Uso de CAR durante ataques de DOS

Contenido

Introducción

A veces, una red recibe un flujo de paquetes de ataque de Negación de servicio (DoS) junto con el tráfico de red normal. En tales situaciones, usted puede utilizar un mecanismo llamado “tarifa que limita” para permitir que el rendimiento de la red degrade, de modo que siga habiendo la red para arriba. Usted puede utilizar el software del ® del Cisco IOS para alcanzar la tarifa que limita con estos esquemas:

- Committed Access Rate (CAR)
- Modelado de tráfico
- Modelado y regulación del tráfico a través de la Interfaz de Línea de Comando de Calidad de Servicio Modular (QoS CLI)

Este documento discute el COCHE para el uso en los ataques DOS. Los otros esquemas son apenas variantes del concepto básico.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS Software Release 11.1CC y mainline 12.0, que utilizan el COCHE.
- Cisco IOS Software Release 11.2 y Posterior, que utilizan el modelado de tráfico.
- Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, que utilizan la Calidad del servicio (QoS) modular CLI.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Límite de velocidad ICMP/Smurf

Configure estas Listas de acceso:

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

```
interface <interface> <interface #>
  rate-limit input access-group 102 256000 8000 8000 conform-action transmit
  exceed-action drop
```

Para activar el COCHE, usted debe activar el Cisco Express Forwarding (CEF) en el cuadro. Además, usted debe configurar un interfaz CEF-cambiado para el COCHE.

La salida de muestra utiliza los valores de ancho de banda para DS3 el tipo anchos de banda. Elija los valores basados en el ancho de banda de la interfaz y la tarifa en los cuales usted quiere limitar un tipo determinado de tráfico. Para interfaces de ingreso más pequeñas, usted puede configurar a las menores velocidad.

Paquetes SYN del límite de velocidad TCP

11.1(X)CC

Si usted sabe qué host está bajo ataque, configure estas Listas de acceso:

```
access-list 103 deny tcp any host 10.0.0.1 established
```

```
!--- Let sessions in progress run. access-list 103 permit tcp any host 10.0.0.1 !--- Rate limit
the initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 103
8000 8000 8000 conform-action transmit exceed-action drop
```

Nota: En este ejemplo, el host bajo ataque es 10.0.0.1.

Si usted no le conoce qué host está bajo ataque DOS, y quiere proteger una red, configure estas Listas de acceso:

```
access-list 104 deny tcp any any established
!--- Let sessions in progress run. access-list 104 permit tcp any any !--- Rate limit the
initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 104
64000 8000 8000 conform-action transmit exceed-action drop
```

Nota: Límite de velocidad a 64000 BPS para todos los paquetes SYN TCP.

12.0(X)[S/T/M]

Si usted sabe qué host está bajo ataque, configure estas Listas de acceso:

```
access-list 105 permit tcp any host 10.0.0.1 syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 105 8000 8000 8000 conform-action transmit exceed-action drop
```

Nota: En este ejemplo, 10.0.0.1 es el host bajo ataque.

Si usted no está seguro que el host es bajo ataque, y usted quiere proteger una red, configure estas Listas de acceso:

```
access-list 106 permit tcp any any syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 106 64000 8000 8000 conform-action transmit exceed-action drop
```

Nota: Límite de velocidad a 64000 BPS para todos los paquetes SYN TCP.

El COCHE hizo con frecuencia las preguntas

¿Cómo identificar los valores para utilizar para el COCHE gobierna a los paquetes SYN del límite de velocidad?

Entienda su red. El tipo de tráfico determina el número de sesiones TCP activas para una cantidad fija de datos.

- El tráfico WWW tiene una mezcla mucho más alta de paquetes SYN TCP que el tráfico de la granja del ftp server.
- Las pilas del cliente de la PC tienden a reconocer por lo menos cada otro paquete TCP. Otras pilas pueden reconocer menos o más a menudo.
- Controle si usted necesita aplicar estas reglas del COCHE en el borde del usuario residencial o en el borde de la red del cliente.

```
users ---- { ISP } --- web farm
```

Para el WWW, aquí está la mezcla del tráfico:

Para cada fichero 5k que usted descargue de la granja de la red, la granja de la red recibe 560 bytes, como se muestra aquí:

- 80 [SYN, ACK] de los bytes
- 400 estructura del byte HTTP de los bytes [320, 2 ACK]
- 80 bytes [FIN, ACK]

Asuma que la relación de transformación entre el tráfico de salida de la granja de la red y el Tráfico de ingreso de la red cultiva is10:1. La cantidad de tráfico que compone los paquetes SYN es 120:1.

Si usted tiene un link OC3, usted limita la tarifa de los paquetes SYN TCP al 155 mbps/120 1.3 mbps del ==.

En la interfaz de ingreso en el router de granja Web, configure:

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```

Paquete TCP Syn la tarifa consigue tan más pequeña que la longitud de sus sesiones TCP consigue más de largo.

```
users ---- { ISP } --- MP3/FTP Farm
```

Los ficheros MP3 tienden a ser 4 a 5 mgbps de tamaño en una media. La transferencia directa de un fichero de 4 mgbps genera el Tráfico de ingreso esas cantidades a 3160 bytes:

- 80 [SYN, ACK] de los bytes
- 3000 [ACKs + FTP get] de los bytes
- 80 bytes [FIN, ACK]

El índice de TCP SYNs al tráfico de salida es == 155 mbps/120000 1.3 Kbps.

