Network Security - BSCH4

Assignment 1

Galdan MOULINNEUF – 2927686

Question 1.

Firewall	Port	Source	Direction	Destination	Port2	Action
FW1	P1	192.168.0.0/24	ANY	192.168.1.50	443	**Permit**
FW1	P1	192.168.0.0/24	ANY	192.168.1.99	80	**Permit**
FW1	P1	192.168.0.0/24	ANY	192.168.1.99	25	**Permit**
FW2	P0	192.168.0.0/24	OUT	ANY	ANY	**Permit**
FW1	P1	10.10.0.0/24	ANY	192.168.1.50	443	**Permit**
FW2	P0	10.10.0.0/24	OUT	ANY	ANY	**Permit**
FW2	P1	ANY	IN	192.168.1.50	443	**Permit**
FW1	P0	192.168.0.12	ANY	192.168.1.99	22	**Permit**
FW1	P0	192.168.0.20	ANY	192.168.1.50	22	**Permit**
FW1	ANY	ANY	ANY	ANY	ANY	**Deny**
FW2	ANY	ANY	ANY	ANY	ANY	**Deny**

Question 2.

1. It's better to place a standard list as close to the destination so I would place it on the « Router C » at the interface "FA1".
2. Same reasoning as before so I would place it on the « Router E » at the interface "EO".
3. I would place it on the « Router C » at the interface "FA1".
4. Since extended ACL possesses destination IP, it's better to check it as close to the source so on the « Router F » at the interface "FA1".
5. I would place it on the « Router E » at the interface "E0".
6. I would place it on the « Router E » at the interface "E0".
7. Wildcard mask: 0.0.0.255
8. Wildcard mask: 0.255.255.255
9. Wildcard mask: 0.0.0.7
10. Wildcard mask: 0.0.31.255

Question 3.

Since the ACL is a standard list, it should be placed on router “B” at interface “FA1”. My ACL number will be 22.

Then the rules will be as follow:

Router B(config)#access-list 22 deny 192.168.15.0 0.0.0.31

Router B(config)#access-list 22 deny host 192.32.10.25

Router B(config)#access-list 22 permit any

Question 4.

Since the ACL is an extended list, it should be placed on router “A” at interface “E0”.

Then the rules will be as follow:

Router A(config)#access-list extended Godzilla

Router A(config)#access-list Godzilla deny ip 172.120.0.0 0.0.255.255 210.168.70.0 0.0.0.255

Router A(config)#access-list Godzilla deny ip 172.120.0.0 0.0.255.255 10.250.1.0 0.0.0.255

Router A(config)#access-list Godzilla permit ip any any

Question 5.

RADIUS versus TACACS+

RADIUS and TACACS+ are both protocols that uses the AAA principle. The main difference between the two protocols is that they're not used for the same thing.

Indeed, TACACS+ will be "Device-oriented", it means that it will controls how the device should be used, who has access to it and in what way it has access to it (which commands for example).

Everything a user do on the device will be controlled, whereas, RADIUS is "Network-oriented", it means that it will not controls a simple device but the network itself. Who has access to the network is the main purpose of the RADIUS protocol.

That's why TACACS+ separate the AAA in three distinct functions (Authentication, Authorization and Accounting) because it's relevant on a device, where RADIUS combines Authentication AND Authorization which make sense since it controls a network and split it would have no sense because almost everybody can **try** to access a network. It's no use to verify if a user is authorized since it will be authentified afterward.

Links:

Rivier Academic Journal (Academic Papers)

Cisco Comparison (Manufacturer instructions)

TACACAS Documentation (Manufacturer instructions)

NetworkWorld (Technical Blog)

TechExams (Technical Blog)