

PSF Administration Guide, StarOS Release 21.21

First Published: 2020-10-01

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

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 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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

About this Guide v

Conventions Used v

Supported Documents and Resources vi

Contacting Customer Support vii

CHAPTER 1

Personal Stateful Firewall Overview 1

Firewall Overview 1

Supported Features 2

Protection against Denial-of-Service Attacks 2

Types of Denial-of-Service Attacks 3

Source-IP based Flood Attack Detection 4

Protection against Port Scanning 4

Application-level Gateway Support 5

Stateful Packet Inspection and Filtering Support 6

Stateless Packet Inspection and Filtering Support 7

Host Pool, IMSI Pool, and Port Map Support 7

Port Control Protocol Support 7

Flow Recovery Support 9

ICSR Support for Dynamic Firewall Access Rules 10

SNMP Thresholding Support 10

Logging Support 10

Enhanced Syslog Reporting 11

How Personal Stateful Firewall Works 13

Disabling Firewall Policy 14

Mid-session Firewall Policy Update 14

Firewall-and-NAT Checkpointing 14

Packet Flow in Stateful Firewall Processing 14
Understanding Rules with Stateful Inspection 16
Connection State and State Table in Personal Stateful Firewall 17
Transport and Network Protocols and States 18
Application-Level Traffic and States 20

CHAPTER 2 **Personal Stateful Firewall Configuration** 23
Before You Begin 23
Configuring the System 23
Configuring Stateful Firewall 24
Enabling the ECS Subsystem and Creating the ECS Service 25
Configuring Firewall License Parameters 25
Configuring Port Maps 25
Configuring Host Pools 26
Configuring IMSI Pools 26
Configuring Access Ruledefs 27
Configuring Firewall-and-NAT Policies 28
Configuring Protection from DoS and Other Attacks 28
Configuring Server Protection Support for Uplink flows 31
Configuring Uplink IP-Sweep 32
Configuring Downlink IP-Sweep 32
Configuring Maximum Number of Servers to Track for DoS Attacks 33
Configuring Action on Packets Dropped by Stateful Firewall 33
Configuring Dynamic Pinholes/ALGs 33
Enabling Stateful Firewall Support for APN/Subscribers 34
Configuring Default Firewall-and-NAT Policy 35
Configuring PCP Service 36
Configuring Stateful Firewall Thresholds 37
Configuring Bulk Statistics Schema 37
Configuring Flow Recovery 38
Optional Configurations 38
Gathering Stateful Firewall Statistics 39
Managing Your Configuration 40



About this Guide

Note The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *PSF Administration Guide*, how it is organized and its document conventions.

Personal Stateful Firewall (PSF) is a StarOS™ in-line service application that runs on Cisco® ASR 5500 and virtualized platforms.

The PSF in-line service inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

- Conventions Used, on page v
- Supported Documents and Resources, on page vi
- Contacting Customer Support, on page vii

Conventions Used

The following tables describe the conventions used throughout this documentation.

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.

Typeface Conventions	Description
Text represented as a `screen display`	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**

Supported Documents and Resources

Related Common Documentation

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (platform dependant)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependant)
- *Thresholding Configuration Guide*

Related Product Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following product documents are also available and work in conjunction with CF:

- *ECS Administration Guide*
- *GGSN Administration Guide*

- *P-GW Administration Guide*
- *SaMOG Administration Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

`http://www.cisco.com/cisco/web/psa/default.html`

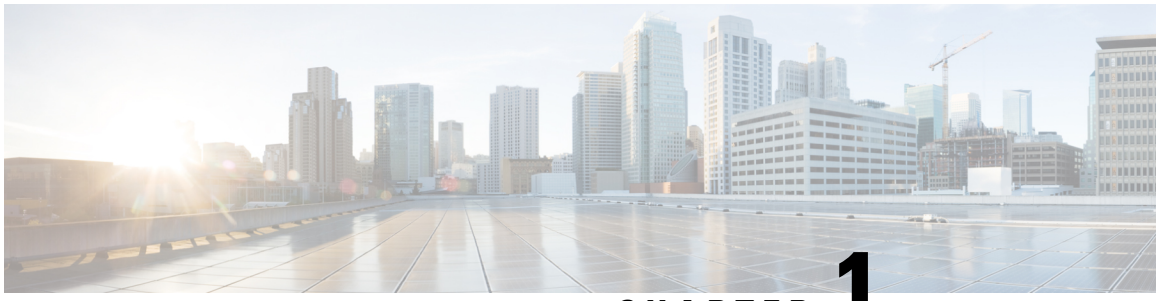
Use the following path selections to access the CF documentation:

Products > Wireless > Mobile Internet > In-Line Services > Cisco Subscriber Firewall

Contacting Customer Support

Use the information in this section to contact customer support.

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 are required to access this site. Please contact your Cisco sales or service representative for additional information.



