Protocoles de l'Internet – les bases
25 Novembre 2015

1IR
Documents non autorisés

La menace fantôme

1. Un réseau privé (6 points)

Une société plutôt douteuse souhaite avoir des accès un peu partout dans le monde pour pouvoir couvrir ses activités. Toutefois elle souhaite que ce réseau soit unique et utilise une solution VPN qui n'est pas du tout l'objet de cet examen (considérez si vous en avez besoin qu'il s'agit d'une liaison point à point entre ses sites). Elle choisit une solution d'adressage privée mais avec unicité du réseau, il faut donc qu'elle mettre en œuvre des sous-réseaux.

1.1. Adressage (2 points)

L'entreprise dispose de 7 sites : Paradis 10 machines (îles Caïmans), Vodka 20 machines (Russie), Mafia 38 machines (Sicile), Coca 12 machines (Colombie), Fourrure 29 machines (Afrique du Sud), Requin 8 machines (Philippines) et Tissus 61 machines(Inde).

Pour l'unicité du réseau, l'adresse 192.168.190.0/24 a été choisie. Proposer une découpe en sous-réseaux permettant l'existence de ces sept sous-réseaux. Si ce n'est pas possible, vous proposerez une autre solution.

1.2. Interconnexion des sites (1 point)

Chaque site est interconnecté aux autres en utilisant un VPN (que l'on qualifiera plus tard d'interne) que l'on considérera comme une liaison point à point en IP.

Combien cela fait-il de liaisons point-à-point ? Combien faut-il d'adresses IP pour les configurer ? Peut-on le faire avec l'adressage précédent ? Si oui proposez un adressage, sinon proposez une autre solution.

1.3. Routage (2 points)

Représentez le réseau Coca et son routeur C de sortie avec ses 7 interfaces. Donnez la table de routage de ce routeur pour que le réseau Coca puisse communiquer avec tous les autres sous-réseaux.

1.4. Auto-configuration (1 point)

Comment les différents équipements utilisateurs des réseaux privés peuvent-ils être configurés automatiquement ? Peut-on mettre en place la partie serveur de ce protocole à un seul endroit du réseau 192.168.190.0/24. Si oui, comment ? Si non, pourquoi ?

Bonus (1 point) :

Est-il vraiment judicieux de faire des VPN IP entre les sites ? Pourquoi et avez-vous une idée d'une meilleure solution pour alléger les questions 1.2, 1.3 et 1.4.

2. Tapis dans l'ombre (3 points)

Malheureusement, avoir un simple adressage privé n'est pas suffisant pour se cacher dans Internet.

2.1. Privé et communication (0,5 point)

Est-il possible de communiquer avec une machine quelconque d'Internet directement avec une adresse privée ? Pourquoi ?

2.2. Communiquer en privé (1 point)

Comment peut-on faire pour communiquer du monde privé vers le monde public ? Expliquer le principe.

2.3. Sept portes de sortie (0,5 point)

Peut-on utiliser un seul routeur pour sortir pouvoir avoir une sortie sur chaque pays ? Pourquoi ?

2.4. Se cacher derrière plusieurs adresses publiques (1 point)

On souhaite pour une même porte de sortie, avoir plusieurs adresses publiques possibles. Quel peut être l'utilité de plusieurs adresses IP publiques ici ? Quel problème cela pose t'il en terme de routage ?

Bonus (1 point) :

Donner une règle permettant de mettre en place cette fonctionnalité le site de votre choix. (On pourra reprendre CoCa si cela peut convenir.)

3. Traquer l'invisible (4 points)

L'entreprise à installer ses serveurs illicites derrière ses NAT, se pose alors la question de savoir s'ils sont vraiment si invisibles que cela ?

3.1. Accès à un serveur caché (1 point)

Que faut-il mettre en place pour donner accès à un serveur situé derrière un NAT. On donnera un exemple avec un serveur d'un des sites, par exemple COCA[1].

3.2. L'oublie du NAT (3 points)

Le NAT change classiquement les champs d'adresse et de port d'un datagramme. En revanche les autres champs sont rarement changés, en tout cas par les configurations par défaut, notamment le TTL. En quoi le TTL peut-il trahir la présence d'un NAT ? On pourra illustrer cela via un traceroute en considérant la figure de la partie 4.

4. Solution applicative (9 points)

Réalisant que le NAT n'est pas un gage de sécurité, l'entreprise décide d'opter pour une solution de passerelles applicatives, tout en gardant le NAT actif. Sur chaque site, une passerelle applicative est installée dont le rôle est de masquer l'utilisateur. Ce type de passerelle porte classiquement le nom de proxy et est souvent associée à une connexion VPN. Toutefois, la partie VPN, ne nous intéressera pas ici, si ce n'est peut-être son impact sur la MTU.

La figure suivante représente succinctement une partie de cette architecture.

Pour simplifier le problème, on utilise un proxy de type http et tous les réseaux sont de type Ethernet (il n'y a donc pas d'autres routeurs visibles que ceux représentés).

On rappelle que la MTU d'Ethernet est de 1500B. VPN et VPN i(nterne) présente un en-tête de 20B.

4.1. NAT, localisation et MTU (1 point)

Sur ce schéma, quel(s) équipement(s) est/sont en charge du NAT ? Pourquoi ?

Le NAT a-t-il un impact sur la MTU utilisable ? Pourquoi ?

4.2. Protocole manquant (1 point)

Remplissez le protocole manquant dans le dessin. Quel est le protocole manquant dans le schéma ?

4.3. MSS de la communication entre l'utilisateur et le proxy (1 point)

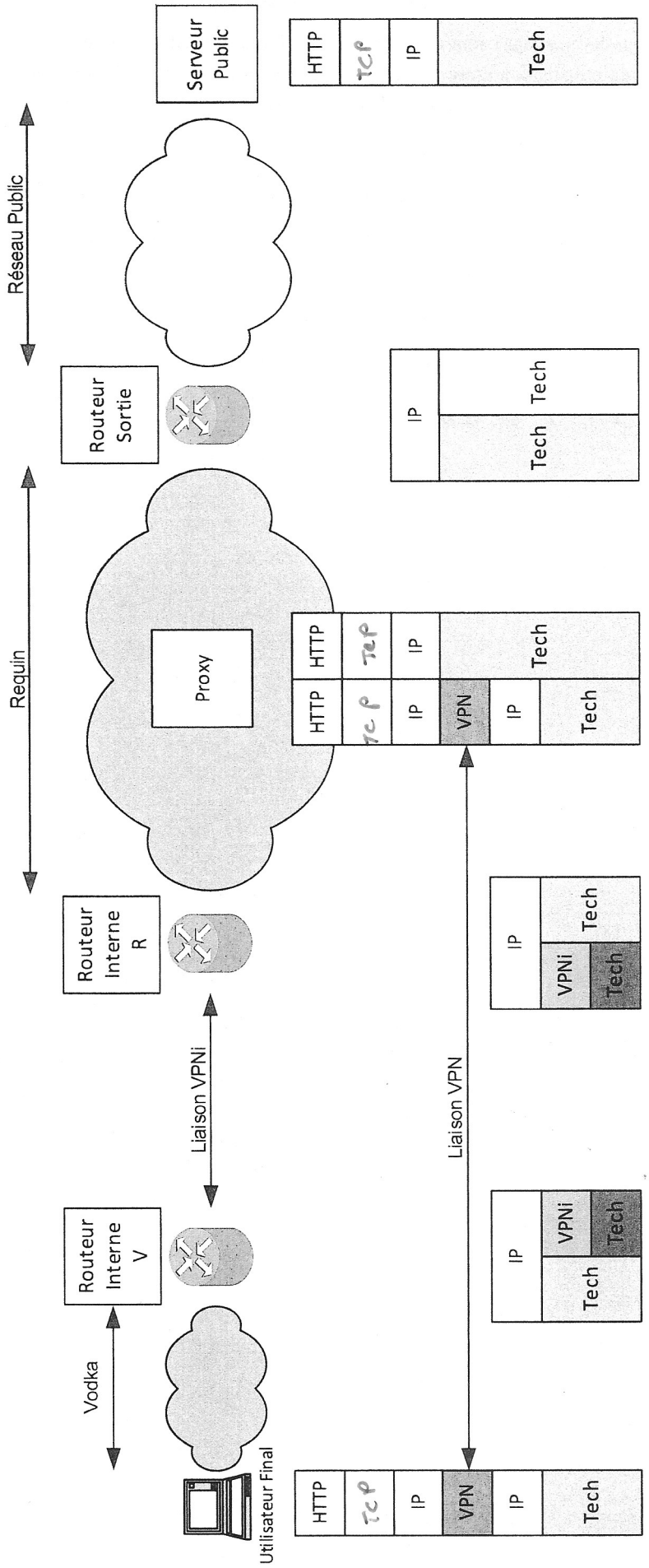
Quelle est la MSS utilisable sur la communication entre l'utilisateur et son proxy ?

4.4. MSS de la communication entre le proxy et le serveur public (1 point)

La MSS entre le serveur public et le proxy a-t-elle la même valeur ? Pourquoi ?

$MSS = MTU - h_{TCP} - h_{IP}$

[1] Je ne demande pas la commande mais juste la règle !


Serveur Public
HTTP
TCP
IP
Tech
Réseau Public
Routeur Sortie
IP
Tech
Tech
Requin
Proxy
HTTP
HTTP
TCP
TCP
IP
IP
VPN
IP
Tech
Tech
Routeur Interne R
IP
VPNi
Tech
Tech
Liaison VPNi
Liaison VPN
Routeur Interne V
IP
VPNi
Tech
Tech
Vodka
HTTP
TCP
IP
VPN
IP
Tech
Utilisateur Final

4.5. Emission d'un GET http de U vers S via P (2 points)

On part du principe que les machines sont déjà configurées, les tables ARP remplies, les adresses IP connues, les VPN en fonction. Le délai de propagation entre S et P est de 20ms, le délai de propagation entre U et P est de 100ms. Les temps d'émission sont négligés. P n'envoie le GET http à S que lorsqu'il a reçu celui de U.

Tracer le chronogramme entre U, P et S permettant jusqu'à la réception du GET par S.

4.6. Transfert de données entre U et S via P (3 point)

La page web demandée fait 14600B. Les débits sont partout à 1Mbit/s (on arrondi à 10ms près). Awnd de U vaut 5000B, awnd de P vaut 7300 B, et awnd de S vaut 14000B.

Tracer le chronogramme de la communication, sachant que le troisième segment est perdu sur le routeur interne de Requin.

awnd → fenêtre de réception

RTO = 2 RTT