アクセス ポイントの ACL フィルタ設定例

内容

概要

このドキュメントでは、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、Cisco Aironet Access Point（AP; アクセス ポイント）で Access Control List（ACL; アクセス コントロール リスト）ベースのフィルタを設定する方法について説明しています。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- Aironet AP および Aironet 802.11 a/b/g クライアント アダプタを使用する無線接続の設定。
- ACL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS®ソフトウェアリリース12.3JA1が稼働するAironet 1200シリーズAP
- Aironet 802.11a/b/g クライアント アダプタ
- Aironet Desktop Utility（ADU）ソフトウェア リリース 2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

AP でフィルタを使用すると、次の作業を実行できます。

- 無線 LAN（WLAN）ネットワークへのアクセス制限。
- 無線セキュリティのレイヤの追加。

次の項目に基づいたトラフィックのフィルタリングには、さまざまなタイプのフィルタが使用できます。

- 特定のプロトコル
- クライアント デバイスの MAC アドレス
- クライアント デバイスの IP アドレス

また、フィルタを有効にして、有線 LAN 上のユーザからのトラフィックを制限することもできます。IP アドレスと MAC アドレスのフィルタによって、特定の IP アドレスや MAC アドレス間で送受信されるユニキャストおよびマルチキャスト パケットの転送を許可または禁止できます。

プロトコル ベースのフィルタでは、さらに詳細なフィルタを行うことができ、AP のイーサネット インターフェイスと無線インターフェイスを通過する特定のプロトコルへのアクセスを制限できます。AP 上でのフィルタの設定には、次のいずれかの方法を使用できます。

- Web GUI
- CLI

このドキュメントでは、CLI でフィルタを設定するための、ACL の使用方法について説明します。GUI によるフィルタの設定方法については、『フィルタの設定』を参照してください。

CLI を使用して、AP に次のタイプの ACL ベースのフィルタを設定できます。

- 標準 ACL を使用するフィルタ
- 拡張 ACL を使用するフィルタ
- MAC アドレスの ACL を使用するフィルタ

注：ACLで許可されるエントリの数は、APのCPUによって制限されます。クライアントの MAC アドレスのリストのフィルタリングのように、多数のエントリを ACL に追加する場合は、ネットワーク上でこのようなタスクの処理能力のあるスイッチを使用してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

このドキュメントで使用されているコマンドの詳細を調べるには、コマンド検索ツール（登録ユーザ専用）を使用してください。

このドキュメントの設定はすべて、無線接続がすでに確立されていることを前提としています。このドキュメントでは、CLI を使用してフィルタを設定することにだけ焦点をあてています。基本的な無線接続が確立されていない場合は、『基本的な無線 LAN 接続の設定例』を参照してください。

標準アクセス リストを使用するフィルタ

標準の ACL を使用すると、クライアント デバイスの WLAN ネットワークへの参加の許可や禁止が、クライアントの IP アドレスに基づいて行えます。標準 ACL では、トラフィックを制御するために、IP パケットの送信元アドレスと ACL に設定されたアドレスが比較されます。このタイプの ACL は、送信元 IP アドレスベースの ACL と呼ばれます。

標準 ACL のコマンド構文の形式は、**access-list** ***access-list-number*** ***{permit*** **|** **deny}** **{host** ***ip-address*** **|** ***source-ip source-wildcard*** **|** **any}**。

Cisco IOS®ソフトウェアリリース12.3(7)JAでは、ACL番号は1 ~ 99の任意の番号にすることができます。標準ACLでは、1300 ~ 1999の拡張範囲も使用できます。これらの追加番号は、拡張された IP ACL です。

あるクライアントに、標準 ACL でアクセス拒否が設定されている場合でも、そのクライアントの AP へ関連付けは保持されています。しかし、この AP とクライアントとの間でデータの通信は行われません。

この例では、IP アドレスが 10.0.0.2 のクライアントを、無線インターフェイス (radio0 インターフェイス) からフィルタリングするように設定された、標準 ACL を示しています。 AP の IP アドレスは 10.0.0.1 です。

この ACL を設定すると、IP アドレスが 10.0.0.2 のクライアントは、AP と関連付けされている場合でも、WLAN ネットワーク上でデータを送受信できなくなります。

CLI を使用して標準 ACL を作成するには、次の手順を実行します。

1. CLI を使用して AP にログインします。コンソール ポートまたは Telnet を使用して、イーサネット インターフェイスまたは無線インターフェイス経由で ACL にアクセスします。
2. AP でグローバル コンフィギュレーション モードに入ります。
   ```
   AP#configure terminal
   ```
3. 次のコマンドを発行して、標準 ACL を作成します。
   ```
   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. 次のコマンドを発行して、この ACL を無線インターフェースに適用します。
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

標準の Named ACL (NACL; 名前付きアクセス コントロール リスト) を作成することもできます。 NACL では、番号ではなく名前を使用して ACL を定義します。

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

標準 NACL を使用して、ホスト 10.0.0.2 が WLAN ネットワークへアクセスするのを拒否するには、次のコマンドを発行します。

```
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.
```

拡張アクセス リストを使用するフィルタ

拡張 ACL では、トラフィックを制御するために、IP パケットの送信元アドレスおよび宛先アドレスと ACL に設定されたアドレスが比較されます。拡張 ACL では、特定のプロトコルに基づいてトラフィックをフィルタリングすることもできます。これにより、WLAN ネットワークでのフィルタの実装がより細かく制御できます。

拡張 ACL ではあるクライアントに対して、ネットワーク上の一部のリソースへのアクセスは許可し、他のリソースへのアクセスは拒否するという設定ができます。たとえば、あるクライアントに対して、DHCP と Telnet のトラフィックは許可し、他のトラフィックはすべて制限するというフィルタを実装できます。

拡張 ACL のコマンド構文を次に示します。

注：このコマンドは、スペースの関係上4行に折り返されています。

```
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ソフトウェアリリース12.3(7)JAでは、拡張ACLは100 ~ 199の範囲の番号を使用できます。拡張ACLは2000 ~ 2699の範囲の番号を使用することもできます。これは拡張 ACL 用の拡張範囲です。

注：個々のACLエントリの最後にあるlogキーワードは次のように表示されます。

- ACL の番号と名前
- そのパケットが許可されているか、または拒否されているか
- ポート固有の情報

拡張 ACL では、番号の代わりに名前も使用できます。拡張 NACL を作成するための構文は、次のとおりです。

```
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]
```

この設定例では、拡張 NACL を使用しています。ここでの要件は、拡張 NACL がクライアントに対して Telnet アクセスを許可することです。この WLAN ネットワークでは、他のプロトコルをすべて制限する必要があります。また、クライアントは DHCP を使用して IP アドレスを取得します。次のような拡張 ACL を作成する必要があります。

- DHCP と Telnet のトラフィックを許可する
- 他のすべてのタイプのトラフィックを拒否する

この拡張 ACL を無線インターフェイスに適用すると、クライアントは AP に関連付けられ、DHCP サーバから IP アドレスを取得します。クライアントは Telnet も使用できます。他のすべてのタイプのトラフィックは拒否されます。

AP に拡張 ACL を作成するには、次の手順を実行します。

1. CLI を使用して AP にログインします。コンソール ポートまたは Telnet を使用して、イーサネット インターフェイスまたは無線インターフェイス経由で ACL にアクセスします。
2. AP でグローバル コンフィギュレーション モードに入ります。
   ```
   AP#configure terminal
   ```
3. 次のコマンドを発行して、拡張 ACL を作成します。
   ```
   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. 次のコマンドを発行して、ACL を無線インターフェースに適用します。
   ```
   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 ベースの ACL を使用するフィルタ

MAC アドレスベースのフィルタを使用すると、ハードコードされた MAC アドレスに基づくクライアント デバイスのフィルタリングを行うことができます。クライアントが MAC ベースのフィルタでアクセスを拒否されると、そのクライアントは AP と関連付けできません。MAC アドレスのフィルタによって、特定の MAC アドレスへ送受信されるユニキャストおよびマルチキャストのパケットの転送を、許可または禁止することができます。

MAC アドレスベースの ACL を AP 上に作成するためのコマンド構文は次のとおりです。

注：このコマンドは、スペースの関係上2行に渡って表示されています。

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

Cisco IOS ソフトウェア リリース 12.3(7)JA では、MAC アドレスによる ACL には、ACL 番号と

して 700 ~ 799 の範囲の番号が使用できます。また、1100 ~ 1199 の拡張範囲の番号も使用できます。

この例は、MAC アドレスが **0040.96a5.b5d4** のクライアントをフィルタリングするために、CLI を使用して MAC ベースのフィルタを設定する方法を説明しています。

1. CLI を使用して AP にログインします。コンソール ポートまたは Telnet を使用して、イーサネット インターフェイスまたは無線インターフェイス経由で ACL にアクセスします。
2. AP の CLI でグローバル コンフィギュレーション モードに入ります。
   ```
   AP#configure terminal
   ```
3. MAC アドレスの ACL 700 を作成します。この ACL では、クライアント 0040.96a5.b5d4 が AP に関連付けられるのを禁止します。
   ```
   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. 次のコマンドを発行して、この MAC ベース ACL を無線インターフェースに適用します。
   ```
   dot11 association mac-list 700

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

このフィルタを AP に設定すると、この MAC アドレスを持つクライアントは、以前にその AP に関連付けされていても、関連付けが解除されます。AP のコンソールからは次のメッセージが送られます。

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

時間ベースの ACL を使用するフィルタ

時間ベースの ACL は、特定の期間に有効または無効にできる ACL です。この機能により、特定の種類のトラフィックを許可または拒否するアクセス コントロール ポリシーを定義するための口バストネスと柔軟性が提供されます。

この例では、CLI を使用して時間ベースの ACL を設定し、平日の営業時間中に Inside ネットワークから Outside ネットワークへの Telnet 接続を許可する方法について説明しています。

注：時間ベースのACLは、要件に基づいて、ファストイーサネットポートまたはAironet APの無線ポートで定義できます。ただし、Bridge Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) には適用されません。

1. CLI を使用して AP にログインします。コンソール ポートまたは Telnet を使用して、イーサネット インターフェイスまたは無線インターフェイス経由で ACL にアクセスします。
2. AP の CLI でグローバル コンフィギュレーション モードに入ります。
   ```
   AP#configure terminal
   ```
3. 時間の範囲を作成します。これを行うには、グローバル コンフィギュレーション モードで次のコマンドを発行します。
   ```
   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 101 を作成します。

```
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.
```

   この ACL は、平日に AP への Telnet セッションを許可します。
5. 次のコマンドを発行して、この時間ベース ACL をイーサネット インターフェースに適用します。

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

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

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

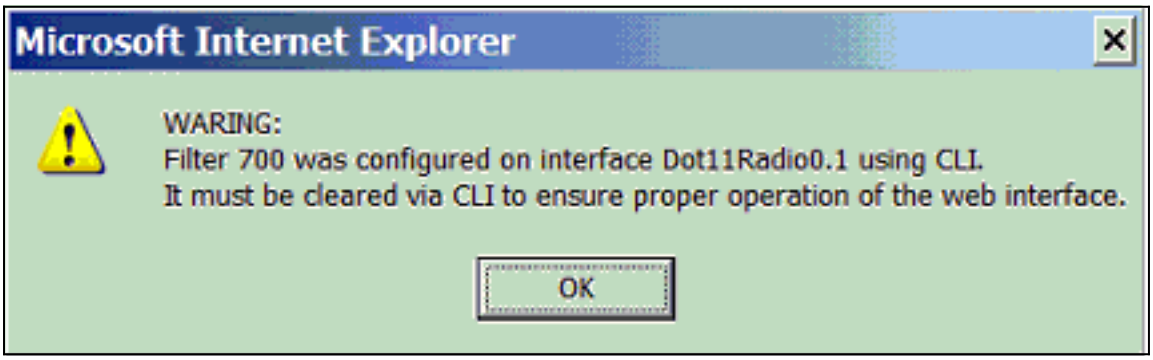
インターフェイスから ACL を削除するには、次の手順を実行します。

1. インターフェイス設定モードに入ります。
2. 次の例で示すように、**ip access-group** コマンドの前に no を付けて入力します。

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

設定のトラブルシューティングを行うには、**show access-list** *name* | *number*コマンドを発行します。**show ip access-list** コマンドでは、どの ACL エントリがヒットされているかを示すパケット カウントが表示されます。

無線デバイスを設定するために CLI と Web ブラウザ インターフェイスの両方を使用するのは避けてください。CLI を使用して無線デバイスを設定する場合は、Web ブラウザ インターフェイスに不正確な設定が表示される可能性があります。ただし、不正確な表示は、無線デバイスが誤って設定されていることを必ずしも意味するわけではありません。たとえば、CLI を使用して ACL を設定している場合は、Web ブラウザ インターフェイスに次のメッセージが表示されることがあります。



このメッセージが表示された場合は、CLI を使用して ACL を削除し、Web ブラウザ インターフェイスを使用して再度設定を行ってください。

関連情報

- フィルタの設定
- ワイヤレスに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems