paloalto TECHDOCS

Prácticas recomendadas de protección DoS y de zonas

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

October 6, 2023

Table of Contents

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Prácticas recomendadas de protección DoS y de zonas

Esta lista de comprobación de pasos previos a la implementación, implementación y pasos posteriores a la implementación le ayuda a implementar las prácticas recomendadas de denegación de servicio (DoS) y protección de zona. Los enlaces a la Guía del administrador de PAN-OS proporcionan detalles de configuración.

Un **ataque de denegación de servicio (DoS)** es una fuente única que congestiona un servidor de destino. Un **Ataque de denegación de servicio distribuido (DDoS)** es varias fuentes que congestionan un único servidor de destino. Los ataques DDoS intentan iniciar más sesiones que los ataques DoS y requieren más recursos para defenderse. Dado a que los cortafuegos se basan en sesiones, son una parte de una estrategia de defensa DoS/DDoS por niveles, no la única defensa.

Los ataques DoS hacen que un dispositivo o recurso no esté disponible para los usuarios legítimos y provienen de Internet o de dispositivos internos mal configurados o comprometidos. El método típico es congestionar el objetivo con solicitudes que consumen sus recursos (memoria, ciclos de CPU y ancho de banda) para que el objetivo no esté disponible para los usuarios legítimos. Los objetivos típicos son dispositivos que se conectan a internet a los que los usuarios acceden de forma externa desde la red corporativa, como servidores web y de base de datos. Los cortafuegos de Palo Alto Networks brindan tres herramientas de mitigación como parte de un enfoque por niveles a la protección DoS.

Los Zone Protection Profiles (Perfiles de protección de zonas) protegen las zonas de entrada individuales según la cantidad de sesiones nuevas que entran a una zona. Limitan las conexiones por segundo (CPS) al cortafuegos para una amplia protección frente a ataques de congestión y protegen frente al reconocimiento (escaneos de puertos y barridos de host), ataques basados en paquetes y ataques basados en protocolo de capa 2.

Los perfiles de protección DoS y las reglas de políticas protegen los dispositivos críticos frente a nuevas congestiones de sesiones. Las políticas clasificadas protegen dispositivos individuales. Las políticas agregadas protegen grupos de dispositivos.

Un beneficio importante de la protección DoS clasificada es colocar automáticamente las direcciones IP de origen que exceden la tasa máxima de CPS en la lista de bloqueo de hardware (ahorra recursos de software en las plataformas que lo admiten) o la lista de bloqueo de software, según la **Max Rate (Tasa máxima)**del perfil de protección DoS. Si la tabla de bloqueos de hardware se llena, el cortafuegos utiliza la tabla de bloqueos de software.

La Protección DoS gestiona la mayoría de los ataques dirigidos a servidores individuales y la Protección de zona protege ampliamente toda la zona si la protección DoS no es suficiente. La protección DoS aprovecha las tablas de bloques, por lo que consume menos recursos que la protección de zona.

Protección de búfer de paquetes: brinda protección frente a los ataques DoS de sesión única de las sesiones existentes que intentan sobrecargar el búfer de paquetes del cortafuegos. La protección de búfer de paquetes pone en cuarentena las direcciones IP atacantes en la tabla de hardware si la plataforma lo admite.

La serie de libros de prácticas recomendadas de Palo Alto Networks ofrece consejos sobre prácticas recomendadas en temas como el descifrado, la protección del acceso administrado y mucho más.

©2024 Palo Alto Networks, Inc.

Planificación de implementación de prácticas recomendadas de protección DoS y de zonas

Esta sección analiza las prácticas recomendadas de lo que necesita saber y planificar antes de implementar la protección DoS y de zona, incluidos:

- Diferentes tipos de ataques DoS para los que prepararse.
- Cómo aumentar sus defensas usando múltiples mecanismos de prevención.
- Dónde colocar sus cortafuegos.
- Cómo comprender el promedio de conexiones por segundo (CPS) normales y máximas de referencia de las zonas y los dispositivos críticos que desea proteger y su efecto en el consumo de la CPU.
- Cómo comprender la capacidad de los recursos de su cortafuegos con todas las demás funciones que consumen recursos ejecutándose.

Si su plataforma es compatible con una tabla de bloqueos de hardware, planifique usar la protección DoS clasificada tanto como sea posible para proteger servidores individuales críticos. La protección DoS clasificada aprovecha la tabla de bloqueos de hardware para almacenar direcciones IP bloqueadas, lo que ahorra recursos de software del sistema y mejora el rendimiento. Estas plataformas admiten la tabla de bloqueos de hardware:

- *Cortafuegos de PA-3200 Series*
- *Solo cortafuegos PA-5200 Series*
- *Cortafuegos PA-5400 Series*
- *Cortafuegos PA-7000 Series*

Para usar la tabla de bloqueos de hardware para la protección DoS, además del soporte de la plataforma:

- *La **Action (Acción)** de la política de protección DoS debe ser **Protect (Proteger)**.*
- *El perfil de Protección de DoS debe ser un perfil clasificado.*
- *Debes usar RED como mecanismo de descarte.*
- *Debe usar **source-ip-only** o **src-dest-ip-both** como la **Address (Dirección)** clasificada en la política de protección DoS.*

©2024 Palo Alto Networks, Inc.

STEP 1 | Planifique su defensa contra cada tipo de ataque DoS.

- **Ataques basados en aplicaciones:** aborde las debilidades de una aplicación determinada e intente agotar sus recursos para los usuarios legítimos no puedan usarla. Un ejemplo de ello es el ataque Slowloris.
- **Ataques basados en protocolos**: también denominados como ataques de agotamiento de estado, estos ataques apuntan a los puntos débiles del protocolo. Un ejemplo común es un ataque de congestión de SYN.
- **Ataques volumétricos**: ataques de gran volumen que pretenden sobrecargar los recursos de red disponibles, especialmente el ancho de banda, y derribar el objetivo para evitar que los usuarios legítimos accedan a sus recursos. Un ejemplo de ello es un ataque de congestión de UDP. Estos ataques pueden originarse en una única IP de origen (ataque DoS) o en muchas IP de origen (ataque DDoS; las direcciones IP de origen pueden rotar y el ataque puede tener una alta tasa de CPS y/o un gran volumen de tráfico).

STEP 2 | Planifique un enfoque por capas para evitar ataques DoS.

El cortafuegos brinda la visibilidad del tráfico de aplicación que los dispositivos dedicados de protección DoS no proporcionan. Combine la protección DDoS de alto volumen en el perímetro de la red con capas de protección DoS para dispositivos individuales y protección de zona para toda la zona según sea necesario para defender su red y dispositivos individuales críticos frente a ataques DoS:

- ❑ Use un dispositivo dedicado de protección DDoS de gran volumen o un enrutador de perímetro, conmutador u otro dispositivo de descarte de paquetes basado en hardware con las listas de control de acceso (ACL) apropiadas como la primera capa de defensa en el perímetro de red accesible desde Internet. Coloque los dispositivos DDoS dedicados de alto volumen frente a los cortafuegos perimetrales para defenderlos frente a ataques de alto volumen, que el cortafuegos basado en sesiones no está diseñado para gestionar.
- ❑ Aplique Perfiles de protección de zona como una capa de protección amplia y agregada para proteger zonas individuales de ataques de congestión y para aumentar el dispositivo DDoS dedicado en el perímetro.
- ❑ Aplique la Protección de búfer de paquetes para evitar que los ataques DoS consuman recursos del búfer de paquetes del cortafuegos.
- ❑ Aplique perfiles clasificados y políticas de protección DoS para proteger objetivos de alto valor individuales o en pequeños grupos (perfiles y reglas de la política de Protección DoS):
  - Proteja los servidores críticos con acceso a internet limitando el CPS a cada servidor.
  - Evite que hosts internos comprometidos o configurados incorrectamente transmitan un ataque DoS limitando las CPS desde el origen sospechoso (solo zonas con acceso interno, no zonas accesibles desde Internet) o hacia el destino afectado.
  - Supervise un origen determinado (solo zonas con acceso interno) y alertarlo si las CPS de ese origen alcanzan un determinado umbral, que puede indicar un host comprometido o configurado de manera incorrecta.
  - Defiende dispositivos específicos dentro de una zona si el cortafuegos admite el uso de la tabla de bloqueos de hardware.
  - Obtenga visibilidad de las direcciones IP asociadas con el ataque en los logs, independientemente de si el cortafuegos admite el uso de la tabla de bloqueos de hardware o la tabla de bloqueos de software.

