ASA/PIX：准许网络流量从互联网访问Microsoft媒体服务器(MMS)/视频流配置示例

目录

简介

本文档说明如何配置自适应安全设备 (ASA)，以允许客户端或用户从 Internet 访问 Microsoft Media Server (MMS) 或位于 ASA 网络内部的视频流。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- ASA 的基本配置
- MMS 已配置并工作正常

使用的组件

本文档中的信息以运行软件版本 7.x 和更高版本的 Cisco ASA 为基准。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文档中的信息也适用于运行软件版本 7.x 和更高版本的 Cisco PIX 防火墙。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Windows Media Services 9 系列的防火墙信息

使用流媒体协议

Microsoft ® Windows媒体®服务9系列用途两份流媒体协议交付内容作为单播流对客户端：

- 实时流协议 (RTSP)
- Microsoft Media Server (MMS) 协议

上述协议支持客户端控制操作，如对带索引的 Windows Media 文件执行停止、暂停、快退和快进。

RTSP 是专门创建的应用层协议，用于提供实时数据（如音频和视频内容）的受控传送。您能使用RTSP放出内容到运行以后的Windows梅迪亚普莱耶9系列或的计算机，对使用Windows梅迪亚普莱耶9系列ActiveX ®控制的客户端，或者到该其他的计算机Run窗口9系列的媒体服务。RTSP 与实时传输协议 (RTP) 结合使用，以格式化多媒体内容数据包并协商用于向客户端传送数据流的最高效的传输层协议（用户数据报协议 (UDP) 或传输控制协议 (TCP)）。可以通过 Windows Media Services Administrator 中的 WMS RTSP 服务器控制协议插件实现 RTSP。此插件默认处于启用状态。

MMS 是针对 Windows Media Services 早期版本开发的专用应用层协议。您能使用MMS放出内容到运行Windows ® XP的前Windows梅迪亚普莱耶或的计算机。可以通过 Windows Media Services Administrator 的 WMS MMS 服务器控制协议插件实现 MMS。此插件默认处于启用状态。

使用 HTTP

如果不可能打开您的防火墙的端口， Windows媒体®服务能放出与HTTP的内容在端口80。HTTP 可用于向所有 Windows Media Player 版本传送数据流。可以通过 Windows Media Services Administrator 的 WMS HTTP 服务器控制协议插件实现 HTTP。此插件默认处于未启用状态。如果另一项服务（如 Internet 信息服务(IIS)）对相同的 IP 地址使用端口 80，则无法启用该插件。

HTTP 还可用于以下用途：

- 在 Windows Media 服务器之间分发数据流
- 从 Windows Media 编码器寻找内容来源
- 从 Web 服务器下载动态生成的播放列表

必须在 Windows Media Services Administrator 中配置数据源插件，才能支持这些附加的 HTTP 流方案。

关于协议反转

例如如果支持RTSP的客户端连接到运行Windows媒体®服务以RTSP URL标记的服务器(rtsp://)或MMS URL标记(例如， mms://)，服务器使用协议反转放出内容对客户端提供一最佳的流体验。如果服务器尝试协商最佳协议并为客户端提供最佳流媒体体验，则可能会发生从 RTSP/MMS 到采用基于 UDP 或基于 TCP 的传输的 RTSP（RTSPU 或 RTSPT）的自动协议反转，甚至是 HTTP（如果已启用 WMS HTTP 服务器控制协议插件）。支持 RTSP 的客户端包括 Windows Media Player 9 系统或更高版本，或包括使用 Windows Media Player 9 系列 ActiveX 控件的其他播放器。

Windows Media Player 的早期版本（如 Windows Media Player for Windows XP）不支持 RTSP 协议，但是 MMS 协议为这些客户端提供协议反转支持。因此，当早期版本的 Windows Media Player 尝试使用 MMS URL 标记连接到服务器时，如果服务器尝试协商最佳协议并为这些客户端提供最佳流媒体体验，则可能会发生从 MMS 到采用基于 UDP 或基于 TCP 的传输的 MMS（MMSU 或 MMST）的自动协议反转，甚至是 HTTP（如果已启用 WMS HTTP 服务器控制协议插件）。

为确保您的内容可用于连接到服务器的所有客户端，必须针对可以在协议反转内使用的所有连接协议打开防火墙的端口。

您能强制您的Windows媒体服务器使用一份特定协议，如果识别用于通告文件的协议(例如， rtspu://server/publishing_point/file)。为了为所有客户端版本提供最佳的流媒体体验，我们建议 URL 使用一般 MMS 协议。如果客户端使用带有 MMS URL 标记的 URL 连接到您的数据流，则会自动进行所有必要的协议反转。请注意，用户可以在 Windows Media Player 的属性设置中禁用流媒体协议。如果用户禁用某个协议，则会在反转中跳过该协议。例如，如果禁用 HTTP，URL 不会反转为 HTTP。

