ASA 8.x/ASDM 6.x : Ajoutez les nouvelles informations d'homologue VPN dans un site à site existant VPN utilisant l'ASDM

Contenu

Introduction

Ce document fournit des informations au sujet des modifications basées sur la configuration pour faire quand un nouvel homologue VPN est ajouté à la configuration du VPN existante de site à site utilisant Adaptive Security Device Manager (ASDM). Ceci est exigé dans ces scénarios :

- Le fournisseur de services Internet (ISP) a été changé et un nouvel ensemble de plage IP de public est utilisé.
- Une nouvelle conception complète du réseau à un site.
- Le périphérique utilisé comme passerelle VPN à un site est migré vers un nouveau périphérique avec une différente adresse IP publique.

Ce document suppose que le site à site VPN est déjà configuré correctement et fonctionne bien. Ce document fournit les étapes pour suivre afin de changer des informations d'homologue VPN en configuration du VPN L2L.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de ce thème :

- Exemple de configuration du VPN de site à site ASA

Composants utilisés

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

- Gamme 5500 d'appareils de Sécurité de Cisco Adapative avec la version de logiciel 8.2 et plus tard
- Security Device Manager de Cisco Adapative avec la version de logiciel 6.3 et plus tard

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Les informations de Backround

Le site à site VPN fonctionne bien entre le HQASA et le BQASA. Supposez que le BQASA a une nouvelle conception complète de réseau et le schéma IP a été modifié au niveau ISP, mais tous les détails internes de sous-réseau demeurent les mêmes.

Cette configuration d'échantillon utilise ces adresses IP :

- BQASA existant en dehors de l'adresse IP - 200.200.200.200
- Nouveau BQASA en dehors de l'adresse IP - 209.165.201.2

Remarque: Ici, seulement les informations de pair seront modifiées. Puisqu'il n'y a aucun autre changement de sous-réseau interne, les cryptos Listes d'accès demeurent les mêmes.

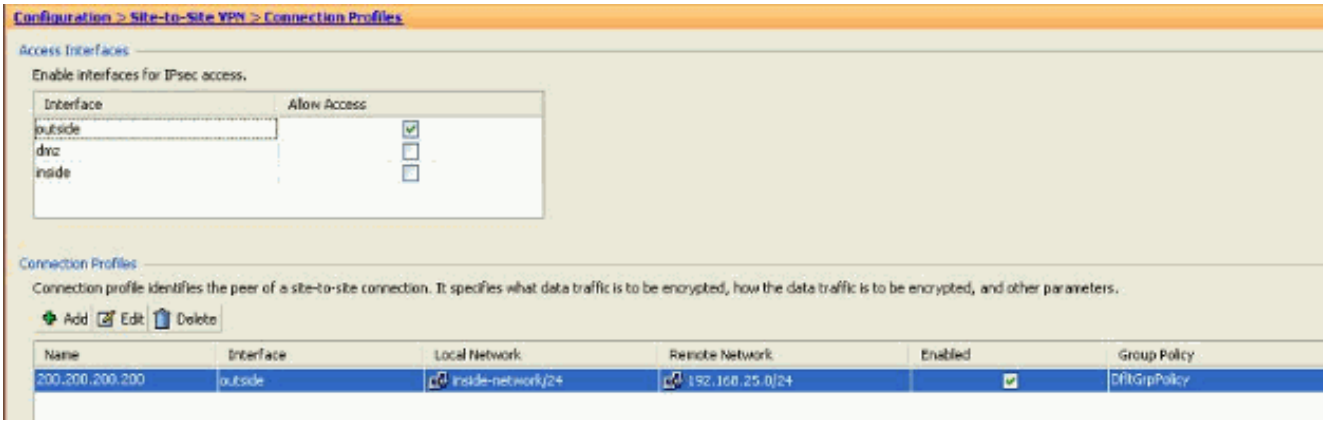
Configuration ASDM

Cette section fournit des informations au sujet des méthodes possibles utilisées pour changer les informations d'homologue VPN sur HQASA utilisant l'ASDM.

Créez un nouveau profil de connexion

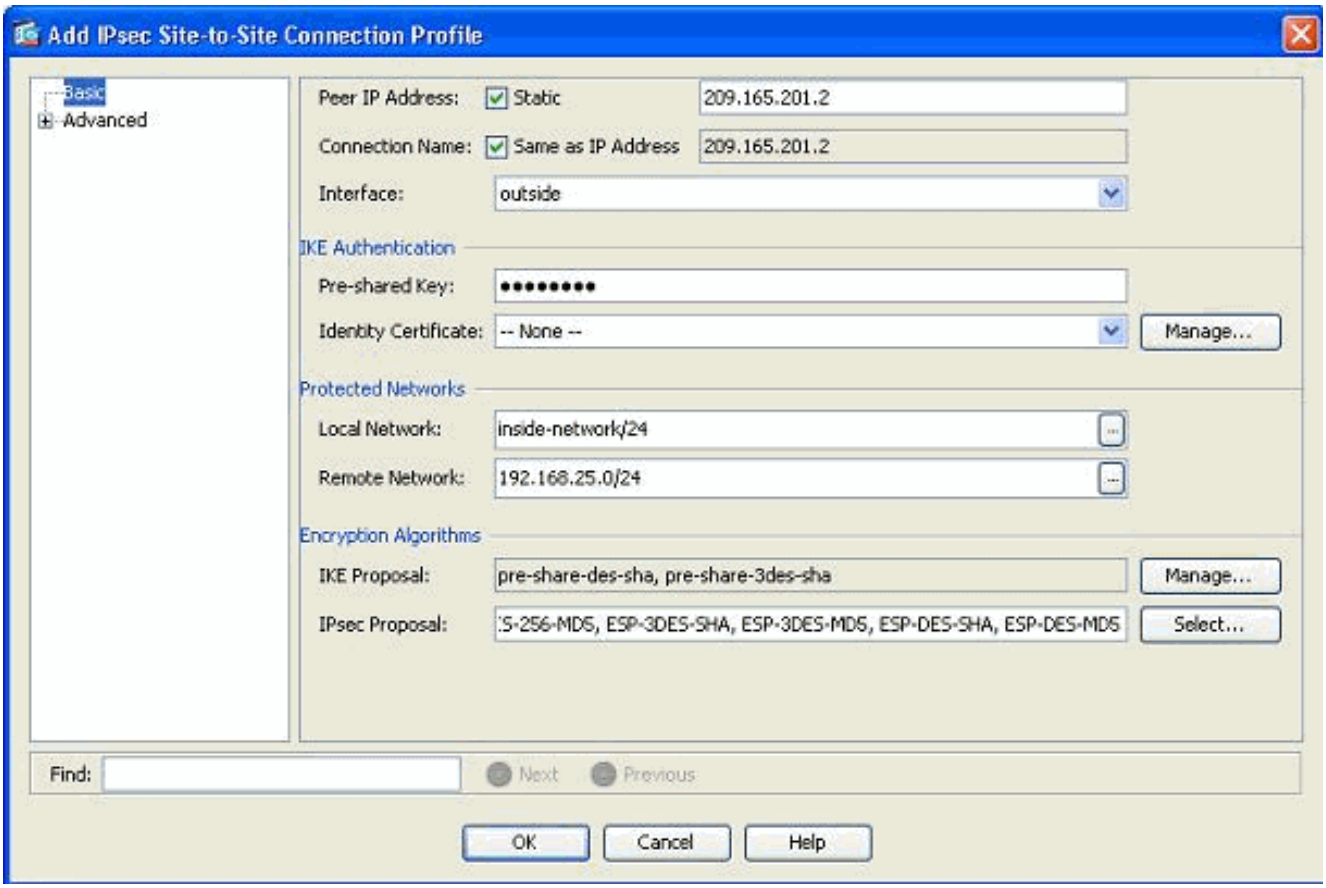
Ceci peut être la méthode plus facile parce qu'il ne touche pas à la configuration du VPN existante et peut créer un nouveau profil de connexion avec les informations relatives de nouvel homologue VPN.

1. Allez à la *configuration > au site à site VPN > profils de connexion* et cliquez sur Add sous la région de profils de
connexion.

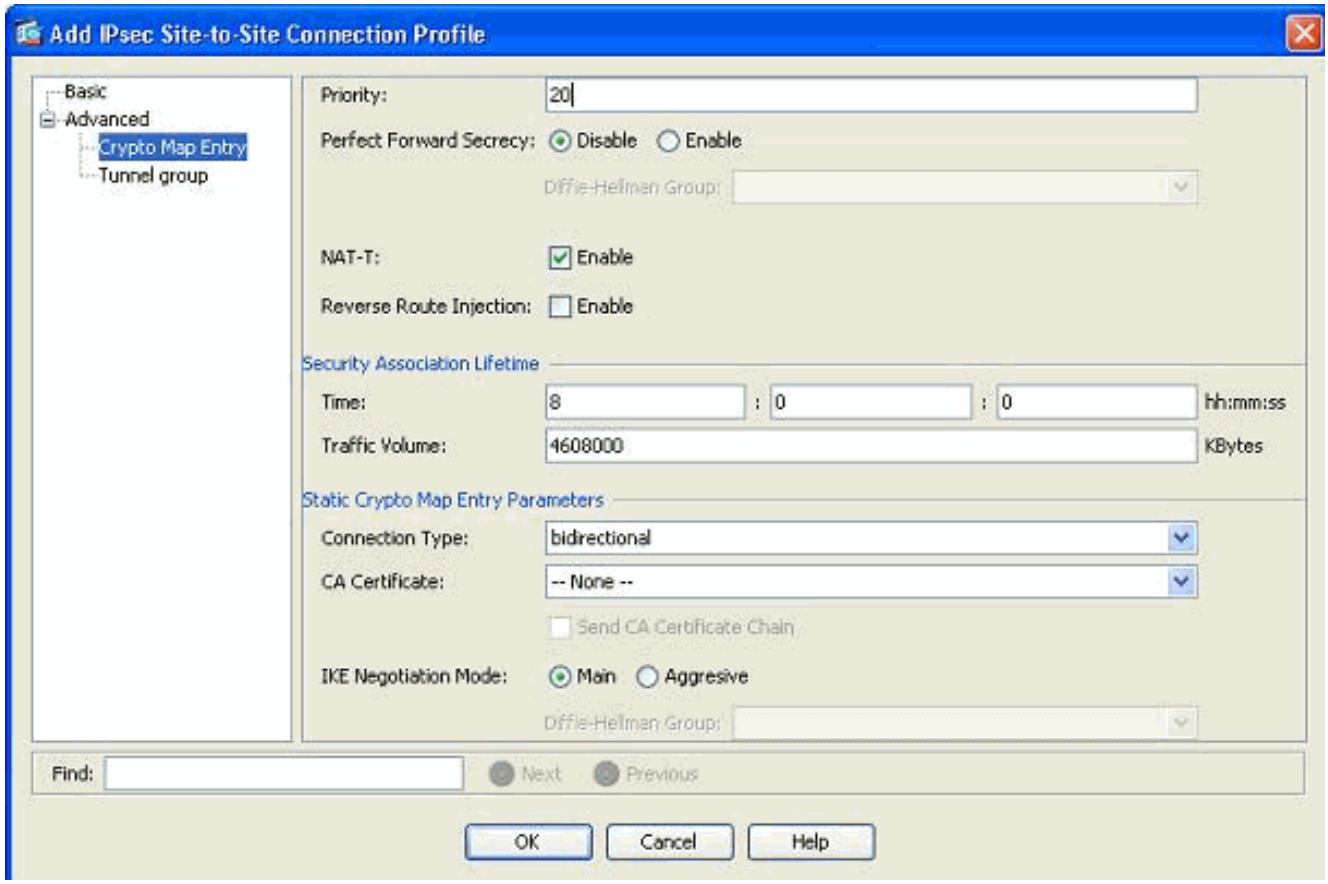


La fenêtre de *profil de connexion d'IPSec site à site d'ajouter* s'ouvrent.

2. Sous l'onglet de base, fournissez les détails pour l'*adresse IP de pair*, la *clé pré-partagée*, et les *réseaux protégés*. Utilisez tous les mêmes paramètres que le VPN existant, excepté les informations de pair. Cliquez sur
OK.



3. Sous le menu avancé, *entrée de crypto map de* clic. Référez-vous à l'onglet *prioritaire*. Cette priorité est égale au numéro de séquence dans sa configuration équivalente CLI. Quand un peu de nombre que l'entrée existante de crypto map est assigné, ce nouveau profil est exécuté d'abord. Plus le numéro prioritaire est élevé, les moins la valeur. Ceci est utilisé pour changer la commande de l'ordre qu'un crypto map spécifique sera exécuté. Cliquez sur OK pour se terminer en créant le nouveau profil de
connexion.



Ceci crée automatiquement un nouveau groupe de tunnels avec un crypto map associé. Assurez-vous que vous pouvez atteindre le BQASA avec la nouvelle adresse IP avant que vous utilisiez ce nouveau profil de connexion.

Éditez la configuration du VPN existante

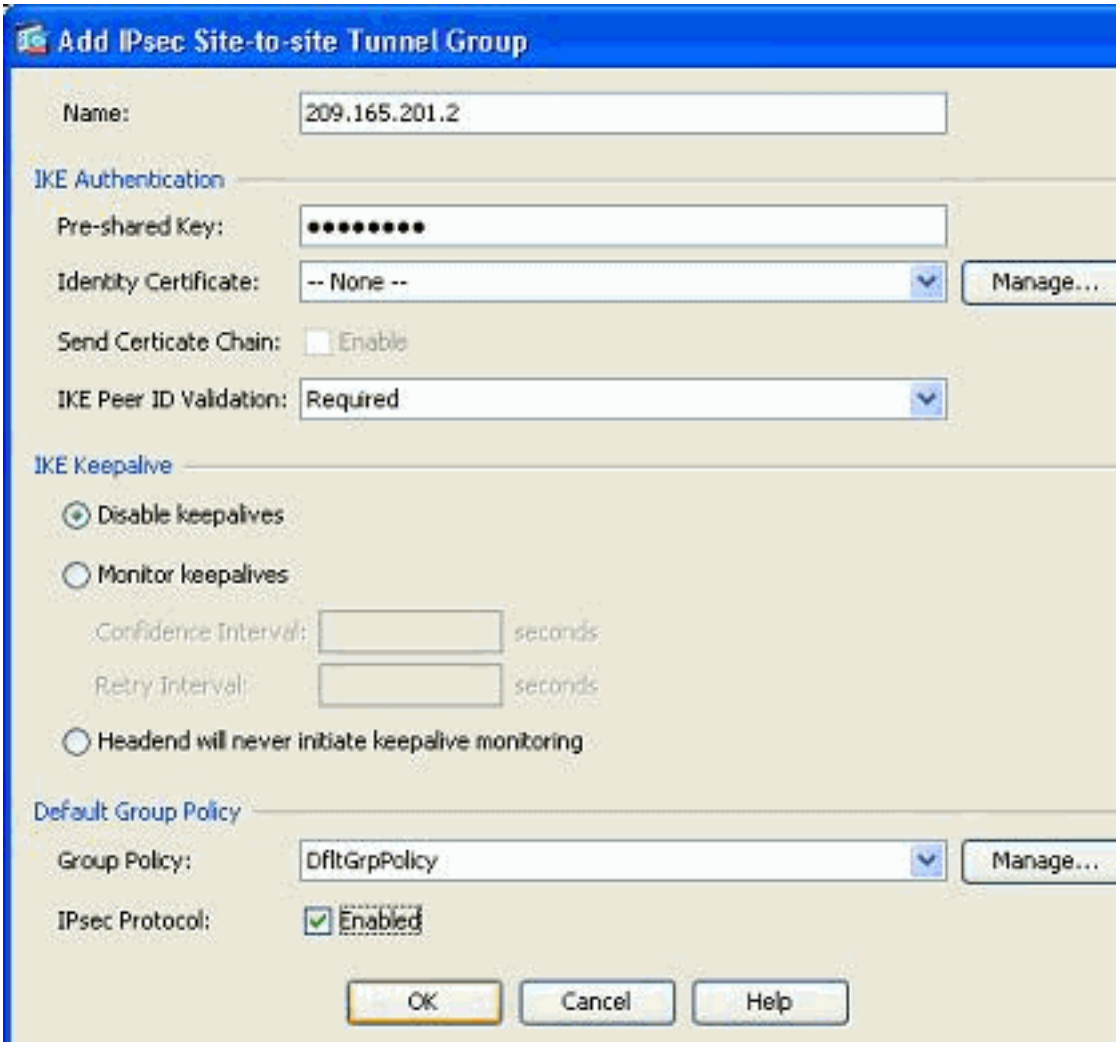
Une autre manière d'ajouter un nouveau pair est de modifier la configuration existante. Le profil de connexion existante ne peut pas être édité pour les nouvelles informations de pair parce qu'il est lié à un pair spécifique. Afin d'éditer la configuration existante, vous devez exécuter ces étapes :

1. Créez un nouveau groupe de tunnel
2. Éditez le crypto map existant

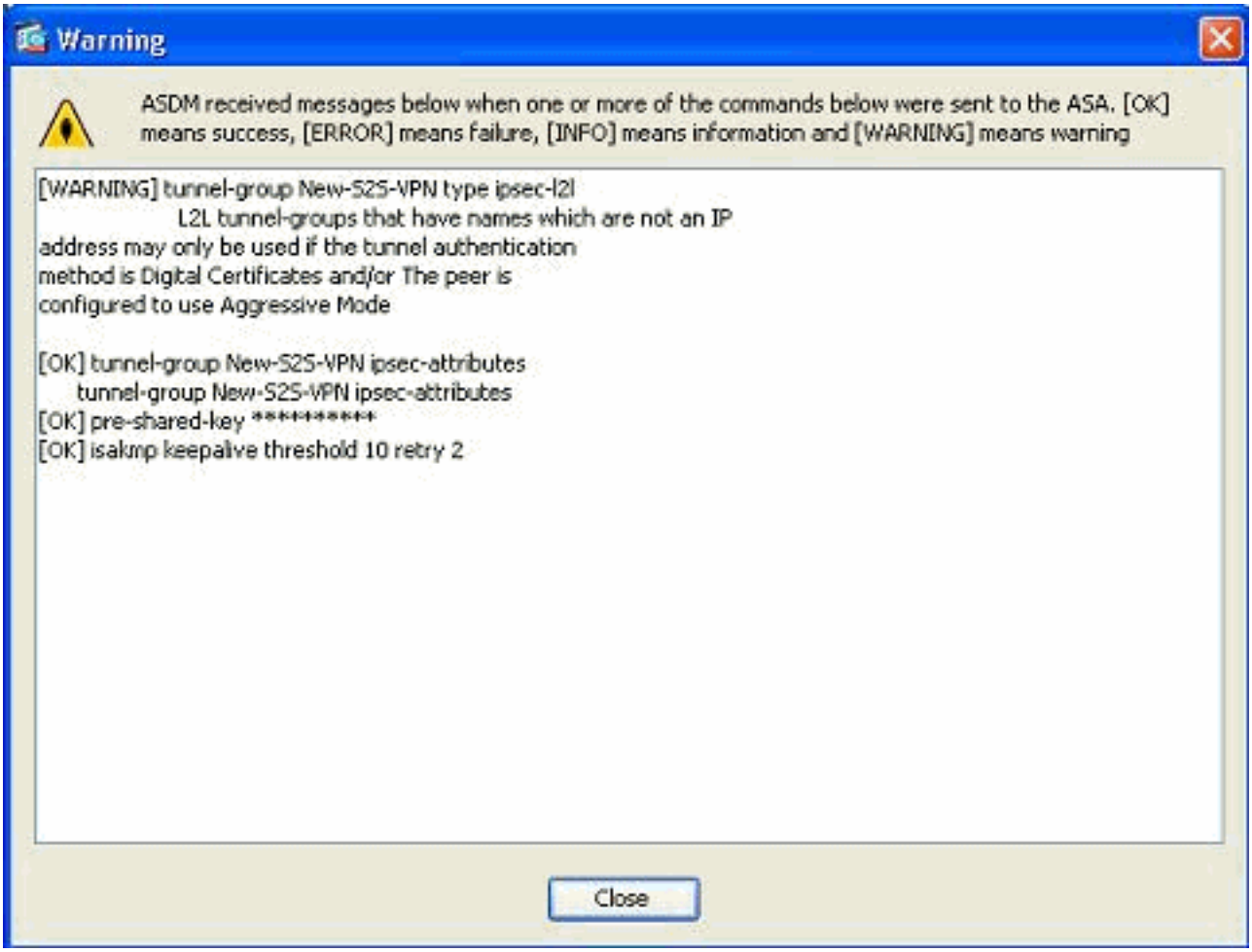
Créez un nouveau groupe de tunnel

Allez à la *configuration > au site à site VPN > a avancé > des groupes de tunnel* et clique sur Add pour créer un nouveau groupe de tunnels qui contient les nouvelles informations d'homologue VPN. Spécifiez le *nom* et les zones de tri *pré-partagées*, puis cliquez sur OK.

Remarque: Assurez-vous que la clé pré-partagée apparie l'autre fin du VPN.



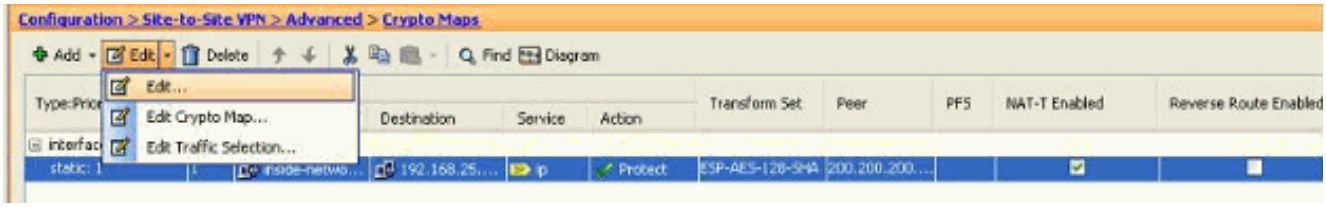
Remarque: Dans la zone d'identification, seulement l'adresse IP du pair distant devrait être écrite quand l'authentication mode est des clés pré-partagées. N'importe quel nom peut être utilisé seulement quand la méthode d'authentification est par des Certificats. Cette erreur apparaît quand un nom est ajouté dans la zone d'identification et la méthode d'authentification est pré-partagée :



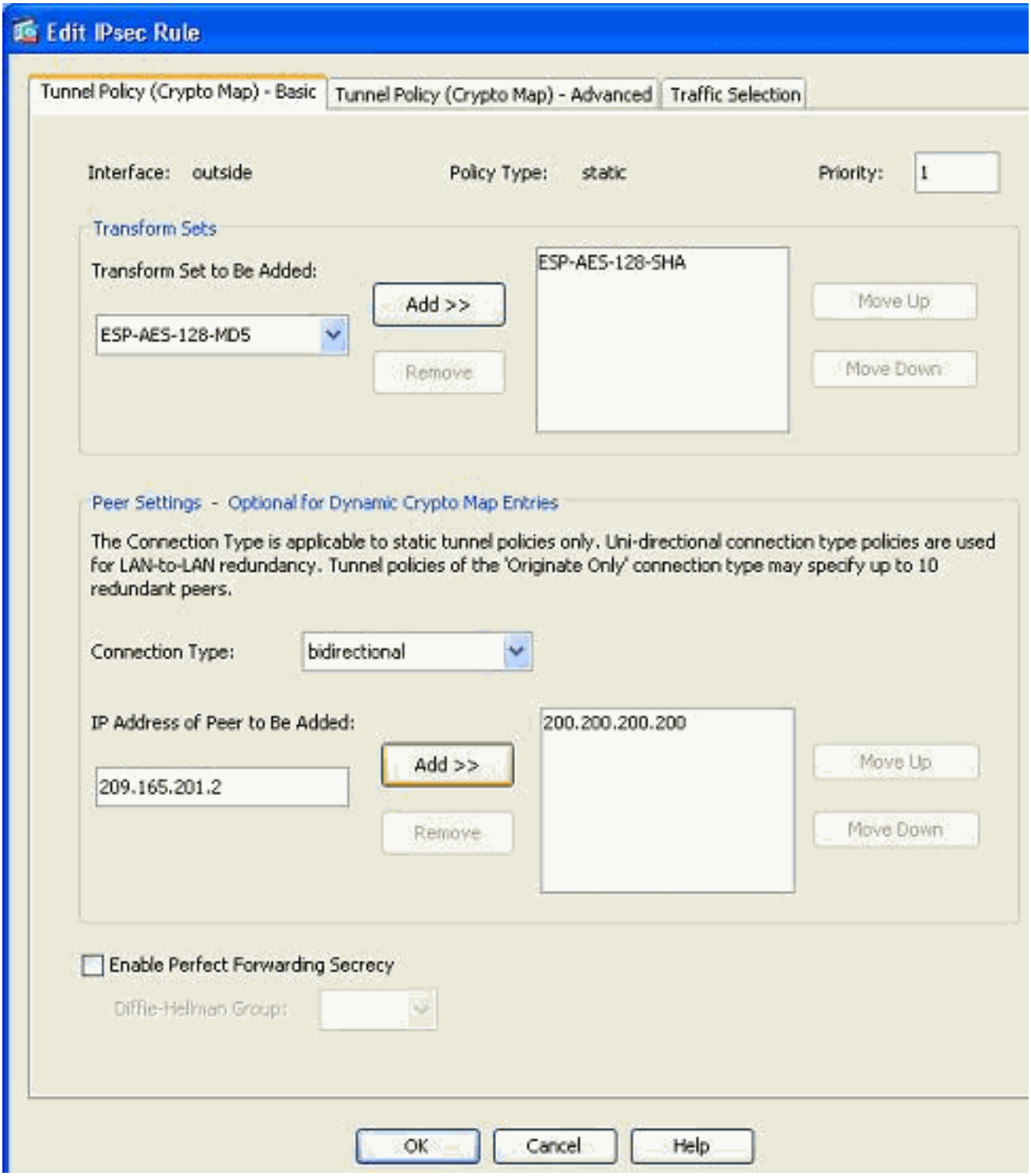
Éditez le crypto map existant

Le crypto map existant peut être édité afin d'associer les nouvelles informations de pair.

