Cisco IOS 디바이스 강화 가이드

목차

RSA 키에 대한 SSHv2 개선 사항
콘솔 및 AUX 포트
vty 및 tty 줄 제어
vty 및 tty 라인에 대한 제어 전송
경고 배너
인증, 권한 부여 및 계정 관리
TACACS+ 인증
인증 대체
유형 7 비밀번호 사용
TACACS+ 명령 권한 부여
TACACS+ 명령 계정 관리
이중화 AAA 서버
Simple Network Management Protocol 강화
SNMP 커뮤니티 문자열
ACL을 사용하는 SNMP 커뮤니티 문자열
인프라 ACL
SNMP 보기
SNMP 버전 3
관리 플레인 보호
모범 사례 로깅
중앙 위치로 로그 전송
로깅 레벨
콘솔 또는 모니터 세션에 로그인하지 않음
버퍼된 로깅 사용
로깅 소스 인터페이스 구성
로깅 타임스탬프 구성
Cisco IOS 소프트웨어 구성 관리
구성 교체 및 구성 롤백
단독 구성 변경 액세스
Cisco IOS Software 복원력 구성
디지털 서명 Cisco 소프트웨어
구성 변경 알림 및 로깅
컨트롤 플레인
일반 컨트롤 플레인 강화
IP ICMP 리디렉션
ICMP 연결 불가
프록시 ARP
컨트롤 플레인 트래픽의 CPU 영향 제한
컨트롤 플레인 트래픽 이해
인프라 ACL
수신 ACL
CoPP
컨트롤 플레인 보호
하드웨어 레이트 리미터
보안 BGP

소개

이 문서에서는 Cisco IOS® 시스템 장치를 보호하는 데 도움이 되는 정보를 설명하며, 이는 네트워크의 전반적인 보안을 향상시킵니다.네트워크 디바이스의 기능을 분류할 수 있는 세 가지 플레인을 중심으로 구성된 이 문서에서는 포함된 각 기능에 대한 개요와 관련 설명서에 대한 참조를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

네트워크의 3가지 기능 평면, 관리 플레인, 컨트롤 플레인, 데이터 플레인은 각각 보호해야 하는 서로 다른 기능을 제공합니다.

- **관리 플레인** - 관리 플레인은 Cisco IOS 디바이스로 전송되는 트래픽을 관리하며 SSH(Secure Shell) 및 SNMP(Simple Network Management Protocol)와 같은 애플리케이션 및 프로토콜로 구성됩니다.

- **컨트롤 플레인** - 네트워크 디바이스의 컨트롤 플레인은 네트워크 인프라의 기능을 유지하기 위해 가장 중요한 트래픽을 처리합니다.컨트롤 플레인은 BGP(Border Gateway Protocol)를 포함하는 네트워크 디바이스 간의 애플리케이션 및 프로토콜과 EIGRP(Enhanced Interior Gateway Routing Protocol) 및 OSPF(Open Shortest Path First) 같은 IGP(Interior Gateway Protocols)로 구성됩니다.

- **데이터 플레인** - 데이터 플레인이 네트워크 장치를 통해 데이터를 전달합니다.데이터 플레인에는 로컬 Cisco IOS 디바이스로 전송되는 트래픽이 포함되지 않습니다.

이 문서의 보안 기능을 사용하면 기능을 구성할 수 있는 충분한 세부 정보를 제공할 수 있습니다.그러나 그렇지 않은 경우에는 기능에 대한 추가 주의가 필요한지 여부를 평가할 수 있는 방식으로 기능이 설명되어 있습니다.가능한 적절한 경우, 이 문서에는 구현된 경우 네트워크 보안에 도움이 되는 권장 사항이 포함되어 있습니다.

보안 운영

보안 네트워크 운영이 중요한 주제입니다.이 문서의 대부분은 Cisco IOS 디바이스의 보안 컨피그레이션에 사용되지만 컨피그레이션만으로는 네트워크의 보안을 완벽하게 보장할 수 없습니다.네트워크에서 사용 중인 운영 절차는 기본 디바이스의 컨피그레이션만큼 보안에 기여합니다.

이러한 항목에는 구현해야 할 운영 권장 사항이 포함되어 있습니다.이 주제에서는 네트워크 운영의 특정 핵심 영역을 강조 표시하지만 포괄적이지는 않습니다.

Cisco 보안 권고 및 응답 모니터링

Cisco PSIRT(Product Security Incident Response Team)는 Cisco 제품의 보안 관련 문제를 위해 일반적으로 PSIRT Advisories라고 하는 발행물을 작성하고 유지 관리합니다.덜 심각한 문제의 통신에 사용되는 방법은 Cisco Security Response입니다.보안 자문 및 응답은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

이러한 커뮤니케이션 수단에 대한 추가 정보는 Cisco 보안 취약성 정책에서 확인할 수 있습니다.

보안 네트워크를 유지 관리하려면 릴리스된 Cisco 보안 권고 및 응답을 알아야 합니다.네트워크에 발생할 수 있는 위협을 평가하기 전에 취약성에 대한 지식이 있어야 합니다.이 평가 프로세스에 대한 지원은 Risk Triage for Security Vulnerability Announcements를 참조하십시오.

인증, 권한 부여 및 계정 관리 활용

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스를 보호하는 데 매우 중요합니다.AAA 프레임워크는 관리 세션에 대한 인증을 제공하며 사용자를 특정 관리자 정의 명령으로 제한하고 모든 사용자가 입력한 모든 명령을 로깅할 수도 있습니다.AAA 활용 방법에 대한 자세한 내용은 이 문서의 Authentication, Authorization, and Accounting 섹션을 참조하십시오.

로그 수집 및 모니터링 중앙 집중화

보안 인시던트와 관련된 기존, 신규 및 기록 이벤트에 대한 정보를 얻으려면 조직에서 이벤트 로깅 및 상관관계를 위한 통합 전략을 갖추어야 합니다.이 전략에서는 모든 네트워크 디바이스에서 로깅을 활용하고 사전 패키지화되고 맞춤화된 상관관계 기능을 사용해야 합니다.

중앙 집중식 로깅이 구현된 후 분석 및 사고 추적을 로깅하기 위한 구조화된 접근 방식을 개발해야 합니다.조직의 요구 사항에 따라, 이 접근 방식은 로그 데이터의 간단한 검토, 고급 규칙 기반 분석 등 다양합니다.

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

가능한 경우 보안 프로토콜 사용

중요한 네트워크 관리 데이터를 전달하기 위해 많은 프로토콜이 사용됩니다.가능하면 보안 프로토콜을 사용해야 합니다.보안 프로토콜 선택에는 인증 데이터와 관리 정보가 모두 암호화되도록 텔넷 대신 SSH를 사용하는 것이 포함됩니다.또한 컨피그레이션 데이터를 복사할 때 보안 파일 전송 프로토콜을 사용해야 합니다.예를 들어 FTP 또는 TFTP 대신 SCP(Secure Copy Protocol)를 사용하는 경우를 들 수 있습니다.

Cisco IOS 장치의 보안 관리에 대한 자세한 내용은 이 문서의 Secure Interactive Management Sessions 섹션을 참조하십시오.

NetFlow로 트래픽 가시성 확보

NetFlow를 사용하면 네트워크의 트래픽 흐름을 모니터링할 수 있습니다.원래 네트워크 관리 애플리케이션으로 트래픽 정보를 내보내기 위해 NetFlow를 사용하여 라우터에 플로우 정보를 표시할 수도 있습니다.이 기능을 사용하면 어떤 트래픽이 네트워크를 실시간으로 이동하는지 확인할 수 있습니다.플로우 정보를 원격 컬렉터로 내보내는지 여부에 관계없이, 필요한 경우 다시 사용할 수 있도록 NetFlow용 네트워크 디바이스를 구성하는 것이 좋습니다.

이 기능에 대한 자세한 내용은 이 문서의 Traffic Identification and Traceback 섹션 및 http://www.cisco.com/go/netflow에서 확인할 수 있습니다(등록된 고객만 해당).

구성 관리

구성 관리는 구성 변경 사항을 제안, 검토, 승인 및 구축하는 프로세스입니다.Cisco IOS 디바이스 컨피그레이션의 맥락에서 구성 관리의 두 가지 추가 측면이 중요합니다.구성 아카이브 및 보안.

구성 아카이브를 사용하여 네트워크 디바이스에 적용된 변경 사항을 롤백할 수 있습니다.보안 상황에서 구성 아카이브를 사용하여 어떤 보안 변경 사항이 적용되었는지, 언제 변경되었는지 확인할 수도 있습니다.이 정보는 AAA 로그 데이터와 함께 네트워크 디바이스의 보안 감사를 지원할 수 있습니다.

Cisco IOS 디바이스의 컨피그레이션에는 많은 중요한 세부 정보가 포함되어 있습니다.사용자 이름, 비밀번호 및 액세스 제어 목록의 내용은 이러한 유형의 예입니다.Cisco IOS 디바이스 컨피그레이션을 아카이브하기 위해 사용하는 리포지토리를 보호해야 합니다.이 정보에 대한 안전하지 않은 액세스는 전체 네트워크의 보안을 해칠 수 있습니다.

관리 플레인

관리 플레인은 네트워크의 관리 목표를 달성하는 기능으로 구성됩니다.여기에는 SSH를 사용하는 대화형 관리 세션과 SNMP 또는 NetFlow를 사용한 통계 수집이 포함됩니다.네트워크 디바이스의 보안을 고려하는 경우 관리 플레인을 보호하는 것이 중요합니다.보안 사고가 관리 플레인의 기능을 손상시킬 수 있는 경우 네트워크를 복구하거나 안정화하는 것이 불가능할 수 있습니다.

이 문서의 다음 섹션에서는 관리 플레인을 강화하는 데 도움이 되는 Cisco IOS 소프트웨어에서 사용할 수 있는 보안 기능 및 구성에 대해 자세히 설명합니다.

일반 관리 플레인 강화

관리 플레인은 디바이스를 액세스, 구성 및 관리할 뿐만 아니라 해당 운영 및 디바이스가 구축된 네트워크를 모니터링하는 데 사용됩니다.관리 플레인은 이러한 기능의 운영을 위해 트래픽을 수신하고 전송하는 플레인입니다.제어 평면의 작업이 관리 평면의 작업에 직접 영향을 주므로 디바이스의 관리 평면과 컨트롤 플레인을 모두 보호해야 합니다.이 프로토콜 목록은 관리 플레인에서 사용됩니다.

- 간단한 네트워크 관리 프로토콜
- Telnet

- SSH(Secure Shell Protocol)
- 파일 전송 프로토콜
- HyperText 전송 프로토콜/보안 하이퍼텍스트 전송 프로토콜
- Trivial 파일 전송 프로토콜
- Secure Copy 프로토콜
- TACACS+
- RADIUS
- NetFlow
- 네트워크 시간 프로토콜
- Syslog

보안 사고 동안 관리 및 컨트롤 플레인의 생존이 보장되도록 해야 합니다.이러한 플레인 중 하나가 성공적으로 악용되면 모든 플레인이 손상될 수 있습니다.

비밀번호 관리

비밀번호는 리소스 또는 디바이스에 대한 액세스를 제어합니다.이 작업은 요청을 인증하는 데 사용되는 암호 또는 암호를 정의하여 수행합니다.리소스 또는 디바이스에 대한 액세스 요청이 수신되면 요청에서 비밀번호 및 ID의 확인을 요청하며, 결과에 따라 액세스 권한을 부여, 거부 또는 제한할 수 있습니다.보안 모범 사례로서, 비밀번호는 TACACS+ 또는 RADIUS 인증 서버로 관리되어야 합니다.그러나 TACACS+ 또는 RADIUS 서비스에 장애가 발생할 경우에도 권한 액세스를 위해 로컬로 구성된 비밀번호가 여전히 필요합니다.디바이스에는 NTP 키, SNMP 커뮤니티 문자열 또는 라우팅 프로토콜 키와 같은 다른 비밀번호 정보가 해당 컨피그레이션에 있을 수도 있습니다.

enable **secret** 명령은 Cisco IOS 시스템에 대한 권한 있는 관리 액세스를 부여하는 비밀번호를 설정하는 데 사용됩니다.이전 enable **password** 명령 대신 enable secret 명령을 사용해야 합니다 .enable **password** 명령은 약한 암호화 알고리즘을 사용합니다.

enable secret이 설정되지 않고 콘솔 tty 라인에 대해 비밀번호가 구성된 경우 원격 vty(virtual tty) 세션에서도 특권 액세스를 수신하기 위해 콘솔 비밀번호를 사용할 수 있습니다.이 작업은 거의 확실히 원치 않으며 enable secret을 구성해야 하는 또 다른 이유입니다.

service **password-encryption** 전역 컨피그레이션 명령은 Cisco IOS 소프트웨어가 비밀번호, CHAP(Challenge Handshake Authentication Protocol) 암호 및 컨피그레이션 파일에 저장된 유사 데이터를 암호화하도록 지시합니다.이러한 암호화는 일반 관찰자가 관리자 검열을 통해 화면을 볼 때와 같은 암호를 읽지 못하도록 하기 위해 유용합니다.그러나 **service password-encryption** 명령에서 사용하는 알고리즘은 간단한 Vigen re 암호입니다.이 알고리즘은 약간 정교한 공격자의 심각한 분석으로부터 컨피그레이션 파일을 보호하도록 설계되지 않았으므로 이러한 용도로 사용해서는 안 됩니다.암호화된 비밀번호를 포함하는 모든 Cisco IOS 컨피그레이션 파일은 동일한 비밀번호의 일반 텍스트 목록에 사용되는 것과 동일하게 취급되어야 합니다.

이 약한 암호화 알고리즘은 enable **secret** 명령에서 사용되지 않지만, enable **password** 전역 컨피그레이션 명령 및 **password** line configuration 명령에서 사용됩니다.이 유형의 비밀번호를 제거하고 enable **secret** 명령 또는 향상된 비밀번호 보안 기능을 사용해야 합니다.

enable **secret** 명령 및 Enhanced Password Security 기능에서는 비밀번호 해싱에 MD5(Message Digest 5)를 사용합니다.이 알고리즘은 많은 공개 검토를 거쳤기 때문에 되돌릴 수 없는 것으로 알려져 있습니다.그러나 알고리즘은 사전 공격을 받습니다.사전 공격에서 공격자는 일치하는 항목을 찾기 위해 사전에 있는 모든 단어 또는 후보 비밀번호 목록에 있는 모든 단어를 시도합니다.따라서 컨피그레이션 파일은 안전하게 저장되고 신뢰할 수 있는 개인과만 공유되어야 합니다.

향상된 비밀번호 보안

Cisco IOS Software Release 12.2(8)T에 도입된 향상된 비밀번호 보안 기능을 통해 관리자는 **username** 명령에 대한 비밀번호의 MD5 해싱을 구성할 수 있습니다.이 기능 이전에는 두 가지 유형의 비밀번호가 있었습니다.일반 텍스트 비밀번호인 Type 0과 Vigen re 암호의 알고리즘을 사용하는 Type 7입니다.향상된 비밀번호 보안 기능은 일반 텍스트 비밀번호를 검색해야 하는 프로토콜(예: CHAP)과 함께 사용할 수 없습니다.

MD5 해싱을 사용하여 사용자 비밀번호를 암호화하려면 **username secret** 전역 컨피그레이션 명령을 실행합니다.

```
!

username <name> secret <password>

!
```

이 기능*에* 대한 자세한 내용은 향상된 비밀번호 보안을 *참조하십시오*.

로그인 비밀번호 재시도 잠금

Cisco IOS Software Release 12.3(14)T에 추가된 Login Password Retry Lockout(로그인 비밀번호 재시도 잠금) 기능을 사용하면 구성된 횟수만큼 로그인 시도 실패 후 로컬 사용자 계정을 잠글 수 있습니다.사용자가 잠기면 잠금을 해제할 때까지 해당 계정이 잠깁니다.권한 레벨 15로 구성된 권한 있는 사용자는 이 기능을 사용하여 잠글 수 없습니다.권한 수준이 15인 사용자 수는 최소 수준으로 유지해야 합니다.

실패한 로그인 시도 횟수에 도달하면 인증된 사용자가 디바이스에서 자신을 잠글 수 있습니다.또한 악의적인 사용자는 유효한 사용자 이름으로 인증하려는 시도가 반복된 DoS(Denial of Service) 조건을 생성할 수 있습니다.

다음 예에서는 로그인 비밀번호 재시도 잠금 기능을 활성화하는 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)와 같은 인증 방법에도 적용됩니다.

서비스 비밀번호 복구 없음

Cisco IOS Software Release 12.3(14)T 이상에서 No Service Password-Recovery 기능은 콘솔 액세스 권한이 있는 사용자가 디바이스 컨피그레이션에 비보안 상태로 액세스하여 비밀번호를 지울 수 없도록 합니다.또한 악의적인 사용자가 컨피그레이션 레지스터 값을 변경하고 NVRAM에 액세스하는 것도 허용하지 않습니다.

```
!

no service password-recovery

!
```
Cisco IOS 소프트웨어는 시스템 시작 시 Break 키를 사용하여 ROMMON(ROM Monitor Mode)에 액세스하는 데 의존하는 비밀번호 복구 절차를 제공합니다.ROMMON에서 새 비밀번호를 포함하는 새 시스템 컨피그레이션을 프롬프트하기 위해 디바이스 소프트웨어를 다시 로드할 수 있습니다.

현재 비밀번호 복구 절차를 사용하면 콘솔 액세스 권한이 있는 모든 사용자가 디바이스 및 해당 네트워크에 액세스할 수 있습니다.서비스 비밀번호 복구 없음 기능은 시스템 시작 중에 브레이크 키 시퀀스가 완료되고 ROMMON이 입력되는 것을 방지합니다.

디바이스에서 **서비스 비밀번호 복구**를 활성화하지 않은 경우 디바이스 컨피그레이션의 오프라인 복사본을 저장하고 컨피그레이션 아카이빙 솔루션을 구현하는 것이 좋습니다.이 기능을 활성화한 후 Cisco IOS 디바이스의 비밀번호를 복구해야 하는 경우 전체 컨피그레이션이 삭제됩니다.

이 기능*에* 대한 자세한 내용은 Secure ROMMON Configuration Example을 *참조하십시오*.

사용하지 않는 서비스 비활성화

보안 모범 사례로서 불필요한 서비스를 비활성화해야 합니다.이러한 불필요한 서비스, 특히 UDP(User Datagram Protocol)를 사용하는 서비스는 합법적인 용도로 자주 사용되지 않지만, 패킷 필터링에 의해 차단되는 DoS 및 기타 공격을 실행하는 데 사용할 수 있습니다.

TCP 및 UDP 소규모 서비스를 비활성화해야 합니다.이러한 서비스는 다음과 같습니다.

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

스몰 서비스 남용을 방지하거나 스푸핑 방지 액세스 목록을 통해 덜 위험하게 만들 수 있지만, 네트워크 내에서 액세스 가능한 모든 디바이스에서 서비스를 비활성화해야 합니다.소규모 서비스는 Cisco IOS Software Release 12.0 이상에서 기본적으로 비활성화되어 있습니다.이전 소프트웨어에서는 **no service tcp-small-servers** 및 **no service udp-small-servers** 전역 컨피그레이션 명령을 실행하여 비활성화할 수 있습니다.

사용하지 않는 경우 비활성화해야 하는 추가 서비스 목록입니다.

- **no ip finger** 전역 컨피그레이션 명령을 실행하여 Finger 서비스를 비활성화합니다.12.1(5) 및 12.1(5)T 이후 버전의 Cisco IOS 소프트웨어 릴리스는 기본적으로 이 서비스를 비활성화합니다.

- BOOTP(Bootstrap Protocol)를 비활성화하려면 **no ip bootp server** 전역 컨피그레이션 명령을 실행합니다.

- Cisco IOS Software Release 12.2(8)T 이상에서 BOOTP를 비활성화하려면 전역 컨피그레이션 모드에서 **ip dhcp bootp ignore** 명령을 실행합니다.이렇게 하면 DHCP(Dynamic Host Configuration Protocol) 서비스가 활성화됩니다.

- DHCP 릴레이 서비스가 필요하지 않은 경우 DHCP 서비스를 비활성화할 수 있습니다.글로벌 컨피그레이션 모드에서 **no service dhcp** 명령을 실행합니다.

- MOP(Maintenance Operation Protocol) 서비스를 비활성화하려면 인터페이스 컨피그레이션 모드에서 **no mop enabled** 명령을 실행합니다.

- DNS(Domain Name System) 확인 서비스를 비활성화하려면 **no ip domain-lookup** 전역 컨피그레이션 명령을 실행합니다.

- X.25 네트워크에 사용되는 PAD(Packet Assembler/Disassembler) 서비스를 비활성화하려면 전역 컨피그레이션 모드에서 **no service pad** 명령을 실행합니다.

- 글로벌 컨피그레이션 모드에서 **no ip http server** 명령을 사용하여 HTTP 서버를 비활성화할 수 있으며, **no ip http secure-server** 전역 컨피그레이션 명령을 사용하여 HTTPS(Secure HTTP) 서버를 비활성화할 수 있습니다.

- Cisco IOS 디바이스가 시작 중에 네트워크에서 컨피그레이션을 검색하지 않는 경우 **no service config** 전역 컨피그레이션 명령을 사용해야 합니다.이렇게 하면 Cisco IOS 디바이스가 TFTP를 사용하여 네트워크에서 컨피그레이션 파일을 찾으려고 시도하지 않습니다.

- Cisco CDP(Discovery Protocol)는 인접 디바이스 인접성 및 네트워크 토폴로지를 위해 다른 CDP 지원 디바이스를 검색하는 데 사용되는 네트워크 프로토콜입니다.CDP는 NMS(Network Management Systems)에서 사용하거나 문제 해결 중에 사용할 수 있습니다.신뢰할 수 없는 네트워크에 연결된 모든 인터페이스에서 CDP를 비활성화해야 합니다.이 작업은 **no cdp enable** interface 명령**으로** 수행됩니다.또는 **no cdp run** 전역 컨피그레이션 명령을 사용하여 CDP를 전역적으로 비활성화할 수 있습니다.CDP는 악의적인 사용자가 정찰 및 네트워크 매핑을 위해 사용할 수 있습니다.

- LLDP(Link Layer Discovery Protocol)는 802.1AB에 정의된 IEEE 프로토콜입니다.LLDP는 CDP와 유사합니다.그러나 이 프로토콜은 CDP를 지원하지 않는 다른 디바이스 간의 상호 운용성을 허용합니다.LLDP는 CDP와 동일한 방식으로 처리되어야 하며 신뢰할 수 없는 네트워크에 연결된 모든 인터페이스에서 비활성화되어야 합니다.이를 위해 no lldp transmit 및 **no lldp receive** interface 컨피그레이션 명령을 실행합니다.LLDP를 전역적으로 비활성화하려면 **no lldp run** global configuration 명령을 실행합니다.LLDP는 악의적인 사용자가 정찰 및 네트워크 매핑에 사용할 수도 있습니다.

- sdflash에서 부팅을 지원하는 스위치의 경우 플래시에서 부팅하고 "no sdflash" configuration 명

령으로 sdflash를 비활성화하여 보안을 강화할 수 있습니다.

EXEC 시간 초과

EXEC 명령 인터프리터가 세션을 종료하기 전에 사용자 입력을 기다리는 간격을 설정하려면 **exec-timeout** line configuration 명령을 실행합니다.유휴 **상태로** 남아 있는 vty 또는 tty 라인에서 세션을 로그아웃하려면 exec-timeout 명령을 사용해야 합니다.기본적으로 10분 동안 사용하지 않으면 세션이 끊어집니다.

```
!

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

TCP 세션에 대한 keepalive

service tcp-**keepalives-in** 및 **service tcp-keepalives-out** 전역 컨피그레이션 명령을 사용하면 디바이스에서 TCP 세션에 대한 TCP keepalives를 전송할 수 있습니다.디바이스에 대한 인바운드 연결 및 디바이스에서 나가는 아웃바운드 연결에 TCP keepalive를 활성화하려면 이 컨피그레이션을 사용해야 합니다.이렇게 하면 연결의 원격 끝에 있는 디바이스에 계속 액세스할 수 있으며, 로컬 Cisco IOS 디바이스에서 절반이 열려 있거나 분리된 연결이 제거됩니다.

```
!

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

관리 인터페이스 사용

디바이스의 관리 플레인은 물리적 또는 논리적 관리 인터페이스에서 대역 내 또는 대역 외(out-of-band)에 액세스합니다.네트워크 중단 시 관리 플레인에 액세스할 수 있도록 각 네트워크 디바이스에 대해 대역 내 및 대역 외 관리 액세스가 모두 존재하는 것이 이상적입니다.

디바이스에 대한 대역 내 액세스에 사용되는 가장 일반적인 인터페이스 중 하나는 논리적 루프백 인터페이스입니다.루프백 인터페이스는 항상 작동하지만 물리적 인터페이스는 상태를 변경할 수 있으며, 인터페이스에 액세스할 수 없습니다.각 디바이스에 루프백 인터페이스를 관리 인터페이스로 추가하고 관리 플레인에만 사용하는 것이 좋습니다.이를 통해 관리자는 관리 플레인에 대한 네트워크 전체에 정책을 적용할 수 있습니다.디바이스에 루프백 인터페이스가 구성되면 트래픽을 보내고 받기 위해 SSH, SNMP, syslog와 같은 관리 플레인 프로토콜에서 루프백 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 Memory Threshold Notification 기능을 사용하면

디바이스의 메모리 부족 상태를 완화할 수 있습니다.이 기능은 다음 두 가지 방법을 사용하여 이를 수행합니다.메모리 임계값 알림 및 메모리 예약.

Memory Threshold Notification은 디바이스의 사용 가능한 메모리가 구성된 임계값보다 낮음을 나타내기 위해 로그 메시지를 생성합니다.이 컨피그레이션 예에서는 **memory free low-watermark** 전역 컨피그레이션 명령을 사용하여 이 기능을 활성화하는 방법을 보여줍니다.이렇게 하면 사용 가능한 메모리가 지정된 임계값보다 낮아질 때 디바이스에서 알림을 생성할 수 있으며, 사용 가능한 메모리가 지정된 임계값보다 5% 더 높은 경우에도 다시 알림을 생성할 수 있습니다.

```
!

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

메모리 예약은 중요한 알림에 충분한 메모리를 사용할 수 있도록 사용됩니다.이 컨피그레이션 예에서는 이 기능을 활성화하는 방법을 보여 줍니다.이렇게 하면 디바이스의 메모리가 모두 소모되어도 관리 프로세스가 계속 작동합니다.

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

이 기능*에* 대한 자세한 내용은 메모리 임계값 알림을 참조하십시오.

CPU 임계값 알림

Cisco IOS Software Release 12.3(4)T에 도입된 CPU Thresholding Notification 기능을 사용하면 디바이스의 CPU 로드가 구성된 임계값을 초과할 때 이를 탐지하고 알림을 받을 수 있습니다.임계값을 초과하면 디바이스가 SNMP 트랩 메시지를 생성하고 전송합니다.Cisco IOS 소프트웨어에서는 두 가지 CPU 사용률 임계값 지정 방법이 지원됩니다.상승 임계값 및 낙하 임계값.

다음 예제 컨피그레이션에서는 CPU 임계값 알림 메시지를 트리거하는 Rising 및 Falling Thresholds를 활성화하는 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 기능*에* 대한 자세한 내용은 CPU 임계값 알림 을 *참조하십시오*.

콘솔 액세스를 위한 메모리 예약

Cisco IOS Software Release 12.4(15)T 이상에서는 Reserve Memory for Console Access 기능을 사용하여 관리 및 문제 해결을 위해 Cisco IOS 디바이스에 대한 콘솔 액세스를 보장하기에 충분한 메모리를 예약할 수 있습니다.이 기능은 디바이스의 메모리가 부족한 경우 특히 유용합니다

.**memory reserve console** 전역 컨피그레이션 명령을 실행하여 이 기능을 활성화할 수 있습니다.이 예에서는 이 용도로 4096KB를 예약하도록 Cisco IOS 디바이스를 구성합니다.

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

이 기능*에* 대한 자세한 내용은 콘솔 액세스를 위한 메모리 예약을 참조하십시오.

메모리 누수 탐지기

Cisco IOS Software Release 12.3(8)T1에 도입된 메모리 누수 탐지기 기능을 사용하면 디바이스에서 메모리 누수를 탐지할 수 있습니다.메모리 누수 탐지기는 모든 메모리 풀, 패킷 버퍼 및 청크에서 누수를 찾을 수 있습니다.메모리 유출은 유용한 용도로 사용되지 않는 메모리의 정적 또는 동적 할당입니다.이 기능은 동적 메모리 할당에 중점을 둡니다.메모리 누수가 있는지 확인하기 위해 **show memory debug leaks** EXEC 명령을 사용할 수 있습니다.

버퍼 오버플로:Redzone 손상 탐지 및 수정

Cisco IOS Software 릴리스 12.3(7)T 이상에서는 버퍼 오버플로:메모리 블록 오버플로를 탐지하고 수정하고 작업을 계속하기 위해 디바이스에서 Detection and Correction of Redzone Corruption 기능을 활성화할 수 있습니다.

이러한 전역 컨피그레이션 명령을 사용하여 이 기능을 활성화할 수 있습니다.구성한 후에는 **show memory overflow** 명령을 사용하여 버퍼 오버플로 탐지 및 수정 통계를 표시할 수 있습니다.

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

향상된 Crashinfo 파일 모음

고급 Crashinfo 파일 수집 기능은 기존 crashinfo 파일을 자동으로 삭제합니다.Cisco IOS Software Release 12.3(11)T에 추가된 이 기능을 사용하면 디바이스에서 디바이스 충돌 시 새 crashinfo 파일을 생성하기 위해 공간을 재확보할 수 있습니다.이 기능을 사용하면 저장할 crashinfo 파일 수를 구성할 수도 있습니다.

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

네트워크 시간 프로토콜

NTP(Network Time Protocol)는 특별히 위험한 서비스가 아니지만 불필요한 서비스는 공격 벡터를 나타낼 수 있습니다.NTP를 사용하는 경우 신뢰할 수 있는 시간 소스를 명시적으로 구성하고 적절한 인증을 사용하는 것이 중요합니다.1단계 인증을 위한 인증서에 따라 성공적인 VPN 연결뿐만 아니라 잠재적 공격에 대한 포렌식 조사 중 등의 syslog 목적을 위해 정확하고 안정적인 시간이 필요합니다.

- **NTP Time Zone** - NTP를 구성할 때 타임스탬프가 정확하게 상호 연결될 수 있도록 표준 시간대를 구성해야 합니다.일반적으로 네트워크에 글로벌 프레전스를 사용하는 디바이스의 표준

시간대를 구성하는 두 가지 방법이 있습니다.한 가지 방법은 UTC(Coordinated Universal Time)(이전의 GMT(Greenwich Mean Time)로 모든 네트워크 디바이스를 구성하는 것입니다. 다른 방법은 로컬 표준 시간대로 네트워크 디바이스를 구성하는 것입니다.이 기능에 대한 자세한 내용은 Cisco 제품 설명서의 "clock timezone"에서 확인할 수 있습니다.

- **NTP 인증** - NTP 인증을 구성하는 경우 NTP 메시지가 신뢰할 수 있는 NTP 피어 간에 교환된다는 보장을 제공합니다.

NTP 인증을 사용한 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
```

Smart Install 사용 안 함

Cisco SMI(Smart Install) 기능에 대한 보안 모범 사례는 특정 고객 환경에서 이 기능이 어떻게 사용되는지에 따라 달라집니다.Cisco는 다음과 같은 활용 사례를 차별화합니다.

- Smart Install 기능을 사용하지 않는 고객
- 제로터치 구축에만 스마트 설치 기능을 활용하는 고객
- 제로터치 구축(컨피그레이션 및 이미지 관리)을 위해 Smart Install 기능을 활용하는 고객

다음 섹션에서는 각 시나리오에 대해 자세히 설명합니다.

- Smart Install 기능을 사용하지 않는 고객
- Cisco Smart Install 기능을 사용하지 않고, 명령이 제공되는 Cisco IOS 및 Cisco IOS XE 소프트웨어 릴리스를 실행하는 고객은 **no vstack** 명령으로 Smart Install 기능을 비활성화해야 합니다.

  참고:vstack 명령은 Cisco IOS Release 12.2(55)SE03에서 도입되었습니다.

다음은 Smart Install 클라이언트 기능이 비활성화된 Cisco Catalyst Switch의 **show vstack** 명령의 샘플 출력입니다.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

제로터치 구축에만 스마트 설치 기능을 활용하는 고객

제로 터치 설치가 완료된 후 Smart Install 클라이언트 기능을 비활성화하거나 **no vstack** 명령을 사용합니다.

no vstack 명령을 네트워크로 전파하려면 다음 방법 중 하나를 사용합니다.

- 모든 클라이언트 스위치에 **no vstack** 명령을 수동 또는 스크립트로 입력합니다.
- 제로 터치 설치의 일부로 각 Smart Install 클라이언트에 푸시되는 Cisco IOS 컨피그레이션의 일부로 no vstack 명령을 추가합니다.
- vstack 명령(Cisco IOS Release 12.2(55)SE02 및 이전 릴리스)을 지원하지 않는 릴리스에서는 클라이언트 스위치에 ACL(Access Control List)을 적용하여 TCP 포트 4786의 트래픽을 차단합니다.

나중에 Smart Install 클라이언트 기능을 활성화하려면 수동 또는 스크립트로 모든 클라이언트 스위치에 vstack 명령을 입력합니다.

제로터치 구축에서 스마트 설치 기능을 활용하는 고객

Smart Install 아키텍처 설계에서는 신뢰할 수 없는 사용자가 인프라 IP 주소 공간에 액세스할 수 없도록 주의해야 합니다.vstack 명령을 지원하지 않는 릴리스에서는 **Smart Install** 디렉터만 포트 4786의 모든 Smart Install 클라이언트에 TCP 연결이 설정되어 있는지 확인합니다.

관리자는 영향을 받는 디바이스에서 Cisco Smart Install 구축에 대해 다음 보안 모범 사례를 사용할 수 있습니다.

- 인터페이스 ACL
- CoPP(컨트롤 플레인 폴리싱). 이 기능은 일부 Cisco IOS 소프트웨어 릴리스에서는 사용할 수 없습니다.

다음 예에서는 Smart Install 디렉터 IP 주소가 10.10.10.1이고 Smart Install 클라이언트 IP 주소가 10.10.10.200인 인터페이스 ACL을 보여줍니다.

```
ip access-list extended SMI_HARDENING_LIST
Permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
deny tcp any any eq 4786
permit ip any any
```

이 ACL은 모든 클라이언트의 모든 IP 인터페이스에 구축되어야 합니다.또한 스위치를 처음 구축할 때 디렉터를 통해 푸시할 수도 있습니다.

인프라 내의 모든 클라이언트에 대한 액세스를 추가로 제한하려면 관리자는 네트워크의 다른 디바이스에서 다음 보안 모범 사례를 사용할 수 있습니다.

- 인프라 액세스 제어 목록(iACL)
- VACL(VLAN Access Control List)

인프라 ACL로 네트워크에 대한 액세스 제한

네트워크 디바이스와의 무단 직접 통신을 방지하기 위해 고안된 iACL(infrastructure access control list)은 네트워크에서 구현할 수 있는 가장 중요한 보안 제어 중 하나입니다.인프라 ACL은 거의 모든 네트워크 트래픽이 네트워크를 통과하며 네트워크 자체에 도달하지 않는다는 개념을 활용합니다.

네트워크 디바이스에 허용해야 하는 호스트 또는 네트워크와의 연결을 지정하기 위해 iACL을 구성하고 적용합니다.이러한 연결 유형의 일반적인 예는 eBGP, SSH 및 SNMP입니다.필요한 연결이 허용되면 인프라에 대한 다른 모든 트래픽이 명시적으로 거부됩니다.그러면 네트워크를 통과하며 인프라 디바이스로 이동되지 않는 모든 전송 트래픽이 명시적으로 허용됩니다.

iACL에서 제공하는 보호는 관리 플레인과 컨트롤 플레인과 관련이 있습니다.네트워크 인프라 디바이스에 대해 별도의 주소 지정을 사용하여 iACL을 더욱 쉽게 구현할 수 있습니다.IP 주소 지정의 보안에 미치는 영향에 대한 자세한 내용은 IP 주소 지정에 대한 보안 중심 접근 방식을 *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
!
```

생성된 iACL은 비 인프라 디바이스에 연결된 모든 인터페이스에 적용해야 합니다.여기에는 다른 조직, 원격 액세스 세그먼트, 사용자 세그먼트, 데이터 센터의 세그먼트에 연결하는 인터페이스가 포함됩니다.

자세한 내용은 코어 보호:인프라 ACL에 대한 자세한 내용은 Infrastructure Protection Access Control List를 참조하십시오.

ICMP 패킷 필터링

ICMP(Internet Control Message Protocol)는 IP 제어 프로토콜로 설계되었습니다.따라서 이 메시지가 전달하는 메시지는 일반적으로 TCP 및 IP 프로토콜에 광범위한 영향을 미칠 수 있습니다.네트워크 트러블슈팅 툴이 **ping** 및 **traceroute**에서 ICMP를 사용하지만, 외부 ICMP 연결은 네트워크의 올바른 작동을 위해 거의 필요하지 않습니다.

Cisco IOS 소프트웨어는 이름 또는 유형 및 코드별로 ICMP 메시지를 구체적으로 필터링하기 위한 기능을 제공합니다.이전 예제의 ACE(Access Control Entry)와 함께 사용해야 하는 이 예제 ACL은 신뢰할 수 있는 관리 스테이션 및 NMS 서버의 ping을 허용하고 다른 모든 ICMP 패킷을 차단합니다.

```
!

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 조각 필터링

프래그먼트된 IP 패킷에 대한 필터 프로세스는 보안 디바이스에 문제가 될 수 있습니다.이는 TCP 및 UDP 패킷을 필터링하기 위해 사용되는 레이어 4 정보가 초기 프래그먼트에만 있기 때문입니다.Cisco IOS 소프트웨어는 구성된 액세스 목록과 비교하여 초기가 아닌 프래그먼트를 확인하기 위해 특정 방법을 사용합니다.Cisco IOS 소프트웨어는 ACL에 대해 이러한 비초기 프래그먼트를 평가하고 레이어 4 필터링 정보를 무시합니다.이렇게 하면 구성된 ACE의 레이어 3 부분에서만 초기가 아닌 프래그먼트가 평가됩니다.

이 예제 컨피그레이션에서 **포트 22**에서 **192.168.1.1로** 향하는 TCP 패킷이 전송 중에 프래그먼트화되면 패킷 내의 레이어 4 정보를 기반으로 두 번째 ACE에서 예상한 대로 초기 프래그먼트가 삭제됩니다.그러나 나머지(초기가 아닌) 프래그먼트는 패킷과 ACE의 레이어 3 정보를 완전히 기반으로 첫 번째 ACE에서 모두 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 처리의 직관적이지 않은 특성 때문에 ACL에서 실수로 IP 프래그먼트를 허용하는 경우가 많습니다.프래그먼트화는 침입 탐지 시스템의 탐지를 회피하려는 시도에도 자주 사용됩니다.이러한 이유로 인해 IP 프래그먼트가 공격에 자주 사용되고, 구성된 모든 iACL의 맨 위에서 이를 명시적으로 필터링해야 합니다.이 예제 ACL에는 IP 프래그먼트의 포괄적인 필터링이 포함됩니다.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
!
```

ACL이 조각화된 IP 패킷을 처리하는 방법에 대한 자세한 내용은 Access Control Lists and IP Fragments를 *참조하십시오*.

IP 옵션 필터링을 위한 ACL 지원

Cisco IOS Software Release 12.3(4)T는 ACL을 사용하여 패킷에 포함된 IP 옵션을 기반으로 IP 패킷을 필터링할 수 있는 지원을 추가했습니다.IP 옵션은 예외 패킷으로 처리해야 하므로 네트워크 디바이스에 대한 보안 문제가 발생합니다.이를 위해서는 네트워크를 통과하는 일반적인 패킷에 필요하지 않은 CPU 작업이 필요합니다.패킷에 IP 옵션이 있으면 네트워크에서 보안 제어를 전복하거나, 그렇지 않으면 패킷의 전송 특성을 변경하려는 시도를 나타낼 수도 있습니다.IP 옵션이 있는 패킷은 네트워크 에지에서 필터링되어야 하는 이유는 다음과 같습니다.

IP 옵션이 포함된 IP 패킷의 전체 필터링을 포함하려면 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 값에 대한 필터링 ACL 지원

Cisco IOS Software Release 12.4(2)T는 TTL(Time to Live) 값을 기반으로 IP 패킷을 필터링하는 ACL 지원을 추가했습니다.IP 데이터그램의 TTL 값은 패킷이 소스에서 대상으로의 흐름에 따라 각 네트워크 디바이스에 의해 감소됩니다.초기 값은 운영 체제에 따라 다르지만 패킷의 TTL이 0에 도달하면 패킷을 삭제해야 합니다.TTL을 0으로 감소시켜 패킷을 삭제하는 디바이스는 ICMP Time Exceeded 메시지를 생성하여 패킷의 소스로 전송하기 위해 필요합니다.

이러한 메시지의 생성 및 전송은 예외 프로세스입니다.라우터는 만료 예정인 IP 패킷 수가 적지만 만료 예정인 패킷 수가 높을 경우 사용 가능한 모든 CPU 리소스를 사용할 수 있습니다.이는 DoS 공격 벡터를 나타냅니다.따라서 만료 예정인 높은 비율의 IP 패킷을 사용하는 DoS 공격에 대해 디바이스를 강화해야 합니다.

네트워크 에지에서 TTL 값이 낮은 IP 패킷을 필터링하는 것이 좋습니다.TTL 값이 충분하지 않은 패

킷을 완전히 필터링하면 네트워크를 통과할 수 없으므로 TTL 기반 공격의 위협이 완화됩니다.

이 예제 ACL은 TTL 값이 6보다 작은 패킷을 필터링합니다.이는 최대 5홉의 너비로 네트워크에 대한 TTL 만료 공격을 차단합니다.

```
!

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 프로토콜은 TTL 값이 낮은 패킷을 합법적으로 사용합니다.eBGP는 그러한 프로토콜 중 하나입니다.TTL 만료 기반 공격의 완화에 대한 자세한 내용은 TTL 만료 공격 식별 및 완화를 참조하십시오.

이 기능*에* 대한 자세한 내용은 TTL 값의 필터링을 위한 ACL 지원을 *참조하십시오*.

Secure Interactive Management 세션

디바이스에 대한 관리 세션을 사용하면 디바이스 및 해당 작업에 대한 정보를 보고 수집할 수 있습니다.이 정보가 악의적인 사용자에게 노출될 경우 디바이스는 추가 공격을 수행하기 위해 공격, 보안 침해, 사용되는 공격 대상이 될 수 있습니다.디바이스에 대한 액세스 권한이 있는 모든 사용자는 해당 디바이스에 대한 모든 관리 권한을 가질 수 있습니다.정보 공개와 무단 액세스를 방지하려면 관리 세션을 보호해야 합니다.

관리 플레인 보호

Cisco IOS Software Release 12.4(6)T 이상에서는 MPP(Management Plane Protection) 기능을 사용하여 관리자가 디바이스에서 수신할 수 있는 인터페이스 관리 트래픽을 제한할 수 있습니다.이를 통해 관리자는 디바이스와 디바이스에 액세스하는 방법을 추가로 제어할 수 있습니다.

다음 예에서는 GigabitEthernet0/1 인터페이스에서 SSH 및 HTTPS만 허용하도록 MPP를 활성화하는 방법을 보여줍니다.

```
!

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

MPP에 대한 자세한 내용은 관리 평면 보호를 참조하십시오.

컨트롤 플레인 보호

CPPr(Control Plane Protection)은 IOS 디바이스의 라우트 프로세서로 향하는 제어 평면 트래픽을 제한하여 폴리싱하기 위해 컨트롤 플레인 폴리싱의 기능을 기반으로 합니다.Cisco IOS Software Release 12.4(4)T에 추가된 CPPr은 컨트롤 플레인을 하위 인터페이스라고 하는 별도의 컨트롤 플레인 카테고리로 나눕니다.3개의 컨트롤 플레인 하위 인터페이스가 있습니다.호스트, 전송 및 CEF 예외.또한 CPPr에는 다음과 같은 추가적인 컨트롤 플레인 보호 기능이 포함되어 있습니다.

- **포트 필터링 기능** - 이 기능은 닫히거나 수신되지 않는 TCP 및 UDP 포트로 이동하는 패킷을 폴리싱하거나 삭제하는 기능을 제공합니다.

- **Queue-threshold 정책 기능** - 이 기능은 제어 평면 IP 입력 대기열에서 허용되는 지정된 프로토콜의 패킷 수를 제한합니다.

CPPr을 사용하면 관리자가 호스트 하위 인터페이스를 사용하여 관리 목적으로 디바이스로 전송되는 트래픽을 분류, 보안 및 제한할 수 있습니다.호스트 하위 인터페이스 카테고리에 대해 분류된 패킷의 예로는 SSH 또는 텔넷 및 라우팅 프로토콜과 같은 관리 트래픽이 있습니다.

> **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 세션에서 정보를 공개할 수 있으므로 악의적인 사용자가 전송되는 데이터에 액세스할 수 없도록 이 트래픽을 암호화해야 합니다.트래픽 암호화를 사용하면 디바이스에 대한 보안 원격 액세스 연결을 허용합니다.관리 세션의 트래픽이 일반 텍스트로 네트워크를 통해 전송되는 경우 공격자는 디바이스 및 네트워크에 대한 중요한 정보를 얻을 수 있습니다.

관리자는 SSH 또는 HTTPS(Secure Hypertext Transfer Protocol) 기능을 사용하여 디바이스에 암호화된 보안 원격 액세스 관리 연결을 설정할 수 있습니다.Cisco IOS 소프트웨어는 인증 및 데이터 암호화에 SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security)를 사용하는 SSH 버전 1.0(SSHv1), SSHv2(SSH Version 2.0) 및 HTTPS를 지원합니다.SSHv1 및 SSHv2는 호환되지 않습니다.SSHv1은 안전하지 않으며 표준화되지 않으므로 SSHv2가 옵션인 경우에는 권장하지 않습니다.

Cisco IOS 소프트웨어는 또한 SCP(Secure Copy Protocol)를 지원합니다. 이 SCP는 디바이스 컨피그레이션 또는 소프트웨어 이미지를 복사하기 위해 암호화된 보안 연결을 허용합니다.SCP는 SSH를 사용합니다.이 예제 컨피그레이션은 Cisco IOS 디바이스에서 SSH를 활성화합니다.

```
!

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
!
```

이 컨피그레이션 예에서는 SCP 서비스를 활성화합니다.

```
!

ip scp server enable
!
```

다음은 HTTPS 서비스의 컨피그레이션 예입니다.

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

Cisco IOS 소프트웨어 SSH 기능에 대한 자세한 내용은 Cisco IOS 및 SSH(Secure Shell)를 실행하는 라우터 및 스위치에서 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 이전 버전의 Cisco IOS Software에서 구현되었습니다.) SSH는 신뢰할 수 있는 전송 계층 위에서 실행되며 강력한 인증 및 암호화 기능을 제공합니다.SSH에 대해 정의된 유일한 신뢰할 수 있는 전송은 TCP입니다.SSH는 네트워크를 통해 다른 컴퓨터 또는 디바이스에서 명령에 안전하게 액세스하고 안전하게 실행할 수 있는 방법을 제공합니다.SSH를 통해 터널링되는 SCP(Secure Copy Protocol) 기능을 사용하면 파일을 안전하게 전송할 수 있습니다.

ip ssh 버전 **2** 명령이 명시적으로 구성되지 않은 경우 Cisco IOS는 SSH 버전 1.99를 활성화합니다. SSH 버전 1.99는 SSHv1 및 SSHv2 연결을 모두 허용합니다.SSHv1은 안전하지 않은 것으로 간주되며 시스템에 부정적인 영향을 줄 수 있습니다.SSH가 활성화된 경우 ip ssh version **2** 명령을 사용하여 SSHv1을 비활성화하는 것이 좋습니다.

이 예제 컨피그레이션은 Cisco IOS 디바이스에서 SSHv2(SSHv1이 비활성화됨)를 활성화합니다.

```
!

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 Secure Shell 버전 2 지원을 참조하십시오.

RSA 키에 대한 SSHv2 개선 사항

Cisco IOS SSHv2는 키보드 인터랙티브 및 비밀번호 기반 인증 방법을 지원합니다.RSA Keys용 SSHv2 개선 기능은 클라이언트와 서버에 대한 RSA 기반 공개 키 인증도 지원합니다.

사용자 인증의 경우 RSA 기반 사용자 인증은 인증을 위해 각 사용자와 연결된 개인/공개 키 쌍을 사용합니다.사용자는 클라이언트에서 개인/공개 키 쌍을 생성하고 Cisco IOS SSH 서버에서 공개 키를 구성해야 인증을 완료할 수 있습니다.

자격 증명을 설정하려는 SSH 사용자는 개인 키를 사용하여 암호화된 서명을 제공합니다.인증을 위해 서명 및 사용자의 공개 키가 SSH 서버로 전송됩니다.SSH 서버는 사용자가 제공한 공개 키를 통해 해시를 계산합니다.서버에 일치하는 항목이 있는지 확인하기 위해 해시가 사용됩니다.일치하는 항목이 발견되면 공개 키를 사용하여 RSA 기반 메시지 확인이 수행됩니다.따라서 사용자는 암호화된 서명에 따라 액세스 권한을 인증 또는 거부합니다.

서버 인증을 위해 Cisco IOS SSH 클라이언트는 각 서버에 대해 호스트 키를 할당해야 합니다.클라이언트가 서버와 SSH 세션을 설정하려고 하면 키 교환 메시지의 일부로 서버의 서명을 받습니다.클라이언트에서 엄격한 호스트 키 확인 플래그가 활성화된 경우 클라이언트는 사전 구성된 서버에 해당하는 호스트 키 항목이 있는지 확인합니다.일치하는 항목이 발견되면 클라이언트는 서버 호스트 키로 서명을 검증하려고 시도합니다.서버가 성공적으로 인증되면 세션 설정이 계속됩니다.그렇지 않으면 종료되고 **Server Authentication Failed** 메시지가 표시됩니다.

이 예제 컨피그레이션에서는 Cisco IOS 디바이스에서 SSHv2와 함께 RSA 키를 사용할 수 있습니다.

```
!
! 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
!
```

*SSHv2*와 함께 RSA 키를 사용하는 방법에 대한 자세한 내용은 RSA 키의 Secure Shell 버전 2 개선 사항을 *참조하십시오*.

이 예제 컨피그레이션은 Cisco IOS SSH 서버가 RSA 기반 사용자 인증을 수행할 수 있도록 합니다 .서버에 저장된 RSA 공개 키가 클라이언트에 저장된 공개 또는 개인 키 쌍으로 확인되면 사용자 인증이 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.)
!
```

*SSHv2*와 함께 RSA 키를 사용하는 방법에 대한 자세한 내용은 RSA 기반 사용자 인증을 수행하도록 Cisco IOS SSH 서버 구성을 *참조하십시오*.

이 예제 컨피그레이션을 사용하면 Cisco IOS SSH 클라이언트가 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
!
```

*SSHv2*와 함께 RSA 키를 사용하는 방법에 대한 자세한 내용은 RSA 기반 서버 인증을 수행하도록 Cisco IOS SSH 클라이언트 구성을 *참조하십시오*.

콘솔 및 AUX 포트

Cisco IOS 디바이스에서 콘솔 및 보조(AUX) 포트는 디바이스에 대한 로컬 및 원격 액세스에 사용할 수 있는 비동기식 회선입니다.Cisco IOS 디바이스의 콘솔 포트에는 특별한 권한이 있어야 합니다.특히 이러한 권한을 통해 관리자는 비밀번호 복구 절차를 수행할 수 있습니다.비밀번호 복구를 수행하려면 인증되지 않은 공격자가 콘솔 포트에 액세스할 수 있어야 하며 디바이스에 대한 전원을 중단하거나 디바이스가 충돌하도록 해야 합니다.

디바이스의 콘솔 포트에 액세스하기 위해 사용되는 모든 방법은 디바이스에 대한 특별 권한 액세스

에 적용되는 보안과 동일한 방식으로 보안되어야 합니다.보안 액세스를 위해 사용되는 방법에는 모뎀이 콘솔에 연결된 경우 AAA, exec-timeout 및 모뎀 비밀번호를 사용해야 합니다.

비밀번호 복구가 필요하지 않은 경우 관리자는 **no service password-recovery** 전역 컨피그레이션 명령을 사용하여 비밀번호 복구 절차 수행 기능을 제거할 수 있습니다.그러나 **no service password-recovery** 명령이 활성화되면 관리자가 디바이스에서 더 이상 비밀번호 복구를 수행할 수 없습니다.

대부분의 경우 무단 액세스를 방지하려면 디바이스의 AUX 포트를 비활성화해야 합니다.다음 명령을 사용하여 AUX 포트를 비활성화할 수 있습니다.

```
!

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

vty 및 tty 줄 제어

Cisco IOS 소프트웨어의 대화형 관리 세션에서는 tty 또는 vty(virtual tty)를 사용합니다.tty는 장치에 대한 로컬 액세스를 위해 또는 디바이스에 대한 전화 접속 액세스를 위해 모뎀에 터미널을 연결할 수 있는 로컬 비동기 회선입니다.tty는 다른 디바이스의 콘솔 포트에 연결하는 데 사용할 수 있습니다.이 기능을 사용하면 tty 라인이 있는 디바이스가 콘솔 서버 역할을 할 수 있습니다. 이 콘솔 서버는 네트워크를 통해 tty 라인에 연결된 디바이스의 콘솔 포트에 연결할 수 있습니다.네트워크를 통한 이러한 역방향 연결의 tty 라인도 제어해야 합니다.

프로토콜(예: SSH, SCP 또는 텔넷)에 관계없이 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 제어를 적용해야 합니다.Cisco IOS 디바이스에는 제한된 수의 vty 라인이 있습니다.사용 가능한 행 수는 show line EXEC 명령으로 확인할 수 있습니다.모든 vty 라인이 사용 중인 경우 새 관리 세션을 설정할 수 없으므로 디바이스에 액세스하기 위한 DoS 조건이 생성됩니다.

디바이스의 vty 또는 tty에 대한 가장 간단한 액세스 제어 형식은 네트워크 내의 디바이스 위치에 관계없이 모든 라인에서 인증을 사용하는 것입니다.vty 라인은 네트워크를 통해 액세스할 수 있으므로 이 기능은 vty 라인에 매우 중요합니다.디바이스에 대한 원격 액세스에 사용되는 모뎀에 연결된 tty 회선 또는 다른 디바이스의 콘솔 포트에 연결된 tty 회선도 네트워크를 통해 액세스할 수 있습니다.CoPP 및 CPPr 기능을 사용하거나 디바이스의 인터페이스에 액세스 목록을 적용하는 경우 **transport input** 또**는 access-class** 컨피그레이션 명령을 사용하여 다른 형식의 vty 및 tty 액세스 제어를 적용할 수 있습니다.

인증은 디바이스에 대한 인증 액세스를 위한 권장 방법인 AAA를 사용하거나 로컬 사용자 데이터베이스를 사용하거나 vty 또는 tty 라인에 직접 구성된 간단한 비밀번호 인증을 통해 적용할 수 있습니다.

유휴 **상태로** 남아 있는 vty 또는 tty 라인에서 세션을 로그아웃하려면 exec-timeout 명령을 사용해야 합니다.디바이스로의 **수신 연결에서 TCP keepalives**를 활성화하려면 service tcp-keepalives-in 명령도 사용해야 합니다.이렇게 하면 연결의 원격 끝에 있는 디바이스에 계속 액세스할 수 있으며, 로컬 IOS 디바이스에서 절반이 열려 있거나 분리된 연결이 제거됩니다.

vty 및 tty 라인에 대한 제어 전송

디바이스 또는 콘솔 서버로 사용되는 디바이스에 대한 암호화된 보안 원격 액세스 관리 연결만 허용하려면 vty 및 tty를 구성해야 합니다.이 섹션에서는 이러한 행을 다른 디바이스의 콘솔 포트에 연결할 수 있으므로 tty를 네트워크를 통해 액세스할 수 있습니다.관리자와 디바이스 간에 전송되는 데이터에 대한 정보 공개나 무단 액세스를 방지하기 위해 텔넷 및 로그인과 같은 일반 텍스트 프로토콜 대신 **전송 입력 ssh**를 사용해야 합니다.tty에서 **transport input none** 컨피그레이션을 활성화할 수 있으며, 이는 사실상 역방향 콘솔 연결에 tty 라인 사용을 비활성화합니다.

vty 및 tty 줄 모두 관리자가 다른 디바이스에 연결할 수 있습니다.관리자가 발신 연결에 사용할 수 있는 전송 유형을 제한하려면 **transport output** line configuration 명령을 사용합니다.발신 연결이 필요하지 않으면 **전송 출력**을 사용하지 않아야 합니다.그러나 발신 연결이 허용되면 **전송 출력 ssh**를 사용하여 연결에 대해 암호화된 보안 원격 액세스 방법을 적용해야 합니다.

> **참고:**IPSec은 디바이스에 대한 암호화된 보안 원격 액세스 연결에 사용할 수 있습니다(지원되는 경우).IPSec을 사용하는 경우 디바이스에 CPU 오버헤드도 추가로 추가됩니다.그러나 IPSec을 사용하는 경우에도 SSH는 전송으로 계속 시행되어야 합니다.

경고 배너

일부 법적 관할권에서는 악의적인 사용자가 시스템을 사용할 수 없다는 알림을 받지 않는 한 이를 기소할 수 없으며 이를 모니터링하는 것은 불법일 수 있습니다.이 알림을 제공하는 한 가지 방법은 Cisco IOS 소프트웨어 배너 로그인 명령으로 구성된 배너 메시지에 이 정보를 넣는 것입니다.

법적 고지 요건은 복잡하고 관할권과 상황에 따라 다르며 법률 담당자와 논의해야 합니다.사법권 내에서도 법적 의견이 다를 수 있다.상담원과 협력하여 배너는 다음 정보의 일부 또는 전체를 제공할 수 있습니다.

- 시스템을 로그인 또는 사용해야 하며, 특정 권한 있는 직원 및 사용 권한을 부여할 수 있는 사용자에 대한 정보도 필요합니다.
- 시스템의 무단 사용은 불법이며 민형사상 처벌을 받을 수 있습니다.
- 추가 통지 없이 시스템의 모든 사용을 기록하거나 모니터링할 수 있으며 결과 로그를 법정에서 증거로 사용할 수 있습니다.
- 현지 법률에 명시된 구체적인 통지.

법적 관점이 아닌 보안 관점에서 로그인 배너에는 라우터 이름, 모델, 소프트웨어 또는 소유권에 대한 특정 정보가 포함되지 않아야 합니다.이 정보는 악의적인 사용자가 악용할 수 있습니다.

인증, 권한 부여 및 계정 관리

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스에 대한 대화형 액세스를 보호하기 위해 매우 중요합니다.AAA 프레임워크는 네트워크 요구 사항에 따라 맞춤화할 수 있는 고도로 구성 가능한 환경을 제공합니다.

TACACS+ 인증

TACACS+는 Cisco IOS 디바이스가 원격 AAA 서버에 대한 관리 사용자 인증에 사용할 수 있는 인

증 프로토콜입니다.이러한 관리 사용자는 SSH, HTTPS, 텔넷 또는 HTTP를 통해 IOS 디바이스에 액세스할 수 있습니다.

TACACS+ 인증 또는 일반적으로 AAA 인증에서는 각 네트워크 관리자에 대해 개별 사용자 계정을 사용할 수 있습니다.단일 공유 비밀번호에 의존하지 않을 경우 네트워크의 보안이 향상되고 책임이 강화됩니다.

RADIUS는 TACACS+와 비슷한 프로토콜입니다.그러나 네트워크를 통해 전송되는 비밀번호만 암호화합니다.반면 TACACS+는 사용자 이름과 비밀번호를 모두 포함하는 전체 TCP 페이로드를 암호화합니다.따라서 AAA 서버에서 TACACS+를 지원하는 경우 RADIUS에 앞서 TACACS+를 사용해야 합니다.이 두 프로토콜의 자세한 비교는 TACACS+ 및 RADIUS 비교를 참조하십시오.

TACACS+ 인증은 다음 예와 유사한 컨피그레이션으로 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 인증에 사용할 하나 이상의 보안 프로토콜을 지정할 수 있으므로 초기 방법이 실패할 경우 인증을 위한 백업 시스템을 확인할 수 있습니다.Cisco IOS 소프트웨어는 사용자를 성공적으로 승인하거나 거부하는 첫 번째 나열된 방법을 사용합니다.이후 메서드는 서버 가용성 또는 잘못된 구성으로 인해 이전 메서드가 실패한 경우에만 시도됩니다.

명명된 메서드 목록의 컨피그레이션에 대한 자세한 내용은 인증에 대해 명명된 메서드 목록을 참조하십시오.

인증 대체

구성된 모든 TACACS+ 서버를 사용할 수 없게 되면 Cisco IOS 디바이스는 보조 인증 프로토콜을 사용할 수 있습니다.일반적인 컨피그레이션에는 구성된 모든 TACACS+ 서버를 사용할 수 없는 경우 로컬 또는 enable 인증을 사용하는 것이 포함됩니다.

온디바이스 인증을 위한 전체 옵션 목록에는 enable, local 및 line이 포함됩니다.이러한 각 옵션에는 이점이 있습니다.회선 또는 로컬 인증을 위해 Type 7 비밀번호와 함께 사용되는 암호화 알고리즘보다 본질적으로 더 안전한 단방향 알고리즘으로 비밀번호가 해시되므로 enable 비밀을 사용하는 것이 좋습니다.

그러나 로컬로 정의된 사용자에 대해 비밀 비밀번호 사용을 지원하는 Cisco IOS 소프트웨어 릴리스에서는 로컬 인증으로 대체하는 것이 바람직할 수 있습니다.이렇게 하면 하나 이상의 네트워크 관리자를 위해 로컬로 정의된 사용자를 생성할 수 있습니다.TACACS+를 완전히 사용할 수 없게 되면 각 관리자는 로컬 사용자 이름과 비밀번호를 사용할 수 있습니다.이 작업은 TACACS+ 중단 시 네트워크 관리자의 책임을 개선하지만, 모든 네트워크 디바이스의 로컬 사용자 계정을 유지 관리해야 하기 때문에 관리 부담이 크게 증가합니다.

이 컨피그레이션 예는 enable secret 명령으로 로컬로 구성된 비밀번호에 대한 대체 인증을 포함하기 위해 이전 TACACS+ 인증 예를 기반으로 구축됩니다.

