

Configuração de regras de acesso em roteadores VPN RV320 e RV325

Objetivo

Listas de controle de acesso (ACLs) são listas que bloqueiam ou permitem que o tráfego seja enviado de e para determinados usuários. As regras de acesso podem ser configuradas para serem aplicadas o tempo todo ou com base em uma programação definida. Uma regra de acesso é configurada com base em vários critérios para permitir ou negar acesso à rede. A regra de acesso é agendada com base no tempo em que as regras de acesso precisam ser aplicadas ao roteador. Este artigo descreve e descreve o Assistente de configuração da regra de acesso usado para determinar se o tráfego tem permissão para entrar na rede através do firewall do roteador ou não para garantir a segurança na rede.

Dispositivos aplicáveis | Versão do firmware

- Roteador VPN WAN duplo RV320 | V 1.1.0.09 ([Download mais recente](#))
- Roteador VPN WAN duplo RV325 Gigabit | V 1.1.0.09 ([Download mais recente](#))

Configuração da regra de acesso

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Firewall>Access Rules**. A página *Regras de acesso* é aberta:



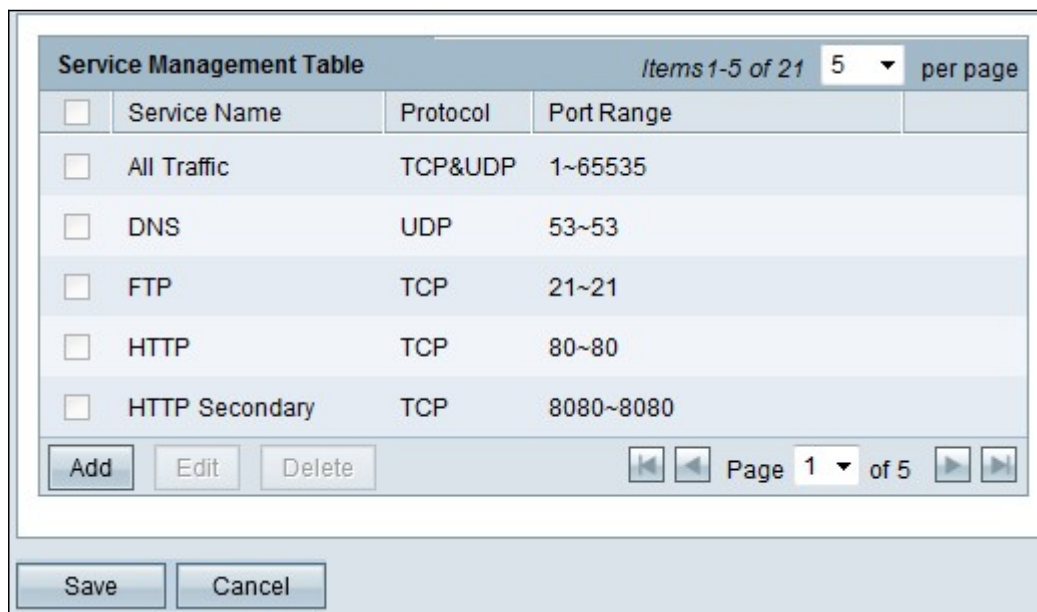
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

A Tabela de regras de acesso contém as seguintes informações:

- Prioridade — Mostra a prioridade da regra de acesso
- Ativar — Mostra se a regra de acesso está ativada ou desativada
- Ação — Mostra que a regra de acesso é permitida ou negada.
- Serviço — Mostra o tipo de serviço.
- SourceInterface — Mostra a qual interface a regra de acesso é aplicada.
- Origem — Mostra o endereço IP do dispositivo de origem
- Destino — Mostra o endereço IP do dispositivo de destino
- Hora — Mostra a hora em que a regra de acesso deve ser aplicada
- Dia — Mostra durante uma semana quando a regra de acesso é aplicada

Gerenciamento de serviço

Etapa 1. Clique em **Gerenciamento de serviços** para adicionar um novo serviço. A página da *tabela Gerenciamento de serviços* é aberta:

