



Bell Connexion totale

Exigences relatives aux connexions et au coupe-feu

Table des matières

Introduction	3
Interprétation des tableaux des règles de coupe-feu dans le présent document	3
Exemple d'architecture de réseau Bell Connexion totale	1
Exigences de connexion pour les applications Bell Connexion totale	2
Exigences concernant le Protocole DHCP et le serveur DNS	2
Règles de coupe-feu pour les applications Bell Connexion totale	2
Les règles de coupe-feu pour l'application de bureau Bell Connexion totale avec voix sur Internet	2
Règles de coupe-feu pour l'application de bureau Bell Connexion totale avec voix sur MPLS	4
Règles de coupe-feu pour l'application mobile Bell Connexion totale	5
Firewall rules for Bell Total Connect for Skype for Business	6
Règles de coupe-feu pour l'application Réceptionniste de Bell Connexion totale	7
Règles de coupe-feu pour l'application de bureau Bell Connexion totale Webex (standard)	7
Règles de coupe-feu pour l'application mobile Webex de Bell Connexion totale	8
Règles de coupe-feu pour l'application de bureau Bell Connexion totale Webex avec vidéo maillée	9
Table WX-Média	10
Utilisation du contrôleur CSP sur place comme serveur mandataire	10
Exigences de connexion pour l'équipement Bell Connexion totale	11
Options DHCP	11
Règles de coupe-feu pour l'équipement Bell Connexion totale (accès RPVIP)	11
Règles de coupe-feu pour les équipements Bell Connexion totale (contournement ou Internet)	18
Exigences de connexion pour les contrôleurs CSP-E sur place	20
Règles de coupe-feu pour les contrôleurs CSP-E sur place	20
Firewall rules for on-premises E-SBC devices	20
Règles de coupe-feu pour le contrôleur CSP-E sur place (du côté réseau étendu du système de soutien VoIP de Bell)	21
Règles de coupe-feu pour le contrôleur CSP-E sur place (du côté réseau étendu vers d'autres destinations)	21
Règles de coupe-feu pour le routage de basculement à Internet	22
Mediatix 41xx and C7xx series	24
Polycom VVX series	24
Annexe : Processus de connexion pour les applications et l'équipement	26
Processus de connexion de l'application de bureau Bell Connexion totale	26
Processus de connexion de l'application Réceptionniste de Bell Connexion totale	26
Processus de connexion des téléphones Bell Connexion totale	26

Introduction

Le présent guide présente les principales exigences auxquelles doivent satisfaire les adresses IP et les coupe-feu pour que les applications et appareils Bell Connexion totale fonctionnent correctement. Les spécialistes du réseau ou des TI de l'entreprise devraient consulter ce guide pour déterminer s'ils doivent modifier leurs paramètres réseau lors de la configuration initiale du service Bell Connexion totale.

Ce guide facilitera également le dépannage d'éventuels problèmes de connexion éprouvés par les utilisateurs finaux lorsque le service Bell Connexion totale sera en fonction.

Il est fortement recommandé que les étapes décrites dans ce document soient appliquées avec l'aide d'un ingénieur ou d'un expert des services professionnels de Bell.

Interprétation des tableaux des règles de coupe-feu dans le présent document

La nature du trafic IP entre les applications/appareils sur place et l'équipement local ou distant de Bell/du partenaire peut être l'une des suivantes :

- Unidirectionnelle (p. ex., Journal système)
- Demande/réponse (p. ex. HTTPS)
- Service bidirectionnel en temps réel (p. ex. Protocolee de transmission en temps réel (RTP) pour les appels audio/vidéo)

Une fonction de sécurité de couche 3, comme une liste de contrôle d'accès (ACL) ou un coupe-feu statique de couche 4, devrait tenir compte de toutes les directions possibles du trafic IP pour contrôler ce trafic

adéquatement. Les deux directions peuvent être impliquées dans les flux bidirectionnels en temps réel, décrits individuellement sous forme de règles distinctes de source/destination dans le présent document. Veuillez noter qu'en rendant ces règles bidirectionnelles explicites, elles peuvent aussi être utilisées pour les coupe-feu

dynamiques de couche 4, car le destinataire local ou distant peut établir la « connexion » de couche 4 impliquée dans les flux bidirectionnels en temps réel. Ce serait le cas pour les flux RTP du Protocolee UDP utilisés pour les appels audio/vidéo. Les coupe-feu dynamiques de couche 4 définissent ensuite des politiques explicites pour chaque orientation de connexion possible.

Lorsque des coupe-feu dynamiques de couche 4 et la traduction d'adresse de port réseau (NAPT) sont utilisés (habituellement le cas des applications Bell Connexion totale sur les appareils Internet ou du routage de basculement vers Internet), seules les connexions sécurisées à non sécurisées (ou réseau local à réseau étendu) ont lieu, même pour les flux en temps réel naturellement bidirectionnels. Plus précisément, toutes les connexions impliquant une application ou un appareil Bell Connexion totale sous cette topologie, que ce soit le Protocolee de contrôle de transmission (TCP) ou le Protocolee UDP, sont établies à partir du réseau de l'entreprise et ciblent un contrôleur de session en périphérie (CSP) Internet de Bell.

Pour gérer cette « direction forcée » du trafic autrement bidirectionnel en temps réel, le CSP Internet de Bell exécute une fonction de traversée de traduction d'adresse de réseau hébergée (NAT). Cela signifie que les applications et appareils sur place lancent toutes les connexions de Protocolee d'ouverture de session (SIP)/ Sécurité de la couche transport (TLS) et le CSP Internet de Bell. Après avoir détecté la présence de la NAT du client, ils réutilisent toujours cette connexion de couche 4 établie pour transmettre la signalisation d'appel dans la direction inverse (de Bell à l'application/appareils).

Dans cette topologie, le CSP Internet de Bell n'amorce jamais le flux de données RTP vers le client. Elle attend que la connexion RTP opposée soit établie à partir des locaux du client et envoie son trafic RTP au sein de cette connexion de couche 4. Cette fonction du CSP s'appelle la « transmission symétrique en temps réel » (RTP symétrique).

En résumé, lorsqu'on utilise un coupe-feu dynamique de couche 4 avec Protocolee NAPT, les règles de source/ destination Bell à client décrites dans les tableaux du présent document sont redondantes et quelque peu non applicables directement. Seuls les flux entre le client et Bell doivent être mis en œuvre comme des politiques de coupe-feu.

