Table of Contents

DoS and Zone Protection Best Practices................................................................. 5
  Plan DoS and Zone Protection Best Practice Deployment........................................ 7
  Deploy DoS and Zone Protection Using Best Practices.......................................... 9
  Follow Post Deployment DoS and Zone Protection Best Practices....................... 13
DoS and Zone Protection Best Practices

This document is a streamlined checklist of pre-deployment, deployment, and post-deployment best practices you can follow to implement DoS and Zone Protection, including links to detailed configuration information in the PAN-OS 8.1 Admin Guide.

A Denial-of-Service (DoS) attack attempts to make a network device or resource unavailable to legitimate users by disrupting services. These attacks usually come from the internet but can come from misconfigured or compromised internal devices. The typical method is to flood the target with resource requests until the requests consume all of the target's available resources—memory, CPU cycles, and bandwidth—and the target becomes unavailable. Typical targets are internet-facing devices users can access from outside the corporate network, such as web servers and database servers. As part of a layered approach to DoS protection, Palo Alto Networks firewalls provide three DoS attack mitigation tools.

Zone Protection Profiles—Apply only to new sessions in ingress zones and provide broad protection against flood attacks by limiting the connections-per-second (CPS) to the firewall, plus protection against reconnaissance (port scans and host sweeps), packet-based attacks, and layer 2 protocol-based attacks.

Dos Protection Profiles and Policy Rules—Provide granular protection of specific, critical devices for new sessions. Classified policies protect individual devices by limiting the CPS for a specific device or specific devices. Aggregate policies limit the total CPS for a group of devices but don’t limit the CPS for a particular device in the group to less than the total allowed for the group, so one device may still receive the majority of the connection requests.

Packet Buffer Protection—Protects against single-session DoS attacks from existing sessions that attempt to overwhelm the firewall’s packet buffer.

- Plan DoS and Zone Protection Best Practice Deployment
- Deploy DoS and Zone Protection Using Best Practices
- Follow Post Deployment DoS and Zone Protection Best Practices
Plan DoS and Zone Protection Best Practice Deployment

Take different types of DoS attacks into account. Plan to layer your defenses with multiple prevention mechanisms and position firewalls close to the devices they protect. Understand the average normal and peak baseline connections-per-second (CPS) of the critical devices you want to protect, the capacity of your firewalls, and the effect of other features that affect firewall capacity, such as how much traffic you decrypt.

STEP 1 | Plan your defense against each type of DoS attack.

- **Application-Based Attacks**—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can’t use it. An example is the Slowloris attack.
- **Protocol-Based Attacks**—Also known as state-exhaustion attacks, they target protocol weaknesses. A common example is a SYN flood attack.
- **Volumetric Attacks**—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing its resources. An example is a UDP flood attack.

STEP 2 | Use a layered approach to preventing DoS attacks.

- Use a dedicated, high-volume DDoS protection device and a perimeter router, switch, or other hardware-based packet drop device with appropriate access control lists (ACLs) as the first layer of defense at the internet-facing network perimeter, in front of perimeter firewalls. Perimeter protection defends against volumetric attacks that the session-based firewall isn’t designed to handle.
- Use the firewall as an extra layer of defense against DoS attacks to protect individual zones (Zone Protection profile and Packet Buffer Protection) and individual or small groups of high-value targets such as web servers (DoS Protection profiles and policy rules). The firewall provides visibility into application traffic that dedicated DoS protection devices don’t provide. Firewall use cases include:
  - Applying Zone Protection profiles as a second layer of broad protection.
  - Applying Aggregate DoS Protection profiles as a third layer of broad protection for groups of critical servers.
  - Applying Classified DoS Protection profiles to protect critical internet-facing servers by limiting the CPS to each server.
  - Applying Classified DoS Protection profiles to prevent misconfigured or compromised internal hosts from carrying out a DoS attack by limiting the CPS either from the suspect source (internally-facing zones only, not internet-facing zones) or to the affected destination.
  - Applying Classified DoS Protection profiles to monitor a particular source (internally-facing zones only) and alert you if the CPS from that source reaches a certain threshold, which may indicate a compromised or misconfigured host.
  - Applying Packet Buffer Protection to prevent DoS attacks from consuming firewall resources.

STEP 3 | Position firewalls as close as possible to the resources they protect.

The firewall treats packets as sessions and inspects each packet at the port, protocol, IP, and application level. Firewalls don’t scale to millions of CPS because they are session-based, so the closer you place the firewall to the resources you’re protecting, the fewer sessions and firewall resources consumed.

- Do not place firewalls in front of perimeter DDoS devices or perimeter routers or switches. Use high-capacity devices at the edge (both local and cloud edge) to mitigate volumetric attacks from the internet and prevent the firewall from being exposed to those attacks.
Position perimeter firewalls *behind* dedicated DDoS devices and routers or switches that drop DoS traffic using ACLs so the firewalls segment the internal network into zones and protect sensitive devices in those zones. The closer a firewall is to the perimeter, the greater its capacity should be because of higher traffic volumes.

Consider examining network zone segmentation. If it isn’t granular enough, consider creating smaller zones. Smaller zones increase security in many ways, including better prevention of lateral movement of malware, increased visibility into traffic, and reducing the potential scope of internal DoS attacks.

**STEP 4** | Take baseline measurements of the average and peak CPS of the devices and zones you want to protect, and understand the capacity of your firewalls so flood thresholds don’t inadvertently throttle traffic or allow DoS attacks.

- Take baseline measurements of average and peak CPS for critical devices (potential targets).
  - Take baseline CPS measurements for critical internet-facing devices over at least one business week, during business hours. The longer the data collection time span, the more accurate the measurements.
  - Work with application teams to understand the normal and peak CPS to their servers and the maximum CPS those servers can support.
  - Filter firewall Traffic and Threat logs for the destination IP addresses of critical devices to baseline normal and peak session activity.
  - Take into account special events, quarterly events, and annual events that may increase traffic, change traffic patterns, or use applications that aren’t usually on the network.
- Understand the capacity of your firewalls and the resources (CPU and memory) other features consume so you know the capacity available for DoS Protection.
  - Take baseline CPS measurements for each firewall zone over at least one business week, during business hours. The longer the data collection time span, the more accurate the measurements. Measure normal and peak CPS for each individual zone so you can set Zone Protection flood thresholds tailored to each zone’s CPS load.
  - If you use Panorama to manage your firewalls, use Device Monitoring to measure CPS values. Device monitoring can also show you a 90-day trend line of CPU average and peak usage to help you understand the typical available capacity of each firewall.
    
    If you can’t use Panorama’s Device Monitoring, you can use your management tools to poll the following three MIBs to gather historical CPS data: PanZoneActiveTcpCps, PanZoneActiveUdpCps, and PanZoneOtherIpCps.
  - Use third-party tools such as Wireshark or NetFlow to collect and analyze network traffic.
  - Consider using scripts to automate CPS information collection and continuous monitoring, and to mine information from the logs.
Deploy DoS and Zone Protection Using Best Practices

DoS and Zone Protection help defend individual critical servers (DoS Protection) and zones (Zone Protection) against application-based and protocol-based flood attacks, and provide the next layer of defense against volumetric attacks after your dedicated DDoS prevention device at the internet perimeter.

**STEP 1** | Create and apply a **Zone Protection profile** to defend each zone.

Zone Protection profiles apply to new sessions in ingress zones and protect against flood attacks, reconnaissance (port scans and host sweeps), packet-based attacks, and layer 2 protocol-based attacks.

- Set **Alarm Rate**, **Activate**, and **Maximum** thresholds to prevent SYN, UDP, ICMP, ICMPv6, and Other IP new session floods from taking down the firewall, and set the **Action** for SYN floods.

  - **Measure CPU consumption** to ensure the firewall can support DoS and Zone Protection and other features that consume CPU cycles, such as decryption.

