Listes de contrôle d'accès sur les WLC - Règles, limitations et exemples

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Conventions](#)
[Comprendre les ACL sur un WLC](#)
[Règles et limitations ACL](#)
[Limites des ACL basées sur WLC](#)
[Règles pour les ACL basées sur WLC](#)
[Configurations](#)
[Exemple de liste de contrôle d'accès avec DHCP, PING, HTTP et DNS](#)
[Exemple de liste de contrôle d'accès avec DHCP, PING, HTTP et SCCP](#)
[Annexe : Ports de téléphone IP 7920](#)
[Informations connexes](#)

Introduction

Ce document fournit des informations au sujet des listes de contrôle d'accès sur les contrôleurs de réseau local sans fil. Ce document explique les limitations et les règles actuelles et donne des exemples pertinents. Ce document n'est pas destiné à remplacer les ACL sur l'exemple de configuration du contrôleur LAN sans fil, mais à fournir des informations supplémentaires.

Remarque : pour les listes de contrôle d'accès de couche 2 ou pour plus de flexibilité dans les règles de la couche 3, Cisco recommande de configurer les listes de contrôle d'accès sur le routeur du premier saut connecté au contrôleur.

L'erreur la plus courante se produit lorsque le champ de protocole est défini sur IP (protocol=4) dans une ligne de liste de contrôle d'accès avec l'intention d'autoriser ou de refuser des paquets IP. Comme ce champ sélectionne ce qui est encapsulé dans le paquet IP, tel que TCP, UDP (User Datagram Protocol) et ICMP (Internet Control Message Protocol), il se traduit par le blocage ou l'autorisation des paquets IP dans IP. À moins que vous ne souhaitiez bloquer les paquets IP mobiles, IP ne doit pas être sélectionné dans une ligne de liste de contrôle d'accès. L'ID de bogue Cisco CSCsh2975 (clients enregistrés uniquement) change IP en IP-in-IP.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de la configuration du WLC et du point d'accès léger (LAP) pour le fonctionnement de base
- Connaissance de base du protocole de point d'accès léger (LWAPP) et des méthodes de sécurité sans fil

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Comprendre les ACL sur un WLC

Les listes de contrôle d’accès se composent d’une ou de plusieurs lignes, suivies d’un « deny any any » implicite à la fin de la liste. Chaque ligne comporte les champs suivants :

- Numéro d'ordre
- Direction
- Adresse IP source et masque
- Adresse IP et masque de destination
- Protocol
- Port Src
- Port de destination
- DSCP
- Action

Ce document décrit chacun de ces champs :

- Sequence Number : indique l'ordre dans lequel les lignes ACL sont traitées par rapport au paquet. Le paquet est traité par rapport à la liste de contrôle d’accès jusqu’à ce qu’il corresponde à la première ligne. Elle vous permet également d'insérer des lignes de liste de contrôle d'accès n'importe où dans la liste même après sa création. Par exemple, si vous disposez d'une ligne de liste de contrôle d'accès dont le numéro d'ordre est 1, vous pouvez insérer une nouvelle ligne de liste de contrôle d'accès devant si elle est 1. La ligne active est automatiquement déplacée vers le bas dans la liste de contrôle d’accès.

- Direction : indique au contrôleur dans quelle direction appliquer la ligne de la liste de contrôle d'accès. Il existe 3 directions : Inbound, Outbound et Any. Ces directions sont prises à partir d'une position relative au WLC et non au client sans fil.
    - Entrant : les paquets IP provenant du client sans fil sont inspectés pour voir s'ils correspondent à la ligne ACL.
    - Sortant : les paquets IP destinés au client sans fil sont inspectés pour voir s'ils correspondent à la ligne ACL.
    - Any : les paquets IP provenant du client sans fil et destinés au client sans fil sont inspectés pour voir s'ils correspondent à la ligne ACL. La ligne ACL est appliquée aux directions entrantes et sortantes.

      Remarque : la seule adresse et le seul masque à utiliser lorsque vous sélectionnez Any (Tous) pour la direction est 0.0.0.0/0.0.0.0 (Tous). Vous ne devez pas spécifier un hôte ou un sous-réseau spécifique avec la direction « Tout », car une nouvelle ligne serait nécessaire avec les adresses ou les sous-réseaux échangés pour permettre le trafic de retour.

      La direction Any ne doit être utilisée que dans des situations spécifiques où vous souhaitez bloquer ou autoriser un protocole IP ou un port spécifique dans les deux directions, allant vers les clients sans fil (sortant) et venant des clients sans fil (entrant).

      Lorsque vous spécifiez des adresses IP ou des sous-réseaux, vous devez spécifier la direction comme Inbound ou Outbound et créer une seconde ligne ACL pour le trafic de retour dans la direction opposée. Si une liste de contrôle d’accès est appliquée à une interface et qu’elle n’autorise pas spécifiquement le trafic de retour, le trafic de retour est refusé par l’instruction implicite « deny any any » à la fin de la liste de contrôle d’accès.
- Source IP Address and Mask : définit les adresses IP source d'un hôte unique vers plusieurs sous-réseaux, en fonction du masque. Le masque est utilisé conjointement avec une adresse IP afin de déterminer quels bits d'une adresse IP doivent être ignorés lorsque cette adresse IP est comparée à l'adresse IP dans le paquet.

  Remarque : les masques d'une liste de contrôle d'accès WLC ne sont pas comme les masques génériques ou inverses utilisés dans les listes de contrôle d'accès Cisco IOS®. Dans les listes de contrôle d'accès du contrôleur, 255 signifie correspondre exactement à l'octet de l'adresse IP, tandis que 0 est un caractère générique. L'adresse et le masque sont combinés bit par bit.
    - Un bit de masque 1 signifie vérifier la valeur de bit correspondante. La spécification de 255 dans le masque indique que l’octet dans l’adresse IP du paquet qui est inspecté doit correspondre exactement avec l’octet correspondant dans l’adresse de la liste de contrôle d’accès.
    - Un bit de masque 0 signifie ne pas vérifier (ignorer) cette valeur de bit correspondante.

La spécification de 0 dans le masque indique que l'octet dans l'adresse IP du paquet qui est inspecté est ignoré.

- 0.0.0.0/0.0.0.0 équivaut à « Toute » adresse IP (0.0.0.0 comme adresse et 0.0.0.0 comme masque).

- Destination IP Address and Mask : suit les mêmes règles de masque que l'adresse IP source et le masque.
- Protocol : spécifie le champ de protocole dans l'en-tête du paquet IP. Certains des numéros de protocole sont traduits pour la commodité du client et sont définis dans le menu déroulant. Les différentes valeurs sont les suivantes :
  - Tous (tous les numéros de protocole correspondent)
  - TCP (protocole IP 6)
  - UDP (protocole IP 17)
  - ICMP (IP protocol 1)
  - ESP (protocole IP 50)
  - AH (protocole IP 51)
  - GRE (protocole IP 47)
  - IP (protocole IP 4 IP-in-IP [CSCsh22975])
  - Eth over IP (protocole IP 97)
  - OSPF (protocole IP 89)
  - Autre (préciser)

  La valeur Any correspond à n'importe quel protocole dans l'en-tête IP du paquet. Il est utilisé pour bloquer complètement ou autoriser les paquets IP vers/depuis des sous-réseaux spécifiques. Sélectionnez IP pour faire correspondre les paquets IP-in-IP. Les sélections courantes sont UDP et TCP, qui permettent de définir des ports source et de destination spécifiques. Si vous sélectionnez Autre, vous pouvez spécifier n'importe quel numéro de protocole de paquet IP défini par l'IANA.
- Src Port : peut uniquement être spécifié pour les protocoles TCP et UDP. 0-65535 équivaut à Any port.
- Dest Port : peut uniquement être spécifié pour les protocoles TCP et UDP. 0-65535 équivaut à Any port.
- Differentiated Services Code Point (DSCP) : permet de spécifier des valeurs DSCP spécifiques à faire correspondre dans l'en-tête du paquet IP. Les options du menu déroulant sont spécifiques ou Any (Tous). Si vous configurez des paramètres spécifiques, vous

indiquez la valeur dans le champ DSCP. Par exemple, des valeurs comprises entre 0 et 63 peuvent être utilisées.

- Action : les 2 actions sont deny ou permit. Deny bloque le paquet spécifié. Autoriser le transfert du paquet.

Règles et limitations ACL

Limites des ACL basées sur WLC

Voici les limitations des ACL basées sur WLC :

- Vous ne pouvez pas voir quelle ligne de liste de contrôle d'accès correspond à un paquet (référez-vous à l'ID de bogue Cisco CSCse36574 (clients enregistrés uniquement)).
- Vous ne pouvez pas consigner les paquets qui correspondent à une ligne de liste de contrôle d'accès spécifique (référez-vous à l'ID de bogue Cisco CSCse36574 (clients enregistrés uniquement)).
- Les paquets IP (tout paquet dont le champ de protocole Ethernet est égal à IP [0x0800]) sont les seuls paquets inspectés par la liste de contrôle d'accès. Les autres types de paquets Ethernet ne peuvent pas être bloqués par les listes de contrôle d'accès. Par exemple, les paquets ARP (protocole Ethernet 0x0806) ne peuvent pas être bloqués ou autorisés par la liste de contrôle d'accès.
- Un contrôleur peut avoir jusqu'à 64 ACL configurées ; chaque ACL peut avoir jusqu'à 64 lignes.
- Les listes de contrôle d'accès n'affectent pas le trafic de multidiffusion et de diffusion qui est transféré depuis ou vers les points d'accès (AP) et les clients sans fil (référez-vous à l'ID de bogue Cisco CSCse65613 (clients enregistrés uniquement)).
- Avant la version 4.0 du WLC, les ACL sont contournées sur l'interface de gestion, de sorte que vous ne pouvez pas affecter le trafic destiné à l'interface de gestion. Après la version 4.0 du WLC, vous pouvez créer des ACL de CPU. Référez-vous à Configurer les ACL du CPU pour plus d'informations sur la façon de configurer ce type d'ACL.

  Remarque : les listes de contrôle d'accès appliquées aux interfaces Management et AP-Manager sont ignorées. Les listes de contrôle d'accès sur le WLC sont conçues pour bloquer le trafic entre le réseau sans fil et le réseau câblé, et non le réseau câblé et le WLC. Par conséquent, si vous voulez empêcher les AP dans certains sous-réseaux de communiquer entièrement avec le WLC, vous devez appliquer une liste d'accès sur vos commutateurs intermittents ou votre routeur. Cela bloquera le trafic LWAPP de ces AP (VLAN) vers le WLC.
- Les listes de contrôle d'accès dépendent du processeur et peuvent affecter les performances du contrôleur en cas de charge importante.

- Les listes de contrôle d’accès ne peuvent pas bloquer l’accès à l’adresse IP virtuelle (1.1.1.1). Par conséquent, DHCP ne peut pas être bloqué pour les clients sans fil.
- Les ACL n'affectent pas le port de service du WLC.

Règles pour les ACL basées sur WLC

Voici les règles pour les ACL basées sur WLC :

- Vous ne pouvez spécifier des numéros de protocole que dans l’en-tête IP (UDP, TCP, ICMP, etc.) des lignes de liste de contrôle d’accès, car les listes de contrôle d’accès sont limitées aux paquets IP. Si IP est sélectionné, cela indique que vous souhaitez autoriser ou refuser les paquets IP-in-IP. Si Any est sélectionné, cela indique que vous voulez autoriser ou refuser les paquets avec n'importe quel protocole IP.
- Si vous sélectionnez Any (Tous) pour la direction, la source et la destination doivent être Any (0.0.0.0/0.0.0.0).
- Si l'adresse IP source ou de destination n'est pas Any, la direction du filtre doit être spécifiée. En outre, une instruction inverse (avec échange d'adresse IP source/port et d'adresse IP de destination/port) dans la direction opposée doit être créée pour le trafic de retour.
- Il y a un « deny any any » implicite à la fin de la liste de contrôle d’accès. Si un paquet ne correspond à aucune ligne de la liste de contrôle d'accès, il est abandonné par le contrôleur.

Configurations

Exemple de liste de contrôle d’accès avec DHCP, PING, HTTP et DNS

Dans cet exemple de configuration, les clients peuvent uniquement :

- Recevoir une adresse DHCP (DHCP ne peut pas être bloqué par une liste de contrôle d’accès)
- Envoi d’une requête ping et envoi d’une requête ping (tout type de message ICMP ne peut pas être limité aux requêtes ping uniquement)
- Établir des connexions HTTP (sortantes)
- Résolution DNS (Domain Name System) (sortante)

Afin de configurer ces exigences de sécurité, la liste de contrôle d'accès doit avoir des lignes pour permettre :

- Tout message ICMP dans l'une ou l'autre direction (ne peut pas être limité à la requête ping uniquement)
- Tout port UDP vers DNS entrant

- DNS vers tout port UDP sortant (trafic de retour)
- Tout port TCP vers HTTP entrant
- HTTP vers un port TCP sortant (trafic de retour)

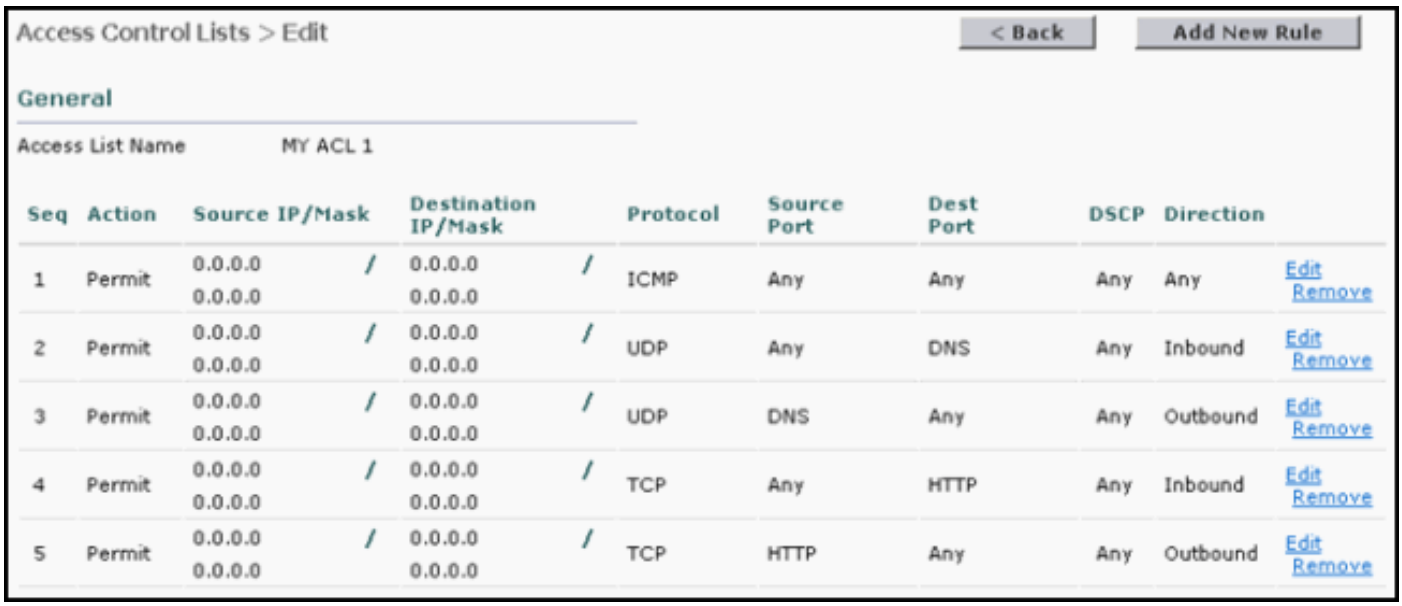
Voici à quoi ressemble la liste de contrôle d'accès dans le résultat de la commande show acl detailed "MY ACL 1" (les guillemets ne sont nécessaires que si le nom de la liste de contrôle d'accès est supérieur à 1 mot) :

```
Seq  Direction  Source IP/Mask    Dest IP/Mask      Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------   ---------------   --------  --------  ---------  ----  ------
1      Any      0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0      1      0-65535   0-65535     Any  Permit
2      In       0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0     17      0-65535   53-53       Any  Permit
3      Out      0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0     17      53-53     0-65535     Any  Permit
```

La liste de contrôle d’accès peut être plus restrictive si vous spécifiez le sous-réseau sur lequel se trouvent les clients sans fil au lieu de « Toute adresse IP » dans les lignes DNS et HTTP ACL.

Remarque : les lignes de la liste de contrôle d'accès DHCP ne peuvent pas être restreintes en sous-réseaux car le client reçoit initialement son adresse IP à l'aide de 0.0.0.0, puis renouvelle son adresse IP via une adresse de sous-réseau.

Voici à quoi ressemble la même liste de contrôle d’accès dans l’interface graphique :



Exemple de liste de contrôle d’accès avec DHCP, PING, HTTP et SCCP

Dans cet exemple de configuration, les téléphones IP 7920 peuvent uniquement :

- Recevoir une adresse DHCP (ne peut pas être bloquée par une liste de contrôle d’accès)
- Envoi d’une requête ping et envoi d’une requête ping (tout type de message ICMP ne peut

pas être limité aux requêtes ping uniquement)

- Autoriser la résolution DNS (entrante)
- Connexion du téléphone IP au CallManager et vice versa (Any Direction)
- Connexions des téléphones IP au serveur TFTP (CallManager utilise un port dynamique après la connexion TFTP initiale au port UDP 69) (Sortant)
- Autoriser les communications entre téléphones IP 7920 (dans toutes les directions)
- Interdire l'accès Web au téléphone IP ou à l'annuaire téléphonique (sortant). Cette opération est effectuée via une ligne de liste de contrôle d'accès implicite « deny any any » à la fin de la liste.

  Cela permettra les communications vocales entre les téléphones IP ainsi que les opérations de démarrage normales entre le téléphone IP et CallManager.

Afin de configurer ces exigences de sécurité, la liste de contrôle d'accès doit avoir des lignes pour permettre :

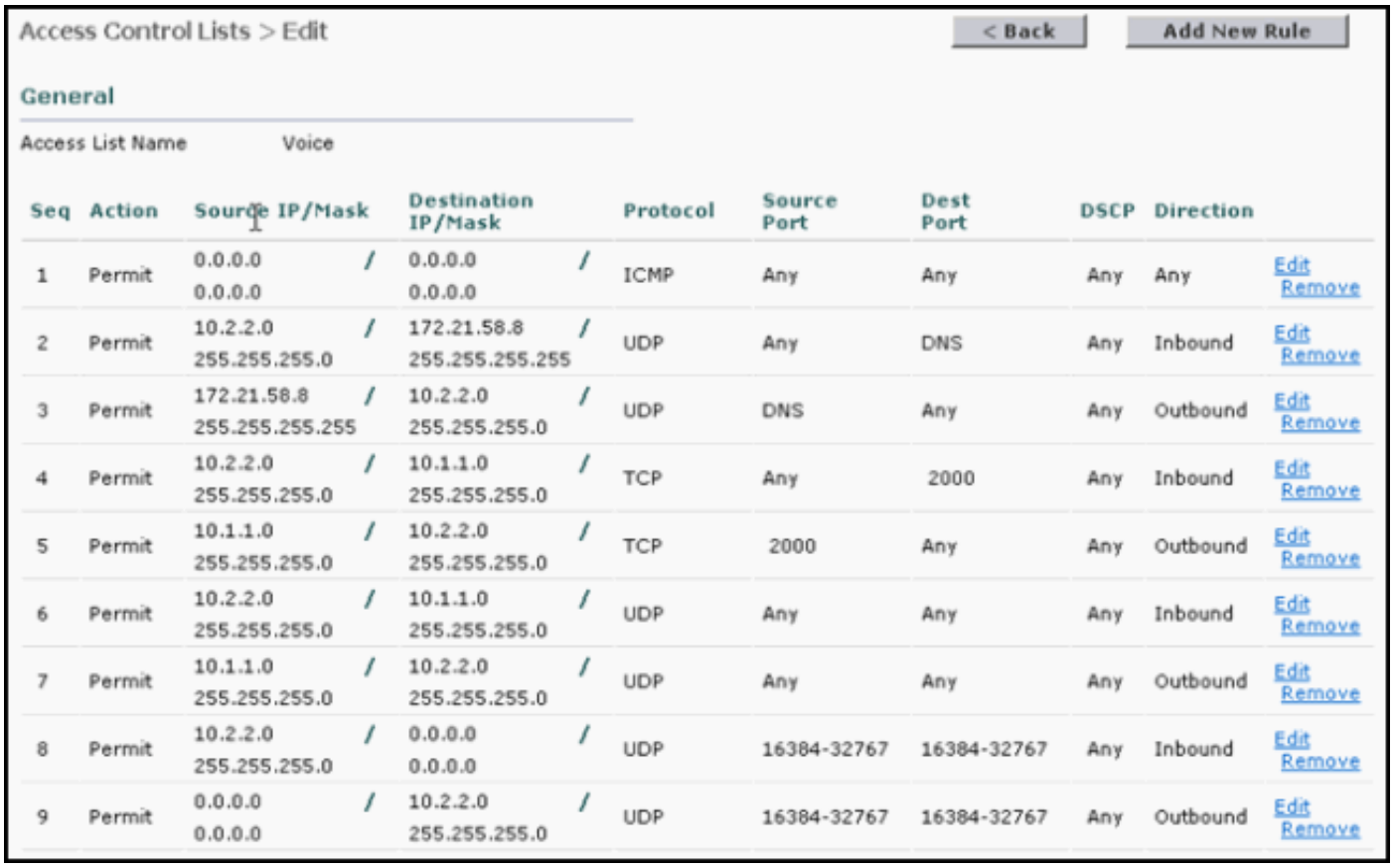
- Tout message ICMP (ne peut pas être limité à la requête ping uniquement) (Toute direction)
- Téléphone IP vers le serveur DNS (port UDP 53) (entrant)
- Le serveur DNS vers les téléphones IP (port UDP 53) (sortant)
- Ports TCP du téléphone IP vers le port TCP 2000 de CallManager (port par défaut) (entrant)
- Port TCP 2000 du CallManager vers les téléphones IP (sortant)
- Port UDP du téléphone IP au serveur TFTP. Cette opération ne peut pas être limitée au port TFTP standard (69), car CallManager utilise un port dynamique après la demande de connexion initiale pour le transfert de données.
- Port UDP pour le trafic audio RTP entre téléphones IP (ports UDP16384-32767) (dans toutes les directions)

Dans cet exemple, le sous-réseau du téléphone IP 7920 est 10.2.2.0/24 et le sous-réseau CallManager est 10.1.1.0/24. Le serveur DNS est 172.21.58.8. Voici le résultat de la commande show acl detail Voice :

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port  DSCP  Actio
--- --------- --------------          --------------          -------- --------  ---------  ----  -----
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535    Any  Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any  Permit
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any  Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any  Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any  Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any  Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any  Permit
```

```
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0           17 16384-32767 16384-32767 Any  Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0    17 16384-32767 16384-32767 Any  Permit
```

Voici à quoi il ressemble dans l'interface graphique :



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name Voice

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

Annexe : Ports de téléphone IP 7920

Voici les descriptions récapitulatives des ports utilisés par le téléphone IP 7920 pour communiquer avec Cisco CallManager (CCM) et d'autres téléphones IP :

- Téléphone vers CCM [TFTP] (port UDP 69 initialement puis port dynamique [Ephemeral] pour le transfert de données) : protocole TFTP (Trivial File Transfer Protocol) utilisé pour télécharger les microprogrammes et les fichiers de configuration.
- Phone to CCM [Web Services, Directory] (TCP port 80) : URL du téléphone pour les applications XML, l'authentification, les répertoires, les services, etc. Ces ports peuvent être configurés par service.
- Phone to CCM [Voice Signaling] (TCP port 2000) : protocole SCCP (Skinny Client Control Protocol). Ce port est configurable.
- Téléphone vers CCM [signalisation vocale sécurisée] (port TCP 2443) : protocole SCCPS (Secure Skinny Client Control Protocol)
- Phone to CAPF [Certificates] (Port TCP 3804) : port d'écoute CAPF (Certificate Authority

Proxy Function) pour émettre des certificats LSC (Locally Significative Certificates) vers des téléphones IP.

- Support vocal vers/depuis le téléphone [appels téléphoniques] (ports UDP 16384 - 32768) : protocole RTP (Real-Time Protocol), protocole SRTP (Secure Real-Time Protocol).

  Remarque : CCM utilise uniquement les ports UDP 24576-32768, mais les autres périphériques peuvent utiliser la plage complète.

- IP Phone to DNS Server [DNS] (UDP port 53) : les téléphones utilisent DNS pour résoudre le nom d'hôte des serveurs TFTP, des CallManagers et des noms d'hôte des serveurs Web lorsque le système est configuré pour utiliser des noms plutôt que des adresses IP.

- IP Phone to DHCP server [DHCP] (UDP port 67 [client] & 68 [serveur]) : le téléphone utilise DHCP pour récupérer une adresse IP si elle n'est pas configurée de manière statique.

Les ports avec lesquels CallManager 5.0 communique sont disponibles sur Cisco Unified CallManager 5.0 TCP and UDP Port Usage. Il dispose également des ports spécifiques qu'il utilise pour communiquer avec le téléphone IP 7920.

Les ports avec lesquels CallManager 4.1 communique sont disponibles sur Cisco Unified CallManager 4.1 TCP and UDP Port Usage. Il dispose également des ports spécifiques qu'il utilise pour communiquer avec le téléphone IP 7920.

Informations connexes

- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.