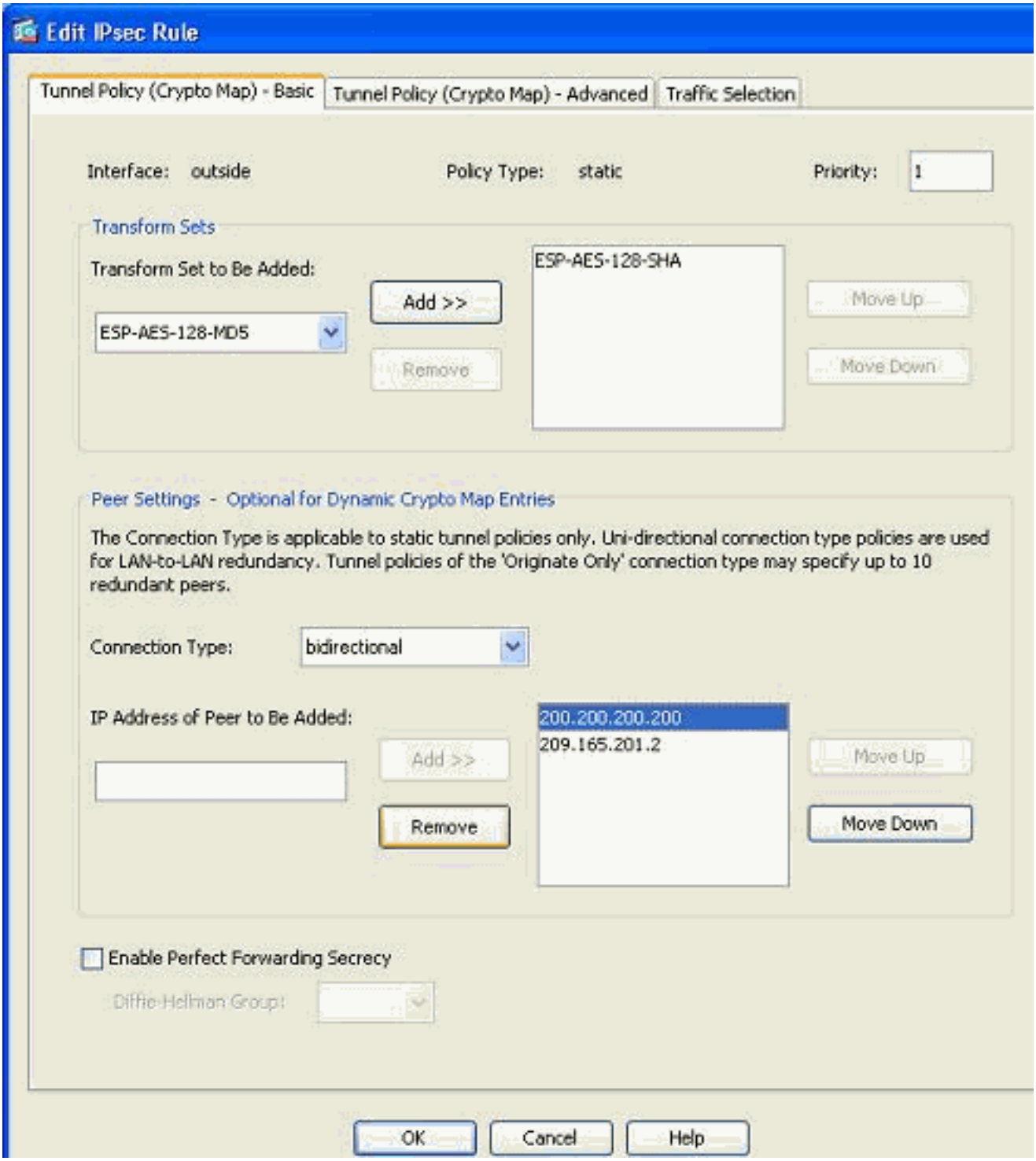
Procédez comme suit :

1. Allez à la *configuration > au site à site VPN > a avancé > des crypto map*, puis sélectionne le crypto map requis et clique sur
   Edit.
   

   La fenêtre de *règle IPSec d'éditer* apparaît.
2. Sous l'onglet (de base) de stratégie de tunnel, dans la région de configurations de pair, spécifiez le nouveau pair dans l'adresse IP du pair pour être champ ajouté. Puis, cliquez sur Add.

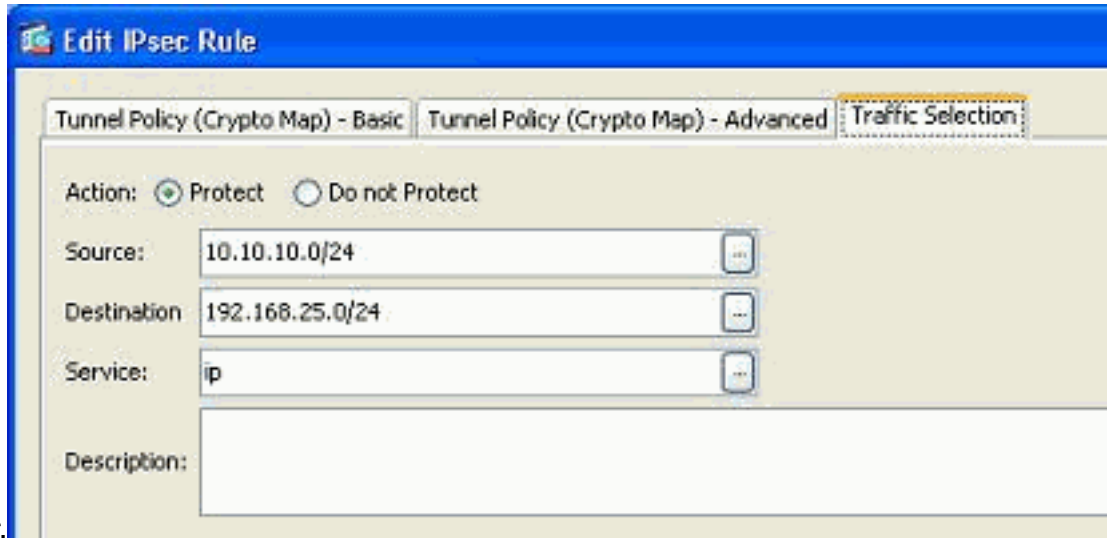


3. Sélectionnez l'adresse IP existante de pair et le clic *retirent* pour retenir les nouvelles informations de pair seulement. Cliquez sur
OK.



