Cisco Webex Calling et Cisco BroadCloud pour les opérateurs

Considérations relatives au pare-feu, à la sécurité et au réseau

Exigences

Dernière mise à jour le 2 février 2021

Considérations relatives au pare-feu, à la sécurité et au réseau Cisco BroadCloud[MC] Exigences

Notification

BroadSoft BroadCloud a été renommé Cisco BroadCloud. Depuis septembre 2018, le nom Cisco, le logo de l'entreprise, ainsi que le nouveau nom de produit sont affichés sur le logiciel, la documentation et l'emballage. En raison du processus de transition, les deux marques, Broadsoft et Cisco, ainsi que d'anciens noms de produits pourraient être affichés. Ces produits respectent les mêmes normes élevées de qualité qui distinguent BroadSoft et Cisco dans l'industrie.

Mention relative aux droits d'auteur

Marques de commerce

Tous les noms de produits mentionnés dans ce document peuvent être des marques de commerce ou des marques déposées de leurs sociétés respectives et sont reconnus par la présente.

Ce document est imprimé aux États-Unis d'Amérique.

Historique des révisions du document

Publication	Version	Raison de la modification	Date	Auteur
Brouillon	0.1	Document créé.	*9 mars 2017*	BroadCloud Engineering
Brouillon	0.2	Ajout d'adresses DNS/NTP	9 juin 2017	BroadCloud Engineering
1	1.0	Document publié	17 juillet 2017	BroadCloud Engineering
1	1.1	Ajout d'informations au sujet de l'audit de session SIP et de la traduction d'adresses réseau	7 mars 2018	Cisco BroadCloud Engineering
1	1.2	Mise à jour de la Section 4 - AN commercial avec les adresses IP supplémentaires pour CH et DA et les nouvelles adresses IP pour LA et NY pour Hosted, SIPConnect et Apps Mise à jour de la Section 4 - AN FedRAMP avec les adresses IP supplémentaires pour CH et DA pour Hosted, SIPConnect et Apps	24 avril 2018	Cisco BroadCloud Engineering
1	1.3	Document réédité avec une mise à jour mineure à la Section 4 - AN FedRAMP pour Apps	22 juin 2018	Cisco BroadCloud Engineering
1	1.4	Ajout d'adresses SY3 en AU + panasonic.broadcloud.com.au	7 septembre 2018	Cisco BroadCloud Engineering
1	1.5	Renseignements plus détaillés sur NAT/PAT	2 octobre 2018	Cisco BroadCloud Engineering
1	1.6	Section 4 plus enrichie pour AN, EMEA et APAC en incluant l'adresse IP SBC et les détails de port pour la signalisation SIP et multimédia pour le service basé sur le chiffrement Mise à jour de la Section 4 - AN FedRAMP en supprimant les adresses IP obsolètes	8 octobre 2018	Cisco BroadCloud Engineering
1	1.7	Ajout de UC-SaaS pour US/EMEA sous Applications	22 octobre 2018	Cisco BroadCloud Engineering
1	1.8	Plus de détails sur les temporisateurs NAT recommandés	22 novembre 2018	Cisco BroadCloud Engineering
1	1.9	Informations ajoutées au sujet de Webex Calling	20 février 2019	Cisco BroadCloud Engineering

2	2.0	Ajout des renseignements de destination de la carte PIV FedRAMP PIV Modification de l'adresse UCaaS de l'opérateur US afin de remplacer une référence FedRAMP incorrecte	28 février 2019	Cisco BroadCloud Engineering
2	2.1	Ajout d'une nouvelle URL de mise en service pour un dispositif Cisco spécifique pour un opérateur BroadCloud	7 mars 2019	Cisco BroadCloud Engineering
2	2.2	Modification d'adresses IP de **Trafic de contrôleur SBC** en sous-réseau IP pour l'opérateur BroadCloud Modification d'adresses IP de **Trafic de contrôleur SBC** en sous-réseau IP pour FedRAMP	20 mars 2019	Cisco BroadCloud Engineering
2	2.3	Étoffement des offres de produits en AN avec l'ajout d'un sous-réseau pour Chicago et Dallas	17 juillet 2019	Cisco BroadCloud Engineering
2	2.4	Ajout de la région du Japon à Webex Calling	30 juillet 2019	Cisco BroadCloud Engineering
2	2.5	Déplacement du Cisco SPA122 de spa.sipflash.com à cisco.sipflash.com pour les mises en service américaines	16 septembre 2019	Cisco BroadCloud Engineering
2	2.6	Retrait de l'énoncé erroné au sujet de l'assistance NTP personnalisée	17 octobre 2019	Cisco BroadCloud Engineering
2	2.7	Ajout de la région du Canada plus de nouveaux sous-réseaux pour Dallas et Chicago	20 avril 2020	Cisco BroadCloud Engineering
2	2.8	Ajout de Gigaset/Panasonic/Obihai/Mediatrix à la région EU, ajout de Obihai/Mediatrix/Patton/Vtech à la région US, ajout de Gigaset/Obihai/Mediatrix à la région AU	19 mai 2020	Cisco BroadCloud Engineering
2	2.9	Ajout de DNS pour le Canada et d'URL DMS et d'acodes spécifiques à des URL	20 mai 2020	Cisco BroadCloud Engineering
2	2.10	Ajout d'adresses IP/ports de partage du bureau du client invité pour CA	1 septembre 2020	Cisco BroadCloud Engineering
3	3.0	Mise à jour des IP DMZ utilisées par FED, vers FED DMZ	20 janvier 2021	Cisco BroadCloud Engineering
3	3.1	Ajout de nouvelles plages publiques WxC	2 février 2021	Cisco BroadCloud Engineering

Table des matières

Historique des révisions du document 3
1 Introduction 8
2 Meilleures pratiques en matière de pare-feu et de sécurité 9
3 Meilleures pratiques de déploiement client 10
Meilleures pratiques en matière de stratégie de mot de passe 10
Exigences en matière d'accès au déploiement 10
Déploiements de liaisons par protocole d’ouverture de session 10
Pare-feu 11
Accès à distance 11
Stratégies de mot de passe pour l’équipement des locaux d'abonné 11
SIP ALG 12
Audit de session SIP 12
NAT/PAT 12
DHCP, DNS et NTP 13
NTP 13
4 Exigences en matière d’adresse IP et de ports 14
IMPORTANT 14
Amérique du Nord - AN - Opérateur Cisco BroadCloud 15
Téléphones IP, ATA et équipements d'accès intégré 15
Enregistrement des jonctions SIP, des IP-PBX et des passerelles 17
Applications 18
Service DNS/NTP Cisco BroadCloud 20
PacketSmart 20
Amérique du Nord - AN - Webex Calling 21
Téléphones IP, ATA et équipements d'accès intégré 21
Enregistrement des passerelles 22
Applications 23
Amérique du Nord - AN - Programme fédéral FedRAMP Cisco BroadCloud 24
Téléphones IP, ATA et équipements d'accès intégré 24
Enregistrement des jonctions SIP, des IP-PBX et des passerelles 24
Applications 25
Service DNS/NTP Cisco BroadCloud 25
Canada - CA - Opérateur Cisco BroadCloud 27
Téléphones IP, ATA et équipements d'accès intégré 27
Enregistrement des jonctions SIP, des IP-PBX et des passerelles 28
Applications 28

Service DNS/NTP Cisco BroadCloud 29
Canada - CA - Webex Calling 31
Téléphones IP, ATA et équipements d'accès intégré 31
Enregistrement des passerelles 31
Applications 31
Europe - EMEA - Opérateur Cisco BroadCloud 33
Téléphones IP, ATA et équipements d'accès intégré 33
Enregistrement des jonctions SIP, des IP-PBX et des passerelles 34
Applications 35
Service DNS/NTP Cisco BroadCloud 36
PacketSmart 36
Europe - EMEA - Webex Calling 38
Téléphones IP, ATA et équipements d'accès intégré 38
Enregistrement des passerelles 38
Applications 39
Australie - AU - Opérateur Cisco BroadCloud 40
Téléphones IP, ATA et équipements d'accès intégré 40
Enregistrement des jonctions SIP, des IP-PBX et des passerelles 41
Applications 42
Service DNS/NTP Cisco BroadCloud 43
PacketSmart 43
Australie - AU - Webex Calling 45
Téléphones IP, ATA et équipements d'accès intégré 45
Enregistrement des passerelles 45
Applications 46
Japon - JP - Webex Calling 47
Téléphones IP, ATA et équipements d'accès intégré 47
Enregistrement des passerelles 47
Applications 48
Global 49
Accès au portail Web 49
Examinet - Accès Packetsmart 49
Bêta - Webex Calling 51
Téléphones IP, ATA et équipements d'accès intégré 51
Enregistrement des passerelles 51
Applications 52
Annexe A - Fraude 53
La prévention des fraudes 53

La détection des fraudes 53
Les autocommutateurs IP, les passerelles multimédias et la fraude 53
Les actions du partenaire en cas de fraude détectée 53

1 Introduction

Ce document donne un aperçu des protocoles requis pour exécuter le service sur la plateforme, y compris les ports utilisés.

Il incombe à notre partenaire de s'assurer que l'équipement des locaux de leurs abonnés est configuré de manière sécurisée conformément aux meilleures pratiques de l'industrie.

L'identification des protocoles et des ports à utiliser représente la première étape de la conception d'une stratégie de sécurité qui fait usage de pare-feu et/ou de listes de contrôle d'accès (LCA) afin de limiter l'accès aux services requis uniquement.

Dans le cadre de la réussite du déploiement et de l'exploitation de l'équipement des locaux d'abonnés, tous les périphériques, les fonctionnalités, les portails et les applications requis situés dans la *Section 4, Exigences relatives aux ports,* doivent répondre aux exigences LAN/WAN correspondantes pour le service mis en œuvre et testé avant que les appels des clients ne soient mis en ligne.

2 Meilleures pratiques en matière de pare-feu et de sécurité

Un pare-feu correctement configuré est ***essentiel pour tous*** les déploiements des clients.

Ce ne sont pas toutes les configurations de pare-feu qui nécessitent l'ouverture de ports. Si le client exécute des règles de l'intérieur vers l'extérieur, les ports doivent alors être ouverts pour autoriser les protocoles requis pour la sortie de service.

Il ne devrait y avoir aucune raison pour que le client ouvre des ports entrants sur le pare-feu lorsque la traduction d'adresses IP est utilisée, si des périodes de liaison raisonnables sont définies et qu'aucune manipulation SIP (« SIP Aware ») n'est effectuée sur le dispositif de traduction d'adresses IP.

3 Meilleures pratiques de déploiement client

Meilleures pratiques en matière de stratégie de mot de passe

L'équipement des locaux d'abonnés qui est configuré manuellement, y compris, sans toutefois s'y limiter, les routeurs et les pares-feux, doit toujours être configuré avec des mots de passe conformes aux meilleures pratiques de l'industrie en matière de stratégies de mot de passe.

Les mots de passe devraient :

- Être longs
  - Comporter un minimum de 8 caractères
- Être complexes
  - Comprenant :
    - Des lettres majuscules et minuscules
    - Des chiffres
    - Des symboles que l'équipement des locaux d'abonné peut prendre en charge
- Ne comprendre aucun mot du dictionnaire
  - Ne pas comprendre le nom du client
- Ne pas comprendre le numéro de téléphone du client
- Être crypté et conservé dans un endroit sûr
  - Être accessible uniquement par le personnel autorisé
  - Être changé régulièrement
- Ne pas être partagé par courriel

Exigences en matière d'accès au déploiement

La section *Exigences en matière de ports* de ce document définit les ports et les protocoles requis pour le bon fonctionnement du service selon les différents déploiements disponibles pour les clients.

Si le déploiement de votre client est un déploiement *« mixte »* englobant à la fois des points de terminaison IP et des points de terminaison avec liaison par protocole d'ouverture de session, il pourrait être nécessaire de tenir compte de plus d'une section.

Sélectionnez la section qui s'applique à la région de déploiement de votre client.

Si votre client exploite un réseau d'entreprise avec des règles strictes concernant l'accès à Internet pour ses employés et utilise une liste de contrôle d'accès (LCA) pour les sites Web, veuillez vous référer à la section Portails.

Déploiements de liaisons par protocole d'ouverture de session

Les déploiements de liaisons par protocole d'ouverture de session peuvent nécessiter la configuration manuelle de l'équipement des locaux de l'abonné et inclure des exigences ou exiger un accès à distance pour la maintenance et l'assistance. Il faut tenir compte de considérations supplémentaires.

Ceci est extrêmement important pour tout autocommutateur IP et pour toute passerelle multimédia accessible sur Internet par l'intermédiaire d'une adresse IP. D'autres protocoles, comme Telnet et FTP/TFTP, sont couramment utilisés pour les mises à niveau et les sauvegardes de configuration. Il faut donc également les prendre en compte.

Veuillez vous assurer que toutes les recommandations et meilleures pratiques du fabricant pour la sécurisation de l'équipement des locaux d'abonné sont mises en œuvre.

Pare-feu

Lors de l'utilisation d'un accès Internet standard pour se connecter à Cisco BroadCloud, tous les autocommutateurs IP et toutes les passerelles multimédias doivent être derrière un pare-feu correctement configuré pour empêcher l'accès à l'équipement des locaux d'abonné à partir de sources inconnues.

Accès à distance

Si l'accès à distance à l'autocommutateur IP ou à la passerelle multimédia est requis pour l'assistance et la maintenance, veuillez vous reporter aux recommandations relatives aux meilleures pratiques en matière de sécurité du fabricant.
Si le fabricant ne le recommande pas déjà comme meilleure pratique, vous pouvez envisager de configurer l'accès VPN pour autoriser l'accès à l'équipement des locaux d'abonné uniquement à partir de vos adresses IP autorisées.

Stratégies de mot de passe pour l'équipement des locaux d'abonné

Lors de l'installation de l'équipement des locaux d'abonné, modifiez **IMMÉDIATEMENT tout mot de passe d'accès par défaut du fabricant.**
Cela peut inclure l'accès administrateur et s'étendre à tout accès à l'équipement des locaux d'abonné par l'utilisateur final autorisé.

Veuillez vous reporter à la documentation du fabricant pour vous assurer que TOUS les mots de passe d'accès sont mis à jour.

Tous les mots de passe configurés manuellement sur l'équipement des locaux d'abonné doivent être conformes aux standards de l'industrie relatifs aux mots de passe. Ces standards sont décrits dans la *Section 3.1, Meilleures pratiques en matière de stratégie de mot de passe.*

De plus, veuillez vous assurer que :

- Les mots de passe d'accès de chaque appareil de votre client sont uniques et réservés au seul déploiement de ce client
- Les mots de passe sont conservés dans des fichiers et des emplacements chiffrés
    - Les mots de passe ne doivent pas :
        - Être conservés dans les fichiers non protégés par mot de passe
        - Être conservés dans les téléphones intelligents
- Les mots de passe ne sont accessibles que par du personnel autorisé et ayant reçu une formation complète
    - Les mots de passe ne doivent pas être partagés ouvertement avec :
        - Les utilisateurs finaux
        - Les entrepreneurs
        - Le personnel n'ayant reçu aucune formation
- Tous les mots de passe utilisés par votre client doivent être modifiés :
    - À intervalles réguliers
    - Lorsqu'il y a du mouvement de personnel

SIP ALG

Si un routeur ou un pare-feu est « SIP Aware », c'est-à-dire que SIP ALG ou une passerelle semblable est activée, nous vous recommandons de DÉSACTIVER cette fonctionnalité pour assurer un bon fonctionnement du service.

Pour plus d'informations au sujet de la désactivation de SIP ALG sur des appareils spécifiques, reportez-vous à la documentation pertinente du fabricant.

Audit de session SIP

Pour vous protéger contre les fraudes potentielles lors d'appels plus longs, la plateforme effectue un audit de session toutes les 15 minutes. L'audit de session fournira un message SIP de MISE À JOUR ou de RÉINVITATION selon ce que l'appareil peut prendre en charge et une réponse 200 OK est attendue. Si 200 OK n'est pas reçu, la MISE À JOUR ou la RÉINVITATION sera relancée et si aucune réponse n'est reçue, l'appel sera considéré comme non valide et sera aimablement interrompu.

NAT/PAT

Pour certaines conceptions de réseau d'entreprise et de fournisseur de services, il est courant de masquer l'intégralité de l'espace d'adresse IP d'un client, généralement composé d'adresses IP privées (rfc 1918), derrière une seule adresse IP (ou dans certains cas un petit groupe d'adresses IP) dans un autre espace d'adresse IP généralement public. La fonction PAT est déployée sur le routeur/pare-feu de l'équipement des locaux d'abonné ou au sein du réseau du fournisseur de services qui traduit plusieurs adresses IP source d'un client en une seule adresse IP mappée. Elle exécute ceci en convertissant l'adresse IP source du client et le port TCP/UDP source en adresse IP source « externe » mappée et en port TCP/UDP à source unique.

En général, chaque connexion client TCP ou UDP nécessite une traduction PAT distincte pour être configurée dans le routeur/pare-feu, car le port source de la connexion client diffère pour chaque connexion sortante. Une telle traduction PAT ou entrée dynamique reste dans le tableau NAT/PAT du routeur/pare-feu tant que le trafic circule entre l'application client et la destination du serveur. Une fois la communication client/serveur arrêtée, les traductions dynamiques ont un délai d'expiration après lequel elles sont purgées du tableau de traduction.

Le routeur/pare-feu du client doit autoriser un temporisateur de liaison NAT (Network Address Translation « Traduction d'adresse réseau ») configurable; la valeur du temporisateur dépend de la configuration réseau spécifique.

Cisco BroadCloud recommande que le délai NAT minimal pour UDP soit défini sur 300 secondes. Généralement, le délai des temporisateurs TCP standard est beaucoup plus élevé et donc suffisant. Cependant, dans les cas où cela peut poser un problème, il est recommandé de définir également cette valeur sur 300 secondes ou plus. Veuillez noter que nous ne recommandons pas de réduire le délai par défaut des temporisateurs pour les aligner sur ces valeurs, car cela peut avoir un impact négatif sur d'autres applications.

Impacts opérationnels de la source PAT IP/NAT dynamique :

- La fonction NAT dynamique ajoute des frais supplémentaires d'exploitation et d'administration réseau (avec les dispositifs de routage, c.-à-d. les routeurs, les pares-feux,

etc.), car elle introduit un tableau d'état de traduction de connexion dans les éléments de routage/pare-feu du réseau :
    - Les nouvelles connexions PAT peuvent être rejetées si la réserve de ports IP extérieurs est épuisée
    - L'état de fonctionnement du routeur (mémoire, UC) doit être étroitement surveillé dans les déploiements à volume élevé de trafic du client.
    - La réserve NAT/PAT d'adresses IP doit être augmentée si le nombre de sessions client commence à atteindre le nombre de ports TCP/UDP externes disponibles. En général, la réserve PAT est composée de ports 1024-65535 disponibles par adresse IP externe unique
- Il ne doit jamais y avoir deux opérations PAT IP source ou NAT dynamique effectuées sur le trafic du client au sein d'une seule connexion de bout en bout. En raison de l'existence de temporisateurs NAT/PAT et de l'allocation globale des ports éphémères pendant la traduction, la double source PAT introduira un comportement négatif inattendu dans l'application client.
- L'assurance que la propagation de toutes étiquettes QoS (DSCP) est maintenue dans le paquet IP après la traduction PAT est nécessaire. Dans certaines implantations PAT de routeur/pare-feu, les étiquettes DCSP peuvent être supprimées des paquets IP et donc affecter la qualité du service vocal sur le réseau.

DHCP, DNS et NTP

Lors du déploiement de périphériques, en particulier de téléphones IP sur un site, il est prévu que le protocole DHCP soit fourni localement, ce qui définira également les serveurs DNS et possiblement NTP pour le réseau local.

NTP

Cisco BroadCloud définira les sources NTP dans le cadre de la configuration standard du téléphone IP.

Les téléphones IP ne pourront pas terminer leur cycle d'actualisation de configuration initiale ou en cours sans qu'une ressource NTP précise ne soit définie.

4 Exigences en matière d’adresse IP et de ports

Cette section identifie l'adresse IP et les ports TCP/UDP nécessaires au bon fonctionnement du service. Les sections suivantes sont divisées en différents produits, éléments réseau et protocoles requis. Veuillez vous référer à la région qui s’applique à votre déploiement client.

IMPORTANT

Ce qui suit ne s'applique pas aux déploiements **SIP Entreprise/RTCP opérateur**, car ils peuvent faire l'objet de modifications et sont personnalisés. Les informations requises seront fournies pendant le processus de configuration.

Si vous choisissez de limiter la connectivité au-delà des instructions données, cela peut avoir un impact sur le fonctionnement futur du service et nécessiter une correction de la configuration du pare-feu.

Amérique du Nord - AN - Opérateur Cisco BroadCloud

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Téléphone IP / ATA / équipement d'accès intégré	**NTP** Synchronisation de l'horloge du terminal	ntp.broadcloudpbx.net	199.59.65.181 199.59.66.181	UDP 123
Téléphone IP / ATA / équipement d'accès intégré	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement		UDP/TCP 53
Trafic du contrôleur SBC **Terminaux IP**	**SIP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux IP**	**RTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.59.71.0/25 199.59.70.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux IP**	**SIP/TLS**	Dallas	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24	TCP 8934

		Chicago New York Los Angeles	128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	
Trafic du contrôleur SBC **Terminaux IP**	**SRTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 à 65535
Téléphones IP SPA Cisco et SPA8000, SPA2102 ATA	**HTTPS**	spa.sipflash.com	128.177.36.192 128.177.14.192	TCP 443
Téléphones 3PCC Cisco avec microprogramme MPP, Cisco SPA122, 191 et 192 ATA, DECT Cisco	**HTTPS**	cisco.sipflash.com	199.59.65.228 199.59.66.228	TCP 443
Téléphone IP Polycom	**HTTP/HTTPS**	plcm.sipflash.com	128.177.36.191 128.177.14.191	TCP 80 443
Téléphone IP Snom	**HTTPS**	snom.sipflash.com	128.177.36.193 128.177.14.193	TCP 443
Téléphone IP Yealink	**HTTPS**	yealink.sipflash.com	128.177.36.213 128.177.14.213	TCP 443
Téléphone IP Audiocodes	**HTTPS**	acodes.sipflash.com	128.177.36.189 128.177.14.194	TCP 443
Téléphone IP Aastra/Mitel	**HTTPS**	aastra.sipflash.com	128.177.36.190 128.177.14.195	TCP 443
Panasonic Téléphone IP	**HTTPS**	panasonic.sipflash.com	128.177.36.218 128.177.14.218	TCP 443

Téléphone IP Gigaset	**HTTPS**	mediatrix.sipflash.com	199.59.65.173 199.59.66.173	TCP 443
Téléphone IP Obihai	**HTTPS**	obihai.sipflash.com	199.59.65.241 199.59.66.241	TCP 443
Téléphone IP Patton	**HTTPS**	patton.sipflash.com	199.59.65.240 199.59.66.240	TCP 443
Téléphone IP vtech	**HTTPS**	vtech.sipflash.com	199.59.65.171 199.59.66.171	TCP 443

Enregistrement des jonctions SIP, des IP-PBX et des passerelles

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminal SIP-T	**NTP** Synchronisation de l'horloge du terminal	Fourni localement	Fourni localement	UDP 123
Terminal SIP-T	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 8933
Trafic du contrôleur SBC **Terminal SIP-T**	**RTP**	Dallas Chicago New York	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25	UDP 19560 à 65535

		Los Angeles	199.59.70.0/25	
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP/TLS**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	TCP 8934
Trafic du contrôleur SBC **Terminal SIP-T**	**SRTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 à 65535

Applications

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminaux de CU **(Clients)**	**HTTP/HTTPS** **CAP** **XMPP** Applications Cisco BroadCloud, IM&P, transfert de fichiers et partage du bureau	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 80 443 1081 2208 8443 5222 5280 à 5281 52644 à 52645
Trafic du contrôleur SBC **Terminaux de CU**	**SIP**	Dallas Chicago	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25	UDP/TCP 8933

			135.84.172.0/25 199.19.199.0/24	
		New York	199.59.71.0/25	
		Los Angeles	199.59.70.0/25	
Trafic du contrôleur SBC **Terminaux de CU**	**RTP**	Dallas	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24	UDP 19560 à 65535
		Chicago	128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24	
		New York	199.59.71.0/25	
		Los Angeles	199.59.70.0/25	
Trafic du contrôleur SBC **Terminaux de CU**	**SIP/TLS**	Dallas	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24	TCP 8934
		Chicago	128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24	
		New York	199.59.71.0/25	
		Los Angeles	199.59.70.0/25	
Trafic du contrôleur SBC **Terminaux de CU**	**SRTP**	Dallas	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24	UDP 19560 à 65535
		Chicago	128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24	
		New York	199.59.71.0/25	
		Los Angeles	199.59.70.0/25	
UC-One SaaS	**XSI/CTI**	Instance cliente	35.239.73.31 35.224.174.163	TCP 8012

WebRTC (Client invité)	**HTTPS** Partage du bureau	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 8443
WebRTC (Client invité)	**XMPP/TLS** IM&P	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 5222
WebRTC (Client invité)	**SIP**	wrs.broadcloudpbx.net wrs02.broadcloudpbx.net	128.177.36.131 128.177.14.132 199.59.65.207 128.177.14.207	TCP 8060 8070
WebRTC (Client invité)	**RTP**	wrs.broadcloudpbx.net wrs02.broadcloudpbx.net	128.177.36.131 128.177.14.132 199.59.65.207 128.177.14.207	UDP 16000 à 19000

Service DNS/NTP Cisco BroadCloud

Dispositif	Protocole	Destination/DNS	IP	Port de destination
NTP	**NTP** Utilisation facultative du service NTP public fourni par Cisco BroadCloud	ntp.broadcloudpbx.net	199.59.65.181 199.59.66.181	UDP 123
DNS	**DNS** Utilisation facultative du service DNS fourni par Cisco BroadCloud pour les clients VPN	Aucun DNS	199.59.65.181 199.59.66.181	UDP/TCP 53

PacketSmart

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Serveur PacketSmart	**HTTP/HTTPS** Mises à niveau du micrologiciel	load.packetsmart.broadsoft.com	128.177.36.233 199.19.195.250	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail/rapports de données	packetsmartbeta.broadsoft.com	128.177.36.230	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS**	packetsmartusa.broadsoft.com	128.177.36.226	TCP 80

	Rapports de données			443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail	packetsmart.broadsoft.com	128.177.36.231	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail/rapports de données	packetsmartapac.broadsoft.com	128.177.36.229	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail/rapports de données	packetsmartsa.broadsoft.com	128.177.36.228	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail de rapports	packetsmartreports.broadsoft.com	128.177.36.232	TCP 80 443
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**SIP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	128.177.36.182 128.177.36.183 128.177.36.181 128.177.36.185	TCP/UDP 5060 à 5061
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**RTP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	128.177.36.182 128.177.36.183 128.177.36.181 128.177.36.185	UDP 15000 à 16000
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**TRACEROUTE** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	128.177.36.182 128.177.36.183 128.177.36.181 128.177.36.185	UDP 33434 à 33534

Amérique du Nord - AN - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	199.59.65.181 199.59.66.181	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53

SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25 199.19.197.0/24 199.19.199.0/24 139.177.64.0/24 139.177.65.0/24	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25 199.19.197.0/24 199.19.199.0/24 139.177.64.0/24 139.177.65.0/24	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	199.59.65.228 199.59.66.228	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25 199.19.197.0/24 199.19.199.0/24 139.177.64.0/24 139.177.65.0/24	8934
SRTP Média d'appels	IP du dispositif	8000 à 48000 Peut être réduit par l'administrateur*	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25	19560 à 65535

				135.84.172.0/25 199.19.197.0/24 199.19.199.0/24 139.177.64.0/24 139.177.65.0/24	

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	123	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25 199.19.197.0/24 199.19.199.0/24	8934
SIP† Signalisation de commande d'appel	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 139.177.64.0/24 139.177.65.0/24	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25 199.19.197.0/24 199.19.199.0/24 139.177.64.0/24 139.177.65.0/24	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	128.177.36.138 128.177.14.181	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Amérique du Nord - AN - Programme fédéral FedRAMP Cisco BroadCloud

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Téléphone IP / ATA / équipement d'accès intégré	**NTP** Synchronisation de l'horloge du terminal	ntp.broadcloudgov.us	139.177.94.5 139.177.95.5	UDP 123
Téléphone IP / ATA / équipement d'accès intégré	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement		UDP/TCP 53
Trafic du contrôleur SBC **Terminaux IP**	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934
Trafic du contrôleur SBC **Terminaux IP**	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 à 65535
Téléphone IP Cisco	**HTTPS**	cisco.broadcloudgov.us	139.177.94.10 139.177.95.10	TCP 443
Téléphone IP Polycom	**HTTPS**	polycom.broadcloudgov.us	139.177.94.11 139.177.95.11	TCP 443

Enregistrement des jonctions SIP, des IP-PBX et des passerelles

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminal SIP-T	**NTP** Synchronisation de l'horloge du terminal	Fourni localement	Fourni localement	UDP 123
Terminal SIP-T	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements	Fourni localement	Fourni localement	UDP/TCP 53

	SRV du contrôle d'appel			
Trafic du contrôleur SBC Terminal SIP-T	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934
Trafic du contrôleur SBC Terminal SIP-T	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 à 65535

Applications

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminaux de CU (Clients)	**HTTP/HTTPS** **CAP** **XMPP** Applications Cisco BroadCloud, IM&P, transfert de fichiers et partage du bureau	apps.broadcloudgov.us	139.177.94.9 139.177.95.9	TCP 80 443 1081 2208 8443 5222 5280 à 5281 52644 à 52645
Trafic du contrôleur SBC Terminaux de CU	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934
Trafic du contrôleur SBC Terminaux de CU	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 à 65535
Terminaux de CU (Clients)	**HTTPS** Vérification d'identité personnelle (PIV), authentification par carte	ucone-piv.broadcloudgov.us	139.177.94.9 139.177.95.9	TCP 443

Service DNS/NTP Cisco BroadCloud

Dispositif	Protocole	Destination/DNS	IP	Port de destination
NTP	**NTP** Utilisation facultative du service NTP public fourni par Cisco BroadCloud	ntp.broadcloudgov.us	139.177.94.5 139.177.95.5	UDP 123

DNS	**DNS** Utilisation facultative du service DNS fourni par Cisco BroadCloud pour les clients VPN	Aucun DNS	139.177.94.5 139.177.95.5	UDP/TCP 53

Canada - CA - Opérateur Cisco BroadCloud

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Téléphone IP / ATA / équipement d'accès intégré	**NTP** Synchronisation de l'horloge du terminal	ntp-ca.bcld.webex.com	135.84.173.152 135.84.174.152	UDP 123
Téléphone IP / ATA / équipement d'accès intégré	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement		UDP/TCP 53
Trafic du contrôleur SBC **Terminaux IP**	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux IP**	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux IP**	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
Trafic du contrôleur SBC **Terminaux IP**	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535
Configurations du téléphone	**HTTPS**	dms-ca.bcld.webex.com polycom-ca.bcld.webex.com yealink-ca.bcld.webex.com cisco-ca.bcld.webex.com spa-ca.bcld.webex.com panasonic-ca.bcld.webex.com	135.84.173.155 135.84.174.155	TCP 443 80

Configurations du téléphone	**HTTPS**	acodes-ca.bcld.webex.com	135.84.173.140 135.84.174.140	TCP 443 80

Enregistrement des jonctions SIP, des IP-PBX et des passerelles

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminal SIP-T	**NTP** Synchronisation de l'horloge du terminal	Fourni localement	Fourni localement	UDP 123
Terminal SIP-T	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 8933
Trafic du contrôleur SBC **Terminal SIP-T**	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
Trafic du contrôleur SBC **Terminal SIP-T**	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535

Applications

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminaux de CU **(Clients)**	**HTTP/HTTPS** **CAP** **XMPP** Applications Cisco BroadCloud, IM&P, transfert de fichiers	client-ca.bcld.webex.com	135.84.173.154 135.84.174.154	TCP 80 443 1081 2208

	et partage du bureau			8443 5222 5280 à 5281 52644 à 52645
Trafic du contrôleur SBC **Terminaux de CU**	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux de CU**	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux de CU**	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
Trafic du contrôleur SBC **Terminaux de CU**	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 à 65535
WebRTC **(Client invité)**	**HTTPS** Partage du bureau	apps-ca.bcld.webex.com	135.84.173.154 135.84.174.154	TCP 8443
WebRTC **(Client invité)**	**XMPP/TLS** IM&P	imp-ca.bcld.webex.com	135.84.173.158 135.84.174.158	TCP 5222
WebRTC **(Client invité)**	**SIP**	wrscl01-ca.bcld.webex.com	135.84.173.132 135.84.173.133 135.84.174.132 135.84.174.133	TCP 8060 8070
WebRTC **(Client invité)**	**RTP**	wrscl01-ca.bcld.webex.com	135.84.173.132 135.84.173.133 135.84.174.132 135.84.174.133	UDP 16000 à 19000

Service DNS/NTP Cisco BroadCloud

Dispositif	Protocole	Destination/DNS	IP	Port de destination
NTP	**NTP** Utilisation facultative du service NTP public fourni par Cisco	ntp-ca.bcld.webex.com	135.84.173.152 135.84.174.152	UDP 123

	BroadCloud			
DNS	**DNS** Utilisation facultative du service DNS fourni par Cisco BroadCloud pour les clients VPN	Aucun DNS	135.84.173.152 135.84.174.152	UDP/TCP 53

Canada - CA - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	135.84.173.152 135.84.174.152	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	135.84.173.155 135.84.174.155	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SRTP Média d'appels	IP du dispositif	8000 à 48000 Peut être réduit par l'administrateur*	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 à 65535

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	123	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SIP† Signalisation de commande d'appel	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	135.84.173.154 135.84.174.154	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Europe - EMEA - Opérateur Cisco BroadCloud

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Téléphone IP / ATA / équipement d'accès intégré	**NTP** Synchronisation de l'horloge du terminal	ntp.broadcloud.eu	85.119.57.218 85.119.56.218	UDP 123
Téléphone IP / ATA / équipement d'accès intégré	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement		UDP/TCP 53
Trafic du contrôleur SBC **Terminaux IP**	**SIP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux IP**	**RTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux IP**	**SIP/TLS**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	TCP 8934
Trafic du contrôleur SBC **Terminaux IP**	**SRTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535
Téléphones IP SPA Cisco et SPA122, SPA8000, SPA2102 ATA	**HTTPS**	spa.broadcloud.eu	85.119.57.214 85.119.56.219	TCP 443
Téléphones 3PCC Cisco avec microprogram	**HTTPS**	cisco.broadcloud.eu	85.119.56.198 85.119.57.198	TCP 443

me MPP, Cisco 191 et 192 ATA, DECT Cisco				
Téléphone IP Polycom	**HTTPS**	polycom.broadcloud.eu	85.119.56.200 85.199.57.200	TCP 443
Téléphone IP Snom	**HTTPS**	snom.broadcloud.eu	85.119.56.201 85.119.57.201	TCP 443
Téléphone IP Yealink	**HTTP/HTTPS**	yealink.broadcloud.eu	85.119.56.205 85.119.57.205	TCP 80 443
Téléphone IP Audiocodes	**HTTPS**	acodes.broadcloud.eu	85.119.56.211 85.119.57.211	TCP 443
Téléphone IP Aastra/Mitel	**HTTPS**	aastra.broadcloud.eu	85.119.56.199 85.119.57.199	TCP 443
Téléphone IP Panasonic	**HTTPS**	panasonic.broadcloud.eu	85.119.56.216 85.119.57.216	TCP 443
Téléphone IP Gigaset	**HTTPS**	gigaset.broadcloud.eu	85.119.56.219 85.119.57.219	TCP 443
Téléphone IP Mediatrix	**HTTPS**	mediatrix.broadcloud.eu	85.119.56.220 85.119.57.220	TCP 443
Téléphone IP Obihai	**HTTPS**	obihai.broadcloud.eu	85.119.56.227 85.119.57.	TCP 443

Enregistrement des jonctions SIP, des IP-PBX et des passerelles

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminal SIP-T	**NTP** Synchronisation de l'horloge du terminal	Fourni localement	Fourni localement	UDP 123
Terminal SIP-T	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP**	Francfort	85.119.56.128/26 185.115.197.0/25	UDP 8933

		Londres	85.119.57.128/26 185.115.196.0/25	
Trafic du contrôleur SBC **Terminal SIP-T**	**RTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP/TLS**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	TCP 8934
Trafic du contrôleur SBC **Terminal SIP-T**	**SRTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535

Applications

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminaux de CU **(Clients)**	**HTTP/HTTPS** **CAP** **XMPP** Applications Cisco BroadCloud, IM&P, transfert de fichiers et partage du bureau	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu umscl01-imp.broadcloud.eu	85.119.56.197 85.119.57.197 85.119.56.197 85.119.57.197	TCP 80 443 1081 2208 8443 5222 5280 à 5281 52644 à 52645
Trafic du contrôleur SBC **Terminaux de CU**	**SIP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux de CU**	**RTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux de CU**	**SIP/TLS**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	TCP 8934

Trafic du contrôleur SBC **Terminaux de CU**	**SRTP**	Francfort Londres	85.119.56.128/26 185.115.197.0/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 à 65535
WebRTC (Client invité)	**HTTPS** Partage du bureau	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu	 85.119.56.197 85.119.57.197	TCP 8443
WebRTC (Client invité)	**XMPP/TLS** IM&P	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu	 85.119.56.197 85.119.57.197	TCP 5222
WebRTC (Client invité)	**SIP**	wrs01.broadcloud.eu	85.119.57.231 85.119.56.231	TCP 8060 8070
WebRTC (Client invité)	**RTP**	wrs01.broadcloud.eu	85.119.57.231 85.119.56.231	UDP 16000 à 19000
UC-One SaaS	**XSI/CTI**	Instance cliente	35.198.108.52 35.242.245.59	TCP 8012

Service DNS/NTP Cisco BroadCloud

Dispositif	Protocole	Destination/DNS	IP	Port de destination
NTP	**NTP** Utilisation facultative du service NTP public fourni par Cisco BroadCloud	ntp.broadcloud.eu	85.119.57.218 85.119.56.218	UDP 123
DNS	**DNS** Utilisation facultative du service DNS fourni par Cisco BroadCloud pour les clients VPN	Aucun DNS	85.119.57.218 85.119.56.218	UDP/TCP 53

PacketSmart

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Serveur PacketSmart	**HTTP/HTTPS**	packetsmartuk.broadsoft.com	85.119.57.247	TCP 80 443

	Accès au portail/rapports de données			
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail/rapports de données	packetsmartde.broadsoft.com	85.119.56.247	TCP 80 443
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**SIP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	85.119.57.242 85.119.56.242	TCP/UDP 5060 à 5061
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**RTP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	85.119.57.242 85.119.56.242	UDP 15000 à 16000
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**TRACEROUTE** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	85.119.57.242 85.119.56.242	UDP 33434 à 33534

Europe - EMEA - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	85.119.57.218 85.119.56.218	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24 139.177.67.0/24	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24 139.177.67.0/24	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	85.119.56.198 85.119.57.198	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24	8934

				139.177.67.0/24	
SRTP Média d'appels	IP du dispositif	8000 à 48000 Peut être réduit par l'administrateur*	UDP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24 139.177.67.0/24	19560 à 65535

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	Tout	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25	8934
SIP† Signalisation de commande d'appel	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24 139.177.67.0/24	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	85.119.56.128/26 85.119.57.128/26 185.115.196.0/25 185.115.197.0/25 139.177.66.0/24 139.177.67.0/24	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	85.119.56.197 85.119.57.197	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Australie - AU - Opérateur Cisco BroadCloud

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Téléphone IP / ATA / équipement d'accès intégré	**NTP** Synchronisation de l'horloge du terminal	ntp.broadcloud.com.au	199.59.64.152 199.59.67.152	UDP 123
Téléphone IP / ATA / équipement d'accès intégré	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement		UDP/TCP 53
Trafic du contrôleur SBC **Terminaux IP**	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP/TCP 8933
Trafic du contrôleur SBC **Terminaux IP**	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC **Terminaux IP**	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
Trafic du contrôleur SBC **Terminaux IP**	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535
Téléphones IP SPA Cisco et SPA122, SPA8000, SPA2102 ATA	**HTTPS**	spa.broadcloud.com.au	199.59.64.155 199.59.67.155	TCP 443
Téléphones 3PCC Cisco avec microprogramme MPP, Cisco 191 et 192 ATA, DECT Cisco	**HTTPS**	cisco.broadcloud.com.au	199.59.64.143 199.59.67.143	TCP 443
Téléphone IP Polycom	**HTTPS**	polycom.broadcloud.com.au	199.59.64.144 199.59.67.144	TCP 443

Téléphone IP Snom	**HTTPS**	snom.broadcloud.com.au	199.59.64.148 199.59.67.148	TCP 443
Téléphone IP Yealink	**HTTP/HTTPS**	yealink.broadcloud.com.au	199.59.64.145 199.59.67.145	TCP 80 443
Téléphone IP Audiocodes	**HTTPS**	acodes.broadcloud.com.au	199.59.64.147 199.59.67.147	TCP 443
Téléphone IP Aastra/Mitel	**HTTPS**	aastra.broadcloud.com.au	199.59.64.146 199.59.67.146	TCP 443
Téléphone IP Panasonic	**HTTPS**	panasonic.broadcloud.com.au	199.59.64.151 199.59.67.151	TCP 443
Téléphone IP Gigaset	**HTTPS**	gigaset.broadcloud.com.au	199.59.64.215 199.59.67.215	TCP 443
Téléphone IP Mediatrix	**HTTPS**	mediatrix.broadcloud.com.au	199.59.64.211 199.59.67.211	TCP 443
Téléphone IP Obihai	**HTTPS**	obihai.broadcloud.com.au	199.59.64.216 199.59.67.216	TCP 443

Enregistrement des jonctions SIP, des IP-PBX et des passerelles

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminal SIP-T	**NTP** Synchronisation de l'horloge du terminal	Fourni localement	Fourni localement	UDP 123
Terminal SIP-T	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53
Trafic du contrôleur SBC **Terminal SIP-T**	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 8933
Trafic du contrôleur SBC **Terminal SIP-T**	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535

Trafic du contrôleur SBC Terminal SIP-T	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
Trafic du contrôleur SBC Terminal SIP-T	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535

Applications

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Terminaux de CU (Clients)	**HTTP/HTTPS** **CAP** **XMPP** Applications Cisco BroadCloud, IM&P, transfert de fichiers et partage du bureau	apps.broadcloud.com.au apps1.broadcloud.com.au apps2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 80 443 1081 2208 8443 5222 5280 à 5281 52644 à 52645
Trafic du contrôleur SBC Terminaux de CU	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP/TCP 8933
Trafic du contrôleur SBC Terminaux de CU	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535
Trafic du contrôleur SBC Terminaux de CU	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
Trafic du contrôleur SBC Terminaux de CU	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 à 65535
WebRTC (Client invité)	**HTTPS** Partage du bureau	apps.broadcloud.com.au apps1.broadcloud.com.au app2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 8443
WebRTC (Client invité)	**XMPP/TLS** IM&P	apps.broadcloud.com.au apps1.broadcloud.com.au app2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 5222
WebRTC (Client invité)	**SIP**	wrs01.broadcloud.com.au	199.59.64.191 199.59.67.191	TCP 8060 8070
WebRTC (Client invité)	**RTP**	wrs01.broadcloud.com.au	199.59.64.191 199.59.67.191	UDP 16000 à 19000

Service DNS/NTP Cisco BroadCloud

Dispositif	Protocole	Destination/DNS	IP	Port de destination
NTP	**NTP** Utilisation facultative du service NTP public fourni par Cisco BroadCloud	ntp.broadcloud.com.au	199.59.64.152 199.59.67.152	UDP 123
DNS	**DNS** Utilisation facultative du service DNS fourni par Cisco BroadCloud pour les clients VPN	Aucun DNS	199.59.64.152 199.59.67.152	UDP/TCP 53

PacketSmart

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Serveur PacketSmart	**HTTP/HTTPS** Rapports de données	packetsmartdsau.broadsoft.com	199.59.67.226	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail	packetsmartau.broadsoft.com	199.59.67.227	TCP 80 443
Serveur PacketSmart	**HTTP/HTTPS** Accès au portail de rapports	packetsmartreportsau.broadsoft.com	199.59.67.228	TCP 80 443
Serveur PacketSmart MediaSink (Cible de l'appel d'évaluation)	**SIP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	199.59.67.231 199.59.67.232	TCP/UDP 5060 à 5061
Serveur PacketSmart MediaSink (évaluations)	**RTP** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	199.59.67.231 199.59.67.232	UDP 15000 à 16000
Serveur PacketSmart MediaSink (évaluations)	**TRACEROUTE** Utilisation limitée : S'applique à l'inspection de site avec l'évaluation PacketSmart	Aucun DNS	199.59.67.231 199.59.67.232	UDP 33434 à 33534

Australie - AU - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	199.59.64.152 199.59.67.152	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	199.59.64.143 199.59.67.143	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	8934
SRTP Média d'appels	IP du dispositif	8000 à 48000 Peut être réduit par l'administrateur*	UDP	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	19560 à 65535

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	Tout	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	199.59.64.0/25 199.59.67.0/25	8934
SIP† Signalisation de commande d'appel	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	199.59.64.0/25 199.59.67.0/25 139.177.70.0/24 139.177.71.0/24	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	199.59.64.140 199.59.67.140	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Japon - JP - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	135.84.169.154 135.84.170.154	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	135.84.169.186 135.84.170.186	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	8934
SRTP Média d'appels	IP du dispositif	8000 à 48000 Peut être réduit par l'administrateur*	UDP	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	19560 à 65535

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	Tout	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	135.84.169.0/25 135.84.170.0/25	8934
SIP† Signalisation de commande d'appel	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	135.84.169.0/25 135.84.170.0/25 139.177.68.0/24 139.177.69.0/24	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	135.84.169.185 135.84.170.185	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Global

Accès au portail Web

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Les ordinateurs de tous les utilisateurs (Y compris ExamiNet)	**HTTP/HTTPS** Tableaux de bord du portail du fournisseur de services	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142	TCP 80 443
Ordinateurs ExamiNet	**HTTP** Test de ExamiNet pour valider la disponibilité de la bande passante et les mesures de performances réseau	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au examinet-ca.bcld.webex.com	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142 135.84.173.157	TCP/UDP 1025
Ordinateurs Examinet	**HTTP** Test de ExamiNet pour vérifier si le port est accessible	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142	TCP 8933 à 8943 19560 à 65535
Ordinateurs ExamiNet	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53

Examinet - Accès Packetsmart

Dispositif	Protocole	Destination/DNS	IP	Port de destination
Les ordinateurs de tous les utilisateurs (Y compris ExamiNet)	**HTTP/HTTPS** Tableaux de bord du portail du fournisseur de services	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP 80 443

		examinetpsde.broadcloudpbx.com		
Ordinateurs ExamiNet	**HTTP** Test de ExamiNet pour valider la disponibilité de la bande passante et les mesures de performances réseau	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com examinetpsde.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP/UDP 1025
Ordinateurs Examinet	**HTTP** Test de ExamiNet pour vérifier si le port est accessible	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com examinetpsde.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP 8933 à 8943 19560 à 65535
Ordinateurs ExamiNet	**DNS** Pour la résolution des enregistrements du serveur de configuration A et les enregistrements SRV du contrôle d'appel	Fourni localement	Fourni localement	UDP/TCP 53

Bêta - Webex Calling

Toutes les destinations doivent être configurées sur le pare-feu du client pour assurer la continuité du service.

Téléphones IP, ATA et équipements d'accès intégré

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	51494	UDP	199.59.65.181 199.59.66.181	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	5060 à 5080	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	8934
SRTP Média d'appels	IP du dispositif	19560 à 19660	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	19560 à 65535
Configuration du dispositif et gestion du micrologiciel	IP du dispositif	Tout	TCP	199.59.65.227 199.59.66.227	443 80

Enregistrement des passerelles

Objet	IP Src.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP du dispositif	Tout	UDP	Défini par le client	123
DNS Résolution de noms	IP du dispositif	Tout	UDP/TCP	Défini par le client	53
SIP Signalisation de commande d'appel	IP du dispositif	8000 à 65535	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	8934
SRTP Média d'appels	IP du dispositif	8000 à 48000	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25	19560 à 65535

		Peut être réduit par l'administrateur*		199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	

* Défini en fonction de la définition de la ***plage de ports RTP*** dans la configuration CUBE.

Applications

Objet	IP Srp.	Ports Src.	Protocole	IP Dst.	Ports Dst.
NTP Synchronisation date/heure	IP de l'hôte client	123	UDP	Défini par l'hôte	123
DNS Résolution de noms	IP de l'hôte client	Tout	UDP/TCP	Défini par l'hôte	53
SIP Signalisation de commande d'appel	IP de l'hôte client	Tout	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	8934
SIP† Signalisation de commande d'appel	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	Tout	TCP	IP de l'hôte client	8934
SRTP Média d'appels	IP de l'hôte client	Tout	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25 135.84.171.0/25 135.84.172.0/25	19560 à 65535
Configuration du client	IP de l'hôte client	Tout	TCP	128.177.36.137 128.177.14.182	80 443

† Ce flux est seulement nécessaire lorsqu'il n'y a pas de traduction d'adresses réseau entre le client et Webex Calling, c.-à-d. que l'adresse de l'hôte client est publique.

Annexe A - Fraude

La prévention des fraudes

Protéger tous les aspects de notre service contre la fraude est une priorité essentielle pour BroadSoft. Cette section détaille les mesures de prévention de la fraude.

Tous les équipements locaux des abonnés (CPE) qui nécessitent un fichier de configuration du service sont gérés de manière centralisée contre la fraude. Tous les mots de passe d'authentification SIP sont à la fois complexes et cryptés au sein de la signalisation afin d'éliminer toute possibilité qu'ils ne puissent être interceptés. L'administration du mot de passe est gérée par BroadSoft et n'est pas accessible aux clients finaux dont le portail d'accès Web est également fermé.

Lorsqu'un mot de passe est requis pour un dispositif configuré manuellement, comme un autocommutateur IP ou une passerelle multimédia, le portail de mise en service de la plateforme génère de manière aléatoire un mot de passe complexe qui doit être utilisé dans l'équipement des locaux d'abonné.

La détection des fraudes

BroadSoft exploite un outil complexe de détection des fraudes qui analyse activement les modèles d'appel sur le système afin de détecter toute activité suspecte. Le système peut prendre des mesures proactives pour empêcher la fraude lorsque des modèles d'appel anormaux sont détectés et il peut les bloquer.

Le déploiement de cet outil ne doit pas être traité comme un filet de sécurité permettant le déploiement ou l'utilisation d'un équipement de locaux d'abonné mal protégé.

Les autocommutateurs IP, les passerelles multimédias et la fraude

Comme indiqué dans les sections précédentes, des mesures rigoureuses ont été prises pour protéger le service de base; nous recommandons que le même niveau de rigueur soit appliqué aux terminaux des clients, qu'il s'agisse d'un téléphone IP, d'un autocommutateur IP ou d'une passerelle multimédia. En raison de la nécessité de configurer manuellement et d'autoriser potentiellement l'accès à distance à des fins d'assistance et de maintenance, les autocommutateurs IP et les passerelles multimédias peuvent faire l'objet d'accès non autorisés.

Pour éviter cette situation, nos partenaires devraient suivre les recommandations basées sur les meilleures pratiques qui sont inscrites à la *Section 2* et à la *Section 3* du présent document.

Les actions du partenaire en cas de fraude détectée

Si un accès non autorisé se produit et que nous informons notre partenaire que son client n'a pas été autorisé à faire et à transférer des appels à coût élevé, notre partenaire doit au minimum :

- Vérifier si le réseau du client est sécurisé
  - Le pare-feu ne doit permettre l'accès qu'aux adresses IP, aux ports et aux protocoles requis pour le service dont les renseignements sont inscrits dans la partie pertinente de la Section 4, exigences relatives aux ports
- Retirer le dispositif de l'Internet public, le cas échéant
- Modifier les identifiants d'accès de l'équipement des locaux d'abonné

    - Assurez-vous que les identifiants d'accès respectent les meilleures pratiques relatives aux mots de passe qui sont inscrites dans la *Section 3.1* et la *Section 3.3.3*
- Modifier les renseignements d’authentification SIP