Configuração de uma Regra de Acesso IPv6 em Roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Uma regra de acesso ajuda o roteador a determinar que tráfego tem permissão para passar pelo firewall. Isso ajuda a adicionar segurança ao roteador.

Este artigo explica como adicionar uma regra de acesso IPv6 nos roteadores VPN RV016, RV042, RV042G e RV082.

Dispositivos aplicáveis

- RV016
- RV042
- RV042G
- RV082

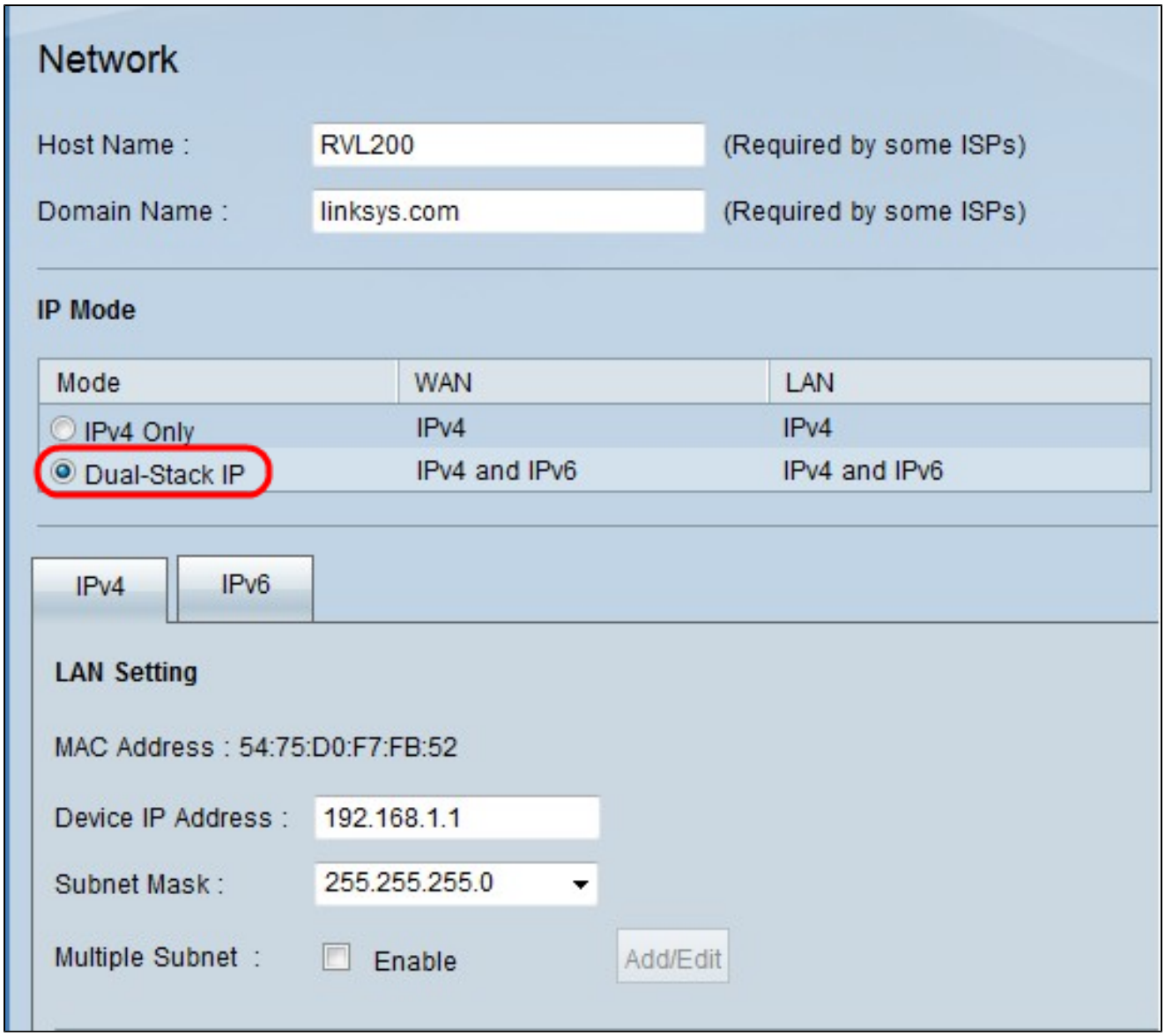
Versão de software

- v4.2.1.02

Configuração de uma Regra de Acesso IPv6

Habilitar Modo IPv6

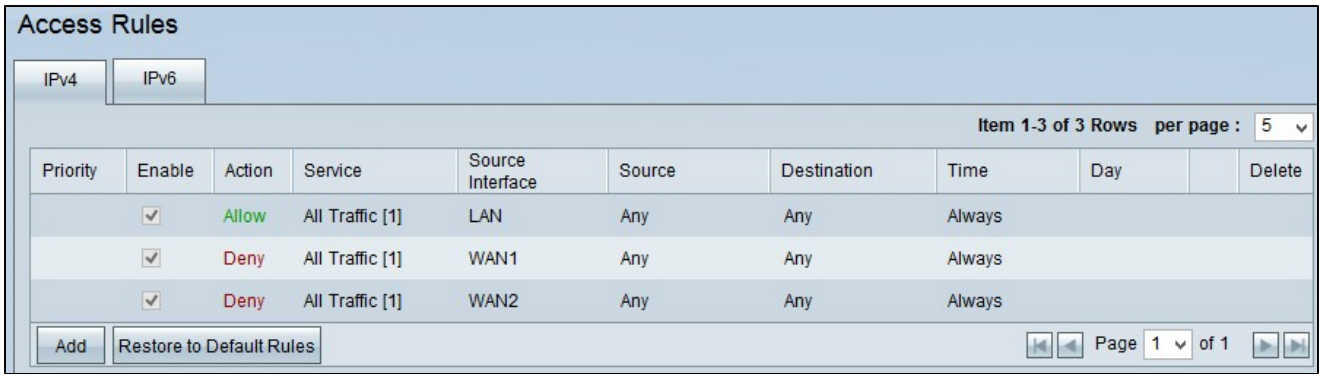
Etapa 1. Faça login no utilitário de configuração da Web e escolha Setup > Network. A página Rede é aberta:



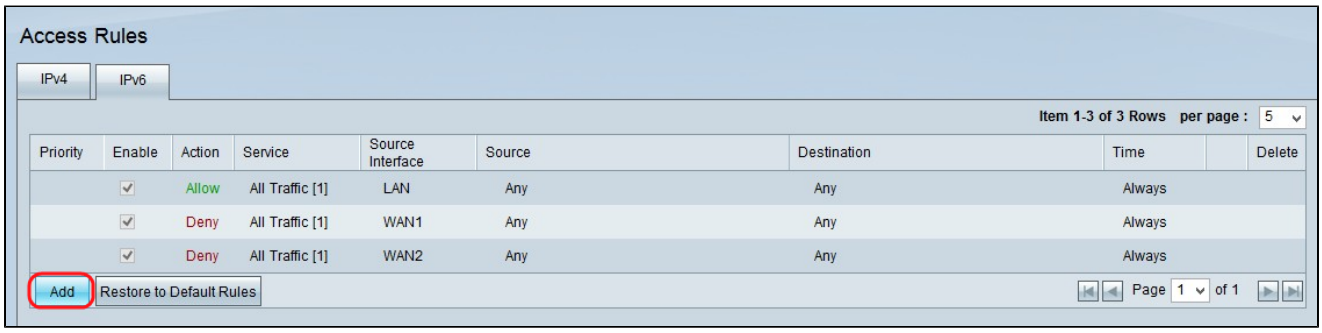
Etapa 2. Clique no botão de opção Dual-Stack IP. Isso permite que IPv4 e IPv6 sejam executados ao mesmo tempo. Se a comunicação IPv6 for possível, essa será a comunicação preferida.

Configuração de Regra de Acesso IPv6

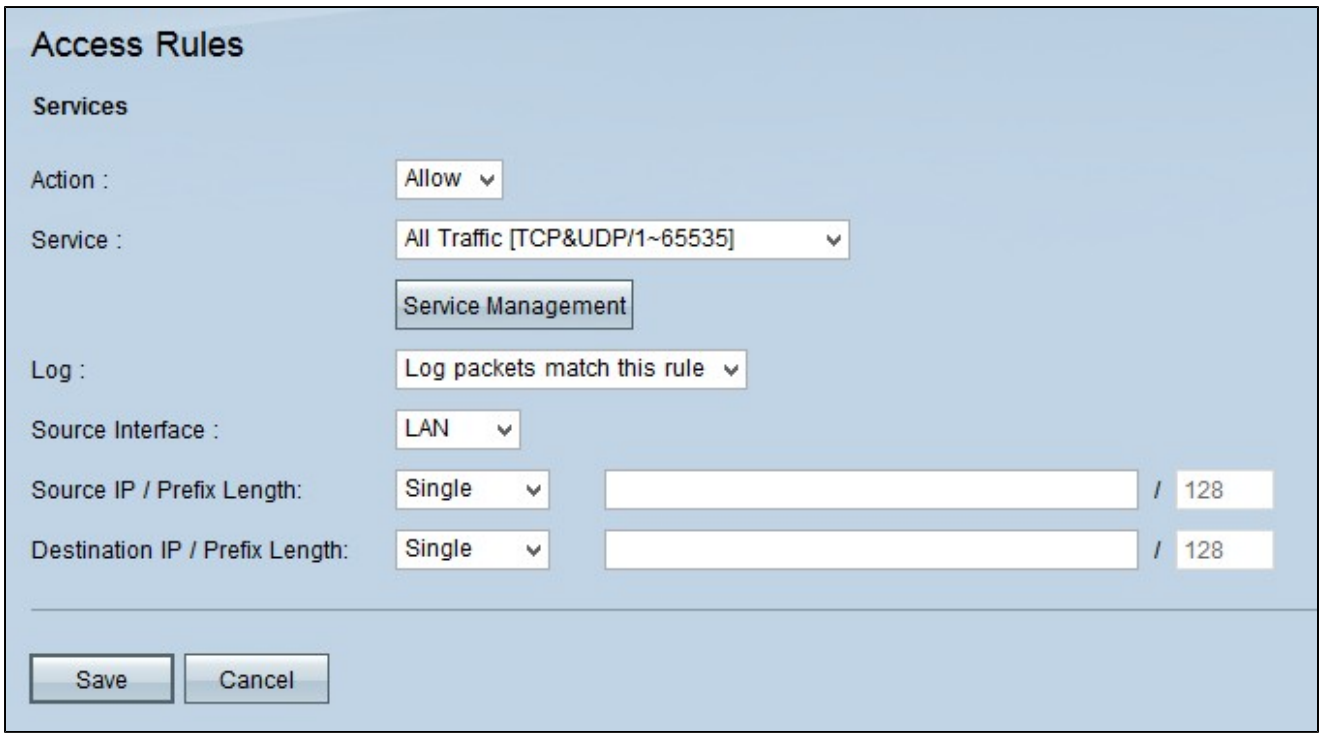
Etapa 1. Faça login no utilitário de configuração da Web e escolha Firewall > Access Rules. A página Regras de Acesso é aberta:



Etapa 2. Clique na guia IPv6. Isso abre a página IPv6 Access Rules.



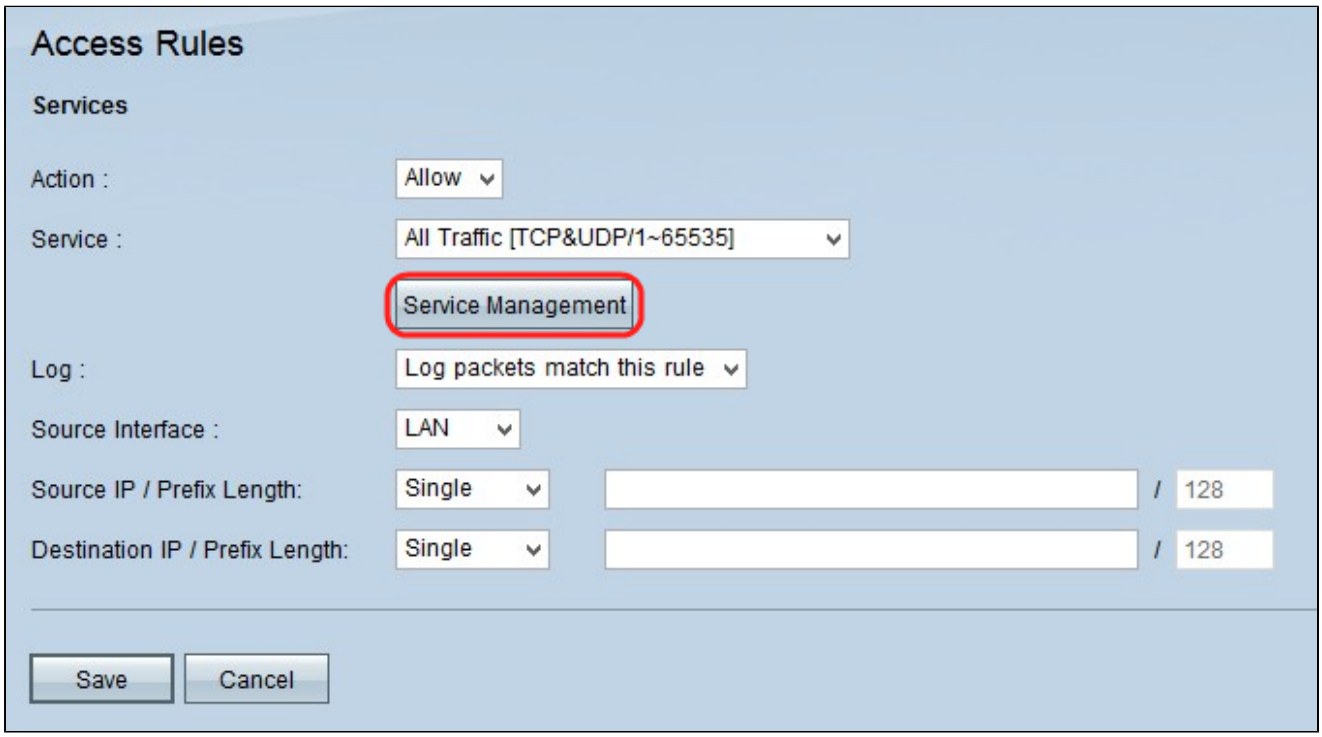
Etapa 3. Clique em Adicionar para adicionar as regras de acesso. A página Access Rules é exibida para configurar as regras de acesso para IPv6.



Etapa 4. Escolha Permitir na lista suspensa Ação se o tráfego tiver que ser permitido. Escolha Negar para negar o tráfego.

Etapa 5. Escolha o serviço apropriado na lista suspensa Serviço.

Economizador de tempo: se o serviço desejado estiver disponível, vá para a Etapa 12.



Etapa 6. Se o serviço apropriado não estiver disponível, clique em Gerenciamento de serviços. A janela Gerenciamento de serviços é exibida.

Service Name :

Protocol : TCP

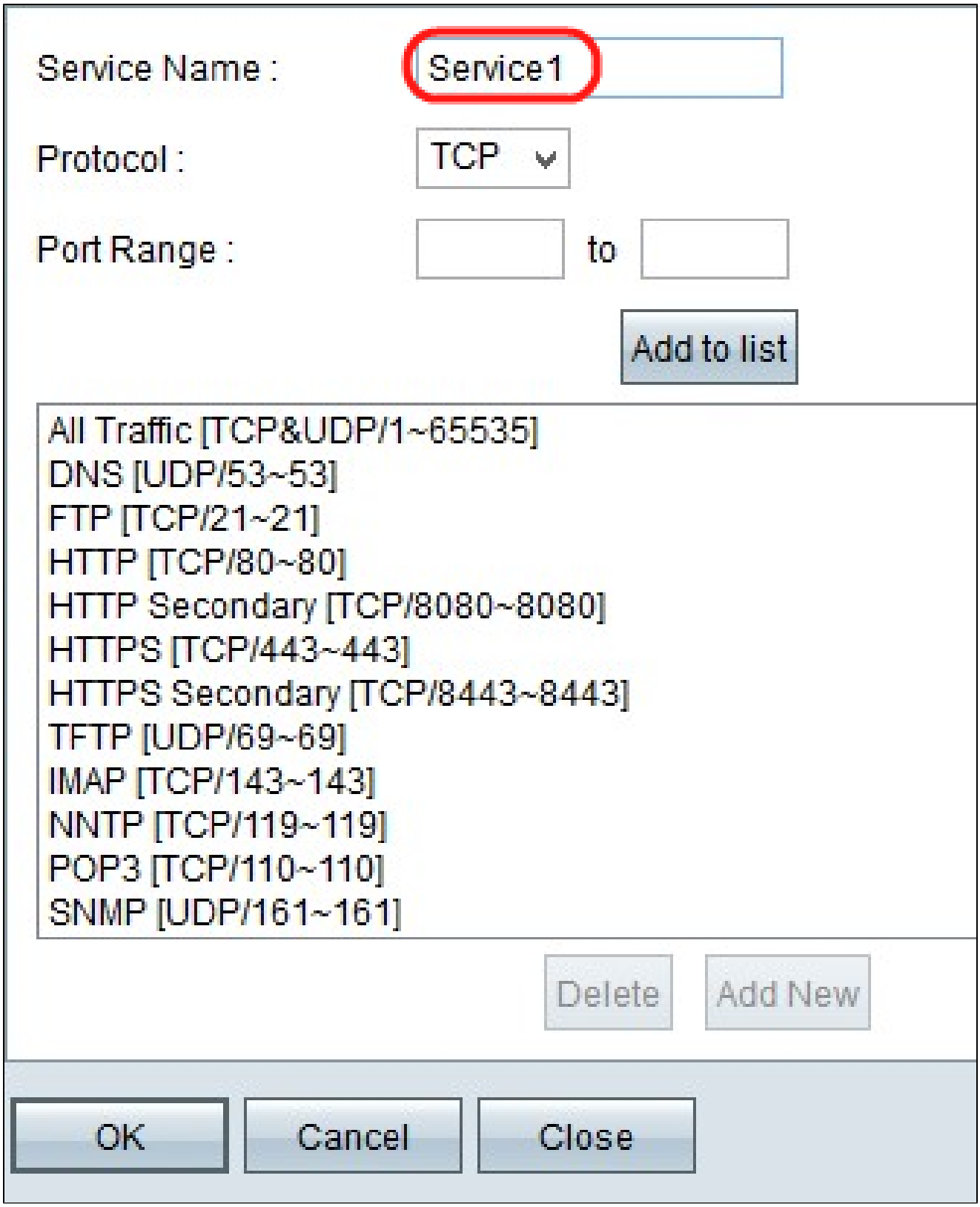
Port Range : to

Add to list

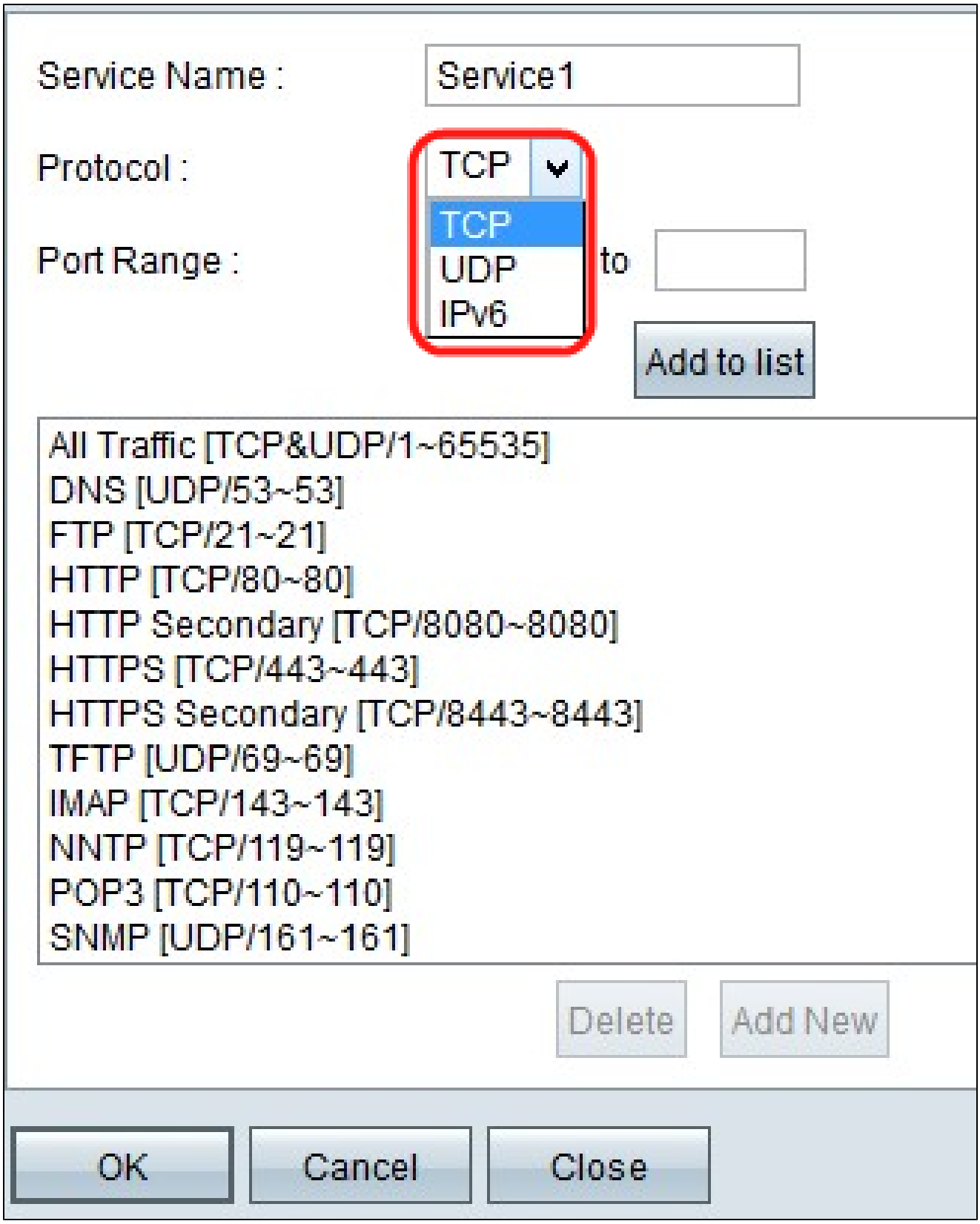
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete Add New

OK Cancel Close



Passo 7. Informe um nome para o novo serviço no campo Nome do Serviço.

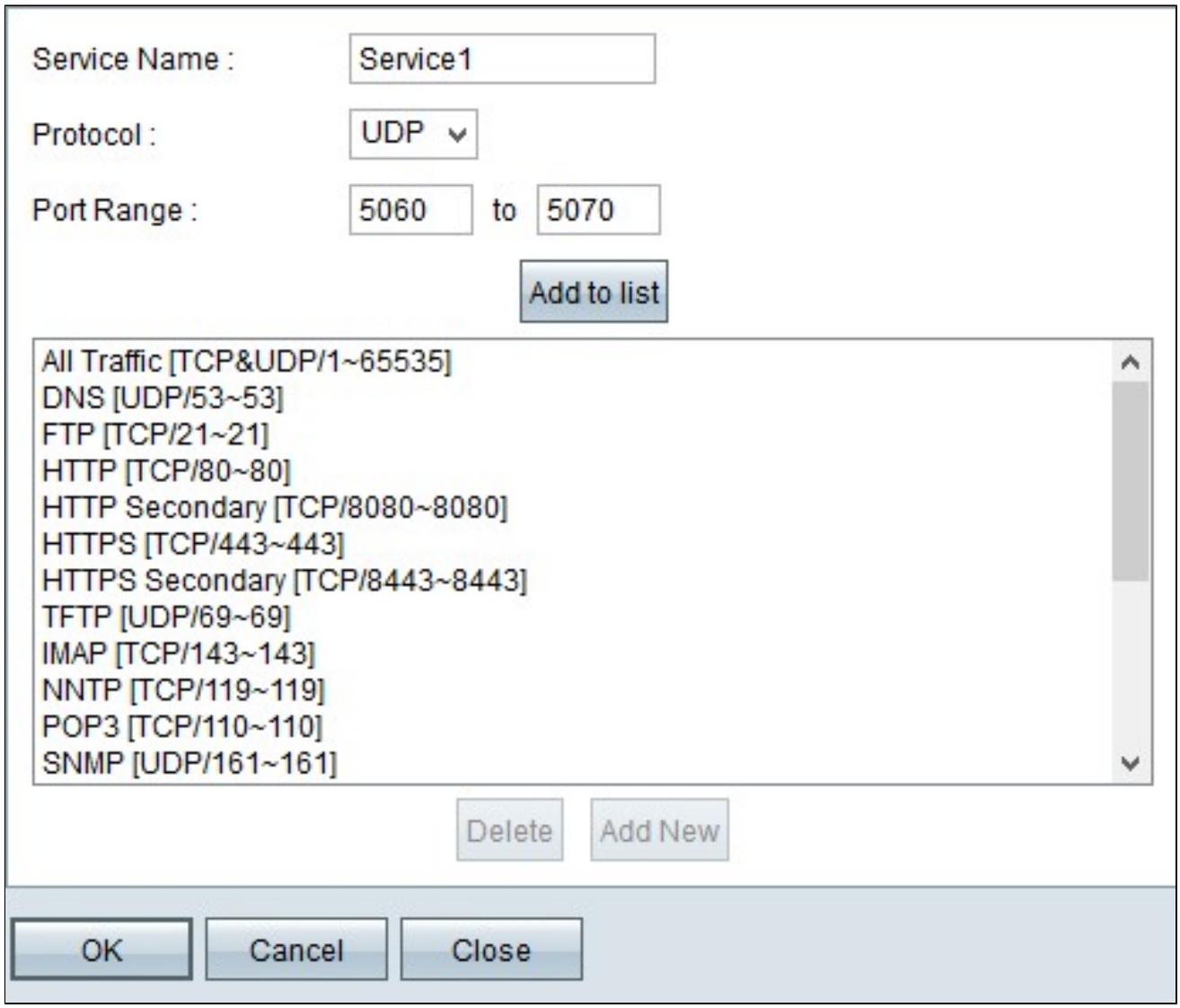


Etapa 8. Escolha o tipo de protocolo apropriado na lista suspensa Protocolo.

· TCP (Transmission Control Protocol) — Um protocolo da camada de transporte usado por aplicativos que requer entrega garantida.

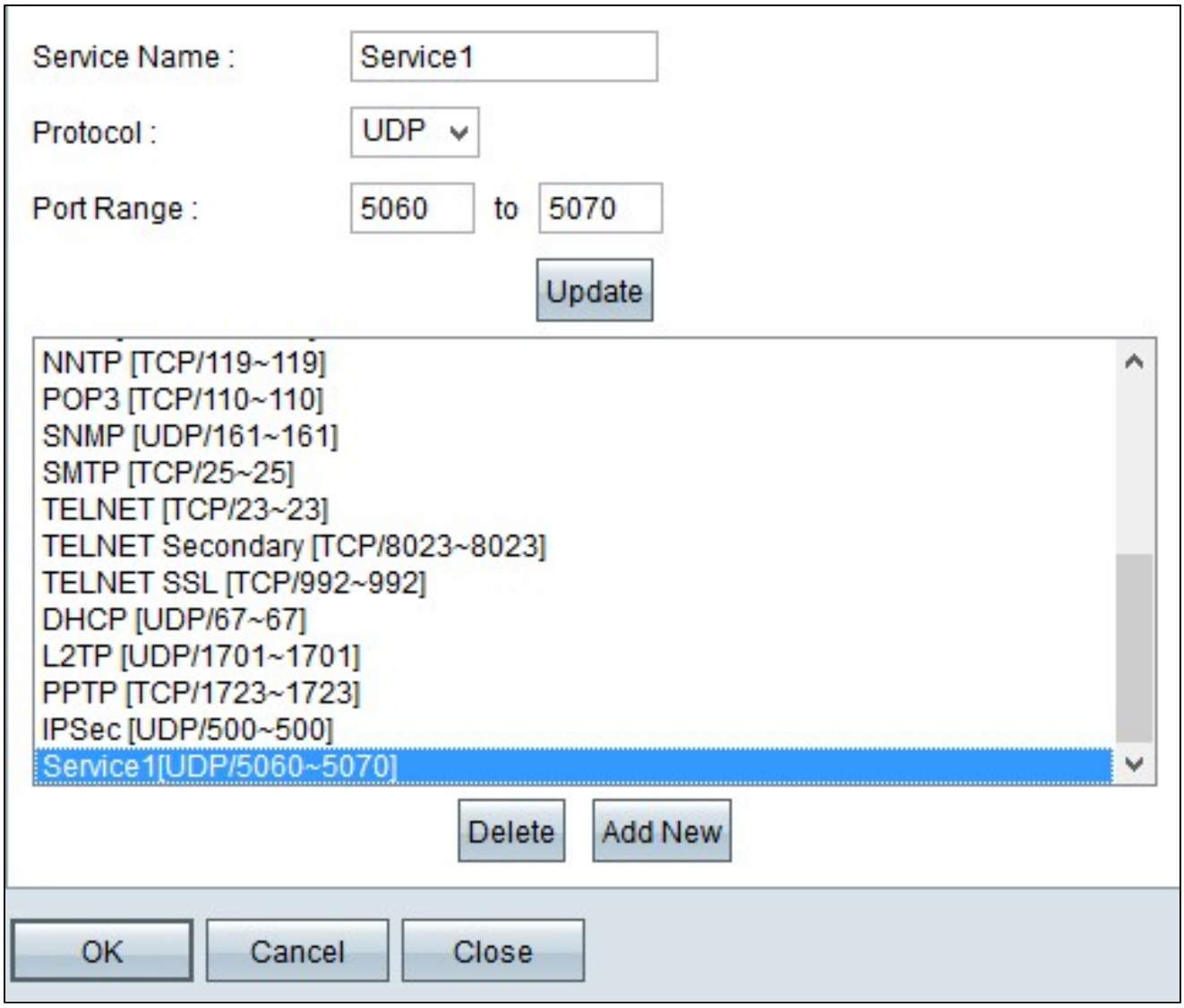
· UDP (User Datagram Protocol) — usa soquetes de datagramas para estabelecer comunicações host a host. A entrega de UDP não é garantida.

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



Etapa 9. Insira o intervalo de portas no campo Intervalo de portas. Esse intervalo depende do protocolo escolhido na etapa acima.

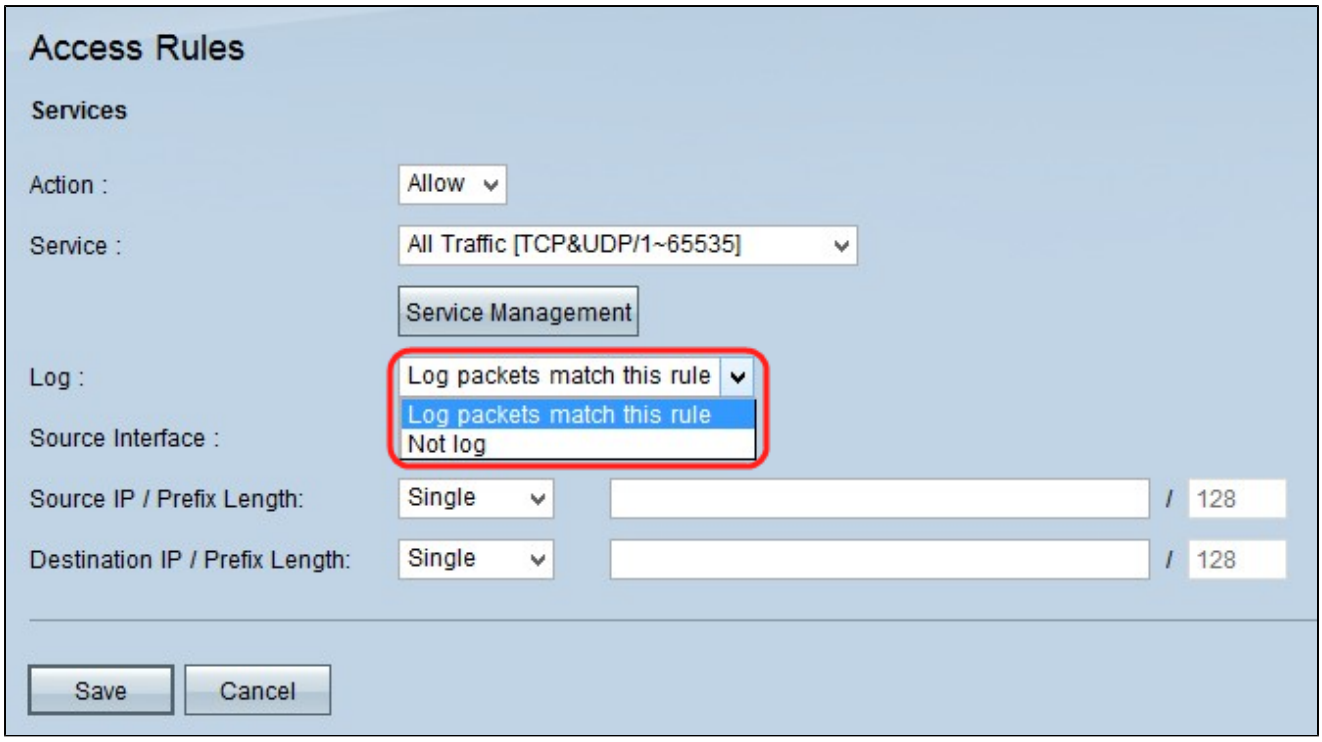
Etapa 10. Clique em Adicionar à lista. Isso adiciona o Serviço à lista suspensa Serviço.



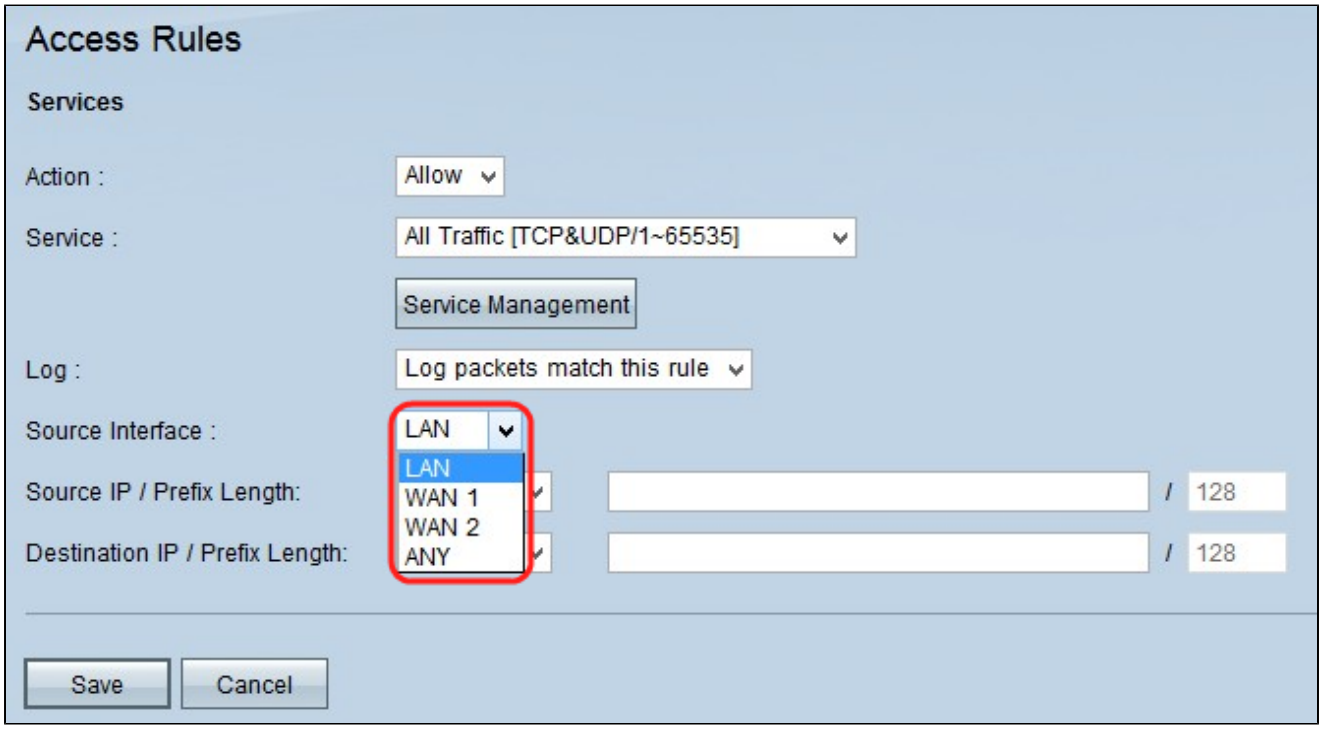
Nota: Se quiser excluir um serviço da lista de serviços, escolha o serviço na lista de serviços e clique em Excluir. Se desejar atualizar a entrada de serviço, escolha o serviço a ser atualizado na lista de serviços e clique em Atualizar. Para adicionar outro novo serviço à lista, clique em Add New.

Etapa 11. Click OK. Isso fecha a janela e leva o usuário de volta à página Regra de acesso.

Observação: se você clicar em Add New, siga as etapas 7 a 11.



Etapa 12. Para registrar os pacotes que correspondem à regra de acesso, escolha Registrar pacotes correspondentes a esta regra na lista suspensa Registro. Caso contrário, escolha Não registrar.



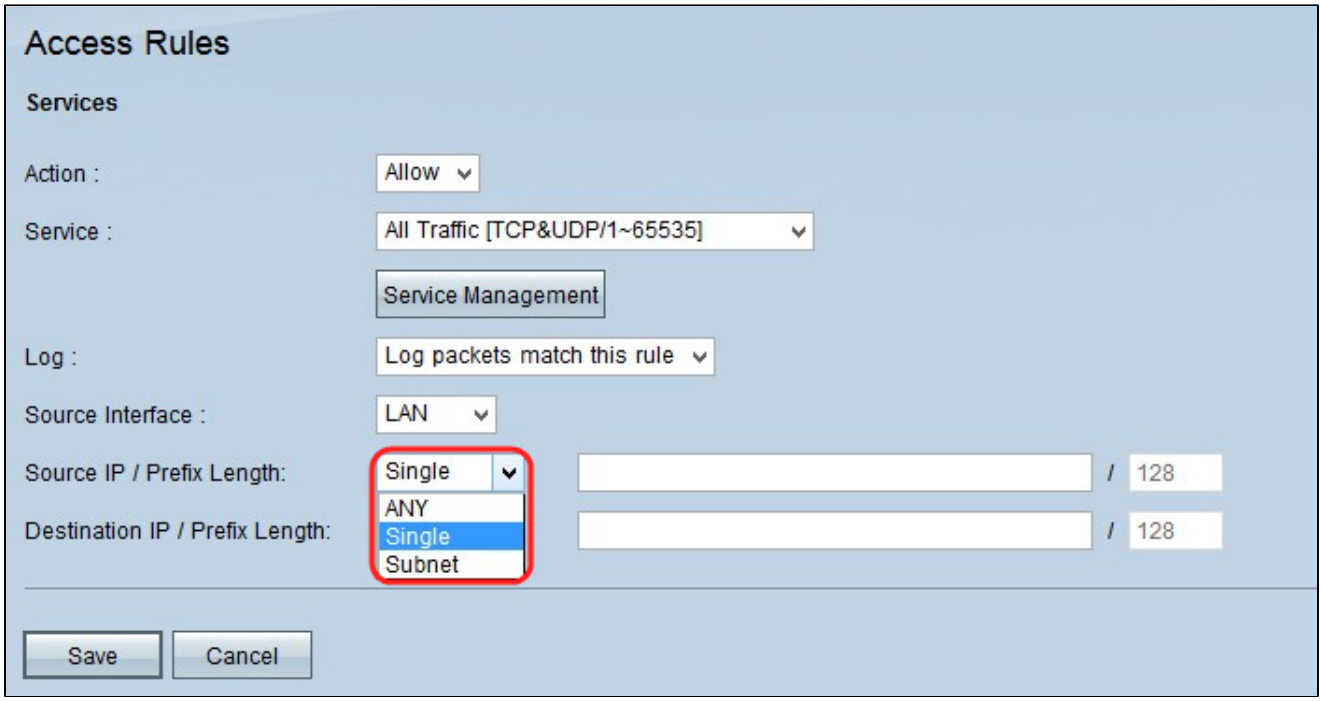
Etapa 13. Escolha a interface afetada por esta regra na lista suspensa Interface de origem. A interface de origem é a interface a partir da qual o tráfego é iniciado.

· LAN — A rede local do roteador.

· WAN1 — 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 — O mesmo que WAN1, exceto que é uma rede secundária.

· ANY — Permite que qualquer interface seja usada.

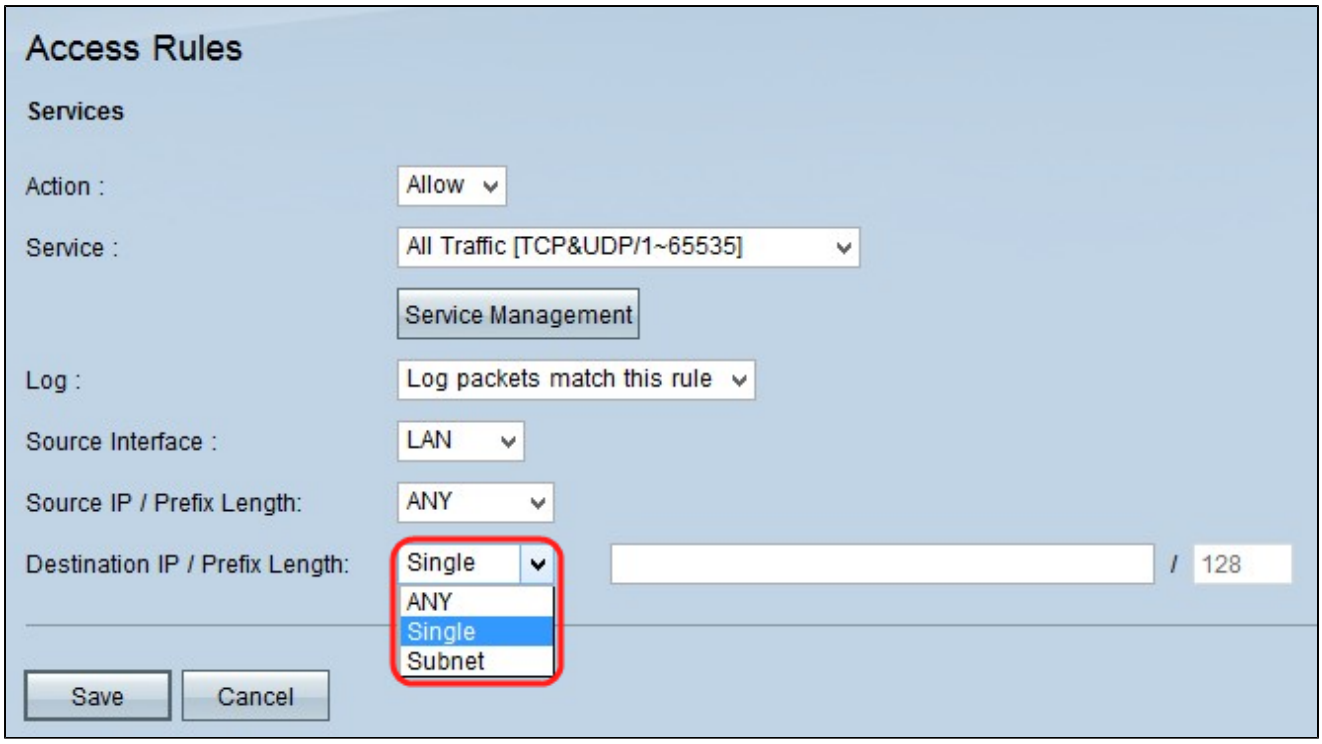


Etapa 14. Na lista suspensa IP de origem, escolha uma opção para especificar o endereço IP de origem ao qual a regra de acesso será aplicada.

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

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

· Sub-rede — 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 15. Na lista suspensa IP de destino; escolha uma opção para especificar o endereço IP de destino ao qual a regra de acesso será aplicada.

Qualquer — 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 — A regra de acesso será aplicada em um único endereço IP à interface de destino. Insira o endereço IP desejado no campo de endereço.

· Sub-rede — 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.

Etapa 16. Clique em Salvar para salvar todas as alterações feitas na regra de acesso IPv6.

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.