Laboratório 4.6.2: Configuração avançada de segurança

Diagrama de topologia

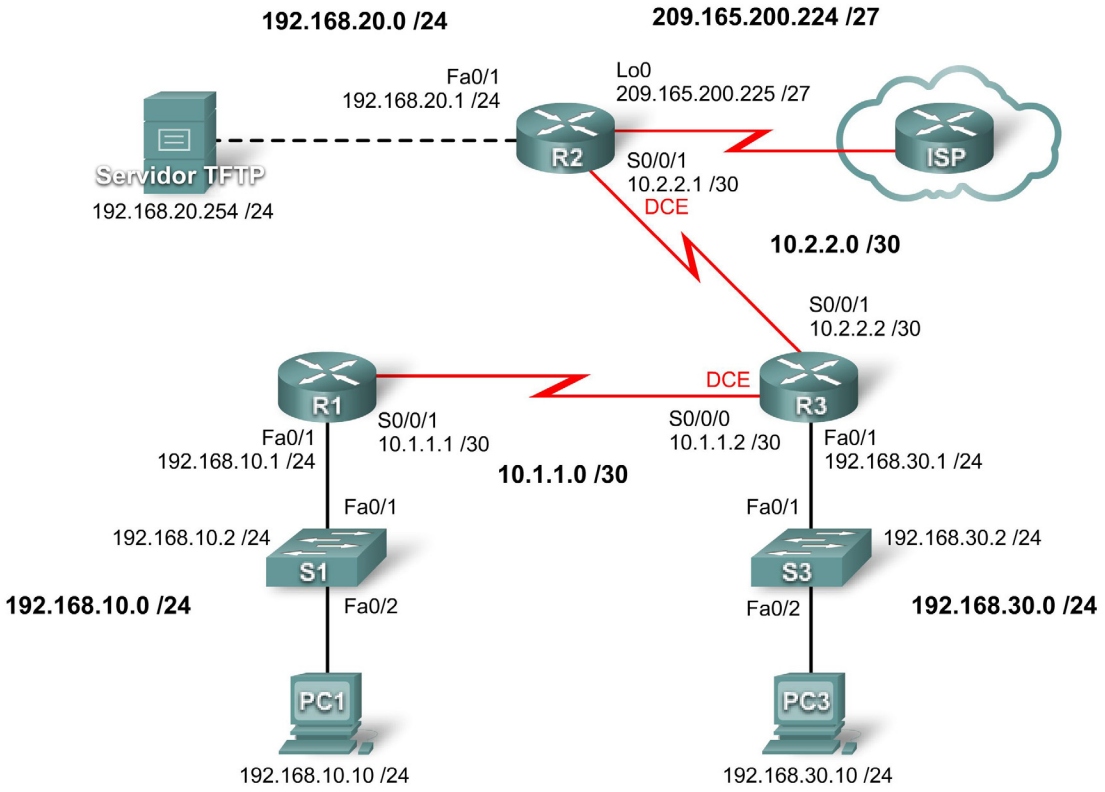

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/1	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
	S0/0/0	10.1.1.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	Placa de rede	192.168.10.10	255.255.255.0	192.168.10.1
PC3	Placa de rede	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	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:

- Cabo de rede de acordo com o diagrama de topologia.
- Apagar a configuração de inicialização e recarregar o roteador no estado padrão.
- Executar tarefas de configuração básica em um roteador.
- Configurar e ativar interfaces.
- Configurar a segurança básica do roteador.
- Desabilitar os serviços e as interfaces Cisco não usados.
- Proteja redes de empresa de ataques externos e internos básicos.
- Entender e gerenciar os arquivos de configuração do Cisco IOS e o sistema de arquivos da Cisco.
- Configurar e utilizar o Cisco SDM (Security Device Manager) para configurar a segurança básica do roteador.

Cenário

Neste laboratório, você irá configurar a segurança usando a rede mostrada no diagrama de topologia. Se você precisar de assistência, consulte o laboratório de segurança básico. No entanto, tente fazer o máximo possível. Para este laboratório, não use a proteção por senha ou login em nenhuma linha de console porque isso pode causar o logout acidental. No entanto, você ainda deve proteger a linha de console usando outros meios. Use **ciscoccna** para todas as senhas deste laboratório.

Tarefa 1: Preparar a rede

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

Etapa 2: Apagar todas as configurações existentes nos roteadores.

Etapa 2: Executar configurações básicas do roteador

Etapa 1: Configurar roteadores.

Configure os roteadores R1, R2 e R3 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 um banner de mensagem do dia.
- Configure endereços IP em interfaces em R1, R2 e R3.
- Habilite RIPv2 em todos os roteadores para todas as redes.
- Crie uma interface de loopback em R2 para simular a conexão com a Internet.
- Crie VLANs nos switches S1 e S3 e configure as respectivas interfaces para participar das VLANs.
- Configure roteador R3 para conectividade segura de SDM.
- Instale SDM em PC3 ou R3 caso ele ainda não esteja instalado.

Etapa 2: Configurar interfaces Ethernet.

Configure as interfaces Ethernet do PC1, do PC3 e do Servidor TFTP com os endereços IP e os gateways na tabela de endereçamento no início do laboratório.

Etapa 3: Testar a configuração do PC, executando ping no gateway padrão em todos os PCs e no servidor TFTP.

Tarefa 3: Acesso seguro a roteadores

Etapa 1: Configurar senhas seguras e autenticação AAA utilizando um banco de dados local.

Crie uma senha segura para o acesso ao roteador. Crie o nome de usuário **ccna** para ser armazenado localmente no roteador. Configure o roteador para utilizar o banco de dados de autenticação local. Lembre-se de usar **ciscoccna** para todas as senhas deste laboratório.

Etapa 2: Proteger as linhas de console e vty.

Configure as linhas de console e vty para bloquear um usuário que digita um nome de usuário incorreto e uma senha cinco vezes em 2 minutos. Bloqueie tentativas de login adicionais por 2 minutos.

Etapa 3: Verificar se tentativas de conexão são negadas após o limite de tentativas com falha ser atingido.

Tarefa 4: Acesso seguro à rede

Etapa 1: Proteger o protocolo de roteamento RIP.

Não envie atualizações RIP para roteadores que não estejam na rede (qualquer roteador que não esteja neste cenário). Autentique e criptografe atualizações RIP.

Etapa 2: Verificar se o roteamento RIP ainda funciona.

Tarefa 5: Registrando a atividade em log com protocolo de gerenciamento de rede comum (SNMP)

Etapa 1: Configurar registro em log SNMP no servidor syslog em 192.168.10.250 em todos os dispositivos.

Etapa 2: Registrar mensagens em log com nível de gravidade 4 no servidor syslog.

Tarefa 6: Desabilitando serviços de rede Cisco não utilizados

Etapa 1: Desabilitar interfaces não utilizadas em todos os dispositivos.

Etapa 2: Desabilitar serviços globais não utilizados em R1.

Etapa 3: Desabilitar serviços da interface não utilizados em R1.

Etapa 4: Utilizar AutoSecure para proteger R2.

Lembre-se de usar **ciscoccna** para todas as senhas deste laboratório.

Tarefa 7: Gerenciando arquivos de configuração e do IOS Cisco

Etapa 1: Identificar onde o arquivo de configuração de execução está localizado na memória do roteador.

Etapa 2: Transferir o arquivo de configuração de execução de R1 para R2 utilizando TFTP.

Etapa 3: Interromper R1 e recuperá-lo utilizando ROMmon.

Copie e cole os seguintes comandos em R1 e recupere R1 utilizando ROMmon.

```
line vty 0 4
 exec-timeout 0 20
line console 0
 exec-timeout 0 20
end
copy run start
exit
```

Etapa 4: Restaurar o arquivo de configuração salvo em R1 de R2 utilizando TFTP.

Etapa 5: Apagar a configuração salva em R2.

Tarefa 8: Utilizando SDM para proteger R3

Etapa 1: Conectar-se a R3 utilizando PC3.

Etapa 2: Navegar até o recurso Security Audit.

Etapa 3: Executar uma auditoria de segurança.

Etapa 4: Escolher configurações a serem aplicadas ao roteador.

Etapa 5: Aplicar a configuração ao roteador.

Tarefa 9: Documentar as configurações do roteador

Em cada roteador, emita o comando **show run** e capture as configurações.

Tarefa 10: Limpar

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

