ACL no exemplo da configuração de controle do Wireless LAN

Índice

Introdução

Este documento explica como configurar o Access Control Lists (ACLs) no filtrar tráfego dos controladores do Wireless LAN (WLC) que incorpora e sae de um WLAN.

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar o WLC e o Access point de pouco peso (REGAÇO) para a operação básica
- Conhecimento básico de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2000 Series WLC que executa o firmware 4.0
- REGAÇO do Cisco 1000 Series

- Adaptador de cliente Wireless de Cisco 802.11a/b/g que executa o firmware 2.6
- Versão 2.6 do utilitário de desktop do Cisco Aironet (ADU)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

ACL em WLC

Os ACL no WLC são significados restringir ou permitir clientes Wireless aos serviços em seu WLAN.

Antes da versão de firmware 4.0 WLC, os ACL são contorneados na interface de gerenciamento, assim que você não pode afetar o tráfego destinado ao WLC a não ser impedir que os clientes Wireless controlem o controlador com o **Gerenciamento através da** opção **wireless**. Consequentemente, os ACL podem somente ser aplicados às interfaces dinâmica. Na versão de firmware 4.0 WLC, há o CPU ACL que pode filtrar tráfego destinado para a interface de gerenciamento. Um exemplo de como configurar CPU ACL é fornecido mais tarde neste documento.

Você pode definir até 64 ACL, cada um com até 64 regras (ou filtros). Cada regra tem os parâmetros que afetam sua ação. Quando um pacote combina todos os parâmetros para uma regra, a ação ajustada para essa regra está aplicada ao pacote. Você pode configurar ACL com o GUI ou o CLI.

Estes são algumas das regras que você precisa de compreender antes que você configure um ACL no WLC:

- Se a fonte *e o* destino são **alguma**, o sentido em que este ACL é aplicado pode ser **algum**.
- Se a fonte *ou o* destino não são **alguma**, a seguir o sentido do filtro deve ser especificado, e uma indicação inversa na direção oposta deve ser criada.
- A noção do WLC de entrada contra de partida é nonintuitive. É da perspectiva do WLC que enfrenta para o cliente Wireless, um pouco do que da perspectiva do cliente. Assim, a direção de entrada significa que um pacote que entre o WLC do cliente Wireless e da direção externa significa um pacote esse saídas do WLC para o cliente Wireless.
- Há um implícito nega no fim do ACL.

Considerações ao configurar ACL nos WLC

Os ALC nos WLC trabalham diferentemente do que no Roteadores. Estas são algumas coisas a recordar quando você configura ACL nos WLC:

- A maioria de erro comum é selecionar o IP quando você pretende negar ou permitir pacotes IP. Porque você seleciona o que é dentro do pacote IP, você termina acima a negação ou

permitir de pacotes do IP in IP.

- O controlador ACL não pode obstruir 1.1.1.1 (endereço IP de Um ou Mais Servidores Cisco ICM NT virtual), e daqui pacotes DHCP para clientes Wireless.
- O controlador ACL não pode obstruir o tráfego multicast recebido das redes ligadas com fio que é destinado aos clientes Wireless. O controlador ACL é processado para o tráfego multicast iniciado dos clientes Wireless, destinados às redes ligadas com fio ou aos outros clientes Wireless no mesmo controlador.
- Ao contrário de um roteador, o ACL controla o tráfego nos ambos sentidos quando aplicado a uma relação, mas não executa o firewall do stateful. Se você esquece abrir um furo no ACL para o tráfego de retorno, este causa um problema.
- O controlador ACL obstrui somente pacotes IP. Você não pode obstruir a camada 2 ACL ou mergulhar 3 pacotes que não são IP.
- O controlador ACL não usa máscaras inversas como o Roteadores. Aqui, 255 significam o fósforo esse octeto do endereço IP de Um ou Mais Servidores Cisco ICM NT exatamente.
- Os ACL no controlador são feitos no desempenho de encaminhamento do software e do impacto.

Note: Se você aplica um ACL a uma relação ou a um WLAN, a taxa de transferência wireless está degradada e pode conduzir à Perda potencial de pacotes. A fim melhorar a taxa de transferência, remover o ACL da relação ou do WLAN e mover o ACL para um dispositivo prendido vizinho.

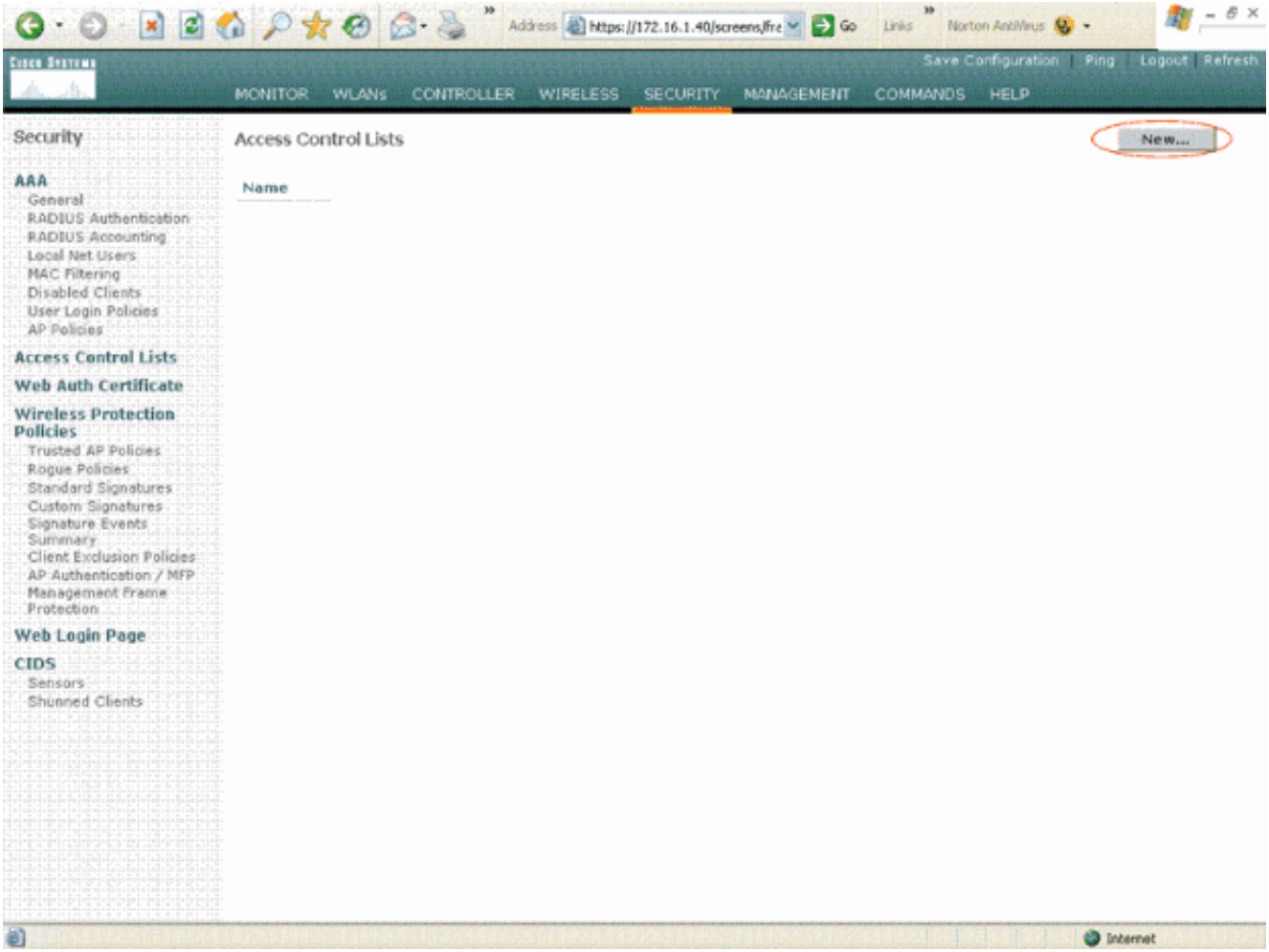
Configurar o ACL em WLC

Esta seção descreve como configurar um ACL no WLC. O objetivo é configurar um ACL que permita que os clientes do convidado alcancem estes serviços:

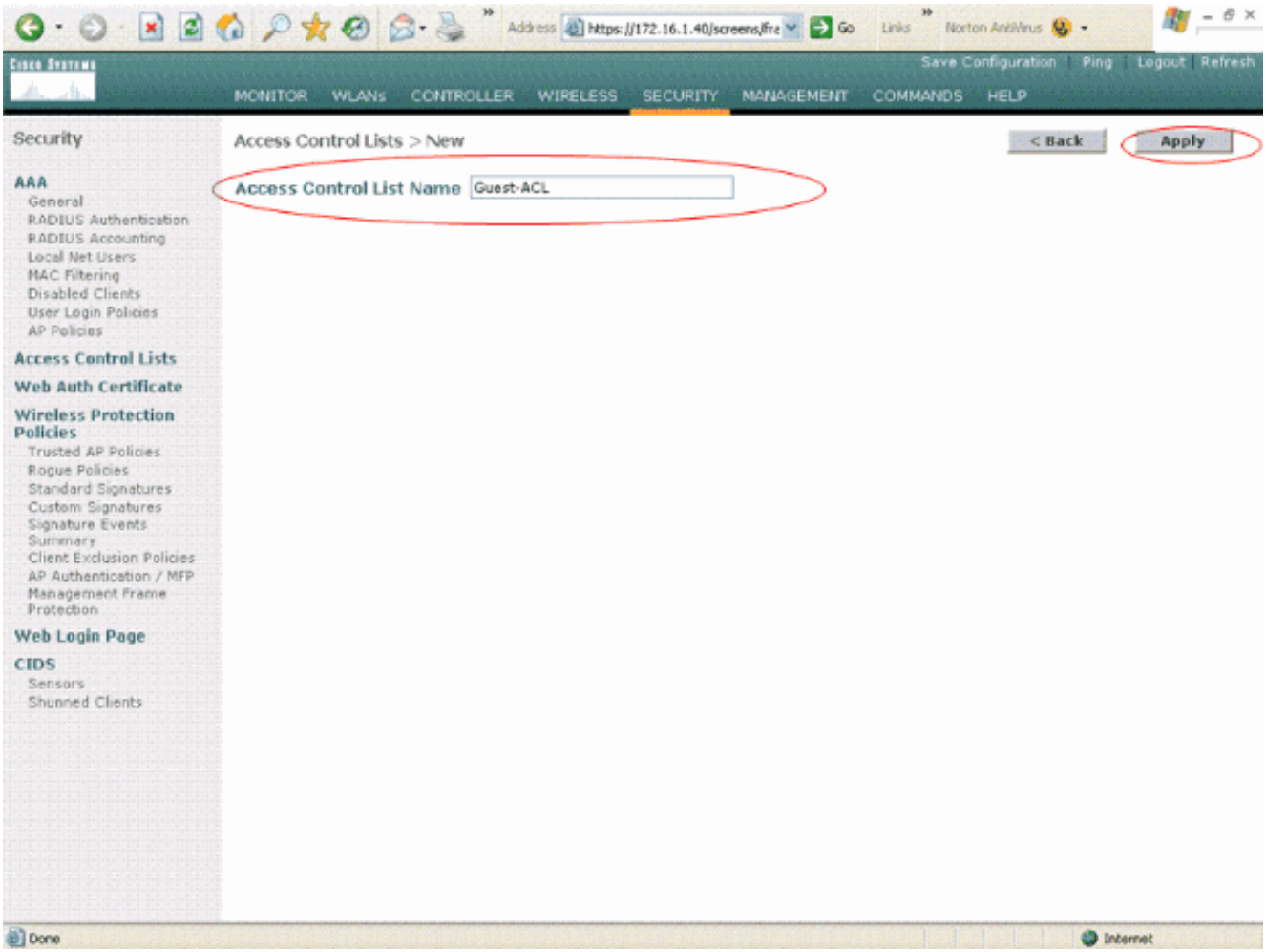
- Protocolo de configuração dinâmica host (DHCP) entre os clientes Wireless e o servidor DHCP
- Internet Control Message Protocol (ICMP) entre todos os dispositivos na rede
- Domain Name System (DNS) entre os clientes Wireless e o servidor DNS
- Telnet a uma sub-rede específica

Todos os outros serviços devem ser obstruídos para os clientes Wireless. Termine estas etapas a fim criar o ACL usando o WLC GUI:

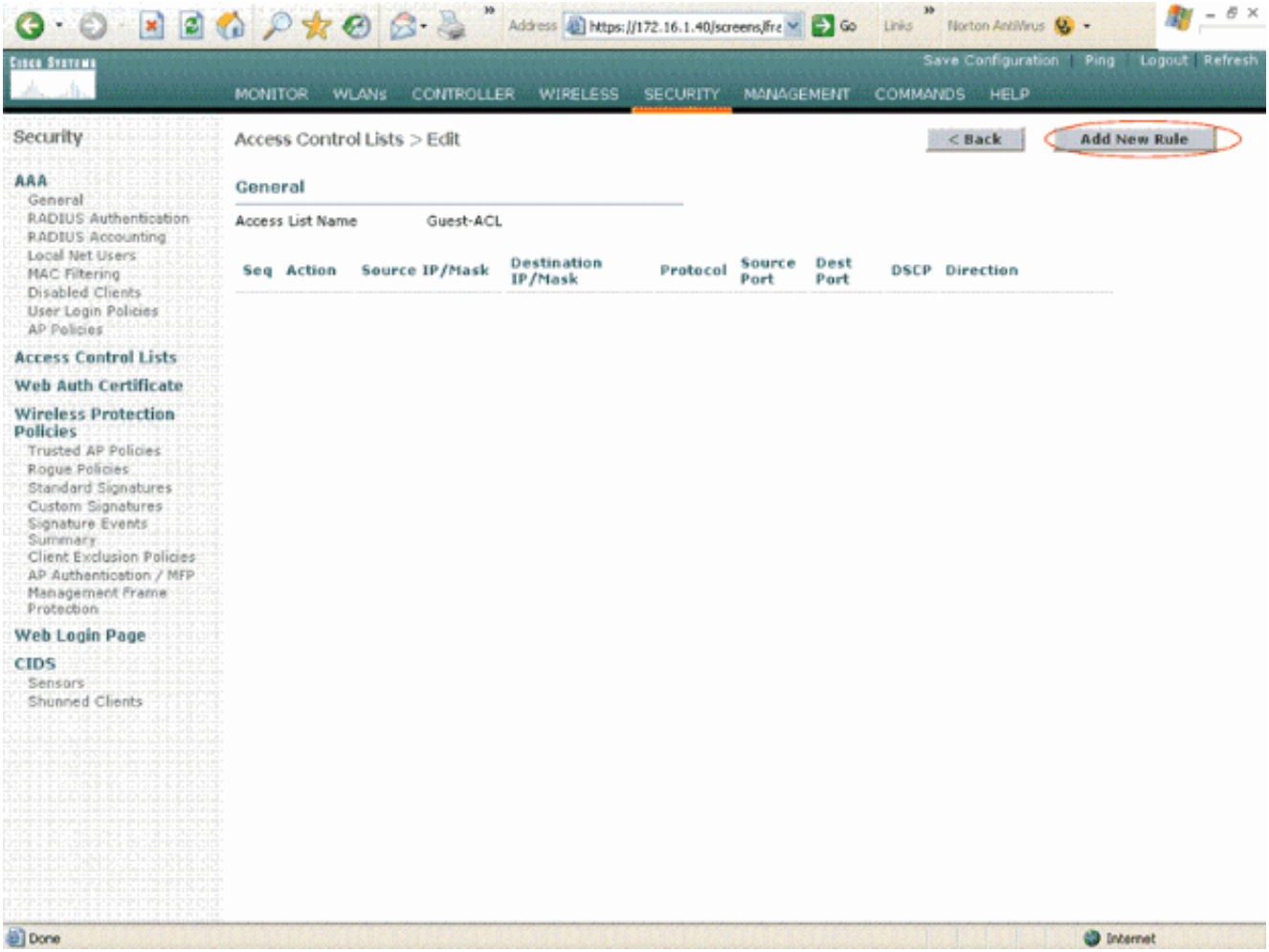
1. Vá ao WLC GUI e escolha a **Segurança > as listas de controle de acesso**.A página das listas de controle de acesso publica-se. Esta página alista os ACL que são configurados no WLC. Igualmente permite-o de editar ou remover alguns dos ACL. A fim criar um ACL novo, clique **novo**.



2. Dê entrada com o nome do ACL e do clique **aplicam-se**.Você pode incorporar até 32 caráteres alfanuméricos. Neste exemplo, o nome do ACL é Convidado-**ACL**. Uma vez que o ACL é criado, o clique **edita** a fim criar regras para o ACL.



3. Quando as listas de controle de acesso > editam a página publica-se, clique **adiciona a regra nova**.As listas de controle de acesso > ordenam > página nova aparecem.



4. Configurar as regras que permitem a um usuário convidado estes serviços:DHCP entre os clientes Wireless e o servidor DHCPICMP entre todos os dispositivos na redeDNS entre os clientes Wireless e o servidor DNSTelnet a uma sub-rede específica

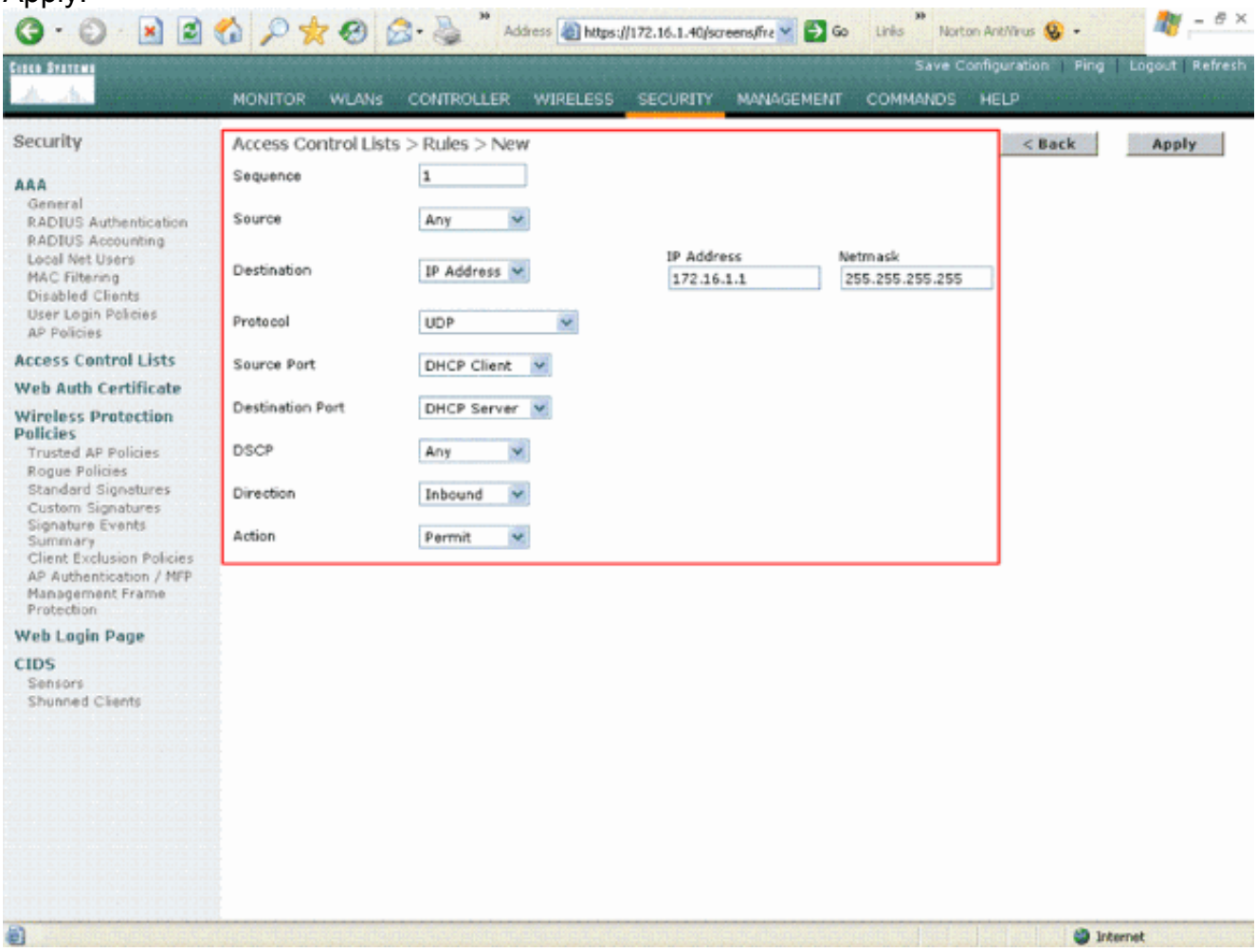
Configurar as regras que permitem serviços do usuário convidado

Esta seção mostra um exemplo para que como configure as regras para estes serviços:

- DHCP entre os clientes Wireless e o servidor DHCP
- ICMP entre todos os dispositivos na rede
- DNS entre os clientes Wireless e o servidor DNS
- Telnet a uma sub-rede específica

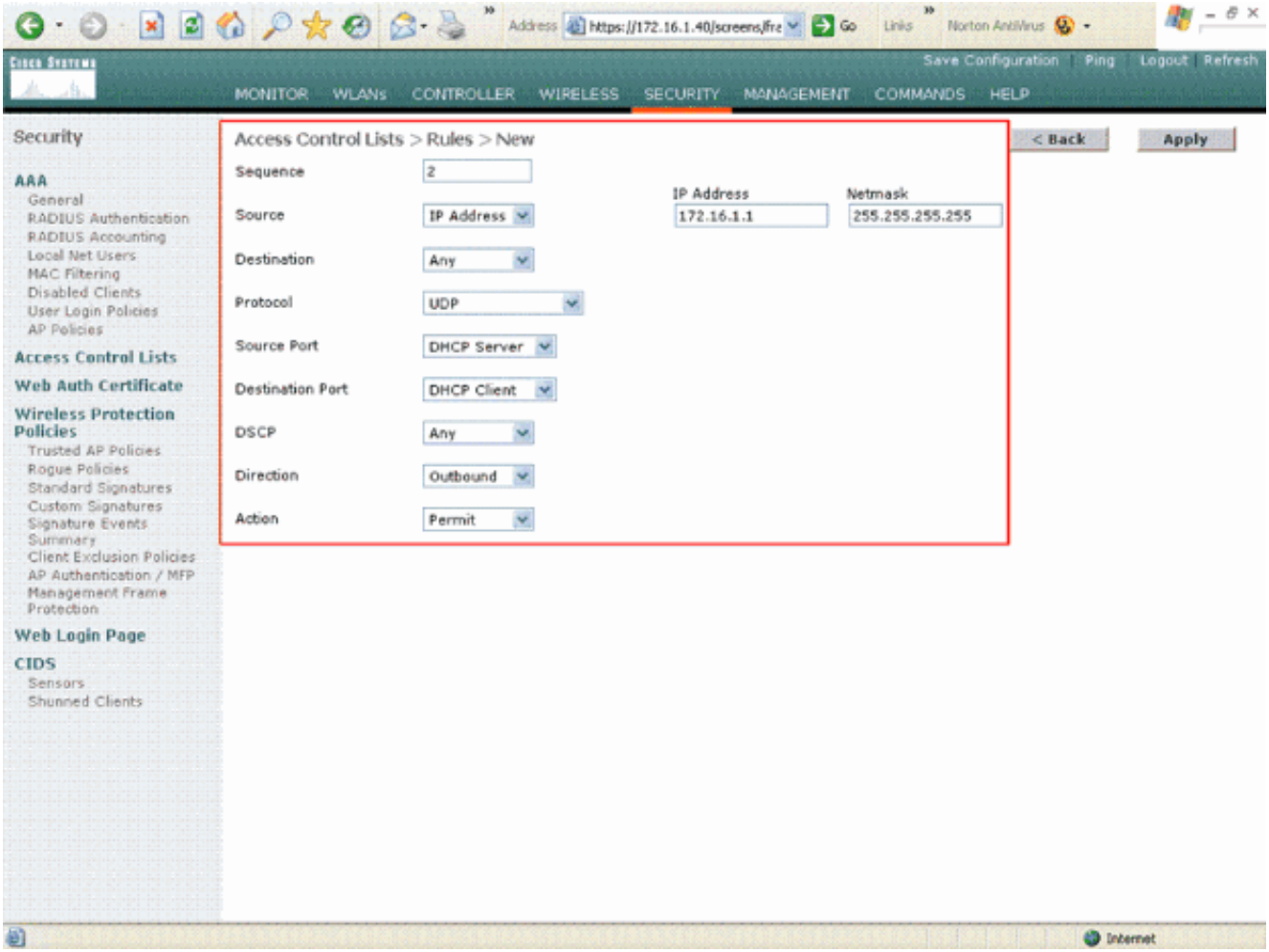
1. A fim definir a regra para o serviço DHCP, selecione a fonte e as escalas do IP de destino.Este exemplo usa **alguns** para a fonte que significa que o acesso está permitido a todo o cliente Wireless ao servidor DHCP. Neste exemplo, o server 172.16.1.1 atua como o DHCP e o servidor DNS. Assim, o endereço IP de destino é 172.16.1.1/255.255.255.255 (com uma máscara do host).Porque o DHCP é um protocolo baseado em UDP, **UDP** seleto do campo da gota-para baixo do protocolo. Se você escolheu o TCP ou o UDP na etapa precedente, dois parâmetros adicionais aparecem: Porta de origem e porta do destino. Especifique os detalhes da porta de origem e de destino. Para esta regra, a porta de origem é **DHCP Client** e a porta do destino é **servidor DHCP**.Escolha o sentido em que o ACL deve ser aplicada. Porque esta regra é do cliente ao server, os usos deste exemplo **de entrada**. Da caixa suspensa da ação, escolha a **licença** para fazer com que este ACL permita pacotes DHCP do cliente Wireless ao servidor DHCP. O valor padrão é nega. Clique em

Apply.

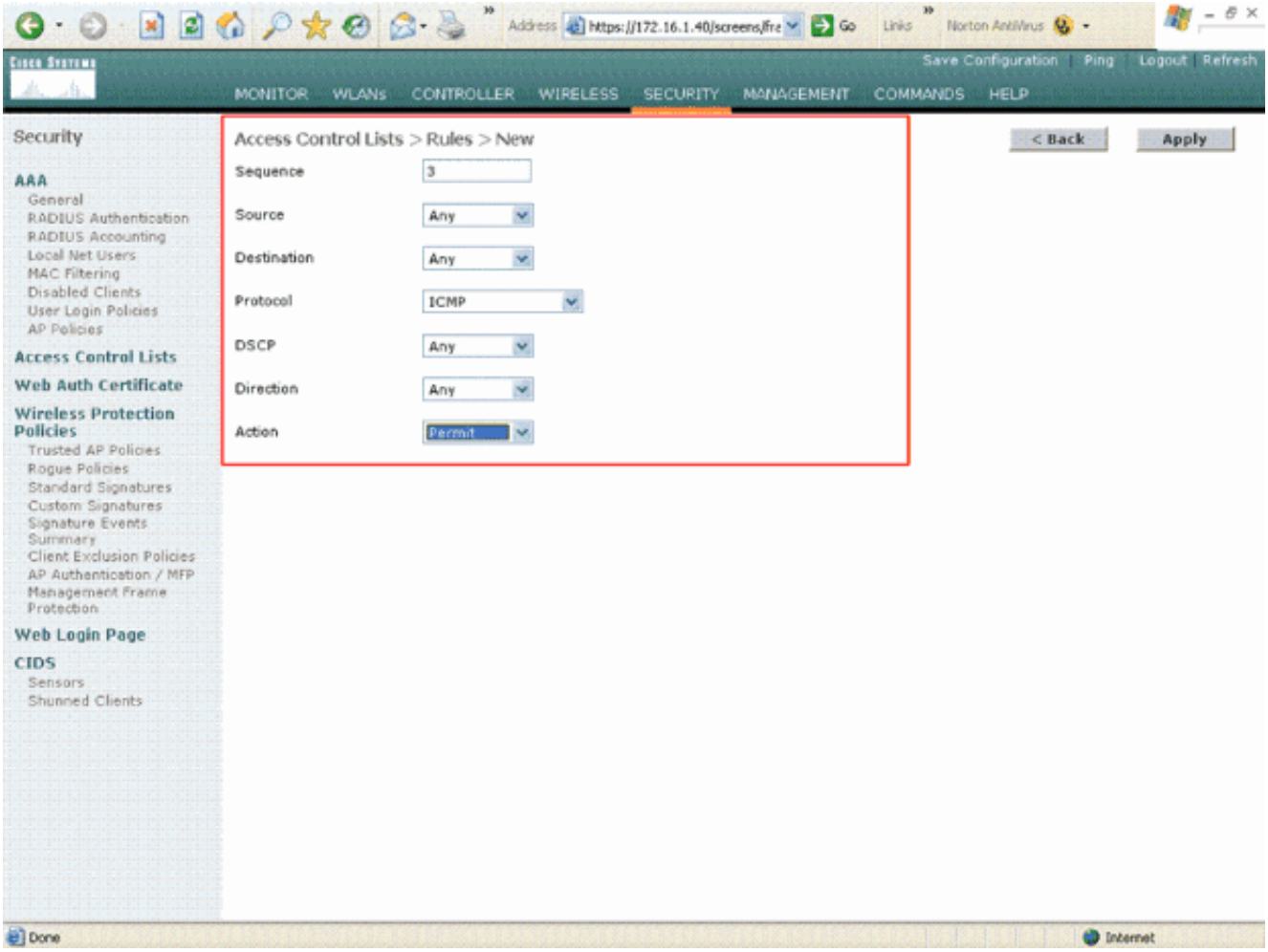


Se a fonte ou o destino não são **alguma**, a seguir uma indicação inversa na direção oposta deve ser criada.

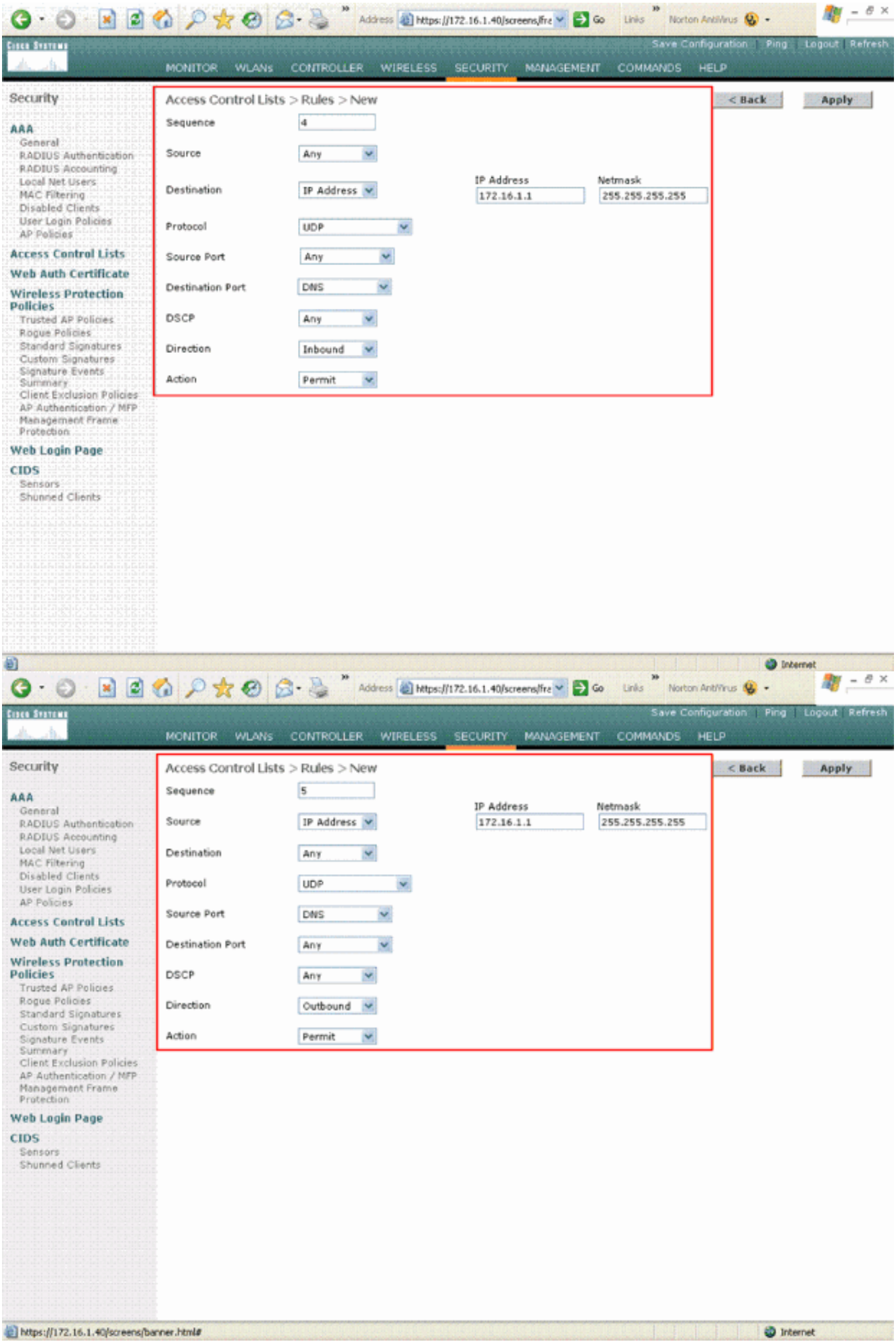
Exemplo:



2. A fim definir uma regra que permita pacotes ICMP entre todos os dispositivos, selecione **alguns** para a fonte e os campos de destino. Este é o valor padrão.Escolha o **ICMP do** campo da gota-para baixo do protocolo. Porque este exemplo usa **alguns** para a fonte e os campos de destino, você não tem que especificar o sentido. Pode ser deixado em seu valor padrão de **alguns**. Também, a indicação inversa na direção oposta não é exigida.Do menu suspenso da ação, escolha a **licença** a fim fazer com que este ACL permita pacotes DHCP do servidor DHCP ao cliente Wireless. Clique em
Apply.

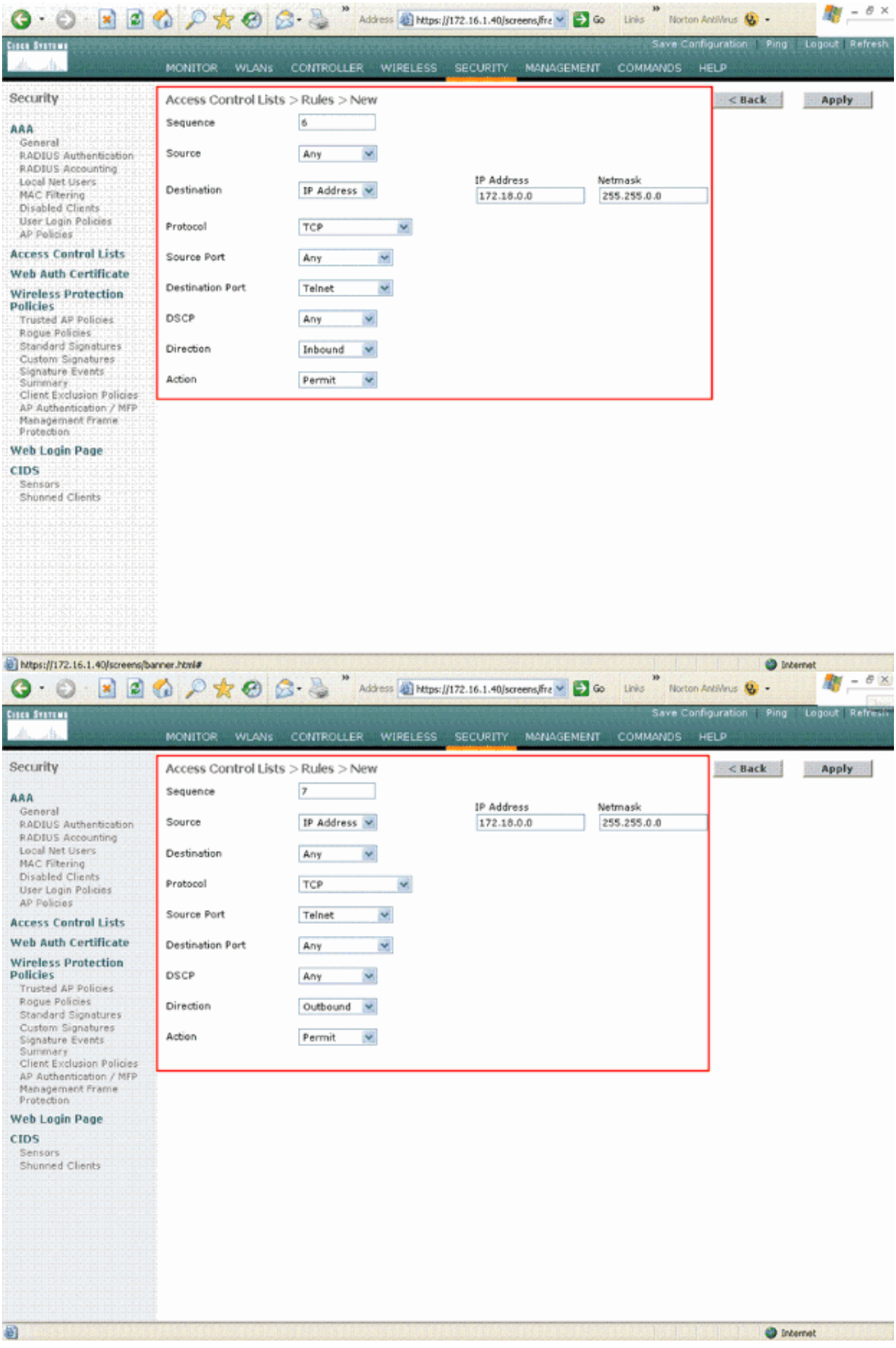


3. Similarmente, crie as regras que permitem o acesso do servidor DNS a todos os clientes Wireless e o acesso do servidor Telnet para o cliente Wireless a uma sub-rede específica. Estão aqui os
exemplos.

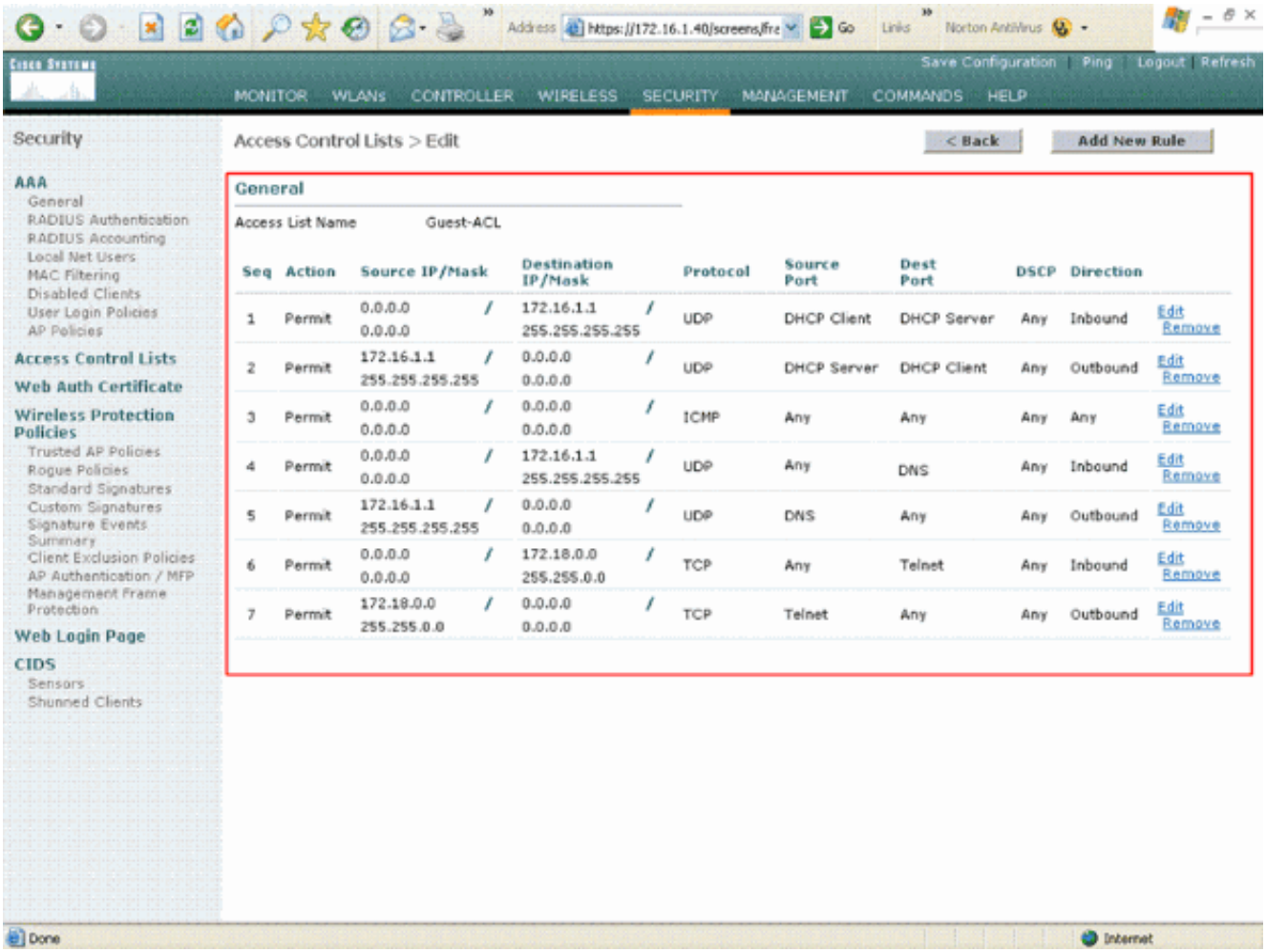


Defina esta regra a fim permitir o acesso para o cliente Wireless ao serviço de

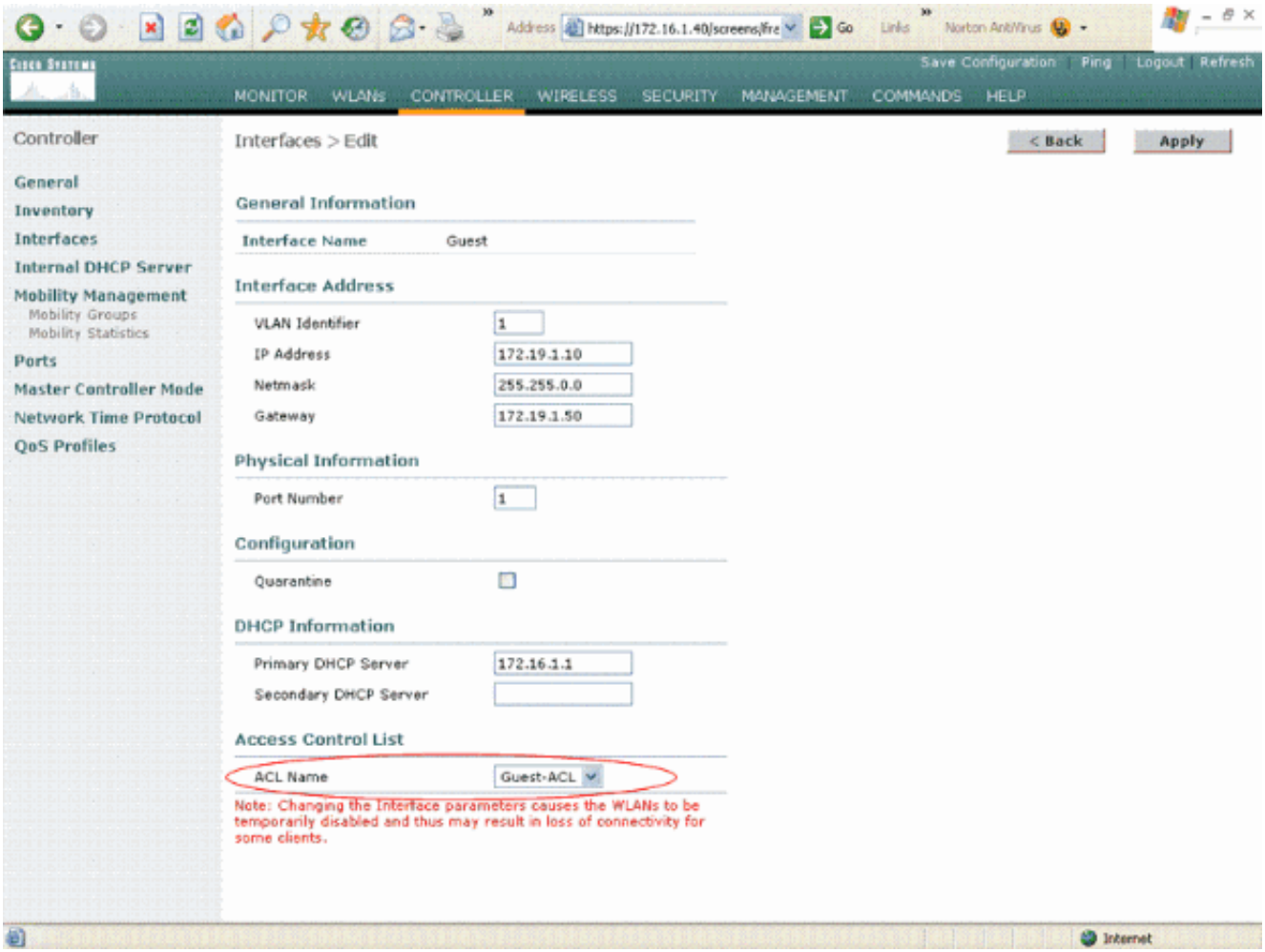
telnet.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence 6
Source Any
Destination IP Address
IP Address 172.16.0.0
Netmask 255.255.0.0
Protocol TCP
Source Port Any
Destination Port Telnet
DSCP Any
Direction Inbound
Action Permit
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence 7
Source IP Address
IP Address 172.16.0.0
Netmask 255.255.0.0
Destination Any
Protocol TCP
Source Port Telnet
Destination Port Any
DSCP Any
Direction Outbound
Action Permit

O ACL > edita a página alista todas as regras que são definidas para o ACL.



4. Uma vez que o ACL é criado, precisa de ser aplicado a uma interface dinâmica. A fim aplicar o ACL, escolha o **controlador > as relações** e edite a relação a que você quer aplicar o ACL.
5. **Nas relações > edite a** página para a interface dinâmica, escolhem o ACL apropriado do menu suspenso das listas de controle de acesso.
   Exemplo:



Uma vez que isto é feito, o ACL permite e nega o tráfego (baseado nas regras configuradas) no WLAN que usa esta interface dinâmica. O Relação-ACL pode somente ser aplicado H-para colher AP no modo conectado mas não no modo independente.

Note: Refira a utilização do CLI para configurar listas de controle de acesso para obter informações sobre de como criar um ACL com o CLI no WLC.

Note: Este documento supõe que os WLAN e as interfaces dinâmica estão configurados. Refira VLAN no exemplo de configuração dos controladores do Wireless LAN para obter informações sobre de como criar interfaces dinâmica em WLC.

Configurar CPU ACL

Previamente, os ACL em WLC não tiveram uma opção para filtrar o tráfego de dados LWAPP/CAPWAP, o tráfego de controle LWAPP/CAPWAP, e o tráfego da mobilidade destinados às relações do Gerenciamento e do gerente AP. A fim endereçar estes edição e filtro LWAPP e mobilidade trafique, CPU ACL foram introduzidos com versão de firmware 4.0 WLC.

A configuração de CPU ACL envolve duas etapas:

1. Configurar regras para o CPU ACL.
2. Aplique o CPU ACL no WLC.

As regras para o CPU ACL devem ser configuradas em uma maneira similar aos outros ACL. Refira a seção CPU ACL de fixar os controladores do Wireless LAN (WLC) para obter mais informações sobre de CPU ACL.

Verificar

Cisco recomenda que você testa suas configurações ACL com um cliente Wireless a fim se assegurar de que você as configure corretamente. Se não se operam corretamente, verifique os ACL no página da web ACL e verifique que suas mudanças ACL estiveram aplicadas à relação do controlador.

Você pode igualmente usar estes **comandos show** a fim verificar sua configuração:

- **mostre o sumário acl** — A fim indicar os ACL que são configurados no controlador, use o **comando summary acl da mostra**.Aqui está um exemplo:

```
(Cisco Controller) >show acl summary

ACL Name                         Applied
-------------------------------- -------
Guest-ACL                        Yes
```

- **mostre o *acl_name* detalhado acl** — Indica a informação detalhada nos ACL configurados.Aqui está um exemplo:

```
(Cisco Controller) >show acl detailed Guest-ACL

                  Source                        Destination               Source Port
Dest Port
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
Range    DSCP Action
-- --- ------------------------------ ------------------------------ ---- ---------- ----
------- ---- ------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
67-67     Any Permit
 2 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67
68-68     Any Permit
 3 Any        0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-65535
0-65535  Any Permit
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65535
53-53     Any Permit
 5 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53
0-65535  Any Permit
 6  In         0.0.0.0/0.0.0.0             172.18.0.0/255.255.0.0             60-65535
23-23     Any Permit
 7 Out      172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-23
0-65535  Any Permit
```

- **mostre o processador central acl** — A fim indicar os ACL configurados no CPU, use o **comando cpu acl da mostra**.Aqui está um exemplo:

```
(Cisco Controller) >show acl detailed Guest-ACL

                  Source                        Destination               Source Port
Dest Port
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
Range    DSCP Action
-- --- ------------------------------ ------------------------------ ---- ---------- ----
------- ---- ------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
67-67     Any Permit
 2 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67
68-68     Any Permit
 3 Any        0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-65535
0-65535  Any Permit
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65535
53-53     Any Permit
```

```
 5 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53
0-65535  Any Permit
 6  In         0.0.0.0/0.0.0.0              172.18.0.0/255.255.0.0             60-65535
23-23     Any Permit
 7 Out      172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-23
0-65535  Any Permit
```

Troubleshooting

O Software Release 4.2.61.0 ou Mais Recente do controlador permite-o de configurar contadores ACL. Os contadores ACL podem ajudar em determinar que ACL foram aplicados aos pacotes transmitidos através do controlador. Esta característica é útil quando você pesquisa defeitos seu sistema.

Os contadores ACL estão disponíveis nestes controladores:

- 4400 Series
- Cisco WiSM
- Interruptor integrado 3750G do controlador do Wireless LAN do catalizador

A fim permitir esta característica, termine estas etapas:

1. Escolha a **Segurança > as listas de controle de acesso > as listas de controle de acesso** a fim abrir a página das listas de controle de acesso.Esta página alista todos os ACL que foram configurados para este controlador.
2. A fim ver se os pacotes estão batendo alguns dos ACL configurados em seu controlador, verifique a caixa de verificação dos **contadores da possibilidade** e o clique **aplica-se**. Se não, deixe a caixa de verificação desmarcada. Este é o valor padrão.
3. Se você quer cancelar os contadores para um ACL, paira seu cursor sobre a seta azul da gota-para baixo para esse ACL e escolhe **contadores claros**.

Informações Relacionadas

- Configurando e aplicando listas de controle de acesso
- VLAN no exemplo de configuração dos controladores do Wireless LAN
- Registro de AP leve (LAP) em um Wireless LAN Controller (WLC)
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte por tecnologia do Sem fio/Mobilidade
- Suporte Técnico e Documentação - Cisco Systems