Configurar regras do acesso em RV160 e em Roteadores do RV260 Series

Objetivo

Seu roteador é responsável para receber dados da rede externa e é a primeira linha de defesa quando se trata de sua Segurança da rede local. Permitindo o acesso ordena em seu roteador, você pode filtrar os pacotes baseados em parâmetros específicos tais como o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o número de porta. Com as etapas forneceu abaixo, alvos deste documento para guiá-lo em como configurar regras do acesso para controlar melhor os pacotes que incorporam sua rede. Este documento igualmente destacará alguns melhores prática para usar regras do acesso a seu potencial completo para a melhor Segurança.

Dispositivos aplicáveis

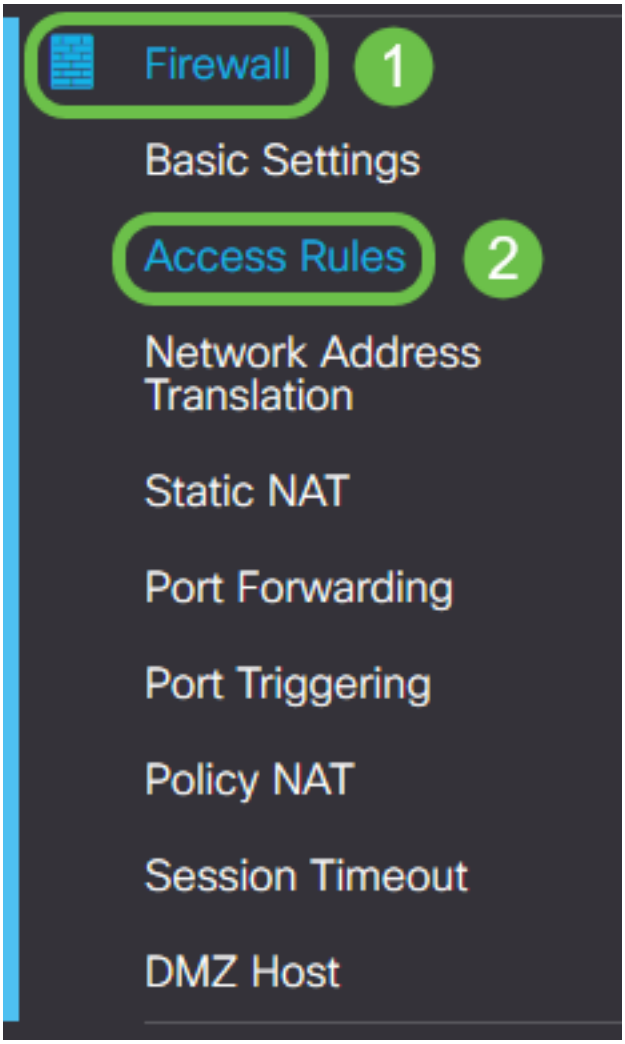
- RV160x
- RV260x

Versão de software

- 1.0.00.13

Configurar regras do acesso

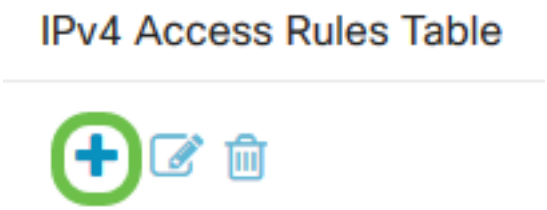
Etapa1. Do painel de navegação no lado esquerdo do utilitário de configuração, selecione **regras do Firewall > do acesso.**



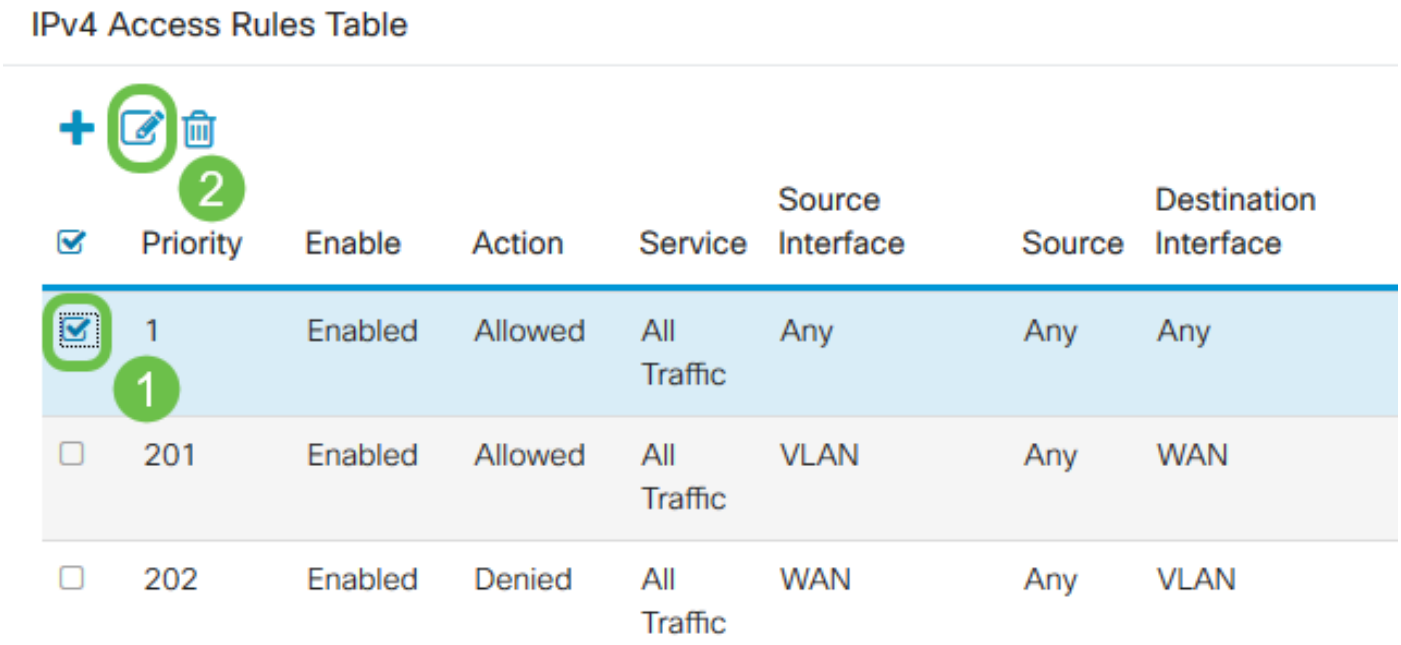
A página das regras do acesso publica-se. Nesta página há tabelas que contêm lista de regras do acesso e de seus atributos para o IPv4 e o IPv6 respectivamente. Aqui de você pode adicionar uma regra nova do acesso, editar uma regra existente, ou remover uma regra existente.

Adicionar/edite uma regra do acesso

Etapa 2. Para adicionar uma regra nova do acesso, clique o ícone azul para adicionar na tabela das regras do acesso do IPv4 ou das regras do acesso do IPv6 segundo que protocolo você como a regra se aplicaria. Nesta instância, o IPv4 é usado.

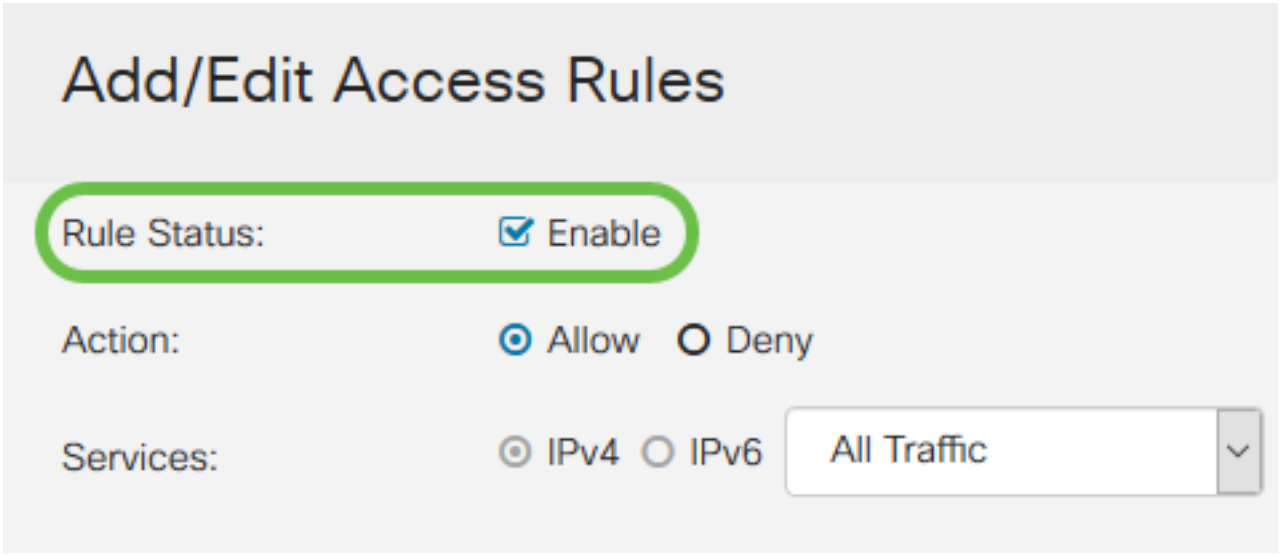


Para editar uma entrada existente, selecione a caixa de seleção ao lado da regra do acesso que você gostaria de alterar. Selecione então o azul editam o ícone na parte superior da tabela correspondente. Somente uma regra pode ser selecionada em um momento para editar.

