Roteamento entre VLANs em um roteador RV34x com restrições de ACL direcionadas

Objetivo

Este artigo explica como configurar o roteamento de Rede Local Inter-Virtual (VLAN - Inter-Virtual Local Area Network) em um roteador da série RV34x com ACL (Access Control List) direcionada para restringir determinados tráfegos. O tráfego pode ser restrito por endereço IP, um grupo de endereços ou por tipo de protocolo.

Introduction

As VLANs são ótimas, elas definem domínios de broadcast em uma rede de Camada 2. Os domínios de broadcast são normalmente limitados por roteadores porque eles não encaminham quadros de broadcast. Os switches de Camada 2 criam domínios de broadcast com base na configuração do switch. O tráfego não pode passar diretamente para outra VLAN (entre domínios de broadcast) dentro do switch ou entre dois switches. As VLANs permitem manter diferentes departamentos independentes entre si. Por exemplo, talvez você não queira que o departamento de vendas tenha qualquer envolvimento com o departamento de contabilidade.

A independência é fantástica, mas e se você quiser que os usuários finais nas VLANs sejam capazes de rotear entre si? O departamento de vendas pode precisar enviar registros ou folhas de horas para o departamento de contabilidade. O departamento de contabilidade pode querer enviar notificações para a equipe de vendas em seus números de pagamento ou de vendas. É quando o roteamento entre VLANs salva o dia!

Para comunicação entre VLANs, é necessário um dispositivo da camada 3 de Interconexões de Sistemas Abertos (OSI - Open Systems Interconnections), geralmente um roteador. Esse dispositivo de camada 3 precisa ter um endereço IP (Internet Protocol) em cada interface VLAN e ter uma rota conectada a cada uma dessas sub-redes IP. Os hosts em cada sub-rede IP podem então ser configurados para usar os respectivos endereços IP da interface VLAN como seu gateway padrão. Depois de configurados, os usuários finais podem enviar uma mensagem para um usuário final na outra VLAN. Parece perfeito, certo?

Mas espere, e o servidor em contabilidade? Há informações confidenciais nesse servidor que devem permanecer protegidas. Não tenha medo, também há uma solução para isso! As regras ou políticas de acesso no roteador da série RV34x permitem que a configuração de regras aumente a segurança na rede. As ACLs são listas que bloqueiam ou permitem que o tráfego seja enviado de e para determinados usuários. As regras de acesso podem ser configuradas para estarem em vigor o tempo todo ou com base nos agendamentos definidos.

Este artigo o guiará pelas etapas de configuração de uma segunda VLAN, roteamento entre VLANs e uma ACL.

Dispositivos aplicáveis

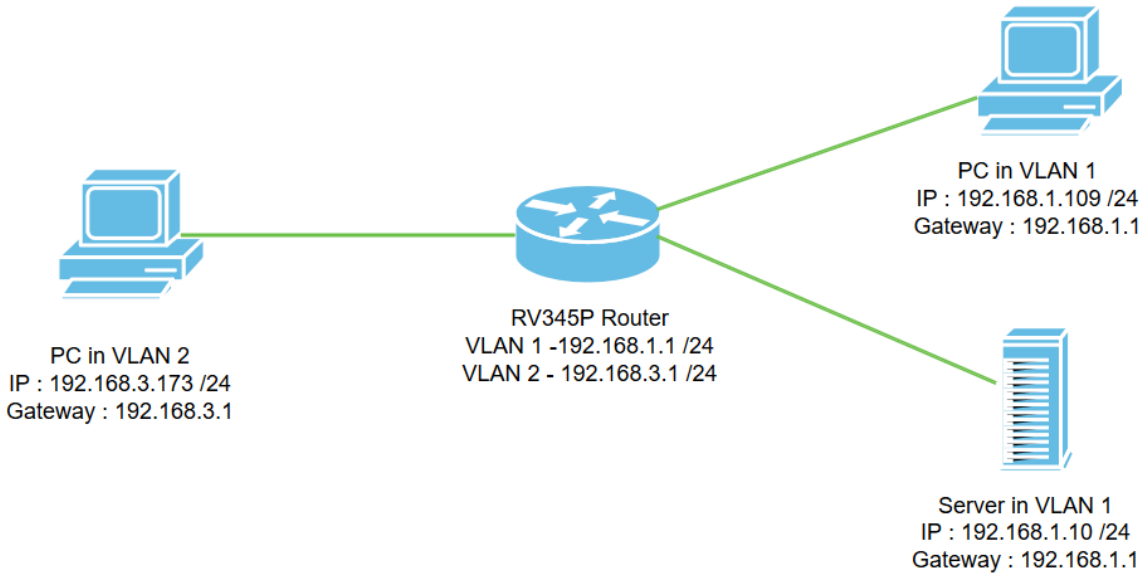
- RV340
- RV340W
- RV345

- RV345P

Versão de software

- 1.0.03.16

Topologia



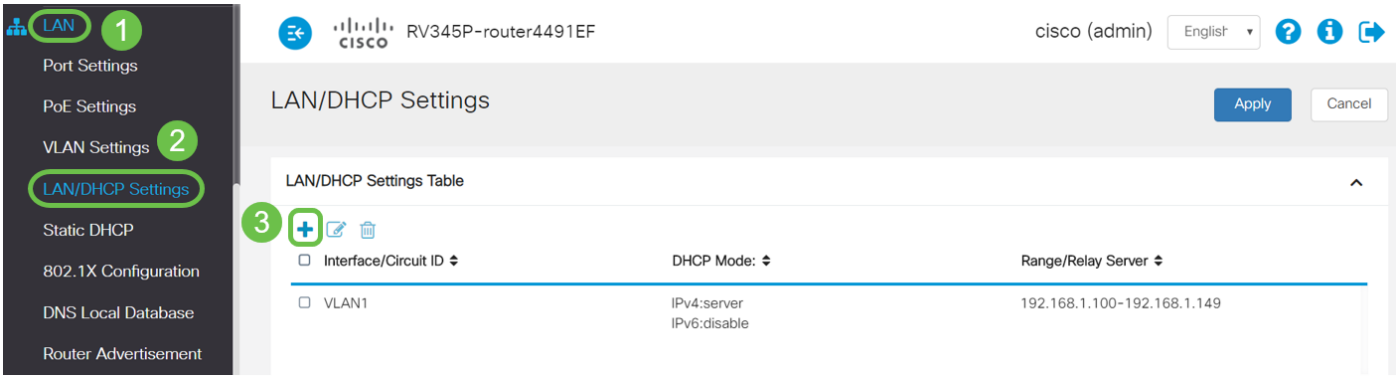
Neste cenário, o roteamento entre VLANs será ativado para VLAN1 e VLAN2 para que os usuários nessas VLANs possam se comunicar entre si. Como medida de segurança, evitaremos que os usuários de VLAN2 possam acessar o servidor de VLAN1 [Internet Protocol versão 4 (IPv4)]: 192.168.1.10 /24].

Portas do roteador usadas:

- O PC (Personal Computer) na VLAN1 está conectado na porta *LAN1*.
- O PC (Personal Computer) na VLAN2 está conectado na porta *LAN2*.
- O servidor na VLAN1 está conectado na porta *LAN3*.

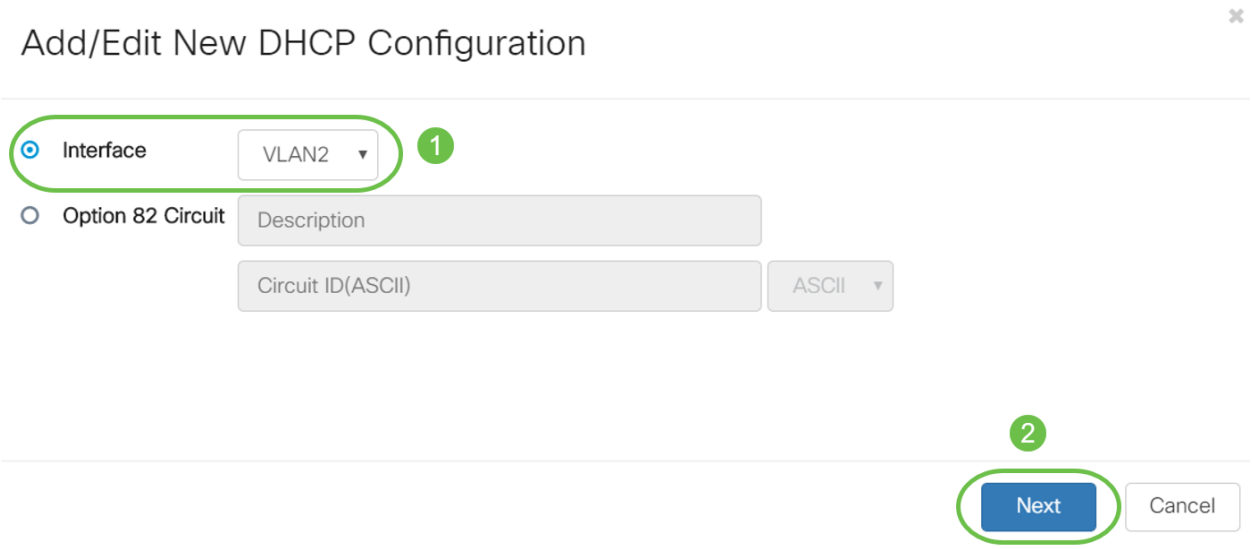
Configuração

Etapa 1. Faça login no utilitário de configuração da Web do roteador. Para adicionar uma nova interface VLAN no roteador, navegue para **LAN > Configurações de LAN/DHCP** e clique no **ícone de mais** na *Tabela de configurações de LAN/DHCP*.

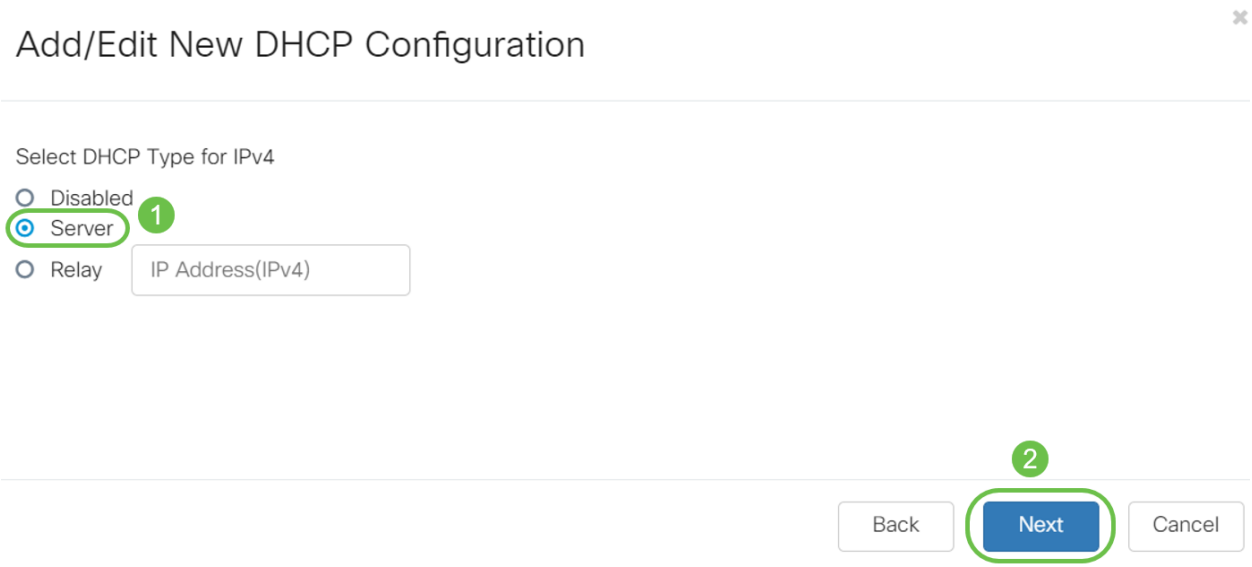


Note: A interface VLAN1 é criada no roteador RV34x por padrão e o servidor DHCP para IPv4 está ativado.

Etapa 2. Uma nova janela pop-up será aberta com a **interface** *VLAN2* selecionada e clique em **Avançar**.



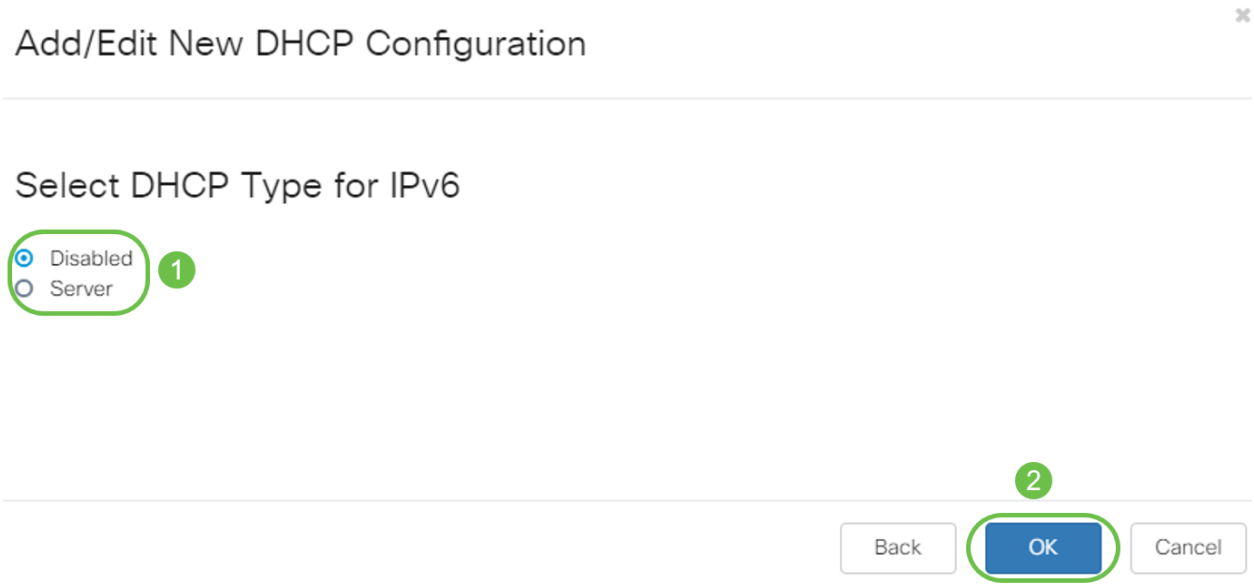
Etapa 3. Para habilitar o servidor DHCP na interface VLAN2, em *Select DHCP Type for IPv4,* selecione **Server**. Clique em Next.



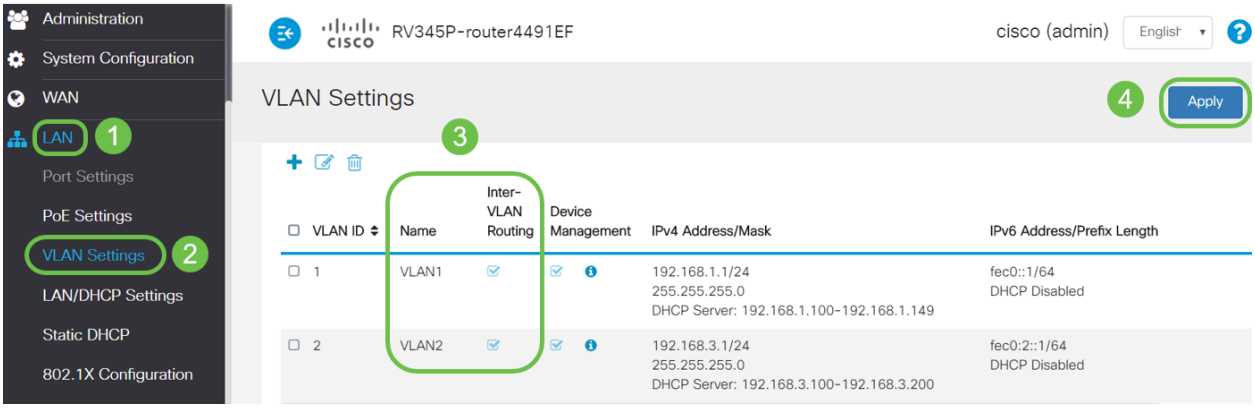
Etapa 4. Insira os parâmetros de configuração do servidor DHCP incluindo *Client Lease Time, Range Start, Range End* e *DNS Server.* Clique em Next.

Etapa 5. (Opcional) Você pode desabilitar o *tipo de DHCP para IPv6* marcando a caixa de seleção **Desabilitado**, pois este exemplo é baseado em IPv4. Click **OK**. A configuração do servidor DHCP está concluída.

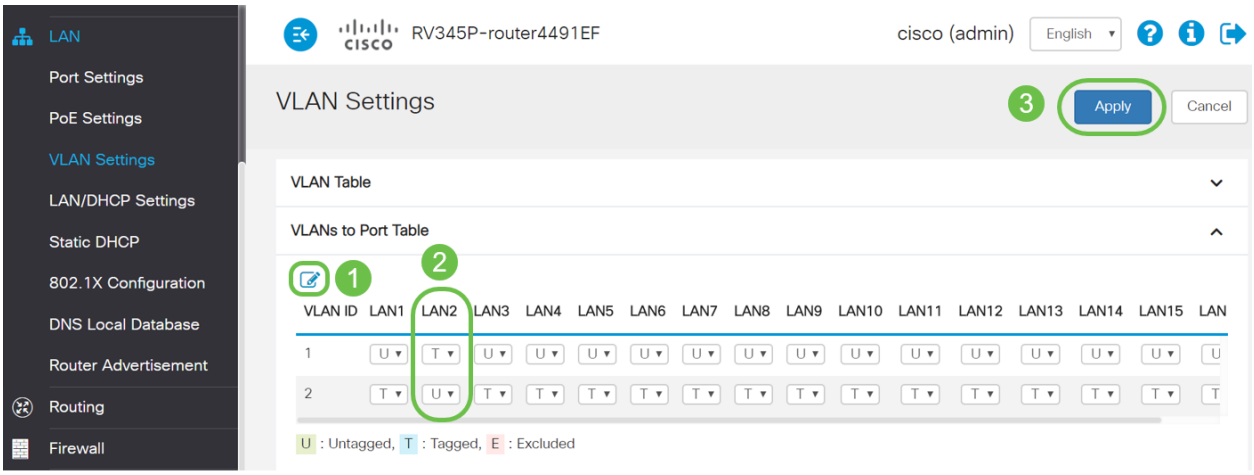
Note: Você pode usar IPv6.



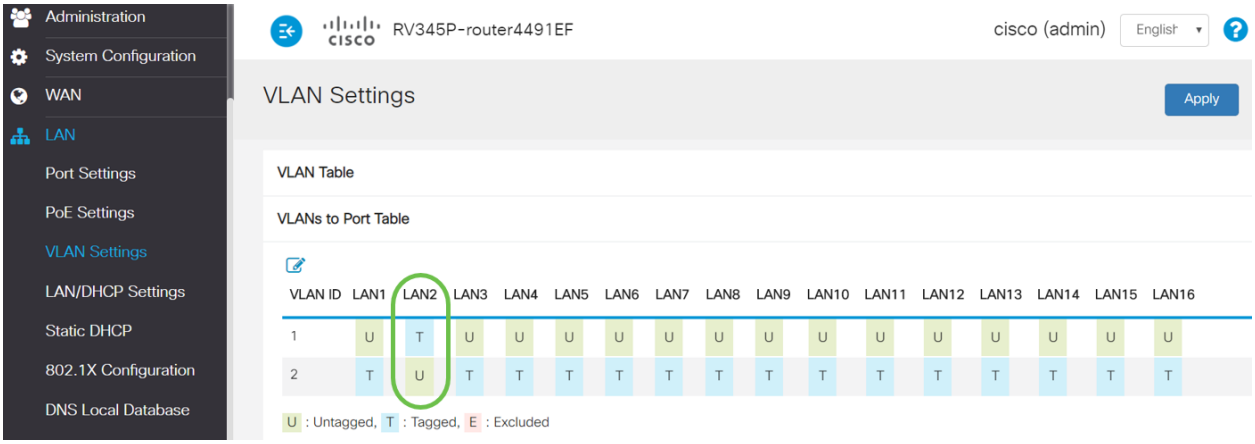
Etapa 6. Navegue até **LAN > VLAN Settings** e verifique se o *Inter-VLAN Routing* está ativado para VLANs, VLAN1 e VLAN2. Essa configuração permitirá a comunicação entre ambas as VLANs. Clique em Apply.



Passo 7. Para atribuir o tráfego não marcado para VLAN2 na porta *LAN2*, clique no botão de edição na opção *VLANs para Tabela de Portas*. Agora, na porta LAN2, selecione a opção **T** (Marcado) para *VLAN1* e **U** (Não Marcado) para *VLAN2* no menu suspenso. Clique em **Apply** para salvar a configuração. Essa configuração encaminhará o tráfego não marcado para VLAN2 na porta LAN2 para que a placa de rede (NIC) do PC, normalmente não capaz de rotulação de VLAN, possa obter o IP DHCP da VLAN2 e fazer parte da VLAN2.

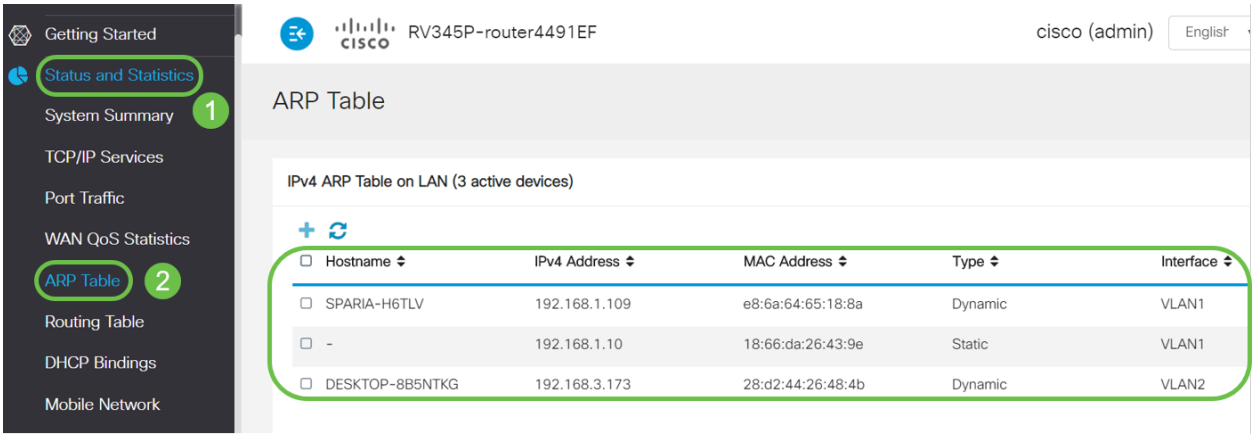


Etapa 8. Verifique se as configurações de VLAN2 para a porta *LAN2* estão sendo exibidas como U *(Não Marcado)*. Para as portas LAN restantes, as configurações de VLAN2 serão *T (Marcado)* e o tráfego de VLAN1 será *U (Não Marcado)*.

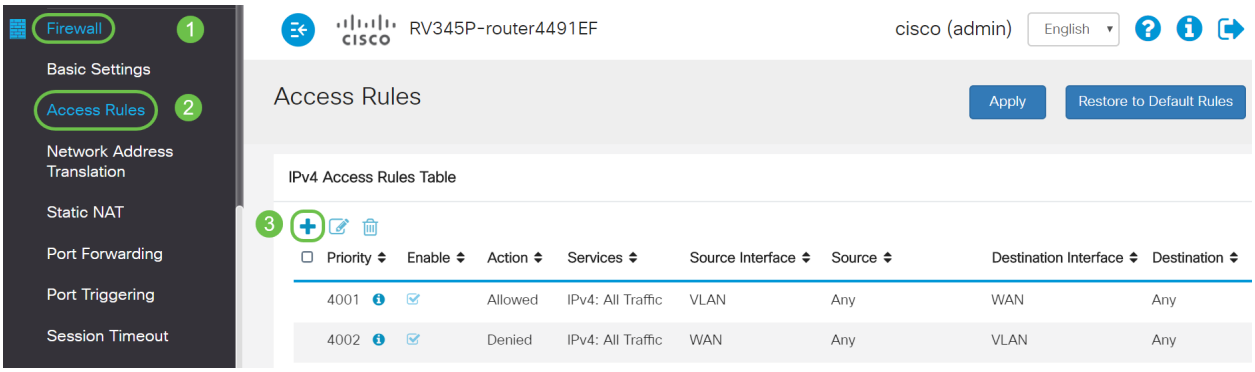


Etapa 9. Navegue até **Status and Statistics > ARP Table** e verifique o *endereço IPv4* dinâmico dos PCs em VLANs diferentes.

Note: O IP do servidor na VLAN1 foi atribuído estaticamente.



Etapa 10. Aplicar ACL para restringir o servidor (IPv4: 192.168.1.10/24) dos usuários da VLAN2. Para configurar a ACL, navegue até **Firewall > Access Rules** e clique no **ícone de mais** para adicionar uma nova regra.



Etapa 11. Configure os parâmetros *das regras de acesso*. Para esse cenário, os parâmetros serão os seguintes:

Status da regra: Enable

Ação: Negar

Serviços: Todo o tráfego

Registro: Verdadeiro

Interface de origem: VLAN2

Endereço de origem: qualquer um

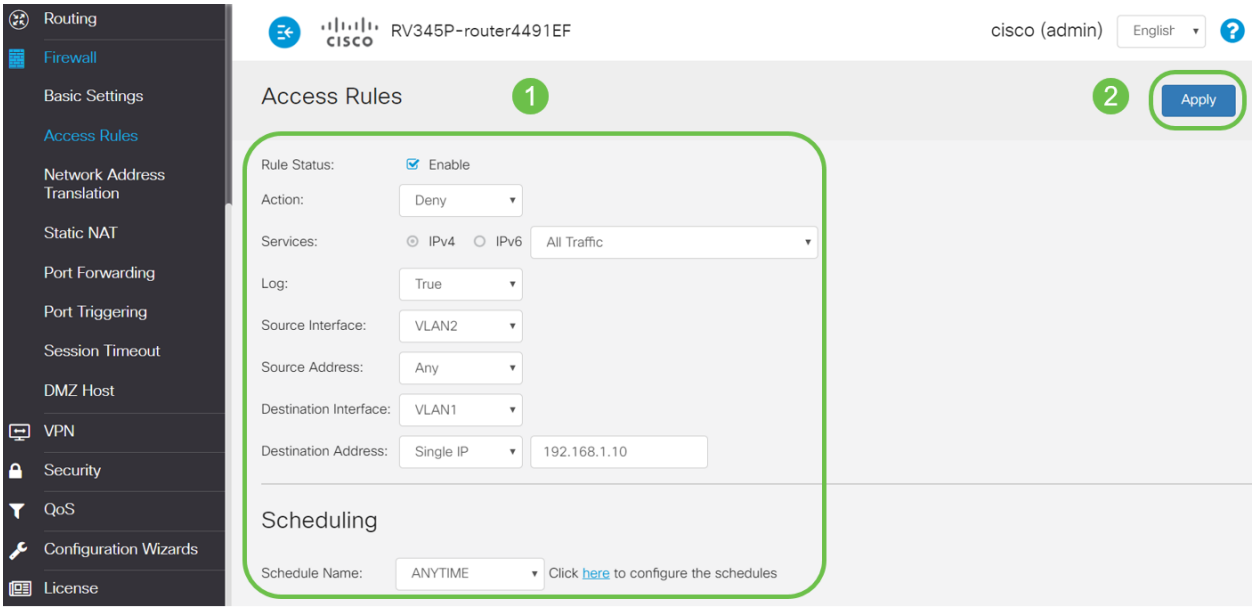
Interface de destino: VLAN1

endereço de destino: IP único 192.168.1.10

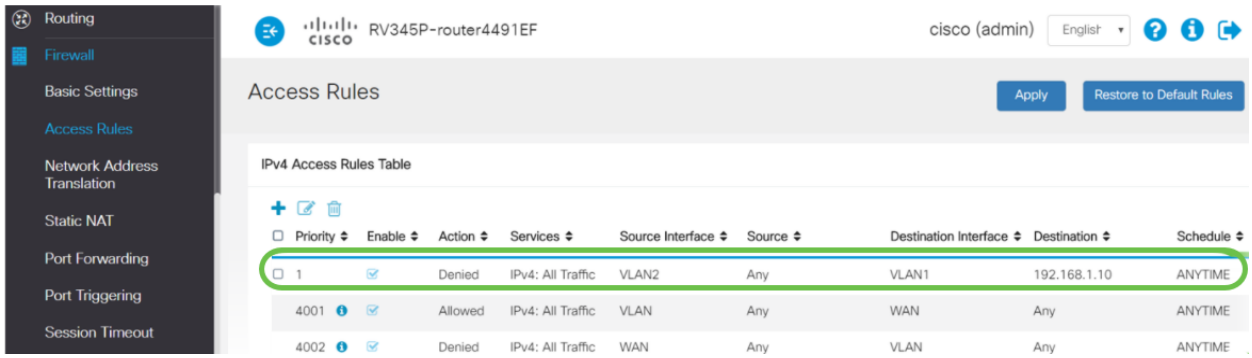
Nome da programação: A qualquer momento

Clique em Apply.

Note: Neste exemplo, negamos o acesso de qualquer dispositivo da VLAN2 ao servidor e, em seguida, permitimos o acesso aos outros dispositivos na VLAN1. Suas necessidades podem variar.



Etapa 12. A lista *de regras de acesso* será exibida da seguinte forma:



A regra de acesso é definida explicitamente para restringir o acesso do servidor, 192.168.1.10, dos usuários da VLAN2.

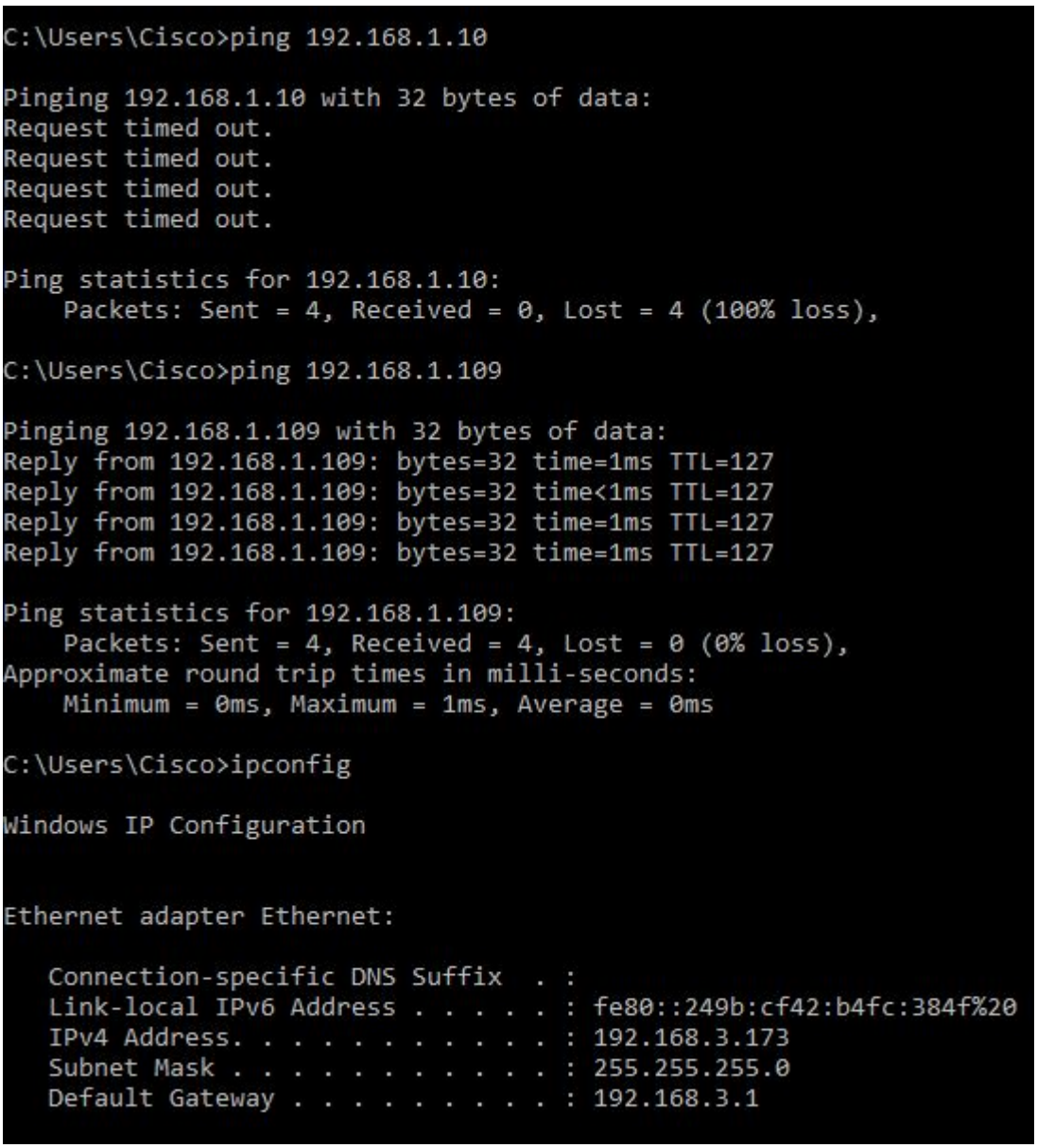
Verificação

Para verificar o serviço, abra o prompt de comando. Nas plataformas Windows, isso pode ser feito clicando no botão Windows e digitando **cmd** na caixa inferior esquerda de pesquisa no

computador e selecione **Command Prompt** no menu.

Insira os seguintes comandos:

- No PC (192.168.3.173) na VLAN2, faça ping no servidor (IP: 192.168.1.10). Você receberá uma notificação *de tempo limite de solicitação*, o que significa que a comunicação não é permitida.
- No PC (192.168.3.173) na VLAN2, faça ping no outro PC (192.168.1.109) na VLAN1. Você receberá uma resposta bem-sucedida.



Conclusão

Você viu as etapas necessárias para configurar o roteamento entre VLANs em um roteador da série RV34x e como fazer uma restrição de ACL direcionada. Agora você pode pegar todo esse conhecimento e usá-lo para criar VLANs em sua rede que se adaptarão às suas necessidades!