ACL's configureren op draadloze LAN-controller - voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de toegangscontrolelijsten (ACL's) op draadloze LAN-controllers (WLAN's) kunt configureren om verkeer door het WLAN te filteren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe de WLC en Lichtgewicht access point (LAP) te configureren voor basisbediening
- Basiskennis van Lichtgewicht access point protocol (LWAP) en draadloze beveiligingsmethoden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2000 Series WLC voor firmware 4.0
- Cisco 1000 Series router
- Cisco 802.11a/b/g draadloze clientadapter waarop firmware 2.6 wordt uitgevoerd
- Cisco Aironet Desktop Utility (ADU) versie 2.6

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

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

ACL's op WLC's

ACL's op de WLC zijn bedoeld om draadloze clients te beperken of toe te staan tot services op zijn WLAN.

Vóór WLC firmware versie 4.0 worden ACL's overgeslagen op de Management Interface, zodat u geen invloed hebt op verkeer dat bestemd is voor de WLC, kunt u alleen voorkomen dat draadloze clients het beheer van de controller met de optie **Management Via Wireless**. Daarom kunnen ACL's alleen op dynamische interfaces worden toegepast. In WLC-firmware versie 4.0 zijn er CPU-ACL's die verkeer kunnen filteren dat bestemd is voor de beheerinterface. Zie de sectie CPU ACL's configureren voor meer informatie.

U kunt maximaal 64 ACL's definiëren, elk met maximaal 64 regels (of filters). Elke regel heeft parameters die de werking ervan beïnvloeden. Wanneer een pakket alle parameters voor een regel aanpast, wordt de actie die voor die regel is ingesteld, op het pakket toegepast. U kunt ACL's configureren via de GUI of de CLI.

Dit zijn enkele regels die u moet begrijpen voordat u een ACL op de WLC vormt:

- Als de bron en de bestemming om het **even welk** zijn, kan de richting waarin deze ACL wordt toegepast om het **even welk zijn** .
- Als de bronbestemming **niet** bestaat, moet de richting van het filter worden opgegeven en moet er een omgekeerde verklaring in de tegenovergestelde richting worden aangemaakt.
- De WLC notie van inkomende versus uitgaande is niet-intuïtief. Het is vanuit het perspectief van de WLC gericht op de draadloze client, in plaats van vanuit het perspectief van de klant. Dus, inkomende richting betekent een pakket dat in de WLC van de draadloze client komt en uitgaande richting betekent een pakket dat van de WLC naar de draadloze client gaat.
- Er is impliciet ontkennen aan het eind van ACL.

Overwegingen wanneer ACL's in WLC's zijn geconfigureerd

ALC's in WLC's werken anders dan in routers. Dit zijn een paar dingen om te onthouden wanneer u ACL's in WLC's configureert:

- De meest voorkomende fout is om IP te selecteren wanneer u van plan bent om IP-pakketten te weigeren of toe te staan. Omdat u selecteert wat zich binnen het IP-pakket bevindt, ontkent u IP-in-IP-pakketten of staat u deze toe.
- ControllerACL's kunnen het virtuele IP-adres WLC niet blokkeren en dus DHCP-pakketten voor draadloze clients.
- ControllerACL's kunnen multicast verkeer dat van bekabelde netwerken wordt ontvangen en dat bestemd is voor draadloze clients, niet blokkeren. ControllerACL's worden verwerkt voor

multicast-verkeer dat vanuit draadloze clients wordt gestart en bestemd is voor bekabelde netwerken of andere draadloze clients op dezelfde controller.
- In tegenstelling tot een router, controleert ACL verkeer in beide richtingen wanneer toegepast op een interface, maar het voert geen stateful firewalling uit. Als u vergeet een gat in de ACL te openen voor terugkeerverkeer, veroorzaakt dit een probleem.
- Controller ACL's blokkeren alleen IP-pakketten. U kunt Layer 2 ACL's of Layer 3-pakketten die geen IP zijn, niet blokkeren.
- ControllerACL's gebruiken geen omgekeerde maskers zoals de routers. Hier betekent 255 dat het octet van het IP-adres exact overeenkomt.
- ACL's op de controller worden uitgevoerd in software en impact doorsturen prestaties.

Opmerking: als u een ACL op een interface of een WLAN toepast, wordt de draadloze doorvoersnelheid beperkt en kan dit leiden tot mogelijk verlies van pakketten. Om productie te verbeteren, verwijder ACL uit de interface of WLAN en verplaats ACL naar een naburig bekabeld apparaat.

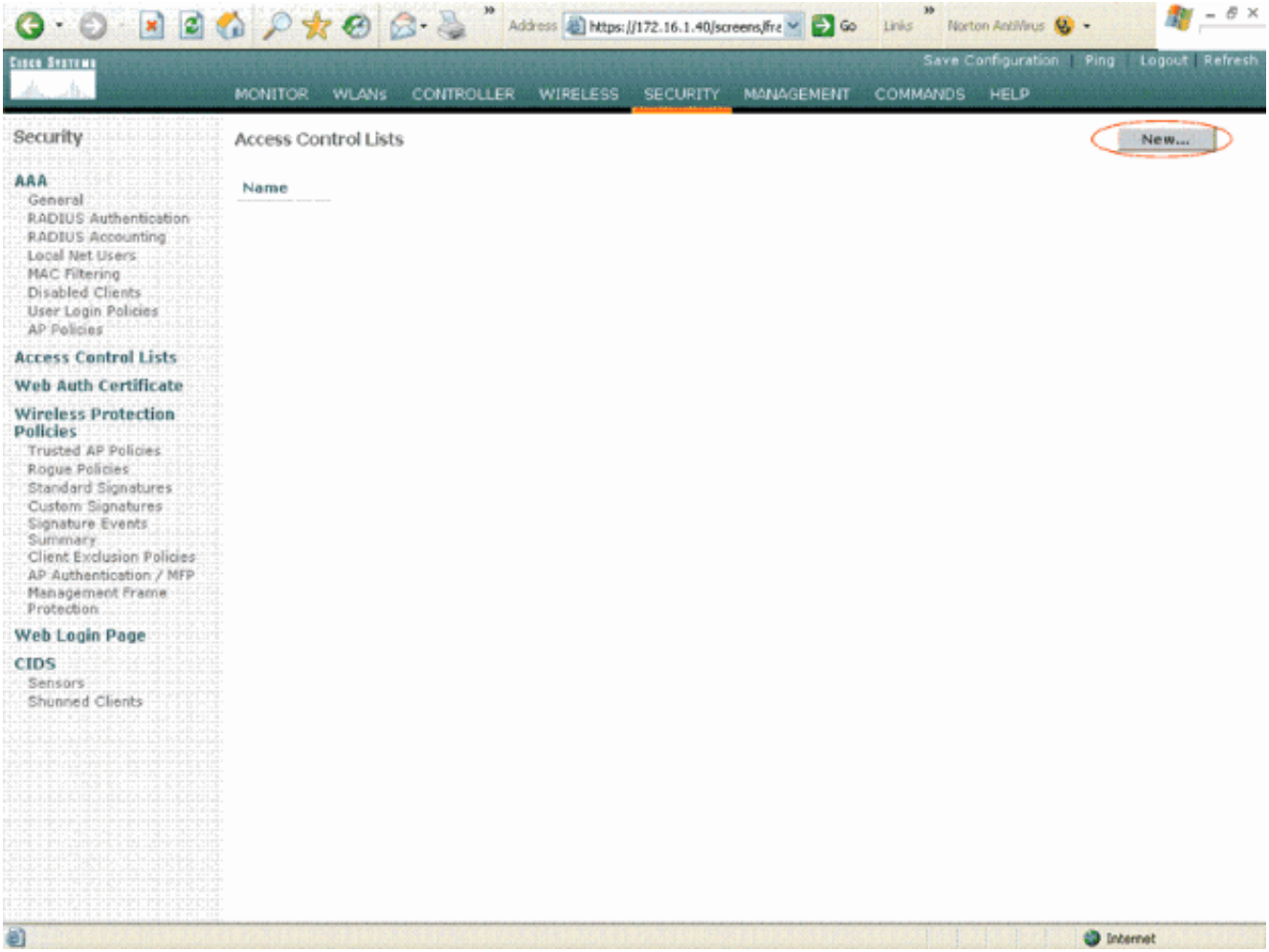
Configureer ACL op WLC's

In deze sectie wordt beschreven hoe u een ACL op de WLC kunt configureren. Het doel is een ACL te configureren die gastclients toegang biedt tot deze services:

- Dynamic Host Configuration Protocol (DHCP) tussen de draadloze clients en DHCP-server
- ICMP-protocol (Internet Control Message Protocol) tussen alle apparaten in het netwerk
- Domain Name System (DNS) tussen de draadloze clients en de DNS-server
- Telnet naar een specifieke subnetverbinding

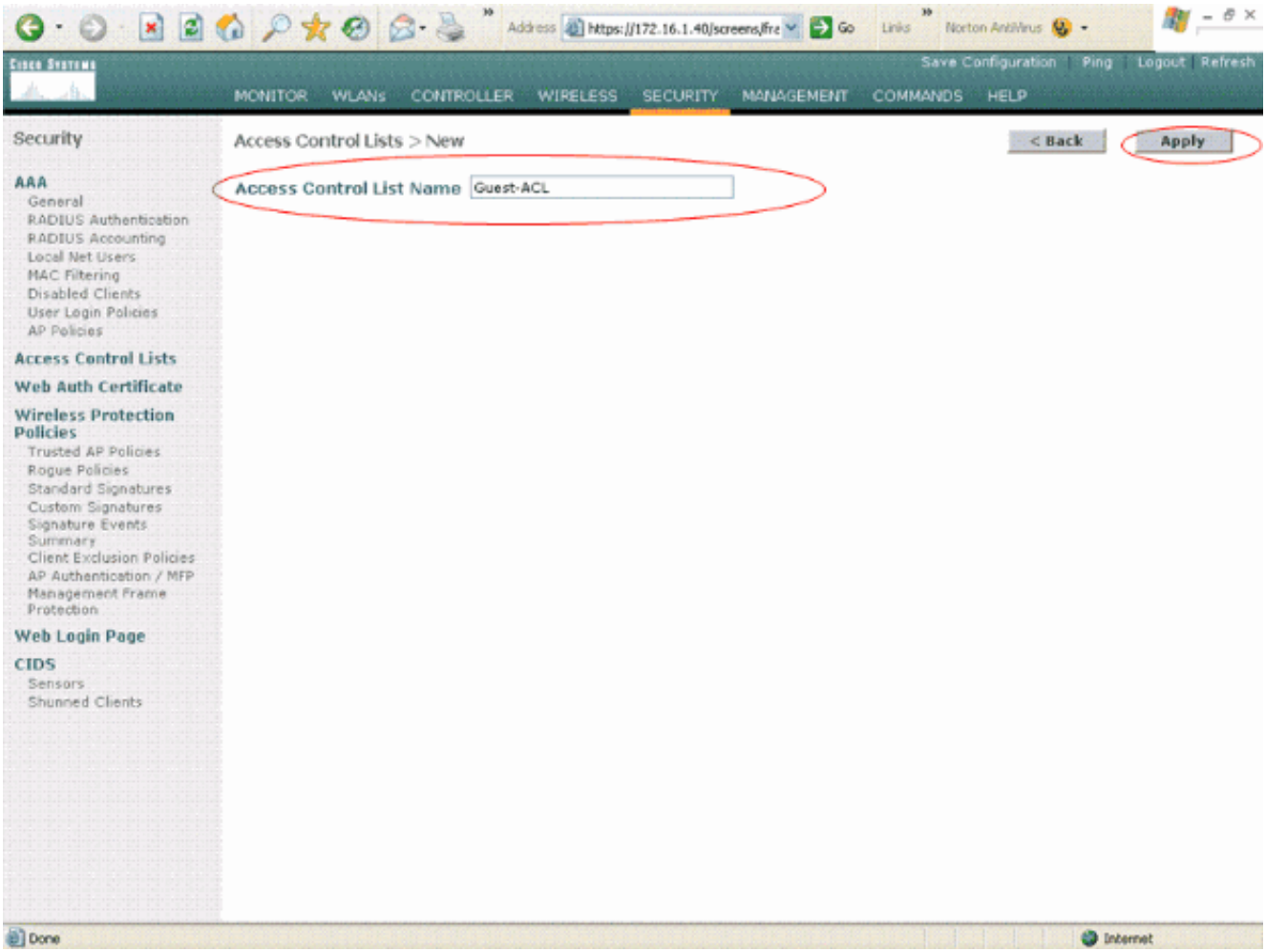
Alle andere services moeten worden geblokkeerd voor de draadloze clients. Voltooi deze stappen om ACL met WLC GUI te creëren:

1. Ga naar de WLC GUI en kies **Security > Access Control Lists**.De pagina Toegangscontrolelijsten verschijnt. Deze pagina maakt een lijst van de ACL's die op de WLC zijn geconfigureerd. Het laat u ook toe om het even welke ACLs uit te geven of te verwijderen. Klik op **Nieuw** om een nieuwe ACL te maken.



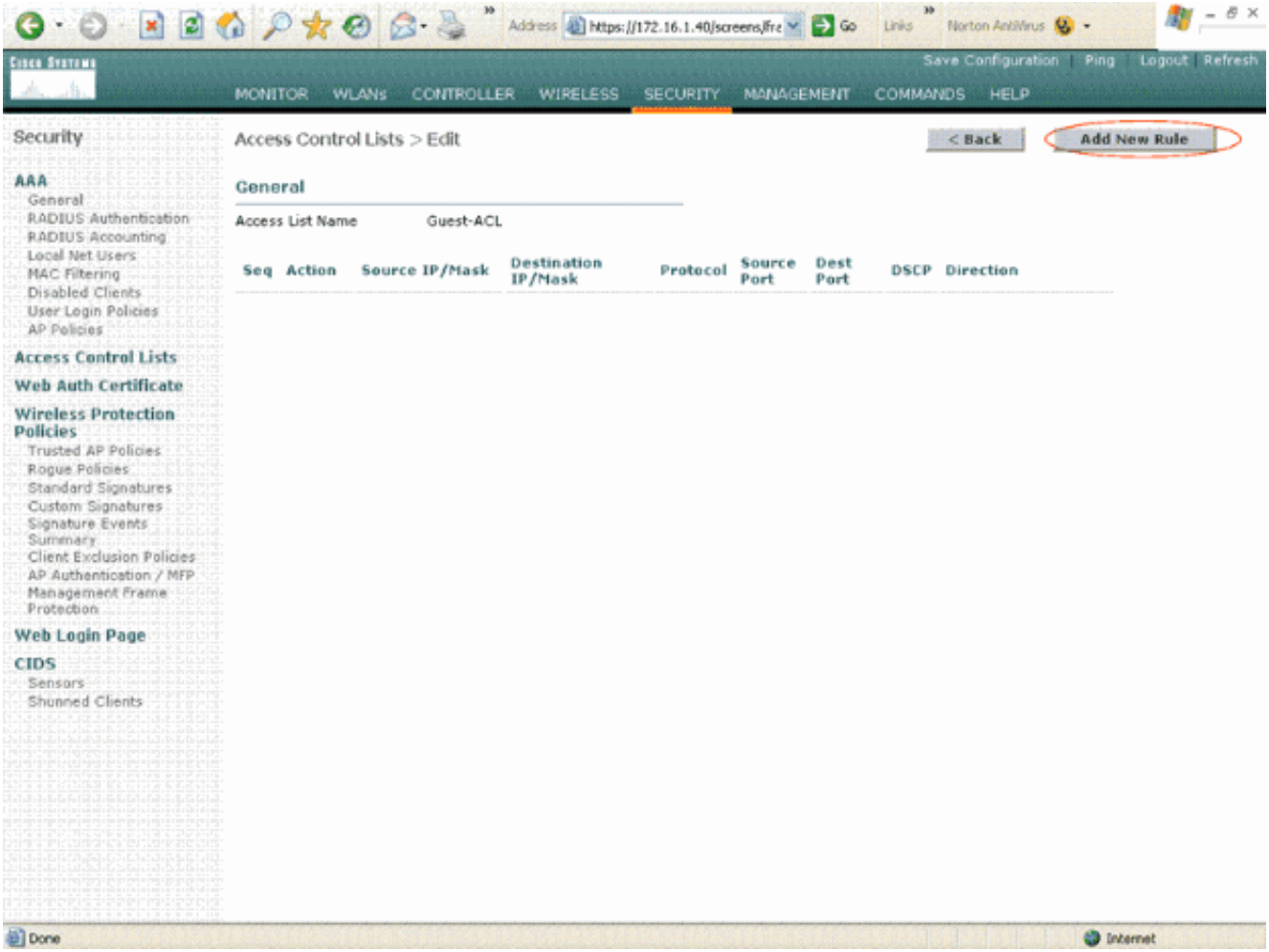
Toegangscontrolelijsten

2. Voer de naam van de ACL in en klik op **Toepassen**.U kunt maximaal 32 alfanumerieke tekens invoeren. In dit voorbeeld is de naam van de ACL **Guest-ACL**. Zodra de ACL is gemaakt, klikt u op **Bewerken** om regels voor de ACL te maken.



Voer de naam van de ACL in

3. Wanneer de pagina Toegangscontrolelijsten > Bewerken verschijnt, klikt u op **Nieuwe regel toevoegen**.De toegangscontrolelijsten > Regels > Nieuwe pagina verschijnt.



Nieuwe ACL-regels toevoegen

4. Configureer regels die een gastgebruiker deze services toestaan:DHCP tussen de draadloze clients en DHCP-serverICMP tussen alle apparaten in het netwerkDNS tussen de draadloze clients en de DNS-serverTelnet naar een specifieke subnetverbinding

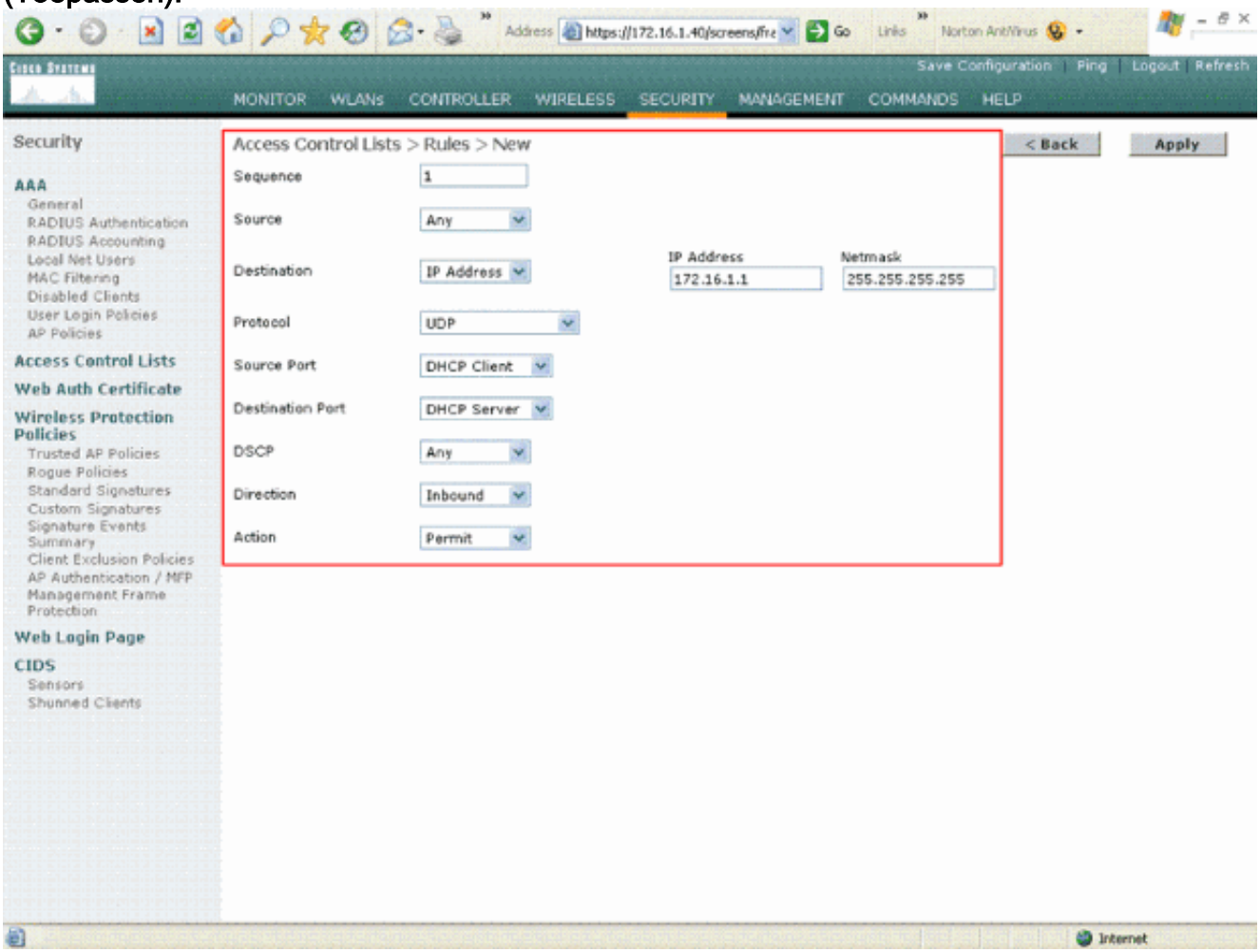
Regels configureren die gastgebruikersservices toestaan

Deze sectie toont een voorbeeld voor hoe te om de regels voor deze diensten te vormen:

