Beveiliging van uw eenvoudige netwerkbeheerprotocol

Inhoud

Inleiding

Dit document beschrijft hoe u uw Simple Network Management Protocol (SNMP) kunt beveiligen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SNMP View — Cisco IOS®-softwarerelease 10.3 of hoger.
- SNMP versie 3 — geïntroduceerd in Cisco IOS-softwarerelease 12.0(3)T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Het is belangrijk om uw SNMP te beveiligen vooral wanneer de kwetsbaarheden van SNMP herhaaldelijk kunnen worden geëxploiteerd om een denial of service (DoS) te produceren.

Strategieën voor beveiligde SNMP

Kies een goede SNMP-community-string

Het is geen goede gewoonte om **publiek** als alleen-lezen en **privé** te gebruiken als gemeenschapssnaren voor lezen-schrijven.

SNMP-weergave instellen

Het Setup SNMP view Met deze opdracht kan de gebruiker worden geblokkeerd, met alleen toegang tot de Limited Management Information Base (MIB). Standaard is er geen SNMP view entry exists . Deze opdracht wordt geconfigureerd op de globale configuratiemodus en voor het eerst geïntroduceerd in Cisco IOS-softwareversie 10.3. Het werkt vergelijkbaar met **access-list** in dat geval als u een SNMP View op bepaalde MIB-bomen, elke andere boom wordt onverklaarbaar ontkend. Echter, de volgorde is niet belangrijk en het gaat door de gehele lijst voor een match voordat het stopt.

Om een weergaveingang te maken of bij te werken, gebruikt u de **snmp-server view global configuration** uit. Als u de gespecificeerde SNMP-serverweergave wilt verwijderen, gebruikt u de **no** vorm van deze opdracht.

Syntaxis:

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

no snmp-server view view-name
```

Syntax Beschrijving:

- view-name—Label voor de weergaverecord die u bijwerkt of maakt. De naam wordt gebruikt om naar de record te verwijzen.
- oid-tree —Object identifier van de Abstract Syntax Notation One (ASN.1) subboom op te nemen of uit te sluiten van de weergave. Om de substructuur te identificeren, specificeert u een tekststring die uit getallen bestaat, zoals 1.3.6.2.4, of een woord, zoals system. Vervang een enkele subidentificator door de wildcard voor sterretje (*) om een subboomfamilie op te geven; bijvoorbeeld 1.3.*.4.
- included | excluded—Type weergave. U moet opgeven of dit wel of niet moet gebeuren.

Er kunnen twee standaard voorgedefinieerde weergaven worden gebruikt wanneer er een weergave nodig is in plaats van een weergave die moet worden gedefinieerd. Een daarvan is alles, wat aangeeft dat de gebruiker alle objecten kan zien. De andere is *beperkt* , wat aangeeft dat de gebruiker drie groepen kan zien: system, snmpStats, en snmpParties. De vooraf gedefinieerde weergaven worden beschreven in RFC 1447.

> **Opmerking**: het eerste snmp-server Met de opdracht die u invoert, kunt u beide versies van SNMP inschakelen.

Dit voorbeeld maakt een weergave die alle objecten in de MIB-II systeemgroep bevat, behalve voor sysServices (Systeem 7) en alle objecten voor interface 1 in de groep MIB-II interfaces:

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

Dit is een volledig voorbeeld voor hoe de MIB met community string en de output van de snmpwalk met view op zijn plaats. Deze configuratie definieert een weergave waarmee de SNMP-toegang voor de ARP-tabel (Address Resolution Protocol) wordt geweigerd (atEntry) en maakt het mogelijk voor MIB-II en Cisco Private 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
```

Dit is de opdracht en de uitvoer voor de MIB-II-systeemgroep:

```
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 %
```

Dit is de opdracht en de uitvoer voor de lokale Cisco System-groep:

```
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
```

Dit is de opdracht en de uitvoer voor de MIB-II ARP-tabel:

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

SNMP-community met toegangslijst instellen

De beste huidige praktijken adviseren dat u de Lijsten van het Toegangsbeheer (ACLs) op communautaire koorden toepast en ervoor zorgt dat de verzoeken communautaire koorden niet identiek zijn aan berichten communautaire koorden. Toegangslijsten bieden verdere bescherming wanneer zij worden gebruikt in combinatie met andere beschermingsmaatregelen.

