

Streaming Video and Firewalls

Is It Safe?

Firewalls exist to prevent unwanted data from passing between any two networks. Typically, one network is your LAN (also known as your “inside” network), and the other the public Internet (also known as the “outside” network).

With network horror stories reaching urban legend proportions, network administrators and their firewalls are faced with the impossible task of “proving a negative” -- make the network safe from all possible dangers. If data from the “outside” is to be allowed to enter the “inside” network through their firewall, they are asked to prove it is safe. The smart network administrator already knows that the only truly “safe” configuration is one where the power is switched off, so obviously we all must live with some level of risk if we are to benefit from the enormous gains modern network computing has brought us.

Fundamentals

All networking is based on the concept of “senders” and “receivers”. In the last few years, a new concept has entered our networking lexicon, “good guys” and “bad guys”. You, we assume, are among the “good guys”. The “bad guys” wish to use the public Internet to enter your network and steal or damage something.

Think of your network as an airport terminal with a long hallway with many gates. To reach the gates you must show your boarding pass (e.g. IP address, port number, protocol, etc.). The fact that you may pass through security does not guarantee you will be getting on an airplane (the flight could be cancelled). The firewall in your network is similar to this security checkpoint (indeed, like the airport security, you will want to size your firewall to deal with the expected traffic to minimize delay).

To continue the airport analogy, let's assume you arrive in the terminal hallway but your flight is cancelled. In other words, there is no "receiver" for you. You can wander around the terminal all you like, but you can't pass through a gate.

So it is with networking. A data packet that arrives in your network simply cannot do anything unless it is received. A theoretical "packet of death" that passes through a firewall can do nothing unless it is received. There must be an active device with that packet's destination address and port number in order for it to be received. And the receiver must be susceptible to bad things happening if the "packet of death" is received on that specific port number.

The Rub

To receive streaming media efficiently, you might choose to open a number of UDP ports on your firewall. But before you do this, you are asked to prove nothing bad will happen now or at any time in the future. In other words, you are asked to prove a negative -- a virtually impossible task (and of course, if you open the ports and some time later an unrelated network event occurs, what will be the most convenient thing to blame?).

It is common for network administrators to block UDP traffic, citing unarticulated "security concerns". Indeed, it is good practice to block everything that you do not specifically want. Unfortunately, blocking UDP for streaming video has an unintended consequence. Video servers and their desktop players simply negotiate to use http (port 80 or sometimes port 8080) via "tunneling". The same data arrives at the same computer and from the same source, but with more overhead. Delivering that same data with more overhead does not increase security. Moreover, the increase in overhead translates to a decrease in efficiency that directly affects the Internet access connection utilization, for which most organizations pay a monthly fee. In other words, blocking UDP as a matter of universal policy can actually cost a company more money than if they did not block all UDP.

NAT

Even the least expensive home access router uses Network Address Translation, creating an “inside” network that is isolated from the “outside” network. Perhaps the computer on your “inside” network has an address of 192.168.1.100 while your Internet Service Provider has given you an address of 204.80.240.121.

Someone on the “outside” cannot reach your 192.168.1.100 computer even when they know your 203.80.240.121 address. Your router/firewall simply blocks any packets that come from the “outside” unless it is in response to a request made by you.

Streaming media is no different. No traffic, either UDP or HTTP gets through your router unless you have requested it, and if it arrives via UDP, so be it.

Port Scans

Bad guys can take your outside address and attempt to access every possible address and port. Several firewall vendors offer online tools that will conduct a port scan on your network (see <http://scan.sygate.com/quickscan.html> for an example). Warning: firewall vendors are motivated to suggest an open UDP port represents a security hazard. As discussed earlier, the fact that a range of UDP ports is open does not, by itself, represent a security concern.

Inbound and Outbound

Some firewalls can be configured to block both inbound and outbound traffic. Blocking outbound traffic does not appear to be necessary to address security concerns, but may be present for other “unknown” reasons. Perhaps an organization wishes to limit

UDP Port Scanning

While the UDP protocol is simpler than TCP, scanning it is actually significantly more difficult to do. This is because open ports don't have to send an acknowledgement in response to a probe, and closed ports aren't even required to send an error packet. Some hosts do send an ICMP_PORT_UNREACH error when you send a packet to a closed UDP port. Thus you can find out if a port is NOT open, and by exclusion determine which ports are. Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners must also implement retransmission of packets. Scanning is typically quite slow because of compensation for machines that comply with RFC 1812 and limit ICMP error message rate. Because of the difficulty and richer hunting grounds, UDP port scanning is not often not conducted but any open port could represent a security concern.

Ping relies on Internet Control Message Protocol packets. Therefore no "ping" tool (windows, unix, etc.) can "ping ports". Remember that ports are only reachable at "Layer 4 - Transport Layer" communications involving UDP or TCP. Ping operates only at "Layer 3 - Network Layer" using ICMP (i.e. 'echo request' and 'echo reply' packets).

outbound bandwidth usage, or perhaps it is done as part of a “if you don’t need it open, keep it closed” policy. If sourcing video from within an “inside” network to a reflector (as would be the case with sending MPEG-4 to a reflector service), the selected UDP ports must be opened, and such configuration represents no known security issues.

HTTP Tunneling

As discussed earlier, if UDP is blocked, many players will revert to alternative protocols such as “HTTP Tunneling”. As the name suggests, “HTTP Tunneling” creates a session, not unlike a web page session, between the users client and a streaming server, and uses TCP rather than UDP. TCP uses retransmission and acknowledgement mechanisms that do nothing to enhance streaming media and simply increases the overhead. All too often HTTP Tunnels are used because the IT staff has not opened the necessary ports to allow more efficient streaming.

RTSP

The Real Time Streaming Protocol is a well-established standard for streaming media. With RTSP, a client (a desktop player or a Set Top Box) makes a request to a video source using TCP port 554. The player and the video source then negotiate the ports and the protocol they will use. For MPEG-4, the ports used start with UDP port 6970 through 6973. Each additional viewer is assigned the next four UDP ports (e.g. 6974 through 6977).

Some firewalls have a setting to “enable streaming media”, and they automatically enable RTSP and open the required TCP and UDP ports.

Behind The Firewall

Few organizations install firewalls between departments or on the “inside” of their network. Organizations deploying live and stored video in their private networks and on their VPN’s rarely need to worry about firewall issues.

Multicast

Incredibly, there are some institutions who are connected to multicast-capable networks such as the Internet-2 yet have firewalls configured to block all multicast traffic. Certainly multicast should be blocked if the outside network does not support it. Sending multicast to a typical ISP will result in a continuous spewing of error messages from the ISP's router. But if the network supports multicast, you are very lucky because it is the best way to participate in the most bandwidth efficient way to collaborate and to view broadcast quality video.

Common Ports

Data	20	FTP	21
SSH	22	Telnet	23
SMTP	25	DNS	53
DCC	53	Finger	79
WEB	80	POP3	110
IDENT	113	LOC	135
NetBios	139	HTTPS	443
Server Msg	445	SOCKS	1080
UpnP	5000	WEB Proxy	8080
Popular Trojans	1243, 1999, 6776, 7789,12345, 31337, 54320, 54321		

[Related Reading: Streaming Live MPEG-4, the V-Basics](#)