paloalto
TECHDOCS

Protection DoS et protection de zones respectant les meilleures pratiques

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

Protection DoS et Protection de Zones Respectant les Bonnes Pratiques

Cette liste de contrôle des étapes de pré-déploiement, de déploiement et de post-déploiement vous aide à mettre en œuvre les meilleures pratiques de Denial-of-Service (déni de service – DoS) et de protection de zone. Les liens vers le Guide de l'administrateur PAN-OS fournissent des détails de configuration.

Une **attaque DoS** est une source unique saturant un serveur cible. Une **attaque Distributed Denial-of-Service (déni de service distribué – DDoS)** consiste en plusieurs sources saturant un seul serveur cible. Les attaques DDoS tentent de lancer plus de sessions que les attaques DoS et davantage de ressources sont nécessaires pour s'en défendre. Étant donné que les pare-feu sont basés sur la session, ils font partie d'une stratégie de défense DoS/DDoS par couches, et ne représentent pas la seule défense.

Les attaques DoS rendent un périphérique ou une ressource indisponible pour les utilisateurs légitimes et proviennent d'Internet ou de périphériques internes mal configurés ou compromis. La méthode typique consiste à saturer la cible de requêtes qui consomment ses ressources (mémoire, cycles de processeur et bande passante) pour rendre la cible indisponible pour les utilisateurs légitimes. Les cibles les plus courantes sont les périphériques communiquant avec Internet, auxquels on peut accéder depuis l'extérieur du réseau d'entreprise, comme les serveurs Web et de base de données. Les pare-feu de Palo Alto Networks vous fournissent trois outils de réduction des risques dans le cadre de son approche multiple de la protection DoS.

Les Zone Protection Profiles (profils de protection de zone) protègent les zones d'entrée individuelles en fonction du nombre de nouvelles sessions entrant dans une zone. Ils limitent les connexions par seconde (CPS) au pare-feu pour une protection étendue contre les attaques par saturation et protègent contre la reconnaissance (analyses de ports et balayages d'hôtes), les attaques basées sur les paquets et les attaques basées sur le protocole de couche 2.

Les profils de protection DoS et les règles de politique protègent les périphériques critiques contre les saturations de nouvelle session. Les politiques classées protègent les périphériques individuels. Les politiques cumulées protègent des groupes de périphériques.

Un avantage majeur de la protection DoS classée est de placer automatiquement les adresses IP source qui dépassent le taux de CPS maximum dans la liste de blocage du matériel (permet d'économiser les ressources logicielles sur les plateformes qui le prennent en charge) ou dans la liste de blocage des logiciels, en fonction du **Max Rate** (Taux max)du profil de protection DoS. Si la table de blocage du matériel est pleine, le pare-feu utilise la table de blocage des logiciels.

La protection DoS gère la plupart des attaques qui ciblent des serveurs individuels et la protection de zone protège largement la zone entière si la protection DoS ne suffit pas. La protection DoS exploite les tables de blocage, elle consomme donc moins de ressources que la protection de zone.

Packet Buffer Protection (Protection de la mémoire tampon des paquets) : elle protège contre les attaques DoS sur une session unique à partir de sessions existantes qui tentent de saturer la mémoire tampon des paquets des pare-feu. La protection de la mémoire tampon des paquets met en quarantaine les adresses IP attaquantes dans la table du matériel si la plateforme prend cela en charge.

- Planification du déploiement de la protection DoS et de la protection de zones respectant les meilleures pratiques

- Déploiement de la protection DoS et de la protection de zones respectant les meilleures pratiques
- Meilleures pratiques concernant le suivi du déploiement de la protection DoS et de la protection de zones

La série de livres sur les meilleures pratiques de Palo Alto Networks offre des conseils à propos des meilleures pratiques sur des sujets tels que le décryptage, la sécurisation de l’accès administratif, et bien plus encore.

Planification du déploiement de la protection DoS et de la protection de zones respectant les meilleures pratiques

Cette section décrit les meilleures pratiques relatives à ce que vous devez savoir et planifier avant de mettre en œuvre une protection DoS et de zone, notamment :

- différents types d'attaques DoS pour lesquels se préparer ;
- comment superposer vos défenses à l'aide de plusieurs mécanismes de prévention ;
- où positionner vos pare-feu ;
- comment comprendre la moyenne normale et maximale des connexions par seconde (CPS) de référence des zones et des périphériques critiques que vous souhaitez protéger et son effet sur la consommation du processeur ;
- comment comprendre la capacité de vos ressources de pare-feu avec toutes les autres fonctionnalités consommatrices de ressources en cours d'exécution.

Si votre plateforme prend en charge une table de blocage du matériel, prévoyez d'utiliser autant que possible la protection DoS classée pour protéger les serveurs individuels critiques. La protection DoS classée exploite la table de blocage du matériel pour stocker les adresses IP bloquées, ce qui permet d'économiser les ressources logicielles du système et d'améliorer les performances. Les plateformes suivantes prennent en charge la table de blocage du matériel :

- *Pare-feu PA-3200 Series*
- *Pare-feu PA-5200 Series*
- *Pare-feu PA-5400 Series*
- *Pare-feu PA-7000 Series*

Afin d'utiliser la table de blocage du matériel pour la protection DoS, en plus de la prise en charge de la plateforme :

- *l'**Action** de la politique de protection DoS doit être **Protect** (Protéger) ;*
- *le profil de protection DoS doit être un profil classé ;*
- *vous devez utiliser RED comme mécanisme d'abandon ;*
- *vous devez utiliser **source-ip-only** ou **src-dest-ip-both** comme **Adresse** classée dans la politique de protection DoS.*

STEP 1 | Planifiez votre défense contre chaque type d'attaque DoS.

- **Attaques basées sur des applications**—Elles ciblent les vulnérabilités dans une application spécifique et tentent d'épuiser ses ressources afin que des utilisateurs légitimes ne puissent pas l'utiliser. L'attaque Slowloris en est un exemple.
- **Attaques basées sur le protocole** : aussi connues sous le nom d'attaques par épuisement d'état, elles ciblent les vulnérabilités des protocoles. Parmi elles, on compte l'attaque SYN flood très répandue.
- **Attaques volumétriques** : attaques à volume élevé, qui tentent de submerger les ressources réseau disponibles, et plus particulièrement la bande passante, afin de neutraliser la cible dans le but d'empêcher des utilisateurs légitimes d'accéder à ses ressources. Parmi elles, on compte l'attaque par UDP flooding. Ces attaques peuvent provenir d'une seule adresse IP source (attaque DoS) ou de nombreuses adresses IP sources (attaque DDoS ; les adresses IP sources peuvent pivoter et l'attaque peut se présenter sous la forme d'un taux de CPS élevé et/ou d'un volume de trafic élevé).

STEP 2 | Planifiez une approche multiple pour prévenir les attaques DoS.

Le pare-feu apporte de la visibilité sur le trafic des applications que les périphériques dédiés à la protection DoS ne sont pas en mesure de fournir. Combinez une protection DDoS à volume élevé au niveau du périmètre réseau avec des couches de protection DoS pour les périphériques individuels et de protection de zone pour l'ensemble de la zone, selon les besoins, afin de protéger votre réseau et vos périphériques individuels critiques contre les attaques DoS :

- Utilisez un périphérique dédié à la protection DDoS, capable de traiter de gros volumes, ou un routeur de périmètre, un commutateur de périmètre ou tout autre périphérique dédié à l'abandon de paquets avec des listes de contrôles d'accès (ACL) adéquates comme première ligne de défense au niveau du périmètre du réseau faisant face à Internet. Placez les périphériques de protection DDoS dédiés à volume élevé devant les pare-feu de périmètre pour les protéger contre les attaques à volume élevé, que le pare-feu basé sur la session n'est pas conçu pour gérer.
- Appliquez des profils de protection de zone sous la forme d'une couche de protection étendue et cumulée pour protéger les zones individuelles contre les attaques par saturation et pour augmenter le périphérique de protection DDoS dédié au périmètre.
- Appliquez la Protection de la mémoire tampon des paquets pour empêcher que les attaques DoS ne consomment les ressources de mémoire tampon des paquets du pare-feu.

- Appliquez des profils et des politiques de protection DoS classés pour protéger des cibles individuelles ou de petits groupes de cibles de grande valeur (profils de protection DoS et règles de politique) :
  - Protégez les serveurs critiques communiquant avec Internet en limitant les CPS à chaque serveur.
  - Empêchez des hôtes internes compromis ou configurés de manière incorrecte de mener une attaque DoS en limitant les CPS au niveau de la source douteuse (zones communiquant avec l'intranet uniquement, et non avec Internet) ou au niveau de la destination affectée.
  - Surveillez une source spécifique (zones communiquant avec l'intranet uniquement) et soyez alerté lorsque les CPS de cette source atteignent un certain seuil, ce qui pourrait être le signe d'un hôte compromis ou configuré de manière incorrecte.
  - Protégez des périphériques spécifiques à l'intérieur d'une zone si le pare-feu prend en charge l'utilisation de la table de blocage du matériel.
  - Obtenez une visibilité sur les adresses IP associées à l'attaque dans les journaux, que le pare-feu prenne en charge l'utilisation de la table de blocage du matériel ou de la table de blocage des logiciels.
- Les politiques et profils de protection DoS cumulés fournissent une couche supplémentaire de protection étendue pour les groupes de serveurs critiques, si nécessaire. Dans la plupart des cas, la protection DoS classée pour les serveurs critiques individuels et la protection de zone pour l'ensemble de la zone sont suffisantes et évitent la complexité de la configuration. En outre, les journaux de protection DoS cumulés n'indiquent pas les adresses IP associées à une attaque et les politiques n'exploitent pas la table de blocage du matériel. Pour obtenir une visibilité sur les adresses IP attaquantes, utilisez la protection DoS classée.

  La protection DoS cumulée diffère de la protection de zone dans la mesure où la protection de zone protège une zone entière contre les attaques, tandis que la protection DoS cumulée protège un petit groupe de périphériques critiques à l'intérieur d'une zone. La protection DoS cumulée diffère de la protection DoS classée dans la mesure où la protection DoS classée définit un seuil de CPS pour chaque périphérique individuel, tandis que la protection DoS cumulée définit un seuil de CPS pour un groupe de périphériques.

Apprenez-en davantage sur les différences entre la protection DoS classée et cumulée pour pouvoir comprendre laquelle utiliser dans différents scénarios.

Planification des seuils pour l'utilisation conjointe de la protection de zone et de la protection DoS : si votre plateforme prend en charge une table de blocage du matériel, prévoyez de définir des seuils de protection DoS classée inférieurs aux seuils de protection de zone afin que la protection DoS s'active en premier et que la protection de zone fournisse une couche de protection supplémentaire, si nécessaire. Si vous souhaitez optimiser la protection d'un groupe de périphériques critiques, par exemple, des serveurs Web ou des serveurs de fichiers communiquant avec Internet, ajoutez une protection DoS cumulée avec des seuils définis à des valeurs supérieures à celles des seuils de protection DoS classés et inférieures à celles des seuils de protection de zone. (Ainsi, la protection DoS classée s'active en premier, la protection DoS cumulée s'active en deuxième et la protection de zone s'active en troisième, si nécessaire.)

Si votre plateforme ne prend pas en charge une table de blocage du matériel, la même méthodologie s'applique toujours, mais vous n'obtenez pas l'avantage supplémentaire de décharger vers la table de blocage du matériel.

STEP 3 | Positionnez les pare-feu au plus près possible des ressources qu'ils protègent.

Les pare-feu ne s'adaptent pas à des millions de CPS, car ils sont basés sur des sessions. Plus vous placez les pare-feu proches des ressources que vous protégez, moins le trafic consomme de sessions et de ressources de pare-feu.

- Placez les pare-feu de périmètre *derrière* des périphériques de protection DDoS de périmètre haute capacité dédiés ou des routeurs ou commutateurs de périmètre qui utilisent des listes de contrôle d'accès pour abandonner le trafic DoS. Cela protège les pare-feu qui segmentent le réseau d'entreprise en zones et protègent les périphériques dans ces zones. Plus un pare-feu est proche du périmètre, plus sa capacité doit être grande pour gérer le volume de trafic plus élevé.
- Examinez la segmentation de votre zone réseau. S'il n'est pas suffisamment granulaire, envisagez de créer de plus petites zones. De plus petites zones renforcent la sécurité de nombreuses façons, y compris en prévenant de manière plus efficace les mouvements latéraux de logiciels malveillants, en améliorant la visibilité sur le trafic, et en réduisant l'étendue potentielle d'attaques DoS internes.

STEP 4 | Prenez des mesures de référence des moyennes et des valeurs de crête des CPS des périphériques individuels critiques pour les zones que vous souhaitez protéger, et ayez une vision claire des capacités de vos pare-feu pour que les seuils de saturation n'étranglent pas le trafic ou n'autorisent pas des attaques DoS de manière accidentelle. Mesurez les CPS avec d'autres fonctionnalités consommatrices de ressources normales comme le décryptage, le filtrage des URL et GlobalProtect en cours d'exécution pendant les heures de trafic maximal et les heures de trafic normal.

- Pour les seuils de profil de protection de zone, si vous exécutez PAN-OS 10.0 ou version ultérieure, utilisez les alertes de recommandation de seuil de profil de protection de zone du service cloud AIOps qui utilise la télémétrie système pour fournir des estimations précises des valeurs de CPS de pointe moyennes et moyennes. Inscrivez des pare-feu et Panorama pour le service. (Avec PAN-OS 10.2.1 ou version ultérieure, vous pouvez installer le plug-in AIOps pour Panorama afin d'appliquer de manière proactive les vérifications de sécurité sur les configurations avant de les pousser vers des pare-feu gérés.)

  Si vous ne pouvez pas utiliser AIOps, utilisez le pare-feu ACC et d'autres outils pour prendre des mesures de CPS de référence pour chaque zone de pare-feu pendant au moins une semaine ouvrable, pendant les heures de ouvrables. Plus la période de collecte de données sera longue, plus les mesures seront précises. Mesurez les CPS normales ainsi que les CPS maximales pour chaque zone individuelle afin de définir des seuils de saturation de protection de zone appropriés pour chaque zone.

- Pour la protection DoS, prenez des mesures de référence des moyennes et des valeurs de crête des CPS des périphériques essentiels (cibles potentielles). Utilisez les mêmes outils pour examiner l'utilisation de la mémoire tampon.
  - Prenez des mesures de référence des CPS des périphériques essentiels faisant face à Internet sur une semaine ouvrable au moins, pendant les heures ouvrables. Plus la période de collecte de données sera longue, plus les mesures seront précises.
  - Collaborez avec des équipes d'application pour avoir une idée des moyennes et des valeurs de crête des CPS sur leurs serveurs et des valeurs maximales que leurs serveurs peuvent supporter.
  - Filtrez le Trafic du pare-feu et les journaux de Menaces pour les adresses IP destinations de périphériques essentiels pour avoir une mesure de référence des activités de session normales et maximales.
  - Prenez en compte des événements spéciaux, les événements trimestriels et les événements annuels pouvant augmenter le trafic, changer les modèles du trafic, ou utiliser des applications qui ne sont pas sur le réseau habituellement.

  Comprendre les CPS maximales normales des zones et des périphériques individuels est crucial pour définir des valeurs de seuils appropriées dans les profils de protection de zone et de protection DoS. Si vous êtes trop agressif (en définissant des seuils trop bas et en autorisant trop peu de CPS), vous risquez par inadvertance de limiter le trafic légitime pendant les pics d'activité. Si vous êtes trop passif (en définissant des seuils trop élevés et en autorisant trop de CPS), la protection peut ne pas être suffisante pour atténuer une attaque DoS et les ressources que vous essayez de protéger peuvent être affectées.
- Comprenez la capacité de vos pare-feu et les ressources (processeur et mémoire) que les autres fonctionnalités consomment afin de connaître la capacité disponible pour la protection DoS. Mesurez les CPS avec d'autres fonctionnalités consommatrices de ressources normales exécutées pendant les heures de trafic maximale et les heures de trafic normal.
  - Si vous utilisez Panorama pour gérer les pare-feu, utilisez Surveillance de périphérique pour mesurer les valeurs de CPS. La surveillance de Périphérique peut également vous afficher une courbe de tendance sur 90 jours de l'utilisation moyenne du processeur ainsi que de ses pics d'utilisation, pour vous aider à comprendre la capacité disponible habituelle de chaque pare-feu.

    Si vous ne pouvez pas utiliser la fonction Device Monitoring (Surveillance de périphérique) de Panorama et que vous utilisez SNMP, vous pouvez utiliser vos outils de gestion pour sonder les trois bases d'information de gestion (MIBs) suivantes dans le but de recueillir un historique des données : PanZoneActiveTcpCps, PanZoneActiveUdpCps, et PanZoneOtherIpCps.

    Les MIB affichent deux fois la valeur de CPS réelle, car les MIB comptent les segments de session C2S et S2C séparément plutôt que comme une seule session. Par exemple, si un MIB exprime une valeur CPS de 10 000, la valeur CPS réelle est 5 000.
  - Utilisez des outils tiers tels que Wireshark ou NetFlow pour recueillir des données relatives au trafic réseau et les analyser.
  - Pensez à utiliser des scripts pour automatiser la collecte d'informations relatives aux CPS et la surveillance continue, ainsi que pour extraire des informations des journaux.

