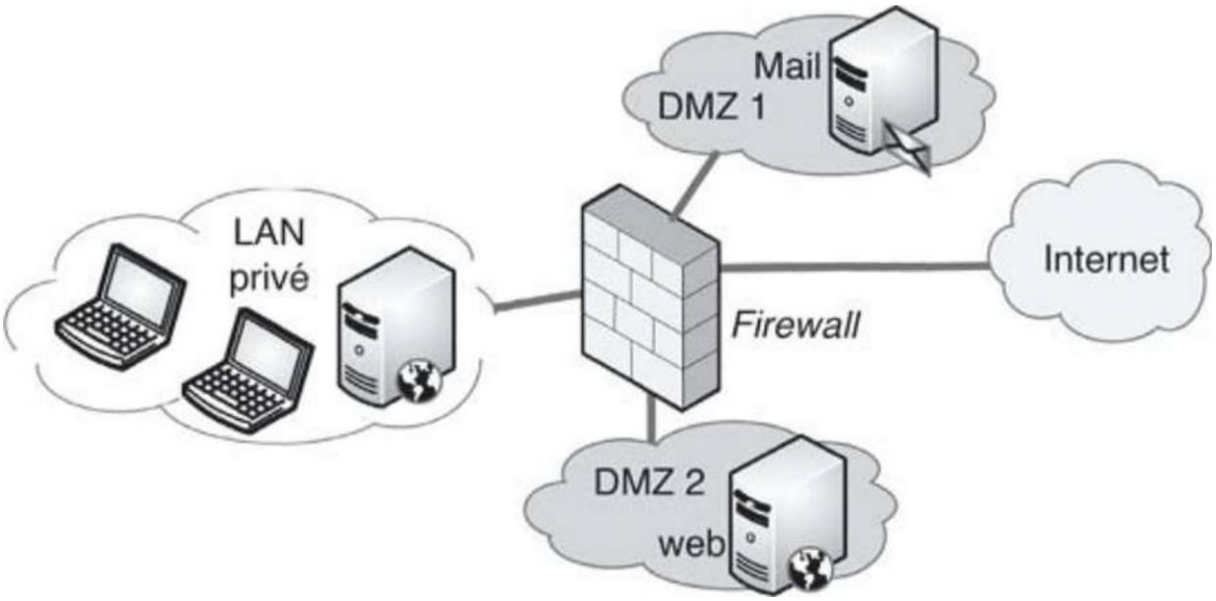
Exercice dirigé 2 – sécurité systèmes et réseaux

Exercice 1

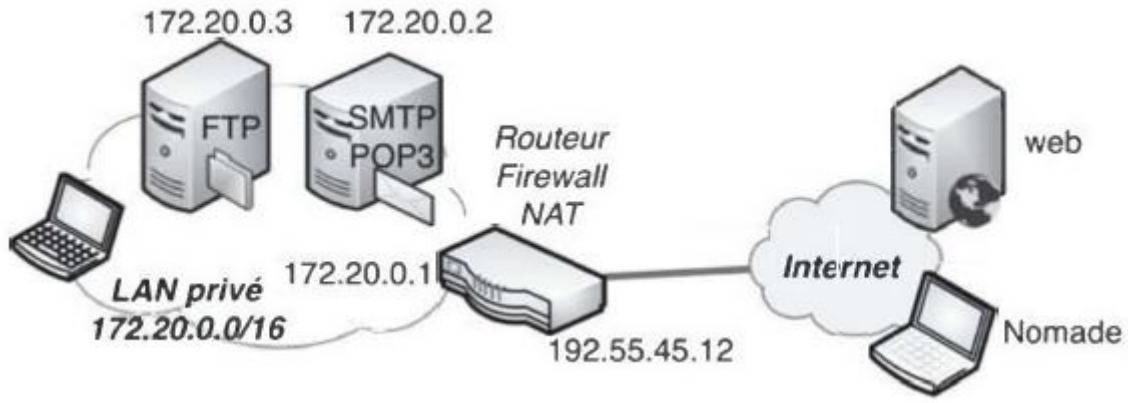
La règle A *du firewall* permet aux machines du LAN privé d'accéder à DMZ2, alors que la règle C devait l'interdire. Comment remédier à cela ?



Règle	@ src	@ dest.	Protocole	Port source	Port dest.	Action
A	Toutes	DMZ 2	TCP	Tous	80	Autorisé
B	LAN	DMZ 1	TCP	Tous	25	Autorisé
C	LAN	Toutes	TCP	Tous	Tous	Refusé
E	Tous	Tous	Tous	Tous	Tous	Refusé

Exercice 2

Un réseau sécurisé d'entreprise est décrit par la figure :



a) Écrire le tableau de règles du ***firewall*** permettant de ne laisser passer que les transferts de messagerie vers le serveur interne (protocoles SMTP et POP3) et de navigation vers l'extérieur (protocole HTTP). Dans ce dernier cas, la connexion devra obligatoirement être initiée de l'intérieur.
b) Le système de translation d'adresse (NAT) intégré au ***firewall*** utilise une adresse publique pour offrir un accès Internet aux stations et aux serveurs. Expliquer en quoi la translation d'adresse participe à la sécurisation du LAN privé. S'agit-il de DNAT ou de SNAT ?
c) D'après le schéma, quelle est l'adresse destination portée par un paquet entrant à destination du serveur SMTP ? Quelle information permet au routeur/NAT de savoir qu'il doit diriger ce paquet vers le serveur SMTP ?

Exercice 3

Vous utilisez un système de chiffrement asymétrique. Vous venez de perdre votre clé privée, mais vous avez encore la clé publique correspondante.

a) Pouvez-vous encore envoyer des mails de manière confidentielle ? Lire les mails chiffrés que vous recevez ?
b) Pouvez-vous encore signer les mails que vous envoyez ? Vérifier les signatures des mails que vous recevez ?
c) Que devez-vous faire pour de nouveau être capable d'effectuer toutes les opérations citées ?

Exercice 4

Alice transmet un document à Bob. Ce document n'a pas besoin d'être chiffré mais Alice souhaite être sûre que Bob recevra le bon document et non un document qui pourrait être fourni par l'homme au milieu.

a) Comment Alice doit-elle procéder ? Vous donnerez, en les comparant, les deux solutions avec les deux types de cryptage. Vous préciserez ce qui distingue une signature d'une authentification.
b) Ces deux solutions sont-elles totalement sécurisées contre une attaque de l'homme au milieu ?

Exercice 5 : Réseaux privés virtuels

a) Expliquez le concept et le fonctionnement d'un VPN. Vous préciserez en particulier les équipements mis en œuvre, la gestion des adresses IP et comment les messages sont encryptés.
b) Quelles sont les principales différences entre des tunnels VPN utilisant PPTP, IPSec et SSL ?

Exercice 6

Dans un paiement par carte bancaire (CB) sécurisé par le protocole https,

a) Comment le client est-il averti que la transaction est sécurisée ?

b) Comment le numéro de CB transmis est-il protégé ?

c) Quelle clé de cryptage le client utilise-t-il pour crypter les informations transmises ?

d) Comment le client est-il sûr qu'il dialogue bien avec le serveur choisi ?

e) Comment le serveur est-il sûr qu'il dialogue bien avec un client « légal » ?