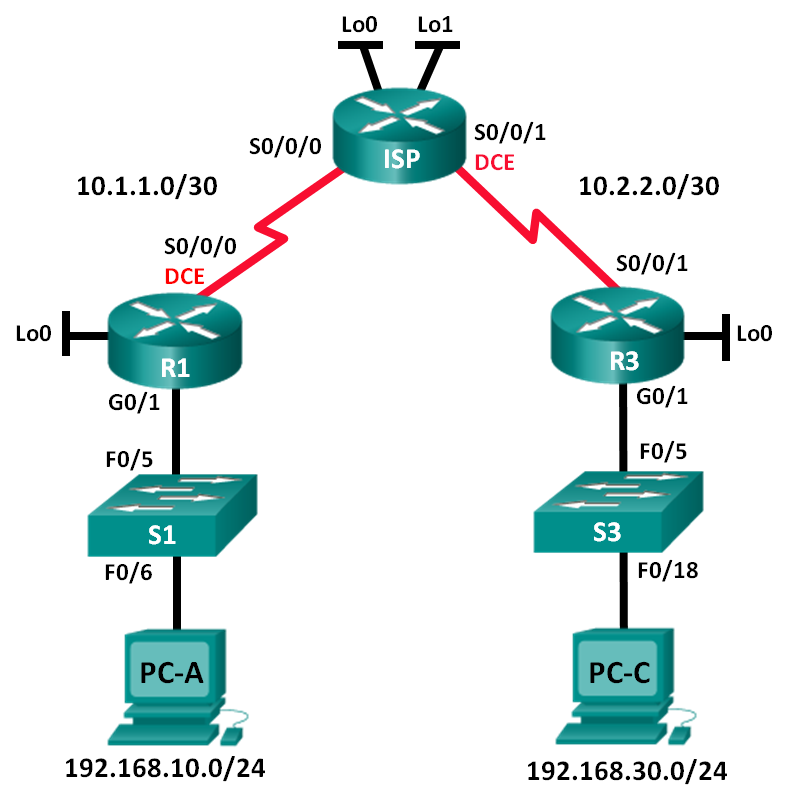
**9.3.2.13: Configuración y verificación de ACL extendidas**

1. Topología



1. Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/A |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| ISP | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
|  | Lo1 | 209.165.201.1 | 255.255.255.224 | N/A |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/A |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

1. Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

* Configurar los parámetros básicos de las computadoras, los routers y los switches.
* Configurar los procesos de routing EIGRP en el R1, el ISP y el R3.

Parte 3: configurar y verificar ACL extendidas numeradas y con nombre

* Configurar, aplicar y verificar una ACL extendida numerada.
* Configurar, aplicar y verificar una ACL extendida con nombre.

Parte 4: modificar y verificar ACL extendidas

1. Información básica/situación

Las listas de control de acceso (ACL) extendidas son sumamente eficaces. Ofrecen un mayor grado de control que las ACL estándar en cuanto a los tipos de tráfico que se pueden filtrar y también en cuanto al lugar de origen y el destino del tráfico.

En esta práctica de laboratorio, establecerá reglas de filtrado para dos oficinas representadas por el R1 y el R3. La administración estableció algunas políticas de acceso entre las redes LAN ubicadas en el R1 y el R3, que usted debe implementar. El router ISP que se ubica entre el R1 y el R3 no tiene ninguna ACL. Usted no tiene permitido el acceso administrativo al router ISP, dado que solo puede controlar y administrar sus propios equipos.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

1. Recursos necesarios

* 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
* 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
* 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
* Cables Ethernet y seriales, como se muestra en la topología

1. establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, si fuera necesario.

1. realizar el cableado de red tal como se muestra en la topología.
2. inicializar y volver a cargar los routers y los switches.
3. Configurar dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos en los routers, los switches y las computadoras. Consulte la topología y la tabla de direccionamiento para conocer los nombres de los dispositivos y obtener información de direcciones.

1. configurar las direcciones IP en la PC-A y en la PC-C.
2. configurar los parámetros básicos en el R1.
3. Desactive la búsqueda del DNS.
4. Configure el nombre del dispositivo como se muestra en la topología.
5. Cree una interfaz loopback en el R1.
6. Configure las direcciones IP de interfaz, como se muestra en la topología y en la tabla de direccionamiento.
7. Configure class como la contraseña del modo EXEC privilegiado.
8. Asigne la frecuencia de reloj 128000 a la interfaz S0/0/0.
9. Asigne cisco como la contraseña de vty y la contraseña de consola, y habilite el acceso por Telnet. Configure logging synchronous para las líneas de consola y las líneas vty.
10. Habilite el acceso web en el R1 para simular un servidor web con autenticación local para el usuario admin.

R1(config)# ip http server

R1(config)# ip http authentication local

R1(config)# username admin privilege 15 secret class

1. configurar los parámetros básicos en el ISP.
2. Configure el nombre del dispositivo como se muestra en la topología.
3. Cree las interfaces loopback en el ISP.
4. Configure las direcciones IP de interfaz, como se muestra en la topología y en la tabla de direccionamiento.
5. Desactive la búsqueda del DNS.
6. Asigne class como la contraseña del modo EXEC privilegiado.
7. Asigne la frecuencia de reloj 128000 a la interfaz S0/0/1.
8. Asigne cisco como la contraseña de vty y la contraseña de consola, y habilite el acceso por Telnet. Configure logging synchronous para las líneas de consola y las líneas vty.
9. Habilite el acceso web en el ISP. Utilice los mismos parámetros que en el paso 2h.
10. configurar los parámetros básicos en el R3.
11. Configure el nombre del dispositivo como se muestra en la topología.
12. Cree una interfaz loopback en el R3.
13. Configure las direcciones IP de interfaz, como se muestra en la topología y en la tabla de direccionamiento.
14. Desactive la búsqueda del DNS.
15. Asigne class como la contraseña del modo EXEC privilegiado.
16. Asigne cisco como la contraseña de consola y configure logging synchronous en la línea de consola.
17. Habilite SSH en el R3.

R3(config)# ip domain-name cisco.com

R3(config)# crypto key generate rsa modulus 1024

R3(config)# line vty 0 4

R3(config-line)# login local

R3(config-line)# transport input ssh

1. Habilite el acceso web en el R3. Utilice los mismos parámetros que en el paso 2h.
2. (optativo) configurar los parámetros básicos en el S1 y el S3.
3. Configure los nombres de host como se muestra en la topología.
4. Configure las direcciones IP de las interfaces de administración como se muestra en la topología y en la tabla de direccionamiento.
5. Desactive la búsqueda del DNS.
6. Configure class como la contraseña del modo EXEC privilegiado.
7. Configure la dirección de gateway predeterminado.
8. Configure el routing de EIGRP en el R1, el ISP y el R3.
9. Configure el sistema autónomo (AS) número 10 y anuncie todas las redes en el R1, el ISP y el R3. Desactivar la sumarización automática.
10. Después de configurar EIGRP en el R1, el ISP y el R3, verifique que todos los routers tengan tablas de routing completas con todas las redes. De lo contrario, resuelva el problema.
11. verificar la conectividad entre los dispositivos.

Nota: es muy importante verificar la conectividad antes de configurar y aplicar ACL. Asegúrese de que la red funcione adecuadamente antes de empezar a filtrar el tráfico.

1. Desde la PC-A, haga ping a la PC-C y a las interfaces loopback y de serie en el R3.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_si

1. Desde el R1, haga ping a la PC-C y a las interfaces loopback y serial en el R3.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_ si

1. Desde la PC-C, haga ping a la PC-A y a las interfaces loopback y serial en el R1.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_ si

1. Desde el R3, haga ping a la PC-A y a las interfaces loopback y serial en el R1.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_ si

1. Desde la PC-A, haga ping a las interfaces loopback en el router ISP.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_ si

1. Desde la PC-C, haga ping a las interfaces loopback en el router ISP.

¿Los pings se realizaron correctamente? \_\_\_\_\_\_\_\_ si

1. Abra un navegador web en la PC-A y vaya a [http://209.165.200.225](https://www.google.com/url?q=http://209.165.200.225&sa=D&ust=1611621058865000&usg=AOvVaw3HkORNExZK13PBKEYiuI95) en el ISP. Se le pide que introduzca un nombre de usuario y contraseña. Utilice admin como el nombre de usuario y class como la contraseña. Si se le solicita que acepte una firma, acéptela. El router cargará Cisco Configuration Professional (CCP) Express en una ventana diferente. Es posible que se le solicite un nombre de usuario y una contraseña. Utilice admin como el nombre de usuario y class como la contraseña.
2. Abra un navegador web en la PC-C y vaya a [http://10.1.1.1](https://www.google.com/url?q=http://10.1.1.1&sa=D&ust=1611621058865000&usg=AOvVaw0mvuJ-5IOJqRQhsGBFduuk) en el R1. Se le pide que introduzca un nombre de usuario y contraseña. Utilice admin como el nombre de usuario y class como la contraseña. Si se le solicita que acepte una firma, acéptela. El router cargará CCP Express en una ventana diferente. Es posible que se le solicite un nombre de usuario y una contraseña. Utilice admin como el nombre de usuario y class como la contraseña.
3. configurar y verificar ACL extendidas numeradas y con nombre

**Las ACL extendidas filtran el tráfico de diferentes formas. Las ACL extendidas pueden realizar el filtrado según direcciones IP de origen, puertos de origen, dirección IP de destino y puertos de destino, así como según varios protocolos y servicios.**

**Las políticas de seguridad son las siguientes:**

1. **Permitir que el tráfico web que se origina en la red 192.168.10.0/24 vaya a cualquier red.**
2. **Permitir una conexión SSH a la interfaz serial del R3 desde la PC-A.**
3. **Permitir que los usuarios en la red 192.168.10.0.24 accedan a la red 192.168.20.0/24.**
4. **Permitir que el tráfico web que se origina en la red 192.168.30.0/24 acceda al R1 mediante la interfaz web y la red 209.165.200.224/27 en el ISP. NO se debe permitir que la red 192.168.30.0/24 tenga acceso a cualquier otra red a través de la web.**

Al observar las políticas de seguridad mencionadas anteriormente, sabe que necesitará al menos dos ACL para cumplir con ellas. Una práctica recomendada es colocar ACL extendidas lo más cerca posible del origen. Para estas políticas, respetaremos esta práctica.

**Configurar una ACL extendida numerada en el R1 para las políticas de seguridad 1 y 2.**

1. Usará una ACL extendida numerada en el R1. ¿Cuáles son los rangos de las ACL extendidas?
   1. **199 y 2000 a 2699**
2. Configure la ACL en el R1. Use 100 como el número de la ACL.

**R1(config)# access-list 100 remark Allow Web & SSH Access**

**R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22**

**R1(config)# access-list 100 permit tcp any any eq 80**

1. ¿Qué indica el 80 que aparece en el resultado del comando anterior?

**80 es el puerto de destino. El puerto TCP 80 es un puerto bien conocido que se usa para el protocolo HTTP.**

1. ¿A qué interfaz debe aplicarse la ACL 100?

**Hay dos respuestas posibles aquí: G0/1 y S0/0/0. La colocación de la ACL en G0/1 podría bloquear el acceso de los usuarios en la red 192.168.10.0/24 a otras LAN conectadas al R1, como la red 192.168.20.0/24. Por este motivo, la colocará en S0/0/0.**

1. ¿En qué sentido se debería aplicar la ACL 100?

**Si en la respuesta anterior se mencionó la interfaz G0/1, la ACL 100 debe aplicarse en sentido de entrada. Si el estudiante respondió con S0/0/0, la ACL 100 debe aplicarse en sentido de salida.**

1. Aplique la ACL 100 a la interfaz S0/0/0.

**R1(config)# int s0/0/0**

**R1(config-if)# ip access-group 100 out**

**Verifique la ACL 100**

1. Establezca una conexión SSH de la PC-A al R3 con 10.2.2.1 como dirección IP. Inicie sesión con las credenciales admin y class. La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.
2. En la petición de entrada del modo EXEC privilegiado en el R1, emita el comando show access-lists.

**R1# show access-lists**

**Extended IP access list 100**

**10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)**

**20 permit tcp any any eq www (111 matches)**

1. Desde el símbolo del sistema de la PC-A, emita un ping a 10.2.2.1. Explique los resultados.

**Los pings fallaron. El mensaje fue “Reply from 192.168.10.1: Destination net unreachable” (Respuesta desde 192.168.10.1: red de destino inalcanzable). Esto se debe a la instrucción deny any implícita al final de cada ACL. La ACL 100 solo permite tráfico de salida web y SSH.**

**Configurar una ACL extendida con nombre en el R3 para la política de seguridad 3.**

1. Configure la política en el R3. Asigne el nombre WEB-POLICY a la ACL.

**R3(config)# ip access-list extended WEB-POLICY**

**R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

**R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80**

1. Aplique la ACL WEB-POLICY a la interfaz S0/0/1.

**R3(config-ext-nacl)# int S0/0/1**

**R3(config-if)# ip access-group WEB-POLICY out**

**Verifique la ACL WEB-POLICY.**

1. En la petición de entrada del modo EXEC privilegiado en el R3, emita el comando show **ip interface s0/0/1. CORREGIR s0/1/1** ¿Cuál es el nombre de la ACL, si tiene un nombre? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**WEB-POLICY**
2. ¿En qué sentido se aplicó la ACL? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**De salida**
3. Abra un navegador web en la PC-C y vaya a [http://209.165.200.225](https://www.google.com/url?q=http://209.165.200.225&sa=D&ust=1611621058869000&usg=AOvVaw2q8Pr5jTDXDH3Ntq4_tV_z) (el router ISP). La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.
4. Desde la PC-C, inicie una sesión web en [http://10.1.1.1](https://www.google.com/url?q=http://10.1.1.1&sa=D&ust=1611621058869000&usg=AOvVaw19PSnVId92z8QxniVLdHVt) (R1). La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.
5. Desde la PC-C, inicie una sesión web en [http://209.165.201.1](https://www.google.com/url?q=http://209.165.201.1&sa=D&ust=1611621058869000&usg=AOvVaw1NM6GuNcQ9obNNhi4cCw40) (router ISP). La conexión debería fallar; de lo contrario, resuelva el problema.
6. Desde el símbolo del sistema de la PC-C, haga ping a la PC-A. ¿Cuál fue el resultado y por qué?

**Los pings fallaron. En la red 192.168.30.0/24, solo se permite la salida de tráfico web.**

**Modificar y verificar ACL extendidas**

Debido a las ACL aplicadas en el R1 y el R3, no se permiten pings ni ningún otro tipo de tráfico entre las redes LAN en el R1 y el R3. La administración decidió que debe permitirse todo el tráfico entre las redes 192.168.10.0/24 y 192.168.30.0/24. Debe modificar las ACL en el R1 y el R3.

**Modificar la ACL 100 en el R1.**

1. En el modo EXEC privilegiado en el R1, emita el comando show access-lists. ¿Cuántas líneas hay en esta lista de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2 líneas, la n.º 10 y la n.º 20.**
2. Ingrese al modo de configuración global y modifique la ACL en el R1.

**R1(config)# ip access-list extended 100**

**R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255**

**R1(config-ext-nacl)# end**

1. Emita el comando **show access-lists**. ¿En qué lugar de la ACL 100 apareció la línea nueva que acaba de agregar?

**Línea n.º 30. La última línea de la ACL.**

**Modificar la ACL WEB-POLICY en el R3.**

1. En el modo EXEC privilegiado en el R3, emita el comando show access-lists. ¿Cuántas líneas hay en esta lista de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **2 líneas, la n.º 10 y la n.º 20.**
2. Ingrese al modo de configuración global y modifique la ACL en el R3.

**R3(config)# ip access-list extended WEB-POLICY**

**R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

**R3(config-ext-nacl)# end**

1. Emita el comando **show access-lists** para verificar que la línea nueva se haya agregado al final de la ACL.

**Verificar las ACL modificadas.**

1. Desde la PC-A, haga ping a la dirección IP de la PC-C. ¿Tuvieron éxito los pings? \_\_\_\_\_\_\_\_\_\_\_\_\_\_ si
2. Desde la PC-C, haga ping a la dirección IP de la PC-A. ¿Tuvieron éxito los pings? \_\_\_\_\_\_\_\_\_\_\_\_\_\_ si
3. **VERIFICAR PINGS HACIA OTRAS REDES NO DEBE FUNCIONAR**

¿Por qué las ACL funcionaron inmediatamente para los pings después de que las cambió?

**Las ACL en el R1 y el R3 todavía estaban aplicadas a las interfaces respectivas con el comando ip access-group command.**

**Reflexión**

1. ¿Por qué es necesario planificar y probar meticulosamente las ACL?

**Las ACL pueden bloquear involuntariamente la entrada o la salida de tráfico legítimo en una red**

1. Qué tipo de ACL es mejor: ¿estándar o extendida?

**Ambas tienen un propósito y un lugar en una red. Las ACL estándar son fáciles de componer y configurar, si necesita permitir o denegar todo el tráfico. La desventaja de las ACL estándar es que solo pueden revisar direcciones de origen y no tienen granularidad. Las ACL extendidas se pueden escribir para que filtren prácticamente todo tipo de tráfico generado. Sin embargo, puede ser complicado configurarlas y entenderlas.**

Configuraciones de dispositivos

Router R1

R1# show run

Current configuration : 1811 bytes

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no ip domain lookup

!

username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

interface Loopback0

ip address 192.168.20.1 255.255.255.0

!

interface GigabitEthernet0/1

ip address 192.168.10.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

ip access-group 100 out

clock rate 128000

!

router eigrp 10

network 10.1.1.0 0.0.0.3

network 192.168.10.0

network 192.168.20.0

!

ip http server

ip http authentication local

no ip http secure-server

!

access-list 100 remark Allow Web & SSH Access

access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22

access-list 100 permit tcp any any eq www

access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255

!

line con 0

password cisco

logging synchronous

login

line vty 0 4

password cisco

logging synchronous

login

transport input all

!

end

Router ISP

ISP# sh run

Building configuration...

Current configuration : 1657 bytes

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname ISP

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no ip domain lookup

!

username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

interface Loopback0

ip address 209.165.200.225 255.255.255.224

!

interface Loopback1

ip address 209.165.201.1 255.255.255.224

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 128000

!

router eigrp 10

network 10.1.1.0 0.0.0.3

network 10.2.2.0 0.0.0.3

network 209.165.200.224 0.0.0.31

network 209.165.201.0 0.0.0.31

!

ip http server

ip http authentication local

no ip http secure-server

!

line con 0

password cisco

logging synchronous

login

line vty 0 4

password cisco

logging synchronous

login

transport input all

!

end

Router R3

R3# show run

Building configuration...

Current configuration : 1802 bytes

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no ip domain lookup

ip domain name cisco.com

!

username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

ip ssh version 1

!

interface Loopback0

ip address 192.168.40.1 255.255.255.0

!

interface GigabitEthernet0/1

ip address 192.168.30.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

ip access-group WEB-POLICY out

!

router eigrp 10

network 10.2.2.0 0.0.0.3

network 192.168.30.0

network 192.168.40.0

!

ip http server

ip http authentication local

no ip http secure-server

!

ip access-list extended WEB-POLICY

permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq www

permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq www

permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

!

line con 0

password cisco

logging synchronous

login

line vty 0 4

login local

transport input ssh

!

end

Switch S1

S1# sh run

Building configuration...

Current configuration : 1416 bytes

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.10.11 255.255.255.0

!

ip default-gateway 192.168.10.1

ip http server

ip http secure-server

line con 0

line vty 5 15

!

end

Switch S3

S3# show run

Building configuration...

Current configuration : 1416 bytes

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S3

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

interface Vlan1

ip address 192.168.30.11 255.255.255.0

!

ip default-gateway 192.168.30.1

ip http server

ip http secure-server

!

line con 0

line vty 5 15