LifeSize®

Video Conferencing and Security

Using the Open Internet and Encryption for Secure Video Communications & Guidelines for Selecting the Right Level of Security for Your Organization

LifeSize®

Table of Contents

1. OVERVIEW

This document is created to provide security information and considerations for video conferencing. By ensuring that security is set up properly, mainstream users of video conferencing will have the confidence to use video for a wide variety of applications. At LifeSize, we have a unique perspective on security and due to our advanced, high performance architecture we are able to ensure strong security while maintaining high quality video and feature performance. We also believe that security plays into the total cost of ownership (TCO) for a video conferencing network from two perspectives: 1) we believe that using the open Internet for video communications combined with encryption is a very secure communication method for most applications and reduces the need for more expensive, private network wide area networks (WANs); 2) that there should be no tradeoffs in quality of video or multipoint conferencing when using security features such as encryption – it should be transparent to the user, leading to greater usage and return on investment (ROI). In this paper, we will cover the levels of security to consider, firewall and NAT traversal considerations, our point of view on security, and implementation recommendations.

2. WHO SHOULD READ THIS DOCUMENT

This document is generally written in layman's terms but will be particularly useful to network and IT administrators as well as managers who have primary responsibility for implementing video conferencing solutions and communications technologies on IP networks.

“ At LifeSize, we believe that using the open Internet for video communications combined with encryption is a very secure communication method for most applications and reduces the need for expensive, private network WANs. ”

3. VIDEO CONFERENCING & THE OPEN INTERNET

Video over IP (H.323 and SIP unified communications platforms) has transformed the way we experience video communications. Over the past several years, many technology advancements have aligned to take video conferencing into the mainstream. The three most important changes have been: 1) widespread, inexpensive bandwidth availability; 2) increased processing performance that has improved quality of experience, particularly with HD; and 3) the ability for users to connect with each other easily over the open Internet. High definition video quality over the open Internet is game changing. The adoption and acceptance of video conferencing is at an all time high, and the market is projected to grow at a 16.3% CAGR, from $1.7B to $4.2B in 2014. You could say that video conferencing is crossing the chasm into the mainstream market[1].

*"Crossing the Chasm: Marketing and Selling High Tech Products to Mainstream Customers", Geoffrey A. Moore

High definition quality over the open Internet is game changing.

Wait, we just said "high definition video conferencing over the open Internet". Yes, that's right. It's happening every day, with profound benefits to users and organizations. This does beg the question, what about security. While it is much more challenging to hack a videoconference call than a transaction, it is clear that using video communications must be a secure endeavor.

The use of the open Internet is significant because of the reduced cost and elimination of the need for running video over a secure, MPLS enabled WAN. There are a large number of organizations moving away from expensive private WANs because the open Internet is so reliable and highly effective. This may not be true for all applications, but considering the cost can be 40% less, it makes the case for dramatically reducing the total cost of ownership (TCO) of video communications, especially when it can be delivered securely using advanced encryption methods.

Read on to learn about various applications and our stance on security. The goal is to keep the network as open as possible so that people reap the benefits of high quality, cost effective video communications and do so in a secure manner.

4. VIDEO CONFERENCING SECURITY TIERS

a. MAINSTREAM APPLICATIONS

For most video conferencing applications, we believe that video over the open Internet with AES (128-bit, SSL) encryption enabled is very secure. This is the same encryption used by financial institutions that offer online banking, ecommerce and customer relationship management systems (CRM). CRM systems host an organization's complete customer and prospect database with access via the open Internet using 128-bit AES encryption. The world's largest financial institutions and retailers trust encryption for online transactions over the Internet. A good example is Salesforce.com, the leading CRM system. Salesforce.com uses AES encryption and serves customers such as Dell, Amazon and many others who certainly take their data very seriously. Read Salesforce.com's security document: http://www.salesforce.com/assets/pdf/datasheets/security.pdf

b. DEDICATED NETWORKS

There are some institutions for which the open internet is not a viable option for their applications and desired security levels. This requirement often has more to do with guaranteeing a certain level of quality of service (QoS) more so than security needs. In cases where a certain level of security must be achieved, we recommend combining a secure, dedicated LAN or WAN network with encryption. In some cases, the user will choose to use an MPLS

(multiprotocol label switching) network to prioritize traffic and offer service levels. In this environment, out of network calls for some organizations are "off limits" or encryption may be used in combination with a properly configured firewall and NAT traversal solution.

c. GOVERNMENT & MILITARY (CLASSIFIED)

The highest level of security is a custom security application often employed by government agencies and the military. In this case, the security is not commercially available and the open Internet is not a viable option. Specially designed algorithms and hardware are utilized to provide certified, government-grade encryption.

5. ENCRYPTION

a. ENCRYPTION WITHOUT SACRIFICING QUALITY

At LifeSize, we strongly recommend using AES encryption for video conferencing calls. One of the objections to using AES is that it could degrade video quality or features by using some of the processing resources to perform the encryption algorithm. While this may be the case with some vendor systems and legacy architectures, only LifeSize can operate with encryption while maintaining the industry's highest quality video and audio and key features that make the experience natural and effective.

The world's largest financial institutions and ecommerce retailers rely on 128-bit AES encryption for billions of transactions.

The use of encryption combined with a properly configured firewall will ensure a secure video network. Moreover, it will allow the organization to leverage the immense benefits of the open Internet without requiring a dedicated network or secure WAN. This makes connectivity far easier and less expensive. These are key parts of a well-used video network resulting in stronger return on investment.

The purpose-built Full HD architecture of LifeSize Room 200 supports AES enabled point to point calls and multi-party calls with up to 4 sites in continuous presence in full HD 720p60 and 1080p30 quality.. This is true whether customers choose to use the H.323 protocol or the SIP protocol for their video communications. Fundamentally, we believe that you should not have to choose between security and the highest quality, most immersive communication experience for users.

Because of the performance advantages of the purpose-built, LifeSize HD architecture, users will not experience reduced quality to operate with encryption. This is very significant for video conferencing security and should be a key consideration when investing in systems. While other vendors are beginning to develop more cost-effective, HD capable systems that emulate LifeSize, their systems often require difficult tradeoffs and limit performance. The result is that users may experience degradation in quality to perform encryption, or may not be able to operate all features. All LifeSize encryption is standards-based and can interoperate with other platforms.

Operating on-demand video communications over the open Internet is secure and highly cost-effective for over 90% of the industry's applications.

b. ENCRYPTION BACKGROUND

Encryption is the process of transforming information to make it unreadable to anyone except those possessing the key. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many types of civilian systems. Encryption is also used to protect data in transit, for example data being transferred via networks. Encrypting data in transit helps to secure it since it can be difficult to physically secure all access to networks or electronic communications.

c. METHODS CURRENTLY USED IN VIDEO CONFERENCING

i. AES - Advanced Encryption Standard became a standard by the National Institute of Standards and Technology (NIST) in 2002. AES is a standard that was adopted by the U.S. government with approval for the use of AES to protect classified information in 2003. The standard comprises three block ciphers, that can be implemented with a 128, 192 or 256-bit key.

ii. DES - Data Encryption Standard (DES) is a block cipher that was selected by the National Bureau of Standards as an official Federal Information Processing Standard for the United States in 1976. It is based on a symmetric-key algorithm that uses a 56-bit key. The cipher has been superseded by the Advanced Encryption Standard (AES).

iii. Triple-DES (DES3) - This is an approach that applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Triple-DES with three independent keys has a key length of 168 bits, but it provides the effective security of a 112 bit key.

iv. GOVERNMENT SECURITY - The government uses their own proprietary algorithms and hardware that are not commercially available to provide high levels of security for classified communications. Examples include: KIV7 and KG194.

6. FIREWALLS

Firewalls have become an essential part of securing a corporate LAN and are widely used. Video conferencing calls must be able to interoperate with firewalls to maintain corporate security and provide secure video conferencing calls inside and outside of the organization. This enables secure communications with customers, partners, suppliers and colleagues around the globe who are not within the corporate LAN or WAN. The challenge is that conducting video calls requires the opening and closing of communication ports, potentially leaving networks vulnerable to attacks and security issues. Firewall and NAT traversal need to be standards based and easy to use and manage.

a. FIREWALL/NAT TRAVERSAL BACKGROUND

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt or proxy all

computer traffic between different security domains based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized video conferencing users from accessing private networks, such as intranets, connected to the video conferencing. All data entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firewalls can present a challenge for H.323/SIP video conferencing. A solution is needed to ensure strong security while traversing a firewall for high quality video and audio communication in keeping with the corporate or institution's security policies.

