Vidyo™

Personal Telepresence

TECHNICAL NOTE

Secure VidyoConferencing

Protecting your communications

www.vidyo.com
1.866.99.VIDYO

SECVIDYO_110510_TECHNOTE_US

A holistic approach to secured communication

Vidyo has made telepresence both personal and affordable with its revolutionary VidyoRouter™ architecture that leverages Scalable Video Coding (SVC), enabling end users to participate in high quality Vidyo™ conferences from just about anywhere using standard broadband Internet connections. While the Internet affords us great flexibility in access and endpoints, we also recognize the importance of protecting sensitive information transmitted over this medium from would-be hackers with malicious intent. This document provides an overview of the features of Vidyo's Secure VidyoConferencing[SM] option, designed to guard the integrity of your network and keep your communication and private information safe.

More than just encryption

- User authentication/ login
- Component authentication
- Component access protection
- Database protection
- Signaling encryption
- Media encryption
- Secure firewall traversal

Key Security Features

- AES-128 bit media encryption
- HTTPS with certification login
- TLS with certification for signaling
- Password hashing in database
- New component blocking for spoof prevention
- Hardened Linux based appliances for component access control
- Optional firewall traversal using built-in VidyoProxy™ software
- Optional explicit IP-to-IP firewall traversal using cascaded VidyoRouter™ deployment
- Encrypted token technology for session security
- No login information kept at the desktop

User login and database security

Ensuring that only administered users and administrators are able to gain access to user accounts and the system administration portal respectively is fundamental to securing the VidyoConferencing system. Vidyo establishes this critical front line of defense in a similar manner to the way online banking access is secured. With secure VidyoConferencing system option enabled, the VidyoPortal™ automatically establishes an encrypted HTTPS channel with the each Vidyo endpoint that attempts to access the system and performs certificate exchange, issued by third party certifying authority. Once certificate verification is completed, login and password information is transmitted securely to the VidyoPortal over the same encrypted HTTPS channel.

To safeguard user login credentials, no login information is kept at the VidyoDesktop™ client and the password information is always hashed in the database. Additionally, VidyoPortal connections to the database are done over secured HTTPS links.

Media Encryption

To ensure that the content of your Vidyo conferences cannot be intercepted and decoded without your knowledge, Vidyo employs AES-128 bit encryption over SRTP for audio, video and shared content. A set of keys is used for each form of media for each leg of the Vidyo conference. The VidyoRouter decrypts and re-encrypts each media stream as it passes through for unprecedented security from one endpoint to the

other over public networks. With media encryption enabled for the system, a single VidyoRouter is able to support 70 concurrent HD 1080p connections, significantly more capacity than MCUs costing 5 to 10 times as much.

Based upon general purpose Intel architecture, Vidyo is poised to take advantage of the AES-IN instruction set and leading edge Intel processors for even higher levels of performance and security. At the 2010 Intel Developers Forum, Dadi Perlmutter, Executive Vice President of Intel Architecture Group, demonstrated an AES-256 bit encrypted multipoint Vidyo conference on the next generation Sandy Bridge platform, leveraging the AES-IN instruction set. There was a 10X increase in decryption/encryption performance using the AES-IN instruction set.

Signaling Encryption

Signaling is the way different components within the Vidyo architecture communicate with one another. Ensuring that the information that is passed in this machine to machine communication is not viewable by would-be hackers is important for securing the network. Secure VidyoConferencing leverages HTTPS with certificate support for all web access signaling as described in the "User login and database security" section of this document. For the client/ server application signaling, TLS is employed with key exchange taking place over secured TLS connections and support for the same certificate process as HTTPS.

Component Authentication (spoof prevention) & Session Security

"Spoofing" refers to a tactic used by hackers to "steal" the identity of a trusted component of a network to gain access. Vidyo prevents spoofing through a rigorous component authentication scheme. Each machine in the Vidyo network has a unique identifier which is communicated to the VidyoPortal over a secure link and is otherwise not accessible. New components added to the network go to the VidyoPortal for configuration. If the VidyoPortal doesn't have a configuration defined for that machine's specific ID, the machine is blocked from joining the network until the administrator accepts the new ID and manually configures the component.

