Intitulé de l'épreuve : 21/02/2019 Réseaux & 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 : 1ère Norme définissant le protocole de communication sans-fil Wifi

2) Modèle OSI :

Couche 1 : Physique. Transmettre de l'information binaire dans le support physique. Unité : bit

Couche 2 : Liaison. Adressage physique des cartes réseaux et communication dans un réseau local Unité : Trame

Couche 3 : Réseau. Objectif : adressage logique des interfaces réseaux pour permettre la communication entre réseaux interconnectés. Unité : Paquet

Couche 4 : Transport. Fiabiliser et définir le transport de données entre deux interlocuteurs Unité : Segment

3) ARP : Address Resolution Protocol. Vise à permettre d'établir le lien entre adresse physique et logique, en particulier de connaitre l'adresse physique à partir de la seule logique (Ex : @IP => @MAC)

DNS : Domain Name Service, permet de résoudre un nom de domaine en une adresse IP logique (et inversement)

SFTP : Secure File Transfer Protocol : Le protocole servant à l'échange de fichiers entre un client et un serveur de façon sécurisée.

NTP : Network Time Protocol. Protocole permettant à plusieurs ordinateurs dans un réseau, de synchroniser leur horloge sur un référentiel de temps.

4) 192.168.1.0/26

↳ @ Réseau = 192.168.1.0
@ Diffusion = 192.168.1.63
@ hôtes = 192.168.1.1 → 192.168.1.62
Soit 62 adresses

192.168.1.64/26

↳ @ Réseau = 192.168.1.64
@ Diffusion = 192.168.1.127
@ hôtes = 192.168.1.65 → 192.168.1.126
Soit 62 adresses

192.168.1.128/25

↳ @ Réseau = 192.168.1.128
@ Diffusion = 192.168.1.255
@ hôtes = 192.168.1.129 → 254
Soit 126 adresses

N° 1.1.3.

5) IDS : Intrusion Detection System.
Mécanismes et outils, réseaux ou systèmes permettant notamment au moyen de l'écoute des flux, de détecter dans le réseau une tentative d'intrusion par l'introduction d'une charge virale.

7) Dynamic Host Configuration Protocol vise à automatiser l'attribution d'une adresse IP à toute nouvelle machine arrivant dans le réseau (attribut° + configuration).

Etape 1 : Une machine arrivant dans le réseau diffuse (Niveau 2) une requête de demande de service DHCP. (DHCP Discover)

Etape 2 : Le serveur DHCP répond directement (niveau 2) à la station en proposant une adresse à la station (DHCP Offer)

Etape 3 : La station fait la requête au serveur DHCP de la proposition faite en 2/ (DHCP REQUEST)

Etape 4 : Le serveur acquitte (ou pas) la demande de la station (ACK)

La sélection parmi 2 offres DHCP se fait par ordre chronologique. Premier reçu premier choisi.

Le DHCP spoofing consiste à une machine dans le réseau local de répondre à l'étape 1 à la place du vrai serveur DHCP afin de détourner l'adressage d'une machine.

6) Je perçois une ambiguïté dans les "2 types de requêtes DNS possibles. J'ai donc 2 réponses possibles.
a) Soit il s'agit des requêtes itératives vs recursives pour le parcours des différents serveurs d'autorité.
Itératif : Le client interroge successivement tous les serveurs d'autorité (SOA) dans la hiérarchie du FQDN

N° 1.1.3.

Récursif: Le client n'interroge que le SOA du "top level domain" (TLD) qui lui relaye au SOA inférieur, qui lui même relay au SOA inférieur etc .... jusqu'à trouver la réponse et la faire remonter jusqu'au client. Problème: Peut engorger les SOA des Global TLD.

b) Soit il s'agit du type de résolution des requêtes.

"Forward" : pour la résolution NOM -> IP
Soit "Reverse" : Pour la résolution IP -> NOM

8) Au déchiffrement de la trame il apparait:

a) @IP SRC Trame1 = $(84.00\ 00\ 01)_{16}$ (hexa)
$= 10000100.0.0.1$
$= \underline{(132.0.0.1)_{10}}$

C'est donc une classe B

b) @MAC SRC de Trame1 =

$\underline{00:0a:b7:a3:4a:00}$

c) @IP DST Trame 1 (ou @IP SRC Trame 2)

$= (c2\ 00\ 00\ 01)_{16}$
$= 11000010.0.0.1$
$= \underline{(194.0.0.1)_{10}}$

Classe : C

d) @MAC DST Trame1 ou @MAC SRC Trame 2

$\underline{00:01:02:6f:5e:9b}$

e) TTL Trame 1 = $(40)_{16}$:
TTL Trame 2 = $(3a)_{16}$

Intitulé de l'épreuve : 21/02/2019 Réseaux & télécoms

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 (Suite)

8/ e) Suite

... : $TTL\ 1 - TTL\ 2 = (6)_{10}$

Six sauts sont mesurés entre la trame 1 et 2. Si la route est symétrique, ça signifie qu'il y a 3 routeurs qui séparent les 2 machines.

g) C'est la commande ping qui est à l'origine de cet échange. On le voit dans le champ protocole du paquet IP : $(01)_{16} = (1)_{10}$ = ICMP

f)

Partie 2

1/ Il manque une entrée dans la table de routage sur Router 1, on devrait trouver

D 192.168.5.0/24 via 10.1.2.1 tunnel1

N° 2/3

[redacted]

cad

router eigrp 100
network 10.1.2.0 0.0.0.3
network 192.168.0.0

à configurer sur router 1

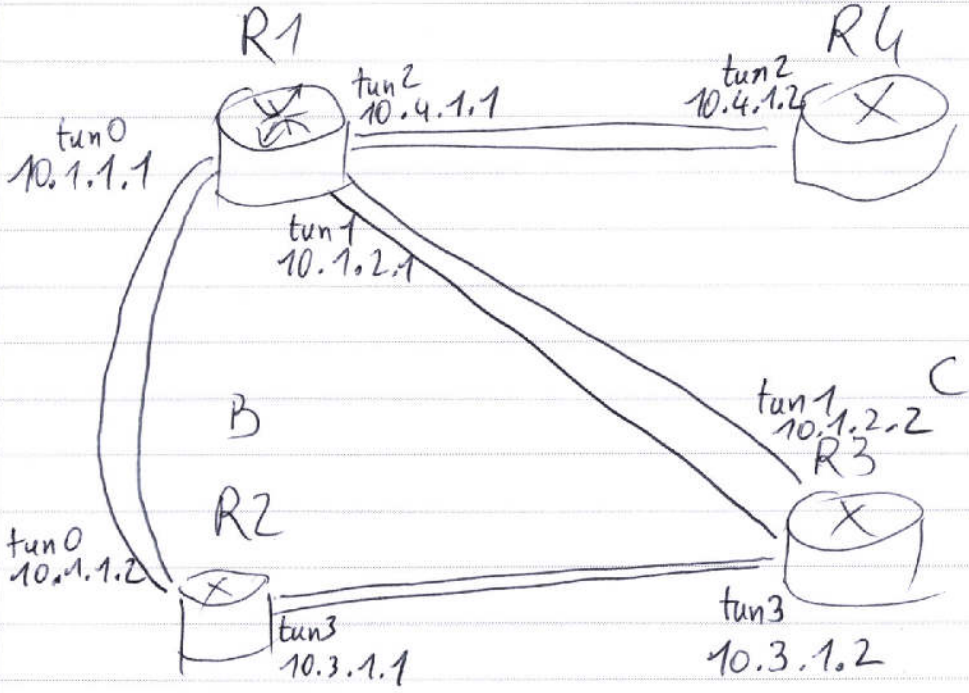
2/ L'interface Tunnel 2 est mal configurée sur Router 4

Elle est configurée avec l'@ 10.4.1.5/30 au lieu de 10.4.1.2/30

Correction Router 4

interface Tunnel2
ip address 10.4.1.2 255.255.255.252
mtu 1476
tunnel source GigaBit Ethernet 0/0
tunnel destination 80.1.0.2

4/ A D



3/ Routeur 2 du site B

interface FastEth 0/0/0
switchport access vlan 2
" mode access
" nonegotiate

interface FastEth 0/0/1
switchport acces vlan 3
" mode access
" nonegotiate

interface Vlan2
ip aoldress 192.168.3.254 255.255.255.0

interface Vlan 3
ip aoldress 192.168.4.254 255.255.255.0

N° 2.1.3

```
interface Gigabit Eth 0/0
    ip address 80.2.0.2 255.255.255.252 (/30)
    duplex auto
    speed auto

interface Tunnel 0
    ip address 10.1.1.2 255.255.255.252 (/30)
    mtu 1476
    tunnel source Gigabit Eth 0/0
    tunnel destination 80.1.0.2

interface Tunnel 3
    ip address 10.3.1.1 /30
    mtu 1476
    tunnel soura Gigabit Eth 0/0
    tunnel destination 80.3.0.2

router eigrp 95
    network 10.1.1.0 0.0.0.3
    network 10.3.1.0 0.0.0.3
    network 192.168.3.0

router eigrp 100
    network 10.3.1.0 0.0.0.3
    network 192.168.4.0
```

N° 2.13

Intitulé de l'épreuve : 21/02/2019 Réseaux & 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

* Durcir les configurations des equipements réseaux.

+ Bannir tout protocole de connexion aux equipements qui soit non sécurisé (ex telnet). Préférer une authentification par SSH, par clé de chiffrement.
+ Configurer des liste d'accès (ACL) qui explicitent uniquement les flux autorisés à transiter, bloquer tout le reste par défaut.
+ Pour la commutation : mettre en place du controle sur le nombre de MAC autorisées à s'enregistrer (Port security).
+ Mettre en silo les zones réseaux qui n'ont pas de raison de dialoguer ensemble (L2 Vlan différents)
+ Isoler de manière très stricte le réseau d'administration des équipements du reste du SI, réseau séparé idéalement.
+ Mettre en place une zone démilitarisé (DMZ) minimaliste pour les services qui ont accès/sont accéder par Internet et filtrer très strictement les flux de cette DMZ.

[redacted]

* Mettre en place un système permettant de contrôler les différents équipements qui se connectent au réseau

+ N'autoriser qu'une seule MAC par port sur le commutateur
+ N'ouvrir sur le commutateur que les ports utilisés, fermer tous les autres
+ Pour le wifi, mise en place d'un portail captif.

* Mettre en place un outil de supervision centralisé

+ Supervision fonctionnelle : Déploiement d'outils comme Centréon ou Eyes of Network qui, à l'aide de sondes est en mesure à la fois de donner une indication immédiate de l'état de santé du réseau mais peut également historiser sous formes de graphes les métriques récoltées. La métrologie permet de contextualiser dans le temps les informations collectées, ce qui aide à la détection d'anomalies.
+ Supervision analytique : Déploiement d'outis tels que Splunk ou ELK qui eux se basent sur l'analyse des journaux d'informations de l'ensemble des équipements. Cette analyse et collecte permet également de remonter des indicateurs forts, de corréler les informations entre différentes sources pour détecter des comportements anormaux. Il est nécessaire de centraliser tous les journaux dans un collecteur.

N° 3.1.3.

* Mettre en place un moyen de protection permettant de maitriser les flux entrants et sortants.

1) Flux entrants

+ Mise en place de pare-feu à la sortie de la liaison opérateur. Plus d'un, et de constructeurs différents,

+ Etude avec l'opérateur de solution anti Dos / DDos

+ Mise en place d'un point d'entrée unique pour tous les flux (Reverse Proxy) pour assurer une rupture protocolaire

+ Chiffrement de tous les flux entrants sur le Reverse Proxy (ex: Big IP)

+ Déchiffrement de tous les flux : une fois derriere le reverse proxy, associé à une capture de tous les flux dans un système de supervision analytique tel qu'évoqué plus tôt

2) Flux sortants

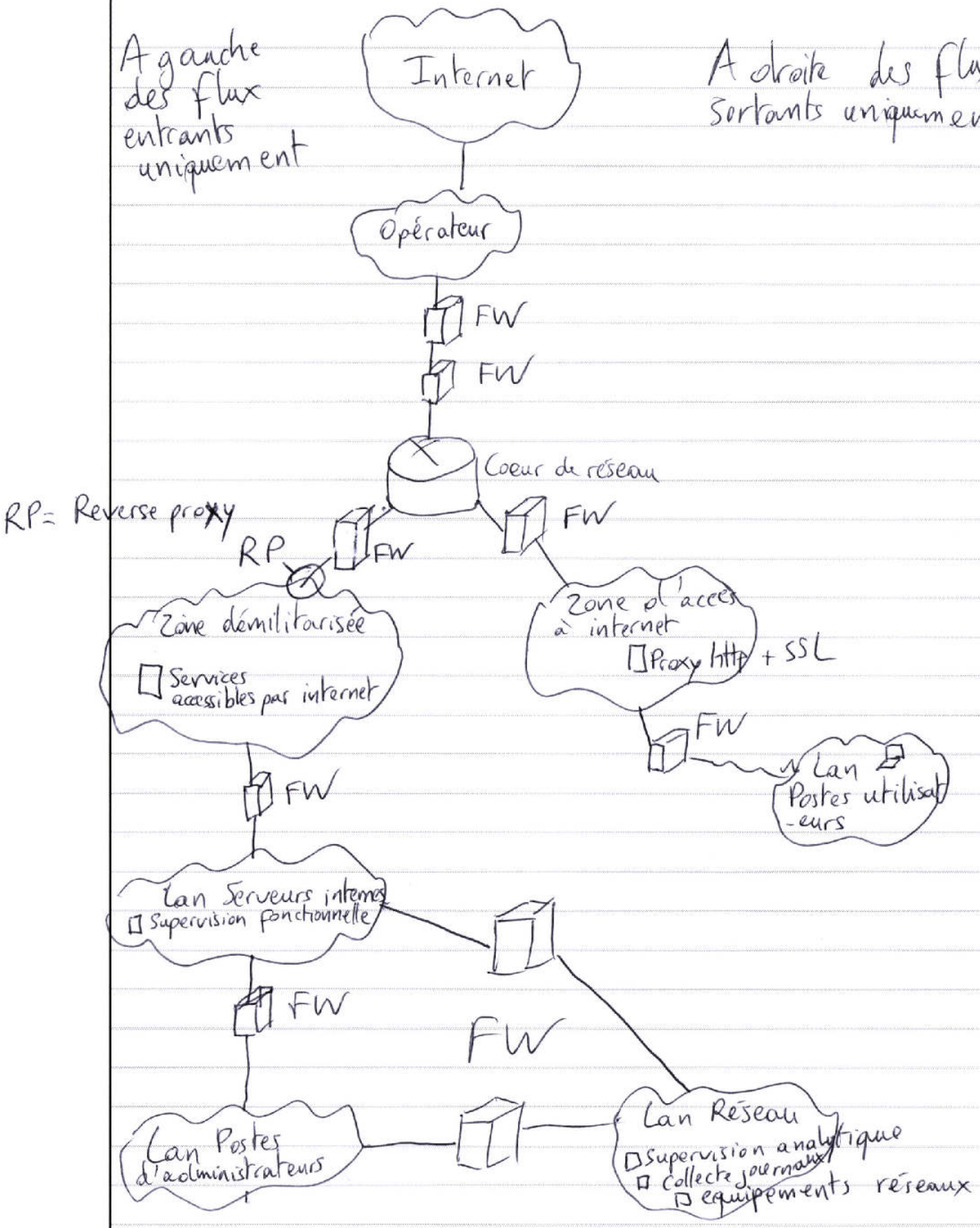
+ Installation de proxy http/https et gestion d'une liste blanche d'accès à internet

+ Installation d'un proxy SSL qui assure une rupture protocolaire entre les postes des usagers et les serveurs sur internet.

* Centralisation des évènements et alarmes

+ Mise en place d'un serveur de collecte de journaux (Rsyslog, Syslog NG) et configuration de tous les équipements pour renvoyer les journaux vers celui-ci

Schéma 


A gauche des flux entrants uniquement
Internet
A droite des flux sortants uniquement
Opérateur
FW
FW
Coeur de réseau
RP= Reverse proxy
RP
FW
FW
Zone démilitarisée
Services accessibles par internet
Zone d'accès à internet
Proxy http + SSL
FW
Lan Postes utilisateurs
FW
Lan Serveurs internes
Supervision fonctionnelle
FW
FW
Lan Postes d'administrateurs
Lan Réseau
Supervision analytique
Collecte journaux
équipements réseaux

N° 3.13