Compte Rendu du TP : Sécurité des Équipements Réseaux

EST Beni Mellal

Filière : Bachelor en Cybersécurité

Module : Sécurité Informatique

Professeur : H.KHALOUFI

Étudiant : Youssef HACHIMI

Année Universitaire : 2025-2026

1. Introduction

Ce TP porte sur la sécurité des équipements réseaux, en utilisant Cisco Packet Tracer pour simuler un environnement réseau complexe. Il vise à configurer et sécuriser des routeurs, switches, un firewall ASA, un point d'accès Wi-Fi, et à implémenter des mécanismes de sécurité avancés tels que SSH, NTP, Syslog, ACL, ZPF (Zone-Based Policy Firewall) et IPS (Intrusion Prevention System). Le TP est divisé en plusieurs parties, couvrant la configuration de base jusqu'aux mesures de sécurité avancées. Toutes les configurations ont été testées dans Packet Tracer, et les pings et connexions ont été vérifiés pour confirmer la connectivité et la sécurité.

Ajout Spécifique : Sur la base du lien fourni, une nouvelle partie a été ajoutée pour détailler la configuration de base de l'ASA, incluant les commandes CLI pour les paramètres de base, interfaces VLAN, NAT/PAT, DHCP, AAA, ACL et vérifications. Cette configuration est alignée avec la topologie existante, avec des ajustements mineurs (par exemple, VLAN 3 pour DMZ au lieu de VLAN 2 dans certains cas). La table d'adressage du lien est similaire, avec DMZ sur 192.168.2.0/24 et serveur DMZ à 192.168.2.3.

2. Objectifs du TP

Les objectifs principaux sont les suivants :

TP 1 : Configurer les paramètres de base des périphériques.

TP 2 : Configurer l'accès administratif sécurisé aux routeurs (mots de passe, bannière, SSH, AAA, NTP, Syslog).

TP 3 : Configurer un pare-feu ZPF et un IPS sur un ISR.

TP 4 : Sécuriser les commutateurs réseaux (mots de passe, VLAN, ports sécurisés, protection STP).

TP 5 : Configurer les paramètres de base ASA et le pare-feu (interfaces VLAN, PAT, DHCP, AAA, DMZ).

TP 6 : Configurer une DMZ, NAT statique et ACL sur ASA.

3. Topologie du Réseau et Table d'Adressage

La topologie inclut 3 routeurs (R1, R2, R3), 3 switches (S1, S2, S3), un firewall ASA 5505, un point d'accès AP-PT, 4 PCs (A, B, C, D), un laptop, un serveur Syslog et un serveur TFTP.

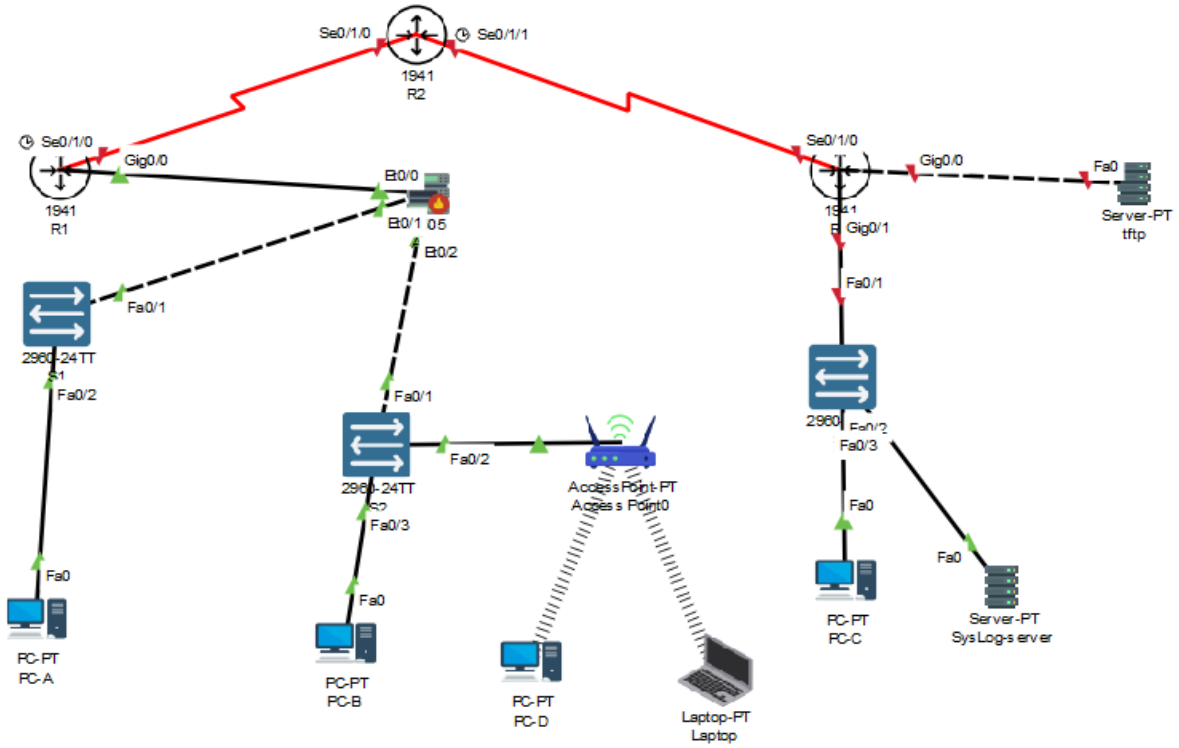


Table d'Adressage (Originale) :

Equipement	Interface	@IP	Masque	Default Gateway	Port du Switch
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
	Loopback 1	172.20.1.1	255.255.255.0	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	G0/0	1.1.1.1	255.0.0.0	N/A	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
S1	VLAN 1	192.168.2.11	255.255.255.0	192.168.2.1	N/A
S2	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1	N/A
S3	VLAN 1	172.16.1.11	255.255.255.0	172.30.3.1	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	N/A	R1 G0/0
	VLAN 2 (E0/2)	192.168.2.1	255.255.255.0	N/A	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18
PC-D	Wifi	192.168.1.4	255.255.255.0	192.168.1.1	PA wifi
Laptop	Wifi	192.168.1.2	255.255.255.0	192.168.1.1	PA wifi
Syslog Server	NIC	172.16.3.4	255.255.255.0	172.16.3.1	S3 F0/3
TFTP Server	NIC	1.1.1.2	255.0.0.0	1.1.1.1.1	R3 G0/0

Inside (VLAN 1) : 192.168.1.0/24 (ASA : 192.168.1.1/24)

Outside (VLAN 2) : 209.165.200.224/29 (ASA : 209.165.200.226/29, R1 G0/0 : 209.165.200.225/29)

DMZ (VLAN 3) : 192.168.2.0/24 (ASA : 192.168.2.1/24, Serveur DMZ : 192.168.2.3/24)

NAT Statique pour Serveur DMZ : 209.165.200.227

Hôte de Gestion Distant (Outside) : 172.16.3.3

Serveur DNS : 209.165.201.2 (assigné via DHCP)

Note : La topologie du lien est similaire, avec l'ASA connecté à Inside, DMZ et Outside. Utiliser VLAN 3 pour DMZ pour éviter conflits.

4. Matériel et Outils Utilisés

Cisco Packet Tracer .

Équipements simulés : Routeurs 1941 avec HWIC-2T, Switches 2960, ASA 5505, AP-PT, PCs avec cartes Wi-Fi.

Configurations effectuées en mode CLI (Command Line Interface).

5. Partie I : Configuration de Base des Équipements Réseau

1) Câblage Réseau et Mise en Place d'Infrastructure

Sélection des équipements comme indiqué.

Connexions automatiques via Packet Tracer.

Ajout de cartes Wi-Fi sur PC-D et Laptop.

2) Configuration Basique des Routeurs

Noms des routeurs :

Router#configure terminal

Router(config)# hostname R1

R1(config-if)# ip address 209.165.200.225 255.255.255.248

R1(config-if)# no shutdown

R1(config)# int s0/1/0

R1(config-if)# ip address 10.1.1.1 255.255.255.252

R1(config)# int loopback 1

R1(config-if)# ip address 172.20.1.1 255.255.255.0

Désactivation DNS lookup :

R1(config)# no ip domain-lookup

```
Router>enable
Router#config t
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostna
Router(config)#hostname R1
R1(config)#interface g0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.248
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

R1(config-if)#exit
R1(config)#
```

Routes par défaut sur R1 et R3 :

R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

```
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)#end
R1#
```

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
R3(config)#end
R3#
```

Routes statiques sur R2 :

R2(config)# ip route 172.16.3.0 255.255.255.0 10.2.2.1

R2(config)# ip route 209.165.200.224 255.255.255.248 10.1.1.1

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookuo
                             ^
% Invalid input detected at '^' marker.

R2(config)#no ip domain-lookup
R2(config)#interface s0/1/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 172.16.3.0 255.255.255.0 10.2.2.1
R2(config)#ip route 209.165.200.224 255.255.255.248 10.1.1.1
R2(config)#ip route 1.0.0.0 255.0.0.0 10.2.2.1
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip-domain-lookup
                ^
% Invalid input detected at '^' marker.

R3(config)#no ip domain-lookup
R3(config)#interface g0/1
R3(config-if)#ip address 172.16.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface g0/0
R3(config-if)#ip address 1.1.1.1 255.0.0.0
R3(config-if)#exit
R3(config)#interface s0/1/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
```

4) Configuration de Base des Switches et du Point d'Accès

Noms et adresses VLAN 1 (exemple S1) :

```
Switch(config)# hostname S1

S1(config)# int vlan 1

S1(config-if)# ip address 192.168.2.11 255.255.255.0

S1(config-if)# no shutdown

S1(config)# ip default-gateway 192.168.2.1

S1(config)# no ip domain-lookup
```

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.2.11 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

S1(config-if)#exit
S1(config)#ip default-gateway 192.168.2.1
S1(config)#
```

Switch 2 :

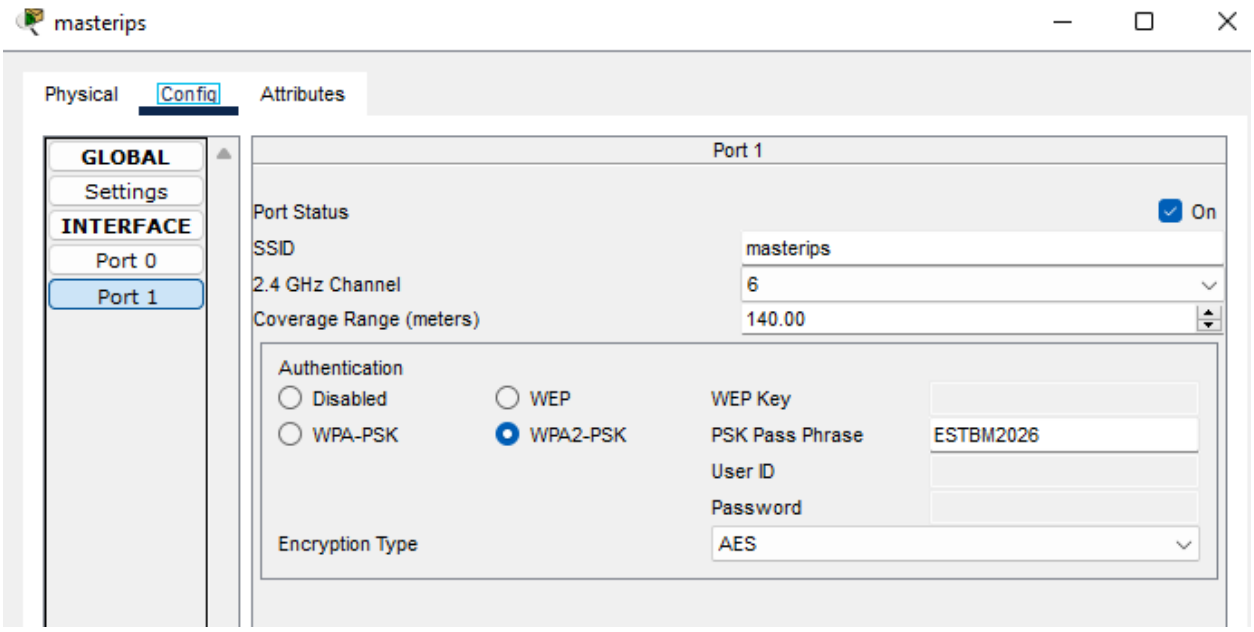
```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.11 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
to up

S2(config-if)#exit
S2(config)#ip default-gateway 192.168.1.1
```

Switch 3 :

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#interfac
S3(config)#interface vlan 1
S3(config-if)#ip address 172.16.3.11 255.255.255.0
S3(config-if)#no shu
S3(config-if)#no shutdown

S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

S3(config-if)#exit
S3(config)#ip default-gateway 172.16.3.1
```

Point d'accès : SSID = masterips.

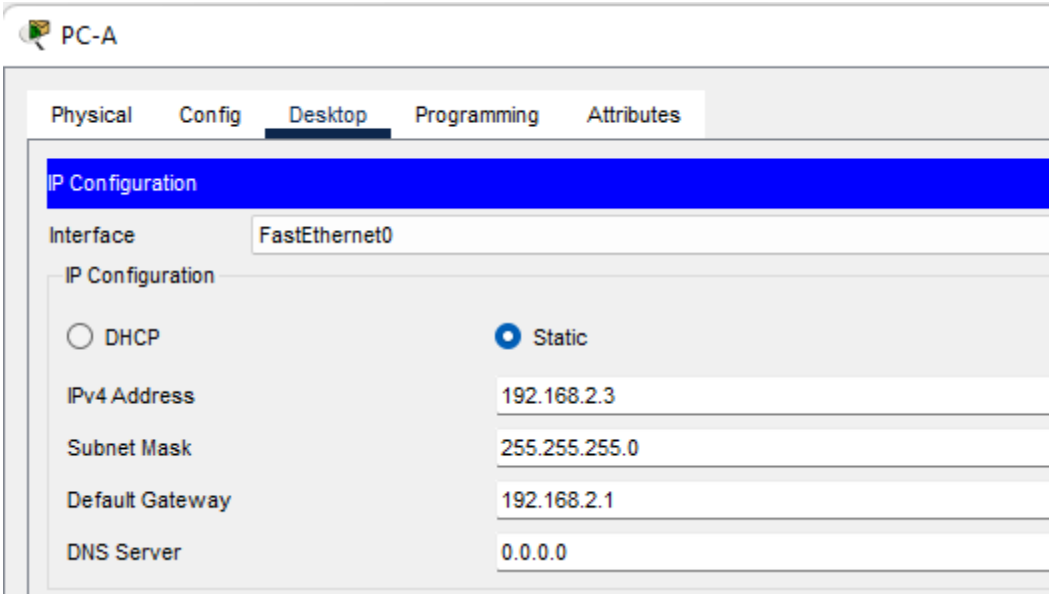
Tests pings : Succès entre PCs wired et wireless.



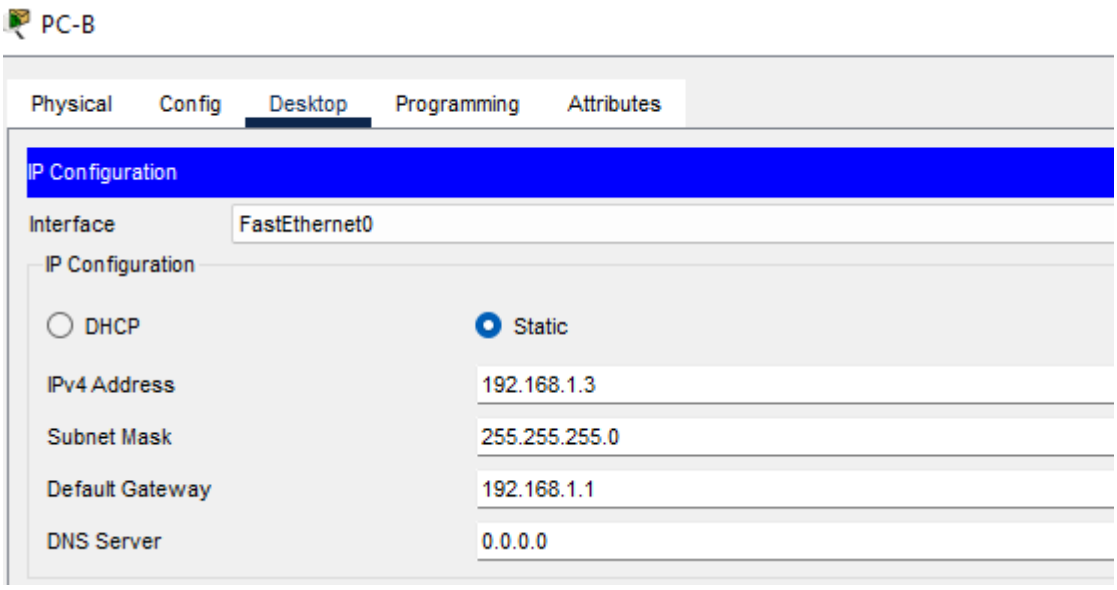
5) Configuration des PCs et Laptop

Adresses IP statiques comme dans la table.

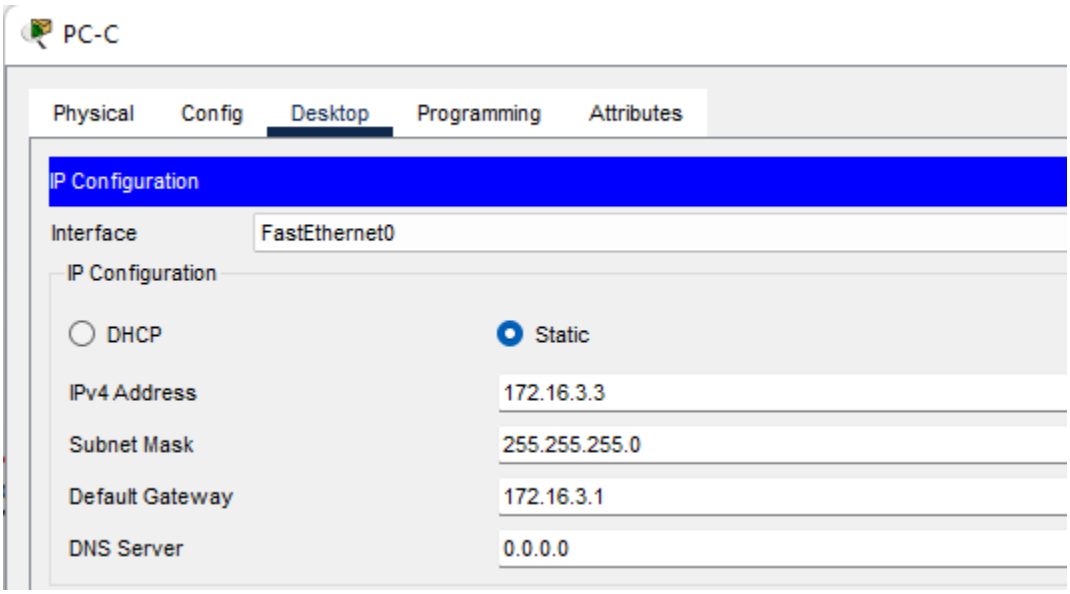
PC-A



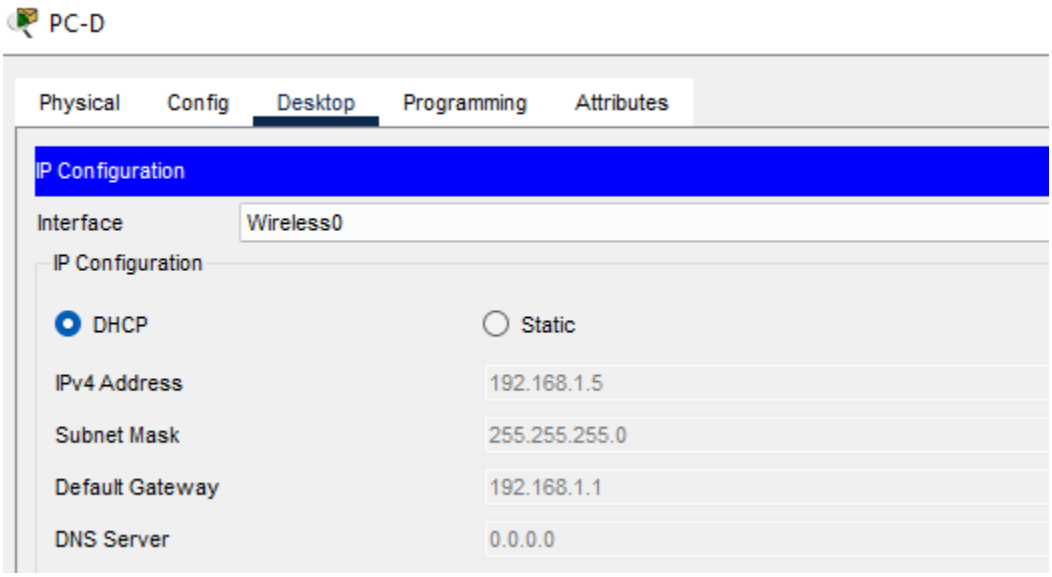
PC–B :


PC-B
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0

PC–C :


PC-C
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
172.16.3.3
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.1
DNS Server
0.0.0.0

PC-D :



6. Partie II : Sécurité d'Accès aux Routeurs

1) Configuration de Paramètres pour R1 et R3

Longueur minimale mot de passe :

```
R1(config)# security passwords min-length 10
```

Chiffrement mots de passe :

```
R1(config)# service password-encryption
```

Bannière MOTD :

```
R1(config)# banner motd $$   Unauthorized access strictly
prohibited!   $$
```

Enable secret :

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#service password-encryption
R1(config)#banner motd $Unauthorized access strictly prohibited and prosecuted to the
full extent of the law!$
R1(config)#enable algorithm-type scrypt secret cisco12345
                  ^
```

```
R1(config)#
R1(config)#
R1(config)#
R1(config)#username Admin01 privilege 15 secret Admin01pa55
R1(config)#aaa new-model
R1(config)#aaa authentication login default local-case enable
R1(config)#line con
R1(config)#line console 0
R1(config-line)#privi
R1(config-line)#privilege level 15
R1(config-line)#exec-timeout 15 0
R1(config-line)#logg
R1(config-line)#logging sy
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

Base utilisateurs locaux :

R1(config)# username Admin01 privilege 15 algorithm-type scrypt secret Admin01pa55

AAA :R1(config)# aaa new-model

R1(config)# aaa authentication login default local-case enable

Ligne console :

R1(config)# line console 0

R1(config-line)# privilege level 15

R1(config-line)# exec-timeout 15 0

R1(config-line)# logging synchronous

Lignes VTY :

R1(config)# line vty 0 4

R1(config-line)# privilege level 15

R1(config-line)# exec-timeout 15 0

R1(config-line)# transport input ssh

Enregistrement activités connexion :

R1(config)# login on-success log

R1(config)# login on-failure log

show login : Affiche infos supplémentaires sur blocages et tentatives.

Activation HTTP (pour tests) : ip http server sur R1.

2) Configuration SSH sur R1 et R3

Nom de domaine :

R1(config)# ip domain-name computersecurity.ma

Clés RSA :

R1(config)# crypto key generate rsa general-keys modulus 1024

SSH v2 : R1(config)# ip ssh version 2

Délais SSH :R1(config)# ip ssh time-out 90

R1(config)# ip ssh authentication-retries 2

Vérification : SSH depuis PC-C vers R1/R3 réussi.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name computersecurity.ma
R1(config)#ip domain-name computersecurity.ma
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1(config)#ip ssh time-out 90
R1(config)#ip ssh authentication-retries 2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip ssh
SSH Disabled - version 2
%Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 90 secs; Authentication retries: 2
R1#
```

```
C:\>ssh -l Admin01 172.16.3.1

Password:
R3#exit
```

3) Sécuriser contre Attaques Connexion et IOS sur R1

Sécurité connexion avancée :

R1(config)# login block-for 60 attempts 2 within 30

R1(config)# login on-failure log

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#login block-for 60 attempts 2 within 30
R1(config)#login on-failure log
R1(config)#login on-success log
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Sécuriser IOS et config :

R1(config)# secure boot-image

R1(config)# secure boot-config

Vérification : show secure bootset – Nom fichier config archivé basé sur flash.

Restauration : no secure boot-image et no secure boot-config.

4) Configuration NTP

R2 serveur NTP master :

R2# clock set 11:51:30 Jan 3 2026

R2(config)# ntp authentication-key 1 md5 NTPpassword

R2(config)# ntp trusted-key 1

R2(config)# ntp authenticate

R2(config)# ntp master 1

```
R2>show clock
*1:15:23.89 UTC Mon Mar 1 1993
R2>clock set 11:51:30 Jan 3 2026
          ^
% Invalid input detected at '^' marker.

R2>clock s
R2>clock set
R2>enable
R2#clock set 11:51:30 Jan 3 2026
R2#show clock
11:51:40.125 UTC Sat Jan 3 2026
R2#
```

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp authentication-key 1 md5 NTPpassword
R2(config)#ntp trusted-key 1
R2(config)#ntp authenticate
R2(config)#ntp master 1
```

Clients R1/R3 :

R1(config)# ntp authentication-key 1 md5 NTPpassword

R1(config)# ntp trusted-key 1

R1(config)# ntp authenticate

R1(config)# ntp server 10.1.1.2

R1(config)# ntp update-calendar

Vérification : show ntp associations et show clock – Synchronisation réussie.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp authentication-key 1 md5 NTPpassword
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

```
R1#clock set 11:51:30 Jan 3 2026
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 10.1.1.2
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

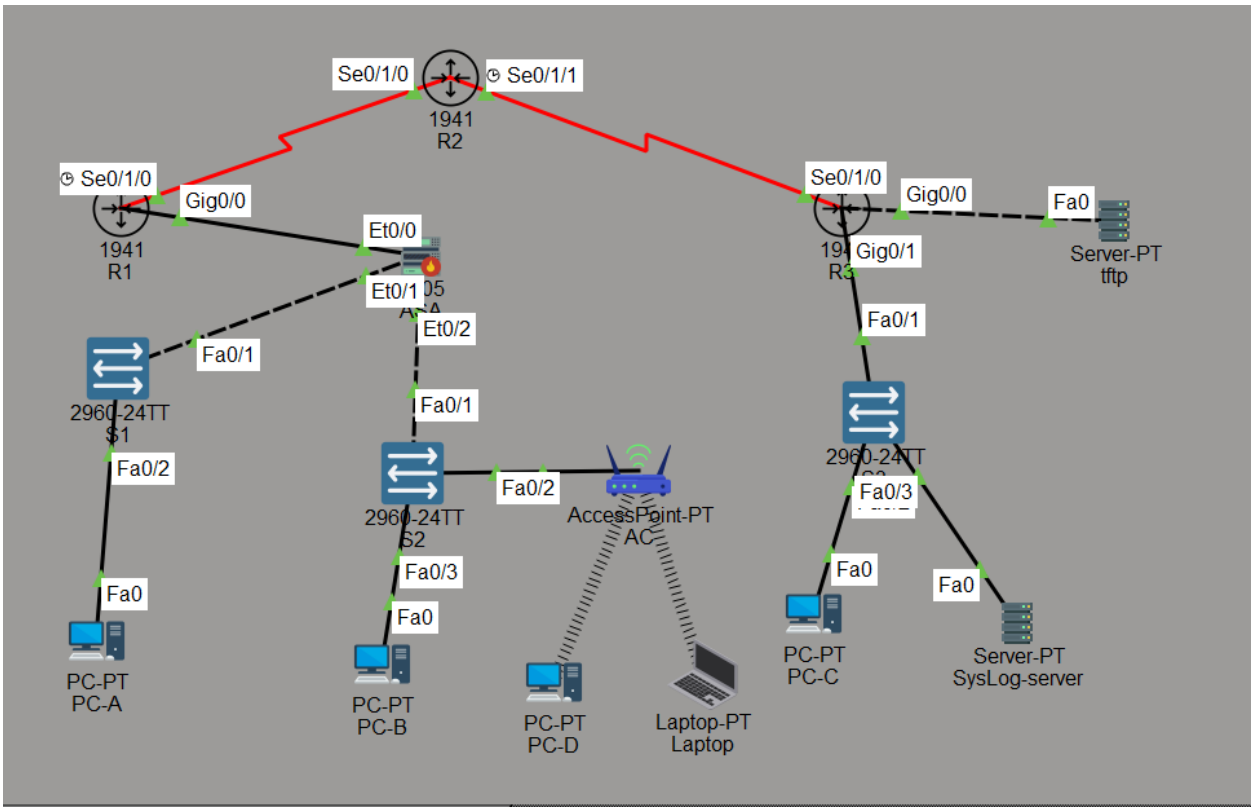
Router R3 :

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ntp authentication-key 1 md5 NTPpassword
R3(config)#ntp trusted-key 1
R3(config)#ntp authenticate
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ntp server 10.2.2.2
R3(config)#ntp update-calendar
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3(config)#ntp trusted-key 1
R3(config)#ntp authenticate
R3(config)#ntp server 10.2.2.2
R3(config)#ntp update-calendar
R3(config)#
```

Toplogie :



5) Configuration Syslog sur R3

Ajout serveur Syslog (172.16.3.4) sur S3 F0/3.

Ping vérifié.

Configuration R3 :

R3(config)# service timestamps log datetime msec

R3(config)# logging host 172.16.3.4

show logging : Affiche config syslog active.

7. Partie III : Configuration de la Sécurité des Switches

1) Configuration Sécurité Basique sur S1

Désactivation HTTP/HTTPS :

S1(config)# no ip http server

S1(config)# no ip http secure-server

Enable secret :

S1(config)# enable secret cisco12345

Chiffrement mots de passe :

S1(config)# service password-encryption

Bannière MOTD : S1(config)# banner motd $$ Unauthorized access strictly prohibited! $$

```
S1(config)#enable secret cisco12345
S1(config)#service password-encryption
S1(config)#banner motd $Unauthorized access strictly prohibited!$
S1(config)#ip domain-n
S1(config)#ip domain-name computersecurity.ma
S1(config)#username Admin01 privilege 15 secret Admin01pa55
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.computersecurity.ma

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 2 2:0:11.493: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh version 2
S1(config)#ip ssh time-out 90
S1(config)#ip ssh authentication-retries 2
S1(config)#show ip ssh
           ^
% Invalid input detected at '^' marker.

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
S1#
```

2) Configuration SSH sur S1

Nom de domaine, utilisateur, clés RSA, SSH v2, délais : Similaire à routeurs.

3) Configuration Console et Lignes VTY

Console et VTY avec login local, privilege 15, exec-timeout 5, transport SSH.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

4) Sécurité Ports et Désactivation Ports Inutilisés

Sur F0/1 :

```
S1(config)# int f0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
```

Ports inutilisés :

```
S1(config)# int range f0/2-5, f0/7-23, g0/1-2
```

S1(config-if-range)# shutdown

```
S1(config-if)#switchpor
S1(config-if)#switchport port-sec
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security  maximum 1
S1(config-if)#switchport port-security  violation shu
S1(config-if)#switchport port-security  violation shutdown
S1(config-if)#switchport port-security  mac
S1(config-if)#switchport port-security  mac-address sticky
S1(config-if)#no
S1(config-if)#no sh
S1(config-if)#no shutdown
```

```
S1(config)#interface fas
S1(config)#interface fastEthernet 0/
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#spann
S1(config-if)#spanning-tree po
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#span
S1(config-if)#spanning-tree bpdu
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/1 with
BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/1, putting 0/1 in err-disable state


S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

S1(config-if)#
```

Configurations similaires pour S2 et S3.

8. Partie IV : Configuration de la Sécurité WPA2-PSK sur le Point d'Accès

SSID : masterips.

Cryptage AES avec clé "testing1".

Machines wireless déconnectées initialement.

Adaptation WPA2-PSK sur PC-D et Laptop avec clé "testing1".

Pings réussis après reconfiguration.

9. Partie V : Filtrage ACL et Contrôle d'Accès

1) Routeur R3 : ACL pour Réseau 172.16.3.0/24

SSH vérifié depuis TFTP (1.1.1.2) et PC-C.

ACL :

```
R3(config)# access-list 1 permit 172.16.3.0 0.0.0.255
R3(config)# line vty 0 15
R3(config-line)# access-class 1 in
```

Résultat : SSH depuis TFTP échoue, depuis PC-C réussit.

2) Switch S3 : ACL pour PC-C

SSH vérifié depuis R3 et PC-C.

ACL : S3(config)# access-list 2 permit host 172.16.3.3

```
S3(config)# line vty 0 15
S3(config-line)# access-class 2 in
```

Résultat : SSH depuis R3 échoue, depuis PC-C réussit.

10. Partie VI : Configuration d'une ZPF et d'un IPS

1) Configuration ZPF sur R3

Zones :R3(config)# zone security INSIDE

R3(config)# zone security OUTSIDE

Class-map et policy : R3(config)# class-map type inspect match-any INSIDE-PROTOCOLS

R3(config-cmap)# match protocol tcp

R3(config-cmap)# match protocol udp

R3(config-cmap)# match protocol icmp

R3(config)# policy-map type inspect INSIDE-TO-OUTSIDE-POLICY

R3(config-pmap)# class type inspect INSIDE-PROTOCOLS

R3(config-pmap-c)# inspect

Zone-pair : R3(config)# zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE

R3(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-OUTSIDE-POLICY

Attribution interfaces :

R3(config)# int g0/1

R3(config-if)# zone-member security INSIDE

R3(config)# int s0/0/1

R3(config-if)# zone-member security OUTSIDE

Vérification : show zone-pair security, etc. - Trafic INSIDE vers OUTSIDE autorisé.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#zone s
R3(config)#zone security INSIDE
R3(config-sec-zone)#zone security OUTSIDE
R3(config-sec-zone)#class-map type inspect match-any INSIDE-PROTOCOLS
R3(config-cmap)#match protocol tcp
R3(config-cmap)#match protocol udp
R3(config-cmap)#match protocol icmp
R3(config-cmap)#exit
R3(config)#policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
R3(config-pmap)#class type inspect IN
R3(config-pmap)#class type inspect INSIDE-PROTOCOLS
R3(config-pmap-c)#inspect
R3(config-pmap-c)#exit
R3(config-pmap)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE
destination OUTSIDE
R3(config-sec-zone-pair)#exit
R3(config)#zone-pair security INSIDE-TO-OUTSIDE
% Incomplete command.
R3(config)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination
OUTSIDE
R3(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE-
POLICY
R3(config-sec-zone-pair)#interface g0
R3(config-sec-zone-pair)#interface g0/1
R3(config-if)#zone-member security INSIDE
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface s0/1/0
R3(config-if)#zone-member security OUTSIDE
R3(config-if)#exit
R3(config)#exit
R3#
*Jan 04, 14:43:33.4343: SYS-5-CONFIG_I: Configured from console by
R3#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R3#mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash:IPSDIR
```

2) Configuration IPS sur R3

Répertoire IPSDIR : R3# mkdir IPSDIR

Règle IPS :R3(config)# ip ips name IOSIPS

R3(config)# ip ips config location flash:IPSDIR

R3(config)# ip ips signature-category

R3(config-ips-category)# category all

R3(config-ips-category-action)# retired true

R3(config-ips-category)# category ios_ips basic

R3(config-ips-category-action)# retired false

Application R3(config)# int s0/0/1

R3(config-if)# ip ips IOSIPS in

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ips name IOSIPS
R3(config)#ip ips config location flash:IPSDIR
R3(config)#ip ips signature-category
R3(config-ips-category)#cat
R3(config-ips-category)#category all
R3(config-ips-category-action)#retired true
R3(config-ips-category-action)#exit
R3(config-ips-category)#category ios_ips basic
R3(config-ips-category-action)#re
R3(config-ips-category-action)#retired false
R3(config-ips-category-action)#exit
R3(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine
will be scanned

R3(config)#
```

Vérification : show ip ips all – IPS actif avec 1 signature.

```
R3#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:IPSDIR
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0
```

11. Nouvelle Partie VII : Configuration de Base de l'ASA (Basée sur le Lien Fourni)

Cette partie intègre les configurations de base de l'ASA extraites du lien fourni, adaptées à la topologie existante. Elle couvre les paramètres de base, interfaces VLAN, route par défaut, NAT/PAT, ACL, DHCP, AAA/SSH et politique d'inspection MPF. Note : Utiliser VLAN 3 pour DMZ pour cohérence avec le lien ; ajuster si nécessaire pour VLAN 2 dans la topologie originale. Le serveur DMZ (PC-A à 192.168.2.3) est mappé via NAT statique à 209.165.200.227.

1) Paramètres de Base

```
textenable

!<Enter> for password

conf t

hostname CCNAS-ASA

domain-name ccnasecurity.com

enable password ciscoenpa55

clock set 13:52:51 Jan 6 2026
```

2) Configuration des Interfaces (VLANs)

```
ciscoasa#conf t
ciscoasa(config)#hostname ASA
ASA(config)#domain-name ccnasecurity.com
ASA(config)#enable password Admin01
ASA(config)#clock set 13:52:51 Jan 3 2026
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#security-level 100
ASA(config-if)#interface vlan 2
ASA(config-if)#nameif outside
ASA(config-if)#ip address 209.165.200.226 255.255.255.248
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down.Starting a new one
ASA(config-if)#security-level 0
ASA(config-if)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config)#object network inside-net
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic
interface
ASA(config-network-object)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
```

textinterface vlan 1

nameif inside

ip address 192.168.1.1 255.255.255.0

security-level 100

interface vlan 2

nameif outside

ip address 209.165.200.226 255.255.255.248

security-level 0

```
interface vlan 3
ip address 192.168.2.1 255.255.255.0
no forward interface vlan 1
nameif dmz
security-level 70

interface Ethernet0/2
switchport access vlan 3
3) Route par Défaut
route outside 0.0.0.0 0.0.0.0 209.165.200.225
4) Configuration NAT/PAT
object network inside-net
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface

object network dmz-server
host 192.168.2.3
nat (dmz,outside) static 209.165.200.227
5) Configuration ACL
textaccess-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
access-group OUTSIDE-DMZ in interface outside
6) Configuration DHCP
textdhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 209.165.201.2 interface inside
dhcpd enable inside
no dhcpd auto_config outside
```

```
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
ASA(config)#dhcpd dns 209.165.201.2 interface inside
ASA(config)#dhcpd enable inside
need to define address pool range first
dhcpd enable command failed
ASA(config)#username admin password adminpa55
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named
<Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
ASA(config)#ssh timeout 10
ASA(config)#interface vlan 3
ASA(config-if)#ip address 192.168.2.1 255.255.255.0
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down.Starting a new one
ASA(config-if)#no forward interface vlan 1
ASA(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA(config-if)#security-level 70
ASA(config-if)#interface Ethernet0/2
```

7) Authentification AAA

textusername admin password adminpa55

aaa authentication ssh console LOCAL

8) Configuration SSH

textcrypto key generate rsa modulus 1024

no

ssh 192.168.1.0 255.255.255.0 inside

ssh 172.16.3.3 255.255.255.255 outside

```
ssh timeout 10
```

L'ASA commence avec 20% des éléments préconfigurés dans Packet Tracer.

La politique MPF par défaut doit être créée manuellement.

Test d'accès externe au serveur DMZ limité dans Packet Tracer.

Niveaux de sécurité : Inside (100), DMZ (70), Outside (0).

DHCP assigné pour Inside, avec DNS 209.165.201.2.

12. Vérifications et Observations

Tous les pings et SSH ont été testés : Succès où autorisé, échecs où bloqué par ACL/ZPF.

NTP synchronisé : Heures cohérentes.

Syslog : Messages envoyés au serveur.

SSH sécurisé : Pas de Telnet, mots de passe forts.

Observations : Packet Tracer limite certaines commandes (ex. scrypt non disponible sur switches 2960), mais simulations réussies. L'ajout de l'ASA du lien renforce la sécurité avec NAT statique et ACL pour DMZ.

13. Conclusion

Ce TP a permis de maîtriser la sécurisation d'un réseau Cisco, de la configuration de base à des mécanismes avancés. Il souligne l'importance de couches multiples de sécurité (authentification, chiffrement, filtrage). Les configurations ont renforcé la résilience contre les attaques, avec une emphase sur SSH, ACL et ZPF/IPS. L'ajout de la configuration ASA du lien complète le pare-feu avec des fonctionnalités comme NAT statique et inspection ICMP.