CCBN Webcasting: Corporate Firewalls and Proxy Servers

This document describes issues around corporate firewalls and their impact on the ability to listen to streaming media within corporate intranets.

Background

The streaming media formats used by CCBN are compatible with most commercially available firewalls in use at corporations. However, there are some specific firewall settings that must be configured in order to ensure that end users can listen to and view webcast content.

A firewall is a piece of hardware or software that prevents data from either entering or leaving a specified network, thereby preventing unauthorized access to a company's intranet. A firewall's role is to ensure that all incoming and outgoing communications between a company's network and the Internet conforms to an organization's security policies. Because Windows Media and Real Media formats require two-way traffic between the end-user's PC and streaming media servers on the Internet, corporate firewalls must be configured to allow this two-way communication.

Details

Firewalls monitor and, in some cases, block traffic that is not allowed on the local network. This is to prevent unauthorized access to content and applications. For security reasons, many organizations shut down *ports* on the corporate firewall used by uncommon or non-standard protocols.

This can have the effect of not allowing some streaming media content onto the corporate network. Both Windows Media and Real Media formats will try multiple ports, in cascading order of precedence, when attempting to access a corporate network.

Below is a table that shows these *rollover protocols* and ports for current versions Windows Media and Real Media content:

Media Format	Initial Protocol	Initial Port	Rollover Protocol	Rollover Port
Windows Media	MMS (Multimedia Streaming)	1755	HTTP Cloaking (method by which a protocol is wrapped inside an HTTP protocol to allow streaming through the HTTP port, typically port 80 or 8080)	Range of TCP ports, usually 1755-5000
Real G2	RTSP (Real-time Streaming Protocol)	554	HTTP Cloaking	7070, 8080
Real, pre-G2	RTSP	7070	HTTP Cloaking	7070, 8080

Note, for the most up-to-date data for each media type, please refer to the links below pertaining to Windows Media and Real Media formats and their respective firewall settings.

Additional Information

In order to ensure that end-users can view and listen to streaming media in either the Windows Media or Real Media format, your firewall must be configured to accept streaming media content through the appropriate ports. Your corporate network administrator can configure your firewall or proxy servers to properly enable the necessary two-way communication. Information on configuring corporate firewalls for streaming media can be found at the following links:

Windows Media

Go to http://support.microsoft.com for assistance with Windows Media Services on corporate intranets. Specifically, refer to the articles on "*Firewalls and Ports Used by Windows Media Services*" at:

http://www.microsoft.com/windows/windowsmedia/serve/firewall.asp

and

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q189416

Real Media

Go to http://service.real.com/firewall/index.html for more information on the Real Media format and firewalls. Specifically, refer to the "*Firewall Admin Support"* links for information on configuring your proxy server/firewall to enable the Real Media format across your firewall:

http://service.real.com/firewall/fadmin.html

and

http://service.real.com/firewall/adminfw.html