# Simple Network Management Protocolの保護

## 内容



## 概要

このドキュメントでは、Simple Network Management Protocol（SNMP；簡易ネットワーク管理プロトコル）を保護する方法について説明します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- SNMPビュー：Cisco IOS®ソフトウェアリリース10.3以降。
- SNMP バージョン 3：Cisco IOS ソフトウェア リリース 12.0(3)T で導入されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

# 背景説明

特に、SNMPの脆弱性が繰り返し悪用されてサービス拒否(DoS)が発生する可能性がある場合は、SNMPを保護することが重要です。

# SNMPを保護するための戦略

## 有効なSNMPコミュニティストリングを選択する

public を読み取り専用コミュニティ ストリングとして使用し、private を読み取りと書き込みコミュニティ ストリングとして使用するのは、有効な方法ではありません。

## SNMP ビューのセットアップ

「 Setup SNMP view コマンドは、制限付きの管理情報ベース(MIB)へのアクセスだけを持つユーザをブロックできます。デフォルトでは、 SNMP view entry exists .このコマンドはグローバル コンフィギュレーション モードで設定され、Cisco IOS ソフトウェア バージョン 10.3 で初めて導入されました。これは次のように動作します access-list もし何か SNMP View 特定のMIBツリーでは、他のすべてのツリーが不可解に拒否されます。しかしシーケンスは重要でなく、リスト全体が検索され一致があったところで停止します。

ビューエントリを作成または更新するには、 snmp-server view global configuration コマンドが表示されない場合もあります。指定したSNMPサーバビューのエントリを削除するには、 no このコマンドの形式。

**構文：**

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

no snmp-server view view-name
```

**構文の説明：**

- view-name – 更新または作成するビューレコードのラベル。この名前は、レコードを参照するために使用します。
- oid-tree – ビューに含める、またはビューから除外する抽象構文記法1 (ASN.1)サブツリーのオブジェクト識別子。サブツリーを識別するには、1.3.6.2.4などの数字または次のような単語で構成されるテキスト文字列を指定します system. サブツリーファミリを指定するには、1つのサブ識別子をアスタリスク(*)のワイルドカードに置き換えます（ 例：1.3.*.4 ）。
- included | excluded – ビューのタイプ。included または excluded のいずかを指定します。

ビューが必要な場合は、定義する必要があるビューの代わりに、2つの標準の定義済みビューを使用できます。1 つは everything であり、ユーザはすべてのオブジェクトを表示できます。もう1つは*restricted*です。これは、ユーザが次の3つのグループを表示できることを示します。 system、snmpStats,と snmpParties.事前定義されたビューは、RFC 1447 で説明されています。

**注**：最初の snmp-server コマンドを入力すると、両方のバージョンのSNMPが有効になります。

この例では、MIB-IIシステムグループ内のすべてのオブジェクトを含むビューを作成します。ただし、 sysServices (System 7)およびMIB-IIインターフェイスグループのインターフェイス1のすべてのオブジェクト：

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

次に、コミュニティストリングを使用してMIBを適用する方法の完全な例と、 snmpwalk さらにトラブルシューティングを行うために、 view 適切な場所に。この設定では、アドレス解決プロトコル(ARP)テーブルのSNMPアクセスを拒否するビューを定義します( atEntry MIB-IIおよびCiscoプライベートMIBに対応しています。

```
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
```

次に MIB-II System グループのコマンドと出力を示します。

```
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 %
```

次にローカルの Cisco System グループのコマンドと出力を示します。

```
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
```

次に MIB-II ARP テーブルのコマンドと出力を示します。

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

## アクセスリストで SNMP コミュニティをセットアップする

現在のベストプラクティスでは、アクセスコントロールリスト(ACL)をコミュニティストリングに適用し、要求コミュニティストリングが通知コミュニティストリングと同一にならないようにすることをお勧めします。アクセス リストを他の保護措置と組み合わせて使用すれば、保護機能が高められます。

次に ACL をコミュニティ ストリングに設定する例を示します。

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

要求とトラップメッセージに異なるコミュニティストリングを使用すると、攻撃者によってコミュニティストリングが発見された場合に、さらなる攻撃や侵害の可能性が低くなります。そうしないと、攻撃者はリモートデバイスを侵害したり、ネットワークからトラップメッセージを傍受したりして、認証を受けることができない可能性があります。

コミュニティストリングを使用してトラップを有効にすると、一部のCisco IOSソフトウェアではSNMPアクセス用にストリングを有効にできます。このコミュニティは明示的にディセーブルする必要があります。 以下に、いくつかの例を示します。

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

## SNMP バージョン3のセットアップ

SNMPバージョン 3 は Cisco IOS ソフトウェア バージョン 12.0 で初めて導入されましたが、ネ

ットワーク管理ではまだ一般的に使用されていません。SNMPバージョン3を設定するには、次の手順を実行します。

1. SNMP エンティティのエンジン ID を割り当てます（オプション）。
2. グループgroupone に属するユーザuserone を定義し、このユーザにnoAuthentication（パスワードなし）およびnoPrivacy（暗号化なし）を適用します。
3. グループgrouptwo に属するユーザusertwo  ;を定義し、このユーザにnoAuthentication（パスワードなし）およびnoPrivacy（暗号化なし）を適用します。
4. グループgroupthree に属するユーザuserthree を定義し、このユーザにAuthentication（パスワードはuser3passwd）とnoPrivacy（暗号化なし）を適用します。
5. グループgroupfour に属するユーザuserfour を定義し、このユーザにAuthentication（パスワードはuser4passwd）とPrivacy（des56暗号化）を適用します。
6. ユーザセキュリティモデル(USM)V3を使用してグループgrouponeを定義し、v1defaultビュー（デフォルト）で読み取りアクセスを有効にします。
7. USM V3を使用してグループgrouptwo を定義し、myview ビューでの読み取りアクセスを有効にします。
8. USM V3を使用してグループgroupthreeを定義し、認証を使用してv1defaultビュー（デフォルト）での読み取りアクセスを有効にします。
9. USM V3を使用してグループgroupfourを定義し、認証およびプライバシーを使用してv1defaultビュー（デフォルト）での読み取りアクセスを有効にします。
10. MIB-II での読み取りアクセスを提供し、プライベートな Cisco MIB での読み取りアクセスを拒否する myview ビューを定義します。「show running コミュニティストリングRead-Only publicが定義されているため、出力にはグループpublicに対する行が追加されます。「show running 出力にuserthreeが表示されません。

例：

```
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
```

次に、userone ユーザのMIB-II Systemグループに対するコマンドと出力を示します。

```
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 %
```

ユーザusertwoのMIB-II Systemグループに対するコマンドと出力を次に示します。**usertwo**:

```
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
```

次に、ユーザ**userone**のCisco Local Systemグループに対するコマンドと出力を示します。

```
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"
```

次のコマンドと出力は、ユーザ**usertwo**でCisco Local Systemグループを取得できないことを示しています。

```
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 %
```

このコマンドと出力結果は、カスタマイズされた **tcpdump**（SNMPバージョン3のサポートとprintfの追補のためのパッチ）:

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

Module SNMPV2-TC not found
```

```
system.sysName.0 = clumsy.cisco.com
```

## インターフェイスでの ACL 設定

ACL機能は、IPスプーフィングなどの攻撃を防ぐセキュリティ対策を提供します。ACL はルータの着信インターフェイスまたは発信インターフェイスに適用できます。

受信 ACL（rACL）を使用するオプションのないプラットフォームでは、インターフェイス ACL を使用して、信頼できる IP アドレスからルータへの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックを許可することができます。

次の拡張アクセスリストをネットワークに適用できます。次の例での前提事項は、ルータのインターフェイスに IP アドレス 192.168.10.1 および 172.16.1.1 が設定されていること、すべての SNMP アクセスが IP アドレス 10.1.1.1 の管理ステーションに限定されていること、およびその管理ステーションが IP アドレス192.168.10.1とだけ通信する必要があることです。

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

「 access-list その後、次の設定コマンドを使用して、すべてのインターフェイスに適用する必要があります。

```
interface ethernet 0/0

ip access-group 101 in
```

UDPポートでルータと直接通信するすべてのデバイスは、前のアクセスリストに具体的にリストされている必要があります。Cisco IOS ソフトウェアは、49152 から 65535 までの範囲のポートを Domain Name System（DNS; ドメイン ネーム システム）クエリーなどのアウトバウンド セッションのソース ポートに使用します。

多数のIPアドレスが設定されているデバイスや、ルータと通信する必要がある多数のホストの場合、これは常にスケーラブルなソリューションとは限りません。

## 受信 ACL（rACL）

分散プラットフォームでは、Cisco 12000シリーズギガビットスイッチルータ(GSR)のCisco IOSソフトウェアリリース12.0(21)S2およびCisco 7500シリーズのリリース12.0(24)Sで開始されるオプションとして、rACLを使用できます。受信アクセス リストは、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。受信パス ACLもネットワークセキュリティのベストプラクティスと考えられており、この特定の脆弱性に対する回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。CPU 負荷がライン カード プロセッサに分散されるため、メイン ルート プロセッサの負荷を軽減させるのに役立ちます。ホワイトペーパーの『GSR: Receive Access Control Lists』は、正当なトラフィックの識別に役立ちます。このホワイトペーパーを使用して、正当なトラフィックをデバイスに送信し、不要なパケットをすべて拒否する方法を理解してください。

## インフラストラクチャ ACL

ネットワークを通過するトラフィックをブロックするのは困難な場合が多いですが、インフラストラクチャデバイスに対して絶対に許可してはならないトラフィックを特定し、ネットワークの

境界でそのトラフィックをブロックすることは可能です。インフラストラクチャACL(iACL)は、ネットワークセキュリティのベストプラクティスと考えられており、ここでの特定の脆弱性に対する回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能としても考慮する必要があります。ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』には、iACLのガイドラインと推奨される導入方法が記載されています。

### Cisco Catalyst LAN スイッチのセキュリティ機能

IP 許可リスト機能は、権限のない送信元 IP アドレスからスイッチへの着信 Telnet アクセスおよび SNMP アクセスを制限します。違反または不正アクセスが発生したときに管理システムに通知するため、syslog メッセージと SNMP トラップがサポートされています。

ルータと Cisco Catalyst スイッチの管理には、Cisco IOS ソフトウェアのセキュリティ機能を組み合わせて使用できます。スイッチとルータにアクセスできる管理ステーションの数を制限するセキュリティポリシーを確立する必要があります。

IP ネットワークのセキュリティを強化する方法の詳細については、『IP ネットワークでのセキュリティ強化』を参照してください。

## SNMP エラーをチェックする方法

SNMPコミュニティACLを設定するには、 log キーワード.モニタ syslog 失敗した場合に使用します。

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

誰かがコミュニティpublicを使用してルータにアクセスしようとすると、 syslog 次に似ています。

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

この出力は、アクセス リスト 10 がホスト 172.16.1.1 からの SNMP パケットを 5 つ拒否したことを意味します。

SNMPのエラーを定期的にチェックし、 show snmp コマンドを発行します。

```
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
```

これらの脆弱性の不正利用の試みを示す可能性がある工ラー率の予期しない増加について、**とマークされたカウンタを監視します。セキュリティ問題を報告するには、『シスコのセキュリティ問題対応製品』を参照してください。

# 関連情報

- Cisco セキュリティ アドバイザリ SNMP の脆弱性
- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。