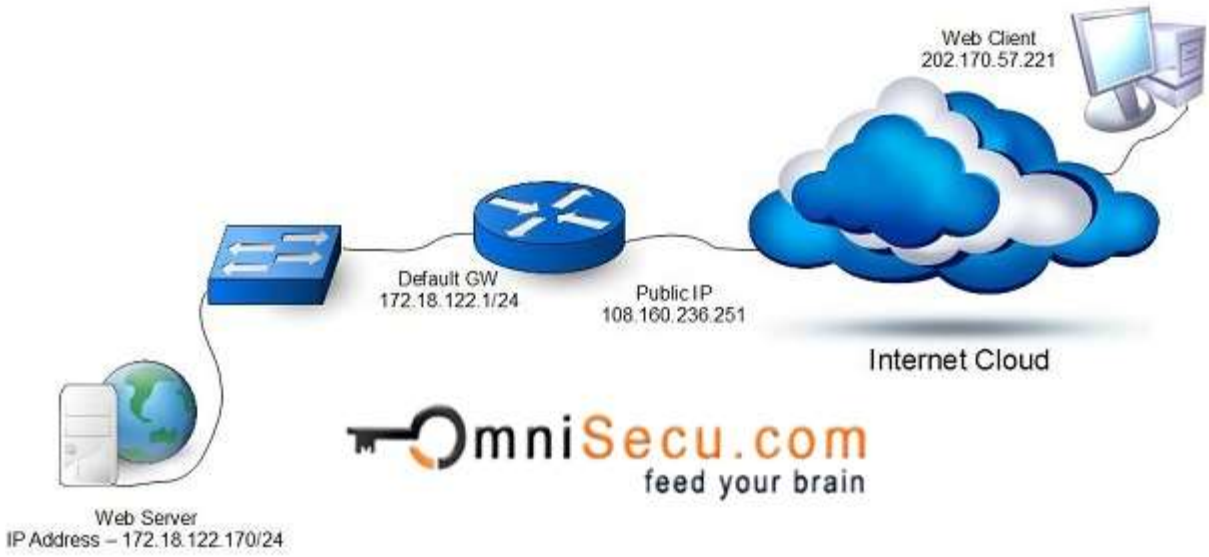
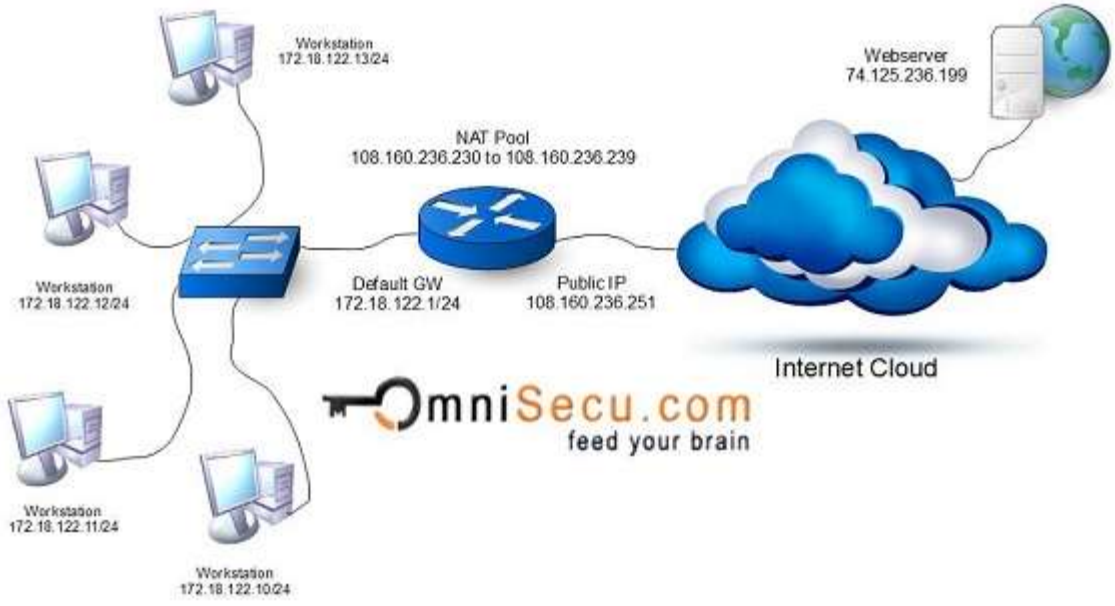
| BTS SIO<br>SISR 5 | **Le NAT et le VPN**<br>*Point du programme :*<br>- *Sécuriser une infrastructure réseau* | Fiche de synthèse<br>N° 11 |
|---|---|---|

**Le NAT :**

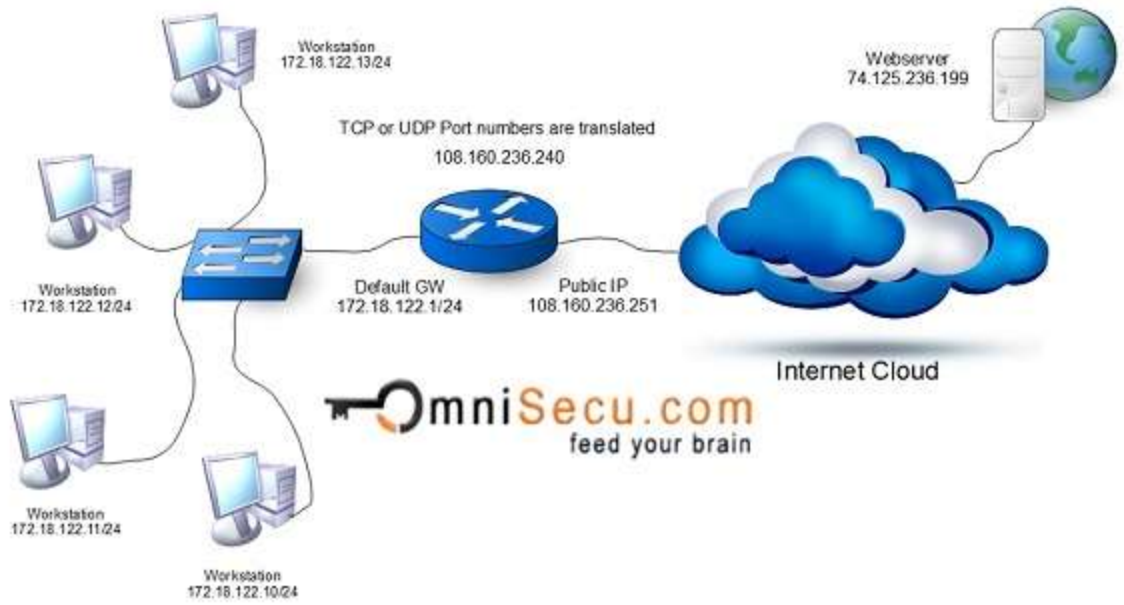
**NAT statique** (traduction d'adresse réseau) est le mappage un-à-un d'une adresse IP privée à une adresse IP publique. Le NAT statique (Network Address Translation) est utile lorsqu'un périphérique réseau à l'intérieur d'un réseau privé doit être accessible depuis Internet.




**NAT dynamique** (traduction d'adresses réseau) peut être défini comme le mappage d'une adresse IP privée à une adresse IP publique à partir d'un groupe d'adresses IP publiques appelées en tant que pool NAT. Le NAT dynamique établit un mappage un-à-un entre une adresse IP privée et une adresse IP publique. Ici, l'adresse IP publique provient du pool d'adresses IP configurées sur le routeur NAT final. Le mappage public / privé peut varier en fonction de l'adresse IP publique disponible dans le pool NAT.



**PAT (Port Address Translation)** la traduction d'adresse de port (PAT) est un autre type de NAT dynamique qui peut mapper plusieurs adresses IP privées à une seule adresse IP publique en utilisant une technologie connue sous le nom de traduction d'adresse de port. Ici, lorsqu'un client du réseau interne communique avec un hôte sur Internet, le routeur modifie le numéro du port source (TCP ou UDP) avec un autre numéro de port. Ces mappages de ports sont conservés dans une table. Lorsque le routeur reçoit d'Internet, il se référera à la table qui conserve les mappages de ports et transmet le paquet de données à l'expéditeur d'origine.




**Le VPN :**

Le VPN signifie « Virtual Private Network », en français « Réseau Virtuel Privé ». Comme son nom l'indique. Il permet de créer des réseaux virtuels. Le principe du VPN, est de créer un réseau sécurisé auquel on peut se connecter, peu importe l'endroit où l'on se trouve. Le VPN est un protocole qui permet d'échanger des données dans un tunnel chiffré.

Le VPN permet de créer un réseau virtuel privé. On pourrait se dire « Oui le VPN n'est pas très utile, pourquoi devrais t'on en utiliser un ? ». L'un des plus grands avantages du VPN est de pouvoir relier des hôtes/réseau à différents lieux géographiques, en chiffrant les données et flux transmit à l'aide d'un tunnel chiffré, ce qui rend en théorie les données indéchiffrables.

Le VPN peut être utilisé pour chiffrer une connexion, qui de base ne supporte pas le chiffrement, ou encore, si l'on se connecte sur un réseau public type « wifi gratuit », on ne sait pas, s'il n'y a pas une personne qui écoute le réseau, ou bien un « man in the middle » qui intercepte le trafic. De plus le chiffrement de données et flux permet donc de chiffrer des protocoles qui ne sont pas supportés par le chiffrement, comme le Telnet, http, ftp, etc….

Nous pouvons faire passer tous les flux dans ce tunnel, contrairement au SSH, qui lui est chiffré, mais, qui ne fait pas passer tous les flux. La différence du VPN et le SSH : le SSH permet de faire passer des flux, cependant des protocoles spéciaux et adapter au tunnel SSH doivent être développés car, ils interviennent sur la couche 3 du modèle OSI. Le SSH est utilisé par plusieurs protocoles comme « le sftp », qui est un serveur ftp passant dans un tunnel SSH, afin de chiffrer les échanges.

Le VPN intervient au niveau de la couche 2 du modèle « OSI » qui permet d'encapsuler les données et de chiffrer le contenu, car la couche 2 du modèle « OSI » permet de fournir les moyens de transférer les données à d'autres hôtes. C'est pour cela, que l'on peut faire passer tous les flux, car c'est en dessous des couches des autres protocoles.

De plus, quand on fait passer les informations dans un VPN chiffré, notre « FAI » sait que le contenu est chiffré il va en destination du serveur VPN, il n'a aucune idée des destinataires auxquels nos informations vont être envoyé. On peut utiliser un VPN pour contourner la censure ou les restrictions « des FAI ».

Les technologies VPN utilisées pour encapsuler les données et informations, qui transitent dans le tunnel les plus utilisées et les plus connues sont :

***VPN SSL:***

Aussi appelé « clientless », n'a pas besoin d'un logiciel client, seul un navigateur internet compatible avec l'ouverture des sessions HTTPS SSL/TLS est suffisant. Contrairement au VPN IPsec, le tunnel VPN SSL ne permet pas le transport de différents protocoles de communication.

***VPN IPsec:***

L'installation d'un logiciel « agent » est nécessaire, afin d'établir un tunnel vers un serveur VPN. Un Tunnel VPN IPsec permet de véhiculer différents protocoles de communication tels que Telnet, RDP, SMB, SMTP, IMAP, etc…

***OpenVPN:***

Comme son nom l'indique, OpenVPN est un protocole VPN open source qui utilise « Secure Socket Layer (SSL) » pour créer une authentification pour une connexion Internet cryptée. Dans l'ensemble, le protocole OpenVPN offre l'une des meilleures combinaisons de performances et de sécurités, il peut être utilisé pour contourner facilement les pares feux ainsi que les restrictions des FAI. Pour ce qui est des protocoles de transport OpenVPN peut utiliser l'UDP ou le TCP