There are a few types of firewalls and NAT implementations. Some firewalls have multiple attributes:

i. Packet Filtering: This method looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly common, effective and transparent to users.

ii. Application gateway: This method applies security mechanisms to specific applications, such as Telnet and FTP servers. This is very effective, but can degrade performance in some implementations.

iii. Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

iv. Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

v. NAT (network address translation): NAT is a general term for techniques that establish and maintain TCP/IP network connections traversing network address translation (NAT) gateways. NAT is often used in conjunction with firewalls. NAT enables the use of a range of IP addresses internally, while sharing a smaller range of public IP addresses. Internal users will be able to see the public video conferencing, but the public video conferencing users can't see individual devices on the internal side of the NAT.

vi. DMZ: A DMZ or demilitarized zone is another segment of a LAN and is a subnetwork that contains and exposes an organization's external services to a larger, untrusted network. A DMZ adds an additional layer of security to a LAN so that an external hacker only has access to equipment in the DMZ, rather than the whole of the network. Video conferencing endpoints can be deployed in the LAN on the WAN (not recommended because they can be attacked) or in a DMZ.

b. ADDRESSING FIREWALL AND NAT TRAVERSAL

One typical way to address firewall and NAT traversal is an enterprise-class firewall and NAT traversal solution that supports tunneling.

As an example, LifeSize offers a product called LifeSize Transit™. It enables end points to communicate with each other through firewalls without the need for intermediate nodes or unsafe opening of communications ports.

When looking for a firewall or NAT traversal option, it is important to select a standards-based solution. In the case of LifeSize Transit, it supports both H.323/H.460 and SIP/STUN-TURN-ICE.

Video endpoints should be preconfigured and ready for use with the firewall and NAT traversal solution. All LifeSize endpoints are enabled with standards based H.460 and STUN-TURN-ICE software, out of the box at no additional cost.

Where you deploy the firewall is another key consideration. Often the IT organization will deploy firewalls in the demilitarized zone (DMZ). The DMZ should be setup to only allow traffic in/out on ports 1720 (H323 signaling), 5060 (SIP signaling) and user configurable ports. This will ensure the SSH, SNMP and HTTP/HTTPS ports are not open to attack. If the customer prefers a LAN deployment and chooses to not use Static NAT, then LifeSize Transit can be used for firewall/NAT traversal.

7. ISDN Networks

While most networks are moving to an IP H.323 network, there are still some networks in migration. Some networks are mixed IP and ISDN. ISDN has traditionally been a secure environment, and it is very difficult to intercept an ISDN video call. In order to do so, one would need to access at least one of the ISDN switches during a call. There are also multiple B-channels and in some cases multiple switches to contend with and bonding would need to occur to tap into the call. In addition, ISDN calls can be encrypted.

8. GOVERNMENT COMPLIANCE: FIPS, JITC & IPv6

Video communications solutions for use in government and military applications require special certifications and security credentials. Depending on the requirements, the following standards or credentials apply:

a. Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal Government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.)

The LifeSize Cryptographic Security Kernel has been placed on the In Process Listing for the Federal Information Processing Standards Publications (FIPS) 140-2 Validation: Security Requirements for Cryptographic Modules. Additional information is available upon request.

b. Joint Interoperability Test Command (JITC) provides interoperability testing provides a full-range of testing, evaluations and certification services to support rapid acquisition and fielding of global net-centric war-fighting capabilities.

LifeSize has been placed on the Department of Defense's (DoD) Unified Capabilities (UC) for Video Conferencing equipment testing schedule to obtain an interoperability and information assurance certification from the Joint Interoperability Test Command (JITC).

9. SUMMARY

This is an exciting time for people and organizations who need to take advantage of the many benefits of video communications. With strong encryption, video conferencing over the open Internet is secure. Mainstream users can meet face-to-face cost-effectively, without needing private WANs. And with the LifeSize's purpose-built Full HD architecture, users can do so without experiencing performance tradeoffs. No longer is video only for top executives using a private corporate network. Secure video over the open Internet makes video communications so cost-effective that it can be widely deployed for inter-organization communication in offices, conference rooms, homes, educational institutions and many other environments. Now you can have video conferences with virtually anyone you need to at any time - securely. Strong encryption technology combined with properly set, enterprise-class firewall and NAT traversal provides a secure method of communication. LifeSize is committed to providing industry leading, standards-based solutions – delivering the highest quality and best customer experience without compromising security.

Corporate Headquarters:
901 S. Mopac Expressway
Building 3, Suite 300
Austin, Texas 78746 USA

Phone: +1 512 347 9300
Fax: +1 512 347 9301
Email: info@lifesize.com
www.lifesize.com

EMEA:
LifeSize Communications, Ltd.
United Kingdom
Phone: 008000 999 09 799

APAC:
LifeSize Hong Kong Ltd.
Hong Kong
Phone: +852 8239 3695