Université Sultan Moulay Slimane – EST BM
Prof. Hayat KHALOUFI

FILIÉRE : Bacheler Cybersecurité/ 2025-2026

Travaux pratiques : Sécurité des équipements Réseaux

Topologie du Réseau

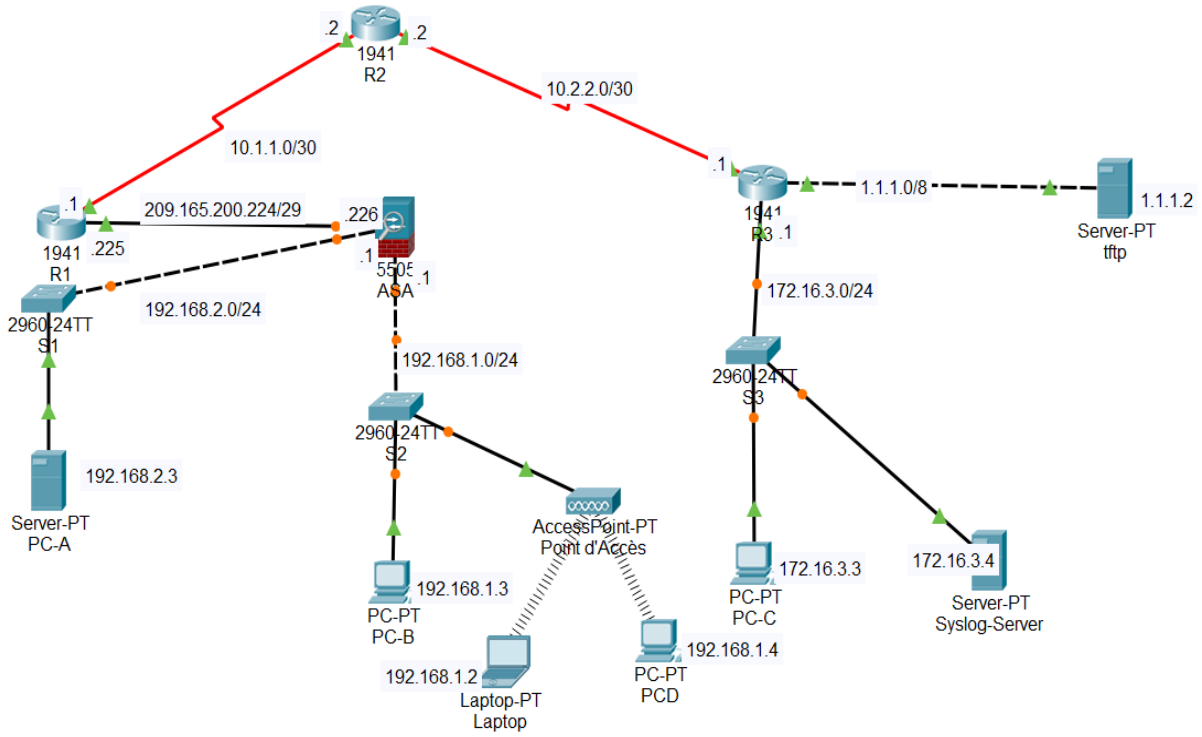


Table d'adressage

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

Les objectifs

TP 1: Configurer les paramètres de base du périphérique

TP 2: Configurer l'accès administratif au routeur sécurisé

• Configurez des mots de passe chiffrés et une bannière de connexion.

• Configurez la valeur du délai d'exécution sur les lignes de la console et VTY.

• Configurez les taux d'échec de connexion et les améliorations de connexion VTY.

• Configurez l'accès Secure Shell (SSH) et désactivez Telnet.

• Configurez l'authentification d'utilisateur, d'authentification et de comptabilité (AAA) locale.

• Sécurisez le routeur contre les attaques de connexion et sécurisez l'image IOS et le fichier de configuration.

• Configurez un serveur NTP de routeur et des clients NTP de routeur.

• Configurez les rapports de syslog du routeur et un serveur syslog sur un hôte local.

TP 3: Configurer un pare-feu de stratégie et un système de prévention des intrusions par zones

• Configurez un pare-feu de stratégie sur zone (ZPF) sur un ISR à l'aide de la CLI.

• Configurez un système de prévention d'intrusion (IPS) sur un ISR à l'aide de la CLI.

TP 4: Commutateurs réseau sécurisés

• Configurez des mots de passe et une bannière de connexion.

• Configurez l'accès VLAN de gestion.

• Ports d'accès sécurisés.

• Protégez-vous contre les attaques STP (Spanning Tree Protocol).

• Configurez la sécurité du port et désactivez les ports inutilisés.

TP 5: Configurer les paramètres de base ASA et le pare-feu

• Configurez les paramètres de base, les mots de passe, la date et l'heure.

• Configurez les interfaces VLAN interne et externe.

• Configurez la traduction d'adresse de port (PAT) pour le réseau interne.

• Configurez un serveur DHCP (Dynamic Host Configuration Protocol) pour le réseau interne.

• Configurez l'accès administratif via Telnet et SSH.

• Configurez une route statique par défaut pour le dispositif ASA (Adaptive Security Appliance).

• Configurez l'authentification d'utilisateur AAA local.

• Configurez une zone démilitarisée avec un NAT et une ACL statiques.

• Vérifiez la fonctionnalité de traduction d'adresse et de pare-feu.

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

TP 7 (à rendre): Configuration de l'accès à distance VPN SSL SSL sans client ASA avec ASDM

• Configurez un VPN SSL d'accès distant à l'aide de l'ASDM (Cisco Adaptive Security Device Manager).

• Vérifiez l'accès VPN SSL au portail.

TP 8 (à rendre) : Configurer un VPN de site à site entre l'ASA et l'ISR

• Configurez un VPN site à site IPsec entre ASA et R3 à l'aide de ASDM et de la CLI.

• Activez et vérifiez le tunnel VPN site à site IPsec entre l'ASA et le serveur R3.

Partie I : Configuration de base des équipements réseau

1) Câblage réseau et mise en place d'infrastructure

Dans cette étape vous allez mettre en place l'infrastructure de la figure ci-dessus. Dans Packet tracer :

- Sélectionner un firewall de type ASA 5505
- Sélectionner 3 routeurs de type 1941
- Pour chaque routeur ajouter une interface de type HWIC-2T (éteindre l'équipement avant l'ajout de l'interface)
- Sélectionner 3 switchs de type 2960
- Sélectionner 1 point d'accès de type AP-PT
- Sélectionner 4 PC de type PC-PT
- Pour le PC-D et le Laptop ajouter des cartes wireless de types PT-HOST-NM-1W et PT-LAPTOP-NM-1W respectivement (éteindre les machines avant l'ajout des cartes)
- Sélectionner un Laptop
- Connectez les périphériques, comme indiqué dans le diagramme de topologie, et câblez si nécessaire. (Choisir câblage automatique)

2) Configuration basique des routeurs

- Configurez les noms des routeurs, comme indiqué dans la topologie.

```
Router>enable
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

- Configurez les adresses IP des interfaces, comme indiqué dans le tableau d'adressage IP.

Routeur R1

➢ Interface GigabitEthernet 0/0

```
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.248
```

```
R1(config-if)#no shutdown
```

- Interface Serial 0/0/0

```
R1(config)#int serial 0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
```

- Interface Loopback1

```
R1(config)#interface loopback 1
R1(config-if)#ip address 172.20.1.1 255.255.255.0
```

Routeur R2

- Interface Serial 0/0/0

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
```

- Interface Serial 0/0/1

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
```

Routeur R3

- Interface GigabitEthernet 0/1

```
Router>en
Router#conf t
Router(config)#hostname R3
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip address 172.16.3.1 255.255.255.0
```

- Interface Serial 0/0/1

```
R3(config)#interface serial 0/0/1
```

```
R3(config-if)#ip address 10.2.2.1 255.255.255.252
```

- Désactiver DNS lookup sur chaque routeur.

```
R1(config)# no ip domain-lookup
```

3) Configuration du routage statique par défaut sur R1, R2 et R3

- Configurez une route statique par défaut de R1 à R2 et de R3 à R2.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

- Configurez les routes statiques de R2 vers le sous-réseau de R1 Fa0/0-to-ASA et vers le réseau LAN de R3.

```
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
```

4) Configuration de base des switchs et du point d'accès

- Configurez les noms des switchs, comme indiqué dans la topologie.

```
Switch>enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

- Configurez l'adresse de management du VLAN 1 sur chaque switch, comme indiqué dans le tableau d'adressage.

```
S1(config)# interface vlan 1
S1(config)# ip address 192.168.2.11 255.255.255.0
S1(config)# no shutdown

S2(config)# interface vlan 1
S2(config)# ip address 192.168.1.11 255.255.255.0
S2(config)# no shutdown

S3(config)# interface vlan 1
S3(config)# ip address 172.16.3.11 255.255.255.0
```

```
S3(config)# no shutdown
```

- Configurez la passerelle IP par défaut pour chacun des trois switchs.

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

S2(config)# ip default-gateway 192.168.1.1

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

- Désactiver DNS lookup sur chaque switch.

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

- Configurer la point d'accès avec un SSID=masterips
- Tester les pings entre les différents PCs wirless et wired

5) Configurez les paramètres IP des PCs et du laptop.

Configurez une adresse IP statique, un masque de sous-réseau et une passerelle par défaut pour chaque PC, comme indiqué dans le tableau Adressage IP.

6) Vérifiez la connectivité entre PC-C et R1 G0 / 0.

```
PC-C:\> ping 209.165.200.225
```

7) Enregistrez la configuration courante de base pour chaque routeur et commutateur.

Partie II : Sécurité d'accès aux routeurs

1) Configuration de paramètres pour R1 et R3

- Configurez une longueur de mot de passe minimale de 10 caractères

```
R1(config)# security passwords min-length 10
R3(config)# security passwords min-length 10
```

Chiffrement des mots de passe en clair.

```
R1(config)# service password-encryption
R3(config)# service password-encryption
```

- Configurez une bannière d'avertissement de connexion.

Configurez un avertissement destiné aux utilisateurs non autorisés avec une bannière MOTD (Message of the Day) indiquant: **Unauthorized access strictly prohibited and prosecuted to the full extent of the law!.**

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R3(config)# banner motd $Unauthorized access strictly prohibited!$
```

- Configurer enable secret password

Utilisez **cisco12345** comme mot de passe d'activation secret. Utilisez le type de cryptage le plus puissant disponible.

```
R1(config)# enable algorithm-type scrypt secret cisco12345
R3(config)# enable algorithm-type scrypt secret cisco12345
```

- Configurez la base de données d'utilisateurs locaux.

Créez un compte d'utilisateur local Admin01 avec un mot de passe secret Admin01pa55 et un niveau de privilège de 15. Utilisez le type de cryptage le plus puissant disponible.

```
R1(config)# username Admin01 privilege 15 algorithm-type scrypt secret
Admin01pa55
R3(config)# username Admin01 privilege 15 algorithm-type scrypt secret
Admin01pa55
```

- Activer les services aaa

```
R1(config)# aaa new-model
R3(config)# aaa new-model
```

- Implémenter les services AAA en utilisant la base de données locale

Créez la liste des méthodes d'authentification de connexion par défaut. Utilisez l'authentification locale sensible à la casse comme première option et le mot de passe enable comme alternative à utiliser en cas d'erreur liée à l'authentification locale.

```
R1(config)# aaa authentication login default local-case enable
R3(config)# aaa authentication login default local-case enable
```

- Configurer la ligne de console

Configurez la ligne de la console pour l'accès de niveau de privilège 15 lors de la connexion. Définissez la valeur exec-timeout pour vous déconnecter après 15 minutes d'inactivité. Empêcher les messages de la console d'interrompre la saisie des commandes

```
R1(config)# line console 0
R1(config-line)# privilege level 15
R1(config-line)# exec-timeout 15 0
R1(config-line)# logging synchronous

R3(config)# line console 0
R3(config-line)# privilege level 15
R3(config-line)# exec-timeout 15 0
R3(config-line)# logging synchronous
```

- Configurez les lignes VTY

Configurez les lignes VTY pour l'accès de niveau de privilège 15 lors de la connexion. Définissez la valeur exec-timeout pour déconnecter une session après 15 minutes d'inactivité. Autoriser l'accès à distance à l'aide de SSH uniquement.

```
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

R3(config)# line vty 0 4
R3(config-line)# privilege level 15
R3(config-line)# exec-timeout 15 0
R3(config-line)# transport input ssh
```

- Configurez le routeur pour enregistrer les activités de connexion.

Configurez le routeur pour générer des messages de journalisation du système pour les tentatives de connexion réussies et infructueuses. Configurez le routeur pour qu'il enregistre chaque connexion réussie. Configurez le routeur pour qu'il enregistre chaque seconde tentative de connexion infructueuse.

```
R1(config)# login on-success log
R1(config)# login on-failure log

R3(config)# login on-success log
R3(config)# login on-failure log
```

- Émettez la commande show login. Quelles informations supplémentaires sont affichées ?

Activer l'accès http

Activer le serveur HTTP sur R1 pour simuler une cible Internet pour des tests ultérieurs

2) **Configurez le serveur SSH sur R1 et R3**

- Configurez un nom de domaine **computersecurity.ma**

```
R1(config)# ip domain-name computersecurity.ma
R3(config)# ip domain-name computersecurity.ma
```

- Générez la paire de clés RSA

```
R1(config)# crypto key generate rsa general-keys modulus 1024
R3(config)# crypto key generate rsa general-keys modulus 1024
```

- Configurez SSH v2

```
R1(config)# ip ssh version 2
R3(config)# ip ssh version 2
```

- Configurez les délais d'expiration SSH et les paramètres d'authentification.

Les délais d'expiration SSH et les paramètres d'authentification par défaut peuvent être modifiés pour être plus restrictifs. Fixez le délai d'attente SSH (time-out) à 90 secondes et le nombre de tentatives d'authentification à 2.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2

R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
```

- Vérifiez la connectivité SSH vers R1 et R3 à partir de PC-C.

Lancez le client SSH sur PC-C, entrez l'adresse IP R1 S0/0/0 (10.1.1.1) et connectez-vous en tant que **Admin01** avec le mot de passe **Admin01pa55**.

Tapez la commande **show run** à partir de la session SSH sur PC-C. La configuration du routeur R1 devrait être affichée.

3) **Sécuriser contre les attaques de connexion et sécuriser l'IOS et le fichier de configuration de R1**

- Configurer une sécurité de connexion avancée

Si un utilisateur fait deux tentatives de connexion infructueuses dans un délai de 30 secondes, désactivez les connexions pendant une minute. Enregistrez toutes les tentatives de connexion infructueuses

```
R1(config)# login block-for 60 attempts 2 within 30
R1(config)# login on-failure log
```

Sécurisez l'image de Cisco IOS et archivez une copie de la configuration en cours.

La commande **secure boot-image** active la résilience des images Cisco IOS, qui masque le fichier à partir du répertoire et les commandes **show**. Le fichier ne peut pas être visualisé, copié, modifié ou supprimé à l'aide de commandes en mode EXEC. (Il peut être visualisé en mode ROMMON.)

ROMmon est un système de restauration du routeur Cisco en cas de problème majeurs ne pouvant être réparé. Ainsi ce sera grâce à lui que nous pourrons pourvoir passer de l'adresse **0x2102** à l'adresse **0x2142** pouvoir réinitialiser le mot de passe.

(https://www.supinfo.com/articles/single/1171-reinitialiser-mot-passe-votre-routeur-cisco)

```
R1(config)# secure boot-image
```

La commande **secure boot-config** prend une snapshot de la configuration du routeur en cours d'exécution et l'archive de manière sécurisée dans la mémoire flash.

```
R1(config)# secure boot-config
```

Vérifiez que votre image et votre configuration sont sécurisées.

```
R1# show secure bootset
```

Quel est le nom du fichier de configuration en cours d'exécution archivé et sur quoi est basé le nom?

Restaurez l'IOS et les fichiers de configuration sur les paramètres par défaut.

Vous avez vérifié les paramètres de Secure IOS et du fichier de configuration. A présent, utilisez les commandes **no secure boot-config** et **no secure boot-config** pour restaurer les paramètres par défaut de ces fichiers.

```
R1(config)# no secure boot-image
R1(config)# no secure boot-config
```

4) Configurer une source de temps synchronisée à l'aide de NTP

- Configurez R2 en tant que serveur NTP master à l'aide des commandes Cisco IOS.

R2 est le serveur NTP maître dans ce TP. Tous les autres routeurs et commutateurs en tirent l'heure, directement ou indirectement. Pour cette raison, vous devez vous assurer que R2 est correctement configuré en UTC.

Utilisez la commande **show clock** pour afficher l'heure actuelle définie sur le routeur.

```
R2# show clock
```

```
*1:21:28.517 UTC Mon Mar 1 1993
```

- Utilisez la commande **clock set** time pour régler l'heure sur le routeur.

```
R2#clock set 11:51:30 Nov 11 2019
```

- Configurez l'authentification NTP en définissant le numéro de clé d'authentification 1 avec hachage md5 et un mot de passe **NTPpassword**. Le mot de passe est sensible à la casse.

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

- Configurez la clé de confiance qui sera utilisée pour l'authentification sur R2.

```
R2(config)# ntp trusted-key 1
```

- Activez la fonctionnalité d'authentification NTP sur R2.

```
R2(config)# ntp authenticate
```

- Configurez R2 en tant que NTP master à l'aide de la commande **ntp master** *stratum-number* en mode de configuration globale. Le numéro de la strate (*stratum-number*) indique la distance par rapport à la source d'origine. Pour ce TP, utilisez un nombre de strates de 1 sur R2. Lorsqu'un périphérique apprend l'heure d'une source NTP, son numéro de strate devient supérieur à celui de sa source.

```
R2(config)# ntp master 1
```

- Configurez R1 et R3 en tant que clients NTP à l'aide de la CLI.

```
R1(config)# ntp authentication-key 1 md5 NTPpassword
R3(config)# ntp authentication-key 1 md5 NTPpassword
```

- Configurez la clé de confiance qui sera utilisée pour l'authentification. Cette commande offre une protection contre la synchronisation accidentelle du périphérique avec une source de temps non approuvée.

```
R1(config)# ntp trusted-key 1
R3(config)# ntp trusted-key 1
```

- Activer la fonctionnalité d'authentification NTP.

```
R1(config)# ntp authenticate
```

```
R3(config)# ntp authenticate
```

- R1 et R3 deviendront des clients NTP de R2. Utilisez la commande de mode de configuration globale **ntp server** *hostname*. Utilisez l'adresse IP série de R2 pour le hostname. Exécutez la commande **ntp update-calendar** sur R1 et R3 pour mettre à jour périodiquement le calendrier avec l'heure NTP.

```
R1(config)# ntp server 10.1.1.2
R1(config)# ntp update-calendar

R3(config)# ntp server 10.2.2.2
R3(config)# ntp update-calendar
```

- Utilisez la commande **show ntp associations** pour vérifier que R1 a établi une association avec R2. L'association NTP peut prendre un certain temps pour se former.

```
R1#sh ntp associations

address ref clock st when poll reach delay offset disp
*~10.1.1.2 127.127.1.1 1 14 16 377 2.00 0.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

- Vérifiez l'heure sur R1 et R3 après avoir établi des associations NTP avec R2.

```
R1# show clock
12:20:55.84 UTC Mon Nov 11 2019
```

5) Configurer la prise en charge de Syslog sur R3 et un serveur Syslog

- Ajouter un serveur Syslog à l'interface Fa0/3 du Switch S3. (donner comme adressage 172.16.3.4 au nouveau serveur).
- Vérifier le ping entre le serveur syslog et l'interface d'adresse IP 172.16.3.1 du routeur.
- Configurez R3 pour enregistrer les messages sur le serveur syslog à l'aide de la CLI.

NTP a été configuré dans la tâche 4 pour synchroniser l'heure sur le réseau. L'affichage de l'heure et de la date correctes dans les messages syslog est essentiel lorsque vous utilisez syslog pour surveiller un réseau. Si l'heure et la date correctes d'un message ne sont pas connues, il peut être difficile de déterminer quel événement réseau a provoqué le message.

- Vérifiez que le service d'horodatage pour la journalisation est activé sur le routeur à l'aide de la commande **show run**. Utilisez la commande **service timestamps log datetime msec** si le service d'horodatage n'est pas activé.

```
R3(config)# service timestamps log datetime msec
```

- Configurez le service syslog sur le routeur pour envoyer des messages syslog au serveur syslog.

```
R3(config)# logging host 172.16.3.4
```

- Configurez le niveau de gravité de la journalisation sur R3

Les interruptions de journalisation peuvent être configurées pour prendre en charge la fonction de journalisation. Une interruption est un seuil qui déclenche un message de journal. Le niveau des messages de journalisation peut être ajusté pour permettre à l'administrateur de déterminer quels types de messages sont envoyés au serveur syslog. Les routeurs prennent en charge différents niveaux de journalisation. Les huit niveaux vont de 0 (urgences), ce qui indique que le système est instable, à 7 (débogage), qui envoie des messages contenant des informations sur le routeur.

Remarque: Le niveau par défaut pour syslog est 6 (journalisation informationnelle). La journalisation par défaut de la console et du moniteur est 7 (débogage)

Les niveaux de journalisation sont :

- **Emergency (severity 0)**—The system is unusable
- **Alert (severity 1)**—Immediate action is needed
- **Critical (severity 2)**—Critical condition
- **Error (severity 3)**—Error condition
- **Warning (severity 4)**—Warning condition
- **Notification (severity 5)**—Normal but significant condition
- **Informational (severity 6)**—Informational message
- **Debugging (severity 7)**—Debugging message

Dans Packet tracer juste le niveau 7 existe, donc c'est lui qu'on va configurer.

Utilisez la commande **logging rtap** pour définir le niveau de gravité de R3 sur 7 (debugging).

```
R3(config)# logging trap debugging
```

Utilisez la commande **show logging** pour voir le type et le niveau de journalisation activés.

```
R3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.
```

```
Console logging: level debugging, 14 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 14 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level debugging, 14 message lines logged
Logging to 172.16.3.4 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
3 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
R3#
```

Partie III : Configuration de la sécurité des switchs

1) Configuration de sécurité basique sur S1

- Désactiver http et https servers

```
S1(config)# no ip http server
S1(config)# no ip http secure-server
```

- Utilisez un mot *enable* de **cisco12345**. Utilisez le cryptage le plus puissant disponible.

```
S1(config)# enable secret cisco12345
```

La version 15.3 de l'OS cisco n'est pas disponible sur Packet Tracer pour les Switch 2960, donc on ne peut pas utiliser la commande *enable algorithm-type scrypt secret cisco12345*

- Faire le chiffrement des mots de passe en clair

```
S1(config)# service password-encryptio
```

- Configurez un avertissement pour les utilisateurs non autorisés avec une bannière MOTD indiquant "**Unauthorized access strictly prohibited!**".

```
S1(config)# banner motd $Unauthorized access strictly prohibited!$
```

2) Configuration de SSH sur S1

- Configurer le nom de domaine **computersecurity.ma**

```
S1(config)# ip domain-name computersecurity.ma
```

- Créez un compte d'utilisateur local Admin01 avec un mot de passe secret Admin01pa55 et un niveau de privilège de 15. Utilisez le type de cryptage le plus puissant disponible.

```
S1(config)# username Admin01 privilege 15 secret Admin01pa55
```

- Générez la paire de clés RSA

```
S1(config)# crypto key generate rsa general-keys modulus 1024
```

- Configurer SSH v2

```
S1(config)# ip ssh version 2
```

- Configurez les délais d'expiration SSH et les paramètres d'authentification.

Les délais d'expiration SSH et les paramètres d'authentification par défaut peuvent être modifiés pour être plus restrictifs. Fixez le délai d'attente SSH (time-out) à 90 secondes et le nombre de tentatives d'authentification à 2.

```
S1(config)# ip ssh time-out 90
S1(config)# ip ssh authentication-retries 2
```

3) Configuration de la console et des lignes VTY

- Configurez la ligne de la console pour l'accès de niveau de privilège 15 lors de la connexion. Définissez la valeur exec-timeout pour déconnecter une session après 5 minutes d'inactivité. Empêcher les messages de la console d'interrompre la saisie de la commande.

```
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
```

- Configurez les lignes VTY pour l'accès de niveau de privilège 15 lors de la connexion. Définissez la valeur exec-timeout pour déconnecter une session après 5 minutes d'inactivité. Autoriser l'accès à distance à l'aide de SSH uniquement.

```
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
```

4) Configuration de la sécurité des ports et désactivation des ports inutilisés.

- Désactiver le trunking sur le port F0/1

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode access
```

- Activer PortFast sur F0/1

```
S1(config-if)# spanning-tree portfast
```

- Activer bpduguard sur F0/1

```
S1(config-if)# spanning-tree bpduguard enable
```

- Appliquez la sécurité du port au port F0/1, en définissant le maximum des adresses MAC autorisées sur 1 et en cas de violation le port se met à shutdown. L'apprentissage des adresses MAC se fait dynamiquement.

```
S1(config-if)# shutdown
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
```

```
S1(config-if)# no shutdown
```

- Désactiver les ports inutilisés sur S1

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

5) Sauvegarder la config du switch S1 et refaire le même travail de cette partie pour les switch S2 et S3.

Partie IV : Configuration de la sécurité WPA2-PSK sur le point d'accès

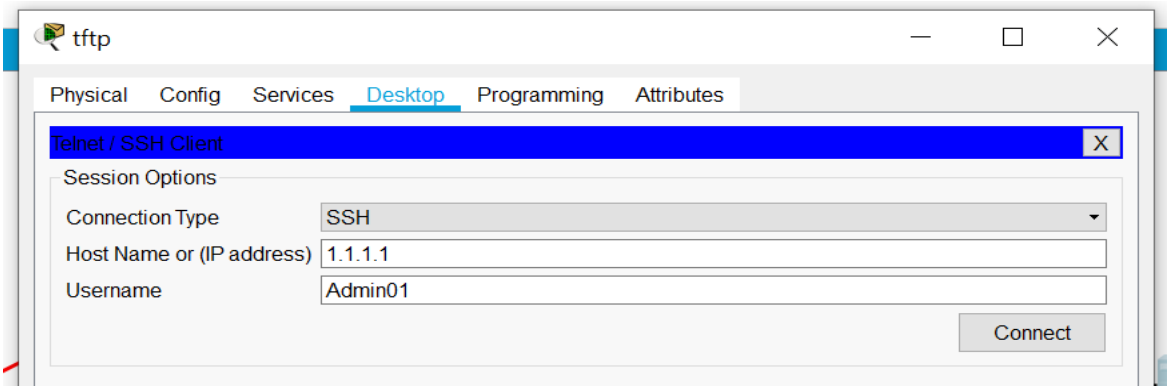
- Configurer le SSID : **masterips**
- Configurez le cryptage AES avec ***testing1*** comme clé
- Constatez que les deux machines wireless ne sont plus connectées
- Adaptez les paramètres de sécurité sur les deux machines wireless (même stratégie WPA2-PSK evec **testing1** comme clé)
- Testez de nouveaux des pings entre l'ensemble des ressources du réseau

Partie V : Filtrage ACL et contrôle d'accès

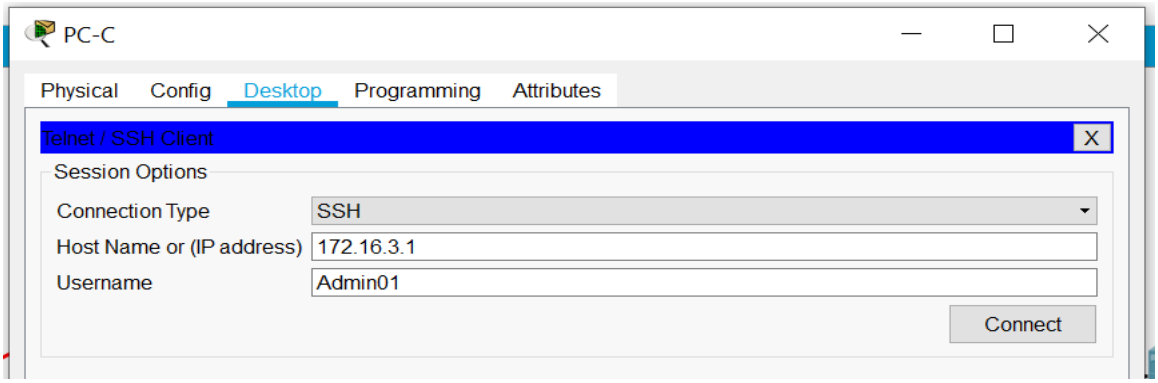
Dans cette partie nous allons configurer des ACL standards pour limiter l'accès SSH au routeur R3 et au Switch S3.

1) Routeur R3 : Autoriser l'accès à partir du réseau 172.16.3.0/24

- Vérifier qu'on est capable de se connecter en SSH au routeur R3 (interface 1.1.1.1) à partir du serveur TFTP (1.1.1.2)



- Vérifier qu'on est capable de se connecter en SSH au routeur R3 (interface 172.16.3.1) à partir de la machine PC-C.



- Au niveau du routeur R3 créez une ACL standard numérotée 1 permettant d'autoriser le réseau 172.16.3.0/24.

```
R3(config)# access-list 1 permit 172.16.3.0 0.0.0.255
```

- Appliquer cette ACL pour ne permettre l'accès SSH au routeur R3 qu'à partir du réseau172.16.3.0/24.

```
R3(config)# line vty 0 15
R3(config-line)# access-class 1 in
```

- Essayer de se connecter de nouveau en SSH à partir du serveur TFTP(1.1.1.2) et de la machine PC-C. Qu'est-ce que vous remarquez ?

2) Switch S3 : Autoriser l'accès juste à partir de la machine PC-C

- Vérifier qu'on est capable de se connecter en SSH au Switch S3 à partir du routeur R3

```
R3# ssh –l Admin01 172.16.3.11
```

- Vérifier aussi qu'on est capable de se connecter au Switch S3 à partir de la machine PC-C.
- Au niveau du Switch S3 créez une ACL standard numérotée 2 permettant d'autoriser la machine PC-C.

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

- Appliquer cette ACL pour ne permettre l'accès SSH au Switch S3 qu'à partir du PC-C.

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

- Essayer de se connecter de nouveau en SSH à partir du routeur R3 puis à partir de la machine PC-C. Qu'est-ce que vous remarquez ?

Partie VI : Configurer une ZPF et un IPS

Dans cette partie, vous allez configurer une ZPF et un IPS sur R3 à l'aide de la CLI.

1) Configurer une ZPF sur R3 à l'aide de la CLI

- Création des zones de sécurité
- Créez les zones de sécurité INSIDE et OUTSIDE.

```
R3(config)# zone security INSIDE
R3(config)# zone security OUTSIDE
```

- Créez une class-map d'inspection pour faire correspondre le trafic à autoriser de la zone INSIDE à la zone OUTSIDE. Parce que nous faisons confiance à la zone INSIDE, nous autorisons tous les protocoles principaux. Utilisez le mot clé **match-any** pour indiquer au routeur que les instructions de protocole de correspondance suivantes seront considérées comme une correspondance (matching) réussie. Cela entraîne l'application d'une policy. Match pour les paquets TCP, UDP ou ICMP.

```
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
```

- Créez une policy-map d'inspection nommée **INSIDE-TO-OUTSIDE-POLICY**. Liez la class-map **INSIDE-PROTOCOLS** à la policy-map. Tous les paquets correspondants à la class-map **INSIDE-PROTOCOLS** seront inspectés.

```
R3(config)# policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
R3(config-pmap)# class type inspect INSIDE-PROTOCOLS
R3(config-pmap-c)# inspect
```

- Créez une zone de paire appelée **INSIDE-TO-OUTSIDE** qui autorise le trafic initié du réseau interne vers le réseau externe mais ne permet pas au trafic en provenance du réseau externe d'atteindre le réseau interne.

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

- Appliquez la policy-map à la zone-pair

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

- Attribuez l'interface G0/1 de R3 à la zone de sécurité **INSIDE** et l'interface S0/0/1 à la zone de sécurité **OUTSIDE**.

```
R3(config)# interface g0/1
R3(config-if)# zone-member security INSIDE
R3(config)# interface s0/0/1
R3(config-if)# zone-member security OUTSIDE
```

- Vérifiez votre configuration ZPF à l'aide des commandes **show zone-pair security**, **show policy-map type inspect zone-pair sessions**, et **show zone security**.

2) Configuration de IPS sur R3 à l'aide de CLI

- Vérifiez ou créez le répertoire IPS (**IPSDIR**) dans la mémoire flash du routeur R3. À partir de la CLI R3, affichez le contenu de la mémoire flash et vérifiez si le répertoire **IPSDIR** existe.

```
R3# show flash
```

- Si le répertoire **IPSDIR** n'est pas trouvé, créez-le en mode d'exécution privilégié à l'aide de la commande **mkdir**.

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

- Créez une règle IPS et nommez-la IOSIPS.

```
R3(config)# ip ips name IOSIPS
```

- Définissez l'emplacement de stockage de la signature IPS sur le répertoire IPSDIR que vous avez créé à l'étape précédente.

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

- Configurez IOS IPS pour utiliser l'une des catégories de signature prédéfinies.

```
R3(config)# ip ips signature-category
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)# retired false
R3(config-ips-category-action)# exit
```

```
R3(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>


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 b
e scanned
```

- Appliquez la règle IPS au trafic entrant vers l'interface S0/0/1 de R3.

```
R3(config)# interface serial0/0/1
R3(config-if)# ip ips IOSIPS in
```

- Utilisez la commande **show ip ips all** pour afficher le résumé de l'état de la configuration IPS.

```
R3#sh 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
```

```
IPS Packet Scanning and Interface Status
IPS Rule Configuration
IPS name IOSIPS
IPS fail closed is disabled
IPS deny-action ips-interface is false
Fastpath ips is enabled
Quick run mode is enabled
Interface Configuration
Interface Serial0/0/1
Inbound IPS rule is IOSIPS
Outgoing IPS rule is not set

IPS Category CLI Configuration:
Category all
Retire: True
Category ios_ips basic
Retire: False
R3#
```