Adicionar e configurar regras de acesso em RV130 e RV130W

Objetivo

Os dispositivos de rede fornecem recursos básicos de filtragem de tráfego com regras de acesso. Uma regra de acesso é uma única entrada em uma ACL (Access Control List, lista de controle de acesso) que especifica uma regra de permissão ou negação (para encaminhar ou descartar um pacote) com base no protocolo, em um endereço IP de origem e de destino ou na configuração da rede.

O objetivo deste documento é mostrar como adicionar e configurar uma Regra de acesso no RV130 e RV130W.

Dispositivos aplicáveis

•RV130

RV130W

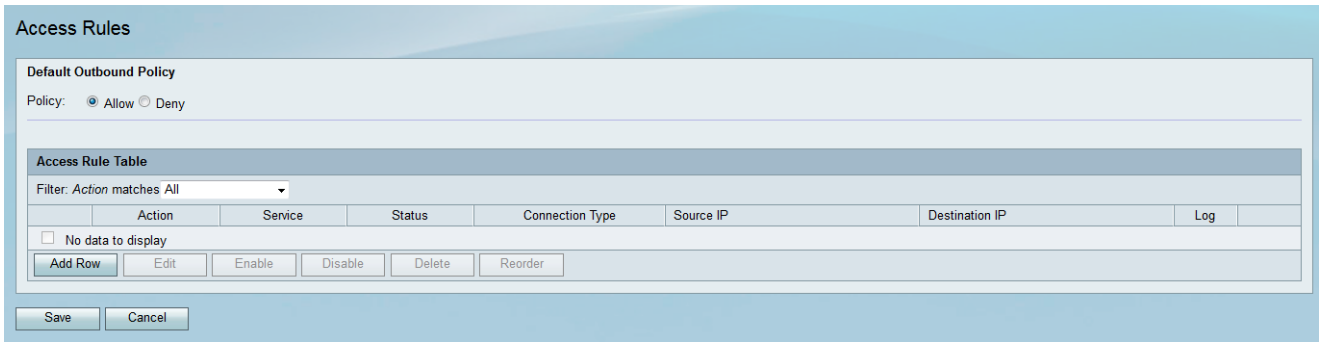
Versões de software

· Versão 1.0.1.3

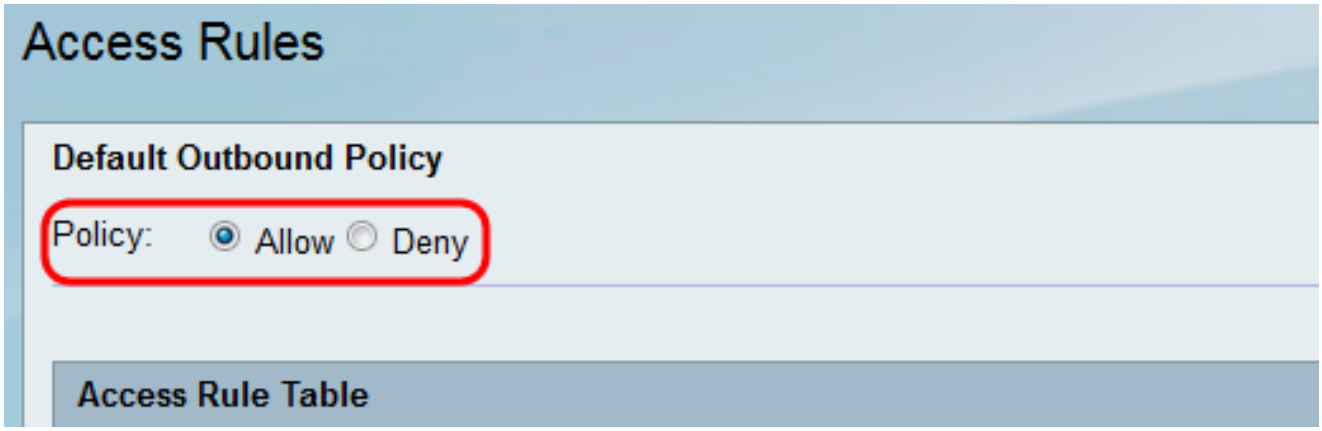
Como adicionar e configurar uma regra de acesso

Definindo Política de Saída Padrão

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



Etapa 2. Na área Política de saída padrão, clique no botão de opção desejado para escolher uma política para o tráfego de saída. A política é aplicada sempre que não há regras de acesso ou políticas de acesso à Internet configuradas. A configuração padrão é Allow, que permite a passagem de todo o tráfego para a Internet.

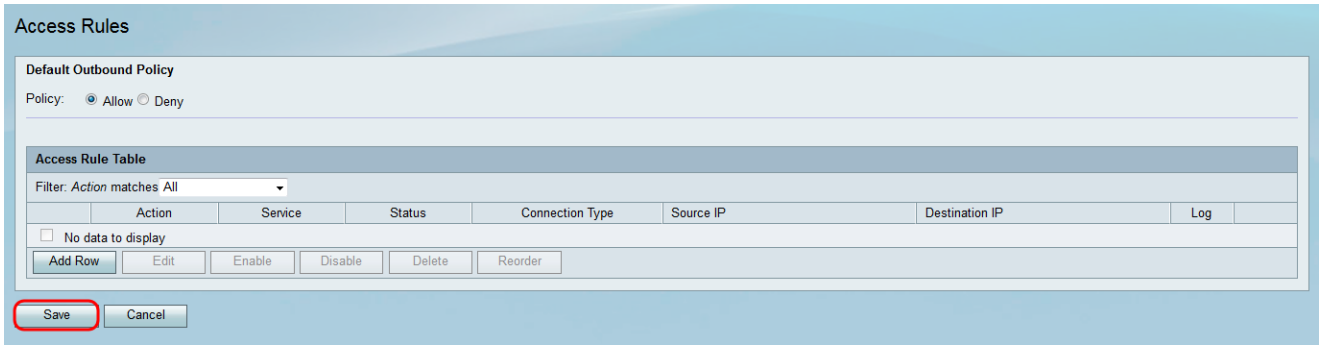


As opções disponíveis são definidas da seguinte forma:

· Permitir — Permitir todos os tipos de tráfego que saem da LAN para a Internet.

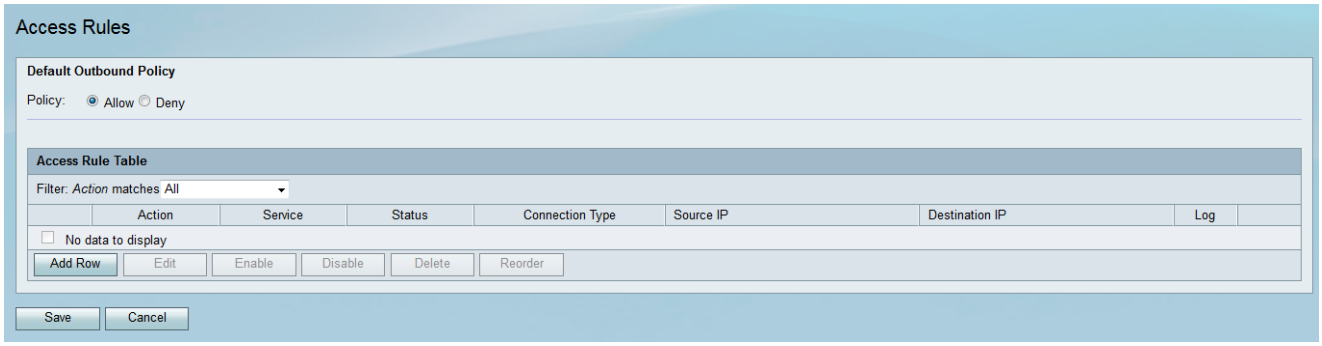
· Negar — Bloquear todos os tipos de tráfego que saem da LAN para a Internet.

Etapa 3. Clique em Save (Salvar) para salvar as configurações.

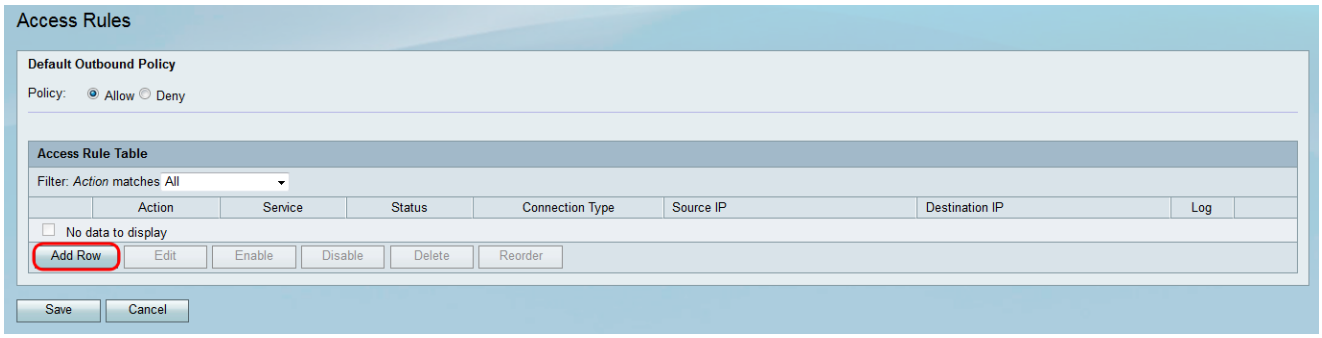


Adicionando uma regra de acesso

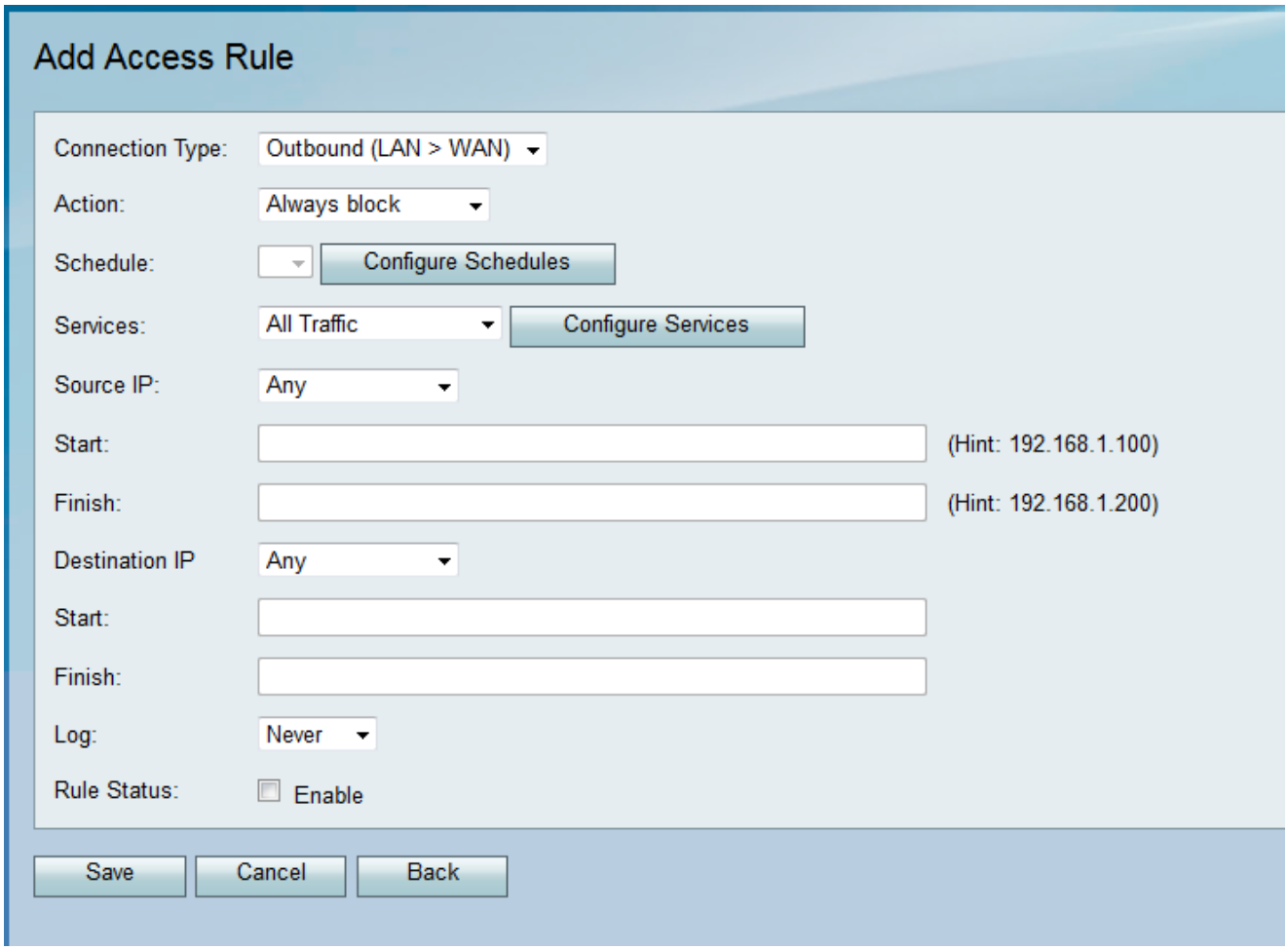
Etapa 1. Faça login no utilitário de configuração da Web e escolha Firewall > Access Rules. A janela Regras de Acesso é aberta:



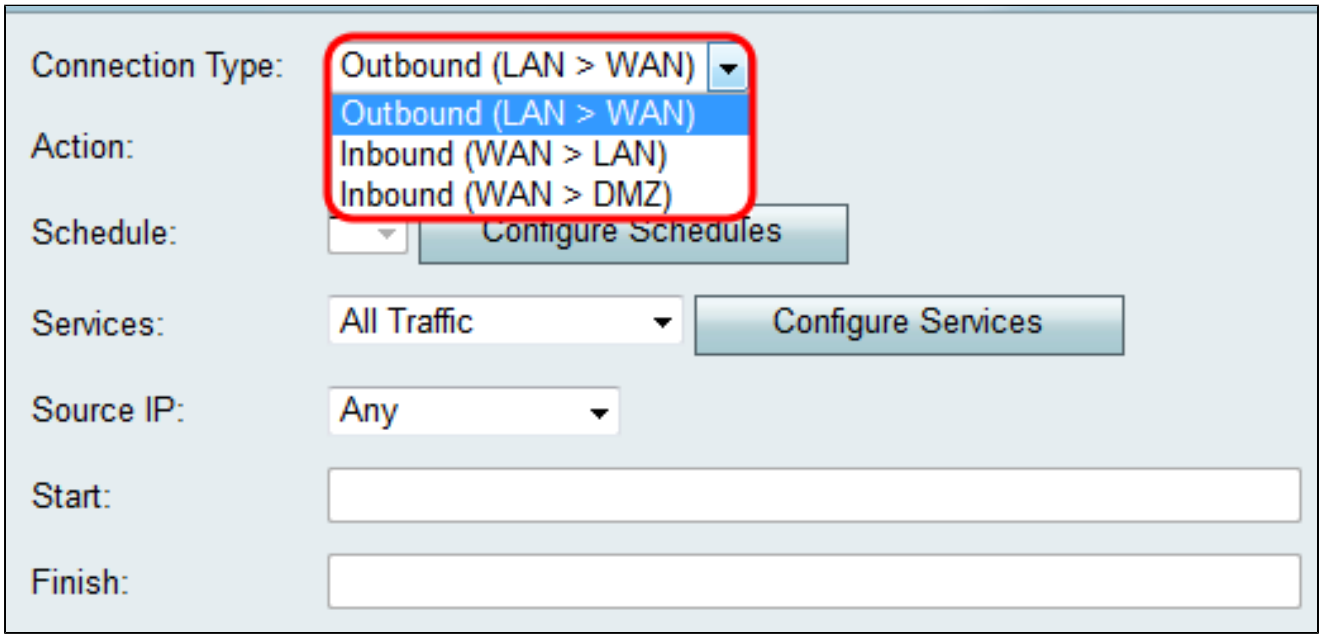
Etapa 2. Clique em Adicionar linha na Tabela de regras de acesso para adicionar uma nova regra de acesso.



A página Adicionar regra de acesso é aberta:



Etapa 3. Na lista suspensa Tipo de conexão, escolha o tipo de tráfego ao qual a regra se aplica.



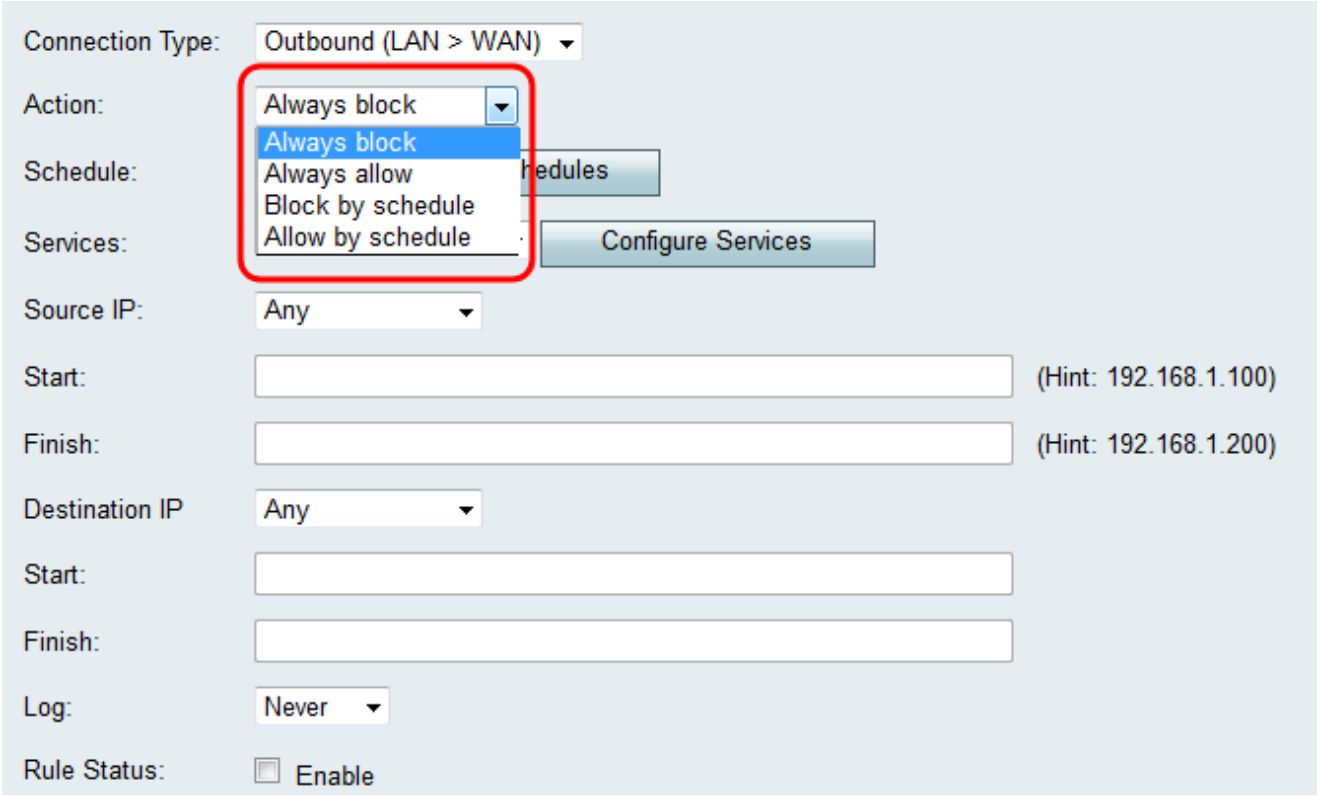
As opções disponíveis são definidas da seguinte forma:

· Saída (LAN > WAN) — A regra afeta os pacotes que vêm da rede local (LAN) e saem para a Internet (WAN).

· Entrada (WAN > LAN) — A regra afeta os pacotes que vêm da Internet (WAN) e vão para a rede local (LAN).

· Entrada (WAN > DMZ) — A regra afeta os pacotes que vêm da Internet (WAN) e vão para a sub-rede da zona desmilitarizada (DMZ).

Etapa 4. Na lista suspensa Ação, escolha a ação a ser tomada quando uma regra for correspondida.



As opções disponíveis são definidas da seguinte forma:

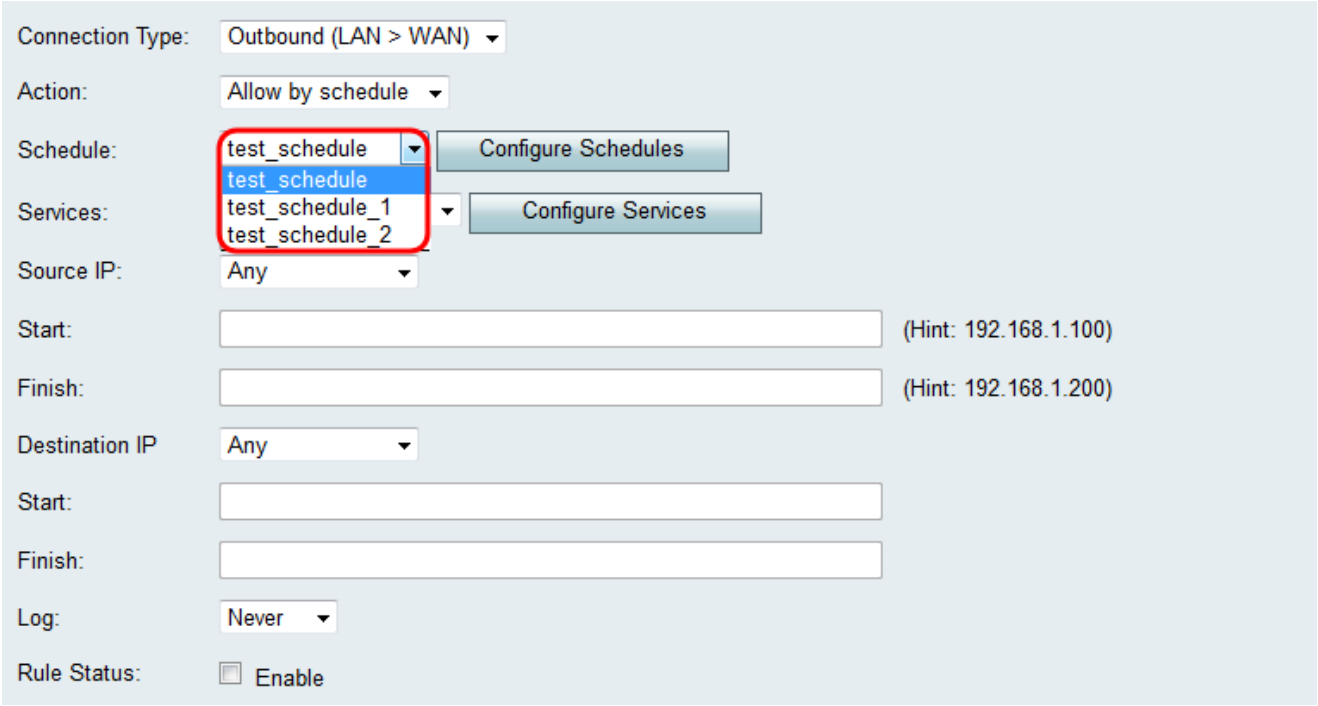
· Sempre bloquear — Sempre negue o acesso se as condições corresponderem. Vá para a Etapa 6.

· Sempre Permitir — Sempre permitir acesso se as condições corresponderem. Vá para a Etapa 6.

· Bloquear por agendamento — Negue o acesso se as condições forem atendidas durante um agendamento pré-configurado.

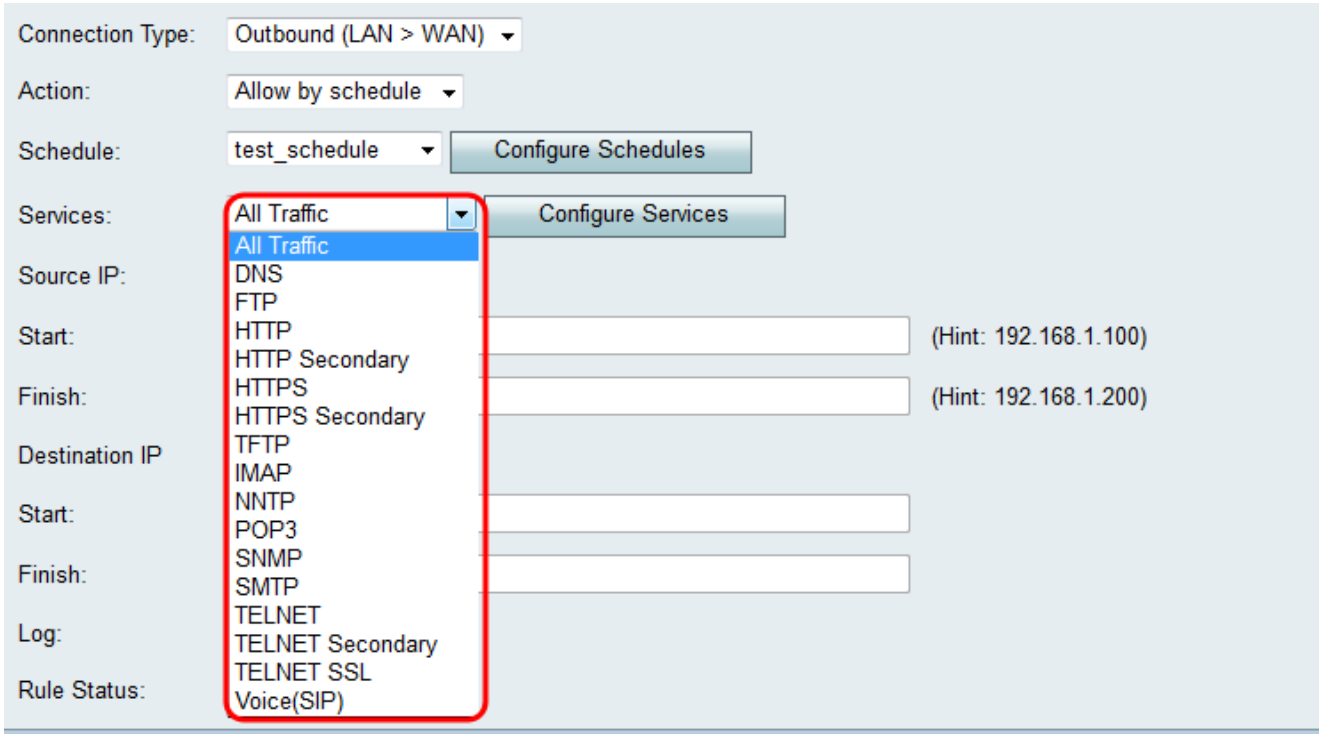
· Permitir por agendamento — Permitir o acesso se as condições forem atendidas durante um agendamento pré-configurado.

Etapa 5. Se você escolher Bloquear por agendamento ou Permitir por agendamento na Etapa 4, escolha o agendamento apropriado na lista suspensa Agendamento.



Observação: para criar ou editar um agendamento, clique em Configurar Agendamentos. Consulte Configuração de Agendamentos no RV130 e RV130W para obter mais informações e diretrizes.

Etapa 6. Escolha o tipo de serviço ao qual a regra de acesso se aplica na lista suspensa Serviços.



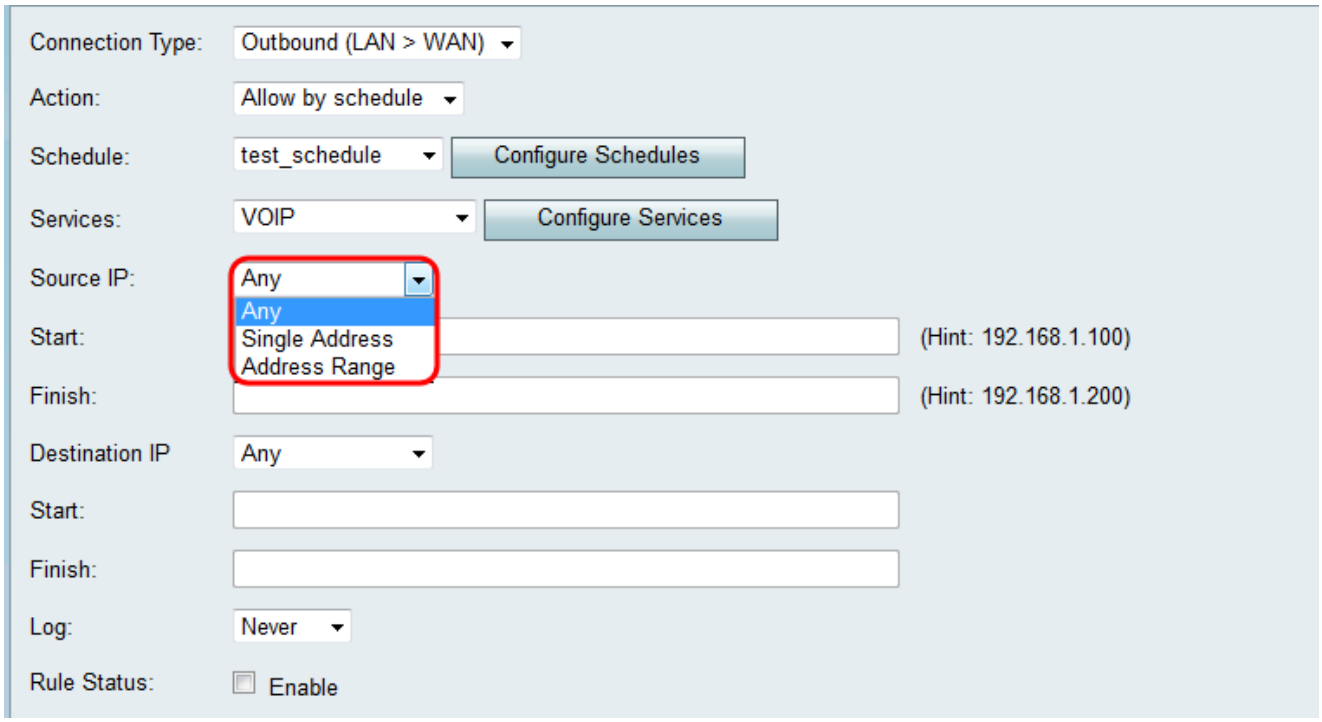
Observação: se quiser adicionar ou editar um serviço, clique em Configurar serviços. Consulte Service Management Configuration no RV130 e RV130W para obter mais informações e diretrizes.

Configurando IP de origem e destino para tráfego de saída

Siga as etapas nesta seção se Outbound (LAN > WAN) tiver sido selecionado como o Tipo de conexão na Etapa 3 de Adicionando uma regra de acesso.

Observação: se um Tipo de conexão de entrada tiver sido selecionado na Etapa 3 de Adicionando uma regra de acesso, vá para a próxima seção: Configurando IP de origem e destino para tráfego de entrada.

Etapa 1. Escolha como você deseja definir o IP de origem na lista suspensa IP de origem. Para o tráfego de saída, o IP de origem refere-se ao endereço ou endereços (na LAN) aos quais a regra de firewall se aplicaria.



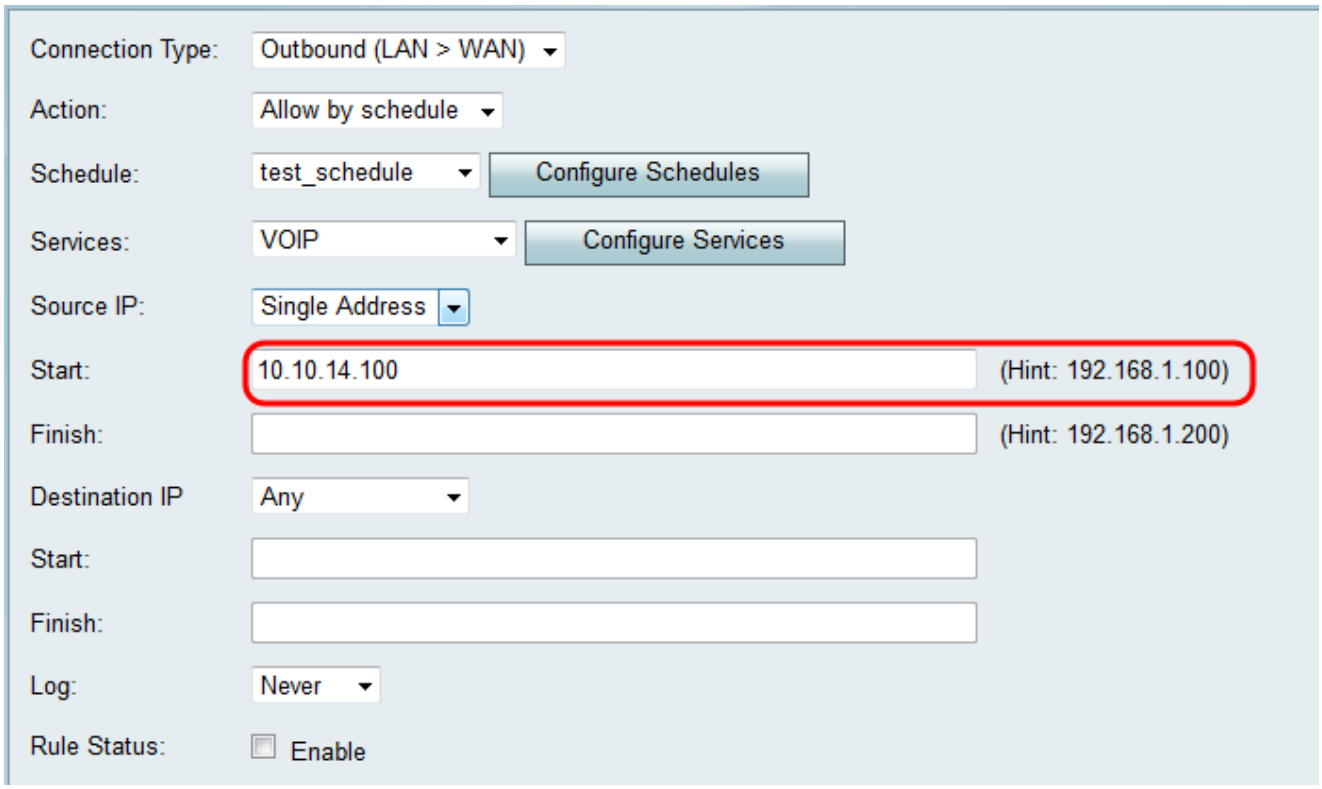
As opções disponíveis são definidas da seguinte forma:

· Qualquer — Aplica-se ao tráfego originário de qualquer endereço IP na rede local. Portanto, deixe os campos Start e Finish em branco. Vá para a Etapa 4 se você escolher essa opção.

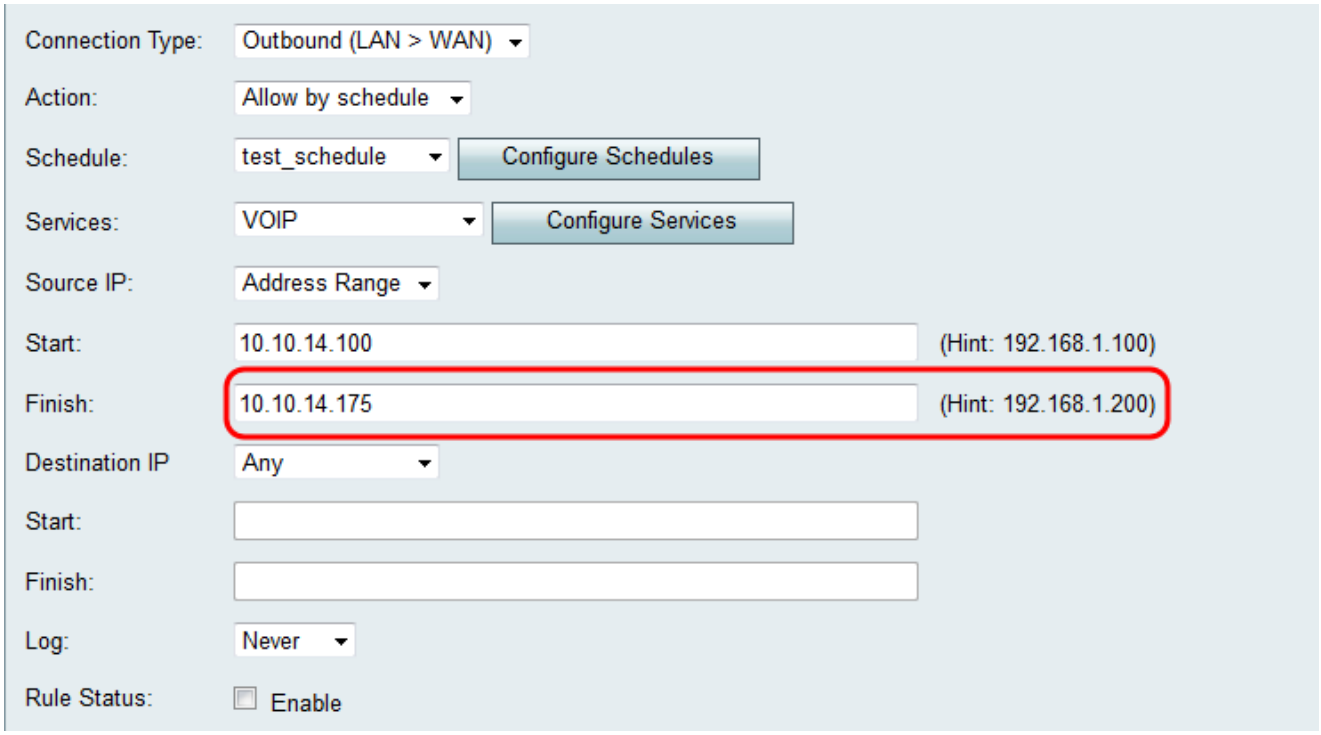
· Endereço único — Aplica-se ao tráfego originado de um único endereço IP na rede local. Insira o endereço IP no campo Start.

· Intervalo de endereços — Aplica-se ao tráfego originário de um intervalo de endereços IP na rede local. Insira o endereço IP inicial do intervalo no campo Start e o endereço IP final no campo Finish para definir o intervalo.

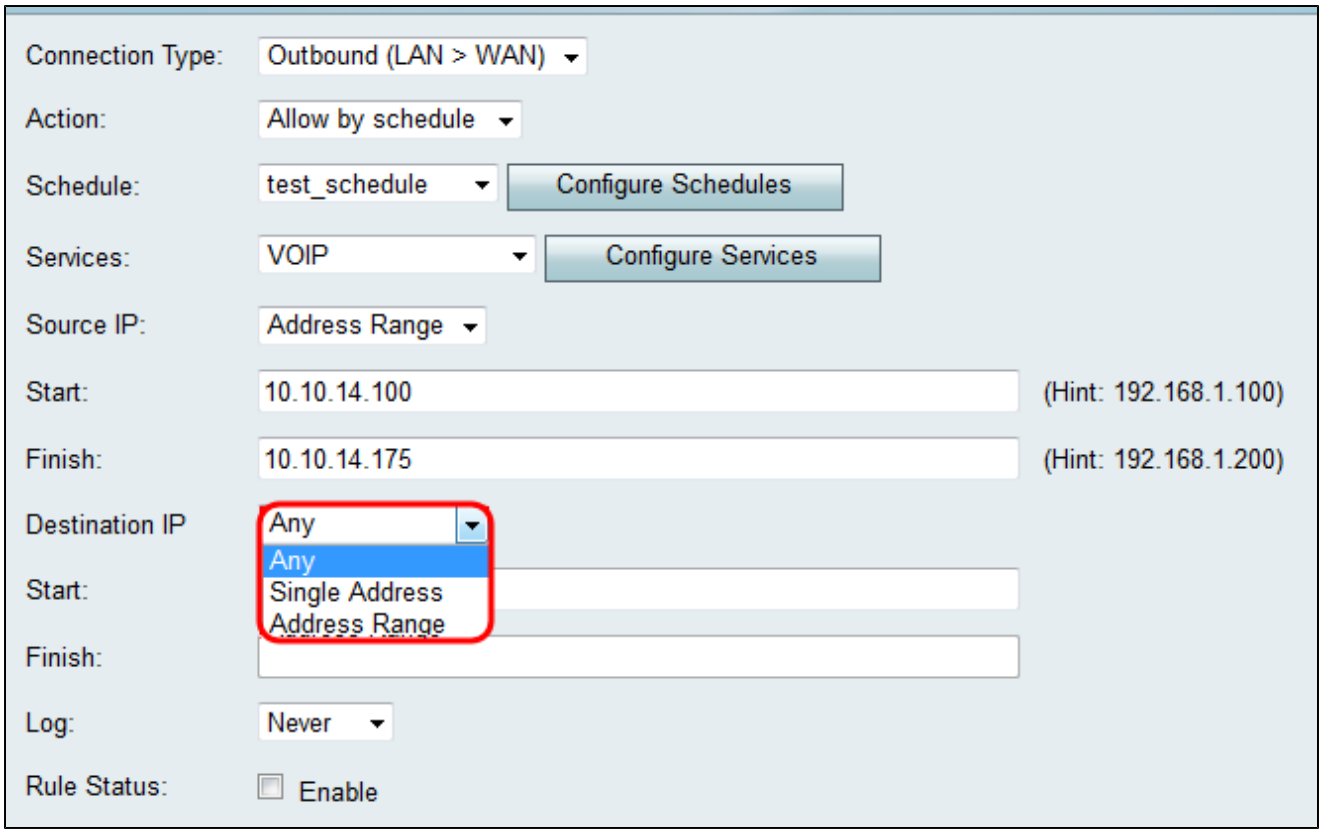
Etapa 2. Se você escolheu Single Address na Etapa 1, insira o endereço IP que será aplicado à regra de acesso no campo Start e vá para a Etapa 4. Se você escolheu Intervalo de endereços na Etapa 1, insira um endereço IP inicial que será aplicado à regra de acesso no campo Início.



Etapa 3. Se você escolheu Address Range na Etapa 1, insira o endereço IP final que encapsulará o intervalo de endereços IP para a regra de acesso no campo Finish.



Etapa 4. Escolha como você deseja definir o IP de destino na lista suspensa IP de destino. Para o tráfego de saída, o IP de destino se refere ao endereço ou endereços (na WAN) para os quais o tráfego é permitido ou negado na rede local.



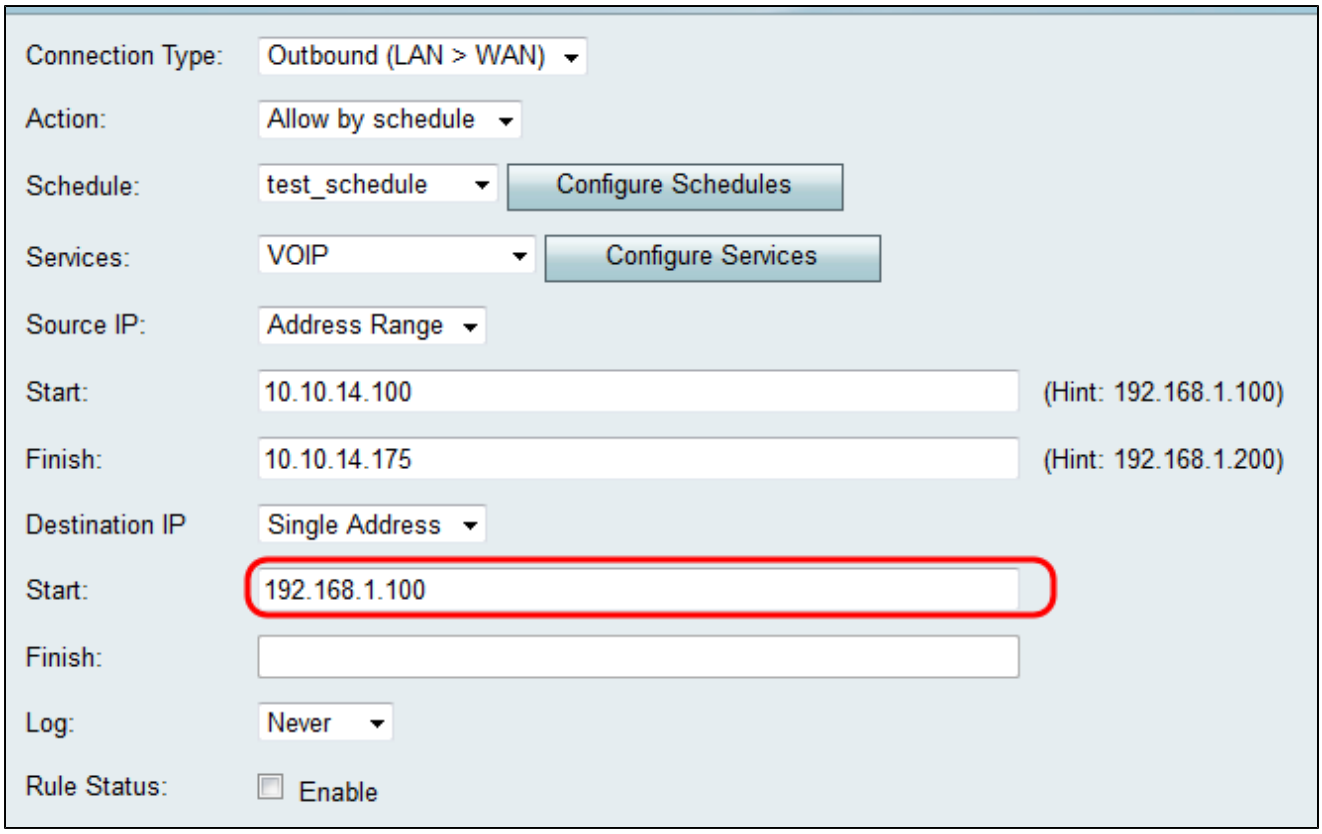
As opções disponíveis são definidas da seguinte forma:

· Qualquer — Aplica-se ao tráfego direcionado a qualquer endereço IP na Internet pública. Portanto, deixe os campos Start e Finish em branco.

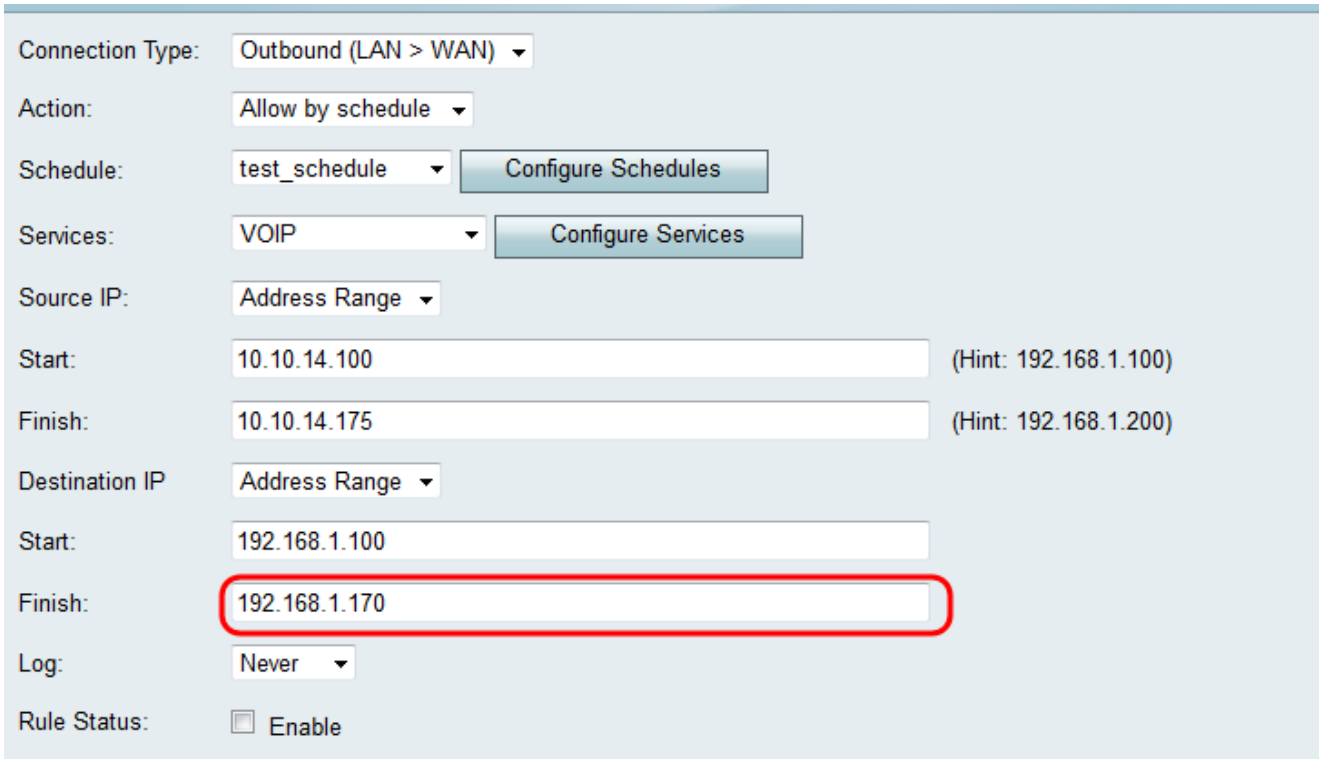
· Endereço único — Aplica-se ao tráfego direcionado a um único endereço IP na Internet pública. Insira o endereço IP no campo Start.

· Intervalo de endereços — Aplica-se ao tráfego direcionado a um intervalo de endereços IP na Internet pública. Insira o endereço IP inicial do intervalo no campo Start e o endereço IP final no campo Finish para definir o intervalo.

Etapa 5. Se você escolheu Single Address na Etapa 4, insira o endereço IP que será aplicado à regra de acesso no campo Start. Se você escolheu Intervalo de endereços na Etapa 4, insira um endereço IP inicial que será aplicado à regra de acesso no campo Início.



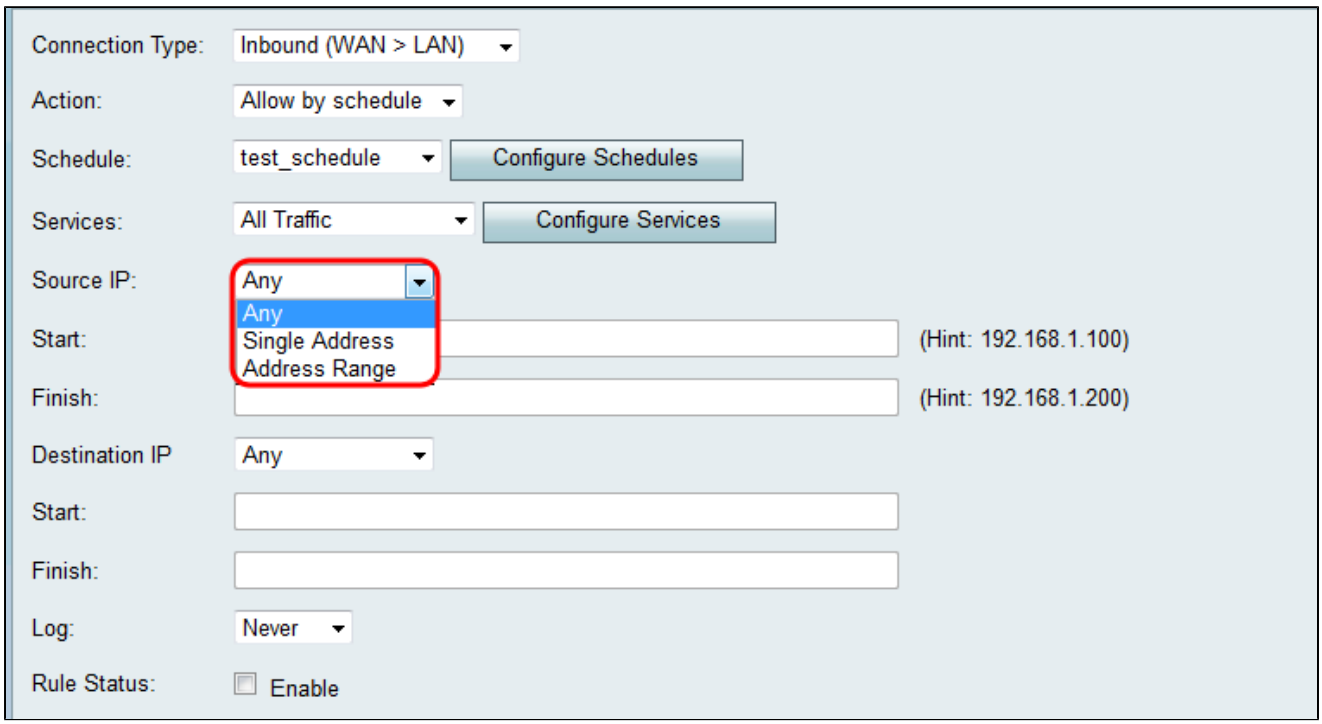
Etapa 6. Se você escolheu Address Range na Etapa 4, insira o End IP Address que encapsulará o IP Address range para a regra de acesso no campo Finish.



Configurando IP de origem e destino para tráfego de entrada

Siga as etapas nesta seção se Inbound (WAN > LAN) ou Inbound (WAN > DMZ) tiver sido selecionado como o Tipo de Conexão na Etapa 3 de Adicionando uma Regra de Acesso.

Etapa 1. Escolha como você deseja definir o IP de origem na lista suspensa IP de origem. Para o tráfego de entrada, o IP de origem se refere ao endereço ou endereços (na WAN) aos quais a regra de firewall se aplicaria.



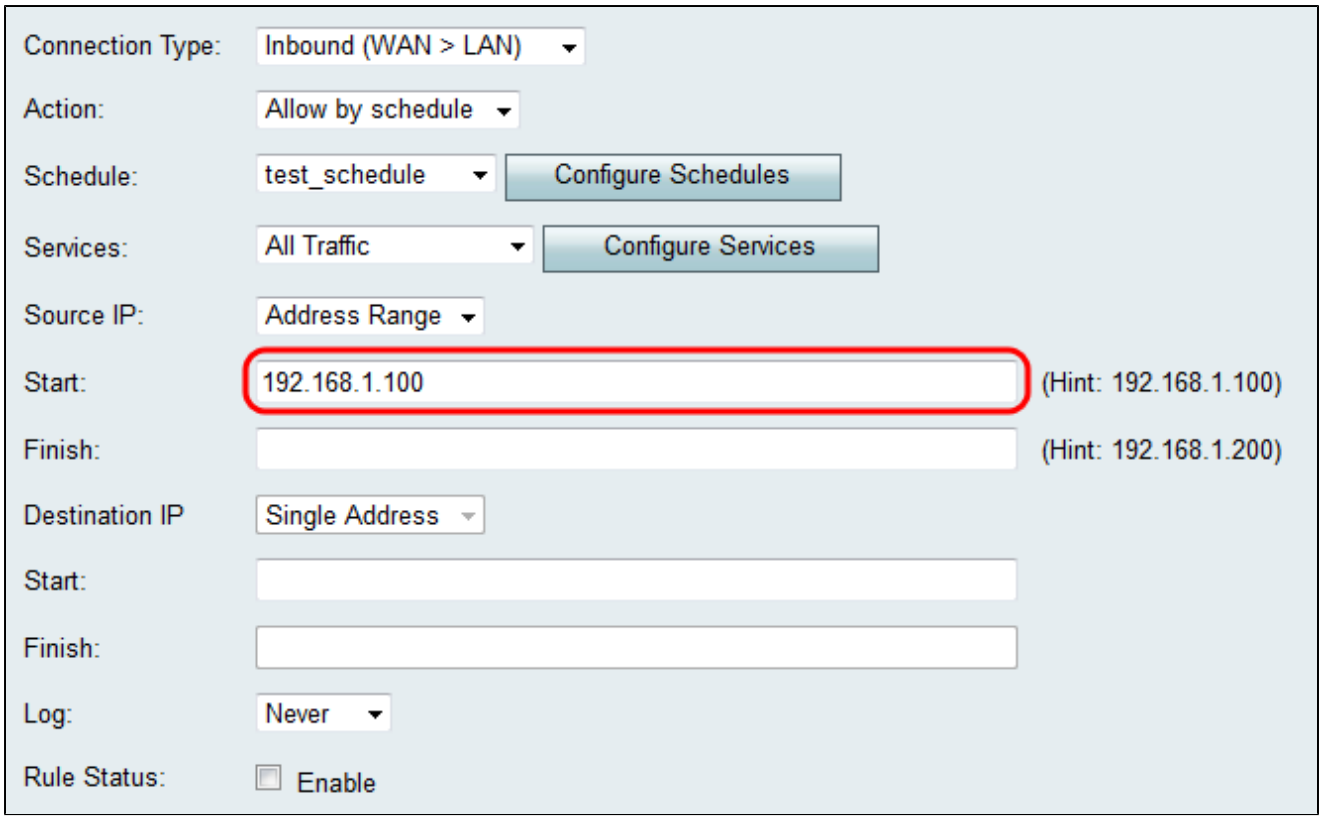
As opções disponíveis são definidas da seguinte forma:

· Qualquer — Aplica-se ao tráfego originado de qualquer endereço IP na Internet pública. Portanto, deixe os campos Start e Finish em branco. Vá para a Etapa 4 se você escolher essa opção.

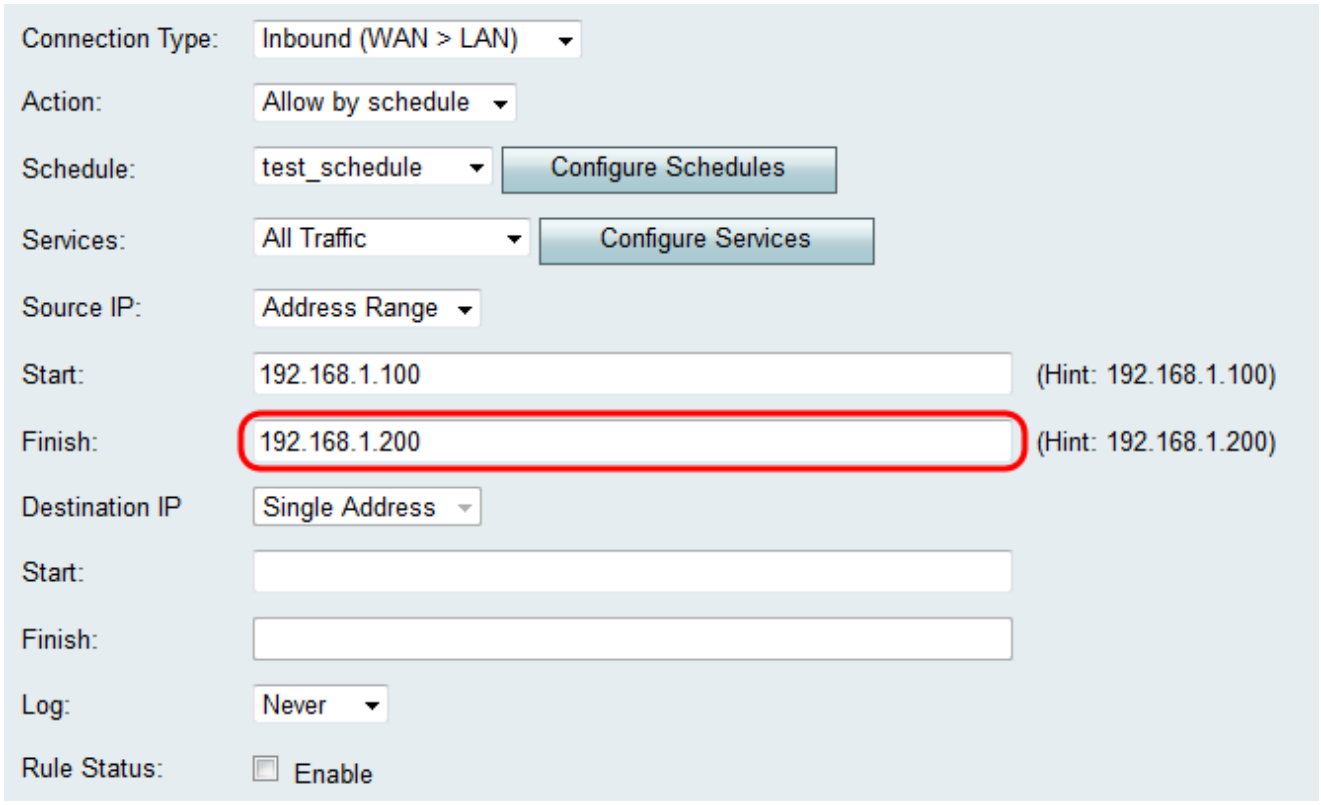
· Endereço único — Aplica-se ao tráfego originado de um único endereço IP na Internet pública. Insira o endereço IP no campo Start.

· Intervalo de endereços — Aplica-se ao tráfego originário de um intervalo de endereços IP na Internet pública. Insira o endereço IP inicial do intervalo no campo Start e o endereço IP final no campo Finish para definir o intervalo.

Etapa 2. Se você escolheu Single Address na Etapa 1, insira o endereço IP que será aplicado à regra de acesso no campo Start e vá para a Etapa 4. Se você escolher Intervalo de endereços na Etapa 1, insira um endereço IP inicial que será aplicado à regra de acesso no campo Início.

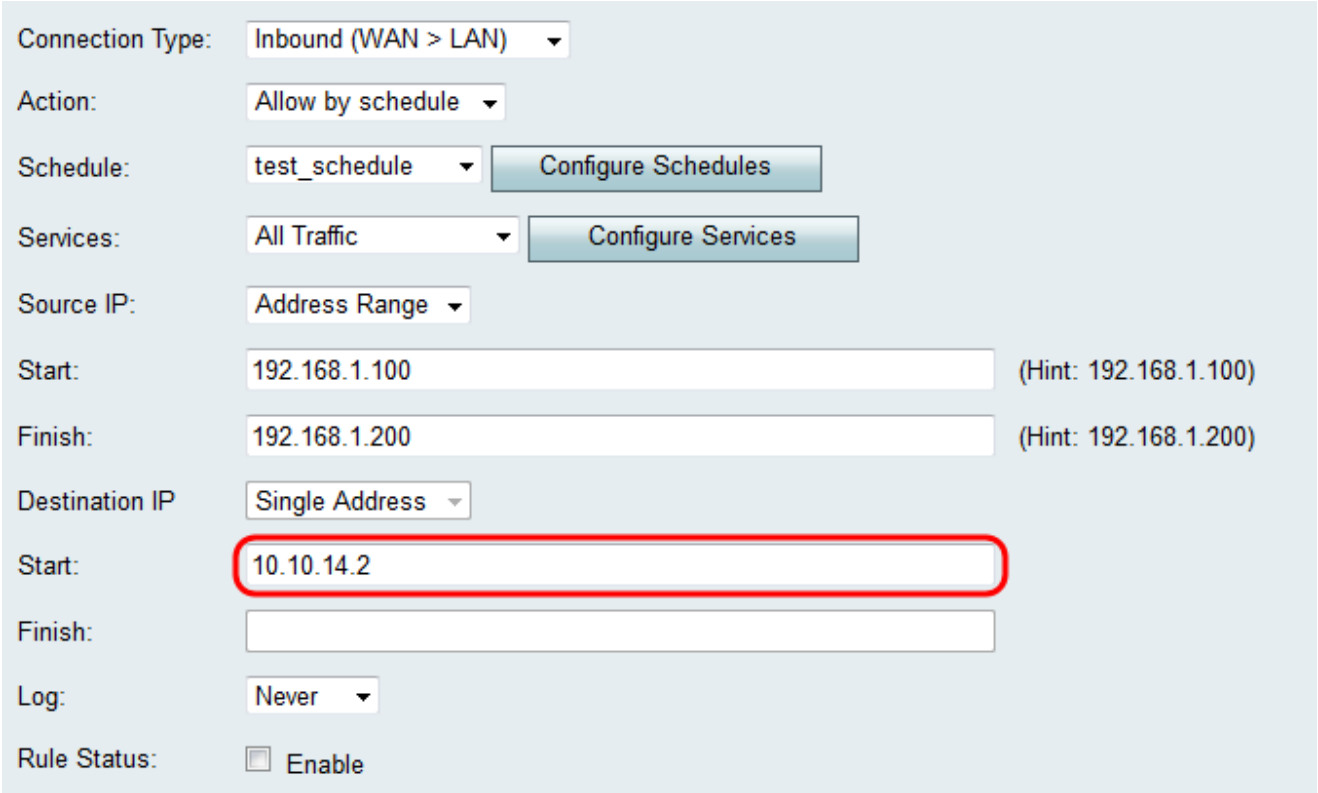


Etapa 3. Se você escolheu Address Range na Etapa 1, insira o endereço IP final que encapsulará o intervalo de endereços IP para a regra de acesso no campo Finish.



Etapa 4. Insira um único endereço para o IP de destino no campo Start abaixo da lista suspensa Destination IP. Para o tráfego de entrada, o IP de destino se refere ao endereço

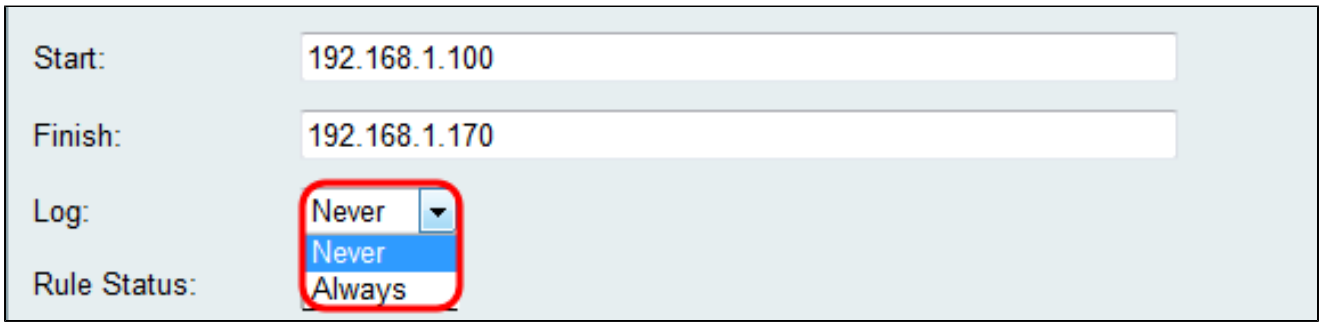
(na LAN) para o qual o tráfego é permitido ou negado a partir da Internet pública.



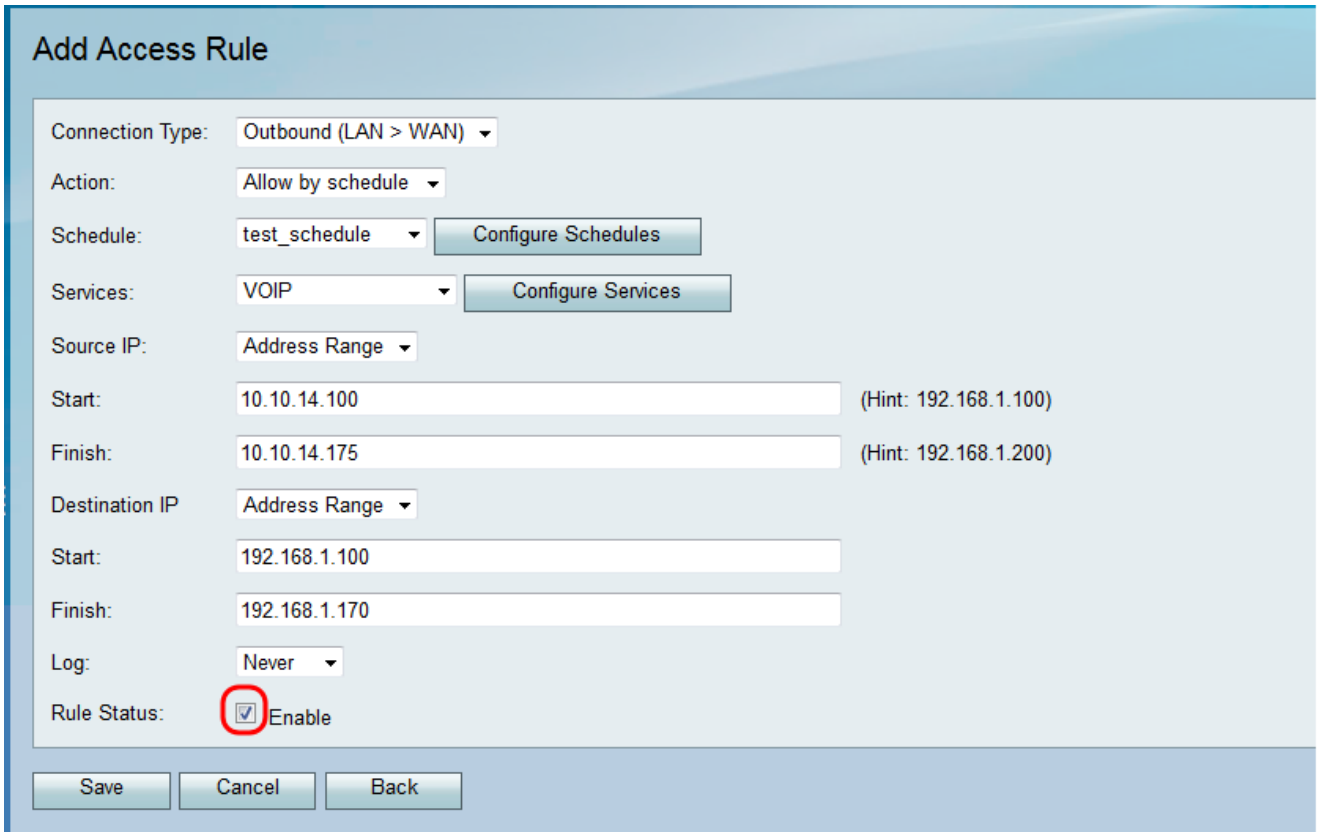
Observação: se Inbound (WAN > DMZ) foi selecionado como o Connection Type (Tipo de conexão) na Etapa 3 de Adding an Access Rule, o Single Address (Endereço único) para o IP de destino será automaticamente configurado com o endereço IP do host DMZ ativado.

Registrando e Ativando a Regra de Acesso

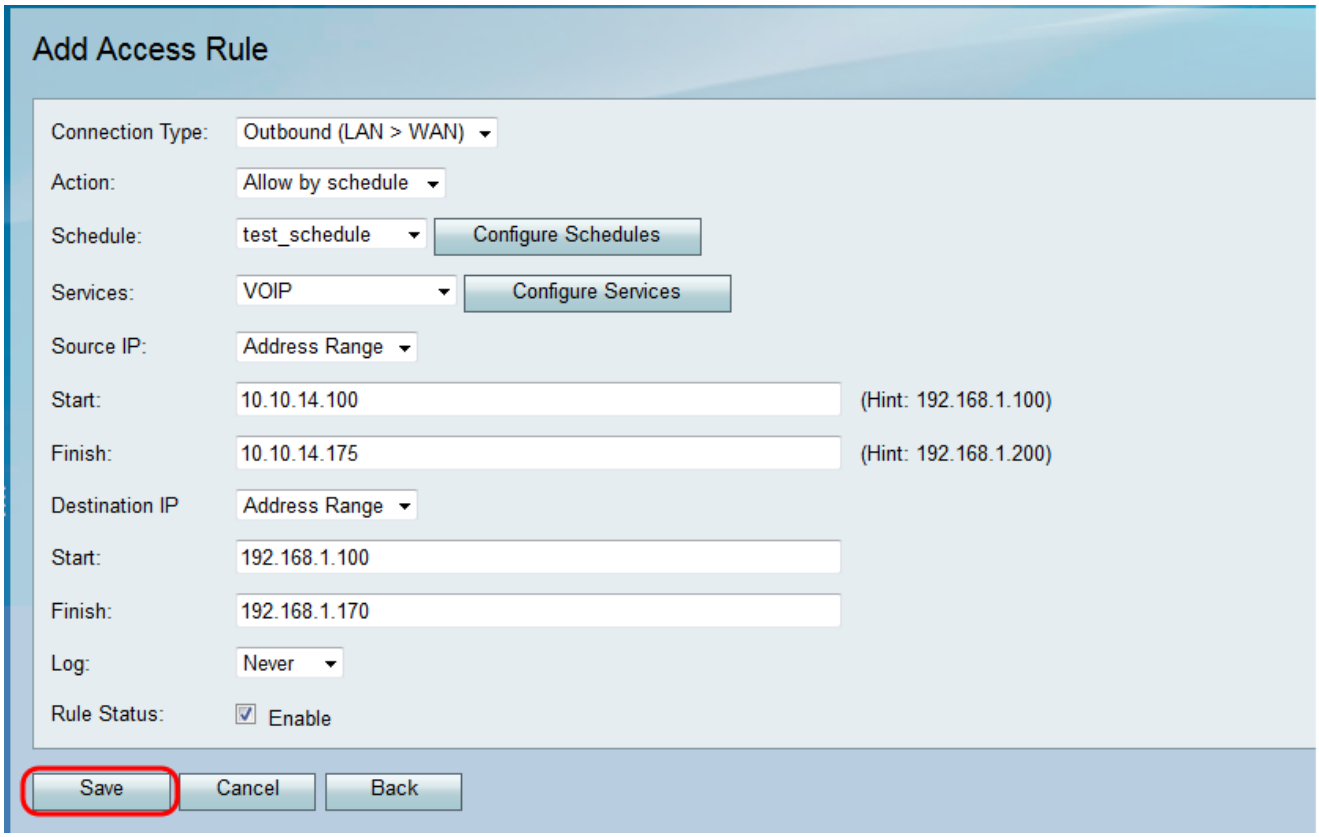
Etapa 1. Selecione Always na lista suspensa Log se quiser que o roteador crie logs sempre que um pacote corresponder a uma regra. Selecione Nunca se quiser que o registro nunca ocorra quando uma regra for correspondida.



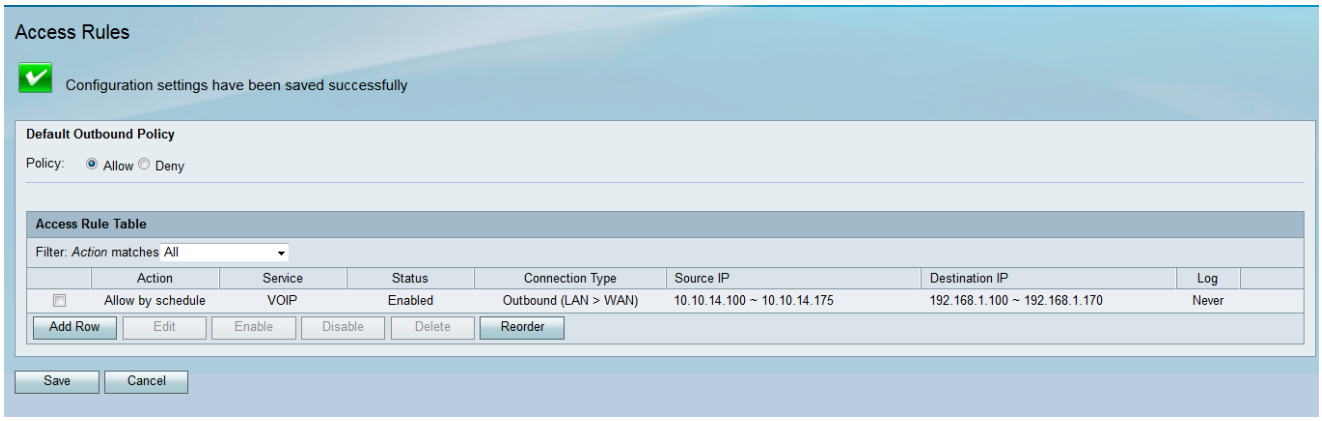
Etapa 2. Marque a caixa de seleção Enable para habilitar a regra de acesso.



Etapa 3. Clique em Salvar para salvar suas configurações.



A Tabela de Regras de Acesso é atualizada com a regra de acesso recém-configurada.


Access Rules
Configuration settings have been saved successfully
Default Outbound Policy
Policy: Allow Deny
Access Rule Table
Filter: Action matches All
Action
Service
Status
Connection Type
Source IP
Destination IP
Log
Allow by schedule
VOIP
Enabled
Outbound (LAN > WAN)
10.10.14.100 ~ 10.10.14.175
192.168.1.100 ~ 192.168.1.170
Never
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel

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.