University of Msila | Faculty of Mathematics and Computer Science
Department of Computer Science | Network administration & Security
Speciality : Master2 RTIC | First Name:: Last Name:

Exam

Exercise1(10 pts): select the correct answer from the given choices:

1/ Which attack of Switch is incorrect? :
a- reconfiguration of SPAN port
b- switch jamming
c- switch poisoning
d- Cam table manipulation

2/ What is the weakest layer among the seven security layers
a- human layer
b- endpoint layer
c- network layer
d-application layer

3/ Which function among main network administration functions that supervision and administration systems must implement, is incorrect:
a- security management
b -performance management
c- fault management
d- configuration management
e- devices management

4/Which attack is being used when threat actors use pings to discover subnets and hosts on a protected network, to generate flood attacks, and to alter host routing tables?
a- Address Spoofing Attack
b- Amplification and Reflection Attacks
c- ICMP Attack
d- MiTM Attack
e- Session Hijacking

5/ Which attack being used is when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user?
a- Address Spoofing Attack
b- Amplification and Reflection Attacks
c- ICMP Attack
d-Session Hijacking

6/ What type of attack is port scanning?
a- Reconnaissance
b- Access
c- DoS
d- Social Engineering

7/ Which penetration testing tool identifies whether a remote host is susceptible to a security attack?
a- Packet Sniffers
b- Encryption Tools
c- Vulnerability Exploitation Tools
d- Debuggers

8/. Which attack exploits the three-way handshake?
a-TCP reset attack
b- UDP flood attack
c- TCP SYN Flood attack
d- TCP session hijacking

9. Which attack is being used when the threat actor spoofs the IP address of one host, predicts the next sequence number, and sends an ACK to the other host?

- TCP reset attack
- TCP SYN Flood attack
- DoS attack
- TCP session hijacking

10/ Which network security device ensures that internal traffic can go out and come back, but external traffic cannot initiate connections to inside hosts?

- VPN
- Firewall
- IPS

11/ What is the term used to describe a mechanism that takes advantage of a vulnerability?

- mitigation
- exploit
- vulnerability
- threat

12/. In which type of attack is falsified information used to redirect users to malicious Internet sites?

- DNS amplification and reflection
- ARP cache poisoning
- DNS cache poisoning
- domain generation

13/ In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?

- address spoofing
- MITM
- session hijacking
- DoS

14/ What type of VPN can be established with a web browser using HTTPS?

- IPsec
- Client-based VPN
- Site-to-Site VPN
- Clientless VPN

15/ True or False? Tunneling protocols such as IPsec do not work well through NAT.

- True x
- False

16. Which protocol is attacked when a cybercriminal provides an invalid gateway in order to create a man-in-the-middle attack?

- DHCP
- DNS
- ICMP
- HTTP or HTTPS

17. In what way are zombies used in security attacks?

- They target specific individuals to gain corporate or personal information.
- They probe a group of machines for open ports to learn which services are running.
- They are maliciously formed code segments used to replace legitimate applications.
- **They are infected machines that carry out a DDoS attack.**

18. Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?

- man-in-the-middle attack
- SYN flood attack
- DoS attack
- ICMP attack

19. the HIDS is:

a- anomaly based IDS

b-signature based IDS

c- Hybride based IDS

20- Where should a standard ACL be placed?

- Standard ACL location is not important.
- Standard ACLs should be placed as close to the destination as possible.
- Standard ACLs should be placed as close to the source as possible.
- Standard ACLs should be placed on serial interfaces.

Exercice2 (3.5 pts):

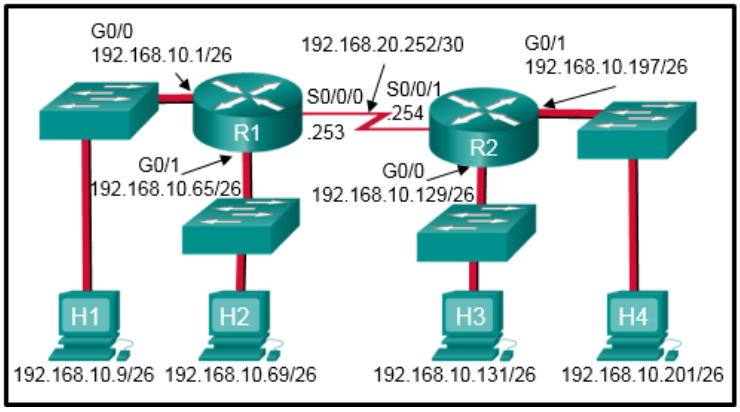
1. Which wildcard mask would permit only hosts from the 10.10.0.0/25 network?

