Protección DDoS de F5: Prácticas recomendadas (Volumen 1)

La denegación de servicio distribuida (DDoS) es una de las principales preocupaciones de muchos organizaciones de hoy en día, desde marcas de alto perfil del sector financiero hasta proveedores de servicios. Los administradores experimentados saben que F5 los equipos no sólo son adecuados para...

Libro blanco

por David Holmes

1 Concepto

La denegación de servicio distribuida (DDoS) es una de las principales preocupaciones de muchas organizaciones hoy en día, desde marcas de alto nivel del sector financiero hasta proveedores de servicios. Experiencia en los administradores saben que los equipos de F5 no sólo son adecuados para mitigar los DDoS ataques, pero a veces es el único equipo que puede mitigar ciertos tipos de DDoS. Lo que muchos administradores no saben es que un sistema completo en las instalaciones la solución DDoS puede lograrse con un complemento de productos F5.

Un ataque DDoS puede ser un compromiso estresante donde partes de la red serán no responde y el equipo puede estar fallando por todas partes. Ese no es el momento de estar planificar una defensa: preparar sus aplicaciones de red en "tiempos de paz" será un largo camino para ayudarle a mitigar el ataque en el futuro.

Esta guía asume que usted tiene una solución de red de F5 y un F5 opcional solución de seguridad.

Se supone que todas las configuraciones, comandos y plataformas son de TMOS 11.3.0 a menos que se indique lo contrario.

Aunque gran parte de la información técnica es específica de los equipos F5, algunos de las estrategias (como el uso de grupos SNAT para evitar el agotamiento de los puertos) pueden aplicarse a los dispositivos de otros vendedores también.

2 Arquitectura resistente a DDoS

Es posible construir una red de entrega de aplicaciones que sea resistente a los DDoS. Este la sección analiza el trabajo que se puede hacer antes de un ataque para que la red y aplicaciones resistentes.

2.1 Arquitectura recomendada por F5

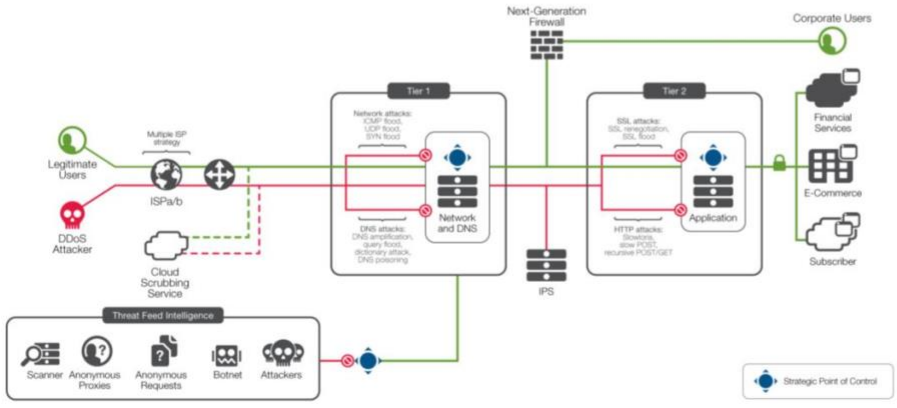


Figura 1: F5 recomienda un enfoque de DDoS de dos niveles

Muchas organizaciones están rediseñando su arquitectura para la resistencia a los DDoS. Para muchos clientes, F5 recomienda una solución DDoS de dos niveles, donde el primer nivel (perímetro) se compone de una red de capa 3 y 4 firewalling y un simple equilibrio de carga a un segundo nivel de servicios más sofisticados (y también más intensivos en cuanto a la CPU) que incluyen terminación de SSL y Firewalling de Aplicaciones Web.

El enfoque de dos niveles tiene varias ventajas:

- La mitigación puede aislarse para que las capas 3 y 4 se mitiguen en el nivel 1, con protección de aplicaciones en el nivel 2.
- Los niveles pueden ser escalados independientemente unos de otros. Por ejemplo, si WAF
  Si el uso crece, se puede añadir otro aparato (o blade) al segundo nivel sin afectar al primer nivel.
- Los niveles pueden tener diferentes tipos de plataforma e incluso diferentes programas informáticos versiones.
- Cuando se aplican nuevas políticas en el segundo nivel, el primer nivel puede dirigir sólo un parte del traffic a las nuevas políticas hasta que estén completamente validadas.

	Nivel 1	Nivel 2	DMZ
Componentes F5	AFM + LTM	LTM + ASM	GTM DNS Express
Modelo OSI	Capas 3 + 4	Capa 7+	DNS
Capacidades	Cortafuegos de red	Terminación SSL	
	Equilibrio de carga de primer nivel	Cortafuegos de aplicaciones web	Resolución del DNS
	Listas negras de reputación IP	Equilibrando	
Ataques mitigados	Inundaciones SYN	Slowloris	
	Inundaciones ICMP	Puesto lento	Inundaciones de la UDP
	Paquetes malformados	Asesino de apaches	Inundaciones de DNS
	Inundación TCP	RUDY / Manténgase muerto	Inundaciones NXDOMAIN
	Actores malos conocidos	Renegociación SSL	DNSSEC

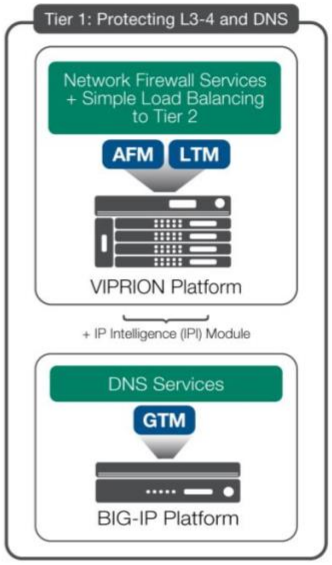
2.2 Nivel 1: Defensa de la red

El primer nivel se construye alrededor del muro de la red. Es casi seguro que ya tiene un red firewall (puede o no ser F5) y un equipo de red firewall (o al menos un administrador). En este nivel preparará las defensas en torno a las capas 3 y 4 (IP y TCP). Aquí es donde se mitigan los floods SYN, los floods TCP y se bloquea la Fuente direcciones durante un ataque DDoS.

Las siguientes secciones se aplican al equipo del nivel 1, ya sea el F5 AFM Módulo firewall o un equilibrador de carga F5 LTM frente a la red de otro proveedor firewall.

2.2.1 Elección de los tipos de servidores virtuales

Las organizaciones que utilizan el F5 firewall (AFM) o el F5 load-balancer (LTM) en el nivel 1 tienen una opción sobre cómo estructurar su configuración. Hay cuatro opciones para definir un objeto de "escucha". Aunque todas estas son formas válidas de organizar el configuración, algunos tienen diferentes puntos fuertes cuando se trata de DDoS.



- Los servidores virtuales Full-Proxy son los servidores virtuales estándar en un F5 configuración. Estos oyentes establecen una conexión real con cada uno de los cliente antes de iniciar una conexión secundaria con el servidor. El propio acto de la terminación y validación de la conexión del cliente proporciona una amplia gama de protección antes de que se invoque el segundo nivel.

- Los **servidores virtuales de reenvío** funcionan más rápido y siguen protegiendo contra SYN floods, pero no proporcionan el nivel más amplio como la protección que el proxy virtual complete los servidores lo hacen.

- Los servidores virtuales comodín permiten **desacoplar las reglas de firewall del servidor virtual de aplicaciones**. Esto permite la creación de una regla que dice "para cualquier dirección que suministre servicios FTP, aplique este conjunto de reglas, esta política de duplicación, y esta política de NAT de origen".

- Los **Dominios de Ruta**, que aíslan las subredes IP duplicadas en redes lógicas y separadas tablas de enrutamiento, son comunes en los entornos de los proveedores de servicios. Mientras que la ruta los dominios proporcionan poco o ningún beneficio con respecto a los DDoS en sí mismos, pero pueden utilizarse como clavijas en las que colgar las políticas de seguridad de la capa 4.

Figura 2: Los servidores comodín son una opción en el nivel 1

```
ltm virtual ws_ftp {
destino 0.0.0.0:ftp
protocolo ip tcp
perfiles { ftp { } tcp { } }
traducir-dirección deshabilitada
}
```

En general, **F5 recomienda el uso de Proxy Completo o Reenvío Virtual Servidores** en el nivel 1 cuando el DDoS es una de las principales preocupaciones.

2.2.2 Mitigar los floods SYN en el nivel 1

Los floods TCP SYN son siempre mitigados por F5. En la versión 11.5, F5 incluso migra SYN floods contra servidores virtuales de Retorno Directo del Servidor (DSR). Para verificar que su BIG-IP es gestionar la protección de SYN flood, puede ver las estadísticas de SYN flood de cada individual del servidor virtual con el simple comando **show**.

```
% tmsh show ltm virtual vip1
…

Cookies SYN

  Estado del software
  completo

  Instancias de cookies de hardware SYN
  0

  Software SYN Cookie Instances 2

  Caché SYN actual 0

  Desbordamiento de la
  caché SYN 0

  Total Software 432.2K

  Total de programas informáticos
  aceptados 0

  Total de programas informáticos
  rechazados 0

  Total Hardware 0
  Total de equipos aceptados 0
```

Muchas plataformas F5 pueden mitigar los floods SYN en el hardware, lo que permite que el principal CPUs de dirección de traffic para realizar otras tareas.

Plataforma	Hardware SYNs por segundo	Versión
Cuchilla B4300	80M	11.3
Cuchilla B2100	40M	11.3
10200V	80M	11.3
10000S	40M	11.4
7200V	40M	11.4
7000S	20M	11.4
5200V	40M	11.4
5000S	20M	11.4
Las plataformas más antiguas, como las 8800, 8400, 6800 y 6400, también incluyen soporte de cookies SYN por hardware; sin embargo, estos modelos no son compatibles con la versión 11.3, que es la base de este documento.		

