

RV160/RV260ルータのDMZオプション

目的

このドキュメントでは、RV160X/RV260Xシリーズルータで非武装地帯(DMZ)ホストとDMZサブネットワークを設定する2つのオプションについて説明します。

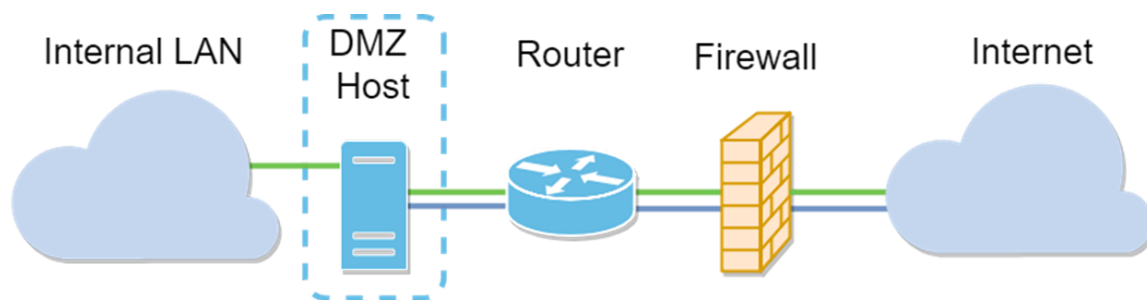
要件

- RV160X
- RV260X

概要

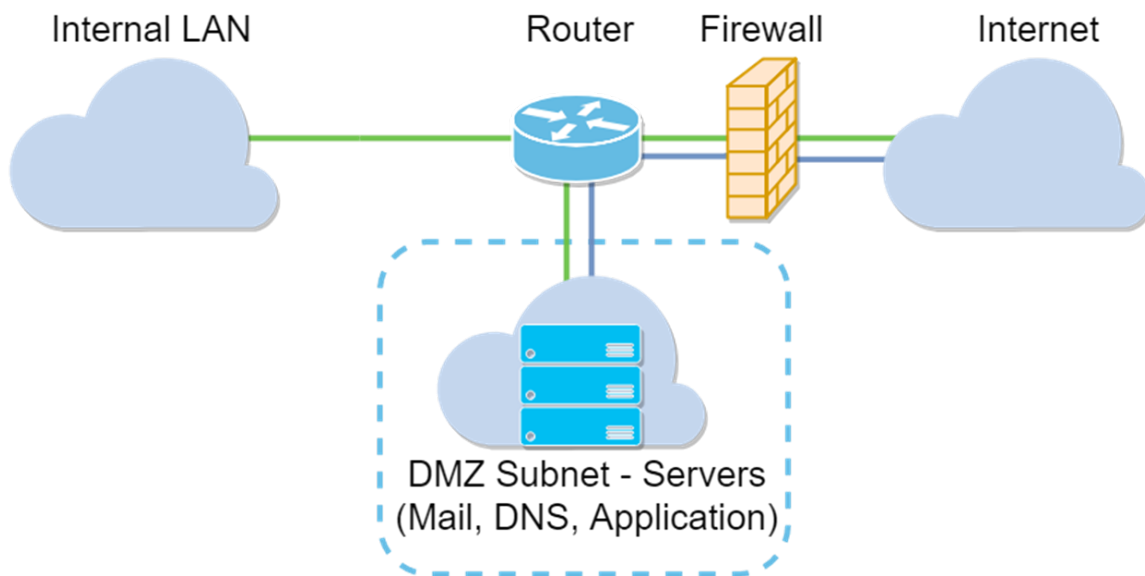
DMZは、ファイアウォールの背後にあるローカルエリアネットワーク(LAN)を保護しながら、インターネットに接続できるネットワーク上の場所です。メインネットワークを単一のホストまたはサブネットワーク全体、または「サブネット」から分離することで、DMZ経由でWebサイトのサーバにアクセスするユーザがLANにアクセスできなくなります。シスコでは、ネットワーク内でDMZを使用する2つの方法を提供しています。どちらも、DMZの動作方法に関して重要な違いを持っています。次に、2つの動作モードの違いを視覚的に示します。

ホストDMZトポロジ



注：ホストDMZを使用している場合、ホストが悪者によって侵害されると、内部LANはセキュリティ上の侵入を受ける可能性があります。

サブネットDMZトポロジ



DMZタイプ	比較	コントラスト
ホスト	トラフィックの分離	単一ホスト、インターネットに対して完全にオープン
サブネット/範囲	トラフィックの分離	複数のデバイスとタイプ、インターネットに完全にオープン。 RV260ハードウェアでのみ利用可能。

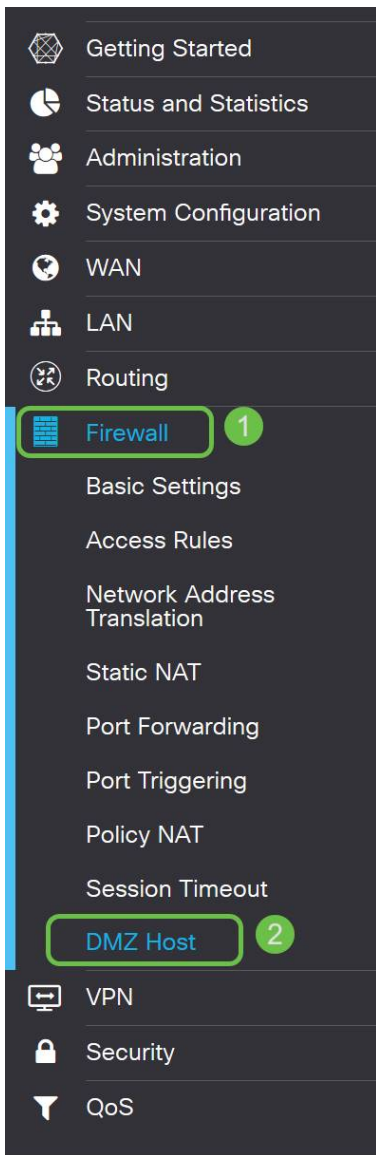
IPアドレスについて

この記事では、IPアドレッシング方式を使用します。IPアドレッシング方式には、なんらかのニュアンスが含まれています。DMZの計画では、プライベートIPアドレスまたはパブリックIPアドレスを使用することを検討できます。プライベートIPアドレスは、LAN上でのみ一意になります。パブリックIPアドレスは組織に固有であり、インターネットサービスプロバイダーによって割り当てられます。パブリックIPアドレスを取得するには、(ISP)に連絡する必要があります。

DMZホストの設定

この方法に必要な情報には、目的のホストのIPアドレスが含まれます。IPアドレスはパブリックまたはプライベートにできますが、パブリックIPアドレスはWAN IPアドレスとは異なるサブネットに配置する必要があります。DMZ Hostオプションは、RV160XとRV260Xの両方で使用できます。次の手順に従ってDMZホストを設定します。

ステップ1: ルーティングデバイスにログインした後、左側のメニューバーで[Firewall] > [DMZ Host]をクリックします。



ステップ2:[Enable]チェックボックスをクリックします。



DMZ Host

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

ステップ3:WANアクセスを開始するホストの指定IPアドレスを入力します。



RV160-router5402D9

DMZ Host

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

ステップ4 : アドレスに問題がなければ、[apply]ボタンをクリックします。

Apply

Cancel

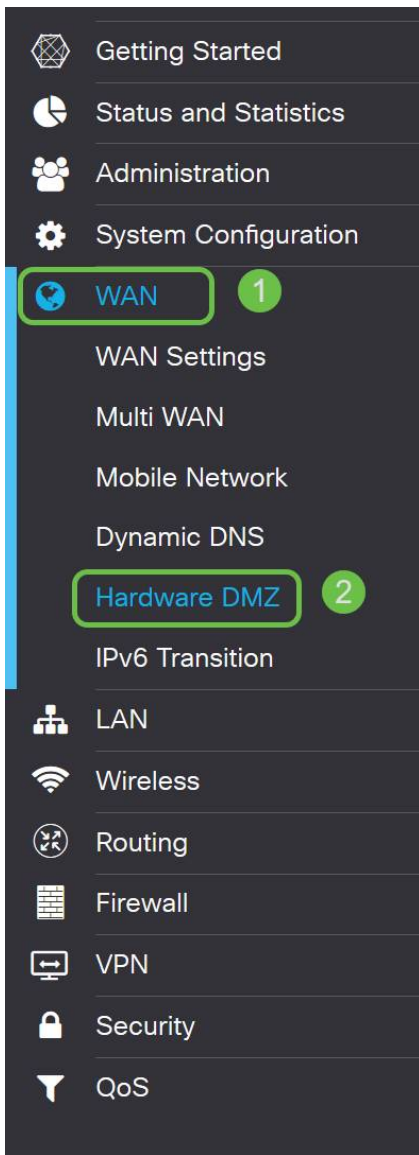
注 : RV160Xシリーズのみを使用していて、検証手順に進む場合は、[ここをクリックしてこのドキュメントのそのセクションに移動してください](#)。

ハードウェアDMZの設定

RV260Xシリーズでのみ利用可能です。この方法では、選択した方法に基づいて異なるIPアドレス情報が必要です。どちらの方法も実際にサブネットワークを使用してゾーンを定義します。その違いは、サブネットワークの使用量が非武装地帯を作成する点です。この場合のオプションは、すべてまたは一部です。サブネット(*all*)方式では、サブネットマスクとともにDMZ自体のIPアドレスが必要です。この方法は、そのサブネットワークに属するすべてのIPアドレスを占有します。一方、範囲(*一部*)方式では、DMZ内に配置するIPアドレスの連続した範囲を定義できます。

注 : どちらの場合も、ISPと協力して、サブネットワークのIPアドレッシング方式を定義する必要があります。

ステップ1:RV260Xデバイスにログインした後、[WAN] > [Hardware DMZ]をクリックします



注：スクリーンショットは、RV260Xユーザインターフェイスから取得したものです。次に、このページに表示されるハードウェアDMZオプションのスクリーンショットを示します。



Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

ステップ2:[Enable (Change LAN8 to DMZ port)]チェックボックスをオンにします。これにより、ルータの8番目のポートがDMZ専用の「ウインドウ」に変換され、セキュリティの強化が必要なサービスに変換されます。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

ステップ3:[Enable]をクリックした後、**選択可能なオプションの下に情報メッセージが表示されます。** ネットワークに影響を与える可能性のあるポイントの詳細を確認し、**[OK, I agree with the above]**チェックボックスをクリックします。

⚠ When hardware DMZ is enabled, the dedicated DMZ Port (LAN8) will be:

- * Disabled as Port Mirror function, if Port Mirror Destination is DMZ Port (LAN > Port Settings);
- * Removed from LAG Port (LAN > Port Settings);
- * Removed from Monitoring Port of Port Mirror (LAN > Port Settings);
- * Changed to "Force Authorized" in Administrative State (LAN > 802.1X Configuration);
- * Changed to "Excluded" in "Assign VLANs to ports" table (LAN > VLAN Settings).

OK, I agree with the above.

ステップ4：次のステップでは、サブネットと範囲の2つのオプションに分割します。次の例では、サブネット方式を選択しました。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address: 164.33.100.250

Subnet Mask: 255.255.255.248

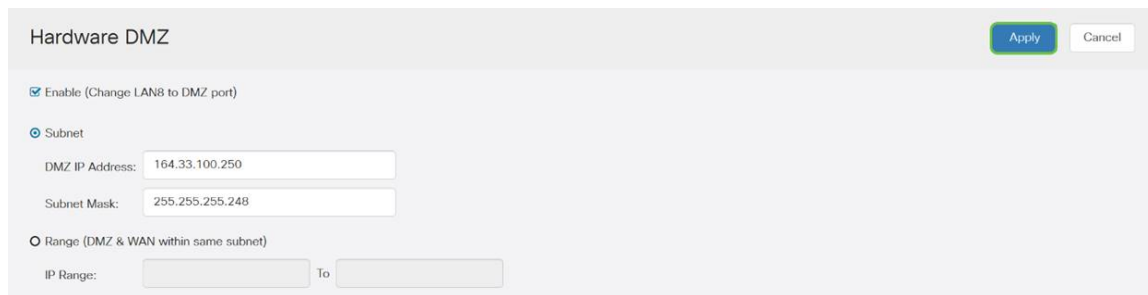
Range (DMZ & WAN within same subnet)

IP Range:

To

注：Rangeメソッドを使用する場合は、**Range** radialボタンをクリックし、ISPによって割り当てられたIPアドレスの範囲を入力する必要があります。

ステップ6:[Apply] (右上隅) をクリックしてDMZ設定を確定します。

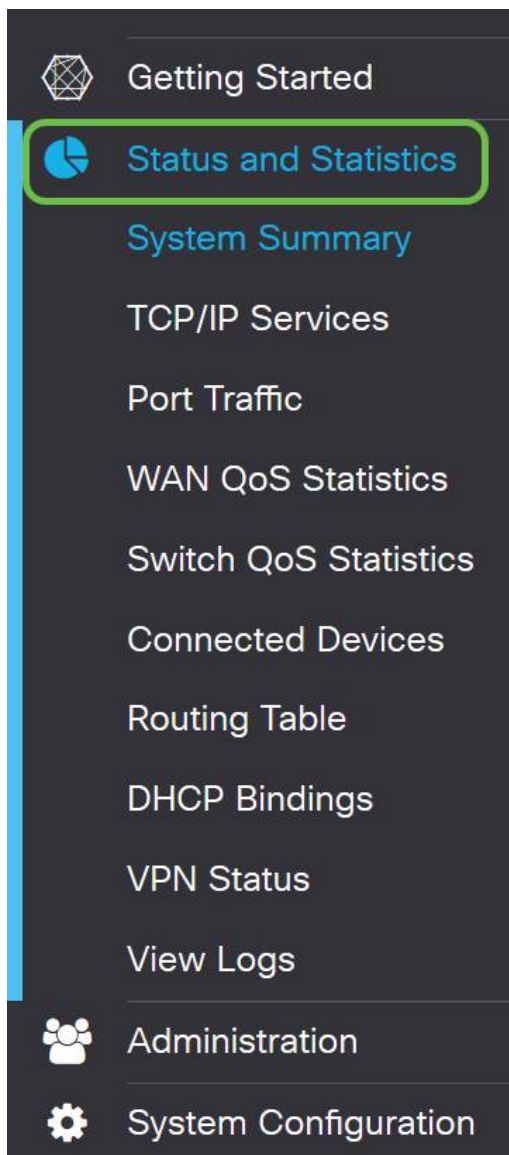


The screenshot shows the 'Hardware DMZ' configuration page. The 'Enable' checkbox is checked. The 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range' radio button is unselected. The 'Apply' button is highlighted in green, and the 'Cancel' button is in grey.

DMZが正しく設定されていることを確認する

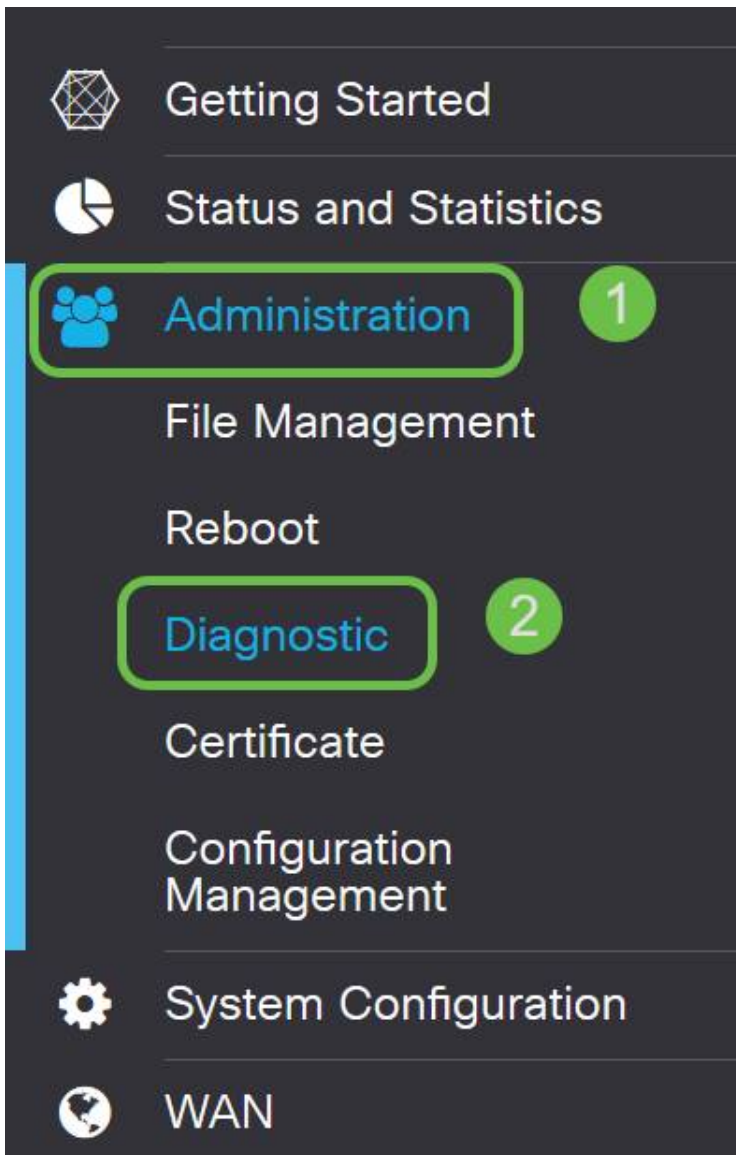
ゾーン外の送信元からのトラフィックを適切に受け入れるようにDMZが設定されていることを確認するには、pingテストで十分です。最初に、管理インターフェイスでDMZのステータスを確認します。

ステップ1:DMZが設定されていることを確認するには、[Status & Statistics]に移動します。このページでは、[System Summary]ページが自動的にロードされます。ポート8または「Lan 8」は、DMZのステータスを「*Connected*」としてリストします。

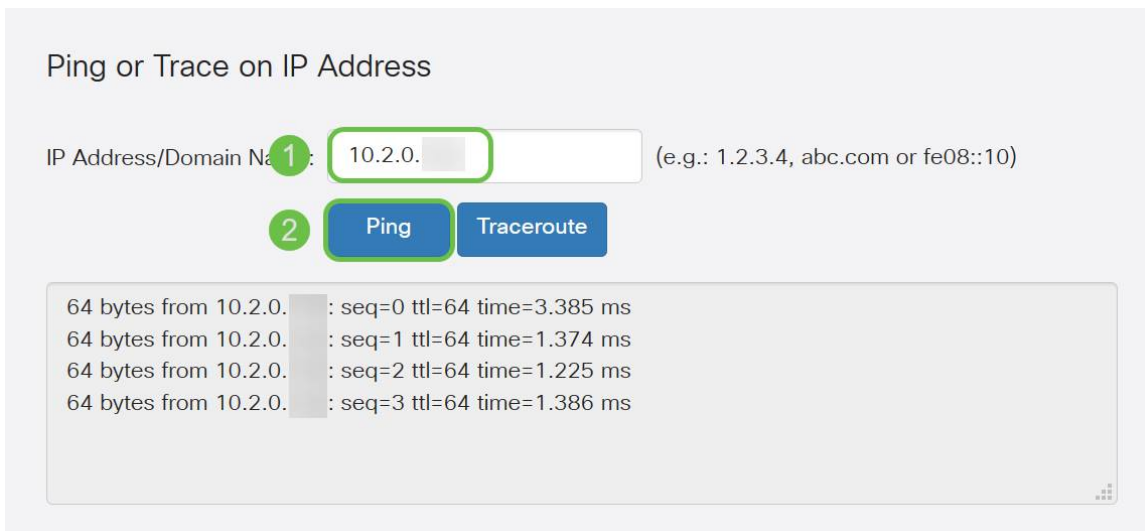


信頼できるICMP ping機能を使用して、DMZが期待どおりに動作しているかどうかをテストできます。ICMPメッセージまたは単に「ping」を実行すると、DMZのドアをノックしようとします。DMZが「Hello」と応答すると、pingは完了します。

ステップ2：ブラウザをping機能に移動するには、[Administration] > [Diagnostic]をクリックします。



ステップ3:DMZのIPアドレスを入力し、[Ping]ボタンをクリックします。



pingが成功すると、上記のようなメッセージが表示されます。pingが失敗した場合は、DMZに到達できないことを意味します。DMZの設定を確認して、適切に設定されていることを確認します。

結論

これでDMZの設定が完了したので、LANの外部からサービスへのアクセスを開始できます。