액세스 포인트 ACL 필터 컨피그레이션 예

목차

소개

이 문서에서는 CLI(Command Line Interface)를 사용하여 Cisco Aironet Access Point(AP)에서 ACL(Access Control List) 기반 필터를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Aironet AP 및 Aironet 802.11 a/b/g Client Adapter를 사용하여 무선 연결을 구성하는 방법
- ACL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.3(7)JA1을 실행하는 Aironet 1200 Series AP
- Aironet 802.11a/b/g Client Adapter
- Aironet Desktop Utility(ADU) 소프트웨어 릴리스 2.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

AP에서 필터를 사용하여 다음 작업을 수행할 수 있습니다.

- 무선 LAN(WLAN) 네트워크에 대한 액세스 제한
- 추가적인 무선 보안 계층 제공

다음과 같이 다양한 유형의 필터를 사용하여 트래픽을 필터링할 수 있습니다.

- 특정 프로토콜
- 클라이언트 장치의 MAC 주소
- 클라이언트 장치의 IP 주소

유선 LAN에서 사용자의 트래픽을 제한하기 위해 필터를 활성화할 수도 있습니다. IP 주소 및 MAC 주소 필터는 특정 IP 또는 MAC 주소로 또는 특정 MAC 주소로 전송되는 유니캐스트 및 멀티캐스트 패킷의 전달을 허용하거나 허용하지 않습니다.

프로토콜 기반 필터는 AP의 이더넷 및 무선 인터페이스를 통해 특정 프로토콜에 대한 액세스를 제한하는 더욱 세분화된 방법을 제공합니다. 다음 방법 중 하나를 사용하여 AP에서 필터를 구성할 수 있습니다.

- 웹 GUI
- CLI

이 문서에서는 ACL을 사용하여 CLI를 통해 필터를 구성하는 방법에 대해 설명합니다. GUI를 통해 필터를 구성하는 방법에 대한 자세한 내용은 필터 구성을 참조하십시오.

CLI를 사용하여 AP에서 다음 유형의 ACL 기반 필터를 구성할 수 있습니다.

- 표준 ACL을 사용하는 필터
- 확장 ACL을 사용하는 필터
- MAC 주소 ACL을 사용하는 필터

참고: ACL에서 허용되는 항목 수는 AP의 CPU로 제한됩니다. ACL에 추가할 항목이 많은 경우, 예를 들어 클라이언트의 MAC 주소 목록을 필터링할 때 작업을 수행할 수 있는 네트워크의 스위치를 사용합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 정보를 찾습니다.

이 문서의 모든 컨피그레이션에서는 무선 연결이 이미 설정된 것으로 가정합니다. 이 문서에서는 필터를 구성하기 위해 CLI를 사용하는 방법에만 초점을 둡니다. 기본 무선 연결이 없는 경우 기본 무선 LAN 연결 구성 예를 참조하십시오.

표준 액세스 목록을 사용하는 필터

표준 ACL을 사용하여 클라이언트의 IP 주소를 기반으로 WLAN 네트워크에 클라이언트 장치의 입력을 허용하거나 허용하지 않을 수 있습니다. 표준 ACL은 트래픽을 제어하기 위해 ACL에 구성된 주소와 IP 패킷의 소스 주소를 비교합니다. 이 ACL 유형을 소스 IP 주소 기반 ACL이라고 할 수 있습니다.

표준 ACL의 명령 구문 형식은 **access-list** ***access-list-number*** **{permit입니다. | 거부} {host** ***ip-address*** **|** ***source-ip source-wildcard*** **| any}**.

Cisco IOS® Software Release 12.3(7)JA에서 ACL 번호는 1~99의 숫자일 수 있습니다. 표준 ACL은 1300~1999의 확장 범위를 사용할 수도 있습니다. 이러한 추가 숫자는 확장 IP ACL입니다.

표준 ACL이 클라이언트에 대한 액세스를 거부하도록 구성된 경우 클라이언트는 여전히 AP에 연결됩니다. 그러나 AP와 클라이언트 간에는 데이터 통신이 없습니다.

이 예에서는 무선 인터페이스(radio0 인터페이스)에서 클라이언트 IP 주소 10.0.0.2을 필터링하도록 구성된 표준 ACL을 보여 줍니다. AP의 IP 주소는 10.0.0.1입니다.

이 작업을 수행한 후에는 클라이언트가 AP에 연결되어 있더라도 IP 주소가 10.0.0.2인 클라이언트가 WLAN 네트워크를 통해 데이터를 보내거나 받을 수 없습니다.

CLI를 통해 표준 ACL을 생성하려면 다음 단계를 완료합니다.

1. CLI를 통해 AP에 로그인합니다.콘솔 포트를 사용하거나 텔넷을 사용하여 이더넷 인터페이스 또는 무선 인터페이스를 통해 ACL에 액세스합니다.
2. AP에서 전역 컨피그레이션 모드를 시작합니다.
   ```
   AP#configure terminal
   ```
3. 표준 ACL을 생성하려면 다음 명령을 실행합니다.
   ```
   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. 이 ACL을 라디오 인터페이스에 적용하려면 다음 명령을 실행합니다.
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

표준 ACL(NACL)을 생성할 수도 있습니다. NACL은 숫자 대신 이름을 사용하여 ACL을 정의합니다.

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

표준 NACL을 사용하여 WLAN 네트워크에 대한 호스트 10.0.0.2 액세스를 거부하려면 다음 명령을 실행합니다.

```
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.
```

확장 액세스 목록을 사용하는 필터

확장 ACL은 트래픽을 제어하기 위해 IP 패킷의 소스 및 목적지 주소를 ACL에 구성된 주소와 비교합니다. 확장 ACL은 특정 프로토콜을 기반으로 트래픽을 필터링하는 수단도 제공합니다. 이렇게 하면 WLAN 네트워크에서 필터를 구현하기 위한 더욱 세분화된 제어가 가능합니다.

확장 ACL을 사용하면 클라이언트가 네트워크의 일부 리소스에 액세스할 수 있지만 클라이언트는 다른 리소스에 액세스할 수 없습니다. 예를 들어, DHCP 및 텔넷 트래픽을 클라이언트에 허용하는 필터를 구현하고 다른 모든 트래픽을 제한할 수 있습니다.

확장 ACL의 명령 구문입니다.

참고: 이 명령은 공간 고려 사항으로 인해 4줄로 래핑됩니다.

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***]**

Cisco IOS Software Release 12.3(7)JA에서 확장 ACL은 100~199 범위의 숫자를 사용할 수 있습니다. 확장 ACL은 2000~2699 범위의 숫자를 사용할 수도 있습니다. 확장 ACL의 확장 범위입니다.

참고: 개별 ACL 항목의 끝에 있는 log 키워드는 다음과 같습니다.

- ACL 번호 및 이름
- 패킷이 허용 또는 거부되었는지 여부
- 포트별 정보

확장 ACL은 숫자 대신 이름을 사용할 수도 있습니다. 확장 NACL을 생성하는 구문입니다.

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***]**

이 컨피그레이션 예에서는 확장 NACL을 사용합니다. 확장 NACL은 클라이언트에 대한 텔넷 액세스를 허용해야 합니다. WLAN 네트워크에서 다른 모든 프로토콜을 제한해야 합니다. 또한 클라이언트는 IP 주소를 가져오기 위해 DHCP를 사용합니다. 다음과 같은 확장 ACL을 생성해야 합니다.

- DHCP 및 텔넷 트래픽 허용
- 다른 모든 트래픽 유형을 거부합니다.

이 확장 ACL을 라디오 인터페이스에 적용하면 클라이언트는 AP와 연결하고 DHCP 서버에서 IP 주소를 가져옵니다. 클라이언트는 텔넷을 사용할 수도 있습니다. 다른 모든 트래픽 유형은 거부됩니다.

AP에 확장 ACL을 생성하려면 다음 단계를 완료합니다.

1. CLI를 통해 AP에 로그인합니다.이더넷 인터페이스 또는 무선 인터페이스를 통해 ACL에 액세스하려면 콘솔 포트 또는 텔넷을 사용합니다.
2. AP에서 전역 컨피그레이션 모드를 시작합니다.
   ```
   AP#configure terminal
   ```
3. 확장 ACL을 생성하려면 다음 명령을 실행합니다.
   ```
   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. 라디오 인터페이스에 ACL을 적용하려면 다음 명령을 실행합니다.
   ```
   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.
   ```

MAC 기반 ACL을 사용하는 필터

하드 코딩된 MAC 주소를 기반으로 클라이언트 디바이스를 필터링하려면 MAC 주소 기반 필터를 사용할 수 있습니다. 클라이언트가 MAC 기반 필터를 통해 액세스가 거부되면 클라이언트는 AP와 연결할 수 없습니다. MAC 주소 필터는 특정 MAC 주소에서 전송되거나 지정된 유니캐스트 및 멀티캐스트 패킷의 전달을 허용하거나 허용하지 않습니다.

AP에서 MAC 주소 기반 ACL을 생성하기 위한 명령 구문입니다.

참고: 이 명령은 공간 고려 사항으로 인해 두 줄로 래핑되었습니다.

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

Cisco IOS Software Release 12.3(7)JA에서 MAC 주소 ACL은 700~799 범위의 숫자를 ACL 번호로 사용할 수 있습니다. 또한 1100~1199의 확장된 범위에서 숫자를 사용할 수 있습니다.

다음 예에서는 MAC 주소가 0040.96a5.b5d4인 클라이언트를 필터링하기 위해 CLI를 통해 MAC 기반 필터를 구성하는 방법을 보여 줍니다.

1. CLI를 통해 AP에 로그인합니다.이더넷 인터페이스 또는 무선 인터페이스를 통해 ACL에 액세스하려면 콘솔 포트 또는 텔넷을 사용합니다.
2. AP CLI에서 전역 컨피그레이션 모드를 시작합니다.
   ```
   AP#configure terminal
   ```
3. MAC 주소 ACL 700을 만듭니다.이 ACL에서는 클라이언트 0040.96a5.b5d4를 AP와 연결할 수 없습니다.

   ```
   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. 이 MAC 기반 ACL을 라디오 인터페이스에 적용하려면 다음 명령을 실행합니다.

```
dot11 association mac-list 700

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

AP에서 이 필터를 구성하면 이전에 AP에 연결되었던 이 MAC 주소를 가진 클라이언트의 연결이 해제됩니다. AP 콘솔은 다음 메시지를 전송합니다.

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

시간 기반 ACL을 사용하는 필터

시간 기반 ACL은 특정 기간 동안 활성화하거나 비활성화할 수 있는 ACL입니다. 이 기능은 견고성과 유연성을 통해 특정 종류의 트래픽을 허용하거나 거부하는 액세스 제어 정책을 정의할 수 있습니다.

다음 예에서는 CLI를 통해 시간 기반 ACL을 구성하는 방법을 보여 줍니다. 여기서 업무 시간 중에 평일 내에서 외부 네트워크로 텔넷 연결이 허용됩니다.

참고: 시간 기반 ACL은 요구 사항에 따라 고속 이더넷 포트 또는 Aironet AP의 무선 포트에서 정의할 수 있습니다. BVI(Bridge Group Virtual Interface)에는 적용되지 않습니다.

1. CLI를 통해 AP에 로그인합니다.이더넷 인터페이스 또는 무선 인터페이스를 통해 ACL에 액세스하려면 콘솔 포트 또는 텔넷을 사용합니다.
2. AP CLI에서 전역 컨피그레이션 모드를 시작합니다.
   ```
   AP#configure terminal
   ```
3. 시간 범위를 만듭니다. 이렇게 하려면 글로벌 컨피그레이션 모드에서 이 명령을 실행합니다.
   ```
   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. ACL 101을 생성합니다.
   ```
   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.
   ```
   이 ACL은 평일에 AP에 대한 텔넷 세션을 허용합니다.
5. 이더넷 인터페이스에 이 시간 기반 ACL을 적용하려면 다음 명령을 실행합니다.

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

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

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

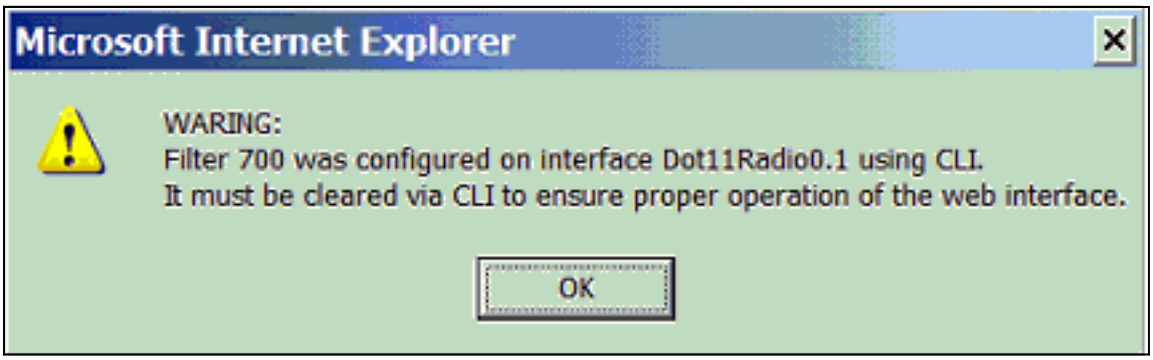
인터페이스에서 ACL을 제거하려면 다음 단계를 완료합니다.

1. 인터페이스 컨피그레이션 모드로 들어갑니다.
2. **ip access-group** 명령 앞에 no를 입력합니다. 다음 예는 다음과 같습니다.

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

show access-list *이름*을 사용할 수도 있습니다. **|** ***number*** 명령을 입력하여 컨피그레이션을 트러블슈팅합니다. show **ip access-list** 명령은 적중 중인 ACL 항목을 표시하는 패킷 수를 제공합니다.

CLI와 웹 브라우저 인터페이스를 모두 사용하여 무선 디바이스를 구성하지 마십시오. CLI를 사용하여 무선 디바이스를 구성할 경우 웹 브라우저 인터페이스에서 컨피그레이션에 대한 부정확한 해석을 표시할 수 있습니다. 그러나 부정확성이 무선 장치가 잘못 구성되었음을 의미하지는 않습니다. 예를 들어, CLI를 사용하여 ACL을 구성하는 경우 웹 브라우저 인터페이스에 다음 메시지가 표시될 수 있습니다.



이 메시지가 표시되면 CLI를 사용하여 ACL을 삭제하고 웹 브라우저 인터페이스를 사용하여 다시 구성합니다.

관련 정보

- 필터 구성
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems