ISE 対応の汎用 WLC FlexConnect の設定

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者：Hosuk Won

日付：2012 年 12 月

目次

WLC FlexConnect への ISE の統合

本書は、AP が FlexConnect モードで展開されている CUWN 環境に ISE を統合する際の手順ガイドとして準備されています。FlexConnect モード（旧称 H-REAP モード）を使用すると、AP が特定の WLAN（通常はブランチ オフィスに展開された WLAN）のユーザ トラフィックをローカルで切り替えられるようになります。これにより、ワイヤレス トラフィックをブランチ オフィス内にとどめておくことができます。

設計の概要：

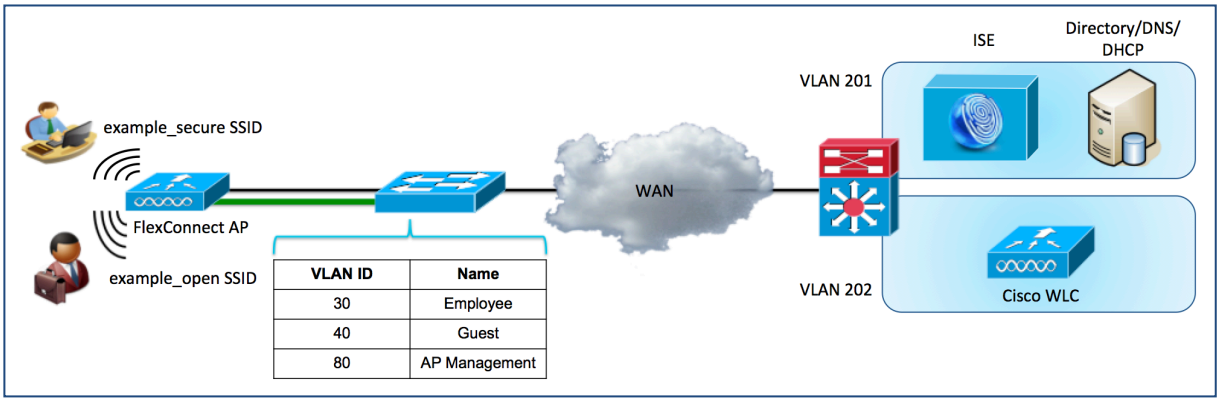

図 1. WLC FlexConnect との ISE の統合

上記の図に、コンポーネントの全体的なレイアウトが示されています。セントラル サイトには、次の 2 つの VLAN が定義されます。

表 1.

VLAN ID（Admin. VLAN ID）	名前	使用方法
201	Server	ISE、AD、DNS、DHCP
202	WLC	WLC 管理

リモート オフィスには、次の 3 つの VLAN が定義されます。

表 2.

VLAN ID（Admin. VLAN ID）	名前	使用方法
80	AP Management	FlexConnect AP ネイティブ VLAN
30	Employee	マッピングされたセキュア WLAN
40	Guest	マッピングされたオープン WLAN

この設計では、エンドポイントが FlexConnect 対応 WLAN に関連付けられるときに、そのエンドポイントは LAP からコントローラへの CAPWAP トンネルを介して認証を行います。ただし、一度認証されると、LAP からローカル LAN へのトラフィックの切り替えは、中央のワイヤレス コントローラを介してではなくローカルで行われます。設定されている WLAN は 2 つあります。1 つは、MAC フィルタリングを行うオープン SSID、もう 1 つは WPA2/802.1X 対応の WLAN です。example_open SSID に関連付けられたエンドポイントは、FlexConnect AP にローカルに定義された VLAN 40 に切り替えられます。一方、example_secure SSID に関連付けられたエンドポイントは VLAN 30 に切り替えられます。example_open SSID に関連付けられるエンドポイントは、WLC に定義された FlexConnect ACL を使用したインターネット アクセスだけに制限され、FlexConnect AP で公開されます。この ACL は、認証の際に、AireSpace RADIUS 属性を使用した ISE からのセッションに適用されます。

FlexConnect モードでは、ローカル認証などの追加設定がサポートされますが、これらのオプションは ISE 統合の項目では説明されません。また、本書は、FlexConnect モードとの ISE 統合に必要な設定について詳しく説明しますが、本書では取り上げない、プロファイリングやゲスト アクセスの詳細などの設定もあります。これらの設定について詳しくは、該当するハウツー ガイドを参照してください。

使用されるコンポーネント

- Cisco ISE 1.2.0.899
- Cisco 2504 CUWN AireOS 7.5.102.0
- Cisco LWAP 3602（RADIUS を使用する FlexConnect ACL は、レガシーおよびメッシュ AP モデルの 1130、1240、1520、1550 ではサポートされません）。FlexConnect モードおよび AAA オーバーライド機能について詳しくは、WLC ガイド（http://www.cisco.com/en/US/docs/wireless/controller/7.5/config_guide/b_cg75_chapter_010001010.html）を参照してください。
- MS Windows 2008 Server（AD/DNS/DHCP サーバとして使用）

注：ここで説明する、ACL を認証として使用する FlexConnect は、サポートされている AP モデルを使用して AireOS 7.5.102.0 以降を実行する WLC でのみサポートされます。他のバージョンの WLC および AP の場合、トラフィックを制御する代わりに、FlexConnect グループ レベルで静的 VLAN 割り当てを使用できます。FlexConnect VLAN 割り当てを使用する方法については、次の URL にある BYOD 2.5 CVD で説明されています。
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Wireless.html

スイッチの設定

この設計では、ローカル VLAN を異なる WLAN にマッピングしなければならないため、LAP に接続するインターフェイスは、トランク ポートとして設定する必要があります。

```
Remote-Switch(config)#interface GigabitEthernet x/y/z
Remote-Switch(config-if)#description AP
Remote-Switch(config-if)#switchport mode trunk
Remote-Switch(config-if)#switchport trunk native vlan 80
Remote-Switch(config-if)#no shut
```

WLC に接続するインターフェイスは、トランク インターフェイスまたはアクセス インターフェイスのいずれかにすることができます。ローカル モードで展開された AP と同じく、WLC が中央でユーザ トラフィックを切り替える場合は、トランクが必要です。本書では FlexConnect モードの AP を中心に扱うため、ここではインターフェイスをアクセス ポートとして設定します。

```
DC-Switch(config)#interface GigabitEthernet x/y/z
DC-Switch(config-if)#description WLC
DC-Switch(config-if)#switchport mode access
DC-Switch(config-if)#switchport access vlan 202
DC-Switch(config-if)#no shut
```

WLC の設定手順

初期 WLC 設定

次の手順に従って、シスコ ワイヤレス LAN コントローラの初期設定を行います。

ステップ 1 WLC のコンソール ポートに接続します。次の設定を参照して WLC のブートストラップを行います。

出力例

```
 (Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:yes
AUTO-INSTALL: process terminated -- no configuration loaded

System Name [Cisco_91:e2:64] (31 characters max): 2500wlc-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): ********
Re-enter Administrative Password                : ********

Service Interface IP Address Configuration [static][DHCP]:dhcp

Enable Link Aggregation (LAG) [yes][NO]: no

Management Interface IP Address: 192.168.202.61
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.202.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 192.168.201.72

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: example
Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:us

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 192.168.201.72
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

RADIUS サーバとしての ISE の設定

Cisco WLC は、Cisco ISE を RADIUS サーバとして使用します。次の手順に従って、Cisco ISE を RADIUS サーバとして使用するように、Cisco WLC を設定します。

ステップ 1 WLC GUI にアクセスし、[セキュリティ(Security)] → [RADIUS] → [認証(Authentication)] に移動します。

ステップ 2 右上隅にある [新規...(New…)] をクリックして、新しい RADIUS 認証サーバを追加します。

次の表に、RADIUS 認証サーバの設定を記載します(表に指定されていない場合は、デフォルト値を使用してください)。

表 3.

属性(Attribute)	値(Value)
サーバ インデックス(Server Index)(優先順位)	1
サーバの IP アドレス	192.168.201.88
共有秘密鍵形式(Shared Secret Format)	ASCII
共有秘密鍵(Shared Secret)	cisco123
ポート番号(Port Number)	1812
サーバ ステータス(Server Status)	有効(Enabled)(オン)
RFC 3576 のサポート(Support for RFC 3576)	有効(Enabled)(オン)
サーバ タイムアウト(Server timeout)	10 秒
ネットワーク ユーザ(Network User)	有効(Enabled)(オン)

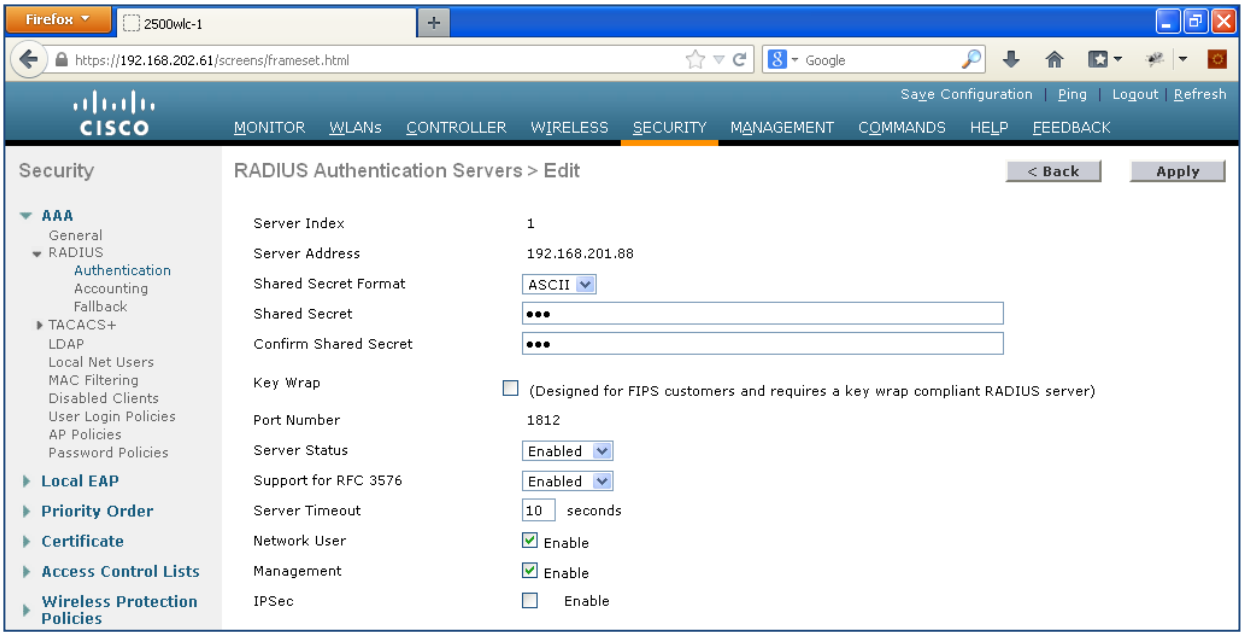

図 2.

ステップ 3 [適用（Apply）]、[設定の保存（Save Configuration）] の順にクリックします。

ステップ 4 [アカウンティング（Accounting）]、[新規...（New...）] の順にクリックし、RADIUS アカウンティング サーバを追加します。

次の表に、RADIUS アカウンティング サーバの設定を記載します（表に指定されていない場合は、デフォルト値を使用してください）。

表 4.

属性（Attribute）	値（Value）
サーバ インデックス（Server Index）（優先順位）	1
サーバの IP アドレス	192.168.201.88
共有秘密鍵形式（Shared Secret Format）	ASCII
共有秘密鍵（Shared Secret）	cisco123
ポート番号（Port Number）	1813
サーバ ステータス（Server Status）	有効（Enabled）（オン）
サーバ タイムアウト（Server timeout）	10 秒
ネットワーク ユーザ（Network User）	有効（Enabled）（オン）

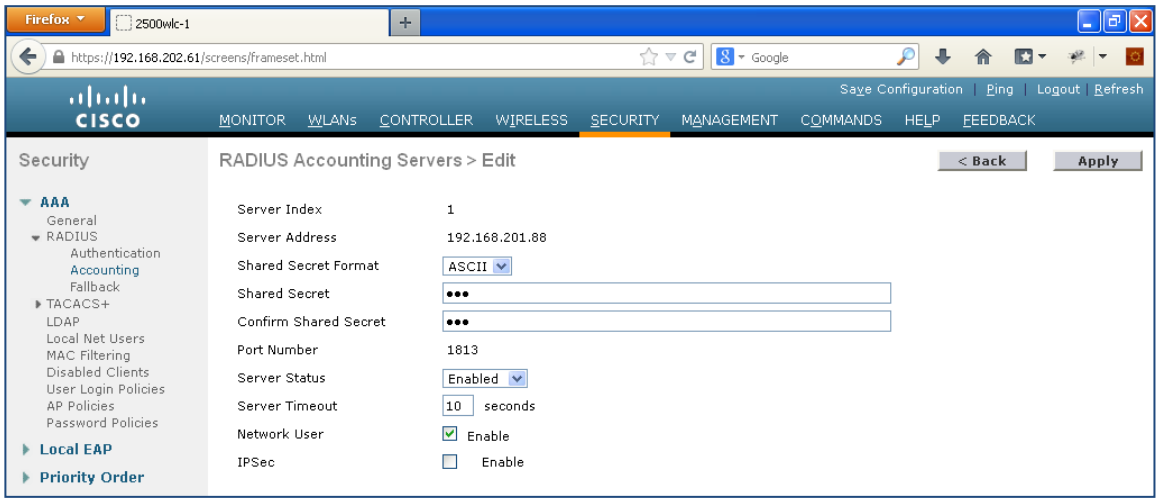

図 3.

ステップ 5 [適用(Apply)]、[設定の保存(Save Configuration)] の順にクリックします。

RADIUS フォールバック オプションの設定

プライマリ RADIUS サーバ(最も小さいサーバ インデックスを持つサーバ)は、Cisco WLC の最優先サーバであると見なされます。プライマリ サーバが応答しなくなると、コントローラは次にアクティブなバックアップ サーバ(2 番目に小さいサーバ インデックスを持つサーバ)に切り替えます。コントローラは、プライマリ RADIUS サーバが回復して応答可能になるとそのサーバにフォールバックするように設定されているか、使用可能なバックアップ サーバの中からより優先されるサーバにフォールバックするように設定されていない限り、このバックアップ サーバを引き続き使用します。

ステップ 1 [セキュリティ(Security)] → [AAA] → [RADIUS] → [フォールバック(Fallback)] に移動します。
ステップ 2 [フォールバックモード(Fallback Mode)] を [アクティブ(Active)] に設定します。

注: [アクティブ(Active)] を選択すると、Cisco WLC は、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断します。コントローラは、すべてのアクティブな RADIUS 要求に対して、すべての非アクティブ サーバを無視します。[パッシブ(Passive)] を選択すると、Cisco WLC は、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行します。コントローラは、しばらくの間すべての非アクティブ サーバを無視し、あとで RADIUS メッセージの送信が必要になったときに再試行します。

ステップ 3 [ユーザ名(Username)] に、「radius-test」と入力します。この名前が、非アクティブ サーバ プローブで送信されます。
ステップ 4 [間隔(秒)(Interval in Sec.)] フィールドに値を再入力します。

この間隔は、パッシブ モードでの非アクティブ時間、およびアクティブ モードでのプローブ間隔としての意味を持ちます。有効な値の範囲は 180 ～ 3600 秒で、デフォルト値は 300 秒です。

AP から FlexConnect AP への変更

CUWN を使用する場合、LAP を展開できるさまざまなモードがあります。典型的な集中型ワイヤレス展開では、LAP をローカル モードで展開します。この場合、すべてのトラフィックが LAP から CAPWAP トンネルを介して WLC に送信され、WLC によって、WLAN と一致する VLAN に切り替えられます。トラフィックを LAP でローカルに切り替えるには、AP モードを FlexConnect モードに変更する必要があります。

ステップ 1 [ワイヤレス(Wireless)] に移動して、FlexConnect モードの AP に変換する AP をクリックします。

ステップ 2 [AP モード(AP Mode)] プルダウン メニューから [FlexConnect] を選択し、[適用(Apply)] をクリックします。この操作により、AP がリロードされ、FlexConnect モードの AP として再び加わります。

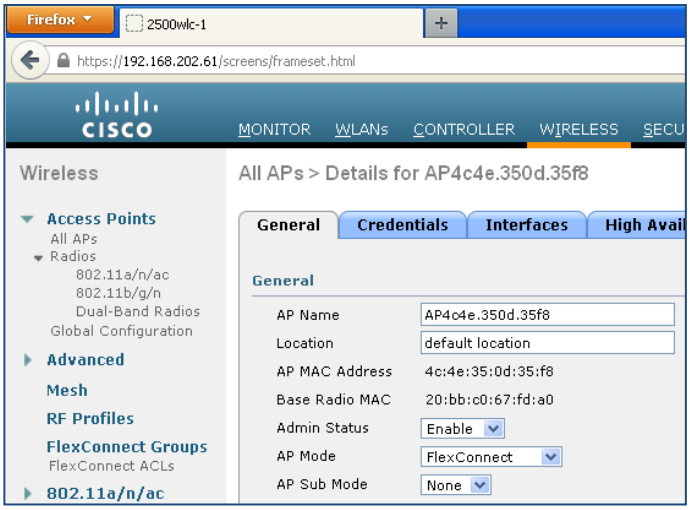

図 4. FlexConnect AP

ステップ 3 AP が WLC に再参加したら、AP をクリックして [FlexConnect] タブをクリックし、トランキングを設定します。

ステップ 4 [VLAN サポート(VLAN Support)] をオンにし、LAP の接続先スイッチに設定されているネイティブ VLAN を入力します。スパニング ツリーがあるため、AP が WLC に再接続するまでに数秒かかる場合があります。

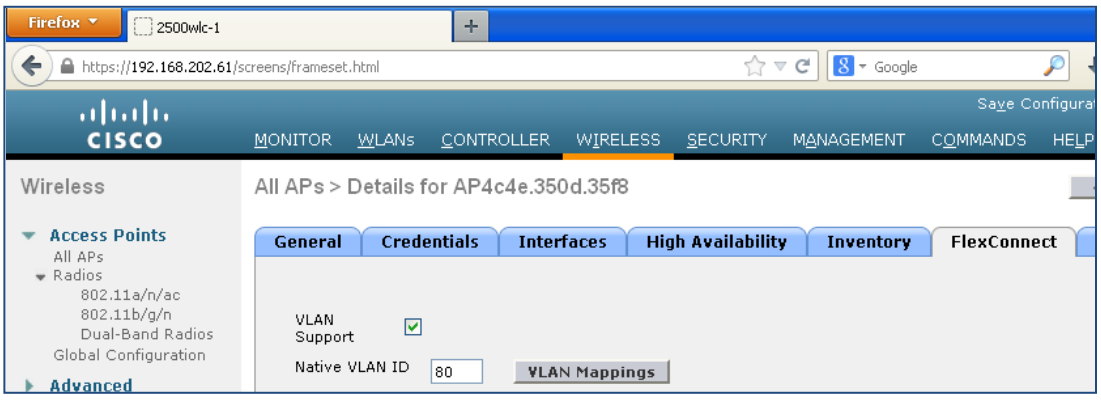

図 5. AP

注: VLAN マッピングを設定して、AP レベルで VLAN と WLAN をマッピングすることもできますが、複数の AP での一般設定を簡素化するために、ここでは FlexConnect グループを設定します。

ステップ 5 **[適用(Apply)]** をクリックします。

セキュア WLAN の作成

セキュア WLAN は、802.1X と WPA2/AES を使用して設定し、従業員に内部リソースへのアクセスを許可するために使用します。BYOD で単一の SSID 展開を使用する場合、これが作成する必要のある唯一の SSID となります。

ステップ 1 [WLAN] に移動します。
ステップ 2 [新規追加(Add New)] をクリックし、次のパラメータを指定して WLAN を作成します。

表 5.

属性(Attribute)	値(Value)
WLAN ID	1
プロファイル名(Profile Name)/SSID	Example_secure
レイヤ 2 セキュリティ	WPA+WPA2、AES、802.1X
AAA サーバ(AAA Servers)	[認証(Authentication)] と [アカウンティング(Accounting)] を [有効(Enabled)]
RADIUS サーバ アカウンティング(RADIUS Server Accounting)	[有効(Enabled)]、900
AAA オーバーライドを許可(Allow AAA Override)	[有効(Enabled)]
セッションタイムアウトを有効化(Enable Session Timeout)	[有効(Enabled)]、7200
クライアントユーザアイドルタイムアウト(Client user idle timeout)	[有効(Enabled)]、7200
FlexConnect ローカル スイッチング(FlexConnect Local Switching)	[有効(Enabled)]
NAC 状態(NAC State)	[RADIUS NAC]

注: 複数の RADIUS サーバがグローバルに定義されている場合は、RADIUS サーバのリストから、この WLAN に使用する ISE ノードを選択してください。

オープン WLAN の作成

オープン WLAN は、オープン SSID を使用して、MAC フィルタリングによってゲスト アクセスを許可するように設定します。デュアル SSID 展開では、この WLAN を BYOD に使用します。

ステップ 1 [WLAN] に移動します。
ステップ 2 [新規追加（Add New）] をクリックし、次のパラメータを指定して WLAN を作成します。

表 6.

属性（Attribute）	値（Value）
WLAN ID	2
プロファイル名（Profile Name）/SSID	Example_open
レイヤ 2 セキュリティ（Layer 2 Security）	[なし（None）]、[MAC フィルタリング（MAC Filtering）]
AAA サーバ（AAA Servers）	[認証（Authentication）] と [アカウンティング（Accounting）] を [有効（Enabled）]
RADIUS サーバ アカウンティング（RADIUS Server Accounting）	[有効（Enabled）]、900
AAA オーバーライドを許可（Allow AAA Override）	[有効（Enabled）]
カバレッジ ホールの検出（Coverage Hole Detection）	無効
セッションタイムアウトを有効化（Enable Session Timeout）	[有効（Enabled）]、7200
クライアントユーザアイドルタイムアウト（Client user idle timeout）	[有効（Enabled）]、7200
FlexConnect ローカル スイッチング（FlexConnect Local Switching）	[有効（Enabled）]
DHCP アドレス 割り当て（DHCP Addr. Assignment）	[必須（Required）]
NAC 状態（NAC State）	[RADIUS NAC]

注: 複数の RADIUS サーバがグローバルに定義されている場合は、RADIUS サーバのリストから、この WLAN に使用する ISE ノードを選択してください。

FlexConnect ACL の作成

2 つの FlexConnect ACL を作成します。1 つは、ゲスト CWA および BYOD プロセスでトラフィックをリダイレクトするために使用します。もう 1 つは、ゲスト ユーザをインターネット専用アクセスに制限するために使用します。最初に、インターネット専用 ACL を作成します。

ステップ 1 [セキュリティ(Security)] → [アクセスコントロールリスト(Access Control Lists)] → [FlexConnect ACLs] に移動します。

ステップ 2 [新規(New)] をクリックし、次のパラメータを指定して「INTERNET-ONLY」ACL を作成します。

表 7.

操作	送信元 IP/マスク	宛先 IP/マスク	プロトコル	送信元ポート	宛先ポート
許可(Permit)	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	任意(Any)	DNS
拒否(Deny)	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	任意(Any)	任意(Any)	任意(Any)
拒否(Deny)	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	任意(Any)	任意(Any)	任意(Any)
拒否(Deny)	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	任意(Any)	任意(Any)	任意(Any)
許可(Permit)	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	任意(Any)	任意(Any)	任意(Any)

ステップ 3 [戻る(Back)] をクリックし、次のパラメータを指定して「REDIRECT-ACL」ACL を作成します。

表 8.

操作	送信元 IP/マスク	宛先 IP/マスク	プロトコル	送信元ポート	宛先ポート
許可（Permit）	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	任意（Any）	DNS
許可（Permit）	192.168.201.88 / 255.255.255.255	0.0.0.0 / 0.0.0.0	任意（Any）	任意（Any）	任意（Any）
許可（Permit）	0.0.0.0 / 0.0.0.0	192.168.201.88 / 255.255.255.255	任意（Any）	任意（Any）	任意（Any）

ステップ 4 [セキュリティ（Security）] → [アクセスコントロールリスト（Access Control Lists）] → [アクセスコントロールリスト（Access Control Lists）] に移動します。

ステップ 5 [新規（New）] をクリックし、「REDIRECT-ACL」ACL を作成します（設定する必要があるのは、ACL 名のみです）。

注：FlexConnect ACL はリダイレクトに使用しますが、コントローラ上に通常の ACL と一致する ACL がないと、コントローラはリダイレクト ACL をセッションに適用できません。そのような事態に対処するために、コントローラ上に、FlexConnect ACL と同じ名前を持つダミー ACL を作成します。コントローラがローカル モードと FlexConnect LAP の両方に使用されている場合、コントローラのリダイレクト ACL がすでに存在する可能性があります。存在する場合は、FlexConnect ACL 名が既存のコントローラ リダイレクト ACL と一致することを確認するだけで十分です。

FlexConnect グループの作成

FlexConnect グループを設定すると、同様の設定（ACL、VLAN マッピングなど）を共有する複数の FlexConnect LAP を効率的に管理できます。これらの設定は、AP ごとに設定できますが、FlexConnect グループを使用することにより、複数の AP を使用した展開の管理がさらに容易になります。ここでは、リモート オフィスにあるすべての FlexConnect AP に適用されるグループを作成します。

ステップ 1 [ワイヤレス（Wireless）] → [FlexConnect グループ（FlexConnect Groups）] を選択します。

ステップ 2 [新規（New）] をクリックし、「flex1」という名前のグループを作成します。

ステップ 3 グループ名をクリックします。

ステップ 4 [AP の追加（Add AP）] ボタンをクリックして、前に変換した AP をこの FlexConnect グループに追加します。

ステップ 5 [現在のコントローラから AP を選択（Select APs from current controller）] をオンにして、プルダウン メニューから該当する AP を選択します。

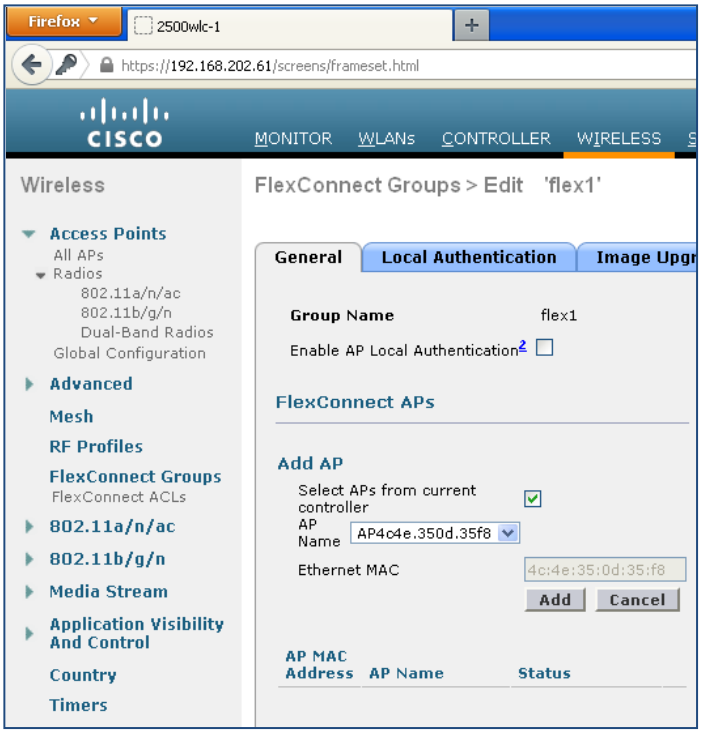

図 6. FlexConnect グループ

ステップ 6 [ACL マッピング（ACL Mapping）] タブをクリックします。
ステップ 7 [ポリシー（Policies）] サブタブをクリックします。
ステップ 8 これまでの手順で作成した 2 つの **FlexConnect ACL** を両方とも追加します。

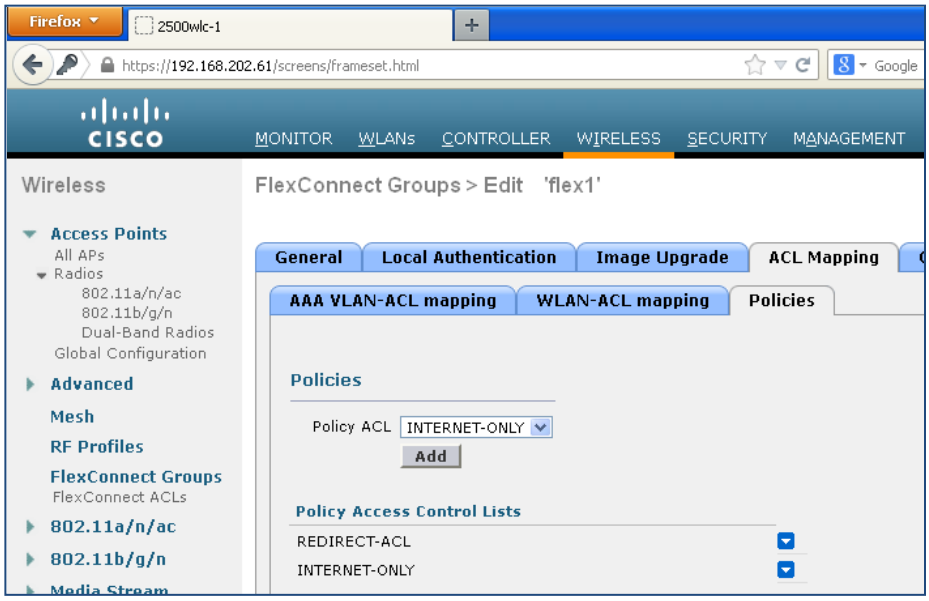

図 7. FlexConnect ACL

ステップ 9 [**WLAN VLAN** マッピング（**WLAN VLAN Mapping**）] タブをクリックします。
ステップ 10 次のパラメータを設定して **WLAN VLAN** マッピングを追加します。

表 9.

WLAN ID	VLAN ID（Admin. VLAN ID）
1	30
2	40

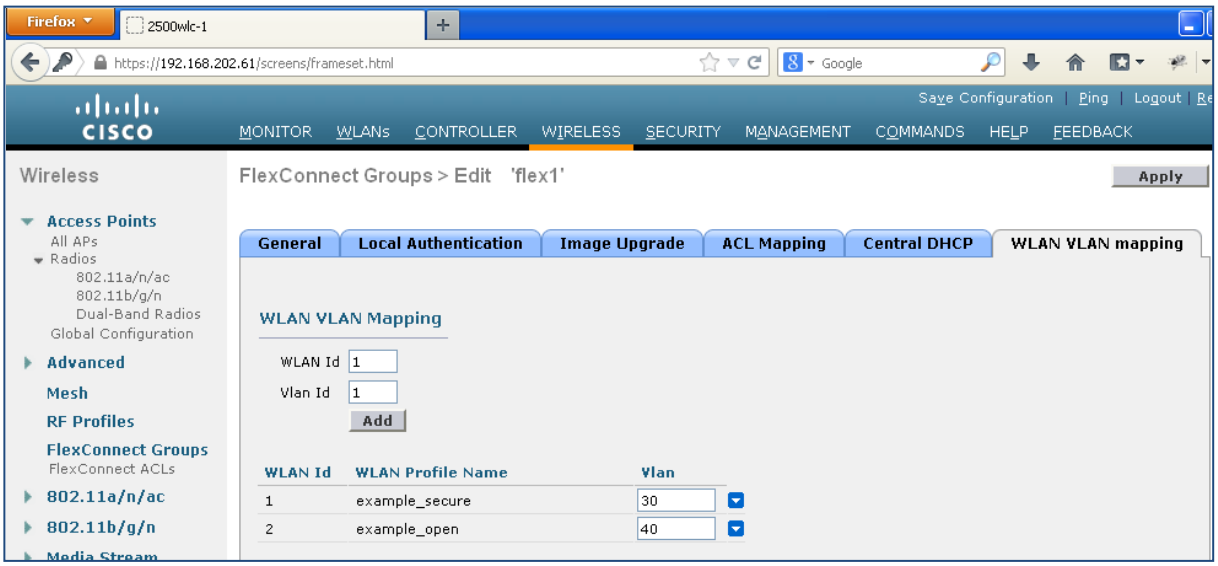

図 8.

ステップ 11 [適用（Apply）] をクリックします。

その他の WLC 機能の設定

ステップ 1 高速 SSID 変更機能を有効にするために、[コントローラ（Controller）] → [一般（General）] に移動します。
ステップ 2 [高速 SSID 変更（Fast SSID Change）] を有効にします。

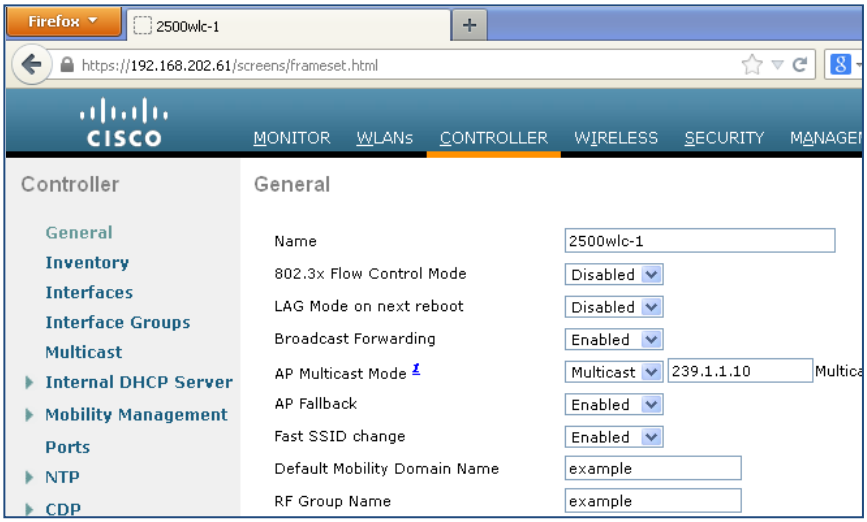

図 9.

注:高速 SSID 変更機能により、クライアントはある SSID から別の SSID に遅延なしで移動できます。BYOD のデュアル SSID のシナリオでは、この機能を使用することで、クライアントがオープン SSID からセキュア SSID に移動できるようになります。これは主に、短時間で SSID 間を移動する Apple iOS デバイスに対応するための機能です。

ステップ 3 キャプティブ ポータル バイパス機能を有効にするために、WLC CLI に移動します。

ステップ 4 キャプティブ バイパス コマンドを有効にします。

```
> config network web-auth captive-bypass enable
```

ステップ 5 設定をコントローラに保存します。

```
> save config
```

ステップ 6 この変更を適用するには、コントローラを再起動する必要があります。

```
> reset system
```

注:Apple は、キャプティブ ポータルがある場合のネットワーク アクセスを容易にする iOS 機能を導入しました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を http://www.apple.com/library/test/success.html に送信することにより、キャプティブ ポータルの存在を検出しようとします。応答が受信されると、インターネット アクセスが使用可能であると見なされます。この場合、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされていると見なされ、CNA が疑似ブラウザを自動起動して、管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。

ISE の設定

ワイヤレス アクセス用の 3850 スイッチを統合するために必要な特定の ISE の設定はありません。Catalyst スイッチと同じように 3850 を統合して、CWA、BYOD、ポスチャ アセスメントなどの高度な ISE 機能をサポートすることができます。本書では、BYOD 関連のポリシーを取り上げます。基礎となるサービスを設定して BYOD を有効にする方法については、BYOD ハウツー ガイドを参照してください。必要な設定には、CA サーバ、外部 ID ソース、サプリカント プロビジョニング ポリシーが含まれます。

アイデンティティ シーケンスの作成

スイッチからの認証要求を処理するためのアイデンティティ シーケンスを作成します。このシーケンスでは、証明書、AD、または内部ユーザ データベースを使用してエンドポイントを認証します。

ステップ 1 ISE のプライマリ管理ノードにログインします。
ステップ 2 [管理（Administration）] → [アイデンティティの管理（Identity Management）] → [ID ソースシーケンス（Identity Source Sequences）] を選択します。
ステップ 3 [追加（Add）] をクリックします。
ステップ 4 **CAP_AD_Internal** という名前のシーケンスを作成します。

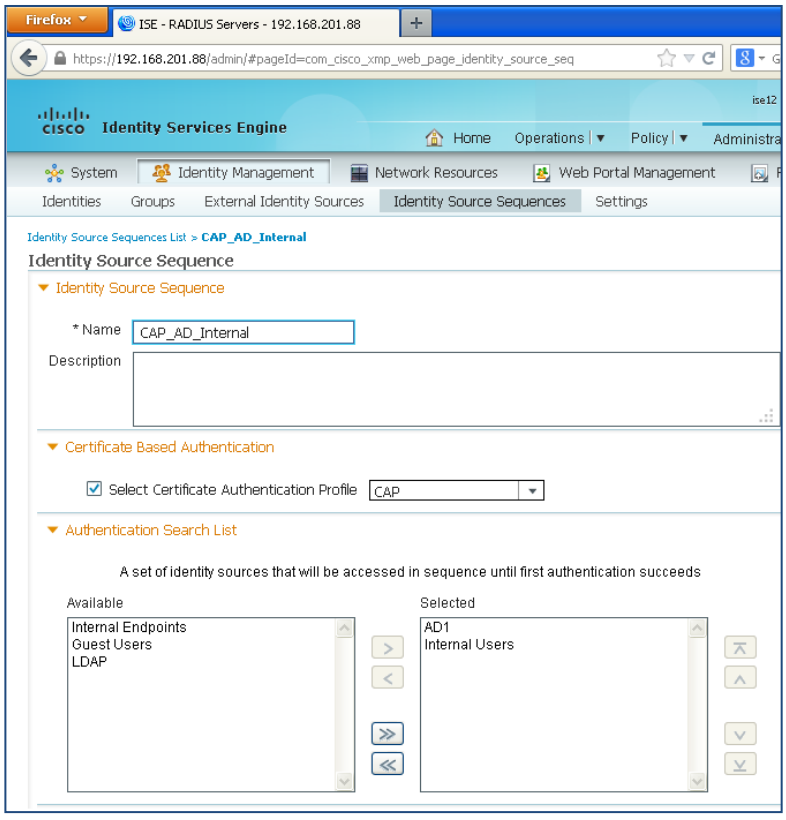

図 10. アイデンティティ シーケンスの作成

ステップ 5 [保存（Save）] をクリックします。

ユーザ グループの作成とユーザの割り当て

この例では、請負業者ユーザは ISE の内部データベースを使用して認証され、従業員ユーザは証明書または AD ユーザ アカウントを使用して認証されます。請負業者ユーザを対象に ISE ユーザ グループを作成します。

ステップ 1 [管理(Administration)] → [アイデンティティの管理(Identity Management)] → [グループ(Groups)] → [ユーザ ID グループ(User Identity Groups)] を選択します。
ステップ 2 [追加(Add)] をクリックします。
ステップ 3 グループ名として **Contractor** と入力してから、[送信(Submit)] をクリックします。
ステップ 4 [管理(Administration)] → [アイデンティティの管理(Identity Management)] → [ID(Identities)] → [ユーザ(Users)] に移動します。
ステップ 5 [追加(Add)] をクリックします。
ステップ 6 ユーザ名として「**contractor1**」を入力し、パスワードを入力します。
ステップ 7 ユーザ グループとして「**Contractor**」を選択し、[送信(Submit)] をクリックします。

ポリシー セットの有効化

ISE 1.2 に含まれるポリシー セット機能を使用して、管理者は複雑なアイデンティティ ポリシーを作成できます。本書では、WLAN のそれぞれにマッピングする 2 つのポリシー セットを作成し、各ポリシー セットに含める基礎となるポリシーを作成します。これにより、ISE のポリシー構造によって個々の使用事例にどのようにポリシーが適用されるかが明確になります。

ステップ 1 ポリシー セット機能を有効にするために、[管理(Administration)] → [システム(System)] → [設定(Settings)] → [ポリシーセット(Policy Sets)] に移動します。
ステップ 2 [有効(Enabled)] を選択し、[保存(Save)] をクリックします。

注: いったんポリシー セット機能を有効にすると、ポリシーを再作成しなければ、クラシック モードに戻ることができなくなります。ただし、この機能が有効にされる際に、初期ポリシーがデフォルト ポリシー セットにコピーされます。

ダウンロード可能 ACL の作成

ここで、認可時に適用する DACL(Downloadable ACL)を作成します。

ステップ 1 [ポリシー(Policy)] → [ポリシー要素(Policy Elements)] → [結果(Results)] → [許可(Authorization)] → [ダウンロード可能 ACL(Downloadable ACLs)] を選択します。
ステップ 2 [追加(Add)] をクリックし、次のパラメータを設定して NSP 認可プロファイルを作成します。

表 10. NSP 認可プロファイル

名前	INTERNET-ONLY
DACL コンテンツ(DACL Content)	permit udp any host 192.168.201.72 eq domain permit udp any any eq bootpc deny ip any any

ステップ 3 [保存(Save)] をクリックします。

認可プロファイルの設定

3 つの認可プロファイルを作成します。

ステップ 1 [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] → [許可（Authorization）] → [許可プロファイル（Authorization Profiles）] を選択します。
ステップ 2 [追加（Add）] をクリックし、次のパラメータを設定して NSP 認可プロファイルを作成します。

名前	NSP
一般的なタスク	Web リダイレクト（Web Redirection）
Web リダイレクトタイプ（Web Redirection Type）	ネイティブ サプリカント プロビジョニング（Native Supplicant Provisioning）
ACL	REDIRECT-ACL

ステップ 3 [保存（Save）] をクリックします。
ステップ 4 [追加（Add）] をクリックし、次のパラメータを設定して WebAuth 認可プロファイルを作成します。

名前	WebAuth
一般的なタスク	Web リダイレクト（Web Redirection）
Web リダイレクトタイプ（Web Redirection Type）	中央集中 Web 認証（Centralized Web Auth）
ACL	REDIRECT-ACL

ステップ 5 [保存（Save）] をクリックします。
ステップ 6 [追加（Add）] をクリックし、次のパラメータを設定してインターネット認可プロファイルを作成します。

名前	インターネット
一般的なタスク	DACL 名（DACL Name）
ACL	INTERNET-ONLY

ポリシーの設定

ステップ 1 [ポリシー(Policy)] → [ポリシーセット(Policy Set)] に移動します。
ステップ 2 左ペインの [+] 記号をクリックし、[上に作成(Create Above)] をクリックします。

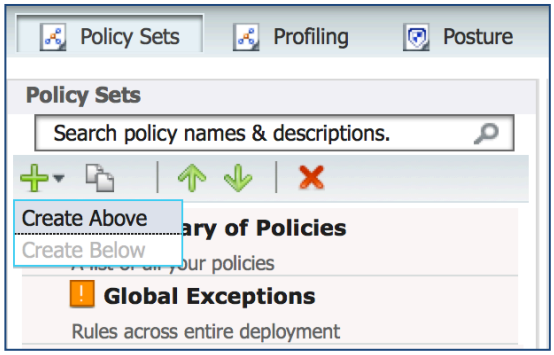

図 11. ポリシーの設定

ステップ 3 次のパラメータを設定して **example_secure** という名前のポリシー セットを定義します。

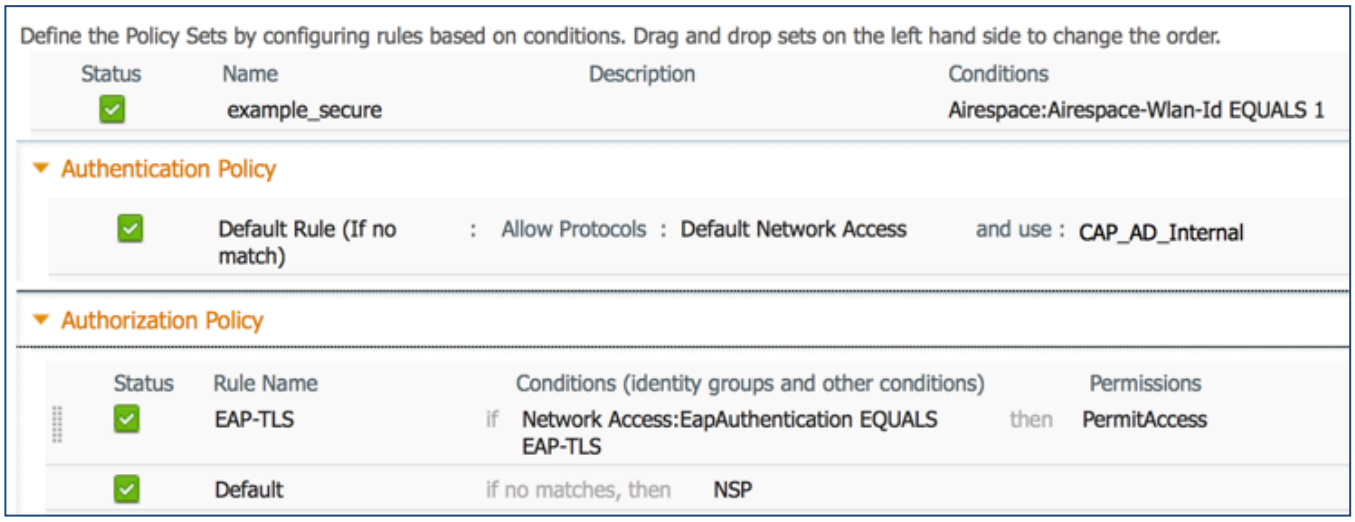

図 12. ポリシーの定義

ステップ 4 [送信(Submit)] をクリックします。
ステップ 5 次のパラメータを設定して「example_open」という名前のポリシー セットを定義します。

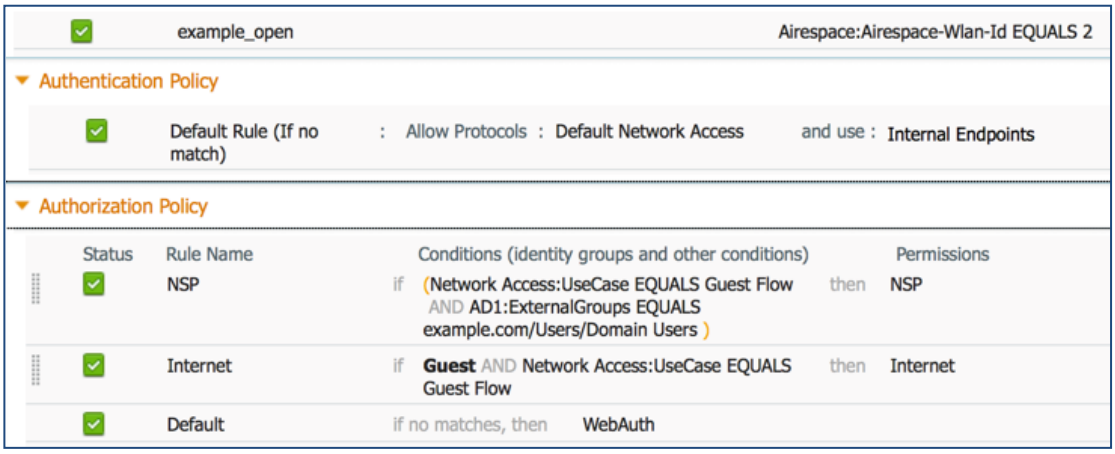

図 13. ポリシーの定義

ステップ 6 [送信(Submit)] をクリックします。

RADIUS テスト メッセージを抑制する ISE の設定

収集フィルタを設定して、モニタリング サーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。抑制を無効にすることもできます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

注: 収集フィルタ数を 20 に制限することを推奨します。

ステップ 1 ISE のプライマリ管理ノードにログインします。
ステップ 2 [管理(Administration)] > [システム(System)] > [ロギング(Logging)] に移動します。
ステップ 3 左ペインの [収集フィルタ(Collection Filters)] をクリックします。
ステップ 4 右ペインの最上部にある [追加(Add)] をクリックします

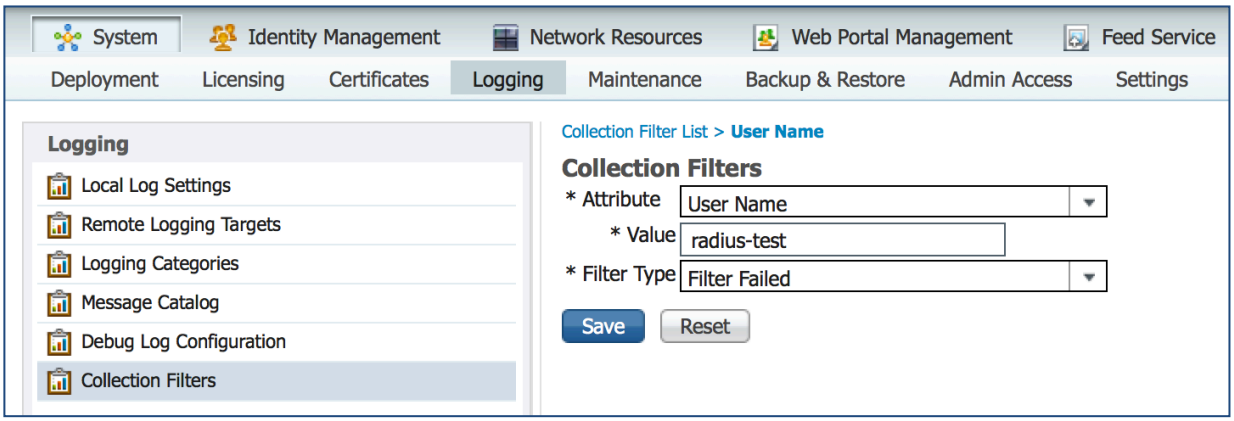

図 14. 収集フィルタの追加

ステップ 5 [属性(Attribute)] プルダウン メニューから [ユーザ名(User Name)] を選択します。
ステップ 6 [値(Value)] として「**radius-test**」と入力します。
ステップ 7 [フィルタタイプ(Filter Type)] プルダウン メニューから [すべてをフィルタ(Filter All)] を選択します。
ステップ 8 [**保存(Save)**] をクリックします。