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 CAR 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 soportan el CAR.
- Cisco IOS Software Release 11.2 y Posterior, que soportan el modelado de tráfico.
- Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, que soportan el Modular QoS 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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Límite de velocidad ICMP/Smurf

Configure estas listas de acceso:

Para habilitar el CAR, usted debe habilitar el Cisco Express Forwarding (CEF) en el cuadro. Además, usted debe configurar una interfaz CEF-Switched para el CAR.

Los valores de ancho de banda de las aplicaciones de salida de muestra para el DS3 teclean los 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:

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:

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:

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:

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

Preguntas frecuentes sobre CAR

¿Cómo identificar los valores para utilizar para las reglas de CAR 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 un intercambio más elevado de los paquetes Syn TCP que el tráfico de bloque de servidores FTP.
- Los stack del PC cliente tienden a reconocer por lo menos cada otro paquete TCP. Otros stack pueden reconocer menos o más a menudo.
- Marque si usted necesita aplicar estas reglas de CAR en el borde del usuario residencial o en el borde de la red del cliente.

Para el WWW, aquí está la mezcla del tráfico:

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

- 80 bytes [SYN, ACK]
- 400 bytes [estructura HTTP de 320 bytes, 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 del 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, configuración:

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

Los archivos MP3 tienden a ser 4 a 5 mgbps de tamaño en una media. La descarga de un archivo del mgbps 4 genera el Tráfico de ingreso esas cantidades a 3160 bytes:

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

La velocidad de salida de tráfico de SYN TCP es de 155 mbps / 120000 == 1.3 kbps

Configure

¿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 habilita el CAR. 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.

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

¿Es posible habilitar CAR en un router de switch Gigabit (GSR)?

Sí. Soporte CAR del linecards del motor 0 y del motor 1. El Cisco IOS Software Release 11.2(14)GS2 y Posterior proporciona el soporte CAR. El impacto del rendimiento del CAR depende del número de reglas de CAR que usted se aplica.

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

¿Puedo habilitar la CAR distribuida (dCAR) en un 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.

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

¿Puedo habilitar CAR en un Cisco 7200?

Sí. El NPE soporta el CAR en el Cisco IOS Software Release 11.1(20)CC, y las 12.0 versiones de software.

CAR impacto en el rendimiento hasta cierto punto, sobre la base de la configuración CAR. Consiga los arreglos para estos bug: Id. de bug Cisco CSCdm85458 (clientes registrados solamente) y CSCdm56071 del Id. de bug Cisco (clientes registrados solamente).

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

Otras funciones y alternativas'vv

ACL de IP de recepción

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

El IP recibe la característica ACL proporciona los filtros básicos para el tráfico destinados para alcanzar al router. El router puede proteger el tráfico del Routing Protocol prioritario 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 el linecards distribuido antes de que el Route Processor 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 Route Processor.

Refiera al IP reciben el APL para más detalles.

Rastreador de origen de IP

El Cisco IOS Software Release 12.0(21)S soporta la característica del Rastreador de origen de IP en el Cisco 12000 Series Internet Router. El Cisco IOS Software Release 12.0(22)S soporta 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 CAR 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