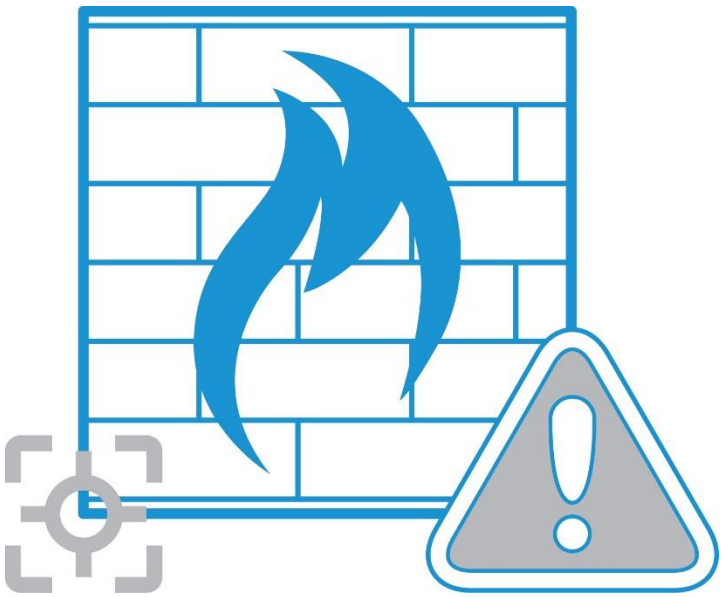
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT centro criptológico nacional

CCN-CERT BP/09

Recomendaciones de protección DoS en cortafuegos



Diciembre 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.09.04 18:26:06 +02'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. INTRODUCCIÓN

Un ataque de denegación de servicio (DoS) es un fenómeno conocido desde hace muchos años. Su importancia ha ido en aumento debido a que el éxito de este tipo de ataques está directamente relacionado con la exposición de servicios a Internet. De esta manera, a medida que los servicios son más importantes y los usuarios dependen más de ellos, el riesgo de su indisponibilidad es más crítico y los ataques de DoS se vuelven más atractivos para los atacantes.

El impacto asociado a una denegación de servicio puede tener una gran repercusión en pérdidas económicas y pérdidas de imagen.

En la actualidad los organismos disponen de dispositivos de protección de perímetro que ofrecen funcionalidades frente a ataques DoS. Si bien no deben ser la única medida de seguridad a aplicar, sí contribuyen en la implementación de una defensa en profundidad en varias capas.

En este documento se presenta una guía para aplicar medidas de protección DoS en dos (2) de las tecnologías de cortafuegos más extendidos en el mercado: Palo Alto y Fortinet.

3. ATAQUES DOS

Un ataque DoS ocurre cuando se agotan los recursos de un sistema inundándolo con paquetes anómalos, impidiendo así que los usuarios legítimos puedan utilizar el servicio proporcionado por dicho sistema.

Un ataque de denegación de servicio distribuido (DDoS) ocurre cuando un atacante utiliza un dispositivo maestro para controlar una red de sistemas comprometidos (conocido como botnet), los cuales de forma colectiva inundan el sistema a atacar mediante excesivos envíos de paquetes anómalos.

Una denegación de servicio ataca a la fuente de información o al canal de transmisión impidiendo el acceso a un recurso informático por parte de usuarios con fines legítimos, como

puede ser navegar por la web, enviar un correo electrónico o un sistema SCADA (Supervisory Control And Data Adquisition).

El objetivo de este tipo de ataques no es conseguir acceso no autorizado para leer o modificar información, sino provocar la inutilización o destrucción de un activo. Esta particularidad hace este tipo de ataques informáticos distinto al resto por lo que la forma de afrontarlos es diferente.

En la actualidad los motivos por los cuales se efectúan este tipo de ataques pueden ser muy diversos. En términos generales los motivos suelen ser desde personales, por venganza, extorsión, sabotaje o prestigio. Y el origen puede ser desde personas que actúan individualmente, grupos organizados o cibercriminales. Incluso pueden deberse a un uso accidental de los recursos.

Podemos clasificar los ataques DoS por su modo de explotación (aprovechando vulnerabilidades o agotando recursos), el origen (válido o falso, fijo o aleatorio), su objetivo (infraestructura, red, recurso, maquina o aplicación), la propagación (localizado, un salto, varios saltos o global), su frecuencia (una vez, constante o variable), caracterización (filtrable, no filtrable, no caracterizable) o el impacto (degradación o disruptivo).

Es importante señalar que una estrategia adecuada para la prevención de ataques DoS deberá ser multicapa, involucrando probablemente otras partes de la red, otros dispositivos de protección de perímetro, así como el proveedor de servicios de Internet.

4. PREVENCIÓN DE ATAQUES DOS EN PALO ALTO

La prevención de ataques de denegación de servicio (DoS) y denegación de servicio distribuidos (DDoS) es posible realizarla a través de dos (2) módulos diferentes que pueden trabajar de manera independiente o combinada: "*Zone Protection*" y "*DoS Protection*".

El módulo de "*Zone Protection*" actúa antes que el de "*DoS Protection*", requiriendo este último más tiempo de procesamiento para obtener la información necesaria de clasificación y tomar una determinación.

Así pues, se aconseja que el módulo de "*DoS Protection*" se emplee para proteger objetivos específicos, mientras que el de "*Zone Protection*" es el mejor mecanismo para proteger aquellas zonas que están de cara a Internet.

Esto se debe a que "*Zone Protection*" utiliza una aproximación de agregación en la zona de entrada del tráfico, independientemente de los interfaces o direcciones IP, y por tanto puede escalar mejor en este tipo de zonas donde los ataques DoS pueden ser masivos.

4.1 ZONE PROTECTION

El módulo de "*Zone Protection*" se configura en base a perfiles que se aplican posteriormente sobre las zonas de seguridad definidas. Trabaja sobre todo el tráfico agregado aplicado sobre la zona en cuestión, manteniendo por tanto un único contador para todo el tráfico, independientemente de las direcciones IP y puertos origen o destino.

En concreto se ofrecen los siguientes mecanismos de prevención dentro de este módulo:

- **Flood Protection.** Previene los ataques volumétricos destinados a inundar algún servicio particular.
- **Reconnaisance Protection.** Detecta y bloqueo los escaneos de puertos y hosts.
- **Packet Based Attack Protection.** Ofrece protección ante determinados ataques específicos para nivel IP.

Los perfiles de "*Zone Protection*" solo pueden ser aplicados a zonas completas. Así pues, es importante investigar cualquier posible problema que surja como falso positivo y que requiera un ajuste de los valores establecidos como umbrales.

4.1.1 CONFIGURACIÓN DE FLOOD PROTECTION

Ubicación. "*Network* > *Network Profiles* > *Zone Protection* > *Flood Protection*".

Acción. Se recomienda configurar "*Flood Protection*" en función del número máximo de paquetes que se deseen permitir. La configuración se aplica a todo el tráfico que entra en la red a través de cualquier interfaz que pertenezca a la zona de seguridad que tiene el perfil activo. La siguiente figura muestra un ejemplo de configuración.

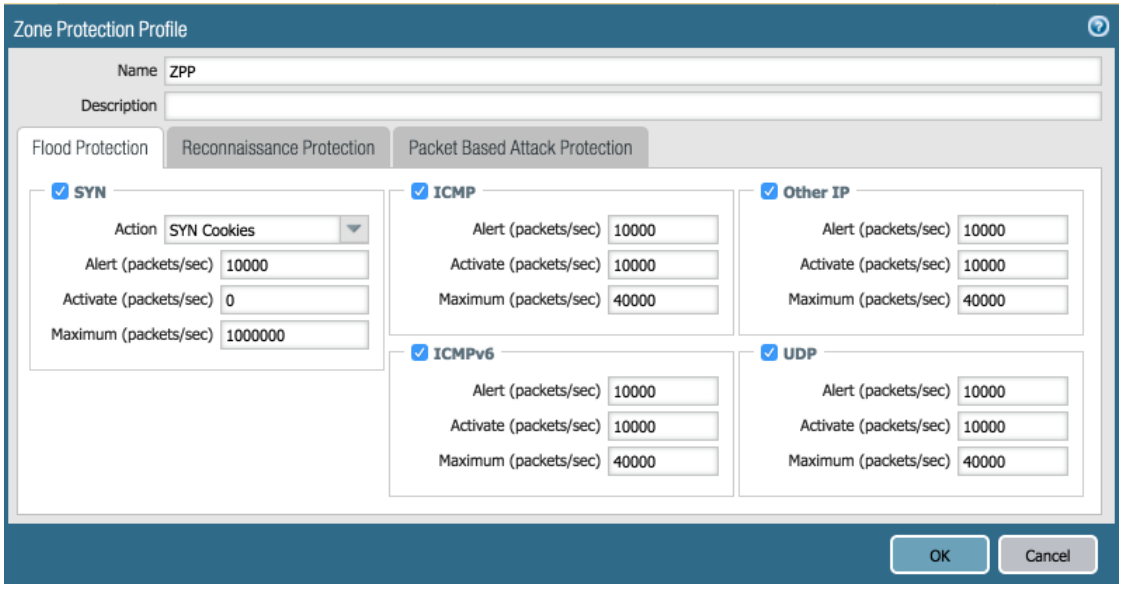


Figura 1.- Ejemplo de configuración de Flood Protection

Es importante indicar que los valores configurados deben ajustarse para cada instalación siendo también importante señalar que, como se describirá posteriormente, para los SYN Floods es preferible utilizar SYN Cookies frente a RED (Random Early Drop).

4.1.2 CONFIGURCIÓN DE RECONNAISANCE PROTECTION

Ubicación. "*Network* > *Network Profiles* > *Zone Protection* > *Reconnaissance Protection*".

Acción. En general se recomienda activar este módulo solo en las zonas externas. Para las zonas internas es importante asegurarse de que la configuración no impactará negativamente sobre ninguna herramienta de monitorización, que en muchas ocasiones utilizan técnicas similares a los escaneos para determinar si los servidores y sus servicios están operativos y funcionando según se espera. La siguiente figura muestra un ejemplo de configuración.

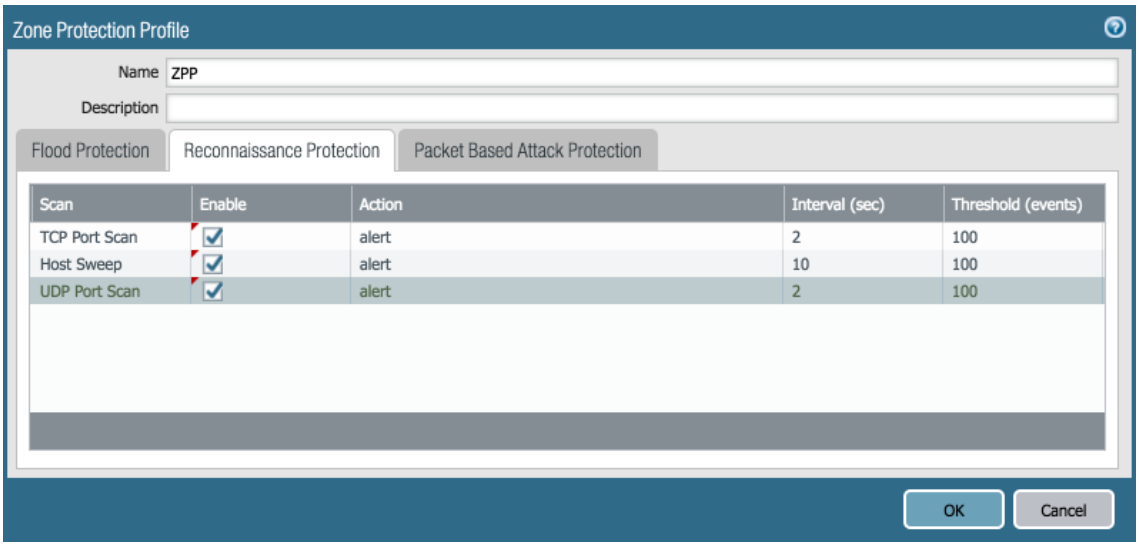


Figura 2.- Ejemplo de configuración de Reconnaisance Protection

4.1.3 CONFIGURACIÓN DE PACKET BASED ATTACK PROTECTION

Ubicación. "*Network > Network Profiles > Zone Protection > Packet Based Attack Protection*".

Acción. Es en general seguro activar este módulo solo para las zonas externas. Para las internas es importante asegurarse que la configuración no afectará negativamente a las comunicaciones de red de algunos dispositivos que pueden utilizar estas técnicas para su operativa normal.

Un caso concreto es el uso ICMP Ping ID 0, que en ocasiones es utilizado por ejemplo por los proxies para chequear la disponibilidad de los hosts con los que necesitan comunicarse.

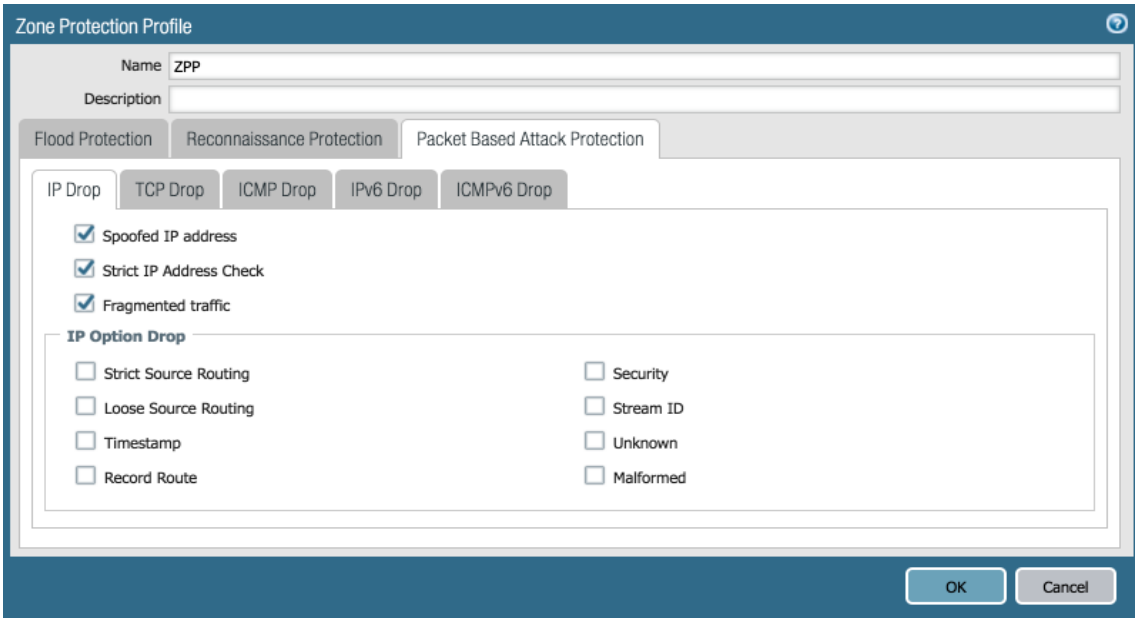


Figura 3.- Ejemplo de configuración de Packet Based Attack Protection

4.1.4 CASO DE USO

En el ejemplo se configurará y habilitará la protección de "*Zone Protection*" en la zona externa, donde el tráfico público alcanza el cortafuegos.

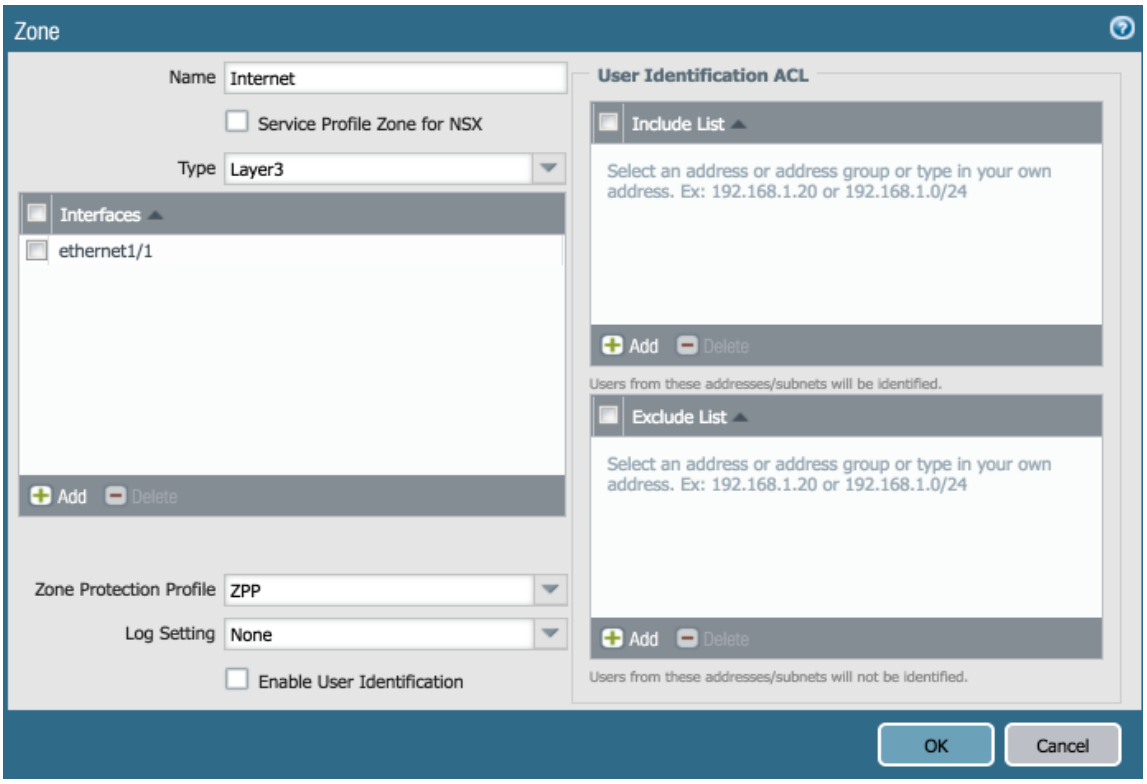


Figura 4.- Aplicación del perfil de Zone Protection en la Zona Internet

Flood Protection. Cuando se dispara un evento de "*Flood Protection*" se envía un log al módulo de "*Threat*". Puesto que el módulo trabaja sobre tráfico agregado, las entradas mostrarán el nombre de la zona para la que el perfil ha hecho *match* tanto en la zona origen como destino, y las direcciones IP aparecerán como 0.0.0.0. La siguiente figura muestra un ejemplo de este tipo de log.

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
		11/17 19:05:51	flood	TCP Flood	LAN	LAN	0.0.0.0		0.0.0.0	0	not-applicable	syncookie-sent	critical
		11/17 19:05:41	flood	TCP Flood	LAN	LAN	0.0.0.0		0.0.0.0	0	not-applicable	syncookie-sent	critical
		11/17 19:05:31	flood	TCP Flood	LAN	LAN	0.0.0.0		0.0.0.0	0	not-applicable	syncookie-sent	critical

Figura 5.- Ejemplo de log de Flood Protection

Reconnaisance Protection. Los escaneos de puertos TCP y UDP generarán un log cuando se escanee un puerto TCP o UDP sobre un único host y la ratio de escaneo sobrepasa el umbral configurado (escaneo de tipo vertical). Los eventos de tipo "*Host Sweep*" se disparan cuando se realiza un escaneo sobre múltiples hosts de uno o varios puertos a través de TCP, UDP o ICMP (escaneo de tipo horizontal).

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
		11/04 16:06:53	scan	SCAN: UDP Port Scan	LAN	Internet	192.168.3.25	80.169.239.226	59349	not-applicable	alert	medium
		11/04 16:04:54	scan	SCAN: UDP Port Scan	LAN	Internet	192.168.3.25	80.169.239.226	64280	not-applicable	alert	medium
		11/04 16:02:54	scan	SCAN: UDP Port Scan	LAN	Internet	192.168.3.25	80.169.239.226	12766	not-applicable	alert	medium

Figura 6.- Ejemplo de log de Reconnaisance Protection

Packet Based Attack Protection. El módulo de "*Packet Based Attack Protection*" se dispara cuando se detectan anomalías en los paquetes. Puesto que este tipo de tráfico se considera ruido no genera ninguna entrada en el "*Threat Log*". No obstante, es posible observar los contadores para paquetes eliminados a través del CLI, ejecutando por ejemplo el siguiente comando:

```
show counter global filter delta yes | match drop
```

Para obtener información detallada sobre el CLI se puede consultar:
https://www.paloaltonetworks.com/documentation/71/pan-os/cli-gsg

4.2 DOS PROTECTION

El módulo de "*DoS Protection*" es un complemento al de "*Zone Protection*" y ofrece políticas de prevención de ataques DoS de red, destinadas a la protección de hosts específicos.

En concreto se ofrecen los siguientes mecanismos de prevención dentro de este módulo:

- **Flood Protection.** Detecta y previene los intentos de inundación con paquetes que terminan creando demasiadas sesiones a medio completar o consumiendo todos los recursos de algún servicio concreto.

  En este tipo de ataque la dirección IP origen suele estar falseada. Este mecanismo puede comenzar a bloquear paquetes en base a perfiles agregados o clasificados, tan pronto como los umbrales configurados se exceden.

- **Resources Protection.** Detecta y previene los intentos de consumir las sesiones de algún servicio. Este tipo de ataque se realiza utilizando una gran cantidad de hosts origen (denominados bots) para crear tantas sesiones completas como sea posible.

  Es más complicado de detectar que el anterior porque las sesiones pueden utilizarse para enviar tráfico que parezca legítimo a los hosts objetivo. El módulo puede limitar la cantidad de sesiones disponibles, de nuevo en base a un perfil agregado o clasificado. Es importante señalar que es posible emplear ambos mecanismos en el mismo perfil de DoS.

