DOS 공격 중 CAR 사용

목차

소개

때로는 네트워크가 일반 네트워크 트래픽과 함께 DoS(Denial of Service) 공격 패킷의 스트림을 수신하기도 합니다.이러한 경우 네트워크 성능이 저하될 수 있도록 "속도 제한"이라는 메커니즘을 사용하여 네트워크가 작동 상태로 유지되도록 할 수 있습니다.Cisco IOS® 소프트웨어를 사용하여 다음 체계를 통해 속도 제한을 달성할 수 있습니다.

- CAR(Committed Access Rate)
- 트래픽 셰이핑
- 모듈형 QoS CLI(Quality of Service Command Line Interface)를 통한 쉐이핑 및 폴리싱

이 문서에서는 DoS 공격에 사용되는 CAR에 대해 설명합니다.다른 계획은 단지 기본 개념의 변형일 뿐이다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 11.1CC 및 12.0 메인라인(CAR 지원)
- 트래픽 셰이핑을 지원하는 Cisco IOS Software 릴리스 11.2 이상.
- Cisco IOS Software 릴리스 12.0XE, 12.1E, 12.1T - 모듈형 QoS CLI를 지원합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

속도 제한 ICMP/Smurf

다음 액세스 목록을 구성합니다.

```
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
```

CAR을 활성화하려면 상자에서 Cisco CEF(Express Forwarding)를 활성화해야 합니다.또한 CAR용 CEF 스위치드 인터페이스를 구성해야 합니다.

샘플 출력은 DS3 유형 대역폭에 대한 대역폭 값을 사용합니다.인터페이스 대역폭 및 특정 트래픽 유형을 제한할 속도를 기반으로 값을 선택합니다.더 작은 인그레스 인터페이스의 경우 낮은 속도를 구성할 수 있습니다.

속도 제한 TCP SYN 패킷

11.1(X)CC

공격 중인 호스트를 알고 있는 경우 다음 액세스 목록을 구성합니다.

```
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
```

참고: 이 예에서는 공격 중인 호스트가 10.0.0.1입니다.

DoS 공격 대상 호스트를 모르고 네트워크를 보호하려는 경우 다음 액세스 목록을 구성합니다.

```
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
```

참고: 모든 TCP SYN 패킷에 대해 속도가 64,000bps로 제한됩니다.

12.0(X)[S/T/M]

공격 중인 호스트를 알고 있는 경우 다음 액세스 목록을 구성합니다.

```
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
```

참고: 이 예에서는 10.0.0.1이 공격 중인 호스트입니다.

어떤 호스트가 공격을 받고 있는지 확실하지 않고 네트워크를 보호하려는 경우 다음 액세스 목록을 구성합니다.

```
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
```

참고: 모든 TCP SYN 패킷에 대해 속도가 64,000bps로 제한됩니다.

CAR FAQ

CAR 규칙에서 SYN 패킷 속도 제한을 위해 사용할 값을 식별하는 방법?

네트워크를 파악하십시오.트래픽 유형은 고정 양의 데이터에 대한 활성 TCP 세션 수를 결정합니다
.

- WWW 트래픽은 FTP 서버 팜 트래픽보다 TCP SYN 패킷이 훨씬 더 많이 혼합되어 있습니다.
- PC 클라이언트 스택은 적어도 다른 모든 TCP 패킷을 승인하는 경향이 있습니다.다른 스택은 더 적게 또는 더 자주 승인할 수 있습니다.
- 가정용 사용자 에지에 이러한 CAR 규칙을 적용할지 고객 네트워크 에지에 적용해야 하는지 확인합니다.

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

WWW의 경우 다음과 같은 트래픽 조합이 있습니다.

웹 팜에서 다운로드하는 모든 5k 파일에 대해 웹 팜은 다음과 같이 560바이트를 수신합니다.

- 80바이트 [SYN, ACK]
- 400바이트 [320바이트 HTTP 구조, 2ACK]
- 80바이트 [FIN, ACK]

웹 팜의 이그레스 트래픽과 웹 팜의 인그레스 트래픽 간의 비율이 10:1이라고 가정합니다. SYN 패킷을 구성하는 트래픽의 양은 120:1입니다.

OC3 링크가 있는 경우 TCP SYN 패킷 속도를 155mbps/120 == 1.3mbps로 제한합니다.

웹 팜 라우터의 인그레스 인터페이스에서 다음을 구성합니다.

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

TCP SYN 패킷 속도는 TCP 세션의 길이가 길수록 작아집니다.

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

MP3 파일의 크기는 평균 4~5mgbps입니다.4mgbps 파일을 다운로드하면 3160바이트에 달하는 인그레스 트래픽이 생성됩니다.

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

이그레스 트래픽에 대한 TCP SYN 속도는 155mbps/12000 == 1.3kbps입니다.

구성:

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

너무 많은 SYN 패킷을 제한하는지 어떻게 알 수 있습니까?

서버의 일반적인 연결 속도를 알고 있는 경우 CAR을 활성화하기 전과 후에 수치를 비교할 수 있습니다.이 비교는 연결 속도가 저하되는 경우를 식별하는 데 도움이 됩니다.속도가 떨어지는 경우 CAR 매개변수를 증가시켜 더 많은 세션을 허용합니다.

사용자가 TCP 세션을 쉽게 설정할 수 있는지 확인합니다.CAR 제한이 너무 제한적인 경우 사용자는 TCP 세션 설정을 여러 번 시도해야 합니다.

GSR(Gigabit Switch Router)에서 CAR을 활성화할 수 있습니까?

예.엔진 0 및 엔진 1 라인 카드는 CAR을 지원합니다.Cisco IOS Software 릴리스 11.2(14)GS2 이상에서는 CAR 지원을 제공합니다.CAR의 성능 영향은 적용하는 CAR 규칙의 수에 따라 달라집니다.

엔진 1 라인 카드에서도 Engine 0 라인 카드보다 성능에 미치는 영향이 큽니다.Engine 0 라인 카드에서 CAR을 활성화하려면 Cisco 버그 ID CSCdp80432를 알고 있어야 합니다(등록된 고객만 해당). CAR에서 멀티캐스트 트래픽 속도를 제한하도록 하려면 Cisco 버그 ID CSCdp32913(등록된 고객만)이 영향을 미치지 않는지 확인합니다.Cisco 버그 ID CSCdm56071(등록된 고객만 해당)은 CAR을 활성화하기 전에 알아야 할 또 다른 버그입니다.

Cisco 7500에서 dCAR(Distributed CAR)을 활성화할 수 있습니까?

예, RSP/VIP 플랫폼은 Cisco IOS Software 릴리스 11.1(20)CC에서 dCAR과 모든 12.0 소프트웨어 릴리스를 지원합니다.

CAR은 성능에 어느 정도 영향을 미칩니다.CAR 구성에 따라 OC3의 VIP2-50 [through dCAR]을 사용하여 라인 레이트[인터넷 혼합 트래픽의 경우]를 달성할 수 있습니다. Cisco 버그 ID CSCdm56071(등록된 고객만 해당)가 영향을 미치지 않는지 확인하십시오.출력 CAR을 사용하려면 Cisco 버그 ID CSCdp52926(등록된 고객만 해당)이 연결에 영향을 줄 수 있습니다.dCAR을 활성화

하면 Cisco 버그 ID CSCdp58615(등록된 고객만 해당)가 VIP 충돌을 일으킬 수 있습니다.

Cisco 7200에서 CAR을 활성화할 수 있습니까?

예.NPE는 Cisco IOS Software 릴리스 11.1(20)CC에서 CAR과 모든 12.0 소프트웨어 릴리스를 지원합니다.

CAR은 CAR 컨피그레이션에 따라 어느 정도 성능에 영향을 미칩니다.다음 버그에 대한 수정 사항 가져오기:Cisco 버그 ID CSCdm85458(등록된 고객만 해당) 및 Cisco 버그 ID CSCdm56071(등록된 고객만 해당).

참고: 인터페이스/하위 인터페이스의 많은 CAR 항목은 성능이 저하됩니다. 라우터가 CAR 문에 대해 선형 검색을 수행하여 일치하는 "CAR" 문을 찾아야 하기 때문입니다.

기타 기능 및 대안

IP 수신 ACL

Cisco IOS Software Release 12.0(22)S에는 Cisco 12000 Series 인터넷 라우터의 IP 수신 ACL 기능이 포함되어 있습니다.

IP Receive ACL 기능은 라우터에 도달할 트래픽에 대한 기본 필터를 제공합니다.이 기능은 인그레스 인터페이스의 모든 ACL(Input Access Control List)을 필터링하므로 라우터는 공격으로부터 높은 우선순위 라우팅 프로토콜 트래픽을 보호할 수 있습니다.IP Receive ACL 기능은 경로 프로세서가 패킷을 수신하기 전에 분산 라인 카드의 트래픽을 필터링합니다.이 기능을 사용하면 라우터에 대한 DoS(Denial of Service) 플러드를 필터링할 수 있습니다.따라서 이 기능은 경로 프로세서의 성능 저하를 방지합니다.

자세한 내용은 IP Receive APL을 참조하십시오.

IP 소스 추적기

Cisco IOS Software Release 12.0(21)S는 Cisco 12000 Series 인터넷 라우터에서 IP Source Tracker 기능을 지원합니다.Cisco IOS Software 릴리스 12.0(22)S는 Cisco 7500 Series 라우터에서 이 기능을 지원합니다.

IP Source Tracker 기능을 사용하면 공격 중인 것으로 의심되는 호스트로 이동하는 트래픽에 대한 정보를 수집할 수 있습니다.또한 이 기능을 사용하면 네트워크의 진입점까지 손쉽게 공격을 추적할 수 있습니다.이 기능을 통해 네트워크 인그레스 포인트를 식별할 경우 ACL 또는 CAR을 사용하여 공격을 효과적으로 차단할 수 있습니다.

자세한 내용은 IP Source Tracker를 참조하십시오.

관련 정보

- Nimda 바이러스로부터 네트워크를 보호하는 방법
- IP 수신 APL
- IP 소스 추적기
- 기술 지원 및 문서 – Cisco Systems