Configurar listas de acesso baseadas em IPv4 nos switches gerenciados 200/300 Series

Objetivo

As listas de acesso são regras que você pode aplicar para permitir ou negar um fluxo de tráfego específico na rede, o que adiciona mais segurança e aumenta o desempenho geral na rede.

O objetivo deste documento é mostrar como configurar listas de acesso baseadas em IPv4 nos Switches Gerenciados da Série 200/300.

Dispositivos aplicáveis

·Switches gerenciados SF/SG 200 e SF/SG 300 Series

Versão de software

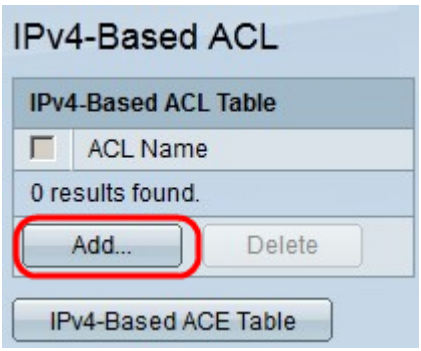
•1.3.0.62

Configuração de ACL e ACE baseadas em IPv4

ACLs baseadas em IPv4

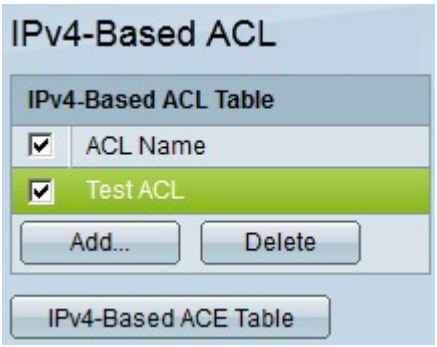
Etapa 1. Faça login no utilitário de configuração da Web e escolha **Controle de acesso > ACL baseada em IPv4**. A página *ACL baseada em IPv4* é aberta.

Etapa 2. Clique em **Adicionar** para adicionar uma nova lista de acesso.



Etapa 3. No campo *Nome da ACL*, insira um nome para a nova lista de acesso.

Etapa 4. Clique em **Aplicar** para salvar a lista de acesso.



Etapa 5. (Opcional) Para excluir uma lista de acesso, marque a caixa de seleção da lista de acesso que deseja excluir e clique em **Excluir**.

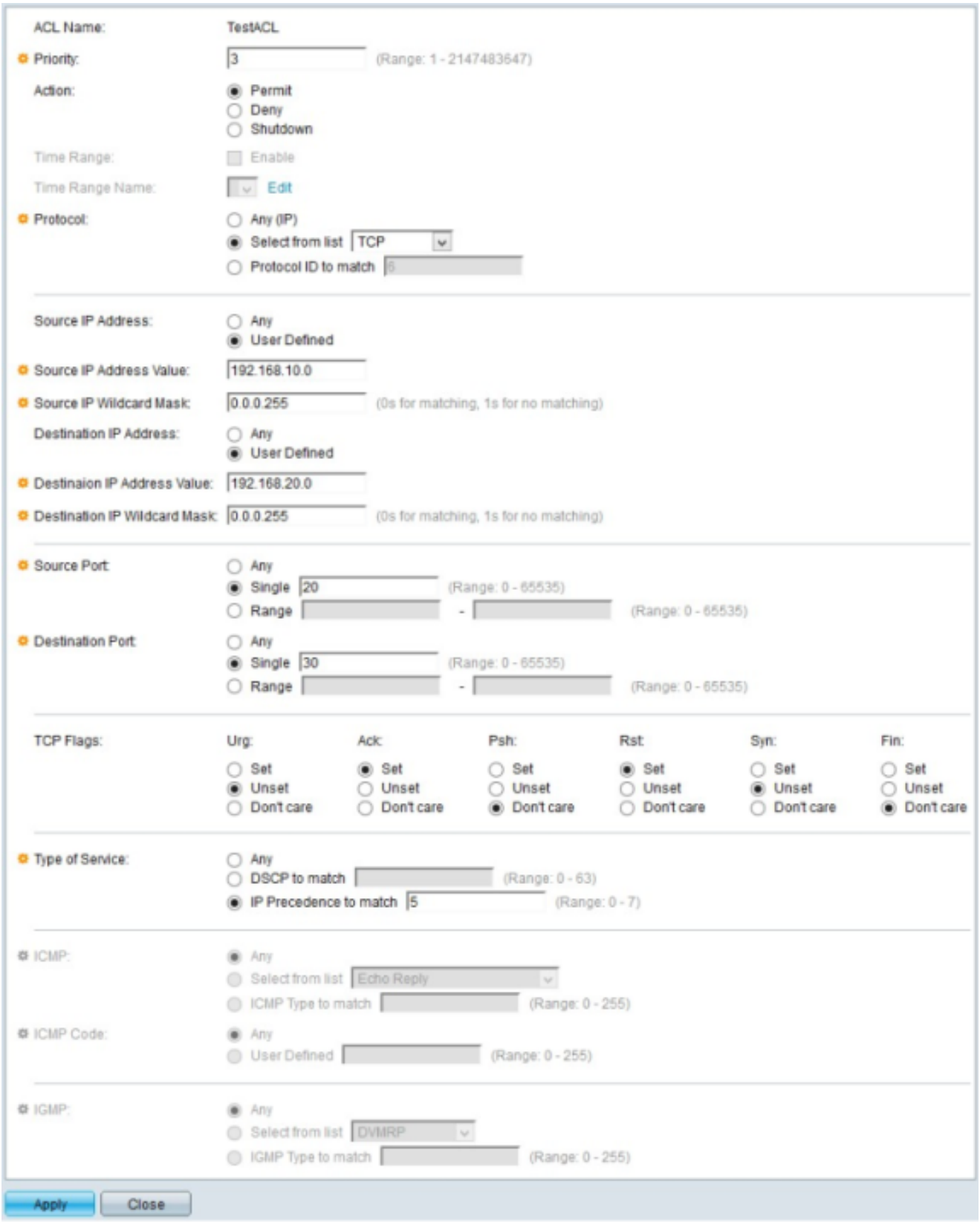
ACEs baseados em IPv4

Para gerenciar uma ACE para uma ACL, as próximas etapas precisam ser seguidas.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Controle de acesso > ACEs baseadas em IPv4**. A página *ACE baseado em IPv4* é aberta.

Etapa 2. Na lista suspensa *Filtro: Nome da ACL igual a*, escolha a lista de acesso à qual deseja atribuir uma regra de acesso.

Etapa 3. Clique em Add. A janela *Add IP-Based ACE* é exibida.



Etapa 4. Insira a prioridade da ACE no campo *Prioridade*. A entrada com a prioridade mais alta é processada primeiro. A prioridade mais alta é 1. Ele tem um intervalo de 1 a 2147483647.

Etapa 5. No campo *Ação*, clique no botão de opção da ação que você deseja que esta regra de acesso execute. As opções disponíveis são:

·Permit — Encaminha pacotes filtrados pela ACE atual.

·Negar — Descarta pacotes filtrados pela ACE atual.

·Shutdown — Descarta os pacotes filtrados pela ACE atual e desativa a porta de onde os pacotes foram recebidos.

Etapa 6. No campo *Protocol*, clique no botão de opção do protocolo que você deseja adicionar ao ACE. A ACE é configurada para todos os protocolos de rede roteados para filtrar os pacotes à medida que eles passam por um roteador. As opções disponíveis são:

· Any — Escolhe qualquer um dos protocolos ACE baseados em IPv4.

·Selecionar na lista — Escolha o protocolo desejado na lista suspensa.

·ID do protocolo a ser correspondido — Essa opção permite que você digite a ID do protocolo que deseja usar.

Passo 7. No campo *Endereço IP de origem*, clique em uma das opções disponíveis como endereço IP de origem:

·Any — Essa opção aplica a regra de acesso a qualquer um dos endereços IP disponíveis em um segmento de rede específico.

·Definido pelo usuário — Esta opção permite que você insira um endereço IP específico.

- Source IP Address Value — (Valor do endereço IP de origem) Nesse campo, insira o endereço IP de origem.

- Source IP Wildcard Mask (Máscara curinga do IP de origem) — Nesse campo, insira a máscara curinga do endereço IP de origem. A máscara curinga permite especificar a qual host do endereço IP de origem essa lista de acesso será aplicada.

Etapa 8. No campo *Endereço IP de destino*, clique em uma das opções disponíveis como endereço IP de destino:

·Any — Essa opção aplica a regra de acesso a qualquer um dos endereços IP disponíveis em um segmento de rede específico.

·Definido pelo usuário — Esta opção permite que você insira um endereço IP específico para aplicar a regra de acesso:

- Destination IP Address Value — (Valor do endereço IP de destino) Nesse campo, insira o endereço IP de destino.

- Destination IP Wildcard Mask (Máscara curinga do IP de destino) — nesse campo, insira a máscara curinga do endereço IP de destino. A máscara curinga permite especificar a quais hosts do endereço IP de destino essa lista de acesso será aplicada.

Etapa 9. O campo *Porta de origem* é ativado apenas quando você escolhe TCP ou UDP na Etapa 5. Clique no botão de opção de uma das opções disponíveis para escolher a porta de origem:

Any — Essa opção aceita qualquer porta de origem.

·Single — Essa opção permite que você insira um único valor de porta de origem.

·Range (Intervalo) — Essa opção permite que você insira um intervalo de portas de origem

disponíveis.

Etapa 10. O campo *Porta de destino* é ativado apenas quando você escolhe TCP ou UDP na Etapa 5. Clique no botão de opção de uma das opções disponíveis para escolher a porta de destino:

Any — Essa opção aceita qualquer porta de destino.

·Único — Essa opção permite inserir um único valor de porta de destino.

·Range (Intervalo) — Esta opção permite que você insira um intervalo de portas de destino disponíveis.

Etapa 11. Os *flags TCP* só serão ativados se você escolher TCP na Etapa 5. Clique em um dos botões de opção de cada flag para escolher qual estado você deseja disparar a regra de acesso:

·Urg — Esse flag identifica os dados recebidos como urgentes.

·Ack — Este flag é usado para confirmar o recebimento de pacotes com êxito.

·Psh — Esse flag é usado para garantir que os dados recebam a prioridade correta e sejam processados na extremidade de envio ou de recebimento.

·Rst — Esse flag é usado quando uma conexão recebe um segmento incorreto.

·Syn — Esse flag é usado para comunicações TCP.

·Fin — Este flag é usado quando a comunicação ou transferência de dados é concluída.

Etapa 12. No campo *Tipo de serviço*, clique em um dos botões de opção disponíveis para escolher um tipo de serviço para o pacote IP:

·Qualquer — Essa opção escolhe qualquer tipo de serviço.

·DSCP para correspondência — Escolha esta opção para implementar o Differentiated Service Code Point (DSCP) como um tipo de serviço. O DSCP é um mecanismo para classificar e gerenciar o tráfego de rede. Insira o valor de DSCP que deseja aplicar à regra de acesso.

·Precedência de IP a ser correspondida — esse tipo de serviço é usado pela rede atual para fornecer a QoS (Qualidade de Serviço) correta. Insira o valor que deseja aplicar à regra de acesso.

Etapa 13. O campo *ICMP (Internet Control Message Protocol)* é ativado somente quando você escolhe ICMP na Etapa 5. O ICMP é usado para enviar mensagens de erro quando um serviço não está disponível ou para testar a conectividade. Clique em um dos botões de opção disponíveis para filtrar os tipos de mensagem ICMP:

·Qualquer — Pode ser qualquer uma das mensagens de erro ou de consulta.

·Selecionar na lista — Escolha qualquer uma das mensagens de controle permitidas na lista suspensa.

·Tipo de ICMP a ser correspondido — Esta opção permite que você digite o número de tipos de ICMP que deseja filtrar.

Etapa 14. O campo *Código ICMP* é ativado somente quando você escolhe ICMP na Etapa 5. Os códigos ICMP são usados para fornecer informações mais específicas sobre as mensagens de controle. Clique em uma das opções disponíveis:

·Qualquer — Pode ser qualquer valor correspondente à mensagem de controle.

·Definido pelo usuário — Digite o código ICMP que deseja filtrar.

Etapa 15. O *campo IGMP (Internet Group Management Protocol)* é ativado apenas quando você escolhe IGMP na Etapa 5. O IGMP gerencia a participação de host em grupos multicast IP em um segmento de rede. Clique em um dos botões de opção disponíveis para filtrar os tipos de mensagem IGMP:

·Qualquer — Essa opção aceita todos os tipos de mensagem IGMP.

·Selecionar na lista — Escolha uma das opções disponíveis na lista suspensa para filtrar:

- DVMRP — Ele usa uma técnica de inundação de caminho reverso, que envia uma

cópia de um pacote recebido através de cada interface, exceto aquela em que o pacote chegou.

- Consulta de host — Envia periodicamente mensagens gerais de consulta de host em cada rede conectada para obter informações

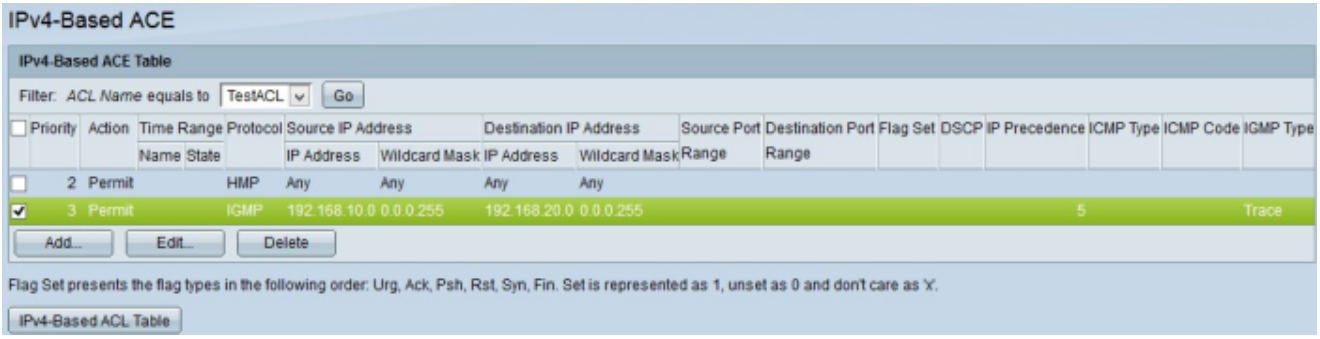
- Host-Reply — Ele responde à consulta .

- PIM — É usado entre os roteadores multicast local e remoto para direcionar o tráfego multicast do servidor multicast para muitos clientes multicast.

- Trace — Fornece informações para ingressar e sair de um grupo multicast IGMP.

·Tipo de IGMP de correspondência — Esta opção permite que você digite o número de tipos de IGMP que deseja filtrar.

Etapa 16. Clique em **Apply** para salvar sua configuração.



Etapa 17. (Opcional) Para editar uma regra de acesso atual, marque a caixa de seleção da regra de acesso que deseja editar e clique em **Editar**.

Etapa 18. (Opcional) Para excluir uma regra de acesso atual, marque a caixa de seleção da regra de acesso que deseja excluir e clique em **Excluir**.

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.