 ©2024 Palo Alto Networks, Inc.

- Los perfiles y las políticas agregados de protección DoS brindan otra capa adicional de protección amplia para grupos de servidores críticos, si es necesario. En la mayoría de los casos, la protección DoS clasificada para servidores críticos individuales y la protección de zona para toda la zona son suficientes, y evitan la complejidad de la configuración. Además, los logs de protección DoS agregados no muestran las direcciones IP asociadas con un ataque y las políticas no aprovechan la tabla de bloqueos de hardware. Para obtener visibilidad de las direcciones IP atacantes, utilice la protección DoS clasificada.

  La protección DoS agregada se diferencia de la protección de zona en que la protección de zona defiende una zona completa de los ataques, mientras que la protección DoS agregada protege un pequeño grupo de dispositivos críticos dentro de una zona. La protección DoS agregada se diferencia de la protección DoS clasificada en que la protección DoS clasificada establece un umbral de CPS para cada dispositivo individual, mientras que la protección DoS agregada establece un umbral de CPS para un grupo de dispositivos.

Obtenga más información sobre las diferencias entre la protección DoS clasificada y agregada para ayudar a comprender cuál usar en diferentes situaciones.

Planificación de umbrales para utilizar Protección de zona y Protección DoS juntos: si su plataforma admite una tabla de bloqueos de hardware, planifique establecer umbrales clasificados de protección DoS más bajos que los umbrales de protección de zona para que la protección DoS se active primero y la Protección de zona proporcione una capa adicional de defensa, si es necesario. Si desea maximizar la protección para un grupo de dispositivos críticos, por ejemplo, servidores web o servidores de archivos con acceso a Internet, agregue protección DoS agregada con umbrales establecidos más altos que los umbrales de protección DoS clasificados, y más bajos que los umbrales de protección de zona. (Esto hace que la protección DoS clasificada se active primero, la protección DoS agregada se active en segundo lugar y la protección de zona se active en tercer lugar, si es necesario).

Si su plataforma no admite una tabla de bloqueos de hardware, se aplica la misma metodología, pero no obtiene el beneficio adicional de descargar en la tabla de bloqueos de hardware.

STEP 3 | Coloque el cortafuegos lo más cerca posible de los recursos que protegen.

Los cortafuegos no escalan a millones de CPS porque están basados en sesiones. Cuanto más cerca coloque los cortafuegos de los recursos que está protegiendo, menos sesiones y recursos de cortafuegos consumirá el tráfico.

- Coloque los cortafuegos perimetrales *detrás* de dispositivos DDoS perimetrales dedicados de alta capacidad o enrutadores o conmutadores perimetrales que usan ACL para descartar el tráfico DoS. Esto protege los cortafuegos que segmentan la red empresarial en zonas y protegen los dispositivos en dichas zonas. Cuanto más cerca esté el cortafuegos del perímetro, mayor deberá ser su capacidad para gestionar el mayor volumen de tráfico.
- Examine su segmentación de la zona de red. Si no es lo suficientemente detallada, considere crear zonas más pequeñas. Las zonas más pequeñas aumentan la seguridad de muchas maneras, lo que incluye una mejor prevención del movimiento lateral del software malintencionado, una mayor visibilidad del tráfico y un alcance de potencial reducido de los ataques DoS internos.

STEP 4 | Tome mediciones de referencia de las CPS máxima y promedio de los dispositivos y zonas que desea proteger, y comprenda la capacidad de sus cortafuegos; de modo que los umbrales de congestión

 ©2024 Palo Alto Networks, Inc.

no limiten el tráfico ni permitan ataques DoS de manera inadvertida. Mida la CPS con otras funciones que consumen recursos normales, como el descifrado, el filtrado de URL y GlobalProtect ejecutándose durante las horas pico y normales de tráfico.

- Para los umbrales del perfil de protección de zona, si ejecuta PAN-OS 10.0 o posterior, use las alertas de recomendación de umbral del perfil de protección de zona del servicio en la nube de AIOps, que utiliza la telemetría del sistema para proporcionar estimaciones precisas de los valores de CPS pico promedio y promedio. Dé de alta cortafuegos y Panorama para el servicio. (Con PAN-OS 10.2.1 o posterior, puede instalar el complemento AIOps para Panorama para hacer cumplir de manera proactiva los controles de seguridad en las configuraciones antes de enviarlas a los cortafuegos gestionados).

  Si no puede utilizar AIOps, use el ACC del cortafuegos y otras herramientas para tomar medidas de CPS de referencia para cada zona de cortafuegos durante al menos una semana laboral, durante el horario comercial. Cuanto mayor sea el período de recopilación de datos, más precisas serán las mediciones. Mida el CPS normal y máxima para cada zona individual para establecer los umbrales de congestión de protección de zona adecuados para cada zona.
- Para la protección DoS, tome mediciones de referencia de las CPS pico y promedio de los dispositivos críticos (objetivos potenciales). Utilice las mismas herramientas para examinar la utilización del búfer.
  - Lleve a cabo mediciones CPS de referencia para dispositivos críticos accesibles desde Internet durante el horario comercial de al menos una semana hábil. Cuanto mayor sea el período de recopilación de datos, más precisas serán las mediciones.
  - Trabaje junto a los equipos de aplicación para comprender las CPS pico y normales a sus servidores y las CPS máximas que estos servidores pueden admitir.
  - Filtre los logs de amenazas y los de tráfico del cortafuegos de las direcciones IP de destino de los dispositivos críticos para obtener una referencia de la actividad de sesión pico y normal.
  - Tenga en cuenta los eventos especiales, trimestrales y anuales que pueden aumentar el tráfico, modificar los patrones de tráfico o usar aplicaciones que generalmente no se encuentran en la red.

  Comprender el pico de CPS normal de las zonas y los dispositivos individuales es crucial para establecer valores de umbral adecuados en los perfiles de protección de zona y protección DoS. Si es demasiado agresivo (establezca umbrales demasiado bajos y permita muy pocos CPS), puede limitar el tráfico legítimo sin darse cuenta durante los picos de actividad. Si es demasiado pasivo (establezca umbrales demasiado altos y permite demasiados CPS), es posible que no sea suficiente protección para mitigar un ataque DoS y los recursos que intenta proteger pueden verse afectados.
- Comprenda la capacidad de sus cortafuegos y los recursos (CPU y memoria) que otras funciones consumen, de esta manera, conocerá la capacidad disponible para la protección DoS. Mida la CPS con otras funciones normales que consumen recursos que se ejecutan durante las horas de tráfico pico y normales.
  - Si utiliza Panorama para gestionar cortafuegos, use la supervisión de dispositivos para medir los valores de CPS. La supervisión de dispositivos también puede mostrarle una línea de tendencia

 ©2024 Palo Alto Networks, Inc.

de 90 días del uso pico y promedio del CPU para ayudarlo a comprender la capacidad típica disponible de cada cortafuegos.

Si no puede usar la supervisión de dispositivos en Panorama, puede utilizar las herramientas de gestión para sondear los siguientes tres MIB y recopilar datos de CPS históricas: PanZoneActiveTcpCps, PanZoneActiveUdpCps y PanZoneOtherIpCps.

Las MIB muestran el doble del valor real de CPS porque las MIB cuentan los segmentos de sesión C2S y S2C por separado en lugar de como una sola sesión. Por ejemplo, Si una MIB muestra un valor de CPS de 10.000, el valor CPS real es 5.000.

- Use herramientas de terceros como Wireshark o NetFlow para recopilar y analizar el tráfico de red.
- Considere usar secuencias de comandos para automatizar la supervisión continua y la recopilación de información de CPS, y extraer información de los logs.

STEP 5 | Configure un activador de reenvío de logs (criterios de coincidencia de tráfico) para hacer que un dispositivo ascendente, como un conmutador, un enrutador o un dispositivo DDoS dedicado, realice automáticamente un filtrado y bloqueo adicional cuando el cortafuegos esté bajo ataque y para proteger los recursos del cortafuegos.

