HES-SO MSE

Network security and architecture

S1-2021

Firewall

04/12/2020

Fabio Baldo

Contents

List of source codes

1 Configuration

1.1 Question P1

In our case having a static or dynamic routing is not important beacuse all the traffic passes through the firewall.

1.2 Question P2

Thanks to the commands

```
$ show run object
```

and

```
$ show run nat
```

the following output has been obtained. This configuration is needed for translating the ip address such that when an inside of the specific subnet, their IPs wil be translated accordingly to the interface. manual

```
ASA# show run object
object network inside-net
 subnet 192.168.10.0 255.255.255.0
ASA# show run nat
!
object network inside-net
 nat (inside,outside) dynamic interface
```

Listing 1: output for question P2

1.3 Question P3

Only the IPs of the subnet `192.168.10.10 255.255.255.0` will be translated to IPs of the interface `interface GigabitEthernet0/0`

1.4 Question P4

1.5 Question P5

Create a username with password:

```
ASA(config)# username cisco password cisco
```

Configure this local username to authenticate with SSH:

```
ASA(config)# aaa authentication ssh console LOCAL
```

Configure this local username to authenticate with Telnet:

```
ASA(config)# aaa authentication telnet console LOCAL
```

Create RSA key pair:

```
ASA(config)# crypto key generate rsa modulus 2048
```

Now specify only particular hosts or network to connect to the device using SSH: from the inside

```
ASA(config)# ssh 192.168.10.0 255.255.255.0 inside
```

from the outside

```
ASA(config)# ssh 172.16.3.10 255.255.255.255 outside
```

as a consequence of the procedure it is possible to connect via ssh to the ASA from HOST B and C

1.6 Question P6

1.7 Question P7

The commands used for testing the communication between the two hosts have been:

```
HostA#nc -n -l -p 80 -v
```

```
HostC#nc -v 209.165.200.227 80
```

1.8 Question P8

For testing the connection from the HostB to the hostC the IP had not to be changed because no rules are applied from the inside to the dmz.

1.9 Question P9

The results of the scans are the followings:

```
HostC# nmap 209.165.200.226
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-03 23:33 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 ↪  --system-dns or specify valid servers with --dns-servers
Nmap scan report for 209.165.200.226
Host is up (0.014s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds

HostC# nmap -sA 209.165.200.226
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-03 23:29 UTC
Nmap scan report for 209.165.200.226
Host is up (0.012s latency).
All 1000 scanned ports on 209.165.200.226 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds

HostC# nmap -Pn 192.168.20.10
Nmap scan report for 192.168.20.10
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.20.10 are filtered

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds

HostC# nmap -Pn 192.168.10.11
Nmap scan report for 192.168.10.11
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.10.11 are filtered

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

Listing 2: Nmap from HostC

1.10 Question P10

1.11 Question P11

problems with java WS

1.12 Question P12

problems with java WS