

ワイヤレスアクセスポイントでのMAC、IPv4、およびIPv6アクセスコントロールリストの設定

目的

アクセスコントロールリスト(ACL)は、セキュリティを向上させるために使用されるネットワークトラフィックフィルタと関連アクションのリストです。権限のないユーザをブロックし、権限のあるユーザが特定のリソースにアクセスできるようにします。ACLには、ネットワークデバイスへのアクセスを許可または拒否するホストが含まれます。ACLは、IPv4アドレスまたはIPv6アドレスのいずれかの方法で定義できます。

この記事では、ACLを正常に作成し、ワイヤレスアクセスポイント(WAP)でIPv4、IPv6、およびメディアアクセスコントロール(MAC)ベースのACLを設定して、ネットワークセキュリティを向上させる方法について説明します。

適用可能なデバイス

- WAP100シリーズ
- WAP300シリーズ
- WAP500シリーズ

[Software Version]

- 1.0.6.2 - WAP121、WAP321
- 1.2.0.2 - WAP371、WAP551、WAP561
- 1.0.1.4 - WAP131、WAP351
- 1.0.0.16 - WAP150、WAP361

ACL の作成

注：この設定で使用するイメージはWAP150のものであります。

ステップ 1：アクセスポイントのWebベースユーティリティにログインし、ACL > ACL Ruleの順に選択します。

▼ **ACL**

ACL Rule

ACL Association

ACL Status

注：WAP121、WAP321、WAP371、WAP551、およびWAP561の場合：アクセスポイントのWebベースユーティリティにログインして、Client QoS > ACLの順に選択します。

▶ **Client QoS**

Global Settings

ACL

Class Map

Policy Map

Client QoS Association

Client QoS Status

ステップ 2：ACL Configurationページが開いたら、ACL NameフィールドにACL名を入力します。

ACL Rule

ACL Configuration

ACL Name:

ACL1

ACL Type:

MAC

Add ACL

ステップ 3 : ACL TypeドロップダウンリストからACL Typeを選択します。

ACL Rule

ACL Configuration

ACL Name:

IPv4

IPv6

ACL Type:

✓ MAC

Add ACL

- IPv4:32ビット (4バイト) のアドレス。
- IPv6:IPv4のサクセサで、128ビット (8バイト) のアドレスで構成されます。
- MAC:MACアドレスは、ネットワークインターフェイスに割り当てられた一意のアドレスです。

ステップ 4 : Add ACLボタンをクリックします。

ACL Rule

ACL Configuration

ACL Name:

ACL1

ACL Type:

MAC

Add ACL

MACを選択した場合は、「[MACベースのACLの設定](#)」に進んでください。

IPv4を選択した場合は、「[IPv4ベースのACLの設定](#)」に進んでください。

IPv6を選択した場合は、「[IPv6ベースのACLの設定](#)」に進んでください。

これで、ACLが正常に作成されました。

MACベースのACLの設定

ステップ 1 : Acl Name - ACL Typeドロップダウンリストから、ルールを追加するACLを選択します。

注 : 次の図では、ACL1 MACが例として選択されています。

ACL Rule Configuration

ACL Name - ACL Type:

✓ ACL1 - MAC

Rule:

New Rule

ステップ 2 : 選択したACLに新しいルールを設定する必要がある場合は、RuleドロップダウンリストからNew Ruleを選択します。それ以外の場合は、Ruleドロップダウンリストから現在のルールのいずれかを選択します。

注 : 1つのACLに最大10のルールを作成できます。

ACL Rule Configuration

ACL Name - ACL Type:

ACL1 - MAC

Rule:

✓ New Rule

ステップ 3 : Actionドロップダウンリストから、ACLルールのアクションを選択します。

注 : この例では、Deny文が作成されます。

Action:

✓ Deny

Permit

Match Every Packet:



- Deny:WAPに出入りするルールの基準を満たすすべてのトラフィックをブロックします。すべてのACLの最後には暗黙的なdeny-allルールがあるため、明示的に許可されていないトラフィックはドロップされます。
- Permit : ルールの基準を満たすすべてのトラフィックがWAPに出入りするのを許可します。基準を満たさないトラフィックはドロップされます。

注：手順4～11はオプションです。チェックされたフィルタが有効になります。この特定のルールに適用しないフィルタのチェックボックスをオフにします。

ステップ4：内容に関係なく、すべてのフレームまたはパケットのルールに一致させるには、Match Every Packetチェックボックスをオンにします。追加の一致基準を設定するには、このチェックボックスをオフにします。

ヒント：[すべてのパケットに一致させる]が既にオンになっている場合は、[ステップ12](#)に進みます。

The screenshot shows a configuration panel with a light blue background. On the left, the text 'Action:' is followed by a dropdown menu containing the word 'Deny'. Below this, the text 'Match Every Packet:' is followed by a blue checkmark icon inside a square box, which is circled in red.

ステップ5：EtherType領域で、オプションボタンを選択して、一致した基準をイーサネットフレームのヘッダー内の値と比較します。次のいずれかのオプションを選択するか、「任意」を選択します。

- Select From List : ドロップダウンリストからプロトコルを選択します。このリストには、appletalk、arp、IPv4、IPv6、ipx、netbios、pppoeのオプションがあります。
- 「値に一致」 - カスタムプロトコル識別子の場合、0600～FFFFの範囲の識別子を入力します。

The screenshot shows a configuration panel with a light blue background. On the left, the text 'Protocol:' is followed by three radio button options: 'Any', 'Select From List:', and 'Match to Value:'. The 'Select From List:' option is selected and circled in red. To the right of these options is a dropdown menu with 'icmp' selected. Below the dropdown is a text input field containing the number '0', with the label '(Range)' to its right.

手順6：Class Of Serviceエリアでオプションボタンを選択し、802.1pユーザプライオリティを入力して、イーサネットフレームと比較します。「任意」または「ユーザー定義」の優先度を選択できます。優先度を0～7の範囲でUser Definedフィールドに入力します。

Class Of Service:

- Any
 User Defined

6

手順 7 : Source MAC領域で、オプションボタンを選択して、送信元MACアドレスをイーサネットフレームと比較します。Anyを選択するか、User Definedを選択して、表示されたフィールドに送信元MACアドレスを入力します。

Source MAC:

- Any
 User Defined

Source MAC Address:

04:FE:36:A5:670B

Source MAC Mask:

ステップ 8 : Source MAC Maskフィールドに、イーサネットフレームと比較する発信元MACのビットを指定する、発信元MACアドレスマスクを入力します。

注:MACマスクが0ビットを使用している場合はアドレスが受け入れられ、1ビットを使用している場合はアドレスが無視されます。

Source MAC:

- Any
 User Defined

Source MAC Address:

04:FE:36:A5:670B

Source MAC Mask:

00:00:00:00:00:00

ステップ 9 : Destination MAC領域で、オプションボタンを選択して、宛先MACアドレスをイーサネットフレームと比較します。Anyを選択するか、User Definedを選択して、表示されたフィールドに宛先MACアドレスを入力します。

Destination MAC:

- Any
 User Defined

Destination MAC Address:

F2:CA:46:11:EA:09

Destination MAC Mask:

ステップ 10 : Destination MAC Maskフィールドに、イーサネットフレームと比較する宛先MACのビットを指定する、宛先MACアドレスマスクを入力します。

注:MACマスクが0ビットを使用する場合、アドレスは受け入れられ、1ビットを使用する場合、アドレスは無視されます。

Destination MAC: Any
 User Defined
Destination MAC Address: F2:CA:46:11:EA:09
Destination MAC Mask: 00:00:00:00:00:00

ステップ 11VLAN ID領域で、オプションボタンを選択して、イーサネットフレームとVLAN IDを比較します。表示されたフィールドに0 ~ 4095の範囲のVLAN IDを入力します。

VLAN ID: Any
 User Defined 52 (Range: 0 - 4095)

ステップ 12[Save] をクリックします。

VLAN ID: Any
 User Defined
Delete ACL:

Save

ステップ13: (オプション) 設定されたACLを削除するには、Delete ACLチェックボックスをオンにして、Saveをクリックします。

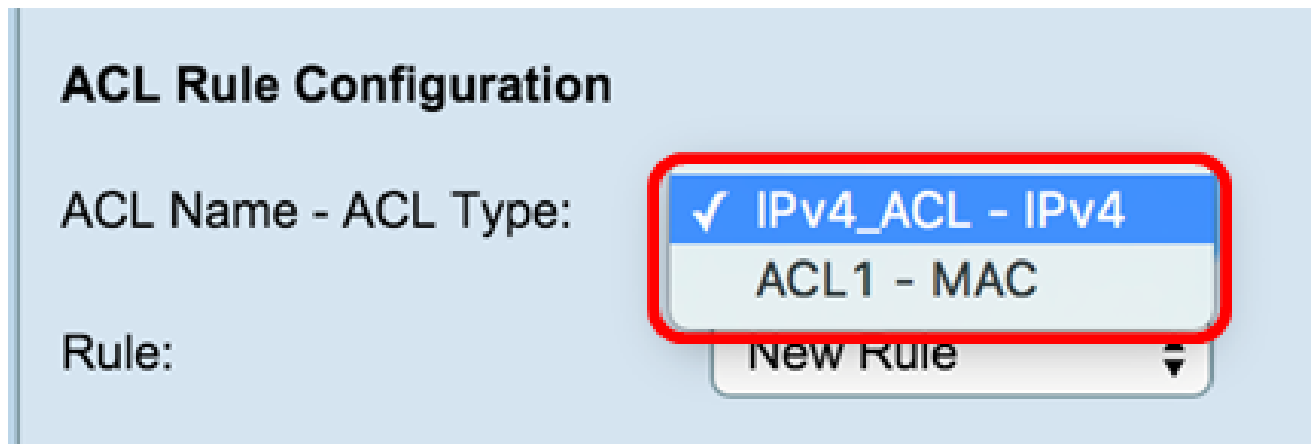
これで、WAPでMAC ACLが正常に設定されました。

IPv4ベースのACLの設定

ステップ 1 : ACL Rule Configuration領域で、次のルールパラメータを設定します。

ACL名 - ACLタイプ : 新しいルールで設定するACLを選択します。

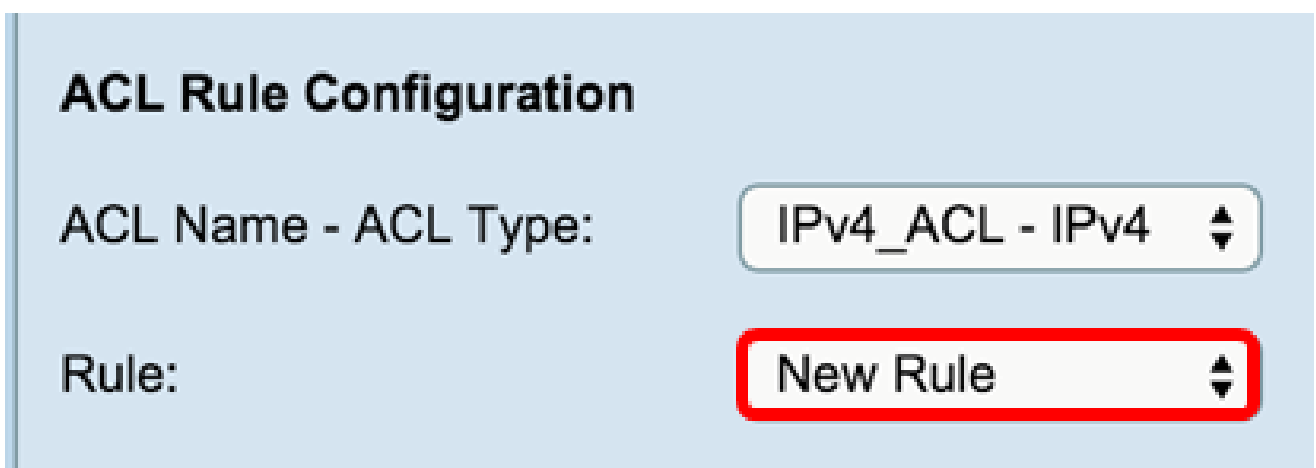
注 : 次の図では、例としてIPv4_ACL-IPv4が選択されています。



The screenshot shows the 'ACL Rule Configuration' section. The 'ACL Name - ACL Type:' field has a dropdown menu open, displaying three options: 'IPv4_ACL - IPv4' (selected with a checkmark), 'ACL1 - MAC', and 'New Rule'. A red box highlights the dropdown menu.