Cuandoconfigura un activador de reenvío de logs y se producen las condiciones de activación, el cortafuegos envía automáticamente una llamada de API al dispositivo ascendente para tomar medidas contra el ataque.

Especifique el dispositivo o dispositivos ascendentes y la llamada de API (la acción que debe realizar el dispositivo o dispositivos ascendentes) en un perfil de servidor HTTP [**Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **HTTP**]. Especifique los dispositivos ascendentes en la pestaña **Servers (Servidores)** y especifique la llamada de API en el campo **Payload (Carga útil)** en la pestaña **Payload Format (Formato de carga útil)**.

Especifique las condiciones de coincidencia de tráfico que activan la llamada de API en un filtro de lista de coincidencias del perfil de reenvío de logs [**Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**].

- Para desencadenar un tipo de ataque en particular, utilice el Generador de filtro para crear un filtro que coincida con los logs de amenazas para el tráfico que desea filtrar o bloquear. Por ejemplo, el siguiente filtro especifica tres ID de amenazas que corresponden al Inicio de sesión de fuerza bruta de FTP, al Ataque de fuerza bruta de solicitud de HTTP y a los ID de amenazas de ataque DOS de fuerza bruta de Apache Benchmark:
  - `(threatid eq 40001) or (threatid eq 39290) or (threatid eq 35075)`

  La configuración del reenvío de logs para que se active en estas firmas de amenazas permite que el cortafuegos envíe la llamada de API que solicita a los dispositivos ascendentes especificados que filtren o bloqueen el tráfico infractor.
- Para proteger los recursos del cortafuegos de los ataques, especialmente en plataformas con tablas de bloqueos más pequeñas, use el generador de filtros en el perfil de reenvío de logs para crear un filtro que se active en condiciones de ataque DoS, para que el dispositivo ascendente bloquee el

 ©2024 Palo Alto Networks, Inc.

tráfico infractor en lugar de permitir que ese tráfico consuma los recursos de la lista de bloqueos del cortafuegos.

Verifique la capacidad del dispositivo ascendente para asegurarse de que pueda gestionar la carga de tráfico.

La configuración del reenvío de logs para que se active en condiciones de tráfico DoS permite que el cortafuegos envíe una llamada de API que solicite a los dispositivos ascendentes especificados que envíen el tráfico a una ruta nula y lo descarten silenciosamente, ahorrando así recursos de la tabla de bloqueos del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Implementación de protección DoS y de zonas con las prácticas recomendadas

La protección de zona y frente a los ataques por denegación de servicio ayudan a defender servidores críticos individuales (DoS Protection) y zonas (Zone Protection) frente a ataques de congestión basados en aplicaciones y protocolos. También proporcionan la siguiente capa de defensa frente a ataques volumétricos tras su dispositivo de prevención DDoS dedicado en el perímetro de Internet.

Mida las conexiones promedio y máximas por segundo (CPS) *para servidores y zonas críticas antes de comenzar la implementación, de modo que comprenda las CPS normales y máximas de referencia, y pueda establecer umbrales de inundación inteligentes.*

La implementación incluye:

- Crear perfiles de protección de zona
- Aplicar reglas y perfiles de políticas de protección DoS
- La habilitación de la protección global del búfer de paquetes
- La habilitación de la protección del búfer de paquetes por zona de ingreso
- Adjuntar perfiles de protección de vulnerabilidades de prácticas recomendadas a las reglas de permiso de la política de seguridad

STEP 1 | Creación de Zone Protection profiles (Perfiles de protección de zona) (**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)**) y su aplicación para defender cada zona.

Los perfiles de protección de zonas se aplican a las sesiones nuevas en las zonas de entrada y las protegen de ataques de congestión, reconocimiento (análisis de puertos y barridos de host), ataques basados en paquetes de IP y ataques de protocolo de capa 2.

- Establezca umbrales para **Alarm Rate (Tasa de alarma)**, **Activate (Activar)** y **Maximum (Máximo)** para descartar el tráfico para evitar que TCP SYN, UDP, ICMP, ICMPv6 y otras nuevas

 ©2024 Palo Alto Networks, Inc.

inundaciones de sesión IP afecten al cortafuegos. Establezca la **Action (Acción)** para inundaciones SYN.

Mida el consumo de CPU para garantizar que el cortafuegos pueda admitir la protección DoS y de zonas, y otras funciones que consumen ciclos de CPU, como el descifrado.

*Si tiene Panorama, use el Supervisor de estado [**Panorama** > **Managed Devices (Dispositivos gestionados)** > **Health (Estado)**] para verificar el consumo de CPU y memoria durante un período de tiempo especificado. Si no tiene Panorama, ejecute* `show running resource-monitor` *y especifique el plazo para medir el consumo de CPU. Si utiliza SNMP, puede extraer la información de su sistema de supervisión.*

Para inundaciones SYN de TCP, establezca la **Action (Acción)** en **Random Early Drop (Descarte aleatoria temprano)** o en **SYN Cookies** para controlar cómo el cortafuegos descarta sesiones cuando se superan los umbrales de inundación. Hay compensaciones entre los métodos:

- **SYN Cookies**: SYN Cookies descarta el tráfico cuando el protocolo de enlace SYN-ACK está mal. SYN Cookies no descarta el tráfico legítimo, solo el tráfico que viola los protocolos de enlace, por lo que es inherentemente más justo que RED porque solo elimina el tráfico incorrecto. SYN Cookies también es más fácil de implementar porque es más fácil establecer los umbrales de inundación. Sin embargo, SYN Cookies consume más recursos, por lo que cuando utilice SYN Cookies, supervise la CPU del cortafuegos y el uso de la memoria.
- **Random Early Drop (Descarte temprano aleatorio)** (RED): elimina el tráfico indiscriminadamente (no basado en amenazas, por lo que se elimina el tráfico malicioso y legítimo) en una curva de probabilidad basada en los umbrales de CPS **Activate (Activar)** y **Maximum (Máximo)** que establezca. Cuando CPS alcanza el umbral **Activate (Activar)**, el cortafuegos comienza a descartar sesiones. A medida que aumenta el número de sesiones, la tasa de descarte aumenta hasta que alcanza el umbral de sesión **Maximum (Máximo)**. Todas las sesiones nuevas por encima de la tasa de CPS máxima se eliminan hasta que la tasa de CPS cae por debajo del umbral máximo. Cuanto mayor es la diferencia entre los umbrales de CPS Activar y Máximo, más lenta es la probabilidad de descarte a medida que las sesiones aumentan del umbral **Activate (Activar)** al umbral **Maximum (Máximo)**.

Si elige SYN Cookies o RED es cuestión de recursos de cortafuegos disponibles, el número de sesiones que desea que soporte una zona y la agresividad con la que desea reducir el tráfico. Dado que SYN Cookies no afecta al tráfico legítimo y RED sí, es posible que prefiera comenzar con

 ©2024 Palo Alto Networks, Inc.

SYN Cookies, supervisar el uso de CPU y memoria, y cambiar a RED si SYN Cookies consume demasiados recursos del sistema.

Cuando establezca umbrales de protección de zona para SYN Cookies o RED, configúrelos lo suficientemente altos para permitir la carga normal y máxima de sesiones legítimas y lo suficientemente bajos para evitar congestiones. Dado que está protegiendo toda la zona, establezca umbrales de protección de zona superiores a los umbrales de protección DoS clasificados y ligeramente superiores a los umbrales de protección DoS agregados. Este método activa la protección DoS clasificada, en primer lugar, para objetivos críticos individuales; la protección DoS agregada (si se usa), en segundo lugar, para grupos de objetivos críticos y la protección de zona en tercer lugar.

SYN Cookies descarta el tráfico que presenta malos protocolos de enlace SYN. Los umbrales **Activate (Activar)** y **Maximum (Máximo)** determinan cuándo empezar a descartar protocolos de enlace SYN defectuosos (Activar) y cuándo dejar de aceptar tráfico SYN (Máximo). Umbrales de SYN cookies:

- **Alarm Rate (Tasa de alarma)**: configúrela por encima del 15 - 20 % de la tasa media de CPS de la zona para adaptarse a fluctuaciones normales.
- **Activate (Activar)**: Dado que SYN Cookies solo castigan el tráfico incorrecto, no el tráfico legítimo, active SYN Cookies inmediatamente (umbral 0 CPS, que es el valor predeterminado) para que no se permita el tráfico con un protocolo de enlace SYN incorrecto.
- **Maximum (Máximo)**: Dado que SYN Cookies solo castigan el tráfico incorrecto, establezca el Máximo en la capacidad máxima de CPS de la plataforma de cortafuegos, teniendo en cuenta otras características activas que requieren muchos recursos, para que no bloquee innecesariamente el tráfico SYN bueno debido a un umbral bajo. (Un Máximo inferior no descarta el tráfico incorrecto de forma más agresiva porque SYN Cookies descarta el tráfico incorrecto en el umbral Activar).

  Cuando SYN Cookies alcanza el umbral máximo, el cortafuegos bloquea todas las sesiones en la dirección de la congestión SYN durante 5 minutos. El tráfico en la otra dirección no se ve afectado. El tiempo de bloqueo de SYN Cookie no es configurable.

Umbrales de RED:

- **Alarm Rate (Tasa de alarma)**: configúrela por encima del 15 - 20 % de la tasa media de CPS de la zona para adaptarse a fluctuaciones normales.
- **Activate (Activar)**: establezca justo por encima de la tasa máxima de CPS normal de la zona para comenzar a descartar conexiones para mitigar congestiones (no comience a descartar el tráfico que está dentro de la actividad máxima normal), que generalmente está 15-20 % por encima de la **Alarm Rate (Tasa de alarma)**.
- **Maximum (Máximo)**: establece la tasa máxima en función de la utilización de CPU del cortafuegos. Si el uso de la CPU del cortafuegos es superior al 50 %, ajuste el CPS máximo al doble de la tasa de **Activate (Activar)**. Si el uso de la CPU del cortafuegos está por debajo del 50 %, ajuste el CPS máximo a tres veces la tasa **Activate (Activar)** y supervise el uso de la CPU. Si el uso de la CPU es demasiado alto, reduzca el máximo al doble de la tasa **Activate (Activar)**.

 ©2024 Palo Alto Networks, Inc.

Si se cruza el umbral, se bloquean las conexiones nuevas hasta que la tasa de CPS disminuye por debajo del umbral.

*Los cortafuegos con varios procesadores del plano de datos (dataplane processors, DP) distribuyen conexiones por los DP. En general, el cortafuegos divide la configuración del umbral de CPS equitativamente en sus DP. Por ejemplo, si un cortafuegos tiene cinco DP y configura la **Alarm Rate (Tasa de alarma)** en 20 000 CPS, cada DP tiene una **Alarm Rate (Tasa de alarma)** de 4000 CPS (20 000/5 = 4000), por lo tanto, si las sesiones nuevas en un DP superan el valor de 4000, se activa el umbral de la Alarm Rate (Tasa de alarma) de ese DP.*

***Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)** y filtre por **Log Type (Tipo de log)** `Flood (Congestión)` para ver las alarmas.*

- Supervise y ajuste los umbrales según sea necesario.

- Habilite la Protección de reconocimiento en todas las zonas para bloquear los barridos de host, diferentes tipos de análisis y otras actividades de reconocimiento. Conserve los valores predeterminados en **Threshold (Umbral)** para registrar algunos paquetes para el análisis antes de bloquear el funcionamiento del reconocimiento. Utilice **Source Address Exclusion (Exclusión de dirección de origen)** para permitir a grupos internos que realizan la prueba de vulnerabilidades de la red.
- Descarte paquetes sospechosos para evitar los ataques basados en paquetes.
  - **IP Drop (Descarte de IP)**: descarte los paquetes en **Unknown (Desconocido)** y **Malformed (Con formato incorrecto)**. Descarte **Strict Source Routing (Enrutamiento de fuente estricto)** y **Loose Source Routing (Enrutamiento de fuente no estricto)** porque el enrutamiento de fuente permite que los adversarios omitan las reglas de política de seguridad que usen la dirección IP de destino como criterio de coincidencia. Solo en las zonas internas, descarte **Spoofed IP address (Dirección IP duplicada)** para garantizar que en la entrada, la dirección de origen coincida con la tabla de enrutamiento del cortafuegos.
  - **TCP Drop (Descarte TCP)**: mantenga las selecciones predeterminadas de descarte **TCP SYN with Data (TCP SYN con datos)** y **TCP SYNACK with Data (TCP SYNACK con datos)**, seleccione **Mismatched overlapping TCP segment (Segmento de TCP superpuesto no coincidente)** y **Split Handshake (Protocolo de enlace dividido)**, y habilite la opción de franja **TCP Timestamp (Marca de tiempo TCP)**.

    *Si configura la inspección de contenido de túnel en una zona y habilita **Rematch Sessions (Volver a cotejar sesiones)**, solo para esa zona, deshabilite **Reject Non-SYN TCP (Rechazar TCP no sincronizados)** de modo que la habilitación o edición de una política de inspección de contenido de túnel no provoque que el cortafuegos descarte sesiones de túnel existentes.*
  - **ICMP Drop (Descarte de ICMP)**: lo que debe bloquear depende de cómo usa ICMP (o si realmente lo utiliza).
  - **IPv6 Drop (Descarte de IPv6)**: si se deben cumplir las normas, descarte paquetes con encabezados de enrutamiento, extensiones, etc. que no cumplen con las normativas.
  - **ICMPv6 Drop (Descarte de ICMPv6)**: si se deben cumplir las normas, descarte determinados paquetes que no coincidan con una regla de política de seguridad.

©2024 Palo Alto Networks, Inc.

- Habilite la protección de protocolo para rechazar protocolos que no usa en su red y evitar los ataques basados en protocolo de capa 2 en la capa 2 y las interfaces vwire.
  - Para las interfaces de vwire que se conectan a la internet pública a través de un dispositivo de capa 3 colocado frente al cortafuegos, habilite **Protocol Protection (Protección de protocolo)** en las zonas orientadas a internet.
  - Para las zonas de capa 2, habilite **Protocol Protection (Protección de protocolo)** en las zonas orientadas a Internet. En las zonas de capa 2 internas, habilite **Protocol Protection (Protección de protocolo)** y utilice la **Include List (Lista de inclusión)** para permitir solo los protocolos de capa 2 que utiliza y bloquear automáticamente todos los demás protocolos. (No utilice la **Exclude List (Lista de exclusión)**, que da acceso a todos los protocolos no incluidos en la lista). Si no configura la **Protocol Protection (Protección de protocolo)**, se permiten todos los protocolos de la capa 2.
- Adjunte un perfil en cada zona (**Network [Red]** > **Zones [Zonas+**) en el campo **Zone Protection Profile (Perfil de protección de zonas)**.

STEP 2 | Aplique la protección DoS a recursos de red específicos y críticos, en especial, sistemas a los que acceden los usuarios desde Internet que con frecuencia son el objetivo de los ataques, como servidores web y de base de datos.

La protección DoS proporciona una capa de defensa para proteger objetivos individuales críticos dentro de una zona. Establece umbrales de CPS de protección de zona para proteger toda una zona, que recibe una tasa de CPS agregada mucho mayor que la que pueden gestionar la mayoría de los dispositivos individuales. Un ataque dirigido a un único servidor crítico puede no tener una tasa de CPS lo suficientemente alta como para activar la protección de zona, razón por la cual configura la protección DoS para destinos críticos dentro de una zona. La protección DoS consiste en:

- Reglas de políticas de Protección DoS, que especifican los dispositivos, usuarios, zonas y servicios que definen el tráfico que desea proteger de los ataques DoS.
- Perfiles de protección DoS, que establecen umbrales de congestión para diferentes tipos de tráfico.

Añada un perfil de protección DoS a una regla de políticas de protección DoS. El perfil define los umbrales de CPS que el cortafuegos aplica al tráfico definido en la regla de políticas.

