Cisco ASA et NAT

- Réseau - Sécurité -

Date de mise en ligne : vendredi 26 septembre 2014

Description :

Cet article vise à donner un aide-mémoire pour la configuration d'une règle de NAT avec une redirection de port permettant d'accéder à une ressource interne depuis un réseau distant.

Sommaire :

I) Présentation

Haut de page

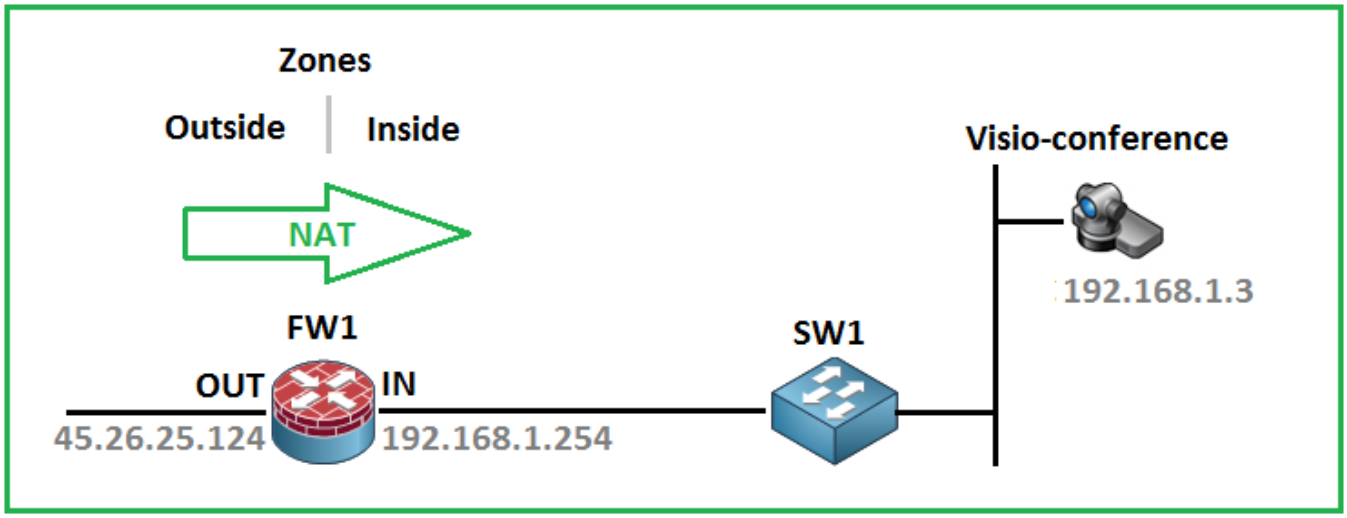
Il est de notoriétés parmi les experts sécurités, que le pare-feu ASA de Cisco n'a jamais été d'une grande simplicité pour la configuration des règles de NAT entre autres choses.

Pourtant, depuis la version 8.3, Cisco a considérablement amélioré son approche de cette fonctionnalité encore grandement utile aujourd'hui. Grâce à l'exemple qui va nous occuper dans cet article et une fois que vous aurez vu les paramètres auxquels il faut faire attention, vous pourrez le constater par vous-même.

La situation est la suivante :
Un administrateur achète les services d'un prestataire pour s'occuper de la maintenance de son équipement de visioconférence. Devant mettre un accès à distance à disposition de ce dernier et, n'ayant pas eu de budget cette année, il ne peut pas acheter de licences qui lui permettraient, par exemple, de mettre en place la solution de connexion à distance Cisco AnyConnect (Client VPN léger).

Il opte alors pour la mise en place d'une règle de NAT avec une redirection de ports.
On peut trouver plusieurs failles à cette solution, bien sûr, mais pour notre administrateur c'est une solution gratuite donc c'est la meilleure !

Nous allons donc voir comment on peut réaliser cette demande et tout d'abord, avec ce schéma de principe :



Légende
FW1 = Firewall Cisco ASA
SW1 = Switch

Le principe de la solution tient en deux choses :
D'abord le pare-feu va examiner le flux entrant et, en particulier, la combinaison adresse IP publique / port de connexion pour déterminer la règle de NAT à exécuter pour remplacer la règle de destination (notre interface OUT) par l'adresse réelle du serveur et changer le port dans le cas d'une redirection de port.
Puis, il va vérifier que le port sur lequel on souhaite atteindre le serveur fait bien partit des flux autorisés dans une règle de pare-feu.
Enfin, suivant le résultat de ces deux tests, il va soit transmettre la requête au serveur soit bloquer le paquet.

1) Introduction

La mise en place d'une règle de NAT avec redirection de port nécessite finalement peu de configuration, néanmoins avant de mettre "les mains dans le cambouis", il faut connaître quelques informations :

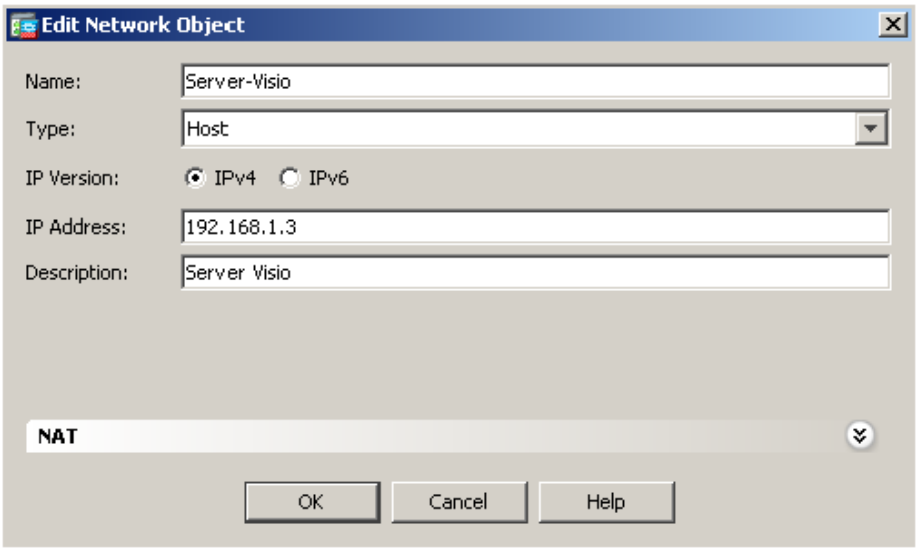
*- L'interface par laquelle on va entrer, ici l'interface OUT (souvent nommée outside dans le pare-feu)
*- Adresse publique de cette interface, ici 45.26..25.124
*- Adresse privée de notre serveur de visio-conférence, ici 192.168.1.3
*- L'interface sur laquelle le réseau du serveur est configurée, ici IN (nommée inside dans le pare-feu)
*- le port réel de connexion sur le serveur, ici le port 443
*- et, enfin, le port qu'on va utiliser lorsqu'on tentera d'accéder au serveur, ici le port 9443

Vous avez ces informations ? Parfait ! Connectez-vous alors sur votre équipement préféré avec votre ASDM et c'est parti !

2) Configurer un "Network objet"

Tout d'abord, nous allons configurer un objet représentant le serveur de visioconférence comme suit :

Allez dans l'onglet **Configuration** puis dans **NAT Rules**
Dans la colonne de droite dans l'ASDM, vous aurez l'onglet "addresses", **cliquez** sur **Add** et suivez l'exemple suivant pour configurer votre objet :



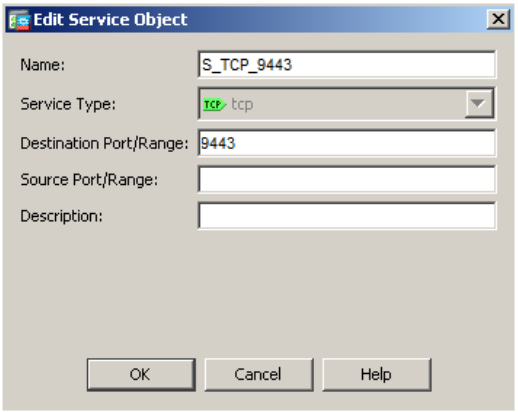
Cliquez sur **OK**

Nota : A ma connaissance, l'objet représentant l'interface "outside" est créée automatiquement par le pare-feu lors de la configuration réseau de ce dernier.
Bien sûr, si ce n'est pas le cas, vous devez recommencer l'étape ci-dessus pour créer cet objet.

3) Configurer un "Service objet"

Ensuite, il faut créer les objets identifiants les ports qui seront utilisés dans la translation :

Toujours dans l'onglet **NAT Rules** et dans la colonne de droite dans l'ASDM, **allez** maintenant dans l'onglet **Services** et configurez vos services en cliquant sur la petite flèche à côté du bouton **Add** et en sélectionnant **Service Object**.
Suivez cet exemple pour configurer vos services :



Cliquez sur **OK**

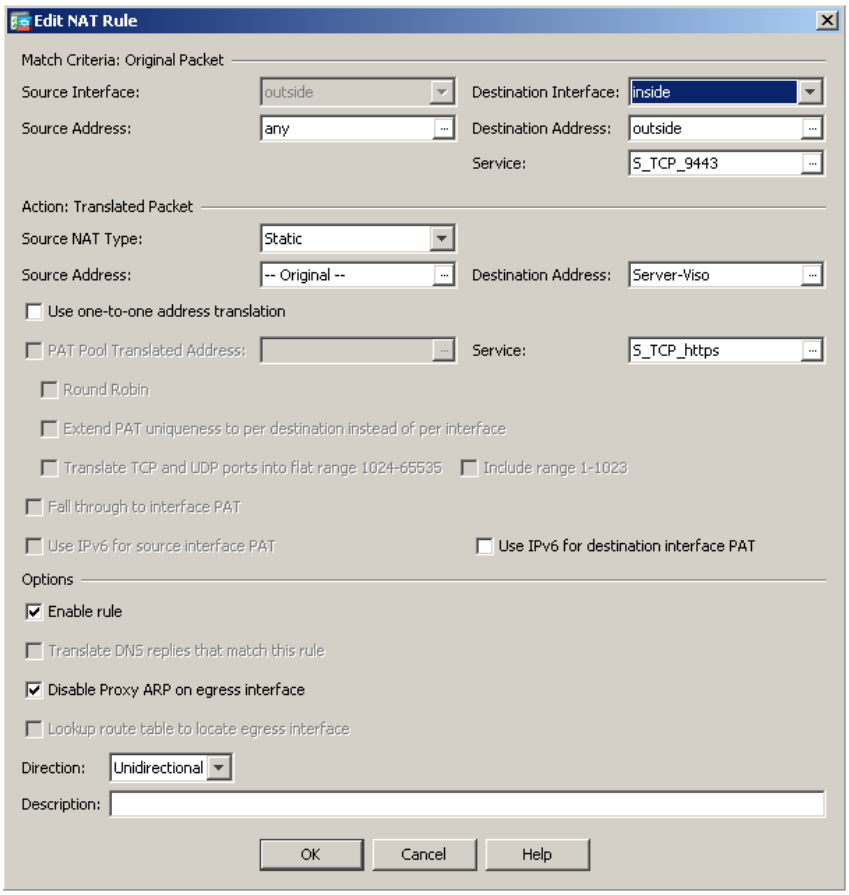
Nota : dans notre situation initiale, il faudra configurer les deux ports utilisés dans la règle de NAT, à savoir 9443 et 443 (https)

4) Configuration d'une Règle de NAT entrante avec redirection de port

Maintenant que nous avons tous les éléments pour travailler, les choses sérieuses vont commencer.

