Cisco IOS 디바이스를 강화하는 Cisco 가이드

TAC **문서 ID: 13608**

작성자: Shashank Singh, Cisco TAC 엔지니어

2016년 1월 6일

목차

- vty 및 tty 라인 제어
- vty 및 tty 라인의 전송 제어
- 경고 배너

인증, 권한 부여 및 계정 관리(AAA)
- TACACS+ 인증
- 인증 폴백
- 유형 7 비밀번호 사용
- TACACS+ 명령어 권한 부여
- TACACS+ 명령어 계정 관리
- 이중화된 AAA 서버

SNMP(Simple Network Management Protocol) 강화
- SNMP 커뮤니티 문자열
- ACL과 SNMP 커뮤니티 문자열
- 인프라 ACL
- SNMP 보기
- SNMP 버전 3
- 관리 플레인 보호

로깅 모범 사례
- 중앙 위치에 로그 보내기
- 로깅 레벨:
- 콘솔 또는 모니터 세션에 기록하지 않음
- 버퍼링된 로깅 사용
- 로깅 소스 인터페이스 구성
- 로깅 타임스탬프 구성

Cisco IOS Software 컨피그레이션 관리
- 컨피그레이션 교체 및 컨피그레이션 롤백
- 전용 컨피그레이션 변경 액세스
- Cisco IOS Software 복원력 컨피그레이션
- 디지털 서명 Cisco 소프트웨어
- 컨피그레이션 변경 알림 및 로깅

컨트롤 플레인

일반 컨트롤 플레인 강화
- IP ICMP 리디렉션
- ICMP 연결 불가능
- 프록시 ARP

컨트롤 플레인 트래픽의 CPU 영향 제한
- 컨트롤 플레인 트래픽 이해
- 인프라 ACL
- 수신 ACL
- 컨트롤 플레인 정책
- 컨트롤 플레인 보호
- 하드웨어 레이트 리미터

보안 BGP
- TTL 기반 보안 보호
- MD5로 BGP 피어 인증
- 최대 접두사 구성
- 접두사 목록으로 BGP 접두사 필터링
- 자동 시스템 경로 액세스 목록으로 BGP 접두사 필터링

보안 내부 게이트웨이 프로토콜
- Message Digest 5로 라우팅 프로토콜 인증 및 검증
- Passive-Interface 명령어

소개

이 문서에는 Cisco IOS® 시스템 디바이스를 보호하는 데 도움이 되는 정보가 포함되어 있어, 전체적인 네트워크 보안을 강화합니다. 네트워크 디바이스 기능을 분류할 수 있는 세 가지 플레인을 중심으로 구성된 이 문서에서는 포함된 각 기능의 개요를 제공하고 관련 문서를 참조합니다.

네트워크의 세 가지 기능 플레인인 관리 플레인, 컨트롤 플레인 및 데이터 플레인에서는 각각 보호해야 하는 서로 다른 기능을 제공합니다.

- **관리 플레인** - 관리 플레인에서는 Cisco IOS 디바이스에 전송된 트래픽을 관리하고, SSH(Secure Shell) 및 SNMP(Simple Network Management Protocol) 등의 프로토콜과 애플리케이션으로 구성됩니다.
- **컨트롤 플레인** - 네트워크 디바이스의 컨트롤 플레인에서는 네트워크 인프라의 기능을 유지관리하는 데 매우 중요한 트래픽을 처리합니다. 컨트롤 플레인은 EIGRP(Enhanced Interior Gateway Routing Protocol) 및 OSPF(Open Shortest Path First) 등의 IGP(Interior Gateway Protocols) 외에도 BGP(Border Gateway Protocol)를 포함하는 네트워크 디바이스 사이의 프로토콜과 애플리케이션으로 구성됩니다.
- **데이터 플레인** - 데이터 플레인에서는 네트워크 디바이스를 통해 데이터를 전달합니다. 데이터 플레인에는 로컬 Cisco IOS 디바이스로 전송되는 트래픽이 포함되지 않습니다.

이 문서에 포함된 보안 기능 범위에서는 기능을 구성하는 데 충분한 세부 정보를 제공하는 경우가 많습니다. 그러나 그렇지 못한 경우 기능에 각별히 주의를 기울여야 하는지 사용자가 평가할 수 있도록 기능이 설명되어 있습니다. 가능하고 적절한 경우 이 문서에는 구현되면 네트워크를 보호하는 데 도움이 되는 권장 사항이 포함되어 있습니다.

사전 요구 사항

요건

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.

보안 운영

보안 네트워크 운영은 중요한 주제입니다. 이 문서의 대부분은 Cisco IOS 디바이스의 보안 컨피그레이션에 관한 내용이지만, 컨피그레이션 자체만으로 네트워크가 완전히 보호되지는 않습니다. 네트워크에서 사용 중인 운영 절차가 기본 디바이스 컨피그레이션에 못지 않게 보안에 중요합니다.

이러한 주제에는 구현 시 권고하는 운영 권장 사항이 포함되어 있습니다. 이러한 주제에서는 중요한 특정 네트워크 운영 영역을 강조하여 설명하지만 포괄적이지는 않습니다.

Cisco 보안 권고 및 대응 모니터링

Cisco PSIRT(Product Security Incident Response Team)에서는 Cisco 제품의 보안 관련 문제에 관한 간행물을 작성하고 유지관리합니다. 이 간행물은 일반적으로 PSIRT Advisories라고 합니다. 덜 심각한 문제의 커뮤니케이션에 사용되는 방법이 Cisco Security Response입니다. 보안 권고 및 대응에 관한 내용은 http://www.cisco.com/go/psirt에서 찾아볼 수 있습니다.

이 커뮤니케이션 수단에 대한 자세한 정보는 Cisco Security Vulnerability Policy에서 찾아볼 수 있습니다.

보안 네트워크를 유지 보수하려면 공개된 Cisco 보안 권고 및 대응을 알아야 합니다. 취약점에 대한 지식이 있어야 네트워크에 발생할 수 있는 위협을 평가할 수 있습니다. 이 평가 프로세스를 지원하는 Risk Triage for Security Vulnerability Announcements를 참조하십시오.

인증, 권한 부여 및 계정 관리(AAA) 활용

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스 보안에 중요합니다. AAA 프레임워크는 관리 세션에 대한 인증을 제공하며, 사용자가 특정 관리자 정의 명령어만 사용하도록 제한하고, 모든 사용자가 입력한 모든 명령어를 기록할 수도 있습니다. AAA 활용 방법에 대한 자세한 내용은 이 문서의 인증, 권한 부여 및 계정 관리 섹션을 참조하십시오.

로그 수집 및 모니터링 중앙 집중화

보안 사고와 관련된 기존 이벤트, 새로운 이벤트 및 이력 이벤트에 대한 지식을 얻으려면 조직에 이벤트 로깅 및 상관관계에 관한 통합 전략이 있어야 합니다. 이 전략에서는 모든 네트워크 디바이스의 로깅을 활용하고 사전 패키지된 맞춤형 상관관계 기능을 사용해야 합니다.

중앙 집중식 로깅을 구현한 후에는 분석과 사고 추적을 기록하는 구조화된 접근 방식을 개발해야 합니다. 조직의 요구 사항에 따라 이 접근 방식은 간단한 로그 데이터 검토부터 고급 규칙 기반 분석까지 다양합니다.

Cisco IOS 네트워크 디바이스에서 로깅을 구현하는 방법에 대한 자세한 내용은 이 문서의 로깅 모범 사례 섹션을 참조하십시오.

가능한 경우 보안 프로토콜 사용

민감한 네트워크 관리 데이터를 전달하기 위해 수많은 프로토콜이 사용됩니다. 가능한 경우 항상 보안 프로토콜을 사용해야 합니다. 인증 데이터와 관리 정보를 모두 암호화하기 위해 텔넷 대신 SSH를 사용하도록 보안 프로토콜을 선택할 수 있습니다. 또한 컨피그레이션 데이터를 복사할 때 보안 파일 전송 프로토콜을 사용해야 합니다. 예를 들어, FTP 또는 TFTP 대신 SCP(Secure Copy Protocol)를 사용합니다.

Cisco IOS 디바이스의 보안 관리에 대한 자세한 내용은 이 문서의 보안 인터랙티브 관리 세션 섹션을 참조하십시오.

NetFlow로 트래픽 가시성 확보

NetFlow를 사용하면 네트워크의 트래픽 흐름을 모니터링할 수 있습니다. 원래 네트워크 관리 애플리케이션에 트래픽 정보를 내보내는 데 사용하는 NetFlow는 라우터에 플로우 정보를 표시하는 데도 사용할 수 있습니다. 이 기능을 사용하면 어떤 트래픽이 실시간으로 네트워크를 이동하는지 볼 수 있습니다. 플로우 정보를 원격 컬렉터에 내보내는지 여부에 상관없이, 필요한 경우 사후 대응식으로 사용할 수 있도록 NetFlow에 대해 네트워크 디바이스를 구성하는 것이 좋습니다.

이 기능에 대한 자세한 내용은 이 문서 및 http://www.cisco.com/go/netflow(등록된 고객만 해당)의 트래픽 식별 및 역추적 섹션에서 찾아볼 수 있습니다.

컨피그레이션 관리

컨피그레이션 관리는 컨피그레이션 변경을 제안, 검토, 승인 및 구축하는 프로세스입니다. Cisco IOS 디바이스 컨피그레이션 상황에서 두 가지 컨피그레이션 관리 측면인 컨피그레이션 아카이브와 보안이 중요합니다.

컨피그레이션 아카이브를 사용하여 네트워크 디바이스의 변경 사항을 롤백할 수 있습니다. 보안 상황에서, 변경된 보안 사항과 변경 시기를 판별하기 위해 컨피그레이션 아카이브를 사용할 수도 있습니다. AAA 로그 데이터와 함께 이 정보를 사용하면 네트워크 디바이스의 보안 감사에 도움이 될 수 있습니다.

Cisco IOS 디바이스의 컨피그레이션에는 여러 민감한 세부 정보가 포함되어 있습니다. 사용자 이름, 비밀번호 및 액세스 제어 목록의 콘텐츠는 이 정보 유형의 예입니다. Cisco IOS 디바이스 컨피그레이션을 아카이브에 보관하는 데 사용하는 저장소는 안전해야 합니다. 이 정보에 대한 액세스가 안전하지 않으면 전체 네트워크의 보안이 저해될 수 있습니다.

관리 플레인

관리 플레인은 네트워크의 관리 목표를 달성하는 기능으로 구성됩니다. 이 기능에는 SNMP 또는 NetFlow를 사용한 통계 수집 외에도 SSH를 사용하는 인터랙티브 관리 세션이 포함됩니다. 네트워크 디바이스의 보안을 고려할 때 관리 플레인을 보호하는 것이 중요합니다. 보안 사고로 인해 관리 플레인의 기능이 저하될 수 있는 경우 네트워크를 복구하거나 안정화할 수 없습니다.

이 문서의 이러한 섹션에서는 Cisco IOS Software에서 사용 가능하며 관리 플레인을 강화하는 데 도움이 되는 보안 기능과 컨피그레이션에 대해 자세히 설명합니다.

일반 관리 플레인 강화

관리 플레인은 디바이스가 구축된 네트워크와 해당 운영을 모니터링할 뿐만 아니라 디바이스에 액세스하고 디바이스를 구성 및 관리하는 데 사용됩니다. 관리 플레인은 이러한 기능의 운영을 위해 트래픽을 수신하고 전송하는 플레인입니다. 컨트롤 플레인의 운영이 관리 플레인의 운영에 직접적인 영향을 미치므로 디바이스의 관리 플레인과 제어 플레인을 모두 보호해야 합니다. 관리 플레인에서 사용하는 프로토콜 목록은 다음과 같습니다.

- Simple Network Management Protocol
- 텔넷
- SSH(Secure Shell) 프로토콜
- FTP(File Transfer Protocol)
- TFTP(Trivial File Transfer Protocol)
- SCP(Secure Copy) 프로토콜
- TACACS+
- RADIUS
- NetFlow
- NTP(Network Time Protocol)
- Syslog

보안 사고 중에 관리 플레인과 컨트롤 플레인이 존속될 수 있도록 하는 단계를 수행해야 합니다. 이러한 플레인 중 하나가 공격을 받으면 모든 플레인에 보안 침해가 일어날 수 있습니다.

비밀번호 관리

비밀번호는 리소스 또는 디바이스에 대한 액세스를 제어합니다. 이 작업은 요청을 인증하기 위해 사용하는 비밀번호 또는 암호를 정의하여 수행합니다. 리소스 또는 디바이스에 대한 액세스 요청을 수신하면 비밀번호와 ID를 확인하기 위해 요청을 검사하고, 결과에 따라 액세스 권한을 부여, 거부 또는 제한할 수 있습니다. 모범 사례에 따라 비밀번호는 TACACS+ 또는 RADIUS 인증 서버로 관리되어야 합니다. 그러나 TACACS+ 또는 RADIUS 서비스가 실패하는 경우에는 권한 부여된 액세스를 위해 로컬에서 구성된 비밀번호가 여전히 필요합니다. 디바이스에는 NTP 키, SNMP 커뮤니티 문자열 또는 라우팅 프로토콜 키와 같이 컨피그레이션에 있는 기타 비밀번호 정보도 있을 수 있습니다.

Cisco IOS 시스템에 대해 권한이 부여된 관리 액세스 권한을 부여하는 비밀번호를 설정하기 위해 **enable secret** 명령어를 사용합니다. 이전의 **enable password** 명령어가 아니라 **enable secret** 명령어를 사용해야 합니다. **enable password** 명령어에서는 취약한 암호화 알고리즘을 사용합니다.

enable secret이 설정되지 않고 콘솔 tty 라인에 맞게 비밀번호가 구성된 경우 콘솔 비밀번호를 사용하여 원격 vty(virtual tty) 세션에서도 권한이 부여된 액세스를 수신할 수 있습니다. 이 작업은 거의 필요하지 않으므로, enable secret을 구성해야 하는 또 다른 이유가 됩니다.

service password-encryption 전역 환경 설정 명령어는 비밀번호, CHAP(Challenge Handshake Authentication Protocol) 암호 및 컨피그레이션 파일에 저장된 비슷한 데이터를 암호화하도록 Cisco IOS Software에 지시합니다. 이러한 암호화는 관찰자가 우연히 관리자 검열을 통해 화면을 볼 때 비밀번호를 읽지 못하게 하는 데 유용합니다. 그러나 **service password-encryption** 명령어에서 사용하는 알고리즘은 간단한 Vigen re 암호입니다. 알고리즘은 다소 정교한 공격자가 신중하게 수행하는 분석으로부터 컨피그레이션 파일을 보호하도록 설계되지 않았으므로 이 용도로 사용하지 않아야 합니다. 암호화된 비밀번호를 포함하는 Cisco IOS 컨피그레이션 파일은 동일한 비밀번호로 구성된 일반 텍스트 목록과 동일하게 주의를 기울여 취급해야 합니다.

이 취약한 암호화 알고리즘은 **enable secret** 명령어에서는 사용되지 않지만, **password** 라인 환경 설정 명령어와 **enable password** 전역 환경 설정 명령어에서는 사용됩니다. 이 유형의 비밀번호는 제거해야 하며, **enable secret** 명령어 또는 향상된 비밀번호 보안(Enhanced Password Security) 기능을 사용해야 합니다.

enable secret 명령어와 향상된 비밀번호 보안 기능에서는 비밀번호 해싱에 MD5(Message Digest 5)를 사용합니다. 이 알고리즘은 공개적으로 상당히 많이 검토되었으며, 원상태로 되돌릴 수 있다고 알려져 있지는 않습니다. 그러나 이 알고리즘은 사전 공격(dictionary attack)을 받을 수 있습니다. 사전 공격에서는 공격자가 사전에 있는 모든 단어 또는 다른 가능한 비밀번호 목록에서 일치하는 사항을 찾으려고 시도합니다. 따라서 컨피그레이션 파일은 안전하게 저장하고 신뢰할 수 있는 개인과만 공유해야 합니다.

향상된 비밀번호 보안

Cisco IOS Software Release 12.2(8)T에 소개된 향상된 비밀번호 보안(Enhanced Password Security) 기능을 사용하면 관리자가 **username** 명령어에 맞게 비밀번호의 MD5 해싱을 구성할 수 있습니다. 이 기능 이전에는 두 가지 유형의 비밀번호가 있었습니다. 즉, 일반 텍스트 비밀번호인 유형 0과 Vigen re 암호의 알고리즘을 사용하는 유형 7입니다. 향상된 비밀번호 보안 기능은 CHAP와 같이 일반 텍스트 비밀번호를 검색해야 하는 프로토콜과 함께 사용할 수 없습니다.

MD5 해싱을 사용하여 사용자 비밀번호를 암호화하려면 **username secret** 전역 환경 설정 명령어를 실행하십시오.

```
!
username <name> secret <password>
!
```

이 기능에 대한 자세한 내용은 향상된 비밀번호 보안을 참조하십시오.

로그인 비밀번호 재시도 잠금

Cisco IOS Software Release 12.3(14)T에 추가된 로그인 비밀번호 재시도 잠금(Login Password Retry Lockout) 기능을 사용하면 실패한 로그인 시도 구성 횟수에 도달한 후에 로컬 사용자 계정을 잠글 수 있습니다. 사용자가 잠기고 나면 잠금을 해제할 때까지 해당 계정이 잠깁니다. 권한 레벨이 15로 구성되어 있는 권한이 부여된 사용자는 이 기능으로 잠글 수 없습니다. 권한 레벨이 15인 사용자 수는 최소로 유지해야 합니다.

실패한 로그인 시도 횟수에 도달하면 권한이 부여된 사용자가 디바이스를 사용하지 못하도록 잠글 수 있습니다. 또한 악의적인 사용자가 유효한 사용자 이름을 사용하여 반복적으로 인증을 시도하는 DoS(Denial of Service) 조건을 만들 수 있습니다.

다음 예에서는 로그인 비밀번호 재시도 잠금 기능을 사용하는 방법을 보여줍니다.

```
!
aaa new-model
aaa local authentication attempts max-fail <max-attempts>
aaa authentication login default local
!
username <name> secret <password>
!
```

이 기능은 CHAP 및 PAP(Password Authentication Protocol) 등의 인증 방법에도 적용됩니다.

서비스 비밀번호 복구 안 함

Cisco IOS Software Release 12.3(14)T 이상에서는 서비스 비밀번호 복구 안 함(No Service Password-Recovery) 기능을 통해 콘솔 액세스 권한이 있는 사용자가 디바이스 컨피그레이션에 비보안 상태로 액세스하여 비밀번호를 지울 수 없게 합니다. 또한 악의적인 사용자가 컨피그레이션 등록 값을 변경하고 NVRAM에 액세스하지 못하게 합니다.

```
!
no service password-recovery
!
```

Cisco IOS Software에서는 시스템 시작 중에 Break 키를 사용하여 ROMMON(ROM Monitor Mode)에 액세스해야 하는 비밀번호 복구 절차를 제공합니다. ROMMON에서 새 비밀번호를 포함하는 새로운 시스템 컨피그레이션을 표시하기 위해 디바이스 소프트웨어를 다시 로드할 수 있습니다.

현재 비밀번호 복구 절차를 사용하면 콘솔 액세스 권한이 있는 모든 사용자가 디바이스와 해당 네트워크에 액세스할 수 있습니다. 서비스 비밀번호 복구 안 함 기능을 사용하면 시스템 시작 중에 ROMMON 입력 및 Break 키 시퀀스 완료를 방지합니다.

디바이스에서 **서비스 비밀번호 복구 안 함**을 사용하도록 설정하는 경우, 디바이스 컨피그레이션의 오프라인 사본을 저장하고 컨피그레이션 아카이브 솔루션을 구현하는 것이 좋습니다. 이 기능을 사용하도록 설정한 다음 Cisco IOS 디바이스의 비밀번호를 복구해야 하는 경우 전체 컨피그레이션이 삭제됩니다.

이 기능에 대한 자세한 내용은 보안 ROMMON 컨피그레이션 예를 참조하십시오.

사용하지 않는 서비스 비활성화

모범 사례에 따라 불필요한 서비스는 비활성화해야 합니다. 특히 UDP(User Datagram Protocol)를 사용하는 불필요한 서비스는 합법적인 용도로는 자주 사용되지 않지만, DoS나 기타 공격을 시작하는 데 사용할 수 있습니다. 이러한 공격은 패킷 필터링으로 방지합니다.

TCP 및 UDP 소규모 서비스는 비활성화해야 합니다. 이러한 서비스에는 다음이 포함됩니다.

- echo(포트 번호 7)
- discard(포트 번호 9)
- daytime(포트 번호 13)
- chargen(포트 번호 19)

소규모 서비스의 남용은 스푸핑 차단 액세스 목록을 사용하여 방지하거나 위험 정도를 줄일 수 있지만, 네트워크에서 액세스 가능한 모든 디바이스에서 해당 서비스를 비활성화해야 합니다. Cisco IOS Software Release 12.0 이상에서는 기본적으로 소규모 서비스가 비활성화됩니다. 이전 소프트웨어에서는 **no service tcp-small-servers** 및 **no service udp-small-servers** 전역 환경 설정 명령어를 실행하여 해당 서비스를 비활성화할 수 있습니다.

다음은 사용 중이지 않은 경우 비활성화해야 하는 추가 서비스 목록입니다.

