

RV042、RV042G、およびRV082 VPNルータの非武装地帯(DMZ)における複数のパブリックIPの設定

目的

非武装地帯(DMZ)は組織の内部ネットワークであり、信頼できないネットワークが利用できるようになっています。DMZはセキュリティ上、信頼ネットワークと非信頼ネットワークの間に位置します。DMZのメンテナンスは、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。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。Access Control List (ACL ; アクセスコントロールリスト) 内のどの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。

このドキュメントの目的は、複数のパブリックIPアドレスを許可するようにDMZポートを設定し、ルータデバイス上のIPに対してアクセスコントロールリスト(ACL)を定義する方法を示すことです。

適用可能なデバイス

- RV042
- RV042G
- RV082

[Software Version]

- v4.2.2.08

DMZの設定

ステップ 1 : Web 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 : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

LAN Setting

MAC Address : 50:57:A8:79:F3:7A

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable Add/Edit

WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

DMZ Setting

Enable DMZ

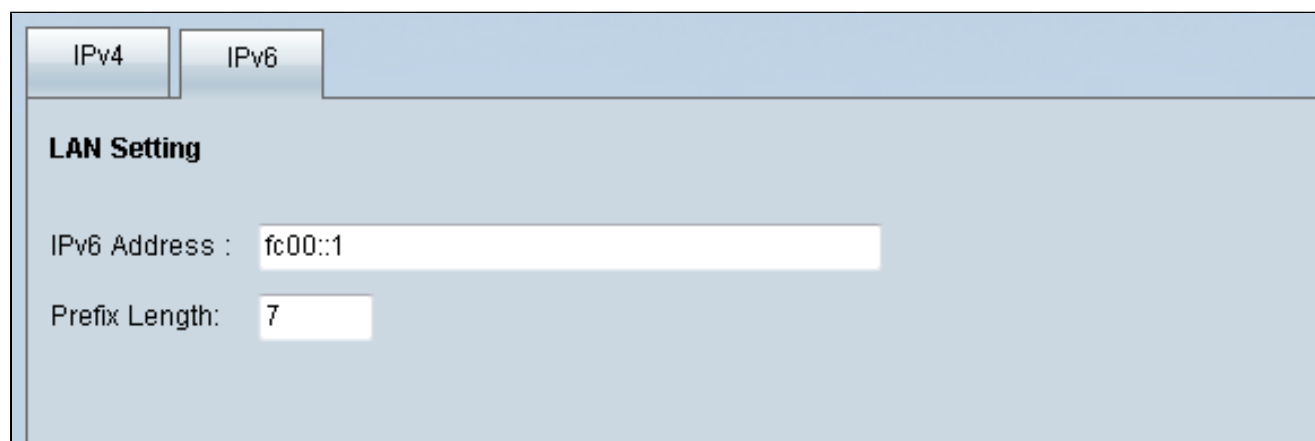
Interface	IP Address	Configuration
DMZ	0.0.0.0	

ステップ 2 : IP Modeフィールドで、Dual-Stack IPオプションボタンをクリックして、IPv6アドレスの設定を有効にします。

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

ステップ 3 : IPv6アドレスでDMZを設定できるようにするには、LAN SettingフィールドにあるIPv6タブをクリックします。



The screenshot shows the 'LAN Setting' configuration page with the 'IPv6' tab selected. The 'IPv6 Address' field contains 'fc00::1' and the 'Prefix Length' field contains '7'.

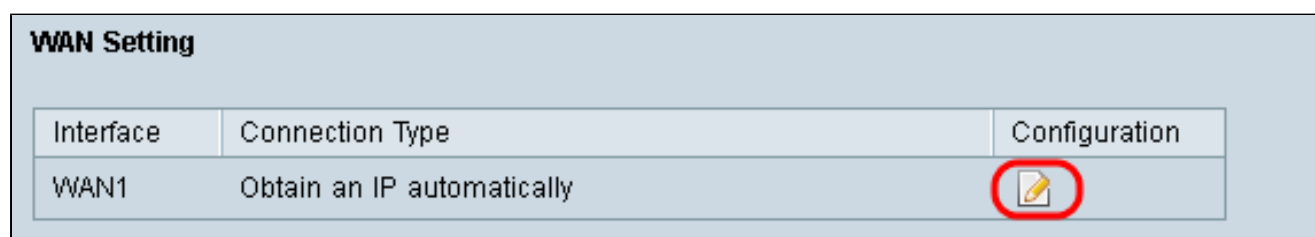
ステップ4:DMZ Setting領域までスクロールし、DMZチェックボックスをクリックしてDMZを有効にします




The screenshot shows the 'DMZ Setting' section. The 'Enable DMZ' checkbox is checked and circled in red. Below it is a table with columns for Interface, IP Address, and Configuration.

Interface	IP Address	Configuration
DMZ	::/64	

ステップ 5 : WAN SettingフィールドでEditボタンをクリックして、WAN1設定のIP Staticを編集します。



The screenshot shows the 'WAN Setting' section. A table lists WAN1 with the connection type 'Obtain an IP automatically'. The edit icon in the Configuration column is circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Networkページが開きます。

Network

Edit WAN Connection

Interface : WAN1

WAN Connection Type : Static IP

Specify WAN IP Address : 192.168.3.1

Subnet Mask : 255.255.255.0

Default Gateway Address : 192.168.3.2

DNS Server (Required) 1 : 0.0.0.0

2 : 0.0.0.0

MTU : Auto Manual 1500 bytes

Save Cancel

手順 6 : WAN Connection Type ドロップダウンリストから、Static IP を選択します。

手順 7 : System Summary ページの Specify WAN IP Address フィールドに表示されている WAN IP アドレスを入力します。

ステップ 8 : Subnet Mask フィールドにサブネットマスクアドレスを入力します。

ステップ 9 : Default Gateway Address フィールドにデフォルトゲートウェイアドレスを入力します。

ステップ 10 : System Summary ページの DNS Server (Required) 1 フィールドに表示されている DNS サーバアドレスを入力します。

注 : DNS サーバアドレス 2 はオプションです。


ステップ 11 最大伝送ユニット (MTU) を自動または手動のどちらかを選択します。manual を

選択した場合は、Manual MTUのバイト数を入力します。

ステップ 12 Saveタブをクリックして、設定を保存します。

ACLの定義

ステップ 1 : Web 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。



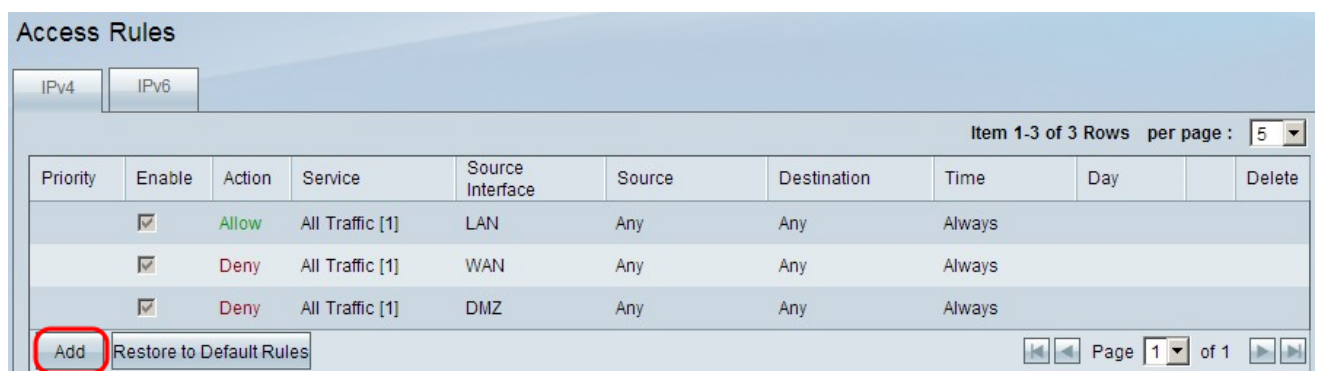
Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

Item 1-3 of 3 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

注 : アクセス規則ページにアクセスすると、デフォルトのアクセス規則は編集できません。

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。



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

Item 1-3 of 3 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

Access Rulesページに、ServiceエリアとSchedulingエリアのオプションが表示されます。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

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] を選択して、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 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 : Source Interface ドロップダウンリストから DMZ を選択します。これは、アクセスルールのソースです。

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Singleを選択します。

ステップ 9 : Destination IP フィールドに、アクセスルールを許可する宛先のIPアドレスを入力します。

ステップ 10 : Scheduling領域で、Time ドロップダウンリストからAlwaysを選択して、アクセスルールを常にアクティブにします。

注 : Time ドロップダウンリストからAlwaysを選択した場合、アクセスルールはデフォルトでEveryにEffective onフィールドに設定されます。

注 : アクセスルールがアクティブになっている特定の時間間隔を選択するには、「Time」ドロップダウンリストから「Interval」を選択します。次に、アクセスルールをアクティブにする日をEffective onチェックボックスから選択します。

ステップ 11 Saveをクリックして設定を保存します。

注 : ポップアップウィンドウが表示されたら、[OK]をクリックして別のアクセスルールを追加するか、[キャンセル]をクリックしてアクセスルールのページに戻ります。

前の手順で作成したアクセスルールが表示されます

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

Item 1-4 of 4 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

ステップ 12 Edit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 13 Delete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。