Cisco IOS Classic Firewall/IPS:서비스 거부 보호를 위한 CBAC(Context-Based Access Control) 구성

목차

소개

이 문서에서는 CBAC를 사용하는 Cisco IOS® Classic Firewall에서 DoS(서비스 거부) 매개변수의 조정 절차에 대해 설명합니다.

CBAC는 고급 트래픽 필터링 기능을 제공하며 네트워크 방화벽의 핵심 요소로 사용할 수 있습니다.

DoS는 일반적으로 WAN 링크 대역폭, 방화벽 연결 테이블, 엔드 호스트 메모리, CPU 또는 서비스 기능과 같은 네트워크 리소스를 의도적으로 또는 의도하지 않게 압도하는 네트워크 활동을 말합니다.최악의 경우, DoS 활동은 리소스를 사용할 수 없게 될 때까지 취약한(또는 대상) 리소스를 압도하며, WAN 연결이나 합법적인 사용자에 대한 서비스 액세스를 금지합니다.

Cisco IOS Firewall이 "절반 개방" TCP 연결 수 카운터와 Classic Firewall(**ip inspect**) 및 Zone-Based Policy Firewall에서 방화벽 및 침입 방지 소프트웨어를 통한 총 연결 속도를 유지하는 경우 DoS 활동의 완화에 기여할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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 규칙을 참조하십시오.

배경 정보

절반이 열린 연결은 TCP 피어가 상호 연결의 매개변수를 협상하기 위해 항상 사용하는 3방향 SYN-SYN/ACK-ACK 핸드셰이크를 완료하지 않은 TCP 연결입니다.DoS 또는 DDoS(distributed-denial-of-service) 공격과 같은 악성 활동을 나타내는 절반 개방 연결이 많을 수 있습니다.한 가지 유형의 DoS 공격의 예로는 인터넷에서 여러 호스트를 감염시키고 SYN 공격을 통해 특정 인터넷 서버에 많은 수의 SYN 연결을 서버에 보내는 지충이나 바이러스와 같이 악의적이고 의도적으로 개발한 소프트웨어가 DoS 공격을 수행합니다. 이 경우 인터넷이나 조직의 개인 네트워크 내에서 여러 호스트에 의해 서버에 SYN 연결이 전송됩니다.서버의 연결 테이블은 서버에 새로운 연결을 처리할 수 있는 것보다 더 빨리 도착하는 "가짜" SYN 연결 시도를 통해 로드할 수 있으므로 SYN 공격은 인터넷 서버에 위험을 줍니다.이는 피해자 서버의 TCP 연결 목록에 있는 많은 수의 연결로 인해 피해자 인터넷 서버에 대한 합법적인 사용자 액세스가 차단되기 때문에 DoS 공격의 유형입니다.

또한 Cisco IOS Firewall은 트래픽이 한 방향으로만 있는 UDP(User Datagram Protocol) 세션을 "half-open"으로 간주합니다. 전송 시 UDP를 사용하는 많은 애플리케이션이 데이터 수신을 승인하기 때문입니다.반환 트래픽이 없는 UDP 세션은 DoS 활동을 나타내거나 호스트 중 하나가 응답하지 않는 두 호스트 간의 연결을 시도할 수 있습니다.로그 메시지, SNMP 네트워크 관리 트래픽, 스트리밍 음성 및 비디오 미디어, 시그널링 트래픽 등 많은 유형의 UDP 트래픽은 트래픽을 전달하는 데 한 방향으로만 트래픽을 사용합니다.이러한 트래픽 유형 중 상당수는 단방향 트래픽 패턴이 방화벽 및 IPS DoS 동작에 부정적인 영향을 주지 않도록 애플리케이션별 인텔리전스를 적용합니다.

