# Simple Network Management Protocol 보안

## 목차



## 소개

이 문서에서는 SNMP(Simple Network Management Protocol)를 보호하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SNMP 보기 - Cisco IOS® 소프트웨어 릴리스 10.3 이상
- SNMP 버전 3 — Cisco IOS Software 릴리스 12.0(3)T에 도입되었습니다.

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

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

# 배경 정보

특히 DoS(Denial of Service)를 생성하기 위해 SNMP의 취약성을 반복적으로 악용할 수 있는 경우 SNMP를 보호하는 것이 중요합니다.

# SNMP 보안 전략

## 양호한 SNMP 커뮤니티 문자열 선택

### public을 읽기 전용, private을 읽기-쓰기 커뮤니티 문자열로 사용하는 것은 좋은 방법이 아닙니다.

## Setup SNMP view

이 Setup SNMP view 명령은 제한된 MIB(Management Information Base)에 대한 액세스만 있는 사용자를 차단할 수 있습니다. 기본적으로 는 SNMP view entry exists . 이 명령은 전역 컨피그레이션 모드에서 구성되며 Cisco IOS Software 버전 10.3에 처음 도입되었습니다. 다음과 유사한 방식으로 작동합니다 access-list ISE에 대해 SNMP View 특정 MIB 트리에서는 다른 모든 트리가 이해할 수 없을 정도로 거부됩니다. 하지만 시퀀스는 중요하지 않으며 정지되기 전에 전체 목록을 확인합니다.

뷰 항목을 생성하거나 업데이트하려면 snmp-server view global configuration 명령을 실행합니다. 지정된 SNMP 서버 보기 항목을 제거하려면 no 이 명령의 형식입니다.

### 구문:

```
snmp-server view view-name oid-tree {included | excluded}

no snmp-server view view-name
```

### 구문 설명:

- view-name- 업데이트하거나 생성하는 뷰 레코드의 레이블입니다. 이름은 레코드를 참조하는 데 사용됩니다.
- oid-tree - 뷰에 포함되거나 제외할 ASN.1(Abstract Syntax Notation One) 하위 트리의 객체 식별자입니다. 하위 트리를 식별하려면 1.3.6.2.4와 같은 숫자 또는 다음과 같은 단어로 구성된 텍스트 문자열을 지정합니다 system. 하위 트리 패밀리를 지정하려면 단일 하위 식별자를 별표(*) 와일드카드로 바꿉니다(예: 1.3.*.4).
- included | excluded- 뷰의 유형입니다. included 또는 excluded를 지정해야 합니다.

정의해야 하는 뷰 대신 뷰가 필요한 경우 두 개의 표준 사전 정의 뷰를 사용할 수 있습니다. 하나는 everything으로, 사용자가 모든 개체를 볼 수 있음을 나타냅니다. 다른 하나는 restricted로, 사용자가 system, snmpStats 및 snmpParties. 사전 정의된 보기는 RFC 1447에 설명되어 있습니다.

**참고**: snmp-server 입력하는 명령은 두 버전의 SNMP를 모두 활성화합니다.

다음 예에서는 MIB-II 시스템 그룹의 모든 객체를 포함하는 뷰를 생성합니다. sysServices (시스템 7) 및 MIB-II 인터페이스 그룹의 인터페이스 1에 대한 모든 개체:

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

snmp-server view agon ifEntry.*.1 included
```

커뮤니티 문자열 및 의 출력을 사용하여 MIB를 적용하는 방법에 대한 완전한 예입니다. snmpwalk 사용 view 있습니다. 이 컨피그레이션에서는 ARP(Address Resolution Protocol) 테이블( atEntry )에서 MIB-II 및 Cisco 사설 MIB를 허용합니다.

```
snmp-server view myview mib-2 included


snmp-server view myview atEntry excluded


snmp-server view myview cisco included


snmp-server community public view myview RO 11


snmp-server community private view myview RW 11


snmp-server contact pvanderv@cisco.com
```

다음은 MIB-II 시스템 그룹에 대한 명령 및 출력입니다.

