Laboratório 4.6.1: Configuração básica de segurança

Diagrama de topologia

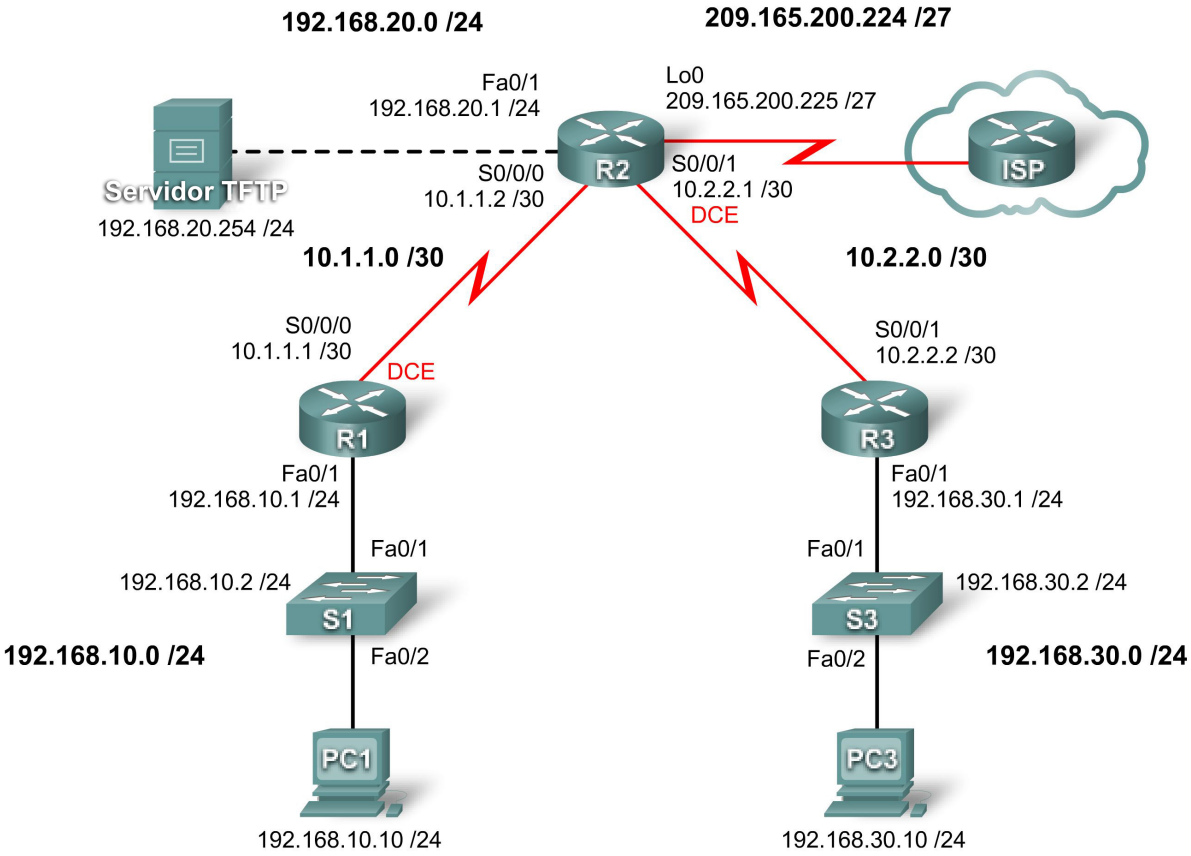


Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
R1	**Fa0/1**	192.168.10.1	255.255.255.0	N/A
	S0/0/0	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	**VLAN10**	192.168.10.2	255.255.255.0	N/A
S3	**VLAN20**	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 a segurança básica de 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) e o SDM Express para configurar a segurança básica do roteador.
- Configurar VLANs nos switches.

Cenário

Neste laboratório, você irá aprender a configurar a segurança de rede básica usando a rede mostrada no diagrama de topologia. Você saberá como configurar segurança do roteador de três maneiras diferentes: utilizando a CLI, o recurso auto-secure e o Cisco SDM. Você também aprenderá a gerenciar o software IOS Cisco.

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 na topologia.

Nota: Este laboratório foi desenvolvido e testado utilizando-se roteadores 1841. Se você usar roteadores da série 1700, 2500 ou 2600, as saídas do roteador e as descrições de interface poderão ser diferentes.

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 R1, R2 e R3.
- Habilite o RIP versão 2 em todos os roteadores de todas as redes.

- Crie uma interface de loopback em R2 para simular a conexão com a Internet.
- Configure um servidor TFTP no PC2. Se você precisar baixar o software do servidor TFTP, uma opção será: http://tftpd32.jounin.net/

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: Proteger o roteador do acesso não autorizado

Etapa 1: Configurar senhas seguras e autenticação AAA.

Utilize um banco de dados local em R1 para configurar senhas seguras. Use **ciscoccna** para todas as senhas deste laboratório.

```
R1(config)#enable secret ciscoccna
```

Como a configuração de uma senha enable secret ajuda a impedir que um roteador seja comprometido por um ataque?

_____

_____

_____

O comando **username** cria um nome de usuário e uma senha armazenados localmente no roteador. O nível de privilégio padrão do usuário é 0 (o menor volume de acesso). Você pode alterar o nível de acesso para um usuário, adicionando a palavra-chave **privilege** *0-15* antes da palavra-chave **password**.

```
R1(config)#username ccna password ciscoccna
```

O comando **aaa** permite AAA (Autenticação, Autorização e Auditoria) globalmente no roteador. Ele é utilizado durante a conexão com o roteador.

```
R1(config)#aaa new-model
```

Você pode criar uma lista de autenticação acessada quando alguém tenta fazer login no dispositivo depois de aplicá-la às linhas vty e de console. A palavra-chave **local** indica que o banco de dados do usuário está armazenado localmente no roteador.

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

Nota: LOCAL_AUTH é um nome de etiqueta que diferencia maiúsculas de minúsculas e que deve corresponder a todos os usos.

Os comandos a seguir informam ao roteador que os usuários que estão tentando se conectar a ele devem ser autenticados utilizando-se a lista recém-criada.

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
```



```
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

O que você observa não ser seguro quanto à seguinte seção da configuração de execução:

```
R1#show run
<saída de comando omitida>
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
<saída de comando omitida>
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 login authentication LOCAL_AUTH
linha auxiliar 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

_____

_____

_____

Para aplicar criptografia simples às senhas, digite o seguinte comando no modo de configuração global:

```
R1(config)#service password-encryption
```

Verifique isso com o comando **show run**.

```
R1#show run
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
<saída de comando omitida>
!
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
```



```
 login authentication LOCAL_AUTH
linha auxiliar 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

Etapa 2: Proteger as linhas de console e VTY.

O roteador pode fazer logout em uma linha ociosa por um determinado período. Se um engenheiro de rede tiver feito login em um dispositivo de rede e for chamado repentinamente, este comando fará o logout do usuário automaticamente depois do período especificado. Os seguintes comandos causam o logout na linha após 5 minutos.

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

O seguinte comando impede tentativas de login de força bruta. O roteador bloqueará tentativas de login durante 5 minutos se houver falha em duas tentativas de login em 2 minutos. Ele é especialmente definido baixo para este laboratório. Uma medida adicional é registrar em log sempre que isso acontecer.

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 2 log
```

Para verificar isso, tente se conectar a R1 em R2 via Telnet com um nome de usuário e senha incorretos.

Em R2:

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication Failed

User Access Verification

Username: cisco
Password:

% Authentication Failed

[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```


Em R1:

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

Tarefa 4: Acesso seguro à rede

Etapa 1: Impedir a propagação da atualização de roteamento RIP.

Quem pode receber atualizações RIP em um segmento de rede onde o RIP esteja habilitado? Essa é a configuração mais desejável?

_____

_____

_____

O comando **passive-interface** impede roteadores de enviar atualizações de roteamento a todas as interfaces, exceto as interfaces configuradas para participar das atualizações de roteamento. Esse comando é emitido como parte da configuração RIP.

O primeiro comando coloca todas as interfaces no modo passivo (a interface só recebe atualizações RIP). O segundo comando passa interfaces específicas do modo passivo para o ativo (enviando e recebendo atualizações RIP).

R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```

Etapa 2: Impedir a recepção não autorizada de atualizações RIP.

Impedir atualizações RIP desnecessárias em toda a rede é a primeira etapa para proteger o RIP. A próxima é proteger a senha de atualizações RIP. Para isso, você deve primeiro configurar uma chave a ser utilizada.

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

Ela precisa ser adicionada a todos os roteadores que receberão atualizações RIP.

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
```



```
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

Para utilizar a chave, todas as interfaces que participam de atualizações RIP precisam ser configuradas. Elas serão as mesmas interfaces habilitadas utilizando-se o comando **no passive-interface** anterior.

R1

```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

A esta altura, R1 deixa de receber atualizações RIP de R2, porque R2 ainda não foi configurado para utilizar uma chave para atualizações de roteamento. Você pode exibir isso em R1, utilizando o comando **show ip route** e confirmando se não há nenhuma rota de R2 exibida na tabela de roteamento.

Limpe rotas IP com **clear ip route *** ou aguarde o timeout das rotas.

```
R1#show ip route
Codes: 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C    192.168.10.0 is directly connected, Serial0/0/0
```

Configure R2 e R3 para utilizar a autenticação de roteamento. Lembre-se de que todas as interfaces ativas devem ser configuradas.

R2

```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```

R3

```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

Etapa 3: Verificar se o roteamento RIP ainda funciona.

Depois de todos os três roteadores serem configurados para utilizar a autenticação de roteamento, as tabelas de roteamento devem ser preenchidas novamente com todas as rotas RIP. Agora R1 deve ter todas as rotas via RIP. Confirme isso com o comando **show ip route**.

```
R1#show ip route
Codes: 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

Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R       10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C       10.1.1.0/24 is directly connected, Serial0/0/0
```

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.

O registro em log SNMP pode ser útil na monitoração da atividade de rede. As informações capturadas podem ser enviadas para um servidor syslog na rede, onde podem ser analisadas e arquivadas. Você deve tomar cuidado ao configurar o registro em log (syslog) no roteador. Ao escolher o host de log designado, lembre-se de que o host de log deve ser conectado a uma rede confiável ou protegida ou à interface de um roteador isolada e dedicada.

Neste laboratório, você irá configurar PC1 como o servidor syslog para R1. Use o comando **logging** para escolher o endereço IP do dispositivo para o qual mensagens SNMP são enviadas. Neste exemplo, o endereço IP do PC1 é utilizado.

```
R1(config)#logging 192.168.10.10
```

Nota: PC1 deverá ter software de syslog instalado e em execução se você quiser exibir mensagens de syslog.

Na próxima etapa, você definirá o nível de gravidade para mensagens a serem enviadas para o servidor syslog.

Etapa 2: Configurar o nível de gravidade SNMP.

O nível de mensagens SNMP pode ser ajustado para permitir ao administrador determinar que tipos de mensagens são enviados para o dispositivo syslog. Roteadores oferecem suporte a níveis diferentes de registro em log. Os oito níveis vão de 0 (emergências), indicando que o sistema está instável, a 7 (depuração), que envia mensagens que incluem informações do roteador. Para configurar os níveis de gravidade, você utiliza a palavra-chave associada ao nível, conforme mostrado na tabela.

Nível de gravidade	Palavra-chave	Descrição
0	emergencies	Sistema inutilizável
1	alerts	Ação imediata obrigatória
2	critical	Condições críticas
3	errors	Condições de erro
4	warnings	Condições de aviso
5	notifications	Condição normal, mas significativa

6	informational	Mensagens informativas
7	debugging	Depurando mensagens

O comando **logging trap** define o nível de gravidade. O nível de gravidade inclui o nível especificado e qualquer coisa abaixo dele (gravidade). Defina R1 para o nível 4 a fim de capturar mensagens com os níveis de gravidade 4, 3, 2 e 1.

```
R1(config)#logging trap warnings
```

Qual é o perigo de definir o nível de gravidade muito alto ou baixo?

_____

_____

_____

Nota: se você tiver instalado software syslog em PC1, gere e procure em um software syslog as mensagens.

Tarefa 6: Desabilitando serviços de rede Cisco não utilizados

Etapa 1: Desabilitar interfaces não utilizadas.

Por que você deve desabilitar interfaces não utilizadas em dispositivos de rede?

_____

_____

_____

No diagrama de topologia, você pode ver que R1 só deve utilizar as interfaces S0/0/0 e Fa0/1. Todas as outras interfaces em R1 devem ser desativadas administrativamente utilizando-o o comando de configuração da interface **shutdown**.

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown

*Sep 10 13:40:24.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Sep 10 13:40:25.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

Para verificar se R1 tem todas as interfaces inativas desativadas, utilize o comando **show ip interface brief**. As interfaces desativadas manualmente são listadas como desativadas administrativamente.

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.10.1    YES manual up                    up
Serial0/0/0            10.1.1.1        YES manual up                    up
```



```
Serial0/0/1            unassigned      YES unset  administratively down down
```

Etapa 2: Desabilitar serviços globais não utilizados.

Muitos serviços não são necessários na maioria das redes modernas. Deixar serviços não utilizados habilitados mantém portas abertas, que podem ser utilizadas para comprometer uma rede. Desabilite todos esses serviços em R1.

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

Etapa 3: Desabilitar serviços da interface não utilizados.

Estes comandos são digitados no nível da interface, devendo ser aplicados a todas as interfaces em R1.

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachables
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

Etapa 4: Utilizar o AutoSecure para proteger um roteador Cisco.

Utilizando um único comando no modo CLI, o recurso AutoSecure permite desabilitar serviços IP comuns que podem ser explorados para ataques de rede e habilitar serviços IP e recursos que podem ajudar na defesa de uma rede sob ataque. O AutoSecure simplifica a configuração de segurança de um roteador e protege a configuração do roteador.

Utilizando o recurso AutoSecure, você pode aplicar os mesmos recursos de segurança que acabou de aplicar (exceto a proteção do RIP) a um roteador muito mais rapidamente. Como você já protegeu R1, utilize o comando **auto secure** em R3.

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

***AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure
```



```
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1

Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0/0            unassigned      YES unset  down        down
FastEthernet0/1            192.168.30.1    YES manual up          up
Serial0/0/0                unassigned      YES manual down        down
Serial0/0/1                10.2.2.2        YES manual up          up
Enter the interface name that is facing the internet: Serial0/0/1
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
Enable secret is either not configured or
 Is the same as enable password
Enter the new enable password: ciscoccna
Confirm the enable password: ciscoccna
Enter the new enable password: ccnacisco
Confirm the enable password: ccnacisco

Configuration of local user database
Enter the username: ccna
Enter the password: ciscoccna
Confirm the password: ciscoccna
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 300

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 120

Configure SSH server? Yes
Enter domain-name: cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
```



```
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC firewall feature: no
Tcp intercept feature is used prevent tcp syn attack
On the servers in the network. Create autosec_tcp_intercept_list
To form the list of servers to which the tcp traffic is to be observed

Enable TCP intercept feature: yes

This is the configuration generated:

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
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
linha auxiliar 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
line tty 192
 login authentication local_auth
 exec-timeout 15 0
```



```
login block-for 300 attempts 5 within 120
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
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
```



```
!
end

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

The name for the keys will be: R3.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
R3#
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

Como você pode ver, o recurso AutoSecure é muito mais rápido a configuração linha por linha. No entanto, há vantagens em fazer isso manualmente, como você verá no laboratório de identificação e solução de problemas. Ao utilizar o AutoSecure, você pode desabilitar um serviço de que precisa. Antes de utilizar o AutoSecure, sempre tome cuidado e pense nos serviços obrigatórios.

Tarefa 7: Gerenciando arquivos de configuração e do IOS Cisco

Etapa 1: Mostrar arquivos do IOS Cisco.

IOS Cisco é o software utilizado por roteadores para operar. O roteador pode ter memória suficiente para armazenar várias imagens do IOS Cisco. É importante saber quais são os arquivos armazenados no roteador.

Emita o comando **show flash** para exibir o conteúdo da memória flash do roteador.

Cuidado: tenha muito cuidado ao emitir comandos que envolvam a memória flash. A digitação errada de um comando pode resultar na exclusão da imagem do IOS Cisco.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4       833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar

8679424 bytes available (23252992 bytes used)
```

Basta observarmos essa lista, e já podemos determinar o seguinte:

- A imagem é para um roteador 1841 (c**1841**-ipbase-mz.124-1c.bin).
- O roteador está utilizando a imagem IP base (c1841-**ipbase**-mz.124-1c.bin).
- A versão do IOS Cisco é 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin).
- O SDM está instalado no dispositivo (**sdm**config-18xx.cfg, **sdm**.tar).

Você pode utilizar o comando **dir all** para mostrar todos os arquivos no roteador.

```
R1#dir all
Directory of archive:/

No files in directory

No space information available
Directory of system:/
```



```
 3  dr-x           0                    <no date>  memory
 1  -rw-         979                    <no date>  running-config
 2  dr-x           0                    <no date>  vfiles

No space information available
Directory of nvram:/

 189  -rw-         979                      <no date>  startup-config
 190  ----           5                      <no date>  private-config
 191  -rw-         979                      <no date>  underlying-config
   1  -rw-           0                      <no date>  ifIndex-table

196600 bytes total (194540 bytes free)
Directory of flash:/

 1 -rw- 13937472  May 05 2007 20:08:50 +00:00  c1841-ipbase-mz.124-1c.bin
 2 -rw-     1821  May 05 2007 20:25:00 +00:00  sdmconfig-18xx.cfg
 3 -rw-  4734464  May 05 2007 20:25:38 +00:00  sdm.tar
 4 -rw-   833024  May 05 2007 20:26:02 +00:00  es.tar
 5 -rw-  1052160  May 05 2007 20:26:30 +00:00  common.tar
 6 -rw-     1038  May 05 2007 20:26:56 +00:00  home.shtml
 7 -rw-   102400  May 05 2007 20:27:20 +00:00  home.tar
 8 -rw-   491213  May 05 2007 20:27:50 +00:00  128MB.sdf
 9 -rw-   398305  May 05 2007 20:29:08 +00:00  sslclient-win-1.1.0.154.pkg
 10 -rw- 1684577  May 05 2007 20:28:32 +00:00  securedesktop-ios-3.1.1.27-
k9.pkg

31932416 bytes total (8679424 bytes free)
```

Etapa 2: Transferir arquivos com TFTP.

O TFTP é utilizado durante o arquivamento e a atualização do software IOS Cisco de um dispositivo. Neste laboratório, no entanto, não utilizamos arquivos do IOS Cisco reais porque qualquer equívoco feito na digitação dos comandos poderia ocasionar a exclusão da imagem do IOS Cisco do dispositivo. Ao final desta seção, há um exemplo de como deve ser uma transferência TFTP no IOS Cisco.

Por que é importante ter uma versão atualizada do software IOS Cisco?

_____

_____

_____

Durante a transferência de arquivos via TFTP, é importante assegurar que o servidor TFTP e o roteador consigam se comunicar. Uma maneira de testar isso é executando ping entre esses dispositivos.

Para começar a transferência do software IOS Cisco, crie um arquivo no servidor TFTP chamado **test** na pasta raiz TFTP. Cada programa TFTP muda de acordo com o local no qual os arquivos estão armazenados. Consulte o arquivo de ajuda do servidor TFTP para determinar a pasta raiz.

Em R1, recupere o arquivo e salve-o na memória flash.

```
R1#copy tftp flash
Address or name of remote host []? 192.168.20.254  (endereço IP do servidor TFTP)
Source filename []? Test  (nome do arquivo criado e salvo no servidor TFTP)
```



```
Destination filename [test]? test-server (Um nome arbitrário para o arquivo quando salvo no roteador)
Accessing tftp://192.168.20.254/test...
Loading test from 192.168.20.254 (via FastEthernet0/1): !
[OK - 1192 bytes]

1192 bytes copied in 0,424 secs (2811 bytes/sec)
```

Verifique a existência do arquivo na memória flash com o comando **show flash**.

```
R1#show flash
-#- -- length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server

8675328 bytes available (23257088 bytes used)
```

Os roteadores também podem funcionar como servidores TFTP. Isso poderá ser útil se houver um dispositivo que precise de uma imagem e você tiver um que já esteja usando essa imagem. Tornaremos R2 um servidor TFTP para R1. Lembre-se de que essas imagens do IOS Cisco são específicas de plataformas de roteador e requisitos de memória. Tome cuidado ao transferir uma imagem do IOS Cisco de um roteador para outro.

A sintaxe do comando é: **tftp-server nvram:** [*nome de arquivo1* [**alias** *nome de arquivo2*]

O comando abaixo configura R2 como um servidor TFTP. R2 fornece seu arquivo de configuração de inicialização para dispositivos que o solicitam via TFTP (estamos utilizando a configuração de inicialização por conta da simplicidade e da facilidade). A palavra-chave **alias** permite a dispositivos solicitar o arquivo utilizando o alias **test**, e não o nome de arquivo completo.

```
R1(config)#tftp-server nvram:startup-config alias test
```

Agora podemos solicitar o arquivo em R2 utilizando R1.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? teste
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]

1192 bytes copied in 0,452 secs (2637 bytes/sec)
```

Novamente, verificar se o arquivo **test** foi copiado com êxito com o comando **show flash**


```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server
12        1192 Sep 12 2007 07:51:04 +00:00 test-router

8671232 bytes available (23261184 bytes used)
```

Como você não deseja que arquivos não utilizados ocupem espaço importante da memória, exclua-os agora da memória flash de R1. **Tome muito cuidado ao fazer isso!** Apagar a memória flash acidentalmente irá significar a necessidade de reinstalação de toda a imagem do IOS do roteador. Se o roteador solicitar **erase flash**, será sinal de que algo está muito errado. É raro você desejar apagar toda a memória flash. O único momento legítimo em que isso acontece é quando você está atualizando o IOS para uma imagem de IOS maior. Se você vir o prompt **erase flash** como neste exemplo, PARE IMEDIATAMENTE. NÃO pressione enter. Peça ajuda ao seu instrutor IMEDIATAMENTE.

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

Verifique se os arquivos foram excluídos, emitindo o comando **show flash**.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg

8679424 bytes available (23252992 bytes used)
```

Este é um exemplo de uma transferência TFTP de um arquivo de imagem do IOS Cisco.

NÃO complete nos roteadores. Apenas leia.


```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via Serial0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<saída de comando omitida>
!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]

13937472 bytes copied in 1113,948 secs (12512 bytes/sec)
```

Etapa 3: Recuperar uma senha utilizando ROMmon.

Se, por alguma razão, não conseguir mais acessar um dispositivo porque você não sabe, perdeu, ou esqueceu uma senha, você ainda assim poderá obter acesso, alterando o registro de configuração. O registro de configuração informa ao roteador que configuração carregar durante a inicialização. No registro de configuração, você pode instruir o roteador a inicializar a partir de uma configuração em branco não protegida por senha.

A primeira etapa da alteração do registro de configuração é exibir a configuração atual utilizando o comando **show version**. Essas etapas são executadas em R3.

```
R3#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

R3 uptime is 25 minutes
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"

Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
Processor board ID FTX1118X0BN
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes de NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Em seguida, recarregue o roteador e envie uma interrupção durante a inicialização. A tecla **Break** é diferente em computadores diferentes. Normalmente, ela fica no canto superior direito do teclado. Uma interrupção faz o dispositivo entrar em um modo chamado ROMmon. Esse modo não exige do dispositivo ter acesso a um arquivo de imagem do IOS Cisco.

Nota: o Hyperterminal exige uma sequência Ctrl-Break. Para outro software de emulação de terminal, verifique as combinações padrão da sequência da tecla Break.


```
R3#reload
Proceed with reload? [confirm]

*Sep 12 08:27:28.670: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload command.
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Readonly ROMMON initialized
rommon 1 >
```

Altere o registro de configuração para um valor que carrega a configuração inicial do roteador. Essa configuração não tem uma senha configurada, mas dá suporte a comandos do IOS Cisco. Altere o valor do registro de configuração para 0x2142.

```
rommon 1 > confreg 0x2142
```

Agora que ele foi alterado, podemos inicializar o dispositivo com o comando **reset**.

```
rommon 2 > reset
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0xd4a9a0
Self decompressing the image :
############################################################
################################################################################
# [OK]

<saída de comando omitida>


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!
```

Etapa 4: Restaurar o roteador.

Agora copiamos a configuração de inicialização para a configuração de execução, restauramos a configuração e alteramos o registro de configuração novamente para o padrão (0x2102).

Para copiar a configuração de inicialização da NVRAM para a memória de execução, digite **copy startup-config running-config**. Tome cuidado! *Não* digite `copy running-config startup-config`, ou você apagará a configuração de inicialização.

```
Router#copy startup-config running-config
Destination filename [running-config]? {enter}

2261 bytes copied em 0,576 secs (3925 bytes/sec)
```



```
R3#:show running-config
<saída de comando omitida>
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
!
<saída de comando omitida>
!
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
<saída de comando omitida>
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

Nessa configuração, o comando **shutdown** é exibido em todas as interfaces porque todas elas estão desativadas no momento. Mas o mais importante é que agora você pode ver as senhas (senha de enable, enable secret, VTY, senhas de console) em um formato criptografado ou desprotegido. Você pode reutilizar senhas não-criptografadas. Você deve alterar senhas criptografadas para uma nova senha.


```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret ciscoccna
R3(config)#username ccna password ciscoccna
```

Emita o comando **no shutdown** em todas as interfaces que você deseja utilizar.

```
R3(config)#interface FastEthernet0/1
R3(config-if)#no shutdown
R3(config)#interface Serial0/0/1
R3(config-if)#no shutdown
```

Você pode emitir um comando **show ip interface brief** para confirmar se a configuração da interface está correta. Todas as interfaces que você deseja usar devem ser exibidas como ativadas.

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
FastEthernet0/1        192.168.30.1    YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Serial0/0/0            10.2.2.2        YES NVRAM  up                    up
```

Digite **Config-register** *valor do registro de configuração*. A variável *valor do registro de configuração* é o valor registrado na Etapa 3 ou 0x2102. Salve a configuração de execução.

```
R3(config)#config-register 0x2102
R3(config)#end
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Quais são as desvantagens da recuperação de senha?

_____

_____

_____

Tarefa 8: Utilizando o SDM para proteger um roteador

Nesta tarefa, você utilizará o Security Device Manager (SDM), a interface gráfica do usuário, para proteger o roteador R2. O SDM é mais rápido que digitar cada comando e oferece mais controle que o recurso AutoSecure.

Verifique se o SDM foi instalado no roteador:

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 Sep 12 2007 08:31:42 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
```



```
9       1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10       398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11         2261 Sep 25 2007 23:20:16 +00:00 Tr(RIP)
12         2506 Sep 26 2007 17:11:58 +00:00 save.txt
```

Se NÃO estiver instalado no roteador, o SDM deverá ser instalado para continuar. Consulte o seu instrutor para obter instruções.

Etapa 1: Conectar-se ao R2 utilizando o servidor TFTP.

Crie um nome de usuário e senha em R2.

```
R2(config)#username ccna password ciscoccna
```

Habilite o servidor http seguro em R2 e conecte-se a R2 utilizando um navegador no servidor TFTP.

```
R2(config)#ip http secure-server
% Generating 1024 bit RSA Keys, Keys Will be non-exportable... [OK]
R2(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue
"write memory" to save new certificate
R2(config)#end
R2#copy run start
```

No servidor TFTP, abra um navegador e navegue até https://192.168.20.1/. Faça login com o nome de usuário e senha configurados anteriormente:

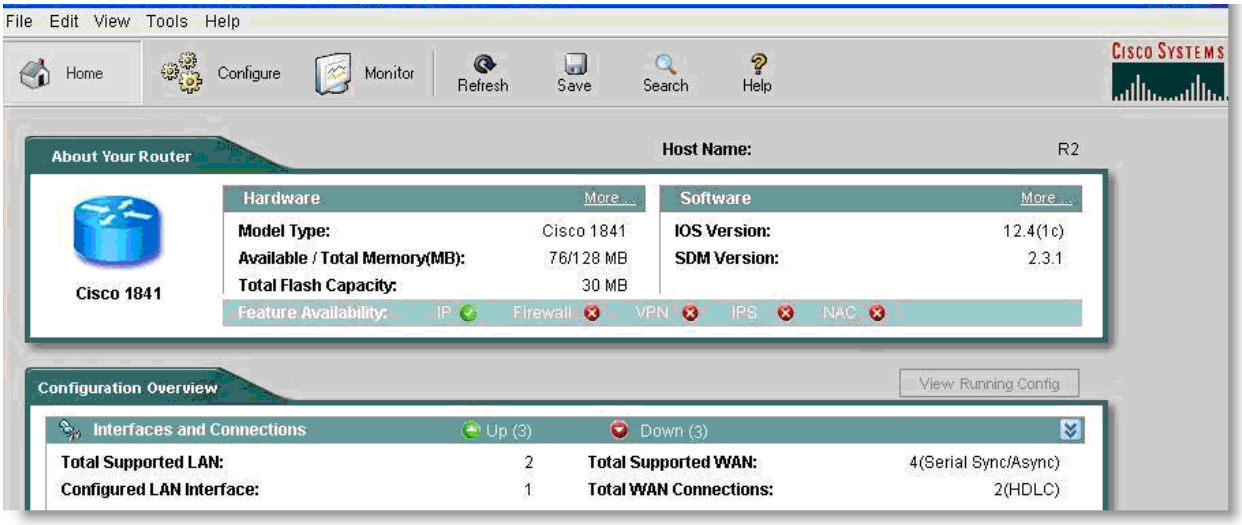
nome de usuário: **ccna**

senha: **ciscoccna**

Selecione **Cisco Router and Security Device Manager**

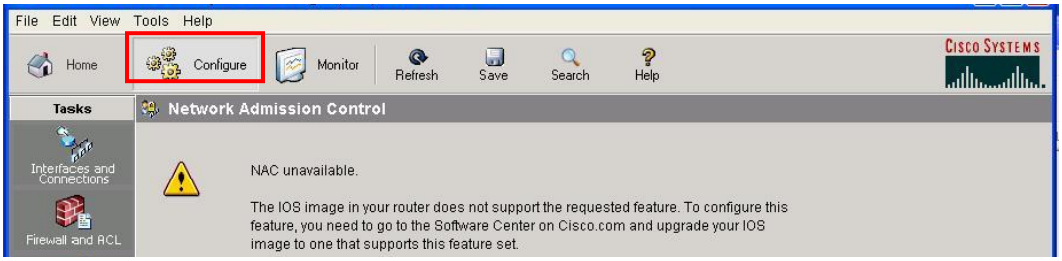
Abra o Internet Explorer e digite o endereço IP para R2 na barra de endereços. Uma nova janela é aberta. Verifique se todos os bloqueadores de popup foram desativados no navegador. Também verifique se o JAVA está instalado e atualizado.

Depois de concluído o carregamento, uma nova janela é aberta para o SDM.

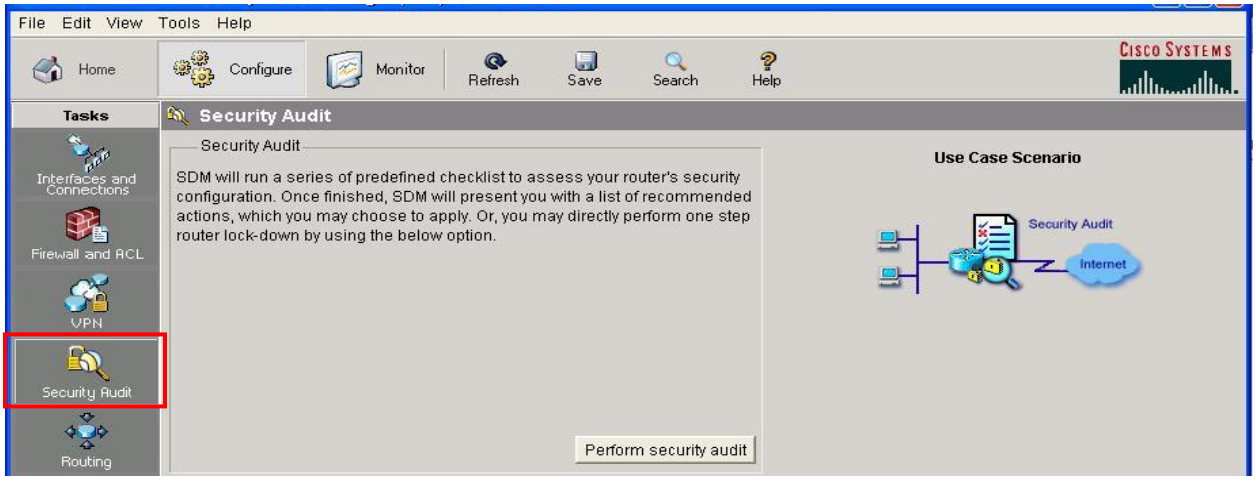


Etapa 2: Navegar até o recurso Security Audit.

Clique no botão **Configure** no canto superior esquerdo da janela.

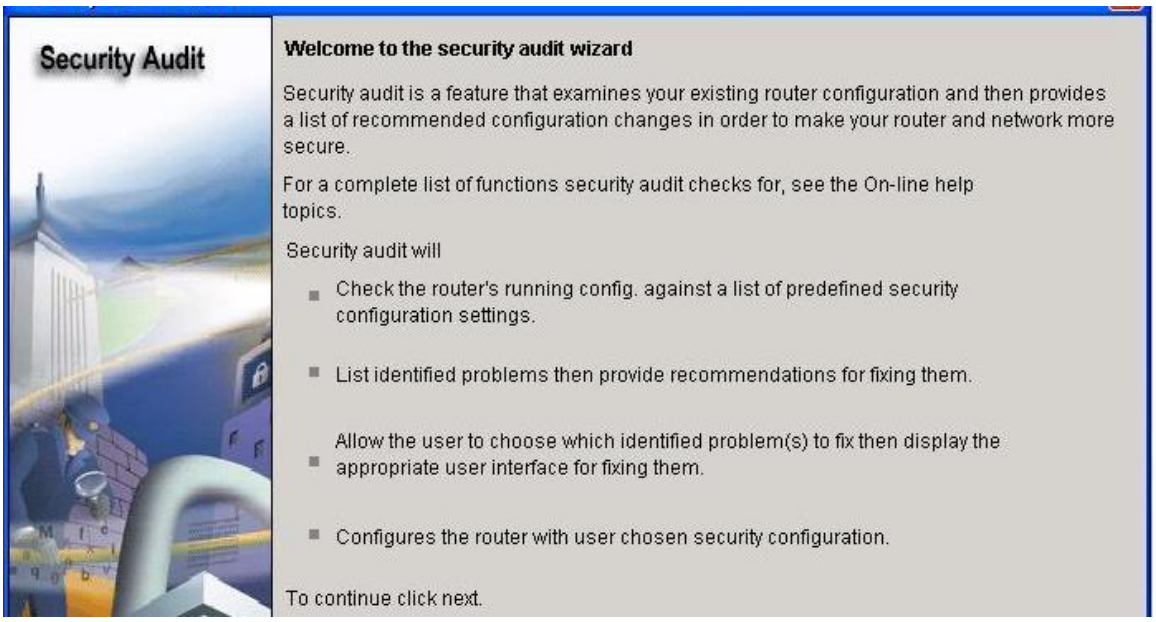


Agora navegue no painel à esquerda até **Security Audit** e clique nele.



Quando você clicar em **Security Audit,** outra janela é aberta.

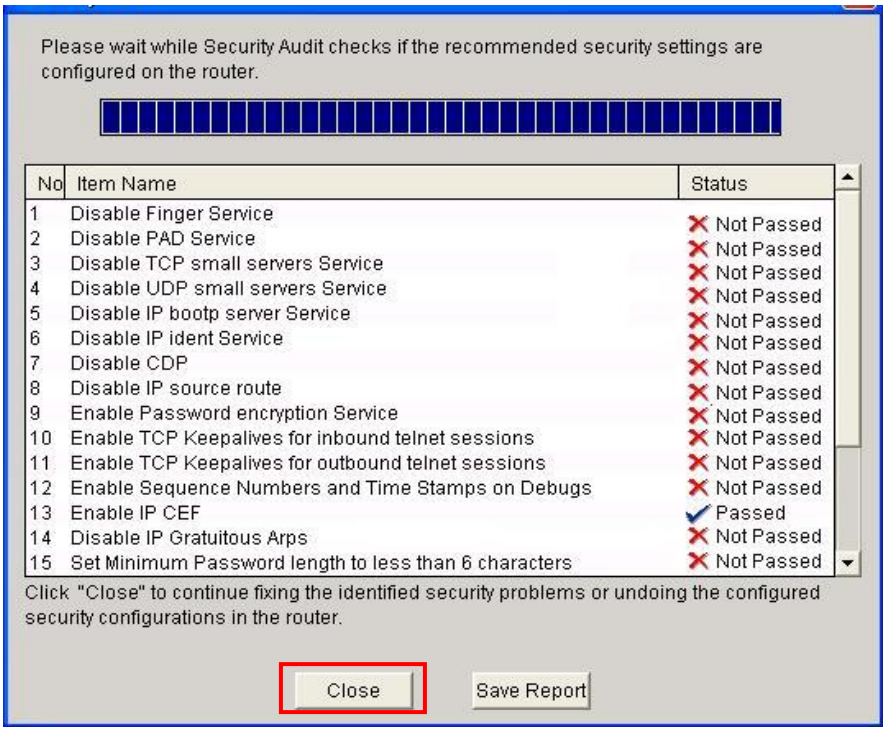
Etapa 3: Executar uma auditoria de segurança.



Ela oferece uma rápida explicação do que o recurso Security Audit faz. Clique em **Next** para abrir a janela Security audit interface configuration.

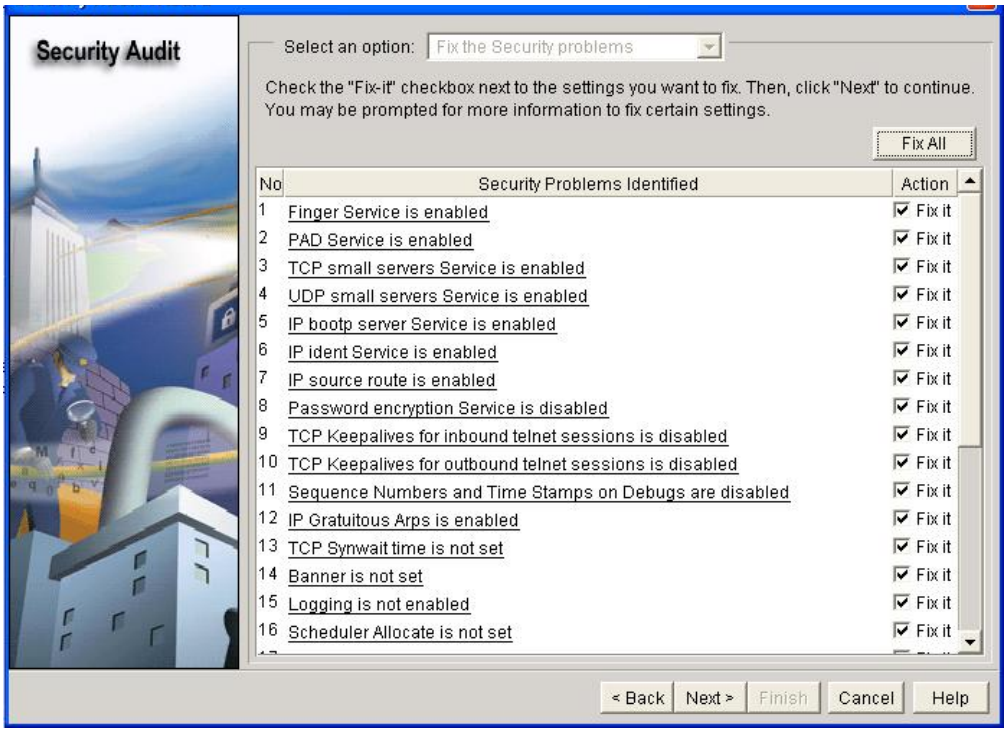
Uma interface deverá ser classificada como externa (não confiável) se você não tiver certeza da legitimidade do tráfego que chega à interface. Nesse exemplo, FastEthernet0/1 e Serial0/1/0 não são confiáveis porque Serial0/1/0 está diante da Internet e Fastethernet0/1 está diante da parte de acesso da rede, e tráfego não legítimo pode ser gerado.

Depois de selecionar as interfaces externa e interna, clique em **Next**. Uma nova janela é aberta indicando que o SDM está realizando uma auditoria de segurança.

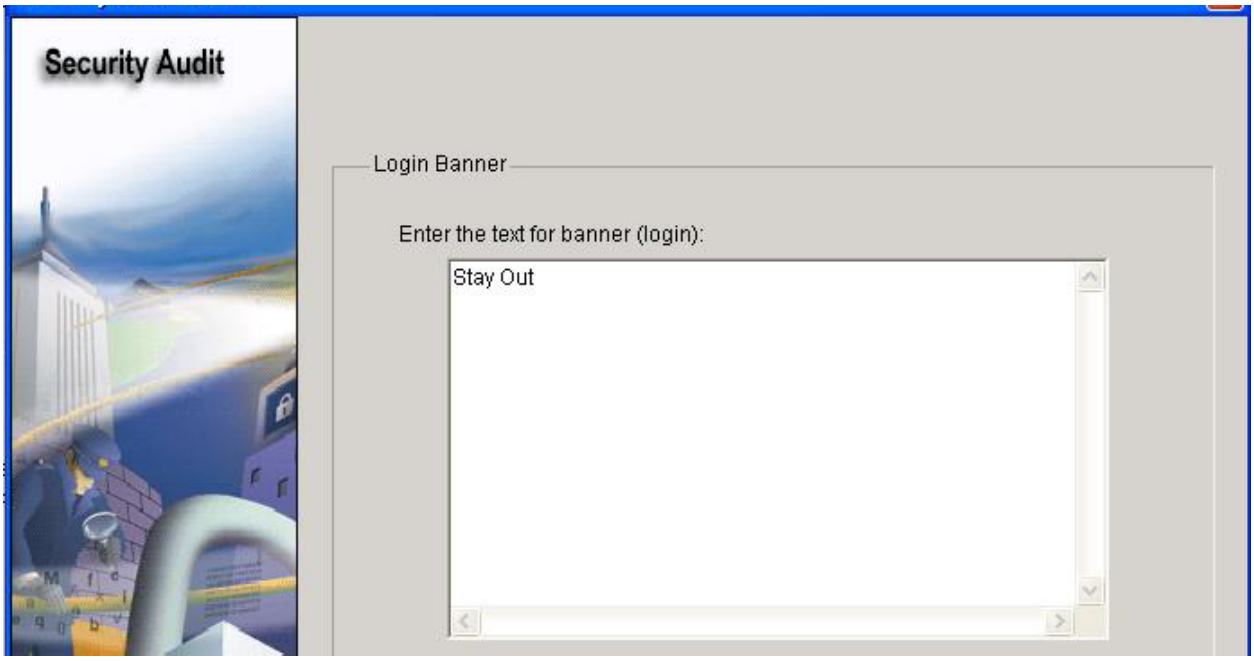


Como você pode ver, a configuração padrão não é segura. Clique no botão **Close** para continuar.

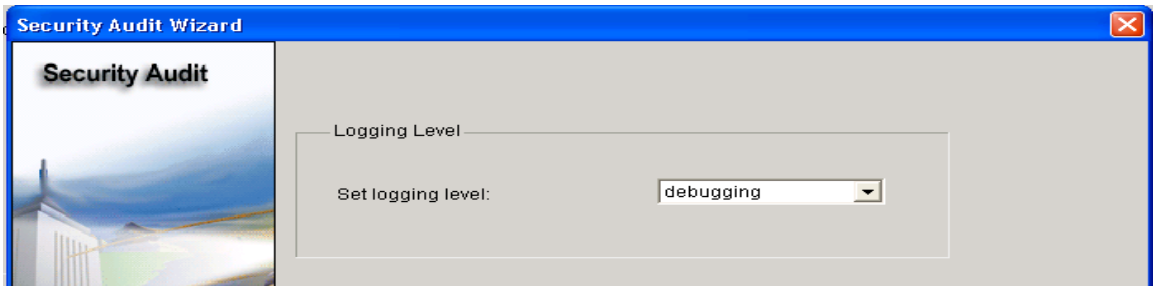
Etapa 4: Aplicar configurações ao roteador.



Clique no botão **Fix All** para fazer todas as alterações de segurança sugeridas. Em seguida, clique no botão **Next**.

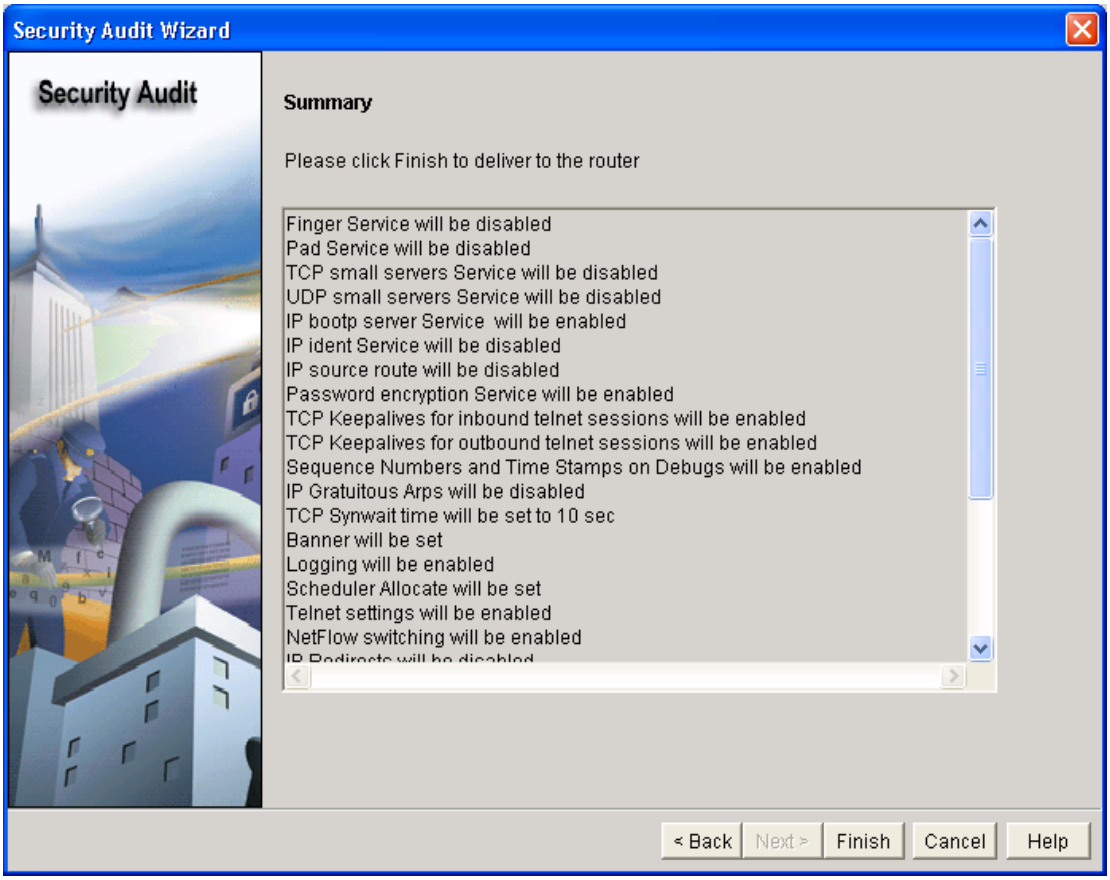


Digite em uma mensagem de banner a ser utilizada como a mensagem do dia para o roteador e clique em **Next**.

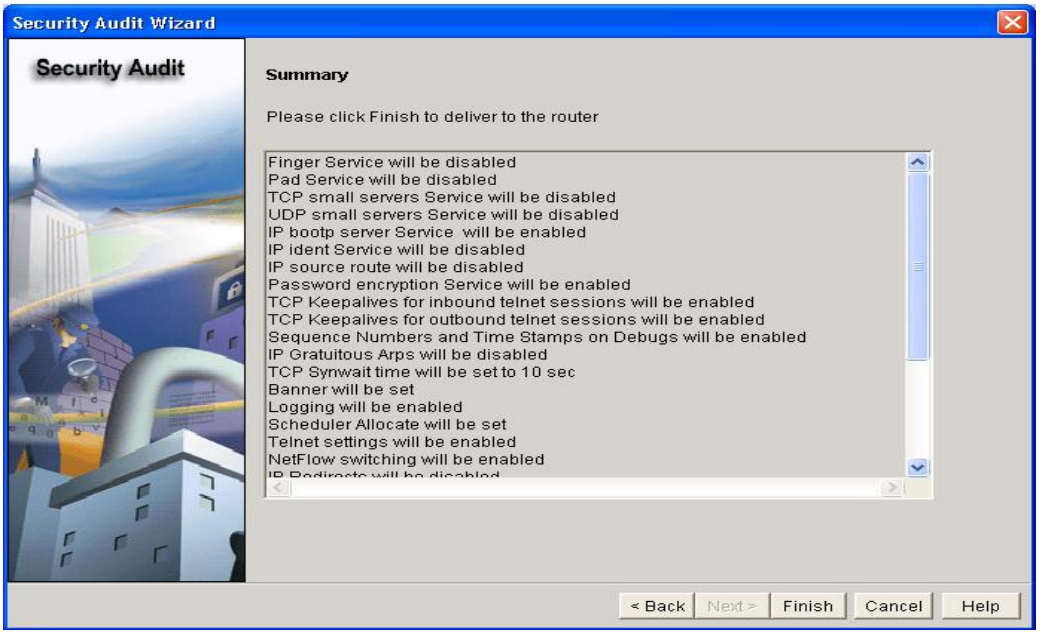


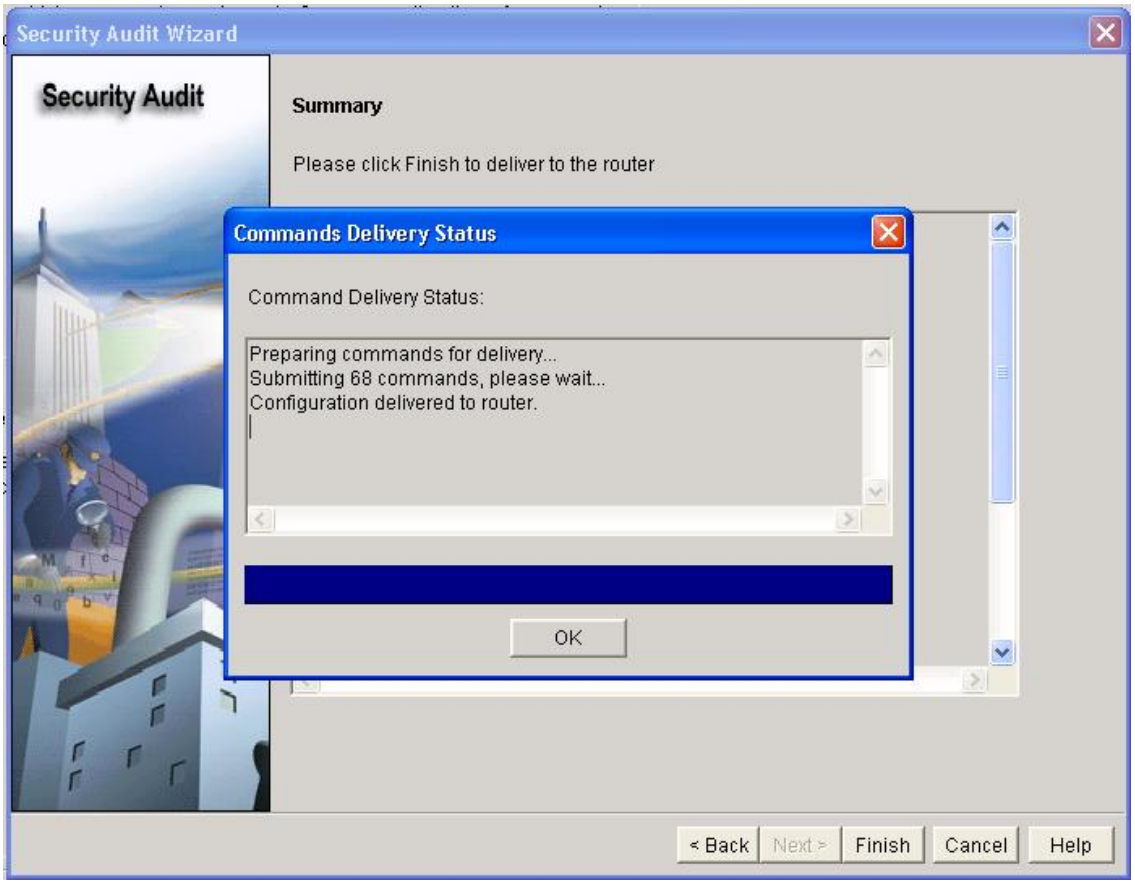
Em seguida, defina o nível de gravidade dos traps de log que o roteador deve enviar ao servidor syslog. O nível de gravidade é definido como depuração para este cenário. Clique em **Next** para exibir uma sumarização das alterações a serem feitas no roteador.

Etapa 5: Aplicar a configuração ao roteador.



Depois de revisar as alterações a serem feitas, clique em **Finish**.





Clique em **OK** e saia do SDM.

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 de PC normalmente conectados a outras redes (como a rede local escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.