L'ajout d'une règle de NAT se fait en **cliquant** sur la flèche à côté du bouton **Add** en haut à gauche de la partie centrale affichée par votre ASDM. **Sélectionnez** ensuite **Insert ...**

Suivez l'exemple suivant pour configurer votre règle de NAT :

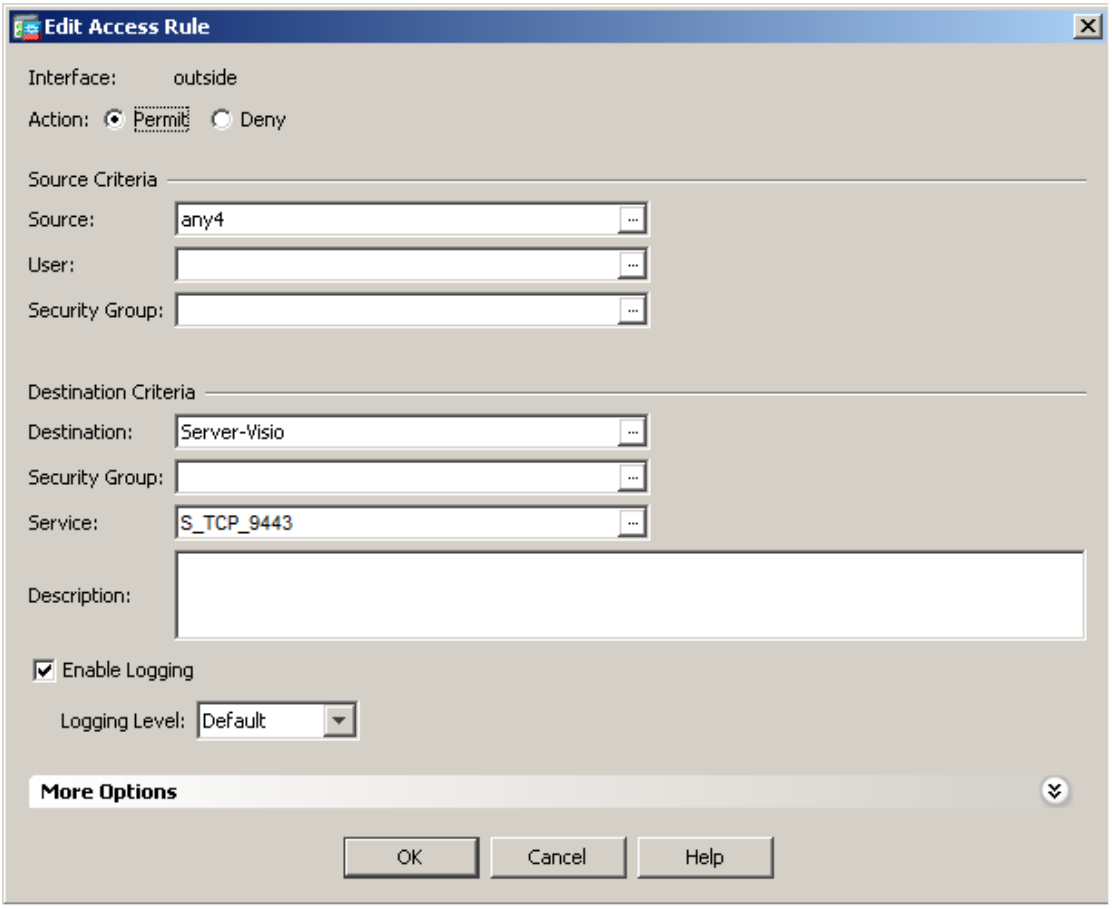


Cliquez sur **OK**

La règle de NAT est maintenant créée. Il ne reste plus qu'à autoriser le flux entrant vers le serveur de visio-conférence

5) Configuration d'une règle d'accès

C'est cette règle qui va permettre l'accès à l'administration du serveur.
Pour cela, **regardez** dans la colonne à gauche, puis **cliquez** sur l'onglet **Access Rules**, **cliquez** sur **Add** et suivez l'exemple suivant pour configurer votre règle d'accès :



Cliquez sur **OK**

6) Conclusion

Dans cet article, vous avez pu voir comment on configure une règle d'accès entrante avec une redirection de port sur le pare-feu Cisco ASA.

Pour aller plus loin avec la mise en place d'un équipement visio et tous les protocoles qui s'y rattache (1720, plages de ports aléatoires pour le RTSP, ...), il suffirait de copier cette configuration en créant un groupe de ports avec les services représentant les ports à ouvrir dans la règle d'accès puis en faisant une règle de NAT pour chaque protocoles.