코어 보호:인프라 보호 액세스 제어 목록

목차

소개

이 문서에서는 인프라 보호 ACL(Access Control List)에 대한 지침 및 권장 구축 기술을 제공합니다. 인프라 ACL은 인프라 장비에 승인된 트래픽만 명시적으로 허용하는 동시에 다른 모든 전송 트래픽을 허용하여 직접 인프라 공격의 위험과 효율성을 최소화하는 데 사용됩니다.

인프라 보호

배경

네트워크 인그레스(ingress) 지점에 인프라 보호 ACL을 구축해야 하는 경우 우발적 및 악의적 위험으로부터 라우터를 보호하려는 노력이 필요합니다.이러한 IPv4 및 IPv6 ACL은 외부 소스에서 라우터 인터페이스와 같은 모든 인프라 주소에 대한 액세스를 거부합니다.동시에 ACL은 루틴 트랜짓 트래픽이 중단 없이 흐르도록 허용하고 기본 RFC 1918 , RFC 3330 및 스푸핑 방지 필터링을 제공합니다.

라우터에서 수신한 데이터는 두 가지 범주로 나눌 수 있습니다.

- 전달 경로를 통해 라우터를 통과하는 트래픽
- 라우터로 향하는 트래픽은 라우트 프로세서 처리를 위한 수신 경로를 통해 전송됩니다.

정상적인 운영에서는 대부분의 트래픽이 최종 목적지로 향하는 라우터를 통해 흐릅니다.

그러나 RP(Route Processor)는 특정 유형의 데이터, 특히 라우팅 프로토콜, 원격 라우터 액세스(SSH[Secure Shell]), 네트워크 관리 트래픽(예: SNMP)을 직접 처리해야 합니다. 또한 ICMP(Internet Control Message Protocol) 및 IP 옵션과 같은 프로토콜은 RP에서 직접 처리해야 할

수 있습니다.대부분 내부 소스에서만 직접 인프라 라우터 액세스가 필요합니다.몇 가지 주목할 만한 예외 사항은 외부 BGP(Border Gateway Protocol) 피어링, 실제 라우터에서 종료되는 프로토콜(예: 일반 라우팅 캡슐화[GRE] 또는 IPv6 over IPv4 터널), 에코 요청 또는 ICMP 비도달 가능 시간 및 트레이스라우트에 대한 만료된 메시지(TTL)와 같은 연결 테스트를 위한 잠재적으로 제한된 ICMP 패킷입니다.

참고: ICMP는 DoS(simple denial-of-service) 공격에 자주 사용되며 필요한 경우 외부 소스에서만 허용되어야 합니다.

모든 RP에는 작동하는 성능 봉투가 있습니다.RP로 향하는 과도한 트래픽은 라우터를 압도할 수 있습니다.이로 인해 CPU 사용량이 높고, 결과적으로 패킷 및 라우팅 프로토콜이 삭제되어 서비스 거부가 발생합니다.외부 소스에서 인프라 라우터에 대한 액세스를 필터링하면 직접 라우터 공격과 관련된 외부 위험 중 많은 부분이 완화됩니다.외부 소싱 공격은 더 이상 인프라 장비에 액세스할 수 없습니다.공격은 인그레스 인터페이스에서 자율 시스템(AS)으로 삭제됩니다.

이 문서에서 설명하는 필터링 기술은 네트워크 인프라 장비를 대상으로 하는 데이터를 필터링하기 위한 것입니다.인프라 필터링과 일반 필터링을 혼동하지 마십시오.인프라 보호 ACL의 유일한 목적은 어떤 프로토콜과 소스가 중요한 인프라 장비에 액세스할 수 있는지를 세분화된 수준으로 제한하는 것입니다.

네트워크 인프라 장비는 다음 영역을 포함합니다.

- 루프백 인터페이스를 포함한 모든 라우터 및 스위치 관리 주소
- 모든 내부 링크 주소:라우터 간 링크(포인트-투-포인트 및 다중 액세스)
- 외부 소스에서 액세스해서는 안 되는 내부 서버 또는 서비스

이 문서에서는 인프라로 이동되지 않는 모든 트래픽을 종종 트랜짓 트래픽이라고 합니다.

기술

다음과 같은 다양한 기술을 통해 인프라를 보호할 수 있습니다.

