Understanding Zone and DoS Protection Event Logs and Global Counters

Revision C
 www.paloaltonetworks.com

Contents

Overview

Palo Alto Networks firewalls provide Zone Protection and DoS Protection profiles to help mitigate against flood attacks, reconnaissance activity, and packet based attacks. As denial of service attacks can originate from many sources at extremely high rates, the firewall will log these types of attacks differently from other logging events to ensure that the firewall's resources are not depleted by the attack. This will ensure that the firewall itself is not DoS'd by attempting to log all the activity from high volume attacks.

Depending on the DoS attack type, the firewall will use either Threat Logs or Global Counters to track the activity. This tech note identifies the key log events and counters of interest.

Threat Events for Zone and DoS Activity Monitoring

The firewall will generate event logs for the following specific DoS attack activity.

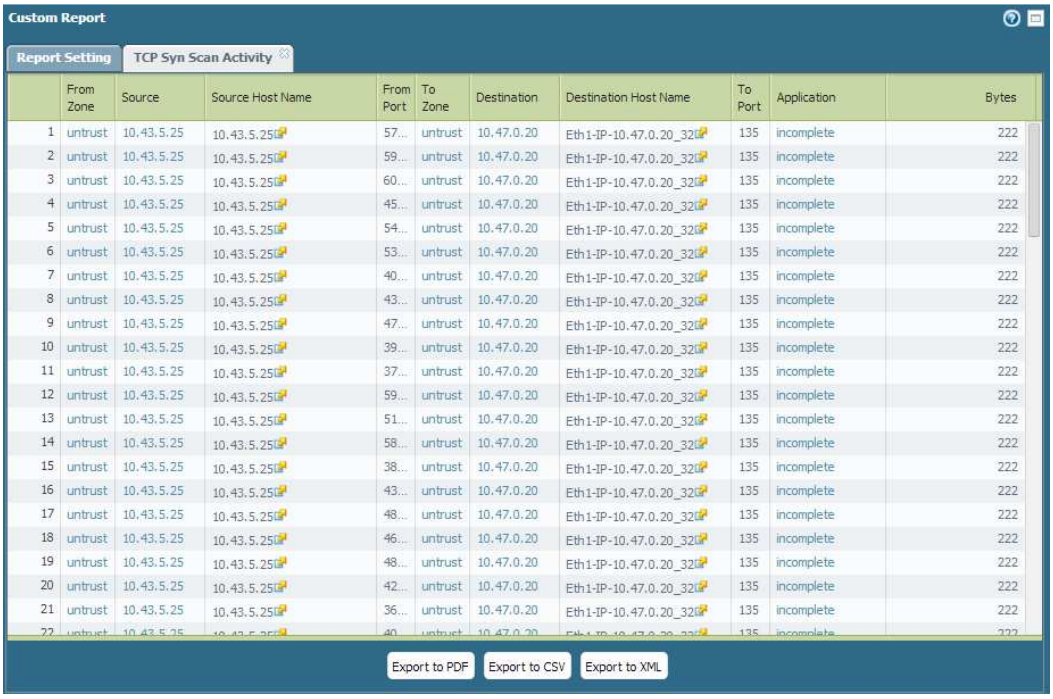
Reconnaissance Protection – When action is set to "alert" a threat event is logged when the scan or sweep activity matches the threshold within the specified time interval.

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
	03/19 11:07:51	scan	SCAN: TCP Port Scan	Untrust	trust	192.168.1.6		1.1.1.2	1864	not-applicable	allow	medium

Zone Reconnaissance protection log details will be provided for the TCP Port Scan, UDP Port Scan, and Host Sweep attacks and will show the Source/Destination Zone and Source/Destination IP Address. Port scan and host sweep attack profiles work in conjunction with security policies and will only product logs for traffic that is allowed through the firewall. T

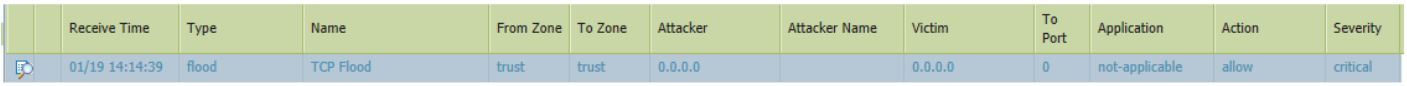
In addition to Threat Logs, Traffic logs can also be used in custom reports to generate port scanning attacks. For example, a custom report with the following filter can be used to look for scan activity or abnormal incomplete application activity.

Custom Report Filter Parameters
Database: Traffic Log
Columns: Source Zone, Source Address, Source Port, Destination Zone, Destination Address, Destination Port, Application, Bytes
Query Builder: (app eq incomplete) and (port.dst leq 1023)



	From Zone	Source	Source Host Name	From Port	To Zone	Destination	Destination Host Name	To Port	Application	Bytes
1	untrust	10.43.5.25	10.43.5.25	57...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
2	untrust	10.43.5.25	10.43.5.25	59...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
3	untrust	10.43.5.25	10.43.5.25	60...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
4	untrust	10.43.5.25	10.43.5.25	45...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
5	untrust	10.43.5.25	10.43.5.25	54...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
6	untrust	10.43.5.25	10.43.5.25	53...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
7	untrust	10.43.5.25	10.43.5.25	40...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
8	untrust	10.43.5.25	10.43.5.25	43...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
9	untrust	10.43.5.25	10.43.5.25	47...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
10	untrust	10.43.5.25	10.43.5.25	39...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
11	untrust	10.43.5.25	10.43.5.25	37...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
12	untrust	10.43.5.25	10.43.5.25	59...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
13	untrust	10.43.5.25	10.43.5.25	51...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
14	untrust	10.43.5.25	10.43.5.25	58...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
15	untrust	10.43.5.25	10.43.5.25	38...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
16	untrust	10.43.5.25	10.43.5.25	43...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
17	untrust	10.43.5.25	10.43.5.25	48...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
18	untrust	10.43.5.25	10.43.5.25	46...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
19	untrust	10.43.5.25	10.43.5.25	48...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
20	untrust	10.43.5.25	10.43.5.25	42...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
21	untrust	10.43.5.25	10.43.5.25	36...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222
22	untrust	10.43.5.25	10.43.5.25	40...	untrust	10.47.0.20	Eth1-IP-10.47.0.20_32	135	incomplete	222

Flood Protection - When “Alert (packets/sec)” threshold is reached for *new connection* attempts (TCP or UDP), a threat event is logged to record the event. The firewall will only record the event once for each 5 second period to prevent flooding the log database.



Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
01/19 14:14:39	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	allow	critical

Zone protection log details will be provided for the Flood attacks and will show the ingress zone and 0.0.0.0:0 for the IP Address and Port.

DoS protection log details will be provided for the TCP Flood, UDP Flood, and ICMP Flood attacks and will show the source/destination zone and the attacker’s IP Address.

Global Counters for DoS Activity Monitoring

To supplement the Threat event logs for Zone and DoS protection, the following CLI commands can provide additional information in the form of global counters and session count information to help identify DoS activity.

```
show counter global name ?                  Lists all global counters
show counter global filter aspect dos       List all global counters with active DoS
                                            aspect values
```

Counter Aspects

PAN-OS allows filtering of the Global Counters by category, aspect, and severity to make it easy to pull the relevant counters for review. Counters of interest that are related to Zone and DoS protection include:

Category:	Flow	Aspect: dos
Category:	Flow	Aspect: parse
Category:	Flow	Aspect: ipfrag

Example of CLI command to extract Flow counters with a DoS aspect:

```
show counter global filter category flow aspect dos
```

Note: Only counters with a non-zero value are displayed with the show commands.

A list of all Flow counters with aspect DoS includes:

```
flow_dos_ag_buckets_upd                 info    Updated aggregate buckets for aging
flow_dos_ag_curr_sess_add_incr          info    Incremented aggregate current session count on session create
flow_dos_ag_curr_sess_del_decr          info    Decremented aggregate current session count on session delete
flow_dos_ag_max_sess_limit              drop    Session limit reached for aggregate profile, drop session
flow_dos_ag_no_rt_sess_add              info    No rt info for aggregate profile in profile runtime tbl during
                                                session
flow_dos_ag_no_rt_sess_del              info    No rt info for aggregate profile in profile runtime tbl during
                                                session
flow_dos_blk_no_empty_entp              info    Unable to find empty block tbl entry during insertion
flow_dos_blk_num_entries                info    Number of entries in DOS block table
flow_dos_blk_tbl_buckets_upd            info    Updated block table buckets for aging
flow_dos_cl_buckets_upd                 info    Updated classified buckets for aging
flow_dos_cl_curr_sess_add_incr          info    Incremented classified current session count on session create
flow_dos_cl_curr_sess_del_decr          info    Decremented classified current session count on session delete
flow_dos_cl_max_sess_limit              drop    Session limit reached for classified profile, drop session
flow_dos_cl_no_rt_sess_add              info    No rt info for classified profile in profile runtime tbl
                                                during session
flow_dos_cl_no_rt_sess_del              info    No rt info for classified profile in profile runtime tbl
                                                during session
flow_dos_cl_rule_del_entp_clr           info    Cleared old rule info from classified tbl
flow_dos_cl_syncookie_ack_err           info    TCP SYN cookies: Invalid ACKs received, classified profile
flow_dos_cl_syncookie_ack_rcv           info    TCP SYN cookies: ACKs to cookies received, classified profile
flow_dos_cl_syncookie_blk_dur           drop    Packets dropped: Flagged for blocking and under block duration
```

