Tunnel VPN dynamique du site à site IKEv2 entre l'exemple de configuration deux ASA

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Informations générales](#)
[Diagramme du réseau](#)
[Configurez](#)
[Solution 1 - Utilisation du DefaultL2LGroup](#)
[Configuration statique ASA](#)
[ASA dynamique](#)
[Solution 2 - Créez un groupe de tunnels défini par l'utilisateur](#)
[Configuration statique ASA](#)
[Configuration dynamique ASA](#)
[Vérifiez](#)
[Sur l'ASA statique](#)
[Sur l'ASA dynamique](#)
[Dépannez](#)

Introduction

Ce document décrit comment configurer un tunnel VPN de la version 2 d'échange de clés Internet (IKE) de site à site (IKEv2) entre deux appliances de sécurité adaptable (ASA) où une ASA a une adresse IP dynamique et l'autre a une adresse IP statique.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 5505 ASA
- Version 9.1(5) ASA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Il y a deux manières que cette configuration peut être installée :

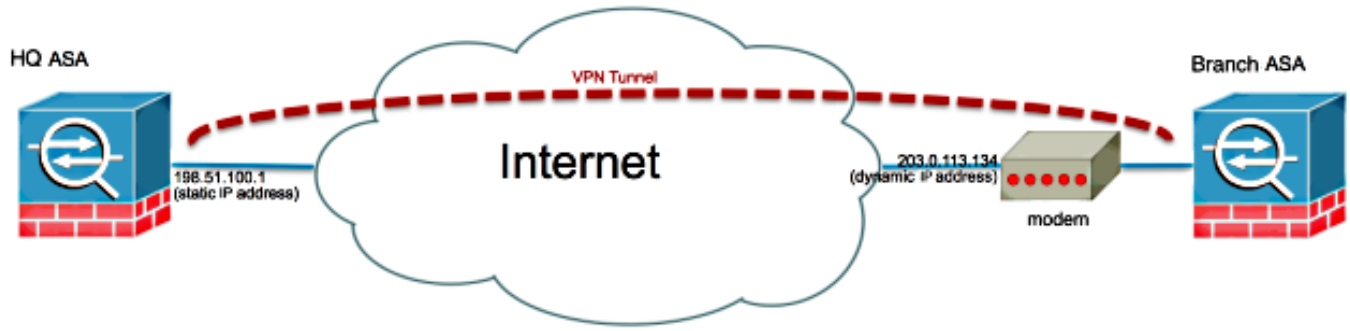
- Avec le groupe de tunnel DefaultL2LGroup
- Avec un groupe Désigné de tunnel

La plus grande différence de configuration entre les deux scénarios est l'ID de Protocole ISAKMP (Internet Security Association and Key Management Protocol) utilisé par le distant ASA. Quand le DefaultL2LGroup est utilisé sur l'ASA statique, l'ID de l'ISAKMP du pair doit être l'adresse. Cependant si un groupe Désigné de tunnel est utilisé, l'ID de l'ISAKMP du pair doit être identique le nom de groupe de tunnel utilisant cette commande :

```
crypto isakmp identity key-id <tunnel-group_name>
```

L'avantage d'utiliser les groupes Désignés de tunnel sur l'ASA statique est que quand le DefaultL2LGroup est utilisé, la configuration sur les ASA dynamiques distantes, qui inclut les clés pré-partagées, doit être identique et il ne tient pas compte de beaucoup de finesse avec l'installation des stratégies.

Diagramme du réseau



Configurez

Cette section décrit la configuration sur chaque ASA selon quelle solution vous décidez d'utiliser.

Solution 1 - Utilisation du DefaultL2LGroup

C'est la manière la plus simple de configurer un tunnel de l'entre réseaux locaux (L2L) entre deux