Exemple d'architecture de réseau Bell Connexion totale

Le service Bell Connexion totale peut être mis en œuvre de diverses façons. La figure 1 ci-dessous présente l'une des architectures de réseau les plus fréquentes.

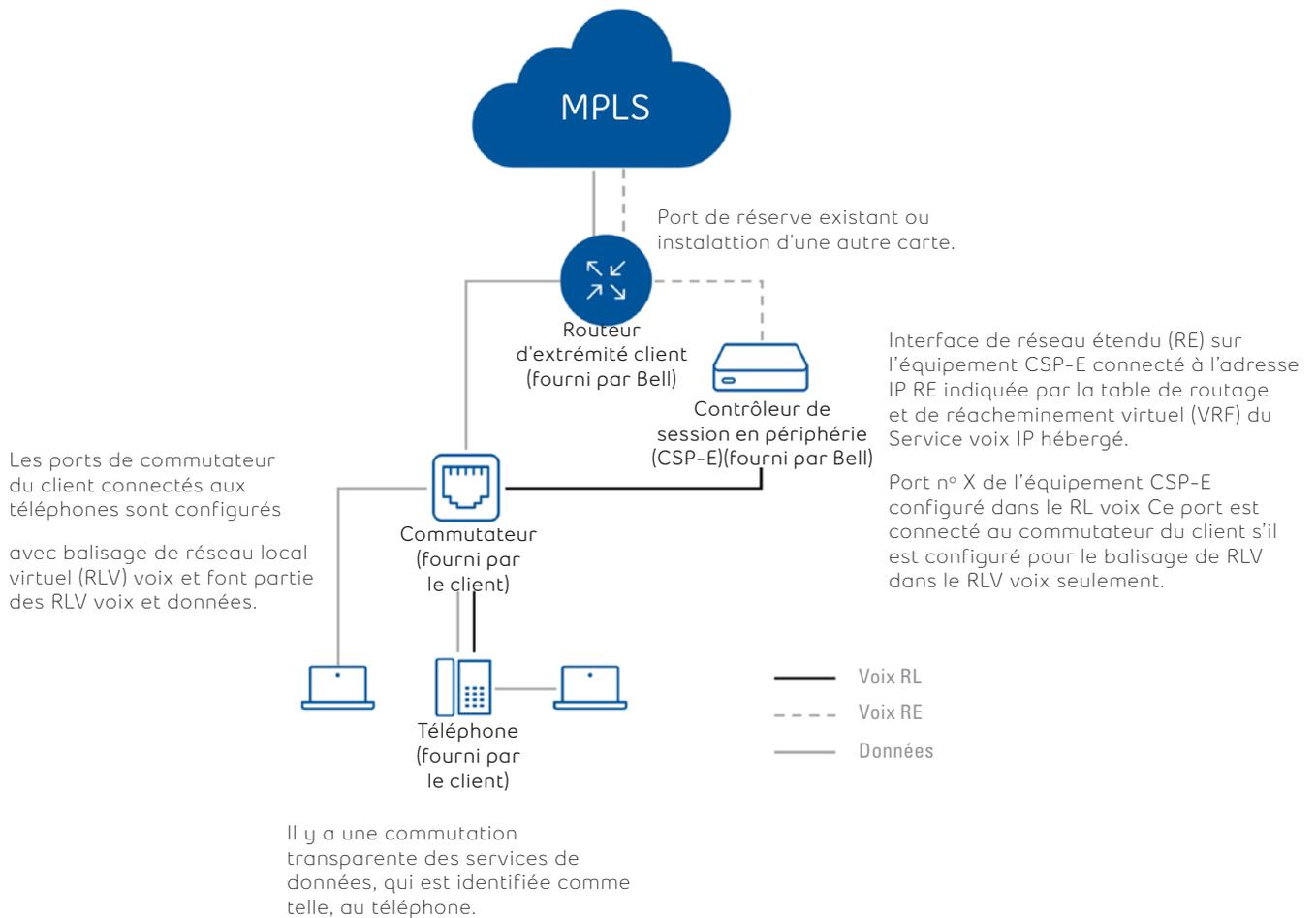


Figure 1. Architecture de réseau local de base

Dans certains cas, le trafic CSP-E (contrôleur de session en périphérie) peut passer par un commutateur ou un coupe-feu avant d'être acheminé au routeur d'extrémité client (CE) appartenant à Bell. Comme des coupe-feu peuvent être insérés à de nombreux points du réseau, il se pourrait que certaines règles de coupe-feu doivent être adaptées et mises en œuvre à plus d'un endroit. (S'il n'y a pas de coupe-feu entre le CSP-E et le routeur CE, les règles de coupe-feu décrites dans le présent document ne seront pas nécessaires.)

Exigences de connexion pour les applications Bell Connexion totale

Selon leurs besoins et les forfaits qui font partis de leur service, les utilisateurs du service Bell Connexion totale peuvent choisir d'installer d'autres applications : l'application de bureau ainsi que l'application Réceptionniste de Bell Connexion totale (console d'appels), qui est habituellement réservée à un petit groupe d'utilisateurs à qui on a attribué des fonctions de réceptionniste. Toutes les applications utilisent les données RLV de votre réseau local pour se connecter au réseau Internet public et sont lancées depuis l'ordinateur de l'utilisateur.

Exigences concernant le Protocole DHCP et le serveur DNS

Les adresses IP des ordinateurs de chacun des utilisateurs sont fournies par le serveur DHCP (Protocole de configuration dynamique de l'hôte) de votre organisation et sont réutilisées par l'application de bureau et l'application Réceptionniste (console d'appels).

Les applications Bell Connexion totale se servent du système de nom par domaine (DNS) pour repérer les différents éléments réseau. Un ordinateur sur lequel tourne une application Bell Connexion totale/Webex doit avoir accès à un serveur DNS qui peut traduire les noms d'hôte des serveurs intégrés à l'application de bureau et/ ou à l'application Réceptionniste (console d'appels).

Remarque : Les noms d'hôte et les adresses IP figurant au présent document sont susceptibles d'être modifiés.

Règles de coupe-feu pour les applications Bell Connexion totale

Les règles suivantes s'appliquent si le réseau local qui gère l'interaction des applications Bell Connexion totale emploie des coupe-feu pour le trafic sortant.

