Supported GTP Message Types on page 24

Understanding GTP Control Message Path Rate Limiting

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: You can configure both the **rate-limit** and the **path-rate-limit** options at the same time.

Related Documentation

- Example: Limiting the Message Rate and Path Rate for GTP Control Messages on page 28

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

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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
```

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

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message-Rate Limiting on page 27
- Supported GTP Message Types on page 24

Example: Enabling GTP Sequence Number Validation

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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.

Related Documentation

- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Understanding GTP IP Fragmentation

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

A GPRS tunneling protocol (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.

Related Documentation

- Understanding GTP Information Elements on page 35
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

CHAPTER 5

Configuring GTP Information Elements

Understanding GTP Information Elements

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: 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.

Related Documentation

- Understanding GTP IP Fragmentation on page 34
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Understanding GTP APN Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Example: Setting a GTP APN and a Selection Mode on page 37
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Setting a GTP APN and a Selection Mode

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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.

Related Documentation

- Understanding GTP APN Filtering on page 36
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Understanding IMSI Prefix Filtering of GTP Packets

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Example: Setting a Combined IMSI Prefix and APN Filter on page 39
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Setting a Combined IMSI Prefix and APN Filter

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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.

Related Documentation

- Understanding IMSI Prefix Filtering of GTP Packets on page 39
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

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

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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).

Related Documentation

- Example: Removing R6 Information Elements from GTP Messages on page 44
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Supported R6 Information Elements

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Junos OS supports all 3GPP R6 IEs for GTP), as listed in Table 4 on page 41.

Table 4: 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 4: 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
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

Table 4: Supported Information Elements *(continued)*

IE Type Value	Information Element
140	RAB Setup Information
141	Extension Header Type List
142	Trigger Id
143	OMC Identity
144	RAN Transparent Container
145	PDP Context Prioritization
146	Additional RAB Setup Information
147	SGSN Number
148	Common Flags
149	APN Restriction
150	Radio Priority LCS
151	RAT Type
152	User Location Information
153	MS Time Zone
154	IMEI-SV
155	CAMEL Charging Information Container
156	MBMS UE Context
157	Temporary Mobile Group Identity (TMGI)
158	RIM Routing Address
159	MBMS Protocol Configuration Options
160	MBMS Service Area
161	Source TNC PDCP context Information
162	Additional Trace Information
163	Hop Counter

Table 4: Supported Information Elements *(continued)*

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

Related Documentation

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Example: Removing R6 Information Elements from GTP Messages on page 44
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Removing R6 Information Elements from GTP Messages

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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
   ```

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

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Supported R7 Information Elements

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Junos OS supports all 3GPP R7 IEs for GTP, as listed in Table 5 on page 46.

Table 5: 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

Related Documentation

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Example: Removing R7 Information Elements from GTP Messages on page 46
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Removing R7 Information Elements from GTP Messages

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to remove R7 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 R7 IEs from the GTP message.

Configuration

Step-by-Step Procedure

To remove R7 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 R7
   ```

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

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Supported R8 Information Elements

Supported Platforms SRX1500, SRX5400, SRX5600, vSRX

Junos OS supports all 3GPP R8 IEs for GTP, as listed in Table 6 on page 47.

Table 6: Supported Information Elements

IE Type Value	Information Element
189	RFSP Index

Related Documentation

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Example: Removing R8 Information Elements from GTP Messages on page 48
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11

- Supported GTP Message Types on page 24

Example: Removing R8 Information Elements from GTP Messages

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to remove R8 information elements from GTP messages.

- Requirements on page 48
- Overview on page 48
- Configuration on page 48
- Verification on page 48

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 R8 IEs from the GTP message.

Configuration

Step-by-Step Procedure

To remove R8 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 R8
   ```

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

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3

- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Supported R9 Information Elements

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Junos OS supports all 3GPP R9 IEs for GTP, as listed in Table 7 on page 49.

Table 7: 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)

Related Documentation

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Example: Removing R9 Information Elements from GTP Messages on page 49
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Removing R9 Information Elements from GTP Messages

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to remove R9 information elements from GTP messages.

- Requirements on page 50
- Overview on page 50

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 R9 IEs from the GTP message.

Configuration

Step-by-Step Procedure

To remove R9 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 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.

Related Documentation

- Understanding R6, R7, R8, and R9 Information Elements Removal on page 40
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Understanding GTPv1 Information Element Removal

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: The IE removal feature supports GTPv1 only.

Related Documentation

- Understanding GTP Information Elements on page 35
- Example: Removing GTPv1 Information Elements Using IE Number on page 51

Example: Removing GTPv1 Information Elements Using IE Number

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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

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.

Related Documentation

- Understanding GTP Information Elements on page 35
- Understanding GTPv1 Information Element Removal on page 50

CHAPTER 6

Configuring NAT for GTP

Understanding NAT for GTP

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: 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.

Related Documentation

- Understanding GTP IP Fragmentation on page 34
- Understanding GTP Inspection Objects on page 17
- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Configuring GTP Inspection in NAT

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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

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

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.

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Understanding GTP Message Filtering on page 21
- Supported GTP Message Types on page 24

Understanding Network Address Translation-Protocol Translation

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- GPRS Overview on page 3
- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Features Overview on page 112
- Example: Enhancing Traffic Engineering by Configuring NAT-PT Between an IPv4 and an IPv6 Endpoint with SCTP Multihoming on page 59

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

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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 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 3 on page 60 illustrates the network topology used in this example.

Figure 3: NAT-PT Between an IPv4 Endpoint and an IPv6 Endpoint

For configuring NAT-PT details between IPv4 and IPv6 endpoints, see Table 8 on page 60.

Table 8: Configuring NAT-PT Details Between IPv4 and IPv6 Endpoints

Endpoints	Address One	Address Two
A (IPv6)	2a.1.1.1/96	2c.3.3.3/96
B (IPv4)	2.2.2.2/24	4.4.4.4/34

Configuration

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 1.1.1.100/24
set interfaces ge-4/0/0 unit 0 family inet6 address 2a::1:1:100/96
set interfaces ge-4/0/1 unit 0 family inet address 2.2.2.100/24
set interfaces ge-4/0/1 unit 0 family inet6 address 2b::2:2:100/96
set interfaces ge-4/0/2 unit 0 family inet address 3.3.3.100/24
set interfaces ge-4/0/2 unit 0 family inet6 address 2c::3:3:100/96
set interfaces ge-4/0/3 unit 0 family inet address 4.4.4.100/24
set interfaces ge-4/0/3 unit 0 family inet6 address 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
  2b::2:2:2/128
set security nat static rule-set sctp-natpt-from-zone1 rule r1-dst then static-nat prefix
  2.2.2.2/32
set security nat static rule-set sctp-natpt-from-zone1 rule r3-dst match
  destination-address 2d::4:4:4/128
set security nat static rule-set sctp-natpt-from-zone1 rule r3-dst then static-nat prefix
  4.4.4.4/32
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 1.1.1.1/32
set security nat static rule-set sctp-natpt-from-zone2 rule r2-dst then static-nat prefix
  2a::1:1:1/128
set security nat static rule-set sctp-natpt-from-zone2 rule r4-dst match
  destination-address 3.3.3.3/32
set security nat static rule-set sctp-natpt-from-zone2 rule r4-dst then static-nat prefix
  2c::3:3:3/128
```

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 1.1.1.100/24
user@host# set ge-4/0/0 unit 0 family inet6 address 2a::1:1:100/96
user@host# set ge-4/0/1 unit 0 family inet address 2.2.2.100/24
user@host# set ge-4/0/1 unit 0 family inet6 address 2b::2:2:100/96
user@host# set ge-4/0/2 unit 0 family inet address 3.3.3.100/24
user@host# set ge-4/0/2 unit 0 family inet6 address 2c::3:3:100/96
user@host# set ge-4/0/3 unit 0 family inet address 4.4.4.100/24
user@host# set ge-4/0/3 unit 0 family inet6 address 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 2b::2:2:2/128
user@host# set static rule-set sctp-natpt-from-zone1 rule r1-dst then static-nat
  prefix 2.2.2.2/32
user@host# set static rule-set sctp-natpt-from-zone1 rule r3-dst match
  destination-address 2d::4:4:4/128
user@host# set static rule-set sctp-natpt-from-zone1 rule r3-dst then static-nat
  prefix 4.4.4.4/32
```

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 1.1.1.1/32
user@host# set static rule-set sctp-natpt-from-zone2 rule r2-dst then static-nat
  prefix 2a::1:1:1/128
user@host# set static rule-set sctp-natpt-from-zone2 rule r4-dst match
  destination-address 3.3.3.3/32
user@host# set static rule-set sctp-natpt-from-zone2 rule r4-dst then static-nat
  prefix 2c::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 1.1.1.100/24;
    }
    family inet6 {
      address 2a::1:1:100/96;
    }
  }
}
ge-4/0/1 {
  unit 0 {
    family inet {
      address 2.2.2.100/24;
    }
    family inet6 {
      address 2b::2:2:100/96;
    }
```

```
    }
  }
  ge-4/0/2 {
    unit 0 {
      family inet {
        address 3.3.3.100/24;
      }
      family inet6 {
        address 2c::3:3:100/96;
      }
    }
  }
  ge-4/0/3 {
    unit 0 {
      family inet {
        address 4.4.4.100/24;
      }
      family inet6 {
        address 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 2b::2:2:2/128;
      }
      then {
        static-nat {
          prefix {
            2.2.2.2/32;
          }
        }
      }
    }
    rule r3-dst {
      match {
        destination-address 2d::4:4:4/128;
      }
      then {
        static-nat {
          prefix {
            4.4.4.4/32;
          }
        }
      }
    }
  }
  rule-set sctp-natpt-from-zone2 {
    from zone sctp_zone2;
    rule r2-dst {
      match {
        destination-address 1.1.1.1/32;
      }
      then {
        static-nat {
          prefix {
            2a::1:1:1/128;
          }
        }
      }
    }
    rule r4-dst {
      match {
        destination-address 3.3.3.3/32;
      }
      then {
        static-nat {
          prefix {
            2c::3:3:3/128;
          }
        }
      }
    }
  }
```

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

Verification

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     : 2b::2:2:2
  Host addresses            : 2.2.2.2
  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     : 2d::4:4:4
  Host addresses            : 4.4.4.4
  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     : 1.1.1.1
  Host addresses            : 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     : 3.3.3.3
  Host addresses            : 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

- Understanding Network Address Translation-Protocol Translation on page 58

CHAPTER 7

Configuring GGSN

Understanding GGSN Redirection

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

GGSN Pooling Scenarios Overview

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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 on page 68
- Understanding GGSN Pooling for Scenario 2 on page 69

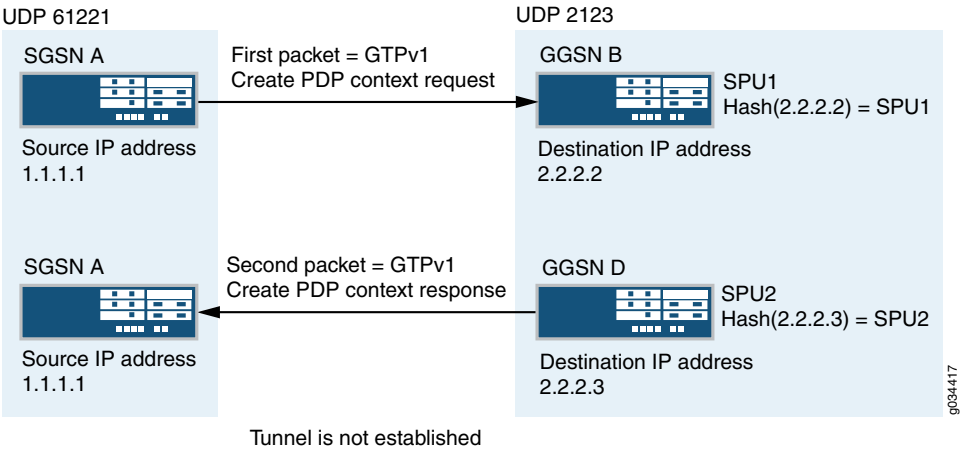
Understanding GGSN Pooling for Scenario 1

In Figure 4 on page 68, 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 4: GGSN Pooling Scenario 1



NOTE: SPU2 cannot retrieve request information from SPU1.

Install Request Information to Remote SPU

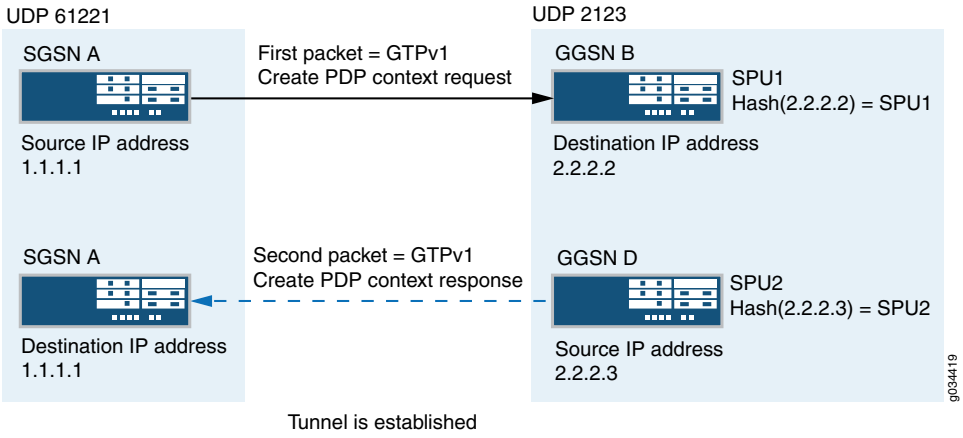
In this scenario, the PDP response packet was dropped because of a lack of request information, and the GTP tunnel was not established. This can be resolved by installing the request information on the correct SPU.

In Figure 5 on page 69, 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 (1.1.1.1) = 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 5: 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. See the following examples:

- Example: Configuring a GGSN Custom Policy on page 71
- Example: Configuring Custom Applications on page 74

Understanding GGSN Pooling for Scenario 2

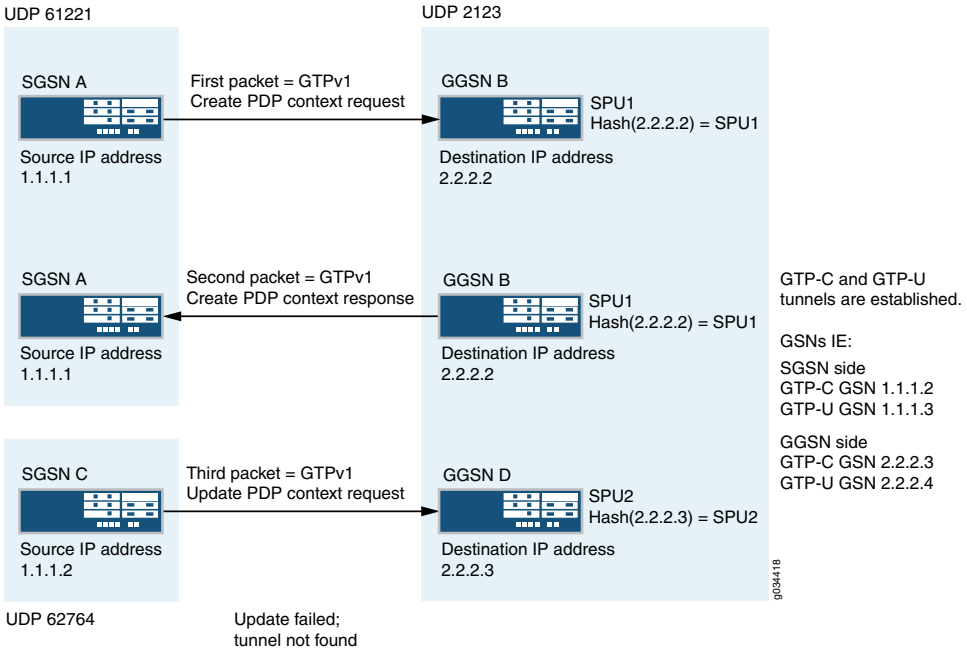
In Figure 6 on page 70, a packet data protocol (PDP) context request is sent from SGSN A to GGSN B during a GTP tunnel creation procedure. After receiving the PDP context request message, GGSN B sends the PDP context response message to SGSN A. After receiving the PDP context response message, the GTP-C 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 1.1.1.2 and the GTP-U is established on data IP 1.1.1.3. Likewise, the response message sent from GGSN indicates that GTP-C is established on control IP 2.2.2.3 and GTP-U is established on data IP 2.2.2.4.

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 6: GGSN Pooling Scenario 2



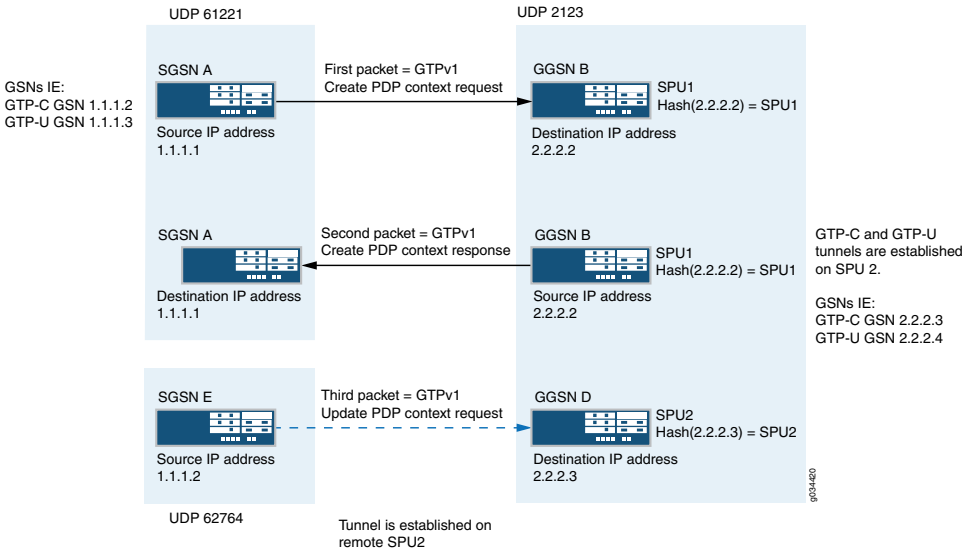
Install Tunnel Information to Remote SPU

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 7 on page 71, 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 7: Functionality : GGSN Pooling Scenario 2



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

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTP on page 11
- Supported GTP Message Types on page 24

Example: Configuring a GGSN Custom Policy

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to configure a Gateway GPRS Support Node (GGSN) custom policy 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

Before you begin, you should be familiar with GGSN pooling scenarios. See "GGSN Pooling Scenarios Overview" on page 67.

Overview

In this example, you set security zones from zone ggsn and to zone sgsn. Next you set the GGSN policy name to ggsn-pool-g2s. You set the name of the match source address to ggsn-1 and the match destination address to sgsn-1.

Then you set the port based application to src_2123 and src_3386. You set the action type to permit. Then you set the application services name to gprs-gtp-profile and the GTP profile name to test. Finally, you set the default policy name to deny-all.

Configuration

Configuring a GGSN Custom Policy

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 policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s
set security policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
  source-address ggsn-1
set security policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
  destination-address sgsn-1
set security policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match application
  src_2123
set security policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match application
  src_3386
set security policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s then permit
  application-services gprs-gtp-profile test
set security policies default-policy deny-all
```

Step-by-Step Procedure

To configure a GGSN custom policy:

1. Configure the GGSN custom policy.

   ```
   [edit security ]
   user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s
   ```

2. Configure the source address.

   ```
   [edit security]
   user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
     source-address ggsn-1
   ```

3. Configure the destination address.

   ```
   [edit security]
   user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
     destination-address sgsn-1
   ```

4. Configure the policy applications.

```
[edit security]
user@host#set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
  application src_2123
user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s match
  application src_3386
```

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

```
[edit security]
user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s then
  permit
user@host# set policies from-zone ggsn to-zone sgsn policy ggsn-pool-g2s then
  permit application-services gprs-gtp-profile test
```

6. Configure the default policy.

```
[edit security]
user@host#  set policies default-policy deny-all
```

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 zone-name to-zone zone-name {
    from-zone ggsn to-zone sgsn {
      policy ggsn-pool-g2s {
        match {
          source-address ggsn-1;
          destination-address sgsn-1;
          application [ src_2123 src_3386 ];
        }
        then {
          permit {
            application-services {
              gprs-gtp-profile test;
            }
          }
        }
      }
      }
    }
    default-policy {
      deny-all;
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying the Configuration on page 74

Verifying the Configuration

Purpose Verify that the GGSN custom policy configuration is correct.

Action From operational mode, enter the **show security** command.

Sample Output

```
user@host>show security policies
From zone: sgsn, To zone: ggsn
  Policy: ggsn-pool-g2s, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
    Source addresses: ggsn1
    Destination addresses: sgsn1
    Applications: src_2123 src_3386
    Action: permit, application services: gprs-gtp-profile test
    Default policy: Deny-all
```

This output shows a summary of policy configuration.

Related Documentation

- Example: Configuring Custom Applications on page 74
- GGSN Pooling Scenarios Overview on page 67

Example: Configuring Custom Applications

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to configure custom applications to support GGSN pooling scenario 1.

- Requirements on page 74
- Overview on page 75
- Configuration on page 75

Requirements

This example uses the following hardware and software components:

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

Before you begin, configure the required GGSN policy. See "Example: Configuring a GGSN Custom Policy" on page 71.

Overview

In this example, you create applications src_2123 and src_3386 to identify source ports 2123 and 3386 for both TCP and UDP.

First you configure a custom application called src_2123.You set the application protocol to gprs-gtp-c. Then you set the networking protocol type to UDP. You set the source port to 2123 and the destination port to 0-0.

Then you configure another custom application called src_3386. You set the application protocol to gprs-gtp-v0. Then you set the networking protocol type to UDP. Finally, you set the source port to 3386 and the destination port to 0-0.

Configuration

Configuring Custom Applications

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 src_2123 application-protocol gprs-gtp-c
set applications application src_2123 protocol udp
set applications application src_2123 source-port 2123
set applications application src_2123 destination-port 0-0
set applications application src_3386 application-protocol gprs-gtp-v0
set applications application src_3386 protocol udp
set applications application src_3386 source-port 3386
set applications application src_3386 destination-port 0-0
```

Step-by-Step Procedure

To configure custom policy applications:

1. Configure the first custom application and application protocol name.

   ```
   [edit applications]
   user@host# set application src_2123 application-protocol gprs-gtp-c
   ```

2. Configure the networking protocol type.

   ```
   [edit applications]
   user@host# set application src_2123 protocol udp
   ```

3. Configure the source port number.

   ```
   [edit applications]
   user@host#set application src_2123 source-port 2123
   ```

4. Configure the TCP or UDP destination port number.

   ```
   [edit applications]
   ```

```
user@host# set application src_2123 destination-port 0-0
```

5. Configure the second custom application and application protocol name.

```
[edit applications]
user@host# set application src_3386 application-protocol gprs-gtp-v0
```

6. Configure the networking protocol type.

```
[edit applications]
user@host# set application src_3386 protocol udp
```

7. Configure the source port number.

```
[edit applications]
user@host#  set application src_3386 source-port 3386
```

8. Configure the destination port number.

```
[edit applications]
user@host# set application src_3386 destination-port 0-0
```

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

```
[edit]
user@host# show applications
  application src_2123 {
    application-protocol gprs-gtp-c;
    protocol udp;
    source-port 2123;
    destination-port 0-0;
  }
  application src_3386 {
    application-protocol gprs-gtp-v0;
    protocol udp;
    source-port 3386;
    destination-port 0-0;
  }
```

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

Related Documentation

- Example: Configuring a GGSN Custom Policy on page 71
- GGSN Pooling Scenarios Overview on page 67

PART 3

Configuring GPRS Tunnel Protocol v2

CHAPTER 8

Configuring GTPv2

Understanding GTPv2

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

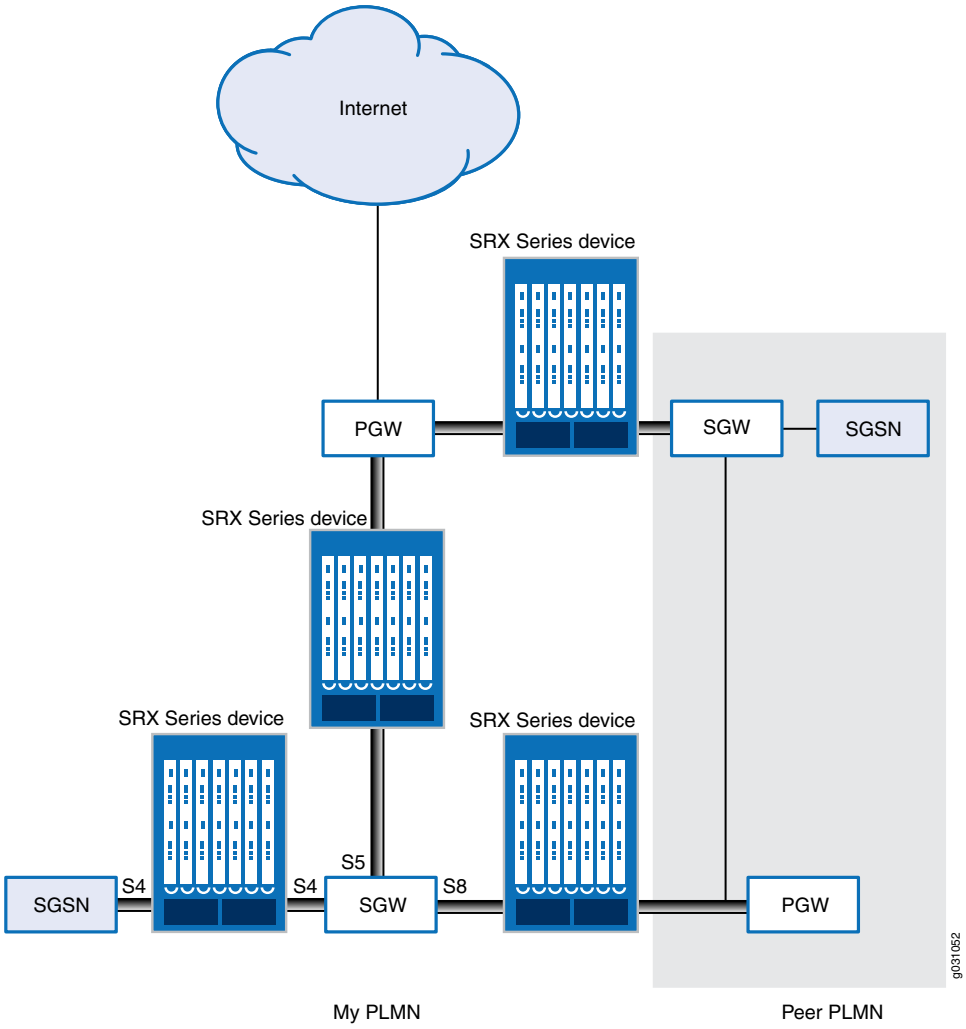
The GPRS tunneling protocol (GTP) establishes a GTP tunnel between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) for individual Mobile Stations (MS). In previous releases, only GTP version 0 (GTPv0) and GTP version 1 (GTPv1) were deployed. GTP version 2 (GTPv2) is implemented in the Junos operating system (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 8 on page 80 shows the following LTE interfaces where SRX Series devices are deployed in the public land mobile network (PLMN).

Figure 8: 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.

Related Documentation

- GPRS Overview on page 3
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Understanding Policy-Based GTPv2

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: **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.

Related Documentation

- Example: Enabling GTPv2 Inspection in Policies on page 81
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Example: Enabling GTPv2 Inspection in Policies

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to enable GTPv2 inspection in policies.

- Requirements on page 82
- Overview on page 82

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

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

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.

Related Documentation

- Understanding Policy-Based GTPv2 on page 81
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Understanding GTP Path Restart

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Example: Restarting a GTPv2 Path on page 85
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91
- Understanding GTPv2 Information Elements on page 101

Example: Restarting a GTPv2 Path

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to restart a GTPv2 path.

Requirements

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

Overview

NOTE: **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

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

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

Related Documentation

- Understanding GTP Path Restart on page 84
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91
- Understanding GTPv2 Information Elements on page 101

Understanding GTPv2 Tunnel Cleanup

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Example: Setting the Timeout Value for GTPv2 Tunnels on page 87
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

Example: Setting the Timeout Value for GTPv2 Tunnels

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

- Requirements on page 87
- Overview on page 87
- Configuration on page 87
- Verification on page 88

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

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

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

Related Documentation

- Understanding GTPv2 Tunnel Cleanup on page 86
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

Understanding GTPv2 Traffic Logging

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Example: Enabling GTPv2 Traffic Logging on page 89
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91
- Understanding GTPv2 Information Elements on page 101

Example: Enabling GTPv2 Traffic Logging

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

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

- Understanding GTPv2 Traffic Logging on page 88
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81

CHAPTER 9

Configuring GTPv2 Message Filtering

Understanding GTPv2 Message Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

When a device receives a GPRS tunneling protocol version 2 (GTPv2) packet, it checks the packet against GTPv2 policies configured on the device. If the packet matches a policy, then the device inspects the packet based on the GTPv2 inspection object applied to the policy. If the packet fails to match any of the configuration parameters, it is dropped. If the packet matches all the configuration parameters, it is forwarded.

Related Documentation

- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message-Length Filtering on page 96
- Understanding GTPv2 Message-Type Filtering on page 98
- Supported GTPv2 Message Types on page 91

Supported GTPv2 Message Types

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Table 9 on page 92 lists the message types supported in GTPv2. You can use these message types to configure GTPv2 message-type filtering.

Table 9: GTPv2 Messages

Message	Message Type
bearer resource command	bearer-resource
bearer resource failure	bearer-resource
change notification request	change-notification
change notification response	change-notification
context request	context
context response	context
context acknowledgement	context
configuration transfer tunnel	config-transfer
create bearer request	create-bearer
create bearer response	create-bearer
create indirect data forwarding tunnel request	create-data-forwarding
create indirect data forwarding tunnel response	create-data-forwarding
create forwarding tunnel request	create-tnl-forwarding
create forwarding tunnel response	create-tnl-forwarding
create session request	create-session
create session response	create-session
CS paging indication	cs-paging
delete bearer request	delete-bearer
delete bearer response	delete-bearer
delete bearer command	delete-command
delete bearer failure	delete-command
delete indirect data forwarding tunnel request	delete-data-forwarding

Table 9: GTPv2 Messages *(continued)*

Message	Message Type
delete indirect data forwarding tunnel response	delete-data-forwarding
delete PDN connection set request	delete-pdn
delete PDN connection set response	delete-pdn
delete session request	delete-session
delete session response	delete-session
detach notification	detach
detach acknowledgement	detach
downlink data notification	downlink-notification
downlink data acknowledgement	downlink-notification
downlink data notification failure	downlink-notification
echo request	echo
echo response	echo
forward access context notification	fwd-access
forward access context acknowledgement	fwd-access
forward relocation request	fwd-relocation
forward relocation response	fwd-relocation
forward relocation complete	fwd-relocation
forward relocation acknowledgement	fwd-relocation
identification request	identification
identification response	identification
MBMS session start request	mbms-sess-start
MBMS session start response	mbms-sess-start
MBMS session stop request	mbms-sess-stop
MBMS session stop response	mbms-sess-stop

Table 9: GTPv2 Messages *(continued)*

Message	Message Type
MBMS session update request	mbms-sess-update
MBMS session update response	mbms-sess-update
modify bearer request	modify-bearer
modify bearer response	modify-bearer
modify bearer command	modify-command
modify bearer failure	modify-command
release access-bearer request	release-access
release access-bearer response	release-access
relocation cancel request	relocation-cancel
relocation cancel response	relocation-cancel
resume notification	resume
resume acknowledgement	resume
stop paging indication	stop-paging
suspend notification	suspend
suspend acknowledgement	suspend
trace session activation	trace-session
trace session deactivation	trace-session
update bearer request	update-bearer
update bearer response	update-bearer
update PDN connection set request	update-pdn
update PDN connection set response	update-pdn
version not supported	ver-not-supported

Related Documentation

- Understanding GTPv2 Message Filtering on page 91

- Understanding GTPv2 Message-Type Filtering on page 98
- Example: Permitting and Denying GTPv2 Message Types on page 95s
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTP Message Types on page 24

Example: Permitting and Denying GTPv2 Message Types

Supported Platforms SRX Series, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to permit and deny GTPv2 message types.

- Requirements on page 95
- Overview on page 95
- Configuration on page 95
- Verification on page 96

Requirements

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

Overview

In this example, for the gtp2 profile, you configure the device to drop the echo and create-session message types for version 2.

Configuration

Step-by-Step Procedure To permit and deny GTPv2 message types:

1. Specify the GTPv2 profile.

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

2. Drop the echo messages for version 2.

   ```
   [edit]
   user@host# set security gprs gtp profile gtp2 drop echo 2
   ```

3. Drop the create-session messages for version 2.

   ```
   [edit]
   user@host# set security gprs gtp profile gtp2 drop create-session 2
   ```

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.

Related Documentation

- Understanding GTPv2 Message-Type Filtering on page 98
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Understanding GTPv2 Message-Length Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

You can configure a device to drop GPRS tunneling protocol version 2 (GTPv2) packets that do not meet the specified minimum or maximum message lengths. In the GTPv2 header, the message length field indicates the length, in octets, of the GTPv2 payload. The message length does not include the length of the GTPv2 header itself, the UDP header, the TCP header, or the IP header.

The default minimum and maximum GTPv2 message lengths are 0 and 65,535 bytes, respectively. Therefore, you can specify the GTPv2 message length range from 0 to 65,535 bytes.

Related Documentation

- Example: Setting GTPv2 Message Lengths on page 96
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Example: Setting GTPv2 Message Lengths

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to set GTPv2 message lengths.

Requirements

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

Overview

In this example, you configure the minimum GTPv2 message length to 10 octets and the maximum GTPv2 message length to 1500 octets for the GTPv2 inspection object named gtp2.

Configuration

Step-by-Step Procedure

To configure GTPv2 message lengths:

1. Specify the GTPv2 profile.

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

2. Specify the minimum message length.

   ```
   [edit]
   user@host# set security gprs gtp profile gtp2 min-message-length 10
   ```

3. Specify the maximum message length.

   ```
   [edit]
   user@host# set security gprs gtp profile gtp2 max-message-length 1500
   ```

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.

Related Documentation

- Understanding GTPv2 Message-Length Filtering on page 96
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81

- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

Understanding GTPv2 Message-Type Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

You can configure a device to filter GPRS tunneling protocol version 2 (GTPv2) packets based on their message types. By default, the device permits all GTPv2 message types.

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.

You can use the **set security gprs gtp profile profile name drop message-type number** configuration statement to discard GTPv2 message types. If the version number is not mentioned, message types for all versions are discarded. If a configured message type is not valid for the particular GTP version, the specific configuration does not take effect.

NOTE: **Message types valid for GTP version 1 (GTPv1) might not be valid for GTPv2, and vice versa.**

A GTPv2 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 message type. For example, if you drop the identification message type, then you automatically drop the identification-request and identification-response messages. Also, if you drop the create-pdp message type for version 2, then only the create-pdp-request and create-pdp-response messages for version 2 are dropped.

Related Documentation

- Example: Permitting and Denying GTPv2 Message Types on page 95
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Understanding GTPv2 Message-Rate Limiting

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

You can configure a device to limit the rate of control traffic going to GPRS tunneling protocol version 2 (GTPv2) gateways. GTPv2 gateways are important resources in a public land mobile network (PLMN) and require protection. You can use the **set security**

gprs gtp profile name rate-limit messages per second configuration statement to limit the rate of control traffic to the GTPv2 gateways.

Related Documentation

- Example: Limiting the GTPv2 Message Rate on page 99
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

Example: Limiting the GTPv2 Message Rate

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to limit the GTPv2 message rate.

- Requirements on page 99
- Overview on page 99
- Configuration on page 99
- Verification on page 100

Requirements

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

Overview

In this example, you limit the rate of incoming GTPv2 messages to 200 packets per second to any GTPv2 gateway.

Configuration

Step-by-Step Procedure To configure the GTPv2 message rate limit:

1. Specify the GTPv2 profile.

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

2. Set the rate limit.

   ```
   [edit]
   user@host# set security gprs gtp profile gtp2 rate-limit 200
   ```

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

- Understanding GTPv2 Message-Rate Limiting on page 98
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Understanding GTPv2 Message Filtering on page 91
- Supported GTPv2 Message Types on page 91

CHAPTER 10

GTPv2 Information Elements Overview

Understanding GTPv2 Information Elements

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

Understanding GTPv2 IMSI Prefix and APN Filtering

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: 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.

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

Related Documentation

- Example: Setting a Combined IMSI Prefix and APN Filter on page 39
- Understanding GTPv2 Information Elements on page 101
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

Example: Setting a Combined GTPv2 IMSI Prefix and APN Filter

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

This example shows how to set a combined GTPv2 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.mcc789.gprs as an APN and use the wildcard (*). You set the selection mode as network for this APN. You also set the IMSI prefix as 123678.

Configuration

Step-by-Step Procedure

To set the combined IMSI prefix and APN filter:

1. Specify the GTPv2 profile.

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

2. Set the selection mode for the APN.

```
[edit]
user@host# set security gprs gtp profile gtp2 apn
   *example.com.mnc123.mcc789.gprs imsi-prefix 123678 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.

Related Documentation

- Understanding GTPv2 IMSI Prefix and APN Filtering on page 101
- Understanding GTPv2 Information Elements on page 101
- GPRS Overview on page 3
- Understanding GTPv2 on page 79
- Understanding Policy-Based GTPv2 on page 81
- Example: Enabling GTPv2 Inspection in Policies on page 81
- Supported GTPv2 Message Types on page 91

PART 4

Configuring Stream Control Transmission Protocol

CHAPTER 11

Configuring SCTP

Understanding Stream Control Transmission Protocol

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

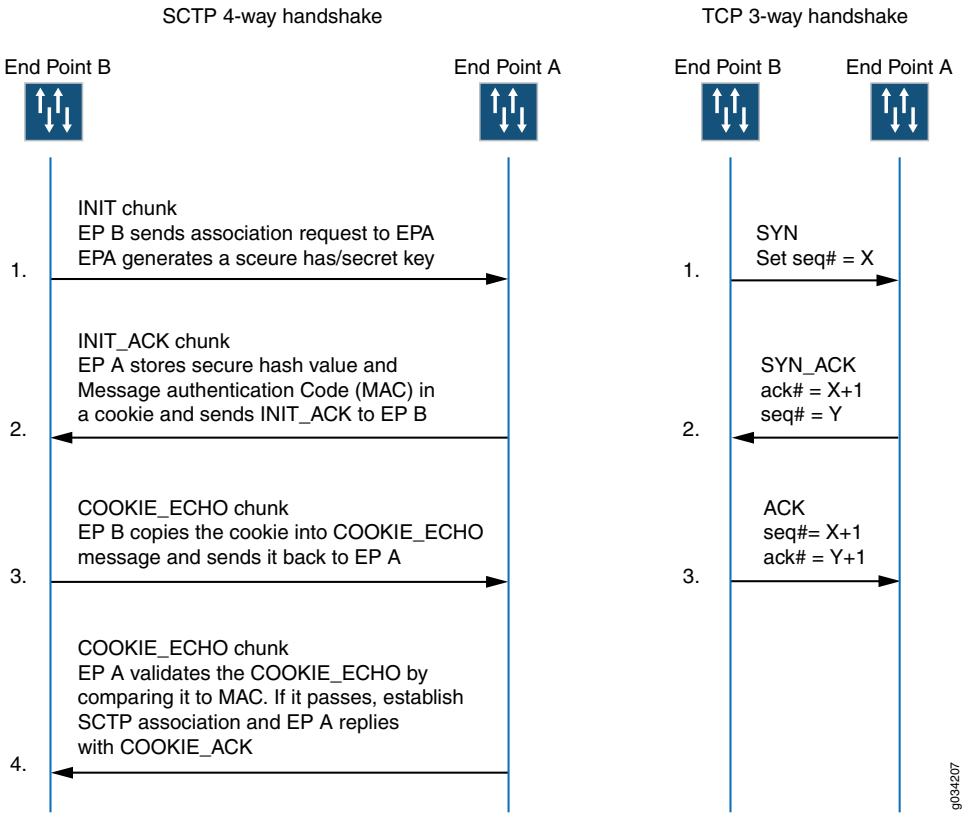
Stream Control Transmission Protocol (SCTP) is an IP Transport Layer protocol. SCTP exists at an equivalent level with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), which provides transport layer functions to many Internet applications. SCTP is a reliable transport protocol operating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

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 9 on page 108 illustrates the SCTP 4-way handshake and TCP 3-way handshake.

Figure 9: SCTP 4-way Handshake and TCP 3-way Handshake



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 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

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).

Release History Table

Release	Description
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

- SCTP Configuration Overview on page 118
- SCTP Packet Structure Overview on page 116
- SCTP Features Overview on page 112
- Understanding SCTP Behavior in Chassis Cluster on page 113

SCTP Features Overview

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Packet Structure Overview on page 116
- Understanding SCTP Behavior in Chassis Cluster on page 113
- Example: Configuring a Security Policy to Permit or Deny SCTP Traffic on page 121

Understanding Central Point Architecture Support for SCTP

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

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.

Related Documentation

- *Understanding Enhancements to Central Point Architecture for the SRX5000 Line*

Understanding SCTP Behavior in Chassis Cluster

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE:

- 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.

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Packet Structure Overview on page 116
- SCTP Features Overview on page 112

Understanding SCTP Multihoming

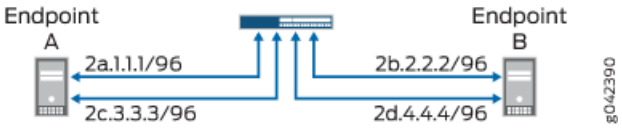
Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

A Stream Control Transmission Protocol (SCTP) endpoint can be a multihomed host with either all IPv4 addresses or all IPv6 addresses. In Figure 10 on page 115, endpoint A is connected to an SRX Series device with two IPv4 addresses, and endpoint B is connected to an SRX Series device 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 10: SCTP Multihoming with Two IPv4 Endpoints

In Figure 11 on page 115, endpoint A is connected to an SRX Series device with two IPv6 addresses, and endpoint B is connected to an SRX Series device 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 11: SCTP Multihoming with Two IPv6 Endpoints



Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Features Overview on page 112
- Understanding Network Address Translation-Protocol Translation on page 58

Understanding SCTP Multichunk Inspection

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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.

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Packet Structure Overview on page 116

SCTP Packet Structure Overview

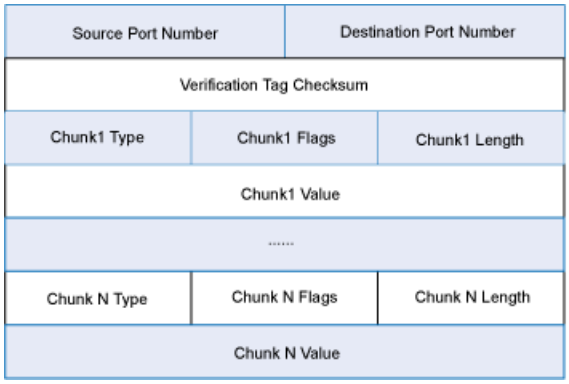
Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

An SCTP packet consists of the following sections:

- Common header section
- Data chunk section

Figure 12 on page 117 illustrates the structure of the SCTP packet.

Figure 12: 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 10 on page 117 describes the fields in the common header section:

Table 10: 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—This section occupies the remaining portion of the packet. Table 11 on page 117 describes the fields in the data chunk section:

Table 11: 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.

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

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Features Overview on page 112
- Understanding SCTP Behavior in Chassis Cluster on page 113

SCTP Configuration Overview

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

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

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Packet Structure Overview on page 116
- SCTP Features Overview on page 112
- Understanding SCTP Behavior in Chassis Cluster on page 113
- Example: Configuring a Security Policy to Permit or Deny SCTP Traffic on page 121

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

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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.

NOTE: 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

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.

NOTE: 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

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

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Packet Structure Overview on page 116
- SCTP Features Overview on page 112
- Understanding SCTP Behavior in Chassis Cluster on page 113
- Example: Configuring a Security Policy to Permit or Deny SCTP Traffic on page 121

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

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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 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 118.

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.

NOTE: 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:

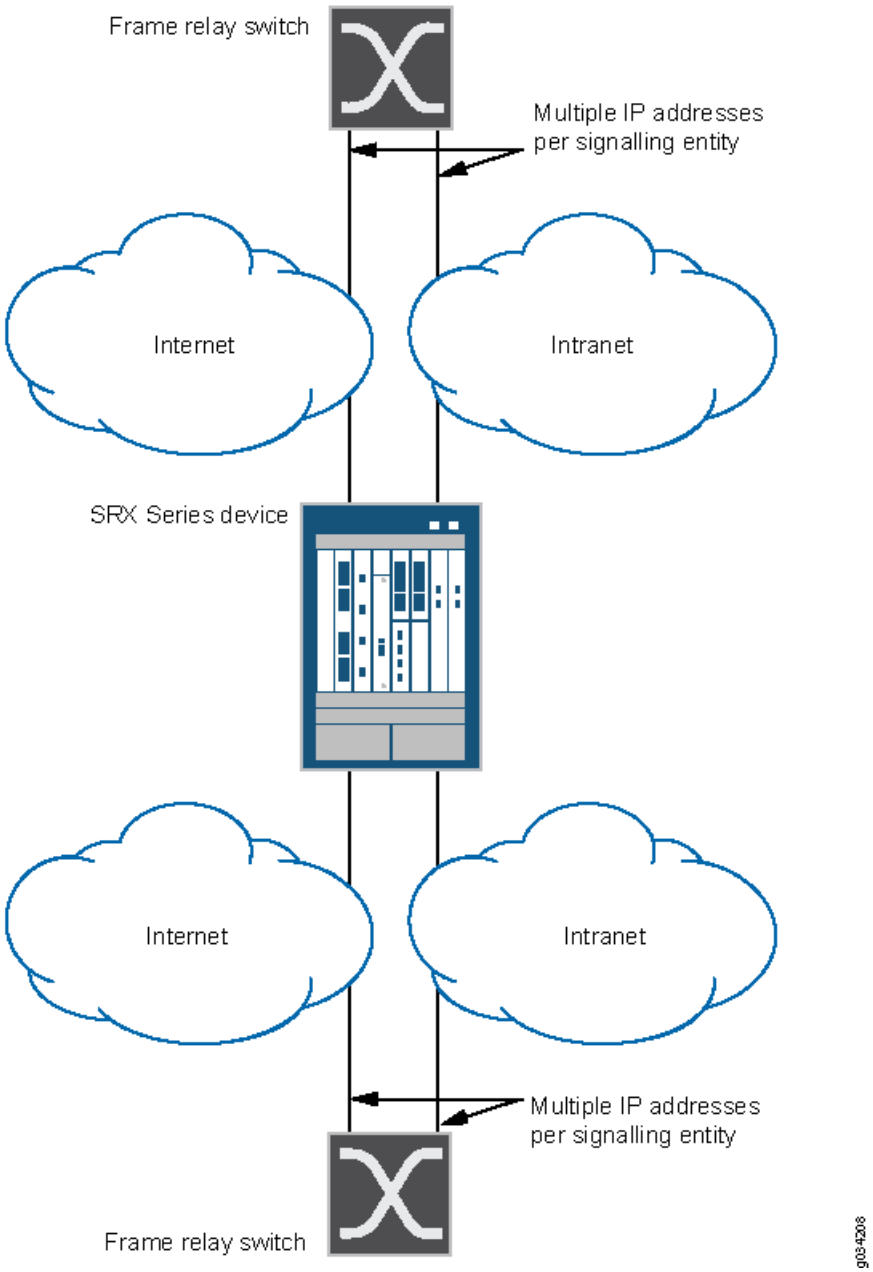
- Uneven hash results on the association ports pairs.
- The number of port pairs is less than, or not much greater than, the number of SPUs.

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 10.1.1.1/32 in the trust zone to the untrust zone with the SCTP configuration specified in the roam2att profile.

Figure 13 on page 123 shows the SCTP firewall implementation.

Figure 13: SCTP Firewall Implementation



Configuration

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 untrust zone to the trust zone.

```
[edit security policies from-zone untrust to-zone trust]
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

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**

Related Documentation

- Understanding Stream Control Transmission Protocol on page 107
- SCTP Configuration Overview on page 118
- SCTP Packet Structure Overview on page 116
- SCTP Features Overview on page 112
- Understanding SCTP Behavior in Chassis Cluster on page 113

PART 5

Configuration Statements and Operational Commands

CHAPTER 12

Configuration Statements

action (APN GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
action {
  drop;
  pass;
  selection (ms|net|vrf);
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* apn *pattern-string* mcc-mnc *mcc-mnc-number*]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure GTP profile access point (AP) name filtering action to allow or deny access to specific access points.

Options

- **drop**—Specify to deny GTP packets from all selection modes for the specified access points.
- **pass**—Specify to permit GTP packets from all selection modes for the access points.
- **selection**—Specify one of the following selection modes for the access points:
  - **ms**—The access point name is provided by a mobile station, and the user-subscription is not verified.
  - **net**—The access point name is provided by a network, and the user subscription is not verified.
  - **vrf**— The access point name is provided by a network or an MS, and the user-subscription is verified.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

alarm-threshold (Security GPRS)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
alarm-threshold {
    forward number;
    reverse number;
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type (create-req | delete-req | echo-req | other)]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify an alarm threshold for path rate limit.

Options *number*—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

apn

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
apn pattern-string {
  imsi-prefix imsi-prefix-digits {
    action {
      drop;
      pass;
      selection (ms|net|vrf);
    }
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4. Option mcc-mnc replaced with imsi-prefix in Junos OS Release 12.1X44-D10.

Description Allow or deny access to specific access point names (APNs).

Options

- *pattern-string*—Set an APN suffix, such as “example.net.mcc123.mnc456.gprs”.
- *imsi-prefix-digits*—Specify an IMSI prefix.
- **drop**—Specify to deny GTP packets from all selection modes for the APN.
- **pass**—Specify to permit GTP packets from all selection modes for the APN.
- **selection**—Specify one of the following selection modes for the APN:
  - **ms**—The APN is provided by a Mobile Station (MS), and the user-subscription is not verified.
  - **net**—The APN is provided by a network, and the user-subscription is not verified.
  - **vrf**—The APN is provided by a network or an MS, and the user-subscription is verified.

NOTE: Because APN filtering is based on a perfect match, using the wildcard (*) when setting an APN suffix can prevent the inadvertent exclusion of APNs you would otherwise authorize. The security device automatically denies all other APNs that do not match, if the action is pass. You can only use the wildcard as the first character in the APN string.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

application-services (Security Forwarding Process)

Supported Platforms SRX Series, vSRX

Syntax

```
application-services {
  enable-gtpu-distribution;
  maximize-alg-sessions;
  maximize-idp-sessions {
    weight (equal | firewall | idp);
  }
  packet-ordering-mode {
    (hardware | software);
  }
}
```

Hierarchy Level [edit security forwarding-process]

Release Information Statement introduced in Junos OS Release 9.6. Statement updated in Junos OS Release 10.4. Statement updated in Junos OS Release 15.1X49-D40 with the **enable-gtpu-distribution** option.

Description You can configure SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices to switch from an integrated firewall mode to maximize intrusion detection and prevention (IDP) mode to increase the capacity of IDP processing with the **maximize-idp-sessions** option. When you maximize IDP, you are decoupling IDP processes from firewall processes, allowing the device to support the same number of firewall and IDP sessions.

You can configure maximum Application Layer Gateway (ALG) sessions by using the **maximize-alg-sessions** option. By default, the session capacity number for Real-Time Streaming Protocol (RTSP), FTP, and Trivial File Transfer Protocol (TFTP) ALG sessions is 10,000 per flow Services Processing Unit (SPU). You must reboot the device (and its peer in chassis cluster mode) for the configuration to take effect. The **maximize-alg-sessions** option now enables you to increase defaults as follows:

- RTSP, FTP, and TFTP ALG session capacity: 25,000 per flow SPU
- TCP proxy connection capacity: 40,000 per flow SPU

NOTE: **Flow session capacity is reduced to half per flow SPU; therefore the aforementioned capacity numbers will not change on central point flow.**

Options The remaining statements are explained separately. See the CLI Explorer.

Required Privilege Level security—To view this in the configuration.
security-control—To add this to the configuration.

Related Documentation
- *Juniper Networks Devices Processing Overview*

association-timeout

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax association-timeout *time-in-minutes*;

Hierarchy Level [edit security gprs sctp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.2. The association timeout range increased in Junos OS Release 12.1X45-D10.

Description Set the association timeout for Stream Control Transmission Protocol (SCTP).

Options ***time-in-minutes***—Number of minutes of association time that elapse before the session is terminated.

Range: 10 through 6000 (100 hours).

Default: 300 minutes (5 hours).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

create-req

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
create-req {
  alarm-threshold {
    forward number;
    reverse number;
  }
  drop-threshold {
    forward number;
    reverse number;
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit the number of packets per second for GTP create request.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

delete-req

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
delete-req {
  alarm-threshold {
    forward number;
    reverse number;
  }
  drop-threshold {
    forward number;
    reverse number;
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit the number of packets per second for GTP delete request.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

drop (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
drop {
    aa-create-pdp (0 | 1 | 2 | all);
    aa-delete-pdp (0 | 1 | 2 | all);
    bearer-resource (0 | 1 | 2 | all);
    change-notification (0 | 1 | 2 | all);
    config-transfer (0 | 1 | 2 | all);
    context (0 | 1 | 2 | all);
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
```

```
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
    ver-not-supported (0 | 1 | 2 | all);
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. New GTP message types added in Junos OS Release 11.4. Support for GTPv2 added in Junos OS Release 11.4

Description Drop GTP message types. Specify **All** to drop messages for all GTP versions. Specify **0**, **1**, or **2** to drop messages for GTP versions 0, 1, or 2, respectively.

Options The following lists CLI keywords that each represent a GTP message type.

You must specify *(0 | 1 | 2 | all)* to specify the GTP release version number for the specified message type. The possible versions are 0, 1, 2, or all.

NOTE: A GTP message type includes one or many messages. When you drop a message type, you automatically drop all messages of the specified type.

- **aa-create-pdp** —Represents Create AA PDP Context Request and Create AA PDP Context Response messages.
- **aa-delete-pdp** —Represents Delete AA PDP Context Request and Delete AA PDP Context Response messages.
- **bearer-resource**—Represents Bearer Resource Command and Bearer Resource Failure messages.

- **change-notification**—Represents Change Notification Request and Change Notification Response messages.
- **context**—Represents Context Request and Context Response messages.
- **config-transfer**—Represents Configuration Transfer Tunnel messages.
- **create-bearer**—Represents Create Bearer Request and Create Bearer Response messages.
- **create-data-forwarding**—Represents Create Indirect Data Forwarding Request and Create Indirect Data Forwarding Response messages.
- **create-tnl-forwarding**—Represents Create Forwarding Tunnel Request and Create Forwarding Tunnel Response messages.

- **create-pdp**—Represents Create PDP Context Request and Create PDP Context Response messages.
- **create-session**—Represents Create Session Request and Create Session Response messages.
- **cs-paging**—Represents CS Paging Indication messages.
- **data-record**—Represents Data Record Request and Data Record Response messages.
- **delete-bearer**—Represents Delete Bearer Request and Delete Bearer Response messages.
- **delete-command**—Represents Delete Bearer Command and Delete Bearer Failure messages.
- **delete-data-forwarding**—Represents Delete Indirect Data Forwarding Request and Delete Indirect Data Forwarding Response messages.
- **delete-pdn**—Represents Delete PDN Connection Set Request and Delete PDN Connection Set Response messages.
- **delete-pdp**—Represents Delete PDP Context Request and Delete PDP Context Response messages.
- **delete-session**—Represents Delete Session Request and Delete Session Response messages.
- **detach**—Represents Detach Notification and Detach Acknowledgement messages.
- **downlink-notification**—Represents Downlink Data Notification, Downlink Data Acknowledgement, and Downlink Data Notification Failure Indication messages.
- **echo**—Represents Echo Request and Echo Response messages.
- **error-indication**—Represents Error Indication messages.
- **failure-report**—Represents Failure Report Request and Failure Report Response messages.
- **fwd-access**—Represents Forward Access Context Notification and Forward Access Context Acknowledgment messages.
- **fwd-relocation**—Represents Forward Relocation Request, Forward Relocation Response, Forward Relocation Complete, and Forward Relocation Complete Acknowledge messages.
- **fwd-srns-context**—Represents Forward SRNS Context Request and Forward SRNS Context Response messages.
- **g-pdu**—Represents G-PDU and T-PDU messages.
- **identification**—Represents Identification Request and Identification Response messages.
- **mbms-sess-start**—Represents MBMS Session Start Request and MBMS Session Start Response messages.
- **mbms-sess-stop**—Represents MBMS Session Stop Request and MBMS Session Stop Response messages.

- **mbms-sess-update**—Represents MBMS Session Update Request and MBMS Session Update Response messages.
- **modify-bearer**—Represents Modify Bearer Request and Modify Bearer Response messages.
- **modify-command**—Represents Modify Bearer Command and Modify Bearer Failure messages.
- **node-alive**—Represents Node Alive Request and Node Alive Response messages.
- **note-ms-present**—Represents Note MS GPRS Present Request and Note MS GPRS Present Response messages.
- **pdu-notification**—Represents PDU Notification request and PDU Notification response messages.
- **ran-info**—Represents Ran Info Relay messages.
- **redirection**—Represents Redirection Request and Redirection Response messages.
- **relocation-cancel**—Represents Relocations Cancel Request and Relocation Cancel Response messages.
- **resume**—Represents Resume Notification and Resume Acknowledgement messages.
- **send-route**—Represents Send Route Info Request and Send Route Info Response messages.
- **sgsn-context**—Represents SGSN Context Request and SGSN Context Response messages.
- **stop-paging**—Represents Stop Paging Indication messages.
- **supported-extension**—Represents Supported Extension Headers Notification messages.
- **suspend**—Represents Suspend Notification and Suspend Acknowledgement messages.
- **trace-session**—Represents Trace Session Activation and Trace Session Deactivation messages.
- **update-bearer**—Represents Update Bearer Request and Update Bearer Response messages.
- **update-pdn**—Represents Update PDN Set Connection Request and PDN Set Connection Response messages.
- **update-pdp**—Represents Update PDP Request and Update PDP Response messages.
- **ver-not-supported**—Represents Version Not Supported messages.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

drop (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
drop {
  m3ua-service {
    isup;
    sccp;
    tup;
  }
  payload-protocol {
    id;
    all;
    asap;
    bicc;
    ddp-segment;
    ddp-stream;
    diameter-dtls;
    diameter-sctp;
    dua;
    enrp;
    h248;
    h323;
    iua;
    m2pa;
    m2ua;
    m3ua;
    qipc;
    reserved;
    s1ap;
    simco;
    sua;
    tali;
    v5ua;
    x2ap;
  }
}
```

Hierarchy Level [edit security gprs sctp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.2. Support for the **payload-protocol** statement was modified n Junos OS Release 12.1X46-D10.

Description Display information about the configuration of the current Stream Control Transmission Protocol (SCTP) inspection.

Options

- **m3ua-services**—M3UA data service indicator. The following values are supported:
  - **isup**—ISDN Upper Part.
  - **sccp**—Signaling Connection Control Part.

- **tup**—Telephone User Part.

- **payload-protocol**—SCTP payload protocol identifier. The following values are supported.
  - **id**—Specify payload protocol ID.
  - **all**—All SCTP payload protocol identifiers (id:0~63).
  - **asap**—Aggregate Server Access Protocol.
  - **bicc**—Bearer Independent Call Control.
  - **ddp-segement**—Direct Data Placement Segment chunk.
  - **ddp-stream**—Direct Data Placement Stream session control.
  - **diameter-dtls**—Diameter in a DTLS/SCTP DATA chunk.
  - **diameter-sctp**—Diameter in a SCTP DATA chunk.
  - **dua**—DPNSS/DASS 2 extensions to IUA Protocol.
  - **enrp**—Endpoint Handlespace Redundancy Protocol.
  - **h248**—H.248 Protocol.
  - **h323**—H.323 Protocol.
  - **iua**—ISDN User Adaptation Layer.
  - **m2pa**—MTP2 User Peer-to-Peer Adaption Layer.
  - **m2ua**—MTP2 User Adaption Layer.
  - **m3ua**—MTP3 User Adaption Layer.
  - **qipc**—Q.IPC.
  - **reserved**—Reserved by SCTP.
  - **s1ap**—S1 Application Protocol (S1AP).
  - **simco**—Simple Middlebox Configuration.
  - **sua**—SCCP User Adaption Layer.
  - **tali**—Transport Adapter Layer Interface.
  - **v5ua**—v5.2 User Adaption Layer.
  - **x2ap**—X2 Application Protocol (X2AP).

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

drop-threshold (Security GPRS)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
drop-threshold {
    forward number;
    reverse number;
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type (create-req | delete-req | echo-req | other)]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify drop threshold for path rate limit.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

echo-req

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
echo-req {
  alarm-threshold {
    forward number;
    reverse number;
  }
  drop-threshold {
    forward number;
    reverse number;
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit the number of packets per minute for GTP echo request.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

enable-gtpu-distribution

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax enable-gtpu-distribution;

Hierarchy Level [edit security forwarding-process application-services]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Enable GPRS tunneling protocol, user plane(GTP-U) session distribution to distribute GTP-U traffic handled by a gateway GPRS support node (GGSN) and a Serving GPRS Support Node (SGSN) pair on all Services Processing Units (SPUs) by switching using tunnel-based session distribution where the GTP-U traffic of different tunnels is spread across different SPUs.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding Central Point Architecture Support for GTP on page 6

end-user-address-validated (GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax end-user-address-validated;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify the validated address of the end user.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

forward

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax forward *number*;

Hierarchy Level
[edit security gprs gtp profile *profile-name* path-rate-limit message-type create-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type delete-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type echo-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type other (alarm-threshold | drop-threshold)]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit messages in the forward direction.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

gprs

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
gprs {
  gtp {
    profile profile-name {
      apn pattern-string {
        imsi-prefix imsi-prefix-digits {
          action {
            drop;
            pass;
            selection (ms|net|vrf);
          }
        }
      }
      drop {
        aa-create-pdp (0 | 1 | 2 | all);
        aa-delete-pdp (0 | 1 | 2 | all);
        bearer-resource (0 | 1 | 2 | all);
        change-notification (0 | 1 | 2 | all);
        config-transfer (0 | 1 | 2 | all);
        context (0 | 1 | 2 | all);
        create-bearer (0 | 1 | 2 | all);
        create-data-forwarding (0 | 1 | 2 | all);
        create pdp (0 | 1 | 2 | all);
        create-session (0 | 1 | 2 | all);
        create-tnl-forwarding (0 | 1 | 2 | all);
        cs-paging (0 | 1 | 2 | all);
        data-record (0 | 1 | 2 | all);
        delete-bearer (0 | 1 | 2 | all);
        delete-command (0 | 1 | 2 | all);
        delete-data-forwarding (0 | 1 | 2 | all);
        delete-pdn (0 | 1 | 2 | all);
        delete-pdp (0 | 1 | 2 | all);
        delete-session (0 | 1 | 2 | all);
        detach (0 | 1 | 2 | all);
        downlink-notification (0 | 1 | 2 | all);
        echo (0 | 1 | 2 | all);
        error-indication (0 | 1 | 2 | all);
        failure-report (0 | 1 | 2 | all);
        fwd-access (0 | 1 | 2 | all);
        fwd-relocation (0 | 1 | 2 | all);
        fwd-srns-context (0 | 1 | 2 | all);
        g-pdu (0 | 1 | 2 | all);
        identification (0 | 1 | 2 | all);
        mbms-sess-start (0 | 1 | 2 | all);
        mbms-sess-stop (0 | 1 | 2 | all);
        mbms-sess-update (0 | 1 | 2 | all);
        modify-bearer (0 | 1 | 2 | all);
        modify-command (0 | 1 | 2 | all);
        node-alive (0 | 1 | 2 | all);
        note-ms-present (0 | 1 | 2 | all);
        pdu-notification (0 | 1 | 2 | all);
```

```
            ran-info (0 | 1 | 2 | all);
            redirection (0 | 1 | 2 | all);
            release-access (0 | 1 | 2 | all);
            relocation-cancel (0 | 1 | 2 | all);
            resume (0 | 1 | 2 | all);
            send-route (0 | 1 | 2 | all);
            sgsn-context (0 | 1 | 2 | all);
            stop-paging (0 | 1 | 2 | all);
            supported-extension (0 | 1 | 2 | all);
            suspend (0 | 1 | 2 | all);
            trace-session (0 | 1 | 2 | all);
            update-bearer (0 | 1 | 2 | all);
            update-pdn (0 | 1 | 2 | all);
            update-pdp (0 | 1 | 2 | all);
            ver-not-supported (0 | 1 | 2 | all);
          }
          gtp-in-gtp-denied;
          handover-on-roaming-intf;
          log {
            forwarded (basic | detail);
            prohibited (basic | detail);
            rate-limited {
              (basic | detail);
              frequency-number number;
            }
            state-invalid (basic | detail);
          }
          max-message-length number;
          min-message-length number;
          rate-limit limit;
          remove-ie {
            version v1 {
            number ie-number;
            release (R6 | R7 | R8 | R9);
            }
          }
          req-timeout;
          restart-path (all | create | echo);
          timeout (value);
        }
        traceoptions {
          file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
          }
          flag flag;
          no-remote-trace;
        }
      }
      sctp {
        log {
          association;
          configuration;
```

```
    control-message-all;
    control-message-drop;
    data-message-drop;
    rate-limit;
  }
  profile profile-name {
    association-timeout time-in-minutes;
    drop {
      m3ua-service {
        isup;
        sccp;
        tup;
      }
      payload-protocol {
        all;
        asap;
        bicc;
        ddp-segment;
        ddp-stream;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
        reserved;
        simco;
        sua;
        tali;
        v5ua;
      }
    }
    handshake-timeout time-in-seconds;
    limit {
      rate {
        address ip-address {
          sccp rate-limit;
          ssp rate-limit;
          sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
      }
    }
    nat-only;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
```

```
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40.

Description Configure General Packet Radio Service (GPRS) features.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

gprs-gtp-profile

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax gprs-gtp-profile *profile-name*;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information Statement introduced in Junos OS Release 11.1.

Description Specify the name of the GPRS tunneling protocol profile.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

gprs-sctp-profile

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax gprs-sctp-profile *profile-name*;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information Statement introduced in Junos OS Release 11.1.

Description Specify the name of the GPRS stream control protocol profile.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

gtp

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
gtp {
  profile profile-name {
    apn pattern-string {
      imsi-prefix imsi-prefix-digits {
        action {
          drop;
          pass;
          selection (ms|net|vrf);
        }
      }
    }
    drop {
      aa-create-pdp (0 | 1 | 2 | all);
      aa-delete-pdp (0 | 1 | 2 | all);
      bearer-resource (0 | 1 | 2 | all);
      change-notification (0 | 1 | 2 | all);
      config-transfer (0 | 1 | 2 | all);
      context (0 | 1 | 2 | all);
      create-bearer (0 | 1 | 2 | all);
      create-data-forwarding (0 | 1 | 2 | all);
      create pdp (0 | 1 | 2 | all);
      create-session (0 | 1 | 2 | all);
      create-tnl-forwarding (0 | 1 | 2 | all);
      cs-paging (0 | 1 | 2 | all);
      data-record (0 | 1 | 2 | all);
      delete-bearer (0 | 1 | 2 | all);
      delete-command (0 | 1 | 2 | all);
      delete-data-forwarding (0 | 1 | 2 | all);
      delete-pdn (0 | 1 | 2 | all);
      delete-pdp (0 | 1 | 2 | all);
      delete-session (0 | 1 | 2 | all);
      detach (0 | 1 | 2 | all);
      downlink-notification (0 | 1 | 2 | all);
      echo (0 | 1 | 2 | all);
      error-indication (0 | 1 | 2 | all);
      failure-report (0 | 1 | 2 | all);
      fwd-access (0 | 1 | 2 | all);
      fwd-relocation (0 | 1 | 2 | all);
      fwd-srns-context (0 | 1 | 2 | all);
      g-pdu (0 | 1 | 2 | all);
      identification (0 | 1 | 2 | all);
      mbms-sess-start (0 | 1 | 2 | all);
      mbms-sess-stop (0 | 1 | 2 | all);
      mbms-sess-update (0 | 1 | 2 | all);
      modify-bearer (0 | 1 | 2 | all);
      modify-command (0 | 1 | 2 | all);
      node-alive (0 | 1 | 2 | all);
      note-ms-present (0 | 1 | 2 | all);
      pdu-notification (0 | 1 | 2 | all);
      ran-info (0 | 1 | 2 | all);
```

```
            redirection (0 | 1 | 2 | all);
            release-access (0 | 1 | 2 | all);
            relocation-cancel (0 | 1 | 2 | all);
            resume (0 | 1 | 2 | all);
            send-route (0 | 1 | 2 | all);
            sgsn-context (0 | 1 | 2 | all);
            stop-paging (0 | 1 | 2 | all);
            supported-extension (0 | 1 | 2 | all);
            suspend (0 | 1 | 2 | all);
            trace-session (0 | 1 | 2 | all);
            update-bearer (0 | 1 | 2 | all);
            update-pdn (0 | 1 | 2 | all);
            update-pdp (0 | 1 | 2 | all);
            ver-not-supported (0 | 1 | 2 | all);
        }
        gtp-in-gtp-denied;
        handover-on-roaming-intf;
        log {
            forwarded (basic | detail);
            prohibited (basic | detail);
            rate-limited {
                (basic | detail);
                frequency-number number;
            }
            state-invalid (basic | detail);
        }
        max-message-length number;
        min-message-length number;
        rate-limit limit;
        remove-ie {
            version v1 {
            number ie-number;
            release (R6 | R7 | R8 | R9);
            }
        }
        req-timeout;
        restart-path (all | create | echo);
        timeout (value);
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level [edit security gprs]

Release Information Statement introduced in Junos OS Release 10.0. The **restart-path** option added in Junos OS Release 11.4. New GPRS tunneling protocol (GTP) message types added in Junos OS Release 11.4. Support for GTPv2 added in Junos OS Release 11.4. Statement modified in Junos OS Release 15.1X49-D40.

Description Use the GTP commands to enable the GTP service, configure GTP objects, set traceoptions, remove GTP inspection object configurations, and obtain configuration information.

A Juniper Networks security device provides firewall protection for the following types of General Packet Radio Service (GPRS) interfaces:

- Gn—The Gn interface is the connection between a Serving GPRS Support Node (SGSN) and a gateway GPRS support node (GGSN) within the same public land mobile network (PLMN).
- Gp—The Gp interface is the connection between two PLMNs.
- Gi—The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

gtp-in-gtp-denied

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax gtp-in-gtp-denied;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Select this option to enable the security device to detect and drop a GTP packet that contains another GTP packet in its message body.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

handover-on-roaming-intf

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax handover-on-roaming-intf;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Select this option to enable the security device to receive context and forward relocation messages, inspect the packets, and to set up PDP contexts on the device.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

handshake-timeout

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax handshake-timeout *time-in-seconds*;

Hierarchy Level [edit security gprs sctp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Set the handshake time for Stream Control Transmission Protocol (SCTP).

Options ***time-in-seconds***—Number of seconds of handshake time that elapse before the session is terminated. **Range:** 10 to 30 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

imsi-prefix

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
imsi-prefix imsi-prefix-digits {
  action {
    drop;
    pass;
    selection (ms|net|vrf);
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* apn *pattern-string*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4. Option mcc-mnc replaced with imsi-prefix in Junos OS Release 12.1X44-D10.

Description Specify an International Mobile Station Identity (IMSI) prefix for filtering GTP packets.

You can also filter GTP packets based on the combination of an IMSI prefix and an access point name (APN).

Options *imsi-prefix-digits*—Specify an IMSI prefix.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

limit (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
limit {
    address ip-address {
        payload-protocol {
            id {
                rate number;
            }
            asap {
                rate number;
            }
            bicc {
                rate number;
            }
            ddp-segment {
                rate number;
            }
            ddp-stream {
                rate number;
            }
            diameter-dtls {
                rate number;
            }
            diameter-sctp {
                rate number;
            }
            dua {
                rate number;
            }
            enrp {
                rate number;
            }
            h248 {
                rate number;
            }
            h323 {
                rate number;
            }
            iua {
                rate number;
            }
            m2pa {
                rate number;
            }
            m2ua {
                rate number;
            }
            m3ua {
                rate number;
            }
            others {
                rate number;
```

```
        }
        qipc {
            rate number;
        }
        reserved {
            rate number;
        }
        s1ap {
            rate number;
        }
        simco {
            rate number;
        }
        sua {
            rate number;
        }
        tali {
            rate number;
        }
        v5ua {
            rate number;
        }
        x2ap {
            rate number;
        }
    }
}
payload-protocol {
    id {
        rate number;
    }
    asap {
        rate number;
    }
    bicc {
        rate number;
    }
    ddp-segment {
        rate number;
    }
    ddp-stream {
        rate number;
    }
    diameter-dtls {
        rate number;
    }
    diameter-sctp {
        rate number;
    }
    dua {
        rate number;
    }
    enrp {
        rate number;
    }
    h248 {
```

```
            rate number;
        }
        h323 {
            rate number;
        }
        iua {
            rate number;
        }
        m2pa {
            rate number;
        }
        m2ua {
            rate number;
        }
        m3ua {
            rate number;
        }
        others {
            rate number;
        }
        qipc {
            rate number;
        }
        reserved {
            rate number;
        }
        s1ap {
            rate number;
        }
        simco {
            rate number;
        }
        sua {
            rate number;
        }
        tali {
            rate number;
        }
        v5ua {
            rate number;
        }
        x2ap {
            rate number;
        }
    }
    rate {
        address ip-address {
            sccp rate-limit;
            ssp rate-limit;
            sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
    }
}
```

Hierarchy Level [edit security gprs sctp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.2. Statement is modified in Junos OS Release 12.1X46-D10. Support for **address** option accepting both IPv4 and IPv6 formats added in Junos OS Release 12.1X47-D10.

Description Set the rate limit per association for local Services Processing Unit (SPU) packets.

Options

address *ip-address*—Set Signalling Connection Control Part (SCCP), Subsystem-Prohibited (SSP), and Subsystem Status Test (SST) messages rate limit to an IP address. The IP address can accept either an IPv4 address or an IPv6 address.

sccp *rate-limit*—Set the SCCP messages rate limit.

ssp *rate-limit*—Set the SSP messages rate limit.

sst *rate-limit*—Set the SSP messages rate limit.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

log (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
log {
  forwarded (basic | detail);
  prohibited (basic | detail);
  rate-limited {
    (basic | detail);
    frequency-number number;
  }
  state-invalid (basic | detail);
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Configure GTP logs to be viewed from the console or syslog.

NOTE: By default, all logs are disabled on the device.

Options

- **forwarded**—A packet that the security device transmitted because it was valid.
- **prohibited**—A packet that the security device dropped because it was invalid.
- **rate-limited**—A packet that the security device dropped because it exceeded the maximum rate limit of the destination GSN.
  - **frequency-number *number***—Logging frequency over threshold set by rate-limit (2–500).
- **state-invalid**—A packet that the security device dropped because it failed stateful inspection.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

log (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
log {
  association;
  configuration;
  control-message-all;
  control-message-drop;
  data--message-drop;
  rate-limit;
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Junos OS Release 10.2. The options **association**, **control-message-all**, **control-message-drop**, and **data-message-drop** added in Junos OS Release 12.1X45-D10.

Description Configure Stream Control Transmission Protocol (SCTP) logs to be viewed from the console or system log.

Options

association—To log association events.

configuration—To log the CLI configuration.

control-message-all—To log both dropped and passed control messages.

control-message-drop—To log the dropped control messages.

data-message-drop—To log the dropped data messages.

rate-limit—To log the rate limit.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

max-message-length

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax max-message-length *number*;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Set the maximum message payload length (in bytes) the security device accepts for a GTP message. The default maximum message length is 65,535 bytes. The message length range is from 1 through 65,535 bytes.

Options *number*—Set the maximum message payload length in bytes.

Range: 1 through 65,535 bytes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

message-type

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
message-type {
  create-req {
    alarm-threshold {
      forward number;
      reverse number;
    }
    drop-threshold {
      forward number;
      reverse number;
    }
  }
  delete-req {
    alarm-threshold {
      forward number;
      reverse number;
    }
    drop-threshold {
      forward number;
      reverse number;
    }
  }
  echo-req {
    alarm-threshold {
      forward number;
      reverse number;
    }
    drop-threshold {
      forward number;
      reverse number;
    }
  }
  other {
    alarm-threshold {
      forward number;
      reverse number;
    }
    drop-threshold {
      forward number;
      reverse number;
    }
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify the group of control messages.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

min-message-length

Supported Platforms SRX5400, SRX5400, SRX5600, SRX5600, SRX5800, SRX5800, vSRX

Syntax min-message-length *number*;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Set the minimum message payload length (in bytes) the security device accepts for a GTP message. The default minimum message length is 0 bytes. The message length range is from 0 through 65,535 bytes.

Options *number*—Set the minimum message payload length in bytes.
Range: 0 through 65,535 bytes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

multichunk-inspection

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax multichunk-inspection (enable | disable);

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Junos OS Release 12.1X47-D10.

Description Configure the Stream Control Transmission Protocol (SCTP) firewall to enable or disable multichunk inspection.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

nullpdu

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
nullpdu {
  protocol (ID-0x0000 | ID-0xFFFF);
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Junos OS Release 12.1X47-D10.

Description Configure the Stream Control Transmission Protocol (SCTP) null protocol data unit (PDU) value.

Options **protocol**—Specify the SCTP null PDU payload protocol identifier.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

number

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax number *ie-number*

Hierarchy Level [edit security gprs gtp profile *profile-name* remove-ie version *v1*]

Release Information Statement introduced in Junos OS Release 12.1.

Description Specify the user-configured IE number. IE removal by IE number supports all IEs, ranging from 1 to 255.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

other

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
other {
  alarm-threshold {
    forward number;
    reverse number;
  }
  drop-threshold {
    forward number;
    reverse number;
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name* path-rate-limit message-type]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit the number of packets per second for all the other GTPv0/GTPv1-C/GTPv2-C messages.

Options *number*—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

path-rate-limit

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
path-rate-limit {
  message-type {
    create-req {
      alarm-threshold {
        forward number;
        reverse number;
      }
      drop-threshold {
        forward number;
        reverse number;
      }
    }
    delete-req {
      alarm-threshold {
        forward number;
        reverse number;
      }
      drop-threshold {
        forward number;
        reverse number;
      }
    }
    echo-req {
      alarm-threshold {
        forward number;
        reverse number;
      }
      drop-threshold {
        forward number;
        reverse number;
      }
    }
    other {
      alarm-threshold {
        forward number;
        reverse number;
      }
      drop-threshold {
        forward number;
        reverse number;
      }
    }
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit control messages based on an IP pair.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

permit (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
permit {
  payload-protocol {
    id;
    all;
    asap;
    bicc;
    ddp-segment;
    ddp-stream;
    diameter-dtls;
    diameter-sctp;
    dua;
    enrp;
    h248;
    h323;
    iua;
    m2pa;
    m2ua;
    m3ua;
    qipc;
    reserved;
    s1ap;
    simco;
    sua;
    tali;
    v5ua;
    x2ap;
  }
}
```

Hierarchy Level [edit security gprs sctp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X46-D10.

Description Display information about the configuration of the current Stream Control Transmission Protocol (SCTP) inspection.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

profile (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
profile profile name {
  apn pattern-string {
    imsi-prefix imsi-prefix-digits {
      action {
        drop;
        pass;
        selection (ms|net|vrf);
      }
    }
  }
  drop {
    aa-create-pdp (0 | 1 | 2 | all);
    aa-delete-pdp (0 | 1 | 2 | all);
    bearer-resource (0 | 1 | 2 | all);
    change-notification (0 | 1 | 2 | all);
    config-transfer (0 | 1 | 2 | all);
    context (0 | 1 | 2 | all);
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
```

```
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
    ver-not-supported (0 | 1 | 2 | all);
  }
  gtp-in-gtp-denied;
  handover-on-roaming-intf;
  log {
    forwarded (basic | detail);
    prohibited (basic | detail);
    rate-limited {
      (basic | detail);
      frequency-number number;
    }
    state-invalid (basic | detail);
  }
  max-message-length number;
  min-message-length number;
  rate-limit limit;
  remove-ie {
    version v1 {
      number ie-number;
      release (R6 | R7 | R8 | R9);
    }
  }
  req-timeout;
  restart-path (all | create | echo);
  timeout (value);
  }
}
```

Hierarchy Level [edit security gprs gtp]

Release Information Statement introduced in Junos OS Release 10.0. The **restart-path** option added in Junos OS Release 11.4. New GPRS tunneling protocol (GTP) message types added in Junos OS Release 11.4. Support for GTPv2 added in Junos OS Release 11.4. Statement modified in Junos OS Release 15.1X49-D40.

Description Create a profile for the GTP feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

profile (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
profile profile-name {
  association-timeout time-in-minutes;
  drop {
    m3ua-service {
      isup;
      sccp;
      tup;
    }
    payload-protocol {
      id;
      all;
      asap;
      bicc;
      ddp-segment;
      ddp-stream;
      diameter-dtls;
      diameter-sctp;
      dua;
      enrp;
      h248;
      h323;
      iua;
      m2pa;
      m2ua;
      m3ua;
      qipc;
      reserved;
      s1ap;
      simco;
      sua;
      tali;
      v5ua;
      x2ap;
    }
  }
  handshake-timeout time-in-seconds;
  limit {
    address ip-address {
      payload-protocol {
        id {
          rate number;
        }
        asap {
          rate number;
        }
        bicc {
          rate number;
        }
        ddp-segment {
          rate number;
```

```
}
ddp-stream {
    rate number;
}
diameter-dtls {
    rate number;
}
diameter-sctp {
    rate number;
}
dua {
    rate number;
}
enrp {
    rate number;
}
h248 {
    rate number;
}
h323 {
    rate number;
}
iua {
    rate number;
}
m2pa {
    rate number;
}
m2ua {
    rate number;
}
m3ua {
    rate number;
}
others {
    rate number;
}
qipc {
    rate number;
}
reserved {
    rate number;
}
s1ap {
    rate number;
}
simco {
    rate number;
}
sua {
    rate number;
}
tali {
    rate number;
}
v5ua {
```

```
            rate number;
        }
        x2ap {
            rate number;
        }
    }
}
payload-protocol {
    id {
        rate number;
    }
    asap {
        rate number;
    }
    bicc {
        rate number;
    }
    ddp-segment {
        rate number;
    }
    ddp-stream {
        rate number;
    }
    diameter-dtls {
        rate number;
    }
    diameter-sctp {
        rate number;
    }
    dua {
        rate number;
    }
    enrp {
        rate number;
    }
    h248 {
        rate number;
    }
    h323 {
        rate number;
    }
    iua {
        rate number;
    }
    m2pa {
        rate number;
    }
    m2ua {
        rate number;
    }
    m3ua {
        rate number;
    }
    others {
        rate number;
    }
```

```
        qipc {
            rate number;
        }
        reserved {
            rate number;
        }
        s1ap {
            rate number;
        }
        simco {
            rate number;
        }
        sua {
            rate number;
        }
        tali {
            rate number;
        }
        v5ua {
            rate number;
        }
        x2ap {
            rate number;
        }
    }
    rate {
        address ip-address {
            sccp rate-limit;
            ssp rate-limit;
            sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
    }
}
nat-only;
permit {
    payload-protocol {
        id;
        all;
        asap;
        bicc;
        ddp-segment;
        ddp-stream;
        diameter-dtls;
        diameter-sctp;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
```

```
            reserved;
            s1ap;
            simco;
            sua;
            tali;
            v5ua;
            x2ap;
        }
    }
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Junos OS Release 10.2. Support for the **nat-only** option added in Junos OS Release 12.1X45-D10. Support for the **permit** option is added in Junos OS Release 12.1X46-D10.

Description Create a profile of the Stream Control Transmission Protocol (SCTP) feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

rate-limit (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax rate-limit *value*;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Set the limit rate of control traffic to any GSN defined in a GTP profile.

Options **Range:** 1 through 80,000 messages per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

remove-ie

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
remove-ie {
  version v1 {
  number ie-number;
  release (R6 | R7 | R8 | R9);
  }
}
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enable the security device to detect and remove 3G-specific attributes from the GTP packet header when the packet passes into a 2G network. This allows you to retain interoperability when roaming between 2G and 3G networks.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

req-timeout

Supported Platforms

Syntax req-timeout;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X46-D35.

Description Specify a GTP request message timeout. The default timeout value is 5 seconds.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

restart-path

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax restart-path (all | create | echo);

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4. Support for GTPv2 added in Junos OS Release 11.4.

Description Restart a GTP path. Restarting a GTP path deletes all GTP tunnels between two devices.

Options

- **all**—Restart GTP paths by detecting the changed restart number obtained from the Recovery information element (IE) in all GTP messages.
- **create**—Restart GTP paths by detecting the changed restart number obtained from the Recovery IE in create-session messages.
- **echo**—Restart GTP paths by detecting the changed restart number obtained from the Recovery IE in echo messages.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

reverse

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax reverse *number*;

Hierarchy Level
[edit security gprs gtp profile *profile-name* path-rate-limit message-type create-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type delete-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type echo-req (alarm-threshold | drop-threshold)]
[edit security gprs gtp profile *profile-name* path-rate-limit message-type other (alarm-threshold | drop-threshold)]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Limit messages in the reverse direction.

Options ***number***—Limit messages in forward or reverse direction.

Range: 1 through 10,000

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sctp

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
sctp {
  log {
    association;
    configuration;
    control-message-all;
    control-message-drop;
    data-message-drop;
    rate-limit;
  }
  multichunk-inspection (enable | disable);
  nullpdu {
    protocol (ID-0x0000 | ID-0xFFFF);
  }
  profile profile-name {
    association-timeout time-in-minutes;
    drop {
      m3ua-service {
        isup;
        sccp;
        tup;
      }
      payload-protocol {
        id;
        all;
        asap;
        bicc;
        ddp-segment;
        ddp-stream;
        diameter-dtls;
        diameter-sctp;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
        reserved;
        s1ap;
        simco;
        sua;
        tali;
        v5ua;
        x2ap;
      }
    }
    handshake-timeout time-in-seconds;
    limit {
```

```
address ip-address {
  payload-protocol {
    id {
      rate number;
    }
    asap {
      rate number;
    }
    bicc {
      rate number;
    }
    ddp-segment {
      rate number;
    }
    ddp-stream {
      rate number;
    }
    diameter-dtls {
      rate number;
    }
    diameter-sctp {
      rate number;
    }
    dua {
      rate number;
    }
    enrp {
      rate number;
    }
    h248 {
      rate number;
    }
    h323 {
      rate number;
    }
    iua {
      rate number;
    }
    m2pa {
      rate number;
    }
    m2ua {
      rate number;
    }
    m3ua {
      rate number;
    }
    others {
      rate number;
    }
    qipc {
      rate number;
    }
    reserved {
      rate number;
    }
```

```
        s1ap {
            rate number;
        }
        simco {
            rate number;
        }
        sua {
            rate number;
        }
        tali {
            rate number;
        }
        v5ua {
            rate number;
        }
        x2ap {
            rate number;
        }
    }
}
payload-protocol {
    id {
        rate number;
    }
    asap {
        rate number;
    }
    bicc {
        rate number;
    }
    ddp-segment {
        rate number;
    }
    ddp-stream {
        rate number;
    }
    diameter-dtls {
        rate number;
    }
    diameter-sctp {
        rate number;
    }
    dua {
        rate number;
    }
    enrp {
        rate number;
    }
    h248 {
        rate number;
    }
    h323 {
        rate number;
    }
    iua {
        rate number;
```

```
        }
        m2pa {
            rate number;
        }
        m2ua {
            rate number;
        }
        m3ua {
            rate number;
        }
        others {
            rate number;
        }
        qipc {
            rate number;
        }
        reserved {
            rate number;
        }
        s1ap {
            rate number;
        }
        simco {
            rate number;
        }
        sua {
            rate number;
        }
        tali {
            rate number;
        }
        v5ua {
            rate number;
        }
        x2ap {
            rate number;
        }
    }
    rate {
        address ip-address {
            sccp rate-limit;
            ssp rate-limit;
            sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
    }
}
nat-only;
permit {
    payload-protocol {
        id;
        all;
        asap;
        bicc;
```

```
            ddp-segment;
            ddp-stream;
            diameter-dtls;
            diameter-sctp;
            dua;
            enrp;
            h248;
            h323;
            iua;
            m2pa;
            m2ua;
            m3ua;
            qipc;
            reserved;
            s1ap;
            simco;
            sua;
            tali;
            v5ua;
            x2ap;
          }
        }
      }
      traceoptions {
        file {
          filename;
          files number;
          match regular-expression;
          size maximum-file-size;
          (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
      }
    }
```

Hierarchy Level [edit security gprs]

Release Information Statement introduced in Junos OS Release 10.2. Support for the **nat-only** option added in Junos OS Release 12.1X45-D10. Support for the **profile** statement added in Junos OS Release 12.1X46-D10.

Description Use the Stream Control Transmission Protocol (SCTP) commands to configure SCTP objects, configure SCTP logs, set trace options, and set address rate limit.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

seq-number-validated (GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax seq-number-validated;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify the validated sequence number.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax timeout *value*;

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Set the tunnel timeout value in hours. The default is 36 hours.

If a device detects no activity in a tunnel for a specified period, it removes the tunnel from the state table.

Options **Range:** 1 through 1,000 hours.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

traceoptions (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security gprs gtp]

Release Information Statement introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Enable the device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification.

Options

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace everything.
  - **chassis-cluster**—Trace chassis cluster events.
  - **configuration**—Trace configuration events.
  - **flow**—Trace flow events.
  - **parser**—Trace parser events.
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (Security SCTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Junos OS Release 10.2. The flag statement **detail** introduced in Junos OS Release 12.1X45-D10.

Description Set the trace options for Stream Control Transmission Protocol (SCTP).

Options **file**—Configure the trace file options.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.

files *number*—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files.

Default: 10 files.

match *regular-expression*—Refine the output to include lines that contain the regular expression.

size *maximum-file-size*—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB.

