Understanding DoS Protection in PAN-OS
Tech Note

Contents

Overview **3**

Zone-Based Protection **3**

Flood Protection 3
SYN Floods 3
How does RED work? *3*
How does SYN Cookie work? *4*
Tuning Thresholds – Case Studies 5
Scenario 1: Maximizing Performance *5*
Scenario 2: Protecting your Session Table *8*
ICMP Floods 9
UDP Floods 10
Packets Per Second vs. Sessions Per Second 10
Reconnaissance Protection 10
Actions *10*
Packet Based Attacks 11
IP Spoof Protection *11*
Fragmented Traffic *12*
Mismatched Overlapping TCP segment *12*
Reject non-SYN TCP packet *12*
Asymmetric Path *12*
IP Option Drop *12*
ICMP ping ID 0 ..... *13*
ICMP Fragment *13*
Suppress ICMP TTL Expired Error *13*
Suppress ICMP NEEDFRAG *13*
IPv6 Drop *13*
ICMPv6 Drop *13*
Configuration and Troubleshooting 13
Logs with Random Early Drop *15*
Logs with SYN cookie *16*

End Point Protection (DoS Profile and Rule base) **17**

Scenario: 17
DoS Protection Rules 18
DoS Rule Match Criteria *18*
DoS Rule Actions *18*
DoS Protection Profiles 19
Aggregate Profiles *19*
Classified Profiles *19*
DoS Profile Types 19
Flood (Behavior-based) Protection *19*
Resource Based Protection *19*
Protection Precedence and Limitations 19
Configuration and Troubleshooting 20

Summary **21**

Revision History **21**

Overview

A Denial of Service (DoS) attack is an attempt to disrupt network services by overloading the network with unwanted traffic. PAN-OS DoS protection features protect your firewall and in turn your network resources and devices from being exhausted or overwhelmed in the event of network floods, host sweeps, port scans and packet based attacks. The DoS protection features provide flexibility by varying the granularity of protection and provide usability through a variety of options that cover most of the attacks in the current DoS landscape. In this tech note we will explain the deployment of DoS protection features with the help of best practices and guidelines, analyze threshold parameters using specific scenarios, discuss real-world applications and enable effective end point protection.

DoS Protection in PAN-OS takes a two-pronged approach to mitigate DoS attacks:

1. Zone-Based Protection – A broad-based comprehensive DoS template at the edge to prevent the enterprise network from volumetric DoS attacks. It acts as a first line of defense for the network.
2. End Host Protection (DoS Rule base and Profiles) – A flexible policy rule base that provides a scalpel-like granularity in protecting specific end hosts (web servers, DNS servers, user subnets), which are critical or have been historically prone to DoS attacks. It also protects from attacks originating within the private network by filtering on compromised servers and rogue end hosts.

The above mentioned approaches complement each other and are recommended to be deployed in tandem to achieve the best results against the various DoS attacks observed on the internet today. These are explained in detail in the sections below.

Zone-Based Protection

A zone protection profile offers protection against most common floods, reconnaissance attacks and other packet-based attacks. It can be used as a template configuration for applying similar settings to multiple zones. These settings apply to the ingress zone (i.e. the zone where traffic enters the firewall). Zone protection settings apply to all interfaces within the zone for which the profile is configured.

Note: Zone protection is only enforced when there is no session match for the packet. If the packet matches an existing session, it will bypass the zone protection setting.

Flood Protection

The Flood Protection sub-tab in the zone protection profile has configuration options to protect against SYN, UDP, ICMP, ICMPv6 and other IP floods. The value set in the Alert, Activate and Maximum fields are the packets per second from one or many hosts to one or many destinations. Flood protection settings are applied to the ingress zone of the traffic. Packets from any host entering the firewall from the zone that has zone protection profile enabled are sampled at an interval of one second. This is to determine if the rate matches the threshold values. Once the thresholds are reached, an appropriate action is taken depending on the type of the threshold. For example an alert log is generated, a flood protection mechanism is activated or the incoming packets are dropped.

SYN Floods

Flooding a host or a network with incomplete TCP connections, the attacker can eventually fill up the memory buffers or spike the CPU utilization of the victim device. Once the buffers are full or the CPU is overwhelmed, the host cannot process new TCP connection requests. The flood might even damage the victim's operating system. Either way, the attack disables the victim and its normal operations. PAN-OS supports SYN cookie and Random Early Detection (RED) for protection against such SYN floods.

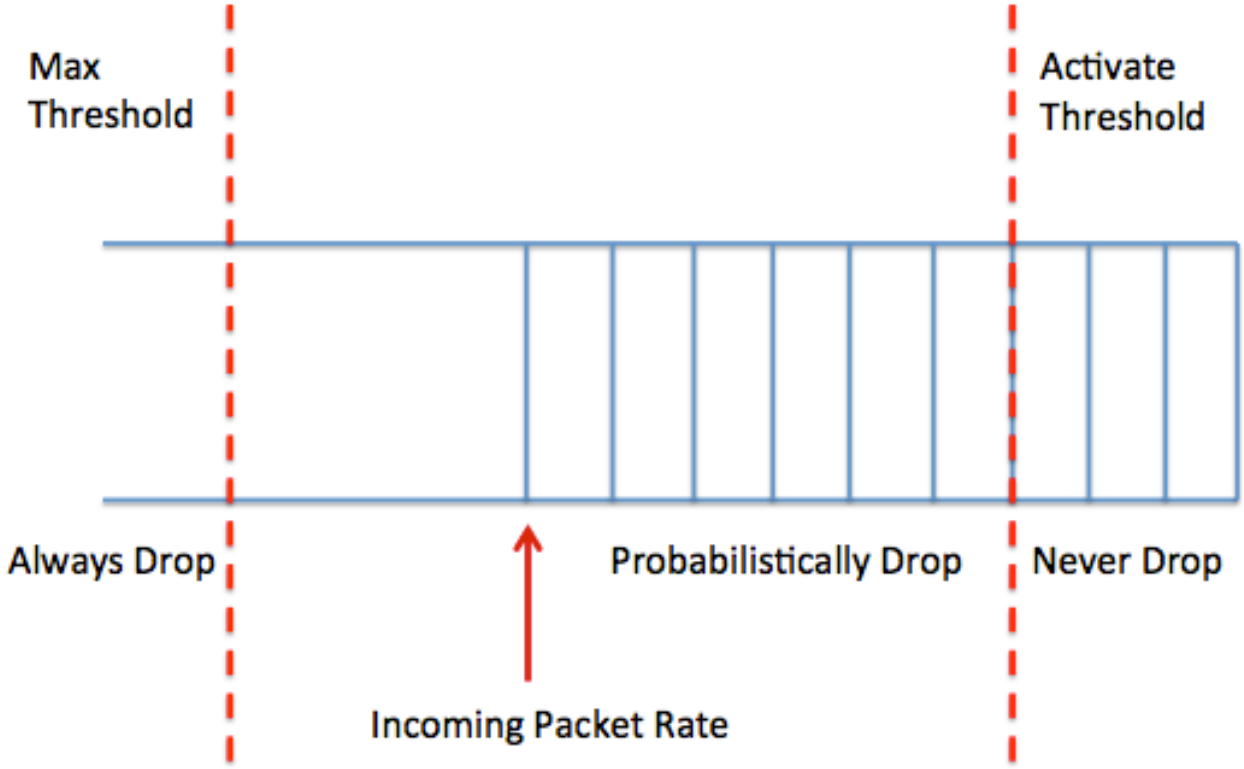
How does RED work?

An Active Queue Management (AQM) algorithm like Random Early Detection (also known as Random Early Drop or RED) is one of the most common methods to protect against SYN flood attacks. With RED, given a packet rate within one sampling interval:

- If the rate falls between [0 and Activate threshold - 1], packet drop probability is 0.
- If the rate falls between [Activate threshold and Maximum threshold – 1], drop probability linearly increases from 0 to 1.

