Configuração de uma Regra de Acesso IPv4 em Roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Uma regra de acesso ajuda o roteador a determinar, com base nos requisitos do usuário, qual tráfego tem permissão para passar e qual tráfego deve ser negado pelo firewall. Isso ajuda a adicionar segurança ao roteador.

Este documento explica o procedimento para adicionar ou excluir uma regra de acesso nos RV016, RV042, RV042G e RV082 VPN Routers.

Dispositivos aplicáveis

- â€¢RV016
- â€¢RV042
- â€¢RV042G
- â€¢RV082

Versão de software

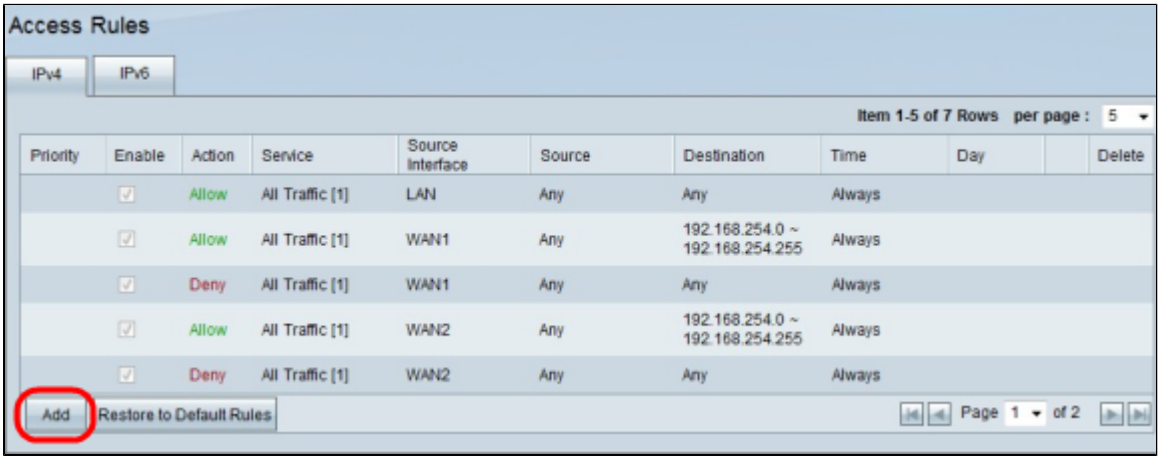
- â€¢4.2.1.02

Gerenciar Regras de Acesso IPv4

O agendamento de regras de acesso IPv4 é uma configuração opcional.

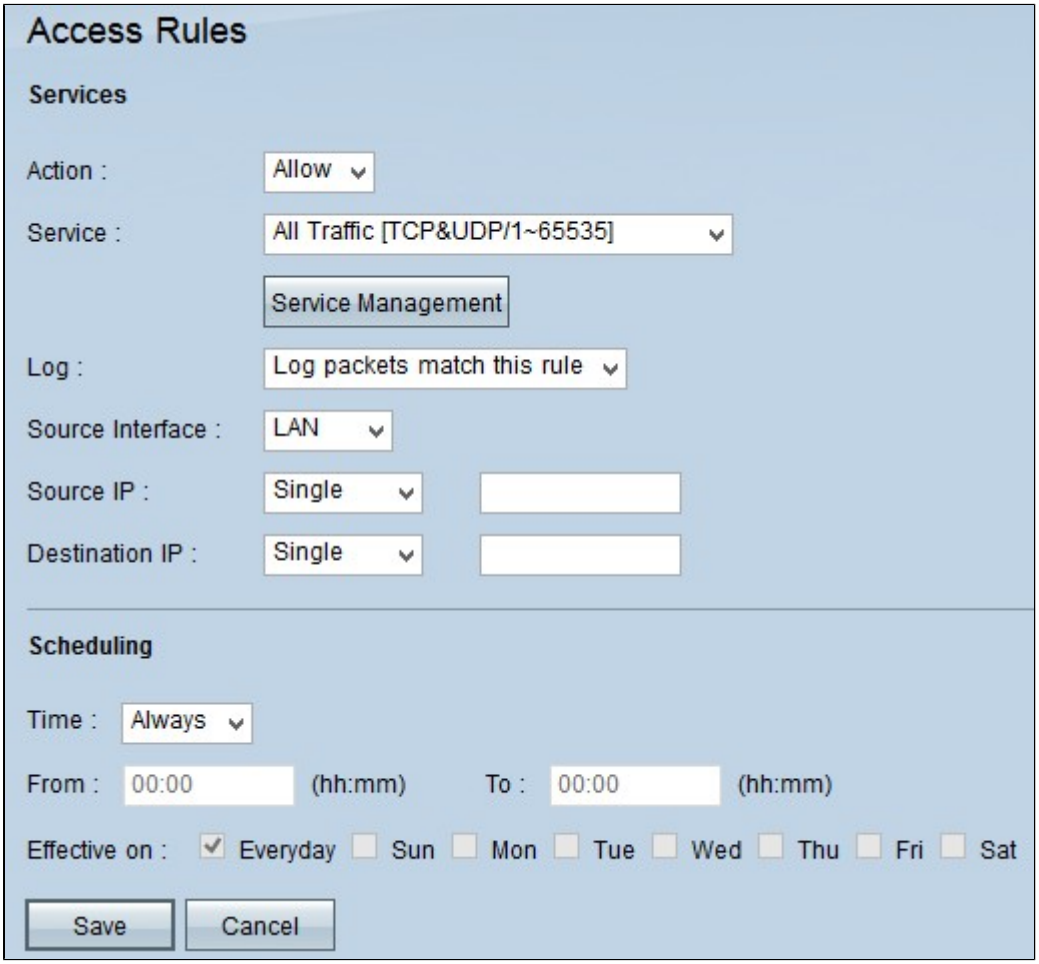
Adicionar ou Excluir Regras de Acesso IPv4

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Firewall > Access Rules**. A página *IPv4 Access Rules* é aberta. Clique em Add.



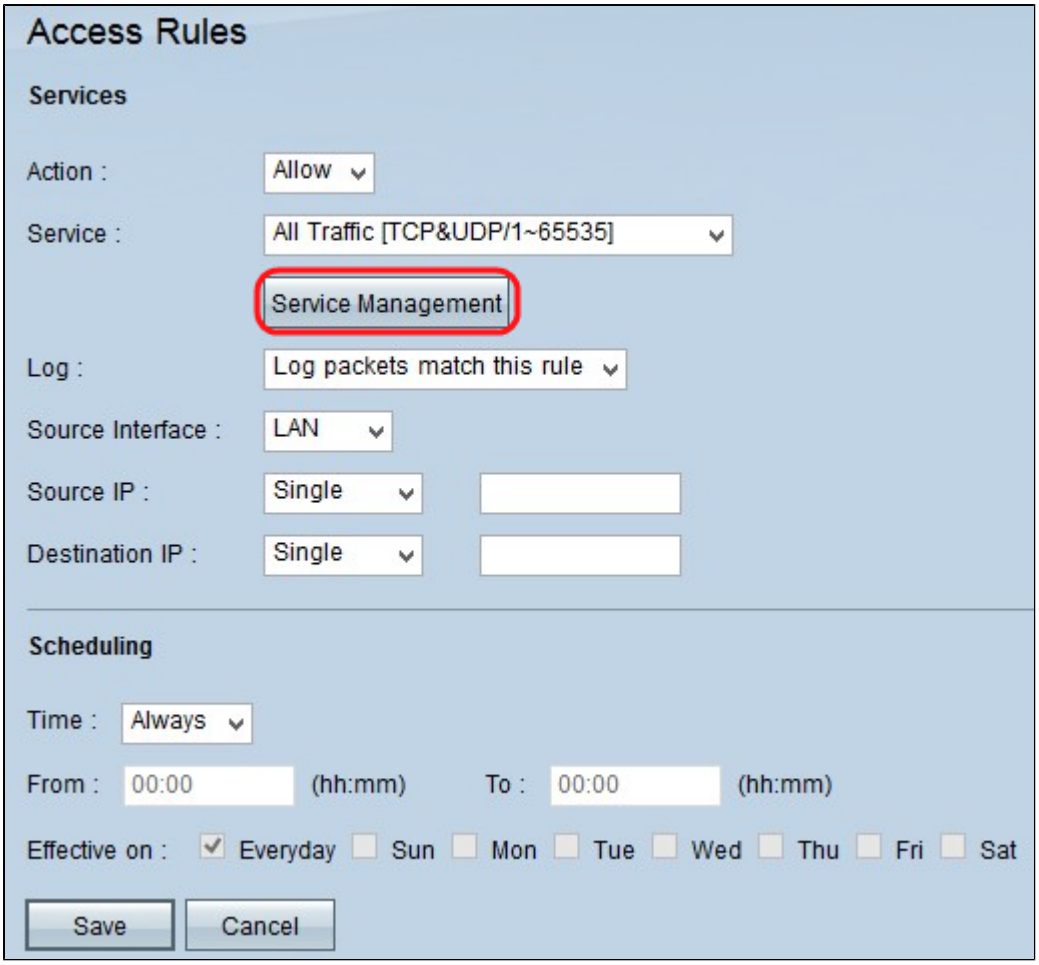
Etapa 2. A página *Access Rules Service* é aberta. Na lista suspensa Ação, escolha **Permitir** para permitir o

tráfego. Caso contrário, escolha **Negar** para negar o tráfego.



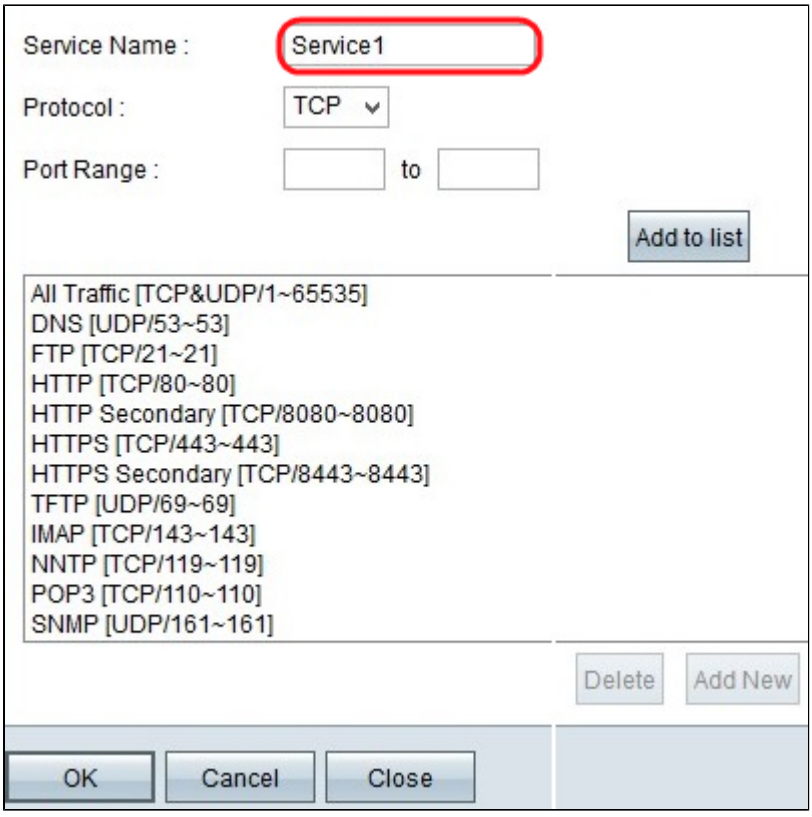
Etapa 3. Escolha o serviço apropriado na lista suspensa Serviço. Se o serviço apropriado não estiver disponível, clique em **Gerenciamento de serviços.**

Observação: se o serviço desejado estiver disponível, vá para a Etapa 6.



Etapa 4.

Uma nova janela é exibida. Digite um nome de serviço no campo Nome do serviço.

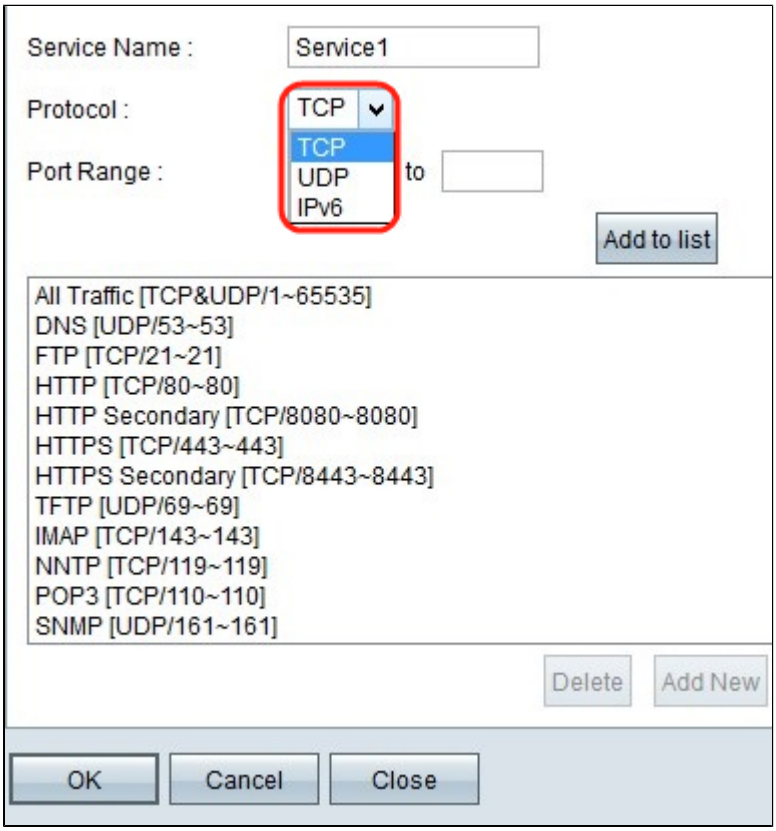


Etapa 5. Escolha o tipo de protocolo apropriado na lista suspensa Protocolo.

· TCP (Transmission Control Protocol) â€” Um protocolo da camada de transporte usado por aplicativos que exigem entrega garantida.

· UDP (User Datagram Protocol) â€” usa soquetes de datagramas para estabelecer comunicações host a host. Ele é mais rápido que o TCP, mas não tem tanta probabilidade de ser entregue com êxito.

· IPv6 (Internet Protocol version 6) â€” Direciona o tráfego da Internet entre hosts em pacotes que são roteados através de redes especificadas por endereços de roteamento.

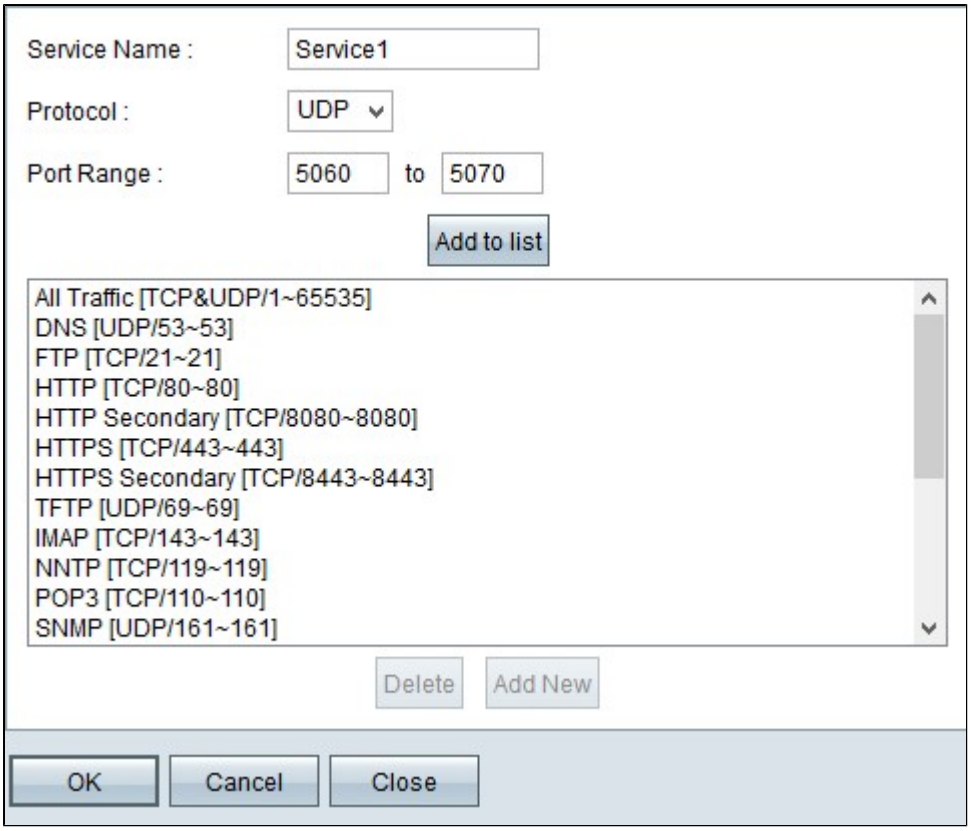


Etapa 6. Insira o intervalo de portas nos campos Port Range (Intervalo de portas). Esse intervalo depende do protocolo escolhido.

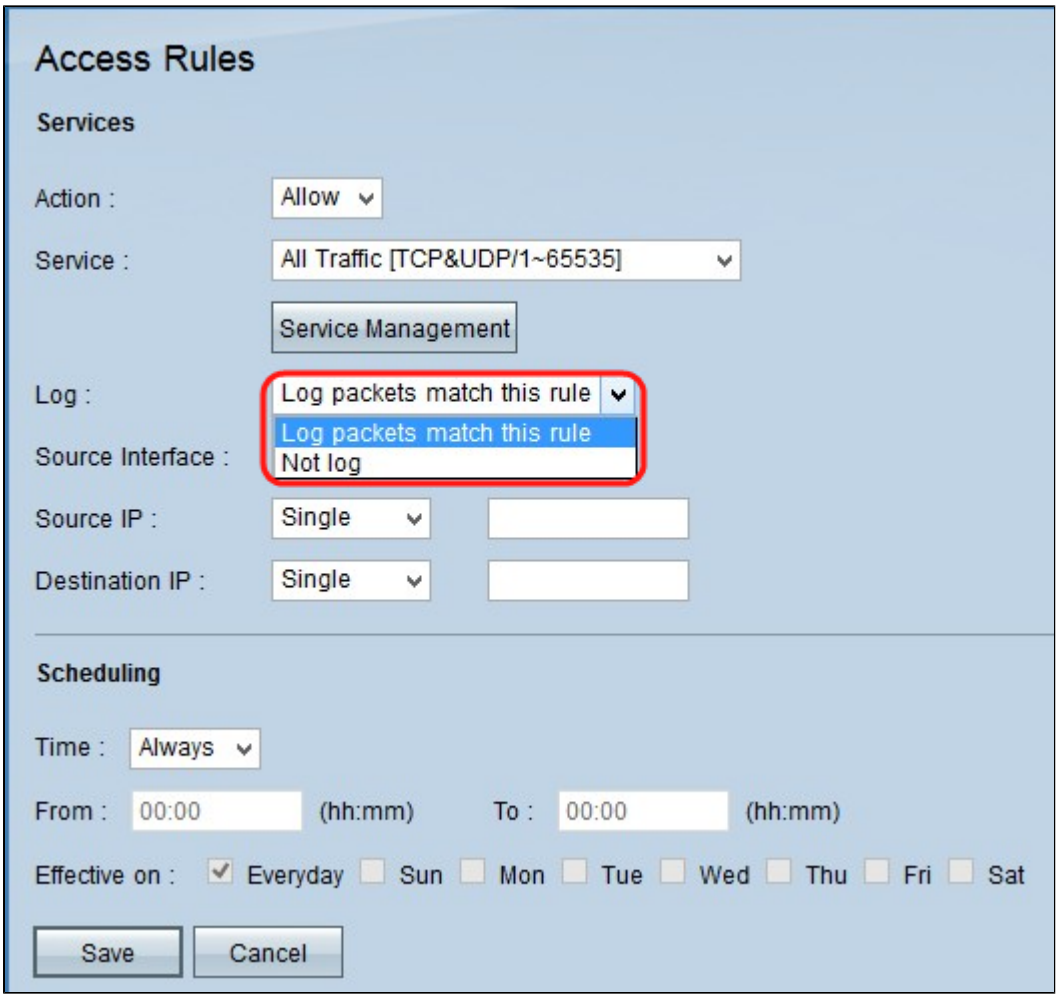
Clique em **Adicionar à lista**. Isso adiciona o Serviço à lista suspensa Serviço.

Outras opções aqui incluem **Delete**, **Update** ou **Add New**.

Click **OK**. Isso fecha a janela e leva o usuário de volta à página *Access Rule Service*.



Passo 7. Na lista suspensa Log, escolha **Log packets** match this rule para registrar os pacotes recebidos que correspondem à regra de acesso. Caso contrário, escolha **Não registrar**.



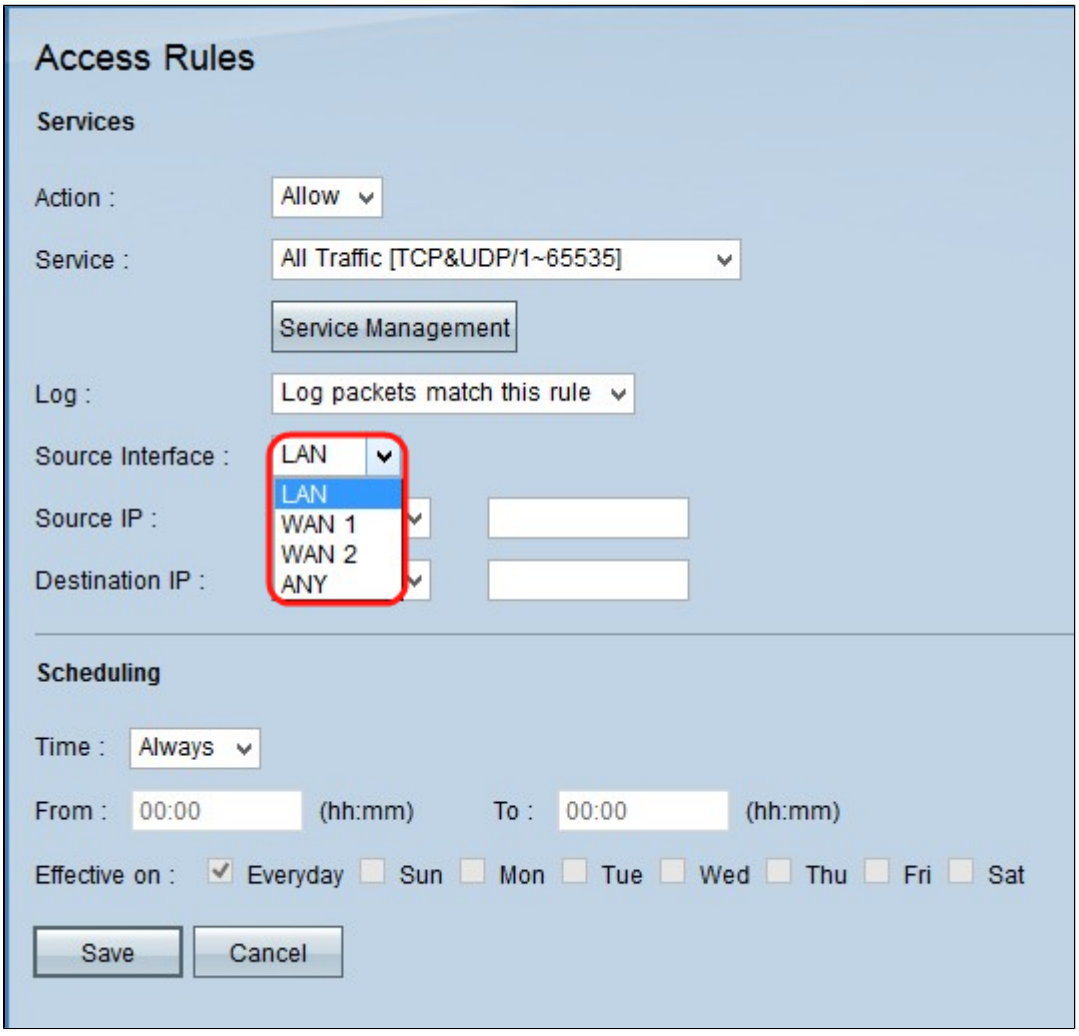
Etapa 8. Escolha a interface afetada por esta regra na lista suspensa Interface de origem. A interface de origem é a interface a partir da qual o tráfego é iniciado.

· LAN â€" A rede local do roteador.

· WAN1 â€" A rede de longa distância ou a rede a partir da qual o roteador obtém a Internet do ISP ou do roteador do próximo salto.

· WAN2 â€" O mesmo que WAN1, exceto que é uma rede secundária.

· ANY â€" Permite que qualquer interface seja usada.

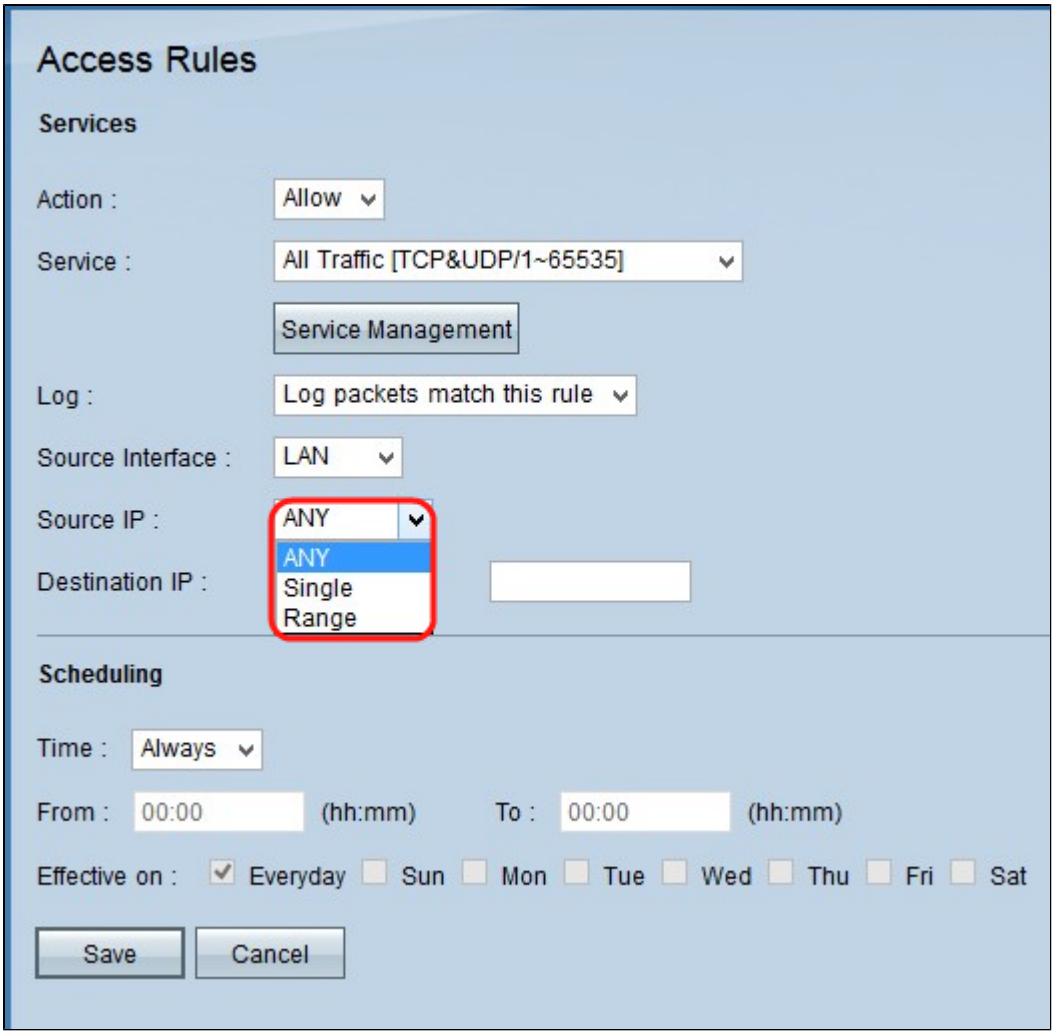


Etapa 9. Na lista suspensa IP de origem, escolha uma opção para especificar o intervalo de endereços IP de origem que devem ser permitidos ou negados pela interface. Os pacotes que chegam à interface são verificados pelo IP origem e pelo IP destino.

· Qualquer â€" A regra de acesso será aplicada a todo o tráfego da interface de origem. Não haverá campos disponíveis à direita da lista suspensa.

· Único â€" A regra de acesso será aplicada em um único endereço IP da interface de origem. Insira o endereço IP desejado no campo de endereço.

· Intervalo â€" A regra de acesso será aplicada em uma rede de sub-rede a partir da interface de origem. Insira o endereço IP e o comprimento do prefixo.



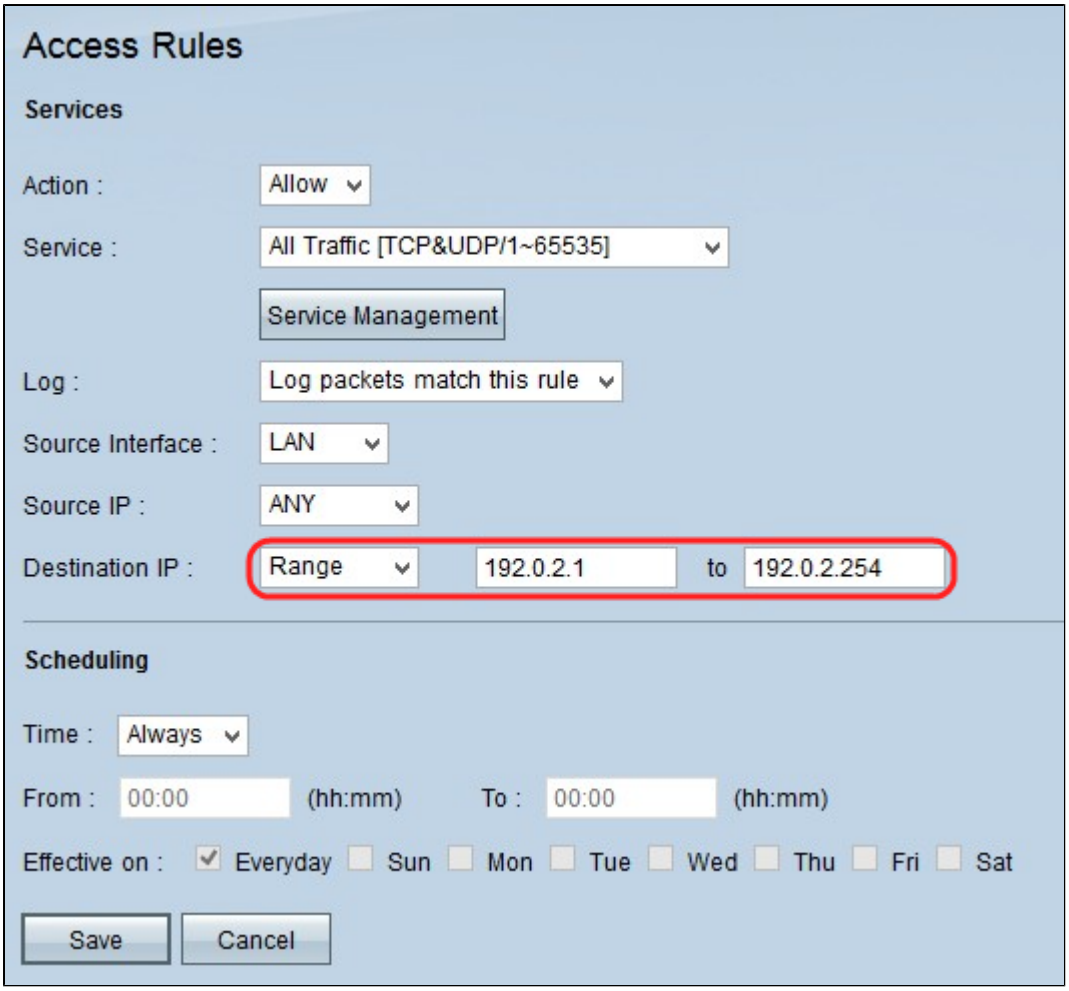
Etapa 9. Na lista suspensa Destino, escolha uma opção para especificar o intervalo de endereços de destino que devem ser permitidos ou negados pela interface. Os pacotes que chegam à interface são verificados pelo IP origem e pelo IP destino.

Qualquer â€" A regra de acesso será aplicada em todo o tráfego para a interface de destino. Não haverá campos disponíveis à direita da lista suspensa.

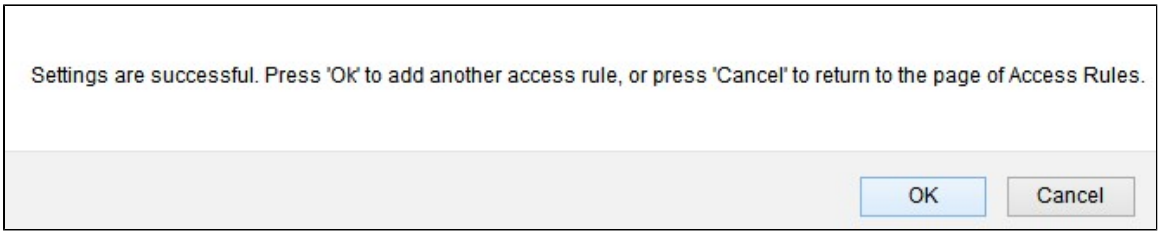
· Único â€" A regra de acesso será aplicada em um único endereço IP à interface de destino. Insira o endereço IP desejado no campo de endereço.

· Intervalo â€" A regra de acesso será aplicada em uma rede de sub-rede à interface de destino. Insira o endereço IP e o comprimento do prefixo.

