TD : Sécurité réseau avec Pare Feu, NAT et DMZ

1. Principes de fonctionnement de la sécurité réseau

- Historiquement, ni le réseau Internet, ni aucun des protocoles de la suite TCP/IP n'était sécurisé. L'ouverture d'Internet aux opérateurs commerciaux et aux fournisseurs d'accès, donc aux particuliers, a rapidement débouché sur un foisonnement d'attaques (chevaux de Troie, vers, déni de service, etc). Plusieurs outils et protocoles sont alors apparus pour combler cette lacune. On peut citer entre autres :
  - Le pare feu qui filtre les paquets entrants et sortants selon le contenu des entêtes des paquets. Il est alors dit *stateless*. Si le pare feu surveille aussi l'état des connexions pendant toute leur durée de vie il est alors dit *stateful*.
  - Les versions sécurisées par cryptographie des protocoles existants (IPsec, SSH, DNSSEC, etc).
  - Les protocoles de sécurité utilitaires annexes (Kerberos, ISAKMP, IKE, etc).
  - Les bibliothèques et protocoles de cryptographie (SSL, GPG, etc) permettant de sécuriser les protocoles applicatifs (HTTPS, POP3S, IMAPS, etc).
  - Le *Network Address Translation* (NAT) qui permet d'utiliser des adresses IP privées non globalement routables et qui effectue la traduction de ces adresses privées vers des adresses publiques globalement routables et vice-versa.
  - La *De-Militarized Zone* (DMZ) qui permet de définir un réseau intermédiaire entre l'Internet et un réseau privé interne (intranet). Cette zone contient généralement des serveurs qui doivent être accessibles depuis l'extérieur.
- L'architecture de sécurité pour le protocole IP est définie dans la RFC 2401 qui est récupérable ici http://www.ietf.org/rfc/rfc2401. Il y a en tout plus de quatre cent RFCs qui traitent des mécanismes liés à la sécurité des protocoles de l'Internet.

2. Mise en place

1. Ce TD utilise l'émulateur système **`Qemu`** avec le module d'accélération matérielle **`KVM`** qui est installé sur les machines du CREMI. Pour activer **`KVM`** il faut taper la commande :
   a. **`$ ksu $USER –e /usr/bin/sudo /usr/sbin/service qemu-kvm start`**
2. Récupérez l'image **`debian1.qcow2.gz`** pour les hôtes clients et serveurs et l'image **`vyatta1.qcow2.gz`** pour les routeurs sécurisés (incluant pare feu, NAT, VPN, etc) situées sur **`/net/stockage/dmagoni`** et copiez les dans votre répertoire **`~/espaces/travail`**.
3. Récupérez la documentation de Vyatta située sur **`/net/stockage/dmagoni`** pour savoir comment configurer les routeurs.
4. Les commandes **Debian** et **Vyatta** données ci-dessous sont **à compléter correctement**, grâce aux documents fournis avec les images et au Web.
5. Pour chaque machine virtuelle, son interface **`eth0`** est connectée à l'Internet par SLIRP et elle est configurée par DHCP. Vous pouvez ainsi télécharger des paquets logiciels en utilisant la commande **`apt-get install`**.

3. Réseau intranet avec pare feu

Un réseau intranet simple est présenté sur la figure 1a. Le réseau intranet est un réseau local de type Ethernet connecté à l'Internet via un routeur d'accès. Le réseau intranet est public, donc toutes les machines ont des adresses IP publiques. Un pare feu *stateless* permet de filtrer les paquets entrants et sortants.

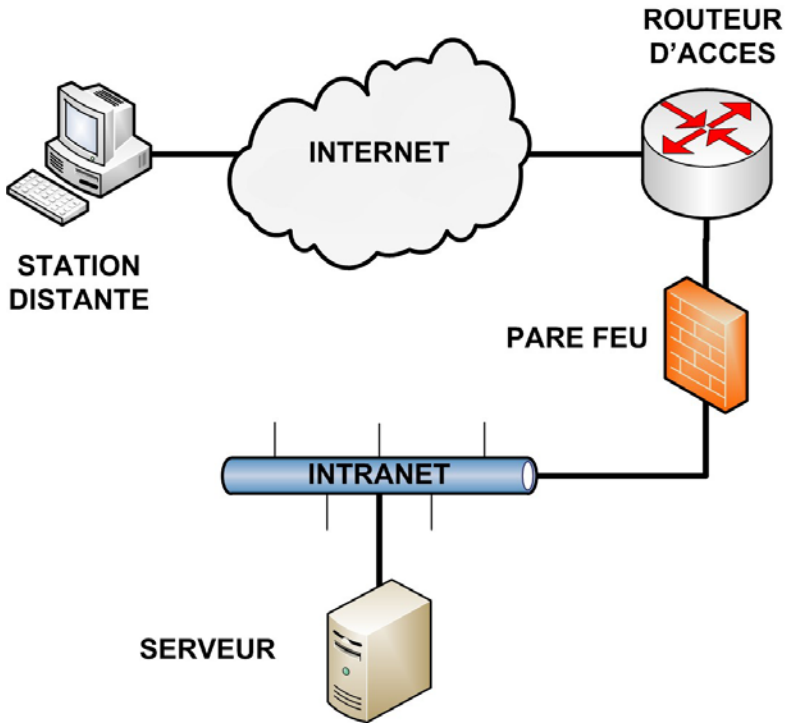

Figure 1a. Réseau intranet avec pare feu et NAT.

Pour le TD vous allez mettre en place la topologie présentée dans la figure 1b ci-dessous et que l'on considérera équivalente à celle de la figure 1a ci-dessus.

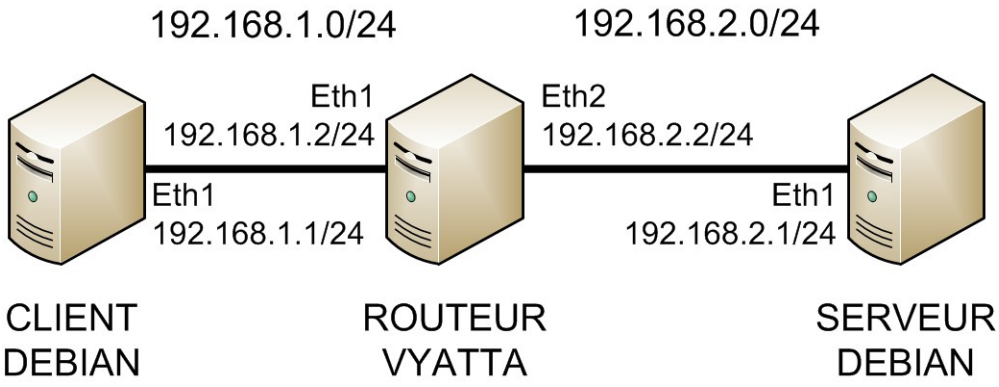

Figure 1b. Réseau 1a implémenté avec Qemu / Vyatta.

6. Créez la topologie ci-dessus en récupérant et en lançant le script **`nat1.sh`** qui va déployer les machines virtuelles et connecter les machines par des VLANs fournis par Qemu..
7. Choisissez des plages d'adresses pour chaque sous-réseau. Etablir un plan d'adressage précisant les adresses de toutes les interfaces. Vous pouvez utilisez le plan d'adressage fourni sur la figure 1b si vous le souhaitez. Configurez les interfaces des machines avec **`ifconfig`**. Configurez les interfaces des routeurs avec **`set interfaces`**. Vérifier les connexions directes par des **`ping`**.
8. Remplissez les tables de routage des machines de manière statique avec **`route`**. Remplissez les tables de routage des routeurs de manière statique avec **`set protocols static`**. Vérifiez que toutes les machines peuvent communiquer entre elles par des **`ping`**.
9. Configurez un serveur HTTP sur le serveur, un serveur Telnet sur la station distante et un serveur SSH sur le routeur.
10. Lancez **`nmap`** depuis la station distante vers le serveur. Qu'observez-vous ?

11. Lancez **`nmap`** depuis le serveur vers la station distante. Qu'observez-vous ?
12. Configurez le pare feu dans le routeur avec les règles suivantes :
    a. Autorisez les connexions depuis l'Internet vers le serveur pour le service HTTP.
    b. Interdisez toutes les autres connexions entrantes.
    c. Autorisez toutes les connexions sortantes.
    d. Autorisez uniquement les connexions SSH sur le routeur.
13. Lancez **`nmap`** depuis la station distante sur le serveur. Qu'observez-vous ?
14. Lancez **`nmap`** depuis le serveur vers la station distante. Qu'observez-vous ?
15. Configurez NAT sur le routeur d'accès (Vyatta).
16. Observez avec **`wireshark`** une connexion Telnet depuis le serveur vers la machine distante. Qu'observez-vous ?
17. A partir de quelle information le routeur identifie-t-il les connexions TCP (ou les flots UDP) de façon à retransmettre les paquets correspondants vers la bonne destination au sein du réseau intranet ?
18. Montrez comment le NAT gère le trafic ICMP à l'aide de **`ping`** et de **`wireshark`**.
19. Est-ce que le service Web est accessible ? Modifiez les règles du NAT afin qu'il fonctionne comme à la question 8.

4. Réseau avec pare feu, NAT et bastion

Un réseau intranet avec bastion est présenté sur la figure 2a. Le réseau intranet est un réseau local multipoint connecté à l'Internet via un routeur d'accès faisant pare feu et NAT. Un bastion est une machine du réseau intranet qui doit être accessible par L'Internet. Cette machine est généralement un serveur qui héberge des services devant être visibles de l'extérieur tels que le courrier électronique, le site Web, etc. Elle est situé sur un sous réseau IP spécial nommé DMZ et qui est différent du réseau intranet privé local. Elle est configurée de manière très sécurisée afin de ne pas être piratable facilement d'où le nom de bastion. Lorsqu'il n'y a, comme ici, qu'un seul bastion, celui-ci est généralement connecté directement sur le routeur et la DMZ n'est pas un réseau local multipoint. Le réseau intranet est désormais privé, donc toutes les machines ont des adresses IP privées. Un pare feu *stateful* permet de surveiller les connexions entrantes et sortantes.

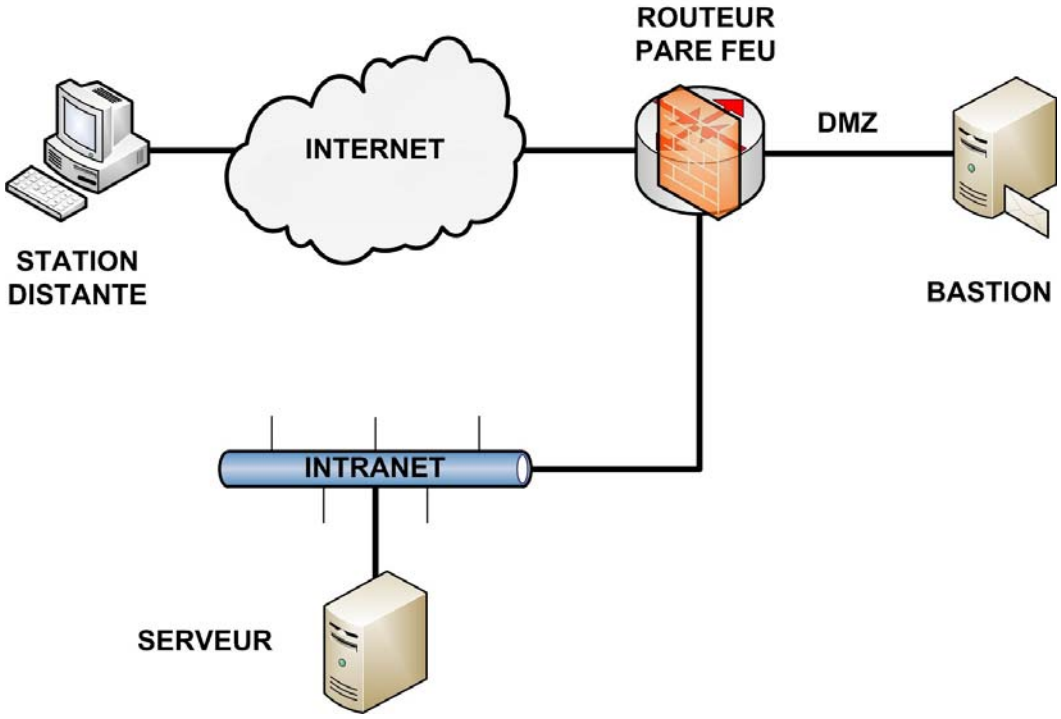

Figure 2a. Réseau Intranet avec pare feu, NAT et bastion.

Pour le TD vous allez mettre en place la topologie présentée dans la figure 2b ci-dessous et que l'on considérera équivalente à celle de la figure 2a ci-dessus.

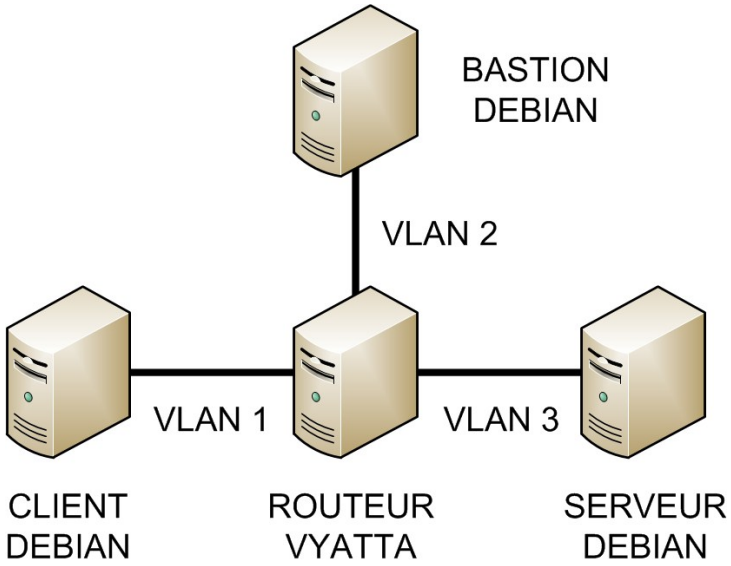

Figure 1b. Réseau 2a implémenté avec Qemu / Vyatta.

20. A partir de votre réseau précédent et en conservant sa configuration, rajoutez une machine virtuelle qui représentera le bastion et placez la dans une DMZ.
21. Configurez un serveur FTP dans le bastion. Quelle est la différence entre le mode passif et le mode actif ? Configurez le routeur pour que le service FTP soit filtré par un pare feu *stateful*.
22. Configurez un proxy HTTP dans le bastion. Observez le cheminement de deux requêtes identiques successives. Filtrez les requêtes vers les sites commerciaux.

5. Réseau intranet avec double pare feux, NAT et DMZ

Un réseau intranet avec double pare feux est présenté sur la figure 3a. Le réseau intranet est un réseau local privé connecté à un routeur interne faisant pare feu et NAT. Une DMZ contenant un ou plusieurs bastions est connectée à ce routeur interne ainsi qu'à un routeur externe faisant pare feu et routeur d'accès vers l'Internet. Cette fois la DMZ est un sous réseau IP constitué sur un réseau local multipoint de type Ethernet. Elle est protégée par le routeur pare feu externe. Les deux pare feux *stateful* permettent de surveiller les connexions entrantes et sortantes.

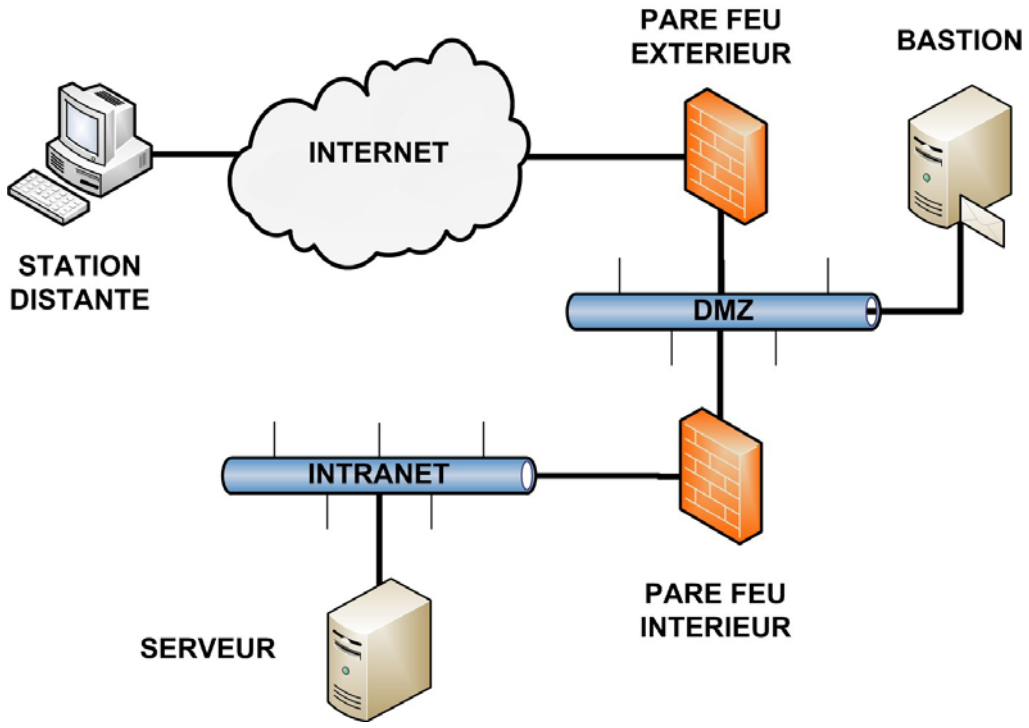

Figure 3a. Réseau intranet avec double pare feux, NAT et DMZ.

Pour le TD vous allez mettre en place la topologie présentée dans la figure 3b ci-dessous et que l'on considérera équivalente à celle de la figure 3a ci-dessus.

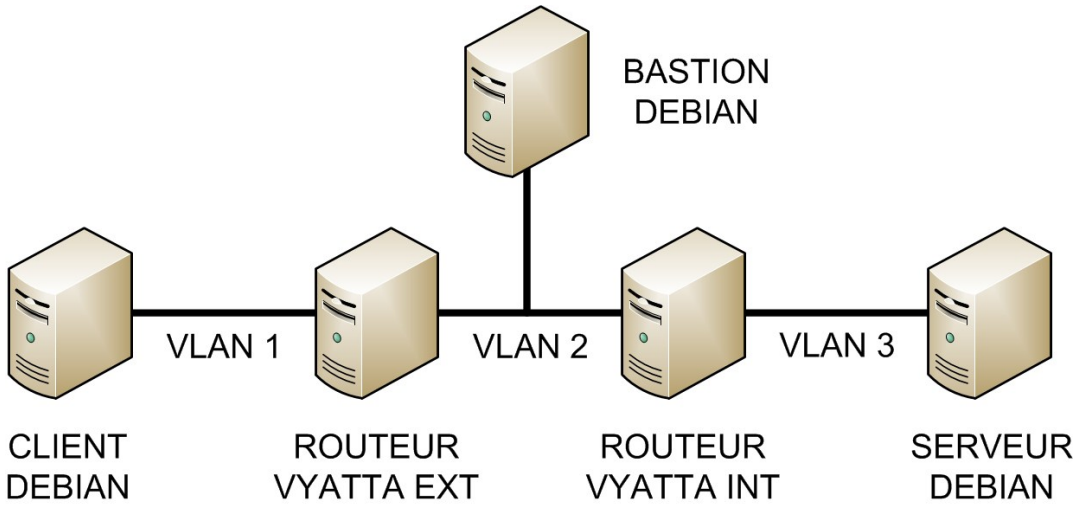

Figure 1b. Réseau 3a implémenté avec Qemu / Vyatta.

23. On suppose maintenant que la station distante est une machine d'un collaborateur nomade. Configurez les machines afin de créer un tunnel IPsec entre la machine nomade et l'intranet. Observez le trafic avec **`wireshark`** entre le client et les serveurs sur les liens VLAN 1 et VLAN 2 et commentez-le.

6. Travail à rendre

A la fin des séances de ce TD, vous rendrez un rapport de TD par binôme, au format PDF, que vous enverrez par e-mail à votre chargé de TD. Ce rapport contiendra les réponses aux questions posées dans ce sujet en y incluant tous les justificatifs nécessaires :

- Extraits pertinents des fichiers de configuration des machines et des listings des commandes Debian GNU/Linux et Vyatta utilisées pour résoudre les questions.
- Extraits pertinents des tables de routage des machines.
- Extraits pertinents des captures de trames prises par **`wireshark`** ou **`tcpdump`**.
- Sorties des commandes **`ping`**, **`traceroute`**, **`telnet`**, **`nmap`**.