```
NMSPrompt 82 % snmpwalk cough system
system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software
Cisco IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(1)T,RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Wed 04-Nov-98 20:37 by dschwart
system.sysObjectID.0 : OBJECT IDENTIFIER:
   .iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco2520
system.sysUpTime.0 : Timeticks: (306588588) 35 days, 11:38:05.88
system.sysContact.0 : DISPLAY STRING- (ASCII):pvanderv@cisco.com
system.sysName.0 : DISPLAY STRING- (ASCII):cough
system.sysLocation.0 : DISPLAY STRING- (ASCII):
system.sysServices.0 : INTEGER: 78
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00

NMSPrompt 83 %
```

다음은 로컬 Cisco System 그룹에 대한 명령 및 출력입니다.

```
NMSPrompt 83 % snmpwalk cough lsystem

cisco.local.lsystem.romId.0 : DISPLAY STRING- (ASCII):
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems

cisco.local.lsystem.whyReload.0 : DISPLAY STRING- (ASCII):power-on
```

```
cisco.local.lsystem.hostName.0 : DISPLAY STRING- (ASCII):cough
```

다음은 MIB-II ARP 테이블에 대한 명령 및 출력입니다.

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

## access-list 포함 SNMP 커뮤니티 설정

현재 모범 사례에서는 ACL(Access Control List)을 커뮤니티 문자열에 적용하고 요청 커뮤니티 문자열이 알림 커뮤니티 문자열과 동일하지 않은지 확인하는 것이 좋습니다. 액세스 목록은 다른 보호 조치와 함께 사용할 경우 추가 보호를 제공합니다.

이 예시에서는 ACL을 커뮤니티 문자열로 설정합니다.

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

요청 및 트랩 메시지에 다른 커뮤니티 문자열을 사용할 경우, 커뮤니티 문자열이 공격자에 의해 발견될 경우 추가 공격이나 보안 침해가 발생할 가능성이 줄어듭니다. 그렇지 않으면 공격자가 권한 부여 없이 원격 디바이스를 손상시키거나 네트워크에서 트랩 메시지를 스니핑할 수 있습니다.

커뮤니티 문자열로 트랩을 활성화하면 일부 Cisco IOS 소프트웨어에서 SNMP 액세스를 위해 문자열을 활성화할 수 있습니다. 이 커뮤니티를 명시적으로 비활성화해야 합니다. 예를 들면 다음과 같습니다.

```
access-list 10 deny any
snmp-server host 10.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

## SNMP 버전 3 설정

SNMP 버전 3은 Cisco IOS 소프트웨어 버전 12.0에서 처음 도입되었지만 아직 네트워크 관리에서 일반적으로 사용되지는 않습니다. SNMP 버전 3을 구성하려면 다음 단계를 수행합니다.

1. SNMP 엔터티에 대한 엔진 ID를 할당합니다(선택 사항).
2. 사용자, 그룹 **그룹**에 속한 사용자**를** 정의하고 **noAuthentication**(비밀번호 없음) 및 **noPrivacy**(암호화 없음)를 이 사용자에게 적용합니다.
3. 그룹 2에 속한 사용자 **usertwo 를** 정의하고 이 사용자에게 **noAuthentication**(비밀번호 없음) 및 **noPrivacy**(암호화 없음)를 적용합니다.
4. 그룹 3에 속하는 사용자 **userthree를** 정의하고 **Authentication**(password는 user3passwd) 및 noPrivacy(no encryption)를 이 사용자에게 적용합니다.
5. 그룹 4에 속하는 **사용자 userfour**를 정의하고 **이 사용자**에게 **인증**(비밀번호는 user4passwd)

및 **개인 정보**(des56 암호화)를 적용합니다.

6. USM(User Security Model) V3을 통해 그룹인 그룹을 정의하고 **v1default** 뷰(기본값)에서 읽기 액세스를 활성화합니다.
7. USM V3을 통해 그룹 **grouptwo**를 정의하고 view myview에서 읽기 액세스를 **활성화합니다**.
8. USM V3을 통해 그룹 **3을** 정의하고, 인증을 통해 **v1default** 보기(기본값)에서 읽기 액세스를 **활성화합니다**.
9. USM V3을 사용하여 그룹 **groupfour**를 정의하고 **Authentication** 및 Privacy를 사용하여 **v1default** 보기(기본값)에서 읽기 액세스를 **활성화합니다**.
10. MIB-II에 대한 읽기 액세스 권한을 제공하고 프라이빗 Cisco MIB에 대한 읽기 액세스 권한을 거부하는 보기 myview를 정의합니다.이 **show running** 정의된 커뮤니티 문자열 Read-Only **public**이 있으므로 출력에서 그룹 public에 대해 추가 **행**을 제공합니다.이 **show running** 출력에 userthree가 **표시되지 않습니다**.

**예:**

```
snmp-server engineID local 1111000000000000000000000
snmp-server user userone groupone v3
snmp-server user usertwo grouptwo v3
snmp-server user userthree groupthree v3 auth md5 user3passwd
snmp-server user userfour groupfour v3 auth md5 user4passwd priv des56
  user4priv
snmp-server group groupone v3 noauth
snmp-server group grouptwo v3 noauth read myview
snmp-server group groupthree v3 auth
snmp-server group groupfour v3 priv
snmp-server view myview mib-2 included
snmp-server view myview cisco excluded
snmp-server community public RO
```

사용자 userone이 있는 MIB-II 시스템 그룹에 대한 명령 및 **출력입니다**.

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system
Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco IOS (TM) 4500 Software (C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 23-Feb-99 03:59 by ccai
system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28208096) 3 days, 6:21:20.96
system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com
system.sysLocation.0 =
system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
NMSPrompt 95 %
```

사용자 usertwo가 있는 MIB-II 시스템 그룹에 대한 명령 및 **출력입니다**.

```
NMSPrompt 95 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system

Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco IOS (TM) 4500 Software (C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 23-Feb-99 03:59 by ccai
system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28214761) 3 days, 6:22:27.61
system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com
system.sysLocation.0 =
system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

사용자 userone이 있는 Cisco Local System 그룹에 대한 명령 및 **출력입니다**.

```
NMSPrompt 98 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1

Module SNMPV2-TC not found
enterprises.9.2.1.1.0 = "..System Bootstrap, Version 5.2(7b) [mkamson 7b],
   RELEASE SOFTWARE (fc1)..Copyright (c) 1995 by cisco Systems,
Inc..."
enterprises.9.2.1.2.0 = "reload"
enterprises.9.2.1.3.0 = "clumsy"
enterprises.9.2.1.4.0 = "cisco.com"
```

사용자 usertwo가 있는 Cisco Local System 그룹을 가져올 수 없음을 보여주는 명령 및 **출력입니다** .

```
NMSPrompt 99 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1

Module SNMPV2-TC not found
enterprises.9.2.1 = No more variables left in this MIB View

NMSPrompt 100 %
```

이 명령 및 출력 결과는 사용자 지정된 tcpdump (SNMP 버전 3 지원 및 printf 부록용 패치):

```
NMSPrompt 102 % snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0

Module SNMPV2-TC not found
system.sysName.0 = clumsy.cisco.com
```

## 인터페이스에 ACL 설정

ACL 기능은 IP 스푸핑과 같은 공격을 방지하는 보안 조치를 제공합니다. ACL은 라우터의 수신 또는 발신 인터페이스에 적용할 수 있습니다.

수신 ACL(rACL)을 사용하는 옵션이 없는 플랫폼에서는 인터페이스 ACL을 사용하여 신뢰할 수 있는 IP 주소에서 라우터로 UDP(User Datagram Protocol) 트래픽을 허용할 수 있습니다.

다음 확장 액세스 목록은 네트워크에 맞게 조정할 수 있습니다. 이 예시에서는 라우터의 인터페이스에 IP 주소 192.168.10.1 및 172.16.1.1이 설정되어 있고 모든 SNMP 액세스는 IP 주소가 10.1.1.1인 관리 스테이션으로만 제한되며 관리 스테이션은 IP 주소 192.168.10.1과의 통신만 필요하다고 가정합니다.

```
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1
```

이 access-list 그런 다음 다음 다음 컨피그레이션 명령을 사용하여 모든 인터페이스에 적용해야 합니다.

```
interface ethernet 0/0

ip access-group 101 in
```

UDP 포트의 라우터와 직접 통신하는 모든 디바이스는 이전 액세스 목록에 구체적으로 나열되어야 합니다. Cisco IOS 소프트웨어는 DNS(Domain Name System) 쿼리와 같은 아웃바운드 세션의 소스 포트로 49152~65535 범위의 포트를 사용합니다.

