Yvan Soh, François Aubert,

Emmanuel Dupal, Carl Ake, Matthieu Barthes

Atelier de professionnalisation Mr El-Idrissi

Conception et prise en charge des réseaux informatiques StadiumCompany

**Mission 3 : NAT, SSH, ACL**

# I/ Contexte

Il est important de privilégier la sécurité pour prévenir l’introduction malveillante d’autres utilisateurs ou programmes. L’accès internet devient encore plus important pour entreprises qu’on plusieurs sites que sont reliés pour se communiquer ou pour se servir de services ou bases de données centralisées sur l’un de sites.

Il est important d’utiliser l’authentification et la sécurisation des données transférés.

Pour l’authentification : L’authentification permet aussi de définir différents types de permissions selon l’utilisateurs (administrateurs, utilisateur).

Pour la sécurisation des données : Il existe différentes formes de sécuriser les données (PKI, TLS/SSL,

Telnet/SSH, PGP/GPG), ou même la combinaison de plusieurs méthodes (HTTPS, SFTP. Cette

sécurisation, ou encryptions de données, est important, parce que, même si l’accès est authentifié, si un malveillant s’introduit entre les clients et le serveur, il aura la communication en clair.

Il y a aussi le filtrage : Il est aussi important de mettre en place un système de filtrage sur le réseau que va permettre d’augmenter la sécurité du domaine, on parle d’access list. Ces listes, les ACL (Access Control List) nous permet filtrer la transmission selon l’utilisateur, à partir de leur adresse IP ou de filtrer aussi leur demande/service, selon le protocole ou le port de destination demandé.

# II/ Analyse et besoin

De forme à répondre au cahier de charges et tout l’ensemble de requis des besoins pour sécurisation des interconnexions entre les sites et l’accès internet, ainsi qu’une solution d’accès à distance on invoquer les différentes options et leurs caractéristiques respectifs de forme à arriver à une solution fiable, adaptable et évolutif.

## Configuration de Telnet et SSH

Telnet :

Utilisé pour l'accès à distance de réseaux fermés (universités, grandes entreprises), Telnet avait pour objectif de permettre l'accès, en tenant compte la nature des réseaux en question, où la transmission des données d’utilisateurs et leurs mots de passe en clair, ne représentait pas un problème.

Telnet fournit aux utilisateurs un système de communication interactif bidirectionnel, orienté texte en utilisant une connexion de terminal virtuel sur 8 octets. Les données utilisateur sont entrecoupées avec de contrôle d’informations telnet sur le protocole de contrôle de transmission (TCP).

Tout seul, c’est donc une méthode accès non sécurisé et non conseillé aux accès en réseaux comme l’internet, mais, malgré sa nature non sécure, il est possible d’utiliser autres services ensemble avec le Telnet pour sécuriser les communications.

**Commande** : R(config)# line vty 0 4

R(config-line)# pass *cisco*

R(config-line)# login local

R(config-line)# transport input telnet R(config-line)# logg sync

La syntaxe pour accéder à un serveur via Telnet est : telnet hostname port

SSH :

Avec l'évolution technologique, les réseaux se sont ouverts au monde via l’Internet et avec cela sont venus les risques de sécurité de la transmission de données en clair. Tatu Ylonen à pourtant développé SSH (**S**ecure **SH**ell) pour faire face à ces menaces.

Bien que toujours utilisé dans certains scénarios, Telnet a été largement remplacé par SSH. On estime que plus de la moitié des serveurs Internet dans le monde utilisent SSH, et presque tous les ordinateurs Unix et Linux utilisent également SSH pour la gestion à distance.

Le SSH peut utiliser différentes possibilités de méthodes d’encryptions (clé symétrique, asymétrique,

etc) pour chiffrer les données.

Le SSH utilise, par défaut, la port 22, mais les bonnes pratiques nous disent qu’il est important de

configurer un autre port pour pas s’appuyer que sur le binôme utilisateur/mot-de-passe.