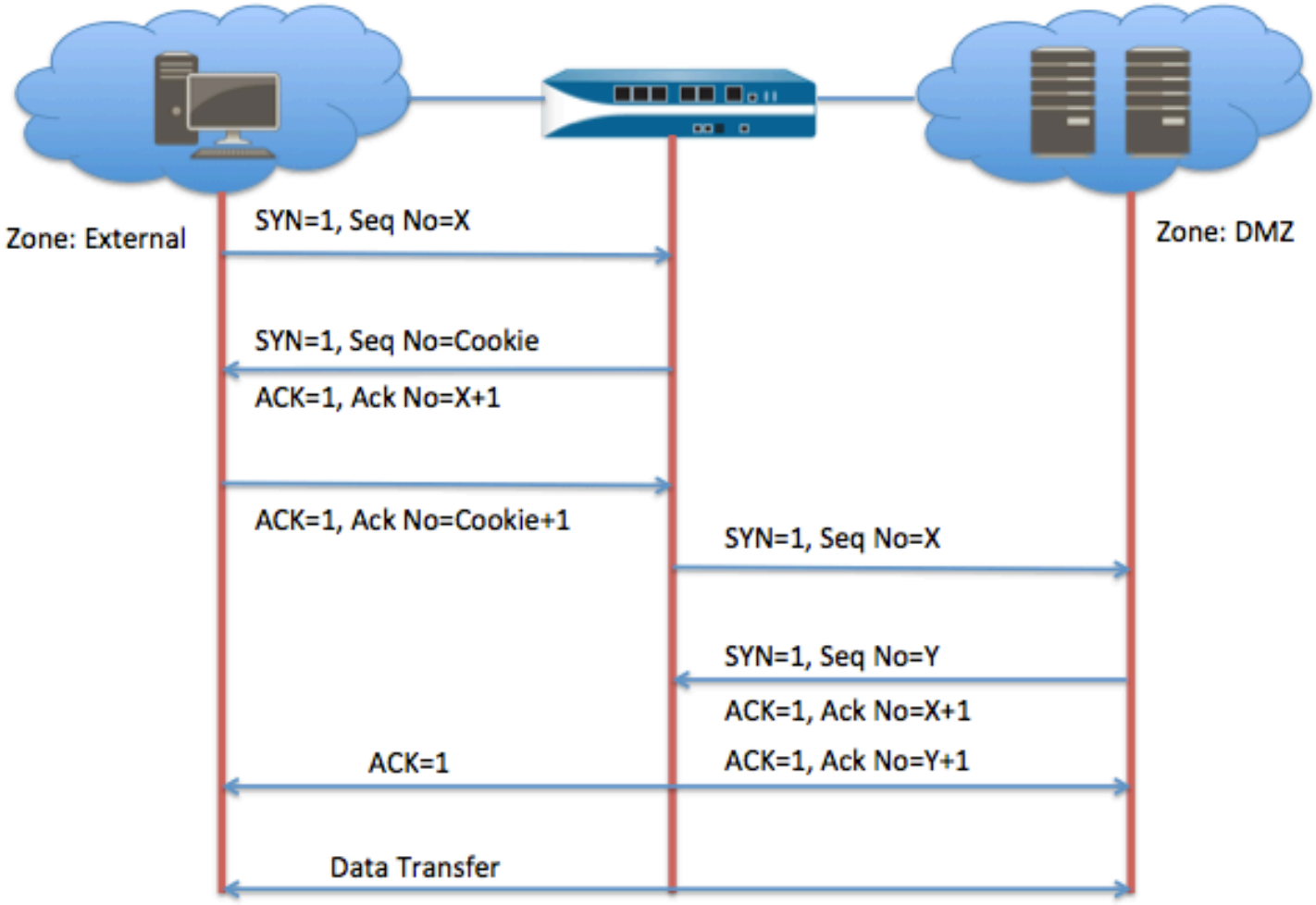
You can calculate the number of dropped packets, given rate X in [A to M], where A is the activate threshold, M is the maximum, then roughly (M – A) * sum (1/N, N in [M-X, M-A]) – (X – A).
This means that when X is less than A, the probability of a packet being dropped is 0 and if X is M the probability is 1 (100%). So after you go beyond A, probability linearly grows from point where at A no packets will be dropped to M where all packets will be dropped. If more packets are sent more will be dropped.

The effectiveness of RED depends on the proper calculation of the Activate and Maximum thresholds. If the thresholds are kept very low the algorithm can penalize legitimate traffic thereby being unfair. In contrast if the thresholds are set to very high values, it may not detect Low-rate DoS (LDoS) attacks. Also it requires maintenance of state for malicious traffic, which may lead to CPU and resource overhead.



How does SYN Cookie work?

SYN Cookie is a near stateless SYN proxy mechanism. Unlike traditional SYN proxy mechanisms, when a SYN segment is received SYN cookie does not set up a session or do policy or route lookups. It also doesn't maintain a connection request queue. This enables the firewall to maintain optimal CPU loads and prevent exhaustion of packet buffers. With SYN Cookie, the firewall acts as man-in-the-middle for the TCP handshake. The figure below shows how a connection is established between an initiating host and a server when SYN Cookie is active on a PAN-OS device. If SYN cookie is activated and the connection is found to be legitimate, the firewall does the sequence number translation for established connections. SYN Cookie is a recommended method as opposed to RED for its obvious advantages of fairness for legitimate traffic and less CPU overhead.



The intention behind using SYN Cookie is to not use any local resources to remember a SYN packet entering the firewall, because it might be a malicious one. However there are few pieces of information like maximum segment size (MSS), TCP window scaling option (WSOPT), selective acknowledgments (SACK), and so on that we need later on for legitimate connections. Hence some processing and resource overhead is introduced with SYN Cookie, albeit not as much as with other SYN proxy mechanisms or RED.

Tuning Thresholds – Case Studies

SYN Cookie protection involves the use of three threshold values, which play an important part in the performance and effectiveness of the mechanism against various scales of SYN flood attacks:

Alert: The number of SYN packets per second entering the ingress zone after which alarms are generated. Alarms can be viewed under threat logs, or dashboard. SNMP traps and syslog messages can also be sent.
Activate: The number of SYN packets per second entering the ingress zone after which RED or SYN cookie is triggered.
Maximum: The number of SYN packets per second entering the ingress zone after which any new SYN packet to any host in the zone is dropped. All other non-TCP traffic to the zone will pass normally.

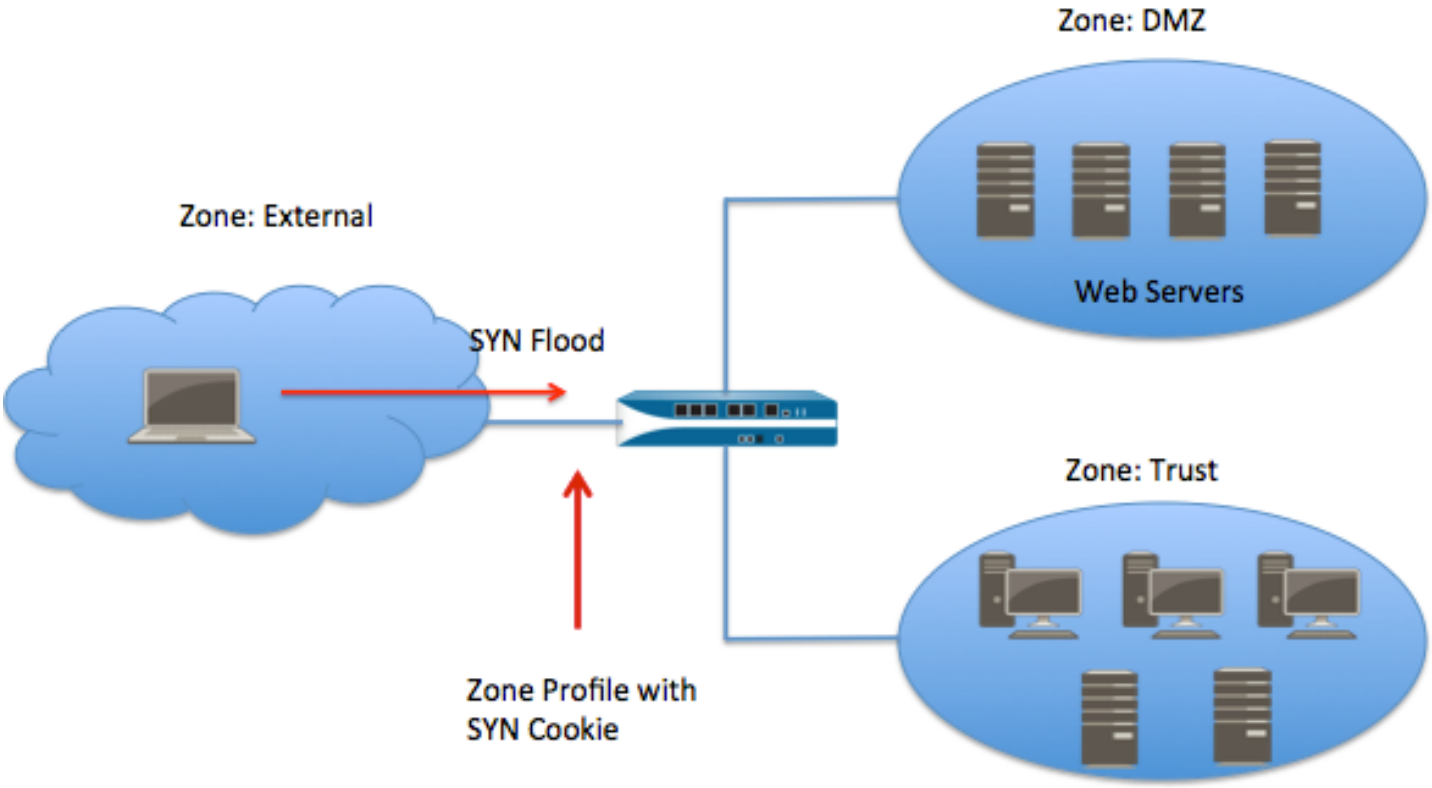
The optimal values of these threshold parameters depend on the following factors:

- Production traffic flowing through the network
- Resources that need to be protected

Scenario 1: Maximizing Performance

In this scenario a major online retail company, BayZon, has deployed Palo Alto Networks firewall(s) to secure its corporate network; the deployment topology is shown in the figure below. The corporate network has been segmented into three

Zones: Untrust (External facing), Trust (Internal corporate users and servers) and DMZ (guest application and web servers). Being in online retail business, BayZon has a security initiative to protect its web servers from malicious DoS attacks, which overrun the memory buffers, and spike up the server loads almost every other month. The security admin also observes that the firewall packet buffers and resource utilization increases to critical levels during these attacks. The security admin wants to have a broad-based protection mechanism from such external attacks without adding to the performance overhead of the firewall.



```
admin@PA-5060-2> show running resource-monitor second last 10

DP 0:

Resource monitoring sampling data (per second):

CPU load sampling by group:

flow_lookup                    :    61%

flow_fastpath                  :    61%

flow_slowpath                  :    61%

flow_forwarding                :    61%

flow_mgmt                      :   100%

flow_ctrl                      :    68%

nac_result                     :    61%

flow_np                        :    64%

dfa_result                     :    61%

module_internal                :    61%

aho_result                     :    61%

zip_result                     :    61%

pktlog_forwarding              :    55%

lwm                            :     0%

flow_host                      :    68%

CPU load (%) during last 10 seconds:

core   0   1   2   3   4   5   6   7   8   9  10  11

       0 100  67  69  64  61  59  57  56  56  55  53

       0 100  72  74  69  67  65  64  63  62  62  61

       0  98  58  57  54  51  50  49  48  47  47  46

       0  92  76  76  74  73  72  71  71  70  70  70

       0  97  83  85  82  80  79  78  78  77  77  76

       0 100  51  48  44  41  39  38  37  37  36  36

       0 100  52  49  46  44  43  42  42  41  41  41

       0  99  75  76  74  72  71  71  71  70  70  69

       0  80  94  95  94  94  94  93  93  93  93  93

Resource utilization (%) during last 30 seconds:

session:

  9   9   9  10  10   9  10  10  10   9

packet buffer:

 92  92  92  92  92  91  95  93  91  91

packet descriptor:
```

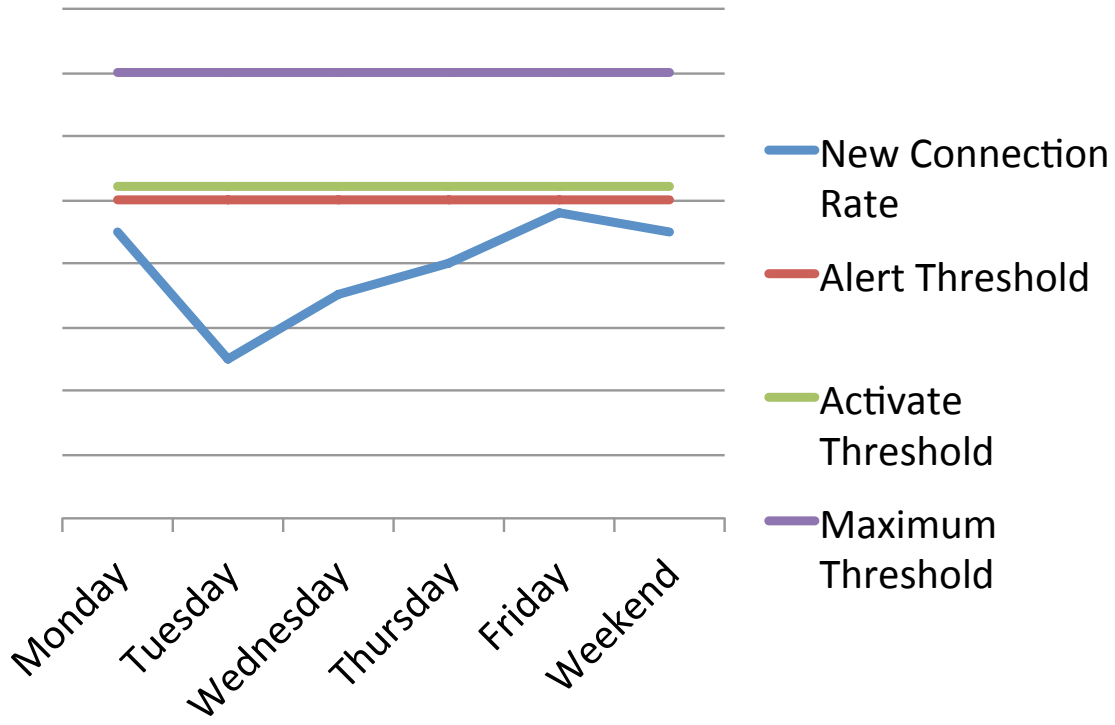
```
 35   35   35   35   35   35   36   35   34   34   35

packet descriptor (on-chip):

  9   10   11    9   10    9    8    8   25   17    8
```

Solution: Traffic Profiling

During a typical weekday/weekend the retail website traffic should be profiled using the Alert threshold knob. We can start tuning upwards from 10,000 pps, which is the default value. It is set to a value whereby you do not receive an alert log under the Monitor tab. After that we set the Activate threshold to match the Alert threshold or slightly above. To further improve the performance, bring down the maximum threshold from a default of one million pps to a value above the Activate threshold. This would ensure that additional sessions that cannot be handled by SYN cookie mechanism do not overwhelm the data plane CPU. A good rule of thumb is to put the Alert threshold approximately 10% above the average peak traffic, Activate to 10% above alert and finally Maximum to 20% to 30% above Activate.

Can we set Activate=0?

Yes we can and in some scenarios we should which will be discussed in the next section. However as we mentioned before there is some processing involved with SYN cookie as we have to wait for the ACK to come back from the receiver and then send back a packet to the sender. Setting a blanket value to a conservative minimum will activate SYN Cookie right away and will affect the CPU, packet buffers and packet descriptors utilization levels. This will negate the advantage of using SYN cookie in the first place. Instead a threshold value tuned to match the traffic profile of production traffic will protect the resources by activating SYN cookie at the appropriate incoming SYN rate. Yes it will allow some malicious connections to come in and increase the session table utilization before SYN cookie mechanism kicks in, but that is trade-off we need account for when setting the threshold values.

