Bell Total Connect

Firewall and connection requirements

Contents

Introduction 3

How to interpret firewall rule tables in this document 3

Sample Bell Total Connect network architecture 1

Connection requirements for Bell Total Connect apps 2

DHCP and DNS requirements 2

Firewall rules for Bell Total Connect apps 2

Firewall rules for the Bell Total Connect desktop app with voice over Internet 2

Firewall rules for Bell Total Connect desktop app with voice Over MPLS 4

Firewall rules for Bell Total Connect mobile application 5

Firewall rules for Bell Total Connect for Skype for Business 6

Firewall rules for the Bell Total Connect receptionist application 7

Firewall rules for Bell Total Connect with Webex Desktop client (Standard - no Video Mesh) 7

Firewall rules for Bell Total Connect with Webex Mobile client 8

Firewall rules for Bell Total Connect with Webex Desktop client with Video Mesh 9

Table WX-Media 10

Using the on-premises session border controller as a proxy 10

Connection requirements for Bell Total Connect devices 11

DHCP options 11

Firewall rules for Bell Total Connect devices (IP VPN based site access) 11

Firewall rules for Bell Total Connect devices (over Internet) 19

Connection requirements for on-premises E-SBC devices 21

Firewall rules for on-premises E-SBC devices 21

Firewall rules for on-premises E-SBC devices 21

Firewall rules for on-premises E-SBC (WAN side to Bell VoIP support system) 22

Firewall rules for on-premises E-SBC (WAN side to other destinations) 22

Firewall rules for on-premises E-SBC (WAN side to Bell VoIP support system) 23

Mediatrix 41xx and C7xx series 25

Polycom VVX series 25

Appendix: Connection processes for apps and devices 27

Bell Total Connect desktop app connection process 27

Bell Total Connect receptionist web app connection process 27

Bell Total Connect phone connection process 27

Introduction

This guide outlines the main IP and firewall requirements for the correct functioning of Bell Total Connect apps and devices. An organization's network and/or IT specialists should use this guide to determine if changes are required to their network settings when first setting up Bell Total Connect.

This guide will also help troubleshoot any connection issues experienced by end users once Bell Total Connect is up and running.

It is highly recommended that the steps described in this document are implemented with the support of a Bell engineer or professional services expert.

How to interpret firewall rule tables in this document

The nature of the IP traffic between on-premises apps/devices and local or remote Bell/partner equipment can be one of the followingbelow:

- Unidirectional (ex: syslog)
- Request/response-based (ex: HTTPS)
- Real-time bidirectional (ex. Real-time Transport Protocol (RTP) in audio/video calls)

A layer 3 security function, such as an Access Control List (ACL) or layer 4 stateless firewall, would have to account for all possible IP traffic directions to police this traffic adequately. Both directions may be involved in real-time bidirectional flows, described individually in the form of distinct source/destination rules in this document. Note that by making such bidirectional rules explicit, they can also hold for layer 4 stateful firewalls, because either the local or remote party can initiate the layer 4 connection involved in real-time bidirectional flows. This would be the case for User Diagram Protocol (UDP) RTP streams involved in audio/video calls. Layer 4 stateful firewalls would then define explicit policies for each possible connection directions.

When layer 4 stateful firewalls and Network Address Port Translation (NAPT) are involved (typically the case for Bell Total Connect apps over the Internet devices or failover routing to the Internet), only trusted-to-untrusted (or LAN-to-WAN) connections actually take place, even for naturally -bidirectional real-time flows. Specifically, all connections involving a Bell Total Connect app or device under this topology, whether Transmission Control Protocol (TCP) or UDP, are initiated from the corporate network, targeting a Bell Internet Session Border Controller (SBC).

To cope with this forced directionality of otherwise bidirectional real-time traffic, Bell's Internet SBC performs a Hosted Network Address Translation (NAT) traversal function. This means that on-premises apps and devices initiate all Session Initiation Protocol (SIP)/Transport Layer Security (TLS) connections. and Bell's Internet SBC, after having detected the presence of the customer NAT, always reuses this established layer 4 connection to convey call signalling in the reverse (Bell-to-app/device) direction.

In this topology, Bell's Internet SBC never initiates RTP media flows towards the customer. It awaits the opposite RTP connection to be established from the customer premises and sends its RTP traffic within this layer 4 connection. This SBC function is called Symmetric RTP.

In summary, when using a layer 4 stateful firewall with NAPT, the Bell-to-customer source/destination rules described in the tables of this document are redundant and somewhat not applicable directly. Only the customer-to-Bell flows have to be implemented as firewall policies.

Sample Bell Total Connect network architecture

There are a number of ways for organizations to implement Bell Total Connect. Figure 1 below illustrates a common network architecture.

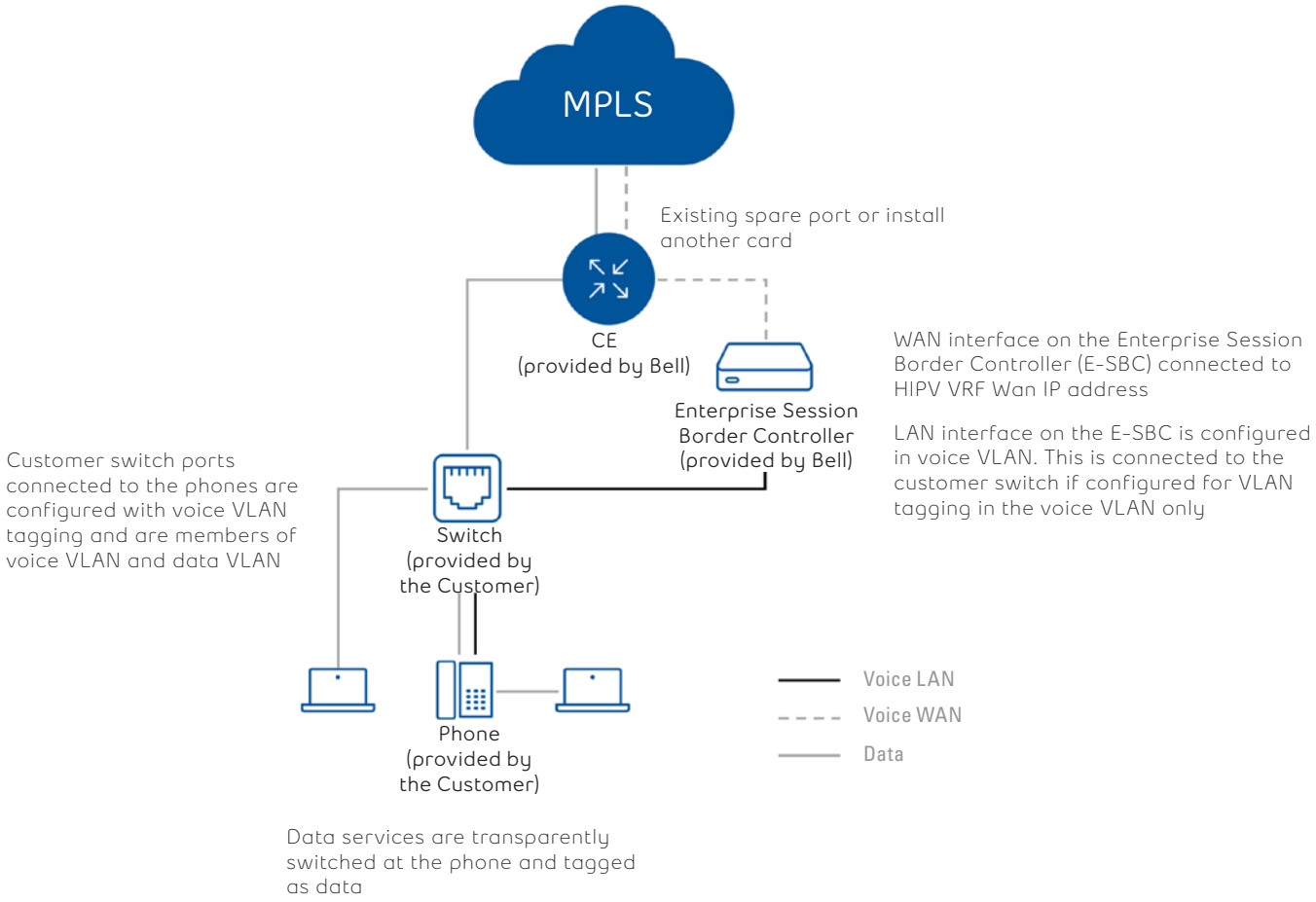

Figure 1. Basic LAN architecture

In some instances, on-premises session border controller (E-SBC) traffic may transit via a switch or firewall before going to the Bell-owned customer edge (CE) router. Because firewalls can be inserted in numerous places in the network, specific firewall rules may need to be adapted and implemented in more than one location. (If there is no firewall between the E-SBC and the CE router, the firewall rules described in this document will not be required.)

Connection requirements for Bell Total Connect apps

Depending on their needs and subscribed packages, Bell Total Connect users may choose to install a desktop app and the Bell Total Connect receptionist app (call dashboard), which is typically used by a limited group of users with designated receptionist roles. All apps use the data VLAN of your organization's LAN to connect to the public Internet and launch from the user's PC.

DHCP and DNS requirements

IP addresses for each user's PC are provided by your organization's dynamic host configuration protocol (DHCP) server and are reused by the desktop app and receptionist app (call dashboard).

The Bell Total Connect apps use the domain name system (DNS) to locate various network elements. A PC running a Bell Total Connect with Webex app must have access to a DNS server that can resolve the hostnames of servers provisioned into the desktop app and/or receptionist app (call dashboard).

Note: Hostnames and IP addresses listed in this document are subject to change.

Firewall rules for Bell Total Connect apps

The following rules apply if the LAN supporting the interaction of the Bell Total Connect apps employs outbound-specific firewalls.

Note: A firewall using a session initiation protocol (SIP) application layer gateway (ALG) is not recommended for use with Bell Total Connect. Although these gateways generally work, in some cases they can cause SIP messages to be lost because the ALG cannot correctly identify them.

Firewall rules for the Bell Total Connect desktop app with voice over Internet

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
Any PC	>1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-tor2.totalconnect.bell.ca xsi-tor3.totalconnect.bell.ca xsi-mtl.totalconnect.bell.ca xsi-mtl2.totalconnect.bell.ca xsi-mtl3.totalconnect.bell.ca dms.totalconect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Any PC	45001	mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	SIP	UDP
mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	Any PC	45001	SIP	UDP
Any PC	>1024	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180 (This is the connection-establishing flow)	5061	Secure SIP	TCP
184.150.213.164 184.150.213.172 184.150.213.180 184.150.213.178	5061	Any PC (This flow always reuses pre-established connections – see above)	>1024	Secure SIP	TCP
Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	mtl-sbc.totalconnect.bell.ca 67.69.255.68	49152 - 65535[1]	RTP Audio RTP Video	UDP

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
mtl-sbc.totalconnect.bell.ca 67.69.255.68	49152 to 65535[1]	Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	RTP Audio RTP Video	UDP
Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152 to 65535[1]	SRTP Audio SRTP Video	UDP
184.150.213.164 184.150.213.172 184.150.213.180 184.150.213.178	49152 to 65535[1]	Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	SRTP Audio SRTP Video	UDP
Any PC	45001	tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	SIP	UDP
tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	Any PC	45001	SIP	UDP
Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	tor-sbc.totalconnect.bell.ca 67.69.186.20	49152 - 65535[1]	RTP Audio RTP Video	UDP
tor-sbc.totalconnect.bell.ca 67.69.186.20	49152 - 65535[1]	Any PC	8500 to 8598[1] (Audio) 8600 to 8698[1] (Video)	RTP Audio RTP Video	UDP
Any PC	>1024	Customer LDAP server	389 636	LDAP LDAPS	TCP
Any PC	>1023	xmpp.totalconnect.bell.ca 67.69.237.0/24 67.69.241.0/24	5222 1081 443	XMPP SOCKS HTTPS	TCP
Any PC	>1023	sharing.totalconnect.bell.ca 67.69.237.0/24 67.69.241.0/24	443	TLS/WSS	TCP

[1] This is required by the vendor for voice and video calls.

Firewall rules for Bell Total Connect desktop app with voice Over MPLS

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
Any PC	> 1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-tor2.totalconnect.bell.ca xsi-tor3.totalconnect.bell.ca xsi-mtl.totalconnect.bell.ca xsi-mtl2.totalconnect.bell.ca xsi-mtl3.totalconnect.bell.ca dms.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Any PC	45001	eSBC LAN IP	5060	SIP	UDP
eSBC LAN IP	5060	Any PC	45001	SIP	UDP
Any PC	8500 to 8598 [1] (Audio) 8600 to 8698 [1] (Video)	eSBC LAN IP	49152 to 65535 [1]	RTP Audio	UDP
eSBC LAN IP	49152 to 65535 [1]	Any PC	8500 to 8598 [1] (Audio)	RTP Audio	UDP
Any PC	45001	eSBC LAN IP	5060	SIP	UDP
eSBC LAN IP	5060	Any PC	45001	SIP	UDP
Any PC	8500 to 8598 [1] (Audio) 8600 to 8698 [1] (Video)	eSBC LAN IP	49152 to 65535 [1]	RTP Audio	UDP
eSBC LAN IP	49152 to 65535 [1]	Any PC	8500 to 8598 [1] (Audio)	RTP Audio	UDP
Any PC	>1024	Customer LDAP server	389 636	LDAP LDAPS	TCP
Any PC	>1023	xmpp.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	5222 1081 443	XMPP SOCKS HTTPS	TCP
Any PC	>1023	sharing.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	43	TLS/ WSS	TCP

[1]This is required by the vendor for voice and video call.

Firewall rules for Bell Total Connect mobile application

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
Any mobile	>1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-mtl. totalconnect.bell.ca xsi-mob.totalconnect. bell.ca xsi-mob-tor.totalconnect.bell.ca xsi-mob- mtl.totalconnect.bell.ca 67.69.241.203 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Any mobile	5061	mtl-sbcs.totalconnect.bell.ca 67.69.255.74 tor-sbcs.totalconnect.bell.ca 184.150.214.132 cal-sbcs.totalconnect.bell.ca 184.150.214.212	5061	Secure SIP	TCP
mtl-sbcs. totalconnect.bell.ca 67.69.255.74 tor-sbcs. totalconnect.bell.ca 184.150.214.132 cal-sbcs. totalconnect.bell.ca 184.150.214.212	5061	Any Mobile	5061	Secure SIP	TCP
Any mobile	8500-8598 (Audio)[1] 8600-8698 (Video)[1]	mtl-sbcs.totalconnect.bell.ca 67.69.255.74 tor-sbcs.totalconnect.bell.ca 184.150.215.132 cal-sbcs.totalconnect.bell.ca 184.150.214.212	40000-59999	SRTP-Audio SRTP-Video	UDP
mtl-sbcs. totalconnect.bell.ca 67.69.255.74 tor-sbcs. totalconnect.bell.ca 184.150.214.132 cal-sbcs. totalconnect.bell.ca 184.150.214.212	40000-59999	Any Mobile	8500-8598[1] 8600-8698[1]	SRTP	UDP
iOS devices	>1023	Apple push notification 17.0.0.0/8	5223 443	HTTPS	TCP
Android devices	>1023	Google does not provide specific IPs for servers	5228 5229 5230	HTTPS	TCP
Any mobile	>1023	Instant messaging & presence xmpp.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	5222 443	XMPP TLS HTTPS	TCP

[1]This is required by the vendor for voice and video call.

Firewall rules for Bell Total Connect for Skype for Business

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
Any PC	> 1023	hipv-xsp2.bell.ca xsi-mtl.totalconnect.bell.ca xsi-mtl2.totalconnect.bell.ca xsi-mtl3.totalconnect.bell.ca xsi-tor.totalconnect.bell.ca xsi-tor2.totalconnect.bell.ca xsi-tor3.totalconnect.bell.ca dms.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Any PC	45001	mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	SIP	UDP
mtl-sbc. totalconnect.bell.ca 67.69.255.68	5060	Any PC	45001	SIP	UDP
Any PC	8500 to 8598[1]	mtl-sbc.totalconnect.bell.ca 67.69.255.68	49152 to 65535[1]	RTP	UDP
mtl-sbc. totalconnect.bell.ca 67.69.255.68	49152 to 65535[1]	Any PC	8500 to 8598[1]	RTP	UDP
Any PC	45001	tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	SIP	UDP
tor-sbc. totalconnect.bell.ca 67.69.186.20	5060	Any PC	45001	SIP	UDP
Any PC	8500 to 8598[1]	tor-sbc.totalconnect.bell.ca 67.69.186.20	49152 to 65535[1]	RTP	UDP
tor-sbc. totalconnect.bell.ca 67.69.186.20	49152 to 65535[1]	Any PC	8500 to 8598[1]	RTP	UDP

[1]This is required by the vendor for voice and video call.

Firewall rules for the Bell Total Connect receptionist application

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocol
Any PC	> 1023	totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP

Firewall rules for Bell Total Connect with Webex Desktop client (Standard - no Video Mesh)

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocol	Purpose
Any PC	>1023	ANY	443	HTTPS, WSS	TCP	Secure signaling and messaging
Any PC	>1023	See Table WX-Media	5004 9000 33434	SRTP	UDP	Secure audio, video, and content sharing on Webex Teams devices, primary and backup ports
Any PC	>1023	See Table WX-Media	5004 9000 33434	SRTP	TCP	Used for secure content sharing on Webex Teams devices as failback if UDP cannot be used, primary and backup ports
Any PC	>1023	See Table WX-Media	33434- 33598 49152- 59999	SRTP	UDP	Secure audio, video and content sharing media
Any PC	>1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-mtl.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP	Retrieval of Bell Total Connect connection and profile information
Any PC	>1023	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	5061	Secure SIP	TCP	Secure signaling and messaging with Bell
Any PC	>1023	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180 (This is the connection-establishing flow)	49152 - 65535	SRTP	UDP	Secure audio and video with Bell
142.177.151.188 184.150.213.180 184.150.213.164 184.150.213.172	49152 - 65535	Any PC (This flow always reuses pre-established connections – see above)	>1023	SRTP	UDP	Secure audio and video with Bell

Firewall rules for Bell Total Connect with Webex Mobile client

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocol	Purpose
Any PC	>1023	ANY	443	HTTPS, WSS	TLS	Secure signalling and messaging
Any PC	>1023	See Table WX-Media	5004 9000 33434	SRTP	UDP	Secure audio, video and content sharing on Webex Teams devices, primary and backup ports
Any PC	>1023	See Table WX-Media	5004 9000 33434	SRTP	TCP	Used for secure content sharing on Webex Teams devices as failback if UDP cannot be used, primary and backup ports
Any PC	>1023	See Table WX-Media	33434- 33598 49152- 59999	SRTP	UDP	Secure audio, video and content sharing media
Any PC	>1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-mtl.totalconnect.bell.ca xsi-mob.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TLS	Retrieval of Bell Total Connect connection and profile information
Any PC	>1023	mtl-sbcs.totalconnect.bell.ca 67.69.255.74 tor-sbcs.totalconnect.bell.ca 184.150.214.132 cal-sbcs.totalconnect.bell.ca 184.150.214.212	5061	SIP	TLS	Secure signalling and messaging with Bell
Any PC	>1023	mtl-sbcs.totalconnect.bell.ca 67.69.255.74 tor-sbcs.totalconnect.bell.ca 184.150.215.132 cal-sbcs.totalconnect.bell.ca 184.150.214.212	5061	SRTP	UDP	Secure audio and video with Bell

Firewall rules for Bell Total Connect with Webex Desktop client with Video Mesh

Relatively few customers choose to deploy Video Mesh. Customers who choose Video Mesh should use the following rules instead of the rules in section 2.2.6. By deploying Video Mesh, customers can limit the volume of traffic exiting their network, going over the Internet and reduce the amount of direct communication between end devices and Cisco.

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocol	Purpose
Video Mesh Node	>1023	ANY	444	HTTPS	TLS	Video Mesh Node Secure Cascade Signalling to the Webex cloud
Video Mesh Nodes Hybrid Data Security Nodes Webex Hybrid Services Connectors	>1023	ANY	123	NTP	UDP	Network Time Protocol (NTP)
Video Mesh Nodes Hybrid Data Security Nodes Webex Hybrid Services Connectors	>1023	ANY	53	DNS	UDP, TCP	Domain Name System (DNS)
Any PC	>1023	See Table WX-Media	5004 9000	SRTP	UDP	Secure audio, video and content sharing on Webex Teams devices
Any PC	>1023	See Table WX-Media	5004 9000	SRTP	TCP SRTP	Used for secure content sharing on Webex Teams devices as failback if UDP cannot be used
Any PC	>1023	See Table WX-Media	5004 9000	SRTP	UDP	Secure audio, video and content sharing media from Video Mesh Node to the Webex Cloud
Any PC	>1023	See Table WX-Media	5004 9000	SRTP	TCP SRTP	Secure audio, video and content sharing media from Video Mesh Node to the Webex Cloud (backup)
Any PC	>1023	See Table WX-Media	33434-33598 and 49152-59999		UDP SRTP	Secure audio, video and content sharing media
Any PC	>1023	hipv-xsp2.bell.ca xsi-tor.totalconnect.bell.ca xsi-mtl.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TLS	Retrieval of BTC connection and profile information
Any PC	>1023	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	5061	Secure SIP	TCP	Secure signalling and messaging with Bell
Any PC	>1023	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180 (This is the connection-establishing flow)	49152 - 65535	SRTP	UDP	Secure audio and video with Bell
142.177.151.188 184.150.213.180 184.150.213.164 184.150.213.172	49152 - 65535	Any PC (This flow always reuses pre-established connections – see above)	>1023	SRTP	UDP	Secure audio and video with Bell

Table WX-Media

Due to the number of IP addresses/subnets involved in the operation of Webex, they have been listed in the table below to allow the firewall rule tables to remain readable.

Note: All of the addresses in the following subnets are reserved for exclusive use by Cisco; however, they are registered to Cisco, Microsoft Azure and Amazon Web Services (AWS) in terminated geographically in North American and Europe

IP subnets for media services		
3.22.157.0/26	18.181.178.128/25	69.26.160.0/19
3.25.56.0/25	18.181.204.0/25	114.29.192.0/19
3.101.70.0/25	18.230.160.0/25	150.253.128.0/17
3.101.71.0/24	20.50.235.0/24	155.190.254.0/23
3.101.77.128/28	20.68.154.0/24	170.72.0.0/16
3.235.73.128/25	40.119.234.0/24	170.133.128.0/18
3.235.80.0/23	44.234.52.192/26	173.39.224.0/19
3.235.122.0/24	52.232.210.0/24	173.243.0.0/20
3.235.123.0/25	62.109.192.0/18	207.182.160.0/19
18.132.77.0/25	64.68.96.0/19	209.197.192.0/19
18.141.157.0/25	66.114.160.0/20	210.4.192.0/20
18.181.18.0/25	66.163.32.0/19	216.151.128.0/19

Using the on-premises session border controller as a proxy

Should your organization not allow access to the public Internet or to the specific ports required for the PC-based apps to function correctly, a customer-specific application (CSAP) can be implemented to allow the receptionist app to use the on-premises session border controller (E-SBC) to reach the Bell VoIP core network servers. Please contact your sales representative to discuss this option.

Connection requirements for Bell Total Connect devices

Unlike Bell Total Connect PC-based apps, Bell Total Connect IP devices use the voice VLAN to communicate with the on-premises E-SBC and reach the Bell Total Connect servers in the Bell network.

DHCP options

IP addresses for Bell Total Connect devices are provided by your organization's DHCP server (with the device redirected to the on-premises E-SBC as an SIP and outbound proxy) or by the on-premises E-SBC LAN (with the IP subnet and range provided by your organization and excluded from your DHCP server).

Note: The IP address range for the Bell Total Connect device is blocked and cannot be reused in your DHCP servers for other Bell Total Connect apps.

Firewall rules for Bell Total Connect devices (IP VPN based site access)

The following rules apply if a firewall is placed between the Bell Total Connect IP devices and the on-premises E-SBC LAN side. (It is recommended that this firewall placement be avoided if possible.)

Note: All end-points connected thought IPVPN will register to the E-SBC at least once every 60 seconds, this registration will work properly when your firewall pinhole timeout for SIP is set up for 60s and greater.

Cisco SPA 5xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060-5080 [1]	eSBC LAN IP	5060	SIP	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060-5080 [1]	SIP	TCP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTP	UDP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTCP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 20 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device
[3]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Cisco CP 78xx and 88xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Customer-reserved IP address range	> 1023	hipv-xsp2.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060-5080	eSBC LAN IP	5060	SIP	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060-5080 [1]	SIP	TCP
Customer-reserved IP address range	16384-32764 [2]	eSBC LAN IP	16384-32764 [3]	RTP RTCP	UDP
eSBC LAN IP	16384-32764 [3]	Customer-reserved IP address range	16384-32764 [2]	RTP RTPC	UDP

[1]This is required by Cisco to be able to perform up to 20 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device
[3]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Cisco ATA 192

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 8443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060-5063 [1]	eSBC LAN IP	5060	SIP	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060-5063	SIP	TCP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTP	UDP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTCP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 4 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device
[3]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Cisco ATAs 122 and 8000

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 8443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060-5063 [1]	eSBC LAN IP	5060	SIP	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060-5063	SIP	TCP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTP	UDP
Customer-reserved IP address range	16384-16482 [2]	eSBC LAN IP	16386-20385 [3]	RTCP	UDP
eSBC LAN IP	16386-20385 [3]	Customer-reserved IP address range	16384-16482 [2]	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 4 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device
[3]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Aastra 67xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	>1023	eSBC LAN IP	5060	SIP	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	>1023	SIP	TCP
Customer-reserved IP address range	3000 – 2x number of lines [1]	eSBC LAN IP	16386-20385 [2]	RTP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	3000 – 2x number of lines [1]	RTP	UDP
Customer-reserved IP address range	3000 – 2x number of lines [1]	eSBC LAN IP	16386-20385 [2]	RTCP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	3000 – 2x number of lines [1]	RTCP	UDP

[1]This is required by Aastra RTP is described in RFC1889. The UDP port used for RTP streams is traditionally an even-numbered port, and the RTCP control is on the next port up. A phone call therefore uses one pair of ports for each media stream. The RTP port is assigned to the first line on the phone, and is then incremented for each subsequent line available within the phone to provide each line a unique RTP port for its own use.
[2]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.
[3]Number of lines per Aastra models: 5 lines for 6731i and 9 lines for all other supported models.

Mediatrix 41xx and C7xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	16000 + number of FXS ports [1]	eSBC LAN IP	5060	SIP[3]	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	16000+number of FXS ports	SIP	TCP
Customer-reserved IP address range	5004+2x number of calls	eSBC LAN IP	16386-20385 [2]	RTP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	5004+2x number of calls	RTP	UDP
Customer-reserved IP address range	5004+2x number of calls	eSBC LAN IP	16386-20385 [2]	RTCP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	5004+2x number of calls	RTCP	UDP

[1]This is required by Media5 to have a specific SIP port per FXS port.
[2]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.
[3]This is required by Media5 to be able to reach the maximum number of concurrent calls per device.

Polycom VVX series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server or the eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	69	TFTP	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060	eSBC LAN IP	5060	SIP[3]	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060	SIP	TCP
Customer-reserved IP address range	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [1]	eSBC LAN IP	16386-20385 [2]	RTP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [1]	RTP	UDP
Customer-reserved IP address range	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 [1]	eSBC LAN IP	16386-20385 [2]	RTCP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 [1]	RTCP	UDP

[1]This is required by Polycom to be able to perform up to 24 concurrent calls per device. From Polycom vendor explanation: The starting port for RTP packets. Ports are allocated from a pool starting with this port up to a value of (start-port '50000'+ 47) for VVX310/410 or (start-port '50000'+ 95) for a VVX500/501/600/601.

[2]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Polycom SSIP series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server or the eSBC LAN IP	67	DHCP	UDP
Customer-reserved IP address range	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
Customer-reserved IP address range	> 1023	eSBC LAN IP	21	FTP	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Customer-reserved IP address range	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Customer-reserved IP address range	5060	eSBC LAN IP	5060	SIP[3]	TCP
eSBC LAN IP	5060	Customer-reserved IP address range	5060	SIP	TCP
Customer-reserved IP address range	2222-2268 [1]	eSBC LAN IP	16386-20385 [2]	RTP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	2222-2268 [1]	RTP	UDP
Customer-reserved IP address range	2222-2268 [1]	eSBC LAN IP	16386-20385 [2]	RTCP	UDP
eSBC LAN IP	16386-20385 [2]	Customer-reserved IP address range	2222-2268 [1]	RTCP	UDP

[1]This is required by Polycom to be able to perform up to 24 concurrent calls per device. From Polycom vendor explanation: the value 2222 will be used for the first allocated RTP port. Subsequent ports will be allocated from a pool starting with the specified port plus two up to a value of (start-port + 46), after which the port number will wrap back to the starting value.
[2]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Firewall rules for Bell Total Connect devices (over Internet)

The following rules apply if a firewall is placed between the Bell Total Connect IP devices (supported over Internet) and the Internet connection.

For each specific device, we need to apply one more rule to allow access to the vendor's ZTP server. This rule is described in the following sections.

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
Any Bell device over Internet	> 1023	hipv-xsp2.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Any Bell device over Internet	> 1023	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180 (This is the connection-establishing flow)	5061	Secure SIP	TCP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	5061	Any Bell device over Internet (This flow reuses pre-established connections)	> 1023	Secure SIP	TCP
Any Bell device over Internet	> 1023	time.nrc.ca 132.246.11.227 132.246.11.229 132.246.11.238 [2] 132.246.11.237 [2]	123	NTP	UDP

[1]This is required by the vendor for voice and video call.
[2]NTP service is offered by the Government of Canada NRC. These addresses are subject to change, hence it is recommended to trust time.nrc.ca instead of filtering by IP.

Cisco (CP6821, CP6871, CP7841, CP8841, CP8851)

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
Cisco phones	> 1023	webapps.cisco.com 0.0.0.0/0 [1]	443	HTTPS	TCP
Cisco phones	16384-32764	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	SRTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	Customer-reserved IP address range (This flow reuses pre-established connections)	16384-32764	SRTP	UDP

[1]Here we need to allow the entire IP range because the vendor's ZTP server can use different addresses over time.

Cisco ATA 192

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
Cisco phones	> 1023	webapps.cisco.com 0.0.0.0/0 [1]	443	HTTPS	TCP
Cisco phones	16384-32764	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell. ca sbc5-6halifax01.secure.btc.bell. ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	SRTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	Customer-reserved IP address range (This flow reuses pre-established connections)	16384-32764	SRTP	UDP

[1]Here we need to allow the entire IP range because the vendor's ZTP server can use different addresses over time.

Polycom Polycom (VVX150, VVX250, VVX310/311, VVX350, VVX410/411, VVX450, VVX500/501, VVX600/601, TRIO8300)

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
Polycom phones	> 1023	ztp.polycom.com 0.0.0.0/0 [1]	443	HTTPS	TCP
Polycom phones	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [2]	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	16386-20385 [3]	SRTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	16386-20385 [3]	Polycom phones	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [2]	SRTP	UDP

[1]Here we need to allow the entire IP range because the vendor's ZTP server can use different addresses over time.
[2]This is required by Polycom to be able to perform up to 24 concurrent calls per device. From Polycom vendor explanation: The starting port for RTP packets. Ports are allocated from a pool starting with this port up to a value of (start-port '50000'+ 47) for VVX310/311/410/411 or (start-port '50000'+ 95) for a VVX500/501/600/601.
[3]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.

Mediatrix (Mediatrix4102, MediatrixC711, MediatrixS724)

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
Mediatrix devices	> 1023	ems2.media5corp.com 0.0.0.0/0 [1]	443	HTTPS	TCP
Mediatrix devices	5004+2x number of calls [3]	sbc23-24toronto01.secure.btc.bell.ca sbc21-22montreal02.secure.btc.bell.ca sbc5-6halifax01.secure.btc.bell.ca sbc5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	SRTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535 [2]	Mediatrix devices	5004+2x number of calls [3]	SRTP	UDP

[1]Here we need to allow the entire IP range because the vendor's ZTP server can use different addresses over time.
[2]The ports used in the eSBC 4k are to be able to perform up to 2k concurrent calls per eSBC. From eSBC vendor explanation: Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least twice as many ports as RTP streams you want to handle.
[3]This is required by Media5 to be able to reach the maximum number of concurrent calls per device.

Connection requirements for on-premises E-SBC devices

Your organization's on-premises E-SBC is the Bell Total Connect service demarcation point. Monitored and controlled by the centralized VoIP support system located in the Bell network, it provides various services to the Bell Total Connect phones, including:

- SIP proxy for Bell Total Connect phones
- TFTP and FTP service for phone provisioning
- Call admission control (CAC)
- Voice quality monitoring
- Security and service-assurance functions
- Voice VLAN tagging

Note: In a standard installation, only Bell Total Connect phones use the on-premises E-SBC (i.e., the Bell Total Connect PC-based apps do not use the on- premises E-SBC).

Firewall rules for on-premises E-SBC devices

If a firewall is located between the on-premises E-SBC and the customer edge (CE) router, the firewall must be configured to pass VoIP protocols through to the on-premises E-SBC. The firewall cannot perform NAT – doing so will break VoIP protocol. Because the on-premises E-SBC is a VoIP proxy, all VoIP packets will have a source or destination IP address of the on-premises E-SBC WAN interface.

The on-premises E-SBC WAN IP address is provided by:

- Bell - if the IP VPN CE router has a direct connection to the on-premises E-SBC (this is the standard installation scenario)
- Your organization - if traffic goes through your LAN to reach the CE router, meaning there is no direct connection between the on-premises E-SBC and the CE router (this is the CSAP installation scenario)

Your organization's on-premises eSBC is the Bell Total Connect service demarcation point. Monitored and controlled by the centralized VoIP support system located in the Bell network, it provides various services to the Bell Total Connect, including:

- SIP proxy for Bell Total Connect phones
- TFTP and FTP service for phone provisioning
- Call admission control (CAC)
- Voice quality monitoring
- Security and service-assurance functions
- Voice VLAN tagging

Note: The Bell Total Connect desktop app uses the Internet by default to convey its VoIP traffic, but can use the on-premises E-SBC instead when configuring, via the BTC portal, a service option called "QoS".

Firewall rules for on-premises E-SBC devices

If a firewall is located between the on-premises E-SBC and the customer edge (CE) router, the firewall must be configured to pass VoIP protocols through to the on-premises eSBC. The firewall cannot perform NAT – doing so will break VoIP protocol. Because the on-premises eSBC is a VoIP proxy, all VoIP packets will have a source or destination IP address of the on-premises E-SBC WAN interface.

The on-premises E-SBC WAN IP address is provided by:

- Bell – if the IP VPN CE router has a direct connection to the on-premises E-SBC (this is the standard installation scenario)
- Your organization – if traffic goes through your LAN to reach the CE router, meaning there is no direct connection between the on-premises E-SBC and the CE router (Optional scenario. Please contact your Bell Sales team for further information and support regarding this option)

Note: Because traffic is bidirectional unless otherwise specified, the source and destination may be reversed in some cases. The source (or initiator) of the communication will typically have > 1023 as the source port and communicate to the protocol fixed port number.

Firewall rules for on-premises E-SBC (WAN side to Bell VoIP support system)

Source		Destination			
IP	Port	FQDN/ IP	Ports	Application	Protocol
E-SBC WAN address	> 1023	VoIP support system 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	80 443 8443	HTTP HTTPS	TCP
E-SBC WAN address	514	VoIP support system 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	514	SYSLOG	UDP
E-SBC WAN address	> 1023	VoIP support system 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	123	NTP	TCP
VoIP support system 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	> 1023	E-SBC WAN address	22	SSH	TCP
VoIP support system 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	> 1023	E-SBC WAN address	161	SNMP	UDP
E-SBC WAN address	Any	Any	160	SNMP	UDP

Firewall rules for on-premises E-SBC (WAN side to other destinations)

Source		Destination			
IP	Port	FQDN/ IP	Ports	Application	Protocol
E-SBC WAN address	> 1023	DNS server 10.90.13.137 10.90.8.137	53	DNS	UDP
E-SBC WAN address	5060 to 5351	On-premises E-SBC VIP 10.175.0.38 (VIP) 10.175.0.36 (SBC5) 10.175.0.37 (SBC6)	5060 to 5351	SIP	UDP
E-SBC WAN address	16386 - 20385	On-premises E-SBC VIP 10.175.0.38 (VIP) 10.175.0.36 (SBC5) 10.175.0.37 (SBC6)	49152-65535	RTP	UDP
E-SBC WAN address	16386 - 20385	On-premises E-SBC VIP 10.175.0.38 (VIP) 10.175.0.36 (SBC5) 10.175.0.37 (SBC6)	49152-65535	RTCP	UDP

Notes:

- SIP using RTP or TCP is not used at this time but is available in IP phones.
- Terminal server to the on-premises E-SBC is not used (remote access uses SSH).

Firewall rules for on-premises E-SBC (WAN side to Bell VoIP support system)

The following rules apply if a firewall is placed between Bell Total Connect IP devices and the Internet.

Note: All end-points connected over the Internet will register to the SBC at least once every 600 seconds. This registration will work properly when your firewall pinhole timeout for SIP is set up for 600s and greater.

Cisco SPA 5xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	5060-5080 [1]	SBC Internet VIP IP: 67.69.255.72	5060	SIP4	TCP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	5060-5080 [1]	SIP	TCP
Customer-reserved IP address range	16384-16482 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535 [3]	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-16482 [2]	RTP	UDP
Customer-reserved IP address range	16384-16482 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-16482	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 20 concurrent sip sessions per device.

[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device

Cisco 68xx, 78xx and 88xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	5060-5080 [1]	SBC Internet VIP IP: 67.69.255.72	5060	SIP	UDP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	5060-5080 [1]	SIP	UDP
Customer-reserved IP address range	16384-32764 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-32764 [2]	RTP	UDP
Customer-reserved IP address range	16384-32764 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-32764	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 20 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device

Cisco ATAs 122 and 8000

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	5060-5063 [1]	SBC Internet VIP IP: 67.69.255.72	5060	SIP[4]	UDP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	5060-5063 [1]	SIP	UDP
Customer-reserved IP address range	16384-16482 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-16482 [2]	RTP	UDP
Customer-reserved IP address range	16384-16482 [2]	SBC Internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535	Customer-reserved IP address range	16384-16482 [2]	RTCP	UDP

[1]This is required by Cisco to be able to perform up to 4 concurrent sip sessions per device.
[2]This is required by Cisco to be able to perform up to 24 concurrent calls per device

Aastra 67xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	>1023	SBC Internet VIP IP: 67.69.255.72	5060	SIP[2]	TCP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	>1023	SIP	TCP
Customer-reserved IP address range	3000 – 2x number of lines	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	3000 – 2x number of lines	RTP	UDP
Customer-reserved IP address range	3000 – 2x number of lines	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	3000 – 2x number of lines	RTCP	UDP

[1]This is required by Aastra RTP is described in RFC1889. The UDP port used for RTP streams is traditionally an even-numbered port, and the RTCP control is on the next port up. A phone call therefore uses one pair of ports for each media stream. The RTP port is assigned to the first line on the phone, and is then incremented for each subsequent line available within the phone to provide each line a unique RTP port for its own use.
[2]Number of lines per Aastra models: 5 lines for 6731i and 9 lines for all other supported models.

Mediatrix 41xx and C7xx series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	16000 + number of FXS ports[1]	SBC Internet VIP IP: 67.69.255.72	5060	SIP[2]	UDP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	16000+number of FXS ports [1]	SIP	UDP
Customer-reserved IP address range	5004+2x number of calls	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	5004+2x number of calls	RTP	UDP
Customer-reserved IP address range	5004+2x number of calls	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	5004+2x number of calls	RTCP	UDP

[1]This is required by Media5 to have a specific SIP port per FXS port.

[2]This is required by Media5 to be able to reach the maximum number of concurrent calls per device.

Polycom VVX series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	5060	SBC Internet VIP IP: 67.69.255.72	5060	SIP[3]	UDP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	5060	SIP	UDP
Customer-reserved IP address range	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [1]	SBC Internet VIP IP: 67.69.255.72	49152-65535 [2]	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 [1]	RTP	UDP
Customer-reserved IP address range	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 [1]	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTCP	UDP

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 [1]	RTCP	UDP

[1]This is required by Polycom to be able to perform up to 24 concurrent calls per device. From vendor explanation: The starting port for RTP packets. Ports are allocated from a pool starting with this port up to a value of (start-port '50000'+ 47) for VVX310/410 or (start-port '50000'+ 95) for a VVX500/600.
[2]The ports used in the SBC ~16k are to be able to perform ~8k concurrent calls per SBC.

Polycom SSIP series

Source		Destination			
Phone IP	Port	IP	Port	Application	Protocol
0.0.0.0	68	255.255.255.255	67	DHCP discovery	UDP
Customer-reserved IP address range	68	Customer DHCP server	67	DHCP	UDP
Customer-reserved IP address range	> 1023	Customer Configured DNS server	53	DNS	UDP
Customer-reserved IP address range	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Customer-reserved IP address range	> 1023	TBD	123	NTP	UDP
Customer-reserved IP address range	5060	SBC Internet VIP IP: 67.69.255.72	5060	SIP	UDP
SBC Internet VIP IP: 67.69.255.72	5060	Customer-reserved IP address range	5060	SIP	UDP
Customer-reserved IP address range	2222-2268 [1]	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	2222-2268 [1]	RTP	UDP
Customer-reserved IP address range	2222-2268 [1]	SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	RTCP	UDP
SBC Internet VIP IP: 67.69.255.72	49152-65535 [1]	Customer-reserved IP address range	2222-2268 [1]	RTCP	UDP

[1]This is required by Polycom to be able to perform up to 24 concurrent calls per device. From Polycom vendor explanation: the value 2222 will be used for the first allocated RTP port. Subsequent ports will be allocated from a pool starting with the specified port plus two up to a value of (start-port + 46), after which the port number will wrap back to the starting value.

Appendix: Connection processes for apps and devices

This section outlines the steps involved when Bell Total Connect apps and devices connect and interact with the network.

Bell Total Connect desktop app connection process

1. When the desktop app starts it will connect to https://hipv-xsp2.bell.ca/bc/pc (67.69.241.0/24, 67.69.237.0/24)
2. The desktop app will authenticate the user and use HTTPS to download the user's configuration file from dms.totalconnect.bell.ca, which contains the credentials for all the other services below
3. The desktop app will then connect to the following:
   - https://totalconnect.bell.ca (67.69.237.0/24, 67.69.241.0/24) to load the 9-1-1 location banner
   - xmpp.totalconnect.bell.ca 67.69.237.0/24, 67.69.241.0/24, after performing xmpp service discovery) to sign in to the instant messaging and presence server
   - mtl-sbc.totalconnect.bell.ca (67.69.255.68, after performing SIP registrar discovery) to register as an SIP endpoint
   - If mtl-sbc.totalconnect.bell.ca does not respond, the desktop app will turn to tor-sbc.totalconnect.bell.ca (67.69.186.20)

Bell Total Connect receptionist web app connection process

1. When the receptionist web application starts for the first time, it will connect to the Bell Total Connect portal to download the Java libraries required to run the application. At each subsequent execution, the application will verify if updated libraries exist and will download them.
2. Subsequent traffic exchanges will occur between the receptionist app and the Bell Total Connect core network for call information on control messages using HTTPS.

Note: 'Keep alive' and network time protocol (NTP) messages will also be exchanged between the receptionist app and the Bell Total Connect core network.

Bell Total Connect phone connection process

The exact files exchanged and boot-up sequence will vary slightly between phone vendors. The sequence below uses Cisco phones as a typical example.

1. Phone at initial power-up or is factory reset (phone does not go to the on-premises E-SBC on a reboot)
2. Phone performs link layer discovery protocol (LLDP) to find out if there is a voice VLAN
3. Phone performs DHCP discovery on the voice VLAN (or native VLAN)
4. On-premises E-SBC provides:
   - IP address to phone
   - DNS server information
   - Itself as the FTP server and default gateway
5. Phone requests default configuration file to the on-premises E-SBC
6. Phone resolves Bell Total Connect device management server address using the DNS server address provided by the on-premises E-SBC
7. Phone updates firmware if required from the Bell Total Connect device management server
8. Phone gets second configuration file for its model from the Bell Total Connect device management server
9. Phone prompts technician to enter username and password for this particular user
10. Phone gets user-specific configuration files from the Bell Total Connect device management server
11. Phone resets and is ready to use

The phone will periodically fetch its user-specific configuration file and update its configuration if required.

If a user changes the language of the phone display, the phone will get the proper language file from the Bell Total Connect device management server if required.