**Réalisation d’un réseau d’entreprise sécurisé**

**Par M. Saidi (saidi@univ-paris13.fr)**

Les réseaux de grandes entreprises peuvent s’étaler géographiquement sur plusieurs sites (ex. le réseau de l’université Sorbonne Paris Nord est un parfait exemple). Concevoir de tels réseaux requiert souvent l’interconnexion de plusieurs sites en traversant des réseaux non sûrs (Internet). Plusieurs méthodes et procédés existent pour interconnecter ces sites, parmi lesquels nous citons la technologie MPLS (qui offre plusieurs garanties de service mais qui reste coûteuse pour les entreprises) ou les tunnels sécurisés (Ipsec, ssh, ..), ou non (GRE pour l’IP dans IP, ..).

Dans ce projet, nous proposons d’utiliser des tunnels sécurisés (Ipsec/Isakmp/Esp) pour relier au travers de l’Internet deux sites d’une même entreprise. Cela permettra par exemple aux employés du site 2 d’accéder aux services réseaux déployés sur le site 1 (intranet) alors que les autres utilisateurs de l’Internet n’ont pas accès à ces services (filtrage aux entrées des sites 1 et 2).

Pour aller plus loin, nous proposons d’implanter un extranet pour les clients de l’entreprise. Cet extranet offrira un serveur web aux clients de l’entreprise. Nous n’implémenterons pas de méthode d’authentification (nous supposerons que tous les utilisateurs de l’Internet sont potentiellement des clients de l’entreprise) mais nous nous assurerons que la compromission de ce serveur web (ou du réseau supportant ce serveur) n’ait pas de conséquences ou d’impact sur la sécurité des réseaux des deux sites de l’entreprise. Pour ce faire, nous implémenterons géographiquement ce service web près du site 1 mais dans un réseau isolé (site 3), c’est-à-dire dans une zone démilitarisée (DMZ).

Pour les besoins de ce projet, un fichier .pkt (packet tracer) vous sera fourni. A vous de compléter les configurations afin d’implémenter le réseau de l’entreprise en suivant sa politique de sécurité.

Pour ce projet, vous consulterez le fichier pkt pour identifier les bouts du tunnel Ipsec, déterminer les adresses IP à utiliser, etc. Toutes les informations nécessaires à la réalisation de ce projet sont renseignées ci-après ou dans le fichier pkt.

**Mots clés :** partitionnement d’un réseau sur plusieurs sites, IPSEC/ISAKMP/ESP, firewall, intranet, extranet, zone démilitarisée.

**Logiciel :** Cisco Packet Tracer 8.1. Un compte netacad est nécessaire pour utiliser ce logiciel.

**Documents :** Nombreux sur Internet les documents qui décrivent les procédures de création de tunnels Isakmp/Ipsec et la configuration de firewall.

**Tâches :**

Plusieurs tâches doivent être réalisées :

1. Routage static pour assurer la connectivité depuis/vers l’Internet. Cette tâche est déjà réalisée dans certains projets.
2. Tunnel Ipsec à établir entre les équipements illustrés dans le fichier pkt.
3. NAT pour les réseaux des différents sites pour accéder à l’Internet (sauf mention contraire explicite dans le pkt).
4. Filtrage de tout le trafic externe aux sites 1 et 2. Seules des réponses aux requêtes (TCP, UDP et ICMP) initiées par des machines des deux derniers sites sont admises.
5. Filtrage du trafic IP issus des interfaces autres que celles sur lesquelles sont connectés les réseaux des sites 1 et 2.
6. Implémentation du zone démilitarisée (site 3) accessible de l’extérieur pour un seule machine sur le port 80.
7. Configuration et initialisation de machines + serveurs (effectués dans le pkt).
8. Tests.

**Documents :**

Listes de filtrage:

https://www.cisco.com/c/fr\_ca/support/docs/ip/access-lists/44541-tacl.html

ASA to ASA VPN :

http://net.cmed.us/Home/cisco/asa-83-vpns/asa-to-asa-vpn-83

NAT :

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

ASA static routing :

https://www.networkstraining.com/configure-static-routing-on-cisco-asa-firewall/

Access rules :

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\_84\_cli\_config/access\_rules.html

Introduction listes d'accès :

https://www.technologuepro.com/reseaux/Configuration-des-ACLs/les-ACLs.html