为 Windows Media Services 分配端口

大部分防火墙用于控制发往服务器的“入站数据流”；它们通常不控制发往客户端的“出站数据流”。如果对服务器网络实施了更加严密的安全策略，可能会关闭防火墙中用于出站数据流的端口。此部分描述Windows媒体®服务默认端口分配两的入站和出站通流量(显示作为“在”和“”在表里里)，以便您能配置所有端口当必要时。

在某些情况下，可以将出站数据流定向到可用端口范围内的某一个端口。表中显示的端口范围表示可用端口的整个范围，但端口范围内可以分配的端口更少一些。在决定打开的端口数时，应权衡安全性与可访问性，并且仅打开足以允许所有客户端建立连接的端口即可。首先，确定希望用于 Windows Media Services 的端口数，然后多打开 10% 以应对与其他程序的重叠。建立此端口数后，请监控数据流以确定是否需要进行任何调整。

端口范围限制会对所有共享系统的远程过程调用 (RPC) 和分布式组件对象模型 (DCOM) 应用程序产生潜在影响，而不仅仅影响 Windows Media Services。如果分配的端口范围不够广，竞争性服务（如 IIS）可能会因各种错误而失败。端口范围必须能够容纳使用 RPC、COM 或 DCOM 服务的所有潜在的系统应用程序。

为简化防火墙配置，可以将 Windows Media Services Administrator 中的每个服务器控制协议插件（RTSP、MMS 和 HTTP）配置为使用一个特定端口。如果网络管理员已打开一系列端口供 Windows Media 服务器使用，您可以将这些端口相应地分配给控制协议。否则，可以要求网络管理员打开每个协议的默认端口。如果无法打开防火墙的端口，Windows Media Services 可通过端口 80 使用 HTTP 协议传送流内容。

下面是用于传送单播数据流的 Windows Media Services 默认防火墙端口分配：

应用	协	波尔特	说明

协议	议		
RTSP	TCP	554（入/出）	用于接受入站 RTSP 客户端连接，以及向使用 RTSPT 传送数据流的客户端传送数据包。
RTSP	UDP	5004（出）	用于向使用 RTSPU 传送数据流的客户端传送数据包。
RTSP	UDP	5005（入/出）	用于从客户端接收数据包丢失信息，以及为使用 RTSPU 传送数据流的客户端提供同步信息。
MMS	TCP	1755（入/出）	用于接受入站 MMS 客户端连接，以及向使用 MMST 传送数据流的客户端传送数据包。
MMS	UDP	1755（入/出）	用于从客户端接收数据包丢失信息，以及为使用 MMSU 传送数据流的客户端提供同步信息。
MMS	UDP	1024-5000（出）	用于向使用 MMSU 传送数据流的客户端传送数据包。请仅打开必要数量的端口。
HTTP	TCP	80（入/出）	用于接受入站 HTTP 客户端连接，以及向使用 HTTP 传送数据流的客户端传送数据包。

为确保您的内容可用于连接到服务器的所有客户端版本，必须针对可以在协议反转内使用的所有连接协议打开表中列出的所有端口。如果在运行 Windows Server™ 2003 Service Pack 1 (SP1) 的计算机上运行 Windows Media Services，必须在 Windows 防火墙中将 Windows Media Services 程序 (wmserver.exe) 添加为例外才能打开用于单播数据流传送的默认入站端口，而不是手动打开防火墙的端口。

注意： 有关 MMS 防火墙配置的详细信息，请参阅 Microsoft 网站 。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置

本文档使用以下配置：

ASA 配置

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **Show access-list** — 显示 ASA/PIX 中配置的 ACL`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** — 显示 NAT 策略和计数器。`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`

视频流故障排除

本部分提供的信息可用于对配置进行故障排除。

检查 RTSP 是 ASA 的一项默认配置。它会中断 MMS 数据流，因为安全设备无法对 RTSP 消息执行 NAT，原因是嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。可以对数据包进行分段，但安全设备无法对分段数据包执行 NAT。

应急方案：如果按下面的方法禁用这种特定 MMS 数据流的 RTSP 检查，可以解决此问题：

```
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
```

相关信息

- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持 - Cisco Systems
- Cisco ASA 支持页
- 技术支持和文档 - Cisco Systems