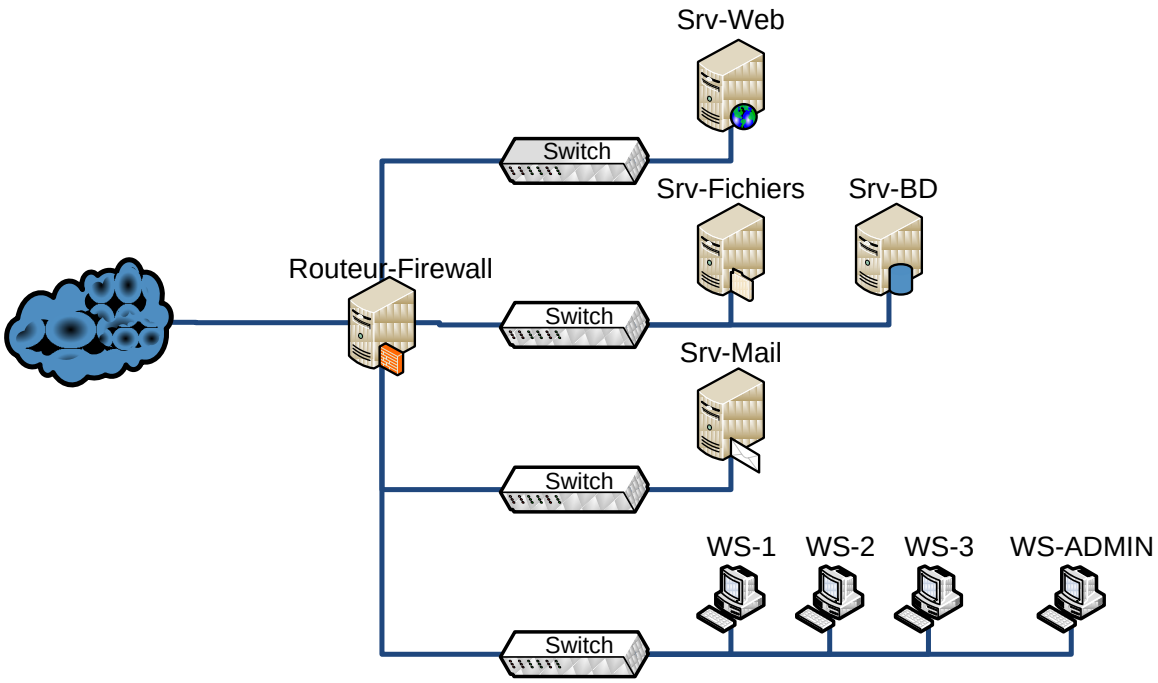
Examen Blanc
RSX112 – Sécurité et Réseaux

Tous documents et calculatrices autorisés – Durée : 2h30
Le sujet comporte 5 pages.

Exercice 1 – *Pare-feu* *– 10 Points*

Soit le schéma réseau suivant :

