保護您的簡單網路管理協定

目錄

簡介

本檔案將說明如何保護您的簡易網路管理通訊協定(SNMP)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- SNMP檢視 — Cisco IOS®軟體版本10.3或更高版本。
- SNMP版本3 — 在Cisco IOS軟體版本12.0(3)T中匯入。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

保護您的SNMP非常重要，尤其是當可以重複利用SNMP的漏洞來產生拒絕服務(DoS)時。

保護SNMP的策略

選擇良好的SNMP社群字串

將public用作唯讀或private用作讀取/寫入社群字串並不**是良**好的作法。

設定SNMP檢視

其 Setup SNMP view 命令可以阻止僅訪問有限管理資訊庫(MIB)的使用者。預設情況下，沒有 SNMP view entry exists .此命令在全域性配置模式下配置，並首先在Cisco IOS軟體版本10.3中引入。它的作用類似於 access-list 如果你有任何 SNMP View 在一些MIB樹上，其他所有樹都會被莫名其妙地拒絕。但是，序列並不重要，它會在停止之前瀏覽整個清單以尋找相符專案。

要建立或更新檢視條目，請使用 snmp-server view global configuration 指令。要刪除指定的SNMP伺服器檢視條目，請使用 no 命令形式。

語法:

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

no snmp-server view view-name
```

語法說明:

- view-name — 為更新或建立的檢視記錄新增標籤。該名稱用於引用記錄。
- oid-tree — 要包括在檢視中或從檢視中排除的抽象語法表示法One(ASN.1)子樹的對象識別符號。要標識子樹，請指定由數字（如1.3.6.2.4）或單詞（如）組成的文本字串 system. 用星號(*)萬用字元替換單個子識別符號以指定子樹族；例如1.3.*.4。
- included | excluded — 檢視型別。必須指定included或excluded。

當需要檢視而不是必須定義的檢視時，可以使用兩個標準的預定義檢視。一個是全部，表示使用者可以看到所有對象。另一個是*受限*，這表示使用者可以看到三個組： system中， snmpStats,和 snmpParties.RFC 1447中介紹了預定義的檢視。

> **註**：第一 snmp-server 您輸入的命令會啟用兩個版本的SNMP。

此示例將建立一個檢視，其中包含MIB-II系統組中除以下對象以外的所有對象 sysServices （系統7）和MIB-II介面組中介面1的所有對象：

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

以下是一個完整的示例，說明如何將MIB與社群字串和 snmpwalk 與 view 就位。此組態定義一個檢視，用於拒絕位址解析通訊協定(ARP)表的SNMP存取(atEntry)，並允許MIB-II和Cisco專用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系統組的命令和輸出：

```
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 System組的命令和輸出：

```
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表的命令和輸出：

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

使用存取清單設定SNMP社群

目前的最佳實踐建議您將存取控制清單(ACL)套用到社群字串，並確保要求社群字串與通知社群字串不同。存取清單在與其他保護措施結合使用時會提供進一步保護。

以下範例將ACL設定為社群字串：

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

對請求和陷阱消息使用不同的社群字串時，如果攻擊者發現社群字串，就會降低進一步攻擊或危害的可能性。否則，攻擊者可能會未經授權而攻擊遠端裝置或從網路嗅探陷阱消息。

使用社群字串啟用陷阱後，可以在某些Cisco IOS軟體中為SNMP存取啟用該字串。您必須明確停用此社群。 例如：

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

設定SNMP版本3

SNMP第3版最初是在Cisco IOS軟體版本12.0中匯入，但是尚未在網路管理中普遍使用。執行以下步驟配置SNMP版本3:

1. 為SNMP實體分配引擎ID（可選）。
2. 定義一個使用者，**使用者**，該使用者屬於組**groupone**，然後對此使用者應用**noAuthentication**（無密碼）和**noPrivacy**（無加密）。
3. 定義屬於組**grouptwo**的使用者 **usertwo **，並向此使用者應用**noAuthentication**（無密碼）和**noPrivacy**（無加密）。
4. 定義使用者、**組groupthree**的userthree並應用**Authentication**(password is user3passwd)和**noPrivacy**(no encryption)到此使用者。
5. 定義屬於組**groupfour**的使用者**userfour**，並將**Authentication**(password is user4passwd)和**Privacy**（des56加密）應用到此使用者。
6. 通過使用者安全模型(**USM)V3定義組groupone**，並在**v1預設檢視（預設）上啟用讀**取訪問許可權（預設）。
7. 通過**USM V3定義**組grouptwo，並啟用對myview檢視的讀取**訪問**。
8. 通過**USM V3**定義組**組**，並通過身份驗證在**v1預設檢視(預設**值)上啟用讀取**訪問**。
9. 通過**USM V3**定義組 **groupfour**，並通過**Authentication** 和**Privacy** 對**v1預設檢視（預設）啟用讀取訪問。**
10. 定義一個檢視 **myview**，用於提供MIB-II的讀取訪問並拒絕對專用Cisco MIB的讀取訪問。其

show running 由於已定義社群字串Read-Only public，output為group public提供其他行。其 show running 輸出不顯示userthree字元。

範例：

```
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
```

以下是具有使用者userone的MIB-II系統組的命令和輸出:

```
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 %
```

以下是具有使用者usertwo的MIB-II系統組的命令和輸出:

```
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
```

以下是具有使用者userone的Cisco Local System群組的命令和輸出:

```
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"
```

以下是顯示無法使用user usertwo取得Cisco Local System群組的命令和**輸出**:

```
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 %
```

此命令和輸出結果用於自定義 tcpdump （針對SNMP版本3支援的補丁和printf的附錄）：

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

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

在介面上設定ACL

ACL功能提供防止IP欺騙等攻擊的安全措施。ACL可以應用於路由器的傳入或傳出介面。

在沒有選擇使用接收ACL(rACL)的平台上，可以允許使用者資料包通訊協定(UDP)流量從具有介面ACL的受信任IP位址到達路由器。

下一個擴展訪問清單可調整為適合您的網路。此範例假設路由器在其介面上設定了IP位址192.168.10.1和172.16.1.1，所有SNMP存取都必須限制在IP位址為10.1.1.1的管理站上，且管理站只需與IP位址192.168.10.1通訊即可：

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

其 access-list 然後必須使用以下配置命令應用到所有介面：

```
interface ethernet 0/0

ip access-group 101 in
```

在UDP埠上與路由器直接通訊的所有裝置都需要具體列在以前的訪問清單中。Cisco IOS軟體使用49152至65535範圍內的連線埠作為傳出作業階段(例如網域名稱系統(DNS)查詢)的來源連線埠。

對於配置了許多IP地址的裝置或需要與路由器通訊的許多主機，這並非總是可擴展的解決方案。

rACL

對於分散式平台，rACL可以是啟動於Cisco 12000系列Gigabit交換器路由器(GSR)的Cisco IOS軟體版本12.0(21)S2和啟動於Cisco 7500系列的12.0(24)S的選項。接收訪問清單可在流量影響路由處理器之前保護裝置免受有害流量影響。接收路徑ACL也被視為網路安全的最佳做法，必須將其視為對良好網路安全的長期附加措施，以及針對這一特定漏洞的解決方法。CPU負載分佈到線卡處理器，並幫助減輕主路由處理器上的負載。標題為「GSR:Receive Access Control Lists」的白皮書可幫助識別合法流量。使用該白皮書瞭解如何向您的裝置傳送合法流量並拒絕所有不需要的資料包。

基礎架構ACL

雖然攔截穿過您的網路的流量通常非常困難，但可以識別決不能允許以您的基礎設施裝置為目標的流量，並在網路邊界攔截該流量。基礎架構ACL(iACL)視為網路安全最佳實踐，必須視為對良好網路安全的長期強化措施，以及針對此特定漏洞的解決方法。白皮書《保護您的核心：基礎設施保護訪問控制清單》介紹了iACL的准則和推薦的部署技術。

Cisco Catalyst LAN交換器安全功能

IP Permit List（IP允許清單）功能限制來自未經授權的源IP地址的入站Telnet和SNMP訪問交換機。支援系統日誌消息和SNMP陷阱在出現違規或未授權訪問時通知管理系統。

Cisco IOS軟體安全功能的組合可用於管理路由器和Cisco Catalyst交換機。需要建立安全策略，以限制可以訪問交換機和路由器的管理站的數量。

有關如何提高IP網路安全性的詳細資訊，請參閱提高IP網路安全性。

如何檢查SNMP錯誤

使用 log 關鍵字。監視 syslog 失敗嘗試，如下所示。

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

當有人嘗試使用社群公共訪問路由器時，您會看到 syslog 類似於：

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

此輸出表示存取清單10已拒絕來自主機172.16.1.1的五個SNMP封包。

定期檢查SNMP中是否存在錯誤 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
```

觀察標有錯誤率**意外增加的計數器，這些錯誤率可能表示試圖利用這些漏洞。要報告任何安全問題，請參閱思科產品安全事件響應。

相關資訊

- **思科安全諮詢SNMP漏洞**
- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。