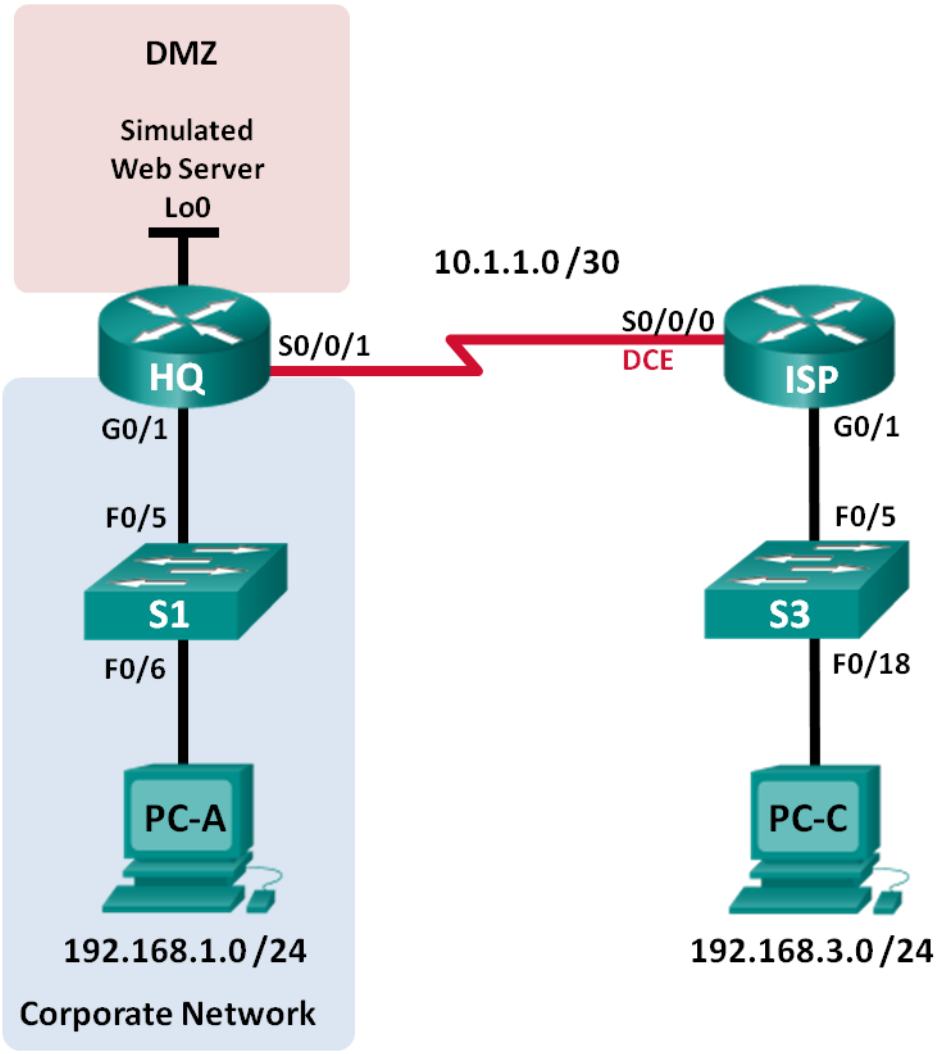
Ćwiczenie – Rozwiązywanie problemów z konfiguracją i miejscem ustawienia listy ACL w sieci

Topologia



Tablica adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
HQ	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
	S0/0/1	10.1.1.2	255.255.255.252	Nie dotyczy
	Lo0	192.168.4.1	255.255.255.0	Nie dotyczy
ISP	G0/1	192.168.3.1	255.255.255.0	Nie dotyczy
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Nie dotyczy
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	Karta sieciowa	192.168.3.3	255.255.255.0	192.168.3.1

Cele

Część 1: Budowa sieci i ustawienie podstawowej konfiguracji na urządzeniach

Część 2: Rozwiązywanie problemów z dostępem wewnętrznym

Część 3: Rozwiązywanie problemów z dostępem zdalnym

Scenariusz

Lista kontroli dostępu (ACL) jest serią poleceń IOS, które mogą zapewnić podstawowe filtrowanie ruchu na routerze Cisco. Listy ACL są używane do wyboru rodzaju ruchu, który ma być przetwarzany. Pojedynczy wpis w ACL jest nazywany wpisem kontroli dostępu (ACE). Wpisy w liście są wywoływane od góry do dołu z niejawną odmową na jej końcu. Krytyczne, przy prawidłowym przetwarzaniu ruchu jest rozmieszczenie list ACL w sieci.

Mała firma właśnie dodała serwer WWW w sieci, aby umożliwić klientom dostęp do informacji poufnych. Sieć firmowa podzielona jest na dwie strefy: strefę korporacyjną i strefę zdemilitaryzowaną (DMZ). Strefa sieci firmowej obejmuje serwery tylko do użytku wewnętrznego dostępne dla klientów wewnętrznych. DMZ obejmuje serwery dla dostępu publicznego (dla klientów zewnętrznych) (symulowane przez Lo0 na HQ). Ponieważ firma może administrować własnym routerem HQ, wszystkie listy kontroli dostępu ACL muszą być założone na routerze HQ.

- ACL 101 jest założona do ograniczenia ruchu wychodzącego na zewnątrz strefy korporacyjnej. Ta strefa obejmuje serwery prywatne (do użytku wewnętrznego) i klientów wewnętrznych. (192.168.1.0/24). Z żadnej innej sieci nie może być do niej dostępu.
- ACL 102 jest użyta do ograniczenia ruchu do sieci korporacyjnej. Tylko odpowiedzi na zapytania zainicjowane z wnętrza sieci korporacyjnej mogą do niej wracać. Obejmuje to ruch IP uług typu WWW i FTP. Ruch ICMP jest dozwolony do sieci w celu rozwiązywania problemów z łącznością. Tak więc ruch ICMP wygenerowany poleceniem ping powinien być odbierany przez wewnętrzne hosty.
- ACL 121 kontroluje zewnętrzny ruch do DMZ i sieci korporacyjnej. Tylko ruch HTTP jest dozwolony do serwera WWW w strefie DMZ (symulowany prze Lo0 na R1). Pozostały ruch w sieci jak EIGRP jest dopuszczony z sieci zewnętrznych. Ponadto, prawidłowe prywatne adresy wewnętrzne, takie jak 192.168.1.0, adres sprzężenia zwrotnego, Lo0 127.0.0.0 i adresy rozgłoszeniowe mają mieć zablokowane wejście do sieci korporacyjnej, aby zapobiec złośliwym atakom przez użytkowników sieci z zewnątrz.

Uwaga: Routery użyte do przygotowania instrukcji to Cisco 1941 IRS (Integrated Serwices Routers) z zainstalowanym systemem IOS wydanie 15.2(4)M3 (obraz universalk9). Przełączniki użyte do przygotowania instrukcji to Cisco Catalyst 2960 z obrazem systemu operacyjnego Cisco IOS wydanie

15.0(2) (lanbasek9). Do realizacji ćwiczenia mogą być użyte zarówno inne routery oraz przełączniki lub urządzenia z inną wersją systemu IOS. W zależności od użytego modelu urządzenia oraz wersji IOS dostępne komendy oraz komunikaty na ekranie mogą się różnić od tych zamieszczonych w instrukcji. Dostępne interfejsy na poszczególnych typach routerów zostały zebrane w tabeli na końcu niniejszej instrukcji laboratoryjnej.

Uwaga: Upewnij się, że przełączniki nie są skonfigurowane oraz nie przechowują pliku z konfiguracją startową. Jeśli nie jesteś tego pewien skontaktuj się z instruktorem.

Wymagane zasoby

- 3 routery (Cisco 1941 z Cisco IOS wydanie 15.2(4)M3, obraz „universal" lub kompatybilny)
- 2 przełączniki (Cisco 2960 z Cisco IOS wydanie 15.0(2) obraz „lanbasek9" lub kompatybilny)
- 2 komputery PC (Windows 7, Vista lub XP z zainstalowanym emulatorem terminala jak np.: Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy.
- Kable ethernetowe i serialowe jak pokazano na rysunku topologii sieci

Część 1: Budowa sieci i ustawienie podstawowej konfiguracji na urządzeniach

W części 1, masz zestawić topologię sieci i skonfigurować podstawowe ustawienia na routerach i przełącznikach, takie jak hasła i adresy IP. Wstępne ustawienia są dostarczone w instrukcji. W tej części musisz również skonfigurować komputery PC.

Krok 1: Zestawienie sieci zgodnie z topologią.

Krok 2: Skonfiguruj komputery PC .

Krok 3: Inicjuj i przeładuj routery i przełączniki jeśli to konieczne.

Krok 4: (Opcjonalnie) Skonfiguruj podstawowe ustawienia dla każdego przełącznika.

a. Wyłącz DNS lookup.
b. Skonfiguruj nazwę urządzeń jak pokazano to na schemacie.
c. Skonfiguruj adresy IP i bramę domyślna jak w tabeli adresacji
d. Przypisz **cisco** jako hasło do konsoli i vty.
e. Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
f. Skonfiguruj **logging synchronous** zarówno dla połączenia konsolowego jak i vty.

Krok 5: Skonfiguruj podstawowe ustawienia na każdym routerze.

a. Wyłącz DNS lookup.
b. Skonfiguruj nazwę urządzeń jak pokazano to na schemacie.
c. Przypisz **cisco** jako hasło do konsoli i vty.
d. Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
e. Skonfiguruj **logging synchronous** zarówno dla połączenia konsolowego jak i vty.

Krok 6: Skonfiguruj dostęp HTTP i poświadczenia użytkownika na HQ router.

Lokalne poświadczenia użytkownika są skonfigurowane do dostępu do symulowanego serwera WWW (192.168.4.1).

```
HQ(config)# ip http server
```

```
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Krok 7: Załaduj konfigurację routerów.

Konfiguracja dla routerów ISP i HQ jest zamieszczona poniżej. W konfiguracją są błędy. Twoim zadaniem jest określenie błędów w konfiguracji i ich korekcja.

Router ISP

```
hostname ISP
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
```

Router HQ

```
hostname HQ
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 out
 !ip access-group 101 in
 ip access-group 102 in
 !ip access-group 102 out
 no shutdown
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 ip access-group 121 in
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 network 192.168.4.0
 no auto-summary
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
!access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
!access-list 121 permit tcp any host 192.168.4.1 eq www
access-list 121 deny icmp any host 192.168.4.11
!access-list 121 deny icmp any host 192.168.4.1
```

```
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny ip 127.0.0.0 0.255.255.255 any
access-list 121 deny ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
end
```

Część 2: Rozwiązywanie problemów dla dostępu wewnętrznego

W części 2 testowane są listy ACL na routerze HQ w celu określenia, czy są one skonfigurowane poprawnie.

Krok 1: Rozwiąż problemy z ACL 101

ACL 101 jest zaimplementowana celem ograniczenia ruchu wychodzącego poza strefę korporacyjną. Ta strefa obejmuje tylko klientów wewnętrznych i serwery do użytku wewnętrznego. Tylko ruch z sieci 192.168.1.0/24 może opuścić strefę korporacyjną.

a. Czy ping z PC-A do swojej bramy domyślnej powiódł się? _____ Nie

b. Po weryfikacji, że PC-A został skonfigurowany poprawnie, sprawdź router HQ celem znalezienia błędów przez przeglądniecie podsumowania listy ACL 101. Wprowadź komendę **show access-lists 101**.

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```

c. Czy są jakieś problemy z ACL 101?

_____

Tak. ACL 101 przepuszcza ruch sieci 192.168.11.0 /24 zamiast 192.168.1.0 /24.

d. Sprawdź interfejs bramy domyślnej dla sieci 192.168.1.0 /24 network. Zweryfikuj, czy ACL 101 jest założona w poprawnym kierunku na interfejsie G0/1. Wprowadź komendę **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 102
```

Czy kierunek dla interfejsu G0/1 jest skonfigurowany poprawnie dla ACL 101?

_____

Nie. Dla ACL 101 kierunek powinien być in.

e. Popraw znalezione błędy dotyczące ACL 101 i sprawdź czy ruch z sieci 192.168.1.0 / 24 może opuścić sieć firmową. Zapisz polecenia użyte do skorygowania błędów.

_____

_____

_____

_____

_____

HQ(config)# **no access-list 101**
HQ(config)# **access-list 101 permit ip 192.168.1.0 0.0.0.255 any**
HQ(config)# **access-list 101 deny ip any any**
HQ(config)# **interface g0/1**
HQ(config-if)# **ip access-group 101 in**

f. Sprawdź czy ping z PC-A do interfejsu jego bramy domyślnej powiódł się.

Krok 2: Rozwiązywanie problemów z ACL 102

ACL 102 jest zaimplementowana w celu ograniczenia ruchu do sieci firmowej. Ruch pochodzący z zewnątrz sieci nie jest dopuszczony do sieci firmowej. Ruch zdalny jest dozwolony do sieci firmowej jeżeli został wywołany z sieci wewnętrznej. Komunikaty ICMP replay są dozwolone w celu rozwiązywania problemów.

a. Czy ping z PC-A do PC-C zakończył się sukcesem? _____Nie

b. Sprawdź router HQ, aby znaleźć ewentualne błędy konfiguracyjne przeglądając podsumowanie ACL 102. Wprowadź polecenie **show access-lists 102**.

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. Czy są jakieś problemy z ACL 102?_____ Nie

d. Upewnij się, że lista ACL 102 jest zastosowana w odpowiednim kierunku na interfejsie G0/1. Wprowadź polecenie **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 101
```

e. Czy są jakieś problemy z zastosowaniem listy ACL 102 na interfejsie G0/1?

_____

Tak. Skonfigurowana jest ACL101 w kierunku out, a powinna być 102.

f. Skoryguj błędy dotyczące listy ACL 102. Zapisz komendy użyte do poprawienia błędów.

_____

_____

HQ(config)# **interface g0/1**
HQ(config-if)# **ip access-group 102 out**

g. Czy ping z PC-A do PC-C powiódł się? _____ Tak

Część 3: Rozwiązywanie problemów ze zdalnym dostępem

W części 3, ACL 121 jest skonstruowana w celu zapobiegania atakom typu spoofing (podszywanie się pd inny element sieci lub systemu) z sieci zewnętrznych i dopuszczenie tylko dostępu HTTP do serwera WWW (192.168.4.1) w DMZ.

a. Zweryfikuj czy ACL 121 jest skonfigurowana poprawnie. Wprowadź komendę **show ip access-list 121**.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny ip 127.0.0.0 0.255.255.255 any
    50 deny ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

Czy są jakieś problemy z tą listą ACL?

_____

_____

Tak. Numer portu w linii 10 powinien być 80. Adres hosta dla serwera www w linii 20 powinien być 192.168.4.1

b. Zweryfikuj czy ACL 121 jest założona we właściwym kierunku na interfejsie R1 S0/0/1. Wprowadź komendę **show ip interface s0/0/1**.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
<output omitted>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

Czy są jakieś problemy z zastosowaniem tej listy?

_____

_____

Nie. Jest zastosowana na S0/0/1 w kierunku in.

c. Jeśli znaleziono jakieś błędy, wykonaj i zapisz konieczne zmiany w konfiguracji ACL 121.

_____

_____

_____

_____

_____

_____

_____

_____

HQ(config)# **no access-list 121**

HQ(config)# **access-list 121 permit tcp any host 192.168.4.1 eq 80**

HQ(config)# **access-list 121 deny icmp any host 192.168.4.1**
HQ(config)# **access-list 121 deny ip 192.168.1.0 0.0.0.255 any**
HQ(config)# **access-list 121 deny ip 127.0.0.0 0.255.255.255 any**
HQ(config)# **access-list 121 deny ip 224.0.0.0 31.255.255.255 any**
HQ(config)# **access-list 121 permit ip any any**
HQ(config)# **access-list 121 deny ip any any**

d. Upewnij się, że PC-C mają dostęp tylko do symulowanego serwera WWW na HQ za pomocą przeglądarki internetowej. Podaj nazwę użytkownika i hasło, aby dostać się do serwera WWW (192.168.4.1).

Do przemyślenia

1. W jakiej kolejności powinny być tworzone wpisy w liście ACL? Od ogólnych do szczegółowych czy odwrotnie?

_____

_____

Kolejność powinna być od szczegółowych do bardziej ogólnych ponieważ ACL jest wykonywana od góry do dołu w sekwencyjnej kolejności. Kiedy warunek jest spełniony przetwarzanie listy jest zatrzymywane i nie ma kolejnych porównań.

2. Jeśli skasujecie listę poprzez użycie komendy **no access-list**, a ACL jest wciąż zastosowana na interfejsie, to co się stanie?

_____

_____

Domyślny wpis deny any nadal działa. Dlatego należy być ostrożnym podczas usuwania list, które są zastosowane na działających interfejsach.

Tabela –podsumowanie interfejsów routera

Podsumowanie interfejsów routera				
Model routera	**Interfejs ethernetowy #1**	**Interfejs ethernetowy #2**	**Interfejs szeregowy #1**	**Interfejs szeregowy #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)
Uwaga: Aby dowiedzieć się, jaka jest konfiguracja sprzętowa routera, obejrzyj interfejsy, aby zidentyfikować typ routera oraz aby określić liczbę interfejsów routera. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Tabela ta zawiera identyfikatory możliwych kombinacji interfejsów szeregowych i Ethernet w urządzeniu. Tabela nie zawiera żadnych innych rodzajów interfejsów, mimo iż dany router może jakieś zawierać Przykładem może być interfejs ISDN BRI. Łańcuch w nawiasie jest skrótem, który może być stosowany w systemie operacyjnym Cisco IOS przy odwoływaniu się do interfejsu..				

Konfiguracje urządzeń

Router ISP

```
ISP#show run
Building configuration...
```

```
Current configuration : 1423 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
```

```
!
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
!
ip forward-protocol nd
!
no ip http server

no ip http secure-server
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router HQ (Poprawiona)

```
HQ# show run
Building configuration...

Current configuration : 2292 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
```

```
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
!
!
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
!shutdown
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 ip access-group 121 in
!
interface Serial0/0/1
 no ip address
!shutdown
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
```

```
 network 192.168.1.0
 network 192.168.4.0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 deny   ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny   ip any any
access-list 121 permit tcp any host 192.168.4.1 eq www
access-list 121 deny   icmp any host 192.168.4.1
access-list 121 deny   ip 192.168.1.0 0.0.0.255
access-list 121 deny   ip 127.0.0.0 0.255.255.255
access-list 121 deny   ip 224.0.0.0 31.255.255.255
access-list 121 permit ip any any
access-list 121 deny   ip any any
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```