Remarque : Un coupe-feu utilisant une passerelle SIP de la couche application n'est pas recommandé pour le service Bell Connexion totale. Bien qu'en général ces passerelles fonctionnent adéquatement, elles peuvent parfois provoquer la perte des messages SIP qu'elles ne parviennent pas à identifier correctement.

Les règles de coupe-feu pour l'application de bureau Bell Connexion totale avec voix sur Internet

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocole
N'importe quel ordinateur	>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
N'importe quel ordinateur	45001	mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	SIP	UDP
mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	>1024	sb23-24toronto01.secure.btc.bell.ca sb21-22montreal02.secure.btc.bell.ca sb5-6halifax01.secure.btc.bell.ca sb5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180 (Ceci est le processus d'établissement d'une connexion)	5061	SIP sécurisé	TCP

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocole
184.150.213.164 184.150.213.172 184.150.213.180 184.150.213.178	5061	N'importe quel ordinateur (Ce processus a toujours recours à des connexions préétablies; consultez le processus ci-dessus.)	>1024	SIP sécurisé	TCP
N'importe quel ordinateur	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
mtl-sbc.totalconnect.bell.ca 67.69.255.68	49152 to 65535 ¹	N'importe quel ordinateur	8500 to 8598 ¹ (Audio) 8600 to 8698 ¹ (Video)	RTP Audio RTP Video	UDP
N'importe quel ordinateur	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	N'importe quel ordinateur	8500 to 8598 ¹ (Audio) 8600 to 8698 ¹ (Video)	SRTP Audio SRTP Video	UDP
N'importe quel ordinateur	45001	tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	SIP	UDP
tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	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	N'importe quel ordinateur	8500 to 8598 ¹ (Audio) 8600 to 8698 ¹ (Video)	RTP Audio RTP Video	UDP
N'importe quel ordinateur	>1024	Customer LDAP server	389 636	LDAP LDAPS	TCP
N'importe quel ordinateur	>1023	xmpp.totalconnect.bell.ca 67.69.237.0/24 67.69.241.0/24	5222 1081 443	XMPP SOCKS HTTPS	TCP
N'importe quel ordinateur	>1023	sharing.totalconnect.bell.ca 67.69.237.0/24 67.69.241.0/24	443	TLS/WSS	TCP

¹ C'est ce qu'exige le fournisseur pour les appels vocaux et vidéo.

Règles de coupe-feu pour l'application de bureau Bell Connexion totale avec voix sur MPLS

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocole
N'importe quel ordinateur	> 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
N'importe quel ordinateur	45001	Adresse IP de RL CSP-E	5060	SIP	UDP
Adresse IP de RL CSP-E	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	8500 to 8598 ¹ (Audio) 8600 to 8698 ¹ (Video)	Adresse IP de RL CSP-E	49152 to 65535 ¹	RTP Audio	UDP
Adresse IP de RL CSP-E	49152 to 65535 ¹	N'importe quel ordinateur	8500 to 8598 ¹ (Audio)	RTP Audio	UDP
N'importe quel ordinateur	45001	Adresse IP de RL CSP-E	5060	SIP	UDP
Adresse IP de RL CSP-E	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	8500 to 8598 ¹ (Audio) 8600 to 8698 ¹ (Video)	Adresse IP de RL CSP-E	49152 to 65535 ¹	RTP Audio	UDP
Adresse IP de RL CSP-E	49152 to 65535 ¹	N'importe quel ordinateur	8500 to 8598 ¹ (Audio)	RTP Audio	UDP
N'importe quel ordinateur	>1024	Customer LDAP server	389 636	LDAP LDAPS	TCP
N'importe quel ordinateur	>1023	xmpp.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	5222 1081 443	XMPP SOCKS HTTPS	TCP
N'importe quel ordinateur	>1023	sharing.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	43	TLS/ WSS	TCP

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

Règles de coupe-feu pour l'application mobile Bell Connexion totale

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocole
N'importe quel téléphone 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 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
N'importe quel téléphone 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	SIP sécurisé	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	N'importe quel téléphone mobile	5061	SIP sécurisé	TCP
N'importe quel téléphone 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	N'importe quel téléphone mobile	8500-8598 ¹ 8600-8698 ¹	SRTP	UDP
iOS devices	>1023	Notifications push d'Apple 17.0.0.0/8	5223 443	HTTPS	TCP
Android Devices	>1023	Google ne fournit pas d'adresses IP particulières pour les serveurs.	5228 5229 5230	HTTPS	TCP
N'importe quel téléphone mobile	>1023	Messagerie instantanée et gestion de la présence xmpp.totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	5222 443	XMPP TLS HTTPS	TCP

¹This 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	Protocole
N'importe quel ordinateur	> 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
N'importe quel ordinateur	45001	mtl-sbc.totalconnect.bell.ca 67.69.255.68	5060	SIP	UDP
mtl-sbc. totalconnect.bell.ca 67.69.255.68	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	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	N'importe quel ordinateur	8500 to 8598 ¹	RTP	UDP
N'importe quel ordinateur	45001	tor-sbc.totalconnect.bell.ca 67.69.186.20	5060	SIP	UDP
tor-sbc. totalconnect.bell.ca 67.69.186.20	5060	N'importe quel ordinateur	45001	SIP	UDP
N'importe quel ordinateur	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	N'importe quel ordinateur	8500 to 8598 ¹	RTP	UDP

¹C'est ce qu'exige le fournisseur pour les appels vocaux et vidéo.

Règles de coupe-feu pour l'application Réceptionniste de Bell Connexion totale

Source		Destination			
IP	Port	FQDN/IP	Port	Application	Protocole
N'importe quel ordinateur	>1023	totalconnect.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP

Règles de coupe-feu pour l'application de bureau Bell Connexion totale Webex (standard – sans vidéo maillée)

