ターゲットACL制限を使用したRV34xルータでのVLAN間ルーティング

目的

この記事では、特定のトラフィックを制限するために、対象のアクセスコントロールリスト(ACL)を使用するRV34xシリーズルータでInter-Virtual Local Area Network(VLAN)ルーティングを設定する方法について説明します。トラフィックは、IPアドレス、アドレスグループ、またはプロトコルタイプによって制限できます。

概要

VLANは優れており、レイヤ2ネットワークでブロードキャストドメインを定義します。ルータはブロードキャストフレームを転送しないため、ブロードキャストドメインは通常、ルータによって制限されます。レイヤ2スイッチは、スイッチの設定に基づいてブロードキャストドメインを作成します。トラフィックは、スイッチ内の別のVLAN（ブロードキャストドメイン間）または2つのスイッチ間を直接通過できません。VLANを使用すると、異なる部門を相互に独立させることができます。たとえば、営業部門が会計部門に関与しないようにすることができます。

独立は素晴らしいことですが、VLAN内のエンドユーザが相互にルーティングできるようにしたい場合はどうすればいいですか。営業部門は、会計部門にレコードまたはタイムシートを提出する必要がある場合があります。経理部門は、自分の給与または営業番号に関する通知を営業チームに送信する場合があります。VLAN間ルーティングによって一日を節約できます。

VLAN間通信には、Open Systems Interconnections(OSI)レイヤ3デバイス（通常はルータ）が必要です。このレイヤ3デバイスは、各VLANインターフェイスにインターネットプロトコル(IP)アドレスを持ち、それらの各IPサブネットへの接続ルートを持っている必要があります。各IPサブネットのホストは、それぞれのVLANインターフェイスのIPアドレスをデフォルトゲートウェイとして使用するように設定できます。設定が完了すると、エンドユーザは他のVLANのエンドユーザにメッセージを送信できます。完璧に聞こえるだろ？

ではアカウンティングのサーバはどうでしょうか？そのサーバには、保護を維持する必要がある機密情報があります。心配するな、解決策もある！RV34xシリーズルータのアクセスルールまたはポリシーを使用すると、ルールを設定してネットワークのセキュリティを強化できます。ACLは、特定のユーザとの間で送受信されるトラフィックをブロックまたは許可するリストです。アクセスルールは、常に有効になるように、または定義されたスケジュールに基づいて設定できます。

この記事では、2番目のVLAN、VLAN間ルーティング、およびACLを設定する手順について説明します。

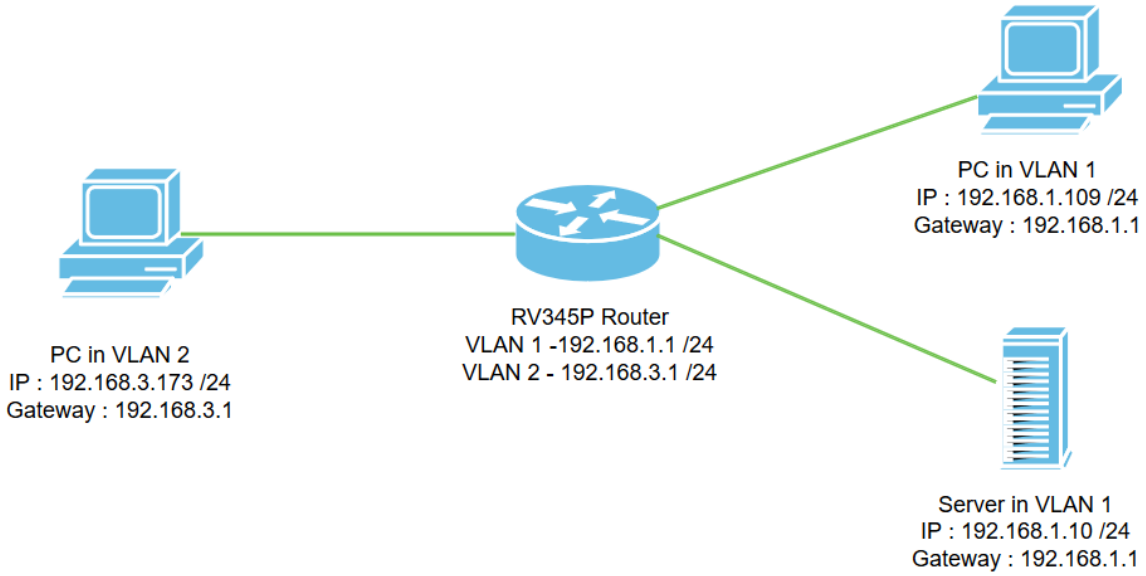
該当するデバイス

- RV340
- RV340W
- RV345
- RV345P

[Software Version]

- 1.0.03.16

トポロジ



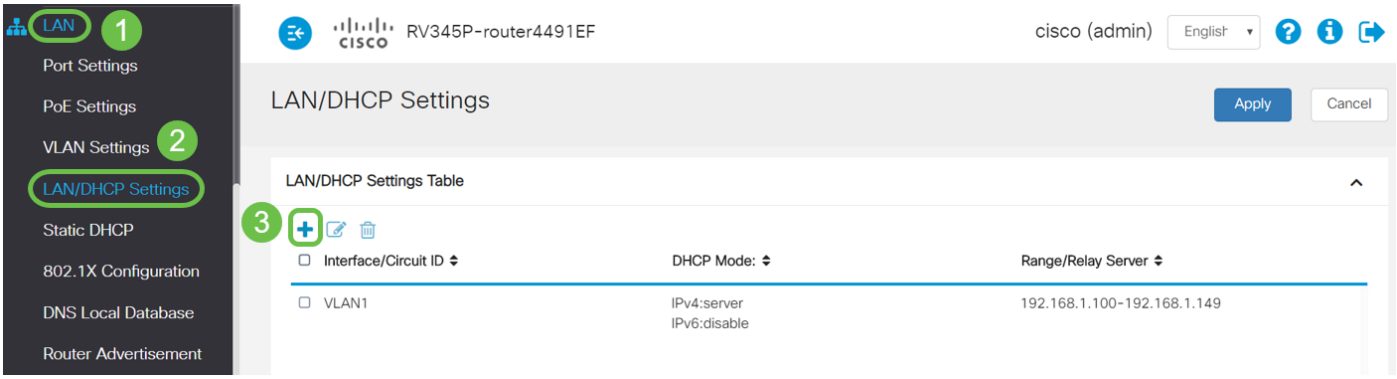
このシナリオでは、VLAN1とVLAN2の両方でVLAN間ルーティングを有効にして、これらのVLANのユーザが相互に通信できるようにします。セキュリティ対策として、VLAN2ユーザがVLAN1サーバ[インターネットプロトコルバージョン4(IPv4):192.168.1.10 /24]。

使用されるルータポート：

- VLAN1のパーソナルコンピュータ(PC)が*LAN*1ポートに接続されています。
- VLAN2のパーソナルコンピュータ(PC)は*LAN*2ポートに接続されます。
- VLAN1のサーバは*LAN*3ポートに接続されています。

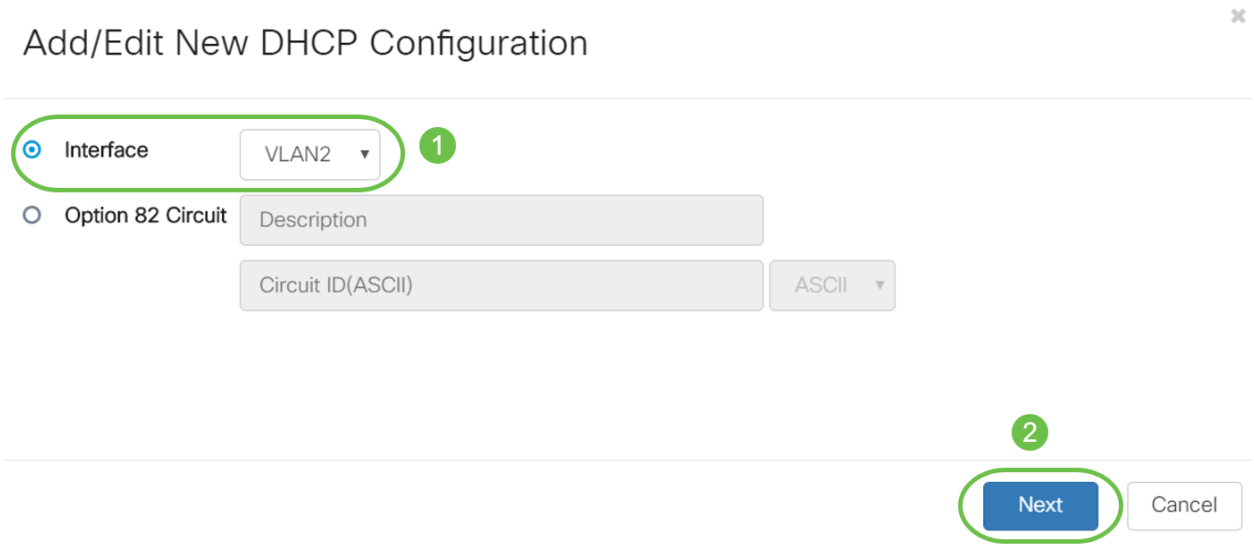
コンフィギュレーション

ステップ1：ルータのWeb設定ユーティリティにログインします。ルータに新しいVLANインターフェイスを追加するには、**[LAN] > [LAN/DHCP Settings]に移動**し、[*LAN/DHCP Settings Table*]の下にあるプラス**アイコンをクリックします。**

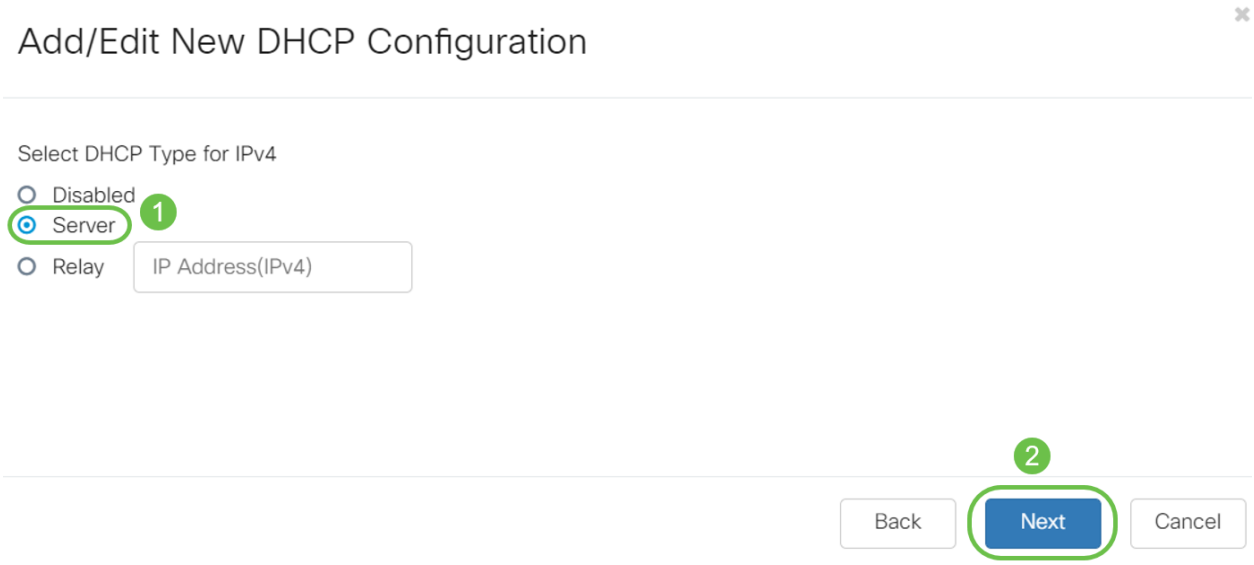


注：VLAN1インターフェイスはデフォルトでRV34xルータに作成され、IPv4用のDynamic Host Configuration Protocol(DHCP)サーバが有効になります。

