保护您的简单网络管理协议

目录

简介

本文档介绍如何保护您的简单网络管理协议(SNMP)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SNMP视图 — Cisco IOS®软件版本10.3或更高版本。
- SNMP版本3 - Cisco IOS软件版本12.0(3)T中引入。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

背景信息

保护您的SNMP非常重要，尤其是当SNMP的漏洞可能被反复利用来产生拒绝服务(DoS)时。

保护SNMP的策略

选择好的 SNMP 社区字符串

将public用作只读，将**private**用作读**写**社区字符串并不**是**一种好的做法。

设置 SNMP 视图

此 Setup SNMP view 命令可以阻止仅有权访问有限管理信息库(MIB)的用户。默认情况下，没有 SNMP view entry exists .此命令在全局配置模式下配置，并首先在Cisco IOS软件版本10.3中引入。它的工作方式类似于 **access-list** 如果你有任何 SNMP View 在某些MIB树上，其他所有树都会被莫名其妙地拒绝。但是，顺序并不重要，它会在停止之前浏览整个列表以查找匹配项。

要创建或更新视图条目，请在执行模式下使用 **snmp-server view global configuration** 命令。要删除指定的SNMP服务器视图条目，请在执行模式下使用 **no** 此命令形式。

语法:

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

no snmp-server view view-name
```

语法说明:

- view-name — 为更新或创建的视图记录添加标签。名称用于引用记录。
- oid-tree — 要从视图包含或排除的抽象语法标记一(ASN.1)子树的对象标识符。要标识子树，请指定包含数字（如1.3.6.2.4）或单词（如）的文本字符串 system. 用星号(*)通配符替换单个子标识符以指定子树系列；例如1.3.*.4。
- included | excluded — 视图类型。必须指定included或excluded。

当需要视图而不是必须定义的视图时，可以使用两个标准的预定义视图。一个是全部，表示用户可以看到所有对象。另一个是*restricted*，表示用户可以看到三个组： system, snmpStats,和 snmpParties.RFC 1447中介绍了预定义视图。

注：第一个 snmp-server 输入的命令启用两个版本的SNMP。

此示例将创建一个视图，其中包含MIB-II系统组中除以下对象以外的所有对象 **sysServices**（系统7）和MIB-II接口组中接口1的所有对象：

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

这是一个完整的示例，说明如何将MIB与社区字符串和 snmpwalk 与 view 就位。此配置定义一个视图，用于拒绝对地址解析协议(ARP)表的SNMP访问(atEntry)，并允许MIB-II和思科专用MIB:

```
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
```

以下是MIB-II系统组的命令和输出：

```
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 %
```

以下是本地Cisco系统组的命令和输出：

```
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
```

以下是MIB-II ARP表的命令和输出：

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

使用 access-list 设置 SNMP团体

当前的最佳实践建议您对社区字符串应用访问控制列表(ACL)，并确保请求社区字符串与通知社区字符串不同。访问列表在与其他保护措施结合使用时可提供进一步保护。

此示例将ACL设置为社区字符串：

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

当您将不同的社区字符串用于请求和陷阱消息时，如果社区字符串被攻击者发现，就会降低进一步攻击或危害的可能性。否则，攻击者可能会未经授权而入侵远程设备或从网络中嗅探陷阱消息。

使用社区字符串启用陷阱后，可以在某些Cisco IOS软件中为SNMP访问启用该字符串。您必须明确禁用此社区。 例如：

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

设置 SNMP 版本3

SNMP第3版最初是在Cisco IOS软件版本12.0中引入的，但是尚未用于网络管理。执行以下步骤配置SNMP第3版：

1. 为SNMP实体分配引擎ID（可选）。
2. 定义属于组groupone的用户、用户，并向此用户应用noAuthentication(no password)和noPrivacy(no encryption)。
3. 定义属于组组2的用户usertwo ，并向此用户应用noAuthentication(no password)和noPrivacy(no encryption)。
4. 定义属于组组3的用户userthree并应用Authentication(password is user3passwd)和noPrivacy（无加密）到此用户。
5. 定义属于组groupfour的用户userfour，并将Authentication(password is user4passwd)和Privacy（des56加密）应用于此用户。
6. 通过用户安全模型(USM)V3定义组，并启用对v1默认视图（默认）的读取访问权限。
7. 通过USM V3定义一个组，组2，并启用对myview视图的读取访问。
8. 通过USM V3定义一个组，组3，并通过身份验证启用v1默认视图（默认）上的读取访问。
9. 通过USM V3定义组 group，并通过Authentication和Privacy对v1默认视图（默认）启用读取访问。
10. 定义一个视图 myview，用于提供MIB-II的读取访问并拒绝对专用Cisco MIB的读取访问。此 show running 由于已定义社区字符串Read-Only public，因此输出为组public提供其他行。此

show running 输出不显示userthree。

示例：

```
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
```

以下是包含用户userone的MIB-II系统组的命令和**输出**:

```
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 %
```

以下是包含用户usertwo的MIB-II系统组的命令和**输出**:

```
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
```

以下是带有用户userone的Cisco本地系统组的命令和**输出**:

```
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"
```

以下命令和输出显示您无法使用用户usertwo获取Cisco本地系统组:

```
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 %
```

此命令和输出结果适用于自定义 tcpdump （针对SNMP版本3支持和printf附录的补丁）：

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

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

在接口上设置ACL

ACL功能提供安全措施，防止诸如IP欺骗等攻击。ACL 可以应用到路由器的传入或传出接口。

在没有选择使用接收ACL(rACL)的平台上，可以允许从具有接口ACL的受信任IP地址到路由器的用户数据报协议(UDP)流量。

下一个扩展访问列表可适应您的网络。本示例假设路由器接口上配置了IP地址192.168.10.1和172.16.1.1，所有SNMP访问都限制在IP地址为10.1.1.1的管理站上，并且管理站仅需要与IP地址192.168.10.1通信：

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

此 access-list 然后必须使用以下配置命令应用到所有接口：

```
interface ethernet 0/0

ip access-group 101 in
```

在UDP端口上与路由器直接通信的所有设备都需要明确列在之前的访问列表中。Cisco IOS软件使用49152到65535范围内的端口作为出站会话(例如域名系统(DNS)查询)的源端口。

对于配置了许多IP地址的设备或需要与路由器通信的许多主机，此解决方案并非总是可扩展的。

rACLs

对于分布式平台，rACL可以是从Cisco 12000系列千兆位交换机路由器(GSR)的Cisco IOS软件版本12.0(21)S2和Cisco 7500系列的12.0(24)S版本开始的选项。接收访问列表在流量影响路由处理器之前保护设备免受有害流量的影响。接收路径ACL也被视为网络安全最佳实践，必须将其视为良好的网络安全性的长期补充，以及针对此特定漏洞的解决方法。CPU负载分布到线卡处理器，有助于减轻主路由处理器上的负载。标题为"GSR：接收访问控制列表"的白皮书有助于识别合法流量。使用该白皮书了解如何向您的设备发送合法流量并拒绝所有不必要的数据包。

基础架构 ACL

虽然拦截经过您的网络的流量通常非常困难，但可以识别决不允许以您的基础设施设备为目标的流量，并在网络边界拦截该流量。基础设施ACL(iACL)被视为网络安全的最佳实践，必须将其视为良好的网络安全性的长期补充，以及针对此特定漏洞的解决方法。白皮书《保护您的核心：基础设施保护访问控制列表》(Protecting Your Core: Infrastructure Protection Access Control Lists)介绍了iACL的指南和推荐的部署技术。

Cisco Catalyst LAN交换机安全功能

ip permit列表功能限制从未授权的源IP地址到交换机的Inbound Telnet和SNMP访问。当发生违规或未经授权的访问时，支持系统日志消息和SNMP陷阱通知到管理系统。

Cisco IOS软件安全功能的组合可用于管理路由器和Cisco Catalyst交换机。需要建立安全策略，以限制可以访问交换机和路由器的管理站的数量。

有关如何提高IP网络安全性的详细信息，请参阅提高IP网络安全性。

如何检查 SNMP 错误

使用配置SNMP社区ACL **log** 关键字.监控 **syslog** 失败尝试，如下所示。

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

当有人尝试通过社区公共访问路由器时，您会看到 syslog 类似于：

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

此输出意味着access-list 10已拒绝来自主机172.16.1.1的五个SNMP数据包。

定期检查SNMP是否存在错误 show snmp 命令，如下所示：

```
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
```

观察标有**误率意外增加的计数器，这些错误率可能表示有人试图利用这些漏洞。要报告任何安全问题，请参阅思科产品安全事件响应。

相关信息

- **思科安全公告SNMP漏洞**
- **思科技术支持和下载**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。