Cisco IOS Software Release 12.4(11)T 및 12.4(10) 이전에 Cisco IOS Stateful Packet Inspection은 검사 규칙이 적용될 때 DoS 공격으로부터 기본적으로 보호를 제공했습니다.Cisco IOS Software Release 12.4(11)T 및 12.4(10)는 DoS 보호가 자동으로 적용되지 않도록 기본 DoS 설정을 수정했지만 연결 활동 카운터가 여전히 활성 상태입니다.DoS 보호가 활성화된 경우, 즉, 이전 소프트웨어 릴리스에서 기본값이 사용되거나 트래픽에 영향을 미치는 범위로 값이 조정된 경우, DoS 보호는 검사가 적용되는 인터페이스(방화벽이 적용되는 방향으로)에서 검사할 방화벽 정책 컨피그레이션 프로토콜에 대해 활성화됩니다.DoS 보호는 트래픽이 TCP 연결 또는 UDP 세션에 대해 초기 트래픽(SYN 패킷 또는 첫 번째 UDP 패킷)의 동일한 방향으로 적용된 검사가 있는 인터페이스에 들어오거나 나가는 경우에만 네트워크 트래픽에서 활성화됩니다.

Cisco IOS Firewall 검사는 DoS 공격으로부터 보호하기 위해 몇 가지 조정 가능한 값을 제공합니다.12.4(11)T 및 12.4(10) 이전 Cisco IOS Software 릴리스에는 기본 DoS 값이 있으며, 연결 속도가 기본값을 초과하는 네트워크에서 적절한 네트워크 활동 레벨에 대해 구성되지 않은 경우 적절한 네트워크 작동을 방해할 수 있습니다.이러한 매개변수를 사용하면 방화벽 라우터의 DoS 보호가 적용되는 지점을 구성할 수 있습니다.라우터의 DoS 카운터가 기본값 또는 구성된 값을 초과할 경우, 절반 열기 세션 수가 최대 미완료 낮은 값 아래로 떨어질 때까지 라우터는 구성된 최대 미완료 또는 1분 높은 값을 초과하는 모든 새 연결에 대해 이전의 1/2 열기 연결을 재설정합니다.로깅이 활성화된 경우 라우터는 syslog 메시지를 전송하고, 라우터에 IPS(Intrusion Prevention System)가 구성된

경우, 방화벽 라우터는 SDEE(Security Device Event Exchange)를 통해 DoS 서명 메시지를 전송합니다. DoS 매개변수가 네트워크의 정상적인 동작으로 조정되지 않으면 정상적인 네트워크 활동으로 DoS 보호 메커니즘이 트리거되어 애플리케이션 장애, 네트워크 성능 저하, Cisco IOS Firewall 라우터의 높은 CPU 활용률이 발생할 수 있습니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

Cisco IOS Software Classic(IP Inspect) 방화벽 및 침입 방지 시스템에 대한 서비스 거부 튜닝

기존 Cisco IOS 방화벽은 라우터에 대한 전역 DoS 카운터 집합을 유지 관리하며, 모든 인터페이스의 모든 방화벽 정책에 대한 모든 방화벽 세션은 전역 방화벽 카운터 집합에 적용됩니다.

Cisco IOS Classic Firewall Inspection은 Classic Firewall이 적용될 때 기본적으로 DoS 공격으로부터 보호합니다.DoS 보호는 검사가 적용되는 모든 인터페이스에서 방화벽이 적용되는 방향으로 방화벽 정책이 검사하도록 구성된 각 서비스 또는 프로토콜에 대해 활성화됩니다.Classic Firewall은 DoS 공격으로부터 보호할 수 있도록 몇 가지 값을 조정할 수 있습니다.표 1에 나와 있는 레거시 기본 설정(릴리스 12.4(11)T 이전)은 연결 속도가 기본값을 초과하는 네트워크에서 적절한 네트워크 활동 수준에 대해 구성되지 않은 경우 적절한 네트워크 작동을 방해할 수 있습니다.DoS 설정은 exec 명령 **show ip inspect config**로 볼 수 있으며, 이 설정은 sh ip inspect **all**의 출력에 포함됩니다.