- Finger 서비스를 비활성화하려면 **no ip finger** 전역 환경 설정 명령어를 실행합니다. 12.1(5) 및 12.1(5)T 이상의 Cisco IOS Software Release에서는 기본적으로 이 서비스를 비활성화합니다.
- BOOTP(Bootstrap Protocol)를 비활성화하려면 **no ip bootp server** 전역 환경 설정 명령어를 실행합니다.
- Cisco IOS Software Release 12.2(8)T 이상에서 BOOTP를 비활성화하려면 전역 환경 설정 모드에서 **ip dhcp bootp ignore** 명령어를 실행합니다. 그러면 DHCP(Dynamic Host Configuration Protocol) 서비스가 활성화된 상태로 남게 됩니다.
- DHCP 릴레이 서비스가 필요하지 않은 경우 DHCP 서비스를 비활성화할 수 있습니다. 전역 환경 설정 모드에서 **no service dhcp** 명령어를 실행합니다.
- MOP(Maintenance Operation Protocol) 서비스를 비활성화하려면 인터페이스 환경 설정 모드에서 **no mop enabled** 명령어를 실행합니다.
- DNS(Domain Name System) 변환(resolution) 서비스를 비활성화하려면 **no ip domain-lookup** 전역 환경 설정 명령어를 실행합니다.
- X.25 네트워크에 사용되는 PAD(Packet Assembler/Disassembler) 서비스를 비활성화하려면 전역 환경 설정 모드에서 **no service pad** 명령어를 실행합니다.
- HTTP 서버는 전역 환경 설정 모드에서 **no ip http server** 명령어를 사용하여 비활성화할 수 있으며, HTTPS(Secure HTTP) 서버는 **no ip http secure-server** 전역 환경 설정 명령어를 사용하여 비활성화할 수 있습니다.
- Cisco IOS 디바이스가 시작 중에 네트워크에서 컨피그레이션을 검색하지 않는 경우 **no service config** 전역 환경 설정 명령어를 사용해야 합니다. 그러면 Cisco IOS 디바이스가 TFTP를 사용하는 네트워크에서 컨피그레이션 파일을 찾으려고 시도하지 않습니다.
- CDP(Cisco Discovery Protocol)는 네이버 인접성 및 네트워크 토폴로지를 위해 기타 CDP 지원 디바이스를 검색하는 데 사용되는 네트워크 프로토콜입니다. CDP는 NMS(Network Management Systems)에서 사용하거나 트러블슈팅 중에 사용할 수 있습니다. CDP는 신뢰할 수 없는 네트워크에 연결된 모든 인터페이스에서 비활성화되어야 합니다. 이 작업은 **no cdp enable** 인터페이스 명령어를 사용하여 수행합니다. 또는 **no cdp run** 전역 환경 설정 명령어를 사용하여 전역적으로 CDP를 비활성화할 수 있습니다. CDP는 악의적인 사용자가 네트워크 매핑 및 정찰에 사용할 수 있습니다.
- LLDP(Link Layer Discovery Protocol)는 802.1AB에 정의된 IEEE 프로토콜입니다. LLDP는 CDP와 비슷합니다. 그러나 이 프로토콜은 CDP를 지원하지 않는 기타 디바이스 사이의 상호운용성을 허용합니다. LLDP는 CDP와 동일한 방식으로 취급해야 하며, 신뢰할 수 없는 네트워크에 연결하는 모든 인터페이스에서 비활성화해야 합니다. 이 작업을 수행하려면 **no lldp transmit** 및 **no lldp receive** 인터페이스 환경 설정 명령어를 실행합니다. LLDP를 전역적으로 비활성화하려면 **no lldp run** 전역 환경 설정 명령어를 실행합니다. LLDP도 악의적인 사용자가 네트워크 매핑 및 정찰에 사용할 수 있습니다.

EXEC 시간 초과

EXEC 명령어 해석기가 세션을 종료하기 전에 사용자가 입력할 때까지 기다리는 간격을 설정하려면 **exec-timeout** 라인 환경 설정 명령어를 실행합니다. 유휴 상태로 남아 있는 vty 또는 tty 라인에서 세션을 로그아웃하려면 **exec-timeout** 명령어를 사용해야 합니다. 기본적으로 10분 동안 아무 작업도 수행되지 않으면 세션의 연결이 끊깁니다.

```
!

line con 0
 exec-timeout <minutes> [seconds]
line vty 0 4
 exec-timeout <minutes> [seconds]
!
```

TCP 세션을 위한 Keepalives

service tcp-keepalives-in 및 **service tcp-keepalives-out** 전역 환경 설정 명령어를 사용하면 디바이스에서 TCP 세션에 대해 TCP keepalives를 전송할 수 있습니다. 이 컨피그레이션은 디바이스로 들어가는 인바운드 연결과 디바이스에서 나오는 아웃바운드 연결에서 TCP keepalives를 활성화하는 데 사용해야 합니다. 이렇게 하면 원격에 있는 연결 종단의 디바이스에 계속해서 액세스할 수 있으며 일부만 개방된 연결이나 격리된 연결이 로컬 Cisco IOS 디바이스에서 제거됩니다.

```
!

service tcp-keepalives-in
service tcp-keepalives-out
!
```

관리 인터페이스 사용

디바이스의 관리 플레인은 물리적 또는 논리적 관리 인터페이스의 대역 내(In-Band) 또는 대역 외(Out-of-Band)에서 액세스합니다. 네트워크 중단 중에 관리 플레인에 액세스할 수 있도록 각 네트워크 디바이스에 대역 내 및 대역 외 관리 액세스가 모두 존재하는 것이 이상적입니다.

디바이스에 대한 대역 내 액세스에 사용되는 가장 일반적인 인터페이스 중 하나는 논리 루프백 인터페이스입니다. 루프백 인터페이스는 항상 작동하는 반면 물리적 인터페이스는 상태를 변경할 수 있고, 인터페이스에 액세스하지 못할 수도 있습니다. 각 디바이스에 루프백 인터페이스를 관리 인터페이스로 추가하고 관리 플레인에만 사용하는 것이 좋습니다. 그러면 관리자가 관리 플레인을 위한 네트워크 전체에 정책을 적용할 수 있습니다. 디바이스에 루프백 인터페이스가 구성되면 트래픽을 받고 보내기 위해 SSH, SNMP 및 syslog와 같은 관리 플레인 프로토콜에서 해당 인터페이스를 사용할 수 있습니다.

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
```

메모리 임계값 알림

Cisco IOS Software Release 12.3(4)T에 추가된 메모리 임계값 알림(Memory Threshold Notification) 기능을 사용하면 디바이스에서 메모리 부족 상태를 줄일 수 있습니다. 이 기능에서는 이 작업을 수행하기 위해 메모리 임계값 알림 및 메모리 예약의 두 가지 방법을 사용합니다.

메모리 임계값 알림에서는 디바이스의 여유 메모리가 구성된 임계값보다 낮음을 나타내기 위해 로그 메시지를 생성합니다. 이 컨피그레이션 예에서는 **memory free low-watermark** 전역 환경 설정 명령어로 이 기능을 사용하도록 설정하는 방법을 보여줍니다. 사용 가능한 여유 메모리가 지정된 임계값보다 낮을 때 디바이스에서 알림을 생성하고, 사용 가능한 여유 메모리가 지정된 임계값보다 5% 높아지면 디바이스에서 다시 알림을 생성할 수 있습니다.

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

중요한 알림을 위해 충분한 메모리를 사용할 수 있도록 메모리 예약을 사용합니다. 이 컨피그레이션 예에서는 이 기능을 활성화하는 방법을 설명합니다. 이렇게 하면 디바이스의 메모리가 모두 소모되어도 관리 프로세스가 계속 작동합니다.

```
!
memory reserve critical <value>!
```

이 기능에 대한 자세한 내용은 메모리 임계값 알림을 참조하십시오.

CPU 임계값 알림

Cisco IOS Software Release 12.3(4)T에 도입된 CPU 임계값 알림(CPU Thresholding Notification) 기능을 사용하면 디바이스의 CPU 로드가 구성된 임계값을 초과하는 경우 이를 탐지하여 알림을 받을 수 있습니다. 임계값을 초과하면 디바이스에서 SNMP 트랩 메시지를 생성하여 보냅니다. Cisco IOS Software에서 임계값 증가 및 임계값 저하의 두 가지 CPU 사용률 임계값 방법이 지원됩니다.

이 예제 컨피그레이션에서는 CPU 임계값 알림 메시지를 트리거하는 임계값 증가 및 저하를 사용하도록 설정하는 방법을 보여줍니다.

```
!

snmp-server enable traps cpu threshold
!

snmp-server host <host-address> <community-string> cpu
!

process cpu threshold type <type> rising <percentage> interval <seconds>
     [falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

이 기능에 대한 자세한 내용은 CPU 임계값 알림을 참조하십시오.

콘솔 액세스용 메모리 예약

Cisco IOS Software Release 12.4(15)T 이상에서는 콘솔 액세스용 메모리 예약(Reserve Memory for Console Access) 기능을 사용하여 관리 및 트러블슈팅을 목적으로 Cisco IOS 디바이스에 대한 콘솔 액세스를 보장할 정도의 충분한 메모리를 예약할 수 있습니다. 이 기능은 디바이스의 메모리가 부족한 상태로 실행되는 경우에 특히 유용합니다. 이 기능을 활성화하기 위해 **memory reserve console** 전역 환경 설정 명령어를 실행할 수 있습니다. 이 예에서는 이러한 목적으로 4096KB를 예약하도록 Cisco IOS 디바이스를 구성합니다.

```
!
memory reserve console 4096
!
```

이 기능에 대한 자세한 내용은 콘솔 액세스용 메모리 예약을 참조하십시오.

메모리 누수 탐지기

Cisco IOS Software Release 12.3(8)T1에 도입된 메모리 누수 탐지기(Memory Leak Detector) 기능을 사용하면 디바이스의 메모리 누수를 탐지할 수 있습니다. 메모리 누수 탐지기를 통해 모든 메모리 풀, 패킷 버퍼 및 청크에서 누수를 찾을 수 있습니다. 메모리 누수는 유용하게 사용되지 않는 메모리의 정적 또는 동적 할당입니다. 이 기능은 동적인 메모리 할당에 중점을 둡니다. 메모리 누수가 있는지 탐지하기 위해 **show memory debug leaks** EXEC 명령어를 사용할 수 있습니다.

버퍼 오버플로: 레드 존 손상 탐지 및 정정

Cisco IOS Software Release 12.3(7)T 이상에서는 메모리 블록 오버플로를 탐지하여 정정하고 운영을 계속하기 위해 디바이스에서 버퍼 오버플로: 레드 존 손상 탐지 및 정정(Buffer Overflow: Detection and Correction of Redzone Corruption) 기능을 활성화할 수 있습니다.

이러한 전역 환경 설정 명령어를 사용하여 이 기능을 활성화할 수 있습니다. 구성한 후에는 버퍼 오버플로 탐지 및 정정 통계를 표시하기 위해 **show memory overflow** 명령어를 사용할 수 있습니다.

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

향상된 Crashinfo 파일 수집

향상된 Crashinfo 파일 수집(Enhanced Crashinfo File Collection) 기능은 오래된 crashinfo 파일을 자동으로 삭제합니다. Cisco IOS Software Release 12.3(11)T에 추가된 이 기능을 사용하면 디바이스 충돌 시 디바이스에서 새로운 crashinfo 파일을 생성하기 위한 공간을 재확보할 수 있습니다. 또한 이 기능을 통해 저장할 crashinfo 파일 수를 구성할 수 있습니다.

```
!
exception crashinfo maximum files <number-of-files>
!
```

Network Time Protocol

NTP(Network Time Protocol)가 특별히 위험한 서비스는 아니지만, 불필요한 모든 서비스는 공격 벡터를 나타낼 수 있습니다. NTP를 사용하는 경우 신뢰할 수 있는 시간 소스를 명시적으로 구성하고 적절한 인증을 사용하는 것이 중요합니다. 인증서에 의존하여 1단계 인증을 수행할 때 성공적으로 VPN을 연결하는 용도 외에 syslog 용도(예: 잠재적 공격의 포렌식 검사 중)로도 정확하고 신뢰할 수 있는 시간이 필요합니다.

- **NTP 시간대** - NTP를 구성할 때 타임스탬프가 정확하게 상관관계를 보여줄 수 있도록 시간대를 구성해야 합니다. 전역적으로 존재하는 네트워크에서 디바이스의 시간대를 구성하는 방법은 일반적으로 두 가지가 있습니다. 한 가지 방법은 이전에는 GMT(Greenwich Mean Time)라고 한 UTC(Coordinated Universal Time)로 모든 네트워크 디바이스를 구성하는 것입니다. 다른 방법은 로컬 시간대로 네트워크 디바이스를 구성하는 것입니다. 이 기능에 대한 자세한 내용은 Cisco 제품 문서의 "시계 시간대"에서 확인할 수 있습니다.

- **NTP 인증** - NTP 인증을 구성하면 신뢰할 수 있는 NTP 피어 간에 NTP 메시지를 확실히 교환할 수 있습니다.

NTP 인증을 사용하는 샘플 컨피그레이션
클라이언트:

(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5

서버:

(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5

인프라 ACL로 네트워크에 대한 액세스 제한

네트워크 디바이스와 무단으로 직접 통신하지 않도록 고안된 iACL(infrastructure Access Control List)은 네트워크에서 구현할 수 있는 가장 중요한 보안 제어 중 하나입니다. 인프라 ACL에서는 거의 모든 네트워크 트래픽이 네트워크를 통과하며 네트워크 자체가 대상이 되지 않는다는 개념을 활용합니다.

네트워크 디바이스에 허용해야 하는 네트워크 또는 호스트의 연결을 지정하기 위해 iACL을 구성하여 적용합니다. 일반적으로 이러한 연결 유형의 예는 eBGP, SSH 및 SNMP입니다. 필수 연결을 허용하고 나면 인프라로 향하는 기타 모든 트래픽이 명시적으로 거부됩니다. 네트워크를 통과하고 인프라 디바이스를 대상으로 하지 않는 모든 통과 트래픽은 명시적으로 허용됩니다.

iACL에서 제공하는 보호는 관리 플레인과 컨트롤 플레인 모두와 관련이 있습니다. iACL은 네트워크 인프라 디바이스의 개별 주소를 사용하면 더 쉽게 구현할 수 있습니다. IP 주소 지정이 보안에 미치는 영향에 대한 자세한 내용은 보안 중심 IP 주소 지정 방법을 참조하십시오.

이 예제 iACL 컨피그레이션에서는 iACL 구현 프로세스를 시작할 때 시작점으로 사용해야 하는 구조를 설명합니다.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit required connections for routing protocols and
!--- network management
!

 permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
 permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
 permit tcp host <trusted-management-stations> any eq 22
 permit udp host <trusted-netmgmt-servers> any eq 161
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

생성한 후에는 비인프라 디바이스를 향하는 모든 인터페이스에 iACL을 적용해야 합니다. 여기에는 다른 조직, 원격 액세스 세그먼트, 사용자 세그먼트 및 데이터 센터의 세그먼트에 연결하는 인터페이스가 포함됩니다.

인프라 ACL에 대한 자세한 내용은 코어 보호: 인프라 보호 액세스 제어 목록을 참조하십시오.

ICMP 패킷 필터링

ICMP(Internet Control Message Protocol)는 IP 제어 프로토콜로 설계되었습니다. 따라서 이 프로토콜이 전달하는 메시지는 일반적으로 TCP 및 IP 프로토콜에 광범위한 영향을 미칩니다. 네트워크 트러블슈팅 툴인 **ping**과 **traceroute**에서 ICMP를 사용하는 반면, 네트워크가 제대로 작동하는 경우에는 외부 ICMP 연결이 거의 필요하지 않습니다.

Cisco IOS Software에서는 이름 또는 유형과 코드별로 ICMP 메시지를 구체적으로 필터링하기 위한 기능을 제공합니다. 이전 예제에서 ACE(Access Control Entry)와 함께 사용되어야 하는 이 예제 ACL을 사용하면 신뢰할 수 있는 관리 스테이션 및 NMS 서버에서 Ping을 허용하고 기타 모든 ICMP 패킷을 차단할 수 있습니다.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!

 permit icmp host <trusted-management-stations> any echo
 permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!
```

```
 permit ip any any
!
```

IP 프래그먼트 필터링

프래그먼트화된 IP 패킷에 대한 필터링 프로세스로 인해 보안 디바이스에 문제가 발생할 수 있습니다. TCP와 UDP 패킷을 필터링하기 위해 사용하는 레이어 4 정보가 초기 프래그먼트에만 있기 때문입니다. Cisco IOS Software에서는 구성된 액세스 목록과 비교하여 초기가 아닌 프래그먼트를 확인하기 위해 특정 방법을 사용합니다. Cisco IOS Software에서는 ACL과 비교하여 초기가 아닌 프래그먼트를 평가하고 모든 레이어 4 필터링 정보를 무시합니다. 따라서 구성된 ACE의 레이어 3 부분에서만 초기가 아닌 프래그먼트가 평가됩니다.

이 예제 컨피그레이션에서 **포트 22**의 **192.168.1.1**를 대상으로 하는 TCP 패킷이 이동 중에 프래그먼트화되면, 패킷에 포함된 레이어 4 정보를 기반으로 두 번째 ACE에서 예상대로 초기 프래그먼트를 삭제합니다. 그러나 나머지 모든(초기가 아닌) 프래그먼트는 전적으로 패킷과 ACE의 레이어 3 정보를 기반으로 하는 첫 번째 ACE에서 허용됩니다. 이 시나리오는 다음 컨피그레이션에 표시됩니다.

```
!

ip access-list extended ACL-FRAGMENT-EXAMPLE
 permit tcp any host 192.168.1.1 eq 80
 deny tcp any host 192.168.1.1 eq 22
!>
```

프래그먼트 처리가 직관적이지 않다는 특성으로 인해, ACL에서 우연히 IP 프래그먼트를 허용하는 경우가 자주 있습니다. 프래그멘테이션은 침입 탐지 시스템을 우회하려는 시도에서도 자주 사용됩니다. 이러한 이유로 IP 프래그먼트가 공격에서 자주 사용되며, 구성된 모든 iACL에 앞서 해당 프래그먼트를 명시적으로 필터링해야 합니다. 이 예제 ACL에는 IP 프래그먼트의 포괄적인 필터링이 포함되어 있습니다. 이 예제의 기능은 이전 예제의 기능과 함께 사용해야 합니다.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

 deny tcp any any fragments
 deny udp any any fragments
 deny icmp any any fragments
 deny ip any any fragments
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

ACL에서 프래그먼트화된 IP 패킷을 처리하는 방법에 대한 자세한 내용은 액세스 제어 목록과 IP 프래그먼트를 참조하십시오.

IP 옵션 필터링을 위한 ACL 지원

Cisco IOS Software Release 12.3(4)T에는 패킷에 포함된 IP 옵션을 기반으로 IP 패킷 필터링에 ACL 사용을 지원하는 기능이 추가되었습니다. IP 옵션은 예외 패킷으로 처리되어야 하므로, 네트워크 디바이스에 대한 보안 문제를 나타냅니다. 따라서 네트워크를 통과하는 일반 패킷에 필요하지 않은 CPU 레벨의 작업이 필요합니다. 패킷에 IP 옵션이 있으면 네트워크에 보안 제어를 파괴하려는 시도가 있거나, 그렇지 않으면 패킷의 이동 특성을 변경하려는 시도가 있음을 나타낼 수 있습니다. 그러므로 IP 옵션이 포함된 패킷은 네트워크 에지에서 필터링되어야 합니다.

IP 옵션을 포함하는 IP 패킷의 완벽한 필터링을 포함하도록 이전 예제의 ACE와 함께 이 예제를 사용해야 합니다.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets containing IP options
!

 deny ip any any option any-options
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

TTL 값 필터링을 위한 ACL 지원

Cisco IOS Software Release 12.4(2)T에는 TTL(Time to Live) 값을 기반으로 IP 패킷을 필터링하는 ACL 지원이 추가되었습니다. IP 데이터그램의 TTL 값은 패킷이 소스에서 대상으로 이동함에 따라 각 네트워크 디바이스별로 감소됩니다. 초기 값은 운영 체제마다 다르지만 패킷의 TTL이 0에 도달하면 패킷이 삭제되어야 합니다. ICMP 시간 초과 메시지를 생성하여 패킷의 소스에 전송하려면 TTL을 0으로 감소시켜 패킷을 삭제하는 디바이스가 필요합니다.

이러한 메시지의 생성 및 전송은 예외 프로세스입니다. 만료 예정인 IP 패킷의 수가 적으면 라우터에서 이 기능을 수행할 수 있지만, 만료 예정인 패킷의 수가 많으면 이러한 메시지를 생성하고 전송하는 데 사용 가능한 모든 CPU 리소스가 소모될 수 있습니다. 이는 DoS 공격 벡터를 나타냅니다. 따라서 만료 예정인 높은 비율의 IP 패킷을 활용하는 DoS 공격에 대비하여 디바이스를 강화해야 합니다.

조직에서는 네트워크의 에지에서 TTL 값이 낮은 IP 패킷을 필터링하는 것이 좋습니다. 네트워크를 통과하는 데 충분하지 않은 TTL 값이 있는 패킷을 완벽하게 필터링하면 TTL 기반의 공격 위협이 차단됩니다.

이 예제 ACL에서는 TTL 값이 6 미만인 패킷을 필터링합니다. 이렇게 하면 너비가 최대 5개의 홉인 네트워크에 대한 TTL 만료 공격이 차단됩니다.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets with TTL values insufficient to traverse the network
!

 deny ip any any ttl lt 6
!
!--- Deny all other IP traffic to any network device
!
```

```
 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

참고: 일부 프로토콜에서는 TTL 값이 낮은 패킷을 합법적으로 사용합니다. 이러한 프로토콜의 예로는 eBGP가 있습니다. TTL 만료 기반 공격 차단에 대한 자세한 내용은 TTL 만료 공격 식별 및 차단을 참조하십시오.

이 기능에 대한 자세한 내용은 TTL 값 필터링을 위한 ACL 지원을 참조하십시오.

보안 인터랙티브 관리 세션

디바이스 관리 세션을 사용하면 디바이스와 해당 운영에 대한 정보를 보고 수집할 수 있습니다. 이 정보가 악의적인 사용자에게 노출되면 디바이스가 공격의 대상이 되어 보안 침해가 일어나거나 추가 공격을 수행하는 데 사용될 수 있습니다. 디바이스에 대한 액세스 권한이 부여된 사용자는 해당 디바이스에 대한 전체 관리 제어를 수행할 수 있습니다. 정보 공개 및 무단 액세스를 방지하려면 관리 세션을 보호해야 합니다.

관리 플레인 보호

Cisco IOS Software Release 12.4(6)T 이상에서 MPP(Management Plane Protection) 기능을 사용하면 관리자가 디바이스에서 수신할 수 있는 인터페이스 관리 트래픽을 제한할 수 있습니다. 또한 관리자가 디바이스와 디바이스 액세스 방법을 추가로 제어할 수 있습니다.

다음 예에서는 GigabitEthernet0/1 인터페이스에서 SSH와 HTTPS만 허용하기 위해 MPP를 활성화하는 방법을 보여줍니다.

