Configuration minimale requise du réseau

carrier.webex.com/fr/minimum-network-requirements/

11 janvier 2019

Accueil | Guides de l'administrateur | Configuration minimale requise du réseau

Ce que vous devez savoir :

La conception et la configuration du réseau du client comportent de nombreuses variables, dont beaucoup peuvent affecter la performance et la qualité du service de la voix sur IP (VOIP). Pour que le service VOIP BroadCloud fonctionne dans la plupart des environnements de réseau du client, il existe un ensemble d'exigences minimales auxquelles le réseau du client doit répondre.

Résumé des exigencesDétail des exigences Serveur DHCPServeur DNSPare-feuTraduction d'adresses de réseauPasserelle de la couche applicationParamètres de la qualité de serviceLargeur de bande InternetEstimation de la largeur de bande nécessaireLargeur de bande du réseau localSpécifications de configuration du pare-feu du clientRetour en haut de la page

Résumé des exigences

La conception et la configuration du réseau du client comportent de nombreuses variables, dont beaucoup peuvent affecter la performance et la qualité du service de la voix sur IP (VOIP). Pour que le service VOIP BroadCloud fonctionne dans la plupart des environnements de réseau client, il y a un ensemble d'exigences minimales que le réseau client doit satisfaire pour assurer que le service fonctionne comme prévu. Ces exigences s'appliquent à la fois aux téléphones SIP et aux adaptateurs analogiques (généralement appelés à partir de ce point comme les périphériques SIP). Vous trouverez ci-dessous un résumé de ces exigences :

- le LAN du client doit contenir un serveur DHCP capable de fournir une adresse IP aux périphériques SIP lors de leur démarrage.
- le réseau local du client doit contenir un serveur DNS ou fournir une fonctionnalité de relais DNS pour permettre la résolution des URL utilisées par les périphériques SIP pour communiquer avec des plateformes de service externes.
- le serveur DNS doit être capable de résoudre les enregistrements SRV et A.
- le pare-feu du client doit autoriser le trafic HTTP (port TCP 80) et HTTPS (port TCP 443) pour que les périphériques SIP puissent communiquer avec les serveurs de configuration externes.
- le pare-feu du client doit autoriser les protocoles SIP et RTP pour permettre aux périphériques SIP de passer et de recevoir des appels.

- le routeur du client doit définir le délai de liaison NAT (Network Address Translation) à une valeur supérieure ou égale à 30 secondes.
- le routeur/pare-feu du client ne doit pas manipuler les paquets SIP ou RTP au niveau de la couche d'application. Si des périphériques CPE peuvent fonctionner comme une passerelle de couche d'accès (ALG) SIP, la fonctionnalité ALG doit être désactivée.
- Le routeur du client doit prendre en charge le DSCP (Differentiated Service Code Point) et veiller à ce que les paquets de priorité supérieure aient la priorité sur les paquets de priorité inférieure pour tous les paquets sortants.
- Le routeur du client doit être configuré pour marquer tous les paquets SIP et RTP provenant des plateformes de contrôle d'appel BroadCloud comme étant de haute priorité afin de s'assurer que ces paquets ont la priorité sur les paquets de priorité inférieure pour tous les paquets entrants. Les plateformes de contrôle d'appel BroadCloud peuvent être identifiées de manière unique par un ensemble d'adresses IP spécifiques. Les paquets SIP et RTP peuvent être identifiés de manière unique par les ports définis dans la section Pare-feu de ce document.
- La bande passante Internet du client doit être calibrée pour permettre la quantité minimale de bande passante de données requise plus le nombre total d'appels vocaux simultanés requis par le bureau.
- Le réseau local (LAN) du client doit être calibré pour permettre la quantité maximale de bande passante de données requise plus le nombre total d'appels vocaux simultanés requis par le bureau.

Détail des exigences Serveur DHCP

Le protocole de configuration dynamique des hôtes (DHCP) est un protocole utilisé par les organisateurs en réseau pour obtenir divers paramètres nécessaires pour que les périphériques fonctionnent dans un réseau IP. Les paramètres DHCP fournis par le serveur DHCP du site qui sont nécessaires pour que le service BroadCloud fonctionne correctement sont l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS.

Les serveurs DHCP sont généralement intégrés dans le routeur du client, mais ils peuvent être un serveur autonome dédié à la seule fonction DHCP. Pour la plupart des applications à large bande, le serveur DHCP sera intégré au routeur à large bande fourni par le fournisseur de services. Dans ce cas, la configuration du serveur DHCP (y compris s'il est activé ou désactivé) peut être contrôlée en se connectant au routeur à large bande.

Tous les périphériques SIP BroadCloud sont configurés par défaut pour obtenir l'adresse IP et les informations du serveur DNS à partir d'un serveur DHCP local. Lorsqu'un périphérique SIP est démarré, il tente de localiser le serveur DHCP local et d'obtenir ces informations. Si le réseau du client ne contient pas de serveur DHCP ou ne fournit pas les informations requises, le périphérique SIP ne démarre pas correctement et devient inutilisable.

Certains serveurs DHCP sont capables de fournir des « options » dans le cadre de leur réponse à la demande d'un client. Pour les applications SIP, l'option 66 est généralement utilisée pour fournir au client, dans ce cas un périphérique SIP, l'adresse du serveur de configuration qu'il doit contacter pour obtenir sa configuration. Dans le cas du service BroadCloud, cette option n'est pas nécessaire. Tous les périphériques SIP BroadCloud sont codés de manière à pointer vers une adresse de serveur de configuration spécifique et si une option 66 est reçue par le périphérique SIP en réponse à une demande DHCP, le périphérique SIP l'ignorera.

Serveur DNS

Le système de noms de domaine (DNS) est un service Internet qui traduit les noms de domaine en adresses IP. Il permet de nommer les périphériques Internet à l'aide de mots plus faciles à retenir que l'adresse IP numérique réelle des périphériques. En outre, certains types d'enregistrements DNS sont capables d'associer un nom de mot unique à une liste d'adresses IP. Cette fonctionnalité est utile dans les cas où la redondance des périphériques est utilisée pour améliorer les performances et/ou la fiabilité.

Tous les périphériques SIP BroadCloud ont besoin du DNS pour traduire les noms de domaine en adresses IP. Pendant le processus de démarrage, le nom de domaine du serveur de configuration du périphérique SIP est traduit afin que le périphérique SIP puisse localiser et recevoir les informations de configuration du serveur de configuration approprié. De même, une fois que le téléphone a terminé le processus de démarrage, le nom de domaine des serveurs de contrôle des appels est traduit afin que le périphérique SIP puisse localiser ces serveurs de contrôle des appels et communiquer avec eux. Si un serveur DNS n'est pas disponible pour assurer la traduction des noms, le périphérique SIP ne pourra pas démarrer correctement et sera inutilisable.

Il existe plusieurs types d'enregistrements DNS. Le service BroadCloud utilise les types d'enregistrement « A » (adresse) et « SRV » (service). Les enregistrements « SRV » sont utilisés pour fournir un mécanisme de redondance pour les plateformes de contrôle des appels. Pour que le service BroadCloud fonctionne correctement, ces deux types d'enregistrement doivent être pris en charge par le réseau du client.

Pare-feu

Un pare-feu est un périphérique ou un ensemble de périphériques dans un réseau de données configuré pour protéger le réseau contre le trafic potentiellement dangereux. L'une des fonctions générales d'un pare-feu est d'autoriser ou de refuser le passage de services de types spécifiques sur l'interface du réseau public. Une application de cette fonctionnalité consiste à restreindre les types de services auxquels les utilisateurs du réseau privé peuvent accéder publiquement ou à restreindre l'accès public au réseau privé afin d'assurer la sécurité du réseau.

Les pare-feu peuvent empêcher les périphériques SIP de communiquer avec les serveurs de configuration, les serveurs de contrôle des appels, les passerelles de réseau et d'autres périphériques SIP. Pour que le service BroadCloud fonctionne correctement, les pare-feu doivent autoriser les services suivants :

HTTP (port 80) - requis pour la communication entre les périphériques SIP locaux et les serveurs de configuration qui contiennent les informations de configuration des périphériques SIP.

HTTPS (port 443) - requis pour la communication entre les périphériques SIP locaux et les serveurs de configuration qui contiennent les informations de configuration des périphériques SIP.

SIP (port 5060) - requis pour la communication entre les périphériques SIP locaux et les périphériques SIP distants, y compris les plateformes de contrôle des appels, les passerelles de réseau et d'autres périphériques SIP.

SIP (ports 8933 à 8943) - requis pour la communication entre les périphériques SIP locaux et les périphériques SIP distants, notamment les plateformes de contrôle des appels, les passerelles de réseau et d'autres périphériques SIP. Remarque : Cette plage de ports n'est pas communément associée au SIP. Dans ce cas, elle est utilisée pour éviter les rencontres avec la fonctionnalité ALG (Application Layer Gateway) qui pourrait endommager la charge utile des paquets SIP. Pour plus d'informations, reportez-vous à la section Passerelle de la couche d'application de ce document.

RTP (ports 19560-65535) - requis pour la communication entre les périphériques SIP locaux et les périphériques SIP distants, y compris les plateformes de contrôle des appels, les passerelles réseau et les autres périphériques SIP. Remarque : Les ports 19560-65535 ne sont pas généralement associés au protocole RTP. Dans ce cas, ils sont utilisés pour éviter les rencontres avec la fonctionnalité ALG (Application Layer Gateway) qui pourrait endommager la charge utile des paquets RTP. Pour plus d'informations, reportez-vous à la section Passerelle de la couche d'application de ce document. Avec ces services autorisés, les périphériques SIP devraient être en mesure de communiquer correctement avec toutes les sources externes nécessaires.

L'outil de préparation du réseau CScan est utilisé pour déterminer si le service BroadCloud fonctionnera correctement sur le réseau testé. Pour que cet outil et le périphérique PacketSmart fonctionnent correctement, le pare-feu doit permettre aux ordinateurs exécutant le test CScan et au périphérique PacketSmart d'accéder, à travers le pare-feu du client, à des terminaux IP spécifiques.

Une liste des ports, des protocoles, des services, des adresses IP de destination et de l'objectif de l'accès source est présentée dans la section 3 de ce document.

Traduction d’adresses de réseau

La traduction d’adresses réseau (NAT) est une fonction courante des routeurs qui permet de traduire plusieurs adresses IP privées sur un réseau local en une seule adresse IP publique sur le réseau étendu. La principale raison pour laquelle la fonctionnalité NAT existe est de conserver les adresses IP publiques. Il n’y a pas assez d’adresses IP dans IPv4 pour permettre à chaque ordinateur connecté à Internet d’avoir une adresse IP publique unique. En outre, la fonctionnalité NAT offre un certain niveau de sécurité aux périphériques dotés d’adresses IP privées, car ces périphériques ne sont pas toujours adressables publiquement.

Bien que nécessaire, la fonctionnalité NAT crée des problèmes pour le trafic VOIP. Un NAT typique traduit uniquement les informations IP du privé au public au niveau de la couche TCP/IP. Il ne traduit cependant aucune information d’adresse IP au niveau de la couche application. Cela signifie que toutes les informations relatives aux adresses IP contenues dans les données utiles de la couche d’application des paquets VOIP ne sont pas traduites. Comme ces adresses sont privées, elles ne sont pas routables dans un domaine public et sont effectivement inaccessibles. Dans le cas du protocole SIP, l’adresse IP et le port que le périphérique SIP souhaite annoncer pour établir une connexion sont contenus dans les données utiles du protocole SDP joint aux messages SIP. Si ces informations ne sont pas traduites, le destinataire distant ne sera pas en mesure de communiquer avec le périphérique SIP. Cela crée généralement un phénomène communément appelé RTP à sens unique (la voie vocale n’est disponible que dans un sens).

Un autre problème lié à la fonctionnalité NAT est que les périphériques privés ne sont pas joignables publiquement à moins qu’une traduction, communément appelée « liaison », ne soit créée entre l’adresse IP privée et l’adresse IP publique. Cette opération est effectuée de manière dynamique chaque fois qu’un périphérique privé tente de communiquer avec un périphérique public. Le fait de demander une communication amène le NAT à créer une liaison temporaire entre l’adresse IP privée qui demande la communication et l’adresse IP publique avec laquelle elle tente de communiquer. La durée de la liaison est contrôlée par une minuterie qui expirera et entraînera la suppression de la liaison s’il y a une période d’inactivité sur la liaison égale à la durée de la minuterie. Pendant que la liaison est active, la communication entre le public et le privé est possible, mais lorsque la liaison devient inactive, le périphérique privé n’est plus accessible publiquement. La durée la plus courante de cette minuterie est comprise entre 30 et 60 secondes. En outre, les liens peuvent souvent être configurés de manière statique dans un NAT. Cette fonctionnalité est souvent appelée réacheminement de port. Lorsque cela est fait, le NAT est configuré avec un lien permanent entre une adresse privée et une adresse publique.

Avec le produit BroadCloud, les défis présentés par la présence d'un NAT sont résolus. Une technique appelée NAT Traversal est utilisée pour surmonter les problèmes créés par la présence d'un NAT. Une partie de la plateforme de contrôle des appels BroadCloud est chargée de maintenir une communication constante avec tous les périphériques SIP. Cette communication constante garantit que le délai de liaison NAT n'expire jamais, rendant ainsi la liaison dynamique permanente. Sans cela, un périphérique SIP situé dans un réseau privé ne serait pas en mesure de recevoir des appels. De plus, la plateforme de contrôle des appels BroadCloud utilise une technique appelée Relais de médias (Media Relay) pour surmonter le problème où le NAT ne manipule pas les informations de la couche application. Cette fonctionnalité permet à la plateforme de contrôle des appels de découvrir l'adresse IP publique et le port du flux RTP dès que le périphérique SIP envoie son premier paquet RTP. La plateforme de contrôle des appels remplit cette fonction aux deux extrémités d'un appel et établit un pont entre les deux segments de l'appel, relayant ainsi efficacement le trafic d'un périphérique à l'autre.

Passerelle de la couche d'application

La passerelle de couche d'application (Application Layer Gateway (ALG)) est une méthode de manipulation des informations d'adresse IP et de port au niveau de la couche d'application. Elle est similaire à la fonctionnalité NAT en ce sens qu'elle traduit généralement les informations privées d'adresse IP et de port créées par un périphérique SIP sur un réseau privé en informations publiques d'adresse IP et de port sur le côté WAN du routeur qui exécute la fonction ALG. Si elle est correctement réalisée, cette fonctionnalité rend inutile la fonctionnalité de relais de médias, car toutes les informations annoncées dans la couche d'application peuvent être acheminées publiquement.

Bien que cette fonctionnalité soit destinée à améliorer le traitement du trafic VOIP, tous les périphériques ALG ne réalisent pas correctement la traduction des paquets de la couche d'application. Dans de nombreux cas, des parties du paquet sont modifiées alors qu'elles ne devraient pas l'être, ce qui entraîne des problèmes d'interfonctionnement entre le périphérique SIP et la plateforme de contrôle des appels. Lorsque cela se produit, l'ALG empêche le périphérique SIP de fonctionner correctement.

Avec le produit BroadCloud, il est recommandé de désactiver toute la fonctionnalité ALG entre le périphérique SIP et la plateforme de contrôle des appels. Ainsi, l'ALG ne risque pas de traduire incorrectement les paquets, ce qui pourrait rendre le service inutilisable. Cependant, dans certains cas, cette fonctionnalité peut ne pas être configurable. Pour s'adapter à ce cas, le produit BroadCloud utilise des ports peu communs pour le trafic SIP et RTP. Les ports 8933 à 8943 sont utilisés au lieu de 5060 qui est le port communément utilisé pour SIP. Étant donné que la plupart des ALG supposent un port SIP de 5060, l'utilisation des ports 8933 à 8943 conduira généralement l'ALG à ignorer complètement le paquet et à n'effectuer aucune manipulation. Il en va de même pour RTP. Bien qu'elle ne soit pas définie

par une norme spécifique, la plage de ports la plus courante utilisée pour RTP est de 16384 à 16482. Pour éviter le potentiel d'interaction ALG, le produit BroadCloud utilise les ports RTP 19560-65535.

Paramètres de qualité de service

La qualité de service (QOS) fait référence à la capacité de fournir une priorité différente à différentes applications sur une connexion de réseau de données afin de s'assurer que le trafic de priorité supérieure a la priorité sur le trafic de priorité inférieure. Une conversation vocale se déroule en temps réel et le trafic associé à un appel vocal doit être traité efficacement, faute de quoi des problèmes tels que des coupures ou un son saccadé se produiront. D'autre part, le trafic Internet normal est de type best-effort. Si des paquets sont abandonnés ou différés, le service n'est généralement pas perturbé de façon notable. Par conséquent, le trafic vocal est généralement considéré comme un trafic plus prioritaire que le trafic de données.

Le produit BroadCloud utilise le DSCP (Differentiated Services Code Point), également appelé DiffServ, comme mécanisme de marquage de la priorité des paquets. Chaque périphérique SIP définit automatiquement chaque paquet qu'il envoie comme hautement prioritaire. Toutefois, cela ne garantit pas que tous les équipements du réseau de données situés sur le trajet du trafic respecteront ce paramètre et permettront au trafic vocal de prendre la priorité sur le trafic de données.

Pour que les paquets vocaux soient prioritaires par rapport aux paquets de données, les routeurs des clients doivent être correctement configurés pour gérer le DSCP. Cette fonctionnalité est parfois appelée classe de service (COS) ou file d'attente prioritaire. Dans les deux cas, il est recommandé de configurer le routeur avec une mise en file d'attente prioritaire stricte permettant aux paquets marqués avec des valeurs DSCP plus élevées d'avoir une priorité plus élevée. Si cela n'est pas fait correctement, la qualité d'appel perçue pourrait se détériorer sensiblement pendant les pics de trafic.

De plus, les paquets définis avec une priorité élevée par les périphériques SIP ne concernent que le trafic envoyé par le périphérique SIP vers d'autres périphériques en dehors du réseau du client. Ils ne concernent pas les paquets entrants dans le périphérique SIP. Ces paquets ne sont normalement pas marqués d'une priorité plus élevée lorsqu'ils sont reçus par le routeur du client, car les valeurs de priorité ne sont normalement pas maintenues sur un réseau étendu. Par conséquent, sans configuration supplémentaire, ces paquets ne seront pas prioritaires par rapport au trafic de données normal. Pour résoudre ce problème, il est recommandé d'établir des règles de priorité pour permettre à tout le trafic SIP et RTP entrant d'avoir une priorité plus élevée que tout autre trafic. Les ports spécifiques associés à SIP et RTP sont définis dans la section Pare-feu de ce document. Il peut également être nécessaire de définir les adresses IP des plateformes de contrôle des appels BroadCloud pour qu'elles aient une priorité plus élevée sur tout autre trafic. Une liste

spécifique de ces adresses IP n'est pas définie dans ce document car elles sont actuellement sujettes à des modifications. Si la priorisation des adresses IP est nécessaire pour une application spécifique du client, les adresses IP uniques qui doivent être provisionnées seront fournies sur demande.

Bande passante Internet

La bande passante Internet est la quantité de capacité disponible pour le trafic Internet sur le réseau d'un client. Cette quantité est déterminée par le service fourni par le fournisseur de services Internet. La quantité de bande passante disponible détermine la quantité d'appels vocaux et de trafic de données simultanés que la connexion Internet peut supporter. S'il est correctement dimensionné et avec les paramètres QOS appropriés dans le routeur du client, le service BroadCloud fonctionnera correctement. Cependant, s'il est insuffisant ou si la qualité de service n'est pas fournie correctement, la qualité d'appel perçue peut se détériorer sensiblement pendant les pics de trafic. Les informations suivantes fournissent des informations et des directives pour adapter correctement le service vocal à une bande passante Internet donnée.

estimer la bande passante requise

Voici des conseils généraux pour estimer la largeur de bande minimale requise pour un client ou un emplacement :

- la moyenne conservatrice requise est de 100 Kbps par appel audio, ce qui inclut la signalisation, le média et les frais généraux. La bande passante requise peut être réduite par la compression, mais cette estimation prudente est utile pour la planification du réseau.
- Les appels simultanés par nombre de périphériques sont une fonction qui dépend du type de client ou d'entreprise.
- Les bureaux dont les routeurs sont configurés pour donner la priorité au trafic vocal sur le trafic de données pourront traiter davantage d'appels vocaux sans compromettre la qualité des appels. Cependant, si les volumes d'appels sont extrêmement importants, la qualité du trafic de données pourrait être affectée. Par conséquent, nous recommandons que l'ingénierie de la bande passante soit effectuée en considérant qu'une partie seulement de la bande passante globale est disponible pour le trafic vocal.

Bande passante du réseau local

La bande passante du réseau local (LAN) est la quantité de capacité que le réseau interne d'un client peut supporter. Cette quantité est déterminée par les spécifications de débit de l'infrastructure du réseau local. Dans la plupart des applications clients, l'infrastructure du réseau local est constituée d'un seul commutateur de couche 2. La quantité de bande

passante disponible déterminera la quantité d'appels vocaux et de trafic de données simultanés que le LAN pourra prendre en charge. S'il est correctement dimensionné, le service BroadCloud fonctionnera correctement. Cependant, s'il est sous-dimensionné, la qualité perçue des appels pourrait se détériorer sensiblement pendant les périodes de pointe. Il est de la responsabilité du client de s'assurer que son réseau interne est correctement dimensionné pour supporter l'ajout de la VOIP à son réseau.

Spécifications de configuration du pare-feu du client

Les paramètres du pare-feu requis pour que le service BroadCloud fonctionne correctement sont documentés dans le guide Paramètres du pare-feu du client pour les environnements des États-Unis et de l'Union européenne.