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocole	Objectif
N'importe quel ordinateur	>1023	n'importe laquelle	443	HTTPS, WSS	TCP	Sécuriser la signalisation et la messagerie
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000 33434	SRTP	UDP	Sécuriser le son, la vidéo et le partage de contenu sur les appareils Webex Teams, sur les ports primaires et sur les ports secondaires
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000 33434	SRTP	TCP	Utilisé pour sécuriser le partage de contenu sur les appareils Webex Teams en tant que réacheminement de secours si UDP ne peut pas être utilisé; ports primaires et secondaires
N'importe quel ordinateur	>1023	See Table WX-Media	33434- 33598 49152- 59999	SRTP	UDP	Sécuriser les médias audio, vidéo et de partage de contenu
N'importe quel ordinateur	>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	Récupérer la connexion Bell Connexion totale et les renseignements du profil
N'importe quel ordinateur	>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	SIP sécurisé	TCP	Sécuriser la signalisation et la messagerie avec Bell
N'importe quel ordinateur	>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	Sécuriser le son et la vidéo avec Bell
142.177.151.188 184.150.213.180 184.150.213.164 184.150.213.172	49152 - 65535	N'importe quel ordinateur (Ce processus a toujours recours à des connexions préétablies; consultez le processus ci-dessus.)	>1023	SRTP	UDP	Sécuriser le son et la vidéo avec Bell

Règles de coupe-feu pour l'application mobile Webex de Bell Connexion totale

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocole	Objectif
N'importe quel ordinateur	>1023	n'importe laquelle	443	HTTPS, WSS	TLS	Sécuriser la signalisation et la messagerie
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000 33434	SRTP	UDP	Sécuriser le son, la vidéo et le partage de contenu sur les appareils Webex Teams, sur les ports primaires et sur les ports secondaires
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000 33434	SRTP	TCP	Utilisé pour sécuriser le partage de contenu sur les appareils Webex Teams en tant que réacheminement de secours si UDP ne peut pas être utilisé; ports
N'importe quel ordinateur	>1023	See Table WX-Media	33434- 33598 49152- 59999	SRTP	UDP	Sécuriser les médias audio, vidéo et de partage de contenu
N'importe quel ordinateur	>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	Récupérer la connexion Bell Connexion totale et les renseignements du profil
N'importe quel ordinateur	>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	Sécuriser la signalisation et la messagerie avec Bell
N'importe quel ordinateur	>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	Sécuriser le son et la vidéo avec Bell

Règles de coupe-feu pour l'application de bureau Bell Connexion totale Webex avec vidéo maillée

Peu de clients choisissent de déployer Video Mesh. Les clients qui choisissent Vidéo Mesh doivent suivre les règles suivantes au lieu des règles à la section 2.2.6. En déployant Video Mesh, les clients peuvent limiter le volume du trafic sortant de leur réseau sur Internet et réduire le nombre de communications directes entre les appareils finaux et Cisco.Source Destination

Source		Destination				
IP	Port	FQDN/IP	Port	Application	Protocole	Objectif
Video Mesh Node	>1023	n'importe laquelle	444	HTTPS	TLS	Signalisation en cascade sécurisée du nœud Video Mesh sur le nuage Webex
Video Mesh Nodes Hybrid Data Security Nodes Webex Hybrid Services Connectors	>1023	n'importe laquelle	123	NTP	UDP	Protocolee de synchronisation réseau (NTP)
Video Mesh Nodes Hybrid Data Security Nodes Webex Hybrid Services Connectors	>1023	n'importe laquelle	53	DNS	UDP, TCP	Système de nom par domaine (DNS)
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000	SRTP	UDP	Sécuriser le son, la vidéo et le partage de contenu sur les appareils Webex Teams
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000	SRTP	TCP SRTP	Utilisé pour sécuriser le partage de contenu sur les appareils Webex Teams en tant que réacheminement de secours si UDP ne peut pas être utilisé
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000	SRTP	UDP	Sécuriser les médias audio, vidéo et de partage de contenu du nœud Video Mesh au nuage Webex
N'importe quel ordinateur	>1023	See Table WX-Media	5004 9000	SRTP	TCP SRTP	Sécuriser les médias audio, vidéo et de partage de contenu du nœud Video Mesh au nuage Webex (solution de secours)
N'importe quel ordinateur	>1023	See Table WX-Media	33434- 33598 and 49152- 59999		UDP SRTP	Sécuriser les médias audio, vidéo et de partage de contenu
N'importe quel ordinateur	>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	Récupérer la connexion BCT et les renseignements du profil
N'importe quel ordinateur	>1023	sb23-24toronto01.secure.btc.bell.ca sb21-22montreal02.secure.btc.bell.ca sb5-6halifax01.secure.btc.bell.ca sb5-6calgary42.secure.btc.bell.ca 184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	5061	SIP sécurisé	TCP	Sécuriser la signalisation et la messagerie avec Bell
N'importe quel ordinateur	>1023	sb23-24toronto01.secure.btc.bell.ca sb21-22montreal02.secure.btc.bell.ca sb5-6halifax01.secure.btc.bell.ca sb5-6calgary42.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	Sécuriser le son et la vidéo avec Bell
142.177.151.188 184.150.213.180 184.150.213.164 184.150.213.172	49152 - 65535	N'importe quel ordinateur (This flow always reuses pre-established connections – see above)	>1023	SRTP	UDP	Sécuriser le son et la vidéo avec Bell

Table WX-Média

Le tableau ci-dessous fait la liste des nombreuses adresses IP et des nombreux sous-réseaux IP liés à l'exploitation de Webex, pour permettre aux tableaux de règles de coupe-feu de rester lisibles.

Remarque : Toutes les adresses dans les sous-réseaux suivants sont réservées à l'usage exclusif de Cisco; cependant, elles sont enregistrées auprès de Cisco, de Microsoft Azure et des Amazon Web Services (AWS) en Amérique du Nord et en Europe.

Sous-réseau IP pour les services médias		
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

Utilisation du contrôleur CSP sur place comme serveur mandataire

Si votre organisation ne permet pas l'accès au réseau Internet public ou aux ports spécifiques nécessaires au bon fonctionnement des applications sur les ordinateurs, nous pouvons mettre en œuvre un processus d'adaptation de solutions clients (PASC) pour permettre à l'application Réceptionniste d'utiliser le contrôleur de session en périphérie (CSP-E) sur place pour joindre les serveurs du réseau fédérateur Voix sur IP (VoIP) de Bell. Si vous souhaitez discuter de cette situation, veuillez vous adresser à votre conseiller en communications.

Exigences de connexion pour l'équipement Bell Connexion totale

Contrairement aux applications Bell Connexion totale sur ordinateur, l'équipement IP Bell Connexion totale se sert du RLV voix pour communiquer avec le contrôleur CSP sur place et joindre les serveurs Bell Connexion totale dans le réseau de Bell.