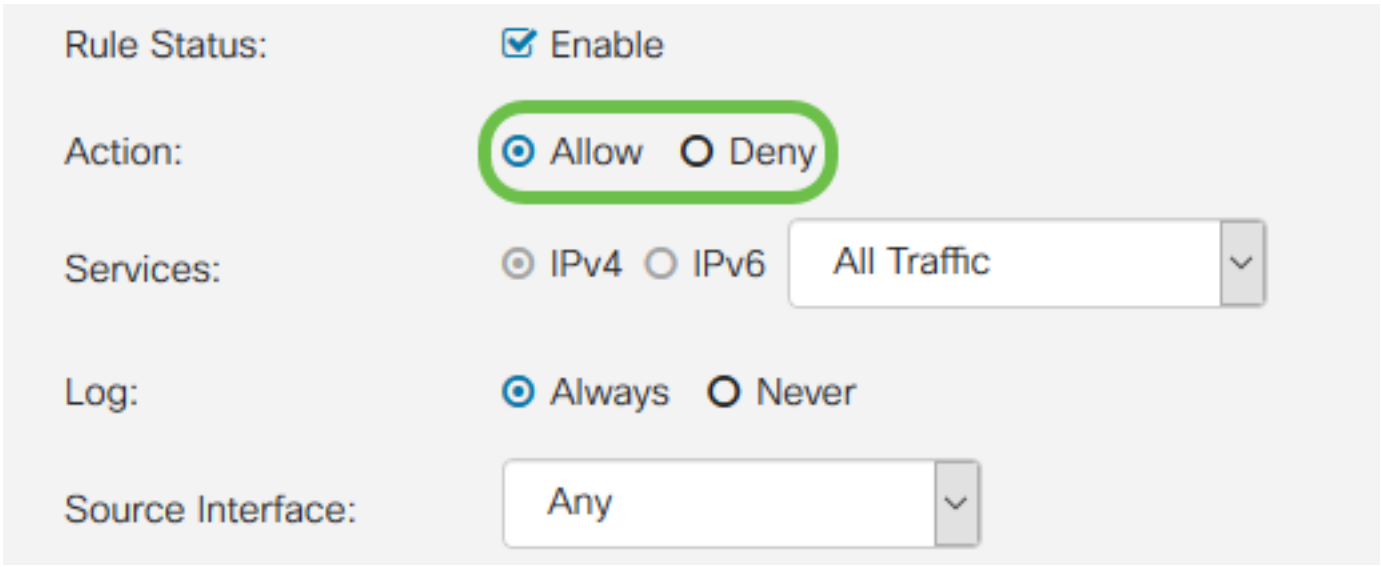


Adicionar/edita regras que do acesso a página se publica.

Etapa 3. Verifique/desmarcar a caixa de seleção para que o estado da regra permita ou desabilitem a regra do acesso durante a operação. Isto é útil quando você tem uma regra do acesso que você goste de salvar para se aplicar em um outro dia.

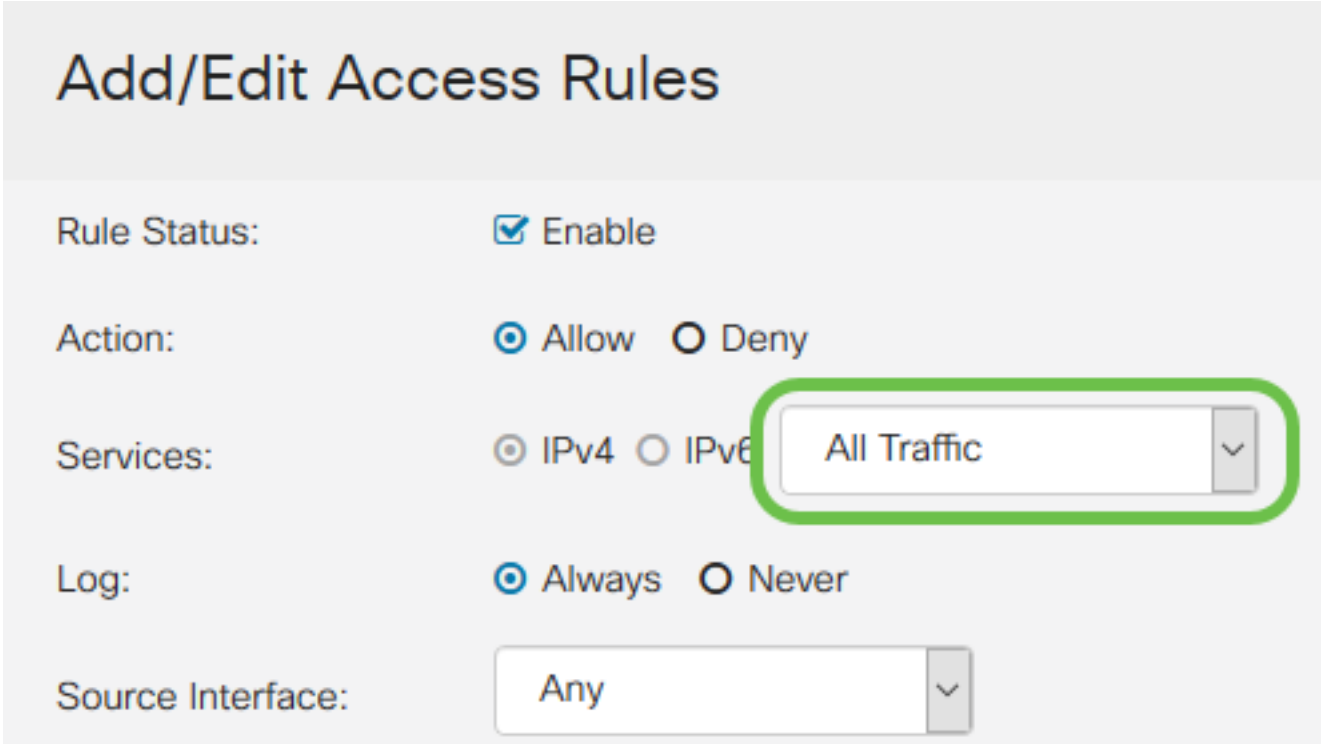


Etapa 4. Do campo de *ação*, selecione se a regra deve permitir ou negar o acesso ao tráfego de rede entrante a ser especificado.



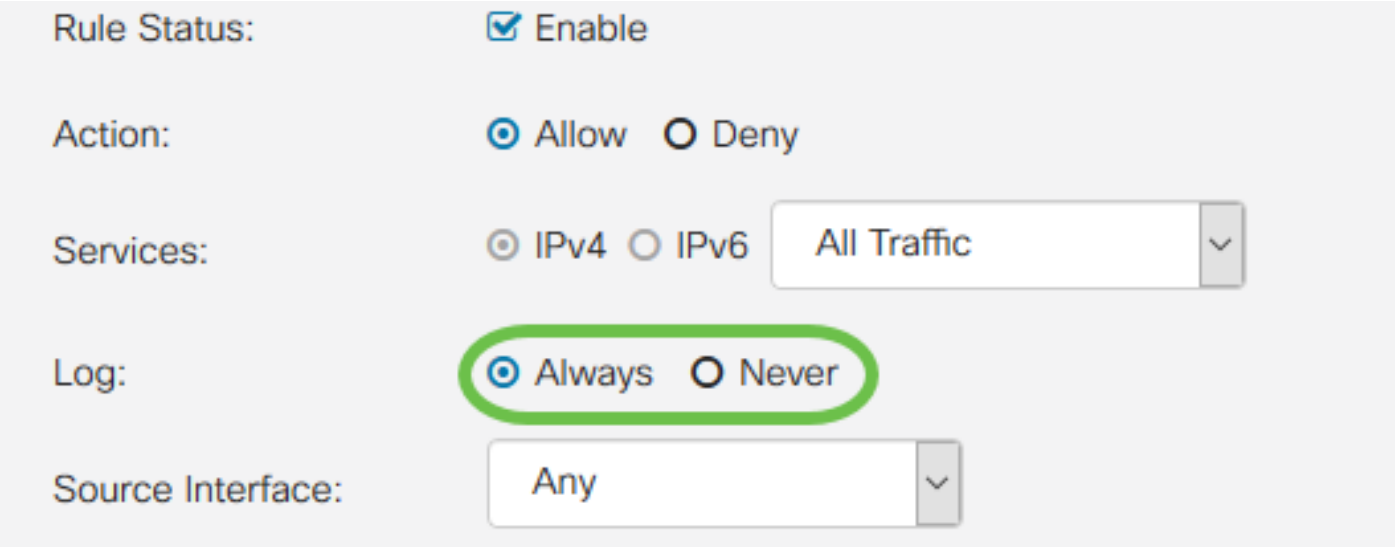
Nota: Recomenda-se para que a melhor Segurança ajuste as regras do acesso que permitem somente o tráfego que você espera receber, um pouco do que tentando negar somente o tráfego indesejável. Isto protegerá melhor sua rede contra ameaças desconhecidas.

Etapa 5. *Nos serviços* coloque, selecione do menu suspenso o serviço que do tipo de rede você como a regra do acesso se aplicaria a.

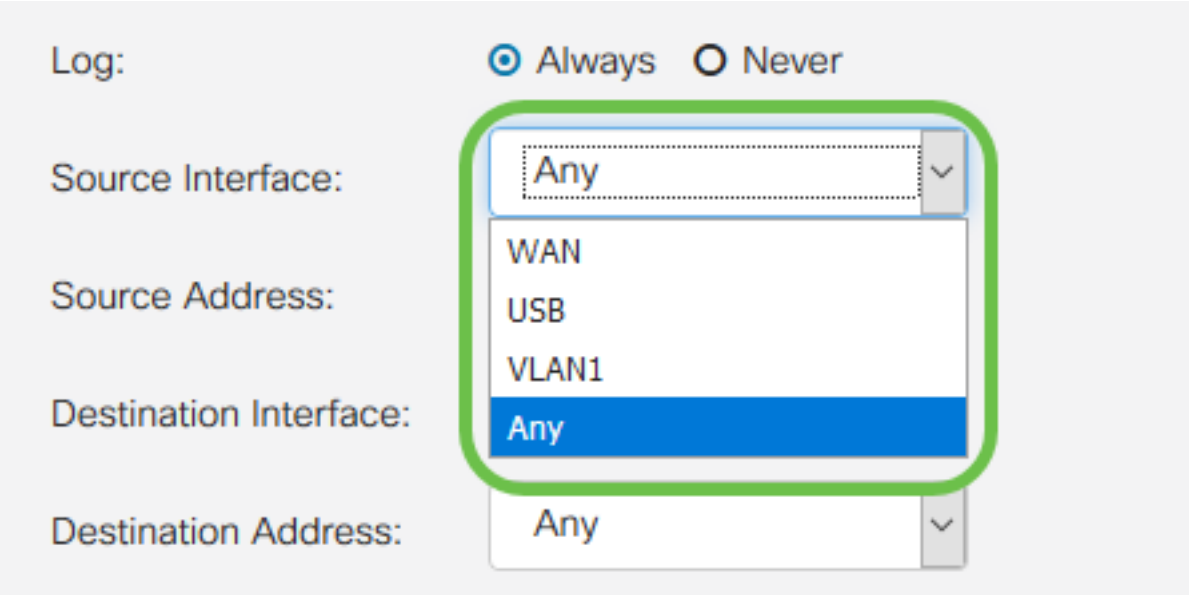


Nota: O botão de rádio do IPv4 ou do IPv6 é selecionado automaticamente com base na tabela que você escolheu aplicar a regra do acesso da página das *regras do acesso*.

Etapa 6. Selecione do campo do *log* se você como o roteador geraria os pacotes de um mensagem de registro uma vez que incorporam sua rede está combinando as regras aplicadas.



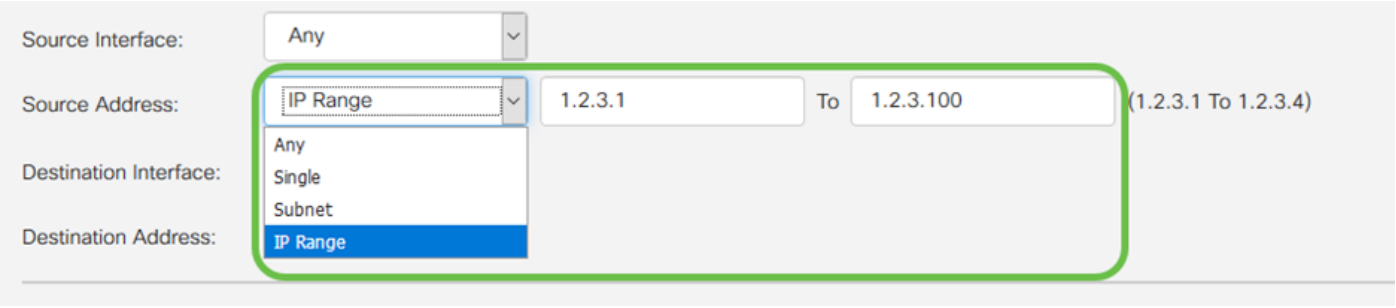
Passo 7. Da lista de drop-down da *interface de origem*, selecione a interface de rede para os pacotes recebidos que a regra do acesso se aplicará para.



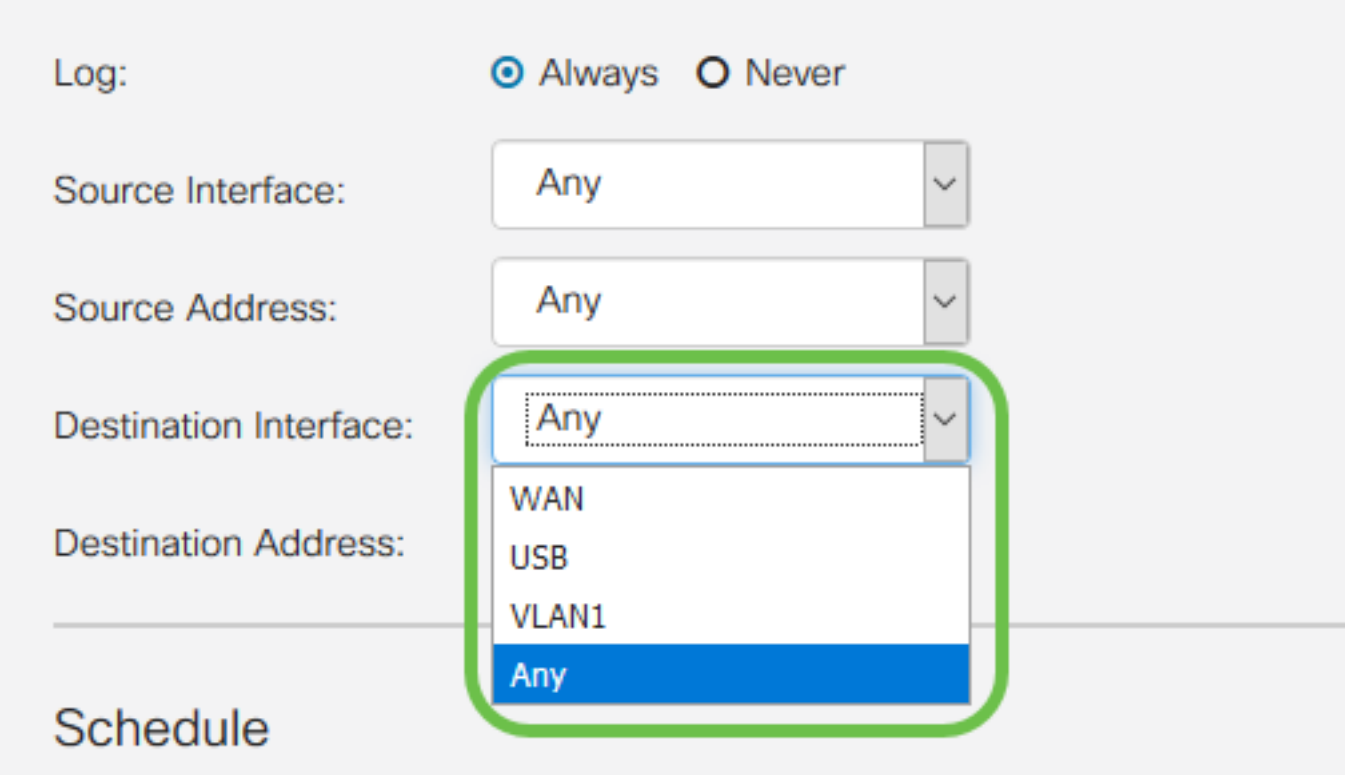
Etapa 8. Selecione da lista de drop-down do *endereço de origem o* tipo de endereço que entrante a regra do acesso se aplicará a. As opções são como segue:

