

Configuração da porta de zona desmilitarizada com máscara de sub-rede nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Uma zona desmilitarizada (DMZ) é parte de uma rede interna de uma organização que é disponibilizada para uma rede não confiável, como a Internet. Uma DMZ ajuda a melhorar a segurança na rede interna de uma empresa. Em vez de todos os recursos internos estarem disponíveis na Internet, apenas alguns hosts, como servidores Web, estão disponíveis.

Quando uma ACL (Access Control List, lista de controle de acesso) é vinculada a uma interface, as regras ACE (Access Control Element, elemento de controle de acesso) são aplicadas aos pacotes que chegam a essa interface. Os pacotes que não correspondem a nenhuma das ACEs na ACL correspondem a uma regra padrão cuja ação é descartar pacotes incomparáveis. Este artigo mostra como configurar a porta DMZ e permitir o tráfego da DMZ para endereços IP de destino específicos.

Dispositivos aplicáveis

- RV016
- RV042
- RV042G
- RV082

Versão de software

- v4.2.2.08

Configuração de DMZ com sub-rede

Etapa 1. Faça login na página Router Configuration Utility e escolha **Setup > Network**. A página *Rede* é aberta:

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 : 64:9E:F3:88:C6:88

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

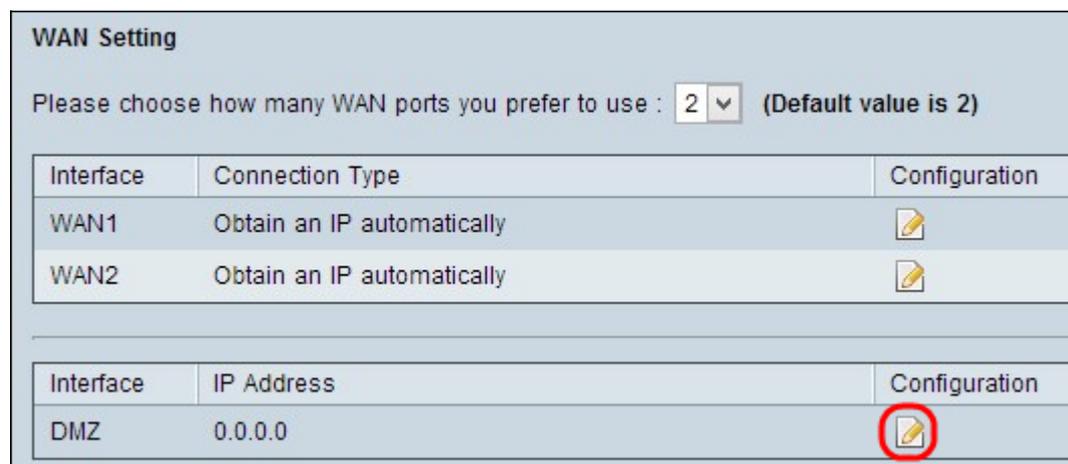
Enable DMZ

Interface	IP Address	Configuration
DMZ	0.0.0.0	

Etapa 2. Para configurar DMZ no endereço IPv4 ou IPv6, clique na guia correspondente localizada no campo LAN Setting (Configuração de LAN).

Note: O IP de pilha dupla na área *do modo IP* deve ser ativado se você quiser configurar o IPv6.

Etapa 3. Role para baixo até o campo DMZ Setting (Configuração de DMZ) e clique no botão de opção **Enable DMZ (Habilitar DMZ)** para habilitar DMZ.



Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Interface	IP Address	Configuration
DMZ	0.0.0.0	

Etapa 4. Clique no ícone de configuração DMZ para configurar a sub-rede. A configuração pode ser feita para [IPv4](#) e [IPv6](#) da seguinte maneira:

Configuração IPv4



Network

Edit DMZ Connection

Interface : DMZ

Subnet Range (DMZ & WAN within same subnet)

Specify DMZ IP Address : 10.10.10.1

Subnet Mask : 255.255.255.0

Save Cancel

Etapa 5. Clique no botão de opção **Sub-rede** para configurar DMZ para outra sub-rede diferente da WAN. Para o IP da sub-rede, deve-se configurar o seguinte

- Especificar endereço IP DMZ — Insira o endereço IP DMZ no campo **Especificar endereço IP DMZ**.

- Máscara de sub-rede — Insira a máscara de sub-rede no campo **Máscara de sub-rede**.

aviso: Os hosts com um endereço IP na DMZ não são tão seguros quanto os hosts dentro da LAN interna.

Etapa 6. Clique em **Intervalo** para configurar a DMZ para estar na mesma sub-rede da WAN. O intervalo dos endereços IP deve ser inserido no campo **Intervalo de IPs da porta DMZ**.

Configuração do IPv6

Network

Edit DMZ Connection

Interface : DMZ

Specify DMZ IPv6 Address : 2001:DB8:0:AB::2

Prefix Length : 64

Save Cancel

Note: Para a configuração do IPv6, estão disponíveis as seguintes opções:

Passo 7. Especificar endereço IPv6 DMZ — Insira o endereço IPv6.

Etapa 8. Comprimento do prefixo — O comprimento do prefixo do domínio de endereço IP DMZ mencionado acima deve ser inserido.

Etapa 9. Clique em **Salvar** para salvar a configuração.

Configuração das regras de acesso

Essa configuração é feita para definir as listas de acesso para os IPs configurados nas várias máscaras de sub-rede.

Etapa 1. Efetue login na página Utilitário de configuração do roteador e escolha **Firewall > Access Rules**. A página *Regras de acesso* é aberta:

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

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		

Add Restore to Default Rules Page 1 of 1

Note: As regras de acesso padrão não podem ser editadas.

Etapa 2. Clique no botão **Adicionar** para adicionar uma nova regra de acesso. A página *Regras de acesso* é alterada para mostrar as áreas *Serviços* e *Agendamento*.

Note: Essa configuração pode ser feita para IPv4 e IPv6 selecionando as respectivas guias na página *Regras de acesso*. As etapas de configuração específicas para IPv4 e IPv6 são mencionadas nas etapas a seguir.

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

Etapa 3. Escolha **Permitir** na lista suspensa Ação para permitir o serviço.

Etapa 4. Escolha **All Traffic [TCP&UDP/1~65535]** na lista suspensa Service para habilitar todos os serviços para a DMZ.

Etapa 5. Escolha **Pacotes de log que correspondam a essa regra** na lista suspensa Log para escolher somente logs que correspondam à regra de acesso.

Etapa 6. Escolha **DMZ** na lista suspensa Interface de origem, que é a origem das regras de acesso.

Passo 7. Escolha **Qualquer** na lista suspensa IP de origem.

Etapa 8. Escolha qualquer uma das seguintes opções disponíveis na lista suspensa IP de destino.

Single - Escolha single para aplicar essa regra a um único endereço IP.

Intervalo — Escolha o intervalo para aplicar esta regra a um intervalo de endereços IP. Insira o primeiro e o último endereço IP do intervalo. Essa opção está disponível somente no IPv4.

Sub-rede — Escolha Sub-rede para aplicar essas regras a uma sub-rede. Insira o endereço IP e o número de notação CIDR usados para alocar endereços IP e rotear pacotes de protocolo de Internet para a sub-rede. Essa opção está disponível somente no IPv6.

Any (Qualquer) — Escolha Any (Qualquer) para aplicar a regra a qualquer um dos

endereços IP.

Proteção de tempo: Vá para a Etapa 10 se estiver configurando regras de acesso IPv6.

Etapa 9. Escolha um método para definir quando as regras estão ativas na lista suspensa Hora. São elas:

Sempre — Se você escolher Sempre na lista suspensa Hora, as regras de acesso sempre serão aplicadas ao tráfego.

• Intervalo — Você pode escolher um intervalo de tempo específico no qual as regras de acesso estão ativas se selecionar Intervalo na lista suspensa Hora. Depois de especificar o intervalo de tempo, escolha os dias em que deseja que as regras de acesso estejam ativas nas caixas de seleção Efetivo em.

Etapa 10. Clique em **Salvar** para salvar suas configurações.

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		

Etapa 11. Clique no ícone **Editar** para editar a regra de acesso criada.

Etapa 12. Clique no ícone **Excluir** para excluir a regra de acesso criada.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.