



Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide

Version 12.0

Last Updated April 30, 2011

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24894-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide

© 2011 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide	V
Conventions Used.....	vi
Contacting Customer Support	viii
Personal Stateful Firewall Overview	9
Supported Platforms and Products	10
Licenses	11
Overview	12
Supported Features	13
Protection against Denial-of-Service Attacks	13
Types of Denial-of-Service Attacks.....	13
Protection against Port Scanning	16
Application-level Gateway Support.....	16
PPTP ALG Support	16
TFTP ALG Support	17
Stateful Packet Inspection and Filtering Support.....	17
Stateless Packet Inspection and Filtering Support	17
Host Pool, IMSI Pool, and Port Map Support	18
Host Pool Support.....	18
IMSI Pool Support	18
Port Map Support.....	18
Flow Recovery Support.....	18
SNMP Thresholding Support	19
Logging Support	19
How Personal Stateful Firewall Works	21
Disabling Firewall Policy	21
Mid-session Firewall Policy Update.....	22
How it Works.....	22
Understanding Rules with Stateful Inspection	26
Connection State and State Table in Personal Stateful Firewall.....	27
Transport and Network Protocols and States	27
Application-Level Traffic and States	29
Personal Stateful Firewall Configuration	31
Before You Begin.....	32
Configuring the System.....	33
Configuring Stateful Firewall.....	34
Enabling the ECS Subsystem and Creating the ECS Service	35
Configuring Port Maps	35
Configuring Host Pools	35
Configuring IMSI Pools	36
Configuring Access Ruledefs	37
Configuring Firewall-and-NAT Policies	38
Configuring Protection from DoS and Other Attacks.....	38
Configuring Maximum Number of Servers to Track for DoS Attacks	41
Configuring Action on Packets Dropped by Stateful Firewall.....	41
Configuring Dynamic Pinholes/ALGs.....	42





Creating Routing Ruledefs	42
Configuring Routing Ruledefs in the Rulebase	43
Enabling Stateful Firewall Support for APN/Subscribers	43
Enabling Stateful Firewall for APN.....	43
Enabling Stateful Firewall for Subscribers	44
Enabling IPv4/IPv6 Stateful Firewall for Subscribers	44
Configuring Default Firewall-and-NAT Policy.....	45
Configuring Stateful Firewall Thresholds	45
Enabling Thresholds	45
Configuring Threshold Poll Interval.....	45
Configuring Threshold Limits	46
Configuring Bulk Statistics Schema.....	46
Configuring Flow Recovery	47
Optional Configurations.....	48
Changing Stateful Firewall Policy in Mid-session	48
Configuring Stateless Firewall	48
Saving the Configuration	50
Gathering Stateful Firewall Statistics.....	51
Managing Your Configuration	52
Verifying and Saving Your Configuration	55
Verifying the Configuration	56
Feature Configuration.....	56
Service Configuration.....	66
Context Configuration.....	66
System Configuration.....	66
Finding Configuration Errors	67
Saving the Configuration	68
Saving the Configuration on the Chassis	69
Sample Personal Stateful Firewall Configuration	71

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: Login:
Text represented as commands	This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a command variable	This typeface represents a variable that is part of a command, for example: show card slot_number slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Command Syntax Conventions	Description
{ keyword or <i>variable</i> }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[keyword or <i>variable</i>]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
	<p>With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter).</p> <p>Pipe filters can be used in conjunction with required or optional keywords or variables. For example:</p> <p>{ nonce timestamp }</p> <p>OR</p> <p>[count <i>number_of_packets</i> size <i>number_of_bytes</i>]</p>

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of <http://www.cisco.com> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of <https://support.starentnetworks.com/> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.



Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1

Personal Stateful Firewall Overview

This chapter provides an overview of the Personal Stateful Firewall In-line Service.

This chapter covers the following topics:

- [Supported Platforms and Products](#)
- [Licenses](#)
- [Overview](#)
- [Supported Features](#)
- [How Personal Stateful Firewall Works](#)
- [Understanding Firewall Rules with Stateful Inspection](#)

Supported Platforms and Products

The Personal Stateful Firewall is an in-line service feature available on the Cisco ASR 5000 chassis running 3GPP, 3GPP2, and WiMAX core network services.



Important: For information on ASR 5000, please refer to the *Product Overview Guide*.

Licenses

The Personal Stateful Firewall is a licensed in-line service feature requiring the following license:

Cisco PID [ASR5K-00-CS01FW] *Per-Subscriber Stateful Firewall, 1K Sessions*, or Starent part number [600-00-7571] *Per Subscriber Stateful Firewall 1k sessions*



Important: For information on license requirements for any customer-specific features, please contact your local sales/service representative.



Important: For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Overview

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.

In stateless inspection, the firewall inspects a packet to determine the 5-tuple—source and destination IP addresses and ports, and protocol—information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer / layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state. For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgement numbers of the packets traversing the connection, TCP packet flags, etc. is maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded. For more information see the [Connection State and State Table in Personal Stateful Firewall](#) section.

The Enhanced Charging Service (ECS) / Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

Supported Features

The Personal Stateful Firewall supports the following features:

- [Protection against DoS Attacks](#)
- [Application-level Gateway \(ALG\) Support](#)
- [Stateful Packet Filtering and Inspection Support](#)
- [Stateless Packet Filtering and Inspection Support](#)
- [Host Pool, IMSI Pool, and Port Map Support](#)
- [Flow Recovery Support](#)
- [SNMP Thresholding Support](#)
- [Logging Support](#)

Protection against Denial-of-Service Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks can deprive network resources/services unavailable to its intended users.

DoS attacks can result in:

- A host consuming excessive resources — memory, disk space, CPU time, etc. — eventually leading to a system crash or providing very sluggish response.
- Flooding of the network to the extent that no valid traffic is able to reach the intended destination.
- Confusing target TCP/IP stack on destination hosts by sending crafted, malformed packets eventually resulting in system crash.

In this release, malformity check is enhanced for IPv6 and ICMPv6 packets. Port-scan and Flooding attacks are also enhanced to support IPv6. Protection against other L4 attacks are similar to IPv4. The Attacking server feature is also enhanced to store IPv6 servers.

DoS attacks can destroy data in affected mobile nodes. Stateful Firewall is designed to defend subscribers and prevent the abuse of network bandwidth from DoS attacks originating from both the Internet and the internal network.

Types of Denial-of-Service Attacks

Personal Stateful Firewall can detect the following DoS attacks.

The DoS attacks are listed based on the protocol layer that they work on.

- IP-based Attacks:
 - Land attacks
 - Jolt attacks
 - Teardrop attacks — Detected only in downlink direction, i.e. traffic coming from the external network towards the mobile subscribers
 - Invalid IP option length
 - IP-unaligned-timestamp attack — Detected only in downlink direction
 - Short IP header length
 - IP checksum errors
 - IP reassembly failure (downlink)
 - IP reassembly failure (uplink)
 - Source router — Detected only in downlink direction
 - IPv6 header checks
- TCP-based Attacks:
 - Data packets received after RST/FIN
 - Invalid SEQ number received with RST
 - Data without connection established
 - Invalid TCP connection requests
 - Invalid TCP pre-connection requests
 - Invalid ACK value (cookie enabled)
 - Invalid TCP packet length
 - Short TCP header length
 - TCP checksum errors
 - SEQ/ACK out-of-range
 - TCP null scan attacks
 - Post connection SYN
 - No TCP flags set
 - All TCP flags set
 - Invalid TCP packets
 - Flows closed by RST before 3-Way handshake
 - Flows timed-out in SYN_RCVD1 state
 - Flows timed-out in SYN_RCVD2 state
 - TCP-SYN flood attacks — Detected only in downlink direction
 - FTP bounce attack — Detected only in downlink direction
 - MIME flood attacks — Detected only in downlink direction
 - Exceeding reset message threshold

- Source port zero
- WinNuke attack — Detected only in downlink direction
- TCP-window-containment — Detected only in downlink direction
- UDP-based Attacks:
 - Invalid UDP echo response
 - Invalid UDP packet length
 - UDP checksum errors
 - Short UDP header length
 - UDP flood attack — Detected only in downlink direction
- ICMP-based Attacks:
 - Invalid ICMP response
 - ICMP reply error
 - Invalid ICMP type packet
 - ICMP error message replay attacks
 - ICMP packets with duplicate sequence number
 - Short ICMP header length
 - Invalid ICMP packet length
 - ICMP flood attack — Detected only in downlink direction
 - Ping of death attacks
 - ICMP checksum errors
 - ICMP packets with destination unreachable message
 - ICMP echo packets with ID zero
- Other DoS Attacks:
 - Port-scan attacks — Detected only in downlink direction

Various header integrity checks are performed for IPv6 to ensure the integrity of an IPv6 packet. IPv6 packets with unknown extension headers will not be dropped by Firewall; such packets will be allowed by Firewall. Firewall performs the following header checks:

- Limiting extension headers
- Hop-by-hop Options filtering
- Destination Options filtering
- Router Header filtering
- Fragment Header filtering

Protection against Port Scanning

Port scanning is a technique used to determine the states of TCP/UDP ports on a network host, and to map out hosts on a network. Essentially, a port scan consists of sending a message to each port on the host, one at a time. The kind of response received indicates whether the port is used, and can therefore be probed further for weakness. This way hackers find potential weaknesses that can be exploited.

Stateful Firewall provides protection against port scanning by implementing port scan detection algorithms. Port-scan attacks are only detected in the downlink direction—traffic from external network towards mobile subscribers.

Application-level Gateway Support

A stateful firewall while ensuring that only legitimate connections are allowed, also maintains the state of an allowed connection. Some network applications require additional connections to be opened up in either direction and information regarding such connections is sent in the application payload. For these applications to work properly, a stateful firewall must inspect, analyze, and parse these application payloads to get the additional connection information, and open partial connections/pinholes in the firewall to allow the connections.

To parse application payloads, firewall employs ALGs. ALGs also check for application-level attacks. Personal Stateful Firewall provides ALG functionality for the following protocols:

- File Transfer Protocol (FTP)
- Real Time Protocol (RTP)
- Real Time Streaming Protocol (RTSP)
- Point-to-Point Tunneling Protocol (PPTP)
- Trivial File Transfer Protocol (TFTP)

ALG support for Simple Mail Transfer Protocol (SMTP) and HTTP is ECS functionality. The ALGS listed above also support IPv6 traffic.

H323 and SIP ALGs work only for IPv4 traffic. For IPv6 traffic, Stateful Firewall is bypassed.

PPTP ALG Support

PPTP exchanges IP or port specific information over its control connection and that information will be used to transfer the data over tunnel. If a PPTP client resides behind NAT and uses private IP to communicate with the outside world, it is possible that the information exchange over PPTP control flow consists of private IPs. So NAT translates the private IP specific information to public IP (NATed IP) for good communication. To achieve this, PPTP ALG is supported.

To establish a GRE session, PPTP exchanges call IDs from both peers to form a unique triple value, that is, client IP, server IP and Call ID. For Many-to-One NAT, PPTP analyzer is implemented to analyze the PPTP Control Flow traffic. It can be configured to send all the PPTP Control Flow packets to PPTP analyzer. PPTP analyzer analyzes the packet and allocates a new unique Call ID. Packet payload will be modified for the new Call ID and the binding between the two Call IDs will be maintained. Similarly, the PPTP first packet will be NAT-ed, Call ID translated and sent to the PPTP Server. This Call ID translation happens for all the downlink packets after the first packet. For GRE Data Tunnel

Flow translation, it can be configured to send all the GRE downlink packets to PPTP analyzer. PPTP analyzer then analyzes the GRE header and translates the GRE Call ID if a Call ID binding exists.

TFTP ALG Support

Trivial File Transfer Protocol (TFTP) ALG enables Firewall or NAT enabled users to seamlessly use applications using TFTP Protocol. TFTP ALG feature analyzes the TFTP packets and selectively allows the downlink data flow by creating pin holes. This feature also ensures NAT/PAT IP/Port translation for NAT enabled users.

TFTP ALG analyzes the packets for basic TFTP signatures. A TFTP analyzer is implemented for this purpose. A routing rule is created for routing the packets to TFTP analyzer. Potential TFTP packets are parsed and information like query type and mode are stored. After confirming that the packet is TFTP, a dynamic route is created for MS IP, MS Port, Server IP and Protocol. When the data flow starts, dynamic route is matched and data is sent to the TFTP analyzer. For NAT enabled calls, same Client port used for the control connection will be used for Data flow.

Stateful Packet Inspection and Filtering Support

As described in the Overview section, stateful packet inspection and filtering uses Layer-4 information as well as the application-level commands up to Layer-7 to provide good definition of the individual connection states to defend from malicious security attacks.

Personal Stateful Firewall overcomes the disadvantages of static packet filters by disallowing any incoming packets that have the TCP SYN flag set (which means a host is trying to initiate a new connection). If configured, stateful packet filtering allows only packets for new connections initiated from internal hosts to external hosts and disallows packets for new connections initiated from external hosts to internal hosts.

TCP stateful processing is enhanced for processing IPv6 packets. The functionality is similar to IPv4 packets.

Stateless Packet Inspection and Filtering Support

Stateful Firewall service can be configured for stateless processing. In stateless processing, packets are inspected and processed individually.

Stateless processing is only applicable for TCP and ICMP protocols. By nature UDP is a stateless protocol without any kind of acking or request and reply mechanism at transport level.

When TCP FSM is disabled, flows can start with any kind of packet and need not respect the TCP FSM. Such flows are marked as dummy (equivalent to flows established during flow recovery timer running). For these flows only packet header check is done; there will be no FSM checks, sequence number validations, or port scan checks done.

When ICMP FSM is disabled, ICMP reply without corresponding requests, ICMP error message without inner packet data session, and duplicate ICMP requests are allowed by firewall.

Host Pool, IMSI Pool, and Port Map Support

This section describes the Host Pool, IMSI Pool, and Port Map features that can be used while configuring access ruledefs.

Host Pool Support

Host pools allow operators to group a set of host or IP addresses that share similar characteristics together. Access rule definitions (ruledefs) can be configured with host pools. Up to 10 sets of IP addresses can be configured in each host pool. Host pools are configured in the ACS Host Pool Configuration Mode.

Host pools are enhanced to support IPv6 addresses and address ranges. It can also be a combination of IPv4 and IPv6 addresses.

IMSI Pool Support

IMSI pools allow the operator to group a set of International Mobile Station Identifier (IMSI) numbers together. Up to 10 sets of IMSI numbers can be configured in each IMSI pool. IMSI pools are configured in the ACS IMSI Pool Configuration Mode.

Port Map Support

Port maps allow the operator to group a set of port numbers together. Access ruledefs can be configured with port maps. Up to 10 sets of ports can be configured in each port map. Port maps are configured in the ACS Port Map Configuration Mode.

The Personal Stateful Firewall uses standard application ports to trigger ALG functionality. The operator can modify the existing set to remove/add new port numbers.

Flow Recovery Support

Stateful Firewall supports call recovery during session failover. Flows associated with the calls are recovered.

A recovery-timeout parameter is configurable for uplink and downlink directions. If the value is set to zero, firewall flow recovery is disabled. If the value is non-zero, then firewall will be bypassed for packets from MS/Internet until the time configured (uplink/downlink). Once the manager recovers, the recovery-timeout timer is started. During this time:

- If any ongoing traffic arrives from the subscriber and no association is found, and flow recovery is enabled, basic checks like header processing, attacks, etc. are done (stateful checks of packet is not done), and if all is okay, an association is created and the packet is allowed to pass through.

- If any ongoing traffic arrives from the Internet to MS and no association is found, and flow recovery is not enabled, it is dropped. No RESET is sent. Else, basic checks like header processing, flooding attack check are done (stateful checks are not done), and if all is okay, an association is created and the packet is allowed to pass through.
- In case flow recovered from ongoing traffic arrives from Internet to MS, and MS sends a NACK, the Unwanted Traffic Suppression feature is triggered, i.e. upon repeatedly receiving NACK from MS for a 5-tuple, further traffic to the 5-tuple is blocked for some duration and not sent to MS.
- If any new traffic (3-way handshake) comes, whether it is a new flow or a new flow due to pin-hole, based on the direction of packet and flow-recovery is enabled, basic checks like header processing, attacks, etc. are done (stateful checks are not done) and if all is okay, an association is created and the packet is allowed to pass through.

For any traffic coming after the recovery-timeout:

- If any ongoing traffic arrives, it is allowed only if an association was created earlier. Else, it is dropped and reset is sent.
- If any new traffic (3-way handshake) arrives, the usual Stateful Firewall processing is done.

If recovery-timeout value is set to zero, Stateful Firewall flow recovery is not done.

Stateful Firewall now supports IPv6 flows recovery similar to IPv4 flows.

SNMP Thresholding Support

Personal Stateful Firewall allows to configure thresholds to receive notifications for various events that are happening in the system. Whenever a measured value crosses the specified threshold value at the given time, an alarm is generated. And, whenever a measured value falls below the specified threshold clear value at the given time, a clear alarm is generated. The following events are supported for generating and clearing alarms:

- Dos-Attacks: When the number of DoS attacks crosses a given value, a threshold is raised, and it is cleared when the number of DoS attacks falls below a value in a given period of time.
- Drop-Packets: When the number of dropped packets crosses a given value, a threshold is raised, and it is cleared when the number of dropped packets falls below a value in a given period of time.
- Deny-Rule: When the number of Deny Rules cross a given value, a threshold is raised, and it is cleared when the number of Deny Rules falls below a value in a given period of time.
- No-Rule: When the number of No Rules cross a given value, a threshold is raised, and it is cleared when the number of No Rules falls below a value in a given period of time.

Logging Support

Stateful Firewall supports logging of various messages on screen if logging is enabled for firewall. These logs provide detailed messages at various levels, like critical, error, warning, and debug. All the logs displaying IP addresses are enhanced to display IPv6 addresses.

■ Supported Features

Logging is also supported at rule level, when enabled through rule a message will be logging whenever a packet hits the rule. This can be turned on/off in a rule.

These logs are also sent to a syslog server if configured in the system.

How Personal Stateful Firewall Works

This section describes how Personal Stateful Firewall works.



Important: In release 8.x, Stateful Firewall for CDMA and early UMTS releases used rulebase-based configurations, whereas later UMTS releases used policy-based configurations. In release 9.0, Stateful Firewall for UMTS and CDMA releases, both use policy-based configurations. For more information, please contact your local service representative.

Firewall-and-NAT policies are configured in the Firewall-and-NAT Policy Configuration Mode. Each policy contains a set of access ruledefs and the firewall configurations. Multiple such policies can be configured, however, only one policy is applied to a subscriber at any point of time.

The policy used for a subscriber can be changed either from the CLI, or by dynamic update of policy name in Diameter and RADIUS messages.

The Firewall-and-NAT policy to be used for a subscriber can be configured in:

- **ACS Rulebase:** The default Firewall-and-NAT policy configured in the ACS rulebase has the least priority. If there is no policy configured in the APN/subscriber template, and/or no policy to use is received from the AAA/OCS, only then the default policy configured in the ACS rulebase is used.
- **APN/Subscriber Template:** The Firewall-and-NAT policy configured in the APN/subscriber template overrides the default policy configured in the ACS rulebase. To use the default policy configured in the ACS rulebase, in the APN/subscriber configuration, the command to use the default rulebase policy must be configured.
- **AAA/OCS:** The Firewall-and-NAT policy to be used can come from the AAA server or the OCS. If the policy comes from the AAA/OCS, it will override the policy configured in the APN/subscriber template and/or the ACS rulebase.



Important: The Firewall-and-NAT policy received from the AAA and OCS have the same priority. Whichever comes latest, either from AAA/OCS, is applied.

The Firewall-and-NAT policy to use can be received from RADIUS during authentication.

Disabling Firewall Policy



Important: By default, Stateful Firewall processing for subscribers is disabled.

Stateful Firewall processing is disabled for subscribers in the following cases:

- If Stateful Firewall is explicitly disabled in the APN/subscriber template configuration.

- If the AAA/OCS sends the SN-Firewall-Policy AVP with the string “disable”, the locally configured firewall policy does not get applied.
- If the SN-Firewall-Policy AVP is received with the string “NULL”, the existing policy will continue.
- If the SN-Firewall-Policy AVP is received with a name that is not configured locally, the subscriber session is terminated.

Mid-session Firewall Policy Update

The Firewall-and-NAT policy can be updated mid-session provided firewall policy was enabled during call setup.



Important: When the firewall AVP contains “disable” during mid-session firewall policy change, there will be no action taken as the Firewall-and-NAT policy cannot be disabled dynamically. The policy currently applied will continue.



Important: When a Firewall-and-NAT policy is deleted, for all subscribers using the policy, Firewall processing is disabled, also ECS sessions for the subscribers are dropped. In case of session recovery, the calls are recovered but with Stateful Firewall disabled.

How it Works

The following figures illustrate packet flow in Stateful Firewall processing for a subscriber.

Figure 1. Stateful Firewall Processing

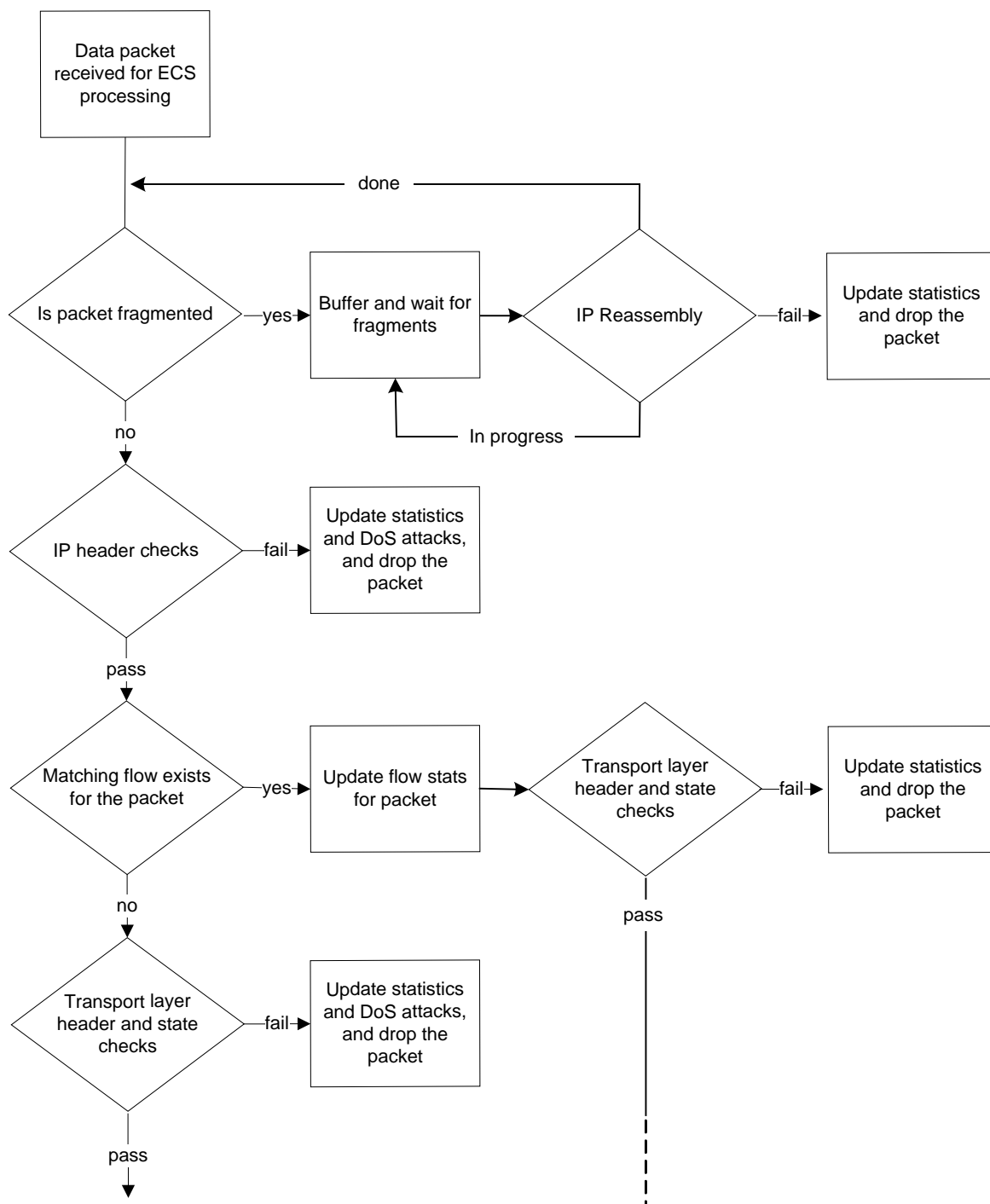


Figure 2. Continued... Stateful Firewall Processing

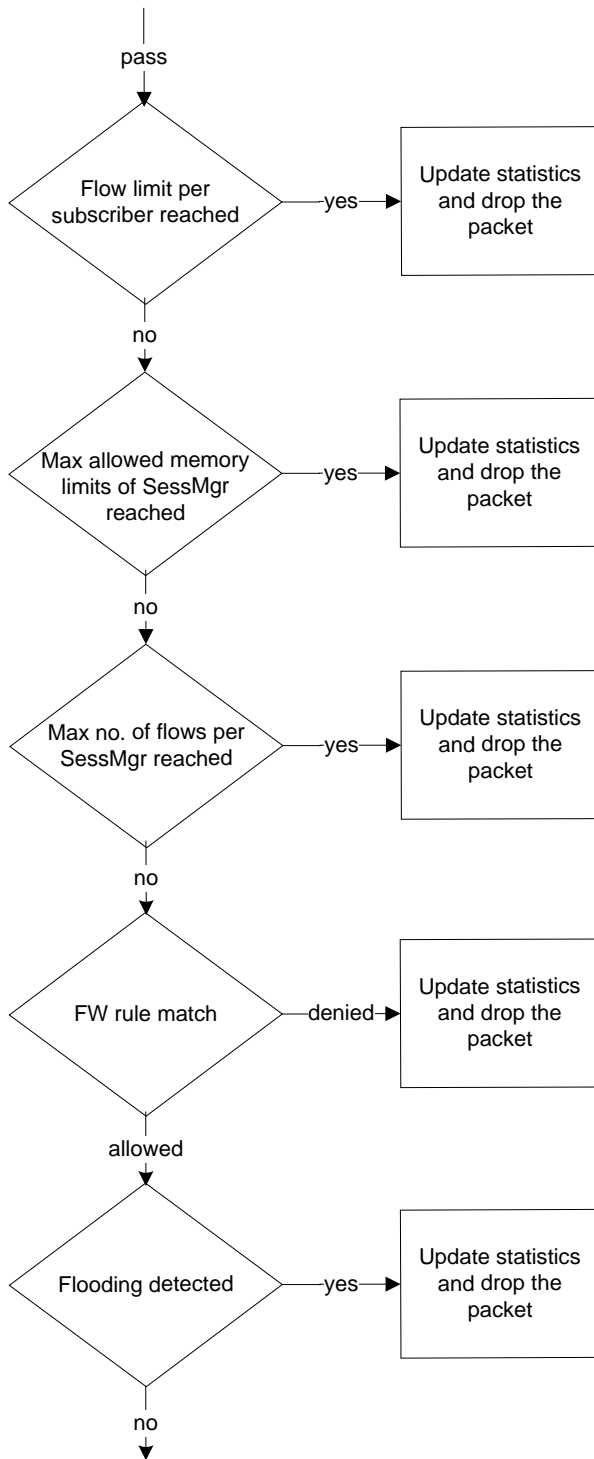
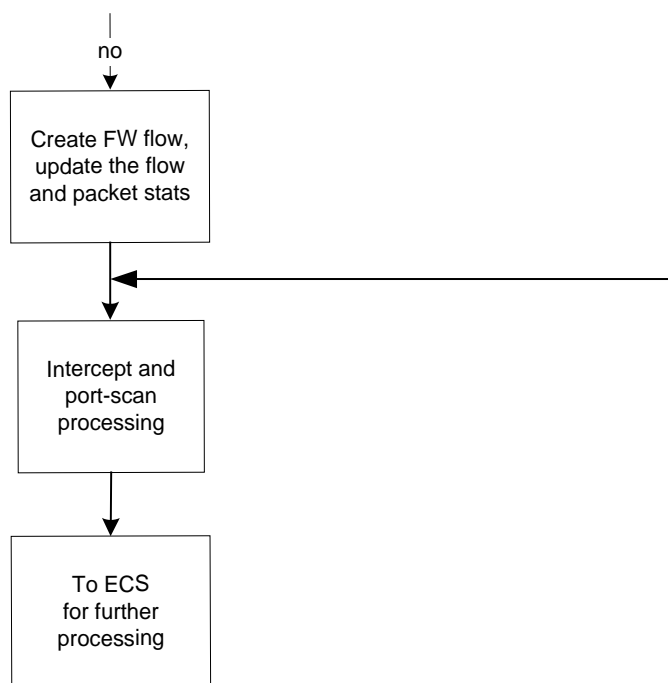


Figure 3. Continued... Stateful Firewall Processing



Understanding Rules with Stateful Inspection

This section describes terms used in the Personal Stateful Firewall context.

- **Access Ruledefs:** The Personal Stateful Firewall's stateful packet inspection feature allows operators to configure rule definitions (ruledefs) that take active session information into consideration to permit or deny incoming or outgoing packets.

An access ruledef contains the criteria for multiple actions that could be taken on packets matching the rules. These rules specify the protocols, source and destination hosts, source and destination ports, direction of traffic parameters for a subscriber session to allow or reject the traffic flow.

An access ruledef consists of the following fields:

- Ruledef name
- Source IP address
- Source port number — not required if the protocol is other than TCP or UDP
- Destination IP address
- Destination port number — not required if the protocol is other than TCP or UDP
- Transport protocol (TCP/UDP/ICMP/ICMPv6/AH/ESP)
- Direction of connection (Uplink/Downlink)
- Bearer (IMSI-pool and APN)
- Logging action (enable/disable)
- IP version - IPv4 or IPv6

An access ruledef can be added to multiple Firewall-and-NAT policies.

A combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + firewall/access ruledefs + routing ruledefs) can be created in a system. Access ruledefs are different from ACS ruledefs.

In release 12.0, Firewall access ruledefs are enhanced to support IPv6 addresses and parameters like IP version and ICMPv6 protocol. The existing rule lines "ip src-address" and "ip dst-address" are capable of accepting both IPv4 and IPv6 addresses hence there is no CLI level change for them.

- **Firewall-and-NAT Policy:** Firewall policies can be created for individual subscribers, domains, or all callers within a referenced context. Each policy contains a set of access ruledefs with priorities defined for each rule and the firewall configurations. Firewall-and-NAT policies are configured in the Firewall-and-NAT Policy Configuration Mode.
- **Service Definition:** User-defined firewall service for defining Stateful Firewall policy for initiating an outgoing connection on a primary port and allowing opening of auxiliary ports for that association in the reverse direction.
- **Maximum Association:** The maximum number of Stateful Firewall associations for a subscriber.

Connection State and State Table in Personal Stateful Firewall

This section describes the state table and different connection states for transport and network protocols.

After packet inspection, the Personal Stateful Firewall stores session state and other information into a table. This state table contains entries of all the communication sessions of which the firewall subsystem is aware of. Every entry in this table holds a list of information that identifies the subscriber session it represents. Generally this information includes the source and destination IP address, flags, sequence, acknowledgement numbers, etc.

When a connection is permitted through the Personal Stateful Firewall enabled chassis, a state entry is created. If a session connection with same information (source address, source port, destination address, destination port, protocol) is requested the firewall subsystem compares the packet's information to the state table entry to determine the validity of session. If the packet is currently in a table entry, it allows it to pass, otherwise it is dropped.

Transport and Network Protocols and States

Transport protocols have their connection's state tracked in various ways. Many attributes, including IP address and port combination, sequence numbers, and flags are used to track the individual connection. The combination of this information is kept as a hash in the state table.

TCP Protocol and Connection State

TCP is considered as a stateful connection-oriented protocol that has well defined session connection states. TCP tracks the state of its connections with flags as defined for TCP protocol. The following table describes different TCP connection states.

Table 1. TCP Connection States

State Flag	Description
TCP (Establishing Connection)	
CLOSED	A “non-state” that exists before a connection actually begins.
LISTEN	The state a host is in waiting for a request to start a connection. This is the starting state of a TCP connection.
SYN-SENT	The time after a host has sent out a SYN packet and is waiting for the proper SYN-ACK reply.
SYN-RCVD	The state a host is in after receiving a SYN packet and replying with its SYN-ACK reply.
ESTABLISHED	The state a host is in after its necessary ACK packet has been received. The initiating host goes into this state after receiving a SYN-ACK.
TCP (Closing Connection)	
FIN-WAIT-1	The state a connection is in after it has sent an initial FIN packet asking for a graceful termination of the TCP connection.
CLOSE-WAIT	The state a host's connection is in after it receives an initial FIN and sends back an ACK to acknowledge the FIN.

State Flag	Description
FIN-WAIT-2	The connection state of the host that has received the ACK response to its initial FIN, as it waits for a final FIN from its connection peer.
LAST-ACK	The state of the host that just sent the second FIN needed to gracefully close the TCP connection back to the initiating host while it waits for an acknowledgement.
TIME-WAIT	The state of the initiating host that received the final FIN and has sent an ACK to close the connection and waiting for an acknowledgement of ACK from the connection peer. Note that the amount of time the TIME-STATE is defined to pause is equal to the twice of the Maximum Segment Lifetime (MSL), as defined for the TCP implementation.
CLOSING	A state that is employed when a connection uses the unexpected simultaneous close.

UDP Protocol and Connection State

UDP is a connection-less transport protocol. Due to its connection-less nature, tracking of its state is a more complicated process than TCP. The Personal Stateful Firewall tracks a UDP connection in a different manner than TCP. A UDP packet has no sequence number or flag field in it. The port numbers used in UDP packet flow change randomly for any given session connection. So the Personal Stateful Firewall keeps the status of IP addresses.

UDP traffic cannot correct communication issues on its own and it relies entirely on ICMP as its error handler. This method makes ICMP an important part of a UDP session for tracking its overall state.