On the client side, a unique token is generated and encrypted by the VidyoPortal and sent to the VidyoDesktop™ or VidyoRoom™ at login over a secured link after the Vidyo endpoint has sent the VidyoPortal its unique identifier. The encrypted token is stored at the Vidyo endpoint and the session is kept alive until the next time the user successfully logs in, whether from the same machine or a different machine, at which point a new token is issued and a new session is started. Each time the Vidyo endpoint attempts to access the VidyoPortal for services (such as call initiation), the endpoint presents its session token to the VidyoPortal, ensuring that the endpoint is in fact the machine where the credentialed user last logged in.

Component Access Protection

The Vidyo infrastructure appliances are all Linux based. To prevent hackers from accessing the box itself, Vidyo leverages the security features of Linux while hardening the box by closing all ports that are not relevant or used and making it impossible to access the board without VidyoAdmin and root passwords.

Secure Firewall Traversal

Depending on the specific deployment model, Vidyo provides optional methods of secure firewall traversal, enabling organizations to leverage the public network to provide connectivity for mobile end users without compromising the integrity of the private network or requiring additional expensive equipment.

For implementations where the necessary range of UDP ports are opened on the company network, the VidyoDesktop™ client uses industry standard ICE/STUN to negotiate UDP ports directly with the VidyoRouter™. These same protocols are employed for NAT traversal.

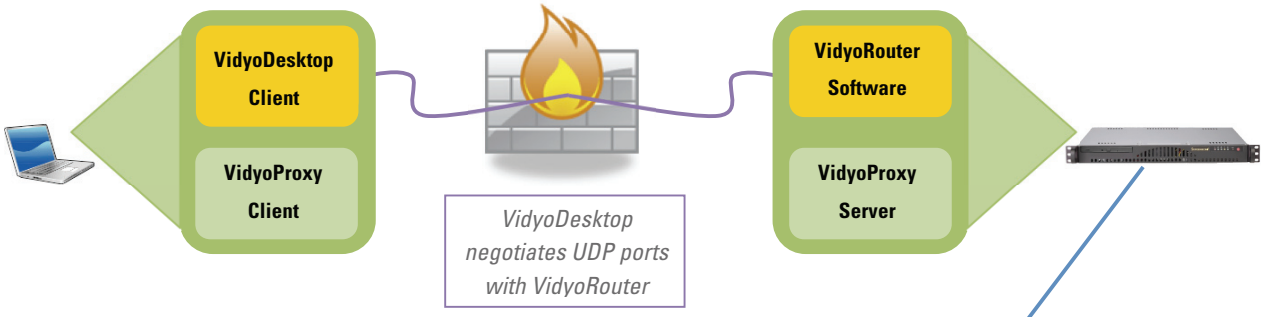

Fig 1: Firewall with UDP Port Range Opened

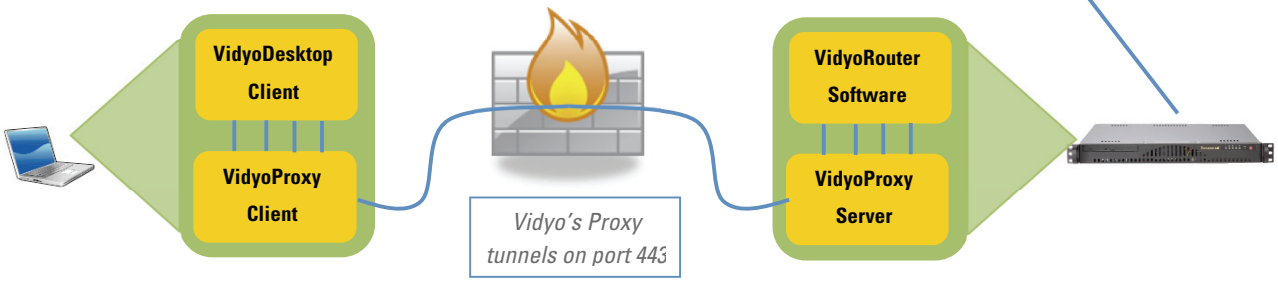

Fig 2: Firewall with UDP Ports Closed

For implementations where the UDP ports are closed on the company network, Vidyo's proxy solution overcomes these blocking issues in a secure fashion by tunneling on port 443 using industry standard TCP. The VidyoDesktop is able to auto-detect if firewall blocking is taking place and automatically switch to Vidyo's proxy configuration as needed. If the firewall configuration is known, auto-detection can be easily overridden. Vidyo's proxy client software is included with the VidyoDesktop application and the proxy server software is included with the VidyoRouter application. The same proxy client and server software modules are also able to traverse Web Proxies, enabling the Vidyo deployment to fully integrate with existing web proxy devices and follow established policies rather than working around them.

For deployments where multiple VidyoRouters are networked together, a single low cost VidyoRouter can be positioned on each side of the firewall. The combination of the robust component authentication described in the "Component Authentication (spoof prevention) & Session Security" section of the this document and a set of explicit IP-to-IP rules on the firewall enable the VidyoRouters to communicate securely with one another without the performance impact that tunneling on port 443 may have and without compromising the security of the private network.

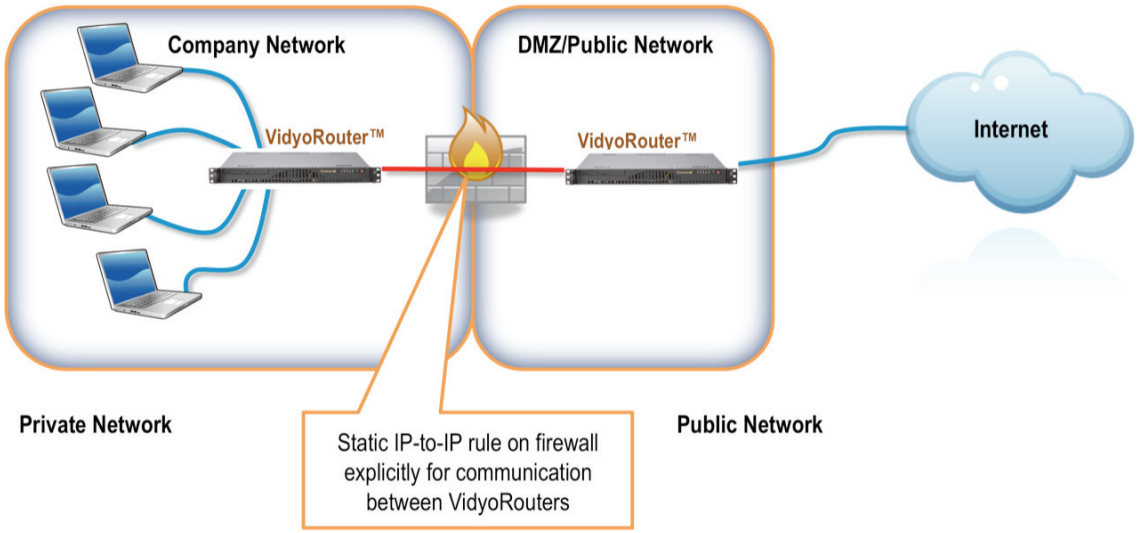

Fig 3: Firewall with explicit IP-to-IP rules for communication between VidyoRouters

Regardless of whether an organization deploys a DMZ, VPN or other network topology, Vidyo's suite of cost effective firewall traversal solutions integrate with the topology and extend the reach of your video communications infrastructure beyond the private network securely.

User Meeting Room Access

Whether you utilize a VidyoDesktop or a VidyoRoom end point, your Vidyo meeting room is the core of your virtual office. Just like with a physical office, you may want to have an open door policy for your Vidyo meeting room where anyone with an account on your VidyoPortal can drop in any time, or you may wish to "close the door" to your Vidyo meeting room and selectively control access. Vidyo affords you the flexibility to do both. If you prefer open door, you need not do anything. If you wish to control access, you have the ability to define a password for your room and share it only with the people that you want to have access to your room. Additionally, if you take advantage of "guest linking" to your room (inviting an unregistered user to join your conference room via hyperlink), every user has the ability to change their hashed hyperlink to their personal meeting space as frequently as desired. Once in conference, the virtual room owner has the ability to "lock the door" so that no additional participants may enter.

Conclusion

By enabling the Secure VidyoConferencing option on the VidyoPortal, administrators and IT departments can rest easy, knowing that the VidyoConferencing network is safe and user data and communications will be secure.

For more information: 1.866.99.VIDYO or VidyoInfo@vidyo.com