ASDM 6.4: туннель VPN типа «узел-узел» с примером конфигурации IKEv2

Содержание

Введение

Этот документ описывает настройку сквозного VPN-туннеля между двумя устройствами адаптивной защиты Cisco (ASA) с использованием протокола обмена ключами между сетями (IKE) версии 2. Описывается порядок действий для настройки VPN-туннеля в графическом интерфейсе мастера диспетчера устройств адаптивной защиты (ASDM).

Предварительные условия

Требования

Удостоверьтесь, что Cisco ASA был настроен с базовыми параметрами.

Используемые компоненты

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

- Многофункциональные устройства защиты Cisco ASA серии 5500, работающие под управлением ПО версии 8.4 и позже
- Версия программного обеспечения 6.4 Cisco ASDM и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

IKEv2, усовершенствование к существующему протоколу IKEv1, который включает эти преимущества:

- Меньше обменов сообщениями между узлами IKE
- Методы однонаправленной проверки подлинности
- Встроенная поддержка для Dead Peer Detection (DPD) и прохождения NAT
- Использование Протокола EAP для аутентификации
- Устраняет риск простых cookie антизасорения использования атак DoS

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

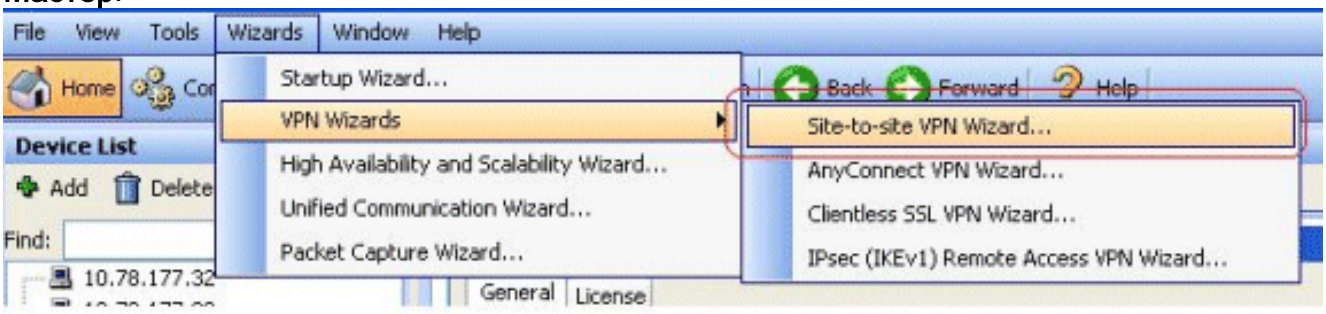
Этот документ показывает конфигурацию туннеля VPN типа «узел-узел» на ASA HQ. То же могло придерживаться как зеркало на BQ-ASA.

Конфигурация ASDM на ASA HQ

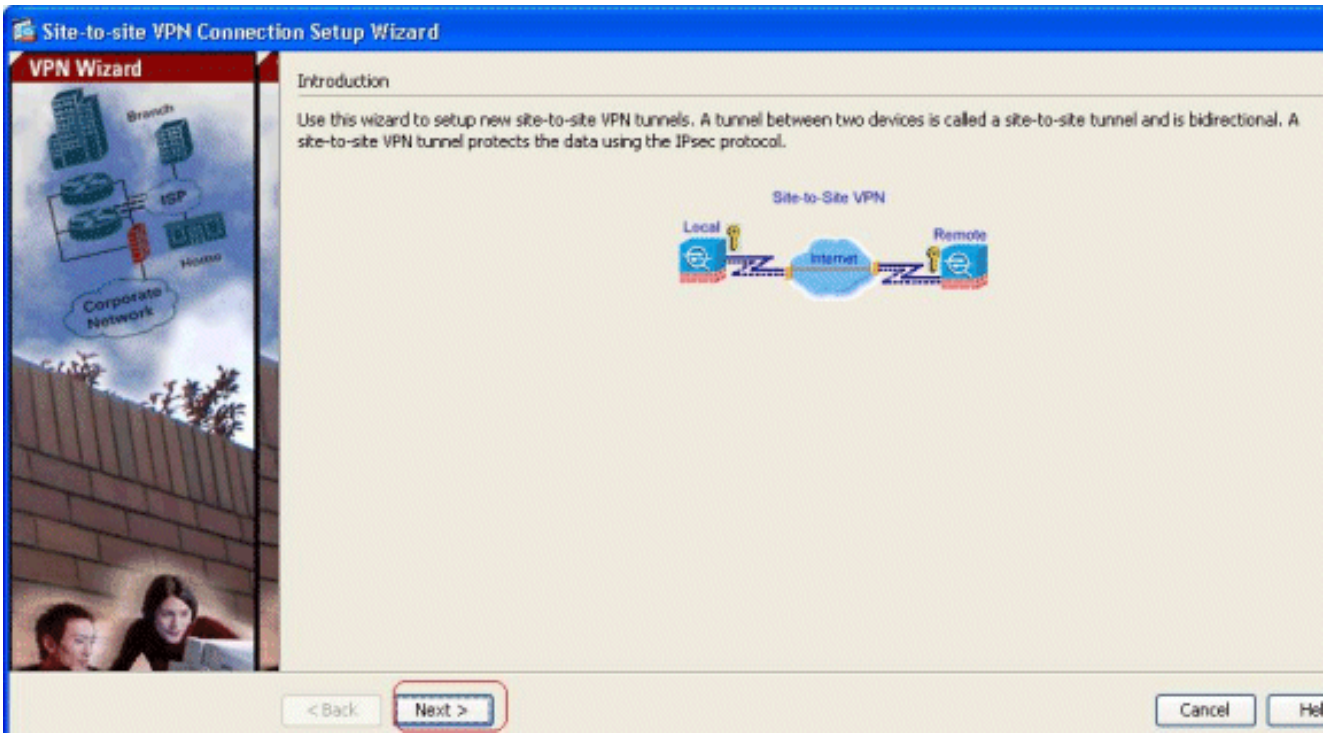
Этот VPN-туннель мог быть настроен с помощью простого в использовании мастера графического интерфейса пользователя.