		for classified profile
flow_dos_cl_syncookie_max	drop	Packet dropped: SYN cookies maximum threshold reached, classified profile
flow_dos_cl_syncookie_sent	info	TCP SYN cookies: cookies sent, classified profile
flow_dos_curr_sess_add_no_entp	info	Unable to find classified entry to update session count on session create
flow_dos_curr_sess_decr_failed	drop	Unable to decrement current session count on session delete
flow_dos_curr_sess_del_no_entp	info	Unable to find classified entry to update session count on session delete
flow_dos_curr_sess_incr_failed	drop	Unable to increment current session count on session create
flow_dos_drop_ip_blocked	drop	Packets dropped: Flagged for blocking and under block duration by oth
flow_dos_ip6_IPv6ExtHdrDestOpt	drop	Packets dropped: Zone protection option 'dest-option-hdr'
flow_dos_ip6_IPv6ExtHdrHopByHop	drop	Packets dropped: Zone protection option 'hop-by-hop-hdr'
flow_dos_ip6_IPv6ExtHdrRouting	drop	Packets dropped: Zone protection option 'routing-hdr'
flow_dos_ip6_OptionsInvalidIPv6	drop	Packets dropped: Zone protection option 'options-invalid-ipv6-discard
flow_dos_ip6_acast	drop	Packets dropped: Zone protection option 'anycast-source'
flow_dos_ip6_icmpv6ErrorInvalid	drop	Packets dropped: Zone protection option 'icmpv6-too-big-small-mtu-dis
flow_dos_ip6_ip4cmpt	drop	Packets dropped: Zone protection option 'ipv4-compatible-address'
flow_dos_ip6_needlessIpv6FragHdr	drop	Packets dropped: Zone protection option 'needless-fragment-hdr'
flow_dos_ip6_route0	drop	Packets dropped: Zone protection option 'routing-header'
flow_dos_ip6_rsvdSet	drop	Packets dropped: Zone protection option 'reserved-field-set-discard'
flow_dos_no_empty_entp	info	Unable to find empty classified entry during insertion
flow_dos_pf_badoption	drop	Packets dropped: Zone protection option 'discard-malformed-option'
flow_dos_pf_icmperr	drop	Packets dropped: Zone protection option 'discard-icmp-error'
flow_dos_pf_icmpfrag	drop	Packets dropped: Zone protection option 'discard-icmp-frag'
flow_dos_pf_icmplpkt	drop	Packets dropped: Zone protection option 'discard-icmp-large-packet'
flow_dos_pf_ipfrag	drop	Packets dropped: Zone protection option 'discard-ip-frag'
flow_dos_pf_ipspoof	drop	Packets dropped: Zone protection option 'discard-ip-spoof'
flow_dos_pf_loosesource	drop	Packets dropped: Zone protection option 'discard-loose-source-routing
flow_dos_pf_noreplyneedfrag	drop	Packets dropped: Zone protection option 'suppress-icmp-needfrag'
flow_dos_pf_noreplyttl	drop	Packets dropped: Zone protection option 'suppress-icmp-timeexceeded'
flow_dos_pf_ping0	drop	Packets dropped: Zone protection option 'discard-icmp-ping-zero-id'
flow_dos_pf_recordroute	drop	Packets dropped: Zone protection option 'discard-record-route'
flow_dos_pf_satnetid	drop	Packets dropped: Zone protection option 'discard-stream-id'
flow_dos_pf_security	drop	Packets dropped: Zone protection option 'discard-security'
flow_dos_pf_strictsource	drop	Packets dropped: Zone protection option 'discard-strict-source-routing’
flow_dos_pf_tcpoverlappingmismatch	drop	Packets dropped: Zone protection option 'discard-overlapping-tcp-segment’
flow_dos_pf_timestamp	drop	Packets dropped: Zone protection option 'discard-timestamp'
flow_dos_pf_unknown	drop	Packets dropped: Zone protection option 'discard-unknown-option'
flow_dos_red_icmp	drop	Packets dropped: Zone protection protocol 'icmp' RED
flow_dos_red_icmp6	drop	Packets dropped: Zone protection protocol 'icmpv6' RED
flow_dos_red_ip	drop	Packets dropped: Zone protection protocol 'other-ip' RED
flow_dos_red_tcp	drop	Packets dropped: Zone protection protocol 'tcp-syn' RED
flow_dos_red_udp	drop	Packets dropped: Zone protection protocol 'udp' RED
flow_dos_rule_ag_blk_dur	drop	Packets dropped: Flagged for blocking and under block duration for aggregate
flow_dos_rule_ag_red_act	drop	Packets dropped: Activate aggregate RED threshold reached, random early drop
flow_dos_rule_ag_red_max	drop	Packets dropped: Maximal aggregate RED threshold reached
flow_dos_rule_allow	info	Packets allowed: Allowed action by DoS policy
flow_dos_rule_allow_under_rate	info	Packets allowed: Rate within thresholds of DoS policy
flow_dos_rule_deny	drop	Packets dropped: Denied action by DoS policy
flow_dos_rule_drop	drop	Packets dropped: Rate limited or IP blocked
flow_dos_rule_drop_aggr	drop	Packets dropped: due to aggregate rate limiting
flow_dos_rule_drop_cl_blk_dur	drop	Packets dropped: Flagged for blocking and under block duration for classified
flow_dos_rule_drop_cl_red_act	drop	Packets dropped: Activate classified RED threshold reached, random early drop
flow_dos_rule_drop_cl_red_max	drop	Packets dropped: Maximal classified RED threshold reached
flow_dos_rule_drop_classified	drop	Packets dropped: due to classified rate limiting
flow_dos_rule_match	info	Packets matched DoS policy

```
flow_dos_rule_nomatch                    info    Packets not matched DoS policy
flow_dos_syncookie_ack_err               info    TCP SYN cookies: Invalid ACKs received, aggregate
                                                 profile/zone
flow_dos_syncookie_ack_rcv               info    TCP SYN cookies: ACKs to cookies received, aggregate
                                                 profile/zone
flow_dos_syncookie_blk_dur               drop    Packets dropped: Flagged for blocking and under block
                                                 duration for aggregate profile/zone
flow_dos_syncookie_cookie_sent           info    TCP SYN cookies: cookies sent, aggregate profile/zone
flow_dos_syncookie_max                   drop    Packet dropped: SYN cookies maximum threshold reached,
                                                 aggregate profile/zone
flow_dos_syncookie_svr_ack_rcv           info    TCP SYN cookies: Server ACKs received, aggregate profile/zone
flow_dos_zone_red_act                    drop    Packets dropped: Activate zone RED threshold reached, random
                                                 early drop
flow_dos_zone_red_max                    drop    Packets dropped: Maximal zone RED threshold reached
```

The following two Flow DoS counter groups display how many times a Zone protection profile option was hit.

```
flow_dos_pf_                                     Packet drops for Zone Protection options
flow_dos_red_                                    Packet drops for Zone Protection RED conditions
```

Other Flow counters that show Network Processor statistics for flow parsing drop activity can be of interest when researching DoS attacks. Specific counters for land attack, ping-of-death, and teardrop are included.

```
flow_parse_l2_err                        drop    Packets dropped: layer2 receive error
flow_parse_l4_cksm                       drop    Packets dropped: TCP/UDP checksum failure
flow_parse_l4_hdr                        drop    Packets dropped: TCP (UDP) packet too short
flow_parse_l4_len                        drop    Packets dropped: TCP/UDP length and IP length mismatch
flow_parse_l4_port                       drop    Packets dropped: illegal TCP/UDP port 0
flow_parse_l4_tcpfin                     drop    Packets dropped: invalid TCP flags (FIN only)
flow_parse_l4_tcpfinrst                  drop    Packets dropped: invalid TCP flags (FIN+RST+*)
flow_parse_l4_tcpsynfin                  drop    Packets dropped: invalid TCP flags (SYN+FIN+*)
flow_parse_l4_tcpsynrst                  drop    Packets dropped: invalid TCP flags (SYN+RST+*)
flow_parse_l4_tcpsynurg                  drop    Packets dropped: invalid TCP flags (SYN+URG+*)
flow_parse_l4_tcpzero                    drop    Packets dropped: invalid TCP flags (0)
flow_parse_land                          drop    Packets dropped: land attack
flow_parse_pingofdeath                   drop    Packets dropped: ping-of-death attack
flow_parse_teardrop                      drop    Packets dropped: teardrop attack
flow_parse_unmatched_icmperr             info    Packets dropped: Unmatched ICMP error message
```

Fragmentation counters that can show abnormal fragmentation in the flows include the following flow counters. Drops, errors, and fragments received are the most interesting.

Note: Fragmentation attacks are detected in the flow engines, which can also detect mal-formed packets and discard them. Since the firewall reassembles fragmented packets to retrieve the 5-tuple and content, any mal-formed packets hidden in fragmentation attacks will be detected and dropped.

```
  flow_ipfrag_del_fail                   info      IP fragment entry delete failure
  flow_ipfrag_del_fail_after_fwd         info      IP fragment entry delete failure after fwd
  flow_ipfrag_frag                       info      IP fragments transmitted
  flow_ipfrag_frag_err                   drop      Packet dropped: IP fragmentation error
  flow_ipfrag_free                       info      IP fragments freed after defragmentation
  flow_ipfrag_fwd                        info      IP fragments fwd to owner
  flow_ipfrag_ins_fail                   info      IP fragment entry insert failure
  flow_ipfrag_maxpkt_err                 error     IP fragments dropped due to reaching max pkt threshold
  flow_ipfrag_merge                      info      IP defragmentation completed
  flow_ipfrag_pkt                        info      packets held by IP fragmentation
  flow_ipfrag_pkt_alloc_err              error     Packet allocation failure for IP fragmentation processing
  flow_ipfrag_query                      info      IP fragments owner query
  flow_ipfrag_recv                       info      IP fragments received
  flow_ipfrag_refrag                     info      IP packets re-fragmented
  flow_ipfrag_swbuf                      info      Software buffers allocated for reassembled IP packet
  flow_ipfrag_tcp                        warn      TCP packets processed by IP fragmentation
```

Other TCP counters that may be of interest include the following warning and informational items. These counters can show abnormal TCP session activity.

```
tcp_drop_out_of_wnd                      warn      out-of-window packets dropped
tcp_exceed_flow_oo_seg_limit             warn      out-of-window packets dropped due to the limitation on tcp
```

```
                                                  out-of-order sequence
tcp_exceed_flow_seg_limit                warn     packets dropped due to the limitation on tcp out-of-order
                                                  queue size
tcp_exceed_seg_limit                     warn     packets dropped due to the limitation on global tcp out-of-
                                                  order pack
tcp_invalid_ts_option                    info     tcp packets with invalid timestamp option
tcp_new_syn                              warn     A new SYN packet in tcp session
tcp_oo_syn                               info     out-of-order SYN
tcp_syn_missing                          info     miss SYN packet for tcp session
```

Other Commands for Zone/DoS Protection Monitoring

The CLI command to display Zone configuration information with thresholds, current, and dropped packet statistics is: `show zone-protection zone` *zone_name*. This command can show attack activity with the "dropped" packet counts.

```
Zone L3-Trusted, vsys vsys1, profile Flood Protection Profile 1
------------------------------------------------------------------------------------------
  tcp-syn              SYN cookie enabled: yes
    DP alarm rate:         200 pps, activate rate:     300 pps, maximal rate:    1000 pps
    current:                 0 packets
    dropped:                 0 packets
------------------------------------------------------------------------------------------
  udp                  RED enabled: yes
    DP alarm rate:        1000 pps, activate rate:    1500 pps, maximal rate:    4000 pps
    current:                 0 packets
    dropped:                 0 packets
------------------------------------------------------------------------------------------
  icmp                 RED enabled: yes
    DP alarm rate:         200 pps, activate rate:     200 pps, maximal rate:     400 pps
    current:                 0 packets
    dropped:                 0 packets
------------------------------------------------------------------------------------------
  other-ip             RED enabled: no
------------------------------------------------------------------------------------------
  icmpv6               RED enabled: yes
    DP alarm rate:         200 pps, activate rate:     200 pps, maximal rate:     400 pps
    current:                 0 packets
    dropped:                 0 packets
------------------------------------------------------------------------------------------
IPv(4/6) Filter:
  discard-ip-spoof:                          enabled: yes, packet dropped: 0
  discard-ip-frag:                           enabled: yes, packet dropped: 0
  tcp-reject-non-syn:                        enabled: yes, (global), packet dropped: 1851
  asymmetric-path:                           enabled: no  (global)
IPv4 packet filter:
  discard-icmp-ping-zero-id:                 enabled: yes, packet dropped: 0
  discard-icmp-frag:                         enabled: yes, packet dropped: 0
  discard-icmp-large-packet:                 enabled: yes, packet dropped: 0
  discard-icmp-error:                        enabled: no
  suppress-icmp-timeexceeded:                enabled: no
  suppress-icmp-needfrag:                    enabled: no
  discard-strict-source-routing:             enabled: no
  discard-loose-source-routing:              enabled: no
  discard-timestamp:                         enabled: no
  discard-record-route:                      enabled: no
  discard-security:                          enabled: no
  discard-stream-id:                         enabled: no
  discard-unknown-option:                    enabled: yes, packet dropped: 0
  discard-malformed-option:                  enabled: yes, packet dropped: 0
  discard-overlapping-tcp-segment-mismatch:  enabled: no
IPv6 packet filter:
  routing-header:                            enabled: yes, packet dropped: 0
  ipv4-compatible-address:                   enabled: no
  anycast-source:                            enabled: no
```

In addition, the `show dos-protection` command can provide additional information for the DoS protection profiles.

Additional Helpful Commands

In addition to the global counters, several other CLI commands can be very helpful to extract interface, packet, connection and protocol statistics. These can be used as guidelines to set starting points for Zone and DoS protection profiles.

```
set system setting target-vsys          Set the target vsys to run commands
show interface ethernet1/1              Get the packets transmitted and received as well as key
                                         attack traffic
```

```
--------------------------------------------------------------------------------
Physical port counters read from MAC:
--------------------------------------------------------------------------------
rx-broadcast                  853620
rx-bytes                      9634407930
rx-multicast                  1012047
rx-unicast                    8600886
tx-broadcast                  35280
tx-bytes                      1827647835
tx-multicast                  0
tx-unicast                    7834584
--------------------------------------------------------------------------------

Hardware interface counters read from CPU:
--------------------------------------------------------------------------------
bytes received                          10246581155
bytes transmitted                       1795015413
packets received                        14055636
packets transmitted                     7869885
receive errors                          5862
packets dropped                         0
--------------------------------------------------------------------------------

Logical interface counters read from CPU:
--------------------------------------------------------------------------------
bytes received                          10242372819
bytes transmitted                       1795015413
packets received                        14049800
packets transmitted                     7869885
receive errors                          0
packets dropped                         714188
packets dropped by flow state check     92147
forwarding errors                       0
no route                                0
arp not found                           2
neighbor not found                      0
neighbor info pending                   0
mac not found                           0
packets routed to different zone        0
land attacks                            0
ping-of-death attacks                   0
teardrop attacks                        0
ip spoof attacks                        0
mac spoof attacks                       0
ICMP fragment                           0
layer2 encapsulated packets             0
layer2 decapsulated packets             0
--------------------------------------------------------------------------------
```

`show system statistics session` Get the packet rate, throughput rate, active sessions (UDP, TCP, ICMP)

```
System Statistics: ('q' to quit, 'h' for help)

Device is up          : 15 days 0 hour 28 mins 53 sec
Packet rate           : 2/s
Throughput            : 0 Kbps
Total active sessions : 21
Active TCP sessions   : 5
Active UDP sessions   : 16
Active ICMP sessions  : 0
```

`show system statistics application vsys` Get the application statistics running on the vsys specified – sessions, packets, bytes

```
Top 20 Application Statistics: ('q' to quit, 'h' for help)

Virtual System: vsys1
application                    sessions   packets      bytes
------------------------------ ---------- ------------ ------------
ironmountain-connected         4          1306960      619896323
itunes-mediastore              52         292435       339907004
ssl                            10466      10495227     8884521008
dns                            516342     2958799      289440438
web-browsing                   6097       350234       262551791
unknown-udp                    12         187101       260321392
netflow                        4          119616       167227528
grooveshark                    128        99850        113048332
paloalto-updates               121        91200        99786875
google-video-base              10         38586        30923913
itunes-base                    457        27055        15221899
gmail-base                     93         21851        13105738
google-plus-base               144        20393        12422606
linkedin-base                  193        14811        8816179
concur                         42         9935         7552599
flash                          36         7486         7363877
icloud-base                    175        12272        4689111
http-video                     2          4195         3748369
bugzilla                       116        5226         3151163
facebook-base                  126        5632         2890402
```