CBAC는 시간 초과 및 임계값을 사용하여 세션에 대한 상태 정보를 관리하는 기간을 결정하고 완전히 설정되지 않은 세션을 삭제할 시기를 결정합니다.이러한 시간 제한 및 임계값은 모든 세션에 전체적으로 적용됩니다.

표 1 기존 방화벽 기본 DoS 보호 제한

DoS 보호 가치	12.4(11)T/12.4(10) 이전	12.4(11)T/12.4(10) 이상
최대 불완전한 높은 *값*	500	무제한
최대 불완전한 낮은 *값*	400	무제한
1분 높은 *가치*	500	무제한
1분 낮은 *가치*	400	무제한
tcp max-incomplete 호스트 *값*	50	무제한

Cisco IOS VRF 인식 방화벽을 적용하도록 구성된 라우터는 각 VRF에 대해 하나의 카운터 집합을 유지 관리합니다.

"ip inspect 1분 high" 및 "ip inspect 1분 low"에 대한 카운터는 라우터가 정상적으로 연결되었는지 여부에 관계없이 모든 TCP, UDP 및 ICMP(Internet Control Message Protocol) 연결 시도에 대한 합계를 유지 관리합니다.연결 속도가 증가하면 사설 네트워크의 WORM 감염 또는 서버에 대한 DoS

공격 시도를 나타낼 수 있습니다.

방화벽의 DoS 보호를 "비활성화"할 수는 없지만, 방화벽 라우터의 세션 테이블에 열려 있는 연결 수가 매우 많아야 DoS 보호가 적용되지 않도록 DoS 보호를 조정할 수 있습니다.

DoS 방화벽 보호

방화벽의 DoS 보호를 네트워크 활동에 맞게 조정하려면 다음 절차를 따르십시오.

1. 네트워크가 잘못된 절반 열기 연결 값 또는 시도한 연결 속도로 이어질 수 있는 바이러스나 기생충에 감염되지 않았는지 확인하십시오.네트워크가 "정상"이 아니면 방화벽의 DoS 보호를 제대로 조정할 수 없습니다.일반적인 활동 기간 내에 네트워크의 활동을 관찰해야 합니다.낮은 또는 유휴 상태의 네트워크 활동 기간 내에 네트워크의 DoS 보호 설정을 조정하면 정상 활동 수준이 DoS 보호 설정을 초과할 수 있습니다.
2. max-incomplete high 값을 매우 높은 값으로 설정합니다.

   ```
   ip inspect max-incomplete high 20000000
   ip inspect one-minute high 100000000
   ip inspect tcp max-incomplete host 100000 block-time 0
   ```

   이렇게 하면 네트워크의 연결 패턴을 관찰하는 동안 라우터가 DoS 보호를 제공하지 않습니다.DoS 보호를 사용하지 않도록 설정하려면 지금 이 절차를 중지합니다.**참고:** 라우터가 Cisco IOS Software Release 12.4(11)T 이상 또는 12.4(10) 이상을 실행하는 경우 기본 DoS 보호 값을 올릴 필요가 없습니다.기본적으로 최대 한도로 이미 설정되어 있습니다.**참고:** 호스트에 대한 연결 시작 차단을 포함하는 보다 적극적인 TCP 호스트별 서비스 거부 방지를 활성화하려면 **ip inspect tcp max-incomplete host** 명령에 지정된 블록 시간을 설정해야 합니다.
3. 다음 명령을 사용하여 Cisco IOS 방화벽 통계를 지웁니다.

   ```
   show ip inspect statistics reset
   ```

4. 라우터를 이 상태로 24~48시간 정도 유지하여 일반적인 네트워크 활동 주기의 최소 하루 종일 네트워크 패턴을 관찰할 수 있습니다.**참고:** 값이 매우 높은 수준으로 조정되지만, 네트워크는 Cisco IOS Firewall 또는 IPS DoS 보호 기능의 혜택을 받지 못합니다.
5. 관찰 기간이 지난 후 다음 명령으로 DoS 카운터를 확인합니다.