La definición de los perfiles de protección "*DoS Protection*" depende en gran medida de qué tipo de servicios se quiere proteger y los usuarios que lo utilizarán. Puesto que cada entorno es diferente es necesario en general hacer un análisis previo, al igual que ocurría con "*Zone Protection*".

Es importante poner especial atención a los siguientes factores:

Valores por defecto. Los valores por defecto no representan valores que se deban considerar como buenas prácticas. Los umbrales deben ser configurados en base a la información real de sesiones para el entorno en cuestión en el que se desean aplicar.

Un mecanismo adecuado para obtener esta información es configurar el reporting a través de Netflow en el cortafuegos y enviarlo a un analizador que lo interprete.

Para obtener información detallada sobre cómo configurar Netflow en los cortafuegos de Palo Alto Networks se puede consultar:
https://www.paloaltonetworks.com/documentation/7.1/CLI

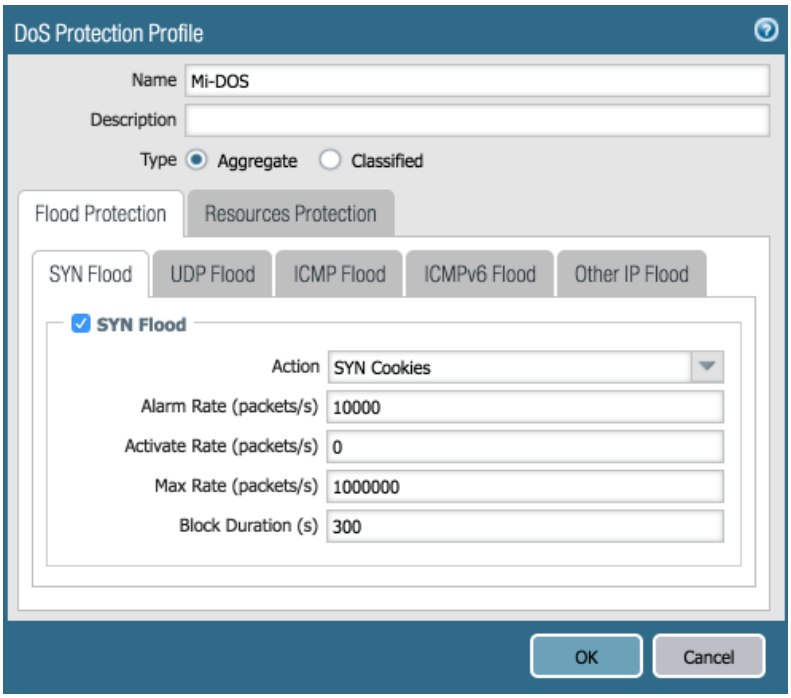


Figura 7.- Ejemplo de protección con los valores por defecto.

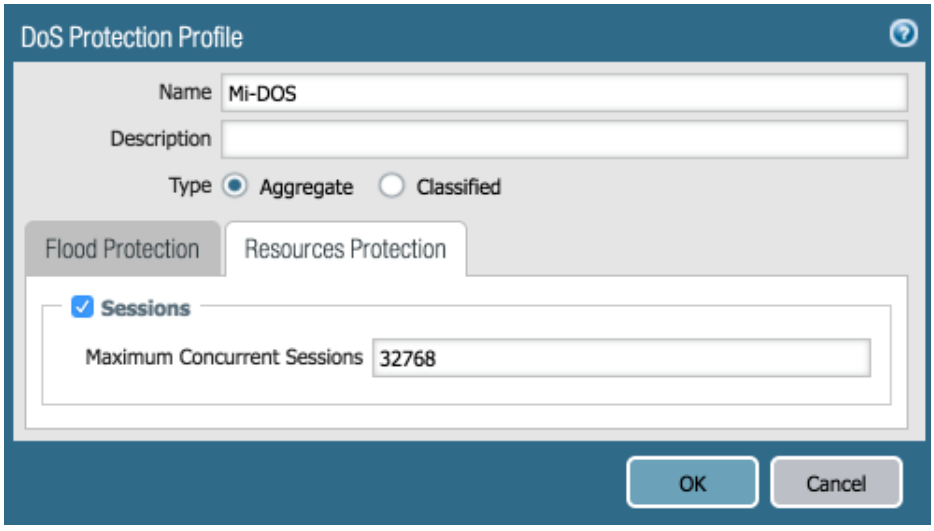


Figura 8.- Ejemplo de Flood Protection en un perfil de Dos Policies

Ratios Máximos. Cuando se exceden los umbrales establecidos en los "*Maximal Rate*" cualquier paquete que haga match con la política de "*Protection*" de DoS, y el criterio de clasificación si se utiliza un perfil de tipo "*Classified*", será descartado.

El valor por defecto para SYN-cookie es 1000000 lo que hará que en la mayoría de los entornos no se dispare y, por tanto, es necesario ajustar los valores adecuados para los siguientes escenarios:

- Para ofrecer protección frente a inundaciones de tipo TCP SYN, cuando se utiliza como mecanismo de defensa RED.
- Para ofrecer protección frente a inundaciones de tipo UDP, ICMP u otras.

Cuando se utiliza SYN Cookies como mecanismo de prevención frente a ataques de tipo SYN Flood, en lugar de RED, el mecanismo ya ofrece protección en sí mismo y por ese motivo el

valor "*Maximal Rate*" no ofrece protección adicional a ningún servicio excepto al propio servicio de SYN-Cookie del cortafuegos.

Perfiles agregados vs clasificados. Cuando se configuran los umbrales DoS para "*Flood Protection*" y "*Resource Protection*", es importante comprender la diferencia entre perfiles de tipo agregado y clasificado:

- **Agregado.** Los umbrales DoS definidos en el perfil se aplican a todos los paquetes que hagan match con el criterio definido en la regla de DoS en cuestión. Por ejemplo, una regla agregada con una protección frente a flujos UDP de 10000 paquetes por segundo (pps), cuenta todos los paquetes que hagan match con esa regla particular.
- **Clasificado.** Los umbrales de DoS definidos en el perfil se aplican a todos los paquetes que hagan match con la regla y también con el criterio de clasificación, que puede ser "*source IP*", "*destination IP*" o "*source and destination IP*". Por ejemplo, una regla clasificada con una protección frente a flujos UDP de 10000 pps y un criterio de clasificación de tipo "*source-ip*", comienza a descartar paquetes cuando una dirección IP origen en concreto alcanza ese umbral y solamente descartará paquetes para ese origen.

A partir de estas definiciones se puede inferir que los perfiles agregados son la mejor opción para protegerse frente ataques que vengan desde Internet. Un perfil clasificado para Internet es menos apropiado porque puede haber múltiples clientes detrás de una dirección de NAT y porque además es posible saturar la tabla de sesiones dada la diferente cantidad potencial de direcciones IPv4 e IPv6.

Por el contrario, para clientes internos que no estén detrás de una dirección IP de NAT, una clasificación basada en "source-ip" es probablemente la mejor opción para controlar el uso de los recursos. Por ejemplo, en los entornos educativos, donde los usuarios internos pueden en muchas ocasiones utilizar cualquier software, como p2p que consume muchos recursos, se puede utilizar un perfil clasificado para limitar el número de sesiones concurrentes por cliente y prevenir la saturación.

SYN-cookie vs Random Early Drop. El mecanismo de SYN-cookie es superior para contrarrestar los ataques de tipo SYN Flood y, por tanto, es preferible frente a RED.

Para cualquier otro tipo de inundación, RED es la única opción. Este algoritmo comienza a descartar paquetes de manera aleatoria si la ratio de paquetes por segundo se encuentra entre los valores "*Activate Rate*" y "*Maximal Rate*".