- **ACL(rACL) 수신**Cisco 12000 및 7500 플랫폼은 RP로 향하는 모든 트래픽을 필터링하고 전송 트래픽에 영향을 주지 않는 rACL을 지원합니다.인증된 트래픽은 명시적으로 허용되어야 하며 rACL은 모든 라우터에 구축되어야 합니다. GSR 참조:액세스 제어 목록 수신에 대한 자세한 내용
- **hop-by-hop 라우터 ACL**라우터는 라우터의 인터페이스에 대한 인증된 트래픽만 허용하는 ACL을 정의하여 보호될 수 있으며, 전송 트래픽을 제외한 다른 모든 트래픽은 거부하며 명시적으로 허용되어야 합니다.이 ACL은 rACL과 논리적으로 유사하지만 전송 트래픽에 영향을 미치므로 라우터의 전달 속도에 부정적인 영향을 미칠 수 있습니다.
- **인프라 ACL을 통한 에지 필터링**ACL은 네트워크 에지에 적용할 수 있습니다.서비스 공급자(SP)의 경우 AS의 가장자리입니다.이 ACL은 인프라 주소 공간으로 향하는 트래픽을 명시적으로 필터링합니다.에지 인프라 ACL을 구축하려면 이 공간에 액세스하는 필수/승인된 프로토콜과 인프라 공간을 명확하게 정의해야 합니다.ACL은 피어링 연결, 고객 연결 등과 같은 외부 연결 모두에서 네트워크에 인그레스(ingress)에 적용됩니다.이 문서에서는 에지 인프라 보호 ACL의 개발 및 구축에 대해 중점적으로 설명합니다.

ACL 예

이러한 IPv4 및 IPv6 액세스 목록은 보호 ACL에 필요한 일반적인 항목의 간단하면서도 현실적인 예

를 제공합니다.이러한 기본 ACL은 로컬 사이트별 컨피그레이션 세부사항으로 사용자 정의되어야 합니다.이중 IPv4 및 IPv6 환경에서는 두 액세스 목록이 모두 구축됩니다.

IPv4 예

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

IPv6 예

IPv6 access-list는 명명된 확장 액세스 목록으로 적용해야 합니다.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6 any any
```

참고: log 키워드를 사용하여 지정된 프로토콜의 소스 및 대상에 대한 추가 세부 정보를 제공할 수 있습니다.이 키워드는 ACL 적중 세부 정보에 대한 중요한 정보를 제공하지만 **log** 키워드를 사용하는 ACL 항목에 대한 과도한 적중 수는 CPU 사용률을 높입니다.로깅과 관련된 성능 영향은 플랫폼에 따라 다릅니다.또한 log 키워드를 사용하면 access-list 문과 일치하는 패킷에 대해 Cisco CEF(Express Forwarding) 스위칭이 비활성화됩니다.대신 이 패킷이 빠르게 전환됩니다.

보호 ACL 개발

일반적으로 인프라 ACL은 4개의 섹션으로 구성됩니다.

- AS에 속하는 소스 주소와 비합법적인 소스 및 패킷이 외부 소스에서 AS로 입력되는 것을 거부하는 특수 사용 주소 및 스푸핑 방지 항목**참고:** RFC 3330은 필터링이 필요할 수 있는 IPv4 특수 사용 주소를 정의합니다.RFC 1918은 인터넷에서 유효한 소스 주소가 아닌 IPv4 예약 주소 공간을 정의합니다.RFC 3513은 IPv6 주소 지정 아키텍처를 정의합니다.RFC 2827 은 인그레스 필터링 지침을 제공합니다.
- 명시적으로 허용된 외부 소스 트래픽은 인프라 주소로 전송됨
- 인프라 주소로 나가는 기타 모든 외부 소스 트래픽에 대한 거부 명령문
- **비인프라** 대상으로 라우팅되는 일반 백본 트래픽에 대한 기타 모든 트래픽에 대한 permit 문

인프라 ACL의 최종 라인은 전송 트래픽을 명시적으로 허용합니다.**ip any** for IPv4 및 permit ipv6 **any any for IPv**6. 이 항목은 모든 IP 프로토콜이 코어를 통해 허용되고 고객이 문제 없이 애플리케이션을 계속 실행할 수 있도록 합니다.

인프라 보호 ACL을 개발하는 첫 번째 단계는 필요한 프로토콜을 이해하는 것입니다.모든 사이트에는 특정 요구 사항이 있지만, 특정 프로토콜은 일반적으로 구축되며 파악해야 합니다.예를 들어 외

부 피어에 대한 외부 BGP는 명시적으로 허용되어야 합니다.인프라 라우터에 직접 액세스해야 하는 다른 모든 프로토콜도 명시적으로 허용되어야 합니다.예를 들어, 코어 인프라 라우터에서 GRE 터널을 종료할 경우 GRE(Protocol 47)도 명시적으로 허용해야 합니다.마찬가지로, 코어 인프라 라우터에서 IPv4를 통한 IPv6 터널을 종료할 경우 프로토콜 41(IPv6 over IPv4)도 명시적으로 허용되어야 합니다.

분류 ACL을 사용하여 필요한 프로토콜을 식별할 수 있습니다.분류 ACL은 인프라 라우터로 이동할 수 있는 다양한 프로토콜에 대한 **permit** 문으로 구성됩니다.전체 목록은 Cisco IOS® Software에서 지원되는 IP 프로토콜의 부록을 참조하십시오.show access-**list 명령** 명령을 사용하여 ACE(access control entry) 적중 수를 표시하면 필요한 프로토콜이 식별됩니다.예기치 않은 프로토콜에 대한 **허용** 설명을 생성하기 전에 의심스러운 또는 놀라운 결과를 조사하고 파악해야 합니다.

예를 들어 이 IPv4 ACL은 GRE, IPsec(ESP) 및 IPv6 터널링(IP Protocol 41)을 허용해야 하는지 여부를 결정하는 데 도움이 됩니다.

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any

interface <int>
 ip access-group 101 in
```

