ASA 8. x/ASDM 6. x: Добавьте Новые Сведения об одноранговом узле сети VPN в Существующем Сквозном VPN-соединение ASDM использования

Содержание

Введение

Когда новый узел VPN добавлен к существующей сквозной VPN-соединение конфигурации с помощью Менеджера устройств адаптивной безопасности (ASDM) (ASDM), этот документ предоставляет сведения о конфигурационных изменениях для создания. Это требуется в этих сценариях:

- Интернет-провайдер (ISP) был изменен, и используется новый набор общего диапазона IP.
- Завершенная модернизация сети на узле.
- Устройство, используемое в качестве Шлюза VPN на узле, перемещено на новое устройство с другим открытым IP - адресом.

Этот документ предполагает, что сквозное VPN-соединение уже настроено должным образом и хорошо работает. Этот документ предоставляет шаги для придержаний для изменения сведений об одноранговом узле сети VPN в конфигурации VPN L2L.

Предварительные условия

Требования

Компания Cisco рекомендует ознакомиться с этой темой:

- ASA Сквозной VPN-соединение пример конфигурации

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Серия 5500 Устройства безопасности Cisco Adapative с версией программного обеспечения 8.2 и позже
- Security Device Manager Cisco Adapative с версией программного обеспечения 6.3 и позже

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Информация о Backround

Сквозное VPN-соединение хорошо работает между HQASA и BQASA. Предположите, что BQASA имеет модернизацию полной сети, и схема IP модифицировалась на уровне интернет-провайдера, но все подробные данные внутренней подсети остаются тем же.

Этот пример конфигурации использует эти IP-адреса:

- Существующий Внешний IP - адрес BQASA - 200.200.200.200
- Новый Внешний IP - адрес BQASA - 209.165.201.2

Примечание: Здесь, только сведения об одноранговом узле сети будут модифицироваться. Поскольку нет никакого другого изменения во внутренней подсети, крипто-access-lists остаются тем же.

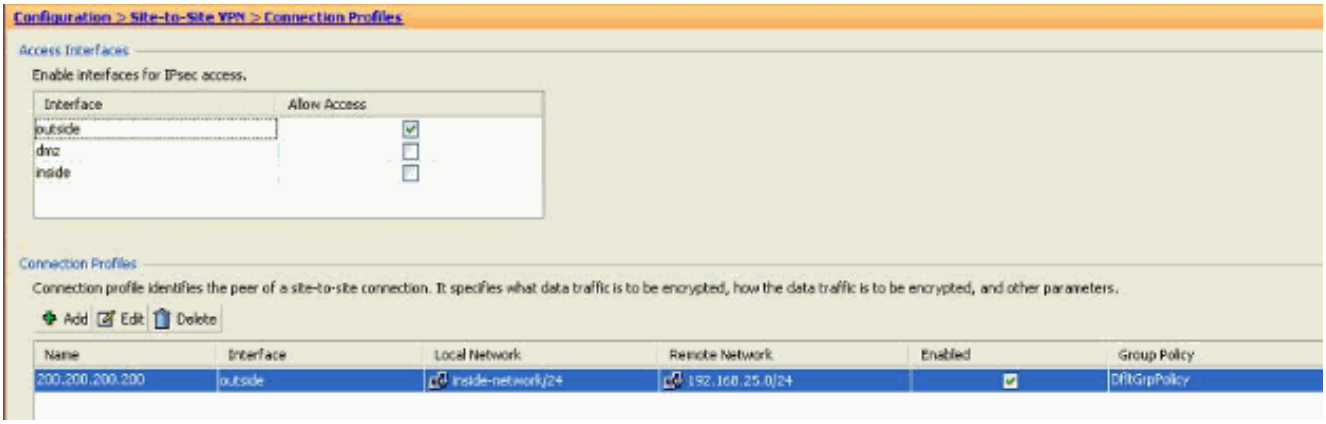
Настройка посредством ASDM

Этот раздел предоставляет сведения о возможных методах, используемых для изменения сведений об одноранговом узле сети VPN на HQASA использование ASDM.

Создайте профиль нового соединения

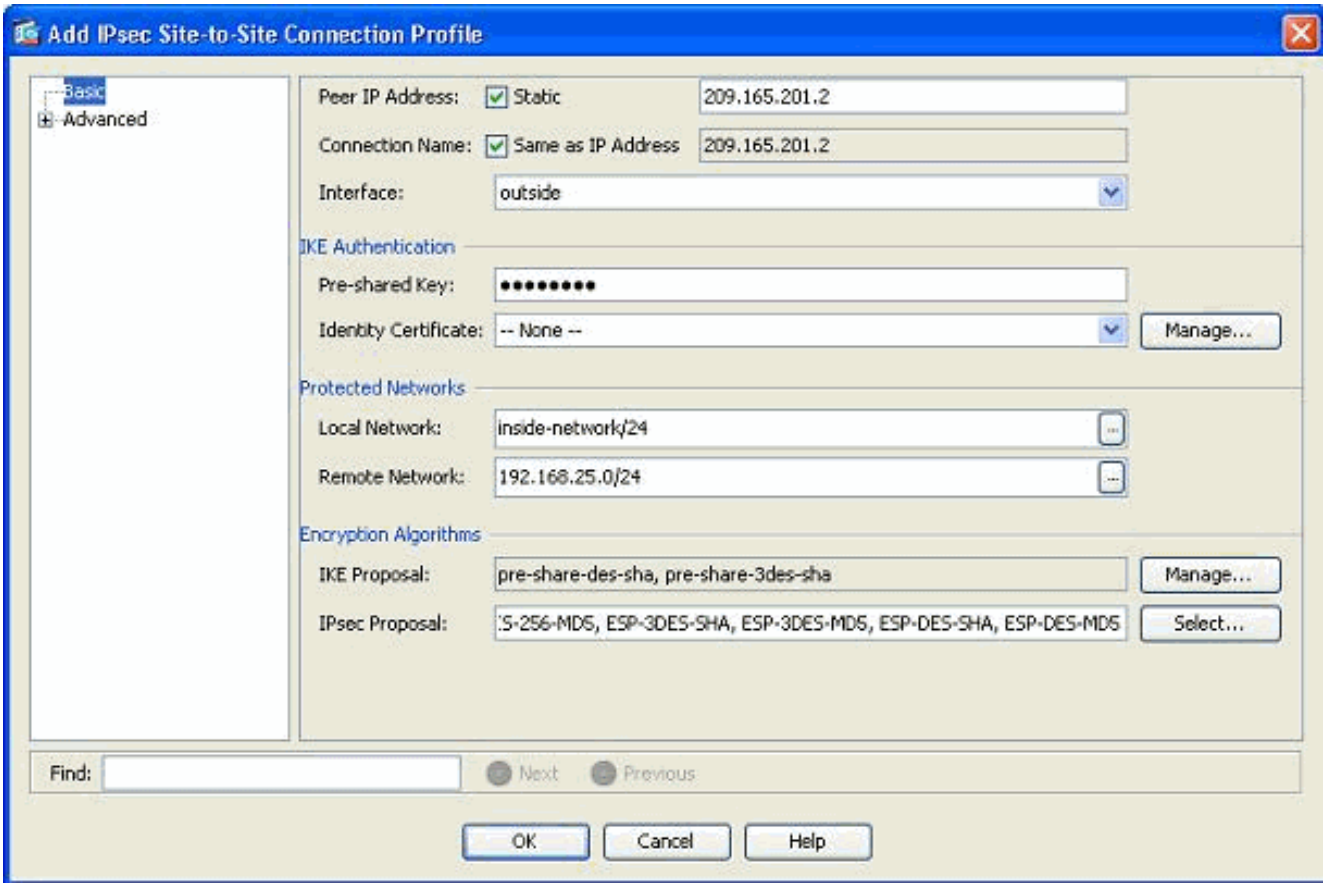
Это может быть более легким методом, потому что он не нарушает существующую конфигурацию VPN и может создать профиль нового соединения с новыми одноранговыми дополнительными сведениями VPN.

1. Перейдите *к Конфигурации> Сквозной VPN-соединение> Профили подключения* и *нажмите Add* под областью Connection Profiles.

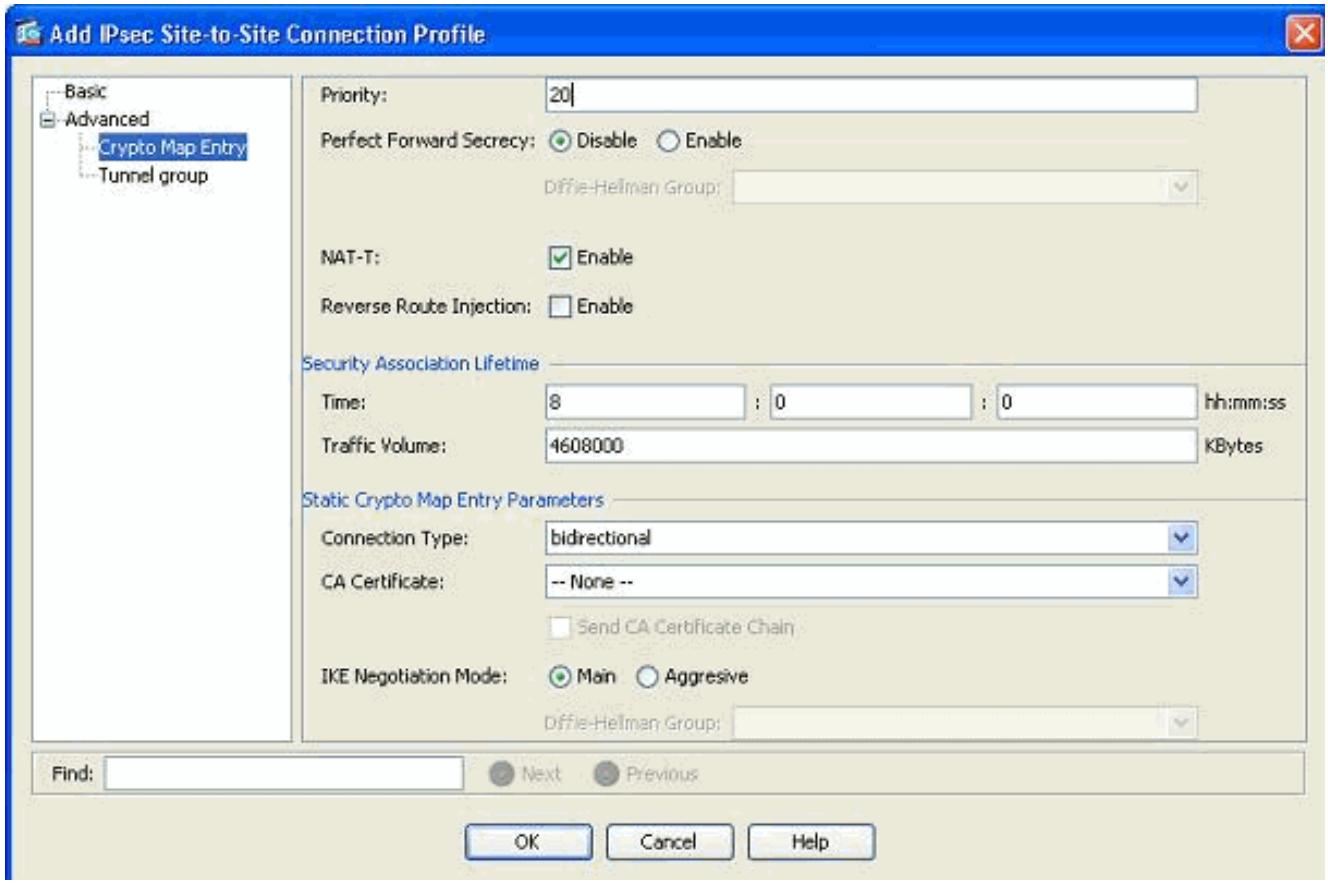


Окно *Add IPSec Site-to-Site Connection Profile* открывается.

2. Под вкладкой Basic предоставьте подробную информацию для *IP - адреса адресуемого точки*, *Предварительного общего ключа* и *Защищенных сетей*. Используйте весь одинаковый параметры в качестве существующей VPN, кроме сведений об одноранговом узле сети. *Нажмите кнопку OK.*



3. В соответствии с меню Advanced, нажмите *Crypto Map Entry*. См. вкладку *Priority*. Этот Приоритет равен порядковому номеру в его эквивалентной конфигурации CLI. Когда меньший номер, чем существующий элемент криптокарты назначен, этот новый профиль выполняется сначала. Чем выше указатель приоритета, тем меньший значение. Это используется для изменения заказа последовательности, что будет выполняться определенная криптокарта. Нажмите *OK* для завершения создания профиля нового соединения.



Это автоматически создает новую туннельную группу наряду с связанной криптокартой. Удостоверьтесь, что можно достигнуть BQASA с новым IP-адресом перед использованием этого профиля нового соединения.

Отредактируйте существующую конфигурацию VPN

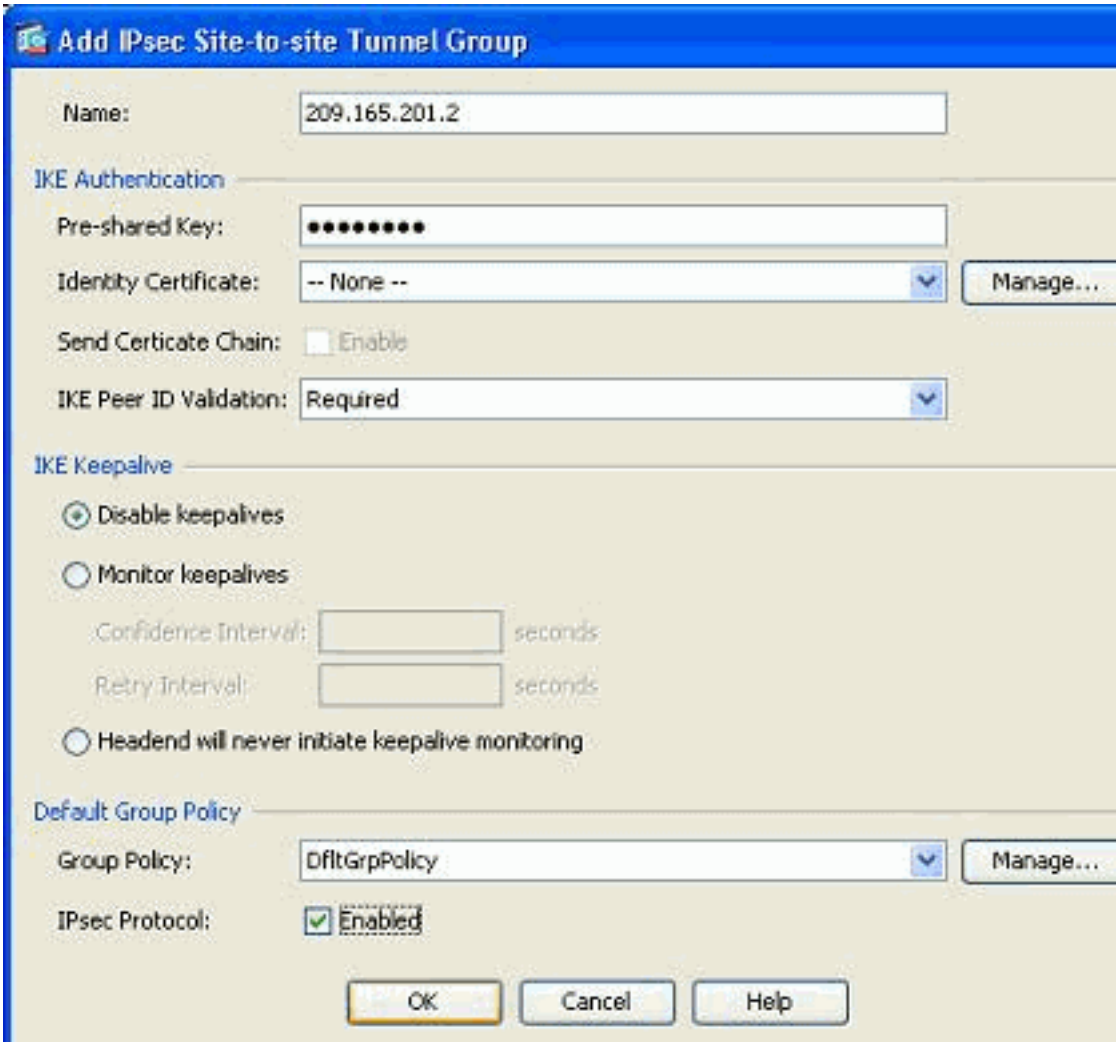
Другой способ добавить новый узел состоит в том, чтобы модифицировать существующую конфигурацию. Профиль существующего соединения не может быть изменен для новых сведений об одноранговом узле сети, потому что это связано с определенным узлом. Для редактирования существующей конфигурации необходимо выполнить эти шаги:

1. Создайте новую туннельную группу
2. Отредактируйте существующую криптокарту

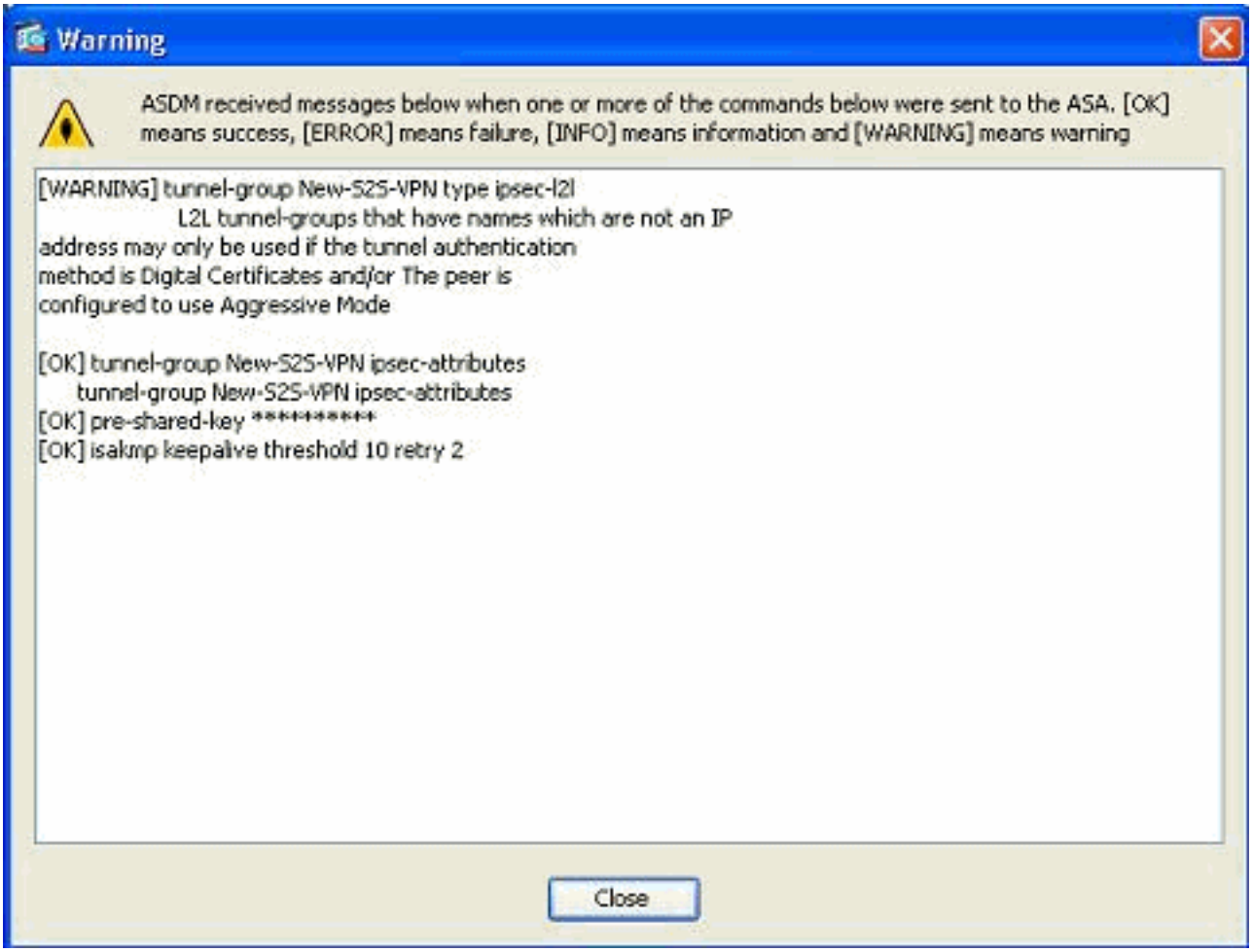
Создайте новую туннельную группу

Перейдите *к Конфигурации> Сквозной VPN-соединение> Усовершенствованный> Туннельные группы* и *нажмите Add* для создания новой туннельной группы, которая содержит новые сведения об одноранговом узле сети VPN. Задайте поля *Name и Pre-shared Key*, затем нажмите *OK*.

Примечание: Удостоверьтесь, что Предварительный общий ключ совпадает с другим концом VPN.



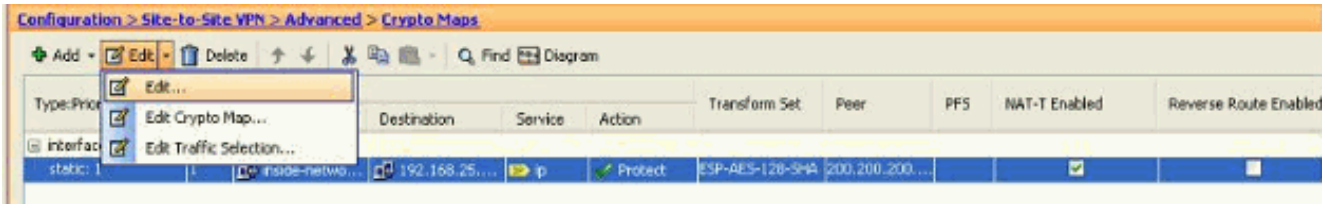
Примечание: Когда режим аутентификации является предварительными общими ключами, в Поле имени только должен быть введен IP-адрес удаленного узла. Любое название может использоваться только, когда метод аутентификации через сертификаты. Эта ошибка появляется, когда название добавлено в Поле имени, и метод аутентификации является предварительным общим:



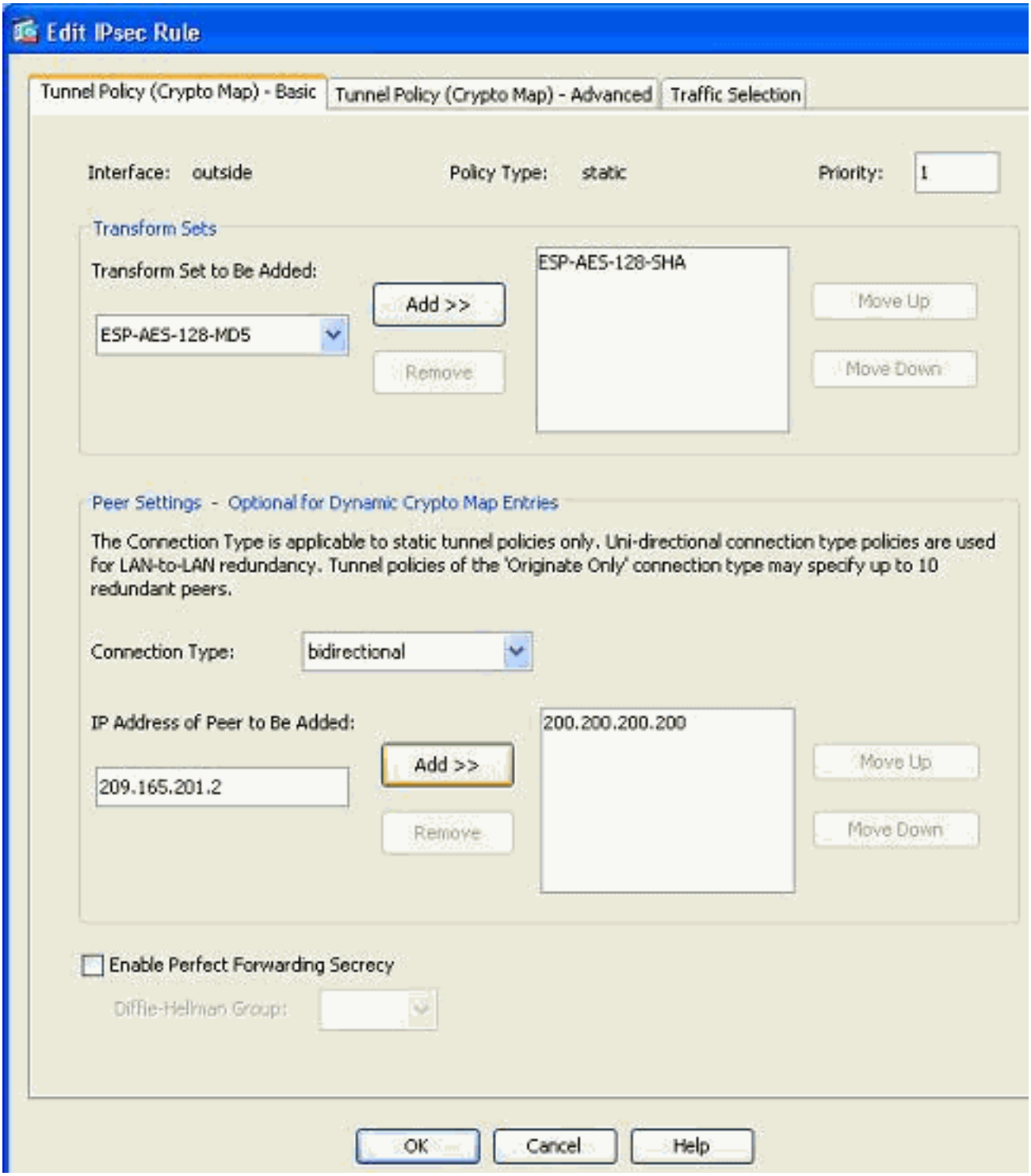
Отредактируйте существующую криптокарту

Существующая криптокарта может быть отредактирована для соединения новых сведений об одноранговом узле сети.

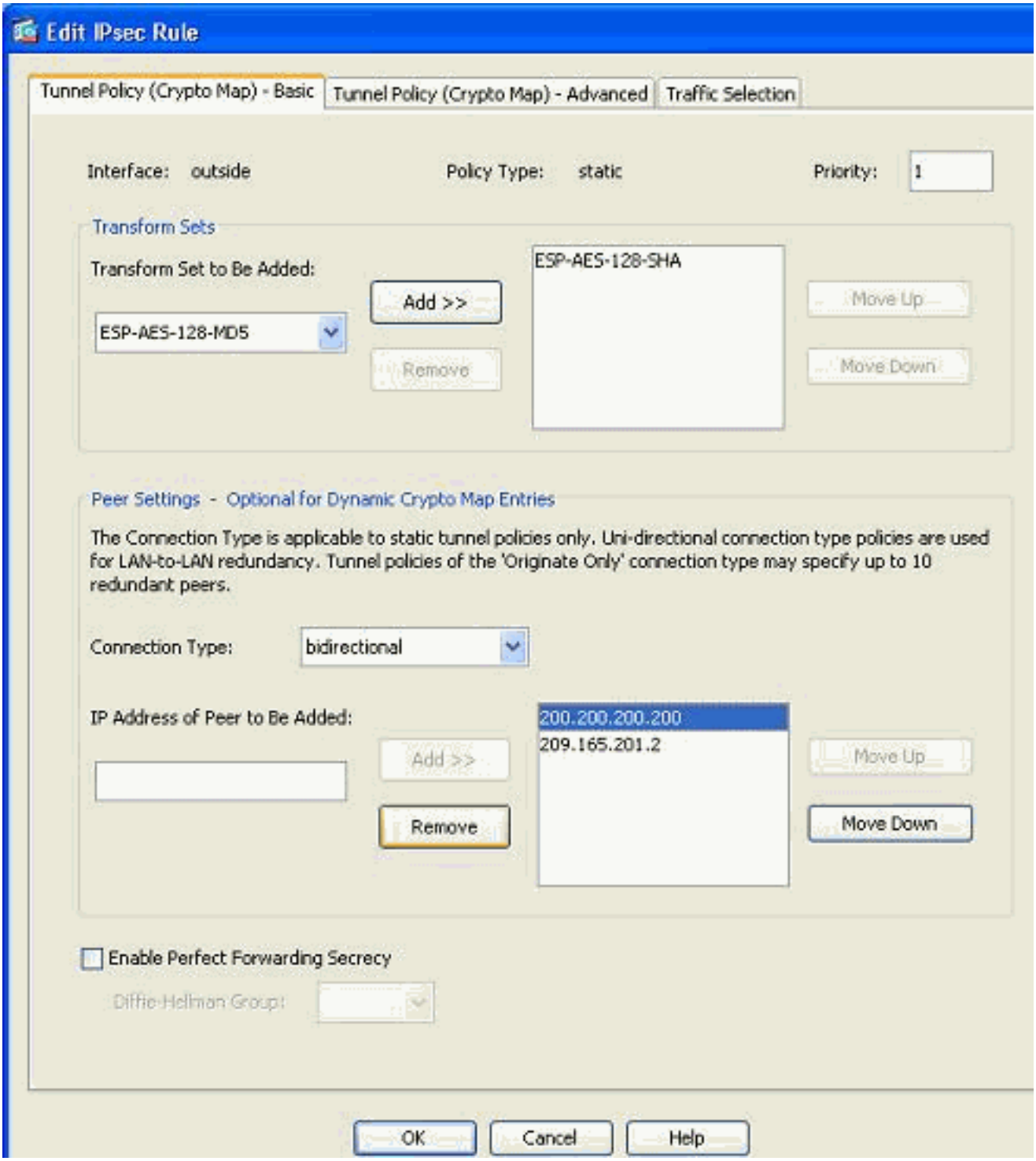
Выполните следующие действия:

1. Перейдите *к Конфигурации> Сквозной VPN-соединение> Усовершенствованный> Криптокарты*, затем выберите требуемую криптокарту и нажмите *Edit*.


Окно *Edit IPSec Rule* появляется.
2. Под вкладкой Tunnel Policy (Basic), в области Peer Settings, задают новый узел в IP-адресе Узла, чтобы быть добавленным полем. *Потом нажмите кнопку Add (добавить).*

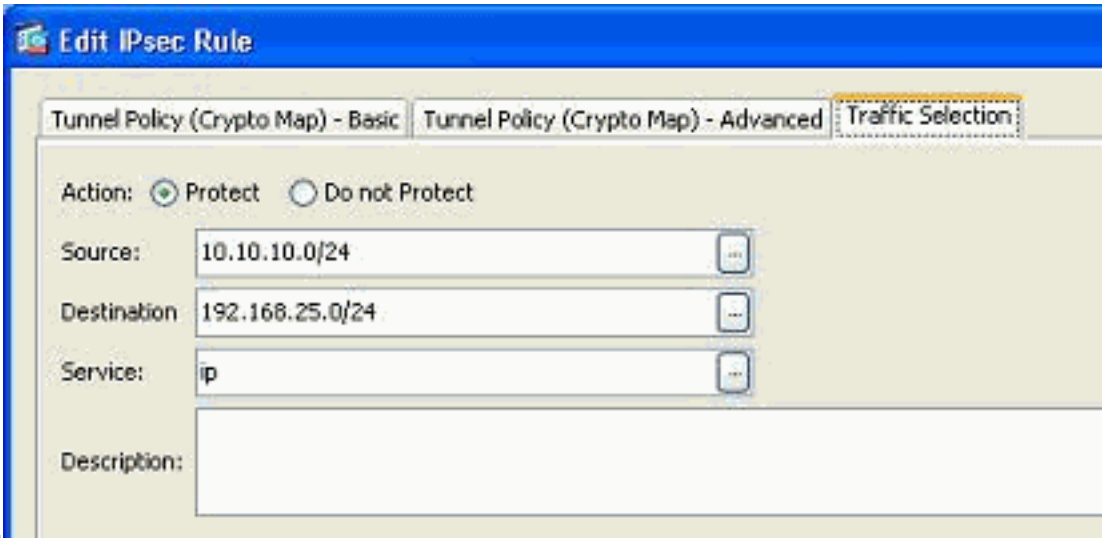


3. Выберите существующий IP - адрес адресуемой точки и нажмите *Remove* для сохранения новых сведений об одноранговом узле сети только. *Нажмите кнопку OK.*



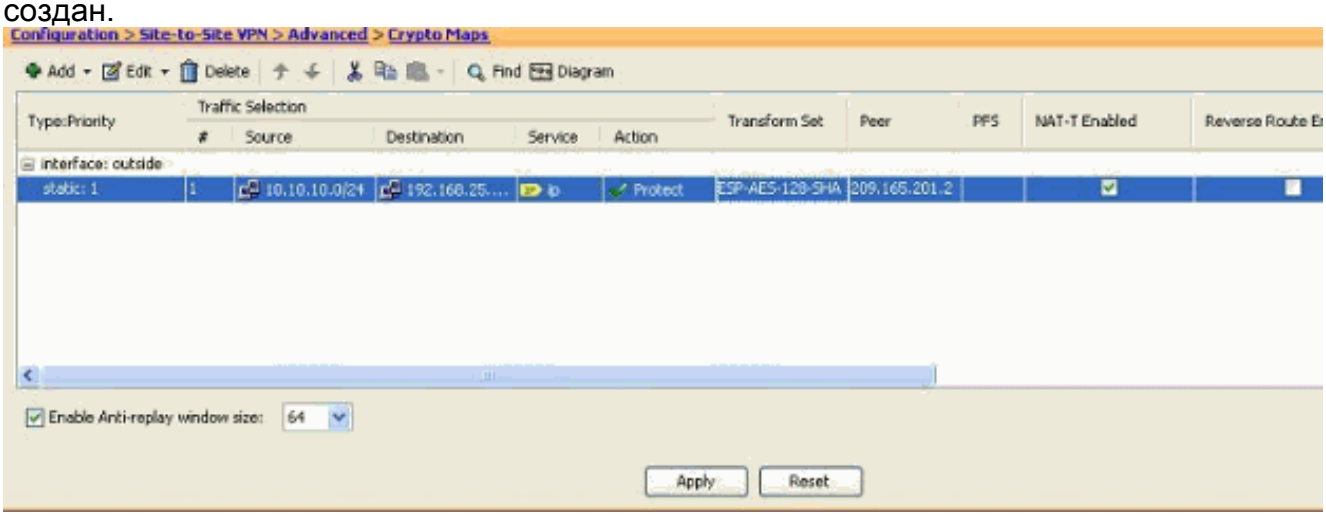
Примечание: После изменения сведений об одноранговом узле сети в текущей криптокарте Профиль подключения, привязанный к этой криптокарте, удален немедленно в окне ASDM.

4. Подробные данные шифрованных сетей остаются тем же. Если необходимо модифицировать их, перейдите к вкладке *Traffic*



Selection.

5. Перейдите к области *Configuration> Site-to-Site VPN> Advanced> Crypto Maps* для просмотра модифицированной криптокарты. Однако эти изменения не имеют место, пока вы не нажимаете *Apply*. После того, как вы нажимаете *Apply*, переходите *к Конфигурации> Сквозной VPN-соединение> Усовершенствованный>* меню *Туннельных групп*, чтобы проверить, присутствует ли связанная туннельная группа или нет. Да, если, то связанный *Профиль подключения* будет создан.



Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- Используйте эту команду для просмотра параметров сопоставления безопасности, определенных для одиночного узла:узел show crypto ipsec sa <IP - адрес адресуемой точки>

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Инициатор IKE, неспособный найти политику: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251

Эта ошибка отображена в сообщениях журнала при попытке изменить узел VPN от концентратора VPN до ASA.

Решение:

Это может быть результатом действий неверной конфигурации, выполненных во время миграции. Гарантируйте, что крипто-привязка с интерфейсом удалена перед добавлением нового узла. Кроме того, удостоверьтесь, что вы использовали IP-адрес узла в туннельной группе, но не название.

Дополнительные сведения

- Узел к узлу (L2L) VPN с ASA
- Наиболее распространенные проблемы VPN
- Страница технической поддержки ASA
- Cisco Systems – техническая поддержка и документация