Tabla 1: Lista de plataformas compatibles con el hardware de SYN Flood

Para habilitar la carga de hardware para la mitigación de SYN flood para un servidor virtual específico, crear un profile tcp con una postura de seguridad más estricta. Este ejemplo establece dos DDoS- variables relacionadas. Activa **las cookies de** hardware **SYN**. También establece el **diferido-aceptar** la variable que reduce el impacto que pueden tener los ataques TCP de "ventana cero" en el servidor virtual.

```
% tmsh create ltm profile tcp tcp_ddos { hardware-syn-cookie deferre
d-accept
enabled zero-window-timeout 10000 }
```

A continuación, asocie el nuevo profile tcp con el servidor virtual sustituyendo el existente "tcp" profile.

```
% tmsh list ltm virtual vip1 profiles

% tmsh modify ltm virtual vip1 profiles replace-all-with { tcp_ddos
mi_ddos1
http }
```

2.2.3 Denegar UDP y UDP Floods en el nivel 1

Los floods UDP son un vector común de DDoS, porque son fáciles de generar y pueden ser difícil de defender. En general, no permita el traffic de UDP a un servidor virtual a menos que el la aplicación que hay detrás la acepta activamente.

Incluso en el caso de las aplicaciones que aceptan UDP, un flujo de UDP puede saturar el sistema, y puede encontrar necesario negar temporalmente el tráfico UDP a la aplicación virtual servidor.

```
% tmsh create security firewall rule-list drop_udp { rules add { dro
p_udp_rule
{ action drop ip-protocolo  u d p   place-after first } } }

% tmsh modify ltm virtual vip1 fw-rules { drop_udp_vip1 { rule-list
drop_udp }
} }
```

Cuando el ataque haya cesado, puede eliminar la regla del servidor virtual.

La versión 11.5 puede supervisar y mitigar los floods UDP con excepciones granulares. Este permite que una línea base de trafficación UDP pase por un servidor virtual en el nivel 1. Si el UDP si el tráfico excede los umbrales, se descarta, a menos que coincida con uno de los ocho usuarios excepciones de puertos definidos (por ejemplo, RTSP o DNS).

2.2.4 Denegar inundaciones ICMP

ICMP es otro vector común de DDoS. Los fragmentos ICMP son fáciles de generar y fácil de falsificar, y puede ocupar recursos en muchos tipos de redes diferentes dispositivos.

AFM puede diferenciar entre una cantidad normal de ICMP y una flood basada en en el análisis de patrones de tráfico. Cuando el firewall de red de AFM está habilitado en una red virtual servidor, vigilará el aumento de varios tipos de traffic. Una cantidad normal será se permite, con el resto de la comida prohibida.

2.2.5 Utilizar el Profile de Dispositivo DDoS de AFM

Una de las formas en que los atacantes pueden consumir recursos del firewall es lanzando floods de paquetes no válidos especialmente diseñados. El firewall tendrá que mirar (y registrar) cada paquete. F5 ha descubierto que las combinaciones sospechosas de flags (como PSH+ACK con cargas vacías) puede ser popular un mes y luego ser abandonado en favor de un combinación diferente más tarde.

Este panorama cambiante hace que sea difícil predecir qué ataques L3/L4 es probable que se produzcan. El administrador de seguridad (para los firewalls de otros proveedores) debe ser conscientes de estos ataques y estar preparados para insertar reglas para bloquearlos, teniendo cuidado de evitar el uso de más CPU de lo necesario.

El enfoque de F5 a este problema ha sido trasladar gran parte del protocolo L3/L4 validación en la lógica de hardware personalizada en las plataformas TMOS que lo soportan. Por defecto, el módulo AFM supervisa docenas de ataques DDoS de capa 3 y 4 vectores como los paquetes de árbol de Navidad o los paquetes de ataque LAND. Casi todos los de estos paquetes se descartan independientemente de cualquier configuración de BIG-IP. AFM puede enviar un mensaje de registro especial cuando se detecta un flood de estos paquetes.

La tabla 1 muestra las plataformas TMOS que soportan L3/L4 asistida por hardware la validación del protocolo. Estas son las mismas plataformas que tienen hardware SYN flood apoyo.

Todas las plataformas (incluida la edición virtual) permiten gestionar los parámetros que rastrear estos paquetes sospechosos L3/L4 floods. La pantalla de gestión está disponible en la pestaña Seguridad de la interfaz de usuario. A continuación, seleccione **Protección DoS** y **Dispositivo Configuración**.

Attack Type	Detection Threshold PPS	Detection Threshold Percent	Default Internal Rate Limit
L2 Length >> IP Length	10000	500	100000
IPV6 Fragment	10000	500	100000
Payload Length < L2 Length	10000	500	100000
TCP Header Length Too Short (Length < 5)	10000	500	100000
IPV6 Source Address == Destination Address	100	500	1000
FIN Only Set	10000	500	100000
Header Length > L2 Length	10000	500	100000
Bad IPV6 Version	10000	500	100000
Bad IPV6 Hop Count	10000	500	100000
Bad TCP Checksum	10000	500	100000
IPV6 Length > L2 Length	10000	500	100000
ICMP Flood	100	500	500
Bad UDP Checksum	10000	500	100000
IP Length > L2 Length	10000	500	100000
IPV6 Extended Header Frames	10000	500	100000

Figura 3: Ajustes de configuración de la red DDoS

Estos ajustes también están disponibles a través de la línea de comandos con la **seguridad dos** comando **device-config**. También tenga en cuenta que estos ajustes son por gestión de traffic microkernel (tmm), no por plataforma. En la tabla, las columnas se corresponden con estos valores.

- **Umbral de detección PPS.** Es el número de paquetes por segundo (de este tipo de ataque) que el sistema BIG-IP utiliza para determinar si se está produciendo un ataque. Cuando el número de paquetes por segundo supera la cantidad umbral,

el sistema BIG-IP registra e informa del ataque, y luego sigue comprobando cada segundo, y marca el umbral como un ataque siempre que el umbral se sobrepasa.

- **Porcentaje de umbral de detección.** Es el valor de incremento porcentual que especifica que se está produciendo un ataque. El sistema BIG-IP compara la tasa actual a una tarifa media de la última hora. Por ejemplo, si la tarifa media de la última hora es de 1000 paquetes por segundo, y se establece el porcentaje de aumento umbral a 100, se detecta un ataque al 100% por encima de la media, o 2000 paquetes por segundo. Cuando se supera el umbral, se registra un ataque y se informa de ello. El sistema BIG-IP instituye entonces automáticamente un límite de velocidad igual a la media de la última hora, y todos los paquetes que superen ese límite se se ha caído. El sistema BIG-IP sigue comprobando cada segundo hasta que el la tasa de paquetes entrantes cae por debajo del umbral de incremento porcentual. Tasa la limitación continúa hasta que la tasa cae de nuevo por debajo del límite especificado.
- **Límite de velocidad interna por defecto.** Este es el valor, en paquetes por segundo, que no puede ser superado por paquetes de este tipo. Todos los paquetes de este tipo sobre el umbral se eliminan. La limitación de la tasa continúa hasta que la tasa cae por debajo del límite especificado de nuevo.

2.2.6 Mitigar las inundaciones de la conexión TCP

Los floods de conexión TCP son una anomalía de capa 4 y pueden afectar a cualquier dispositivo con estado en la red, especialmente los muros de seguridad. A menudo, estos archivos están vacíos de contenido real. LTM o AFM en el primer nivel puede mitigarlos absorbiendo las conexiones en tablas de conexión de gran capacidad.

Plataforma	Conexión TCP Tamaño de la tabla	Conexión SSL Tamaño de la tabla
VIPRION 4480 (4 X B4300)	144 millones	32 millones
VIPRION 4480 (1 X B4300)	36 millones	8 millones
VIPRION 4400 (4 X B4200)	48 millones	5 millones
VIPRION 4400 (1 x B4200)	12 millones	1 millón
VIPRION 2400 (4 x B2100)	48 millones	10 millones
VIPRION 2400 (1 x B2100)	12 millones	2,5 millones
Serie 11000	24-30 millones	2,64-3,9 millones
Serie 10200	36 millones	7 millones
Serie 8900	12 millones	2,64 millones

Plataforma	Conexión TCP Tamaño de la tabla	Conexión SSL Tamaño de la tabla
Serie 7000	24 millones	4 millones
Serie 6900	6 millones	660 mil
Serie 5000	24 millones	4 millones
Serie 4200V	10 millones	2,4 millones
Serie 3900	6 millones	660 mil
Edición virtual	3 millones	660 mil

2.2.7 Configurar la cosecha adaptativa

Incluso con tablas de conexión de alta capacidad, todavía hay ajustes que pueden ser ajustado para profundizar el profile de protección contra los ataques de flood.

En el caso de que la tabla de conexiones del BIG-IP se llene, las conexiones se "cosechado" según los ajustes de cosecha adaptativa de aguas bajas y aguas altas. Estos pueden ajustarse a la baja desde los valores por defecto de 85 y 95 para empezar a mitigar un DDoS "espinoso" más rápidamente, y así reducir la ventana durante la cual el ataque inicial cargará los servidores.

```
% tmsh modify ltm global-settings connection adaptive-reaper-lowater
  75
```

2.2.8 Modificar los tiempos de espera para combatir la conexión vacía Inundaciones

Aunque los floods de conexión de capa 4 no suelen suponer un alto riesgo para los dispositivos F5, sí que sin duda, afecta a otros dispositivos con estado, como otros firewalls. Estos dispositivos casi siempre se colapsan mucho antes de que las tablas de estado F5 se llenen (véase la Tabla 2 en la sección 2.2.6). Si la conexión flood está formada principalmente por conexiones vacías, puede instruir a BIG-IP para que sea más agresivo a la hora de cerrar estas conexiones vacías.

Hay tres profiles principales asociados a la capa 4 en BIG-IP:

- fastL4-el profile TCP de alto rendimiento asistido por hardware
- tcp-el profile TCP estándar utilizado por la mayoría de los servidores virtuales
- u d p - e l profile estándar UDP

Nota: Es posible que vea otros, como los asociados a la optimización de la WAN, que se basan en los profiles tcp o udp.

Utilice los siguientes atributos de estos profiles para controlar el tiempo de inactividad de una conexión antes de que sea cerrado por BIG-IP. Durante un ataque intenso, utilice valores cada vez más pequeños.

Para el profile fastL4, anule los valores de **reset-on-timeout** y **idle-timeout**. La dirección el tiempo de espera por defecto es de 300 segundos, que debe ser recortado significativamente durante un ataque.

```
% tmsh create ltm profile fastl4 fastl4_ddos { reset-on-timeout dis
abled idle- timeout 15 }
```

Para cada servidor virtual fastL4 atacado, sustituya la profile fastL4 por su nueva uno.

Para la profile tcp, anule los mismos dos valores por las mismas razones. Mientras allí, es posible que también desee ajustar el **hardware-syn-cookie** y el **zero-window-**valores de **tiempo de espera**. Véase el apartado 2.2.2.

Para el profile udp, reduzca sólo el valor del **tiempo de espera de inactividad** (el valor predeterminado es 60 segundos).

2.2.9 Control de la velocidad de la transmisión

Otra técnica defensiva que puede desplegarse rápidamente es el rate-shaping. La conformación puede limitar la tasa de traffic de entrada en el BIG-IP y puede ser la forma más fácil para hacer frente a un ataque volumétrico. Aunque es potente, el modelado de la tasa es un método menos...que una técnica ideal para defenderse de los DDoS. Porque no distingue entre las solicitudes buenas y las malas, el rate-shaping puede descartar su traffic buena también, que probablemente no es lo que quieres.

Se configuran manualmente los profiles de ajuste de velocidad y luego se asignan a un virtual servidor.

En este ejemplo, la clase de regulación de velocidad denominada "protect_apache" garantiza que en menos 1mbs de traffic alcanzará el objetivo, pero que no más de 10mbs serán permitido.

```
net rate-shaping class protect_apache { rate 1mbps ceiling 10mbps }
```

A continuación, aplique esta clase de regulación de la velocidad a cada uno de sus servidores virtuales objetivo.

2.2.10 Establecer la tasa máxima de rechazo de ICMP

La variable del sistema **TM.MaxRejectRate** puede reducir los efectos de una denegación de ataque de servicio permitiéndole limitar el número de RST TCP o ICMP paquetes inalcanzables que el sistema BIG-IP envía en respuesta a paquetes entrants conexiones que no pueden coincidir con las conexiones del servidor virtual. El valor por defecto el valor de la variable del Sistema **TM.MaxRejectRate** es de 250 RST TCP o 250 ICMP paquetes inalcanzables por segundo.

Bajar el valor a 100 puede contribuir a reducir la congestión de salida sin que ello afecte al rendimiento de la red.

```
% tmsh modify sys db tm.maxrejectrate value 100
```

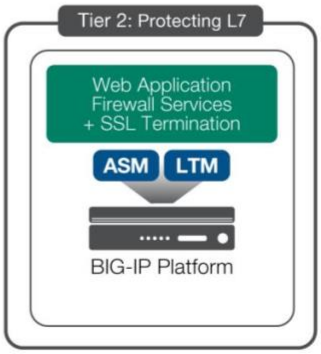
2.3 Nivel 2-Defensa de la aplicación

El segundo nivel es donde se despliega la defensa consciente de la aplicación y con uso intensivo de la CPU mecanismos como login-walls, política de firewall de aplicaciones web y LTM iRules. El nivel 2 es también es el lugar donde suele producirse la terminación del SSL. Aunque algunas organizaciones terminar SSL en el nivel 1, es menos común allí debido a la sensibilidad de las claves SSL y las políticas en contra de mantenerlos en el perímetro de seguridad.

2.3.1 Entender las inundaciones del GET

Los GET y POST recursivos se encuentran entre los ataques más perniciosos de la actualidad. Pueden ser muy difícil de distinguir del tráfico legítimo.

Las inundaciones GET pueden saturar las bases de datos y los servidores. Los GET Floods también pueden causar un "reverse full pipe". F5 registró un atacante que enviaba 100Mbs de GET consultas en una víctima y sacando 20Gbs de datos.



Si tiene una solución anti-DDoS basada en firmas (de F5 u otro proveedor) aprovéchelo para proteger su aplicación. Con LTM y ASM, F5 proporciona muchos diferentes maneras de mitigar los ataques difíciles de la capa de aplicación.

Las estrategias de mitigación de GET floods incluyen:

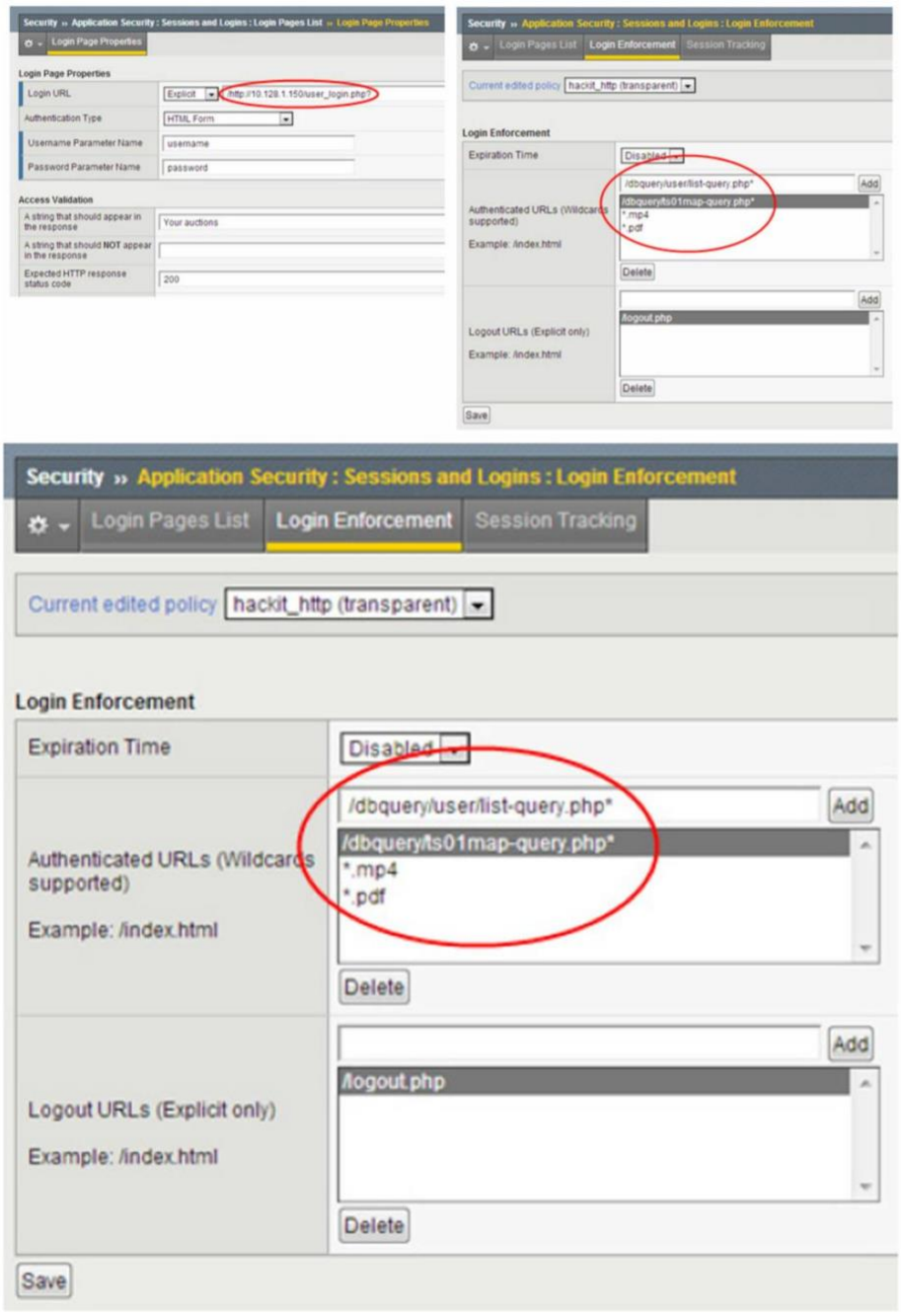
- La defensa del muro de entrada
- Profiles de protección DDoS
- Aplicación del navegador real
- CAPTCHA
- Reglas de aceleración de solicitudes
- Regla i personalizada

2.3.2 Reducir la superficie de la amenaza mediante la configuración de un muro de acceso

La técnica más poderosa para frustrar los ataques a nivel de aplicación es permitir solo usuarios autenticados para acceder a las partes de la base de datos de su aplicación. Creación de un el muro de acceso puede ser un trabajo delicado que es mucho mejor hacer en tiempos de paz y no durante un ataque DDoS agitado. Tenga en cuenta que no todas las aplicaciones pueden depender de los registros usuarios y tienen que procesar tráfico anónimo, pero para los que pueden, los muros de acceso son la defensa.

2.3.2.1 Designar un muro de entrada con ASM

ASM ofrece facilidades para hacerlo dentro de la política de ASM mediante el uso de páginas de acceso y la imposición del inicio de sesión. Esta función hará que los usuarios no puedan interactuar con un conjunto de URLs hasta que se hayan autentificado con éxito en una de las páginas de acceso.



En primer lugar, defina las páginas de inicio de sesión desde Seguridad → Seguridad de la aplicación → Sesiones y la pantalla de inicio de sesión.

A continuación, utilice la pestaña de **Aplicación del inicio de sesión** para especificar las páginas que deben protegerse.

Lo ideal es que se trate de objetos de gran tamaño, como archivos .MP4 y .PDF, y cualquier base de datos consultas que podrían ser utilizadas en su contra en un ataque asimétrico.

