Введение.

Вы наверняка слышали термин VPN большое количество раз. Он расшифровывается как Virtual Private Network (Виртуальная частная сеть). Такие сети позволяют создавать частные сети через сеть Интернет, они включают в себя приватность передаваемых данных и туннелирование протоколов, не относящихся к классу TCP/IP.

Такой тип сетей используется по всему миру ежедневно, обеспечивая работу удаленных пользователей и изолированных сетей через общественные сети, таких как Интернет, заменяя при этом более дорогостоящие виды постоянных подключений.

Имена, присвоенные видам таких сетей, базируются на ролях, которые им присущи в бизнесе. Есть три различных категории виртуальных частных сетей:

Remote access VPNs (Виртуальные частные сети удаленного доступа)

Виртуальные частные сети удаленного доступа позволяют удаленным пользователям, сотрудникам, работающим вне офиса получить безопасный доступ к корпоративной сети, где бы они не находились.

Site-to-site VPNs (Виртуальные частные сети между двумя пунктами)

Позволяет компаниям присоединять удаленные офисы к корпоративной опорной сети без особого риска поверх сети Интернет, исключая при этом более дорогостоящие WAN соединения.

Extranet VPNs (Виртуальные частные сети корпоративного доступа**)**

Позволяет организациям поставщикам, партнерам, клиентам соединится с корпоративной сетью в ограниченной форме для обмена бизнес-информацией (B2B, business-to-business).

Теперь вы заинтересованы? Да!? А так как виртуальные частные сети являются недорогими и безопасными, я предполагаю, у вас есть сильная потребность узнать, как создаются виртуальные частные сети. Есть больше чем один способ обеспечить VPN в бытие. Первый подход использует IPSec для создания аутентификации и шифрования между конечными точками по сети IP. Второй путь через туннельные протоколы, что позволяет установить туннель между конечными точками в сети. И тут

становится понятно, что туннель сам по себе является средством для передачи данных или протоколы, инкапсулированные внутри другого протокола!

Прежде чем я объясню суть IPSec, я хочу описать четыре из наиболее распространённых протоколов туннелирования:

Layer 2 Forwarding (L2F, Протокол эстафетной передачи второго уровня)

Является собственным протоколом туннелирования компании Cisco, и это был их первый туннельный протокол, созданный для виртуальных частных коммутируемых сетей (VPDNs, Virtual Private Dial-up Networks). VPDN позволяет устройству использовать модемное подключение для создания безопасного подключения к корпоративной сети. L2F был позже заменен L2TP, который имеет обратную совместимость с L2F.

Point-to-Point Tunneling Protocol (PPTP, туннельный протокол типа «точка-точка»)

Была создан Microsoft, для безопасной передачи данных из удаленных сетей в корпоративную сеть.

Layer 2 Tunneling Protocol (L2TP, протокол туннелирования второго уровня)

Был создан Cisco и Microsoft, чтобы заменить L2F и PPTP. L2TP объединенил возможности двух L2F и PPTP в один протокол туннелирования.

Generic Routing Encapsulation (GRE, протокол общей инкапсуляции маршрутов)

Является еще одним Cisco-протоколом туннельного уровня. Он образует виртуальное соединение типа "точка-точка ", что позволяет различным протоколам, инкапсулироваться в туннелях IP.

Проще говоря, IPSec является отраслевым стандартом набором протоколов и алгоритмов, что позволяет осуществлять безопасную передачу данных через IP-сеть, которая функционирует на уровне 3 сетевом уровне модели OSI.

Вы заметили, я сказал: "IP-сети"? Это действительно важно, потому что сам по себе, IPSec не может быть использован для шифрования не IP трафика. Это означает, что если вы столкнетесь с ситуацией, когда у вас есть для шифрования не IP трафик, вам нужно создать GRE туннель для него, а затем использовать IPSec для шифрования этого туннеля!

Протоколы безопасности

Два основных протокола безопасности, используются в IPSec:

Протокол заголовка идентификации (Authentication Header, AH)

Обеспечивает целостность путём проверки того, что ни один бит в защищаемой части пакета не был изменён во время передачи. Не будем вдаваться в подробности, какая часть пакета защищается и где находятся данные AH заголовка, так как это зависит от используемого типа шифрования и в деталях, с диаграммами описывается в соответствующем RFC. Отметим лишь, что использование AH может вызвать проблемы, например, при прохождении пакета через NAT устройство. NAT меняет IP адрес пакета, чтобы разрешить доступ в Интернет с закрытого локального адреса. Так как пакет в таком случае изменится, то контрольная сумма AH станет неверной. Также стоит отметить, что AH разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путём шифрования содержимого пакета.

Инкапсулирующий протокол безопасности (Encapsulating Security Protocol, ESP)

Инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность. В режиме транспорта ESP заголовок находится между оригинальным IP заголовком и заголовком TCP или UDP. В режиме туннеля заголовок ESP размещается между новым IP заголовком и полностью зашифрованным оригинальным IP пакетом.

Оба протокола - AH и ESP добавляют собственные заголовки, они имеют свой ID протокола, по которому можно определить, что последует за заголовком IP. Каждый тип заголовка имеет собственный номер. Например, для TCP это 6, а для UDP - 17. При работе через межсетевой экран важно не забыть настроить фильтры, чтобы пропускать пакеты с ID AH и/или ESP протокола. Для AH номер ID - 51, а ESP имеет ID протокола

равный 50. При создании правила не забывайте, что ID протокола не то же самое, что номер порта.

Третий протокол, используемый IPSec - это **IKE** или **Internet Key Exchange protocol**. Как следует из названия, он предназначен для обмена ключами между двумя узлами VPN. Несмотря на то, что генерировать ключи можно вручную, лучшим и более масштабируемым вариантом будет автоматизация этого процесса с помощью IKE. Помните, что ключи должны часто меняться, и вам наверняка не хочется полагаться на свою память, чтобы найти время для совершения этой операции вручную.