ステップ 2 : 選択したACLに新しいルールを設定する必要がある場合は、RuleドロップダウンリストからNew Ruleを選択します。それ以外の場合は、Ruleドロップダウンリストから現在のルールのいずれかを選択します。

注 : 1つのACLに最大10のルールを作成できます。

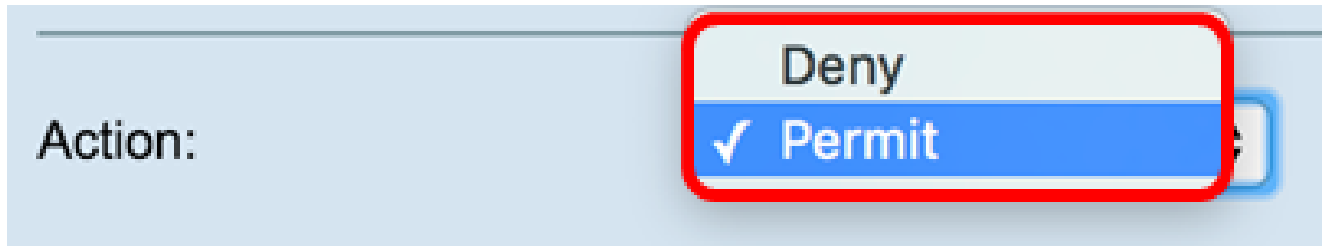


The screenshot shows the 'ACL Rule Configuration' section. The 'ACL Name - ACL Type:' field is set to 'IPv4_ACL - IPv4'. The 'Rule:' field has a dropdown menu open, displaying 'New Rule'. A red box highlights the dropdown menu.

ステップ 3 : Actionドロップダウンリストから、ACLルールのアクションを選択します。

注 : この例では、Permit文が作成されます。

- Deny:WAPに出入りするルールの基準を満たすすべてのトラフィックをブロックします。すべてのACLの最後には暗黙的なdeny-allルールがあるため、明示的に許可されていないトラフィックはドロップされます。
- Permit : ルールの基準を満たすすべてのトラフィックがWAPに出入りすることを許可します。基準を満たさないトラフィックはドロップされます。



注：手順4～9はオプションです。チェックされたフィルタが有効になります。この特定のルールにフィルタを適用しない場合は、フィルタのチェックボックスをオフにします。

ステップ4：内容に関係なく、すべてのフレームまたはパケットのルールに一致させるには、**Match Every Packet**チェックボックスをオンにします。追加の一致基準を設定するには、このボックスのチェックマークを外します。



ヒント：Match Every Packetはデフォルトで有効になっています。この設定を保持する場合は、[ステップ11](#)に進んでください。

ステップ5：Protocol領域で、オプションボタンを選択して、一致した基準をイーサネットフレームのヘッダー内の値と比較します。「任意」を選択するか、ドロップダウンリストから選択します

- Select From List : 次のいずれかのプロトコルを選択します。
 - IP : ネットワーク間でデータをリレーするための、Internet Protocol Suite (IP ; インターネットプロトコルスイート) の主要な通信プロトコル。
 - ICMP : ルータなどのデバイスがエラーメッセージを送信するために使用する、インターネットプロトコルスイートのプロトコル。
 - IGMP:IPv4ネットワークでマルチキャストグループメンバーシップを確立するためにホストによって使用される通信プロトコル。
 - TCP — 2台のホストが接続を確立し、データのストリームを交換できるようにします。
 - UDP : コネクションレス型伝送モデルを使用するインターネットプロトコルスイートのプロトコル。
- 「値に一致」 — IANAが割り当てた標準のプロトコルIDを0～255の範囲で入力します。この方法を選択すると、[選択元]ボックスの一覧に名前が表示されていないプロトコルが識別されます。

Protocol:

Any
 Select From List:
 Match to Value:

icmp (Range)

0

手順 6 : Source IPエリアで、オプションボタンを選択して、照合条件に送信元のIPアドレスを含めます。AnyまたはUser Definedを選択し、それぞれのフィールドに送信元のIPアドレスとワイルドカードマスクを入力できます。

- Source IP Address : この基準を適用するIPアドレスを入力します。
- Wild Card Mask : 宛先IPアドレスのワイルドカードマスクを入力します。ワイルドカードマスクは、使用するビットと無視するビットを決定します。ワイルドカードマスク255.255.255.255は、ビットが重要でないことを示します。ワイルドカード0.0.0.0は、すべてのビットが重要であることを示します。このフィールドは、[送信元IPアドレス]が選択されている場合に必要です。

注 : ワイルドカードマスクは基本的にサブネットマスクの逆です。たとえば、条件を1つのホストアドレスに一致させるには、ワイルドカードマスク0.0.0.0を使用します。条件を24ビットのサブネット(192.168.10.0/24など)に一致させるには、ワイルドカードマスク0.0.0.255を使用します。

Source IP:

Any
 User Defined
 Source IP Address: 192.168.1.100 (xxx
 Wild Card Mask: 0.0.0.255 (xxx

手順 7 : Source Port領域で、オプションボタンを選択して、照合条件に送信元ポートを含めます。Anytoを選択して任意の送信元ポートに一致させるか、次の項目を選択できます。

- 「リストから選択」 - 「リストから選択」ドロップダウンリストからソースポートを選択します。オプションは次のとおりです。

— FTP (ファイル転送プロトコル) — FTPは、インターネットなどのTCP (伝送制御プロトコル) ベースのネットワークを介して、あるホストから別のホストにファイルを転送するために使用される標準のネットワークプロトコルです。

— FTPデータ : 通常はポート20を介してクライアントに接続されているサーバによって開始されるデータチャネル。

— Hypertext Transfer Protocol (HTTP ; ハイパーテキスト転送プロトコル) : HTTPは、World Wide Webのデータ通信の基盤となるアプリケーションプロトコルです。

— Simple Mail Transfer Protocol (SMTP ; シンプルメール転送プロトコル) : SMTPは、電子メール (電子メール) 送信のインターネット標準です。

— Simple Network Management Protocol(SNMP):SNMPは、IPネットワーク上のデバイスを管理するためのインターネット標準プロトコルです。

— Telnet : 双方向の対話式テキスト指向の通信を提供するためにインターネットまたはローカルエリアネットワークで使用されるセッション層プロトコル。

— Trivial File Transfer Protocol (TFTP ; トリビアルファイル転送プロトコル) :TFTPは、FTPよりも簡単に使用でき、それほど機能のないファイル転送用のインターネットソフトウェアユーティリティです。

— World Wide Web(WWW) — WWWは、HTTP形式のドキュメントをサポートするインターネットサーバシステムです。

- 「ポートに一致」 – リストに表示されていないポート番号を入力します。リストにない送信元ポートのMatch to Portフィールドでは、ポート番号の範囲は0 ~ 65535です。範囲には、3種類のポートが含まれます。範囲は次のとおりです

— 0 ~ 1023 – ウェルノウンポート

— 1024 ~ 49151 – 登録ポート

— 49152 ~ 65535 – ダイナミックポートまたはプライベートポート

- Mask : ポートマスクを入力します。マスクは、使用するビットと無視するビットを決定します。16進数(0 ~ 0xFFFF)のみを使用できます。0はビットが重要であることを意味し、1はこのビットを無視する必要があることを意味します。

Source Port:

Any

Select From List:

Match to Port:

Mask:

www (Range: 0 - 65535)

(Range: 0 ~ 0xffff, 0s)

ステップ 8 : Destination IPエリアで、オプションボタンを選択して、照合条件に宛先のIPアドレスを含めます。AnyまたはUser Definedを選択し、それぞれのフィールドに宛先のIPアドレスとワイルドカードマスクを入力できます。

- Destination IP Address : この基準を適用するIPアドレスを入力します。
- Wild Card Mask : 宛先IPアドレスのワイルドカードマスクを入力します。ワイルドカードマスクは、使用するビットと無視するビットを決定します。ワイルドカードマスク255.255.255.255は、ビットが重要でないことを示します。ワイルドカード0.0.0.0は、すべてのビットが重要であることを示します。宛先IPアドレスが選択されている場合、このフィールドは必須です。

注 : ワイルドカードマスクは基本的にサブネットマスクの逆です。たとえば、条件を1つのホストアドレスに一致させるには、ワイルドカードマスク0.0.0.0を使用します。条件を24ビットのサブネット(192.168.10.0/24など)に一致させるには、ワイルドカードマスク0.0.0.255を使用します。

Destination IP:

Any

User Defined

Destination IP Address: 192.168.1.110 (xxx.xxx.xxx.xxx)

Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx -)

ステップ 9 : Destination Port領域で、オプションボタンを選択して、照合条件に宛先ポートを含めます。任意の宛先ポートに

一致するようにAnyを選択するか、または次の項目を選択できます。

- Select From List : ドロップダウンリストから宛先ポートを選択します。オプションは次のとおりです
 - FTP : インターネットなどのTCPベースのネットワークを介してホスト間でファイルを転送するために使用される標準のネットワークプロトコル。
 - FTPデータ : 通常はポート20を介してクライアントに接続されているサーバによって開始されるデータチャネル。
 - HTTP:World Wide Webのデータ通信の基盤となるアプリケーションプロトコル。
 - SMTP : 電子メール (Eメール) 送信のインターネット標準。
 - SNMP:IPネットワーク上のデバイスを管理するためのインターネット標準プロトコル。
 - Telnet : 双方向の対話式テキスト指向の通信を提供するためにインターネットまたはローカルエリアネットワークで使用されるセッション層プロトコル。
 - TFTP : ファイル転送用のインターネットソフトウェアユーティリティで、FTPよりも簡単に使用できますが、機能は劣ります。
 - WWW —HTTP形式のドキュメントをサポートするインターネットサーバのシステム。
- 「ポートに一致」 - リストに表示されていないポート番号を入力します。リストにない送信元ポートのMatch to Portフィールドでは、ポート番号の範囲は0 ~ 65535です。範囲には、3種類のポートが含まれます。範囲は次のとおりです。
 - 0 ~ 1023 - 既知のポート
 - 1024 ~ 49151 - 登録ポート
 - 49152 ~ 65535 - ダイナミックポートまたはプライベートポート
- Mask : ポートマスクを入力します。マスクは、使用するビットと無視するビットを決定します。16進数(0 ~ 0xFFFF)のみを使用できます。0はビットが重要であることを意味し、1はこのビットを無視する必要があることを意味します。

Destination Port:

Any

Select From List:

Match to Port: (Range: 0 - 65535)

Mask: (Range: 0 ~ 0xFFFF)

ステップ 10 : Service Type領域で、オプションボタンを選択し、特定のサービスタイプに基づいてパケットを照合します。「任意」を選択するか、または次の中から選択できます。

- IP DSCP Select From List:Differentiated Services Code Point(DSCP)のAssured Forwarding(AS)、Class of Service(CS)、または Expedited Forwarding(EF)の値に基づいてパケットを照合します。
- IP DSCP値への一致 : カスタムDSCP値に基づいてパケットを照合します。選択した場合は、このフィールドに0 ~ 63の値を入力します。
- IP Precedence:IP優先順位値に基づいてパケットを照合します。選択した場合は、0 ~ 7のIP優先順位値を入力します。
- IP TOSビット : 一致基準としてIPヘッダー内のパケットのTOSビットを使用する値を指定します。
- パケット内のIP TOSフィールドは、IPヘッダー内のサービスタイプ (サービスタイプ) オクテットの8ビットすべて

として定義されます。IP TOSビット値は、00 ~ ffの2桁の16進数です。上位3ビットはIP優先順位値を表します。上位6ビットはIP DSCP値を表します。

- IP TOSマスク：IP TOSマスク値を入力して、パケットのIP TOSフィールドとの比較に使用されるIP TOSビット値のビット位置を特定します。
- IP TOSマスク値は、反転（つまりワイルドカード）マスクを表す、00 ~ FFの2桁の16進数です。IP TOSマスク内の0値のビットは、パケットのIP TOSフィールドとの比較に使用されるIP TOSビット値のビット位置を示します。たとえば、ビット7と5が設定され、ビット1がクリアされたIP TOS値（ビット7が最も重要）をチェックするには、IP TOSビット値0とIP TOSマスク00を使用します。

Service Type

Any

IP DSCP Select From List

IP DSCP Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF)

IP TOS Mask: (Range: 00 - FF)

ステップ 11[Save] をクリックします。

VLAN ID:

Any

User Defined

Delete ACL:

Save

これで、IPv4ベースのACLが正常に設定されました。

IPv6ベースのACLの設定

ステップ 1：ACL Rule Configuration領域で、次のルールパラメータを設定します。

ACL Name - ACL Type：新しいルールを使用して設定するACLを選択します。

注：次の図では、IPv6_ACL — Pv6が例として選択されています。

ACL Rule Configuration

ACL Name - ACL Type:

IPv6_ACL - IPv6

Rule:

New Rule

ステップ 2 : 選択したACLに新しいルールを設定する必要がある場合は、RuleドロップダウンリストからNew Ruleを選択します。それ以外の場合は、「規則」ドロップダウンリストから現在の規則のいずれかを選択します。

注 : 1つのACLに最大10のルールを作成できます。

ACL Rule Configuration

ACL Name - ACL Type:

IPv6_ACL - IPv6

Rule:

New Rule

ステップ 3 : Actionドロップダウンリストから、ACLルールのアクションを選択します

- Deny:WAPに出入りするルールの基準を満たすすべてのトラフィックをブロックします。すべてのACLの最後には暗黙的なdeny-allルールがあるため、明示的に許可されていないトラフィックはドロップされます。
- Permit : ルールの基準を満たすすべてのトラフィックがWAPに出入りするのを許可します。基準を満たさないトラフィックはドロップされます。

Action:

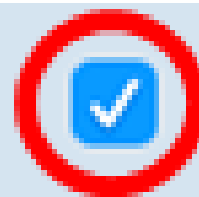
✓ Deny
Permit

Match Every Packet:

注 : 手順4 ~ 11はオプションです。チェックされたフィルタが有効になります。この特定のルールにフィルタを適用しない場合は、フィルタのチェックボックスをオフにします。

ステップ 4 : *Match Every Packet* チェックボックスをオンにして、その内容に関係なく、すべてのフレームまたはパケットのルールに一致させます。追加の一致基準を設定するには、このボックスのチェックマークを外します。

Match Every Packet:



ヒント : 「すべてのパケットに一致」はデフォルトで有効になっています。この設定を維持する場合は、[ステップ12](#)に進んでください。

ステップ 5 : Protocol 領域で、オプションボタンを選択して、一致した基準をイーサネットフレームのヘッダー内の値と比較します。次のいずれかのオプションを選択するか、「任意」を選択します。

- Select From List : 次のいずれかのプロトコルを選択します。
 - IP : ネットワーク間でデータをリレーするための、Internet Protocol Suite (IP ; インターネットプロトコルスイート) の主要な通信プロトコル。
 - ICMP : ルータなどのデバイスがエラーメッセージを送信するために使用する、インターネットプロトコルスイートのプロトコル。
 - IGMP:IPv4 ネットワークでマルチキャストグループメンバーシップを確立するためにホストによって使用される通信プロトコル。
 - TCP — 2台のホストが接続を確立し、データのストリームを交換できるようにします。
 - UDP : コネクションレス型伝送モデルを使用するインターネットプロトコルスイートのプロトコル。
- 「値に一致」 — IANA が割り当てた標準のプロトコル ID を 0 ~ 255 の範囲で入力します。この方法を選択すると、[選択] ボックスの一覧に名前が表示されていないプロトコルが識別されます。

手順 6 : Source IPv6 領域で、オプションボタンを選択して、照合条件に送信元の IPv6 アドレスを含めます。Any または User Defined を選択してから、IPv6 アドレスと送信元 IPv6 プレフィクス長を入力できます。

- 「送信元 IPv6 アドレス」 - この条件を適用する IPv6 アドレスを入力します。
- Source IPv6 Prefix Length : 送信元 IPv6 アドレスのプレフィクス長を入力します。

手順 7 : Source Port 領域で、オプションボタンを選択して、照合条件に送信元ポートを含めます。Any を選択して任意の送信元ポートに一致させるか、または次の項目を選択できます。

- Select From List: *Select From List* ドロップダウンリストから送信元ポートを選択します。オプションは次のとおりです。
 - FTP : インターネットなどのTCPベースのネットワークを介してホスト間でファイルを転送するために使用される標準のネットワークプロトコル。
 - FTPデータ : 通常はポート20を介してクライアントに接続されているサーバによって開始されるデータチャネル。
 - HTTP: World Wide Webのデータ通信の基盤となるアプリケーションプロトコル。
 - SMTP : 電子メール (Eメール) 送信のインターネット標準。
 - SNMP: IPネットワーク上のデバイスを管理するためのインターネット標準プロトコル。
 - Telnet : 双方向の対話式テキスト指向の通信を提供するためにインターネットまたはローカルエリアネットワークで使用されるセッション層プロトコル。
 - TFTP : ファイル転送用のインターネットソフトウェアユーティリティで、FTPよりも簡単に使用できますが、機能は劣ります。
 - WWW — HTTP形式のドキュメントをサポートするインターネットサーバのシステム。
- 「ポートに一致」 - リストに表示されていないポート番号を入力します。リストにない送信元ポートの *Match to Port* フィールドでは、ポート番号の範囲は0 ~ 65535です。範囲には、3種類のポートが含まれます。範囲は次のとおりです。
 - 0 ~ 1023 - 既知のポート
 - 1024 ~ 49151 - 登録ポート
 - 49152 ~ 65535 - ダイナミックポートまたはプライベートポート
- Mask : ポートマスクを入力します。マスクは、使用するビットと無視するビットを決定します。16進数(00xFFFF)のみ使用できます。0はビットが重要であることを意味し、1はこのビットを無視する必要があることを意味します。

ステップ 8 : Destination IPv6領域で、オプションボタンを選択して、照合条件に宛先のIPアドレスを含めます。Anyを選択するか、User Definedを選択します。IPv6アドレスと宛先IPv6プレフィクス長を入力します。

- 「宛先IPv6アドレス」 - この条件を適用するIPv6アドレスを入力します。
- Destination IPv6 Prefix Length : 宛先IPv6アドレスのプレフィクス長を入力します。

ステップ 9 : Destination Port領域で、オプションボタンを選択して、照合条件に宛先ポートを含めます。任意の宛先ポートに一致するようにAnyを選択するか、または次の項目を選択できます。

- Select From List: *Select From List* ドロップダウンリストから宛先ポートを選択します。オプションは、FTP、FTPデータ、HTTP、SNMP、SMTP、TFTP、Telnet、WWWです。
- 「ポートに一致」 - リストに表示されていないポート番号を入力します。リストにない送信元ポートの *Match to Port* フィールドでは、ポート番号の範囲は0 ~ 65535です。範囲には、3種類のポートが含まれます。範囲は次のとおりです。

— 0 ~ 1023 - 既知のポート

— 1024 ~ 49151 - 登録ポート

— 49152 ~ 65535 - ダイナミックポートまたはプライベートポート

- Mask : ポートマスクを入力します。マスクは、使用するビットと無視するビットを決定します。16進数(0 ~ 0xFFFF)のみを使用できます。0はビットが重要であることを意味し、1はこのビットを無視する必要があることを意味します。

ステップ 10 : IPv6フローラベル領域で、オプションボタンを選択して、一致条件にIPv6フローラベルを含めます。AnyまたはUser Definedを選択して、IPv6パケットに固有の20ビットの数値を入力できます。範囲は0 ~ 0xffffです。

ステップ 11 IPv6 DSCP領域で、オプションボタンを選択して、パケットをIP DSCP値と照合します。「任意」を選択するか、または次の項目を選択できます。

- リストから選択 : DSCP保証転送(AF)、サービスクラス(CS)、緊急転送(EF)のいずれかの値を選択します。
- 「値に一致」 — 0 ~ 63の範囲のカスタムDSCP値を入力します。

ステップ 12 [Save] をクリックします。

IPv6 DSCP: Any
 Select From List:
 Match to Value:

Delete ACL:

Save

ステップ13: (オプション) ACLを削除するには、ACL名 – ACLタイプリストでACL名が選択されていることを確認してから、Delete ACLにチェックマークを付けます。

これで、IPv6ベースのACLが正常に設定されました。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。