paloalto TECHDOCS

DoS 和区域保护最佳实践

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 6, 2023

Table of Contents

DoS 和区域保护最佳实践

这份包含部署前、部署中和部署后步骤的清单可帮助您实施拒绝服务 (DoS) 和区域保护最佳实践。PAN-OS 管理员指南的的链接提供了配置详细信息。

DoS 攻击是泛洪目标服务器的单一来源。分布式拒绝服务 **(DDoS)** 攻击是指来自多个来源的流量淹没单个目标服务器。与 DoS 攻击相比，DDoS 攻击会尝试启动更多会话，并且需要更多的资源来防御。由于防火墙是基于会话的，因此，它们是分层 DoS/DDoS 防御策略的一部分，而不是唯一的防御。

DoS 攻击会使合法用户无法使用设备或资源，这些攻击来自互联网或配置错误/被入侵的内部设备。典型的方法是向目标发送大量请求，这些请求会消耗其资源（内存、CPU 周期和带宽），从而使合法用户无法访问该目标。典型的攻击目标包括可从公司网络外部访问的面向互联网的设备，比如 Web 服务器和数据库服务器。作为分层 DoS 保护的一部分，Palo Alto Networks 提供三种 DoS 攻击防御工具。

区域保护配置文件根据进入区域的新会话数量保护单个入口区域。它们会限制与防火墙的每秒连接数 (CPS)，以广泛防御泛洪攻击，防范侦察（端口扫描和主机扫描），基于数据包的攻击和基于第 2 层协议的攻击。

DoS 保护配置文件和策略规则保护关键设备免遭新的会话泛洪的影响。保密策略保护单个设备。聚合策略保护设备组。

分类的 DoS 保护的一个主要好处是，根据 DoS 保护配置文件的 **Max Rate**（最大速率），自动将超过最大 CPS 速率的源 IP 地址添加到硬件阻止列表（在支持该列表的平台上节省软件资源）或软件阻止列表中。如果硬件阻止表已填满，则防火墙将使用软件阻止表。

DoS 保护可以处理大多数针对单个服务器的攻击，如果 DoS 保护还不够，区域保护会广泛保护整个区域。DoS 保护利用阻止表，因此，与区域保护相比，它消耗的资源更少。

数据包缓冲区保护 — 防御从现有会话发起的单次会话 DoS 攻击。该类攻击试图占用防火墙的数据包缓冲区。如果平台支持，数据包缓冲保护会隔离硬件表中的攻击 IP 地址。

- 策划 DoS 和区域保护最佳实践部署
- 用最佳实践部署 DoS 和区域保护
- DoS 和区域保护部署后最佳实践跟进

Palo Alto Networks 系列最佳实践书籍提供了有关解密、保护管理访问权限等主题的最佳实践建议。

策划 DoS 和区域保护最佳实践部署

本节讨论在实施 DoS 和区域保护之前需要了解和规划的内容的最佳实践，包括：

- 需要为其做好准备的不同 DoS 攻击类型。
- 如何使用多种预防机制来实施不同防御层级。
- 在何处布置防火墙。
- 如何了解要保护的区域和关键设备的平均正常和峰值每秒基准连接数 (CPS) 及其对 CPU 消耗的影响。
- 如何在运行所有其他消耗资源的功能的情况下了解防火墙资源的容量。

如果您的平台支持硬件区阻止表，请计划尽可能使用分类的 *DoS* 保护来保护关键的单个服务器。分类的 *DoS* 保护利用硬件阻止表来存储被阻止的 *IP* 地址，从而节省系统软件资源并提高性能。以下平台支持硬件阻止表：

- *PA-3200* 系列防火墙
- *PA-5200* 系列防火墙
- *PA-5400* 系列防火墙
- *PA-7000* 系列防火墙

除平台支持外，要使用硬件阻止表进行 *DoS* 保护，请执行以下操作：

- *DoS* 保护策略 ***Action***（操作）必须为 ***Protect***（保护）。
- *DoS* 保护配置文件必须是机密配置文件。
- 您必须使用 *RED* 作为丢弃机制。
- 您必须在 *DoS* 保护策略中使用 ***source-ip-only*** 或 ***src-dest-ip-both*** 作为分类的 ***Address***（地址）。

STEP 1 | 设立抵御各类 DoS 攻击的防御策略。

- 基于应用程序的攻击——攻击特定应用程序软肋，耗尽应用程序资源，致使合法用户无法使用应用程序。Slowloris 攻击为其中一个常见案例。
- **Protocol-Based Attacks**（基于协议的攻击）——又称静态耗尽攻击，其针对协议弱点进行攻击。SYN 洪泛攻击为其中一个常见案例。
- 容量耗尽攻击 — 容量耗尽攻击将侵占可用网络资源（特别是带宽），并夺取目标以阻止合法用户访问相关资源。UDP 协议洪泛攻击为其中一个常见案例。这些攻击可能来自单一来源

IP（DoS 攻击）或多个来源 IP（DDoS 攻击；源 IP 地址可能会轮换，攻击可能导致高 CPS 速率和/或高流量）。

STEP 2 | 采用分层方法防止 DoS 攻击。

防火墙具备应用程序流量可视化功能。专用 DoS 保护设备无法实现该功能。根据需要将网络边界的大量 DDoS 保护与针对单个设备的 DoS 保护层和整个区域的区域保护相结合，以保护您的网络和关键单个设备免受 DoS 攻击：

- 在面向 Internet 的网络边界处，即边界防火墙前，使用专用大容量 DDoS 保护设备和边界路由器、交换机或其他具有适当的访问控制列表 (ACL) 的硬件式数据包丢弃设备作为第一层防御。将专用的高容量 DDoS 设备置于外围防火墙前，以防御大规模攻击，而基于会话的防火墙并不是为应对这些攻击而设计的。
- 应用区域保护配置文件作为广泛的聚合保护层，以保护单个区域免受泛洪攻击，并增强外围的专用 DDoS 设备。
- 运用数据包缓冲区保护，防止 DoS 攻击消耗防火墙资源。
- 应用分类的 DoS 保护配置文件和策略来保护单个或一小部分高价值目标（DoS 保护配置文件和策略规则）：
  - 通过将 CPS 限制到每台服务器来保护面向互联网的关键服务器。
  - 通过限制来自可疑源（仅限面向内部区域，不包括面向 Internet 的区域）或是传输到受影响目标的 CPS，阻止配置错误或遭到入侵的内部主机执行 DoS 攻击。
  - 监控特定源（仅限面向内部的区域），并在来自该源的 CPS 达到某个阈值时发出警报，从而表明主机可能已遭到入侵或出现了配置错误。
  - 如果防火墙支持使用硬件阻止表，则保护区域内的特定设备。
  - 无论防火墙支持使用硬件阻止表还是软件阻止表，您都可以在日志中查看与攻击相关的 IP 地址。
- 如果需要，聚合 DoS 保护配置文件和策略可为关键服务器组提供另一层额外的广泛保护。在大多数情况下，对单个关键服务器进行分类的 DoS 保护和整个区域的分级 DoS 保护就已经足够，可以避免配置的复杂性。此外，聚合 DoS 保护日志不显示与攻击相关的 IP 地址，策略也不会利用硬件阻止表。要了解攻击的 IP 地址，请使用分类的 DoS 保护。

聚合 *DoS* 保护与区域保护的不同之处在于，区域保护可以保护整个区域免受攻击，而聚合 *DoS* 保护则保护区域内的一小部分关键设备。聚合 *DoS* 保护与分类的 *DoS* 保护的不同之处在于，分类的 *DoS* 保护为每台设备设置 *CPS* 阈值，而聚合 *DoS* 保护为一组设备设置 *CPS* 阈值。

详细了解分类和聚合 DoS 保护之间的区别，以帮助了解在不同场景中应使用哪种防护。

同时使用区域保护和 **DoS** 保护的阈值规划 — 如果您的平台支持硬件阻止表，请计划将分类的 DoS 保护阈值设置为低于区域保护阈值，这样 DoS 保护会首先激活，如果需要，区域保护会提供额外的防御层。如果要最大限度地保护一组关键设备，例如 Web 服务器或面向 Internet 的文件服务器，请添加聚合 DoS 保护，其阈值设置高于分类的 DoS 保护阈值且低于区域保护阈

值。（如果需要，这将使分类的 DoS 保护首先激活，然后激活聚合 DoS 保护，最后激活区域保护。）

如果您的平台不支持硬件阻止表，同样的方法仍然适用，但你无法获得将负载分摊到硬件阻止表的额外好处。

STEP 3 | 尽可能将防火墙设立在目标保护资源附近。

防火墙无法扩展到数百万个 CPS，因为它们是基于会话的。将防火墙放置在距离要保护的资源越近，流量消耗的会话和防火墙资源就越少。

- 将外围防火墙置到专用的高容量外围 DDoS 设备或使用 ACL 丢弃 DoS 流量的外围路由器或交换机后。这可以保护将企业网络分成区域的防火墙并保护这些区域中的设备。通常，防火墙越靠近外围，它的容器就必须越大，才能处理流量更高的流量。
- 检查您的网络区域分段。如果不够细化可以考虑创建更小的区域。较小区域可以从诸多方面提高安全性，包括更好地防止恶意软件横向移动，增加流量可视化，以及减少内部 DoS 攻击的潜在范围。

STEP 4 | 对您想要保护的设备和区域的 CPS 平均值和峰值进行基准测量，了解防火墙容量，从而让洪泛阈值不会意外阻碍流量或允许 DoS 攻击。使用其他常规资源消耗功能（例如解密、URL 过滤和 GlobalProtect）在高峰和正常流量高峰时段运行，测量 CPS。

- 对于区域保护配置文件阈值，如果您运行 PAN-OS 10.0 或更高版本，请使用 AIOps 云服务提供的区域保护配置文件阈值建议警报，该服务使用系统遥测来提供平均和平均峰值 CPS 值的准确估计。为该服务注册防火墙和 Panorama。（在 PAN-OS 10.2.1 或更高版本中，您可以安装适用于 Panorama 的 AIOps 插件，以便在将配置推送到托管防火墙之前主动对配置进行安全检查。）

  如果您无法使用 AIOps，请使用防火墙 ACC 和其他工具在至少一个工作周的营业时间内对每个防火墙区域进行基准 CPS 测量。数据采集时间跨度越长，测量结果越准确。测量每个区域的正常和峰值 CPS，为每个区域设置相应的区域保护泛洪阈值。
- 对关键设备（潜在目标）的 CPS 平均值和峰值进行基准测量。使用相同的工具检查缓冲区的利用率。
  - 运营期间，至少对面向 Internet 的关键设备进行为期一周的基准 CPS 测量。数据采集时间跨度越长，测量结果越准确。
  - 与应用程序团队合作，了解服务器的 CPS 正常值和峰值，以及服务器的最大 CPS 支持量。
  - 过滤防火墙流量和威胁日志中的关键设备目标 IP 地址，以测量正常和峰值会话活动的基准。
  - 考虑可能增加流量、更改流量模式或非网络常用应用程序的特殊事件、季度事件和年度事件。

  了解区域和单个设备的正常峰值 CPS 对于在区域保护和 DoS 保护配置文件中设置适当的阈值至关重要。如果您过于激进（将阈值设置得太低且允许的 CPS 太少），则可能会在活动高

峰期无意中限制合法流量。如果您过于保守（设置的阈值过高且允许的 CPS 过多），则可能不足以缓解 DoS 攻击，并且您尝试保护的资源可能会受到影响。

- 了解防火墙容量以及其他特性消耗的资源（CPU 和内存），以便了解 DoS 保护的有效容量。使用在高峰和正常交通时段运行的其他正常资源消耗功能来测量 CPS。
  - 如果使用 Panorama 管理防火墙，则可以利用设备监测测量 CPS 值。设备监测功能可以显示 CPU 平均值和峰值用度 90 天趋势线，以帮助您了解每个防火墙的典型可用容量。

    如果无法使用 Panorama 的设备监视功能，但可以使用 SNMP，则可以通过管理工具轮询以下三个 MIB，从而收集历史 CPS 数据：PanZoneActiveTcpCps、PanZoneActiveUdpCps 和 PanZoneOtherIpCps。

    MIB 显示的是实际 *CPS* 值的两倍，因为 *MIB* 分别计算 *C2S* 和 *S2C* 会话分段，而不是按单个会话计算。例如，如果一个 *MIB* 显示 *CPS* 值为 *10,000*，则真实 *CPS* 值为 *5,000*。
  - 使用如 Wireshark 或 NetFlow 等第三方工具收集和分析网络流量。
  - 考虑使用脚本实现自动化 CPS 信息收集和持续监测，从日志中挖掘信息。

STEP 5 | 配置日志转发触发器（流量匹配标准），自动使上游设备（例如交换机、路由器或专用 DDoS 设备）在防火墙受到攻击时执行额外的过滤和阻止，并保护防火墙资源。

当您配置日志转发触发器并出现触发条件时，防火墙会自动向上游设备发送 API 调用以对攻击采取措施。

在 HTTP 服务器或配置文件（**Device**（设备） > **Server Profiles**（服务器配置文件） > **HTTP**）中指定上游设备或设备和 API 调用。在 **Servers**（服务器）选项卡中指定上游设备，并在 **Payload Format**（负载格式）选项卡的 **Payload**（负载）字段中指定 API 调用。

在日志转发配置文件（**Objects**（对象） > **Log Forwarding**（日志转发））匹配列表筛选器中指定触发 API 调用的流量匹配条件。

- 要触发特定类型的攻击，请使用 Filter Builder 为要过滤或屏蔽的流量创建与威胁日志相匹配的过滤器。例如，以下过滤器指定了三个威胁 ID，分别对应于 FTP 暴力登录、HTTP 请求暴力破解攻击和 Apache Brute Force DOS 攻击威胁 ID：

  - **`(threatid eq 40001)`** 或 **`(threatid eq 39290)`** 或 **`(threatid eq 35075)`**

  将日志转发配置为在这些威胁签名时触发，使防火墙能够发送 API 调用，要求指定的上游设备过滤或阻止违规流量。
- 要保护防火墙资源免受攻击，尤其是在阻止表较小的平台上，请使用日志转发配置文件中的过滤器生成器创建在 DoS 攻击条件下触发的过滤器，这样上游设备就可以阻止违规流量，而不是允许该流量消耗防火墙阻止列表资源。

  检查上游设备的容量，确保它能够处理流量负载。

  将日志转发配置为在 DoS 流量条件下触发使防火墙能够发送 API 调用，要求指定的上游设备将流量发送到空路由并静默丢弃流量，从而节省防火墙阻止表资源。

用最佳实践部署 DoS 和区域保护

DoS 和区域保护有助于保护单个关键服务器（DoS 保护）和区域（区域保护），防止基于应用程序和协议的泛洪攻击。这些防护还针对位于互联网边界的专用 DDoS 防护设备后的容量耗尽攻击提供了下一层防御。

开始部署之前，请先测量关键服务器和区域的每秒连接数 (CPS) 的平均值和峰值，以便了解基准正常和峰值 *CPS*，并且可以设置智能泛洪阈值。

部署包括：

- 创建区域保护配置文件
- 应用 DoS 保护策略规则和配置文件
- 启用全局数据包缓冲区保护
- 启用 per-ingress-zone 数据包缓冲区保护
- 将最佳实践漏洞保护配置文件附加到安全策略允许规则

STEP 1 | 创建 Zone Protection profiles（区域保护配置文件）（**Network**（网络） > **Network Profiles**（网络配置文件） > **Zone Protection**（区域保护））并进行应用，从而为每个区域防御威胁。

区域保护配置文件适用于入口区域中的新会话，可以防止洪泛攻击、侦察（端口扫描和主机扫描）、基于数据包的攻击和基于第二层协议的攻击。

- 设置丢弃流量的 **Alarm Rate**（报警率）、**Activate**（激活）和 **Maximum**（最大）阈值，从而防止 TCP SYN、UDP、ICMP、ICMPv6 和其他 IP 新会话泛洪影响防火墙。设置 SYN 泛洪的 **Action**（操作）。

  评估 *CPU* 消耗率，从而确保防火墙能够支持 *DoS* 和区域保护以及消耗 *CPU* 处理周的其他期功能，例如解密。

  如果您有 *Panorama*，请使用运行状况监视器（***Panorama*** > ***Managed Devices***（托管设备） > ***Health***（运行状况）），以便检查指定时间段内的 *CPU* 和内存消耗。如果没有 *Panorama*，请运行正在运行的资源监视器，并指定测量 *CPU* 消耗率的时间范围。如果使用 *SNMP*，则可以从监视系统中提取信息。

  对于 TCP SYN 泛洪，请将 **Action**（操作）设置为 **Random Early Drop**（随机早期丢弃）或 **SYN Cookie**，以便在超出泛洪阈值时控制防火墙丢弃会话的方式。以下方法需要相互权衡：

  - **SYN Cookies** — 当 SYN-ACK 发生握手错误时，SYN Cookie 会丢弃流量。SYN Cookie 不会丢弃合法流量，只会丢弃违反握手协议的流量，因此它在本质上比 RED 更公平，因为它只会丢弃非法流量。SYN Cookie 也更容易部署，因为它更容易设置泛洪阈值。但

是，SYN Cookie 会消耗更多资源，因此，在使用 SYN Cookie 时，请监控防火墙 CPU 和内存利用率。

- 随机早期丢弃 (RED) — 根据您设置的基于 **Activate**（激活）和 **Maximum**（最大） CPS 阈值的几率曲线，不加区分地丢弃流量（非基于威胁，因此恶意和合法流量都会被丢弃）。当 CPS 达到 **Activate**（激活）阈值时，防火墙会开始丢弃会话。随着会话数量增加，丢弃率会升高，直到达到 **Maximum**（最大）会话阈值。这时，所有高于最大 CPS 率的新会话都会被删除，直到 CPS 率降至最大阈值以下。随着会话从 **Activate**（激活）阈值增加到 **Maximum**（最大）阈值，激活阈值和最大 CPS 阈值之间的差异越大，丢弃概率上升得越慢。

选择 SYN Cookie 还是 RED 取决于可用的防火墙资源、您希望区域支持的会话数以及您希望丢弃流量的力度。由于 SYN Cookie 不会影响合法流量，而 RED 会影响合法流量，因此，您可能更愿意先使用 SYN Cookie，同时监控 CPU 和内存使用率，当 SYN Cookie 消耗过多系统资源时，再切换到 RED。

为 *SYN Cookie* 或 *RED* 设置区域保护阈值时，请将其设置得足够高，从而允许合法会话的正常和峰值负载，同时也要设置得足够低，从而防止泛洪。由于要保护整个区域，因此，请将区域保护阈值设置为高于分类的 *DoS* 保护阈值（略高于聚合 *DoS* 保护阈值）。此方法首先为单个关键目标激活分类 *DoS* 保护，然后为关键目标组激活聚合 *DoS* 保护（如果使用），最后激活区域保护。

SYN Cookie 会丢弃表现为错误 SYN 握手的流量。**Activate**（激活）和 **Maximum**（最大）阈值确定何时开始丢弃错误的 SYN 握手（激活）以及何时停止接受 SYN 流量（最大值）。SYN Cookie 阈值：

