Usando CAR durante ataques de DOS

Índice

Introdução

Às vezes, uma rede recebe um córrego de pacotes do ataque de recusa de serviço (DOS) junto com o tráfego de rede regular. Em tais situações, você pode usar um mecanismo chamado “taxa que limita” a fim permitir que o desempenho da rede degrade, de modo que a rede permaneça acima. Você pode usar o software do ® do Cisco IOS para conseguir a taxa que limita com estes esquemas:

- Committed Access Rate (CAR)
- Modelagem de tráfego
- Modelagem e vigilância através da interface da linha de comando da Qualidade de Serviço modular (QoS CLI)

Este documento discute o CAR para o uso em ataques DoS. Os outros esquemas são apenas variações do conceito básico.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS Software Release 11.1CC e mainline 12.0, que apoiam o CAR.
- Cisco IOS Software Release 11.2 e Mais Recente, que apoiam o modelagem de tráfego.
- Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, que apoiam o Modular QoS CLI.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Limite de taxa ICMP/Smurf

Configurar estas listas de acesso:

```
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
```

A fim permitir o CAR, você deve permitir o Cisco Express Forwarding (CEF) na caixa. Além, você deve configurar uma relação comutado por CEF para o CAR.

O exemplo de saída usa valores de largura de banda para DS3 o tipo larguras de banda. Escolha os valores baseados na largura de banda de interface e na taxa em que você quer limitar um tipo particular de tráfego. Para interfaces de ingresso menores, você pode configurar taxas mais baixa.

Pacotes SYN de TCP do limite de taxa

11.1(X)CC

Se você sabe que host está sob o ataque, configurar estas Listas de acesso:

```
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: Neste exemplo, o host sob o ataque é 10.0.0.1.

Se você não o conhece que host está sob o ataque DoS, e quer proteger uma rede, configurar estas Listas de acesso:

```
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: Limite de taxa a 64000 bps para todos os pacotes SYN de TCP.

12.0(X)[S/T/M]

Se você sabe que host está sob o ataque, configurar estas Listas de acesso:

```
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: Neste exemplo, 10.0.0.1 é o host sob o ataque.

Se você não é certo que o host é sob o ataque, e você quer proteger uma rede, configurar estas Listas de acesso:

```
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: Limite de taxa a 64000 bps para todos os pacotes SYN de TCP.

Perguntas mais freqüentes sobre o CAR

Como identificar os valores para se usar para as regras CAR aos pacotes SYN do limite de taxa?

Compreenda a sua rede. O tipo de tráfego determina o número de sessões de TCP ativas para uma quantidade fixa de dados.

- O tráfego de WWW tem uma combinação muito mais alta de pacotes TCP Syn do que o tráfego do server farm de FTP.
- As pilhas do cliente de PC tendem a reconhecer pelo menos cada outro pacote de TCP. Outras pilhas podem reconhecer menos ou mais frequentemente.
- Verifique se você precise de aplicar estas regras CAR na borda do usuário residencial ou na margem de rede do cliente.

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

Para o WWW, está aqui a mistura do tráfego:

Para cada arquivo 5k que você transfere da exploração agrícola da Web, a exploração agrícola da Web recebe 560 bytes, como mostrado aqui:

- 80 bytes [SYN, ACK]
- 400 bytes [estrutura HTTP de 320 bytes, 2 ACKs]
- 80 bytes [FIN, ACK]

Supõe que a relação entre o tráfego de saída da exploração agrícola da Web e o tráfego de ingresso da Web cultiva is10:1. A quantidade de tráfego que compõe pacotes SYN é 120:1.

Se você tem um link OC3, você limita a taxa dos pacotes SYN de TCP ao 155 mbps/120 1.3 mbps do ==.

Na interface de ingresso no roteador farm da Web, configurar:

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

A taxa do pacote SYN de TCP obtém por mais menor que o comprimento de suas sessões de TCP obtenha mais por muito tempo.

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

Os arquivos MP3 tendem a ser 4 ao mgbps 5 em tamanho em uma média. A transferência de um arquivo de 4 mgbps gerencie o tráfego de ingresso essas quantidades a 3160 bytes:

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

A taxa de TCP SYNs para tráfego de saída é de 155 mbps / 120000 == 1,3 kbps.

Configurar:

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

Como eu sei se eu restrinjo pacotes SYN demais?

Se você conhece sua taxa de conexão usual em seus server, você pode comparar as figuras antes e depois de que você permite o CAR. A comparação ajuda-o a identificar a ocorrência de uma gota em sua taxa de conexão. Se você encontra uma gota na taxa, incremente seus parâmetros CAR para permitir mais sessões.

Verifique se os usuários possam estabelecer facilmente sessões de TCP. Se seus limites CAR são demasiado restritivos, necessidade de usuários de fazer tentativas do múltiplo de estabelecer uma sessão de TCP.

Posso ativar o CAR em um Gigabit Switch Router (GSR)?

Yes. As placas de linha do motor 0 e do motor 1 apoiam o CAR. O Cisco IOS Software Release 11.2(14)GS2 e Mais Recente fornece o apoio CAR. O impacto no desempenho do CAR depende do número de regras CAR que você se aplica.

O impacto no desempenho é igualmente maior em placas de linha do motor 1 do que em placas de linha do motor 0. Se você quer permitir o CAR em placas de linha do motor 0, você deve estar

ciente da identificação de bug Cisco CSCdp80432 (clientes registrados somente). Se você quer permitir o tráfego multicast do taxa-limite CAR, assegure-se de que a identificação de bug Cisco CSCdp32913 (clientes registrados somente) não o afete. O CSCdm56071 da identificação de bug Cisco (clientes registrados somente) é um outro erro que você deve estar ciente de antes que você permita o CAR.

Posso ativar CAR (dCAR) distribuído em um Cisco 7500?

Sim, o dCAR dos suportes a plataforma RSP/VIP no Cisco IOS Software Release 11.1(20)CC, e todos os 12.0 software release.

CAR impacta NO desempenho em certa medida. Baseado na configuração CAR, você pode conseguir a linha [for Internet Mix traffic] da taxa com um [through dCAR] VIP2-50 em um OC3. Assegure-se de que o CSCdm56071 da identificação de bug Cisco (clientes registrados somente) não o afete. Se você quer se usar para output o CAR, a identificação de bug Cisco CSCdp52926 (clientes registrados somente) pode afetar sua Conectividade. Se você permite o dCAR, a identificação de bug Cisco CSCdp58615 (clientes registrados somente) pode causar um travamento de VIP.

É possível habilitar CAR em um Cisco 7200?

Yes. O NPE apoia o CAR no Cisco IOS Software Release 11.1(20)CC, e todos os 12.0 software release.

CAR impacta NO desempenho em certa medida, com base na configuração CAR. Obtenha reparos para estes erros: Identificação de bug Cisco CSCdm85458 (clientes registrados somente) e CSCdm56071 da identificação de bug Cisco (clientes registrados somente).

Nota: Um grande número entradas de CAR em uma relação/relação degradam o desempenho porque o roteador precisa de executar uma pesquisa linear nas declarações de CAR para encontrar a indicação “CAR” que combina.

Outros recursos e alternativas

ACL de recebimento de IP

O Cisco IOS Software Release 12.0(22)S contém o IP recebe recursos ACL no Cisco 12000 Series Internet Router.

O IP recebe recursos ACL fornece os filtros básicos para o tráfego destinados para alcançar o roteador. O roteador pode proteger o tráfego do protocolo de roteamento prioritário de um ataque porque a característica filtra todo o Access Control List da entrada (ACL) na interface de ingresso. O IP recebe recursos ACL que os filtros traficam nas placas de linha distribuídas antes que o processador de rotas receba pacotes. Esta característica permite que os usuários filtrem a recusa de inundações do serviço (DoS) contra o roteador. Consequentemente, esta característica impede a degradação do desempenho do processador de rotas.

Refira o IP recebem o APL para mais detalhes.

Rastreador de fonte de IP

O Cisco IOS Software Release 12.0(21)S apoia a característica IP Source Tracker no Cisco 12000 Series Internet Router. O Cisco IOS Software Release 12.0(22)S apoia esta característica no Cisco 7500 Series Router.

A característica IP Source Tracker permite que você recolha a informação sobre o tráfego que flui a um host que você suspeite esteja sob o ataque. Esta característica igualmente permite que você siga facilmente um ataque de volta ao ponto de entrada na rede. Quando você identifica o ponto de ingresso de rede através desta característica, você pode usar ACL ou CAR para obstruir eficazmente o ataque.

Refira o IP Source Tracker para mais informação.

Informações Relacionadas

- Como proteger sua rede contra o vírus Nimda
- O IP recebe o APL
- Rastreador de fonte de IP
- Suporte Técnico e Documentação - Cisco Systems