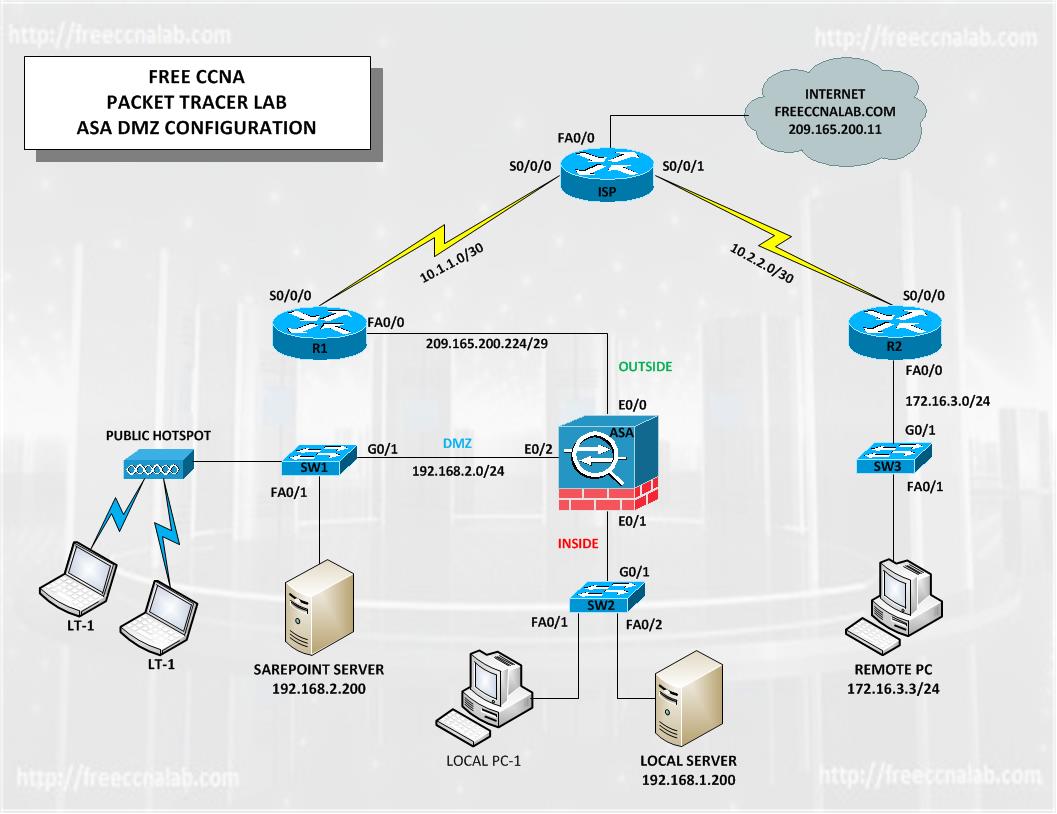
Configuration d’un Firewall DMZ ASA Lab

Dans ce TP, nous allons travailler sur le schéma de la figure suivante :



Pour cette raison lancer le fichier « ASA-DMZ.pkt » ci-joint.

Vous serai amené à configurer les routeurs R1, R2, ISP et finalement l’équipement Firewall (pour l’équipement Firewall) il faut utiliser au moins la version 6 de packet tracer.

Ci-après, la configuration des éléments mentionnés :

**Pour le routeur R1 :**

hostname R1

!

no ip cef

no ipv6 cef

!

license udi pid CISCO2901/K9 sn FTX1524R86E

!

spanning-tree mode pvst

!

interface GigabitEthernet0/0

ip address 209.165.200.225 255.255.255.248

duplex auto

speed auto

ipv6 ospf cost 1

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

clock rate 2000000

!

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

!

ip flow-export version 9

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

end

wr

**La configuration de R2 :**

hostname R2

!

no ip cef

no ipv6 cef

!

license udi pid CISCO2901/K9 sn FTX1524KCTL

!

spanning-tree mode pvst

!

interface GigabitEthernet0/0

ip address 172.16.3.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 10.2.2.1 255.255.255.252

!

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

end

wr

**La configuration de ISP :**

hostname ISP

!

no ip cef

no ipv6 cef

!

license udi pid CISCO2911/K9 sn FTX1524FMQ0

!

spanning-tree mode pvst

!

interface GigabitEthernet0/0

ip address 209.165.200.9 255.255.255.248

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

clock rate 2000000

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 2000000

!

interface Vlan1

no ip address

shutdown

!

ip classless

ip route 209.165.200.224 255.255.255.248 Serial0/0/0

ip route 172.16.3.0 255.255.255.0 Serial0/0/1

ip route 209.165.200.8 255.255.255.248 GigabitEthernet0/0

!

ip flow-export version 9

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

end

wr

**Finalement la configuration de l’équipement Firewall ASA:**

hostname ASA

names

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

switchport access vlan 1

!

interface Ethernet0/2

switchport access vlan 3

!

interface Ethernet0/3

switchport access vlan 1

!

interface Ethernet0/4

switchport access vlan 1

!

interface Ethernet0/5

switchport access vlan 1

!

interface Ethernet0/6

switchport access vlan 1

!

interface Ethernet0/7

switchport access vlan 1

!

interface Vlan1

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

!

interface Vlan2

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

!

interface Vlan3

no forward interface Vlan1

nameif dmz

security-level 50

ip address 192.168.2.1 255.255.255.0

!

object-group service DM\_INLINE\_SERVICE\_1

service-object tcp destination eq 80

service-object tcp destination eq 23

object network Webserver

host 192.168.2.100

object network Webserver-Ext

host 209.165.200.230

object network dmz-subnet

subnet 192.168.2.0 255.255.255.0

object network inside-subnet

subnet 192.156.1.0 255.255.255.0

!

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

!

access-list Outside\_access\_in extended permit object-group DM\_INLINE\_SERVICE\_1 any object Webserver

!

access-group Outside\_access\_in in interface outside

object network Webserver

nat (dmz,outside) static 209.165.200.230

object network dmz-subnet

nat (dmz,outside) dynamic interface

object network inside-subnet

nat (inside,outside) dynamic interface

!

class-map global-class

match default-inspection-traffic

!

policy-map global-policy

class global-class

inspect dns

inspect ftp

inspect h323

inspect http

inspect icmp

inspect tftp

!

service-policy global-policy global

!

telnet timeout 5

ssh timeout 5

!

dhcpd address 192.168.1.1-192.168.1.99 inside

dhcpd dns 209.165.200.10 interface inside

dhcpd enable inside

!

dhcpd auto\_config outside

!

dhcpd address 192.168.2.10-192.168.2.100 dmz

dhcpd dns 209.165.200.10 interface dmz

dhcpd enable dmz

!

Pour tester votre travail, voici les mesures demandées :

### Inside:

1. From the Local PC-1 ping 209.165.200.11. (this may require doing it twice)
2. From the Local PC-1 ping 192.168.1.200. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com
4. From the Local PC-1 open the desktop and browse to SharePoint.

### DMZ:

1. From the Local LT-1 ping 192.168.2.200. (this may require doing it twice)
2. From the Local LT-1 ping 209.165.200.11. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com.
4. From the Local PC-1 open the desktop and browse to Local.

### Remote:

1. From the Remote PC ping 209.165.200.11. (this may require doing it twice)
2. From the Remote PC ping 192.168.1.200.
3. From the Remote PC ping 192.168.2.200.
4. From the Remote PC open the desktop and browse to freeccnalab.com.
5. From the Remote PC open the desktop and browse to SharePoint.
6. From the Remote PC open the desktop and browse to Local.