이 IPv6 ACL을 사용하여 GRE 및 IPsec(ESP)을 허용해야 하는지 확인할 수 있습니다.

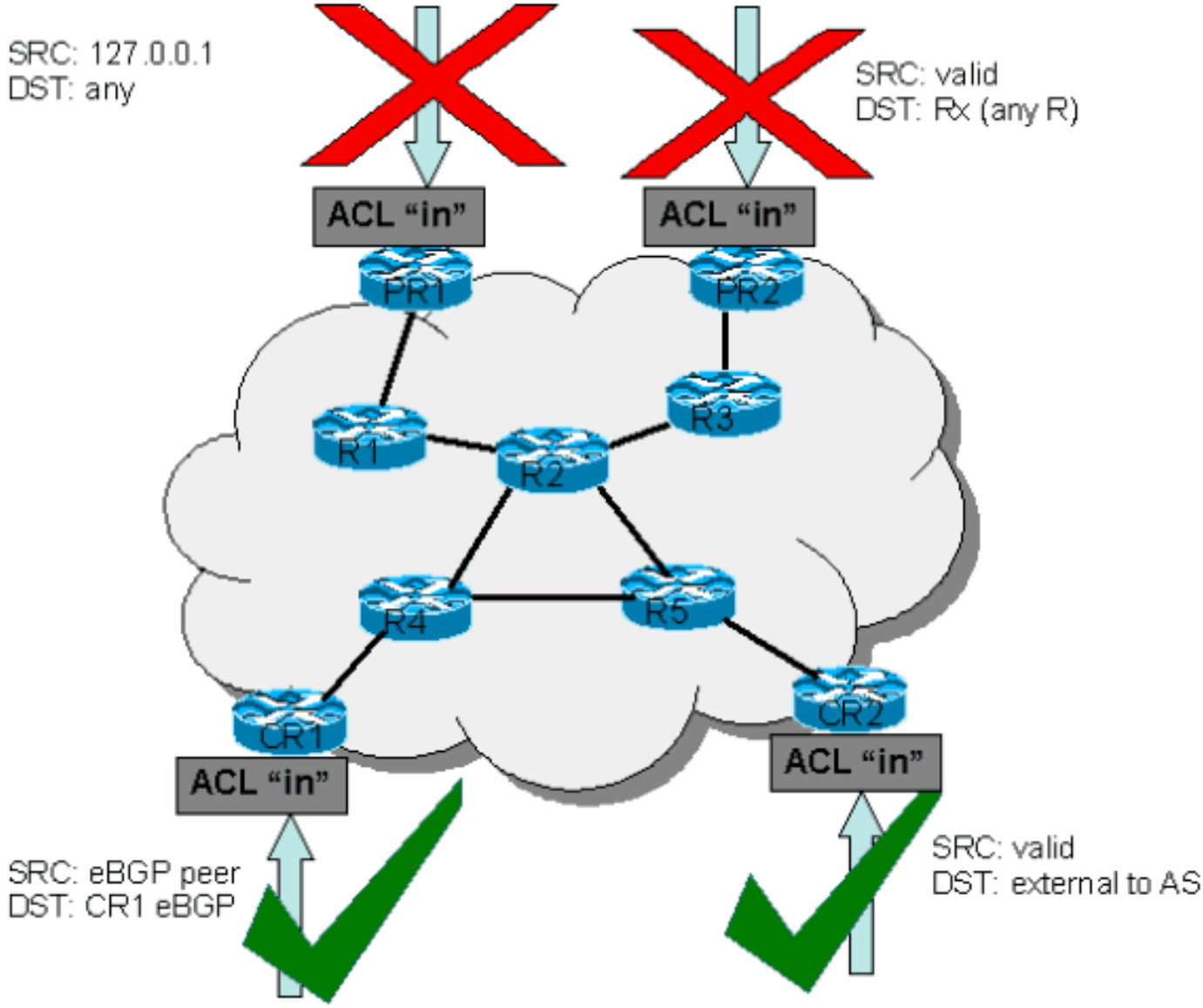
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

