CAR gebruiken tijdens DOS-aanvallen

Inhoud

Inleiding

Soms ontvangt een netwerk een stream van Denial of Service (DoS) aanval pakketten samen met het normale netwerkverkeer. In dergelijke situaties kunt u een mechanisme gebruiken dat "rate limit" wordt genoemd om de netwerkprestaties te laten afbreken, zodat het netwerk omhoog blijft. U kunt de software van Cisco IOS® gebruiken om snelheidsbeperking door deze programma's te realiseren:

- Committed Access Rate (CAR)-beperking
- traffic shaping
- Shaping en toezicht door modulaire Quality of Service Opdracht Line Interface (QoS CLI)

In dit document wordt de CAR besproken voor gebruik in DOD-aanvallen. De andere regelingen zijn slechts varianten van het basisconcept.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 11.1CC en 12.0 hoofdlijn, die CAR ondersteunen.
- Cisco IOS-softwarerelease 11.2 en hoger, die traffic shaping ondersteunen.
- Cisco IOS-softwarereleases 12.0XE, 12.1E, 12.1T, die modulaire QoS CLI ondersteunen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Snelheidslimiet ICMP/Smurf

Configuratie van deze toegangslijsten:

```
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
```

Om CAR in te schakelen moet u Cisco Express Forwarding (CEF) in het vakje inschakelen. Daarnaast moet u een CEF-switched interface voor CAR configureren.

De steekproefuitvoer gebruikt bandbreedtewaarden voor DS3 type bandbreedte. Kies waarden op basis van de interfacebandbreedte en het tarief waarmee u een bepaald type verkeer wilt beperken. Voor kleinere ingangsinterfaces kunt u lagere snelheden configureren.

Snelheidsbeperking TCP SYN-pakketten

11.1(X)CC

Als u weet welke host wordt aangevallen, moet u deze toegangslijsten configureren:

```
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
```

Opmerking: In dit voorbeeld is de gastheer onder aanval 10.0.0.1.

Als u niet weet welke host onder een DoS-aanval valt en u een netwerk wilt beveiligen, moet u deze toegangslijsten configureren:

```
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
```

Opmerking: Snelheidsbeperking tot 64000 bps voor alle TCP SYN-pakketten.

12.0(X)[S/T/M]

Als u weet welke host wordt aangevallen, moet u deze toegangslijsten configureren:

```
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
```

Opmerking: In dit voorbeeld is 10.0.0.1 de gastheer onder aanval.

Als u niet zeker bent welke host onder aanval staat en u een netwerk wilt beveiligen, moet u deze toegangslijsten configureren:

```
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
```

Opmerking: Snelheidsbeperking tot 64000 bps voor alle TCP SYN-pakketten.

CAR vaak gestelde vragen

Hoe identificeert u de waarden die u moet gebruiken voor de CAR-regels voor de snelheidsbeperking in SYN-pakketten?

Begrijp uw netwerk. Het type verkeer bepaalt het aantal actieve TCP sessies voor een vaste hoeveelheid gegevens.

- WW-verkeer heeft een veel hogere mix van TCP SYN-pakketten dan FTP-serverboerderij.
- PC client stacks hebben de neiging om ten minste elk ander TCP-pakket te erkennen. Andere zakken kunnen minder of vaker erkennen.
- Controleer of u deze CAR-regels moet toepassen op de rand van de gebruiker of op de rand van het netwerk van de klant.

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

Voor WW, hier is de verkeersmix:

Voor elk 5k bestand dat u vanuit de webboerderij downloaden, ontvangt de webboerderij 560 bytes, zoals hier wordt getoond:

- 80 bytes [SYN, ACK]

- 400 bytes [320 bytes HTTP-structuur, 2 ACK's]
- 80 bytes [FIN, ACK]

Stel dat de verhouding tussen het drukverkeer van de webinderij en het toegangsverkeer van de webboerderij 10:1 is. De hoeveelheid verkeer die SYN-pakketten opstelt, is 120:1.

Als u een OC3 Link hebt, beperkt u de TCP SYN-pakketsnelheid tot 155 mbps / 120 = 1.3 mbps.

Op de ingangsinterface in de router van de Web landbouwbedrijf, moet u configureren:

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

De TCP SYN-pakketsnelheid wordt kleiner naarmate de lengte van uw TCP-sessies langer wordt.

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

MP3-bestanden hebben gemiddeld 4 tot 5 Gbps groot. Downloaden van een 4 Gbps bestand genereert toegangsverkeer met een waarde van 3160 bytes:

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

Het aantal TCP SYNs dat op hoger verkeer drukt is 155 mbps / 12000 = 1,3 kbps.

Configureren:

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

Hoe weet ik of ik te veel SYN-pakketten beperk?

Als u uw gebruikelijke verbindingssnelheid op uw servers kent, kunt u de cijfers vergelijken voor en na het inschakelen van de CAR. De vergelijking helpt u het voorkomen van een daling in uw verbindingssnelheid te identificeren. Als je een daling in de snelheid vindt, verhoog dan je CAR parameters om meer sessies toe te staan.

