GSR:액세스 제어 목록 수신

목차

소개

이 문서에서는 rACL(Receive Access Control List)[1]이라는 새로운 보안 기능에 대해 설명하고 rACL 구축에 대한 권장 사항 및 지침을 제공합니다.수신 ACL은 라우터의 기가비트 GRP(route processor)를 불필요하고 잠재적으로 악의적인 트래픽으로부터 보호함으로써 Cisco 12000 라우터의 보안을 강화하는 데 사용됩니다.수신 ACL은 Cisco IOS ® Software Release 12.0.21S2의 유지 보수 스로틀(privacy exclusion)에 추가되었고 Cisco IOS Software Release 12.0(22)S에 통합되었습니다.

GRP 보호

GSR(Gigabit Switch Router)에서 수신한 데이터는 크게 두 가지 범주로 나눌 수 있습니다.

- 전달 경로를 통해 라우터를 통과하는 트래픽입니다.
- 추가 분석을 위해 GRP에 대한 수신 경로를 통해 전송해야 하는 트래픽.

정상적인 운영에서는 대부분의 트래픽이 GSR을 통해 다른 목적지로 라우팅됩니다.그러나 GRP는 특정 유형의 데이터, 특히 라우팅 프로토콜, 원격 라우터 액세스, 네트워크 관리 트래픽(예: SNMP[Simple Network Management Protocol])을 처리해야 합니다. 이 트래픽 외에도 다른 레이어 3 패킷에는 GRP의 처리 유연성이 필요할 수 있습니다.여기에는 특정 IP 옵션 및 특정 형식의 ICMP(Internet Control Message Protocol) 패킷이 포함됩니다.rACL과 GSR의 수신 경로 트래픽에 대한 자세한 내용은 수신 인접성 및 펀치된 패킷에 대한 부록을 참조하십시오.

GSR에는 여러 데이터 경로가 있으며, 각 경로는 서로 다른 형태의 트래픽을 서비스합니다.트랜짓 트래픽은 인그레스 라인 카드(LC)에서 패브릭으로 전달된 다음 이그레스 카드로 전달되어 다음 홉을 전달합니다.GSR은 트랜짓 트래픽 데이터 경로 외에도 로컬 처리가 필요한 트래픽에 대해 두 개

의 다른 경로를 가집니다.LC에서 LC CPU로, LC에서 LC CPU로 GRP로 패브릭에 연결합니다.다음 표는 자주 사용되는 여러 기능 및 프로토콜의 경로를 보여줍니다.

