WAP121およびWAP321アクセスポイントでのIPv4ベースアクセスコントロールリスト(ACL)のルールの作成と設定

目的

アクセスコントロールリスト(ACL)は、セキュリティの向上に使用されるネットワークトラフィックフィルタと関連付けられたアクションのリストです。ACLには、ネットワークデバイスへのアクセスを許可または拒否するホストが含まれます。QoS機能には、トラフィックをストリームに分類し、定義されたホップ単位の動作に従って特定のQoS処理を行えるDiffServサポートが含されています。

この記事では、WAP121およびWAP321アクセスポイント(WAP)でIPv4ベースのACLを作成および設定する方法について説明します。

該当するデバイス

- WAP121
- WAP321

[Software Version]

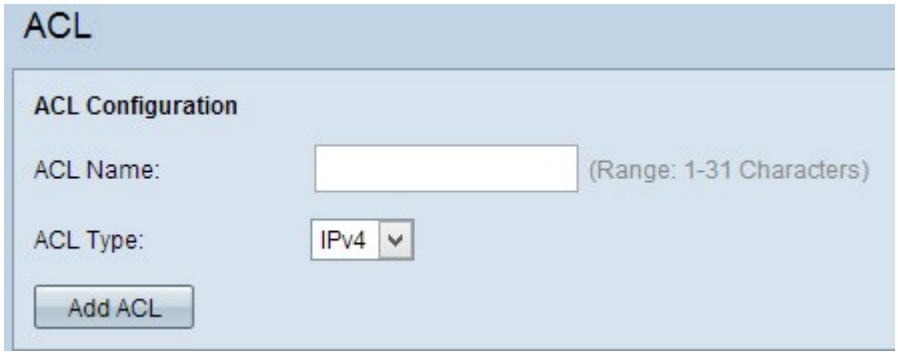
- v1.0.3.4

IPv4ベースのACL設定

IP ACLは、IPスタックのレイヤ3のトラフィックを分類します。各ACLは、ワイヤレスクライアントから送信されたトラフィック、またはワイヤレスクライアントが受信するトラフィックに適用される最大10のルールのセットです。各ルールは、ネットワークへのアクセスを許可または拒否するために、特定のフィールドの内容を使用するかどうかを指定します。ルールはさまざまな基準に基づいて設定でき、送信元または宛先IPアドレス、送信元または宛先ポート、パケットで伝送されるプロトコルなど、パケット内の1つ以上のフィールドに適用できます。