Para a completo explicación de el Inicio de sesión Aplicación de la ley característica, véase el sección "Creación de Inicio de sesión Páginas" en el ASM configuración guía.

Nota: Si no está seguro de los recursos que debe proteger, puedeReconocer su propio

Aplicaciones> puede reconocer sus propias aplicaciones - véase la sección 3.2.2.

2.3.2.2 Guión de un muro de acceso

Puede hacer un muro de acceso con sólo una iRule LTM estableciendo una cookie específica en el página de inicio de sesión, y luego comprobar esa cookie en todas las demás páginas. Cree esta iRule, adjúntalo y pruébalo. A continuación, sepáralo y guárdalo en tu biblioteca para activarlo como necesario.

Aquí hay un enlace a una iRule de login-wall en DevCentral.

2.3.2.3 Proteger las aplicaciones con Profiles de Protección DoS

El F5 Web Application Firewall, ASM, incluye "profiles DoS" específicos para cada aplicación.

Estos potentes profiles detectan las condiciones de DoS mediante la monitorización de **la latencia del servidor o tasas de solicitud http**. ASM puede entonces desencadenar un evento opcional de iRule cuando el ataque es mitigado.
Las opciones de mitigación son:

Utilice los siguientes comandos para crear un profile de DoS y adjuntarlo a la aplicación:

```
% tmsh create security dos profile my_dos_prof { application add { L
regla1 {
basado en la latencia { url-rate-limiting enabled mode blocking } } } }

% tmsh modify ltm virtual my_vip1 profiles add { my_dos_prof }
```

Puede acceder a este profil de DoS desde la pestaña Seguridad. A continuación, seleccione Protección DoS.

Desde esa pantalla, compruebe la seguridad de las aplicaciones y luego configure el L7DOS parámetros de protección.

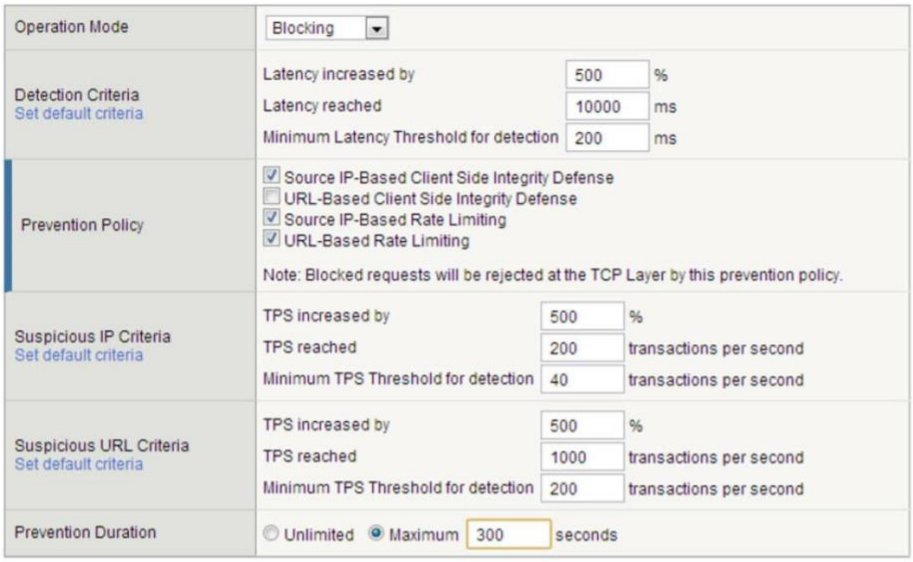


Figura 4. Configuración de la protección integral L7DOS del módulo ASM

2.3.2.4 Aplicar los navegadores reales

Además de la autenticación y la detección basada en tps (sección 2.3.2.3), existen formas adicionales en que los dispositivos F5 pueden separar los navegadores web reales de los probables bots.

La forma más fácil, con ASM, es crear una profile de protección DoS y activar el Opción "Source IP-Based Client Side Integrity Defense". Esto inyectará un JavaScript redirigir en el flujo del cliente y verificar cada conexión la primera vez que la IP de origen se ve la dirección.

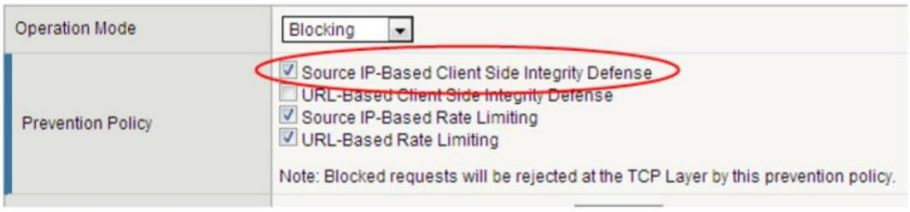


Figura 5. Insertar una redirección Javascript para verificar un navegador real

Desde la línea de comandos:

```
% modificar perfil de seguridad dos mi_ddos1 aplicación modificar { Lrule1
{ tps-based { ip-client-side-defense enabled } } }
```

2.3.2.5 Inundaciones de solicitudes GET a través de un script

La comunidad de F5 DevCentral ha desarrollado varias potentes iRules que acelerar automáticamente las solicitudes GET. Los clientes los refijan continuamente para estar al día con las técnicas de ataque actuales.

Esta es una de las iRules que es lo suficientemente simple como para ser representada en este documento.

El en vivo versión puede ser encontrar en este DevCentral página: HTTP-Request-Throttle

```
cuando RULE_INIT {

  # Life timer of the subtable object. Define el tiempo que este objeto e
xisten en el
subtabla

  set static::maxRate 10

  # Esto define cuánto tiempo es la ventana deslizante para contar las solicitudes
.

  # Este ejemplo permite 10 peticiones en 3 segundos

  set static::windowSecs 3

  set static::timeout 30

}

cuando HTTP_REQUEST
{
  if { [HTTP::method] eq "GET" } {

  set getCount [clave de la tabla -conteo -subtabla [IP::client_addr]]

  if { $getCount < $static::maxRate } {

  incr getCount 1

  table set -subtabla [IP::client_addr] $getCount "ignore"
$static::timeout $static::windowSecs

  } si no {
HTTP::respond 501 contenido "Petición bloqueadaSe han superado las
peticiones/seg límite".
```

```
    devolver
    }
    }
  }
```

Otra iRule, que de hecho desciende de la anterior, es una versión avanzada que también incluye una forma de gestionar las direcciones IP prohibidas desde la iRule

sí mismo:

- Abandona las conexiones sospechosas.
- Devuelve una redirección JavaScript al cliente para reforzar que un navegador está siendo utilizado.
- Limitación de velocidad por dirección de cliente o URI.
- Limitador de peticiones URI iRule: elimina las peticiones HTTP excesivas a URIs específicas
  - o desde una IP

2.3.2.6 Utilizar CAPTCHAs para eliminar los bots

Otra forma de mitigar los floods de GET es verificar la "humanidad" utilizando un mecanismo CAPTCHA. El mecanismo CAPTCHA muestra imágenes de imágenes codificadas palabras al usuario, que demuestra su humanidad tecleando las palabras en una web-formulario. Los CAPTCHAs siguen siendo una de las mejores formas de distinguir a los humanos de ordenadores a pesar de que los hackers e investigadores han intentado "romperlos" desde hace más de diez años. Los avances en los algoritmos de reconocimiento de patrones parecen aportar atacantes cerca de automatizar el sistema CAPTCHA. Sin embargo, es la experiencia de F5, que el trabajo computacional necesario para "romper" un CAPTCHA disminuye enormemente la ventaja asimétrica de un atacante moderno de DDoS, y esto mantiene estos ataques teórico por ahora. Esto significa que los CAPTCHAs siguen siendo un medio eficaz de repeliendo las redes de bots.

Google ofrece el servicio reCAPTCHA, que realiza esta función a la vez que descifrar textos antiguos. Hay una iRule de Google ReCAPTCHA en DevCentral que puede utilizarse para verificar que hay una persona al otro lado de la línea conexión. Descargue la iRule (aproximadamente 150 líneas) y edítela para proporcionar algunos de los datos básicos (como su clave reCAPTCHA de Google y su DNS servidor). Hágalo disponible en su BIG-IP. Adjúntelo a un servidor virtual y pruébelo, y luego mantenerlo listo para el despliegue.

2.3.3 Guión de una mitigación personalizada

Si hay que descartar todas las demás técnicas, puede que sea necesario escribir un iRule para defender su aplicación de un ataque a la capa de aplicación. Estas reglas personalizadas

Las iRules suelen ser de dos categorías: filtering y bloqueo indiscriminado.

Aunque esta es quizás la más "manual" de todas las técnicas de este documento, es también el más potente y el más utilizado entre los clientes ágiles de F5. El extremo la programabilidad de F5 iRules permite al administrador bloquear casi cualquier tipo de ataque siempre que sepa hacer un buen guión. Reglas de seguridad proteger a muchas organizaciones hoy en día y son uno de los verdaderos diferenciadores de F5 para ataques DDoS en la capa de aplicación.

Si el ataque te deja con algún acceso a Internet de salida, busca devcentral.f5.com para algunas de las palabras clave que podrían coincidir con su ataque. Usted puede y ya se ha escrito una iRule para ti.

Para escribir su propia iRule, primero diseccione el traffic de ataque y busque una característica sobre el traffic de ataque entrante que puede utilizar para distinguir el traffic malo del bueno. A continuación, escriba una iRule que detecte ese traffic y lo elimine. Si no es un autor de iRule, hay iRules dispersas en este documento (y en todo DevCentral) que puede utilizar como ejemplo. Adjunte su nueva iRule al servidor virtual de la aplicación.

Un ejemplo de una simple iRule de seguridad es esta primera iRule de **Dirt Jumper**, que introduce en el hecho de que el malware no incluye un // en su campo de referencia.

```
cuando HTTP_REQUEST
{
  if { [HTTP::header exists "Referer"] } {

  if { not ([HTTP::header "Referer"] contains "\x2F\x2F") }

  gota a
  gota

  }

  }

}
```

Si no puede distinguir fácilmente el traffic bueno del malo, puede escribir una iRule que descarta el traffic en función del objeto solicitado. Por ejemplo, si el atacantes solicitan un archivo PDF o MP4 de gran tamaño, puede utilizar una iRule para abandona todas las peticiones a ese objeto.

```
  ltm data-group internal block_uris { records { /faqs/faq.mp4 { } /l
ocator/locations.pdf { } /cgi-bin { } } type string }
```

También puede utilizar grupos de datos externos que estén alojados fuera del BIG-IP.

A continuación, utilice una simple iRule de depuración para descartar las solicitudes que pidan URIs que coincidan con el clase de datos.

```
ltm data-group internal block_uris {

  registros {

  /faqs/faq.mp4 { }

  /locator/locations.pdf { }

  /cgi-bin { }

  }

  tipo de cadena

}
```

Esta no es, sin duda, la mejor solución, ya que rechazará también el buen tráfico como malo. Puede mantener sus servidores vivos, pero si tiene el tiempo y la capacidad de escribir un regla como la anterior, normalmente se puede encontrar algo para distinguir el buen traffic de lo malo.

2.3.4 Mitigar el DDoS SSL en el nivel 2

Aunque es posible, y a veces preferible, terminar el SSL en cualquiera de los dos niveles, F5 recomienda un dispositivo físico (no virtual) para la terminación de SSL en el nivel 2. Muchos los ataques DDoS con SSL se verán mitigados por la propia presencia de la aceleración SSL hardware utilizado en los dispositivos físicos de F5. Estos incluyen:

- Ataques al protocolo SSL
- Ataques de repetición de SSL
- Conexión SSL floods

  Tanto si se utiliza hardware como si no, F5 también mitigará la conexión SSL floods con cosecha adaptativa (véase el apartado 2.2.7) y una tabla de conexiones de gran capacidad (sección 2.2.6).

  El ataque de renegociación SSL puede mitigarse de dos maneras. En la mayoría de los casos, puede simplemente desactivar temporalmente la función de renegociación SSL en el profil del cliente SSL del servidor virtual. Sin embargo, las conexiones de muy larga duración (como los cajeros automáticos o las conexiones a bases de datos) seguirán necesitando la capacidad de renegociación.

2.3.5 Entender la multiplexación de la conexión y el puerto Agotamiento

En general, no realice funciones como la multiplexación de conexiones y la SNAT en nivel 1. Estas funciones y los extras asociados, como la inserción de la X-La cabecera Forwarded-For debe ser procesada en el nivel 2.

2.3.5.1 Multiplexación de la conexión

Un DDoS de capa 7 puede agotar los recursos del back-end, como las tablas de conexión.

Una forma de combatir este efecto es multiplexar las conexiones a través del equilibrador de carga. En LTM esta función se llama OneConnect y puede disminuir el número de conexiones TCP utilizadas por un orden de magnitud mientras mantener (o incluso mejorar) el número de solicitudes por segundo.

La función OneConnect debe probarse con cada aplicación antes de ser utilizado como defensa DDoS. Algunas aplicaciones pueden depender de conexiones separadas por usuario.

2.3.5.2 Agotamiento del puerto

Un SNAT admite aproximadamente 64.000 conexiones simultáneas por IP de destino. Un alto volumen de solicitudes puede superar la conexión de 64.000 límite y provocar el agotamiento de los puertos TCP. Puede utilizar un pool SNAT para supercar esta limitación. Configure y establezca la dirección IP adecuada dentro del SNAT piscina para mitigar el agotamiento.

Por ejemplo, si su servidor virtual **vip1** está utilizando la fuente simple de automap traducción de direcciones, puede cambiarla para que utilice un conjunto de direcciones IP con el siguientes comandos. Este ejemplo utiliza sólo tres direcciones para aumentar la puertos disponibles de 64.000 a 192.000.

```
% tmsh create ltm snatpool ddos_snatpool members add { 10.1.20.
161 10.1.20.162
10.1.20.163 }

% tmsh modify ltm virtual vip1 source-address-translation { poo
l ddos_snatpool }
```

Para cada dirección añadida al pool de SNAT, es posible que desee asignar un valor de tiempo de espera (el valor por defecto es indefinido). Con un tiempo de espera inactivo, BIG-IP puede cerrar conexiones inactivas y ayudar a proteger los firewalls de estado de la red.

```
 % tmsh modify ltm snat-translation 10.128.20.161 { ip-idle-tim
eout 60 }
```

Repite este comando para cada una de las direcciones de tu snatpool (10.1.20.162 y 10.1.20.163 en el ejemplo anterior).

Otras 3 prácticas recomendadas en materia de DDoS

3.1 Mitigar el DNS DDoS

El DNS es el segundo servicio más atacado después del HTTP. Cuando se interrumpe el DNS, todos los servicios externos del centro de datos (no sólo una única aplicación) se ven afectados. Este punto único de fallo total, junto con el DNS históricamente infradotado infraestructura, hace que el DNS sea un objetivo muy tentador para los atacantes. Incluso cuando los atacantes no tienen como objetivo específico el DNS, pero a menudo lo hacen inadvertidamente: si el los clientes de ataque están consultando la IP del host de destino antes de lanzar su floods, el resultado es un ataque indirecto contra el DNS.

Debido a que el protocolo DNS, basado en UDP, es relativamente sencillo, un ataque DNS tiene dos características principales:

- Los ataques de DNS son fáciles de generar.
- Los ataques de DNS son difíciles de defender.

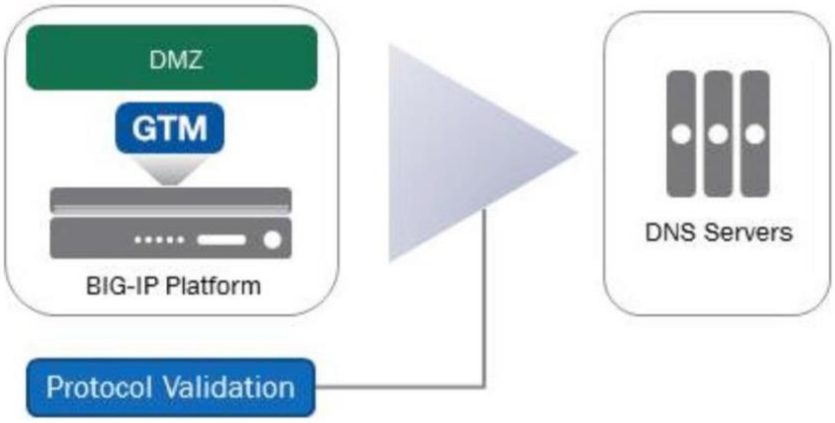


Figura 6: Mitigación de DNS DDoS

Existen cuatro estrategias locales para mitigar los ataques DNS DDoS:

- Utilizar la validación del protocolo.
- Detecta y previene los floods del DNS.
- Sobreaprovisionamiento de servicios DNS contra la consulta NXDOMAIN floods.
- Lista negra como último recurso.

3.1.1 Considerar la colocación de los servicios DNS

Puede observar que en la Figura 1 el servicio DNS existe como un conjunto propio de dispositivos detrás del perímetro de seguridad. A menudo el DNS se sirve desde este llamado DMZ entre los niveles de seguridad. Esto se hace para mantener el DNS independiente del aplicaciones a las que sirve, por ejemplo, si esa parte del centro de datos se oscuro, el DNS puede redirigir las solicitudes a un centro de datos secundario (o a la nube). **F5 recomienda esta estrategia de mantener el DNS separado** de la seguridad y niveles de aplicación para una máxima flexibilidad y disponibilidad.

Algunas grandes empresas con múltiples centros de datos irán un paso más allá y servir DNS fuera del perímetro de seguridad principal utilizando una combinación de F5 GTM DNS Express y el módulo AFM firewall. El principal beneficio de esta es que los servicios de DNS sigan estando disponibles incluso en el caso de que el nivel 1 los muros de seguridad se deshabilitan debido a los DDoS.

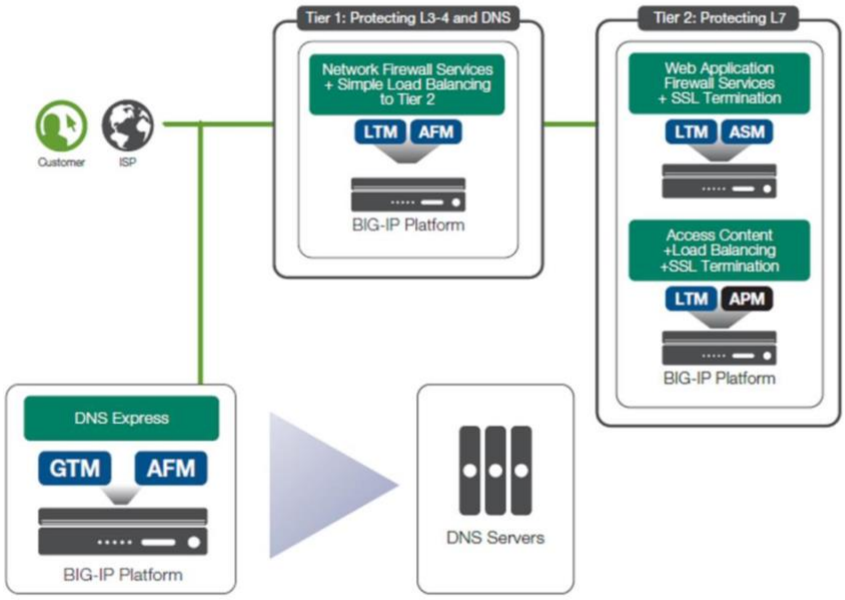


Figura 7: Arquitectura alternativa de DNS externo

3.1.2 Utilizar la validación de protocolos para proteger los servicios DNS

Independientemente de si sirve DNS dentro o fuera de la DMZ, puede utilizar GTM o AFM para validar las peticiones DNS antes de que lleguen al DNS servidor.

Si tiene GTM realizando el balanceo de carga del servidor global, es probable que sea bloqueando ya muchos ataques DNS DDoS. Puede ver el DNS rendimiento de la consulta/respuesta desde el panel principal de la GUI de GTM. Dado que GTM es un proxy completo para DNS, validará automáticamente cada solicitud y descartar los no válidos.

Sin embargo, es posible que sus servidores sigan estando saturados de gente con apariencia válida solicitudes. Si tiene el módulo AFM de F5 firewall, puede utilizar un **Protocolo Profile de seguridad** para filtrar sólo tipos específicos de solicitudes DNS.

En la **pestaña de Seguridad**, seleccione **Seguridad del Protocolo** y luego **Seguridad Profiles**. Seleccione **DNS** y pulse el botón **Crear**. En esta pantalla puede construir un protocolo de seguridad para filtrar o bloquear diferentes tipos de solicitudes.

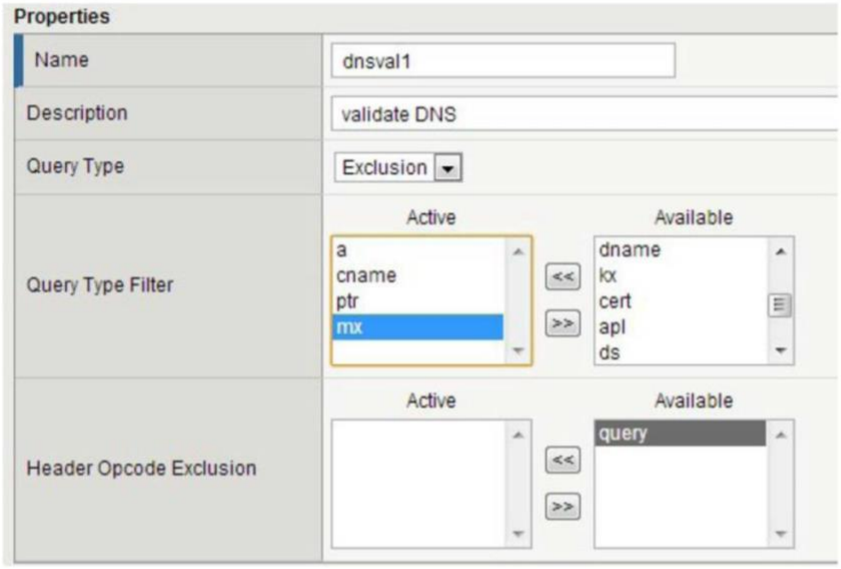


Figura 8: Validación del protocolo DNS

3.1.3 Detectar inundaciones de DNS

El módulo firewall AFM de F5 tiene una potente función DNS DDoS: puede detector DNS floods por tipo de registro. En la pestaña **Seguridad,** seleccione **Protección DoS**, luego los **Profiles DoS** y finalmente **crear**. En la pantalla de creación, haga clic en el botón casilla de verificación para DNS y establecer y aceptar los parámetros del umbral.

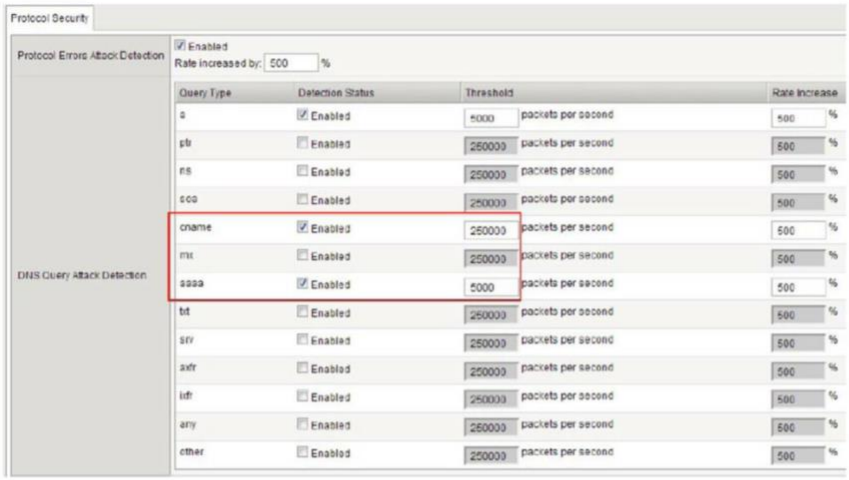


Figura 9: Detección de inundaciones de DNS

La casilla de verificación de los errores de protocolo significa que el sistema detecta los errores maliciosos o consultas DNS malformadas, y muestra, en porcentaje, la cantidad de el aumento del tráfico de consultas DNS es legal antes de que el sistema rastree las consultas malformadas y consultas DNS maliciosas.

Nota: En este momento, esta función de firewall detecta los alimentos pero no los deja caer paquetes para mitigarlos.

3.1.4 Sobreaprovisionamiento de servicios DNS contra inundaciones de consultas

Los servicios de DNS han estado históricamente infradotados. Parte de la razón para esto es que para muchas organizaciones la propiedad del DNS no ha sido un desarrollo positivo para cualquier equipo en particular. Cualquiera que sea la verdadera razón, un porcentaje significativo de los despliegues de DNS están infradotados hasta el punto de que donde son incapaces de soportar incluso ataques DDoS de tamaño pequeño o mediano.

Los cachés de DNS se han hecho populares porque pueden aumentar la percepción de rendimiento de una caché DNS y han proporcionado cierta resistencia contra ataques de consulta DNS estándar. Los atacantes han cambiado a lo que se llama el ataques "no such domain" (o NXDOMAIN), que agotan rápidamente el rendimiento que proporciona la caché.

La forma recomendada por F5 para remediar esto es enfrentar el servicio DNS con el módulo especial de proxy DNS de alto rendimiento llamado DNS Express. DNS Express actúa como un resolvedor absoluto frente a los servidores DNS existentes. Se carga la información de zona de los servidores y luego resuelve cada una de las solicitudes o devuelve NXDOMAIN. No es un caché y no se puede vaciar mediante Consulta NXDOMAIN floods.

En GTM o Servicios DNS, DNS Express puede servir 250.000 peticiones por segundo por CPU y, por tanto, es resistente a todos los DNS, excepto a los más virulentos ataques. Los servidores DNS permanecen en su lugar para gestionar los datos de la zona.

3.1.5 Lista negra como último recurso

El tráfico de DNS es tradicionalmente UDP, que es fácil de generar y de falsificar. Las defensas convencionales de las capas 3 y 4, como las listas negras por IP de origen, son suele ser ineficaz frente a un flood de DNS. De hecho, el bloqueo de las peticiones DNS por la IP de origen puede ser francamente peligrosa. Por ejemplo, si sin saberlo bloquear las solicitudes de un ISP importante, puede negar el servicio a muchos usuarios sin darse cuenta.

Véase "Sistemas BIG-IP: Implementaciones de protección DOS y cortafuegos de protocolo" (capítulo 3-Detección y prevención de ataques DNS DDoS).

3.1.6 Cuidado con la participación de DDoS A ack

3.1.6.1 Tipos de consulta no utilizados

Un atacante puede engañar a un servicio DNS para que bombardee un objetivo de terceros mediante enviar consultas por servicios no utilizados. Utilice las pantallas de AFM (véase la figura 9 más arriba) para desactivar los tipos de consulta que no está utilizando. Entonces, cuando las consultas vengan para estos tipos serán descartados. No se proporcionará ninguna respuesta, por lo que ayudando a evitar la participación en un ataque DDoS.

Esto es especialmente cierto para MX (servicios de correo) y transferencias de zona. Si su organización hace una transferencia en momentos conocidos y específicos, mantiene el IXFR, los tipos AXFR y ZXFR están desactivados en el resto de ocasiones.

3.1.6.2 DNSSEC

DNSSEC es una evolución importante en el servicio global de nombres de dominio. En última instancia, reducirá las prácticas engañosas, como el phishing. La página web el panorama es más complicado para el DNS DDoS. Las respuestas de DNSSEC son a veces entre 10 y 20 veces más grandes que las respuestas UDP del DNS tradicional. Este significa que los servidores DNSSEC son realmente engañados para atacar a otros ordenadores bombardeándolos inadvertidamente con respuestas no válidas.

Con GTM, F5 tiene la solución DNSSEC de mayor rendimiento del mercado.

La capacidad de GTM podría ser un arma potente si se utilizara como un vector de ataque. Por lo tanto, GTM le permite limitar el número de respuestas para evitar participar en un ataque.

```
% tmsh modify sys db dnssec.maxnsec3persec value 10
```

La variable **dnssec.maxnsec3persec** controla el límite superior de NSEC3 mensajes NXDOMAIN autoritativos que GTM enviará por segundo. 0 es ilimitado y el valor por defecto. Un valor más restrictivo, como por ejemplo entre 10 y 100 por segundo, puede impedir que el propio GTM se utilice durante un ataque.

```
% tmsh modify sys db dnssec. signaturecachensec3 value true
```

Al establecer la variable **dnssec.signaturecachensec3** como falsa se evita los mensajes NXDOMAIN no utilizan la caché de GTM en absoluto, lo que impide que un atacante de llenar la caché de GTM con respuestas de "no hay tal dominio".

3.2 Preparación adicional de las mejores prácticas de DDoS Procedimientos

El tiempo dedicado a la preparación de un ataque DDoS aumentará la eficacia de su defensa. Aquí hay algunas formas más de preparar su organización para un ataque DDoS.

3.2.1 Configurar y verificar el registro

Durante un ataque es muy probable que se envíen diagnósticos y el registro de anomalías y picos de tráfico. El alto rendimiento es fundamental cuando para hacer frente a un gran ataque DDoS. La instrumentación también es importante, lo que significa que querrá utilizar la función de registro de alta velocidad de BIG-IP para enviar esta información a un dispositivo de registro de terceros, como Splunk o un SIEM como ArcSight.

Nota: Debe utilizar las facilidades de High-Speed-Logging de BIG-IP en el nivel 1 al mitigar un ataque DDoS. No utilice el registro local; una intense Los ataques DDoS pueden sobrecargar el registro local basado en disco.

3.2.1.1 Configurar el registro de alta velocidad

- Cree un pool para asignar a sus servidores de registro externos (en este caso son syslog). Reescriba según sea necesario para ArcSight, TrustWave o cualquier solución SIEM que soporta su entorno. A continuación, cree el registro configurado para formatear y reenviar las cadenas correctamente.

```
% tmsh create ltm pool hsl_pool members add { 10.128.10.25
0:514 }

% tmsh create sys log-config destination remote-high-speed
-log log_dest_HSL {
pool-name hsl_pool }

% tmsh create sys log-config destination remote-syslog log
_dest_format { formato
rfc5424 remote-high-speed-log log_dest_HSL }

% tmsh create sys log-config publisher log_pub_ddos { dest
inaciones { log_
dest_HSL log_dest_format } }
```

- Cree un objeto de profile de registro utilizando la GUI..

Acceda a la **página Seguridad > Registros de eventos > Profiles de registro.** Cree un profile de registro utilizando lo siguiente:

Nombre del Profile	ddos_log_profile
Cortafuegos de red	Activado
Cortafuegos de red: Editorial	log_pub_ddos
Reglas de registro de coincidencias	Aceptar, abandonar y rechazar
Registro de errores de IP	Activado
Registro de errores TCP	Activado
Registro de eventos TCP	Activado
Formato de almacenamiento	field-list Seleccione todos los elementos disponibles y muévalos a la lista de elementos seleccionados

- Asocie ese objeto de profile de registro con los servidores virtuales que protegen su aplicación.

```
% tmsh modify /ltm virtual vip1 { security-log-profiles a
dd { ddos_ log_profile } }
```

3.2.2 Reconocer sus propias aplicaciones

Los atacantes modernos de DDoS reconocerán una aplicación días o semanas antes de lanzar su ataque DDoS. Ellos arañarán su sitio web y recuperar el **tiempo de carga** y el **tamaño de los datos** para cada URI válido. Al ordenar el conjunto de datos resultante, aislarán rápidamente su mayor cantidad de CPU o base de datos. consultas intensivas y sus objetos más grandes (como PDFs y MP4s). Durante el ataque DDoS consultarán repetidamente estos objetos, abrumando su infraestructura.

Aunque la sección 3.8 le ayudará a mitigar ese ataque cuando se produzca, puede ayudarse a sí mismo de antemano reconociendo su propia aplicaciones. Esto le proporcionará una visibilidad avanzada sobre qué URIs y subsistemas serán objetivos probables, lo que le permitirá hacer más decisiones de triaje más tarde.

Lo ideal es tener una herramienta como LoadRunner u otra de rendimiento herramienta de monitorización que puede proporcionarle las métricas que necesita. Si usted carecen de esta capacidad, quizás la forma más sencilla de recuperar la tabla básica de la URL, el tiempo de carga y el tamaño de los datos es ejecutar la utilidad wget, que es disponible en la mayoría de las distribuciones de Linux. Ejecútelo con la siguiente sintaxis:

```
% wget -r --spider http://10.128.10.150 2>&1 | grep saved

2013-08-25 15:44:29 (2.48 MB/s) - `10.128.1.150/index.html
' guardado [22304]

2013-08-25 15:44:29 (5,53 MB/s) - `10.128.1.150/index.php'
  guardado [22304]

2013-08-25 15:44:29 (7,06 MB/s) - `10.128.1.150/sell.php'
guardado [41695]
```

El último número (entre corchetes) es el tamaño de los datos de la solicitud. Usted tendrá que obtener el tiempo de carga restando los tiempos (segundo campo) de entre sí.

3.2.3 Validar el estado de los dispositivos BIG-IP existentes con iHealth

F5 proporciona un servicio de diagnóstico y heurística basado en la nube llamado iHealth. iHealth examinará la configuración de un dispositivo F5 y hará recomendaciones para mantener BIG-IP rápido, seguro y disponible. Mientras que el la mayoría de los ajustes pueden ser más aplicables a los dos primeros, algunos de estas configuraciones pueden aplicarse a la disponibilidad y, por extensión, a los DDoS-resiliencia.

En este ejemplo, iHealth muestra que un grupo de SNAT ha sido configurado sin valores de tiempo de espera. Esto puede ser un recordatorio para un administrador consciente de los recursos para asegurarse de que el grupo SNAT utilizado para sus servidores virtuales reforzados deben incluir tiempos de espera para mantener el número de conexiones y evitar que un firewall de la parte superior de la propina.

Consulte el sitio web de iHealth para obtener más información al respecto.

3.2.4 Preparar un libro de jugadas DDoS

Un DDoS Playbook o Runbook es un manual de procedimiento para ayudar a su equipo de TI empleados en la lucha contra un ataque DDoS. Un buen libro de jugadas ayudará a los nuevos (y existentes) los administradores combaten un ataque DDoS. El libro de jugadas debe mantenerse al día con listas blancas actualizadas e información de contacto.

Algunas organizaciones realizan periódicamente simulacros (o incluso pruebas) de DDoS contra sí mismos para mantenerse al día y poner a prueba el libro de jugadas. Intentar tener su personal practique los procedimientos del libro de jugadas cuando las personas clave no están presentes: los ataques no siempre se producen en el momento más conveniente el horario.

Si no tiene un libro de jugadas, hay uno disponible en F5.

3.2.5 Repasar las tácticas defensivas en los dos niveles Arquitectura

Algunas de las tácticas defensivas descritas en las secciones anteriores son merece la pena revisarlo, especialmente para los administradores que utilicen una red que no sea F5 firewall.

Recuerda:

- Los grupos SNAT mitigan el agotamiento de los puertos en el nivel 1.
- Forma de traffic en el nivel 1.
- Cosechar agresivamente las conexiones TCP.
- Poner el DNS en la lista negra sólo como último recurso.
- Implantar muros de acceso y CAPTCHAs en el nivel 2.
- Desactivar las funciones opcionales de uso intensivo de la CPU en el nivel 2.
- Utilice siempre el registro remoto de alta velocidad.

Aplicando las sugerencias propuestas en esta guía de buenas practices habrá hecho mucho para preparar sus aplicaciones para un ataque DDoS.

4 Conclusión

Comprender el moderno espectro de amenazas de los ataques de denegación de servicio es importante. Entender cómo hacer uso de la defensa equipo que ya tiene es aún más importante.

Dependiendo de sus recursos y necesidades, puede que ya tenga rediseñado su red para la resistencia a los DDoS. Si esto es algo que que está considerando, entonces preste mucha atención a la arquitectura de varios niveles descrita en la sección 2.1. Aunque su red seguridad no se construye completamente a partir de la tecnología de F5, sigue teniendo sentido para hacer frente a la capa 4 y a la capa 7 de forma independiente a efectos de DDoS.

Siguiendo las prácticas recomendadas, estará preparando su red, las aplicaciones y las personas para que sean resistentes a los ataques.

El paso final en las prácticas recomendadas por F5 para la mitigación de DDoS es preparar un libro de jugadas DDoS. Este libro de jugadas es un procedimiento en tiempo real guía para mitigar un ataque que incluye hojas de trabajo y registros. F5 puede le proporcionan una plantilla para empezar.

Los expertos prevén que los DDoS serán un problema en Internet durante mucho tiempo por venir. Pronto, estar preparado no será sólo una opción, sino una requisito.

Anexo

Aplicación A ack Taxonomía y Contramedidas

En la siguiente sección se recomiendan mitigaciones para ataques específicos de la capa 7 vectores. Muchos de ellos son ataques del tipo "lento y lento" que pueden ser particularmente pernicioso.

Contenido

- Slowloris
- Manténgase muerto
- Cañón de iones de órbita baja (LOIC)
- POSTs lentos
- Ataques de ventana cero
- Ataque de lectura lenta
- RUDY
- Asesino de apaches
- Renegociación SSL
- Dirt Jumper iRule

Slowloris

Slowloris es un vector HTTP común donde un atacante enviará (muy lentamente) pequeñas cabeceras HTTP para mantener viva la sesión HTTP (por ejemplo, "X-a: b" cada 299 segundos). Si el servidor virtual está equilibrando la carga en capa 4, considere cambiarla a la capa 7. Esto añadirá algo de protección cuando se añade el profil de HTTP.

```
% tmsh list ltm virtual vip1
ltm virtual vip1 {
destino 10.128.10.141:http
perfiles {
fastL4 { }
}
}

% tmsh modify ltm virtual vip1 profiles replace-all-with {
  tcp http }
```

Esto hará que BIG-IP absorba las conexiones de Slowloris. Si usted se preocupan de que se acumulen demasiados y causen problemas para otros dispositivos (como un firewall), utilice la siguiente iRule de Slowloris para abandonar cualquier conexión que no se haya completado después de 10 segundos (siéntase libre para ajustar este número).

```
# Slowloris iRule

cuando CLIENT_ACCEPTED {

  set hsl [HSL::open -proto UDP -pool hsl_pool]

  set rtimer 0

  después de 10000
  {
  si { no $rtimer } {

  gota a gota

  HSL::send $hsl "Dropped [IP::client_addr] - connection to
o
lento"

  }

  }

}

cuando HTTP_REQUEST
{
  set rtimer 1

}
```

Manténgase muerto

Este ataque se basa en el consumo de CPU y RAM. Utilizando Keep-Alive y el método HTTP HEAD, puede crear una serie de peticiones sin activando una defensa firewall que se basa en el número de conexiones abierto al servidor.

