Proteja su protocolo simple de gestión de red

Contenido

Introducción

En este documento se describe cómo proteger el protocolo simple de administración de red (SNMP).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- SNMP View: versión 10.3 o posterior del software Cisco IOS®.
- SNMP versión 3: introducido en la versión 12.0(3)T del software del IOS de Cisco.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Antecedentes

Es importante proteger el SNMP, especialmente cuando las vulnerabilidades de SNMP se pueden aprovechar repetidamente para producir una denegación de servicio (DoS).

Estrategias para proteger SNMP

Elija una cadena de comunidad SNMP correcta

No es recomendable utilizar **public** como cadenas de comunidad de sólo lectura y **private** como cadenas de comunidad de lectura y escritura.

Setup SNMP view

Setup SNMP view puede bloquear al usuario sólo con acceso limitado a la base de información de administración (MIB). De forma predeterminada, no hay SNMP view entry exists . Este comando se configura en el modo de configuración global y se introduce por primera vez en la versión 10.3 del software del IOS de Cisco. Funciona de forma similar a **access-list** en que si tiene alguna SNMP View en ciertos árboles MIB, cada otro árbol es denegado inexplicablemente. Sin embargo, la secuencia no es importante y pasa por toda la lista para una coincidencia antes de que se detenga.

Para crear o actualizar una entrada de vista, utilice el **snmp-server view global configuration** comando. Para quitar la entrada de vista de servidor SNMP especificada, utilice el comando **no** de este comando.

Sintaxis:

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

no snmp-server view view-name
```

Descripción de la Sintaxis:

- view-name: etiqueta del registro de vista que se actualiza o se crea. El nombre se utiliza para hacer referencia al registro.
- oid-tree : identificador de objeto del subárbol ASN.1 (Abstract Syntax Notation One) que se va a incluir o excluir de la vista. Para identificar el subárbol, especifique una cadena de texto compuesta por números, como 1.3.6.2.4, o una palabra, como system. Sustituya un único subidentificador por el comodín asterisco (*) para especificar una familia de subárboles; por ejemplo, 1.3.*.4.
- included | excluded: tipo de vista. Debe especificar incluido o excluido.

Se pueden utilizar dos vistas predefinidas estándar cuando se requiere una vista en lugar de una vista que se debe definir. Una es todo, lo que indica que el usuario puede ver todos los objetos. El

otro es *restringido*, lo que indica que el usuario puede ver tres grupos: system, snmpStats,y snmpParties. Las vistas predefinidas se describen en RFC 1447.

Nota: la primera snmp-server el comando que introduzca activa ambas versiones de SNMP.

En este ejemplo se crea una vista que incluye todos los objetos del grupo de sistema MIB-II excepto **sysServices** (Sistema 7) y todos los objetos para la interfaz 1 en el 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 es un ejemplo completo de cómo aplicar la MIB con la cadena de comunidad y el resultado de la snmpwalk con view en su lugar. Esta configuración define una vista que deniega el acceso SNMP para la tabla del Protocolo de resolución de direcciones (ARP) (atEntry) y lo permite para MIB-II y MIB privado de 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 es el comando y el resultado para el 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 es el comando y el resultado para el grupo local 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 es el comando y el resultado para la tabla ARP MIB-II:

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

Configuración de comunidad de SNMP con lista de acceso

Las prácticas recomendadas actuales recomiendan aplicar listas de control de acceso (ACL) a las cadenas de comunidad y asegurarse de que las cadenas de comunidad de solicitudes no sean idénticas a las cadenas de comunidad de notificaciones. Las listas de acceso proporcionan una mayor protección cuando se utilizan en combinación con otras medidas de protección.

Este ejemplo configura la ACL en una cadena de comunidad:

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Cuando se utilizan diferentes cadenas de comunidad para solicitudes y mensajes de trampa, se reduce la probabilidad de nuevos ataques o riesgos si la cadena de comunidad es descubierta por un atacante. De lo contrario, un atacante podría poner en peligro un dispositivo remoto o detectar un mensaje de trampa de la red sin autorización.

Una vez que habilita la trampa con una cadena de comunidad, la cadena se puede habilitar para el acceso SNMP en algún software del IOS de Cisco. Debe deshabilitar explícitamente esta comunidad. Por ejemplo:

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

Configurar SNMP Versión 3

La versión 3 de SNMP se introdujo por primera vez en la versión 12.0 del software del IOS de Cisco, pero todavía no se usa comúnmente en la administración de redes. Siga estos pasos para configurar la versión 3 de SNMP:

1. Asigne un ID de motor para la entidad SNMP (opcional).
2. Defina un usuario, **userone** que pertenezca al grupo **grouphone** y aplique **noAuthentication** (sin contraseña) y **noPrivacy** (sin cifrado) a este usuario.
3. Defina un usuario, **usertwo ;**que pertenezca al grupo **grouptwo** y aplique **noAuthentication** (sin contraseña) y **noPrivacy** (sin cifrado) a este usuario.
4. Defina un usuario, **userthree** que pertenezca al grupo **groupthree** y aplique la autenticación (la contraseña es user3passwd) y **noPrivacy** (sin cifrado) a este usuario.
5. Defina un usuario, **userfour**, que pertenezca al grupo **groupfour** y aplique la **autenticación** (la contraseña es user4passwd) y la **privacidad** (cifrado des56) a este usuario.
6. Defina un grupo, **groupone**, mediante el Modelo de seguridad del usuario (USM) V3 y habilite el acceso de lectura en la vista **v1default** (predeterminada).
7. Defina un grupo, **grupo dos**, mediante USM V3 y habilite el acceso de lectura en la vista **myview** .
8. Defina un grupo, el **grupo tres**, mediante USM V3, y habilite el acceso de lectura en la vista **v1default** (el valor predeterminado), mediante la **autenticación** .
9. Defina un grupo, **groupfour**, mediante USM V3, y habilite el acceso de lectura en la vista **v1default** (la predeterminada), mediante **Authentication** y **Privacy** .
10. Defina una vista, **myview**, que proporcione acceso de lectura en la MIB-II y deniegue el acceso de lectura en la MIB de Cisco privada.show running El resultado proporciona líneas adicionales para el grupo **public**, debido al hecho de que hay una cadena de comunidad Read-Only **public** que se ha definido.show running el resultado no muestra el **userthree**.

Ejemplo:

```
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 es el comando y el resultado para el grupo de sistema MIB-II con el usuario **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 es el comando y el resultado para el grupo de sistema MIB-II con el usuario **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 es el comando y el resultado para el grupo de Cisco Local System con el usuario **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 es el comando y el resultado que muestra que no puede obtener el grupo Sistema local de Cisco con el usuario **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 %
```

Este comando y el resultado de salida son para una **tcpdump** (parche para SNMP versión 3 y apéndice 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
```

Configuración de ACL en interfaces

La función ACL proporciona medidas de seguridad que previenen ataques como la suplantación de IP. La ACL puede aplicarse en interfaces entrantes o salientes en routers.

En las plataformas que no tienen la opción de utilizar ACL de recepción (rACL), es posible permitir el tráfico UDP (protocolo de datagramas de usuario) al router desde direcciones IP fiables con ACL de interfaz.

La siguiente lista de acceso ampliada se puede adaptar a su red. Este ejemplo asume que el router tiene las direcciones IP 192.168.10.1 y 172.16.1.1 configuradas en sus interfaces, que todo el acceso SNMP debe restringirse a una estación de administración con la dirección IP 10.1.1.1 y que la estación de administración sólo necesita comunicarse con la dirección IP 192.168.10.1:

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

access-list A continuación, se debe aplicar a todas las interfaces con estos comandos de configuración:

```
interface ethernet 0/0

ip access-group 101 in
```

Todos los dispositivos que se comunican directamente con el router en los puertos UDP deben estar enumerados específicamente en la lista de acceso anterior. El software Cisco IOS utiliza puertos en el rango de 49152 a 65535 como el puerto de origen para las sesiones salientes como las consultas del Sistema de nombres de dominio (DNS).

Para dispositivos que tienen muchas direcciones IP configuradas o muchos hosts que necesitan comunicarse con el router, esta no siempre es una solución escalable.

rACL

Para las plataformas distribuidas, las rACL pueden ser una opción que comience en la versión 12.0(21)S2 del software del IOS de Cisco para el router de switch Gigabit (GSR) de la serie 12000 de Cisco y la versión 12.0(24)S para la serie 7500 de Cisco. Las listas de acceso de recepción protegen al dispositivo del tráfico dañino antes de que el tráfico pueda afectar al procesador de ruta. Las ACL de ruta de recepción también se consideran una práctica recomendada de seguridad de la red y deben considerarse como una adición a largo plazo a una buena seguridad de la red, así como una solución alternativa para esta vulnerabilidad específica. La carga de la CPU se distribuye a los procesadores de tarjetas de línea y ayuda a mitigar la carga en el procesador de ruta principal. El informe técnico titulado GSR: Listas de control de acceso de recepción ayuda a identificar el tráfico legítimo. Utilice ese informe técnico para comprender cómo enviar tráfico legítimo a su dispositivo y también para denegar todos los paquetes no deseados.

ACL de Infraestructura

Aunque a menudo resulta difícil bloquear el tráfico que transita por la red, es posible identificar el

tráfico que nunca debe estar dirigido a los dispositivos de infraestructura y bloquear dicho tráfico en el borde de la red. Las ACL de infraestructura (iACL) se consideran una práctica recomendada de seguridad de la red y deben considerarse como una adición a largo plazo a una buena seguridad de la red, así como una solución alternativa para esta vulnerabilidad específica. El informe técnico Protecting Your Core: Infrastructure Protection Access Control Lists, presenta directrices y técnicas de implementación recomendadas para iACL.

Función Cisco Catalyst LAN Switch Security

La característica de la lista de IP permitidas restringe el acceso entrante de SNMP y Telnet al switch a direcciones IP de origen no autorizadas. Se admiten mensajes de Syslog y notificaciones de trampa SNMP para notificar a un sistema de administración cuando ocurre una violación o acceso no autorizado.

Se puede utilizar una combinación de las funciones de seguridad del software Cisco IOS para administrar routers y switches Cisco Catalyst. Es necesario establecer una política de seguridad que limite el número de estaciones de administración que pueden acceder a los switches y routers.

Para obtener más información sobre cómo aumentar la seguridad en redes IP, consulte Aumento de la seguridad en redes IP.

Cómo verificar errores SNMP

Configure las ACL de comunidad SNMP con el **log** palabra clave. Monitor **syslog** para intentos fallidos, como se muestra a continuación.

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

Cuando alguien intenta acceder al router con el público de la comunidad, aparece un syslog similar a esto:

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

Esta salida significa que la lista de acceso 10 ha denegado cinco paquetes SNMP del host 172.16.1.1.

Verifique periódicamente el SNMP en busca de errores con el show snmp , como se muestra aquí:

```
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 los contadores marcados con ** para ver aumentos inesperados en las tasas de error que pueden indicar intentos de aprovechamiento de estas vulnerabilidades. Para notificar cualquier problema de seguridad, consulte Respuesta ante incidentes de seguridad de productos de Cisco.

Información Relacionada

- Vulnerabilidades SNMP de los avisos de seguridad de Cisco
- Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).