TP Sécurité Licence Professionnelle RIMS

Pare-feu (2022-2023)

I - Objectifs

Dans ce TP nous allons utiliser un pare-feu (firewall) pour connecter un réseau d'entreprise à Internet. Plusieurs aspects vont être abordés :

- La définition des différents réseaux de l'entreprise
- Le routage et l'interconnexion
- La mise en place des règles de translation
- La définition des règles de sécurité
- La connexion par Réseau privé virtuel (VPN) de clients distants

II - Présentation de la plate-forme

1 - Description générale

Pour ces travaux pratiques, vous disposez de :

UTILISATEUR DE DROITE

- 2 postes sur un réseau local (en fait deux machines virtuelles sur le poste physique droit) **ServinX** et **PosteX**.
- 1 pare-feu matériel ASA 5505 CISCO SP.

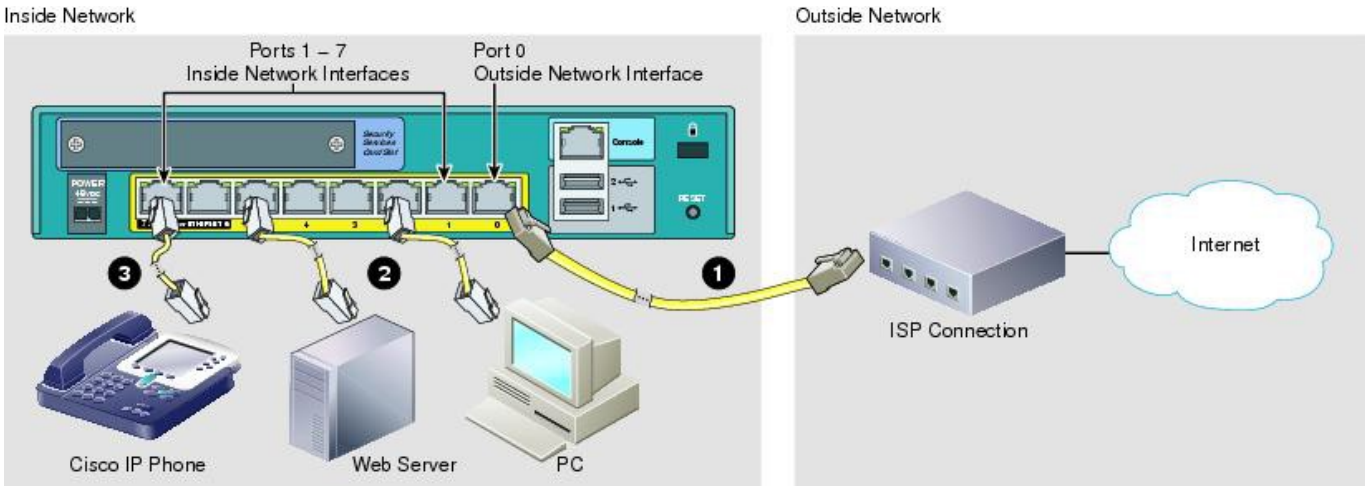
UTILISATEUR DE GAUCHE

- 1 poste serveur Web de l'entreprise dans la DMZ (machine virtuelle dans la machine physique gauche) **ServeurX**
- 1 poste utilisateur extérieur (machine virtuelle dans la machine physique gauche) **ClientX**

Vous serez amenés à utiliser les logiciels suivant à télécharger directement sur Internet (ou à récupérer sur la page du Professeur http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/lpro/for_labs/Firewall-lab.zip) :

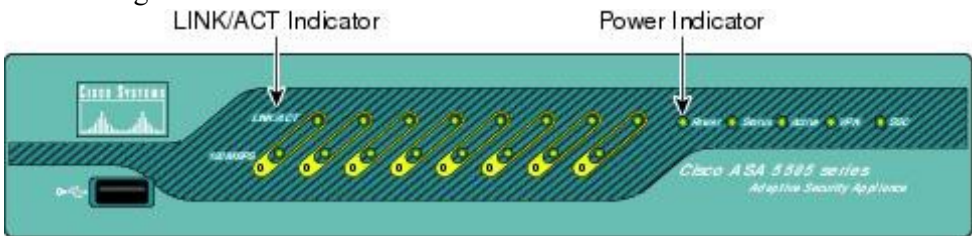
- Wireshark et la bibliothèque Winpcap : Logiciel d'analyse de trames
- Putty : Console en mode texte pour accès telnet et SSH (Secure Shell)
- JRE : Java Runtime Environment version 6 **(n'utilisez que cette version !, pas une version plus récente). => Accessible sur** http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/lpro/for_labs/Firewall-lab.zip

Le pare-feu que nous allons utiliser est un ASA 5505 de la société CISCO. **CISCO** propose entre autres dans son catalogue des gammes de routeurs, de commutateurs et de pare-feu. Les pare-feu récents se nomment **ASA Gamme 5500** (modèle 5505, 5510 ou 5515). On trouvait auparavant l'appellation **PIX** pour les pare-feu Cisco. Le modèle à disposition aujourd'hui est donc le **ASA 5505**, plus petit pare-feu de la gamme. La licence présente est la licence « Security Plus ». Vous pouvez voir en annexe les différences entre la licence de base et cette licence « Security Plus ». Les performances de ce pare-feu permettent une utilisation dans des structures relativement importantes (plusieurs dizaines d'utilisateurs). Son prix était d'environ 1000€ HT avec les différentes licences d'utilisation. En face arrière, on retrouve 8 ports, comme le présente la figure suivante issue de la documentation Cisco livrée avec le pare-feu.



Le **port 0** sera utilisé pour l'interface **externe**.
Les **ports 1 à 7** permettent la connexion des équipements internes.
Les **ports 6 et 7** permettent au besoin la connexion d'équipements de type POE (téléphone IP ou caméra par exemple). POE signifie Power Over Ethernet, soit alimentation électrique par le câble ethernet.
Il est possible de paramétrer plusieurs VLANS sur ce switch interne, typiquement 3 pour les réseaux interne, externe et une DMZ.
Notons la présence du bouton RESET en bas à droite.

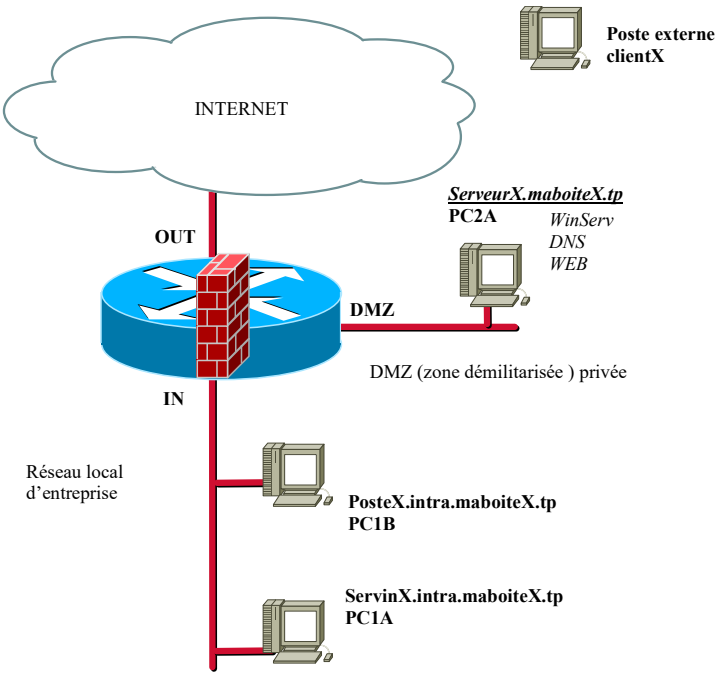
ATTENTION : SVP : la connectique d'alimentation est très très fragile !!!! Manipulez avec précaution le matériel.
La face avant de l'équipement est visible sur la figure ci-dessous :



Du classique donc, avec des leds pour indiquer les différents états. Le modèle 5505 n'est pas "rackable 19 pouces". Mais des kits permettent son adaptation à ce standard, afin de l'insérer dans une armoire réseau. Ses grands frères par contre le sont. Le système installé est le firmware de version 8.3.

L'adresse pour l'interface externe sera 10.X.1.11, avec X votre numéro classique de binôme dans les salles de TP Réseaux.

Nom et adresse IP	**Groupe X**
Entreprise	**MaboiteX**
*IN (adresse **réseau**)*	**192.168.1.0/24**
IN interface	**192.168.1.254**
OUT interface	**10.1.X.11**
DMZ interface	**192.168.2.254**
Client externe *adresse IP*	**clientX** **10.1.X.10 (« réseau public »)**
Machine PC1B	**PosteX.intra.maboiteX.tp**
Machine PC1A	**ServinX.intra.maboiteX.tp**
Machine PC2A	**ServeurX.maboiteX.tp** **192.168.2.51**
SI BESOIN MACHINE PHYSIQUE GAUCHE	**10.1.X.1**
MACHINE PHYSIQUE DROITE	**10.1.X.2**



2 - Mise en place du réseau

PosteX (PC1B) et ServinX (PC1A) sont des machines virtuelles dans la machine physique de DROITE.
ServeurX (PC2A) et le « client externe » sont des machines virtuelles dans la machine physique de GAUCHE
Câbler le réseau à partir des indications données.