- 0.0.0.63
- 0.0.0.31
- 0.0.0.255
- 0.0.0.127

What wild card mask will match networks 172.16.0.0 through 172.19.0.0?

- 0.0.3.255
- 0.252.255.255
- 0.3.255.255
- 0.0.255.255

2. Refer to the exhibit. Which two ACLs would permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface? (Choose two.)



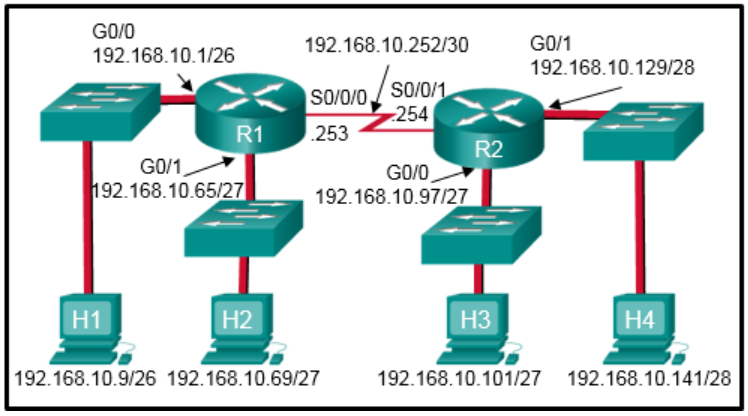
- access-list 1 permit 192.168.10.0 0.0.0.127
- access-list 2 permit host 192.168.10.9
  access-list 2 permit host 192.168.10.69
- access-list 5 permit 192.168.10.0 0.0.0.63
  access-list 5 permit 192.168.10.64 0.0.0.63
- access-list 3 permit 192.168.10.128 0.0.0.63
- access-list 4 permit 192.168.10.0 0.0.0.255

3. A network administrator has configured ACL 9 as shown. Users on the 172.31.1.0 /24 network cannot forward traffic through router CiscoVille. What is the most likely cause of the traffic failure?

```
CiscoVille#
CiscoVille# configure terminal
CiscoVille(config)# access-list 9 permit 172.29.0.0 0.0.0.255
CiscoVille(config)# access-list 9 permit 172.30.0.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255
CiscoVille(config)# access-list 9 permit 172.31.1.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 192.168.1.0 0.0.0.255
CiscoVille(config)# access-list 9 permit any
CiscoVille(config)# interface fastethernet0/1
CiscoVille(config-if)# ip access-group 9 in
CiscoVille(config-if)# end
```

- The established keyword is not specified.
- The sequence of the ACEs is incorrect.
- The port number for the traffic has not been identified with the eq keyword.
- The permit statement specifies an incorrect wildcard mask.

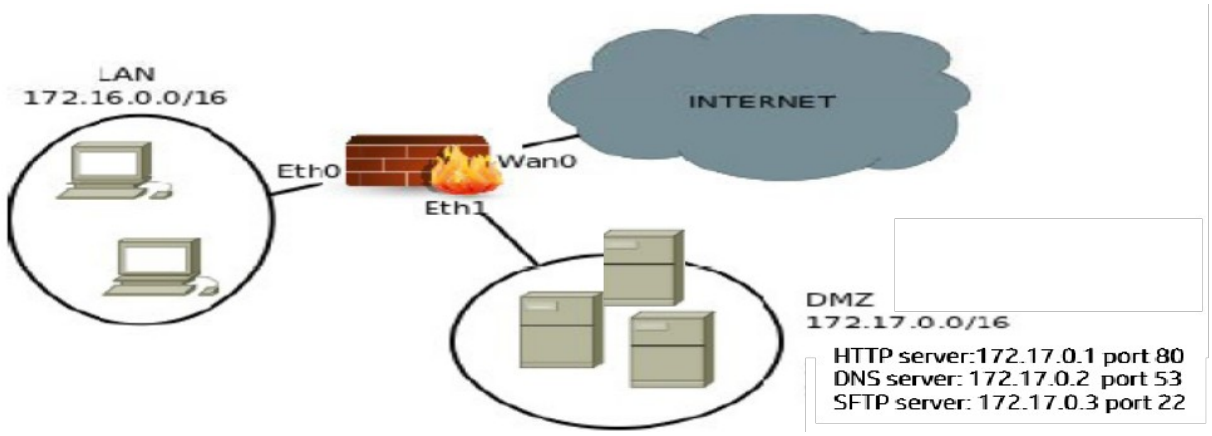
4. Refer to the exhibit. Which command would be used in a standard ACL to allow only devices on the network attached to R2 G0/0 interface to access the networks attached to R1?



- access-list 1 permit 192.168.10.128 0.0.0.63
- access-list 1 permit 192.168.10.0 0.0.0.255
- access-list 1 permit 192.168.10.96 0.0.0.31
- access-list 1 permit 192.168.10.0 0.0.0.63

Exercise 3 (6 pts):

A company has a firewall to restrict access to and from machines on its internal network. The company's network architecture also includes a demilitarized zone (DMZ) for deploying the company's own web DNS ,and SFTP servers. The security policy applied by the firewall is described in Table 1.



University of Msila | Faculty of Mathematics and Computer Science
Department of Computer Science | Network administration & Security
Speciality : Master2 RTIC | First Name:: Last Name:

N°	In Interface	Out Interface	Src Ip	Des IP	protocol	Src Port	Dst Port	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	>1024	80	Permit
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	>1024	Permit
3	Wan0	Eth1	*	172.17.0.1	TCP	>1024	80	Permit
4	Eth1	Wan0	172.17.0.1	*	TCP	80	>1024	Permit
5	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	>1024	53	Permit
6	Eth1	Eth0	172.17.0.2	172.16.0.0	UDP	53	>1024	Permit
7	Eth0	Eth1	172.16.0.0	172.17.0.3	TCP	>1024	22	Permit
8	Eth1	Eth0	172.17.0.3	172.16.0.0	TCP	22	>1024	Permit
9	Wan0	Eth0	*	172.16.0.0	TCP	80	>1024	Permit
10	Eth1	Wan0	172.16.0.0	*	TCP	80	80	Permit
11	*	*	*	*	*	*	*	Deny

1) Give the corresponding policy for each pair of rules (2.5 Pts) :

(1-2):

(3-4):

(5-6):

(7-8):

(9-10).

2) Specify the rule that will check each of the following packets and say whether the packet will be accepted or rejected. (3.5 points)

p1- IP source: 172.16.0.30 IP destination: 12.230.24.45 Protocol: TCP Source port: 1045 app protocol=HTTPS

Rule: Action:

p2- IP source: 172.16.10.5 IP destination: 172.17.0.2 Protocol: UDP Source port: 6810 app protocol=DNS

Rule: Action:

p3- IP source: 140.10.2.1 IP destination: 172.17.0.1 Protocol: TCP Source port: 8000 app protocol=HTTP

Rule: Action:

p4-IP source: 172.17.2.1 IP destination: 172.17.0.3 Protocol: TCP Source port: 8000 Destination port: 22

Rule: Action:

p5- IP source: 172.14.3.3 IP destination: 172.17.0.2 Protocol: UDP Source port: 6000 Destination port: 53

Rule: Action:

p6- IP source: 172.17.0.1 IP destination: 1.2.3.4 Protocol: TCP Source port: 80 Destination port: 9999

Rule: Action:

p7- IP source: 172.16.10.5 IP destination: 172.17.0.3 Protocol: TCP Source port: 8000 app protocol= SSH

Rule: Action:

University of Msila
Department of Computer Science
Speciality : Master2 RTIC

Faculty of Mathematics and Computer Science
Network administration & Security
First Name:: Last Name:

Solution:

Exercice1:

1/ Which attack of Switch is incorrect? :
a- reconfiguration of SPAN port
b- switch jamming
c- switch poisoning x
d- Cam table manipulation

2/ What is the weakest layer among the seven security layers
a- human layer x
b- endpoint layer
c- network layer
d-application layer

3/ Which function among main network administration functions that supervision and administration systems must implement, is incorrect:
a- security management
b -performance management
c- fault management
d- configuration management
e- devices management x

4/Which attack is being used when threat actors use pings to discover subnets and hosts on a protected network, to generate flood attacks, and to alter host routing tables?
a- Address Spoofing Attack
b- Amplification and Reflection Attacks
c- ICMP Attack x
d- MiTM Attack
e- Session Hijacking

5/ Which attack being used is when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user?
a- Address Spoofing Attack x
b- Amplification and Reflection Attacks
c- ICMP Attack
d-Session Hijacking

6/ What type of attack is port scanning?

a- Reconnaissance x
b- Access
c- DoS
d- Social Engineering

7/ Which penetration testing tool identifies whether a remote host is susceptible to a security attack?

a- Packet Sniffers
b- Encryption Tools
c- Vulnerability Exploitation Tools x
d- Debuggers

8/. Which attack exploits the three-way handshake?

a-TCP reset attack
b- UDP flood attack
c- TCP SYN Flood attack x
d- TCP session hijacking

9. Which attack is being used when the threat actor spoofs the IP address of one host, predicts the next sequence number, and sends an ACK to the other host?

- TCP reset attack
- TCP SYN Flood attack
- DoS attack
- TCP session hijacking x

10/ Which network security device ensures that internal traffic can go out and come back, but external traffic cannot initiate connections to inside hosts?

- VPN
- Firewall x
- IDS
- IPS

11/ What is the term used to describe a mechanism that takes advantage of a vulnerability?

- mitigation
- **exploit** x
- vulnerability
- threat

12/. In which type of attack is falsified information used to redirect users to malicious Internet sites?

- DNS amplification and reflection
- ARP cache poisoning
- **DNS cache poisoning** x
- domain generation

13/ In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?

- address spoofing
- MITM
- session hijacking
- **DoS** x

14/ What type of VPN can be established with a web browser using HTTPS?

- IPsec
- Client-based VPN
- Site-to-Site VPN
- Clientless VPN x

15/ True or False? Tunneling protocols such as IPsec do not work well through NAT.

- True x
- False

16. Which protocol is attacked when a cybercriminal provides an invalid gateway in order to create a man-in-the-middle attack?

- **DHCP** x
- DNS
- ICMP
- HTTP or HTTPS

17. In what way are zombies used in security attacks?

- They target specific individuals to gain corporate or personal information.
- They probe a group of machines for open ports to learn which services are running.
- They are maliciously formed code segments used to replace legitimate applications.
- **They are infected machines that carry out a DDoS attack.** x

18. Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?

- **man-in-the-middle attack x**
- SYN flood attack
- DoS attack
- ICMP attack

19. the HIDS is:

a- anomaly based IDS x

b-signature based IDS

c- Hybride based IDS

20- Where should a standard ACL be placed?

- Standard ACL location is not important.
- Standard ACLs should be placed as close to the destination as possible.
- Standard ACLs should be placed as close to the source as possible. x
- Standard ACLs should be placed on serial interfaces.

Exercise 2 (4 pts):

1. Which wildcard mask would permit only hosts from the 10.10.0.0/25 network?

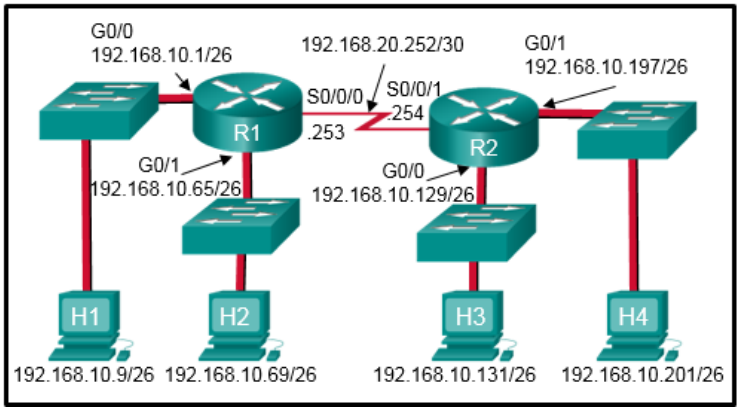
- 0.0.0.63
- 0.0.0.31

- 0.0.0.255
- **0.0.0.127**

What wild card mask will match networks 172.16.0.0 through 172.19.0.0?

- 0.0.3.255
- 0.252.255.255
- **0.3.255.255**
- 0.0.255.255

2. Refer to the exhibit. Which two ACLs would permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface? (Choose two.)



- **access-list 1 permit 192.168.10.0 0.0.0.127** **x**
- access-list 2 permit host 192.168.10.9
  access-list 2 permit host 192.168.10.69
- **access-list 5 permit 192.168.10.0 0.0.0.63** **x**
  access-list 5 permit 192.168.10.64 0.0.0.63 **x**
- access-list 3 permit 192.168.10.128 0.0.0.63
- access-list 4 permit 192.168.10.0 0.0.0.255

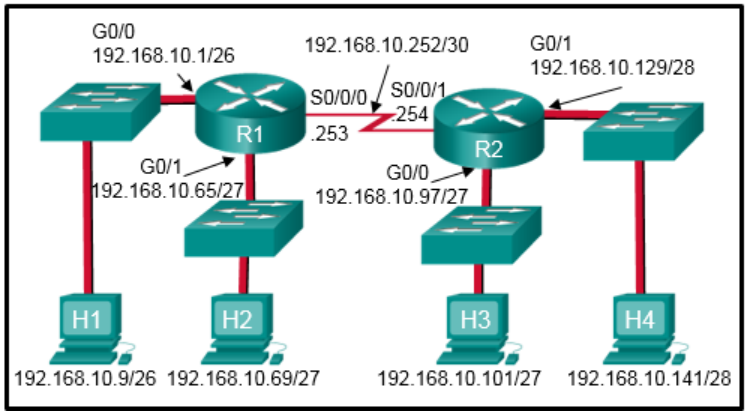
3. A network administrator has configured ACL 9 as shown. Users on the 172.31.1.0 /24 network cannot forward traffic through router CiscoVille. What is the most likely cause of the traffic failure?

```
CiscoVille#
CiscoVille# configure terminal
CiscoVille(config)# access-list 9 permit 172.29.0.0 0.0.0.255
CiscoVille(config)# access-list 9 permit 172.30.0.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255
CiscoVille(config)# access-list 9 permit 172.31.1.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 192.168.1.0 0.0.0.255
CiscoVille(config)# access-list 9 permit any
CiscoVille(config)# interface fastethernet0/1
CiscoVille(config-if)# ip access-group 9 in
CiscoVille(config-if)# end
```

- The established keyword is not specified.
- **The sequence of the ACEs is incorrect.** **x**
- The port number for the traffic has not been identified with the eq keyword.
- The permit statement specifies an incorrect wildcard mask.

University of Msila | Faculty of Mathematics and Computer Science
Department of Computer Science | Network administration & Security
Speciality : Master2 RTIC | First Name:: Last Name:

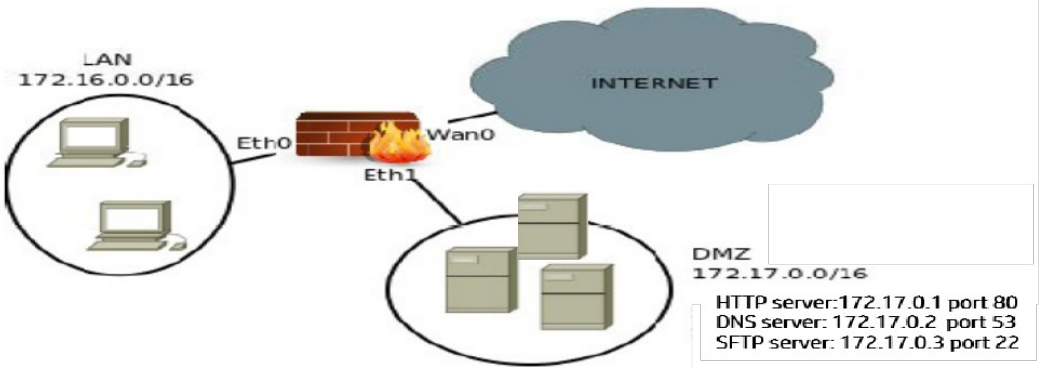
4. Refer to the exhibit. Which command would be used in a standard ACL to allow only devices on the network attached to R2 G0/0 interface to access the networks attached to R1?



- access-list 1 permit 192.168.10.128 0.0.0.63
- access-list 1 permit 192.168.10.0 0.0.0.255
- **access-list 1 permit 192.168.10.96 0.0.0.31** **x**
- access-list 1 permit 192.168.10.0 0.0.0.63

Exercise 3 (6,5 pts):

A company has a firewall to restrict access to and from machines on its internal network. The company's network architecture also includes a demilitarized zone (DMZ) for deploying the company's own web DNS ,and SFTP servers. The security policy applied by the firewall is described in Table 1.



N°	In Interface	Out Interface	Src Ip	Des IP	protocol	Src Port	Dst Port	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	>1024	80	Permit
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	>1024	Permit
3	Wan0	Eth1	*	172.17.0.1	TCP	>1024	80	Permit
4	Eth1	Wan0	172.17.0.1	*	TCP	80	>1024	Permit
5	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	>1024	53	Permit
6	Eth1	Eth0	172.17.0.2	172.16.0.0	UDP	53	>1024	Permit
7	Eth0	Eth1	172.16.0.0	172.17.0.3	TCP	>1024	22	Permit
8	Eth1	Eth0	172.17.0.3	172.16.0.0	TCP	22	>1024	Permit

9	Wan0	Eth0	*	172.16.0.0	TCP	80	>1024	Permit
10	Eth0	Wan0	172.16.0.0	*	TCP	80	80	Permit
11	*	*	*	*	*	*	*	Deny

1) Give the corresponding policy for each pair of rules (2.5 Pts) :

(1-2): local users can send and receive HTTP response from local HTTP server

(3-4): internet users can send and receive HTTP response from local HTTP server

(5-6):local users can send and receive DNS response from local DNS server

(7-8): local users can send and receive SFTP response from local SFTP server

(9-10).ocal users can send and receive HTTP response from internet HTTP server

2) Specify the rule that will check each of the following packets and say whether the packet will be accepted or rejected. (3.5 points)

p1- IP source: 172.16.0.30 IP destination: 12.230.24.45 Protocol: TCP Source port: 1045 app protocol=HTTPS

Rule: 11 Action: deny

p2- IP source: 172.16.10.5 IP destination: 172.17.0.2 Protocol: UDP Source port: 6810 app protocol=DNS

Rule: 5 Action: permit

p3- IP source: 140.10.2.1 IP destination: 172.17.0.1 Protocol: TCP Source port: 8000 app protocol=HTTP

Rule: 3 Action: permit

p4-IP source: 172.17.2.1 IP destination: 172.17.0.3 Protocol: TCP Source port: 8000 Destination port: 22

Rule: in the same network Action: without rule

p5- IP source: 172.14.3.3 IP destination: 172.17.0.2 Protocol: UDP Source port: 6000 Destination port: 53

Rule: 11 Action: deny

p6- IP source: 172.17.0.1 IP destination: 1.2.3.4 Protocol: TCP Source port: 80 Destination port: 9999

Rule: 4 Action: permit

p7- IP source: 172.16.10.5 IP destination: 172.17.0.3 Protocol: TCP Source port: 8000 app protocol= SSH

Rule: 7 Action: permit