Laboratório - Configurar Recursos de Segurança Automatizados .

Topologia

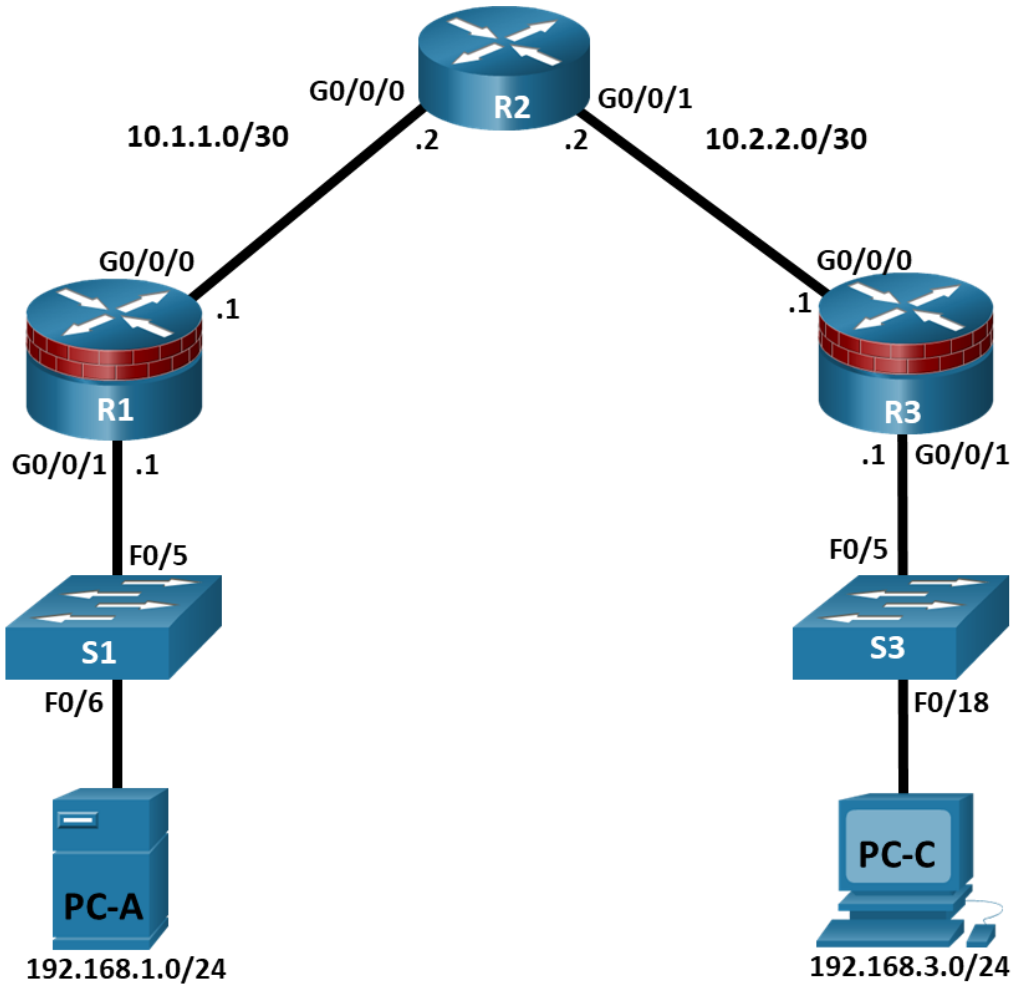

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
R1	G0/0/0	10.1.1.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.1.1	255.255.255.0	N/D	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/D	N/D
	G0/0/1	10.2.2.2	255.255.255.252	N/D	N/D
R3	G0/0/0	10.2.2.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.3.1	255.255.255.0	N/D	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objetivos

Parte 1: Implementar as Configurações Básicas do Dispositivo

- Cabeie a rede conforme mostrado na topologia.
- Configure o endereçamento IP básico para roteadores e PCs.

- Configure o roteamento de OSPF.
- Configure os PCs hosts.
- Verifique a conectividade entre hosts e roteadores.

Parte 2: Configurar Recursos de Segurança Automatizados

- Bloqueie um roteador usando autosegure e verifique a configuração.
- Contraste usando autosegure com a proteção manualmente um roteador usando a linha de comando.

Histórico/Cenário

O roteador é um componente crítico em qualquer rede. Controla o movimento de dados dentro e fora da rede e entre dispositivos dentro da rede. É particularmente importante proteger os roteadores de rede porque a falha de um dispositivo de roteamento pode fazer seções da rede ou toda a rede, inacessível. Controlando o acesso a roteadores e a ativação de relatórios em roteadores é fundamental para a segurança de rede e deve fazer parte de uma política de segurança abrangente.

Neste laboratório, você criará uma rede multi-roteador e configurará os roteadores e os hosts. Você usará recursos de segurança automatizados no roteador R3.

Nota: Os roteadores usados com laboratórios hands-on são Cisco 4221 com a versão 16.9.6 do Cisco Ios Xe (Universife9). Os switches usados nos laboratórios são Cisco Catalyst 2960+ com a versão Cisco IOS 15.2 (7) (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: Antes de começar, verifique se os roteadores e os comutadores foram apagados e não têm configurações de inicialização.

Recursos necessários

- 3 roteadores (Cisco 4221 com a Cisco Xe Release 16.9.6 Imagem universal ou comparável com uma licença de pacote de tecnologia de segurança)
- 2 switches (Cisco 2960+ com lançamento do Cisco IOS 15.2 (7) imagem lanbasek9 ou comparável)
- 2 PCs (SO Windows com um programa de emulação de terminal, como Tera Term ou PuTTy instalado)
- Cabos de console para configurar dispositivos de rede Cisco
- Cabos ethernet conforme mostrado na topologia

Instruções

Parte 1: Implementar as Configurações Básicas do Dispositivo

Nesta parte, configure a topologia da rede e configure as configurações básicas, como endereços IP da interface.

Etapa 1: Conectar a rede.

Anexar os dispositivos, conforme mostrado no diagrama de topologia e cabo conforme necessário.

Etapa 2: Defina as configurações básicas de cada Roteador.

a. Use o console para se conectar ao roteador e ative o modo EXEC privilegiado.

```
Router> enable
```

```
Router# configure terminal
```

Configure os nomes de host conforme mostrado na topologia.

```
R1(config)# hostname R1
```

Configure endereços IP da interface conforme mostrado na tabela de endereçamento IP.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1 (configuração) # interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

b. Para evitar que o roteador tente traduzir comandos inseridos incorretamente como se fossem nomes de host, desative a pesquisa de DNS. R1 é mostrado aqui como exemplo.

```
R1(config)#no ip domain-lookup
```

Etapa 3: Configure o roteamento do OSPF nos roteadores.

a. Use o comando **router ospf** no modo de configuração global para ativar o OSPF em R1.

```
R1(config)# router ospf 1
```

b. Configure as instruções **network** para as rede em R1. Use um ID de área igual a 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure o OSPF em R2 e R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Emita o comando **passive-interface** Para alterar a interface G0/0/1 em R1 e R3 para passivo.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Etapa 4: Verifique os vizinhos OSPF e as informações de roteamento.

a. Emita o comando **show ip ospf neighbor** para verificar se cada roteador lista os outros roteadores na rede como vizinhos.

```
R1# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 1 FULL/BDR 00:00:37 10.1.1.2 GigabitEthernet0/0/0
```

b. Emita o comando **show ip route** para verificar se todas as redes são exibidas na tabela de roteamento em todos os roteadores.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set.

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O 10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O 192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Etapa 5: Defina as configurações de IP do host do PC.

Configure um endereço IP estático, máscara de sub-rede e gateway padrão para PC-A e PC-C, conforme mostrado na tabela de endereçamento IP.

Etapa 6: Verifique a conectividade entre PC-A e PC-C.

a. Faça ping de R1 para R3.

Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

b. Ping do PC-A, na LAN R1, para PC-C, na LAN R3.

Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

Nota: Se você puder ping do PC-A para PC-C, você demonstrou que o roteamento OSPF é configurado e funcionando corretamente. Se você não puder ping, mas as interfaces do dispositivo são para cima e os endereços IP estão corretos, use os comandos **show run, show ip ospf neighbor,** e **show ip route** para ajudar a identificar problemas relacionados ao protocolo de roteamento.

Parte 2: Configurar configurações de segurança básicas no R1

Nesta parte, copie e cole os seguintes comandos em R1 para configurar as configurações básicas de segurança.

```
enable
configure terminal
service password-encryption
security passwords min-length 10
```

```
Ativar algoritmo-tipo scrypt secreto cisco12345
ip domain name netsec.com
nome de usuário user01 tipo de algoritmo scrypt secret user01pass
username admin privilege 15 algorithm-type scrypt secret adminpasswd
banner motd " Unauthorized access is strictly prohibited! "
line con 0
 exec-timeout 5 0
login local
 logging synchronous
line aux 0
 exec-timeout 5 0
login local
line vty 0 4
 exec-timeout 5 0
 privilege level 15
transport input ssh
 login local
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
```

Parte 3: Configurar recursos de segurança automatizados

Nesta parte, você fará o seguinte:

- Use AutoSecure para garantir R3.
- Revise as configurações de segurança do roteador com CLI.

Ao usar um único comando no modo CLI, o recurso AutoSecure permite desativar serviços IP comuns que podem ser explorados para ataques de rede. Também pode habilitar serviços e recursos IP que podem ajudar na defesa de uma rede quando sob ataque. Autosecure simplifica a configuração de segurança de um roteador e endurece a configuração do roteador.

Etapa 1: Use o recurso AutoSecure Cisco IOS no R3.

a. Entre no modo EXEC privilegiado usando o comando **enable**.

b. Emita o comando **auto secure** no R3 para bloquear o roteador. R2 representa um roteador ISP, então assuma que R3 G0/0/0 está conectado à Internet quando solicitado pelas perguntas AutoSecure. Responda às perguntas do AutoSecure, conforme mostrado na saída a seguir. As respostas são negrito.

```
R3# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
o roteador, mas não vai fazer roteador absolutamente seguro
de todos os ataques de segurança***

All the configuration done as part of AutoSecure will be
shown here. For more details of why and how this configuration
```

```
is useful, and any possible side effects, please refer to Cisco
documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: yes

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing internet [1]:
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 10.2.2.1 YES manual up up
GigabitEthernet0/0/1 192.168.3.1 YES manual up up
Serial0/1/0 unassigned YES unset up up
Serial0/1/1 unassigned YES unset up up
Enter the interface name that is facing internet: GigabitEthernet0/0/0

Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Aqui está um exemplo de banner de segurança a ser mostrado
em todos os acessos ao dispositivo. Modifique para se adequar ao seu
requisitos da empresa.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
```

```
  are logged. Any violations of access policy will result
  in disciplinary action.

Digite o banner de segurança {colocar o banner entre
k e k, onde k é qualquer caracteres}:
# Unauthorized Access Prohibited #
Ativar segredo não está configurado ou
 é o mesmo que a senha de habilitação
Digite a nova senha de enable: cisco12345
Confirme a senha de enable: cisco12345
Digite a nova senha enable: 12345cisco
Confirme a senha enable: 12345cisco

Configuração do banco de dados do usuário local
Digite o nome de usuário: admin
Digite a senha: adminpasswd
Confirme a senha: adminpasswd
Configurando a AAA Local Autenticação
Configurando console, linhas Aux e vty para
autenticação local, exec-timeout, transporte
Protegendo o dispositivo contra ataques de login
Configurar os seguintes parâmetros

Período de bloqueio quando o ataque de login detectado: 60

Falhas de login máximos com o dispositivo: 2

Período máximo de tempo para cruzar as tentativas de login com falha: 30

Configurar o servidor SSH? [yes]: [Enter]
Digite o nome do domínio: www.netsec.com

Configurando serviços automáticos específicos da interface
Desativando os seguintes serviços IP em todas as interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply

Protegendo os serviços do plano de encaminhamento

Ativando o Unicast RPF em todas as interfaces conectadas
a internet
```

```
Configurar o recurso CBAC Firewall? [yes/no]: no

Esta é a configuração gerada:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
banner motd ^C Unauthorized Access Prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$lubv$Rdx4gHUcijbxV7p2z76/71
enable password 7 110A1016141D5D5B5C737B
username admin password 7 02050D4808095E731F1A5C
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
login block-for 60 attempts 2 within 30
ip domain-name www.netsec.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
```

```
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int GigabitEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int GigabitEthernet0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip access-list extended 100
 permit udp any any eq bootpc
interface GigabitEthernet0/0/0
 ip verify unicast source reachable-via rx 100
!
end


Apply this configuration to running-config? [yes]: [Enter]


Applying the config generated to running-config


 WARNING: Command has been added to the configuration using a type 5
password. However, type 5 passwords will soon be deprecated. Migrate to a
supported password type

 WARNING: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to a
supported password type

 WARNING: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to a
supported password typeThe name for the keys will be: R3.www.netsec.com


% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 0 seconds)


R3#
```

Nota: As perguntas feitas e a saída pode variar depender dos recursos da imagem e do dispositivo iOS.

Etapa 2: Estabelecer uma conexão SSH do PC-C para R3.

a. Inicie PuTTY ou outro cliente SSH, e faça login com a conta de **admin** e senha **adminpasswd** criado quando AutoSecure foi executado. Digite o endereço IP da interface R3 G0/0/1 **192.168.3.1**.

b. Como o SSH foi configurado usando AutoSecure no R3, você receberá um aviso de segurança PuTTY. Clique em **Yes** para se conectar de qualquer maneira.

c. Entre com o modo de EXEC privilegiado com a senha **cisco12345**, e verifique a configuração R3 usando o comando **show run** .

Etapa 3: Contraste a configuração gerada pelo AutoSecure de R3 com a configuração manual do R1.

1. Quais alterações de configuração relacionadas à segurança foram realizadas no R3 por AutoSecure que não foram executadas em seções anteriores do laboratório no R1?

2. Quais alterações de configuração relacionadas à segurança foram realizadas em seções anteriores do laboratório que não foram executadas por AutoSecure?

3. Identifique pelo menos cinco serviços desnecessários que foram bloqueados pela Autosecure e pelo menos três medidas de segurança aplicadas a cada interface.

   Nota: Alguns dos serviços listados como desativados na saída AutoSecure acima podem não aparecer no **show running-config** saída porque eles já estão desativados por padrão para este roteador e versão do Cisco IOS.

   Os serviços desativados incluem:

   Para cada interface, o seguinte foi desativado:

4. Quais são algumas vantagens em usar AutoSecure?

Tabela de resumo das interfaces dos roteadores

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
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)
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. A string entre parênteses é a abreviatura legal que pode ser usada no comando do Cisco IOS para representar a interface.