Options DHCP

Les adresses IP de l'équipement Bell Connexion totale sont fournies par le serveur DHCP de votre organisation (avec réacheminement au contrôleur CSP-E sur place qui fait office de serveur mandataire SIP ou de sortie) ou par le réseau local CSP-E sur place (avec le sous-réseau et la plage d'adresses IP fournis par votre organisation et exclus de votre serveur DHCP).

Remarque : La plage d'adresses IP d'un équipement Bell Connexion totale est bloquée dans vos serveurs DHCP et ne peut être réutilisée pour d'autres applications Bell Connexion totale.

Règles de coupe-feu pour l'équipement Bell Connexion totale (accès RPVIP)

Les règles suivantes s'appliquent lorsqu'un coupe-feu est placé entre l'équipement IP Bell Connexion totale et le contrôleur CSP-E sur place (du côté réseau local). (Il est recommandé d'éviter de placer le coupe-feu à cet endroit dans la mesure du possible.)

Remarque : Tous les points d'extrémité connectés par RPV IP tentent de s'enregistrer dans le CSP-E à intervalles de 60 secondes. Ces tentatives réussissent lorsque la durée d'ouverture du port du coupe-feu utilisé par le protocole SIP est d'au moins 60 secondes.

Cisco series SPA 5xx

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-5080 ¹	Adresse IP de RL CSP-E	5060	SIP	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060-5080 ¹	SIP	TCP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à 20 séances SIP simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

³Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie

Cisco CP 78xx and 88xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp2.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-5080	Adresse IP de RL CSP-E	5060	SIP	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060-5080 ¹	SIP	TCP
Plage d'adresses IP réservée au client	16384-32764 ²	Adresse IP de RL CSP-E	16384-32764 ³	RTP RTCP	UDP
Adresse IP de RL CSP-E	16384-32764 ³	Plage d'adresses IP réservée au client	16384-32764 ²	RTP RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à 20 séances sip simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

³Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4k doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux rtp à acheminer nécessite deux ports (un pour rtp et un pour rtcp). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux rtp que vous voulez traiter.

Cisco ATA 192

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-50631	Adresse IP de RL CSP-E	5060	SIP	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060-5063	SIP	TCP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTCP	UDP

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à quatre séances SIP simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

³Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

Cisco ATAs 122 and 8000

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 8443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-50631	Adresse IP de RL CSP-E	5060	SIP	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060-5063	SIP	TCP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Adresse IP de RL CSP-E	16386-20385 ³	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ³	Plage d'adresses IP réservée au client	16384-16482 ²	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à quatre séances SIP simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

³Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

Aastra 67xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	>1023	Adresse IP de RL CSP-E	5060	SIP	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	>1023	SIP	TCP
Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes ¹	RTP	UDP
Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes ¹	RTCP	UDP

¹Requis par le protocole RTP d'Aastra, conformément à la description fournie dans la DC 1889. Le port UDP utilisé pour les flux RTP est traditionnellement un port pair, et le contrôle RTCP est sur le port suivant. Un appel téléphonique utilise donc une paire de ports pour chaque flux média. Le port RTP est attribué à la première ligne du téléphone, puis il change pour chaque ligne subséquente disponible dans le téléphone pour fournir à chaque ligne un port RTP unique pour sa propre utilisation.

²Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

³Nombre de lignes par modèle Aastra : 5 lignes pour 6731i et 9 lignes pour tous les autres modèles pris en charge.

Mediatrix 41xx and C7xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	16000 + nombre de ports FXS ¹	Adresse IP de RL CSP-E	5060	SIP ³	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	16000+nombre de ports FXS	SIP	TCP
Plage d'adresses IP réservée au client	5004+2x nombre d'appels	Adresse IP de RL CSP-E	16386-20385 ²	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	5004+2x nombre d'appels	RTP	UDP
Plage d'adresses IP réservée au client	5004+2x nombre d'appels	Adresse IP de RL CSP-E	16386-20385 ²	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	5004+2x nombre d'appels	RTCP	UDP

¹Exigé par Media5 pour avoir un port SIP spécifique par port FXS.

²Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

³Ceci est requis par Media5 pour atteindre le nombre maximum d'appels simultanés par appareil.

Séries Polycom VVX

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client or the Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	69	TFTP	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060	Adresse IP de RL CSP-E	5060	SIP ³	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060	SIP	TCP
Plage d'adresses IP réservée au client	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	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
Plage d'adresses IP réservée au client	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	Port nombre impair 50001 to 50047 on VVX 310 and 410 50001 to 50095 on VVX 500 and 600 ¹	RTCP	UDP

¹Ceci est requis par Polycom pour effectuer jusqu'à 24 appels simultanés par appareil. Selon l'explication du fournisseur Polycom : le port de départ pour les paquets RTP. Les ports sont attribués à partir d'une réserve en commençant par ce port jusqu'à une valeur de (port initial 50000 + 47) pour VVX310/410 ou (port initial 50000 + 95) pour VVX500/600.

²Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

Polycom series SSIP

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client or the Adresse IP de RL CSP-E	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	Adresse IP de RL CSP-E	21	FTP	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Plage d'adresses IP réservée au client	> 1023	67.69.237.133 67.69.237.134	123	NTP	UDP
Plage d'adresses IP réservée au client	5060	Adresse IP de RL CSP-E	5060	SIP ³	TCP
Adresse IP de RL CSP-E	5060	Plage d'adresses IP réservée au client	5060	SIP	TCP
Plage d'adresses IP réservée au client	2222-2268 ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	2222-2268 ¹	RTP	UDP
Plage d'adresses IP réservée au client	2222-2268 ¹	Adresse IP de RL CSP-E	16386-20385 ²	RTCP	UDP
Adresse IP de RL CSP-E	16386-20385 ²	Plage d'adresses IP réservée au client	2222-2268 ¹	RTCP	UDP

¹Ceci est requis par Polycom pour effectuer jusqu'à 24 appels simultanés par appareil. Explication du fournisseur Polycom : la valeur 2222 sera utilisée pour le premier port RTP attribué. Les ports ultérieurs seront attribués à partir d'une réserve en commençant par le port indiqué plus deux jusqu'à une valeur de (port initial + 46), après quoi le numéro de port reviendra à la valeur de départ.

²Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

Règles de coupe-feu pour les équipements Bell Connexion totale (contournement ou Internet)

Les règles suivantes s'appliquent si un pare-feu est placé entre les appareils IP Bell Connexion totale (pris en charge sur Internet) et la connexion Internet.

Pour chaque appareil en particulier, nous devons appliquer une règle supplémentaire pour permettre l'accès au serveur ZTP du fournisseur. Cette règle est décrite dans les sections suivantes. Source Destination

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
Tout appareil de contournement de Bell	> 1023	hipv-xsp2.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Tout appareil de contournement de Bell	> 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	SIP sécurisé	TCP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	5061	Tout appareil de contournement de Bell (This flow reuses pre-established connections)	> 1023	SIP sécurisé	TCP
Tout appareil de contournement de Bell	> 1023	time.nrc.ca 132.246.11.227 132.246.11.229 132.246.11.238 132.246.11.237 ²	123	NTP	UDP

¹C'est ce qu'exige le fournisseur pour les appels vocaux et vidéo.

²Le service NTP (temps réseau) est offert par le Conseil national de recherches Canada. Ces adresses peuvent changer, donc il est recommandé de filtrer en employant time.nrc.ca plutôt que les adresses IP.

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

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
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	Plage d'adresses IP réservée au client (Ce flux réutilise une connexion)	16384-32764	SRTP	UDP

¹Ici, nous devons autoriser la gamme entière d'adresses IP parce que le serveur ZTP du fournisseur peut utiliser des adresses différentes au fil du temps.

Cisco 192 ATA

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
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

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	Plage d'adresses IP réservée au client (Ce flux réutilise une connexion)	16384-32764	S RTP	UDP

¹Ici, nous devons autoriser la gamme entière d'adresses IP parce que le serveur ZTP du fournisseur peut utiliser des adresses différentes au fil du temps.

Polycom Polycom (V VX150, V VX250, V VX310/311, V VX350, V VX410/411, V VX450, V VX500/501, V VX600/601, TRIO8300)

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
Polycom phones	> 1023	ztp.polycom.com 0.0.0.0/0 ¹	443	HTTPS	TCP
Polycom phones	Even port 50000 to 50047 on V VX 310/311 and 410/411 50000 to 50095 on V VX 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	49152-65535 ³	S RTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535 ³	Polycom phones	Even port 50000 to 50047 on V VX 310/311 and 410/411 50000 to 50095 on V VX 500/501 and 600/601 ²	S RTP	UDP

¹Ici, nous devons autoriser la gamme entière d'adresses IP parce que le serveur ZTP du fournisseur peut utiliser des adresses différentes au fil du temps.

²Ceci est requis par Polycom pour effectuer jusqu'à 24 appels simultanés par appareil. Selon l'explication du fournisseur Polycom : le port de départ pour les paquets RTP. Les ports sont attribués à partir d'une réserve en commençant par ce port jusqu'à une valeur de (port initial 50000 + 47) pour V VX310/311/410/411 ou (port initial 50000 + 95) pour V VX500/501/600/601.

³Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

Mediatrix (Mediatrix4102, MediatrixC711, MediatrixS724)

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
Dispositifs Mediatrix	> 1023	ems2.media5corp.com 0.0.0.0/0 ¹	443	HTTPS	TCP
Dispositifs Mediatrix	5004+2x nombre d'appels 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	S RTP	UDP
184.150.213.164 184.150.213.172 142.177.151.188 184.150.213.180	49152-65535	Dispositifs Mediatrix	5004+2x nombre d'appels ³	S RTP	UDP

¹Ici, nous devons autoriser la gamme entière d'adresses IP parce que le serveur ZTP du fournisseur peut utiliser des adresses différentes au fil du temps.

²Les ports utilisés dans le contrôleur de session en périphérie d'entreprise 4K doivent être en mesure d'effectuer jusqu'à 2 000 appels simultanés par contrôleur de session en périphérie d'entreprise. Explication du fournisseur de contrôleur de session en périphérie d'entreprise : chaque flux RTP à acheminer nécessite deux ports (un pour RTP et un pour RTCP). Cela signifie que vous aurez besoin, au minimum, du double de ports que le nombre de flux RTP que vous voulez traiter.

³Ceci est requis par Media5 pour atteindre le nombre maximum d'appels simultanés par appareil.

Exigences de connexion pour les contrôleurs CSP-E sur place

Le contrôleur CSP-E sur place de votre organisation représente le point de démarcation du service Bell Connexion totale. Surveillé et contrôlé par le système de soutien VoIP centralisé qui se trouve dans le réseau de Bell, il fournit différents services aux téléphones Bell Connexion totale, notamment :

- Serveur mandataire SIP pour les téléphones Bell Connexion totale
- Service TFTP et FTP pour l'approvisionnement des téléphones
- Contrôle d'admission d'appel
- Surveillance de la qualité du signal vocal
- Fonctions de sécurité et d'assurance du service
- Balisage RLV voix

Remarque : Dans une installation standard, seuls les téléphones Bell Connexion totale utilisent le contrôleur CSP-E sur place (c.-à-d. que les applications Bell Connexion totale sur ordinateur ne l'utilisent pas).

Règles de coupe-feu pour les contrôleurs CSP-E sur place

Si un coupe-feu se trouve entre le contrôleur CSP-E sur place et le routeur d'extrémité client (CE), il doit être configuré pour l'acheminement des protocoles VoIP par le contrôleur CSP-E sur place. Le coupe-feu ne peut pas faire la traduction d'adresse réseau (NAT) – cela contreviendrait au protocole VoIP. Comme le contrôleur CSP-E sur place est un serveur mandataire VoIP, tous les paquets VoIP auront comme adresse IP source ou de destination l'interface réseau étendu du contrôleur CSP-E sur place.

L'adresse IP du réseau étendu du contrôleur CSP-E sur place est fournie par :

- **Bell** – si le routeur CE de réseau privé virtuel IP (RPV IP) a une connexion directe au contrôleur CSP-E sur place (c'est le scénario d'installation standard)
- **Votre organisation** – si le trafic passe par votre réseau local pour atteindre le routeur CE, ce qui signifie qu'il n'y a pas de connexion directe entre le contrôleur CSP-E sur place et le routeur CE (c'est le scénario d'installation avec PASC)

Remarque : Étant donné que le trafic est bidirectionnel à moins d'indication contraire, la source et la destination peuvent être interverties dans certains cas. La source de la communication (ou demandeur) aura généralement > 1023 comme port source et communiquera avec le numéro de port fixé pour le protocole.

Firewall rules for on-premises E-SBC devices

Si un coupe-feu se trouve entre le contrôleur CSP-E sur place et le routeur d'extrémité client (CE), il doit être configuré pour l'acheminement des protocoles VoIP par le contrôleur CSP-E sur place. Le coupe-feu ne peut pas faire la traduction d'adresse réseau (NAT) – cela contreviendrait au protocole VoIP. Comme le contrôleur CSP-E sur place est un serveur mandataire VoIP, tous les paquets VoIP auront comme adresse IP source ou de destination l'interface réseau étendu du contrôleur CSP-E sur place.

L'adresse IP du réseau étendu du contrôleur CSP-E sur place est fournie par :

- **Bell** – si le routeur CE de réseau privé virtuel IP (RPV IP) a une connexion directe au contrôleur CSP-E sur place (c'est le scénario d'installation standard)
- **Votre organisation** – si le trafic passe par votre réseau local pour atteindre le routeur CE, ce qui signifie qu'il n'y a pas de connexion directe entre le contrôleur CSP-E sur place et le routeur CE (c'est le scénario d'installation avec PASC)

Remarque : Étant donné que le trafic est bidirectionnel à moins d'indication contraire, la source et la destination peuvent être interverties dans certains cas. La source de la communication (ou demandeur) aura généralement > 1023 comme port source et communiquera avec le numéro de port fixé pour le protocole.

Règles de coupe-feu pour le contrôleur CSP-E sur place (du côté réseau étendu du système de soutien VoIP de Bell)

Source		Destination			
IP	Port	FQDN/ IP	Ports	Application	Protocole
Adresse RE du contrôleur CSP-E	> 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
Adresse RE du contrôleur CSP-E	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
Adresse RE du contrôleur CSP-E	> 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
Système de soutien VoIP 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	> 1023	Adresse RE du contrôleur CSP-E	22	SSH	TCP
Système de soutien VoIP 67.69.237.138 (VIP) 67.69.237.133 (EVS01) 67.69.237.134 (EVS02) 67.69.237.128 /25	> 1023	Adresse RE du contrôleur CSP-E	161	SNMP	UDP
Adresse RE du contrôleur CSP-E	Tous	Tous	160	SNMP	UDP

Règles de coupe-feu pour le contrôleur CSP-E sur place (du côté réseau étendu vers d'autres destinations)

Source		Destination			
IP	Port	FQDN/ IP	Ports	Application	Protocole
Adresse RE du contrôleur CSP-E	> 1023	Serveur DNS 10.90.13.137 10.90.8.137	53	DNS	UDP
Adresse RE du contrôleur CSP-E	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
Adresse RE du contrôleur CSP-E	16386 - 20385	Contrôleur CSP sur place VIP 10.175.0.38 (VIP) 10.175.0.36 (SBC5) 10.175.0.37 (SBC6)	49152-65535	RTP	UDP
Adresse RE du contrôleur CSP-E	16386 - 20385	Contrôleur CSP sur place VIP 10.175.0.38 (VIP) 10.175.0.36 (SBC5) 10.175.0.37 (SBC6)	49152-65535	RTCP	UDP

Remarques :

- Le protocole SIP n'est pas utilisé avec les protocoles RTP ou TCP pour l'instant, mais cette option est disponible dans les téléphones IP.
- Le serveur de terminaux pour le contrôleur CSP-E sur place n'est pas utilisé (l'accès à distance utilise le protocole SSH).

Règles de coupe-feu pour le routage de basculement à Internet

Les règles suivantes s'appliquent lorsqu'un coupe-feu est placé entre l'équipement IP Bell Connexion totale et Internet

Cisco SPA 5xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-5080 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP4	TCP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	5060-5080 ¹	SIP	TCP
Plage d'adresses IP réservée au client	16384-16482 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ³	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-16482 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-16482	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à 20 séances SIP simultanées par appareil.

²Les ports utilisés dans le CSP (environ 16 000 ports) sont en mesure d'effectuer environ 8 000 appels simultanés par CSP.

Cisco 68xx, 78xx and 88xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-5080 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	5060-5080 ¹	SIP	UDP
Plage d'adresses IP réservée au client	16384-32764 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-32764 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-32764 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-32764	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à 20 séances sip simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

ATA 122 et 8000 de Cisco

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80 443	HTTP HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	5060-5063 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP ⁴	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	5060-5063 ¹	SIP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-16482 ²	RTP	UDP
Plage d'adresses IP réservée au client	16384-16482 ²	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535	Plage d'adresses IP réservée au client	16384-16482 ²	RTCP	UDP

¹Cisco doit donc être en mesure de tenir jusqu'à quatre séances SIP simultanées par appareil.

²Cisco doit être en mesure d'effectuer jusqu'à 24 appels simultanés par appareil.

Aastra 67xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	>1023	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP ²	TCP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	>1023	SIP	TCP
Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes	RTP	UDP
Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	3000 – 2x nombre de lignes	RTCP	UDP

¹Requis par le protocole RTP d'Aastra, conformément à la description fournie dans la DC 1889. Le port UDP utilisé pour les flux RTP est traditionnellement un port pair, et le contrôle RTCP est sur le port suivant. Un appel téléphonique utilise donc une paire de ports pour chaque flux média. Le port RTP est attribué à la première ligne du téléphone, puis il change pour chaque ligne subséquente disponible dans le téléphone pour fournir à chaque ligne un port RTP unique pour sa propre utilisation.

Mediatrix 41xx and C7xx series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	16000 + nombre de ports FXS ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP ²	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	16000+nombre de ports FXS ¹	SIP	UDP
Plage d'adresses IP réservée au client	5004+2x nombre d'appels	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	5004+2x nombre d'appels	RTP	UDP
Plage d'adresses IP réservée au client	5004+2x nombre d'appels	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	5004+2x nombre d'appels	RTCP	UDP

¹Exigé par Media5 pour avoir un port SIP spécifique par port FXS.

²Ceci est requis par Media5 pour atteindre le nombre maximum d'appels simultanés par appareil.