   ```
   show ip inspect statistics
   ```

   DoS 보호를 튜닝할 매개 변수를 **굵게** 강조 표시합니다.

   ```
   Packet inspection statistics
      [process switch:fast switch]
     tcp packets: [218314:7878692]
     udp packets: [501498:65322]
      packets: [376676:80455]
      packets: [5738:4042411]
     smtp packets: [11:11077]
     ftp packets: [2291:0]
   Interfaces configured for inspection 2
   Session creations since subsystem
      startup or last reset 688030
   Current session counts
      (estab/half-open/terminating) [0:0:0]
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   Last session created 00:00:05
   ```

```
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. **ip inspect max-incomplete high**를 라우터의 표시된 최대 세션 수 절반 개방 값보다 25% 높은 값으로 구성합니다.1.25 승수는 관찰된 동작보다 25% 높은 헤드룸을 제공합니다. 예를 들면 다음과 같습니다.

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

구성:

```
router(config)
   #ip inspect max-incomplete high 70
```

참고: 이 문서에서는 DoS 보호 작업에 대한 제한을 설정하기 위해 네트워크의 일반적인 활동보다 1.25배 배까지 배수를 사용하는 방법에 대해 설명합니다.일반적인 네트워크 활동 최고점 내에서 네트워크를 관찰하는 경우, 일반적인 경우와는 달리 라우터의 DoS 보호가 활성화되지 않도록 적절한 여유 공간을 제공해야 합니다.네트워크에서 정기적으로 이 값을 초과하는 합법적 네트워크 활동이 폭증하는 것을 볼 경우 라우터는 DoS 보호 기능을 활용하므로 일부 네트워크 트래픽에 부정적인 영향을 미칠 수 있습니다.라우터 로그에서 DoS 활동의 탐지를 모니터링하고 **IP inspect max-incomplete high** 및/또는 **ip inspect 1분**의 **high** 제한을 조정하여 정상적인 네트워크 활동 결과로 제한이 발생했음을 확인한 후 DoS가 트리거되지 않도록 해야 합니다.다음과 같은 로그 메시지가 있으면 DoS 보호 애플리케이션을 인식할 수 있습니다.

7. **ip inspect max-incomplete low**를 라우터가 최대 세션 수 절반이 열린 값에 대해 표시하는 값으로 구성합니다. 예를 들면 다음과 같습니다.

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

구성:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. **ip inspect**에 대한 카운터는 라우터 작업**의** 이전 분(연결 성공 여부)에 모든 TCP, UDP 및 ICMP(Internet Control Message Protocol) 연결 시도를 합산하여 1분의 **high** 및 **1분** low를 유지합니다.연결 속도가 증가하면 사설 네트워크에서 WORM 감염 또는 서버에 대한 DoS 공격 시도를 나타낼 수 있습니다.세션 생성 속도에 대한 상위 워터마크를 나타내기 위해 12.4(11)T 및 12.4(10)의 **show ip inspect statistics** 출력에 추가 검사 통계가 추가되었습니다.12.4(11)T 또는 12.4(10) 이전 버전의 Cisco IOS Software Release를 실행하는 경우 검사 통계에 다음 행이 포함되지 않습니다.

```
Maxever session creation rate [value]
```

12.4(11)T 및 12.4(10) 이전의 Cisco IOS Software 릴리스는 검사 최대 1분 연결 속도에 대한 값을 유지하지 않으므로 관찰된 "최대 세션 수" 값을 기준으로 적용해야 합니다.프로덕션에서 Cisco IOS Firewall Release 12.4(11)T의 상태 기반 검사를 사용하는 여러 네트워크를 관찰한 결과, Maxever 세션 생성 비율은 "최대 세션 수"에서 세 값(설정, 반열기, 종료)의 합을 약 10%씩 초과하는 것으로 나타났습니다.ip inspect 1분 낮은 값을 계산하려면 표시된 "established" 값에 1.1을 곱합니다(예:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

구성:

```
ip inspect one-minute low 328
```

라우터가 Cisco IOS Software Release 12.4(11)T 이상 또는 12.4(10) 이상을 실행하는 경우 "Maxever session creation rate" 검사 통계에 표시된 값을 간단히 적용할 수 있습니다.