In dit voorbeeld wordt ACL ingesteld op community string:

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Wanneer u verschillende community strings voor verzoeken en trap berichten gebruikt, vermindert het de kans op verdere aanvallen of compromissen als de community string wordt ontdekt door een aanvaller. Anders, kon een aanvaller een ver apparaat compromitteren of een valbericht van het netwerk zonder vergunning snuiven.

Als u trap met een community-string inschakelt, kan de string worden ingeschakeld voor SNMP-toegang in bepaalde Cisco IOS-software. U moet deze community expliciet uitschakelen. Voorbeeld:

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

SNMP versie 3 installeren

SNMP versie 3 is eerst geïntroduceerd in Cisco IOS-softwareversie 12.0, maar wordt nog niet veel gebruikt in netwerkbeheer. Voer deze stappen uit om SNMP versie 3 te configureren:

1. Wijs een Engine-ID toe aan de SNMP-entiteit (optioneel).
2. Definieer een gebruiker, **gebruiker** die behoort tot de groep **groep** en pas **geen verificatie** (geen wachtwoord) en **geen privacy** (geen encryptie) toe op deze gebruiker.
3. Definieer een gebruiker, **usertwo ;**die tot de groep **group two** behoort en pas **geen verificatie** (geen wachtwoord) en **geen privacy** (geen encryptie) toe op deze gebruiker.
4. Definieer een gebruiker, **user-three** die behoort tot de groep **drie** en pas **verificatie** (wachtwoord is user3passwd) en **noPrivacy** (geen encryptie) toe op deze gebruiker.
5. Definieer een gebruiker, **userfour**, die tot de groep **group four** behoort en pas **verificatie** (wachtwoord is user4password) en **Privacy** (des56 encryptie) op deze gebruiker toe.
6. Definieer een groep, **groeptoon** door middel van User Security Model (USM) V3 en schakel leestoegang in op de **v1default** view (de standaard).
7. Definieer een groep, **groep twee**, met behulp van USM V3 en laat leestoegang op de weergave **myview** toe.
8. Definieer een groep, **groep drie** , met behulp van USM V3, en laat gelezen toegang op de **v1default** view (de standaard) toe door middel van **authenticatie** .
9. Definieer een groep, **groep vier** , met behulp van USM V3, en laat leestoegang toe op de **v1default** view (de standaard), door middel van **Verificatie** en **Privacy** .
10. Definieer een weergave, **myview**, die leestoegang biedt op de MIB-II en die leestoegang ontzegt op de privé Cisco MIB.Het **show running** output geeft extra regels voor het **publiek** van de groep, vanwege het feit dat er een community string Read-Only **publiek** is dat is gedefinieerd.Het **show running** de output toont niet de **user drie**.

Voorbeeld:

```
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
```

Dit is de opdracht en de uitvoer voor de MIB-II-systeemgroep met **gebruikersinterface** :

```
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 %
```

Dit is de opdracht en de uitvoer voor de MIB-II-systeemgroep met **gebruikersinterface twee**:

```
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
```

Dit is de opdracht en de uitvoer voor de groep Lokaal systeem van Cisco met **gebruikersinterface**:

```
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"
```

Dit is de opdracht en de uitvoer die laat zien dat u de groep Lokaal systeem van Cisco niet kunt krijgen met **gebruikersinterface**:

```
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 %
```

Deze opdracht en het uitvoerresultaat zijn voor een aangepaste **tcpdump** (patch voor SNMP versie 3 ondersteuning en addendum bij print):

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

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

ACL-waarden op interfaces instellen

De ACL-functie biedt beveiligingsmaatregelen die aanvallen zoals IP-spoofing voorkomen. ACL kan op inkomende of uitgaande interfaces op routers worden toegepast.

Op platforms die niet de optie hebben om ACL's (rACL's) te gebruiken, is het mogelijk om verkeer met User Datagram Protocol (UDP) toe te staan aan de router vanaf vertrouwde IP-adressen met interface-ACL's.

De volgende uitgebreide toegangslijst kan worden aangepast aan uw netwerk. In dit voorbeeld wordt ervan uitgegaan dat de router IP-adressen 192.168.10.1 en 172.16.1.1 op zijn interfaces heeft geconfigureerd, dat alle SNMP-toegang moet worden beperkt tot een beheerstation met het IP-adres van 10.1.1.1 en dat het beheerstation alleen hoeft te communiceren met IP-adres 192.168.10.1:

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

Het access-list moet dan op alle interfaces met deze configuratiebevelen worden toegepast:

```
interface ethernet 0/0

ip access-group 101 in
```

Alle apparaten die rechtstreeks met de router communiceren op UDP-poorten moeten specifiek worden vermeld in de vorige toegangslijst. Cisco IOS-software maakt gebruik van poorten in de 49152 om als bronpoort te 65535 voor uitgaande sessies zoals DNS-vragen (Domain Name System).

Voor apparaten die veel IP-adressen geconfigureerd hebben, of veel hosts die met de router moeten communiceren, is dit niet altijd een schaalbare oplossing.

ACL's

Voor gedistribueerde platforms kunnen rACL's een optie zijn die begint in Cisco IOS-softwarerelease 12.0(21)S2 voor de Cisco 12000 Series Gigabit Switch Router (GSR) en release 12.0(24)S voor Cisco 7500 Series. De ontvangsttoegangslijsten beschermen het apparaat tegen schadelijk verkeer voordat het verkeer de routeprocessor kan beïnvloeden. Ontvang pad ACL's ook worden beschouwd als een best practice voor netwerkbeveiliging, en moet worden beschouwd als een lange-termijntoevoeging aan goede netwerkbeveiliging, evenals een tijdelijke oplossing voor deze specifieke kwetsbaarheid. De CPU-belasting wordt gedistribueerd naar de lijnkaartprocessors en helpt de belasting op de hoofdrouteprocessor te verminderen. Het witboek GSR: Receive Access Control Lists helpt bij het identificeren van legitiem verkeer. Gebruik dat white paper om te begrijpen hoe je legitiem verkeer naar je apparaat te sturen en ontken ook alle ongewenste pakketten.

Infrastructuur ACL's

Hoewel het vaak moeilijk is om verkeer te blokkeren dat uw netwerk doorkruist, is het mogelijk om verkeer te identificeren dat nooit moet worden toegestaan om uw infrastructuurapparaten te richten en dat verkeer aan de grens van uw netwerk te blokkeren. Infrastructuur ACL's (iACL's) worden beschouwd als best practice voor netwerkbeveiliging en moeten worden beschouwd als een langetermijntoevoeging aan goede netwerkbeveiliging en als een tijdelijke oplossing voor deze specifieke kwetsbaarheid. Het witboek, Protected Your Core: Infrastructure Protection Access Control Lists, presenteert richtlijnen en aanbevolen implementatietechnieken voor iACL's.

Cisco Catalyst LAN-Switch beveiligingsfunctie

De functie IP-toegangslijst beperkt inkomende Telnet- en SNMP-toegang tot de switch vanaf onbevoegde IP-bronadressen. Syslog-berichten en SNMP-traps worden ondersteund om een beheersysteem op de hoogte te stellen wanneer een schending of onbevoegde toegang optreedt.

Een combinatie van de Cisco IOS-softwareveiligheidsfuncties kan worden gebruikt voor het beheer van routers en Cisco Catalyst-switches. Er moet een beveiligingsbeleid worden vastgesteld dat het aantal beheerstations beperkt dat toegang kan krijgen tot de switches en routers.

Raadpleeg Beveiliging verhogen op IP-netwerken voor meer informatie over het verhogen van de beveiliging op IP-netwerken.

SNMP-fouten controleren

De SNMP-community-ACL's configureren met de **log** trefwoord. Monitor (bewaken) **syslog** voor mislukte pogingen, zoals hieronder wordt getoond.

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

Wanneer iemand probeert toegang te krijgen tot de router met het publiek in de community, ziet u een syslog vergelijkbaar met deze:

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

Deze output betekent dat access-list 10 vijf SNMP-pakketten ontkent van de host 172.16.1.1.

Controleer SNMP regelmatig op fouten met de show snmp bevel, zoals hier getoond:

```
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
```

Kijk naar de tellers die ** zijn voor onverwachte toenames in foutpercentages die kunnen duiden op pogingen om deze kwetsbaarheden te exploiteren. Als u een beveiligingsprobleem wilt melden, raadpleegt u Cisco Product Security Incident Response (Productbeveiliging).

Gerelateerde informatie

- Cisco Security Advisories SNMP-kwetsbaarheden
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.