Seguridad de la dirección IP y de cable source-verify

Contenido

Introducción
Antes de comenzar
Convenciones
prerrequisitos
Componentes Utilizados
El entorno DOCSIS sin protección
Base de datos CMTS CPE
El comando cable source-verify
Ejemplo 1: escenario con direcciones IP duplicadas
Ejemplo 2: escenario con dirección IP duplicada – Utilización de una dirección IP que aún no se haya usado.
Ejemplo 3: uso de un número de red no suministrado por el proveedor de servicio
Cómo configurar el cable Source-Verify
Agente Relay
Conclusión
Información Relacionada

Introducción

Cisco ha incorporado mejoras en los productos Cisco Cable Modem Termination System (CMTS) que inhiben ciertos tipos de ataques de negación del servicio basados en la simulación de direcciones IP y robo de direcciones IP en los sistemas de cable de Data-over-Cable Service Interface Specifications (DOCSIS). **Este documento describe el conjunto de comandos cable source-verify que forman parte de esas mejoras de seguridad para las direcciones IP.**

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

El entorno DOCSIS sin protección

Un dominio de Control de acceso de medios (MAC) de DOCSIS es similar en su naturaleza a un segmento Ethernet. Si se deja desprotegido, los usuarios en el segmento son vulnerables a muchos tipos de ataques de Negación de servicio basados en el direccionamiento de Capa 2 y Capa 3. Además, es posible que los usuarios sufran un nivel degradado de servicio debido al malconfiguration de la dirección en el equipo del otro usuario. Los ejemplos de esto incluyen:

- Configuración de direcciones IP duplicadas en nodos diferentes.
- Configurar los MAC Address duplicado en diversos Nodos.
- Uso no autorizado de direcciones IP estáticas en lugar de direcciones IP asignadas por el Protocolo de configuración de host dinámico (DHCP).
- El uso no autorizado de los distintos números de redes dentro de un segmento.
- Una configuración incorrecta de los nodos extremos para responder las peticiones ARP en nombre de la porción del segmento de subred IP.

Mientras estos tipos de problemas son fáciles de controlar y mitigar en un entorno Ethernet LAN por medio de la localización física y la desconexión del equipo ofensivo, tales problemas en redes DOCSIS pueden ser más difíciles de aislar, resolver y prevenir debido al tamaño potencialmente grande de la red. Además, es posible que los usuarios finales que controlan y configuran el Equipo en las instalaciones del cliente (CPE) no cuenten con un equipo local de soporte IS que les asegure que sus estaciones de trabajo y PC no estén mal configuradas, ya sea intencionalmente o no.

Base de datos CMTS CPE

La familia de productos CMTS de Cisco mantiene una base de datos interna que se completa dinámicamente con direcciones MAC e IP del CPE. La base de datos CPE también contiene detalles sobre los módems de cable correspondientes a los que pertenecen estos dispositivos CPE.

Puede obtenerse una vista parcial de la base de datos de CPE correspondiente a un cablemódem particular mediante la ejecución del comando CMTS oculto show interface cable X/Y modem Z. Aquí, X es el número de tarjeta de línea, Y es el número de puerto de flujo descendente y Z es el identificador de servicio (SID) del cable módem. Z se puede fijar a 0 para ver los detalles sobre todo el Cable módems y el CPE en una interfaz del flujo descendente particular. El siguiente ejemplo muestra una salida típica generada por este comando.

```
CMTS# show interface cable 3/0 modem 0
SID   Priv bits  Type      State     IP address    method    MAC address
1     00         host      unknown   192.168.1.77  static    000C.422c.54d0 1     00
modem     up         10.1.1.30     dhcp      0001.9659.4447 2     00         host      unknown
192.168.1.90  dhcp      00a1.52c9.75ad 2     00         modem     up         10.1.1.44
dhcp      0090.9607.3831
```

Nota: Puesto que se oculta este comando, está conforme al cambio y no se garantiza para estar disponible en todas las versiones del software de Cisco IOS®.

En el ejemplo anterior, enumeran a la columna del método del host con la dirección IP 192.168.1.90 como DHCP. Esto significa que CMTS se enteró de este host observando las transacciones DHCP entre el host y el servidor DHCP del proveedor de servicios.

El host con dirección IP 192.168.1.77 se lista con método estático. Esto significa que el CMTS primero no aprendió de este host vía una transacción DHCP entre este dispositivo y un servidor DHCP. En su lugar, el CMTS primero detectó otros tipos de tráfico IP desde este host. Este tráfico pudo haber sido navegador de páginas de internet, correo electrónico o paquetes “ping”.

Mientras puede parecer que 192.168.77 ha sido configurado con una dirección IP estática, puede ser que este host haya adquirido un arrendamiento de DHCP pero el CMTS pudo haber sido reiniciado desde el evento y, por lo tanto, no recuerda la transacción.

La base de datos CPE normalmente está compuesta por información de recolección CMTS sobre las transacciones DHCP entre dispositivos CPE y el servidor DHCP del proveedor del servicio. Además, el CMTS es capaz de escuchar otro tráfico IP proveniente de dispositivos de CPE a fin de determinar qué direcciones MAC e IP de CPE pertenecen a los distintos cablemódems.

El comando cable source-verify

Cisco ha implementado el comando interfaz del cable: cable source-verify [dhcp]. Este comando hace que el CMTS utilice la base de datos de CPE para verificar la validez de los paquetes IP que recibe el CMTS en sus interfaces de cable y permite que el CMTS tome decisiones inteligentes respecto a reenviarlos o no.

El siguiente diagrama de flujo muestra el procesamiento extra que debe atravesar un paquete IP recibido en una interfaz de cable antes de ser admitido a través del CMTS.

Diagrama de flujo 1

El diagrama de flujo comienza con un paquete recibido por un puerto ascendente en el CMTS y termina con el paquete ya sea habiéndosele permitido continuar para continuar el procesamiento, o bien habiéndose perdido.

Ejemplo 1: escenario con direcciones IP duplicadas

El primer escenario de Negación de servicio que trataremos es la situación que incluye direcciones IP duplicadas. Digamos que un cliente A está conectado a su proveedor de servicios y obtuvo una licencia DHCP válida para su PC. Conocerán al cliente de la dirección IP que A ha obtenido como X.

Después de que A adquiere su arrendamiento DHCP, el cliente B decide configurar su PC con una dirección IP estática que es la misma que la que está usando el equipo del cliente A. La información de base de datos CPE con respecto a la dirección IP X cambiaría dependiendo de qué último del dispositivo CPE envió un pedido ARP en nombre del X.

En una red DOCSIS desprotegida, es posible que el cliente B esté en condiciones de convencer al router de saltos (en la mayoría de los casos, el CMTS) que tiene derecho a usar la dirección de IP X, simplemente mediante el envío de una solicitud ARP a nombre de X al CMTS o al router de saltos siguiente. De esta manera, se detendría el reenvío del tráfico del proveedor de servicios al Cliente A.

Habilitando el cable fuente-verifique, el CMTS podría ver que el IP y los paquetes ARP para el IP Address X eran originados del cablemódem incorrecto y por lo tanto, estos paquetes sería caído, ve el organigrama 2. Esto incluye todos los paquetes del IP con la dirección de origen X y los pedidos ARP en nombre del X. Los registros CMTS mostrarían un mensaje a lo largo de las líneas de:

%UBR7200-3-BADIPSOURCE: Interfaz Cable3/0, paquete del IP del origen no válido. IP=192.168.1.10, MAC=0001.422c.54d0, SID esperado=10, SID real=11

Organigrama 2

Mediante esta información se identifica a ambos clientes y se puede desactivar el cable módem con la dirección IP duplicada conectada.

Ejemplo 2: escenario con dirección IP duplicada – Utilización de una dirección IP que aún no se haya usado.

Otro escenario está para que un usuario asigne estáticamente hasta ahora una dirección IP inusitada a su PC que baje dentro del rango legítimo de los direccionamientos del CPE. Este escenario no causa ninguna interrupción de servicios a nadie en la red. Digamos que el cliente B ha asignado la dirección Y para su PC.

El problema siguiente que puede presentarse es ese cliente que el C pudo conectar su puesto de trabajo con la red de proveedor de servicio y que adquiere un arriendo del DHCP para la dirección IP Y. La base de datos CPE marcaría temporalmente la dirección IP Y como perteneciendo detrás del módem de cable del cliente c. Sin embargo, puede ser que no esté mucho antes de que el cliente B, el usuario NON-legítimo envía la secuencia apropiada de tráfico ARP para convencer el Next-Hop que él era el propietario legítimo de la dirección IP Y, por lo tanto causando una interrupción al servicio del cliente c.

Semejantemente, el segundo problema se puede solucionar girando el **cable fuente-verifica**. Cuando el cable de verificación de fuente está encendido, una entrada de base de datos CPE que se ha generado recogiendo detalles de una transacción DHCP no puede ser desplazada por otras clases de tráfico IP. Solamente otra transacción DHCP para esa dirección IP o la entrada ARP en el CMTS que mide el tiempo hacia fuera para esa dirección IP puede desplazar la entrada. Esto se asegura de que si un usuario final adquiere con éxito un arriendo del DHCP para una dirección IP dada, ese cliente no tenga que preocuparse del CMTS confuso y que piensa que su dirección IP pertenece a otro usuario.

El primer problema de los usuarios cesantes de usar hasta ahora los IP Addresses inusitados se puede solucionar con el **cable fuente-verifica el DHCP**. Agregando el parámetro DHCP al final de este comando, el CMTS puede marcar la validez de cada nueva dirección IP de origen que oye alrededor publicando un tipo especial de mensaje DHCP llamado un LEASEQUERY al servidor DHCP. Vea el diagrama de flujo 3.

Organigrama 3

Para una dirección IP de CPE determinada, el mensaje LEASEQUERY consulta cuáles son las direcciones MAC y de Cable Módem correspondientes. Para obtener más detalles, consulte el Mensaje DHCPLEASEQUERY.

En esta situación, si el cliente B conecta su estación de trabajo a la red de cables con la dirección

estática Y, el CMTS enviará una LEASEQUERY (consulta sobre arrendamiento) al servidor DHCP para verificar si la dirección Y ha sido arrendada a la PC del cliente B. El servidor DHCP puede informarle al CMTS que no se ha otorgado ningún arrendamiento a la dirección IP Y y que, por lo tanto, se le denegará el acceso al cliente B.

Ejemplo 3: uso de un número de red no suministrado por el proveedor de servicio

Los usuarios pueden tener estaciones de trabajo configuradas detrás de sus cable módems con direcciones IP estáticas que no pueden entrar en conflicto con ninguno de los números de red actuales del proveedor de servicio, pero pueden ocasionar problemas en un futuro. Por lo tanto, al utilizar el cable de verificación de fuente, un CMTS puede filtrar paquetes que vienen de direcciones IP de origen que no pertenecen al rango configurado en la interfaz del cable CMTS.

Nota: Para que esto trabaje correctamente, usted también necesita configurar el **comando ip verify unicast reverse-path** para prevenir los IP Source Address del spoofed. Refiera a los comandos del cable: telegrafíe s para más información.

Algunos clientes pueden tener un router como un dispositivo CPE y acordar que el proveedor del servicio enrute el tráfico a este router. Si el CMTS recibe tráfico IP del router CPE con una dirección IP de origen de Z, entonces cable source-verify dejará pasar este paquete siempre y cuando el CMTS posea una ruta que hacia la red a la que pertenezca Z vía ese dispositivo CPE. Consulte el Diagrama de flujo 3.

Ahora considere el siguiente ejemplo:

Aparece la siguiente configuración en CMTS:

```
interface cable 3/0
 ip verify unicast reverse-path
 ip address 10.1.1.1 255.255.255.0
 ip address 24.1.1.1 255.255.255.0 secondary
 cable source-verify
!
ip route 24.2.2.0 255.255.255.0 24.1.1.2
```

Note: This configuration shows only what is relevant for this example

Si se asume que un paquete con la dirección IP de origen 172.16.1.10 llegó el CMTS del módem de cable 24.2.2.10, el CMTS vería que 24.2.2.10 no reside en la base de datos CPE, el **módem 0 del x/y del cable de la demostración internacional**, no obstante el **IP verifica el** Unicast Reverse Path Forwarding de los permisos del **trayecto inverso del unicast** (unicast RPF), que marca cada paquete recibido en una interfaz para verificar que la dirección IP de origen del paquete aparece en las tablas de ruteo que pertenece a esa interfaz. **El cable fuente-verifica los** controles para ver cuáles es el salto siguiente para 24.2.2.10. En la configuración anterior tenemos una ruta ip 24.2.2.0 255.255.255.0 24.1.1.2 lo que significa que el siguiente salto es 24.1.1.2. Ahora al asumir que 24.1.1.2 es una entrada válida en la base de datos CPE, el CMTS determina que el paquete está bien y entonces lo procesará de acuerdo con el diagrama de flujo 4.

Organigrama 4

Cómo configurar el cable Source-Verify

Configurando el **cable fuente-verifique** implica simplemente el agregar del **comando cable source-verify a la** interfaz del cable que usted quisiera activar la función encendido. Si usted está

utilizando los Paquetes de interfaces de cableado, después usted necesita agregar el **cable fuente-verifica a la** configuración de la interfaz principal.

Cómo configurar el `cable fuente-verifique el DHCP`

Nota: el cable fuente-verifica primero fue introducido en el Cisco IOS Software Release 12.0(7)T y se soporta en los Cisco IOS Software Release 12.0SC, 12.1EC y 12.1T.

La configuración de cable source-verify dhcp requiere algunos pasos.

Asegúrese de que su servidor DHCP admita el mensaje DHCP LEASEQUERY especial.

Para hacer uso del **cable fuente-para verificar las** funciones **DHCP**, su servidor DHCP debe contestar a los mensajes según lo especificado por draft-ietf-dhcp-leasequery-XX.txt. Las versiones registrares de la red de Cisco 3.5 y arriba pueden contestar a este mensaje.

Aseegurese que su servidor DHCP soporta el proceso de la opción de información de agente de relé. Vea por favor estas instrucciones.

Otra función que su servidor DHCP debe admitir es el procesamiento con Opción de información de relé DHCP. Esto se conoce de otra manera como opción 82 que procesa. Esta opción se describe en Opción de información de relé DHCP (RFC 3046). Las versión de Cisco Network Registrar 3.5 y posteriores soportan el procesamiento de Opción de información del agente de relevo, sin embargo debe ser activado mediante la utilidad de línea de comandos nrcmd de Cisco Network Registrar con la siguiente secuencia de comandos:

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp enable save-relay-agent-data

nrcmd - U admin - Changeme P - Salvaguardia de 127.0.0.1 del C

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp reload

Es posible que deba sustituir el nombre del usuario, la contraseña y la dirección IP correspondientes del servidor, anteriormente se muestran los valores predeterminados. Alternativamente, si usted está en el prompt del nrcmd, >nrcmd usted apenas teclea el siguiente:

permiso salvaguardia-retransmisión-agente-DATA DHCP

guardar

recarga DHCP

Active el procesamiento de la opción de información de relé DHCP en el CMTS.

Agente Relay

El CMTS debe marcar los pedidos de DHCP con etiqueta del Cable módems y el CPE con la opción de información de agente de relé para que el **cable fuente-verifica el DHCP** para ser eficaz. Los siguientes comandos deben ser ingresados en el modo de configuración global en los Cisco IOS Software Release 12.1EC corrientes CMTS, 12.1T o versiones posteriores del Cisco IOS.

Opción ip dhcp relay information

Si su CMTS ejecuta la versión 12.0SC de software del IOS de Cisco capacite al IOS de Cisco y ejecute el comando cable relay-agent-option cable interface en su lugar.

Tenga cuidado de utilizar los comandos apropiados, dependiendo de la versión del Cisco IOS que usted está funcionando con. Aseegurese poner al día su configuración si usted transborda trenes del Cisco IOS.

Los comandos relay information option agregan una opción especial llamada Opción 82, o la opción de información de relé, al paquete DHCP transmitido cuando CMTS transmite paquetes DHCP.

La opción 82 contiene una subopción, la ID del circuito del agente, que hace referencia a la interfaz física en el CMTS en el cual se oyó el pedido de DHCP. Además de esto, otra subopción, el ID remoto del agente, se completa con la dirección MAC de 6 bytes del cable módem del que se recibió o por el que pasó la petición DHCP.

Así pues, por ejemplo, si un PC con la dirección MAC 99:88:77:66:55:44 que está detrás del módem de cable aa: bb: cc: DD: ee: el FF envía un pedido de DHCP, el CMTS remitirá el pedido de DHCP que fija el submarino option del ID del agente remoto de la opción 82 a la dirección MAC del módem de cable, aa: bb: cc: DD: ee: FF.

Al tener la opción de información de relé incluida dentro de la solicitud DHCP de un dispositivo CPE, el servidor DHCP puede almacenar información acerca de cuál CPE debe ubicarse detrás de cuál cablemódem. Es especialmente útil cuando el comando cable source-verify dhcp está configurado en el CMTS, dado que el servidor DHCP puede enviar información en forma confiable al CMTS sobre qué dirección MAC tiene un cliente en particular y a qué cliente de cablemódem debería estar conectado.

Habilitar el comando cable source-verify dhcp bajo la interfaz de cable apropiada.

El paso final es ingresar el comando cable source-verify dhcp en la interfaz del cable en la cual se desea activar la función. Si el CMTS está utilizando los Paquetes de interfaces de cableado entonces usted debe ingresar el comando bajo el conjunto principal interconecta.

Conclusión

El cable source-verify suites de los comandos permite que un proveedor servicio proteja la red del cable contra usuarios con direcciones IP no autorizadas para usar la red.

El comando cable source-verify en sí mismo constituye una forma eficaz y simple de implementar la seguridad de la dirección IP. Si bien no cubre todos los escenarios, al menos garantiza que los clientes que tienen derecho a utilizar direcciones de IP asignadas no detecten ninguna interrupción cuando otras personas utilizan sus direcciones de IP.

En su forma más simple según lo descrito en este documento, un dispositivo CPE no configurado vía el DHCP no puede obtener el acceso a la red. Ésta es la mejor manera de asegurar el espacio de IP Address y de aumentar la estabilidad y la confiabilidad de los datos sobre el servicio de cable. Sin embargo los operadores de servicio múltiple (MSO) que tienen los servicios comerciales que los requirieron utilizar a las direcciones estáticas quisieron implementar la Seguridad estricta del commandcable fuente-**verifican el DHCP**.

La versión registrar de la red de Cisco 5.5 tiene una nueva capacidad de la respuesta a la interrogación del arriendo para los direccionamientos “reservados”, aunque la dirección IP no fue obtenida vía el DHCP. El servidor DHCP incluye los datos de la reserva del arriendo en las respuestas DHCPLEASEQUERY. En las versiones anteriores de Network Registrar, las respuestas DHCPLEASEQUERY eran posibles sólo para clientes alquilados o previamente alquilados para los cuales se almacenó la dirección MAC. Los Agentes Relay del uBR de Cisco, por ejemplo, desechan los datagramas DHCPLEASEQUERY que no tienen una dirección MAC y un Tiempo de validez (opción del Dhcp-lease-time).

Network Registrar vuelve al tiempo de validez predeterminado de un año (31536000 segundos) para arriendos reservados en una respuesta DHCPLEASEQUERY. Si el direccionamiento se arrienda realmente, el network registrar vuelve su Tiempo de validez restante. Más características se pueden encontrar en la sección de los arriendos que pregunta de configurar los alcances de DHCP y los arriendos.

Información Relacionada

- Opción de información del relé DHCP (RFC 3046)
- Soporte Técnico y Documentación - Cisco Systems