Cisco Business Router に関する VLAN のベストプラクティスとセキュリティのヒント

目的

この記事の目的は、Cisco Business 機器で VLAN を設定する際のベストプラクティスとセキュリティのヒントを実行するための概念と手順を説明することです。

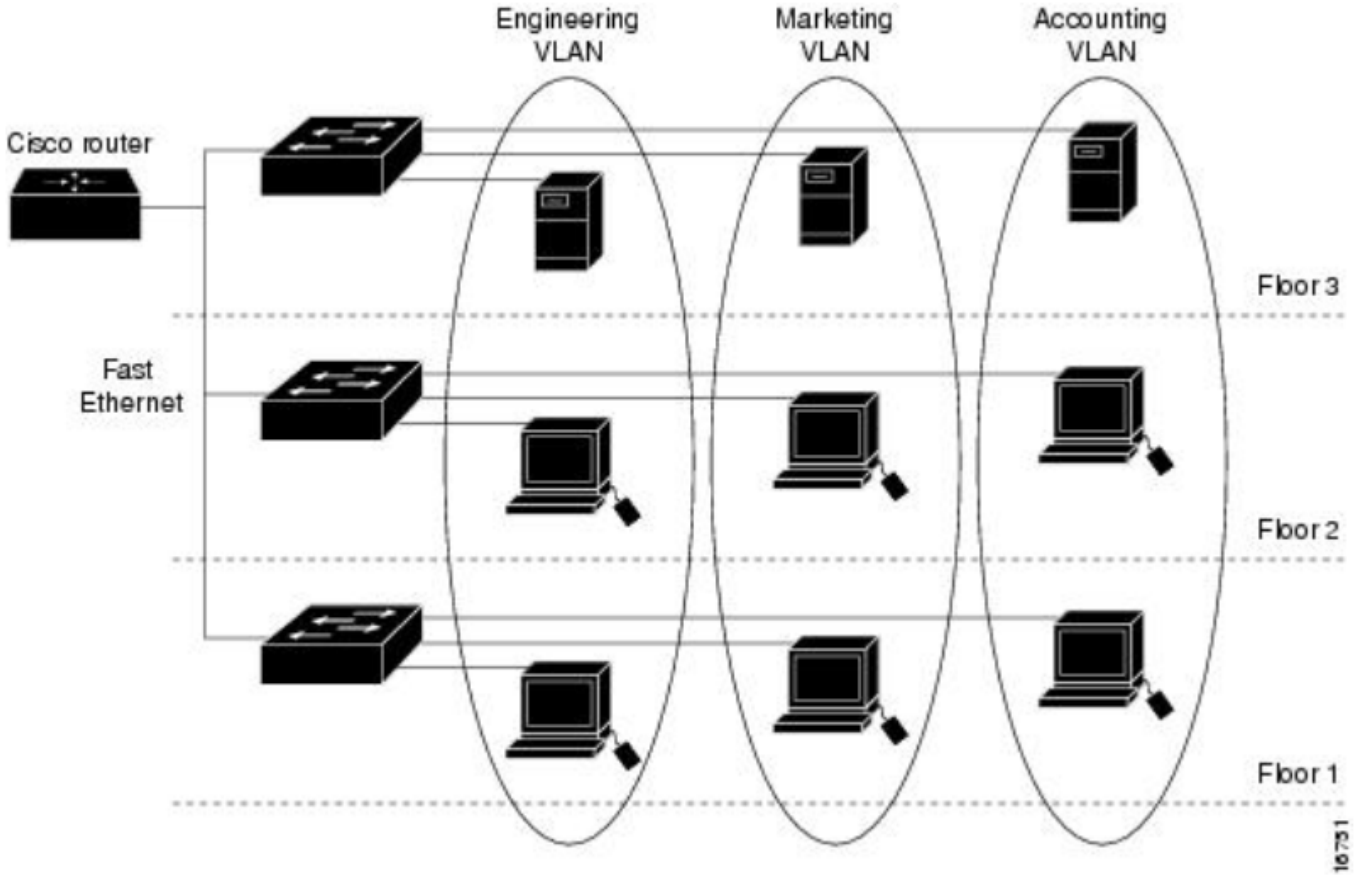
目次

概要

ビジネスネットワークのセキュリティを維持しながら、ネットワークの効率性を高めたいとお考えですか。これを行う方法の1つは、仮想ローカルエリアネットワーク(VLAN)を正しく設定することです。

VLANは、地理的な分散にもかかわらず、同じローカルエリアネットワーク(LAN)上に存在しているように見えるワークステーション、サーバ、およびネットワークデバイスの論理グループです。簡単に言えば、同じVLAN上のハードウェアを使用すると、機器間のトラフィックを分離して安全性を高めることができます。

たとえば、エンジニアリング、マーケティング、および会計部門があるとします。各部門の従業員は建物の異なるフロアにいますが、各部門内の情報にアクセスして通信する必要があります。ドキュメントとWebサービスの共有に不可欠です。



ネットワークを安全に保つには、VLANをベストプラクティスに基づいて設定する必要があります。VLANを設定する際には、次の項目を選択します。後悔はしないぞ！

該当するデバイス

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

RV160またはRV260シリーズルータでは最大16のVLANを伝送でき、RV34xシリーズルータでは最大32のVLANを伝送できることを知りたいと思うかもしれません。RV320は最大7つのVLANをサポートします。ルータが伝送できるVLANの数を知りたい場合は、 シスコWebサイトで使用しているモデルのデータシートを確認してください。[Support] を選択してモデル番号を入力するか、データシートとモデル番号を検索します。

初心者のための簡単な語彙

アクセス ポート:アクセスポートは1つのVLANのトラフィックのみを伝送します。アクセスポートは、タグなしポートと呼ばれることがよくあります。そのポートにはVLANが1つしかなく、トラフィックはタグなしで渡されるからです。

トランクポート：複数のVLANのトラフィックを伝送するスイッチ上のポート。トランクポートは、そのポートに複数のVLANが存在し、1つのVLAN以外のすべてのトラフィックにタグを付ける必要があるため、タグ付きポートと呼ばれることがよくあります。

ネイティブVLAN:タグを受信しないトランクポート内の1つのVLAN。タグのないトラフィックは、ネイティブVLANに送信されます。そのため、トランクの両側で、ネイティブVLANが同じであるか、またはトラフィックが正しい場所に移動しないかを確認する必要があります。

ベストプラクティス#1 - VLANポートの割り当て

ポート割り当ての基本

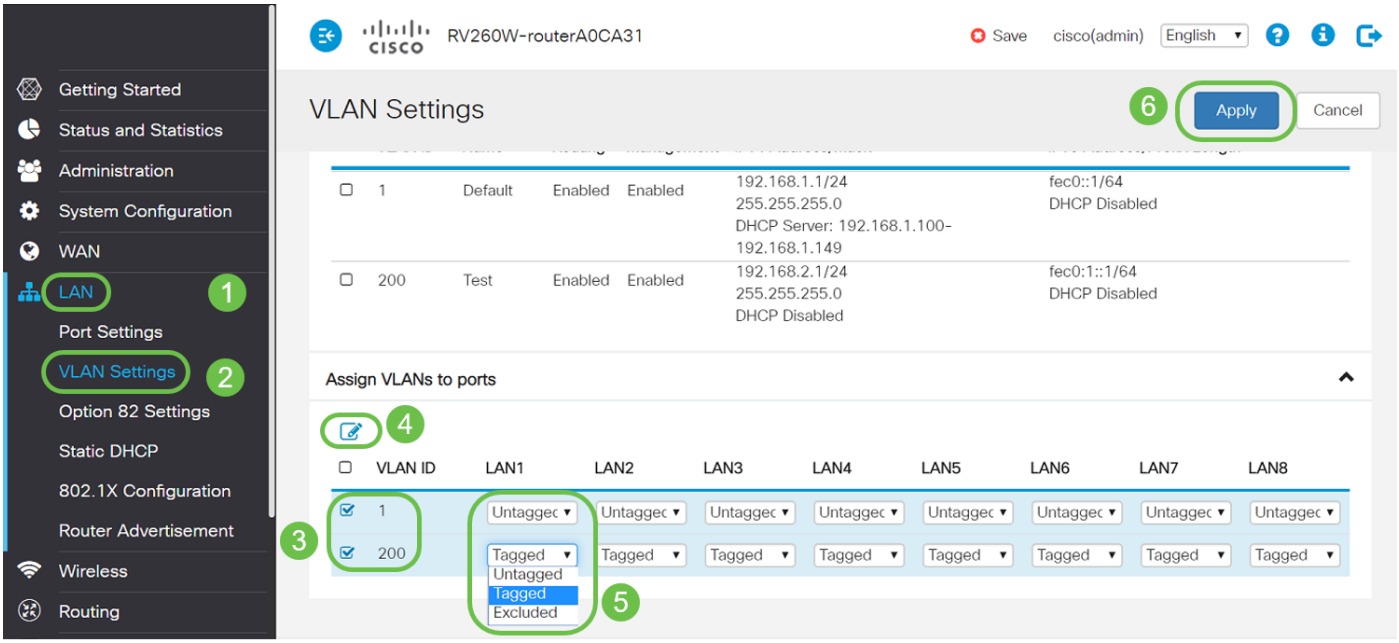
- 各LANポートは、アクセスポートまたはトランクポートとして設定できます。
- トランク上に不要なVLANは除外する必要があります。
- VLANは複数のポートに配置できます。

アクセスポートの設定

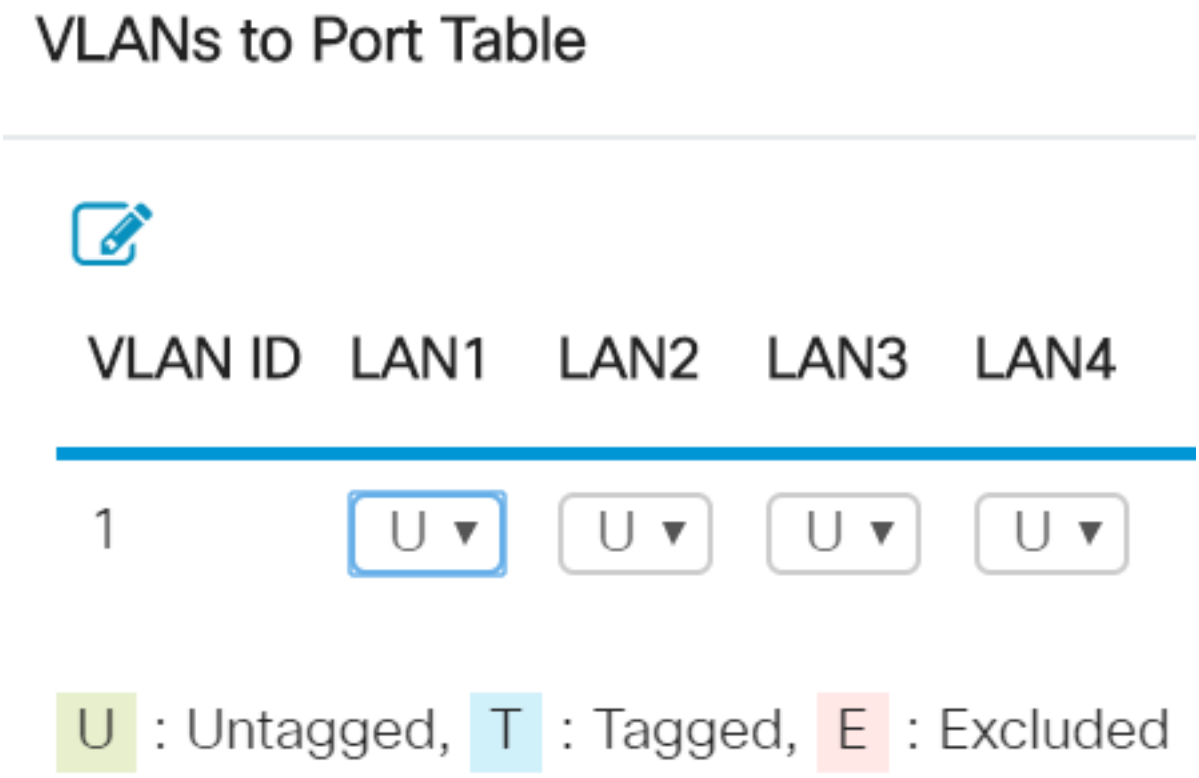
- LANポートに割り当てられた1つのVLAN
- このポートに割り当てられたVLANには、*Untagged*というラベルを付ける必要があります
- その他のすべてのVLANには、そのポートに対して*Excluded*というラベルを付ける必要があります

これらを正しく設定するには、[LAN] > [VLAN Settings] に移動します。*VLAN ID*を選択し、*edit*アイコンを**クリックします**。リストされているVLANのLANインターフェイスのドロップダウンメニューを選択して、VLANタギングを編集します。[Apply] をクリックします。

独自のLANポートを割り当てた各VLANの例を次に示します。



このグラフィカルユーザインターフェイス(GUI)イメージは、RV260Wルータから取得したものです。オプションは若干異なることがあります。たとえば、RV34xシリーズでは、ラベル *Untagged*、 *Excluded*、および *Tagged*は最初の文字のみに短縮されます。プロセスは同じです。

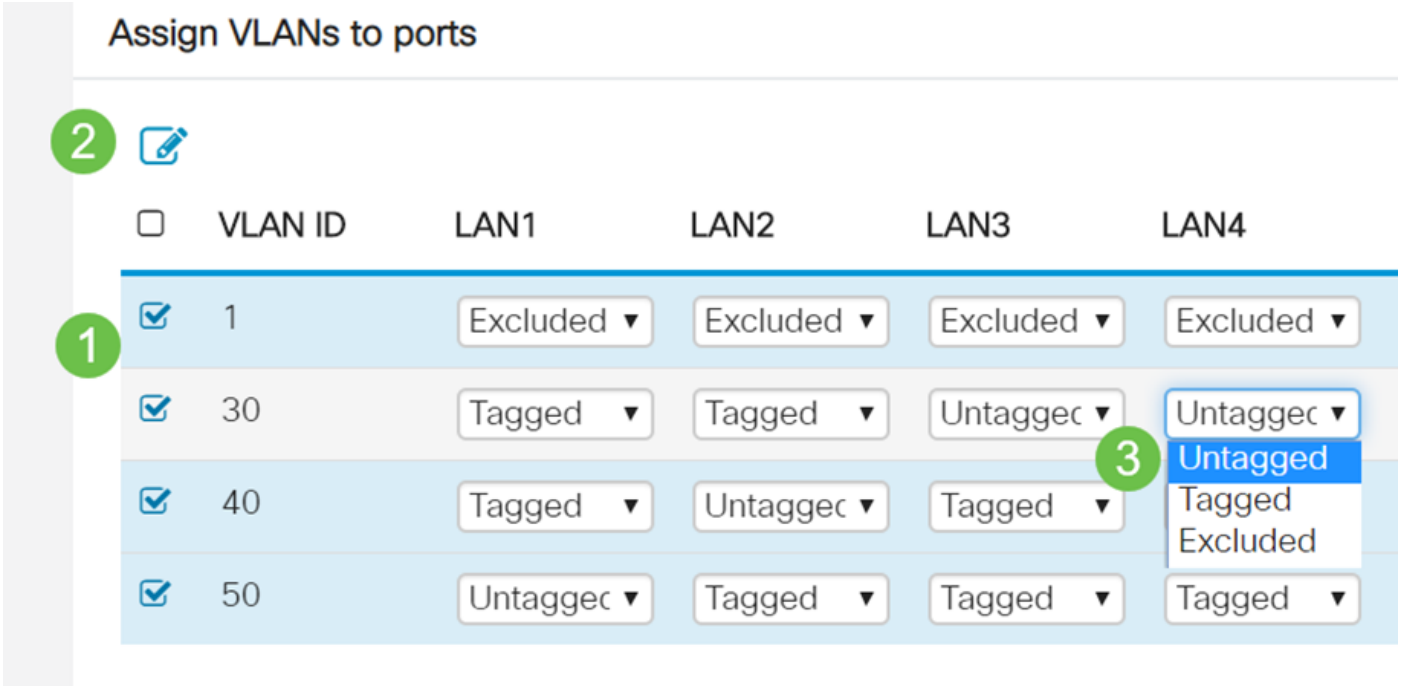


トランクポートの設定

- 2つ以上のVLANが1つのLANポートを共有
- VLANの1つに*Untagged*というラベルを付けることができます。
- トランクポートの一部である残りのVLANには、*Tagged*というラベルを付ける必要があります。
- トランクポートの一部ではないVLANには、そのポートに対して*Excluded*というラベルを付ける必要があります。

次に、すべてのVLANがトランクポート上にある例を示します。これらを正しく設定するには、編集する必要がある*VLAN ID*を選択します。*edit*アイコンをクリックします。上記の推奨事項に従

って、必要に応じて変更します。ところで、VLAN 1がすべてのLANポートから除外されていることに気づきましたか。これについては、「デフォルトVLAN 1のベストプラクティス」セクションで説明します。



よく寄せられる質問（FAQ）

VLANがそのポート上の唯一のVLANなのに、VLANがタグなしのままなのはなぜですか。

アクセスポートにはVLANが1つだけ割り当てられているため、ポートからの発信トラフィックはフレーム上にVLANタグなしで送信されます。フレームがスイッチポート（着信トラフィック）に到達すると、スイッチはVLANタグを追加します。

VLANがトランクの一部である場合、VLANにタグが付けられるのはなぜですか。

これは、通過するトラフィックがそのポートの誤ったVLANに送信されないようにするためです。VLANはそのポートを共有しています。住所に追加された部屋番号と同様に、メールがその共有建物内の正しいアパートに届くようにします。

トラフィックがネイティブVLANの一部である場合にタグ付けされないままになるのはなぜですか。

ネイティブVLANは、タグ付けされていないトラフィックを1つ以上のスイッチで伝送する方法です。スイッチは、タグ付きポートに着信するタグなしフレームをネイティブVLANに割り当てます。ネイティブVLAN上のフレームがトランク（タグ付き）ポートを離れると、スイッチはVLANタグを取り除きます。

VLANがそのポート上にない場合、VLANが除外されるのはなぜですか。

これにより、ユーザが特に必要とするVLANに対してのみ、そのトランク上のトラフィックが保持されます。これはベストプラクティスと見なされます。

ベストプラクティス#2 – デフォルトVLAN 1および未使用ポート

すべてのポートは、ネイティブVLANを含む1つ以上のVLANに割り当てる必要があります。Cisco Businessルータには、デフォルトですべてのポートにVLAN 1が割り当てられています。