Configure

```
 rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```

¿Cómo sé si restrinjo demasiados paquetes SYN?

Si usted conoce su velocidad de conexión usual en sus servidores, usted puede comparar las figuras antes y después de que usted activa el COCHE. La comparación le ayuda a identificar el acontecimiento de un descenso en su velocidad de conexión. Si usted encuentra un descenso en la tarifa, incremente sus parámetros CAR para permitir más sesiones.

Controle si los usuarios pueden establecer a las sesiones TCP fácilmente. Si sus límites del COCHE son demasiado restrictivos, necesidad de usuarios de hacer las tentativas del múltiplo de establecer a una sesión TCP.

¿Puedo activar el COCHE en un router de switch Gigabit (GRS)?

Yes. Los linecards del motor 0 y del motor 1 utilizan el COCHE. El Cisco IOS Software Release 11.2(14)GS2 y Posterior proporciona la ayuda del COCHE. El impacto del rendimiento del COCHE depende del número de COCHE le gobierna se aplica.

El impacto del rendimiento es también mayor en los linecards del motor 1 que en los linecards del motor 0. Si usted quiere activar el COCHE en los linecards del motor 0, usted debe ser consciente del ID de bug CSCdp80432 (clientes registrados de Cisco solamente). Si usted quiere activar el tráfico Multicast del tarifa-límite del COCHE, asegúrese de que el ID de bug CSCdp32913 (clientes registrados de Cisco solamente) no le afecte. El ID de bug CSCdm56071 (clientes registrados de Cisco solamente) es otro bug que usted debe ser consciente de antes de que usted active el COCHE.

¿Puedo activar el CAR distribuido (dCAR) en Cisco 7500?

Sí, el dCAR de los Soportes de la plataforma RSP/VIP en el Cisco IOS Software Release 11.1(20)CC, y las 12.0 versiones de software.

El COCHE afecta el funcionamiento hasta cierto punto. De acuerdo con la configuración del COCHE, usted puede alcanzar la línea tarifa [for Internet Mix traffic] con un VIP2-50 [through dCAR] en un OC3. Asegúrese de que el ID de bug CSCdm56071 (clientes registrados de Cisco solamente) no le afecte. Si usted quiere utilizar para hacer salir el COCHE, el ID de bug CSCdp52926 (clientes registrados de Cisco solamente) puede afectar a su Conectividad. Si usted activa el dCAR, el ID de bug CSCdp58615 (clientes registrados de Cisco solamente) puede causar una caída VIP.

¿Puedo activar el COCHE en Cisco 7200?

Yes. El NPE utiliza el COCHE en el Cisco IOS Software Release 11.1(20)CC, y las 12.0 versiones de software.

El COCHE afecta el funcionamiento hasta cierto punto, sobre la base de la configuración del COCHE. Consiga los arreglos para estos bug: ID de bug CSCdm85458 (clientes registrados de Cisco solamente) y ID de bug CSCdm56071 (clientes registrados de Cisco solamente).

Nota: Un gran número de entradas del COCHE en un interfaz/un sub-interfaz degradan el funcionamiento porque el router necesita realizar una búsqueda lineal en los anunciados CAR para encontrar la declaración del “COCHE” que hace juego.

Otras funciones y alternativas'vv

El IP recibe el ACL

El Cisco IOS Software Release 12.0(22)S contiene el IP recibe la característica ACL en el router de Internet de las Cisco 12000 Series.

El IP recibe la característica ACL proporciona a los filtros básicos para el tráfico destinados para alcanzar al router. El router puede proteger el tráfico de protocolo prioritario de la encaminamiento contra un ataque porque la característica filtra todo el Access Control List de la entrada (ACL) en la interfaz de ingreso. El IP recibe los filtros de la característica ACL trafica en los linecards distribuidos antes de que el procesador de la ruta reciba los paquetes. Esta característica permite que los usuarios filtren las inundaciones de la negación de servicio (DOS) contra el router. Por lo

tanto, esta característica previene la degradación del rendimiento del procesador de la ruta.

Refiera al IP reciben el APL para más detalles.

Rastreador de origen de IP

El Cisco IOS Software Release 12.0(21)S utiliza la característica del Rastreador de origen de IP en el router de Internet de las Cisco 12000 Series. El Cisco IOS Software Release 12.0(22)S utiliza esta característica en el Cisco 7500 Series Router.

La característica del Rastreador de origen de IP permite que usted recopile la información sobre el tráfico que fluye a un host que usted sospeche esté bajo ataque. Esta característica también permite que usted rastree fácilmente un ataque al punto de entrada en la red. Cuando usted identifica el punto de ingreso a la red a través de esta característica, usted puede utilizar los ACL o el COCHE para bloquear el ataque con eficacia.

Refiera al Rastreador de origen de IP para más información.

Información Relacionada

- Cómo proteger su red del virus Nimda
- El IP recibe el APL
- Rastreador de origen de IP
- Soporte Técnico y Documentación - Cisco Systems