```
!

control-plane host
  management-interface GigabitEthernet 0/1 allow ssh https

!
```

MPP에 대한 자세한 내용은 관리 플레인 보호를 참조하십시오.

컨트롤 플레인 보호

IOS 디바이스의 RP(Route Processor)를 대상으로 하는 컨트롤 플레인 트래픽을 제한하고 감시하기 위해 CoPP(Control Plane Policing) 기능을 기반으로 CPPr(Control Plane Protection)을 구축합니다. Cisco IOS Software Release 12.4(4)T에 추가된 CPPr은 컨트롤 플레인을 하위 인터페이스라고 하는 개별 컨트롤 플레인 카테고리로 나눕니다. 호스트, 이동 및 CEF 예외의 세 가지 컨트롤 플레인 하위 인터페이스가 있습니다. 또한 CPPr에는 다음과 같은 추가 컨트롤 플레인 보호 기능이 포함되어 있습니다.

- **포트 필터링 기능** - 이 기능을 사용하면 폐쇄되거나 수신하지 않는 TCP 및 UDP 포트로 이동하는 패킷을 삭제하거나 감시할 수 있습니다.
- **큐 임계값 정책 기능** - 이 기능은 컨트롤 플레인 IP 입력 큐에서 허용되는 지정된 프로토콜의 패킷 수를 제한합니다.

CPPr을 사용하면 관리자가 호스트 하위 인터페이스를 사용하여 관리를 목적으로 디바이스에 전송한 트래픽을 분류하고 감시하며 제한할 수 있습니다. 호스트 하위 인터페이스 카테고리로 분류되는 패킷의 예에는 SSH나 텔넷 및 라우팅 프로토콜과 같은 관리 트래픽이 포함됩니다.

참고: CPPr은 IPv6을 지원하지 않으며 IPv4 입력 경로로 제한됩니다.

Cisco CPPr 기능에 대한 자세한 내용은 컨트롤 플레인 보호 기능 가이드 - 12.4T 및 컨트롤 플레인 보호 이해를 참조하십시오.

관리 세션 암호화

인터랙티브 관리 세션에 정보가 공개될 수 있으므로 악의적인 사용자가 전송되는 데이터에 대한 액세스 권한을 획득할 수 없도록 이 트래픽을 암호화해야 합니다. 트래픽 암호화를 사용하면 디바이스에 대한 보안 원격 액세스 연결이 가능합니다. 일반 텍스트로 네트워크를 통해 관리 세션의 트래픽을 전송하면 공격자가 디바이스와 네트워크에 대한 민감한 정보를 확보할 수 있습니다.

관리자가 SSH 또는 HTTPS(Secure Hypertext Transfer Protocol) 기능을 사용하여 디바이스에 암호화된 보안 원격 액세스 관리 연결을 설정할 수 있습니다. Cisco IOS Software에서는 인증 및 데이터 암호화에 SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security)를 사용하는 HTTPS, SSHv1(SSH Version 1.0) 및 SSHv2(SSH Version 2.0)를 지원합니다. SSHv1과 SSHv2는 호환되지 않습니다.

Cisco IOS Software에서는 디바이스 컨피그레이션 또는 소프트웨어 이미지를 복사하기 위해 암호화된 보안 연결을 허용하는 SCP(Secure Copy Protocol)도 지원합니다. SCP는 SSH를 사용합니다. 다음 예제 컨피그레이션에서는 Cisco IOS 디바이스에서 SSH를 사용하도록 설정합니다.

```
!

ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1
!

line vty 0 4
 transport input ssh

!
```

다음 컨피그레이션 예에서는 SCP 서비스를 사용하도록 설정합니다.

```
!

ip scp server enable
!
```

다음은 HTTPS 서비스를 위한 컨피그레이션 예입니다.

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

Cisco IOS Software SSH 기능에 대한 자세한 내용은 Cisco IOS 및 SSH(Secure Shell)를 실행 중인 라우터와 스위치에서 SSH(Secure Shell) 구성 FAQ를 참조하십시오.

SSHv2

Cisco IOS Software Release 12.3(4)T에 도입된 SSHv2 지원 기능을 사용하면 사용자가 SSHv2를 구성할 수 있습니다. (SSHv1 지원은 Cisco IOS Software의 이전 릴리스에서 구현되었습니다.) SSH는 신뢰할 수 있는 전송 레이어에서 실행되어 강력한 인증 및 암호화 기능을 제공합니다. SSH에 정의된 신뢰할 수 있는 전송 방법은 TCP뿐입니다. SSH는 다른 컴퓨터 또는 네트워크를 통해 연결된 디바이스에 안전하게 액세스하고 안전하게 명령어를 실행할 수 있는 방법을 제공합니다. SSH를 통해 터널링된 SCP(Secure Copy Protocol) 기능을 사용하면 파일을 안전하게 전송할 수 있습니다.

이 예제 컨피그레이션에서는 Cisco IOS 디바이스에서 SSHv2(SSHv1은 비활성화됨)를 사용하도록 설정합니다.

```
!

hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1

!

ip ssh version 2

!

line vty 0 4
transport input ssh

!
```

SSHv2 사용에 대한 자세한 내용은 SSHv2(Secure Shell Version 2) 지원을 참조하십시오.

RSA 키를 위한 SSHv2 개선 기능

Cisco IOS SSHv2에서는 키보드 인터랙티브 인증 방법 및 비밀번호 기반 인증 방법을 지원합니다. RSA 키를 위한 SSHv2 개선 기능은 클라이언트와 서버의 RSA 기반 공개 키 인증도 지원합니다.

사용자 인증을 위해 RSA 기반 사용자 인증에서는 인증할 각 사용자와 연결된 개인/공개 키 쌍을 사용합니다. 인증을 완료하려면 사용자가 클라이언트에 개인/공개 키 쌍을 생성하고 Cisco IOS SSH 서버에 공개 키를 구성해야 합니다.

자격 증명을 설정하려는 SSH 사용자가 개인 키로 암호화된 시그니처를 제공합니다. 인증을 위해 시그니처와 사용자의 공개 키를 SSH 서버에 전송합니다. SSH 서버에서는 사용자가 제공한 공개 키를 통해 해시를 계산합니다. 해시는 서버에 일치하는 항목이 있는지 판별하는 데 사용합니다. 일치 항목이 있는 경우 공개 키를 사용하여 RSA 기반 메시지 검증이 수행됩니다. 따라서 암호화된 시그니처를 기반으로 사용자의 액세스를 인증하거나 거부합니다.

서버 인증을 위해 Cisco IOS SSH 클라이언트에서 각 서버의 호스트 키를 할당해야 합니다. 클라이언트에서 서버에 SSH 세션을 설정하려고 할 때 키 교환 메시지의 일부로 서버의 시그니처를 수신합니다. 엄격한 호스트 키 확인 플래그가 클라이언트에서 활성화된 경우 클라이언트에서 사전 구성된 서버에 해당하는 호스트 키 항목이 있는지 확인합니다. 일치 항목이 있는 경우 클라이언트에서 서버 호스트 키로 시그니처를 검증하려고 시도합니다. 서버가 성공적으로 인증되면 세션 설정이 계속됩니다. 그렇지 않은 경우 세션 설정이 종료되고 **서버 인증 실패** 메시지가 표시됩니다.

다음 예제 컨피그레이션에서는 Cisco IOS 디바이스에서 SSHv2를 통한 RSA 키를 사용하도록 설정합니다.

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Specify the name of the RSA key pair (in this case, "sshkeys") to use for SSH
!

 ip ssh rsa keypair-name sshkeys
!
! Enable the SSH server for local and remote authentication on the router using
! the "crypto key generate" command
! For SSH version 2, the modulus size must be at least 768 bits
!

 crypto key generate rsa usage-keys label sshkeys modulus 2048
!
! Configure an ssh timeout (in seconds)
!
! The following enables a timeout of 120 seconds for SSH connections
!

ip ssh time-out 120
!
! Configure a limit of five (5) authentication retries
!

ip ssh authentication-retries 5
!
! Configure SSH version 2
!

ip ssh version 2
!
```

SSHv2와 함께 RSA 키 사용에 대한 자세한 내용은 RSA 키에 대한 SSHv2(Secure Shell Version 2) 개선 기능을 참조하십시오.

이 예제 컨피그레이션을 통해 Cisco IOS SSH 서버에서 RSA 기반 사용자 인증을 수행할 수 있습니다. 서버에 저장된 RSA 공개 키를 클라이언트에 저장된 공개 또는 개인 키 쌍으로 검증하면 사용자 인증에 성공합니다.

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
```

```
!
! Configure the SSH username
!

        username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

SSHv2와 함께 RSA 키 사용에 대한 자세한 내용은 RSA 기반 사용자 인증을 수행하도록 Cisco IOS SSH 서버 구성을 참조하십시오.

이 예제 컨피그레이션을 통해 Cisco IOS SSH 클라이언트에서 RSA 기반 서버 인증을 수행할 수 있습니다.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

        server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

SSHv2와 함께 RSA 키 사용 대한 자세한 내용은 RSA 기반 서버 인증을 수행하도록 Cisco IOS SSH 클라이언트 구성을 참조하십시오.

콘솔 및 AUX 포트

Cisco IOS 디바이스에서 콘솔과 보조(AUX) 포트는 디바이스에 로컬 및 원격으로 액세스하는 데 사용할 수 있는 비동기 라인입니다. Cisco IOS 디바이스의 콘솔 포트에 특수 권한이 있음을 알아야 합니다. 특히 이러한 권한을 사용하면 관리자가 비밀번호 복구 절차를 수행할 수 있습니다. 비밀번호 복구를 수행하려면 인증되지 않은 공격자가 콘솔 포트에 액세스해야 하며 디바이스에 입력되는 전원을 차단하거나 디바이스가 충돌하게 할 수 있어야 합니다.

디바이스의 콘솔 포트에 액세스하는 데 사용되는 모든 방법은 권한을 통해 디바이스에 액세스하기 위해 적용되는 보안과 동일한 방식으로 보호되어야 합니다. 액세스 보안을 위해 사용되는 방법에는 AAA 사용, exec 시간 초과 및 모뎀 비밀번호(모뎀이 콘솔에 추가된 경우)가 포함되어야 합니다.

비밀번호 복구가 필요하지 않으면 관리자가 **no service password-recovery** 전역 환경 설정 명령어를 사용하여 비밀번호 복구 절차를 수행하는 기능을 제거할 수 있습니다. 그러나 **no service password-recovery** 명령어를 사용하도록 설정한 후에는 관리자가 더 이상 디바이스에서 비밀번호 복구를 수행할 수 없습니다.

대부분의 경우 무단 액세스를 방지하려면 디바이스의 AUX 포트가 비활성화되어야 합니다. AUX 포트는 다음 명령어를 사용하여 비활성화할 수 있습니다.

```
!

line aux 0
 transport input none
 transport output none
 no exec
 exec-timeout 0 1
 no password
!
```

vty 및 tty 라인 제어

Cisco IOS Software의 인터랙티브 관리 세션에서는 tty 또는 vty(virtual tty)를 사용합니다. tty는 다이얼업을 통해 디바이스에 액세스하기 위해 모뎀에 추가하거나 디바이스에 로컬로 액세스하기 위해 터미널을 추가할 수 있는 로컬 비동기 라인입니다. tty는 다른 디바이스의 콘솔 포트에 연결하는 데 사용할 수 있습니다. 이 기능을 사용하면 tty 라인이 있는 디바이스가 콘솔 서버 역할을 수행할 수 있습니다. 여기에서 네트워크를 통해 tty 라인에 연결된 디바이스의 콘솔 포트에 연결을 설정할 수 있습니다. 네트워크를 통한 역방향 연결용 tty 라인도 제어해야 합니다.

프로토콜(예: SSH, SCP 또는 텔넷)과 상관없이 디바이스에서 지원하는 다른 모든 원격 네트워크 연결에 vty 라인이 사용됩니다. 로컬 또는 원격 관리 세션을 통해 디바이스에 액세스할 수 있도록 vty 및 tty 라인 모두에 적절한 제어가 적용되어야 합니다. Cisco IOS 디바이스에는 제한된 수의 vty 라인이 있습니다. 사용 가능한 라인 수는 show line EXEC 명령어를 통해 판별할 수 있습니다. 모든 vty 라인이 사용 중이면 새 관리 세션을 설정할 수 없으므로, 디바이스에 액세스하기 위한 DoS 조건이 생성됩니다.

디바이스의 vty 또는 tty에 대한 액세스를 제어하는 가장 간단한 형식은 네트워크 내의 디바이스 위치와 상관없이 모든 라인에서 인증을 사용하는 것입니다. vty 라인은 네트워크를 통해 액세스할 수 있으므로 이 형식은 vty 라인에 중요합니다. 디바이스에 원격으로 액세스하는 데 사용되는 모뎀에 연결된 tty 라인 또는 다른 디바이스의 콘솔 포트에 연결된 tty 라인도 네트워크를 통해 액세스할 수 있습니다. CoPP 및 CPPr 기능을 사용하거나 디바이스의 인터페이스에 액세스 목록을 적용하는 경우, **transport input** 또는 **access-class** 환경 설정 명령어를 통해 다른 형식의 vty 및 tty 액세스 제어를 적용할 수 있습니다.

인증은 AAA를 사용하여 적용할 수 있습니다. 이 방법은 로컬 사용자 데이터베이스를 사용하거나 vty 또는 tty 라인에 직접 구성된 간단한 비밀번호 인증을 통해 디바이스에 대한 인증된 액세스를 수행하는 방법으로 권장됩니다.

유휴 상태로 남아 있는 vty 또는 tty 라인에서 세션을 로그아웃하려면 **exec-timeout** 명령어를 사용해야 합니다. 디바이스로 수신되는 연결에서 TCP keepalives를 활성화하려면 **service tcp-keepalives-in** 명령어도 사용해야 합니다. 이렇게 하면 원격에 있는 연결 종단의 디바이스에 계속해서 액세스할 수 있으며 일부만 개방된 연결이나 격리된 연결이 로컬 IOS 디바이스에서 제거됩니다.

vty 및 tty 라인의 전송 제어

암호화된 보안 원격 액세스 관리 연결만 디바이스에 허용하거나 디바이스를 통과하도록(콘솔 서버로 사용하는 경우) 허용하려면 vty와 tty를 구성해야 합니다. 이러한 라인은 다른 디바이스의 콘솔 포트에 연결되어, 네트워크를 통해 tty에 액세스가 가능하게 되므로 이 섹션에서는 tty에 대해 설명합니다. 정보가 공개되거나 관리자와 디바이스 간에 전송되는 데이터에 무단으로 액세스하지 못하게 하려면 일반 텍스트 프로토콜(예: 텔넷 및 rlogin)이 아니라 **transport input ssh**를 사용해야 합니다. tty에서 **transport input none** 컨피그레이션을 활성화할 수 있습니다. 그러면 역방향 콘솔 연결을 위해 tty 라인 사용이 비활성화됩니다.

관리자가 vty와 tty 라인 모두에서 다른 디바이스에 연결할 수 있습니다. 관리자가 발신 연결에 사용할 수 있는 전송 유형을 제한하려면 **transport output** 라인 환경 설정 명령어를 사용합니다. 발신 연결이 필요하지 않으면 **transport output none**을 사용해야 합니다. 그러나 발신 연결이 허용되는 경우 **transport output ssh**를 사용하여 연결을 위해 암호화된 보안 원격 액세스 방법을 적용해야 합니다.

참고: IPSec이 지원되는 경우 디바이스에 대한 암호화된 보안 원격 액세스 연결에 IPSec을 사용할 수 있습니다. IPSec을 사용하는 경우 디바이스에 CPU 오버헤드도 추가됩니다. 그러나 IPSec을 사용하는 경우에도 여전히 SSH를 전송 방법으로 적용해야 합니다.

경고 배너

일부 법적 관할권에서는 악의적인 사용자에게 시스템을 사용할 수 없다고 알리지 않은 경우 악의적인 사용자를 기소할 수 없으며 모니터링하는 것이 불법일 수 있습니다. 이 알림을 제공하는 방법 중 하나는 Cisco IOS Software 배너 로그인 명령어로 구성된 배너 메시지에 이 정보를 표시하는 것입니다.

법적 알림 요구 사항은 복잡하며 법적 관할권과 상황에 따라 다르므로, 법률 고문과 논의해야 합니다. 법적 관할권 내에서도 법적 의견이 다를 수 있습니다. 법률 고문과 협력하여 다음 정보 중 일부 또는 전부를 배너를 통해 제공할 수 있습니다.

- 구체적으로 권한이 부여된 사용자만 시스템에 로그인하거나 사용할 수 있으며, 시스템 사용을 허가할 수 있는 사용자에 대한 정보를 통해서도 로그인하거나 사용할 수 있습니다.
- 시스템의 무단 사용은 불법이므로 민형사상 처벌을 받을 수 있습니다.
- 추후 통보 없이 시스템 사용을 기록하거나 모니터링할 수 있으며 결과적으로 얻은 로그를 법정에서 증거로 사용할 수 있습니다.
- 현지 법률에 따라 명확히 통보해야 합니다.

법률이 아니라 보안 관점에서 로그인 배너에는 라우터 이름, 모델, 소프트웨어 또는 소유권에 대한 구체적인 정보가 없어야 합니다. 이 정보는 악의적인 사용자가 오용할 수 있습니다.

인증, 권한 부여 및 계정 관리(AAA)

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스에 대한 인터랙티브 액세스 보안에 중요합니다. AAA 프레임워크에서는 네트워크 요구 사항에 따라 조정할 수 있는 구성하기 쉬운 환경을 제공합니다.

TACACS+ 인증

TACACS+는 Cisco IOS 디바이스에서 원격 AAA 서버에 대해 관리 사용자를 인증하는 데 사용할 수 있는 인증 프로토콜입니다. 이러한 관리 사용자는 SSH, HTTPS, 텔넷 또는 HTTP를 통해 IOS 디바이스에 액세스할 수 있습니다.

TACACS+ 인증 또는 더욱 일반적으로 AAA 인증에서는 각 네트워크 관리자가 개별 사용자 계정을 사용하는 기능을 제공합니다. 단일 공유 비밀번호에 의존하지 않는 경우 네트워크 보안이 향상되므로 사용자의 책임이 강화됩니다.

RADIUS는 용도 면에서 TACACS+와 비슷한 프로토콜이지만, 네트워크를 통해 전송된 비밀번호만 암호화합니다. 반면, TACACS+는 사용자 이름과 비밀번호를 모두 포함하는 전체 TCP 페이로드를 암호화합니다. 따라서 AAA 서버에서 TACACS+를 지원하는 경우 RADIUS보다 우선적으로 TACACS+를 사용해야 합니다. 이러한 두 가지 프로토콜의 자세한 비교는 TACACS+ 및 RADIUS 비교를 참조하십시오.

TACACS+ 인증은 컨피그레이션이 다음 예와 비슷한 Cisco IOS 디바이스에서 활성화할 수 있습니다.

```
!

aaa new-model
aaa authentication login default group tacacs+
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

이전 컨피그레이션은 조직별 AAA 인증 템플릿의 시작점으로 사용할 수 있습니다. AAA 컨피그레이션에 대한 자세한 내용은 인증, 권한 부여 및 계정 관리를 참조하십시오.

방법 목록은 사용자를 인증하기 위해 쿼리할 인증 방법을 설명하는 순차적 목록입니다. 방법 목록을 사용하면 하나 이상의 보안 프로토콜을 인증에 사용하도록 지정할 수 있으므로, 초기 방법이 실패하는 경우 백업 시스템에서 인증할 수 있습니다. Cisco IOS Software에서는 사용자를 성공적으로 승인 또는 거부한 첫 번째로 나열된 방법을 사용합니다. 후속 방법은 서버 사용 불가능 또는 올바르지 않은 컨피그레이션으로 인해 이전 방법이 실패한 경우에만 사용합니다. 명명된 방법 목록 컨피그레이션에 대한 자세한 내용은 인증용으로 명명된 방법 목록을 참조하십시오.

인증 폴백

구성된 모든 TACACS+ 서버가 사용 불가능하게 되면 Cisco IOS 디바이스에서 보조 인증 프로토콜을 사용할 수 있습니다. 일반적인 컨피그레이션에서는 구성된 모든 TACACS+ 서버가 사용 불가능한 경우 로컬 또는 인증 활성화 사용을 포함합니다.

온 디바이스(on-device) 인증을 위한 전체 옵션 목록에는 활성화, 로컬 및 라인이 포함됩니다. 이러한 옵션은 각각 장점이 있습니다. 라인 또는 로컬 인증용 유형 7 비밀번호와 함께 사용하는 암호화 알고리즘에 비해 본질적으로 더욱 안전한 단방향 알고리즘으로 암호를 해시하므로 암호 활성화를 사용하는 것이 낫습니다.

그러나 로컬로 정의된 사용자에 대해 비밀 암호 사용을 지원하는 Cisco IOS Software Release에서는 로컬 인증으로 폴백(fallback)하는 것이 바람직할 수 있습니다. 그러면 하나 이상의 네트워크 관리자가 로컬로 정의된 사용자를 생성할 수 있습니다. TACACS+가 완전히 사용 불가능하게 되면 각 관리자가 로컬 사용자 이름과 비밀번호를 사용할 수 있습니다. 이 작업을 수행해도 TACACS+ 중지 시 네트워크 관리자의 책임이 늘어나지는 않지만 모든 네트워크 디바이스에 있는 로컬 사용자 계정을 유지관리해야 하므로 관리 부담이 현저히 늘어납니다.

이 컨피그레이션 예는 **enable secret** 명령어를 사용하여 로컬에 구성된 비밀번호에 대한 폴백 인증을 포함하기 위해 이전 TACACS+ 인증을 기반으로 구축합니다.

```
!

enable secret <password>
!

aaa new-model
aaa authentication login default group tacacs+ enable
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

AAA와 함께 폴백 인증 사용에 대한 자세한 내용은 인증 구성을 참조하십시오.

유형 7 비밀번호 사용

원래 저장된 비밀번호를 신속하게 암호 해독할 수 있도록 설계된 유형 7 비밀번호는 안전한 비밀번호 스토리지 형식이 아닙니다. 이러한 비밀번호를 쉽게 암호 해독할 수 있는 툴이 많이 있습니다. Cisco IOS 디바이스에서 사용 중인 기능에 필요한 경우가 아니면 유형 7 비밀번호를 사용하지 않아야 합니다.

이 유형의 비밀번호는 AAA 인증 및 향상된 비밀번호 보안(Enhanced Password Security) 기능을 사용하면 쉽게 제거할 수 있습니다. 이 기능을 사용하면 **username** 전역 환경 설정 명령어를 통해 로컬에 정의된 사용자에 비밀 암호를 사용할 수 있습니다. 완벽하게 유형 7 비밀번호의 사용을 방지할 수 없는 경우 이러한 비밀번호를 암호화하는 대신 모호하게 만드십시오.

유형 7 비밀번호 제거에 대한 자세한 내용은 이 문서의 일반 관리 플레인 강화 섹션을 참조하십시오.

TACACS+ 명령어 권한 부여

TACACS+ 및 AAA를 사용한 명령어 권한 부여에서는 관리 사용자가 입력한 각 명령어를 허용하거나 거부하는 메커니즘을 제공합니다. 사용자가 EXEC 명령어를 입력하면 Cisco IOS에서 각 명령어를 구성된 AAA 서버에 전송합니다. 그러면 AAA 서버에서 그러한 특정 사용자의 명령어를 허용하거나 거부하기 위해 구성된 정책을 사용합니다.

명령어 권한 부여를 구현하기 위해 다음 컨피그레이션을 이전 AAA 인증 예에 추가할 수 있습니다.

```
!

aaa authorization exec default group tacacs none
aaa authorization commands 0 default group tacacs none
aaa authorization commands 1 default group tacacs none
aaa authorization commands 15 default group tacacs none
!
```

명령어 권한 부여에 대한 자세한 내용은 인증 구성을 참조하십시오.

TACACS+ 명령어 계정 관리

구성된 경우, AAA 명령어 계정 관리에서 입력한 각 EXEC 명령어에 대한 정보를 구성된 TACACS+ 서버에 전송합니다. TACACS+ 서버에 전송된 정보에는 실행된 명령어, 실행된 날짜 및 명령어를 입력한 사용자의 사용자 이름이 포함됩니다. 명령어 계정 관리는 RADIUS에서는 지원되지 않습니다.

다음 예제 컨피그레이션에서는 권한 레벨 0, 1 및 15에서 입력된 EXEC 명령어에 대한 AAA 명령어 계정 관리를 활성화합니다. 이 컨피그레이션은 TACACS 서버의 컨피그레이션을 포함하는 이전 예를 기반으로 구축합니다.

```
!

aaa accounting exec default start-stop group tacacs
aaa accounting commands 0 default start-stop group tacacs
aaa accounting commands 1 default start-stop group tacacs
aaa accounting commands 15 default start-stop group tacacs
!
```

AAA 계정 관리 컨피그레이션에 대한 자세한 내용은 계정 관리 구성을 참조하십시오.

이중화된 AAA 서버

환경에서 활용되는 AAA 서버는 이중화되어야 하며 내결함성 방식으로 구축되어야 합니다. 그러면 AAA 서버를 사용할 수 없는 경우 SSH와 같은 인터랙티브 관리 액세스가 가능하게 됩니다.

이중화된 AAA 서버 솔루션을 설계하거나 구현할 때 다음과 고려 사항을 기억하십시오.

- 네트워크에 장애가 발생할 수 있는 경우 AAA 서버 가용성
- AAA 서버를 지리적으로 분산 배치
- 안정 상태 및 장애 조건에서 개별 AAA 서버의 로드
- 네트워크 액세스 서버와 AAA 서버 간 네트워크 레이턴시
- AAA 서버 데이터베이스 동기화

자세한 내용은 액세스 제어 서버 구축을 참조하십시오.

SNMP(Simple Network Management Protocol) 강화

이 섹션에서는 IOS 디바이스에서 SNMP를 안전하게 구축하는 데 사용할 수 있는 여러 방법을 설명합니다. 네트워크 데이터와 이 데이터를 전송할 네트워크 디바이스 모두의 기밀성, 무결성 및 가용성을 보호하려면 SNMP의 보안을 적절하게 설정하는 것이 중요합니다. SNMP에서는 네트워크 디바이스의 상태에 대한 풍부한 정보를 제공합니다. 네트워크를 대상으로 공격을 수행하기 위해 이 데이터를 활용하려는 악의적인 사용자로부터 정보를 보호해야 합니다.

SNMP 커뮤니티 문자열

커뮤니티 문자열은 디바이스에서 SNMP 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 모두 제한하기 위해 IOS 디바이스에 적용되는 비밀번호입니다. 모든 비밀번호와 마찬가지로 이 커뮤니티 문자열을 평범하지 않도록 신중하게 선택해야 합니다. 커뮤니티 문자열은 정기적으로 네트워크 보안 정책에 따라 변경해야 합니다. 예를 들어, 네트워크 관리자의 역할이 변경되거나 퇴사하는 경우 문자열을 변경해야 합니다.

이러한 컨피그레이션 라인은 읽기 전용 커뮤니티 문자열인 READONLY와 읽기-쓰기 커뮤니티 문자열인 READWRITE를 구성합니다.

```
!

snmp-server community READONLY RO
snmp-server community READWRITE RW
!
```

참고: 이전 커뮤니티 문자열 예는 이러한 문자열의 사용을 명확하게 설명하기 위해 선택되었습니다. 프로덕션 환경에서는 커뮤니티 문자열을 신중하게 선택해야 하며, 일련의 영문자, 숫자 및 비영숫자 기호로 구성해야 합니다. 평범하지 않은 비밀번호를 선택하는 데 대한 자세한 내용은 강력한 비밀번호 생성 권장 사항을 참조하십시오.

이 기능에 대한 자세한 내용은 IOS SNMP 명령어 참조를 참고하십시오.

ACL과 SNMP 커뮤니티 문자열

커뮤니티 문자열 외에도 소스 IP 주소 선택 그룹에 대한 SNMP 액세스를 더욱 제한하는 ACL을 적용해야 합니다. 이 컨피그레이션은 192.168.100.0/24 주소 공간에 있는 종단 호스트 디바이스에 대한 SNMP 읽기 전용 액세스를 제한하고, 192.168.100.1에 있는 종단 호스트 디바이스에 대해서만 SNMP 읽기-쓰기 액세스를 제한합니다.

참고: 요청된 SNMP 정보에 액세스하려면 이러한 ACL에서 허용한 디바이스에 적절한 커뮤니티 문자열이 있어야 합니다.

```
!

access-list 98 permit 192.168.100.0 0.0.0.255
access-list 99 permit 192.168.100.1
!
```

```
snmp-server community READONLY RO 98
snmp-server community READWRITE RW 99

!
```

이 기능에 대한 자세한 내용은 Cisco IOS 네트워크 관리 명령어 참조에서 snmp-server community를 참고하십시오.

인프라 ACL

신뢰할 수 있는 IP 주소가 있는 종단 호스트만 IOS 디바이스에 SNMP 트래픽을 보낼 수 있도록 iACL(Infrastructure ACL)을 구축할 수 있습니다. iACL에는 UDP 포트 161에서 무단 SNMP 패킷을 거부하는 정책을 포함해야 합니다.

iACL 사용에 대한 자세한 내용은 이 문서의 인프라 ACL로 네트워크에 대한 액세스 제한 섹션을 참조하십시오.

SNMP 보기

SNMP 보기는 특정 SNMP MIB에 대한 액세스를 허용하거나 거부할 수 있는 보안 기능입니다. 보기를 생성한 다음 **snmp-server community** 커뮤니티 문자열 보기 전역 환경 설정 명령어를 사용하여 커뮤니티 문자열에 적용한 후에 MIB 데이터에 액세스하는 경우, 보기에 정의된 권한으로 제한됩니다. 적절한 경우 보기를 사용하여 SNMP 사용자가 필요한 데이터만 사용하도록 제한하는 것이 좋습니다.

이 컨피그레이션 예제에서는 커뮤니티 문자열 LIMITED를 사용하여 SNMP 액세스를 시스템 그룹에 있는 MIB 데이터로 제한합니다.

```
!

snmp-server view VIEW-SYSTEM-ONLY system include
!

snmp-server community LIMITED view VIEW-SYSTEM-ONLY RO
!
```

자세한 내용은 SNMP 지원 구성을 참조하십시오.

SNMP 버전 3

SNMPv3(SNMP Version 3)은 RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 및 RFC3415로 정의되며 네트워크 관리용으로 상호 운용 가능한 표준 기반 프로토콜입니다. SNMPv3에서는 네트워크를 통해 패킷을 인증하고 선택적으로 암호화하므로 디바이스에 대한 보안 액세스를 제공합니다. 지원되는 경우, SNMP를 구축할 때 다른 보안 레이어를 추가하기 위해 SNMPv3을 사용할 수 있습니다. SNMPv3은 다음 세 가지 기본 컨피그레이션 옵션으로 구성됩니다.

- **no auth** - 이 모드에서는 SNMP 패킷의 암호화나 인증이 필요하지 않습니다.
- **auth** - 이 모드에서는 암호화하지 않고 SNMP 패킷을 인증해야 합니다.
- **priv** - 이 모드에는 각 SNMP 패킷의 인증과 암호화(개인정보 보호)가 모두 필요합니다.

SNMP 패킷을 처리하는 데 SNMPv3 보안 메커니즘인 인증 또는 인증 및 암호화를 사용하려면 권한있는 엔진 ID가 있어야 합니다. 기본적으로 엔진 ID는 로컬로 생성됩니다. 엔진 ID는 이 예에 표시된 대로 **show snmp engineID** 명령어를 사용하여 표시할 수 있습니다.

```
router#show snmp engineID
   Local SNMP engineID: 8000000903000015 2BD35496
   Remote Engine ID          IP-addr    Port
```

참고: 엔진 ID가 변경되면 모든 SNMP 사용자 계정을 다시 구성해야 합니다.

다음 단계에서는 SNMPv3 그룹을 구성합니다. 이 명령어는 SNMP 서버 그룹 AUTHGROUP으로 SNMPv3에 맞게 Cisco IOS 디바이스를 구성하고 **auth** 키워드로 이 그룹의 인증만 사용하도록 설정합니다.

```
!
snmp-server group AUTHGROUP v3 auth
!
```

이 명령어는 SNMP 서버 그룹 PRIVGROUP으로 SNMPv3에 맞게 Cisco IOS 디바이스를 구성하고 **priv** 키워드로 이 그룹의 인증과 암호화를 모두 사용하도록 설정합니다.

```
!
snmp-server group PRIVGROUP v3 priv
!
```

이 명령어는 MD5 인증 비밀번호인 **authpassword**와 3DES 암호화 비밀번호인 **privpassword**를 사용하여 SNMPv3 user snmpv3user를 구성합니다.

```
!

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des
     privpassword
!
```

snmp-server user 환경 설정 명령어는 RFC 3414에서 요구하는 대로 디바이스의 컨피그레이션 출력에 표시되지 않으므로, 컨피그레이션에서 사용자 비밀번호를 볼 수 없습니다. 구성된 사용자를 보려면 다음 예에 표시된 대로 **show snmp user** 명령어를 입력합니다.

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

이 기능에 대한 자세한 내용은 SNMP 지원 구성을 참조하십시오.

관리 플레인 보호

Cisco IOS Software의 MPP(Management Plane Protection) 기능은 디바이스에서 SNMP 트래픽을 종료할 수 있는 인터페이스를 제한하므로 SNMP 보안에 도움이 되도록 이 기능을 사용할 수 있습니다. MPP 기능을 사용하면 관리자가 하나 이상의 인터페이스를 관리 인터페이스로 지정할 수 있습니다. 관리 트래픽은 이러한 관리 인터페이스를 통해서만 디바이스에 입력될 수 있습니다. MPP가 활성화되면 지정된 관리 인터페이스 이외의 인터페이스에서 디바이스를 대상으로 하는 네트워크 관리 트래픽을 승인하지 않습니다.

MPP는 CPPr 기능의 하위 집합이므로 CPPr을 지원하는 IOS 버전이 필요합니다. CPPr에 대한 자세한 내용은 컨트롤 플레인 보호 이해를 참조하십시오.

이 예에서는 SNMP 및 SSH 액세스를 FastEthernet 0/0 인터페이스로만 제한하기 위해 MPP를 사용합니다.

```
!
control-plane host
 management-interface FastEthernet0/0 allow ssh snmp
!
```

자세한 내용은 관리 플레인 보호 기능 가이드를 참조하십시오.

로깅 모범 사례

이벤트 로깅을 사용하면 Cisco IOS 디바이스의 운영과 해당 디바이스가 구축된 네트워크에 대한 가시성을 제공합니다. Cisco IOS Software에서는 조직의 네트워크 관리 및 가시성 목표를 달성하는 데 도움이 되는 여러 유연한 로깅 옵션을 제공합니다.

이러한 섹션에서는 관리자가 Cisco IOS 디바이스에 미치는 로깅의 영향은 최소화하면서 성공적으로 로깅을 활용하는 데 도움이 되는 기본 로깅 모범 사례를 제공합니다.

중앙 위치에 로그 보내기

원격 syslog 서버에 로깅 정보를 전송하는 것이 좋습니다. 그러면 네트워크 디바이스 전체에서 네트워크와 보안 이벤트의 상관성을 더욱 효율적으로 분석하고 이들을 감사할 수 있습니다. UDP 및 일반 텍스트로 전송되는 syslog 메시지는 신뢰할 수 없습니다. 따라서 syslog 트래픽을 포함하려면 네트워크에서 관리 트래픽(예: 암호화 또는 대역 외 액세스)에 제공할 수 있는 보호를 확장해야 합니다.

이 컨피그레이션 예제에서는 원격 syslog 서버에 로깅 정보를 전송하도록 Cisco IOS 디바이스를 구성합니다.

```
!
logging host <ip-address>
!
```

로그 상관관계에 대한 자세한 내용은 방화벽 및 IOS 라우터 Syslog 이벤트를 사용하여 사고 식별을 참조하십시오.

12.4(15)T에 통합되었으며 12.0(26)S에 처음 도입된 로컬 비휘발성 스토리지(ATA 디스크)에 로깅(Logging to Local Nonvolatile Storage) 기능을 사용하면 ATA(Advanced Technology Attachment) 플래시 디스크에 시스템 로깅 메시지를 저장할 수 있습니다. ATA 드라이브에 저장된 메시지는 라우터를 재부팅한 후에도 지속됩니다.

이 컨피그레이션 라인은 134,217,728바이트(128MB)의 로깅 메시지를 ATA 플래시(disk0)의 syslog 디렉터리에 구성하며 16,384바이트의 파일 크기를 지정합니다.

```
logging buffered
logging persistent url disk0:/syslog size 134217728 filesize 16384
```

ATA 디스크의 파일에 로깅 메시지를 쓰기 전에 Cisco IOS Software에서는 디스크 공간이 충분한지 확인합니다. 충분하지 않으면 가장 오래된 로깅 메시지 파일(타임스탬프 기준)이 삭제되며 현재 파일이 저장됩니다. 파일 이름 형식은 log_month:day:year::time입니다.

참고: ATA 플래시 드라이브에는 제한된 디스크 공간이 있으므로 저장된 데이터를 덮어쓰지 않도록 유지관리해야 합니다.

이 예에서는 유지관리 절차의 일부로 로깅 메시지를 라우터 ATA 플래시 디스크에서 FTP 서버 192.168.1.129의 외부 디스크로 복사하는 방법을 보여줍니다.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

이 기능에 대한 자세한 내용은 로컬 비휘발성 스토리지(ATA 디스크)에 로깅을 참조하십시오.

로깅 레벨:

Cisco IOS 디바이스에서 생성한 각 로그 메시지에는 레벨 0, 긴급부터 레벨 7, 디버그에 이르는 8가지 심각도 중 하나가 할당됩니다. 특별히 필요한 경우가 아니면 레벨 7의 로깅은 피하는 것이 좋습니다. 레벨 7의 로깅을 수행하면 디바이스의 CPU 로드가 높아지므로 디바이스와 네트워크가 불안정해질 수 있습니다.

원격 syslog 서버에 전송할 로깅 메시지를 지정하기 위해 전역 환경 설정 명령어 **logging trap** 레벨을 사용합니다. 지정된 레벨은 심각도가 가장 낮은 전송 메시지를 표시합니다. 버퍼링된 로깅을 위해 **logging buffered** 레벨 명령어를 사용합니다.

다음 컨피그레이션 예제는 원격 syslog 서버에 보낸 로그 메시지와 로컬 로그 버퍼를 심각도 6(정보)부터 0(긴급)까지로 제한합니다.

```
!

logging trap 6
logging buffered 6
!
```

자세한 내용은 트러블슈팅, 결함 관리 및 로깅을 참조하십시오.

콘솔 또는 모니터 세션에 기록하지 않음

Cisco IOS Software를 사용하면 로그 메시지를 모니터 세션과 콘솔에 전송할 수 있습니다. 모니터 세션은 EXEC 명령어 **terminal monitor**가 실행된 인터랙티브 관리 세션입니다. 그러나 IOS 디바이스의 CPU 로드가 증가할 수 있으므로 권장되지 않습니다. 대신 **show logging** 명령어를 사용하여 볼 수 있는 로컬 로그 버퍼에 로깅 정보를 전송하는 것이 좋습니다.

콘솔 및 모니터 세션에 로깅을 비활성화하려면 전역 환경 설정 명령어 **no logging console** 및 **no logging monitor**를 사용합니다. 다음 컨피그레이션 예에서는 이러한 명령어의 사용을 보여줍니다.

```
!

no logging console
no logging monitor
!
```

전역 환경 설정 명령어에 대한 자세한 내용은 Cisco IOS 네트워크 관리 명령어 참조를 참고하십시오.

버퍼링된 로깅 사용

Cisco IOS Software에서는 관리자가 로컬에서 생성한 로그 메시지를 볼 수 있도록 로컬 로그 버퍼 사용을 지원합니다. 콘솔 또는 모니터 세션에 로깅하는 것보다 버퍼링된 로깅을 사용하는 것이 훨씬 좋습니다.

버퍼링된 로깅을 구성할 때 적절한 두 가지 컨피그레이션 옵션은 버퍼에 저장되는 메시지 심각도와 로깅 버퍼 크기입니다. **로깅 버퍼**의 크기는 전역 환경 설정 명령어 **logging buffered** 크기로 구성합니다. 버퍼에 포함된 가장 낮은 심각도는 logging buffered 심각도 명령어로 구성합니다. 관리자가 **show logging** EXEC 명령어를 통해 로깅 버퍼의 콘텐츠를 볼 수 있습니다.

다음 컨피그레이션 예에는 레벨 0(긴급)부터 6(정보)까지의 메시지가 저장됨을 나타내는 심각도 6, 정보 외에도 16384바이트의 로깅 버퍼 컨피그레이션이 포함되어 있습니다.

```
!

logging buffered 16384 6

!
```

버퍼링된 로깅에 대한 자세한 내용은 Cisco IOS 네트워크 관리 명령어 참조를 참고하십시오.

로깅 소스 인터페이스 구성

로그 메시지를 수집하고 검토할 때 향상된 레벨의 일관성을 제공하려면 로깅 소스 인터페이스를 정적으로 구성하는 것이 좋습니다. **logging source-interface** 인터페이스 명령어를 통해 정적으로 로깅 소스 인터페이스를 구성하면 개별 Cisco IOS 디바이스에서 보낸 모든 로깅 메시지에 동일한 IP 주소가 표시됩니다. 안정성을 강화하려면 루프백 인터페이스를 로깅 소스로 사용하는 것이 좋습니다.

이 컨피그레이션 예제에서는 모든 로그 메시지에 루프백 0 인터페이스의 IP 주소를 사용하도록 지정하기 위해 **logging source-interface** 인터페이스 전역 환경 설정 명령어 사용법에 대해 설명합니다.

```
!
logging source-interface Loopback 0
!
```

자세한 내용은 Cisco IOS 명령어 참조를 참고하십시오.

로깅 타임스탬프 구성

로깅 타임스탬프 컨피그레이션은 네트워크 디바이스 전체의 이벤트 상관관계를 지정하는 데 도움이 됩니다. 로깅 데이터 상관관계를 지정할 수 있으려면 정확하고 일관된 로깅 타임스탬프 컨피그레이션을 구현해야 합니다. 밀리초 정밀도의 날짜 및 시간을 포함하고 디바이스에서 사용 중인 시간대를 포함하도록 로깅 타임스탬프를 구성해야 합니다.

다음 예제에는 UTC(Coordinated Universal Time) 시간대에 속한 밀리초 정밀도의 로깅 타임스탬프 컨피그레이션이 포함되어 있습니다.

```
!
service timestamps log datetime msec show-timezone
!
```

UTC에 대해 시간을 기록하지 않으려는 경우 특정 로컬 시간대를 구성하고 해당 정보가 생성된 로그 메시지에 표시되도록 구성할 수 있습니다. 다음 예제는 PST(Pacific Standard Time) 시간대의 디바이스 컨피그레이션을 보여줍니다.

```
!

clock timezone PST -8
service timestamps log datetime msec localtime show-timezone
!
```

Cisco IOS Software 컨피그레이션 관리

Cisco IOS Software에는 Cisco IOS 디바이스에서 컨피그레이션 관리 형식을 활성화할 수 있는 여러 기능이 있습니다. 이러한 기능에는 컨피그레이션을 아카이브하고 컨피그레이션을 이전 버전으로 롤백하며 자세한 컨피그레이션 변경 로그를 생성하는 기능도 포함됩니다.

컨피그레이션 교체 및 컨피그레이션 롤백

Cisco IOS Software Release 12.3(7)T 이상에서 컨피그레이션 교체 및 컨피그레이션 롤백 기능을 사용하면 디바이스에서 Cisco IOS 디바이스 컨피그레이션을 아카이브할 수 있습니다. 현재 실행 중인 컨피그레이션을 **configure replace** 파일 이름 명령어로 교체하려면 수동 또는 자동으로 저장된 이 아카이브의 컨피그레이션을 사용할 수 있습니다. 이 명령어는 **copy** 파일 이름 **running-config** 명령어와 반대입니다. **configure replace** 파일 이름 명령어는 **copy** 명령어를 통해 수행하는 병합과 반대로 실행 중인 컨피그레이션을 교체합니다.

네트워크의 모든 Cisco IOS 디바이스에서 이 기능을 활성화하는 것이 좋습니다. 활성화한 후에는 관리자가 **archive config** 권한 부여된 EXEC 명령어를 사용하여 현재 실행 중인 컨피그레이션을 아카이브에 추가하도록 할 수 있습니다. 아카이브된 컨피그레이션은 **show archive** EXEC 명령어로 볼 수 있습니다.

이 예에서는 자동 컨피그레이션 아카이브의 구성을 설명합니다. 이 예에서는 관리자가 **write memory** EXEC 명령어를 실행할 때 disk0: 파일 시스템에 archived-config-N이라는 파일로 아카이브된 컨피그레이션을 저장하고, 최대 14개의 백업을 유지관리하며, 하루에 한 번(1440분) 아카이브하도록 Cisco IOS 디바이스에 지시합니다.

```
!

archive
 path disk0:archived-config
 maximum 14
 time-period 1440
 write-memory
!
```

컨피그레이션 아카이브 기능을 통해 최대 14개의 백업 컨피그레이션을 저장할 수 있지만 **maximum** 명령어를 사용하기 전에 공간 요구 사항을 고려하는 것이 좋습니다.

전용 컨피그레이션 변경 액세스

Cisco IOS Software Release 12.3(14)T에 추가된 전용 컨피그레이션 변경 액세스(Exclusive Configuration Change Access) 기능을 사용하면 한 명의 관리자만 지정된 시간에 Cisco IOS 디바이스의 컨피그레이션을 변경할 수 있습니다. 이 기능을 사용하면 관련 컨피그레이션 구성요소를 동시에 변경하는 데 따른 원치 않는 영향을 없앨 수 있습니다. 이 기능은 전역 환경 설정 명령어 **configuration mode exclusive** 모드로 구성되며 자동 및 수동의 두 가지 모드 중 하나에서 작동합니다. 자동 모드에서는 관리자가 **configure terminal** EXEC 명령어를 실행하면 컨피그레이션이 자동으로 잠깁니다. 수동 모드에서는 환경 설정 모드가 되면 컨피그레이션을 잠그기 위해 관리자가 **configure terminal lock** 명령어를 사용합니다.

다음 예에서는 자동 컨피그레이션 잠금을 위한 이 기능의 컨피그레이션을 설명합니다.

```
!
configuration mode exclusive auto
!
```

Cisco IOS Software 복원력 컨피그레이션

Cisco IOS Software Release 12.3(8)T에 추가된 복원력 컨피그레이션(Resilient Configuration) 기능을 사용하면 현재 Cisco IOS 디바이스에서 사용되는 디바이스 컨피그레이션과 Cisco IOS Software 이미지의 사본을 안전하게 저장할 수 있습니다. 이 기능을 활성화하면 해당 백업 파일을 변경하거나 제거할 수 없습니다. 의도치 않거나 악의적으로 이러한 파일을 삭제하려는 시도를 방지하려면 이 기능을 활성화하는 것이 좋습니다.

```
!
secure boot-image
secure boot-config!
```

이 기능이 활성화된 후에는 삭제된 컨피그레이션 또는 Cisco IOS Software 이미지를 복원할 수 없습니다. 이 기능의 현재 실행 상태는 **show secure boot** EXEC 명령어를 사용하여 표시할 수 있습니다.

디지털 서명 Cisco 소프트웨어

Cisco 1900, 2900 및 3900 Series 라우터용 Cisco IOS Software Release 15.0(1)M에 추가된 디지털 서명 Cisco 소프트웨어(Digitally Signed Cisco Software) 기능을 사용하면 보안 비대칭(공개 키) 암호화를 통해 디지털로 서명되어 신뢰할 수 있는 Cisco IOS Software를 쉽게 사용할 수 있습니다.

디지털로 서명된 이미지는 암호화된(개인 키 사용) 해시를 수반합니다. 확인 시 디바이스에서 키 저장소에 포함된 키 중에서 해당하는 공용 키로 해시의 암호를 해독하고 이미지의 고유 해시도 계산합니다. 암호 해독된 해시가 계산된 이미지 해시와 일치하면 이미지가 변조되지 않은 것이므로 신뢰할 수 있습니다.

디지털로 서명된 Cisco 소프트웨어 키는 키의 유형과 버전으로 식별합니다. 키는 특수, 프로덕션 또는 롤오버 키 유형일 수 있습니다. 프로덕션 및 특수 키 유형에는 키를 취소하고 교체할 때마다 알파벳이 증가하는 연관된 키 버전이 있습니다. 디지털 서명 Cisco 소프트웨어 기능을 사용할 때 ROMMON과

일반 Cisco IOS 이미지는 모두 특수 또는 프로덕션 키로 서명합니다. ROMMON 이미지는 업그레이드할 수 있으므로 로드된 특수 또는 프로덕션 이미지와 동일한 키로 서명해야 합니다.

다음 명령어는 디바이스 키 저장소의 키로 플래시에 있는 c3900-universalk9-mz.SSA 이미지의 무결성을 검증합니다.

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```

디지털 서명 Cisco 소프트웨어 기능은 Cisco Catalyst 4500 E-Series Switch용 Cisco IOS XE Release 3.1.0.SG에도 통합되었습니다.

이 기능에 대한 자세한 내용은 디지털 서명 Cisco 소프트웨어를 참조하십시오.

Cisco IOS Software Release 15.1(1)T 이상에서 디지털 서명 Cisco 소프트웨어의 키 교체 기능이 도입되었습니다. 키 교체 및 취소를 수행하면 플랫폼의 키 스토리지에서 디지털 서명 Cisco 소프트웨어 확인에 사용되는 키를 교체하고 제거합니다. 키가 손상되는 경우 특수 키와 프로덕션 키만 취소할 수 있습니다.

(특수 또는 프로덕션) 이미지의 새로운 (특수 또는 프로덕션) 키는 이전 특수 키나 프로덕션 키를 취소하는 데 사용되는 (프로덕션 또는 취소) 이미지에 제공됩니다. 취소 이미지 무결성은 플랫폼에 미리 저장되어 제공되는 롤오버 키로 검증됩니다. 롤오버 키는 변경되지 않습니다. 프로덕션 키를 취소할 때 취소 이미지를 로드하고 나면 수반되는 새 키가 키 저장소에 추가되므로, ROMMON 이미지를 업그레이드하고 새 프로덕션 이미지를 부팅하기만 하면 해당 이전 키를 취소할 수 있습니다. 특수 키를 취소할 때 프로덕션 이미지가 로드됩니다. 이 이미지가 새 특수 키를 추가하고 이전 특수 키를 취소할 수 있습니다. ROMMON을 업그레이드한 후 새로운 특수 이미지를 부팅할 수 있습니다.

다음 예에서는 특수 키의 취소를 설명합니다. 다음 명령어는 현재 프로덕션 이미지에서 키 저장소에 새 특수 키를 추가하고, 새 ROMMON 이미지(C3900_rom-monitor.srec.SSB)를 스토리지 영역(usbflash0:)에 복사하며, ROMMON 파일을 업그레이드하고, 이전 특수 키를 취소합니다.

```
software authenticity key add special
copy tftp://192.168.1.129/C3900_rom-monitor.srec.SSB usbflash0:
upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
software authenticity key revoke special
```

그런 다음 새로운 특수 이미지(c3900-universalk9-mz.SSB)를 로딩할 플래시에 복사하고 새로 추가한 특수 키(.SSB)를 사용하여 이미지의 시그니처를 검증할 수 있습니다.

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```

Cisco IOS XE Software를 실행하는 Catalyst 4500 E-Series Switch에서는 디지털 서명 Cisco 소프트웨어 기능은 지원하지만, 키 취소 및 대체는 지원하지 않습니다.

이 기능에 대한 자세한 내용은 디지털 서명 Cisco 소프트웨어 가이드의 디지털 서명 Cisco 소프트웨어 키 취소 및 교체 섹션을 참조하십시오.

컨피그레이션 변경 알림 및 로깅

Cisco IOS Software Release 12.3(4)T에 추가된 컨피그레이션 변경 알림 및 로깅(Configuration Change Notification and Logging) 기능을 사용하면 Cisco IOS 디바이스의 컨피그레이션 변경을 기록할 수 있습니다. 로그는 Cisco IOS 디바이스에서 유지관리되며 변경한 개인의 사용자 정보, 입력한 환경 설정 명령어 및 변경된 시간을 포함합니다. 이 기능은 **logging enable** 컨피그레이션 변경 로거 환경 설정 모드 명령어로 활성화합니다. 선택적 명령어 **hidekeys** 및 **logging size** 항목은 비밀번호 데이터의 기록을 방지하고 변경 로그의 길이를 늘리므로 기본 컨피그레이션을 향상시키는 데 사용됩니다.

Cisco IOS 디바이스의 컨피그레이션 변경 이력을 쉽게 이해할 수 있도록 이 기능을 활성화하는 것이 좋습니다. 또한 컨피그레이션을 변경할 때 syslog 메시지의 생성을 지원하기 위해 **notify syslog** 환경 설정 명령어를 사용하는 것이 좋습니다.

```
!

archive
 log config
  logging enable
  logging size 200
 hidekeys
  notify syslog
!
```

컨피그레이션 변경 알림 및 로깅 기능을 활성화한 후, 컨피그레이션 로그를 보기 위해 권한 부여된 EXEC 명령어 **show archive log config all**을 사용할 수 있습니다.

컨트롤 플레인

컨트롤 플레인 기능은 소스에서 대상으로 데이터를 이동하기 위해 네트워크 디바이스 간에 통신하는 프로토콜과 프로세스로 구성됩니다. 여기에는 ICMP 및 RSVP(Resource Reservation Protocol)와 같은 프로토콜 외에도 BGP(Border Gateway Protocol) 등의 라우팅 프로토콜이 포함되어 있습니다.

관리 및 데이터 플레인의 이벤트가 컨트롤 플레인에 부정적인 영향을 미치지 않아야 합니다. DoS 공격과 같은 데이터 플레인 이벤트가 컨트롤 플레인에 영향을 미치는 경우 전체 네트워크가 불안정해질 수 있습니다. Cisco IOS Software 기능 및 컨피그레이션에 대한 정보를 사용하면 컨트롤 플레인의 복원력을 보장할 수 있습니다.

일반 컨트롤 플레인 강화

컨트롤 플레인을 통해 관리 플레인과 데이터 플레인이 유지관리되고 작동하므로 네트워크 디바이스의 컨트롤 플레인을 보호해야 합니다. 보안 사고 중에 컨트롤 플레인이 불안정하게 되면 네트워크의 안정성을 복구할 수 없습니다.

불필요한 패킷을 처리하는 데 필요한 CPU 로드 양을 최소화하기 위해 대부분의 경우 인터페이스에서 특정 유형의 메시지 수신 및 전송을 비활성화할 수 있습니다.

IP ICMP 리디렉션

동일한 인터페이스에서 패킷을 수신하고 전송할 때 라우터에서 ICMP 리디렉션 메시지를 생성할 수 있습니다. 이 경우, 라우터는 패킷을 전달하고 원래 패킷의 발신자에게 ICMP 리디렉션 메시지를 다시 전송합니다. 이 행동을 통해 발신자가 라우터를 우회하고 추가 패킷을 대상(또는 대상에 가까운 라우터)에 직접 전달할 수 있습니다. 제대로 작동하는 IP 네트워크에서는 라우터가 고유 로컬 서브넷에 있는 호스트에만 리디렉션을 전송합니다. 즉, ICMP 리디렉션은 레이어 3 경계를 넘어 이동하지 않아야 합니다.

ICMP 리디렉션 메시지에는 호스트 주소용 리디렉션과 전체 서브넷용 리디렉션의 두 가지 유형이 있습니다. 악의적인 사용자가 패킷을 계속 라우터에 전송하여 ICMP 리디렉션을 전송하는 라우터의 기능을 악용할 수 있습니다. 그러면 라우터가 ICMP 리디렉션 메시지에 응답해야 하므로 라우터의 성능과 CPU에 부정적인 영향을 미칠 수 있습니다. 라우터에서 ICMP 리디렉션을 전송하지 않게 하려면 **no ip redirects** 인터페이스 환경 설정 명령어를 사용하십시오.

ICMP 연결 불가능

인터페이스 액세스 목록으로 필터링하면 ICMP 연결 불가능 메시지를 필터링된 트래픽의 소스에 다시 전송합니다. 이러한 메시지를 생성하면 디바이스의 CPU 사용률이 증가할 수 있습니다. Cisco IOS Software에서 ICMP 연결 불가능 생성은 기본적으로 500밀리초마다 하나의 패킷으로 제한됩니다. ICMP 연결 불가능 메시지 생성은 인터페이스 환경 설정 명령어 **no ip unreachables**로 비활성화할 수 있습니다. ICMP 연결 불가능 속도 제한은 **ip icmp rate-limit unreachable** interval-in-ms 전역 환경 설정 명령어를 사용하여 기본값에서 다른 값으로 변경할 수 있습니다.

프록시 ARP

프록시 ARP는 일반적으로 라우터인 한 디바이스에서 다른 디바이스를 위한 ARP 요청에 응답하는 기술입니다. 라우터에서는 신원을 "위조"하여 실제 대상으로 패킷을 라우팅해야 하는 작업을 승인합니다. 프록시 ARP는 라우팅 또는 기본 게이트웨이를 구성하지 않고 서브넷의 머신이 원격 서브넷에 연결되도록 지원할 수 있습니다. 프록시 ARP는 RFC 1027에 정의되어 있습니다.

프록시 ARP를 이용하는 경우 몇 가지 단점이 있습니다. 네트워크 세그먼트의 ARP 트래픽 양, 리소스 소모 및 중간자 공격(man-in-the-middle attack)이 증가할 수 있습니다. 프록시된 각 ARP 요청에서는 적은 양의 메모리를 사용하므로 프록시 ARP는 리소스 소모 공격 벡터를 나타냅니다. 공격자가 다수의 ARP 요청을 전송하는 경우 사용 가능한 모든 메모리를 소진할 수 있습니다.

중간자 공격(man-in-the-middle attack)은 네트워크의 호스트를 사용하여 라우터의 MAC 주소를 스푸핑하므로, 결국 의심하지 않는 호스트가 공격자에게 트래픽을 전송하게 됩니다. 프록시 ARP는 인터페이스 환경 설정 명령어인 **no ip proxy-arp**로 비활성화할 수 있습니다.

이 기능에 대한 자세한 내용은 프록시 ARP 활성화를 참조하십시오.

컨트롤 플레인 트래픽의 CPU 영향 제한

컨트롤 플레인을 보호하는 것은 매우 중요합니다. 데이터와 관리 트래픽이 없어도 애플리케이션 성능과 최종 사용자 경험이 저하될 수 있으므로 컨트롤 플레인의 복원력을 통해 다른 두 플레인이 유지관리되고 작동할 수 있습니다.

컨트롤 플레인 트래픽 이해

Cisco IOS 디바이스의 컨트롤 플레인을 적절히 보호하려면 CPU에서 프로세스를 전환하는 트래픽 유형을 이해하는 것이 중요합니다. 프로세스 전환 트래픽은 일반적으로 두 가지 유형의 트래픽으로 구성됩니다. 첫 번째 트래픽 유형은 Cisco IOS 디바이스로 향하며 Cisco IOS 디바이스 CPU에서 직접 처리해야 합니다. 이 트래픽은 다음 카테고리로 구성됩니다.

- **수신 인접 트래픽** - 이 트래픽에는 다음 라우터 홉이 디바이스 자체인 CEF(Cisco Express Forwarding) 표의 항목을 포함합니다. 이 항목은 **show ip cef** CLI 출력에 수신된 용어로 표시됩니다. 이 표시는 인터페이스 IP 주소, 멀티캐스트 주소 공간 및 브로드캐스트 주소 공간을 포함하는 Cisco IOS 디바이스 CPU에서 직접 처리해야 하는 IP 주소입니다.

CPU에서 처리되는 두 번째 트래픽 유형은 CPU에서 특별히 처리해야 하는 데이터 플레인 트래픽입니다. 이 트래픽에는 Cisco IOS 디바이스 자체를 넘어선 대상이 있습니다. 데이터 플레인 트래픽에 영향을 미치는 전체 CPU 목록은 아니지만 이러한 유형의 트래픽은 프로세스 전환 트래픽이므로 컨트로로 플레인의 운영에 영향을 미칠 수 있습니다.

- **액세스 제어 목록 로깅** - ACL 로깅 트래픽은 log 키워드를 사용하는 ACE가 일치(허용 또는 거부)하여 생성된 패킷으로 구성됩니다.

- **유니캐스트 RPF(Unicast Reverse Path Forwarding)** - ACL과 함께 사용되는 유니캐스트 RPF를 사용하면 특정 패킷의 프로세스가 전환될 수 있습니다.
- **IP 옵션** - 포함된 옵션이 있는 모든 IP 패킷은 CPU에서 처리되어야 합니다.
- **프래그멘테이션** - 프래그멘테이션이 필요한 모든 IP 패킷은 처리를 위해 CPU에 전달해야 합니다.
- **TTL(Time-to-live) 만료** - TTL 값이 1 이하인 패킷에는 전송할 ICMP(Internet Control Message Protocol) 시간 초과(ICMP 유형 11, 코드 0) 메시지가 있으므로, CPU 처리가 수행됩니다.
- **ICMP 연결 불가능** - 라우팅, MTU 또는 필터링으로 인해 ICMP 연결 불가능 메시지를 생성하는 패킷은 CPU에서 처리합니다.
- **ARP 요청이 필요한 트래픽** - ARP 항목이 없는 대상은 CPU에서 처리해야 합니다.
- **비IP 트래픽** - 모든 비IP 트래픽은 CPU에서 처리합니다.

이 목록에는 Cisco IOS 디바이스 CPU에서 처리 중인 트래픽 유형을 판별하는 몇 가지 방법이 자세히 설명되어 있습니다.

- **show ip cef** 명령어는 CEF 표에 포함되어 있는 각 IP 접두사에 대한 다음 홉 정보를 제공합니다. 앞서 표시된 대로 "다음 홉"으로 수신을 포함하는 항목은 수신 인접성으로 간주되며 트래픽을 CPU에 직접 보내야 함을 나타냅니다.
- **show interface switching** 명령어는 디바이스에서 프로세스를 전환한 패킷 수에 대한 정보를 제공합니다.
- **show ip traffic** 명령어는 다음과 같은 IP 패킷 수에 대한 정보를 제공합니다.
    - ♦ 로컬 대상(즉, 수신 인접 트래픽) 포함
    - ♦ 옵션 포함
    - ♦ 프래그멘테이션 필요
    - ♦ 브로드캐스트 주소 공간에 전송
    - ♦ 멀티캐스트 주소 공간에 전송
- 수신 인접 트래픽은 **show ip cache flow** 명령어를 사용하여 식별할 수 있습니다. Cisco IOS 디바이스를 대상으로 하는 모든 플로우에는 로컬의 DstIf(Destination Interface)가 있습니다.
- **컨트롤 플레인 정책**은 Cisco IOS 디바이스의 컨트롤 플레인에 도달하는 트래픽 유형과 속도를 식별하는 데 사용할 수 있습니다. 컨트롤 플레인 정책은 세분화된 분류 ACL 사용, 로깅 및 **show policy-map control-plane** 명령어를 사용하여 수행할 수 있습니다.

인프라 ACL

iACL(Infrastructure ACL)은 네트워크 디바이스에 대한 외부 통신을 제한합니다. 인프라 ACL은 이 문서의 인프라 ACL을 사용하여 네트워크에 대한 액세스 제한 섹션에서 광범위하게 다룹니다.

모든 네트워크 디바이스의 컨트롤 플레인을 보호하려면 iACL을 구현하는 것이 좋습니다.

수신 ACL

분산 플랫폼에서 rACL(Receive ACL)은 Cisco IOS Software Releases 12.0(21)S2(12000 (GSR)의 경우), 12.0(24)S(7500의 경우) 및 12.0(31)S(10720의 경우)의 옵션일 수 있습니다. rACL은 트래픽이 RP(Route Processor)에 영향을 미치기 전에 유해한 트래픽으로부터 디바이스를 보호합니다. 수신 ACL은 구성된 디바이스만 보호하도록 설계되어 있으며 통과 트래픽은 rACL의 영향을 받지 않습니다. 결과적으로 아래 예제 ACL 항목에 사용된 대상 IP 주소는 라우터의 물리적 IP 주소나 가상 IP 주소만 참조합니다. 수신 ACL은 네트워크 보안 모범 사례로 간주되므로 우수한 네트워크 보안을 위해 장기간 추가해야 합니다.

다음은 192.168.100.0/24 네트워크의 신뢰할 수 있는 호스트에서 SSH(TCP 포트 22) 트래픽을 허용하도록 작성된 수신 경로 ACL입니다.

```
!
!--- Permit SSH from trusted hosts allowed to the device.
!

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22
!
!--- Deny SSH from all other sources to the RP.
!

access-list 151 deny tcp any any eq 22
!
!--- Permit all other traffic to the device.
!--- according to security policy and configurations.
!

access-list 151 permit ip any any
!
!--- Apply this access list to the receive path.
!

ip receive access-list 151
!
```

디바이스에 대한 합법적인 트래픽을 식별하여 허용하고, 원치 않는 패킷은 모두 거부하는 데 도움이 되도록 GSR: 수신 액세스 제어 목록을 참조하십시오.

컨트롤 플레인 정책

인프라 디바이스를 대상으로 하는 IP 패킷을 제한하는 데 CoPP(Control Plane Policing, 컨트롤 플레인 정책) 기능을 사용할 수 있습니다. 이 예에서는 신뢰할 수 있는 호스트의 SSH 트래픽만 Cisco IOS 디바이스 CPU에 도달할 수 있습니다.

참고: 알 수 없거나 신뢰할 수 없는 IP 주소에서 트래픽을 삭제하면 동적으로 할당된 IP 주소를 사용하는 호스트가 Cisco IOS 디바이스에 연결되는 것을 방지할 수 있습니다.

```
!

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22
access-list 152 permit tcp any any eq 22
access-list 152 deny ip any any
!


class-map match-all COPP-KNOWN-UNDESIRABLE
 match access-group 152
!

policy-map COPP-INPUT-POLICY
 class COPP-KNOWN-UNDESIRABLE
  drop
!

control-plane
 service-policy input COPP-INPUT-POLICY
!
```

이전 CoPP 예에서 무단 패킷을 허용 작업과 일치시키는 ACL 항목은 정책 맵 삭제 기능을 통해 해당 패킷을 버리는 반면 거부 작업과 일치하는 패킷은 정책 맵 삭제 기능의 영향을 받지 않습니다.

CoPP는 일련의 Cisco IOS Software Release 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 및 12.4T에서 사용할 수 있습니다.

CoPP 기능의 컨피그레이션 및 사용에 대한 자세한 내용은 컨트롤 플레인 정책 구축을 참조하십시오.

컨트롤 플레인 보호

Cisco IOS Software Release 12.4(4)T에 도입된 CPPr(Control Plane Protection)은 Cisco IOS 디바이스의 CPU를 대상으로 하는 컨트롤 플레인 트래픽을 제한하거나 감시하는 데 사용할 수 있습니다. CPPr은 CoPP와 비슷하지만, 더 세분화하여 트래픽을 제한하는 기능이 있습니다. CPPr은 통합 컨트롤 플레인을 하위 인터페이스라고 하는 개별 컨트롤 플레인 카테고리로 나눕니다. 호스트(Host), 통과(Transit) 및 CEF 예외(CEF-Exception) 트래픽 카테고리에는 하위 인터페이스가 있습니다. CPPr에는 다음과 같은 컨트롤 플레인 보호 기능도 포함됩니다.

- **포트 필터링 기능** - 이 기능을 사용하면 폐쇄되거나 수신하지 않는 TCP 및 UDP 포트로 보내는 패킷을 삭제하고 감시할 수 있습니다.
- **큐 임계값 지정 기능** - 이 기능을 사용하면 컨트롤 플레인 IP 입력 큐에서 허용되는 지정된 프로토콜의 패킷 수를 제한합니다.

CPPr 기능 컨피그레이션 및 사용에 대한 자세한 내용은 컨트롤 플레인 보호 및 컨트롤 플레인 보호 이해를 참조하십시오.

하드웨어 레이트 리미터

Cisco Catalyst 6500 Series Supervisor Engine 32 및 Supervisor Engine 720에서는 특수 네트워킹 시나리오를 위해 플랫폼별 HWRL(Hardware-based Rate Limiter)을 지원합니다. 이 하드웨어 레이트 리미터는 특정하게 사전 정의된 IPv4, IPv6, 유니캐스트 및 멀티캐스트 DoS 시나리오 세트를 처리하므로 특수 케이스 레이트 리미터라고도 합니다. HWRL은 CPU에서 패킷을 처리해야 하는 다양한 공격으로부터 Cisco IOS 디바이스를 보호할 수 있습니다.

기본적으로 활성화되는 몇 가지 HWRL이 있습니다. 자세한 내용은 PFC3 하드웨어 기반 레이트 리미터 기본 설정을 참조하십시오.

HWRL에 대한 자세한 내용은 PFC3에 대한 하드웨어 기반 레이트 리미터를 참조하십시오.

보안 BGP

BGP(Border Gateway Protocol)는 인터넷의 라우팅 기반입니다. 따라서 연결 요구 사항이 정상보다 많은 조직에서는 종종 BGP를 사용합니다. BGP는 편재성을 비롯한 소규모 조직의 BGP 컨피그레이션에 존재하는 "설정 후 자동 설치(set and forget)"되는 특성 때문에 공격자의 목표가 되는 경우가 많습니다. 그러나 BGP 컨피그레이션의 보안을 강화하는 데 활용할 수 있는 BGP별 보안 기능이 많이 있습니다.

여기에서는 가장 중요한 BGP 보안 기능의 개요를 제공합니다. 해당하는 경우 컨피그레이션 권장 사항이 있습니다.

TTL 기반 보안 보호

각 IP 패킷에는 TTL(Time-To-Live)이라고 하는 1바이트 필드가 있습니다. IP 패킷이 통과하는 각 디바이스에서 이 값이 1만큼씩 감소됩니다. 시작 값은 운영 체제에 따라 다르며 일반적으로 범위는 64에서 255까지입니다. TTL 값이 0이 되면 패킷이 삭제됩니다.

GTSM(Generalized TTL-based Security Mechanism) 및 BTSH(BGP TTL Security Hack) 둘 다로 알려진 TTL 기반 보안 보호에서는 BGP 패킷이 직접 연결된 피어에서 수신될 수 있도록 IP 패킷의 TTL 값을 활용합니다. 이 기능은 종종 피어링 라우터에서 조정해야 하지만, 활성화고 나면 BGP에 대한 여러 TCP 기반 공격을 완벽하게 차단할 수 있습니다.

BGP용 GTSM은 **neighbor** BGP 라우터 환경 설정 명령어의 **ttl-security** 옵션을 사용하여 활성화됩니다. 다음 예에서는 이 기능의 컨피그레이션을 설명합니다.

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> ttl-security hops <hop-count>
!
```

BGP 패킷을 받으면 TTL 값을 확인합니다. 이 값은 255에서 지정된 홉 수를 뺀 값 이상이어야 합니다.

MD5로 BGP 피어 인증

MD5를 사용하여 피어를 인증하면 BGP 세션의 일부로 보낸 각 패킷의 MD5 요약이 생성됩니다. 특히 다이제스트를 생성하기 위해 IP 및 TCP 헤더의 일부, TCP 페이로드 및 암호 키를 사용합니다.

생성된 요약은 RFC 2385에서 특별히 이 용도로 생성한 TCP 옵션 19 유형에 저장됩니다. 수신 BGP 스피커에서는 동일한 알고리즘과 암호 키를 사용하여 메시지 다이제스트를 다시 생성합니다. 수신되어 계산된 다이제스트가 같지 않으면 패킷을 버립니다.

MD5를 사용한 피어 인증은 **neighbor** BGP 라우터 환경 설정 명령어의 **password** 옵션을 사용하여 구성합니다. 이 명령어의 사용법은 다음에 설명되어 있습니다.

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> password <secret>
!
```

MD5를 사용한 BGP 피어 인증에 대한 자세한 내용은 네이버 라우터 인증을 참조하십시오.

최대 접두사 구성

BGP 접두사는 라우터에서 메모리에 저장합니다. 라우터에서 보유해야 하는 접두사가 많을수록 BGP에서 더 많은 메모리를 사용해야 합니다. 사업자의 고객 네트워크에 대해 하나 이상의 기본 경로만 사용하는 컨피그레이션과 같이 일부 컨피그레이션에서는 모든 인터넷 접두사의 하위 집합만 저장할 수 있습니다.

메모리 소모를 방지하려면 피어별로 허용되는 접두사의 최대 수를 구성하는 것이 중요합니다. BGP 피어별로 한계를 구성하는 것이 좋습니다.

neighbor maximum-prefix BGP 라우터 환경 설정 명령어를 사용하여 이 기능을 구성할 때 하나의 인수, 즉 피어를 종료하기 전에 허용되는 접두사의 최대 수가 필요합니다. 또는 1에서 100까지의 수를 입력할 수도 있습니다. 이 수는 로그 메시지를 보내는 시점의 최대 접두사의 백분율 값을 나타냅니다.

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>
!
```

피어당 최대 접두사에 대한 자세한 내용은 BGP 최대 접두사 기능 구성을 참조하십시오.

접두사 목록으로 BGP 접두사 필터링

네트워크 관리자가 BGP를 통해 보내거나 받는 특정 접두사를 허용하거나 거부하는 데 접두사 목록을 사용할 수 있습니다. 대상 경로를 통해 네트워크 트래픽을 보낼 수 있도록 가능한 경우 접두사 목록을 사용해야 합니다. 인바운드와 아웃바운드 방향 모두로 각 eBGP 피어에 접두사 목록을 적용해야 합니다.

구성된 접두사 목록은 보내거나 받을 접두사를 네트워크 라우팅 정책에서 특별히 허용되는 접두사로 한정합니다. 수신된 접두사 수가 커서 이와 같이 한정할 수 없는 경우 알려진 잘못된 접두사를 특별히 차단하도록 접두사 목록을 구성해야 합니다. 이와 같이 알려진 잘못된 접두사에는 RFC 3330에서 내부용 또는 테스트용으로 예약한 네트워크 및 할당되지 않은 IP 주소 공간이 있습니다. 조직에서 알리려는 접두사만 특별히 허용하도록 아웃바운드 접두사 목록을 구성해야 합니다.

이 컨피그레이션 예에서는 파악하여 알릴 경로를 제한하기 위해 접두사 목록을 사용합니다. 접두사 목록 BGP-PL-INBOUND에서는 기본 경로만 허용되며, GP-PL-OUTBOUND에서 알리도록 허용된 경로는 접두사 192.168.2.0/24뿐입니다.

```
!

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0
ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24
!

router bgp <asn>
 neighbor <ip-address> prefix-list BGP-PL-INBOUND in
 neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out
!
```

BGP 접두사 필터링의 전체 범위는 외부 BGP를 사용하여 통신 사업자에 연결을 참조하십시오.

자동 시스템 경로 액세스 목록으로 BGP 접두사 필터링

BGP AS(Autonomous System) 경로 액세스 목록을 사용하면 접두사의 AS 경로 속성을 기반으로 수신되고 알려진 접두사를 필터링할 수 있습니다. 이 목록은 강력한 필터링 집합을 설정하기 위해 접두사 목록과 함께 사용할 수 있습니다.

이 컨피그레이션 예에서는 원격 AS에서 시작된 접두사로 인바운드 접두사를 제한하고 로컬 자동 시스템에서 시작한 접두사로 아웃바운드 접두사를 제한하기 위해 AS 경로 액세스 목록을 사용합니다. 기타 모든 자동 시스템에서 제공하는 접두사는 필터링되어 라우팅 테이블에 설치되지 않습니다.

```
!

ip as-path access-list 1 permit ^65501$
ip as-path access-list 2 permit ^$
!

router bgp <asn>
 neighbor <ip-address> remote-as 65501
 neighbor <ip-address> filter-list 1 in
 neighbor <ip-address> filter-list 2 out
!
```

보안 내부 게이트웨이 프로토콜

네트워크에서 적절하게 트래픽을 전달하고 토폴로지 변경 또는 결함으로부터 복구하는 기능은 정확한 토폴로지 보기에 따라 달라집니다. 이 보기를 제공하기 위해 종종 IGP(Interior Gateway Protocol)를 실행할 수 있습니다. 기본적으로 IGP는 동적이며 사용 중인 특정 IGP와 통신하는 추가 라우터를 검색합니다. IGP에서는 네트워크 링크 장애 시 사용할 수 있는 경로도 검색합니다.

이러한 하위 섹션에서는 가장 중요한 IGP 보안 기능의 개요를 제공합니다. 적절한 경우, RIPv2(Routing Information Protocol Version 2), EIGRP(Enhanced Interior Gateway Routing Protocol) 및 OSPF(Open Shortest Path First)를 포함하는 권장 사항과 예가 제공됩니다.

Message Digest 5로 라우팅 프로토콜 인증 및 검증

라우팅 정보를 안전하게 교환하지 못하면 공격자가 네트워크에 잘못된 라우팅 정보를 전달할 수 있습니다. 라우터 간 라우팅 프로토콜에서 비밀번호 인증을 사용하여 네트워크 보안을 강화할 수 있습니다. 그러나 이 인증은 일반 텍스트로 전송되므로 공격자가 간단하게 이 보안 제어를 파괴할 수 있습니다.

MD5 해시 기능을 인증 프로세스에 추가하면 라우팅 업데이트에 더 이상 일반 텍스트 비밀번호가 포함되지 않으며, 라우팅 업데이트의 전체 콘텐츠를 부정하게 변경하기가 어려워집니다. 그러나, 보안이 약한 비밀번호를 선택하면 MD5 인증을 사용해도 여전히 무차별 대입 공격과 사전 공격을 받을 수 있습니다. 충분하게 무작위로 추출할 수 있는 비밀번호를 사용하는 것이 좋습니다. MD5 인증은 비밀번호 인증과 비교하여 훨씬 안전하므로 이러한 예는 MD5 인증에만 해당합니다. 라우팅 프로토콜을 검증하고 보호하기 위해 IPSec를 사용할 수도 있지만, 이러한 예에서는 사용을 자세히 설명하지 않습니다.

EIGRP 및 RIPv2에서는 컨피그레이션의 일부로 키 체인을 사용합니다. 키 체인 컨피그레이션 및 사용에 대한 자세한 내용은 키를 참조하십시오.

다음은 MD5를 사용한 EIGRP 라우터 인증의 예제 컨피그레이션입니다.

```
!

key chain <key-name>
 key <key-identifier>
 key-string <password>

!

interface <interface>
 ip authentication mode eigrp <as-number> md5
 ip authentication key-chain eigrp <as-number> <key-name>
!
```

다음은 RIPv2의 MD5 라우터 인증 컨피그레이션 예입니다. RIPv1에서는 인증을 지원하지 않습니다.

```
!

key chain <key-name>
 key <key-identifier>
 key-string <password>
!

interface <interface>
 ip rip authentication mode md5
 ip rip authentication key-chain <key-name>
!
```

다음은 MD5를 사용한 OSPF 라우터 인증의 예제 컨피그레이션입니다. OSPF에서는 키 체인을 사용하지 않습니다.

```
!

interface <interface>
 ip ospf message-digest-key <key-id> md5 <password>
!

router ospf <process-id>
 network 10.0.0.0 0.255.255.255 area 0
 area 0 authentication message-digest
!
```

자세한 내용은 OSPF 구성을 참조하십시오.

Passive-Interface 명령어

정보를 유출하거나 IGP에 거짓 정보를 유입하는 것은 라우팅 정보 알림을 제어하는 데 도움이 되는 **passive-interface** 명령어를 통해 완화할 수 있습니다. 관리 제어 범위에 속하지 않은 네트워크에는 정보를 알리지 않는 것이 좋습니다.

다음 예에서는 이 기능의 사용을 설명합니다.

```
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
!
```

경로 필터링

네트워크에 거짓 라우팅 정보를 유입할 가능성을 줄이기 위해 경로 필터링을 사용해야 합니다. **passive-interface** 라우터 환경 설정 명령어와 달리 라우팅은 경로 필터링을 활성화한 후에 수행되지만, 알림 또는 처리된 정보는 제한됩니다.

EIGRP 및 RIP의 경우 **distribute-list** 명령어와 함께 **out** 키워드를 사용하면 알려지는 정보가 제한되는 반면 **in** 키워드를 사용하면 처리되는 업데이트가 제한됩니다. **distribute-list** 명령어는 OSPF에 사용 가능하지만 라우터가 필터링된 경로로 전파되는 것은 막지 못합니다. 대신 **area filter-list** 명령어를 사용할 수 있습니다.

다음 EIGRP 예에서는 **distribute-list** 명령어와 접두사 목록을 사용하여 아웃바운드 알림을 필터링합니다.

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
 distribute-list prefix <list-name> out <interface>
!
```

다음 EIGRP 예에서는 접두사 목록으로 인바운드 업데이트를 필터링합니다.

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
 distribute-list prefix <list-name> in <interface>
!
```

라우팅 업데이트 알림 및 처리를 제어하는 방법에 대한 자세한 내용은 IP 라우팅 프로토콜 독립 기능 구성을 참조하십시오.

다음 OSPF 예에서는 OSPF별 **area filter-list** 명령어와 접두사 목록을 사용합니다.

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router ospf <process-id>
 area <area-id> filter-list prefix <list-name> in
!
```

라우팅 프로세스 리소스 사용

라우팅 프로토콜 접두사는 라우터가 메모리에 저장하므로, 라우터가 보유해야 하는 접두사가 추가될 때마다 리소스 사용이 늘어납니다. 리소스 소진을 방지하려면 리소스 사용을 제한하도록 라우팅 프로토콜을 구성하는 것이 중요합니다. 링크 상태 데이터베이스 오버로드 보호(Link State Database Overload Protection) 기능을 사용하는 경우 OSPF에서 이 구성을 수행할 수 있습니다.

다음 예에서는 OSPF 링크 상태 데이터베이스 오버로드 보호 기능의 컨피그레이션을 설명합니다.

```
!

router ospf <process-id>
 max-lsa <maximum-number>
!
```

OSPF 링크 상태 데이터베이스 오버로드 보호에 대한 자세한 내용은 OSPF 프로세스의 자체 생성 LSA 수 제한을 참조하십시오.

보안 FHRP(First Hop Redundancy Protocol)

FHRP(First Hop Redundancy Protocol)는 기본 게이트웨이 역할을 수행하는 디바이스의 복원력과 이중화를 제공합니다. 레이어 3 디바이스 쌍에서 서버나 워크스테이션을 포함하는 VLAN 집합이나 네트워크 세그먼트의 기본 게이트웨이 기능을 제공하는 환경에서는 이러한 프로토콜과 조건이 일반적입니다.

GLBP(Gateway Load-Balancing Protocol), HSRP(Hot Standby Router Protocol) 및 VRRP(Virtual Router Redundancy Protocol)는 모두 FHRP입니다. 기본적으로 이 프로토콜은 무단 커뮤니케이션과 통신합니다. 이러한 유형의 통신을 사용하면 공격자가 FHRP 통신 디바이스를 가장하여 네트워크에서 기본 게이트웨이 역할을 수행할 수 있습니다. 이와 같이 인계받으면 공격자가 중간자 공격(man-in-the-middle attack)을 수행하여 네트워크에 있는 모든 사용자 트래픽을 가로챌 수 있습니다.

이 유형의 공격을 방지하려면 Cisco IOS Software에서 지원하는 모든 FHRP에 MD5 또는 텍스트 문자열과의 인증 호환성이 포함되어야 합니다. 무단 FHRP에서 제기하는 위협으로 인해 이러한 프로토콜의 인스턴스에서 MD5 인증을 사용하는 것이 좋습니다. 다음 컨피그레이션 예에서는 GLBP, HSRP 및 VRRP MD5 인증 사용에 대해 설명합니다.

```
!

interface FastEthernet 1
 description *** GLBP Authentication ***
 glbp 1 authentication md5 key-string <glbp-secret>
 glbp 1 ip 10.1.1.1
!

interface FastEthernet 2
 description *** HSRP Authentication ***
 standby 1 authentication md5 key-string <hsrp-secret>
 standby 1 ip 10.2.2.1
!

interface FastEthernet 3
 description *** VRRP Authentication ***
 vrrp 1 authentication md5 key-string <vrrp-secret>
 vrrp 1 ip 10.3.3.1
!
```

데이터 플레인

데이터 플레인에서 데이터를 소스에서 대상으로 이동하는 작업을 수행하지만, 보안 상황에서는 데이터 플레인이 세 플레인 중에서 중요도가 가장 떨어집니다. 따라서 네트워크 디바이스 보안을 설정할 때 데이터 플레인보다 관리 플레인과 컨트롤 플레인을 보호하는 것이 중요합니다.

그러나 데이터 플레인 자체에 트래픽을 보호하는 데 도움이 되는 여러 기능과 컨피그레이션 옵션이 있습니다. 이러한 섹션에서는 더욱 쉽게 네트워크 보안을 설정할 수 있는 기능과 옵션에 대해 자세히 설명합니다.

일반 데이터 플레인 강화

데이터 플레인 트래픽의 대부분은 네트워크의 라우팅 컨피그레이션을 통해 판별한 대로 네트워크를 이동합니다. 그러나 네트워크 전체의 패킷 경로를 변경하는 IP 네트워크 기능이 있습니다. IP 옵션(특히 소스 라우팅 옵션)과 같은 기능으로 인해 현재 네트워크의 보안 과제가 생성됩니다.

데이터 플레인을 강화하는 데도 이동 ACL을 사용할 수 있습니다. 자세한 내용은 이 문서의 이동 ACL로 통과 트래픽 필터링 섹션을 참조하십시오.

IP 옵션 선택적 삭제

IP 옵션으로 인해 제기되는 보안 문제는 두 가지가 있습니다. IP 옵션을 포함하는 트래픽은 Cisco IOS 디바이스에서 프로세스를 전환해야 하므로, CPU 로드가 증가할 수 있습니다. IP 옵션에는 트래픽이 네트워크를 통과하는 경로를 변경하는 기능도 포함되어 있어, 보안 제어를 파괴할 가능성이 있습니다.

이러한 문제로 인해 전역 환경 설정 명령어 **ip options {drop | ignore}**가 Cisco IOS Software Releases 12.3(4)T, 12.0(22)S 및 12.2(25)S에 추가되었습니다. 이 명령어의 첫 번째 형식인 **ip options drop**에서는 Cisco IOS 디바이스에서 수신한 IP 옵션을 포함하는 모든 IP 패킷이 삭제됩니다. 따라서 IP 옵션을 통해 활성화될 수 있는 보안 제어 파괴와 CPU 로드 증가가 방지됩니다.

이 명령어의 두 번째 형식인 **ip options ignore**에서는 수신된 패킷에 포함된 IP 옵션을 무시하도록 Cisco IOS 디바이스를 구성합니다. 그러면 로컬 디바이스의 IP 옵션과 관련된 위협이 차단되는 반면 IP 옵션이 있으면 다운스트림 디바이스에 영향을 줄 수 있습니다. 따라서 이 명령어의 **drop** 형식을 사용하는 것이 좋습니다. 이 내용은 다음 컨피그레이션 예에 설명되어 있습니다.

```
!
ip options drop
!
```

RSVP와 같은 일부 프로토콜에서는 합법적으로 IP 옵션을 사용할 수 있습니다. 이러한 프로토콜의 기능은 이 명령어의 영향을 받습니다.

IP 옵션 선택적 삭제(IP Options Selective Drop) 기능이 활성화되고 나면 IP 옵션으로 인해 삭제된 패킷 수를 판별하기 위해 **show ip traffic** EXEC 명령어를 사용할 수 있습니다. 이 정보는 강제 삭제 카운터에 표시됩니다.

이 기능에 대한 자세한 내용은 ACL IP 옵션 선택적 삭제를 참조하십시오.

IP 소스 라우팅 비활성화

IP 데이터그램의 소스를 통해 패킷의 네트워크 경로를 지정할 수 있도록 IP 소스 라우팅에서는 느슨한 소스 경로 및 레코드 경로(Loose Source Route and Record Route) 옵션을 함께 사용하거나 레코드 경로(Record Route) 옵션과 함께 엄격한 소스 경로(Strict Source Route)를 사용합니다. 이 기능은 네트워크의 보안 제어를 위해 트래픽을 라우팅하는 데 사용할 수 있습니다.

IP 옵션 선택적 삭제 기능만으로는 IP 옵션이 완벽하게 비활성화되지 않은 경우, IP 소스 라우팅을 비활성화하는 것이 중요합니다. 모든 Cisco IOS Software Release에서 기본적으로 활성화된 IP 소스 라우팅은 **no ip source-route** 전역 환경 설정 명령어를 통해 비활성화합니다. 다음 컨피그레이션 예에서는 이 명령어의 사용을 설명합니다.

```
!
no ip source-route
!
```

ICMP 리디렉션 비활성화

IP 대상에 도달하는 더 좋은 경로를 네트워크 디바이스에 알리려면 ICMP 리디렉션을 사용합니다. 기본적으로 Cisco IOS Software에서는 수신한 인터페이스를 통해 라우팅해야 하는 패킷을 받는 경우 리디렉션을 보냅니다.

경우에 따라 공격자로 인해 Cisco IOS 디바이스에서 여러 ICMP 리디렉션 메시지를 보낼 수 있으므로, CPU 로드가 증가하게 됩니다. 따라서 ICMP 리디렉션 전송을 비활성화하는 것이 좋습니다. 다음 예제 컨피그레이션에 표시된 대로 ICMP 리디렉션은 인터페이스 환경 설정 **no ip redirects** 명령어로 비활성화합니다.

```
!

interface FastEthernet 0
 no ip redirects
!
```

IP Directed Broadcast 비활성화 또는 제한

IP Directed Broadcast를 사용하면 IP 브로드캐스트 패킷을 원격 IP 서브넷에 보낼 수 있습니다. 원격 네트워크에 도달하면 포워딩 IP 디바이스에서 서브넷에 있는 모든 스테이션에 패킷을 레이어 2 브로드캐스트로 보냅니다. 이 Directed Broadcast 기능은 스머프 공격 등의 여러 공격에서 확장 및 반사하는 데 도움을 주는 기능으로 활용되었습니다.

현재 Cisco IOS Software 버전에서는 기본적으로 이 기능을 비활성화합니다. 그러나 이 기능은 **ip directed-broadcast** 인터페이스 환경 설정 명령어를 통해 활성화할 수 있습니다. Cisco IOS Software 12.0 릴리스 이전 버전에서는 기본적으로 이 기능이 활성화되어 있습니다.

네트워크에 Directed Broadcast 기능이 절대적으로 필요한 경우 해당 기능의 사용을 제어해야 합니다. 이 기능은 **ip directed-broadcast** 명령어에 대한 옵션으로 액세스 제어 목록을 사용하여 제어할 수 있습니다. 다음 컨피그레이션 예에서는 신뢰할 수 있는 네트워크, 192.168.1.0/24에서 시작하는 UDP 패킷으로 directed broadcast를 제한합니다.

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

interface FastEthernet 0
 ip directed-broadcast 100
!
```

이동 ACL을 사용하여 통과 트래픽 필터링

tACL(transit ACL, 이동 ACL)을 사용하여 네트워크에서 이동할 트래픽을 제어할 수 있습니다. 이 ACL은 네트워크 자체를 대상으로 하는 트래픽을 필터링하는 인프라 ACL과 대조적입니다. tACL에서 제공하는 필터링은 네트워크를 이동하는 트래픽 또는 특정 디바이스 그룹의 트래픽을 필터링해야 하는 경우 유용합니다.

일반적으로 이 유형의 필터링은 방화벽에서 수행합니다. 그러나 필터링을 수행해야 하지만 방화벽이 없는 경우와 같이 네트워크의 Cisco IOS 디바이스에서 이 필터링을 수행해야 하는 경우 유용할 수 있습니다.

이동 ACL은 정적 스푸핑 차단 보호를 구현하는 데도 적절합니다. 자세한 내용은 이 문서의 스푸핑 차단 보호 섹션을 참조하십시오.

tACL에 대한 자세한 내용은 이동 액세스 제어 목록: 에지에서 필터링을 참조하십시오.

ICMP 패킷 필터링

ICMP(Internet Control Message Protocol)는 IP의 제어 프로토콜로 설계되었습니다. 따라서 이 프로토콜이 전달하는 메시지는 일반적으로 TCP 및 IP 프로토콜에 지대한 영향을 미칩니다. 경로 MTU 검색뿐 아니라 네트워크 트러블슈팅 툴인 **ping**과 **traceroute**에서 ICMP를 사용합니다. 그러나 네트워크가 제대로 작동하는 경우에는 외부 ICMP 연결이 거의 필요하지 않습니다.

Cisco IOS Software에서는 이름 또는 유형과 코드별로 ICMP 메시지를 구체적으로 필터링하기 위한 기능을 제공합니다. 다음 예제 ACL에서는 신뢰할 수 있는 네트워크의 ICMP는 허용하지만 다른 소스의 ICMP 패킷은 모두 차단합니다.

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Permit ICMP packets from trusted networks only
!

 permit icmp host <trusted-networks> any
!
!--- Deny all other IP traffic to any network device
!

 deny icmp any any
!
```

IP 프래그먼트 필터링

이 문서의 인프라 ACL을 사용하여 네트워크에 대한 액세스 제한 섹션에서 앞서 자세히 설명한 대로 프래그먼트화된 IP 패킷을 필터링하면 j보안 디바이스에 문제가 발생할 수 있습니다.

