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 :	router88	0688	(Required by some ISPs)			
Domain Name : router88c688.com			(Required by some ISPs)			
IP Mode						
Mode	1	WAN		LAN		
C IPv4 Only		IPv4		IPv4		
Dual-Stack IF	2	IPv4 and IPv6		IPv4 and IPv6		
IPv4 IP	V6					
LAN Setting						
MAC Address :	64:9E:F3:88:C6	5:88				
Device IP Addre	ess : 192.168	8.1.1				
Subnet Mask :	255.255	5.255.0 💌				
Multiple Subnet	: 🗖 Ena	able	Add/Edit			
WAN Setting						
Interface	Connection Ty	pe			Configuration	
WAN1	Static IP	<u> </u>				
DMZ Setting	2					
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。

VAN Setting	se how many WAN ports you prefer to use : 2	 (Default value is 2)
Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	
Interface	IP Address	Configuration
DMZ	0.0.0.0	

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。<u>IPv4</u>と <u>IPv6</u>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

Network		
Edit DMZ Connection		
Interface :	DMZ	
	Subnet	O Range (DMZ & WAN within same subnet)
Specify DMZ IP Address :	10.10.10.1	
Subnet Mask :	255.255.255.0	
Save Cancel		

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

Network	
Edit DMZ Connection	
Interface :	DMZ
Specify DMZ IPv6 Address :	2001:DB8:0:AB::2
Prefix Length :	64
Save Cancel	

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。

Access F	Rules									
IPv4	IPv6									
							Item 1-3	of 3 Rows per	page :	5 💌
Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
		Allow	All Traffic [1]	LAN	Any	Any	Always			
	V	Deny	All Traffic [1]	WAN	Any	Any	Always			
	M	Deny	All Traffic [1]	DMZ	Any	Any	Always			
Add	Restore to I	Default Ru	les					Page 1	of 1	

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。

Access Rules	
Services	
Action :	Allow 🔽
Service :	All Traffic [TCP&UDP/1~65535]
s	ervice Management
Log:	Log packets match this rule 💌
Source Interface :	DMZ -
Source IP :	ANY
Destination IP :	Single 192.168.10.27
Cabadulina	
Scheduling	
Time : Always 💌	
From : 00:00	(hh:mm) To : 00:00 (hh:mm)
Effective on : 🔽 Eve	ryday 🗖 Sun 🗖 Mon 🗖 Tue 🗖 Wed 🗖 Thu 🗖 Fri 🗖 Sat
Save Canc	el

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。

Access F	Rules									
IPv4	IPv6									
	20 						Item	1-4 of 4 Rows per	page :	5 💌
Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
1-	V	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always			Ĩ
		Allow	All Traffic [1]	LAN	Any	Any	Always			
	M	Deny	All Traffic [1]	WAN	Any	Any	Always			
	V	Deny	All Traffic [1]	DMZ	Any	Any	Always			
Add	Restore to [Default Ru	les					Page 1	of 1	

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。