Implementación de la mejora de las características ASA SNMP

Contenido

Introducción

Este documento describe las nuevas características del Simple Network Management Protocol (SNMP) que están disponibles para el Firewall adaptante de las 5500-X Series del dispositivo de seguridad de Cisco (ASA) en el Software Release 9.1.5 y las versiones 9.2.(1) y posterior.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Firewall de las 5500-X Series de Cisco ASA que funciona con el Software Release 9.1.5 del ® de Cisco ASA y libera 9.2.(1) y posterior.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

En las Versiones de ASA 9.1.5 y 9.2.1, se introducen estas mejoras SNMP:

- El soporte para los host 128 SNMP se agrega.
- Soporte para los identificadores de objeto del cpmCPUTotal5minRev SNMP (OID) se agrega.
- El soporte para los mensajes snmp 1,472-byte se agrega.

Soporte para los host 128 SNMP

Esta característica permite que el ASA soporte más que la corriente 32 host SNMP.

Propósito

Actualmente, el ASA tiene un límite duro de total de 32 host SNMP. Esto incluye los host que se pueden configurar para los desvíos y para sondear. Las siguientes secciones describen las influencias que esta característica tiene en los modos solos y del multi-contexto.

Modo del Solo-contexto

- Permite que un número perceptiblemente más elevado de las entradas (host totales) sea configurado, hacia arriba de 4,096. Sin embargo, fuera de estas entradas, solamente el 128 se puede utilizar para los desvíos.
- Para sondear los fines de la configuración, se permite a hasta 4,096 host y host trampa que sondean 128 ser configurado. Sin embargo, el número real de servidores que sondean el sistema se deben restringir menos que el 128, pues los impactos del rendimiento de un número más elevado de los host son desconocidos y no soportados.

Modo del Multi-contexto

- Para los fines de la configuración, hasta 4,000 host por el contexto se permiten y un límite sistema-ancho de 64,000 host totales se impone.
- Los host configurados total de los, solamente 128 (por el contexto) se pueden utilizar para los

desvíos, y el límite de general del sistema para los desvíos en el modo del multi-contexto son 32,000.

- Aunque usted pueda configurar hasta 4,000 host totales por el contexto, el número real de servidores que sondeen cualquier contexto se debe limitar al 128.

Descripción

Usted puede ser que prefiera monitorear los dispositivos de red de un pool grande de los host SNMP. Idealmente, usted quiere la capacidad de especificar un intervalo de direcciones IP y/o una subred de los IP Addresses que se permiten monitorear los dispositivos de red. El ASA no proporciona esa flexibilidad y limita actualmente los host del máximo SNMP a 32.

El soporte para esta característica implica dos aspectos:

- Proporcione la capacidad para que el ASA dirija hasta los host 128 SNMP.

- Proporcione los comandos required configuration de modo que usted pueda configurar un número perceptiblemente más elevado de los host, como se detalla en la sección anterior vía un comando único.

El diseño actual en el ASA es tal que los host individuales pueden ser configurados vía el CLI. Para esta característica, estos requisitos de diseño adicionales eran considerados:

- La introducción del comando CLI del host-**grupo del SNMP-servidor** con la retención del comando CLI del **host del SNMP-servidor**.

- La capacidad para que entradas vengan del host-**grupo del SNMP-servidor** y de los comandos CLI del **host del SNMP-servidor**.

- Para el SNMP versión 3, la introducción del comando CLI del **userlist del SNMP-servidor** con la retención del comando CLI del **usuario del SNMP-servidor**.

- Una coincidencia de la configuración debe también ser soportada. Por ejemplo, los comandos múltiples del host-**grupo** se pueden dar con los host que solapan en los objetos de red. Semejantemente, usted puede especificar un host con una dirección IP que solape con los host actuales o el grupo del host. Esto proporciona un mecanismo que se pueda utilizar para sobregrabar los parámetros para algunos host en un grupo, sin la necesidad de configurar de nuevo al grupo completo.

Algunas restricciones del software y advertencias que se asocian a esta característica son:

- Como parte del comando del host-**grupo del SNMP-servidor**, el valor por defecto es **encuesta** si **[desvío|la encuesta]** no se especifica. Es también importante observar que para este comando, los desvíos y la interrogación no se pueden habilitar para el mismo grupo del host. Si se requiere esto, Cisco recomienda que usted utiliza el **comando snmp-server host** para los host relevantes.

- Usted puede especificar los objetos de red que solapan en diversos comandos del host-**grupo**. Los valores que se especifican en el grupo más reciente del host toman el efecto para

el conjunto común de host en los diversos objetos de red.

Aquí tiene un ejemplo:

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

Ingrese el **comando snmp-server host de la demostración** para ver las entradas de host:

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

Aquí están algunas NOTAS IMPORTANTES sobre el uso de esta característica:

- Si borran a un grupo del host o a un host que solapan con otros grupos del host, los host se configuran otra vez con los valores que se utilizan para los grupos configurados del host.
- Los valores o los parámetros que se asocian a los host son dependientes sobre la orden que los comandos están ejecutados.
- La lista de usuario se configura que no puede ser borrada si la lista es utilizada por un grupo del host determinado.
- El usuario SNMP no puede ser borrado si refieren al usuario en una lista de usuario determinado.
- Un objeto de red no puede ser borrado si es utilizado por el comando CLI del host-**grupo**.

Configurar

Utilice la información que se describe en esta sección para configurar el ASA para implementar esta nueva función.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Comandos CLI

Para el SNMP versión 3, el administrador puede asociar a los diversos usuarios a un grupo especificado de host. Esto es útil si el administrador quisiera que un conjunto de los usuarios tuviera la capacidad de acceder el ASA de un grupo de host. Utilizan a este comando CLI para configurar una lista de usuario para los usuarios múltiples:

```
ASA(config)# [no] snmp-server user-list <list_name> username <user_name>
```

Para asociar la lista de usuario a un grupo del host, ingrese este comando en el CLI:

```
[no] snmp-server host-group <interface> <network-object> [trap|poll]
[community [enc_type] <text>] [version {1 | 2c | 3 [user name | user-list
<list-name>]}] [udp-port <port_number>]
```

Con este comando único, usted puede especificar un objeto de red para indicar los host múltiples que deben ser agregados. Con el objeto de red, usted puede especificar una máscara de subred o el rango de los IP Addresses que debe ser agregado, con el uso de un comando único. Todos los IP Addresses que se enumera como parte del objeto de red se agregan como entradas de host SNMP. Semejantemente, para cada uno de los usuarios que se especifican en la lista de usuario, hay una entrada de host separada SNMP.

Estos comandos se utilizan para permitir que los administradores borren y que vean las nuevas opciones de configuración para los servidores SNMP:

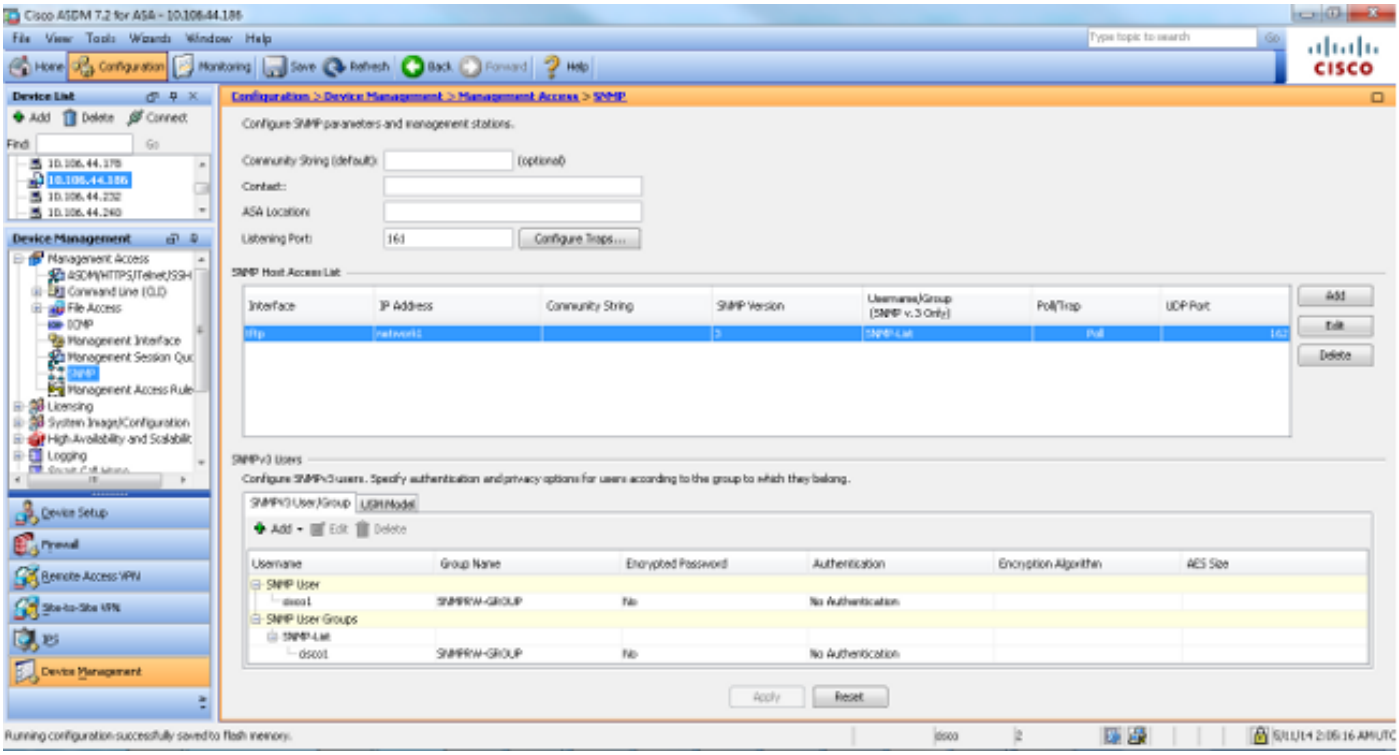
- **borre la lista de usuario del SNMP-servidor de la configuración**
- **borre el host-grupo del SNMP-servidor de la configuración**
- **muestre la lista de usuario del SNMP-servidor de los ejecutar-config**
- **muestre el host-grupo del SNMP-servidor de los ejecutar-config**

Ejemplo de configuración

Complete estos pasos para utilizar las nuevas opciones del grupo SNMP y crear un grupo del host del servidor SNMP para la interrogación de la versión 2c:

1. Cree un objeto de red:
   ```
   asa(config)# object network network1
   asa(config-network-object)# range 64.103.236.40 64.103.236.50
   ```
2. Defina el grupo del host SNMP:
   ```
   asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
   ```
3. Defina el grupo del SNMP versión 3:
   ```
   asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
   ```
4. Ate a los grupos a los usuarios:
   ```
   asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
   asa(config)#snmp-server user-list SNMP-List username cisco1
   asa(config)#snmp-server host-group inside network1 poll version 3 user-list SNMP-List
   ```

Esta imagen ilustra los cambios que se realizan dentro del Cisco Adaptive Security Device Manager (ASDM):



Soporte para el cpmCPUTotal5minRev SNMP OID

Esta característica permite que el ASA soporte el **cpmCPUTotal5minRev** SNMP OID.

Propósito

Esta característica agrega el soporte para el **cpmCPUTotal5minRev** y el **cpmCPUTotal1minRev** OID en el ASA y desaprueba el **cpmCPUTotal5min** OID y el **cpmCPUTotal1min** soportado actualmente. El propósito de estos OID es monitorear el USO de la CPU. Los OID soportado actualmente se extienden a partir de la 1 a 100, mientras que los OID nuevo-soportados se extienden a partir de la 0 a 100. Por lo tanto, el soporte fue agregado para OID más nuevos, como cubren una gama más amplia.

Es importante observar que puesto que se actualizan los OID desaprobados (**cpmCPUTotal5min** y **cpmCPUTotal1min**) se soportan no más en el ASA, si el ASA y se sondean los OID desaprobados, el ASA no devuelve ninguna información para esos OID. Después de que una actualización del ASA, usted ahora se requiera monitorear el **cpmCPUTotal5minRev** y el **cpmCPUTotal1minRev** para el USO de la CPU.

Comandos CLI

No hay cambios CLI introducidos con esta nueva función.

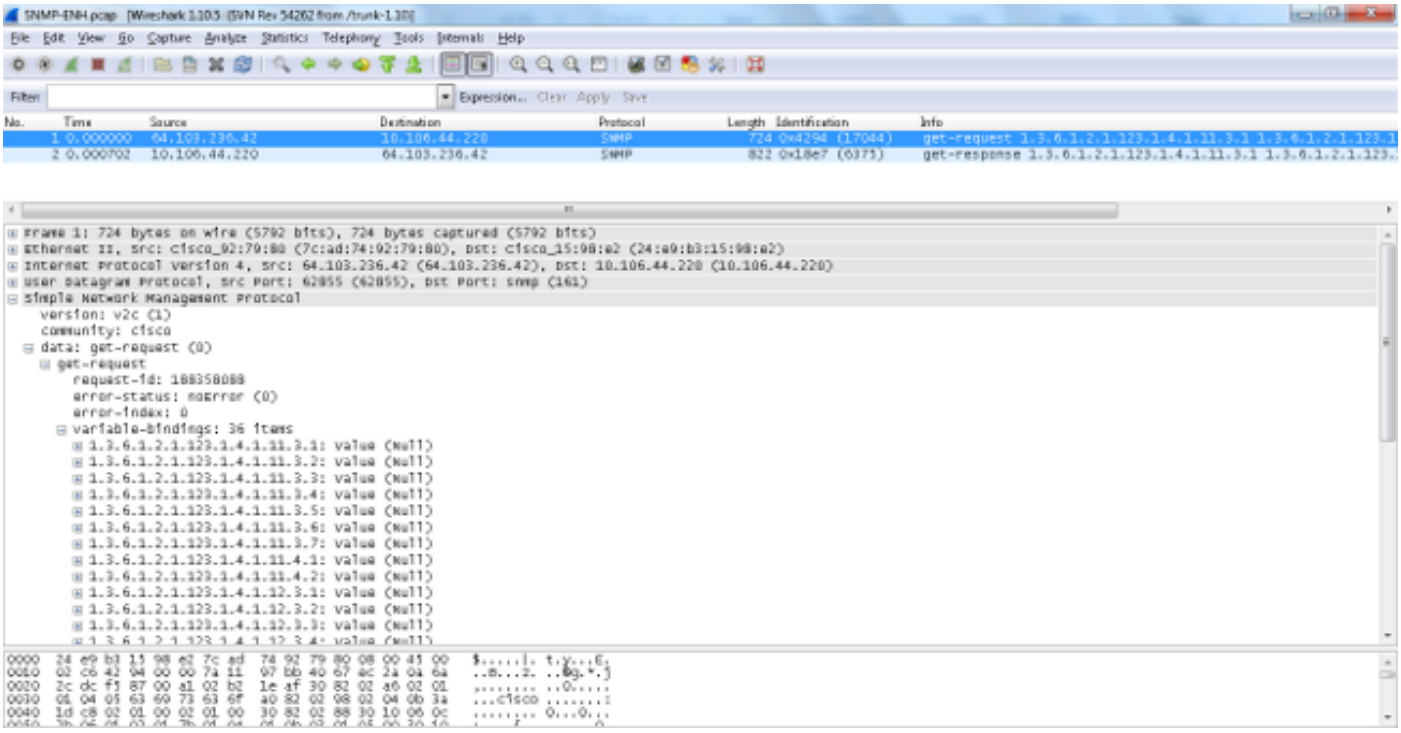
Nuevos OID

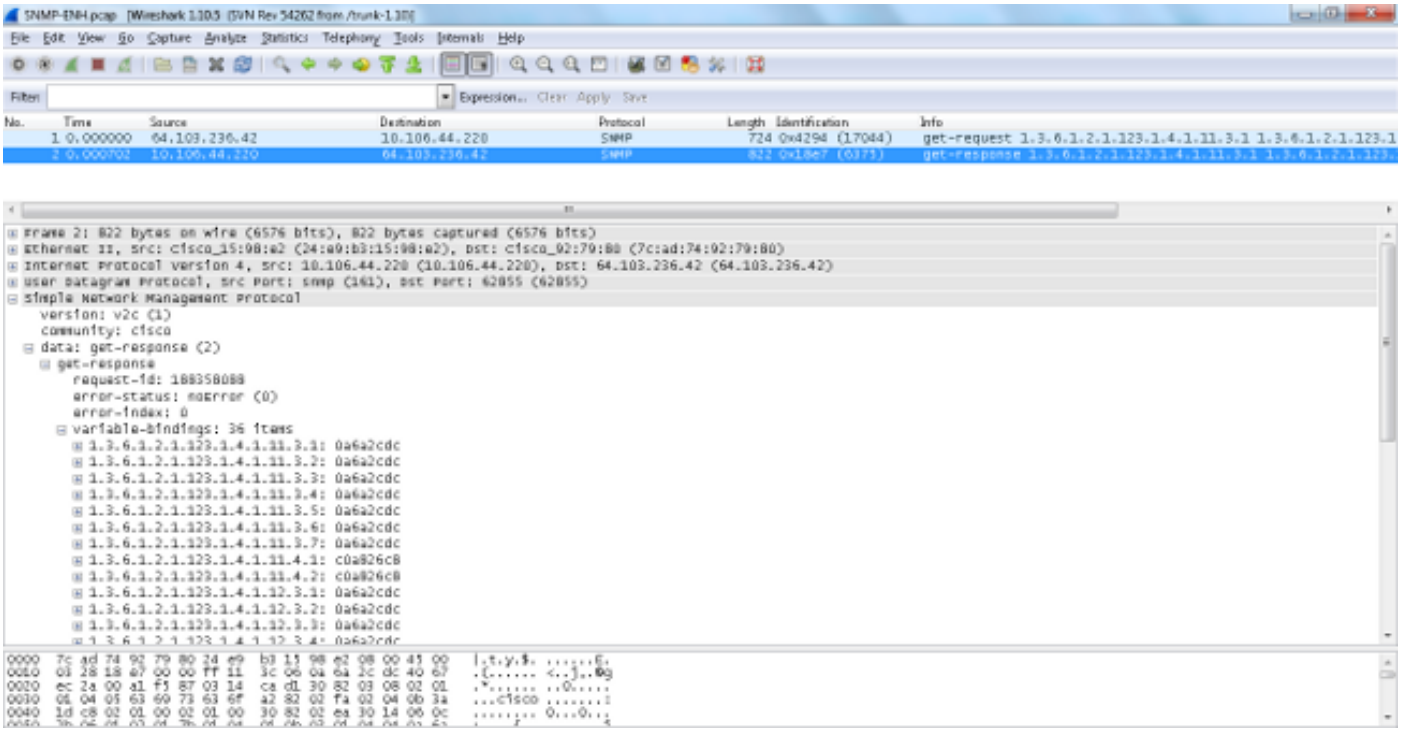
Éstos son los nuevos OID que se agregan con esta característica:

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

Soporte para los mensajes snmp 1,472-Byte

Las Plataformas ASA limitan el tamaño máximo de paquete para las peticiones SNMP a 512 bytes. Cuando usted realiza una interrogación a granel para un gran número de MIB OID dentro de una sola petición SNMP, los time-out de Conexión SNMP y un Syslog del error se genera en el ASA. El RFC3417 sugiere que el tamaño máximo de paquete para las peticiones SNMP sea 1,472 bytes. Éste es el tamaño del payload SNMP para el paquete. Además, el encabezado Ethernet y el tamaño del encabezado IP se deben agregar para computar el tamaño total del paquete.





Nota: Soportan el solo-contexto y a los modos de contexto múltiple con esta característica.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas los problemas del sistema en el ASA.

Comandos show

Estos **comandos show** pueden ser útiles cuando las tentativas se hacen para resolver problemas los problemas en el ASA:

- **host-grupo del SNMP-servidor del funcionamiento de la demostración del** asa# host-grupo del SNMP-servidor dentro de la SNMP-lista de la lista de usuario de la versión 3 de la encuesta network1

- **lista de usuario del SNMP-servidor del funcionamiento de la demostración del** asa# nombre de usuario cisco1 de la SNMP-lista de la lista de usuario del SNMP-servidor

- **host del SNMP-servidor de la demostración del** asa#

Este comando CLI visualiza las entradas que están presentes en la tabla de direcciones del servidor SNMP, que incluye el host y las configuraciones de grupo del host:

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
object network network3
range 64.103.236.60 64.103.236.70 ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

Como se muestra, estos comandos show todos los host que se configuran vía el comando del host-**grupo**. Usted puede utilizar este comando para verificar si todas las entradas están disponibles y también cruz-verificar los grupos del host que solapan.