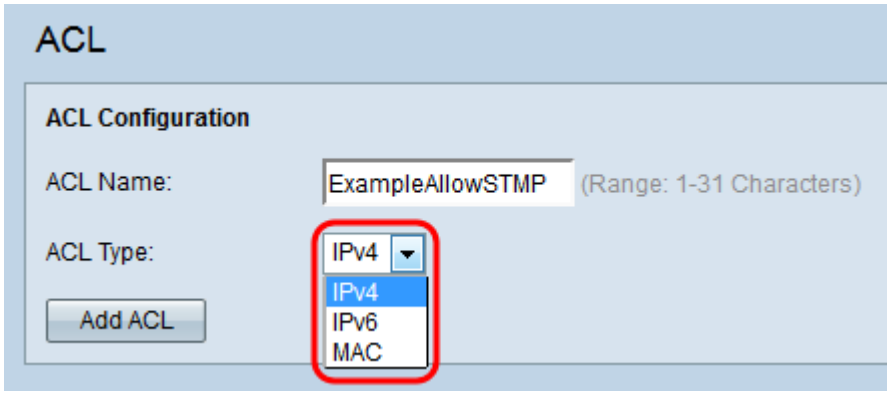
IPv4 ACLの作成

ステップ1：アクセスポイント設定ユーティリティにログインし、**[Client QoS] > [ACL]を選択します。**[*ACL*]*ページ*が開きます。

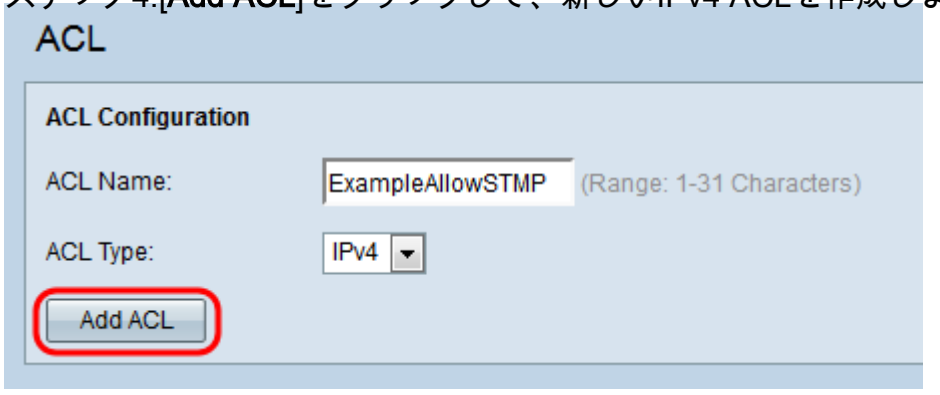


ステップ2:[ACL Name]フィールドにACLの名前を入力します。

ステップ3:[ACL Type]ドロップダウンリストから、ACLのIPv4タイプを選択します。



ステップ4:[Add ACL]をクリックして、新しいIPv4 ACLを作成します。



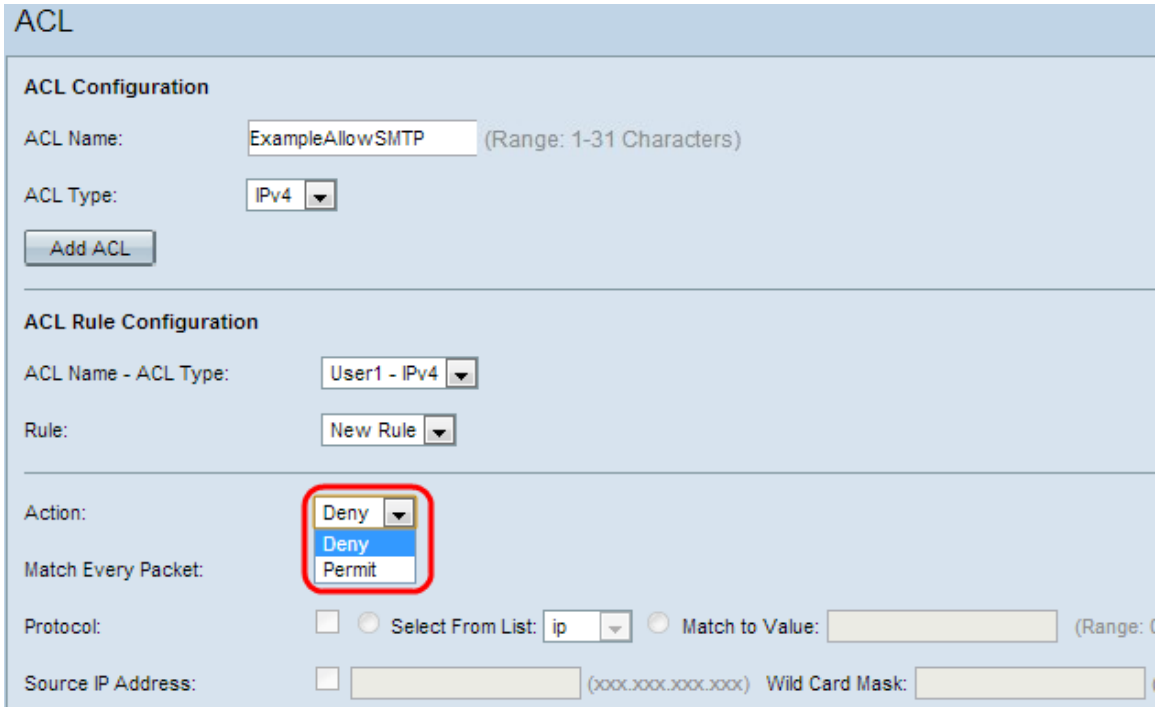
IPv4 ACLのルールの設定

ステップ1:[ACL Name-ACL Type] ドロップダウンリストから、ルールを設定するACLを選択します。

ステップ2：選択したACLに対して新しいルールを設定する必要がある場合は、[Rule]ドロップダウンリストから[*New Rule*]を選択します。それ以外の場合は、「規則」(*Rule*)ドロップダウンリストから*現在の規則*のいずれかを選択します。

注：1つのACLに対して最大10のルールを作成できます。

ステップ3:[Action]ドロップダウンリストからACLルールのアクションを選択します。

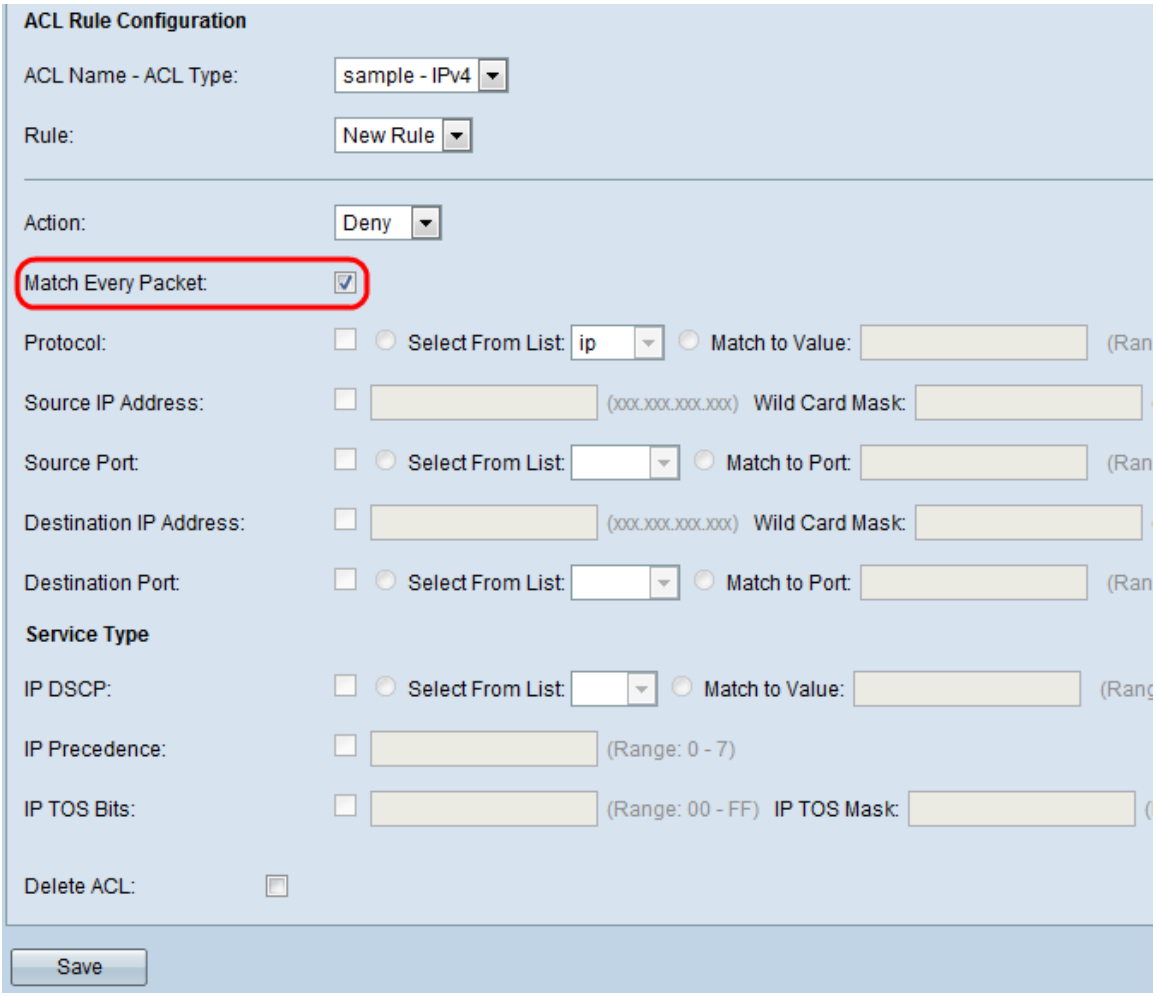


使用可能なオプションは次のとおりです。

・ Deny：ルール基準を満たすすべてのトラフィックをブロックして、WAPデバイスに出入りします。

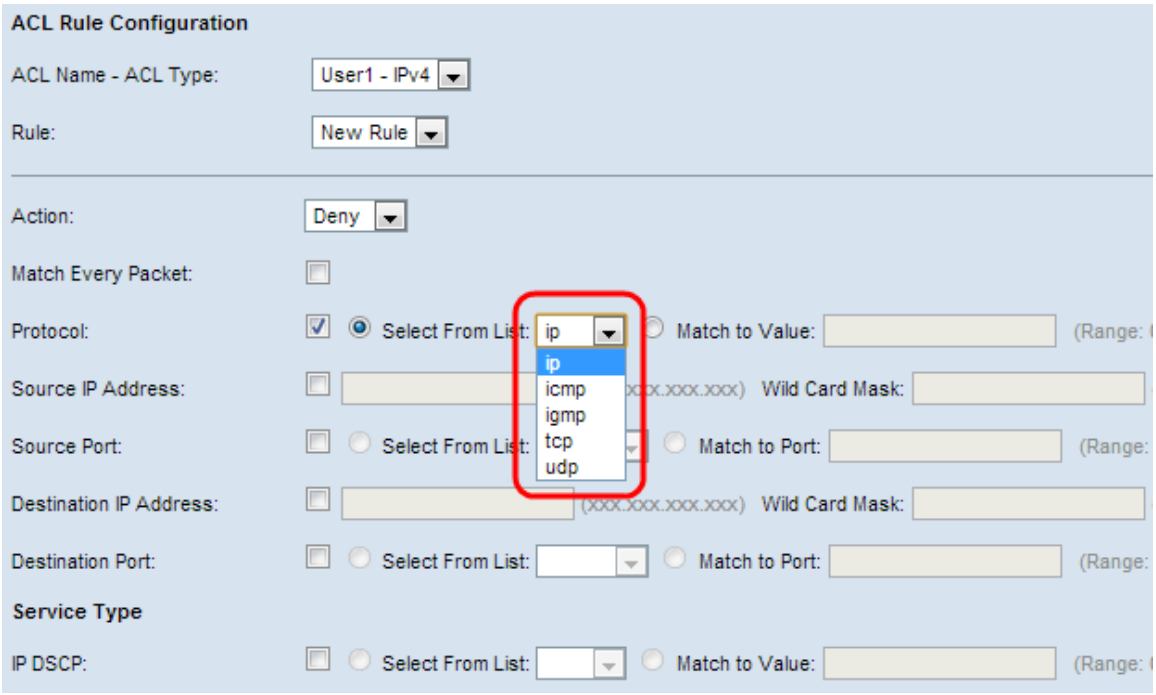
・ Permit：ルール基準を満たすすべてのトラフィックがWAPデバイスに出入りできるようにします。

ステップ4:[Match *Every Packet]チェックボックスをオン*にすると、その内容に関係なく、すべてのフレームまたはパケットのルールに一致します。特定の一致基準を設定する場合は、[Match Every Packet]チェックボックスを*オフ*にします。



タイムサーバ：[Match *Every Packet]チェックボックスをオン*にした場合は、ステップ13に進みます。

ステップ5:（オプション）IPv4パケットのIP Protocolフィールドの値に基づいて、L3またはL4プロトコルの照合条件の*Protocol*チェックボックスをオンにします。[プロトコル]チェックボックスがオンになっている場合は、次のいずれかのオプションボタンをクリックします。

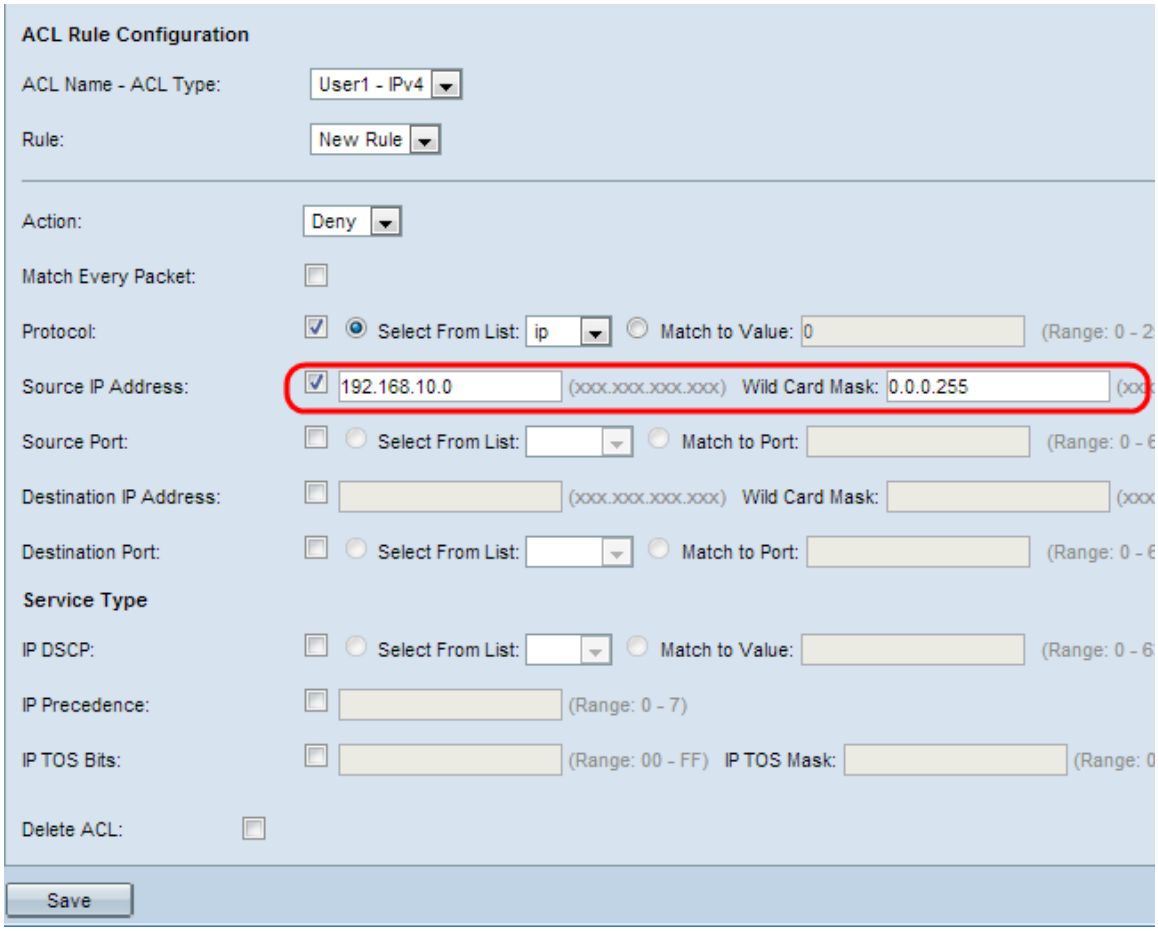


オプションは次のとおりです。

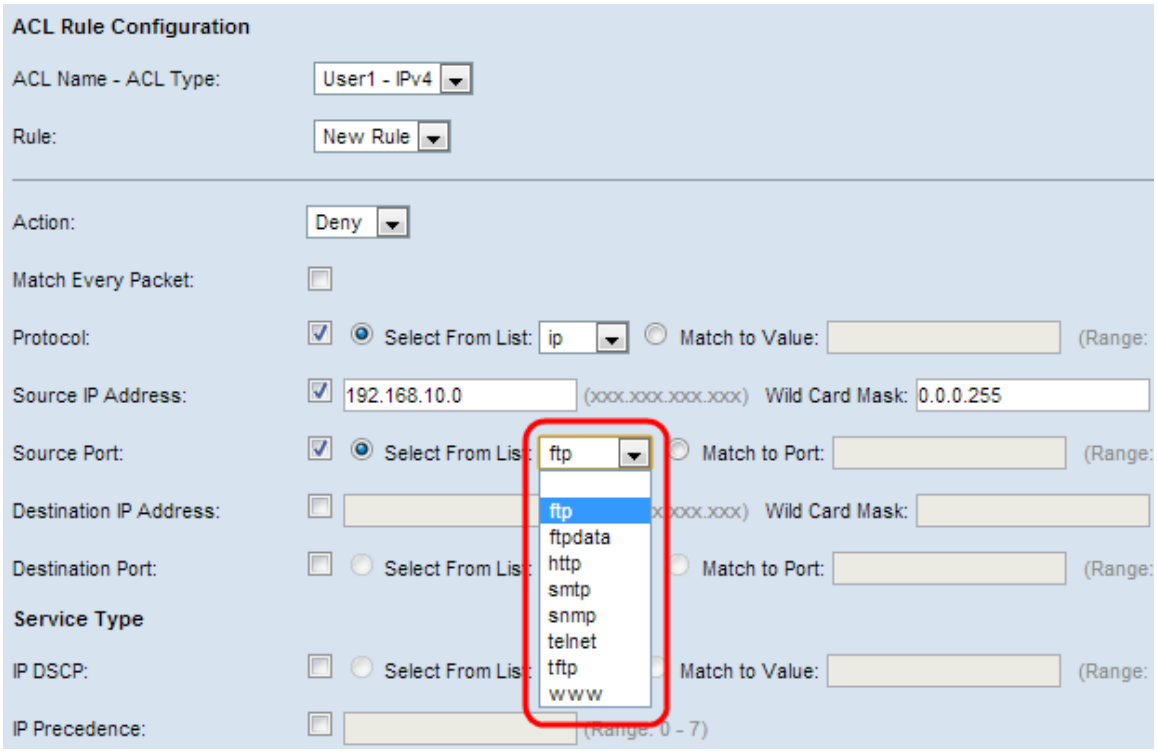
・ [リストから選択]:[リストから選択]ドロップダウンリストからプロトコルを選択します。ドロップダウンリストには、ip、icmp、igmp、tcp、udpプロトコルがあります。

・ Match to Value：プロトコルがリストに表示されない。0 ~ 255の範囲でIANAによって割り当てられる標準プロトコルIDを入力します。

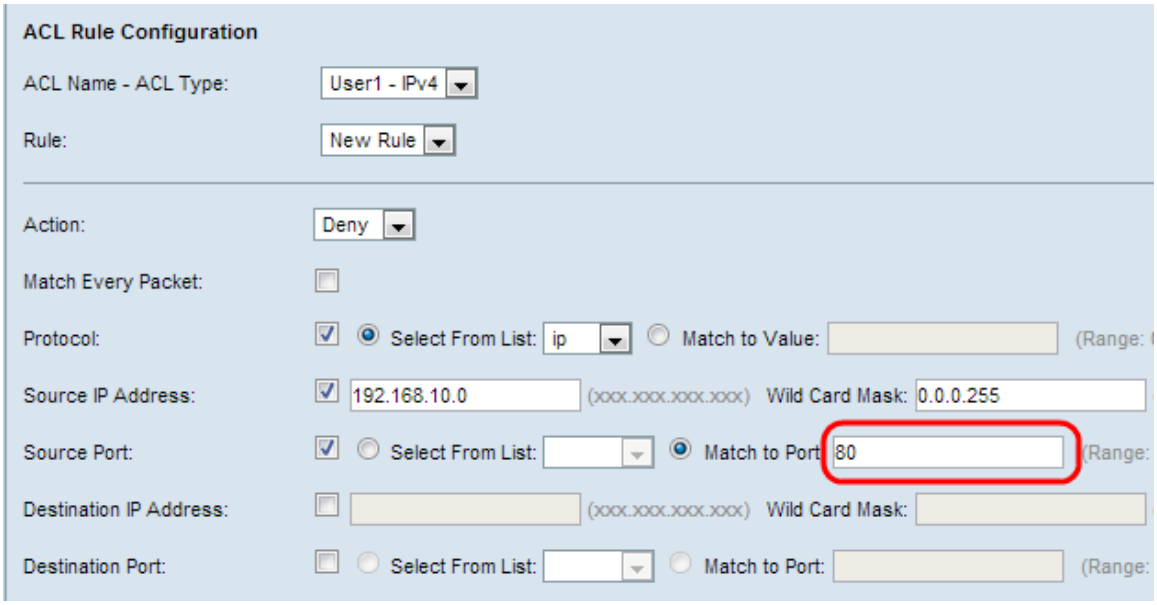
ステップ6: (オプション) [*Source IP Address*]チェックボックスをオンにして、照合条件に送信元のIPアドレスを含めます。各フィールドに送信元のIPアドレスとワイルドカードマスクを入力します。ワイルドカードマスクでは、このアクセスリストを適用する送信元IPアドレスのホストを指定できます。



ステップ7: (オプション) [Source Port]チェックボックスをオフにすると、一致条件に送信元ポートが含まれます。[*Source Port*]チェックボックスがオンになっている場合は、次のいずれかのラジオボタンをクリックします。

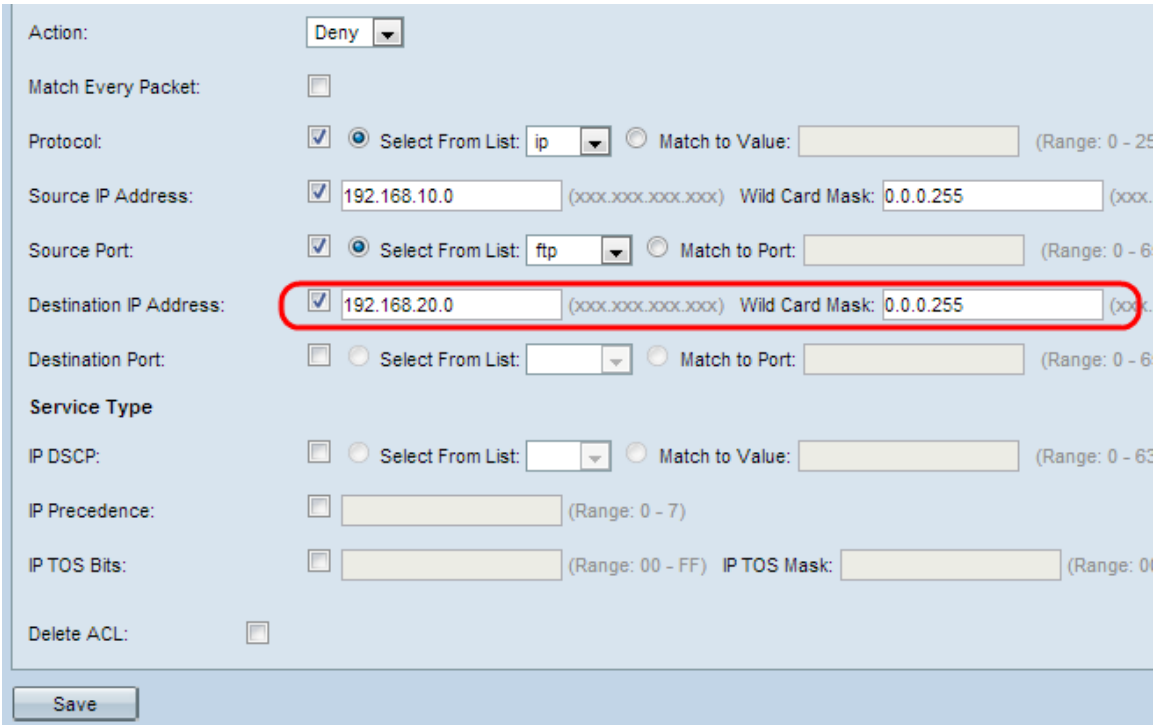


・ [リストから選択(Select From List)]:[リストから選択(*Select From List)]*ドロップダウンリストから送信元ポートを選択します。ドロップダウンリストには、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwの各ポートがあります。

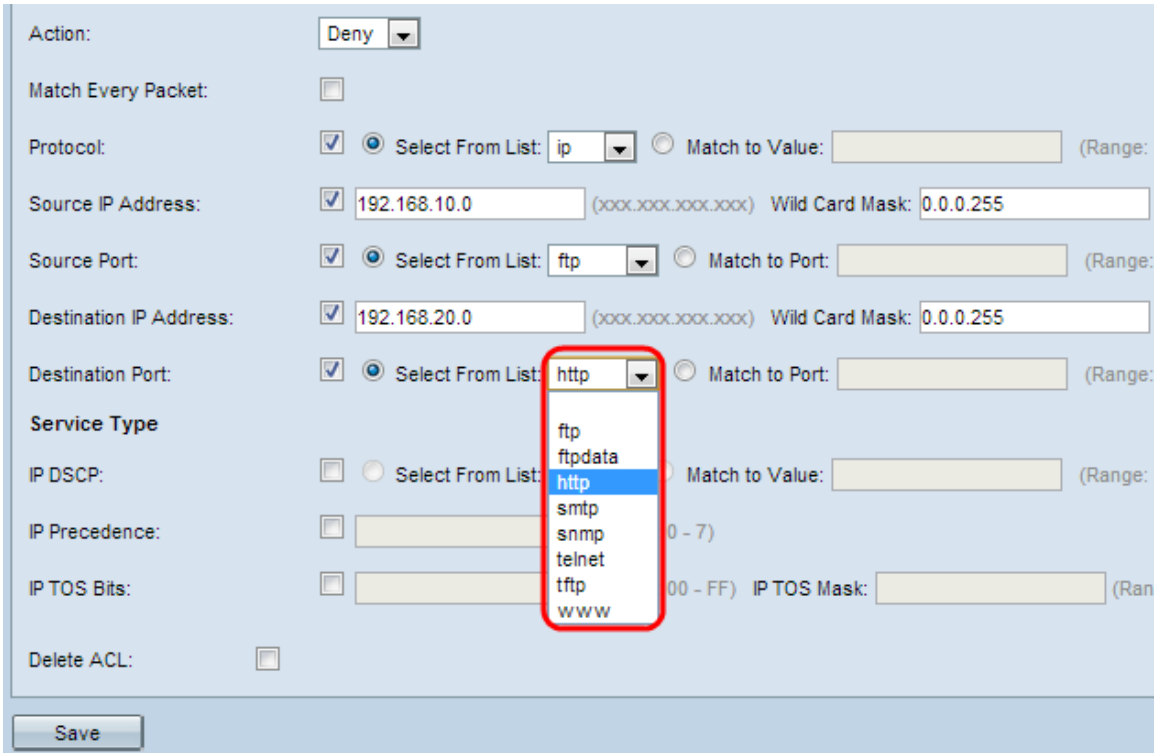


・ Match to Port：リストに表示されていない送信元ポートの場合。0 ~ 65535の範囲のポート番号を入力します。

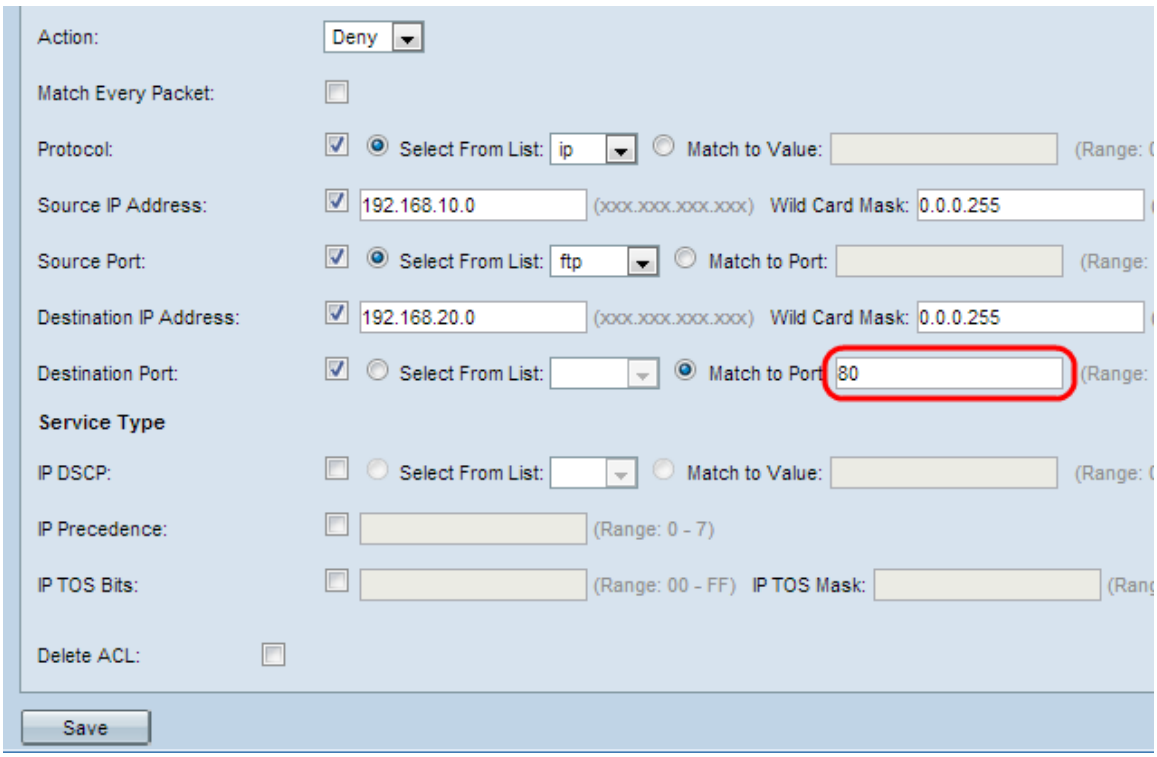
ステップ8:（オプション）[Destination IP Address]チェックボックスをオンにして、照合条件に宛先のIPアドレスを含めます。宛先のIPアドレスとワイルドカードマスクをそれぞれのフィールドに入力します。ワイルドカードマスクでは、このアクセスリストを適用する宛先IPアドレスのホストを指定できます。



ステップ9:（オプション）[宛先ポート(Destination Port)]**チェックボックス**をオンにして、一致する条件に宛先ポートを含めます。[宛先ポート]チェックボックスがオンになっている場合は、これらのオプションボタンのいずれかをクリックします。



・ [リストから選択(Select From List)]:[リストから選択(*Select From List)]*ドロップダウンリストから宛先ポートを選択します。ドロップダウンリストには、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwの各ポートがあります。

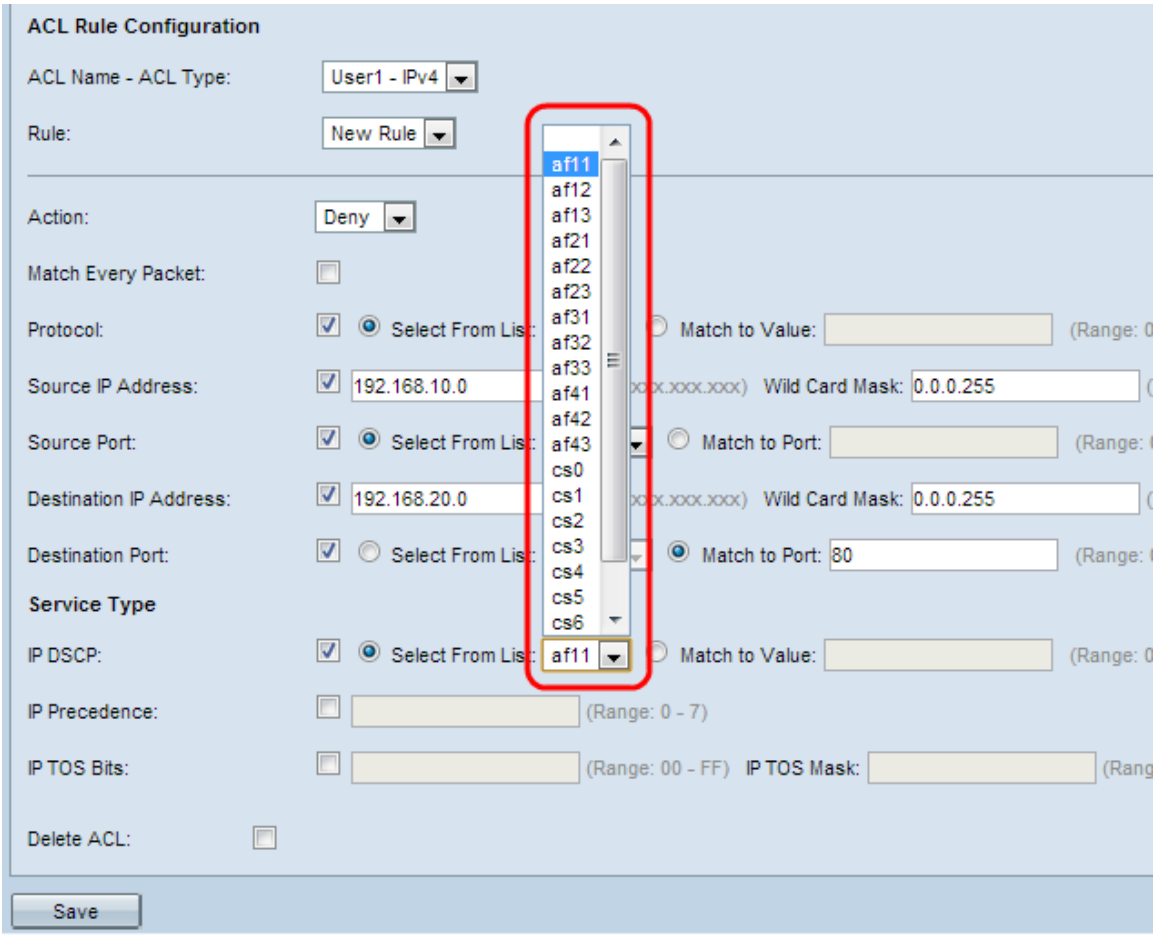


・ Match to Port：リストに表示されていない宛先ポートの場合。[Match to Port]フィールドに0 ～ 65535の範囲のポート番号を入力します。

注：[サービスタイプ(Service Type)]領域から選択できるサービス*は1*つだけで、一致条件に追加できます。

ステップ10:（オプション）IP DSCP値に基づいてパケットを照合するには、[IP DSCP]チェックボックスをオンにします。[IP DSCP]チェックボックスがオンになっている場合は、次のいずれかのオプションボタンをクリックします。DSCPは、フレームのIPヘッダー上で

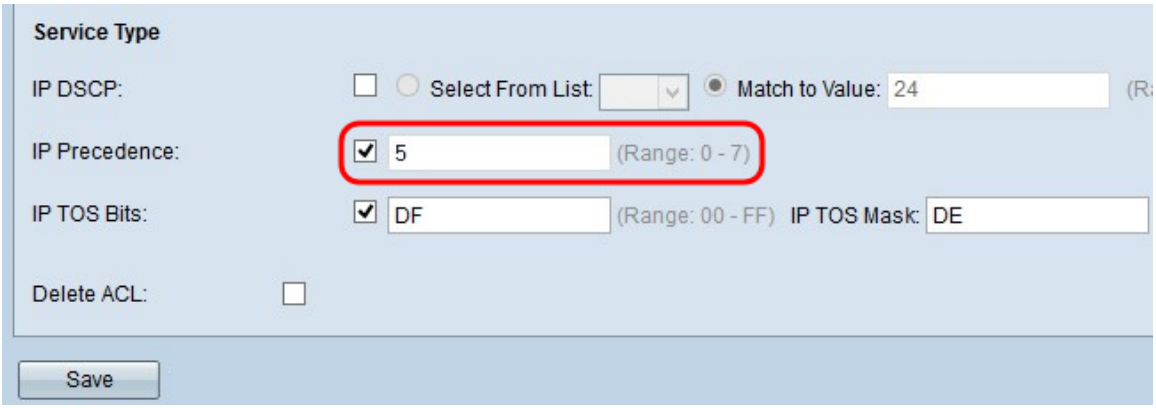
トラフィックの優先順位を指定するために使用されます。これにより、関連付けられたトラフィックストリームのすべてのパケットが、リストから選択したIP DSCP値で分類されます。DSCPの詳細については、こちらを参照してください。



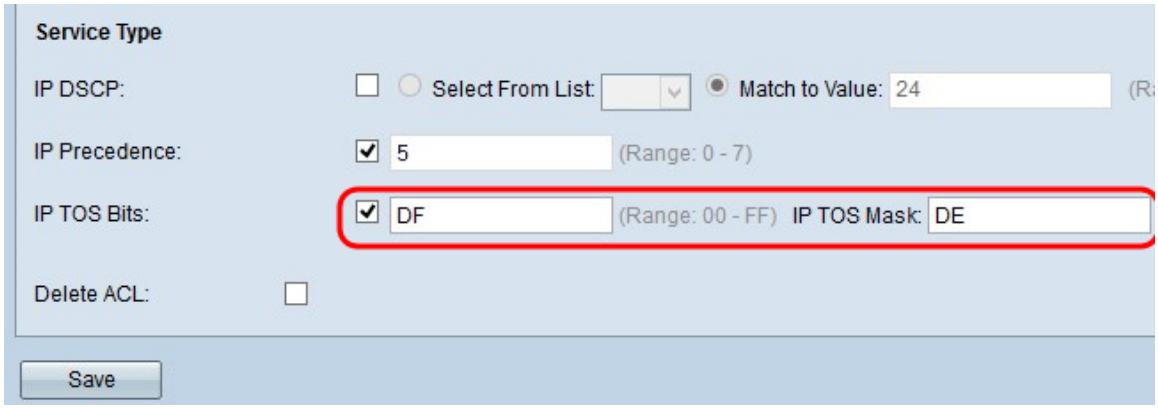
・ [リストから選択(Select From List)]:[リストから選択(*Select From List)]ドロップダウンリストからIP DSCP値を選択します。ドロップダウンリストには、DSCP Assured Forwarding(AS)、Class of Service(CS)、またはExpedited Forwarding(EF)の値があります。

・ Match to Value:DSCP値をカスタマイズします。[Match to Value]フィールドに0 ~ 63の範囲のDSCP値を入力します。

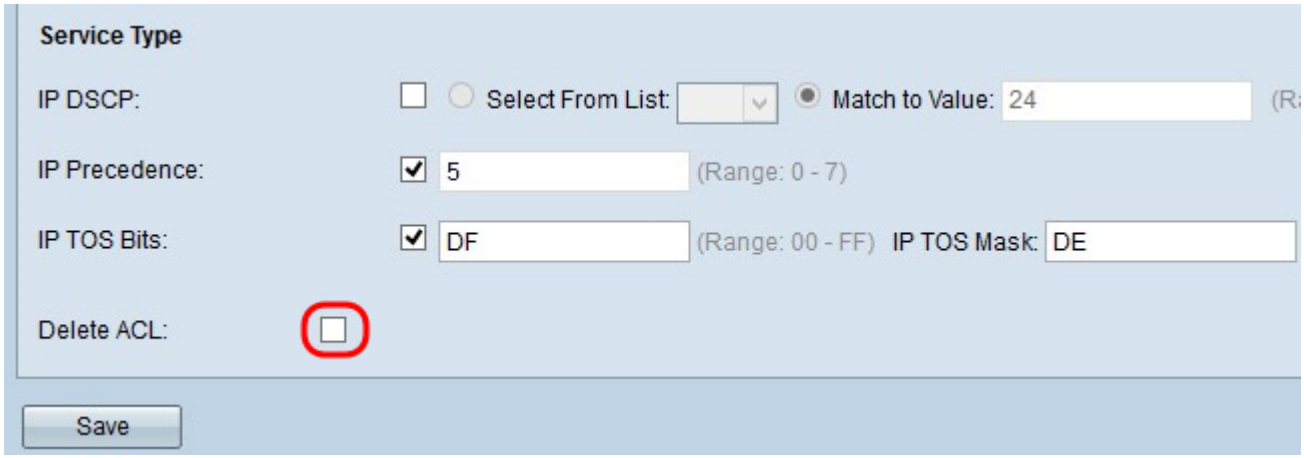
ステップ11: (オプション) [*IP Precedence]チェックボックスをオンにして、一致条件にIP Precedence値を含めます。[IP Precedence]チェックボックスをオンにした場合は、0 ~ 7の範囲のIP precedence値を入力します。IP Precedenceの詳細については、ここを参照してください。



ステップ12:（オプション）IPヘッダーのパケットのタイプオブサービス(Type of Service)ビットを照合基準として使用する場合は、[*IP TOS Bits*]チェックボックスをオンにします。[IP TOS Bits]チェックボックスがオンになっている場合は、00-FFの範囲のIP TOSビットと、00-FFの範囲のIP TOSマスクを各フィールドに入力します。



ステップ13:（オプション）設定済みのACLを削除する場合は、[ACLの削除]チェックボックスをオンにします。



ステップ14:[**Save**]をクリックして、設定を保存します。