Configuring Corporate Firewalls for Sorenson Videophones

Overview and Instructions

October 19, 2021

Videophones Inside Firewalls

Secure Firewall Traversal

Network security and firewall integrity are primary concerns for the IT professionals who manage corporate or institutional networks. Requests for approval of the installation of any device that communicates across the corporate firewall always involve close scrutiny by IT management. The videophone devices used by Deaf and hard-of-hearing persons represent a unique class of network device because videophones transmit and receive large amounts of data between multiple trusted entities across a corporate firewall.

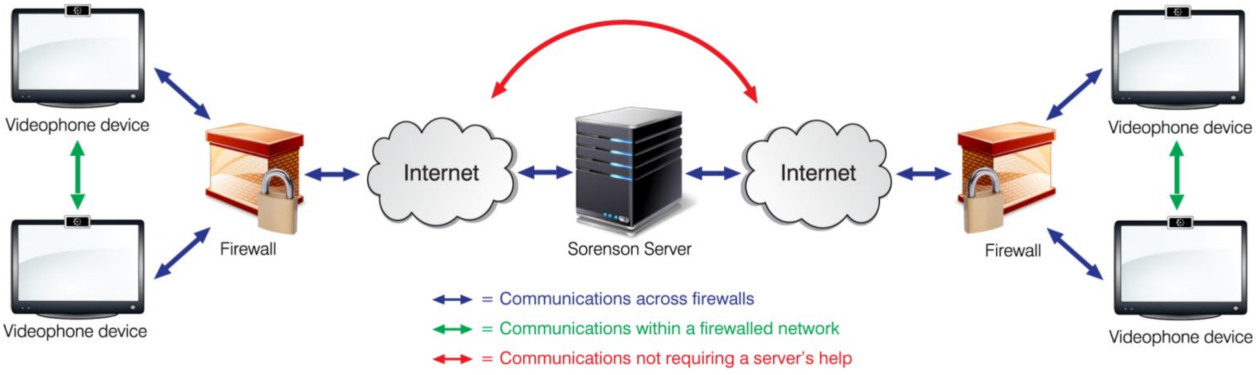
Sorenson Communications, the leading provider of videophone devices and relay services, has integrated NAT/firewall traversal capabilities into its videophone products. Sorenson's traversal solution allows for efficient data transfers across corporate firewalls, increases endpoint performance, and minimizes network security concerns.

Advanced Technologies

Sorenson's firewall traversal solution helps IT professionals maintain network security as they accommodate requests for support of videophone devices. Some details and advantages of Sorenson's Firewall Traversal solution are:

- Firewall traversal technology is based on industry-standard ICE (RFC 5245) protocol
- Automatic creation of the temporary firewall pinholes needed to support videophone multimedia traffic
- Multiple videophones behind a firewall "find" each other by phone number, not IP address
- Prevents excess outbound traffic and bandwidth use by letting videophones inside the network connect directly
- Eliminates the need for manual NAT "fixups" or other manual workarounds
- Eliminates the security risks and costs associated with using dedicated Public IP addresses for each videophone

The figure below shows data communication pathways between Sorenson videophones installed on multiple networks protected by firewalls and Sorenson servers.


Videophone device
Videophone device
Firewall
Internet
Sorenson Server
Internet
Firewall
Videophone device
Videophone device
= Communications across firewalls
= Communications within a firewalled network
= Communications not requiring a server's help

Simple Firewall Configuration

Sorenson's Firewall Traversal solution is easily integrated into most environments. No extra hardware is needed and only minimal firewall configuration is required. These are the steps for deploying Sorenson's solution in your environment:

- Review the configuration requirements described on the next page of this document
- Contact Sorenson to discuss enabling the firewall traversal solution on your network
- Make any configuration changes needed for your brand and version of firewall
- Set up and connect Sorenson videophone devices to your network via Ethernet
- Configure videophones to use DHCP to obtain their IP addresses from your server
- Test outbound, inbound and internal (videophone-to-videophone) calls

Sorenson's full line of videophone endpoint devices support our Firewall Traversal solution. For more information and help getting started, please contact our Customer Care team at: BusinessHelp@Sorenson.com.

Sorenson Firewall Requirements

Follow the steps below to configure a firewall to support Sorenson videophone endpoints:

Step 1 — Add Sorenson Subnets/Ports to Firewall "White List" Rules/Policies

Sorenson's Firewall Traversal solution uses the ICE (RFC 5245) protocol to make SIP calls. Corporate firewalls are sometimes configured to use inspection rules for SIP traffic which may create a conflict with Sorenson's SIP/ICE protocol. The SIP inspection rules issue can be easily addressed by adding the range of Sorenson subnets to the firewall's "White List." The Sorenson subnets to be added to the firewall's White List are listed in the table below.

Add These Sorenson Subnets/Ports to the Firewall "White List" for SIP Traffic	
Subnet	Ports
52.224.77.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
52.250.86.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
65.37.250.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
65.37.253.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
67.221.38.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.228.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.230.0/24	80, 443, 444, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.233.0/24	80, 443, 444, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.236.0/24	80, 443, 444, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.242.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)
209.169.253.0/24	80, 443, 3478, 5060, 5061, 50060 (TCP/UDP)

Step 2 — Disable Global SIP Inspection

Global SIP Inspection may need to be disabled in the firewall because the use of global rules can interfere with Sorenson calls. If needed, user-created inspection rules can be used instead because they do not attempt to change data packets.

Step 3 – Add a Specific Set of Domains to Content Filter/Proxy Server Allow List

If a Content filter or a Proxy server is used on a network, Sorenson's Enterprise Domain servers must be added to the Content filter or Proxy server's "Allow List." Access is also required to the OpenWeatherMap service.

Depending on its configuration, a Content filter or Proxy server may interfere with videophone endpoint operation by filtering or denying traffic completely or by preventing the endpoints from registering themselves with Sorenson's servers. The symptoms below can occur if a Content filter or Proxy server blocks traffic on Ports 80 or 443:

- Videophone cannot register with Sorenson servers when first installed
- Videophone shows a "black video screen" even though incoming ports are open
- Videophone cannot receive or play Sorenson SignMail videos
- Videophone cannot get online even though the IP information is correct

Add These Domains to your Content Filter Allow List	
*.svrs.net	*.sorenson2.biz
*.svrs.cc	*.sorensonprod.biz
*.sorenson.com	*.sorensonprod.com
*.sorensonvrs.com	pro.openweathermap.org
*.sorensonaws.com	

Step 4 — Add a Specific Set of Domains to Firewall FQDN Allow List

Sorenson endpoints are designed to access a few external servers that provide some **optional** services for the endpoints through the firewall. These domains provide Sorenson endpoints with relay system server status; screensaver file downloads and related weather information for the screensavers; and quicker firmware updates. If you decide to provide access to these external servers, add the domain names shown below to the firewall's FQDN Allow list.

Add These Domains to your Firewall FQDN Allow List	
download.sorensonvrs.com	Used to update themes and screensavers
pro.openweathermap.org	Used to display weather information in screensavers
www.svrsstatus.com	Used to display service outage notifications
endpointupdates.sorensonprod.com	Used to provide quicker endpoint firmware updates

Step 5 – Contact Sorenson Customer Care for Problem Resolution

Please contact Sorenson Customer Care at BusinessHelp@Sorenson.com for help with any issue such as those listed below:

- You have questions about any of the requirements listed in this document.
- You have questions about using a specific brand of Content filter or Proxy server.
- If you need help configuring a specific brand of firewall.