

White Paper

VCON

Video over IP (H.323) Conferencing and Security: How to Conduct Videoconferences with Firewalls and Proxy Servers



Sept 2000



The Video over IP Company

Table of Contents

Introduction

Definition of a Firewall

Definition of a Proxy Server

General Issues Relating to Videoconferencing and Firewalls

Intelligent Firewalls and the H.323 Solution

Trusted Information Systems Gauntlet Family of Firewall Products

Enhancing Security with Proxies

VCON Compatibility

Current and Future Capabilities of VCON Pertaining to Firewalls

Other Videoconferencing Vendors and Firewalls

Sara Morris
Technical Support

Introduction

When crossing a firewall, the H.323 protocol requires the use of certain static ports as well as a number of "dynamic" ports, i.e. ports which are selected at random from anywhere within the range of 1024-65535. In order to enable this to take place, all ports within this range must therefore be kept open to all traffic. This clearly compromises the ability to guarantee the security of an intranet and would render a firewall virtually ineffective.

In this document we will describe how it is possible to configure an intelligent firewall to "snoop" on the control channel in order to determine which dynamically-selected ports are in use for a given H.323 session. The firewall will then be capable of only allowing traffic through these specific ports and only for the period during which the control channel is active. We will also explain how even greater security can be achieved with the addition of a proxy server.

Definition of a Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users of other networks. (The term also applies to the security policy that is used with the programs.) An enterprise with an intranet which is connected to the wider Internet normally installs a firewall to prevent outsiders from accessing its own private data resources and to control which outside resources its own users have access to.

A firewall works closely with a router program to filter all network packets and to determine whether to forward them on to their destination. A firewall also includes, or works with, a proxy server that makes network requests on behalf of workstation users. A firewall is generally installed in a specially designated computer, separate from the rest of the network, so that no incoming request can directly access private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. For mobile users, firewalls allow remote access to the private network by means of secure logon procedures and authentication certificates.

A number of companies make firewall products. Features include logging and reporting, automatic alarms at given thresholds of attack and a graphical user interface to control the firewall.

Definition of a Proxy Server

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security and administrative control and provide a caching service. A proxy server is associated with, or is part of, both a gateway server, that separates the enterprise network from the outside network, and a firewall server, that protects the enterprise network from outside intrusion.

A proxy server receives requests for Internet services (such as a Web page request) from a user. If the request passes filtering requirements, the proxy server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without the need to forward the user's request on to the Internet. If the page is not in the cache, the proxy server acts as a client on behalf of the user and uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server forwards it on to the user.

The proxy server is invisible to the user; all Internet requests and returned responses appear to be directly addressed to the Internet server. (The proxy is not quite invisible as its IP address has to be specified as a configuration option to the browser or other protocol program.)

An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. In fact, there are special servers called cache servers.

General Issues Relating to Videoconferencing and Firewalls

Signaling

H.323 uses only one well-known port (1720) for Q.931 signaling (Q.931 is the call signaling protocol for setup and termination of calls). Ports or sockets used for H.245 signaling for audio, video or data channels are dynamically negotiated between end points. This use of dynamic sockets makes it difficult to implement security, policy, and traffic shaping.

H.323 data conferencing uses both "reliable" (TCP) and "unreliable" (UDP) communications. Reliable transport is required for control signals and data, because signals must be received in proper order and cannot be lost. Unreliable transport is used for audio and video streams, where time-sensitivity becomes the priority.

Delayed audio and video packets are dropped. Consequently, TCP is applied to the H.245 control channel, the T.120 data channels and the call signaling channel while UDP is applied to audio, video, and RAS channels.

The H.323 Protocol

The H.323 standard is a logical extension of the H.320 standard to enable corporate intranets and packet-switched networks to transport multimedia and conference traffic. The H.323 standard spans the technical requirements for narrow-band visual telephony services that include one or more LANs. H.323 recommendations cover the IP devices that participate and control H.323 sessions and the elements that interact with the switched circuit network (SCN). H.323 standards do not include the LAN itself, nor the transport layer that interconnects LAN segments.

Intelligent Firewalls and the H.323 Solution

Since H.323-compliant applications use dynamically allocated sockets for audio, video and data channels, a firewall must be able to allow H.323 traffic through on an intelligent basis. The firewall must be either H.323-enabled with an H.323 proxy, or able to "snoop" on the control channel to determine which dynamic sockets are in use for H.323 sessions, and to allow traffic through only as long as the control channel is active.

- *Granting access to an H.323 protocol via the firewall.* H.323 is a complex, dynamic protocol, consisting of several inter-related subprotocols. How ports/sockets are allocated and released via this protocol requires a detailed inspection of the H.323 call setup session states as they progress. Some firewalls are intelligent: they support dynamic access control.
- *Network Address Translation (NAT) interaction with H.323 protocols.* If H.323 terminals co-exist with local, interior IP addresses that must be translated to valid exterior addresses using NAT, then the firewall must be able to decode and translate all addresses passed among the H.323 protocols.

Among the firewalls that provide these solutions are the following:

- Check Point Software's Check Point FireWall-1
- Cisco's PIX Firewall series
- Trusted Information Systems' Gauntlet family

Both the Cisco PIX Firewall and Cisco IOS Firewall Feature Set allow H.323 traffic on an as-required basis by "snooping" on the control channel.

Trusted Information Systems Gauntlet Family of Firewall Products

The Gauntlet firewall is an application relay, or proxy firewall - the most secure form of firewall. The Gauntlet H.323 proxy application will monitor and control all H.323 calls between the organization's internal network and the Internet (or between Intranet domains). The proxy can ensure that only valid H.323 traffic is permitted through the Gauntlet firewall. It can also enforce access control policies to determine which users can initiate or receive H.323 calls, what destinations are appropriate, and whether a particular user is allowed to use video facilities.

Enhancing Security with Proxies

When terminals signal each other directly, they must have direct access to each other's IP address. This potentially exposes key information about a network to an attacker. Using a proxy only exposes limited address information, keeping all other terminal and gateway addresses hidden.

Furthermore, the network firewall may not support H.323 signaling. Using H.323 protocols successfully in conjunction with a firewall depends on the degree to which the firewall is capable of dealing with the complex H.323 protocol suite.

If a firewall does not support dynamic access control based on the inspection of session states, a proxy can be used inside the firewall to provide a simple access control scheme. Since the gatekeeper (via RAS) and the proxy (via call setup protocols) are the only nodes which interact with devices outside the firewall, it is easy to set up access control lists on the firewall to pass traffic destined for either the gatekeeper or the proxy directly on to them.

If a firewall cannot translate addresses, a proxy may be used as an adjunct to the firewall. The proxy is placed next to the firewall, with interfaces leading to both the inside network and the firewall. The firewall will not perform the NAT function for traffic directed to the Proxy, and only proxy traffic - i.e. an H.323 protocol that is terminated on the inside and then repeated to the outside, and vice versa - can pass through the proxy server.

Another configuration serves in those instances where it may be desirable to place both proxy and gatekeeper outside the firewall. This works where NAT is not present and the firewall supports H.323-compliant dynamic access control.

The reasons for restrictions regarding NAT and the proxy server are:

- If NAT is active, each endpoint must register with the gatekeeper for the duration of the time that the endpoint is online. This could quickly overwhelm the firewall by requiring it to maintain a huge number of relatively static internal-to-external address maps.

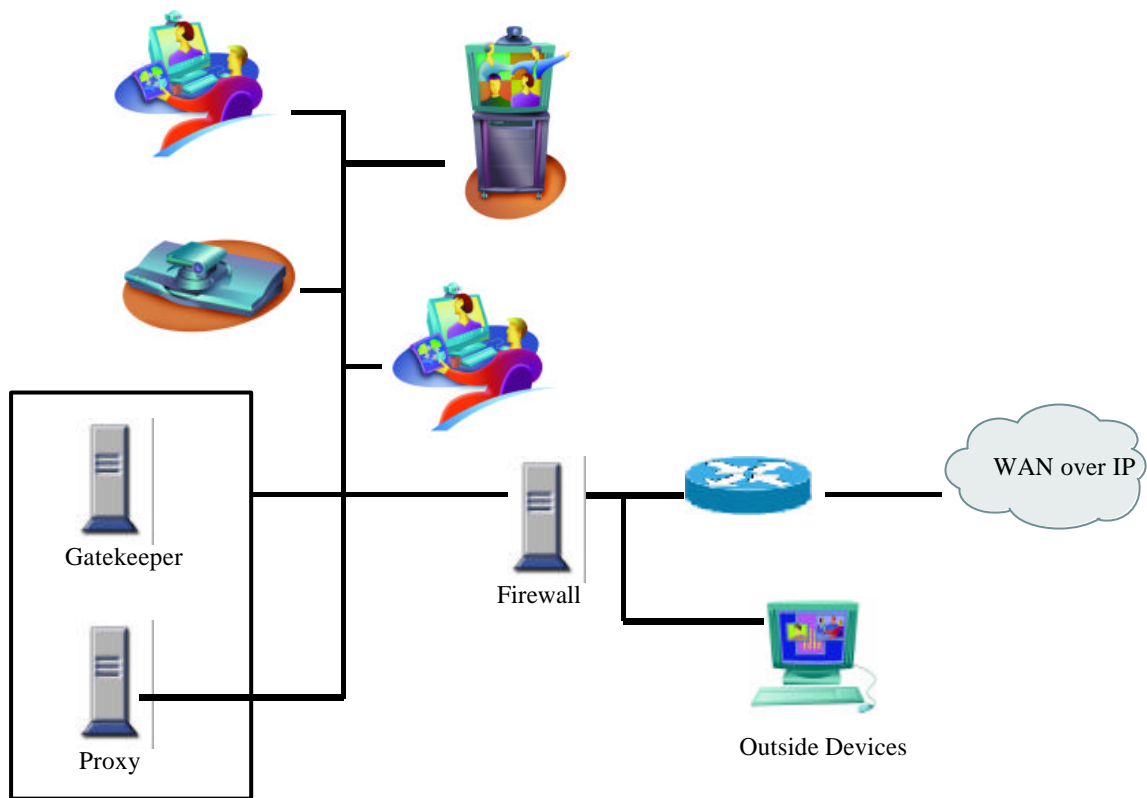


Figure 1: The general placement of a Gatekeeper and proxy in a network.

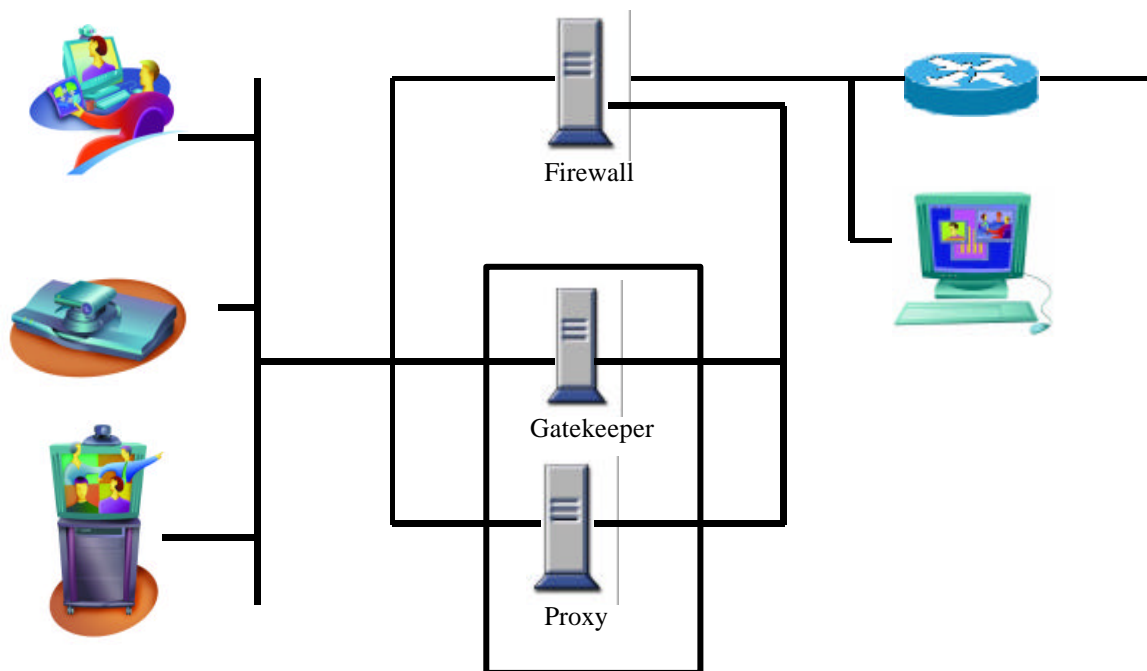


Figure 2: Proxy usage with a firewall doing Network Address Translation.

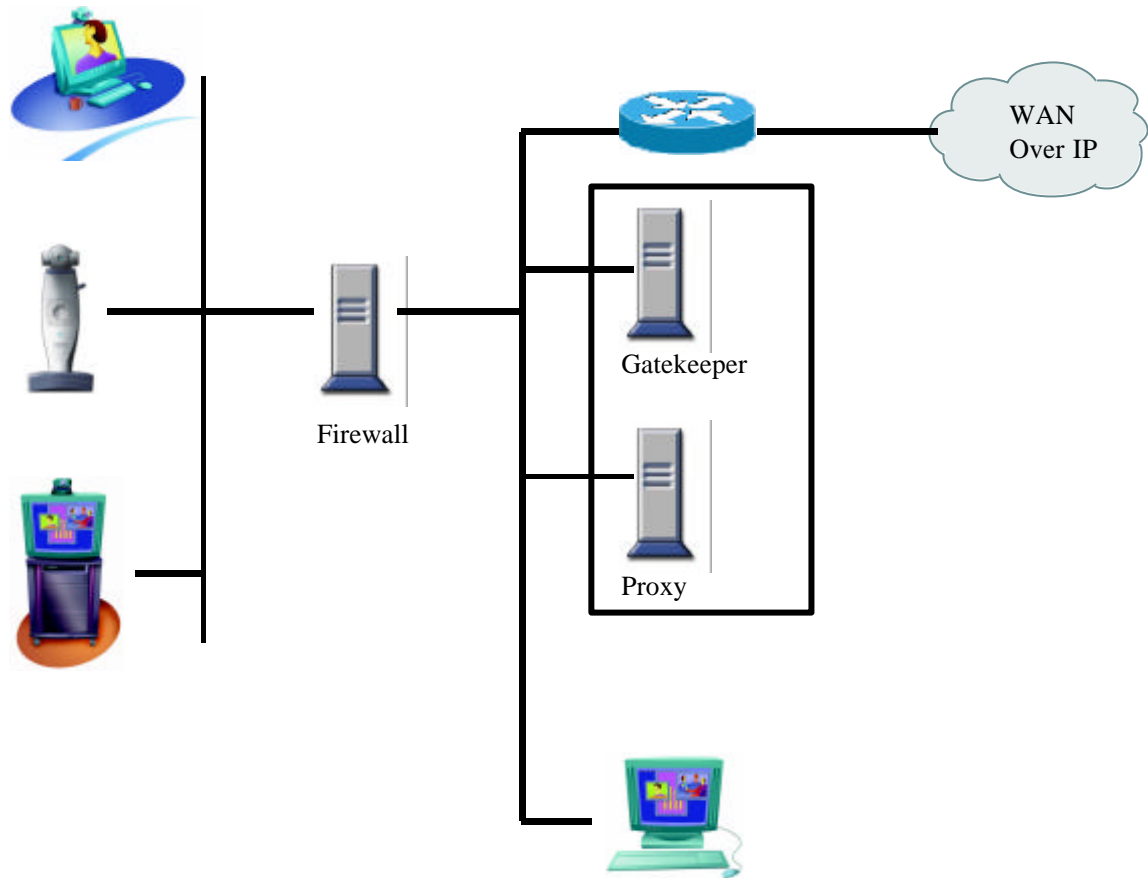


Figure 3: It may be desirable to place both proxy and gatekeeper outside the firewall (when NAT is not present, and the firewall supports H.323-compliant dynamic access control).

- If the firewall does not support H.323-compliant dynamic access control, it could be configured with static access lists for the proxy and gatekeeper nodes, but this renders the network vulnerable to IP spoofing.

VCON Compatibility

VCON software is compatible with any firewall that supports the H.323 protocol. As already explained above, since the H.323 protocol uses dynamic ports, in order to allow VCON videoconferencing traffic through a firewall, all ports in the range 1024 - 65535 (see table below) must remain accessible. This clearly compromises security and would defeat the purpose of the firewall. However, two solutions are available. Firstly, security can be obtained by using an intelligent firewall which is capable of "snooping" on the control channel to determine which dynamically-selected sockets are in use for the H.323 session and

then only allowing traffic to pass through these specific ports for the period during which the control channel is active. Security can be further enhanced by the addition of an H.323 proxy server.

Current and Future Capabilities of VCON Pertaining to Firewalls

It is possible in current versions of MeetingPoint, VCONs videoconferencing software, to control the audio and video streams so that they use static ports. The signaling stream will remain dynamic. The fact that the RTP ports can be controlled means that at least the UDP ports (audio and video streams) can be controlled and do not need to be opened globally. This could be significant, as opening UDP is more risky than opening TCP. Furthermore the VCON endpoint can restrict the range of the media streams. This is done as a configuration change in the registry, but is also a VCON Development Kit (VDK) parameter so it is possible to control the range of ports by a GUI that is written over the VDK.

VCON's Video exchange Manager Server (IP-VxM) is a product that enables the network managers to define the UDP ports per endpoints from a central location rather than needing to manually modify each endpoint's registry

Other Videoconferencing Vendors and Firewalls

This problem is not unique to VCON, it applies to all vendors of media streaming products that are built on the H.323 standard. The solutions that are available to VCON are the same as those recommended by other companies that provide videoconferencing solutions, for example, PictureTel.

PORT	TYPE	DESCRIPTION	H.323 Client	Microsoft ILS	H.323 MCU	H.323 GK
80	Static TCP	HTTP Interface (Optional)		X		
389	Static TCP	ILS Registration (LDAP)	X	X		
1503	Static TCP	T.120	X		X	
1718	Static TCP	Gatekeeper Discovery	X		X	X
1719	Static TCP	Gatekeeper RAS	X		X	X
1720	Static TCP	H.323 Call Setup	X		X	
1731	Static TCP	Audio Call Control	X		X	
8080	Static TCP	HTTP Server Push (Optional)		X		
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)	X		X	
1024 - 65535	Dynamic UDP	RTP (Video Data Streams)	X		X	
1024 - 65535	Dynamic UDP	RTP (Audio Data Streams)	X		X	
1024 - 65535	Dynamic UDP	RTCP (Control Information)	X		X	

White Paper



DOC 11039 Rev1.0 9.00

VCON International
Ph: +972-9-959-0059
Fx: +972-9-956-7244

VCON China
Ph: +86-10-6526-9791
Fx: +86-10-6526-9790

VCON France
Ph: +33-1-5584-0175
Fx: +33-1-5584-0179

VCON GmbH
Ph: +49-6103-7505-7
Fx: +49-6103-7505-850

VCON Inc.
Ph: +1-512-583-7700
Fx: +1-512-583-7701

VCON Japan
Ph: +81-3-5280-7789
Fx: +81-3-5280-7784

VCON Spain
Ph: +34-91-444-0900
Fx: +34-91-444-0907

VCON United Kingdom
Ph: +44-1628-829555
Fx: +44-1628-829777
VC: +44-1628-823366

www.vcon.com

info@vcon.com

The Video over IP Company