Выполните следующие действия:

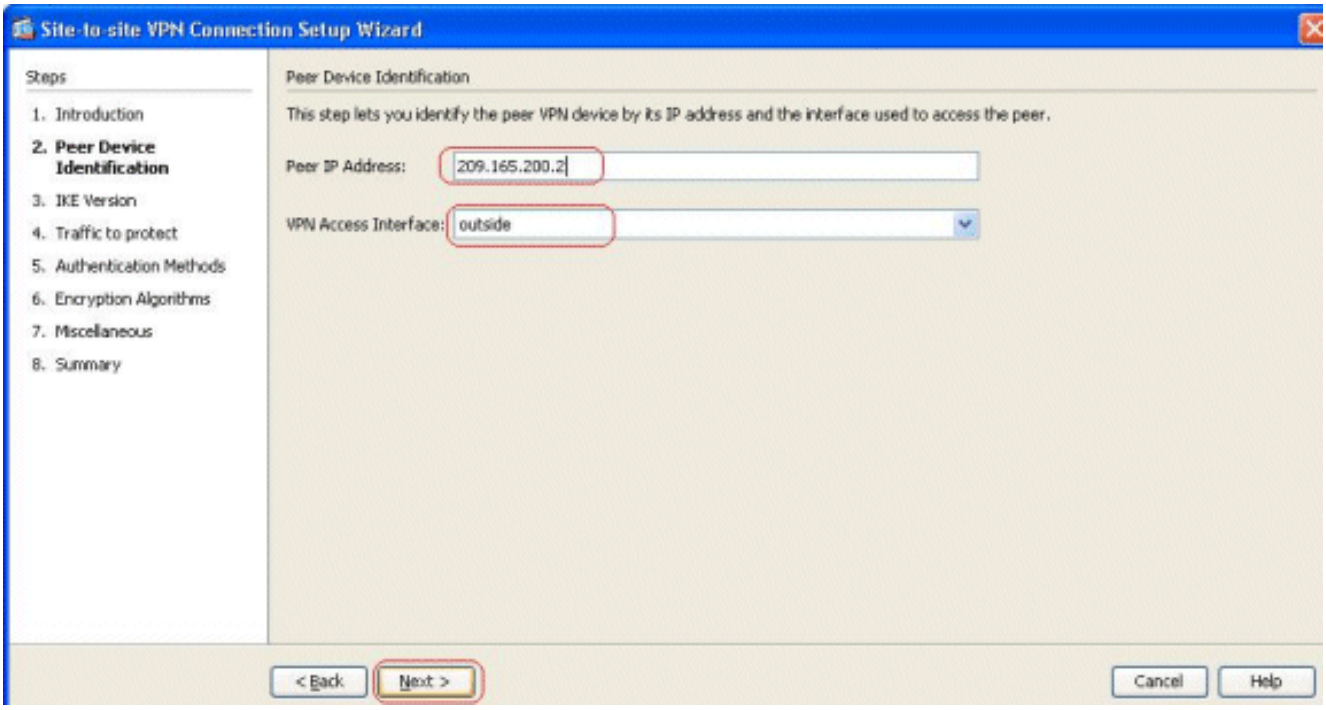
1. Войдите к ASDM и перейдите **к Мастерам> Мастера VPN> Сквозной VPN-соединение Мастер**.



