Intitulé de l'épreuve : 21/02/19 Réseaux et Télécommunications

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 1

1. 802.11 : défini la norme Wifi (sécurisation, signal)

2. 4 premières couches du modèle OSI :

	Couche	PDUs
1	Physique	PPDU
2	Données	Frame
3	Réseau	Paquet
4	Transport	Segment

(IPv4)

3. ARP : Assymetric Request Protocol → associe une @ MAC à une @ IP / couche 2 vers 3

DNS : Domain Name Service
→ associe un nom à une adresse IP.

SFTP : Secure File Transfert Protocol
→ Version sécurisée du FTP, protocole de transfert de fichier

N° 11.3

NTP : Network Time Protocol

→ permet de gérer un système client/server de gestion de l'heure afin que tous les terminaux soient à la même heure (serveur de temps de référence)

4. 192.168.1.0/24

→ 2 sous-réseaux de 60 machines :

192.168.1.0/26

- 192.168.1.0 : @ réseau
- /26 : masque
- 192.168.1.63 : @ diffusion
- .1 à .62 : 62 hôtes

192.168.1.64/26

- 192.168.1.64 : @ réseau
- /26 : masque
- 192.168.1.127 : @ diffusion
- .65 à .126 : 62 hôtes

→ 1 sous-réseau d'au plus 124 machines

192.168.1.128/25

- 192.168.1.128 : @ réseau
- /25 : masque
- 192.168.1.255 : @ diffusion
- .129 à .254 : 126 hôtes

5. IDS : Intrusion Detection System

IPS : Intrusion Prevention System

IDS sert à détecter quand une intrusion non autorisée a été réalisée

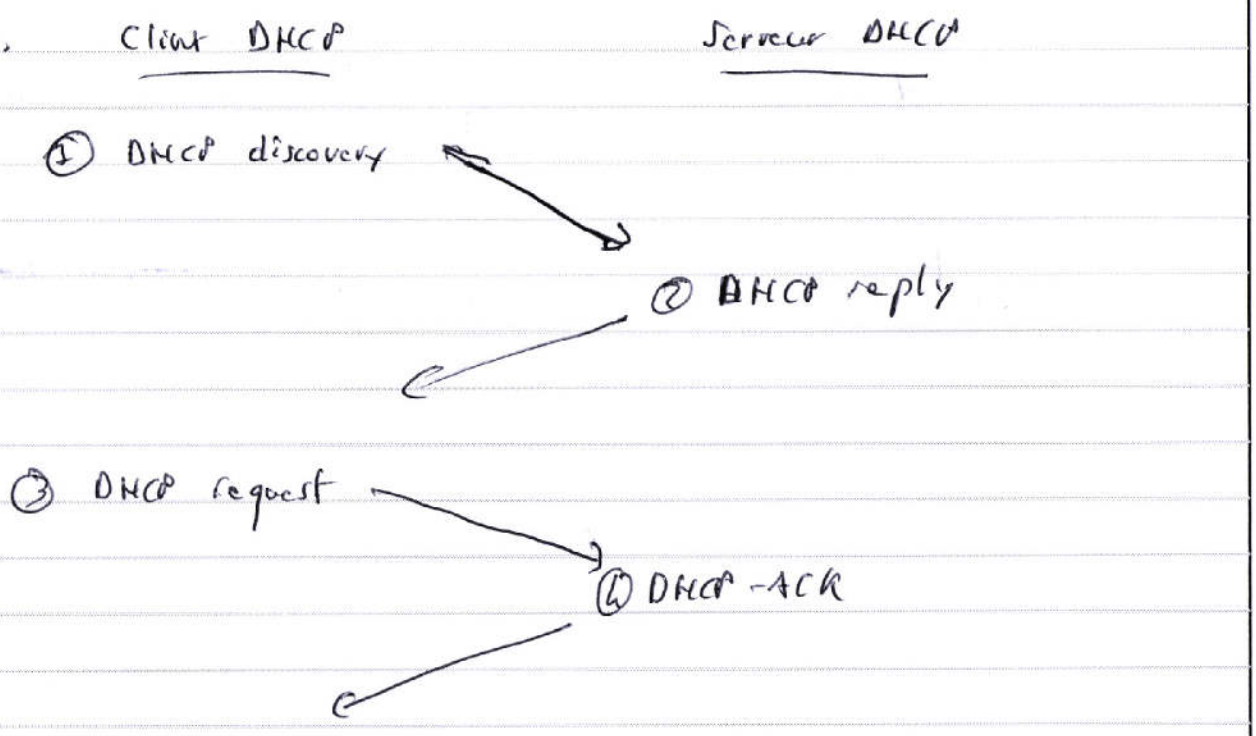
IPS sert à empêcher qu'une intrusion ait lieu

N° .11..3

Ce sont deux systèmes complémentaires.
L'IPS se situe en amont de l'attaque afin d'éviter sa survenance.
L'IDS lui analyse l'état du système afin de savoir si un utilisateur aurait un comportement anormal sur le système.

6. Il existe des requêtes DNS de type A et type CNAME.
Le type A associe un nom à une IP
Le type CNAME associe un alias à un nom

7.



① Le client fait du broadcast pour demander une IP sur le réseau

② Les serveurs DHCP présents sur le réseau y répondent

③ Le client DHCP prévient le serveur qu'il a pris l'IP proposée

④ Le serveur DHCP informe le client que son IP est bien réservée.

N° 2.1.3

La station choisit le premier serveur DHCP qui lui répond.

Le DHCP spoofing est un mécanisme qui permet de se faire passer pour le serveur DHCP.
Un pirate peut l'utiliser pour donner des adresses IP erronées à des clients

On peut s'en prémunir en mettant des sécurités sur le port des switchs.
On identifie les ports clients et serveurs :
si un client veut faire du DHCP spoofing, son "DHCP reply" sera poubellisé par le switch.

P) d) adresse physique machine ~~initiant l'échange~~ répondant
00:0a:67:a3:4a:00

b) adresse physique de la machine ~~ayant répondu~~ initiant l'échange
00:01:02:6F:5e:96.

a) adresse IP de la machine ayant initié l'échange : 132.0.0.1
→ classe B

c) adresse IP de la machine ayant répondu :
194.0.0.1
→ classe C

e) le TTL est passé de 64 à 58. donc on a traversé 6 routeurs

F) La fin du paquet ne coincide pas avec la fin de la trame car il faut rajouter les bits de bourrage à 0.

g) On voit que le champ protocole est à 1 donc c'est de l'ICMP, commande ping

N° 113.

Intitulé de l'épreuve : 21/02/19 Réseaux et télécommunications

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 2

1. A1 ne peut pas joindre C1 car il manque une route au routeur A1.

D 192.168.5.0/24 via 10.1.2.1, Tunnel 1

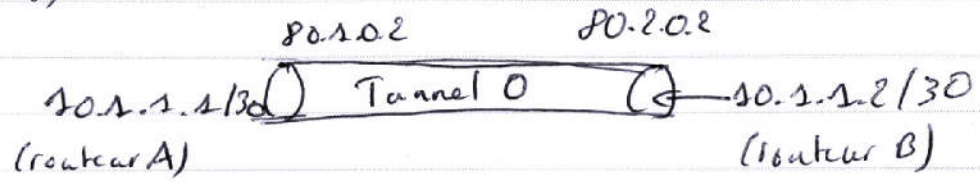
Le soucis vient de C1 qui n'annonce pas son réseau dans le routeur eigrp 100.

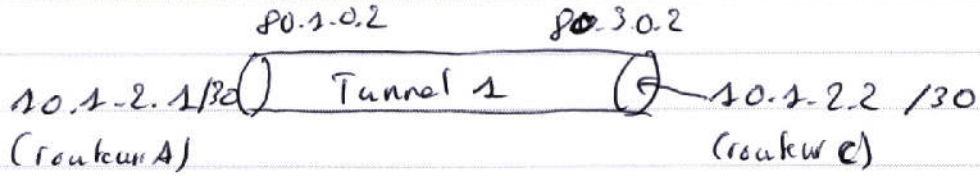
2) L'IP du tunnel 2 du routeur du site D n'est pas correcte.
Elle doit être en 10.4.1.2

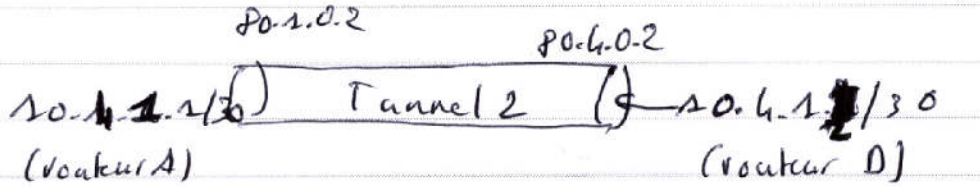
conf: interface Tunnel 2
ip address 10.4.1.2 255.255.255.252

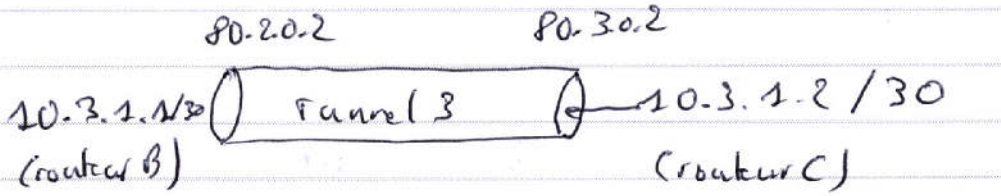
N° 21.3

4)


80.1.0.2
80.2.0.2
10.1.1.1/30
Tunnel 0
10.1.1.2/30
(routeur A)
(routeur B)


80.1.0.2
80.3.0.2
10.1.2.1/30
Tunnel 1
10.1.2.2 /30
(routeur A)
(routeur C)


80.1.0.2
80.4.0.2
Tunnel 2
(routeur A)
(routeur D)


80.2.0.2
80.3.0.2
10.3.1.1/30
Tunnel 3
10.3.1.2 /30
(routeur B)
(routeur C)

N° 2.1.3

3) configuration du routeur B.

```
interface Tunnel 0
 ip address 10.1.1.2 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/0
 tunnel destination 80.1.0.2
!
interface Tunnel 3
ip address 10.3.1.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet 0/0
tunnel destination 80.3.0.2
!
interface GigabitEthernet 0/0
ip address 80.2.0.2 255.255.255.252
duplex auto
speed auto.
!
interface FastEthernet 0/0/0
 switchport access vlan 2
  switchport mode access
  switchpat nonegociate.
!
 interface FastEthernet 0/0/1
  switchpat access vlan 3
   switchpat mode access
    switchpat nonegociate.
!
interface Vlan 2
 ip address 192.168.3.254 255.255.255.0
!
interface Vlan 3
 ip address 192.168.4.254 255.255.255.0
!
```

```
router eigrp 90
 network 10.1.1.0  0.0.0.3
 network 192.168.3.0
 network 10.3.1.0  0.0.0.3
!
router eigrp 100
 network 10.3.1.0 0.0.0.3
 network 192.168.4.0
```

B1 vers A1 etc1

B2 vers C1

Intitulé de l'épreuve : 21/02/19 Réseaux et Télécommunications

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 3

1) durcir les configurations de vos équipements réseaux
   ↳ connexion par radius
   ↳ modification du mot de passe admin
   ↳ mettre en place des ACLs

configuration :
- " aaa authentication radius IP_Radius mdp-clé "
- " aaa user admin password NOTREMOTPASSE "
- ip access-list standard Administrateurs_
  10 réseau_confiance masque accept
  20 deny all

2) mettre en place un système permettant de contrôler les différents équipements qui se connectent au réseau.

   ↳ mettre en place une sécurité par adresse MAC sur les ports des switchs
   ↳ apprentissage d'une ou deux adresses MAC (Téléphone + PC) puis blocage si 2nd MAC non reconnue.

→

N° 3.13.

↳ configuration : interface X/x mac-security @mac
↑
reconnue

=> il faudra être prévenu avant tout déménagement afin de désactiver cette sécurité en amont.

3) mettre en place un outil de supervision centralisé
↳ se baser sur du pooling SNMP
↳ recevoir les traps émises par les équipements
↳ dessiner la carte des équipements avec les différents liens d'interconnexion.

configuration
↳ "snmp version v2c" (ou v3)
↳ "snmp community COMMUNAUTE_PRIVEE"
↳ "snmp trap receiver @IP serveur-SNMP-SUPERVISION"

4) mettre en place un moyen de supervision vous permettant de maîtriser les flux entrants et sortants de votre réseau sur Internet.
↳ utilisation d'une DMZ Proxy
↳ couple de FWs pour séparer : LAN | DMZ | Internet
↳ Proxy servant de passerelle Internet aux postes de travail pour accéder à Internet
↳ utilisation d'un fichier wpad pour savoir quand router les flux vers le Proxy ou en direct

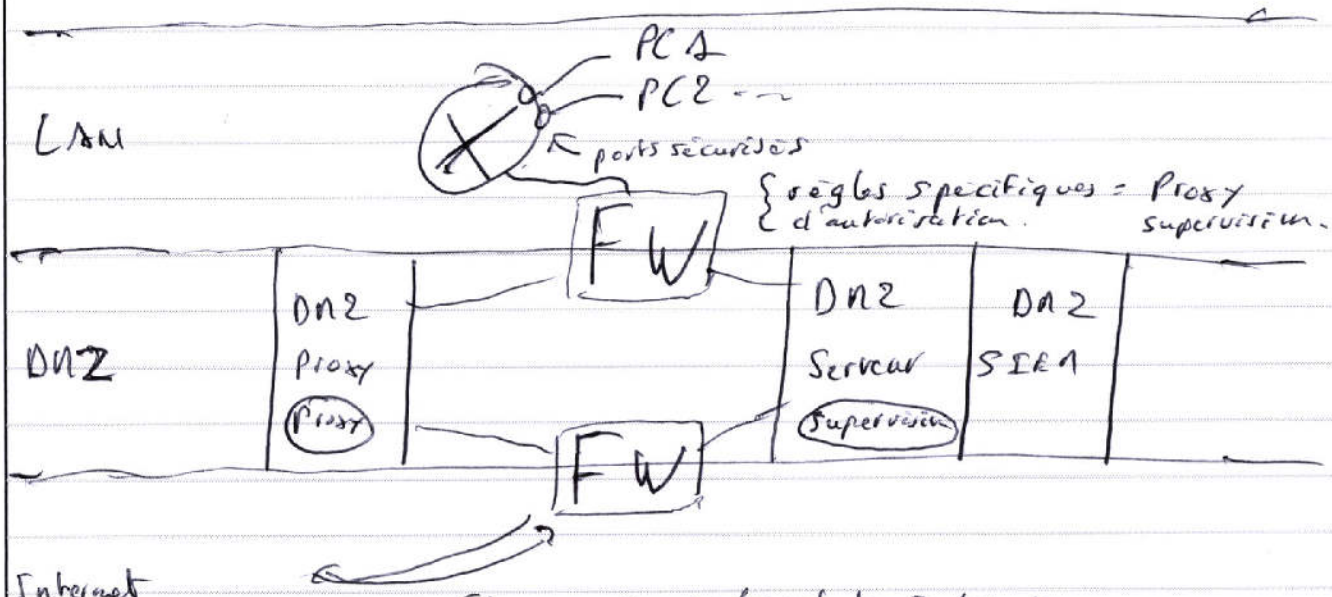
Configuration : filtrage FW : SOURCE IP du PROXY est AUTORISÉE à SORTIR sur Internet

N° 31.3

5) Centraliser les évènements et alarme des différents équipements.

↳ utilisation d'un socle de sécurité SIEM pour recevoir et aggréger les logs et alerte des différents équipements.

Architecture :



Flux entrants/sortants Internet

↳ de limitations pour les flux entrants

N° 3.13.