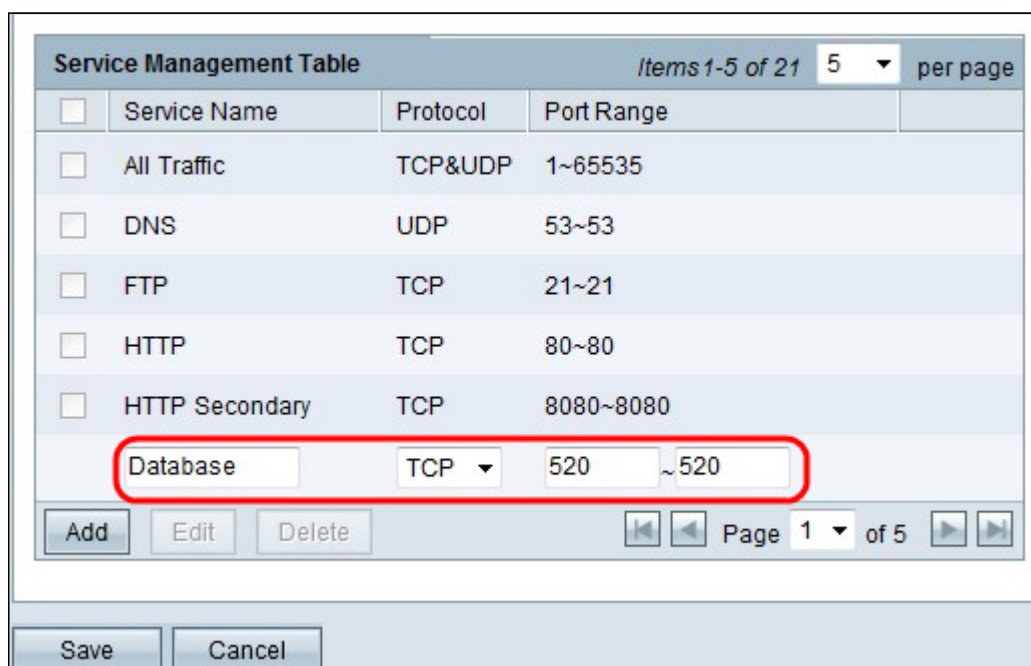


The screenshot shows a web interface titled "Service Management Table". At the top right, it says "Items 1-5 of 21" and "5 per page". Below this is a table with the following columns: "Service Name", "Protocol", and "Port Range". The table contains five rows of services, each with a checkbox in the first column:

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080

Below the table are three buttons: "Add", "Edit", and "Delete". At the bottom of the interface are "Save" and "Cancel" buttons. The page navigation shows "Page 1 of 5".

Etapa 2. Clique em **Adicionar** para adicionar um novo serviço.



This screenshot is identical to the previous one, but with a new row added to the table. The new row is highlighted with a red rectangle and contains the following data:

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080
<input type="checkbox"/>	Database	TCP	520 ~ 520

Etapa 3. Configure os campos a seguir.

- Nome do serviço — Com base no seu requisito, forneça um nome para o serviço
- Protocolo — Escolha um protocolo TCP ou UDP para seu serviço
- Intervalo de portas — Insira o intervalo de números de portas com base em seu requisito e o número de porta deve estar no intervalo (1-65536).

Etapa 4. Clique em **Salvar** para salvar as alterações

Configuração da regra de acesso em IPv4

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management...

Page 1 of 1

Etapa 1. Clique em **Adicionar** para configurar uma nova regra de acesso. A janela *Editar regras de acesso* é exibida.

Edit 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

Save Cancel Back

Etapa 2. Escolha a opção apropriada na lista suspensa **Ação** para permitir ou restringir o tráfego para a regra que você está prestes a configurar. As regras de acesso limitam o acesso à rede com base em vários valores.

- Permitir — Permite todo o tráfego.
- Negar — Restringe todo o tráfego.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on: Mon Tue Wed Thu Fri Sat

Etapa 3. Escolha o serviço apropriado que você precisa filtrar na lista suspensa Serviço.

Edit 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 4. Escolha a opção Log apropriada na lista suspensa Log. A opção de log determina se o dispositivo mantém um log do tráfego que corresponde às regras de acesso definidas.

- Pacotes de log correspondentes a essa regra de acesso — O roteador mantém um log que rastreia o serviço selecionado.
- Not Log (Sem registro) — O roteador não mantém registros para a regra de acesso.

Edit 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 5. Na lista suspensa Interface, escolha a interface de origem apropriada. Esta interface é onde a regra de acesso será aplicada.

- LAN — A regra de acesso afeta somente o tráfego da LAN.
- WAN 1 — A regra de acesso afeta somente o tráfego da WAN 1.
- WAN 2 — A regra de acesso afeta somente o tráfego da WAN 2.
- Qualquer — A regra de acesso afeta todo o tráfego em qualquer uma das interfaces do dispositivo.

Edit 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 6. Escolha o tipo de IP de origem apropriado ao qual a regra de acesso é aplicada na lista suspensa IP de origem.

- Qualquer — Qualquer endereço IP da rede do dispositivo tem a regra aplicada a ele.
- Único — Somente um único endereço IP especificado na rede do dispositivo tem a regra aplicada a ele. Insira o endereço IP desejado no campo adjacente.
- Intervalo — Somente um intervalo especificado de endereços IP na rede do dispositivo tem a regra aplicada a eles. Se você escolher Intervalo, precisará inserir o primeiro e o último endereços IP para o intervalo nos campos adjacentes.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

Passo 7. Escolha o tipo de IP de destino apropriado ao qual a regra de acesso é aplicada na lista suspensa disponível.

- Qualquer — Qualquer endereço IP de destino tem a regra aplicada a ele.
- Único — Somente um único endereço IP especificado tem a regra aplicada a ele. Insira o endereço IP desejado no campo adjacente.
- Intervalo — Somente um intervalo especificado de endereços IP fora do alcance da rede do dispositivo tem a regra aplicada a eles. Se você escolher Intervalo, precisará inserir o primeiro e o último endereços IP para o intervalo nos campos adjacentes.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Economizador de tempo: Por padrão, a hora é definida como Sempre. Para aplicar a regra de acesso a uma hora ou dia específicos, siga as etapas 8 a 11. Caso contrário, vá para a Etapa 12.

Etapa 8. Escolha **Intervalo** na lista suspensa, as regras de acesso estão ativas para algumas horas específicas. você precisa inserir o intervalo de tempo para que a regra de acesso seja aplicada.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Etapa 9. Insira a hora em que deseja começar a aplicar a lista de acesso no campo De. O formato da hora é hh:mm.

Etapa 10. Insira a hora em que não deseja mais aplicar a lista de acesso no campo To (Para). O formato da hora é hh:mm.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Etapa 11. Marque a caixa de seleção dos dias específicos em que deseja aplicar a lista de acesso.

Etapa 12. Clique em **Salvar** para salvar as alterações.

Access Rules

IPv4 IPv6

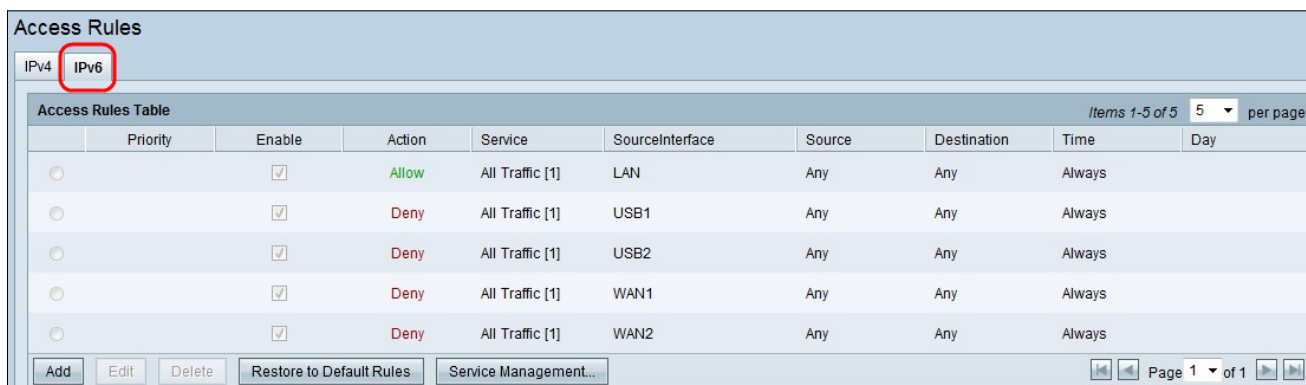
Access Rules Table Items 1-5 of 6 5 ▾

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input checked="" type="radio"/>	1 ▾	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