`netstat interfaces yes` Get interface packet OK and Err statistics

```
jwan@pm-firewall(active)> netstat interfaces yes
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0 111162688      0      0      0 124299308      0      0      0 BMRU
eth1       1500   0        0      0      0      0        0      0      0      0 BMU
lo        16436   0 89040446      0      0      0 89040446      0      0      0 LRU
pci0       1500   0 43976635      0      0      0 47645209      0      0      0 BMRU
vr1        1500   0  5024671      0      0      0  3605676      0      0      0 BMRU
vr2        1500   0        0      0      0      0       21      0      0      0 BMRU
vr3        1500   0        0      0      0      0        8      0      0      0 BMRU
vr251      1500   0  7160428      0      0      0  5573653      0      0      0 BMRU
jwan@pm-firewall(active)>
```

`netstat statistics yes` Get detailed IP, ICMP, ICMPMsg, TCP and UDP statistics

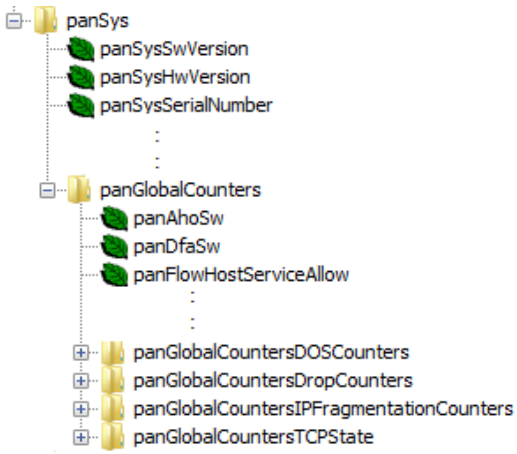
```
jwan@pm-firewall(active)> netstat statistics yes
Ip:
    255646035 total packets received
    9289 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    254682116 incoming packets delivered
    265118048 requests sent out
    606125 reassemblies required
    212518 packets reassembled ok
    926295 fragments received ok
    5520544 fragments created
Icmp:
    8789380 ICMP messages received
    12 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 943442
        timeout in transit: 14
        echo requests: 1140366
        echo replies: 6705558
    9848374 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 862013
        echo request: 7845995
        echo replies: 1140366
IcmpMsg:
        InType0: 6705558
        InType3: 943442
        InType8: 1140366
        InType11: 14
        OutType0: 1140366
        OutType3: 862013
        OutType8: 7845995
Tcp:
    8035024 active connections openings
    710735 passive connection openings
    173138 failed connection attempts
    10964 connection resets received
    138 connections established
    189100961 segments received
    199135664 segments send out
    482154 segments retransmited
    21 bad segments received.
    11393 resets sent
Udp:
    56713176 packets received
    3 packets to unknown port received.
    499 packet receive errors
    55651854 packets sent
    RcvbufErrors: 499
UdpLite:
error parsing /proc/net/netstat: Success
```

PAN-OS DoS Counter MIB

Starting with PAN-OS v7.0.0, the following counters can also be accessed through Palo Alto Networks private MIBs:

- panGlobalCountersDOSCounters
- panGlobalCountersDropCounters
- panGlobalCountersIPFragmentationCounters
- panGlobalCountersTCPState

By monitoring MIB counters with an external management system, you can track historical information and build trending information for critical DoS counters.



Other Network Monitoring Options

NetFlow can be used to profile network utilization and help identify abnormal traffic patterns. There are many free or low cost NetFlow collectors, but not all of them will collect and display DoS related statistics. The following products are a few popular NetFlow collectors:

- SolarWinds
- PRTG Network Monitor
- Manage Engine Netflow Analyzer

Note: Palo Alto Networks does not endorse any of these NetFlow collectors or provide support for them. Support should be obtained from the manufacturer.

Revision History

Date	Revision	Comment
Mar 19, 2014	A	• Created document
Jan 23, 2015	B	• Updated with Zone protection Port and Host Sweep logging
Jun 18, 2015	C	• Updated with PAN-OS 7.0.0 DoS counter MIB