Exercice 1

Soit un réseau de machines derrière un pare-feu pratiquant la NAT dynamique avec une IP externe 109.11.108.64. Quatre des machines internes ayant comme IP 192.168.0.10, 192.168.0.11, 192.168.0.12 et 192.168.0.13 consultent en même temps le site ayant comme adresse IP 51.144.108.120 sur le port 80

1- Compléter le tableau de la NAT dynamique suivant :

Interne				Externe			
IP_src	Port_src	IP_dest	Port_dest	IP_src	Port_src	IP_dest	Port_dest
192.168.0.10	53310	51.144.108.120	80				
192.168.0.11	53310	51.144.108.120	80				
192.168.0.12	53310	51.144.108.120	80				
192.168.0.13	53310	51.144.108.120	80				

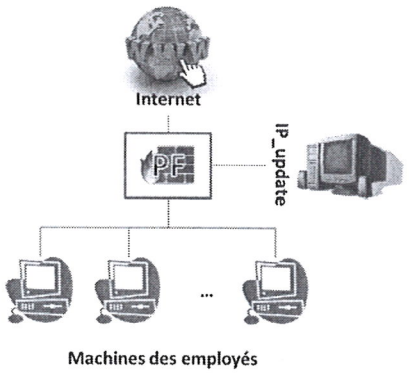
2- Quel risque comporte un protocole en UDP pour lequel la taille de la réponse émise est plus grande que la taille de la requête reçue ?

Pour éviter le déni de service par SYN Flood qui consiste à noyer la cible une succession de requêtes SYN, le numéro d'acquittement est généré par une fonction $f(IP_{src}, IP_{dest}, D)$, où D est la date limite de validité de la session. Ainsi, il n'est plus nécessaire de garder en mémoire l'état de la connexion tant qu'un message d'acquittement n'a pas été reçu.

3- Quel risque encourt-on lorsque la fonction f est connue ?

Exercice 2

Soit le réseau d'une agence représenté dans la figure à droite. Le personnel a le droit seulement de se connecter à un seul site externe en HTTPS qui a l'IP notée sous la variable : IP_site sur le port 443 (trafic sortant). L'IP_site est une IP externe utilisée par le site du siège. Aussi l'ensemble des postes du personnel, nommé IP_emploi, doit être capable de se mettre à jour à travers une machine interne ayant l'adresse IP nommée IP_update. Cette machine dédiée à la mise à jour accepte un trafic sortant en HTTPS vers un ensemble d'adresses externes nommé IP_Ext_update. Dans le passé, pour se connecter au site https:// site.com (port 443), les utilisateurs tapaient sur leur navigateur http://site.com au lieu de l'adresse sécurisée, ce qui obligeait à accepter le trafic sortant en http sur le port 80. Les utilisateurs étaient par la suite redirigés sur https://site.com.



Voici la configuration du Pare feu de l'entreprise :

N°	IP_src	Port_src	IP_dest	Port_dest	Protocole	Action
1	IP_update	Any	IP_ Ext_update	443	TCP	Accept
2	IP_emploi	Any	IP_ site	80	TCP	Accept
3	IP_emploi	Any	IP_ site	443	TCP	Accept
4	IP_emploi	Any	IP_update	443	TCP	Accept
5	Any	Any	Any	Any	Any	Drop

1- Existe-t-il des postes concernés par la NAT statique ? (oui ou non et expliquez avec une phrase)

La redirection de http://site.com vers https://site.com comporte le risque suivant : un intrus intercepte la connexion http://site.com et se met au milieu en redirigeant la connexion par exemple vers https://site.**hack** (MITM : Man In The Middle) pour par exemple récupérer le mot de passe. Pour éviter ce type d'attaque, le siège utilise actuellement HSTS (HTTP Strict Transport Security) qui fonctionne sommairement de la manière suivante : lorsque le siège reçoit une requête http, un message d'erreur HSTS demande au navigateur de remplacer dorénavant http par https avant de lancer la requête. Le navigateur garde cette information par la suite. Pour éviter la première erreur, le site du siège fait partie des adresses renseignées au niveau des nouvelles versions des navigateurs IE, Chrome et Firefox dans la liste « HSTS préétablie ». Ainsi dès que l'utilisateur écrit http://site.com, le navigateur remplace automatiquement la requête de l'utilisateur par https://site.com. En supposant que tous les postes sont mises à jour :

2- Donner la nouvelle configuration du pare-feu

L'agence s'est dotée d'un proxy https :

3- Où le placeriez-vous ?

Exercice 3

1- A quelle opération parmi les opérations suivantes sert la S-BOX dans AES : SubBytes, ShiftRows ou MixColumns ?
2- Combien d'octets contient un bloc AES ?

Soit le cops de Galois fini défini sur l'ensemble des éléments $E = \{0,1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$ ett utilisant le polynôme irréductible $x^3 + x^2 + 1$. (Pour les questions 3, 4, 6 et 7)

3- Convertir les éléments de l'ensemble E en la base décimale
4- Calculer les inverses de 6 et de 4 puis vérifier que l'inverse 5 est 7.
5- Calculer $\begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix}\begin{bmatrix}3\\ 5\end{bmatrix}$

Supposons que le mode de chiffrement des blocs B_i utilisé est CBC, et que chaque bloc contient qu'un seul chiffre entre 0 et 7, à savoir 3 bits. Supposons aussi que le message déchiffré est considéré avec « bourrage correct » lorsque le dernier bloc (chiffre) est égal 0. Soient Alice ayant envoyé le texte chiffré 2||4||7||4, à savoir que $C_0||C_1||C_2||C_3$=2||4||7||4, au serveur Bob et Kevin ayant intercepté le message grâce à l'attaque de l'homme du milieu. Kevin souhaite avoir le contenu $B_0||B_1||B_2||B_3$. Comme le bourrage est correct il sait que B_3 correspond à 0. Il veut maintenant obtenir B_2. En volant la session d'Alice et en envoyant 5||7 à Bob, Bob confirme que le bourrage est correct :

6- Déduire B_2. (indication : on considère un procédé similaire à Padding oracle attacks)
7- Que doit-il faire maintenant pour calculer B_1 ?

Bon courage