El módulo ASM puede rechazar las peticiones HEAD (que no suelen ser utilizado por los navegadores). Se pueden rechazar las peticiones HEAD configurando la opción "Métodos permitidos" en la política de seguridad de la aplicación en cuestión.

Consulte la solución 12312 para obtener más información.

Cañón de iones de órbita baja (LOIC)

El cañón de iones de baja órbita es una herramienta de botnet voluntaria estrechamente asociada con el grupo hacktivista Anonymous. Aunque la herramienta utiliza SYN floods y UDP floods, es más famoso por sus HTTP floods de capa 7. Suponiendo que que los floods SYN y UDP han sido mitigados (ver secciones 2.2.2 y 2.2.3), el último paso es mitigar el LOIC GET floods.

A menudo, la forma más rápida de hacerlo es filtrarlo en el ataque "de protesta". mensaje" incluido en cada petición HTTP de LOIC. Utilice Wireshark o tcpdump u otra herramienta para aislar el mensaje, y luego añadir ese mensaje a un grupo de datos. Utilice %20 para representar los espacios. El mensaje puede cambiar con el tiempo y es posible que tenga que vigilarlo mientras dure la ataque.

```
ltm data-group anonmsgs { records { Somos%20legi { } U%20
dun%20goofed { } } tipo cadena }
```

Tenga en cuenta que puede utilizar clases de datos externas que estén alojadas fuera del BIG-IP-vea "**help search data-group**" en el shell del comando tmsh.

A continuación, utilice una simple iRule de depuración para descartar las solicitudes que contengan cualquier cargas útiles en esa clase de datos.

```
ltm rule loic_defense_rule {

  cuando CLIENT_ACCEPTED
  {
  set hsl [HSL::open -proto UDP -pool hsl_pool]

  }

  cuando HTTP_REQUEST
  {
  if { [class match [HTTP::uri] contains anonmsgs] } {

  gota a gota

  HSL::send $hsl "Dropped [IP::client_addr] - suspected Low
  Cañón de iones en órbita"

  }

  }

}
```

Slow-POSTs

El corazón del ataque Slow-POST se basa en el envío de una petición POST con una "longitud de contenido" determinada, que suele ser un número grande, y luego enviando muy lentamente el cuerpo del mensaje al servidor, mientras se mantiene el tiempo de inactividad largo. El servidor dejará la conexión abierta mientras continua para recibir datos. Si se ejecuta un gran número de estas peticiones contra un servidor, existe la posibilidad de agotar la tabla de conexiones, lo que dejaría al servidor incapaz de responder a más peticiones.

Si tienes el módulo ASM, puedes mitigar la lentitud de los envíos con dos de las variables que se encuentran en la pantalla de variables del sistema ASM- Navegue **hasta Seguridad : Opciones : Seguridad de aplicaciones : Configuración avanzada : Variables del sistema y** modificar las siguientes variables.

slow_transaction_timeout (por defecto 10 segundos). Reduzca este valor según sea necesario.

max_slow_transactions (por defecto 25 transacciones). Bajar este valor a 5 o menos según sea necesario.

Si no tiene ASM, consulte esta iRule de LTM para mitigar Slow-POST.

Se puede utilizar con la iRule de lectura lenta de la siguiente sección (sólo hay que adjuntar como dos iRules separadas) porque la iRule de lectura lenta es de servidor y la iRule Slow-POST está basada en el cliente.

Ventana cero A acks

El ataque Zero Window es un ataque de capa 4 difícil de detectar. Funciona mediante establecer una conexión TCP con el objetivo, solicitar algunos datos y luego establecer el tamaño de la ventana TCP a cero. Esto detiene la conexión en el servidor, la caché o el middleware.

Si el atacante está estableciendo una longitud de ventana TCP cero contra un BIG-IP usted puede utilizar el valor de la profile tcp de tiempo de espera cero mencionada en la sección 2.2.2 para mitigar.

Lectura lenta A ack

El ataque de lectura lenta funciona enviando peticiones HTTP legítimas y luego leer las respuestas HTTP muy lentamente desde el buffer, con el objetivo de mantener el mayor número posible de conexiones en estado activo en la víctima.

En la versión 11.3.0, la prevención de baja y lenta del módulo ASM funciona en peticiones de entrada, como un POST lento. Para la lectura lenta, utilice la opción tras la mitigación de la iRule LTM:

```
cuando
SERVER_CONNECTED {


  TCP::collect
```

```
}

cuando SERVER_DATA
{

  set rtimer 0

# Tiempo en milisegundos antes de que se considere la lectura de la
respuesta HTTP
ered slow:

  después de 5000
  {

  si { no $rtimer} {

  set hsl [HSL::open -proto UDP -pool hsl_pool]

# Lectura lenta detectada para esta respuesta del servidor. Incrementar t
a cuenta añadiendo un
entrada de la tabla:

# Añade la IP de origen del cliente::puerto a la subtabla con un ti
meout

  table set -subtabla "MyApp" "[IP::client_addr]:[TCP::clie
nt_port]"
"ignorado" 180

# Si estamos por encima del límite de concurrencia entonces
rechazar

  si { [claves de la tabla -subtabla "MyApp" -cuenta] > 5} {

  lado del cliente {rechazo}

  table delete -subtabla "MyApp" "[IP::client_addr]:[TCP::c
liente_
puerto]"

  HSL::send $hsl "Dropped [IP::client_addr] - reading too s
bajo"

  }

  }
```

```
  }

  Respuesta de TCP::notify

  TCP::liberación

  TCP::collect

}

cuando
USER_RESPONSE {

  set rtimer 1

}

cuando CLIENT_CLOSED
{

  table delete -subtabla "MyApp" "[IP::client_addr]:[TCP::c
lient_port]"

}
```

RUDY

R-U-Dead-Yet (RUDY para abreviar) utiliza Slow-POST y un HTTP genérico Ataque DoS a través de envíos de campos largos.

Asesino de apaches

El Apache Killer también se conoce como Range Attack. Cuando un cliente navegador (como el de un teléfono móvil) sólo necesita una parte de puede solicitar un "rango" de datos con un rango HTTP de la cabecera. Si el cliente quiere sólo los primeros 100 bytes, podría decir:

```
  Rango:bytes=0-100
```

El ataque Apache Killer funciona solicitando múltiples y superpuestas rangos que confunden a los servidores web como Apache:

```
  Rango:bytes=0-,5-1,5-2,5-3,...
```

Hay tres maneras de mitigar el Apache Killer. Puede modificar el HTTP profile simplemente eliminar la cabecera Range. Por ejemplo, si su http Si el nombre del profile fuera "http_ddos2", se ejecutaría este comando:

```
  % tmsh modify ltm profile http http_ddos2 { header-erase
gama }
```

Una forma más quirúrgica de mitigar el Apache Killer es con la siguiente iRule, que sólo elimina las solicitudes de rango cuando hay más de cinco rangos solicitado.

```
cuando CLIENT_ACCEPTED
{
  set hsl [HSL::open -proto UDP -pool hsl_pool]

}

cuando HTTP_REQUEST
{
  # eliminar las solicitudes de rango para CVE-2011-3192 si más de fi
os rangos son
solicitado

  if { [HTTP::header "Range"] matches_regex {bytes=([0-9\-
  ])+,){5,}} } {

  HTTP::header remove Range

  HSL::send $hsl "El cliente [IP::client_addr] ha enviado más de 5
  rangos. Borrar
cabecera de rango".

  }

}
```

El tercer método de mitigación con las soluciones BIG-IP es utilizar el siguiente firma de ataque ASM para detectar y actuar sobre un ataque utilizando esta técnica.

```
  pcre:"/Rango:[\t ]*bytes=(([0-9\- ])+,){5,}/Hi";
```

Renegociación SSL

Si ves que se producen muchas renegociaciones desde un especificador SSL clientes, podría estar sufriendo un ataque de renegociación SSL. Lo más fácil la forma de mitigarlo es desactivar la renegociación de SSL desde el servidor virtual profile del cliente asociado. Sin embargo, si necesita apoyar renegociación para los clientes legítimos (como los antiguos "step-up" o navegadores con criptografía cerrada) mientras se mitiga el ataque, se puede utilizar esta iRule, u otras similares. Esta regla cierra cualquier conexión que intenta más de cinco renegociaciones en un minuto:

```
cuando RULE_INIT {

  set static::maxquery 5

  set static::mseconds 60000

}

cuando CLIENT_ACCEPTED
{

  set ssl_hs_reqs 0

  set hsl [HSL::open -proto UDP -pool hsl_pool]

}

cuando
CLIENTSSL_HANDSHAKE {

  incr ssl_hs_reqs

  after $static::mseconds { if {$ssl_hs_reqs > 0} {incr ssl
_hs_reqs -1} }

  if { $ssl_hs_reqs > $static::maxquery } {

  después de 5000

  gota a gota

  HSL::send $hsl "Dropped [IP::client_addr] - too many SSL
renegociaciones"

  }
```

```
}
```

Dirt Jumper iRule

Algunas versiones de la herramienta Dirt Jumper no incluyen un // en su campo de referencia. Aquí hay una simple iRule para detectar y dejar caer Dirt Jumper conexiones.

```
cuando CLIENT_ACCEPTED
{
  set hsl [HSL::open -proto UDP -pool hsl_pool]

}

cuando HTTP_REQUEST
{
  if { [HTTP::header exists "Referer"] } {

  if { not ([HTTP::header "Referer"] contains "\x2F\x2F") }
  {

  HSL::send $hsl "DDoS Dirt-Jumper HTTP Header Structure mi
ssing x2f x2f
Identificador de protocolo de referencia de [IP::client_addr]"

  gota a
  gota
  }

  }

}
```

Descargar Volumen 2

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

América
info@f5.com

Asia-Pacífico
apacinfo@f5.com

Europa/Oriente Medio/África
emeainfo@f5.com

Japón
f5j-info@f5.com