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:

- Firewall Overview, on page 1
- Supported Features, on page 2
- How Personal Stateful Firewall Works, on page 13
- Understanding Rules with Stateful Inspection, on page 16

Firewall 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 in-line service works in conjuction with the following products:

- GGSN
- HA
- PDSN
- P-GW

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, on page 17 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*.

Qualified Platforms

PSF is a StarOS in-line service application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

The Personal Stateful Firewall is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.



Important A session with PDN Type IPv4 or IPv6 require a single PSF license. A session with PDN Type IPv4v6 requires two PSF licenses.

Supported Features

The Personal Stateful Firewall supports the following features:

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 — Detected in downlink and uplink direction
  - Teardrop attacks — Detected in downlink and uplink direction
  - Invalid IP option length — Detected in downlink and uplink direction
  - 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
  - Source-IP based flood attack — Detected in downlink and uplink directions
- 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 in downlink and uplink direction
  - FTP bounce attack — Detected only in downlink direction
  - MIME flood attacks — Detected in downlink and uplink direction
  - Exceeding reset message threshold — Detected in downlink and uplink direction
  - Source port zero
  - WinNuke attack — Detected in downlink and uplink 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 in downlink and uplink 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 in downlink and uplink direction
  - Ping of death attacks — Detected in downlink and uplink direction
  - ICMP checksum errors
  - ICMP packets with destination unreachable message
  - ICMP echo packets with ID zero

- Other DoS Attacks:
  - Port scan attacks — Detected in downlink and uplink 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

Source-IP based Flood Attack Detection

The Source-IP based flood attack detection feature is implemented to limit the number of new flows originating from a source IP per unit time to various destinations in both uplink and downlink directions. Limiting the number of connections from a single source IP to different destinations will be applied only per SMGR instance. CLI support is added for enabling and disabling uplink/downlink IP Sweep protection. Statistics support is added to show details of packets dropped due to IP Sweep protection and the list of internet hosts doing a flood attack.

An Internet host can flood mobiles by sending packets while firewall downlink action is configured as “permit”. At present there is no mechanism to prevent flood attacks from a host going to multiple destinations.

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.

Port scans are mainly classified into two types:

- **Horizontal scan**: In the case of Horizontal scanning, a port scanner probes multiple destination addresses (i.e. hosts) for the same port for profiling active hosts.
- **Vertical scan**: In the case of Vertical scanning, a port scanner probes a set of ports on the same machine to find out which services are running on the machine.

Vertical scans get detected easily when compared to horizontal scans. Stateful Firewall provides protection against port scanning by implementing port scan detection algorithms. Port scan attacks are detected in both the downlink and uplink direction—traffic from external network towards mobile subscribers. Horizontal scan detection is limited to a particular session manager in the downlink direction. Detection in the uplink direction will be supported in a future release.

Limitations:

- The maximum number of requests analyzed per source need to be limited due to memory constraints and this may result in false negatives.

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. Stateful Firewall provides ALG functionality for the following protocols. ALG support for Simple Mail Transfer Protocol (SMTP) and HTTP is ECS functionality.

Table 1: Protocol Support for ALG Type

ALG Type	Support in IPv4 Firewall	Support in IPv6 Firewall
File Transfer Protocol (FTP)	Yes	Yes
H323	Yes	No
Point-to-Point Tunneling Protocol (PPTP)	Yes	Yes
Real Time Streaming Protocol (RTSP)	Yes	Yes
Session Initiation Protocol (SIP TCP)	Yes	Yes
Session Initiation Protocol (SIP UDP)	Yes	Yes
Trivial File Transfer Protocol (TFTP)	Yes	Yes

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.



Important In 9.0 and earlier releases, GRE flow was detected and identified as a 3-tuple. In later releases, GRE flow is identified as a 5-tuple as part of the PPTP analyzer implementation. For the PPTP traffic to work after upgrade, a PPTP analyzer need to be configured in the rulebase or add a downlink allow rule for GRE traffic in Firewall-and-NAT policy.

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 packets with SYN flag set and destination port zero will be dropped like TCP packets with source port zero are dropped.

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.

Port Control Protocol Support

The Port Control Protocol (PCP) feature provides a mechanism to control how incoming packets are forwarded by upstream devices such as Network Address Translation IPv4/IPv4 (NAT44) and IPv4 firewall devices, and to reduce application keepalive traffic.

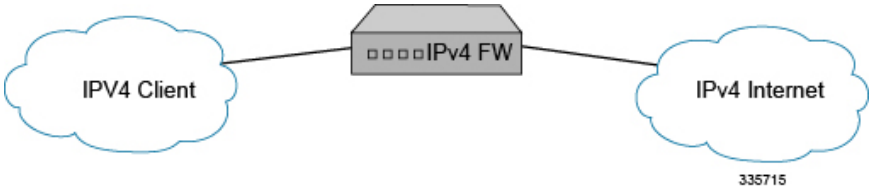
Important The PCP feature is customer specific. Contact your Cisco account representative for more information.

Important PCP is a licensed Cisco feature. Contact your Cisco account representative for more information. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The PCP server is supported on ASR 5500 chassis running in-line services such as NAT44 and Stateful Firewall(s) individually or in collocated configurations. PCP supports the following functions:

- A host to control how incoming packets are forwarded by upstream devices such as Network Address Translation (NAT44) and Stateful Firewall (IPv4).
- A host to reduce the application keepalive messages.
- A host to operate a server for a long duration (e.g. webcam) or a short duration (e.g. while playing a game or on a phone call) when behind a NAT device, including a CGN operated by an Internet service provider.
- Applications to create mappings from an external IP address and port to an internal (target) IP address and port. These mappings are required for successful inbound communications destined to machines located behind a NAT or Firewall.
- Applications to create mappings in NAT and Firewall, and reducing the incentive to deploy ALGs in NAT and Firewalls.

The following figure shows IPv4 Firewall and PCP Server on ASR 5500.



The PCP service has to be associated with a PCP server IP address. The PCP server IP address is picked from the destination context associated with the subscriber. Only, if such an IP address is available and the status is up, the PCP service will listen to PCP requests on that IP address. The PCP service will be bound only to an IPv4 address and listens on UDP port (5351 (default port) or can be configured).

In case of system failure, the PCP service recovers along with subscriber's PCP enabled status. In case of stand-alone recovery and ICSR, only the subscriber PCP enabled status will be check-pointed.

PCP supports interworking with the following existing NAT ALGs:

- FTP
- RTSP
- SIP

Bulk Statistics Support for the Port Control Protocol Feature

Bulk statistics reporting for the PCP feature is supported.

For the PCP feature the following bulk statistics are available in the ECS schema:

- total-pcp-svc-req
- total-pcp-svc-rsp
- total-pcp-svc-unknown-rsp
- total-pcp-svc-invalid-rsp
- total-pcp-svc-map-req
- total-pcp-svc-map-valid-req
- total-pcp-svc-map-invalid-req
- total-pcp-svc-map-rsp
- total-pcp-svc-map-rsp-success
- total-pcp-svc-peer-rsp-error
- total-pcp-svc-peer-req
- total-pcp-svc-peer-valid-req
- total-pcp-svc-peer-invalid-req
- total-pcp-svc-peer-rsp
- total-pcp-svc-peer-rsp-success
- total-pcp-svc-peer-rsp-error
- total-pcp-svc-announce-req
- total-pcp-svc-announce-vaild-req
- total-pcp-svc-announce-invaild-req
- total-pcp-svc-announce-rsp
- total-pcp-svc-announce-rsp-success
- total-pcp-svc-announce-rsp-error
- total-pcp-svc-subscribers
- current-pcp-svc-subscribers

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 the 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.

ICSR Support for Dynamic Firewall Access Rules

ICSR recovery is supported for dynamic Firewall access rules. Firewall access rules can be enabled either statically or dynamically. After ICSR switchover, the Firewall access rules can be dynamically activated or deactivated from the Gx server. This feature currently works only for default bearers and not for dedicated bearers.

The following attributes are used to activate or deactivate Firewall access rules from the Gx server:

- Charging-Rule-Install
- Charging-Rule-Remove

Earlier, Firewall access rules enabled dynamically by PCRF were checkpointed only for standalone recovery. ICSR checkpointing was not done for dynamically enabled access rules. After ICSR switchover, the dynamically enabled Firewall rule will be enabled.

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.

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.

Enhanced Syslog Reporting

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All Products
Applicable Platform(s)	• ASR 5500 • VPC - Di • VPC - Si
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *NAT Administration Guide* • *PSF Administration Guide*

Revision History

Revision Details	Release
With this feature, the port information of the dropped packet is included in the logs.	21.3.1
First introduced.	Pre 21.2

Feature Description

Firewall and NAT attack logs provide information on the source IP address, destination IP address, protocol, or attack type for any packet dropped due to an attack. Prior to this release, when an attack happened, the logs did not carry any information about the ports.

With this feature, the port information of the dropped packet is included in the logs. The port information such as source port and destination port are important while configuring access rules to allow or block certain traffic.

Following are some important points to be considered:

- Typically, attack logs are at INFO/DEBUG level. At this level, there are too many logs generated even for normal traffic. Hence, to segregate the attack logs, the attack logs are moved to the WARNING level.
- Firewall and NAT attack logs are moved to WARNING level from Info/Debug level. The source port and destination port are logged as part of Firewall/NAT attack logs.
- Both IPv4 and IPv6 traffic is supported.

- The source port and destination port are valid for TCP/UDP protocols. However, for other protocols, the ports are logged as zero.

Previous Behavior: Earlier, the attack logs did not carry any port information and the logs were of the type Info/Debug.

New Behavior: With this feature, firewall and NAT attack log levels have been changed to WARNING from INFO/DEBUG for event IDs 96188, 96995, 96186,96185, 96159, and 96203. Source port and destination port information are now displayed in the attack logs.

Impact on Customer: The attack logs are per packet logs seen at WARNING level. If you enable WARNING and above logs for Firewall (NAT) facility, and when there is an attack, log rate is very high.

Limitations

Following are the limitations of this feature:

- The attack logs are per packet logs and when an attack is in progress, log generation rate is very high.
- Under extreme attack conditions, evlogd CPU might go up.
- Event IDs for the attack logs:
  - firewall 96188 warning
  - firewall 96995 warning
  - firewall 96186 warning
  - firewall 96203 warning
  - firewall 96159 warning
  - firewall 96185 warning
- When there are too many logs generated under attack conditions, the following event IDs must be disabled:
  - eventid 96188: Disables Firewall Attack log generation
  - eventid 96186: Disables Port Scan Attack log generation
  - eventid 96995: Disables NAT Attack log generation
  - eventid 96203: Disables logging for TCP reset message threshold breach
  - eventid 96159: Disables logging for packets denied by rule
  - eventid 96185: Disables logging for ICMP unreachable message threshold breach

Configuring Logging Event ID

When there are too many logs generated under attack conditions, use the following command to disable the event IDs:

- To disable firewall attack log generation:

```
[local]asr5500(config)# logging disable eventid 96188
```

- To disable port scan log generation:

```
[local]asr5500(config)# logging disable eventid 96186
```

- To disable NAT attack log generation:

```
[local]asr5500(config)# logging disable eventid 96995
```

- To disable logging for TCP reset message threshold breach:

```
[local]asr5500(config)# logging disable eventid 96203
```

- To disable logging for packets denied by rule:

```
[local]asr5500(config)# logging disable eventid 96159
```

- To disable logging for ICMP unreachable message threshold breach:

```
[local]asr5500(config)# logging disable eventid 96185
```

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. A Firewall-and-NAT policy defined with no Firewall or NAT enabled will not drop the call but will disable the configured Firewall or NAT.

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

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

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

- 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. Firewall-and-NAT policy can also be updated during mid-session rulebase update through Gx and Gy if the new rulebase has Firewall-and-NAT policy configured and the old Firewall-and-NAT policy is configured through old rulebase.

Important When the SN-Firewall-Policy 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.

Firewall-and-NAT Checkpointing

The “Firewall-and-NAT Policy ID” can be used for checkpointing the Firewall-and-NAT Policy unlike “Firewall-and-NAT Policy-Name” used in previous releases. Backward compatibility has been provided to support checkpointing the Firewall-and-NAT Policy-Name by older versions of peer-chassis. If the older chassis sends Policy-name in checkpointing, then this has to be handled appropriately by the new chassis.

Packet Flow in Stateful Firewall Processing

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

Figure 1: Stateful Firewall Processing

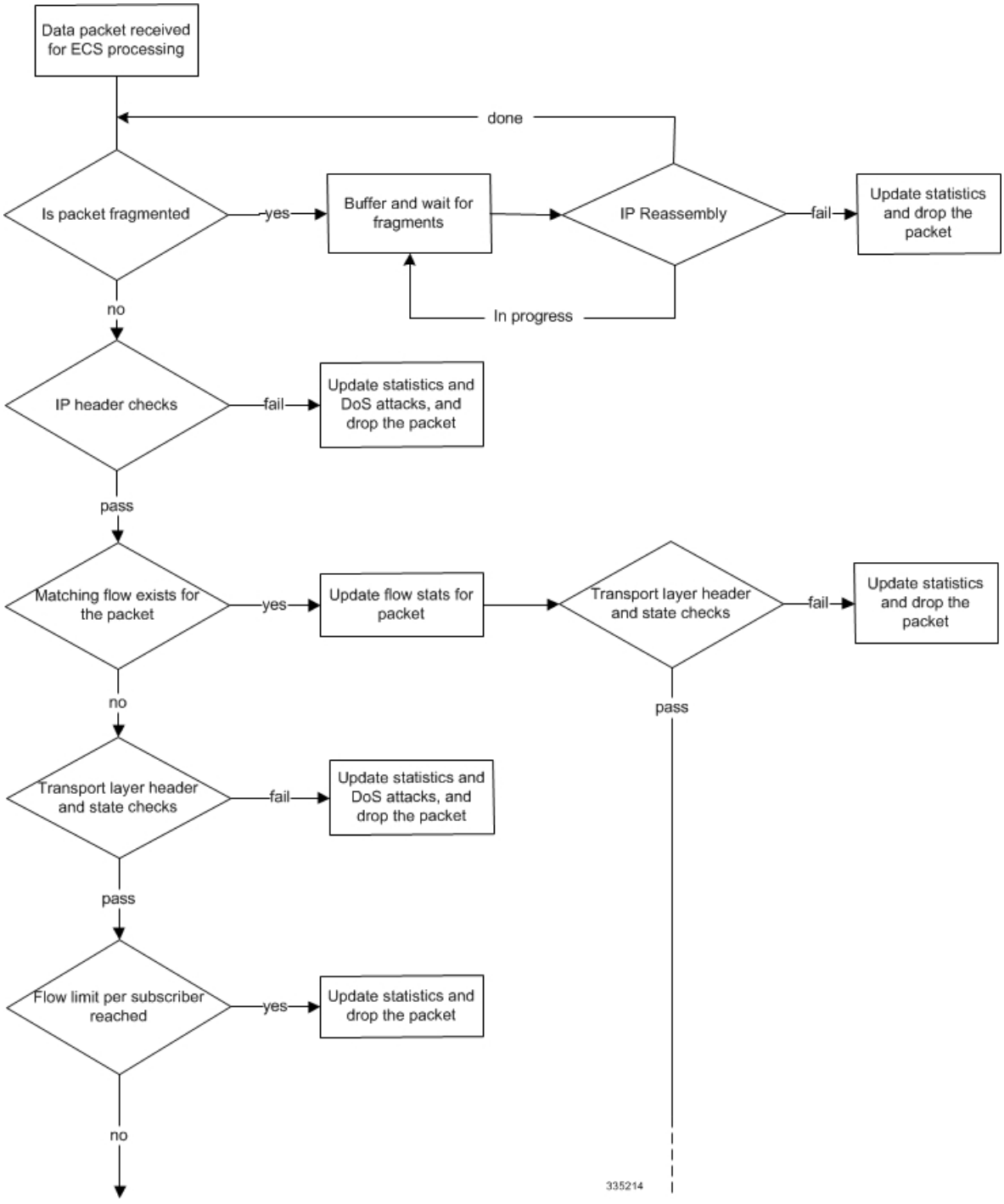
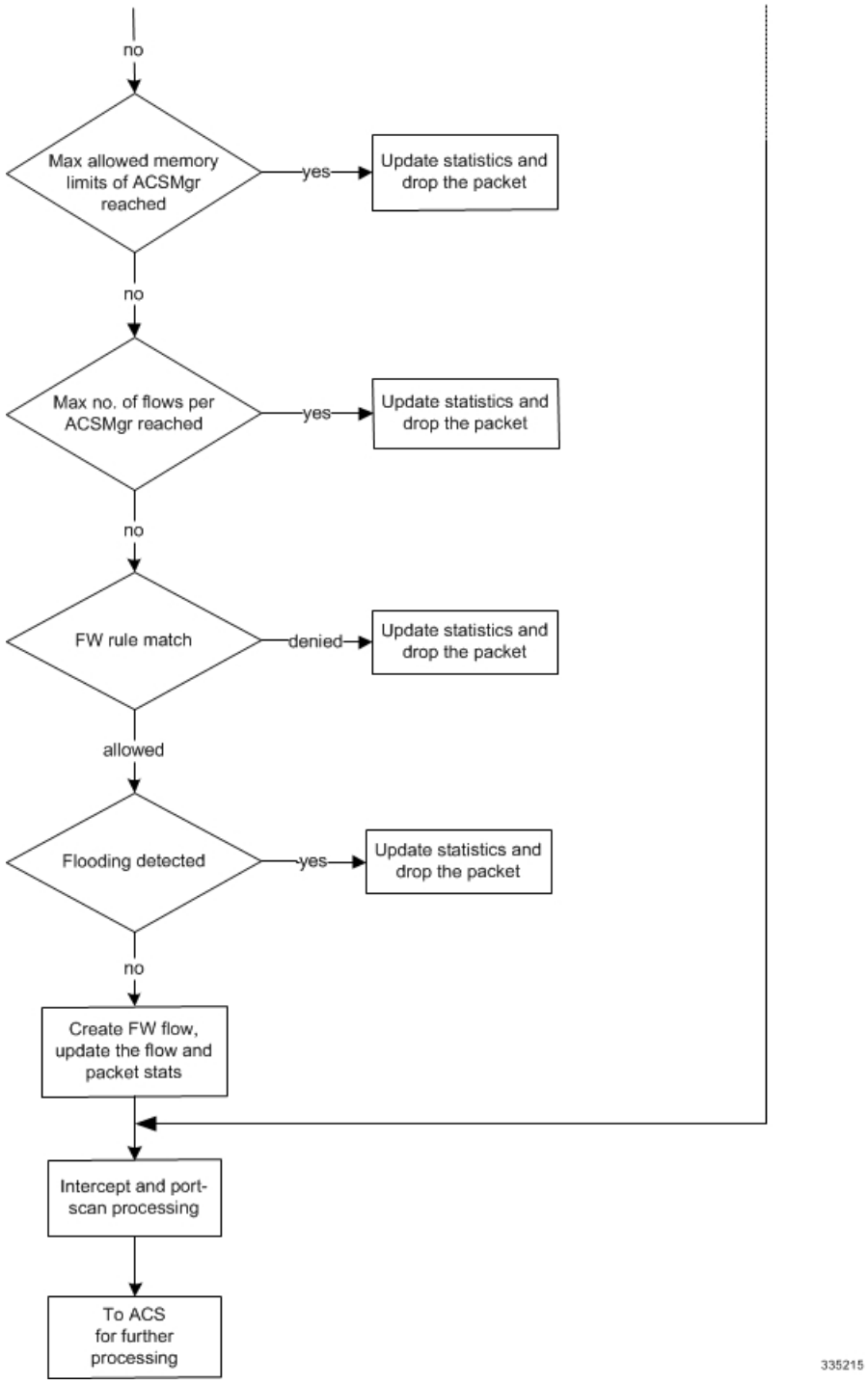


Figure 2: Stateful Firewall Processing (Contd.)



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
  - Client port number — TCP or UDP
  - Server port number — TCP or UDP

  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.

  Firewall access ruledefs 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.

  Access ruledefs can be switched on/off from PCRF (Gx). Charging ruledef attributes can be used for this purpose. Access ruledefs that need to be switched on/off must be configured as "dynamic-only" or "static-and-dynamic" in Firewall-and-NAT policy. If configured as "dynamic-only", the rule will be disabled by default and can be switched on from PCRF. If configured as "static-and-dynamic", the rule will behave as "dynamic-only" for Gx enabled call and as static rule for non-Gx calls.

- **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 2: 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

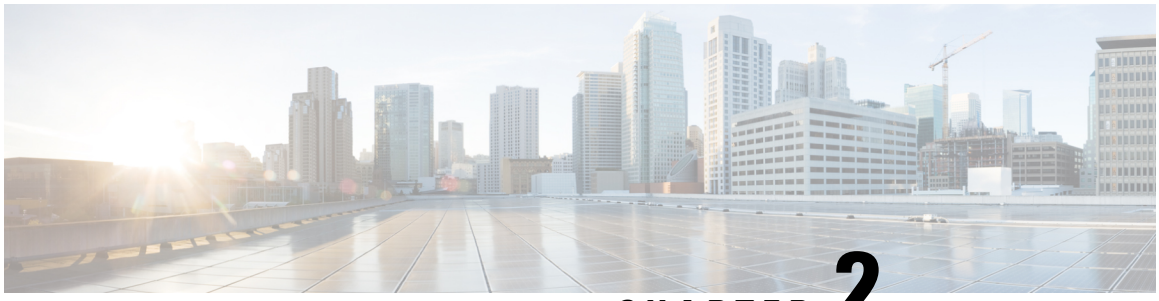
FTP is an application to move files between systems across the network. This is a two way connection and uses TCP as its transport protocol.

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:

- Before You Begin, on page 23
- Configuring the System, on page 23
- Configuring Stateful Firewall, on page 24
- Optional Configurations, on page 38
- Gathering Stateful Firewall Statistics, on page 39
- Managing Your Configuration, on page 40

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 Configuring the System, on page 23.

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 Configuring Stateful Firewall, on page 24.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and *Command Line Interface Reference*.

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 Enabling the ECS Subsystem and Creating the ECS Service, on page 25.

Step 2 Configure Firewall license parameters as described in Configuring Firewall License Parameters , on page 25.

Step 3 (Optional) Configure application-port maps for TCP and UDP protocols as described in Configuring Port Maps, on page 25.

Step 4 (Optional) Configure host pools as described in Configuring Host Pools.

Step 5 (Optional) Configure IMSI pools as described in Configuring IMSI Pools.

Step 6 Configure access ruledefs as described in Configuring Access Ruledefs.

Step 7 Configure Firewall-and-NAT policies as described in Configuring Firewall-and-NAT Policies.

Step 8 Configure protection from DoS and other attacks as described in Configuring Protection from DoS and Other Attacks, on page 28.

Step 9 Configure ALGs as described in Configuring Dynamic Pinholes/ALGs, on page 33.

Step 10 Enable Stateful Firewall support for APN/subscribers as described in Enabling Stateful Firewall Support for APN/Subscribers, on page 34.

Step 11 (Optional) Configure the default Firewall-and-NAT policy as described in Configuring Default Firewall-and-NAT Policy, on page 35.

Step 12 (Optional) Configure the PCP service as described in Configuring PCP Service, on page 36.

Step 13 Configure Stateful Firewall threshold limits and polling interval for DoS-attacks, dropped packets, deny rules, and no rules as described in Configuring Stateful Firewall Thresholds, on page 37.

Step 14 Enable bulk statistics schema for the Personal Stateful Firewall service as described in Configuring Bulk Statistics Schema, on page 37.

Step 15 Enable Stateful Firewall Flow Recovery as described in Configuring Flow Recovery, on page 38.

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, use the following configuration:

```
configure
   require active-charging service
   active-charging service acs_service_name [ -noconfirm ]
   end
```

Configuring Firewall License Parameters

To configure the Firewall license parameters, use the following configuration:

```
configure
   active-charging service acs_service_name
     firewall license exceed-action { disable-feature | drop-call | ignore
 }
      end
```

Notes:

One of the following parameters can be configured:

- **disable-feature**: Disables the service when license is exceeded.
- **drop-call**: Drops the call if call fails to get a Stateful Firewall license.
- **ignore**: Continues using the Stateful Firewall license even if license is exceeded. This is the default behavior.

Configuring Port Maps

This is an optional configuration. To create and configure a port map, use the following configuration:

```
configure
   active-charging service acs_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 a host pool, use the following configuration:

```
configure
   active-charging service acs_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 an IMSI pool, use the following configuration:

```
configure
   active-charging service acs_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 acs_service_name
      access-ruledef access_ruledef_name [ -noconfirm ]
         bearer apn [ case-sensitive ] operator value
         bearer imsi { operator msid | { !range | range } imsi-pool imsi_pool }
         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 | { client-port |  dst-port |
either-port | server-port | src-port } { operator port_number | { !range | range
 } { start_range to end-range | port-map port_map_name } } }
         udp { any-match operator condition | { client-port |  dst-port |
either-port | server-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 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.
- TCP/UDP client port and server port support is added for Firewall Access Ruledefs. When a Firewall//NAT rule match is performed, for an uplink packet, the destination port in the packet must be considered as server port and rule match must be done accordingly. Similarly the source port of an uplink packet must be considered as the client port. For a downlink packet, the source port must be considered as the server port and the destination port as the client port.
- 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 Server IP Address

To configure an access rule definition to analyze user traffic based on server IP address, use the following configuration:

```
configure
   active-charging service acs_service_name
      access-ruledef access_ruledef_name
         [ no ] ip server-ip-address { operator { ipv4/ipv6_address |
ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
         end
```

Notes:

The **ip server-ip-address** command is added in access rule definitions to avoid configuring multiple rule options as part of Firewall rules. If any address or host-pool range is specified as the server IP address, this address in the uplink direction will be treated as the destination address, and in downlink direction will be treated as the source address.

Configuring Firewall-and-NAT Policies

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

```
configure
   active-charging service acs_service_name
      fw-and-nat policy fw_nat_policy_name [ -noconfirm ]
         firewall policy [ ipv4-and-ipv6 | ipv4-only | 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

This section describes how to configure protection from DoS and other attacks.

This section covers the following topics:

- Configuring Server Protection Support for Uplink flows, on page 31
- Configuring Uplink IP-Sweep, on page 32
- Configuring Downlink IP-Sweep, on page 32
- Configuring Maximum Number of Servers to Track for DoS Attacks, on page 33

- Configuring Action on Packets Dropped by Stateful Firewall, on page 33

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

```
configure
  active-charging service acs_service_name
    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 | | 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 **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. This command is now 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. This command is now 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.

For more information regarding commands in this section, refer to the *Command Line Interface Reference*.

Configuring Server Protection Support for Uplink flows

To enable server protection for uplink flows, use the following configuration:

```
configure
   active-charging service acs_service_name
      firewall dos-protection flooding { { icmp | tcp-syn | udp }
protect-servers { all | host-pool hostpool_name } packet limit packet_limit |
 inactivity-timeout timeout | uplink-sample-interval interval }
      firewall dos-protection port-scan protect-servers { all | host-pool
 hostpool_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 } }
      firewall protect-servers { all | host-pool } policy policy_name
      idle-timeout { icmp | tcp | udp } <idle_timeout>
      end
```

Notes:

- The **firewall dos-protection flooding** command is used to enable Stateful Firewall protection from different types of DoS attacks for all servers or those servers mentioned in the host pool. This allows users to safeguard their own servers and other hosts. DoS attacks are also detected in the downlink direction by configuring the firewall dos-protection command in the FW-and-NAT Policy Configuration mode.
- The **firewall dos-protection port-scan** CLI command can be configured to enable port scan in the uplink direction.
- The **firewall port-scan** CLI command configures protection from port scanning.
- The **firewall port-scan protocol { tcp | udp } response-timeout** CLI command allows for a range of 1 to 30 seconds. Port scan detection can now happen in less time, and ensures detection at less number of SYN packets.

- The **firewall protect-servers** CLI command is configured to protect ISP servers from mobile space devices. The subscriber need not be Firewall/NAT enabled to enable server protection. The same or different Firewall policy for uplink and downlink firewall can be used.
- The **idle-timeout { icmp | tcp | udp }** *<idle_timeout_duration>* CLI command in the Active Charging Service Configuration Mode configures Stateful Firewall idle timeout settings.
- For more information regarding commands in this section, refer to the *Command Line Interface Reference*.

Configuring Uplink IP-Sweep

To detect Source IP-based flooding for uplink direction, use the following configuration:

```
configure
   active-charging service acs_service_name
      firewall dos-protection ip-sweep { icmp | tcp-syn | udp }
protect-servers { all | host-pool hostpool_name } packet limit packet_limit |
downlink-server-limit server_limit | inactivity-timeout timeout |
sample-interval interval }
      default firewall dos-protection ip-sweep { downlink-server-limit |
icmp | inactivity-timeout | sample-interval | tcp-syn | udp }
      no firewall dos-protection ip-sweep { icmp | tcp-syn | udp }
      end
```

Important In StarOS 17.0 and later releases, the Uplink IP sweep feature is not enabled in the ACS Configuration mode, and must be enabled in the Firewall-and-NAT Policy Configuration mode. Hence, the **firewall dos-protection ip-sweep** command in the ACS Configuration mode is no longer supported and left in place for backward compatibility.

Notes:

- This command is used to enable or disable IP Sweep Protection in the uplink direction for mobile subscribers and internet hosts on a per protocol basis.
- IP Sweep attacks detected in the downlink direction can be configured using the **firewall dos-protection ip-sweep** command in the FW-and-NAT Policy Configuration mode.
- The configuration values of packet limit and sampling interval are common for both uplink and downlink.

For more information regarding commands in this section, refer to the *Command Line Interface Reference*.

Configuring Downlink IP-Sweep

To detect Source IP-based flooding for downlink direction, use the following configuration:

```
configure
   active-charging service acs_service_name
      fw-and-nat policy policy_name
         [ no ] firewall dos-protection ip-sweep { icmp | tcp-syn | udp }
         default firewall dos-protection
         end
```

Notes:

- IP Sweep attacks detected in the uplink direction can be configured using the **firewall dos-protection ip-sweep** command in the ACS Configuration mode.
- The configuration values of packet limit and sampling interval are common for both uplink and downlink.

For more information regarding commands in this section, refer to the *Command Line Interface Reference*.

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
      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.

For more information regarding commands in this section, refer to the *Command Line Interface Reference*.

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, on page 33
- Configuring Routing Ruledefs in Rulebase, on page 34
- Configuring SIP ALG Parameters, on page 34

Creating Routing Ruledefs

To configure routing rules 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 routing ruledef for each protocol.
- The routing rule must be defined by IP/port matching for packets to get routed to a particular ALG/analyzer.

Configuring Routing Ruledefs in Rulebase

To configure the routing ruledefs in the rulebase for FTP, H323, PPTP, RTSP, SIP, and TFTP protocols use the following configuration:

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      route priority priority ruledef ruledef_name analyzer { ftp-control |
h323 | pptp | tftp | rtsp | sip } [ description description ]
      rtp dynamic-flow-detection
      end
```

Notes:

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

Configuring SIP ALG Parameters

To enable SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests, use the following configuration:

```
configure
  active-charging service acs_name
    sip advanced out-of-dialog-request retain-tag
    end
```

Enabling Stateful Firewall Support for APN/Subscribers

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

The following topics are covered in this section:

- Enabling Stateful Firewall for APN, on page 35
- Enabling Stateful Firewall for Subscribers, on page 35
- Enabling IPv4/IPv6 Stateful Firewall for Subscribers, on page 35

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 who use this APN, 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 acs_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 acs_service_name
      rulebase rulebase_name
         fw-and-nat default-policy fw_nat_policy_name
         end
```

Configuring PCP Service

This section describes how to configure PCP service for the PCP Server feature.

Important The PCP Server feature is customer specific. For more information contact your Cisco account representative.

Configuring PCP Service and PCP Policy Control

To create and configure a PCP Service, and configure PCP Policy Control related parameters, use the following configuration:

```
configure
   active-charging service acs_service_name
      pcp-service pcp_svc_name [ -noconfirm ]
         policy-control
            request-opcode [ announce | map [ filter | prefer-failure ] | peer
 ]
            response-opcode { map | peer } [ error { long life-time life_time |
short life-time life_time } | success life-time life_time ]
            server ipv4-address ipv4_address [ port port_num ]
            end
```

Important A maximum of 5 PCP services can be configured in the ACS.

Enable/Disable PCP Service in Rulebase

To enable or disable the PCP service to associate subscribers with in the rulebase, use the following configuration:

```
configure
   active-charging service acs_service_name
      rulebase rulebase_name
         pcp-service pcp_svc_name
         end
```

Important The PCP service in rulebase is disabled by default.

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.

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.

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-torulebase 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 acs_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.

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 *Command Line Interface Reference*.

Table 3: 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 *fw_nat_policy_name*	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 *fw_nat_policy_name*	The output displays information for the specified Firewall-and-NAT policy.
	show active-charging subscribers full all	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.

Statistics	Command	Information to Look For
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.
PCP service statistics	**show active-charging pcp-service all** **show active-charging pcp-service name** *pcp_service_name* **show active-charging pcp-service statistics**	The output displays detailed statistics of the configured PCP service.

Managing Your Configuration

This section explains how to review the Personal Stateful Firewall configurations after saving them in a .cfg file, and also to retrieve errors and warnings within an active configuration for a service. For additional information on how to verify and save configuration files, refer to *System Administration Guide* and *Command Line Interface Reference*.

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

Table 4: 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	

To do this:	Enter this command:
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** *user_name*
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** *user_name*
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**

To do this:	Enter this command:
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 { notrequired | 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**
View the IP Sweep server list involved in IP Sweep attacks.	**show active-charging firewall dos-protection ip-sweep server-list { all | instance** *instance_num* **} [| { grep** *grep_options* **| more }]**