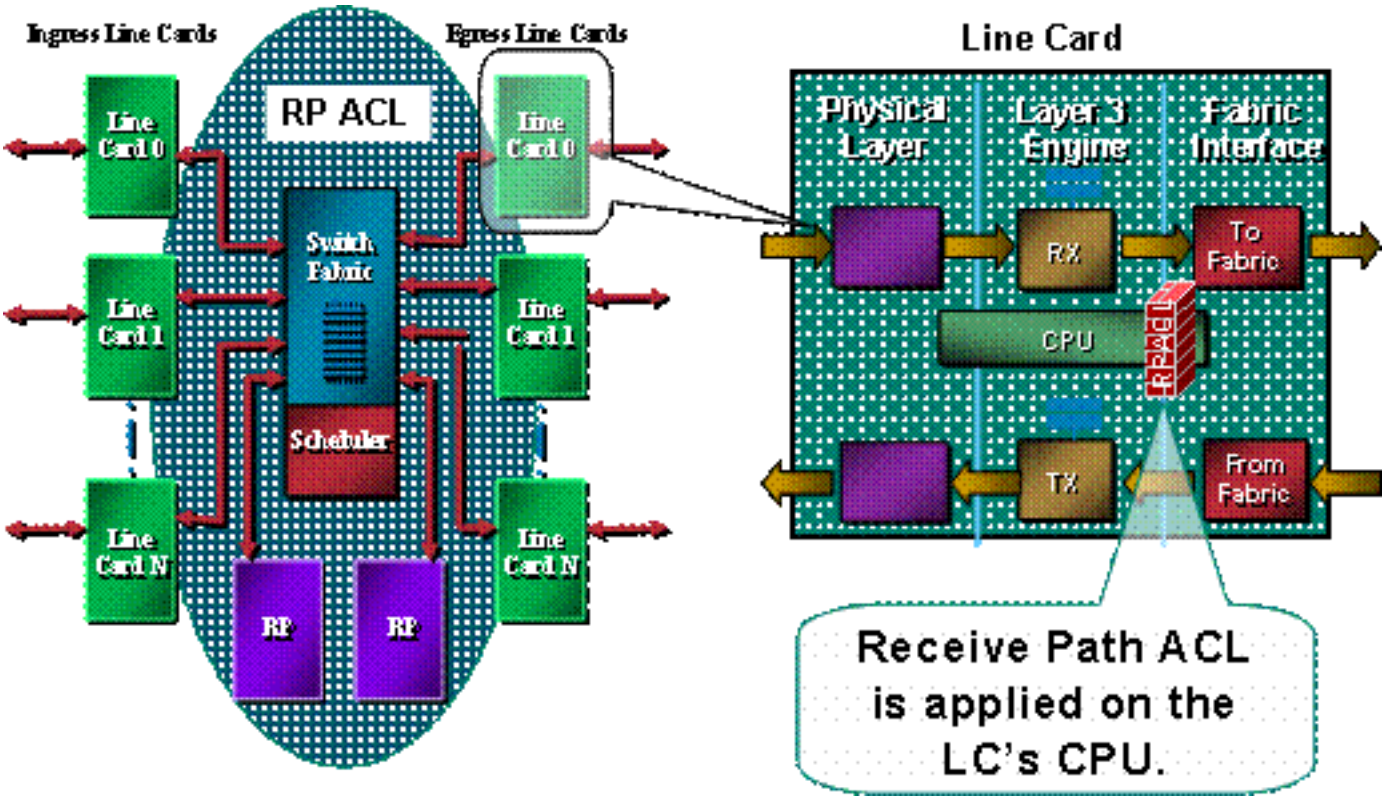
트래픽 유형	데이터 경로
일반(전송) 트래픽	LC에서 패브릭 대 LC로
라우팅 프로토콜/SSH/SNMP	LC에서 LC CPU로 GRP로 패브릭 연결
ICMP 에코(ping)	LC-LC CPU
로깅	

GSR의 경로 프로세서에는 GRP 자체를 대상으로 하는 LC에서 전달되는 트래픽을 처리할 수 있는 제한된 용량이 있습니다.많은 양의 데이터가 GRP로 펀팅되어야 하는 경우 해당 트래픽이 GRP를 압도할 수 있습니다.따라서 DoS(denial-of-service) 공격이 효과적입니다.GRP의 CPU는 패킷 검사를 따라잡기 위해 고군분투하며 패킷을 삭제하기 시작하여 입력 보류 및 SPD(Selective Packet Discard) 큐를 플러딩합니다.[2] GSR은 [3]가지 시나리오에서 보호되어야 하며, 이는 라우터의 GRP에 대한 DoS 공격으로부터 발생할 수 있습니다.

- 정상적인 우선순위 플러드로부터 라우팅 프로토콜 패킷 손실
- 일반 우선순위 플러드로 인한 관리 세션(텔넷, SSH(Secure Shell), SNMP) 패킷 손실
- 스푸핑된 높은 우선순위 플러드로부터 패킷 손실

일반 우선순위 플러드 중 라우팅 프로토콜 데이터의 잠재적인 손실은 현재 정적 분류 및 LC에서 GRP로 향하는 트래픽 속도 제한에 의해 완화됩니다.그러나 이러한 접근 방식에는 한계가 있습니다.여러 LC를 통해 공격이 전달되는 경우 GRP로 향하는 일반 우선 순위 트래픽의 속도 제한은 우선 순위가 높은 라우팅 프로토콜 데이터에 대한 보호를 보장하는 데 충분하지 않습니다.이러한 보호를 제공하기 위해 일반 우선순위 데이터가 삭제되는 임계값을 낮추면 일반 우선순위 플러드로부터 관리 트래픽의 손실이 심화됩니다.

이 그림에서 볼 수 있듯이, rACL은 패킷이 GRP로 전송되기 전에 각 LC에서 실행됩니다.



GRP에 대한 보호 메커니즘이 필요합니다.ACL은 수신 인접성으로 인해 GRP로 전송되는 트래픽에 영향을 줍니다.수신 인접성은 라우터의 IP 주소로 향하는 트래픽에 대한 Cisco Express Forwarding 인접성입니다(예: 라우터 인터페이스에 구성된 브로드캐스트 주소 또는 주소).[3] 수신 인접성 및 펀칭된 패킷에 대한 자세한 내용은 부록 섹션을 참조하십시오.

LC로 들어오는 트래픽은 먼저 LC의 로컬 CPU로 전송되며, GRP에서 처리해야 하는 패킷은 경로 프로세서로 전달하도록 대기열에 추가됩니다.수신 ACL은 GRP에서 생성된 다음 다양한 LC의 CPU로 푸시됩니다.LC CPU에서 GRP로 트래픽을 전송하기 전에 트래픽을 rACL과 비교합니다.허용된 경우 트래픽은 GRP로 전달되고 다른 모든 트래픽은 거부됩니다.rACL은 LC-GRP 속도 제한 기능 이전에 검사됩니다.rACL은 모든 수신 인접성에 사용되기 때문에 LC CPU에서 처리하는 일부 패킷(예: 에코 요청)도 rACL 필터링의 적용을 받습니다.이는 rACL 항목을 디자인할 때 고려해야 합니다.

수신 ACL은 라우터의 리소스를 보호하기 위한 다중 부품 프로그램 범위의 일부입니다.향후 작업에는 rACL에 대한 속도 제한 구성 요소가 포함됩니다.

성능에 미치는 영향

단일 컨피그레이션 항목 및 정의된 액세스 목록 자체를 유지하는 데 필요한 메모리 이외의 메모리는 사용되지 않습니다.각 LC에 rACL이 복사되므로 각 LC에서 메모리 영역이 약간 다릅니다.전체적으로 활용되는 리소스는 구축 혜택과 비교할 때 매우 미미한 수준입니다.

수신 ACL은 전달된 트래픽의 성능에 영향을 주지 않습니다.rACL은 수신 인접성 트래픽에만 적용됩니다.전달된 트래픽은 rACL의 영향을 받지 않습니다.트랜짓 트래픽은 인터페이스 ACL을 사용하여 필터링됩니다.이러한 "일반" ACL은 지정된 방향의 인터페이스에 적용됩니다.트래픽은 rACL 처리 전에 ACL 처리를 거쳐야 하므로 인터페이스 ACL에서 거부된 트래픽은 rACL에서 수신되지 않습니다.[4]

실제 필터링을 수행하는 LC(즉, rACL에 의해 필터링된 트래픽을 수신하는 LC)는 rACL의 처리 때문에 CPU 사용률이 증가하게 됩니다.그러나 이러한 CPU 사용률이 증가한 것은 GRP로 향하는 트래픽이 많기 때문입니다.rACL 보호 GRP의 이점은 LC에서 증가된 CPU 사용률보다 훨씬 큽니다.LC의 CPU 사용률은 LC 엔진 유형에 따라 달라집니다.예를 들어, 동일한 공격을 받으면 엔진 3 LC의 CPU 사용률이 엔진 0 LC보다 낮습니다.

access-list compiled 명령을 사용하여 터보 ACL을 활성화하면 ACL이 매우 효율적인 일련의 조회 테이블 항목으로 변환됩니다.터보 ACL이 활성화된 경우 rACL 깊이는 성능에 영향을 주지 않습니다.즉, 처리 속도는 ACL의 항목 수와 독립적입니다.rACL이 짧으면 터보 ACL이 성능을 크게 향상시키지는 않지만 메모리를 사용합니다.짧은 rACL을 사용하면 컴파일된 ACL이 필요하지 않을 수 있습니다.

GRP를 보호함으로써 rACL은 공격 중 라우터 및 궁극적으로 네트워크 안정성을 보장합니다.위에서 설명한 대로 rACL은 LC CPU에서 처리되므로 라우터에서 대량의 데이터를 전송하면 각 LC의 CPU 사용률이 증가합니다.E0/E1 및 일부 E2 번들에서 CPU 사용률이 100% 이상이면 라우팅 프로토콜 및 링크 레이어 삭제로 이어질 수 있습니다.이러한 삭제는 카드에 현지화되어 GRP 라우팅 프로세스가 보호되므로 안정성이 유지됩니다.E2 카드(스로틀링 지원 마이크로코드[5])는 로드가 많은 경우 스로틀 모드를 활성화하고 우선순위 6 및 7 트래픽만 라우팅 프로토콜로 전달합니다.다른 엔진 유형에는 멀티큐 아키텍처가 있습니다.예를 들어, E3 카드에는 CPU에 대한 3개의 대기열이 있으며, 라우팅 프로토콜 패킷(우선순위 6/7)은 각각 다른 우선 순위가 높은 대기열에 있습니다.우선 순위가 높은 패킷으로 인해 발생하는 경우가 아니면 LC CPU가 높으면 라우팅 프로토콜이 삭제되지 않습니다.우선 순위가 더 낮은 대기열에 대한 패킷은 tail-dropp됩니다.마지막으로, E4 기반 카드는 CPU에 8개의 대기열을 가지며, 하나는 라우팅 프로토콜 패킷 전용으로 사용됩니다.

구문

수신 ACL은 라우터의 각 LC에 rACL을 배포하기 위해 다음 전역 컨피그레이션 명령과 함께 적용됩니다.

```
[no] ip receive access-list
```

이 구문에서 *<num>은* 다음과 같이 정의됩니다.

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

기본 템플릿 및 ACL 예

이 명령을 사용하려면 라우터와 통신할 수 있어야 하는 트래픽을 식별하는 액세스 목록을 정의해야 합니다.액세스 목록에는 라우팅 프로토콜과 관리 트래픽(BGP[Border Gateway Protocol], OSPF[Open Shortest Path First], SNMP, SSH, Telnet)이 모두 포함되어야 합니다. 자세한 내용은 구축 지침에 대한 섹션을 참조하십시오.

다음 샘플 ACL은 간단한 개요를 제공하고 특정 용도에 맞게 조정할 수 있는 몇 가지 컨피그레이션 예를 제공합니다.ACL은 일반적으로 필요한 여러 서비스/프로토콜에 필요한 컨피그레이션을 보여줍니다.SSH, 텔넷 및 SNMP의 경우 루프백 주소가 대상으로 사용됩니다.라우팅 프로토콜의 경우 실제 인터페이스 주소가 사용됩니다.rACL에서 사용할 라우터 인터페이스 선택은 로컬 사이트 정책 및 작업에 따라 결정됩니다.예를 들어 모든 BGP 피어링 세션에 looback을 사용하는 경우 BGP에 대한 **permit** 문에서 해당 루프백만 허용해야 합니다.

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

모든 Cisco ACL과 마찬가지로 액세스 목록 끝에 암시적 **거부** 문이 있으므로 ACL의 항목과 일치하지 않는 모든 트래픽은 거부됩니다.

참고: log 키워드는 허용되지 않는 GRP로 향하는 트래픽을 분류하는 데 사용할 수 있습니다.log 키워드는 ACL 적중 세부사항에 대한 중요한 정보를 제공하지만 이 키워드를 사용하는 ACL 항목에 대한 과도한 적중 수는 LC CPU 사용률을 높입니다.로깅과 관련된 성능 영향은 LC 엔진 유형에 따라 달라집니다.일반적으로 로깅은 엔진 0/1/2에 필요한 경우에만 사용해야 합니다. 엔진 3/4/4+의 경우

, 로깅은 CPU 성능 및 멀티큐 아키텍처의 증가로 인해 큰 영향을 미치지 않습니다.

이 액세스 목록의 세분성 수준은 로컬 보안 정책(예: OSPF 네이버에 필요한 필터링 레벨)에 따라 결정됩니다.

ACLS 및 단편화된 패킷

ACL에는 **fragments** 키워드가 있으며, 이 키워드는 특화된 프래그먼트 패킷 처리 동작을 활성화합니다.일반적으로 ACL의 L3 문(L4 정보와 상관없음)과 일치하는 비초기 프래그먼트는 일치하는 항목의 **permit** 또는 **deny 문**의 영향을 받습니다.**fragments** 키워드를 사용하면 ACL이 더 세분화된 비초기 프래그먼트를 거부하거나 허용하도록 할 수 있습니다.

rACL 컨텍스트에서 필터링 프래그먼트는 초기가 아닌 프래그먼트만 사용하는 DoS 공격에 대한 추가 보호 레이어를 추가합니다(예: FO > 0). rACL의 시작 부분에 초기가 아닌 프래그먼트에 대한 deny 문을 사용하면 모든 초기가 아닌 프래그먼트가 라우터에 액세스하는 것을 거부합니다.드문 경우지만, 유효한 세션은 프래그먼트화가 필요할 수 있으므로 **deny fragment** 문이 rACL에 있는 경우 필터링됩니다.