구성된 IP 주소가 많은 디바이스 또는 라우터와 통신해야 하는 호스트가 많은 경우 이 솔루션이 항상 확장 가능한 솔루션은 아닙니다.

### rACL

분산형 플랫폼의 경우 Cisco 12000 Series GSR(Gigabit Switch Router)의 경우 Cisco IOS Software Release 12.0(21)S2, Cisco 7500 Series의 경우 Release 12.0(24)S에서 시작하는 옵션이 rACL이 될 수 있습니다. 수신 액세스 목록은 트래픽이 RP(Route Processor)에 영향을 미치기 전에 유해한 트래픽으로부터 디바이스를 보호합니다. 수신 경로 ACL도 네트워크 보안 모범 사례로 간주되므로 우수한 네트워크 보안에 장기적인 추가 요소로 간주하고 이러한 특정 취약성을 해결할 수 있어야 합니다. CPU 로드는 라인 카드 프로세서로 배포되며, 기본 경로 프로세서의 로드를 완화하는 데 도움이 됩니다. 백서 GSR: Receive Access Control Lists는 합법적인 트래픽을 식별하는 데 도움이 됩니다. 이 백서를 사용하여 합법적인 트래픽을 디바이스로 전송하는 방법을 이해하고 원하지 않는 모든 패킷을 거부합니다.

### 인프라 ACL

네트워크를 통과하는 트래픽을 차단하기는 어렵지만 인프라 디바이스를 대상으로 해서는 안 되는 트래픽을 식별하고 네트워크 경계에서 해당 트래픽을 차단할 수 있습니다. iACL(Infrastructure ACL)은 네트워크 보안 모범 사례로 간주되며, 이러한 특정 취약성에 대한 해결 방법은 물론 우수한 네트워크 보안에 장기간 추가하는 것으로 간주해야 합니다. Protecting Your Core: Infrastructure Protection Access Control List 백서는 iACL에 대한 지침과 권장 구축 기술을 소개합니다.

### Cisco Catalyst LAN 스위치 보안 기능

IP 허용 목록 기능은 권한이 없는 소스 IP 주소에서 스위치에 대한 인바운드 Telnet 및 SNMP 액세스를 제한합니다. 시스템 로그 메시지와 SNMP 트랩은 위반 또는 무단 액세스가 발생할 때 관리 시스템에 알리기 위해 지원됩니다.

Cisco IOS 소프트웨어 보안 기능의 조합을 사용하여 라우터와 Cisco Catalyst 스위치를 관리할 수 있습니다. 스위치와 라우터에 액세스할 수 있는 관리 스테이션의 수를 제한하는 보안 정책을 설정해야 합니다.

IP 네트워크에서 보안을 강화하는 방법에 대한 자세한 내용은 IP 네트워크에서 보안 향상을 참조하십시오.

## SNMP 오류 확인 방법

SNMP 커뮤니티 ACL을 log 키워드로 패킷 암호화를 허용하기 때문입니다. 모니터링 syslog 시도에 실패한 경우(아래 표시).

```
access-list 10 deny any log
snmp-server community public RO 10
```

누군가가 커뮤니티 퍼블릭을 사용하여 라우터에 액세스하려고 하면 syslog 이와 비슷합니다.

```
%SEC-6-IPACCESSLOGS: list 10 denied 172.16.1.15packet
```

이 출력은 access-list 10에서 호스트 172.16.1.1의 SNMP 패킷 5개를 거부했음을 의미합니다.

SNMP에서 주기적으로 show snmp 명령, 여기에 표시된 대로

```
router#show snmp Chassis: 21350479 17005 SNMP packets input

37 Bad SNMP version errors**
15420 Unknown community name**
0 Illegal operation for community name supplied
1548 Encoding errors**
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs 0 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
0 Trap PDUs
```

** 표시된 카운터에서 이러한 취약성에 대한 익스플로잇 시도를 나타낼 수 있는 오류율이 예기치 않게 증가하는지 확인합니다. 보안 문제를 보고하려면 Cisco 제품 보안 사고 대응을 참조하십시오.

# 관련 정보

- Cisco 보안 권고 SNMP 취약점
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.