

Firewall Information for Streaming Media

Accessing Windows Media Streams

If you have problems delivering or receiving Windows Media streams, you may need to open additional ports in your firewall. This document briefly explains firewalls, describes how Windows Media interacts with firewalls, and offers suggested firewall settings.

General Protocol and Firewall Information

A firewall is a piece of hardware or software that prevents data packets from either entering or leaving a specified network. To control the flow of traffic, numbered ports in the firewall are either opened or closed to types of packets. The firewall looks at two pieces of information in each arriving or departing packet: the protocol through which the packet is being delivered, and the port number to which it is being sent. If the firewall is configured to accept the specified protocol through the targeted port, the packet is allowed through.

Windows Media and Firewalls

Windows Media normally streams via UDP/IP on a wide range of ports (see below for those port numbers). Microsoft is aware of the possible security issues which this can cause, so we have also enabled Windows Media to stream with TCP/IP through a single port (1755). For those sites where opening a non-"well-known port" is a problem, Windows Media can also stream via HTTP on port 80.

Note HTTP streaming from Windows Media Services is disabled by default.

Windows Media Technologies was formerly known as NetShow; some firewalls have a pre-configured NetShow setting, which may work for Windows Media.

When you allocate ports for Windows Media files, you must open all of the UDP and TCP ports corresponding to those port numbers. The number ranges in the documentation below indicate an entire range of available ports; typically, the actual number of ports allocated will be far less.

Firewall Settings for Windows Media

In the examples below, the In port is the port that the server uses to get past the firewall. The Out port is the port that Microsoft Windows Media

Player or other clients use to communicate with the server. The port assignment is random between 1024 and 5000.

Server to Client Behind a Firewall

A firewall configuration that allows users with the Windows Media Player behind a firewall to access Windows Media servers outside the firewall is:

Streaming ASF with UDP

Out: TCP on 1755

Out: UDP on 1755

In: UDP between port 1024-5000 (Only open the necessary number of ports.)

Streaming ASF with TCP

In/Out: TCP on port 1755

Streaming ASF with HTTP

In/Out: TCP on Port 80

Firewall and Registry Settings for DCOM

DCOM dynamically allocates one port per process. You need to decide how many ports you want to allocate to DCOM processes, which is equivalent to the number of simultaneous DCOM processes through the firewall. You must open all of the UDP and TCP ports corresponding to the port numbers you choose. You also need to open TCP/UDP 135, which is used for RPC End Point Mapping, among other things. In addition, you must edit the registry to tell DCOM which ports you reserved. You do this with the "HKEY_LOCAL_MACHINES\Software\Microsoft\Rpc\Internet" registry key, which you will probably have to create using the Registry Editor.

The following example tells DCOM to restrict its port range to 10 ports:

Named Value: Ports

Type: REG_MULTI_SZ

Setting: Range of port. Can be multiple lines such as:

3001-3010

135

Named Value: PortsInternetAvailable

Type: REG_SZ

Setting:"Y"

Named Value: UseInternetPorts

Type: REG_SZ
Setting: "Y"

Accessing Real Media Streams

Your firewall must be RealPlayer-aware. If it is not, RealNetworks has a free RTSP proxy service which includes source code and specifications for building your own proxy. It's simple and easy to set up. To get your copy, fill out the request form at <http://proforma.real.com/rn/misc/rtspproxy/index.html>, or have your firewall administrator send an e-mail request to firewall@real.com. You will get an immediate response telling you where to download the proxy.

Most major firewall vendors support RealPlayer. If your firewall vendor is not listed (see list at: <http://service.real.com/firewall/vendors.html>) as supporting RealPlayer, ask your firewall representative to contact RealNetworks at <mailto:firewall@real.com> about joining their firewall developers program.

Network-level Firewalls

Network-level firewalls, such as packet filters, use access control lists to allow traffic destined for some ports to pass from the Internet to the organization's internal network and to block packets for other ports. To allow any version of RealAudio Player or RealPlayer to play correctly, it is only necessary for the router to allow packets to pass to the inner network that are bound for the following range of ports:

- TCP port 554 and 7070 for connecting to G2 RealServers
- UDP ports 6970 - 7170 (inclusive) for incoming traffic only

The TCP port is used by RealPlayer to initiate a conversation with an external RealServer, to authenticate RealPlayer to the server, and to pass control messages during playback (such as pausing or stopping the stream). RealSystem G2 uses two TCP protocols for conversations between Players and Servers.

For an even safer firewall, configure the router's access control list to allow TCP connections on port 7070 and/or port 554 to be initiated from the inside network exclusively. Incoming traffic, on the other hand, should only be allowed if it is part of an ongoing connection. This is assured by requiring incoming TCP packets to have the ACK bit set in the TCP header carried by every packet. The syntax for setting the ACK bit varies with the kind of router you own. For Cisco routers the flag "ESTABLISHED" can be put at the end of the line in an access rule to specify that an incoming packet must be part of an ongoing conversation.

The range of UDP ports, on the other hand, carries the incoming stream. These ports begin to carry traffic only after RealPlayer and RealServer have performed the authentication routine, and should be enabled only for incoming traffic.

You may also want to use a proxy server in conjunction with a network-level firewall.

When RealPlayer versions G2, 7, or 8 are in use, do one of the following:

- Open ports 6970 - 7170 in your firewall for UDP.
- Open ports 7070 - 7071 and 554 in your firewall for TCP and instruct RealPlayers to use TCP for all content (visit here for more information: <http://service.real.com/firewall/configRP6.html#tcp>) . Playback quality will not be as good with this option.
- Configure your firewall to receive UDP through only one port and instruct Players to use UDP (visit here for more information: <http://service.real.com/firewall/configRP6.html#udp>) with the port you chose.
- Tell users to configure RealPlayer to request that RealServer send all media in HTTP format. This creates more overhead on your network than any of the other options.