Configure perfiles de protección DoS clasificados y/o agregados y aplique uno o ambos a una regla de política de protección DoS (cada regla de política puede tener uno de cada tipo de perfil). Los perfiles *clasificados* establecen umbrales que se aplican a cada dispositivo individual especificado en una regla y aprovechan la tabla de bloqueos de hardware en plataformas que tienen uno. Los perfiles *agregados* establecen umbrales que se aplican al grupo combinado de dispositivos especificados en una regla (la tasa de CPS combinada del grupo debe superar el umbral para activar la protección DoS) y utilizan la tabla de software.

Al igual que la Protección de zona, puede establecer la **Action (Acción)** para SYN Cookies o para el Random Early Drop (Descarte aleatorio temprana) (RED) para controlar cómo el cortafuegos mitiga los ataques. También similar, cuál elegir depende de los recursos de cortafuegos disponibles, el número de sesiones que desea que admita una zona y la agresividad con la que desea descartar el tráfico. Supervise

 ©2024 Palo Alto Networks, Inc.

el uso de recursos del sistema y, si SYN Cookies consume demasiados recursos, cambie a RED. Siempre use RED si no tiene un dispositivo de prevención de DDoS dedicado delante del cortafuegos.

Cuando establezca umbrales de protección DoS, establezca los umbrales de protección DoS clasificados en lo más bajo para que se activen primero para proteger objetivos individuales críticos. Si utiliza la protección DoS agregada, establezca esos umbrales más altos que los umbrales de protección DoS clasificados y más bajos que los umbrales de protección de zona, de modo que la protección DoS agregada se active solo cuando la protección DoS clasificada no sea suficiente, pero antes de la protección de zona.

- Cree un Perfil de protección DoS [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **DoS Protection (Protección DoS)**] para cada dispositivo crítico o conjunto de dispositivos críticos que desee proteger. Configure SYN, UDP, ICMP, ICMPv6 y otros umbrales de congestión de IP y **Action (Acción)** para las congestiones SYN. Con frecuencia, los valores del umbral predeterminado no son apropiados porque cada red es diferente; configure los umbrales de acuerdo con la capacidad de los dispositivos que desea proteger.

  Mida el consumo de CPU del cortafuegos *para garantizar que el cortafuegos pueda admitir la protección DoS y de zonas, y otras funciones que consumen ciclos de CPU, como el descifrado.*

  Cuando configura SYN Cookies como la **Action (Acción)** para congestiones SYN:

  - **Alarm Rate (Tasa de alarma)**: en los perfiles clasificados, configúrela del 15 al 20 % por encima de la tasa de CPS promedio del dispositivo para tener en cuenta las fluctuaciones normales.

    Para los perfiles agregados, configure la tasa del 15 al 20 % por sobre la tasa de CPS promedio del grupo.
  - **Activate Rate (Tasa de activación)**: los perfiles clasificados aplican límites de CPS específicos a dispositivos individuales. Base los límites en la capacidad de los dispositivos individuales, para que no necesite acelerar CPS gradualmente y pueda establecer la **Activate Rate (Tasa de activación)** en el mismo umbral que la **Max Rate (Tasa máxima)**. Configure la **Activate Rate (Tasa de activación)** para que sea menor que la **Max Rate (Tasa máxima)** solo si desea comenzar a descartar tráfico antes de que llegue a la **Max Rate (Tasa máxima)**.

    Para los perfiles agregados, establezca el umbral justo por encima de la tasa de CPS máxima normal para el grupo para evitar la pérdida de tráfico que esté dentro de las expectativas de actividad normales. Esto es generalmente 15-20 % por encima de la **Alarm Rate (Tasa de alarma)**.
  - **Max Rate (Tasa máxima)**: para perfiles clasificados, establezca la **Max Rate (Tasa máxima)** en la capacidad máxima de los dispositivos que está protegiendo para que no se puedan congestionar pero puedan aceptar su carga de tráfico máxima.

    En los perfiles agregados, establezca el umbral en 80-90 % de la capacidad del grupo. Cuando las CPS lleguen al umbral, el cortafuegos descarta conexiones nuevas durante el período especificado en **Block Duration (Duración del bloqueo)**.
  - **Block Duration (Duración del bloqueo**: utilice el valor predeterminado (300 segundos) para bloquear la sesión del atacante sin penalizar sesiones legítimas del mismo origen durante demasiado tiempo.

 ©2024 Palo Alto Networks, Inc.

- Supervise y ajuste los umbrales según sea necesario.

Cuando configura RED como la **Action (Acción)**:

- **Alarm Rate (Tasa de alarma)**: en los perfiles clasificados, configúrela del 15 al 20 % por encima de la tasa de CPS promedio del dispositivo para tener en cuenta las fluctuaciones normales.

  Para los perfiles agregados, configure la tasa del 15 al 20 % por sobre la tasa de CPS promedio del grupo.
- **Activate Rate (Tasa de activación)**: para perfiles clasificados, establezca el umbral justo por encima de la tasa de CPS máxima normal objetivo para comenzar a descartar conexiones y mitigar ataques (no establezca umbrales más bajos que descarten el tráfico que está dentro de la actividad máxima normal), que generalmente está entre un 15 % y un 20 % por encima de la **Alarm Rate (Tasa de alarma)**.

  Para los perfiles agregados, establezca el umbral justo por encima de la tasa de CPS máxima normal para el grupo para evitar la pérdida de tráfico que esté dentro de las expectativas de actividad normales. Esto es generalmente 15-20 % por encima de la **Alarm Rate (Tasa de alarma)**.
- **Max Rate (Tasa máxima)**: para perfiles clasificados y agregados, establezca la tasa máxima según el uso de la CPU del cortafuegos. Si el uso de la CPU del cortafuegos es superior al 50 %, ajuste el CPS máximo al doble de la tasa de **Activate (Activar)**. Si el uso de la CPU del cortafuegos está por debajo del 50 %, ajuste el CPS máximo a tres veces la tasa **Activate (Activar)** y supervise el uso de la CPU. Si el uso de la CPU es demasiado alto, reduzca el máximo al doble de la tasa **Activate (Activar)**. Si se cruza el umbral máximo, se bloquean las conexiones nuevas hasta que la tasa de CPS cae por debajo del umbral.

  > *No establezca la tasa máxima superior por encima de la capacidad del dispositivo individual (clasificado) o el 80-90 % de la capacidad del grupo (agregado) para evitar permitir más conexiones de las que el objetivo puede gestionar.*

  Cuando la tasa de CPS llega al umbral, el cortafuegos descarta conexiones nuevas durante el período especificado en **Block Duration (Duración del bloqueo)**.
- **Block Duration (Duración del bloqueo**: utilice el valor predeterminado (300 segundos) para bloquear la sesión del atacante sin penalizar sesiones legítimas del mismo origen durante demasiado tiempo.
- Supervise y ajuste los umbrales según sea necesario.

- Crear Reglas de políticas de protección de DoS [**Policies (Políticas)** > **DoS Protección (Protección DoS)**]. Cree cada regla lo más específica posible para proteger dispositivos críticos y, al mismo

©2024 Palo Alto Networks, Inc.

tiempo, preservar los recursos de memoria y CPU del cortafuegos. Adjunte perfiles de protección DoS a las políticas de protección DoS. En la regla de política. establezca:

- **Service (Servicio)**: especifique los servicios (puertos) en uso en los servidores que protege. Si protege servidores web, especifique HTTP, HTTPS y otros puertos de servicio apropiados para las aplicaciones web.

  Use reglas de política de protección DoS diferentes para los puertos de servicio no usados de los servidores críticos.

- **Action (Acción)**: seleccione **Protect (Proteger)** para aplicar los perfiles de protección DoS de la regla en los dispositivos especificados. Proteger es la única **Action (Acción)** que aplica la protección DoS.
- **Reenvío de logs**: para lograr una gestión más sencilla, reenvíe por separado los logs DoS de los demás logs de amenazas directamente a los administradores por correo electrónico y a un servidor de logs.
- **Aggregate (Agregado)**: use perfiles agregados para proteger los grupos de servidores críticos.
- **Profile (Perfil)** > **Classified (Clasificado)**: utilice perfiles clasificados para proteger servidores individuales críticos. Debe utilizar un perfil clasificado para aprovechar la tabla de bloqueos de hardware.
- **Address (Dirección)** > **Classified (Clasificada)**: los contadores consumen recursos del cortafuegos. Para los perfiles de protección DoS clasificados, especifique si las conexiones se contabilizan como parte de los umbrales del perfil sobre la base de los campos coincidentes de **source-IP-only (Solo IP de origen)**, **destination-IP-only (Solo IP de destino)**, o ambas (**src-dest-ip-both [IP de origen y de destino]**). Sus objetivos de protección DoS, lo que desea proteger y si los dispositivos protegidos están en zonas accesibles desde Internet determinan cómo configurar el contador del umbral.

  No use **src-ip-only (Solo IP de origen)** o **src-dest-ip-both (IP de origen y de destino** para zonas accesibles desde Internet porque el cortafuegos no puede almacenar contadores para todas las direcciones IP posibles de Internet. Use **destination-IP-only (Solo IP de destino)** en las zonas del perímetro.

  Use **destination-IP-only (Solo IP de destino)** para proteger dispositivos individuales críticos. Establezca el umbral máximo por debajo de la tasa de CPS que puede gestionar cada dispositivo especificado en la política.

  Use **source-IP-only (Solo IP de origen)** y el umbral **Alarm (Alarma)** para supervisar hosts sospechosos (zonas no accesibles desde Internet).

  El cortafuegos consume más recursos para registrar los contadores **src-dest-ip-both (IP de origen y de destino)** que para registrar solo el contador de IP de origen o el de IP de destino.

  *Para utilizar la tabla de bloqueos de hardware en plataformas compatibles, debe usar **source-ip-only** o **src-dest-ip-both**. **Destination-ip-only** utiliza la tabla de software.*

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Habilite Protección de búfer de paquetes a nivel global para proteger los búferes del cortafuegos de ataques DoS de sesión única, de ataques desde una dirección IP de origen única y de direcciones IP de origen que crean muchas sesiones pequeñas que se combinan para consumir búferes de paquetes.

La protección de búfer de paquetes global es la primera fase de una estrategia de dos fases para proteger los búferes del cortafuegos y está habilitada de forma predeterminada. (El paso 4 muestra la segunda fase, protección de búfer de paquetes por zona, que también está activada de forma predeterminada). La protección de búfer de paquetes global detecta sesiones individuales o direcciones de IP de origen que amenazan con consumir el búfer de paquetes del cortafuegos y aplica RED a esas sesiones o paquetes para descartar más paquetes a medida que aumenta la congestión del búfer.

El objetivo de Protección de búfer de paquetes es evitar que el cortafuegos entre y permanezca en un estado de alta latencia y alta utilización del buffer aplicando primero RED para descartar paquetes ofensivos (protección global) y luego descartando la sesión ofensiva o bloqueando la dirección IP de origen ofensiva (bloqueo de sesión o host) si el ataque continúa (protección por zona). La idea es proteger los buffers de paquetes tanto a nivel de software como de hardware y al mismo tiempo tener baja latencia y pérdida de paquetes, y descartar o bloquear el tráfico que comete la infracción en el momento adecuado.

Protección de búfer de paquetes también protege los buffers del cortafuegos si un host envía una gran cantidad de tráfico que el cortafuegos procesa y niega en serie sin configurar una sesión. Este tráfico suele tener el mismo identificador de 6 tuplas (IP de origen y destino, puerto de origen y destino, protocolo y zona de entrada). Los recursos necesarios para procesar cada paquete y luego denegarlo consumen recursos de cortafuegos si no habilita la Protección de búfer de paquetes.

Si la protección de búfer de paquetes por zona está habilitada y el consumo de búfer alcanza un nivel alto y se mantiene durante un período de tiempo configurable, el cortafuegos descarta solo las sesiones ofensivas o los hosts. Si la protección de búfer de paquetes por zona está deshabilitada, el cortafuegos realiza RED pero no descarta ni bloquea el tráfico.

- Use las mediciones de referencia de uso del búfer de paquetes para comprender la capacidad del cortafuegos y asegurarse de que este tenga el tamaño correcto, de modo que solo un ataque provoque un pico importante en el uso del búfer. Comprenda el uso del búfer de paquetes durante el funcionamiento normal en horas pico y en qué momento se producen problemas de latencia o caídas. Si la capacidad del cortafuegos es lo suficientemente baja como para que el tráfico normal cause picos en el uso del búfer, es posible que necesite un cortafuegos de mayor capacidad.

  En PAN-OS 10.0 y posteriores, considere usar el modo**Monitor Only (Solo supervisión)** [**Dispositivo (Device)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Ajustes de sesión)**] para comprender la utilización básica del búfer de paquetes e identificar fuentes agresivas. En el modo **Monitor Only (Solo supervisión)**, el cortafuegos supervisa la utilización del búfer de paquetes y alerta sobre sesiones y fuentes infractoras, pero no las bloquea ni las descarta. La desventaja es que puede experimentar con diferentes umbrales de **Alert (Alerta)** y **Activate (Activar)** y ver los resultados en los registros de amenazas sin afectar el tráfico, pero el cortafuegos no está protegido contra ataques de búfer de paquetes. Si puede replicar el tráfico de producción en un entorno que no es de producción, puede experimentar de forma segura con los umbrales de **Alert (Alerta)** y **Activate (Activar)** para ver qué sesiones se penalizan con diferentes configuraciones de umbral y qué umbrales comienzan a afectar el tráfico legítimo.
- Establezca los umbrales de protección de búfer de paquetes globales [**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)**] según el uso

 ©2024 Palo Alto Networks, Inc.

del búfer o la latencia de procesamiento de la CPU. La protección de buffer de paquetes basada en la latencia de procesamiento de CPU responde ante grandes ráfagas repentinas de paquetes más rápido que la protección de buffer basada en el porcentaje de utilización de buffer.

La protección de búfer de paquetes basada en el porcentaje de uso del búfer está habilitada de forma predeterminada:

- **Alert (Alerta)**: empiece con el valor predeterminado (50 %), supervise el uso del búfer de paquetes y ajuste los umbrales según sea necesario.
- **Activate (Activar)**: el umbral de la opción **Activate (Activar)** predeterminada es 80 % en PAN-OS 10.0 y versiones posteriores y 50 % en PAN-OS 9.1 y versiones anteriores. En lugar de utilizar los valores predeterminados, es más seguro establecer el umbral de activación entre un 10% y un 20% por encima de su uso básico y luego supervisar la utilización del búfer de paquetes. Ajuste el umbral hasta que la Protección del búfer de paquetes se active a tiempo para penalizar las sesiones infractoras, pero sin penalizar el uso normal.

  El ajuste de **Activate (Activar)** correcto depende de su entorno y de los recursos de procesamiento disponibles, por lo que suele ser necesario experimentar. Cuanto más bajo sea el umbral de **Activate (Activar)**, es más probable que se bloquee el tráfico legítimo, pero la mitigación de ataques comienza antes. Cuanto más alto sea el umbral, más tiempo llevará comenzar a mitigar un ataque, pero es menos probable que el tráfico legítimo se vea afectado.

  Si el umbral de activación es demasiado alto para el entorno, experimentará el efecto de la alta carga y/o latencia en el tráfico legítimo antes de que se active la protección del búfer de paquetes.

  Si el umbral de activación es demasiado bajo para el entorno, el cortafuegos descarta innecesariamente demasiados paquetes legítimos aunque haya recursos disponibles para gestionar el tráfico. (Esto también podría ocurrir si hay otros problemas de red).

  Si el umbral de activación es el adecuado para el entorno, se elimina muy poco tráfico legítimo y no se sobrecargan los recursos del cortafuegos. Conocer la carga de referencia del búfer de paquetes es clave para ajustar los umbrales de forma correcta. Por ejemplo, si sabe que durante las horas pico, la utilización del búfer de paquetes puede aumentar al 40-50 % de la capacidad del cortafuegos y que experimenta problemas cuando la utilización del búfer de paquetes alcanza el 60-70 %, establezca el umbral de **Activate (Activar)** entre 55 y 60 %.

*En PAN-OS 10.0 y versiones posteriores, puede experimentar configurando umbrales de **Alert (Alerta)** y **Activate (Activar)** y viendo los resultados usando el modo **Monitor Only (Solo supervisión)**. El modo **Monitor Only (Solo supervisión)** no toma ninguna medida contra el tráfico infractor, pero le brinda visibilidad sobre cómo los umbrales afectan el tráfico antes de activar la Protección de búfer de paquetes.*

Para medir el uso del búfer de paquetes, utilice Supervisión de estado de Panorama. Además, los siguientes comandos operativos de CLI son útiles:

- El comando **`> show running Resource-Monitor`** muestra las estadísticas de la CPU. La opción **`ingress-backlogs`** muestra sesiones que consumen al menos el 2 por ciento de los descriptores de paquetes en el chip.

 ©2024 Palo Alto Networks, Inc.

- Para las sesiones en las que la Protección de búfer de paquetes protege activamente el cortafuegos, el comando **`> show session package-buffer-protection`** muestra las sesiones que consumen la mayor cantidad de recursos de CPU del plano de datos.

La **Latency Based Activation (Activación basada en latencia)** de la protección de búfer de paquetes está deshabilitada de forma predeterminada. La protección basada en latencia no puede defenderse frente a ataques DoS donde una fuente envía constantemente paquetes que el cortafuegos niega, lo que consume recursos pero no se ve como latencia porque el cortafuegos nunca configura una sesión para el tráfico denegado. (Sin embargo, la protección de búfer de paquetes basado en la utilización del búfer previene este tipo de ataques).

La **Latency Based Activation (Activación basada en latencia)** mitiga el alto consumo de descriptores en el chip cuando el uso del búfer de paquetes aún no es alta y es el mejor método cuando desea que el cortafuegos reaccione antes de que se agoten los búferes de paquetes.

Seleccione la **Latency Based Activation (Activación basada en la latencia)** para basar la protección en la latencia de procesamiento de la CPU en lugar de en base al porcentaje del uso del búfer. Los siguientes tres ajustes sustituyen a los ajustes de **Alert (Alerta)** y **Active (Activa)** basados en la utilización:

- **Latency Alert (Alerta de latencia)**: comience con el valor predeterminado (50 milisegundos), supervise la latencia y ajuste los umbrales si es necesario.
- **Latency Activate (Activar latencia)**: comience con el valor predeterminado (200 milisegundos), supervise la latencia y ajuste los umbrales si es necesario.
- **Latency Max Tolerance (Máx. tolerancia de latencia)**: comience con los valores predeterminados (500 milisegundos), supervise la latencia y ajuste los umbrales si es necesario. Cuando el tráfico alcanza el umbral de **Latency Activate (Activar latencia)**, el cortafuegos usa RED para empezar a descartar el tráfico y aumenta la tasa de descarte hasta que la latencia alcanza la **Latency Max Tolerance (Máx. tolerancia de latencia)**. En **Latency Max Tolerance (Máx. tolerancia de latencia)**, la probabilidad de la tasa de descarte es cercana al 100 %.

Mida la latencia en cada cortafuegos:

- ***`fw-1> debug dataplane pow performance | match pbp`*** *comando operacional.*
- *Habilite el registro cuando la carga del plano de datos es alta para recibir notificaciones y ver la información del log [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Logging and Reporting (Logs e informes)** y **Enable Log on High DP Load (Habilitar log con carga alta)**]. Compruebe la carga del plano de datos mediante el comando operativo de la CLI **`show running resource monitor`**. También puede crear un archivo de soporte técnico y revisar el log del plano de datos en formato de texto.*

- Establezca umbrales y temporizadores [**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)**] para definir cuándo descartar una sesión ofensiva o bloquear una dirección IP de origen infractora. El cortafuegos solo utiliza estos umbrales y temporizadores si habilita la Protección de búfer de paquetes por zona. Si solo está habilitada la

 ©2024 Palo Alto Networks, Inc.

protección de búfer de paquetes global, el cortafuegos realiza RED en el tráfico, pero no lo descarta ni bloquea.

Basa la configuración en las experiencias y mediciones de la latencia y la utilización del búfer, su tolerancia a la latencia y el descarte de paquetes debido a la congestión del búfer y la agresividad con la que desea reducir el tráfico para evitar la latencia y el consumo de búfer de paquetes que afectan a la red y a sus usuarios.

- **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)**: el porcentaje de utilización del búfer o umbral de latencia en milisegundos que inicia la cuenta regresiva para descartar o bloquear el tráfico infractor. Cuando la congestión o latencia del búfer alcanza el umbral de **Block Countdown Threshold (Bloquear umbral de cuenta regresiva)**, el **Block Hold Time (Tiempo de espera de bloqueo)** comienza a disminuir. (Cuando se agota el tiempo de espera del bloqueo, el cortafuegos descarta sesiones o bloquea a los hosts infractores).

  Establezca **Block Countdown Threshold (Bloquear umbral de cuenta regresiva** un 10% por debajo del umbral **Activate (Activar)** o **Latency Activate (Activar latencia)**, supervise la utilización del búfer de paquetes y ajuste el valor según sea necesario. Este método bloquea las direcciones IP infractoras más rápido que el ajuste predeterminado (80 % o 500 ms para latencia). Cuanto menor sea el valor del **Block Hold Time (Tiempo de espera de bloqueo)**, antes el cortafuegos comenzará a mitigar la congestión del búfer descartando la sesión o bloqueando la IP de origen infractora. Cuanto mayor sea el valor, más tiempo puede continuar un ataque antes de que el cortafuegos lo mitigue.

- **Block Hold Time (Tiempo de espera de bloqueo)**: la cantidad de tiempo que la sesión infractora puede permanecer por encima del **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)** antes de que el cortafuegos descarte la sesión o bloquee la dirección IP de origen. Cuanto menor sea el valor, antes el cortafuegos activa la Protección del búfer de paquetes y aprovecha la tabla de bloques de hardware y/o la tabla de bloques de software (ambas en sistemas que tienen una tabla de bloqueos de hardware) para proteger los búferes de paquetes.

  Comience con un valor de 30 segundos, supervise la utilización del búfer de paquetes y ajuste el tiempo si es necesario. Este método bloquea las direcciones IP infractoras más rápido que el ajuste predeterminado (60 segundos). Cuanto mayor sea el valor del tiempo, más tiempo puede continuar un ataque antes de que el cortafuegos lo mitigue.

  El tiempo de espera del bloqueo disminuye mientras la congestión permanezca por encima del valor de **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)**. Cuando **Block Hold Time (Tiempo de espera de bloqueo)** llega a 0, el cortafuegos descarta la sesión o bloquea la dirección IP de origen.

- **Block Duration (Duración del bloqueo)**: la cantidad de tiempo después de que expire el **Block Hold Time (Tiempo de espera de bloqueo)** que la dirección IP de origen está en cuarentena (bloqueada). Comience con el valor predeterminado (3600 segundos) o reduzca el valor si bloquear una dirección IP de origen durante una hora es una penalización demasiado grande para las condiciones de su negocio. Supervise el uso de búfer de paquetes y ajuste el valor según sea necesario.

La forma en que establezca los umbrales de los búferes de paquetes depende de su tráfico de red y de cómo desee tratar ese tráfico:

- Los ajustes predeterminados son conservadores y favorecen permitir que la congestión del búfer de paquetes continúe más tiempo antes de descartar sesiones o bloquear direcciones IP de origen para evitar que se penalice al tráfico legítimo. El cortafuegos no bloquea las sesiones y fuentes potencialmente legítimas con la misma rapidez durante los períodos de congestión y es posible que

 ©2024 Palo Alto Networks, Inc.

ralentice las sesiones legítimas que no están causando la congestión del buffer de paquetes. Es por eso que la práctica recomendada es comenzar con umbrales más bajos y agresivos.

- Las quejas de los usuarios sobre la lentitud de la red pueden indicar que los umbrales del búfer de paquetes son demasiado conservadores. Para abordar estas quejas, baje la tasa de **Activate (Activación)** y el **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)** para iniciar el descarte del paquete RED antes. Disminuya el **Block Hold Time (Tiempo de espera de bloqueo)** para que el cortafuegos comience a bloquear direcciones IP o a descartar sesiones más rápido después de que la tasa de consumo de búfer alcance el **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)**.

  Descartar o bloquear el tráfico infractor más rápido significa que el tráfico legítimo que no está causando problemas de consumo de búfer de paquetes no estará sujeto a problemas de latencia o descarte de paquetes debido al tráfico infractor, pero el tráfico infractor se colocará en cuarentena. Sin embargo, una sesión legítima o dirección IP de origen que envía mucho tráfico también podría ponerse en cuarentena más rápido.
- Si le preocupa que establecer la tasa de **Activate (Activación)** y **Block Countdown Threshold (Bloquear umbral de la cuenta regresiva)** más bajos podría bloquear el tráfico legítimo importante, como DNS u otro tráfico de infraestructura crítica, aumente el **Block Hold Time (Tiempo de espera de bloqueo)** a un valor más alto para retrasar la acción de cuarentena y supervisar el uso del búfer de paquetes.
- Ajuste los umbrales de protección de búfer de paquetes para lograr el equilibrio de latencia y descarte de paquetes frente a cuándo descartar sesiones o bloquear direcciones IP de origen que tenga sentido para su red.

STEP 4 | La segunda fase de la Protección de búfer de paquetes protege los búferes del cortafuegos por zona de entrada y está activada de forma predeterminada en PAN-OS 10.0 y versiones posteriores (desactivada de forma predeterminada en PAN-OS 9.1 y versiones anteriores), pero también debe estar activada la Protección de búfer de paquetes global o la Protección de búfer de paquetes por zona no funcionará. La protección de búfer de paquetes por zona descarta las sesiones infractoras y

 ©2024 Palo Alto Networks, Inc.

bloquea las direcciones IP de origen infractoras, y es una práctica recomendada cuando necesita una capa adicional de protección para determinadas zonas de entrada.

Desactive la protección de búfer de paquetes por zona cuando no desee bloquear las direcciones IP de origen o descartar sesiones para una zona en particular (de forma predeterminada, el cortafuegos también aplica RED globalmente, por lo que los búferes de paquetes aún tienen una capa primaria de protección). El bloqueo de una dirección IP de origen bloquea todo el tráfico desde esa dirección, no solo la sesión infractora. Si la dirección IP de origen es un dispositivo NAT, podría suponer un gran número de flujos de usuarios que se origina detrás del dispositivo NAT.

- Para deshabilitar o habilitar la protección por zona, **Network (Red)** > **Zones (Zonas)**, seleccione una zona existente o seleccione **Add (Añadir)** una zona y, a continuación, seleccione o anule la selección **Enable Packet Buffer Protection (Habilitar protección de búfer de paquetes**.

Cuando considere habilitar o deshabilitar la protección de búfer de paquetes por zona, piense no solo en las zonas vulnerables a ataques desde el exterior y también en la red interna. Considere posibles amenazas internas, dispositivos internos mal configurados accidentalmente, adaptadores NIC defectuosos que generan grandes cantidades de tráfico ilegítimo y configuración incorrecta del cortafuegos.

Todo esto puede denegar el tráfico de cualquier fuente legítima que también envíe una cantidad significativa de tráfico al cortafuegos porque el cortafuegos identifica todas las fuentes de tráfico significativas por sus identificadores únicos de 6 tuplas (IP de origen y destino, puerto de origen y destino, protocolo y zona de entrada). Durante los períodos de congestión del búfer de paquetes, RED afecta a las fuentes legítimas que envían una cantidad significativa de tráfico junto con las fuentes infractoras.

STEP 5 | Adjunte el perfil de protección frente a vulnerabilidades recomendado a todas las reglas de la política de seguridad.

La combinación de la protección DDoS dedicada de alto volumen en el perímetro, los perfiles de protección de zonas, las reglas de política y los perfiles de protección DoS, la protección del búfer de paquetes y la protección frente a vulnerabilidades para el tráfico permitido brindan varias capas de protección DoS para su red y recursos más críticos.

 ©2024 Palo Alto Networks, Inc.

Prácticas recomendadas de protección DoS y de zonas posteriores a la implementación

Luego de que implemente la protección DoS y de zonas, asegúrese de que todo funcione con el nivel esperado y realice los pasos necesarios para garantizar que siga siendo así a medida que su red evolucione.

STEP 1 | Mida el rendimiento del cortafuegos para asegurarse de que está dentro de las normas aceptables y de modo que pueda comprender el efecto de la protección DoS y de zonas en los recursos del cortafuegos.

Si los niveles de protección DoS y de zonas (combinados con otras funciones que consumen recursos, como el descifrado) consume demasiados recursos del cortafuegos, la práctica recomendada es aumentar los recursos en lugar de comprometer la seguridad.

STEP 2 | Configure el reenvío de logs..

Para lograr una gestión más sencilla, use perfiles de reenvío de logs diferentes para reenviar por separado los logs de eventos del umbral DoS y de zona de los logs de amenazas. Envíe logs DoS y de zonas directamente a los administradores relevantes por correo electrónico y también a un servidor de logs, de modo que las notificaciones contengan solo los eventos que son ataques DoS potenciales. Configure el reenvío de logs DoS en la regla de política de protección DoS (**Policies [Políticas]** > **DoS Protection [Protección DoS]**) y configure el reenvío de logs de eventos de zona en cada zona (**Network [Red]** > **Zones [Zonas]**).

Configure los mensajes de logs de eventos del umbral **Alarm Rate (Tasa de alarma)** en el nivel de gravedad informativo o bajo. Configure la protección DoS **Activate (Activación)** y **Maximum (Máxima)** y los mensajes de logs de eventos de protección de zona **Activate Rate (Tasa de activación)** y **Max Rate (Tasa máxima)** en el nivel de gravedad crítico. Luego de configurar correctamente los umbrales de congestión, los logs le muestran los ataques de congestión potenciales en la red porque solo ve eventos anómalos y amenazas. Si ve demasiadas alertas falsas, los umbrales están configurados a un nivel demasiado bajo o el cortafuegos no tiene el tamaño correcto para el tráfico que debe gestionar.

El cortafuegos registra logs cada 10 segundos para mantener el volumen a un nivel que se pueda gestionar, evitar la sobrecarga de los servidores de logs y preservar los recursos del cortafuegos.

STEP 3 | Observe e investigue otros indicadores de ataques DoS.

Además de configurar el reenvío de logs de modo que los administradores reciban notificaciones cuando se cruzan los umbrales de congestión, verifique los indicadores de ataques e investigue los ataques DoS potenciales:

- Revise la actividad de amenazas DoS (**ACC** > **Threat Activity [Actividad de amenazas]**) y busque patrones de abuso.
- En los modelos de cortafuegos que lo admitan (PA-3050, PA-3060, PA-3200 Series, PA-5200 Series y PA-7000 Series), supervise las direcciones IP bloqueadas (**Monitor [Supervisar]** > **Block IP List [Lista de bloqueo de IP]**) para las direcciones IP que el cortafuegos bloqueó debido a un

©2024 Palo Alto Networks, Inc.

posible ataque DoS. La columna **Block Source (Origen del bloqueo)** identifica el nombre del perfil de protección DoS clasificado que bloqueó la dirección IP.

- Una interrupción total o parcial del tráfico del cortafuegos, navegación web o conectividad con el extremo lenta, o sesiones nuevas fallidas pueden indicar un ataque DoS. El alto uso del CPU, el agotamiento de descriptores y búfer de paquetes, y un pico en la cantidad de sesiones activas también puede indicar un ataque DoS.
- Obtenga más información sobre los contadores globales y logs de eventos de la protección DoS y de zonas para supervisar la actividad DoS.

Las infracciones del umbral de congestión pueden indicar un ataque DoS, pero también pueden indicar valores CPS mal configurados, una configuración incorrecta de otro dispositivo interno, adaptadores NIC defectuosos, amenazas potenciales de fuentes internas o tamaños incorrectos del cortafuegos.

STEP 4 | Los patrones del tráfico de red cambian con el tiempo, se añaden nuevos dispositivos a la red y se quitan dispositivos antiguos, y los eventos especiales pueden temporalmente afectar los patrones de tráfico.

Por estos motivos, lleve a cabo mediciones de CPS nuevas periódicamente y vuelva a revisar la configuración del umbral de congestión DoS y de zonas; debido a que las redes evolucionan constantemente, la protección DoS y de zonas requiere un enfoque iterativo.

©2024 Palo Alto Networks, Inc.