Uso di CAR durante gli attacchi DOS

Sommario

Introduzione

A volte, una rete riceve un flusso di pacchetti DoS (Denial of Service) che attaccano insieme al normale traffico di rete. In tali situazioni, è possibile utilizzare un meccanismo denominato "limitazione della velocità" per ridurre le prestazioni della rete e mantenere attiva la rete. È possibile utilizzare il software Cisco IOS® per ottenere limitazioni di velocità tramite questi schemi:

- Committed Access Rate (CAR)
- Traffic Shaping
- Shaping e applicazione di policy tramite l'interfaccia della riga di comando Modular Quality of Service (QoS CLI)

In questo documento viene descritto l'uso di CAR negli attacchi DoS. Gli altri schemi sono solo varianti del concetto di base.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 11.1CC e 12.0 mainline, che supportano CAR.
- Software Cisco IOS versione 11.2 e successive, che supporta Traffic Shaping.
- Software Cisco IOS release 12.0XE, 12.1E, 12.1T, che supportano Modular QoS CLI.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Limite di velocità ICMP/Smurf

Configurare i seguenti elenchi degli accessi:

```
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
```

Per abilitare CAR, è necessario abilitare Cisco Express Forwarding (CEF) nella confezione. Inoltre, è necessario configurare un'interfaccia a commutazione CEF per CAR.

L'output di esempio utilizza i valori della larghezza di banda per le larghezze di banda di tipo DS3. Selezionare i valori in base alla larghezza di banda dell'interfaccia e alla velocità alla quale si desidera limitare un particolare tipo di traffico. Per interfacce in entrata più piccole, potete configurare velocità inferiori.

Limite di velocità - Pacchetti TCP SYN

11.1(X)CC

Se si conosce l'host sotto attacco, configurare i seguenti elenchi degli accessi:

```
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: nell'esempio, l'host sotto attacco è 10.0.0.1.

Se non si conosce l'host soggetto ad attacchi DoS e si desidera proteggere una rete, configurare i seguenti elenchi degli accessi:

```
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: la velocità massima è di 64000 bps per tutti i pacchetti TCP SYN.

12.0(X)[S/T/M]

Se si conosce l'host sotto attacco, configurare i seguenti elenchi degli accessi:

```
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: nell'esempio, 10.0.0.1 è l'host sotto attacco.

Se non si è certi dell'host soggetto a attacco e si desidera proteggere una rete, configurare i seguenti elenchi degli accessi:

```
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: la velocità massima è di 64000 bps per tutti i pacchetti TCP SYN.

Domande frequenti su CAR

Come identificare i valori da utilizzare per le regole CAR per limitare la velocità dei pacchetti SYN?

Comprendere la rete. Il tipo di traffico determina il numero di sessioni TCP attive per una quantità fissa di dati.

- Il traffico WWW presenta una combinazione molto più ampia di pacchetti TCP SYN rispetto al traffico della server farm FTP.
- Gli stack di client PC tendono a riconoscere almeno un pacchetto TCP ogni due. Altri stack possono riconoscere meno o più spesso.
- Verificare se è necessario applicare queste regole CAR sul perimetro dell'utente residenziale o sul perimetro della rete del cliente.

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

Per WWW, ecco il mix di traffico:

Per ogni file da 5 KB scaricato dalla Web farm, la Web farm riceve 560 byte, come illustrato di seguito:

- 80 byte [SYN, ACK]
- 400 byte [struttura HTTP da 320 byte, 2 ACK]
- 80 byte [FIN, ACK]

Si supponga che il rapporto tra il traffico in uscita dalla Web farm e il traffico in entrata dalla Web farm sia 10:1. La quantità di traffico che costituisce i pacchetti SYN è 120:1.

Se si dispone di un collegamento OC3, la velocità dei pacchetti TCP SYN viene limitata a 155 mbps / 120 = 1,3 mbps.

Nell'interfaccia in entrata del router della Web farm configurare:

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

La velocità del pacchetto TCP SYN diminuisce con l'aumentare della lunghezza delle sessioni TCP.

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

I file MP3 tendono ad avere in media dimensioni da 4 a 5 Mbps. Il download di un file da 4 mgbps genera un traffico in entrata pari a 3160 byte:

- 80 byte [SYN, ACK]
- 3000 byte [ACK + FTP get]
- 80 byte [FIN, ACK]

La velocità delle SYN TCP per il traffico in uscita è 155 mbps / 12000 = 1,3 kbps.

Configurazione:

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

Come è possibile stabilire se si limitano troppi pacchetti SYN?