Default: 128 KB.

world-readable | no-world-readable—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- all—Trace everything.
- chassis-cluster—Trace chassis cluster events.
- configuration—Trace configuration events.
- detail—Trace information used for debugging.
- flow—Trace flow events.
- parser—Trace parser events.

no-remote-trace—Set remote tracing as disabled.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

u-tunnel-validated (GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax
```
u-tunnel-validated;
```

Hierarchy Level [edit security gprs gtp profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specify the validated GTP-U tunnel.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

version (Security GTP)

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
version v1 {
  number ie-number;
  release (R6 | R7 | R8 | R9);
}
```

Hierarchy Level [edit security gprs gtp profile profile-name remove-ie]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify GTP version.

Options

- **v1**—GTP version 1.
- **release** —Specify release number. Available options are:
  - Release R6—Specify R6 IE removal.
  - Release R7—Specify R7 IE removal.
  - Release R8—Specify R8 IE removal.
  - Release R9—Specify R9 IE removal.
- **number** —Specify the user-configured IE number. IE removal by IE number supports all IEs, ranging from 1 to 255.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

CHAPTER 13

Operational Commands

- clear gtp tunnels
- clear security gprs gtp counters
- clear security gprs sctp association
- clear security gprs sctp counters
- show gtp tunnels
- show security gprs gtp counters
- show security gprs gtp counters path-rate-limit
- show security gprs gtp gsn statistics
- show security gprs sctp association
- show security gprs sctp counters

clear gtp tunnels

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax **clear security gprs gtp tunnel <all | *identifier*>**

Release Information Command introduced in Junos OS Release 10.0. Support for GTPv2 added in Junos OS Release 11.4.

Description Clear all or specified GTP tunnels on the device.

Options

- *identifier*—Clear a single tunnel by entering the tunnel ID. To view current tunnel IDs, type **show security gprs gtp tunnels**.
- all—Clear all existing tunnels.

Required Privilege Level clear

clear security gprs gtp counters

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax clear security gprs gtp counters <*all* | *error* | *ha* | *message* <*message-name*> | *packet* | *request* | *tunnel* | *path-rate-limit*>

Release Information Command introduced in Junos OS Release 12.1X44-D10.

Description Clear all GTP counters on the device.

Options

- **all**—Clear all GTP counters.
- **error**—Clear GTP error counters.
- **ha**—Clear GTP HA counters.
- **message** ***message-name***—Clear GTP message counters.
- **packet**—Clear GTP packet counters.
- **request**—Clear GTP request counters.
- **tunnel**—Clear GTP tunnel counters.
- **path-rate-limit**—Clear path-rate-limit counters.

Required Privilege Level clear

Related Documentation

- show security gprs gtp counters on page 204

List of Sample Output

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security gprs gtp counters all

```
user@host> clear security gprs gtp counters all
All GTP counters have been cleared
```

clear security gprs gtp counters error

```
user@host> clear security gprs gtp counters error
GTP error counter has been cleared
```

clear security gprs gtp counters ha

```
user@host> clear security gprs gtp counters ha
GTP HA counter has been cleared
```

clear security gprs gtp counters message v0-create-aa-pdp-req

```
user@host> clear security gprs gtp counters message v0-create-aa-pdp-req
GTPv0 create AA PDP request message counter has been cleared
```

clear security gprs gtp counters packet

```
user@host> clear security gprs gtp counters packet
GTP packet counter has been cleared
```

clear security gprs gtp counters request

```
user@host> clear security gprs gtp counters request
GTP request counter has been cleared
```

clear security gprs gtp counters tunnel

```
user@host> clear security gprs gtp counters tunnel
GTP tunnel counter has been cleared
```

clear security gprs gtp counters path-rate-limit

```
user@host> clear security gprs gtp counters path-rate-limit
GTP path-rate-limit counter has been cleared
```

clear security gprs sctp association

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax
clear security gprs sctp association
<all>
<destination-ip>
<desitnation-port>
<guid>
<init>
<source-ip>
<source-port>

Release Information Command introduced in Junos OS Release 12.1X45-D10.

Description Clear the Stream Control Transmission Protocol (SCTP) association.

Options

none—Clear the live SCTP associations.

all—Clear all the SCTP associations, both initiated and live. All SCTP traffic is blocked while the associations are being cleared, which can take up to one minute.

destination-ip—Clear the destination IP SCTP association.

destination-port—Clear the destination port SCTP association.

guid—Clear the globally unique identifier SCTP association.

init—Clear the initiated SCTP associations.

source-ip—Clear the source IP address SCTP association.

source-port—Clear the source port SCTP association.

Required Privilege Level clear

Related Documentation
- show security gprs sctp association on page 214

List of Sample Output clear security gprs sctp association on page 199

Sample Output

clear security gprs sctp association

```
user@host> clear security gprs sctp association


Clear Association Information for FPC: 2    PIC: 0
Cleared matched SCTP association information:
Has cleared matched association: 0
```

```
Clear Association Information for FPC: 2    PIC: 1
Cleared matched SCTP association information:
Has cleared matched association: 9


Clear Association Information for FPC: 2    PIC: 2
Cleared matched SCTP association information:
Has cleared matched association: 8


Clear Association Information for FPC: 2    PIC: 3
Cleared matched SCTP association information:
Has cleared matched association: 10


Clear Association Information for FPC: 5    PIC: 0
Cleared matched SCTP association information:
Has cleared matched association: 7


Clear Association Information for FPC: 5    PIC: 1
Cleared matched SCTP association information:
Has cleared matched association: 6
```

clear security gprs sctp counters

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax clear security gprs sctp counters

Release Information Command introduced in Junos OS Release 10.2.

Description Clear the statistics of the dropped Stream Control Transmission Protocol (SCTP) counters.

Options none—Clear all dropped SCTP counters.

Required Privilege Level clear

Related Documentation
- show security gprs sctp counters on page 216

List of Sample Output clear security gprs sctp counters on page 201

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security gprs sctp counters

```
user@host> clear security gprs sctp counters
```

show gtp tunnels

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax **show security gprs gtp tunnels (brief | summary | detail)**

Release Information Command introduced in Junos OS Release 10.0. Support for GPRS tunneling protocol version 2 (GTPv2) added in Junos OS Release 11.4. Command output updated in Junos OS Release 15.1X49-D40.

Description Display all existing GTP tunnels.

Options

- brief—Display a short listing of all GTP tunnels.
- summary—Display a summary of all GTP tunnels.
- detail–Display detailed information about all the GTP tunnels.

Required Privilege Level view

List of Sample Output

show security gprs gtp tunnels on page 202
show security gprs gtp tunnels summary on page 202
show security gprs gtp tunnels detail on page 203

Sample Output

show security gprs gtp tunnels

```
user@host> show security gprs gtp tunnels

FPC 7 PIC 0:

 Index: 72000002, EBI/LBI: 5/5(V2)to sgw, Timeout: 1440m
 User: 61.0.0.102, 12345678 --> 62.0.0.102, 00000021
 Control: 61.0.0.101, 00325ac1 --> 62.0.0.101, 00000001

FPC 8 PIC 0:

 Index: 0x02000040 Tunnel ID: 0x50502410121507f5(V0), Timeout: 59m
 User: 20.1.0.1, 00000001 -> 20.0.2.1, 00000001
 Ctrl: 20.1.0.1, 00000001 -> 20.0.2.1, 00000001

 3 tunnels active in total
```

show security gprs gtp tunnels summary

```
user@host> show security gprs gtp tunnels summary

FPC 1 PIC 0:

FPC 1 PIC 1:

FPC 2 PIC 0:
```



```
FPC 2 PIC 1:

2 tunnels active in total
```

show security gprs gtp tunnels detail

```
user@host> show security gprs gtp tunnels detail
node0:
--------------------------------------------------------------------------
 FPC 0 PIC 0:

 FPC 0 PIC 1:

 FPC 0 PIC 2:

 FPC 0 PIC 3:

Index: 0x02000040 Tunnel ID: 0x505024101215O7f5(V0), Timeout: 59m
User: 20.1.0.1, 00000001 -> 20.0.2.1, 00000001
Ctrl: 20.1.0.1, 00000001 -> 20.0.2.1, 00000001

 1 tunnels active in total
```

show security gprs gtp counters

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax show security gprs gtp counters <*all* | *error* | *ha* | *message* <*message-name*> | *packet* | *request* | *tunnel* | *path-rate-limit*>

Release Information Command introduced in Junos OS Release 12.1X44-D10.

Description Display counters that can be used to indicate the number of GTP tunnel counters (Allocated and Freed), GTP packet counters (Received, Passed, and Dropped), Brief message counters (Receive, Forward, and Drop), Error counters, Request counters, HA counters, and Path-rate-limit counters (Drop and Alarm).

Options

- **all**—Show all GTP counters.
- **error**—Show GTP error counters.
- **ha**—Show GTP HA counters.
- **message** ***message-name***—Show GTP message counters.
- **packet**—Show GTP packet counters.
- **request**—Show GTP request counters.
- **tunnel**—Show GTP tunnel counters.
- **path-rate-limit**—Show path-rate-limit counters.

Required Privilege Level view

Related Documentation

- clear security gprs gtp counters on page 197

List of Sample Output

show security gprs gtp counters all on page 206
show security gprs gtp counters error on page 208
show security gprs gtp counters ha on page 209
show security gprs gtp counters message v0-create-aa-pdp-req on page 209
show security gprs gtp counters packet on page 209
show security gprs gtp counters request on page 210
show security gprs gtp counters tunnel on page 210
show security gprs gtp counters path-rate-limit on page 210

Output Fields Table 12 on page 205 lists the output fields for the **show security gprs gtp counters** command.

Table 12: show security gprs gtp counters all Output Fields

Field Name	Field Description
Tunnel counters	Tunnel counters are used to track the number of tunnels that are created on the device. There are two entries: • Allocated • Freed Active tunnel number = Number of Allocated counters - Number of Freed counters
Packet counters	Packet counters indicate the number of GTP packets that are received and processed on the device. There are three entries: • Received – Number of GTP packet messages received. • Passed – Number of GTP packet messages passed. • Dropped – Number of GTP packet messages dropped because of an error. Number of Received counters = Number of Dropped counters + Number of Passed counters
Brief message counters	GTP messages counters indicate the number of GTP messages that are received and processed on the device. There are three entries: • Receive – Number of GTP messages received. • Forward – Number of GTP messages forwarded. • Drop – Number of GTP messages dropped because of an error. Number of Received counters = Number of Dropped counters + Number of Forward counters
Error counters	Drop reason and drop counters indicate the number of GTP packets that are dropped as a result of an error. Total error = Sum of all the following errors (see Sample Output)
Request counters	Request counters indicate the number of GTP request messages that are received and processed on the device. This information can be used for debugging purpose.
HA counters	HA counters indicate the number of messages that are received or sent by the device.

Table 12: show security gprs gtp counters all Output Fields *(continued)*

Field Name	Field Description
Path-rate-limit counters	Path-rate-limit counters indicate the number of PDP Create, Delete, Echo, and Other messages that are received and processed on the device after drop-threshold and alarm-threshold are reached. • Create Request – Number of create PDP messages. • Delete Request – Number of delete PDP messages. • Echo Request– Number of PDP Echo messages. • Others – Control messages other than the above messages. Drop - Indicate the number of packets dropped. Alarm – Indicate the number of packets transferred after the alarm-threshold is reached.

Sample Output

show security gprs gtp counters all

```
user@host> show security gprs gtp counters all


 Tunnel counters:
                 Total      GTPv0     GTPv1-c     GTPv1-u     GTPv2-c     GTPv2-u
  Allocated          0          0           0           0           0           0
  Freed              0          0           0           0           0           0

Packet counters:
                 Total      GTPv0      GTPv1      GTPv2       GTP'
  Received           0          0          0          0          0
  Passed             0          0          0          0          0
  Dropped            0          0          0          0          0

Brief message counters:
                                 Receive    Forward       Drop
GTPv0
  Create PDP Request                   0          0          0
  Create PDP Response                  0          0          0
  Update PDP Request                   0          0          0
  Update PDP Response                  0          0          0
  Delete PDP Request                   0          0          0
  Delete PDP Response                  0          0          0
  Create AA PDP Request                0          0          0
  Create AA PDP Response               0          0          0
  Delete AA PDP Request                0          0          0
  Delete AA PDP Response               0          0          0
  Others                               0          0          0
GTPv1
  Create PDP Request                   0          0          0
  Create PDP Response                  0          0          0
  Update PDP Request                   0          0          0
  Update PDP Response                  0          0          0
  Delete PDP Request                   0          0          0
  Delete PDP Response                  0          0          0
  Others                               0          0          0
GTPv2
  Create Session Request               0          0          0
```

```
  Create Session Response          0          0          0
  Delete Session Request           0          0          0
  Delete Session Response          0          0          0
  Create Bearer Request            0          0          0
  Create Bearer Response           0          0          0
  Modify Bearer Request            0          0          0
  Modify Bearer Response           0          0          0
  Delete Bearer Request            0          0          0
  Delete Bearer Response           0          0          0
  Others                           0          0          0

Error counters:
        Total error            : 0
        Exception              : 0
        Gate failed            : 0
        Invalid header         : 0
        Message length         : 0
        Zero IMSI              : 0
        Zero charge ID         : 0
        Sequence               : 0
        APN filter             : 0
        Port not match         : 0
        GTP-in-GTP             : 0
        Message too short      : 0
        Message too long       : 0
        GSN not exist          : 0
        Over GSN rate limit    : 0
        Request not found      : 0
        Retransmit response    : 0
        Missing IE             : 0
        Unexpected IE          : 0
        Unknown IE type        : 0
        IE order               : 0
        IE length              : 0
        Duplicate IE           : 0
        Non-digit TID/TEID     : 0
        Non-zero TID/TEID      : 0
        Zero TID/TEID          : 0
        Control TID/TEID       : 0
        Data TID/TEID          : 0
        Control GSN IE         : 0
        Data GSN IE            : 0
        End user IE            : 0
        GGSN IP for handover   : 0
        Disallowed v0 message  : 0
        Disallowed v1 message  : 0
        Disallowed v2 message  : 0
        Invalid message type   : 0
        No tunnel0             : 0
        No control tunnel      : 0
        No user tunnel         : 0
        Invalid tunnel0        : 0
        Invalid control tunnel : 0
        Invalid user tunnel    : 0
        Create tunnel0         : 0
        Create control tunnel  : 0
        Create user tunnel     : 0
        No request             : 0
        Out of request         : 0
        No action              : 0
        Out of action          : 0
```

```
        GTPv2 TEID not exist   : 0
        GTPv2 Missing TEID     : 0
        GTPv2 Non-zero EBI     : 0
        GTPv2 EBI not found    : 0
        GTPv2 IE context       : 0

HA counters:
        Total message received              : 0
        Message received success            : 0
        Bad message received                : 0
        Unknown message type received       : 0
        Unknown message version received    : 0
        Total message send                  : 0
        Message send success                : 0
        Message send failed                 : 0
        Memory allocate failed              : 0

Request counters:
        Request allocated        : 0
        Request freed            : 0
        Request activated        : 0
        Request died             : 0
        Request action allocated : 0
        Request action freed     : 0

Path-rate-limit counters:
                             Drop           Alarm
  Create Request              0              0
  Delete Request              0              0
  Echo Request                0              0
  Others                      0              0
```

show security gprs gtp counters error

```
user@host> show security gprs gtp counters error
Error counters:
        Total error            : 0
        Exception              : 0
        Gate failed            : 0
        Invalid header         : 0
        Message length         : 0
        Zero IMSI              : 0
        Zero charge ID         : 0
        Sequence               : 0
        APN filter             : 0
        Port not match         : 0
        GTP-in-GTP             : 0
        Message too short      : 0
        Message too long       : 0
        GSN not exist          : 0
        Over GSN rate limit    : 0
        Request not found      : 0
        Retransmit response    : 0
        Missing IE             : 0
        Unexpected IE          : 0
        Unknown IE type        : 0
        IE order               : 0
        IE length              : 0
        Duplicate IE           : 0
        Non-digit TID/TEID     : 0
        Non-zero TID/TEID      : 0
```