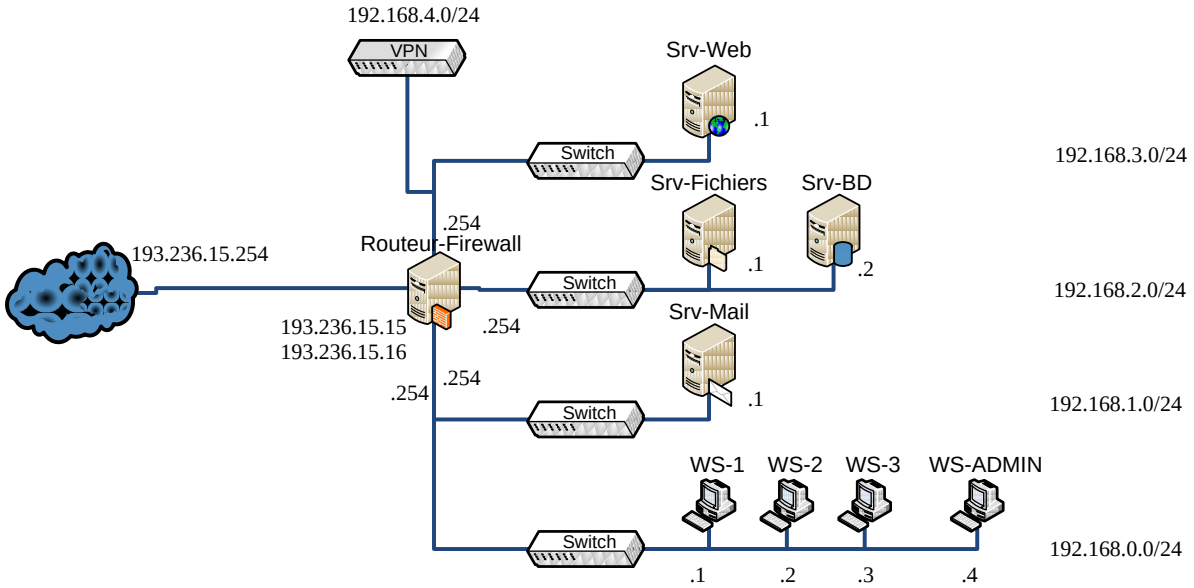


Le routeur-firewall dispose de deux IP publiques : 193.236.15.15 et 193.236.15.16, et le premier routeur vers Internet est 193.236.15.254.

Voici les services qui devront être disponible à travers le réseau et/ou Internet :

a. On souhaite que seul le serveur web soit accessible depuis Internet (protocole HTTP (port 80) et HTTPS (port 443)).
b. Les utilisateurs doivent avoir la possibilité de se connecter depuis l'extérieur du site à certaines parties du réseau de l'entreprise, par l'intermédiaire de VPN (le routeur-firewall faisant également concentrateur VPN).
c. Le serveur de base de données doit être accessible depuis le serveur web.
d. Le serveur de fichiers et de base de données doit être accessible depuis le réseau des utilisateurs (WS-*) et le VPN
e. Le serveur de mail doit être accessible depuis le réseau des utilisateurs et le VPN, mais non consultable depuis l'extérieur. Par contre, il devra pouvoir recevoir des mails depuis Internet.
f. La station ws-admin doit pouvoir prendre le contrôle en Remote Desktop (port 3389) sur tous les serveurs et administrer le firewall sur le port 4000 en HTTPS.

1) Etablir un plan d'adressage du réseau privé. **2 points**



2) Donner la table de routage du routeur. **2 points**

Correction :

Dest	Interface	Passerelle	
192.168.4.0/24	192.168.4.254	-	
192.168.3.0/24	192.168.3.254	-	
192.168.2.0/24	192.168.2.254	-	
192.168.1.0/24	192.168.1.254	-	
192.168.0.0/24	192.168.0.254	-	
193.236.15.0/24	193.236.15.15	-	
*	193.236.15.15	193.236.15.254	

3) Donner la table de translation de port NAT/PAT. **2 points**

Les réseaux 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, (192.168.4.0/24 ?) utilisent le NAT pour sortir sur Internet.
Les ports 80 et 443 de l'IP 193.236.15.16 sont PAT vers 192.168.3.1.
Le VPN est ouvert sur l'IP 193.236.15.15 (port 500 au minimum d'ouvert).
Le port 25 de l'IP 193.236.15.16 est PAT vers 192.168.1.1.

4) Donner la table de filtrage. **2 points**

(on suppose le FW statefull)

IP source	port source	IP dest	port dest	ALLOW/DENY
192.168.0.0 192.168.1.0 192.168.2.0 192.168.3.0	ANY	ANY	80/443/21	ALLOW
ANY	ANY	192.168.3.1	80/443	ALLOW
ANY	ANY	192.168.1.1	25	ALLOW
192.168.3.1	ANY	192.168.2.2	PORTBD	ALLOW
192.168.0.0 192.168.4.0	ANY	192.168.2.1	PARTFICHIER	ALLOW
192.168.0.0 192.168.4.0	ANY	192.168.1.1	POP3,SMTP	ALLOW
192.168.0.4	ANY	192.168.1.1 192.168.2.1 192.168.2.2 192.168.3.1	3389	ALLOW
~~192.168.0.4~~	~~ANY~~	~~192.168.0.254~~	~~4000~~	~~ALLOW~~
ANY	ANY	ANY	ANY	DENY

5) Donner la configuration associée au VPN. **1 point**

L2TP/IPSEC, avec certificats (serveurs et utilisateurs)

6) Discuter des avantages et inconvénients de votre configuration VPN. **1 point**

Déployer les certificats.
Mais si on utiliser PSK ou mot de passe, plus simple à mettre en place et à déployer, mais moins sécurisé.

Exercice 2 – *Cryptage* – *5 Points*

1) Décrypter le texte suivant (les espaces ont été chiffré, les éventuels caractères de ponctuations du texte initial ont été chiffrés comme un espace, le texte ne contient que des lettres et des espaces)

```
ENTAR LNTSD FQTAY NAEAN INGBD BNALQ

TFQSA ENTAT LDHZQ SNT

ZANSZ MEDGA LQAUE ZQAYA ZYGNT TZXN

YLAGN TNZLA UGDHN
```

```
MAYFQ QNGAE ZASZM ENAYN AGFLS ZXN

YLAGF LSNLG

BAYFQ QNGAE ZASZM ENAYN ASGZQ TEZSD FQ

QZSAU ZS

YAYFQ QNGAE ZASZM ENAYN ACDES GZXN
```

Remarques : les espaces ne sont là que pour la mise ne page.

Correction :
les questions de l exercice un
sont les suivantes
A Etablir un plan d adressage
du réseau privé
B Donner la table de routage
du routeur
C Donner la table de translation
NAT/PAT
D Donner la table de filtrage

Exercice 3 – *RSA* *– 5 Points*

On donne les valeurs numériques suivantes : p = 5, q = 11.

1) Calculer les valeurs des nombres d et e vérifiant les conditions de l'algorithme de chiffrage RSA. Pour avoir un couple unique on prend la plus petite valeur possible de d et pour cette valeur la plus petite valeur possible de e.

   n est codé sur 6 bits, donc M sera découpé en mots de 5 bits, et C sera une séquence de mots de 6 bits.

   *n = p.q = 5*11 = 55*
   *z = φ (n) = (p-1).(q-1) = 4*10 = 40*
   e = 3 (premier avec z)
   ed = kz + 1 soit 3d = k40 + 1 soit 3d – k40 = 1
   *d =27 (3*27 = 1 (mod 40)) ou 3*27 mod 40 = 1*

   Quelle est la clé publique et quelle est la clé secrète?

   Clé publique : (e, n) = (3, 55)
   Clé secrète : (d, n) = (27, 55)

2) Soit le message de 3 chiffres 1, 6, 15 soit par blocs de 5 bits la configuration de bits suivante :
   00001 00110 01111
   Coder ce message en utilisant les paramètres de chiffrement RSA précédents.

   $M^e \pmod n = 1^3 \pmod{55} = 1$
   $M^e \pmod n = 6^3 \pmod{55} = 51$
   $M^e \pmod n = 15^3 \pmod{55} = 20$

   $C^d \pmod n = 1^{27} \pmod{55} = 1$
   $C^d \pmod n = 51^{27} \pmod{55} = 6$
   $C^d \pmod n = 20^{27} \pmod{55} = 15$
   /!\ aux precisions des calculs…

3) On reçoit le message suivant par blocs de 6 bits (2, 4, 20):
   000100 001110 011000
   Donner la valeur initiale du message (texte en clair), en prenant les mêmes valeurs pour d, e et k qu'à la question 2.

   $C^d \pmod n = 2^{27} \pmod{55} = 18$
   $C^d \pmod n = 4^{27} \pmod{55} = 49$
   $C^d \pmod n = 20^{27} \pmod{55} = 15$

4) Pourquoi ne peut-on prendre p et q petits ?

   Car trop facilement décryptable… (force brute)

5) Que se passe-t-il lorsque p et q sont de l'ordre de $l0^{l0}$?

   Il est beaucoup plus difficile de décrypter (grand nombres).
   Par contre, il faut des algorithmes de calculs efficaces face aux grands nombres.