NetLab
10

Firewall sistemi i Cisco Access liste (ACL)

Cilj vežbe

Cilj ove vežbe je upoznavanje sa osnovnim konceptima firewall sistema, access listama (ACL) i filtriranjem mrežnih paketa.

Filtriranje mrežnog saobraćaja i filtriranje paketa predstavljaju jednu od osnovnih funkcija firewall sistema (mrežni zid/mrežna barijera). Firewall sistemi predstavljaju osnovni vid zaštite računarskih mreža i sistema.

U ovoj vežbi je opisano kako se mogu koristi Cisco IP access control liste (ACLs) za filtriranje mrežnog saobraćaja. Vežba takođe sadrži i kratak opis osnovnih tipova access lista. Za sličan oblik zaštite na Linux sistemima koristi se iptables.

Napomena: Za filtriranje paketa potrebno je znati i dodeljene brojeve portova za mrežne servise. Ti brojevi se nalaze u dokumentu RFC 1700. Dokument RFC 1918 sadrži informacije o privatnim IP adresama. Predznanje i iskustvo iz sličnih vežbi na Linux OS-u i sa paketom iptables je takođe poželjno.

Tipovi access lista

Standardne ACL

Standardne ACL su najstariji tip lista. Datiraju još od verzije Cisco IOS Software Release 8.3. Standardne access liste kontrolišu saobraćaj na osnovu poređenja adrese izvorišta IP paketa sa adresama konfigurisnaim u access listama. Sintaksa naredbe standardnih ACL je data u nastavku:

```
access-list access-list-number {permit|deny}
{host|source source-wildcard|any}
```

U svim verzijama Cisco IOS softvera brojevi rezervisani za standardne access liste su od 1 do 99. U verzijama od Cisco IOS Software Release 12.0.1, standardne ACL koriste i dodatne brojeve (1300 to 1999).

Kada se za source/source–wildcard koristi 0.0.0.0/255.255.255.255 to se može specificirati kao any. Wildcard se može izostaviti ako su u pitanju sve nule. Tako za host 10.1.1.2 0.0.0.0, se može navesti samo host 10.1.1.2. Kada se ACL definišu potrebno je primeniti ih na određenom interfejsu (inbound ili outbound). U ranijim verzijama Cisco IOS softvera out je bila podrazumevana (default) vrednost, ako se ovaj parametar izostavi. U novijim verzijama softvera ovaj parametar se mora navesti, tj. ne sme se izostaviti. Inbound se koristi za dolazni saobraćaj, a outbound se koristi za odlazni saobraćaj.

```
interface <interface>
ip access-group number {in|out}
```

Primer upotrebe standardne ACL da bi se blokirao sav saobraćaj osim sa mreže 10.1.1.x.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
access-list 1 permit 10.1.1.0 0.0.0.255
```

Extended ACL

Extended ACL liste su podržane od verzije Cisco IOS Software Release 8.3. Ovaj tip se koristi za kontrolisanje saobraćaja poređenjem izvorišne i odredišne adrese IP paketa sa adresama konfigurisanim u listama. Sintaksa naredbe je sledeća (naredba je prikazana u više redova zbog veće pregeldnosti, na sistemu se unosi u jednom redu):

IP

```
access-list access-list-number
[dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence]
[tos tos] [log | log-input] [time-range time-range-name]
```

ICMP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard
destination destination-wildcard
[icmp-type | [[icmp-type icmp-code] | [icmp-message]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]
```

TCP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]
```

UDP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]
```

U svim verzijama softvera brojevi za access–liste su u rasponu od 101 do 199. Od Cisco IOS Software Release 12.0.1, extended ACL mogu da koriste i brojeve od 2000 do 2699.

Vrednost 0.0.0.0/255.255.255.255 i u ovom slučaju se može zameniti sa any. Posle definisanja access liste potrebno je da se ona primeni na interfejsu kao inbound ili outbound (dolazna ili odlazna).

```
interface <interface>
ip access-group {number|name} {in|out}
```

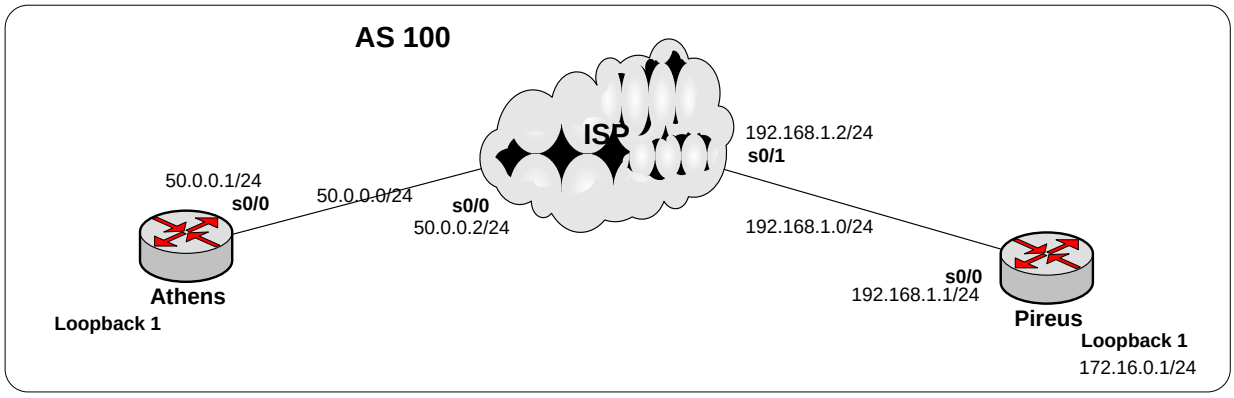
Sledeći set naredbi se koristi da bi se dozvolio saobraćaj na mrežu 10.1.1.x i da bi se zabranio ping saobraćaj spolja:

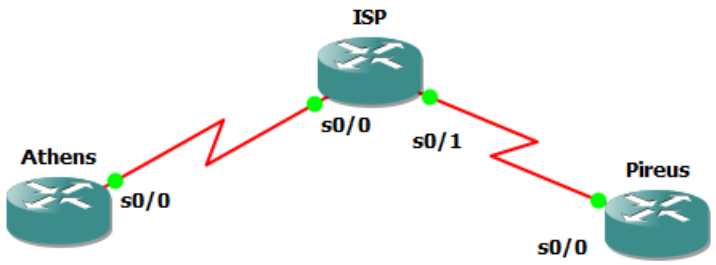
```
interface Ethernet0/1
ip address 172.16.1.2 255.255.255.0
ip access-group 101 in
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 101 permit ip any 10.1.1.0 0.0.0.255
```

U nekim slučajevima, kao što je upravljanje mrežom, potrebno je omogućiti ping zbog keepalive funkcije. U tom slučaju, moguće je limitirano blokirati dolazni ping ili biti detaljniji u specificiranju adresa sa kojih je saobraćaj dozvoljen ili zabranjen.

1. Konfiguracija osnovne funkcionalne mreže i EIGRP protokola

Za potrebe vežbe potrebno je kreirati mrežni scenario kao na slici. Za osnovno konfigurisanje rutera izvršiti na primeru iz prethodne vežbe. Za rutiranje koristi RIP protokol, kao u prethodnoj vežbi.





Korak 1.1

Osnovna konfiguracija OSPF protokola vrši se sledećim komandama:

Potrebno je iskonfigurisati ruter Athens, sledećim komandama:

```
Athens#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Athens(config)#no logging console
Athens(config)#interface s0/0
Athens(config-if)#ip address 50.0.0.1 255.255.255.0
Athens(config-if)#no shutdown
Athens(config-if)#interface loop 1
Athens(config-if)#ip address 10.1.1.1 255.255.255.0
Athens(config-if)#router ospf 1
Athens(config-router)#router-id 50.0.0.1
Athens(config-router)#network 50.0.0.0 0.0.0.255 area 0
Athens(config-router)#network 10.1.1.0 0.0.0.255 area 0
Athens(config-router)#exit
Athens(config)#exit
Athens#
Athens#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Athens#
```

Korak 1.2.

Zatim je potrebno iskonfigurisati ruter ISP.

```
ISP#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#no logging console
ISP(config)#interface s0/0
ISP(config-if)#ip address 50.0.0.2 255.255.255.0
ISP(config-if)#no shutdown
ISP(config)#interface s0/1
ISP(config-if)#ip address 192.168.1.2 255.255.255.0
ISP(config-if)#no shutdown
ISP(config-if)#router ospf 1
ISP(config-router)#router-id 50.0.0.2
ISP(config-router)#network 50.0.0.0 0.0.0.255 area 0
ISP(config-router)#network 192.168.1.0 0.0.0.255 area 0
ISP(config-router)#exit
ISP(config)#exit
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

Korak 1.3.

I na kraju ruter Pireus:

```
Pireus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pireus(config)#no logging console
Pireus(config)#interface s0/0
Pireus(config-if)#ip address 192.168.1.1 255.255.255.0
Pireus(config-if)#no shutdown
Pireus(config-if)#interface loop 1
Pireus(config-if)#ip address 172.16.0.1 255.255.255.0
Pireus(config-if)#router ospf 1
Pireus(config-router)#router-id 192.168.1.1
Pireus(config-router)#network 192.168.1.0 0.0.0.255 area 0
Pireus(config-router)#network 172.16.0.0 0.0.0.255 area 0
Pireus(config-router)#exit
Pireus(config)#exit
Pireus#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Pireus#
```

Korak 1.4.

Provera konekcije sa ruterom Pireus sa rutera Athens se vrši komandom:

```
Athens#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/40/68 ms
Router#
```

2. Konfiguracija Telnet servisa

Korak 2.1.

Na ruteru Pireus potrebno je konfiguristai telnet servis.

```
Pireus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pireus(config)#line vty 0 4
Pireus(config-line)#login
% Login disabled on line 130, until 'password' is set
```

```
% Login disabled on line 131, until 'password' is set
% Login disabled on line 132, until 'password' is set
% Login disabled on line 133, until 'password' is set
% Login disabled on line 134, until 'password' is set
Pireus(config-line)#password proba
Pireus(config-line)#enable password proba
Pireus(config)#exit
Pireus#
```

Korak 2.2.

Zatim je potrebno proveriti da li radi Telnet pristup sa rutera Athens i sa ISP-a (pristup sa ISP-a simboliše pristup sa celog Interneta).

```
Athens#telnet 172.16.0.1
Trying 172.16.0.1 ... Open


User Access Verification

Password:
Pireus>enable
Password:
Pireus#exit
```

I ping:

```
Athens#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/44 ms
```

Telnet pristup bi trebao da radi sa oba rutera.

3. Konfigurisanje standardnih ACL na ruteru Pireus

Korak 3.1.

Sada je na ruteru Pireus potrebno postaviti firewall pravila, tj. ACL, koja omogućava pristup sa rutera Athens, sav ostali pristup je po default-u zabranjen. ACL se konfiguriše na sledeći način:

```
Pireus(config)#interface s0/0
Pireus(config-if)#ip access-group 1 in
Pireus(config-if)#exit
Pireus(config)#access-list 1 permit 50.0.0.1 0.0.0.0
```

Korak 3.2.

Sada će sa rutera Athens biti dozvoljen Telnet:

```
Athens#telnet 172.16.0.1
Trying 172.16.0.1 ... Open


User Access Verification

Password:
Pireus>enable
Password:
Pireus#exit
```

i ping:

```
Athens#ping 172.16.0.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
Router#
```

Tako će isto i telnet i ping biti dozvoljeni sa rutera ISP

```
ISP#telnet 172.16.0.1
Trying 172.16.0.1 ... Open


User Access Verification

Password:
Pireus>exit
Password:
Pireus#exit
```

Kao i ping

```
ISP#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/41/52 ms
```

Korak 3.3.

A sa rutera ISP neće:

```
ISP#telnet 172.16.0.1
Trying 172.16.0.1 ...
% Destination unreachable; gateway or host down
```

Kao ni ping:

```
ISP#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
ISP#
```

Obavezno pročitati

Napomena: Ovo će raditi samo kratko vreme. Budući da je ovim firewall-om dozvoljen saobraćaj na ruter Pireus samo sa rutera sa IP adresom 50.0.0.1 (Athens), vremenom će is OSPF rute na ruterima Athens i ISP prema mreži 172.16.0.0 nestati jer taj ruter neće primati OSPF pakete. Za posledicu telnet i ping neće raditi ni sa Athens ni sa ISP rutera. Da bi se ovo prevazišlo potrebno je koristi extended ACL koje omogućavaju filtriranje pristupa po aplikaciji, tj. po portu kojem pristupaju.

4. Konfigurisanje extended ACL

Sada je na ruteru Pireus potrebno postaviti extended ACL, koja omogućava Telnet i OSPF saobraćaj, tj. pristup sa svim servisima koji koriste TCP i OSPF protokol, a zabranjuje ping saobraćaj, tj. pristup paketima koji koriste ICMP protokol:

Korak 4.1.

```
Pireus(config)#interface s0/0
```

```
Pireus(config-if)#no ip access-group 1 in
Pireus(config-if)#ip access-group 102 in
Pireus(config-if)#exit
Pireus(config)#access-list 102 permit tcp any any
Pireus(config)#access-list 102 permit ospf any any
Pireus(config)#access-list 102 deny icmp any any
```

Ovim naredbama dozvoljava se saobraćaj (permit) za TCP protokol koji koristi telnet i OSPF protokol da bi se omogućilo rutiranje, a zabranjuje (deny) saobraćaj za ICMP protokol koji koristi ping. Zbog provere možete uneti komandu `no access-list 102 deny icmp any any`. Proveriti da ne radi ping sa Athens na `172.16.0.1`, pa ponovo uneti `access-list 102 deny icmp any any` i proveriti da radi ping sa Athens na `172.16.0.1`. Treba biti strpljiv jer te promene nisu trenutne i ne moraju biti odmah vidljive.

Korak 4.2.

Proveriti sa rutera Athens i ISP (Interneta), šta je dozvoljeno, a šta ne (Telnet i ping).

5. Konfigurisanje extended ACL i zabrana pristupa sa Interneta

Korak 5.1.

Sada je na ruteru Pireus potrebno dozvoliti pristup za TCP i ICMP saobraćaj sa rutera Athens (50.0.0.1) u okviru ACL pod brojem 103. Pre toga je potrebno ukloniti ACL 102 sa interfesja s0/0. Obratiti pažnju da se sa dva pravila dozvoljava pristup sa 50.0.0.1 za tcp i icmp protokol. Celokupan ostali saobraćaj je pod default-u zabranjen te za to nije potrebno posebno navoditi pravilo. Da bi rutiranje radilo i da bi računari imali međusobnu vezu potrebno je dozvoliti saobraćaj OSPF paketima naredbom `access-list 103 permit ospf any any`.

```
Pireus(config)#int s0/0
Pireus(config-if)#no ip access-group 102 in
Pireus(config-if)#exit
Pireus(config)#access-list 103 permit tcp 50.0.0.1 0.0.0.255  any
Pireus(config)#access-list 103 permit icmp 50.0.0.1 0.0.0.255  any
Pireus(config)#access-list 103 permit ospf any any
Pireus(config)#int s0/0
Pireus(config-if)#ip access-group 103 in
```

Korak 5.2.

Proveriti sa rutera Athens i ISP (Interneta), šta je dozvoljeno, a šta ne (Telnet i ping). Sa ISP-a neće biti dozvoljeno ništa, a sa rutera Athens sve:

```
[Connection to 172.16.0.1 closed by foreign host]
ISP#telnet 172.16.0.1
Trying 172.16.0.1 ...
% Destination unreachable; gateway or host down

ISP#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
U.U..
Success rate is 0 percent (0/5)
```

6. Konfigurisanje SSH servera na ruteru Pireus i dozvola pristupa SSH sa Interneta

Korak 6.1.

Na ruteru Pireus potrebno je konfigurisati SSH server

```
Pireus#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Pireus(config)#hostname Pireus
Pireus(config)#ip domain-name pireus.com
Pireus(config)#logging console
Pireus(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Pireus.pireus.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Pireus(config)#
*Mar  1 01:16:21.071: %SSH-5-ENABLED: SSH 1.99 has been enabled
Pireus#
Pireus#
*Mar  1 01:16:36.511: %SYS-5-CONFIG_I: Configured from console by console


Pireus(config)#username admin priv 15 secret proba
Pireus(config)#aaa new-model
Pireus(config)#enable secret proba
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.

Pireus(config)#line vty 0 4
Pireus(config-line)#transport input all
Pireus(config-line)#
```

Korak 6.2.

Pristup pomoću SSH klijenta još uvek nije moguć sa ISP-a.

```
ISP#ssh -l admin 172.16.0.1
% Destination unreachable; gateway or host down
```

Korak 6.3.

Na ruteru Pireus potrebnoj je dodati sledeće pravilo u kojem se dozvoljava pristup sa jedne IP adrese ISP-a (192.168.1.2) samo na port 22, tj. SSH server.

```
Pireus(config)#access-list 103 permit tcp 192.168.1.2 0.0.0.255 any eq 22
```

Korak 6.4.

Za proveru se može uspešno pristupi SSH serveru na rutera Pireus sa ISP-a. Ping i Telnet će i dalje biti onemogućeni:

```
ISP#ssh -l admin 172.16.0.1

Password:

Pireus>exit
```

Telnet ne radi:

```
[Connection to 172.16.0.1 closed by foreign host]
Router#telnet 172.16.0.1
Trying 172.16.0.1 ...
% Destination unreachable; gateway or host down
```

Kao ni ping:

```
Router#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
```

```
U.U.U
Success rate is 0 percent (0/5)
```

Pitanje: Da li će raditi SSH pristup sa rutera Athens i ako ne kako to omogućiti?

Literatura

[1] Cisco Inc., Cisco IOS Firewall, Configuring IP Access Lists, Document ID: 23602, Cisco Inc. web site, Updated: Dec 27, 2007 [Online]. Available: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml#netdiag [Accessed: 17 September 2012].