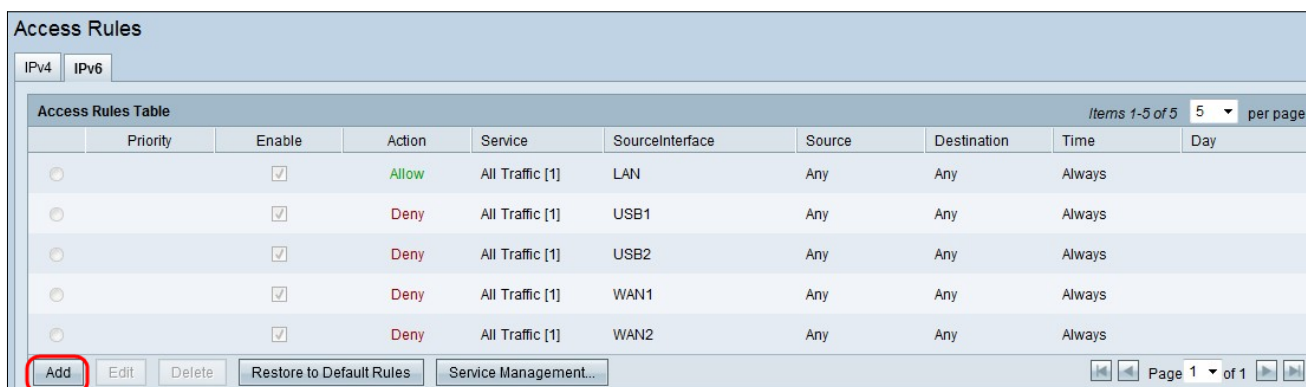
Add Edit Delete Restore to Default Rules Service Management... Page 1 of 2

Etapa 13. (Opcional) Se quiser restaurar as regras padrão, clique em **Restaurar para Regras Padrão**. Todas as regras de acesso configuradas por você são perdidas.

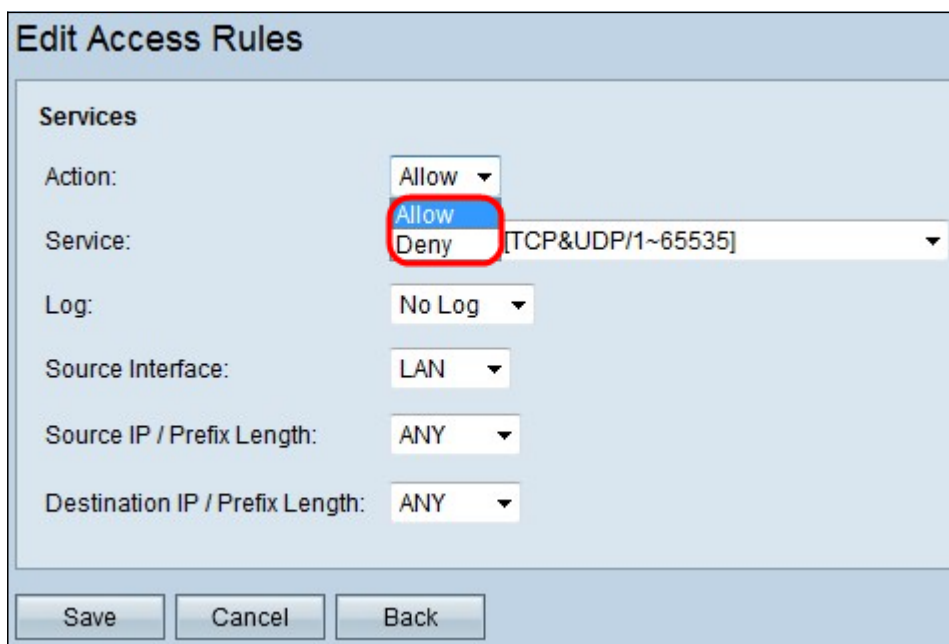
Configuração da regra de acesso em IPv6



Etapa 1. Clique na guia IPv6 para configurar regras de acesso IPv6.



Etapa 2. Clique em Adicionar para adicionar uma nova regra de acesso IPv6. A janela *Editar regras de acesso* é exibida.



Etapa 3. Escolha a opção apropriada na lista suspensa Ação para permitir ou restringir a regra que você precisa configurar. As regras de acesso limitam o acesso à rede, permitindo ou negando o acesso ao tráfego de serviços ou dispositivos específicos.

- Permitir — Permite todo o tráfego.
- Negar — Restringe todo o tráfego.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: All Traffic [TCP&UDP/1~65535]

Source Interface: DNS [UDP/53~53]

Source IP / Prefix Length: FTP [TCP/21~21]

Destination IP / Prefix Length: HTTP [TCP/80~80]

HTTP Secondary [TCP/8080~8080]

HTTPS [TCP/443~443]

HTTPS Secondary [TCP/8443~8443]

TFTP [UDP/69~69]

IMAP [TCP/143~143]

NNTP [TCP/119~119]

POP3 [TCP/110~110]

SNMP [UDP/161~161]

SMTP [TCP/25~25]

TELNET [TCP/23~23]

TELNET Secondary [TCP/8023~8023]

TELNET SSL [TCP/992~992]

DHCP [UDP/67~67]

L2TP [UDP/1701~1701]

PPTP [TCP/1723~1723]

IPSec [UDP/500~500]

Ping [ICMP/255~255]

data [TCP/520~521]

Save Cancel

Etapa 4. Escolha o serviço apropriado que você precisa filtrar na lista suspensa Serviço.

Note: Para permitir todo o tráfego, escolha **All Traffic [TCP&UDP/1~65535]** na lista suspensa de serviços se a ação tiver sido definida para permitir. A lista contém todos os tipos de serviços que você pode querer filtrar.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: No Log

Source Interface: Enabled

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

Etapa 5. Escolha a opção Log apropriada na lista suspensa Log. A opção de log determina se o dispositivo manterá um log do tráfego que corresponda às regras de acesso definidas.

- Habilitado — Permite que o roteador mantenha o rastreamento de log para o serviço selecionado.
- Not Log (Sem registro) — Desativa o roteador para manter o rastreamento de log.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel Back

Etapa 6. Clique na lista suspensa Interface e escolha a interface de origem apropriada. Esta interface é onde a regra de acesso será aplicada.

- LAN — A regra de acesso afeta somente o tráfego da LAN.
- WAN 1 — A regra de acesso afeta somente o tráfego da WAN 1.
- WAN 2 — A regra de acesso afeta somente o tráfego da WAN 2.
- Qualquer — A regra de acesso afeta todo o tráfego em qualquer uma das interfaces do dispositivo.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: ANY

Destination IP / Prefix Length:

Save Cancel Back

Passo 7. Escolha o tipo de IP de origem apropriado ao qual a regra de acesso é aplicada na lista suspensa Tamanho do prefixo/IP de origem.

- ANY — Qualquer pacote recebido de uma rede do dispositivo tem a regra aplicada a ele.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Único — Somente um único endereço IP especificado na rede do dispositivo tem a regra aplicada a ele. Insira o endereço IPv6 desejado no campo adjacente.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Sub-rede — Somente os endereços IP de uma sub-rede têm a regra aplicada a ela. Insira o endereço de rede IPv6 e o comprimento do prefixo da sub-rede desejada nos campos adjacentes.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

- ANY
- Single
- Subnet

Save Cancel Back

Etapa 8. Escolha o tipo de IP de destino apropriado ao qual a regra de acesso é aplicada na lista suspensa IP de destino/comprimento do prefixo.

- Qualquer — Qualquer endereço IP de destino tem a regra aplicada a ele.
- Único — Somente um único endereço IP especificado na rede do dispositivo tem a regra aplicada a ele. Insira o endereço IPv6 desejado.
- Sub-rede — Somente os endereços IP de uma sub-rede têm a regra aplicada a ela. Insira o endereço de rede IPv6 e o comprimento do prefixo da sub-rede desejada nos campos adjacentes.

Etapa 9. Clique em **Salvar** para que as alterações sejam efetivas.

Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)