

ASA/PIX: Allow the Network Traffic to Access the Microsoft Media Server (MMS)/ Streaming Video from the Internet Configuration Example

Document ID: 100308

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Firewall Information for Windows Media Services 9 Series

- Use Streaming Media Protocols
- Use HTTP
- About Protocol Rollover
- Allocate Ports for Windows Media Services

Configure

- Network Diagram
- Configurations

Verify

Streaming Video Troubleshoot

Related Information

Introduction

This document describes how to configure the Adaptive Security Appliance (ASA) in order to allow the client or user from the Internet to access the Microsoft Media Server (MMS) or streaming video placed in the inside network of ASA.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic configuration of ASA
- MMS is configured and works properly

Components Used

The information in this document is based on the Cisco ASA that runs Software Version 7.x and later.

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.

Related Products

The information in this document is also applicable to Cisco PIX Firewall that runs Software Version 7.x and later.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Firewall Information for Windows Media Services 9 Series

Use Streaming Media Protocols

Microsoft® Windows Media® Services 9 Series uses two streaming media protocols to deliver content as a unicast stream to clients:

- Real Time Streaming Protocol (RTSP)
- Microsoft Media Server (MMS) protocol

These protocols support client control actions such as stop, pause, rewind, and fast-forward indexed Windows Media files.

RTSP is an application-layer protocol that was created specifically to provide controlled delivery of real-time data, such as audio and video content. You can use RTSP to stream content to computers that run Windows Media Player 9 Series or later, to clients that use the Windows Media Player 9 Series ActiveX® control, or to other computers that run Windows Media Services 9 Series. RTSP works in tandem with Real-Time Transport Protocol (RTP) to format packets of multimedia content and negotiate the most efficient transport-layer protocol, either User Datagram Protocol (UDP) or Transport Control Protocol (TCP), to use when you deliver the stream to clients. You can implement RTSP through the WMS RTSP Server Control Protocol plug-in in Windows Media Services Administrator. This plug-in is enabled by default.

MMS is a proprietary application-layer protocol that was developed for earlier versions of Windows Media Services. You can use MMS to stream content to computers that run Windows Media Player for Windows® XP or earlier. You can implement MMS through the WMS MMS Server Control Protocol plug-in in Windows Media Services Administrator. This plug-in is enabled by default.

Use HTTP

If ports on your firewall cannot be opened, Windows Media® Services can stream content with HTTP over port 80. HTTP can be used to deliver streams to all Windows Media Player versions. You can implement HTTP through the WMS HTTP Server Control Protocol plug-in in Windows Media Services Administrator. This plug-in is not enabled by default. If another service, such as Internet Information Services (IIS), uses port 80 on the same IP address, you cannot enable the plug-in.

HTTP can also be used for these:

- Distribute streams between Windows Media servers
- Source content from a Windows Media encoder
- Download dynamically generated playlists from a Web server

Data source plug-ins must be configured in Windows Media Services Administrator to support these additional HTTP streaming scenarios.

About Protocol Rollover

If clients that support RTSP connect to a server that runs Windows Media[®] Services with an RTSP URL moniker (for example, rtsp://) or an MMS URL moniker (for example, mms://), the server uses protocol rollover to stream the content to the client to provide an optimal streaming experience. Automatic protocol rollover from RTSP/MMS to RTSP with UDP-based or TCP-based transports (RTSPU or RTSPT), or even HTTP (if the WMS HTTP Server Control Protocol plug-in is enabled) can occur as the server tries to negotiate the best protocol and provide an optimal streaming experience for the client. Clients that support RTSP include Windows Media Player 9 Series or later or other players that use the Windows Media Player 9 Series ActiveX control.

Earlier versions of Windows Media Player, such as Windows Media Player for Windows XP, do not support the RTSP protocol, but the MMS protocol provides protocol rollover support for these clients. Thus, when an earlier version of the Player attempts to connect to the server with an MMS URL moniker, automatic protocol rollover from MMS to MMS with UDP-based or TCP-based transports (MMSU or MMST), or even HTTP (if the WMS HTTP Server Control Protocol plug-in is enabled), can occur as the server tries to negotiate the best protocol and provide an optimal streaming experience for these clients.

In order to make sure that your content is available to all clients that connect to your server, ports on your firewall must be opened for all of the connection protocols that can be used within protocol rollover.

You can force your Windows Media server to use a specific protocol if you identify the protocol to be used in the announcement file (for example, rtspu://server/publishing_point/file). In order to provide an optimal streaming experience for all client versions, we recommend that the URL use the general MMS protocol. If clients connect to your stream with a URL with an MMS URL moniker, any necessary protocol rollover occurs automatically. Be aware that users can disable streaming protocols in the property settings of Windows Media Player. If a user disables a protocol, it is skipped within rollover. For example, if HTTP is disabled, the URLs do not roll over to HTTP.

Allocate Ports for Windows Media Services

Most firewalls are used to control "inbound traffic" to the server; they generally do not control "outbound traffic" to clients. Ports in your firewall for outbound traffic can be closed if a more stringent security policy is implemented on your server network. This section describes the default port allocation for Windows Media[®] Services for both inbound and outbound traffic (shown as "In" and "Out" in the tables) so that you can configure all ports as needed.

In some scenarios, outbound traffic can be directed to one port in a range of available ports. Port ranges shown in the tables indicate the entire range of available ports, but you can allocate fewer ports within the port range. When you decide how many ports to open, balance security with accessibility and open just enough ports to allow all clients to make a connection. First, determine how many ports you expect to use for Windows Media Services, and then open 10 percent more to account for overlap with other programs. After you have established this number, monitor your traffic to determine if any adjustments are necessary.

Port range restrictions potentially affect all remote procedure call (RPC) and Distributed Component Object Model (DCOM) applications that share the system, not just Windows Media Services. If the allocated port range is not broad enough, competitive services such as IIS can fail with random errors. The port range must be able to accommodate all potential system applications that use RPC, COM, or DCOM services.

In order to make firewall configuration easier, you can configure each server control protocol plug-in (RTSP, MMS, and HTTP) in Windows Media Services Administrator to use a specific port. If your network administrator has already opened a series of ports for use by your Windows Media server, you can allocate those ports to the control protocols accordingly. If not, you can ask the network administrator to open the

default ports for each protocol. If it is not possible to open ports on your firewall, Windows Media Services can stream content with the HTTP protocol over port 80.

This is the default firewall port allocation for Windows Media Services in order to deliver a unicast stream:

Application Protocol	Protocol	Port	Description
RTSP	TCP	554 (In/Out)	Used to accept inbound RTSP client connections and to deliver data packets to clients that are streaming with RTSPT.
RTSP	UDP	5004 (Out)	Used to deliver data packets to clients that are streaming with RTSPU.
RTSP	UDP	5005 (In/Out)	Used to receive packet loss information from clients and provide synchronization information to clients that are streaming with RTSPU.
MMS	TCP	1755 (In/Out)	Used to accept inbound MMS client connections and to deliver data packets to clients that are streaming with MMST.
MMS	UDP	1755 (In/Out)	Used to receive packet loss information from clients and provide synchronization information to clients that are streaming with MMSU.
MMS	UDP	1024–5000 (Out)	Used to deliver data packets to clients that are streaming with MMSU. Open only the necessary number of ports.
HTTP	TCP	80 (In/Out)	Used to accept inbound HTTP client connections and to deliver data packets to clients that are streaming with HTTP.

In order to make sure that your content is available to all client versions that connect to your server, open all ports described in the table for all of the connection protocols that can be used within protocol rollover. If you run Windows Media Services on a computer that runs Windows Server" 2003 Service Pack 1 (SP1), you must add the Windows Media Services program (wmserver.exe) as an exception in Windows Firewall to open the default inbound ports for unicast streaming, rather than open ports in the firewall manually.

Note: Refer to the Microsoft website in order to know more about the MMS firewall configuration.

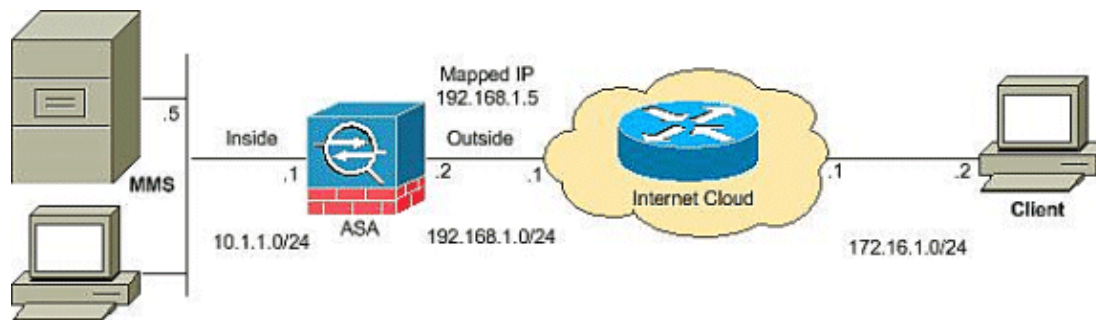
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses that have been used in a lab environment.

Configurations

This document uses these configurations:

ASA Configuration
<pre>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 !</pre>

```
!--- 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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **Show access-list** Displays the ACLs configured in the 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** Displays NAT policies and counters.

```
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
```

Streaming Video Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Inspect RTSP is a default configuration on the ASA. It breaks the MMS traffic since the security appliance cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets can be fragmented, and the security appliance cannot perform NAT on fragmented packets.

Workaround: This problem can be resolved if you disable the RTSP inspection for this particular MMS traffic as shown:

```
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
```

Related Information

- [Cisco PIX Firewall Software](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support – Cisco Systems](#)
 - [Cisco ASA Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 26, 2009

Document ID: 100308