Создание частной виртуальной сети между двумя пунктами

Есть пять общих шагов в жизненном цикле любого IPSec VPN. Шаги, описанные здесь, применяются специально для виртуальных частных сетей между двумя пунктами, но эти шаги являются, применимы для любых двух конечных точек. Пять шагов создания IPSec VPN:

Шаг 1 Определения полезности трафика, который будет передаваться через туннель

Полезный трафик лучше рассматривать как трафик, который должен быть защищен IPSec VPN туннелем. Когда IPSec VPN туннель работает между двумя сайтами, трафик, который рассматривается, как полезный передается через защищенный VPN туннель на удаленный компьютер. Оказавшись внутри VPN, данные находятся в безопасности, пока не достигнет другого конце туннеля. При условии, что трафик не обнаружен, он не может быть изменен, и не может быть прочитан кем-либо в середине (если работает инкапсулирующий протокол безопасности).

Расширенный список контроля доступа (Extended ACL, access control list) используется для указания направления трафика. Трафик, который направлен или допущен этим списком контроля доступа, соответствует политике безопасности, в свою очередь применим к пакетам, только после этого пакеты проникают в туннель IPSec VPN. Однако, если туннель еще не создан, то приход первого пакета инициирует событие, необходимое для создания туннеля.

Если IPSec туннель уже существует, то трафик, который считается полезным (шаг 1) передается через туннель (шаг 4)

Шаг 2 Первая фаза обмена интернет ключом

Теперь давайте посмотрим, как всё это работает. Установка и поддержка работы VPN туннеля происходит в два этапа. На первом этапе (фазе) два узла договариваются о методе идентификации, алгоритме шифрования, хэш алгоритме и группе Диффи-Хеллмана. Они также идентифицируют друг друга. Всё это может пройти в результате обмена тремя нешифрованными пакетами (т.н. агрессивный режим) или через обмен шестью нешифрованными пакетами (стандартный режим - main mode). Предполагая, что операция завершилась успешно, создаётся SA первой Фазы).

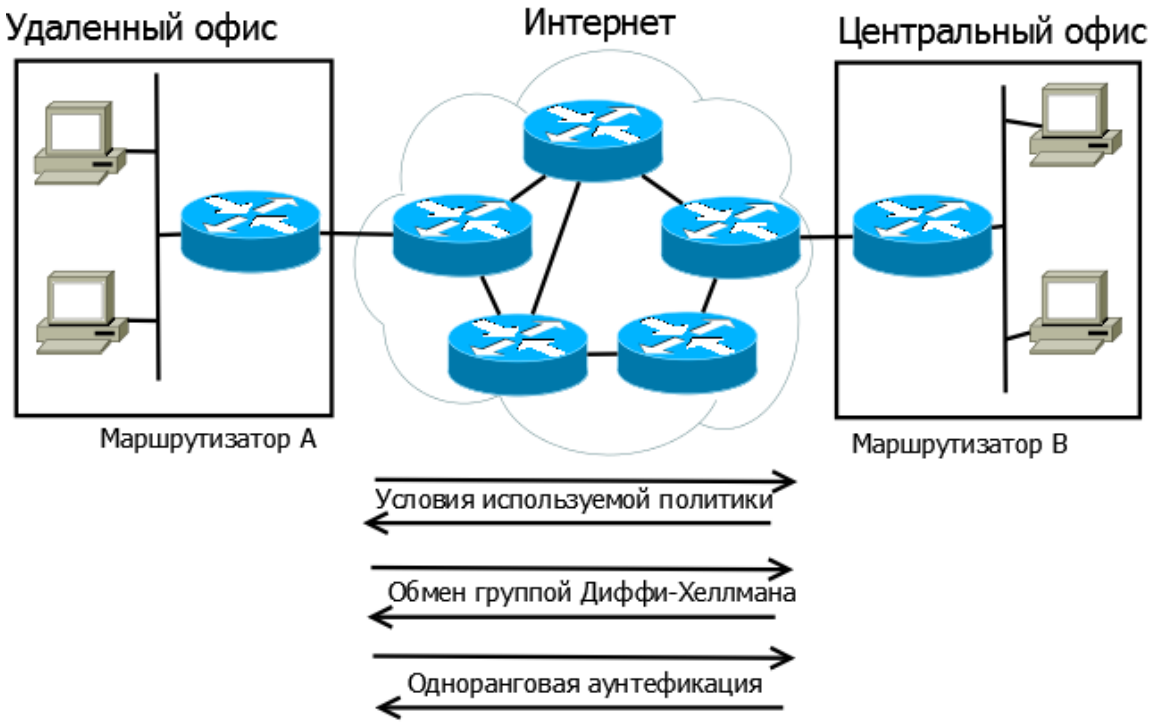


Рис.1 Стандартный режим

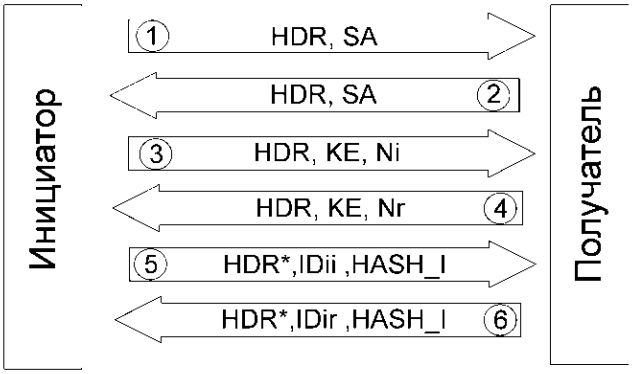


Рис.2 Обмен данными при идентификации IKE с помощью разделяемого ключа в основном режиме фазы 1

Агрессивный режим IKE Фазы 1 уменьшает обмен на три пакета:

Первый пакет идет от инициатора к получателю. Он посылает предложение политики безопасности, открытый ключ Диффи-Хеллмана, в тоже время его подписывают и возвращают для проверки.

Второй пакет идет от получателя обратно к инициатору. Он содержит предложение о принимаемых политиках безопасности, открытый ключ, подписанный для проверки подлинности.

Последний пакет, пакет подтверждения от инициатора к получателю.

