ASA/PIX:允許網路流量從網際網路訪問Microsoft Media Server(MMS)/影片流配置示例

目錄

簡介

本文檔介紹如何配置Adaptive Security Appliance(ASA)，以便允許來自Internet的客戶端或使用者訪問ASA內部網路中的Microsoft Media Server(MMS)或流影片。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- ASA的基本配置
- MMS已配置且工作正常

採用元件

本文檔中的資訊基於運行軟體版本7.x及更高版本的Cisco ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本文檔中的資訊也適用於運行軟體版本7.x及更高版本的Cisco PIX防火牆。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

Windows Media Services 9系列的防火牆資訊

使用流媒體協定

Microsoft® Windows Media® Services 9系列使用兩種流媒體協定將內容作為單播流傳輸到客戶端：

- 即時串流通訊協定(RTSP)
- Microsoft Media Server(MMS)協定

這些協定支援客戶端控制操作，如停止、暫停、倒帶和快速轉發索引Windows Media檔案。

RTSP是專門為提供即時資料（如音訊和影片內容）的控制傳輸而建立的應用層協定。您可以使用RTSP將內容流式傳輸到運行Windows Media Player 9系列或更高版本的電腦、使用Windows Media Player 9系列ActiveX®控制元件的客戶端或運行Windows Media Services 9系列的其他電腦。RTSP與即時傳輸協定(RTP)配合工作，格式化多媒體內容的資料包，並協商將流傳送到客戶端時要使用的最有效的傳輸層協定，即使用者資料包協定(UDP)或傳輸控制協定(TCP)。可通過Windows Media Services Administrator中的WMS RTSP伺服器控制協定外掛實施RTSP。預設情況下啟用此外掛。

MMS是為早期版本的Windows Media Services開發的專有應用層協定。您可以使用MMS將內容流式傳輸到運行Windows® XP或更低版本Windows Media Player的電腦。您可以通過Windows Media Services Administrator中的WMS MMS伺服器控制協定外掛實施MMS。預設情況下啟用此外掛。

使用HTTP

如果防火牆上的埠無法開啟，則Windows Media®服務可以通過埠80使用HTTP流式傳輸內容。HTTP可用於向所有Windows Media Player版本傳輸流。您可以通過Windows Media Services Administrator中的WMS HTTP伺服器控制協定外掛實施HTTP。預設情況下未啟用此外掛。如果其他服務(如Internet Information Services(IIS))在同一IP地址上使用埠80，則無法啟用該外掛。

HTTP也可用於以下專案：

- 在Windows Media伺服器之間分發流
- 來自Windows Media編碼器的源內容
- 從Web伺服器下載動態生成的播放清單

必須在Windows Media Services Administrator中配置資料來源外掛，以支援這些其他HTTP流方案。

關於協定回滾

如果支援RTSP的客戶端連線到運行Windows Media® Services的伺服器，該伺服器帶有RTSP URL標籤符(例如，rtsp://)或MMS URL標籤符(例如，mms://)，則伺服器使用協定滾動更新將內容流式傳輸到客戶端，以提供最佳流傳輸體驗。當伺服器嘗試協商最佳協定並為客戶端提供最佳流傳輸體驗時，可能會發生從RTSP/MMS到RTSP的自動協定滾動更新(使用基於UDP或基於TCP的傳輸（RTSPU或RTSPT），甚至是HTTP（如果啟用WMS HTTP伺服器控制協定外掛）。支援RTSP的客戶端包括Windows Media Player 9系列或更高版本或使用Windows Media Player 9系列ActiveX控制元件的其他播放器。

早期版本的Windows Media Player（如Windows XP的Windows Media Player）不支援RTSP協定，但MMS協定為這些客戶端提供協定滾動支援。因此，當早期版本的播放器嘗試連線到具有MMS URL標籤的伺服器時，當伺服器嘗試協商最佳協定並為這些客戶端提供最佳流體驗時，可能會發生從MMS到具有基於UDP或基於TCP的傳輸（MMSU或MMST）甚至HTTP（如果已啟用WMS HTTP伺服器控制協定外掛）的MMS的自動協定翻轉。

為了確保您的內容對連線到伺服器的所有客戶端都可用，必須針對協定滾動更新中可以使用的所有連線協定開啟防火牆上的埠。

如果您確定要在通知檔案(例如，rtspu://server/publishing_point/file)中使用的協定，則可以強制Windows Media伺服器使用特定的協定。 為了為所有客戶端版本提供最佳流體驗，我們建議使用URL的通用MMS協定。如果客戶端使用帶有MMS URL標籤的URL連線到您的流，則任何必要的協定滾動更新都會自動發生。請注意，使用者可以在Windows Media Player的屬性設定中禁用流協定。如果使用者禁用協定，則在滾動更新過程中會跳過該協定。例如，如果禁用HTTP，則URL不會滾動到HTTP。

為Windows Media Services分配埠

大多數防火牆用於控制到伺服器的「入站流量」；它們通常不控制到客戶端的「出站流量」。如果在伺服器網路上實施更嚴格的安全策略，則可以關閉防火牆中用於出站流量的埠。本節介紹入站和出站流量的Windows Media®服務的預設埠分配（在表中顯示為「內送」和「外寄」），以便您可以根據需要配置所有埠。