Se si conosce la frequenza di connessione abituale sui server, è possibile confrontare le cifre prima e dopo l'abilitazione di CAR. Il confronto consente di identificare l'occorrenza di un calo nella velocità di connessione. Se si riscontra un calo della velocità, incrementare i parametri CAR per consentire più sessioni.

Verificare se gli utenti sono in grado di stabilire facilmente sessioni TCP. Se i limiti CAR sono troppo restrittivi, gli utenti devono eseguire più tentativi per stabilire una sessione TCP.

È possibile abilitare l'autenticazione CAR su un router switch Gigabit (GSR)?

Sì. Il motore 0 e le schede di linea del motore 1 supportano CAR. Il software Cisco IOS versione 11.2(14)GS2 e successive supporta le unità CAR. L'impatto sulle prestazioni di CAR dipende dal numero di regole CAR applicate.

L'impatto sulle prestazioni è maggiore anche sulle schede di linea del motore 1 rispetto alle schede di linea del motore 0. Per abilitare l'autenticazione CAR sulle schede di linea del motore 0, è necessario conoscere l'ID bug Cisco CSCdp80432 (solo utenti registrati). Se si desidera abilitare la funzionalità CAR per limitare la velocità del traffico multicast, verificare che l'ID bug Cisco CSCdp32913 (solo utenti registrati) non influisca sull'utente. Un altro bug di cui è necessario essere a conoscenza prima di abilitare l'ACL è l'ID bug Cisco CSCdm56071 (solo utenti registrati).

È possibile abilitare Distributed CAR (dCAR) su un Cisco 7500?

Sì, la piattaforma RSP/VIP supporta dCAR nel software Cisco IOS versione 11.1(20)CC e in tutte le versioni 12.0.

La CAR ha un impatto sulle prestazioni in una certa misura. In base alla configurazione CAR, è possibile ottenere la velocità della linea [per il traffico Internet Mix] con un VIP2-50 [tramite dCAR] su una OC3. Verificare che l'ID bug Cisco CSCdm56071 (solo utenti registrati) non influisca sulla configurazione. Se si desidera utilizzare l'output CAR, l'ID bug Cisco CSCdp52926 (solo utenti registrati) può influire sulla connettività. Se si abilita dCAR, l'ID bug Cisco CSCdp58615 (solo utenti registrati) può causare un crash del VIP.

Posso abilitare CAR su Cisco 7200?

Sì. NPE supporta CAR nel software Cisco IOS versione 11.1(20)CC e tutte le versioni 12.0.

CAR ha un impatto sulle prestazioni in una certa misura, in base alla configurazione CAR. Correzioni ai seguenti bug: ID bug Cisco CSCdm85458 (solo utenti registrati) e ID bug Cisco CSCdm56071 (solo utenti registrati).

Nota: un numero elevato di voci CAR in un'interfaccia/sottointerfaccia riduce le prestazioni in quanto il router deve eseguire una ricerca lineare sulle istruzioni CAR per trovare l'istruzione "CAR" corrispondente.

Altre caratteristiche e alternative

ACL di ricezione IP

Il software Cisco IOS versione 12.0(22)S contiene la funzionalità IP Receive ACL su Cisco serie 12000 Internet Router.

La funzionalità IP Receive ACL fornisce filtri di base per il traffico destinato a raggiungere il router. Il router può proteggere il traffico del protocollo di routing ad alta priorità da un attacco perché la funzione filtra tutti gli elenchi di controllo di accesso (ACL) di input sull'interfaccia in entrata. La funzionalità IP Receive ACL filtra il traffico sulle schede di linea distribuite prima che il processore di routing riceva i pacchetti. Questa funzionalità consente agli utenti di filtrare i flussi DoS (Denial of Service) contro il router. Pertanto, questa funzione impedisce il peggioramento delle prestazioni del processore di routing.

Per ulteriori informazioni, fare riferimento a IP Receive APL.

Tracker origine IP

Il software Cisco IOS versione 12.0(21)S supporta la funzione IP Source Tracker sui router Internet Cisco serie 12000. Il software Cisco IOS versione 12.0(22)S supporta questa funzione sui router Cisco serie 7500.

La funzionalità Tracker origine IP consente di raccogliere informazioni sul traffico che fluisce verso un host che si sospetta sia sotto attacco. Questa funzione consente anche di tracciare facilmente un attacco al punto di ingresso nella rete. Quando si identifica il punto di ingresso della rete tramite questa funzione, è possibile usare gli ACL o l'CAR per bloccare l'attacco in modo efficace.

Per ulteriori informazioni, fare riferimento a IP Source Tracker.

Informazioni correlate

- Come proteggere la rete dal virus Nimda
- APL di ricezione IP
- Tracker origine IP
- Documentazione e supporto tecnico – Cisco Systems