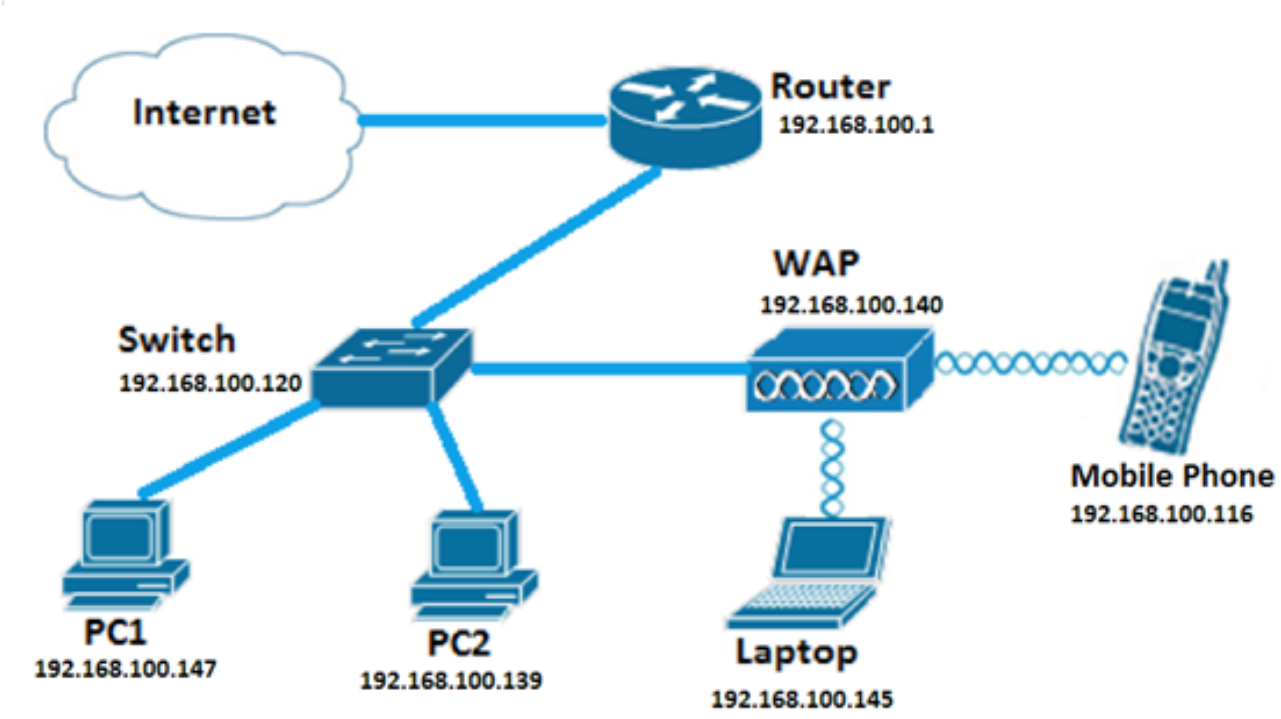
WAP125 および WAP581 の設定 IPv4 ACL

概要

Internet Protocol（IP）バージョン 4（IPv4）はおよび Internet Protocol（IP）バージョン 6（IPv6）アクセス コントロール リスト（ACL）ワイヤレスアクセスポイント（WAP）受信されるパケットに適用される一組の規則です。 各ルールがネットワークへのアクセスが許可されるか、または拒否する必要があるかどうか判別するのに使用されています。 ACL は出典のようなフレームのフィールドをか宛先 IP アドレス、Virtual Local Area Network（VLAN; バーチャル LAN）識別子（ID）、または Class of Service（CoS）点検するために設定することができます。 フレームが WAP デバイス ポートを入力するとき、フレームを点検し、フレームのコンテンツに対して ACL ルールをチェックします。 ルールのうちのどれかがコンテンツを一致する場合、割り当てか拒否処置はフレームでとられます。

IPv4 ACL をネットワークで『Devices』 を選択 するために設定することが一般的に ネットワークリソースにアクセスを許可するのに使用されています。

注: 作成される各ルールの終わりに暗黙の deny があります。



注: このシナリオでは、PC2 からのすべてのトラフィックはネットワークにアクセスすることができます。 他のホストからの他のトラフィックはすべて拒否されます。

目標

この技術情報は WAP125 および WAP581 アクセス ポイントの IPv4 ACL を設定する方法を示すことを向けます。

適当なデバイス

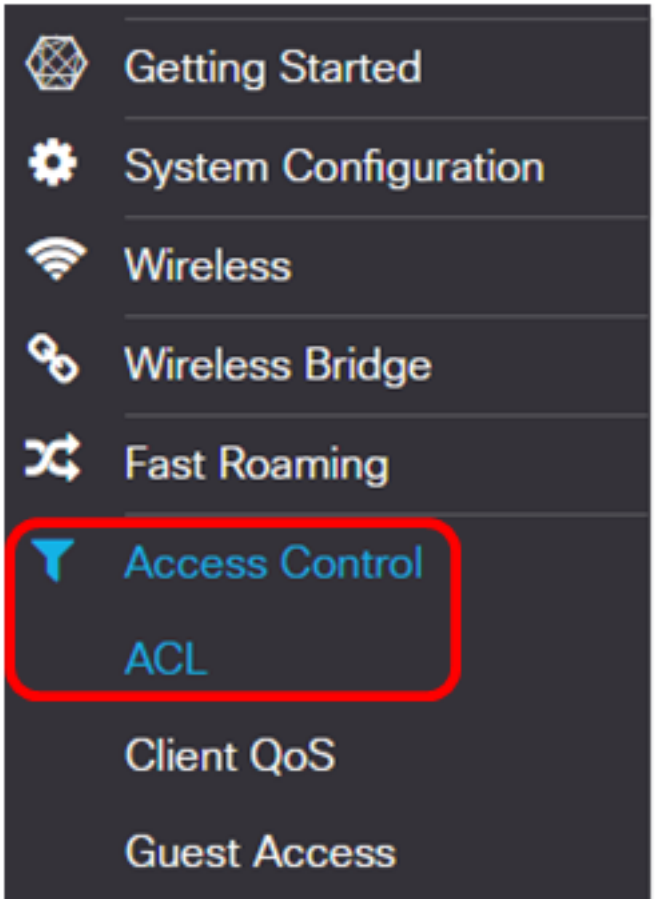
- WAP125
- WAP581

[Software Version]

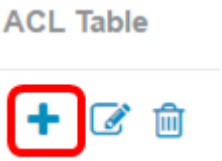
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

IPv4 ACL を設定して下さい

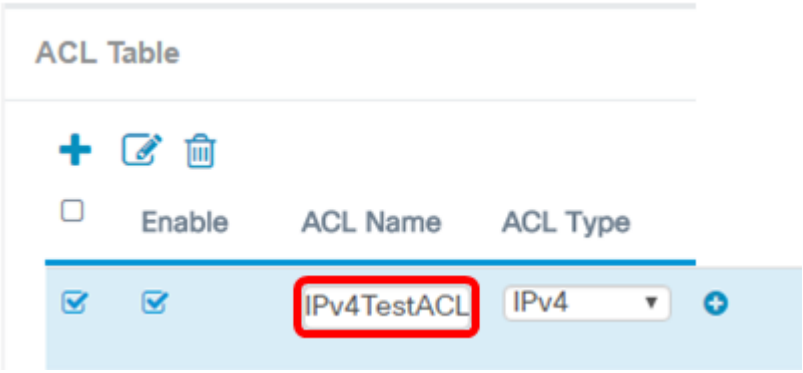
ステップ 1. WAP の Webベース ユーティリティへのログインは**アクセスコントロール > ACL** を選択し。



ステップ 2.新しい ✚ ACL を作成するためにボタンをクリックして下さい。

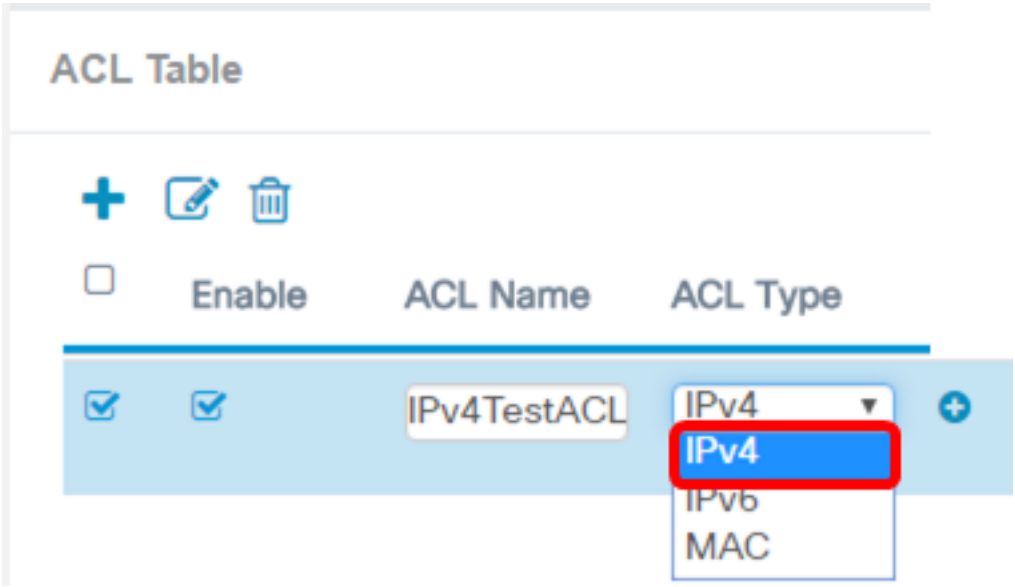


ステップ 3. *ACL Name フィールド*で ACL の名前を入力して下さい。



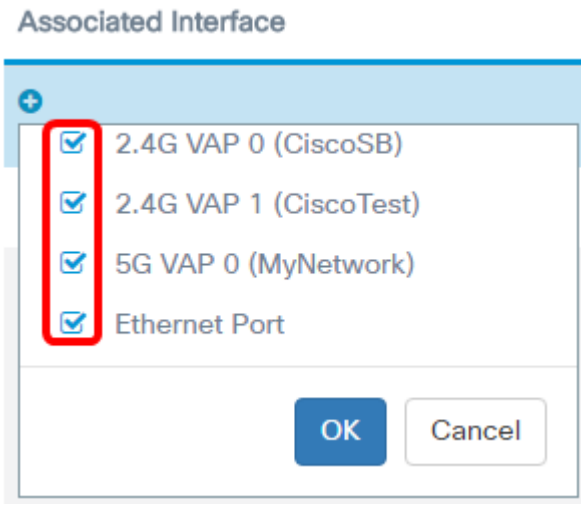
注: この例では、IPv4TestACL は入ります。

ステップ 4. ACL 型ドロップダウン リストから IPv4 を選択して下さい。



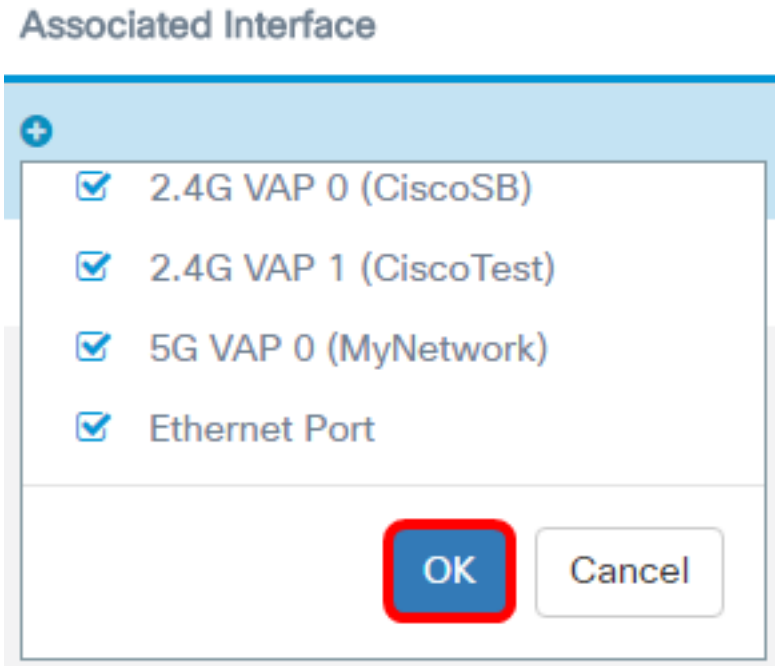
ステップ 5.ボタンを クリックし、関連するインターフェイス ドロップダウン リストからインターフェイスを選択して下さい。 次のオプションがあります。

- 2.4G VAP 0（SSID 名前）は 2.4 GHz バーチャルアクセス アクセス・ポイント（VAP）に—このオプション MAC ACL を適用します。 SSID 名前セクションは WAP で設定される SSID 名前によって変更するかもしれません。
- 5G VAP0（SSID 名前）—このオプションは 5 GHz VAP に MAC ACL を適用します。
- イーサネットポート—このオプションは WAP のイーサネットインターフェイスに MAC ACL を適用します。

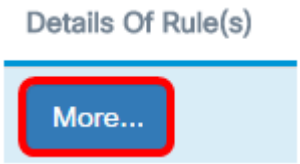


注: マルチプルインターフェイスは ACL に関連付けることができます。 ただし、それは ACL に別の ACL に既に関連付けられていたら関連付けることができません。 この例では、すべてのインターフェイスは IPv4TestACL に関連付けられています。 ACL からのインターフェイスを引き離すためにボックスのチェックを外して下さい。