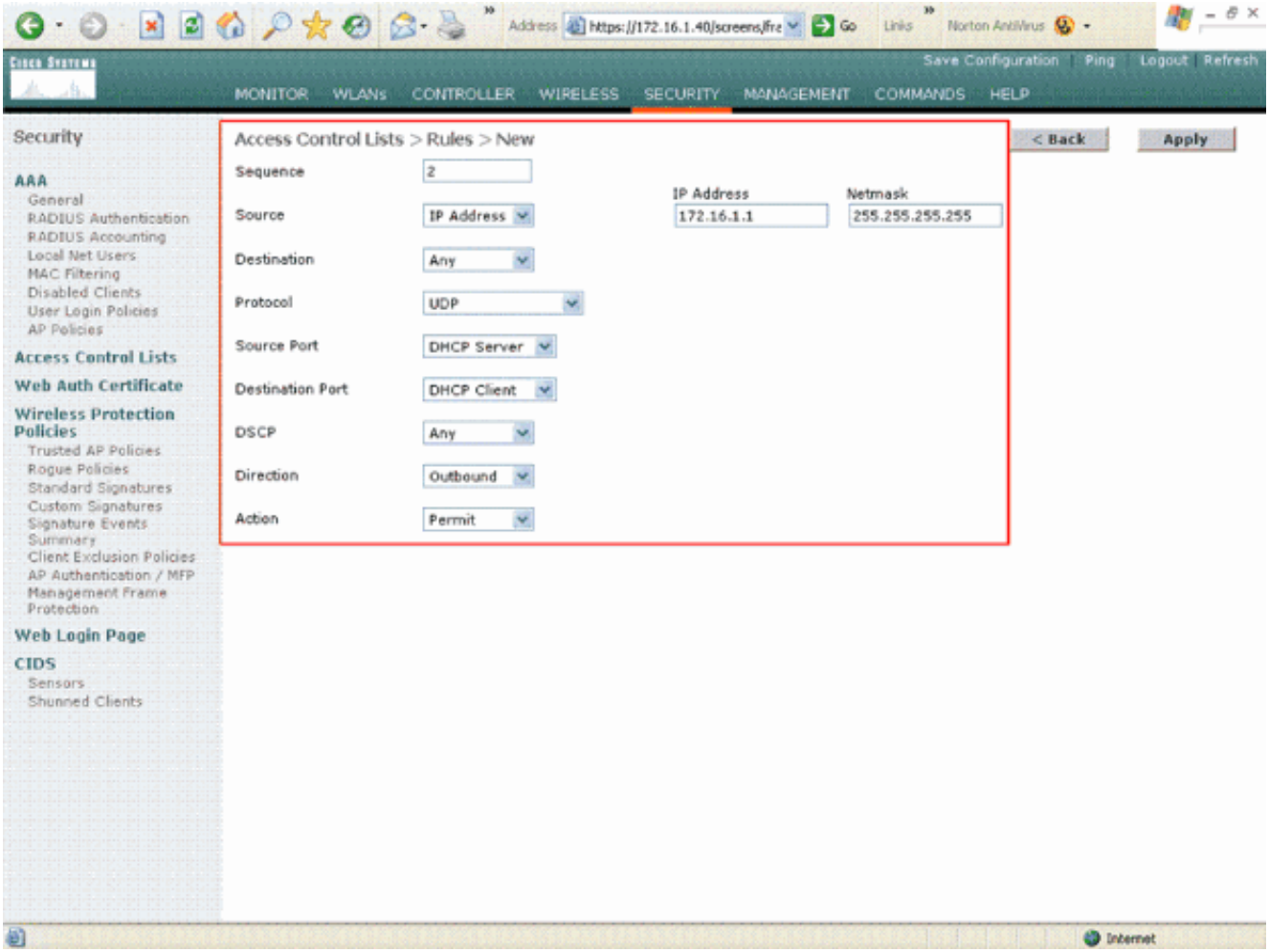
- DHCP tussen de draadloze clients en DHCP-server
- ICMP tussen alle apparaten in het netwerk
- DNS tussen de draadloze clients en de DNS-server
- Telnet naar een specifieke subnetverbinding

1. Selecteer het IP-bereik voor de bron en de bestemming om de regel voor DHCP-service te definiëren.In dit voorbeeld wordt **elke** bron gebruikt, wat betekent dat elke draadloze client toegang heeft tot de DHCP-server. In dit voorbeeld fungeert de server 172.16.1.1 als de DHCP- en DNS-server. Het IP-adres van de bestemming is dus 172.16.1.1/255.255.255.255 (met een hostmasker).Omdat DHCP een op UDP gebaseerd protocol is, selecteert u **UDP in** het veld Protocol vervolgkeuzelijst. Als u in de vorige stap TCP of UDP hebt gekozen, worden er twee extra parameters weergegeven: Source Port en Destination Port. Specificeer de bron- en doelpoortgegevens. Voor deze regel is de bronpoort de **DHCP-client** en de doelpoort is de **DHCP-server** .Kies de Richting waarin de ACL moet worden toegepast. Omdat deze regel van de client naar de server loopt, wordt in dit voorbeeld **Inbound** gebruikt. Kies in de vervolgkeuzelijst Actie de optie **Toestaan** om deze ACL te veroorzaken om DHCP-

pakketten toe te staan van de draadloze client naar de DHCP-server. De standaardwaarde is Deny. Klik op **Apply**
(Toepassen).

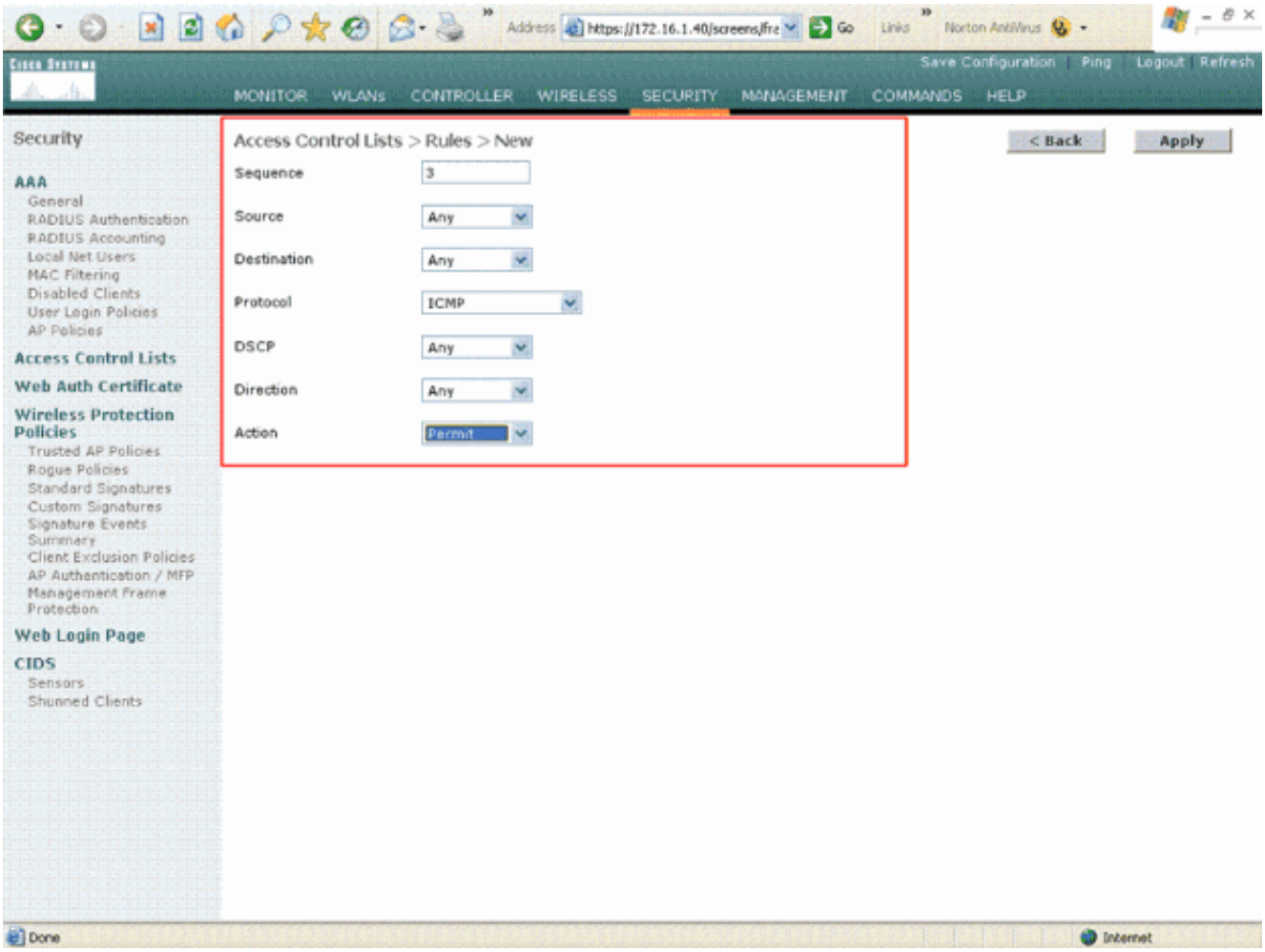


Selecteer Vergunning om ACL te veroorzaken om DHCP-pakketten toe te staan Als de bron of de bestemming niet **om het even welk** zijn, dan moet een omgekeerde verklaring in de tegenovergestelde richting worden tot stand gebracht. Hierna volgt een
voorbeeld.



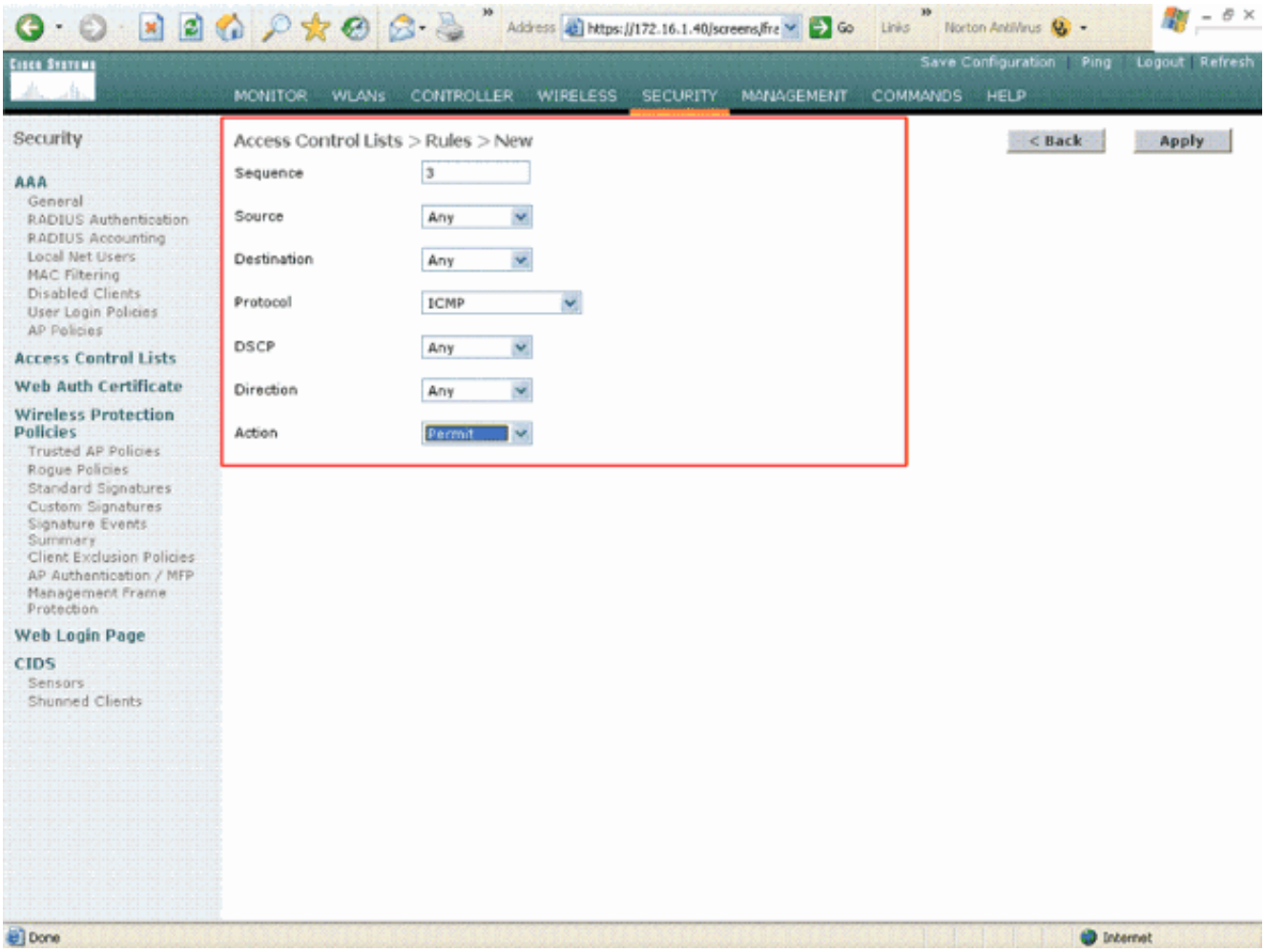
Bron of bestemming ingesteld op Any

2. Om een regel te definiëren die ICMP-pakketten tussen alle apparaten toestaat, selecteert u **een willekeurige regel** voor de velden Bron en Bestemming. Dit is de standaardwaarde.Kies **ICMP** in het veld Protocol. Omdat dit voorbeeld **om het even welk** voor de Bron en van de Bestemming velden gebruikt, moet u niet de richting specificeren. Het kan worden achtergelaten op de standaardwaarde van **elke** waarde. Ook is de omgekeerde stelling in de tegenovergestelde richting niet vereist.Kies in het vervolgkeuzemenu Actie de optie **Toestaan** om deze ACL te veroorzaken, zodat DHCP-pakketten van de DHCP-server naar de draadloze client worden toegestaan. Klik op Apply (Toepassen).

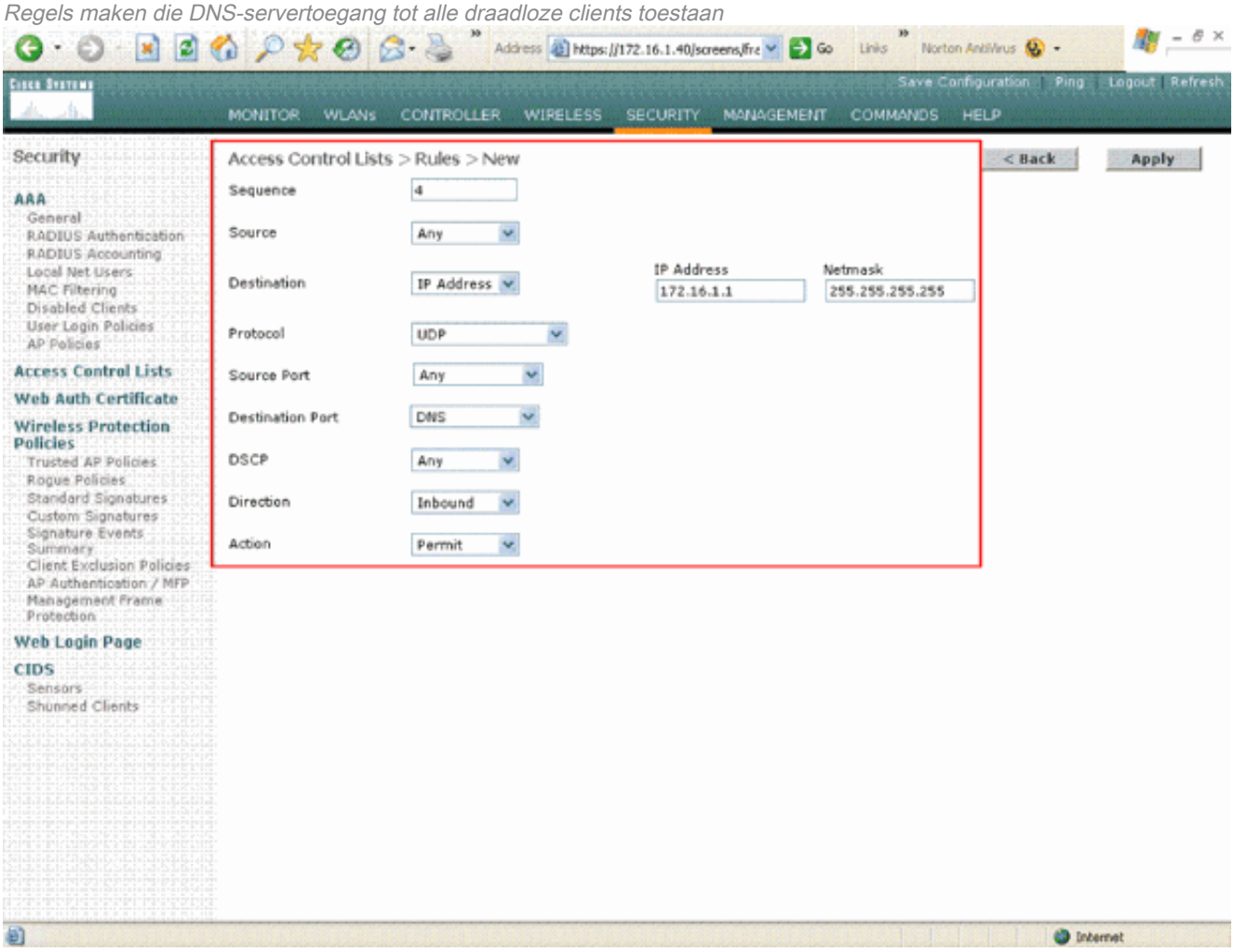


Vergunning om ACL te veroorzaken om DHCP-pakketten toe te staan van DHCP-server naar draadloze client

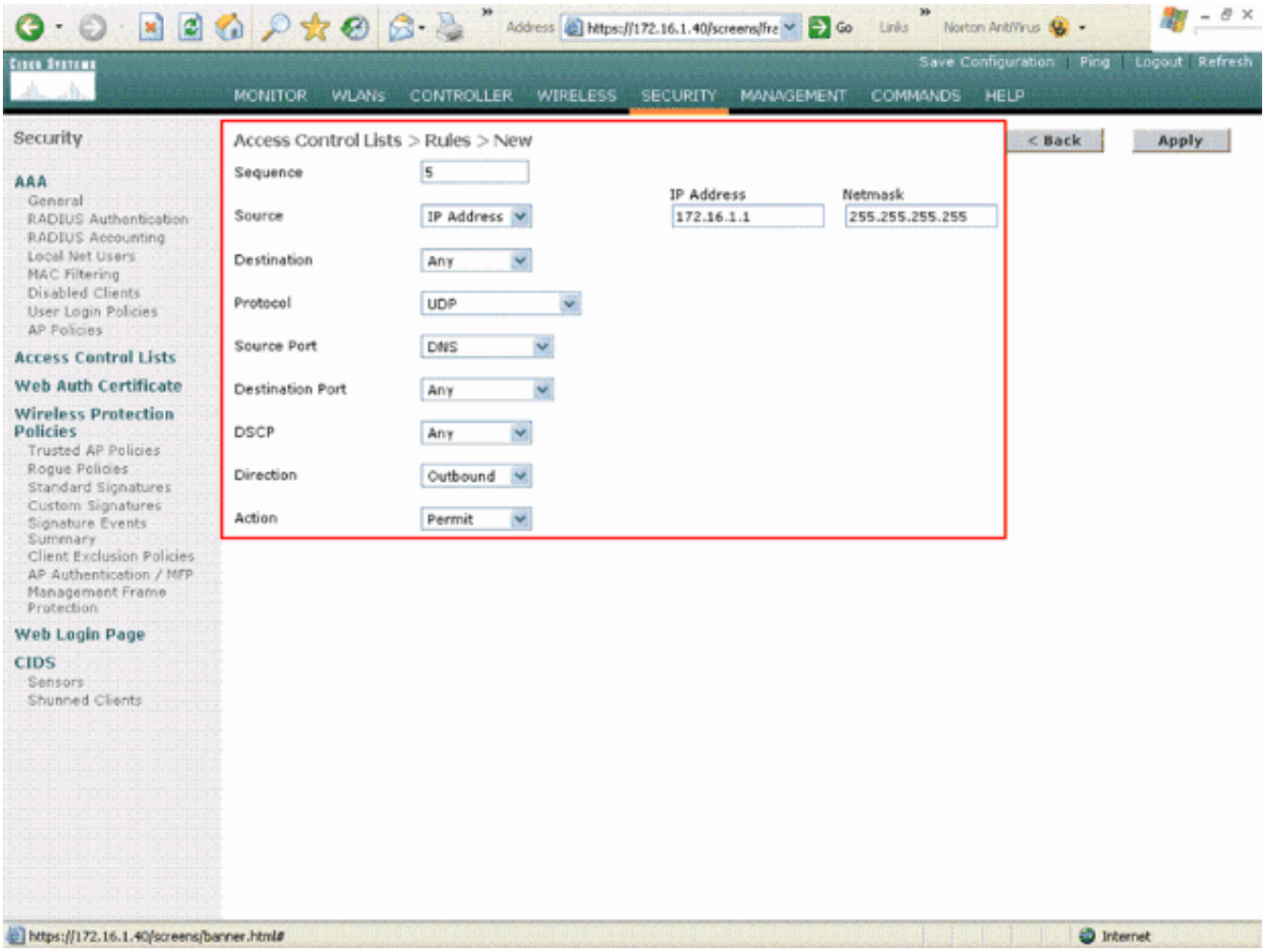
3. Op dezelfde manier creeer regels die DNS servertoegang tot alle draadloze cliënten en de servertoegang van Telnet voor de draadloze cliënt aan specifieke subnet verlenen. Hier zijn de
voorbeelden.



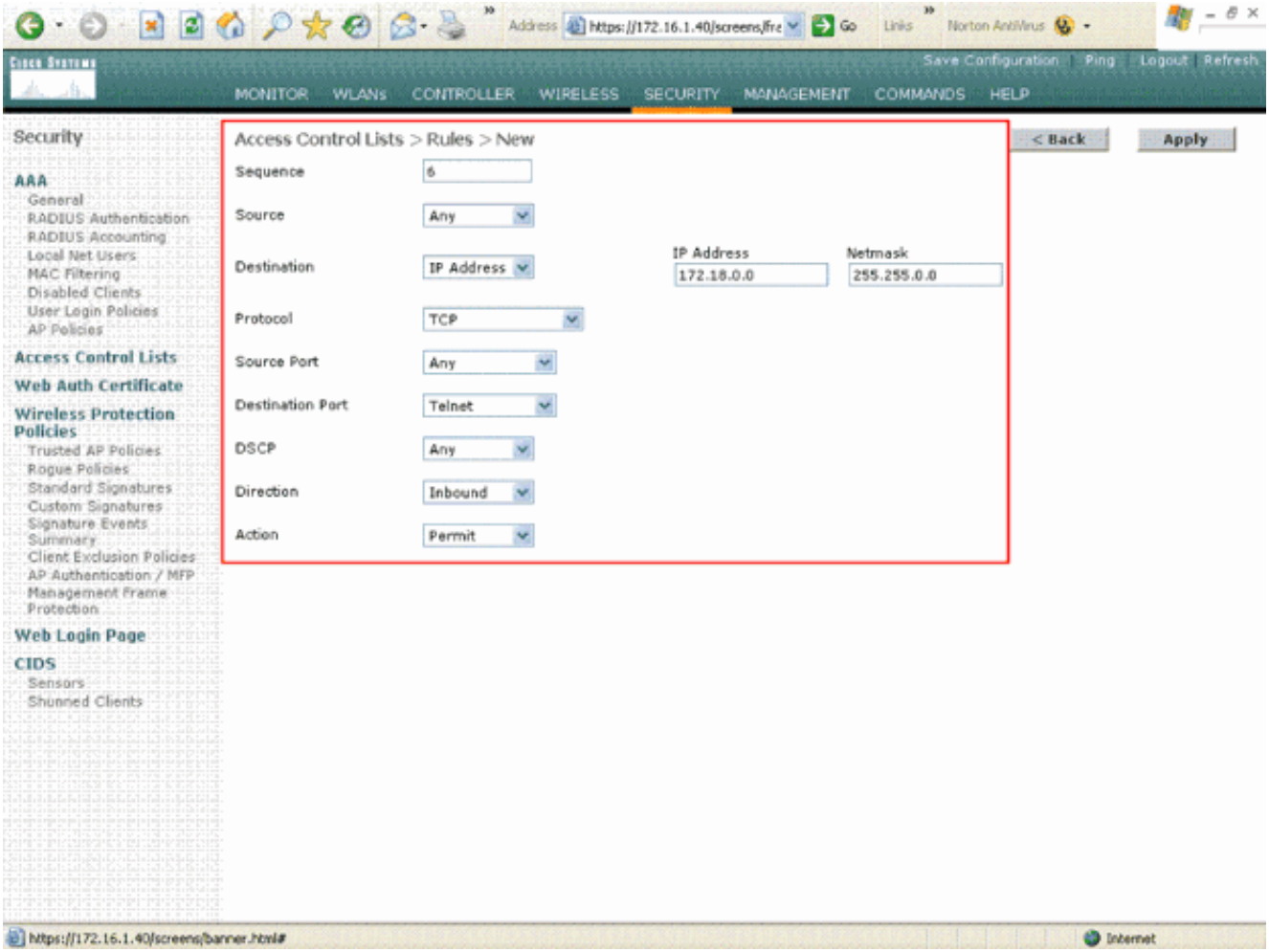
Regels maken die DNS-servertoegang tot alle draadloze clients toestaan



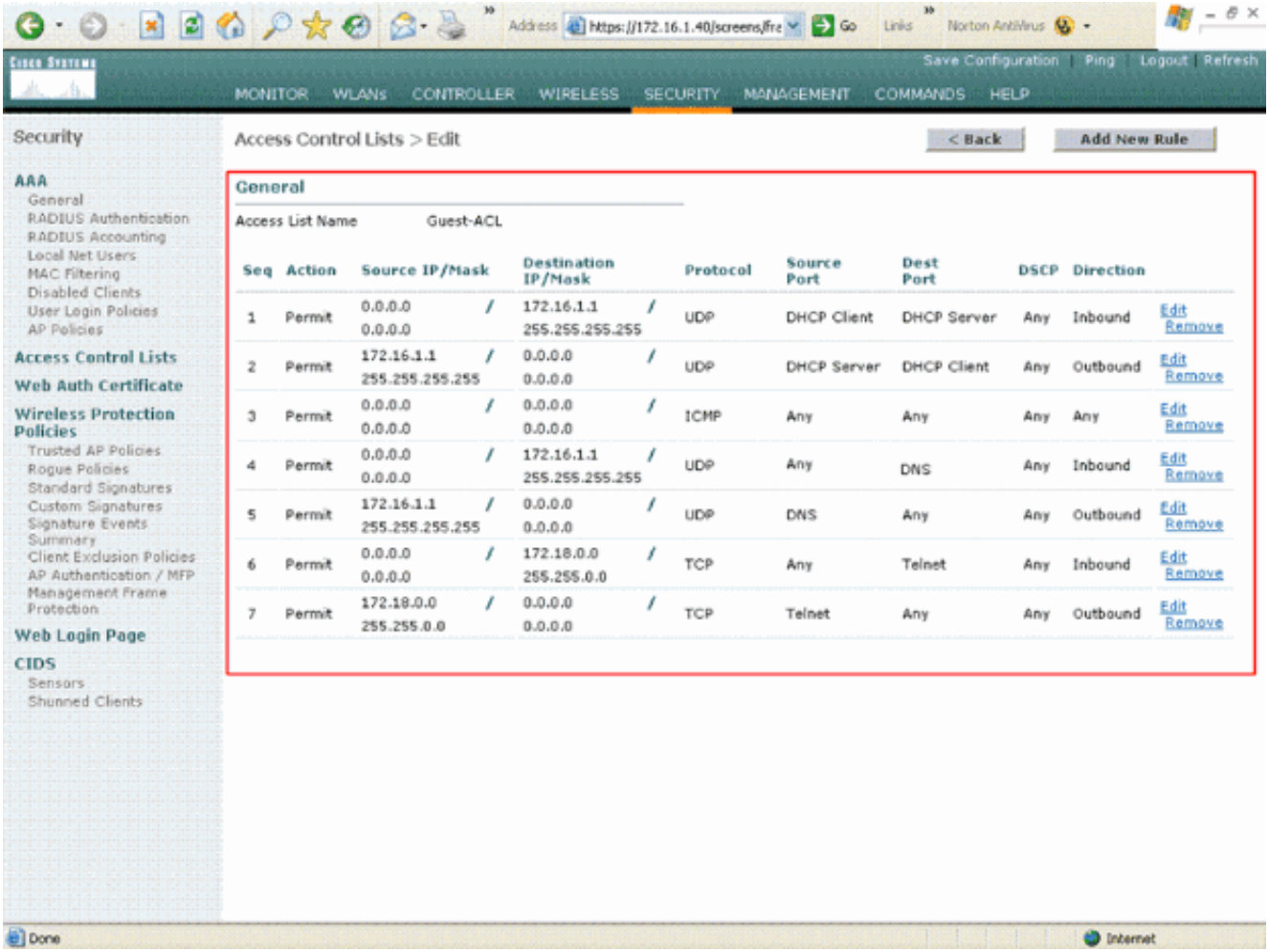
Regels maken die Telnet Server toegang voor de draadloze client tot een subnet toestaan Definieer deze regel om de draadloze client toegang te geven tot de Telnet-service.



Toestaan van toegang voor de draadloze client tot de Telnet-service

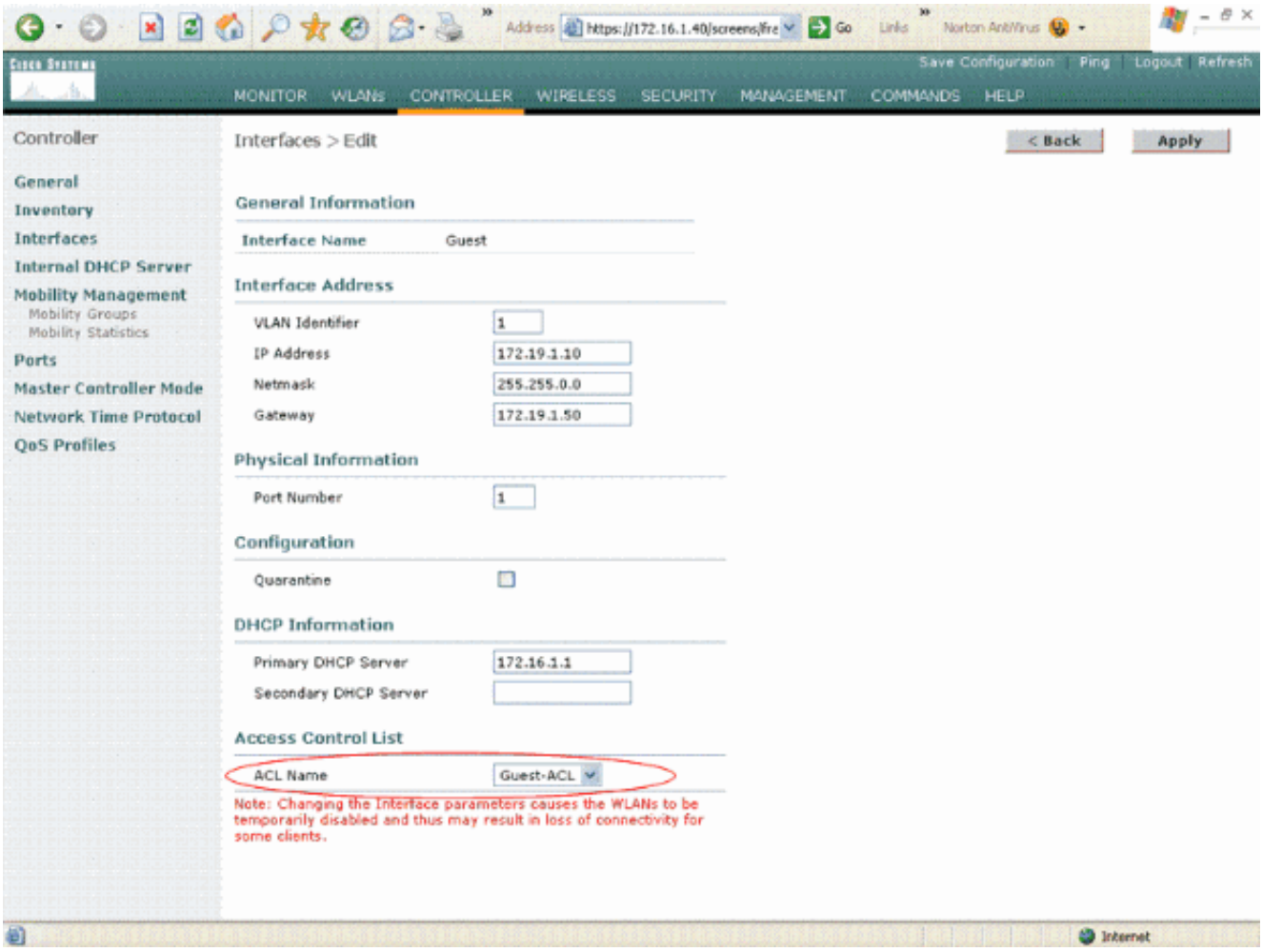


Een ander voorbeeld van draadloze clienttoegang tot de Telnet-service ACL **> Bewerk** pagina maakt een lijst van alle regels die voor ACL worden bepaald.



Pagina's bewerken Lijsten met alle regels die voor de ACL zijn gedefinieerd

4. Zodra ACL is gemaakt, moet deze worden toegepast op een dynamische interface. Om ACL toe te passen, kies **Controller > Interfaces** en bewerk de interface waarop u ACL wilt toepassen.
5. In de pagina **Interfaces > Bewerken** voor de dynamische interface kiest u de juiste ACL in het vervolgkeuzemenu Toegangscontrolelijsten. Hierna volgt een voorbeeld.



Kies de juiste ACL in het menu Toegangscontrolelijst

Zodra dit wordt gedaan, laat ACL verkeer (dat op de gevormde regels wordt gebaseerd) op WLAN toe en ontkent dat deze dynamische interface gebruikt. Interface-ACL kan alleen worden toegepast op H-Reap AP's in Connected Mode, maar niet in Standalone modus.

> **Opmerking**: in dit document wordt ervan uitgegaan dat WLAN's en dynamische interfaces zijn geconfigureerd. Raadpleeg VLAN's configureren op draadloze LAN-controllers of informatie over het maken van dynamische interfaces op WLC's.

CPU-ACL's configureren

Eerder hadden ACL's in WLC's geen optie om LWAP/CAPWAP-dataverkeer, LWAP/CAPWAP-controleverkeer en mobiliteitsverkeer te filteren dat bestemd is voor de interfaces Management en AP Manager. Om dit probleem aan te pakken en LWAPP en mobiliteitsverkeer te filteren, werden CPU ACL's geïntroduceerd met WLC firmware release 4.0.

De configuratie van CPU ACL's omvat twee stappen:

1. Configureer regels voor de CPU-ACL.
2. Pas de CPU ACL op de WLC toe.

De regels voor de CPU ACL moeten op dezelfde manier worden geconfigureerd als de andere ACL's.

Verifiëren

Cisco raadt u aan de ACL-configuraties met een draadloze client te testen om er zeker van te zijn dat u deze correct hebt geconfigureerd. Als zij er niet in slagen correct te werken, verifieer de ACL's op de ACL-webpagina en controleer dat uw ACL-wijzigingen werden toegepast op de controller-interface.

U kunt deze **show**bevelen ook gebruiken om uw configuratie te verifiëren:

- **toon acl samenvatting** —om de ACLs te tonen die op het controlemechanisme worden gevormd, gebruik het **show acl summiere** bevel.Hierna volgt een voorbeeld:

```
(Cisco Controller) >show acl summary

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

- **toon acl gedetailleerde ACL_Name** —Hier wordt gedetailleerde informatie over de geconfigureerde ACL's weergegeven.Hierna volgt een voorbeeld:

```
(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
```

- **toon acl cpu** —gebruik de opdracht **cpu** van de **show** om de ACL's weer te geven die op de CPU zijn geconfigureerd.Hierna volgt een voorbeeld:

```
(Cisco Controller) >show acl cpu

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

Problemen oplossen

Controller softwarerelease 4.2.x of hoger stelt u in staat om ACL-tellers te configureren. ACL-tellers kunnen helpen bepalen welke ACL's werden toegepast op pakketten die via de controller worden verzonden. Deze functie is handig wanneer u problemen met uw systeem oplost.

Er zijn ACL-tellers beschikbaar op deze controllers:

- 4400 Series

- Cisco WiSM
- Catalyst 3750G geïntegreerde draadloze LAN-controller Switch

Voltooi de volgende stappen om deze functie in te schakelen:

1. Kies **Beveiliging > Toegangscontrolelijsten > Toegangscontrolelijsten** om de pagina Toegangscontrolelijsten te openen.Deze pagina maakt een lijst van alle ACL's die voor deze controller zijn geconfigureerd.
2. Om te zien of pakketten een van de op uw controller geconfigureerde ACL's raken, schakelt u het aanvinkvakje **Tellers inschakelen in** en klikt u op **Toepassen** . Anders laat u het aankruisvakje onaangevinkt. Dit is de standaardwaarde.
3. Als u de tellers voor ACL wilt ontruimen, hang uw curseur over de blauwe vervolgkeuzepijl voor die ACL en kies **Duidelijke Tellers** .

Gerelateerde informatie

- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 6.0
- VLAN's configureren op draadloze LAN-controllers
- Een Lightweight AP troubleshooten dat niet wordt verbonden met een WLC
- Cisco technische ondersteuning en downloads

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.