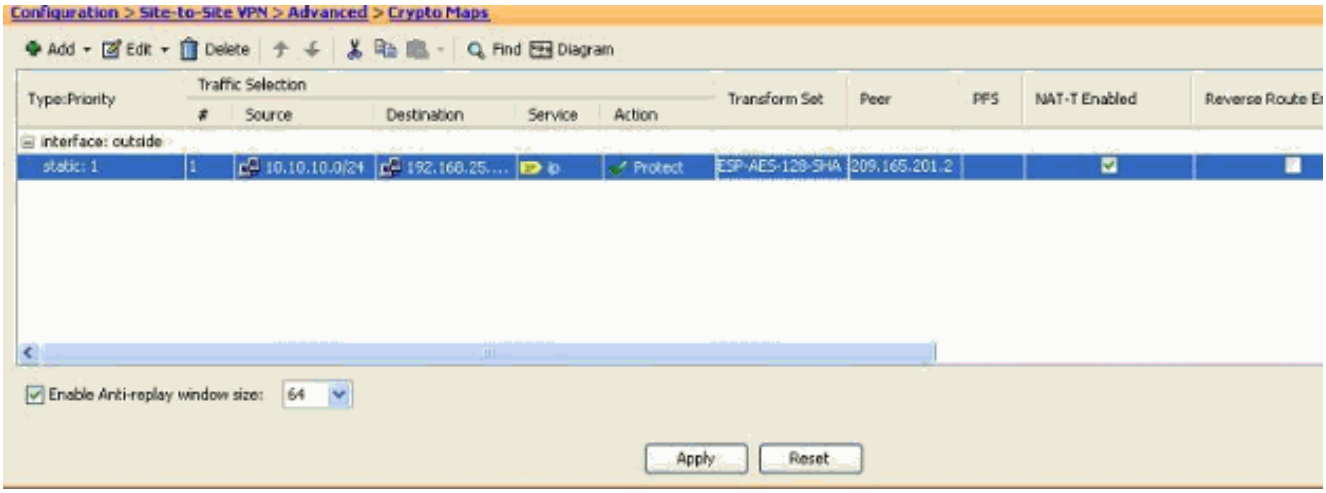
Remarque: Après que vous modifiiez les informations de pair dans le crypto map en cours, le profil de connexion associé avec ce crypto map est supprimé immédiatement dans la fenêtre ASDM.

4. Les détails des réseaux chiffrés demeurent les mêmes. Si vous devez modifier ces derniers, allez à l'onglet de *sélection du*



trafic.

5. Allez à la *configuration > au site à site VPN > a avancé >* volet de *crypto map* afin de visualiser le crypto map modifié. Cependant, ces modifications n'interviennent pas jusqu'à ce que vous cliquiez sur Apply. Après que vous cliquiez sur Apply, allez à la *configuration > au site à site VPN > a avancé >* menu de *groupes de tunnel* afin de vérifier si un groupe de tunnels associé est présent ou pas. Si oui, alors un *profil* associé de *connexion* sera créé.



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- Utilisez cette commande de visualiser les paramètres d'association de sécurité spécifiques à un pair simple :adresse IP de <Peer de pair de show crypto ipsec sa >

Dépannez

Utilisez cette section pour dépanner votre configuration.

IKE Initiator unable to find policy: Test_ext d'Intf, Src : 172.16.1.103, Dst : 10.1.4.251

Cette erreur est affichée dans les messages de log en essayant de changer l'homologue VPN d'un concentrateur VPN à l'ASA.

Solution :

Ceci peut être un résultat des étapes de configuration incorrecte suivies pendant le transfert. Assurez-vous que la crypto attache à l'interface est retirée avant que vous ajoutiez un nouveau pair. En outre, assurez-vous que vous avez utilisé l'adresse IP du pair au groupe de tunnels, mais pas le nom.

Informations connexes

- Site à site (L2L) VPN avec l'ASA
- La plupart des problèmes communs VPN
- Page de Soutien technique ASA
- Support et documentation techniques - Cisco Systems