Listes de contrôle d'accès sur les contrôleurs de réseau local sans fil : Règles, limitations et exemples

Contenu

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 limites et les règles en cours, et donne des exemples appropriés. Ce document n'est pas censé pour être un remplacement pour ACLs sur l'exemple Sans fil de configuration de contrôleur LAN, mais pour fournir des informations supplémentaires.

Note: Pour la couche 2 ACLs ou la flexibilité supplémentaire dans des règles d'ACL de la couche 3, Cisco recommande que vous configuriez ACLs sur le premier routeur connecté de saut au contrôleur.

L'erreur la plus commune se produit quand le champ de protocole est placé à IP (protocol=4) dans une ligne d'ACL avec l'intention de permettre ou de refuser des paquets IP. Puisque ce champ sélectionne réellement ce qui est encapsulé à l'intérieur du paquet IP, tel que le TCP, le Protocole UDP (User Datagram Protocol), et le Protocole ICMP (Internet Control Message Protocol), il se traduit en bloquer ou permettre des paquets d'IP-in-IP. À moins que vous vouliez bloquer des paquets d'IP mobile, l'IP ne doit pas n'être sélectionné dans aucune ligne d'ACL. L'ID de bogue Cisco CSCsh22975 (clients enregistrés seulement) change l'IP à l'IP-in-IP.

Conditions préalables

Conditions requises

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

- La connaissance de la façon configurer le WLC et le 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.

Comprenez ACLs sur un WLC

ACLs se en composent d'un ou plusieurs lignes d'ACL suivies d'un implicite « refusent tous les » à la fin de l'ACL. Chaque ligne a ces champs :

- Numéro de séquence
- Direction
- Adresse IP source et masque
- Adresse IP et masque de destination
- Protocol
- Port de Src
- Port DEST
- DSCP
- Action

Ce document décrit chacun de ces champs :

- **Numéro de séquence** — Indique la commande que des lignes d'ACL sont traitées contre le paquet. Le paquet est traité contre l'ACL jusqu'à ce qu'il apparie la première ligne d'ACL. Il te permet également pour insérer des lignes d'ACL n'importe où dans l'ACL même après que l'ACL est créé. Par exemple, si vous avez une ligne d'ACL avec un numéro de séquence de 1, vous pouvez insérer une nouvelle ligne d'ACL dans l'avant s'il par la mise dans un numéro de séquence de 1 dans la nouvelle ligne d'ACL. Ceci déplace automatiquement la ligne actuelle vers le bas dans l'ACL.
- **Direction** — Dit le contrôleur en lequel direction pour imposer la ligne d'ACL. Il y a 3 directions : D'arrivée, sortant, et quels. Ces directions ne sont prises d'une position relativement au WLC et pas au client sans fil.D'arrivée — Des paquets IP originaires du client sans fil sont examinés pour voir s'ils apparient la ligne d'ACL.Sortant — Des paquets IP destinés au client sans fil sont examinés pour voir s'ils apparient la ligne d'ACL.Quels — Des paquets IP originaires du client sans fil et destinés au client sans fil sont examinés pour voir s'ils

apparient la ligne d'ACL. La ligne d'ACL est appliquée à d'arrivée et aux directions sortantes.**Note**: La seuls adresse et masque qui devraient être utilisés quand vous en sélectionnez pour la direction est 0.0.0.0/0.0.0.0 (quels). Vous ne devez pas spécifier un hôte spécifique ou un sous-réseau avec la « aucune » direction parce qu'une nouvelle ligne serait exigée avec les adresses ou les sous-réseaux permutée pour tenir compte du trafic de retour.La n'importe quelle direction devrait seulement être utilisée dans des situations spécifiques où vous voulez bloquer ou permettre un protocole IP de particularité ou mettre en communication dans les deux directions, allant aux clients sans fil (sortants) et provenant les clients sans fil (d'arrivée).Quand vous spécifiez des adresses IP ou des sous-réseaux, vous devez spécifier la direction en tant que d'arrivée ou sortant et créer une deuxième nouvelle ligne d'ACL pour le trafic de retour dans le sens inverse. Si un ACL est appliqué à une interface et ne permet pas spécifiquement le trafic de retour de retour, le trafic de retour en est refusé par l'implicite « refusent tous les » à la fin de la liste d'ACL.

- **Adresse IP source et masque** — Définit les adresses IP de source d'un seul hôte à de plusieurs sous-réseaux, qui dépend du masque. Le masque est utilisé en même temps qu'une adresse IP afin de déterminer quels bits dans une adresse IP devraient être ignorés quand cette adresse IP est comparée à l'adresse IP dans le paquet.**Note**: Les masques dans un ACL WLC ne sont pas comme le masque ou les masques inverses utilisés dans le Cisco IOS® ACLs. Dans le contrôleur ACLs, 255 signifie la correspondance l'octet dans l'adresse IP exactement, alors que 0 est un masque. L'adresse et le masque sont combinés peu à peu.Un bit de masque 1 signifie le contrôle la valeur de bit correspondant. La spécification de 255 dans le masque indique que l'octet dans l'adresse IP du paquet qui est examiné doit s'assortir exactement avec l'octet la correspondance dans l'adresse d'ACL.Un bit de masque 0 signifie ne vérifient pas (ignorer) cette valeur de bit correspondant. La spécification de 0 dans le masque indique que l'octet dans l'adresse IP du paquet qui est examiné est ignoré.0.0.0.0/0.0.0.0 est équivalent à « n'importe quelle » adresse IP (0.0.0.0 comme adresse et 0.0.0.0 comme masque).
- **Adresse IP et masque de destination** — Suit les mêmes règles de masque que l'adresse IP source et le masque.
- **Protocol** — Spécifie le champ de protocole dans l'en-tête de paquet IP. Certains des nombres de protocole sont traduits pour la commodité de client et sont définis dans le menu de traction vers le bas. Les différentes valeurs sont :Quels (tous les nombres de protocole sont appariés)TCP (protocole IP 6)UDP (protocole 17 IP)ICMP (protocole IP 1)L'ESP (protocole 50 IP)OH (protocole 51 IP)GRE (protocole 47 IP)IP (IP-in-IP [CSCsh22975] de protocole 4 IP)Eth au-dessus d'IP (protocole 97 IP)OSPF (protocole 89 IP)Autre (spécifiez)La n'importe quelle valeur apparie n'importe quel protocole dans l'en-tête IP du paquet. Ceci est utilisé complètement pour bloquer ou permettre des paquets IP à/de des sous-réseaux spécifiques. IP choisi pour apparier des paquets d'IP-in-IP. Les sélections communes sont UDP et TCP qui prévoient placer la source spécifique et les destinations port. Si vous sélectionnez autre, vous pouvez spécifier les nombres l'uns des de protocole de paquet IP définis par l'IANA .
- **Port de Src** — Peut seulement être spécifié pour le protocole de TCP et UDP. 0-65535 est équivalent à n'importe quel port.
- **Port DEST** — Peut seulement être spécifié pour le protocole de TCP et UDP. 0-65535 est équivalent à n'importe quel port.
- **Differentiated Services Code Point (DSCP)** — Te permet pour spécifier des valeurs DSCP spécifiques pour apparier dans l'en-tête de paquet IP. Les choix dans le menu de traction en baisse en sont spécifiques ou. Si vous configurez la particularité, vous indiquez la valeur dans le domaine de DSCP. Par exemple, des valeurs de 0 à 63 peuvent être utilisées.

- **Action** — Les 2 actions sont refusent ou laissent. Refusez à des blocs le paquet spécifié. Autorisation en avant le paquet.

Règles et limites d'ACL

Les limites de WLC ont basé ACLs

Ce sont les limites d'ACLs basé sur WLC :