Polycom VVX series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	443	HTTPS	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	5060	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP ³	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	5060	SIP	UDP
Plage d'adresses IP réservée au client	Even port 50000 to 50047 on VVX 310/311 and 410/411 50000 to 50095 on VVX 500/501 and 600/601 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ²	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	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
Plage d'adresses IP réservée au client	Odd port 50001 to 50047 on VVX 310/311 and 410/411 50001 to 50095 on VVX 500/501 and 600/601 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTCP	UDP

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	Port nombre impair 50001 to 50047 on V VX 310/311 and 410/411 50001 to 50095 on V VX 500/501 and 600/601 ¹	RTCP	UDP

¹Ceci est requis par Polycom pour effectuer jusqu'à 24 appels simultanés par appareil. Selon l'explication du fournisseur : le port de départ pour les paquets RTP. Les ports sont attribués à partir d'une réserve en commençant par ce port jusqu'à une valeur de (port initial 50000 + 47) pour V VX310/311/410/411 ou (port initial 50000 + 95) pour V VX500/501/600

Polycom SSIP series

Source		Destination			
Adresse IP du téléphone	Port	IP	Port	Application	Protocole
0.0.0.0	68	255.255.255.255	67	Découverte DHCP	UDP
Plage d'adresses IP réservée au client	68	Serveur DHCP du client	67	DHCP	UDP
Plage d'adresses IP réservée au client	> 1023	Serveur DNS configuré par le client	53	DNS	UDP
Plage d'adresses IP réservée au client	> 1023	hipv-xsp.bell.ca 67.69.241.0/24 67.69.237.0/24	80	HTTP	TCP
Plage d'adresses IP réservée au client	> 1023	TBD	123	NTP	UDP
Plage d'adresses IP réservée au client	5060	Contrôleur CSP internet VIP IP: 67.69.255.72	5060	SIP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	5060	Plage d'adresses IP réservée au client	5060	SIP	UDP
Plage d'adresses IP réservée au client	2222-2268 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	2222-2268 ¹	RTP	UDP
Plage d'adresses IP réservée au client	2222-2268 ¹	Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	RTCP	UDP
Contrôleur CSP internet VIP IP: 67.69.255.72	49152-65535 ¹	Plage d'adresses IP réservée au client	2222-2268 ¹	RTCP	UDP

¹Ceci est requis par Polycom pour effectuer jusqu'à 24 appels simultanés par appareil. Explication du fournisseur Polycom : la valeur 2222 sera utilisée pour le premier port RTP attribué. Les ports ultérieurs seront attribués à partir d'une réserve en commençant par le port indiqué plus deux jusqu'à une valeur de (port initial + 46), après quoi le numéro de port reviendra à la valeur de départ.

Annexe : Processus de connexion pour les applications et l'équipement

Cette section décrit les différentes étapes des processus mis en œuvre lorsque les applications et l'équipement Bell Connexion totale se connectent au réseau et interagissent avec lui.

Processus de connexion de l'application de bureau Bell Connexion totale

1. Lorsqu'elle démarre, l'application de bureau se connecte à <https://hipv-xsp2.bell.ca/> (67.69.241.0/24, 67.69.237.0/24).
2. L'application de bureau authentifiera l'utilisateur et se servira du protocole HTTPS pour télécharger le fichier de configuration de l'utilisateur à partir de dms.totalconnect.bell.ca, contenant les données d'authentification pour tous les autres services ci-dessous.
3. L'application de bureau se connectera ensuite à :
 - https://totalconnect.bell.ca (67.69.237.0/24, 67.69.241.0/24) pour charger la bannière des emplacements d'urgence 9-1-1
 - xmpp.totalconnect.bell.ca (67.69.237.0/24, 67.69.241.0/24, après la découverte du service xmpp), pour se connecter au serveur de messagerie instantanée et de gestion de présence
 - mtl-sbc.totalconnect.bell.ca (67.69.255.68, après la découverte du registraire SIP), pour s'enregistrer comme point d'extrémité SIP
 - Si le site mtl-sbc.totalconnect.bell.ca ne répond pas, l'application de bureau tente de se connecter à l'adresse tor-sbc.totalconnect.bell.ca (67.69.186.20)

Processus de connexion de l'application Réceptionniste de Bell Connexion totale

1. Lorsque l'application Web Réceptionniste démarre pour la première fois, elle se connecte au portail Bell Connexion totale pour télécharger les bibliothèques Java nécessaires à son exécution. Lors de chaque exécution subséquente, l'application vérifiera si des bibliothèques mises à jour existent et les téléchargera, le cas échéant.
2. Par la suite, l'application Réceptionniste et le réseau fédérateur Bell Connexion totale échangeront les données d'appel au moyen de messages de contrôle et du protocole HTTPS.

Remarque : L'application Réceptionniste et le réseau fédérateur Bell Connexion totale échangeront aussi des messages de maintien de la connexion et NTP (protocole de synchronisation réseau).

Processus de connexion des téléphones Bell Connexion totale

Les fichiers spécifiques échangés et la séquence précise de démarrage varient légèrement d'un fournisseur de téléphones à l'autre. La séquence ci-dessous est un exemple typique avec des téléphones Cisco.

1. Téléphone lors de la mise en marche initiale ou après réinitialisation des réglages par défaut (le téléphone n'accède pas au contrôleur CSP-E sur place au redémarrage).
2. Le téléphone utilise le protocole LLDP (Link Layer Discovery Protocol) pour découvrir s'il y a un RLV voix.
3. Le téléphone exécute la découverte DHCP du RLV voix (ou RLV natif).
4. Le contrôleur CSP-E sur place fournit :
 - Une adresse IP au téléphone
 - L'information sur le serveur DNS
 - Lui-même comme serveur FTP et passerelle par défaut
5. Le téléphone demande le fichier de configuration par défaut au contrôleur CSP-E sur place.
6. Le téléphone traduit l'adresse du serveur de gestion d'équipement Bell Connexion totale à l'aide de l'adresse de serveur DNS fournie par le contrôleur CSP-E sur place.
7. Si nécessaire, le téléphone met à jour son microprogramme à partir du serveur de gestion d'équipement Bell Connexion totale
8. Le téléphone obtient un deuxième fichier de configuration pour son modèle du serveur de gestion d'équipement Bell Connexion totale.

9. Le téléphone invite le technicien à entrer le nom d'utilisateur et le mot de passe pour cet utilisateur.
10. Le téléphone récupère les fichiers de configuration propres à l'utilisateur sur le serveur de gestion d'équipement Bell Connexion totale.
11. Le téléphone se réinitialise et est prêt à être utilisé.

Le téléphone récupère périodiquement le fichier de configuration propre à l'utilisateur et met à jour sa configuration au besoin.

Si un utilisateur change la langue d'affichage du téléphone, le téléphone récupère le fichier de langue approprié sur le serveur de gestion d'équipement Bell Connexion totale au besoin.