Laboratório - Dispositivos de rede seguros

Topologia

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
R1	G0/0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Implementar as Configurações Básicas dos Dispositivos

Parte 2: Implementar as Medidas Básicas de Segurança no Roteador

Parte 3: Implementar as Medidas Básicas de Segurança no Switch

Histórico/cenário

É recomendável configurar todos os dispositivos de rede com, pelo menos, um conjunto mínimo de comandos de segurança de práticas recomendadas. Isso inclui dispositivos de usuário final, servidores e dispositivos de rede, como roteadores e switches.

Neste laboratório, você configurará os dispositivos de rede na topologia para aceitar sessões SSH para gerenciamento remoto. Você também usará a CLI do IOS para configurar medidas de segurança de práticas recomendadas comuns e básicas. Você testará as medidas de segurança para verificar se foram implementadas e se funcionam corretamente.

Nota: Os roteadores usados nos laboratórios práticos do CCNA são o Cisco 4221 com o Cisco IOS XE Release 16.9.4 (imagem universalk9). Os comutadores usados nos laboratórios são o Cisco Catalyst 2960s com Cisco IOS Release 15.2 (2) (imagem lanbasek9). Outros roteadores, switches e versões do Cisco IOS podem ser usados. De acordo com o modelo e a versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado nos laboratórios. Consulte a Tabela de resumo de interfaces dos roteadores no final do laboratório para saber quais são os identificadores de interface corretos.

Nota: Verifique se os roteadores e comutadores foram apagados e se não há configurações de inicialização. Se tiver dúvidas, fale com o instrutor.

Recursos necessários

- 1 roteador (Cisco 4221 com imagem universal do Cisco IOS XE Release 16.9.4 ou comparável)
- 1 Switch (Cisco 2960 com imagem lanbasek9 do Cisco IOS Release 15.2 (2) ou comparável)
- 1 PC (Windows com um programa de emulação de terminal, como Tera Term)

- Cabos de console para configurar os dispositivos Cisco IOS por meio das portas de console
- Cabos ethernet conforme mostrado na topologia

Instruções

Parte 1: Implementar as Configurações Básicas dos Dispositivos

Na Parte 1, você vai configurar a topologia de rede e implementar as configurações básicas, como os endereços IP das interfaces, o acesso a dispositivos e as senhas nos dispositivos.

Etapa 1: Instalar os cabos da rede conforme mostrado na topologia.

Conecte os dispositivos mostrados na topologia e instale os cabos, conforme necessário.

Etapa 2: Inicializar e recarregar o roteador e o switch.

Etapa 3: Configure o roteador e o switch.

a. Use o console para se conectar ao dispositivo e habilite o modo EXEC privilegiado.

b. Atribua o nome do dispositivo conforme a Tabela de Endereçamento.

c. Desative a pesquisa DNS para evitar que o roteador tente converter comandos inseridos incorretamente como se fossem nomes de host.

d. Atribua class como a senha criptografada do EXEC privilegiado.

e. Atribua cisco como a senha de console e ative o login.

f. Atribua cisco como a senha de VTY e ative o login.

g. Crie um banner para avisar às pessoas que o acesso não autorizado é proibido.

h. Configure e ative a interface G0/0/1 no roteador usando as informações contidas na Tabela de Endereçamento.

i. Configure a SVI padrão no switch com as informações de endereço IP contidas na Tabela de Endereçamento.

j. Salve a configuração atual no arquivo de configuração inicial.

Etapa 4: Configure o PC-A.

a. Configure o PC-A com um endereço IP e uma máscara de sub-rede.

b. Configure um gateway padrão para o PC-A.

Etapa 5: Verificar a conectividade da rede.

Faça ping em R1 e S1 no PC-A. Se algum dos pings falhar, solucione o problema da conexão.

Parte 2: Implementar as Medidas Básicas de Segurança no Roteador

Etapa 1: Configure medidas de segurança.

a. Criptografe todas as senhas de texto não criptografado.

b. Configure o sistema para exigir uma senha mínima de 12 caracteres.

c. Altere as senhas (exec privilegiado, console e vty) para atender ao novo requisito de comprimento.

1) Defina uma senha exec privilegiada para **$cisco!PRIVA***

2) Defina a senha do console como **$cisco!!CON***

3) Defina uma senha da linha vty para **$cisco!!VTY***

d. Configurar o roteador para aceitar somente conexões SSH de locais remotos

   1) Configure o nome do usuário **SSHAdmin** com uma senha criptografada pelo **55Hadm!n2020**

   2) O nome de domínio do roteador deve ser definido como ccna-lab.com

   3) O módulo de chave deve ser 1024 bits.

e. Defina configurações de segurança e práticas recomendadas no console e nas linhas vty.

   1) Os usuários devem ser desconectados após 5 minutos de inatividade.

   2) O roteador não deve permitir logins por 2 minutos e 3 tentativas de login que ocorrem dentro de 1 minuto.

Parte 3: Configure medidas de segurança.

Etapa 1: Verificar se todas as portas não utilizadas estão desativadas.

Por padrão, as portas do roteador são desativadas, mas é sempre prudente verificar se todas as portas não utilizadas estão em um estado “administratively down”. Isso pode ser verificado rapidamente emitindo o comando **show ip interface brief**. Todas as portas não utilizadas que não estão em um estado administrativamente inoperante devem ser desativadas usando o comando **shutdown** no modo de configuração de interface.

Etapa 2: Verificar se as medidas de segurança foram implementadas corretamente.

a. Use Tera Term no PC-A para telnet para R1.

   O R1 aceita a conexão Telnet? Explique.

b. Use Tera Term no PC-A para SSH para R1.

   O R1 aceita a conexão SSH?

c. Digite errado intencionalmente as informações de usuário e senha para ver se o acesso de login é bloqueado após duas tentativas.

   O que aconteceu após o login falhar pela segunda vez?

d. De sua sessão de console no roteador, emita **o comando login** para examinar o status de login. No exemplo abaixo, o comando **show login** foi emitido no período de bloqueio de login de 120 segundos e mostra que o roteador está no Modo silencioso. O roteador não aceitará nenhuma tentativa de login por mais 111 segundos.

e. Após os 120 segundos, SSH para R1 novamente e efetue login usando o nome de usuário **SSHadmin** e **55HAdm!N2020** para a senha.

   Após você fazer o login com êxito, o que foi exibido?

f. Entre no modo EXEC privilegiado e use **$cisco!PRIV*** para a senha.

Se você digitar incorretamente essa senha, será desconectado da sua sessão SSH após três tentativas falhas dentro de 60 segundos? Explique.

g. Emita o comando **show running-config** no prompt do EXEC privilegiado para visualizar as configurações de segurança aplicadas.

Parte 4: Implementar as Medidas Básicas de Segurança no Switch

Etapa 1: Configure medidas de segurança.

a. Criptografe todas as senhas de texto não criptografado.

b. Configurar o sistema para exigir uma senha mínima de 12 caracteres

c. Altere as senhas (exec privilegiado, console e vty) para atender ao novo requisito de comprimento.

1) Defina uma senha exec privilegiada para **$cisco!PRIVA***

2) Defina a senha do console como **$cisco!!CON***

3) Defina a senha da linha vty para **$cisco!!VTY***

d. Configure ou alterne para aceitar somente conexões SSH de locais remotos.

1) Configure o nome de usuário **SSHadmin** com uma senha criptografada de **55HAdm!N2020**

2) O nome de domínio do switch deve ser definido como ccna-lab.com

3) O módulo de chave deve ser 1024 bits.

e. Defina configurações de segurança e práticas recomendadas no console e nas linhas vty.

1) Os usuários devem ser desconectados após 5 minutos de inatividade.

2) O switch não deve permitir logins por 2 minutos e 3 tentativas de login que ocorrem dentro de 1 minuto.

f. Desative todas as portas não utilizadas.

Etapa 2: Verificar se todas as portas não utilizadas estão desativadas.

Por padrão, as portas do switch são habilitadas. Desative todas as portas que não estejam em uso no switch.

a. Você pode verificar o status da porta do switch usando o comando **show ip interface brief**.

b. Use o comando **interface range** para desligar várias interfaces de uma vez.

c. Verifique se todas as interfaces inativas foram administrativamente desligadas.

Etapa 3: Verificar se as medidas de segurança foram implementadas corretamente.

a. Verifique se o Telnet foi desativado no switch.

b. Use SSH no switch e digite errado intencionalmente as informações de usuário e senha para ver se o acesso de login está bloqueado.

c. Após os 30 segundos, SSH para S1 novamente e efetue login usando o nome de usuário **SSHadmin** e **55HAdm!N2020** para a senha.

O banner foi exibido após o login com êxito?

d. Entre no modo EXEC privilegiado usando **$cisco!PRIV*** como a senha.

e. Emita o comando **show running-config** no prompt do EXEC privilegiado para visualizar as configurações de segurança aplicadas.

Perguntas para reflexão

1. O comando **password cisco** foi inserido para o console e as linhas VTY em sua configuração básica na parte 1. Quando essa senha é usada depois que as medidas de segurança de práticas recomendadas foram aplicadas?

2. As senhas pré-configuradas são menores que 10 caracteres afetadas pelo **comando de senhas de segurança comprimento mínimo 12**?

Tabela de resumo das interfaces dos roteadores

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para descobrir como o roteador está configurado, consulte as interfaces para identificar o tipo de roteador e quantas interfaces o roteador possui. Não há como listar efetivamente todas as combinações de configurações para cada classe de roteador. Esta tabela inclui identificadores para as combinações possíveis de Ethernet e

Interfaces seriais no dispositivo. Esse tabela não inclui nenhum outro tipo de interface, embora um roteador específico possa conter algum. Um exemplo disso poderia ser uma interface ISDN BRI. O string entre parênteses é a abreviatura legal que pode ser usada em comandos do Cisco IOS para representar a interface.