프래그먼트 처리가 직관적이지 않다는 특성으로 인해, ACL에서 우연히 IP 프래그먼트를 허용하는 경우가 자주 있습니다. 프래그멘테이션은 침입 탐지 시스템의 탐지를 우회하려는 시도에서도 자주 사용됩니다. 이러한 이유로 인해 IP 프래그먼트가 공격에서 자주 사용되며, 구성된 tACL에 앞서 해당 프래그먼트를 명시적으로 필터링해야 합니다. 아래 ACL에는 IP 프래그먼트의 포괄적인 필터링이 포함되어 있습니다. 이 예에 설명된 기능은 이전 예의 기능과 함께 사용해야 합니다.

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

 deny tcp any any fragments
 deny udp any any fragments
 deny icmp any any fragments
 deny ip any any fragments
!
```

ACL에서 프래그먼트화된 IP 패킷을 처리하는 데 대한 자세한 내용은 액세스 제어 목록과 IP 프래그먼트를 참조하십시오.

IP 옵션 필터링을 위한 ACL 지원

Cisco IOS Software Release 12.3(4)T 이상의 Cisco IOS Software에서는 패킷에 포함된 IP 옵션을 기반으로 IP 패킷을 필터링하는 데 ACL을 사용하는 기능을 지원합니다. 패킷에 IP 옵션이 있으면 네트워크에 보안 제어를 파괴하려는 시도가 있거나, 그렇지 않으면 패킷의 이동 특성을 변경하려는 시도가 있음을 표시할 수 있습니다. 따라서 IP 옵션을 사용하는 패킷을 네트워크 에지에서 필터링해야 합니다.

IP 옵션을 포함하는 IP 패킷의 완벽한 필터링을 포함하도록 이전 예의 콘텐츠와 함께 이 예를 사용해야 합니다.

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP packets containing IP options
!

 deny ip any any option any-options
!
```

스푸핑 차단 보호

많은 공격에서 소스 IP 주소 스푸핑을 사용하여 공격을 시행하거나 실제 공격 소스를 숨겨 정확한 역추적을 방해합니다. Cisco IOS Software에서는 소스 IP 주소 스푸핑을 사용한 공격을 막기 위해 유니캐스트 RPF와 IPSG(IP Source Guard)를 제공합니다. 또한 수동으로 스푸핑을 방지하는 방법으로 ACL과 null 라우팅이 구축되는 경우가 많습니다.

IP 소스 가드는 스위치 포트, MAC 주소 및 소스 주소 검증을 수행하여 직접 관리 제어하는 네트워크의 스푸핑을 최소화합니다. 유니캐스트 RPF에서는 소스 네트워크 검증을 제공하고 직접 관리 제어하지 않는 네트워크에서 스푸핑 공격을 줄일 수 있습니다. 액세스 레이어에서 MAC 주소를 검증하기 위해 포트 보안을 사용할 수 있습니다. 동적 ARP(Address Resolution Protocol) 검사(DAI)를 수행하면 로컬 세그먼트에서 ARP 포이즈닝을 사용하는 공격 벡터가 차단됩니다.

유니캐스트 RPF

유니캐스트 RPF를 사용하면 디바이스가 패킷을 받은 인터페이스를 통해 전달된 패킷의 소스 주소에 연결할 수 있는지 확인할 수 있습니다. 스푸핑을 차단하는 데 유니캐스트 RPF에만 의존해서는 안됩니다. 소스 IP 주소로 반환되는 적절한 경로가 있는 경우 스푸핑 패킷에서 유니캐스트 RPF 지원 인터페이스를 통해 네트워크를 입력할 수 있습니다. 유니캐스트 RPF에서는 사용자가 각 디바이스에서 Cisco Express Forwarding을 사용하도록 설정해야 하며, 이 RPF는 인터페이스별로 구성되어 있습니다.

유니캐스트 RPF는 느슨하거나 엄격한 모드 중 하나로 구성할 수 있습니다. 비대칭 라우팅이 있는 경우 엄격한 모드에서는 패킷을 삭제하는 것으로 알려져 있으므로 느슨한 모드를 사용하는 것이 좋습니다. **ip verify** 인터페이스 환경 설정 명령어를 구성하는 중에 **any** 키워드는 느슨한 모드를 구성하는 반면 **rx** 키워드는 엄격한 모드를 구성합니다.

다음 예에서는 이 기능의 컨피그레이션을 설명합니다.

```
!

ip cef
!

interface <interface>
  ip verify unicast source reachable-via <mode>
!
```

유니캐스트 RPF 사용 및 컨피그레이션에 대한 자세한 내용은 유니캐스트 역방향 경로 전달 이해를 참조하십시오.

IP 소스 가드

IP 소스 가드는 레이어 2 인터페이스를 제어할 수 있는 경우 사용할 수 있는 효율적인 스푸핑 방지 방법입니다. IP 소스 가드에서는 DHCP Snooping의 정보를 사용하여 레이어 2 인터페이스에서 PACL(Port Access Control List)을 동적으로 구성하며, IP 소스 바인딩 표에서 연관되지 않은 IP 주소의 트래픽을 거부합니다.

IP 소스 가드는 DHCP Snooping 지원 VLAN에 속한 레이어 2 인터페이스에 적용할 수 있습니다. 다음 명령어는 DHCP Snooping을 활성화합니다.

```
!

ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

DHCP Snooping을 활성화하고 나면 다음 명령어가 IPSG를 활성화합니다.

```
!
interface <interface-id>
   ip verify source
!
```

ip verify source port security 인터페이스 환경 설정 명령어를 사용하여 포트 보안을 활성화할 수 있습니다. 이 작업을 수행하려면 전역 환경 설정 명령어 **ip dhcp snooping information option**이 필요합니다. 또한 DHCP 서버에서 DHCP 옵션 82를 지원해야 합니다.

이 기능에 대한 자세한 내용은 DHCP 기능 및 IP 소스 가드 구성을 참조하십시오.

포트 보안

액세스 인터페이스에서 MAC 주소 스푸핑을 차단하기 위해 포트 보안을 사용합니다. 포트 보안에서는 초기 컨피그레이션을 쉽게 수행하기 위해 동적으로 파악한(고착된) MAC 주소를 사용할 수 있습니다. 포트 보안에서 MAC 위반을 판별하고 나면 다음 네 가지 위반 모드 중 하나를 사용할 수 있습니다. 해당 모드는 보호, 제한, 종료 및 VLAN 종료입니다. 포트에서만 표준 프로토콜을 사용하여 단일 워크스테이션의 액세스를 제공하는 경우 최대 1개만으로도 충분할 수 있습니다. 최대수가 1로 설정되면 HSRP와 같은 가상 MAC 주소를 활용하는 프로토콜은 작동하지 않습니다.

```
!

interface <interface>
  switchport
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security maximum <number>
  switchport port-security violation <violation-mode>
!
```

포트 보안 컨피그레이션에 대한 자세한 내용은 포트 보안 구성을 참조하십시오.

동적 ARP 검사

로컬 세그먼트에서 ARP 포이즈닝 공격을 차단하는 데 DAI(Dynamic ARP Inspection)를 사용할 수 있습니다. ARP 포이즈닝 공격은 공격자가 위조된 ARP 정보를 로컬 세그먼트에 보내는 방법입니다. 이 정보는 다른 디바이스의 ARP 캐시를 손상시키도록 설계되었습니다. 공격자가 중간자(man-in-the-middle) 공격을 수행하기 위해 종종 ARP 포이즈닝을 사용합니다.

DAI에서 신뢰할 수 없는 포트에서 모든 ARP 패킷의 IP-MAC 주소 관계를 인터셉트하여 검증합니다. DHCP 환경에서 DAI는 DHCP Snooping 기능을 통해 생성한 데이터를 사용합니다. 신뢰할 수 있는 인터페이스에서 받은 ARP 패킷은 검증하지 않고 신뢰할 수 없는 인터페이스의 유효하지 않은 패킷은 버립니다. 비DHCP 환경에서는 ARP ACL을 사용해야 합니다.

다음 명령어는 DHCP Snooping을 활성화합니다.

```
!
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

DHCP Snooping이 활성화된 후에 다음 명령어로 DAI를 활성화합니다.

```
!
ip arp inspection vlan <vlan-range>
!
```

비DHCP 환경에서 DAI를 활성화하려면 ARP ACL이 필요합니다. 다음 예에서는 ARP ACL을 사용하는 DAI의 기본 컨피그레이션을 설명합니다.

```
!

arp access-list <acl-name>
 permit ip host <sender-ip> mac host <sender-mac>
!

ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

DAI 구성 방법에 대한 자세한 내용은 동적 ARP 검사 구성을 참조하십시오.

스푸핑 차단 ACL

수동으로 구성한 ACL에서는 알려진 미사용의 신뢰할 수 없는 주소 공간을 사용하는 공격에 대해 정적 스푸핑 차단 보호를 제공할 수 있습니다. 일반적으로 이러한 스푸핑 차단 ACL은 네트워크 경계에서 인그레스(ingress) 트래픽에 대형 ACL의 구성 요소로 적용됩니다. 스푸핑 차단 ACL은 자주 변경될 수 있으므로 정기적으로 모니터링해야 합니다. 유효한 로컬 주소로만 트래픽을 한정하는 아웃바운드 ACL을 적용하는 경우 로컬 네트워크에서 시작하는 트래픽에서 스푸핑을 최소화할 수 있습니다.

다음 예에서는 IP 스푸핑을 제한하기 위해 ACL을 사용하는 방법을 설명합니다. 이 ACL은 원하는 인터페이스의 인바운드에 적용됩니다. 이 ACL을 구성하는 ACE는 포괄적이지 않습니다. 이러한 유형의 ACL을 구성하는 경우 확정된 최신 참조를 구하십시오.

```
!

ip access-list extended ACL-ANTISPOOF-IN
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
!

interface <interface>
 ip access-group ACL-ANTISPOOF-IN in
!
```

액세스 제어 목록을 구성하는 방법에 대한 자세한 내용은 일반적으로 사용하는 IP ACL 구성을 참조하십시오.

할당되지 않은 공식 인터넷 주소 목록은 Cymru 팀에서 유지관리합니다. 사용하지 않는 주소를 필터링하는 데 대한 자세한 내용은 Bogon 참조 페이지에 있습니다.

데이터 플레인 트래픽이 CPU에 미치는 영향 제한

라우터와 스위치의 주된 용도는 디바이스를 통해 패킷과 프레임을 최종 목적지에 전달하는 것입니다. 네트워크 전체에 구축된 디바이스를 통과하는 이러한 패킷은 디바이스의 CPU 운영에 영향을 미칠 수 있습니다. 관리 및 컨트롤 플레인의 운영을 보장하려면 네트워크 디바이스를 통과하는 트래픽으로 구성된 데이터 플레인의 보안을 설정해야 합니다. 통과 트래픽으로 인해 디바이스에서 스위치 트래픽을 처리할 수 있는 경우, 디바이스의 컨트롤 플레인이 영향을 받아 운영이 중단될 수 있습니다.

CPU에 영향을 미치는 기능 및 트래픽 유형

이 목록은 포괄적이지는 않지만 특수 CPU 처리가 필요한 데이터 플레인 트래픽 유형을 포함하며 CPU에서 프로세스를 전환합니다.

- **ACL 로깅** - ACL 로깅 트래픽은 **log** 키워드를 사용하는 ACE가 일치(허용 또는 거부)하여 생성된 패킷으로 구성됩니다.
- **유니캐스트 RPF** - ACL과 함께 사용하는 유니캐스트 RPF를 사용하면 특정 패킷의 프로세스가 전환될 수 있습니다.
- **IP 옵션** - 포함된 옵션이 있는 모든 IP 패킷은 CPU에서 처리되어야 합니다.
- **프래그멘테이션** - 프래그멘테이션이 필요한 모든 IP 패킷은 처리를 위해 CPU에 전달해야 합니다.
- **TTL(Time-to-Live) 만료** - TTL 값이 1 이하인 패킷에는 보낼 ICMP(Internet Control Message Protocol) 시간 초과(ICMP 유형 11, 코드 0) 메시지가 있으므로, CPU 처리가 수행됩니다.
- **ICMP 연결 불가능** - 라우팅, MTU 또는 필터링으로 인해 ICMP 연결 불가능 메시지를 초래하는 패킷은 CPU에서 처리합니다.
- **ARP 요청이 필요한 트래픽** - ARP 항목이 없는 대상은 CPU에서 처리해야 합니다.
- **비IP 트래픽** - 모든 비IP 트래픽은 CPU에서 처리합니다.

데이터 플레인 강화에 대한 자세한 내용은 이 문서의 일반 데이터 플레인 강화 섹션을 참조하십시오.

TTL 값 필터링

Cisco IOS Software Release 12.4(2)T에 도입된 ACL의 TTL 값 필터링 지원(ACL Support for Filtering on TTL Value) 기능을 확장 IP 액세스 목록에서 사용하여 TTL 값을 기반으로 패킷을 필터링할 수 있습니다. 이 기능은 TTL 값이 0 또는 1인 통과 트래픽을 받는 디바이스를 보호하는 데 사용할 수 있습니다. TTL 값이 네트워크 지름 이상이 되도록 하여, TTL 만료 공격으로부터 다운스트림 인프라 디바이스의 컨트롤 플레인을 보호하기 위해 TTL 값을 기반으로 패킷을 필터링하는 기능도 사용할 수 있습니다.

traceroute와 같은 일부 애플리케이션과 툴에서는 테스트 및 진단 용도로 TTL 만료 패킷을 사용합니다. IGMP와 같은 일부 프로토콜에서는 TTL 값인 1을 사용할 수 있습니다.

이 ACL 예에서는 TTL 값이 6 미만인 IP 패킷을 필터링하는 정책을 생성합니다.

```
!

!--- Create ACL policy that filters IP packets with a TTL value
!--- less than 6
!

ip access-list extended ACL-TRANSIT-IN
```

```
 deny ip any any ttl lt 6
 permit ip any any
!
!--- Apply access-list to interface in the ingress direction
!

interface GigabitEthernet 0/0
 ip access-group ACL-TRANSIT-IN in
!
```

TTL 값을 기반으로 패킷을 필터링하는 데 대한 자세한 내용은 TTL 만료 공격 식별 및 차단을 참조하십시오.

이 기능에 대한 자세한 내용은 ACL의 TTL 값 필터링 지원을 참조하십시오.

Cisco IOS Software Release 12.4(4)T 이상에서는 관리자가 FPM(Flexible Packet Matching)을 사용하여 임의의 패킷 비트를 일치시킬 수 있습니다. 이 FPM 정책은 TTL 값이 6 미만인 패킷을 삭제합니다.

```
!

load protocol flash:ip.phdf
!

class-map type access-control match-all FPM-TTL-LT-6-CLASS
 match field IP ttl lt 6
!

policy-map type access-control FPM-TTL-LT-6-DROP-POLICY
 class  FPM-TTL-LT-6-CLASS
  drop
!

interface FastEthernet0
 service-policy type access-control input FPM-TTL-LT-6-DROP-POLICY
!
```

이 기능에 대한 자세한 내용은 Cisco IOS Flexible Packet Matching 홈 페이지에 있는 FPM(Flexible Packet Matching)을 참조하십시오.

IP 옵션 필터링

Cisco IOS Software Release 12.3(4)T 이상에서는, 명명된 확장 IP 액세스 목록에서 ACL의 IP 옵션 필터링 지원(ACL Support for the Filtering IP Options) 기능을 사용하여 IP 옵션이 있는 IP 패킷을 필터링할 수 있습니다. 인프라 디바이스의 컨트롤 플레인을 통해 CPU 레벨에서 이러한 패킷을 처리할 필요가 없도록 IP 옵션을 기반으로 하는 IP 패킷 필터링도 사용할 수 있습니다.

ACL의 IP 옵션 필터링 지원 기능은 명명된 확장 ACL에서만 사용할 수 있습니다. 또한 RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP 버전 2와 3 및 IP 옵션 패킷을 사용하는 기타 프로토콜의 경우 해당 패킷이 삭제되면 제대로 작동할 수 없습니다. 네트워크에서 이러한 프로토콜을 사용 중인 경우 ACL의 IP 옵션 필터링 지원을 사용할 수 있습니다. 그러나 ACL IP 옵션 선택적 삭제 기능을 통해 이 트래픽을 삭제할 수 있으며 해당 프로토콜이 제대로 작동하지 않을 수 있습니다. IP 옵션이 필요한 프로토콜을 사용 중이지 않은 경우 ACL IP 옵션 선택적 삭제를 사용하여 해당 패킷을 삭제하는 것이 좋습니다.

이 ACL 예에서는 IP 옵션을 포함하는 IP 패킷을 필터링하는 정책을 생성합니다.

```
!

ip access-list extended ACL-TRANSIT-IN
 deny ip any any option any-options
 permit ip any any
!

interface GigabitEthernet 0/0
```

```
 ip access-group ACL-TRANSIT-IN in
!
```

이 예제 ACL에서는 5개의 특정 IP 옵션으로 IP 패킷을 필터링하는 정책을 설명합니다. 다음 옵션을 포함하는 패킷은 거부됩니다.

- 0 옵션 목록의 끝(eool)
- 7 레코드 경로(record-route)
- 68 타임스탬프(timestamp)
- 131 - 느슨한 소스 경로(lsr)
- 137 - 엄격한 소스 경로(ssr)

```
!

ip access-list extended ACL-TRANSIT-IN
 deny ip any any option eool
 deny ip any any option record-route
 deny ip any any option timestamp
 deny ip any any option lsr
 deny ip any any option ssr
 permit ip any any
!

interface GigabitEthernet 0/0
 ip access-group ACL-TRANSIT-IN in
!
```

ACL IP 옵션 선택적 삭제에 대한 자세한 내용은 이 문서의 일반 데이터 플레인 강화 섹션을 참조하십시오.

통과 및 에지 트래픽 필터링에 대한 자세한 내용은 이동 액세스 제어 목록: 에지에서 필터링을 참조하십시오.

IP 옵션으로 패킷을 필터링하는 데 사용할 수 있는 Cisco IOS Software의 또 다른 기능은 CoPP입니다. Cisco IOS Software Release 12.3(4)T 이상에서는 관리자가 CoPP를 사용하여 컨트롤 플레인 패킷의 트래픽 흐름을 필터링할 수 있습니다. Cisco IOS Software Release 12.3(4)T에 도입된 CoPP를 지원하고 ACL의 IP 옵션 필터링 지원을 사용하는 디바이스에서는 액세스 목록 정책을 사용하여 IP 옵션을 포함하는 패킷을 필터링할 수 있습니다.

IP 옵션이 있으면 이 CoPP 정책을 통해 디바이스에서 받은 통과 트래픽을 삭제합니다.

```
!

ip access-list extended ACL-IP-OPTIONS-ANY
 permit ip any any option any-options
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS-ANY
!

policy-map COPP-POLICY
 class ACL-IP-OPTIONS-CLASS
  drop

!

control-plane
 service-policy input COPP-POLICY
!
```

IP 옵션이 있으면 이 CoPP 정책을 통해 디바이스에서 받은 통과 트래픽을 삭제합니다.

- 0 옵션 목록의 끝(eool)
- 7 레코드 경로(record-route)
- 68 타임스탬프(timestamp)
- 131 느슨한 소스 경로(lsr)
- 137 엄격한 소스 경로(ssr)

```
!

ip access-list extended ACL-IP-OPTIONS
 permit ip any any option eool
 permit ip any any option record-route
 permit ip any any option timestamp
 permit ip any any option lsr
 permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS
!

policy-map COPP-POLICY
 class ACL-IP-OPTIONS-CLASS
  drop
!

control-plane
 service-policy input COPP-POLICY
!
```

이전 CoPP 정책에서 패킷을 허용 작업과 일치시키는 ACE(Access Control List Entry)는 정책 맵 삭제 기능을 통해 해당 패킷을 버리는 반면 거부 작업(표시되지 않음)과 일치하는 패킷은 정책 맵 삭제 기능의 영향을 받지 않습니다.

CoPP 기능에 대한 자세한 내용은 컨트롤 플레인 정책 구축을 참조하십시오.

컨트롤 플레인 보호

Cisco IOS Software Release 12.4(4)T 이상에서는 Cisco IOS 디바이스의 CPU에서 컨트롤 플레인 트래픽을 제한하거나 감시하기 위해 CPPr(Control Plane Protection)을 사용할 수 있습니다. CPPr은 CoPP와 비슷하지만, CoPP보다 세분화하여 트래픽을 제한하거나 감시하는 기능이 있습니다. CPPr은 통합 컨트롤 플레인을 하위 인터페이스라고 하는 개별 컨트롤 플레인 카테고리로 나눕니다. 하위 인터페이스에는 호스트(Host), 이동(Transit) 및 CEF 예외(CEF-Exception)가 있습니다.

이 CPPr 정책은 TTL 값이 6 미만인 디바이스에서 받은 통과 패킷과 TTL 값이 0 또는 1인 디바이스에서 받은 통과 또는 비통과 패킷을 삭제합니다. CPPr 정책은 디바이스에서 받은 선택한 IP 옵션이 있는 패킷도 삭제합니다.

```
!

ip access-list extended ACL-IP-TTL-0/1
 permit ip any any ttl eq 0 1
!

class-map ACL-IP-TTL-0/1-CLASS
 match access-group name ACL-IP-TTL-0/1
!

ip access-list extended ACL-IP-TTL-LOW
 permit ip any any ttl lt 6
!

class-map ACL-IP-TTL-LOW-CLASS
 match access-group name ACL-IP-TTL-LOW
!
```

```
ip access-list extended ACL-IP-OPTIONS
 permit ip any any option eool
 permit ip any any option record-route
 permit ip any any option timestamp
 permit ip any any option lsr
 permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS
!

policy-map CPPR-CEF-EXCEPTION-POLICY
 class ACL-IP-TTL-0/1-CLASS
  drop
 class ACL-IP-OPTIONS-CLASS
  drop
!

!-- Apply CPPr CEF-Exception policy CPPR-CEF-EXCEPTION-POLICY to
!-- the CEF-Exception CPPr sub-interface of the device

!

control-plane cef-exception
 service-policy input CPPR-CEF-EXCEPTION-POLICY
!

policy-map CPPR-TRANSIT-POLICY
 class ACL-IP-TTL-LOW-CLASS
  drop
!

control-plane transit
 service-policy input CPPR-TRANSIT-POLICY
!
```

이전 CPPr 정책에서 패킷을 허용 작업과 일치시키는 액세스 제어 목록 항목은 정책 맵 삭제 기능을 통해 해당 패킷을 버리는 반면 거부 작업(표시되지 않음)과 일치하는 패킷은 정책 맵 삭제 기능의 영향을 받지 않습니다.

CPPr 기능에 대한 자세한 내용은 컨트롤 플레인 보호 및 컨트롤 플레인 보호 이해를 참조하십시오.

트래픽 식별 및 역추적

특히 사고 대응 중이나 네트워크 성능이 저조한 동안 네트워크 트래픽을 신속하게 식별하여 역추적해야 하는 경우도 있습니다. Cisco IOS Software에서 이 작업을 수행하는 두 가지 주요 방법은 NetFlow와 분류 ACL입니다. NetFlow에서는 네트워크의 모든 트래픽을 표시할 수 있습니다. 또한 장기간의 트렌드와 자동 분석을 제공할 수 있는 컬렉터와 함께 NetFlow를 구현할 수 있습니다. 분류 ACL은 ACL의 구성 요소이며 분석 중에 특정 트래픽과 수동 개입을 식별하기 위한 사전 계획이 필요합니다. 이러한 섹션에서는 각 기능의 개요를 제공합니다.

NetFlow

NetFlow에서는 네트워크 흐름을 추적하여 비정상적인 보안 관련 네트워크 활동을 식별합니다. NetFlow 데이터는 CLI를 통해 보고 분석할 수 있습니다. 또는 집계와 분석을 위해 커머셜 또는 프리웨어 NetFlow 컬렉터에 데이터를 내보낼 수 있습니다. 장기간의 트렌드를 통해 NetFlow 컬렉터에서는 네트워크 행동과 사용 분석을 제공할 수 있습니다. NetFlow는 IP 패킷에서 특정 속성을 분석하고 흐름을 생성하여 작동합니다. 버전 5가 가장 일반적으로 사용되는 NetFlow 버전이지만, 버전 9가 더욱 포괄적입니다. NetFlow 흐름은 트래픽 양이 많은 환경에서 샘플링된 트래픽 데이터를 사용하여 생성할 수 있습니다.

NetFlow를 활성화하려면 CEF나 분산 CEF가 있어야 합니다. NetFlow는 라우터와 스위치에서 구성할 수 있습니다.

다음 예에서는 이 기능의 기본 컨피그레이션을 설명합니다. Cisco IOS Software의 이전 릴리스에서는 인터페이스에서 NetFlow를 활성화하는 명령어가 **ip flow {ingress | egress}**가 아니라 **ip route-cache flow**입니다.

```
!

ip flow-export destination <ip-address> <udp-port>
ip flow-export version <version>
!

interface <interface>
 ip flow <ingess|egress>
!
```

다음은 CLI의 NetFlow 출력 예입니다. SrcIf 속성을 사용하면 역추적에 도움이 될 수 있습니다.

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):

   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  55 active, 65481 inactive, 1014683 added
  41000680 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds

IP Sub Flow Cache, 336520 bytes
  110 active, 16274 inactive, 2029366 added, 1014683 added to flow
  0 alloc failures, 0 force free
  1 chunk, 15 chunks added
  last clearing of statistics never

Protocol         Total     Flows   Packets  Bytes  Packets Active(Sec)  Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt      /Sec    /Flow      /Flow
TCP-Telnet       11512       0.0        15    42       0.2     33.8       44.8
TCP-FTP           5606       0.0         3    45       0.0     59.5       47.1
TCP-FTPD          1075       0.0        13    52       0.0      1.2       61.1
TCP-WWW          77155       0.0        11   530       1.0     13.9       31.5
TCP-SMTP          8913       0.0         2    43       0.0     74.2       44.4
TCP-X              351       0.0         2    40       0.0      0.0       60.8
TCP-BGP            114       0.0         1    40       0.0      0.0       62.4
TCP-NNTP           120       0.0         1    42       0.0      0.7       61.4
TCP-other       556070       0.6         8   318       6.0      8.2       38.3
UDP-DNS         130909       0.1         2    55       0.3     24.0       53.1
UDP-NTP         116213       0.1         1    75       0.1      5.0       58.6
UDP-TFTP           169       0.0         3    51       0.0     15.3       64.2

UDP-Frag             1       0.0         1  1405       0.0      0.0       86.8
UDP-other        86247       0.1       226    29      24.0     31.4       54.3

ICMP             19989       0.0        37    33       0.9     26.0       53.9

IP-other           193       0.0         1    22       0.0      3.0       78.2

Total:         1014637       1.2        26    99      32.8     13.8       43.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Pkts
Gi0/1         192.168.128.21  Local         192.168.128.20  11 CB2B 07AF   3
Gi0/1         192.168.150.60  Gi0/0         10.89.17.146    06 0016 101F  55
Gi0/0         10.89.17.146    Gi0/1         192.168.150.60  06 101F 0016   9
Gi0/1         192.168.150.60  Local         192.168.206.20  01 0000 0303  11
Gi0/0         10.89.17.146    Gi0/1         192.168.150.60  06 07F1 0016   1
```

NetFlow 기능에 대한 자세한 내용은 Cisco IOS NetFlow를 참조하십시오.

NetFlow의 기술 개요는 Cisco IOS NetFlow 소개 - 기술 개요를 참조하십시오.

분류 ACL

분류 ACL에서는 인터페이스를 통과하는 트래픽을 표시합니다. 분류 ACL은 네트워크의 보안 정책을 변경하지 않으며, 일반적으로 개별 프로토콜, 소스 주소 또는 대상을 분류하도록 구성됩니다. 예를 들어, 모든 트래픽을 허용하는 ACE는 특정 프로토콜 또는 포트로 분리할 수 있습니다. 이와 같이 트래픽을 더욱 세분화하여 특정 ACE로 분류하면 각 트래픽 카테고리에 고유 히트 카운터가 있으므로 네트워크 트래픽을 파악하는 데 도움이 됩니다. 거부된 트래픽의 유형을 식별하는 데 도움이 되도록 관리자가 ACL의 끝에서 암시적 거부를 세분화된 ACE로 분리할 수도 있습니다.

관리자가 **show access-list** 및
clear ip access-list counters EXEC 명령어와 함께 분류 ACL을 사용하면 더 신속하게 사고에 대응할 수 있습니다.

다음 예에서는 기본 거부 전에 SMB 트래픽을 식별하는 분류 ACL의 컨피그레이션을 설명합니다.

```
!

ip access-list extended ACL-SMB-CLASSIFY
 remark Existing contents of ACL
 remark Classification of SMB specific TCP traffic
 deny   tcp any any eq 139
 deny   tcp any any eq 445
 deny   ip any any
!
```

분류 ACL을 사용하는 트래픽을 식별하려면 **show access-list** acl-name EXEC 명령어를 사용하십시오. ACL 카운터는 **clear ip access-list counters** acl-name EXEC 명령어를 사용하여 지울 수 있습니다.

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
    10 deny tcp any any eq 139 (10 matches)
    20 deny tcp any any eq 445 (9 matches)
    30 deny ip any any (184 matches)
```

ACL에서 로깅 기능을 활성화하는 방법에 대한 자세한 내용은 액세스 제어 목록 로깅 이해를 참조하십시오.

VLAN 맵 및 포트 액세스 제어 목록을 사용하여 액세스 제어

VACL(VLAN Access Control List) 또는 VLAN 맵 및 PACL(Port ACL)에서는 라우팅된 인터페이스에 적용되는 액세스 제어 목록보다 엔드포인트 디바이스에 가까운 라우팅되지 않은 트래픽에서 액세스 제어를 시행하는 기능을 제공합니다.

이러한 섹션에서는 VACL 및 PACL의 잠재적 사용 시나리오, 기능 및 혜택의 개요를 제공합니다.

VLAN 맵으로 액세스 제어

VLAN에 입력되는 모든 패킷에 적용되는 VACL 또는 VLAN 맵에서는 인트라 VLAN 트래픽에서 액세스 제어를 시행하는 기능을 제공합니다. 이 작업은 라우팅된 인터페이스에서 ACL로 수행할 수 없습니다. 예를 들어, 동일한 VLAN에 포함된 호스트가 서로 통신할 수 없게 하여, 로컬 공격자나 웜이 동일한 네트워크 세그먼트에 있는 호스트를 공격하는 기회를 줄이도록 VLAN 맵을 사용할 수 있습니다. VLAN 맵을 사용하지 못하게 패킷을 거부하려면 트래픽과 일치하는 ACL(Access Control List)을 생성하고 VLAN 맵에서 삭제할 작업을 설정할 수 있습니다. VLAN 맵을 구성하고 나면 LAN에 입력되는 모든 패킷을 구성된 VLAN 맵과 비교하여 순차적으로 평가합니다. VLAN 액세스 맵에서는 IPv4 및 MAC 액세스 목록을 지원합니다. 그러나 로깅이나 IPv6 ACL은 지원하지 않습니다.

다음 예에서는 이 기능의 컨피그레이션을 설명하는 명명된 확장 액세스 목록을 사용합니다.

```
!

ip access-list extended <acl-name>
 permit <protocol> <source-address> <source-port> <destination-address>
      <destination-port>
!

vlan access-map <name> <number>
 match ip address <acl-name>
 action <drop|forward>
!
```

다음 예에서는 vines-ip 프로토콜 외에도 TCP 포트 139와 445를 거부하기 위해 VLAN 맵을 사용하는 방법에 대해 설명합니다.

```
!

ip access-list extended VACL-MATCH-ANY
 permit ip any any
!

ip access-list extended VACL-MATCH-PORTS
 permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
 permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!

mac access-list extended VACL-MATCH-VINES
 permit any any vines-ip
!

vlan access-map VACL 10
 match ip address VACL-MATCH-VINES
 action drop
!

vlan access-map VACL 20
 match ip address VACL-MATCH-PORTS
 action drop

!

vlan access-map VACL 30
 match ip address VACL-MATCH-ANY
 action forward
!

vlan filter VACL vlan 100
!
```

VLAN 맵의 컨피그레이션에 대한 자세한 내용은 ACL로 네트워크 보안 구성을 참조하십시오.

PACL로 액세스 제어

PACL은 스위치의 레이어 2 물리적 인터페이스에서 인바운드 방향에만 적용할 수 있습니다. VLAN 맵과 비슷하게 PACL에서는 라우팅되지 않은 트래픽 또는 레이어 2 트래픽에 대한 액세스 제어를 제공합니다. VLAN 맵과 라우터 ACL보다 우선하는 PACL 생성의 구문은 라우터 ACL과 동일합니다. ACL이 레이어 2 인터페이스에 적용되면 PACL이라고 합니다. 컨피그레이션을 수행할 때 IPv4, IPv6 또는 MAC ACL을 생성한 다음 레이어 2 인터페이스에 적용합니다.

다음 예에서는 이 기능의 컨피그레이션을 설명하기 위해 명명된 확장 액세스 목록을 사용합니다.

```
!

ip access-list extended <acl-name>
 permit <protocol> <source-address> <source-port> <destination-address>
      <destination-port>
!
```

```
interface <type> <slot/port>
 switchport mode access
 switchport access vlan <vlan_number>
 ip access-group <acl-name> in
!
```

PACL 컨피그레이션에 대한 자세한 내용은 ACL로 네트워크 보안 구성의 PACL(Port ACL) 섹션을 참조하십시오.

MAC로 액세스 제어

인터페이스 환경 설정 모드에서 다음 명령어를 사용하여 IP 네트워크에 MAC 액세스 제어 목록 또는 확장 목록을 적용할 수 있습니다.

```
Cat6K-IOS(config-if)#mac packet-classify
```

참고: 레이어 3 패킷을 레이어 2 패킷으로 분류합니다. 이 명령어는 Cisco IOS Software Release 12.2(18)SXD(Sup 720의 경우) 및 Cisco IOS Software Releases 12.2(33)SRA 이상에서 지원됩니다.

이 인터페이스 명령어는 인그레스(ingress) 인터페이스에 적용해야 하며 포워딩 엔진에 IP 헤더를 검사하지 않도록 지시합니다. 결과적으로 IP 환경에서 MAC 액세스 목록을 사용할 수 있습니다.

프라이빗 VLAN 사용

프라이빗 VLAN(PVLAN)은 VLAN에 있는 워크스테이션 또는 서버 간 연결을 제한하는 레이어 2 보안 기능입니다. PVLAN이 없으면 레이어 2 VLAN의 모든 디바이스가 자유롭게 통신할 수 있습니다. 단일 VLAN에 있는 디바이스 간 통신을 제한하여 보안을 강화할 수 있는 네트워킹 조건이 있습니다. 예를 들어, 공개적으로 액세스 가능한 서브넷에 있는 서버 간의 통신을 금지하기 위해 PVLAN을 종종 사용합니다. 단일 서버가 손상되는 경우, PVLAN을 적용하여 다른 서버에 연결하지 못하게 하면 손상을 한 서버로 한정하는 데 도움이 될 수 있습니다.

프라이빗 VLAN의 유형은 격리 VLAN, 커뮤니티 VLAN 및 기본 VLAN의 세 가지가 있습니다. PVLAN의 컨피그레이션에서는 기본 및 보조 VLAN을 사용합니다. 기본 VLAN에는 뒷부분에 설명되어 있는 모든 프로미스큐어스(promiscuous) 포트가 포함되어 있으며, 격리 또는 커뮤니티 VLAN이 될 수 있는 보조 VLAN이 하나 이상 포함되어 있습니다.

격리 VLAN

보조 VLAN을 격리 VLAN으로 구성하면 보조 VLAN에 있는 디바이스 간 통신이 완전히 차단됩니다. 기본 VLAN별로 격리 VLAN은 하나뿐일 수 있으며, 프로미스큐어스 포트에서만 격리 VLAN의 포트와 통신할 수 있습니다. 격리 VLAN은 게스트를 지원하는 네트워크와 같은 신뢰할 수 없는 네트워크에서 사용해야 합니다.

이 컨피그레이션 예에서는 VLAN 11을 격리 VLAN으로 구성한 다음 기본 VLAN, VLAN 20에 연결합니다. 아래 예제에서는 인터페이스 FastEthernet 1/1도 VLAN 11의 격리 포트로 구성합니다.

```
!

vlan 11
 private-vlan isolated
!

vlan 20
 private-vlan primary
 private-vlan association 11
!

interface FastEthernet 1/1
 description *** Port in Isolated VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 11
!
```

커뮤니티 VLAN

커뮤니티 VLAN으로 구성된 보조 VLAN을 사용하면 기본 VLAN의 프로미스큐어스 포트 외에도 VLAN의 멤버와 통신할 수 있습니다. 그러나 두 개의 커뮤니티 VLAN 사이의 통신이나 커뮤니티 VLAN과 격리 VLAN 사이의 통신은 가능하지 않습니다. 서로 연결해야 하는 서버를 그룹화하려면 커뮤니티 VLAN을 사용해야 합니다. 이 경우 VLAN에 있는 기타 모든 디바이스에 대한 연결은 필요하지 않습니다. 이 시나리오는 공개적으로 액세스 가능한 네트워크나 서버에서 신뢰할 수 없는 클라이언트에 콘텐츠를 제공하는 경우에 일반적입니다.

이 예에서는 단일 커뮤니티 VLAN을 구성하고 스위치 포트 FastEthernet 1/2를 해당 VLAN의 멤버로 구성합니다. 커뮤니티 VLAN, VLAN 12는 기본 VLAN 20의 보조 VLAN입니다.

```
!

vlan 12
 private-vlan community
!

vlan 20
 private-vlan primary
 private-vlan association 12
!
interface FastEthernet 1/2
 description *** Port in Community VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 12
!
```

프로미스큐어스 포트

기본 VLAN에 있는 스위치 포트는 프로미스큐어스(promiscuous) 포트라고 합니다. 프로미스큐어스 포트는 기본 VLAN과 보조 VLAN의 다른 모든 포트와 통신할 수 있습니다. 라우터나 방화벽 인터페이스가 이러한 VLAN에서 가장 일반적인 디바이스입니다.

이 컨피그레이션 예에서는 이전의 격리 VLAN 예와 커뮤니티 VLAN 예를 결합하고, 인터페이스 FastEthernet 1/12의 컨피그레이션을 프로미스큐어스 포트로 추가합니다.

```
!

vlan 11
 private-vlan isolated
!

vlan 12
 private-vlan community
!

vlan 20
 private-vlan primary
 private-vlan association 11-12
!

interface FastEthernet 1/1
 description *** Port in Isolated VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 11
!

interface FastEthernet 1/2
 description *** Port in Community VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 12
!

interface FastEthernet 1/12 description
 *** Promiscuous Port ***
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 20 add 11-12
!
```

PVLAN을 구현할 때 레이어 3 컨피그레이션에서 PVLAN의 제한 사항을 지원하며 PVLAN 컨피그레이션의 손상을 허용하지 하도록 확인하는 것이 중요합니다. 라우터 ACL 또는 방화벽을 통한 레이어 3 필터링을 사용하면 PVLAN 컨피그레이션의 손상을 방지합니다.

프라이빗 VLAN의 사용 및 컨피그레이션에 대한 자세한 내용은 LAN 보안 홈 페이지에 있는 PVLAN(Private VLAN) - 프로미스큐어스, 격리 및 커뮤니티를 참조하십시오.

결론

이 문서에서는 Cisco IOS 시스템 디바이스의 보안을 설정하기 위해 사용할 수 있는 방법에 대한 대략적인 개요를 제공합니다. 디바이스의 보안을 설정하면 관리하는 네트워크의 전체 보안이 강화됩니다. 이 개요에서는 관리, 제어 및 데이터 플레인의 보호에 대해 설명하며 컨피그레이션 권장 사항도 제공합니다. 가능한 경우 연관된 각 기능의 컨피그레이션을 위한 세부 정보를 충분히 제공합니다. 그러나 추가로 평가하는 데 필요한 정보를 제공하기 위해 항상 포괄적인 참조를 제공합니다.

감사의 말

이 문서의 일부 기능에 대한 설명은 Cisco 정보 개발 팀에서 작성했습니다.

부록: Cisco IOS 디바이스 강화 체크리스트

이 체크리스트는 이 가이드에 제공된 모든 강화 단계 모음입니다. 기능이 적용되지 않았으므로 구현되지 않은 경우에도 관리자가 Cisco IOS 디바이스에 사용 및 고려된 모든 강화 기능을 다시 기억하는 데 사용할 수 있습니다. 관리자가 옵션을 구현하기 전에 각 옵션의 잠재적인 위험을 평가하는 것이 좋습니다.

관리 플레인

- 비밀번호
  - ♦ 활성화 및 로컬 사용자 비밀번호용 MD5 해싱(암호 옵션) 활성화
  - ♦ 비밀번호 재시도 잠금 구성
  - ♦ 비밀번호 복구 비활성화(위험 고려)
- 사용하지 않는 서비스 비활성화
- 관리 세션의 TCP keepalive 구성
- 메모리 및 CPU 임계값 알림 설정
- 구성
  - ♦ 메모리 및 CPU 임계값 알림
  - ♦ 콘솔 액세스용 메모리 예약
  - ♦ 메모리 누수 탐지기
  - ♦ 버퍼 오버플로 탐지
  - ♦ 향상된 Crashinfo 수집
- iACL을 사용하여 관리 액세스 제한
- 필터(위험 고려)
  - ♦ ICMP 패킷
  - ♦ IP 프래그먼트
  - ♦ IP 옵션
  - ♦ 패킷의 TTL 값
- 컨트롤 플레인 보호
  - ♦ 포트 필터링 구성
  - ♦ 큐 임계값 구성

- 관리 액세스
    - ♦ 관리 플레인 보호를 사용하여 관리 인터페이스 제한
    - ♦ EXEC 시간 초과 설정
    - ♦ CLI 액세스에 암호화된 전송 프로토콜(예: SSH) 사용
    - ♦ vty 및 tty 라인의 전송 제어(액세스 클래스 옵션)
    - ♦ 배너를 사용하여 경고
- AAA
    - ♦ 인증 및 폴백에 AAA 사용
    - ♦ 명령어 권한 부여에 AAA(TACACS+) 사용
    - ♦ 계정 관리에 AAA 사용
    - ♦ 이중화된 AAA 서버 사용
- SNMP
    - ♦ SNMPv2 커뮤니티 구성 및 ACL 적용
    - ♦ SNMPv3 구성
- 로깅
    - ♦ 중앙 집중식 로깅 구성
    - ♦ 모든 관련 구성 요소의 로깅 레벨 설정
    - ♦ 로깅 소스 인터페이스 설정
    - ♦ 로깅 타임스탬프 세분화 구성
- 컨피그레이션 관리
    - ♦ 교체 및 롤백
    - ♦ 전용 컨피그레이션 변경 액세스
    - ♦ 소프트웨어 복원력 컨피그레이션
    - ♦ 컨피그레이션 변경 알림

컨트롤 플레인

- 비활성화(위험 고려)
    - ♦ ICMP 리디렉션
    - ♦ ICMP 연결 불가능
    - ♦ 프록시 ARP
- NTP를 사용 중인 경우 NTP 인증 구성
- 컨트롤 플레인 감시/보호(포트 필터링, 큐 임계값) 구성
- 보안 라우팅 프로토콜
    - ♦ BGP(TTL, MD5, 최대 접두사, 접두사 목록, 시스템 경로 ACL)
    - ♦ IGP(MD5, 수동 인터페이스, 경로 필터링, 리소스 사용)
- 하드웨어 레이트 리미터 구성
- 보안 FHRP(First Hop Redundancy Protocol)(GLBP, HSRP, VRRP)

데이터 플레인

- IP 옵션 선택적 삭제 구성
- 비활성화(위험 고려)
    - ♦ IP 소스 라우팅
    - ♦ IP Directed Broadcast
    - ♦ ICMP 리디렉션
- IP Directed Broadcast 제한
- tACL 구성(위험 고려)
    - ♦ ICMP 필터링
    - ♦ IP 프래그먼트 필터링
    - ♦ IP 옵션 필터링
    - ♦ TTL 값 필터링

- 필수 스푸핑 차단 보호 구성
  - ♦ ACL
  - ♦ IP 소스 가드
  - ♦ 동적 ARP 검사
  - ♦ 유니캐스트 RPF
  - ♦ 포트 보안
- 컨트롤 플레인 보호(control-plane cef-exception)
- 트래픽 식별을 위한 NetFlow 및 분류 ACL 구성
- 필수 액세스 제어 ACL 구성(VLAN 맵, PACL, MAC)
- 프라이빗 VLAN 구성

업데이트 날짜: 2016년 1월 6일 문서 ID: 13608