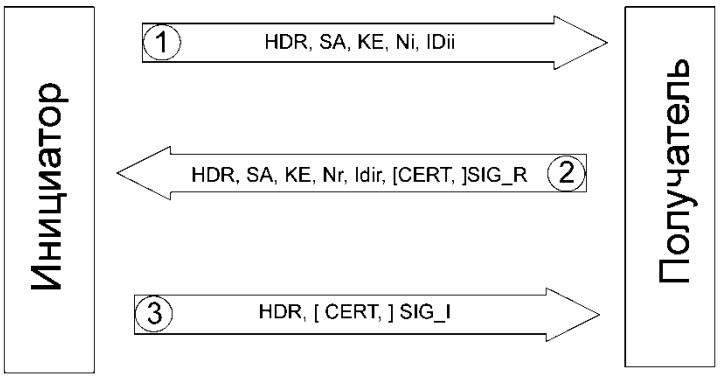


Рис.3 Агрессивный режим IKE фазы 1

Преобразования набора IKE (IKE Transform Sets)

В протоколе обмена интернет ключами, многочисленные индивидуальные параметры должны быть скоординированы. Вместо того, чтобы вести переговоры с каждой из них в отдельности, различные комбинации параметров безопасности сгруппированы в группы преобразование, также известные как IKE политики. Администраторы, как правило, создают эти политики на оконечных устройствах. Всегда две конечные точки ведут переговоры о параметрах безопасности, которыми они обмениваются IKE политики. Если у пары устройств есть общая политика (общий набор параметров безопасности), то настройка IPsec VPN может быть продолжена. Если нет единого набора параметров между двумя устройствами, создание IPsec VPN туннеля не происходит.

Есть пять параметров, которые должны быть согласованы в течение фазы 1 IKE:

- Алгоритм шифрования IKE (DES, 3DES, или AES)
- Алгоритм аутентификации IKE (MD5 или SHA-1)
- Ключ IKE (предварительная аунтефикация - preshare, электронная подпись RSA, случайный тип)
- Группа Диффи-Хеллмана (1,2 или 5)
- Время жизни туннеля IKE (временной или байтовый счетчики)

На рисунке 2, маршрутизатор A и маршрутизатор B пытаются вести переговоры об условиях используемой политики. Предположим, что маршрутизатор A начинает переговорный процесс. Маршрутизатор посылает два вида IKE политики, 10 и 20, к маршрутизатору B. Изменение одного параметра делает совершенно новую IKE политику.

Когда маршрутизатор B получает два вида политики, он сравнивает содержимое каждой со своими. Это сравнение проводится по местной политики IKE.

В этом примере, IKE политика 10 из маршрутизатора A совпадают с IKE политикой 25 в маршрутизаторе B. В ответ маршрутизатору A придет согласие на использование политики 10 и подтверждение создания IKE SA. Если маршрутизатор B не смог найти никаких точных параметров безопасности, то IKE туннель не будет построен.

Маршрутизатор A и маршрутизатор B нашли общую политику IKE, поэтому IKE SA может быть установлено.

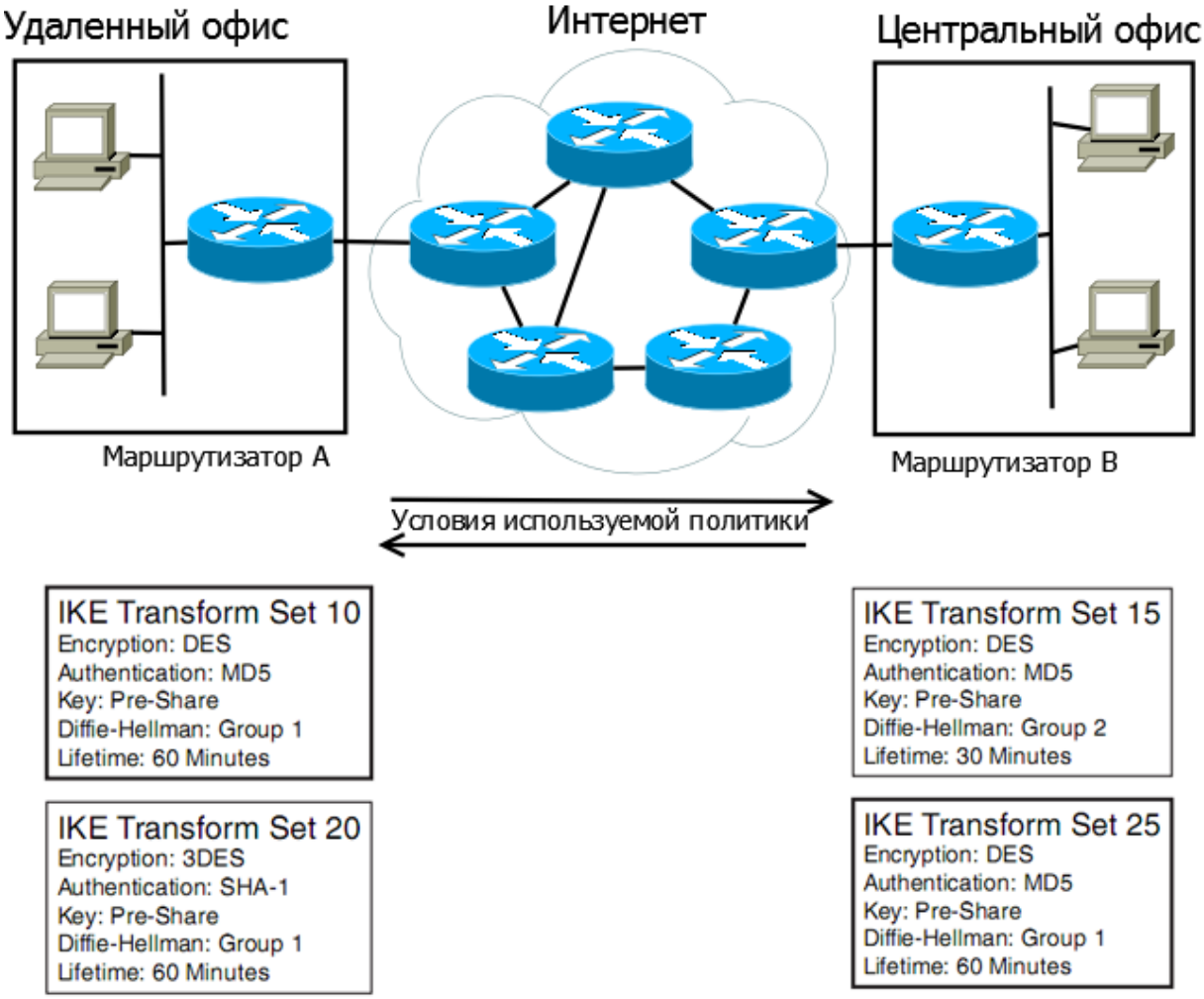


Рис.4

Обмен ключами Диффи-Хеллмана

Есть семь различных групп Диффи-Хеллмана (1-7). VPN устройства Cisco поддерживают только группы 1, 2 и 5, которые используют 768-битное, 1024-битное, и 1536-битное шифрование. Оба IPSec устройства должны договориться о группе Диффи-Хеллмана в преобразование множеств. Как правило, рекомендуется избегать использования группы Диффи-Хеллмана 1 сегодня, хотя группы 2 и 5 вычислительно дороже.

Одноранговая аунтефикация

Существуют три метода используемые для аунтефикации:

- Открытый ключ (Preshared keys)
- Сертификат (RSA signatures)
- RSA-encrypted nonces

Шаг 3 Вторая фаза обмена интернет ключом

На втором этапе генерируются данные ключей, узлы договариваются насчёт используемой политики. Этот режим, также называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются. Такое положение дел усложняет решение проблем в случае неполадок на второй фазе при успешном завершении первой. Правильное завершение второй фазы приводит к появлению фазы 2 SA или IPSec SA, и на этом установка туннеля считается завершённой.

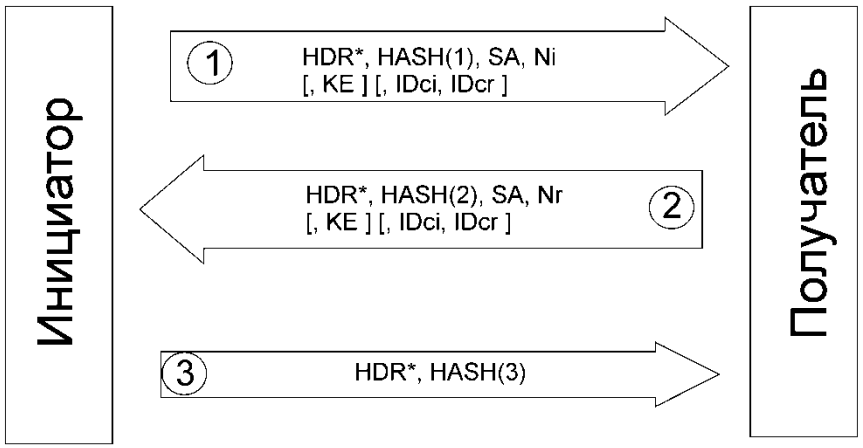


Рис 5

Следующие функции выполняются во второй фазе:

- Переговоры о применяемых параметрах безопасности
- Создание однонаправленных туннелей IPsec (IPsec SAS)
- Перепроверка однонаправленных туннелей для обеспечения безопасности
- дополнительный обмен Диффи-Хеллмана (опция)

Преобразования набора IPsec (IPsec Transform Sets)

Набор преобразований, который описан в контексте IKE политики, является группой атрибутов, которой обмениваются две стороны, поэтому устраняется необходимость в координации и обсуждения отдельных параметров. Разница между IKE преобразованиями и IPsec преобразованиями являются набор атрибутов.

Пять параметров IPSec должны быть согласованы во время быстрого режима между сторонами:

- Протокол IPSec (ESP или AH)
- Тип шифрования IPsec (DES, 3DES, AES или)
- Аутентификации IPsec (MD5 или SHA-1)
- Режиме IPsec (туннель или транспорт)
- Время жизни IPsec SA туннеля (в секундах или килобайтах)

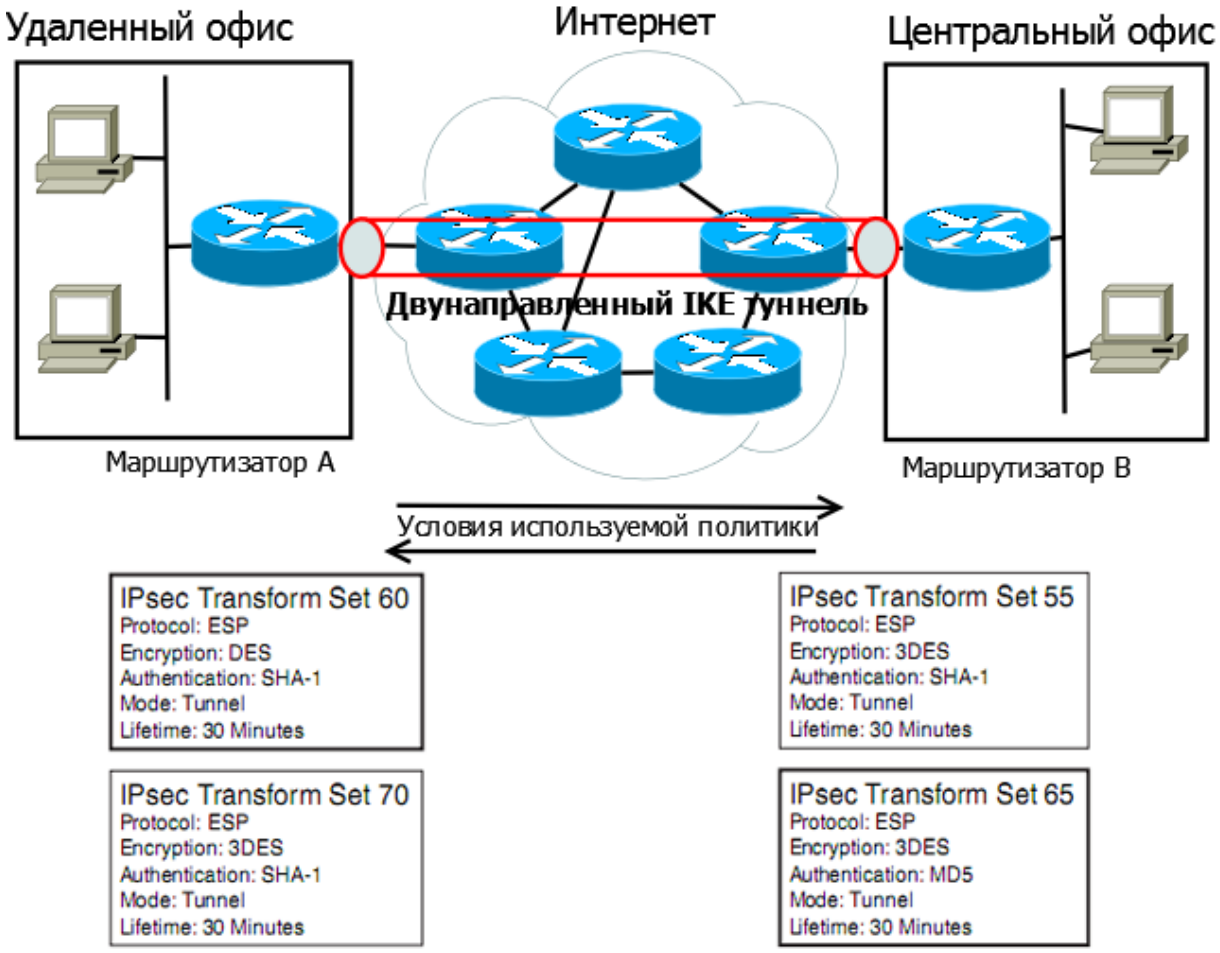


Рис 6

На рисунке, маршрутизатор A и маршрутизатор B пытаются вести переговоры параметров IPsec SA. Предположим, что маршрутизатор входит в IKE фазу 2 переговорного процесса. Маршрутизатор A отправляет маршрутизатор B информацию о двух IPsec наборах преобразований, 60 и 70. Одно изменение любого параметра делает весь набор преобразований отличным от другого. Набор IPsec преобразований может быть использован для сопоставления по многим направлениям, так как нет необходимости создавать идентичные наборы преобразований для каждой конечной точки IPsec туннеля.

Безопасность ассоциаций (Security Associations)

Это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Устройства на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

Каждый SA ссылается на индекс параметра безопасности (SPI, Security Parameter Index). SPI путешествует в каждом пакете IPSec и используется для ведения и подтверждения параметров безопасности по прибытии пакета на конечную точку. Использования SPI устраняет необходимость отправлять параметры безопасности с каждым пакетом IPSec.

Каждый IPSec клиент использует базу данных SA (SAD, SA Database). Помните, что для любого удаленного клиента, будет два SA. База данных SA содержит следующую информацию о каждом IPSec соединения (SA):

- IP адрес получателя (Destination IP address)
- Номер индекса параметра безопасности (SPI number)
- Протокол IPsec (ESP or AH)

Вторая база данных, политика безопасности баз данных (SPD, Security Policy Database), содержит параметры безопасности, которые были

согласованны для каждой SA.

Для каждого SA, эта база данных содержит:

- Алгоритм шифрования (DES, 3DES, or AES)
- Алгоритм аутентификации (MD5 or SHA-1)
- Режим IPsec (туннельный или транспортный)
- Время жизни ключа (секунды и килобайты)

Использование как SAD и SPD позволяет любому клиенту IPSec быстро отслеживать IPSec атрибуты для всех входящих или исходящих пакетов для любого удаленного клиента.

Шаг 4 Безопасная передача данных

После IPSec преобразований SAD и SPD были обновлены на каждом конце, следовательно, трафик может проходить через туннель IPSec. Помните, что не весь трафик разрешен через туннель. Только указанный трафик уходит в туннель. Весь остальной трафик продолжает течь через интерфейс, а не через туннель IPSec VPN.

Шаг 5 Завершение работы IPSec туннеля

Есть два события, которые могут вызвать завершение работы IPsec туннеля. Как упоминалось ранее, если время жизни SA истекает (время и/или число байт), то туннеля должны прекратить свою работу.

Кроме того, можно вручную удалить IPSec туннель. Обычно это делается путем администратором. В большинстве случаев, автоматического прекращение туннеля (из-за истечения времени или использование килобайт) достаточно и администратор не вмешиваться.

ПРАКТИКА

Конфигурирование межсайтового IPSEC VPN

Теперь, когда вы понимаете компоненты межсайтового IPsec VPN настало время для его настройки с использованием Cisco IOS. Как вы уже знаете, есть пять шагов в жизненном цикле IPsec. Однако, не все из этих шагов требует конфигурации. Таким образом, не может быть одинакового количества шагов между IPsec конфигурированием и конфигурацией межсайтового IPsec VPN. Шесть шагов конфигурации IPSec VPN:

- Шаг 1 Настройка политики ISAKMP (IKE фаза 1).
- Шаг 2 Настройка IPSec преобразований (IKE фаза 2, завершение работы туннеля).
- Шаг 3 Настройка шифрования ACL (безопасная передача данных).
- Шаг 4 Настройка криптокарты (IKE фаза 2).
- Шаг 5 Примените криптокарты к интерфейсу (IKE фаза 2).
- Шаг 6 Настройка интерфейса ACL.

Шаг 1 Настройка политики ISAKMP (IKE фаза 1)

Конфигурация политики ISAKMP для IKE Фазы 1, описана ранее. Помните, что фаза IKE 1 устанавливает безопасный двунаправленный туннель, который используется для обмена ключами IPSec SA. В следующем списке приведены параметры настройки фазы IKE 1:

- Алгоритм шифрования IKE (DES, 3DES, AES или)
- Алгоритм аутентификации IKE (MD5 или SHA-1)
- ключ IKE (цифровой подписью, открытым ключом и разделяемым ключ)
- версия ДХ (1, 2 или 5)
- Время жизни IKE туннеля (время и / или количество байт)

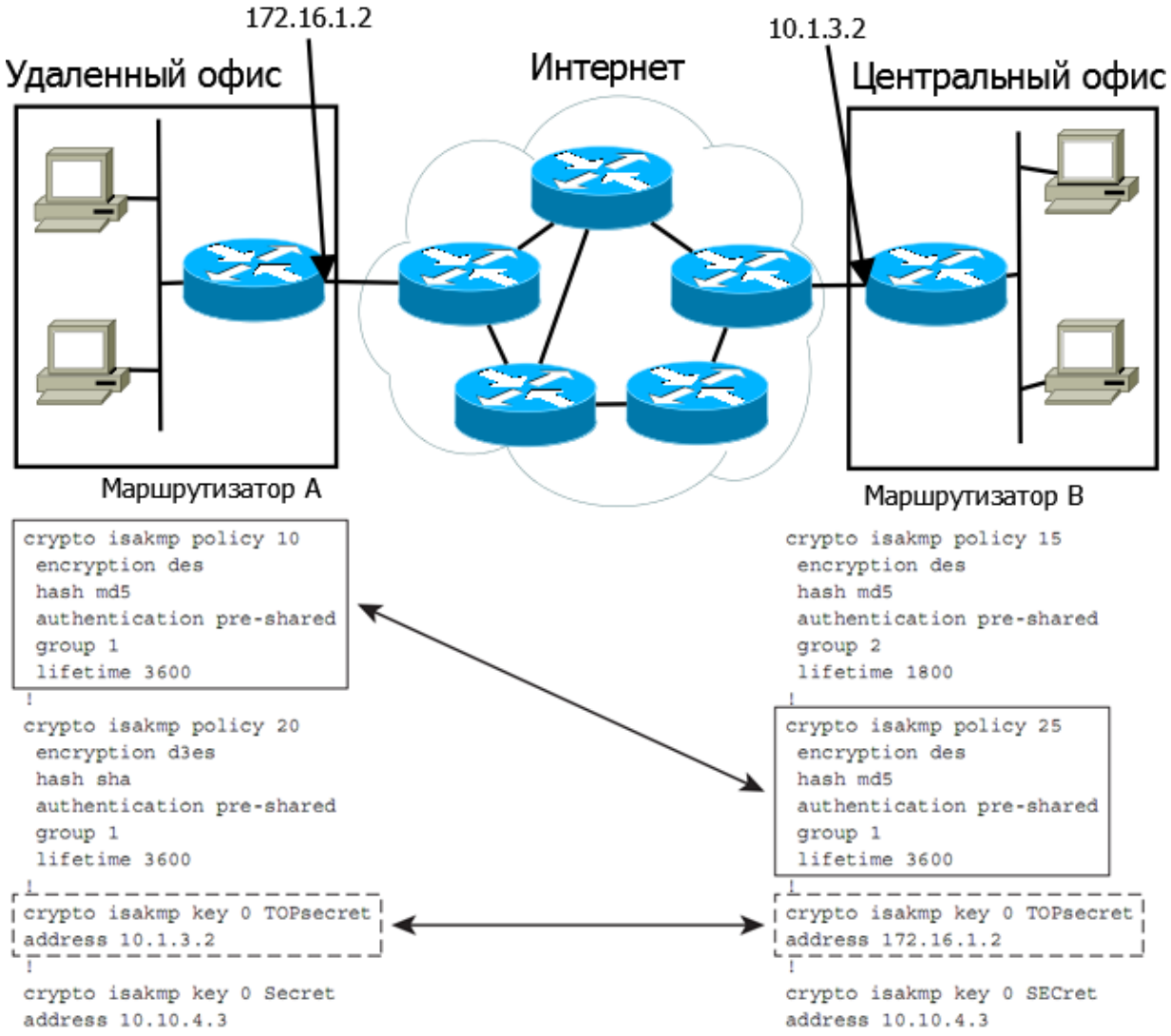


Рис7

Как было показано ранее, параметры безопасности IKE настраиваются с помощью IKE преобразований. Общие параметры IKE, которые были показаны на рисунке 4 теперь настраиваются на рисунке 7. Каждый маршрутизатор имеет две настроенные ISAKMP политики. Поскольку используются, разделяемые ключи, ключи ISAKMP должны быть установлены. Эти политики, передаются в течение фазы IKE 1. Политика 10 маршрутизатора B совпадает с политикой 25 маршрутизатора B и соответствующий ключ (TOPsecret) между двумя сторонами совпадает. Таким образом, безопасный туннель IKE создается с помощью этих атрибутов.

В действительности, более защищенные политики должны быть настроены первыми, поскольку преимущество отдается тем политикам, чьи номера начинаются с меньших порядковых чисел.

Шаг 2 Настройка IPSec преобразований

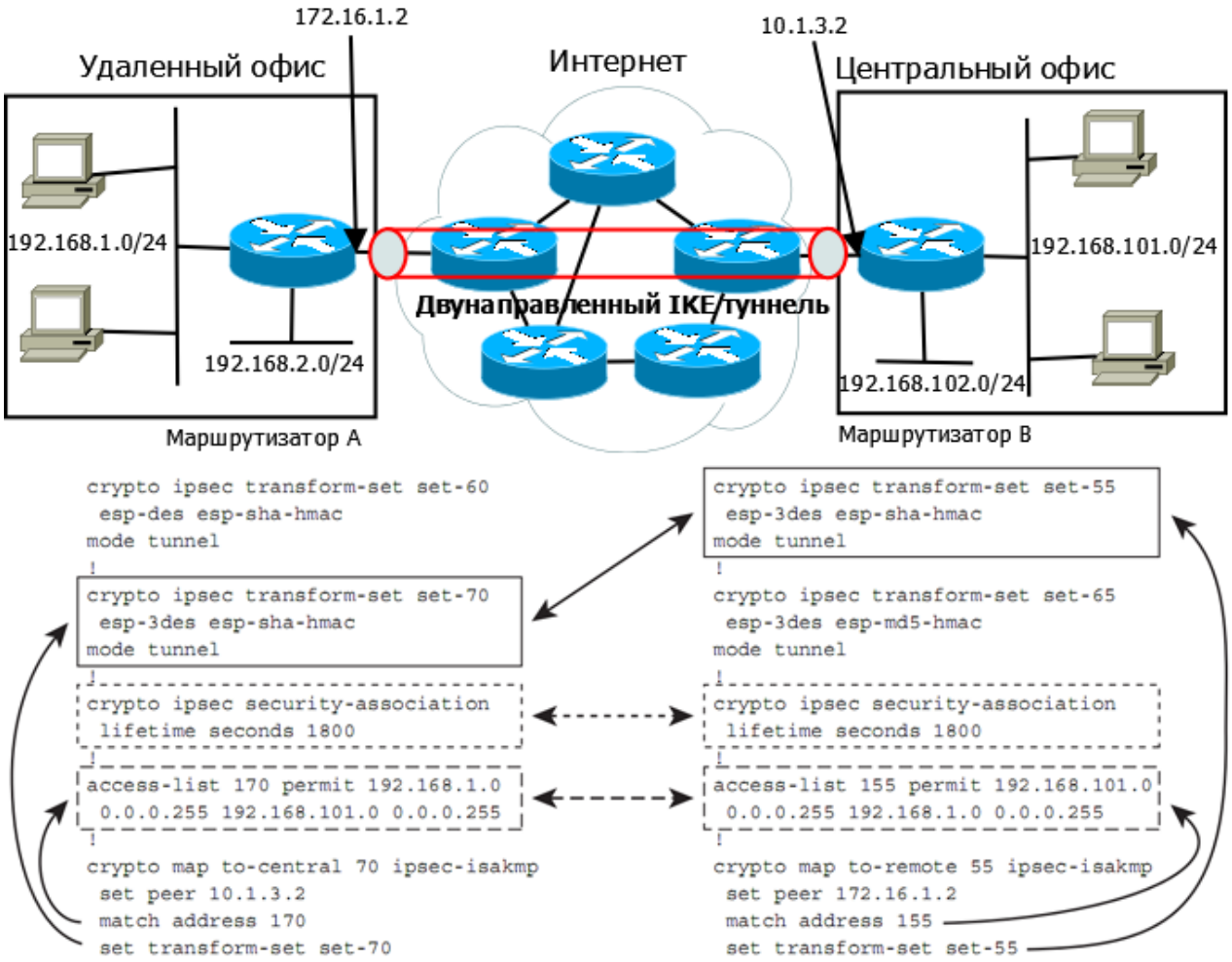
Конфигурирование IPSec преобразований фактически покрывает три шага конфигурирования IPSec показанных ранее. IPSec преобразования, криптокарты, крипто ACL тесно связаны друг с другом. Не возможно говорить об одном исключая другое.

Каждая конечная IPSec точка определяет одно или несколько преобразований. Термины **esp-3des** и **esp-sha-hmac** определены как ESP протокола IPSec, по сравнению с AH.

Таблица 1 показывает соответствие IPSec преобразований для определенного вида сертификации:

Тип преобразования	**Преобразования в IOS**	**Описание**
Преобразования AH	ah-md5-hmac	AH с MD5 аутентификацией
	ah-sha-hmac	AH с SHA аутентификацией
Преобразование шифрования ESP	esp-aes	ESP с 128-bit AES шифрованием
	esp-aes 192	ESP с 192-bit AES шифрованием
	esp-aes 256	ESP с 256-bit AES шифрованием
	esp-des	ESP с 56-bit DES шифрованием
	esp-3des	ESP с 168-bit DES шифрованием
Преобразование аутентификации ESP	esp-md5-hmac	ESP с MD5 аутентификацией
	esp-sha-hmac	ESP с SHA аутентификацией

Команда **crypto ipsec transform-set** используется для выбора AH преобразования, преобразования шифрования ESP, преобразования аутентификации ESP. Только одно IOS преобразование может быть выбрано из каждого класса общих преобразований.



Шаг 3 Настройка Crypto ACL

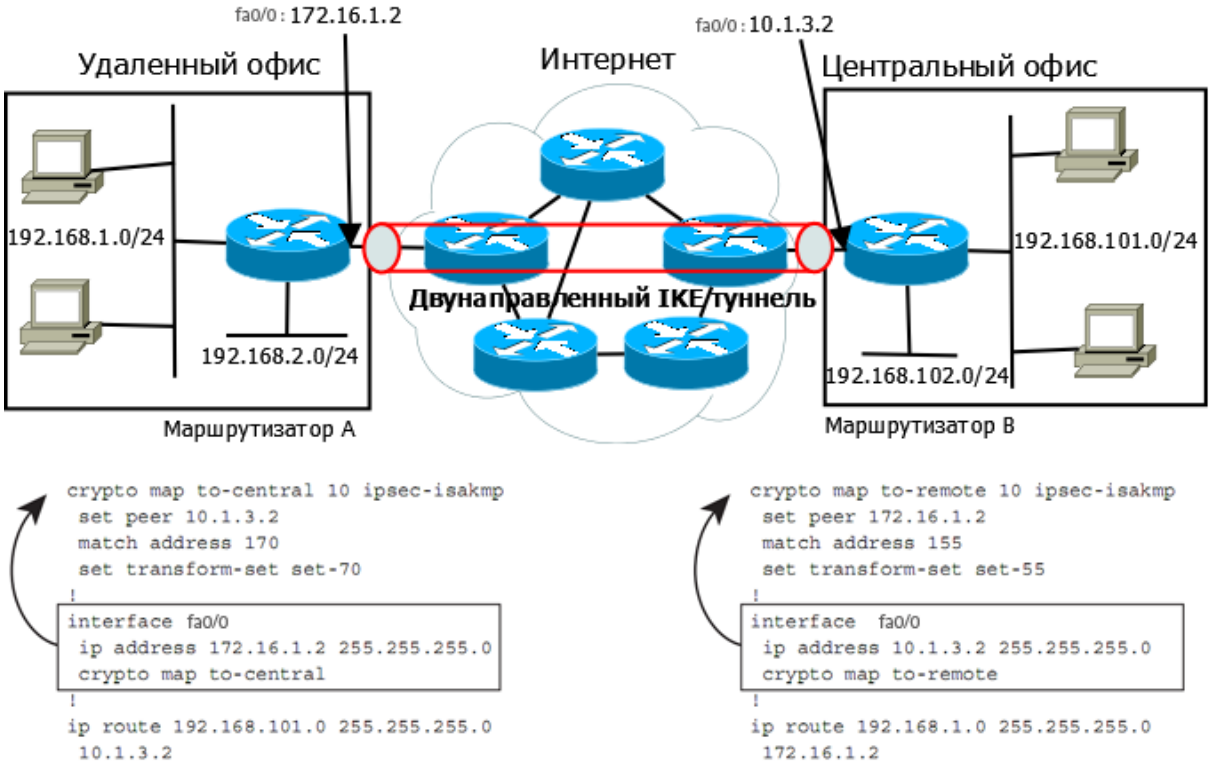
Расширенный список доступа используется для определения движения типа трафика через туннель. Списки доступа показаны штриховой линией. Каждый список определяет адреса источника и назначения трафика, который будет передан через IPSec туннели. Списки доступа должны быть зеркальны. Стандартный список доступа не может быть использован для выявления предпочитаемого трафика, потому что он не имеет возможности указания адреса назначения.

Шаг 4 Настройка крипто карты

Последним шагом в конфигурировании является криптокарта, она связывает наборы преобразований и списки доступа. В удаленном офисе, крипто карта **to-central** создает SA к 10.1.3.2 и защищает любой тип трафика соответствующий списку доступа 170.

Шаг 5 Применение крипто карты к интерфейсу

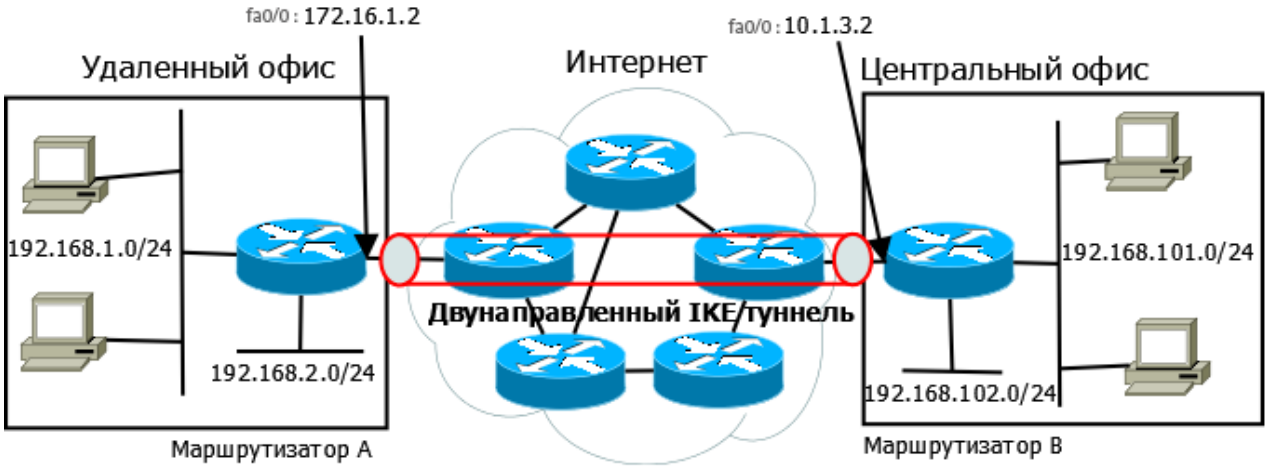
После того как крипто карта успешно настроена она должна быть применена к интерфейсу, для того чтобы началось ее применение. Помните, что крипто карта представляет собой набор IP-адресов из удаленного узла.



Предполагается, что из удаленного офиса все устройства на 192.168.1.0/24 будут общаться с устройствами подсети 192.168.101.0/24 через IPSec VPN. Однако, маршрутизатор A ничего не знает о подсети 192.168.101.0/24. Так статический маршрут добавляется в каждый маршрутизатор.

Шаг 6 Конфигурирование списка доступа на интерфейсах

Вполне вероятно, что интернет-подключение устройств на сегодняшний день будет проходить сквозь брандмауэры. В любом случае, важно, чтобы были разрешены IPSec пакеты так, чтобы IKE и IPSec SA-могли быть установлены.




```
access-list 110 permit ahp host
 10.1.3.2 host 172.16.1.2
access-list 110 permit esp host
 10.1.3.2 host 172.16.1.2
access-list 110 permit udp host
 10.1.3.2 host 172.16.1.2 eq isakmp
!
interface  fa0/0
 ip address 172.16.1.2 255.255.255.0
 crypto map to-central
 ip access-group 110 in
```

```
access-list 120 permit ahp host
 172.16.1.2 host 10.1.3.2
access-list 120 permit esp host
 172.16.1.2 host 10.1.3.2
access-list 120 permit udp host
 172.16.1.2 host 10.1.3.2 eq isakmp
!
interface  fa0/0
 ip address 10.1.3.2 255.255.255.0
 crypto map to-remote
 ip access-group 120 in
```

Примеры

R1

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!

no ip domain lookup
```

```
!

crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco address 10.1.5.2
!
crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
!
crypto map vpn 1 ipsec-isakmp
set peer 10.1.5.2
set transform-set esp-3des-sha
match address 104
!
interface FastEthernet0/0
ip address 10.1.5.1 255.255.255.0
duplex auto
speed auto
crypto map vpn
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 104 permit ip 10.1.5.0 0.0.0.255 10.1.5.0 0.0.0.255
!

control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
!
End
```

R2

```
!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco address 10.1.5.1
!
crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
!
crypto map vpn 1 ipsec-isakmp
set peer 10.1.5.1
set transform-set esp-3des-sha
match address 104
!
interface FastEthernet0/0
ip address 10.1.5.2 255.255.255.0
duplex auto
speed auto
crypto map vpn
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 104 permit ip 10.1.5.0 0.0.0.255 10.1.5.0 0.0.0.255
!
control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
end
```