```
!

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>
!
```

*AAA*를 사용한 대체 인증 사용에 대한 자세한 내용은 인증 구성을 참조하십시오.

유형 7 비밀번호 사용

원래 저장된 비밀번호를 신속하게 해독할 수 있도록 설계된 Type 7 비밀번호는 안전한 비밀번호 저장 형식이 아닙니다.이러한 비밀번호를 쉽게 해독할 수 있는 툴이 많이 있습니다.Cisco IOS 디바이스에서 사용 중인 기능에 필요하지 않은 경우 유형 7 비밀번호를 사용하지 않아야 합니다.

가능한 경우 Type 9(scrypt)를 사용해야 합니다.

```
username <username> privilege 15 algorithm-type scrypt secret <secret>
```

이 유형의 비밀번호는 AAA 인증 및 향상된 비밀번호 보안 기능을 사용하여 쉽게 제거할 수 있습니다. 그러면 **username** 전역 컨피그레이션 명령을 통해 로컬로 정의된 사용자와 비밀 비밀번호를 사용할 수 있습니다.유형 7 비밀번호 사용을 완전히 차단할 수 없는 경우, 이러한 비밀번호는 암호화되지 않고 난독 처리되었음을 고려하십시오.

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

TACACS+ 명령 권한 부여

TACACS+ 및 AAA를 통한 명령 권한 부여는 관리 사용자가 입력하는 각 명령을 허용하거나 거부하는 메커니즘을 제공합니다.사용자가 EXEC 명령을 입력하면 Cisco IOS는 구성된 AAA 서버에 각 명령을 전송합니다.그런 다음 AAA 서버는 해당 특정 사용자에 대한 명령을 허용하거나 거부하기 위해 구성된 정책을 사용합니다.

명령 권한 부여를 구현하기 위해 이 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
!
```

명령 권한 부여에 대한 자세한 내용은 권한 부여 구성 을 참조하십시오.

TACACS+ 명령 계정 관리

구성된 경우 AAA 명령 어카운팅은 구성된 TACACS+ 서버에 입력된 각 EXEC 명령에 대한 정보를 전송합니다.TACACS+ 서버로 전송되는 정보에는 명령 실행, 명령 실행 날짜 및 명령을 입력한 사용자의 사용자 이름이 포함됩니다.명령 어카운팅은 RADIUS에서 지원되지 않습니다.

이 예제 컨피그레이션에서는 권한 레벨 0, 1 및 15에서 입력된 EXEC 명령에 대해 AAA 명령 어카운팅을 활성화합니다. 이 컨피그레이션은 TACACS 서버 컨피그레이션을 포함하는 이전 예를 기반으로 구축됩니다.

```
!

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 어카운팅 컨피그레이션에 대한 자세한 내용은 Configuring Accounting을 *참조하십시오*.

이중화 AAA 서버

환경에서 활용되는 AAA 서버는 이중화되어야 하며 내결함성 방식으로 구축되어야 합니다.이를 통해 AAA 서버를 사용할 수 없는 경우 SSH와 같은 인터랙티브 관리 액세스가 가능합니다.

이중화 AAA 서버 솔루션을 설계하거나 구현할 때 다음 사항을 고려해야 합니다.

- 잠재적인 네트워크 장애 시 AAA 서버 가용성
- 지리적으로 분산된 AAA 서버 배치
- 정상 상태 및 장애 조건에서 개별 AAA 서버에 로드
- 네트워크 액세스 서버와 AAA 서버 간의 네트워크 레이턴시
- AAA 서버 데이터베이스 동기화

*자세한 내용*은 액세스 제어 서버 구축을 참조하십시오.

Simple Network Management Protocol 강화

이 섹션에서는 IOS 디바이스 내에서 SNMP의 구축을 보호하기 위해 사용할 수 있는 몇 가지 방법을 중점적으로 설명합니다.네트워크 데이터와 이 데이터가 전송되는 네트워크 디바이스 모두의 기밀성, 무결성 및 가용성을 보호하려면 SNMP를 올바르게 보호해야 합니다.SNMP는 네트워크 디바이스의 상태에 대한 풍부한 정보를 제공합니다.이 정보는 네트워크에 대한 공격을 수행하기 위해 이 데이터를 활용하려는 악의적인 사용자로부터 보호되어야 합니다.

SNMP 커뮤니티 문자열

커뮤니티 문자열은 디바이스의 SNMP 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 모두 제한하기 위해 IOS 디바이스에 적용되는 비밀번호입니다.모든 비밀번호와 마찬가지로 이러한 커뮤니티 문자열을 신중하게 선택하여 단순 문자열이 아닌지 확인해야 합니다.커뮤니티 문자열은 정기적으

로 네트워크 보안 정책에 따라 변경해야 합니다.예를 들어, 네트워크 관리자가 역할을 변경하거나 퇴사할 때 문자열을 변경해야 합니다.

다음 컨피그레이션 라인은 읽기 전용 커뮤니티 문자열 READONLY와 읽기-쓰기 커뮤니티 문자열 READWRITE를 구성합니다.

```
!

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

> **참고:**이러한 문자열의 사용을 명확하게 설명하기 위해 이전 커뮤니티 문자열 예를 선택했습니다.프로덕션 환경에서는 커뮤니티 문자열을 신중하게 선택해야 하며 일련의 영문자, 숫자 및 영숫자 이외의 기호로 구성되어야 합니다.간단한 비밀번호 선택에 대한 자세한 내용은 강력한 비밀번호 생성 권장 사항을 참조하십시오.

이 기능*에* 대한 자세한 내용은 IOS SNMP 명령 참조를 참조하십시오.

ACL을 사용하는 SNMP 커뮤니티 문자열

커뮤니티 문자열 외에도 SNMP 액세스를 소스 IP 주소의 선택 그룹에 추가로 제한하는 ACL을 적용해야 합니다.이 컨피그레이션은 192.168.100.0/24 주소 공간에 상주하는 엔드 호스트 디바이스에 대한 SNMP 읽기 전용 액세스를 제한하고 SNMP 읽기-쓰기 액세스를 192.168.100.1의 엔드 호스트 디바이스로만 제한합니다.

> **참고:**이러한 ACL에서 허용하는 디바이스는 요청된 SNMP 정보에 액세스하려면 적절한 커뮤니티 문자열이 필요합니다.

```
!

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 기능*에* 대한 자세한 내용은 Cisco IOS Network Management Command Reference의 snmp-server 커뮤니티를 *참조하십시오*.

인프라 ACL

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

iACL 사용에 대한 자세한 내용은 이 문서의 Limiting Access to the Network with Infrastructure ACLs 섹션을 참조하십시오.

SNMP 보기

SNMP 보기는 특정 SNMP MIB에 대한 액세스를 허용하거나 거부할 수 있는 보안 기능입니다 .snmp-**server community**-string view global configuration 명령을 사용하여 커뮤니티 문자열에 뷰를 생성하고 적용하면 MIB 데이터에 액세스하는 경우 보기에 정의된 권한으로 제한됩니다.적절한 경우 보기를 사용하여 SNMP 사용자를 필요한 데이터로 제한하는 것이 좋습니다.

이 컨피그레이션 예에서는 커뮤니티 문자열이 LIMITED인 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(SNMPv3)는 RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 및 RFC3415에 의해 정의되며 네트워크 관리를 위한 상호 운용 가능한 표준 기반 프로토콜입니다.SNMPv3는 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 .SNMPv3는 다음과 같은 3가지 기본 구성 옵션으로 구성됩니다.

- **no auth** - 이 모드에서는 SNMP 패킷의 인증이나 암호화가 필요하지 않습니다.
- **auth** - 이 모드에서는 암호화 없이 SNMP 패킷의 인증이 필요합니다.
- **priv** - 이 모드에서는 각 SNMP 패킷의 인증 및 암호화(프라이버시)가 모두 필요합니다.

SNMP 패킷을 처리하기 위해 SNMPv3 보안 메커니즘(인증 또는 인증 및 암호화)을 사용하려면 권한 있는 엔진 ID가 있어야 합니다.기본적으로 엔진 ID는 로컬로 생성됩니다.엔진 ID는 다음 예와 같이 **show snmp engineID** 명령을 사용하여 표시할 수 있습니다.

```
router#show snmp engineID
Local SNMP engineID: 800000090300000152BD35496
Remote Engine ID IP-addr Port
```

참고:engineID가 변경되면 모든 SNMP 사용자 계정을 다시 구성해야 합니다.

다음 단계는 SNMPv3 그룹을 구성하는 것입니다.이 명령은 SNMP 서버 그룹 AUTHGROUP을 사용하여 SNMPv3용 Cisco IOS 디바이스를 구성하고 auth 키워드를 사용하여 이 그룹에 대한 인증만 활성화합니다.

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

이 명령은 SNMP 서버 그룹 PRIVGROUP을 사용하여 SNMPv3용 Cisco IOS 디바이스를 구성하고 priv 키워드를 사용하여 이 그룹에 대한 인증 및 암호화를 모두 **활성화합니다.**

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

이 명령은 authpassword의 MD5 인증 비밀번호와 **privpassword**의 3DES 암호화 비밀번호를 사용하여 SNMPv3 사용자 snmpv3 사용자를 구성합니다.

```
!

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

RFC **3414**에서 요구하는 대로 디바이스의 컨피그레이션 출력에는 snmp-server user 컨피그레이션 명령이 표시되지 않습니다.따라서 컨피그레이션에서 사용자 비밀번호를 볼 수 없습니다.구성된 사용자를 보려면 다음 예와 같이 **show snmp user** 명령을 입력합니다.

```
router#show snmp user
User name: snmpv3user
Engine ID: 800000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

이 기능*에* 대한 자세한 내용은 SNMP 지원 구성 을 *참조하십시오*.

관리 플레인 보호

Cisco IOS 소프트웨어의 MPP(Management Plane Protection) 기능은 SNMP를 보호하는 데 사용할 수 있습니다. SNMP 트래픽이 디바이스에서 종료될 수 있는 인터페이스를 제한하기 때문입니다.관리자는 MPP 기능을 사용하여 하나 이상의 인터페이스를 관리 인터페이스로 지정할 수 있습니다.관리 트래픽은 이러한 관리 인터페이스를 통해서만 디바이스를 입력할 수 있습니다.MPP가 활성화된 후에는 지정된 관리 인터페이스 이외의 어떤 인터페이스도 디바이스로 향하는 네트워크 관리 트래픽을 수락하지 않습니다.

MPP는 CPPr 기능의 하위 집합이며 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 설명서를 참조하십시오.

모범 사례 로깅

이벤트 로깅을 통해 Cisco IOS 디바이스 및 해당 디바이스가 구축된 네트워크에 대한 가시성을 제공합니다.Cisco IOS 소프트웨어는 조직의 네트워크 관리 및 가시성 목표를 달성하는 데 도움이 되는 몇 가지 유연한 로깅 옵션을 제공합니다.

이 섹션에서는 관리자가 Cisco IOS 디바이스에 대한 로깅의 영향을 최소화하면서 성공적으로 로깅을 활용하는 데 도움이 되는 몇 가지 기본 로깅 모범 사례를 제공합니다.

중앙 위치로 로그 전송

원격 syslog 서버에 로깅 정보를 전송하는 것이 좋습니다.이를 통해 네트워크 디바이스 전반에 걸쳐 네트워크 및 보안 이벤트의 상관관계를 파악하고 더 효과적으로 감사할 수 있습니다.syslog 메시지는 UDP와 일반 텍스트로 신뢰할 수 없이 전송됩니다.따라서 네트워크에서 관리 트래픽(예: 암호화 또는 대역 외 액세스)에 대해 제공하는 모든 보호는 syslog 트래픽을 포함하도록 확장되어야 합니다.

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

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

로그 상관관계*에* 대한 자세한 내용은 방화벽 및 IOS 라우터 Syslog 이벤트를 사용하여 인시던트 식별 을 *참조하십시오*.

12.4(15)T에 통합되고 원래 12.0(26)S에 도입된 Logging to Local Nonvolatile Storage (ATA Disk) 기능은 시스템 로깅 메시지를 ATA(Advanced Technology Attachment) 플래시 디스크에 저장할 수 있도록 합니다.라우터가 재부팅된 후에도 ATA 드라이브에 저장된 메시지는 계속 유지됩니다.

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

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

ATA 디스크의 파일에 메시지를 기록하기 전에 Cisco IOS Software에서 디스크 공간이 충분한지 확인합니다.그렇지 않으면 가장 오래된 로깅 메시지 파일(타임스탬프별)이 삭제되고 현재 파일이 저장됩니다.파일 이름 형식은 **log_month:day:year::time입니다**.

> **참고:**ATA 플래시 드라이브는 디스크 공간이 제한되어 있으므로 저장된 데이터를 덮어쓰지 않도록 유지 관리해야 합니다.

다음 예에서는 유지 관리 절차의 일환으로 라우터 ATA 플래시 디스크에서 FTP 서버 192.168.1.129의 외부 디스크로 로깅 메시지를 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 생성되는 각 로그 메시지에는 레벨 0, Emergency, 레벨 7, Debug의 8가지 심각도 중 하나가 할당됩니다.특별히 필요한 경우가 아니면 레벨 7에서 로깅하지 않는 것이 좋습니다. 레벨 7에서 로깅하면 디바이스에서 높은 CPU 로드가 생성되어 디바이스 및 네트워크 불안정이 발생할 수 있습니다.

전역 컨피그레이션 명령 **logging trap** level은 원격 syslog 서버로 어떤 로깅 메시지를 보낼지 지정하기 위해 사용됩니다.지정된 레벨은 전송된 가장 낮은 심각도 메시지를 나타냅니다.버퍼링된 로깅의 경우 logging buffered level 명령**이** 사용됩니다.

이 컨피그레이션 예에서는 원격 syslog 서버 및 로컬 로그 버퍼로 전송되는 로그 메시지를 심각도 6(정보)에서 0(긴급)으로 제한합니다.

```
!

logging trap 6
logging buffered 6
!
```

자세한 내용은 트러블슈팅, 결함 관리 및 로깅을 참조하십시오.

콘솔 또는 모니터 세션에 로그인하지 않음

Cisco IOS 소프트웨어를 사용하면 로그 메시지를 모니터 세션으로 보낼 수 있습니다. 모니터 세션은 EXEC 명령 **터미널 모니터**가 실행된 인터랙티브 관리 세션과 콘솔입니다.그러나 이렇게 하면 IOS 디바이스의 CPU 로드가 상승될 수 있으므로 권장되지 않습니다.대신 **show logging** 명령으로 볼 수 있는 로컬 로그 버퍼에 로깅 정보를 보내는 것이 좋습니다.

콘솔에 대한 로깅을 비활성화하고 세션을 모니터링하려면 전역 컨피그레이션 명령 **no logging console** 및 **no logging monitor**를 사용합니다.이 컨피그레이션 예에서는 다음 명령의 사용을 보여줍니다.

```
!

no logging console
no logging monitor
!
```

전역 컨피그레이션 명령*에* 대한 자세한 내용은 Cisco IOS Network Management Command Reference를 *참조하십시오*.

버퍼된 로깅 사용

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

버퍼된 로깅을 구성할 때 관련된 두 가지 구성 옵션이 있습니다.버퍼에 저장된 로깅 버퍼 크기 및 메시지 심각도로깅 **버퍼**의 크기는 전역 컨피그레이션 명령 로깅 버퍼링 크기로 **구성됩니다**.버퍼에 포함된 최저 심각도는 logging buffered severity 명령으로 구성됩니다.관리자는 **show logging** EXEC 명령을 통해 로깅 버퍼의 내용을 볼 수 있습니다.

이 컨피그레이션 예에는 16384바이트의 로깅 버퍼의 컨피그레이션 및 심각도 6의 정보(레벨 0(긴급)에서 6(정보)까지의 메시지가 저장됨을 나타냅니다.

