ASA/PIX: Ejemplo de Configuración de Permitir que el Tráfico de Red Acceda a Microsoft Media Server (MMS) / Streaming Video desde Internet

Contenido

Introducción

Este documento describe cómo configurar Adaptive Security Appliance (ASA) para permitir que el cliente o usuario de Internet acceda a Microsoft Media Server (MMS) o a la transmisión de vídeo ubicada en la red interna de ASA.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Configuración básica de ASA
- MMS está configurado y funciona correctamente

Componentes Utilizados

La información de este documento se basa en Cisco ASA que ejecuta la versión de software 7.x y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

La información en este documento también es aplicable a Cisco PIX Firewall que ejecuta la versión de software 7.x y posteriores.

Convenciones

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

Información del firewall para los servicios de Windows Media serie 9

Uso de los protocolos de transmisión multimedia

Microsoft® Windows Media® Services serie 9 utiliza dos protocolos de transmisión multimedia para ofrecer contenido como flujo de unidifusión a los clientes:

- Protocolo de transmisión en tiempo real (RTSP)
- Protocolo de Microsoft Media Server (MMS)

Estos protocolos admiten acciones de control de cliente como detener, pausar, rebobinar y avanzar rápidamente a los archivos de Windows Media indexados.

RTSP es un protocolo de capa de aplicación creado específicamente para proporcionar entrega controlada de datos en tiempo real, como contenido de audio y vídeo. Puede utilizar RTSP para transmitir contenido a equipos que ejecutan Windows Media Player 9 Series o versiones posteriores, a clientes que utilizan el control ActiveX® de Windows Media Player 9 Series o a otros equipos que ejecutan Windows Media Services 9 Series. El RTSP funciona junto con el protocolo de transporte en tiempo real (RTP) para dar formato a los paquetes de contenido multimedia y negociar el protocolo de capa de transporte más eficiente, ya sea el protocolo de datagramas de usuario (UDP) o el protocolo de control de transporte (TCP), para utilizarlo cuando envíe la secuencia a los clientes. Puede implementar RTSP a través del plug-in de WMS RTSP Server Control Protocol en el administrador de servicios de Windows Media. Este plug-in está habilitado de forma predeterminada.

MMS es un protocolo de capa de aplicación propietario desarrollado para versiones anteriores de Windows Media Services. Puede utilizar MMS para transmitir contenido a equipos que ejecutan Windows Media Player para Windows® XP o anterior. Puede implementar MMS a través del plug-in del protocolo de control de servidor MMS de WMS en el administrador de servicios de Windows Media. Este plug-in está habilitado de forma predeterminada.

Utilizar HTTP

Si los puertos del firewall no se pueden abrir, los servicios Windows Media® pueden transmitir contenido con HTTP a través del puerto 80. HTTP se puede utilizar para enviar secuencias a todas las versiones del Reproductor de Windows Media. Puede implementar HTTP a través del complemento WMS HTTP Server Control Protocol en el Administrador de servicios de Windows Media. Este plug-in no está habilitado de forma predeterminada. Si otro servicio, como Servicios de Internet Information Server (IIS), utiliza el puerto 80 en la misma dirección IP, no puede habilitar el complemento.

HTTP también se puede utilizar para estos:

- Distribuir secuencias entre servidores Windows Media
- Contenido de origen de un codificador de Windows Media
- Descargar listas de reproducción generadas dinámicamente desde un servidor Web

Los complementos de origen de datos se deben configurar en el administrador de servicios de Windows Media para admitir estos escenarios de transmisión HTTP adicionales.

Acerca de la Renovación del Protocolo

Si los clientes que admiten RTSP se conectan a un servidor que ejecuta Windows Media® Services con un moniker de URL RTSP (por ejemplo, rtsp://) o un moniker de URL MMS (por ejemplo, mms://), el servidor utiliza la renovación de protocolos para transmitir el contenido al cliente para proporcionar una experiencia de transmisión óptima. La reversión automática del protocolo de RTSP/MMS a RTSP con transportes basados en UDP o basados en TCP (RTSPU o RTSPT), o incluso HTTP (si se habilita el complemento WMS HTTP Server Control Protocol), puede ocurrir cuando el servidor intenta negociar el mejor protocolo y proporcionar una experiencia de transmisión óptima para el cliente. Entre los clientes que admiten RTSP se incluyen el Reproductor de Windows Media serie 9 o posterior u otros reproductores que utilizan el control ActiveX del Reproductor de Windows Media serie 9.

Las versiones anteriores del Reproductor de Windows Media, como el Reproductor de Windows Media para Windows XP, no admiten el protocolo RTSP, pero el protocolo MMS proporciona compatibilidad con la renovación de protocolos para estos clientes. Por lo tanto, cuando una versión anterior del Player intenta conectarse al servidor con un MMS URL moniker, la transferencia automática del protocolo de MMS a MMS con transportes basados en UDP o basados en TCP (MMSU o MMST), o incluso HTTP (si el WMS HTTP Server Control Protocol está habilitado), puede ocurrir cuando el servidor intenta negociar el mejor protocolo y proporcionar una experiencia de transmisión óptima para estos clientes.

Para asegurarse de que el contenido está disponible para todos los clientes que se conectan al servidor, los puertos de su firewall deben abrirse para todos los protocolos de conexión que se pueden utilizar dentro de la renovación del protocolo.

Puede obligar al servidor de Windows Media a utilizar un protocolo específico si identifica el protocolo que se utilizará en el archivo de anuncio (por ejemplo, rtspu://server/publishing_point/file). Para proporcionar una experiencia de transmisión óptima para todas las versiones del cliente, recomendamos que la URL utilice el protocolo MMS general. Si los clientes se conectan a su flujo con una URL con un MMS URL moniker, cualquier renovación de protocolo necesaria se produce automáticamente. Tenga en cuenta que los usuarios pueden deshabilitar los protocolos de transmisión en la configuración de propiedades del Reproductor de Windows Media. Si un usuario inhabilita un protocolo, se omite dentro de la renovación. Por ejemplo, si HTTP está desactivado, las URL no se transmiten a HTTP.

Asignar puertos para servicios de Windows Media

La mayoría de los firewalls se utilizan para controlar el "tráfico entrante" al servidor; generalmente no controlan el "tráfico saliente" a los clientes. Los puertos del firewall para el tráfico saliente se pueden cerrar si se implementa una política de seguridad más estricta en la red del servidor. En esta sección se describe la asignación de puertos predeterminada para los servicios de Windows Media® tanto para el tráfico entrante como saliente (que se muestran como "Entrada" y "Salida" en las tablas) para que pueda configurar todos los puertos según sea necesario.

En algunos escenarios, el tráfico saliente se puede dirigir a un puerto en un rango de puertos disponibles. Los intervalos de puertos que se muestran en las tablas indican el rango completo de puertos disponibles, pero puede asignar menos puertos dentro del intervalo de puertos. Cuando decide cuántos puertos abrir, equilibre la seguridad con la accesibilidad y abra suficientes puertos para que todos los clientes puedan establecer una conexión. En primer lugar, determine cuántos puertos espera utilizar para Windows Media Services y, a continuación, abra un 10% más para tener en cuenta la superposición con otros programas. Después de haber establecido este número, controle el tráfico para determinar si es necesario realizar algún ajuste.

Las restricciones del intervalo de puertos pueden afectar a todas las aplicaciones de llamada a procedimiento remoto (RPC) y Modelo de objetos componentes distribuidos (DCOM) que comparten el sistema, no solo a los servicios de Windows Media. Si el intervalo de puertos asignado no es lo suficientemente amplio, los servicios de la competencia como IIS pueden fallar con errores aleatorios. El intervalo de puertos debe poder alojar todas las aplicaciones del sistema potenciales que utilizan servicios RPC, COM o DCOM.

Para facilitar la configuración del firewall, puede configurar cada plug-in de protocolo de control de servidor (RTSP, MMS y HTTP) en el administrador de servicios de Windows Media para utilizar un puerto específico. Si el administrador de red ya ha abierto una serie de puertos para su uso en el servidor de Windows Media, puede asignar esos puertos a los protocolos de control en consecuencia. Si no es así, puede solicitar al administrador de la red que abra los puertos predeterminados para cada protocolo. Si no es posible abrir puertos en el firewall, Windows Media Services puede transmitir contenido con el protocolo HTTP a través del puerto 80.

Ésta es la asignación predeterminada de puertos de firewall para los servicios de Windows Media para ofrecer un flujo de unidifusión:

Protocolo de aplicación	Protocolo	Puerto	Descripción
RTSP	TCP	554 (Entrada/Salida)	Se utiliza para aceptar conexiones entrantes del cliente RTSP y para entregar paquetes de datos a los clientes que se transmiten con RTSPT.
RTSP	UDP	5004 (salida)	Se utiliza para enviar paquetes de datos a los clientes que se transmiten con RTSPU.
RTSP	UDP	5005 (Entrad	Se utiliza para recibir información de pérdida de paquetes de los

		a/Salida)	clientes y para proporcionar información de sincronización a los clientes que se transmiten con RTSPU.
MMS	TCP	1755 (Entrada/Salida)	Se utiliza para aceptar conexiones entrantes del cliente MMS y para entregar paquetes de datos a los clientes que se transmiten con MMST.
MMS	UDP	1755 (Entrada/Salida)	Se utiliza para recibir información de pérdida de paquetes de los clientes y para proporcionar información de sincronización a los clientes que se transmiten con MMSU.
MMS	UDP	1024-5000 (salida)	Se utiliza para enviar paquetes de datos a los clientes que se transmiten con MMSU. Abra sólo el número necesario de puertos.
HTTP	TCP	80 (Entrada/Salida)	Se utiliza para aceptar conexiones de cliente HTTP entrantes y para entregar paquetes de datos a clientes que están transmitiendo con HTTP.

Para asegurarse de que su contenido esté disponible para todas las versiones de cliente que se conectan a su servidor, abra todos los puertos descritos en la tabla para todos los protocolos de conexión que se pueden utilizar dentro de la renovación de protocolo. Si ejecuta Windows Media Services en un equipo que ejecuta Windows Server™ 2003 Service Pack 1 (SP1), debe agregar el programa Windows Media Services (wmserver.exe) como excepción en Firewall de Windows para abrir los puertos entrantes predeterminados para la transmisión de unidifusión, en lugar de abrir manualmente los puertos en el firewall.

Nota: Refiérase al sitio web de Microsoft para saber más sobre la configuración del firewall MMS.

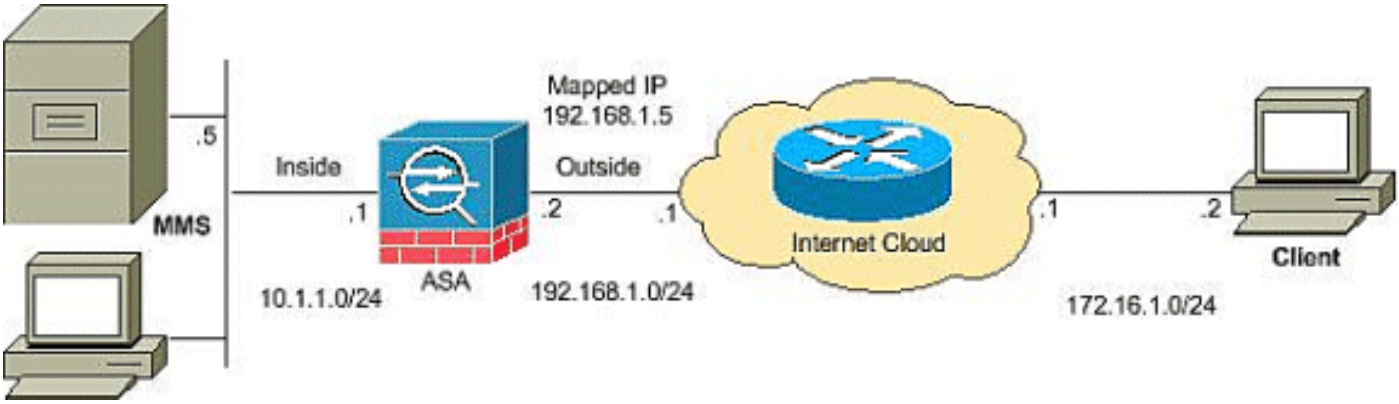
Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) 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 utilizados 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.

- **Show access-list**: muestra las ACL configuradas 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) 0x4
2606263
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) 0x5
6fa336f
```

- **Show nat**: muestra las políticas y los contadores de NAT.

```
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
```

Resolución de problemas de transmisión de vídeo

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

Inspeccionar RTSP es una configuración predeterminada en el ASA. Rompe el tráfico de MMS porque el dispositivo de seguridad no puede realizar NAT en los mensajes RTSP porque las direcciones IP incrustadas están contenidas en los archivos SDP como parte de los mensajes HTTP o RTSP. Los paquetes se pueden fragmentar y el dispositivo de seguridad no puede realizar NAT en los paquetes fragmentados.

Solución alternativa: Este problema se puede resolver si inhabilita la inspección RTSP para este tráfico MMS en particular como se muestra a continuación:

```
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