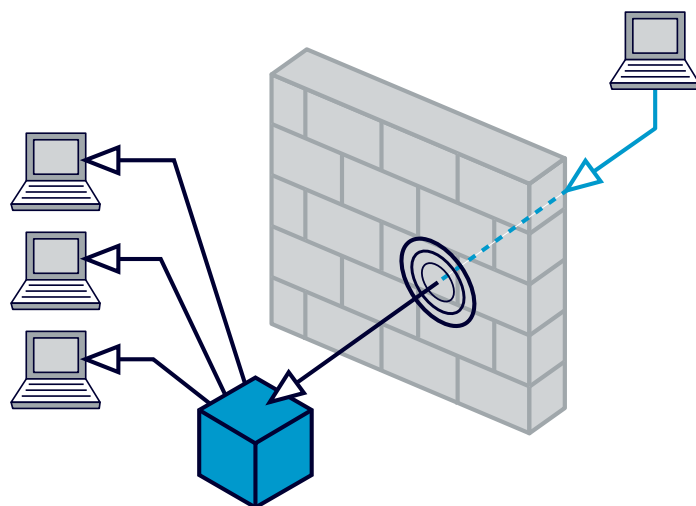


Webcasting: Penetrating the Firewall

by Chris Bartot, Senior Producer

If you browse the web while you are at work, you have probably heard the term firewall.

A firewall is a special hardware and/or software package dedicated to monitoring data transmitted from inside the company and received from the outside World Wide Web. Through a series of filters or rules, certain data is allowed to pass through the wall, while other data is dropped. In this day and age where computer viruses and hackers run rampant, a firewall provides a much needed and sometimes massive measure of security, protecting your company's data from outsiders while preventing users from visiting malicious websites that are equally damaging.



Here's how it works:

Let's say that there are 500 employees in your company. The company will therefore have hundreds of computers with network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T-1 or T-3 lines. Without a firewall in place, all of those computers are accessible to anyone on the Internet. A hacker can probe those computers and make connections to them. With a firewall in place this cyber intrusion is less likely.

As much security and safety as a firewall offers, events like webcasts are often blocked, too, because they involve an active and on-going data stream from an unfamiliar source. If a large number of internal users are logged onto the webcasting stream at one time, your company's overall network usage and speed can be burdened. Imagine those 500 employees using 500 kbps (kilobits-per-second) or 50,000Mbps of simultaneous streaming. If your company only has one T-1 line, your network could be crippled for those employees who are not participating in the webcast.

When approaching a webcast project, it's important to form a close partnership with your Information Technology team, starting the process as far in advance of the live event as possible in order to address the firewall and any connectivity issues it may pose. This is not normally a simple procedure. A firewall is not a piece of technology that can be toggled on and off like a light. Never underestimate a company's firewall. Never just hope for the best. Always, do your homework and have more than one solution in case of hurdles, as no two firewalls are alike.

Pre-Webcast preparation involves testing all segments of the Webcast's path from the point of origination to a viewer's computer. To help illustrate the relationship between firewalls and Webcast engagement, let's take a look at a recent project.

Webcasting: Penetrating the Firewall (continued)

Quicksilver Example

Earlier this year, Quicksilver produced a live, 3-day Webcast for a global human resources consulting firm. Historically, they had held an annual face-to-face meeting for their leadership team. The state of the economy prompted them to look for an alternative means to effectively communicate messages to their large and dispersed internal audience. They chose to produce a Webcast. Upon engaging Quicksilver the decision was made to originate the live event from the Milwaukee headquarters of their parent company, in a brand new building with a brand new computer network.

With less than three weeks before the first live event, Quicksilver's Webcast producer and live streaming specialist immediately opened a line of communication with the client's IT teams in Philadelphia and Milwaukee. The strength of the



company's firewall and the fact that a live Webcast had not yet been attempted, required careful planning. First, we requested four IP (Internet Protocol) addresses for

our streaming computers. These addresses were needed to allow the streaming computers to "talk" to the client's network and route data between networks. Quicksilver traveled to Milwaukee for a day to perform our first live test from the room where the Webcast would originate.

The plan was to send a full motion video and audio signal through main and back-up devices, which converted the feeds to high- and medium-bandwidth media streams. From there, the live streams went into the wall and began their journey to our webcast portal in Minneapolis. Prior to arriving on-site, we had entered the proper IP addresses into our computers' network settings. However, immediately upon connection, the client's firewall stopped our outgoing streams dead in their tracks.

Why? Because, the proper ports needed for sending video and audio data through the firewall had not been opened. This was a process that would take 2-3 days because the switches for the client's network were in a hosting facility in another part of the city. Once the proper ports were opened, the video and audio streams passed through as planned and made their way to the Webcast portal.

From there, we were able to route the signal through the Web interface and see an example of the Webcast



as it would play during the live events. To summarize, conduct streaming and IT tests as far in advance of the live Webcast event as possible, minimally one week prior. Never take anything for granted, especially not technology. Remember also the more pre-production and planning you do, the fewer the surprises you'll experience on-site. Oh, there will still be surprises on site, but experienced Webcast producers are ready for almost anything – once we make it past the firewall!

Chris Bartot is celebrating 12 years as a senior producer with Quicksilver Associates. Webcasting is a natural extension of his finely honed skills as a meeting and video producer for such global clients as the Young President's Organization, Microsoft and Right Management.

Quicksilver has been producing successful global Webcasts since 2000 for clients ranging from consulting firms to technology manufacturers to healthcare financial services organizations.

[Click on this link](#) to view three case studies or [contact our sales team](#) for more information on Quicksilver's Webcasting solution.