FlexConnect のセキュリティ

FlexConnect ACL

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）。ACL を使用すると、ネットワーク トラフィックのアクセス制御を行えます。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 WLAN に適用できます。ACL を使用すると、ワイヤレス クライアントと送受信されるデータ トラフィックやコントローラの CPU へのデータ トラフィックを制御できます。FlexConnect アクセス ポイント上で ACL を設定して、ローカルにスイッチされるアクセス ポイント上のデータ トラフィックの効率的な使用およびアクセス制御を実現できます。

FlexConnect ACL は、入力と出力の両方のモードのアクセス ポイントで VLAN インターフェイスに適用できます。

アクセス ポイントの既存のインターフェイスを ACL にマッピングできます。インターフェイスは、FlexConnect アクセス ポイントで WLAN-VLAN マッピングを設定することによって作成できます。

FlexConnect ACL は、VLAN サポートが FlexConnect アクセス ポイントで有効になっている場合のみ、アクセス ポイントの VLAN に適用できます。

関連情報

- ロケーション認証を設定するには、エンタープライズ モビリティの設計ガイド [英語] の「*FlexConnect*」の章を参照してください。
- FlexConnect 向けワイヤレス BYOD 導入ガイド

FlexConnect アクセス コントロール リストの制約事項

- FlexConnect ACL は FlexConnect のアクセス ポイントにのみ適用できます。設定は、AP および VLAN ごとに適用されます。
- FlexConnect ACL はネイティブ VLAN でサポートされます。

（注） FlexConnect グループから設定されている場合、FlexConnect ACL はネイティブ VLAN ではサポートされません。

- シスコ ワイヤレス コントローラには最大 512 の ACL を設定できます。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。パケットがルールに関連するすべてのパラメータに一致すると、そのルールに関連するアクション設定がパケットに適用されます。
  - 各 ACL には 64 の IPv4 アドレス ベースのルールを定義できます。
- コントローラに設定されている非 FlexConnect ACL は FlexConnect AP には適用できません。
- FlexConnect ACL では、ルールごとの方向はサポートされていません。通常の ACL とは異なり、Flexconnect ACL では方向を持たせて設定することはできません。ACL 全体を入力または出力としてインターフェイスに適用する必要があります。
- ネットワークの ACL は、Control and Provisioning of Wireless Access Points（CAPWAP）が Lightweight Access Point Protocol （LWAPP）で使用されているものとは異なるポートを使用するため、変更を必要とする場合があります。
- 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、対応するアクセス ポイントによってドロップされます。
- WLAN-VLAN マッピングを使用して AP で作成された VLAN の ACL マッピングは、AP ベースごとでのみ実行する必要があります。VLAN は AAA Override の FlexConnect グループで作成できます。これらの VLAN に WLAN のマッピングはありません。
- FlexConnect グループで作成された VLAN の ACL は、FlexConnect グループのみでマッピングする必要があります。同じ VLAN が、対応する AP および FlexConnect グループにある場合、AP VLAN が優先されます。つまり、ACL が AP にマッピングされていない場合、FlexConnect グループの VLAN にマッピングされていても VLAN には ACL がないということです。
- FlexConnect ローカル スイッチングに WLAN を設定する際、FlexConnect ACL と標準 ACL 名が同じでないことを確認します。
- AAA クライアントの ACL のサポート

- AAA がクライアント ACL を送信する前に、ACL が FlexConnect グループまたは AP で作成されることを確認してください。ACL は、クライアントが AP に関連付けられるときに AP に動的にダウンロードされることはありません。
- 最大 96 の ACL を AP で設定できます。各 ACL には最大 64 のルールを設定できます。
- FlexConnect ACL には方向がありません。ACL 全体が入力または出力として適用されます。
- AAA によって返される ACL は、クライアントの 802.11 側の入力と出力の両方に適用されます。

- Cisco Aironet 2800 シリーズ AP：FlexConnect ACL が有線インターフェイスと 802.11 インターフェイスの両方に適用されている場合、クライアント トラフィックは 802.11 インターフェイスにマッピングされている ACL のみ受け入れ、有線インターフェイスにマッピングされている ACL は受け入れません。

（注） ローカル スイッチング WLAN が設定され、ACL は、ACL を使用して FlexConnect グループにマッピングされます。ACL には、「deny および permit」ルールのセットが定義されています。あるクライアントを WLAN に関連付ける場合、そのクライアントは、IP アドレスを取得するために追加される DHCP の permit ルールが必要になります。

FlexConnect 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]** > **[FlexConnect Access Control Lists]** の順に選択します。

[FlexConnect ACL] ページが表示されます。

このページには、コントローラ上で設定したすべての FlexConnect ACL が一覧表示されます。このページには、対応するコントローラで作成した FlexConnect ACL も表示されます。ACL を削除するには、該当する ACL 名の横にある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 2 [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 3 [Access Control List Name] フィールドに新しい 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。

ステップ 5 [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。

[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 6 次の手順に従い、特定の FlexConnect ACL の IP アドレス ベースのルールを設定します。

a) [IP Rule] を選択して、IP アドレス ベースのルールを作成します。

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

b) コントローラは IP アドレスベースの ACL ごとに最大 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] フィールドで、値（1 ～ 64）を入力し、この ACL に定義されているその他のルールとの関連で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、そのルールはルール 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自動的に調整されます。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。

c) [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、該当するフィールドに送信元の IP アドレスとネットマスクを入力します。

d) [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、該当するフィールドに IP アドレスと宛先の詳細を入力します。

e) [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。使用できるプロトコル 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**
- **[UDP]**
- ICMP：Internet Control Message Protocol（インターネット制御メッセージ プロトコル）
- [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]：IP-in-IP パケットを許可または拒否します

- [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] フィールド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（アドレス解決プロトコル（ARP）パケットなど）は指定できません。

[TCP] または [UDP] を選択すると、[Source Port] と [Destination Port] の 2 つの追加パラメータが表示されます。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。

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サービスの質を定義するのに使用できる IP ヘッダー フィールドです。

- [Any]：任意の DSCP（これはデフォルト値です）。
- [Specific]：[DSCP] フィールドに入力する特定の DSCP（0 ～ 63）。

g) [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。

h) [Apply] をクリックします。

[Access Control Lists > Edit] ページが表示され、この ACL のルールが示されます。

i) 必要に応じて、この 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。

関連トピック

アクセス コントロール リストの設定

FlexConnect アクセス コントロール リストの設定（CLI）

FlexConnect ACL を設定するには、コントローラで次のコマンドを使用します。

手順

- 次のコマンドを入力して、FlexConnect アクセス ポイントで ACL を作成または削除します。

  config flexconnect acl {**create** | **delete** } *name*

IPv4 ACL 名は最大 32 文字までサポートされています。

- FlexConnect ACL を WLAN に関連付けます。
  a) 次のコマンドを入力して、Web 認証を有効にします。

     config wlan security web-auth enable *wlan_id*

  b) 次のコマンドを入力して、FlexConnect ACL を WLAN に設定します。

     config wlan security web-auth flexacl *wlan_idacl_name*

- ACL の IP アドレス ベースのルールを設定します。
  a) 次のコマンドを入力して、FlexConnect ACL に IP アドレス ベースのルールを追加します。

     config flexconnect acl rule add *acl-name rule-index*

  b) 次のコマンドを入力して、ルールの送信元 IP アドレスとネットマスクを設定します。

     config flexconnect acl rule source address *acl-name rule-index ipv4-addr subnet-mask*

  c) 次のコマンドを入力して、ルールの送信元ポートの範囲を設定します。

     config flexconnect acl rule source port range *acl-name rule-index start-port end-port*

  d) 次のコマンドを入力して、ルールの宛先IPアドレスとネットマスクを設定します。

     IPv4：**config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask*

  e) 次のコマンドを入力して、ルールの宛先ポートの範囲を設定します。

     config flexconnect acl rule destination port range*acl-name rule-index start-port end-port*

  f) 次のコマンドを入力して、ルールの IP プロトコルを設定します。

     config flexconnect acl rule protocol *acl-name rule-index* **protocol**

     インデックス値（0 ～ 64）を指定します。プロトコル値（0 ～ 255 または「any」）を指定します。デフォルトは「any」です。

  g) 次のコマンドを入力して、ルール インデックスの Differentiated Services Code Point（DSCP）値を指定します。

     config flexconnectacl rule dscp *acl-name rule-index dscp-value*

     DSCP は、インターネット上のサービスの質を定義するのに使用できる IP ヘッダーです。0 ～ 63 の値または値 **any** を入力します。デフォルト値は **any** です。

  h) 次のコマンドを入力して、ルールに対する許可または拒否アクションを設定します。

     config flexconnect acl rule actionacl-name *rule-index* **{permit |deny}**

  i) 次のコマンドを入力して、ACL ルールのインデックス値を変更します。

     config flexconnectacl rule change index *acl-name old-index new-index*

j) 次のコマンドを入力して、2 つのルール間でインデックス値を切り替えます。

config flexconnect acl rule swap *acl-name index-1 index-2*

k) 次のコマンドを入力して、FlexConnect AVC のルールを削除します。

config flexconnect acl rule delete *name*

l) 次のコマンドを入力して、FlexConnect アクセス ポイントに ACL を適用します。

config flexconnect acl apply *acl-name*

- （オプション）次のコマンドを入力して、FlexConnect アクセス ポイントで VLAN を追加します。

  config ap flexconnect vlan add *acl vlan-id ingress-aclname egress-acl-name ap-name*

関連トピック

アクセス コントロール リスト ルールの設定（CLI）

FlexConnect アクセス コントロール リストの表示とデバッグ（CLI）

FlexConnect ACL に関する情報を表示するには、コントローラで次のコマンドを使用します。

手順

- **show flexconnect acl summary**：ACL のサマリを表示します。
- **show client detail** *mac-address*：AAA オーバーライド ACL を表示します。
- **show flexconnect acl detailed acl-name**：ACL に関する詳細情報を表示します。
- **debug flexconnect acl {enable | disable}**：FlexConnect ACL のデバッグを有効または無効にします。
- **debug capwap reap**：CAPWAP のデバッグを有効にします。

FlexConnect の AAA オーバーライド

認証、認可、アカウンティング オーバーライドについて

WLAN の [Allow Authentication, Authorization, Accouting (AAA) Override] オプションを使用すれば、WLAN を認証用に設定することができます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、QoS、および ACL を適用できます。

FlexConnect アクセス ポイントに対する AAA Override は、ローカルにスイッチされたクライアントへダイナミック VLAN の割り当てを提供します。また、FlexConnect の AAA オーバーライドは、オーバーライドするクライアントの高速ローミング（Opportunistic Key Caching（OKC）/Cisco Centralized Key management（CCKM））もサポートします。

FlexConnect の VLAN オーバーライドは、中央で認証されたクライアントとローカルで認証されたクライアントの両方に適用されます。VLAN は、FlexConnect グループで設定することができます。

AP の VLAN が WLAN-VLAN を使用して設定されている場合、対応する ACL の AP 設定が適用されます。VLAN が FlexConnect グループを使用して設定されている場合は、FlexConnect グループ上で設定された対応する ACL が適用されます。同じ VLAN が FlexConnect グループと AP の両方で設定されている場合は、ACL を使用した AP 設定が優先されます。WLAN-VLAN マッピングからの新しいVLAN用のスロットが存在しない場合は、最後に設定されたFlexConnect グループ VLAN が置き換えられます。

AAA から戻された VLAN が AP 上に存在しない場合、クライアントは WLAN に設定されたデフォルト VLAN にフォールバックされます。

AAA オーバーライドを設定する前に、アクセス ポイント上で VLAN が作成されている必要があります。これらの VLAN は、アクセス ポイントの既存の WLAN-VLAN マッピングか、VLAN-ACL マッピングで作成できます。

IPv6 ACL の AAA Override

Cisco Identity Services Engine（ISE）、ACS などの一元化された AAA サーバによるアクセス コントロールのサポートのために、AAA Override 属性を使用して各クライアントについて IPv6 ACL をプロビジョニングできます。この機能を使用するには、IPv6 ACL をコントローラで設定し、AAA Override 機能をイネーブルにして WLAN を設定する必要があります。IPv6 ACL の AAA 属性は IPv4 ベースの ACL をプロビジョニングするために使用される *Airespace-ACL-Name* 属性に似た *Airespace-IPv6-ACL-Name* です。AAA 属性が返すコンテンツは、コントローラ上で設定された IPv6 ACL の名前と一致する文字列にする必要があります。

AP とコントローラの双方向レート制限の AAA オーバーライド

FlexConnect AP の AAA オーバーライドで、QoS レベルまたは帯域幅コントラクトを、Web 認証済み WLAN と 802.1X 認証済み WLAN の両方でローカルにスイッチされるトラフィックに動的に割り当てることができます。アップストリームとダウンストリームの両方のパラメータが、対応する AP に送信されます。

表 *1:* 双方向レート制限の実装

アップストリーム/ダウンストリーム	ローカル モード	FlexConnect 中央スイッチング	FlexConnect ローカル スイッチング	FlexConnect スタンドアロン
クライアント単位ダウンストリーム	AP	AP	AP	AP
クライアント単位アップストリーム	AP	AP	AP	AP

表 *2:* レート制限パラメータ

AAA	AAA の QoS プロファイル	WLAN	WLAN の QoS プロファイル	クライアントに適用
100 Kbps	200 Kbps	300 Kbps	400 Kbps	100 Kbps
×	—	—	—	200 Kbps
×	×	—	—	300 Kbps
×	×	×	—	400 Kbps
×	×	×	×	Unlimited

FlexConnect の AAA Override に関する制約事項

- AAA Override を設定する前に、VLAN をアクセス ポイントで作成する必要があります。これらの VLAN は、アクセス ポイントの既存の WLAN-VLAN マッピングを使用するか、または FlexConnect グループ VLAN-ACL マッピングを使用して作成できます。
- 常に、AP には最大 16 の VLAN があります。まず、VLAN は AP 設定（WLAN-VLAN）に従って選択され、残りの VLAN は FlexConnect グループで設定または表示されている順序で FlexConnect グループからプッシュされます。VLAN スロットがフルの場合、エラーメッセージが表示されます。
- VLAN、ACL、QoS、レート制限は、ローカルおよび中央のスイッチング WLAN でサポートされます。
- ダイナミック VLAN の割り当ては、Access Control Server（ACS）のコントローラの Web 認証ではサポートされていません。
- AP およびコントローラの双方向レート制限の AAA Override は、次の 802.11n の非メッシュ アクセス ポイントのすべてでサポートされます。
  - 1040
  - 1140
  - 1250
  - 1260
  - 1600
  - 2600
  - 3500
  - 3600

  この機能は、メッシュ およびレガシー の AP プラットフォームでサポートされていません。
  - 1130

- 1240
- 1520
- 1550

- 双方向レート制限の場合
  - 双方向レート制限がない場合、AAA Override は実行されません。
  - 対応する WLAN の QoS プロファイルが Silver であっても、クライアントの QoS プロファイルは Platinum に設定できます。AP では、クライアントが音声キューにパケットを送信できます。ただし、セッション開始プロトコル（SIP）スヌーピングを WLAN 上で無効にして、SIP クライアントのトラフィックが音声キューに送信されないようにする必要があります。
  - ISE サーバがサポートされています。
  - アップストリーム レート制限パラメータは、AAA Override のダウンストリーム パラメータと同様です。
  - ローカル認証はサポートされていません。

アクセスポイント上のFlexConnectに対するAAAOverrideの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[All]** > **[APs]** を選択します。

[All APs] ページが表示されます。このページに、コントローラにアソシエータされているアクセス ポイントが一覧表示されます。

ステップ 2 対応する AP 名をクリックします。

ステップ 3 [FlexConnect] タブをクリックします。

ステップ 4 [Native VLAN ID] の値を入力します。

ステップ 5 [VLAN Mappings] ボタンをクリックして、[AP VLANs] マッピングを設定します。

次のようなパラメータが表示されます。

- [AP Name]：アクセス ポイント名。
- [Base Radio MAC]：AP のベース無線。
- [WLAN-SSID-VLAN ID Mapping]：コントローラで設定された各 WLAN に対して、対応する SSID および VLAN ID が表示されます。WLAN の VLAN ID 列を編集して WLAN-VLAN ID マッピングを変更します。
- [Centrally Switched WLANs]：中央でスイッチされる WLAN が設定されている場合、WLAN–VLAN マッピングが一覧表示されます。
- [AP Level VLAN ACL Mapping]：次のパラメータを使用できます。

- [VLAN ID]：VLAN ID。
- [Ingress ACL]：VLAN に対応する入力 ACL。
- [Egress ACL]：VLAN に対応する出力 ACL。

各 ACL タイプのドロップダウン リストからマッピングを選択して、入力 ACL および出力 ACL マッピングを変更します。

- [Group Level VLAN ACL Mapping]：次のグループ レベルの VLAN ACL マッピング パラメータが使用できます。
  - [VLAN ID]：VLAN ID。
  - [Ingress ACL]：この VLAN に対する入力 ACL。
  - [Egress ACL]：この VLAN に対する出力 ACL。

ステップ 6 [Apply] をクリックします。

アクセス ポイント上の FlexConnect に対する VLAN Override の設定（CLI）

FlexConnect アクセス ポイントの VLAN Override を設定するには、次のコマンドを使用します。

config ap flexconnect vlan add *vlan-id* **acl** *ingress-acl egress-acl ap_name*