- **Alarm Rate**（警报率） — 为了适应正常波动，请将值设置为高于平均区域 CPS 值的 15-20%。
- **Activate**（激活）— 由于 SYN Cookie 仅惩罚错误流量，而不惩罚合法流量，因此，请立即激活 SYN Cookie（0 CPS 阈值，这是默认值），以便不允许具有错误 SYN 握手的流量。
- **Maximum**（最大值）— 由于 SYN Cookie 仅惩罚不良流量，因此，请将最大值设置为防火墙平台的最大 CPS 容量，同时，请考虑其他活动资源密集型功能，这样您就不会因为

阈值低而不必要地阻止正常 SYN 流量。（最大值较低就不会激进地丢弃错误流量，因为 SYN Cookie 会在达到激活阈值时丢弃错误流量。）

当 *SYN Cookie* 达到最大阈值时，防火墙会在 *SYN* 泛洪方向上阻止所有会话 *5* 分钟。其他方向的流量不受影响。*SYN Cookie* 阻止时间不可配置。

RED 阈值：

- **Alarm Rate**（警报率） — 为了适应正常波动，请将值设置为高于平均区域 CPS 值的 15-20%。
- **Activate**（激活）— 设置略高于区域的正常峰值 CPS 速率，以便开始断开连接以缓解泛洪（不开始丢弃正常峰值活动内的流量），这通常比 **Alarm Rate**（警报率）高 15-20%。
- **Maximum**（最大值）— 根据防火墙的 CPU 利用率设置最大速率。如果防火墙 CPU 利用率高于 50%，请将最大 CPS 设置为 **Activate**（激活）速率的两倍。如果防火墙 CPU 利用率低于 50%，请将最大 CPS 设置为 **Activate**（激活） 速率的三倍并监控 CPU 使用率。如果 CPU 使用率过高，请将“最大值”降低到 **Activate**（激活）速率的两倍。超过此阈值会阻止新连接，直到 CPS 速率降至阈值以下。

  具有多个数据平面处理器 *(DP)* 的防火墙跨 *DP* 分配连接。防火墙通常会将跨 *DP* 平均分配 *CPS* 阈值设置。例如：如果一个防火墙有五个 *DP*，所设***Alarm Rate***（警报值）为 *20,000 CPS*，那么每个 *DP* 都有一个 *4,000 CPS (20,000 / 5 = 4,000)* 的***Alarm Rate***（警报值）值。因此，如果新 *CPS* 在一个 *DP* 超过 *4,000*，则会触发那个 *DP* 的警报值。

  Monitor（监控） > ***Logs***（日志） > ***Threat***（威胁）并过滤 ***Log Type***（日志类型）`Flood`（泛滥）以查看警报。

  - 监控该阈值，并根据需要进行调整。

- 在所有区域上启用 Reconnaissance Protection（侦测保护），以阻止主机扫描、不同类型的扫描和其他侦测活动。确保设定默认事件**Threshold**（阈值），以便阻止侦察操作之前记录数个数据包进行分析。使用 **Source Address Exclusion**（源地址排除）以允许测试网络漏洞的内部分组。
- 丢弃可疑数据包，以防止以数据包为基础的攻击。
  - **IP Drop**（**IP** 丢弃）——丢弃**Unknown**（未知）和**Malformed**（异常）数据包。丢弃**Strict Source Routing**（严格源路由）和**Loose Source Routing**（松散源路由） 数据包，因为源路由允许攻击者绕过使用目标 IP 地址作为匹配标准的安全策略规则。仅丢弃内部区域的 **Spoofed IP address**（伪造 **IP** 地址）包，以确保在进入时，源地址与防火墙路由表匹配。
  - **TCP Drop**（**TCP** 丢弃）— 保留默认丢弃选择 **TCP SYN with Data**（**TCP SYN** 及数据）和 **TCP SYNACK with Data**（**TCP SYNACK** 及数据），选择 **Mismatched**

overlapping TCP segment（不匹配的重叠 **TCP** 分段）和 **Split Handshake**（分离握手），同时启用剥离选项 **TCP Timestamp**（**TCP** 时间戳）。

如果您在一个区域配置隧道内容检查，并启动***Rematch Sessions***（重新匹配会话），则仅对该区域禁用 ***Reject Non-SYN TCP***（拒绝非 ***SYN TCP***），以便在启用或编辑隧道内容检查策略时，不会导致防火墙丢弃现有隧道会话。

- **ICMP Drop**（**ICMP** 丢弃）——拦截项取决于 ICMP 设置。
- **IPv6 Drop**（**IPv6** 丢弃）——如果存在合规要求，丢弃具有不符合路由头、扩展名等的数据包。
- **ICMPv6 Drop**（**ICMPv6** 丢弃）——如果存在合规要求，丢弃某些不匹配安全策略规则的数据包。

- 启用协议保护以拒绝未在网络上使用的协议，防止第二层和 vwire 接口受到基于第二层协议的攻击。
  - 对于通过位于防火墙前的第 3 层设备连接到公共 Internet 的 Vwire 接口，请在面向 Internet 的区域中启用 **Protocol Protection**（协议保护）。
  - 对于第 2 层区域，请在面向 Internet 的区域中启用 **Protocol Protection**（协议保护）。在内部第 2 层区域中，请启用 **Protocol Protection**（协议保护），并使用 **Include List**（包含列表），以便仅允许您使用的第 2 层协议，同时自动拒绝所有其他协议。（请勿使用 **Exclude List**（包含列表），否则会允许不在该列表中的所有协议。） 如果未配置**Protocol Protection**（协议保护），则所有第二层协议均默认为允许。
- 在每个**Zone Protection Profile**（区域保护配置文件）字段中，为每个区域（**Network**（网络） > **Zones**（区域））附加一个配置文件。

STEP 2 | 将DoS 保护应用于特定关键网络资源，特别是系统用户通过 Internet 访问时经常受到攻击的目标，如 WEB 和数据库服务器。

DoS 保护提供了一层防御来保护区域内的关键单个目标。您可以设置区域保护 CPS 阈值以保护整个区域，该区域接收的聚合 CPS 速率比大多数单个设备可以处理的速率高得多。针对单个关键服务器的攻击可能无法达到足够高的 CPS 速率，因而无法激活区域保护，这就是为区域内的关键目标配置 DoS 保护的原因。DoS 保护包括：

- DoS 保护策略规则，用于指定设备、用户、区域和服务，从而定义要防范 DoS 攻击的流量。
- DoS 保护配置文件，为不同类型的流量设置泛洪阈值。

将 DoS 保护配置文件添加到 DoS 保护策略规则。配置文件定义防火墙应用于策略规则中定义的流量的 CPS 阈值。

配置分类和/或聚合 DoS 保护配置文件，并将一个或两个文件应用于 DoS 保护策略规则（每个策略规则可以具有其中一种类型的配置文件）。分类配置文件设置适用于规则中指定的每个单独设备的阈值，并在具有硬件阻止表的平台上利用硬件阻止表。聚合配置文件设置阈值，这些

阈值适用于规则中指定的组合设备组（组的组合 CPS 速率必须超过阈值才能激活 DoS 保护）并使用软件表。

与区域保护相似，您可以将 **Action**（操作）设置为 SYN Cookie或 Random Early Drop（随机早期丢弃） (RED) 以控制防火墙缓解攻击的方式。同样，选择哪个取决于您的可用防火墙资源，您希望区域支持的会话数以及您希望丢弃流量的激进程度。监控系统资源使用率，并在 SYN Cookie 消耗过多资源时切换到 RED。如果防火墙前没有专用 DDoS 预防设备，请始终使用 RED 。

设置 *DoS* 保护阈值时，请将分类 *DoS* 保护阈值设置为最低值，以便首先将其激活以保护关键的单个目标。如果使用聚合 *DoS* 保护，请将这些阈值设置为高于分类的 *DoS* 保护阈值和低于区域保护阈值，以便聚合 *DoS* 保护仅在分类的 *DoS* 保护不足时，在区域保护之前激活。

- 为要保护的每个关键设备或关键设备集创建 DoS Protection profile（DoS 保护配置文件）（**Objects**（对象） > **Security Profiles**（安全配置文件） > **DoS Protection**（**DoS** 保护））。设置 SYN、UDP、ICMP、ICMPv6 和其他 IP 洪泛阈值，并对 SYN 洪泛设置**Action**（执行）。由于每个网络不尽相同，默认阈值通常不适用——请根据目标保护设备容量设置不同阈值。

  评估防火墙 CPU 消耗率，以确保防火墙能够支持 *DoS* 和区域保护，以及其他消耗 *CPU* 处理周期的功能，例如解密。

  将 SYN Cookie 配置为 SYN 泛洪的 **Action**（操作）时：

  - **Alarm Rate**（警报值） ——针对分类配置文件设置的 CPS 值，需高于设备平均 CPS 值的 15-20%，满足正常波动。

    对于缩合配置文件，设置 CPS 值需高于设备组平均 CPS 值的15-20% 。

  - **Activate Rate**（激活速率）— 分类配置文件将特定的 CPS 限制应用到单个设备。根据单个设备的容量设置限制，因此无需逐渐限制 CPS，并且可以将 **Activate Rate**（激活速

率）设置为与 **Max Rate**（最大速率）相同的阈值。仅在需要流量达到**Max Rate**（最大值）前开始降低流量时，设置**Activate Rate**（激活值）低于**Max Rate**（最大值）。

对于聚合配置文件，请将阈值设置为略高于组的正常峰值 CPS 速率，以免丢弃正常活动预期范围内的流量。这通常比 **Alarm Rate**（报警率）高 15-20%。

- **Max Rate**（最大速率）— 对于分类配置文件，请将 **Max Rate**（最大速率）设置为要保护的设备的最大容量，以便可以接受最大流量负载而不会出现泛洪。

  对于聚合配置文件，请将阈值设置为组容量的 80-90%。当 CPS 达到阈值时，防火墙丢弃**Block Duration**（阻止持续时间）的新连接。

- **Block Duration**（阻止持续时间）— 对于所有配置文件，使用默认值（300 秒），即可以阻止攻击会话，也不会对来自同一源的长时间合法会话作出惩罚。

- 监控该阈值，并根据需要进行调整。

将 RED 配置为 **Action**（操作）时：

- **Alarm Rate**（警报值） ——针对分类配置文件设置的 CPS 值，需高于设备平均 CPS 值的 15-20%，满足正常波动。

  对于缩合配置文件，设置 CPS 值需高于设备组平均 CPS 值的15-20% 。

- **Activate Rate**（激活速率）— 对于分类配置文件，将阈值设置为略高于目标的正常峰值 CPS 速率，以开始丢弃连接和缓解攻击（不要设置较低的阈值来丢弃正常峰值活动内的流量），这通常比 **Alarm Rate**（警报率）高 15-20%。

  对于聚合配置文件，请将阈值设置为略高于组的正常峰值 CPS 速率，以免丢弃正常活动预期范围内的流量。这通常比 **Alarm Rate**（报警率）高 15-20%。

- **Max Rate**（最大速率）— 对于分类和聚合配置文件，请根据防火墙的 CPU 利用率设置最大速率。如果防火墙 CPU 利用率高于 50%，请将最大 CPS 设置为 **Activate**（激活）速率的两倍。如果防火墙 CPU 利用率低于 50%，请将最大 CPS 设置为 **Activate**（激活） 速率

的三倍并监控 CPU 使用率。如果 CPU 使用率过高，请将“最大值”降低到 **Activate**（激活）速率的两倍。超过此阈值可阻止新连接，直到 CPS 速率降至阈值以下。

将最大速率设置为不高于单个设备的容量（分类）或组容量的 *80-90%*（聚合），以避免允许的连接数超过目标可以处理的连接数。

当 CPS 达到阈值时，防火墙会在 **Block Duration**（阻止持续时间）内丢弃新连接。

- **Block Duration**（阻止持续时间）— 对于所有配置文件，使用默认值（300 秒），即可以阻止攻击会话，也不会对来自同一源的长时间合法会话作出惩罚。
- 监控该阈值，并根据需要进行调整。

- 创建 DoS Protection policy rules（DoS 保护策略规则）（**Policies**（策略）> **DoS Protection**（**DoS** 保护））。尽可能具体化每个规则，以保护关键设备，同时保留防火墙 CPU 和内存资源。将 DoS 保护配置文件附加到 DoS 保护策略。在策略规则中，设置：
  - **Service**（服务）——指定正在保护的服务器上所使用的服务（端口）。如果要保护 WEB 服务器，请为 WEB 应用程序指定 HTTP、HTTPS和其他适当的服务端口。

    对关键服务器未使用的服务端口使用单独的 *DoS* 保护策略规则。

  - **Action**（执行） -选择**Protect**（保护），将规则相关的 DoS 保护配置文件应用于指定设备。“保护”是唯一应用 DoS 保护的 **Action**（操作）。
  - 日志转发——为了便于管理，将 DoS 日志与其他威胁日志分开存备，直接通过电子邮件转发给管理员和日志服务器。
  - **Aggregate**（综合） -使用综合配置文件来保护关键服务器组。
  - **Classified**（分类）> **Profile**（配置文件）— 使用分类配置文件保护关键的单个服务器。必须使用分类配置文件来利用硬件阻止表。
  - **Classified**（分类）> **Address**（地址）— 计数器消耗防火墙资源。对于分类 DoS 保护配置文件，规定连接是否计入以**source-IP-only**（仅源 **IP**）或**destination-IP-only**（仅目标 **IP**）为基础，亦或是以两者（**src-dest-ip-both**（源与目标**IP**））为基础的配置文件。DoS

保护目标、保护内容以及受保护设备是否位于面向 Internet 的区域是配置阈值计数器的参考标准。

对于面向 Internet 的区域，切勿使用 **src-ip-only**（仅源 **IP**），或者**src-dest-ip-both**（源与目标 **IP**），因为防火墙无法为所有 Internet IP 地址存储计数器。在边界区域使用 **destination-IP-only**（仅目标 **IP**）。

使用**destination-IP-only**（仅目标 **IP**）保护单个关键设备。将最大阈值设置为低于策略中指定的每个设备可以处理的 CPS 速率。

使用**source-IP-only**（仅源 **IP**）和**Alarm**（警报）阈值监测可疑主机（非面向 Internet 的区域）。

与只跟踪源 IP 或目标 IP 的计数器相比，防火墙需要消耗更多资源，以跟踪**src-dest-ip-both**（源与目标 **IP**）计数器。

要在支持硬件阻止表的平台上使用它，必须使用 ***source-ip-only*** 或 ***src-dest-ip-both***。***Destination-ip-only*** 使用软件表。

STEP 3 | 全局启用 Packet Buffer Protection（数据包缓冲区保护），以保护防火墙缓冲区免遭单会话 DoS 攻击，从单个源 IP 地址发起的攻击，以及从创建许多组合使用数据包缓冲区的小型会话的源 IP 地址发起的攻击。

全局数据包缓冲区保护是一种二阶方法的第一个阶段，可以保护防火墙缓冲区且默认处于启用状态。（步骤 4 介绍了第二个阶段，即每个区域的数据包缓冲区保护，默认情况下也会启用此保护。 全局数据包缓冲区保护可以检测对防火墙数据包缓冲区的消耗造成威胁的个别会话或源 IP 地址，并将 RED 应用到这些会话或数据包，从而在缓冲区拥堵加剧时丢弃更多数据包。

数据包缓冲区保护的目标是防止防火墙进入和保持高延迟、高缓冲区利用率状态，方法是首先应用 RED 丢弃违规数据包（全局保护），然后在攻击继续发生时丢弃违规会话或阻止违规源 IP 地址（会话或主机阻止）（按区域保护）。理念是在软件和硬件级别保护数据包缓冲区，同时实现低延迟和低数据包丢失率，并在正确的时间丢弃或阻止违规流量。

如果主机发送大量流量，以致防火墙在未设置会话的情况下串行处理和拒绝这些流量时，数据包缓冲区保护也可以保护防火墙缓冲区。这种流量通常具有相同的 *6* 元组标识符（源和目标 *IP*、源和目标端口、协议和入口区域）。如果未启用数据包缓冲区保护，则在处理每个数据包后拒绝它所需的资源会消耗防火墙资源。

如果已启用每区域数据包缓冲区保护，并且缓冲区消耗达到较高水平且持续可配置的时间量，则防火墙将仅丢弃违规会话或违规主机。如果已禁用按区域数据包缓冲区保护，则防火墙将执行 RED，但不会丢弃或阻止流量。

- 使用数据包缓冲区利用率的基准测量了解防火墙容量，确保启用适当大小的防火墙，从而保证仅在受到攻击时，才会出现缓冲区使用率大幅上升的情况。了解正常高峰时段操作期间的数据包缓冲区利用率，以及何时出现延迟或丢弃问题。如果防火墙的容量足够低，以致正常的流量也会导致缓冲区达到使用峰值，则可能需要一个更大容量的防火墙。

  在 PAN-OS 10.0 及更高版本中，考虑使用 **Monitor Only**（仅监控）模式（**Device**（设备） > **Setup**（设置） > **Session**（会话） > **Session Settings**（会话设置）），以了解您的基准数据

包缓冲区利用率和识别积极的来源。在 **Monitor Only**（仅监控）模式下，防火墙会监控数据包缓冲区利用率，并在会话和源有异常时发出警报，但不会阻止或丢弃它们。一种权衡方法是，您可以尝试不同 警报和激活阈值，并在不会影响流量的威胁日志中查看结果，但防火墙不受数据包缓冲区攻击的保护。如果可以在非生产环境下复制生产流量，则可以安全地试验警报和激活阈值，以查看哪些会话受到不同阈值设置的惩罚，以及哪些阈值会开始影响合法流量。

- 根据缓冲区利用率或 CPU 处理延迟设置全局数据包缓冲区保护阈值（**Device**（设备） > **Setup**（设置） > **Session**（会话） > **Session Settings**（会话设置））。基于 CPU 处理延迟的数据包缓冲区保护对突然出现的大数据包爆发的响应比基于缓冲区利用率百分比的缓冲区保护更快。

  默认会启用基于缓冲区利用率百分比的数据包缓冲区保护：

  - **Alert**（警报） — 首先使用默认值 (50%)，监视数据包缓冲区利用率，并在必要时调整阈值。
  - **Activate**（激活） - PAN-OS 10.0 及更高版本中的默认 **Activate**（激活）阈值为 80%，在 PAN-OS 9.1 及更早版本中为 50%。最安全的方法是将激活阈值设置为比基准使用量高 10-20%，然后监视数据包缓冲区利用率，而不是使用默认值。调整阈值，直到数据包缓冲区保护及时激活，从而对违规会话进行惩罚，但不惩罚正常使用。

    正确的激活设置取决于环境和可用的处理资源，因此通常需要进行试验。激活阈值越低，阻止合法流量的可能性就越大，但攻击缓解会开始得更快。阈值越高，开始缓解攻击所需的时间就越长，但合法流量受到影响的可能性就越小。

    如果激活阈值对环境来说太高，则在激活数据包缓冲区保护之前，您将遇到高负载和/或延迟对合法流量的影响。

    如果激活阈值对环境来说太低，则防火墙会不必要地丢弃太多合法数据包，即使有资源处理流量也是如此。（如果存在其他网络问题，也可能发生这种情况。）

    如果激活阈值基本适合环境，则丢弃的合法流量很少，并且不会对防火墙资源造成压力。了解基准数据包缓冲区负载是正确调整阈值的关键。例如，如果您知道数据包缓冲区利

用率在高峰时段可能会飙升到防火墙容量的 40-50%，并且在数据包缓冲区利用率达到 60-70% 时会遇到问题，则将 **Activate**（激活）阈值设置为 55-60%。

在 *PAN-OS 10.0* 及更高版本中，您可以尝试设置 ***Alert***（警报）和 ***Activate***（激活）阈值，并使用 ***Monitor Only***（仅监视）模式查看结果。***Monitor Only***（仅监视）模式不会对违规流量执行任何操作，但可以让您在激活数据包缓冲区保护之前了解阈值如何影响流量。

要测量数据包缓冲区利用率，请使用Panorama 运行状况监视器。此外，以下 CLI 操作命令也很有用：

- **`> show running resource-monitor`** 命令显示 CPU 统计数据。**`ingress-backlogs`** 选项显示至少占用 2% 片上数据包描述符的会话。
- 对于数据包缓冲区保护主动保护防火墙的会话，**`> show session packet-buffer-protection`** 命令显示消耗最多数据平面 CPU 资源的会话。

默认会禁用数据包缓冲区保护基于延迟的激活。基于延迟的保护无法防御 DoS 攻击，其中源不断发送防火墙拒绝的数据包，这会消耗资源，但不会被视为延迟，因为防火墙从不为拒绝的流量建立会话。（但是，基于缓冲区利用率的数据包缓冲区保护可防止这些类型的攻击。）

当数据包缓冲区利用率不高时，**Latency Based Activation**（基于延迟的激活）可缓解高片上描述符消耗，当您希望防火墙在数据包缓冲区耗尽之前做出反应时，这是最佳方法。

选择 **Latency Based Activation**（基于延迟的激活），使保护基于 CPU 处理延迟，而不是基于缓冲区利用率的百分比。以下三个设置取代基于利用率的 **Alert**（警报）和 **Active**（活动）设置：

- **Latency Alert**（延迟警报）— 首先使用默认值（50 毫秒），然后监控延迟，并在必要时调整阈值。
- **Latency Activate**（延迟激活）— 首先使用默认值（200 毫秒），然后监控延迟，并在必要时调整阈值。
- **Latency Max Tolerance**（延迟最大容差）— 首先使用默认值（500 毫秒），然后监控延迟，并在必要时调整阈值。当流量达到 **Latency Activate**（延迟激活）阈值时，防火墙使

用 RED 来开始丢弃流量并提高丢弃率，直到延迟达到 **Latency Max Tolerance**（延迟最大容差）。在 **Latency Max Tolerance**（延迟最大容差）下,丢弃率接近 100%。

测量每个防火墙上的延迟：

- ***fw-1> debug dataplane pow performance | match pbp*** 操作命令。
- 在数据平面负载较高时启用日志记录以接收通知和查看日志信息（***Device***（设备） > ***Setup***（设置） > ***Management***（管理） > ***Logging and Reporting***（日志记录和报告）和 ***Enable Log on High DP Load***（在高 ***DP*** 负载时启用日志））。使用操作 *CLI* 命令 ***show running resource monitor*** 检查数据平面负载。您还可以创建技术支持文件并以文本格式浏览数据平面日志。

- 设置阈值和计时器（**Device**（设备） > **Setup**（设置） > **Session**（会话） > **Session Settings**（会话设置）），以定义何时丢弃违规会话或阻止违规源 IP 地址。仅当您启用按区域的数据包缓冲区保护时，防火墙才会使用这些阈值和计时器。如果仅启用全局数据包缓冲区保护，防火墙将对流量执行 RED，但不会丢弃或阻止它。

  根据以下方面进行设置：延迟和缓冲区利用率的经验和测量，由于缓冲区拥塞而导致的延迟和数据包丢弃的容忍度，以及您希望丢弃流量来避免影响网络及其用户的延迟和数据包缓冲区消耗的主动程度。

  - **Block Countdown Threshold**（阻止倒计时阈值）— 缓冲区利用率百分比或延迟阈值（以毫秒为单位），这用于启动倒计时以丢弃或阻止违规流量。当缓冲区拥塞或延迟达到**Block Countdown Threshold**（阻止倒计时阈值）时，**Block Hold Time**（阻止保持时间）开始减少。（当阻止保持时间耗尽时，防火墙将丢弃会话或阻止违规主机。）

    将 **Block Countdown Threshold**（阻止倒计时阈值）设置为比 **Activate**（激活）或 **Latency Activate**（延迟激活阈值）低 10%，监控数据包缓冲区利用率，并根据需要调整值。此方法阻止违规 IP 地址并放弃会话的速度比默认设置（延迟为 80% 或 500 毫秒）更快。**Block Hold Time**（阻止保持时间）值越小，防火墙越早开始通过丢弃会话或阻止有问题的源 IP 来缓解缓冲区拥塞。该值越大，数据包缓冲区攻击在防火墙缓解攻击之前可以持续的时间就越长。

  - **Block Hold Time**（阻止保持时间）— 在防火墙丢弃会话或阻止源 IP 地址之前，违规会话可以保持在**Block Countdown Threshold**（阻止倒计时阈值）以上的时间量。该值越小，防火墙越早激活数据包缓冲区保护，并利用硬件阻止表和/或软件阻止表（在具有硬件阻止表的系统上）来保护数据包缓冲区。

    首先使用默认值，然后监控数据包缓冲区利用率，并在必要时调整该时间值。此方法阻止违规 IP 地址的速度快于默认设置（60 秒）。时间值越大，数据包缓冲区攻击在防火墙缓解之前可以继续的时间就越长。

    只要拥塞保持在 **Block Countdown Threshold**（阻止倒计时阈值）以上，阻止保持时间就会减少。当 **Block Hold Time**（阻止保持时间）达到 0 时，防火墙会放弃该会话或阻止源 IP 地址。

- **Block Duration**（阻止持续时间）— 隔离（阻止）源 IP 地址的 **Block Hold Time**（阻止保持时间）过期后的时间量。首先使用默认值（3600 秒），如果阻止源 IP 地址一小时对您的业务条件来说会造成过大的损失，则减小该值。监测数据包缓冲区利用率，并在必要时调整该阀值。

如何设置数据包缓冲区阈值取决于您的网络流量以及您希望如何处理该流量：

- 默认设置的是保守值，这有利于在丢弃会话或阻止源 IP 地址之前允许数据包缓冲区拥塞持续更长时间，从而防止惩罚合法流量。防火墙不会在拥塞期间快速阻止潜在的合法会话和源，但代价是减慢不会导致数据包缓冲区拥塞的合法会话。这就是为什么最佳做法是从更低和更激进的阈值开始。
- 用户对网络缓慢的抱怨可能表明数据包缓冲区阈值过于保守。要解决这些抱怨，请降低 **Activate**（激活）率和 **Block Countdown Threshold**（阻止倒计时阈值），从而更快地启动 RED 数据包丢弃。降低 **Block Hold Time**（阻止保持时间），以便在缓冲区消耗率达到 **Block Countdown Threshold**（阻止倒计时阈值）后，防火墙更快地开始阻止 IP 地址或丢弃会话。

