ASA/PIX: Permiten tráfico de la red acceder Microsoft servidor de medios ()/vídeo de flujo continuo del MMS del ejemplo de configuración de Internet

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante (ASA) en la orden la permit el cliente o el usuario de Internet para acceder el servidor de medios de Microsoft (MMS) o el vídeo de flujo continuo colocó en la red interna del ASA.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Configuración básica del ASA
- El MMS se configura y trabaja correctamente

Componentes Utilizados

La información en este documento se basa en Cisco ASA que funciona con la versión de software 7.x 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.

Productos Relacionados

La información en este documento es también aplicable al Cisco PIX Firewall que funciona con la versión de software 7.x y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Información del Firewall para las 9 Series de los servicios de multimedios de Windows

Utilice los protocolos de los medios de flujo continuo

Aplicaciones de las 9 Series de los servicios del ® de los multimedios de Windows del Microsoft® dos protocolos de los medios de flujo continuo de entregar el contenido como flujo de datos de unidifusión a los clientes:

- Real-Time Streaming Protocol (RTSP)
- Protocolo del servidor de medios de Microsoft (MMS)

Estas acciones de control de cliente del soporte de los protocolos tales como parada, pausa, rebobinado, y archivos de multimedios de Windows puestos en un índice rápido-delanteros.

El RTSP es un Application Layer Protocol que fue creado específicamente para proporcionar la salida controlada de las informaciones en tiempo real, tales como contenido del audio y del vídeo. Usted puede utilizar el RTSP para fluir el contenido a los ordenadores que ejecutan Windows Media Player 9 Series o más adelante, a los clientes que utilizan el control del ® de Windows Media Player 9 Series ActiveX, o a otros ordenadores que funcionen con las 9 Series de los servicios de multimedios de Windows. El RTSP trabaja con el Real-Time Transport Protocol (RTP) para formatar los paquetes de contenido multimedia y para negociar el protocolo de capa de transporte más eficiente, User Datagram Protocol (UDP) o (TCP) del Control Protocol del transporte, para utilizar cuando usted entrega la secuencia a los clientes. Usted puede implementar el RTSP a través del enchufe del Control Protocol del servidor WM RTSP en el administrador de los servicios de multimedios de Windows. Este enchufe se habilita por abandono.

El MMS es un Application Layer Protocol propietario que fue desarrollado para las versiones anteriores de los servicios de multimedios de Windows. Usted puede utilizar el MMS para fluir el

contenido a los ordenadores que ejecutan Windows Media Player para el ® XP de Windows o anterior. Usted puede implementar el MMS a través del enchufe del Control Protocol del servidor del MMS WM en el administrador de los servicios de multimedios de Windows. Este enchufe se habilita por abandono.

Utilice el HTTP

Si los puertos en su Firewall no pueden ser abiertos, los servicios del ® de los multimedios de Windows pueden fluir el contenido con el HTTP sobre el puerto 80. El HTTP se puede utilizar para entregar las secuencias a todas las versiones de Windows Media Player. Usted puede implementar el HTTP a través del enchufe del Control Protocol del servidor HTTP WM en el administrador de los servicios de multimedios de Windows. Este enchufe no se habilita por abandono. Si otro servicio, tal como Servicios de Internet Information Server (IIS), utiliza el puerto 80 en la misma dirección IP, usted no puede habilitar el enchufe.

El HTTP se puede también utilizar para éstos:

- Distribuya las secuencias entre los servidores de los multimedios de Windows
- Contenido de la fuente de un codificador de los multimedios de Windows
- Listas de temas dinámicamente generadas de la descarga de un servidor Web

Los enchufes de la fuente de datos se deben configurar en el administrador de los servicios de multimedios de Windows para soportar este el HTTP adicional que fluye los escenarios.

Sobre la renovación del protocolo

Si los clientes que soportan el RTSP conectan con un servidor que dirija los servicios del ® de los multimedios de Windows con un apodo RTSP URL (por ejemplo, rtsp://) o un apodo del MMS URL (por ejemplo, mms://), el servidor utilizan la renovación del protocolo para fluir el contenido al cliente para proporcionar una experiencia que fluye óptima. La renovación automática del protocolo de RTSP/MMS al RTSP con los transportes basados en UDP o TCP basados (RTSPU o RTSPT), o aún el HTTP (si se habilita el enchufe del Control Protocol del servidor HTTP WM) puede ocurrir mientras que el servidor intenta negociar el mejor protocolo y proporcionar una experiencia que fluye óptima para el cliente. Los clientes que soportan el RTSP incluyen Windows Media Player 9 Series o más adelante o a otros jugadores que utilicen el control ActiveX de Windows Media Player 9 Series.

Las versiones anteriores de Windows Media Player, tal como Windows Media Player para Windows XP, no soportan el protocolo RTSP, pero el protocolo del MMS proporciona el soporte de la renovación del protocolo para estos clientes. Así, cuando una versión anterior del jugador intenta conectar con el servidor con un apodo del MMS URL, la renovación automática del protocolo del MMS con el MMS con los transportes basados en UDP o TCP basados (MMSU o MMST), o aún el HTTP (si se habilita el enchufe del Control Protocol del servidor HTTP WM), puede ocurrir mientras que el servidor intenta negociar el mejor protocolo y proporcionar una experiencia que fluye óptima para estos clientes.

Para aseegurarse que su contenido está disponible para todos los clientes que conecten con su servidor, los puertos en su Firewall se deben abrir para todos los protocolos de conexión que se puedan utilizar dentro de la renovación del protocolo.

Usted puede forzar su servidor de los multimedios de Windows para utilizar un protocolo específico si usted identifica el protocolo que se utilizará en el archivo del aviso (por ejemplo,

rtspu://server/publishing_point/file). Para proporcionar una experiencia que fluye óptima para todas las versiones de cliente, recomendamos que el uso URL el protocolo general del MMS. Si los clientes conectan con su secuencia con un URL con un apodo del MMS URL, cualquier renovación necesaria del protocolo ocurre automáticamente. Sea consciente que los usuarios pueden inhabilitar los Protocolos de transmisión en los valores de propiedades de Windows Media Player. Si un usuario inhabilita un protocolo, se salta dentro de la renovación. Por ejemplo, si se inhabilita el HTTP, los URL no ruedan encima al HTTP.

Afecte un aparato los puertos para los servicios de multimedios de Windows

La mayoría de los Firewall se utilizan para controlar el “tráfico entrante” al servidor; no controlan generalmente el “tráfico saliente” a los clientes. Los puertos en su Firewall para el tráfico saliente pueden ser cerrados si una política de seguridad más rigurosa se implementa en su red de servidores. Esta sección describe la asignación del puerto predeterminado para los servicios del ® de los multimedios de Windows para ambos tráfico entrante y saliente (mostrado como “en” y “hacia fuera” en las tablas) de modo que usted pueda configurar todos los puertos según las necesidades.

En algunos escenarios, el tráfico saliente se puede dirigir a un puerto en un rango de los puertos disponibles. Los rangos de puertos mostrados en las tablas indican el rango entero de los puertos disponibles, pero usted puede afectar un aparato menos puertos dentro del rango de puertos. Cuando usted decide cuántos puertos para abrirse, la Seguridad de la balanza con la accesibilidad y para abrir los puertos bastante para permitir que todos los clientes hagan una conexión. Primero, determine cuántos puertos usted espera utilizar para los servicios de multimedios de Windows, y entonces abrir el 10 por ciento más para explicar la coincidencia con otros programas. Después de que usted haya establecido este número, monitoree su tráfico para determinar si algunos ajustes son necesarios.

Las restricciones del rango de puertos potencialmente afectan a toda la llamada a procedimiento remoto (RPC) y aplicaciones del Modelo de objeto de componente distribuido (DCOM) que comparten el sistema, no apenas los servicios de multimedios de Windows. Si el rango de puertos afectado un aparato no es bastante amplio, los servicios competitivos tales como IIS pueden fallar con los errores al azar. El rango de puertos debe poder acomodar todas las aplicaciones del sistema potenciales que utilicen los servicios RPC, COM, o DCOM.

Para hacer la configuración de escudo de protección más fácil, usted puede configurar cada enchufe del protocolo del control de servidor (RTSP, MMS, y HTTP) en el administrador de los servicios de multimedios de Windows para utilizar un puerto específico. Si su administrador de la red ha abierto ya una serie de puertos para uso de sus multimedios de Windows servidor, usted puede afectar un aparato esos puertos a los protocolos del control por consiguiente. Si no, usted puede pedir que el administrador de la red abra los puertos predeterminados para cada protocolo. Si no es posible a los puertos abiertos en su Firewall, los servicios de multimedios de Windows pueden fluir el contenido con el protocolo HTTP sobre el puerto 80.

Ésta es la asignación predeterminada del puerto de firewall para los servicios de multimedios de Windows para entregar un flujo de datos de unidifusión:

Application Protocol	Protocolo	Puerto	Descripción

RTSP	TCP	554 (in/out)	Utilizado para validar las conexiones cliente entrantes RTSP y para entregar los paquetes de datos a los clientes que están fluyendo con RTSPT.
RTSP	UDP	5004 (hacia fuera)	Utilizado para entregar los paquetes de datos a los clientes que están fluyendo con RTSPU.
RTSP	UDP	5005 (in/out)	Utilizado para recibir la información de pérdida del paquete de los clientes y para proporcionar la información de sincronización a los clientes que están fluyendo con RTSPU.
MMS	TCP	1755 (in/out)	Utilizado para validar las conexiones cliente entrantes del MMS y para entregar los paquetes de datos a los clientes que están fluyendo con MMST.
MMS	UDP	1755 (in/out)	Utilizado para recibir la información de pérdida del paquete de los clientes y para proporcionar la información de sincronización a los clientes que están fluyendo con MMSU.
MMS	UDP	1024 - 5000 (hacia fuera)	Utilizado para entregar los paquetes de datos a los clientes que están fluyendo con MMSU. Abra solamente el número necesario de puertos.
HTTP	TCP	80 (in/out)	Utilizado para validar las conexiones entrantes del cliente HTTP y para entregar los paquetes de datos a los clientes que están fluyendo con el HTTP.

Para aseegurarse que su contenido está disponible para todas las versiones de cliente que conecten con su servidor, abra todos los puertos descritos en la tabla para todos los protocolos de conexión que se puedan utilizar dentro de la renovación del protocolo. Si usted dirige los servicios de multimedios de Windows en un ordenador que funcione con el Service Pack 1 (SP1) de Windows Server™ 2003, usted debe agregar el programa de servicios de multimedios de Windows (wmserver.exe) como excepción adentro firewall de Windows para abrir los puertos de entrada predeterminados para el unicast que fluye, bastante que los puertos abiertos en el Firewall manualmente.

Nota: Refiera al sitio Web de Microsoft para saber más sobre la configuración de escudo de protección del MMS.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

Configuración ASA

```
CiscoASA#Show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
!--- Output suppressed access-list outside_access_in
extended permit icmp any any access-list
outside_access_in extended permit udp any host
192.168.1.5 eq 1755 !--- Command to open the MMS udp
port access-list outside_access_in extended permit tcp
any host 192.168.1.5 eq 1755 !--- Command to open the
MMS tcp port access-list outside_access_in extended
permit udp any host 192.168.1.5 eq 5005 !--- Command to
open the RTSP udp port access-list outside_access_in
extended permit tcp any host 192.168.1.5 eq www !---
Command to open the HTTP port access-list
outside_access_in extended permit tcp any host
192.168.1.5 eq rtsp !--- Command to open the RTSP tcp
port !--- Output suppressed static (inside,outside)
192.168.1.5 10.1.1.5 netmask 255.255.255.255 !---
Translates the mapped IP 192.168.1.5 to the translated
IP 10.1.1.5 of the MMS. access-group outside_access_in
in interface outside !--- Output suppressed telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp !--- RTSP inspection is enabled by default inspect
skinny inspect esmtp inspect sqlnet inspect sunrpc
inspect tftp inspect sip inspect xdmcp ! service-policy
global_policy global
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **Lista de acceso de la demostración** — Visualiza los ACL configurados en ASA/PIX`ciscoASA#`**`show access-list`** `access-list outside_access_in; 6 elements access-list outside_access_in line 1 extended permit icmp any any (hitcnt=0) 0x71af81e1 access-list outside_access_in line 2 extended permit udp any host 192.168.1.5 eq 1755 (hitcnt=0) 0x42606263 access-list outside_access_in line 3 extended permit tcp any host 192.168.1.5 eq 1755 (hitcnt=0) 0xa 0161e75 access-list outside_access_in line 4 extended permit udp any host 192.168.1.5 eq 5005 (hitcnt=0) 0x3 90e9949 access-list outside_access_in line 5 extended permit tcp any host 192.168.1.5 eq www (hitcnt=0) 0xe5 db0efc access-list outside_access_in line 6 extended permit tcp any host 192.168.1.5 eq rtsp (hitcnt=0) 0x56fa336f`
- **Demostración nacional** — Políticas NAT y contadores de las visualizaciones.`ciscoASA(config)#`**`show nat`** `NAT policies on Interface inside: match ip inside host 10.1.1.5 outside any static translation to 192.168.1.5 translate_hits = 0, untranslate_hits = 0`

Fluir VideoTroubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Examine el RTSP es una configuración predeterminada en el ASA. Rompe el tráfico del MMS puesto que el dispositivo de seguridad no puede realizar el NAT en los mensajes RTSP porque los IP Address incluidos se contienen en los archivos SDP como parte de los mensajes HTTP o RTSP. Los paquetes pueden ser hechos fragmentos, y el dispositivo de seguridad no puede realizar el NAT en los paquetes fragmentados.

Solución alternativa: Este problema puede ser resuelto si usted inhabilita el examen RTSP para este tráfico determinado del MMS como se muestra:

```
access-list rtsp-acl extended deny tcp
   any host 192.168.1.5 eq 554
access-list rtsp-acl extended permit tcp any any eq 554
class-map rtsp-traffic
match access-list rtsp-acl
policy-map global_policy
class inspection_default
no inspect rtsp
class rtsp-traffic
inspect rtsp
```

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems
- Página de soporte de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems