ACLs em WLCs - Regras, Limitações e Exemplos

Contents

Introduction

Este documento fornece informações sobre as lista de controle de acesso (ACL) nos Controllers de LAN Wireless (WLC). Este documento explica as limitações e regras atuais e dá exemplos relevantes. Este documento não se destina a substituir as ACLs no Exemplo de Configuração de Controlador de LAN Wireless, mas a fornecer informações suplementares.

Observação: para ACLs de Camada 2 ou flexibilidade adicional nas regras de ACL de Camada 3, a Cisco recomenda que você configure ACLs no roteador do primeiro salto conectado ao controlador.

O erro mais comum ocorre quando o campo do protocolo é definido como IP (protocol=4) em uma linha ACL com a intenção de permitir ou negar pacotes IP. Como esse campo realmente seleciona o que é encapsulado dentro do pacote IP, como TCP, UDP (User Datagram Protocol) e ICMP (Internet Control Message Protocol), ele se traduz no bloqueio ou na permissão de pacotes IP-em-IP. A menos que você queira bloquear pacotes IP móveis, o IP não deve ser selecionado em nenhuma linha ACL. O bug da Cisco ID CSCsh2975 (somente clientes registrados) altera o IP para IP-em-IP.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar o WLC e o Lightweight Access Point (LAP) para a operação básica
- Conhecimento básico do Lightweight Access Point Protocol (LWAPP) e dos métodos de segurança sem fio

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Entender ACLs em uma WLC

As ACLs são formadas por uma ou mais linhas ACL seguidas por um "deny any any" implícito no final da ACL. Cada linha tem estes campos:

- Número de seqüência
- Direção
- Máscara e endereço IP origem
- Endereço IP destino e máscara
- Protocolo
- Porta Src
- Porta Dest
- DSCP
- Ação

Este documento descreve cada um destes campos:

- **Número de sequência** — Indica a ordem em que as linhas ACL são processadas no pacote. O pacote é processado na ACL até que corresponda à primeira linha da ACL. Ele também permite inserir linhas ACL em qualquer lugar da ACL, mesmo depois que a ACL é criada. Por exemplo, se você tiver uma linha de ACL com um número de sequência 1, poderá inserir uma nova linha de ACL na frente se ela for inserida com um número de sequência 1 na nova linha de ACL. Isso move automaticamente a linha atual para baixo na ACL.
- **Direção** — Informa ao controlador em que direção aplicar a linha ACL. Há três direções: Inbound, Outbound e Any. Essas instruções são obtidas de uma posição relativa à WLC e não ao cliente sem fio.Entrada—Os pacotes IP originados no cliente sem fio são inspecionados para ver se correspondem à linha da ACL.Saída—Os pacotes IP destinados ao cliente sem fio são inspecionados para ver se correspondem à linha da ACL.Qualquer — Os pacotes IP originados no cliente sem fio e destinados ao cliente sem fio são inspecionados para ver se correspondem à linha da ACL. A linha da ACL é aplicada às direções de entrada e de saída.**Observação:** o único endereço e máscara que devem ser usados quando você seleciona Qualquer para a direção é 0.0.0.0/0.0.0.0 (Qualquer). Você não deve especificar um host ou sub-rede específica com a direção "Qualquer", pois uma

nova linha seria necessária com os endereços ou sub-redes trocados para permitir o tráfego de retorno.A opção Qualquer direção só deve ser usada em situações específicas em que você deseja bloquear ou permitir um protocolo IP específico ou uma porta em ambas as direções, indo para os clientes sem fio (Saída) e vindo dos clientes sem fio (Entrada).Ao especificar endereços IP ou sub-redes, você deve especificar a direção como Inbound ou Outbound e criar uma segunda nova linha ACL para tráfego de retorno na direção oposta. Se uma ACL for aplicada a uma interface e não permitir especificamente o tráfego de retorno de volta, o tráfego de retorno será negado pelo "deny any any" implícito no final da lista da ACL.

- **Endereço IP e Máscara de Origem** — Define os endereços IP de origem de um único host para várias sub-redes, o que depende da máscara. A máscara é usada em conjunto com um endereço IP para determinar quais bits em um endereço IP devem ser ignorados quando esse endereço IP é comparado com o endereço IP no pacote.**Observação:** as máscaras em uma ACL de WLC não são como as máscaras curinga ou inversa usadas nas ACLs do Cisco IOS®. Nas ACLs do controlador, 255 significa corresponder exatamente ao octeto no endereço IP, enquanto 0 é um curinga. O endereço e a máscara são combinados bit a bit.Um bit de máscara 1 significa verificar o valor de bit correspondente. A especificação de 255 na máscara indica que o octeto no endereço IP do pacote inspecionado deve corresponder exatamente ao octeto correspondente no endereço da ACL.Um bit de máscara 0 significa não verificar (ignorar) esse valor de bit correspondente. A especificação de 0 na máscara indica que o octeto no endereço IP do pacote inspecionado foi ignorado.0.0.0.0/0.0.0.0 é equivalente a "Qualquer" endereço IP (0.0.0.0 como o endereço e 0.0.0.0 como a máscara).
- **Endereço IP e máscara de destino** — seguem as mesmas regras de máscara que o endereço IP e a máscara de origem.
- **Protocolo** — Especifica o campo do protocolo no cabeçalho do pacote IP. Alguns dos números de protocolo são traduzidos para conveniência do cliente e são definidos no menu suspenso. Os diferentes valores são:Qualquer um (todos os números de protocolo correspondem)TCP (protocolo IP 6)UDP (protocolo IP 17)ICMP (protocolo IP 1)ESP (protocolo IP 50)AH (protocolo IP 51)GRE (protocolo IP 47)IP (IP protocol 4 IP-in-IP [CSCsh22975])Eth Over IP (protocolo IP 97)OSPF (protocolo IP 89)Outro (especificar)O valor Any corresponde a qualquer protocolo no cabeçalho IP do pacote. Isso é usado para bloquear completamente ou permitir pacotes IP de/para sub-redes específicas. Selecione IP para corresponder aos pacotes IP-em-IP. As seleções comuns são UDP e TCP, que fornecem a configuração de portas origem e destino específicas. Se você selecionar Outro, poderá especificar qualquer um dos números de protocolo de pacotes IP definidos pela IANA .
- **Porta Src** — Só pode ser especificado para o protocolo TCP e UDP. 0-65535 equivale a Qualquer porta.
- **Porta Dest** — Só pode ser especificada para os protocolos TCP e UDP. 0-65535 equivale a Qualquer porta.
- **Differentiated Services Code Point (DSCP)** — Permite especificar valores de DSCP específicos para correspondência no cabeçalho do pacote IP. As opções no menu suspenso são específico ou Qualquer. Se você configurar um valor específico, indique o valor no campo DSCP. Por exemplo, podem ser usados valores de 0 a 63.
- **Ação** — As duas ações são deny ou permit. A negação bloqueia o pacote especificado. Permit encaminha o pacote.

Regras e limitações da ACL

Limitações de ACLs baseadas em WLC

Estas são as limitações das ACLs baseadas em WLC:

- Você não pode ver qual linha da ACL foi correspondida por um pacote (consulte o bug da Cisco ID CSCse36574 (somente clientes registrados)).
- Você não pode registrar pacotes que correspondam a uma linha ACL específica (consulte o bug da Cisco ID CSCse36574 (somente clientes registrados)).
- Os pacotes IP (qualquer pacote com um campo de protocolo ethernet igual a IP [0x0800]) são os únicos pacotes inspecionados pela ACL. Outros tipos de pacotes ethernet não podem ser bloqueados pelas ACLs. Por exemplo, os pacotes ARP (Ethernet Protocol 0x0806) não podem ser bloqueados ou permitidos pela ACL.
- Um controlador pode ter até 64 ACLs configuradas; cada ACL pode ter até um máximo de 64 linhas.
- As ACLs não afetam o tráfego multicast e broadcast que é encaminhado de ou para os access points (APs) e clientes sem fio (consulte o bug da Cisco ID CSCse65613 (somente clientes registrados)).
- Antes da versão 4.0 da WLC, as ACLs eram ignoradas na interface de gerenciamento, portanto você não pode afetar o tráfego destinado à interface de gerenciamento. Após a versão 4.0 da WLC, você pode criar ACLs de CPU. Consulte Configurar ACLs da CPU para obter mais informações sobre como configurar esse tipo de ACL.**Observação:** as ACLs aplicadas às interfaces de gerenciamento e gerenciador de AP são ignoradas. As ACLs na WLC são projetadas para bloquear o tráfego entre a rede com e sem fio, não entre a rede com fio e a WLC. Portanto, se você quiser impedir que os APs em certas sub-redes se comuniquem totalmente com a WLC, será necessário aplicar uma lista de acesso em seus switches ou roteadores intermitentes. Isso bloqueará o tráfego LWAPP desses APs (VLANs) para a WLC.
- As ACLs dependem do processador e podem afetar o desempenho do controlador sob carga pesada.
- As ACLs não podem bloquear o acesso ao endereço IP virtual (1.1.1.1). Portanto, o DHCP não pode ser bloqueado para clientes sem fio.
- As ACLs não afetam a porta de serviço da WLC.

Regras para ACLs baseadas em WLC

Estas são as regras para ACLs baseadas em WLC:

- Você só pode especificar números de protocolo no cabeçalho IP (UDP, TCP, ICMP, etc.) em linhas ACL, porque as ACLs são restritas somente a pacotes IP. Se IP for selecionado, isso indica que você deseja permitir ou negar pacotes IP-em-IP. Se a opção Any (Qualquer) estiver selecionada, isso indica que você deseja permitir ou negar pacotes com qualquer protocolo IP.
- Se você selecionar Qualquer para a direção, a origem e o destino devem ser Qualquer (0.0.0.0/0.0.0.0).
- Se o endereço IP origem ou destino não for Qualquer, a direção do filtro deve ser especificada. Além disso, uma instrução inversa (com endereço IP/porta de origem e endereço IP/porta de destino trocados) na direção oposta deve ser criada para o tráfego de retorno.

- Há um "deny any any" implícito no final da ACL. Se um pacote não corresponder a nenhuma linha na ACL, ele será descartado pelo controlador.

Configurações

Exemplo de ACL com DHCP, PING, HTTP e DNS

Neste exemplo de configuração, os clientes só podem:

- Receber um endereço DHCP (o DHCP não pode ser bloqueado por uma ACL)
- Fazer ping e receber ping (qualquer tipo de mensagem ICMP - não pode ser restrito somente ao ping)
- Fazer conexões HTTP (saída)
- Resolução do Sistema de Nomes de Domínio (DNS) (saída)

Para configurar esses requisitos de segurança, a ACL deve ter linhas para permitir:

- Qualquer mensagem ICMP em qualquer direção (não pode ser restrita somente ao ping)
- Qualquer porta UDP para entrada DNS
- DNS para qualquer porta UDP de saída (tráfego de retorno)
- Qualquer porta TCP para entrada HTTP
- HTTP para qualquer porta TCP de saída (tráfego de retorno)

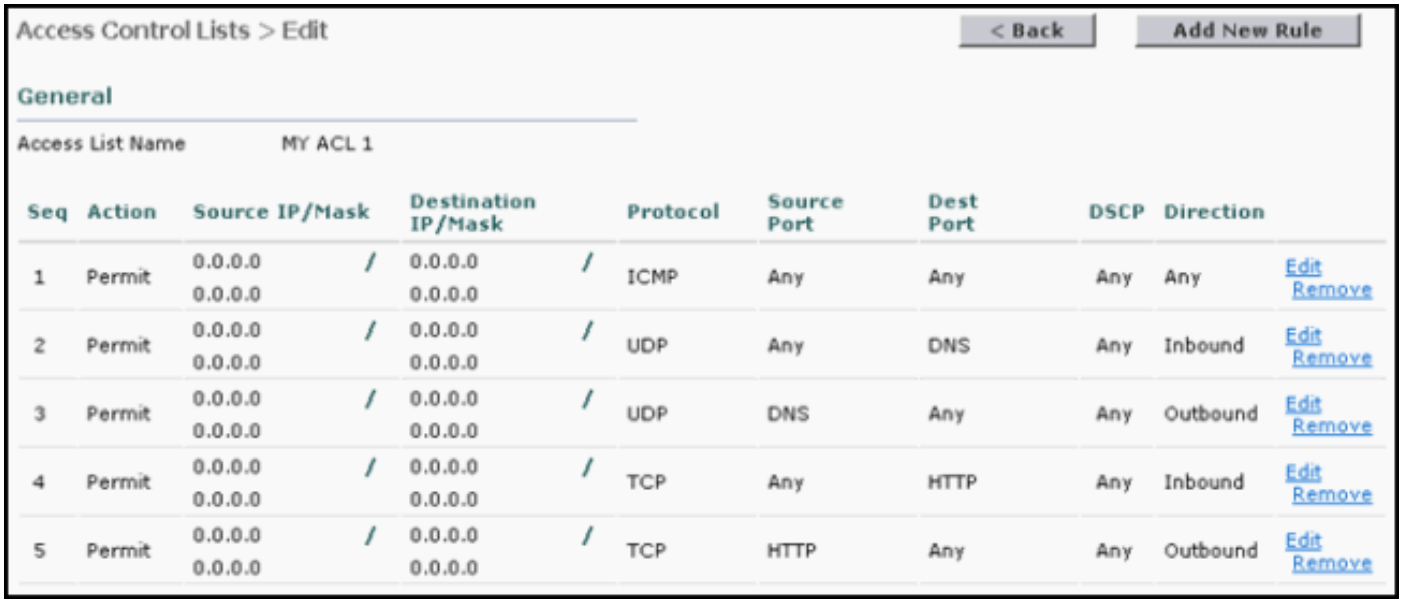
Esta é a aparência da ACL na saída do comando **show acl detailed "MY ACL 1"** (as aspas são necessárias somente se o nome da ACL for maior que 1 palavra):

```
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
```

A ACL pode ser mais restritiva se você especificar a sub-rede na qual os clientes sem fio estão em vez de qualquer endereço IP nas linhas DNS e HTTP ACL.

Observação: as linhas da ACL DHCP não podem ter a sub-rede restrita, pois o cliente recebe inicialmente seu endereço IP usando 0.0.0.0 e, em seguida, renova seu endereço IP por meio de um endereço de sub-rede.

Esta é a aparência da mesma ACL na GUI:



Exemplo de ACL com DHCP, PING, HTTP e SCCP

Neste exemplo de configuração, os telefones IP 7920 só podem:

- Receber um endereço DHCP (não pode ser bloqueado pela ACL)
- Fazer ping e receber ping (qualquer tipo de mensagem ICMP - não pode ser restrito somente ao ping)
- Permitir resolução DNS (Entrada)
- Conexão do telefone IP com o CallManager e vice-versa (Qualquer direção)
- Conexões do telefone IP com o servidor TFTP (o CallManager usa a porta dinâmica após a conexão TFTP inicial com a porta UDP 69) (Saída)
- Permitir comunicação de telefone IP 7920 para telefone IP (qualquer direção)
- Não permitir a Web do telefone IP ou o Phone Diretory (Outbound). Isso é feito por meio de uma linha de ACL "deny any any" implícita no final da ACL.Isso permitirá comunicações de voz entre telefones IP, bem como operações normais de inicialização entre o telefone IP e o CallManager.

Para configurar esses requisitos de segurança, a ACL deve ter linhas para permitir:

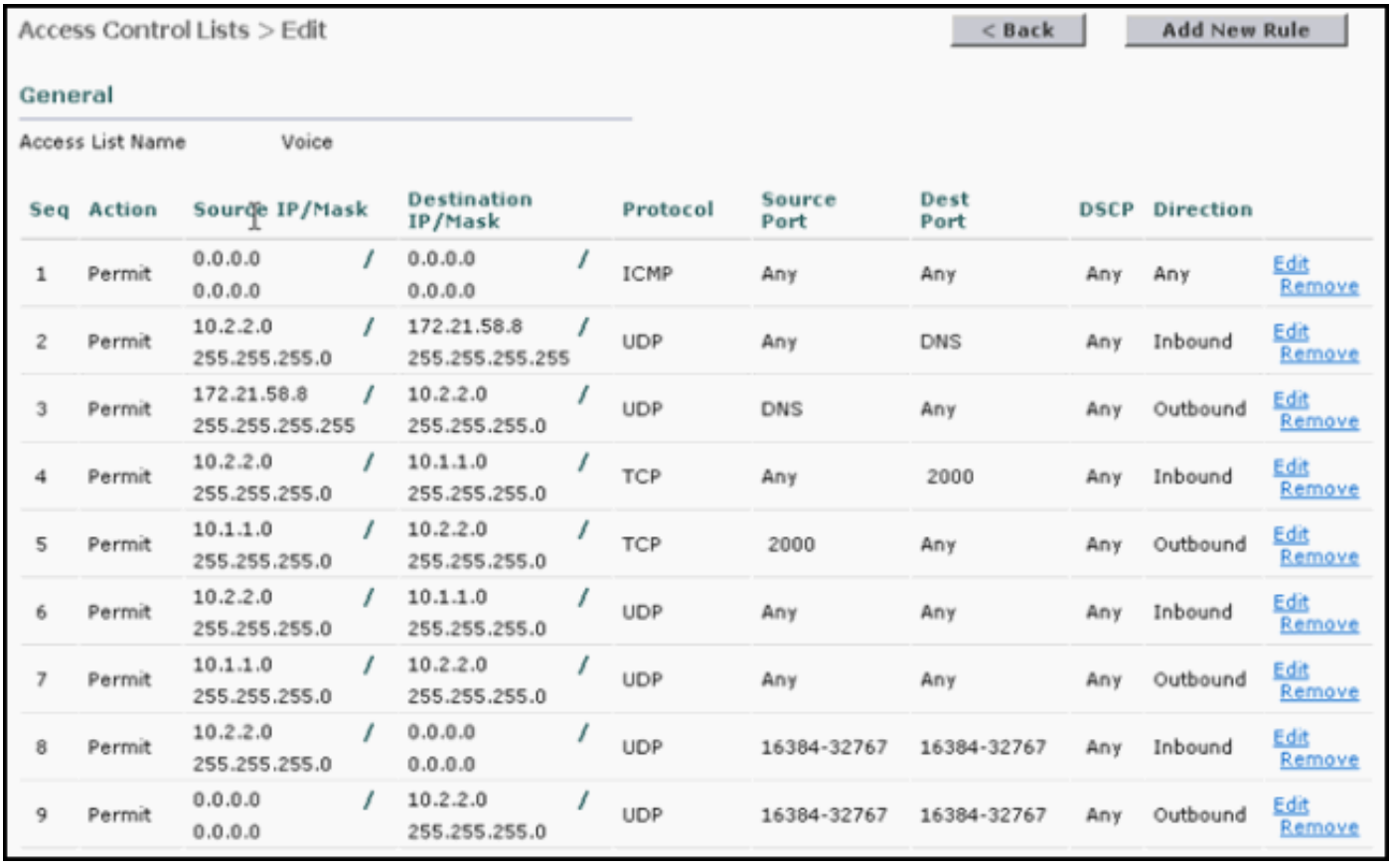
- Qualquer mensagem ICMP (não pode ser restrita somente ao ping) (Qualquer direção)
- Telefone IP para o servidor DNS (porta UDP 53) (entrada)
- O servidor DNS para telefones IP (porta UDP 53) (saída)
- Portas TCP do telefone IP para a porta TCP 2000 do CallManager (porta padrão) (entrada)
- Porta TCP 2000 do CallManager para os telefones IP (Saída)
- Porta UDP do telefone IP para o servidor TFTP. Isso não pode ser restrito à porta TFTP padrão (69) porque o CallManager usa uma porta dinâmica após a solicitação de conexão inicial para transferência de dados.
- Porta UDP para tráfego de áudio RTP entre telefones IP (portas UDP16384-32767) (Qualquer direção)

Neste exemplo, a sub-rede do telefone IP 7920 é 10.2.2.0/24 e a sub-rede do CallManager é 10.1.1.0/24. O servidor DNS é 172.21.58.8. Esta é a saída do comando **show acl detail Voice**:

```
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
```

Esta é a aparência da GUI:



Apêndice: Portas de telefone IP 7920

Estas são as descrições resumidas das portas que o telefone IP 7920 usa para se comunicar com o Cisco CallManager (CCM) e outros telefones IP:

- Telefone para CCM [TFTP] (a porta UDP 69 inicialmente é alterada para a porta dinâmica [Efêmero] para transferência de dados)—Protocolo de Transferência de Arquivos Trivial (TFTP - Trivial File Transfer Protocol) usado para baixar o firmware e os arquivos de configuração.

- Telefone para CCM [Serviços da Web, Diretório] (porta TCP 80)—URLs de telefone para aplicativos XML, autenticação, diretórios, serviços, etc. Essas portas são configuráveis por serviço.
- Telefone para CCM [sinalização de voz] (porta TCP 2000)—Skinny Client Control Protocol (SCCP). Essa porta é configurável.
- Telefone para CCM [Secure Voice Signaling] (porta TCP 2443)—Secure Skinny Client Control Protocol (SCCPS)
- Telefone para CAPF [Certificados] (porta TCP 3804)—Porta de escuta da Certificate Authority Proxy Function (CAPF) para emissão de LSCs (Locally Significant Certificates) para telefones IP.
- Portador de Voz para/do Telefone [Chamadas Telefônicas] (Portas UDP 16384 - 32768)—Protocolo em Tempo Real (RTP - Real-Time Protocol), Protocolo em Tempo Real Seguro (SRTP - Secure Real Time Protocol).**Observação: o** CCM usa apenas portas UDP 24576-32768, mas outros dispositivos podem usar o intervalo completo.
- Telefone IP para Servidor DNS [DNS] (porta UDP 53)—Os telefones usam DNS para resolver o nome de host de servidores TFTP, CallManagers e nomes de host de servidores web quando o sistema está configurado para usar nomes em vez de endereços IP.
- Telefone IP para servidor DHCP [DHCP] (porta UDP 67 [cliente] e 68 [servidor])—O telefone usa DHCP para recuperar um endereço IP se não estiver configurado estaticamente.

As portas que o CallManager 5.0 usa para se comunicar podem ser encontradas em Cisco Unified CallManager 5.0 TCP e UDP Port Usage. Ele também tem as portas específicas que usa para se comunicar com o telefone IP 7920.

As portas que o CallManager 4.1 usa para se comunicar podem ser encontradas em Cisco Unified CallManager 4.1 TCP e UDP Port Usage. Ele também tem as portas específicas que usa para se comunicar com o telefone IP 7920.

Informações Relacionadas

- Exemplo de configuração de ACLs nos Wireless LAN Controllers
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.