  更快地丢弃或阻止违规流量意味着不会导致数据包缓冲区消耗问题的合法流量不会因违规流量而受到延迟或数据包丢弃问题的影响，但违规流量将被隔离。但是，发送大量流量的合法会话或源 IP 地址也可能会更快地被隔离。
- 如果您担心将 **Activate**（激活）速率和 **Block Countdown Threshold**（阻止倒计时阈值）设置得更低可能会阻止重要的合法流量，例如 DNS 或其他关键基础设施流量，请将 **Block Hold Time**（阻止保持时间）增加到更高的值，以延迟隔离操作并监控数据包缓冲区使用情况。
- 调整数据包缓冲区保护阈值，以实现延迟和数据包丢失与何时丢弃会话或阻止源 IP 地址之间的平衡，这对您的网络有意义。

STEP 4 | 数据包缓冲区保护的第二阶段基于按入口区域保护防火墙缓冲区，默认情况下在 PAN-OS 10.0 及更高版本中启用（在 PAN-OS 9.1 及更早版本中默认禁用），但还必须启用全局数据包缓冲区保护，否则按区域的数据包缓冲区保护不起作用。按区域的数据包缓冲区保护会丢弃

违规会话并阻止违规源 IP 地址，当您需要为特定入口区域提供额外的保护层时，这是一种最佳做法。

当您不想阻止特定区域的源 *IP* 地址或丢弃会话时，请禁用按区域的数据包缓冲区保护（默认情况下，防火墙还会全局应用 *RED*，使数据包缓冲区仍具有主要保护层）。如果阻止源 *IP* 地址，则会阻止来自该地址的所有会话，而不仅仅是违规的会话。如果源 *IP* 地址是 *NAT* 设备，则可能表示从 *NAT* 设备后产生了大量用户流。

- 要禁用或启用按区域保护，**Network**（网络） > **Zones**（区域），请选择现有区域或 **Add**（添加）区域，然后选中或取消选中 **Enable Packet Buffer Protection**（启用数据包缓冲区保护）。

在考虑启用或禁用按区域的数据包缓冲区保护时，不仅要考虑易受外部攻击的区域，还要考虑内部网络。考虑潜在的内部威胁，意外错误配置的内部设备，生成大量非法流量的故障 *NIC* 适配器以及防火墙配置错误。

所有这些都可以拒绝来自任何合法源的流量，这些流量也会向防火墙发送大量流量，因为防火墙通过其唯一的 *6* 元组标识符（源和目标 *IP*、源和目标端口、协议和入口区域）标识所有重要流量源。在数据包缓冲区拥塞期间，*RED* 会影响发送大量流量以及违规源的合法源。

STEP 5 | 将最佳实践漏洞保护配置文件附加到所有安全策略允许规则中。

结合专用大容量边界 DDoS 保护、区域保护配置文件、DoS 保护配置文件和策略规则、数据包缓冲区保护和漏洞保护等技术，为您的网络及关键资源提供多层 DoS 保护。

DoS 和区域保护部署后最佳实践跟进

在部署区域和 DoS 保护之后，请确保一切按预期工作，并采取相关措施，确保网络扩展后，一切仍按预期工作。

STEP 1 | 评估防火墙性能，确保相关性能符合可接受标准，以帮助您了解区域和 DoS 保护对防火墙资源产生的效果。

如果区域和 DoS 保护级别（与解密等其他消耗资源功能相结合）消耗了太多的防火墙资源，那么最佳实践方案即为扩大资源，而非牺牲安全性。

STEP 2 | 配置日志转发。

为方便管理，使用独立日志转发配置文件转发 DoS 和区域阈值事件日志，与其他威胁日志区别存放。直接将 DoS 和区域日志通过电子邮件发送给相关管理员和日志服务器。通知内容仅包含可能为 DoS 攻击的事件记录。将 DoS 事件日志转发配置到 DoS 保护策略规则（**Policies**（策略）> **DoS Protection**（**DOS** 保护）），将区域事件日志转发配置到每个区域（**Network**（网络）> **Zones**（区域））。

将**Alarm Rate**（警报值）阈值事件日志消息设置为低级别或信息级别。将 DoS 保护状态设置为**Activate**（激活）、**Maximum**（最大），和区域保护**Activate Rate**（激活值）、**Max Rate**（最大值）阈值事件日志消息为严重程度。在设置恰当的洪泛阈值之后，日志将显示网络潜在洪泛攻击， 仅显示威胁事件和异常事件。如果误报过多，是由于阈值设置得太低，或者防火墙的大小与处理流量不匹配所致。

防火墙每 *10* 秒收集累积日志，以便管理日志容量，避免日志服务器过载，同时保留防火墙资源。

STEP 3 | 留意并调查 DoS 攻击的其他指标。

除了配置日志转发，方便管理员在超过洪泛阈值时接收通知外，还要检查攻击指标，调查潜在的 DoS 攻击：

- 回顾 DoS 威胁活动（**ACC** > **Threat Activity**（威胁活动）），寻找滥用模式。
- 使用支持该功能的防火墙模型（PA-3050、PA-3060、PA-3200 系列、PA-5200 系列和 PA-7000 系列）针对因潜在 DoS 攻击而被防火墙阻止的 IP 地址监测被拦截 IP 地址（**Monitor**（监测）> **Block IP List**（拦截 **IP** 清单））。**Block Source**（拦截源）列标识拦截 IP 地址的分类 DoS 保护配置文件名称。
- 如果部分或所有防火墙流量中断，或出现 WEB 浏览或端点连接缓慢、新会话失败等情况，可能表明存在 DoS 攻击。CPU 利用率高、数据包缓冲区和描述符耗尽，以及活动会话数量激增等情况，也可以存在 DoS 攻击的征兆。
- 了解更多关于区域和 DoS 保护事件日志和全局计数器，以便监测 DoS 活动。

泛洪阈值违规可能表示存在 *DoS* 攻击，但它们也可能表示 *CPS* 值配置错误、另一个内部设备配置错误、*NIC* 适配器故障、来自内部人员的潜在威胁或防火墙大小不正确。

STEP 4 | 网络流量模式会随着时间的推移而变化。当有新设备加入网络，或旧设备被拆除时，这类特殊事件也会暂时影响流量模式。

鉴于上述情况，需要定期进行新的 CPS 测量，重新访问区域和 DoS 洪泛阈值设置 — 因为网络持续扩展，DoS 和区域保护需要迭代的方法。