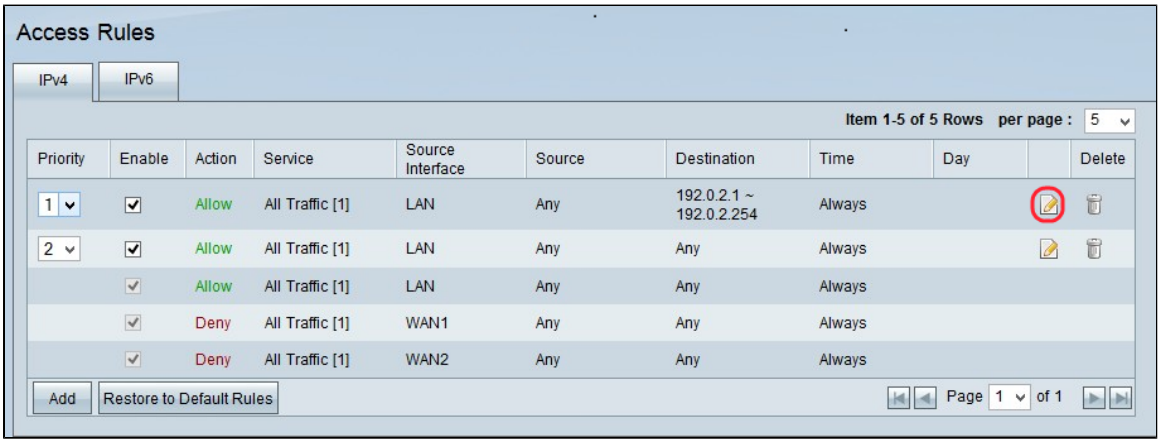
Clique em **Salvar** para salvar todas as alterações feitas na regra de acesso. Uma janela de confirmação é exibida, mostrando o status das alterações feitas no dispositivo.



Etapa 10. Clique em **OK** para adicionar outra regra de acesso. Clique em **Cancelar** para retornar à página *Regras de Acesso*.

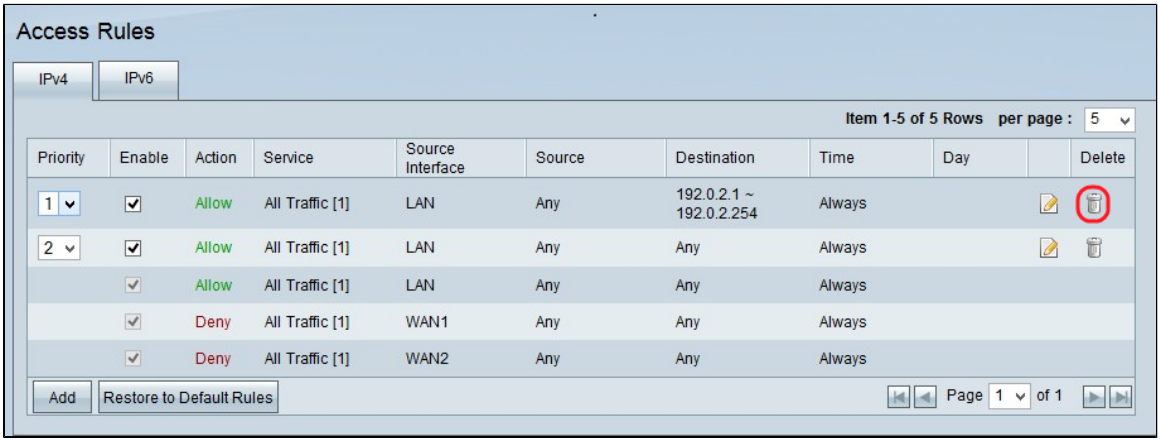


Etapa 11 (opcional). Escolha a regra de acesso desejada na lista e clique no **botão Editar** para editar a configuração da regra de acesso.



Etapa 12 (opcional). Escolha as regras de acesso desejadas na lista e clique no **botão Deletar** para deletar a

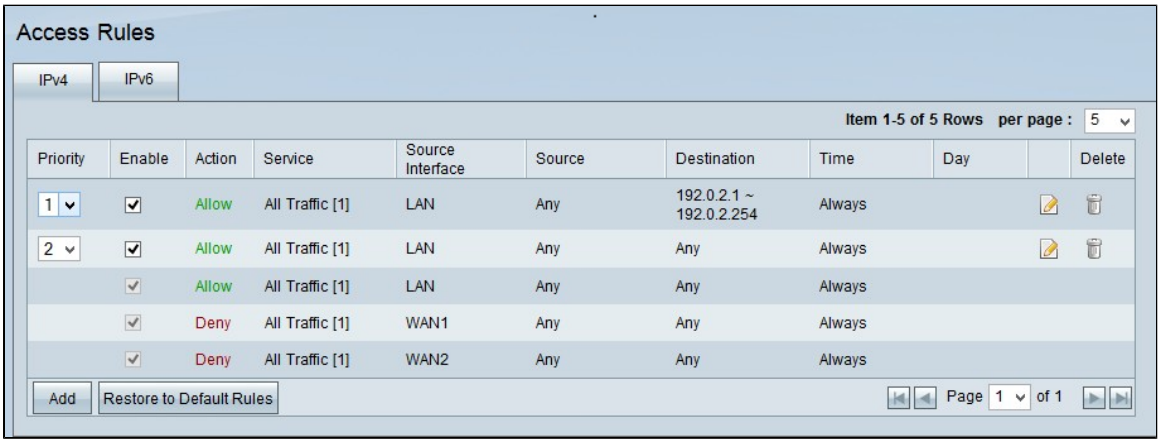
regra de acesso da lista de regras de acesso.



Agendar Regras de Acesso IPv4

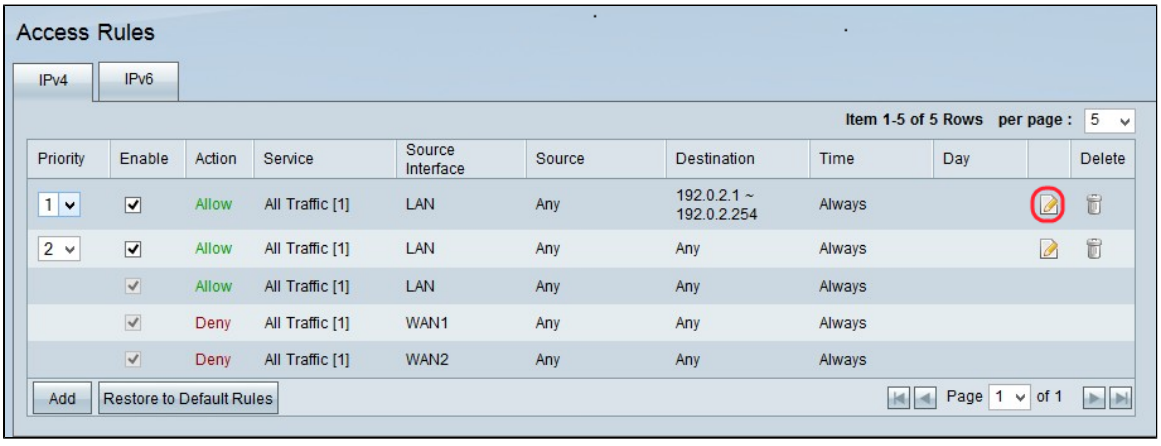
O agendamento de regras de acesso ajuda a especificar um agendamento quando essas regras de acesso estão ativas em termos de dia e hora. Ele só funciona com IPv4.

Etapa 1. Use o utilitário de configuração da Web e escolha **Firewall > Access Rules**. A página *IPv4 Access Rules* é aberta:



Etapa 2. Escolha a regra de acesso na tabela e clique no ícone **Editar** para adicionar o recurso de programação a essa regra de acesso.

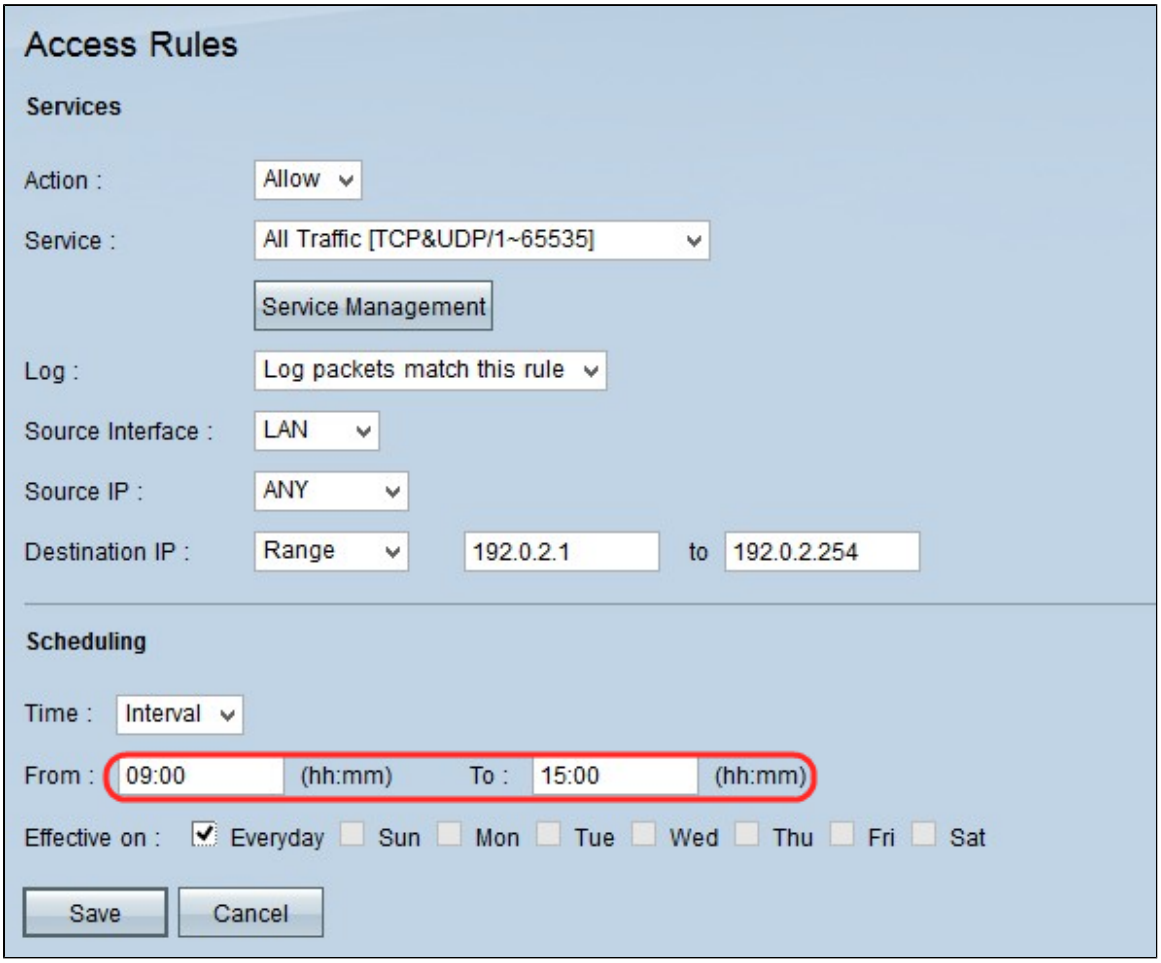
Observação: você também pode adicionar o recurso de agendamento ao adicionar uma nova regra de acesso.



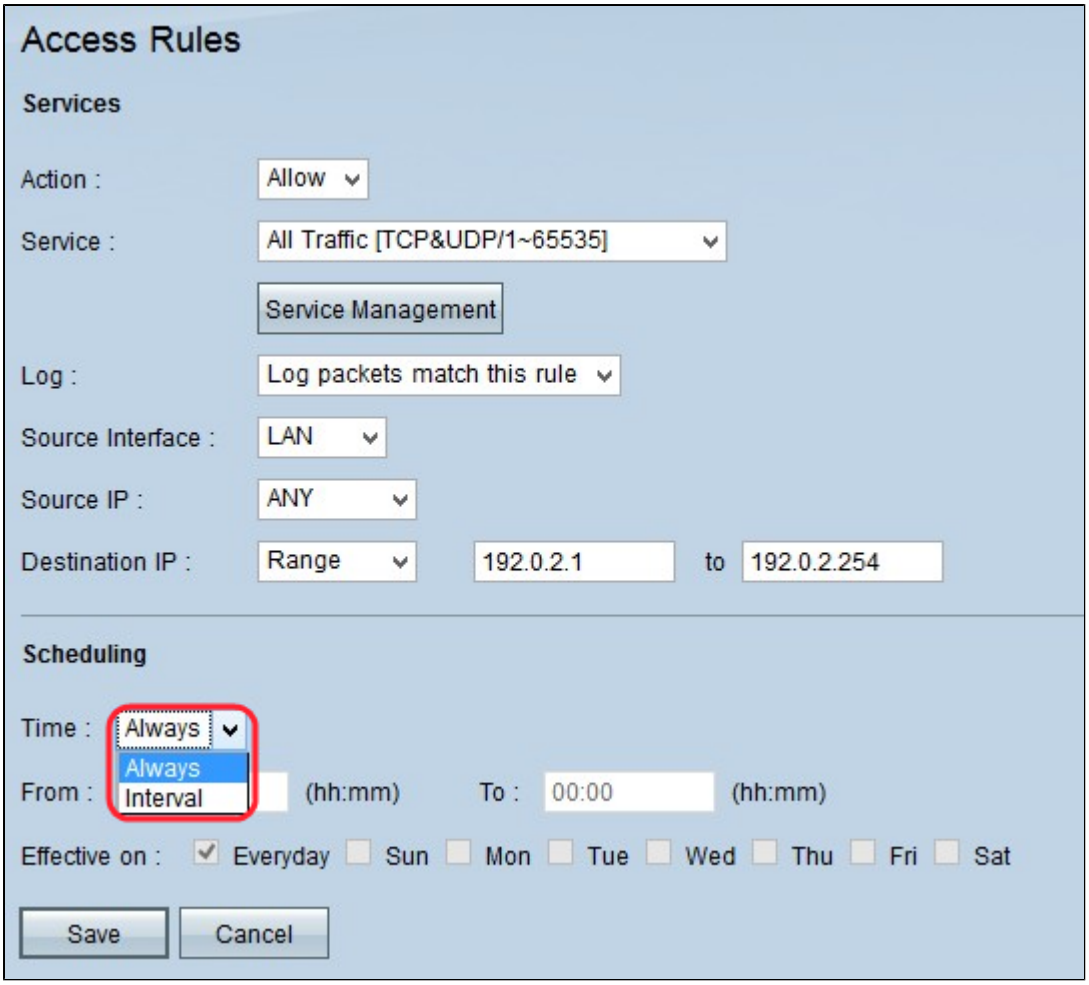
Etapa 3. Escolha a hora na lista suspensa Hora. Especifica quando usar o agendamento.

· Sempre â€" A regra de acesso aplica-se a todos os momentos e em todos os dias da semana. É escolhido por padrão. Se você escolher essa opção, clique em *Save* e vá para a etapa 6.

· Intervalo â€" Com base no intervalo de tempo determinado pelo usuário, a regra de acesso é aplicada.

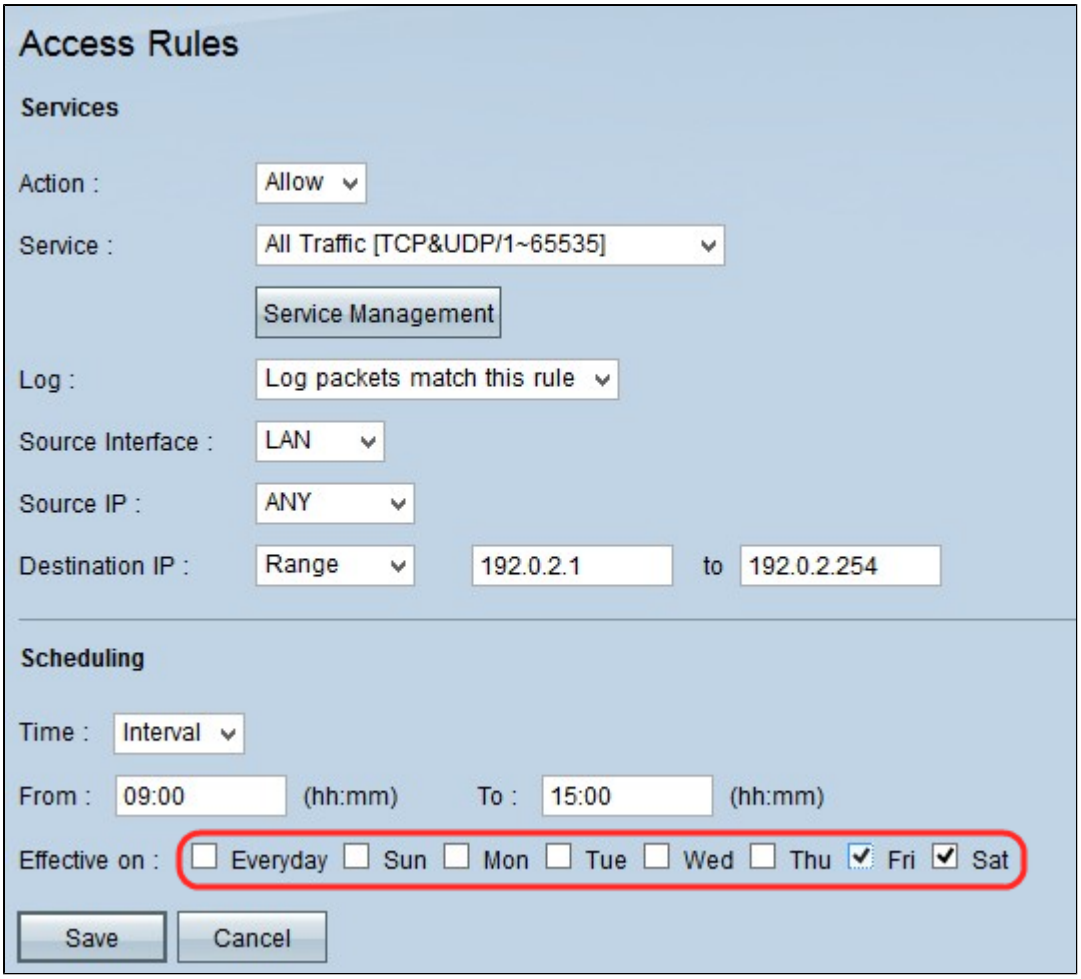


Etapa 4. Insira o intervalo de tempo no formato de 24 horas durante o qual a regra de acesso é aplicada nos campos *De* e *Até*.

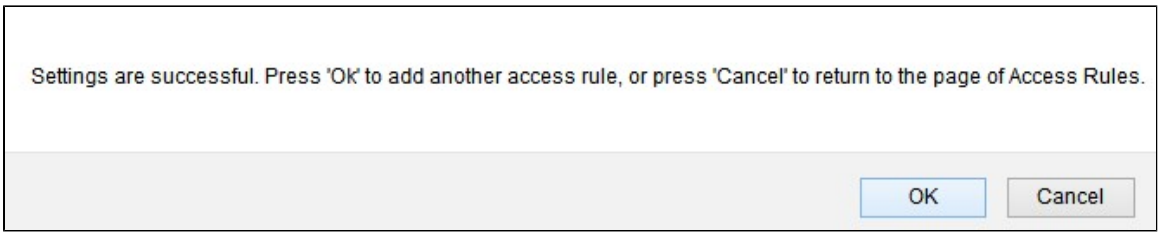


Etapa 5. Marque as caixas de seleção ao lado dos dias em que deseja aplicar a regra de acesso. A regra de acesso será efetiva somente nos dias marcados. Por padrão, *Everyday* (Todos os Dias) é escolhido.

Clique em **Salvar** para salvar todas as alterações feitas na regra de acesso. A janela de confirmação é exibida, mostrando o status das alterações feitas no dispositivo.



Etapa 6. Clique em **OK** para adicionar outra regra de acesso. Clique em **Cancelar** para retornar à página da regra de acesso.



Conclusão

Agora você configurou as regras de acesso IPv4 em seu roteador VPN RV016, RV042, RV042G ou RV082.

Se quiser acessar todo o suporte para esses roteadores, confira a página do produto clicando aqui.

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.