ASA 위협 탐지 기능 및 컨피그레이션 확인

목차

소개

이 문서에서는 위협 탐지 기능 및 컨피그레이션의 세 가지 주요 구성 요소에 대해 설명합니다.

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 Cisco ASA(Adaptive Security Appliance)의 위협 탐지 기능에 대한 기능 및 기본 컨피그레이션에 대해 설명합니다. 위협 탐지는 방화벽 관리자가 내부 네트워크 인프라에 도달하기 전에 공격을 식별, 이해, 차단하는 데 필요한 툴을 제공합니다. 이를 위해 이 기능은 여러 가지 다양한 트리거 및 통계에 의존하며, 이 내용은 이 섹션에서 자세히 설명합니다.

위협 감지는 8.0(2) 이상의 소프트웨어 버전을 실행하는 모든 ASA 방화벽에서 사용할 수 있습니다. 위협 감지가 전용 IDS/IPS 솔루션을 대체하는 것은 아니지만 ASA의 핵심 기능에 대한 추가 보호 레이어를 제공하기 위해 IPS를 사용할 수 없는 환경에서 사용할 수 있습니다.

위협 탐지 기능

위협 탐지 기능에는 세 가지 주요 구성 요소가 있습니다.

1. 기본 위협 탐지
2. 지능형 위협 탐지
3. 스캐닝 위협 감지

이러한 각 구성 요소에 대해서는 다음 섹션에서 자세히 설명합니다.

기본 위협 감지(시스템 레벨 속도)

기본 위협 감지는 8.0(2) 이상을 실행하는 모든 ASA에서 기본적으로 활성화됩니다.

기본 위협 감지는 ASA에서 전체적으로 다양한 이유로 패킷이 삭제되는 속도를 모니터링합니다. 즉, 기본 위협 탐지에 의해 생성된 통계는 전체 어플라이언스에만 적용되며, 일반적으로 위협의 소스 또는 특정 특성에 대한 정보를 제공할 만큼 세분화되지 않습니다. 대신 ASA는 다음 이벤트에 대해 삭제된 패킷을 모니터링합니다.

- ACL 삭제(acl-drop) - 액세스 목록에서 패킷을 거부합니다.
- Bad Pkts(bad-packet-drop) - RFC 표준을 준수하지 않는 L3 및 L4 헤더를 포함하는 잘못된 패킷 형식입니다.
- Conn Limit(conn-limit-drop) - 구성된 또는 전역 연결 제한을 초과하는 패킷입니다.
- DoS 공격(dos-drop) - DoS(Denial of Service) 공격.
- 방화벽(fw-drop) - 기본 방화벽 보안 검사.
- ICMP 공격(icmp-drop) - 의심스러운 ICMP 패킷입니다.
- Inspect(inspect-drop) - 애플리케이션 검사에 의한 거부.
- Interface (interface-drop) - 인터페이스 확인에 의해 삭제된 패킷입니다.
- 스캐닝(스캐닝 위협) - 네트워크/호스트 스캐닝 공격.
- SYN 공격(syn-attack) - TCP SYN 공격 및 반환 데이터가 없는 단방향 UDP 세션을 포함하는

불완전한 세션 공격입니다.

각 이벤트에는 위협을 식별하는 데 사용되는 특정 트리거 집합이 있습니다. 대부분의 트리거는 특정 ASP 삭제 사유와 연결되지만 특정 syslog 및 검사 작업도 고려됩니다. 일부 트리거는 여러 위협 카테고리에서 모니터링됩니다. 전체 목록은 아니지만 가장 일반적인 몇 가지 트리거는 이 표에 요약되어 있습니다.

기본 위협	트리거/ASP 삭제 이유
acl-drop	acl-drop
불량 패킷 삭제	invalid-tcp-hdr-length 올바르지 않은 ip 헤더 inspect dns-pak-too-long inspect-dns-id가 일치하지 않음
conn-limit-drop	연결 제한
도스 드롭	sp 보안 실패
점적	inspect-icmp-seq-num-not-matched inspect dns-pak-too-long inspect-dns-id가 일치하지 않음 sp 보안 실패 acl-drop
icmp-drop	inspect-icmp-seq-num-not-matched
inspect-drop	검사 엔진에 의해 트리거된 프레임 삭제
인터페이스 삭제	sp 보안 실패 경로 없음
스캐닝 위협	tcp-3whs 실패 tcp-not-syn sp 보안 실패 acl-drop

	inspect-icmp-seq-num-not-matched inspect dns-pak-too-long inspect-dns-id가 일치하지 않음
syn 공격	%ASA-6-302014 syslog - "SYN 시간 초과" 해제 이유

각 이벤트에 대해 기본 위협 감지는 구성된 기간 동안 이러한 감소가 발생하는 속도를 측정합니다. 이 기간을 ARI(평균 속도 간격)라고 하며 범위는 600초에서 30일입니다. ARI 내에서 발생한 이벤트 수가 구성된 속도 임계값을 초과하면 ASA는 이러한 이벤트를 위협으로 간주합니다.

기본 위협 탐지에는 이벤트를 위협으로 간주하는 경우에 대해 구성 가능한 두 개의 임계값(평균 속도 및 버스트 속도)이 있습니다. 평균 속도는 단순히 구성된 ARI의 시간 기간 내의 초당 평균 드랍 횟수이다. 예를 들어 ACL 삭제의 평균 속도 임계값이 ARI가 600초인 400으로 구성된 경우 ASA는 지난 600초 동안 ACL에서 삭제된 평균 패킷 수를 계산합니다. 이 수가 초당 400보다 큰 것으로 확인되면 ASA에서 위협을 로깅합니다.

마찬가지로, 버스트 속도는 매우 비슷하지만 BRI(burst rate interval)라고 하는 스냅샷 데이터의 소규모 기간을 살펴봅니다. BRI는 항상 ARI보다 작습니다. 예를 들어, 이전 예에서 빌드할 때 ACL 드롭에 대한 ARI는 여전히 600초이며 이제 버스트 속도가 800입니다. 이 값을 사용하여 ASA는 ACL에 의해 삭제된 평균 패킷 수를 20초 만에 계산합니다. 여기서 20초는 BRI입니다. 이 계산된 값이 초당 800개 삭제를 초과하면 위협이 기록됩니다. 어떤 BRI가 사용되는지 확인하기 위해 ASA는 ARI의 1/30 값을 계산합니다. 따라서 이전에 사용한 예에서 600초 중 1/30은 20초입니다. 그러나 위협 탐지는 최소 BRI가 10초이므로 ARI의 1/30이 10 미만이면 ASA는 여전히 10초를 BRI로 사용합니다. 또한 이러한 동작은 8.2(1) 이전 버전에서 달랐는데, 이는 ARI의 1/30이 아닌 1/60의 값을 사용했습니다. 10초의 최소 BRI는 모든 소프트웨어 버전에서 동일합니다.

기본 위협이 탐지되면 ASA는 syslog %ASA-4-733100을 생성하여 관리자에게 잠재적인 위협이 식별되었음을 알립니다. 각 위협 범주에 대한 평균, 현재 및 총 이벤트 수는 show threat-detection rate 명령을 사용하여 확인할 수 있습니다. 총 누적 이벤트 수는 최근 30개의 BRI 샘플에서 확인된 이벤트 수의 합계입니다.

syslog의 버스트 속도는 현재 BRI에서 현재까지 삭제된 패킷 수를 기반으로 계산됩니다. 계산은 BRI에서 주기적으로 수행됩니다. 보안 침해가 발생하면 syslog가 생성됩니다. BRI에서 하나의 syslog만 생성되도록 제한됩니다. "show threat-detection rate"의 버스트 속도는 마지막 BRI에서 삭제된 패킷 수를 기반으로 계산됩니다. 차이점은 syslog는 시간에 민감하기 때문에 현재 BRI에서 보안 침해가 발생하면 캡처 기회가 있다는 것입니다. "show threat-detection rate"는 시간에 덜 민감하므로 마지막 BRI의 숫자가 사용됩니다.

기본 위협 탐지는 일탈 트래픽을 중지하거나 향후 공격을 방지하기 위해 어떤 조치도 취하지 않습니다. 이러한 의미에서 기본 위협 감지는 순수하게 정보적인 기능이며 모니터링 또는 보고 메커니즘으로 사용될 수 있습니다.

고급 위협 감지(객체 레벨 통계 및 상위 N)

기본 위협 탐지와는 달리, 고급 위협 탐지는 더 세분화된 객체에 대한 통계를 추적하는 데 사용될 수 있습니다. ASA는 호스트 IP, 포트, 프로토콜, ACL 및 TCP 가로채기로 보호되는 서버에 대한 추적 통계를 지원합니다. Advanced Threat Detection은 ACL 통계에 대해서만 기본적으로 활성화됩니다.

호스트, 포트 및 프로토콜 객체의 경우 Threat Detection은 특정 기간 내에 해당 객체가 보내고 받은 패킷, 바이트 및 삭제 수를 추적합니다. ACL의 경우 위협 감지는 특정 기간 내에 가장 많이 발생한 상위 10개 ACE(허용 및 거부 모두)를 추적합니다.

이러한 모든 사례에서 추적되는 기간은 20분, 1시간, 8시간, 24시간이다. 기간 자체는 구성할 수 없지만 객체별로 추적되는 기간 수는 'number-of-rate' 키워드로 조정할 수 있습니다. 자세한 내용은 컨피그레이션 섹션을 참조하십시오. 예를 들어, 'number-of-rate'가 2로 설정된 경우 20분, 1시간 및 8시간 동안의 모든 통계가 표시됩니다. 'number-of-rate'가 1로 설정된 경우 20분, 1시간 동안의 모든 통계가 표시됩니다. 20분짜리가 항상 표시됩니다.

TCP 가로채기가 활성화된 경우 위협 탐지는 공격받고 TCP 가로채기에 의해 보호되는 것으로 간주되는 상위 10개 서버를 추적할 수 있습니다. TCP 가로채기에 대한 통계는 사용자가 특정 평균(ARI) 및 버스트(BRI) 비율과 함께 측정된 속도 간격을 구성할 수 있다는 점에서 기본 위협 탐지와 유사합니다. TCP 가로채기에 대한 고급 위협 감지 통계는 ASA 8.0(4) 이상에서만 사용할 수 있습니다.

Advanced Threat Detection 통계는 show threat-detection statistics 및 show threat-detection statistics top 명령을 통해 표시됩니다. 이는 ASDM의 방화벽 대시보드에서 "상위" 그래프의 모집단을 담당하는 기능이기도 합니다. Advanced Threat Detection에서 생성되는 syslog는 %ASA-4-733104 및 %ASA-4-733105뿐입니다. 이 syslog는 TCP 가로채기 통계에서 평균 및 버스트 속도를 각각 초과할 때 트리거됩니다.

기본 위협 감지와 마찬가지로, 고급 위협 감지도 정보 제공에 불과합니다. Advanced Threat Detection 통계를 기반으로 트래픽을 차단하는 작업은 수행되지 않습니다.

스캐닝 위협 감지

스캐닝 위협 감지는 서브넷에 있는 너무 많은 호스트 또는 호스트/서브넷에 있는 많은 포트에 연결하는 의심되는 공격자를 추적하기 위해 사용됩니다. Scanning Threat Detection은 기본적으로 비활성화되어 있습니다.

Scanning Threat Detection은 스캐닝 공격에 대한 위협 카테고리를 이미 정의한 Basic Threat Detection의 개념을 기반으로 합니다. 따라서 속도 간격, 평균 속도(ARI) 및 버스트 속도(BRI) 설정은 Basic(기본) 및 Scanning Threat Detection(스캐닝 위협 탐지) 간에 공유됩니다. 두 기능의 차이점은 Basic Threat Detection은 평균 또는 버스트 속도 임계값이 초과되었음을 나타내지만, Scanning Threat Detection은 스캔에 관련된 호스트에 더 많은 컨텍스트를 제공하는 데 도움이 될 수 있는 공격자 및 대상 IP 주소의 데이터베이스를 유지 관리한다는 점입니다. 또한 대상 호스트/서브넷에서 실제로 수신한 트래픽만 Scanning Threat Detection에서 고려됩니다. 기본 위협 감지는 트래픽이 ACL에 의해 삭제되더라도 스캐닝 위협을 트리거할 수 있습니다.

스캐닝 위협 감지는 선택적으로 공격자 IP를 차단하여 공격에 대응할 수 있습니다. 따라서 Scanning Threat Detection은 ASA를 통한 연결에 능동적으로 영향을 줄 수 있는 유일한 위협 탐지 기능의 하위 집합입니다.

스캐닝 위협 감지가 공격을 탐지하면 공격자 및/또는 대상 IP에 대해 %ASA-4-733101이 기록됩니

다. 공격자를 차단하도록 이 기능이 구성된 경우 검사 위협 탐지에서 차단733102 생성할 때 %ASA-4-Server가 기록됩니다. shun을 제거하면 %ASA-4-733103이 기록됩니다. show threat-detection scanning-threat 명령을 사용하여 전체 스캐닝 위협 데이터베이스를 볼 수 있습니다.

제한 사항

- 위협 탐지는 ASA 8.0(2) 이상에서만 사용할 수 있습니다. ASA 1000V 플랫폼에서는 지원되지 않습니다.
- 위협 감지는 단일 컨텍스트 모드에서만 지원됩니다.
- Through-the-box 위협만 탐지됩니다. ASA 자체에 전송된 트래픽은 위협 탐지에서 고려되지 않습니다.
- 대상 서버에서 재설정한 TCP 연결 시도는 SYN 공격 또는 스캐닝 위협으로 계산되지 않습니다.

설정

기본 위협 탐지

Basic Threat Detection은 threat-detection basic-threat 명령으로 활성화됩니다.

```
<#root>

ciscoasa(config)#

threat-detection basic-threat
```

기본 속도는 show run all threat-detection 명령으로 볼 수 있습니다.

```
<#root>

ciscoasa(config)#

show run all threat-detection


threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
```

```
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

사용자 지정 값으로 이러한 속도를 조정하려면 적절한 위협 범주에 대해 threat-detection rate 명령을 재구성하면 됩니다.

<#root>

```
ciscoasa(config)#
```

threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550

각 위협 범주에는 최대 3개의 서로 다른 속도가 정의될 수 있습니다(속도 ID가 속도 1, 속도 2, 속도 3임). 초과된 특정 속도 ID는 %ASA-4-733100 syslog에서 참조됩니다.

이전 예에서 위협 탐지는 ACL 삭제 수가 1200초 동안 250개/초 또는 40초 동안 550개/초 삭제 수를 초과하는 경우에만 syslog 733100을 생성합니다.

지능형 위협 탐지

Advanced Threat Detection을 활성화하려면 threat-detection statistics 명령을 사용합니다. 특정 기능 키워드가 제공되지 않으면 이 명령은 모든 통계에 대한 추적을 활성화합니다.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics ?

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host             Keyword to specify IP statistics
 port             Keyword to specify port statistics
 protocol        Keyword to specify protocol statistics
 tcp-intercept    Trace tcp intercept statistics
 <cr>
```

호스트, 포트, 프로토콜 또는 ACL 통계에 대해 추적되는 속도 간격 수를 구성하려면 number-of-rate 키워드를 사용합니다.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics host number-of-rate 2
```

number-of-rate 키워드는 가장 짧은 n개 간격만 추적하도록 Threat Detection을 구성합니다.

TCP 가로채기 통계를 활성화하려면 threat-detection statistics tcp-intercept 명령을 사용합니다.

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept
```

TCP 가로채기 통계에 대한 사용자 지정 속도를 구성하려면 rate-interval, average-rate 및 burst-rate 키워드를 사용합니다.

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

스캐닝 위협 감지

Scanning Threat Detection을 활성화하려면 threat-detection scanning-threat 명령을 사용합니다.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat
```

스캐닝 위협에 대한 속도를 조정하려면 Basic Threat Detection에서 사용하는 동일한 threat-detection rate 명령을 사용합니다.

