

Configurar regras de acesso nos roteadores das séries RV160 e RV260

Objetivo

Seu roteador é responsável por receber dados da rede externa e é a primeira linha de defesa em relação à segurança da rede local. Ao habilitar regras de acesso no roteador, você pode filtrar pacotes com base em parâmetros específicos, como endereço IP ou número de porta. Com as etapas fornecidas abaixo, este documento visa guiá-lo sobre como configurar regras de acesso para melhor controlar os pacotes que entram na sua rede. Este documento também destacará algumas práticas recomendadas para o uso de regras de acesso ao seu potencial total para a melhor segurança.

Dispositivos aplicáveis

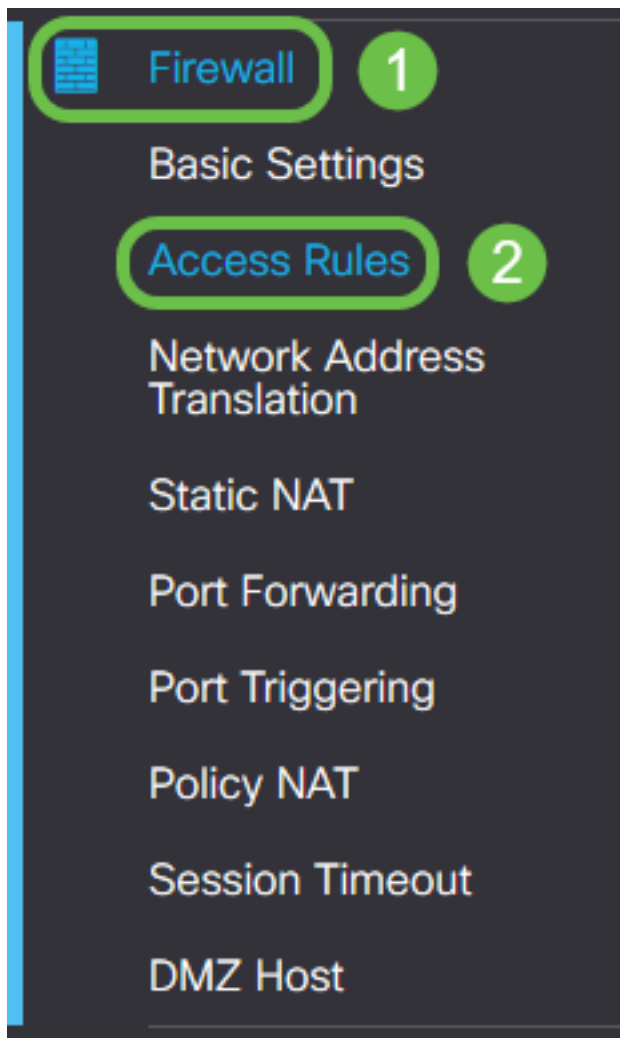
- RV160x
- RV260x

Versão de software

- 1.0.00.13

Configurar regras de acesso

Etapa 1. No painel de navegação no lado esquerdo do utilitário de configuração, selecione **Firewall > Access Rules**.



A página Regras de acesso é exibida. Nesta página, há tabelas contendo listas de regras de acesso e seus atributos para IPv4 e IPv6, respectivamente. A partir daqui, você pode adicionar uma nova regra de acesso, editar uma regra existente ou remover uma regra existente.

Adicionar/editar uma regra de acesso

Etapa 2. Para adicionar uma nova regra de acesso, clique no ícone azul para adicionar à tabela Regras de acesso IPv4 ou Regras de acesso IPv6 dependendo do protocolo ao qual você gostaria que a regra fosse aplicada. Nesse caso, o IPv4 é usado.

IPv4 Access Rules Table



Para editar uma entrada existente, marque a caixa de seleção ao lado da regra de acesso que deseja modificar. Em seguida, selecione o ícone de edição azul na parte superior da tabela correspondente. Somente uma regra pode ser selecionada por vez para edição.

IPv4 Access Rules Table

<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

A página *Adicionar/Editar regras de acesso* é exibida.

Etapa 3. Marque/desmarque a caixa de seleção *Rule Status* para ativar ou desativar a regra de acesso durante a operação. Isso é útil quando você tiver uma regra de acesso que deseja salvar para ser aplicada posteriormente.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Etapa 4. No campo *Ação*, selecione se a regra deve permitir ou negar o acesso ao tráfego de rede de entrada a ser especificado.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Note: Recomenda-se que a melhor segurança defina regras de acesso que permitam apenas o tráfego que você espera receber, em vez de tentar apenas negar tráfego indesejável. Isso protegerá melhor a sua rede contra ameaças desconhecidas.

Etapa 5. No campo *Serviços*, selecione no menu suspenso o tipo de serviço de rede ao qual você deseja que a regra de acesso seja aplicada.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Note: O botão de opção IPv4 ou IPv6 é selecionado automaticamente com base na tabela à qual você escolheu aplicar a regra de acesso na página *Regras de Acesso*.

Etapa 6. Selecione no campo *Log* se deseja que o roteador gere uma mensagem de log quando os pacotes que entram na rede estiverem correspondendo às regras aplicadas.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Passo 7. Na lista suspensa *Interface de Origem*, selecione a interface de rede para os pacotes de entrada aos quais a regra de acesso será aplicada.

Log: Always Never

Source Interface: Any

Source Address:

Destination Interface: Any

Destination Address: Any

Etapa 8. Selecione na lista suspensa *Endereço de origem* o tipo de endereço de entrada ao qual a regra de acesso será aplicada. As opções são as seguintes:

- Qualquer - A regra será aplicada a qualquer endereço IP de entrada
- Único - A regra será aplicada a um único endereço IP definido
- Sub-rede - A regra será aplicada a uma sub-rede definida de uma rede
- Intervalo de IPs - A regra será aplicada a um intervalo definido de endereços IP

Note: Se você selecionar Single (Única), Subnet (Sub-rede) ou IP Range (Intervalo de IP), os campos correspondentes serão exibidos à direita do menu suspenso, no qual você pode inserir os detalhes do endereço. Neste exemplo, é inserido um Intervalo de IP para demonstrar.

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any

Destination Address: IP Range

Etapa 9. Na lista suspensa *Interface de destino*, selecione a interface de rede para os pacotes de

saída aos quais a regra de acesso será aplicada.

The screenshot shows a configuration form with the following fields: Log (radio buttons for Always and Never), Source Interface (dropdown: Any), Source Address (dropdown: Any), Destination Interface (dropdown: Any), and Destination Address. A green rounded rectangle highlights the Destination Interface dropdown menu, which is open and shows options: WAN, USB, VLAN1, and Any (highlighted in blue). Below the form is a 'Schedule' section.

Etapa 10. Selecione na lista suspensa *Endereço de destino* o tipo de endereço de saída ao qual a regra de acesso será aplicada. As opções são as seguintes:

- Qualquer - A regra será aplicada a qualquer endereço IP de saída
- Único - A regra será aplicada a um único endereço IP definido
- Sub-rede - A regra será aplicada a uma sub-rede definida de uma rede
- Intervalo de IPs - A regra será aplicada a um intervalo definido de endereços IP

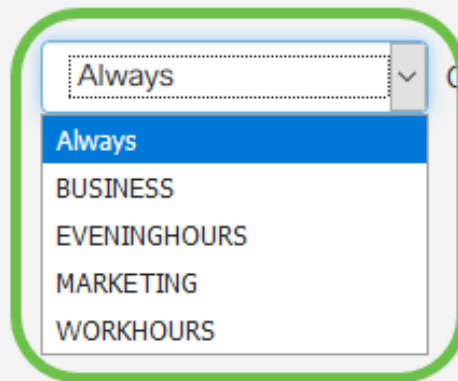
Note: Se você selecionar Single (Única), Subnet (Sub-rede) ou IP Range (Intervalo de IP), os campos correspondentes serão exibidos à direita do menu suspenso, no qual você pode inserir os detalhes do endereço. Neste exemplo, uma sub-rede é inserida para demonstrar.

The screenshot shows a configuration form with the following fields: Destination Interface (dropdown: Any), Destination Address (dropdown: Subnet, input: 1.2.3.4 / 16, text: (1.2.3.4 / 32)), Schedule Name (dropdown: Always), and a link: Click here to configure the schedules. A green rounded rectangle highlights the Destination Address dropdown menu, which is open and shows options: Any, Single, Subnet (highlighted in blue), and IP Range.

Etapa 11. Na lista suspensa *Nome da programação*, selecione a programação de tempo à qual deseja que a regra de acesso seja aplicada.

Schedule

Schedule Name:

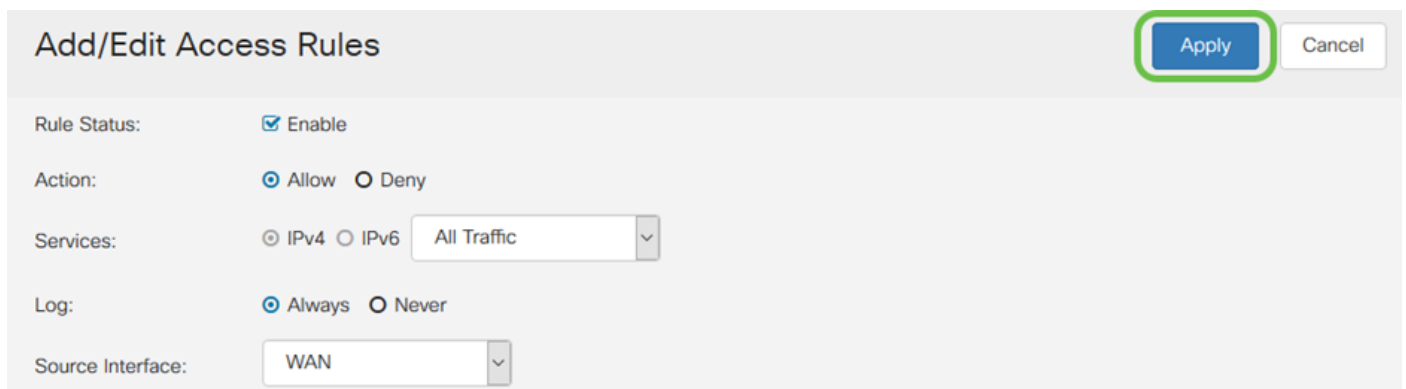
A dropdown menu with a green border. The selected item is 'Always'. Other options listed are BUSINESS, EVENINGHOURS, MARKETING, and WORKHOURS.

Click [here](#) to configure the schedules.

Note: Para aumentar a segurança, é recomendável restringir o acesso não crítico à rede ao horário comercial para garantir que conexões indesejadas sejam negadas quando sua empresa não estiver em operação.

Note: Clique no link à direita da lista suspensa *Nome da programação* se desejar configurar os horários de agendamento para regras de acesso. Mais informações sobre como configurar esses agendamentos [aqui](#).

Etapa 12. Quando estiver satisfeito com a configuração da regra de acesso, clique em **Apply** para confirmar.


A configuration form titled 'Add/Edit Access Rules'. It includes fields for Rule Status (checked 'Enable'), Action (radio buttons for 'Allow' and 'Deny'), Services (radio buttons for 'IPv4' and 'IPv6', and a dropdown for 'All Traffic'), Log (radio buttons for 'Always' and 'Never'), and Source Interface (dropdown for 'WAN'). A blue 'Apply' button and a grey 'Cancel' button are at the top right.

Você será retornado para a página principal *Regras de acesso*.

Note: Quando uma nova regra de acesso é criada, sua prioridade é colocada na parte inferior da lista. Isso significa que, se uma regra de acesso entrar em conflito com outra em um parâmetro específico, as restrições da regra de prioridade mais alta terão precedência. Para mover uma regra em prioridade para cima ou para baixo, você pode usar as setas azuis localizadas na coluna Configurar.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

Etapa 13 (Opcional). Se desejar retornar a lista de regras de acesso ao padrão, clique em **Restaurar padrões** no canto superior direito da página.

Access Rules

Apply

Restore Defaults

Remover uma regra de acesso

Etapa 14. Para remover uma regra de acesso da lista, basta marcar a caixa de seleção da regra correspondente que deseja remover. Em seguida, selecione o ícone da lixeira azul na parte superior da lista. Várias entradas da regra de acesso podem ser removidas de uma só vez.

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	▲ ▼

Gerenciamento de serviço

O gerenciamento de serviços permite adicionar ou editar serviços de rede existentes por número de porta, protocolo e outros detalhes. Esses serviços de rede estarão disponíveis na lista suspensa Serviços ao configurar as regras de acesso. Através do menu de configuração da lista de gestão de serviços, pode criar serviços personalizados que podem ser aplicados às regras de acesso para um controle mais rigoroso do tráfego que entra na sua rede. Para saber mais sobre como configurar o Gerenciamento de serviços, clique [aqui](#).

Conclusão

As regras de acesso quando aplicadas adequadamente são uma ferramenta valiosa para proteger sua conexão WAN. Com o guia acima e as práticas discutidas, você deve ter tudo o que precisa para configurar corretamente as regras de acesso seguro para seu roteador RV160x ou RV260x.