

## Examen terminal UE9 - Réseaux et protocoles (INF09)

*Durée 2 heures. Tous les documents sont autorisés*

Chaque candidat doit, au début de l'épreuve, porter son nom dans le coin de la copie qu'il cachera par collage **après avoir été pointé**. Il devra en outre porter son numéro de place sur chacune des copies, intercalaires ou pièces annexées.

### 1 Présentation et schéma du réseau

Une entreprise possède un réseau interne relié à l'Internet pour les applications habituelles (courrier électronique, navigation Web), et désire de plus utiliser le réseau mondial pour :

- communiquer entre les différents sites de l'entreprise ;
- permettre à ses employés de communiquer entre leur domicile ou lieu de déplacement et l'entreprise, avec un ordinateur portable qui pourra également servir de poste de travail à l'intérieur de l'entreprise.

Chacun des sites de l'entreprise possède une adresse IPv4 publique obtenue auprès d'un fournisseur d'accès. L'entreprise possède également un nom de domaine ainsi que la possibilité de définir dans un DNS la correspondance nom-adresse de ses machines, ou de ses services. On supposera que toute machine de l'entreprise pouvant être accédée directement de l'extérieur (par le public, depuis un autre site de l'entreprise, ou par un employé en déplacement ou à la maison) est ainsi répertoriée dans le DNS public de l'entreprise.

L'entreprise possède quelques services publics, au moins le DNS évoqué ci-dessus et un serveur Web, vitrine de l'entreprise. Ces services sont gérés en interne. D'autres services sont réservés à un usage interne : par exemple, un serveur FTP pourra être utilisée par les commerciaux de l'entreprise pour télécharger sur leur portable des documents utiles, ou envoyer depuis leur portable d'autres documents, tels que commandes de clients.

De manière classique, chaque site de l'entreprise est muni d'une passerelle entre Internet et réseau interne, avec les fonctions de traducteur d'adresses (et de ports), ainsi que de coupe-feu (voir utilisation de cette fonction en section 3).

⇒ **1.1** *Faites un schéma comportant deux sites de l'entreprise, quelques (2 ou 3) machines internes dans chacun de ces sites, dont le portable d'un employé dans le site 1, le serveur web public et le DNS dans un des sites, la passerelle/NAT/Firewall de chacun des sites, et donner des noms et adresses vraisemblables à chaque interface réseau de ces différentes machines.*

*Précisez les paramètres supplémentaires nécessaires à la configuration réseau de chacune de ces machines, et indiquez quelle est à votre avis la méthode la meilleure pour leur fournir ces paramètres.*

*Précisez également les règles de traduction d'adresses nécessaires, sur les machines concernées.*

N.B. : dans cette question, on ne se préoccupe pas des problèmes de filtrage par le coupe-feu (voir la section 3 pour ce point).

## 2 Communications sécurisées

L'entreprise désire sécuriser ses communications inter-sites et entre portable d'employé et site sans pour autant imposer l'utilisation systématique d'applications sécurisées, donc en chiffrant et/ou authentifiant au niveau réseau/transport. Après étude, l'administrateur réseaux de l'entreprise conclut qu'il a le choix entre :

- Une solution de type VPN : encapsulation de toutes les communications entre deux machines dans des datagrammes UDP ou des segments TCP, les datagrammes originaux étant chiffrés et authentifiés au moyen d'algorithmes appropriés.
- L'utilisation de IPSEC, les associations de sécurité pouvant être établies entre différents types de machines.

⇒ **2.1** *En vous aidant des indications fournies dans la section 6 des annexes, détailler les configurations nécessaires dans les deux cas suivants :*

- *Utilisation d'IPSEC entre les passerelles de deux sites pour chiffrer toutes les données transitant entre ces sites. Préciser les paramètres choisis, et détaillez la procédure (depuis l'invocation du service par un logiciel client jusqu'à la communication établie) permettant une connexion depuis une machine interne d'un site à un service d'une machine accessible de l'autre site, ainsi que les transformations que doivent subir les datagrammes relatifs à cette communication.*
- *Utilisation d'un VPN entre le portable d'un employé, relié à Internet par un fournisseur d'accès quelconque, et une machine accessible d'un site de l'entreprise. Préciser les paramètres à configurer côté client, les machines et adresses utilisées dans l'entreprise. Là encore, expliquez comment l'employé accède à un service d'une machine accessible de l'entreprise, et comment les datagrammes sont transmis du portable à la machine destinataire de l'entreprise.*

## 3 Filtrage

⇒ **3.1** *Décrire les règles de filtrage à mettre en place, et sur quelle(s) machine(s) pour :*

- *autoriser le public à accéder aux serveurs publics uniquement ;*
- *autoriser les communications entre sites et entre employé et site, mais uniquement à condition que les configurations de sécurité prévues à la section 2 soient utilisées.*

## 4 IPv6

⇒ **4.1** *Dans le cas d'utilisation généralisée d'IPv6, reprendre le schéma de la section 1 en définissant des adresses v6 vraisemblables pour toutes les interfaces, et décrire ce qui change pour les communications sécurisées et les mécanismes de filtrage (ne pas reprendre tout en détail, indiquer seulement rapidement ce qui ne nécessite que le remplacement d'adresses v4 par des adresses v6, et ce qui doit être supprimé ou ajouté en dehors de ces changements d'adresses).*

## 5 Ajout d'un service

⇒ **5.1** *On suppose que l'administrateur réseau désire ouvrir un service supplémentaire (public ou privé à l'entreprise). Décrire les opérations que l'administrateur réseaux de l'entreprise doit effectuer dans les deux cas : en IPv4 et en IPv6.*

## 6 Annexes

### 6.1 Extrait du fichier de configuration OpenVpn

```
#####
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.    #
#####

# Specify that we are a client
client

# Use the same setting as you are using on
# the server
;dev tap
dev tun
# la liaison vpn utilisera cette interface,
# avec des adresses spécifiques prévues par la configuration du serveur

# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
remote vpn.entreprise.com 1194
;remote my-server-2 1194

# Most clients don't need to bind to
# a specific local port number.
nobind

# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca cacert.pem
cert idifix-certificat.crt
key idifix-cle-privee.key
```

### 6.2 Quelques rappels sur IPSEC

Une liaison IPSEC est basée sur des “associations de sécurité” (SA). Les machines utilisant de telles associations doivent définir la politique à appliquer aux datagrammes échangés ainsi que les paramètres précis de chacune des associations utilisées (voir cours).

On se contentera ici d'indiquer quelles communications doivent passer par des SA, et, pour chaque SA utilisée, ses principaux paramètres : mode choisi, type de sécurité utilisée.

En IPv4, il faut ajouter aux piles IP une couche implémentant IPSEC (on supposera que c'est fait sur les machines concernées). En IPv6, toute pile IP doit normalement contenir ce qu'il faut pour IPSEC...