필수 프로토콜 외에도 ACL이 보호하는 공간이므로 인프라 주소 공간을 식별해야 합니다.인프라 주소 공간에는 내부 네트워크에 사용되는 모든 주소가 포함되며 라우터 인터페이스, 포인트-투-포인트 링크 주소 지정, 중요 인프라 서비스 등 외부 소스에서 거의 액세스하지 않습니다.이러한 주소는 인프라 ACL의 목적지 부분에 사용되므로 요약은 중요합니다.가능한 경우 이러한 주소를 CIDR(Classless Interdomain Routing) 블록으로 그룹화해야 합니다.

식별된 프로토콜과 주소를 사용하여 인프라 ACL을 구축하여 프로토콜을 허용하고 주소를 보호할 수 있습니다.ACL은 직접 보호 외에도 인터넷에서 특정 유형의 잘못된 트래픽에 대한 1차 방어선을 제공합니다.

- RFC 1918 공간은 거부해야 합니다.
- RFC 3330에 정의된 특수 사용 주소 공간에 해당하는 소스 주소의 패킷은 거부되어야 합니다.
- 스푸핑 방지 필터를 적용해야 합니다.(주소 공간은 AS 외부에서 오는 패킷의 소스가 되어서는 안 됩니다.)

새로 생성된 이 ACL은 모든 인그레스(ingress) 인터페이스에 적용되어야 합니다.자세한 내용은 구축 지침 및 구축 예에 대한 섹션을 참조하십시오.



ACL 및 단편화된 패킷

ACL에는 **fragments** 키워드가 있으며, 이 키워드는 특화된 프래그먼트 패킷 처리 동작을 활성화합니다.이 **fragments** 키워드가 없으면 ACL의 Layer 3 문과 일치하는 비초기 프래그먼트가 일치된 엔트리의 permit 또는 deny 문의 영향을 받습니다(레이어 4 정보와 상관없음).그러나 **fragments** 키워드를 추가하여 ACL이 더 세분화된 비초기 프래그먼트를 거부하거나 허용하도록 할 수 있습니다.이 동작은 IPv4 및 IPv6 액세스 목록 모두에서 동일합니다. 단, IPv4 ACL은 Layer 3 및 Layer 4 문 내에서 fragments 키워드를 사용할 수 있지만 IPv6 ACL은 Layer 3 문 내에서 fragments 키워드를 사용할 수 있습니다.

프래그먼트를 필터링하면 초기 이외의 프래그먼트를 사용하는 DoS(Denial of Service) 공격(즉, FO > 0)에 대한 추가적인 보호 레이어가 추가됩니다. ACL 시작 시 비초기 프래그먼트에 대한 deny 문을 사용하면 모든 비초기 프래그먼트가 라우터에 액세스하지 못합니다.드물지만, 유효한 세션에는 프래그먼트화가 필요할 수 있으므로 **deny fragment** 문이 ACL에 있는 경우 필터링됩니다.

예를 들어 다음 부분 IPv4ACL을 고려하십시오.

```
access-list 110 deny tcp any infrastructure_IP fragments
access-list 110 deny udp any infrastructure_IP fragments
access-list 110 deny icmp any infrastructure_IP fragments
```

```
<rest of ACL>
```

이러한 엔트리를 ACL의 시작 부분에 추가하면 코어 라우터에 대한 비초기 프래그먼트 액세스를 거부하며, 조각화되지 않은 패킷 또는 초기 프래그먼트는 **deny fragment** 문의 영향을 받지 않는 ACL의 다음 행으로 전달됩니다.앞의 ACL 명령은 또한 각 프로토콜(UDP(Universal Datagram Protocol), TCP, ICMP)이 ACL에서 별도의 카운터를 증가하므로 공격의 분류를 용이하게 합니다.

다음은 IPv6에 대한 비슷한 예입니다.

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

IPv6 ACL의 시작 부분에 이 항목을 추가하면 코어 라우터에 대한 비초기 프래그먼트 액세스가 거부됩니다.앞서 언급한 대로 IPv6 액세스 목록은 Layer 3 문 내에서 fragments 키워드를 사용할 수만 있습니다.

많은 공격이 프래그먼트된 패킷으로 코어 라우터를 플러딩하는 것에 의존하기 때문에 코어 인프라에 들어오는 프래그먼트를 필터링하면 추가적인 보호 수단이 제공되며 인프라 ACL의 레이어 3 규칙을 일치시켜 공격이 프래그먼트를 주입할 수 없도록 합니다.

옵션에 대한 자세한 내용은 액세스 제어 목록 및 IP 프래그먼트를 참조하십시오.

위험 평가

인프라 보호 ACL을 구축할 때 다음과 같은 두 가지 주요 위험 영역을 고려하십시오.

- 적절한 **permit/deny** 명령문이 있는지 확인합니다.ACL을 적용하려면 모든 필수 프로토콜을 허용해야 하며 올바른 주소 공간은 **deny** 문으로 보호되어야 합니다.
- ACL 성능은 플랫폼마다 다릅니다.ACL을 구축하기 전에 하드웨어의 성능 특성을 검토합니다.

항상 그렇듯이 구축 전에 Lab에서 이 설계를 테스트하는 것이 좋습니다.

부록

Cisco IOS Software에서 지원되는 IP 프로토콜

다음 IP 프로토콜은 Cisco IOS Software에서 지원합니다.

- 1 - ICMP
- 2 - IGMP
- 3 - GGP
- 4 - IP 캡슐화의 IP
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP

- 41 - IPv4 터널링의 IPv6
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 - swipe
- 54 - 나프
- 55 - IP 모빌리티
- 63 - 모든 로컬 네트워크
- 77 - SUN ND
- 80 - ISO IP
- 88 - EIGRP
- 89 - OSPF
- 90 - Sprite RPC
- 91 - LARP
- 94 - KA9Q/NOS 호환 IP over IP
- 103 - PIM
- 108 - IP 압축
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

구축 지침

Cisco는 보수적인 구축 사례를 권장합니다.인프라 ACL을 성공적으로 구축하려면 필요한 프로토콜을 잘 이해하고 주소 공간을 명확하게 식별하고 정의해야 합니다.이 지침은 반복적인 접근 방식을 사용하여 보호 ACL을 구축하는 매우 보수적인 방법을 설명합니다.