La probabilidad de descarte se incrementa linealmente con la ratio de paquetes. Si la ratio de paquetes excede el "*Maximal Rate*", entonces todos los paquetes en exceso son descartados.

Cuando se usan SYN Cookies, y desde la versión de PAN-OS 4.0 y posteriores, la ratio de activación "*Activate Rate*" se configura por defecto a 0 porque el mecanismo es determinista y por tanto no introduce falsos positivos.

4.2.1 CASO DE USO

En el ejemplo se va a suponer que se tiene un servidor web en una DMZ para el que se configurará un perfil de DoS que proteja el servidor frente a ataques de tipo SYN Flood y también frente al uso excesivo de sesiones.

Perfil de DoS Protection. Para la protección frente a ataques de tipo SYN Flood, se recomienda utilizar el mecanismo de SYN-Cookies mejor que el de RED, ya que ofrece mejor cobertura. Para evitar el abuso de las sesiones, deben considerarse las ventajas y desventajas de las siguientes técnicas y elegir la más apropiada o una combinación de varias:

- Usar un perfil clasificado que limite las conexiones concurrentes usando como clasificador "*source-destination-ip*". Esta medida reducirá el impacto que puede crear el ataque desde una botnet y mantendrá el servicio disponible para los usuarios legítimos.

  Si el límite es demasiado bajo puede afectar a los clientes que accedan al servicio web detrás de una dirección IP de NAT. Si por el contrario es muy alto, es fácil para una botnet poder llegar a consumir todas las sesiones disponibles.

- Usar un perfil agregado en combinación con información de dirección IP geolocalizada en la regla de protección DoS.

  Un perfil agregado en sí mismo no es suficiente para prevenir un ataque que agote las sesiones, pero combinado con información "*geo-IP*" puede reducir el impacto de un ataque DDoS global. Esta aproximación es válida si la audiencia del servicio web reside en un conjunto determinado de países.

- Usar un perfil clasificado incluyendo límite de sesiones concurrentes usando como criterio "*source-destination-ip*" junto con datos de localización "*geo-IP*".

  Esta aproximación requerirá algún tiempo de ajuste, pero puede ser muy efectiva una vez implantada.

Reglas de DoS Protection. Una vez que los perfiles de protección DoS necesarios han sido definidos, hay que configurarlos sobre una o varias reglas de protección DoS para activarlos. Las reglas de DoS definen los parámetros de origen y destino sobre los que el perfil se aplicará. Es recomendable intentar que las reglas sean lo más específicas posibles.

En este ejemplo se definirá una regla para cada servicio a proteger. De esta manera, los umbrales aplicarán solamente al servidor definido en la regla y no a los demás.

La siguiente figura muestra un ejemplo de regla de DoS en combinación con información "*geo-IP*". En concreto, se trata de un perfil clasificado por dirección IP origen y destino, que se aplica para todos aquellos orígenes que no vengan desde direcciones IP españolas:

			Source			Destination				Protection	
	Name	Tags	Zone/Interface	Address	User	Zone/Interface	Address	Service	Action	Aggregate	Classified
1	Proteccion Web	none	Internet	ES	any	DMZ	Servidor-web-e...	any	protect	none	profile: Mi-DoS src-dest-ip-both

Figura 9.- Ejemplo de política DoS

Flood Protection. Cuando se dispara el mecanismo, se envían los logs de alerta al log de amenazas (*Threat Log*). Los logs mostrarán entradas diferentes para el origen y destino del ataque en función del tipo de protección configurada.

Así, cuando se utilizan perfiles agregados tanto el origen como el destino mostrarán la dirección 0.0.0.0 y no se ofrece información de zona. Cuando por el contrario se utilizan perfiles clasificados, el log mostrará la información de origen y destino siempre y cuando forme parte del criterio de clasificación. El puerto de destino siempre se muestra como 0.

En la siguiente imagen se puede ver un log de cada tipo. El primero es de un perfil agregado, mientras que el segundo es de un perfil clasificado por origen y, como tal, en el log se muestra la dirección IP origen que creó la entrada.

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
		11/17 19:35:44	flood	UDP Flood	LAN	Internet	192.168.3.25	0.0.0.0	0	not-applicable	random-drop	critical
		11/17 19:31:05	flood	UDP Flood			0.0.0.0	0.0.0.0	0	not-applicable	random-drop	critical

Figura 10.- Ejemplo de logs de Flood Protection

Resource Protection. Cuando se dispara el mecanismo, se envían los logs de alerta al log de amenazas (*Threat Log*) generándose un log de nombre "*Session Limit Event*". Los logs mostrarán entradas diferentes para el origen y destino del ataque en función del tipo de protección, siguiendo la misma lógica descrita en el punto anterior.

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
		11/17 19:42:33	flood	Session Limit Event			192.168.3.25	0.0.0.0	0	not-applicable	drop	critical

Figura 11.- Ejemplo de log de Resource Protection

Es importante tener en cuenta que los equipos de Palo Alto Networks agregan por defecto los logs que son idénticos cada 5 segundos, con el fin de evitar inundar el sistema de logging. No obstante, almacenan en un campo del log extendido, denominado "*Repeat Count*", el volumen total de eventos recibidos para esa entrada, tal y como puede verse en la siguiente imagen.

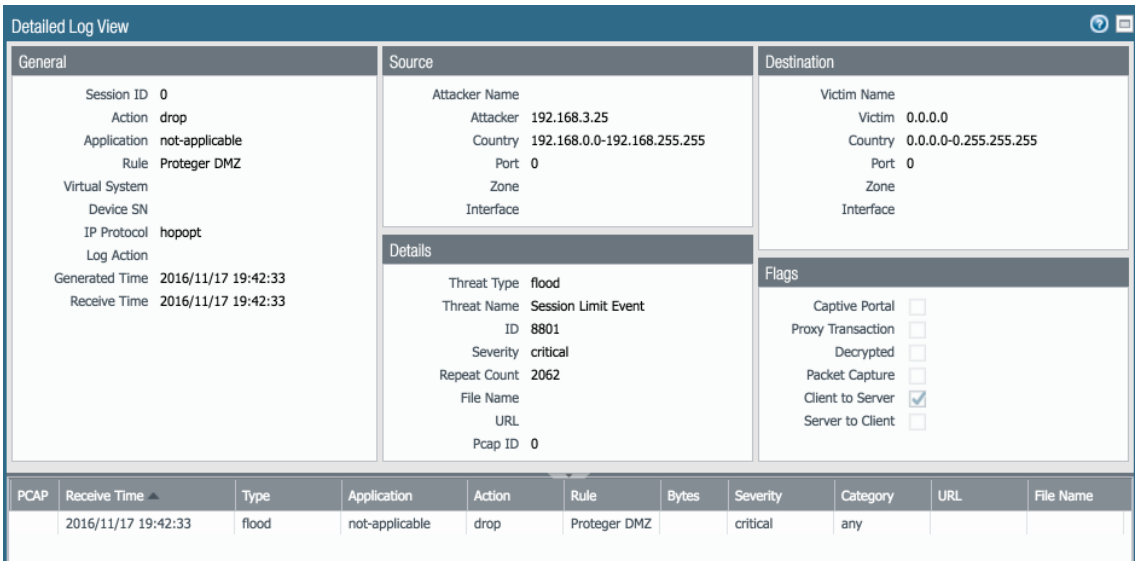


Figura 12.- Ejemplo de log detallado donde se observa el número de eventos totales agregados

5. PREVENCIÓN DE ATAQUES DOS EN FORTINET

FortiOS, sistema operativo de los dispositivos FortiGate, incorpora mecanismos de protección frente a ataques DoS basados en IPv4 e IPv6.

Gracias a la arquitectura hardware de FortiGate, basada en la combinación de CPU de propósito general y procesadores ASIC, como los Content Processors (CP) y Network Processors (NP), el dispositivo FortiGate es capaz de proporcionar un elevado número de sesiones nuevas por segundo y sesiones concurrentes, lo que proporciona altos niveles de protección frente a tipo de ataques DoS.

La protección DoS de FortiOS identifica tráfico potencialmente peligroso, que podría ser parte de un ataque DoS buscando anomalías específicas en el tráfico. Las anomalías del tráfico de un ataque DoS incluyen: TCP SYN floods, UDP floods, ICMP floods, escaneo de puertos TCP, ataques de sesión TCP, ataques de sesión UDP, ataques de sesión ICMP y ataques ICMP sweep.

FortiOS aplica la protección DoS en una fase temprana, cuando se está procesando la secuencia del tráfico, para minimizar el impacto de un ataque DoS en el rendimiento del propio equipo.

La protección DoS es el primer paso para los paquetes que se reciben en la interface de red del FortiGate. También se incluye una funcionalidad de lista de control de acceso (ACL), que utiliza el procesador NP6 para bloquear el tráfico (incluyendo ataques DoS) identificado por una dirección IP de origen, dirección IP de destino y servicio antes de que los paquetes sean enviados a la CPU del sistema.

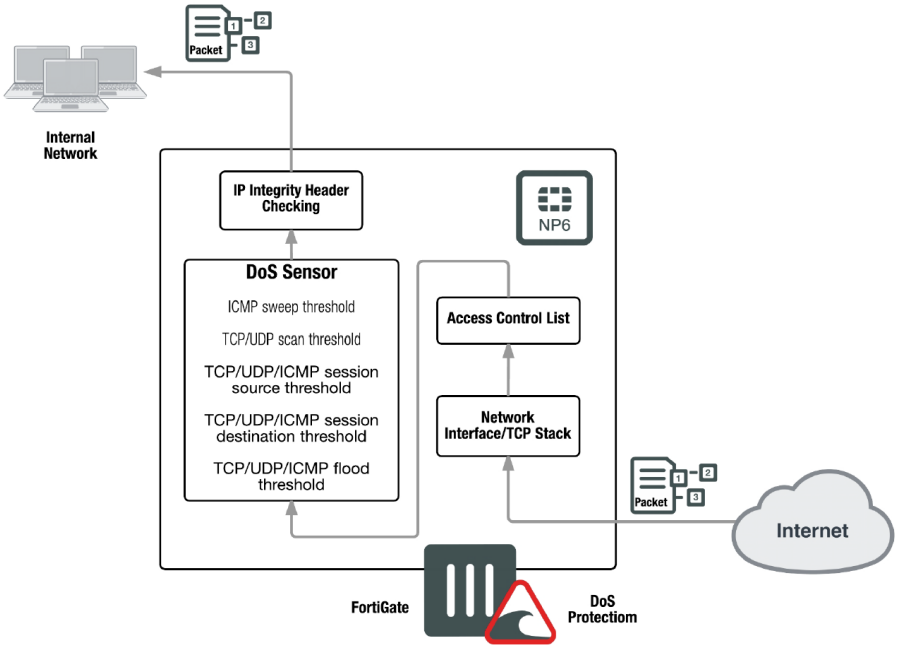


Figura 13.- Arquitectura NP6 en ataques DoS

La protección DoS de FortiGate puede operar en una configuración estándar o fuera de banda (en modo sniffer o one-arm), de forma similar a un sistema de detección de intrusión (IPS). Cuando el FortiGate opera en modo sniffer, los ataques pueden ser detectados y monitorizados, pero no se pueden bloquear.

Las políticas DoS de FortiOS determinan la acción a realizar cuando un tráfico anómalo alcanza el límite configurado por el administrador en el sistema. Se puede bloquear un atacante, bloquear una interface o permitir que el tráfico pase para únicamente monitorizarlo. Esto permite obtener información sobre los ataques, monitorizar el tráfico potencialmente dañino o bloquearlo.

Los equipos de FortiGate con procesador NP6 también soportan la protección DoS SYNproxy, que protege de ataques de tipo TCP SYN flood, ya que es el procesador NP6 quien detecta anomalías TCP SYN antes de que el tráfico sea procesado por la CPU principal.

Además de la protección frente ataques DoS, FortiOS incluye funcionalidades anti DDoS, previniendo la propagación de botnets y la actividad de mando y control de éstas (C&C), pudiendo monitorizar y bloquear intentos de conexión con botnets. La monitorización permite localizar y eliminar clientes de botnet dentro de la red y bloquear de manera preventiva los sistemas infectados que intentan comunicarse con sitios botnet.

5.1 POLÍTICAS DOS IPV4 E IPV6

Las políticas DoS se configuran para monitorizar y parar el tráfico con patrones o atributos anormales, reconociendo el tráfico como una amenaza cuando alcanza un umbral configurado por el administrador. La política determina entonces la acción apropiada (dejar pasar o bloquear la amenaza) así como escribir en los logs cada tipo de anomalía.

La protección de anomalías DoS se aplica a todo el tráfico entrante de una determinada interface, pero es posible delimitar en las políticas sobre qué tipo de servicio, dirección IP de origen o de destino aplica la política. El equipo procesará las políticas DoS en el orden establecido antes de procesar las políticas de cortafuegos.