예를 들어, 아래에 표시된 부분 ACL을 고려하십시오.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

이러한 엔트리를 rACL의 시작 부분에 추가하면 GRP에 대한 비초기 프래그먼트 액세스가 거부되며, 조각화되지 않은 패킷 또는 초기 프래그먼트는 **deny fragment** 문의 영향을 받지 않는 rACL의 다음 행으로 전달됩니다.위의 rACL 코드 조각은 또한 각 프로토콜(UDP(Universal Datagram Protocol), TCP 및 ICMP)이 ACL에서 별도의 카운터를 증가하므로 공격의 분류를 용이하게 합니다.

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

위험 평가

rACL이 라우팅 프로토콜 또는 라우터에 대한 대화형 액세스와 같은 중요 트래픽을 필터링하지 않도록 합니다.필요한 트래픽을 필터링하면 라우터에 원격으로 액세스할 수 없으므로 콘솔 연결이 필요할 수 있습니다.따라서 랩 컨피그레이션은 가능한 한 실제 구축을 모방해야 합니다.

Cisco는 구축 전에 Lab에서 이 기능을 테스트하는 것이 좋습니다.

부록 및 메모

수신 인접성 및 펀티드 패킷

이 문서의 앞부분에서 설명한 대로 일부 패킷에는 GRP 처리가 필요합니다.패킷은 데이터 전달 평면에서 GRP로 펀딩됩니다.GRP 액세스가 필요한 레이어 3 데이터의 일반적인 형식 목록입니다.

- 라우팅 프로토콜
- 멀티캐스트 제어 트래픽(OSPF, HSRP[Hot Standby Router Protocol], TDP[Tag Distribution

Protocol], PIM[Protocol Independent Multicast] 등)
- 프래그먼트화가 필요한 MPLS(Multiprotocol Label Switching) 패킷
- 라우터 알림과 같은 특정 IP 옵션이 있는 패킷
- 멀티캐스트 스트림의 첫 번째 패킷
- 리어셈블리가 필요한 조각화된 ICMP 패킷
- 라우터 자체로 향하는 모든 트래픽(LC에서 처리되는 트래픽 제외)

rACL은 수신 인접성에 적용되므로 rACL은 GRP에 펀딩되지 않지만 수신 인접성인 일부 트래픽을 필터링합니다.가장 일반적인 예는 ICMP 에코 요청(ping)입니다.라우터로 전달되는 ICMP 에코 요청은 LC CPU에서 처리됩니다.요청은 인접성을 수신하므로 rACL에 의해 필터링됩니다.따라서 라우터의 인터페이스(또는 루프백)에 대한 ping을 허용하려면 rACL에서 에코 요청을 명시적으로 허용해야 합니다.

수신 인접성은 **show ip cef** 명령을 사용하여 볼 수 있습니다.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

구축 지침

Cisco는 보수적인 구축 사례를 권장합니다.rACL을 성공적으로 구축하려면 기존 제어 및 관리 플레인 액세스 요구 사항을 잘 이해해야 합니다.일부 네트워크에서는 필터링 목록을 작성하는 데 필요한 정확한 트래픽 프로필을 결정하는 것이 어려울 수 있습니다.다음 지침에서는 반복적인 rACL 구성을 사용하여 트래픽을 식별하고 필터링하는 매우 보수적인 접근 방식을 설명합니다.

1. **분류 ACL을 사용하여 네트워크에서 사용되는 프로토콜을 식별합니다.**GRP에 액세스하는 알려진 모든 프로토콜을 허용하는 rACL을 구축합니다.이 "검색" rACL에는 소스 주소와 대상 주소가 모두 **any**로 설정되어 있어야 합니다.로깅은 프로토콜 **허용** 문과 일치하는 소스 주소 목록을 개발하는 데 사용할 수 있습니다.프로토콜 **permit** 문 외에도 **rACL**의 끝에 있는 모든 **허용** 로그 라인을 사용하여 rACL에 의해 필터링되고 GRP에 대한 액세스가 필요할 수 있는 다른 프로토콜을 식별할 수 있습니다.목표는 특정 네트워크에서 사용하는 프로토콜을 결정하는 것입니다.로깅은 분석에서 라우터와 통신할 수 있는 "기타"를 확인하는 데 사용해야 합니다.**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.트래픽을 분류하는 데 필요한 경우에만 짧은 시간 동안 log 키워드를 사용합니다.
2. **식별된 패킷을 검토하고 GRP에 대한 액세스를 필터링하기 시작합니다.**1단계에서 rACL에 의해 필터링된 패킷이 식별되고 검토되면 허용되는 프로토콜에 대한 **any** 문을 **허용하여** rACL을 구축합니다.1단계에서와 마찬가지로 **log** 키워드는 **허용** 항목과 일치하는 패킷에 대한 자세한 정보를 제공할 수 있습니다.마지막에 **모든 로그**를 거부하면 GRP로 이동할 예기치 않은 패킷을 식별하는 데 도움이 됩니다.이 rACL은 기본 보호를 제공하며 네트워크 엔지니어가 필요한 모든 트래픽이 허용되도록 합니다.IP 소스 및 대상 주소의 명시적 범위를 갖지 않고 라우터와 통신해야 하는 프로토콜 범위를 테스트하는 것이 목적입니다.
3. **소스 주소의 매크로 범위를 제한합니다.**할당된 CIDR(Classless Interdomain Routing) 블록의 전체 범위만 소스 주소로 허용하면 됩니다.예를 들어 네트워크에 171.68.0.0/16을 할당받은 경우 171.68.0.0/16의 소스 주소를 허용합니다.이 단계는 서비스를 중단하지 않고 위험을 줄입니

다.또한 CIDR 블록 외부에서 장비에 액세스할 수 있는 디바이스/사용자의 데이터 포인트를 제공합니다.모든 외부 주소가 삭제됩니다.세션에 대해 허용된 소스 주소가 CIDR 블록 외부에 있기 때문에 외부 BGP 피어에는 예외가 필요합니다.이 단계는 몇 일 동안 유지되어 rACL을 좁히는 다음 단계에 대한 데이터를 수집할 수 있습니다.

4. **알려진 인증된 소스 주소만 허용하도록 rACL 허용 문을 좁힙니다.**소스 주소를 GRP와 통신하는 소스만 허용하도록 점점 더 제한합니다.
5. **rACL에서 대상 주소를 제한합니다(*선택 사항*).**일부 인터넷 서비스 공급자(ISP)는 특정 프로토콜만 라우터의 특정 대상 주소를 사용하도록 선택할 수 있습니다.이 마지막 단계는 프로토콜에 대한 트래픽을 허용할 대상 주소의 범위를 제한하는 것입니다.[6]

구축 예

아래 예는 다음 주소 지정을 기반으로 라우터를 보호하는 수신 ACL을 보여줍니다.

- ISP의 주소 블록은 169.223.0.0/16입니다.
- ISP의 인프라 블록은 169.223.252.0/22입니다.
- 라우터에 대한 루프백은 169.223.253.1/32입니다.
- 라우터는 코어 백본 라우터이므로 내부 BGP 세션만 활성화됩니다.

이 정보가 제공되면 초기 수신 ACL은 아래 예와 같은 것일 수 있습니다.인프라 주소 블록을 알고 있으므로 먼저 전체 블록을 허용합니다.나중에 라우터에 액세스해야 하는 모든 디바이스에 대해 특정 주소를 가져오면 ACE(Access Control Entry)가 더 자세히 추가됩니다.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !--- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Explicit Permit !--- Permit only applications whose destination address !--- is the loopback and whose source addresses !--- come from an valid host.

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

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp ! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !--- Permit designated router multicast address, if needed. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any 169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !--- Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp 169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 - Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
```

```
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example - Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

참고

1. DoS의 내성을 높이기 위한 SPD(Selective Packet Discard) SPD 및 보류 대기열 지침 이해를 참조하십시오.
2. Cisco Express Forwarding 및 인접성에 대한 자세한 내용은 Cisco Express Forwarding Overview를 참조하십시오.
3. ACL 구축 지침 및 관련 명령에 대한 자세한 내용은 Cisco 12000 Series 인터넷 라우터에서 ACL 구현을 참조하십시오.
4. 이는 Vanilla, BGPPA(Border Gateway Protocol Policy Accounting), PIRC(Per Interface Rate Control) 및 FRTP(Frame Relay Traffic Policing) 번들을 의미합니다.
5. 수신 경로 보호의 II 단계에서는 관리 인터페이스를 생성할 수 있으며, 수신 패킷을 수신할 IP 주소를 자동으로 제한합니다.

관련 정보

- 액세스 목록 지원 페이지
- Technical Support - Cisco Systems