ステップ 6. 『OK』 をクリック して下さい。



ステップ 7. ACL のパラメータを設定するために **More ボタンを**クリックして下さい。

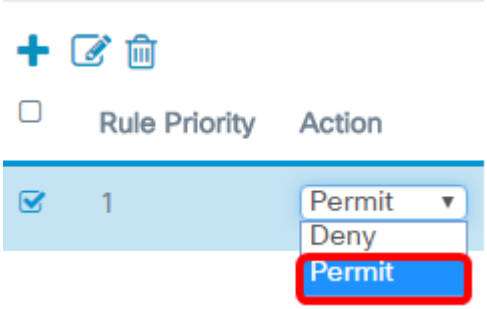


ステップ 8.新しい ✚ ルールを追加するためにボタンをクリックして下さい。

ステップ 9.処理 ドロップダウン リストから操作を選択して下さい。 次のオプションがあり

ます。

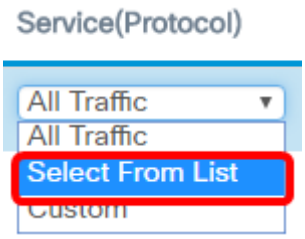
- permit —このオプションはネットワークに接続するために ACL 条件を満たしたパケットを可能にします。
- 拒否—このオプションはからのネットワークに ACL 条件を接続満たしたパケットを防ぎます。



注: この例では、割り当ては選択されます。

ステップ 10.サービス (プロトコル) ドロップダウン リストからフィルタリングされるべきサービスかプロトコルを選択して下さい。 次のオプションがあります。

- すべては ACL フィルタにマッチとして traffic —このオプションすべてのパケットを処理します。
- list —このオプションから ACL のためのフィルタとして IP、ICMP、IGMP、TCP、または UDP を選択することを許可します選択して下さい。 このオプションが選択される場合、ステップ 11.に進んで下さい。
- カスタム—このオプションはパケットのためのフィルタとしてカスタム プロトコル 識別子を入力することを可能にします。 値は四桁 16進数です。 範囲は 0 から 255 です。

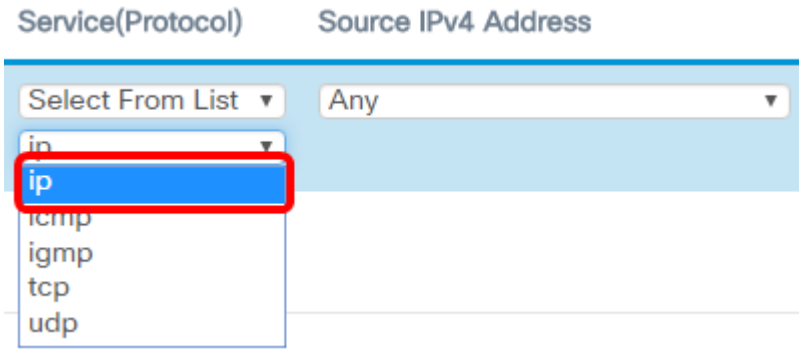


注: この例で、リストから選択されます選択して下さい。

ステップ 11.プロトコルを定義して下さいネットワークに接続することができる必要がある。 次のオプションがあります。

- ip —このオプションはアクセス ポイントがフィルタとして IP アドレスを使用してネットワークにアクセスするホストをフィルタリングするようにします。
- icmp —このオプションはアクセス ポイントがネットワークに入るアクセス ポイントを通してインターネット制御メッセージ プロトコル (ICMP) パケットをフィルタリングするようにします。
- igmp —このオプションはアクセス ポイントがネットワークに入るアクセス ポイントを通してインターネット グループ管理プロトコル (IGMP) パケットをフィルタリングするようにします。
- TCP —このオプションはアクセス ポイントがネットワークに入るアクセス ポイントを通してトランスミッション コントロール プロトコル (TCP) パケットをフィルタリングするようにします。

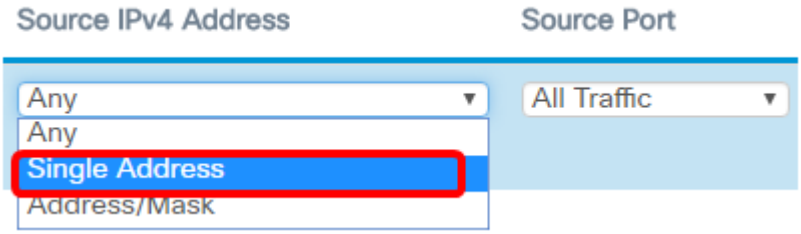
- UDP（ユーザ・データグラム・プロトコル）—このオプションはアクセス ポイントがネットワークに入るアクセス ポイントを通してユーザ データグラム プロトコル（UDP）パケットをフィルタリングするようにします。



注: この例では、IP は選択されます。

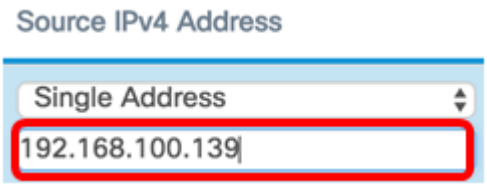
ステップ 12： 出典 IPv4 アドレス ドロップダウン リストからの出典 IPv4 アドレスを定義して下さい。 次のオプションがあります。

- —このオプションは WAP があらゆる IP アドレスからパケットにフィルタを適用するようにします。
- 単一のアドレス—このオプションは WAP が指定IPアドレスからパケットにフィルタを適用するようにします。
- アドレス/マスク—このオプションは WAP が IP アドレスにパケットにフィルタおよび IP のマスクを適用するようにします。



注: この例では、単一のアドレスは選択されます。

ステップ 13： ホストの IP アドレスを入力して下さい許可される必要があるネットワークにアクセスした場合。



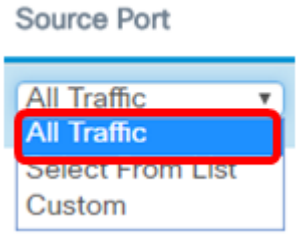
注: この例では、192.168.100.139 は入ります。 これは PC2 の IP アドレスです。

ステップ 14： 状態のための送信元ポートを選択して下さい。 次のオプションがあります。

- すべては traffic —このオプション条件を満たす送信元ポートからのすべてのパケットを割り当てます。
- list —このオプションから ftp、ftpdata、http、smtp、snmp、telnet、tftp および www を選択することを許可します選択して下さい。

- カスタム—このオプションはデータグラム ヘッダで識別された送信元ポートを一致するために IANA ポート番号を入力することを可能にします。 ポート範囲は 0 から 65535 から、次が含まれています:

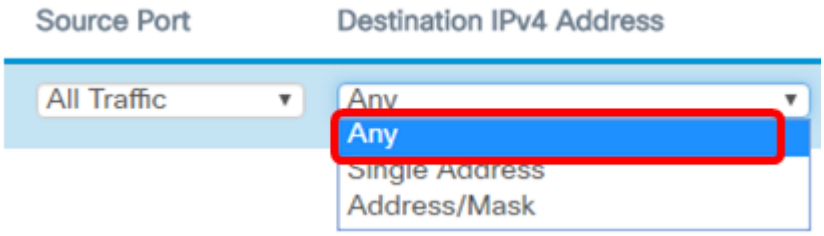
- 0 から 1023 —よく知られたポート
- 1024 — 49151 —登録済みのポート
-ダイナミック 49152 — 65535 —および/または私用 ポート



注: この例では、すべてのトラフィックは選択されます。

ステップ 15： 宛先 IPv4 アドレス ドロップダウン リストから宛先アドレスを選択して下さい。 次のオプションがあります。

- —このオプションは ACL 文に一致として IP アドレスを扱います。
- 単一のアドレス—このオプションは ACL 状態のための特定の IP アドレスを入力することを可能にします。
- アドレス/マスク—このオプションは IPアドレス範囲かマスクを入力することを可能にします。



注: この例では、選択されます。

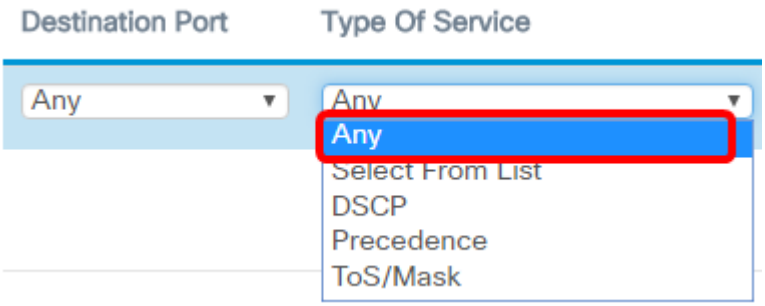
ステップ 16： 宛先ポート ドロップダウン リストから宛先ポートを選択して下さい。 次のオプションがあります。

- —このオプションは ACL の文に一致としてパケットの宛先ポートすべてを扱います。
- list —このオプションから一致するために宛先ポートと対応づけられたキーワードを選択することを許可します選択して下さい。 次のオプションがあります。 ftp、ftpdata、http、smtp、snmp、telnet、tftp および www。 これらのキーワードは対応する ポート数に変換します。
- カスタム—このオプションはデータグラム ヘッダで識別された送信元ポートを一致するために IANA ポート番号を入力することを可能にします。 ポート範囲は 0 から 65535 から、次が含まれています:

  - 0 から 1023 —よく知られたポート
  - 1024 — 49151 —登録済みのポート
  -ダイナミック 49152 — 65535 —および/または私用 ポート

ステップ 17： タイプ オブ サービス（ToS） 一致するためにサービス タイプをドロップダウン リストからのパケットタイプを選択して下さい。 次のオプションがあります。

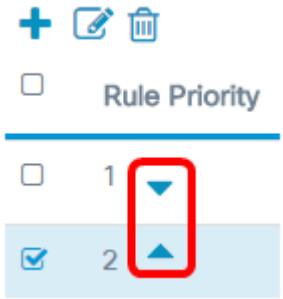
- —このオプションはパケットのための一致としてサービスを扱います。
- list —このオプションから一致します Differentiated Services Code Point、（DSCP）、Class of Service（CoS）、または Expedited Forwarding（EF）値に基づいてパケットと選択して下さい。
- dscp — オプションはカスタム DSCP 値に基づいてパケットと一致します。 このオプションを選択した場合、DSCP Value フィールドで 0 から 63 まで値を入力して下さい。
- 優位—このオプションは IP優先値に基づいてパケットと一致します。 このオプションが選択されるとき、0 から 7.まで IP優先値を入力して下さい。
- TOS/マスク—このオプションはパケットで IP TOS フィールドに対する比較のために使用する IP TOS ビット値のビットポジションを識別するために IP TOS マスクを入力することを可能にします。



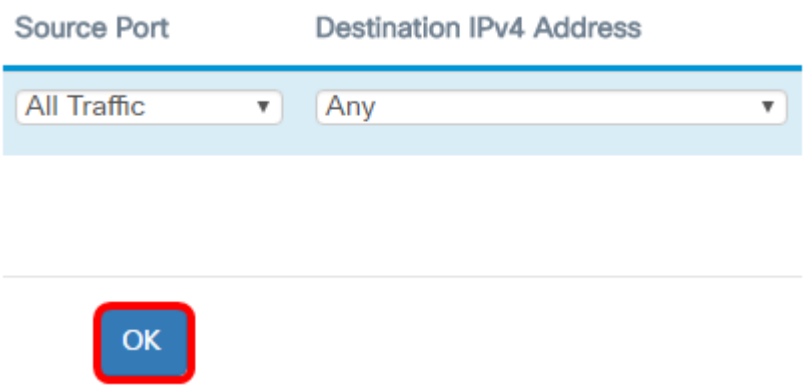
ステップ 18： （オプションの）ACL が完了するまでステップ 8 からステップ 17 を繰り返して下さい。

注: 暗黙の deny が作成される各ルールの終わりにあるのでネットワークのその他のデバイスからアクセスを防ぐ ACL に拒否ルールを追加する必要がありません。

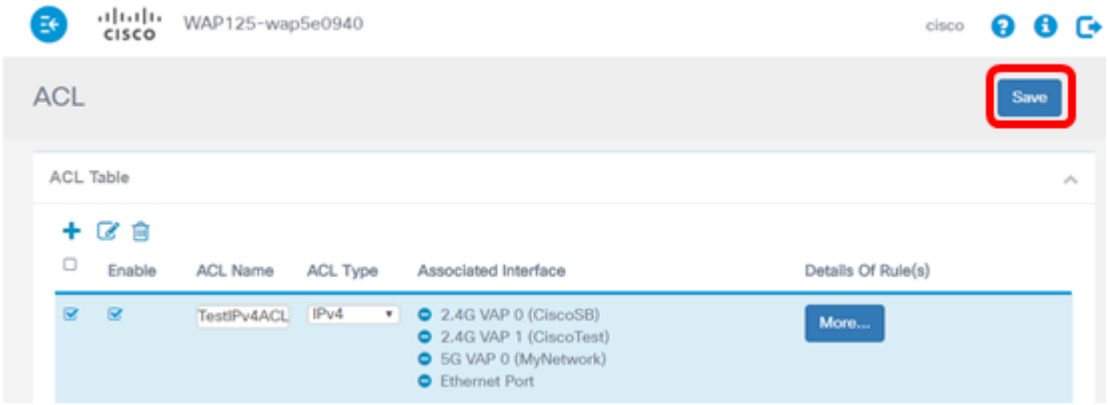
ステップ 19： （オプションの）正しい順序であるまでボタンを上下にクリックして ACL の条件の順序を変更して下さい。



ステップ 20： [OK] をクリックします。



ステップ 21： [Save] をクリックします。



今 1 ホストだけ WAP に接続されたときネットワークにアクセスするようにする IPv4 ACL を設定することを完了する必要があります。