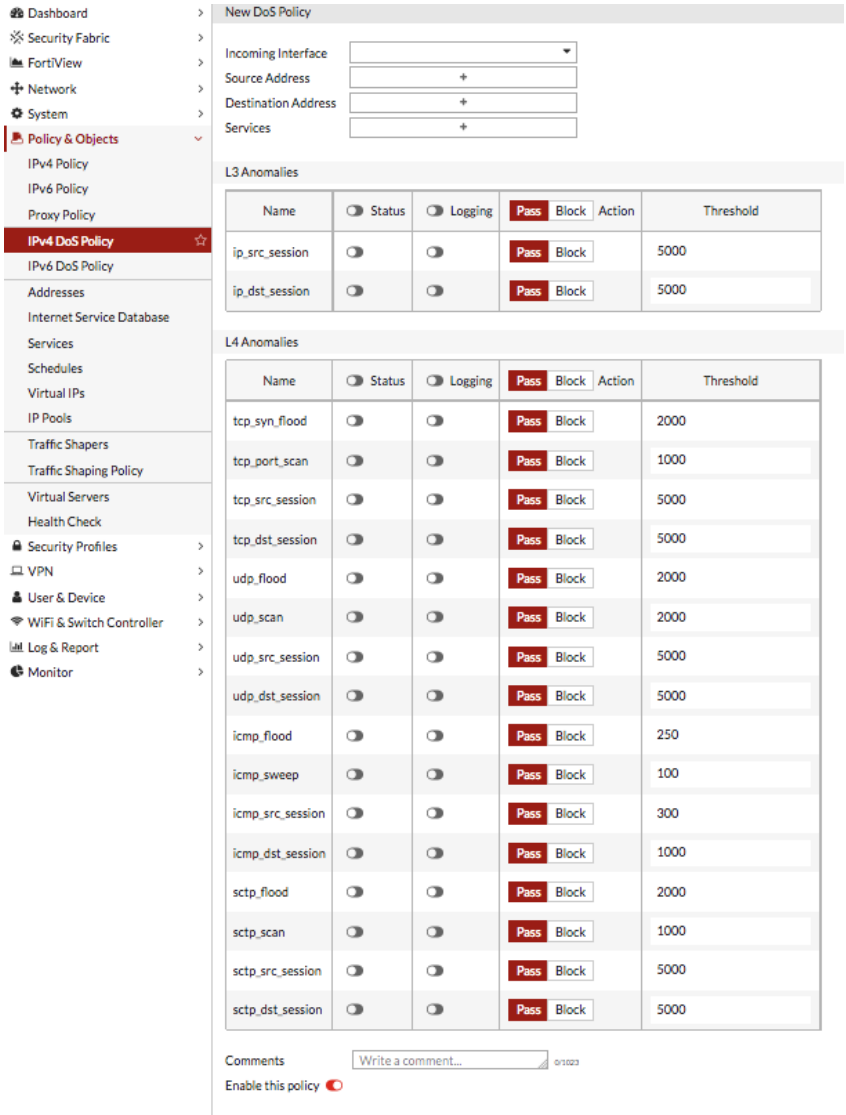


Figura 14.- Detalle de configuración de políticas DoS en FortiOS v.5.6

5.2 RECOMENDACIONES POLÍTICAS DOS

Es importante configurar unos umbrales máximos de número de sesiones/paquetes por segundo adecuados. Cuando se exceda el límite, la acción configurada se ejecutará. Los umbrales por defecto son recomendaciones generales, pero deben ajustarse a la casuística de cada entorno.

Un modo de encontrar los umbrales correctos en cada entorno, es configurar inicialmente la acción "*pass*" y habilitar el log. Tras observar los logs, se pueden ajustar los umbrales hasta que se pueda determinar el valor para el cual el tráfico normal se considera un ataque. Configurar el umbral en valores por encima de este con un margen considerando que cuanto más pequeño es este margen más protegido estará el sistema de ataques DoS, pero también estará más expuesto a generar falsas alarmas.

5.3 PROTECCIÓN DOS EN EL MOTOR DE INSPECCIÓN IPS

Las firmas IPS de FortiGate protegen de ataques DoS para determinado software que presentan ciertas vulnerabilidades. Se recomienda mantener la suscripción FortiGuard IPS para asegurar que el equipo recibe automáticamente las actualizaciones de firmas IPS cada vez que son publicadas.

Además, el motor de inspección IPS dispone de cerca de 30 firmas basadas en "*rate-limits*" que el administrador puede ajustar a sus necesidades para proteger la red de ataques DoS basados en aplicación y en fuerza bruta. Los umbrales (incidentes por minuto) y la acción asociada que debe ejecutarse al superar el límite, puede ser asignada a cada una de las firmas. Cuando la acción seleccionada es bloquear, se puede establecer también el tiempo que permanecerá activo dicho bloqueo.

En FortiOS 5.6, la configuración de firmas "*rate based*" se realiza editando los distintos sensores IPS en el menú *"Security Profiles" -> "Intrusion Prevention"*.

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
	Apache.HTTP.Server.DoS	200	1	Any	Block	None
	Apache.HTTPD.mod_http2.DoS	300	1	Any	Block	None
	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	None
	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	None
	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	None
	FTP.Login.Brute.Force	200	10	Any	Block	None
	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	None
	GlassFish.Login.Brute.Force	200	10	Any	Block	None
	IMAP.Login.Brute.Force	60	10	Any	Block	None
	Iomega.StorCenter.Pro.NAS.Web.Authentication.Bypass	1000	10	Any	Block	None
	Lotus.Domino.Login.Brute.Force	300	10	Any	Block	None
	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	None
	MS.OWA.Brute.Force	15	1	Any	Block	None
	MS.RDP.Connection.Brute.Force	200	10	Any	Block	None
	MS.Windows.Group.Policy.Security.Feature.Bypass	5	2	Any	Block	None
	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	Block	None
	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	Block	None
	MS.Windows.Server.DNS.Response.Caching.Code.Execution	100	1	Any	Block	None
	MS.Windows.UDP.Remote.Code.Execution	100	10	Any	Block	None
	MS.Windows.WPAD.Proxy.Discovery.Privilege.Elevation	500	5	Any	Block	None
	MS.Windows.WPAD.Proxy.Discovery.Response.Privilege.Elevation	2000	1	Any	Block	None
	MS.XML.Core.Services.Memory.Corruption	5	10	Any	Block	None
	MySQL.Login.Brute.Force	60	60	Any	Block	None
	Novell.Open.Enterprise.Server.HTTPSTK.SSL.Free.DoS	10	1	Any	Block	None
	Novell.eDirectory.SOAP.Request.Parsing.DoS	4	2	Any	Block	None
	OpenSSH.kbdint_next_device.Policy.Bypass	30	60	Any	Block	None
	OpenSSL.Private.DH.exponent.Disclosure	35	10	Any	Block	None
	Oracle.Application.Server.SID.Brute.Force	300	10	Any	Block	None
	Oracle.MySQL.Server.InnoDB.Memcached.Plugin.DoS	60	1	Any	Block	None
	Oracle.XML.DB.SID.Brute.Force	300	10	Any	Block	None

Figura 15.- Detalle de las firmas "Rate Based" de IPS

5.4 HOST PROTECTION ENGINE (HPE)

Los equipos FortiGate equipados con el procesador NP6 disponen de la funcionalidad HPE, que puede proteger la red de ataques DoS categorizando los paquetes entrantes basándose en la ratio de paquetes y el coste de procesamiento para aplicar "*packet shaping*" a aquellos paquetes que puedan causar un ataque DoS.

Esta característica se puede configurar desde el CLI de FortiGate para limitar el número máximo de paquetes por segundo recibidos de varios tipos de paquetes por cada procesador NP6.

Por defecto la protección HPE está deshabilitada. Se pueden utilizar los siguientes comandos para habilitarla (en este ejemplo para el procesador NP6_0).

```
config system np6
  edit np6_0
    config hpe
    set enable-shaper enable
  end
```

HPE se puede habilitar y configurar por separado para cada procesador NP6. Cuando se habilita, la configuración por defecto está diseñada para proporcionar una protección DoS básica.

Los siguientes comandos permitirán realizar ajustes de HPE en tiempo real cuando se esté experimentando un ataque.

```
config system np6
  edit np6_0
  config hpe
      set tcpsyn-max
      set tcp-max
      set udp-max
      set icmp-max
      set sctp-max
      set esp-max
      set ip-frag-max
      set ip-others-max
      set arp-max
      set l2-others-max
      et enable-shaper {disable | enable}
end
```

Donde:

- **tcpsyn-max:** aplica el shaping basándose en el número máximo de paquetes TCP SYN recibidos por segundo. El rango 10,000 a 4,000,000,000 pps. El límite de paquetes por segundo por defecto es 5,000,000 pps.
- **tcp-max:** aplica el shaping en función del número máximo de paquetes TCP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 5,000,000 pps.
- **udp-max:** aplica el shaping en función del número máximo de paquetes UDP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 5,000,000 pps.
- **icmp-max:** aplica el shaping en función del número máximo de paquetes ICMP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 1,000,000 pps.
- **sctp-max:** aplica el shaping en función del número máximo de paquetes SCTP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 100,000 pps.
- **esp-max:** shaping NPU HPE basado en el número máximo de paquetes IPSEC ESP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 100,000 pps.
- **ip-frag-max:** aplica el shaping en función del número máximo de paquetes IP fragmentados recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 100,000 pps.
- **ip-others-max:** aplica el shaping en función del número máximo de otros paquetes IP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 100,000 pps.
- **arp-max:** aplica el shaping en función del número máximo de paquetes ARP recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 1,000,000 pps.