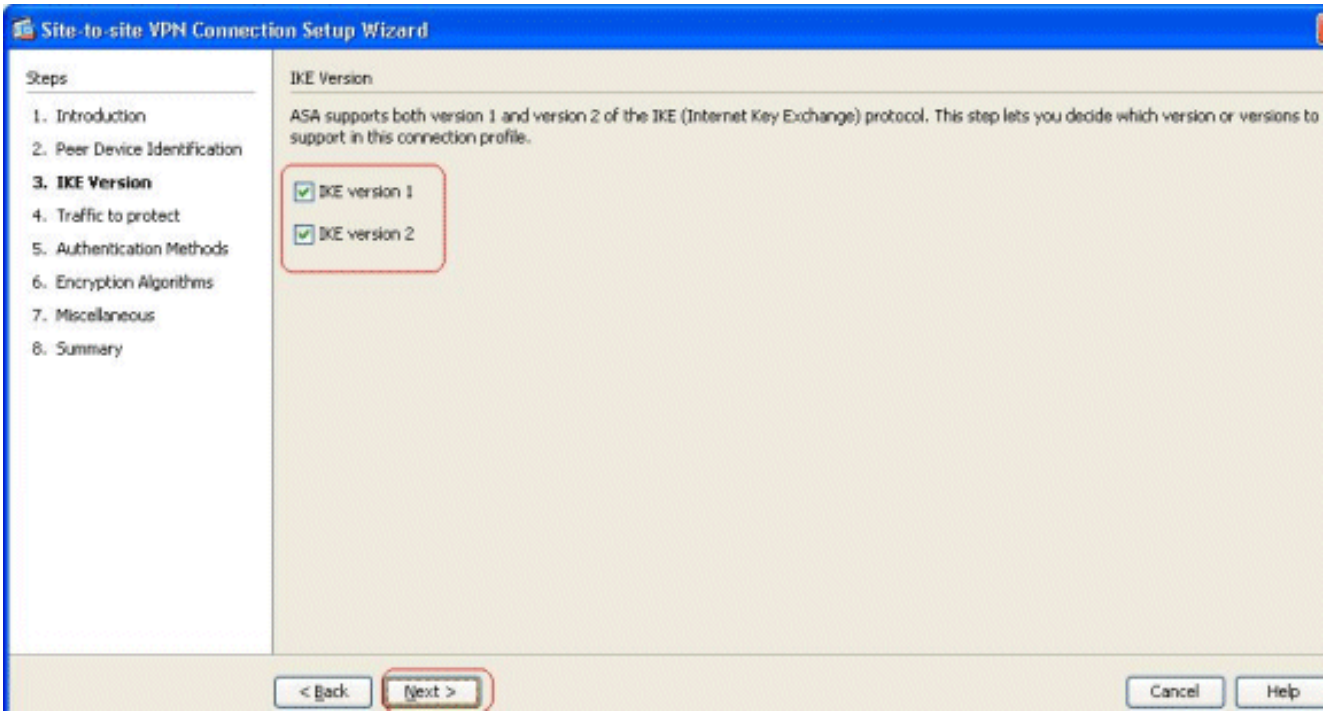
2. Появляется сквозное VPN-соединение окно Настройки подключения. **Нажмите кнопку Next.**



3. Задайте интерфейс доступа VPN и IP - адрес адресуемой точки. **Нажмите кнопку Next.**

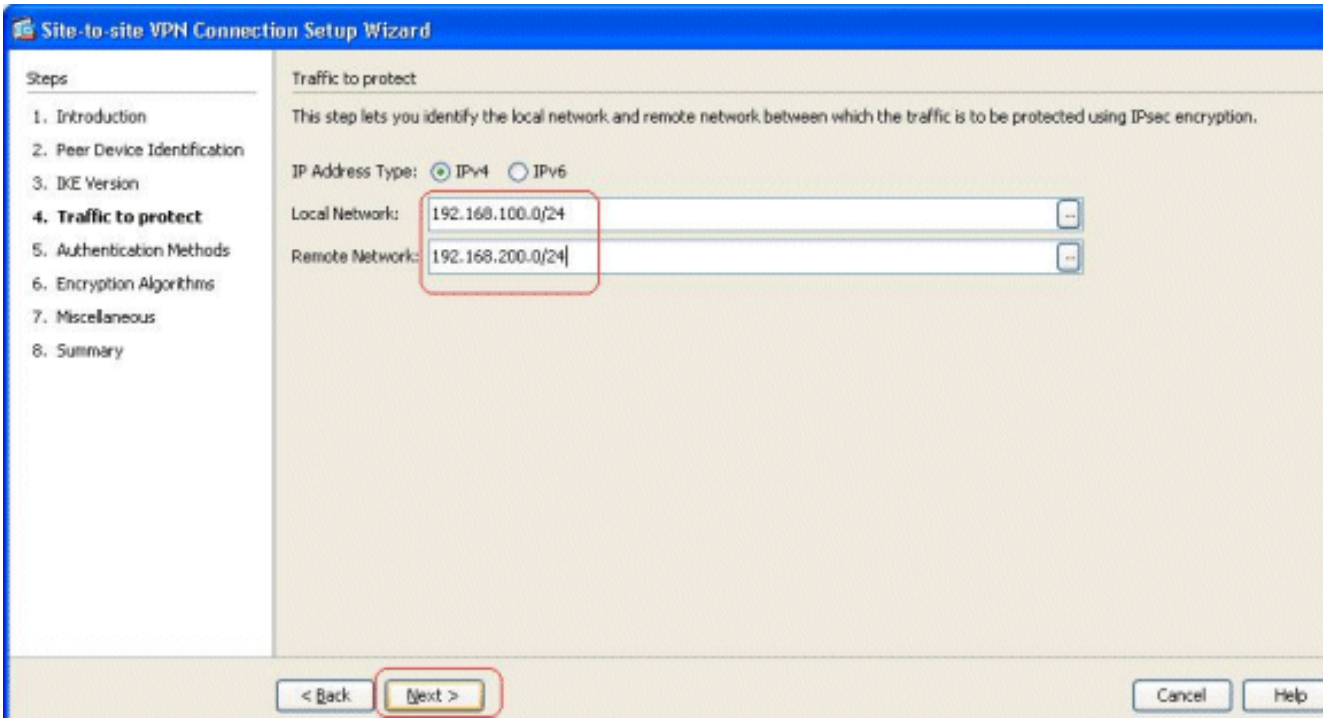


4. Выберите версии IKE и нажмите **Next**.

