Cisco | Networking Academy®
Mind Wide Open™

Laboratório 5.5.1: Listas de controle de acesso básico

Diagrama de topologia

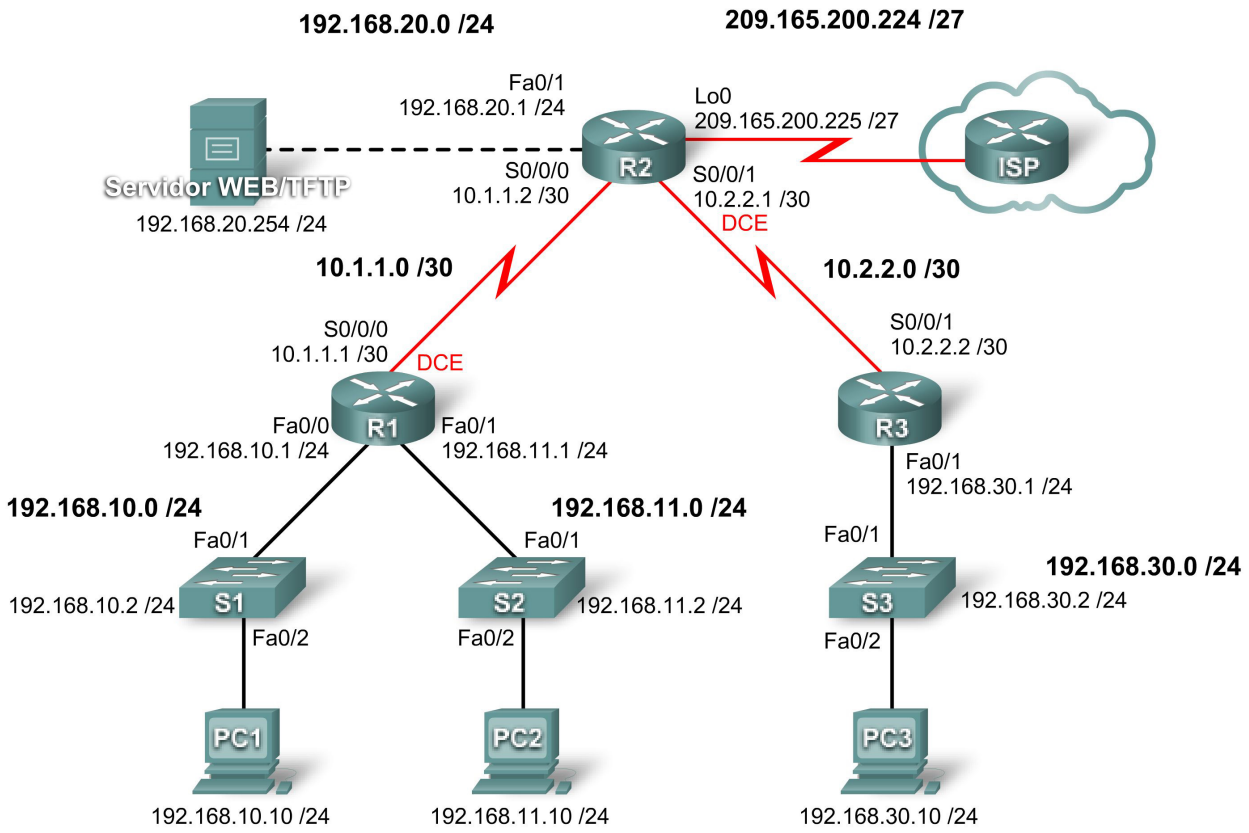

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1

S2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**Placa de rede**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**Placa de rede**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Placa de rede**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	**Placa de rede**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Crie o padrão nomeado e as ACLs estendidas nomeadas.
- Aplique o padrão nomeado e as ACLs estendidas nomeadas.
- Testar as ACLs de nomenclatura padrão e estendida.
- Solucionar problemas das ACLs de nomenclatura padrão e estendida.

Cenário

Neste laboratório, você irá aprender a configurar a segurança de rede básica utilizando listas de controle de acesso. Você irá aplicar ACLs padrão e estendidas.

Tarefa 1: Preparar a rede

Etapa 1: Cabear uma rede de maneira semelhante à presente no diagrama de topologia.

Você pode utilizar qualquer roteador atual em seu laboratório contanto que ele tenha as interfaces exigidas mostradas no diagrama de topologia.

Nota: este laboratório foi desenvolvido e testado utilizando-se 1.841 roteadores. Se você usar roteadores da série 1700, 2500 ou 2600, as saídas do roteador e as descrições de interface poderão ser diferentes. Em roteadores mais antigos, ou versões do IOS anteriores ao 12.4, alguns comandos podem ser diferentes ou inexistentes.

Etapa 2: Apagar todas as configurações existentes nos roteadores.

Etapa 2: Executar configurações básicas do roteador

Configure os roteadores R1, R2, R3, S1, S2 e S3 e os switches de acordo com as seguintes diretrizes:

- Configure o nome de host do roteador de acordo com o diagrama de topologia.
- Desabilite a pesquisa DNS.
- Configure uma senha **class** no modo EXEC.
- Configure um banner de mensagem do dia.
- Configure uma senha cisco para as conexões de console.
- Configure uma senha para as conexões VTY.
- Configure endereços IP e máscaras em todos os dispositivos.
- Habilite o OSPF área 0 com um ID de processo 1 em todos os roteadores de todas as redes.

- Configure uma interface de loopback em R2 para simular o ISP.
- Configure endereços IP para a interface VLAN 1 em cada switch.
- Configure cada switch usando o gateway padrão apropriado.
- Verificar a conectividade completa do IP usando o comando **ping**.

Tarefa 3: Configurando uma ACL padrão

As ACLs padrão só podem filtrar tráfego com base no endereço IP de origem. Uma prática recomendada típica é configurar uma ACL padrão o mais próximo possível do destino. Nesta tarefa, você está configurando uma ACL padrão. A ACL foi projetada para impedir o tráfego da rede 192.168.11.0/24 localizada em um laboratório de aluno de acessar uma rede local em R3.

Esta ACL será aplicada à interface serial do R3. Lembre-se de que toda ACL tem um “deny all” implícito que faz com que todo o tráfego não correspondente a uma instrução na ACL seja bloqueado. Por isso, adicione a instrução **permit any** ao final da ACL.

Antes de configurar e aplicar essa ACL, não se esqueça de testar a conectividade de PC1 (ou a interface Fa0/1 em R1) para PC3 (ou a interface Fa0/1 em R3). Os testes de conectividade devem ser bem-sucedidos antes da aplicação da ACL.

Etapa 1: Criar a ACL no roteador R3.

No modo de configuração global, crie uma ACL nomeada padrão chamada **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

No modo de configuração ACL padrão, adicione uma instrução que nega qualquer pacote com um endereço de origem 192.168.11.0/24 e imprime uma mensagem na console de cada pacote correspondido.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permita todos os demais tráfegos.

```
R3(config-std-nacl)#permit any
```

Etapa 2: Aplicar a ACL.

Aplique a ACL **STND-1** como um filtro em pacotes que entram em R3 pela interface serial 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Etapa 3: Testar a ACL.

Antes de testar a ACL, verifique se a console de R3 é visível. Isso permitirá ver as mensagens do log da lista de acesso quando o pacote for negado.

Testar a ACL executando ping do PC2 para o PC3. Considerando que a ACL foi projetada para bloquear tráfego com endereços de origem da rede 192.168.11.0/24, PC2 (192.168.11.10) não deve ser capaz de executar ping em PC3.

Você também pode utilizar um ping estendido da interface Fa0/1 em R1 para a interface Fa0/1 em R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
```



```
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

Você deve ver a mensagem a seguir na console de R3:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

No modo EXEC privilegiado em R3, emita o comando **show access-lists**. Você vê a saída de dados semelhante ao seguinte. Cada linha de uma ACL tem um contador associado que mostra quantos pacotes corresponderam à regra.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

A finalidade desta ACL foi bloquear hosts da rede 192.168.11.0/24. Qualquer outro host, como os na rede 192.168.10.0/24, deve ter permissão para acessar as redes em R3. Faça outros testes entre PC1 e PC3 para assegurar que esse tráfego não esteja bloqueado.

Você também pode utilizar um ping estendido da interface Fa0/0 em R1 para a interface Fa0/1 em R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Tarefa 4: Configurando uma ACL estendida

Quando for exigida uma maior granularidade, você deve utilizar uma ACL estendida. As ACLs estendidas podem filtrar o tráfego com base em mais de um endereço de origem. As ACLs estendidas podem filtrar o protocolo, os endereços IP de origem e de destino, além dos números de porta de origem e de destino.

Uma política adicional desta rede informa que apenas dispositivos da LAN 192.168.10.0/24 têm permissão para alcançar redes internas. Os computadores nesta LAN não podem acessar a Internet. Portanto, o acesso desses usuários ao endereço IP 209.165.200.225 deve ser bloqueado. Como este requisito precisa ser aplicado na origem e no destino, uma ACL estendida é obrigatória.

Nesta tarefa, você está configurando uma ACL estendida em R1 que impede tráfego com origem em qualquer dispositivo na rede 192.168.10.0/24 de acessar o host 209.165.200.255 (o ISP simulado). Esta ACL será aplicada à saída da interface serial 0/0/0 do R1. Uma prática recomendada típica para aplicar ACLs estendidas é colocá-las o mais próximo possível da origem.

Antes de começar, verifique se você consegue executar ping em 209.165.200.225 no PC1.

Etapa 1: Configurar uma ACL estendida nomeada.

No modo de configuração global, crie uma ACL estendida padrão chamada **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Observe que o prompt do roteador é alterado para indicar que agora você está no modo de configuração ACL estendido. Nesse prompt, adicione as instruções necessárias para bloquear o tráfego da rede 192.168.10.0/24 para o host. Use a palavra-chave **host** ao definir o destino.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Lembre-se de que "deny all" implícito bloqueia todos os demais tráfegos sem a instrução **permit** adicional. Adicione a instrução **permit** para garantir que outro tráfego não esteja bloqueado.

```
R1(config-ext-nacl)#permit ip any any
```

Etapa 2: Aplicar a ACL.

Com ACLs padrão, a prática recomendada é colocar a ACL o mais perto possível do destino. As ACLs estendidas costumam ser colocadas próximas da origem. A ACL **EXTEND-1** será colocada na interface Serial e filtrará o tráfego de saída.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out
R1(config-if)#end
R1#copy run start
```

Etapa 3: Testar a ACL.

Em PC1, execute ping na interface de loopback em R2. Esses pings devem falhar, pois todo o tráfego da rede 192.168.10.0/24 será filtrado quando o destino for 209.165.200.225. Se o destino for qualquer outro endereço, os pings devem ter êxito. Confirme-a, executando ping em R3 a partir do dispositivo de rede 192.168.10.0/24.

Nota: o recurso de ping estendido em R1 não pode ser utilizado para testar essa ACL, porque o tráfego terá origem dentro de R1 e jamais será testado em relação à ACL aplicada à interface serial R1.

Você pode ainda verificar isto emitindo o comando **show ip access-list** em R1 depois de executar ping.

```
R1#show ip access-list
Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Tarefa 5: Controlar acesso às linhas VTY com uma ACL padrão

É uma prática recomendada restringir o acesso a linhas VTY do roteador à administração remota. Uma ACL pode ser se aplicada às linhas VTY, o que permite restringir acesso a hosts específicos ou redes.

Nesta tarefa, você irá configurar uma ACL padrão para permitir que hosts de duas redes acessem as linhas VTY. Todos os demais hosts são negados.

Verifique se você pode enviar um telnet ao R2 do R1 e do R3.

Etapa 1: Configurar os ACL.

Configure uma ACL padrão nomeada em R2 que permita tráfego entre 10.2.2.0/30 e 192.168.30.0/24. Negue todos os demais tráfegos. Chame a ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Etapa 2: Aplicar a ACL.

Entre no modo de configuração das linhas VTY de 0 a 4.

```
R2(config)#line vty 0 4
```

Use o comando **access-class** para aplicar a ACL às linhas vty na direção de entrada. Observe que ele é diferente do comando que costumava aplicar ACLs a outras interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Etapa 3: Testar a ACL

Telnet de R1 para R2. Observe que R1 não tem endereços IP no intervalo de endereços listado nas instruções de permissão ACL TASK-5. Deve haver falha nas tentativas de conexão.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 …
% Connection refused by remote host
```

Em R3, execute telnet em R2. Será apresentado a você um prompt para a senha de linha VTY.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 … Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

Por que as tentativas de conexão de outras redes falham mesmo não estando especificamente listadas na ACL?

_____

_____

Tarefa 6: Identificação e solução de problemas de ACLs

Quando uma ACL é configurada ou aplicada de modo inadequado para a interface errada ou na direção errada, o tráfego da rede pode ser afetado de uma maneira indesejável.

Etapa 1: Remover ACL STND-1 de S0/0/1 de R3.

Em uma tarefa anterior, você criou e aplicou uma ACL padrão nomeada em R3. Use o comando **show running-config** para exibir a ACL e sua localização. Você deve ver que uma ACL chamada **STND-1** foi configurada e aplicada de entrada na Serial 0/0/1. Lembre-se de que essa ACL foi criada para impedir todo o tráfego da rede com um endereço de origem da rede 192.168.11.0/24 de acessar a rede local em R3.

Para remover a ACL, vá para o modo de configuração da interface serial 0/0/1 no R3. Utilize o comando **no ip access-group STND-1 in** para remover a ACL da interface.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Utilize o comando **show running-config** para confirmar se a ACL foi removida da Serial 0/0/1.

Etapa 2: Aplicar ACL STND-1 em S0/0/1 de saída.

Para testar a importância do sentido da filtragem ACL, reaplique a ACL **STND-1** à interface Serial 0/0/1. Desta vez, a ACL filtrará o tráfego de saída em vez do tráfego de entrada. Lembre-se de usar a palavra-chave **out** ao aplicar a ACL.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out
```

Etapa 3: Testar a ACL.

Testar a ACL executando ping do PC2 para o PC3. Como alternativa, use um ping estendido em R1. Observe que ping é executado com êxito desta vez e os contadores ACL não são incrementados. Confirme-a, emitindo o comando **show ip access-list** em R3.

Etapa 4: Restaurar a configuração original da ACL.

Remova a ACL da direção de saída e reaplique-a na direção de entrada.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Etapa 5: Aplicar TASK-5 à interface R2 serial 0/0/0 de entrada.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Etapa 6: Testar a ACL.

Tente se comunicar com qualquer dispositivo conectado a R2 ou R3 de R1 ou redes conectadas. Observe que toda a comunicação é bloqueada; no entanto, os contadores ACL não são incrementados. Isso ocorre por causa do "negar tudo" implícito no final de cada ACL. Essa instrução deny impedirá todo o tráfego de entrada para serial 0/0/0 de qualquer origem que não seja R3. Essencialmente, isso causará a remoção de R1 da tabela de roteamento.

Você deve ver mensagens semelhantes às impressas a seguir nas consoles de R1 e R2 (como demorará um pouco para que o relacionamento de vizinho OSPF seja desativado, tenha paciência):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Quando você receber essa mensagem, emita o comando **show ip route** em R1 e R2 para ver quais rotas foram removidas da tabela de roteamento.

Remova a ACL TASK-5 da interface e salve as configurações.

```
R2(config)#interface serial 0/0/0
```



```
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```

Tarefa 7: Documentar as configurações do roteador

Configurações

Roteador 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
 deny   ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Roteador 2


```
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Roteador 3

```
hostname R3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
```



```
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 in
 no shutdown
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny   192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Tarefa 8: Limpar

Apague as configurações e recarregue os roteadores. Desconecte e guarde o cabeamento. Para PCs normalmente conectados a outras redes, como a LAN escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.