```
<#root>
ciscoasa(config)#
threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

ASA가 스캐닝 공격자 IP를 차단할 수 있도록 하려면 shun 키워드를 threat-detection scanning-threat 명령에 추가합니다.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

그러면 Scanning Threat Detection에서 공격자에 대해 1시간 동안 차단 기능을 생성할 수 있습니다. 차단 기간을 조정하려면 threat-detection scanning-threat shun duration 명령을 사용합니다.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000
```

경우에 따라 ASA에서 특정 IP를 차단하지 못하도록 할 수 있습니다. 이를 위해 threat-detection scanning-threat shun except 명령으로 예외를 생성합니다.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255

ciscoasa(config)#

threat-detection scanning-threat shun except object-group no-shun
```

Performance

Basic Threat Detection은 ASA에 대한 성능에 거의 영향을 미치지 않습니다. 고급 및 스캐닝 위협 감지는 메모리의 다양한 통계를 추적해야 하므로 훨씬 더 리소스가 많이 사용됩니다. shun 기능이 활성화된 Scanning Threat Detection만 허용되었을 트래픽에 능동적으로 영향을 미칠 수 있습니다.

ASA 소프트웨어 버전이 발전함에 따라 위협 탐지의 메모리 사용률이 크게 최적화되었습니다. 그러나 Threat Detection이 활성화되기 전후에 ASA의 메모리 사용률을 모니터링하려면 주의를 기울여야 합니다. 경우에 따라 특정 문제를 적극적으로 해결하는 동안 특정 통계(예: 호스트 통계)만 일시적으로 활성화하는 것이 좋습니다.

Threat Detection 메모리 사용량에 대한 자세한 내용을 보려면 show memory app-cache threat-detection [detail] 명령을 실행합니다.

권장 작업

이 섹션에서는 다양한 위협 탐지 관련 이벤트가 발생할 때 수행할 수 있는 작업에 대한 몇 가지 일반

적인 권장 사항을 제공합니다.

기본 삭제 속도가 초과되고 %ASA-4-733100이 생성된 경우

%ASA-4-733100 syslog에 언급된 특정 위협 범주를 확인하고 이 범주를 의 출력과 연관시킵니다 show threat-detection rate . 이 정보를 사용하여 show asp drop 트래픽을 삭제하는 이유를 확인할 수 있습니다

특정 이유로 인해 삭제된 트래픽에 대한 자세한 내용을 보려면 해당 사유와 함께 ASP 삭제 캡처를 사용하여 삭제된 모든 패킷을 확인합니다. 예를 들어, ACL 삭제 위협이 로깅된 경우 ASP 삭제 이유 acl-drop：

<#root>

ciscoasa#

capture drop type asp-drop acl-drop

ciscoasa#

show capture drop

1 packet captured

```
   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

이 캡처는 삭제된 패킷이 10.10.10.10부터 192.168.1.100까지의 UDP/53 패킷임을 보여줍니다.

%ASA-4-733100에서 검사 위협을 보고할 경우 검사 위협 탐지를 일시적으로 활성화하는 것도 도움이 될 수 있습니다. 따라서 ASA는 공격과 관련된 소스 및 대상 IP를 추적할 수 있습니다.

Basic Threat Detection은 ASP에서 이미 삭제된 트래픽을 대부분 모니터링하므로 잠재적인 위협을 중지하기 위한 직접적인 조치는 필요하지 않습니다. ASA를 통과하는 트래픽과 관련된 SYN 공격 및 스캐닝 위협은 예외입니다.

ASP 삭제 캡처에 표시된 삭제가 네트워크 환경에 적합하거나 필요한 경우 기본 속도 간격을 보다 적절한 값으로 조정합니다.

삭제에 불법적인 트래픽이 표시되면 트래픽이 ASA에 도달하기 전에 트래픽을 차단하거나 속도를 제한하는 조치를 취해야 합니다. 여기에는 업스트림 디바이스의 ACL 및 QoS가 포함될 수 있습니다 .

SYN 공격의 경우 ASA의 ACL에서 트래픽을 차단할 수 있습니다. TCP 가로채기는 대상 서버를 보호하도록 구성할 수도 있지만, 이는 Conn Limit 위협이 대신 로깅되는 결과를 초래할 수 있습니다.

위협을 검사하는 경우 ASA의 ACL에서 트래픽도 차단할 수 있습니다. 를 사용하여 위협 감지 검사 shunASA가 정의된 기간 동안 공격자의 모든 패킷을 사전 대응적으로 차단하도록 하려면 이 옵션을

활성화할 수 있습니다.

스캐닝 위협이 탐지되고 %ASA-4-733101이 로깅된 경우

%ASA-4-733101은 대상 호스트/서브넷 또는 공격자 IP 주소를 나열해야 합니다. 대상 및 공격자의 전체 목록을 보려면 show threat-detection scanning-threat.

공격자 및/또는 대상과 마주하는 ASA 인터페이스의 패킷 캡처는 공격의 본질을 명확하게 하는 데에도 도움이 될 수 있습니다.

탐지된 스캔이 예상하지 못한 경우 트래픽이 ASA에 도달하기 전에 트래픽을 차단하거나 속도를 제한하는 조치를 취해야 합니다. 여기에는 업스트림 디바이스의 ACL 및 QoS가 포함될 수 있습니다. 이 shun이 옵션은 Scanning Threat Detection(스캐닝 위협 탐지) 컨피그레이션에 추가되며, ASA가 지정된 기간 동안 공격자 IP의 모든 패킷을 사전 대응적으로 삭제할 수 있도록 합니다. 마지막으로, ACL 또는 TCP 가로채기 정책을 통해 ASA에서 트래픽을 수동으로 차단할 수도 있습니다.

탐지된 스캔이 오탐인 경우 Scanning Threat 속도 간격을 네트워크 환경에 더 적합한 값으로 조정합니다.

공격자가 차단되고 %ASA-4-733102이 로깅되는 경우

%ASA-4-733102은 차단된 공격자의 IP 주소를 나열합니다. 이 show threat-detection shun 명령을 사용하여 위협 탐지에서 차단한 공격자의 전체 목록을 확인할 수 있습니다. 이 show shun 명령을 사용하여 ASA에서 능동적으로 차단되는 모든 IP의 전체 목록을 확인합니다(위협 탐지가 아닌 소스로부터의 것도 포함).

shun이 합법적인 공격의 일부인 경우 추가 작업이 필요하지 않습니다. 그러나 가능한 한 업스트림에서 소스로 향하는 공격자의 트래픽을 수동으로 차단하는 것이 좋습니다. 이는 ACL 및 QoS를 통해 수행할 수 있습니다. 이렇게 하면 중간 디바이스에서 불법적인 트래픽에 리소스를 낭비할 필요가 없습니다.

shun을 트리거한 스캐닝 위협이 오탐인 경우 clear threat-detection shun [IP_address] 명령을 실행합니다.

%ASA-4-733104 및/또는 %ASA-4-733105이 기록되는 경우

%ASA-4-733104 및 %ASA-4-733105은 현재 TCP 가로채기로 보호되고 있는 공격의 대상 호스트를 나열합니다. 공격 속도 및 보호된 서버에 대한 자세한 내용은 show threat-detection statistics top tcp-intercept .

<#root>

```
ciscoasa#
```

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
```

```
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Advanced Threat Detection에서 이러한 종류의 공격을 탐지하면 ASA는 이미 TCP 가로채기를 통해 대상 서버를 보호합니다. 구성된 연결 제한을 확인하여 공격의 특성 및 속도에 대해 적절한 보호를 제공하는지 확인합니다. 또한, 가능한 한 소스를 향해 멀리 업스트림에서 공격자의 트래픽을 수동으로 차단하는 것이 좋습니다. 이는 ACL 및 QoS를 통해 수행할 수 있습니다. 이렇게 하면 중간 디바이스에서 불법적인 트래픽에 리소스를 낭비할 필요가 없습니다.

탐지된 공격이 오탐인 경우 를 사용하여 TCP 가로채기 공격의 속도를 보다 적절한 값으로 조정합니다. threat-detection statistics tcp-intercept명령을 실행합니다.

수동으로 위협을 트리거하는 방법

테스트와 문제 해결을 위해 다양한 위협을 수동으로 트리거하는 것이 도움이 될 수 있습니다. 이 섹션에서는 몇 가지 일반적인 위협 유형을 트리거하는 방법에 대한 팁을 제공합니다.

기본 위협 - ACL 삭제, 방화벽 및 스캐닝

특정 기본 위협을 트리거하려면 이전 기능 섹션의 표를 참조하십시오. 특정 ASP 삭제 이유를 선택하고 ASA를 통해 적절한 ASP 삭제 이유에 의해 삭제될 트래픽을 전송합니다.

예를 들어, ACL 삭제, 방화벽 및 스캐닝 위협은 모두 acl-drop에 의해 삭제된 패킷의 비율을 고려합니다. 이러한 위협을 동시에 트리거하려면 다음 단계를 완료하십시오.

1. ASA 내부의 대상 서버(10.11.11.11)로 전송된 모든 TCP 패킷을 명시적으로 삭제하는 ASA의 외부 인터페이스에 ACL을 생성합니다.

   ```
   access-list outside_in extended line 1 deny tcp any host 10.11.11.11
   access-list outside_in extended permit ip any any
   access-group outside_in in interface outside
   ```

2. ASA 외부의 공격자(10.10.10.10)로부터 nmap을 사용하여 대상 서버의 모든 포트에 대해 TCP SYN 스캔을 실행합니다.

   ```
   nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
   ```

> 참고: T5는 가능한 한 빨리 스캔을 실행하도록 nmap을 구성합니다. 공격자 PC의 리소스에 따라, 이것은 여전히 일부 기본 속도를 트리거하기에 충분히 빠르지 않다. 이 경우, 보고자 하는 위협에 대해 구성된 속도를 낮추기만 하면 됩니다. ARI 및 BRI를 0으로 설정하면 Basic Threat Detection이 속도에 관계없이 항상 위협을 트리거합니다.

3. 기본 위협은 ACL 삭제, 방화벽 및 스캐닝 위협에 대해 탐지됩니다.

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

참고: 이 예에서는 ACL 삭제 및 방화벽 ARI와 BRI가 0으로 설정되었으므로 항상 위협을 트리거합니다. 따라서 구성된 최대 속도가 0으로 표시됩니다.

고급 위협 - TCP 가로채기

1. ASA(10.11.11.11) 내부의 대상 서버로 전송되는 모든 TCP 패킷을 허용하는 외부 인터페이스에 ACL을 생성합니다.

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. 대상 서버가 실제로 존재하지 않거나 공격자의 연결 시도를 재설정하는 경우, ASA에서 위조 ARP 항목을 구성하여 내부 인터페이스 외부로 공격 트래픽을 블랙홀(blackhole)합니다.

```
arp inside 10.11.11.11 dead.dead.dead
```

3. ASA에서 간단한 TCP 가로채기 정책을 생성합니다.

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

ASA 외부의 공격자(10.10.10.10)로부터 nmap을 사용하여 대상 서버의 모든 포트에 대해 TCP SYN 스캔을 실행합니다.

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Threat Detection은 보호된 서버를 추적합니다.

<#root>

ciscoasa(config)#

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

------------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

스캔 위협

1. ASA(10.11.11.11) 내부의 대상 서버로 전송되는 모든 TCP 패킷을 허용하는 외부 인터페이스에 ACL을 생성합니다.

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

> 참고: Scanning Threat Detection에서 대상 및 공격자 IP를 추적하려면 ASA를 통해 트래픽이 허용되어야 합니다.

2. 대상 서버가 실제로 존재하지 않거나 공격자의 연결 시도를 재설정하는 경우, ASA에서 위조 ARP 항목을 구성하여 내부 인터페이스 외부로 공격 트래픽을 블랙홀(blackhole)합니다.

```
arp inside 10.11.11.11 dead.dead.dead
```

> 참고: 대상 서버에서 재설정된 연결은 위협의 일부로 계산되지 않습니다.

3. ASA 외부의 공격자(10.10.10.10)로부터 nmap을 사용하여 대상 서버의 모든 포트에 대해 TCP SYN 스캔을 실행합니다.

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> 참고: T5는 가능한 한 빨리 스캔을 실행하도록 nmap을 구성합니다. 공격자 PC의 리소스에 따라, 이것은 여전히 일부 기본 속도를 트리거하기에 충분히 빠르지 않다. 이 경우, 보고자 하는 위협에 대해 구성된 속도를 낮추기만 하면 됩니다. ARI 및 BRI를 0으로 설정하면 Basic Threat Detection이 속도에 관계없이 항상 위협을 트리거합니다.

4. 스캐닝 위협이 탐지되고, 공격자의 IP가 추적되며, 공격자는 차단됩니다.

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
```

```
max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

관련 정보

- ASA 컨피그레이션 가이드
- ASA 명령 참조
- Cisco Secure Firewall ASA Series Syslog 메시지
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.