ASA/PIX: Reservam tráfego de rede para alcançar Microsoft servidor de mídia) (MM/vídeo fluente do exemplo de configuração do Internet

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável (ASA) em ordem reservar o cliente ou o usuário do Internet para alcançar o servidor de mídia de Microsoft (MM) ou a vídeo fluente colocou na rede interna do ASA.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Configuração básica do ASA
- Os MM são configurados e trabalham corretamente

Componentes Utilizados

A informação neste documento é baseada em Cisco ASA que executa a versão de software 7.x e mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

A informação neste documento é igualmente aplicável ao Cisco PIX Firewall que executa a versão de software 7.x e mais tarde.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informação do Firewall para o 9 Series dos serviços do Windows Media

Use protocolos da mídia fluente

O ® do Windows Media do ® de Microsoft presta serviços de manutenção a usos do 9 Series dois protocolos da mídia fluente entregar o índice como um fluxo de unicast aos clientes:

- Real-Time Streaming Protocol (RTSP)
- Protocolo do servidor de mídia de Microsoft (MM)

Estas ações de controle do cliente do apoio dos protocolos tais como a parada, a pausa, a rebobinação, e arquivos posicionados rápido-dianteiros do Windows Media.

O RTSP é um protocolo de camada do aplicativo que seja criado especificamente para fornecer entrega controlada dos dados de tempo real, tais como o índice audio e video. Você pode usar o RTSP para fluir o índice aos computadores que executam Windows Media Player 9 Series ou mais tarde, aos clientes que usam o controle do ® de Windows Media Player 9 Series ActiveX, ou a outros computadores que executam o 9 Series dos serviços do Windows Media. O RTSP trabalha com o Real-Time Transport Protocol (RTP) para formatar pacotes de índice de multimédios e para negociar o protocolo de camada de transporte o mais eficiente, User Datagram Protocol (UDP) ou protocolo de controle do transporte (TCP), para usar-se quando você entrega o córrego aos clientes. Você pode executar o RTSP através do encaixe do protocolo de controle do server WM RTSP no administrador dos serviços do Windows Media. Este encaixe é permitido à revelia.

Os MM são um protocolo de camada do aplicativo proprietário que seja desenvolvido para versões anterior de serviços do Windows Media. Você pode usar MM para fluir o índice aos computadores que executam Windows Media Player para o ® XP de Windows ou mais cedo. Você pode executar MM através do encaixe do protocolo de controle do server WM MM no administrador dos serviços do Windows Media. Este encaixe é permitido à revelia.

Use o HTTP

Se as portas em seu Firewall não podem ser abertas, os serviços do ® do Windows Media podem fluir o índice com o HTTP sobre a porta 80. O HTTP pode ser usado para entregar córregos a todas as versões de Windows Media Player. Você pode executar o HTTP através do encaixe do protocolo de controle do Server do HTTP WM no administrador dos serviços do Windows Media. Este encaixe não é permitido à revelia. Se um outro serviço, tal como o Internet Information Services (IIS), usa a porta 80 no mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT, você não pode permitir o encaixe.

O HTTP pode igualmente ser usado para estes:

- Distribua córregos entre server do Windows Media
- Índice da fonte de um codificador do Windows Media
- Listas de reproduções dinamicamente geradas da transferência de um servidor de Web

Os encaixes da origem de dados devem ser configurados no administrador dos serviços do Windows Media para apoiar este o HTTP adicional que flui encenações.

Sobre o derrubamento do protocolo

Se os clientes que apoiam o RTSP conectam a um server que dirija serviços do ® do Windows Media com uma alcunha RTSP URL (por exemplo, rtsp://) ou uma alcunha MM URL (por exemplo, mms://), o server usam o derrubamento do protocolo para fluir o índice ao cliente para fornecer uma experiência de fluência ótima. O derrubamento automático do protocolo de RTSP/MMS ao RTSP com transportes UDP-baseados ou com base em TCP (RTSPU ou RTSPT), ou mesmo o HTTP (se o encaixe do protocolo de controle do Server do HTTP WM é permitido) podem ocorrer enquanto o server tenta negociar o melhor protocolo e fornecer uma experiência de fluência ótima para o cliente. Os clientes que apoiam o RTSP incluem Windows Media Player 9 Series ou mais tarde ou outros jogadores que usam o controle activex de Windows Media Player 9 Series.

As versões anterior de Windows Media Player, tal como Windows Media Player para Windows XP, não apoiam o protocolo RTSP, mas o protocolo MM fornece o apoio do derrubamento do protocolo para estes clientes. Assim, quando uma versão anterior do jogador tenta conectar ao server com uma alcunha MM URL, um derrubamento automático do protocolo dos MM aos MM com os transportes UDP-baseados ou com base em TCP (MMSU ou MMST), ou mesmo um HTTP (se o encaixe do protocolo de controle do Server do HTTP WM está permitido), pode ocorrer enquanto o server tenta negociar o melhor protocolo e fornecer uma experiência de fluência ótima para estes clientes.

A fim certificar-se de que seu índice está disponível a todos os clientes que conectam a seu server, as portas em seu Firewall devem ser abertas para todos os protocolos de conexão que podem ser usados dentro do derrubamento do protocolo.

Você pode forçar seu server do Windows Media para usar um protocolo específico se você identifica o protocolo a ser usado no arquivo do anúncio (por exemplo, rtspu://server/publishing_point/file). A fim fornecer uma experiência de fluência ótima para todas as versões de cliente, nós recomendamos que o uso URL o protocolo geral MM. Se os clientes conectam a seu córrego com uma URL com uma alcunha MM URL, todo o derrubamento necessário do protocolo ocorre automaticamente. Esteja ciente que os usuários podem desabilitar Protocolos streaming nos ajustes da propriedade de Windows Media Player. Se um usuário desabilita um protocolo, está saltado dentro do derrubamento. Por exemplo, se o HTTP é

desabilitado, as URL não rolam sobre ao HTTP.

Atribua portas para serviços do Windows Media

A maioria de Firewall são usados para controlar o “tráfego de entrada” ao server; geralmente não controlam o “tráfego de saída” aos clientes. As portas em seu Firewall para o tráfego de saída podem ser fechadas se uma política de segurança mais estrita é executada em sua rede de servidor. Esta seção descreve a atribuição da porta padrão para serviços do ® do Windows Media para ambos tráfego de entrada e de saída (mostrado como “” e “para fora” nas tabelas) de modo que você possa configurar todas as portas como necessárias.

Em algumas encenações, o tráfego de saída pode ser dirigido a uma porta em uma escala dos portos disponíveis. Os intervalos de porta mostrados nas tabelas indicam a escala inteira dos portos disponíveis, mas você pode atribuir menos portas dentro do intervalo de porta. Quando você decidir quantas portas abrir, Segurança do equilíbrio com acessibilidade e abrir apenas bastante portas para permitir que todos os clientes façam uma conexão. Primeiramente, determine quantas portas você espera usar para serviços do Windows Media, e os por cento 10 abertos mais para esclarecer então a sobreposição com outros programas. Depois que você estabeleceu este número, monitore seu tráfego para determinar se algum ajuste é necessário.

As limitações do intervalo de porta afetam potencialmente toda a chamada de procedimento remoto (RPC) e aplicativos do modelo de objeto de componente distribuído (DCOM) que compartilham do sistema, não apenas serviços do Windows Media. Se o intervalo de porta atribuído não é largo bastante, os serviços competitivos tais como o IIS podem falhar com erros aleatórios. O intervalo de porta deve poder acomodar todos os aplicativos de sistema potenciais que usam serviços RPC, COM, ou DCOM.

A fim facilitar a configuração de firewall, você pode configurar cada encaixe do protocolo de controle do server (RTSP, MM, e HTTP) no administrador dos serviços do Windows Media para usar uma porta específica. Se seu administrador de rede tem aberto já uma série de portas para o uso de seu server do Windows Media, você pode atribuir aquelas portas aos protocolos de controle em conformidade. Se não, você pode pedir que o administrador de rede abra as portas padrão para cada protocolo. Se não é possível às portas aberta em seu Firewall, os serviços do Windows Media podem fluir o índice com o protocolo HTTP sobre a porta 80.

Esta é a atribuição da porta de firewall do padrão para serviços do Windows Media a fim entregar um fluxo de unicast:

Protocolo do aplicativo	Protocolo	Porta	Descrição
RTSP	TCP	554 (entrada/saída)	Usado para aceitar conexões de cliente de entrada RTSP e para entregar pacotes de dados aos clientes que estão fluindo com RTSPT.
RTSP	UDP	5004 (para fora)	Usado para entregar pacotes de dados aos clientes que estão fluindo com RTSPU.
RTS	UD	5005	Usado para receber a informação

P	P	(entrada/saída)	de perda de pacote dos clientes e para fornecer a informação de sincronização aos clientes que estão fluindo com RTSPU.
MM	TCP	1755 (entrada/saída)	Usado para aceitar conexões de cliente de entrada MM e para entregar pacotes de dados aos clientes que estão fluindo com MMST.
MM	UDP	1755 (entrada/saída)	Usado para receber a informação de perda de pacote dos clientes e para fornecer a informação de sincronização aos clientes que estão fluindo com MMSU.
MM	UDP	1024-5000 (para fora)	Usado para entregar pacotes de dados aos clientes que estão fluindo com MMSU. Abra somente o número necessário de portas.
HTTP	TCP	80 (entrada/saída)	Usado para aceitar conexões de entrada do cliente HTTP e para entregar pacotes de dados aos clientes que estão fluindo com HTTP.

A fim certificar-se de que seu índice está disponível a todas as versões de cliente que conectam a seu server, abra todas as portas descritas na tabela para todos os protocolos de conexão que podem ser usados dentro do derrubamento do protocolo. Se você dirige serviços do Windows Media em um computador que execute o pacote de serviços 1 de Windows Server™ 2003 (SP1), você deve adicionar o programa de serviços do Windows Media (wmserver.exe) como uma exceção no Windows Firewall para abrir as portas de entrada do padrão para o unicast que flui, um pouco do que portas aberta no Firewall manualmente.

Nota: Refira a site do microsoft a fim saber mais sobre a configuração de firewall MM.

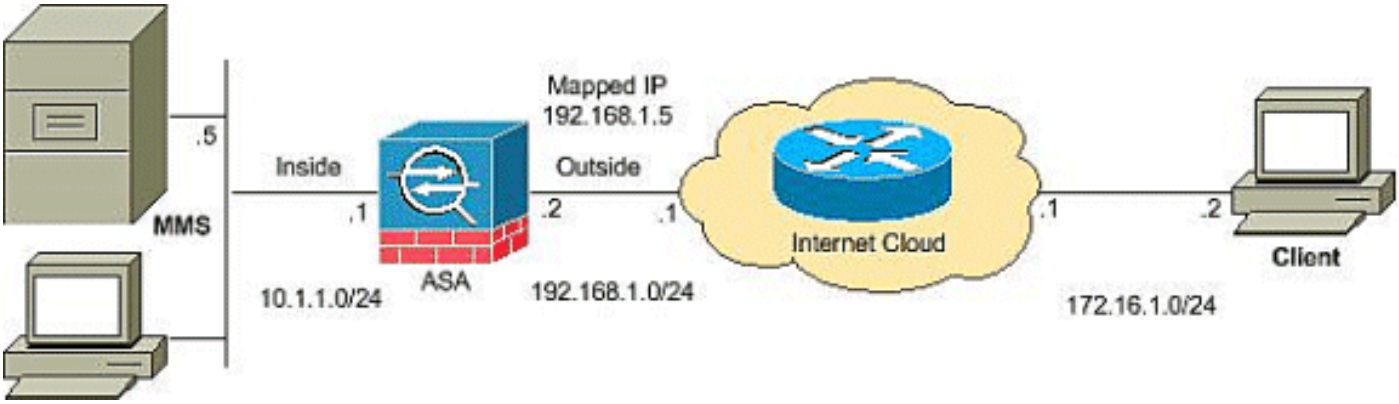
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

Configuração 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **Lista de acesso da mostra** — Indica os ACL configurados no 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`
- **Mostra nat** — Políticas de NAT e contadores dos indicadores.`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`

Fluindo VideoTroubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Inspecione o RTSP é uma configuração padrão no ASA. Quebra os MM trafica desde que a ferramenta de segurança não pode executar o NAT em mensagens RTSP porque os endereços IP incorporados são contidos nos arquivos SDP como parte das mensagens HTTP ou RTSP. Os pacotes podem ser fragmentados, e a ferramenta de segurança não pode executar o NAT em pacotes fragmentados.

Solução: Este problema pode ser resolved se você desabilita a inspeção RTSP para o este MM particulares trafica como mostrado:

```
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
```

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems
- Página de suporte de Cisco ASA

- Suporte Técnico e Documentação - Cisco Systems