ステップ2：新しいポップアップウィンドウが開き、[*VLAN2 Interface]が選択され、*[Next]をクリックします。



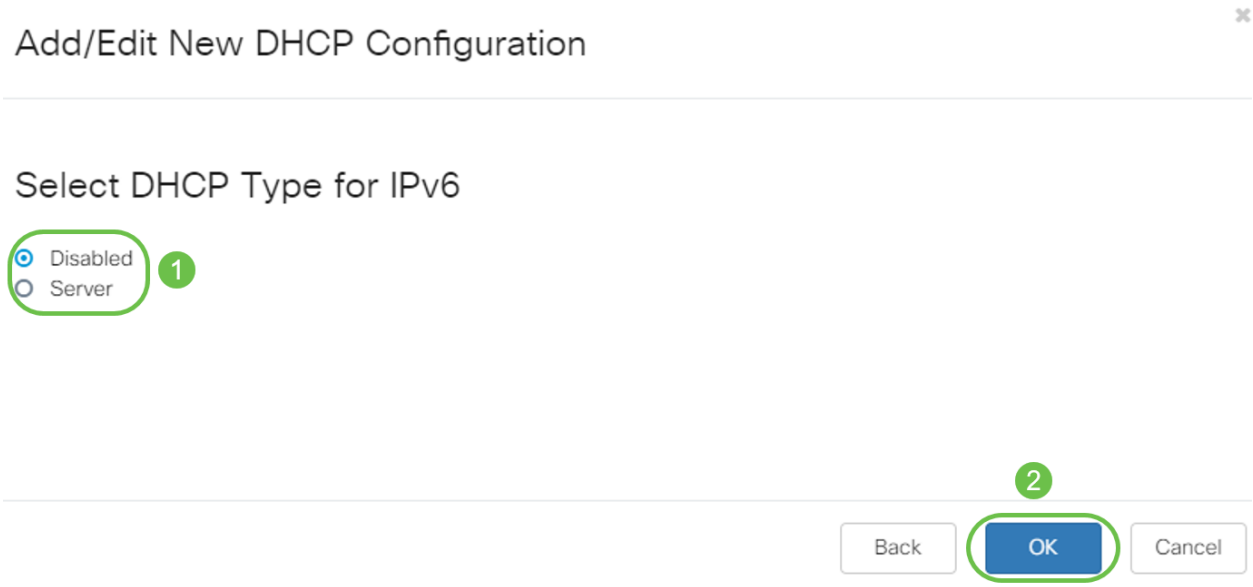
ステップ3:VLAN2インターフェイスでDHCPサーバを有効にするには、[*Select DHCP Type for IPv4]で[***Server**]を選択**します**。[next] をクリックします。



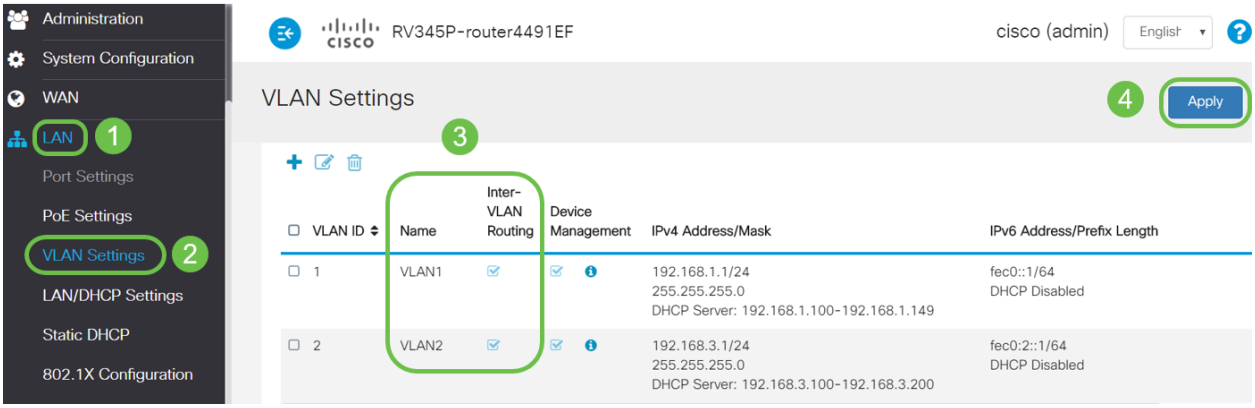
ステップ4：クライアントのリース時間、範囲の開始、範囲の終了、*およびDNSサーバーを含むDHCPサーバーの構成*パラメータを*入力します*。[next] をクリックします。

ステップ5:（オプション）この例ではIPv4に基づいて、[Disabled]チェックボックスをオンにして、**IPv6のDHCPタイプを無効にできます。**[OK]をクリックします。DHCPサーバの設定が完了しました。

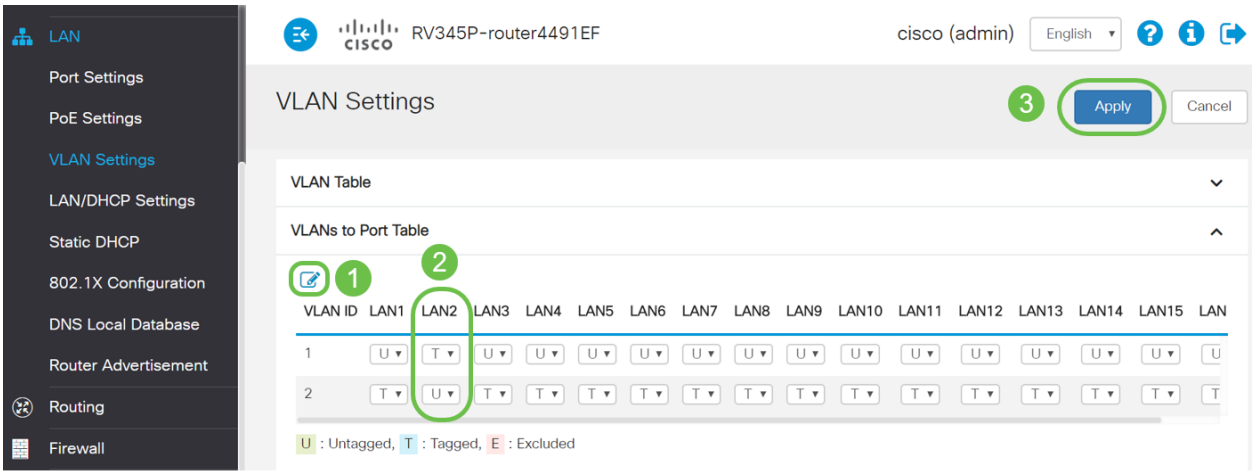
注：IPv6を使用できます。



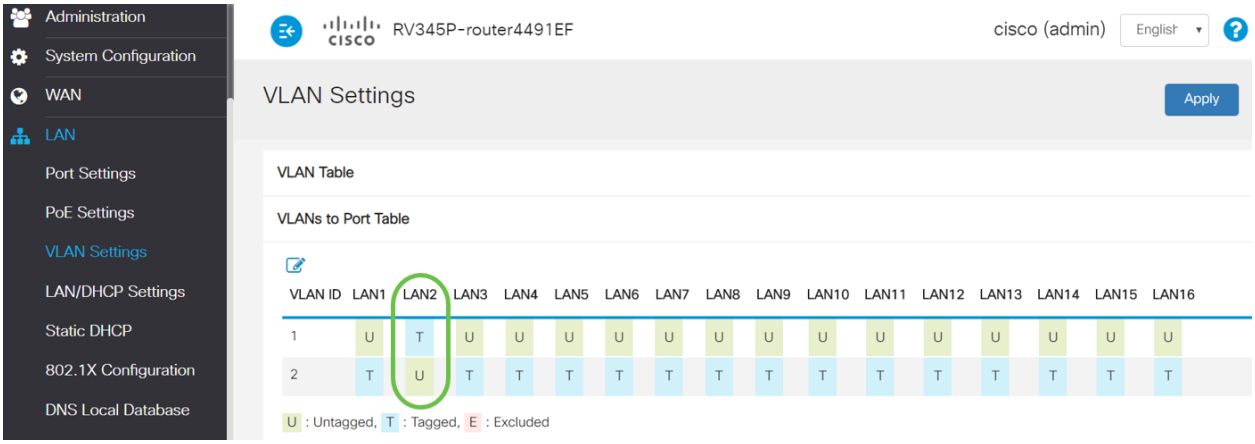
ステップ6:[LAN] > [VLAN Settings] に移動し、VLAN1とVLAN2の両方で*VLAN間ルーティングが有効になっていることを確認します。この設定により、両方のVLAN間の通信が有効になります*。[Apply] をクリックします。



ステップ7:*LAN2*ポート上のVLAN2にタグなしトラフィックを割り当てるには、*[VLANs to Port Table]オプションの下の編集ボタンをクリックします。ここで、LAN2ポートの下で、ドロップダウン・メニューから*VLAN1のT（タグ付き）オプションとVLAN2のU（タグなし）オプションを選択します。[Apply]をクリックし、設定を保存します。この設定では、LAN2ポートのVLAN2のタグなしトラフィックを転送するため、通常はVLANタギングが可能ではないPCネットワークインターフェイスカード(NIC)はVLAN2からDHCP IPを取得し、VLAN2の一部になります。

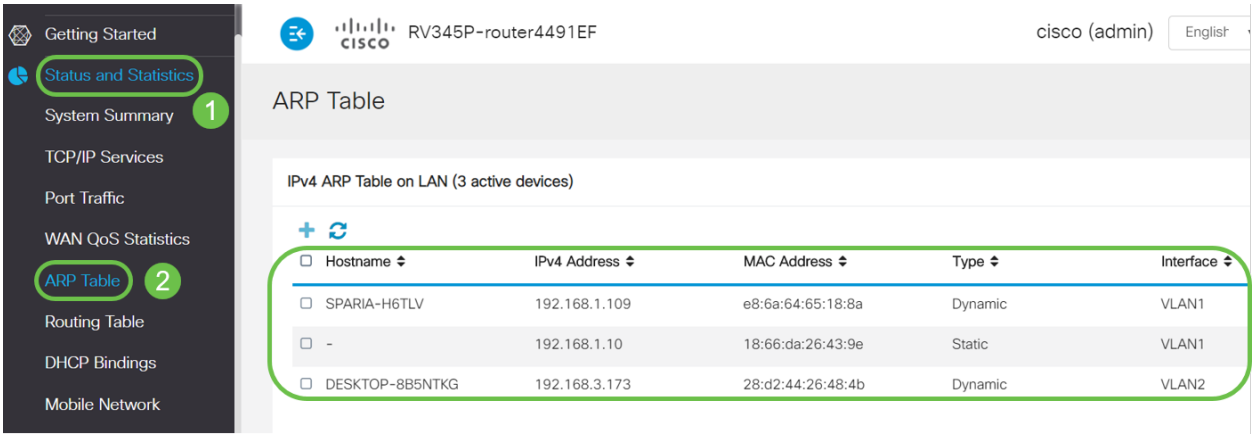


ステップ8:*LAN2*ポートのVLAN2設定が*U(タグなし)と表示されていることを確認します。*残りのLANポートでは、VLAN2の設定は*T（タグ付き）*になり、VLAN1トラフィックは*U（タグなし）*になります。*

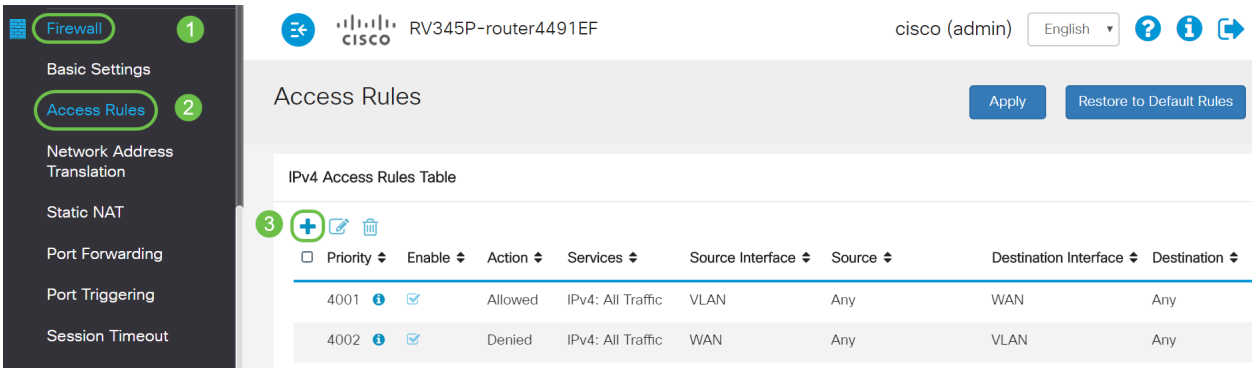


ステップ9:[Status and **Statistics] > [ARP Table]に移動**し、PCのダイナミック*IPv4*アドレスが異なるVLANにあることを確認します。

注：VLAN1のサーバIPは静的に割り当てられています。



ステップ10:ACLを適用してサーバを制限する(IPv4:192.168.1.10/24)にアクセスします。ACLを設定するには、[ファイアウォール] **> [アクセスルール]に移動**し、プラス記号のアイコン**をクリック**して新しいルールを追加します。



ステップ11：アクセスルールのパラメータを設定します。このシナリオでは、パラメータは次のようになります。

ルールステータス：Enable

Action:拒否

サービス：all traffic

ログ:正しい

送信元インターフェイス:VLAN2

発信元アドレス：[Any]

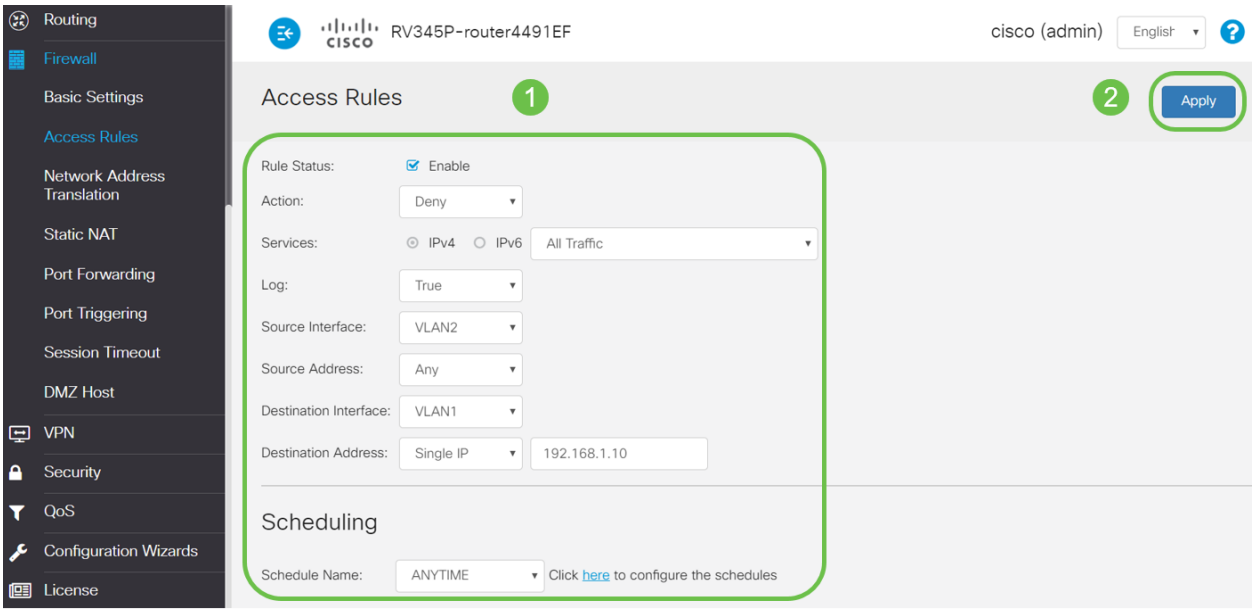
宛先インターフェイス：VLAN1

宛先アドレス:シングルIP 192.168.1.10

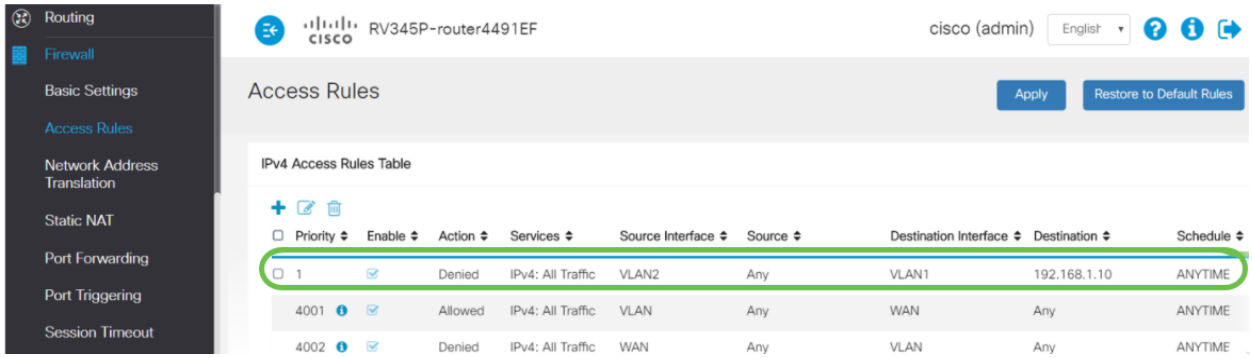
スケジュール名：いつでも

[Apply] をクリックします。

注：この例では、VLAN2からサーバへのデバイスのアクセスを拒否し、VLAN1の他のデバイスへのアクセスを許可しています。ニーズは異なる場合があります。



ステップ12:[アクセスルール]リストは次のようになります。



アクセスルールは、VLAN2ユーザからのサーバ192.168.1.10へのアクセスを制限するために明示的に定義されます。

確認

サービスを確認するには、コマンドプロンプトを開きます。Windowsプラットフォームでは、Windowsボタンをクリックし、コンピュータの左下の検索ボックスに**cmdと入力**して、メニューから**コマンドプロンプトを選択**します。

次のコマンドを入力します。

- VLAN2のPC(192.168.3.173)で、サーバ(IP:192.168.1.10）をキャプチャします。 Request timed out通知が表示され、*通信が許可*されていないことを示します。
- VLAN2のPC(192.168.3.173)で、VLAN1の他のPC(192.168.1.109)にpingを実行します。正常な応答が得られます。

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

結論

RV34xシリーズルータでVLAN間ルーティングを設定するために必要な手順と、ターゲットACL制限を行う方法を確認しました。この知識をすべて活用して、ネットワーク内にニーズに合ったVLANを作成できます。