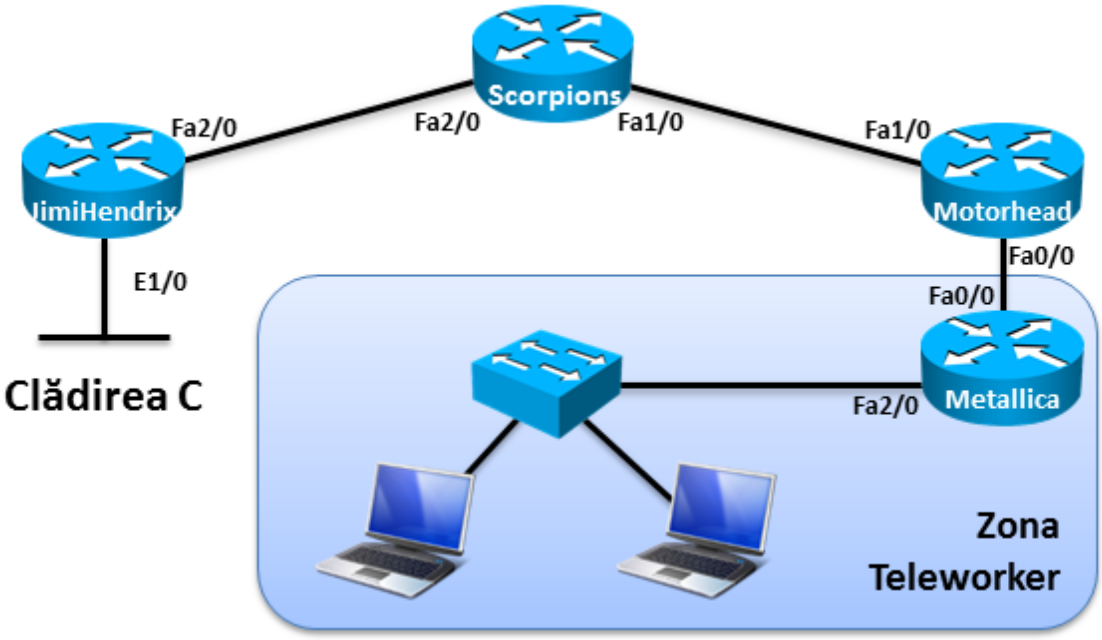
Laborator ACL

1 Motivație

Fiind în continuă creștere a numărului de angajați, compania noastră se vede în situația de a angaja lucrători la distanță pentru departamentele de Marketing și Finanțe (clădirea C). Acest lucru ridică însă o serie de probleme, fiind necesară construcția unei infrastructuri care să impună o serie de reguli de filtrare pentru accesul la resurse al lucrătorilor la distanță.

2 Topologie



3 Cerințe

Rezolvarea următoarelor taskuri va asigura configurarea corectă a echipamentelor pentru a permite accesul lucrătorilor la distanță și implementarea regulilor de filtrare a traficului.

Atenție: Ruterul Scorpions **nu se află sub autoritatea Dvs.**, deci nu îl veți configura. El este deja configurat cu toate rutele necesare.

1. [10p] Asigurați conectivitatea end-to-end pentru întreaga rețea, folosind un număr minim de rute statice.

```
JimiHendrix(config)#ip route 0.0.0.0 0.0.0.0 66.218.168.6
Motorhead(config)#ip route 0.0.0.0 0.0.0.0 191.105.157.1
Motorhead(config)#ip route 192.168.254.0 255.255.255.0 172.29.167.2
Metallica(config)#ip route 0.0.0.0 0.0.0.0  172.29.167.1
```

2. [10p] Pe ruterul JimiHendrix există definit Loopback 0 pe care trebuie să îl aceseze doar angajații din zona Teleworker. Filtrați restul traficului către această interfață.
   - Pentru acest task, permiteți, pe lângă traficul originat din zona Teleworker și traficul originat de pe ruterul Metallica
   - ***Atenție:*** Restul traficului către ruterul JimiHendrix trebuie să funcționeze în continuare!

```
Motorhead#ping 155.17.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.17.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/60/148 ms
```

```
JimiHendrix(config)# ip access-list extended ONLY_TELEWORKER_TO_LOOPBACK
JimiHendrix(config-ext-nacl)# permit ip 192.168.254.0 0.0.0.255 host
155.17.23.1
JimiHendrix(config-ext-nacl)# permit ip host 172.29.167.2 host 155.17.23.1
JimiHendrix(config-ext-nacl)# deny ip any host 155.17.23.1
JimiHendrix(config-ext-nacl)# permit ip any any
JimiHendrix(config)# int fa2/0
JimiHendrix(config-if)# ip access-group ONLY_TELEWORKER_TO_LOOPBACK in
```

```
Metallica(config)#do ping 155.17.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.17.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/78/140 ms
Metallica(config)#do ping 155.17.23.1 source Lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.17.23.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.254.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/79/136 ms
Motorhead#ping 155.17.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.17.23.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

3. [15p] Lucrătorii din zona Teleworker nu au dreptul de a accesa o serie de site-uri web:
   - 208.69.127.83
   - 77.73.36.99
   - 74.125.39.0/24

   Filtrați accesul HTTP la aceste IP-uri.
   Observație: Acest task POATE fi testat. Încercați ☺

```
Metallica(config)#do telnet 208.69.127.83 80
Trying 208.69.127.83, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Fri, 01 Mar 2002 00:22:05 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 208.69.127.83 closed by foreign host]
Metallica(config)#do telnet 77.73.36.99 80
Trying 77.73.36.99, 80 ... Open
[...]
[Connection to 77.73.36.99 closed by foreign host]
Metallica(config)#do telnet 74.125.39.1 80
Trying 74.125.39.1, 80 ... Open
[...]
[Connection to 74.125.39.1 closed by foreign host]
```

```
Motorhead(config)#ip access-list extended NO_HTTP_TELEWORKER
Motorhead(config-ext-nacl)# deny tcp any host 208.69.127.83 eq www
Motorhead(config-ext-nacl)# deny tcp any host 77.73.36.99 eq www
Motorhead(config-ext-nacl)# deny tcp any 74.125.39.0 0.0.0.255 eq www
Motorhead(config-ext-nacl)# permit ip any any
Motorhead(config)#int fa0/0
Motorhead(config-if)#ip access-group NO_HTTP_TELEWORKER in
```

```
Metallica(config)#do telnet 208.69.127.83 80
Trying 208.69.127.83, 80 ...
% Destination unreachable; gateway or host down

Metallica(config)#do telnet 77.73.36.99 80
Trying 77.73.36.99, 80 ...
% Destination unreachable; gateway or host down

Metallica(config)#do telnet 74.125.39.1 80
Trying 74.125.39.1, 80 ...
% Destination unreachable; gateway or host down
```

4. [15p] Permiteți accesul Telnet generat din zona Teleworker către Motörhead, doar pe interfața Loopback 0 a acestuia.
   - Asigurați-vă mai întâi că Motörhead acceptă conexiuni de tip Telnet.
   - ***Observația:*** Lista de access creată nu trebuie să afecteze funcționalitatea niciunui task anterior!

```
Motorhead(config)# line vty 0 4
Motorhead(config-line)# password aceofspades
Motorhead(config-line)# login
Motorhead(config-line)# transport input telnet
Motorhead(config)# ip access-list ext NO_HTTP_TELEWORKER
Motorhead(config-ext-nacl)#33 permit tcp any host 20.20.20.20 eq telnet
Motorhead(config-ext-nacl)#34 deny tcp any host 172.29.167.1 eq telnet
Motorhead(config-ext-nacl)#35 deny tcp any host 191.105.157.2 eq telnet
```

```
Metallica(config)#do telnet 20.20.20.20 /source Lo0
Trying 20.20.20.20 ... Open


User Access Verification

Password:
```

```
Motorhead>exit

[Connection to 20.20.20.20 closed by foreign host]
Metallica(config)#do telnet 172.29.167.1 /source Lo0
Trying 172.29.167.1 ...
% Destination unreachable; gateway or host down

Metallica(config)#do telnet 191.105.157.2 /source Lo0
Trying 191.105.157.2 ...
% Destination unreachable; gateway or host down
```

5. [10p] Datorită riscurilor de securitate, s-a luat decizia ca niciun server al companiei să nu se afle în clădirea C. De aceea, se poate implementa o regulă ce specifică blocarea tuturor pachetelor cu destinația clădirea C ce inițiază o conexiune TCP nouă.
   - ***Observație:*** Pentru a putea testa acest task, cât și următorul, trebuie să porniți ruterul GunsNRoses, însă **NU** trebuie să lucrați pe acesta. După rezolvarea acestora, puteți închide acest ruter.

```
JimiHendrix(config)# ip access-list ext NO_TCP_C
JimiHendrix(config-ext-nacl)# 10 permit tcp any any established
JimiHendrix(config-ext-nacl)# 20 deny tcp any any
JimiHendrix(config)# int e1/0
JimiHendrix(config-if)# ip access-group NO_TCP_C out
```

```
GunsNRoses# telnet 20.20.20.20
Trying 20.20.20.20 ... Open


User Access Verification

Password:
Motorhead>
Motorhead(config-ext-nacl)#do telnet 192.168.231.2
Trying 192.168.231.2 ...
% Destination unreachable; gateway or host down
JimiHendrix(config)#do sh access-l
Extended IP access list NO_TCP_C
    10 permit tcp any any established
    20 deny tcp any any (1 match)
```

6. [20p] Permiteți traficul ICMP de la Clădirea C către zona Teleworker doar dacă acesta este un răspuns la o cerere inițiată din această zonă. Restul traficului ICMP de la JimiHendrix către zona Teleworker trebuie să fie permis, de asemenea.
   - *Hint:* Aplicați o listă de acces reflexivă pe ruterul Motörhead.

```
   Motorhead(config)#do sh ip access ICMP_TO_JH
   Extended IP access list ICMP_TO_JH
       10 permit icmp 172.29.167.0 0.0.0.255 192.168.231.0 0.0.0.255
reflect ICMP1 (11 matches)
       20 permit icmp 192.168.254.0 0.0.0.255 192.168.231.0 0.0.0.255
reflect ICMP2
       30 permit ip any any (15 matches)

   Motorhead(config)#do sh ip access ICMP_FROM_JH
   Extended IP access list ICMP_FROM_JH
       10 evaluate ICMP1
       20 evaluate ICMP2
       30 permit icmp host 66.218.168.5 172.29.167.0 0.0.0.255 (10
matches)
       40 permit icmp host 155.17.23.1 172.29.167.0 0.0.0.255
       50 permit icmp host 172.2.0.1 172.29.167.0 0.0.0.255
       60 permit icmp host 10.10.10.17 172.29.167.0 0.0.0.255
       70 permit icmp host 10.10.10.33 172.29.167.0 0.0.0.255
```

```
        80 permit icmp host 66.218.168.5 192.168.254.0 0.0.0.255 (5
matches)
        90 permit icmp host 155.17.23.1 192.168.254.0 0.0.0.255
        100 permit icmp host 172.2.0.1 192.168.254.0 0.0.0.255
        110 permit icmp host 10.10.10.17 192.168.254.0 0.0.0.255
        120 permit icmp host 10.10.10.33 192.168.254.0 0.0.0.255
```

```
Motorhead(config)#int fa1/0
Motorhead(config-if)#ip access-group ICMP_TO_JH out
Motorhead(config-if)#ip access-group ICMP_FROM_JH in
```

7. [20p] Vrem ca zona Teleworker să poată accesa restul rețelei doar în zilele lucrătoare ale unei săptămâni (Luni - Vineri, în intervalul 9:00 – 18:00). Faceți configurațiile necesare pentru a permite accesul în intervalul respectiv, interzicând complet accesul zonei Teleworker la restul rețelei în afara intervalului specificat.
   - ***Observația*:** Lista de access creată nu trebuie să afecteze funcționalitatea niciunui task anterior!
   - *Hint:* Aplicați lista de acces creată pe ruterul Motörhead, folosind o interfață şi o direcție încă nefolosite.
   - Testați funcționarea acestui task schimbând ceasul pe ruterul pe care ați aplicat lista de acces prin comanda:

```
Router# clock set 01:00:00 Dec 1 2013
```

```
Motorhead(config)#time-range TELEWORKER_TIME
Motorhead(config-time-range)#periodic weekdays 09:00 to 18:00
Motorhead(config)#ip access-list extended TELEWORKER_ACCESS
Motorhead(config-ext-nacl)#permit ip any any time-range TELEWORKER_TIME
Motorhead(config-ext-nacl)#int fa0/0
Motorhead(config-if)#ip access-group TELEWORKER_ACCESS out
```