```
Maxever session creation rate 330
```

구성:

```
ip inspect one-minute low 330
```

9. 1분 **높은 IP 검사를 계산하고 구성합니다**.ip inspect 1분 high 값은 계산된 1분 낮은 값보다 25% 커야 합니다(예:

```
ip inspect one-minute low (330) * 1.25 = 413
```

구성:

```
ip inspect one-minute high 413
```

참고: 이 문서에서는 DoS 보호 작업에 대한 제한을 설정하기 위해 네트워크의 일반적인 활동보다 1.25배 배까지 배수를 사용하는 방법에 대해 설명합니다.일반적인 네트워크 활동 최고점 내에서 네트워크를 관찰하는 경우, 일반적인 경우와는 달리 라우터의 DoS 보호가 활성화되지 않도록 적절한 여유 공간을 제공해야 합니다.네트워크에서 정기적으로 이 값을 초과하는 합법적 네트워크 활동이 폭증하는 것을 볼 경우 라우터는 DoS 보호 기능을 활용하므로 일부 네트워크 트래픽에 부정적인 영향을 미칠 수 있습니다.라우터 로그에서 DoS 활동의 탐지를 모니터링하고 **IP inspect max-incomplete high** 및/또는 **ip inspect 1분**의 **high** 제한을 조정하여 정상적인 네트워크 활동 결과로 제한이 발생했음을 확인한 후 DoS가 트리거되지 않도록 해야 합니다.다음과 같은 로그 메시지가 있으면 DoS 보호 애플리케이션을 인식할 수 있습니다.

10. 서버 기능에 대한 지식에 따라 **ip inspect tcp max-incomplete host**의 값을 정의해야 합니다.이 값은 엔드 호스트 하드웨어 및 소프트웨어 성능에 따라 크게 다르므로 호스트별 DoS 보호 구성에 대한 지침을 제공할 수 없습니다.DoS 보호를 위해 구성할 수 있는 적절한 제한에 대해 잘 모르는 경우 DoS 제한을 정의하는 두 가지 옵션이 있습니다.보다 좋은 옵션은 라우터 기반 호스트별 DoS 보호를 높은 값(최대값 4,294,967,295보다 작거나 같음)으로 구성하고 각 호스트의 운영 체제 또는 Cisco CSA(Security Agent)와 같은 외부 호스트 기반 Intrusion Protection System에서 제공하는 호스트 관련 보호를 적용하는 것입니다.네트워크 호스트의 활동 및 성능 로그를 검사하고 지속 가능한 최대 연결 속도를 확인합니다.Classic Firewall은 하나의 전역 카운터만 제공하므로 모든 네트워크 호스트를 확인한 후 결정하는 최대 값을 최대 연결 속도에 적용해야 합니다.OS별 활동 제한 및 CSA와 같은 호스트 기반 IPS를 사용하는 것이 좋습니다.**참고:** Cisco IOS Firewall은 특정 운영 체제 및 애플리케이션 취약성에 대한 지정 공격으로부터 제한된 보호를 제공합니다.Cisco IOS Firewall의 DoS 보호는 적대적일 가능성이 있는 환경에 노출된 엔드 호스트 서비스에 대한 보안 침해 방지를 보장하지 않습니다.
11. 네트워크에서 DoS 보호 활동을 모니터링합니다.DoS 공격 탐지를 기록하려면 syslog 서버 또는 Cisco MARS(Monitoring and Reporting Station)를 사용하는 것이 좋습니다.탐지가 자주 발생하는 경우 DoS 보호 매개변수를 모니터링하고 조정해야 합니다.TCP SYN DoS 공격에 대한 자세한 내용은 TCP SYN Denial of Service Attacks를 방지하기 위한 전략 정의를 참조하십시오.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems