デフォルト以外の IP またはマルチ VLAN 設定で ASA 5506W-X を設定する

内容

概要

このドキュメントでは、既存のネットワークに適合するようにデフォルトの IP アドレッシング方式を変更する必要がある場合、または複数のワイヤレス VLAN が必要な場合に、Cisco 適応型セキュリティ アプライアンス（ASA） 5506W-X デバイスの初回インストールおよび設定方法について説明します。 ワイヤレス アクセス ポイント（WAP）にアクセスするだけでなく、その他の

サービス（DHCP など）が期待どおりに機能し続けるようにするために、デフォルトの IP アドレスを変更する際に必要になるいくつかの設定変更があります。 また、このドキュメントでは、統合ワイヤレスアクセスポイント(WAP)のCLI設定例を紹介し、WAPの初期設定を簡単に完了できるようにします。このドキュメントは、Cisco Webサイトで提供されている既存のCisco ASA 5506-Xクイックスタートガイドを補足するものです。

前提条件

このドキュメントでは、ワイヤレス アクセス ポイントを含む Cisco ASA5506W-X デバイスの初期構成にのみ適用され、既存の IP アドレッシング方式を変更するか、別のワイヤレス VLAN を追加する場合に必要なさまざまな変更に対処することのみを意図しています。 デフォルト設定のインストールでは、既存の『ASA 5506-X クイック スタート ガイド』を参照する必要があります。

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASA 5506W-X デバイス
- Putty、SecureCRT などの端末エミュレーション プログラムを備えたクライアント マシン
- コンソール ケーブルおよびシリアル PC ターミナル アダプタ（DB-9 から RJ-45）

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。

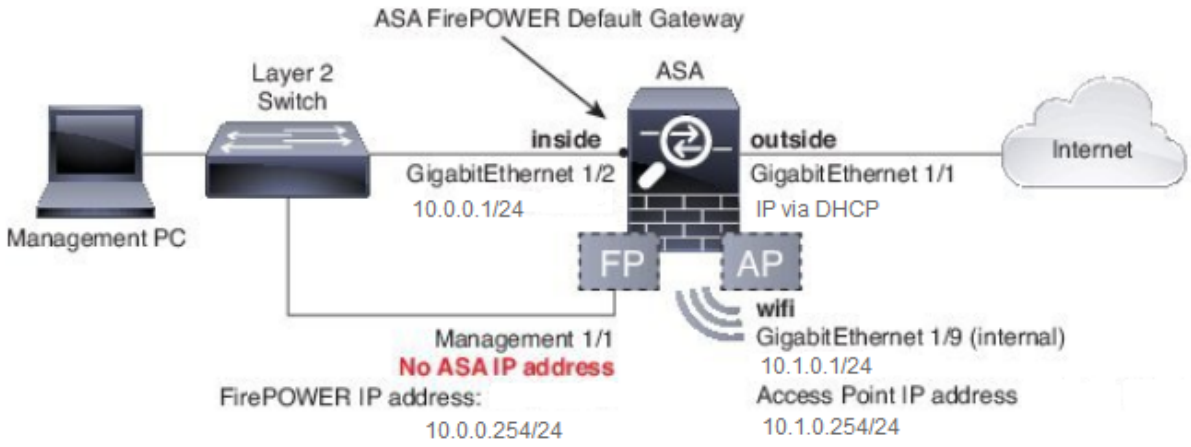
- Cisco ASA 5506W-X デバイス
- Putty、SecureCRT などの端末エミュレーション プログラムを備えたクライアント マシン
- コンソール ケーブルおよびシリアル PC ターミナル アダプタ（DB-9 から RJ-45）
- ASA FirePOWER モジュール
- 統合 Cisco Aironet 702i ワイヤレス アクセス ポイント（組み込み WAP）

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。

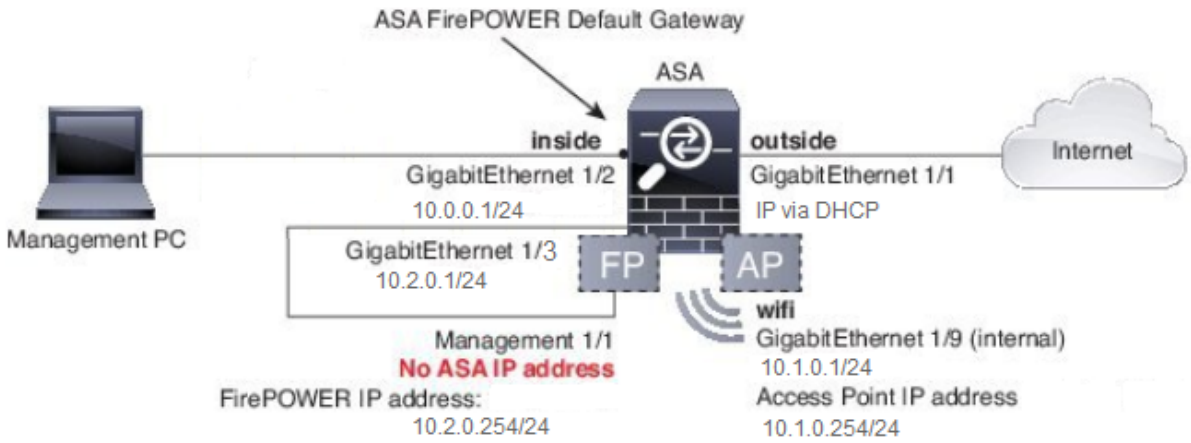
ネットワーク図

次の画像は、2 つの異なるトポロジに適用される IP アドレッシングの例です。

ASA + FirePOWER、内部スイッチあり：



ASA + FirePOWER、内部スイッチなし：



設定

クライアントにコンソール ケーブルを接続し、ASA に電源を入れて起動したら、次の手順を順番どおりに実行する必要があります。

手順 1：ASA 上でインターフェイスの IP 設定を変更する

既存の環境内で、必要に応じて IP アドレスを持つように内部（GigabitEthernet 1/2）インターフェイスと WiFi （GigabitEthernet 1/9）インターフェイスを設定します。 この例では、内部クライアントは 10.0.0.1/24 ネットワーク上にあり、WiFi クライアントは 10.1.0.1/24 ネットワーク上にあります。

```
asa(config)# interface gigabitEthernet 1/2
asa(config-if)# ip address 10.0.0.1 255.255.255.0

asa(config)# interface gigabitEthernet 1/9
asa(config-if)# ip address 10.1.0.1 255.255.255.0
```

注：前述のインターフェイスの IP アドレスを変更すると、この警告が表示されます。 これ

は予想どおりの結果です。

```
Interface address is not on same subnet as DHCP pool
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
```

手順 2：内部インターフェイスと WiFi インターフェイスの両方の DHCP プールの設定を変更する

環境内で ASA が DHCP サーバとして使用される場合、この手順が必要です。 別の DHCP サーバを使用してクライアントに IP アドレスが割り当てられた場合、元の DHCP は ASA 上で完全に無効にする必要があります。 IP アドレッシング方式を変更したので、ASA がクライアントに提供している既存の IP アドレス範囲を変更する必要があります。 次のコマンドは、新しい IP アドレス範囲と一致するように、新しいプールを作成します。

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside
asa(config)# dhcpd address 10.1.0.2-10.1.0.100 wifi
```

また、DHCP プールを変更すると、ASA 上の以前の DHCP サーバを無効にするので、それを再度有効にする必要があります。

```
asa(config)# dhcpd enable inside
asa(config)# dhcpd enable wifi
```

DHCP の変更を行う前にインターフェイスの IP アドレスを変更しないとこの工ラーが表示されます。

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside
Address range subnet 10.0.0.2 or 10.0.0.100 is not the same as inside interface subnet
192.168.1.1
```

手順 3：内部クライアントと WiFi DHCP クライアントに渡す DNS サーバを指定する

クライアントが DHCP 経由で IP アドレスを割り当てる場合、ほとんどのクライアントに DHCP サーバが DNS サーバを割り当てる必要があります。 次のコマンドは、すべてのクライアントに対して、10.0.0.250 にある DNS サーバを含めるように ASA を設定します。 内部 DNS サーバまたは ISP から提供された DNS サーバのいずれかの代わりに 10.0.0.250 を用いる必要があります。

```
asa(config)# dhcpd dns 10.0.0.250 interface inside
asa(config)# dhcpd dns 10.0.0.250 interface wifi
```

手順 4：Adaptive Security Device Manager（ASDM）アクセス用に ASA 上の HTTP アクセスの設定を変更する

IP アドレッシングが変更されているので、内部ネットワークおよび WiFi ネットワーク上のクライアントが ASDM にアクセスして ASA を管理できるように、ASA への HTTP アクセスも変更する必要があります。

```
asa(config)# no http 192.168.1.0 255.255.255.0 inside
asa(config)# no http 192.168.10.0 255.255.255.0 wifi
asa(config)# http 0.0.0.0 0.0.0.0 inside asa(config)# http 0.0.0.0 0.0.0.0 wifi
```

注：この設定では、内部クライアントまたは WiFi インターフェイス上のすべてのクライアントが ASDM 経由で ASA にアクセスできます。 セキュリティのベスト プラクティスとして、アドレスの範囲を信頼できるクライアントのみに制限する必要があります。

手順 5：WLAN コンソールのアクセス ポイント管理（インターフェイス BVI1）用にインターフェイスの IP を変更する

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface BVI1
ap(config-if)#ip address 10.1.0.254 255.255.255.0
```

手順 6：WAP 上でデフォルト ゲートウェイを変更する

この手順は、発信元がローカル サブネットではないすべてのトラフィックの送信先を WAP に知らせるために必要です。 これは、ASA の内部インターフェイス上のクライアントから HTTP 経由で WEB GUI にアクセスするできるようにするのに必要です。

```
ap(config)#ip default-gateway 10.1.0.1
```

手順 7：FirePOWER モジュール管理 IP アドレスを変更する（オプション）

Cisco FirePOWER（別名 SFR）モジュールも導入予定の場合、その IP アドレスを変更し、ASA 上の物理管理 1/1 インターフェイスからそのモジュールにアクセスできるようにする必要があります。ASA および SFR モジュールを設定する方法を決定する 2 つの基本的な導入シナリオがあります。

1. ASA 管理 1/1 インターフェイスが内部スイッチに接続されているトポロジ（通常のクイック スタート ガイドに従う）。
2. 内部スイッチが存在しないトポロジ。

シナリオに応じて、適切な手順は次のとおりです。

ASA 管理 1/1 インターフェイスが内部スイッチに接続されている場合：

モジュールに接続してセッションを開始し、モジュールを内部スイッチに接続する前に ASA からそれを変更できます。 この設定では、10.0.0.254 の IP アドレスを持つ ASA の内部インターフェイスと同じサブネット上に SFR モジュールを配置することで、IP 経由でそのモジュールにアクセスできます。

太字の行は、この例に固有のもので、IP 接続を確立するのに必要です。

イタリックの行は環境ごとに異なります。

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)
Sourcefire3D login: admin
Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:


Enter an IPv4 address for the management interface [192.168.45.45]: 10.0.0.254

Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []:

10.0.0.1


Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco_SFR
Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.250
Enter a comma-separated list of search domains or 'none' [example.net]: example.net
If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Applying 'Default Allow All Traffic' access control policy.
```

> **注**：デフォルトのアクセス コントロール ポリシーを SFR モジュールに適用するには数分かかる場合があります。 適用が完了したら、Ctrl+Shift+6+X（CTRL^ X）を押して SFR モジュール CLI からエスケープし、ASA に戻ることができます。

ASA が内部スイッチに接続されていない場合：

内部スイッチは、一部の小規模な導入では内部スイッチが存在しない可能性があります。 そのようなタイプのトポロジでは、クライアントは一般的に WiFi インターフェイス経由で ASA に接続します。 そのようなシナリオでは、外部スイッチの必要性をなくし、別の物理 ASA インターフェイスに管理 1/1 インターフェイスを相互接続することで、別の ASA インターフェイス経由で SFR モジュールにアクセスできます。

そのような例では、ASA GigabitEthernet 1/3 インターフェイスと管理 1.1 インターフェイスとの間に物理的なイーサネット接続が存在している必要があります。 さらに、ASA と SFR モジュールを別のサブネット上に存在するように設定すると、内部インターフェイスまたは WiFi インターフェイスに配置されたクライアントと ASA の両方から SFR にアクセスできます。

ASA インターフェイスの設定：

```
asa(config)# interface gigabitEthernet 1/3
asa(config-if)# ip address 10.2.0.1 255.255.255.0
asa(config-if)# nameif sfr
INFO: Security level for "sfr" set to 0 by default.
asa(config-if)# security-level 100
asa(config-if)# no shut
```

SFR モジュールの設定：

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)
Sourcefire3D login: admin
Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

```
Enter an IPv4 address for the management interface [192.168.45.45]: 10.2.0.254
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []: 10.2.0.1
```

```
Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco_SFR Enter a comma-
separated list of DNS servers or 'none' []: 10.0.0.250 Enter a comma-separated list of search
domains or 'none' [example.net]: example.net If your networking information has changed, you
will need to reconnect. For HTTP Proxy configuration, run 'configure network http-proxy'
Applying 'Default Allow All Traffic' access control policy.
```

> **注**：デフォルトのアクセス コントロール ポリシーを SFR モジュールに適用するには数分かかる場合があります。 適用が完了したら、Ctrl+Shift+6+X（CTRL^ X）を押して SFR モジュール CLI からエスケープし、ASA に戻ることができます。

SFR の設定が適用されたら、ASA から SFR の管理 IP アドレスに ping を実行できるはずです。

```
asa# ping 10.2.0.254


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
asa#
```

インターフェイスに正常に ping を実行できない場合は、物理的なイーサネット接続の設定および状態を確認します。

手順 8：AP GUI に接続して無線を有効にし、他の WAP 設定を編集する

この時点で、クイック スタート ガイドで説明したように、WAP を管理するために HTTP GUI 経由で接続できるはずです。 5506Wの内部ネットワークに接続されているクライアントのWebブラウザからWAPのBVIインターフェイスのIPアドレスを参照するか、設定例を適用してWAPのSSIDに接続します。次のCLIを使用しない場合は、Gigabit1にASA上の2つのインターフェイス。

CLI を使用して WAP を設定する場合は、ASA から WAP に接続してセッションを開始し、ここでの例の設定を使用できます。これにより、5506W と 5506W_5Ghz という名前のオープン SSID が作成されるので、ワイヤレス クライアントを使用して WAP に接続し、さらなる管理を実行できます。

> **注**：この設定を適用したら、GUI にアクセスして SSID にセキュリティを適用することでワイヤレス トラフィックを暗号化するようにしてください。

修正された IP 範囲を使用する単一のワイヤレス VLAN 用の WAP CLI 設定

```
dot11 ssid 5506W
   authentication open
   guest-mode
dot11 ssid 5506W_5Ghz
   authentication open
   guest-mode
!
interface Dot11Radio0
 !
 ssid 5506W
 !
interface Dot11Radio1
 !
 ssid 5506W_5Ghz
 !
interface BVI1
 ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
 no shut
!
interface Dot11Radio1
 no shut
```

この時点から、通常の手順を実行してWAPの設定を完了し、上記で作成したSSIDに接続されたクライアントのWebブラウザからアクセスできる必要があります。アクセスポイントのデフォルトのユーザ名はCisco、パスワードはCです。

Cisco ASA 5506-X シリーズ クイック スタート ガイド

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

クイック スタート ガイドに記載されているように、192.168.10.2 の代わりに 10.1.0.254 の IP アドレスを使用する必要があります。

設定

設定結果が出力と一致している必要があります (IP 範囲の例を使用した場合。それ以外の場合は、適宜置き換えてください)。

ASA の設定

インターフェイス :

注：イタリックの行は、内部スイッチを持たない場合のみ適用されます。

```
asa# sh run interface gigabitEthernet 1/2


!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0


asa# sh run interface gigabitEthernet 1/3


!
interface GigabitEthernet1/3
 nameif sfr
 security-level 100
 ip address 10.2.0.1 255.255.255.0

asa# sh run interface gigabitEthernet 1/9


!
interface GigabitEthernet1/9
 nameif wifi
 security-level 100
 ip address 10.1.0.1 255.255.255.0
asa#
```

DHCP :

```
asa# sh run dhcpd
```

```
dhcpd auto_config outside **auto-config from interface 'outside' **auto_config dns x.x.x.x
x.x.x.x <-- these lines will depend on your ISP **auto_config domain isp.domain.com <-- these
lines will depend on your ISP ! dhcpd address 10.0.0.2-10.0.0.100 inside dhcpd dns 10.0.0.250
interface inside dhcpd enable inside ! dhcpd address 10.1.0.2-10.1.0.100 wifi dhcpd dns
10.0.0.250 interface wifi dhcpd enable wifi ! asa#
```

HTTP:

```
asa# show run http


http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
asa#
```

Aironet WAP の設定（SSID の設定例を使用しない）

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.



ap#show configuration | include default-gateway


ip default-gateway 10.1.0.1



ap#show configuration | include ip route


ip route 0.0.0.0 0.0.0.0 10.1.0.1


ap#show configuration | i interface BVI|ip address 10


interface BVI1 ip address
10.1.0.254 255.255.255.0
```

FirePOWER モジュール設定（内部スイッチあり）

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===============[ System Information ]===============
Hostname                  : Cisco_SFR
Domains                   : example.net
DNS Servers               : 10.0.0.250
Management port           : 8305
```

```
IPv4 Default route
  Gateway                 : 10.0.0.1



======================[ eth0 ]======================
State                    : Enabled
Channels                 : Management & Events
Mode                     :
MDI/MDIX                 : Auto/MDIX
MTU                      : 1500
MAC Address              : B0:AA:77:7C:84:10


----------------------[ IPv4 ]----------------------

Configuration            : Manual
Address                  : 10.0.0.254
Netmask                  : 255.255.255.0
Broadcast                : 10.0.0.255


----------------------[ IPv6 ]----------------------
Configuration            : Disabled

===============[ Proxy Information ]================
State                    : Disabled
Authentication           : Disabled

>
```

FirePOWER モジュール設定（内部スイッチなし）

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===============[ System Information ]===============
Hostname                 : Cisco_SFR
Domains                  : example.net
DNS Servers              : 10.0.0.250
Management port          : 8305


IPv4 Default route
  Gateway                 : 10.2.0.1



======================[ eth0 ]======================
State                    : Enabled
Channels                 : Management & Events
Mode                     :
MDI/MDIX                 : Auto/MDIX
MTU                      : 1500
MAC Address              : B0:AA:77:7C:84:10
```

```
----------------------[ IPv4 ]---------------------
Configuration              : Manual
Address                    : 10.2.0.254
Netmask                    : 255.255.255.0
Broadcast                  : 10.2.0.255


----------------------[ IPv6 ]----------------------
Configuration              : Disabled

===============[ Proxy Information ]================
State                      : Disabled
Authentication             : Disabled

>
```

確認

インストール プロセスを完了するために、WAP への接続が適切かどうかを確認するには：

1. ASA の内部インターフェイスにテスト クライアントを接続し、予定した IP 範囲内にある DHCP 経由で ASA から IP アドレスを受信できることを確認してください。
2. クライアントの Web ブラウザを使用して https://10.1.0.254 に移動し、AP GUI にアクセスできることを確認します。
3. 内部クライアントおよび ASA から SFR 管理インターフェイスに ping を実行し、接続が適切かどうか確認します。

複数のワイヤレス VLAN を持つ DHCP の設定

この設定は、単一のワイヤレス VLAN を使用することを前提としています。ワイヤレス AP 上のブリッジ仮想インターフェイス（BVI）は、複数の VLAN にブリッジを提供できます。5506W を複数の VLAN 用に DHCP サーバとして設定する場合、Gigabit 1/9 インターフェイス上にサブインターフェイスを作成し、それぞれに名前を付ける必要があります。これは、ASA 上の DHCP の構文が原因です。この項では、デフォルト設定を削除する方法、および複数の VLAN 用に ASA を DHCP サーバとしてセットアップするのに必要な設定を適用する方法について、そのプロセスを段階的に説明します。

手順 1：Gig 1/9 上の既存の DHCP 設定を削除する

最初に、Gig 1/9（WiFi）インターフェイス上の既存の DHCP 設定を削除します。

```
ciscoasa# no dhcpd address 10.1.0.2-10.1.0.100 wifi
ciscoasa# no dhcpd enable wifi
```

手順 2：Gig1/9 上の VLAN ごとにサブインターフェイスを作成する

アクセスポイントに設定したVLANごとに、Gig1/9のサブインターフェイスを設定する必要があります。この設定例では、2つのサブインターフェイスを追加します。

-Gig 1/9.5（nameif vlan5 を持ち、VLAN 5 およびサブネット 10.5.0.0/24 に応答する）

-Gig 1/9.30（nameif vlan30 を持ち、VLAN 30 およびサブネット 10.3.0.0/24 に応答する）

実際には、ここで設定した VLAN とサブネットが、アクセス ポイントで指定した VLAN とサブネットと一致していることが不可欠です。nameif およびサブインターフェイス番号は任意のものを選択できます。 Web GUI を使用してアクセス ポイントを設定するには、前述のクイック スタート ガイドのリンクを参照してください。

```
ciscoasa(config)# interface g1/9.5
ciscoasa(config-if)# vlan 5
ciscoasa(config-if)# nameif vlan5
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.5.0.1 255.255.255.0

ciscoasa(config-if)# interface g1/9.30
ciscoasa(config-if)# vlan 30
ciscoasa(config-if)# nameif vlan30
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.30.0.1 255.255.255.0
```

手順 3：各 VLAN に DHCP プールを指定する

設定中の VLAN ごとに、異なる DHCP プールを作成します。このコマンドの構文には、ASA による問題のプールの提供元となる nameif を指定する必要があります。この例では、次のように VLAN 5 および 30 です。

```
ciscoasa(config)# dhcpd address 10.5.0.2-10.5.0.254 vlan5
ciscoasa(config)# dhcpd address 10.30.0.2-10.30.0.254 vlan30
ciscoasa(config)# dhcpd enable vlan5
ciscoasa(config)# dhcpd enable vlan30
```

手順 4：アクセス ポイントの SSID を設定し、設定を保存し、モジュールをリセットする

最後に、ASA の設定に対応するようにアクセス ポイントを設定する必要があります。アクセス ポイントの GUI インターフェイスを使用すると、内部の ASA の内部（Gigabit 1/2）インターフェイスに接続されたクライアント経由で AP 上の VLAN を設定できます。ただし、CLIを使用してASAコンソールセッション経由でAPを設定し、ワイヤレスでAPを管理する場合は、VLAN 5と30に2つのSSIDを作成するためのテンプレートとして、この設定を使用できます。これは、グローバルコンフィギュレーションモードでAPコンソール入力します。

```
dot11 vlan-name VLAN30 vlan 30
dot11 vlan-name VLAN5 vlan 5
!
dot11 ssid SSID_VLAN30
   vlan 30
   authentication open
   mbssid guest-mode
!
dot11 ssid SSID_VLAN5
   vlan 5
   authentication open
   mbssid guest-mode
!
interface Dot11Radio0
 !
 ssid SSID_VLAN30
 !
 ssid SSID_VLAN5
 mbssid
!
interface Dot11Radio0.5
 encapsulation dot1Q 5
```

```
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 !
 ssid SSID_VLAN30
 !
 ssid SSID_VLAN5
 mbssid
!
 interface Dot11Radio1.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 spanning-disabled
 no bridge-group 5 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
 no shut
!
interface Dot11Radio1
 no shut
```

この時点では、ASAとAPの管理設定が完了し、ASAはVLAN 5および30のDHCPサーバとして機

*能します。APで**write memoryコマンドを使用して設定を保存した後に、接続の問題が解決しない場合は**、新しく作成されたSSIDでIPアドレスを受信すると、これ以上の操作は必要ありません。*

```
ap#write memory
Building configuration...
[OK]
ap#reload
Proceed with reload? [confirm]
Writing out the event log to flash:/event.log ...
```

> **注**：ASA デバイス全体を入力する必要はありません。組み込みのアクセス ポイントのみリロードする必要があります。

AP のリロードが完了すると、WiFi ネットワークまたは内部ネットワーク上のクライアント マシンから AP GUI に接続できるはずです。 AP が完全に再起動するまでに、一般的には約 2 分かかります。 この時点で、通常の手順を実行し、WAP の設定を完了できます。

Cisco ASA 5506-X シリーズ クイック スタート ガイド

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

トラブルシュート

このドキュメントは、初期設定について説明することを意図しているので、ASA の接続に関するトラブルシューティングは、このドキュメントの範囲外です。 すべての手順を正常に完了したかどうか、設定に関する項を参照し、確認してください。