管理VLANは、Telnet、SSH、SNMP、syslog、またはシスコのFindITを使用して、ネットワーク内のデバイスをリモートで管理、制御、監視するために使用されるVLANです。デフォルトでは、これもVLAN 1です。優れたセキュリティ対策は、管理トラフィックとユーザデータトラフィックを分離することです。したがって、VLANを設定する場合は、VLAN 1を管理目的でのみ使用することを推奨します。

管理目的でCiscoスイッチとリモート通信するには、スイッチに管理VLANで設定されたIPアドレスが必要です。他のVLAN内のユーザは、管理VLANにルーティングされない限り、スイッチへのリモートアクセスセッションを確立できず、セキュリティの追加レイヤが提供されます。また、スイッチは、リモート管理のために暗号化されたSSHセッションのみを受け入れるように設定する必要があります。このトピックに関するディスカッションを読むには、シスココミュニティWebサイトの次のリンクをクリックしてください。

- 管理VLANの説明#1
- 管理VLANの説明#2

よく寄せられる質問（FAQ）

ネットワークを仮想的にセグメント化するためにデフォルトのVLAN 1が推奨されないのはなぜですか。

主な理由は、敵対者がVLAN 1がデフォルトであり、頻繁に使用されることを知っているためです。VLANホッピングを使用して他のVLANにアクセスできます。名前が示すように、敵対的な攻撃者は、VLAN 1を装ったスプーフィングされたトラフィックを送信し、トランクポートへのアクセスを可能にして、他のVLANへのアクセスを可能にします。

未使用のポートをデフォルトのVLAN 1に割り当てておくことはできますか。

ネットワークを安全に保つには、そうすべきではありません。これらのポートはすべて、デフォルトのVLAN 1以外のVLANに関連付けるように設定することをお勧めします。

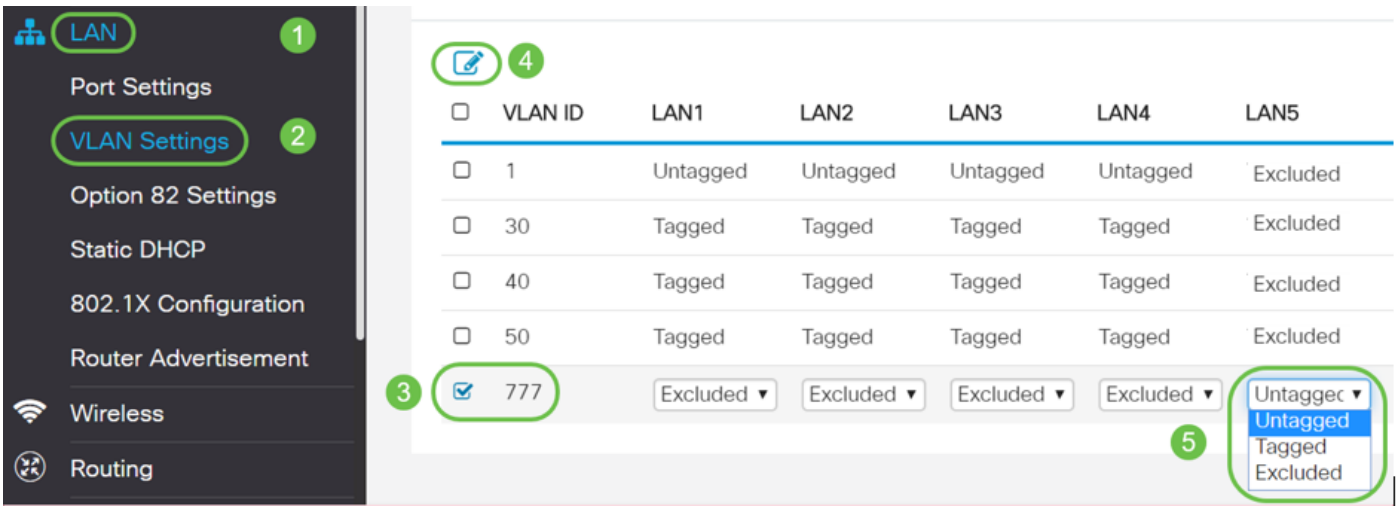
未使用のポートに実稼働VLANを割り当てたくありません。どうすればよいですか。

この記事の次のセクションの手順に従って、「デッドエンド」VLANを作成することをお勧めします。

ベストプラクティス#3 – 未使用ポート用の「デッドエンド」VLANを作成する

ステップ1:[LAN] > [VLAN Settings] に移動します。

VLANの任意の乱数を選択します。このVLANでDHCP、VLAN間ルーティング、またはデバイス管理が有効になっていないことを確認してください。これにより、他のVLANの安全性が高まります。未使用のLANポートをこのVLANに配置します。次の例では、*VLAN 777*が作成され、*LAN5*に割り当てられています。これは、すべての未使用LANポートで実行する必要があります。



他のVLANがこのLANポートから除外されていることに注意してください。
ステップ2:[Apply] ボタンをクリックして、設定の変更を保存します。

ベストプラクティス#4 - VLAN上のIPフォン

音声トラフィックには、厳格なQuality of Service(QoS)要件があります。同じVLAN上にコンピュータとIP電話が存在する企業では、それぞれが他のデバイスを考慮することなく使用可能な帯域幅を使用しようとします。この競合を回避するには、IPテレフォニー音声トラフィックとデータトラフィックに別々のVLANを使用することを推奨します。この設定の詳細については、次の記事とビデオをご覧ください。

- Cisco Tech Talk:Cisco Small Business製品を使用した音声VLANの設定と設定（ビデオ）
- SG500シリーズスイッチでのQoSを使用した自動音声VLANの設定
- 200/300シリーズマネージドスイッチでの音声VLANの設定
- Cisco Tech Talk:SG350およびSG550シリーズスイッチでの自動音声VLANの設定（ビデオ）

ベストプラクティス#5:VLAN間ルーティング

トラフィックを分離できるようにVLANが設定されていますが、VLANが相互にルーティングできるようにする必要がある場合があります。これはVLAN間ルーティングであり、通常は推奨されません。これが会社にとって必要な場合は、できるだけ安全に設定してください。VLAN間ルーティングを使用する場合は、アクセスコントロールリスト(ACL)を使用して、機密情報を含むサーバへのトラフィックを制限してください。

ACLはパケットフィルタリングを実行して、ネットワークを通過するパケットの移動を制御します。パケットフィルタリングは、ネットワークへのトラフィックのアクセスを制限し、ネットワークへのユーザとデバイスのアクセスを制限し、トラフィックがネットワークから出ないようにすることで、セキュリティを提供します。IPアクセスリストは、スプーフィングとサービス拒否攻撃の可能性を低減し、ファイアウォールを介した動的な一時的ユーザアクセスを可能にします。

- ターゲットACL制限のあるRV34xルータでのVLAN間ルーティング
- Cisco Tech Talk:SG250シリーズスイッチでのVLAN間ルーティングの設定（ビデオ）
- Cisco Tech Talk:RV180およびRV180Wでの VLAN間設定（ビデオ）
- RV34x VLAN間アクセス制限(CSCvo92300バグ修正)

結論

これで、安全なVLANを設定するためのベストプラクティスがわかります。ネットワークにVLANを設定する際には、次のヒントに留意してください。以下に、手順を追った説明を含む記事をいくつか示します。これにより、ビジネスに最適な、生産性と効率性に優れたネットワークへと移行できます。

- RV160およびRV260でのVLAN設定
- RV34xシリーズルータでの仮想ローカルエリアネットワーク(VLAN)の設定
- RV320およびRV325 VPNルータでのVLANメンバーシップの設定
- RVシリーズルータでの仮想ローカルエリアネットワーク(VLAN)メンバーシップの設定
- CLIによるSx350またはSG350Xスイッチでの VLANインターフェイスIPv4アドレスの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。