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

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 1.

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 2.

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 3.

Step 2 Configure Firewall license parameters as described in Configuring Firewall License Parameters , on page 3.

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

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 6.

Step 9 Configure ALGs as described in Configuring Dynamic Pinholes/ALGs, on page 11.

Step 10 Enable Stateful Firewall support for APN/subscribers as described in Enabling Stateful Firewall Support for APN/Subscribers, on page 12.

Step 11 (Optional) Configure the default Firewall-and-NAT policy as described in Configuring Default Firewall-and-NAT Policy, on page 13.

Step 12 (Optional) Configure the PCP service as described in Configuring PCP Service, on page 14.

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 15.

Step 14 Enable bulk statistics schema for the Personal Stateful Firewall service as described in Configuring Bulk Statistics Schema, on page 15.

Step 15 Enable Stateful Firewall Flow Recovery as described in Configuring Flow Recovery, on page 16.

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 Action on Packets Dropped by Stateful Firewall, on page 11

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

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 13
- Enabling Stateful Firewall for Subscribers, on page 13
- Enabling IPv4/IPv6 Stateful Firewall for Subscribers, on page 13

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 1: 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 2: 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 }]**