Laborator - Configurarea și Verificarea ACL-urilor extinse

Topologie

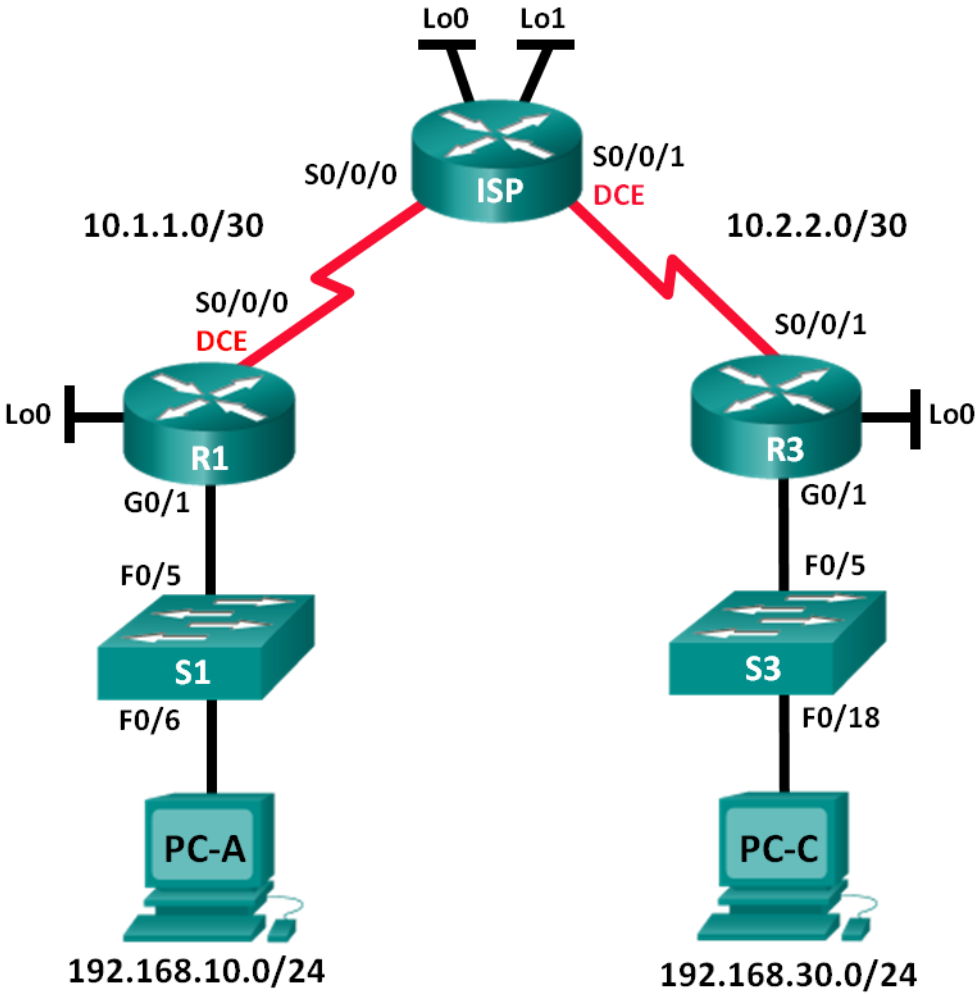

Tabela de Adresare

Echipament	Interfață	Adresă IP	Masca de subreţea	Default Gateway
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

Obiective

Partea 1: Configurați Topologia și Inițializați Dispozitivele

Partea 2: Configurați Echipamentele și Verificați Conectivitatea

- Configurați setările de bază pe calculatoare, routere și switchuri.
- Configurați rutarea EIGRP pe R1, ISP și R3.

Partea 3: Configurați și Verificați ACL-urile Denumite și Numerotate Extinse

- Configurați, aplicați și verificați un ACL numerotat extins.
- Partea 1 : Configurați , Aplicați și Verificați un ACL Extins Denumit

Partea 4: Modificați și Verificați ACL-urile Extinse

Context/Scenariu

ACL-urile extinse sunt extrem de puternice. Oferă un grad de control mai mare în comparație cu ACL-urile standard precum și mai multe tipuri de trafic ce pot fi filtrate și control asupra orginii și destinației traficului.

În acest laborator, veți configura reguli de filtrare pentru două birouri reprezentate de R1 și R3. Managementul a stabilit câteva politici de acces între LAN-urile localizate pe R1 și R3, pe care dumneavoastră trebuie să le implementați. Routerul ISP dintre R1 și R3 nu are ACL-uri plasate pe el. Nu vi se va permite accesul administrativ la un router ISP deoarece puteți controla și gestiona doar echipamentul propriu.

Notă: Router-ele folosite la laboratoarele practice de CCNA sunt: Cisco 1941 Integrated Services Routers (ISR-uri)și Cisco IOS Release 15.2(4)M3 (universalk9 image). Switch-urile folosite sunt Cisco Catalyst 2960

cu Cisco IOS Release 15.0(2) (lanbasek9 image). Pot fi folosite și alte routere, switchuri și versiuni IOS. În funcție de model și de versiunea Cisco IOS, comenzile disponibile și rezultatele produse pot fi diferite față de cele arătate la laboratoare. Pentru a vizualiza identificatorii corecți ai interfeței, puteți consulta Tabelul cu Interfețele Routerelor de la sfârșitul laboratorului.

Notă: Asigurați-vă că routerele și switchurile au fost șterse și că nu au configurații de pornire. Dacă nu sunteți sigur, contactați-vă instructorul.

Resurse necesare

- 3 Routere (Cisco 1941 cu Cisco IOS Release 15.2(4)M3 imagine universală sau comparabilă)
- 2 Switchuri (Cisco 2960 cu Cisco IOS Release 15.0(2) imagine lanbasek9 sau comparabilă)
- 2 Calculatoare (Windows 7, Vista sau XP cu program de emulare a terminalului, cum ar fi Tera Term)
- Cabluri de consolă pentru a configura echipamentele Cisco IOS prin intermediul porturilor de consolă
- Cabluri seriale și Ethernet așa cum se arată în topologie

Part 1: Configurați Topologia și Inițializați Dispozitivele

În partea 1, veți configura topologia rețelei și veți elimina orice configurații dacă este necesar.

Step 1: Cablați rețeaua așa cum se arată în topologie.

Step 2: Inițializați și reîncărcați routerele și switchurile.

Part 2: Configurați Echipamentele și Verificați Conectivitatea

În Partea 2, veți configura setări de bază pe switchuri, routere și calculatoare. Pentru numele dispozitivelor și informații despre adrese, faceți referire la Topologie și la Tabela de Adresare.

Step 1: Configurați adresele IP pe PC-A și PC-C.

Step 2: Configurarți setările de bază pe R1.

a. Dezactivați DNS lookup.

b. Configurați numele echipamentului așa cum se arată în topologie.

c. Creați o interfață loopback pe R1.

d. Configurați adresele IP ale interfeței așa cum se arată în Topologia și Tabela de Adresare.

e. Configurați class ca parolă pentru modul EXEC privilegiat.

f. Alocați o frecvență de ceas de **128000** la interfața S0/0/0.

g. Folosiți **cisco** pentru parola vty și de consolă și activați accesul prin Telnet. Configurați **synchronous logging** pentru liniile de consolă și vty.

h. Activați accesul web la R1 pentru a simula un server de web cu o autentificare locală pentru utilizatorul admin.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Step 3: Configurați setările de bază pe ISP.

a. Configurați numele echipamentului așa cum se arată în topologie.

b. Creați interfețele de loopback pe ISP.

c. Configurați adresele IP ale interfeței așa cum se arată în Topologia și Tabela de Adresare.

d. Dezactivați DNS lookup.

e. Folosiți **class** ca parolă pentru modul EXEC privilegiat.

f. Folosiți o frecvență a ceasului **de** 128000 la interfața S0/0/1.

g. Folosiți **cisco** pentru parola vty și de consolă și activați accesul prin Telnet. Configurați **synchronous logging** pentru liniile de consolă și vty.

h. Permiteți accesul web la ISP. Folosiți aceiași parametri ca și la Pasul 2h.

Step 4: Configurați setările de bază pe R3.

a. Configurați numele echipamentului așa cum se arată în topologie.

b. Creați o interfață de loopback pe R3.

c. Configurați adresele IP ale interfeței așa cum se arată în Topologia și Tabela de Adresare.

d. Dezactivați DNS lookup.

e. Folosiți **class** ca parolă pentru modul EXEC privilegiat.

f. Alocați **cisco** ca parolă de consolă și configurați **logging synchronous** pe linia de consolă.

g. Activați SSH pe 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
```

h. Permite accesul web pe R3. Folosiți aceiași parametri ca și la Pasul 2h.

Step 5: (Opțional) Configurați setările de bază pe S1 și S3.

a. Configurați hostname-urile așa cum se arată în topologie.

b. Configurați adresele IP ale interfeței de management așa cum se arată în Tabela de Adresare și în Topologie.

c. Dezactivați DNS lookup.

d. Configurați class ca parolă pentru modul EXEC privilegiat.

e. Configurați adresa gateway-ului default.

Step 6: Configurați rutarea EIGRP pe R1, ISP și R3.

a. Configurați numărul AS 10 (autonomous system) și anunțați toate rețelele pe R1, ISP și R3. Dezactivați sumarizarea automată.

b. După configurarea EIGRP pe R1, ISP și R3, verificați dacă toate routerele au tabelele de rutare complet care afișează toate rețelele. Depanați dacă acesta nu este cazul.

Step 7: Verificați conectivitatea dintre echipamente.

Notă: Este foarte important să verificați conectivitatea înainte **să** configurați și să aplicați ACL-uri! Asigurați-vă că rețeaua dumneavoastră funcționează corect înainte să începeți filtrarea traficului.

a. Din PC-A, dați ping la PC-C și la interfețele seriale și de loopback de pe R3.

Comenzile ping s-au realizat cu succes? _____

b. Din R1, dați ping PC-C și la interfața serială și de loopback pe R3.

Comenzile ping s-au realizat cu succes? _____

c. Din R1, dați ping PC-A și la interfața de loopback și serială pe R1.

Comenzile ping s-au realizat cu succes? _____

d. Din R3, dați ping la PC-A și la interfața de loopback și serială de pe R1.

Comenzile ping s-au realizat cu succes? _____

e. Din PC-A, dați ping la interfețele de loopback pe routerul ISP.

Comenzile ping s-au realizat cu succes? _____

f. Din PC-C, dați ping la interfețele de loopback pe routerul ISP.

Comenzile ping s-au realizat cu succes? _____

g. Deschideți un navigator web pe PC-A și mergeți la http://209.165.200.225 pe ISP. Vi se va cere un nume de utilizator și o parolă. Folosiți **admin** ca nume de utilizator **și** class pentru parolă. Dacă vi se cere să acceptați o semnătură, acceptați-o. Routerul va încărca Cisco Configuration Professional (CCP) Express într-o fereastră separată. Este posibil să vi se ceară un nume de utilizator și o parolă. Folosiți **admin** ca nume de utilizator și **class** pentru parolă.

h. Deschideți un navigator web pe PC-C și accesați http://10.1.1.1 pe R1. Vi se va cere un nume de utilizator și o parolă. Folosiți **admin** pentru numele de utilizator și **class** pentru parolă. Dacă vi se cere să acceptați o semnătură, acceptați-o. Routerul va încărca CCP Express într-o fereastră separată. Este posibil să vi se ceară un nume de utilizator și o parolă. Folosiți **admin** ca nume de utilizator și **class** pentru parolă.

Part 3: Configurați și Verificați ACL-urile Denumite și Numerotate Extinse.

ACL-urile extinse pot filtra traficul în mai multe moduri. ACL-urile extinse pot filtra adrese IP sursă, porturi sursă, adrese IP de destinație, porturi de destinație, precum și diferite protocoale și servicii.

Politicile de securitate sunt următoarele:

1. Permit traficul web care provine din rețeaua 192.168.10.0/24 să meargă către orice rețea.
2. Permit o conexiune SSH la interfața serială R3 de pe PC-A.
3. Permit utilizatorilor din rețeaua 192.168.10.0.24 să acceseze rețeaua 192.168.20.0/24.
4. Permite traficului de web care provine din rețeaua 192.168.30.0/24 să acceseze R1 prin interfața web și rețeaua 209.165.200.224/27 de pe ISP. Rețeaua 192.168.30.0/24 nu ar trebui să poată accesa nici o altă rețea prin web.

Consultând politicile de securitate de mai sus, veți avea nevoie de minim două ACL-uri pentru a îndeplini politicile de securitate. O practică utilă este să plasați ACL-urile extinse cât mai aproape de sursă posibil. Vom urma această practică pentru aceste politici.

Step 1: Configurați un ACL extins numerotat pe R1 pentru politicile de securitate 1 și 2.

Veți utiliza un ACL extins numerotat pe R1. Care sunt intervalele pentru ACL-urile extinse?

_____

a. Configurați ACL-ul pe R1. Folosiți 100 pentru numărul 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
```

Ce simbolizează 80 în outputul de comandă de mai sus?

_____

La ce interfață ar trebui aplicat ACL 100?

_____

_____

În ce direcție ar trebui aplicat ACL 100?

_____

_____

b. Aplicați ACL 100 la interfața S0/0/0.

```
R1(config)# int s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Verificați ACL 100.

1) Deschideți un browser web pe PC-A și accesați http://209.165.200.225 (routerul ISP). Ar trebui să se realizeze cu succes; depanați, dacă este cazul.

2) Stabiliți o conexiune SSH de la PC-A la R3 folosind 10.2.2.1 pentru adresa IP. Autentificați-vă folosind credențialele **admin** și **class**. Ar trebui să se realizeze cu succes; depanați, dacă este cazul.

3) Din prompt-ul modului EXEC privilegiat de pe R1, lansați comanda **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)
```

4) Din prompt-ul de comandă PC-A, lansați un ping la 10.2.2.1. Explicați-vă rezultatele.

_____

_____

_____

Step 2: Configurați un ACL extins denumit pe R3 pentru politica de securitate cu numărul 3.

a. Configurați politica pe R3. Denumiți ACL-ul WEB-POLICY.

```
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
```

b. Aplicați ACL-ul WEB-POLICY la interfața S0/0/1.

```
R3(config-ext-nacl)# int S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. Verificați ACL-ul WEB-POLICY.

1) Din prompt-ul de comandă al modului EXEC privilegiat de pe R3**, lansați comanda show ip interface** s0/0/1.

Care este numele ACL-ului, dacă ACL-ul există? _____
WEB-POLICY

În ce direcție este aplicat ACL-ul? _____Spre exterior

2) Deschideți un navigator web pe PC-C și accesați http://209.165.200.225 (routerul ISP). Ar trebui să se realizeze cu succes; depanați, dacă este cazul.

3) Din PC-C, deschideți o sesiune web la http://10.1.1.1 (R1). Ar trebui să se realizeze cu succes; depanați, dacă este cazul.

4) Din PC-C, deschideți o sesiune web la http://209.165.201.1 (routerul ISP). Ar trebui să eșueze; altfel, depanați.

5) Din prompt-ul de comandă al lui PC-C, dați ping la PC-A. Care a fost rezultatul și de ce?

_____

Part 4: Modificați și Verificați ACL-urile Extinse

Din cauza ACL-urilor aplicate pe R1 și R3, nu sunt permise ping-urile sau un alt tip de trafic între rețelele LAN de pe R1 și R3. Managementul a decis că tot traficul între rețelele 192.168.10.0/24 și 192.168.30.0/24 ar trebui să fie permis. Trebuie să modificați ambele ACL-uri pe R1 și R3.

Step 1: Modificați ACL 100 pe R1.

a. Din modul EXEC privilegiat al lui R1, lansați comanda **show access-lists.**

Câte linii sunt în această listă de acces? _____

b. Intrați în modul de configurare global și modificați ACL-ul pe 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
```

c. Lansați comanda **show access-lists**.

Un apare noua linie pe care ați adăugat-o în ACL 100?

_____

Step 2: Modificați ACL-ul WEB-POLICY pe R3.

a. Din modul EXEC privilegiat al lui R3, lansați comanda **show access-lists.**

Câte linii suntîn această listă de acces? _____ Intrați în modul de configurare global și modificați ACL-ul pe 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
```

b. Lansați comanda **show access-lists** pentru a verifica dacă noua linie a fost adăugată la finalul ACL-ului.

Step 3: Verificați ACL-uri modificate.

a. Din PC-A, dați ping la adresa IP a lui PC-C. Comenzile ping s-au realizat? _____

b. Din PC-C, dați ping la adresa IP a lui PC-A. Comenzile ping s-au realizat cu succes? _____ De ce ACL-urile au funcționat imediat pentru ping-uri după ce le-ați modificat?

_____

Reflecție

1. De ce este nevoie de planificarea și testarea atentă a ACL-urilor?

_____

_____

2. Ce tip de ACL este mai bun: standard sau extins?

_____

_____

_____

_____

3. De ce pachetele hello EIGRP și actualizările de rutare nu sunt blocate de **ACE implicit** deny any sau intrarea ACL a ACL-urilor aplicate la R1 și R3?

_____

_____

_____

_____

Tabela Interfețelor Routerului

Rezumatul Interfețelor Routerului				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #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)

Notă: Pentru a afla cum este configurat routerul, uitați-vă la interfețe pentru a identifica tipul routerului și câte interfețe are routerul. Nu există o listă efectivă cu toate combinațiile configurărilor pentru fiecare clasă de routere. Acest tabel include identificatorii pentru combinațiile posibile de interfețe Seriale și Ethernet din dispozitiv. Tabelul nu include nici un alt tip de interfață, chiar dacă un anumit router poate. Un astfel de exemplu poate fi interfața ISND BRI. Denumirea din paranteză este prescurtarea legală care poate fi folosită în comenzile Cisco IOS pentru a reprezenta interfața.