```
        Zero TID/TEID          : 0
        Control TID/TEID       : 0
        Data TID/TEID          : 0
        Control GSN IE         : 0
        Data GSN IE            : 0
        End user IE            : 0
        GGSN IP for handover   : 0
        Disallowed v0 message  : 0
        Disallowed v1 message  : 0
        Disallowed v2 message  : 0
        Invalid message type   : 0
        No tunnel0             : 0
        No control tunnel      : 0
        No user tunnel         : 0
        Invalid tunnel0        : 0
        Invalid control tunnel : 0
        Invalid user tunnel    : 0
        Create tunnel0         : 0
        Create control tunnel  : 0
        Create user tunnel     : 0
        No request             : 0
        Out of request         : 0
        No action              : 0
        Out of action          : 0
        GTPv2 TEID not exist   : 0
        GTPv2 Missing TEID     : 0
        GTPv2 Non-zero EBI     : 0
        GTPv2 EBI not found    : 0
        GTPv2 IE context       : 0
```

show security gprs gtp counters ha

```
user@host> show security gprs gtp counters ha
HA counters:
        Total message received              : 0
        Message received success            : 0
        Bad message received                : 0
        Unknown message type received       : 0
        Unknown message version received    : 0
        Total message send                  : 0
        Message send success                : 0
        Message send failed                 : 0
        Memory allocate failed              : 0
```

show security gprs gtp counters message v0-create-aa-pdp-req

```
user@host> show security gprs gtp counters message v0-create-aa-pdp-req
Message counters:
  Received              0
  Forwarded             0
  Dropped               0
```

show security gprs gtp counters packet

```
user@host> show security gprs gtp counters packet
Packet counters:
                Total      GTPv0      GTPv1      GTPv2       GTP'
  Received          0          0          0          0          0
  Passed            0          0          0          0          0
  Dropped           0          0          0          0          0
```

show security gprs gtp counters request

```
user@host> show security gprs gtp counters request

Request counters:
        Request allocated           : 0
        Request freed               : 0
        Request activated           : 0
        Request died                : 0
        Request action allocated    : 0
        Request action freed        : 0
```

show security gprs gtp counters tunnel

```
user@host> show security gprs gtp counters tunnel
Tunnel counters:
                 Total      GTPv0    GTPv1-c    GTPv1-u    GTPv2-c    GTPv2-u
  Allocated          0          0          0          0          0          0
  Freed              0          0          0          0          0          0
```

show security gprs gtp counters path-rate-limit

```
user@host> show security gprs gtp counters path-rate-limit
Path-rate-limit counters:
                           Drop          Alarm
  Create Request            0              0
  Delete Request            0              0
  Echo Request              0              0
  Others                    0              0
```

show security gprs gtp counters path-rate-limit

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax **show security gprs gtp counters path-rate-limit**

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Display information about path-rate-limit counters.

Required Privilege Level view

List of Sample Output show security gprs gtp counters path-rate-limit on page 211

Output Fields Table 13 on page 211 lists the output fields for the **show security gprs gtp counters path-rate-limit** command.

Table 13: show security gprs gtp counters path-rate-limit Output Fields

Field Name	Field Description
Create Request	Specify the number of create request messages received in a second after the alarm-threshold or drop-threshold is reached.
Delete Request	Specify the number of delete request messages received in a second after the alarm-threshold or drop-threshold is reached.
Echo Request	Specify the number of echo request messages received in a minute after the alarm-threshold or drop-threshold is reached.
Other messages	Specify the number of other GTP control messages received in a second after the alarm-threshold or drop-threshold is reached.
Drop	Display the number of packets dropped after the drop-threshold is reached.
Alarm	Display the number of packets received after the alarm-threshold is reached.

Sample Output

show security gprs gtp counters path-rate-limit

```
user@host> show security gprs gtp counters path-rate-limit

Path-rate-limit counters:
                                    Drop                 Alarm
Create Request                      200                   100
Delete Request                      300                   200
Echo Request                        600                   400
Others                              900                   800
```

show security gprs gtp gsn statistics

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax show security gprs gtp gsn statistics

Release Information Command introduced in Junos OS Release 12.1X46-D25.

Description Display a brief summary of GPRS support node (GSN) statistics, including active GSNs, obsolete GSNs, and the usage rate of each SPU.

Required Privilege Level view

Related Documentation
- show security gprs gtp counters path-rate-limit on page 211

List of Sample Output show security gprs gtp gsn statistics on page 213

Sample Output

show security gprs gtp gsn statistics

```
user@host> show security gprs gtp gsn statistics
FPC 1 PIC 0:

Active GSNs: 0 Obsolete GSNs: 0 Use rate: 0%

FPC 2 PIC 0:

Active GSNs: 0 Obsolete GSNs: 0 Use rate: 0%
```

show security gprs sctp association

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax
show security gprs sctp association
<all>
<destination-ip>
<destination-port>
<guid>
<init-state>
<source-ip>
<source-port>
<summary>

Release Information Command introduced in Junos OS Release 12.1X44-D10. The **all**, **destination-ip**, **destination-port**, **guid**, **init**, **source-ip**, **source-port**, and **summary** options introduced in Junos OS Release 12.1X45-D10.

Description Display the Stream Control Transmission Protocol (SCTP) association information.

Options
none—Display the live security SCTP association.

all—Display information about all the SCTP associations, both initiated and live.

destination-ip—Display information about the destination IP address associations.

destination-port—Display information about the destination port associations.

guid—Display information about the globally unique identifier associations.

init—Display information about initiated associations.

source-ip—Display information about the source IP address associations.

source-port—Display information about the source port associations.

summary—Display the output summary.

Required Privilege Level view

Related Documentation
- clear security gprs sctp counters on page 201
- clear security gprs sctp association on page 199

List of Sample Output show security gprs sctp association on page 215

Output Fields Table 14 on page 215 lists the output fields for the **show security gprs sctp association** command. Output fields are listed in the approximate order in which they appear.

Table 14: show security gprs sctp association

Field Name	Field Description
Association Information	Association Information of FPC and PIC.
SCTP association numbers • Total association	Number of established SCTP associations. The SCTP association numbers field contains the total number of associations.
Association GUID	Globally unique association identifier information.

Sample Output

show security gprs sctp association

```
user@host>show security gprs sctp association


SCTP association numbers:
Total association 0

Association Information for FPC: 0      PIC: 1
SCTP association numbers:

Association GUID: 502a161a-a063bc44-0108000000001402
  source:
    10.3.202.118 (10.57.68.118)
    10.3.202.218 (10.57.68.218)
    port: 4215, state: SCTP_ESTABLISHED, tag: 0xe5d562d2;
  destination:
    172.28.34.206 (172.28.34.206)
    192.168.24.2 (192.168.24.2)
    port: 4215, state: SCTP_ESTABLISHED, tag: 0x631b82e4;
time left: 1786 s, access time: 45370 s;
policy id: sctp_policy/1, cfg live timeout: 30 min, handshake timeout: 20 s;

SCTP association numbers:
Total association 1

Association Information for FPC: 1      PIC: 0
SCTP association numbers:
Total association 0

Association Information for FPC: 1      PIC: 1
SCTP association numbers:
Total association 0
```

show security gprs sctp counters

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax **show security gprs sctp counters <detail>**

Release Information Command introduced in Junos OS Release 10.2. Support for the **detail** option added in Junos OS Release 12.1X45-D10. Support for SCTP payload protocols chunk counters added in Junos OS Release 12.1X47-D10.

Description Display the statistics of the received and dropped Stream Control Transmission Protocol (SCTP) chunks.

Options **none**—Display the statistics of all received and dropped SCTP chunks.

detail—Display detailed debugging counters for SCTP chunks.

Required Privilege Level view

Related Documentation
- clear security gprs sctp counters on page 201

List of Sample Output
show security gprs sctp counters on page 217
show security gprs sctp counters detail on page 220

Output Fields Table 15 on page 216 lists the output fields for the **show security gprs sctp counters** command. Output fields are listed in the approximate order in which they appear.

Table 15: show security gprs sctp counters

Field Name	Field Description
Name	Name of the SCTP payload protocol identifier.
Received Counter	Number of SCTP chunk counters received.
Drop Counter	Number of SCTP chunk counters dropped due to error.
Counter Information	Association information of FPC and PIC.
Association detail counters	(detail output only) Number of total and dying associations.
Dbg records	(detail output only) Number and type of debugging records.
Packet error	(detail output only) Number and type of packet errors.
Association matching error	(detail output only) Number of association matching errors.

Table 15: show security gprs sctp counters *(continued)*

Field Name	Field Description
Association state error	(detail output only) Number of state errors.
Over rate drop	(detail output only) Number of messages over the rate limit.
Memory counters	(detail output only) Number and type of memory counters.
Other error	(detail output only) Number and type of other errors.

Sample Output

show security gprs sctp counters

```
user@host> show security gprs sctp counters
Counter Information for FPC: 1 PIC: 0
Association detail counters:
Total association: 0
Dying association: 0
Ready wrap: 0

Dbg records:
pak-without-profile : 0
pak-nat-only : 0
pak-inspection : 0
drop-at-clearing-all : 0
src-pnat : 0
dst-pnat : 0
hostname : 0
dup-init : 0
dup-initack : 0
tag-null-abort : 0
error-chunk : 0
bad-interest : 0
wing-attach : 0
wing-detach : 0
wrap-with-assoc : 0
unwrap-from-assoc : 0
conflict-assoc : 0
conflict-redr : 0
wrong-distribution : 0

Packet error:
chunk-unsupport : 0
cookie-invalid : 0
pkt-len : 0
chunk-len : 0
tag-error : 0
bad-len : 0
bad-chk-hdr : 0

Association matching error:
ha-assoc : 0
data-assoc : 0
initack-assoc : 0
sack-assoc : 0
```

```
hb-assoc : 0
hb-ack-assoc : 0
abort-assoc : 0
shutdown-assoc : 0
shutdown-ack-assoc : 0
err-assoc : 0
cookie-echo-assoc : 0
cookie-ack-assoc : 0
shutdown-complete-assoc : 0
lookup-no-assoc : 0
dup-init-diff-ip-list : 0
dup-init-diff-dst-ip : 0
dup-initack-src-ip-invalid : 0
dup-initack-diff-ip-lis : 0

Associaiton state error:
data-state : 0
init-state : 0
initack-state : 0
sack-state : 0
shutdown-state : 0
shutdown-ack-state : 0
cookie-echo-state : 0
cookie-ack-state : 0
shutdown-complete-state : 0
cookie-echo-retrans-timeout : 0
cookie-ack-retrans-timeout : 0

Association LoadBalance counter:
redirect-assoc-request-send : 0
redirect-assoc-request-ack-recv : 0
redirect-assoc-request-nack-recv : 0
redirect-assoc-request-ack-timeoute : 0
redirect-assoc-request-recv : 0
redirect-assoc-request-ack-send : 0
redirect-assoc-request-nack-send : 0

Over rate drop:
sccp : 0
ssp : 0
sst : 0

Memory counters:
alloc-assoc : 0
free-assoc : 0
alloc-redr : 0
free-redr : 0
alloc-assoc-wrap : 0
free-assoc-wrap : 0
alloc-cookie : 0
free-cookie : 0
alloc-addr : 0
free-addr : 0

HA counters:
invalid-type : 0
bad-msg : 0
no-assoc-info : 0
send-fail : 0
dup-create : 0
no-policy : 0
```

```
no-profile : 0
alloc-fail : 0
non-established-issu: 0

Other error:
over-max : 0
over-min : 0
del-error : 0
sess-cookie-set-fail : 0
sess-cookie-get-fail : 0
no-assoc-install-redr-cb : 0
wrap-alloced-failure : 0
wrap-null-assocp : 0
assoc-alloced-failure : 0
redr-assoc-alloced-failure : 0
invalid-pkt-pointer : 0
nat-jbuf-alloc-fail : 0
evt-cookie-alloc-fail : 0
```

Sample Output

show security gprs sctp counters detail

```
user@host> show security gprs sctp counters detail
Counter Information for FPC: 1 PIC: 0
Association detail counters:
Total association: 0
Dying association: 0
Ready wrap: 0

Dbg records:
pak-without-profile : 0
pak-nat-only : 0
pak-inspection : 0
drop-at-clearing-all : 0
src-pnat : 0
dst-pnat : 0
hostname : 0
dup-init : 0
dup-initack : 0
tag-null-abort : 0
error-chunk : 0
bad-interest : 0
wing-attach : 0
wing-detach : 0
wrap-with-assoc : 0
unwrap-from-assoc : 0
conflict-assoc : 0
conflict-redr : 0
wrong-distribution : 0

Packet error:
chunk-unsupport : 0
cookie-invalid : 0
pkt-len : 0
chunk-len : 0
tag-error : 0
bad-len : 0
bad-chk-hdr : 0

Association matching error:
ha-assoc : 0
data-assoc : 0
initack-assoc : 0
sack-assoc : 0
hb-assoc : 0
hb-ack-assoc : 0
abort-assoc : 0
shutdown-assoc : 0
shutdown-ack-assoc : 0
err-assoc : 0
cookie-echo-assoc : 0
cookie-ack-assoc : 0
shutdown-complete-assoc : 0
lookup-no-assoc : 0
dup-init-diff-ip-list : 0
dup-init-diff-dst-ip : 0
dup-initack-src-ip-invalid : 0
dup-initack-diff-ip-lis : 0
```

```
Associaiton state error:
data-state : 0
init-state : 0
initack-state : 0
sack-state : 0
shutdown-state : 0
shutdown-ack-state : 0
cookie-echo-state : 0
cookie-ack-state : 0
shutdown-complete-state : 0
cookie-echo-retrans-timeout : 0
cookie-ack-retrans-timeout : 0

Association LoadBalance counter:
redirect-assoc-request-send : 0
redirect-assoc-request-ack-recv : 0
redirect-assoc-request-nack-recv : 0
redirect-assoc-request-ack-timeoute : 0
redirect-assoc-request-recv : 0
redirect-assoc-request-ack-send : 0
redirect-assoc-request-nack-send : 0

Over rate drop:
sccp : 0
ssp : 0
sst : 0

Memory counters:
alloc-assoc : 0
free-assoc : 0
alloc-redr : 0
free-redr : 0
alloc-assoc-wrap : 0
free-assoc-wrap : 0
alloc-cookie : 0
free-cookie : 0
alloc-addr : 0
free-addr : 0

HA counters:
invalid-type : 0
bad-msg : 0
no-assoc-info : 0
send-fail : 0
dup-create : 0
no-policy : 0
no-profile : 0
alloc-fail : 0
non-established-issu: 0

Other error:
over-max : 0
over-min : 0
del-error : 0
sess-cookie-set-fail : 0
sess-cookie-get-fail : 0
no-assoc-install-redr-cb : 0
wrap-alloced-failure : 0
wrap-null-assocp : 0
assoc-alloced-failure : 0
```

```
redr-assoc-alloced-failure : 0
invalid-pkt-pointer : 0
nat-jbuf-alloc-fail : 0
evt-cookie-alloc-fail : 0
```