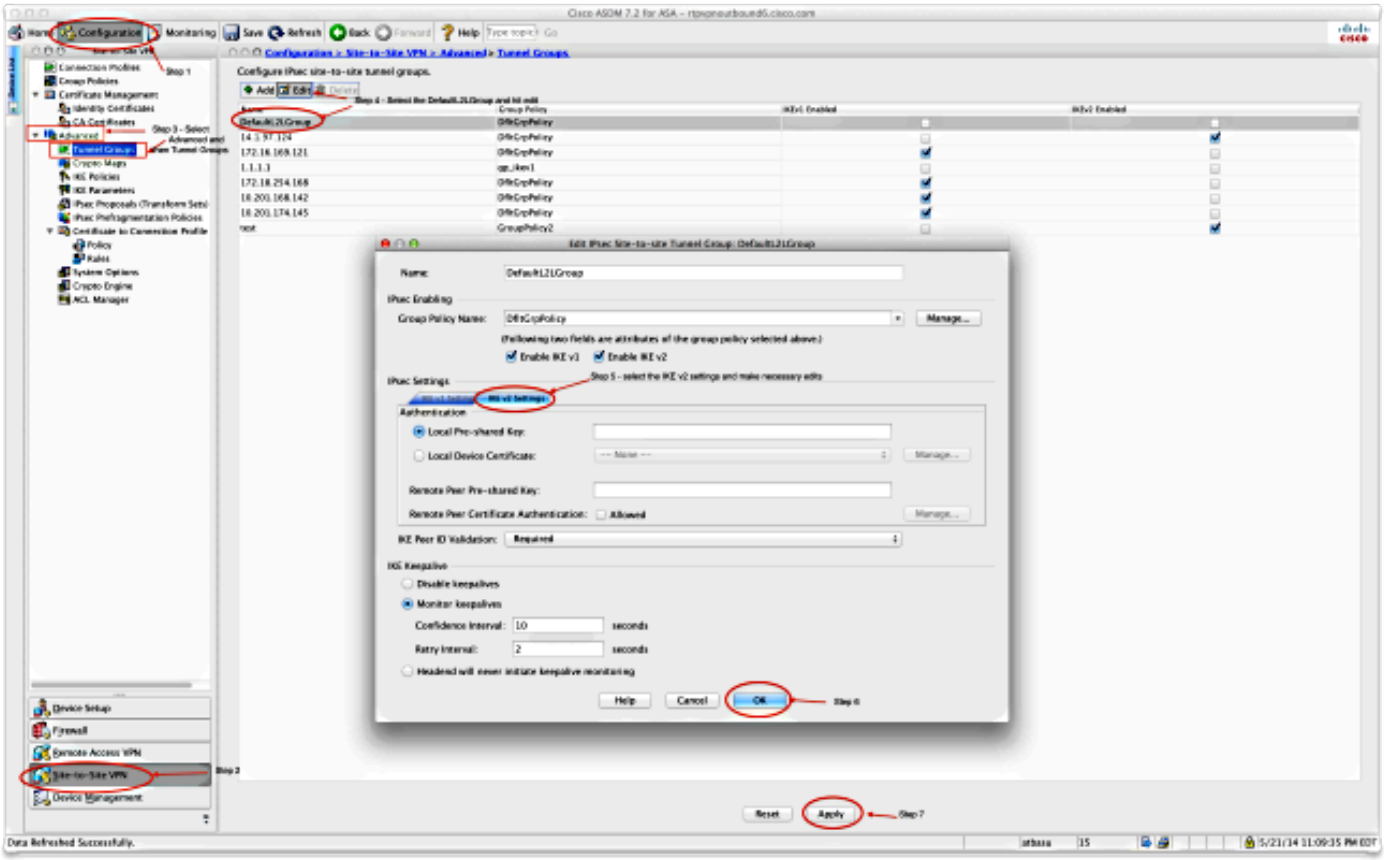
ASA quand une ASA obtient son adresse dynamiquement. Le groupe DefaultL2L est un groupe préconfiguré de tunnel sur l'ASA et tous connexions qui ne font pas explicitement chute particulière de groupe de tunnel de match any sur cette connexion. Puisque l'ASA dynamique n'a pas une constante a prédéterminé l'adresse IP, il signifie que l'admin ne peut pas configurer le Statis ASA afin de permettre la connexion sur un groupe spécifique de tunnel. Dans cette situation, le groupe DefaultL2L peut être utilisé afin de permettre les connexions dynamiques.

> **Conseil** : Avec cette méthode, le du côté incliné est que tous les pairs auront la même clé pré-partagée puisque seulement une clé pré-partagée peut être définie par groupe de tunnels et tous les pairs se connecteront au même groupe de tunnels DefaultL2LGroup.

Configuration statique ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

Sur Adaptive Security Device Manager (ASDM), vous pouvez configurer le DefaultL2LGroup comme affiché ici :



ASA dynamique

```
crypto isakmp identity key-id <tunnel-group_name>
```

Sur l'ASDM, vous pouvez utiliser l'assistant standard afin d'installer le profil approprié de connexion ou vous pouvez simplement ajouter une nouvelle connexion et suivre la procédure standard.

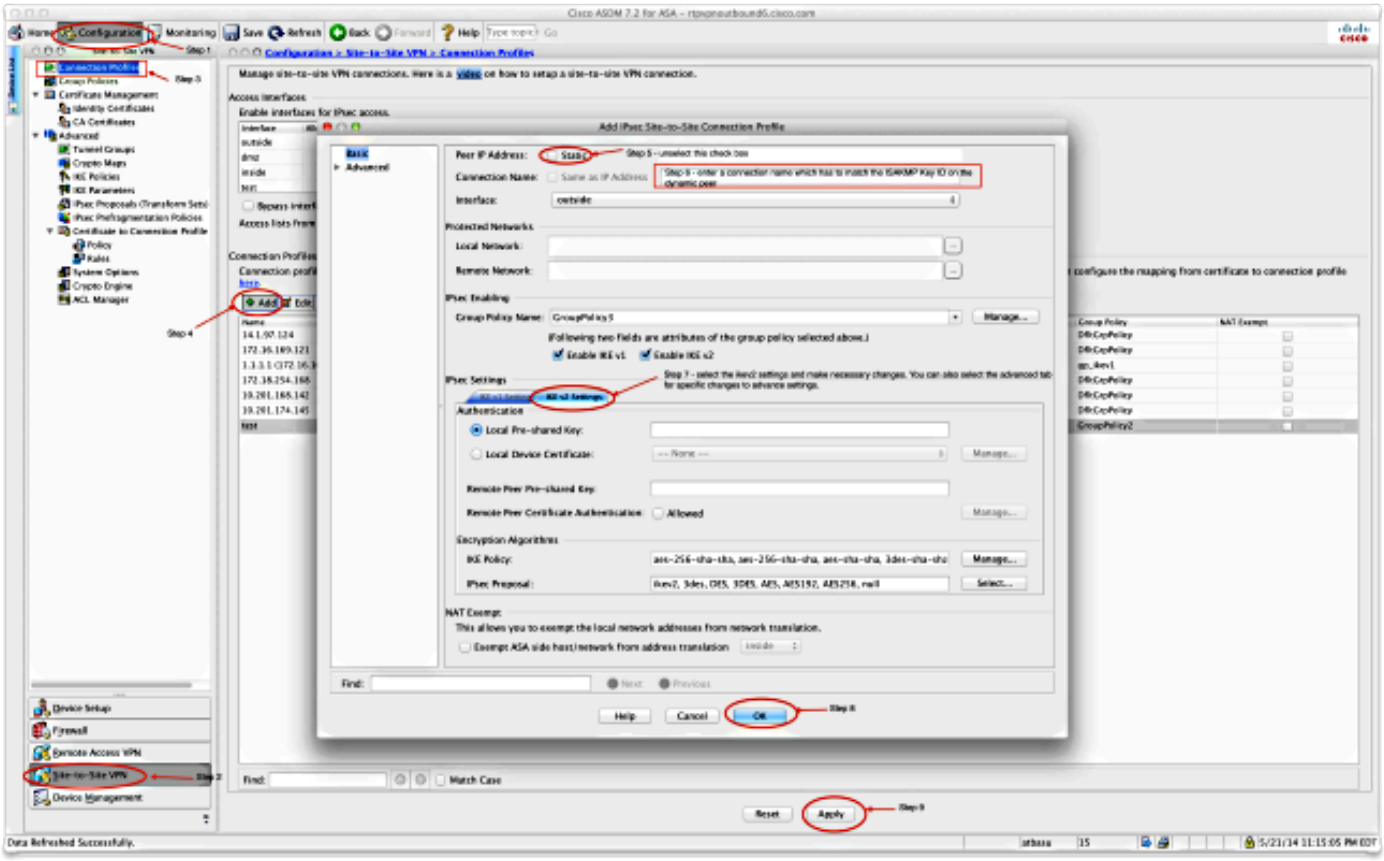
Solution 2 - Créez un groupe de tunnels défini par l'utilisateur

Cette méthode exige slighly plus de configuration, mais elle tient compte de plus de finesse. Chaque pair peut avoir sa propres stratégie distincte et clé pré-partagée. Néanmoins ici il est important de changer l'ID d'ISAKMP sur le pair dynamique de sorte qu'il utilise un nom au lieu d'une adresse IP. Ceci permet à l'ASA statique pour apparier la demande entrante d'initialisation d'ISAKMP au bon groupe de tunnel et pour utiliser les bonnes stratégies.

Configuration statique ASA

`crypto isakmp identity key-id <tunnel-group_name>`

Sur l'ASDM, le nom de profil de connexion est une adresse IP par défaut. Ainsi quand vous le créez, vous devez le changer afin de lui donner un nom suivant les indications du tir d'écran ici :



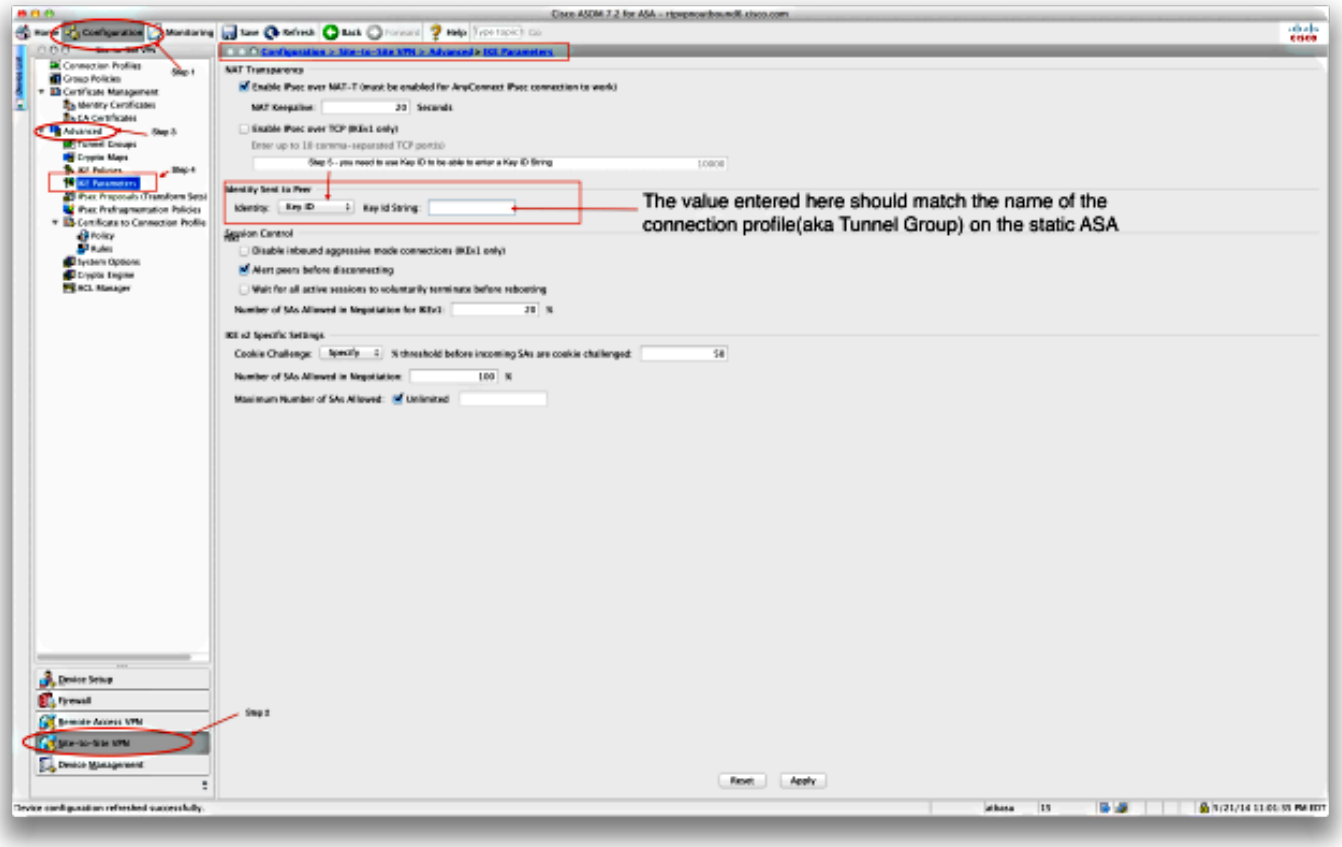
Configuration dynamique ASA

L'ASA dynamique est configurée presque la même manière dans les deux solutions en plus d'une commande comme affiché ici :

`crypto isakmp identity key-id DynamicSite2Site1`

Comme décrit précédemment, par défaut l'ASA utilise l'adresse IP de l'interface que le tunnel VPN est tracé à comme ID de clé d'ISAKMP. Néanmoins dans ce cas, l'ID de clé sur l'ASA dynamique est identique que le nom du groupe de tunnels sur l'ASA statique. Ainsi sur chaque pair dynamique, le clé-id sera différent et un groupe de tunnels correspondant doit être créé sur l'ASA statique avec le bon nom.

Sur l'ASDM, ceci peut être configuré suivant les indications de ce tir d'écran :



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Sur l'ASA statique

Voici le résultat de la **crypto** commande de **det d'IKEv2 SA d'exposition** :

```
crypto isakmp identity key-id DynamicSite2Site1
```

Voici le résultat de la commande de **show crypto ipsec sa** :

```
crypto isakmp identity key-id DynamicSite2Site1
```

Sur l'ASA dynamique

Voici le résultat de la **crypto** commande de **détail d'IKEv2 SA d'exposition** :

```
crypto isakmp identity key-id DynamicSite2Site1
```

Voici le résultat de la commande de **show crypto ipsec sa** :

```
crypto isakmp identity key-id DynamicSite2Site1
```

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **crypto paquet IKEv2 DEB**
- **DEB crypto IKEv2 interne**