STEP 5 | Configurez un déclencheur de transfert des journaux (critères de correspondance du trafic) pour qu'un périphérique en amont tel qu'un commutateur, un routeur ou un périphérique de

protection DDoS dédié effectue automatiquement un filtrage et un blocage supplémentaires lorsque le pare-feu est attaqué et pour protéger les ressources du pare-feu.

Lorsque vousconfigurez un déclencheur de transfert des journaux et que les conditions de déclenchement sont rassemblées, le pare-feu envoie automatiquement un appel d'API au périphérique en amont pour qu'il prenne des mesures contre l'attaque.

Spécifiez le ou les périphériques en amont et l'appel d'API (la mesure que le ou les périphériques en amont doivent prendre) dans un profil de serveur HTTP (**Device** > **Server Profiles** > **HTTP**). Spécifiez le(s) périphérique(s) en amont dans l'onglet **Servers** (Serveurs) et spécifiez l'appel d'API dans le champ **Payload** (Charge utile) de l'onglet **Payload Format** (Format de la charge utile).

Spécifiez les conditions de correspondance de trafic qui déclenchent l'appel d'API dans un filtre de liste de correspondance de profil de transfert des journaux (**Objects** > **Log Forwarding**).

- Pour un déclenchement avec un type particulier d'attaques, utilisez le Filter Builder (Générateur de filtres) pour créer un filtre qui correspond aux journaux des menaces pour le trafic que vous souhaitez filtrer ou bloquer. Par exemple, le filtre suivant spécifie trois ID de menace qui correspondent aux ID de menace FTP Brute Force Login (Connexion par force brute au FTP), HTTP Request Brute Force Attack (Attaque par force brute sur requête HTTP) et Apache Benchmark Brute Force DOS Attack (Attaque DoS par force brute sur Apache Benchmark) :

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

  La configuration du transfert des journaux pour un déclenchement avec ces signatures de menace permet au pare-feu d'envoyer l'appel d'API qui demande au(x) périphérique(s) en amont spécifié(s) de filtrer ou de bloquer le trafic incriminé.
- Pour protéger les ressources du pare-feu contre les attaques, en particulier sur les plateformes comportant des tables de blocage plus petites, utilisez le Filter Builder (Générateur de filtres) dans le profil de transfert des journaux pour créer un filtre qui se déclenche dans des conditions d'attaque DoS afin que le périphérique en amont bloque le trafic incriminé au lieu de permettre à ce trafic de consommer les ressources de la liste de blocage du pare-feu.

  Vérifiez la capacité du périphérique en amont pour vous assurer qu'il peut gérer la charge de trafic.

  La configuration du transfert des journaux pour qu'il se déclenche dans des conditions de trafic DoS permet au pare-feu d'envoyer un appel d'API qui demande au(x) périphérique(s) en amont spécifié(s) d'envoyer le trafic vers une route nulle et de rejeter silencieusement le trafic, économisant ainsi les ressources de la table de blocage du pare-feu.

Déploiement de la protection DoS et de la protection de zones respectant les meilleures pratiques

La protection DoS et la protection de zone permettent de protéger les serveurs critiques individuels (protection DoS) et les zones (protection de zone) contre les attaques par saturation basées sur les applications et les protocoles. Ils fournissent également une couche supplémentaire de protection contre les attaques volumétriques après votre périphérique de prévention DDoS dédié au niveau du périmètre Internet.

Mesurez les connexions par seconde (CPS) moyennes et maximales *des serveurs et des zones critiques avant de commencer le déploiement, pour comprendre les CPS normales et maximales de référence et pouvoir définir des seuils de saturation intelligents.*

Le déploiement comprend :

- Création de profils de protection de zone
- Appliquer les règles et profils des politiques de protection DoS
- Activer la protection globale de la mémoire tampon des paquets
- Activer la protection de la mémoire tampon des paquets sur une zone d'entrée
- Attacher les profils de protection contre les vulnérabilités aux règles d’autorisation de la politique de sécurité

STEP 1 | Créez des profils de protection de zone (**Network** > **Network Profiles** > **Zone Protection**) et appliquez-les pour défendre chaque zone.

Les profils de Protection de Zone s’appliquent aux nouvelles sessions en zones d’entrée et assurent une protection contre les attaques de type flood, contre les opérations de reconnaissance (balayage de port et d’hôtes), les attaques basées sur les paquets et les attaques basées sur le protocole de couche 2.

- Définissez les seuils **Alarm Rate** (Taux de déclenchement d’alarme), **Activate** (Activer) et **Maximum** pour abandonner le trafic afin d’empêcher les saturations de nouvelles sessions TCP

SYN, UDP, ICMP, ICMPv6 et autres IP d'affecter le pare-feu. Définissez l'**Action** pour les saturations SYN.

Mesurez la consommation de ressources processeur pour vous assurer que le pare-feu puisse prendre en charge la Protection DoS et la Protection de Zone ainsi que d'autres fonctionnalités consommant des cycles de processeur, comme le décryptage.

*Si vous avez Panorama, utilisez Health Monitor (Moniteur de santé) (**Panorama** > **Managed Devices** > **Health**) pour vérifier la consommation de ressources processeur et de mémoire sur une période de temps spécifiée. Si vous n'avez pas Panorama, exécutez* `show running resource-monitor` *et spécifiez le délai pour mesurer la consommation de ressources processeur. Si vous utilisez SNMP, vous pouvez extraire les informations de votre système de surveillance.*

Pour les saturations TCP SYN, définissez l'**Action** sur **Random Early Drop** (Abandon anticipé aléatoire) ou sur **SYN Cookies** (Cookies SYN) pour contrôler la méthode employée par le pare-feu pour abandonner les sessions lorsque les seuils de saturation sont dépassés. Il existe des compromis entre les méthodes :

- **SYN Cookies** (Cookies SYN) : SYN Cookies abandonne le trafic lorsque la liaison SYN-ACK est mauvaise. SYN Cookies n'abandonne pas le trafic légitime, uniquement le trafic qui va à l'encontre des protocoles de liaison, cette action est donc intrinsèquement plus juste que le RED, car elle n'abandonne que le mauvais trafic. SYN Cookies est également plus facile à déployer, car il est plus facile de définir les seuils de saturation. Cependant, SYN Cookies consomme plus de ressources, donc lorsque vous l'utilisez, surveillez l'utilisation du processeur et de la mémoire par le pare-feu.
- **Random Early Drop** (RED, Abandon anticipé aléatoire) : abandonne le trafic sans distinction (sans se baser sur les menaces, de sorte que le trafic malveillant et le trafic légitime sont abandonnés) selon une courbe de probabilité basée sur les seuils de CPS **Activate** (Activer) et **Maximum** que vous avez définis. Lorsque les CPS atteignent le seuil **Activate** (Activer), le pare-feu commence à abandonner des sessions. À mesure que le nombre de sessions augmente, le taux d'abandon augmente jusqu'à ce qu'il atteigne le seuil de session **Maximum**. Toutes les nouvelles sessions au-dessus du taux de CPS Maximum sont abandonnées jusqu'à ce que le taux de CPS tombe en dessous du seuil Maximum. Plus la différence entre les seuils de CPS Activate (Activer) et Maximum est grande, plus la probabilité d'abandon augmente lentement à mesure que le nombre de sessions augmente pour passer du seuil **Activate** (Activer) au seuil **Maximum**.

Le choix entre SYN Cookies et RED dépend des ressources de pare-feu disponibles, du nombre de sessions que vous souhaitez qu'une zone prenne en charge et de l'agressivité avec laquelle vous souhaitez abandonner le trafic. Étant donné que SYN Cookies n'a pas d'impact sur le trafic légitime, contrairement à RED, vous pourrez préférer commencer par SYN Cookies, surveiller l'utilisation

du processeur et de la mémoire, et passer à RED si SYN Cookies consomme trop de ressources système.

Lorsque vous définissez des seuils de Protection de Zone pour les actions SYN Cookies et RED, définissez des valeurs suffisamment élevées pour autoriser la charge normale et le pic de charge des sessions légitimes, et suffisamment basses pour éviter les saturations. Étant donné que vous protégez la zone entière, définissez des seuils de Protection de Zone supérieurs aux seuils de protection DoS classés et légèrement supérieurs aux seuils de protection DoS cumulée. Cette méthode active la protection DoS classée en premier pour les cibles critiques individuelles, la protection DoS cumulée en second (le cas échéant) pour les groupes de cibles critiques et la Protection de Zone en troisième.

L'action SYN Cookies abandonne le trafic qui présente de mauvaises liaisons SYN. Les seuils **Activate** (Activer) et **Maximum** déterminent quand commencer à abandonner les mauvaises liaisons SYN (Activate) et quand arrêter d'accepter le trafic SYN (Maximum). Seuils de l'action SYN Cookies :

- **Alarm Rate (Taux de déclenchement d'alarme)** : fixez la valeur à 15-20 % au-dessus du taux moyen des CPS de la zone pour l'adapter aux fluctuations normales.
- **Activate (Activer)** : étant donné que SYN Cookies ne punit que le mauvais trafic, et pas le trafic légitime, activez immédiatement SYN Cookies (seuil de CPS à 0, c'est-à-dire la valeur par défaut) afin qu'aucun trafic avec une mauvaise liaison SYN ne soit autorisé.
- **Maximum** : étant donné que SYN Cookies ne punit que le mauvais trafic, définissez le seuil Maximum sur la capacité de CPS maximale de la plateforme du pare-feu, en tenant compte des autres fonctionnalités actives gourmandes en ressources, afin de ne pas bloquer inutilement le bon trafic SYN à cause d'un seuil bas. (Un seuil Maximum inférieur n'abandonne pas le mauvais trafic de manière plus agressive, car l'action SYN Cookies abandonne le mauvais trafic au seuil Activate.)

  Lorsque SYN Cookies atteint le seuil Maximum, le pare-feu bloque toutes les sessions dans le sens de la saturation SYN pendant 5 minutes. Le trafic dans l'autre sens n'est pas affecté. Le temps de blocage du cookie SYN n'est pas configurable.

Seuils de l'action RED :

- **Alarm Rate (Taux de déclenchement d'alarme)** : fixez la valeur à 15-20 % au-dessus du taux moyen des CPS de la zone pour l'adapter aux fluctuations normales.
- **Activate (Activer)** : définissez-le juste au-dessus du taux maximum de CPS normal de la zone pour commencer à abandonner les connexions afin d'atténuer les saturations (ne commencez pas à abandonner le trafic qui se situe dans le pic d'activité normal), qui sont généralement de 15 à 20 % au-dessus de l'**Alarm Rate** (Taux de déclenchement d'alarme).
- **Maximum** : définissez le taux Maximum en fonction de l'utilisation du processeur par le pare-feu. Si l'utilisation du processeur par le pare-feu est supérieure à 50 %, définissez le seuil de CPS Maximum sur deux fois le taux **Activate** (Activer). Si l'utilisation du processeur par le pare-feu est inférieure à 50 %, définissez le seuil de CPS Maximum sur trois fois le taux **Activate** (Activer) et surveillez l'utilisation du processeur. Si l'utilisation du processeur est trop élevée,

réduisez le seuil Maximum à deux fois le taux **Activate** (Activer). Le dépassement du seuil Maximum bloque les nouvelles connexions jusqu'à ce que le taux de CPS repasse sous le seuil.

*Les pare-feux équipés de processeurs à multiples plans de données (DPs) répartissent les connexions à travers les DPs. Habituellement, le pare-feu partage équitablement les réglages de seuils des CPS à travers ses DPs. Par exemple, si un pare-feu est équipé de cinq DPs et que vous avez fixé le **Alarm Rate (Taux de Déclenchement d'Alarme)** à 20 000 CPS, alors chaque DP a un **Alarm Rate (Taux de Déclenchement d'Alarme)** de 4 000 CPS (20 000 / 5 = 4 000). Ainsi, si le nouveau taux de CPS sur DP dépasse 4 000, il actionne le seuil de déclenchement d'Alarme pour ce DP.*

***Monitor (Surveiller)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par le **Log Type (Type de journal)** **`flood (saturation)`** pour afficher les alarmes.*

- Surveillez et ajustez les seuils selon vos besoins.

- Activez la Reconnaissance Protection (Protection de reconnaissance) sur toutes les zones pour bloquer les balayages d'hôtes, différents types d'analyses et d'autres activités de reconnaissance. Gardez le **Threshold (Seuil)** d'événement par défaut pour journaliser quelques paquets afin de les analyser avant de bloquer les opérations de reconnaissance. Utilisez **Source Address Exclusion** (Exclusion d'adresse source) pour autoriser les groupes internes qui testent les vulnérabilités du réseau.
- Abandonnez les paquets douteux pour empêcher les attaques basées sur les paquets.
  - **IP Drop** : abandonnez les paquets **Unknown (Inconnus)** et **Malformed (Malformés)**. Abandonnez les paquets provenant de **Strict Source Routing (Routage depuis une Source Stricte)** et **Loose Source Routing (Routage depuis une Source Libre)**, car le routage de source permet à vos adversaires de contourner les règles de politiques de Sécurité utilisant l'adresse IP destination comme critère de correspondance. Pour les zones internes uniquement, abandonnez les paquets de **Spoofed IP address (adresse IP usurpée)** pour vous assurer que sur l'entrée, l'adresse source corresponde à la table de routage du pare-feu.
  - **TCP Drop** : conservez les sélections d'abandons par défaut **TCP SYN with Data (TCP SYN avec données)** et **TCP SYNACK with Data (TCP SYNACK avec données)**, sélectionnez **Mismatched overlapping TCP segment (Segments TCP superposés différents)** et **Split Handshake (Établissement de liaison de segmentation)**, puis activez l'option de retirer le **TCP Timestamp (Horodatage TCP)**.

    *Si vous configurez l'Inspection du Contenu du Tunnel sur une zone et activez l'option **Rematch Sessions (Revérifier les sessions)**, pour cette zone uniquement, désactivez **Reject Non-SYN TCP (Refuser Non-SYN TCP)** afin que l'activation ou la modification d'une politique d'Inspection du Contenu du Tunnel n'entraîne le pare-feu à abandonner des sessions de tunnel existantes.*
  - **ICMP Drop (Abandon ICMP)** : ce que vous bloquez dépend de comment vous utilisez ICMP, si vous l'utilisez.
  - **IPv6 Drop (Abandon IPv6)** : si vous êtes concerné par des règles de conformité, abandonnez les paquets de routage avec en-têtes, d'extensions etc. non conformes.

- **ICMPv6 Drop (Abandon ICMPv6)** : si vous êtes concerné par des règles de conformité, abandonnez certains paquets ne correspondant à aucune règle de politique de Sécurité.

- Activez la Protection de Protocole pour refuser les protocoles non utilisés sur votre réseau et pour empêcher les attaques basées sur le protocole de couche 2 et interfaces vwire.
  - Pour les interfaces vWire qui font face à l'Internet public à travers un périphérique de couche 3 situé devant le pare-feu, autorisez **Protocol Protection** (Protection du protocole) sur les zones qui font face à Internet.
  - Pour les zones de couche 2, autorisez **Protocol Protection** (Protection du protocole) sur les zones qui font face à Internet. Sur les zones internes de couche 2, autorisez **Protocol Protection** (Protection du protocole) et utilisez **Include List** (Inclure la liste) pour seulement autoriser les protocoles de couche 2 que vous utilisez et refuser automatiquement tous les autres protocoles. (N'utilisez pas **Exclude List** (Exclure la liste) qui autorise tous les protocoles qui ne figurent pas sur la liste.) Si vous ne configurez pas de **Protection de Protocole**, tous les protocoles de couche 2 sont autorisés.
- Associez un profil à chaque zone (**Network [Réseau]** > **Zones**) dans le champ **Zone Protection Profile (Profil de protection de zone)**.

STEP 2 | Appliquez la Protection DoS à des ressources spécifiques et essentielles, particulièrement les systèmes auxquels les utilisateurs accèdent depuis Internet, souvent ciblées par les pirates informatiques, comme les serveurs web et bases de données.

La protection DoS fournit une couche de défense pour protéger les cibles individuelles critiques à l'intérieur d'une zone. On définit des seuils de CPS de Protection de Zone pour protéger une zone entière, qui reçoit un taux de CPS global beaucoup plus élevé que la plupart des périphériques individuels peuvent gérer. Une attaque qui cible un seul serveur critique peut ne pas avoir un taux de CPS suffisamment élevé pour activer la Protection de Zone, c'est pourquoi vous configurez la protection DoS pour les cibles critiques à l'intérieur d'une zone. La protection DoS se compose de :

- règles de politiques de protection DoS, qui spécifient les périphériques, les utilisateurs, les zones et les services qui définissent le trafic que vous souhaitez protéger contre les attaques DoS ;
- profils de protection DoS, qui définissent les seuils de saturation de différents types de trafic.

Vous ajoutez un profil de protection DoS à une règle de politiques de protection DoS. Le profil définit les seuils de CPS que le pare-feu applique au trafic défini dans la règle de politique.

