Identificar e Solucionar Problemas de Listas de Acesso sobre Rede Virtual Privada em RV016, RV042, RV042G e RV082 VPN Routers

Objetivos

Uma ACL (Access Control List, lista de controle de acesso) é uma coleção de condições de permissão e negação. Uma ACL especifica quais processos do sistema ou usuário recebem acesso a recursos específicos. Uma ACL pode bloquear qualquer tentativa injustificada de acessar recursos de rede. O problema nessa situação pode surgir quando você tem ACLs configuradas em ambos os roteadores, mas um dos roteadores não pode diferenciar entre as listas de tráfego permitidas e negadas permitidas pela ACL. O Zenmap, que é uma ferramenta de código aberto usada para verificar o tipo de filtros de pacote/firewalls ativos, é usado para testar a configuração.

Este artigo explica como solucionar problemas de ACLs permitidas que não funcionam sobre VPN de gateway para gateway entre dois roteadores VPN.

Dispositivos aplicáveis

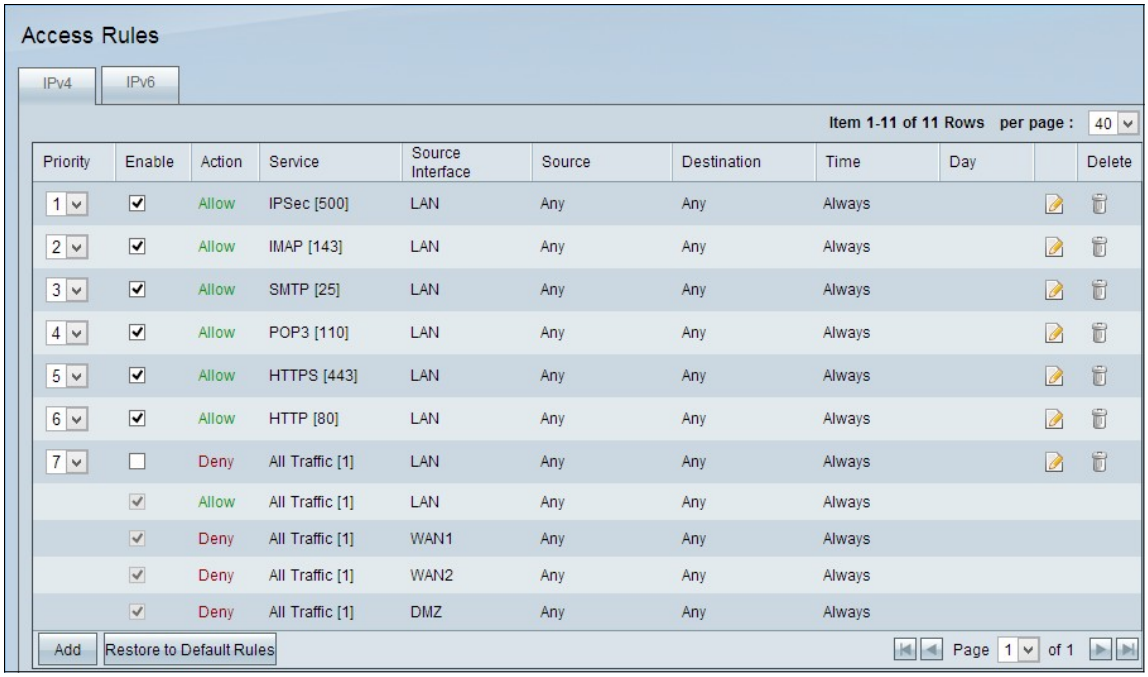
- RV016
- RV042
- RV042G
- RV082

Versão de software

- v4.2.2.08

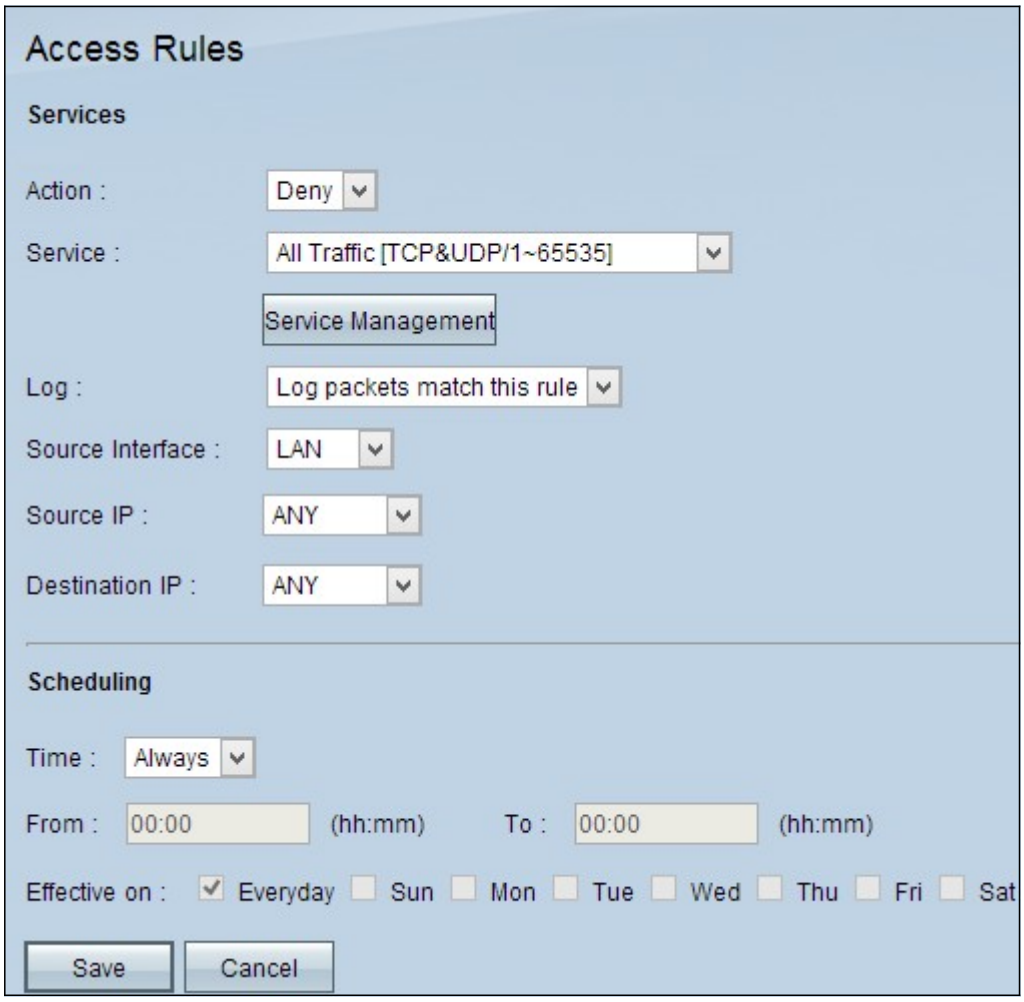
ACL sobre configuração de VPN

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

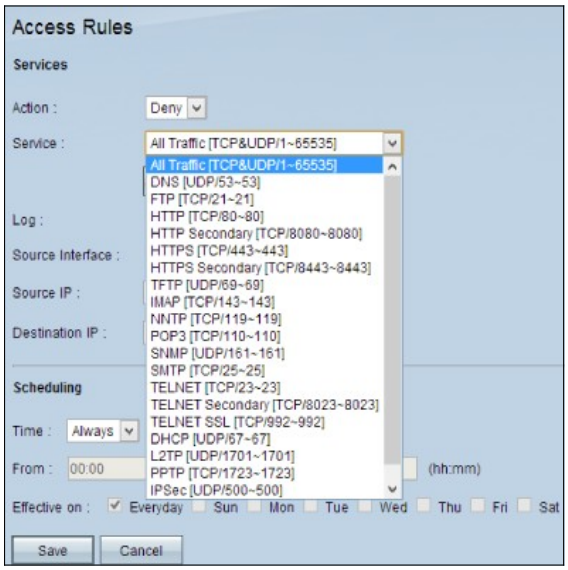


Note: As regras de acesso padrão não podem ser editadas. As regras de acesso mencionadas na imagem acima, que são configuradas pelo usuário, podem ser editadas pelo seguinte processo.

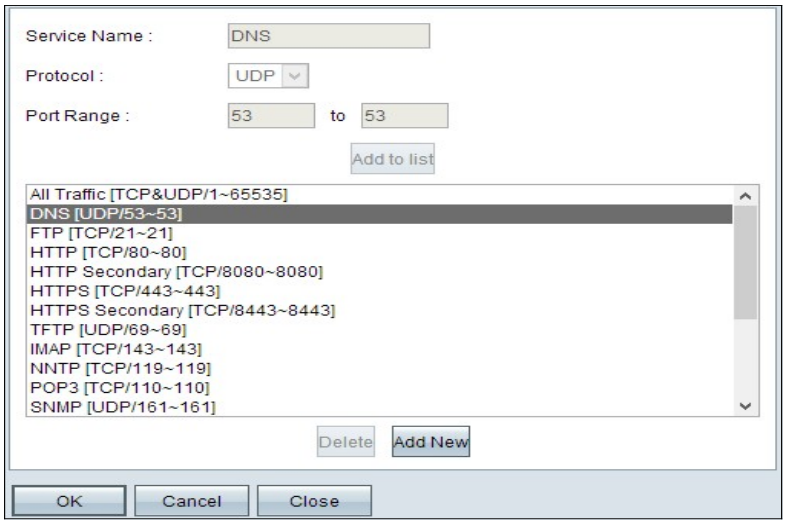
Etapa 2. Clique no botão **Adicionar** para adicionar uma nova regra de acesso. A página *Regras de acesso* é alterada para mostrar as áreas Serviços e Agendamento. A adição de uma regra de acesso é explicada nas etapas a seguir.



Etapa 3. Escolha **Negar** na lista suspensa Ação para negar o serviço.



Etapa 4. Escolha o serviço necessário que é aplicado à regra na lista suspensa **Serviço**.



Etapa 5. (Opcional) Para adicionar um serviço que não está presente na lista suspensa de serviços, clique em **Gerenciamento de serviços**. No Gerenciamento de serviços, um serviço pode ser criado conforme necessário. Depois que um serviço for criado, clique em **OK** para salvar as configurações.

Etapa 6. Escolha **Pacotes de log que correspondam a essa regra** na lista suspensa Log somente para logs que correspondam ou **Não registram** para logs que não correspondem à regra de acesso.

Passo 7. Escolha um tipo de interface na lista suspensa Interface de origem que é a origem das regras de acesso. As opções disponíveis são:

LAN — Escolha LAN se a interface de origem for a Rede de área local.

WAN — Escolha WAN se a interface de origem for o ISP.

DMZ — escolha DMZ se a interface de origem for a zona desmilitarizada.

ANY — Escolha ANY para fazer a interface de origem como qualquer uma das interfaces mencionadas acima.

Etapa 8. Na lista suspensa IP de origem, escolha os endereços de origem desejados que se aplicam à regra de acesso. As opções disponíveis são:

Single - Escolha Single se for um único endereço IP e insira o endereço IP.

Intervalo — Escolha Intervalo se for um intervalo de endereços IP e insira o primeiro e o último endereço IP no intervalo.

ANY — Escolha ANY para aplicar as regras a todos os endereços IP de origem.

Etapa 9. Na lista suspensa IP de destino, escolha os endereços de destino desejados que se aplicam à regra de acesso. As opções disponíveis são:

Single - Escolha Single se for um único endereço IP e insira o endereço IP.

Intervalo — Escolha Intervalo se for um intervalo de endereços IP e insira o primeiro e o último endereço IP no intervalo.

ANY — Escolha ANY para aplicar as regras a todos os endereços IP de destino.

Etapa 10. Escolha um método para definir quando as regras estão ativas na lista suspensa Hora. São elas:

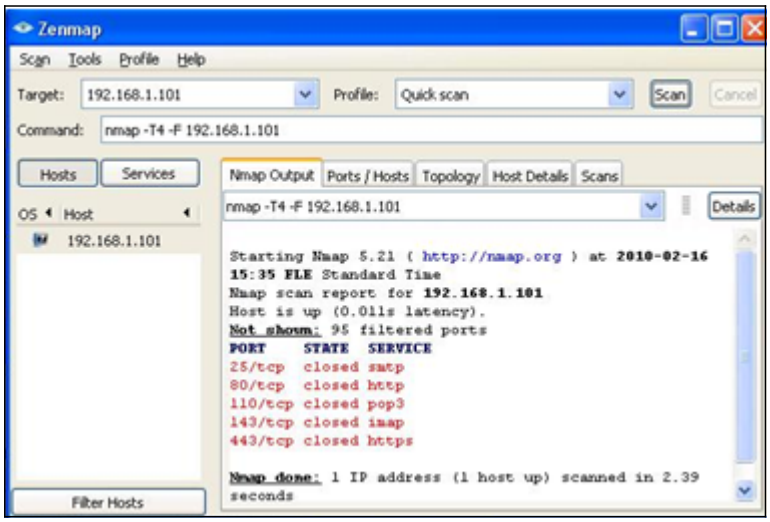
Sempre — Se você escolher Sempre na lista suspensa Hora, as regras de acesso sempre serão aplicadas ao tráfego.

· Intervalo — Você pode escolher um intervalo de tempo específico no qual as regras de acesso estão ativas se selecionar Intervalo na lista suspensa Hora. Depois de especificar o intervalo de tempo, marque as caixas de seleção dos dias em que deseja que as regras de acesso estejam ativas no campo Efetivo ativado.

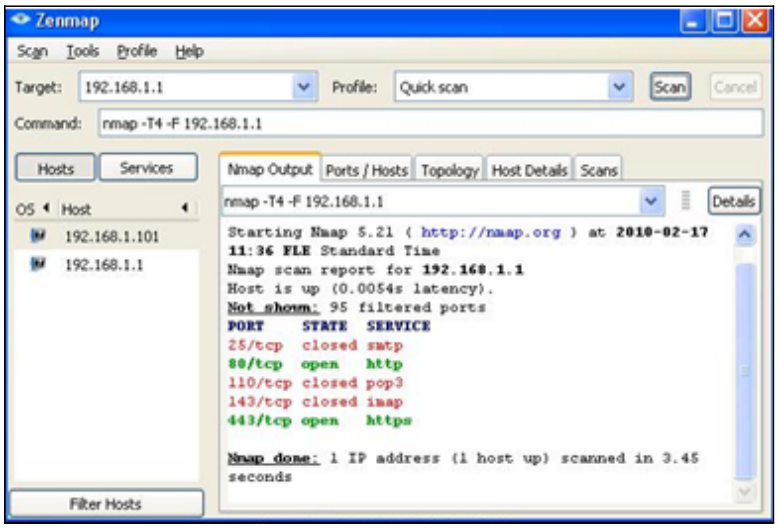
Etapa 11. Clique em **Salvar** para salvar suas configurações.

Etapa 12. Repita as etapas 2 a 10 com os campos correspondentes aos mostrados na imagem respectivamente. As regras de acesso de acordo com o cliente são aplicadas aqui. Os 7 primeiros estão permitindo alguns serviços; o 8 nega todo o tráfego restante. Essa configuração é feita no segundo roteador também. A porta IPSec 500 é permitida.

Note: Faça isso para que os dois roteadores verifiquem se as regras de acesso estão configuradas conforme desejado.



Roteador VPN nº 1

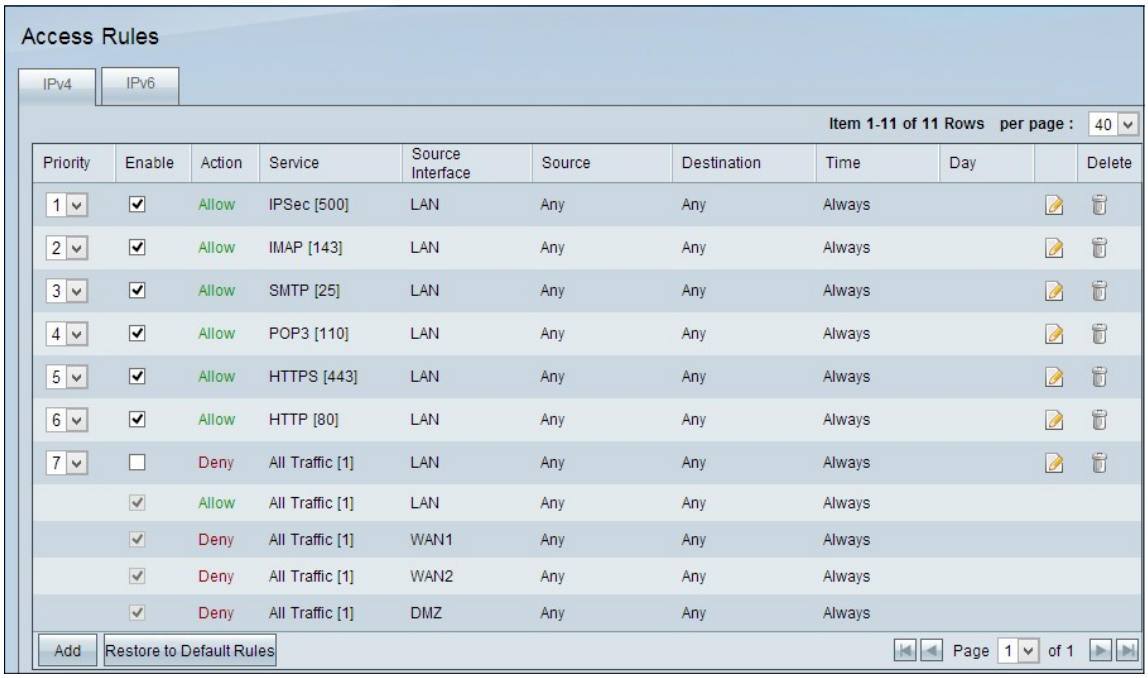


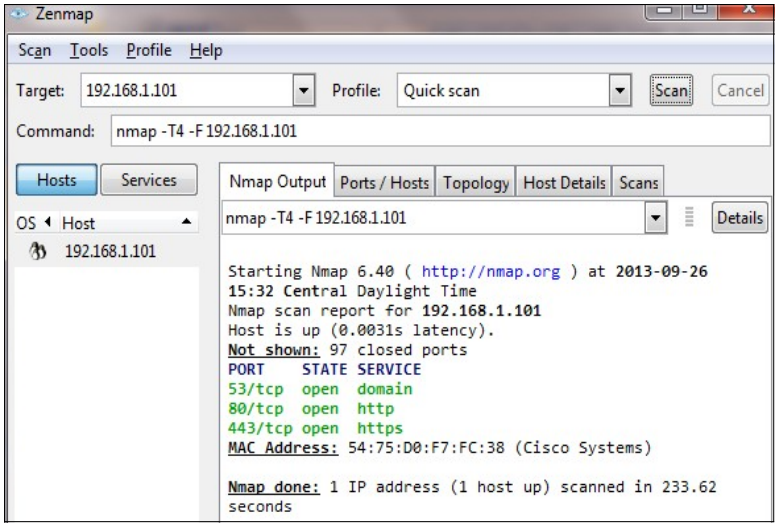
Roteador VPN nº 2

Etapa 13. Instale o Zenmap(NMAP) de http://nmap.org/download.html e inicie-o em um PC na LAN 192.168.2.0.

Note: Essa é a LAN atrás do roteador com as sete ACLs adicionais. O IP de destino (192.168.1.101) é um PC na LAN do Gateway Remoto.

Etapa 14. Selecione **Quick Scan (Verificação rápida)** no perfil e clique em **Scan (Verificar)**. Com isso, podemos saber que as portas são abertas e filtradas de acordo com as ACLs, o resultado mostrado é representado na imagem acima. A saída mostra que essas portas estão fechadas, independentemente das ACLs permitidas serem configuradas no RV0xx # 1. Se tentarmos verificar as portas para o IP da LAN (192.168.1.1) do gateway remoto - descobrimos que as portas 80 e 443 estão abertas (que foram fechadas ao PC 192.168.1.101).





A ACL funciona corretamente após a remoção da 7ª ACL negada e funciona bem como podemos ver na saída.

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.