ACL su WLC - Regole, limitazioni ed esempi

Sommario

Introduzione

In questo documento vengono fornite informazioni sugli Access Control List (ACL) sui Wireless LAN Controller (WLC). Questo documento illustra le limitazioni e le regole correnti e fornisce alcuni esempi pertinenti. Questo documento non deve sostituire gli ACL negli esempi di configurazione dei controller LAN wireless, ma fornire informazioni supplementari.

Nota: per gli ACL di layer 2 o per una maggiore flessibilità nelle regole degli ACL di layer 3, Cisco consiglia di configurare gli ACL sul primo router hop collegato al controller.

L'errore più comune si verifica quando il campo del protocollo è impostato su IP (protocollo=4) in una riga ACL con l'intenzione di autorizzare o negare i pacchetti IP. Poiché questo campo seleziona effettivamente ciò che è incapsulato nel pacchetto IP, ad esempio TCP, UDP (User Datagram Protocol) e ICMP (Internet Control Message Protocol), si traduce nel bloccare o consentire i pacchetti IP-in-IP. A meno che non si desideri bloccare i pacchetti IP mobili, l'indirizzo IP non deve essere selezionato in alcuna riga ACL. L'ID bug Cisco CSCsh22975 (solo utenti registrati) cambia da IP a IP-in-IP.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza di come configurare il WLC e il Lightweight Access Point (LAP) per le operazioni di base
- Conoscenze base di LWAPP (Lightweight Access Point Protocol) e metodi di sicurezza wireless

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Informazioni sugli ACL su un WLC

Gli ACL sono costituiti da una o più righe seguite da un'istruzione implicita di "negazione di qualsiasi" alla fine dell'ACL. Ogni riga contiene i campi seguenti:

- Numero progressivo
- Direzione
- Indirizzo IP di origine e maschera
- Indirizzo IP e maschera di destinazione
- Protocollo
- Src Port
- Porta di destinazione
- DSCP
- Azione

In questo documento vengono descritti i singoli campi seguenti:

- Numero di sequenza: indica l'ordine con cui le righe ACL vengono elaborate in base al pacchetto. Il pacchetto viene elaborato sull'ACL finché non corrisponde alla prima riga dell'ACL. Inoltre, permette di inserire righe in qualsiasi punto dell'ACL, anche dopo la creazione dell'ACL. Ad esempio, se si ha una riga ACL con un numero di sequenza 1, è possibile inserire una nuova riga ACL in primo piano inserendo il numero di sequenza 1 nella nuova riga. In questo modo la riga corrente viene automaticamente spostata verso il basso nell'ACL.
- Direzione (Direction) - Indica al controller in quale direzione applicare la linea ACL. Sono

disponibili 3 direzioni: In entrata, In uscita e Qualsiasi. Queste direzioni vengono prese da una posizione relativa al WLC e non dal client wireless.

- In entrata: i pacchetti IP provenienti dal client wireless vengono ispezionati per verificare che corrispondano alla linea ACL.
- In uscita: i pacchetti IP destinati al client wireless vengono ispezionati per verificare se corrispondono alla linea ACL.
- Any: i pacchetti IP provenienti dal client wireless e destinati al client wireless vengono ispezionati per verificare che corrispondano alla linea ACL. La riga ACL viene applicata sia alla direzione in entrata che a quella in uscita.

  Nota: l'unico indirizzo e l'unica maschera da utilizzare quando si seleziona Qualsiasi per la direzione è 0.0.0.0/0.0.0.0 (Any). Non è necessario specificare un host o una subnet specifici con direzione "Any" perché sarebbe necessaria una nuova riga con gli indirizzi o le subnet scambiati in modo da consentire il traffico di ritorno.

  La direzione Any deve essere utilizzata solo in situazioni specifiche in cui si desidera bloccare o consentire un protocollo IP specifico o una porta in entrambe le direzioni, passando ai client wireless (in uscita) e dai client wireless (in entrata).

  Quando si specificano indirizzi IP o subnet, è necessario specificare la direzione come In entrata o In uscita e creare una seconda nuova linea ACL per il traffico di ritorno nella direzione opposta. Se un ACL viene applicato a un'interfaccia e non consente in modo specifico il traffico di ritorno, il traffico di ritorno viene rifiutato in base al comando implicito "deny any" presente alla fine dell'elenco ACL.

- Source IP Address and Mask: definisce gli indirizzi IP di origine da un singolo host a più subnet, a seconda della maschera. La maschera viene usata insieme a un indirizzo IP per determinare i bit di un indirizzo IP da ignorare quando quell'indirizzo IP viene confrontato con l'indirizzo IP nel pacchetto.

  Nota: le maschere negli ACL WLC non sono simili ai caratteri jolly o alle maschere inverse usati negli ACL Cisco IOS®. Negli ACL dei controller, 255 significa esattamente corrispondenza dell'ottetto nell'indirizzo IP, mentre 0 è un carattere jolly. L'indirizzo e la maschera vengono combinati bit per bit.

  - Il bit 1 della maschera significa controllare il valore del bit corrispondente. La specifica di 255 nella maschera indica che l'ottetto nell'indirizzo IP del pacchetto ispezionato deve corrispondere esattamente all'ottetto corrispondente nell'indirizzo ACL.
  - Il bit 0 della maschera indica che non è necessario verificare (ignorare) il valore corrispondente. La specifica di 0 nella maschera indica che l'ottetto nell'indirizzo IP del pacchetto ispezionato viene ignorato.
  - 0.0.0.0/0.0.0.0 equivale a "Qualsiasi" indirizzo IP (0.0.0.0 come indirizzo e 0.0.0.0 come maschera).

- Indirizzo IP di destinazione e maschera: seguono le stesse regole di maschera dell'indirizzo IP e della maschera di origine.
- Protocollo: per specificare il campo del protocollo nell'intestazione del pacchetto IP. Alcuni numeri di protocollo vengono tradotti per agevolare il cliente e definiti nel menu a discesa. I diversi valori sono:
    - Any (tutti i numeri di protocollo corrispondono)
    - TCP (protocollo IP 6)
    - UDP (protocollo IP 17)
    - ICMP (protocollo IP 1)
    - ESP (protocollo IP 50)
    - AH (protocollo IP 51)
    - GRE (protocollo IP 47)
    - IP (protocollo IP 4 IP-in-IP [CSCsh2975])
    - Eth Over IP (protocollo IP 97)
    - OSPF (protocollo IP 89)
    - Altro (specificare)

  Il valore Any corrisponde a qualsiasi protocollo nell'intestazione IP del pacchetto. Questa opzione viene usata per bloccare o consentire completamente i pacchetti IP da e verso subnet specifiche. Selezionare IP per trovare una corrispondenza con i pacchetti IP-in-IP. Le selezioni più comuni sono UDP e TCP che consentono di impostare porte di origine e di destinazione specifiche. Se si seleziona Altro, è possibile specificare uno qualsiasi dei numeri di protocollo del pacchetto IP definiti da IANA.
- Src Port: può essere specificato solo per i protocolli TCP e UDP. 0-65535 equivale a Any port.
- Dest Port: può essere specificato solo per i protocolli TCP e UDP. 0-65535 equivale a Any port.
- DSCP (Differentiated Services Code Point): consente di specificare valori DSCP specifici da far corrispondere nell'intestazione del pacchetto IP. Le opzioni del menu a discesa sono specifiche o Qualsiasi. Se si configura un valore specifico, è necessario indicarlo nel campo DSCP. Ad esempio, è possibile utilizzare valori compresi tra 0 e 63.
- Azione (Action) - Le due azioni sono nega (Deny) o consenti (Allow). Nega blocca il pacchetto specificato. Permettere di inoltrare il pacchetto.