- Vous ne pouvez pas voir quelle ligne d'ACL a été appariée par un paquet (référez-vous à l'ID de bogue Cisco CSCse36574 (clients enregistrés seulement)).
- Vous ne pouvez pas se connecter les paquets qui apparient une ligne d'ACL spécifique (référez-vous à l'ID de bogue Cisco CSCse36574 (clients enregistrés seulement)).
- Les paquets IP (tout paquet avec un champ de protocole d'Ethernets égal à IP [0x0800]) sont les seuls paquets examinés par l'ACL. D'autres types de paquets Ethernet ne peuvent pas être bloqués par ACLs. Par exemple, on ne peut pas être bloqué ou permis des paquets d'ARP (protocole Ethernet 0x0806) par l'ACL.
- Un contrôleur peut avoir jusqu'à 64 qu'ACLs a configurés ; chaque ACL peut avoir jusqu'à un maximum de 64 lignes.
- ACLs n'affectent pas le trafic de Multidiffusion et d'émission dont est expédié ou aux Points d'accès (aps) et aux clients sans fil (référez-vous à l'ID de bogue Cisco CSCse65613 (clients enregistrés seulement)).
- Avant version 4.0 WLC, ACLs sont sautés sur l'interface de gestion, ainsi vous ne pouvez pas affecter le trafic destiné à l'interface de gestion. Après version 4.0 WLC, vous pouvez créer CPU ACLs. Référez-vous configurent CPU ACLs pour plus d'informations sur la façon configurer ce type d'ACL.**Note**: ACLs s'est appliqué à la Gestion et des interfaces d'AP-gestionnaire sont ignorées. ACLs sur le WLC ne sont conçus pour bloquer le trafic entre la radio et le réseau câblé, pas le réseau câblé et le WLC. Par conséquent, si vous voulez empêcher des aps dans les certains sous-réseaux de communiquer avec le WLC entièrement, vous devez appliquer une liste d'accès sur vos Commutateurs ou routeur intermittents. Ceci bloquera le trafic LWAPP de ces aps (VLAN) au WLC.
- ACLs sont processeur-dépendant et peuvent affecter la représentation du contrôleur sous la charge lourde.
- ACLs ne peut pas bloquer l'accès à l'adresse IP virtuelle (1.1.1.1). Par conséquent, le DHCP ne peut pas être bloqué pour des clients sans fil.
- ACLs n'affectent pas le port de service du WLC.

Les règles pour WLC ont basé ACLs

Ce sont les règles pour ACLs basé sur WLC :

- Vous pouvez seulement spécifier des nombres de protocole dans l'en-tête IP (UDP, TCP, ICMP, etc.) dans les lignes d'ACL, parce qu'ACLs sont limités dans des paquets IP seulement. Si l'IP est sélectionné, ceci indique que vous voulez permettre ou refuser des paquets d'IP-in-IP. Si en est sélectionné, ceci indique que vous voulez permettre ou refuser des paquets avec n'importe quel protocole IP.
- Si vous en sélectionnez pour la direction, la source et la destination en devraient être

(0.0.0.0/0.0.0.0).
- Si la source ou l'adresse IP de destination n'en est pas, la direction du filtre doit être spécifiée. En outre, une déclaration inverse (avec adresse IP source/port et adresse IP de destination/port permuté) dans le sens inverse doit être créée pour le trafic de retour.
- Il y en a un implicite « refusent tous les » à la fin de l'ACL. Si un paquet ne fait pas le match any raye dans l'ACL, il est relâché par le contrôleur.

Configurations

Exemple d'ACL avec le DHCP, le PING, le HTTP, et les DN

Dans cet exemple de configuration, les clients sont puissent seulement :

- Recevez une adresse DHCP (le DHCP ne peut pas être bloqué par un ACL)
- Le ping et soit cinglé (aucun type de message ICMP - ne peut pas être limité pour cingler seulement)
- Établissez les connexions HTTP (sortantes)
- Résolution de Système de noms de domaine (DNS) (sortante)

Afin de configurer ces exigences de sécurité, l'ACL doit avoir des lignes à laisser :

- Tout message ICMP dans l'un ou l'autre de direction (ne peut pas être limité pour cingler seulement)
- Tout port UDP aux DN d'arrivée
- DN à tout port UDP sortant (renvoyez le trafic)
- Tout port TCP au HTTP d'arrivée
- HTTP à tout port TCP sortant (renvoyez le trafic)

C'est ce qui ressemble à l'ACL dans le **show acl détaillé « MA** sortie de commande de l'**ACL 1"** (les devis sont seulement nécessaires si le nom d'ACL est plus de 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
```

L'ACL peut être plus restrictif si vous spécifiez le sous-réseau que les clients sans fil sont en ligne au lieu de n'importe quelle adresse IP dans les lignes d'ACL de DN et de HTTP.

Note: Les lignes d'ACL DHCP ne peuvent pas être sous-réseau limité en tant que client au commencement reçoit son adresse IP utilisant 0.0.0.0, puis renouvelle son adresse IP par l'intermédiaire d'un subnet address.

C'est ce qui ressemble au même ACL dans le GUI :

Exemple d'ACL avec le DHCP, le PING, le HTTP, et le SCCP

Dans cet exemple de configuration, 7920 Téléphones IP sont puissent seulement :

- Recevez une adresse DHCP (ne peut pas être bloqué par ACL)

- Le ping et soit cinglé (aucun type de message ICMP - ne peut pas être limité pour cingler seulement)
- Permettez la résolution de DN (d'arrivée)
- Connexion de téléphone IP au CallManager et vice versa (toute direction)
- Connexions de téléphone IP au serveur TFTP (le CallManager utilise le port dynamique après la connexion initiale TFTP au port UDP 69) (sortant)
- Permettez la communication de téléphone IP à téléphone IP 7920 (toute direction)
- Rejetez le Web ou le répertoire téléphonique de téléphone IP (sortant). Ceci est fait par l'intermédiaire d'un implicite « refusent n'importe quelle n'importe quelle » ligne d'ACL à la fin de l'ACL.Ceci permettra des communications vocales entre les Téléphones IP aussi bien que les exécutions normales d'amorce entre le téléphone IP et le CallManager.

Afin de configurer ces exigences de sécurité, l'ACL doit avoir des lignes à laisser :

- Tout message ICMP (ne peut pas être limité pour cingler seulement) (toute direction)
- Téléphone IP au serveur DNS (port UDP 53) (d'arrivée)
- Le serveur DNS aux Téléphones IP (port UDP 53) (sortant)
- Ports TCP de téléphone IP au port TCP 2000 (port par défaut) de CallManager (d'arrivée)
- Port TCP 2000 du CallManager aux Téléphones IP (sortants)
- Port UDP du téléphone IP au serveur TFTP. Ceci ne peut pas être limité au port standard TFTP (69) parce que le CallManager utilise un port dynamique après la demande de connexion initiale du transfert des données.
- Port UDP pour le RTP sonore du trafic entre les Téléphones IP (UDP ports16384-32767) (toute direction)

Dans cet exemple, le sous-réseau du téléphone IP 7920 est 10.2.2.0/24 et le sous-réseau de CallManager est 10.1.1.0/24. Le serveur DNS est 172.21.58.8. C'est la sortie de la **commande vocale de détail de show acl** :

```
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      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
```

C'est ce qui ressemble à il dans le GUI :

Annexe : 7920 ports de téléphone IP

Ce sont les descriptions sommaires des ports les 7920 utilisations de téléphone IP de communiquer avec le Cisco CallManager (CCM) et d'autres Téléphones IP :

- Téléphonez à CCM [TFTP] (le port UDP 69 changent au commencement alors en le port dynamique [éphémère] pour le transfert des données) — Protocole TFTP (Trivial File Transfer Protocol) utilisé pour télécharger le micrologiciel et les fichiers de configuration.
- Téléphone à CCM [services Web, répertoire] (port TCP 80) — téléphonez l'URLs pour des applications XML, l'authentification, des répertoires, des services, etc. Ces ports sont configurables sur a par base de service.
- Téléphone CCM [signalisation de Voix] (port TCP 2000) — au Skinny Client Control Protocol (SCCP). Ce port est configurable.
- Téléphone CCM [signalisation de voix sécurisée] (port TCP 2443) — au Skinny Client Control Protocol sécurisé (SCCPS)
- Téléphonez à CAPF [Certificats] (port TCP 3804) — port en mode écoute de la fonction de proxy d'autorité de certification (CAPF) pour émettre localement - les Certificats significatifs (LSC) aux Téléphones IP.
- Support de Voix à/de le téléphone [appels téléphoniques] Protocole RTP (Real-Time Protocol) (de ports UDP 16384 – 32768) —, Protocol en temps réel sécurisé (SRTP).**Note**: Seulement les ports UDP des utilisations CCM 24576-32768, mais d'autres périphériques peuvent utiliser la gamme complète.
- Le téléphone IP au serveur DNS [DN] (port UDP 53) — les téléphones utilisent des DN pour résoudre le nom d'hôte des serveurs TFTP, des CallManagers, et des noms d'hôte de web server quand le système est configuré pour utiliser des noms plutôt que des adresses IP.
- Le téléphone IP au serveur DHCP [DHCP] (port UDP 67 [client] et 68 [serveur]) — le téléphone emploie le DHCP pour récupérer une adresse IP sinon statiquement configurée.

Les ports les 5.0 utilisations de CallManager de communiquer avec peuvent être trouvés à l'utilisation de port de TCP et UDP du Cisco Unified CallManager 5.0. Il a également le spécifique le met en communication l'utilise pour communiquer avec les 7920 téléphones IP.

Les ports les 4.1 utilisations de CallManager de communiquer avec peuvent être trouvés à l'utilisation de port de TCP et UDP du Cisco Unified CallManager 4.1. Il a également le spécifique le met en communication l'utilise pour communiquer avec les 7920 téléphones IP.

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
- Support et documentation techniques - Cisco Systems