ACL's op WLC's - regels, beperkingen en voorbeelden

Inhoud

Inleiding

Dit document biedt informatie over toegangscontrolelijsten (ACL's) op draadloze LAN-controllers (WLC's). In dit document worden de huidige beperkingen en regels toegelicht en worden relevante voorbeelden gegeven. Dit document is niet bedoeld als vervanging voor ACL's in het configuratievoorbeeld van een draadloze LAN-controller, maar als aanvulling op de informatie.

Opmerking: voor Layer 2 ACL's of extra flexibiliteit in Layer 3 ACL-regels raadt Cisco aan om ACL's te configureren op de eerste hoprouter die is aangesloten op de controller.

De meest voorkomende fout treedt op wanneer het protocolveld is ingesteld op IP (protocol=4) in een ACL-lijn met de bedoeling IP-pakketten toe te staan of te ontkennen. Omdat dit veld feitelijk selecteert wat er in het IP-pakket is ingesloten, zoals TCP, User Datagram Protocol (UDP) en Internet Control Message Protocol (ICMP), wordt het vertaald in blokkerende of toegestane IP-in-IP-pakketten. Tenzij u mobiele IP-pakketten wilt blokkeren, mag IP in geen enkele ACL-lijn worden geselecteerd. Cisco bug-id CSC22975 (alleen geregistreerde klanten) wijzigt IP in IP-in-IP.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Kennis van hoe u het WLC en Lichtgewicht access point (LAP) kunt configureren voor basisbediening
- Basiskennis van Lichtgewicht access point protocol (LWAP) en draadloze beveiligingsmethoden

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Begrijp ACL's op een WLC

ACL's bestaan uit een of meer ACL-lijnen gevolgd door een impliciete "ontkennen" aan het einde van de ACL. Elke regel bevat de volgende velden:

- Volgnummer
- Richting
- IP-bronadres en -masker
- IP-adres en -masker voor bestemming
- Protocol
- SRC-poort
- Dest Port
- DSCP
- Actie

Dit document beschrijft elk van deze velden:

- **Volgnummer**: geeft de volgorde aan waarin ACL-lijnen tegen het pakket worden verwerkt. Het pakket wordt tegen ACL verwerkt tot het de eerste ACL lijn aanpast. Het staat u ook toe om ACL-lijnen overal in de ACL in te voegen, zelfs nadat de ACL is gemaakt. Als u bijvoorbeeld een ACL-lijn met een volgnummer 1 hebt, kunt u vooraan een nieuwe ACL-lijn invoegen als dit gebeurt door een volgnummer 1 in de nieuwe ACL-lijn in te voegen. Hierdoor wordt de huidige regel automatisch omlaag verplaatst in de ACL.
- **Richting**—Hier wordt de controller verteld in welke richting de ACL-lijn moet worden uitgevoerd. Er zijn 3 richtingen: Inbound, Outbound, en Any. Deze aanwijzingen zijn afkomstig van een positie ten opzichte van de WLC en niet van de draadloze client.Inkomende IP-pakketten die afkomstig zijn van de draadloze client worden geïnspecteerd om te zien of ze overeenkomen met de ACL-lijn.Uitgaand-IP-pakketten die voor de draadloze client zijn bestemd, worden geïnspecteerd om te zien of ze overeenkomen met de ACL-lijn.Any-IP-pakketten die afkomstig zijn van de draadloze client en bestemd zijn voor de draadloze client, worden geïnspecteerd om te zien of ze overeenkomen met de ACL-lijn. De ACL-lijn wordt toegepast op zowel inkomende als uitgaande richtingen.**Opmerking:** het enige adres en masker dat moet worden gebruikt als u Any voor de richting selecteert, is 0.0.0.0/0.0.0.0 (Any). U moet geen specifieke host of subnet met de "Any"-richting specificeren omdat er een

nieuwe regel nodig zou zijn met de adressen of subnetten die worden geruild om ruimte te maken voor terugkeerverkeer.De enige richting zou slechts in specifieke situaties moeten worden gebruikt waar u een specifiek IP protocol of een haven in beide richtingen wilt blokkeren of toestaan, die naar de draadloze cliënten (Uitgaand) gaan en die van de draadloze cliënten (Inkomend) komen.Wanneer u IP-adressen of subnetten specificeert, moet u de richting specificeren als Inkomend of Uitgaand en een tweede nieuwe ACL-lijn maken voor retourverkeer in de tegenovergestelde richting. Als een ACL wordt toegepast op een interface en niet specifiek terugkeerverkeer door toestaat, wordt het terugkeerverkeer ontkend door impliciet "ontkent om het even welk"aan het eind van de ACL lijst.

- **Source IP Address and Mask**-definieert de bron IP-adressen van één host naar meerdere subnetten, die afhankelijk zijn van het masker. Het masker wordt gebruikt in combinatie met een IP-adres om te bepalen welke bits in een IP-adres moeten worden genegeerd wanneer dat IP-adres wordt vergeleken met het IP-adres in het pakket.**Opmerking:** maskers in een WLC ACL zijn niet vergelijkbaar met de jokerteken- of omgekeerde maskers die in Cisco IOS® ACL's worden gebruikt. In controlemechanisme ACLs, 255 middelen passen het octet in het IP adres precies aan, terwijl 0 een vervanging is. Het adres en het masker worden beetje bij beetje gecombineerd.Een maskerbit 1 betekent controle van de bijbehorende bitwaarde. De specificatie van 255 in het masker geeft aan dat het octet in het IP-adres van het pakket dat wordt geïnspecteerd, exact moet overeenkomen met het corresponderende octet in het ACL-adres.Een maskerbit 0 betekent niet controleren (negeren) die corresponderende bitwaarde. De specificatie van 0 in het masker geeft aan dat het octet in het IP-adres van het pakket dat wordt geïnspecteerd, wordt genegeerd.0.0.0.0/0.0.0.0 staat gelijk aan "Any" IP-adres (0.0.0.0 als adres en 0.0.0.0 als masker).
- **IP-adres en masker van bestemming**: hiervoor gelden dezelfde maskerregels als voor het IP-adres en het masker van de bron.
- **Protocol**—Specificeert het protocolveld in de IP-pakketheader. Sommige protocolnummers worden vertaald voor het gemak van de klant en worden gedefinieerd in het keuzemenu. De verschillende waarden zijn:Om het even welk (alle protocolnummers worden aangepast)TCP (IP-protocol 6)UDP (IP-protocol 17)ICMP (IP-protocol 1)ESP (IP-protocol 50)AH (IP-protocol 51)GRE (IP-protocol 47)IP (IP-protocol 4 IP-in-IP [CSCsh22975])Ethernet over IP (IP-protocol 97)OSPF (IP-protocol 89)Overige (specificeren)De Any-waarde komt overeen met elk protocol in de IP-header van het pakket. Dit wordt gebruikt om IP-pakketten volledig te blokkeren of toe te staan naar/van specifieke subnetten. Selecteer IP om IP-in-IP pakketten aan te passen. De gemeenschappelijke selecties zijn UDP en TCP die voor het plaatsen van specifieke bron en bestemmingshavens voorzien. Als u Overige selecteert, kunt u een van de IP-pakketprotocolnummers opgeven die worden gedefinieerd door IANA .
- **SRC-poort**: u kunt alleen opgeven voor het TCP- en UDP-protocol. 0-65535 is gelijk aan elke poort.
- **Dest Port**—Kan alleen worden opgegeven voor het TCP- en UDP-protocol. 0-65535 is gelijk aan elke poort.
- **Gedifferentieerde services code point (DSCP)**—Hiermee kunt u specifieke DSCP-waarden opgeven die moeten worden aangepast in de IP-pakketheader. De keuzemogelijkheden in het keuzemenu zijn specifiek voor Alle. Als u specifiek configureert, geeft u de waarde in het DSCP-veld aan. Er kunnen bijvoorbeeld waarden van 0 tot 63 worden gebruikt.
- **Actie**—De 2 acties zijn ontkend of toegestaan. Ontken blokkeert het opgegeven pakket. Laat het pakket door:sturen.

ACL-regels en -beperkingen

Beperkingen van WLC-gebaseerde ACL's

Dit zijn de beperkingen van op WLC gebaseerde ACL's:

- U kunt niet zien welke ACL-lijn door een pakket is aangepast (raadpleeg Cisco bug-id CSC36574 (alleen geregistreerde klanten)).
- U kunt geen pakketten vastleggen die overeenkomen met een specifieke ACL-lijn (raadpleeg Cisco bug-id CSC36574 (alleen geregistreerde klanten)).
- IP-pakketten (elk pakket met een Ethernet-protocolveld gelijk aan IP [0x080]) zijn de enige pakketten die door de ACL zijn geïnspecteerd. Andere typen Ethernet-pakketten kunnen niet worden geblokkeerd door ACL's. ARP-pakketten (Ethernet Protocol 0x0806) kunnen bijvoorbeeld niet worden geblokkeerd of toegestaan door de ACL.
- Een controller kan maximaal 64 ACL's hebben geconfigureerd; elke ACL kan maximaal 64 lijnen hebben.
- ACL's hebben geen invloed op multicast- en broadcast-verkeer dat wordt doorgestuurd van of naar de access points (AP's) en draadloze clients (raadpleeg Cisco bug-id CSC65613 (alleen geregistreerde klanten)).
- Vóór WLC versie 4.0 worden ACL's op de Management Interface overgeslagen, zodat u geen invloed hebt op verkeer dat is bestemd voor de Management Interface. Na WLC versie 4.0 kunt u CPU-ACL's maken. Raadpleeg CPU ACL's configureren voor meer informatie over het configureren van dit type ACL.**Opmerking:** ACL's die op de beheerinterfaces en AP-Manager interfaces worden toegepast, worden genegeerd. ACL's op de WLC zijn ontworpen om verkeer tussen het draadloze en bekabelde netwerk te blokkeren, niet het bekabelde netwerk en de WLC. Daarom, als u APs in bepaalde subnets wilt verhinderen met WLC volledig te communiceren, moet u een toegangslijst op uw intermitterende switches of router toepassen. Dit zal verkeer LWAPP van die APs (VLANs) aan WLC blokkeren.
- ACL's zijn afhankelijk van de processor en kunnen van invloed zijn op de prestaties van de controller onder zware belasting.
- ACL's kunnen de toegang tot het virtuele IP-adres niet blokkeren (1.1.1.1). DHCP kan daarom niet worden geblokkeerd voor draadloze clients.
- ACL's hebben geen invloed op de servicepoort van de WLC.

Regels voor WLC-gebaseerde ACL's

Dit zijn de regels voor op WLC gebaseerde ACL's:

- U kunt alleen protocolnummers in de IP-kop (UDP, TCP, ICMP, enzovoort) in ACL-lijnen specificeren, omdat ACL's alleen beperkt zijn tot IP-pakketten. Als IP is geselecteerd, geeft dit aan dat u IP-in-IP-pakketten wilt toestaan of weigeren. Als om het even welk wordt geselecteerd, wijst dit erop dat u pakketten met om het even welk IP protocol wilt toestaan of ontkennen.
- Als u om het even welk voor de richting selecteert, zouden de bron en de bestemming om het even welk (0.0.0.0/0.0.0.0) moeten zijn.
- Als het IP-adres van de bron of van de bestemming niet Any is, moet de richting van het filter worden opgegeven. Ook moet er een omgekeerde verklaring (met het IP-adres van de

bron/de poort en het IP-adres van de bestemming/de poort die is geruild) in de tegenovergestelde richting worden aangemaakt voor retourverkeer.
- Er is impliciet "ontken om het even welk"aan het eind van ACL. Als een pakket geen lijnen in ACL aanpast, wordt het gelaten vallen door het controlemechanisme.

Configuraties

ACL-voorbeeld met DHCP, PING, HTTP en DNS

In dit configuratievoorbeeld kunnen clients alleen:

- Ontvang een DHCP-adres (DHCP kan niet worden geblokkeerd door een ACL)
- Pingen en pingen (elk ICMP-berichttype - kan niet worden beperkt tot alleen pingen)
- Maak HTTP-verbindingen (uitgaand)
- Domain Name System (DNS) resolutie (uitgaand)

Om deze beveiligingsvereisten te kunnen configureren, moet de ACL lijnen hebben om toe te staan:

- Om het even welk ICMP- bericht in één van beide richting (kan niet worden beperkt om slechts te pingen)
- Elke UDP-poort naar DNS-inkomende poort
- DNS naar elke UDP-poort uitgaand (retourverkeer)
- Elke TCP-poort naar HTTP inbound
- HTTP naar elke TCP-poort uitgaand (retourverkeer)

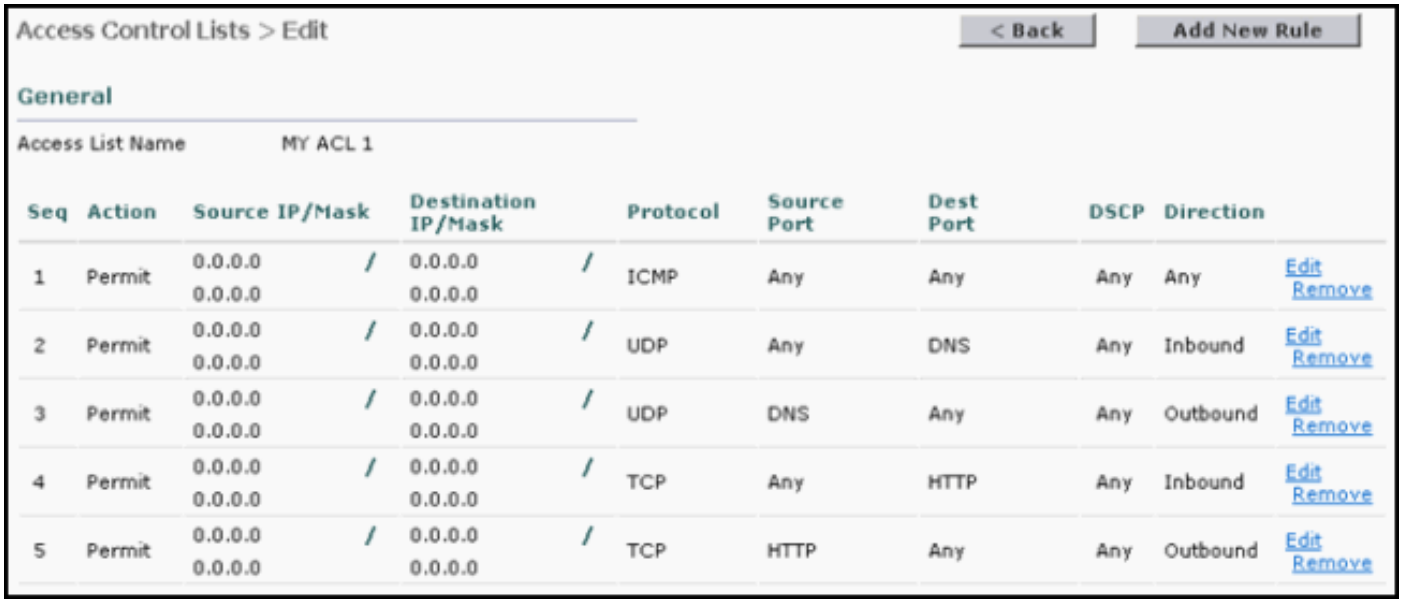
Dit is hoe ACL eruit ziet in de **gedetailleerde "MY ACL 1"-show** (citaten zijn alleen nodig als de ACL-naam meer dan 1 woord is), opdrachtoutput:

```
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
```

De ACL kan beperkender zijn als u het subnet specificeert waarop de draadloze clients zijn ingeschakeld in plaats van een IP-adres in de DNS- en HTTP ACL-lijnen.

Opmerking: de DHCP ACL-lijnen kunnen niet worden beperkt als de client eerst zijn IP-adres ontvangt met 0.0.0.0, en vervolgens zijn IP-adres vernieuwt via een subnetadres.

Dit is hoe dezelfde ACL er in de GUI uitziet:



ACL-voorbeeld met DHCP, PING, HTTP en SCCP

In dit configuratievoorbeeld kunnen 7920 IP-telefoons alleen:

- Ontvang een DHCP-adres (kan niet worden geblokkeerd door ACL)
- Pingen en pingen (elk ICMP-berichttype - kan niet worden beperkt tot alleen pingen)
- Sta DNS-resolutie toe (inkomend)
- IP-telefoonverbinding met CallManager en vice versa (Any Direction)
- IP-telefoonverbindingen met TFTP-server (CallManager gebruikt dynamische poort na eerste TFTP-verbinding met UDP-poort 69) (uitgaand)
- Laat 7920 IP-telefoon toe aan IP-telefooncommunicatie (elke richting)
- Schakel het web of de telefoonmap van IP-telefoon (uitgaand) uit. Dit gebeurt via een impliciete "ontken elke" ACL-lijn aan het einde van de ACL.Dit zal spraakcommunicatie tussen IP-telefoons en normale opstartbewerkingen tussen de IP-telefoon en CallManager mogelijk maken.

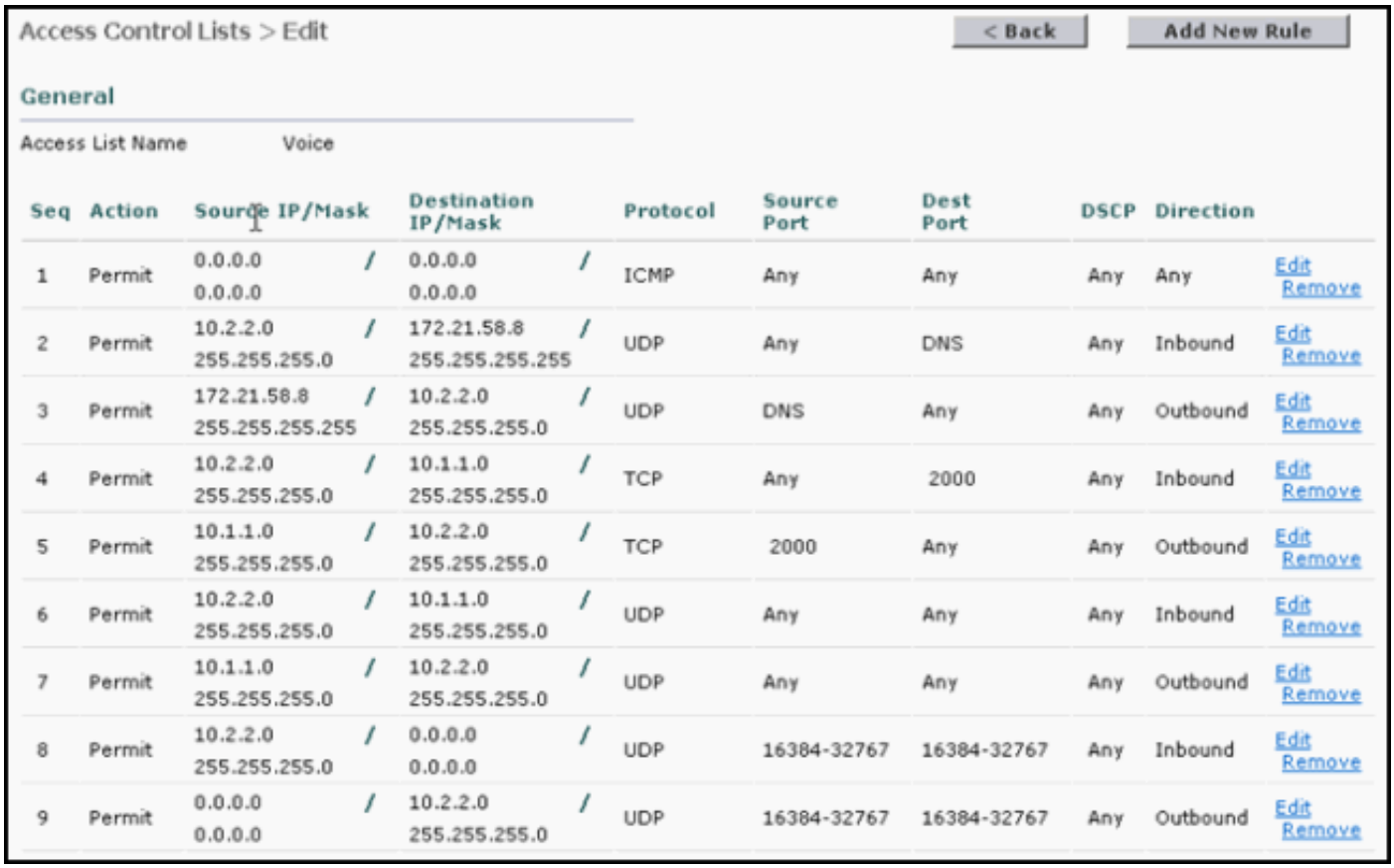
Om deze beveiligingsvereisten te kunnen configureren, moet de ACL lijnen hebben om toe te staan:

- Om het even welk ICMP- bericht (kan niet worden beperkt om slechts te pingen) (Om het even welke richting)
- IP-telefoon naar de DNS-server (UDP-poort 53) (inkomend)
- De DNS-server naar IP-telefoons (UDP-poort 53) (uitgaand)
- IP-telefoon TCP-poorten naar de CallManager TCP-poort 2000 (standaardpoort) (inkomende)
- TCP-poort 2000 van CallManager naar de IP-telefoons (uitgaand)
- UDP-poort van de IP-telefoon naar de TFTP-server. Dit kan niet worden beperkt tot de standaard TFTP-poort (69) omdat CallManager een dynamische poort gebruikt na het eerste verbindingsverzoek voor gegevensoverdracht.
- UDP-poort voor audioverkeer RTP tussen IP-telefoons (UDP-poorten16384-32767) (elke richting)

In dit voorbeeld is het 7920 IP-telefoonsubnetje 10.2.2.0/24 en het CallManager-subnetnummer 10.1.1.0/24. De DNS-server is 172.21.58.8. Dit is de uitvoer van de **show acl detail Voice** opdracht:

```
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
```

Dit is hoe het eruit ziet in de GUI:



Bijlage: 7920 IP-telefoonpoorten

Dit zijn de korte beschrijvingen van de poorten die de 7920 IP-telefoon gebruikt om te communiceren met Cisco CallManager (CCM) en andere IP-telefoons:

- Phone to CCM [TFTP] (UDP-poort 69 verandert eerst in dynamische poort [Ephemeral] voor gegevensoverdracht)—Trivial File Transfer Protocol (TFTP) gebruikt om firmware en

configuratiebestanden te downloaden.
- Phone to CCM [Web Services, Directory] (TCP-poort 80)—Phone URL's voor XML-toepassingen, verificatie, directory's, services, etc. Deze poorten kunnen per service worden geconfigureerd.
- Bel naar CCM [Voice Signaling] (TCP-poort 2000)—Skinny Client Control Protocol (SCCP). Deze poort kan worden geconfigureerd.
- Phone naar CCM [Secure Voice Signaling] (TCP-poort 2443)—Secure Skinny Client Control Protocol (SCCP)
- Bel naar CAPF [Certificates] (TCP-poort 3804) — CAPF-luisterpoort (Certificate Authority Proxy Function) voor het afgeven van LSC's (Local Significant Certificates) aan IP-telefoons.
- Voice Bearer to/from Phone [Phone Call] (UDP-poorten 16384 - 32768)—Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP).**Opmerking:** CCM gebruikt alleen UDP-poorten 24576-32768, maar andere apparaten kunnen het volledige bereik gebruiken.
- IP-telefoon naar DNS-server [DNS] (UDP-poort 53)—De telefoons gebruiken DNS om de hostnaam van TFTP-servers, CallManagers en webserverhostnamen op te lossen wanneer het systeem is geconfigureerd om namen te gebruiken in plaats van IP-adressen.
- IP-telefoon naar DHCP-server [DHCP] (UDP-poort 67 [client] en 68 [server]) - De telefoon gebruikt DHCP om een IP-adres op te halen als dit niet statisch is geconfigureerd.

De poorten waarmee de 5.0 CallManager communiceert, zijn te vinden bij Cisco Unified CallManager 5.0 TCP- en UDP-poortgebruik. Het heeft ook de specifieke poorten die het gebruikt om te communiceren met de 7920 IP-telefoon.

De poorten waarmee de 4.1 CallManager communiceert, zijn te vinden bij Cisco Unified CallManager 4.1 TCP- en UDP-poortgebruik. Het heeft ook de specifieke poorten die het gebruikt om te communiceren met de 7920 IP-telefoon.

Gerelateerde informatie

- Configuratievoorbeeld van ACL's op wireless LAN-controllers
- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 4.0
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.