Práticas recomendadas de ACL em um roteador RV34x Series

Objetivo

O objetivo deste artigo é descrever as melhores práticas para criar listas de controle de acesso (ACLs) com seu roteador RV34x Series.

Dispositivos aplicáveis | Versão do firmware

- RV340 | 1.0.03.20 (baixe o mais recente)
- RV340W | 1.0.03.20 (baixe o mais recente)
- RV345 | 1.0.03.20 (baixe o mais recente)
- RV345P | 1.0.03.20 (baixe o mais recente)

Introduction

Você quer mais controle sobre a sua rede? Deseja tomar medidas adicionais para manter sua rede segura? Em caso afirmativo, uma ACL (Access Control List, lista de controle de acesso) pode ser exatamente o que você precisa.

Uma ACL consiste em uma ou mais entradas de controle de acesso (ACEs) que definem coletivamente o perfil de tráfego de rede. Esse perfil pode ser referenciado por recursos do software da Cisco, como filtragem de tráfego, prioridade ou enfileiramento personalizado. Cada ACL inclui um elemento de ação (permitir ou negar) e um elemento de filtro com base em critérios como endereço de origem, endereço de destino, protocolo e parâmetros específicos do protocolo.

Com base nos critérios que você inseriu, você pode controlar o tráfego de entrada e/ou saída de uma rede. Quando um roteador recebe um pacote, ele examina o pacote para determinar se deve encaminhar ou descartar o pacote com base na sua lista de acesso.

A implementação desse nível de segurança é baseada em casos de uso diferentes, considerando cenários de rede específicos e necessidades de segurança.

Éimportante observar que o roteador pode criar automaticamente uma lista de acesso com base nas configurações do roteador. Nesse caso, você pode ver listas de acesso que não podem ser apagadas a menos que altere as configurações do roteador.

Por que usar listas de acesso

- Na maioria dos casos, usamos ACLs para fornecer um nível básico de segurança para acessar nossa rede. Por exemplo, se você não configurar ACLs, por padrão, todos os pacotes que passam pelo roteador poderão ser permitidos para todas as partes da

nossa rede.
- As ACLs podem permitir um host, um intervalo de endereços IP ou redes e impedir que outro host, um intervalo de endereços IP ou redes acessem a mesma área (host ou rede).
- Usando ACLs, você pode decidir que tipos de tráfego encaminhou ou bloqueou nas interfaces do roteador. Por exemplo, você pode permitir o tráfego do protocolo de transferência de arquivos (SFTP - File Transfer Protocol) do Shell Seguro (SSH - Secure Shell) e, ao mesmo tempo, bloquear todo o tráfego do protocolo de inicialização da sessão (SIP - Session Initiation Protocol).

Quando usar as listas de acesso

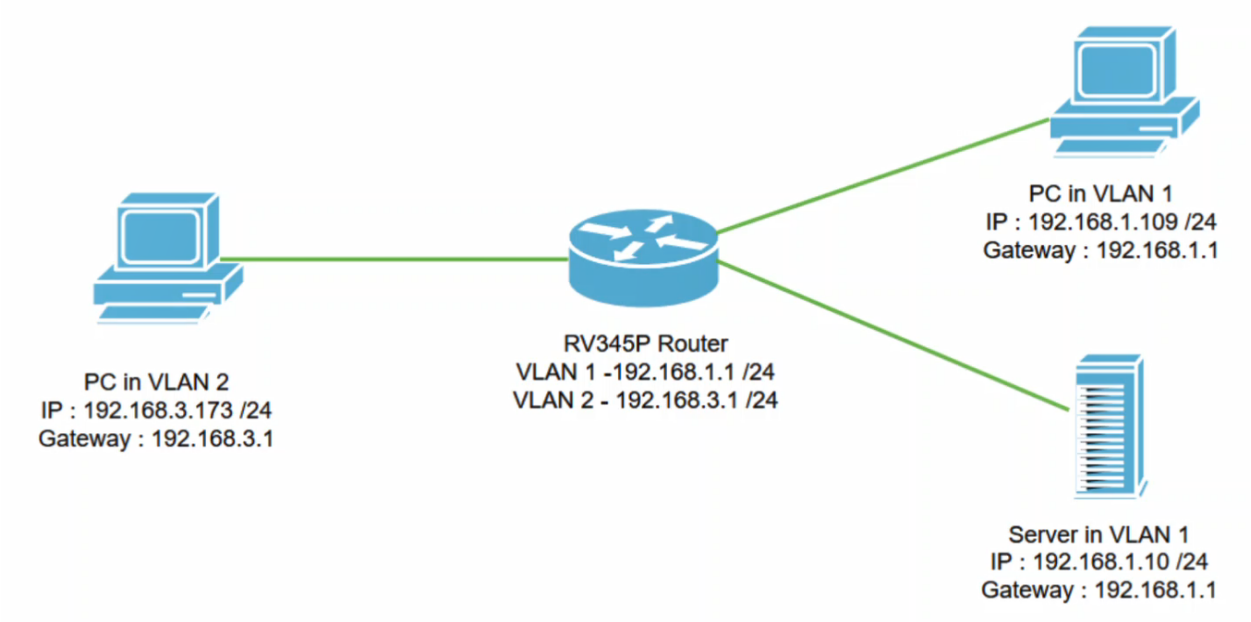
- Você deve configurar ACLs em roteadores posicionados entre nossa rede interna e uma rede externa como a Internet.
- Você pode usar ACLs para controlar o tráfego que entra ou sai de uma parte específica de nossa rede interna.
- Quando você precisar filtrar o tráfego de entrada ou de saída ou ambos em uma interface.
- Você deve definir ACLs por protocolo para controlar o tráfego.

Práticas recomendadas para configurar a segurança básica com listas de acesso

- Implemente ACLs que permitam apenas os protocolos, portas e endereços IP que negam tudo o mais.
- Bloquear pacotes de entrada que afirmam ter o mesmo destino e endereço de origem (ataque terrestre no próprio roteador).
- Ative o recurso de registro em ACLs para um host Syslog interno (confiável).
- Se você usa o SNMP (Simple Network Management Protocol) no roteador, então você precisa configurar a ACL SNMP e a string de comunidade SNMP complexa.
- Permitir que somente endereços internos entrem no roteador a partir das interfaces internas e permitir que somente o tráfego destinado a endereços internos entre no roteador a partir do exterior (interfaces externas).
- Bloquear multicast se não for usado.
- Bloquear alguns tipos de mensagem do Internet Control Message Protocol (ICMP) (redirecionar, eco).
- Sempre considere a ordem na qual você insere as ACLs. Por exemplo, quando o roteador está decidindo se encaminha ou bloqueia um pacote, ele testa o pacote em relação a cada instrução da ACL na ordem em que as ACLs foram criadas.

Implementação da lista de acesso nos roteadores Cisco série RV34x

Exemplo de topologia de rede



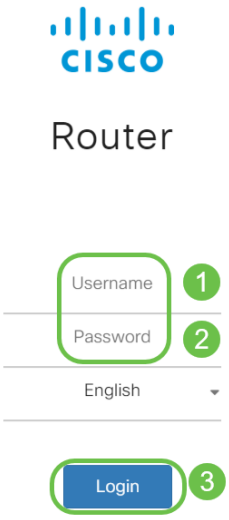
Cenário de exemplo

Neste cenário, replicaremos este diagrama de rede, onde temos um roteador RV345P e duas interfaces VLAN diferentes. Temos um PC na VLAN 1 e na VLAN 2, e também temos um servidor na VLAN 1. O roteamento entre VLANs está ativado, de modo que os usuários da VLAN 1 e da VLAN 2 podem se comunicar entre si. Agora, vamos aplicar a regra de acesso para restringir a comunicação entre o usuário da VLAN 2 em direção a esse servidor na VLAN 1.

Exemplo de configuração

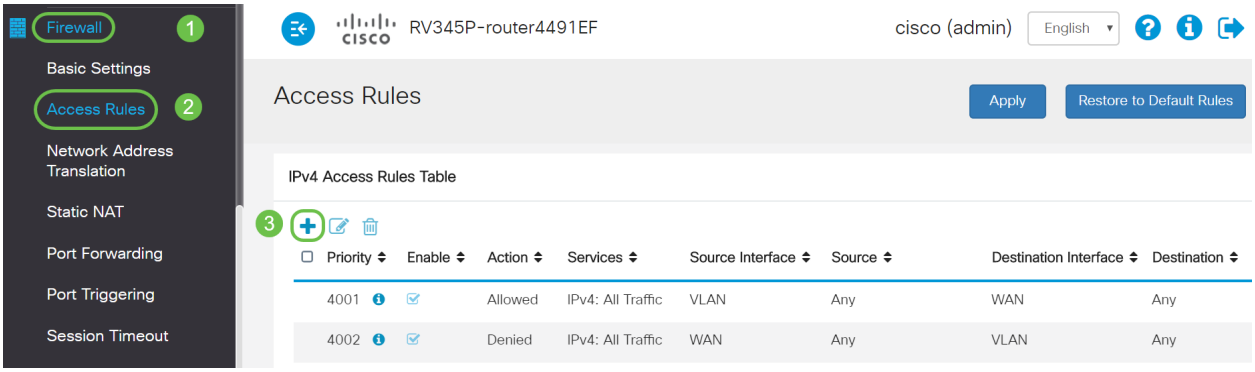
Passo 1

Faça login na Interface de usuário da Web (UI) do roteador usando as credenciais configuradas.



Passo 2

Para configurar a ACL, navegue até **Firewall > Access Rules** e clique no **ícone de mais** para adicionar uma nova regra.



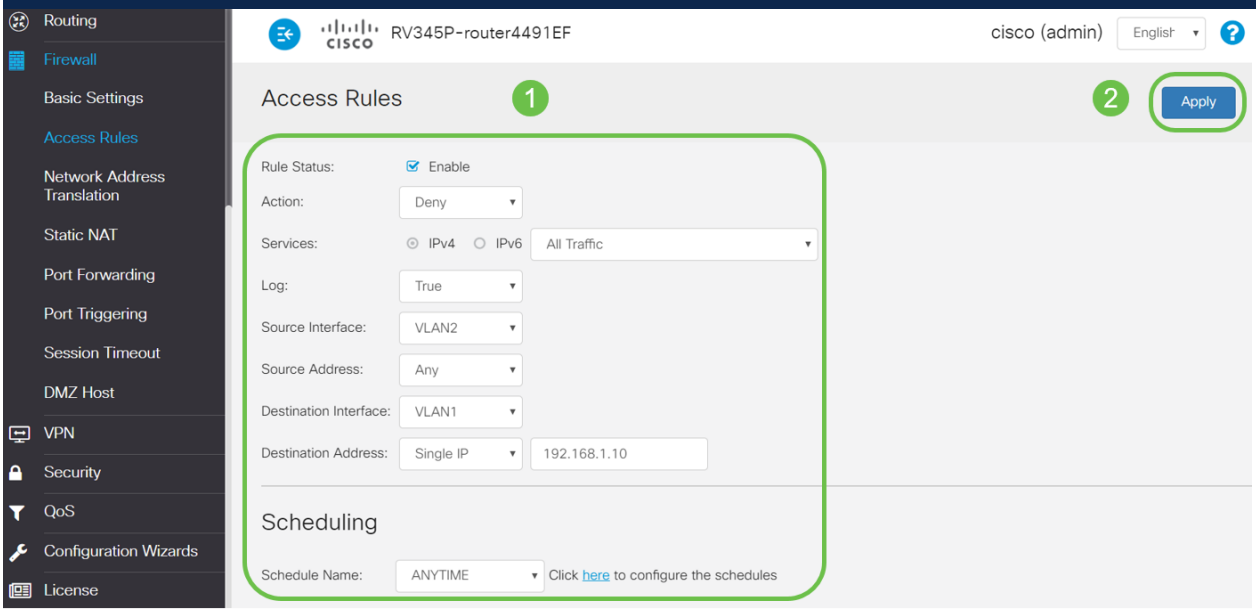
Etapa 3

Configure os parâmetros *das regras de acesso*. Aplicar ACL para restringir o servidor (IPv4: 192.168.1.10/24) dos usuários da VLAN2. 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*

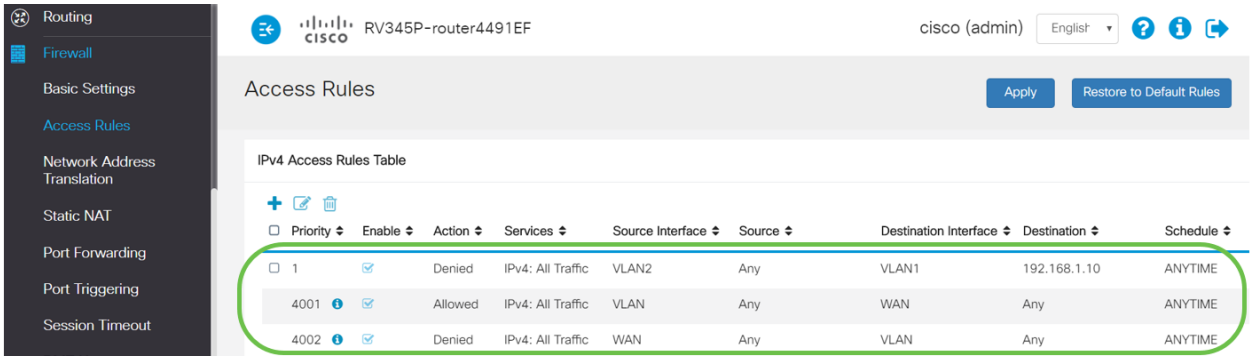
Clique em Apply.

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



Passo 4

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



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.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

Conclusão

Você viu as etapas necessárias para configurar a regra de acesso em um roteador Cisco RV34x Series. Agora você pode aplicá-la para criar uma regra de acesso na sua rede que atenda às suas necessidades!