Beispiel für die Konfiguration von ACLs auf einem Wireless LAN-Controller

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Zugriffskontrolllisten (ACLs) auf Wireless LAN-Controllern (WLAN) so konfigurieren, dass der Datenverkehr durch das WLAN gefiltert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren des WLC und des Lightweight Access Point (LAP) für den Grundbetrieb
- Grundkenntnisse von LWAPP (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco WLC der Serie 2000 mit Firmware 4.0
- Cisco Serie 1000 - LAP
- Cisco 802.11a/b/g Wireless Client-Adapter für Firmware 2.6
- Cisco Aironet Desktop Utility (ADU) Version 2.6

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

ACLs auf WLCs

ACLs auf dem WLC sollen Wireless-Clients die Nutzung von Services im WLAN einschränken oder gestatten.

Vor der WLC-Firmware-Version 4.0 werden ACLs auf der Management-Schnittstelle umgangen. Sie können daher den Datenverkehr zum WLC nicht beeinflussen. Sie können Wireless-Clients nur mit der Option **"Management Via Wireless"** an der Verwaltung des Controllers hindern. Daher können ACLs nur auf dynamische Schnittstellen angewendet werden. In der WLC-Firmware-Version 4.0 gibt es CPU-ACLs, die Datenverkehr filtern können, der für die Management-Schnittstelle bestimmt ist. Weitere Informationen finden Sie im Abschnitt Konfigurieren von CPU-Zugriffskontrolllisten.

Sie können bis zu 64 ACLs mit jeweils bis zu 64 Regeln (oder Filtern) definieren. Jede Regel verfügt über Parameter, die ihre Aktion beeinflussen. Wenn ein Paket mit allen Parametern für eine Regel übereinstimmt, wird der Aktionssatz für diese Regel auf das Paket angewendet. Sie können ACLs entweder über die Benutzeroberfläche oder die CLI konfigurieren.

Dies sind einige der Regeln, die Sie beachten müssen, bevor Sie eine ACL auf dem WLC konfigurieren:

- Wenn die Quelle und das Ziel **any** sind, kann die Richtung, in der diese ACL angewendet wird, **any** sein.
- Wenn entweder die Quelle oder das Ziel **keine** ist, muss die Richtung des Filters angegeben werden, und es muss eine umgekehrte Anweisung erstellt werden.
- Der WLC-Begriff für ein- und ausgehenden Datenverkehr ist nicht intuitiv. Sie ist aus der Perspektive des WLC zum Wireless-Client gerichtet, nicht aus der Perspektive des Clients. Eingehende Richtung bezeichnet ein Paket, das vom Wireless-Client in den WLC eingeht, und ausgehende Richtung ein Paket, das vom WLC zum Wireless-Client ausgeht.
- Am Ende der ACL wird implizit "deny" (Ablehnen) angezeigt.

Überlegungen zur Konfiguration von ACLs in WLCs

ALCs in WLCs funktionieren anders als bei Routern. Bei der Konfiguration von ACLs in WLCs sollten Sie Folgendes berücksichtigen:

- Der häufigste Fehler besteht darin, IP auszuwählen, wenn Sie IP-Pakete ablehnen oder zulassen möchten. Da Sie auswählen, was sich innerhalb des IP-Pakets befindet, können Sie IP-in-IP-Pakete ablehnen oder zulassen.
- Controller-ACLs können die virtuelle WLC-IP-Adresse und somit DHCP-Pakete für Wireless-

Clients nicht blockieren.

- Controller-ACLs können Multicast-Datenverkehr, der von kabelgebundenen Netzwerken empfangen wird und für Wireless-Clients bestimmt ist, nicht blockieren. Controller-ACLs werden für Multicast-Datenverkehr verarbeitet, der von Wireless-Clients initiiert wird und für kabelgebundene Netzwerke oder andere Wireless-Clients auf demselben Controller bestimmt ist.
- Im Gegensatz zu Routern steuert die ACL den Datenverkehr bei Anwendung auf eine Schnittstelle in beide Richtungen, führt aber keine Stateful-Firewall-Funktionalität aus. Wenn Sie vergessen, eine Öffnung in der ACL für den zurückkehrenden Datenverkehr vorzunehmen, tritt ein Problem auf.
- Controller-ACLs blockieren nur IP-Pakete. Sie können Layer-2-ACLs oder Layer-3-Pakete, die keine IP-Adressen sind, nicht blockieren.
- Controller-ACLs verwenden keine inversen Masken wie die Router. 255 bedeutet hier, dass sie genau mit dem Oktett der IP-Adresse übereinstimmen.
- ACLs auf dem Controller werden mithilfe von Software erstellt und beeinträchtigen die Weiterleitungsleistung.

  Hinweis: Wenn Sie eine ACL auf eine Schnittstelle oder ein WLAN anwenden, wird der Wireless-Durchsatz beeinträchtigt, und es kann zu Paketverlusten kommen. Um den Durchsatz zu verbessern, entfernen Sie die ACL von der Schnittstelle oder dem WLAN, und verschieben Sie die ACL auf ein benachbartes kabelgebundenes Gerät.

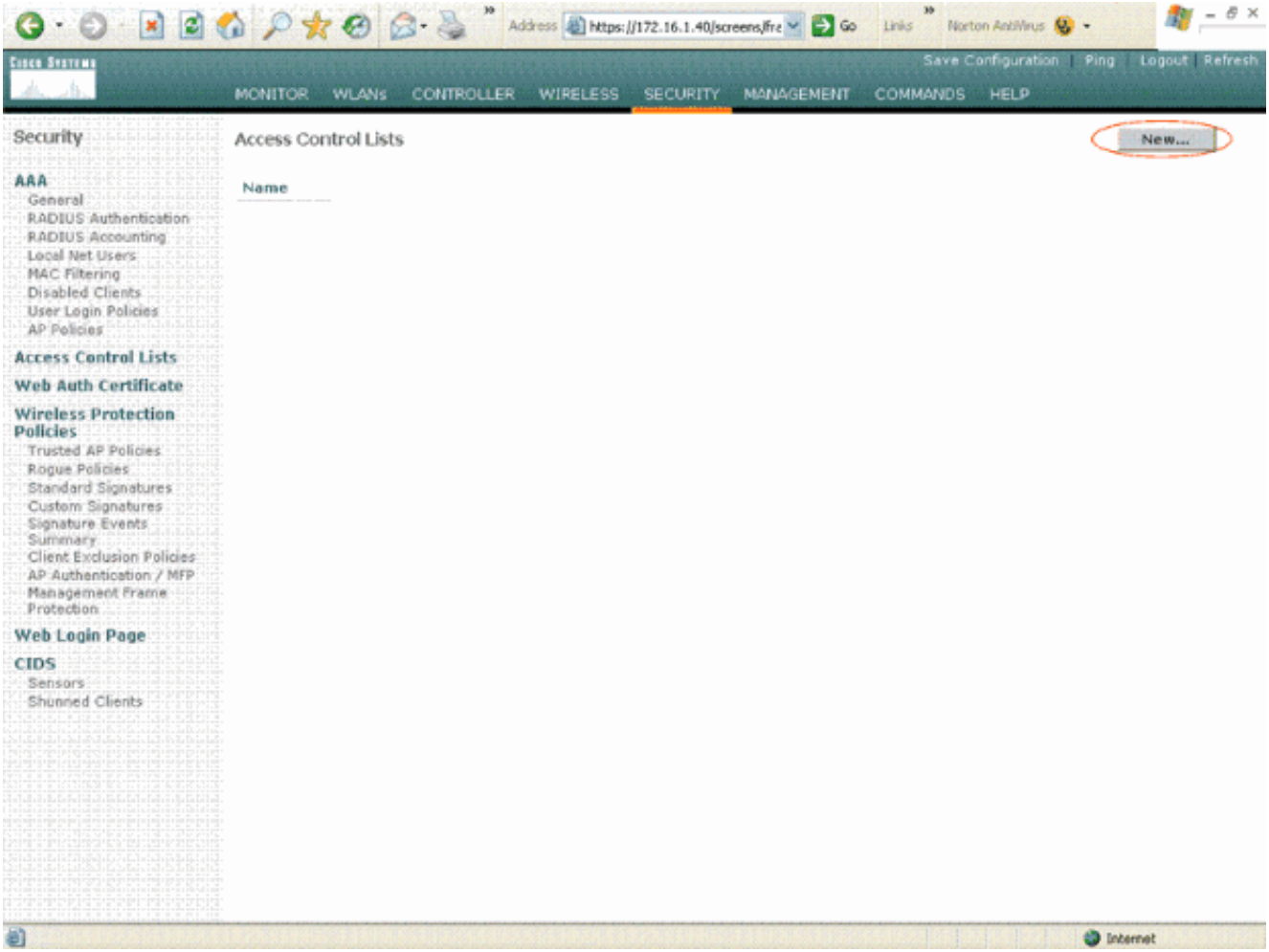
Konfigurieren der ACL auf WLCs

In diesem Abschnitt wird beschrieben, wie Sie eine ACL auf dem WLC konfigurieren. Das Ziel besteht in der Konfiguration einer ACL, die Gastclients den Zugriff auf folgende Dienste ermöglicht:

- Dynamic Host Configuration Protocol (DHCP) zwischen Wireless-Clients und DHCP-Server
- Internet Control Message Protocol (ICMP) zwischen allen Geräten im Netzwerk
- Domain Name System (DNS) zwischen den Wireless-Clients und dem DNS-Server
- Telnet zu einem bestimmten Subnetz

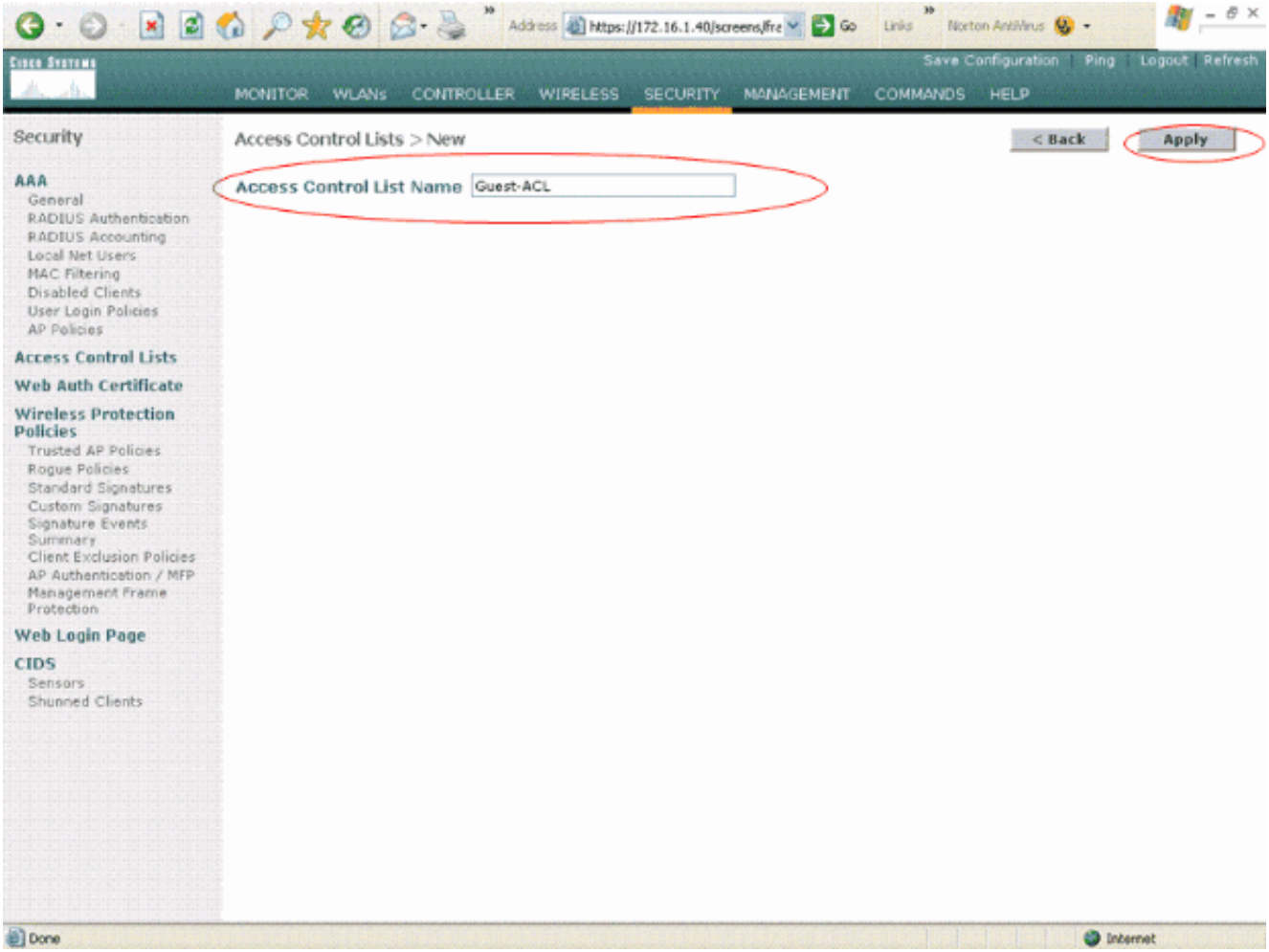
Alle anderen Dienste müssen für die Wireless-Clients blockiert werden. Gehen Sie wie folgt vor, um die ACL mit der WLC-GUI zu erstellen:

1. Öffnen Sie die WLC-GUI, und wählen Sie **Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten)**.Die Seite "Access Control Lists" (Zugriffskontrolllisten) wird angezeigt. Auf dieser Seite werden die auf dem WLC konfigurierten ACLs aufgelistet. Außerdem können Sie damit ACLs bearbeiten oder entfernen. Um eine neue ACL zu erstellen, klicken Sie auf **Neu**
   .



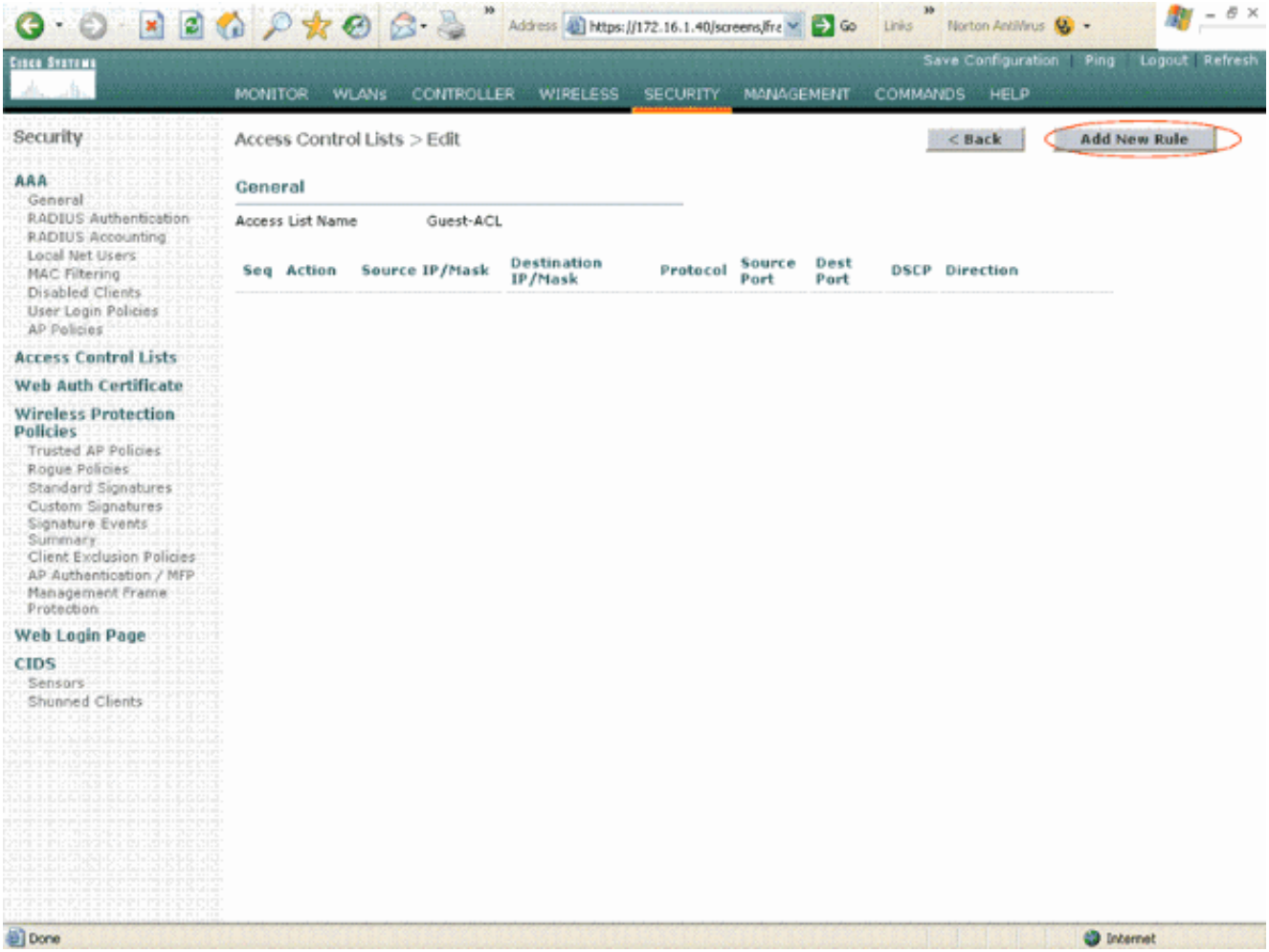
Zugriffskontrolllisten

2. Geben Sie den Namen der ACL ein, und klicken Sie auf **Apply**.Sie können bis zu 32 alphanumerische Zeichen eingeben. In diesem Beispiel lautet der Name der ACL **Guest-ACL** . Klicken Sie nach dem Erstellen der ACL auf **Edit**, um Regeln für die ACL zu erstellen.



Geben Sie den Namen der ACL ein.

3. Wenn die Seite Zugriffskontrolllisten > Bearbeiten angezeigt wird, klicken Sie auf **Neue Regel hinzufügen**.Die Seite Zugriffskontrolllisten > Regeln > Neu wird angezeigt.



Neue ACL-Regeln hinzufügen

4. Konfigurieren Sie Regeln, die Gastbenutzern die folgenden Dienste erlauben:DHCP zwischen Wireless-Clients und DHCP-ServerICMP zwischen allen Geräten im NetzwerkDNS zwischen Wireless-Clients und DNS-ServerTelnet zu einem bestimmten Subnetz

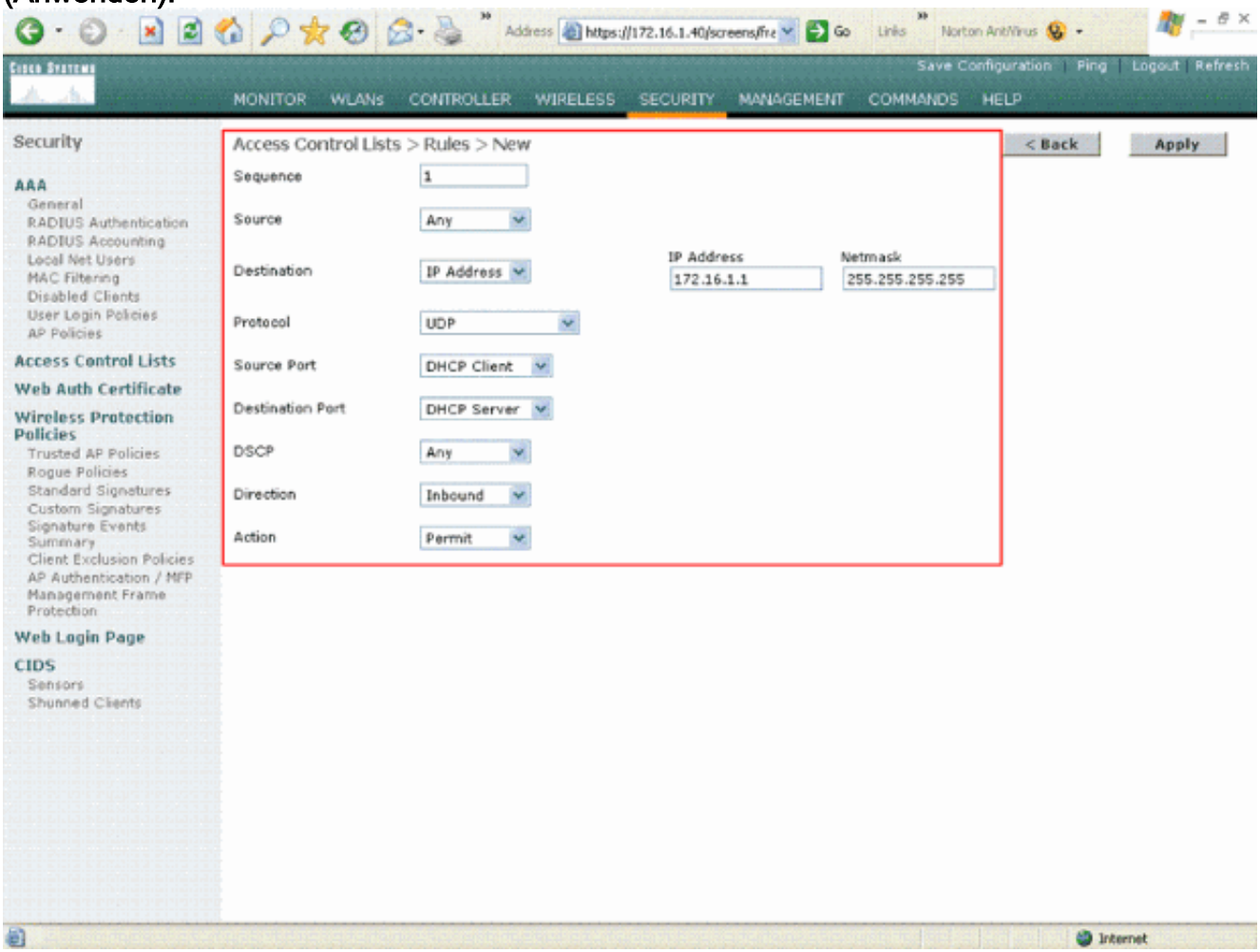
Konfigurieren von Regeln, die Gastbenutzerdienste zulassen

Dieser Abschnitt zeigt ein Beispiel für die Konfiguration der Regeln für diese Dienste:

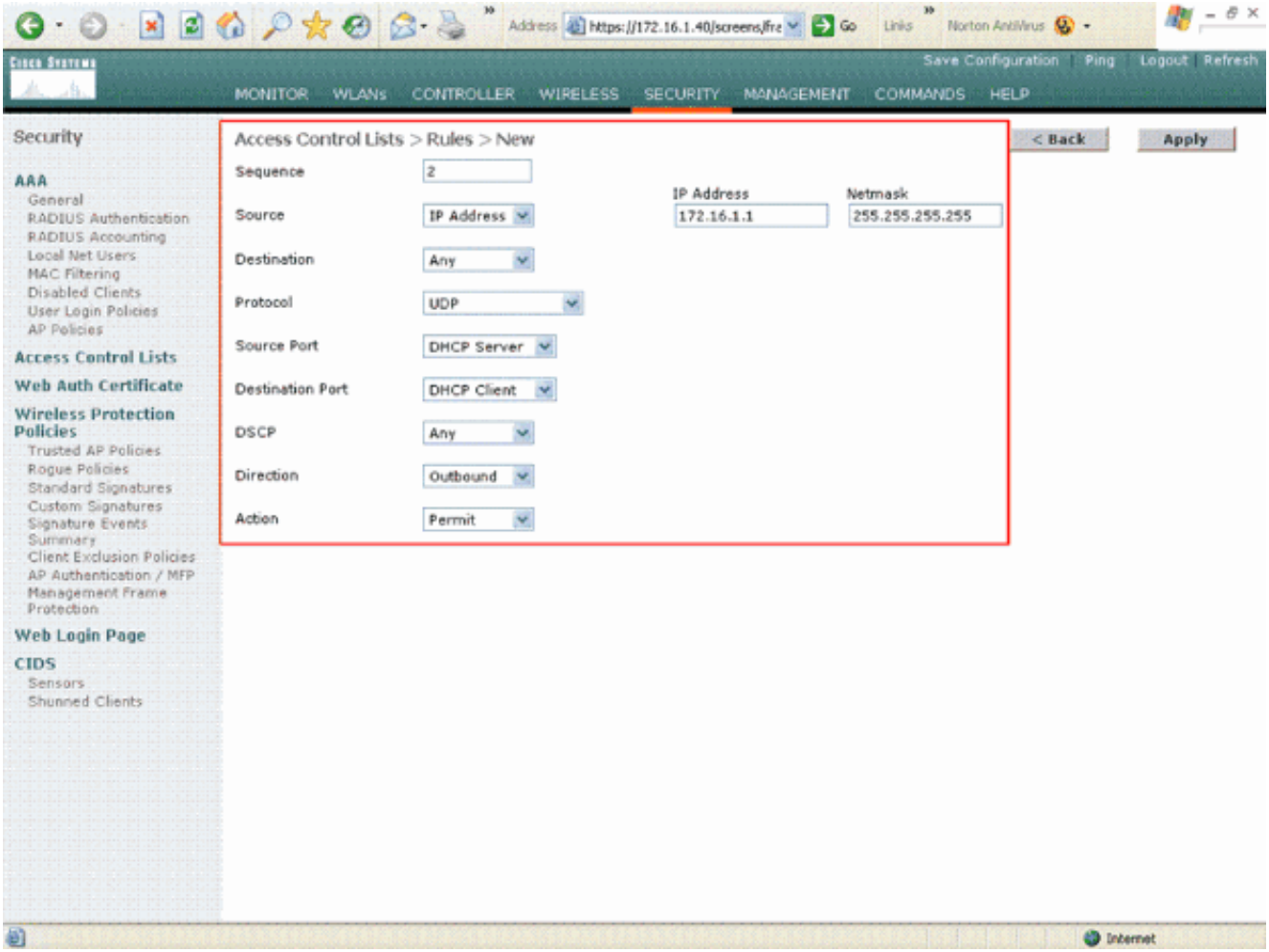
- DHCP zwischen Wireless-Clients und DHCP-Server
- ICMP zwischen allen Geräten im Netzwerk
- DNS zwischen Wireless-Clients und DNS-Server
- Telnet zu einem bestimmten Subnetz

1. Um die Regel für den DHCP-Service zu definieren, wählen Sie den Quell- und den Ziel-IP-Bereich aus.In diesem Beispiel wird für die Quelle **any** verwendet, was bedeutet, dass jedem Wireless-Client der Zugriff auf den DHCP-Server erlaubt wird. In diesem Beispiel fungiert der Server 172.16.1.1 als DHCP- und DNS-Server. Die Ziel-IP-Adresse lautet also 172.16.1.1/255.255.255.255 (mit einer Hostmaske).Da DHCP ein UDP-basiertes Protokoll ist, wählen Sie **UDP** aus dem Dropdown-Feld Protocol (Protokoll) aus. Wenn Sie im vorherigen Schritt TCP oder UDP ausgewählt haben, werden zwei zusätzliche Parameter angezeigt: Quellport und Zielport. Geben Sie die Details für den Quell- und Ziel-Port an. Bei dieser Regel ist der Quell-Port der **DHCP-Client** und der Ziel-Port der **DHCP-Server** .Wählen Sie die Richtung aus, in die die ACL angewendet werden soll. Da diese Regel vom Client zum Server gilt, wird in diesem Beispiel **Inbound** verwendet. Wählen Sie im Dropdown-Feld

Aktion die Option **Zulassen,** damit diese ACL DHCP-Pakete vom Wireless-Client zum DHCP-Server zulässt. Der Standardwert ist "Verweigern". Klicken Sie auf **Apply (Anwenden).**

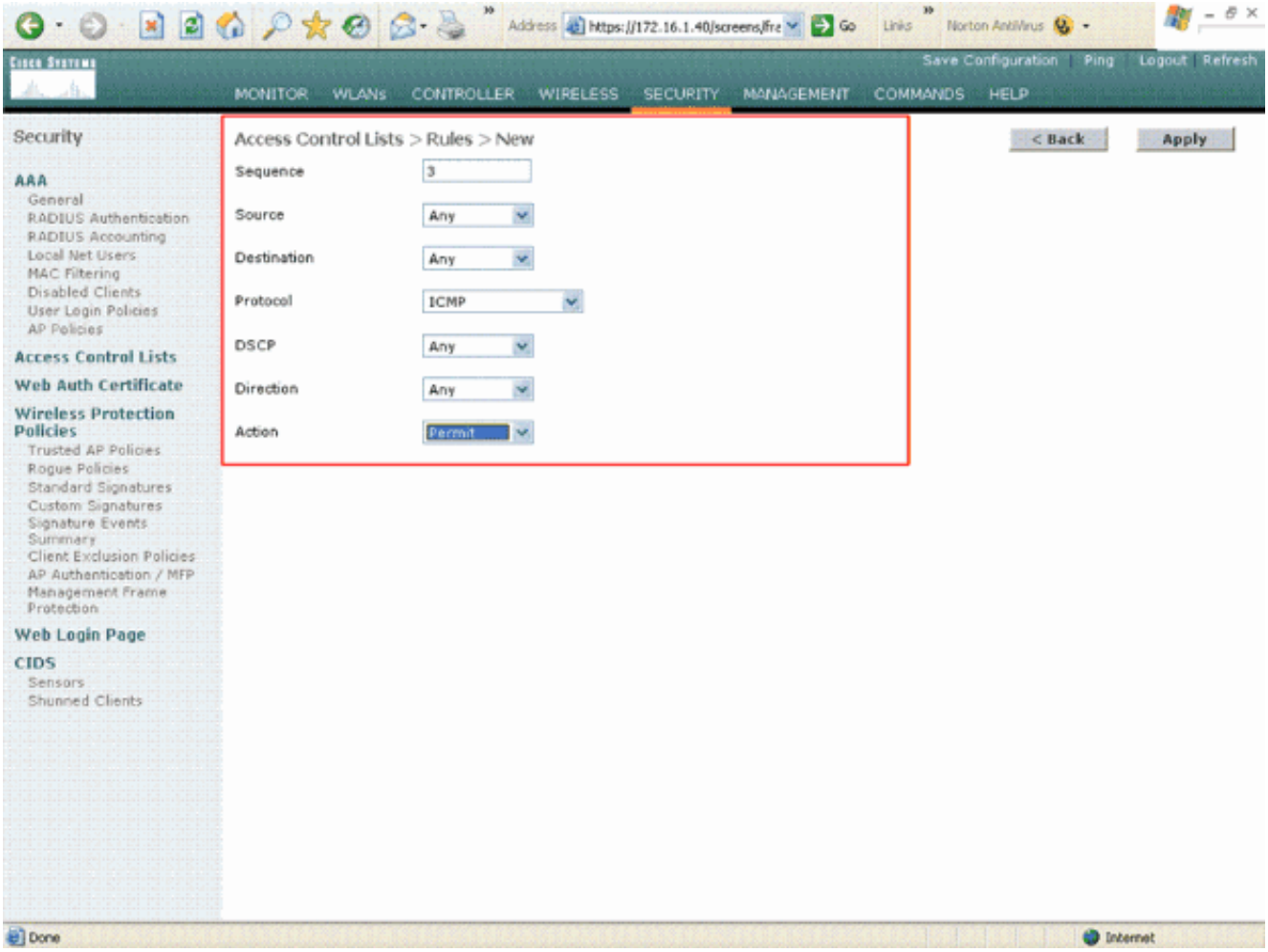


Wählen Sie Zulassen, dass die ACL DHCP-Pakete zulässt. Wenn entweder die Quelle oder das Ziel **keine** ist, muss eine umgekehrte Anweisung erstellt werden. Hier ein Beispiel.



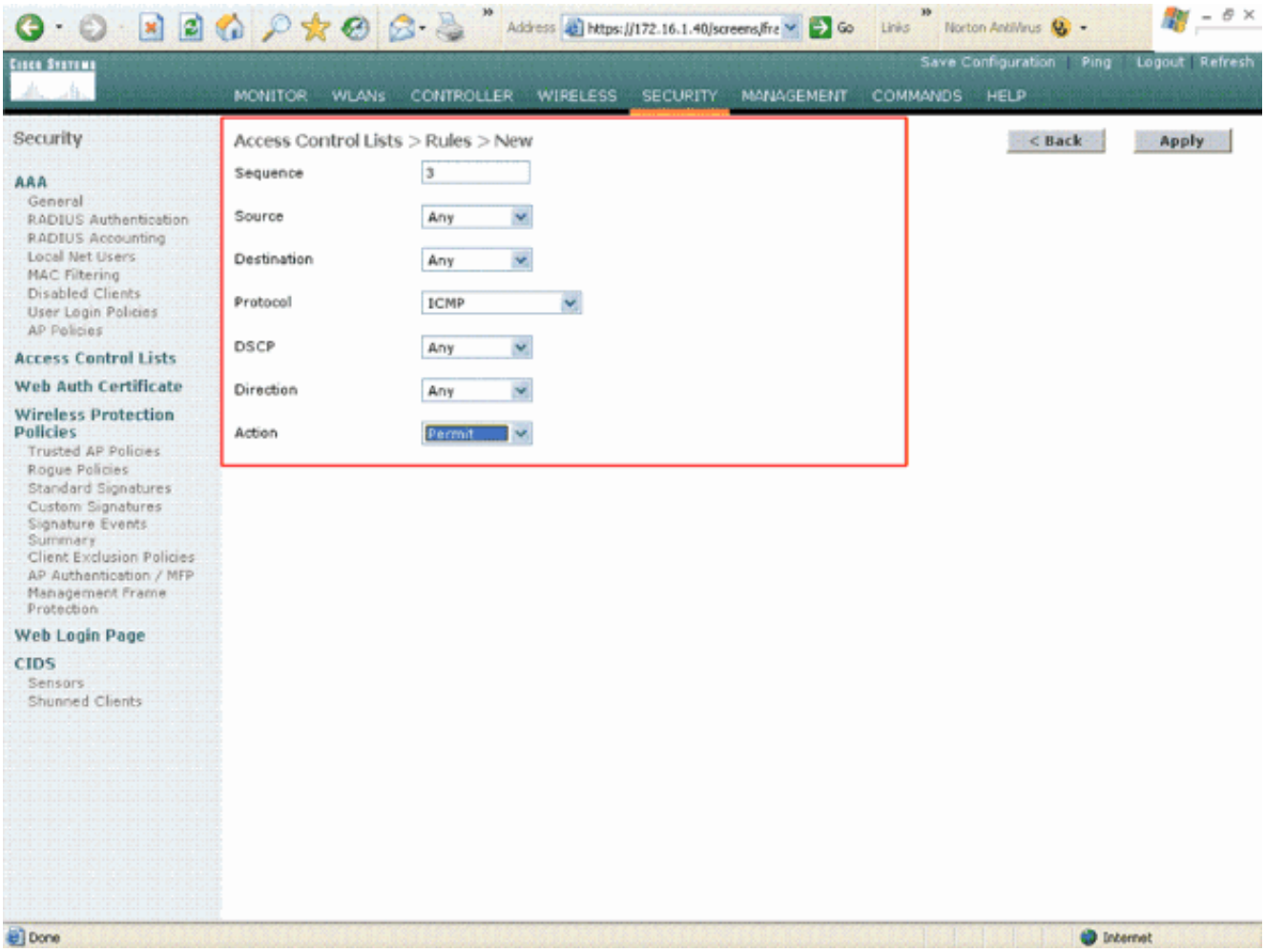
Quelle oder Ziel auf Any (Beliebig) festgelegt

2. Um eine Regel zu definieren, die ICMP-Pakete zwischen allen Geräten zulässt, wählen Sie in den Feldern "Quelle" und "Ziel" **eine beliebige** aus. Dies ist der Standardwert.Wählen Sie **ICMP** aus dem Dropdown-Feld "Protokoll" aus. Da in diesem Beispiel für die Felder "Quelle" und "Ziel" **any** verwendet wird, müssen Sie die Richtung nicht angeben. Der Standardwert **any** kann beibehalten werden. Außerdem ist die umgekehrte Anweisung nicht erforderlich.Wählen Sie im Dropdown-Menü Action (Aktion) die Option **Permit (Zulassen) aus,** damit diese ACL DHCP-Pakete vom DHCP-Server an den Wireless-Client zulässt. Klicken Sie auf Apply
(Anwenden).

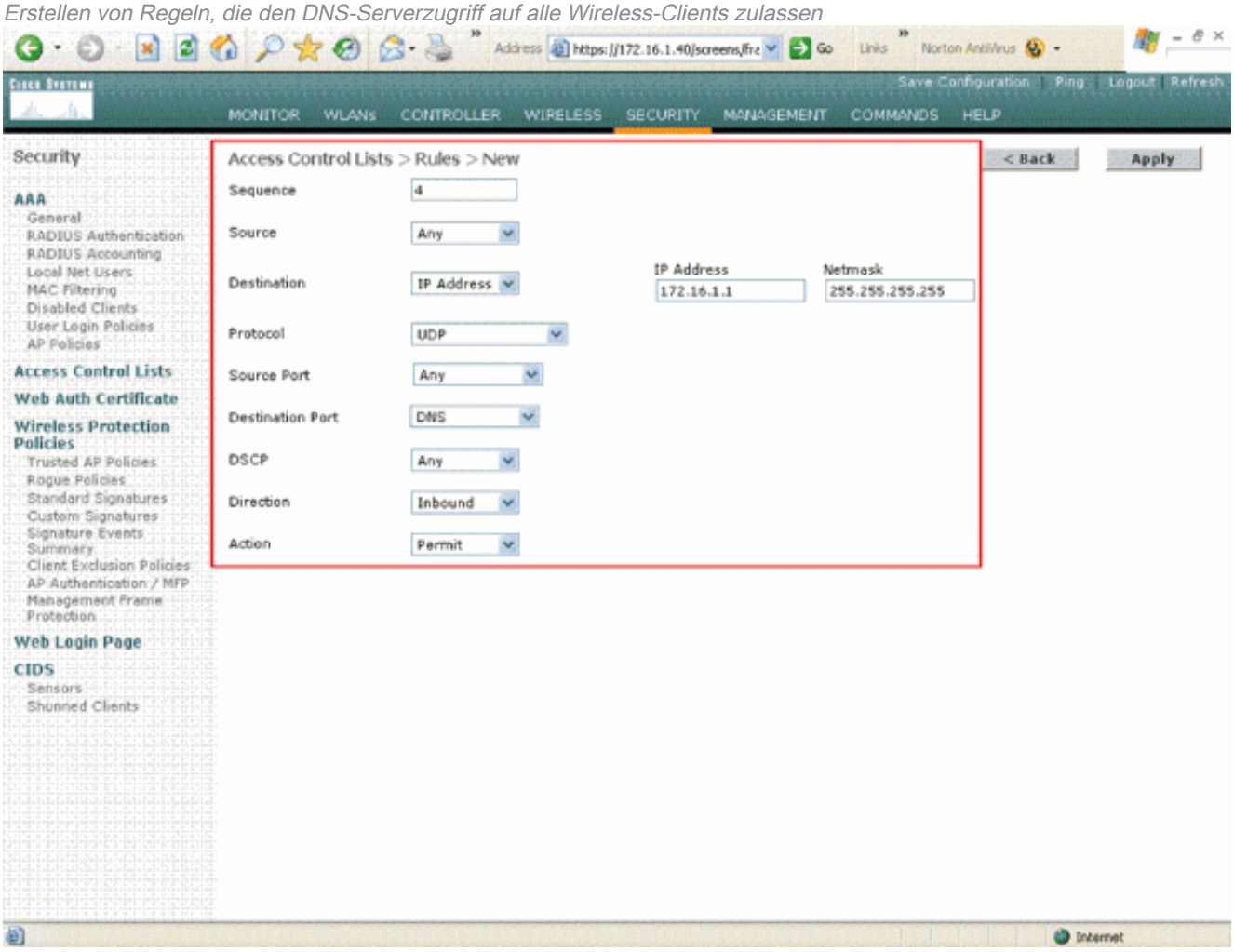


Zulassen, dass die ACL DHCP-Pakete vom DHCP-Server zum Wireless-Client zulässt

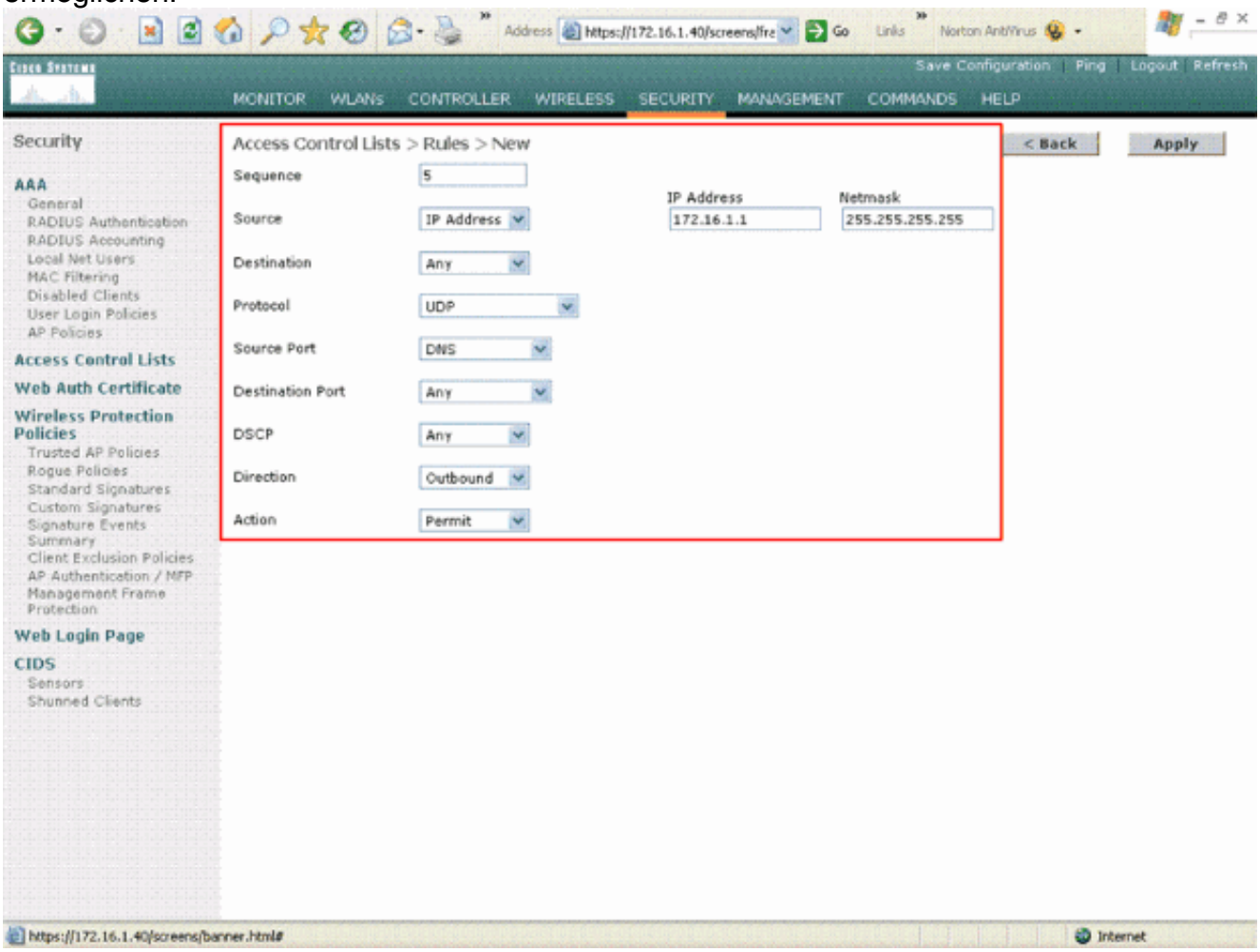
3. Erstellen Sie auf ähnliche Weise Regeln, die den DNS-Serverzugriff auf alle Wireless-Clients und den Telnet-Serverzugriff für den Wireless-Client auf ein bestimmtes Subnetz ermöglichen. Hier sind die
Beispiele.



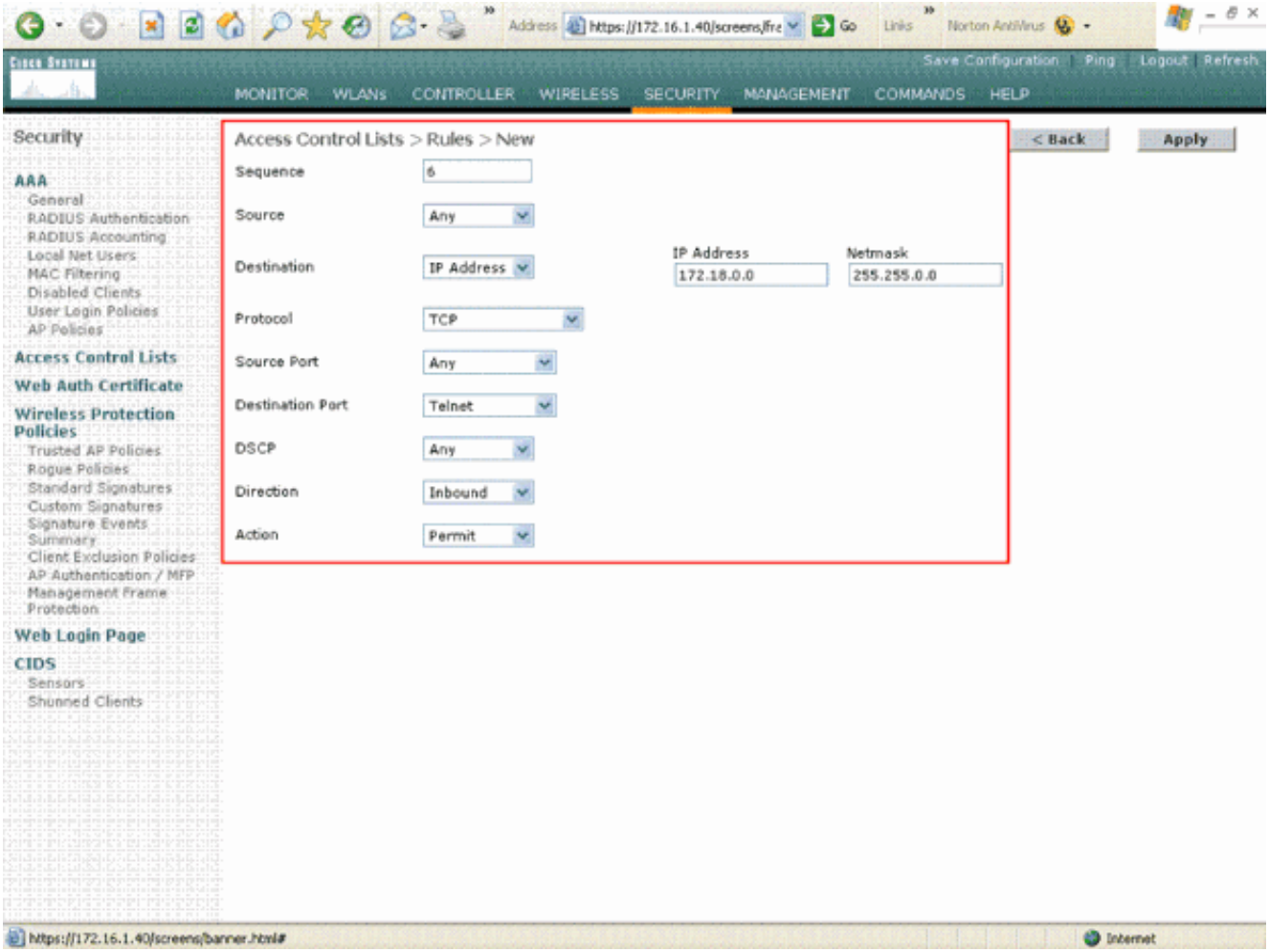
Erstellen von Regeln, die den DNS-Serverzugriff auf alle Wireless-Clients zulassen



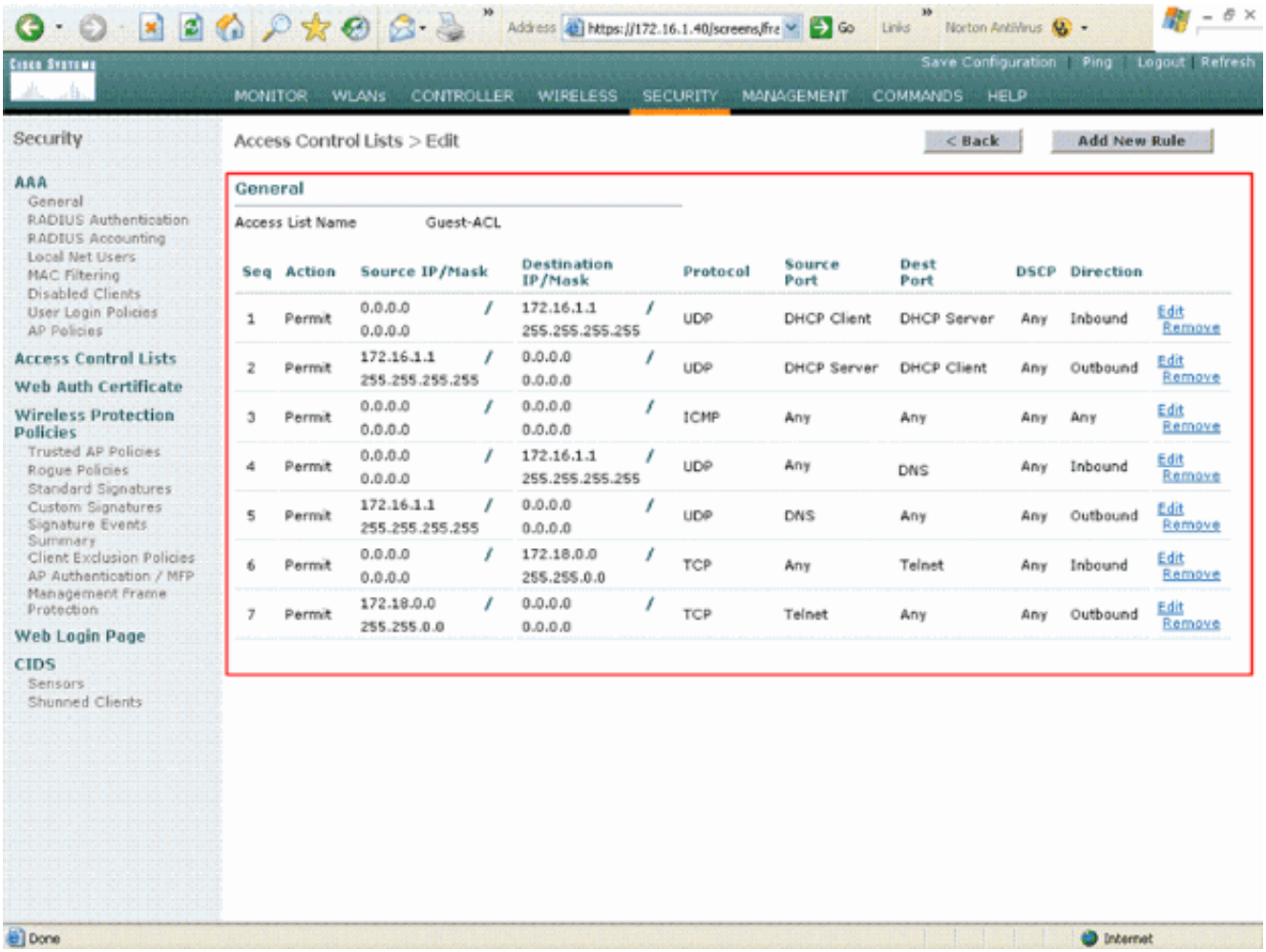
Erstellen von Regeln, die den Telnet-Serverzugriff für den Wireless-Client auf ein Subnetz zulassen Definieren Sie diese Regel, um dem Wireless-Client den Zugriff auf den Telnet-Dienst zu ermöglichen.



Zulassen des Zugriffs des Wireless-Clients auf den Telnet-Dienst

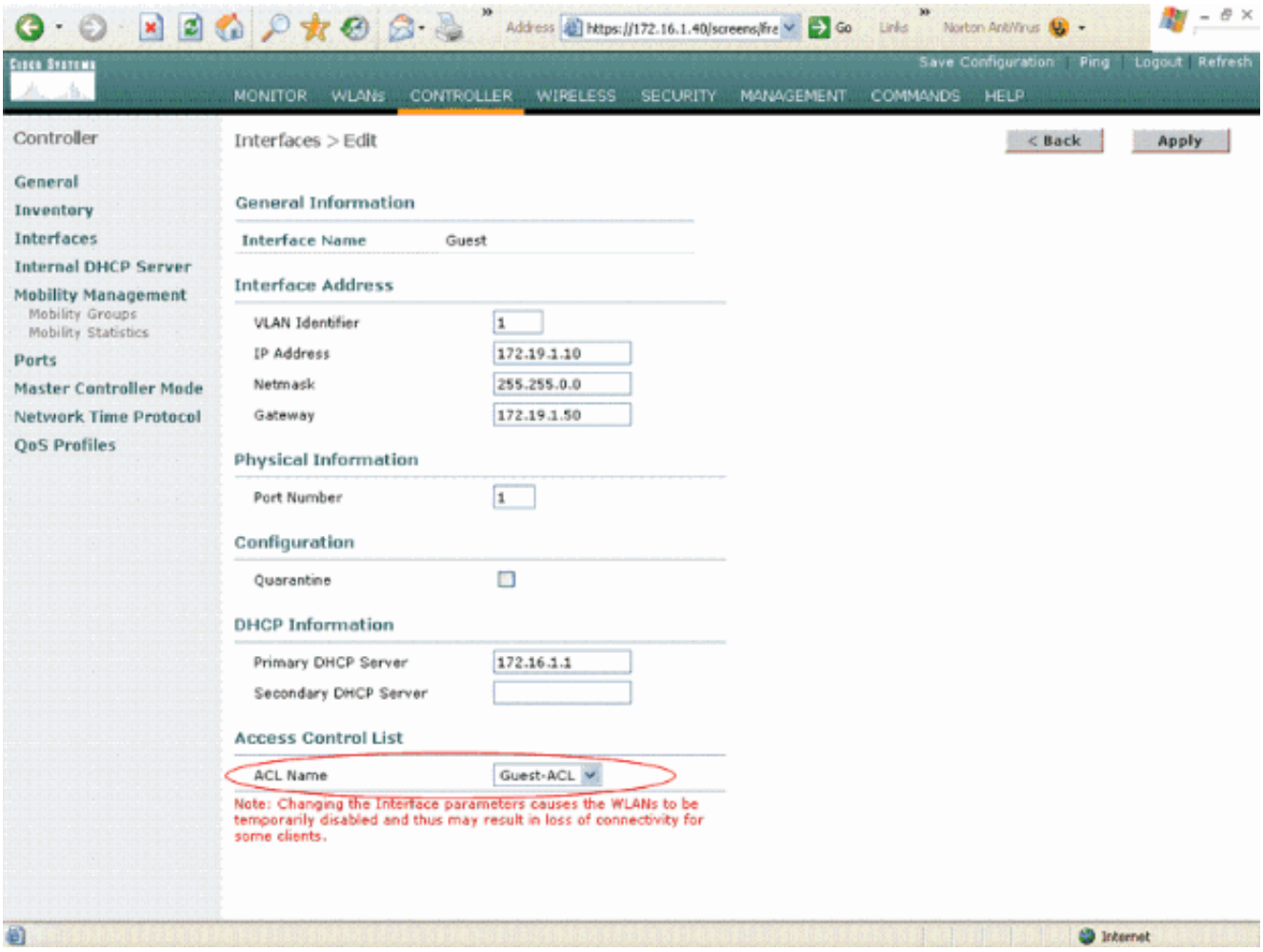


Ein weiteres Beispiel für den Zugriff von Wireless-Clients auf den Telnet-Service Auf der Seite **ACL > Edit** (ACL > Bearbeiten) werden alle Regeln aufgeführt, die für die ACL definiert sind.



Auf der Seite "Bearbeiten" werden alle für die ACL definierten Regeln aufgeführt.

4. Nachdem die ACL erstellt wurde, muss sie auf eine dynamische Schnittstelle angewendet werden. Um die ACL anzuwenden, wählen Sie **Controller > Interfaces (Controller > Schnittstellen)** und bearbeiten die Schnittstelle, auf die die ACL angewendet werden soll.
5. Wählen Sie auf der Seite **Interfaces > Edit (Schnittstellen > Bearbeiten)** für die dynamische Schnittstelle im Dropdown-Menü Access Control Lists (Zugriffskontrolllisten) die entsprechende ACL aus. Hier ein
Beispiel.



Wählen Sie im Menü "Access Control List" (Zugriffskontrollliste) die entsprechende Zugriffskontrollliste aus.

Anschließend lässt die ACL den Datenverkehr (auf Grundlage der konfigurierten Regeln) im WLAN zu, das diese dynamische Schnittstelle verwendet, und verweigert ihn. Schnittstelle-ACL kann nur im verbundenen Modus auf H-Reap-APs angewendet werden, nicht jedoch im Standalone-Modus.

> **Hinweis**: In diesem Dokument wird davon ausgegangen, dass WLANs und dynamische Schnittstellen konfiguriert sind. Weitere Informationen zum Erstellen dynamischer Schnittstellen auf WLCs finden Sie unter Konfigurieren von VLANs auf Wireless LAN-Controllern.

Konfigurieren von CPU-ACLs

Bisher hatten ACLs auf WLCs keine Option zum Filtern von LWAPP-/CAPWAP-Datenverkehr, LWAPP-/CAPWAP-Kontrollverkehr und Mobilitätsverkehr, der für die Management- und AP-Manager-Schnittstellen bestimmt war. Um dieses Problem zu beheben und LWAPP- und Mobilitätsdatenverkehr zu filtern, wurden CPU-ACLs mit der WLC-Firmware Version 4.0 eingeführt.

Die Konfiguration von CPU-ACLs erfolgt in zwei Schritten:

1. Regeln für die CPU-ACL konfigurieren
2. Wenden Sie die CPU-ACL auf den WLC an.

Die Regeln für die CPU-ACL müssen ähnlich wie die anderen ACLs konfiguriert werden.

Überprüfung

Cisco empfiehlt, die ACL-Konfigurationen mit einem Wireless-Client zu testen, um sicherzustellen, dass sie korrekt konfiguriert wurden. Wenn sie nicht ordnungsgemäß funktionieren, überprüfen Sie die ACLs auf der ACL-Webseite, und vergewissern Sie sich, dass die ACL-Änderungen auf die Controller-Schnittstelle angewendet wurden.

Sie können die folgenden **show-**Befehle auch verwenden, um Ihre Konfiguration zu überprüfen:

- **show acl summary** - Verwenden Sie den Befehl **show acl summary**, um die auf dem Controller konfigurierten ACLs anzuzeigen.Hier ein Beispiel:

```
(Cisco Controller) >show acl summary

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

- **show acl detailACL_Name:** Zeigt detaillierte Informationen zu den konfigurierten ACLs an.Hier ein Beispiel:

```
(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 (ACL-CPU anzeigen**): Um die auf der CPU konfigurierten ACLs anzuzeigen, verwenden Sie den Befehl **show acl cpu**.Hier ein Beispiel:

```
(Cisco Controller) >show acl cpu

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

Fehlerbehebung

Mit der Controller-Software-Version 4.2.x oder höher können Sie ACL-Zähler konfigurieren. ACL-Zähler können ermitteln, welche ACLs auf Pakete angewendet wurden, die über den Controller übertragen wurden. Diese Funktion ist nützlich, wenn Sie Probleme mit Ihrem System beheben.

ACL-Zähler sind auf folgenden Controllern verfügbar:

- Serie 4400
- Cisco WiSM
- Catalyst 3750G Integrierter Wireless LAN Controller-Switch

Gehen Sie wie folgt vor, um diese Funktion zu aktivieren:

1. Wählen Sie **Security > Access Control Lists > Access Control Lists**, um die Seite Access Control Lists zu öffnen.Auf dieser Seite werden alle ACLs aufgelistet, die für diesen Controller konfiguriert wurden.
2. Um festzustellen, ob Pakete eine der auf dem Controller konfigurierten ACLs erreichen, aktivieren Sie das Kontrollkästchen **Enable Counters (Zähler aktivieren)**, und klicken Sie auf **Apply (Anwenden)**. Lassen Sie andernfalls das Kontrollkästchen deaktiviert. Dies ist der Standardwert.
3. Wenn Sie die Zähler für eine Zugriffskontrollliste löschen möchten, bewegen Sie den Mauszeiger über den blauen Dropdown-Pfeil für diese Zugriffskontrollliste, und wählen Sie **Zähler löschen** .

Zugehörige Informationen

- Cisco Wireless LAN Controller Configuration Guide, Release 6.0
- Konfigurieren von VLANs auf Wireless LAN-Controllern
- Fehlerbehebung bei einem Lightweight-AP, der einem WLC nicht beitreten kann
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.