Firewall Support in CUPS

- Revision History, on page 1
- Feature Description, on page 1
- Configuring the Default Firewall Feature, on page 2
- Monitoring and Troubleshooting, on page 4
- Show CLIs for CUPS, on page 5
- SNMP Traps, on page 5
- Reassembly Behavior Change, on page 6

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

Subscriber Firewall feature on CUPS architecture allows you to configure Stateless and Stateful packet inspection and packet filtering to protect the subscribers from malicious attacks. The firewall configuration allows the system to inspect each packet of the subscriber data session. It also evaluates the security threat and applies the policies configured on uplink and downlink traffic.

Note The subscriber firewall implementation in CUPS is like the firewall implementation in non-CUPS architecture. For more details on the subscriber firewall in non-CUPS, see the *PSF Administration Guide*.

Overview

Firewall feature includes the support for the following:

- DoS attack
- DDoS attack
- Packet Filtering
- Stateless & stateful packet inspection
- Application level gateways
- SNMP thresholding and logging

Configuring the Default Firewall Feature

Following is the default configuration for the FW policy.

```
configure
          active-charging service service_name
            fw-and-nat policy policy_name
            end
```

Along with the preceding service configuration, Following is the default CLI behavior of various FW related CLI within the service.

```
Dos-Protection:
      Source-Route                        : Disabled
      Win-Nuke                            : Disabled
      Mime-Flood                          : Disabled
      FTP-Bounce                          : Disabled
      IP-Unaligned-Timestamp              : Disabled
      Seq-Number-Prediction               : Disabled
      TCP-Window-Containment              : Disabled
      Teardrop                            : Disabled
      UDP Flooding                        : Disabled
      ICMP Flooding                       : Disabled
      SYN Flooding                        : Disabled
      Port Scan                           : Disabled
      IPv6 Extension Headers Limit        : Disabled
      IPv6 Hop By Hop Options             : Disabled
      Hop By Hop Router Alert Option      : Disabled
      Hop By Hop Jumbo Payload Option     : Disabled
      Invalid Hop By Hop Options          : Disabled
      Unknown Hop By Hop Options          : Disabled
      IPv6 Destination Options            : Disabled
      Invalid Destination Options         : Disabled
      Unknown Destination Options         : Disabled
      IPv6 Nested Fragmentation           : Disabled

    Max-Packet-Size:
      ICMP                          : 65535
      Non-ICMP                      : 65535
    Flooding:
      ICMP limit                    : 1000
      UDP limit                     : 1000
      TCP-SYN limit                 : 1000
```

```
  Sampling Interval              : 1

TCP-SYN Flood Intercept:
  Mode                           : None
  Max-Attempts                   : 5
  Retrans-timeout                : 60
  Watch-timeout                  : 30
Mime-Flood Params:
  HTTP Header-Limit              : 16
  HTTP Max-Header-Field-Size     : 4096

No Firewall Ruledef Match Action:
  Uplink Action                  : permit
  Downlink Action                : deny

TCP RST Message Threshold     : Disabled
ICMP Dest-Unreachable Threshold    : Disabled
Action upon receiving TCP SYN packet with ECN/CWR Flag set    : Permit
Action upon receiving a malformed packet  : Deny
Action upon IP Reassembly Failure   : Deny
Action upon receiving an IP packet with invalid Options : Permit
Action upon receiving a TCP packet with invalid Options : Permit
Action upon receiving an ICMP packet with invalid Checksum: Deny
Action upon receiving a TCP packet with invalid Checksum: Deny
Action upon receiving an UDP packet with invalid Checksum: Deny
Action upon receiving an ICMP echo packet with id zero : Permit
TCP Stateful Checks : Enabled
First Packet Non-SYN Action: Drop
ICMP Stateful Checks: Enabled
TCP Partial Connection Timeout: 30
```

Enabling Firewall for IPv4 and IPv6

Following is the configuration to enable the firewall for IPv4 and IPv6:

```
configure
          active-charging service service_name
             fw-and-nat policy policy_name
                firewall policy ipv4-and-ipv6
                end
```

Configuration Support for Subscriber Firewall

The Control Plane pushes the required configuration for the subscriber firewall to the User Plane through PFD management. Firewall configurations are available under active charging configuration.

- Access-Rule-Defs
- Firewall-Nat Policy

Firewall feature configuration supports activation of firewall feature using rulebase, APN-based, and/or subscriber-based activation.

This section details the different aspect of configuration for the subscriber firewall in CUPS.

- Config delete command deletes the configuration immediately. It doesn't wait for bulk config timer as the said config is removed from the SCT and it's deleted from all Sessmgrs immediately.

- Addition/deletion/Modification of firewall configuration from CP to UP propagates using CLI command "push config-to-up all".

Monitoring and Troubleshooting

Following is the show command output for the default Firewall feature on Control Plane.

show config active-charging service name acs verbose

```
fw-and-nat policy SFW_NAT_TEST
      no firewall dos-protection source-router
      no firewall dos-protection winnuke
      no firewall dos-protection mime-flood
      no firewall dos-protection ftp-bounce
      no firewall dos-protection ip-unaligned-timestamp
      no firewall dos-protection tcp-window-containment
      no firewall dos-protection teardrop
      no firewall dos-protection flooding udp
      no firewall dos-protection flooding icmp
      no firewall dos-protection flooding tcp-syn
      no firewall dos-protection port-scan
      no firewall dos-protection ipv6-extension-hdrs
      no firewall dos-protection ipv6-hop-by-hop
      no firewall dos-protection ipv6-hop-by-hop router-alert
      no firewall dos-protection ipv6-hop-by-hop jumbo-payload
      no firewall dos-protection ipv6-hop-by-hop invalid-options
      no firewall dos-protection ipv6-hop-by-hop unknown-options
      no firewall dos-protection ipv6-dst-options
      no firewall dos-protection ipv6-dst-options invalid-options
      no firewall dos-protection ipv6-dst-options unknown-options
      no firewall dos-protection ipv6-frag-hdr nested-fragmentation
      no firewall dos-protection ip-sweep tcp-syn
      no firewall dos-protection ip-sweep udp
      no firewall dos-protection ip-sweep icmp
      firewall max-ip-packet-size 65535 protocol icmp
      firewall max-ip-packet-size 65535 protocol non-icmp
      firewall flooding protocol icmp packet limit 1000
      firewall flooding protocol udp packet limit 1000
      firewall flooding protocol tcp-syn packet limit 1000
      firewall flooding sampling-interval 1
      firewall tcp-syn-flood-intercept mode none
      firewall tcp-syn-flood-intercept watch-timeout 30
      firewall mime-flood http-headers-limit 16
      firewall mime-flood max-http-header-field-size 4096
      no firewall icmp-destination-unreachable-message-threshold
      access-rule no-ruledef-matches uplink action permit
      access-rule no-ruledef-matches downlink action deny
      firewall tcp-idle-timeout-action reset
      no firewall tcp-reset-message-threshold
      firewall tcp-syn-with-ecn-cwr permit
      firewall malformed-packets drop
      firewall ip-reassembly-failure drop
      no firewall validate-ip-options
      firewall tcp-options-error permit
      firewall icmp-echo-id-zero permit
      firewall icmp-checksum-error drop
      firewall tcp-checksum-error drop
      firewall udp-checksum-error drop
      firewall tcp-fsm first-packet-non-syn drop
      firewall icmp-fsm
```

```
  firewall policy ipv4-and-ipv6
  firewall tcp-partial-connection-timeout 30
  no nat policy
  no nat binding-record
  no nat pkts-drop edr-format
  no nat pkts-drop timeout
  default nat suppress-aaa-update
  nat private-ip-flow-timeout 180
  nat check-point-info basic limit-flows 100
  nat check-point-info sip-alg
  nat check-point-info h323-alg
  nat max-chunk-per-realm single-ip
#exit
```

Show CLIs for CUPS

Following are the show CLIs for the CUPS:

For User Plane:

- show subscribers user-plane-only full all
- show subscribers user-plane-only flows
- show user-plane-service inline-services firewall statistics verbose
- show user-plane-service statistics rulebase all
- show alarm outstanding all
- show alarm outstanding all verbose
- show alarm statistics
- show user-plane-service statistics rulebase name <rulebasename>

For Control Plane:

- show active-charging fw-and-nat policy all
- show active-charging fw-and-nat policy name "fw_nat_policy_name"
- show active-charging firewall track-list attacking-servers
- show active-charging ruledef name

SNMP Traps

Following are the SNMP traps in support of this feature for CUPS, Use the respective trap CLIs on the User Plane to enable the trap.

- **Dos-Attacks**: When the number of DoS attacks exceed the set threshold value, the SNMP trap is generated, and the trap is cleared when the number falls below the threshold value within the time interval configured.
- **Drop-Packets**: When the number of packets dropped exceeds the threshold value, the SNMP trap is generated, the trap is cleared when the number falls below the threshold value within the time interval configured.

- **Deny-Rule**: When the number of Deny Rules exceeds the threshold value, the SNMP trap is generated, the trap is cleared when the number falls below the threshold value within the time interval configured.
- **No-Rule**: When the number of No Rules exceeds the threshold value, the SNMP trap is generated, the trap is cleared when the number falls below the threshold value within the time interval configured.

Reassembly Behavior Change

Following are the details about the CUPS reassembly, which are different from the non-CUPS architecture:

- In non-CUPS architecture, with the default FW configuration, fragments are buffered up to 64K bytes. Beyond 64K, all buffered and subsequent fragments are dropped. In non-CUPS architecture, this 64K limit was configurable from 30000 -> 65535. In CUPS, it is possible to reassemble the packet size of maximum 9k in a maximum of six fragments.
- Following are the four CLIs from the non-CUPS architecture that are deprecated in the CUPS:
  - firewall dos-protection teardrop
  - firewall dos-protection ipv6-frag-hdr nested-fragmentation
  - firewall max-ip-packet-size <30000-65535> protocol non-icmp
  - o firewall max-ip-packet-size <30000-65535>protocol icmp
- The following is a single CLI that covers teardrop attack, nested fragmentation, and general ip-reassembly-failure. Max-ip-packet size support is limited to six fragments (~9000 bytes).
  - o Firewall ip-reassembly-failure
- Following are the counters in firewall statistics, that gets incremented for all the attacks related to reassembly.
  - Packets Dropped due to IPv4 Reassembly Failure
  - Downlink Dropped Bytes on IPv4 Reassembly Failure
  - Uplink Dropped Bytes on IPv4 Reassembly Failure
  - Packets Dropped due to IPv6 Reassembly Failure
  - Downlink Dropped Bytes on IPv6 Reassembly Failure
  - Uplink Dropped Bytes on IPv6 Reassembly Failure