RV016、RV042、RV042G、およびRV082 VPNルータのサブネットマスクを使用した非武装地帯(DMZ)ポートの設定

目的

非武装地帯(DMZ)は組織の内部ネットワークの一部であり、インターネットなどの信頼できないネットワークで使用できるようになっています。DMZは、組織の内部ネットワークのセキュリティの向上に役立ちます。すべての内部リソースをインターネットから利用できる代わりに、Webサーバなどの特定のホストだけが利用できます。

アクセスコントロールリスト(ACL)がインターフェイスにバインドされると、そのインターフェイスに到着するパケットにアクセスコントロール要素(ACE)ルールが適用されます。ACLのどのACEにも一致しないパケットは、一致しないパケットをドロップするアクションを持つデフォルトのルールに一致します。この記事では、DMZポートを設定し、DMZから特定の宛先IPアドレスへのトラフィックを許可する方法について説明します。

適用可能なデバイス

- RV016
- RV042
- RV042G
- RV082

[Software Version]

- v4.2.2.08

サブネットを使用したDMZ設定

ステップ 1：Router Configuration Utilityページにログインし、Setup > Networkの順に選択します。Networkページが開きます。

Network

Host Name : router88c688 (Required by some ISPs)

Domain Name : router88c688.com (Required by some ISPs)

IP Mode

Mode	WAN	LAN
IPv4 Only	IPv4	IPv4
Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4 | IPv6

LAN Setting

MAC Address : 64:9E:F3:88:C6:88

Device IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Multiple Subnet : Enable Add/Edit

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

Enable DMZ

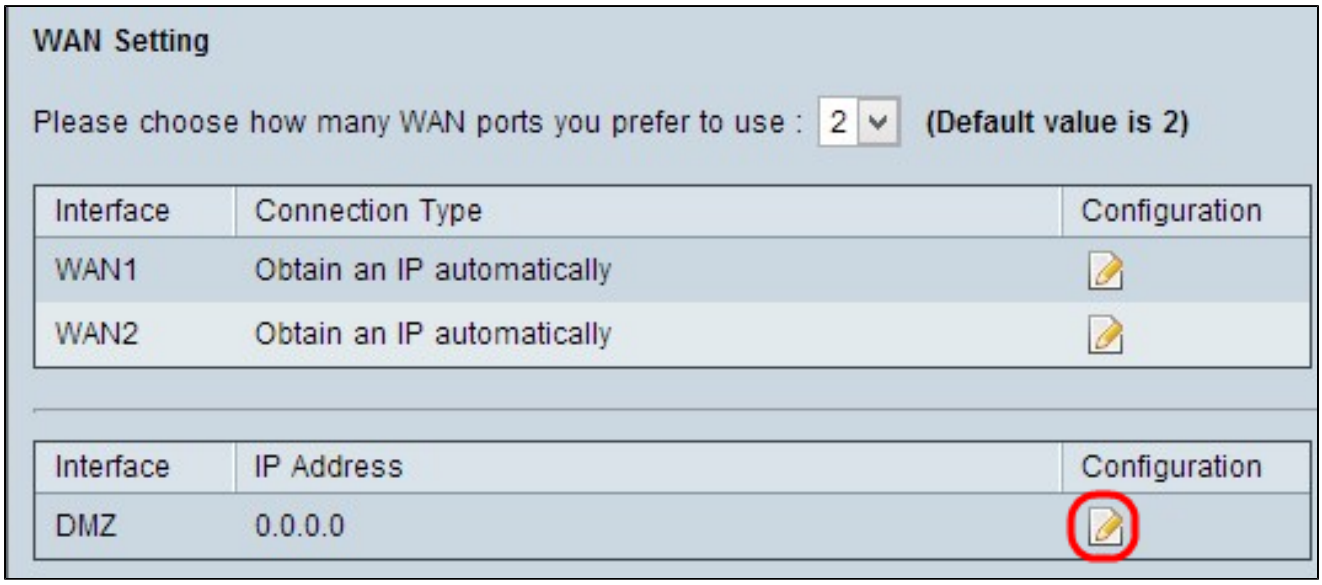
Interface	IP Address	Configuration
DMZ	0.0.0.0	

