Konfigurationsbeispiel für Access Point-ACL-Filter

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie ACL-basierte Filter (Access Control List) auf Cisco Aironet Access Points (APs) mithilfe der Kommandozeile (CLI) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Konfiguration einer Wireless-Verbindung mit einem Aironet AP und einem Aironet 802.11 a/b/g Client-Adapter
- ACLs

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Aironet AP der Serie 1200 mit Cisco IOS® Software Release 12.3(7)JA1

- Aironet 802.11a/b/g Client-Adapter
- Aironet Desktop Utility (ADU) Softwareversion 2.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Hintergrundinformationen

Sie können Filter auf APs verwenden, um folgende Aufgaben auszuführen:

- Beschränkung des Zugriffs auf das WLAN-Netzwerk
- Bereitstellung einer zusätzlichen Sicherheitsebene für Wireless-Netzwerke

Sie können verschiedene Filtertypen verwenden, um Datenverkehr basierend auf folgenden Faktoren zu filtern:

- Spezifische Protokolle
- MAC-Adresse des Client-Geräts
- IP-Adresse des Client-Geräts

Sie können auch Filter aktivieren, um den Datenverkehr von Benutzern im kabelgebundenen LAN zu beschränken. IP-Adressen- und MAC-Adressfilter ermöglichen oder verbieten die Weiterleitung von Unicast- und Multicast-Paketen, die an oder von bestimmten IP- oder MAC-Adressen gesendet werden.

Protokollbasierte Filter bieten eine präzisere Möglichkeit, den Zugriff auf bestimmte Protokolle über die Ethernet- und Funkschnittstellen des Access Points zu beschränken. Sie können eine der folgenden Methoden verwenden, um die Filter auf den APs zu konfigurieren:

- Web-Benutzeroberfläche
- CLI

In diesem Dokument wird erläutert, wie Filter mithilfe von ACLs über die CLI konfiguriert werden. Weitere Informationen zum Konfigurieren von Filtern über die Benutzeroberfläche finden Sie unter Konfigurieren von Filtern.

Sie können die CLI verwenden, um diese Typen von ACL-basierten Filtern auf dem Access Point zu konfigurieren:

- Filter, die standardmäßige ACLs verwenden
- Filter, die erweiterte Zugriffskontrolllisten verwenden
- Filter, die MAC-Adressen-ACLs verwenden

Hinweis: Die Anzahl der zulässigen Einträge in einer ACL wird durch die CPU des Access Points begrenzt. Wenn eine große Anzahl von Einträgen einer ACL hinzugefügt werden soll, z. B. beim Filtern einer Liste von MAC-Adressen für die Clients, verwenden Sie einen Switch im Netzwerk, der diese Aufgabe ausführen kann.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Bei allen Konfigurationen in diesem Dokument wird davon ausgegangen, dass bereits eine Wireless-Verbindung hergestellt wurde. In diesem Dokument wird nur erläutert, wie die CLI zum Konfigurieren von Filtern verwendet wird. Wenn Sie keine grundlegende Wireless-Verbindung haben, finden Sie weitere Informationen unter Konfigurationsbeispiel für eine grundlegende Wireless LAN-Verbindung.

Filter mit Standard-Zugriffslisten

Sie können standardmäßige ACLs verwenden, um die Eingabe von Client-Geräten in das WLAN-Netzwerk basierend auf der IP-Adresse des Clients zu erlauben oder zu untersagen. Standardzugriffskontrolllisten vergleichen die Quelladresse der IP-Pakete mit den Adressen, die in der Zugriffskontrollliste konfiguriert sind, um den Datenverkehr zu kontrollieren. Dieser ACL-Typ kann als Quell-IP-Adresse-basierte ACL bezeichnet werden.

Das Befehlssyntaxformat einer Standard-ACL ist **access-list** ***access-list-number*** **{permit | deny} {host** ***ip address*** **|** ***source-ip source-wildcard*** **| any}**.

In der Cisco IOS® Softwareversion 12.3(7)JA kann die ACL-Nummer eine beliebige Zahl zwischen 1 und 99 sein. Standard-ACLs können auch den erweiterten Bereich von 1300 bis 1999 verwenden. Diese zusätzlichen Nummern sind erweiterte IP-Zugriffskontrolllisten.

Wenn eine Standard-ACL so konfiguriert ist, dass der Zugriff auf einen Client verweigert wird, ordnet der Client dem Access Point noch immer zu. Es gibt jedoch keine Datenkommunikation zwischen dem Access Point und dem Client.

Dieses Beispiel zeigt eine Standard-ACL, die so konfiguriert ist, dass die Client-IP-Adresse 10.0.0.2 von der Wireless-Schnittstelle (Radio0-Schnittstelle) gefiltert wird. Die IP-Adresse des Access Points lautet 10.0.0.1.

Danach kann der Client mit der IP-Adresse 10.0.0.2 keine Daten über das WLAN-Netzwerk senden oder empfangen, obwohl der Client dem WAP zugeordnet ist.

Gehen Sie wie folgt vor, um über die CLI eine Standard-ACL zu erstellen:

1. Melden Sie sich über die CLI beim Access Point an.Verwenden Sie den Konsolenport oder Telnet, um über die Ethernet-Schnittstelle oder die Wireless-Schnittstelle auf die ACL zuzugreifen.
2. Wechseln Sie in den globalen Konfigurationsmodus des Access Points:
   ```
   AP#configure terminal
   ```
3. Führen Sie folgende Befehle aus, um die standardmäßige ACL zu erstellen:
   ```
   AP<config>#access-list 25 deny host 10.0.0.2
   !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2.
   AP<config>#access-list 25 permit any
   ```

```
!--- Allow all other hosts to access the network.
```

4. Führen Sie die folgenden Befehle aus, um diese ACL auf die Funkschnittstelle anzuwenden:

```
AP<config>#interface Dot11Radio 0
AP<config-if>#ip access-group 25 in
!--- Apply the standard ACL to the radio interface 0.
```

Sie können auch eine Standardzugriffskontrollliste (NACL) erstellen. Die NACL verwendet einen Namen anstelle einer Zahl, um die ACL zu definieren.

```
AP#configure terminal
AP<config>#ip access-list standard name
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Führen Sie diese Befehle aus, um den Host 10.0.0.2 mithilfe von Standard-NACLs den Zugriff auf das WLAN-Netzwerk zu verweigern:

```
AP#configure terminal
AP<config>#ip access-list standard TEST
!--- Create a standard NACL TEST.

AP<config-std-nacl>#deny host 10.0.0.2
!--- Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std-
nacl>#permit any
!--- Allow all other hosts to access the network. AP<config-std-nacl>#exit
!--- Exit to global configuration mode. AP<config>#interface Dot11Radio 0
!--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in
!--- Apply the standard NACL to the radio interface.
```

Filter mit erweiterten Zugriffslisten

Erweiterte ACLs vergleichen die Quell- und Zieladressen der IP-Pakete mit den Adressen, die in der ACL konfiguriert sind, um den Datenverkehr zu steuern. Erweiterte ACLs bieten auch die Möglichkeit, Datenverkehr basierend auf bestimmten Protokollen zu filtern. Dies bietet eine präzisere Kontrolle für die Implementierung von Filtern in einem WLAN-Netzwerk.

Erweiterte ACLs ermöglichen einem Client den Zugriff auf einige Ressourcen im Netzwerk, während der Client nicht auf die anderen Ressourcen zugreifen kann. Sie können beispielsweise einen Filter implementieren, der DHCP- und Telnet-Datenverkehr zum Client zulässt, während der gesamte andere Datenverkehr eingeschränkt wird.

Dies ist die Befehlssyntax für erweiterte Zugriffskontrolllisten:

Hinweis: Dieser Befehl wird aus räumlichen Gründen in vier Zeilen eingewickelt.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

In der Cisco IOS Softwareversion 12.3(7)JA können erweiterte ACLs Nummern zwischen 100 und 199 verwenden. Erweiterte ACLs können auch Nummern zwischen 2000 und 2699 verwenden. Dies ist der erweiterte Bereich für erweiterte Zugriffskontrolllisten.

Hinweis: Das **log**-Schlüsselwort am Ende der einzelnen ACL-Einträge zeigt Folgendes:

- ACL-Nummer und -Name
- Ob das Paket zugelassen oder abgelehnt wurde
- Portspezifische Informationen

Erweiterte ACLs können auch Namen anstelle von Zahlen verwenden. Dies ist die Syntax zum Erstellen erweiterter NACLs:

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
name]
```

In diesem Konfigurationsbeispiel werden erweiterte NACLs verwendet. Die erweiterte NACL muss den Telnet-Zugriff auf die Clients ermöglichen. Sie müssen alle anderen Protokolle im WLAN-Netzwerk einschränken. Außerdem verwenden die Clients DHCP, um die IP-Adresse abzurufen. Sie müssen eine erweiterte Zugriffskontrollliste erstellen, die:

- Ermöglicht DHCP- und Telnet-Datenverkehr
- Verweigert alle anderen Datenverkehrstypen

Sobald diese erweiterte ACL auf die Funkschnittstelle angewendet wurde, stellen die Clients eine Verbindung zum AP her und erhalten eine IP-Adresse vom DHCP-Server. Die Clients können auch Telnet nutzen. Alle anderen Datenverkehrstypen werden abgelehnt.

Gehen Sie wie folgt vor, um eine erweiterte Zugriffskontrollliste für den Access Point zu erstellen:

1. Melden Sie sich über die CLI beim Access Point an.Verwenden Sie den Konsolenport oder Telnet, um über die Ethernet-Schnittstelle oder die Wireless-Schnittstelle auf die ACL zuzugreifen.
2. Wechseln Sie in den globalen Konfigurationsmodus des Access Points:
   ```
   AP#configure terminal
   ```
3. Führen Sie die folgenden Befehle aus, um die erweiterte Zugriffskontrollliste zu erstellen:
   ```
   AP<config>#ip access-list extended Allow_DHCP_Telnet
   !--- Create an extended ACL Allow_DHCP_Telnet.

   AP<config-extd-nacl>#permit tcp any any eq telnet
   !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc
   !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps
   !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any
   !--- Deny all other traffic types. AP<config-extd-nacl>#exit
   !--- Return to global configuration mode.
   ```
4. Führen Sie die folgenden Befehle aus, um die ACL auf die Funkschnittstelle anzuwenden:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group Allow_DHCP_Telnet in
   !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.
   ```

Filter mit MAC-basierten ACLs

Sie können MAC-Adressen-basierte Filter verwenden, um Client-Geräte basierend auf der hartkodierten MAC-Adresse zu filtern. Wenn einem Client der Zugriff über einen MAC-basierten Filter verweigert wird, kann der Client keine Verbindung zum AP herstellen. MAC-Adressfilter

ermöglichen oder verbieten die Weiterleitung von Unicast- und Multicast-Paketen, die entweder von bestimmten MAC-Adressen gesendet oder an diese adressiert werden.

Dies ist die Befehlssyntax zum Erstellen einer MAC-Adressen-basierten ACL auf dem Access Point:

Hinweis: Dieser Befehl wurde aus räumlichen Gründen in zwei Zeilen eingeschlossen.

access-list *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

In der Cisco IOS Software, Version 12.3(7)JA, können MAC-Adressen-ACLs Nummern zwischen 700 und 799 als ACL-Nummer verwenden. Sie können auch Nummern im erweiterten Bereich von 1100 bis 1199 verwenden.

In diesem Beispiel wird veranschaulicht, wie ein MAC-basierter Filter über die CLI konfiguriert wird, um den Client mit der MAC-Adresse **0040.96a5.b5d4** zu filtern:

1. Melden Sie sich über die CLI beim Access Point an.Verwenden Sie den Konsolenport oder Telnet, um über die Ethernet-Schnittstelle oder die Wireless-Schnittstelle auf die ACL zuzugreifen.
2. Wechseln Sie in den globalen Konfigurationsmodus der AP-CLI:
   ```
   AP#configure terminal
   ```
3. Erstellen Sie eine MAC-Adresse für ACL 700.Mit dieser ACL kann der Client 0040.96a5.b5d4 nicht mit dem Access Point verknüpft werden.

   ```
   access-list 700 deny 0040.96a5.b5d4 0000.0000.0000
   !--- This ACL denies all traffic to and from !--- the client with MAC address
   0040.96a5.b5d4.
   ```
4. Führen Sie diesen Befehl aus, um diese MAC-basierte ACL auf die Funkschnittstelle anzuwenden:

   ```
   dot11 association mac-list 700

   !--- Apply the MAC-based ACL.
   ```

Nachdem Sie diesen Filter auf dem Access Point konfiguriert haben, wird der Client mit dieser MAC-Adresse, die zuvor dem Access Point zugeordnet war, getrennt. Die AP-Konsole sendet diese Meldung:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
 Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

Filter mit zeitbasierten Zugriffskontrolllisten

Zeitbasierte Zugriffskontrolllisten sind Zugriffskontrolllisten, die für einen bestimmten Zeitraum aktiviert oder deaktiviert werden können. Diese Funktion bietet Robustheit und Flexibilität bei der Definition von Zugriffskontrollrichtlinien, die bestimmte Arten von Datenverkehr entweder zulassen oder verweigern.

In diesem Beispiel wird veranschaulicht, wie eine zeitbasierte Zugriffskontrollliste über die CLI

konfiguriert wird, bei der eine Telnet-Verbindung zwischen dem internen und dem externen Netzwerk an Wochentagen während der Geschäftszeiten zulässig ist:

Hinweis: Je nach Ihren Anforderungen kann eine zeitbasierte Zugriffskontrollliste entweder auf dem Fast Ethernet-Port oder auf dem Radio Port des Aironet AP definiert werden. Sie wird nie auf die Bridge Group Virtual Interface (BVI) angewendet.

1. Melden Sie sich über die CLI beim Access Point an.Verwenden Sie den Konsolenport oder Telnet, um über die Ethernet-Schnittstelle oder die Wireless-Schnittstelle auf die ACL zuzugreifen.
2. Wechseln Sie in den globalen Konfigurationsmodus der AP-CLI:
   ```
   AP#configure terminal
   ```
3. Erstellen Sie einen Zeitbereich. Führen Sie dazu den folgenden Befehl im globalen Konfigurationsmodus aus:
   ```
   AP<config>#time-range Test
   !--- Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to 19:00
   !--- Allows access to users during weekdays from 7:00 to 19:00 hrs.
   ```
4. Erstellen einer ACL 101:
   ```
   AP<config># ip access-list extended 101
   AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test
   !--- This ACL permits Telnet traffic to and from !--- the network for the specified time-range Test.
   ```
   Diese ACL ermöglicht eine Telnet-Sitzung mit dem Access Point an Wochentagen.
5. Geben Sie diesen Befehl ein, um diese zeitbasierte ACL auf die Ethernet-Schnittstelle anzuwenden:

   ```
   interface Ethernet0/0
   ip address 10.1.1.1 255.255.255.0
   ip access-group 101 in

   !--- Apply the time-based ACL.
   ```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

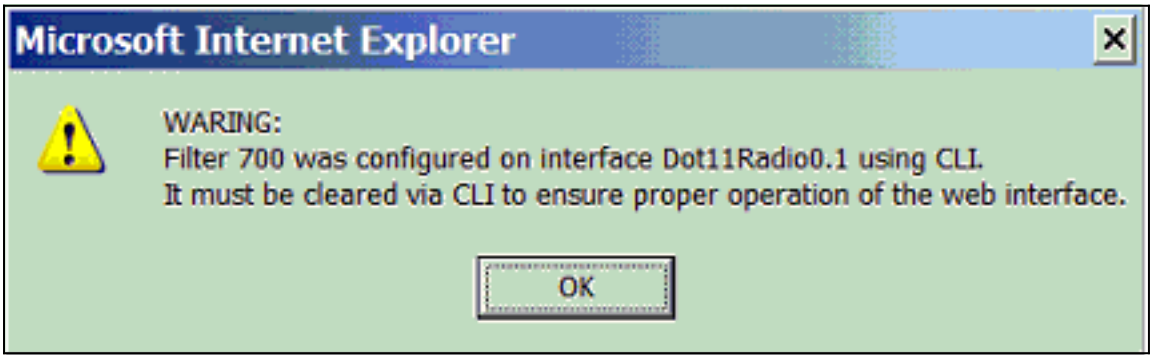
Gehen Sie wie folgt vor, um eine ACL von einer Schnittstelle zu entfernen:

1. Wechseln Sie in den Schnittstellenkonfigurationsmodus.
2. Geben Sie **no** vor dem Befehl **ip access-group ein**, wie im folgenden Beispiel veranschaulicht wird:

   ```
   interface interface
   no ip access-group {access-list-name | access-list-number} {in | out}
   ```

Sie können auch den *Namen der **Zugriffsliste anzeigen*** verwenden. **| numerischer** Befehl, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen. Der Befehl **show ip access-list** gibt eine Paketanzahl an, die anzeigt, welcher ACL-Eintrag betroffen ist.

Vermeiden Sie die Verwendung der CLI und der Webbrowser-Schnittstellen, um das Wireless-Gerät zu konfigurieren. Wenn Sie das Wireless-Gerät mit der CLI konfigurieren, kann die Webbrowser-Oberfläche die Konfiguration ungenau interpretieren. Die Ungenauigkeit bedeutet jedoch nicht unbedingt, dass das Wireless-Gerät falsch konfiguriert ist. Wenn Sie z. B. ACLs mit der CLI konfigurieren, kann die Webbrowser-Schnittstelle die folgende Meldung anzeigen:



Wenn Sie diese Meldung sehen, löschen Sie die Zugriffskontrolllisten mithilfe der CLI, und konfigurieren Sie sie über die Webbrowser-Oberfläche neu.

Zugehörige Informationen

- Konfigurieren von Filtern
- Wireless-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems