Protegendo o Protocolo de Gerenciamento de Rede Simples

Índice

Introdução

Este documento fornece informações sobre como proteger o Simple Network Management Protocol (SNMP). Proteger o SNMP é importante, especialmente quando as vulnerabilidades do SNMP podem ser repetidamente exploradas para produzirem uma negação de serviço (DoS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Opinião SNMP — Software Release 10.3 ou Mais Recente de Cisco IOS®.
- SNMP Versão 3 — Introduzido no Cisco IOS Software Release 12.0(3)T.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Estratégias de proteção de SNMP

Escolha uma série de comunidade do SNMP adequada

Não é uma boa prática usar o **público** tão de leitura apenas e **privado** quanto séries de comunidade de leitura/gravação.

Configurar visualização SNMP

O comando Setup SNMP view pode obstruir o usuário com somente acesso ao Management Information Base limitado (MIB). À revelia, não há nenhuma **entrada de visualização SNMP existe**. Este comando é configurado no modo de configuração global e introduzido primeiramente na versão 10.3 do Cisco IOS Software. Trabalha similar à **lista de acesso n**aquele se você tem qualquer **opinião SNMP em** determinadas árvores de MIB, cada outra árvore é negado inexplicably. Contudo, a sequência não é importante e examina a lista inteira para um fósforo antes que pare.

Para criar ou atualizar uma entrada da vista, use o **comando snmp-server view global configuration**. Para remover a entrada especificada da opinião do servidor SNMP, não use **nenhum** formulário deste comando.

Sintaxe:

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

no snmp-server view view-name
```

Descrição da sintaxe:

- **vista-nome** — Etiqueta para o registro da vista que você está atualizando ou está criando. O nome é usado para prover o registro.
- **OID-árvore** — Identificador de objeto do subtree do Abstract Syntax Notation One (ASN.1) a ser incluído ou excluído da vista. Para identificar o subtree, especifique números consistindo de uma sequência de caracteres de texto, tais como 1.3.6.2.4, ou uma palavra, tal como o **sistema**. Substitua um único secundário-identificador com o convite do asterisco (*) para especificar uma família de subárvore; por exemplo 1.3.*.4.
- **incluído | excluído** — Tipo de vista. Você deve especificar incluído ou excluído.

Dois visualização pré-definida padrões podem ser usados quando uma vista é exigida, em vez de

definir uma vista. Um é tudo, que indica que o usuário pode ver todos os objetos. O outro é *restrito*, que indica que o usuário pode ver três grupos: **sistema**, **snmpStats**, e **snmpParties**. A visualização pré-definida é descrita no RFC 1447.

Note: O primeiro **comando snmp-server** que você inscreve permite ambas as versões do SNMP.

Este exemplo cria uma vista que inclua todos os objetos no grupo de sistemas MIB-II à exceção dos **sysServices** (sistema 7) e todos os objetos para a relação 1 no grupo das relações 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 para que como aplique o MIB com string de comunidade e a saída do **snmpwalk** com **vista** no lugar. Esta configuração define uma vista que negue o acesso SNMP para a tabela do Address Resolution Protocol (ARP) (**atEntry**) e o permita MIB-II e Cisco MIB privado:

```
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
```

Esta é o comando e a saída para o grupo de sistemas MIB-II:

```
NMSPrompt 82 % snmpwalk cough system
system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software
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 %
```

Esta é o comando e a saída para o grupo de sistema Cisco local:

```
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
```

Esta é o comando e a saída para a 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 aplicar o Access Control Lists (ACLs) aos string de comunidade e assegurar-se de que os string de comunidade dos pedidos não sejam idênticos aos string de comunidade das notificações. As Listas de acesso fornecem uma proteção mais adicional quando usadas em combinação com outras medidas de proteção.

Este exemplo ajusta-se - acima do ACL ao string de comunidade:

```
access-list 1 permit 1.1.1.1

snmp-server community string1 ro 1
```

Usar string de comunidade diferentes para pedidos e mensagens de armadilha reduz a probabilidade dos futuros ataques ou dos acordos se o string de comunidade é descoberto por um atacante, quer através de comprometer um dispositivo remoto ou aspirando um mensagem de armadilha da rede sem autorização.

Uma vez que você permite a armadilha com um string de comunidade, a corda pode ser permitida para o acesso SNMP em algum Cisco IOS Software. Você deve explicitamente desabilitar esta comunidade.

Por exemplo:

```
access-list 10 deny any
snmp-server host 1.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

Configuração de SNMP versão 3

O SNMP Versão 3 foi introduzido primeiramente na versão 12.0 do Cisco IOS Software, mas não é de uso geral no Gerenciamento de redes ainda. Para configurar o SNMP Versão 3, termine estas etapas:

1. Atribua um Engine ID para a Entidade SNMP (opcional).
2. Defina um usuário, **userone**, pertencendo ao **groupone do** grupo e aplique o **noAuthentication** (nenhuma senha) e o **noPrivacy** (no encryption) a este usuário.
3. Defina um usuário, **usuário dois**, pertencendo ao **grouptwo do** grupo e aplique o **noAuthentication** (nenhuma senha) e o **noPrivacy** (no encryption) a este usuário.
4. Defina um usuário, **userthree**, pertencendo ao **groupthree do** grupo e aplique a **autenticação** (a senha é user3passwd) e o **noPrivacy** (no encryption) a este usuário.
5. Defina um usuário, **userfour**, pertencendo ao **groupfour do** grupo e aplique a **autenticação** (a senha é user4passwd) e a **privacidade** (criptografia des56) a este usuário.
6. Defina um grupo, **groupone**, usando o User Security Model (US) V3 e tendo o acesso de leitura na opinião **v1default** (o padrão).
7. Defina um grupo, **grouptwo**, usando US V3 e tendo o acesso de leitura no **myview da** vista.
8. Defina um grupo, **groupthree**, usando US V3, tendo o acesso de leitura na opinião **v1default** (o padrão), e usando a **autenticação**.
9. Defina um grupo, **groupfour**, usando US V3, tendo o acesso de leitura na opinião **v1default** (o padrão), e usando a **autenticação** e a **privacidade**.
10. Defina uma vista, o **myview**, que fornece o acesso de leitura no MIB-II e nega o acesso de leitura em Cisco privado MIB.A saída **running da mostra** dá as linhas adicionais para o **público do** grupo, devido ao fato de que há um **público** de leitura apenas do string de comunidade que seja definido.A saída **running da mostra** não mostra o **userthree**.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
```

Esta é o comando e a saída para o grupo de sistemas MIB-II que usa o **userone do** usuário:

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system
Module SNMPV2-TC not found
```

```
system.sysDescr.0 = Cisco Internetwork Operating System Software
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 %
```

Esta é o comando e a saída para o grupo de sistemas MIB-II que usa o **usuário dois do** usuário:

```
NMSPrompt 95 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system

Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
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
```

Esta é o comando e a saída para o grupo de sistema local de Cisco que usa o **userone do** usuário:

```
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 a saída que mostra o não pode obter o grupo de sistema local de Cisco que usa o **usuário dois do** usuário:

```
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 %
```

Estes comando e saídas resultante são para um **tcpdump** personalizado (correção de programa para o apoio do SNMP Versão 3 e o addendum do 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
```

Instalação ACL em relações

O recurso de 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.

Nas Plataformas que não têm a opção a se usar receba ACL (rACLs), ele é possível para permitir o tráfego do User Datagram Protocol (UDP) ao roteador dos endereços IP de Um ou Mais Servidores Cisco ICM NT confiados com relação ACL.

A seguinte lista de acesso extendida pode ser adaptada a sua rede. Este exemplo supõe que o roteador tem os endereços IP 192.168.10.1 e o 172.16.1.1 configurados em suas relações, que todo o acesso SNMP deve ser restringida a uma estação de gerenciamento com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.1.1.1, e que a necessidade da estação de gerenciamento se comunica somente com o endereço IP 192.168.10.1:

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

A lista de acesso deve então ser aplicada a todas as relações usando estes comandos configuration:

```
interface ethernet 0/0

ip access-group 101 in
```

Todos os dispositivos que se comunicam diretamente com o roteador em portas UDP deverão ser alistados especificamente na lista de acessos acima. O Cisco IOS Software usa portas na escala 49152 65535 como a porta de origem para sessões externas tais como perguntas do Domain Name System (DNS).

Para os dispositivos que têm muitos endereços IP de Um ou Mais Servidores Cisco ICM NT configurados, ou os muitos anfitriões que precisam de se comunicar com o roteador, esta não pode ser uma solução escalável.

rACLs

Para plataformas distribuídas, o rACLs pode ser uma opção que começa no Cisco IOS Software Release 12.0(21)S2 para o Gigabit Switch Router (GSR) do Cisco 12000 Series e liberar

12.0(24)S para o Cisco 7500 Series. As Listas de acesso da recepção protegem o dispositivo do tráfego prejudicial antes que o tráfego possa impactar o processador de rotas. Receba o trajeto ACL são considerados igualmente um melhor prática da segurança de rede, e deve ser considerado como uma adição a longo prazo à boa segurança de rede, assim como uma ação alternativa para esta vulnerabilidade específica. A carga de CPU é distribuída aos processadores da placa de linha e as ajudas abrandam a carga no processador da rota principal. O White Paper autorizado GSR: Receba listas de controle de acesso ajudará a identificar e permitir o tráfego legitimado a seu dispositivo e a negar todos os pacotes indesejados.

Infra-estrutura ACL

Embora seja frequentemente difícil obstruir o tráfego que transita por sua rede, é possível identificar o tráfego que deve nunca ser permitido visar seus dispositivos de infraestrutura e obstruir esse tráfego na beira de sua rede. A infraestrutura ACL (iACLs) é considerada um melhor prática da segurança de rede e deve ser considerada como uma adição a longo prazo à boa segurança de rede assim como uma ação alternativa para esta vulnerabilidade específica. O White Paper autorizado protegendo seu núcleo: As listas de controle de acesso da proteção de infraestrutura apresentam diretrizes e técnicas recomendadas do desenvolvimento para iACLs.

Recursos de segurança do switch LAN do Cisco catalyst

A característica da lista da licença IP restringe o telnet de entrada e o acesso SNMP ao interruptor dos endereços IP de Um ou Mais Servidores Cisco ICM NT do 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 Cisco IOS Software pode ser usada para controlar o Roteadores e o Switches do Cisco catalyst. Uma política de segurança precisa de ser estabelecida que limite o número de estações de gerenciamento capazes de alcançar o Switches e o Roteadores.

Para obter mais informações sobre de como aumentar a Segurança em redes IP, refira a segurança crescente em redes IP.

Como verificar erros de SNMP

Configurar a comunidade SNMP ACL com a palavra-chave do **log**. Monitore o **Syslog** para falhas de tentativa, como a mostra abaixo.

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

Quando alguém tenta alcançar o roteador com o público de comunidade, você vê um **Syslog** similar ao seguinte:


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

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

Verifique periodicamente o SNMP para ver se há erros executando um **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
```

Olhe os contadores marcados ** para aumentos inesperados nas taxas de erro que podem indicar a exploração falha destas vulnerabilidades. Para relatar toda a questão de segurança, refira a resposta de incidente de segurança de produto Cisco.

Informações Relacionadas

- Vulnerabilidades de SNMP das Recomendações de Segurança da Cisco
- Instalação SNMP v3 com IO 12.0
- Protocolo simples de gerenciamento de rede (SNMP)
- Configurando o SNMP
- Suporte Técnico - Cisco Systems