Configurez les profils de protection DoS cumulés et classés et associez l'un ou les deux à une règle de politiques de protection DoS (chaque règle de politique peut posséder un profil de chaque type). Les profils *Classified (Classés)* définissent des seuils qui s'appliquent à chaque périphérique individuel spécifié dans une règle et tirent parti de la table de blocage du matériel sur les plateformes qui en ont un. Les profils *Aggregate (Cumulés)* définissent des seuils qui s'appliquent au groupe combiné de périphériques spécifiés dans une règle (le taux de CPS combiné du groupe doit dépasser le seuil pour activer la protection DoS) et utilisent le tableau des logiciels.

De la même manière que la Protection de Zone, vous pouvez définir l'**Action** sur SYN Cookies (Cookies SYN) ou sur Random Early Drop (RED, Abandon anticipé aléatoire) pour contrôler la façon dont le pare-feu réduit les attaques. De même, le choix de l'action dépend des ressources du pare-feu disponibles, du nombre de sessions que vous souhaitez qu'une zone prenne en charge et de l'agressivité avec laquelle vous souhaitez abandonner le trafic. Surveillez l'utilisation des ressources système et si

SYN Cookies consomme trop de ressources, passez à RED. Utilisez toujours RED si vous n'avez pas de périphérique dédié à la prévention DDoS en face du pare-feu.

Lorsque vous définissez des seuils de protection DoS, définissez les seuils de protection DoS classés au plus bas afin qu'ils s'activent en premier pour protéger les cibles individuelles critiques. Si vous utilisez la protection DoS cumulée, définissez ces seuils à des valeurs supérieures aux seuils de protection DoS classée et inférieures aux seuils de Protection de Zone, afin que la protection DoS cumulée ne s'active que lorsque la protection DoS classée n'est pas suffisante, mais avant la Protection de Zone.

- Créez un profil de protection DoS (**Objects [Objets]** > **Security Profiles [Profils de sécurité]** > **DoS Protection [Protection DoS]**) pour chaque périphérique critique ou ensemble de périphériques critiques que vous souhaitez protéger. Fixez les seuils de saturation SYN, UDP, ICMP, ICMPv6, et autres seuils de saturation IP ainsi que l'**Action** pour les SYN floods. Dans la plupart des cas, les valeurs des seuils par défaut sont inadaptées, car chaque réseau est unique : fixez vos seuils sur la capacité du ou des périphériques que vous protégez.

  Mesurez la consommation de ressources processeur du pare-feu *pour vous assurer que le pare-feu puisse prendre en charge la protection DoS et la Protection de Zone ainsi que d'autres fonctionnalités consommant des cycles de processeur, comme le décryptage.*

  Lorsque vous configurez SYN Cookies comme **Action** pour les saturations SYN :

  - **Alarm Rate (Taux de Déclenchement d'Alarme)** : pour les profils classés, fixez la valeur à 15-20 % au-dessus du taux moyen des CPS du périphérique pour l'adapter aux fluctuations normales.

    Pour les profils cumulés, fixez la valeur à 15-20 % au-dessus du taux moyen des CPS du groupe.
  - **Activate Rate (Taux d'activation)** : les profils classés appliquent des limites de CPS spécifiques à des périphériques individuels. Basez les limites sur la capacité des périphériques individuels, de sorte que vous n'ayez pas besoin de limiter progressivement les CPS et que vous puissiez définir l'**Activate Rate (Taux d'activation)** sur le même seuil que le **Max Rate (Taux max)**. Fixez le **Activate Rate (Taux d'Activation)** plus bas que le **Max Rate (Taux Maximal)** uniquement si vous voulez commencer à abandonner du trafic avant qu'il n'atteigne le **Max Rate (Taux Maximal)**.

    Pour les profils cumulés, définissez le seuil juste au-dessus du taux de CPS maximal normal pour le groupe afin d'éviter d'abandonner le trafic qui se situe dans les attentes d'activité normales. Il s'agit généralement de 15 à 20 % au-dessus de l'**Alarm Rate (Taux de déclenchement d'alarme)**.
  - **Max Rate (Taux max)** : pour les profils classés, définissez le **Max Rate** sur la capacité maximale du ou des périphériques que vous protégez pour les empêcher d'être saturés, tout en acceptant leur charge de trafic maximale.

    Pour les profils cumulés, fixez le seuil sur une valeur allant de 80 à 90 % de la capacité du groupe. Quand les CPS atteignent le seuil, le pare-feu abandonne de nouvelles connexions pendant la **Block Duration (Durée du Blocage)**.
  - **Block Duration (Durée du blocage)** : utilisez la valeur par défaut (300 secondes) afin de bloquer la session qui attaque sans pénaliser des sessions légitimes provenant de la même source pour une trop longue période.

- Surveillez et ajustez les seuils selon vos besoins.

Lorsque vous configurez RED comme **Action** :

- **Alarm Rate (Taux de Déclenchement d'Alarme)** : pour les profils classés, fixez la valeur à 15-20 % au-dessus du taux moyen des CPS du périphérique pour l'adapter aux fluctuations normales.

  Pour les profils cumulés, fixez la valeur à 15-20 % au-dessus du taux moyen des CPS du groupe.
- **Activate Rate (Taux d'activation)** : pour les profils classés, définissez le seuil juste au-dessus du taux de CPS maximal normal de la cible pour commencer à abandonner les connexions et à réduire les attaques (ne définissez pas de seuils inférieurs qui abandonnent le trafic dans les limites du pic d'activité normal), qui est généralement de 15 à 20 % au-dessus de l'**Alarm Rate (Taux de déclenchement d'alarme)**.

  Pour les profils cumulés, définissez le seuil juste au-dessus du taux de CPS maximal normal pour le groupe afin d'éviter d'abandonner le trafic qui se situe dans les attentes d'activité normales. Il s'agit généralement de 15 à 20 % au-dessus de l'**Alarm Rate (Taux de déclenchement d'alarme)**.
- **Max Rate (Taux max)** : pour les profils classés et cumulés, définissez le taux maximal en fonction de l'utilisation du processeur par le pare-feu. Si l'utilisation du processeur par le pare-feu est supérieure à 50 %, définissez le seuil de CPS Maximum sur deux fois le taux **Activate** (Activer). Si l'utilisation du processeur par le pare-feu est inférieure à 50 %, définissez le seuil de CPS Maximum sur trois fois le taux **Activate** (Activer) et surveillez l'utilisation du processeur. Si l'utilisation du processeur est trop élevée, réduisez le seuil Maximum à deux fois le taux **Activate** (Activer). Le dépassement du seuil Maximum bloque les nouvelles connexions jusqu'à ce que le taux de CPS repasse sous le seuil.

  Définissez le taux maximal à une valeur ne dépassant pas la capacité du périphérique individuel (classé) ou 80 à 90 % de la capacité du groupe (cumulé) pour éviter d'autoriser plus de connexions que la cible ne peut en gérer.

  Quand le taux de CPS atteint le seuil, le pare-feu abandonne de nouvelles connexions pendant la **Block Duration (Durée du blocage)**.
- **Block Duration (Durée du blocage)** : utilisez la valeur par défaut (300 secondes) afin de bloquer la session qui attaque sans pénaliser des sessions légitimes provenant de la même source pour une trop longue période.
- Surveillez et ajustez les seuils selon vos besoins.

- Créez des règles de politiques de protection DoS (**Policies [Politiques]** > **DoS Protection [Protection DoS]**). Rendez chaque règle la plus précise possible afin de protéger des périphériques

essentiels tout en préservant les ressources et la mémoire du pare-feu. Associez les profils de protection DoS aux politiques de protection DoS. Dans la règle de politique, définissez :

- **Service** : spécifiez les services (ports) utilisés sur le ou les serveurs que vous protégez. Si vous protégez des serveurs web, spécifiez HTTP, HTTPS, et autres ports de services adaptés aux applications web.

  Utilisez des règles de politique de Protection DoS séparées pour les ports inutilisés de serveurs essentiels.

- **Action** : sélectionnez **Protect (Protéger)** pour appliquer le profil de Protection DoS de la règle aux périphériques spécifiés. Protect (Protéger) est la seule **Action** qui applique la protection DoS.
- **Transfert de Journaux** : pour une gestion simplifiée, transférez les journaux DoS séparément des journaux de Menaces directement aux administrateurs par messagerie et sur un serveur de journaux.
- **Aggregate (Cumulés)** : utilisez des profils cumulés pour protéger les groupes de serveurs critiques.
- **Classified** > **Profile** : utilisez des profils classés pour protéger les serveurs individuels critiques. Vous devez utiliser un profil classé pour exploiter la table de blocage du matériel.
- **Classified (Classés)** > **Address (Adresses)** : les compteurs consomment les ressources du pare-feu. Pour les profils de Protection DoS classés, précisez si les connexions sont prises en considération pour les seuils des profils sur la base de la **source-IP-only (IP source uniquement)**, la **destination-IP-only (IP destination uniquement)**, ou les deux (**src-dest-ip-both**). Vos objectifs de protection DoS, ce que vous protégez, et selon que vos périphériques protégés sont dans des zones faisant face à Internet ou non déterminent votre manière de configurer vos seuils de compteur.

  N'utilisez pas **src-ip-only** ou **src-dest-ip-both** pour des zones faisant face à Internet, car le pare-feu ne peut pas enregistrer les compteurs de toutes les adresses IP Internet possibles. Utilisez **destination-IP-only** dans les zones de périmètre.

  Utilisez **destination-IP-only** pour protéger les périphériques essentiels individuellement. Définissez le seuil Maximum en dessous du taux de CPS que chaque périphérique spécifié dans la politique peut gérer.

  Use **source-IP-only** ainsi que le seuil **Alarm (Alarme)** pour surveiller les hôtes douteux (dans des zones faisant face à l'intranet).

  Le pare-feu consomme plus de ressources pour suivre les compteurs de **src-dest-ip-both** que pour suivre uniquement les compteurs source IP ou destination IP.

  *Pour utiliser la table de blocage du matériel sur les plateformes qui la prennent en charge, vous devez utiliser **source-ip-only** ou **src-dest-ip-both**. **Destination-ip-only** utilise le tableau des logiciels.*

STEP 3 | Activez la protection de la mémoire tampon des paquets de manière globale pour protéger les mémoires tampons des pare-feu des attaques DoS sur une session unique, des attaques provenant d'une adresse IP source unique et des adresses IP sources qui créent de nombreuses petites sessions qui se combinent pour consommer les mémoires tampons des paquets.

La protection générale de la mémoire tampon des paquets est la première phase d'une approche à deux phases pour protéger la mémoire tampon du pare-feu et elle est autorisée par défaut. (L'étape 4 montre

la deuxième phase, la protection de la mémoire tampon des paquets par zone, qui est également activée par défaut.) La protection générale de la mémoire tampon des paquets détecte les sessions individuelles ou les adresses IP sources qui menacent de consommer la mémoire tampon des paquets du pare-feu et applique RED à ces sessions ou paquets pour abandonner plus de paquets lorsque la congestion de la mémoire tampon augmente.

L'objectif de la protection de la mémoire tampon des paquets est d'empêcher les pare-feu d'entrer et de rester dans un état de latence élevée et d'utilisation élevée de la mémoire tampon en appliquant d'abord RED pour abandonner les paquets incriminés (protection globale), puis en supprimant la session incriminée ou en bloquant l'adresse IP source incriminée (blocage de session ou d'hôte) si l'attaque continue (protection par zone). L'idée est de protéger les mémoires tampons des paquets aux niveaux logiciel et matériel et en même temps d'avoir une latence et une perte de paquets faibles, et de rejeter ou de bloquer le trafic incriminé au bon moment.

La protection de la mémoire tampon des paquets protège également les mémoires tampons des pare-feu si un hôte envoie un grand volume de trafic que le pare-feu traite et refuse en série sans configurer de session. Ce trafic a généralement le même identifiant à 6 tuples (IP source et de destination, port source et de destination, protocole et zone d'entrée). Les ressources requises pour traiter chaque paquet puis le refuser consomment des ressources de pare-feu si vous n'activez pas la protection de la mémoire tampon des paquets.

Si la protection de la mémoire tampon des paquets par zone est activée et que la consommation de mémoire tampon atteint et maintient un niveau élevé pendant une durée configurable, le pare-feu supprime uniquement les sessions ou les hôtes incriminés. Si la protection de la mémoire tampon des paquets par zone est désactivée, le pare-feu exécute l'action RED, mais ne rejette ni ne bloque le trafic.

- Utilisez les mesures de référence d'utilisation de la mémoire tampon des paquets pour comprendre les capacités du pare-feu et pour vous assurer que celui-ci est correctement adapté, afin qu'une attaque seule ne puisse pas causer un pic soudain dans l'utilisation de la mémoire tampon. Comprendre l'utilisation de la mémoire tampon des paquets pendant le fonctionnement normal lors des pics d'utilisation et à quel moment les problèmes de latence ou de blocage surviennent. Si la capacité du pare-feu est assez faible pour que le trafic normal provoque des pics d'utilisation de la mémoire tampon, vous aurez peut-être besoin d'un pare-feu avec une plus grande capacité.

  Dans PAN-OS 10.0 et versions ultérieures, envisagez d'utiliser le mode **Moniteur seul** (**Device** > **Setup** > **Session** > **Session Settings**) pour comprendre l'utilisation de la mémoire tampon de vos paquets de base et identifier les sources agressives. En mode **Monitor Only (Surveiller uniquement)**, le pare-feu surveille l'utilisation de la mémoire tampon des paquets et les alertes sur les sessions et les sources incriminées, mais ne les bloque pas et ne les supprime pas. Le compromis est que vous pouvez expérimenter différents seuils d'**alerte** et **d'activation** et voir les résultats dans les journaux de menaces sans affecter le trafic, mais le pare-feu n'est pas protégé contre les attaques par tampon de paquets. Si vous pouvez reproduire le trafic de production dans un environnement hors production, vous pouvez expérimenter en toute sécurité les seuils **Alert (Alerte)** et **Activate (Activer)** pour voir quelles sessions sont pénalisées avec différents paramètres de seuil et quels seuils commencent à avoir un impact sur le trafic légitime.
- Configurez les seuils de la protection générale de la mémoire tampon des paquets (**Device** > **Setup** > **Session** > **Session Settings**) en fonction de l'utilisation de la mémoire tampon ou de la latence de traitement du processeur. La protection de la mémoire tampon des paquets basée sur la latence de

traitement du processeur répond plus rapidement aux pics de paquets importants et soudains que la protection de la mémoire tampon basée sur le pourcentage d'utilisation de la mémoire tampon.

La protection de la mémoire tampon des paquets basée sur le pourcentage d'utilisation du tampon est activée par défaut :

- **Alert (Alerte)** : commencez par la valeur par défaut (50 %), surveillez l'utilisation de la mémoire tampon des paquets, et ajustez les seuils si nécessaire.
- **Activate (Activer)** : Le seuil **Activate (Activer)** par défaut est de 80 % dans PAN-OS 10.0 et versions ultérieures et de 50 % dans PAN-OS 9.1 et versions antérieures. Au lieu d'utiliser les valeurs par défaut, il est plus sûr de définir le seuil d'activation à 10-20 % au-dessus de votre utilisation de référence, puis de surveiller l'utilisation de la mémoire tampon des paquets. Ajustez le seuil jusqu'à ce que la protection de la mémoire tampon des paquets s'active à temps pour pénaliser les sessions incriminées, mais ne pénalise pas l'utilisation normale.

  Le bon réglage d'**Activate (Activer)** dépend de votre environnement et des ressources de traitement disponibles, c'est pourquoi il est généralement nécessaire d'expérimenter. Plus le seuil **Activate (Activer)** est bas, plus le trafic légitime est bloqué, mais l'atténuation des attaques commence plus tôt. Plus le seuil est élevé, plus il faut de temps pour commencer à atténuer une attaque, mais moins il est probable que le trafic légitime soit affecté.

  Si le seuil d'activation est trop élevé pour l'environnement, vous subissez l'impact de la charge et/ou de la latence élevées sur le trafic légitime avant que la protection de la mémoire tampon des paquets ne s'active.

  Si le seuil d'activation est trop bas pour l'environnement, le pare-feu supprime inutilement trop de paquets légitimes alors même que des ressources sont disponibles pour gérer le trafic. (Cela peut également se produire s'il y a d'autres problèmes de réseau.)

  Si le seuil d'activation est à peu près adapté à l'environnement, très peu de trafic légitime est abandonné et les ressources du pare-feu ne sont pas sollicitées. Connaître la charge de référence de la mémoire tampon des paquets est essentiel pour ajuster correctement les seuils. Par exemple, si vous savez que pendant les pics d'utilisation, l'utilisation de la mémoire tampon des paquets peut atteindre 40 à 50 % de la capacité du pare-feu et que vous rencontrez des problèmes lorsque l'utilisation de la mémoire tampon des paquets atteint 60 à 70 %, alors définissez le seuil **Activate (Activer)** sur 55 à 60 %.

*Dans PAN-OS 10.0 et versions ultérieures, vous pouvez expérimenter le réglage des seuils **d'alerte** et d'**activation** et la visualisation des résultats en mode **Moniteur seul**. Le mode **Monitor Only (Surveiller uniquement)** ne prend aucune mesure contre le trafic incriminé mais vous donne une visibilité sur la façon dont les seuils affectent le trafic avant d'activer la protection de la mémoire tampon des paquets.*

Pour mesurer l'utilisation de la mémoire tampon des paquets, utilisez le Panorama Health Monitor (Moniteur de santé Panorama). En outre, les commandes opérationnelles CLI suivantes sont utiles :

- La commande **`> show running resource-monitor`** affiche les statistiques du processeur. L'option **`ingress-backlogs`** affiche les sessions qui consomment au moins 2 pour cent des descripteurs de paquets sur puce.

- Pour les sessions dans lesquelles la protection de la mémoire tampon des paquets protège activement le pare-feu, la commande **`> show session packet-buffer-protection`** affiche les sessions qui consomment le plus de ressources du processeur du plan de données.

La **Latency Based Activation** (Activation en fonction de la latence) de la protection de la mémoire tampon des paquets est désactivée par défaut. La protection basée sur la latence ne peut pas se défendre contre les attaques DoS où une source envoie constamment des paquets que le pare-feu refuse, ce qui consomme des ressources, mais n'est pas considéré comme une latence, car le pare-feu ne configure jamais de session pour le trafic refusé. (Cependant, la protection de la mémoire tampon des paquets basée sur l'utilisation de la mémoire tampon empêche ces types d'attaques.)

Latency Based Activation (Activation basée sur la latence) atténue la consommation élevée de descripteurs sur puce lorsque l'utilisation de la mémoire tampon des paquets n'est pas encore élevée et constitue la meilleure méthode lorsque vous voulez que le pare-feu réagisse avant que les mémoires tampons des paquets ne soient épuisées.

Sélectionnez **Latency Based Activation** (Activation en fonction de la latence) pour baser la protection sur la latence de traitement du processeur plutôt que sur un pourcentage de l'utilisation de la mémoire tampon. Les trois paramètres suivants remplacent les paramètres **Alert (Alerte)** et **Active (Actif)** basés sur l'utilisation :

- **Latency Alert (Alerte de latence)** : commencez par la valeur par défaut (50 millisecondes), surveillez la latence et ajustez les seuils si nécessaire.
- **Latency Activate (Activation de la latence)** : commencez par la valeur par défaut (200 millisecondes), surveillez la latence et ajustez les seuils si nécessaire.
- **Latency Max Tolerance (Tolérance maximale de latence)** : commencez par les valeurs par défaut (500 millisecondes), surveillez la latence et ajustez les seuils si nécessaire. Lorsque le trafic atteint le seuil **Latency Activate** (Activation de la latence), le pare-feu utilise RED pour commencer à bloquer le trafic et augmente le taux de blocage jusqu'à ce que la latence atteigne la **Latency Max Tolerance** (Tolérance maximale de latence). Lorsque la **Latency Max Tolerance** (Tolérance maximale de latence) est atteinte, la probabilité de taux d'abandon est proche de 100 %.

Mesurez la latence sur chaque pare-feu :

- *commande opérationnelle* ***`fw-1> debug dataplane pow performance | match pbp`***.
- *Activez la journalisation lorsque la charge du plan de données est élevée pour recevoir des notifications et afficher les informations du journal (**Device** > **Setup** > **Management** > **Logging and Reporting** et **Enable Log on High DP Load** [Activer la journalisation de la charge DP]). Vérifiez la charge du plan de données à l'aide de la commande CLI opérationnelle* ***`show running resource monitor`***. *Vous pouvez également créer un fichier de support technique et consulter le journal du plan de données au format texte.*

- Définissez des seuils et des minuteurs (**Device** > **Setup** > **Session** > **Session Settings**) pour définir quand supprimer une session incriminée ou bloquer une adresse IP source incriminée. Le pare-feu n'utilise ces seuils et minuteurs que si vous activez la protection de la mémoire tampon des paquets

par zone. Si seule la protection globale de la mémoire tampon des paquets est activée, le pare-feu exécute RED sur le trafic, mais ne le rejette ni ne le bloque.

Basez les paramètres sur les expériences et les mesures de la latence et de l'utilisation de la mémoire tampon, votre tolérance à la latence et à la perte de paquets en raison de la congestion de la mémoire tampon, ainsi que sur le degré d'agressivité avec lequel vous souhaitez abandonner le trafic pour éviter une latence et une consommation de la mémoire tampon des paquets qui ont un impact sur le réseau et ses utilisateurs.

- **Block Countdown Threshold (Seuil de compte à rebours de blocage)** : le pourcentage d'utilisation de la mémoire tampon ou le seuil de latence en millisecondes qui démarre le compte à rebours pour supprimer ou bloquer le trafic incriminé. Lorsque la congestion ou la latence de la mémoire tampon atteint le **Block Countdown Threshold** (Seuil de compte à rebours de blocage), le **Block Hold Time** (Délai d'attente du blocage) commence à décrémenter. (Lorsque le temps de blocage est écoulé, le pare-feu supprime les sessions ou bloque les hôtes incriminés.)

  Définissez le **Block Countdown Threshold** (Seuil de compte à rebours de blocage) à 10 % en dessous du seuil **Activate**(Activer) ou **Latency Activate** (Activation de la latence), surveillez l'utilisation de la mémoire tampon des paquets et ajustez la valeur si nécessaire. Cette méthode bloque les adresses IP incriminées et supprime les sessions plus rapidement que le paramètre par défaut (80 % ou 500 ms pour la latence). Plus la valeur **Block Hold Time (Délai de maintien du blocage)** est faible, plus tôt le pare-feu commence à atténuer la congestion de la mémoire tampon en supprimant la session ou en bloquant l'IP source incriminée. Plus la valeur est élevée, plus une attaque peut durer longtemps avant que le pare-feu ne l'atténue.

- **Block Hold Time** (Délai d'attente du blocage) : la durée pendant laquelle la session incriminée peut rester au-dessus du **Block Countdown Threshold** (Seuil de compte à rebours de blocage) avant que le pare-feu ne supprime la session ou ne bloque l'adresse IP source. Plus la valeur est faible, plus tôt le pare-feu active la protection de la mémoire tampon des paquets et exploite la table de blocage du matériel et/ou la table de blocage du logiciel (toutes deux sur les systèmes qui ont une table de blocage du matériel) pour protéger les mémoires tampons des paquets.

  Commencez par une valeur de 30 secondes, surveillez l'utilisation de la mémoire tampon des paquets et ajustez le délai si nécessaire. Cette méthode bloque les adresses IP incriminées plus rapidement que le paramètre par défaut (60 secondes). Plus la valeur du temps est élevée, plus une attaque peut durer longtemps avant que le pare-feu ne l'atténue.

  Le délai d'attente du blocage décrémente tant que la congestion reste au-dessus de la valeur du **Block Countdown Threshold** (Seuil de compte à rebours de blocage). Lorsque le **Block Hold Time** (Délai d'attente du blocage) atteint 0, le pare-feu supprime la session ou bloque l'adresse IP source.

- **Block Duration (Durée du blocage)** : la durée après l'expiration du **Block Hold Time** (Délai d'attente du blocage) pendant laquelle l'adresse IP source est mise en quarantaine (bloquée). Commencez par la valeur par défaut (3 600 secondes) ou réduisez la valeur si le blocage d'une adresse IP source pendant une heure représente une pénalité trop importante pour les conditions de votre entreprise. Surveillez l'utilisation du tampon du paquet, et ajustez la valeur si nécessaire.

La façon dont vous définissez les seuils de mémoire tampon des paquets dépend de votre trafic réseau et de la manière dont vous souhaitez traiter ce trafic :

- Les paramètres par défaut sont prudents et permettent de prolonger la congestion de la mémoire tampon des paquets avant de supprimer des sessions ou de bloquer des adresses IP source pour éviter de pénaliser le trafic légitime. Le pare-feu ne bloque pas les sessions et les sources potentiellement légitimes aussi rapidement pendant les périodes de congestion, mais au prix

potentiel de ralentir les sessions légitimes qui ne provoquent pas de congestion de la mémoire tampon des paquets. C'est pourquoi la meilleure pratique consiste à commencer avec des seuils plus bas et plus agressifs.

- Les plaintes des utilisateurs concernant la lenteur du réseau peuvent indiquer que les seuils de mémoire tampon des paquets sont trop prudents. Pour répondre à ces plaintes, réduisez le taux **Activate** (Activer) et le **Block Countdown Threshold** (Seuil de compte à rebours de blocage) pour démarrer l'abandon de paquets avec l'action RED plus tôt. Réduisez le **Block Hold Time** (Délai d'attente du blocage) afin que le pare-feu commence à bloquer les adresses IP ou à supprimer les sessions plus rapidement une fois que le taux de consommation de la mémoire tampon atteint le **Block Countdown Threshold** (Seuil de compte à rebours de blocage).

  La suppression ou le blocage plus rapide du trafic incriminé signifie que le trafic légitime qui ne cause pas de problèmes de consommation de mémoire tampon des paquets ne subira pas de problèmes de latence ou de perte de paquets en raison du trafic incriminé, mais le trafic incriminé est mis en quarantaine. Cependant, une session légitime ou une adresse IP source qui envoie un volume de trafic important pourrait également être mise en quarantaine plus rapidement.
- Si vous craignez que la configuration d'un taux **Activate** (Activer) et d'un **Block Countdown Threshold** (Seuil de compte à rebours de blocage) inférieurs puisse bloquer un trafic légitime important, comme le DNS ou un autre trafic d'infrastructure critique, augmentez le **Block Hold Time** (Délai d'attente du blocage) à une valeur supérieure pour retarder l'action de mise en quarantaine et surveiller l'utilisation de la mémoire tampon des paquets.
- Ajustez les seuils de protection de la mémoire tampon des paquets pour obtenir un équilibre entre la latence et la perte de paquets et quand supprimer les sessions ou bloquer les adresses IP sources qui a du sens pour votre réseau.

STEP 4 | La deuxième phase de la protection de la mémoire tampon des paquets protège les mémoires tampons des pare-feu sur une base par zone d'entrée. Elle est activée par défaut dans PAN-OS 10.0 et versions ultérieures (désactivée par défaut dans PAN-OS 9.1 et versions antérieures), mais la protection globale de la mémoire tampon des paquets doit également être activée pour que la protection de la mémoire tampon des paquets par zone fonctionne. La protection de la mémoire tampon des paquets par zone supprime les sessions incriminées et bloque les adresses IP source incriminées. Il s'agit

d'une meilleure pratique lorsque vous avez besoin d'une couche de protection supplémentaire pour des zones d'entrée en particulier.

Désactivez la protection de la mémoire tampon des paquets par zone lorsque vous ne souhaitez pas bloquer les adresses IP source ou supprimer les sessions pour une zone en particulier (par défaut, le pare-feu applique également l'action RED globalement afin que les mémoires tampons des paquets disposent toujours d'une couche de protection principale). Bloquer une adresse IP source bloque l'ensemble du trafic provenant de cette adresse, pas seulement la session incriminée. Si l'adresse IP source est un périphérique NAT, cela pourrait générer d'importants flux d'utilisateurs derrière le périphérique NAT.

- Pour désactiver ou activer la protection par zone, **Network** > **Zones**, sélectionnez une zone existante ou **Add** [Ajouter] pour ajouter une zone, puis sélectionnez ou désélectionnez **Enable Packet Buffer Protection** (Activer la protection de la mémoire tampon des paquets).

Lorsque vous envisagez d'activer ou de désactiver la protection de la mémoire tampon des paquets par zone, ne pensez pas seulement aux zones vulnérables aux attaques de l'extérieur, pensez également au réseau interne. Tenez compte des menaces internes potentielles, des périphériques internes accidentellement mal configurés, des adaptateurs de carte réseau défectueux qui génèrent un volume important de trafic illégitime et d'une mauvaise configuration du pare-feu.

Tous ces éléments peuvent refuser le trafic provenant de toute source légitime qui envoie également un volume important de trafic au pare-feu, car le pare-feu identifie toutes les sources de trafic importantes par leurs identifiants uniques à 6 tuples (IP source et de destination, port source et de destination, protocole et zone d'entrée). Pendant les périodes de congestion de la mémoire tampon des paquets, l'action RED affecte les sources légitimes qui envoient un volume important de trafic avec les sources incriminées.

STEP 5 | Associez le profil de Protection contre les Vulnérabilités respectant les meilleures pratiques à toutes les règles d'autorisation de politique de sécurité.

La combinaison de protection DDoS haut volume au niveau du périmètre, de profils de Protection de Zones, de règles de politiques ainsi que de profils de Protection DoS, de Protection du Tampon du Paquet, et de Protection contre les Vulnérabilités pour du trafic autorisé fournit plusieurs couches de protection DoS à votre réseau et ses ressources les plus précieuses.

Meilleures pratiques concernant le suivi du déploiement de la protection DoS et de la protection de zones

Après avoir déployé une protection de zones et une protection DoS, veillez au bon fonctionnement et prenez des mesures pour garantir une bonne continuation au fur et à mesure que votre réseau évolue.

STEP 1 | Évaluez les performances du pare-feu pour vous assurer qu'il réponde à des normes acceptables ainsi que pour mesurer les effets de la protection de zone et de la protection DoS sur les ressources du pare-feu.

Si les niveaux de la protection de zone et de la protection DoS (ainsi que d'autres fonctions gourmandes en ressources comme le décryptage) consomment trop de ressources du pare-feu, la meilleure pratique est d'augmenter les ressources plutôt que compromettre la sécurité.

STEP 2 | Configurez le transfert des journaux.

Pour un entretien simplifié, utilisez des profils de transferts de journaux séparés, et transférez les journaux des événements de seuils séparément des journaux d'autres menaces. Envoyez les journaux de DoS et de zones directement aux administrateurs concernés par messagerie ainsi que sur un serveur de journaux, afin que les notifications ne contiennent que des événements relatifs aux attaques DoS potentielles. Configurez le transfert de journaux des événements DoS dans la règle de politique de Protection DoS (**Policies** > **DoS Protection [Protection DoS]**) et configurez le transfert de journaux des événements de Zone dans chaque zone (**Network [Réseau]** > **Zones**).

Fixez le seuil du **Alarm Rate (Taux de Déclenchement d'Alarme)** dans le journal d'événements à gravité basse ou gravité informationnelle. Fixez les seuils d'**Activate (Activation)**, de **Maximum**, ainsi que du**Activate Rate (Taux d'Activation)** et du **Max Rate (Taux Maximal)** de la protection de zone dans le journal d'événements à gravité critique. Après avoir correctement fixé les seuils de saturation, les journaux vous montrent les attaques de type flood potentielles sur le réseau, car vous ne voyez que les menaces et les événements inhabituels. Si vous voyez trop de fausses alertes, cela signifie que les seuils fixés sont trop bas et que le pare-feu n'est pas correctement adapté à la taille du trafic pris en charge.

Le pare-feu prend des journaux cumulés toutes les 10 secondes afin de maintenir un volume de journaux raisonnable, d'éviter de submerger les serveurs de journaux, et de préserver les ressources du pare-feu.

STEP 3 | Surveillez et examinez d'autres indicateurs d'attaques DoS.

En plus de configurer le transfert de journaux pour notifier les administrateurs quand les seuils de saturation sont franchis, vérifiez les indicateurs d'attaques et examinez les attaques DoS potentielles :

- Analysez l'activité de menace relative aux attaques DoS (**ACC** > **Threat Activity (Activité de Menace)**) et cherchez des signes de violations.
- Sur les modèles de pare-feu la prenant en charge (PA-3050, PA-3060, PA-3200 Series, PA-5200 Series et PA-7000 Series), procédez à la Surveillance d'adresses IP bloquées (**Monitor (Surveillance)** > **Block IP List (Liste d'IP bloquées)**) pour obtenir les adresses IP bloquées par

le pare-feu en raison d'un risque d'attaque DoS. La colonne **Block Source (Source du Blocage)** identifie le nom du profil de Protection DoS classé ayant bloqué l'adresse IP.

- Une interruption totale ou partielle de trafic sur le pare-feu, une navigation web lente ou une connectivité lente sur un terminal, ou encore l'échec de nouvelles sessions, tous peuvent être les signes d'une attaque DoS. Une utilisation élevée du processeur, l'épuisement du tampon du paquet ou du descripteur du paquet ainsi qu'un pic dans le nombre de sessions actives peuvent également être les signes d'une attaque DoS.
- Pour en savoir plus sur la surveillance de l'activité DoS, consultez la section Journaux d'événements de la protection DoS et de la protection de Zone et Compteurs Globaux.

Les dépassements de seuil de saturation peuvent indiquer une attaque DoS, mais ils peuvent également indiquer des valeurs de CPS mal configurées, une mauvaise configuration d'un autre périphérique interne, des adaptateurs de carte réseau défectueux, des menaces internes potentielles ou un dimensionnement incorrect du pare-feu.

STEP 4 | Les modèles de trafic réseau changent avec le temps, de nouveaux périphériques sont ajoutés tandis que d'anciens périphériques sont retirés, et des événements spéciaux peuvent affecter les modèles de trafic de manière temporaire.

Pour toutes ces raisons, réalisez des Mesures CPS régulièrement et revoyez les réglages des seuils de saturation DoS et de zone ; comme les réseaux sont en évolution constante, la protection DoS et la protection de zone requièrent une approche itérative.