Controleer of de gebruikers in staat zijn om TCP sessies makkelijk in te stellen. Als uw CAR beperkingen te restrictief zijn, moeten de gebruikers meerdere pogingen doen om een TCP sessie op te zetten.

Kan ik CAR op een Gigabit-switchrouter (GSR) inschakelen?

Ja. Engine 0 en Engine 1 lijnkaarten ondersteunen CAR. Cisco IOS-softwarerelease 11.2(14)GS2 en biedt later CAR-ondersteuning. De impact van CAR hangt af van het aantal CAR-regels dat u toepast.

Het effect van de prestaties is ook groter op de lijnkaarten van Engine 1 dan op de lijnkaarten van Engine 0. Als u CAR op Engine 0 wilt inschakelen moet u zich bewust zijn van Cisco bug-ID CSCdp80432 (alleen geregistreerde klanten). Als u CAR wilt in staat stellen om multicast verkeer te beperken, zorg er dan voor dat Cisco bug-ID CSCdp32913 (alleen geregistreerde klanten) u niet beïnvloedt. Cisco bug-ID CSCdm56071 (alleen geregistreerde klanten) is een andere bug die u moet kennen voordat u CAR activeert.

Kan ik gedistribueerde CAR (dCAR) inschakelen op een Cisco 7500-netwerk?

Ja, het RSP/VIP-platform ondersteunt dCAR in Cisco IOS-softwarerelease 11.1(20)CC en alle 12.0 softwarereleases.

CAR heeft tot op zekere hoogte invloed op prestaties. Op basis van de CAR-configuratie kunt u lijnsnelheid [voor Internet Mix Traffic] bereiken met een VIP2-50 [via dCAR] op een OC3. Zorg ervoor dat Cisco bug-id CSCdm56071 (alleen geregistreerde klanten) u niet beïnvloedt. Als u uitvoer CAR wilt gebruiken, kan Cisco bug-ID CSCdp52926 (alleen geregistreerde klanten) uw connectiviteit beïnvloeden. Als u dCAR toestaat, kan Cisco bug-ID CSCdp58615 (alleen geregistreerde klanten) een VIP-crash veroorzaken.

Kan ik CAR op een Cisco 7200 inschakelen?

Ja. NPE ondersteunt CAR in Cisco IOS-softwarereleases 11.1(20)CC en alle 12.0 softwarereleases.

CAR heeft tot op zekere hoogte invloed op prestaties op basis van de CAR-configuratie. Zoek fixes voor deze insecten: Cisco bug-ID CSCdm85458 (alleen geregistreerde klanten) en Cisco bug-ID CSCdm56071 (alleen geregistreerde klanten).

Opmerking: Een groot aantal CAR-items in een interface/subinterface verminderen de prestaties omdat de router een lineair zoeken op de CAR-verklaringen moet uitvoeren om de CAR-verklaring te vinden die overeenkomt met de CAR-gegevens.

Overige functies en alternatieven

IP-ontvanger ACL

Cisco IOS-softwarerelease 12.0(22)S bevat de optie IP-ontvanger ACL op Cisco 12000 Series internetrouter.

De functie IP ontvangt ACL's (basisfilters) voor verkeer dat bestemd is om de router te bereiken. De router kan het routeprotocolverkeer met hoge prioriteit tegen een aanval beveiligen omdat de eigenschap alle controlelijst voor ingangstoegang (ACL) op de ingangsinterface filtreert. IP Ontvang ACL de eigenschappen filters verkeer op de verdeelde lijnkaarten alvorens de routeprocessor pakketten ontvangt. Met deze functie kunnen gebruikers water uit de Service (DoS) tegen de router filteren. Daarom voorkomt deze optie dat de routeprocessor afbreekt.

Raadpleeg IP-ontvangerAPL voor meer informatie.

IP-brontracker

Cisco IOS-softwarerelease 12.0(21)S ondersteunt de functie IP-brontracker op Cisco 12000 Series internetrouter. Cisco IOS-softwarerelease 12.0(22)S ondersteunt deze functie op Cisco 7500 Series router.

Met de functie IP Source Tracker kunt u informatie verzamelen over het verkeer dat naar een host stroomt waarvan u vermoedt dat het onder vuur ligt. Met deze functie kunt u een aanval ook eenvoudig terugvinden naar het invoerpunt in het netwerk. Wanneer u het punt van de

netwerkingang door deze eigenschap identificeert, kunt u ACLs of CAR gebruiken om de aanval effectief te blokkeren.

Raadpleeg de IP-brontracker voor meer informatie.

Gerelateerde informatie

- Uw netwerk beschermen tegen het NIMA-virus
- IP-ontvanger APL
- IP-brontracker
- Technische ondersteuning en documentatie – Cisco Systems