Le SSH est aussi utilisé ensemble avec autres protocoles pour ajouter une couche de sécurité, comme les cas de SFTP (FTP+SSH), SCP (Secure copy : rcp-SSH), entre autres.

**Syntaxe** : R(config)# ip domain-name stadiumcompany.com R(config)# crypto key generate rsa

R(config)# 1024

R(config)# line vty 0 4 R(config-line)# login local

R(config-line)# transport input ssh R(config-line)# exit

R(config)# ip ssh version 2

R(config)# ip ssh authentication-retries 3 R(config)# ip ssh time-out 120

R(config)# exit

Logiciels accès Telnet et SSH :

* [**PuTTY**](https://www.ssh.com/ssh/putty/) cliente pour Windows et Linux
* [**OpenSSH**](https://www.ssh.com/ssh/openssh/) serveur pour Unix, Linux

**Conclusion** : SSH

On prend le choix de SSH car le Telnet n’apporte pas sécurité en transmettent les données en clair

dans le réseau.

## Configuration de NAT et PAT

NAT :

Le NAT (Network Address Translation | Traduction d’Adresse réseaux) parallèlement au VLSM (Variable Length Subnet Masking) est crucial au plan d’adressage en raison des limitations du protocole IPv4.

Il utilise un IP valide (publique) pour représenter l’ensemble de hôtes connecté dans un LAN. Cette traduction est vérifiée dans les paquets envoyé/reçu vers internet ou l’équipement qu’effectue la fonction de NAT va remplacer l’adresse IP de la source quand le paquet sort du LAN et change aussi l’adresse d’IP destination quand le paquet revient sur le LAN.

NAT Statique

Le NAT Statique consiste en une configuration ou chaque adresse IP dans le réseau aura un adresse IP privé correspondant pour se communiquer à l’internet. Donc, si une entreprise à 1 utilisateur il aura besoin d’un adresse IP privée. Pour 10 utilisateurs, 10 adresses privées. Ainsi de suite. Donc il-y-a une relation de 1 pour 1 d’adresses publiques pour chaque privée.

NAT Dynamique

L’un des principales différences avec le NAT Statique c’est le fait que le mappage entre les adresses publiques et privées, sont effectué dynamiquement, selon l’ordre d’arrivée des paquets. Une autre différence c’est la possibilité réinitialiser ce mappage ou définir le temps que ce mappage se tient, si la demande de translations s’arrête. Ça permet d’avoir plus hôtes qu’adresses privées, à moins que tous les utilisateurs effectuent leurs demandes au même temps.

PAT (NAT Overloading)

Les solutions de NAT dynamique et statique impose la nécessité d’avoir plusieurs adresses IP privées disponibles pour chaque entreprise/résidence, ce qui va contre le défi de réduire le nombre de adresses IP publiques que les entreprises ont besoin.

Le PAT vient résoudre ce problème une fois qu’il fait usage des informations contenue dans les paquets, notamment les portes TCP utilisé par les hôtes, et ainsi il peut faire une traduction de ses portes, avant envoyer cette information vers l’internet, pour faire dynamiquement un mappage entre les hôtes et le port utilisé par le NAT.

**Conclusion** : NAT Overloading (PAT)

Pour la raison invoquée pendant la description de NAT Overloading (PAT), le choix devient évident, une fois que l’utilisation de plusieurs adresses publiques ajouterait des couts inutiles à l’entreprise sans oublier que l’acquisition d’une plage d’adresses publiques est peu probable car toutes les plages d’adresses publiques ont été déjà attribuées.

## Configuration des ACL

ACL

Les ACL (Access Control List | Liste de contrôle d’accès) permettre l’identification (et ultérieurement décision) des paquets que circulent un réseau. Pour le faire, les ACL identifient values que les routeurs peuvent analyser dans l’IP, TCP, UDP et d’autres entêtes.

On peut utiliser les ACL pour différentes fonctions sur un réseaux, notamment la filtrage, application fonctionnalités de QoS. Pendant ce document, on va explorer l’ACL entant que filtrage sous les formes de ACL Standard et Etendues. Dans ces deux cas, la liste sera déployée sur une interface d’un routeur en précisent le sens (in|out) que on veut enforcer les règles. On verra que, selon le type ACL choisi e le filtre qu’on veut enforcer, il faut être judicieux dans le choix de l’interface/sens e dans quelle router, si dans notre infrastructure il en a plusieurs.

Comme le nom l’indique, les ACL sont composées de listes. C’est une liste de commandes choisi pour filtrer les paquets que circulent. Quand le router reçoit un paquet sur un interface avec une ACL en place, les commandes seront analysées séquentiellement jusqu’à trouver une correspondance. Par défaut si le router n’arrive à trouver aucune correspondance dans cette liste, elle rejet le paquet.

ACL Standard

Les ACL Standard sont les plus simples et fonctionnent en analysent les paquets d’IP pour faire coïncider la source d’adresse IP à sa liste de permissions. Grace a ce fonctionnement, il est conseillable d’implémenter les ACL standard dans l’interface le plus proche de la destination, pour éviter de bloquer par erreur des paquets concernant autres destinations. Comme identifient ils utilisent, les nombres :

* 1-99
* 1300-1999

**Syntaxe** : access-list {1-99 | 1300-1999} {permit|deny} *paramètres de recherche*

**Exemple** : access-list 1 permit 10.1.1.1

access-list 1 deny 10.1.1.0 0.0.0.255 access-list 1 permit any

Dans la syntaxe, il est possible de faire référence à un hôte précis ou sinon a une plage de adresses spécifiques. Pour les règles visent plages d’adresses, il faut indiquer au router quels octets il doit ignorer.

ACL Etendue

La plus grande différence entre les listes Standard, c’est le fait que les ACL Etendues peuvent analyser plusieurs entêtes des paquets et ainsi définir de règles plus spécifiques. On peut, par exemple, créer de commandes pour chercher les correspondances spécifiques de :

* Protocole
* IP Source
* IP destination

Les ACL Etendues utilisent, comme identifient, les nombres ;

* 100-199
* 2000-2699

**Syntaxe** : access-list {100-199 | 2000-2699} {permit|deny} {protocole} {IP Source} {Porte Source} {IP destination} {Porte destination}

**Exemple** : access-list 100 permit tcp 10.1.1.1 0.0.0.255 10.1.1.2 0.0.0.255 eq 21 Les portes de source destination et source, sont optionnelles.

# III/ Application

**Commande SSH :**

enable conf t

enable password cisco enable secret Btssio2022$

ip domain-name stadiumcompany.com crypto key generate rsa

1024

line vty 0 4 login local

transport input ssh ip ssh version 2

ip ssh authentication-retries 3 ip ssh time-out 120

exit

**Commande ACL :**

access-list 10 permit 172.20.0.0 0.0.0.255

access-list 11 permit 172.20.1.0 0.0.0.255

access-list 12 permit 172.20.2.0 0.0.0.255

**Commande NAT :**

enable conf t

int fa 0/0.10 ip nat inside exit

int fa 0/0.11 ip nat inside exit

int fa 0/0.12 ip nat inside exit

int fa 0/0.1

ip nat outside exit

ip nat inside source list 10 interface fa0/1 overload ip nat inside source list 11 interface fa0/1 overload ip nat inside source list 12 interface fa0/1 overload

**IV/ Conclusion**

On prend le choix de SSH car le Telnet n’apporte pas sécurité en transmettent les données en clair dans le réseau. Le choix du PAT peut faire une traduction de ses portes, avant envoyer cette information vers l’internet, pour faire dynamiquement un mappage entre les hôtes et le port utilisé par le NAT.