- **I2-others-max:** aplica el shaping en función del número máximo de otros paquetes de capa 2 recibidos. El rango es 10,000 a 4,000,000,000 pps. Por defecto 100,000 pps.

5.5 PROTECCIÓN COMPLETA ANTI-DDOS CON FORTIDDOS

La protección que brindan los cortafuegos frente a ataques de DDoS es limitada y radica en su propia naturaleza: estos dispositivos solo aplican mitigación de dichos ataques basados en "*rate limit*", es decir, en base al número total de conexiones o al número de conexiones por segundo que se establecen para una determinada regla o servicio.

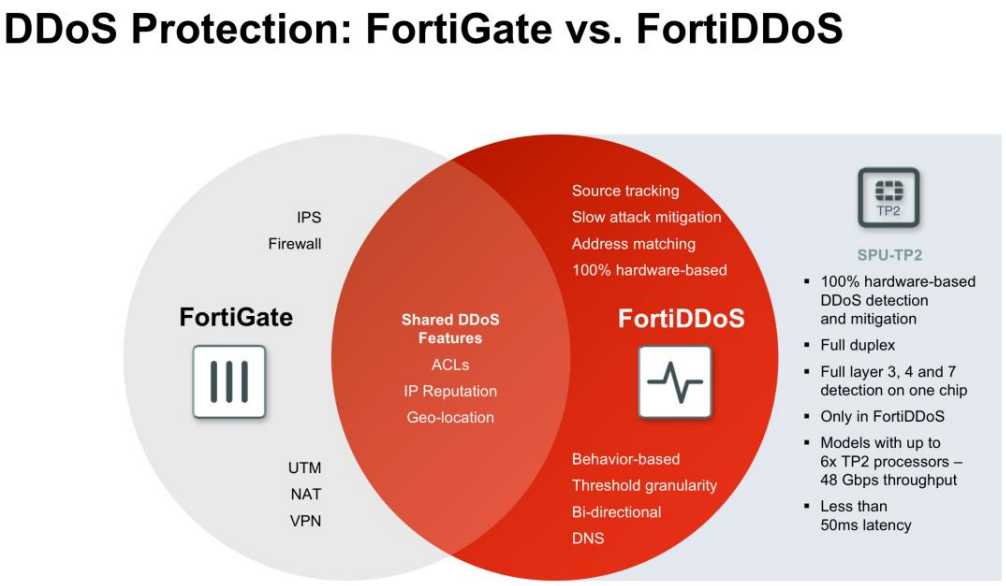


Figura 16.- FotiGate vs. FortiDDoS

Este método es efectivo para salvaguardar los elementos de la infraestructura interna (servidores web, routers, switches, etc.) ante un ataque de DDoS, en el sentido de que sus recursos no se verán sobrepasados, pero el servicio que prestan se verá interrumpido igualmente, haciendo que el ataque de DDoS tenga éxito de todas formas: una vez alcanzados los límites configurados en la política, el tráfico se descartará sin hacer distinción entre tráfico legítimo y tráfico que pertenece al ataque.

Además, los valores que se pueden configurar para limitar dichas variables (conexiones concurrentes y conexiones por segundo) serán fijos y no se adaptan al tráfico cambiante en cada momento, lo que lleva en la mayoría de las ocasiones a la detección de ataques falsos:

- **Si el umbral es muy bajo:** falso positivo, cuando un tráfico que siendo legítimo excede los umbrales establecidos y se descarta por parecer un ataque.
- **Si el umbral es muy alto:** falso negativo o la no detección de ataques reales que no llegan a exceder el umbral.

Aparte de lo comentado hasta ahora, los cortafuegos son más sensibles a determinados tipos de ataques de DDoS con paquetes fragmentados, en los que estos equipos tratarán de reconstruir toda la información antes de poder decidir si se trata de tráfico legítimo o no, o a ataques de capa 7 (de aplicación), o a ataques llamados "*Low and Slow*", que son peticiones legítimas que no generan mucho tráfico, pero que buscan consumir los recursos de los servicios de forma que nadie pueda acceder a ellos.

Por todo ello, Fortinet dispone de una solución específica para la protección frente a ataques DoS/DDoS, llamada FortiDDoS (FDD). Esta solución se basa en el estudio del comportamiento dinámico del tráfico y en la detección de anomalías en tiempo real y su mitigación. Las ventajas de desplegar una solución dedicada para este tipo de amenazas son las siguientes:

- Monitorización de todo el tráfico de la red, con lo que la detección y la mitigación se realiza en menos de 2 segundos a velocidad de línea.
- Adaptación dinámica a los cambios de tráfico, realizando la distinción entre tráfico legítimo y malicioso, y mitigando solo este último.
- Protección frente a todos los vectores de ataque de nivel 3, 4 y 7 (nivel IP, nivel de transporte y nivel de aplicación) y Zero Day.
- Protección frente a ataques de inundación "*Flood*", de paquetes fragmentados, los denominados "*Low and Slow*" y ataques de amplificación contra servicios de DNS, NTP u originados por dispositivos IoT (Internet of Things).
- Informes específicos sobre los detalles de los ataques: tipo, atacantes y servicios atacados en cada momento.

En definitiva, un equipo dedicado como el FDD debería ser la primera línea de defensa.

6. DECALOGO BÁSICO DE SEGURIDAD

Este decálogo de buenas prácticas pretende sentar las bases en las medidas de seguridad frente a ataques DoS en cortafuegos.

	Decálogo Básico de Seguridad
1	La estrategia adecuada deberá ser siempre multicapa, involucrando varios elementos así como al proveedor de servicios de Internet.
2	Deben separarse los elementos internos y externos (o más expuestos) en la protección ya que requerirán distintas medidas.
3	En zonas externas emplear métodos basados en número máximos de paquetes permitidos y reconocimiento de patrones conocidos.
4	Para equipos específicos en zonas internas aplicar mecanismos de control de número de sesiones y consumo de recursos de servicios.
5	Los valores por defecto no representan valores que se deban considerar como buena práctica.
6	Para determinar umbrales máximos, hacer un estudio del tráfico real que debe realizarse periódicamente para detectar cambios.
7	Mantener actualizados los paquetes de firmas de patrones de ataques conocidos.
8	Analizar periódicamente los logs generados para estudiar los eventos de seguridad (positivos y negativos) que no han sido bloqueados o que no se han detectado.
9	Prevenir, monitorizar y bloquear la propagación de botnets y la actividad de servidores de mando y control de éstas (C&C).
10	Valorar soluciones específicas para la protección frente a ataques DoS/DDoS.

Figura 17.- Decálogo de seguridad

REFERENCIAS

- Guía de seguridad de las TIC (CCN-STIC-820). Guía de protección contra Denegación de Servicio.
- Guía de seguridad de las TIC (CCN-STIC-652). Guía de seguridad cortafuegos Palo Alto.
- Guía de seguridad de las TIC (CCN-STIC-650). Guía de seguridad en Fortigate.