在某些情況下，可以將傳出流量定向到可用埠範圍中的一個埠。表中顯示的埠範圍表示可用埠的全部範圍，但您可以在埠範圍內分配更少的埠。當您決定要開啟多少個埠時，請平衡安全性和可訪問性，並只開啟足夠允許所有客戶端進行連線的埠。首先，確定預期用於Windows Media Services的埠數，然後開啟10%以上的埠，以便與其他程式重疊。在建立此編號後，監控您的流量以確定是否需要進行任何調整。

埠範圍限制可能會影響共用系統（而不僅是Windows Media Services）的所有遠端過程呼叫(RPC)和分散式元件對象模型(DCOM)應用程式。如果分配的埠範圍不夠廣，競爭服務（如IIS）可能會因隨機錯誤而失敗。埠範圍必須能夠容納所有使用RPC、COM或DCOM服務的潛在系統應用程式。

為了簡化防火牆配置，您可以在Windows Media Services Administrator中將每個伺服器控制協定外掛（RTSP、MMS和HTTP）配置為使用特定埠。如果您的網路管理員已開啟一系列埠供Windows Media Server使用，您可以相應地將這些埠分配給控制協定。如果不是，可以要求網路管理員開啟每個協定的預設埠。如果無法在防火牆上開啟埠，則Windows Media Services可以通過埠80使用HTTP協定傳輸內容。

這是Windows Media Services的預設防火牆埠分配，用於傳送單播流：

應用	通訊	連接埠	說明

協定	協定		
RTSP	TCP	554（輸入/輸出）	用於接受入站RTSP客戶端連線並將資料包傳送到使用RTSPT進行流式處理的客戶端。
RTSP	UDP	5004（外寄）	用於將資料包傳送到使用RTSPU進行流式處理的客戶端。
RTSP	UDP	5005（輸入/輸出）	用於從客戶端接收丟包資訊並向使用RTSPU進行流式處理的客戶端提供同步資訊。
MMS	TCP	1755（輸入/輸出）	用於接受入站MMS客戶端連線並將資料包傳送到使用MMST進行流式處理的客戶端。
MMS	UDP	1755（輸入/輸出）	用於從客戶端接收丟包資訊並向使用MMSU進行流式處理的客戶端提供同步資訊。
MMS	UDP	1024-5000（外寄）	用於向使用MMSU進行流式處理的客戶端傳輸資料包。僅開啟所需數量的埠。
HTTP	TCP	80（輸入/輸出）	用於接受入站HTTP客戶端連線並將資料包傳送到使用HTTP進行流式處理的客戶端。

為了確保您的內容可用於連線到伺服器的所有客戶端版本，請開啟表中所述的所有埠，瞭解協定滾動更新中可以使用的所有連線協定。如果在運行Windows Server™ 2003 Service Pack 1(SP1)的電腦上運行Windows Media Services，則必須在Windows防火牆中將Windows Media Services程式(wmserver.exe)新增為例外，以開啟單播流的預設入站埠，而不是手動開啟防火牆中的埠。

注意：請參閱Microsoft網站 ，以瞭解有關MMS防火牆配置的詳細資訊。

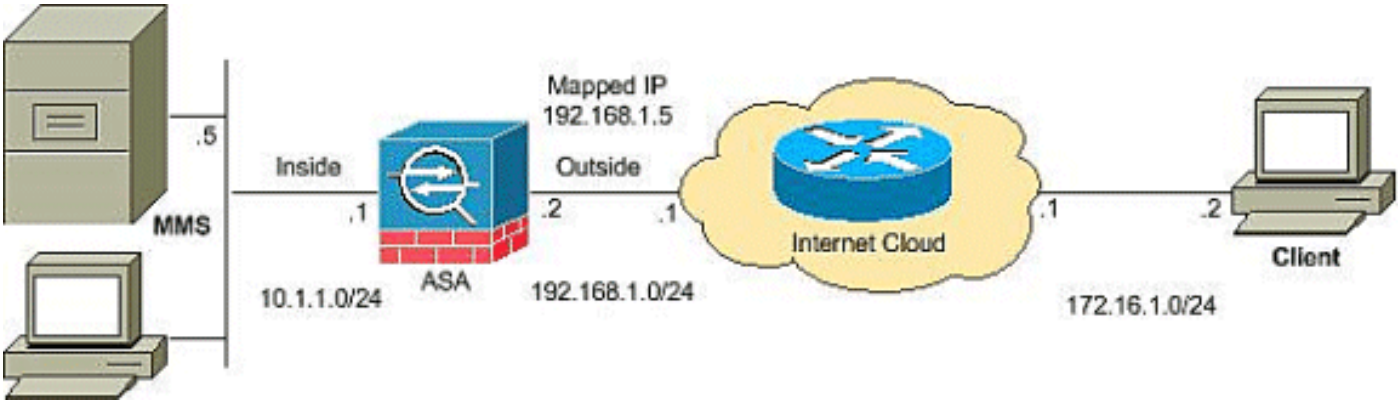
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

組態

本檔案會使用以下設定：

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- Show access-list — 顯示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 — 顯示NAT策略和計數器。

```
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
```

影片流故障排除

本節提供的資訊可用於對組態進行疑難排解。

Inspect RTSP是ASA上的預設配置。它會中斷MMS流量，因為安全裝置無法對RTSP消息執行

NAT，因為嵌入式IP地址作為HTTP或RTSP消息的一部分包含在SDP檔案中。資料包可以分段，安全裝置無法對分段的資料包執行NAT。

因應措施：如果禁用此特定MMS流量的RTSP檢查，則此問題可以解決，如下所示：

```
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
```

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援 - Cisco Systems
- Cisco ASA支援頁面
- 技術支援與文件 - Cisco Systems