Exemplo de configuração de ACLs no controlador de LAN sem fio

Contents

Introduction

Este documento descreve como configurar as listas de controle de acesso (ACLs) em controladoras Wireless LAN (WLAN) para filtrar o tráfego através da WLAN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 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

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

- Cisco 2000 Series WLC que executa o firmware 4.0
- LAP Cisco 1000 Series
- Adaptador de cliente sem fio Cisco 802.11a/b/g que executa o firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versão 2.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

ACLs em WLCs

As ACLs na WLC destinam-se a restringir ou permitir que clientes sem fio acessem serviços em sua WLAN.

Antes da versão 4.0 do firmware da WLC, as ACLs eram ignoradas na interface de gerenciamento, portanto, você não pode afetar o tráfego destinado à WLC. Você só pode impedir que clientes sem fio gerenciem o controlador com a opção **Management Via Wireless** . Portanto, as ACLs só podem ser aplicadas a interfaces dinâmicas. Na versão 4.0 do firmware da WLC, há ACLs da CPU que podem filtrar o tráfego destinado à interface de gerenciamento. Consulte a seção Configurar ACLs da CPU para obter mais informações.

Você pode definir até 64 ACLs, cada uma com até 64 regras (ou filtros). Cada regra tem parâmetros que afetam sua ação. Quando um pacote corresponde a todos os parâmetros de uma regra, o conjunto de ações dessa regra é aplicado ao pacote. Você pode configurar ACLs através da GUI ou da CLI.

Estas são algumas das regras que você precisa entender antes de configurar uma ACL no WLC:

- Se a origem e o destino forem any , a direção na qual essa ACL é aplicada poderá ser **any** .
- Se sourceordestination não for nenhum , a direção do filtro deverá ser especificada e uma instrução inversa na direção oposta deverá ser criada.
- A noção de WLC de entrada versus saída não é intuitiva. É da perspectiva da WLC voltada para o cliente sem fio, e não da perspectiva do cliente. Assim, a direção de entrada significa um pacote que entra na WLC do cliente sem fio e a direção de saída significa um pacote que sai da WLC em direção ao cliente sem fio.
- Há um deny implícito no final da ACL.

Considerações quando as ACLs são configuradas nas WLCs

As ALCs nas WLCs funcionam de forma diferente dos roteadores. Estas são algumas coisas que devem ser lembradas quando você configura ACLs em WLCs:

- O erro mais comum é selecionar o IP quando você pretende negar ou permitir pacotes IP. Como você seleciona o que está dentro do pacote IP, você nega ou permite pacotes IP-em-IP.
- As ACLs do controlador não podem bloquear o endereço IP virtual da WLC e, portanto, pacotes DHCP para clientes sem fio.
- As ACLs do controlador não podem bloquear o tráfego multicast recebido de redes com fio destinadas a clientes sem fio. As ACLs do controlador são processadas para tráfego multicast iniciado de clientes sem fio, destinado a redes com fio ou outros clientes sem fio no mesmo controlador.

- Ao contrário de um roteador, a ACL controla o tráfego em ambas as direções quando aplicada a uma interface, mas não executa firewall stateful. Se você se esquecer de abrir um buraco na ACL para o tráfego de retorno, isso causará um problema.
- As ACLs do controlador bloqueiam apenas pacotes IP. Você não pode bloquear ACLs de Camada 2 ou pacotes de Camada 3 que não sejam IP.
- As ACLs do controlador não usam máscaras inversas como os roteadores. Aqui, 255 significa corresponder exatamente àquele octeto do endereço IP.
- As ACLs no controlador são feitas no software e impactam o desempenho de encaminhamento.

Observação: se você aplicar uma ACL a uma interface ou a uma WLAN, o throughput sem fio será reduzido e poderá levar à perda potencial de pacotes. Para melhorar o throughput, remova a ACL da interface ou da WLAN e mova a ACL para um dispositivo com fio vizinho.

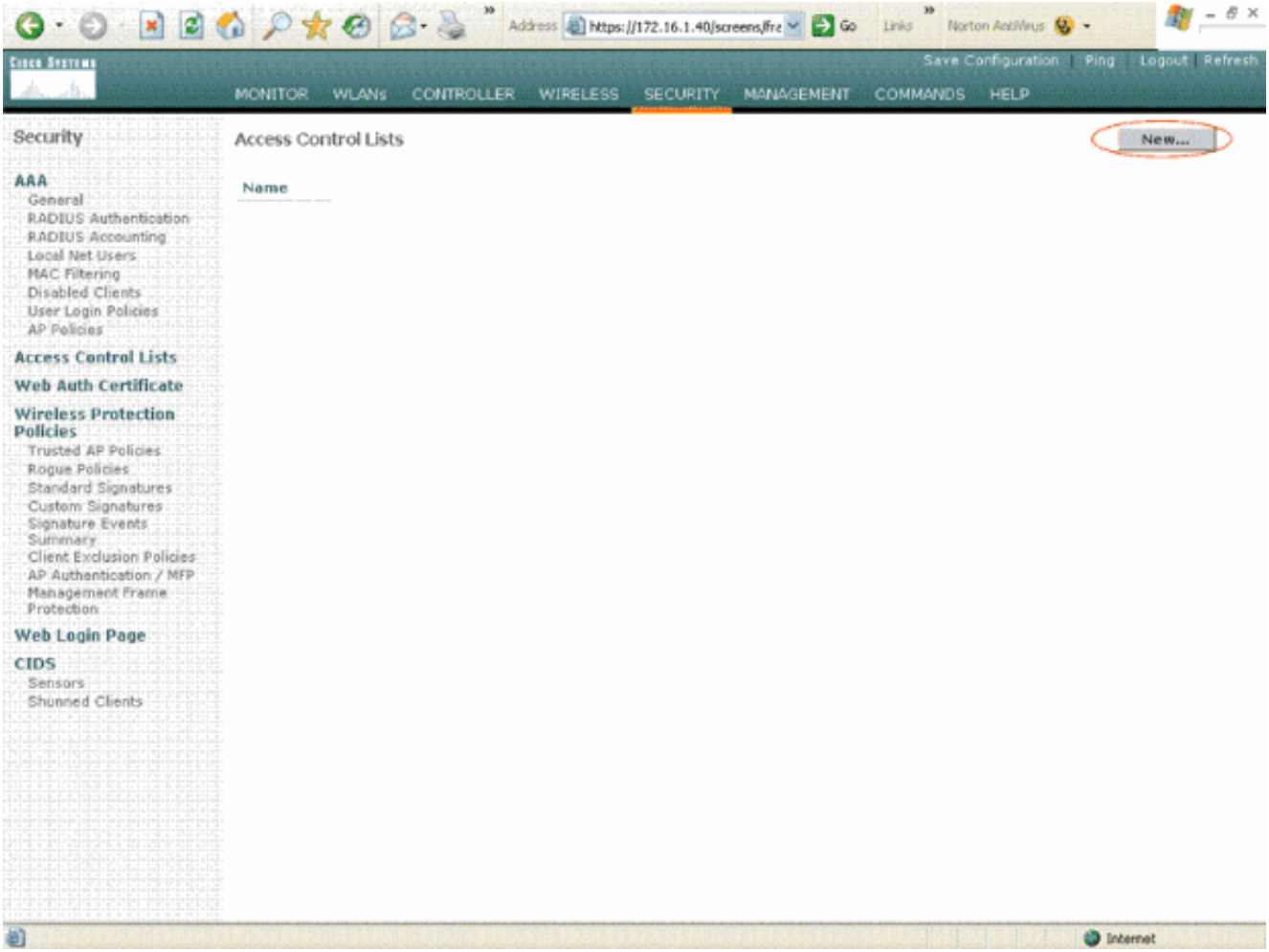
Configurar ACL em WLCs

Esta seção descreve como configurar uma ACL no WLC. O objetivo é configurar uma ACL que permita que clientes convidados acessem estes serviços:

- DHCP (Dynamic Host Configuration Protocol) entre os clientes sem fio e o servidor DHCP
- Internet Control Message Protocol (ICMP) entre todos os dispositivos na rede
- DNS (Domain Name System) entre os clientes sem fio e o servidor DNS
- Executar telnet para uma sub-rede específica

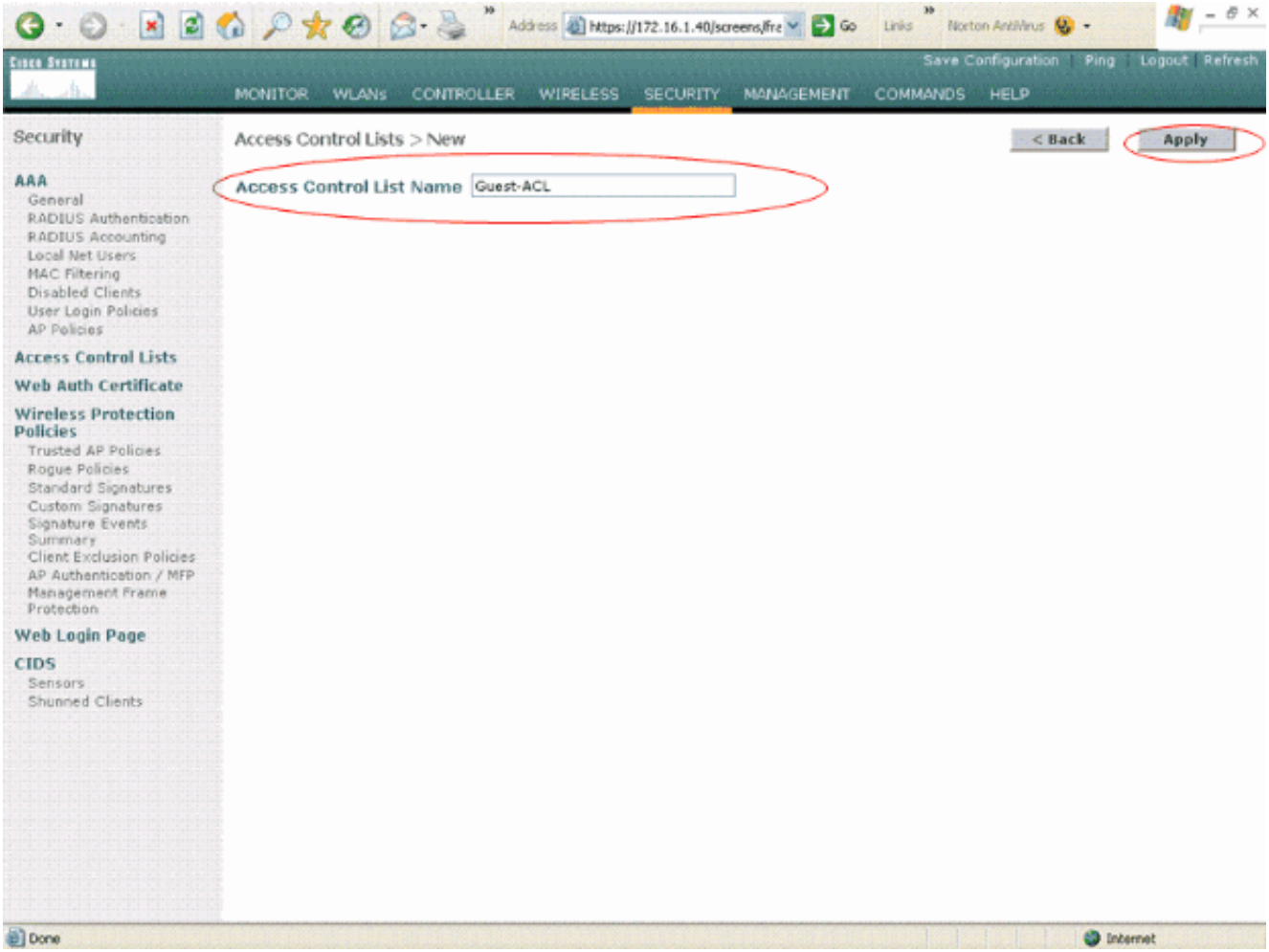
Todos os outros serviços devem ser bloqueados para os clientes sem fio. Conclua estas etapas para criar a ACL com a GUI da WLC:

1. Vá para a GUI da WLC e escolha **Security > Access Control Lists**.A página Listas de Controle de Acesso é exibida. Esta página lista as ACLs configuradas no WLC. Também permite editar ou remover qualquer uma das ACLs. Para criar uma nova ACL, clique em **New**.



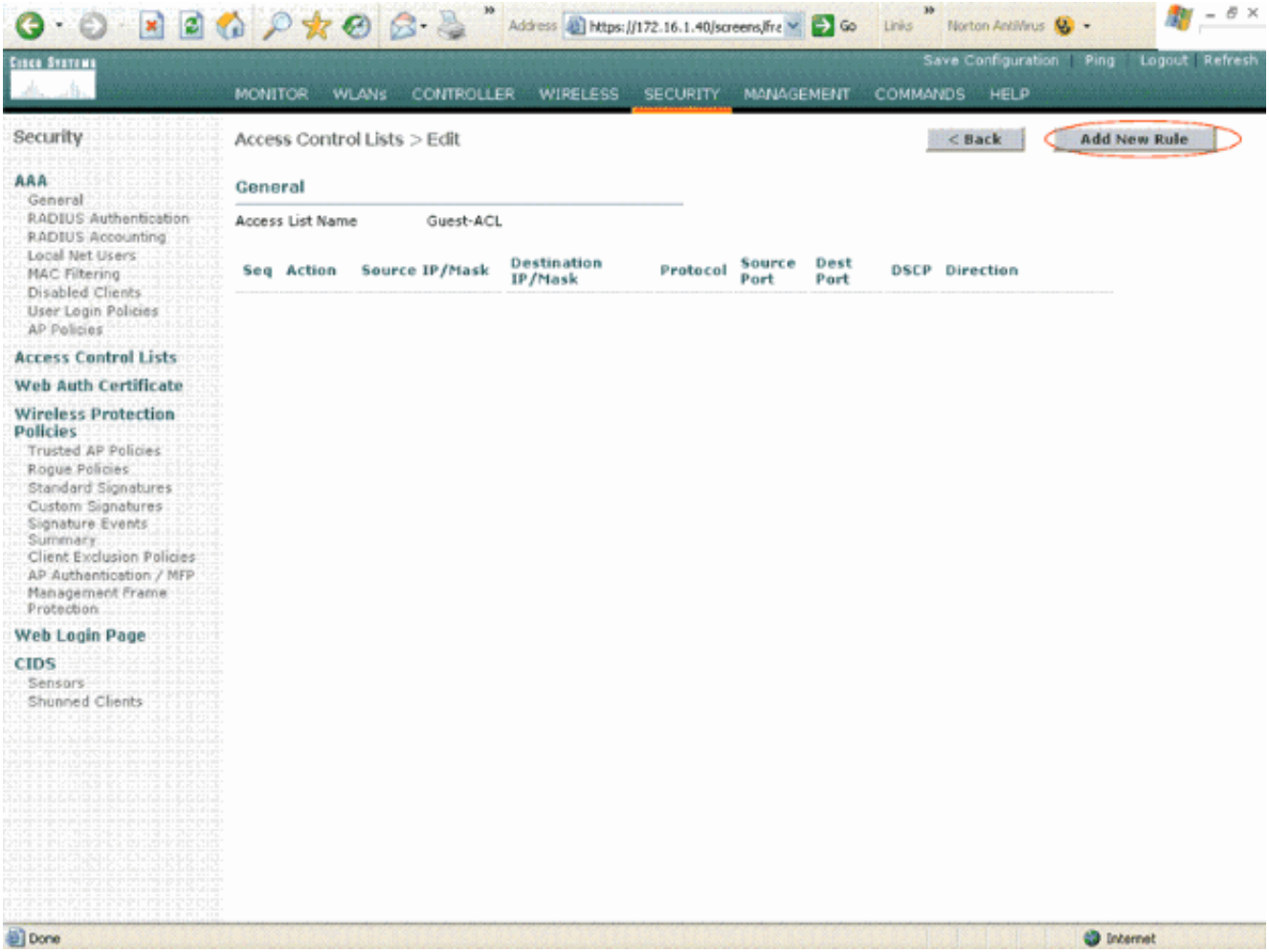
Listas de controle de acesso

2. Insira o nome da ACL e clique em **Apply**.Você pode inserir até 32 caracteres alfanuméricos. Neste exemplo, o nome da ACL é **Guest-ACL** . Depois que a ACL for criada, clique em **Edit** para criar regras para a
ACL.



Insira o nome da ACL

3. Quando a página Listas de controle de acesso > Editar for exibida, clique em **Adicionar nova regra**.A página Listas de Controle de Acesso > Regras > Novo é exibida.



Adicionar novas regras de ACL

4. Configure regras que permitam a um usuário convidado estes serviços:DHCP entre os clientes sem fio e o servidor DHCPICMP entre todos os dispositivos na redeDNS entre os clientes sem fio e o servidor DNSExecutar telnet para uma sub-rede específica

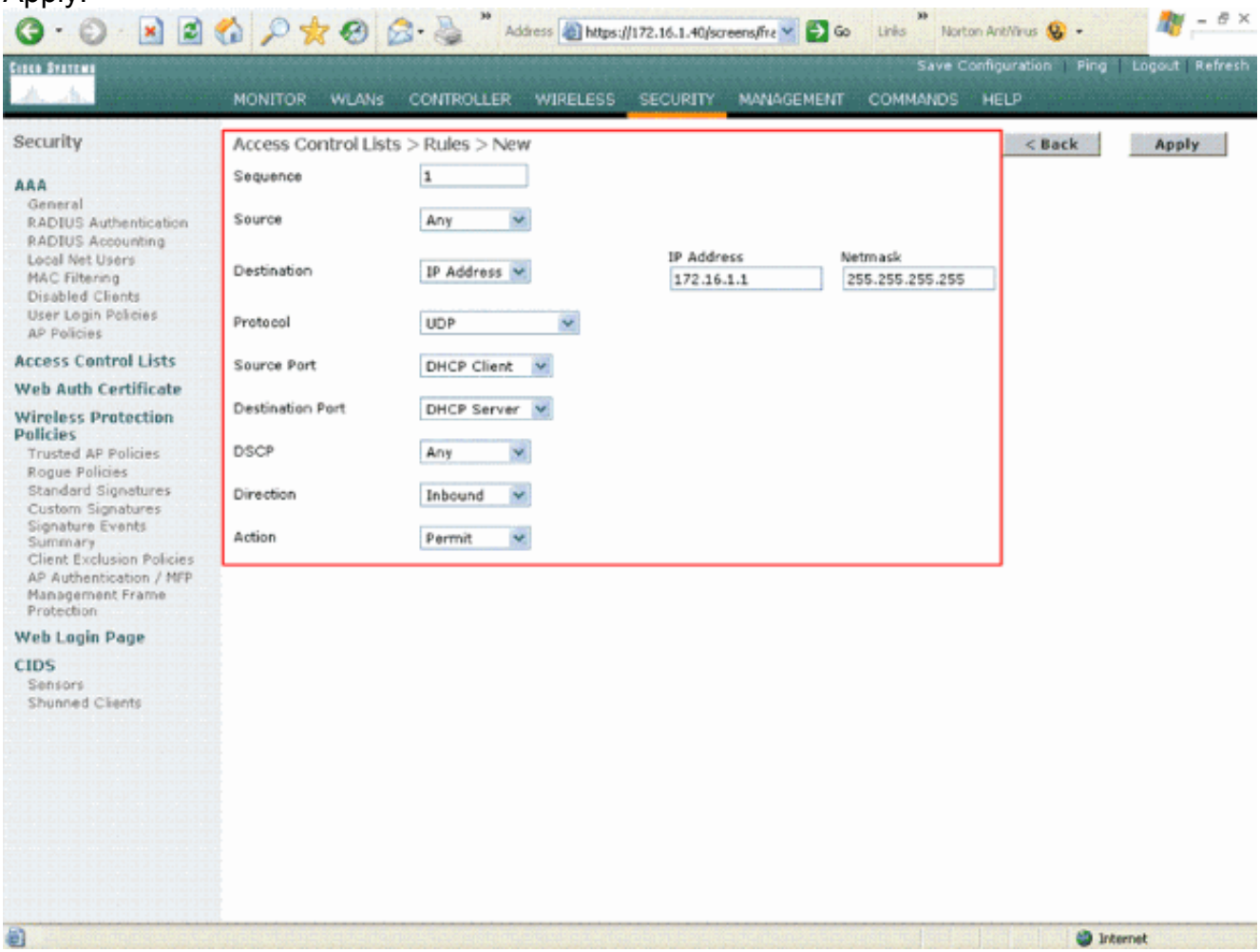
Configurar Regras que Permitem Serviços de Usuário Convidado

Esta seção mostra um exemplo de como configurar as regras para estes serviços:

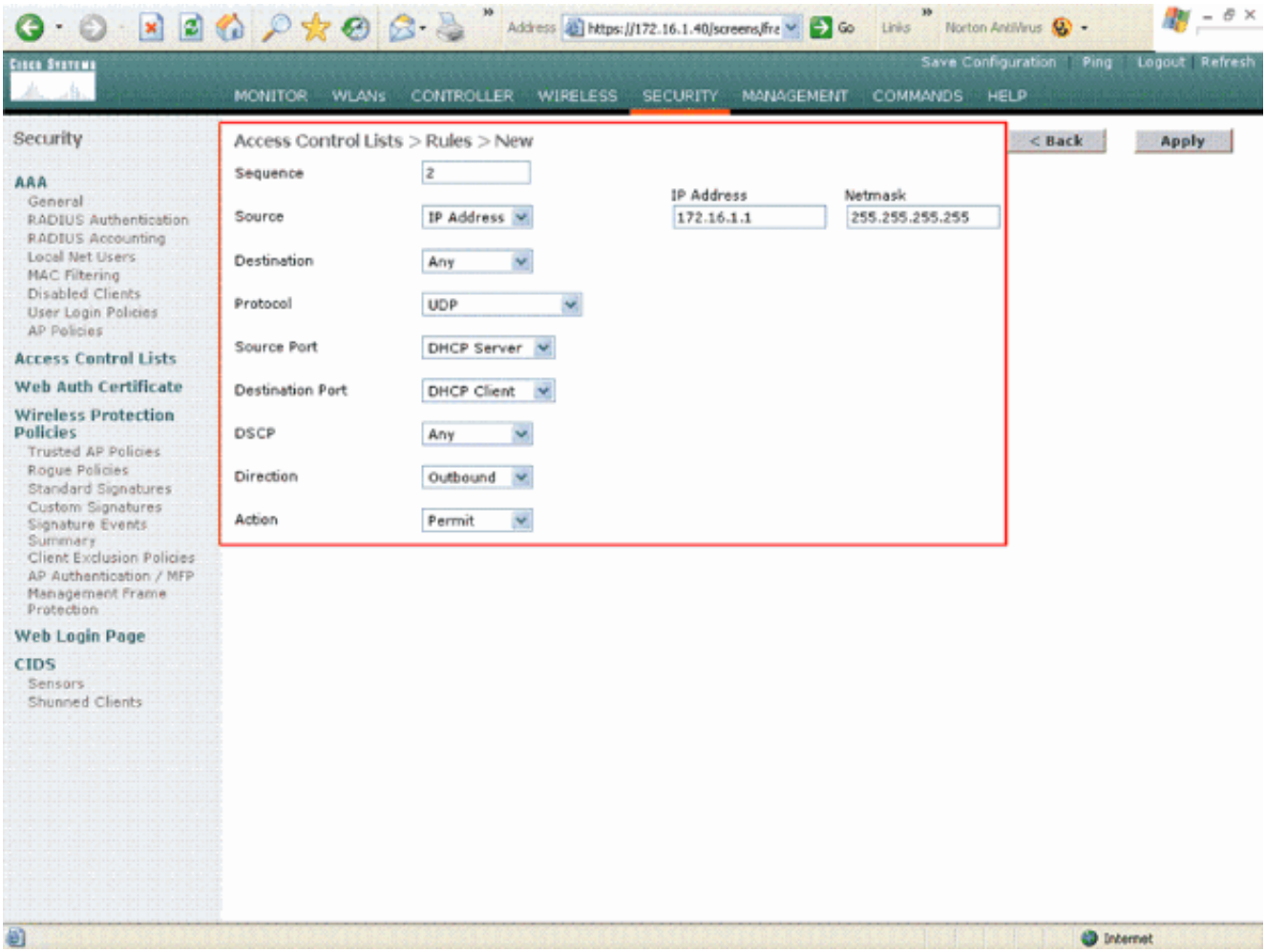
- DHCP entre os clientes sem fio e o servidor DHCP
- ICMP entre todos os dispositivos na rede
- DNS entre os clientes sem fio e o servidor DNS
- Executar telnet para uma sub-rede específica

1. Para definir a regra para o serviço DHCP, selecione os intervalos de IP origem e destino.Este exemplo usa **any** para a origem, o que significa que qualquer cliente sem fio tem permissão para acessar o servidor DHCP. Neste exemplo, o servidor 172.16.1.1 atua como o servidor DHCP e DNS. Portanto, o endereço IP destino é 172.16.1.1/255.255.255.255 (com uma máscara de host).Como o DHCP é um protocolo baseado em UDP, selecione **UDP** no campo suspenso Protocol (Protocolo). Se você escolher TCP ou UDP na etapa anterior, dois parâmetros adicionais serão exibidos: Porta de origem e Porta de destino. Especifique os detalhes das portas de Origem e Destino. Para essa regra, a porta de origem é o **cliente DHCP** e a porta de destino é o **servidor DHCP** .Escolha a direção na qual a ACL deve ser aplicada. Como essa regra é do cliente para o servidor, este exemplo usa **Entrada**. Na caixa suspensa Ação, escolha **Permitir** para fazer

com que essa ACL permita pacotes DHCP do cliente sem fio para o servidor DHCP. O valor padrão é Negar. Clique em
Apply.

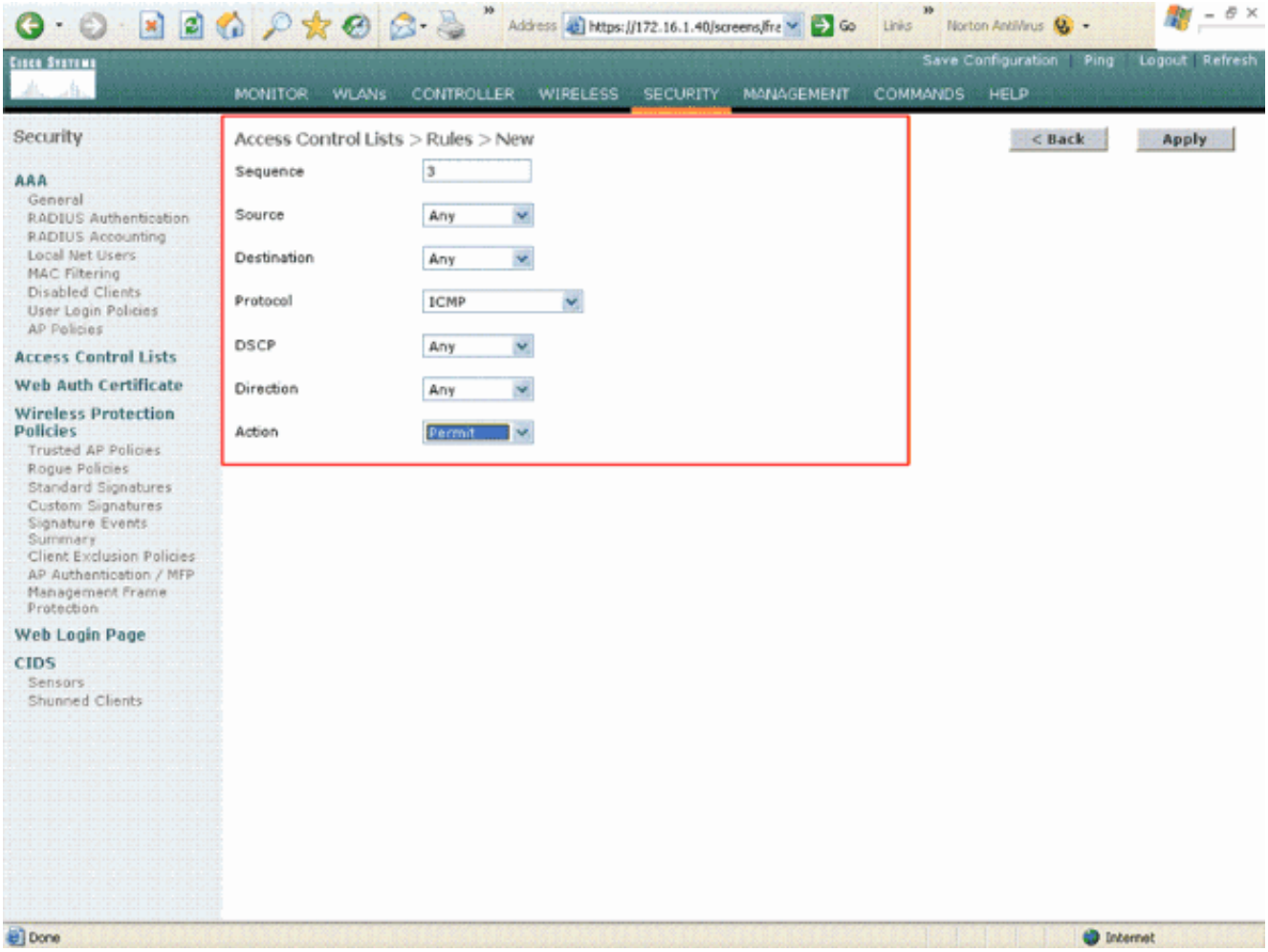


Escolha Permitir para fazer com que a ACL permita pacotes DHCP Se a origem ou o destino não forem **nenhum** , uma instrução inversa na direção oposta deverá ser criada.
Exemplo:



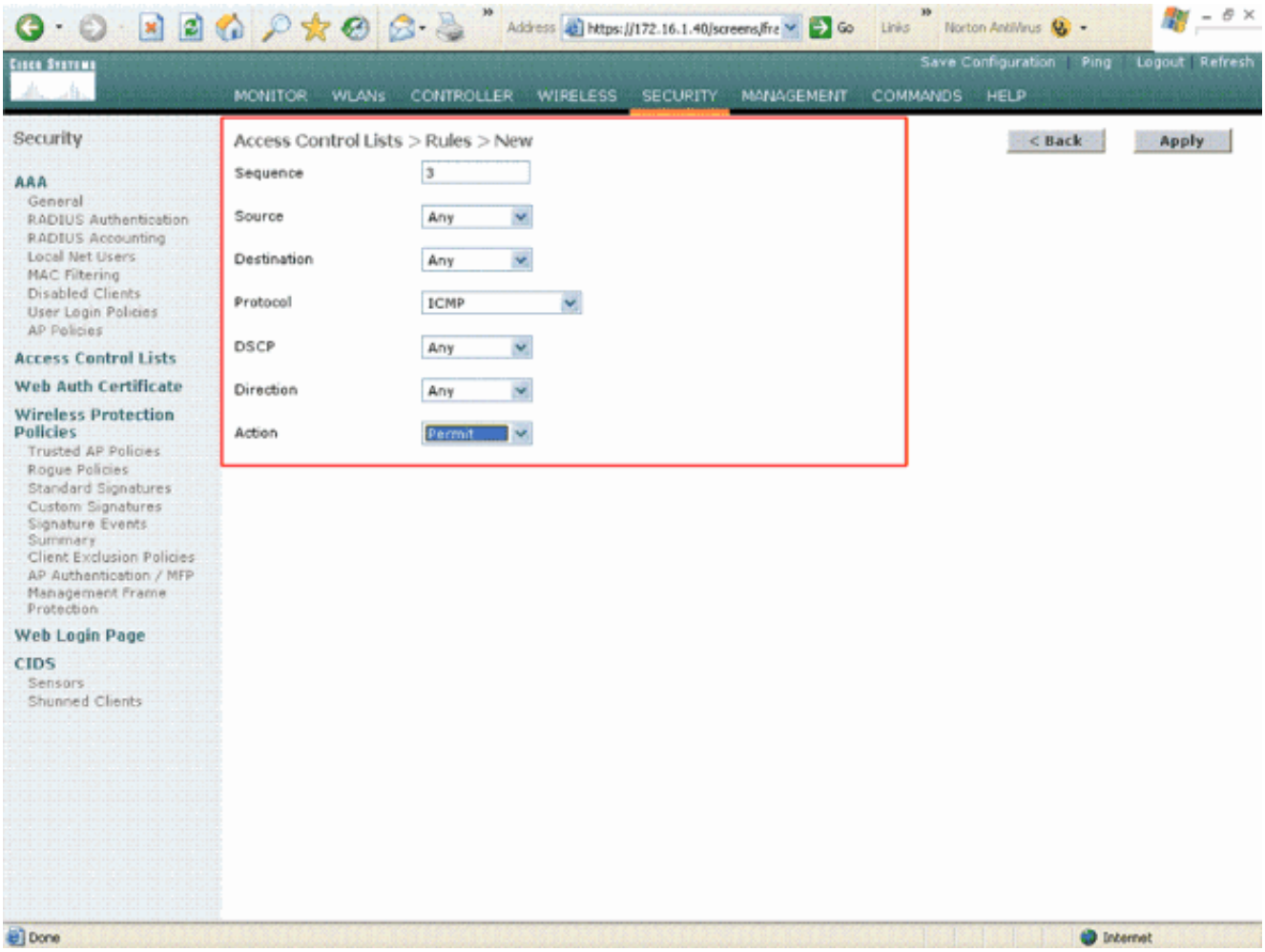
Origem ou Destino definido como Qualquer

2. Para definir uma regra que permita pacotes ICMP entre todos os dispositivos, selecione **any** nos campos Source (Origem) e Destination (Destino). Este é o valor padrão.Escolha **ICMP** no campo suspenso Protocolo. Como este exemplo usa **qualquer** para os campos Origem e Destino, você não precisa especificar a direção. Ele pode ser deixado com o valor padrão de **any**. Além disso, a instrução inversa na direção oposta não é necessária.No menu suspenso Action, escolha **Permit** para fazer com que essa ACL permita pacotes DHCP do servidor DHCP para o cliente sem fio. Clique em
Apply.

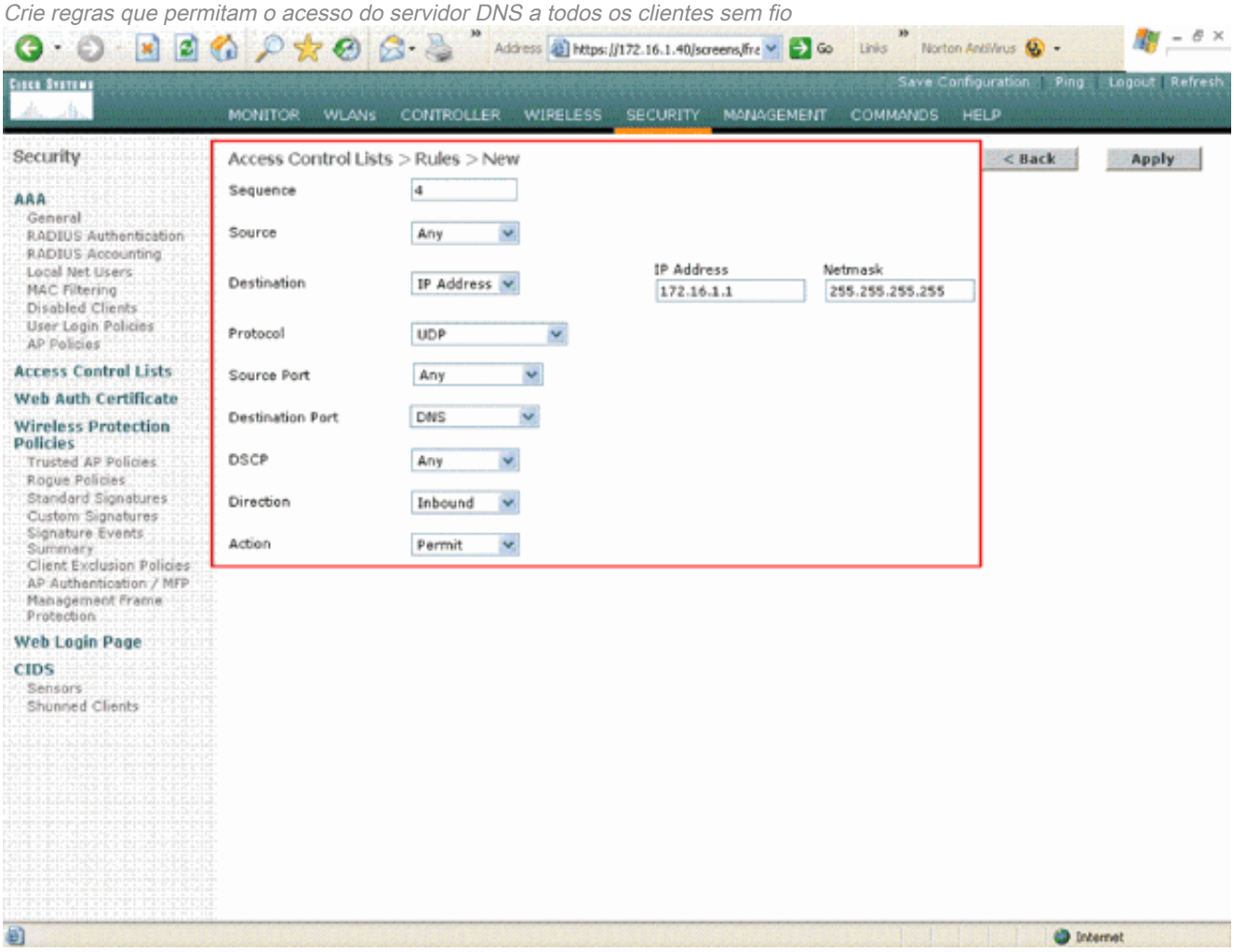


Permitir que faça com que a ACL permita pacotes DHCP do servidor DHCP para o cliente sem fio

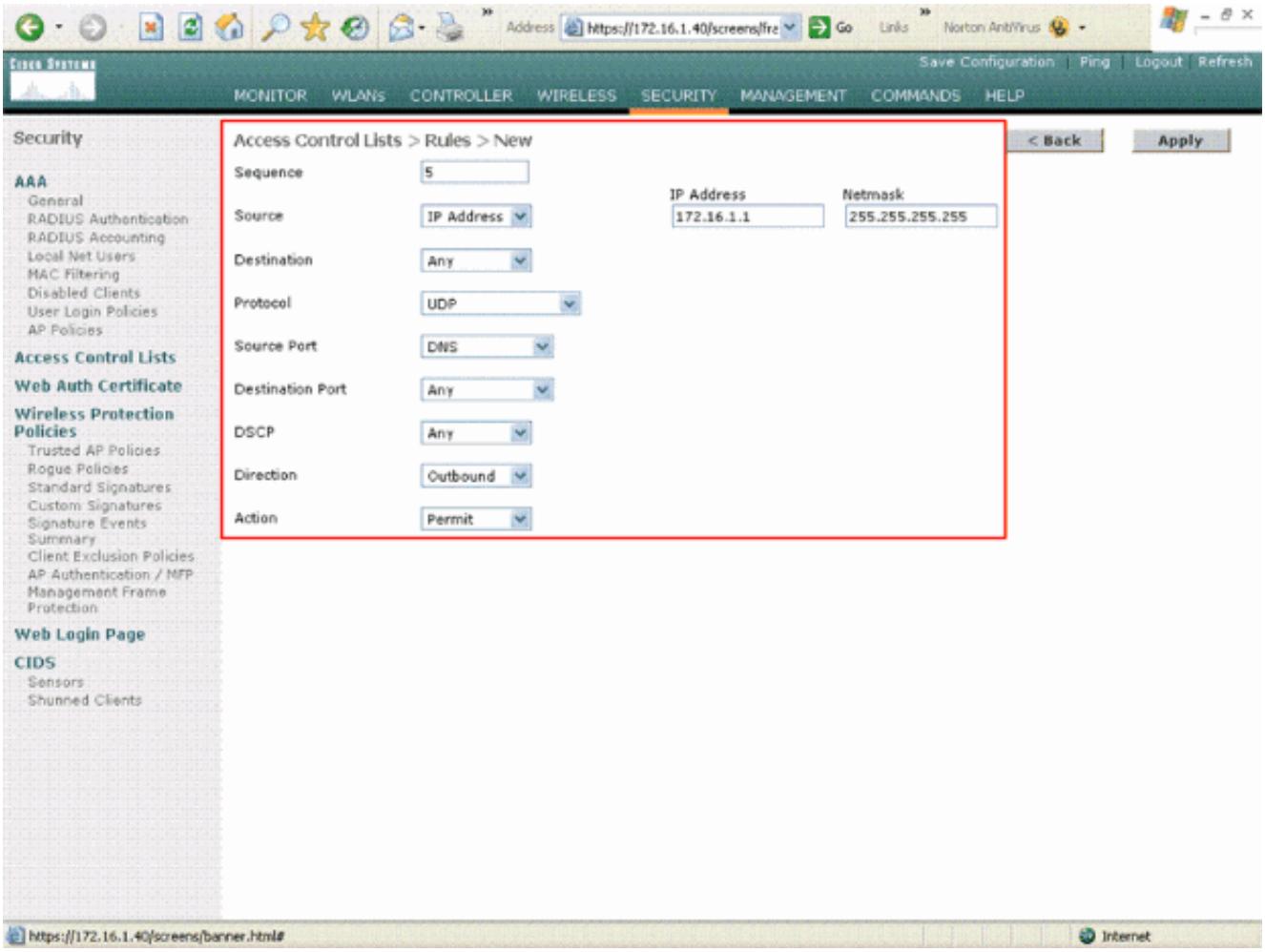
3. Da mesma forma, crie regras que permitam o acesso do servidor DNS a todos os clientes sem fio e o acesso do servidor Telnet para o cliente sem fio a uma sub-rede específica. Aqui estão os
exemplos.



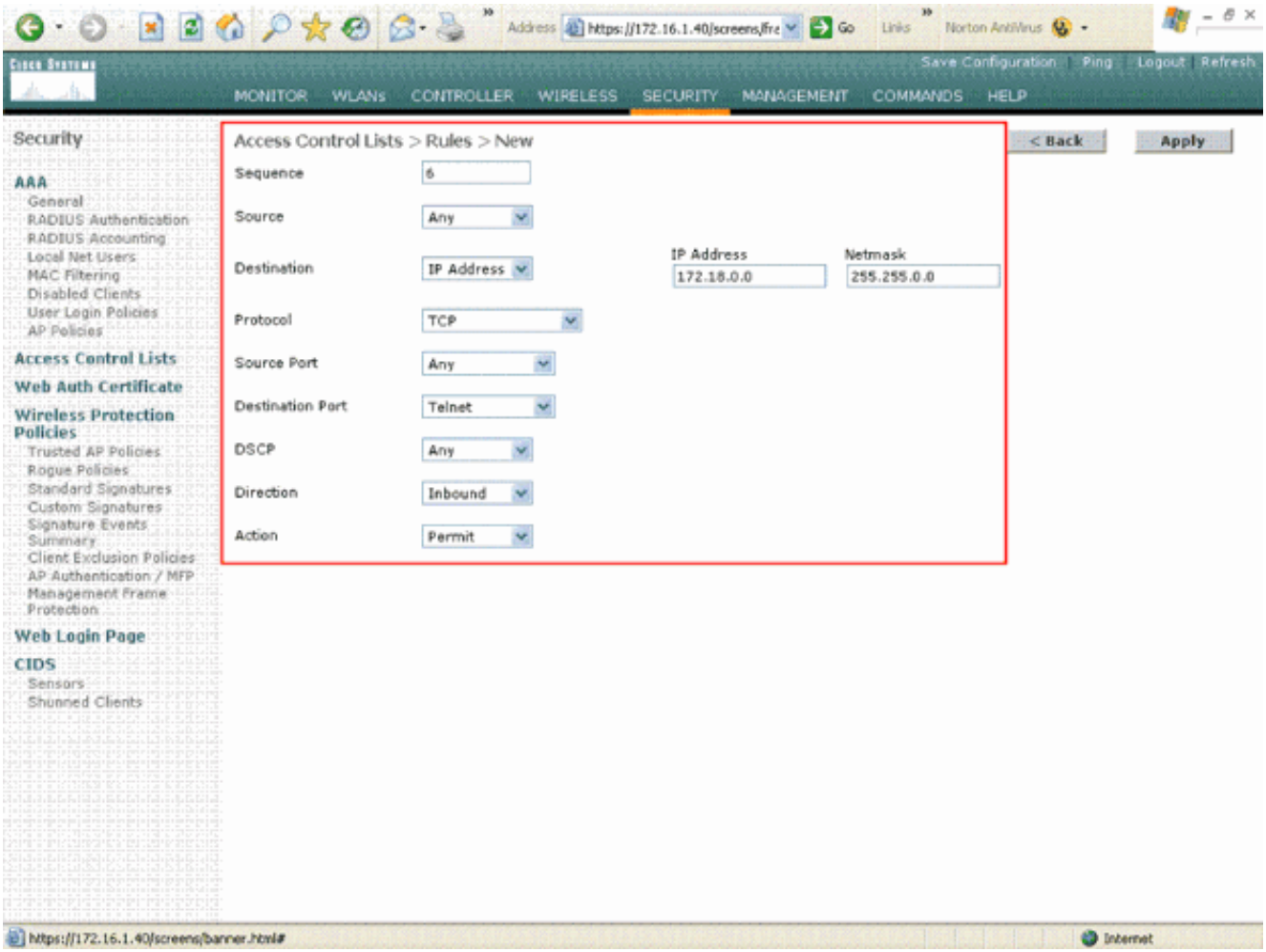
Crie regras que permitam o acesso do servidor DNS a todos os clientes sem fio



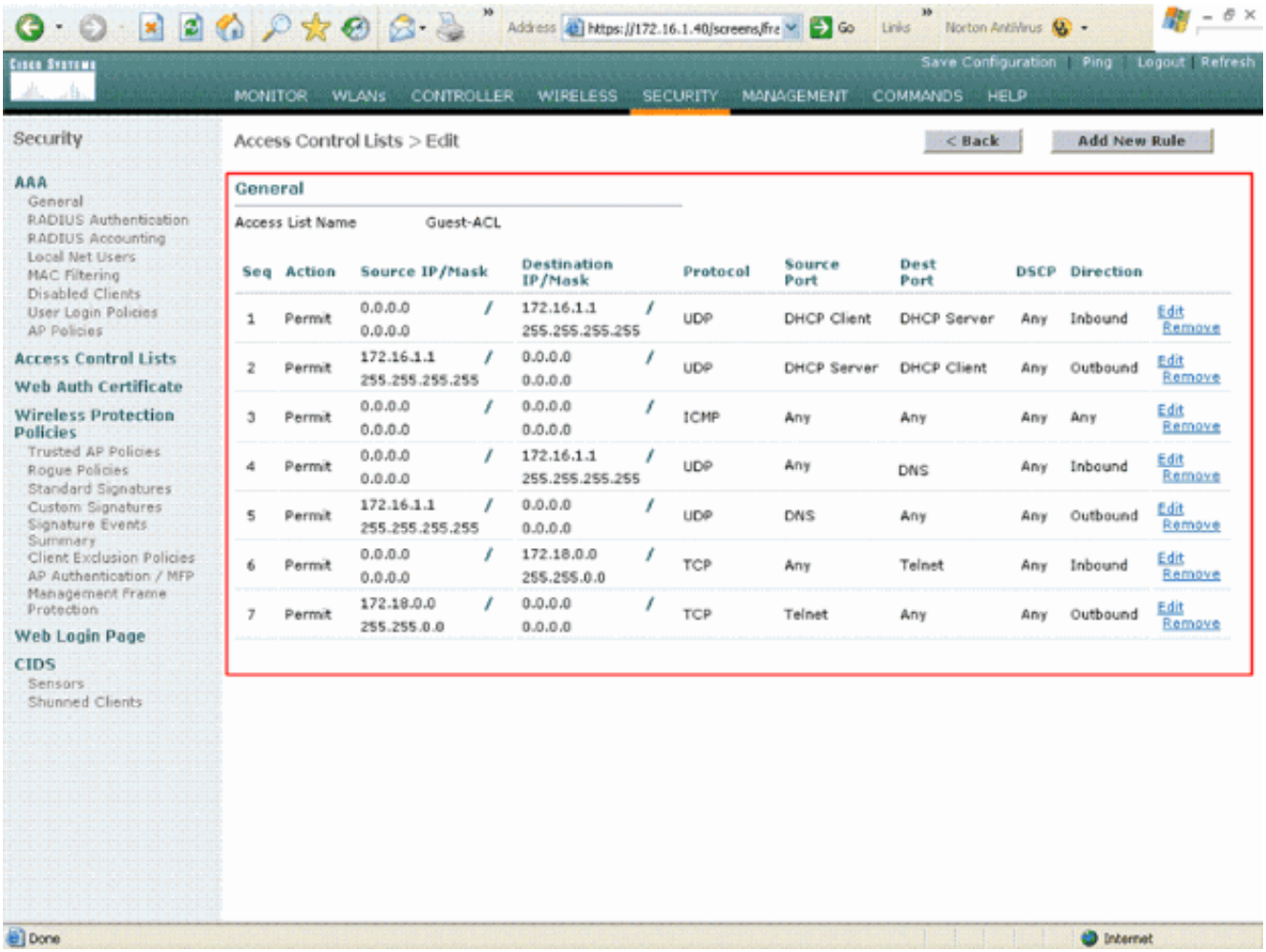
Crie regras que permitam o acesso do servidor Telnet para o cliente sem fio a uma sub-rede Defina esta regra para permitir o acesso do cliente sem fio ao serviço Telnet.



Permitir acesso do cliente sem fio ao serviço Telnet

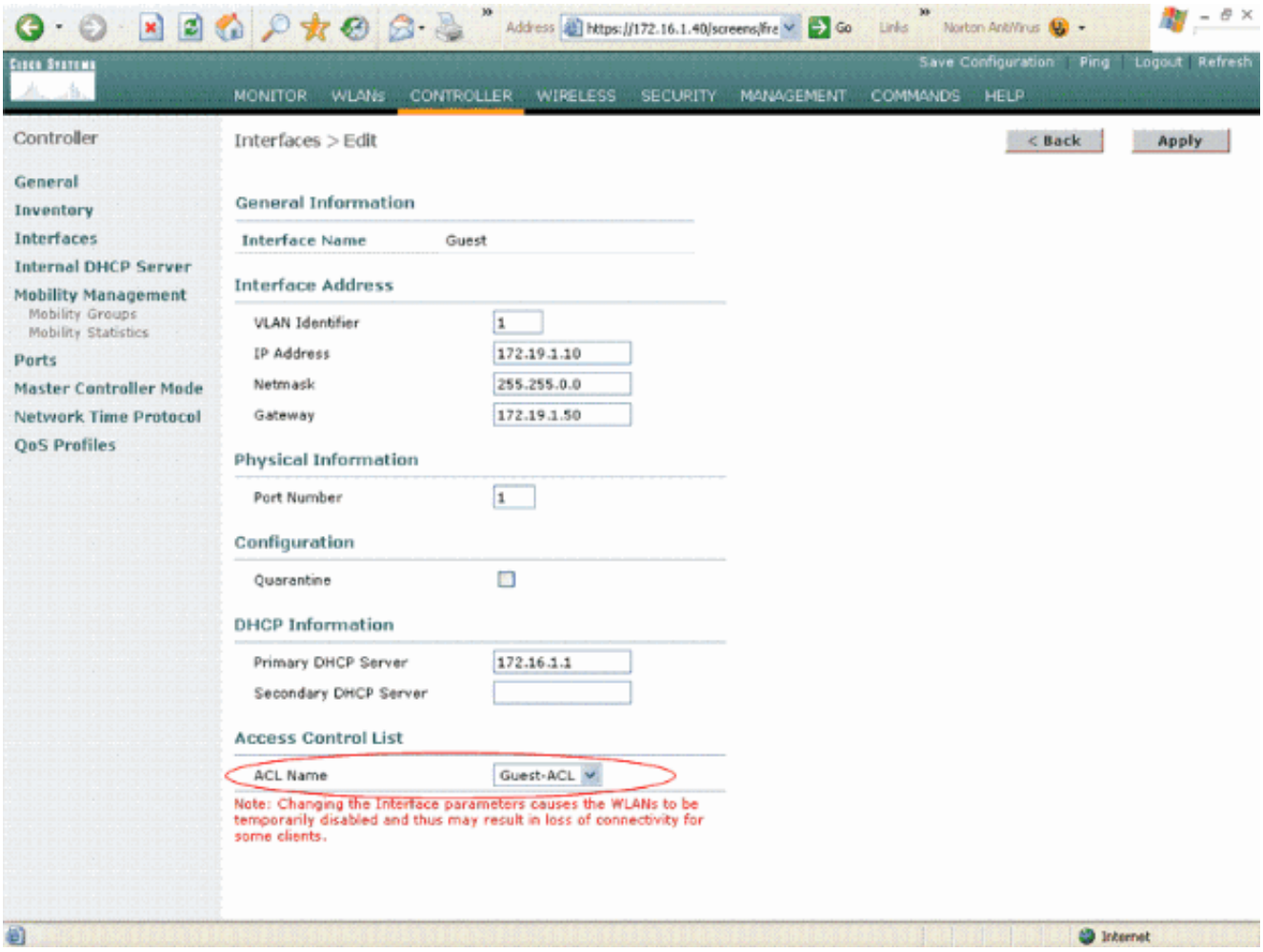


Outro exemplo de acesso de cliente sem fio ao serviço Telnet A página **ACL > Edit** lista todas as regras definidas para a
ACL.



Página Editar lista todas as regras definidas para a ACL

4. Depois de criada, a ACL precisa ser aplicada a uma interface dinâmica. Para aplicar a ACL, escolha **Controller > Interfaces** e edite a interface à qual deseja aplicar a ACL.
5. Na página **Interfaces > Edit** da interface dinâmica, escolha a ACL apropriada no menu suspenso Access Control Lists.
   Exemplo:



Escolha a ACL apropriada no menu Lista de controle de acesso

Uma vez feito isso, a ACL permite e nega o tráfego (com base nas regras configuradas) na WLAN que usa essa interface dinâmica. A interface ACL só pode ser aplicada a APs H-Reap no modo conectado, mas não no modo autônomo.

> **Observação**: este documento supõe que as WLANs e as interfaces dinâmicas estejam configuradas. Consulte Configurar VLANs em Wireless LAN Controllers ou informações sobre como criar interfaces dinâmicas em WLCs.

Configurar ACLs de CPU

Anteriormente, as ACLs nas WLCs não tinham uma opção para filtrar o tráfego de dados LWAPP/CAPWAP, o tráfego de controle LWAPP/CAPWAP e o tráfego de mobilidade destinado às interfaces de gerenciamento e gerenciador de AP. Para resolver esse problema e filtrar o LWAPP e o tráfego de mobilidade, as ACLs da CPU foram introduzidas com o firmware da WLC versão 4.0.

A configuração das ACLs de CPU envolve duas etapas:

1. Configure regras para a ACL da CPU.
2. Aplique a ACL da CPU na WLC.

As regras para a ACL da CPU devem ser configuradas de maneira semelhante às outras ACLs.

Verificar

A Cisco recomenda que você teste as configurações da ACL com um cliente sem fio para garantir que você as configurou corretamente. Se eles não funcionarem corretamente, verifique as ACLs na página da Web da ACL e verifique se as alterações da ACL foram aplicadas à interface do controlador.

Você também pode usar estes comandos **show** para verificar sua configuração:

- **show acl summary** — Para exibir as ACLs configuradas no controlador, use o comando **show acl summary**.Aqui está um exemplo:

```
(Cisco Controller) >show acl summary

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

- show acl **detailedACL_Name — Exibe informações detalhadas sobre as ACLs configuradas.**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
```

- **show acl cpu** — Para exibir as ACLs configuradas na CPU, use o comando **show acl cpu**.Aqui está um exemplo:

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................. CPU-ACL
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

Troubleshoot

A versão 4.2.x ou posterior do software do controlador permite que você configure os contadores ACL. Os contadores de ACL podem ajudar a determinar quais ACLs foram aplicadas aos pacotes transmitidos através do controlador. Esse recurso é útil quando você soluciona problemas no sistema.

Os contadores de ACL estão disponíveis nestes controladores:

- 4400 Series
- WiSM da Cisco
- Switch de controlador de LAN sem fio integrado Catalyst 3750G

Para habilitar este recurso, siga estas etapas:

1. Escolha **Security > Access Control Lists > Access Control Lists** para abrir a página Access Control Lists.Esta página lista todas as ACLs que foram configuradas para este controlador.
2. Para ver se os pacotes atingem qualquer uma das ACLs configuradas em seu controlador, marque a caixa de seleção **Enable Counters** e clique em **Apply** . Caso contrário, deixe a caixa de seleção desmarcada. Este é o valor padrão.
3. Se quiser limpar os contadores de uma ACL, passe o cursor sobre a seta suspensa azul dessa ACL e escolha **Clear Counters** .

Informações Relacionadas

- Guia de configuração de Cisco Wireless LAN Controller, versão 6.0
- Configurar VLANs em controladores de LAN sem fio
- Solucionar problemas de um AP leve que não ingressa em um WLC
- Suporte técnico e downloads da Cisco

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.