IUT1, Département Réseaux & Télécommunications
Licence professionnelle RIMS 2016/2017

Sécurité des réseaux (M25)

N.B. : Tous documents autorisés
Soin, propreté et clarté seront appréciés par le correcteur.
Barême ***indicatif :*** *1 : 8 pts - 2 : 4 pts- 3 : 4 pts - 4 : 4 pts.*

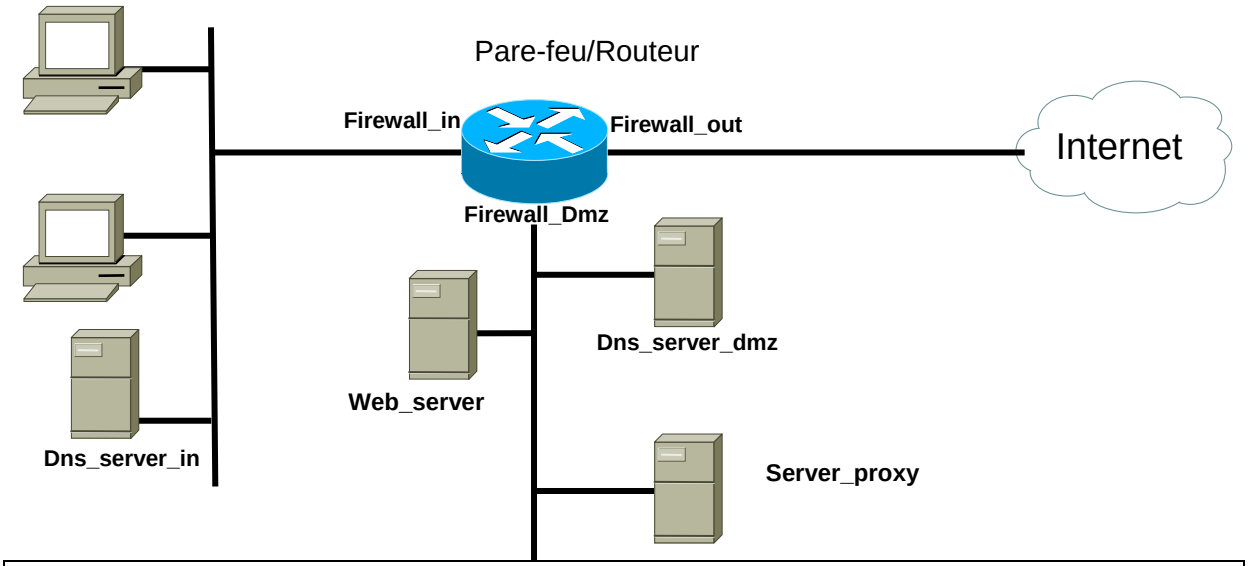
NOM :

PRENOM :

Ex 1 : Architecture autour d'un pare-feu

Un pare-feu est utilisé à l'interface entre un réseau d'entreprise (appelé "network_in"), et l'internet. Ce routeur/pare-feu est constitué de trois interfaces appelées Firewall_XX (figure ci-dessous).
Une DMZ est mise en place dans laquelle se trouvent certains serveurs, le réseau correspondant pourra être appelé « network_dmz ».
Il nous est demandé de concevoir un réseau autour de ce pare-feu/routeur. Pour cela, nous utiliserons des adressages privés pour "network_in" et "network_dmz" et nous avons une interface publique avec l'adresse 142.138.212.13.

1.1 Pouvez-vous préciser l'adressage que vous allez utiliser, sur la figure ci-dessous, sur les machines et interfaces existants ? Précisez sur quelle interface se trouvera l'adresse publique.



Expliquer:

Cahier des charges:

Pour que le réseau fonctionne, les aspects suivants doivent être pris en compte :

- Pour http : Chaque machine du réseau interne (Network_in) ne doit pas pouvoir joindre directement une machine extérieure. Le trafic doit passer par le serveur Proxy (vous pouvez utilise le service ou port “httpproxy” pour joindre le proxy et un service “service_intra” pour joindre le serveur final, ce « service_intra » regroupera par exemple les services/ports http et htttps). Nous considérons ici que les machines clientes sont bien configurées pour passer par ce serveur proxy. Vous devrez gérer les aspects liés à l’infrastructure réseau.
- Le serveur Proxy doit pouvoir joindre n’importe quelle machine à l’extérieur (« services_intra »).
- Chaque machine du réseau interne doit pouvoir atteindre n’importe quelle machine extérieure pour un ping (icmp protocol).
- Chaque machine de la DMZ (network_dmz) doit pouvoir pinguer une machine de l’extérieur MAIS ne doit pas pouvoir pinguer une machine du réseau interne.
- Le serveur DNS du réseau interne doit pouvoir joindre le DNS de la DMZ (un ensemble de services appelés “service_dns” est composé des protocoles tcp et udp, sur le port 53).
- Le serveur DNS de la DMZ doit pouvoir joindre un DNS externe avec « service_dns » (IP: 230.38.12.177).

Questions

Règles de filtrage.

On pourra utiliser une syntaxe de ce type:

'Protocole source destination service action'

Protocole: protocole concerné (on pourra mettre 'tous' si nécessaire)

Source: adresse IP de la **machine** ou du **réseau** source

Destination: adresse IP de la **machine** ou du **réseau** destination (on pourra mettre 'tous' si nécessaire)

Service: numéro de port (on pourra mettre 'tous' si nécessaire)

Action: 'passer' ou 'bloquer'

Ex:

- tcp 10.3.0.0 172.16.6.0 tous passer
- icmp 10.3.0.4 tous tous bloquer
- any 10.3.0.0 any services_intra pass

Règles de filtrage, justifier chaque règle par une phrase. Si certaines régles doivent être ordonnées, précisez pour quelle raison vous les avez ordonnées.

Ex 2 : Infrastructure à base de certificats

1. On vous demande de mettre en place une infrastructure pour héberger les sites web de l'entreprise. Vous pensez tout de suite qu'ils devront être en https. Vous allez donc utiliser des certificats. Votre entreprise a déjà sa propre autorité de certification (CA) qui n'est pas reconnue des navigateurs par défaut.
    a. A quoi vous servira la CA ?

    b. Comment ferez-vous pour que vos clients n'aient pas de message d'avertissement lors de l'accès aux sites ?

    c. Vous hébergez actuellement 3 sites (www.rmis.fr, intranet.rmis.fr, facturation.rmis.fr) dessinez l'arborescence des certificats en partant de la CA.

Ex 3 : <u>Cryptage : Inversion des bits suivant une suite aléatoire</u>

Crypter “Radis” (52 61 64 69 73, code ASCII en hexadécimal) avec la clé (suite aléatoire) (a_n) = (10, 20, 29, 15, 40, 39, 9, 35, 52, 13…) en utilisant la méthode de l'inversion des bits suivant une suite aléatoire sur des paquets de **8 bits**.

- But : Transformer chacun des **paquets de 8 bits** d’un fichier F en inversant certains bits par des opérations de négation binaire
- On considère une suite de nombres pseudo-aléatoires (a_n)
- Pour chaque octet, les bits à inverser sont obtenus en calculant le modulo 8 des termes de la suite (a_n). La suite des nombres modulo 8 sera appelée (b_n)
- Si $b_{n+1} \leq b_n$ alors on passe à l’octet suivant => le nbr de bits inversés dans un octet est aléatoire…

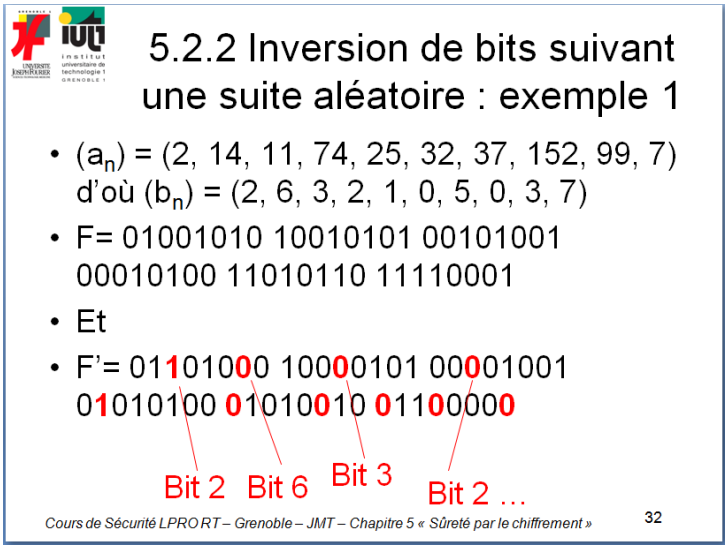


Fig : Illustration de la méthode sur des paquets de 8 bits

Ex 4 : Calcul de CRC

1) Un émetteur transmet la suite 1110 1011 suivie d'un CRC calculé avec le polynôme générateur $G(x)= x^4+x^3+x$.

a. Calculer le CRC (reste) qui sera transmis à la suite des données. Donnez l'expression de R(x) sous forme de polynôme.

b. Précisez sur combien de bits est donné le CRC. Justifiez.

c. Préciser quelle suite binaire sera finalement envoyée par l'émetteur (données + CRC).

Rappel de la méthodologie : **Les codes cycliques:**

EMETTEUR

- **Données (message à transmettre) : suite de bits représentée par M(x)**
- **L'émetteur divise $x^r.M(x)$ par G(x) avec G(x) de degré r (r + 1 bits), polynôme générateur**
- **$x^r.M(x) = G(x).Q(x) + R(x)$, le degré du reste R(x) sera au maximum de r-1 (r bits)**
- **On transmet la trame $T(x) = x^r.M(x) + R(x)$**

RECEPTEUR

- **Le récepteur divise T(x) par G(x) et doit trouver 0**