Proteja seu protocolo simples de gerenciamento de rede

Contents

Introduction

Este documento descreve como proteger seu SNMP (Simple Network Management Protocol).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- SNMP View — Cisco IOS® Software Release 10.3 ou posterior.
- SNMP versão 3 — Introduzido no Cisco IOS Software Release 12.0(3)T.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

Éimportante proteger o SNMP, especialmente quando as vulnerabilidades do SNMP podem ser repetidamente exploradas para produzir uma negação de serviço (DoS).

Estratégias para proteger o SNMP

Escolha uma série de comunidade do SNMP adequada

Não é uma boa prática usar **public** como somente leitura e **private** como strings de comunidade de leitura-gravação.

Configurar visualização SNMP

O Setup SNMP view pode bloquear o usuário com acesso apenas à MIB (Management Information Base) limitada. Por padrão, não há SNMP view entry exists . Esse comando é configurado no modo de configuração global e introduzido pela primeira vez no Cisco IOS Software versão 10.3. Funciona de forma semelhante a **access-list** nesse caso, se você tiver SNMP View em certas árvores MIB, qualquer outra árvore é negada inexplicavelmente. No entanto, a sequência não é importante e percorre toda a lista para obter uma correspondência antes de parar.

Para criar ou atualizar uma entrada de exibição, use o comando **snmp-server view global configuration** comando. Para remover a entrada de visualização do servidor SNMP especificada, use o comando **no** forma desse comando.

Sintaxe:

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

no snmp-server view view-name
```

Descrição da sintaxe:

- view-name—Rótulo para o registro de exibição que você atualiza ou cria. O nome é usado para fazer referência ao registro.
- oid-tree —Identificador de objeto da subárvore ASN.1 (Abstract Syntax Notation One) a ser incluída ou excluída da exibição. Para identificar a subárvore, especifique uma string de texto que consiste em números, como 1.3.6.2.4, ou uma palavra, como system. Substitua um único subidentificador pelo curinga asterisco (*) para especificar uma família de subárvores; por exemplo, 1.3.*.4.
- included | excluded—Tipo de vista. Você deve especificar incluído ou excluído.

Duas exibições padrão predefinidas podem ser usadas quando uma exibição é necessária, em vez de uma exibição que deve ser definida. Um é tudo, o que indica que o usuário pode ver todos os objetos. O outro é *restricted*, que indica que o usuário pode ver três grupos: system, snmpStats,e snmpParties. As visualizações predefinidas são descritas no RFC 1447.

Observação: o primeiro snmp-server que você digitar habilitará ambas as versões do SNMP.

Este exemplo cria uma visualização que inclui todos os objetos no grupo de sistema MIB-II, exceto para **sysServices** (Sistema 7) e todos os objetos para a interface 1 no grupo de interfaces MIB-II:

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

Este é um exemplo completo de como aplicar o MIB com community string e a saída do comando snmpwalk com view em vigor. Essa configuração define uma exibição que nega o acesso de SNMP à tabela ARP (atEntry) e permite MIB-II e MIB privada da Cisco:

```
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
```

Este é o comando e saída para o grupo de sistema MIB-II:

```
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 %
```

Este é o comando e a saída do grupo local do Cisco System:

```
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
```

Este é o comando e a saída da tabela ARP MIB-II:

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

Configurar a comunidade de SNMP com lista de acesso

As melhores práticas atuais recomendam que você aplique Listas de controle de acesso (ACLs) a strings de comunidade e assegure que as strings de comunidade de solicitações não sejam idênticas às strings de comunidade de notificações. As listas de acesso fornecem proteção adicional quando usadas em combinação com outras medidas de proteção.

Este exemplo configura a ACL para community string:

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Quando você usa strings de comunidade diferentes para solicitações e mensagens de interceptação, ela reduz a probabilidade de mais ataques ou comprometimentos se a sequência de comunidade for descoberta por um invasor. Caso contrário, um invasor pode comprometer um dispositivo remoto ou farejar uma mensagem de interceptação (trapping) da rede sem autorização.

Quando você habilita o trap com uma string de comunidade, a string pode ser habilitada para acesso SNMP em algum software Cisco IOS. Você deve desativar explicitamente esta comunidade. Por exemplo:

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

Configuração de SNMP versão 3

O SNMP versão 3 foi introduzido pela primeira vez no Cisco IOS Software versão 12.0, mas ainda não é comumente usado no gerenciamento de rede. Siga estas etapas para configurar a versão 3

do SNMP:

1. Atribua um ID de mecanismo para a entidade SNMP (opcional).
2. Defina um usuário, **userone** que pertença ao grupo **groupone** e aplique **noAuthentication** (sem senha) e **noPrivacy** (sem criptografia) a este usuário.
3. Defina um usuário, **usertwo ;**que pertença ao **grupo dois** e aplique **noAuthentication** (sem senha) e **noPrivacy** (sem criptografia) a este usuário.
4. Defina um usuário, **userthree** que pertença ao **grupo groupthree** e aplique **Authentication** (a senha é user3passwd) e **noPrivacy** (sem criptografia) a este usuário.
5. Defina um usuário, **userfour** , que pertença ao grupo **groupfour** e aplique **Authentication** (a senha é user4passwd) e **Privacy** (criptografia des56) a este usuário.
6. Defina um grupo, **groupone** , por meio do User Security Model (USM) V3 e habilite o acesso de leitura na **exibição v1default** (padrão).
7. Defina um grupo, o **grupo dois** , por meio do USM V3 e habilite o acesso de leitura no modo de exibição **myview** .
8. Defina um grupo, o **grupo três** , por meio do USM V3, e habilite o acesso de leitura na visualização **v1default** (o padrão), por meio da **autenticação** .
9. Defina um grupo, o **grupo quatro** , por meio do USM V3, e habilite o acesso de leitura na visualização **v1default** (o padrão), por meio de **Authentication** e **Privacy** .
10. Defina uma exibição, **myview** , que forneça acesso de leitura no MIB-II e negue o acesso de leitura no MIB privado da Cisco.O show running A saída fornece linhas adicionais para o grupo **public**, devido ao fato de que há uma sequência de comunidade Read-Only **public** que foi definida.O show running a saída não mostra o **usuário três**.

Exemplo:

```
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
```

Este é o comando e saída para o grupo de sistema MIB-II com user **userone** :

```
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 %
```

Este é o comando e saída para o grupo de sistema MIB-II com user **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
```

Este é o comando e saída para o grupo Cisco Local System com user **userone**:

```
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"
```

Este é o comando e saída que mostra que você não pode obter o grupo Cisco Local System com user **usertwo**:

```
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 %
```

Esse comando e o resultado da saída são para um **tcpdump** (patch para suporte de SNMP versão 3 e adendo de printf):

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

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

Configurar a ACL nas interfaces

O recurso ACL fornece medidas de segurança que evitam ataques como falsificação de IP. O ACL pode ser aplicado em interfaces de entrada ou de saída nos roteadores.

Em plataformas que não têm a opção de usar ACLs de recebimento (rACLs), é possível permitir o tráfego do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol) para o roteador a partir de endereços IP confiáveis com ACLs de interface.

A próxima lista de acesso estendida pode ser adaptada à sua rede. Este exemplo pressupõe que o roteador tenha os endereços IP 192.168.10.1 e 172.16.1.1 configurados em suas interfaces, que todo o acesso SNMP deve ser restrito a uma estação de gerenciamento com o endereço IP 10.1.1.1 e que a estação de gerenciamento só precisa se comunicar com o endereço IP 192.168.10.1:

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

O access-list deve ser aplicado a todas as interfaces com estes comandos de configuração:

```
interface ethernet 0/0

ip access-group 101 in
```

Todos os dispositivos que se comunicam diretamente com o roteador em portas UDP precisam estar especificamente listados na lista de acesso anterior. O software Cisco IOS usa portas no intervalo 49152 para 65535 como a porta de origem para sessões de saída, como consultas DNS (Domain Name System).

Para dispositivos que têm muitos endereços IP configurados, ou muitos hosts que precisam se comunicar com o roteador, essa nem sempre é uma solução escalável.

rACLs

Para plataformas distribuídas, rACLs podem ser uma opção que começa no Cisco IOS Software Release 12.0(21)S2 para o Cisco 12000 Series Gigabit Switch Router (GSR) e Release 12.0(24)S para o Cisco 7500 Series. As listas de acesso de recepção protegem o dispositivo contra tráfego prejudicial antes que o tráfego possa impactar o processador de rota. As ACLs de caminho de recepção também são consideradas uma prática recomendada de segurança de rede e devem ser consideradas como um acréscimo de longo prazo à boa segurança de rede, bem como uma solução para essa vulnerabilidade específica. A carga da CPU é distribuída para os processadores da placa de linha e ajuda a reduzir a carga no processador da rota principal. O white paper GSR: Receive Access Control Lists ajuda a identificar o tráfego legítimo. Use esse white paper para entender como enviar tráfego legítimo ao seu dispositivo e também negar todos os pacotes indesejados.

Infra-estrutura ACL

Embora geralmente seja difícil bloquear o tráfego que transita pela rede, é possível identificar o tráfego que nunca deve ter permissão para atingir os dispositivos de infraestrutura e bloquear esse tráfego na borda da rede. As ACLs de infraestrutura (iACLs) são consideradas uma prática

recomendada de segurança de rede e devem ser consideradas como um acréscimo de longo prazo à boa segurança de rede, bem como uma solução para essa vulnerabilidade específica. O white paper Protecting Your Core: Infrastructure Protection Access Control Lists apresenta diretrizes e técnicas de implantação recomendadas para iACLs.

Recurso de segurança do switch LAN Cisco Catalyst

O recurso de Lista de permissão IP restringe o acesso de entrada Telnet e SNMP ao switch a partir de endereços IP de origem não autorizada. As mensagens do syslog e as armadilhas do SNMP são suportadas para notificar um sistema de gerenciamento quando ocorre uma violação ou acesso não autorizado.

Uma combinação dos recursos de segurança do software Cisco IOS pode ser usada para gerenciar roteadores e switches Cisco Catalyst. É necessário estabelecer uma política de segurança que limite o número de estações de gerenciamento que podem acessar os switches e roteadores.

Para obter mais informações sobre como aumentar a segurança em redes IP, consulte Aumentando a Segurança em Redes IP.

Como verificar erros de SNMP

Configure as ACLs da comunidade SNMP com o comando **log** palavra-chave. Monitor **syslog** para tentativas falhas, conforme mostrado abaixo.

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

Quando alguém tenta acessar o roteador com o público da comunidade, você vê um syslog semelhante a:

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

Essa saída significa que a lista de acesso 10 negou cinco pacotes SNMP do host 172.16.1.1.

Verifique periodicamente se há erros de SNMP com o comando show snmp , como mostrado aqui:

```
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
```

Observe os contadores marcados ** para aumentos inesperados nas taxas de erro que podem indicar uma tentativa de exploração dessas vulnerabilidades. Para relatar qualquer problema de segurança, consulte Resposta a incidentes de segurança de produtos da Cisco.

Informações Relacionadas

- Vulnerabilidades de SNMP das Recomendações de Segurança da Cisco
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.