```
!

logging buffered 16384 6
!
```

*버퍼링된 로깅*에 대한 자세한 내용은 Cisco IOS Network Management Command Reference를 참조하십시오.

로깅 소스 인터페이스 구성

로그 메시지를 수집하고 검토할 때 일관성 수준을 높이기 위해 로깅 소스 인터페이스를 정적으로 구성하는 것이 좋습니다.logging source-**interface** interface 명령을 통해 로깅 소스 인터페이스를 정적으로 구성하면 개별 Cisco IOS 디바이스에서 전송되는 모든 로깅 메시지에 동일한 IP 주소가 표시됩니다.안정성을 강화하기 위해 루프백 인터페이스를 로깅 소스로 사용하는 것이 좋습니다.

이 컨피그레이션 예에서는 **logging source-interface** interface 전역 컨피그레이션 명령을 사용하여 루프백 0 인터페이스의 IP 주소를 모든 로그 메시지에 사용하도록 지정합니다.

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

*자세한 내용*은 Cisco IOS 명령 참조를 참조하십시오.

로깅 타임스탬프 구성

로깅 타임스탬프 컨피그레이션을 사용하면 네트워크 디바이스 간에 이벤트를 상호 연결할 수 있습니다.로깅 데이터의 상관관계를 파악할 수 있도록 정확하고 일관된 로깅 타임스탬프 컨피그레이션을 구현하는 것이 중요합니다.밀리초 정밀도의 날짜 및 시간을 포함하고 디바이스에서 사용 중인 시간대를 포함하도록 로깅 타임스탬프를 구성해야 합니다.

다음 예에서는 UTC(Coordinated Universal Time) 영역 내에서 밀리초 정밀도의 로깅 타임스탬프 컨피그레이션을 포함합니다.

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

UTC에 상대적으로 시간을 로깅하지 않으려는 경우 특정 로컬 시간대를 구성하고 생성된 로그 메시지에 해당 정보가 표시되도록 구성할 수 있습니다.다음 예에서는 PST(Pacific Standard Time) 영역에 대한 디바이스 컨피그레이션을 보여줍니다.

```
!

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

Cisco IOS 소프트웨어 구성 관리

Cisco IOS 소프트웨어에는 Cisco IOS 디바이스에서 구성 관리 형식을 활성화할 수 있는 몇 가지 기능이 포함되어 있습니다.이러한 기능에는 컨피그레이션을 아카이브하고 컨피그레이션을 이전 버전으로 롤백하는 기능과 자세한 컨피그레이션 변경 로그를 생성하는 기능이 포함됩니다.

구성 교체 및 구성 롤백

Cisco IOS Software Release 12.3(7)T 이상에서는 Configuration Replace and Configuration

Rollback 기능을 사용하여 디바이스에서 Cisco IOS 디바이스 컨피그레이션을 아카이브할 수 있습니다.수동 또는 자동으로 저장된 이 아카이브의 컨피그레이션을 사용하여 현재 실행 중인 컨피그레이션을 configure replace filename 명령으로 대체할 수 있습니다.이는 copy filename running-**config** 명령과 **대조적입니다**.configure replace **filename** 명령은 copy 명령에 의해 수행되는 병합과 달리 실행 중인 컨피그레이션을 대체합니다.

네트워크의 모든 Cisco IOS 디바이스에서 이 기능을 활성화하는 것이 좋습니다.활성화되면 관리자는 **archive config privileged EXEC** 명령을 사용하여 현재 실행 중인 컨피그레이션을 아카이브에 추가할 수 있습니다.아카이브된 컨피그레이션은 **show archive** EXEC 명령으로 볼 수 있습니다.

이 예에서는 자동 컨피그레이션 아카이브의 컨피그레이션을 보여줍니다.다음 예에서는 Cisco IOS 디바이스에서 아카이브된 컨피그레이션을 disk0에 archived-config-N이라는 파일로 저장하도록 지시합니다.파일 시스템 - 최대 14개의 백업을 유지 관리하고 하루에 한 번(1440분) 보관할 수 있으며 관리자가 write **memory** EXEC 명령을 실행할 때 보관합니다.

```
!

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

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

단독 구성 변경 액세스

Cisco IOS Software Release 12.3(14)T에 추가된 Exclusive Configuration Change Access 기능은 한 명의 관리자만 지정된 시간에 Cisco IOS 디바이스에 대한 컨피그레이션을 변경할 수 있도록 합니다.이 기능을 사용하면 관련 구성 요소를 동시에 변경할 경우 원치 않는 영향을 방지할 수 있습니다.이 기능은 전역 컨피그레이션 명령 컨피그레이션 **모드 단독** 모드로 구성되며 다음 두 모드 중 하나로 작동합니다.자동 및 수동.자동 모드에서는 관리자가 configure **terminal** EXEC 명령을 실행하면 컨피그레이션이 자동으로 잠깁니다.수동 모드에서는 관리자가 컨피그레이션 모드를 시작할 때 컨피그레이션을 잠그기 위해 configure **terminal lock** 명령을 사용합니다.

다음 예에서는 자동 컨피그레이션 잠금을 위한 이 기능의 컨피그레이션을 설명합니다.

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

Cisco IOS Software 복원력 구성

Cisco IOS Software Release 12.3(8)T에 추가된 복원형 컨피그레이션 기능을 사용하면 현재 Cisco IOS 디바이스에서 사용 중인 Cisco IOS 소프트웨어 이미지 및 디바이스 컨피그레이션의 복사본을 안전하게 저장할 수 있습니다.이 기능을 활성화하면 이러한 백업 파일을 변경하거나 제거할 수 없습니다.이 파일을 삭제하려는 의도하지 않은 시도와 악의적인 시도를 모두 방지하려면 이 기능을 활성화하는 것이 좋습니다.

```
!
secure boot-image
```

```
secure boot-config!
```
이 기능이 활성화되면 삭제된 컨피그레이션 또는 Cisco IOS 소프트웨어 이미지를 복원할 수 있습니다.**show secure boot** EXEC 명령을 사용하여 이 기능의 현재 실행 상태를 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 Software 기능은 안전한 비대칭(공개 키) 암호화를 사용하여 디지털 서명 및 신뢰받는 Cisco IOS Software를 쉽게 사용할 수 있도록 합니다.

디지털 서명된 이미지는 암호화된(개인 키 포함) 해시를 전달합니다.확인 시 디바이스는 키 저장소에 있는 키에서 해당 공개 키로 해시를 해독하고 이미지의 자체 해시를 계산합니다.해독된 해시가 계산된 이미지 해시와 일치하면 이미지가 변조되지 않았으며 신뢰할 수 있습니다.

디지털 서명된 Cisco 소프트웨어 키는 키의 유형 및 버전으로 식별됩니다.키는 특수, 프로덕션 또는 롤오버 키 유형일 수 있습니다.프로덕션 및 특수 키 유형에는 키가 취소 및 교체될 때마다 알파벳순으로 증가하는 관련 키 버전이 있습니다.ROMMON 및 일반 Cisco IOS 이미지는 디지털 서명 Cisco 소프트웨어 기능을 사용할 때 특수 또는 프로덕션 키로 서명됩니다.ROMMON 이미지는 업그레이드할 수 있으며 로드된 특수 이미지 또는 프로덕션 이미지와 동일한 키로 서명해야 합니다.

이 명령은 플래시에 있는 c3900-universalk9-mz.SSA 이미지의 무결성을 디바이스 키 저장소의 키와 함께 확인합니다.

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```
디지털 서명 Cisco 소프트웨어 기능은 Cisco Catalyst 4500 E-Series 스위치용 Cisco IOS XE Release 3.1.0.SG에도 통합되었습니다.

이 기능*에* 대한 자세한 내용은 디지털 서명 Cisco 소프트웨어를 참조하십시오.

Cisco IOS Software Release 15.1(1)T 이상에서는 디지털 서명 Cisco 소프트웨어의 키 교체가 도입되었습니다.키 교체 및 취소는 플랫폼의 키 저장소에서 디지털 서명 Cisco 소프트웨어 검사에 사용되는 키를 대체하고 제거합니다.키 손상 시 특수 키와 프로덕션 키만 취소할 수 있습니다.

(특수 또는 프로덕션) 이미지의 새 (특수 또는 프로덕션) 키는 (프로덕션 또는 폐기) 이미지로 제공되는데, 이 이미지는 이전의 특수 또는 프로덕션 키를 취소하는 데 사용됩니다.폐기 이미지 무결성은 플랫폼에 미리 저장된 롤오버 키로 확인됩니다.롤오버 키는 변경되지 않습니다.프로덕션 키를 취소할 때 폐기 이미지가 로드되면 해당 키가 전달하는 새 키가 키 저장소에 추가되고 ROMMON 이미지가 업그레이드되고 새 프로덕션 이미지가 부팅되는 한 해당 기존 키를 취소할 수 있습니다.특수 키를 취소하면 프로덕션 이미지가 로드됩니다.이 이미지는 새 특수 키를 추가하고 이전 특수 키를 취소할 수 있습니다.ROMMON을 업그레이드한 후 새 특수 이미지를 부팅할 수 있습니다.

이 예에서는 특수 키의 취소에 대해 설명합니다.이 명령은 현재 프로덕션 이미지에서 키 저장소에 새 특수 키를 추가하고, 새 ROMMON 이미지(C3900_rom-monitor.srec.SSB)를 스토리지 영역(usbflash0:)으로 복사하고, 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 로드하기 위해 플래시에 복사하고 새로 추가된 특수 키(.SSB)로 이미지의 서명을 확인할 수 있습니다.

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```
Cisco IOS XE Software를 실행하는 Catalyst 4500 E-Series 스위치에서는 키 취소 및 교체가 지원되지 않지만, 이러한 스위치는 디지털 서명 Cisco 소프트웨어 기능을 지원합니다.

*이 기능*에 대한 자세한 내용은 디지털 서명 Cisco 소프트웨어 설명서의 디지털 서명 Cisco 소프트웨어 키 취소 및 교체 섹션을 참조하십시오.

구성 변경 알림 및 로깅

Cisco IOS Software Release 12.3(4)T에 추가된 Configuration Change Notification and Logging 기능을 사용하면 Cisco IOS 디바이스의 컨피그레이션 변경 사항을 기록할 수 있습니다.로그는 Cisco IOS 디바이스에서 유지 관리되며 변경을 수행한 개인의 사용자 정보, 입력한 컨피그레이션 명령 및 변경 시간을 포함합니다.이 기능은 logging enable 컨피그레이션 **변경 로거 컨피그레이션** 모드 명령을 사용하여 활성화됩니다.선택적인 명령**은** 비밀번호 데이터 로깅을 방지하고 변경 로그의 길이를 증가시키기 때문에 기본 컨피그레이션을 개선하기 위해 hidekeys 및 **logging size** 항목을 사용합니다.

Cisco IOS 디바이스의 컨피그레이션 변경 기록을 더 쉽게 이해할 수 있도록 이 기능을 활성화하는 것이 좋습니다.또한 컨피그레이션 변경 시 syslog 메시지 생성을 활성화하려면 notify syslog 컨피그레이션 명령을 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 특권 EXEC 명령 **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 프로토콜은 물론 Border Gateway Protocol과 같은 라우팅 프로토콜도 포함됩니다.

관리 플레인과 데이터 플레인의 이벤트가 컨트롤 플레인에 부정적인 영향을 주지 않는 것이 중요합니다.DoS 공격과 같은 데이터 플레인 이벤트가 컨트롤 플레인에 영향을 미치는 경우 전체 네트워크가 불안정해질 수 있습니다.Cisco IOS 소프트웨어 기능 및 컨피그레이션에 대한 이 정보는 컨트롤 플레인의 복원력을 보장하는 데 도움이 됩니다.

일반 컨트롤 플레인 강화

컨트롤 플레인이 관리 플레인과 데이터 플레인을 유지 관리하고 운영하도록 보장하므로 네트워크 디바이스의 컨트롤 플레인을 보호하는 것이 중요합니다.보안 사고 중에 컨트롤 플레인이 불안정해지면 네트워크의 안정성을 복구하는 것이 불가능할 수 있습니다.

대부분의 경우 불필요한 패킷을 처리하는 데 필요한 CPU 로드의 양을 최소화하기 위해 인터페이스에서 특정 유형의 메시지를 수신하고 전송하는 것을 비활성화할 수 있습니다.

IP ICMP 리디렉션

ICMP 리디렉션 메시지는 패킷이 동일한 인터페이스에서 수신 및 전송될 때 라우터에서 생성될 수 있습니다.이 경우 라우터는 패킷을 전달하고 ICMP 리디렉션 메시지를 원래 패킷의 발신자에게 다시 전송합니다.이 동작을 사용하면 발신자가 라우터를 우회하고 향후 패킷을 대상(또는 대상에 가까운 라우터)으로 직접 전달할 수 있습니다. 제대로 작동하는 IP 네트워크에서 라우터는 자체 로컬 서브넷에 있는 호스트에만 리디렉션을 전송합니다.즉, ICMP 리디렉션은 레이어 3 경계를 넘어서는 안 됩니다.

두 가지 유형의 ICMP 리디렉션 메시지가 있습니다.전체 서브넷에 대한 호스트 주소 및 리디렉션을 위한 리디렉션.악의적인 사용자는 라우터에 패킷을 지속적으로 전송하여 ICMP 리디렉션을 전송하는 라우터의 기능을 악용하여 라우터가 ICMP 리디렉션 메시지로 응답하게 하고, 결과적으로 라우터의 CPU 및 성능에 부정적인 영향을 미칩니다.라우터가 ICMP 리디렉션을 전송하지 못하도록 하려면 no ip redirects interface configuration 명령**을** 사용합니다.

ICMP 연결 불가

인터페이스 액세스 목록을 사용하여 필터링하면 필터링된 트래픽의 소스로 ICMP 도달 불가 메시지 전송이 다시 이루어집니다.이러한 메시지를 생성하면 디바이스의 CPU 사용률이 증가할 수 있습니다.Cisco IOS 소프트웨어에서 ICMP 연결 불가 생성은 기본적으로 500밀리초마다 하나의 패킷으로 제한됩니다.인터페이스 컨피그레이션 명령 no ip unreachables를 사용하여 ICMP 연결 불가능 메시지 생성을 비활성화할 수 **있습니다**.전역 컨피그레이션 명령 ip icmp rate-limit unreachable interval-in-ms를 사용하여 ICMP 도달 불가 속도 제한**을** 기본값에서 변경할 수 있습니다.

프록시 ARP

프록시 ARP는 한 디바이스(일반적으로 라우터)가 다른 디바이스를 위해 의도된 ARP 요청에 응답하는 기술입니다.라우터는 ID를 "위조"하여 패킷을 실제 대상으로 라우팅할 책임을 받습니다.프록시 ARP는 라우팅 또는 기본 게이트웨이를 구성하지 않고도 서브넷의 시스템이 원격 서브넷에 도달할 수 있도록 도와줍니다.프록시 ARP는 RFC 1027에 정의되어 있습니다.

프록시 ARP 활용에는 몇 가지 단점이 있습니다.네트워크 세그먼트의 ARP 트래픽 양과 리소스 소모 및 중간자 공격(man-in-the-middle attack)이 증가할 수 있습니다.프록시 ARP는 프록시된 각 ARP 요청이 적은 양의 메모리를 사용하므로 리소스 소모 공격 벡터를 나타냅니다.공격자가 많은 ARP 요청을 전송할 경우 사용 가능한 모든 메모리를 폐기할 수 있습니다.

Man-in-the-middle 공격은 네트워크의 호스트가 라우터의 MAC 주소를 스푸핑할 수 있게 합니다. 따라서 의심하지 않는 호스트가 공격자에게 트래픽을 전송합니다.인터페이스 컨피그레이션 명령 **no ip proxy-arp**로 프록시 ARP를 비활성화할 수 **있습니다**.

이 기능*에* 대한 자세한 내용은 프록시 ARP 활성화를 참조하십시오.

컨트롤 플레인 트래픽의 CPU 영향 제한

컨트롤 플레인의 보호가 중요합니다.데이터 및 관리 트래픽 없이 애플리케이션 성능 및 최종 사용자 환경에 문제가 발생할 수 있기 때문에 컨트롤 플레인의 존속성을 통해 다른 두 플레인이 유지되고 작동합니다.

컨트롤 플레인 트래픽 이해

Cisco IOS 디바이스의 컨트롤 플레인을 제대로 보호하려면 CPU에서 프로세스를 전환하는 트래픽 유형을 파악하는 것이 중요합니다.프로세스 스위치드 트래픽은 일반적으로 두 가지 유형의 트래픽으로 구성됩니다.첫 번째 트래픽 유형은 Cisco IOS 디바이스로 전달되며 Cisco IOS 디바이스 CPU에서 직접 처리해야 합니다.이 트래픽은 Receive adjacency *traffic* 카테고리로 구성됩니다.이 트래픽에는 Cisco CEF(Express Forwarding) 테이블의 항목이 포함되어 있습니다. 이 항목에서는 다음 라우터 홉이 디바이스 자체이며, **show ip cef** CLI 출력에서 receive라는 용어로 표시됩니다.이 표시는 인터페이스 IP 주소, 멀티캐스트 주소 공간 및 브로드캐스트 주소 공간을 포함하는 Cisco IOS 디바이스 CPU에서 직접 처리해야 하는 모든 IP 주소의 경우입니다.

CPU에서 처리하는 두 번째 트래픽 유형은 데이터 플레인 트래픽, 즉 Cisco IOS 디바이스 자체를 벗어난 대상이 있는 트래픽입니다. 이 트래픽은 CPU에서 특별한 처리를 필요로 합니다.데이터 플레인 트래픽에 영향을 주는 CPU의 전체 목록은 아니지만 이러한 유형의 트래픽은 프로세스 스위칭되므로 컨트롤 플레인 작업에 영향을 줄 수 있습니다.

- **Access Control List 로깅** - ACL 로깅 트래픽은 log 키워드가 사용되는 ACE의 일치(허용 또는 거부)로 인해 생성된 패킷으로 구성됩니다.
- **유니캐스트 RPF(Unicast Reverse Path Forwarding)** - ACL과 함께 사용되는 유니캐스트 RPF는 특정 패킷의 프로세스 전환을 초래할 수 있습니다.
- **IP 옵션** - 옵션이 포함된 모든 IP 패킷은 CPU에서 처리해야 합니다.
- **조각화** - 조각화가 필요한 모든 IP 패킷은 처리를 위해 CPU에 전달되어야 합니다.
- **TTL(Time-to-Live) 만료** - TTL 값이 1보다 작거나 같은 패킷에는 ICMP 유형 11, 코드 0(Internet Control Message Protocol Time Exceeded) 메시지가 전송되어야 CPU 처리가 발생합니다.
- **ICMP Unreachables** - 라우팅, MTU 또는 필터링으로 인해 ICMP에 연결할 수 없는 메시지가 발생하는 패킷은 CPU에서 처리됩니다.
- **ARP 요청이 필요한 트래픽** - ARP 항목이 없는 대상은 CPU에서 처리해야 합니다.
- **비 IP 트래픽** - 모든 비 IP 트래픽은 CPU에서 처리됩니다.

이 목록은 Cisco IOS 디바이스 CPU에서 처리 중인 트래픽 유형을 확인하는 몇 가지 방법을 자세히 설명합니다.

- show **ip cef** 명령은 CEF 테이블에 포함된 각 IP 접두사에 대한 next-hop 정보를 제공합니다.앞에서 설명한 것처럼, "Next Hop"으로 수신하는 항목이 수신 인접성으로 간주되며 트래픽이 CPU로 직접 전송되어야 함을 나타냅니다.
- show **interface switching** 명령은 디바이스에서 처리하는 패킷의 수에 대한 정보를 제공합니다.
- show **ip traffic** 명령은 IP 패킷 수에 대한 정보를 제공합니다.

  로컬 대상(즉, 수신 인접성 트래픽)과 함께옵션 포함프래그먼트화가 필요한 경우브로드캐스트 주소 공간으로 전송됨멀티캐스트 주소 공간으로 전송되는

- 수신 인접성 트래픽은 **show ip cache flow** 명령을 사용하여 식별할 수 있습니다.Cisco IOS 디바이스로 향하는 모든 플로우에는 로컬의 DstIf(Destination Interface)가 있습니다.

- **컨트롤 플레인 폴리싱을** 사용하여 Cisco IOS 디바이스의 컨트롤 플레인에 도달하는 트래픽의 유형 및 속도를 식별할 수 있습니다.세분화된 분류 ACL 사용, 로깅 및 **show policy-map control-plane** 명령을 사용하여 컨트롤 플레인 폴리싱을 수행할 수 있습니다.

인프라 ACL

iACL(Infrastructure ACL)은 네트워크 디바이스에 대한 외부 통신을 제한합니다.인프라 ACL은 이 문서의 Limit Access to the Network with Infrastructure ACLs(인프라 ACL로 네트워크에 대한 액세스 제한) 섹션에서 광범위하게 다룹니다.

모든 네트워크 디바이스의 컨트롤 플레인을 보호하려면 iACL을 구현하는 것이 좋습니다.

수신 ACL

분산 플랫폼의 경우 rACL(Receive ACL)은 12000(GSR)의 Cisco IOS Software Releases 12.0(21)S2, 7500의 12.0(24)S, 10720의 12.0(31)S의 옵션일 수 있습니다. rACL은 유해한 디바이스로부터 보호됩니다. 트래픽이 경로 프로세서에 영향을 미치기 전에 트래픽이 트래픽에 영향을 미칩니다.수신 ACL은 구성된 디바이스만 보호하도록 설계되었으며 전송 트래픽은 rACL의 영향을 받지 않습니다.따라서 아래의 ACL 항목 예제에 사용되는 대상 IP 주소는 라우터의 물리적 또는 가상 IP 주소만 참조합니다.또한 수신 ACL은 네트워크 보안 모범 사례로 간주되며, 좋은 네트워크 보안을 장기적으로 추가하는 것으로 간주해야 합니다.

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
!
```

자세한 내용은 GSR:액세스 제어 목록 수신 - 디바이스에 대한 합법적인 트래픽을 식별하고 허용하고 원치 않는 모든 패킷을 거부하도록 지원합니다.

CoPP

CoPP 기능을 사용하여 인프라 디바이스로 전송되는 IP 패킷을 제한할 수도 있습니다.이 예에서는 신뢰할 수 있는 호스트의 SSH 트래픽만 Cisco IOS 디바이스 CPU에 연결할 수 있습니다.

> **참고:**알 수 없거나 신뢰할 수 없는 IP 주소에서 트래픽을 삭제하면 동적으로 할당된 IP 주소가 있는 호스트가 Cisco IOS 디바이스에 연결하지 못할 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 권한 없는 패킷과 허용 작업과 일치하는 ACL 항목은 policy-map drop 함수에서 이러한 패킷을 폐기하는 반면, 거부 작업과 일치하는 패킷은 policy-map drop 함수에서 영향을 받지 않습니다.

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

CoPP 기능의 구성 및 사용에 대한 자세한 내용은 컨트롤 플레인 폴리싱 구축을 참조하십시오.

컨트롤 플레인 보호

Cisco IOS Software Release 12.4(4)T에 도입된 CPPr(Control Plane Protection)을 사용하여 Cisco IOS 디바이스의 CPU로 향하는 컨트롤 플레인 트래픽을 제한하거나 차단할 수 있습니다.CoPP와 유사하지만 CPPr은 트래픽을 더욱 세분화하여 제한할 수 있습니다.CPPr은 집계 컨트롤 플레인을 하위 인터페이스라고 하는 세 개의 개별 컨트롤 플레인 카테고리로 나눕니다.Host, Transit 및 CEF-Exception 트래픽 범주에 대한 하위 인터페이스가 있습니다.또한 CPPr에는 다음과 같은 컨트롤 플레인 보호 기능이 포함되어 있습니다.

- **포트 필터링 기능** - 이 기능은 닫힘 또는 비수신 TCP 또는 UDP 포트로 전송되는 패킷을 폴리싱하고 삭제하는 기능을 제공합니다.
- **Queue-thresholding 기능** - 이 기능은 제어 평면 IP 입력 대기열에서 허용되는 지정된 프로토콜에 대한 패킷 수를 제한합니다.

CPPr 기능의 구성 및 사용에 대한 자세한 내용은 컨트롤 플레인 보호 및 CPPr(컨트롤 플레인 보호) 이해를 *참조하십시오.*

하드웨어 레이트 리미터

Cisco Catalyst 6500 Series Supervisor Engine 32 및 Supervisor Engine 720은 특수한 네트워킹 시나리오에 대해 플랫폼별 하드웨어 기반 레이트 리미터(HWRL)를 지원합니다.이러한 하드웨어 속도 리미터는 미리 정의된 IPv4, IPv6, 유니캐스트 및 멀티캐스트 DoS 시나리오 세트를 포함하기 때문에 특별 사례 속도 리미터라고 합니다.HWRL은 CPU에서 패킷을 처리해야 하는 다양한 공격으로부터 Cisco IOS 디바이스를 보호할 수 있습니다.

기본적으로 여러 HWRL이 활성화되어 있습니다.자세한 내용은 PFC3 하드웨어 기반 레이트 리미터 기본 설정을 참조하십시오.

HWRL에 대한 자세한 내용은 PFC3의 하드웨어 기반 속도 리미터를 참조하십시오.

보안 BGP

BGP(Border Gateway Protocol)는 인터넷의 라우팅 기반입니다.따라서 적정 수준 이상의 연결 요구사항을 가진 조직은 BGP를 사용하는 경우가 많습니다.BGP는 유비쿼티와 소규모 조직에서 BGP 컨피그레이션의 특성을 *잊기* 때문에 공격자의 표적이 되는 경우가 많습니다.그러나 BGP 컨피그레이션의 보안을 강화하는 데 활용할 수 있는 BGP 관련 보안 기능이 많이 있습니다.

이는 가장 중요한 BGP 보안 기능의 개요를 제공합니다.적절한 경우 컨피그레이션 권장 사항이 제공됩니다.

TTL 기반 보안 보호

각 IP 패킷에는 TTL(Time to Live)이라고 하는 1바이트 필드가 포함되어 있습니다. IP 패킷이 통과하는 각 디바이스는 이 값을 1씩 감소시킵니다.시작 값은 운영 체제에 따라 다르며 일반적으로 범위는 64~255입니다. 패킷의 TTL 값이 0에 도달하면 패킷이 삭제됩니다.

TTL 기반 보안 보호 기능은 GTSM(Generalized TTL-based Security Mechanism) 및 BTSH(BGP TTL Security Hack)라고도 하며, TTL 기반 보안 보호 기능은 IP 패킷의 TTL 값을 활용하여 수신되는 BGP 패킷이 직접 연결된 피어에서 오도록 합니다.이 기능을 사용하려면 피어링 라우터에서 조정해야 하는 경우가 많습니다.그러나 활성화되면 BGP에 대한 많은 TCP 기반 공격을 완전히 차단할 수 있습니다.

BGP용 GTSM은 neighbor BGP 라우터 컨피그레이션 명령에 대한 **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 패킷이 수신되면 TTL 값이 확인되고 지정된 hop-count를 255보다 크거나 같아야 합니다.

MD5를 사용한 BGP 피어 인증

MD5를 사용한 피어 인증은 BGP 세션의 일부로 전송되는 각 패킷의 MD5 다이제스트를 생성합니다.특히 다이제스트를 생성하기 위해 IP 및 TCP 헤더, TCP 페이로드 및 비밀 키의 일부가 사용됩니다.

생성된 다이제스트는 RFC 2385에 의해 특별히 만들어진 TCP 옵션 Kind 19에 저장됩니다.수신 BGP 스피커는 메시지 다이제스트를 재생성하기 위해 동일한 알고리즘과 비밀 키를 사용합니다.수신 및 계산된 다이제스트가 동일하지 않으면 패킷이 삭제됩니다.

MD5를 사용한 피어 인증은 neighbor BGP 라우터 컨피그레이션 명령에 대한 **password** 옵션으로 구성됩니다.이 명령의 사용법은 다음과 같습니다.

```
!

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

MD5*를* 사용한 BGP 피어 인증에 대한 자세한 내용은 네이버 라우터 인증을 *참조하십시오*.

최대 접두사 구성

BGP 접두사는 라우터가 메모리에 저장합니다.라우터가 보유해야 하는 접두사가 많을수록 BGP에서 사용해야 하는 메모리가 더 많습니다.일부 컨피그레이션에서는 모든 인터넷 접두사의 하위 집합을 저장할 수 있습니다. 이를테면 공급자의 고객 네트워크에 대한 기본 경로나 경로만 활용하는 컨피그레이션입니다.

메모리 소모를 방지하려면 피어별로 허용되는 접두사의 최대 수를 구성하는 것이 중요합니다.각 BGP 피어에 대해 제한을 구성하는 것이 좋습니다.

neighbor maximum-prefix BGP 라우터 컨피그레이션 명령을 사용하여 이 기능**을** 구성할 때 하나의 인수가 필요합니다.피어가 종료되기 전에 허용되는 접두사의 최대 수입니다.선택적으로, 1에서 100 사이의 숫자를 입력할 수도 있습니다.이 숫자는 로그 메시지가 전송되는 지점의 최대 접두사 값의 백분율을 나타냅니다.

```
!

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

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

접두사 목록으로 BGP 접두사 필터링

접두사 목록을 사용하면 네트워크 관리자가 BGP를 통해 보내거나 받는 특정 접두사를 허용하거나 거부할 수 있습니다.네트워크 트래픽이 원하는 경로를 통해 전송되도록 하려면 가능한 경우 접두사 목록을 사용해야 합니다.인바운드 및 아웃바운드 방향 모두에서 각 eBGP 피어에 접두사 목록을 적용해야 합니다.

구성된 접두사 목록은 전송되거나 수신되는 접두사를 네트워크의 라우팅 정책에서 특별히 허용하는 접두사로 제한합니다.수신된 접두사 수가 많아 이 작업을 수행할 수 없는 경우, 알려진 잘못된 접두사를 구체적으로 차단하도록 접두사 목록을 구성해야 합니다.이러한 잘못된 접두사는 할당되지 않은 IP 주소 공간과 RFC 3330에서 내부 또는 테스트 목적으로 예약된 네트워크를 포함합니다.아웃바운드 접두사 목록은 조직이 광고하려는 접두사만 특별히 허용하도록 구성해야 합니다.

이 컨피그레이션 예에서는 접두사 목록을 사용하여 학습되고 광고되는 경로를 제한합니다.특히 접

두사 목록 BGP-PL-INBOUND에 의해 인바운드되는 기본 경로만 허용되며 접두사 192.168.2.0/24은 BGP-PL-OUTBOUND에 의해 광고될 수 있는 유일한 경로입니다.

```
!

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 커버리지는 외부 BGP를 사용하여 서비스 공급자에 연결을 참조하십시오.

자동 시스템 경로 액세스 목록을 사용하여 BGP 접두사 필터링

BGP AS(Autonomous System) 경로 액세스 목록을 사용하면 접두사의 AS-path 특성을 기반으로 수신 및 광고된 접두사를 필터링할 수 있습니다.강력한 필터 집합을 설정하기 위해 접두사 목록과 함께 사용할 수 있습니다.

이 컨피그레이션 예에서는 AS 경로 액세스 목록을 사용하여 인바운드 접두사를 원격 AS에 의해 시작된 접두사와 로컬 자동 시스템에 의해 시작된 접두사로 제한합니다.다른 모든 자동 시스템에서 제공된 접두사는 필터링되며 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

네트워크의 토폴로지 변경 사항 또는 결함에서 트래픽을 적절하게 전달하고 복구할 수 있는 기능은 토폴로지의 정확한 보기에 따라 달라집니다.이 보기를 제공하기 위해 IGP(Interior Gateway Protocol)를 실행할 수 있습니다.기본적으로 IGP는 동적이며 사용 중인 특정 IGP와 통신하는 추가 라우터를 검색합니다.또한 IGP는 네트워크 링크 장애 시 사용할 수 있는 경로를 검색합니다.

이 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 다루는 권장 사항과 예가 제공됩니다.

메시지 다이제스트 5를 통한 라우팅 프로토콜 인증 및 확인

라우팅 정보의 교환을 보안하지 못하면 공격자는 네트워크에 잘못된 라우팅 정보를 도입할 수 있습니다.라우터 간 라우팅 프로토콜과 함께 비밀번호 인증을 사용하여 네트워크의 보안을 지원할 수 있습니다.그러나 이 인증은 일반 텍스트로 전송되므로 공격자가 이 보안 제어를 반전시키는 것이

간단할 수 있습니다.

인증 프로세스에 MD5 해시 기능을 추가하면 라우팅 업데이트에 더 이상 일반 텍스트 비밀번호가 포함되지 않으며 라우팅 업데이트의 전체 내용이 변조에 더 잘 방지됩니다.그러나 MD5 인증은 약한 비밀번호를 선택할 경우 여전히 무작위 대입 및 사전 공격에 취약합니다.충분한 임의 지정과 함께 비밀번호를 사용하는 것이 좋습니다.MD5 인증은 비밀번호 인증과 비교할 때 훨씬 안전하므로, 이러한 예제는 MD5 인증에만 해당됩니다.IPSec을 사용하여 라우팅 프로토콜을 검증하고 보호할 수도 있지만, 이러한 예에서는 사용을 자세히 설명하지 않습니다.

EIGRP 및 RIPv2는 컨피그레이션의 일부로 키 체인을 사용합니다.*키 체인* 구성 및 사용에 대한 자세한 내용은 키를 참조하십시오.

다음은 MD5를 사용하는 EIGRP 라우터 인증을 위한 컨피그레이션의 예입니다.

```
!

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 RIPv2에 대한 MD5 라우터 인증 컨피그레이션의 예입니다. RIPv1은 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>
!
```

이것은 MD5를 사용하는 OSPF 라우터 인증을 위한 컨피그레이션의 예입니다. OSPF는 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 구성 을 참조하십시오.

패시브 인터페이스 명령

라우팅 정보의 광고를 제어하는 데 도움이 되는 passive-interface 명령을 사용하여 정보 유출 또는 IGP에 잘못된 정보의 도입을 줄일 수 있습니다.관리 제어 외부에 있는 네트워크에 어떤 정보도 광고하지 않는 것이 좋습니다.

다음 예에서는 이 기능의 사용법을 보여 줍니다.

```
!

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

경로 필터링

네트워크에서 잘못된 라우팅 정보를 도입할 가능성을 줄이려면 경로 필터링을 사용해야 합니다 .passive-interface 라우터 컨피그레이션 명령과 달리 경로 필터링이 활성화되면 인터페이스에서 라우팅이 발생하지만 알림 또는 처리되는 정보는 제한됩니다.

EIGRP 및 RIP의 경우 **out** 키워드를 사용하여 distribute-list 명령을 사용하면 광고되는 정보가 제한되고 in 키워드의 사용에서는 처리되는 업데이트가 제한됩니다.distribute-list 명령은 OSPF에 사용할 수 있지만 라우터가 필터링된 경로를 전파하는 것을 방지하지 않습니다.대신 **area filter-list** 명령을 사용할 수 있습니다.

이 EIGRP 예에서는 distribute-list 명령 및 접두사 목록을 사용하여 아웃바운드 광고를 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>
!
```

이 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 업데이트의 광고 및 처리를 제어하는 방법에 대한 자세한 내용은 IP 라우팅 프로토콜 독립 기능 구성을 *참조하십시오*.

이 OSPF 예에서는 OSPF 특정 **영역 filter-list** 명령과 함께 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
!
```

공정순서 프로세스 자원 소비

라우팅 프로토콜 접두사는 라우터가 메모리에 저장하며, 라우터가 보유해야 하는 접두사가 추가되어 리소스 소비가 증가합니다.리소스 소모를 방지하려면 리소스 소비를 제한하도록 라우팅 프로토콜을 구성하는 것이 중요합니다.Link State Database Overload Protection 기능을 사용하는 경우 OSPF에서 이 작업을 수행할 수 있습니다.

다음 예에서는 OSPF 링크 상태 데이터베이스 오버로드 보호 기능의 컨피그레이션을 보여 줍니다.

```
!

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*.

안전한 First Hop 이중화 프로토콜

FHRP(First Hop Redundancy Protocols)는 기본 게이트웨이 역할을 하는 디바이스에 복원력과 이중화를 제공합니다.이러한 상황과 이러한 프로토콜은 레이어 3 디바이스 쌍이 네트워크 세그먼트나 서버 또는 워크스테이션이 포함된 VLAN 집합에 대해 기본 게이트웨이 기능을 제공하는 환경에서 일반적입니다.

GLBP(Gateway Load-Balancing Protocol), HSRP(Hot Standby Router Protocol) 및 VRRP(Virtual Router Redundancy Protocol)는 모두 FHRP입니다.기본적으로 이러한 프로토콜은 인증되지 않은 통신과 통신합니다.이러한 종류의 통신을 통해 공격자는 FHRP 말하기 장치로 포즈하여 네트워크에서 기본 게이트웨이 역할을 맡을 수 있습니다.이 인계를 통해 공격자는 중간자 공격을 수행하고 네트워크에서 나가는 모든 사용자 트래픽을 차단할 수 있습니다.

이러한 유형의 공격을 방지하기 위해 Cisco IOS 소프트웨어에서 지원하는 모든 FHRP에는 MD5 또는 텍스트 문자열로 된 인증 기능이 포함됩니다.인증되지 않은 FHRP에 의해 발생하는 위협 때문에 이러한 프로토콜의 인스턴스는 MD5 인증을 사용하는 것이 좋습니다.이 컨피그레이션 예에서는 GLBP, HSRP 및 VRRP MD5 인증을 사용하는 방법을 보여 줍니다.

```
!

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 플레인은 소스에서 대상으로 데이터를 이동하는 작업을 담당하지만, 보안 맥락에서 데이터 플레인은 세 평면 중 가장 중요하지 않습니다.따라서 네트워크 디바이스를 보호할 때 데이터 플레인보다 관리 플레인과 컨트롤 플레인을 우선적으로 보호하는 것이 중요합니다.

그러나 데이터 플레인 자체에는 트래픽을 보호하는 데 도움이 되는 다양한 기능과 구성 옵션이 있습니다.이 섹션에서는 네트워크 보안을 더욱 쉽게 유지할 수 있도록 이러한 기능 및 옵션에 대해 자세히 설명합니다.

일반 데이터 플레인 강화

대부분의 데이터 플레인 트래픽은 네트워크의 라우팅 컨피그레이션에 따라 네트워크를 통해 이동합니다.그러나 네트워크 전체의 패킷 경로를 변경하는 IP 네트워크 기능이 있습니다.IP 옵션, 특히 소스 라우팅 옵션과 같은 기능은 오늘날의 네트워크에서 보안 문제를 야기합니다.

트랜짓 ACL의 사용은 데이터 플레인의 강화와도 관련이 있습니다.

*자세한 내용*은 이 문서의 Filter Transit Traffic with Transit ACLs 섹션을 참조하십시오.

IP 옵션 선택적 삭제

IP 옵션에는 두 가지 보안 문제가 있습니다.IP 옵션이 포함된 트래픽은 Cisco IOS 디바이스에서 프로세스를 전환해야 하며, 이로 인해 CPU 로드가 증가할 수 있습니다.또한 IP 옵션에는 트래픽이 네트워크를 통해 이동하는 경로를 변경하는 기능이 포함되어 있어 보안 제어를 파괴할 수 있습니다.

이러한 문제로 인해 전역 구성 명령 **ip 옵션 {drop | ignore}**이(가) Cisco IOS Software 릴리스 12.3(4)T, 12.0(22)S 및 12.2(25)S에 추가되었습니다.이 명령의 첫 번째 형식에서 **ip options drop**은 Cisco IOS 디바이스에서 수신한 IP 옵션이 포함된 모든 IP 패킷이 삭제됩니다.이렇게 하면 IP 옵션이 활성화할 수 있는 보안 컨트롤의 향상된 CPU 로드 및 가능한 하위 버전이 모두 방지됩니다.

이 명령의 두 번째 형식인 **ip options ignore**는 수신된 패킷에 포함된 IP 옵션을 무시하도록 Cisco IOS 디바이스를 구성합니다.이렇게 하면 로컬 디바이스의 IP 옵션과 관련된 위협이 완화되지만, 다운스트림 디바이스가 IP 옵션이 있는 경우 영향을 받을 수 있습니다.따라서 이 명령의 **삭제** 형식을 사용하는 것이 좋습니다.이 내용은 컨피그레이션 예에 나와 있습니다.

```
!
ip options drop
!
```

RSVP와 같은 일부 프로토콜은 IP 옵션을 합법적으로 사용합니다.이러한 프로토콜의 기능은 이 명령의 영향을 받습니다.

IP Options Selective Drop이 활성화되면 **show ip traffic** EXEC 명령을 사용하여 IP 옵션이 있어 삭

제된 패킷 수를 확인할 수 있습니다.이 정보는 강제 드롭 카운터에 있습니다.

이 기능*에* 대한 자세한 내용은 ACL IP 옵션 선택적 삭제를 *참조하십시오*.

IP 소스 라우팅 비활성화

IP 소스 라우팅은 Loose Source Route 및 Record Route 옵션을 Record Route 옵션과 함께 동시에 사용하거나 Strict Source Route를 사용하여 IP 데이터그램의 소스를 활성화하여 패킷이 수행하는 네트워크 경로를 지정합니다.이 기능은 네트워크의 보안 제어 주위로 트래픽을 라우팅하려는 시도에 사용할 수 있습니다.

IP Options Selective Drop 기능을 통해 IP 옵션을 완전히 비활성화하지 않은 경우 IP 소스 라우팅을 비활성화하는 것이 중요합니다.모든 Cisco IOS 소프트웨어 릴리스에서 기본적으로 활성화된 IP 소스 라우팅은 **no ip source-route** 전역 컨피그레이션 명령을 통해 비활성화됩니다.다음 컨피그레이션 예에서는 이 명령의 사용을 보여줍니다.

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

ICMP 리디렉션 비활성화

ICMP 리디렉션은 네트워크 디바이스에 IP 대상에 대한 더 나은 경로를 알리기 위해 사용됩니다.기본적으로 Cisco IOS 소프트웨어는 수신한 인터페이스를 통해 라우팅해야 하는 패킷을 수신하면 리디렉션을 전송합니다.

경우에 따라 공격자가 Cisco IOS 디바이스에서 많은 ICMP 리디렉션 메시지를 전송하도록 하여 CPU 로드가 증가할 수 있습니다.따라서 ICMP 리디렉션 전송을 비활성화하는 것이 좋습니다.ICMP 리디렉션은 인터페이스 컨피그레이션 **no ip redirects** 명령으로 비활성화되며, 예시 컨피그레이션에 나와 있습니다.

```
!

interface FastEthernet 0
no ip redirects
!
```

IP Directed Broadcast 비활성화 또는 제한

IP Directed Broadcast를 사용하면 원격 IP 서브넷에 IP 브로드캐스트 패킷을 전송할 수 있습니다.원격 네트워크에 도달하면 전달 IP 디바이스는 패킷을 레이어 2 브로드캐스트로 서브넷의 모든 스테이션에 전송합니다.이러한 직접 브로드캐스트 기능은 스머프 공격을 비롯한 여러 공격에 대한 증폭과 반사 지원 수단으로 활용되었습니다.

현재 버전의 Cisco IOS 소프트웨어는 기본적으로 이 기능을 비활성화하고 있습니다.그러나 **ip directed-broadcast** interface configuration 명령을 통해 활성화할 수 있습니다.12.0 이전의 Cisco IOS 소프트웨어 릴리스에서는 기본적으로 이 기능이 활성화되어 있습니다.

네트워크에 직접 브로드캐스트 기능이 절대적으로 필요한 경우 그 사용을 제어해야 합니다.이는 액세스 제어 목록을 ip directed-broadcast 명령에 대한 옵션으로 사용할 경우 가능합니다.이 컨피그레이션 예에서는 신뢰할 수 있는 네트워크, 192.168.1.0/24에서 시작하는 UDP 패킷으로 디렉티드 브로드캐스트를 제한합니다.

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

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

통과 ACL을 사용하여 통과 트래픽 필터링

tACL(transit ACL)을 사용하여 네트워크를 통과하는 트래픽을 제어할 수 있습니다. 이는 네트워크 자체를 대상으로 하는 트래픽을 필터링하려는 인프라 ACL과 대조적입니다.tACL에서 제공하는 필터링은 네트워크를 이동하는 특정 디바이스 또는 트래픽 그룹으로 트래픽을 필터링하는 것이 바람직할 때 유용합니다.

이러한 유형의 필터링은 일반적으로 방화벽에 의해 수행됩니다.그러나 네트워크의 Cisco IOS 디바이스에서 이 필터링을 수행하는 것이 유용할 수 있는 인스턴스가 있습니다. 예를 들어, 필터링은 수행해야 하지만 방화벽은 없습니다.

트랜짓 ACL은 또한 정적 스푸핑 방지 보호를 구현하기에 적합한 장소입니다.

*자세한 내용*은 이 문서의 Anti-Spoofing Protections 섹션을 참조하십시오.

자세한 내용은 이동 액세스 제어 목록:tACL에 대한 자세한 내용은 에지에서 필터링

ICMP 패킷 필터링

ICMP(Internet Control Message Protocol)는 IP를 위한 제어 프로토콜로 설계되었습니다.따라서, 이 메시지가 전달하는 메시지는 일반적으로 TCP 및 IP 프로토콜에서 상당히 영향을 미칠 수 있습니다.ICMP는 네트워크 문제 해결 툴 ping 및 **traceroute**와 경로 MTU 검색에 사용됩니다.그러나 네트워크의 올바른 작동을 위해 외부 ICMP 연결이 거의 필요하지 않습니다.

Cisco IOS 소프트웨어는 이름 또는 유형 및 코드별로 ICMP 메시지를 특별히 필터링하는 기능을 제공합니다.이 예제 ACL은 신뢰할 수 있는 네트워크에서 ICMP를 허용하는 동시에 다른 소스에서 오는 모든 ICMP 패킷을 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 조각 필터링

앞서 이 문서의 Limit Access to the Network with Infrastructure ACLs(인프라 ACL을 사용하여 네트

워크에 대한 액세스 제한) 섹션에서 자세히 설명한 것처럼 프래그먼트된 IP 패킷의 필터링은 보안 디바이스에 문제를 일으킬 수 있습니다.

프래그먼트 처리의 직관적이지 않은 특성 때문에 ACL에서 실수로 IP 프래그먼트를 허용하는 경우가 많습니다.프래그먼트화는 침입 탐지 시스템의 탐지를 회피하려는 시도에도 자주 사용됩니다.이러한 이유로 인해 IP 프래그먼트가 공격에 자주 사용되며 구성된 모든 tACL의 맨 위에서 명시적으로 필터링되어야 합니다.아래 ACL에는 IP 프래그먼트의 포괄적인 필터링이 포함되어 있습니다.이 예에서 설명하는 기능은 이전 예제의 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
!
```

프래그먼트된 IP 패킷의 ACL 처리에 대한 자세한 내용은 Access Control Lists and IP Fragments를 *참조하십시오*.

IP 옵션 필터링을 위한 ACL 지원

Cisco IOS Software Release 12.3(4)T 이상에서 Cisco IOS 소프트웨어는 ACL을 사용하여 패킷에 포함된 IP 옵션을 기반으로 IP 패킷을 필터링할 수 있습니다.패킷에 IP 옵션이 있으면 네트워크에서 보안 제어를 뒤집거나 패킷의 트랜짓 특성을 변경하려는 시도가 있을 수 있습니다.IP 옵션이 있는 패킷은 네트워크 에지에서 필터링해야 하는 이유가 여기에 있습니다.

이 예는 IP 옵션이 포함된 IP 패킷의 전체 필터링을 포함하려면 이전 예제의 내용과 함께 사용해야 합니다.

```
!

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

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

스푸핑 방지 보호

많은 공격에서는 소스 IP 주소 스푸핑을 사용하여 공격의 진정한 소스를 숨기거나 정확한 역추적을 방해합니다.Cisco IOS 소프트웨어는 소스 IP 주소 스푸핑에 의존하는 공격을 차단하기 위해 유니캐스트 RPF 및 IPSG(IP Source Guard)를 제공합니다.또한 ACL과 null 라우팅은 스푸핑 방지를 위한 수동 수단으로 구축되는 경우가 많습니다.

IP Source Guard는 스위치 포트, MAC 주소 및 소스 주소 확인을 수행하여 직접 관리 제어 하에 있는 네트워크에 대한 스푸핑을 최소화합니다.유니캐스트 RPF는 소스 네트워크 확인을 제공하며 직

접 관리 제어를 받지 않는 네트워크에서 스푸핑된 공격을 줄일 수 있습니다.포트 보안을 사용하여 액세스 레이어에서 MAC 주소를 검증할 수 있습니다.DAI(Dynamic Address Resolution Protocol)는 로컬 세그먼트에서 ARP 독을 사용하는 공격 벡터를 완화합니다.

유니캐스트 RPF

유니캐스트 RPF를 사용하면 디바이스에서 패킷을 받은 인터페이스를 통해 전달된 패킷의 소스 주소에 연결할 수 있는지 확인할 수 있습니다.스푸핑에 대한 유일한 보호 기능으로서 유니캐스트 RPF에 의존해서는 안 됩니다.소스 IP 주소에 대한 적절한 반환 경로가 있는 경우 스푸핑된 패킷은 유니캐스트 RPF 지원 인터페이스를 통해 네트워크에 들어갈 수 있습니다.유니캐스트 RPF는 각 디바이스에서 Cisco Express Forwarding을 활성화하는 데 사용되며 인터페이스별로 구성됩니다.

유니캐스트 RPF는 다음 두 가지 모드 중 하나로 구성할 수 있습니다.느슨하거나 엄격함.비대칭 라우팅이 있는 경우 이러한 상황에서 패킷을 삭제하는 엄격한 모드가 알려져 있으므로 느슨한 모드가 선호됩니다.**ip verify** interface 컨피그레이션 명령을 구성하는 동안 **any** 키워드는 느슨한 모드를 구성하며 rx 키워드는 **strict** 모드를 구성합니다.

다음 예에서는 이 기능의 컨피그레이션을 설명합니다.

```
!

ip cef
!

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

유니캐스트 RPF 구성 및 사용에 대한 자세한 내용은 유니캐스트 역방향 경로 포워딩 이해를 참조하십시오.

IP 소스 가드

IP Source Guard는 레이어 2 인터페이스를 제어할 경우 사용할 수 있는 효과적인 스푸핑 방지 방법입니다.IP Source Guard는 DHCP 스누핑의 정보를 사용하여 레이어 2 인터페이스에서 PACL(포트 액세스 제어 목록)을 동적으로 구성하며, IP 소스 바인딩 테이블에 연결되지 않은 IP 주소의 트래픽을 거부합니다.

IP Source Guard는 DHCP 스누핑 지원 VLAN에 속하는 레이어 2 인터페이스에 적용할 수 있습니다.이 명령은 DHCP 스누핑을 활성화합니다.

```
!

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

DHCP 스누핑을 활성화한 후 다음 명령은 IPSG를 활성화합니다.

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

ip verify source port security interface configuration 명령을 사용하여 포트 보안을 활성화할 수 있습니다.이렇게 하려면 전역 컨피그레이션 명령 **ip dhcp snooping information 옵션이 필요합니다**.또한 DHCP 서버는 DHCP 옵션 82를 지원해야 합니다.

이 기능*에* 대한 자세한 내용은 DHCP 기능 및 IP Source Guard 구성을 참조하십시오.

포트 보안

포트 보안은 액세스 인터페이스에서 MAC 주소 스푸핑을 완화하기 위해 사용됩니다.포트 보안은 동적으로 학습된(스티커) MAC 주소를 사용하여 초기 컨피그레이션을 쉽게 수행할 수 있습니다.포트 보안에서 MAC 위반을 확인하면 4개의 위반 모드 중 하나를 사용할 수 있습니다.이러한 모드는 VLAN을 보호, 제한, 종료 및 종료합니다.포트가 표준 프로토콜을 사용하는 단일 워크스테이션에 대한 액세스만 제공하는 경우 최대 1개만으로도 충분할 수 있습니다.HSRP와 같은 가상 MAC 주소를 활용하는 프로토콜은 최대 수가 1로 설정된 경우 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 세그먼트에 대한 ARP 공격(ARP fishing)을 완화하기 위해 DAI(Dynamic ARP Inspection)를 사용할 수 있습니다.ARP 포이즈닝 공격은 공격자가 위조된 ARP 정보를 로컬 세그먼트에 전송하는 방법입니다.이 정보는 다른 디바이스의 ARP 캐시를 손상시키기 위해 설계되었습니다.공격자는 중간자 공격을 수행하기 위해 ARP 공격을 사용하는 경우가 많습니다.

DAI는 신뢰할 수 없는 포트에서 모든 ARP 패킷의 IP-MAC 주소 관계를 가로채고 검증합니다 .DHCP 환경에서 DAI는 DHCP 스누핑 기능에 의해 생성된 데이터를 사용합니다.신뢰할 수 있는 인터페이스에서 수신된 ARP 패킷은 검증되지 않으며, 신뢰할 수 없는 인터페이스의 유효하지 않은 패킷은 폐기됩니다.비 DHCP 환경에서는 ARP ACL을 사용해야 합니다.

이 명령은 DHCP 스누핑을 활성화합니다.

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

DHCP 스누핑이 활성화되면 다음 명령은 DAI를 활성화합니다.

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

비 DHCP 환경에서는 DAI를 활성화하려면 ARP ACL이 필요합니다.다음 예에서는 ARP ACL을 사

용하는 DAI의 기본 컨피그레이션을 보여 줍니다.

```
!

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

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

DAi는 지원되는 모든 곳에서 인터페이스별로 활성화할 수도 있습니다.

```
ip arp inspection limit rate <rate_value> burst interval <interval_value>
```

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

스푸핑 방지 ACL

수동으로 구성된 ACL은 알려진 미사용 및 신뢰할 수 없는 주소 공간을 사용하는 공격으로부터 정적 스푸핑 방지 보호를 제공할 수 있습니다.일반적으로 이러한 스푸핑 방지 ACL은 대규모 ACL의 구성 요소로 네트워크 경계에서 인그레스 트래픽에 적용됩니다.스푸핑 방지 ACL은 자주 변경될 수 있으므로 정기적인 모니터링이 필요합니다.트래픽을 유효한 로컬 주소로 제한하는 아웃바운드 ACL을 적용할 경우 로컬 네트워크에서 시작되는 트래픽에서 스푸핑을 최소화할 수 있습니다.

이 예에서는 IP 스푸핑을 제한하기 위해 ACL을 사용하는 방법을 보여 줍니다.이 ACL은 원하는 인터페이스에서 인바운드에 적용됩니다.이 ACL을 구성하는 ACE는 포괄적이지 않습니다.이러한 유형의 ACL을 구성하는 경우 확정된 최신 참조를 찾습니다.

```
!

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 목록*을 구성하는 방법에 대한 자세한 내용은 일반적으로 사용되는 IP ACL 구성을 참조하십시오.

할당되지 않은 인터넷 주소의 공식 목록은 팀 Cymru에서 관리합니다.사용하지 않는 주소 필터링에 대한 추가 정보는 Bogon Reference Page에서 확인할 수 있습니다.

데이터 플레인 트래픽의 CPU 영향 제한

라우터와 스위치의 주요 목적은 디바이스를 통해 패킷과 프레임을 최종 대상으로 전달하는 것입니다.네트워크 전체에 구축된 디바이스를 전송하는 이러한 패킷은 디바이스의 CPU 운영에 영향을 미칠 수 있습니다.네트워크 디바이스를 통과하는 트래픽으로 구성된 데이터 플레인은 관리 및 컨트롤 플레인의 작동을 보장하기 위해 보호되어야 합니다.트랜짓 트래픽으로 인해 디바이스에서 스위치 트래픽을 처리할 수 있는 경우 디바이스의 컨트롤 플레인에 영향을 주어 운영 중단이 발생할 수 있습니다.

CPU에 영향을 주는 기능 및 트래픽 유형

이 목록은 완전하지는 않지만 특수한 CPU 처리가 필요하고 CPU에서 프로세스를 전환하는 데이터 플레인 트래픽 유형을 포함합니다.

- **ACL 로깅** - ACL 로깅 트래픽은 **log** 키워드가 사용되는 ACE의 일치(허용 또는 거부)로 인해 생성된 모든 패킷으로 구성됩니다.
- **유니캐스트 RPF** - ACL과 함께 사용되는 유니캐스트 RPF는 특정 패킷의 프로세스 전환을 초래할 수 있습니다.
- **IP 옵션** - 옵션이 포함된 모든 IP 패킷은 CPU에서 처리해야 합니다.
- **조각화** - 조각화가 필요한 모든 IP 패킷은 처리를 위해 CPU에 전달되어야 합니다.
- **TTL(Time-to-Live) 만료** - TTL 값이 1보다 작거나 같은 패킷에는 ICMP 유형 11, 코드 0(Internet Control Message Protocol Time Exceeded) 메시지를 전송해야 하므로 CPU 처리가 발생합니다.
- **ICMP Unreachables** - 라우팅, MTU 또는 필터링으로 인해 ICMP에 연결할 수 없는 메시지가 발생하는 패킷은 CPU에서 처리됩니다.
- **ARP 요청이 필요한 트래픽** - ARP 항목이 없는 대상은 CPU에서 처리해야 합니다.
- **비 IP 트래픽** - 모든 비 IP 트래픽은 CPU에서 처리됩니다.

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

TTL 값 필터링

확장 IP 액세스 목록에서 Cisco IOS Software Release 12.4(2)T에 도입된 ACL Support for Filtering on TTL Value 기능을 사용하여 TTL 값을 기반으로 패킷을 필터링할 수 있습니다.TTL 값이 0 또는 1인 트랜짓 트래픽을 수신하는 디바이스를 보호하기 위해 이 기능을 사용할 수 있습니다.TTL 값을 기반으로 패킷을 필터링하는 것도 TTL 값이 네트워크의 지름보다 낮지 않은지 확인하기 위해 사용할 수 있으므로 다운스트림 인프라 디바이스의 컨트롤 플레인을 TTL 만료 공격으로부터 보호할 수 있습니다.

traceroute와 같은 일부 애플리케이션 및 툴은 테스트 및 진단 목적으로 TTL 만료 패킷을 사용합니다.IGMP와 같은 일부 프로토콜은 1의 TTL 값을 합법적으로 사용합니다.

이 ACL 예에서는 TTL 값이 6보다 작은 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 기준으로 패킷 필터링에 대한 자세한 내용은 TTL 만료 공격 식별 및 완화를 참조하십시오.

이 기능*에* 대한 자세한 내용은 TTL 값의 필터링을 위한 ACL 지원을 *참조하십시오*.

