

Why broadcast systems need a media firewall

By Stewart McGhie
Head of Sales
Crystal Vision Ltd.

There is currently a good deal of interest in firewalls for uncompressed video over IP. Creating an IP-based broadcast facility allows huge flexibility in the way the system is used and systems designers will create restrictions on their network to suit the individual requirements.

This paper is intended to explore the areas where broadcasters are using a media firewall as well as explain the features that the perfect media firewall should include.

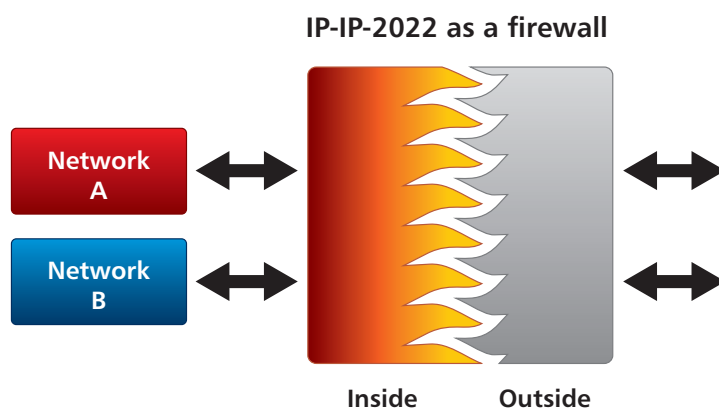
Off the shelf?

If you use a standard “off the shelf” IP switch as a firewall you are reliant on the correct rules having been entered into the system and you are limited to the level of packet inspection that can be carried out.

By contrast, a dedicated firewall product like Crystal Vision’s IP-IP-2022 (a software app running on the MARBLE-V1 media processor and used with SMPTE ST 2022-6 signals) automatically stops everything going through apart from video and audio – as well as including features which sort out all the issues that people are having.

Where are we seeing requirements for a media firewall?

A major application for firewalls is when connecting to the cloud – which allows huge flexibility and scalability of broadcast systems. However cloud services follow standard Internet protocols and practices which is not always appropriate for broadcast systems. The IP systems within broadcasters are being built with a different set of requirements than the general Internet. Therefore a firewall should not only stop unwanted connections and data flows, but should also offer some translation functionality.



There are similar requirements when providing signals to and from Telcos. Although possibly a more closed connection, it is likely that the security of the firewall will still be required. Although the connection may not, in theory, be readily available to the World Wide Web, the reality is that you never actually know *what* can connect to your system, either intentionally because you want to provide open access to your clients or partners, or because someone has hacked a router somewhere and opened up a connection to your system.

Firewalls are regarded as essential for connecting together “inside” areas (within the control of the broadcaster) and “outside” areas (where the control is now with someone else). There is additionally a growing requirement for connecting two “inside” areas together, As well as limiting who or what within your own organisation can connect to a sensitive IP signal distribution system, there are also cases where different options, IP parameters or protocols have been selected for one area of your system compared to another.

What features does the perfect media firewall need?

Some of the applications might not be traditionally considered part of a firewall, but are required for separating one area of video over IP from another.

Network security

Security in IP systems is multi-layered and a media firewall adds a further level to what can be programmed into the IP switch. The switch usually has been designed to pass all data and then additional controls have been put on to try to limit the data types, whereas a dedicated media firewall has been specifically designed to pass only the allowed media data types. This means that there are no user controls to pass other data types.

With Crystal Vision’s IP-IP-2022 app general data packets do not pass through; only the media data can be passed through. There is a media processing core which all data must pass through and if required the video and audio media is processed or delayed as its native data format.

Control of the IP-IP-2022 software app is via dedicated 1Gbit Ethernet ports to the Vision 3 frame, completely isolated from the 10Gbit data ports in the MARBLE-V1. There is no risk of unauthorised control from remote areas that only have access to the data on the 10Gbit ports.

Unicast or multicast

Broadcasters’ IP systems typically have all the media signals sent as multicast (one to many) within their own building. However many Telco-based IP transmission systems require or supply signals in unicast (one to one). A media firewall can be a convenient place to convert from one or the other. This allows an incoming unicast stream to be sent into your system as multicast and so allowing a number of receiving devices to pick it up.

Network Address Translation

The IP address range you use within your facility is likely to be different from the outside world address ranges used by Internet providers. For example internally you may use 192.168... etc. but the connection provided to you may require 96.98... etc. A good firewall will provide

network address translation. Crystal Vision's IP-IP-2022 allows every possible configuration of IP addresses. On a single hardware connection it can provide up to six different IP address translations, each with its own separate VLAN setting.

Data shaping

Each media data stream, whether 1.5Gbs or 3Gbs, is much lower than the 10Gbs bandwidth of Ethernet and so the data is sent as packets with gaps of no data between. The size of the gaps with no data is an issue for the receiving equipment as many types of processing require a constant flow of data as they would normally get with SDI video.

Within the broadcast site itself, data shaping is likely to be a major requirement in the early IP installations. Some converted broadcast equipment is very fussy about having all the data packets evenly spaced, whereas other IP products running on PCs have wide packet distribution (big gaps) where packets are not evenly spaced. Even when the data stream has packets that are created with an even spacing it will become less evenly spaced when they are passed through busy network switches, as any clashing of packets is dealt with by adding delays to one of the packets.

Data shaping as defined in ST 2110-21 is now considered part of the ST 2022 standard. Many installations insist that everything on the local network meets the narrow (evenly spaced) specification. Crystal Vision's IP-IP-2022 app will accept wide distribution (big gaps) and produce a constant narrow output. This is particularly useful when taking IP media from the cloud, as a blade server will often not provide narrow packet distribution and so using the IP-IP-2022 would therefore ensure the incoming feed has the correct data shaping required to meet the SMPTE specification.

Producing narrow distribution IP streams normally involves the expense of dedicated 'broadcast' hardware products. However, areas of a station can be designated as using wide distribution which would allow the use of low-cost standard PCs or blade servers, with the IP-IP-2022 then used to connect these 'wide' areas to the 'narrow' areas. It is probable that all equipment will eventually be made to be tolerant of wide packet distribution – but in the meantime sensitive equipment needs protection.

Flexible redundancy

While IP systems are generally reliable you cannot always guarantee that 100% of the data packets will make it through a big network. When IP routers get overloaded they will drop packets. The easiest solution to this issue is to send the data out on two separate links. They may be described as Main and Protect. Sending them out of two physically separate connections also ensures that should one cable get unplugged or one router fail, you will still have the other carrying the data.

Crystal Vision's IP-IP-2022 app runs on the MARBLE-V1 hardware. This is a media processor which has four 10Gbit Ethernet ports. This allows Main and Protect to be available on both input and output sides of your system. Where a system runs duplicate networks, feeds can be taken from both networks to increase reliability and allow maintenance. Each media flow can use the ports in a different way, with one or two inputs if using ST 2022-7 and one or two outputs. Flows can go in both directions on a single hardware port and so it can utilise just one connection on either side if necessary.

Summary

Using a dedicated firewall product like Crystal Vision's IP-IP-2022 allows live broadcast IP systems to connect together securely, with redundancy and with the knowledge that all network choices are available on both sides of the firewall.