アクセス コントロール リスト

アクセス コントロール リストについて

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは Central Processing Unit（CPU; 中央処理装置）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

または、Web 認証用に事前認証 ACL を作成することもできます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。

IPv4 ACL および IPv6 ACL のどちらもサポートされています。IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

アクセス コントロール リストの制約事項

- IPv4 および IPv6 の両方に最大 64 の ACL を定義し、各 ACL に最大 64 のルール（またはフィルタ）を適用できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。
- すべての ACL で、最後のルールとして暗黙の「deny all」ルールが適用されます。パケットがどのルールとも一致しない場合、コントローラによってドロップされます。
- インターフェイスまたは WLAN に ACL を適用すると、1 Gbps ファイル サーバからのダウンロードの際にワイヤレス スループットが低下します。スループットを改善するには、インターフェイスまたは WLAN から ACL を削除するか、ポリシー レート制限制約機能を持つ隣接有線デバイスに ACL を移動するか、1 Gbps ではなく 100 Mbps を使用してファイル サーバを接続します。
- 有線ネットワークから受信した無線クライアントに向かうマルチキャスト トラフィックは WLC ACL では処理されません。無線クライアントから開始され同じコントローラの有線ネットワークまたはその他のワイヤレス クライアントに向かうマルチキャスト トラフィックは、WLC ACL によって処理されます。
- ACL はコントローラ上で直接設定されるか、Cisco Prime Infrastructure のテンプレートを使用して設定されます。ACL 名は固有の名前でなければなりません。
- クライアント（AAA によって上書きされる ACL）ごと、もしくはインターフェイスまたは WLAN で ACL を設定できます。AAA によって上書きされる ACL の優先度が最も高くなります。ただし、適用する各インターフェイス、WLAN、またはクライアントごとの ACL の設定は、お互いを上書きできます。
- ピアツーピア ブロッキングが有効になると、トラフィックは ACL で許可されてもピア間でブロックされます。
- 認証トラフィックは、DNS ベースの ACL が AP に対してローカルであっても、この機能がサポートされるように Cisco WLC を経由する必要があります。
- ACL を作成する場合は、CLI または GUI から 2 つのアクション（ACL または ACL ルールの作成と、ACL または ACL ルールの適用）を連続して行うことをお勧めします。
- 8.0.100.0 以前のシスコ ワイヤレス リリースでは、（RADIUS 属性経由で返される）Redirect-URL-ACL が正しくなかった可能性があります。ACL は、無線インターフェイスの入力方向のみ（LAN またはディストリビューション システム宛てのトラフィック）で適用されています。またこれらの ACL は、出力方向（ワイヤレス クライアント宛てのトラフィック）に適用する必要があります。したがって、シスコ ワイヤレス リリース 8.0 以降のリリースにアップグレードすると、この動作の変更に対応するために ACL を調整する必要があります。
- ポート 16666 および 16667 に対するモビリティ ping は注目すべき例外で、これらのポートは ACL によってブロックできません。

（注） ACL ID 0 は、Cisco WLC ではサポートされていません。RADIUS/ISE からの受信 ACL 属性が ACL ID 0 にマップされている場合、外部 WLC は url-redirect-acl をアンカー WLC に送信しません。これにより後で、ワイヤレス クライアントで Web リダイレクト障害が発生します。

アクセス コントロール リストの設定と適用（GUI）

アクセス コントロール リストの設定

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択して、[Access Control Lists] ページを開きます。

ステップ 2 パケットがコントローラに設定されたACLのいずれかに一致するかどうかを確認する場合は、[Enable Counters] チェックボックスをオンにして [Apply] をクリックします。それ以外の場合、このチェックボックスはオフ（デフォルト値）のままにしておきます。この機能は、システムのトラブルシューティングを実行する際に役立ちます。

（注） ACLのカウンタをクリアするには、そのACLの青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

ステップ 3 [New] をクリックして、新しい ACL を追加します。[Access Control Lists > New] ページが表示されます。

ステップ 4 [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 5 ACL タイプを選択します。IPv4 と IPv6 の 2 つの ACL のタイプがサポートされています。

ステップ 6 [Apply] をクリックします。[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 7 [Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Access Control Lists > Rules > New] ページが表示されます。

ステップ 8 この ACL のルールを次のように設定します。

a) コントローラは各ACLについて最大64のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキスト ボックスで、値（1 ～ 64）を入力し、このACLに定義されている他のルールに対するこのルールの順番を決定します。

（注） ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b) [Source] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの送信元を指定します。

- [Any]：任意の送信元（これはデフォルト値です）。
- [IP Address]：特定の送信元。このオプションを選択する場合は、テキスト ボックスに送信元の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキスト ボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。

c) [Destination] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any]：任意の宛先（これはデフォルト値です）。
- [IP Address]：特定の宛先。このオプションを選択する場合は、テキスト ボックスに宛先の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキスト ボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。

d) [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコル オプションは次のとおりです。

- [Any]：任意のプロトコル（これはデフォルト値です）
- [TCP]：トランスミッション コントロール プロトコル
- [UDP]：ユーザ データグラム プロトコル
- [ICMP/ICMPv6]：インターネット制御メッセージ プロトコル

  （注） ICMPv6 は IPv6 ACL でのみ使用可能です。

- [ESP]：IP カプセル化セキュリティ ペイロード
- [AH]：認証ヘッダー
- [GRE]：Generic Routing Encapsulation
- [IP in IP]：Internet Protocol（IP）in IP（IP-in-IP パケットのみを許可または拒否）
- [Eth Over IP]：Ethernet-over-Internet プロトコル
- [OSPF]：Open Shortest Path First
- [Other]：その他の Internet Assigned Numbers Authority（IANA）プロトコル

（注） [Other] を選択する場合は、[Protocol] テキスト ボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。

コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。

e) 前の手順で [TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つのパラメータも追加で表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。

（注） ACL タイプに基づく送信元および宛先ポート。

f) [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダー テキスト ボックスです。

- [Any]：任意の DSCP（これはデフォルト値です）
- [Specific]：DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

g) [Direction] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するトラフィックの方向を指定します。

- [Any]：任意の方向（これはデフォルト値です）
- [Inbound]：クライアントから
- [Outbound]：クライアントへ

（注） この ACL をコントローラ CPU に適用する予定の場合、パケットの方向は重要ではないので常に「Any」です。

h) [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

i) [Apply] をクリックして、変更を確定します。[Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。

[Deny Counters] フィールドには、パケットが明示的拒否 ACL ルールに一致した回数が表示されます。[Number of Hits] フィールドには、パケットが ACL ルールに一致した回数が表示されます。これらのフィールドを有効にするには、[Access Control Lists] ページ上で ACL カウンタを有効にする必要があります。

（注） ルールを編集する場合は、目的のルールのシーケンス番号をクリックして、[Access Control Lists] > [Rules] > [Edit] ページを開きます。ルールを削除するには、該当するルールの青いドロップダウン矢印の上にカーソルを置き、[Remove] を選択します。

j) この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 9 [Save Configuration] をクリックして、変更を保存します。

ステップ 10 さらに ACL を追加するにはこの手順を繰り返します。

関連トピック

FlexConnect アクセス コントロール リストの設定（GUI）

インターフェイスへのアクセス コントロール リストの適用

手順

ステップ 1 [Controller] > [Interfaces] の順に選択します。

ステップ 2 目的のインターフェイスの名前をクリックします。そのインターフェイスの [Interfaces > Edit] ページが表示されます。

ステップ 3 [ACL Name] ドロップダウン リストから必要な ACL を選択し、[Apply] をクリックします。デフォルトは [None] です。

（注） インターフェイス ACL としてサポートされるのは IPv4 ACL だけです。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

コントローラ CPU へのアクセス コントロール リストの適用

手順

ステップ 1 [Security] > [Access Control Lists] > [CPU Access Control Lists] の順に選択して、[CPU Access Control Lists] ページを開きます。

ステップ 2 [Enable CPU ACL] チェックボックスをオンにして、指定した ACL でコントローラの CPU への IPv4 トラフィックを制御できるようにするか、チェックボックスをオフにして CPU ACL の機能を無効にし、CPU にすでに適用されている ACL をすべて削除します。デフォルト値はオフです。

ステップ 3 [ACL Name] ドロップダウン リストから、コントローラの CPU への IPv4 トラフィックを制御する ACL を選択します。デフォルト値は [None] で、CPU ACL 機能は無効にされています。

[Enable CPU ACL] チェックボックスをオンにして [None] を選択すると、ACL を選択する必要があることを示すエラー メッセージが表示されます。

（注） このパラメータは、[CPU ACL Enable] チェックボックスをオンにした場合のみ使用できます。

（注） CPU ACL が有効な場合、その CPU ACL は無線トラフィックと有線トラフィックの両方に適用されます。

ステップ 4 [Enable CPU IPv6 ACL] チェックボックスをオンにして、指定した ACL でコントローラの CPU への IPv6 トラフィックを制御できるようにするか、チェックボックスをオフにして CPU ACL の機能を無効にし、CPU にすでに適用されている ACL をすべて削除します。デフォルト値はオフです。

（注） CPU IPv6 ACL の場合、HTTP/Telnet の許可ルールとともに、CPU IPv6 ACL を機能させるために ICMPv6（NA/ND は ICMPv6 を使用）を許可するルールを追加する必要があります。

ステップ 5 [IPv6 ACL Name] ドロップダウン リストから、コントローラの CPU への IPv6 トラフィックを制御する ACL を選択します。デフォルト値は [None] で、CPU ACL 機能は無効にされています。[Enable CPU IPv6 ACL] チェックボックスをオンにして [None] を選択すると、ACL を選択する必要があることを示すエラー メッセージが表示されます。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

WLAN へのアクセス コントロール リストの適用

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

ステップ 4 [Override Interface ACL] ドロップダウン リストから、この WLAN に適用する IPv4 または IPv6 ACL を選択します。選択した ACL は、インターフェイスに設定されたすべての ACL を上書きします。デフォルト値は [none] です。

（注） ISE や ACS などの AAA サーバを介した中央集中型のアクセス制御をサポートするには、コントローラに IPv6 ACL を設定し、WLAN で AAA Override 機能を有効にする必要があります。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

WLAN への事前認証アクセス コントロール リストの適用

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Web Policy] チェックボックスをオンにします。

ステップ 5 [Preauthentication ACL] ドロップダウン リストから目的の ACL を選択し、[Apply] をクリックします。デフォルト値は [none] です。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

アクセス コントロール リストの設定

手順

ステップ 1 次のコマンドを入力して、コントローラ上に設定されているすべての ACL を表示します。

show [**ipv6**] **acl summary**

ステップ 2 次のコマンドを入力して、特定の ACL の詳細情報を表示します。

show [**ipv6**] **acl detailed** *acl_name*

パケットが ACL ルールと一致するたびに、[Counter] テキスト ボックスの値が増加します。[DenyCounter] テキスト ボックスの値は、パケットがいずれのルールとも一致しない場合に増加します。

（注） 許可ルールによってトラフィック/要求がコントローラから許可されると、反対方向でもトラフィック/要求への応答が許可され、ACL の拒否ルールではブロックできなくなります。

ステップ 3 次のコマンドを入力して、コントローラの ACL カウンタを有効または無効にします。

config acl counter {**start** | **stop**}

（注） ACL の現在のカウンタをクリアする場合は、**clear acl counters** *acl_name* コマンドを入力します。

ステップ 4 次のコマンドを入力して、新しい ACL を追加します。

config [ipv6] **acl create** *acl_name*

acl_name パラメータには、最大 32 文字の英数字を入力できます。

（注） スペースが含まれたインターフェイス名を作成しようとすると、コントローラ CLI でインターフェイスは作成されません。たとえば、int3 というインターフェイス名を作成しようとすると、int と 3 の間にスペースがあるため CLI でこのインターフェイス名は作成されません。int 3 をインターフェイス名として使用するには、'int 3' のように単一引用符で囲む必要があります。

ステップ 5 次のコマンドを入力して、ACL のルールを追加します。

config [ipv6] acl rule add acl_name rule_index

ステップ 6 **config [ipv6] acl rule** コマンドを入力して、ACL ルールを設定します。

ステップ 7 次のコマンドを入力して、設定を保存します。

save config

（注） ACL を削除するには、**config** [**ipv6**] **acl delete** *acl_name* コマンドを入力します。ACL ルールを削除するには、**config** [**ipv6**] **acl rule delete** *acl_name rule_index* コマンドを入力します。

アクセス コントロール リストの適用

手順

ステップ 1 IPv4 ACL を適用するには、次のように実行します。

- ACL を IPv4 データ パスに適用するには、次のコマンドを入力します。

  config acl apply acl_name

- ACL をコントローラの CPU に適用して、CPU に転送されるトラフィックの IPv4 タイプ（有線、無線、または両方）を制限するには、次のコマンドを入力します。

  config acl cpu acl_name {wired | wireless | both}

  （注） コントローラ CPU に適用されている ACL を表示するには、**show acl cpu command** を入力します。コントローラ CPU に適用されている ACL を削除するには、**config acl cpu none** コマンドを入力します。

ステップ 2 IPv6 ACL を適用するには、次のように実行します。

- ACL を IPv6 データ パスに適用するには、次のコマンドを入力します。

  config ipv6 acl apply name

- ACL をコントローラの CPU に適用して、CPU に転送されるトラフィックの IPv6 タイプ（有線、無線、または両方）を制限するには、次のコマンドを入力します。

config ipv6 acl cpu {name|none}

ステップ 3 ACL を WLAN に適用するには、次のコマンドを入力します。

- **config wlan acl***wlan_idacl_name*

（注） WLAN に適用されている ACL を表示するには、**show wlan** *wlan_id* コマンドを入力します。WLAN に適用されている ACL を削除するには、**config wlan acl** *wlan_id* **none** コマンドを入力します。

ステップ 4 事前認証 ACL を WLAN に適用するには、次のコマンドを入力します。

- **config wlan security web-authacl** *wlan_id acl_name*

ステップ 5 次のコマンドを入力して、変更を保存します。
save config

レイヤ 2 アクセス コントロール リストの設定

レイヤ 2 アクセス コントロール リストの設定について

パケットに関連付けられた EtherType に基づいてレイヤ 2 アクセス コントロール リスト（ACL）のルールを設定できます。中央スイッチングの WLAN に PPPoE クライアントのみをサポートさせる必要がある場合は、この機能を使用してレイヤ 2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから PPPoE パケットのみを許可することができます。同様に、WLAN に IPv4 クライアントまたは IPv6 クライアントのみをサポートさせる必要がある場合は、レイヤ 2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから IPv4 または IPv6 パケットのみを許可することができます。ローカルにスイッチされる WLAN の場合、WLAN または FlexConnect AP のいずれかに同じレイヤ 2 ACL を適用できます。AP 固有のレイヤ 2 ACL は FlexConnect AP にのみ設定できます。これは、ローカルにスイッチされる WLAN にのみ適用されます。FlexConnect AP に適用されるレイヤ 2 ACL は WLAN に適用されるレイヤ 2 ACL よりも優先されます。

モビリティのシナリオでは、モビリティ アンカー設定が適用できます。

次のトラフィックはブロックされません。

- ワイヤレス クライアントのワイヤレス トラフィック
  - 802.1X
  - Inter-Access Point Protocol
  - 802.11
  - Cisco Discovery Protocol

- 分散システムのトラフィック
  - Broadcast
  - マルチキャスト
  - IPv6 ネイバー探索プロトコル（NDP）
  - アドレス解決プロトコル（ARP）および Gratuitous ARP の保護（GARP）
  - Dynamic Host Configuration Protocol（DHCP）
  - ドメイン ネーム システム（DNS）

WLAN にマッピングされているレイヤ 2 ACL

WLAN にレイヤ 2 ACL をマッピングすると、設定したレイヤ 2 ACL がその WLAN に関連付けられたすべてのクライアントに適用されます。

レイヤ 2 ACL を中央でスイッチされる WLAN にマッピングすると、EtherType に基づいてトラフィックを渡すルールが WLAN に関連付けられたすべてのクライアントに対してファスト パスにより決定されます。ファスト パスは、パケットに関連付けられたイーサネット ヘッダー内を検索し、ACL に対して設定されたものと一致する Ethertype を持つパケットを転送します。

レイヤ 2 ACL をローカルにスイッチされる WLAN にマッピングすると、EtherType に基づいてトラフィックを渡すルールが WLAN に関連付けられたすべてのクライアントに対して AP の転送プレーンにより決定されます。AP の転送プレーンは、パケットに関連付けられたイーサネット ヘッダー内を検索し、Ethertype が ACL に対する設定と一致するアクションに基づいてパケットを転送または拒否します。

（注） 中央スイッチングと中央認証を実行する設定の WLC デバイスには、ローミング ユーザに誤って適用されているレイヤ 2 ACL の名前が表示されます。このような状況が発生するのは、認証デバイスがアンカー コントローラから外部コントローラにレイヤ 3 ローミングを実行したときです。ローミング後、管理者が外部コントローラの CLI で **show acl layer2 summary** コマンドを発行すると、誤った情報が表示されます。アンカーから適用された ACL は、コントローラ間でローミングするとき、認証クライアントに従うと思われます。

レイヤ 2 アクセス コントロール リストの制約事項

- レイヤ 2 ACL に対して最大 16 のルールを作成できます。
- AP 固有のレイヤ 2 ACL は FlexConnect AP にのみ設定できます。これは、ローカルにスイッチされる WLAN にのみ適用されます。
- コントローラには、最大で 64 個の レイヤ 2 ACL を作成できます。
- AP は最大 16 の WLAN をサポートするので、AP ごとに最大 16 のレイヤ 2 ACL がサポートされます。

- AP はレイヤ 2 およびレイヤ 3 の同じ ACL 名をサポートしないため、レイヤ 2 ACL 名が FlexConnect ACL 名と競合しないことを確認します。

レイヤ 2 アクセス コントロール リストの設定（CLI）

手順

- **config acl layer2** {**create** | **delete**} *acl-name*：レイヤ 2 ACL を作成または削除します。
- **config acl layer2 apply** *acl-name*：レイヤ 2 ACL をデータ パスに適用します。
- **config acl layer2 rule** {**add** | **delete**} *acl-rule-name index*：レイヤ 2 ACL を作成または削除します。
- **config acl layer2 rule change index** *acl-rule-name old-index new-index*：レイヤ 2 ACL ルールのインデックスを変更します。
- **config acl layer2 rule action** *acl-rule-name index* {*permit* | *deny*}：ルールのアクションを設定します。
- **config acl layer2 rule etherType** *name index ether-type-number-in-hex ether-type-mask-in-hex*：ルールの宛先 IP アドレスおよびネットマスクを設定します。
- **config acl layer2 rule swap index** *acl-rule-name index-1 index-2*：2 つのルールのインデックス値を入れ替えます。
- **config acl counter** {**start** | **stop**}：ACL カウンタを開始または停止します。このコマンドはすべての ACL のタイプに適用されます。HA 環境では、カウンタは、アクティブ コントローラとスタンバイ コントローラ間では同期されません。
- **show acl layer2 summary**：レイヤ 2 ACL プロファイルの概要を表示します。
- **show acl layer2 detailed** *acl-name*：指定されたレイヤ 2 ACL プロファイルの詳細な説明を表示します。
- **show client detail** *client-mac-addr*：クライアントに適用されるレイヤ 2 ACL ルールを表示します。

WLAN とレイヤ 2 ACL のマッピング（CLI）

これは、中央でスイッチされる WLAN、および FlexConnect アクセス ポイントがなくローカルにスイッチされる WLAN に適用されます。

手順

- **config wlan layer2 acl** *wlan-id acl-name*：レイヤ 2 ACL を中央でスイッチされる WLAN にマッピングします。
- **config wlan layer2 acl** *wlan-id none*：WLAN にマッピングされたレイヤ 2 ACL をクリアします。
- **show wlan** *wlan-id*：WLAN にマッピングされたレイヤ 2 ACL のステータスを表示します。

FlexConnect アクセス ポイントを使用したローカルにスイッチされる WLAN とレイヤ 2 ACL のマッピング（CLI）

これは、FlexConnect アクセス ポイントを持つローカルにスイッチされる WLAN に適用されます。

手順

- **config ap flexconnect wlan l2acl add** *wlan-id ap-name acl-name*：レイヤ 2 ACL をローカルにスイッチされる WLAN にマッピングします。
- **config ap flexconnect wlan l2acl** *delete wlan-id ap-name*：マッピングを削除します。
- **show ap config general** *ap-name*：マッピングの詳細を表示します。

レイヤ 2 アクセス コントロール リストの設定（GUI）

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[Layer2 ACLs]** の順に選択して、[Layer2 Access Control Lists] ページを開きます。

ステップ 2 [New] をクリックして、新しい ACL を追加します。[Layer2 Access Control Lists > New] ページが表示されます。

ステップ 3 [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。[Layer2 Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 5 [Layer2 Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Layer2 Access Control Lists > Rules > New] ページが表示されます。

ステップ 6 この ACL のルールを次のように設定します。

a) コントローラは各 ACL について最大 16 のルールをサポートします。これらのルールは、1 から 16 の順にリストアップされます。[Sequence] テキスト ボックスで、値（1 ～ 16）を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

（注） ルール 1 ～ 4 がすでに定義されている場合にルール 15 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b) [Ether Type] ドロップダウン リストから、次のイーサネット タイプのいずれかのオプションを選択します。

- AppleTalk Address Resolution Protocol
- VLAN-tagged Frame & Short Path Bridging

- IPX (0x8137)
- IPX (0x8138)
- QNS Qnet
- Internet Protocol Version 6
- Ethernet Flow Control
- Slow Protocol
- CobraNet
- MPLS Unicast
- MPLS Multicast
- PPPoE Discovery Stage
- PPPoE Session Stage
- Jumbo Frames
- HomePlug 1.0 MME
- EAP over LAN
- PROFINET over Protocol
- HyperSCSI
- ATA over Ethernet
- EtherCAT Protocol

（注） [Ether Type] ドロップダウン リストから定義済みのイーサネット タイプを選択することもできますし、[Ether Type] ドロップダウン リストのカスタム オプションを使用して独自のイーサネット タイプ値を入力することもできます。

c) [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。
d) [Apply] をクリックして、変更を確定します。[Layer2 Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。
e) この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

ステップ 8 さらに ACL を追加するにはこの手順を繰り返します。

WLAN へのレイヤ 2 アクセス コントロール リストの適用（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

ステップ 4 [Layer2 ACL] ドロップダウン リストから、作成した ACL を選択します。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

WLAN の AP へのレイヤ 2 アクセス コントロール リストの適用（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[All APs]** の順に選択して、[All APs] ページを開きます。

ステップ 2 目的のアクセス ポイントの名前をクリックして、[All APs > Details] ページを開きます。

ステップ 3 [All APs > Details] ページで、[FlexConnect] タブをクリックします。

ステップ 4 [PreAuthentication Access Control Lists] 領域で、[Layer2 ACLs] リンクをクリックして [ACL Mappings] ページを開きます。

ステップ 5 [WLAN ACL Mapping] 領域の [Layer2 ACL] ドロップダウン リストから、作成した ACL を選択して [Add] をクリックします。

ステップ 6 設定を保存します。

DNS ベースのアクセス コントロール リストの設定

DNS ベースのアクセス コントロール リストについて

DNS ベースの ACL は、Apple および Android デバイスなどのクライアント デバイスに使用されます。これらのデバイスを使用する場合、デバイスがアクセス権を持つ範囲を特定するために Cisco WLC に事前認証 ACL を設定できます。

Cisco WLC で DNS ベースの ACL を有効にするには、ACL の許可された URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。Cisco WLC は ACL 名で設定され、事前認証 ACL が適用されるように AAA サーバによって返されます。ACL 名が AAA サーバによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

クライアント認証フェーズでは、ISE サーバが事前認証 ACL （url-redirect acl）を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL が Cisco WLC で受信されると、CAPWAP ペイロードは AP に送信され、クライアントの DNS スヌーピングが有効になり URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。ドメイン名が設定された URL に一致すると、DNS 応答が IP アドレスについて解析され、IP アドレスは CAPWAP ペイロードとして Cisco WLC に送信されます。Cisco WLC によっ

てIPアドレスの許可リストにIPアドレスが追加されるため、クライアントは設定されたURLにアクセスできます。

リリース 8.0 では、ローカル Web 認証に DNS ベースの ACL のサポートが追加されました。

DNS ベースのアクセス コントロール リストの制約事項

- 最大 10 の URL をアクセス コントロール リストに許可できます。
- Cisco WLC では、1 つのクライアントに対して 20 の IP アドレスが許可されています。
- ローカル認証は FlexConnect AP でサポートされていません。
- DNS ベースの ACL は、ローカル スイッチングを使用した FlexConnect AP ではサポートされません。
- 認証トラフィックは、DNS ベースの ACL が AP に対してローカルであっても、この機能がサポートされるように Cisco WLC を経由する必要があります。
- クライアントがアンカーされている場合は、自動アンカーにしないと、ローミング後に、DNS ベースの ACL が動作しません。

DNS ベースのアクセス コントロール リストの設定（CLI）

手順

ステップ 1 ACL を作成するように指定します。最大32文字の英数字でIPv4 ACLの名前を入力できます。

config acl create *name*

例：

```
(Cisco Controller) >> config acl create android
```

ステップ 2 アクセスコントロールリストの新しいURLドメインを追加するように指定します。URLドメイン名は有効な形式（たとえば、Cisco.com、bbc.in、または play.google.com）で指定する必要があります。ホスト名比較は、一致するサブストリングです（ワイルドカードベース）。作成済みの ACL 名を使用する必要があります。

config acl url-domain add *domain-name acl-name*

例：

```
(Cisco Controller) >> config acl url-domain add cisco.com android
(Cisco Controller) >> config acl url-domain add play.google.com android
```

ステップ 3 アクセス コントロール リストの既存の URL ドメインを削除するように指定します。

config acl url-domain delete *domain-name acl-name*

例：

```
(Cisco Controller) >> config acl url-domain delete cisco.com android
```

ステップ 4 ACL を適用するように指定します。

config acl apply *acl-name*

例：

```
(Cisco Controller) >> config acl apply android
```

ステップ 5 次のコマンドを入力して、DNS ベースの ACL 情報を表示します。

show acl summary

例：

```
(Cisco Controller) >> show acl summary

ACL Counter Status              Disabled
----------------------------------------
IPv4 ACL Name                    Applied
-------------------------------- -------
android                          No
StoreACL                         Yes
----------------------------------------
IPv6 ACL Name                    Applied
-------------------------------- -------
```

ステップ 6 次のコマンドを入力して、DNS ベースの ACL 詳細情報を表示します。

show acl detailed *acl-name*

例：

```
(Cisco Controller) >> show acl detailed android
o rules are configured for this ACL.
DenyCounter : 0
URLs configured in this ACL
---------------------------
*.play.google.com
*.store.google.com
```

ステップ 7 次のコマンドを入力して、DNS スヌーピング（DNS ベースの ACL）によって学習されたクライアントごとの IP アドレスを表示します。

show client detail *mac-address*

例：

```
(Cisco Controller) >> show client detail mac-address
```

ステップ 8 DNS ベースの ACL に関連する情報のデバッグを有効にします。

debug aaa events enable

例：

```
(Cisco Controller) >> debug aaa events enable
```

DNS ベースのアクセス コントロール リストの設定（GUI）

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択して、[Access Control Lists] ページを開きます。

ステップ 2 パケットがコントローラに設定されたACLのいずれかに一致するかどうかを確認する場合は、[Enable Counters] チェックボックスをオンにして [Apply] をクリックします。それ以外の場合、このチェックボックスはオフ（デフォルト値）のままにしておきます。この機能は、システムのトラブルシューティングを実行する際に役立ちます。

（注） ACLのカウンタをクリアするには、そのACLの青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

ステップ 3 [New] をクリックして、新しい ACL を追加します。[Access Control Lists > New] ページが表示されます。

ステップ 4 [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 5 ACL タイプとして IPv4 を選択します。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。ACL に IP ルールはありません。青いドロップダウンの矢印の上にカーソルを置き、ドロップダウン リストから [Add-Remove URL] を選択して[URL List] ページを開きます。

ステップ 8 ACL の新しいURL ドメインを追加するには、[URL String Name] テキスト ボックスにアクセス コントロール リストの新しいURL ドメインを入力します。URL ドメイン名は有効な形式（たとえば、Cisco.com、bbc.in、または play.google.com）で指定する必要があります。

ステップ 9 URL ドメインを削除するには、削除する URL 名の下の青いドロップダウン矢印の上にカーソルを置いて [Delete] を選択します。

URL フィルタリングの設定

URL フィルタリングについて

URL フィルタリング機能はインターネット Web サイトへのアクセスを制御します。URL フィルタリング機能は、URL アクセス コントロール リスト（ACL）の情報に基づいて特定の Web サイトへのアクセスを許可または拒否して制御します。URL フィルタリングは、ACL リストに基づいてアクセスを制限します。

ロケーション ベースのフィルタリングで、AP はさまざまな AP グループに分けられ、WLAN のプロファイルが、同じ SSID 内でクライアントを信頼できるクライアントと、信頼できない

クライアントに分類します。信頼できるクライアントが信頼できない AP に移動した場合や、その逆の場合、この分類に従って、新しい VLAN で再認証が実行されます。

コントローラは、最大 64 の ACL をサポートします。これらの ACL は、要求を許可または拒否するよう設定され、さまざまなインターフェイスと関連付けることができ（WLAN、LAN など）、さらに効果的なフィルタリングを実現できます。ポリシーは、WLAN や適用するグローバル ポリシーとは異なる AP グループでローカルに実装できます。

ポリシーの優先順位は次のとおりです。

1. ポリシー（Policy）
2. インターフェイス
3. WLAN

（注） デフォルト設定では、要求 URL が適用した ACL に一致しない場合に要求を拒否します。

各 ACL でサポートされるルール（URL）の数は、コントローラによって異なります。

- Cisco 5508 WLC および WiSM2 は、1 つの ACL で 64 のルールをサポートします。
- Cisco 5520、8540 コントローラは、1 つの ACL で 100 のルールをサポートします。

URL フィルタリングの制約事項

- URL フィルタリングは次のコントローラではサポートされていません。
  - Cisco vWLC
  - Cisco Mobility Express
- この機能は、ローカル スイッチングではなく WLAN 中央スイッチングでのみサポートされています。
- ローカル スイッチングが有効な FlexConnect モードではサポートされていません。
- 次の URL タイプはサポートされていません。
  - ワイルドカードの URL（例：www.uresour*loc.com）。
  - サブ URL（例：www.uresour* loc.com/support）。
  - サブドメイン（例：reach.url.com または sub1.url.com）
- URL 名の長さは 32 文字に制限されています。
- 一致した URL の AVC プロファイルはありません。一致した URL の ACL アクション サポート。

- ホワイト リストとブラックリストは、それぞれ要求を許可または拒否するために、ACL の「*」暗黙のルールを使用して作成できます。
- HTTP URL だけがサポートされています。
- URL フィルタリング ACL 名を返す RADIUS サーバはサポートされていません。
- 次のような状況では、ACL のフィルタ処理が失敗することがあります。
  - URL がフラグメント化されたパケットにまたがっている。
  - IP パケットがフラグメント化されている。
  - URL の代わりに直接 IP アドレスまたはプロキシ設定が使用されている。

URL フィルタリングの設定（GUI）

アクセス コントロール リストの設定（GUI）

WLAN でアクセス コントロール リストを作成または削除するには、以下の手順を実行します。

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[URL ACLs]** を選択し、[URL Access Control Lists] ページを開きます。

ステップ 2 [Enable URL Acl] チェックボックスをオンにし、URL ACL 機能を有効にします。

ステップ 3 [New] をクリックして、新しい ACL を追加します。**[URL Access Control Lists]** > **[New]** ページが表示されます。
[URL ACL Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。

- さらに URL ACL を追加するにはこの手順を繰り返します。
- URL ACL を削除するには、[URL Access Control Lists] ページで、その ACL の青いドロップダウン矢印にマウス カーソルを合わせ、[Remove] を選択します。

（注） ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

URL ACL リストの設定（GUI）

URL ACL リスト内のルールを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**[Security]** > **[Access Control Lists]** > **[URL ACLs]** を選択して、[URL Access Control Lists] ページを開きます。	
ステップ 2	URL ACL を選択します。	**[URL Access Control Lists]** > **[Edit]** ページが表示されます。
ステップ 3	[Add New Rule] を選択します。	
ステップ 4	ドロップダウン メニューからこの ACL のルールを設定します。	• [Rule Index]：1 ～ 100 の範囲。 • [URL]：URL アドレスを入力します。 • [Action]：[Permit] または [Deny] を選択します。
ステップ 5	[Apply] をクリックします。	さらにルールを追加するにはこの手順を繰り返します。 （注） デフォルト ポート 80 の代わりに異なるポート番号を使用する Web サイトにシームレスにアクセスできるようにするには、「URL 名:ポート番号」の形式で、ポート番号を含むルールを作成する必要があります。例：URL に website.com:8080 と入力し、permit アクションを適用します。

URL フィルタリング アクセス コントロール リストのグローバルな適用（GUI）

ネットワーク全体に URL ACL を適用します。

手順

ステップ 1 **[Security]** > **[Local Policies]** を選択して、ローカル ポリシー ページを開きます。

ステップ 2 目的のポリシーを選択します。

[Policy] > **[Edit]** ページが表示されます。

ステップ 3 [Match Role String] をテキスト ボックスに入力します。

ステップ 4 [URL ACL] ドロップダウン リストから URL ACL を選択します。

ステップ 5 [Apply] をクリックします。

（注） [Match Role String] 名は、Cisco AV ペアのロール名に一致する必要があります。

URL フィルタリング アクセス コントロール リストのインターフェイスへの適用（GUI）

ネットワーク内のインターフェイスに URL ACL を適用します。

手順

ステップ 1 Choose **Controller** > **Interfaces** to open the interface page.

ステップ 2 Choose the desired interface.

The interface page for the selected interface appears.

ステップ 3 Select the URL ACL from the **URL ACL** drop-down list.

ステップ 4 Click **Apply**.

WLAN に対する URL フィルタリング アクセス コントロール リストの適用（GUI）

ネットワーク内の WLAN に URL ACL を適用します。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [URL ACL] ドロップダウン リストから、この WLAN に適用する ACL を選択します。

ステップ 5 [Apply] をクリックします。

WLAN へのポリシーのマッピング（GUI）

ネットワーク内の WLAN にポリシーをマッピングします。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 [Policy-Mapping] タブを選択します。

1. [Priority Index] の値を入力します。
2. [Local Policy] ドロップダウン リストからローカル ポリシーを選択します。
3. [Add] をクリックします。

ステップ 4 [Apply] をクリックします。

WLAN のポリシー マッピングの削除（GUI）

この手順は、WLAN のポリシー マッピングを削除するのに役立ちます。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 そのローカル ポリシーの青いドロップダウン矢印にマウス カーソルを合わせます

ステップ 4 [Remove] を選択します。

確認用のダイアログボックスが表示されます。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックします。

AP グループへのポリシーのマッピング（GUI）

ネットワークの AP グループにポリシーをマッピングします。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 **[Advanced]** > **[AP Groups]** を選択します。

ステップ 3 [AP Group] を選択します。

[AP Groups] > **[Edit]** ページが表示されます。

ステップ 4 [WLANs] タブを選択します。

ステップ 5 必要な WLAN の青いドロップダウン矢印にマウス カーソルを合わせ、[Policy-Mapping] を選択します。

ステップ 6 **[AP Group]** > **[Policy]** > **[Mappings]** ページで、

1. [Priority Index] の値を入力します。
2. [Local Policy] ドロップダウン リストからローカル ポリシーを選択します。
3. [Add] をクリックします。

ステップ 7 [Apply] をクリックします。

WLAN と AP グループは、ローカル ロールに基づくポリシーです。

URL フィルタリングの設定（CLI）

URL フィルタリングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、URL ベースのフィルタリング機能を設定します。
config acl url-acl {**enabled | disable**}

ステップ 2 次のコマンドを入力して、URL ACL を作成または削除します。
config acl url-acl{ **create | delete**} *id-token*

ステップ 3 次のコマンドを入力して、URL ACL をデータ パスに適用します。
config acl url-acl apply*acl-name*

ステップ 4 次のコマンドを入力して、ACL をインターフェイスに設定します。
config interface url-acl *interface-name acl-name*

ステップ 5 次のコマンドを入力して、ACL を WLAN に設定します。
config wlan url-acl *wlan-id acl-name*

アクセス コントロール リスト ルールの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、ACL を作成または削除します。
config acl url-acl rule{ **add | delete**} *acl-name index*

ステップ 2 次のコマンドを入力して、有効な形式（例：www.cisco.com）の URL アドレスを設定します。
config acl url-acl rule url*acl-name index url-name*

ステップ 3 次のコマンドを入力して、ルールのアクション を設定します。
config acl url-acl rule action *acl-name index*{ **permit | deny**}

（注） デフォルト ポート 80 の代わりに異なるポート番号を使用する Web サイトにシームレスにアクセスできるようにするには、「URL 名:ポート番号」の形式で、ポート番号を含むルールを作成する必要があります。例：URL に website.com:8080 と入力し、permit アクションを適用します。

ローカル ポリシーの適用（CLI）

手順

ステップ 1 次のコマンドを入力して、ローカル プロファイリング ポリシーを作成または削除します。
config policy *policy-name*{**create | delete**}

ステップ 2 次のコマンドを入力して、ポリシーに一致タイプを設定します。
config policy *policy-name* **match role** {**role-name| none**}

ステップ 3 次のコマンドを入力して、ポリシーにアクションを設定します。
config policy *policy-name* **action url-acl** {**enable | disable**} *acl-name*

ステップ 4 次のコマンドを入力して、WLAN にローカル ポリシーを有効化します。
config wlan policy add *priority-index policy-name wlan-id*

ステップ 5 次のコマンドを入力して、WLAN の AP グループにローカル ポリシーを追加または削除します。
config wlan apgroup policy {**add | delete**} *priority-index policy-name ap-group-name wlan-id*

URL フィルタリングの表示（CLI）

手順

- 次のコマンドを入力して、ACL の概要を表示します。

  show acl url-acl summary

- 次のコマンドを入力して、詳細な URL ACL プロファイル情報を表示します。

  show acl url-acl detailed *acl-name*

- 次のコマンドを入力して、ポリシーの詳細を表示します。

  show policy {**summary**| *policy-name*}

- 次のコマンドを入力して、MAC アドレスごとのクライアントの詳細を表示します。
  show client detail *mac-address*
- 次のコマンドを入力して、WLAN の設定の詳細を表示します。
  show wlan*wlan-id*
- 次のコマンドを入力して、インターフェイスの詳細を表示します。
  show interface detailed *interface-name*
- 次のコマンドを入力して、カウンタをクリアします。
  clear url-acl-counters

URL フィルタリングのトラブルシューティング（CLI）

次のコマンドを入力して、URL フィルタリング機能をトラブルシューティングできます。

手順

- **debug fastpath dump urlacldb** *aclid ruleindex dataplane*
- **debug fastpath dump stats** *dataplane*

  指定可能なデータプレーン オプションは、0、1、All です。

- **debug fastpath dump scbdb**

CNAME IPv6 フィルタリング

CNAME IPv6 フィルタリングについて

この機能では、ネットワーク内の FQDN 経由で IPv6 アドレスを使用して、Cisco WLC と外部の AAA サーバ経由でクライアント トラフィックを認証できます。クライアントの事前認証は、内部または外部の URL ACL を使用するように設定できます。

この機能が作用するためには、SSIDを中央スイッチングに設定し、APをローカルモードに設定する必要があります。

CNAME IPv6 フィルタリングの制約事項

- Cisco 3504、5520、8540 WLC でのみサポートされています。
- サポートされる ACL の最大数は 64 です。
- ACL でサポートされるルールの最大数は 20 です。
- 解決済みの IP の総数は 40 です。
- 異なるパケットでの CNAME 解析はサポートされていません。
- FlexConnect モードの AP はサポートされていません。

CNAME URL ACL の設定（GUI）

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[URL ACLs]** を選択し、[URL Access Control Lists] ページを開きます。

ステップ 2 [New] をクリックして、新しい ACL を追加します。

[URL Access Control Lists] > **[New]** ページが表示されます。[URL ACL Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 3 設定する URL ACL 名をクリックします。

ステップ 4 （注） 要求されたトラフィックのクライアントへの送信を AAA サーバが許可または拒否できるように、WLC の事前認証 IPv4 ACL に IPv6 サーバの FQDN を追加できます。

[Add New Rule] をクリックします。

ステップ 5 ドロップダウンリストからこの ACL のルールを設定します。

- [Rule Index]：1 ～ 100 の範囲。
- [URL]：URL アドレスを入力します。

（注） IPv6 アドレスを使用するには、サーバ アドレスの FQDN を追加します。

ステップ 6 [Apply] をクリックします。

URL ACL にさらにルールを追加する場合はこの手順を繰り返します。

ステップ 7 URL ACL 内のルールを削除する場合は、[URL Access Control Lists] > [Edit] ページで、その ACL の青いドロップダウン矢印にマウス オーバーして、[Remove] を選択します。

ステップ 8 URL ACL を削除するには、[URL Access Control Lists] ページで、その ACL の青いドロップダウン矢印にマウス カーソルを合わせ、[Remove] を選択します。

ステップ 9 ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

WLANでのCNAMEIPv6フィルタリングのためのWeb認証の設定（GUI）

手順

ステップ 1 **[Security]** > **[Authentication]** タブを選択します。

ステップ 2 [New] をクリックして新しい RADIUS サーバを追加するか、既存のサーバの [Server Index] をクリックします。

ステップ 3 [Support for CoA] ドロップダウン リストから [Enable] を選択します。

ステップ 4 **[WLAN]** > **[WLAN ID]** > **[Security]** > **[Layer 3]** を選択して、[Layer 3] ページを開きます。

ステップ 5 [Layer 3 Security] ドロップダウン リストから、[Web Policy] を選択します。

ステップ 6 [Preauthentication ACL IPv4] ドロップダウン リストから URL ACL を選択します。

ステップ 7 [Apply] をクリックします。

外部 RADIUS サーバを使用した CNAME IPv6 フィルタリングのための Web 認証の設定（GUI）

手順

ステップ 1 **[Security]** > **[Authentication]** タブを選択します。

ステップ 2 [New] をクリックして新しい RADIUS サーバを追加するか、既存のサーバの [Server Index] をクリックします。

新しい RADIUS サーバを追加する場合は、各フィールドに適切な詳細情報を入力します。

ステップ 3 [Support for CoA] ドロップダウン リストから [Enable] を選択します。

ステップ 4 **[WLAN]** > **[WLAN ID]** > **[Advanced]** を選択して、[Advanced] ページを開きます。

ステップ 5 [NAC State] ドロップダウン リストから [ISE NAC] を選択します。

ステップ 6 [Apply] をクリックします。

IPv6 CNAME フィルタリングの設定（CLI）

手順

- 次のコマンドを入力して、URL ACL を作成します。
  config acl create *acl-name*
- 次のコマンドを入力して、URL ACL に URL ルールを追加します。
  config acl URL-domain add *domain-name acl-name*
- 次のコマンドを入力して、URL ACL を有効にします。
  cofig acl apply *acl-name*
- 次のコマンドを入力して、ACL の概要を表示します。
  show acl summary
- 次のコマンドを入力して、詳細な ACL プロファイルの統計情報を表示します。
  show acl detailed *acl-name*

ドメインベースのフィルタリング

ドメイン ベースのフィルタリングについて

この機能を使用すると、DNS ベースのアクセス コントロール リスト（ACL）を使用して Web サイトへのアクセスを許可または拒否することで、Web サイトへのアクセスを制御できます。

Cisco 3504、5520、および 8540 ワイヤレス コントローラ（WLC）は、最大 64 の ACL をサポートします。これらの ACL は、任意のプロトコルのホワイトリストやブラックリストに基づいて、トラフィックを許可または拒否するように設定されます。そのため、URL 要求がブロックされると、プロトコルに関係なくアクセスが拒否されます。ACL は、ホワイトリスト（許可）またはブラックリスト（拒否）のいずれかにすることができます。ACL 内では、独立した許可または拒否の設定があるルールはサポートされていません。各 ACL は最大 100 個のルール（URL）をサポートします。

（注） デフォルトでは、適用された ACL に一致しないすべての URL が拒否されます。

ACL は、次の優先順位を使用して、さまざまなインターフェイス（WLAN、LAN など）と関連付けることができます。

1. ロールベースのポリシー
2. インターフェイス
3. WLAN

（注） 適用されたグローバル ポリシーとは異なるポリシーを WLAN または AP グループでローカルに実装できます。

ドメイン ベースのフィルタリングの制約事項

- 次はサポートされていません。
  - vWLC
  - Mobility Express
- WLAN 中央スイッチングでのみサポートされています。
- ローカル スイッチングやローカル スイッチングが有効な FlexConnect モードではサポートされていません。
- ACL には最大 10 のワイルドカードの URL（*. example.com など）とワイルドカードあたり 5 つのサブドメイン（sub.example.com など）を設定できます。
- サブ URL は認められていません（www.example.com/support など）。
- URL 名は最大 255 文字までに制限されています。
- ダイレクト IP アドレス アクセスはホワイトリストでブロックされています。ただし、ブラックリストではブロックされていません。
- レイヤ 2 ローミングはサポートされていません。
- IPv6 はサポートされていません。
- URL フィルタリング ACL 名を返す RADIUS サーバはサポートされていません。
- 次の状況では ACL はフィルタできない場合があります。
  - URL がフラグメント化されたパケットにまたがっている
  - IP パケットがフラグメント化されている

ドメインベースのフィルタリングの設定（GUI）

アクセス コントロール リストの設定（GUI）

URL ACL リスト内のルールを設定します。

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[URL ACLs]** を選択して、[URL Access Control Lists] ページを開きます。

ステップ 2 URL ACL を選択します。

[URL Access Control Lists] > **[Edit]** ページが表示されます。

ステップ 3 [Add New Rule] を選択します。

ステップ 4 この ACL のルールを次のように設定します。

- [Rule Index]：1 ~ 100 の範囲
- [URL]：URL アドレスを入力します。
- [Action]：[Permit] または [Deny] を選択します。

ステップ 5 [Apply] をクリックします。

さらにルールを追加するにはこの手順を繰り返します。

（注） デフォルト ポート 80 の代わりに異なるポート番号を使用する Web サイトにシームレスにアクセスできるようにするには、「URL 名:ポート番号」の形式で、ポート番号を含むルールを作成します。例：URL に website.com:8080 と入力し、permit アクションを適用します。

URL ACL リストの作成（GUI）

WLAN でアクセス コントロール リストを作成または削除するには、次の手順を実行します。

手順

ステップ 1 **[Security]** > **[Access Control Lists]** > **[URL ACLs]** を選択し、[URL Access Control Lists] ページを開きます。

ステップ 2 [Enable URL Acl] チェックボックスをオンにし、URL ACL 機能を有効にします。

ステップ 3 [New] をクリックして、新しい ACL を追加します。**[URL Access Control Lists]** > **[New]** ページが表示されます。
[URL ACL Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。

- さらに URL ACL を追加するにはこの手順を繰り返します。
- URL ACL を削除するには、[URL Access Control Lists] ページで、その ACL の青いドロップダウン矢印にマウス カーソルを合わせ、[Remove] を選択します。

（注） ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

URL フィルタリング アクセス コントロール リストのグローバルな適用（GUI）

ネットワーク全体に URL ACL を適用します。

手順

ステップ 1 **[Security]** > **[Local Policies]** を選択して、ローカル ポリシー ページを開きます。

ステップ 2 目的のポリシーを選択します。

[Policy] > **[Edit]** ページが表示されます。

ステップ 3 [Match Role String] をテキスト ボックスに入力します。

ステップ 4 [URL ACL] ドロップダウン リストから URL ACL を選択します。

ステップ 5 [Apply] をクリックします。

（注） [Match Role String] の名前は、Cisco AV ペアのロール名と一致している必要があります。

URL フィルタリング アクセス コントロール リストのインターフェイスへの適用（GUI）

ネットワーク内のインターフェイスに URL ACL を適用します。

手順

ステップ 1 Choose **Controller** > **Interfaces** to open the interface page.

ステップ 2 Choose the desired interface.

The interface page for the selected interface appears.

ステップ 3 Select the URL ACL from the **URL ACL** drop-down list.

ステップ 4 Click **Apply**.

WLAN に対する URL フィルタリング アクセス コントロール リストの適用（GUI）

ネットワーク内の WLAN に URL ACL を適用します。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [URL ACL] ドロップダウン リストから、この WLAN に適用する ACL を選択します。

ステップ 5 [Apply] をクリックします。

WLAN へのポリシーのマッピング（GUI）

ネットワーク内の WLAN にポリシーをマッピングします。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 [Policy-Mapping] タブを選択します。

1. [Priority Index] の値を入力します。
2. [Local Policy] ドロップダウン リストからローカル ポリシーを選択します。
3. [Add] をクリックします。

ステップ 4 [Apply] をクリックします。

WLAN のポリシー マッピングの削除（GUI）

この手順は、WLAN のポリシー マッピングを削除するのに役立ちます。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 そのローカル ポリシーの青いドロップダウン矢印にマウス カーソルを合わせます

ステップ 4 [Remove] を選択します。

確認用のダイアログボックスが表示されます。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックします。

AP グループへのポリシーのマッピング（GUI）

ネットワークの AP グループにポリシーをマッピングします。

手順

ステップ 1 [WLANs] を選択して、[WLAN] ページを開きます。

ステップ 2 **[Advanced]** > **[AP Groups]** を選択します。

ステップ 3 [AP Group] を選択します。

[AP Groups] > **[Edit]** ページが表示されます。

ステップ 4 [WLANs] タブを選択します。

ステップ 5 必要な WLAN の青いドロップダウン矢印にマウス カーソルを合わせ、[Policy-Mapping] を選択します。

ステップ 6 **[AP Group]** > **[Policy]** > **[Mappings]** ページで、

1. [Priority Index] の値を入力します。
2. [Local Policy] ドロップダウン リストからローカル ポリシーを選択します。
3. [Add] をクリックします。

ステップ 7 [Apply] をクリックします。

WLAN と AP グループは、ローカル ロールに基づくポリシーです。

DNS フィルタリングの設定（CLI）

URL フィルタリングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、URL ベースのフィルタリング機能を設定します。

config acl url-acl {**enabled** | **disable**}

ステップ 2 次のコマンドを入力して、URL ACL を作成または削除します。
config acl url-acl{ **create | delete**} *id-token*

ステップ 3 次のコマンドを入力して、URL ACL をデータ パスに適用します。
config acl url-acl apply*acl-name*

ステップ 4 次のコマンドを入力して、ACL をインターフェイスに設定します。
config interface url-acl *interface-name acl-name*

ステップ 5 次のコマンドを入力して、ACL を WLAN に設定します。
config wlan url-acl *wlan-id acl-name*

アクセス コントロール リスト ルールの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、ACL を作成または削除します。
config acl url-acl rule{ **add | delete**} *acl-name index*

ステップ 2 次のコマンドを入力して、有効な形式（例：www.cisco.com）の URL アドレスを設定します。
config acl url-acl rule url*acl-name index url-name*

ステップ 3 次のコマンドを入力して、ルールのアクションを設定します。
config acl url-acl rule action *acl-name index*{ **permit | deny**}

（注） デフォルト ポート 80 の代わりに異なるポート番号を使用する Web サイトにシームレスにアクセスできるようにするには、「URL 名:ポート番号」の形式で、ポート番号を含むルールを作成します。例：URL に website.com:8080 と入力し、permit アクションを適用します。

ステップ 4 次のコマンドを入力して、ホワイトリストまたはブラックリストの ACL を設定します。
config acl url-acl list-type *acl-name* {*whitelist* | *blacklist*

blacklist/whitelist

ステップ 5 次のコマンドを入力して、Web ページ要求をリダイレクトする外部サーバを設定します。
config acl url-acl external-server-ip *ip-address*

関連トピック

FlexConnect アクセス コントロール リストの設定（CLI）

ローカル ポリシーの適用（CLI）

手順

ステップ 1 次のコマンドを入力して、ローカル プロファイリング ポリシーを作成または削除します。
config policy *policy-name*{**create | delete**}

ステップ 2 次のコマンドを入力して、ポリシーに一致タイプを設定します。
config policy *policy-name* **match role** {**role-name| none**}

ステップ 3 次のコマンドを入力して、ポリシーにアクションを設定します。
config policy *policy-name* **action url-acl** {**enable | disable**} *acl-name*

ステップ 4 次のコマンドを入力して、WLAN にローカル ポリシーを有効化します。
config wlan policy add *priority-index policy-name wlan-id*

ステップ 5 次のコマンドを入力して、WLAN の AP グループにローカル ポリシーを追加または削除します。
config wlan apgroup policy {**add | delete**} *priority-index policy-name ap-group-name wlan-id*

URL フィルタリングの表示（CLI）

手順

- 次のコマンドを入力して、ACL の概要を表示します。
  show acl url-acl summary
- 次のコマンドを入力して、詳細な URL ACL プロファイル情報を表示します。
  show acl url-acl detailed *acl-name*
- 次のコマンドを入力して、ポリシーの詳細を表示します。
  show policy {**summary**| *policy-name*}
- 次のコマンドを入力して、MAC アドレスごとのクライアントの詳細を表示します。
  show client detail *mac-address*
- 次のコマンドを入力して、WLAN の設定の詳細を表示します。
  show wlan*wlan-id*
- 次のコマンドを入力して、インターフェイスの詳細を表示します。
  show interface detailed *interface-name*
- 次のコマンドを入力して、カウンタをクリアします。
  clear url-acl-counters

URL フィルタリングのトラブルシューティング（CLI）

次のコマンドを入力して、URL フィルタリング機能をトラブルシューティングできます。

手順

- **debug fastpath dump urlacldb** *aclid ruleindex dataplane*
- **debug fastpath dump stats** *dataplane*

  指定可能なデータプレーン オプションは、0、1、All です。

- **debug fastpath dump scbdb**