UDP has no set method of connection teardown that announces the session's end. Because of the lack of a defined ending, the Personal Stateful Firewall clears a UDP session's state table entries after a preconfigured timeout value reached.

ICMP Protocol and Connection State

ICMP is also a connection-less network protocol. The ICMP protocol is often used to return error messages when a host or protocol cannot do so on its own. ICMP response-type messages are precipitated by requests using other protocols like TCP or UDP. This way of messaging and its connection-less and one-way communication make the tracking of its state a much more complicated process than UDP. The Personal Stateful Firewall tracks an ICMP connection based on IP address and request message type information in a state table.

Like UDP, the ICMP connection lacks a defined session ending process, the Personal Stateful Firewall clears a state table entry on a predetermined timeout.

Firewall now supports ICMP Traceroute to handle ICMP packets with type value 30 that were being dropped. ICMP packets with ICMP type value 30 are called ICMP Traceroute packets.

It is now possible to allow/deny the ICMP echo packets having identifier value zero. By default, these packets are allowed. This feature will be effective only if Firewall is enabled (Firewall or Firewall+NAT) for a call. For only NAT enabled calls, there is no change in the behavior. Configuration is available only if Firewall license is present.

Application-Level Traffic and States

The Personal Stateful Firewall uses Deep Packet Inspection (DPI) functionality to manage application-level traffic and its state. With the help of DPI functionality, the Personal Stateful Firewall inspects packets up to Layer-7. It takes application behaviors into account to verify that all session-related traffic is properly handled and then decides which traffic to allow into the network.

Different applications follow different rules for communication exchange so the Personal Stateful Firewall manages the different communication sessions with different rules through DPI functionality.

The Personal Stateful Firewall also provides inspection and filtering functionality on application content with DPI. Personal Stateful Firewall is responsible for performing many simultaneous functions and it detect, allow, or drop packets at the ingress point of the network.

HTTP Application and State

HTTP is the one of the main protocols used on the Internet today. It uses TCP as its transport protocol, and its session initialization follows the standard TCP connection method.

Due to the TCP flow, the HTTP allows an easier definition of the overall session's state. It uses a single established connection from the client to the server and all its requests are outbound and responses are inbound. The state of the connection matches with the TCP state tracking.

For content verification and validation on the HTTP application session, the Personal Stateful Firewall uses DPI functionality in the chassis.

PPTP Application and State

Point-to-Point Tunneling Protocol (PPTP) is one of the protocols widely used to achieve Virtual Private Networks (VPN). PPTP allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) to carry PPP packets.

PPTP protocol has 2 connection states - Control connection (TCP) and Data connection (GREv1). PPTP exchanges IP or port specific information over its control connection and that information will be used to transfer the data over tunnel. If a PPTP client resides behind NAT and uses private IP to communicate with the outside world, it is possible that the information exchange over PPTP control flow has private IPs.

TFTP Application and State

Trivial File Transfer Protocol (TFTP) is an application layer protocol which is used by File Transfer applications. TFTP uses UDP (User Datagram Protocol) as its transport protocol and has only basic functionalities. TFTP file operations include sending a file and receiving a file. TFTP supports different modes for File Transfer which are netascii, ascii, octet, and binary.

TFTP has two connection states - Control connection and Data connection that operate on UDP. Initially, TFTP starts the control flow (uses UDP Port 69) for communicating the type of file operation to be performed. The Client initiates the connection towards Server on port 69 (UDP). Server replies to the Client from a port other than 69 and data is transferred in this flow. Negative reply is sent using different error codes supported by TFTP.

File Transfer Protocol and State

FTP is an application to move files between systems across the network. This is a two way connection and uses TCP as its transport protocol.

Due to TCP flow, FTP allows an easier definition of the overall session's state. As it uses a single established connection from the client to the server, the state of the connection matches with the TCP state tracking.

Personal Stateful Firewall uses application-port mapping along with FTP application-level content verification and validation with DPI functionality in the chassis. It also supports Pinhole data structure and Initialization, wherein FTP ALG parses FTP Port command to identify the initiation and termination end points of future FTP DATA sessions. The source/destination IP and destination Port of FTP DATA session is stored.

When a new session is to be created for a call, a check is made to see if the source/destination IP and Destination Port of this new session matches with the values stored. Upon match, a new ACS data session is created.

This lookup in the pinhole list is made before port trigger check and stateful firewall ruledef match. If the look up returns a valid pinhole then a particular session is allowed. Whenever a new FTP data session is allowed because of a pinhole match the associated pinhole is deleted. Pinholes are also expired if the associated FTP Control session is deleted in, or when the subscriber call goes down.

Chapter 2

Personal Stateful Firewall Configuration

This chapter describes how to configure the Personal Stateful Firewall in-line service feature.



Important: In release 8.x, Stateful Firewall for CDMA and early UMTS releases used rulebase-based configurations, whereas in later UMTS releases Stateful Firewall used policy-based configurations. In release 9.0, Stateful Firewall for UMTS and CDMA releases both use policy-based configurations. For more information, please contact your local service representative.

This chapter covers the following topics:

- [Configuring the System](#)
- [Stateful Firewall Configuration](#)
- [Optional Configurations](#)
- [Saving the Configuration](#)
- [Gathering Stateful Firewall Statistics](#)
- [Managing Your Configuration](#)

Before You Begin

This section lists the steps to perform before you can start configuring Stateful Firewall support on a system.

- Step 1 Configure the required core network service on the system as described in the *System Administration Guide*.
- Step 2 Obtain and install the required feature licenses for the required number of subscriber sessions.
- Step 3 Proceed to the [Configuring the System](#) section.

Configuring the System

This section lists the high-level steps to configure Stateful Firewall support on a system.



Important: In release 8.x, Stateful Firewall for CDMA and early UMTS releases used rulebase-based configurations, whereas later UMTS releases used policy-based configurations. In release 9.0, Stateful Firewall for UMTS and CDMA releases both use policy-based configurations. For more information, please contact your local service representative.

- Step 1 Configure Stateful Firewall support as described in the [Stateful Firewall Configuration](#) section.
- Step 2 Save changes to the system configuration as described in the [Saving the Configuration](#) section.

Configuring Stateful Firewall

This section describes how to configure Stateful Firewall support in a system.



Important: In release 8.x, Stateful Firewall for CDMA and early UMTS releases used rulebase-based configurations, whereas later UMTS releases used policy-based configurations. In release 9.0, Stateful Firewall for UMTS and CDMA releases both use policy-based configurations. For more information, please contact your local service representative.

- Step 1 Enable the Enhanced Charging Service (ECS) subsystem and create the ECS service as described in the [Enabling the ECS Subsystem and Creating the ECS Service](#) section.
- Step 2 *Optional:* Configure application-port maps for TCP and UDP protocols as described in the [Configuring Port Maps](#) section.
- Step 3 *Optional:* Configure host pools as described in the [Configuring Host Pools](#) section.
- Step 4 *Optional:* Configure IMSI pools as described in the [Configuring IMSI Pools](#) section.
- Step 5 Configure access ruledefs as described in the [Configuring Access Ruledefs](#) section.
- Step 6 Configure Firewall-and-NAT policies as described in the [Configuring Firewall-and-NAT Policy](#) section.
- Step 7 Configure protection from DoS and other attacks as described in the [Configuring Other Firewall Settings](#) section.
- Step 8 Configure ALGs as described in the [Configuring Dynamic PinholesALGs](#) section.
- Step 9 Enable Stateful Firewall support for APN/subscribers as described in the [Enabling Firewall for APNSubscribers](#) section.
- Step 10 *Optional:* Configure the default Firewall-and-NAT policy as described in the [Configuring Default Firewall-and-NAT Policy](#) section.
- Step 11 Configure Stateful Firewall threshold limits and polling interval for DoS-attacks, dropped packets, deny rules, and no rules as described in the [Configuring Stateful Firewall Thresholds](#) section.
- Step 12 Enable bulk statistics schema for the Personal Stateful Firewall service as described in the [Configuring Bulk Statistics Schema](#) section.
- Step 13 Enable Stateful Firewall Flow Recovery as described in the [Configuring Flow Recovery](#) section.



Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Enabling the ECS Subsystem and Creating the ECS Service

To enable the ECS subsystem and create the enhanced charging service on the system, use the following configuration:

```
configure
  require active-charging
  active-charging service <ecs_service_name> [ -noconfirm ]
end
```

Configuring Port Maps

This is an optional configuration to create and configure port maps to use in access ruledef configuration.

To create and configure a port map use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    port-map <port_map_name> [ -noconfirm ]
      port { <port_number> | range <start_port> to <end_port> }
    end
```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 options can be configured in each port map.

Configuring Host Pools

This is an optional configuration to create and configure host pools to use in access ruledef configuration.

To create and configure a host pool use the following configuration:

```
configure
```

```

active-charging service <ecs_service_name>

    host-pool <host_pool_name> [ -noconfirm ]

        ip { <ip_address> | <ip_address/mask> | range <start_ip_address> to
<end_ip_address> }

    end

```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 options can be configured in each host pool.
- In release 12.0, host pools are enhanced to support IPv6 addresses and address ranges. It can be a combination of IPv4 and IPv6 addresses.

Configuring IMSI Pools

This is an optional configuration to create and configure IMSI pools to use in access ruledef configuration.

To create and configure an IMSI pool use the following configuration:

configure

```

active-charging service <ecs_service_name>

    imsi-pool <imsi_pool_name> [ -noconfirm ]

        imsi { <imsi_number> | range <start_imsi> to <end_imsi> }

    end

```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 options can be configured in each IMSI pool.

Configuring Access Ruledefs

To create and configure an access rule definition use the following configuration:

configure

```

active-charging service <ecs_service_name>

  access-ruledef <access_ruledef_name> [ -noconfirm ]

    bearer apn [ case-sensitive ] <operator> <value>

    bearer imsi { <operator> <msid> | { !range | range } imsi-pool
<imsi_pool_name> }

    bearer username [ case-sensitive ] <operator> <user_name>

    icmp { any-match <operator> <condition> | code <operator> <code> | type
<operator> <type> }

    ip { { { any-match | downlink | uplink } <operator> <condition> } | { {
dst-address | src-address } { { <operator> { <ip_address> | <ip_address/mask> }
} | { !range | range } host-pool <host_pool_name> } | protocol { { <operator> {
<protocol> | <protocol_assignment> } } | { <operator> <protocol_assignment> } }

    tcp { any-match <operator> <condition> | { { dst-port | either-port |
src-port } { { <operator> <port_number> } | { !range | range } { <start_range>
to <end_range> | port-map <port_map_name> } } }

    udp { any-match <operator> <condition> | { { dst-port | either-port |
src-port } { <operator> <port_number> | { !range | range } { <start_range> to
<end_range> | port-map <port_map_name> } } }

    create-log-record

  end

```

Notes:

- If the source IP address is not configured, then it is treated as any source IP.
- If the destination IP address is not configured, then it is treated as any destination IP.
- If the source port number is not configured, then it is treated as any source port.
- If the destination port is not configured, then it is treated as any destination port.
- If no protocol is specified then it is treated as any protocol.
- If both uplink and downlink fields are not configured, then the rule will be treated as either direction, i.e. packets from any direction will match that rule.
- Configuring access ruledefs involves the creation of several ruledefs with different sets of rules and parameters. When an access ruledef is created, the CLI mode changes to the Firewall Ruledef Configuration Mode. For

more information, see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Firewall-and-NAT Policies

To create and configure a Firewall-and-NAT Policy, use the following configuration:

configure

```

active-charging service <ecs_service_name>

    fw-and-nat policy <fw_nat_policy_name> [ -noconfirm ]

        firewall policy { ipv4-only | ipv4-and-ipv6 | ipv6-only }

            access-rule priority <priority> { [ dynamic-only | static-and-dynamic ]
access-ruledef <access_ruledef_name> { deny [ charging-action
<charging_action_name> ] | permit [ trigger open-port { <port_number> | range
<start_port> to <end_port> } direction { both | reverse | same } ] }

            access-rule no-ruledef-matches { downlink | uplink } action { deny [
charging-action <charging_action_name> ] | permit }

        end

```

Notes:

- The **access-rule no-ruledef-matches** CLI command configures the default action on packets with no access ruledef matches. Rule matching is done for the first packet of a flow. Only when no rules match, the **access-rule no-ruledef-matches** configuration is considered. The default settings for uplink direction is “permit”, and for downlink direction “deny”.

Configuring Protection from DoS and Other Attacks

To configure protection from DoS and other attacks, use the following configuration:

configure

```

active-charging service <ecs_service_name>

    firewall port-scan { connection-attempt-success-percentage { non-scanner |
scanner } <percentage> | inactivity-timeout <inactivity_timeout> | protocol {
tcp | udp } response-timeout <response_timeout> | scanner-policy { block
inactivity-timeout <inactivity_timeout> | log-only } }

    idle-timeout { icmp | tcp | udp } <idle_timeout>

    rulebase <rulebase_name>

```

```

        flow limit-across-applications { <limit> | non-tcp <limit> | tcp
<limit> }

        icmp req-threshold <req_threshold>

        exit

        fw-and-nat policy <fw_nat_policy_name>

        firewall dos-protection { all | flooding { icmp | tcp-syn | udp } |
ftp-bounce | ip-unaligned-timestamp | ipv6-dst-options [ invalid-options |
unknown-options ] | ipv6-extension-hdrs [ limit extension_limit | ipv6-frag-hdr
nested-fragmentation | ipv6-hop-by-hop [ invalid-options | jumbo-payload |
router-alert | unknown-options ] mime-flood | port-scan | source-router | tcp-
window-containment | teardrop | winnuke }

        firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit
<packets> } | { sampling-interval <sampling_interval> } }

        firewall icmp-checksum-error { drop | permit }

        firewall icmp-destination-unreachable-message-threshold <messages>
then-block-server

        firewall icmp-echo-id-zero { drop | permit }

        firewall icmp-fsm

        firewall ip-reassembly-failure { drop | permit }

        firewall malformed-packets { drop | permit }

        firewall max-ip-packet-size <max_packet_size> protocol { icmp | non-
icmp }

        firewall mime-flood { http-headers-limit <max_limit> | max-http-header-
field-size <max_size> }

        firewall tcp-checksum-error { drop | permit }

        firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset }
]

        firewall tcp-idle-timeout-action { drop | reset }

        firewall tcp-options-error { drop | permit }

        firewall tcp-partial-connection-timeout timeout

        firewall tcp-reset-message-threshold <messages> then-block-server

        firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] }
| watch-timeout <intercept_watch_timeout> }

        firewall tcp-syn-with-ecn-cwr { drop | permit }

```

```

firewall udp-checksum-error { drop | permit }

firewall validate-ip-options

end

```

Notes:

- The **firewall port-scan** CLI command in the Active Charging Service Configuration Mode configures protection from port scanning.
- The **idle-timeout { icmp | tcp | udp } <idle_timeout_duration>** CLI command in the Active Charging Service Configuration Mode configures Stateful Firewall idle timeout settings.
- The **flow limit-across-applications { <limit> | non-tcp <limit> | tcp <limit> }** CLI command in the Rulebase Configuration Mode configures the maximum number of simultaneous flows per subscriber/APN sent to a rulebase regardless of the flow type, or limits flows based on the protocol type.
- The **icmp req-threshold <req_threshold>** CLI command in the Rulebase Configuration Mode configures the maximum number of outstanding ICMP/ICMPv6 requests to store for ICMP/ICMPv6 reply matching. Stateful Firewall will drop the ICMP/ICMPv6 replies if it does not have any information about ICMP/ICMPv6 requests.
- The **firewall dos-protection** CLI command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks. Note that the following DoS attacks are only detected in the downlink direction: flooding, ftp-bounce, ip-unaligned-timestamp, ipv6-dst-options, ipv6-extension-hdrs, ipv6-frag-hdr, ipv6-hop-by-hop, mime-flood, port-scan, source-router, tcp-window-containment, teardrop, winnuke.
- The **firewall flooding** CLI command configures Stateful Firewall protection from packet flooding attacks.
- The **firewall icmp-checksum-error { drop | permit }** CLI command configures Stateful Firewall action on packets with ICMP Checksum errors.
- The **firewall icmp-destination-unreachable-message-threshold <messages> then-block-server** CLI command configures the threshold on the number of ICMP/ICMPv6 error messages sent by subscribers for a particular data flow.
- The **firewall icmp-echo-id-zero { drop | permit }** CLI command is used to allow/deny the echo packets with ICMP/ICMPv6 ID zero.
- The **firewall icmp-fsm** CLI command enables Stateful Firewall's ICMP/ICMPv6 Finite State Machine (FSM).
- The **firewall ip-reassembly-failure { drop | permit }** CLI command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios.
- The **firewall malformed-packets { drop | permit }** CLI command configures Stateful Firewall action on malformed packets. In release 12.0, this command is enhanced to support IPv6 and ICMPv6 malformed packets.
- The **firewall max-ip-packet-size <packet_size> protocol { icmp | non-icmp }** CLI command configures the maximum IP packet size (after IP reassembly) that Stateful Firewall will permit to prevent packet flooding attacks. In release 12.0, this command is enhanced to support ICMPv6 packets.
- The **firewall mime-flood** CLI command configures the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks. This command is only effective if DoS protection for MIME flood attacks has been enabled using the

firewall dos-protection mime-flood command, and the **route** command has been configured to send HTTP packets to the HTTP analyzer.

- The **firewall tcp-checksum-error { drop | permit }** CLI command configures Stateful Firewall action on packets with TCP Checksum errors.
- The **firewall tcp-fsm [first-packet-non-syn { drop | permit | send-reset }]** CLI command enables Stateful Firewall's TCP Finite State Machine (FSM).
- The **firewall tcp-idle-timeout-action { drop | reset }** CLI command configures action to take on TCP idle timeout expiry.
- The **firewall tcp-options-error { drop | permit }** CLI command configures Stateful Firewall action on packets with TCP Option errors.
- The **firewall tcp-partial-connection-timeout timeout** CLI command configures the idle timeout for partially open TCP connections.
- The **firewall tcp-reset-message-threshold <messages> then-block-server** CLI command configures the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow.
- The **firewall tcp-syn-flood-intercept** CLI command configures the TCP intercept parameters to prevent TCP-SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **firewall dos-protection** command.
- The **firewall tcp-syn-with-ecn-cwr { drop | permit }** CLI command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.
- The **firewall udp-checksum-error { drop | permit }** CLI command configures Stateful Firewall action on packets with UDP Checksum errors.
- The **firewall validate-ip-options** CLI command enables the Stateful Firewall validation of IP options for errors. When enabled, Stateful Firewall will drop packets with IP Option errors.

Configuring Maximum Number of Servers to Track for DoS Attacks

To configure the maximum number of server IPs to be tracked for involvement in any kind of DoS attacks, use the following configuration:

configure

```
active-charging service <ecs_service_name>

  firewall track-list attacking-servers <no_of_servers>

end
```

Configuring Action on Packets Dropped by Stateful Firewall

To configure the accounting action on packets dropped by Stateful Firewall due to any error, use the following configuration:

configure

```

active-charging service <ecs_service_name>

    rulebase <rulebase_name>

        flow any-error charging-action <charging_action_name>

    end

```

Notes:

- For a packet dropped due to any error condition after data session is created, the charging action applied is the one configured in the **flow any-error charging-action** command. Whereas, for a packet dropped due to access ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **access-rule priority** or in the **access-rule no-ruledef-matches** command respectively.

Configuring Dynamic Pinholes/ALGs

This section describes how to configure routing rules to open up dynamic pinholes for ALG functionality.

This section covers the following topics:

- [Creating Routing Ruledefs](#)
- [Configuring Routing Ruledefs in the Rulebase](#)

Creating Routing Ruledefs

To configure routing rules for FTP, SIP, and RTSP protocols use the following configuration:

```

configure

    active-charging service <ecs_service_name>

        ruledef <ruledef_name>

            tcp either-port <operator> <value>

            rule-application routing

        end

```

Notes:

- Create a separate ruledef for each protocol.

Configuring Routing Ruledefs in the Rulebase

To configure the routing ruledefs in the rulebase use the following configuration:

```
configure

  active-charging service <ecs_service_name>

  rulebase <rulebase_name>

    route priority <priority> ruledef <ruledef_name> analyzer { ftp-control
| pptp | tftp | rtsp } [ description <description> ]

    rtp dynamic-flow-detection

  end
```

Notes:

- Add each ruledef as a separate route priority.
- For RTSP ALG to work, in the rulebase, the **rtp dynamic-flow-detection** command must be configured.

Enabling Stateful Firewall Support for APN/Subscribers

This section describes how to enable Stateful Firewall support for APN/subscribers.

This section covers the following topics:

- [Enabling Stateful Firewall for APN](#)
- [Enabling Stateful Firewall for Subscribers](#)
- [Enabling IPv4IPv6 Stateful Firewall for Subscribers](#)

Enabling Stateful Firewall for APN

To configure the Firewall-and-NAT Policy in an APN use the following configuration:

```
configure

  context <context_name>

    apn <apn_name>

      fw-and-nat policy <fw_nat_policy_name>

    end
```

Notes:

- To specify that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers who use this APN, in the APN Configuration Mode, apply the following command: **default fw-and-nat policy**

Enabling Stateful Firewall for Subscribers

To configure the Firewall-and-NAT Policy in a subscriber template use the following configuration:

configure

```
context <context_name>

  subscriber default

    fw-and-nat policy <fw_nat_policy_name>

  end
```

Notes:

- To specify that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers, in the Subscriber Configuration Mode, apply the following command: **default fw-and-nat policy**

Enabling IPv4/IPv6 Stateful Firewall for Subscribers

To enable IPv4/IPv6 Firewall traffic in a subscriber template use the following configuration:

configure

```
active-charging service <ecs_service_name>

  fw-and-nat policy <fw_nat_policy_name>

    firewall policy { ipv4-only | ipv4-and-ipv6 | ipv6-only }

  end
```

Notes:

- Firewall can be enabled and disabled separately for IPv4 and IPv6 traffic.

Configuring Default Firewall-and-NAT Policy

This is an optional configuration to specify a default Firewall-and-NAT policy to use if in the APN/subscriber configurations the following command is configured:

default fw-and-nat policy

To configure the default Firewall-and-NAT policy, use the following configuration:

configure

active-charging service *<ecs_service_name>*

rulebase *<rulebase_name>*

fw-and-nat default-policy *<fw_nat_policy_name>*

end

Configuring Stateful Firewall Thresholds

This section describes how to configure Stateful Firewall threshold limits and polling interval for DoS-attacks, dropped packets, deny rules, and no rules.

This section covers the following topics:

- [Enabling Thresholds](#)
- [Configuring Threshold Poll Interval](#)
- [Configuring Threshold Limits](#)

Enabling Thresholds

To enable thresholds use the following configuration:

configure

threshold monitoring firewall

end

Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

configure

```

threshold poll fw-deny-rule interval <poll_interval>
threshold poll fw-dos-attack interval <poll_interval>
threshold poll fw-drop-packet interval <poll_interval>
threshold poll fw-no-rule interval <poll_interval>
end

```

Configuring Threshold Limits

To configure threshold limits use the following configuration:

configure

```

threshold fw-deny-rule <high_thresh> [ clear <low_thresh> ]
threshold fw-dos-attack <high_thresh> [ clear <low_thresh> ]
threshold fw-drop-packet <high_thresh> [ clear <low_thresh> ]
threshold fw-no-rule <high_thresh> [ clear <low_thresh> ]
end

```

Configuring Bulk Statistics Schema

To configure bulk statistics schema for the Personal Stateful Firewall service use the following configuration:

configure

bulkstats mode

```

context schema <schema_name> format <format_string>
end

```

Notes:

- For more information on *format_string* variable, see the *Bulk Statistics Configuration Mode Commands* chapter of the *Command Line Interface Reference*.
- To configure the various parameters for bulk statistics collection prior to configuring the commands in this section, see the *Configuring and Maintaining Bulk Statistics* chapter of the *System Administration Guide*.

Configuring Flow Recovery

To configure IPv4/IPv6 flow recovery parameters for Stateful Firewall flows, use the following configuration:

configure

```
active-charging service <ecs_service_name>
```

```
firewall flow-recovery { downlink | uplink } [ timeout <timeout> ]
```

```
end
```

Optional Configurations

This section describes optional administrative configurations.

The following topics are covered in this section:

- [Changing Stateful Firewall Policy in Mid-session](#)
- [Configuring Stateless Firewall](#)

Changing Stateful Firewall Policy in Mid-session

To change the Firewall-and-NAT policy in mid-session, in the Exec mode, use the following configuration:

```
update active-charging { switch-to-fw-and-nat-policy <fw_nat_policy_name> |  
switch-to-rulebase <rulebase_name> } { all | callid <call_id> | fw-and-nat-  
policy <fw_nat_policy_name> | imsi <imsi> | ip-address <ipv4_address> | msid  
<msid> | rulebase <rulebase_name> | username <user_name> } [ -noconfirm ]
```

Notes:

- To be able to change the Firewall-and-NAT policy in mid session, Stateful Firewall must have been enabled for the subscriber in the APN/Subscriber template configuration, or in the rulebase (the default policy) during call setup.
- The above command takes effect only for current calls. For new calls, the RADIUS returned/APN/Subscriber template/rulebase configured policy is used.

Configuring Stateless Firewall

This section describes how to configure Stateless Firewall processing wherein stateful checks are disabled.

To configure Stateless Firewall use the following configuration:

configure

```
active-charging service <ecs_service_name>  
  
fw-and-nat policy <fw_nat_policy_name>  
  
no firewall icmp-fsm  
  
no firewall tcp-fsm  
  
end
```

Notes:

- The **no firewall icmp-fsm** CLI command disables Stateful Firewall's ICMP Finite State Machine (FSM). When disabled, ICMP reply without corresponding requests, ICMP error message without inner packet data session, and duplicate ICMP requests are allowed by the firewall.
- The **no firewall tcp-fsm** CLI command disables Stateful Firewall's TCP Finite State Machine (FSM). When disabled, only packet header check is done; there will be no FSM checks, sequence number validations, or port scan checks done.

Saving the Configuration

To save changes made to the system configuration, see the *Verifying and Saving Your Configuration* chapter.

Gathering Stateful Firewall Statistics

The following table lists commands to gather Stateful Firewall statistics.



Important: For more information on these commands, see the *Exec Mode Commands* chapter of the *Command Line Interface Reference*.

Table 2. Gathering Stateful Firewall Statistics

Statistics	Command	Information to Look For
Firewall-and-NAT Policy statistics	show active-charging fw-and-nat policy statistics all	The output displays statistics for all Firewall-and-NAT policies.
	show active-charging fw-and-nat policy statistics name <i><fw_nat_policy_name></i>	The output displays statistics for the specified Firewall-and-NAT policy.
Firewall-and-NAT Policy information	show active-charging fw-and-nat policy all	The output displays information for all Firewall-and-NAT policies.
	show active-charging fw-and-nat policy name <i><fw_nat_policy_name></i>	The output displays information for the specified Firewall-and-NAT policy.
Flow related statistics on a chassis	show active-charging flows all	The output displays statistics for all flows for subscriber session in a system/service.
Detailed disconnect reasons for session flow	show session disconnect-reasons [verbose]	The output of this command displays the disconnect reasons for flows of a subscriber session in a system/service.
Detailed statistics of Stateful Firewall service	show active-charging firewall statistics [verbose]	The output displays detailed Stateful Firewall statistics.
Detailed statistics of rulebases	show active-charging rulebase statistics	The output displays detailed statistics of rulebases in a service.
Detailed statistics of all ruledefs	show active-charging ruledef statistics	The output displays detailed statistics of all ruledefs configured in the ECS service.
Detailed statistics of all charging ruledefs	show active-charging ruledef statistics all charging	The output displays detailed statistics of all charging ruledefs configured in the ECS service.
Detailed statistics of all access ruledefs	show active-charging ruledef statistics all firewall [wide]	The output displays detailed statistics of all access ruledefs configured in the ECS service.

Managing Your Configuration

This section explains how to review the Personal Stateful Firewall configurations after saving them in a .cfg file as described in the *Verifying and Saving Your Configuration* chapter, and also to retrieve errors and warnings with in an active configuration for a service.

Output descriptions for most of these commands are available in the *Command Line Interface Reference*.

Table 3. System Status and Personal Stateful Firewall Service Monitoring Commands

To do this:	Enter this command:
View Administrative Information	
View current administrative user access	
View a list of all administrative users currently logged on to the system	show administrators
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	show administrators session id
View information pertaining to local-user administrative accounts configured for the system	show local-user verbose
View statistics for local-user administrative accounts	show local-user statistics verbose
View information pertaining to your CLI session	show cli
Determining the System's Uptime	
View the system's uptime (time since last reboot)	show system uptime
View Status of Configured NTP Servers	
View status of the configured NTP servers	show ntp status
View System Alarm Status	
View the status of the system's outstanding alarms	show alarm outstanding all
View detailed information about all currently outstanding alarms	show alarm outstanding all verbose
View system alarm statistics	show alarm statistics
View Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	show subscribers configuration username <i><user_name></i>
View Subscriber Information	
View a list of subscribers currently accessing the system	show subscribers all
View information for a specific subscriber	show subscribers full username <i><user_name></i>

To do this:	Enter this command:
View Personal Stateful Firewall Related Information	
View System Configuration	
View the configuration of a context	show configuration context <context_name>
View configuration errors for Active Charging Service/Stateful Firewall Service	show configuration errors section active-charging [verbose] [{ grep <grep_options> more }] show configuration errors verbose
View Personal Stateful Firewall Configuration	
View Personal Stateful Firewall configurations	show configuration grep Firewall
View access policy association with subscriber	show subscribers all grep Firewall show apn all grep Firewall
View Stateful Firewall policy status for specific subscriber/APN	show subscribers configuration username <user_name> grep Firewall show apn name <apn_name> grep Firewall
View all access ruledefs	show active-charging ruledef firewall
View specific access ruledef	show active-charging ruledef name <access_rule_name>
View which DoS attack prevention is enabled	show configuration verbose grep dos
View attack statistics	show active-charging firewall statistics verbose
View ruledef action properties, checksum verification status, etc	show active-charging rulebase name <rulebase_name>
View session disconnect reasons	show session disconnect-reasons [verbose]
View information of sessions with Stateful Firewall processing required or not required as specified.	show active-charging sessions firewall { not-required required }
View information of subscribers for whom Stateful Firewall processing is required or not required as specified.	show subscribers firewall { not-required required }
View the list of servers being tracked for involvement in any DoS attacks.	show active-charging firewall track-list attacking-servers

Chapter 3

Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration

In many configurations, you have to set and verify specific features. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn
authentication context: A
pdp type: ipv4
ehrpd access: N/A
Selection Mode: subscribed
ip source violation: Checked drop limit: 10
ip source violation no accounting: Disabled
accounting mode: gtpv No early PDUs: Disabled
no-interims: Disabled
Bearer Control Mode: none
max-primary-pdp-contexts: 4000000 total-pdp-contexts: 4000000
primary contexts: not available total contexts: not available
max secondary contexts per-subscriber:10 IMS Authorization : disabled
Credit Control : disabled
mbms bearer absolute timeout : 0 mbms bearer idle timeout : 0
mbms ue absolute timeout : 0
permission :
local ip: 0.0.0.0 nexthop gateway addr:
primary dns: 0.0.0.0 secondary dns: 0.0.0.0
```



```
primary nbns: 0.0.0.0 secondary nbns: 0.0.0.0
ppp keep alive period : 0 ppp mtu : 1500
absolute timeout : 0 idle timeout : 0
idle-timeout-activity ignore-downlink: Disabled
long duration timeout: 0 long dur inactivity time: 0
long duration action: Detection
wimax header compression/suppression: none
ip header compression: vj
ip hide service address: Disabled
ip output access-group: ip input access-group:
ipv6 output access-group: ipv6 input access-group:
policy-group in: policy-group out:
permit ip multicast: False
ppp authentication:
eap authentication initial-access-request: authenticate-authorize
allow noauthentication: Enabled imsi authentication: Disabled
msisdn authentication: Disabled
ip destination context : A
Rule Base : default
FW-and-NAT Policy: default
Bandwidth-Policy: default
Link-Monitoring: OFF
Content-Filtering Policy-Id : Not configured
mediation accounting: Disabled
mediation-device context: Not set mediation no early PDUs: Disabled
mediation no-interims: Disabled mediation delay-GTP-response: Disabled
outbound username: N/A
ip address pools: N/A
ip address secondary pools: N/A
```

```
access-link ip-frag: df-ignore
ignore DF-bit data-tunnel: On
ip allocation type: local pool allow user specified ip addr: true
prefer dhcp options: false
allow deferred: false
3gpp qos to dscp mapping:
  qci 1: ef
  qci 2: ef
  qci 3: af11
  qci 4: af11
  qci 5: ef
  qci 6: ef
  qci 7: af21
  qci 8: af21
  qci 9: be
3GPP Qos to DSCP Mapping based on Alloc. Prio:
  qci 5 ( Alloc.P 1): ef
  qci 5 ( Alloc.P 2): ef
  qci 5 ( Alloc.P 3): ef
  qci 6 ( Alloc.P 1): ef
  qci 6 ( Alloc.P 2): ef
  qci 6 ( Alloc.P 3): ef
  qci 7 ( Alloc.P 1): af21
  qci 7 ( Alloc.P 2): af21
  qci 7 ( Alloc.P 3): af21
  qci 8 ( Alloc.P 1): af21
  qci 8 ( Alloc.P 2): af21
  qci 8 ( Alloc.P 3): af21
Copy user-datagram IP TOS : Disabled
```

```
APN defined Charging Characteristics:
  Home Subscribers:
    Behavior Bits: 0x0 Profile Value: 8
  Visiting Subscribers:
    Behavior Bits: 0x0 Profile Value: 8
  Roaming Subscribers:
    Behavior Bits: 0x0 Profile Value: 8
  All (Home/Visiting/Roaming) Subscribers:
    Behavior Bits: 0x0 Profile Value: 8
Subscribers to use APN defined charging characteristics: none
Subscribers to use RADIUS returned charging characteristics: No
PDG Subscribers to use APN defined charging characteristics: none
dhcp service name : Not set
dhcp context name : Not set
dhcp lease expiry policy: auto renew
mobile-ip: Disabled
mobile-ip home-agent : 0.0.0.0
mobile-ip alternate-home-agent(s) : n/a
mobile-ip reverse-tunnel : Enabled
mobile-ip mn-aaa-removal-indication : Disabled
mobile-ip mn-ha-spi: None
mobile-ip mn-ha-hash-algorithm: hmac-md5
proxy-mip: Disabled
proxy-mipv6: Disabled
proxy-mip null-username static home address: Disabled
Tunnel peer load-balancing : random
L3-to-L2 tunnel address-policy no-alloc-validate
tunnel address-policy alloc-validate
NPU QoS Traffic Priority: Derive from packet DSCP
```

APN QoS Attributes

Newcall Policy: Accept

SDU Error Ratio: Residual BER:

qci 1

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled

Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000

Committed Data Rate(in bps): 256000000 Committed Data Rate(in bps): 256000000

Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled

Burst Size: Burst Size:

Auto Readjust: Disabled Auto Readjust: Disabled

Auto Readjust Duration: n/a Auto Readjust Duration: n/a

Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535

Guaranteed Burst Size(bytes): 65535 Guaranteed Burst Size(bytes): 65535

Exceed Action: lower-ip-precedence Exceed Action: lower-ip-precedence

Violate Action: drop Violate Action: drop

qci 2

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled

Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000

Committed Data Rate(in bps): 256000000 Committed Data Rate(in bps): 256000000

Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled

Burst Size: Burst Size:

Auto Readjust: Disabled Auto Readjust: Disabled

Auto Readjust Duration: n/a Auto Readjust Duration: n/a

Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535

Guaranteed Burst Size(bytes): 65535 Guaranteed Burst Size(bytes): 65535

Exceed Action: lower-ip-precedence Exceed Action: lower-ip-precedence

Violate Action: drop Violate Action: drop

qci 3

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled

Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000
Committed Data Rate(in bps): 256000000 Committed Data Rate(in bps): 256000000
Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled
Burst Size: Burst Size:
Auto Readjust: Disabled Auto Readjust: Disabled
Auto Readjust Duration: n/a Auto Readjust Duration: n/a
Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535
Guaranteed Burst Size(bytes): 65535 Guaranteed Burst Size(bytes): 65535
Exceed Action: lower-ip-precedence Exceed Action: lower-ip-precedence
Violate Action: drop Violate Action: drop

qci 4

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled
Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000
Committed Data Rate(in bps): 256000000 Committed Data Rate(in bps): 256000000
Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled
Burst Size: Burst Size:
Auto Readjust: Disabled Auto Readjust: Disabled
Auto Readjust Duration: n/a Auto Readjust Duration: n/a
Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535
Guaranteed Burst Size(bytes): 65535 Guaranteed Burst Size(bytes): 65535
Exceed Action: lower-ip-precedence Exceed Action: lower-ip-precedence
Violate Action: drop Violate Action: drop

qci 5

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled
Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000
Committed Data Rate: n/a Committed Data Rate: n/a
Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled
Burst Size: Burst Size:
Auto Readjust: Disabled Auto Readjust: Disabled

Auto Readjust Duration: n/a Auto Readjust Duration: n/a

Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535

Guaranteed Burst Size(bytes): n/a Guaranteed Burst Size(bytes): n/a

Exceed Action: n/a Exceed Action: n/a

Violate Action: drop Violate Action: drop

qci 6

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled

Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000

Committed Data Rate: n/a Committed Data Rate: n/a

Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled

Burst Size: Burst Size:

Auto Readjust: Disabled Auto Readjust: Disabled

Auto Readjust Duration: n/a Auto Readjust Duration: n/a

Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535

Guaranteed Burst Size(bytes): n/a Guaranteed Burst Size(bytes): n/a

Exceed Action: n/a Exceed Action: n/a

Violate Action: drop Violate Action: drop

qci 7

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled

Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000

Committed Data Rate: n/a Committed Data Rate: n/a

Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled

Burst Size: Burst Size:

Auto Readjust: Disabled Auto Readjust: Disabled

Auto Readjust Duration: n/a Auto Readjust Duration: n/a

Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535

Guaranteed Burst Size(bytes): n/a Guaranteed Burst Size(bytes): n/a

Exceed Action: n/a Exceed Action: n/a

Violate Action: drop Violate Action: drop

qci 8

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled
Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000
Committed Data Rate: n/a Committed Data Rate: n/a
Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled
Burst Size: Burst Size:
Auto Readjust: Disabled Auto Readjust: Disabled
Auto Readjust Duration: n/a Auto Readjust Duration: n/a
Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535
Guaranteed Burst Size(bytes): n/a Guaranteed Burst Size(bytes): n/a
Exceed Action: n/a Exceed Action: n/a
Violate Action: drop Violate Action: drop

qci 9

Downlink Negotiate Limit: Disabled Uplink Negotiate Limit: Disabled
Peak Data Rate(in bps): 256000000 Peak Data Rate(in bps): 256000000
Committed Data Rate: n/a Committed Data Rate: n/a
Downlink Rate Limit: Disabled Uplink Rate Limit: Disabled
Burst Size: Burst Size:
Auto Readjust: Disabled Auto Readjust: Disabled
Auto Readjust Duration: n/a Auto Readjust Duration: n/a
Peak Burst Size(bytes): 65535 Peak Burst Size(bytes): 65535
Guaranteed Burst Size(bytes): n/a Guaranteed Burst Size(bytes): n/a
Exceed Action: n/a Exceed Action: n/a
Violate Action: drop Violate Action: drop

APN-AMBR

Downlink Apn Ambr : Disabled Uplink Apn Ambr : Disabled
Burst Size: Burst Size:
Auto Readjust: Enabled Auto Readjust: Enabled
Auto Readjust Duration: 1 Auto Readjust Duration: 1

```

Violate Action: transmit Violate Action: transmit
ppp accept peer ipv6 ifid : no
ipv6 init router advt interval : 3000
ipv6 init router number of advts : 3
ipv6 address prefix : <none>ipv6 address prefix pool : <none>
ipv6 interface id : <none>
ipv6 dns primary server : <none>
ipv6 dns secondary server : <none>
p-cscf primary ip : 0.0.0.0 p-cscf secondary ip : 0.0.0.0
p-cscf primary ipv6 : <none>
p-cscf secondary ipv6 : <none>
ipv6 egress address filtering : no
ipv6 dsn proxy : no
ipv6 minimum link MTU : 1280
Radius Group: default
Radius Secondary Group: <none>
External AAA Group: default
External AAA Context: A
Radius Returned Framed IP Address 255.255.255.255 Policy: Reject-Call-When-MS-IP
-Not-Supplied
Access-flow traffic-validation: disabled
Virtual APN Configuration:
None
IPv6 Configuration
IPv6 initial number of router advertisements: 3
IPv6 initial router advertisements interval: 3000ms
IPv6 Prefix Pool: Not defined
IPv6 Egress address filtering: Disabled
IPv6 Primary DNS server address: ::

```



```

IPv6 Secondary DNS server address: ::
GTPP Group : <none> GTPP Accounting Context : <none>
Mobile IPv6 Tunnel MTU : 1500
Mobile IPv6 Tunnel MTU Exceed Action : notify-sender
Mobile IPv6 Home Agent: none
Mobile IPv6 Home Link Prefix: ::/0
Mobile IPv6 Home Address: none

```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```

context : isp1:
+-----Type: (P) - Public (R) - Private
| (S) - Static (E) - Resource
|
|+----State: (G) - Good (D) - Pending Delete (R)-Resizing
||
||+--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+--Busyout: (B) - Busyout configured
|||| ||||| vvvvv Pool Name Start Address Mask/End Address Used Avail
-----
PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00
pool1 10.10.0.0 255.255.0.0 0 65534 SG00
vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5

```



Important: To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

```
show <service_type> <service_name>
```

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1
Service-Id : 1
Context : test1
Status : STARTED
Restart Counter : 8
EGTP Service : egtp1
LMA Service : Not defined
Session-Delete-Delay Timer : Enabled
Session-Delete-Delay timeout : 10000(msecs)
PLMN ID List : MCC: 100, MNC: 99
Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

```
show context name <name>
```

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named test1 is configured.

Context Name	ContextID	State
-----	-----	-----
test1	2	Active

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named “service1”, but entered it as “srv1” in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
#####  
  
Displaying Global  
AAA-configuration errors  
#####  
  
Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SMC's CompactFlash or on an installed PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
<i>url</i>	<p>Specifies the path and name to which the configuration file is to be stored. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using one of the following formats:</p> <ul style="list-style-type: none"> { /flash /pcmcia1 /pcmcia2 } [/dir] /file_name file://{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name tftp://{ ipaddress host_name[:port#] } [/directory] /file_name ftp://{ username[:pwd]@ } { ipaddress host_name } [:port#] [/directory] /file_name sftp://{ username[:pwd]@ } { ipaddress host_name } [:port#] [/directory] /file_name <p>/flash corresponds to the CompactFlash on the SMC. /pcmcia1 corresponds to PCMCIA slot 1. /pcmcia2 corresponds to PCMCIA slot 2. <i>ipaddress</i> is the IP address of the network server. <i>host_name</i> is the network server's <i>hostname</i>. <i>port#</i> is the network server's logical port number. Defaults are:</p> <ul style="list-style-type: none"> tftp: 69 - data ftp: 20 - data, 21 - control sftp: 115 - data <p>Note: <i>host_name</i> can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver. <i>username</i> is the username required to gain access to the server if necessary. <i>password</i> is the password for the specified username if required. <i>/directory</i> specifies the directory where the file is located if one exists. <i>/file_name</i> specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.</p>
-redundant	<p>Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the <i>url</i> variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.</p>
-noconfirm	<p>Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).</p>

Keyword/Variable	Description
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.



Important: The **-redundant** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called `system.cfg` to a directory that was previously created called `cfgfiles` on the SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called `simple_ip.cfg` to a directory called `host_name_configs`, using an FTP server with an IP address of `192.168.34.156`, on which you have an account with a username of `administrator` and a password of `secure`, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called `init_config.cfg` to the root directory of a TFTP server with a hostname of `config_server`, enter the following command:

```
save configuration tftp://config_server/init_config.cfg
```

Appendix A

Sample Personal Stateful Firewall Configuration

The following is a sample Personal Stateful Firewall configuration.

```
configure

  license key "\
VER=1|C1M=SanDiskSDJNJKL742749406|C1S=14J3KJI20|DOI=108|DOE=12\
SIG=MC4CFQCf9f7bAibGKJWqMd5XowxVwIVALIVgTVDSVAAogKe7fUHAEUTokw"

  aaa default-domain subscriber radius
  aaa last-resort context subscriber radius

  gtp single-source

  system hostname ABCCH4

  autoconfirm

  clock timezone asia-calcutta

  crash enable encrypted url 123abc456def789ghi

  card 1

    mode active psc

    exit

  card 2

    mode active psc

    exit

  card 4

    mode active psc

    exit

  require session recovery

  require active-charging

  context local

    interface SPI01
```

```
    ip address 1.2.3.4 255.255.255.0
    exit
server ftpd
    exit
ssh key 123abc456def789ghi123abc456def789ghi len 461
server sshd
    subsystem sftp
    exit
server telnetd
    exit
subscriber default
    exit
administrator staradmin encrypted password 123abc456def789ghi ftp
aaa group default
    exit
gtp group default
    exit
ip route 0.0.0.0 0.0.0.0 2.3.4.5 SPI01
    exit
port ethernet 24/1
    no shutdown
    bind interface SPI01 local
    exit
ntp
    enable
    server 10.6.1.1
    exit
snmp engine-id local 77777e66666a55555
active-charging service service_1
```



```
nat allocation-failure send-icmp-dest-unreachable

host-pool host1
    ip range 1.2.3.4 to 2.3.4.5
    exit

host-pool host2
    ip range 3.4.5.6 to 4.5.6.7
    exit

host-pool host3
    ip range 5.6.7.8 to 6.7.8.9
    exit

ruledef ip_any
    ip any-match = TRUE
    exit

ruledef rt_ftp
    tcp either-port = 21
    rule-application routing
    exit

ruledef rt_ftp_data
    tcp either-port = 20
    rule-application routing
    exit

ruledef rt_http
    tcp either-port = 80
    rule-application routing

vexit

ruledef rt_rtp
    rtp any-match = TRUE
    rule-application routing
    exit
```

```
ruledef rt_rtsp
    tcp either-port = 554
    rule-application routing
    exit
access-ruledef fw_icmp
    icmp any-match = TRUE
    exit
access-ruledef fw_tcp
    tcp any-match = TRUE
    exit
access-ruledef fw_udp
    udp any-match = TRUE
    exit
edr-format nbr_format1
    attribute sn-start-time format MM/DD/YYYY-HH:MM:SS priority 5
    attribute sn-end-time format MM/DD/YYYY-HH:MM:SS priority 10
    attribute radius-nas-ip-address priority 15
    attribute sn-correlation-id priority 20
    rule-variable ip subscriber-ip-address priority 25
    rule-variable ip server-ip-address priority 30
    attribute sn-subscriber-port priority 35
    attribute sn-server-port priority 40
    attribute sn-flow-id priority 45
    attribute sn-volume-amt ip bytes uplink priority 50
    attribute sn-volume-amt ip bytes downlink priority 55
    attribute sn-volume-amt ip pkts uplink priority 60
    attribute sn-volume-amt ip pkts downlink priority 65
    attribute sn-volume-amt tcp pkts downlink priority 66
    attribute sn-volume-amt tcp pkts uplink priority 67
```

```
attribute sn-volume-amt tcp bytes downlink priority 68
attribute sn-volume-amt tcp bytes uplink priority 69
rule-variable ip protocol priority 70
attribute sn-app-protocol priority 75
attribute radius-user-name priority 80
attribute radius-calling-station-id priority 85
attribute sn-direction priority 90
attribute sn-volume-dropped-amt ip bytes uplink priority 100
attribute sn-volume-dropped-amt ip bytes downlink priority 110
attribute sn-volume-dropped-amt ip packets uplink priority 115
attribute sn-volume-dropped-amt ip packets downlink priority 120
attribute sn-volume-dropped-amt tcp bytes uplink priority 130
attribute sn-volume-dropped-amt tcp bytes downlink priority 140
attribute sn-volume-dropped-amt tcp packets uplink priority 155
attribute sn-volume-dropped-amt tcp packets downlink priority 160
exit

udr-format udr_format

attribute sn-start-time format MM/DD/YYYY-HH:MM:SS localtime priority 1
attribute sn-end-time format MM/DD/YYYY-HH:MM:SS localtime priority 2
attribute sn-correlation-id priority 4
attribute sn-content-vol bytes uplink priority 6
attribute sn-content-vol bytes downlink priority 7
attribute sn-fa-correlation-id priority 8
attribute radius-fa-nas-ip-address priority 9
attribute radius-fa-nas-identifier priority 10
attribute radius-user-name priority 11
attribute sn-content-vol pkts uplink priority 12
attribute sn-content-vol pkts downlink priority 13
attribute sn-group-id priority 14
```

```
attribute sn-content-id priority 15
exit
xheader-format header
insert Stpid-1 variable bearer sn-rulebase
insert Stpid-2 variable bearer subscriber-ip-address
exit
charging-action ca_nothing
content-id 20
exit
bandwidth-policy bw1
exit
bandwidth-policy bw2
exit
rulebase base_1
tcp packets-out-of-order timeout 30000
tcp packets-out-of-order transmit after-reordering
billing-records udr udr-format udr_format
action priority 1 ruledef ip_any charging-action ca_nothing
route priority 1 ruledef rt_ftp analyzer ftp-control
route priority 10 ruledef rt_ftp_data analyzer ftp-data
route priority 20 ruledef rt_rtsp analyzer rtsp
route priority 30 ruledef rt_rtp analyzer rtp
route priority 40 ruledef rt_http analyzer http
route priority 50 ruledef rt_pptp analyzer pptp
route priority 60 ruledef rt_tftp analyzer tftp
rtp dynamic-flow-detection
bandwidth default-policy bw1
fw-and-nat default-policy base_1
exit
```

```
rulebase base_2
    action priority 1 ruledef ip_any charging-action ca_nothing
    route priority 1 ruledef rt_ftp analyzer ftp-control
    route priority 10 ruledef rt_ftp_data analyzer ftp-data
    route priority 40 ruledef rt_http analyzer http
    route priority 50 ruledef rt_pptp analyzer pptp
    route priority 60 ruledef rt_tftp analyzer tftp
    bandwidth default-policy bw2
    fw-and-nat default-policy base_2
    exit
rulebase default
    exit
fw-and-nat policy base_1
    access-rule priority 1 access-ruledef fw_tcp permit
    access-rule priority 2 access-ruledef fw_udp permit
    firewall dos-protection source-router
    firewall dos-protection winnuke
    firewall dos-protection mime-flood
    firewall dos-protection ftp-bounce
    firewall dos-protection ip-unaligned-timestamp
    firewall dos-protection tcp-window-containment
    firewall dos-protection teardrop
    firewall dos-protection flooding udp
    firewall dos-protection flooding icmp
    firewall dos-protection flooding tcp-syn
    firewall dos-protection port-scan
    firewall dos-protection ipv6-dst-options invalid-options
    firewall dos-protection ipv6-extension-hdrs limit 2
    firewall dos-protection ipv6-hop-by-hop jumbo-payload
```

```
firewall dos-protection ipv6-hop-by-hop router-alert

firewall tcp-first-packet-non-syn reset

firewall policy ipv4-and-ipv6

exit

fw-and-nat policy base_2

    access-rule priority 5 access-ruledf fw_tcp_port_3000 permit trigger
open-port 5000 direction reverse

    access-rule priority 10 access-ruledf fw_tcp permit

    access-rule priority 20 access-ruledf fw_udp permit

    access-rule priority 30 access-ruledf fw_icmp deny

firewall policy ipv4-and-ipv6

exit

nat tcp-2msl-timeout 120

exit

context pdsn

    interface pdsn

        ip address 11.22.33.44 255.255.255.0

        ip address 22.33.44.55 255.255.255.0 secondary

    exit

ssh key 123abc456def789ghi123abc456def789ghi len 461

server sshd

    subsystem sftp

    exit

subscriber default

    ip access-group css-1 in

    ip access-group css-1 out

    ip context-name isp

    mobile-ip send accounting-correlation-info

    active-charging rulebase base_1
```

```
exit

aaa group default

exit

gtpv group default

exit

pdsn-service pdsn

    spi remote-address 1.1.1.1 spi-number 256 encrypted secret
    5c4a38dc2ff61f72 timestamp-tolerance 0

    spi remote-address 2.2.2.2 spi-number 256 encrypted secret
    5c4a38dc2ff61f72 timestamp-tolerance 0

    spi remote-address 3.3.3.3 spi-number 9999 encrypted secret
    5c4a38dc2ff61f72 timestamp-tolerance 0

    authentication pap 1 chap 2 allow-noauth

    bind address 4.4.4.4

exit

edr-module active-charging-service

    file name NBR_nat current-prefix Record rotation time 45 headers edr-
    format-name

exit

exit

context isp

    ip access-list css

        redirect css service service_1 ip any any

    exit

    ip pool pool1 5.5.5.5 255.255.0.0 public 0

    interface isp

        ip address 6.6.6.6 255.255.255.0

    exit

    subscriber default

exit
```

```
aaa group default
    exit

gtpv group default
    exit

ip route 0.0.0.0 0.0.0.0 7.7.7.7 isp

exit

context radius

interface radius
    ip address 8.8.8.8 255.255.255.0
    exit

subscriber default
    exit

subscriber name ABC7-sub
    ip access-group css in
    ip access-group css out
    ip context-name isp
    active-charging rulebase base_1
    exit

subscriber name ABC9-sub
    ip access-group css in
    ip access-group css out
    ip context-name isp1
    active-charging rulebase base_2
    exit

domain ABC7.com default subscriber ABC7-sub

domain ABC9.com default subscriber ABC9-sub

radius change-authorize-nas-ip 77.77.77.77 encrypted key
123abc456def789ghi port 4000

aaa group default
```



```
radius attribute nas-ip-address address 99.99.99.99

radius dictionary custom9

radius server 9.9.9.9 encrypted key 123abc456def789gh port 1645

radius accounting server 8.8.8.8 encrypted key 123abc port 1646

exit

gtp group default

exit

diameter endpoint acs-fire.star.com

    origin host acs-fire.star.com address 44.44.44.44

    peer minid realm star.com address 55.55.55.55

exit

exit

bulkstats collection

bulkstats mode

    sample-interval 1

    transfer-interval 15

    file 1

        remotefile format /localdisk/ABCCH4.bulkstat

        receiver 66.66.66.66 primary mechanism ftp login root encrypted
password 123abc456def789ghi

        context schema sfw-dir format "sfw-dir\nsfw-dnlk-droppkts:%sfw-dnlk-
droppkts%\nsfw-dnlk-dropbytes:%sfw-dnlk-dropbytes%\nsfw-uplnk-droppkts:%sfw-
uplnk-droppkts%\nsfw-uplnk-dropbytes:%sfw-uplnk-dropbytes%\nsfw-ip-
discardpackets:%sfw-ip-discardpackets%\nsfw-ip-malpackets:%sfw-ip-
malpackets%\nsfw-icmp-discardpackets:%sfw-icmp-discardpackets%\nsfw-icmp-
malpackets:%sfw-icmp-malpackets%\nsfw-tcp-discardpackets:%sfw-tcp-
discardpackets%\nsfw-tcp-malpackets:%sfw-tcp-malpackets%\nsfw-udp-
discardpackets:%sfw-udp-discardpackets%\nsfw-udp-malpackets:%sfw-udp-
malpackets%\n-----\n"

        context schema sfw-total format "sfw-
total\nvpname:%vpname%\nvpnid:%vpnid%\nsfw-total-rxpackets:%sfw-total-
rxpackets%\nsfw-total-rxbytes:%sfw-total-rxbytes%\nsfw-total-txpackets:%sfw-
total-txpackets%\nsfw-total-txbytes:%sfw-total-txbytes%\nsfw-total-
injectedpkts:%sfw-total-injectedpkts%\nsfw-total-injectedbytes:%sfw-total-
injectedbytes%sfw-total-malpackets:%sfw-total-malpackets%\nsfw-total-
```

```
dosattacks:%sfw-total-dosattacks%\nsfw-total-flows:%sfw-total-flows%\n-----
-----\n"

    exit

    exit

port ethernet 17/1

    no shutdown

    bind interface pdsn pdsn

    exit

port ethernet 17/2

    no shutdown

    bind interface isp isp

    exit

port ethernet 17/3

    no shutdown

    bind interface radius radius

    exit

port ethernet 17/4

    no shutdown

    exit

port ethernet 17/5

    no shutdown

    exit

end
```