- Alguns - A regra aplicar-se-á a todos os endereços IP de Um ou Mais Servidores Cisco ICM NT entrantes
- Único - A regra aplicar-se-á a um único endereço IP de Um ou Mais Servidores Cisco ICM NT definido
- Sub-rede - A regra aplicar-se-á a uma sub-rede definida de uma rede
- Escala IP - A regra aplicar-se-á a uma escala definida dos endereços IP de Um ou Mais Servidores Cisco ICM NT

Nota: Se você seleciona único, a sub-rede, ou a escala IP, campos correspondentes aparecerão à direita do menu suspenso onde você pode incorporar detalhes do endereço. Neste exemplo uma escala IP é incorporada para demonstrar.



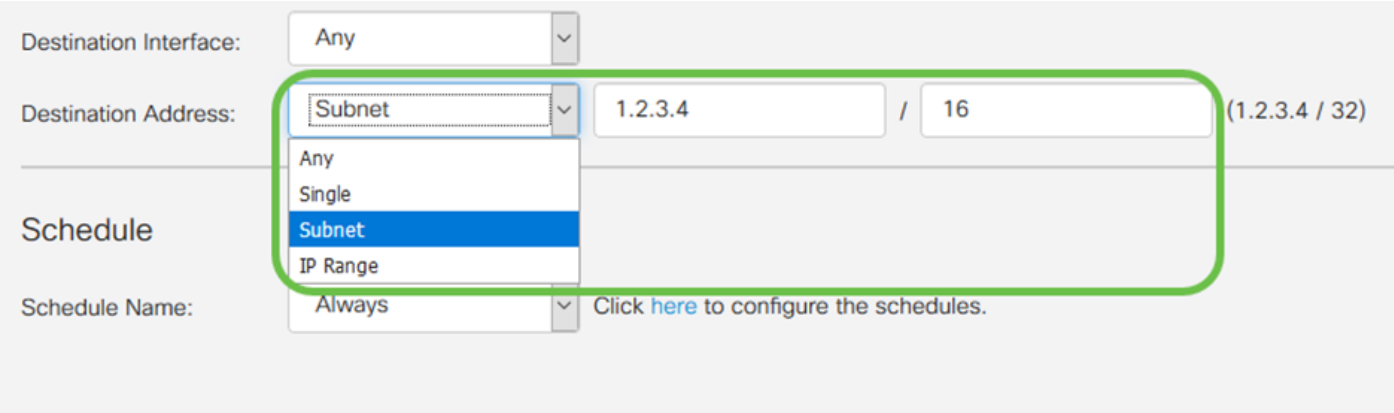
Etapa 9. Da lista de drop-down da *interface de destino*, selecione a interface de rede para os pacotes de saída que a regra do acesso se aplicará para.



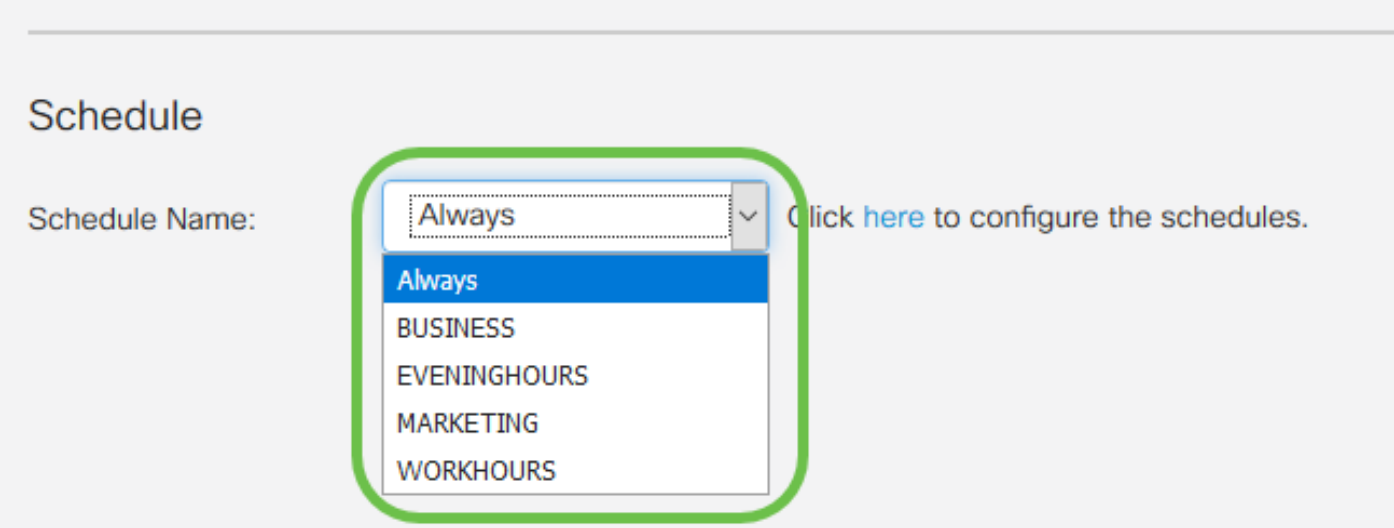
Etapa 10. Selecione da lista de drop-down do *endereço de destino o* tipo de endereço que que parte a regra do acesso se aplicará a. As opções são como segue:

- Alguns - A regra aplicar-se-á a todos os endereços IP de Um ou Mais Servidores Cisco ICM NT que parte
- Único - A regra aplicar-se-á a um único endereço IP de Um ou Mais Servidores Cisco ICM NT definido
- Sub-rede - A regra aplicar-se-á a uma sub-rede definida de uma rede
- Escala IP - A regra aplicar-se-á a uma escala definida dos endereços IP de Um ou Mais Servidores Cisco ICM NT

Nota: Se você seleciona único, a sub-rede, ou a escala IP, campos correspondentes aparecerão à direita do menu suspenso onde você pode incorporar detalhes do endereço. Neste exemplo uma sub-rede é incorporada para demonstrar.



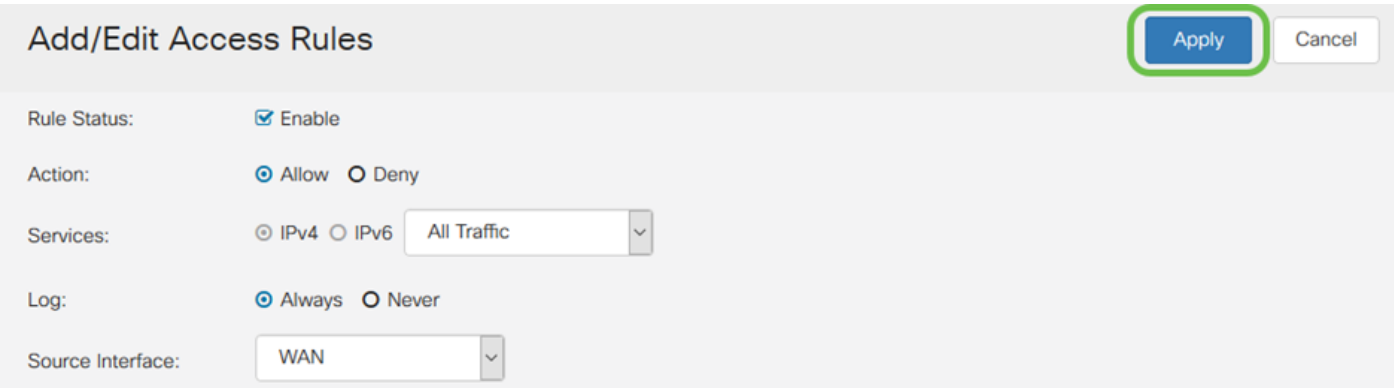
Etapa 11. Da lista de drop-down do *nome da programação*, selecione o horário que você como a regra do acesso se aplicaria a.



Nota: Para a segurança aumentada, é um melhor prática restringir o acesso de rede NON-crítico às horas de negócio para assegurar-se de que as conexões indesejadas estejam negadas quando seu negócio não está na operação.

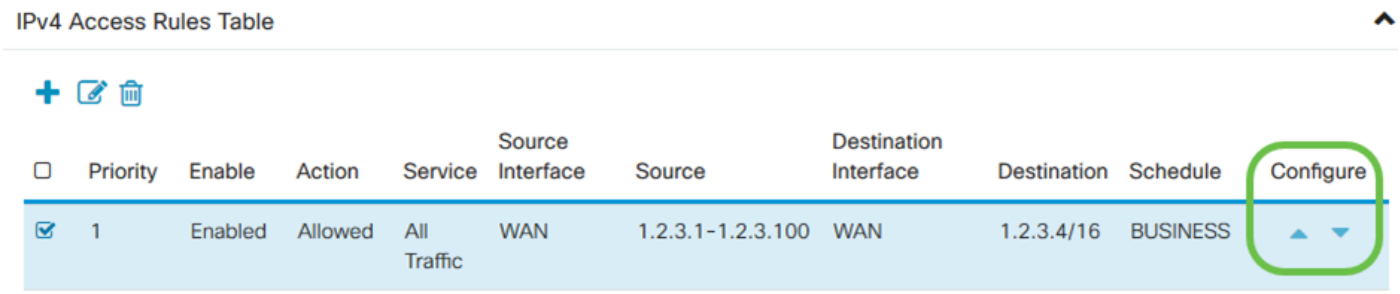
Nota: Clique o link à direita da gota-para baixo do *nome da programação* se você gostaria de configurar os tempos da programação para regras do acesso. Mais informação pode ser encontrada em como configurar aqui estas programações.

Etapa 12. Quando você é satisfeito com a configuração da regra do acesso, o clique **aplica-se** para confirmar.

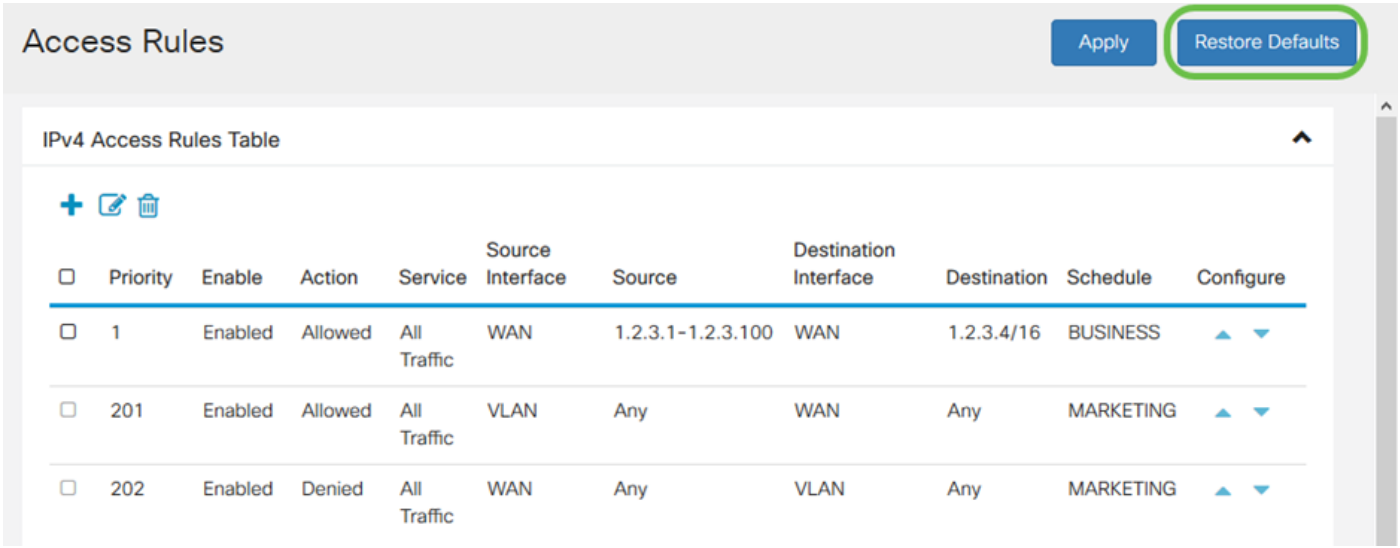


Você será retornado agora à página principal das *regras do acesso*.

Nota: Quando uma regra nova do acesso é criada, sua prioridade está colocada na parte inferior da lista. Isto significa que se uma regra do acesso opõe à outra em um parâmetro específico, as limitações da regra mais prioritária tomarão a precedência. Para mover para cima ou para baixo uma regra na prioridade, você pode usar as setas azul situadas na coluna configurar.

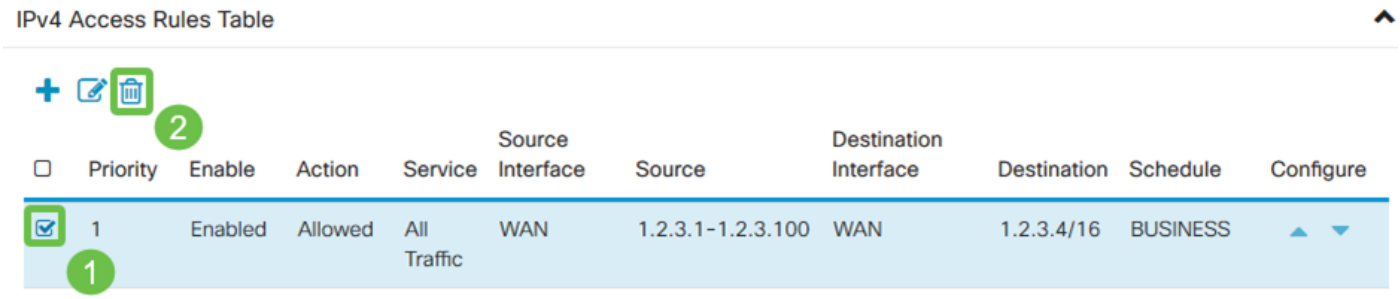


Etapa 13 (opcional). Se você gostaria de retornar o acesso ordena a lista para optar, para clicar **padrões da restauração** no canto superior direito da página.



Remova uma regra do acesso

Etapa 14. Para remover uma regra do acesso da lista, selecione simplesmente a caixa de seleção para a regra que correspondente você gostaria de remover. Selecione então o ícone azul do balde do lixo na parte superior da lista. As entradas da regra do acesso múltiplo podem ser removidas imediatamente.



Gerenciamento de serviço

O Gerenciamento do serviço permite que você adicione ou edite serviços de rede existentes por seu número de porta, por protocolo, e por outros detalhes. Este o servicescwill da rede esteja disponível na gota-para baixo dos serviços ao configurar o acesso ordena. Através do menu de configuração da lista do Gerenciamento do serviço, você pode criar os serviços feitos sob encomenda que podem então ser aplicados às regras do acesso para o controle mais fino sobre o tráfego que incorpora sua rede. Para aprender mais sobre como configurar o Gerenciamento do serviço, clique aqui.

Conclusão

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