- **Action** (SYN flood only)—Start with SYN Cookies, which treats legitimate traffic fairly but consumes more resources, as the drop mechanism for the **Activate** and **Maximum** thresholds. Monitor firewall CPU and memory utilization. If SYN Cookies consumes too many resources, switch to Random Early Drop (RED), which randomly drops connections. If you don’t have a dedicated DDoS prevention device in front of the firewall, always use RED.

- **Alarm Rate**—Set 15-20% above the average zone CPS rate to accommodate normal fluctuations.

- **Activate**—Set just above the zone’s peak CPS rate to begin dropping connections to mitigate floods.

- **Maximum**—Set to 80-90% of firewall capacity. Account for other resource-consuming features. Crossing this threshold blocks new connections until the CPS rate falls below the threshold.

  Alternatively, when you understand the maximum CPS you can support, start by setting the **Maximum** CPS rate to 80-90% of firewall capacity and derive reasonable **Activate** and **Alarm Rate** thresholds based on the **Maximum** threshold.

  **Firewalls with multiple dataplane processors (DPs) distribute connections across DPs. In general, the firewall divides the CPS threshold settings equally across its DPs. For example, if a firewall has five DPs and you set the Alarm Rate to 20,000 CPS, then each DP has an Alarm Rate of 4,000 CPS (20,000 / 5 = 4,000), so if the new CPS on a DP exceeds 4,000, it triggers the Alarm Rate threshold for that DP.**

- Monitor and adjust the thresholds as needed.

- Enable **Reconnaissance Protection** on all zones to block host sweeps and TCP and UDP port scans. Keep the default event **Threshold** to log a few packets for analysis before blocking the reconnaissance operation. Use **Source Address Exclusion** to whitelist internal groups that test for network vulnerabilities.

- Drop suspicious packets to prevent **packet based attacks**.

  - **IP Drop**—Drop **Unknown** and **Malformed** packets. Drop **Strict Source Routing** and **Loose Source Routing** packets because source routing allows adversaries to bypass Security policy rules that use the destination IP address as the matching criteria. For internal zones only, drop **Spoofed IP address** packets to ensure that on ingress, the source address matches the firewall routing table.

  - **TCP Drop**—Retain the default drops, drop **Mismatched overlapping TCP segment** and **Split Handshake** packets, and enable the strip option **TCP Timestamp**.
If you configure Tunnel Content Inspection on a zone and enable Rematch Sessions, for that zone only, disable Reject Non-SYN TCP so that enabling or editing a Tunnel Content Inspection policy doesn’t cause the firewall to drop existing tunnel sessions.

- **ICMP Drop**—What to block depends on how (if) you use ICMP.
- **IPv6 Drop**—If compliance matters, drop packets with non-compliant routing headers, extensions, etc.
- **ICMPv6 Drop**—If compliance matters, drop certain packets that don’t match a Security policy rule.

Enable Protocol Protection to deny protocols you don’t use on your network and prevent layer 2 protocol-based attacks on layer 2 and vWIRE interfaces.

- Use the Include List to whitelist the layer 2 protocols you use and deny all other protocols (the Exclude List is a blacklist that allows all protocols not on the list). If you don’t configure Protocol Protection, all layer 2 protocols are allowed.

Attach a profile to each zone (Network > Zones) in the Zone Protection Profile field.

**STEP 2** | Apply DoS Protection to specific, critical network resources, especially systems users access from the internet that are often attack targets, such as web and database servers.

A DoS attack that targets an individual system can succeed if the aggregate CPS rate doesn’t exceed the Zone Protection profile’s thresholds, so you also need DoS protection. DoS Protection profiles set flood thresholds and DoS Protection policy rules define the devices, users, zones, and services to which DoS Profiles apply. Because DoS Protection is resource-intensive, use it only for critical systems. Configure classified and aggregate DoS Protection profiles and apply one or both to a DoS Protection policy rule (each policy rule can have one of each profile type). Classified profiles set thresholds that apply to each individual device specified in a rule. Aggregate profiles set thresholds that apply to the combined group of devices specified in a rule.

- Create a DoS Protection profile for each critical device or set of critical devices you want to protect. Set SYN, UDP, ICMP, ICMPv6, and Other IP flood thresholds and the Action for SYN floods. Default threshold values often aren’t appropriate because each network is different—base thresholds on the capacity of the device(s) you’re protecting.

  - **Action** (SYN flood only)—Set the SYN Cookies or RED drop mechanism for Activate and Max Rate thresholds. Start with SYN Cookies, which treats legitimate traffic fairly but consumes more resources. Monitor CPU and memory utilization. If SYN Cookies consumes too many resources, switch to RED. Always use RED if you don’t have a dedicated DDoS prevention device in front of the firewall.

  - **Alarm Rate**—For classified profiles, set 15-20% above the device’s average CPS rate to account for normal fluctuations. For aggregate profiles, set 15-20% above the group’s average CPS rate.

  - **Activate Rate**—Classified profiles apply exact CPS limits to individual devices and you base those limits on the capacity of the devices, so you don’t need to throttle CPS gradually and can set the Activate Rate to the same threshold as the Max Rate. Set the Activate Rate lower than the Max Rate only if you want to begin dropping traffic before it reaches the Max Rate. For aggregate profiles, set the threshold just above the peak CPS rate for the group.

  - **Max Rate**—For classified profiles, base the Max Rate on the capacity of the device(s) you’re protecting so they can’t be flooded. For aggregate profiles, set to 80-90% of the group’s capacity. When CPS reaches the threshold, the firewall drops new connections for the Block Duration.

  - **Block Duration**—For all profiles, use the default value (300 seconds) to block the attacking session without penalizing legitimate sessions from the same source for too long a time period.

Measure firewall CPU consumption to ensure that the firewall can support DoS and Zone Protection and other features that consume CPU cycles, such as decryption.
Monitor and adjust the thresholds as needed.

Create **DoS Protection policy rules.** Make each rule as specific as possible to protect critical devices while preserving firewall CPU and memory resources. Attach DoS Protection profiles and set:

- **Service**—Specify the services (ports) in use on the server(s) you're protecting. If you're protecting web servers, specify HTTP, HTTPS, and other appropriate service ports for the web applications.

  *Use separate DoS Protection policy rules for critical servers’ unused service ports.*

- **Action**—Select **Protect** to apply the rule's DoS Protection profile(s) to the specified devices.
- **Log Forwarding**—For easier management, forward DoS logs separately from other Threat logs directly to administrators via email and to a log server.
- **Aggregate**—Use aggregate profiles to protect critical server groups.
- **Classified > Profile**—Use classified profiles to protect individual or small groups of critical servers.
- **Classified > Address**—Counters consume firewall resources. For classified DoS Protection profiles, specify whether connections count toward profile thresholds based on matching the **source-IP-only**, the **destination-IP-only**, or both (**src-dest-ip-both**). Your DoS protection goals, what you are protecting, and whether the protected devices are in internet-facing zones determine how to configure the threshold counter.

  Don’t use **src-ip-only** or **src-dest-ip-both** for internet-facing zones because the firewall can’t store counters for all possible internet IP addresses. Use **destination-IP-only** in perimeter zones.

  Use **destination-IP-only** to protect individual critical devices.

  Use **source-IP-only** and the **Alarm** threshold to monitor suspect hosts (non-internet-facing zones).

  The firewall consumes more resources to track **src-dest-ip-both** counters than to track only the source IP or destination IP counters.

**STEP 3** | Apply **Packet Buffer Protection** to each zone to protect the firewall buffers from single-session DoS attacks.

- Use baseline measurements of packet buffer utilization to understand the firewall’s capacity and ensure that the firewall is properly sized so that only an attack causes a large spike in buffer usage.
- Set global Packet Buffer Protection thresholds:
  - **Alert** and **Activate**—Use the default value (50%), monitor packet buffer utilization, and adjust the thresholds if necessary.
  - **Block Hold Time**—Use the default value (60 seconds) for the amount of time the offending session can continue before the firewall blocks it. Monitor packet buffer utilization and adjust the time if necessary.
  - **Block Duration**—Use the default value (3600 seconds) for the amount of time after the **Block Hold Time** expires to block every session from the offending IP address, or reduce the value if blocking an IP address for one hour is too great a penalty for your business conditions. Monitor packet buffer utilization and adjust the value if necessary.

  *Network Address Translation (NAT) can increase packet buffer utilization because of IP address translation activity. If this affects the utilization thresholds, reduce Block Hold Time to block individual sessions faster and reduce Block Duration so other sessions from the underlying IP address aren’t unduly penalized.*

**STEP 4** | Attach the **best practice Vulnerability Protection profile** to all Security policy allow rules.

The combination of dedicated, high-volume DDoS protection at the perimeter, Zone Protection profiles, DoS Protection profiles and policy rules, Packet Buffer Protection, and Vulnerability Protection...
for allowed traffic provides multiple layers of DoS protection for your network and its most critical resources.
Follow Post Deployment DoS and Zone Protection Best Practices

After you deploy zone and DoS protection, ensure that everything is working as expected and take steps to ensure that it keeps working as expected as you network evolves.

STEP 1 | Measure firewall performance to ensure it’s within acceptable norms and so you understand the effect of zone and DoS protection on firewall resources.

If the levels of zone and DoS protection (combined with other resource-consuming features such as decryption) consume too many firewall resources, the best practice is to scale up the resources rather than to compromise security.

STEP 2 | Configure log forwarding.

For easier management, use separate log forwarding profiles to forward DoS and zone threshold event logs separately from other Threat logs. Send DoS and zone logs directly to the relevant administrators via email and also to a log server, so notifications contain only events that are potential DoS attacks. Configure DoS event log forwarding on the DoS Protection policy rule (Policies > DoS Protection) and configure Zone event log forwarding on each zone (Network > Zones).

Set Alarm Rate threshold event log messages to low or informational severity. Set DoS protection Activate and Maximum and zone protection Activate Rate and Max Rate threshold event log messages to critical severity. After you set the flood thresholds properly, the logs show you the potential flood attacks on the network because you only see threats and anomalous events. If you see too many false alerts, the thresholds are set too low or the firewall isn’t properly sized for the traffic it handles.

The firewall takes cumulative logs every 10 seconds to keep log volume manageable, avoid overwhelming log servers, and preserve firewall resources.

STEP 3 | Watch for and investigate other indicators of DoS attacks.

In addition to configuring log forwarding so administrators receive notifications when flood thresholds are crossed, check attack indicators and investigate potential DoS attacks:

- Review DoS threat activity (ACC > Threat Activity) and look for patterns of abuse.
- On firewall models that support it (PA-3050, PA-3060, PA-3200 Series, PA-5000 Series, PA-5200 Series, and PA-7000 Series), monitor blocked IP addresses (Monitor > Block IP List) for IP addresses the firewall blocked because of a potential DoS attack. The Block Source column identifies the name of the classified DoS Protection profile that blocked the IP address.
- A partial or complete traffic outage on the firewall, slow web browsing or endpoint connectivity, or new sessions failing may indicate a DoS attack. High CPU utilization, packet buffer and descriptor depletion, and a spike in the number of active sessions can also indicate a DoS attack.
- Learn more about Zone and DoS Protection Event Logs and Global Counters to monitor DoS activity.

Flood threshold breaches may indicate a DoS attack, but they may also indicate misconfigured CPS values or incorrect firewall sizing.

STEP 4 | Network traffic patterns change over time, new devices are added to the network and old device are removed, and special events can temporarily affect traffic patterns.

For these reasons, periodically take new CPS measurements and revisit the zone and DoS flood threshold settings—because networks constantly evolve, DoS and zone protection require an iterative approach.