ASA/PIX/IOS 라우터 컨피그레이션을 위한 IPS 차단/차단 예

목차

소개

이 문서에서는 Cisco IPS의 도움을 받아 PIX/ASA/Cisco IOS 라우터에서 연결을 구성하는 방법에 대해 설명합니다.센서의 차단 애플리케이션인 ARC는 라우터, Cisco 5000 RSM 및 Catalyst 6500 Series 스위치, PIX Firewalls, FWSM 및 ASA에서 블록을 시작하고 중지합니다.ARC는 악성 IP 주소에 대해 관리되는 디바이스에 대해 차단 또는 차단 조치를 실행합니다.ARC는 센서가 관리하는 모든 장치에 동일한 블록을 전송합니다.기본 차단 센서가 구성된 경우 이 디바이스로 차단 기능이 전달되고 이 디바이스에서 실행됩니다.ARC는 블록 시간을 모니터링하고 시간이 만료된 후 블록을 제거합니다.

IPS 5.1을 사용하는 경우 차단 요청과 함께 VLAN 정보가 전송되지 않으므로 다중 컨텍스트 모드에서 방화벽에 연결할 때 특별한 주의가 필요합니다.

> **참고:**다중 컨텍스트 FWSM의 관리 컨텍스트에서는 차단이 지원되지 않습니다.

다음 세 가지 유형의 블록이 있습니다.

- Host block(호스트 차단) - 지정된 IP 주소에서 오는 모든 트래픽을 차단합니다.
- Connection block(연결 차단) - 지정된 소스 IP 주소에서 지정된 목적지 IP 주소 및 목적지 포트로의 트래픽을 차단합니다.동일한 소스 IP 주소에서 다른 목적지 IP 주소 또는 목적지 포트로 연결되는 여러 연결 블록은 연결 블록에서 호스트 블록으로 자동으로 전환합니다.**참고:**보안 어플라이언스에서는 연결 블록을 지원하지 않습니다.보안 어플라이언스는 선택적인 포트 및 프로토콜 정보와 함께 호스트 블록만 지원합니다.
- Network block(네트워크 차단) - 지정된 네트워크의 모든 트래픽을 차단합니다.서명이 트리거될 때 수동으로 또는 자동으로 호스트 및 연결 블록을 시작할 수 있습니다.네트워크 블록만 수동으로 시작할 수 있습니다.

자동 블록의 경우 특정 서명에 대한 이벤트 작업으로 Request Block Host 또는 Request Block Connection을 선택해야 서명이 트리거될 때 SensorApp이 ARC로 블록 요청을 보냅니다.ARC가 SensorApp에서 차단 요청을 받으면 디바이스 컨피그레이션을 업데이트하여 호스트나 연결을 차단합니다.서명에 Request Block Host 또는 Request Block Connection 이벤트 작업을 추가하는 절차에 대한 자세한 내용은 5-22 페이지에 Assignature를 참조하십시오.특정 위험 등급의 경보에 Request Block Host 또는 Request Block Connection 이벤트 작업을 추가하는 재정의 구성 절차에 대한 자세한 내용은 7-15페이지의 Configuring Event Action Overrides를 참조하십시오.

Cisco 라우터 및 Catalyst 6500 시리즈 스위치에서 ARC는 ACL 또는 VACL을 적용하여 블록을 생성합니다.ACL과 VACL은 트래픽을 허용하거나 거부하기 위해 각각 방향을 포함하는 인터페이스에 필터를 적용합니다..PIX 방화벽, FWSM 및 ASA는 ACL 또는 VACL을 사용하지 않습니다.내장형 shun **및 no shun** 명령이 사용됩니다.

이 정보는 ARC를 구성하는 데 필요합니다.

- 디바이스가 AAA로 구성된 경우 로그인 사용자 ID
- 로그인 암호
- 비밀번호 활성화 - 사용자에게 enable 권한이 있는 경우 필요하지 않습니다.
- 관리할 인터페이스(예: ethernet0, vlan100)
- 생성된 ACL 또는 VACL의 시작(Pre-Block ACL 또는 VACL) 또는 끝(Post-Block ACL 또는 VACL)에 적용할 기존 ACL 또는 VACL 정보이는 PIX 방화벽, FWSM 또는 ASA에는 적용되지 않습니다. ACL 또는 VACL을 사용하여 차단하지 않기 때문입니다.
- 텔넷 또는 SSH를 사용하여 디바이스와 통신하는지 여부
- 차단하지 않을 IP 주소(호스트 또는 호스트 범위)
- 블록을 얼마 동안 유지하시겠습니까

사전 요구 사항

요구 사항

차단 또는 속도 제한을 위해 ARC를 구성하기 전에 다음 작업을 완료해야 합니다.

- 네트워크 토폴로지를 분석하여 어떤 센서가 차단해야 하는지, 어떤 주소를 차단해서는 안 되는지 파악합니다.
- 각 디바이스에 로그인하는 데 필요한 사용자 이름, 디바이스 비밀번호, 비밀번호 활성화 및 연결 유형(텔넷 또는 SSH)을 수집합니다.
- 디바이스의 인터페이스 이름을 확인합니다.
- 필요한 경우 Pre-Block ACL 또는 VACL의 이름과 Post-Block ACL 또는 VACL을 확인합니다.
- 어떤 인터페이스를 차단해야 하는지, 차단해서는 안 되는지, 어떤 방향(수신 또는 발신)을 파악합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Intrusion Prevention System 5.1 이상을 기반으로 합니다.

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.

참고:기본적으로 ARC는 250개의 블록 엔트리로 제한됩니다.ARC에서 지원하는 차단 장치 목록에 대한 자세한 내용은 지원되는 장치를 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

차단 및 속도 제한을 활성화하는 데 필요한 기본 설정을 구성하려면 차단 페이지를 사용합니다.

ARC는 관리되는 디바이스에 대한 차단 및 속도 제한 작업을 제어합니다.

차단해서는 안 되는 호스트 및 네트워크를 식별하려면 센서를 조정해야 합니다.신뢰할 수 있는 디바이스의 트래픽에서 서명을 실행할 수 있습니다.이 서명이 공격자를 차단하도록 구성된 경우 합법적인 네트워크 트래픽에 영향을 줄 수 있습니다.이 시나리오를 방지하기 위해 디바이스의 IP 주소를 차단 안 함 목록에 나열할 수 있습니다.

차단 안 함 항목에 지정된 넷마스크는 차단 안 함 주소에 적용됩니다.넷마스크를 지정하지 않으면 기본 /32 마스크가 적용됩니다.

참고:센서는 센서와 차단 디바이스 간의 통신을 방해하므로 기본적으로 자체 IP 주소에 대한 블록을 발급할 수 없습니다.그러나 이 옵션은 사용자가 구성할 수 있습니다.

ARC가 차단 장치를 관리하도록 구성되면 차단에 사용되는 차단 장치의 순차 및 ACLs/VACL은 수동으로 변경하면 안 됩니다.이로 인해 ARC 서비스가 중단될 수 있으며 차후 블록이 발행되지 않을 수 있습니다.

참고:기본적으로 Cisco IOS 디바이스에서는 차단만 지원됩니다.속도 제한 또는 차단 + 속도 제한을 선택하는 경우 차단 기본값을 재정의할 수 있습니다.

블록을 발행하거나 변경하려면 IPS 사용자에게 관리자 또는 운영자 역할이 있어야 합니다.

Cisco 라우터를 관리하도록 센서 구성

이 섹션에서는 센서가 Cisco 라우터를 관리하도록 구성하는 방법에 대해 설명합니다.여기에는 다음 항목이 포함됩니다.

- 사용자 프로필 구성
- 라우터 및 ACL
- CLI를 사용하여 Cisco 라우터 구성

사용자 프로필 구성

센서는 사용자 프로필을 설정하기 위해 **user-profiles**_*name* 명령을 사용하여 다른 디바이스를 관리합니다.사용자 프로필에는 사용자 ID, 비밀번호 및 enable 비밀번호 정보가 포함됩니다.예를 들어, 모든 사용자가 동일한 비밀번호와 사용자 이름을 공유하는 라우터는 하나의 사용자 프로필 아래에 있을 수 있습니다.

참고:차단 디바이스를 구성하기 전에 사용자 프로필을 생성해야 합니다.

사용자 프로필을 설정하려면 다음 단계를 완료합니다.

1. 관리자 권한이 있는 계정으로 CLI에 로그인합니다.
2. 네트워크 액세스 모드로 들어갑니다.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. 사용자 프로필 이름을 생성합니다.
```
sensor(config-net)#user-profiles PROFILE1
```
4. 해당 사용자 프로필의 사용자 이름을 입력합니다.
```
sensor(config-net-use)#username username
```
5. 사용자의 비밀번호를 지정합니다.
```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```
6. 사용자의 enable 비밀번호를 지정합니다.
```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```
7. 설정을 확인합니다.
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. 네트워크 액세스 하위 모드를 종료합니다.
```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```
9. Enter를 눌러 변경 사항을 적용하거나 no를 입력하여 취소합니다.

라우터 및 ACL

ACL을 사용하는 차단 장치로 ARC를 구성할 때 ACL은 다음과 같이 구성됩니다.

1. 센서 IP 주소가 있는 허용 회선 또는 지정된 경우 센서의 NAT 주소**참고:**센서를 차단하도록 허용하면 이 줄은 ACL에 나타나지 않습니다.
2. 사전 차단 ACL(지정된 경우):이 ACL은 디바이스에 이미 있어야 합니다.**참고:**ARC는 미리 구성된 ACL의 행을 읽고 이러한 행을 블록 ACL의 시작에 복사합니다.
3. 모든 활성 블록
4. Post-**Block ACL** 또는 **IP any를 허용합니다.사후 차단 ACL**(지정된 경우):이 ACL은 디바이스에

이미 있어야 합니다.**참고:**ARC는 ACL의 행을 읽고 ACL의 끝에 이 행을 복사합니다.**참고:**일치하지 않는 모든 패킷을 허용하려면 ACL의 마지막 줄이 ip any를 허용하는지 확인합니다 .**permit ip any any**(사후 차단 ACL이 지정된 경우 사용되지 않음)

참고:ARC가 만드는 ACL은 사용자 또는 다른 시스템에서 수정해서는 안 됩니다.이러한 ACL은 임시 ACL이며 센서에서 지속적으로 새 ACL을 생성합니다.Pre-Block ACL과 Post-Block ACL만 수정할 수 있습니다.

사전 차단 또는 사후 차단 ACL을 수정해야 하는 경우 다음 단계를 완료합니다.

1. 센서에서 차단을 비활성화합니다.
2. 디바이스의 컨피그레이션을 변경합니다.
3. 센서에서 차단을 다시 활성화합니다.

차단이 다시 활성화되면 센서가 새 디바이스 컨피그레이션을 읽습니다.

참고:단일 센서가 여러 디바이스를 관리할 수 있지만 여러 센서가 단일 디바이스를 관리할 수는 없습니다.여러 센서에서 발급되는 블록이 단일 차단 디바이스에 대한 것인 경우 기본 차단 센서가 설계에 통합되어야 합니다.기본 차단 센서는 여러 센서에서 차단 요청을 수신하고 모든 차단 요청을 차단 디바이스에 보냅니다.

라우터 컨피그레이션에서 Pre-Block 및 Post-Block ACL을 생성하고 저장합니다.이러한 ACL은 이름이 지정되거나 번호가 지정된 확장 IP ACL이어야 합니다.ACL 생성 방법에 대한 자세한 내용은 라우터 설명서를 참조하십시오.

참고: Pre-Block 및 Post-Block ACL은 속도 제한에 적용되지 않습니다.

ACL은 하향식으로 평가되고 첫 번째 일치 작업이 수행됩니다.Pre-Block ACL에는 블록에서 발생한 거부보다 우선하는 허용이 포함될 수 있습니다.

사후 차단 ACL은 사전 차단 ACL 또는 블록에서 처리되지 않은 조건을 확인하는 데 사용됩니다.인터페이스에 기존 ACL이 있고 블록이 발급되는 방향인 경우 해당 ACL을 사후 차단 ACL로 사용할 수 있습니다.사후 차단 ACL이 없는 경우 센서는 새 ACL의 끝에 permit ip any any를 삽입합니다.

센서가 시작되면 두 ACL의 내용을 읽습니다.다음 엔트리와 함께 세 번째 ACL을 생성합니다.

- 센서 IP 주소의 허용 라인
- Pre-Block ACL의 모든 컨피그레이션 라인 사본
- 센서에서 차단된 각 주소의 거부 라인
- 사후 블록 ACL의 모든 컨피그레이션 라인의 복사본

센서는 사용자가 지정한 인터페이스 및 방향에 새 ACL을 적용합니다.

참고:새로운 블록 ACL이 라우터의 인터페이스에 특정 방향으로 적용되면 해당 인터페이스의 기존 ACL을 해당 방향으로 교체합니다.

CLI를 사용하여 Cisco 라우터 구성

차단 및 속도 제한을 수행하기 위해 Cisco 라우터를 관리하도록 센서를 구성하려면 다음 단계를 완

료하십시오.

1. 관리자 권한이 있는 계정으로 CLI에 로그인합니다.
2. 네트워크 액세스 하위 모드로 들어갑니다.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. ARC에서 제어하는 라우터의 IP 주소를 지정합니다.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. 사용자 프로필을 구성할 때 생성한 논리적 디바이스 이름을 입력합니다.
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   참고:ARC는 사용자가 입력하는 모든 것을 허용합니다.사용자 프로필이 있는지 확인하지 않습니다.
5. 센서에 액세스하는 데 사용되는 방법을 지정합니다.
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```

   지정하지 않으면 SSH 3DES가 사용됩니다.**참고:**DES 또는 3DES를 사용하는 경우 디바이스에서 SSH 키를 수락하려면 **ssh host-key ip_address** 명령을 사용해야 합니다.
6. 센서 NAT 주소를 지정합니다.
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   참고:이렇게 하면 ACL의 첫 번째 줄에 있는 IP 주소가 센서 주소에서 NAT 주소로 변경됩니다.NAT 주소는 센서 주소와 차단 장치 사이에 있는 중간 장치에 의해 변환되는 포스트 NAT 센서 주소입니다.
7. 라우터가 차단, 속도 제한 또는 둘 다를 수행할지 지정합니다.**참고:**기본값은 차단입니다.라우터가 차단만 수행하도록 하려면 응답 기능을 구성할 필요가 없습니다.속도 제한만
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

   차단 및 속도 제한 모두
   ```
   sensor(config-net-rou)#response-capabilities block|rate-limit
   ```

8. 인터페이스 이름과 방향을 지정합니다.
   ```
   sensor(config-net-rou)#block-interfaces interface_name {in | out}
   ```

   참고:인터페이스 이름은 **interface** 명령 뒤에 사용할 때 라우터가 인식하는 약어여야 합니다.
9. (선택 사항) 사전 ACL 이름을 추가합니다(차단만 해당).
   ```
   sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
   ```
10. (선택 사항) 사후 ACL 이름을 추가합니다(차단만 해당).
    ```
    sensor(config-net-rou-blo)#post-acl-name post_acl_name
    ```
11. 설정을 확인합니다.
    ```
    sensor(config-net-rou-blo)#exit

    sensor(config-net-rou)#show settings

       ip-address: 10.89.127.97
       ------------------------------------------------
          communication: ssh-3des default: ssh-3des
          nat-address: 19.89.149.219 default: 0.0.0.0
          profile-name: PROFILE1
          block-interfaces (min: 0, max: 100, current: 1)
          ------------------------------------------------
             interface-name: GigabitEthernet0/1
             direction: in
             ------------------------------------------------
                pre-acl-name: <defaulted>
                post-acl-name: <defaulted>
    ```

```
            ------------------------------------------------
          ------------------------------------------------
          response-capabilities: block|rate-limit default: block
        ------------------------------------------------
    sensor(config-net-rou)#
```

12. 네트워크 액세스 하위 모드를 종료합니다.

```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```

13. Enter를 눌러 변경 사항을 적용하거나 no를 입력하여 취소합니다.

Cisco 방화벽을 관리하도록 센서 구성

센서가 Cisco 방화벽을 관리하도록 구성하려면 다음 단계를 완료하십시오.

1. 관리자 권한이 있는 계정으로 CLI에 로그인합니다.
2. 네트워크 액세스 하위 모드로 들어갑니다.

```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```

3. ARC에서 제어하는 방화벽의 IP 주소를 지정합니다.

```
sensor(config-net)#firewall-devices ip_address
```

4. 사용자 프로필을 구성할 때 생성한 사용자 프로필 이름을 입력합니다.

```
sensor(config-net-fir)#profile-name user_profile_name
```

참고:ARC는 사용자가 입력하는 모든 것을 허용합니다.논리적 디바이스가 있는지 확인하지 않습니다.

5. 센서에 액세스하는 데 사용되는 방법을 지정합니다.

```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

지정하지 않으면 SSH 3DES가 사용됩니다.**참고:**DES 또는 3DES를 사용하는 경우 **ssh host-key ip_address** 명령을 사용하여 키를 허용하거나 ARC가 디바이스에 연결할 수 없습니다.

6. 센서 NAT 주소를 지정합니다.

```
sensor(config-net-fir)#nat-address nat_address
```

참고:이렇게 하면 ACL의 첫 번째 줄에 있는 IP 주소가 센서의 IP 주소에서 NAT 주소로 변경됩니다.NAT 주소는 센서 주소와 차단 장치 사이에 있는 중간 장치에 의해 변환되는 포스트 NAT 센서 주소입니다.

7. 네트워크 액세스 하위 모드를 종료합니다.

```
sensor(config-net-fir)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```

8. Enter를 눌러 변경 사항을 적용하거나 no를 입력하여 취소합니다.

PIX/ASA에서 SHUN으로 차단

shun 명령을 **실행하면** 공격 호스트의 연결이 차단됩니다.명령의 값과 일치하는 패킷은 차단 기능이 제거될 때까지 삭제되고 기록됩니다.shun은 지정된 호스트 주소와의 연결이 현재 활성 상태인지 여부에 관계없이 적용됩니다.

목적지 주소, 소스 및 목적지 포트, 프로토콜을 지정할 경우 해당 매개변수와 일치하는 연결로 차단 범위를 좁힙니다.각 소스 IP 주소에 대해 **shun** 명령을 하나만 사용할 수 있습니다.

shun 명령은 공격을 동적으로 차단하는 데 사용되므로 보안 어플라이언스 컨피그레이션에 표시되지 않습니다.

인터페이스가 제거될 때마다 해당 인터페이스에 연결된 모든 shun도 제거됩니다.

이 예에서는 문제의 호스트(10.1.1.27)이 피해자(10.2.2.89)과 TCP에 연결되었음을 보여줍니다.보안 어플라이언스 연결 테이블의 연결은 다음과 같습니다.

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

공격 호스트의 연결을 차단하려면 특별 권한 EXEC 모드에서 **shun** 명령을 사용합니다.다음 옵션과 함께 shun 명령을 적용합니다.

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

이 명령은 보안 어플라이언스 연결 테이블에서 연결을 삭제하고 10.1.1.27:555~10.2.2.89:666(TCP)의 패킷이 보안 어플라이언스를 통과하지 못하도록 합니다.

관련 정보

- Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터 관리를 위한 센서 구성
- 기술 지원 및 문서 – Cisco Systems