Les postes PC1A (**ServinX**, serveur DNS Interne et Active Directory) et pc2A (**ServeurX**, serveur Web et DNS) sont des serveurs WinServ. Les mots de passe sont **Toto123** (ou **toto**).
Les postes PC1B et clientX seront installés en Windows 10.

☝ Veillez à désactiver les pare-feu Windows (ceux-ci empêchent les machines de répondre aux pings).

III - Configuration élémentaire du Pare-feu (UTILISATEUR DE DROITE)

1 - Configuration de base (directement sur la machine physique de droite)

Sur la clef USB si besoin récupérez le programme PUTTY et le copier sur la machine physique de droite
Reliez ensuite le câble console Cisco à ce poste et connectez-le à l'ASA. Puis avec l'outil « **putty** », par une liaison de type « **Serial** », connectez-vous. (Nota : attention de bien configurer l'interface COM).

Les commandes de réinitialisation complètes (SVP, pas d'erreurs en tapant les commandes !!!!) sont les suivantes :

- **enable** (mot de passe vide ou bien **toto**)
- **configure terminal**
- **clear configure all**
- **crypto key zeroize rsa**
- **revert webvpn all**
- **config factory-default 192.168.1.254 255.255.255.0**
- **reload save-config noconfirm**

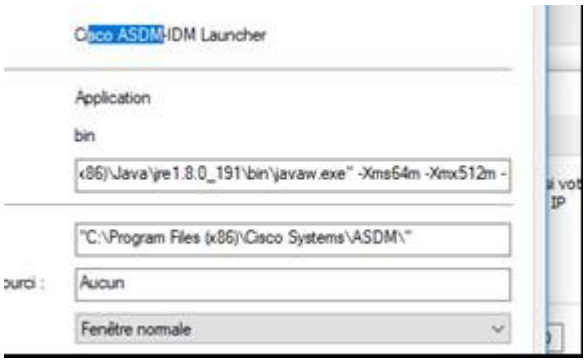
Ces commandes rechargent une configuration « usine » en conservant le mot de passe, et en attribuant une adresse IP à l'interface interne.
Vous pouvez essayer "ping 192.168.1.254" depuis le pare-feu lui-même.

2 - Première connexion au pare-feu :

Reste à installer un environnement Java. L'exécutable est sur le bureau. Installez JRE (VERSION 6 UNIQUEMENT !).
Le pare-feu est alors accessible avec un navigateur Web, à l'adresse https://192.168.1.254. Le mot de passe de l'ASA est vide ou **toto**.

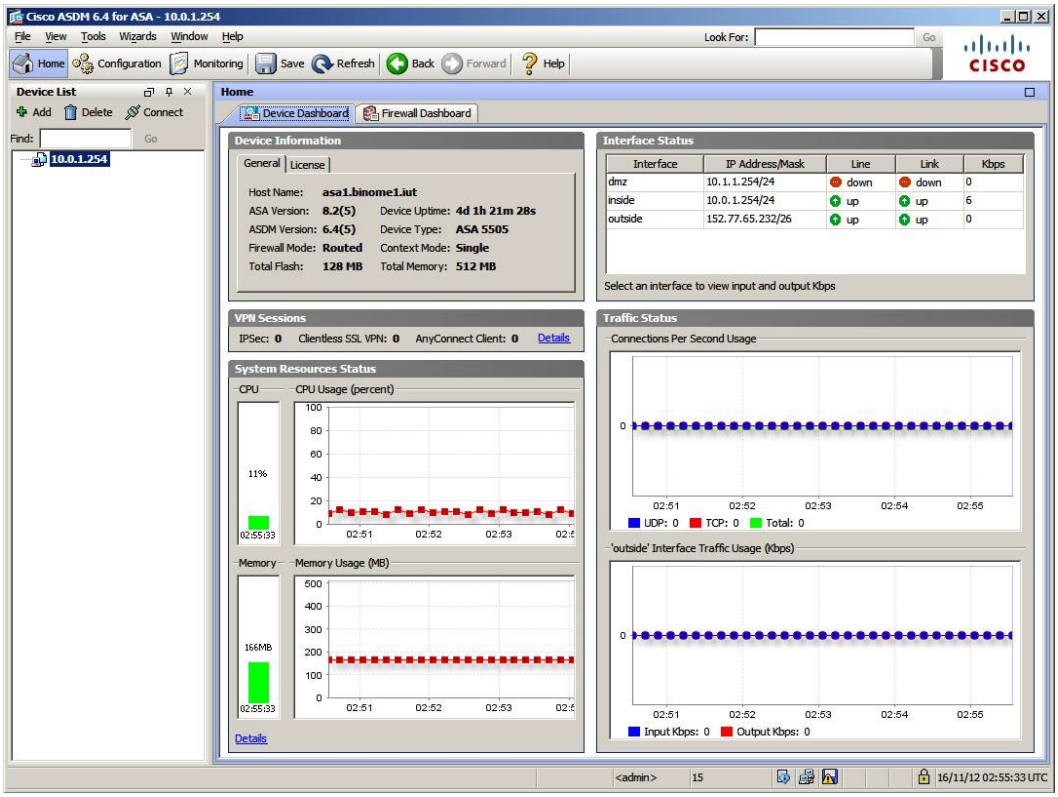
Installez l'interface d'administration ASDM (Choix du haut, le choix « **Run ASDM** » n'installe pas l'outil mais le lance depuis le navigateur). Lancez cet outil (pas de compte, mot de passe vide ou **toto**).

Pour que cela fonctionne, il faudra ici utiliser la version 6 du JRE et exécuter « `javaw.exe` » (et non pas `javawx.exe` »)…



A la question « **Cisco smart Call home** », choix du bas : « **Do not enable Smart Call Home** ».

Une fois connecté voici l'écran d'accueil type :

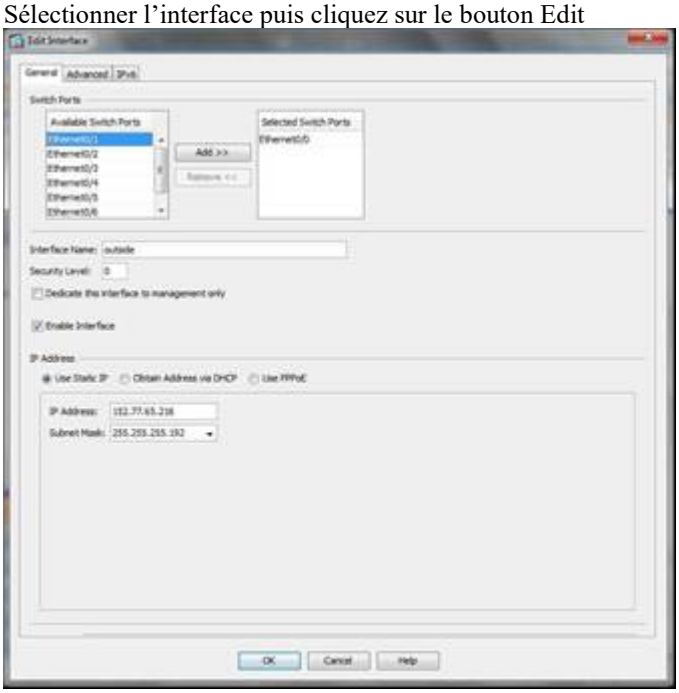


Initialement :

- L'interface Ethernet0/0 est dans le Vlan 2, c'est-à-dire dans le réseau OUTSIDE.
- Les interfaces Ethernet0/1 à 7 sont dans le Vlan 1, c'est-à-dire le réseau INSIDE

On peut alors configurer les différentes interfaces :

- Interface Ethernet 0/0 est déjà dans le réseau OUTSIDE
  - Sélectionner l'interface puis cliquez sur le bouton Edit



Le nom de l'interface doit être outside et l'option security level à 0. Ce champ correspond au niveau de confiance accordé au trafic qui arrive sur cette interface. 0 = aucune confiance

  - Dans IP Address, choisir « Use Static IP »
    Donner une adresse IP et un masque correspondant à votre groupe.

Cliquer sur « OK » pour valider la configuration et changer d'interface.

- Interface Ethernet 0/1 DMZ
  - Cliquez sur le bouton « Add »
  - Dans le menu déroulant « Switch Ports », sélectionnez Ethernet 0/1 puis cliquez sur Add

- Donnez un nom à l'interface dans le champ Interface Name : DMZ
- Donnez un niveau de sécurité. Security Level = 50
- Dans IP Address, choisir « Use Static IP »
- Donnez une adresse IP et un masque de votre réseau DMZ

Cliquer sur « OK » pour valider la configuration et changer d'interface.

- Interfaces de votre réseau interne Ethernet0/2 à 7
  - Rien de plus à faire l'interface a été configurée lors de l'initialisation
  - A noter le Security Level qui est à 100, la valeur maximale.

Valider la configuration par le bouton Apply.

☝ Un bon réflexe consiste à sauvegarder la configuration une fois que vous en avez validé le fonctionnement.

a. *Icône Configuration/Device Setup – Routing*

- Déroulez le Sous menu de routing
  - Choisir StaticRoutes puis le bouton « Add »
  - Choisir l'interface reliée au réseau externe
  - Nous voulons définir la route par défaut Network, elle devra comporter la valeur « any »
  - Pour que le trafic soit envoyé vers le routeur de l'UGA sur l'adresse IP 10.1.X.254
  - Cliquez sur « OK »
  - Cliquez sur « Apply »

b. *Icône Configuration/Firewall - Objects*

Examiner les différents onglets proposés et les valeurs préconfigurées.

- Menu « Objects » puis « Network Objects/Groups ».

Ajouter un item pour chacun des serveurs. On pourra définir un item pour chaque serveur même s'ils sont sur la même machine (On peut par exemple définir l'objet Serv_www et l'objet Serv_ftp avec la même adresse IP)

Définir les objets **Serv_web**, **Serv_ftp**, **Serv_dns_dmz** et **Serv_dns_intra.**

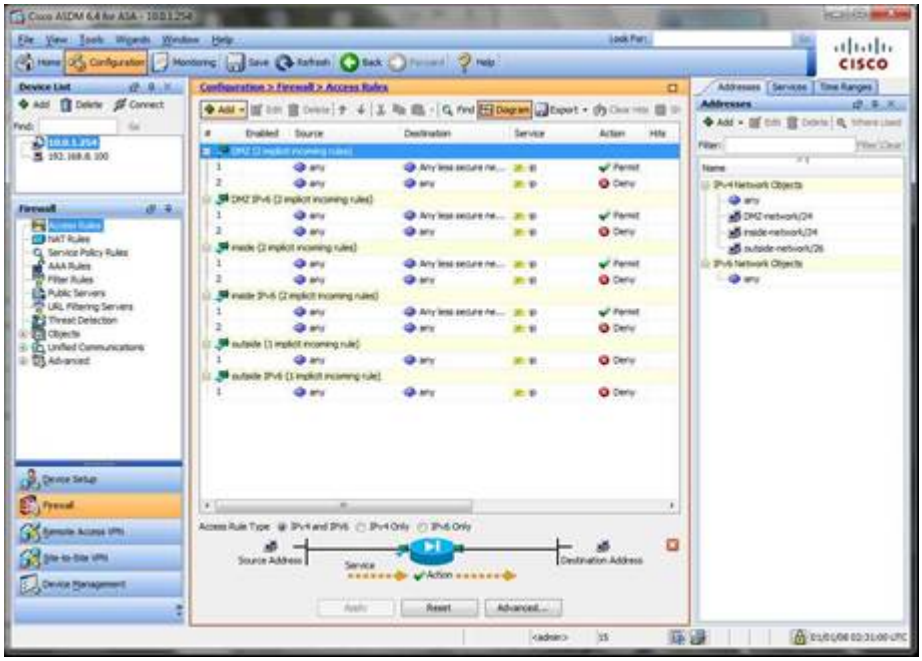
Il faut également créer une machine "routeur_out" avec l'adresse 10.1.X.254.

c. *Icône Configuration/Firewall – NAT Rules*

- Le pare-feu est configuré par défaut avec une règle autorisant tout le trafic du réseau interne à rejoindre l'extérieur.
- Il faut ajouter une règle de NAT pour le réseau de la DMZ. S'inspirer dans un premier temps de la configuration de l'interface « inside » pour configurer la même règle (nous utilisons « NAT dynamique », pas « statique », pourquoi ?).

d. *Icône Configuration/Firewall – Access Rules*

- Par défaut le pare-feu Cisco laisse passer tout le trafic IP d'une interface ayant un « Security Level » élevé vers une autre ayant un niveau inférieur.



Dans cet état de fonctionnement, les machines du réseau interne devraient communiquer librement avec les machines de la DMZ et avoir accès à l'extérieur.

☞ Voir en annexe les différentes possibilités de translation d'adresse :

FAIRE VALIDER - La communication des machines entre elles, et avec l'extérieur (par exemple avec 8.8.8.8)

IV - Configuration des machines

1 - Configuration des serveurs

a. Configurer le serveur Windows Interne (UTILISATEUR DE DROITE)

- Configurer le réseau :
- Adresse IP : 192.168.1.1 /24, Gateway 192.168.1.254, DNS : 127.0.0.1,
- Nom de machine **ServinX.intra.maboiteX.tp**

Allez sous **Démarrer** **=> Server Manager** pour changer le nom de l'ordinateur

Nous allons ajouter les rôles serveur DHCP, active Directory et serveur DNS à votre serveur : (programmes/outils d'administration/gérer votre serveur) (ATTENTION ! Ne pas prendre la configuration par défaut et préférer une installation de chacun des éléments dans l'ordre…)

- Ajouter d'abord le rôle Serveur DHCP
  i. Etendue : **etendueX**
  ii. Plage d'adresses **192.168.1.100 à 192.168.1.250**
  iii. Routeur **192.168.1.254**
  iv. Domaine parent : **intra.maboiteX.tp**
  v. Dns : **dns.intra.maboiteX.tp** (IP : **192.168.1.1**) dns sera un alias pour **ServinX.intra.maboiteX.tp**
  vi. Gérer le serveur DHCP et (dans le menu action) l'autoriser à délivrer des adresses.

Etapes pour l'installation de l'"Active Directory"

Pour utiliser la commande, cliquer sur **Démarrer** => **Exécuter =>** puis écrire **dcpromo, ensuite l'installation sera automatique** => Cliquez **OK**
Suivre ensuite les étapes proposées par l'interface utilisateur :

- Ajouter le rôle contrôleur de domaine Active Directory.
  i. C'est un nouveau domaine dans une nouvelle forêt.
  ii. Le domaine s'appellera **intra.maboiteX.tp**
  iii. Choisir des autorisations conformes au modèle Windows Server
  iv. Valider les propositions suivantes.
  v. Donner un mot de passe pour le mode restauration (choisir **Toto**)
  (N. B. On peut ouvrir ici une console de gestion "mmc" en cliquant sur **Démarrer** => **Exécuter =>** puis taper ensuite **mmc** => Cliquer **OK** et mettre dedans les différents utilitaires "DHCP", "DNS", "Observateurs d'événements", "Active directory"…)
  Note : Vérifiez les contraintes de mots de passe et leurs longueurs
  Nom Netbios = servinX
  Forest root domain name = intra.maboiteX.tp

A la fin de l'installation, la page **Additional Domain Controller Options** apparaîtra, cochez la case qui apparaît et cliquez sur Suivant pour que l'installation se termine.
Redémarrez ensuite le système.

- Ajouter le rôle serveur DNS.
  i. Créer une zone directe et une zone inverse (zone principale) : intra.maboiteX.tp
  ii. Autoriser les mises à jour dynamiques
  iii. Créer la zone inverse **1.168.192.in-addr.arpa**
  iv. Rediriger les requêtes vers le serveur (de la DMZ) 192.168.2.51
  v. Le serveur ne pourra trouver les indications de racine pour le moment, ce n'est pas grave, noter cependant le message d'erreur.
  vi. Dans la zone directe donner un alias à la machine **ServinX** (alias : **dns.intra.maboiteX.tp**)
- Dans la base de données des utilisateurs Active Directory
  i. Créer un compte **Albert Legrand**, login **alegrand**, mot de passe **Toto123** (un mot de passe trop simple est refusé par le système, vérifiez les contraintes de mot de passe)
  ii. L'étude de Active Directory est un très vaste sujet qui ne sera pas abordé aujourd'hui.

b. Configurer le serveur Serveur.maboiteX.tp (UTISATEUR DE GAUCHE).

Sur le serveur Windows Server de la DMZ, nous allons mettre en place partiellement un DNS.

Configurer le réseau :

- Adresse IP : **192.168.2.51**/24, Gateway **192.168.2.254**, DNS : 127.0.0.1,
- Nom de machine **ServeurX.maboiteX.tp**

Ajouter le rôle serveur DNS. (*programmes/outils d'administration/gérer votre serveur*)

i. Créer une zone directe et une zone inverse (zone principale) : **maboiteX.tp**
ii. Ne pas autoriser les mises à jour dynamiques (on n'utilisera ici ni DHCP ni Active Directory)
iii. Créer la zone inverse **2.168.192.in-addr.arpa**
iv. Rediriger les requêtes vers une machine externe : **195.83.24.30** (ou 152.77.1.22)
v. Le serveur ne pourra trouver les indications de racine pour le moment, ce n'est pas grave, noter cependant le message d'erreur.

Configurer le serveur WEB.

- Activer sur le serveur de la DMZ les services WEB. (Gérer votre serveur/installation des services IIS). `(Ajouter un rôle => "Application server" (IIS, ASP.NET) => Manage this application server => "Internet Information Service Manager")`
- Dans la page de gestion du site, repérer l'emplacement de la page par défaut.
  Avec un éditeur de texte changer le titre en « page d'accueil du site de la société **maboiteX** ». sous **Site and rename actions => rename**
- Notre serveur est maintenant prêt à accueillir des connexions.

Tester l'accès en local, cela permet de vérifier que les services IIS (Internet Information Services) sont bien activés.

2 - Configuration du client (UTILISATEUR DE DROITE)

Configurer PosteX en DHCP et lui faire récupérer sa configuration par ipconfig /renew. (**Démarrer** => **Exécuter** => puis taper **cmd** => Cliquer **OK** pour faire apparaître la ligne de commande)

Pour changer le nom en posteX, le domaine le compte **alegrand**, cliquez sur **Démarrer** => **mon ordinateur** => **informations système**.
Insérer le poste au domaine Windows Server.
Note : il vous faudra quelque chose comme ceci **INTRA\alegrand** puis le mot de passe **Toto123** (quel est le nom de ce domaine ?).
Puis, après redémarrage, se loguer sous le compte **alegrand**.

V - Configuration de la sécurité (Etape 1 : pings et web) (UTLISATEUR DE DROITE)

Remarque :
Vous devrez toujours utiliser les adresses réelles des machines même si de la translation d'adresse est mise en oeuvre.

Editer des règles pour chaque service peut conduire à des règles de filtrage de plusieurs dizaines de ligne ou centaines de lignes. Pour réduire la complexité de la configuration il est possible de créer des groupes d'objets ou de service. Les groupes de services vont s'avérer très utiles.
On pourra par exemple utiliser des groupes pour les fonctions Web, pour le mail etc.

***Dans** Configuration/Firewall/objects/Services groups*

- Créer un groupe **services_intra** qui sera utilisé par les clients du réseau interne et inscrire les services http et https, les accès FTP vers l'extérieur.
- Créer un groupe **services_dmz** avec les mêmes propriétés.

Ouvrir les accès depuis le réseau interne vers l'extérieur.

i. Pour les services du groupe **services_intra**
ii. Pour les requêtes ping sortantes.

Ouvrir les accès depuis la DMZ vers l'extérieur.

iii. Pour les requêtes ping sortantes vers l'extérieur (mais pas vers le réseau interne)
iv. Pour les services du groupe **services_dmz.**

QUESTION :
A ce stade, en toute logique, avec les règles de sécurité imposée, on ne devrait même plus pouvoir se connecter au Pare-feu avec l'outil d'administration. Pourtant cela marche quand même. Qu'en pensez-vous ?

Configuration de la sécurité (Etape 2 : DNS)

Faire en sorte que les machines du réseau **intra** puisse effectuer une résolution de nom.
Attention ! Ces machines doivent utiliser **ServinX.intra.maboiteX.tp** comme serveur DNS.
ServinX.intra.maboiteX.tp doit rediriger les requêtes sur **dns.maboiteX.tp**

Il pourra être nécessaire de mettre en oeuvre quelques outils de déboguage, par exemple :
Sur les serveurs DNS, activer les logs (on écrira les logs dans c:\logs\dns)

On peut également télécharger (ou récupérer sur la page web du Professeur) et installer **Wireshark.** (Il est alors nécessaire de télécharger également et d'installer une librairie Winpcap)

ICI, tous les postes doivent accéder au WEB - Faire vérifier les règles de filtrage !!!! Et soyez sûr de bien avoir mis **router_UGA** dans la passerelle par défaut du pare-feu

FAIRE VALIDER - Montrer la console de gestion "mmc"
- Montrer la configuration du PosteX (utilisateur, n° IP)
- Montrer le fonctionnement des pings avec les noms de domaine maboiteX.tp, intra.maboiteX.tp

VI - Mise en oeuvre des logs du Pare-feu – Surveillance (UTILISATEUR DE DROITE)

Utilisation du monitoring intégré au logiciel ASDM Cisco

Dans le Cisco ASDM cliquez sur « Monitoring » puis le menu « Logging ». Choisir « Enable Logging » puis « OK ». Cliquez alors sur le bouton « View »
Nous avons alors une vue en temps réel des connexions transitant par le pare-feu.

- Examinez par exemple quels sont les paquets refusés par le Pare-feu (Quelle règle en est responsable ?).

Cet outil sera très pratique pour déboguer et surveiller le Pare-feu.
N.B. A cause, par exemple, du proxy (port 3128) pour accéder à l'internet, il faudra créer et utiliser un "objet" proxy.
Proposer des règles de filtrage (et créer un objet « serveur-proxy ») permettant de joindre le serveur proxy de l'UGA (en fait sous l'ancien nom UJF) **(www-cache.ujf-grenoble.fr**).

A titre de vérification, prouver le fonctionnement d'une règle à l'aide du Monitoring intégré

VII - Un peu plus loin avec le Pare-feu

1 - Mise en œuvre du filtrage sur protocole : (Configuration/Firewall/Service Policy Rules)

Les précédentes règles de sécurité ont été configurées au niveau des couches 3 et 4 du modèle OSI. Les Pare-feu spécialisés comme le ASA 5505 offrent également des possibilités de filtrage au niveau applicatif, par analyse des messages échangés par les couches hautes. Nous allons ainsi pouvoir éliminer le trafic Internet passant sur le port 80 n'étant pas du vrai trafic http.

Allez dans le menu « Configuration/Service Policy Rules » puis le bouton « Add ». Sélectionnez l'interface concernée (nous allons inspecter le trafic de l'interface inside) puis cliquez sur « Next ». Choisir l'inspection de tout le trafic puis cliquez sur « Next ». Maintenant nous allons appliquer les règles d'inspection pour le trafic http, le bouton « Configure » s'active, cliquez. A présent il est possible de définir des règles de filtrage plus fines. Choisissez la définition de règles personnalisée puis regarder dans les différents menus ce qu'il est possible de faire. On remarquera par exemple qu'il est possible de bloquer le trafic des applications de peer-to-peer qui tentent d'utiliser le port 80.

2 - Translations d'adresse destination (« Configuration/Firewall/Nat Rules »)

Nous avons déjà vu comment permettre aux utilisateurs des réseaux internes d'avoir accès à Internet. Nous allons maintenant voir comment permettre au monde extérieur l'accès à notre serveur WEB.

L'accès se fera pour les utilisateurs extérieurs en se connectant au site à l'adresse **10.1.X.11**…
Le routeur sera alors chargé de rediriger la connexion sur le serveur interne.

- A l'aide de la documentation du Pare-feu, ajouter la règle pertinente dans « Configuration/Firewall/NatRules »

- L'adresse « publique » du site Web est **10.1.X.11**…, on aimerait pouvoir donner cette adresse aux utilisateurs internes, notamment à travers le système DNS. Mais un problème se pose : Un utilisateur interne peut-il accéder au site à travers cette adresse ? Pourquoi ?

Nous allons pour pallier ce défaut, rerouter les requêtes internes à destination du serveur web **10.1.X.11** vers le serveur web de la DMZ.

- Utiliser une redirection pour effectuer cela. (Attention au choix de l'interface sur laquelle s'effectue la redirection).

- Mettre à jour le **serveur dns de la DMZ** pour que le serveur soit accessible de l'intérieur par **www.maboiteX.tp.**

Est-il possible de faire fonctionner la résolution DNS pour les utilisateurs extérieurs ? Pourquoi ?

3 - Configuration de la détection d'attaque

L'ASA 5505 permet de bloquer des hôtes qui tentent des attaques de types DOS ou Scan.

a. Etude du cas de FTP.

En utilisant un poste client de votre réseau, vérifier dans Internet explorer que le client est configuré en mode passif.
Sur le Pare-feu, désactiver le plug-in FTP de l'ASQ.

Essayez de vous connecter au site ftp://ftp.rtgrenoble.fr
Que se passe-t-il ?
Réactiver le plug-in FTP. Vérifier que FTP fonctionne à nouveau. **Expliquer**

b. Etude du cas de http.

De très nombreuses attaques ont lieu par *buffer overflow* sur les serveurs Web.
Une chaîne de caractères imprévue, souvent longue, est passée à un formulaire et déclenche un fonctionnement non conforme du serveur. Pour éviter ceci, il est possible de configurer le pare-feu pour limiter la taille d'une Url qui passe sur le réseau :

- Démarrer le serveur web sur le poste serveur.
- Vérifier que ce serveur est accessible depuis le réseau interne.
- Configurer le plugin http pour limiter la taille d'URL à 128 octets.
- Puis consulter l'URL suivante : http://**10.1.X.51**/123456189123456789 (séquence 123456789 à répéter une quinzaine de fois)
- Consulter les logs et constater la remontée d'une alarme.

D'autres Plug-ins permettent des actions spécifiques, en particulier la vérification de la conformité des messages avec les RFCs.

FAIRE VALIDER
- Fournir un schéma explicatif convaincant du fonctionnement du plug-in FTP.
- Montrer le fonctionnement du filtrage d'URL
- Montrer l'accès au serveur web de la DMZ depuis l'extérieur, et les règles (translation, filtrage) associées.

VIII - Mise en oeuvre d'un tunnel VPN

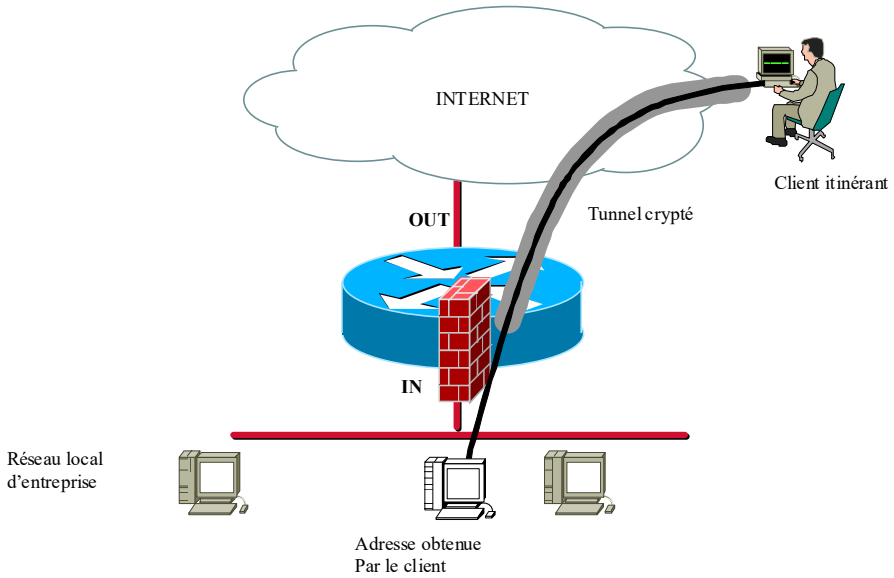
Il existe plusieurs types de VPN, VPN site à site ou VPN pour donner un accès à un client distant afin qu'il puisse accéder aux ressources du réseau de l'entreprise. Commençons par ce second type de VPN.
Plusieurs possibilités sont apparues depuis la mise en place des VPN.
- Les VPNs de type PPTP, (Point to Point Tunneling Protocol) qui sont des VPNS très simples à mettre en place, mais utilisant des algorithmes de base n'offrant pas une grande sécurité. L'avantage est donc cette simplicité de mise en place, la compatibilité avec de nombreux périphériques. PPTP a été élaboré par Microsoft et est livré avec les systèmes Windows depuis Windows 98. Tous les ordinateurs Microsoft peuvent établir des connexions PPTP nativement. Nous ne mettrons pas ce type de VPNs en place, l'ASA permettant des configurations plus intéressantes et beaucoup plus sécurisées.

- Les VPNs de type L2TP, beaucoup plus sécurisés lorsqu'ils sont utilisés avec Ipsec (on parle de tunnel L2TP/Ipsec), sur des bases de L2F de Cisco et PPTP de Microsoft. Ils restent toutefois plus difficiles à mettre en oeuvre.

- Les VPNs de type SSL, (nommés VPNSSL). Dans ce cas, il est possible d'utiliser un client dédié (Anyconnect de Cisco dans notre cas) ou tout simplement un navigateur Web récent. Les possibilités peuvent être vraiment très intéressantes si on utilise des configurations un peu complexes, comme nous allons le voir.

Commençons par utiliser ce dernier type de VPN.
Clientless… donc sans client dédié. La connexion se fera grâce au navigateur présent sur le poste externe. La philosophie est la suivante : la connexion par VPN sera autorisée ou non suivant des stratégies d'accès définies sur l'ASA. Ces stratégies sont appliquées à des utilisateurs, présents dans la base locale des comptes de l'ASA ou des utilisateurs configurés sur un serveur et dans ce cas, le lien entre l'ASA et le serveur peut se faire par l'intermédiaire de plusieurs méthodes.
Nous mettrons en place trois méthodes différentes pour valider l'accès au VPN :
- interrogation d'une base locale de comptes sur l'ASA
- interrogation de l'annuaire LDAP du contrôleur de domaine
- interrogation d'un serveur d'authentification, basé sur le protocole RADIUS.

Commençons par le cas d'une base locale.

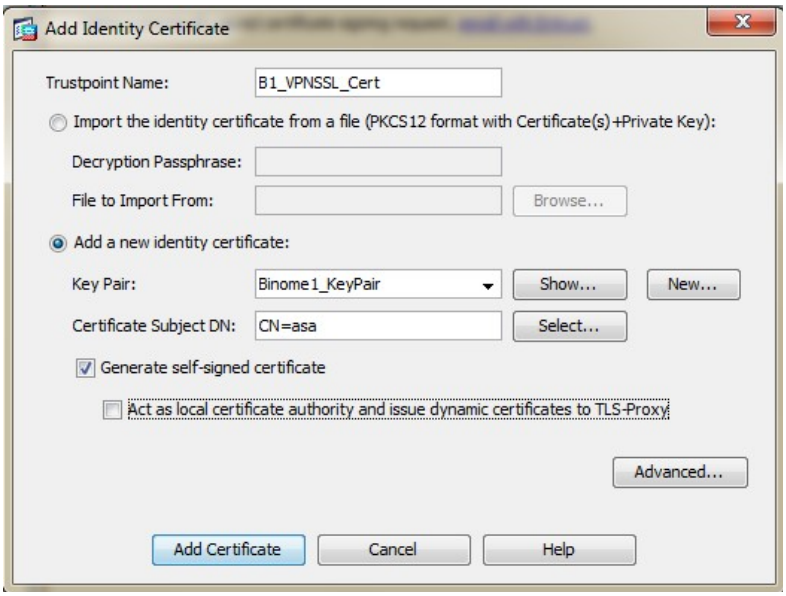


Etape 1 : Création d'un Certificat

Les connexions SSL nécessitent l'échange de clefs publiques au travers de certificats. Il nous faut maîtriser le certificat utilisé dans nos connexions de type SSL.
Créons un certificat pour ce type de VPN.

Dans « **Device Management** », « **Certificate Management** », « **Identity Certificates** ». Sur la droite, deux possibilités :

- Créer son propre certificat, qui ne sera pas reconnu comme étant émis par une autorité de certification connue des navigateurs classiques, mais qui ne nous coûtera rien
- Passer par une autorité de certification (CA) reconnue.

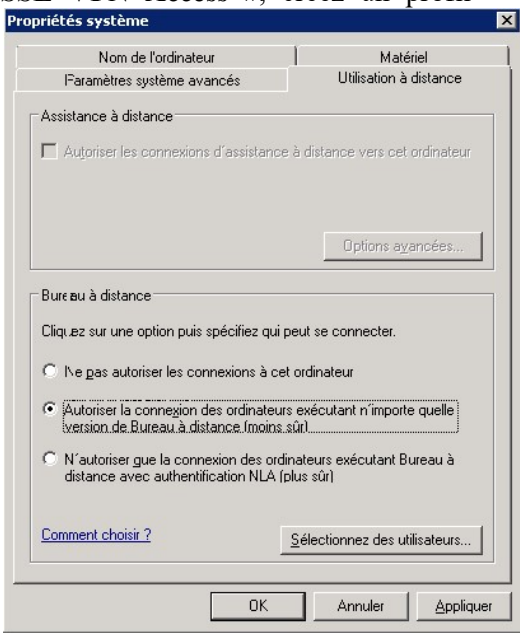


Cliquez sur « **Add** », puis, commencez par générer une nouvelle paire de clefs (« New »), nommée « **BX_KeyPair** ».
Entrez ensuite en haut un nom de certificat (« **BX_Cert** »), cochez « **Generate self-signed certificate** » et cliquez sur « **Advanced** ». FQDN doit avoir la valeur « **asa.binomeX.iut** ». Laissez les deux autres champs vides. « **Ok** » pour revenir, puis « **Add Certificate** ». Montrez le nombre d'années de validité de votre certificat. Voilà, nous avons un certificat pour nos tunnels, dont le tunnel SSL. Continuons les étapes de mise en place.

Etape 2 : Préparation de la page d'accueil.
Dans « **Remote Access VPN** », « **Clientless SSL VPN Access** », de nombreuses possibilités de configuration, mais on peut noter le terme « **Portal** » et le terme « **Customization** ». L'idée générale étant de proposer une page d'accueil aux utilisateurs arrivant par un tunnel SSL, en leur donnant des choix d'accès à des serveurs de type Web, FTP, Windows, SSH et RDP (connexion graphique à un serveur Windows).

Trouvez comment fournir un accès aux données partagées par le serveur Active Directory

Création d'un compte local et d'une stratégie pour ce VPN.
Parmi les « **Wizards** », « **SSL VPN Wizard** » choix « **Clientless SSL VPN Access** », créez un profil de connexion nommé « **BX_Profile_Connexion** », interface « **Outside** », utilisant le certificat précédemment créé (figure de droite).



Repérez les URL pour accéder au tunnel. Etape suivante : indiquez que vous allez utiliser un compte local qu'il faut créer. Le compte se nommera **USERSSL** (mot de passe **USERSSL**).
Etape suivante : créez un nouveau « Policy Group » nommé « **VPNSSL_PolicyGroup** ».

Enfin, étape suivante : ajoutez notre liste de bookmarks.
Le VPN est fonctionnel, mais d'abord, une correction sur le compte **USERSSL**. Vérifiez en éditant ce compte (dans « **AAA/Local Users** », « **Local Users** ») les droits d'accès donnés à ce compte. Inutile que ce compte ait un accès complet, le choix « **No ASDM, SSH, Telnet or Console access** » suffit.
Avant de tester, sur Windows Server, se loguer en admin (« **BINOMEX\Administrateur** » après l'installation d'AD) et faire un clic droit sur l'icône « **Ordinateur** », puis « **Propriétés** ».
La figure au bas de la page précédente vous montre ce qu'il faut faire pour accepter des sessions RDP.

Testez le bon fonctionnement de votre VPN depuis le navigateur du poste client, en utilisant l'adresse **https://@IP_externe.** Bien entendu, le certificat présenté n'est pas reconnu comme de confiance par le navigateur. Acceptez-le. Vous pouvez alors éditer le certificat envoyé et visualiser les données de ce certificat.
Acceptez son utilisation, et vous obtenez la page d'accueil voulue (ci-contre).

Redirection de port
Une autre amélioration très utile est possible : la redirection de port.
Grâce à elle il est possible par exemple de donner au poste externe un accès bureau distant sur le serveur AD.

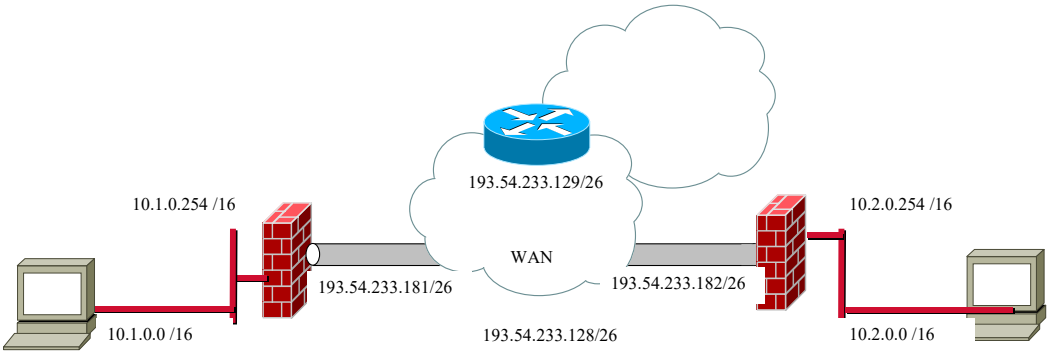
Pour réaliser ceci, les opérations sont très simples sur l'ASA :
Dans « **Remote Access VPN** », « **Clientless SSL VPN Access** », « **Portal** », « **Port Forwarding** », ajoutez une nouvelle liste nommée par exemple « **BX_Ports** ».
Dans cette liste, ajoutez la redirection du port local 10000 vers le port 3389 (port utilisé par RDP) du serveur Windows Server.
Sauvegardez.
Avec « **Assign** », appliquez cette redirection de port au Group Policy « **VPNSSL_PolicyGroup** ».
Appliquez les changements. Reloguez vous depuis le client. Il arrive que les connexions ne fonctionnent plus. Dans ce cas, ce sont des mauvaises déconnexions qui empêchent les nouvelles connexions, le quota ayant été atteint.
Dans ce cas, « **Monitoring** », « **VPN** », « **VPN statistics** », « **Sessions** », puis filtrez les connexions « **Clientless SSL VPN** ». Supprimez les anciennes connexions.
Une fois connecté depuis le client, choisissez « **Application Access** », « **Start Applications** ». La redirection de port fonctionne. Testez depuis l'outil « **Bureau à distance** » la connexion RDP vers le serveur. Elle est entièrement opérationnelle.

FAIRE VALIDER - le fonctionnement du tunnel SSL

IX - Interconnexion de sites par un tunnel VPN IPsec

L'objectif est maintenant d'interconnecter les deux réseaux locaux privés des deux sites des deux groupes d'étudiants à travers un tunnel sécurisé. A travers ce tunnel, toutes les communications seront autorisées.
Le mécanisme de sécurité mis en oeuvre s'appelle IPsec. Le principe consiste comme pour SSL à négocier des paramètres de sécurité, puis à construire un tunnel crypté. Cependant, IPsec possède beaucoup plus de possibilités et est par conséquent plus complexe. (Voir cours sécurité).
Nous allons mettre en place l'architecture suivante dans laquelle les deux réseaux conservent leur accès habituel à Internet mais devront passer par le tunnel pour communiquer ensemble directement :

Nous construirons d'abord un lien IPsec à clés pré-partagées. Dans ce mode, un mot de passe secret connu des deux extrémités sera utilisé pour l'authentification mutuelle. (Attention ! Les adresses IP mentionnées dans la figure ci-dessous ne correspondent pas forcément à la réalité de votre TP).

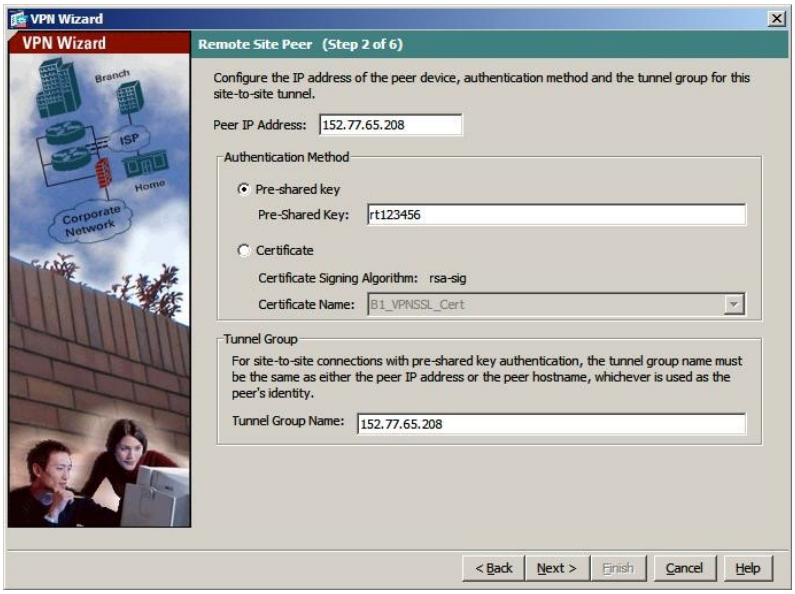


Plusieurs étapes sont nécessaires :

- Définir la clé pré-partagée :
- IPsec se déroulant en deux phases, définir les paramètres de négociation de la phase 1 puis ceux de la phase 2
- Modifier les règles de routage et de filtrage pour autoriser la circulation du flux IPsec.

Créer préalablement les objets :

- **Firewall_distant** (adresse publique de l'autre pare-feu)
- **Réseau _distant** (réseau interne distant)



Dans « **Configuration** », « **Firewall** », « **Objects** », « **Network Objects/Groups** ». Cliquez sur "**Add**" puis sélectionnez « **Network Object** ».
Soit Y le numéro du binôme distant.
Entrez les informations suivantes : nom "**Reseau_BY**", IP Address « **10.0.Y.0** », Netmask « **255.255.255.0** ».
N'oubliez pas d'appliquer vos changements en bas de la fenêtre « **Apply** ». Dans le menu « **Wizards** », sélectionnez l'élément « **IPsec VPN Wizard** ». Sélectionnez « **Site-to-site** », puis « **Next** ». Dans la deuxième fenêtre, vous allez renseigner l'adresse du pare-feu du binôme distant avec lequel vous allez créer ce tunnel. Insérez une clé de partage « **rt123456**».
Effectuer un ping vers le réseau distant. Normalement tout devrait fonctionner. Compte tenu du temps d'établissement du tunnel, il est possible que le premier paquet soit perdu.

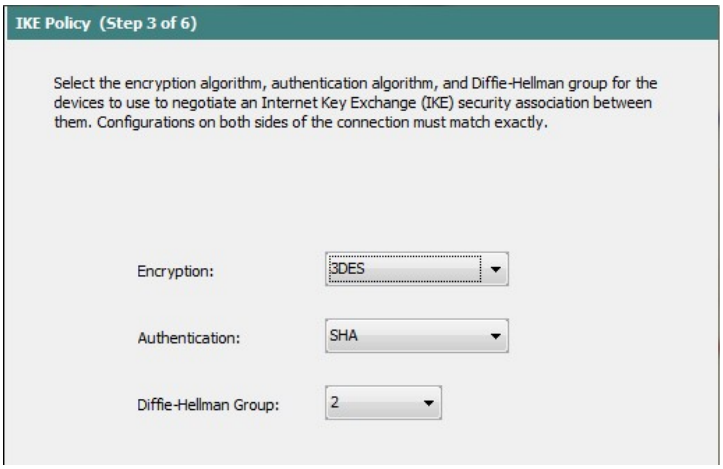
ATTENTION, vous devez avoir la même clé de l'autre côté du tunnel. Ne touchez pas au « **Tunnel Group Name** » proposé par le Wizard.
Les deux prochaines étapes permettent de sélectionner les protocoles de cryptage et les méthodes d'authentification. En effet, l'utilisation d'Ipsec met en place deux phases distinctes.

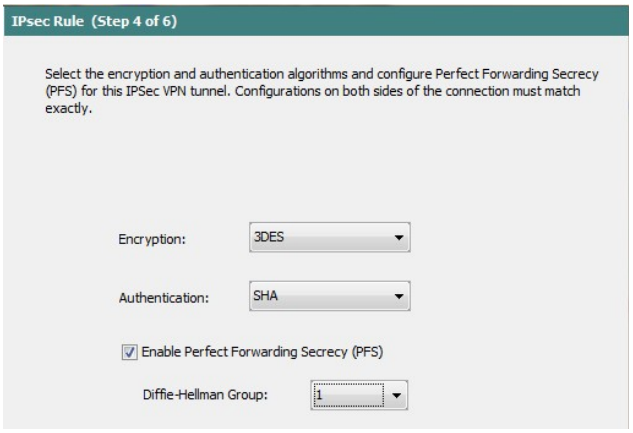
- La première phase permet la reconnaissance des deux entités qui s'échangent des informations et mettent un place un premier tunnel crypté. Le protocole utilisé se nomme IKE (Internet Key Exchange). Les choix proposés ici (3DES, SHA et Diffie-Hellman Group 2) sont des choix sûrs.

Pour information, l'algorithme Diffie-Hellman permet aux deux entités de s'échanger une clef en assurant que seules ces deux entités connaissent la clef échangée (utilisation des signatures).

- La seconde phase s'appuie sur deux protocoles :
  - o Le premier protocole se nomme AH (Authentification Header), il permet de confirmer de façon certaine l'identité des participants au tunnel. AH ne permet pas de crypter les données.
  - o Le second protocole se nomme ESP (Encapsulating Security Payload) qui lui chiffre les données Deux modes possibles, le mode tunnel étant le plus sécurisé.

De nombreux articles expliquent en détail ces protocoles. Pour de plus amples renseignements sur les mécanismes d'encapsulation mis en place par ces protocoles, citons l'article du site suivant :
http://www.securiteinfo.com/cryptographie/IPSec.shtml
Ces protocoles sont configurés par les deux étapes suivantes : laissez les valeurs par défaut et cliquez sur **next**. (Notons qu'il est déconseillé d'utiliser DES et MD5, algorithmes ayant été « cassés », ce qui n'est pas le cas, en principe mais difficile de savoir…, de 3DES, AES, blowfish, SHA et d'autre protocoles présentés).





Dans l'étape 5, sélectionnez votre réseau local et le réseau local distant.
Laissez la dernière ligne cochée. Elle permet de ne pas natter les adresses dans le tunnel.
« **Next** ».
A l'étape 6, un récapitulatif vous est présenté. Vérifiez que tout est correct et cliquez sur finish.
Dans « **Site-to-Site VPN** » « **Connection Profiles** », observez le profil créé, portant le nom de l'adresse IP de l'ASA distant. Vérifiez qu'il soit « **Enabled** ».
Profitez pour jeter un coup d'oeil ce que le « wizard » a inscrit dans « **Tunnel Group** » ainsi que « **Crypto Maps** ».
C'est ici que les différents paramètres et algorithmes ont été placés. Dans « **ACL Manager** », vous pouvez voir que des règles ont été ajoutées. Lesquelles ?

TESTS
Maintenant que vous avez configuré les **deux extrémités** du tunnel, testons si cela fonctionne.

Test 1 : de votre serveur Windows, testez un ping vers le serveur de l'autre binôme. Observez en même temps les logs de l'ASA (« **Monitoring** », « **Logging** », « **View** »). On voit que les paquets ne sont pas autorisés. Repérez le nom de l'ACL qui bloque les paquets icmp.
Dans le menu « **Tools** », sélectionnez « **Packet Tracer** ». Indiquez-lui que vous êtes sur l'interface « **inside** », type de packet « **icmp** », source « **10.0.X.1** », destination « **10.0.Y.1** » de type « **echo** », code « **0** » ID « **1** » puis cliquez sur « **start** ». Visualisez le blocage.

Test 2 : Testez une connexion RDP vers le serveur de l'autre binôme.

X - Messagerie Interne (Optionnel)

Nous allons mettre en place une messagerie simplifiée au niveau de la DMZ.
Elle ne permettra pas de recevoir des mails depuis l'extérieur car notre DNS ne le permet pas mais elle permettra l'échange de messages sur l'Intranet.

Mise en place du serveur de mail sur **ServeurX.maboiteX.tp**

- Gérer le rôle serveur de messagerie
  - Pour la méthode d'authentification, on choisira « comptes Windows locaux, exiger l'authentification par mot de passe sécurisé » (SPA) et « toujours créer un utilisateur associé »
  - Le domaine géré sera **maboiteX.tp**
- Créer deux boîtes mails (**alegrand**, mot de passe **monmail**) et **bdupond**, mot de passe **monmail**.

Configuration du client sur le poste posteX.

- Configurer Outlook express avec deux identités distinctes (alegrand et bdupond).
- Mettre en place la sécurisation.

Tester l'envoi d'un mail de **bdupond** à **adurand**.

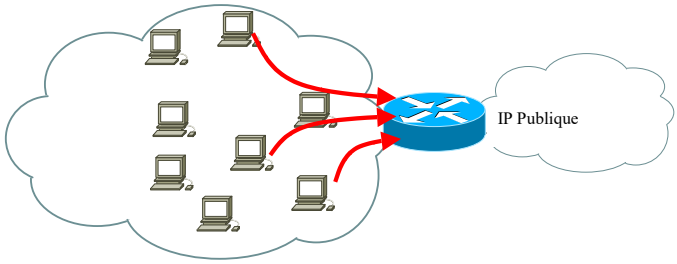
XI - Annexe :

1 - Les translations d'adresse.

L'utilisation de plages d'adresses privées est un élément de souplesse et de sécurité dans la conception du réseau d'entreprise. Mais il est nécessaire de convertir les adresses privées en adresses publiques ou réciproquement pour permettre aux machines des réseaux privés de communiquer avec l'extérieur. On parle alors de translation d'adresse.

Suivant le contexte, différents types de translation d'adresse devront être utilisés. Notons que même si les fonctions proposées sont sensiblement les mêmes chez les différents constructeurs, la terminologie utilisée peut varier. Nous utilisons ici la terminologie Netasq.

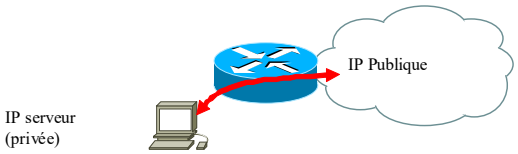
Translation d'adresse unidirectionnelle.
Ce type de translation est utilisé pour permettre à l'ensemble des machines d'un réseau d'avoir accès à INTERNET



L'ensemble des machines du réseau local utilise l'adresse IP publique comme adresse virtuelle.
Les connections se font sur l'initiative d'une machine interne. Aucune machine du LAN ne peut être contactée depuis l'extérieur.

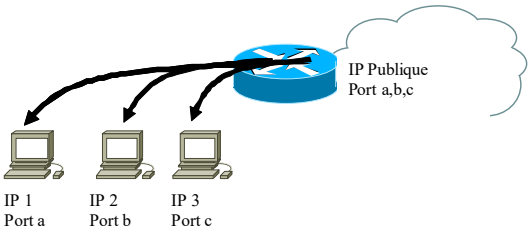
Original	Translaté
Adresse IP sur le Réseau interne	Adresse IP publique

Translation d'adresse bidirectionnelle :
La translation d'adresse bidirectionnelle permet de convertir une adresse en une autre lors du passage par le pare-feu quelle que soit la provenance de la connexion. La translation bidirectionnelle est généralement utilisée pour donner accès depuis l'extérieur à un serveur situé sur le réseau privé de l'entreprise.



Original	Translaté
Adresse IP publique	Adresse IP réelle du serveur

Redirection de port
La redirection de port permet de rediriger un couple (IP, port) vers un autre couple (IP, port). Ainsi différents types de requêtes arrivant vers une adresse publique (WEB, Mail etc.) pourront être redirigés vers des serveurs distincts et des ports librement choisis par l'administrateur.



2 - Commentaires sur PPTP :

Generic Routing Encapsulation GRE (Rfc 2784)
Le tunnel GRE permet d'encapsuler n'importe quel protocole réseau (de type couche 3) sur de l'IP. En pratique, il est souvent utilisé pour fabriquer des tunnels sur des réseaux IP.

<table>
<tr><td colspan="4"></td><td rowspan="4">Entête IP</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td></td><td>N°Proto</td><td colspan="2"></td></tr>
<tr><td colspan="4">@IP Source</td></tr>
<tr><td colspan="4">@IP Destination</td><td></td></tr>
<tr><td colspan="2">Drapeaux</td><td colspan="2">Protocole Encapsulé
0x800 :IP
0x880B : PPP</td><td rowspan="4">Entête GRE</td></tr>
<tr><td colspan="2">Longueur DATA</td><td colspan="2">N°Session</td></tr>
<tr><td colspan="4">Numéro de séquence</td></tr>
<tr><td colspan="4">Numéro Acquittement</td></tr>
<tr><td colspan="4">.
.
.</td><td>Protocole encapsulé</td></tr>
</table>

Il peut être utilisé pour mettre en relation des réseaux munis de protocoles non routables (Netbeui), des réseaux privés, des réseaux autres que Ipv4 (on peut relier par exemple deux réseaux IPV6 à travers un tunnel GRE).
Utilisé tel quel, GRE ne permet ni authentification des extrémités ni cryptage des données.

Dans l'exemple du TP, le protocole porteur est IP, mais d'autres protocoles peuvent se rencontrer, en particulier PPP dans le cas d'une liaison par modem. Il ne faut pas confondre cette liaison avec le transport PPP utilisé à l'intérieur du tunnel.

XII - Tunnel PPTP (Point to Point Tunnel Protocol) RFC 2637

PPTP est un protocole qui permet de construire des tunnels à l'aide de sessions PPP au-dessus d'un tunnel GRE.

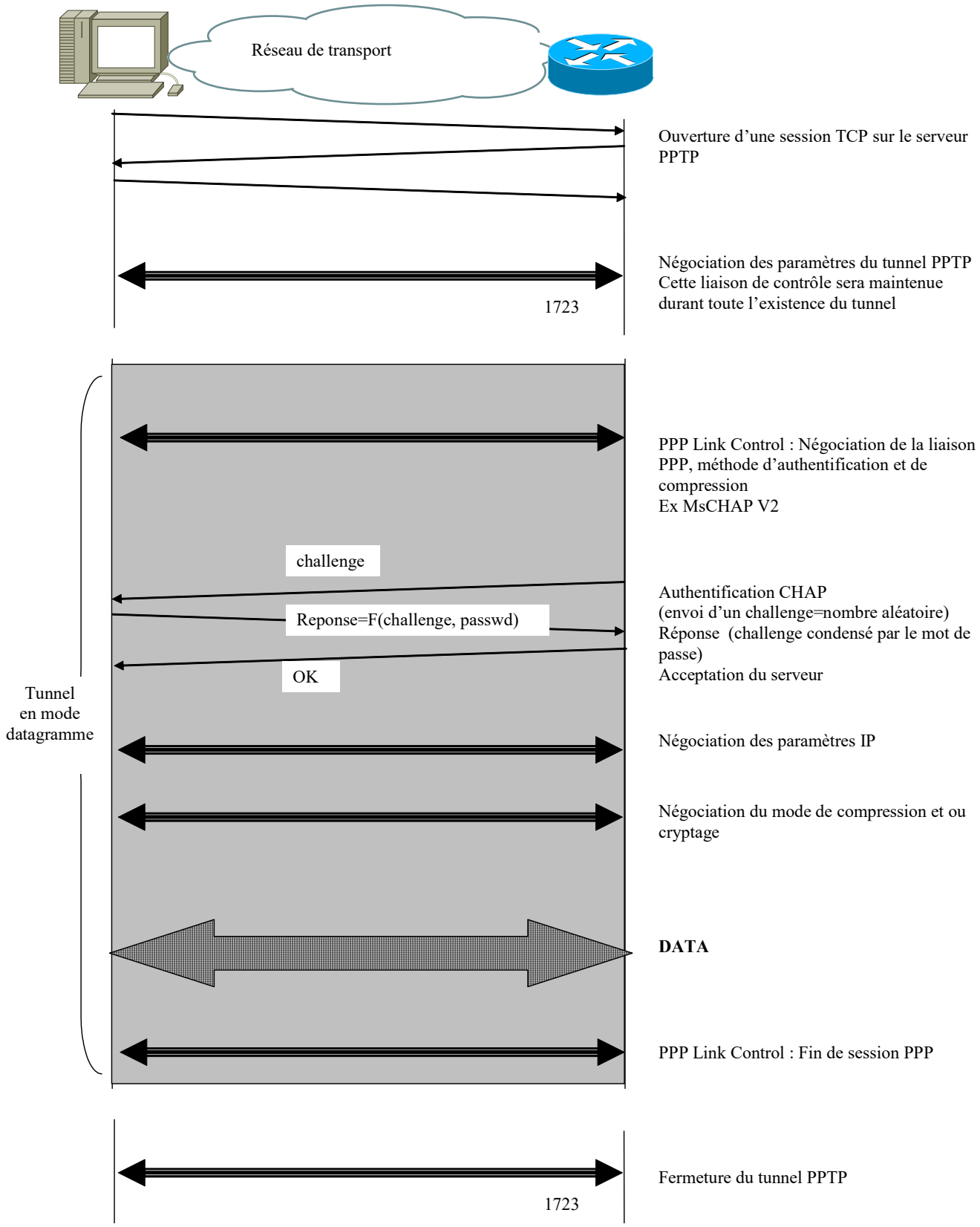
- Le tunnel GRE étendu pour le transport des datagrammes PPP
- Une session TCP permet de contrôler le tunnel

La connexion TCP n'est pas sécurisée, le tunnel GRE non plus.

Deux protocoles gèrent respectivement l'authentification et le cryptage : MS/CHAP et MPPE.

Le premier est une extension du protocole CHAP (Challenge/Handshake Authentication Protocol) déjà largement utilisé pour authentifier les connexions PPP entre les clients et leur ISP. Ce protocole permet de ne pas envoyer de noms d'utilisateurs et mots de passe en clair sur la liaison PPP.
Microsoft a décidé d'ajouter sa propre extension. On différenciera donc le protocole CHAP classique du protocole MS/CHAP.

En ce qui concerne le chiffrement de la connexion, le protocole PPP n'offrait aucune facilité de ce type. MPPE ou Microsoft Point-to-Point Encryption a donc vu le jour. Celui-ci utilise un algorithme de chiffrement RC4 en 40 ou 128 bits.



Network Adress Translation (NAT)
La NAT est a pour rôle de permettre à différentes machines dans un réseau privé d'accéder à l'internet en utilisant une adresse publique unique.

Annexe : Licence “Security Plus” sur le pare-feu ASA 5505

Version "Security Plus" :

- double le nombre maximum de sessions concurrentes simultanées
- double le nombre maximum de tunnels VPN IPSec simultanés
- permet de lever les restrictions sur le VLAN Home pour offrir des services autour d'une réelle zone démilitarisée
- Active le support de VLAN trunk 802.1q
- active le support d'architecture Dual ISP pour proposer la continuité des services fournis par l'ASA 5505 sur une connexion sortante Internet redondée.
- active le support d'un FailOver de type Actif/Passif afin de fournir un service de haute disponibilité entre deux unités ASA 5505.
- Licence pouvant être utilisée pour tous les niveaux de licence utilisateur.