Regole e limitazioni degli ACL

Limitazioni degli ACL basati sui WLC

Di seguito sono riportati i limiti degli ACL basati su WLC:

- Non è possibile visualizzare la riga ACL corrispondente a un pacchetto (fare riferimento all'ID bug Cisco CSCse36574 (solo utenti registrati)).
- Non è possibile registrare pacchetti che corrispondono a una linea ACL specifica (fare riferimento all'ID bug Cisco CSCse36574 (solo utenti registrati)).
- I pacchetti IP (qualsiasi pacchetto il cui campo del protocollo Ethernet è uguale a IP [0x0800]) sono gli unici pacchetti ispezionati dall'ACL. Altri tipi di pacchetti Ethernet non possono essere bloccati dagli ACL. Ad esempio, i pacchetti ARP (protocollo Ethernet 0x0806) non possono essere bloccati o consentiti dall'ACL.
- Un controller può avere fino a 64 ACL configurati; ogni ACL può avere fino a un massimo di 64 linee.
- Gli ACL non influiscono sul traffico multicast e broadcast che viene inoltrato da o verso i punti di accesso (AP) e i client wireless (fare riferimento all'ID bug Cisco CSCse65613 (solo utenti registrati).
- Prima della versione WLC 4.0, gli ACL vengono ignorati sull'interfaccia di gestione, quindi non è possibile influenzare il traffico destinato all'interfaccia di gestione. Dopo la versione WLC 4.0, è possibile creare gli ACL della CPU. Per ulteriori informazioni su come configurare questo tipo di ACL, consultare il documento sulla configurazione degli ACL della CPU.

  Nota: gli ACL applicati alle interfacce di gestione e AP-Manager vengono ignorati. Gli ACL sul WLC sono progettati per bloccare il traffico tra la rete wireless e la rete cablata, non la rete cablata e il WLC. Pertanto, se si desidera impedire che i punti di accesso di determinate subnet comunichino completamente con il WLC, è necessario applicare un elenco degli accessi sugli switch o sul router intermittenti. In questo modo il traffico LWAPP da tali AP (VLAN) al WLC verrà bloccato.
- Gli ACL sono dipendenti dal processore e possono influire sulle prestazioni del controller in caso di carico elevato.
- Gli ACL non possono bloccare l'accesso all'indirizzo IP virtuale (1.1.1.1). Impossibile bloccare DHCP per i client wireless.
- Gli ACL non influiscono sulla porta di servizio del WLC.

Regole per ACL basati su WLC

Di seguito vengono riportate le regole per gli ACL basati su WLC:

- È possibile specificare solo i numeri di protocollo nell'intestazione IP (UDP, TCP, ICMP, ecc.) nelle righe degli ACL, in quanto gli ACL sono limitati ai soli pacchetti IP. Se è selezionato IP, significa che si desidera consentire o negare i pacchetti IP-in-IP. Se è selezionata l'opzione Any (Qualsiasi), significa che si desidera consentire o negare i pacchetti con qualsiasi protocollo IP.
- Se si seleziona Qualsiasi per la direzione, l'origine e la destinazione devono essere Qualsiasi (0.0.0.0/0.0.0.0).
- Se l'indirizzo IP di origine o di destinazione non è Qualsiasi, è necessario specificare la direzione del filtro. Inoltre, per il traffico di ritorno, è necessario creare un'istruzione inversa (con indirizzo IP di origine/porta e indirizzo IP di destinazione/porta scambiati) nella direzione opposta.
- Alla fine dell'ACL, è presente un'implicita clausola "deny any". Se un pacchetto non corrisponde ad alcuna riga nell'ACL, viene scartato dal controller.

Configurazioni

Esempio di ACL con DHCP, PING, HTTP e DNS

In questo esempio di configurazione, i client sono solo in grado di:

- Ricevi un indirizzo DHCP (DHCP non può essere bloccato da un ACL)
- Eseguire il ping e ricevere il ping (qualsiasi tipo di messaggio ICMP - non può essere limitato solo al ping)
- Crea connessioni HTTP (in uscita)
- Risoluzione DNS (Domain Name System) (in uscita)

Per configurare questi requisiti di sicurezza, l'ACL deve avere righe che consentano:

- Qualsiasi messaggio ICMP in entrambe le direzioni (non può essere limitato solo al ping)
- Qualsiasi porta UDP su DNS in ingresso
- DNS su qualsiasi porta UDP in uscita (traffico di ritorno)
- Qualsiasi porta TCP su HTTP in entrata
- HTTP su qualsiasi porta TCP in uscita (traffico di ritorno)

Di seguito viene riportato l'aspetto dell'ACL nell'output del comando show acl dettagliato "MY ACL 1" (le virgolette sono necessarie solo se il nome dell'ACL è superiore a 1 parola):

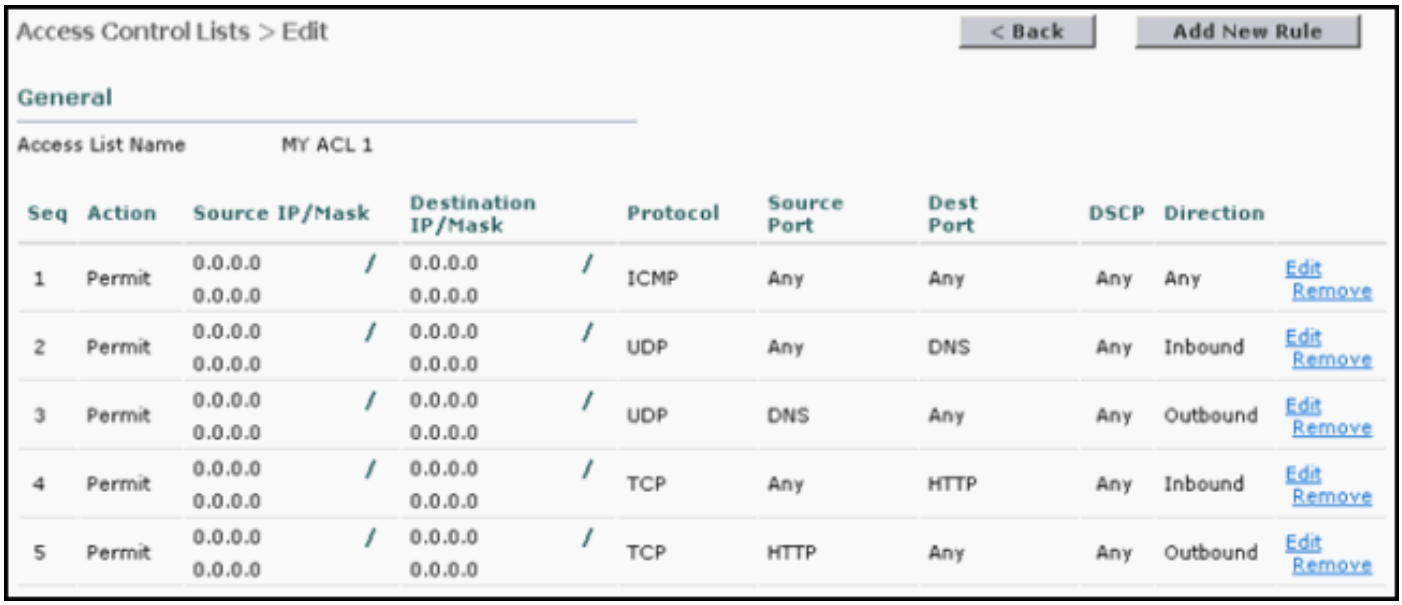
```
Seq  Direction  Source IP/Mask   Dest IP/Mask     Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------  ---------------  --------  --------  ---------  ----  ------
```

```
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 può essere più restrittivo se si specifica la subnet su cui si trovano i client wireless anziché Any IP address nelle righe ACL DNS e HTTP.

Nota: le righe ACL DHCP non possono essere sottoposte a restrizioni per la subnet perché il client riceve inizialmente il proprio indirizzo IP tramite 0.0.0.0, quindi rinnova il proprio indirizzo IP tramite un indirizzo subnet.

Ecco l'aspetto dello stesso ACL nella GUI:



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name: MY ACL 1

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	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTP	Any	Inbound	Edit Remove
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	Edit Remove

Esempio di ACL con DHCP, PING, HTTP e SCCP

In questo esempio di configurazione, i telefoni IP 7920 sono in grado solo di:

- Ricevi un indirizzo DHCP (non può essere bloccato da ACL)
- Eseguire il ping e ricevere il ping (qualsiasi tipo di messaggio ICMP - non può essere limitato solo al ping)
- Consenti risoluzione DNS (in ingresso)
- Connessione telefonica IP a CallManager e viceversa (in qualsiasi direzione)
- Connessioni telefoniche IP al server TFTP (CallManager utilizza una porta dinamica dopo la connessione TFTP iniziale alla porta UDP 69) (in uscita)
- Consenti comunicazione tra telefono IP e telefono IP 7920 (in qualsiasi direzione)
- Non consentire elenco telefonico Web o elenco telefonico IP (in uscita). L'operazione viene eseguita tramite una riga implicita "deny any any" ACL alla fine dell'ACL.

Ciò consentirà la comunicazione vocale tra i telefoni IP e le normali operazioni di avvio tra il telefono IP e CallManager.

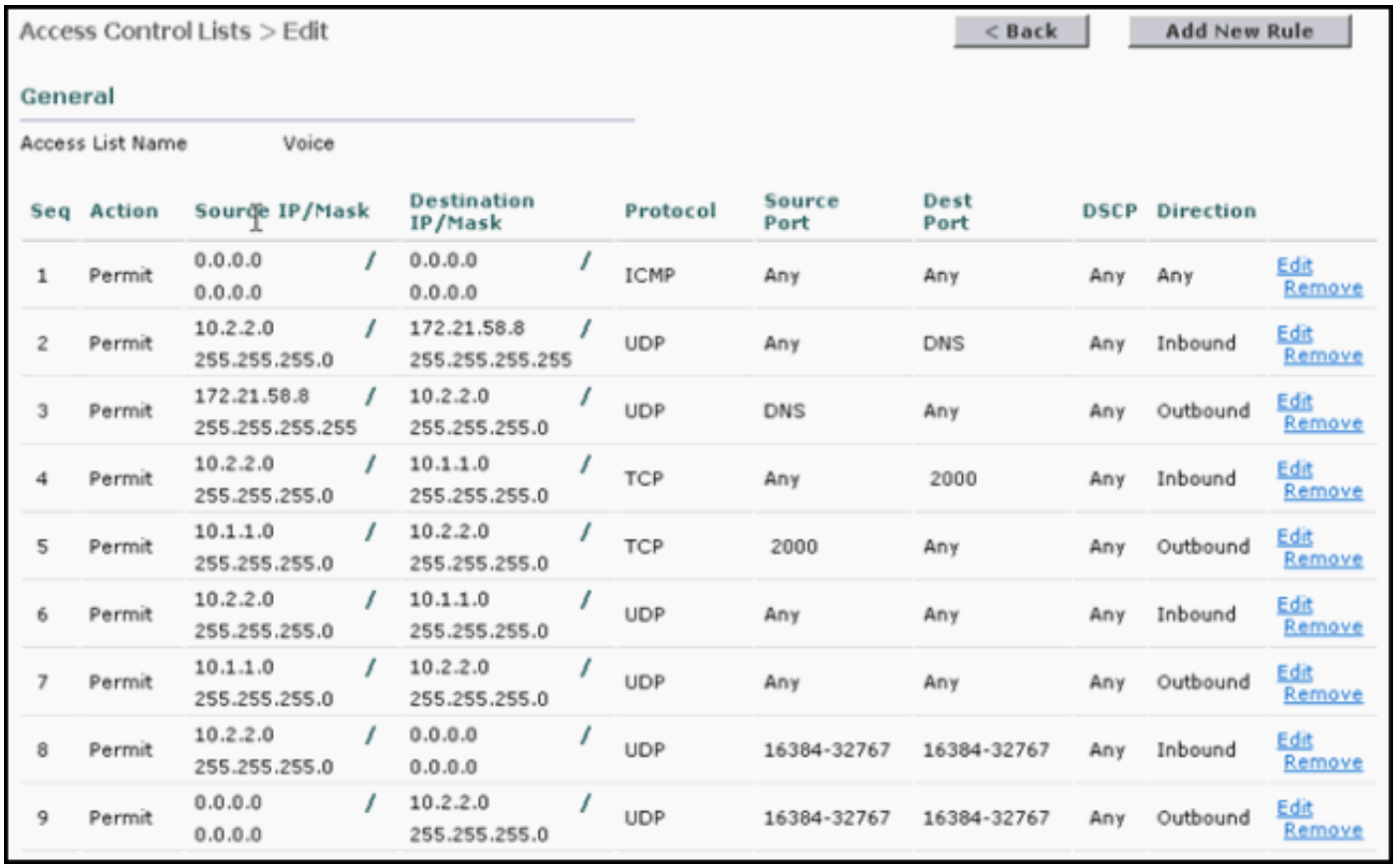
Per configurare questi requisiti di sicurezza, l'ACL deve avere righe che consentano:

- Qualsiasi messaggio ICMP (non può essere limitato solo al ping) (qualsiasi direzione)
- Telefono IP al server DNS (porta UDP 53) (in entrata)
- Server DNS su telefoni IP (porta UDP 53) (in uscita)
- Porte TCP per telefono IP sulla porta TCP 2000 di CallManager (porta predefinita) (in entrata)
- Porta TCP 2000 da CallManager ai telefoni IP (in uscita)
- Porta UDP dal telefono IP al server TFTP. Questa operazione non può essere limitata alla porta TFTP standard (69) perché CallManager utilizza una porta dinamica dopo la richiesta di connessione iniziale per il trasferimento dei dati.
- Porta UDP per traffico audio RTP tra telefoni IP (porte UDP 16384-32767) (tutte le direzioni)

Nell'esempio, la subnet del telefono IP 7920 è 10.2.2.0/24 e la subnet di CallManager è 10.1.1.0/24. Il server DNS è 172.21.58.8. Di seguito viene riportato l'output del comando 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
```

Ecco l'aspetto dell'interfaccia utente:



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

Appendice: porte per telefoni IP 7920

Queste sono le descrizioni riepilogative delle porte usate dal telefono IP 7920 per comunicare con Cisco CallManager (CCM) e altri telefoni IP:

- Phone to CCM [TFTP] (porta UDP 69 inizialmente modificata in porta dinamica [Ephemeral] per il trasferimento dati) - Protocollo TFTP (Trivial File Transfer Protocol) utilizzato per scaricare il firmware e i file di configurazione.
- Phone to CCM [Web Services, Directory] (porta TCP 80): URL telefono per applicazioni XML, autenticazione, directory, servizi, ecc. Queste porte sono configurabili per servizio.
- Phone to CCM [Voice Signaling] (porta TCP 2000) - Protocollo SCCP (Skinny Client Control Protocol). Questa porta è configurabile.
- Phone to CCM [Secure Voice Signaling] (porta TCP 2443) - Protocollo SCCPS (Secure Skinny Client Control Protocol)
- Phone to CAPF [Certificates] (porta TCP 3804) - Porta di ascolto CAPF (Certification Authority Proxy Function) per il rilascio di certificati importanti localmente (LSC) ai telefoni IP.
- Voice Bearer da/verso il telefono [telefonate] (porte UDP 16384 - 32768)—Real-Time Protocol (RTP), Secure Real Time Protocol (SRTP).

  Nota: CCM utilizza solo le porte UDP 24576-32768, ma altri dispositivi possono utilizzare l'intero intervallo.

- IP Phone to DNS Server [DNS] (porta UDP 53): i telefoni utilizzano il DNS per risolvere i nomi host dei server TFTP, dei CallManager e dei nomi host dei server Web quando il sistema è configurato per utilizzare nomi anziché indirizzi IP.
- IP Phone su server DHCP [DHCP] (porta UDP 67 [client] e 68 [server]): il telefono utilizza DHCP per recuperare un indirizzo IP se non è configurato staticamente.

Le porte con cui CallManager 5.0 comunica possono essere individuate in Cisco Unified CallManager 5.0 TCP e UDP Port Usage. Dispone inoltre delle porte specifiche utilizzate per comunicare con il telefono IP 7920.

Le porte con cui CallManager 4.1 comunica possono essere usate all'indirizzo Cisco Unified CallManager 4.1 TCP e UDP Port Usage. Dispone inoltre delle porte specifiche utilizzate per comunicare con il telefono IP 7920.

Informazioni correlate

- Esempio di configurazione di ACL sui Wireless LAN Controller
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).