Cisco IOS Software Release 12.4(4)T 이상에서 FPM(Flexible Packet Matching)을 사용하면 관리자가 패킷의 임의의 비트에서 매칭할 수 있습니다.이 FPM 정책은 TTL 값이 6보다 작은 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
!
```

기능에 대한 자세한 내용은 Cisco IOS Flexible Packet Matching 홈 페이지에 있는 Flexible Packet Matching을 *참조하십시오*.

IP 옵션이 있는 경우 필터링

Cisco IOS Software Release 12.3(4)T 이상에서는 IP 옵션이 있는 IP 패킷을 필터링하기 위해 명명된 확장 IP 액세스 목록에서 IP 옵션 필터링 기능에 대한 ACL 지원을 사용할 수 있습니다.IP 옵션의 존재를 기반으로 하는 IP 패킷을 필터링하는 것도 인프라 디바이스의 컨트롤 플레인이 CPU 레벨에서 이러한 패킷을 처리할 필요가 없도록 하기 위해 사용할 수 있습니다.

ACL Support for Filtering IP Options 기능은 명명된 확장 ACL에서만 사용할 수 있습니다.또한 RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP 버전 2 및 3, IP 옵션 패킷을 사용하는 기타 프로토콜은 이러한 프로토콜에 대한 패킷이 삭제될 경우 제대로 작동하지 않을 수 있습니다.이러한 프로토콜이 네트워크에서 사용 중인 경우 IP 옵션 필터링에 대한 ACL 지원을 사용할 수 있습니다.그러나 ACL IP Options Selective Drop 기능은 이 트래픽을 삭제할 수 있으며 이러한 프로토콜이 제대로 작동하지 않을 수 있습니다.IP 옵션이 필요한 프로토콜을 사용 중인 프로토콜이 없는 경우 ACL IP Options Selective Drop이 이러한 패킷을 삭제하는 데 선호되는 방법입니다.

이 ACL 예에서는 IP 옵션이 포함된 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 ACL은 5개의 특정 IP 옵션으로 IP 패킷을 필터링하는 정책을 보여줍니다.다음 옵션을 포함하는 패킷은 거부됩니다.

- 0 옵션 목록 끝(eool)
- 7 레코드 경로(레코드 경로)
- 68 타임스탬프(타임스탬프)
- 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.

자세한 내용은 이동 액세스 제어 목록:트랜짓 및 에지 트래픽 필터링에 대한 자세한 내용을 보려면 에지에서 필터링하십시오.

Cisco IOS 소프트웨어의 또 다른 기능은 IP 옵션으로 패킷을 필터링하는 데 사용할 수 있는 CoPP입니다.Cisco IOS Software Release 12.3(4)T 이상에서는 관리자가 컨트롤 플레인 패킷의 트래픽 흐름을 필터링할 수 있습니다.Cisco IOS Software Release 12.3(4)T에 도입된 CoPP 및 ACL Support for Filtering IP Options를 지원하는 디바이스는 액세스 목록 정책을 사용하여 IP 옵션이 포함된 패킷을 필터링할 수 있습니다.

이 CoPP 정책은 IP 옵션이 있을 때 디바이스에서 수신하는 전송 패킷을 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
!
```

이 CoPP 정책은 다음 IP 옵션이 있을 때 디바이스에서 수신한 트랜짓 패킷을 삭제합니다.

- 0 옵션 목록 끝(eool)
- 7 레코드 경로(레코드 경로)
- 68 타임스탬프(타임스탬프)
- 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
!
```

앞의 CoPP 정책에서 허용 작업과 패킷을 매칭하는 ACE(액세스 제어 목록 항목)는 정책 맵 삭제 기능에 의해 폐기되는 반면, 거부 작업과 매칭하는 패킷(표시되지 않음)은 정책 맵 삭제 기능의 영향을 받지 않습니다.

*CoPP 기능*에 대한 자세한 내용은 컨트롤 플레인 정책 배포를 참조하십시오.

컨트롤 플레인 보호

Cisco IOS Software Release 12.4(4)T 이상에서 CPPr(Control Plane Protection)을 사용하여 Cisco

IOS 디바이스의 CPU로 컨트롤 플레인 트래픽을 제한하거나 차단할 수 있습니다.CoPP와 유사하지만 CPPr은 CoPP보다 세분화하여 트래픽을 제한하거나 폴리싱할 수 있습니다.CPPr은 집계 컨트롤 플레인을 하위 인터페이스라고 하는 세 개의 개별 컨트롤 플레인 카테고리로 나눕니다.Host, Transit 및 CEF-Exception 하위 인터페이스가 있습니다.

이 CPPr 정책은 TTL 값이 6보다 작고 TTL 값이 0 또는 1인 디바이스에서 수신한 통과 또는 비전송 패킷이 있는 디바이스에서 수신한 전송 패킷을 삭제합니다.또한 CPPr 정책은 디바이스에서 수신한 선택한 IP 옵션이 포함된 패킷을 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 허용 작업과 패킷을 매칭하는 액세스 제어 목록 항목은 이러한 패킷을 정책 맵 삭제 기능에 의해 폐기하는 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

경우에 따라, 특히 사고 대응 또는 네트워크 성능 저하 시 네트워크 트래픽을 신속하게 식별하고 역추적해야 합니다.NetFlow 및 Classification ACL은 Cisco IOS 소프트웨어를 사용하여 이를 수행하는 두 가지 주요 방법입니다.NetFlow는 네트워크의 모든 트래픽에 대한 가시성을 제공할 수 있습니다.또한 NetFlow는 장기적인 트렌드 분석 및 자동화된 분석을 제공할 수 있는 컬렉터와 함께 구현할 수 있습니다.분류 ACL은 ACL의 구성 요소이며, 분석 과정에서 특정 트래픽을 식별하고 수동 작업을 수행하기 위해 사전 계획이 필요합니다.이 섹션에서는 각 기능에 대한 간략한 개요를 제공합니다.

NetFlow

NetFlow는 네트워크 흐름을 추적하여 비정상적이고 보안과 관련된 네트워크 활동을 식별합니다.NetFlow 데이터는 CLI를 통해 보고 분석할 수 있습니다. 또는 데이터를 상업용 또는 프리웨어 NetFlow 컬렉터로 내보내어 어그리게이션 및 분석을 수행할 수 있습니다.NetFlow 컬렉터는 장기적인 트렌드를 통해 네트워크 동작 및 사용 분석을 제공할 수 있습니다.NetFlow는 IP 패킷 내의 특정 특성에 대한 분석을 수행하고 흐름을 생성하여 작동합니다.버전 5는 가장 일반적으로 사용되는 NetFlow 버전이지만 버전 9는 더 확장할 수 있습니다.NetFlow 플로우는 고용량 환경에서 샘플링된 트래픽 데이터로 생성할 수 있습니다.

NetFlow를 활성화하려면 CEF(Distributed CEF)가 필수적입니다.NetFlow는 라우터 및 스위치에 구성할 수 있습니다.

이 예에서는 이 기능의 기본 컨피그레이션을 설명합니다.Cisco IOS 소프트웨어의 이전 릴리스에서 인터페이스에서 NetFlow를 활성화하는 명령은 **ip 흐름 {ingress** 대신 **ip route-cache flow입니다. | 이그레스}**.

```
!

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

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

다음은 CLI에서 NetFlow 출력을 보여 주는 예입니다.SrcIf 특성은 traceback에 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*.

*NetFlow*에 대한 기술 개요는 Cisco IOS NetFlow 소개 - 기술 개요를 참조하십시오.

분류 ACL

분류 ACL은 인터페이스를 통과하는 트래픽에 대한 가시성을 제공합니다.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 구분할 수 있습니다.이러한 트래픽을 특정 ACE로 더욱 세분화하여 분류하면 각 트래픽 카테고리에 고유한 히트 카운터가 있으므로 네트워크 트래픽을 이해하는 데 도움이 될 수 있습니다.관리자는 ACL의 끝에서 암시적 거부를 세분화된 ACE로 분리하여 거부된 트래픽의 유형을 식별할 수도 있습니다.

관리자는 **show access-list** 및 **clear ip access-list counters** EXEC 명령으로 분류 ACL을 사용하여 사고를 신속하게 처리할 수 있습니다.

다음 예에서는 기본 거부 이전에 SMB 트래픽을 식별하기 위한 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 명령을 사용합니다 .ACL 카운터는 clear ip access-list counters acl-name EXEC 명령을 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)
```

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

VLAN 맵 및 포트 액세스 제어 목록을 통한 액세스 제어

VACL(VLAN Access Control Lists) 또는 VLAN 맵 및 PACL(Port ACL)은 라우팅된 인터페이스에 적용되는 액세스 제어 목록보다 엔드포인트 디바이스에 가까운 라우팅되지 않은 트래픽에 액세스 제어를 적용하는 기능을 제공합니다.

이 섹션에서는 VACL 및 PACL의 기능, 이점 및 잠재적 사용 시나리오에 대한 개요를 제공합니다.

VLAN 맵을 통한 액세스 제어

VLAN을 입력하는 모든 패킷에 적용되는 VACL 또는 VLAN 맵은 VLAN 내 트래픽에 액세스 제어를 적용하는 기능을 제공합니다.라우팅된 인터페이스의 ACL에서는 이 작업을 수행할 수 없습니다.예를 들어, 동일한 VLAN에 포함된 호스트가 서로 통신하지 못하도록 VLAN 맵을 사용하여 로컬 공격자나 벌레가 동일한 네트워크 세그먼트의 호스트를 공격할 기회를 줄일 수 있습니다.VLAN 맵을 사용하여 패킷을 거부하려면 트래픽과 일치하는 ACL(Access Control List)을 생성하고 VLAN 맵에서 작업을 삭제로 설정할 수 있습니다.VLAN 맵이 구성되면 LAN에 들어오는 모든 패킷이 구성된 VLAN 맵에 대해 순차적으로 평가됩니다.VLAN 액세스 맵은 IPv4 및 MAC 액세스 목록을 지원합니다.그러나 로깅 또는 IPv6 ACL은 지원하지 않습니다.

이 예에서는 이 기능의 컨피그레이션을 보여 주는 확장된 명명된 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 프로토콜뿐만 아니라 TCP 포트 139 및 445를 거부하기 위해 VLAN 맵을 사용하는 방법을 보여 줍니다.

```
!

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 맵 컨피그레이션*에 대한 자세한 내용은 ACL을 사용하여 네트워크 보안 구성을 참조하십시오.

PACL을 통한 액세스 제어

PACL은 스위치의 레이어 2 물리적 인터페이스의 인바운드 방향에만 적용할 수 있습니다.VLAN 맵과 마찬가지로 PACL은 라우팅되지 않은 트래픽 또는 레이어 2 트래픽에 대한 액세스 제어를 제공합니다.VLAN 맵 및 라우터 ACL보다 우선하는 PACL 생성 구문은 라우터 ACL과 동일합니다.ACL이 레이어 2 인터페이스에 적용되는 경우 이를 PACL이라고 합니다.컨피그레이션에는 IPv4, IPv6 또는 MAC ACL을 생성하고 이를 레이어 2 인터페이스에 적용하는 작업이 포함됩니다.

이 예에서는 이 기능의 컨피그레이션을 설명하기 위해 확장된 명명된 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
!
```

*PACL의 컨피그레이션*에 대한 자세한 내용은 ACL을 사용하여 네트워크 보안 구성의 포트 ACL 섹

션을 참조하십시오.

MAC를 통한 액세스 제어

인터페이스 컨피그레이션 모드에서 이 명령을 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 명령은 Cisco IOS Software 릴리스 12.2(18)SXD(Sup 720용) 및 Cisco IOS Software 릴리스 12.2(33)SRA 이상에서 지원됩니다.

이 interface 명령은 인그레스 인터페이스에 적용되어야 하며 전달 엔진에 IP 헤더를 검사하지 않도록 지시합니다.그 결과 IP 환경에서 MAC 액세스 목록을 사용할 수 있습니다.

프라이빗 VLAN 사용

PVLAN(Private VLAN)은 VLAN 내의 워크스테이션 또는 서버 간의 연결을 제한하는 레이어 2 보안 기능입니다.PVLAN이 없으면 레이어 2 VLAN의 모든 디바이스가 자유롭게 통신할 수 있습니다.단일 VLAN에서 디바이스 간의 통신을 제한하여 보안을 지원할 수 있는 네트워킹 상황이 존재합니다.예를 들어, 공개적으로 액세스 가능한 서브넷에서 서버 간의 통신을 금지하기 위해 PVLAN이 자주 사용됩니다.단일 서버가 손상된 경우 PVLAN을 적용했기 때문에 다른 서버와의 연결이 부족하면 한 서버로 보안 침해를 제한할 수 있습니다.

프라이빗 VLAN에는 세 가지 유형이 있습니다.격리된 VLAN, 커뮤니티 VLAN 및 기본 VLANPVLAN의 컨피그레이션은 기본 및 보조 VLAN을 사용합니다.기본 VLAN에는 나중에 설명되는 모든 프로미스큐어스 포트가 포함되며 격리되거나 커뮤니티 VLAN이 될 수 있는 하나 이상의 보조 VLAN이 포함됩니다.

격리된 VLAN

보조 VLAN을 격리 VLAN으로 구성하면 보조 VLAN의 디바이스 간 통신이 완전히 차단됩니다.기본 VLAN당 하나의 격리된 VLAN만 있을 수 있으며, 프로미스큐어스 포트만 격리된 VLAN의 포트와 통신할 수 있습니다.격리된 VLAN은 게스트를 지원하는 네트워크와 같이 신뢰할 수 없는 네트워크에서 사용해야 합니다.

이 컨피그레이션 예에서는 VLAN 11을 격리된 VLAN으로 구성하고 이를 기본 VLAN, VLAN 20에 연결합니다. 아래 예는 인터페이스 FastEthernet 1/1을 VLAN 11에서 격리된 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 VLAN은 기본 VLAN의 프로미스큐어스 포트뿐만 아니라 VLAN의 멤버 간의 통신을 허용합니다.그러나 두 커뮤니티 VLAN 간 또는 커뮤니티 VLAN에서 격리된 VLAN으로의 통신은 불가능합니다.서로 연결해야 하지만 VLAN의 다른 모든 디바이스에 연결할 필요가 없는 서버를 그룹화하려면 커뮤니티 VLAN을 사용해야 합니다.이 시나리오는 공개적으로 액세스 가능한 네트워크 또는 서버가 신뢰할 수 없는 클라이언트에 콘텐츠를 제공하는 모든 곳에서 일반적입니다.

이 예에서는 단일 커뮤니티 VLAN을 구성하고 스위치 포트 FastEthernet 1/2를 해당 VLAN의 멤버로 구성합니다.커뮤니티 VLAN 12는 기본 VLAN 20에 대한 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 배치된 스위치 포트를 프로미스큐어스 포트라고 합니다.프로미스큐어스 포트는 기본 및 보조 VLAN의 다른 모든 포트와 통신할 수 있습니다.라우터 또는 방화벽 인터페이스는 이러한 VLAN에서 가장 일반적인 디바이스입니다.

이 컨피그레이션 예에서는 이전의 격리 및 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 컨피그레이션이 PVLAN에 의해 적용되는 제한을 지원하고 PVLAN 컨피그레이션이 대체되지 않도록 하는 것이 중요합니다.라우터 ACL 또는 방화벽을 사용한 레이어 3 필터링은 PVLAN 컨피그레이션의 하위 버전을 방지할 수 있습니다.

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

결론

이 문서에서는 Cisco IOS 시스템 디바이스를 보호하기 위해 사용할 수 있는 방법에 대해 간략하게 설명합니다.디바이스를 보호하면 관리하는 네트워크의 전반적인 보안이 향상됩니다.이 개요에서는 관리, 제어 및 데이터 플레인의 보호에 대해 설명하고 구성에 대한 권장 사항을 제공합니다.가능한 경우 각 관련 기능의 컨피그레이션에 대해 충분한 세부사항이 제공됩니다.그러나 모든 경우 추가 평가에 필요한 정보를 제공하기 위해 포괄적인 참조가 제공됩니다.

감사의 말

이 문서의 일부 기능 설명은 Cisco 정보 개발 팀에서 작성했습니다.

부록:Cisco IOS 장치 강화 체크리스트

이 체크리스트는 이 가이드에 나와 있는 모든 강화 단계의 모음입니다.관리자는 Cisco IOS 디바이스에 사용되고 고려되는 모든 강화 기능을 미리 알림으로 사용할 수 있습니다. 단, 기능이 적용되지 않아 구현되지 않은 경우에도 마찬가지입니다.관리자는 옵션을 구현하기 전에 각 옵션의 잠재적 위험을 평가하는 것이 좋습니다.

관리 플레인

- 비밀번호

  활성화 및 로컬 사용자 비밀번호를 위해 MD5 해싱(비밀 옵션)을 활성화합니다.비밀번호 재시도 잠금 구성비밀번호 복구 비활성화(위험 고려)

- 사용하지 않는 서비스 사용 안 함
- 관리 세션에 대한 TCP keepalive 구성
- 메모리 및 CPU 임계값 알림 설정
- 구성

  메모리 및 CPU 임계값 알림콘솔 액세스를 위한 메모리 예약메모리 누수 탐지기버퍼 오버플로 감지향상된 crashinfo 컬렉션
- iACL을 사용하여 관리 액세스 제한
- 필터(위험 고려)

  ICMP 패킷IP 조각IP 옵션패킷의 TTL 값
- 컨트롤 플레인 보호

  포트 필터링 구성대기열 임계값 구성
- 관리 액세스

  관리 평면 보호를 사용하여 관리 인터페이스 제한exec 시간 초과 설정CLI 액세스에 암호화된 전송 프로토콜(예: SSH) 사용vty 및 tty 라인의 전송 제어(액세스 클래스 옵션)배너를 사용하여 경고
- AAA

  인증 및 폴백에 AAA 사용명령 권한 부여에 AAA(TACACS+) 사용어카운팅에 AAA 사용중복 AAA 서버 사용
- SNMP

  SNMPv2 커뮤니티 구성 및 ACL 적용SNMPv3 구성
- 로깅

  중앙 집중식 로깅 구성모든 관련 구성 요소에 대한 로깅 수준 설정로깅 소스 인터페이스 설정로깅 타임스탬프 세분화 구성
- 구성 관리

  교체 및 롤백단독 구성 변경 액세스소프트웨어 복원력 구성구성 변경 알림

컨트롤 플레인

- 비활성화(위험 고려)

  ICMP 리디렉션ICMP 연결 불가프록시 ARP

- NTP를 사용 중인 경우 NTP 인증 구성
- 컨트롤 플레인 정책/보호 구성(포트 필터링, 대기열 임계값)
- 보안 라우팅 프로토콜

  BGP(TTL, MD5, 최대 접두사, 접두사 목록, 시스템 경로 ACL)IGP(MD5, 패시브 인터페이스, 경로 필터링, 리소스 소비)

- 하드웨어 속도 리미터 구성
- 보안 First Hop Redundancy Protocols(GLBP, HSRP, VRRP)

데이터 플레인

- IP 옵션 선택적 삭제 구성
- 비활성화(위험 고려)

  IP 소스 라우팅IP 직접 브로드캐스트ICMP 리디렉션

- IP 직접 브로드캐스트 제한
- tACL 구성(위험 고려)

  ICMP 필터링IP 조각 필터링필터 IP 옵션TTL 값 필터링

- 필요한 스푸핑 방지 보호 구성

  ACLIP 소스 가드동적 ARP 검사유니캐스트 RPF포트 보안

- 컨트롤 플레인 보호(컨트롤 플레인 cef-exception)
- 트래픽 식별을 위한 NetFlow 및 분류 ACL 구성
- 필요한 액세스 제어 ACL 구성(VLAN 맵, PACL, MAC)
- 프라이빗 VLAN 구성