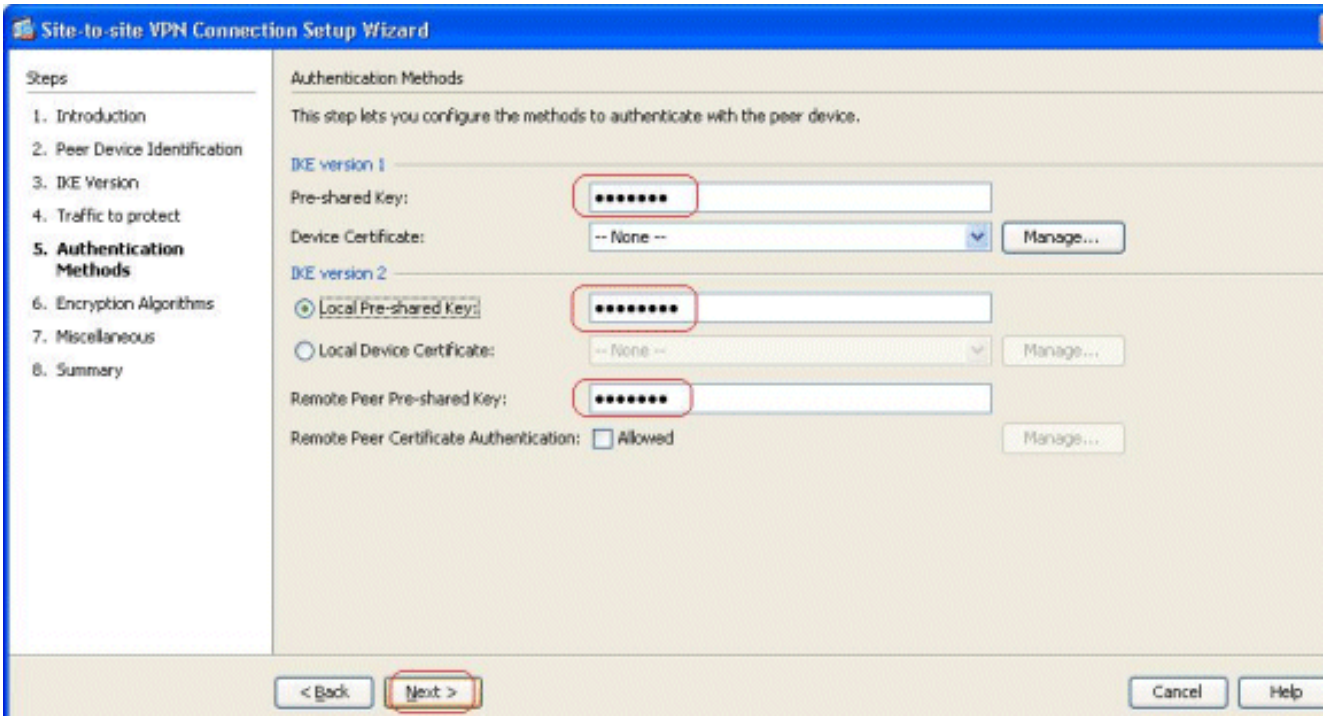


Примечание: Обе версии IKE настроены здесь, потому что у инициатора могла быть резервная копия от IKEv2 до IKEv1, когда отказывает IKEv2.

5. Задайте Локальную сеть и Удаленную сеть так, чтобы трафик между этими сетями был зашифрован и прошелся VPN-туннель. **Нажмите кнопку Next.**

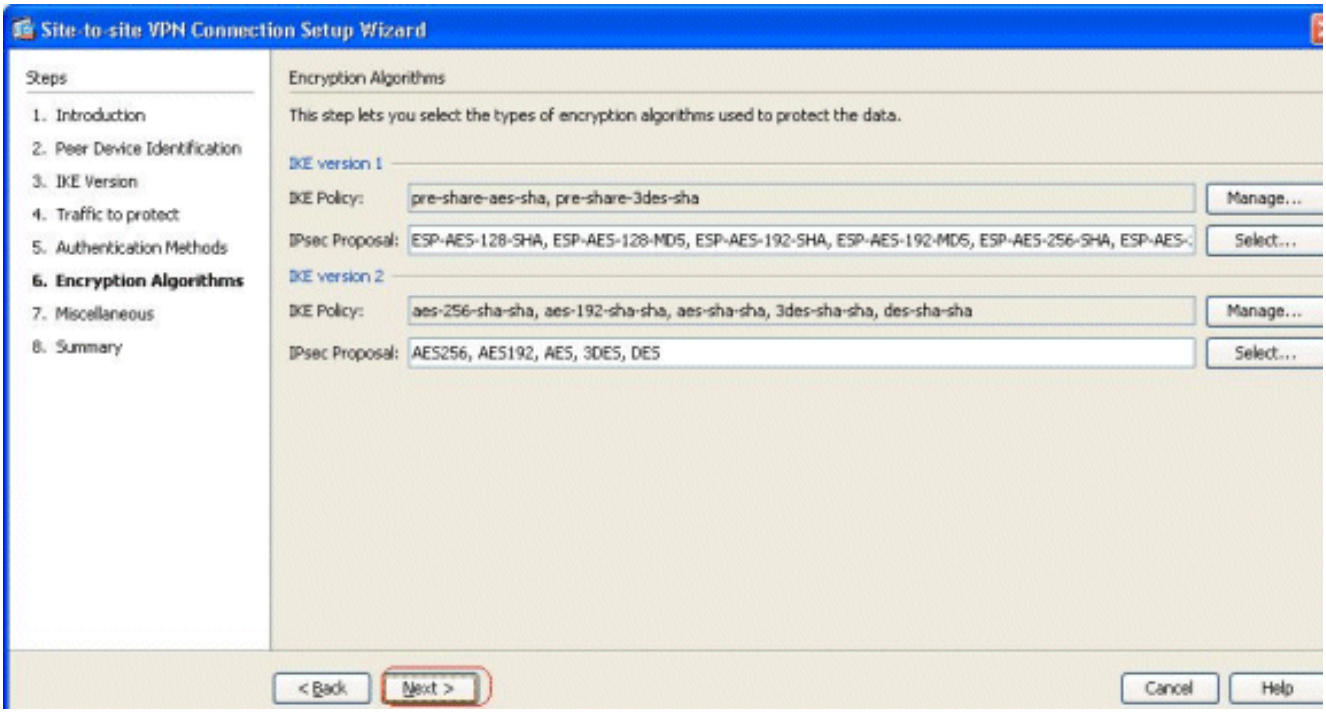


6. Задайте Предварительные общие ключи для обеих версий IKE.

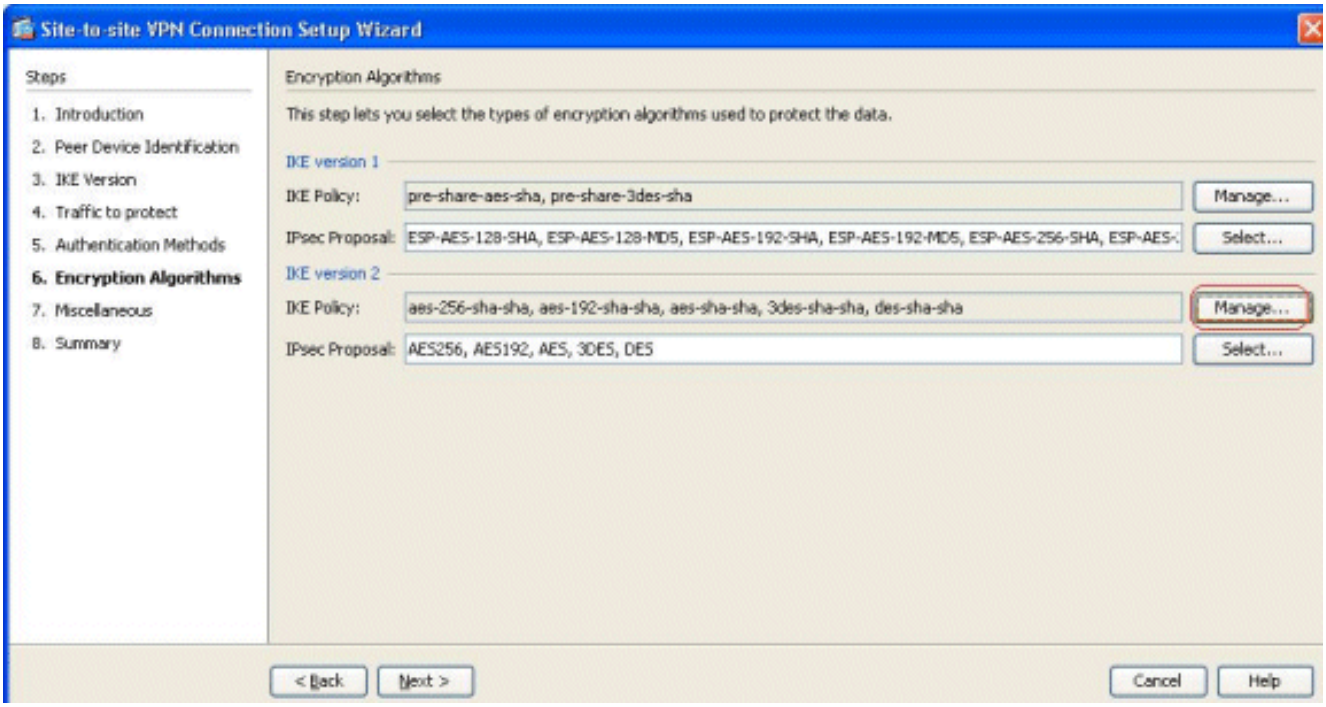


Основное различие между версиями 1 и 2 IKE находится с точки зрения метода аутентификации, который они позволяют. IKEv1 позволяет только один тип аутентификации в обоих концах VPN (т.е. или предварительный общий ключ или сертификат). Однако IKEv2 позволяет асимметричным методам аутентификации быть настроенными (т.е. аутентификация предварительного общего ключа для инициатора, но проверка подлинности сертификата для респондента) использующий отдельные CLI локальной проверки подлинности и удаленной аутентификации.Далее, у вас могут быть другие предварительные общие ключи в обоих концах. Локальный Предварительный общий ключ в конце ASA HQ становится Удаленным Предварительным общим ключом в конце BQ-ASA. Аналогично, Удаленный Предварительный общий ключ в конце ASA HQ становится Локальным Предварительным общим ключом в конце BQ-ASA.

7. Задайте алгоритмы шифрования для обеих версий 1 и 2 IKE. Здесь, значения по умолчанию
приняты:



8. **Щелкните Manage (Управление)...** для изменения Набора правил IKE.



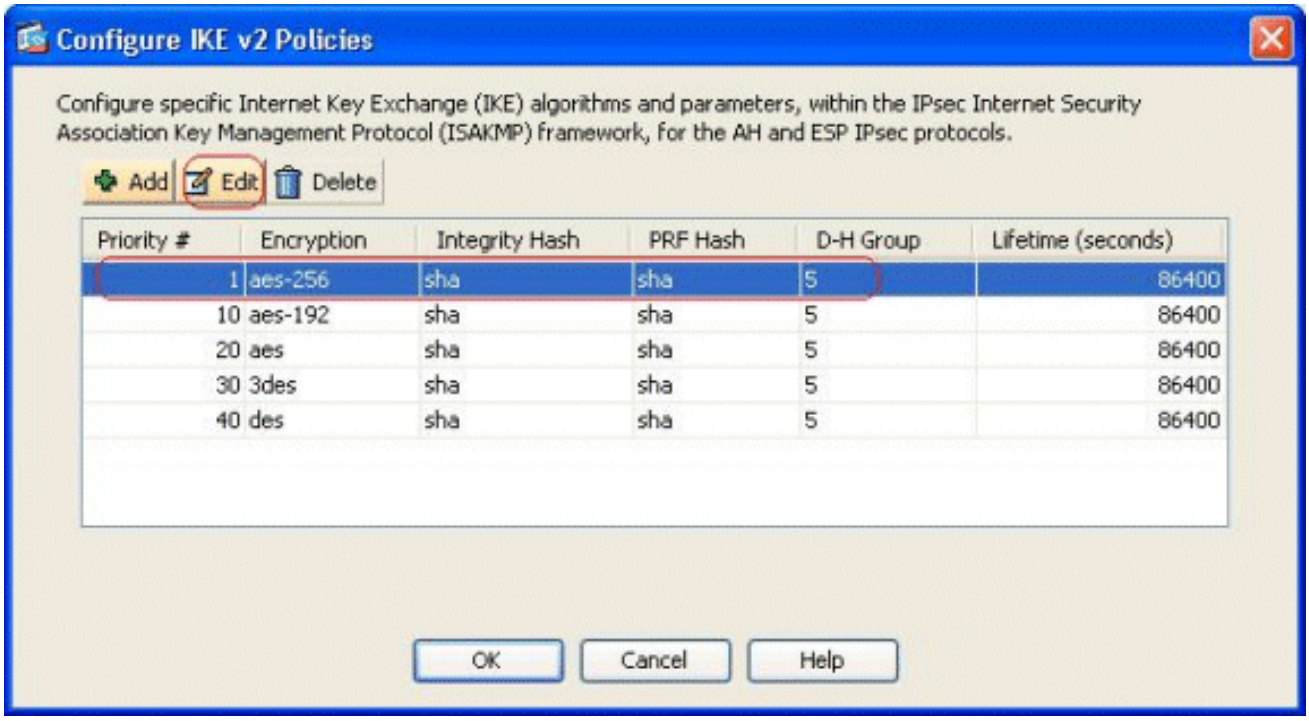
Примечание: Набор правил IKE в IKEv2 синонимичен с **ПОЛИТИКОЙ ISAKMP** в IKEv1.**Предложение по ipsec** в IKEv2 синонимично с **Набором преобразований** в IKEv1.

9. Когда вы пытаетесь модифицировать существующую политику, это сообщение появляется:

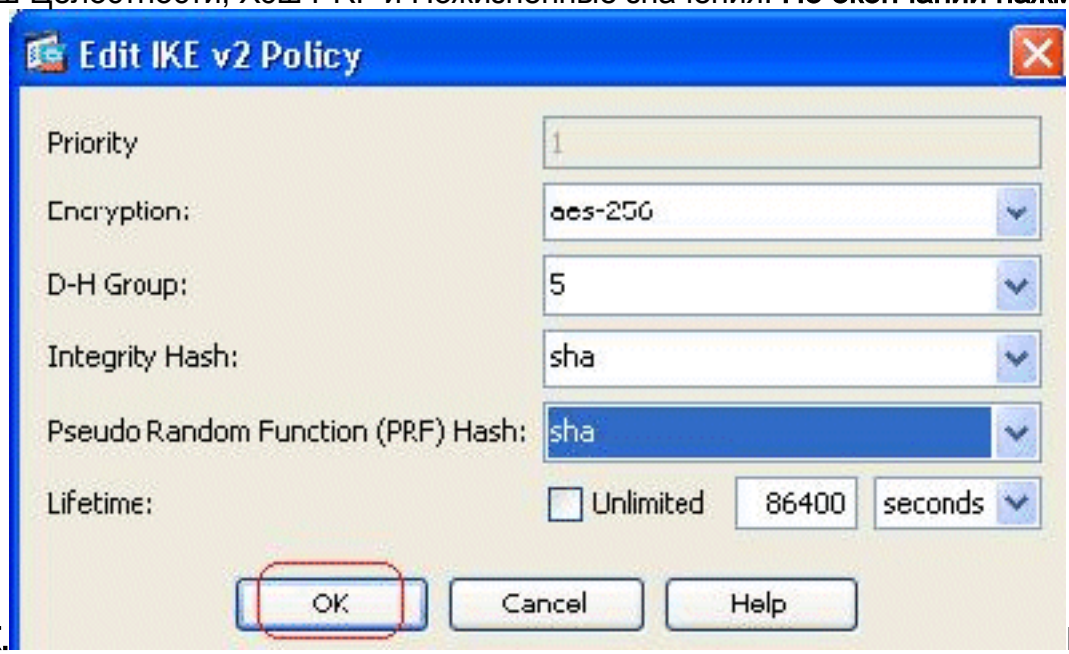
Нажмите **OK** для перехода.

10. Выберите указанный Набор правил IKE и нажмите

Edit.

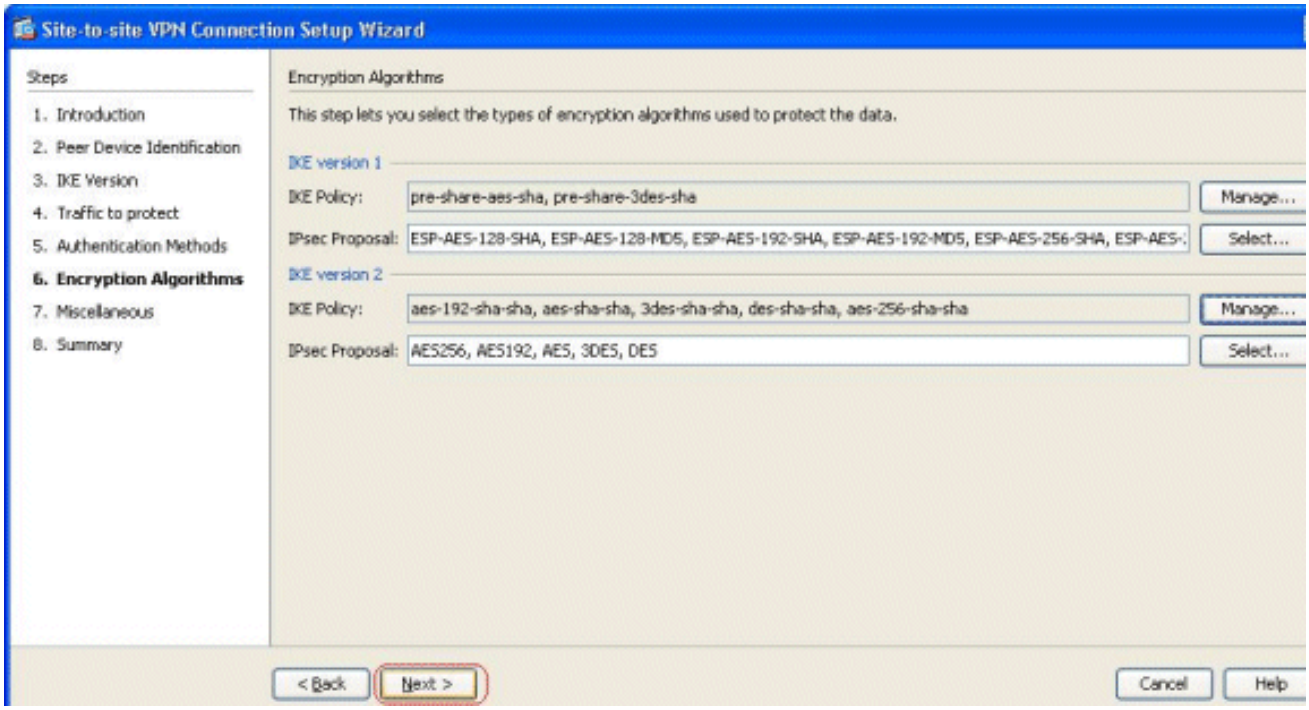


11. Можно модифицировать параметры, такие как Приоритет, Шифрование, D-H Group, Хэш Целостности, Хэш PRF и Пожизненные значения. **По окончании нажмите**

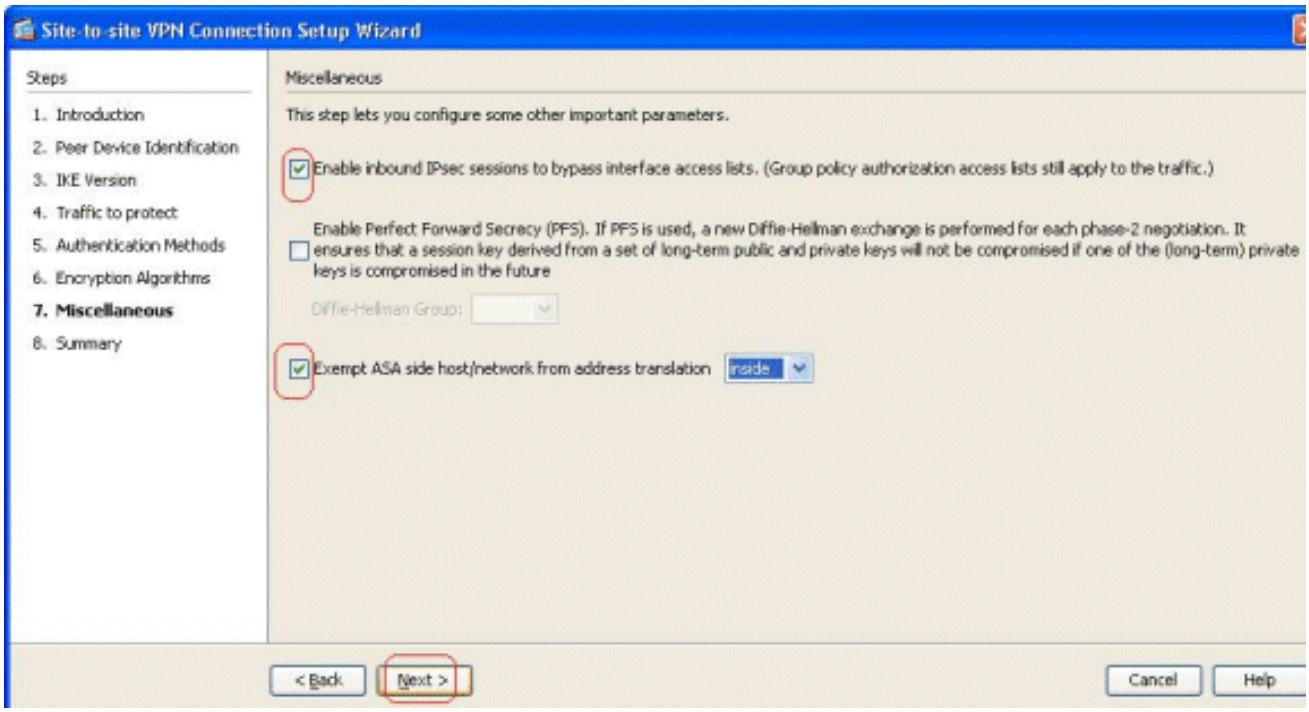


OK. IKEv2 обеспечивает алгоритм Целостности, который будет договорным отдельно от алгоритма Псевдослучайной функции (PRF). Это могло быть настроено в Наборе правил IKE с текущими доступными параметрами, являющимися SHA-1 или MD5.Вы не можете модифицировать параметры предложения по Ipsec, которые определены по умолчанию. Нажмите **Select** рядом с полем IPsec Proposal для добавления новых параметров. Основное различие между IKEv1 и IKEv2, с точки зрения предложений по Ipsec, то, что IKEv1 принимает набор преобразований с точки зрения комбинаций шифрования и алгоритмов аутентификации. IKEv2 принимает шифрование и параметры целостности индивидуально, и наконец делает все возможные комбинации OR из них. Вы могли просмотреть их в конце этого мастера на Итоговом слайде.

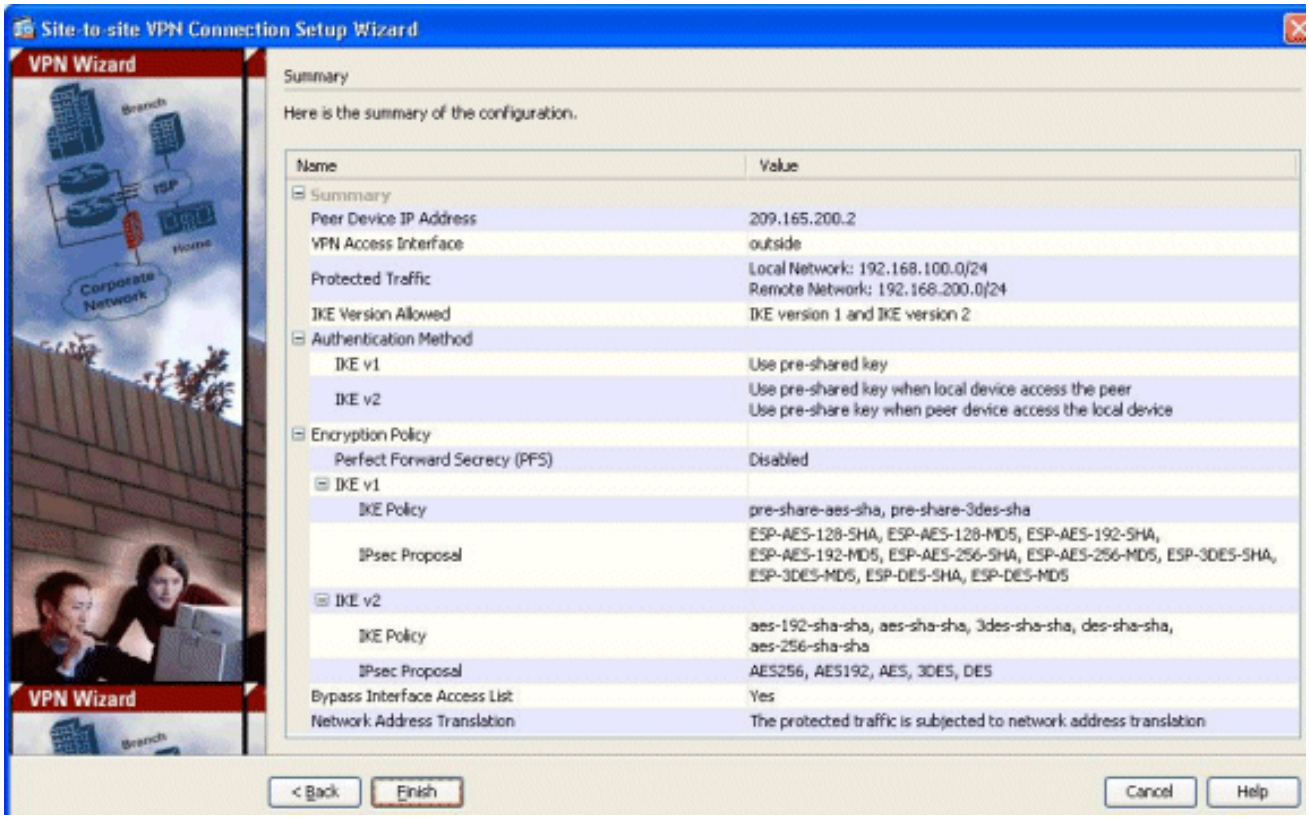
12. **Нажмите кнопку**
Next.



13. Задайте подробные данные, такие как освобождение NAT, безопасная пересылка (PFS) и Интерфейсный Обход ACL. Выберите **Next**.



14. Сводка конфигурации может быть замечена здесь:



Нажмите **Finish** для завершения мастера туннеля VPN типа «узел-узел». Профиль нового соединения создан с настроенными параметрами.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

- **show crypto ikev2 sa** - Отображает базу данных SA во время выполнения IKEv2.
- **подробность покажите vpn-sessiondb l2l** - Отображает информацию о сквозных VPN-соединение сеансах.

Устранение неполадок

Команды для устранения неполадок

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

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug crypto ikev2** - Показывает **сообщения отладки** для IKEv2.

Дополнительные сведения

- Техническая поддержка устройств серии 5500 Cisco ASA
- Cisco Systems – техническая поддержка и документация