Configuração da regra de acesso através do assistente em RV016, RV082, RV042 e RV042G VPN Routers

Objetivo

A regra de acesso é usada para determinar se o tráfego tem permissão para entrar na rede através do firewall do roteador ou não para garantir a segurança na rede. Uma regra de acesso é configurada com base em vários critérios para permitir ou negar acesso à rede. A regra de acesso é agendada de acordo com a hora em que as regras de acesso precisam ser aplicadas ao roteador.

Este artigo explica como configurar regras de acesso através de um assistente nos roteadores VPN RV016, RV082, RV042 e RV042G.

Note: Você pode configurar a regra de acesso por meio do Firewall. Para saber mais sobre como configurar a regra de acesso através do Firewall, consulte *Configuração de uma Regra de Acesso IPv4 em RV016, RV082, RV042 e RV042G VPN Routers* para regra de acesso IPv4 e *Configuração de uma Regra de Acesso IPv6 em RV042 Roteadores VPN 016 e RV042G* para regra de acesso IPv6. Você pode agendar a regra de acesso também por meio do Firewall. Para saber mais sobre como agendar a regra de acesso por meio do Firewall, consulte *Regra de Acesso à Agenda em RV016, RV082, RV042 e RV042G*.

Dispositivos aplicáveis

- RV042
- RV042G
- RV082
- RV016

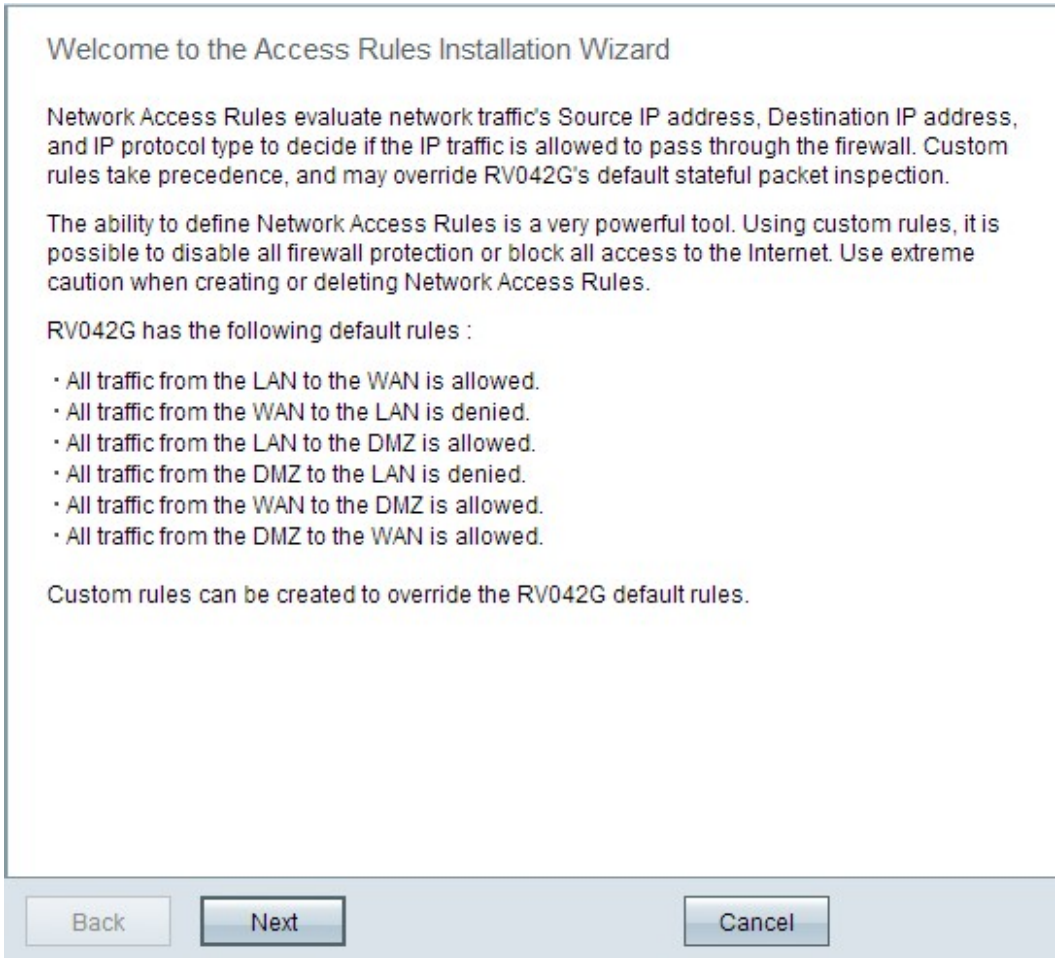
Versão de software

- v4.2.1.02

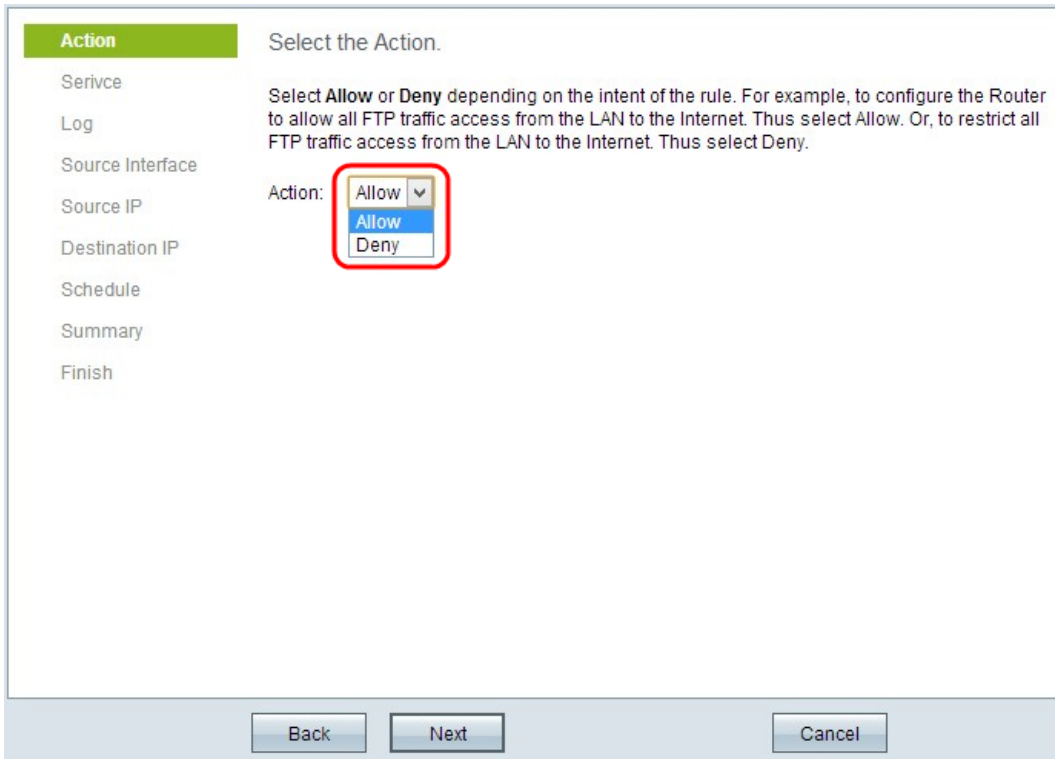
Configuração da regra de acesso

Etapa 1. Use o Utilitário de configuração do roteador para escolher **Wizard**. A página *Assistente* é aberta:

Etapa 2. Clique em **Iniciar agora** na seção Configuração da regra de acesso para configurar o Assistente de instalação da regra de acesso. A página explica as regras de acesso e as regras padrão do roteador.A janela Bem-vindo ao Assistente de Instalação das Regras de Acesso é aberta:



Etapa 3. Clique em **Next (Avançar)** para continuar a configuração.

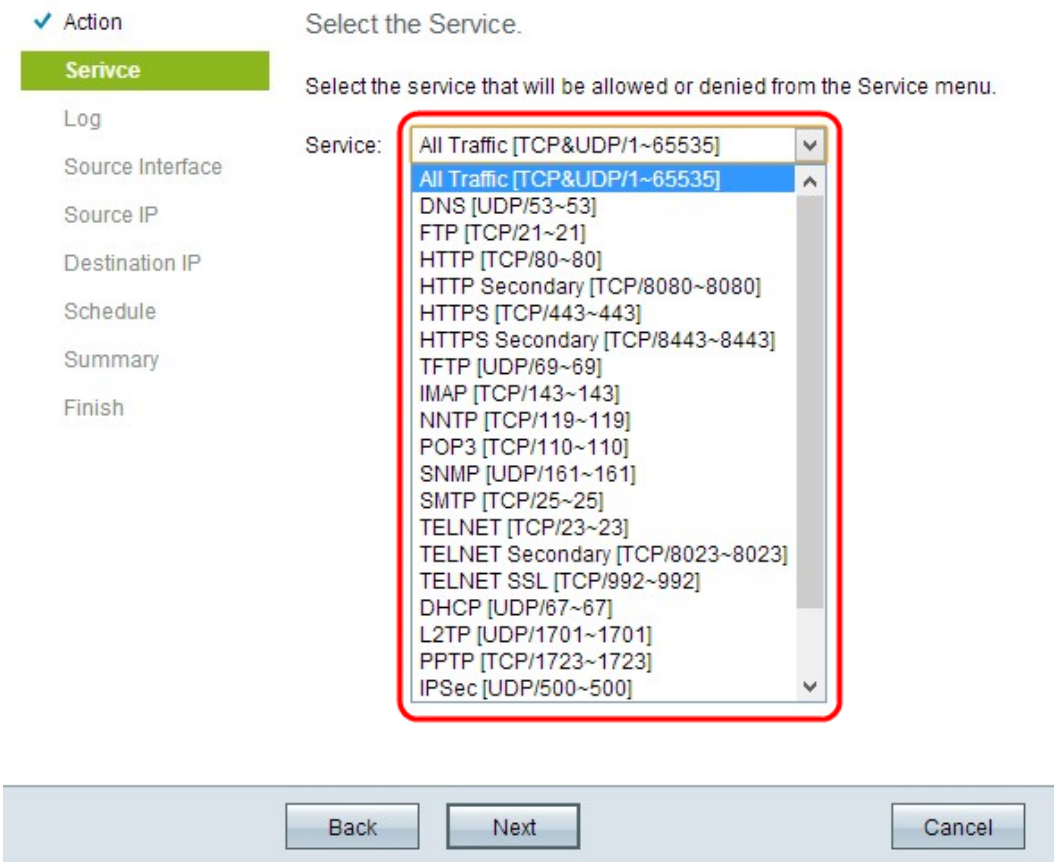


Etapa 4. Escolha o botão de opção apropriado na lista suspensa Ação para permitir ou restringir o tráfego FTP da LAN/WAN para a Internet.

Permitir — Permite que todo o tráfego FTP acesse na Internet a partir da LAN/WAN.

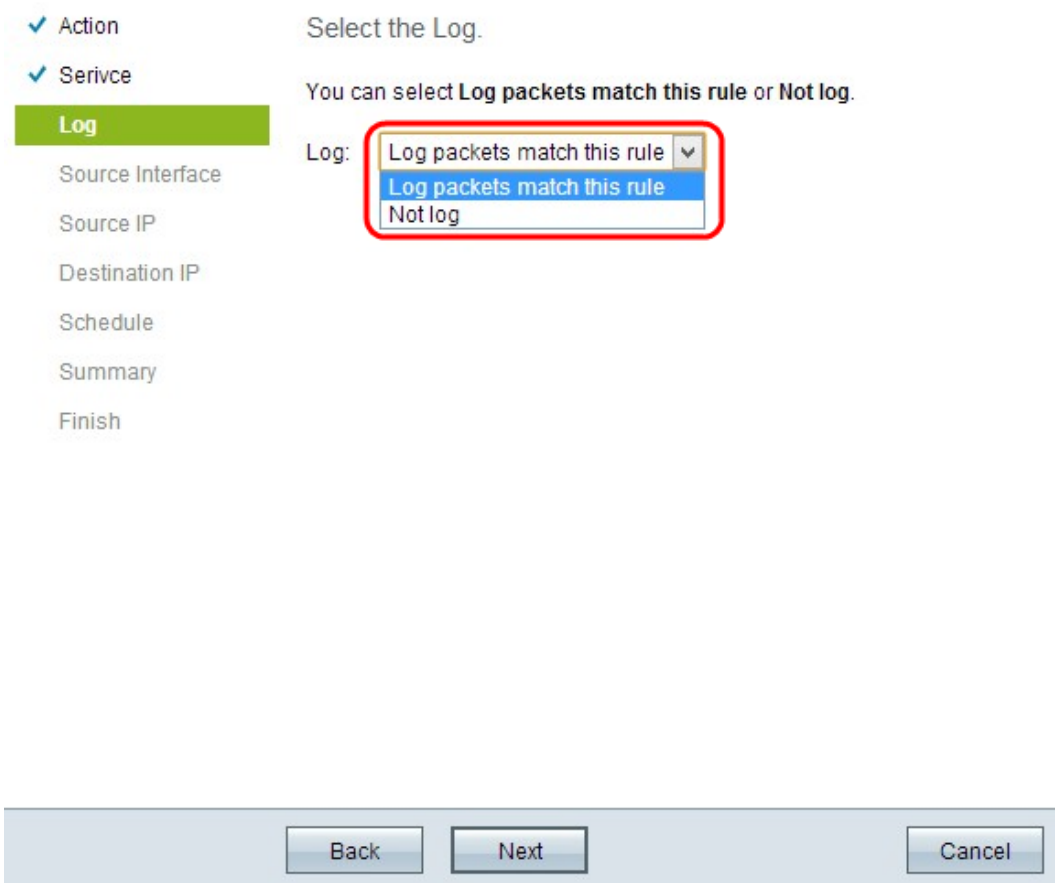
Nega — restringe todo o tráfego FTP ao acesso na Internet a partir da LAN/WAN.

Etapa 5. Clique em **Next (Avançar)** para continuar a configuração.



Etapa 6. Escolha o serviço apropriado que você precisa ter permissão ou negação na lista suspensa Serviço.

Passo 7. Clique em **Next (Avançar)** para continuar a configuração.

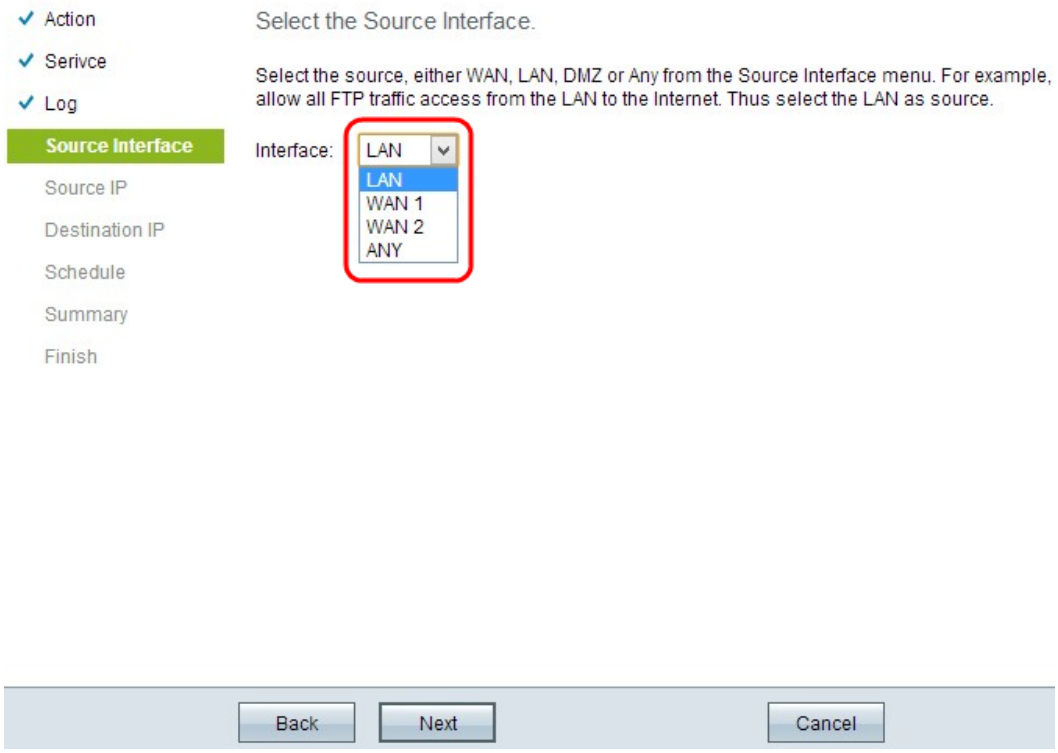


Etapa 8. Escolha a opção Log apropriada na lista suspensa Log.

Os pacotes de log correspondem a essa regra de acesso — Permite que o roteador mantenha o rastreamento de log para o serviço selecionado.

Não registro — Desativa o roteador para manter o rastreamento de log.

Etapa 9. Clique em Avançar para continuar.



Etapa 10. Escolha a interface de origem apropriada na lista suspensa Interface.

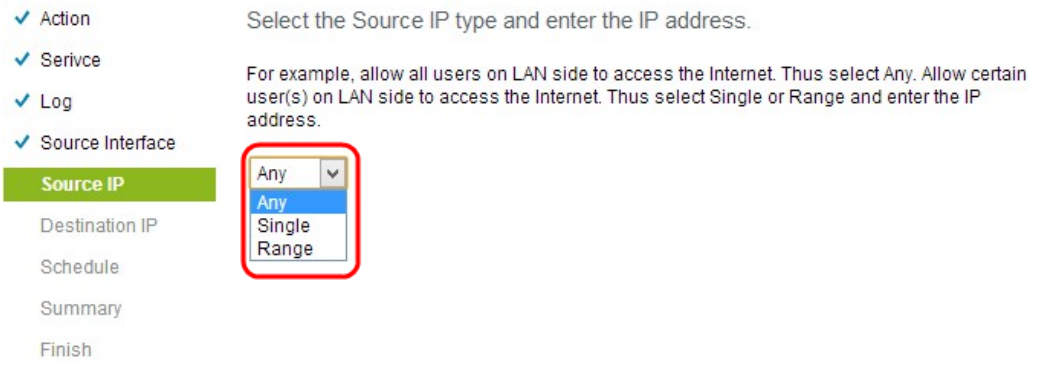
LAN — A interface de origem é Rede local. A regra de acesso afeta somente o tráfego da LAN.

WAN 1 — A interface de origem é Wide Area Network 1. A regra de acesso afeta somente o tráfego da WAN 1.

WAN 2 — A interface de origem é Wide Area Network 2. A regra de acesso afeta somente o tráfego da WAN 2.

Qualquer interface de origem pode ser qualquer rede. A regra de acesso afeta qualquer tráfego.

Etapa 11. Clique em Avançar para continuar.



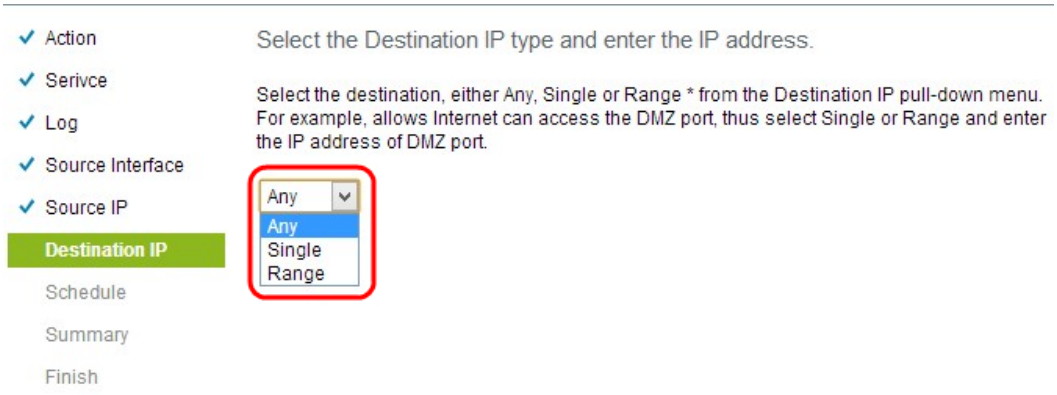
Etapa 12. Escolha o endereço IP de origem apropriado ou um intervalo de endereços IP aos quais a regra de acesso é aplicada na lista suspensa IP de origem.

Qualquer usuário com qualquer endereço IP pode acessar a Internet.

Única — Somente o usuário único com um único endereço IP pode acessar a Internet. Se você escolher Single (Único), será necessário inserir o endereço IP específico.

Intervalo — Somente os usuários com o intervalo de endereços IP podem acessar a Internet. Se você escolher Intervalo, precisará inserir os endereços IP inicial e final.

Etapa 13. Role para baixo e clique em **Next (Avançar)** para continuar a configuração.



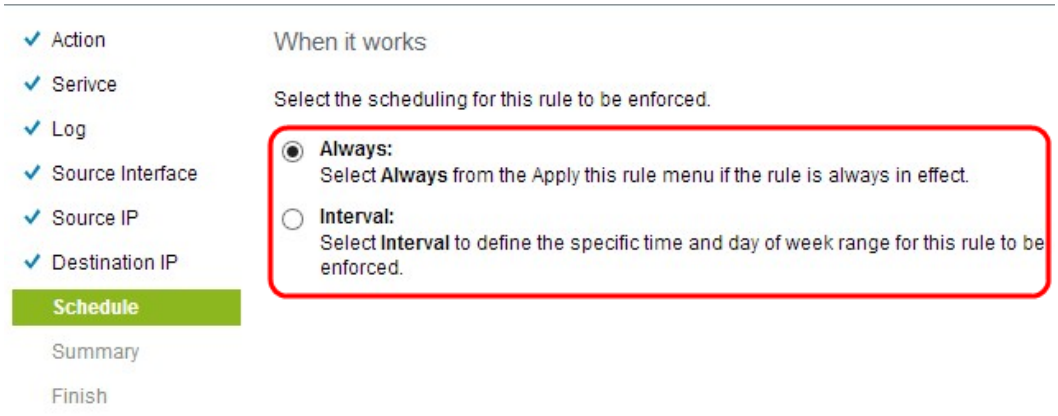
Etapa 14. Escolha o endereço IP de destino apropriado ou o intervalo de endereços IP para a regra de acesso na lista suspensa IP de destino.

Qualquer interface de destino pode ter qualquer endereço IP.

Single - A interface de destino pode ser o endereço IP único específico. Se você escolher Single (Único), precisará inserir o endereço IP único específico.

Intervalo — A interface de destino pode ser qualquer um dos endereços IP do intervalo especificado. Se você escolher Intervalo, precisará inserir os endereços IP inicial e final.

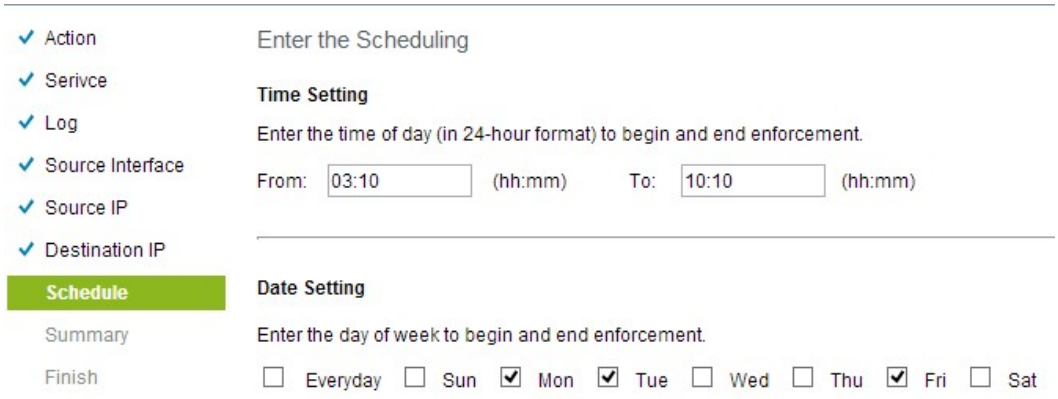
Etapa 15. Role para baixo e clique em **Next (Avançar)** para continuar a configuração.



Etapa 16. Clique no botão de opção apropriado para escolher a hora em que deseja aplicar a regra de acesso no roteador.

Sempre — As regras de acesso sempre se aplicam no roteador. Se você escolher essa opção, pule a Etapa 17 para a Etapa 19. O padrão é Sempre.

Intervalo — As regras de acesso são aplicadas para algumas horas específicas de acordo com a hora definida. Se você escolher essa opção, precisará inserir o intervalo de tempo para que a regra de acesso seja aplicada.

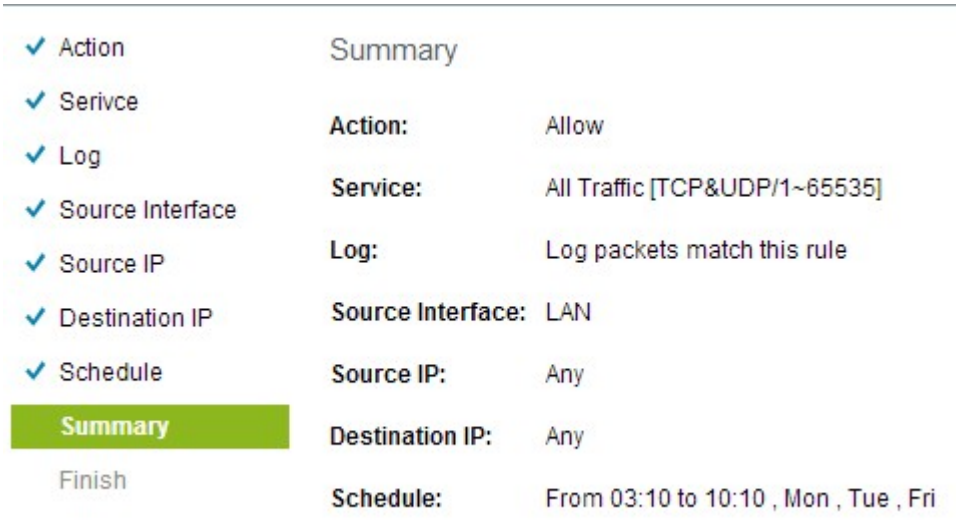


Etapa 17. Insira a hora a partir da qual deseja aplicar a programação para a lista de acesso no campo De. O formato da hora é: milímetro.

Etapa 18. Insira o tempo até o qual deseja aplicar a programação para a lista de acesso no campo Para. O formato da hora é: milímetro.

Etapa 19. Marque a caixa de seleção específica quando quiser aplicar a agenda para a lista de acesso.

Etapa 20. Role para baixo e clique em **Next (Avançar)** para continuar a configuração. A janela Resumo com informações detalhadas da regra de acesso é aberta:



Etapa 21. Role para baixo e clique em **Instalar** para instalar a configuração.

Etapa 22. Clique em **OK** para salvar as configurações e retornar à página Assistente.

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.