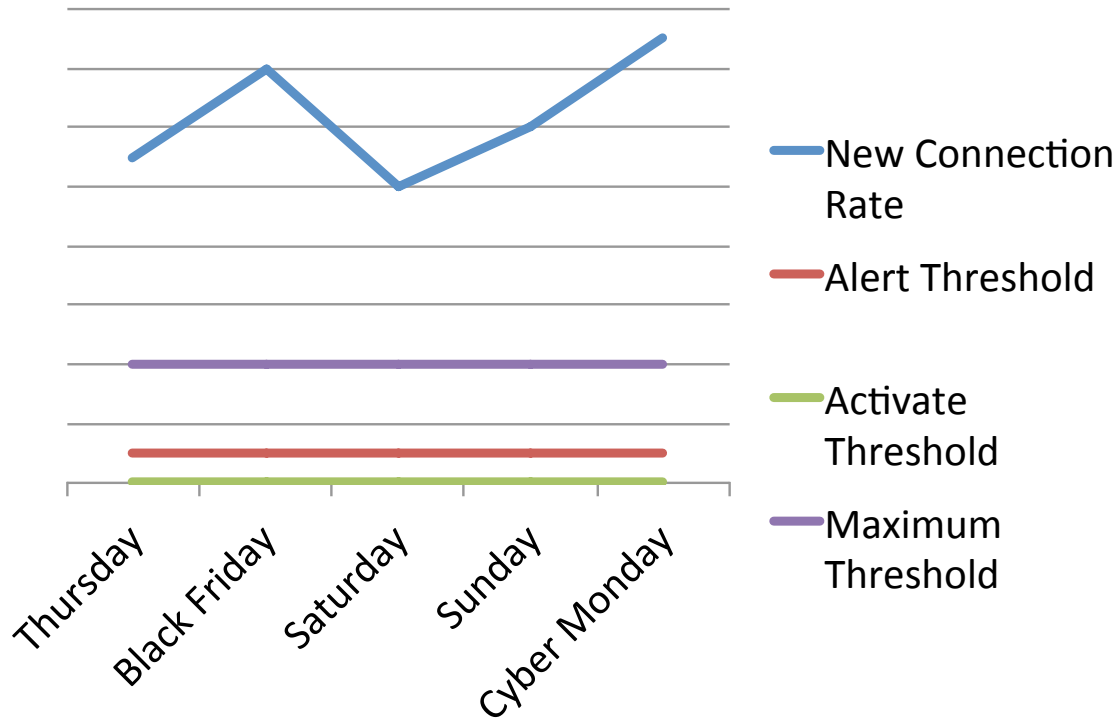


Scenario 2: Protecting your Session Table

BayZon like most online retail companies sees its sales shoot up during the Thanksgiving weekend (or any other holiday weekend). Their website experiences enormous traffic for Black Friday and Cyber Monday deals. Any network downtime or traffic loss during these business-critical holidays will translate into losses of millions of dollars in sales. Due to the heavy traffic seen by the website, the firewall resources may be running with high levels of resource utilization. It may see a lot of new connections coming in and hence high session table utilization. It is imperative to protect the session table from being overrun by any DoS attack during this critical passage of time.

Solution: Conservative Minimum (Activate Threshold = 0)

During business-critical hours of operation where the website sees a lot of traffic, we need to set the Activate threshold to 0. This means that SYN Cookie is activated instantly thereby protecting the session table from brimming over the maximum session capacity of the firewall. Remember it might add a bit of CPU overhead since SYN cookie requires some processing for properly sending an ACK back to the original sender. To further improve the performance, bring down the Maximum threshold from the default of one million pps to an appropriate value above the Activate threshold but less than the maximum session rate supported by the firewall.



Tradeoff

To summarize our discussion above, there exists a tradeoff relationship between performance optimization and session utilization, which is depicted by a spectrum below.

ICMP Floods

ICMP flood protection applies to any type of ICMP packet.

Alert: The number of ICMP packets per seconds entering the ingress zone after which alarms are generated. Alarms can be viewed under threat logs or dashboard. SNMP traps and syslog messages can also be sent.

Activate: The number of ICMP packets per seconds entering the ingress zone after which RED is triggered.

Maximum: The number of ICMP packets per seconds entering the ingress zone after which any new ICMP packets to any host in the zone is dropped. All other non-ICMP traffic to the zone will pass normally.

UDP Floods

Alert: The number of UDP packets per seconds entering the ingress zone after which alarms are generated. Alarms can be viewed under Threat logs or Dashboard. SNMP traps and syslog messages can also be sent.
Activate: The number of UDP packets per seconds entering the ingress zone after which RED is triggered.
Maximum: The number of UDP packets per seconds entering the ingress zone after which any new UDP packets to any host in the zone are dropped. All other non-UDP traffic to the zone will pass normally.

Note:

1. PAN-OS does not log the source and destination IP address in the Threat logs generated during a flood attack. Typically flood attacks come from spoofed IP addresses or even from a DDoS attack. There could be several hundred or thousand source addresses to log.
2. The source and destination zones in the Threat logs will always be the same (the source zone of the attack).
3. It is recommended to use SYN cookie for TCP SYN flood protection.

Packets Per Second vs. Sessions Per Second

The unit of all threshold values under the Flood Protection tab of zone and DoS profiles is packets per second (pps). We mentioned earlier that zone protection applies to packets that do not match an existing session on the firewall. That means that the packets-per-second metric actually stands for new attempted sessions-per-second. For example in the case of SYN floods, 10,000 pps means 10,000 new SYNs per second. The reason we mention this as pps and not cps (connections per second) is because the session has not been created in the session table yet. It is a half connection. A similar concept applies to UDP. UDP floods that have created sessions in the session table will be treated as session-based flows. On the contrary, UDP floods hitting a deny rule will be considered for packet based throttling by the processor. In other words the same rate limit can be packet- or session-based depending on the way the flow is handled in our session table.

Reconnaissance Protection

Reconnaissance protection is used to alert or prevent reconnaissance attempts like port scans and ICMP sweeps. The zone protection profile is always applied to the ingress zone of traffic irrespective of where the servers are located.
Interval: Time between successive probes for open ports. For host sweep it is the time interval between successive probes (ICMP/TCP/UDP) to the network.
Threshold: The number of scanned ports on a destination host within the specified time interval that will trigger reconnaissance protection action.

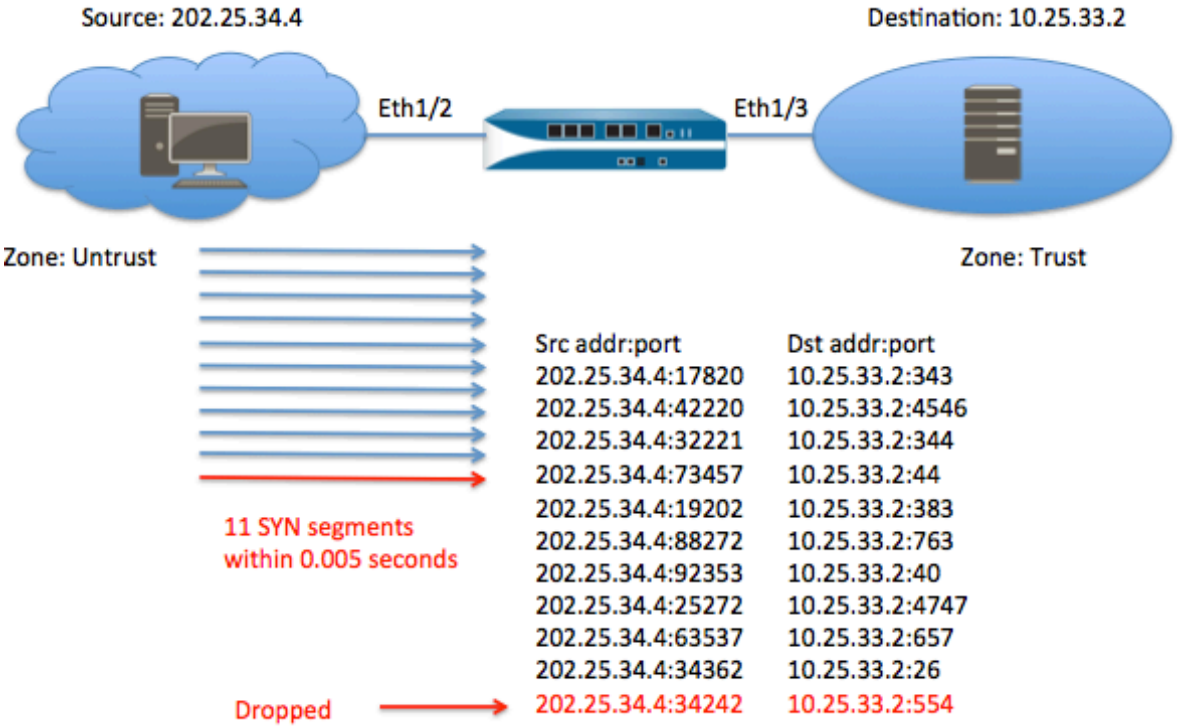
Actions

Allow: Permits the port scan attempts.
Alert: Generates an alert for each scan that matches the threshold within the specified time interval.
Block: Drops all traffic from the source to the destination.
Block IP: Drops all traffic for a specific period of time (in seconds). There are two options:

- Source: Blocks traffic from the source
- Source-and-Destination: Blocks traffic for the source-destination pair

When one source IP address sends IP packets containing TCP SYN segments to a pre-defined number of different ports at the same destination address within a pre-defined interval, it is called a port scan. The purpose of this attack is to scan the available services in the hope that at least one port will respond, thus identifying a service target.

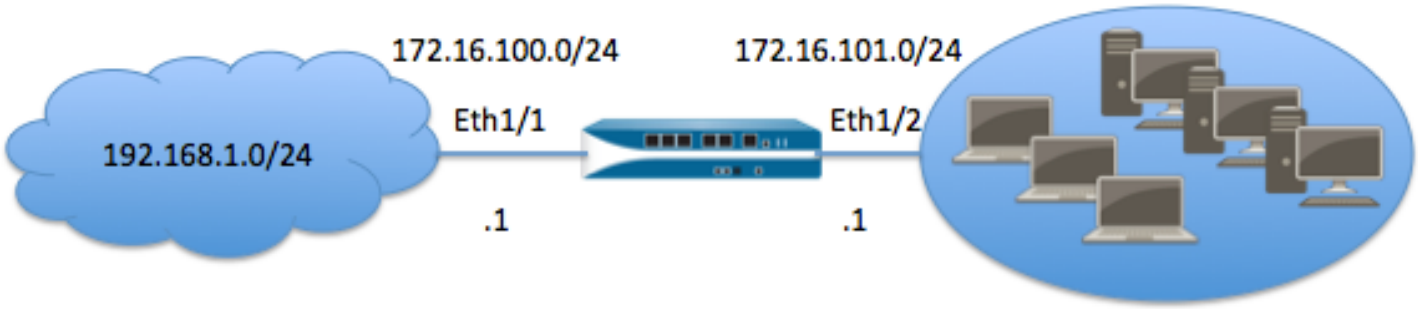
For example if the interval is set to 0.005 seconds and Threshold is set to 10 ports, then after 10 IP packets containing TCP SYN segments to different ports are received at the same destination IP address, PAN-OS creates a Threat log and drops further packets from the source.



Packet Based Attacks

IP Spoof Protection

PAN-OS uses the routing table to verify that the source IP of the traffic is arriving on the appropriate interface. From the example below, if a packet with source IP address 172.16.101.10 arrives at ethernet1/1, but the firewall has a route to 172.16.101.0/24 through ethernet1/2, which is directly connected, IP spoof checking notes that this address arrived at an invalid interface as defined in the routing table. A valid packet from 172.16.101.10 can only arrive via ethernet1/2, not ethernet1/1. Therefore, the device concludes that the packet has a spoofed source IP address and discards it. Similarly packets with source address subnet 192.168.1.0/24 can only arrive from the interface ethernet1/1.



```
admin@PA-4050 > show routing route

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination              nexthop              metric flags      age   interface     next-AS
172.16.100.0/24          172.16.100.1              0 A C              ethernet1/1
172.16.100.1/32          0.0.0.0                   0 A H
172.16.101.0/24          172.16.101.1              0 A C              ethernet1/2
172.16.101.1/32          0.0.0.0                   0 A H
192.168.1.0/24           172.16.100.87            10 A S              ethernet1/1
```

Fragmented Traffic

If the packet size is bigger than the link MTU size the IPv4 router has the capability to fragment the IP packet using the MF (More Flag) field in the IP header. The Fragmented Traffic option discards any packets with MF bit set in the IPv4 header.

Mismatched Overlapping TCP segment

By deliberately constructing connections with overlapping but different data in them, attackers can attempt to cause misinterpretation of the intent of the connection. This can be used to deliberately induce false positives or false negatives. An attacker can use IP spoofing and sequence number prediction to intercept a user's connection and inject his/her own data into the connection. PAN-OS uses this field to discard such frames with mismatched and overlapping data.
The scenarios where the received segment will be discarded are:

1. The segment received is contained within another segment.
2. The segment received overlaps with part of another segment.
3. The segment completely contains another segment.

Reject non-SYN TCP packet

The first packet of every TCP connection has SYN flag set to 1. By setting this option PAN-OS discards any first TCP packet that does not have SYN flag set. This is a zone-based setting. To globally enable or disable non-SYN TCP packets use the CLI.

Asymmetric Path

This particular field provides the ability to either drop packets with out-of-window ACKs and sequence numbers or bypass the scanning of the packets. This is a global setting.

IP Option Drop

The Internet Protocol has provision for optional header fields identified by an option type field. We can use IP options as criteria to drop the unintended packets.

Strict Source Routing	If set, PAN-OS discards packets with IP Option 9 (SSR). This option specifies the complete route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified.
Loose Source Routing	If set, PAN-OS discards packets with IP Option 3 (LSR). This option specifies a partial route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field.
Timestamp	If set, PAN-OS discards packets with IP Option 4 (TS). The timestamps are used for two distinct mechanisms: RTTM (Round Trip Time Measurement) and PAWS (Protect Against Wrapped Sequences).
Record Route	If set, PAN-OS discards packets with IP Option 7 (RR). The Record Route Option provides the means to record the route of an IP datagram.
Security	If set, PAN-OS discards packets with IP Option 2. This option provides a way for hosts to send security, compartmentation, handling restrictions, and TCC (closed user group) parameters.

Stream ID	If set, PAN-OS discards packets with IP Option 8 (SID). This option provides a way for a 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept
Unknown	If set, PAN-OS discards packets if class and option number fields are unknown.
Malformed	If set, PAN-OS discards packets if they have incorrect combinations of class, number and length.

ICMP ping ID 0

PAN-OS uses ICMP identifier and sequence number to create a session. ICMP Ping ID Zero protection will drop packets if either an echo request or echo reply packet is received with identifier as zero.

ICMP Fragment

ICMP provides error reporting and network probe capabilities. ICMP packets contain very short messages; there is no legitimate reason for ICMP packets to be fragmented. PAN-OS drops any IP packet with protocol value =1 (ICMP) and more fragments flag set or that has an offset value indicated in the offset field in the IP header.

Suppress ICMP TTL Expired Error

Every machine that forwards an IP datagram has to decrement the TTL field of the IP header by one; if the TTL reaches 0, an ICMP time-to-live-exceeded-in-transit message is sent to the source of the datagram. Traceroute uses an ICMP echo packet to the named host with a TTL of 1; then with a TTL of 2; then with a TTL of 3 and so on. Traceroute will then get 'TTL expired in transit' message back from routers until the designated host is finally reached and it responds with a standard ICMP 'echo reply' packet. PAN-OS can be set to drop these ICMP packets thereby preventing malicious users discovering the path to a host.

Suppress ICMP NEEDFRAG

A host generates ICMP need-fragment message when it receives a packet with Don't Fragment (DF) bit set to 1 and the path MTU size is too small. ICMP type 3 Code 4 is generated. The sender of the packet upon receiving the ICMP need-fragmentation message lowers the packet size and retransmits the packet. Setting this option will result in the firewall dropping all the ICMP type 3 Code 4 messages traversing through it.

IPv6 Drop

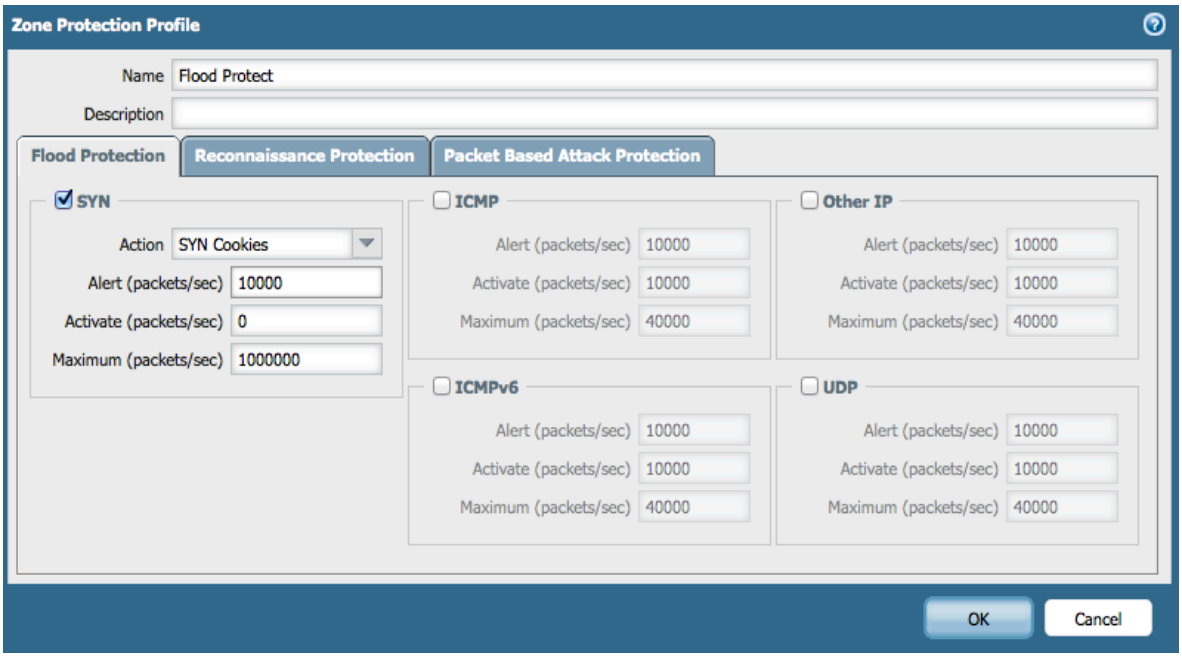
IPv6 drop sub-tab has various options that provide the ability to drop IPv6 packets based on different fields of the IPv6 header like type 0 routing header, anycast source address, hop-by-hop extension, routing extension or if the packet has needless fragmentation, etc.

ICMPv6 Drop

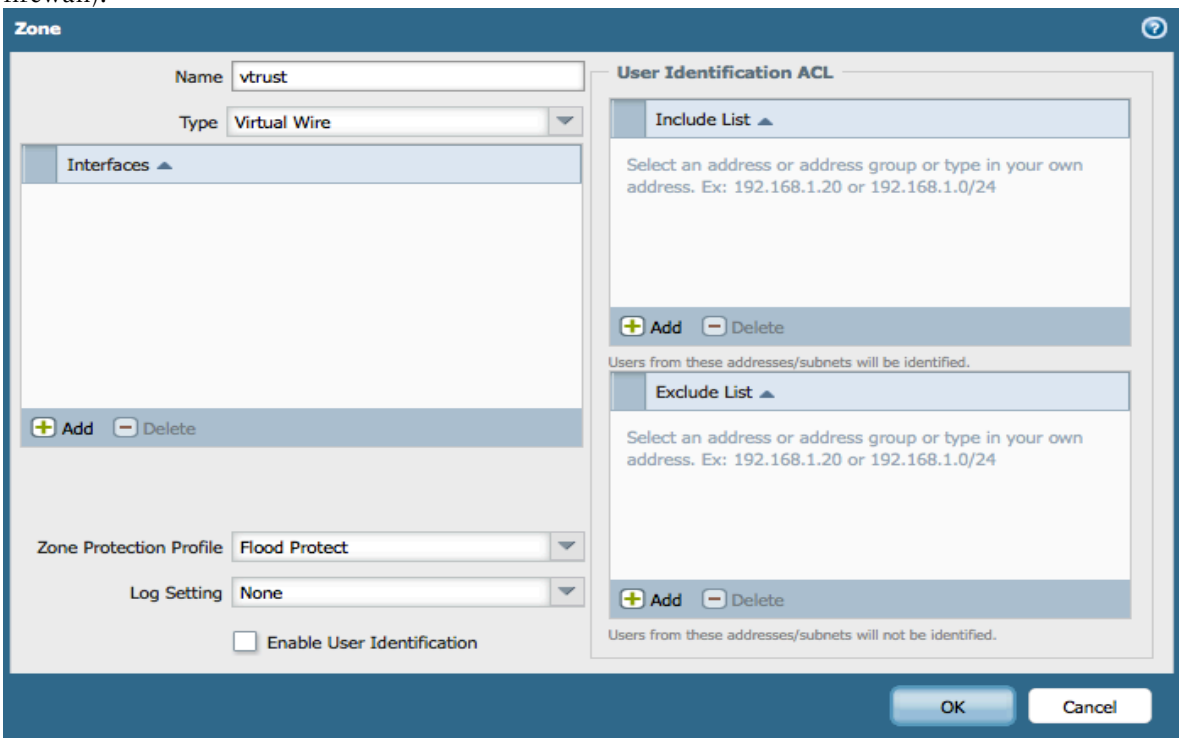
ICMPv6 Drop sub-tab has various options that provide the ability to drop packets based on different error codes of ICMPv6 like destination unreachable, packet-too-big, time exceeded, etc. Each one of these errors requires an explicit security policy match even when they are associated with an existing session.

Configuration and Troubleshooting

Create a zone protection profile using the Network->Network Profiles->Zone Protection tab. Here you can select the type of protection like Flood protection, Reconnaissance or packet-based attack.



After that apply this zone protection profile to a source zone (i.e. the zone from which the traffic is coming in to the firewall).



The zone protection profile can be verified by using the operational mode command
show zone-protection zone <zone_name>

```
admin@PA-5060-2> show zone-protection zone untrust


--------------------------------------------------------------------------------
Zone untrust, vsys vsys1, profile UDP and SYN flood
--------------------------------------------------------------------------------
  tcp-syn               SYN cookies enabled: yes
    alarm rate:   1000pps   activate rate:  10000pps   maximal rate:1000000pps
    current:         0   packets dropped:7382
--------------------------------------------------------------------------------
  udp                   RED enabled: yes
    alarm rate:   1000pps   activate rate:  10000pps   maximal rate:  40000pps
    current:         0   packets dropped:0
--------------------------------------------------------------------------------
  icmp                  RED enabled: no
--------------------------------------------------------------------------------
  other-ip              RED enabled: no
--------------------------------------------------------------------------------
  icmpv6                RED enabled: no
--------------------------------------------------------------------------------
packet filter:
  discard-ip-spoof:                enabled: no

************output truncated**********************
```

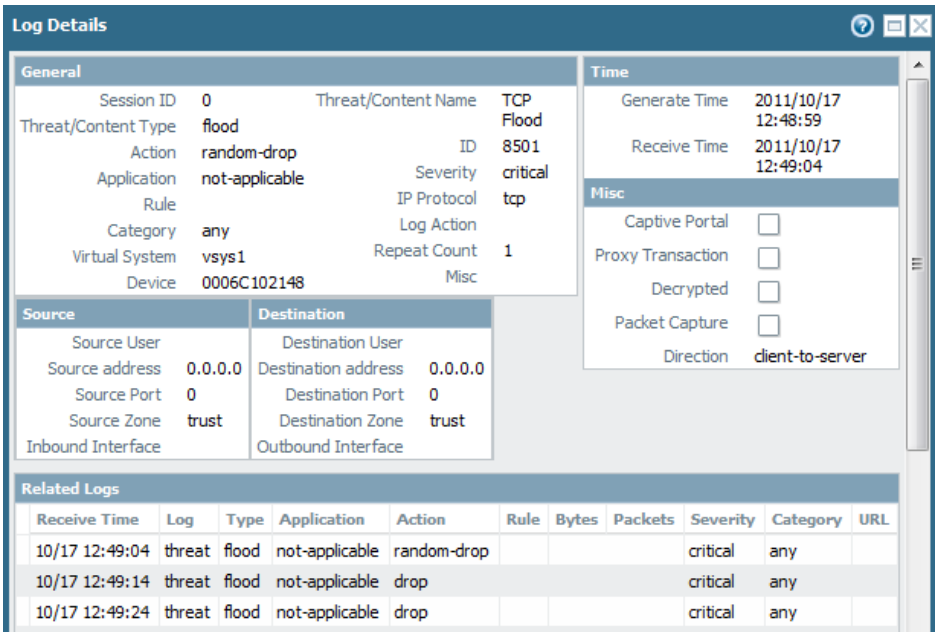
Note: To view zone protection for a VSYS other than the default VSYS, you must set the VSYS context using the command **set system setting target-vsys <name>,** before using the **show zone-protection zone <name>** command.

The zone protection profile logs are stored under Threat logs category. Some of the sample logs when SYN flood protection is enabled are shown below.

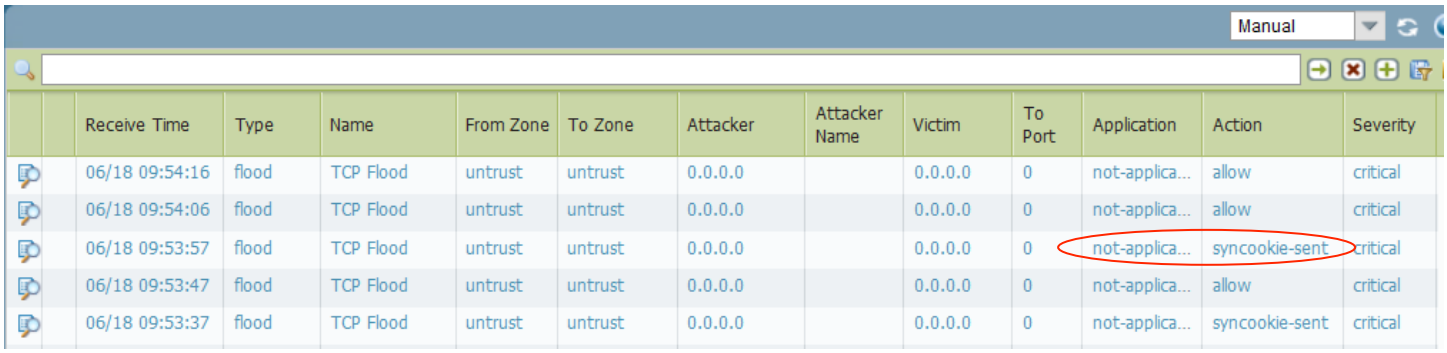
Note: For flood attacks (SYN, UDP, ICMP), the Threat log will show 0.0.0.0 for attacker and victim as there is typically more than one IP address that is the source and destination of the attack.

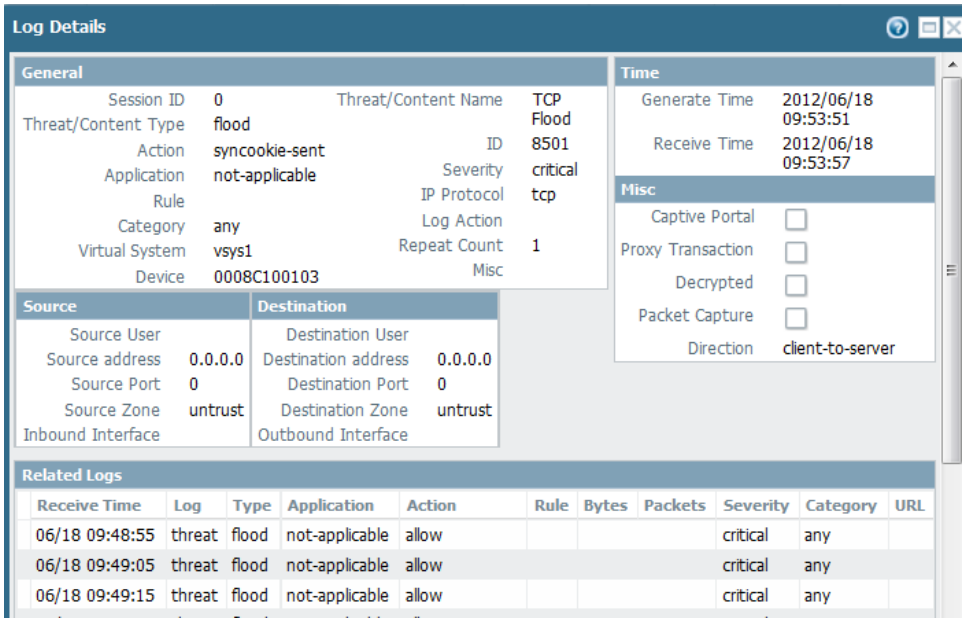
Logs with Random Early Drop

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
10/17 12:50:14	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:50:04	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:54	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:44	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:34	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:24	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:14	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical
10/17 12:49:04	flood	TCP Flood	trust	trust	0.0.0.0		0.0.0.0	0	not-applicable	random-drop	critical



Logs with SYN cookie





The global counters with aspect “dos” will show if any counters are triggered by DoS traffic. An Example of the command is shown below

```
admin@PA-5060-2> show counter global filter delta yes aspect dos

Global counters:
Elapsed time since last sampling: 229.83  seconds

name                                    value     rate severity  category  aspect    description
------------------------------------------------------------------------------------
flow_dos_syncookie_cookie_sent          24308      106 info      flow      dos       TCP SYN
cookies: cookies sent, aggregate profile
/zone
------------------------------------------------------------------------------------
Total counters shown: 1
------------------------------------------------------------------------------------
```

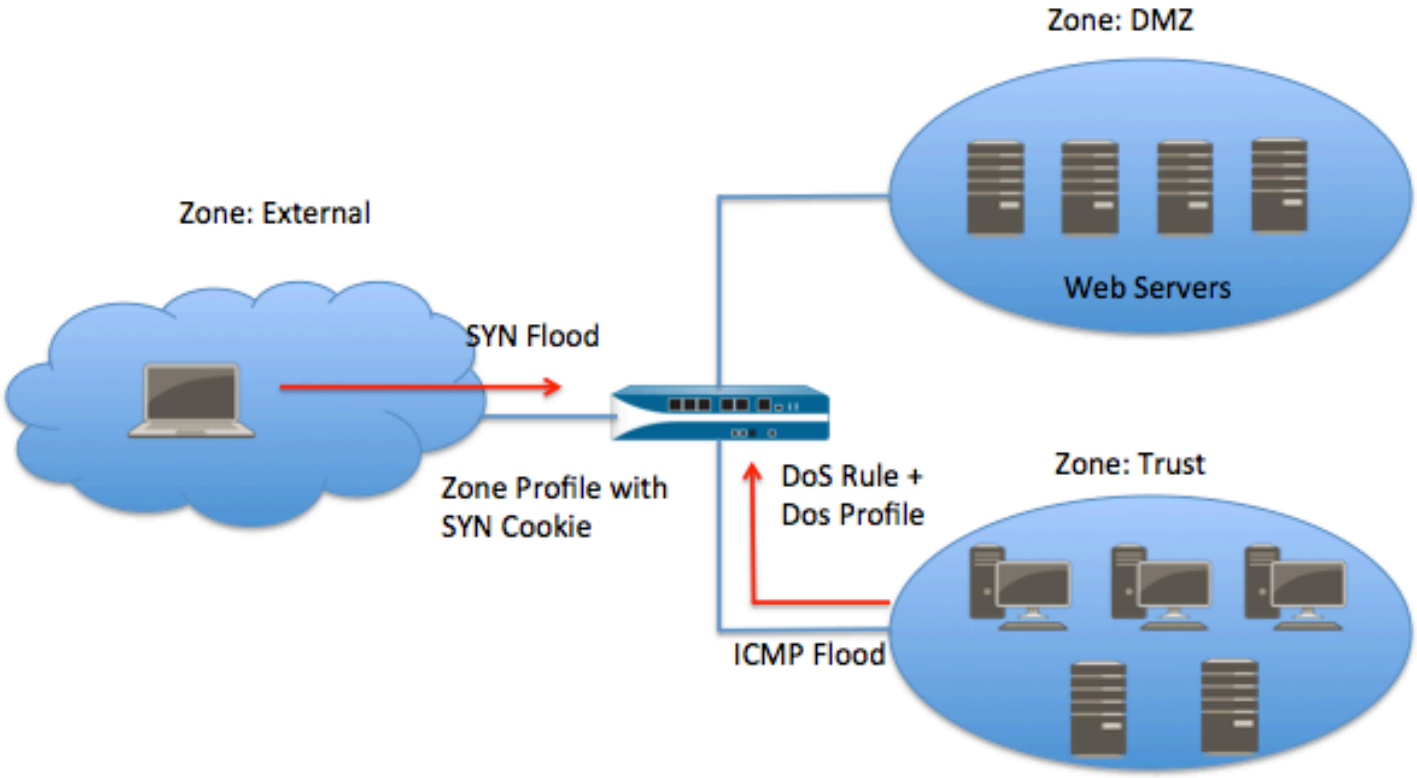
When a zone protection profile includes port scans or when block-ip is enabled (for example within vulnerability profiles for threat-exception for certain threat IDs with action as block-ip), the list of IPs that are currently blocked can be viewed with: **show dos-protection zone <name> blocked source**

End Point Protection (DoS Profile and Rule base)

The DoS protection rule base allows firewall administrators to configure granular policies for DoS mitigation. DoS protection policies can be configured to match zone, interface, IP address or user information as match conditions for mitigating DoS attacks. zone protection profiles are designed to provide broad-based protection at the ingress zone and are not designed to protect a specific end host or traffic going to a particular destination zone. DoS protection profiles are designed for high precision targeting and augment zone protection profiles by allowing to create DoS rules similar to Security policies that allow traffic to and from certain zones, to and from certain addresses or address groups, or from certain users and for certain services to be analyzed for DoS attacks.

Scenario:

In this scenario an enterprise needs to protect its web servers in a certain subnet from DoS attacks that can originate externally as well as internally.



Remember that zone protection is only applied to the source zone and that will not protect the servers from an internal attack in this particular scenario. The best practice here would be to have a DoS policy with a DoS profile action of Protect for the destination subnet under consideration. It is recommended to still have the zone protection profile applied on the external facing zone to have comprehensive DoS protection.

A good protection configuration would incorporate protection from both zone protection profiles and DoS protection rule base, with DoS protection rules used when identity of the end host is known for example which servers to protect or which pairs of source-destination zones need a more aggressive flood rate limit. Both aggregate and classified profiles could be applied to a DoS rule with Aggregate profile rate limits being generally greater than classified rate limits.

DoS Protection Rules

A DoS rule provides multiple keys or criteria to apply DoS protection in a granular and flexible fashion. It also provides a way to have different criteria than the ones used in a security rule to be applied for a DoS profile. However there is an additional lookup involved in the process. DoS rules are applied before security policy lookup (slow-path), but after destination zone determination.

DoS Rule Match Criteria

1. Source zone or source interface
2. Destination zone or destination interface
3. Source IP, ranges, address objects, address groups and countries
4. Destination IP, ranges, address objects, address groups and countries
5. Service (Port and Protocol)
6. Users

DoS Rule Actions

Deny: Block all traffic hitting this rule. No protection thresholds are enforced.

Protect: Enforce protection subject to thresholds in the protection profile.

Allow: Allow all traffic hitting this rule. No protection thresholds are enforced.

DoS Protection Profiles

A DoS Protection profile can be attached to a DoS policy rule When a DoS rule is matched, the parameters of the DoS profile are enforced on the traffic. A DoS protection profile can be attached as an aggregate or a classified profile in a DoS rule.

Aggregate Profiles

Aggregation implies that the attacks selected in the Aggregate DoS protection profile apply to all the traffic hitting the DoS rule from all src/dst IPs, users and services allowed for that rule. In this sense it is similar or can be considered as a subset of the zone protection profile. If flood rate limits need to be applied to general overall traffic, this might be a good place to start. For example a SYN flood threshold of 10,000 pps would count all packets coming from any source IP and going to any destination IP.

Classified Profiles

This method explains the categorization or grouping of hosts that are protected. Different session rate limits can then be enforced for different classes of end hosts. The groupings can be done on the basis of one of following criteria:

1. Source IP address
   - A typical use case is when you don't want any host on your network to start a DoS attack. This is achieved by monitoring the rate of traffic initiated by each of the hosts in a source address group. Each host is tracked is tracked individually for rate limiting.
2. Destination IP address
   - A typical use case is to protect web or DNS servers on your network. Each destination server is monitored individually for incoming traffic to prevent it from going above the configured rate limits for any number of source IPs.
3. Combination of source and destination IP addresses
   - As the name suggests, it tracks the traffic flow between a given source-destination IP pair for the configured rate limits.

Note: If both aggregate and classified profiles are attached to a DoS rule then the aggregate rate limits are checked and enforced before the classified rate limits.

DoS Profile Types

The DoS protection profiles can be used to mitigate following types of DoS attacks.

Flood (Behavior-based) Protection

This section is very similar to the one in zone protection. For SYN Floods we have SYN Cookie and RED as the available methods. For UDP, ICMP, ICMPv6 and other IP floods, RED is the method of choice. We have similar threshold levels as in zone protection (i.e. Alert, Activate and Maximum). In addition to these parameters we have block duration.

Block Duration - Time in seconds the offending IP will be denied.

Note: Packets arriving during the block duration are not accounted towards triggering the next alert, activate or maximum threshold.

Resource Based Protection

This type of protection enforces a quota for the group of hosts. In other words, it restricts the maximum number of sessions allowed for a particular source IP, destination IP or a source-destination pair.

Note: The max concurrent session limit includes both ACTIVE and DISCARD session types as it tracks any session that takes up resource.

Shared Option – We can share a profile between various VSYS thereby avoiding duplication of effort in a multiple VSYS environment.

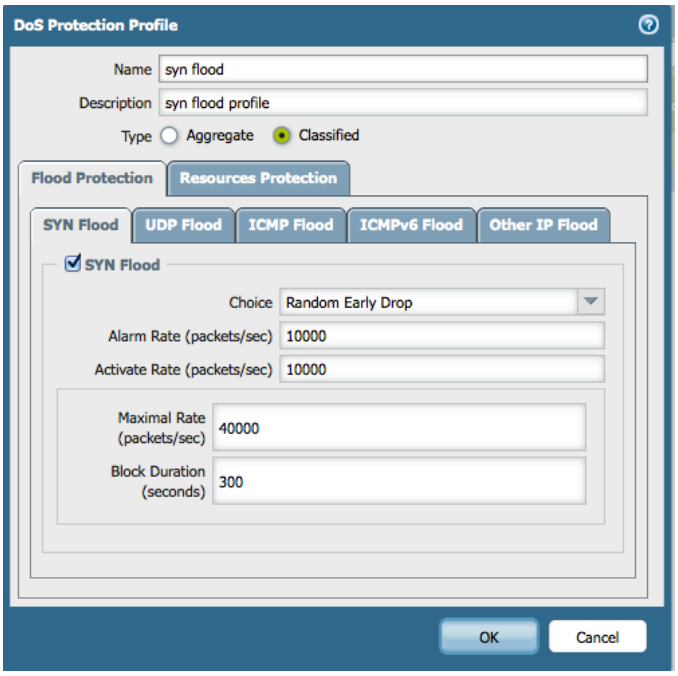
Protection Precedence and Limitations

1. Zone protection will be enforced before DoS policy lookup if an IP happens to be present in both the profiles.

2. The DoS rule base and profiles are per VSYS and can be used on a shared gateway.
3. The DoS rule base does not have reconnaissance protection such as port scans and host sweeps. It also doesn't have packet-based attack protection.
4. Management traffic is exempted from DoS rule base and profiles.
5. Zone protection profiles enforcement and DoS rule base lookups are performed in software (that is in the security processor). They are not performed in the network processor.
   - Incoming packets are subjected to basic session match by formulating the 6 tuple. Based on the 6-tuple match they are scheduled for session setup on one of the cores of the DP. In this stage, zone protection, DoS protection and security policy lookup are performed and in that order.
6. Some firewall models can preemptively drop packets that violate certain rules in the network processor. These should not be confused with the zone protection or DoS profile because they cannot be disabled at this time. A few examples of these rules are bad source address (loopback, multicast, etc.), IP checksum error, and bad IP header.

Configuration and Troubleshooting

Create a DoS protection profile under Objects->Security Profiles->DoS Protection tab. Here you can create profiles of either type 'Aggregate' or 'Classified' and specify rate and resource limits similar to zone protection profiles.

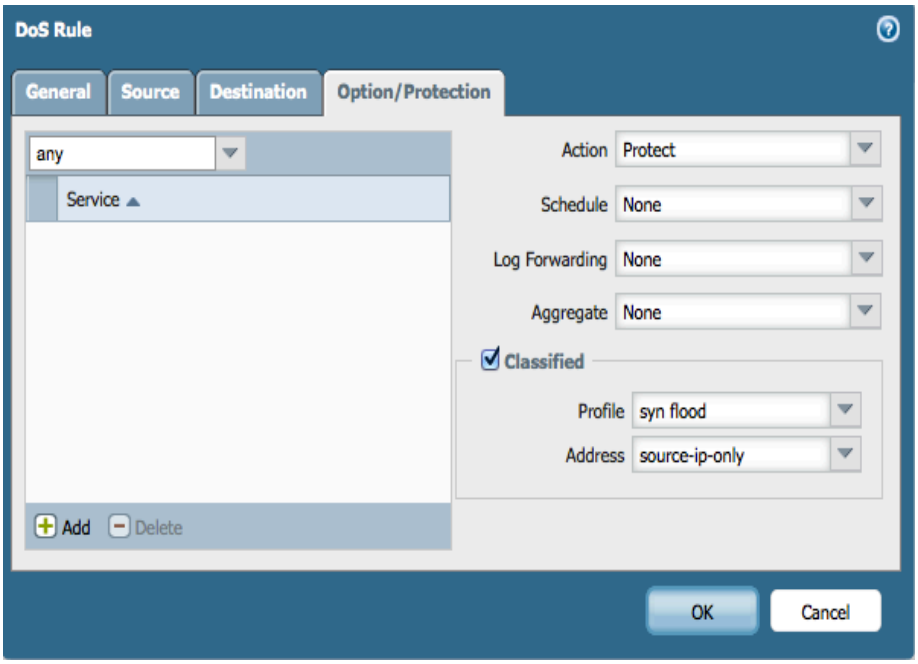


Create a DoS rule similar to security rule. Most parameters are similar to security rules in terms of zones and addresses and are used in a similar manner. Attach an aggregate profile or a classified profile or both to the rule. The 'action' keyword in the rule means the following:

Deny: All traffic hitting this DoS rule is denied.

Allow: All traffic hitting this DoS rule allowed.

Protect: All traffic hitting this DoS rule is checked for rate limits specified by the Aggregate and Classified profiles.



To look for information regarding aggregate and classified protections enabled on a DoS rule, run:
show dos-protection rule <name> settings | statistics

To look for more details like which IPs are being protected, whether they are blocked for some time or how many sessions they are currently associated with, etc. regarding classified profiles, run:
debug dataplane show dos classification-table to view the entire internal classification table
debug dataplane show dos rule <name> classification-table to view information for traffic that hit a given DoS rule

To see globally what's happening with DoS or zone protection, for example to see if max rate was hit for any of the rules, run:
show global counters | match dos

Summary

Palo Alto Networks DoS protection features provide protection against a wide variety of DoS attacks that are observed in the current threat landscape. They empower the security administrators with tools to configure DoS protection against varying attack sizes and provide flexibility to pick and choose particular end points to enforce targeted DoS mitigation. The choices of resources that need to be protected influence the values of the different threshold knobs provided to the end user.

Revision History

Date	Revision	Comment
May 8, 2013		First released of the document