Save Cancel

ステップ 2：IPv4またはIPv6アドレスでDMZを設定するには、LAN Settingフィールドにある対応するタブをクリックします。

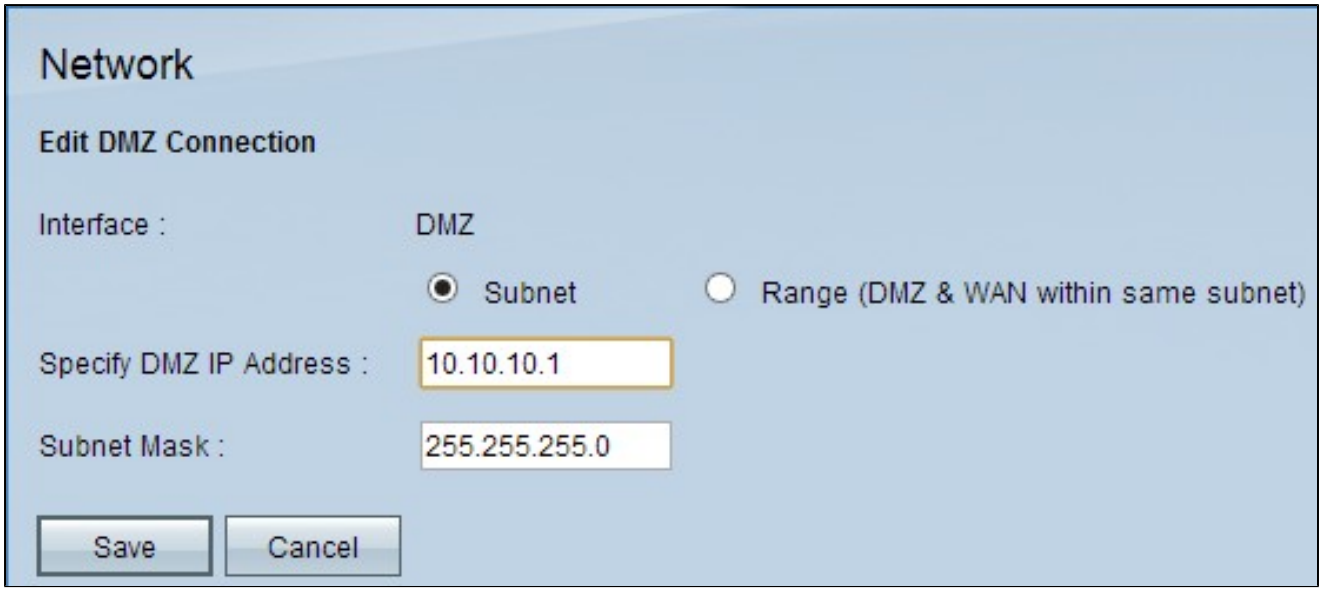
注：IPv6を設定する場合は、IP Modeエリアのデュアルスタック IPを有効にする必要があります。

ステップ 3：DMZ Settingフィールドまでスクロールし、Enable DMZオプションボタンをクリックしてDMZを有効にします。



ステップ 4：サブネットを設定するには、DMZ設定アイコンをクリックします。IPv4とIPv6の両方の設定は、次の方法で行うことができます。

IPv4の設定



ステップ 5：DMZをWANのサブネット以外のサブネットに設定するには、Subnetオプションボタンをクリックします。サブネットIPについては、次のように設定する必要があります

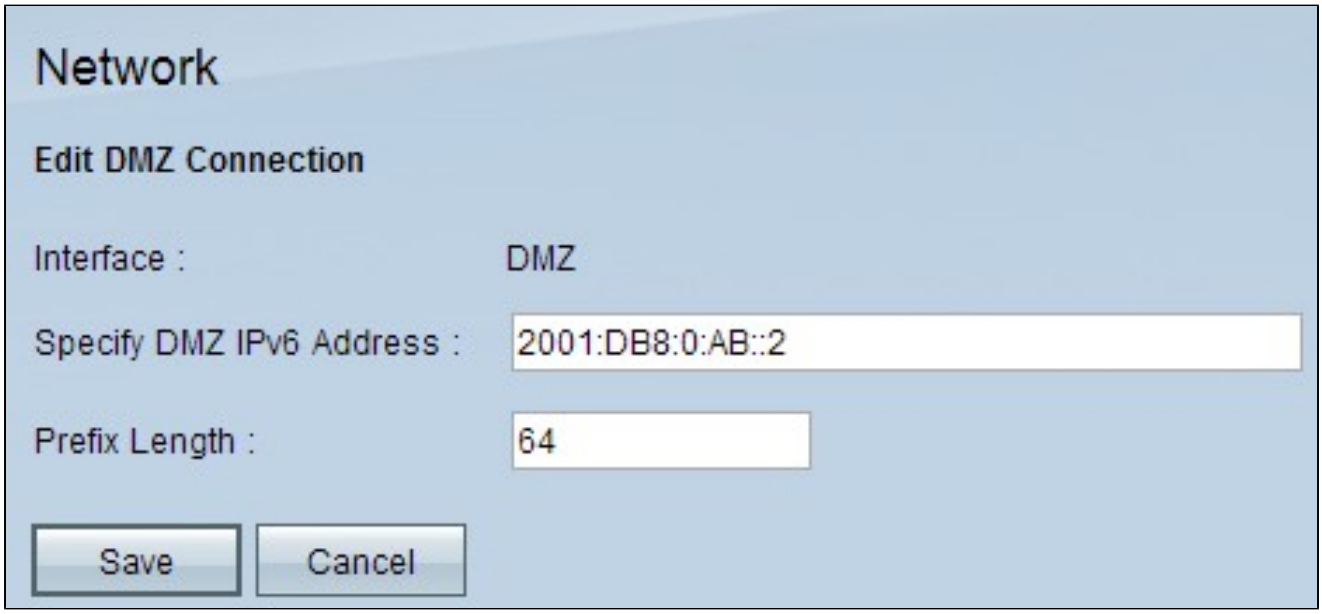
・ Specify DMZ IP Address:Specify DMZ IP AddressフィールドにDMZのIPアドレスを入力します。

・ Subnet Mask:Subnet Maskフィールドにサブネットマスクを入力します。

警告： DMZ内にIPアドレスを持つホストは、内部LAN内のホストほどセキュアではありません。

手順 6：DMZをWANと同じサブネット上に設定するには、Rangeをクリックします。IPアドレスの範囲は、DMZポートのIP範囲フィールドに入力します。

IPv6の設定



注：IPv6設定では、次のオプションを使用できます。

手順 7：「DMZ IPv6アドレスを指定」 — IPv6アドレスを入力します。

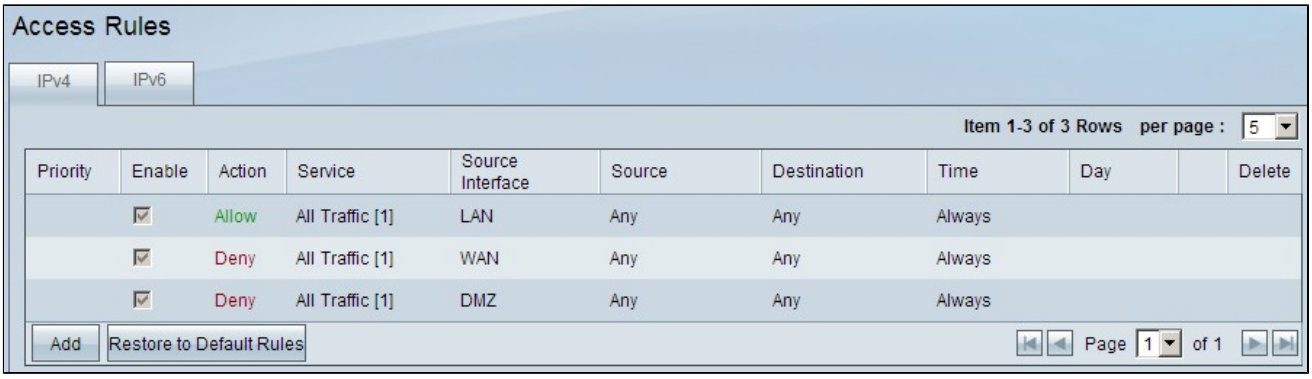
ステップ 8：Prefix Length：上記のDMZ IPアドレスドメインのプレフィックス長を入力します。

ステップ 9：Saveをクリックして、設定を保存します。

アクセスルールの設定

この設定は、複数のサブネットマスクで設定されたIPのアクセスリストを定義するために行います。

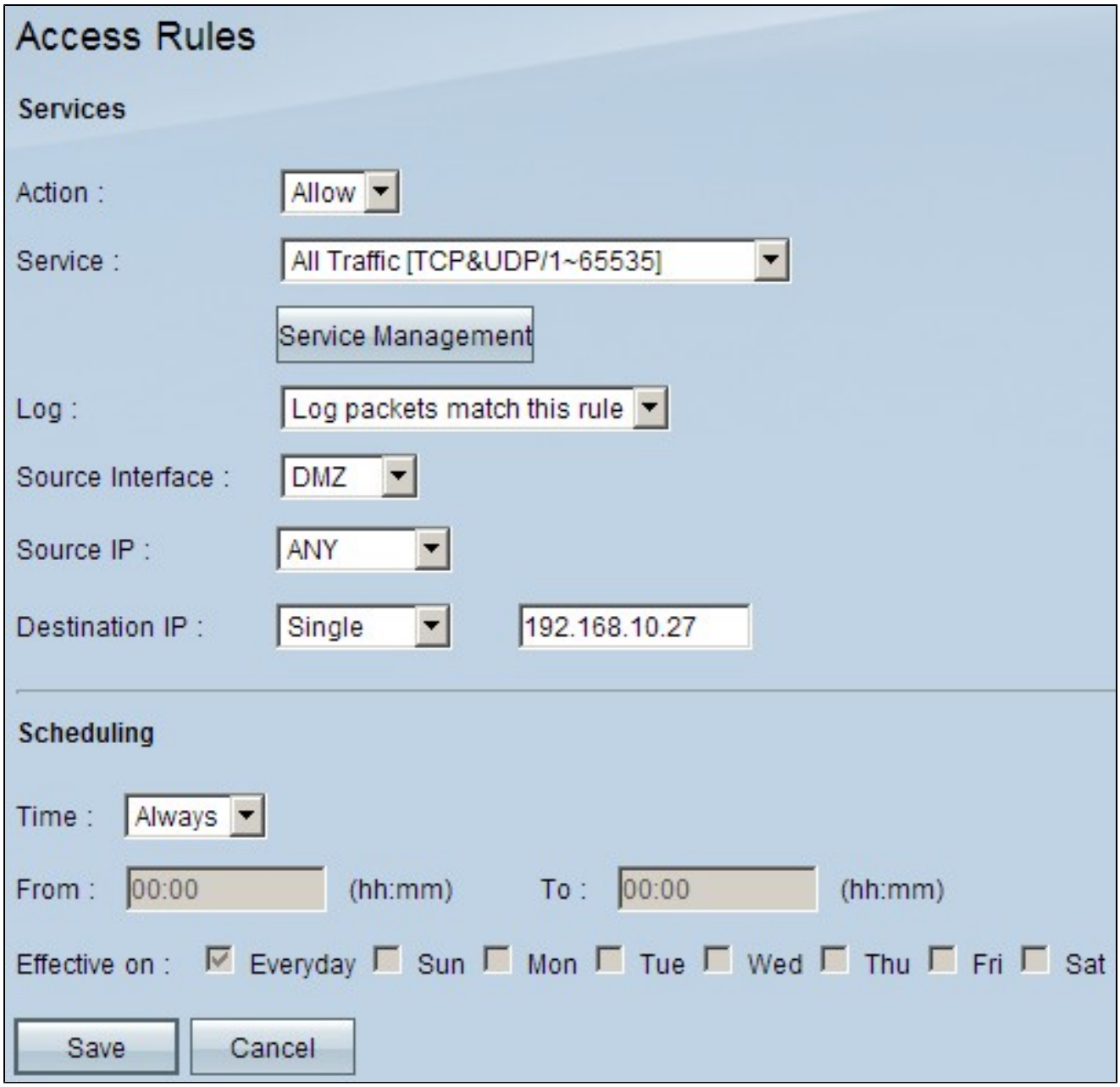
ステップ 1：Router Configuration Utilityページにログインし、Firewall > Access Rulesの順に選択します。アクセスルールページが開きます。



注：デフォルトのアクセスルールは編集できません。

ステップ 2：Addボタンをクリックして、新しいアクセスルールを追加します。アクセスルールページに、サービスエリアとスケジューリングエリアが表示されます。

注：この設定は、IPv4とIPv6の両方に対して、アクセスルールページでそれぞれのタブを選択することで実行できます。IPv4とIPv6に固有の設定手順は、次の手順で説明します。



ステップ 3：Actionドロップダウンリストから**Allow**を選択して、サービスを許可します。

ステップ 4：Serviceドロップダウンリストから**All Traffic [TCP&UDP/1 ~ 65535]** を選択し、DMZのすべてのサービスを有効にします。

ステップ 5：Logドロップダウンリストから**Log packets that match this rule**を選択し、アクセスルールに一致するログだけを選択します。

手順 6：アクセスルールの送信元である**Source Interface**ドロップダウンリストからDMZを選択します。

手順 7：Source IPドロップダウンリストから**Any**を選択します。

ステップ 8：Destination IPドロップダウンリストから次の使用可能なオプションのいずれかを選択します。

・ Single：このルールを単一のIPアドレスに適用するには、singleを選択します。

・ Range：このルールをIPアドレスの範囲に適用する範囲を選択します。範囲の最初と最後のIPアドレスを入力します。このオプションは、IPv4でのみ使用できます。

・サブネット：このルールをサブネットワークに適用するには、[サブネット]を選択します。サブネットにIPアドレスを割り当て、インターネットプロトコルパケットをルーティングするために使用されるIPアドレスとCIDR表記番号を入力します。このオプションは、IPv6でのみ使用できます。

・ Any：任意のIPアドレスにルールを適用するには、[任意]を選択します。

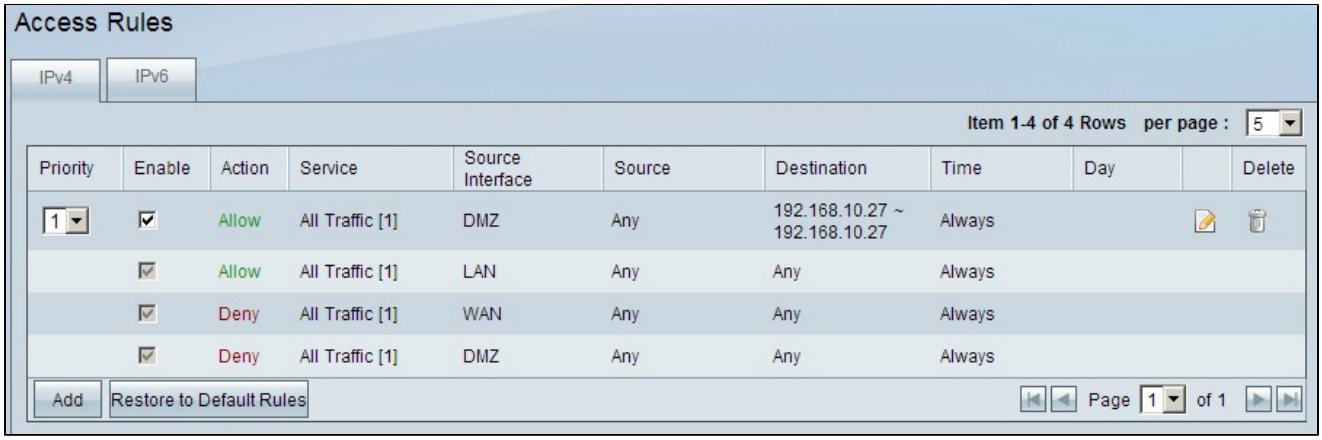
タイムサバー：IPv6アクセスルールを設定する場合は、ステップ10に進みます。

ステップ 9：「時間」ドロップダウンリストから、規則がアクティブになるタイミングを定義する方法を選択します。その内容は次のとおりです。

・ Always:[Time]ドロップダウンリストから[Always]を選択した場合、アクセスルールは常にトラフィックに適用されます。

・ Interval — [Time]ドロップダウンリストから[Interval]を選択すると、アクセスルールがアクティブである特定の時間間隔を選択できます。時間間隔を指定したら、アクセスルールをアクティブにする日付を[有効にする日]チェックボックスから選択します。

ステップ 10：Saveをクリックして設定を保存します。



ステップ 11Editアイコンをクリックして、作成したアクセスルールを編集します。

ステップ 12Deleteアイコンをクリックして、作成したアクセスルールを削除します。

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。