1. **분류 ACL을 사용하여 네트워크에서 사용되는 프로토콜을 식별합니다.**인프라 디바이스에 액세스하는 알려진 모든 프로토콜을 허용하는 ACL을 구축합니다.이 검색 ACL에는 인프라 IP 공간을 포괄하는 **any**와 destination의 소스 주소가 있습니다.로깅은 프로토콜 **허용** 문과 일치하는 소스 주소 목록을 개발하는 데 사용할 수 있습니다.트래픽 흐름을 허용하려면 **ip any**(IPv4) 또**는 ipv6 any**(IPv6)를 허용하는 마지막 행이 필요합니다.목표는 특정 네트워크에서 사용하는 프로토콜을 결정하는 것입니다.로깅은 분석에서 라우터와 통신할 수 있는 다른 항목을 확인하는 데 사용됩니다.**참고: log** 키워드는 ACL 적중 세부사항에 대한 유용한 정보를 제공하지만 이 키워드를 사용하는 ACL 항목에 대한 과도한 적중 횟수가 발생할 경우 로그 항목 수가 엄청나게 많아지고 라우터 CPU 사용량이 높을 수 있습니다.또한 **log** 키워드를 사용하면 access-list 문과 일치하는 패킷에 대해 Cisco CEF(Express Forwarding) 스위칭이 비활성화됩니다.대신 이 패킷이 빠르게 전환됩니다.트래픽을 분류하는 데 필요한 경우에만 짧은 시간 동안 log 키워드를 사용합니다.
2. **식별된 패킷을 검토하고 경로 프로세서 RP에 대한 액세스를 필터링하기 시작합니다.**1단계에서 ACL에 의해 필터링된 패킷이 식별되고 검토되면 허용되는 프로토콜의 인프라 주소에 대한 **소스**를 **허용하는** ACL을 구축합니다.1단계에서와 마찬가지로 **log** 키워드는 **허용** 항목과 일치하는 패킷에 대한 자세한 정보를 제공할 수 있습니다.**deny any**를 사용하면 라우터로 향하는 예기치 않은 패킷을 식별할 수 있습니다.이 ACL의 마지막 줄은 통과 트래픽의 흐름을 허용하려면 **permit ip any**(IPv4) 또는 **permit ipv6 any**(IPv6) 문이어야 합니다.이 ACL은 기본 보호를

제공하며 네트워크 엔지니어가 필요한 모든 트래픽이 허용되도록 합니다.

3. **소스 주소를 제한합니다.**허용해야 하는 프로토콜을 명확하게 이해하면 추가 필터링을 수행하여 해당 프로토콜에 대해 승인된 소스만 허용할 수 있습니다.예를 들어 외부 BGP 네이버 또는 특정 GRE 피어 주소를 명시적으로 허용할 수 있습니다.이 단계를 수행하면 서비스를 중단하지 않고 위험을 줄일 수 있으며 인프라 장비에 대한 세분화된 제어를 적용할 수 있습니다.
4. **ACL의 대상 주소를 제한합니다(*선택 사항*).**일부 인터넷 서비스 공급자(ISP)는 특정 프로토콜만 라우터의 특정 목적지 주소를 사용하도록 선택할 수 있습니다.이 마지막 단계는 프로토콜에 대한 트래픽을 허용할 수 있는 목적지 주소의 범위를 제한하는 것입니다.

구축 예

IPv4 예

이 IPv4 예는 다음 주소 지정을 기반으로 라우터를 보호하는 인프라 ACL을 보여줍니다.

- ISP 주소 블록은 169.223.0.0/16입니다.
- ISP 인프라 블록은 169.223.252.0/22입니다.
- 라우터에 대한 루프백은 169.223.253.1/32입니다.
- 라우터는 피어링 라우터이며 169.254.254.1(주소 169.223.252.1)이 있는 피어링 라우터입니다.

표시되는 인프라 보호 ACL은 이전 정보를 기반으로 개발됩니다.ACL은 외부 피어에 대한 외부 BGP 피어링을 허용하고, 안티스푸핑 필터를 제공하며, 모든 외부 액세스로부터 인프라를 보호합니다.

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).

!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

IPv6 예

이 IPv6 예는 다음 주소 지정을 기반으로 라우터를 보호하는 인프라 ACL을 보여줍니다.

- ISP에 할당된 전체 접두사 블록은 2001:0DB8::/32입니다.
- ISP에서 네트워크 인프라 주소에 사용하는 IPv6 접두사 블록은 2001:0DB8:C18::/48입니다.
- 소스 IPv6 주소가 2001:0DB8:C18:2:1::1인 BGP 피어링 라우터가 있는데, 이 라우터는 목적지 IPv6 주소 2001:0DB8:C19:2:1::F로 피어가 됩니다.

표시되는 인프라 보호 ACL은 이전 정보를 기반으로 개발됩니다.ACL은 외부 피어에 대한 외부 다중 프로토콜 BGP 피어링을 허용하고, 안티스푸핑 필터를 제공하며, 모든 외부 액세스로부터 인프라를 보호합니다.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source. !--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only applications/protocols whose destination !--- address is part of the infrastructure IP block. !-- The source of the traffic should be known and authorized. !--- Note: This template must be tuned to the !--- specific source address environment of the network. Variables in !--- the template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 - Explicit Permit for Transit Traffic permit ipv6 any any
```

관련 정보

- 액세스 목록 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems