Configuration de GNS3

>>> Mise en place d’un Firewall Cisco ASA

Description :

Cet article donne une astuce concernant la configuration de GNS3 pour la mise en place d’un pare-feu Cisco ASA.

Nota : Les constructions présentées ci-dessous ont été réalisées sous environnement Windows 7 avec GNS3 0.8.2 et l’image d’un Firewall ASA 8.2.4.

Configuration de GNS3

>>> Mise en place d'un Firewall Cisco ASA

Sommaire :

I) Ce dont vous avez besoin

Pour mettre en place un réseau virtuel comportant un pare-feu tel que le Cisco ASA, il vous faut les éléments suivants :

- Un **ordinateur** fonctionnant de préférence sous un **système 64bits** (en effet la virtualisation est plus facile avec ce type d'architecture),
- Le **fichier de boot** de l'ASA appelé "initrd.gz",
- Une **image d'un IOS** d'un Firewall ASA appelé "wmlinuz",
- Un **fichier ASDM** pour la prise en main via l'interface WEB,
- Le logiciel TFTPd32 pour des transferts de fichiers,
- la **configuration** suivante pour **Qemu** :

```
-m 1024 -icount auto -hdachs 980,16,32
```

Cette commande permet de créer et configurer une machine virtuelle dans Qemu. On y retrouve, notamment, la configuration de la mémoire. Cette machine supportera le fichier initrd.gz ainsi que, et surtout, l'image de notre ASA.

- La commande noyau suivante :

```
-append ide_generic.probe_mask=0x01 ide_core.chs=0.0:980,16,32 auto nousb console=ttyS0,9600
bigphysarea=65536
```

Elle permet de donner des instructions lors du démarrage de notre pare-feu. Ici, elle donne les éléments nécessaires pour ouvrir une connexion SSH en redirigeant le "ttyS0" vers une fenêtre Putty. Le paramètre précédent permet de configurer le noyau de façon à pouvoir l'exécuter dans un système d'exploitation.

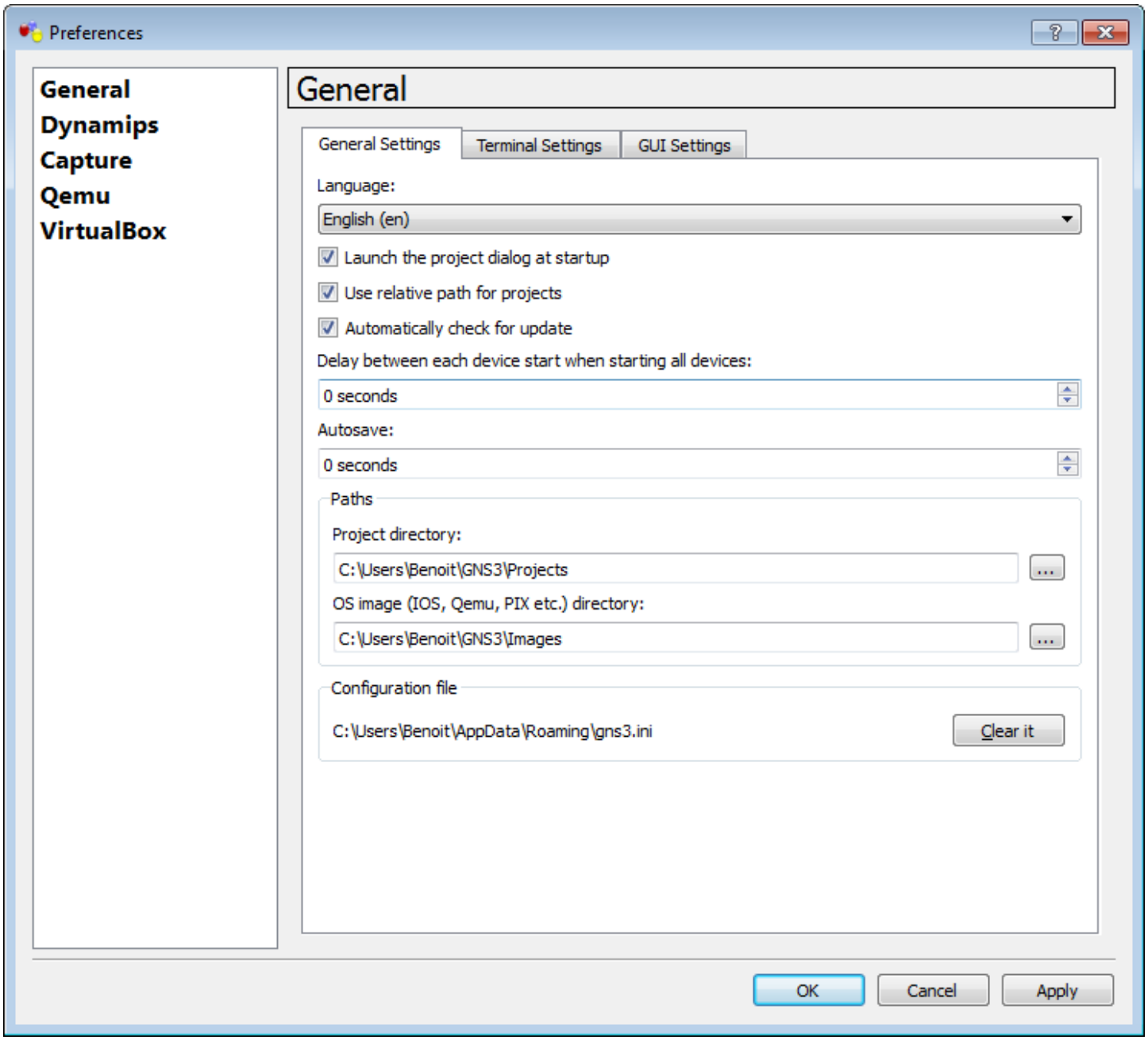
- et, bien sûr, le **logiciel GNS3**, disponible directement sur le site éponyme : Ici, sélectionner la version **"all-in-one"**.

Vous avez toutes les ASA formations qu'il faut ... alors c'est partit, allons en salle de Ciscopération !!!

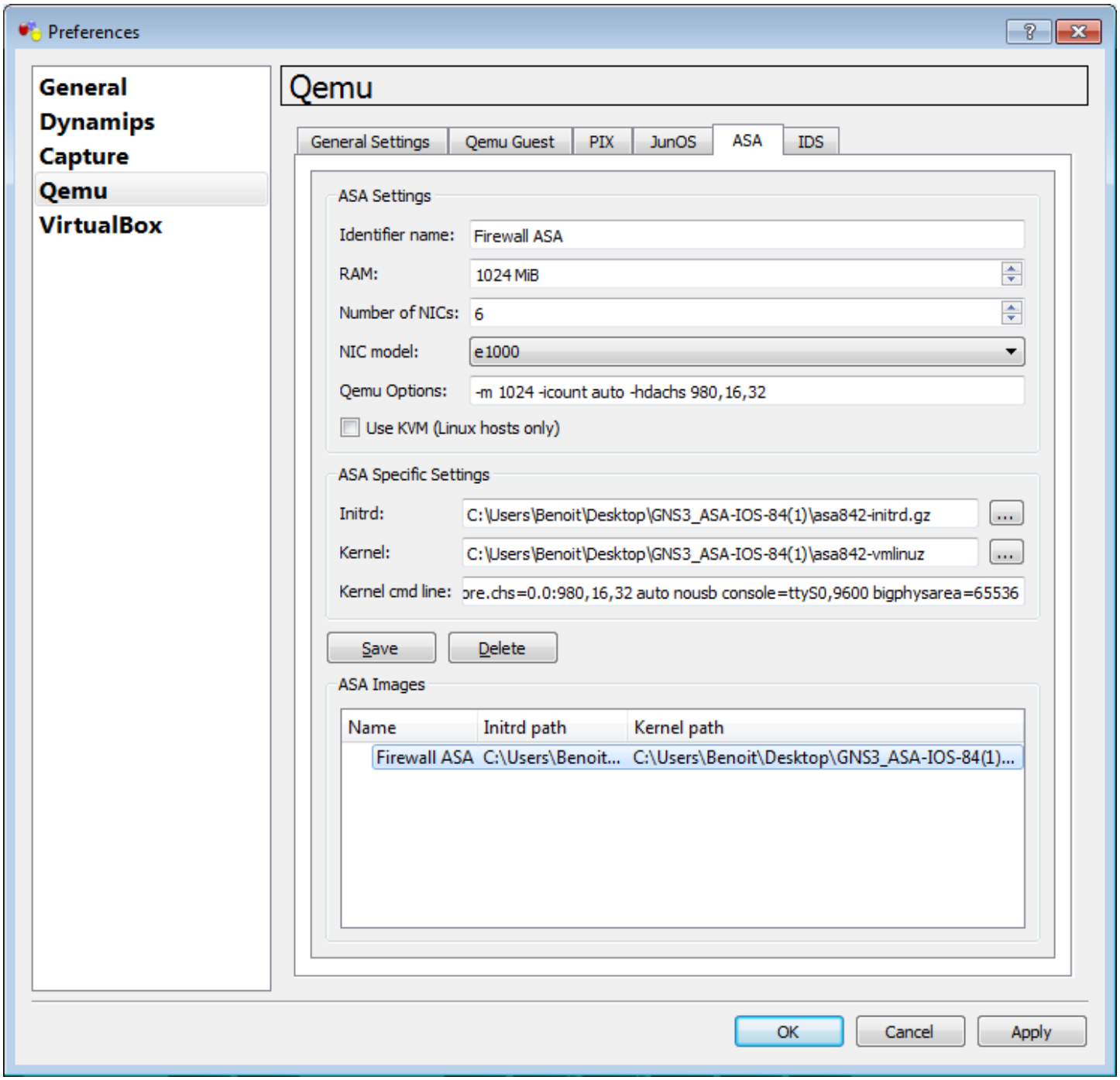
II) La configuration de GNS3

Vous allez voir dans cette partie que la configuration de l'ASA dans GNS3 peut se réduire à quelques clics et ne demande, tout au plus, que 5 petites minutes.

Il faut tout simplement aller dans **[Edit]**, sélectionner **[préférences ...]**. Voici ce que vous devez obtenir :



Ensuite aller dans l'onglet **[Qemu]**(à gauche), puis dans l'onglet **[ASA]**(à droite)



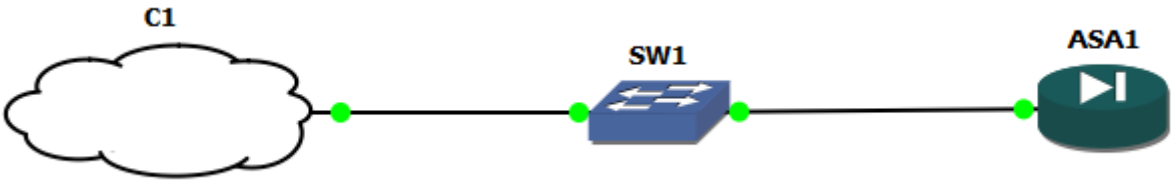
Sur l'image ci-dessus vous pouvez voir la configuration initiale de GNS3. Il ne vous reste plus qu'à faire de même en copiant les informations données dans le Chapitre I aux bons endroits, c'est à dire :

- configurer la mémoire à **1024Mo**,
- Copier la commande Qemu dans le champ **Qemu Options**
- Champ **Initrd :** Aller chercher dans le fichier initrd dans le répertoire où vous l'avez téléchargé,
- Champ **Initrd :** Faire de même en prenant le fichier image IOS (wmlinuz) "désarchivé",
- Copier la commande kernel dans le champ **Kernel cmd line**
- Sauvegarder votre configuration en cliquant sur **Save**
- Enfin, appliquée la en cliquant sur **Apply** puis sur **OK**

Et voilà, il ne vous reste plus qu'à redémarrer GNS3 pour profiter de la configuration que vous venez de réaliser.

III) Les premiers pas sur Cisco ASA

Dans cette partie, nous allons mettre en place une première mise en œuvre très simple de notre nouveau pare-feu. Pour cela, voici la topologie qui sera utilisée :

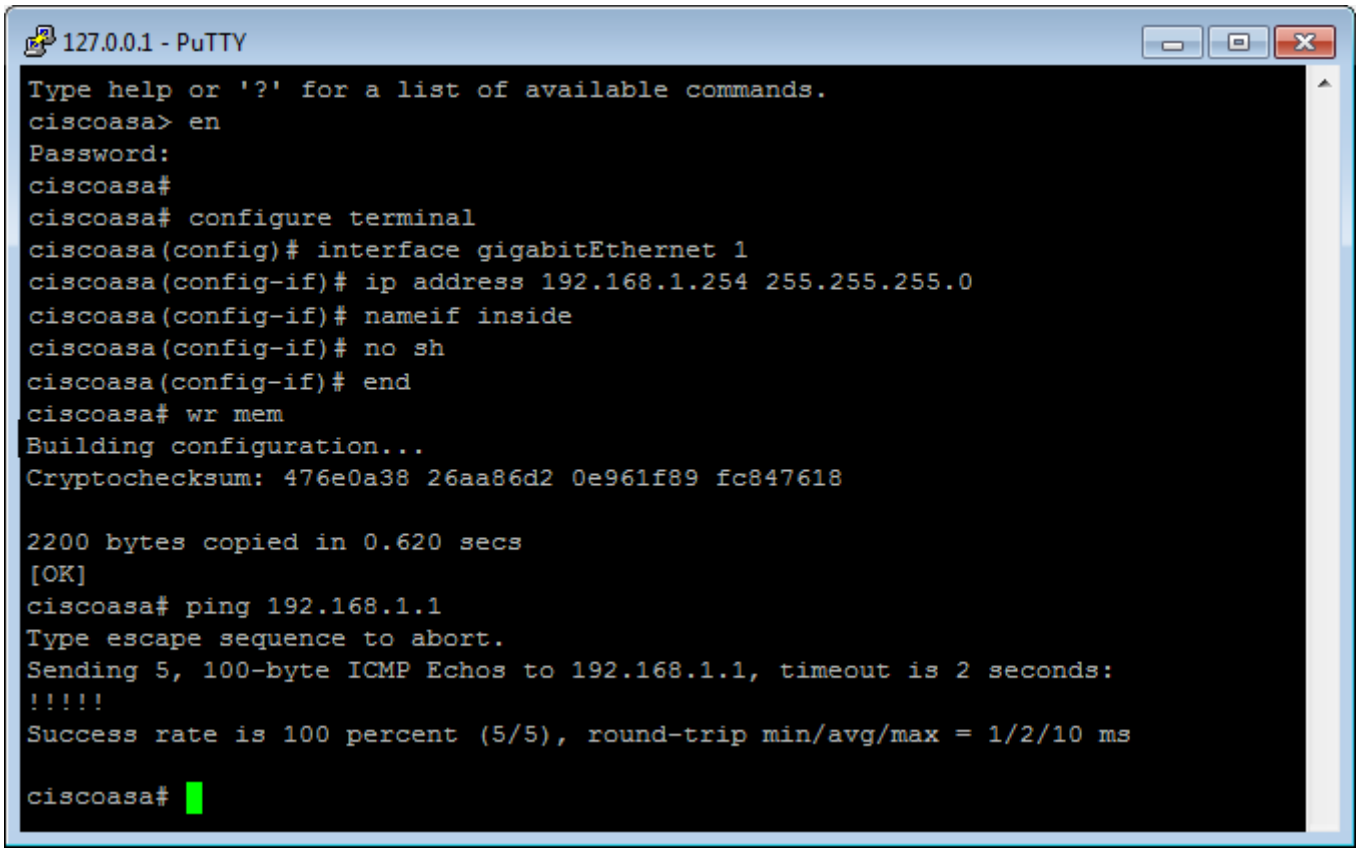


Lorsque vous redémarrez GNS3, ce dernier vous proposer de nommer un nouveau projet.

1) Création de l'ASA

Dans la liste de produit qui se trouve dans la colonne de gauche sélectionnez l'ASA et faite le glisser sur la feuille de projet centrale. Ensuite faite un clique **droit** et cliquez sur **Start**. Une fenêtre Qemu s'ouvre. Il ne faut pas la fermer tout de suite ou vous ne pourrez pas utiliser votre ASA. Si par mégarde vous la fermer, il suffit de relancer l'ASA pour la rouvrir. Pour vérifier la bonne installation et le bon démarrage du Firewall ASA, refaite un clique **droit** et sélectionnez **Console**. Une fenêtre "Putty" va s'ouvrir et vous affichera tout un tas d'informations montrant le démarrage de l'Appliance virtuelle.

Il faut ensuite configurer une interface de votre ASA en saisissant les commandes ci-dessous :



Surtout n'oubliez pas le **write memory** (abrégé en wr mem) ou vous serez obligé de refaire la configuration de l'interface.

Ensuite, il faut arrêter votre ASA pour pouvoir le "câbler" comme nous le verrons dans la suite de l'exercice. Pour cela, faîtes un clic **droit** et sélectionner **Stop**.

2) Création et configuration du switch ethernet

Pour pouvoir connecter l'ASA au nuage, il faut ajouter un switch ethernet entre ces deux éléments. Pour se faire, sélectionner "ethernet switch" dans la colonne de gauche et faîtes le glisser dans la feuille de projet centrale.

Vous pouvez le connecter en utilisant les liens que vous trouverez dans la barre en bas.

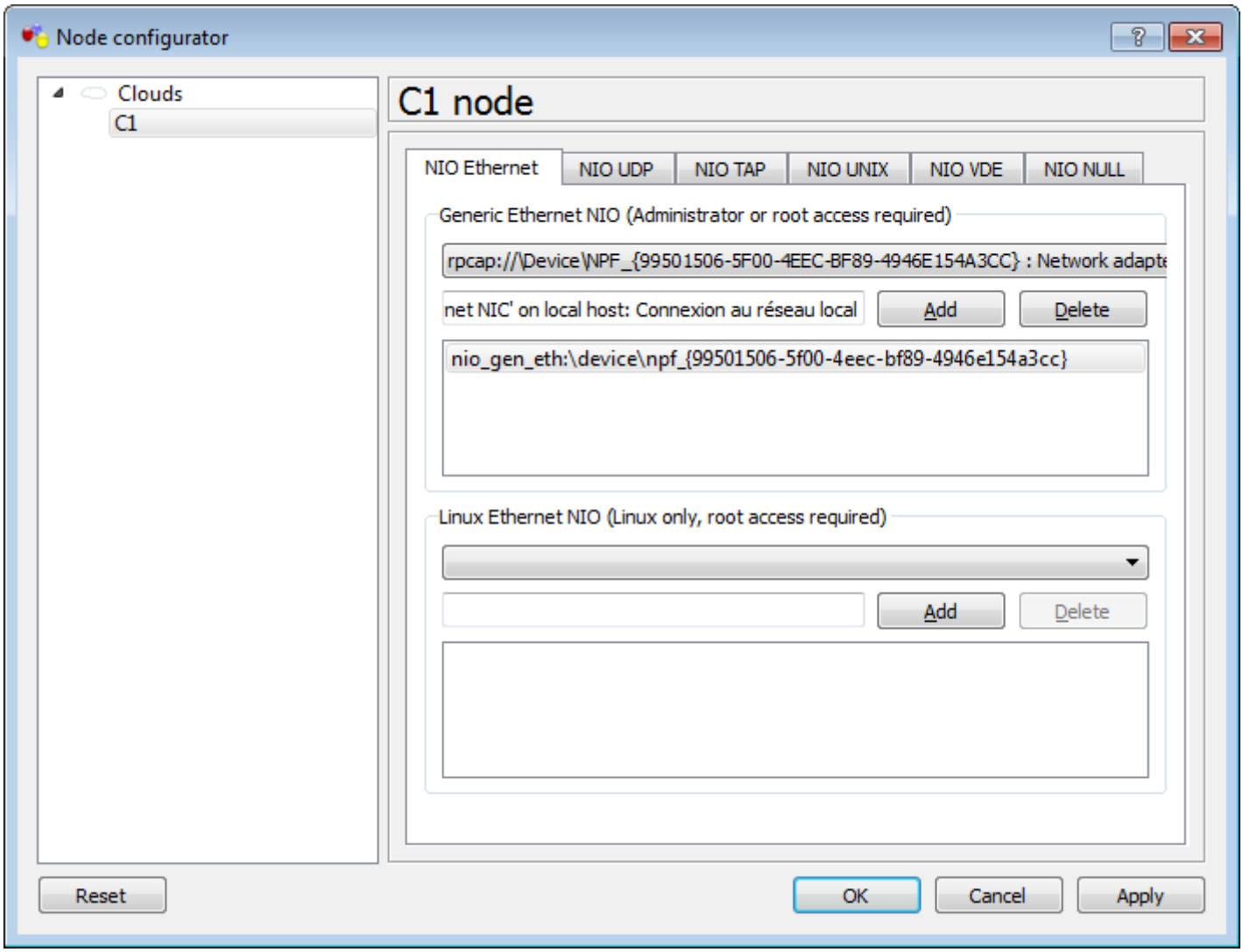
En dehors de cette dernière action, il n'y pas d'autre configuration à apporter à ce composant. En effet, il agira ici comme un simple switch d'interconnexion, il n'y a même pas besoin de configurer de VLAN.

3) Création et configuration du nuage

Ah ! Le fameux nuage ! Celui qui nous fais prédire le mauvais temps et qui nous apporte la pluie voir même l'orage.
Alors, bien sûr, ici il ne s'agit pas de parler des cumulonimbus mais plutôt du nuage qui permet de relier votre réseau virtuel à votre machine hôte voir même à votre réseau "physique". Mais sans plus tarder, passons à la pratique.

Comme les deux autres éléments présentés juste avant, pour ajouter un nuage, il suffit de le sélectionner dans la colonne de gauche et de le faire glisser dans la feuille de projet centrale.

Pour la configuration rien de plus simple : clic droit sur le nuage et sélectionner **Configuration**.
Ensuite, dans le cas où vous avez créé plusieurs nuages, il faut sélectionner celui que vous voulez configurer.
Puis aller dans l'onglet **[NIO ethernet]**
Utilisateur de systèmes d'exploitation Windows, seule la première moitié vous concerne mais le fonctionnement est le même pour les systèmes sous Linux. Vous pouvez voir ci-dessous ce que ça donne une fois configuré :



En préparation du prochain chapitre, nous allons connecter l'interface de réseau local au nuage. Vous pouvez le faire en sélectionnant l'interface correspondante dans la liste, puis ajouter l'interface en cliquant sur **Add**. Pour terminer, cliquez sur **Ok**.

Il ne vous reste plus qu'à connecter votre nuage au switch.

4) Mise en fonction de l'ASA et premier test

Pour redémarrer l'ASA, faîtes comme dans la partie concernant la création du pare-feu : clique **droit** sur l'équipement, sélectionner **Start**. La fenêtre Qemu qui s'ouvre doit rester ouverte. Ensuite, pour afficher la console refaites à nouveau un clique **droit** sur l'ASA et sélectionnez … **Console**.

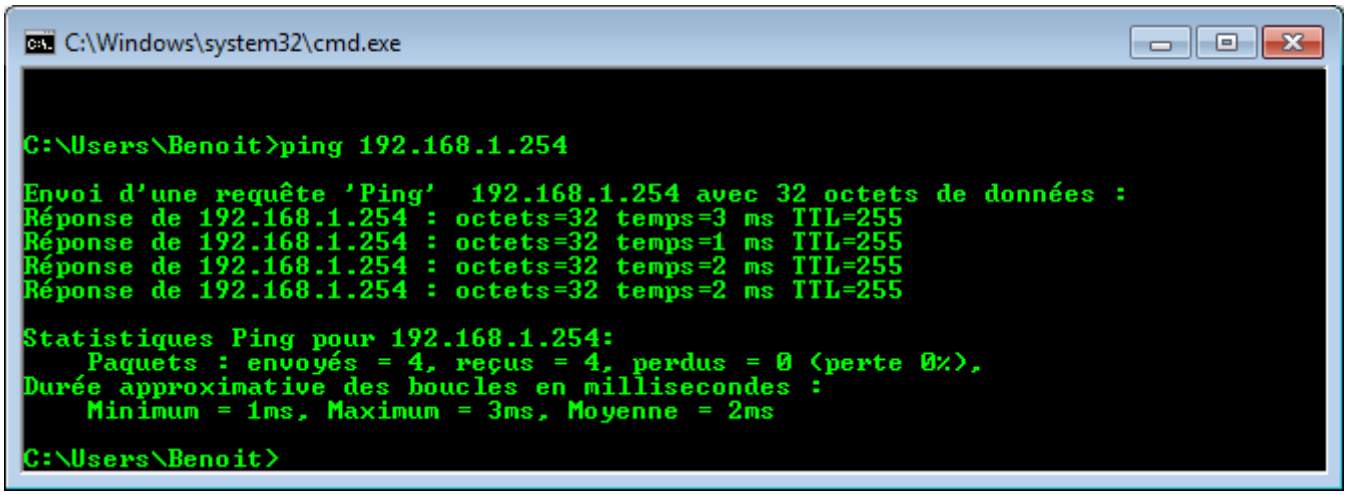
Vous avez à nouvel accès à la configuration de votre ASA.

Avant d'aborder la phase de test, une dernière configuration s'impose : l'adresse réseau de votre carte réseau local.
Pour cela vous pouvez consulter l'article ici qui, si vous ne le savais pas, vous montre comment faire, à la différence prête que vous devrez utiliser la configuration suivante (ou du moins une similaire) :

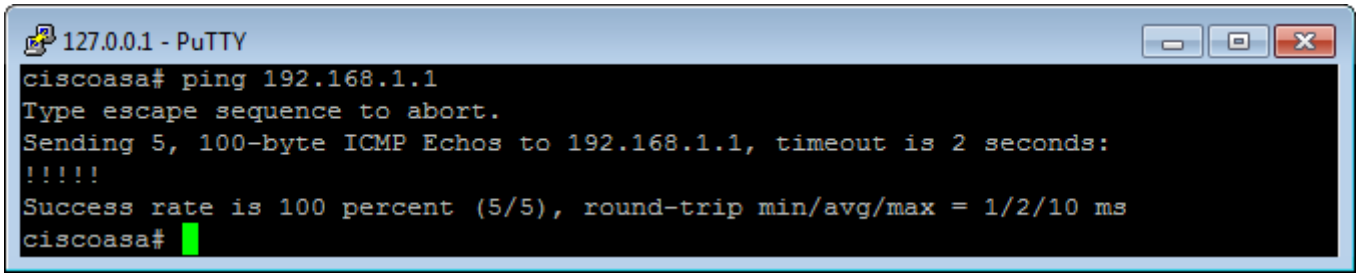
- Adresse IP : 192.168.1.10
- Masque : 255.255.255.0
- passerelle par défaut : 192.168.1.254

Dans cet exercice, nous n'aurons pas besoin de DNS.

Enfin, faite un **"ping"** depuis votre machine hôte vers votre ASA. Si tout fonctionne comme il faut, voici ce que vous devez obtenir :



Faîte de même depuis l'ASA vers votre machine hôte. vous devriez obtenir quelque chose comme ceci :



IV) Se connecter à distance sur l'ASA

1) Via l'ASDM

Si vous ne souhaitez pas configurer votre ASA en ligne de commande en dehors de la configuration minimale que je vous ai présentée auparavant, je vous comprends. Nous allons donc procéder à l'installation de l'ASDM.

Avant toute chose, il faut charger et configurer la version de l'ASDM. Pour cela, démarrer votre serveur TFTP sur votre ordinateur. Configurez le répertoire de travaille de votre serveur pour faire en sorte que l'ASDM soit disponible.
Retournez ensuite dans la console de l'ASA et saisissez la commande suivante :

```
# copy tftp flash:/nom_de_votre_image_ASDM
```

Ensuite, il faut préciser que vous utiliserez cette version en saisissant la commande suivante :

```
# asdm image nom_de_votre_image_ASDM
```

Puis configurer le serveur HTTP qui exécutera l'ASDM via les commandes suivantes :

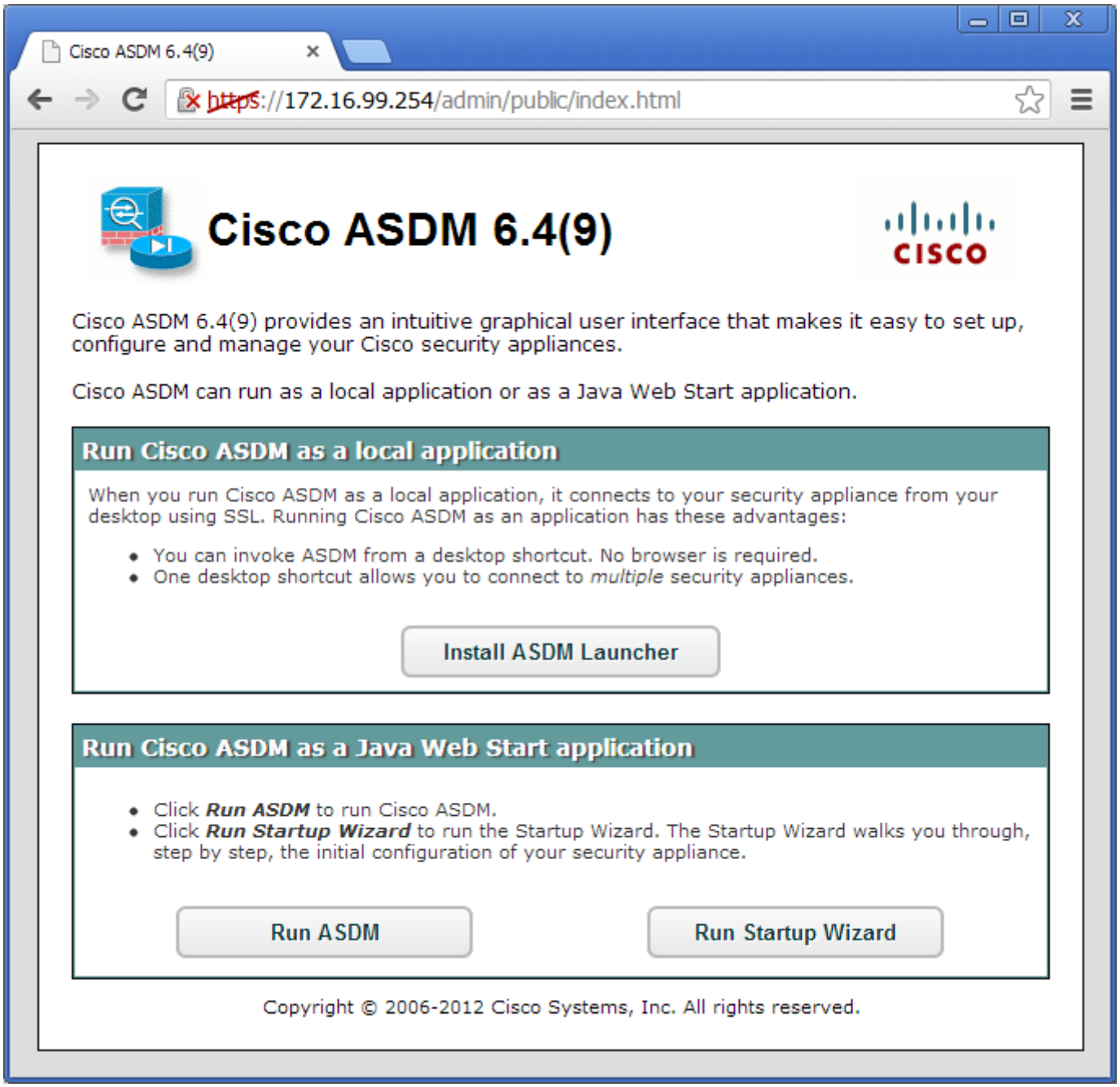
```
# http server enable
# http 172.16.99.0 255.255.255.0 WAN
```

La dernière commande permet d'autoriser l'accès à l'ASDM depuis le WAN.

Pour pouvoir vous connecter à l'ASDM, vous devez configurer un compte, comme suit :

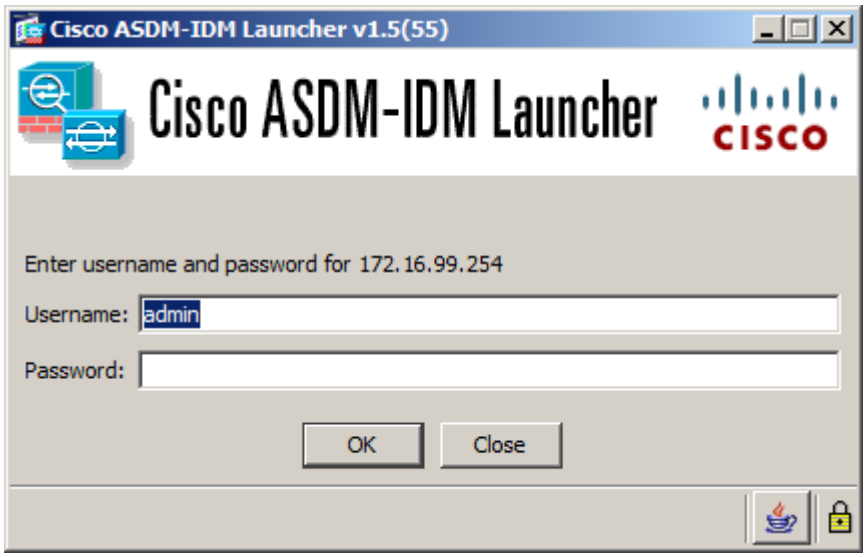
```
# user nom-de-l'utilisateur password mot_de_passe
```

Il ne vous reste plus qu'à tester cet accès en ouvrant un navigateur sur votre ordinateur et en saisissant l'adresse de votre ASA, dans notre exemple il s'agit de https://172.16.99.254. Vous devriez obtenir la page suivante :

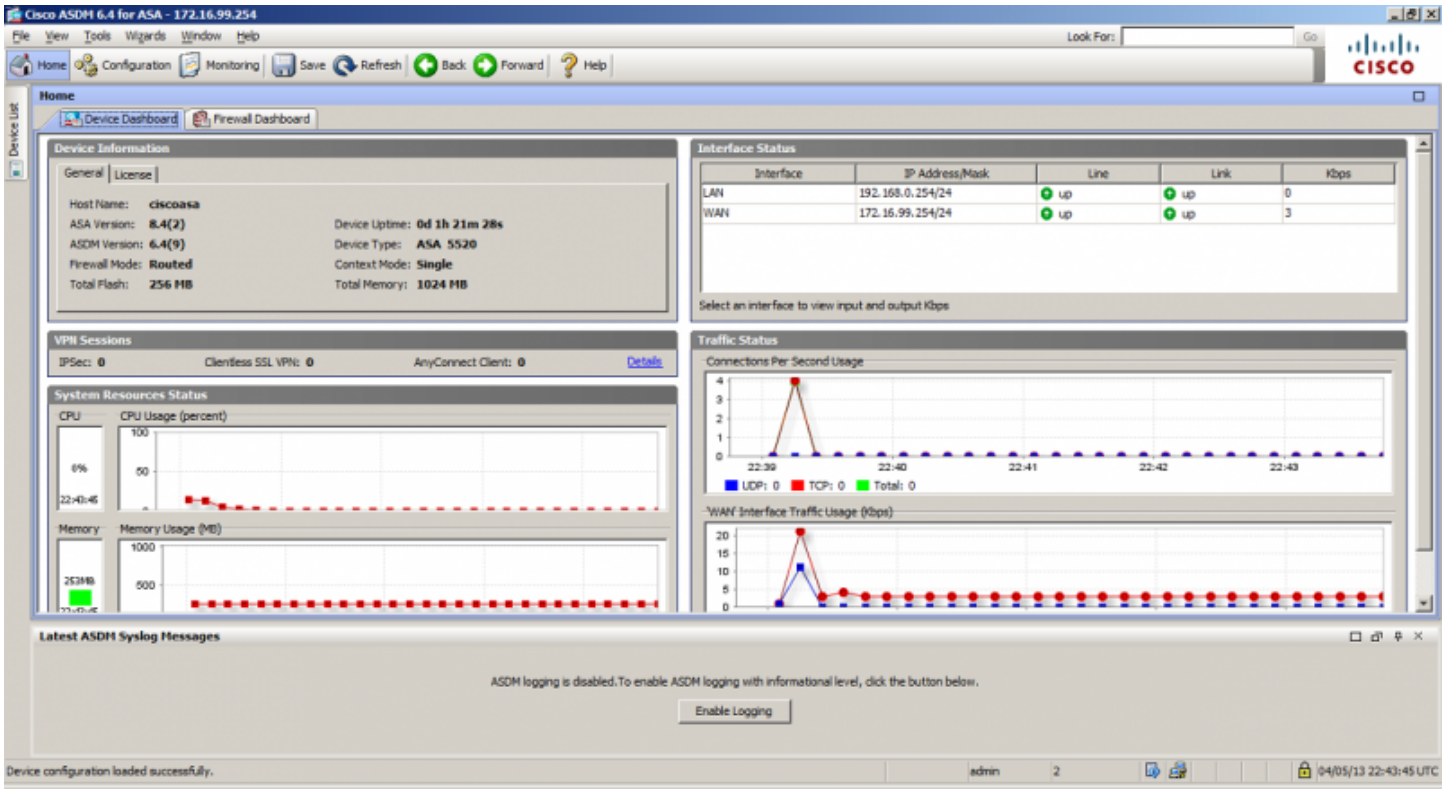


Cliquez sur **Run ASDM**

Votre navigateur va procéder au téléchargement d'un plug-in java. Une fois téléchargé, il vous faut cliquer dessus pour le "lancer". Attention : ceci nécessite d'avoir une version de JAVA à jour. Une fois lancé, vous devez obtenir ceci :



Saisir **les identifiants** créés précédemment. Et voilà votre client ASDM est démarré :



N’oubliez pas de faire un "write mem" pour ne pas perdre votre configuration !

2) Via une session Putty

Si vous souhaitez administrer votre ASA via l’interface CLI (pour récupérer le fichier de configuration, charger un fichier ASDM, simplement faire de débogage) voici comment configurer cette interface :

Il faut commencer par générer une paire de clé dont l’une sera échangée avec le client SSH :

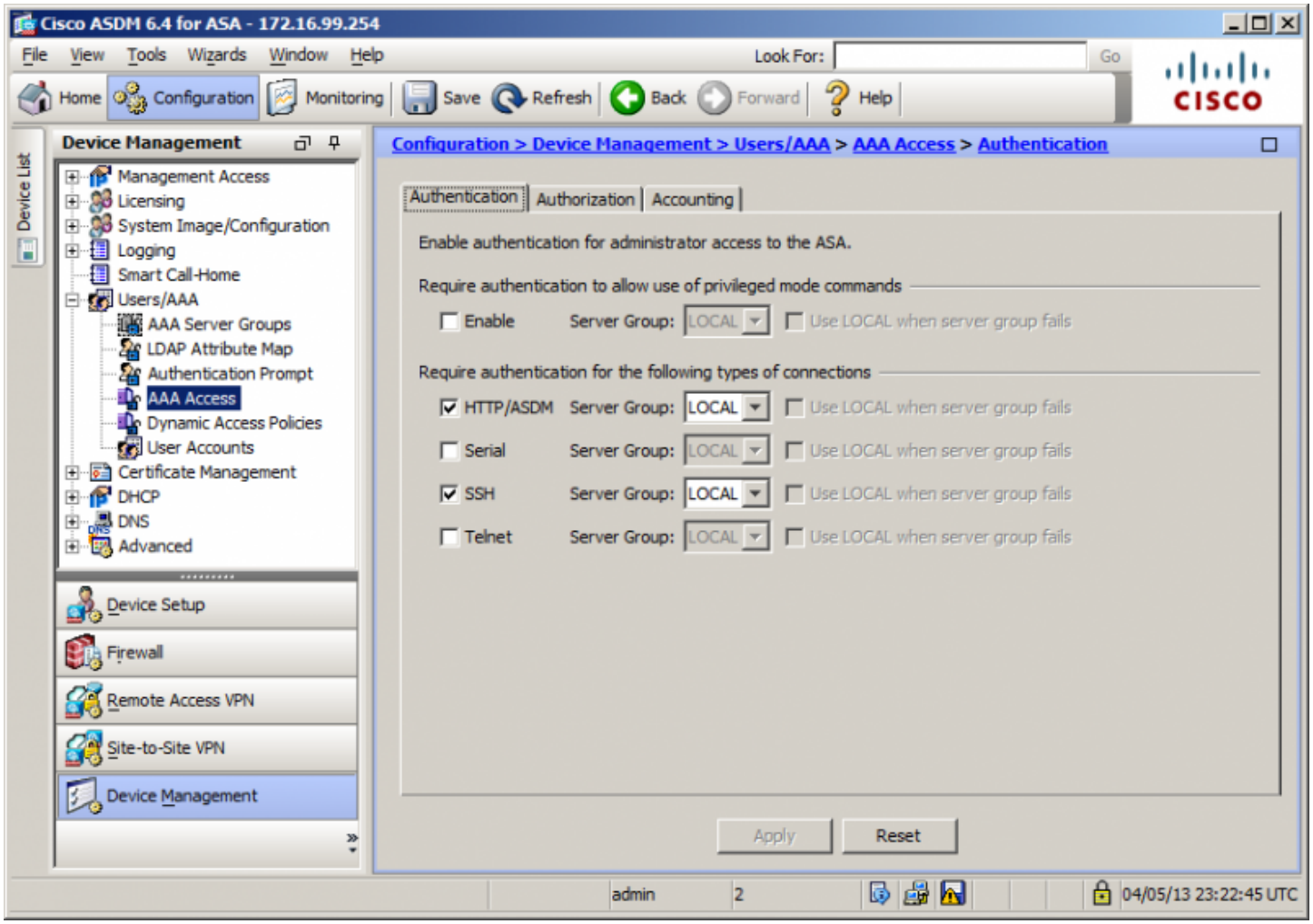
```
# crypto key generate rsa modulus 1024
```

Si l’interface vous demande si vous souhaitez remplacer les clés existantes, répondez par "yes".

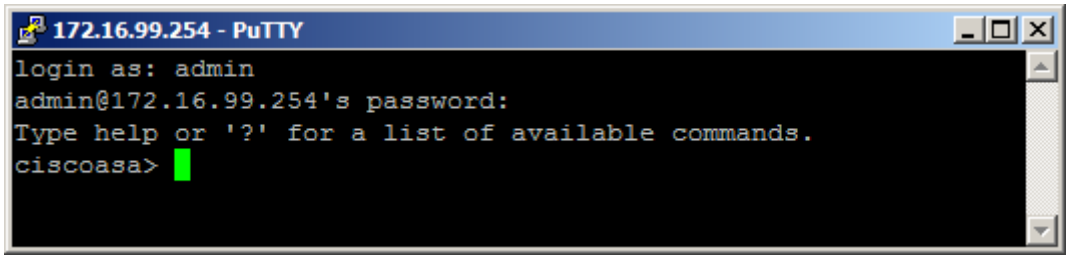
Puis, il faut autoriser l’accès à cette interface (comme pour l’ASDM) :

```
ssh 172.16.99.0 255.255.255.0 WAN
```

Enfin, il faut définir le groupe d'utilisateur autorisé à accéder à l'ASA via l'interface CLI.
Pour cela connecter via votre accès ASDM fraichement installé et aller dans l'onglet **configuration** puis **User/AAA**, et **AAA Access**.
Enfin dans le premier onglet de cette page, vous pouvez configurer le **groupe LOCAL** vous permettant d'utiliser le compte admin créer auparavant.
Pour vous aider, voici une image de ce que vous devriez avoir :



Pour tester cette accès, démarrer un client SSH tel que Putty et saisir l'adresse de votre ASA. Puis lorsque l'interface vous le demande, saisissez les identifiants que vous utilisé pour l'accès à votre interface ASDM.
Vous devriez obtenir ceci :



Et voilà ! Vous avez configuré une topologie de base pour faire vos premiers pas sur l'ASA.

Idum