Мультипротокольные маршрутизаторы NSG

Программное обеспечение NSG Linux

Руководство пользователя

Часть 4

Туннелирование и виртуальные частные сети (VPN)

Версия программного обеспечения 1.0 build 1

Обновлено 14.09.2007

Москва 2007

АННОТАЦИЯ

Данный документ содержит руководство по настройке и применению мультипротокольных маршрутизаторов NSG, оснащенных программным обеспечением NSG Linux. Руководства по применению других продуктов NSG, а также базового программного обеспечения NSG для серий NPS–7e, NSG–500, NX–300 и NSG–800 содержатся в отдельных документах.

Документ состоит из следующих разделов:

Часть 1. Общесистемная конфигурация
Часть 2. Физические порты и службы канального уровня (Ethernet, PPP, Frame Relay)
Часть 3. Маршрутизация и службы IP
Часть 4. Туннелирование и виртуальные частные сети (VPN)
Часть 5. Подсистема X.25

Четвертая часть документа посвящена построению виртуальных частных сетей (VPN) на основе спецификации IPsec. Реализация VPN в устройствах NSG включает современные методы обеспечения целостности данных, защиты от несанкционированного доступа, автоматическое и ручное создание безопасных туннелей через IP-сети общего пользования, а также совместимость с VPN-устройствами других производителей.

Общее описание системы, описание общесистемных параметров и командного языка системы приведены в Части 1. Вопросы настройки физических портов и организации трафика средствами канального уровня (Ethernet bridging, VLAN, коммутация пакетов Frame Relay, организация PPP-доступа) рассмотрены в Части 2. Настройка IP-маршрутизации и связанных с ней служб, а также усовершенствованных механизмов управления IP-трафиком (VPN, QoS и т.п.) описана в Части 3. В Части 5 рассмотрено использование устройств NSG в сетях X.25 и интеграция этих сетей с сетями IP.

ВНИМАНИЕ Продукция компании непрерывно совершенствуется, в связи с чем возможны изменения отдельных аппаратных и программных характеристик по сравнению с настоящим описанием. Сведения о последних изменениях приведены в файлах README.TXT, CHANGES, а также в документации на отдельные устройства.

Замечания и комментарии по документации NSG принимаются по адресу: doc@nsg.net.ru.

ООО «Эн–Эс–Джи»
Россия 105187 Москва
ул. Кирпичная, д.39, офис 1302
Тел.: (+7–095) 918–32–11
Факс: (+7–095) 918–27–39

http://www.nsg.ru/
mailto:info@nsg.net.ru
mailto:sales@nsg.net.ru
mailto:support@nsg.net.ru

§ СОДЕРЖАНИЕ §

Часть 4. Туннелирование и виртуальные частные сети (VPN)

§4.1. Общие сведения о виртуальных частных сетях (VPN)

§4.1.1. Технология построения VPN

Программное обеспечение NSG Linux поддерживает построение виртуальных частных сетей (VPN) при помощи IP-туннелирования на основе спецификации IPsec. Настройка VPN складывается из следующих этапов:

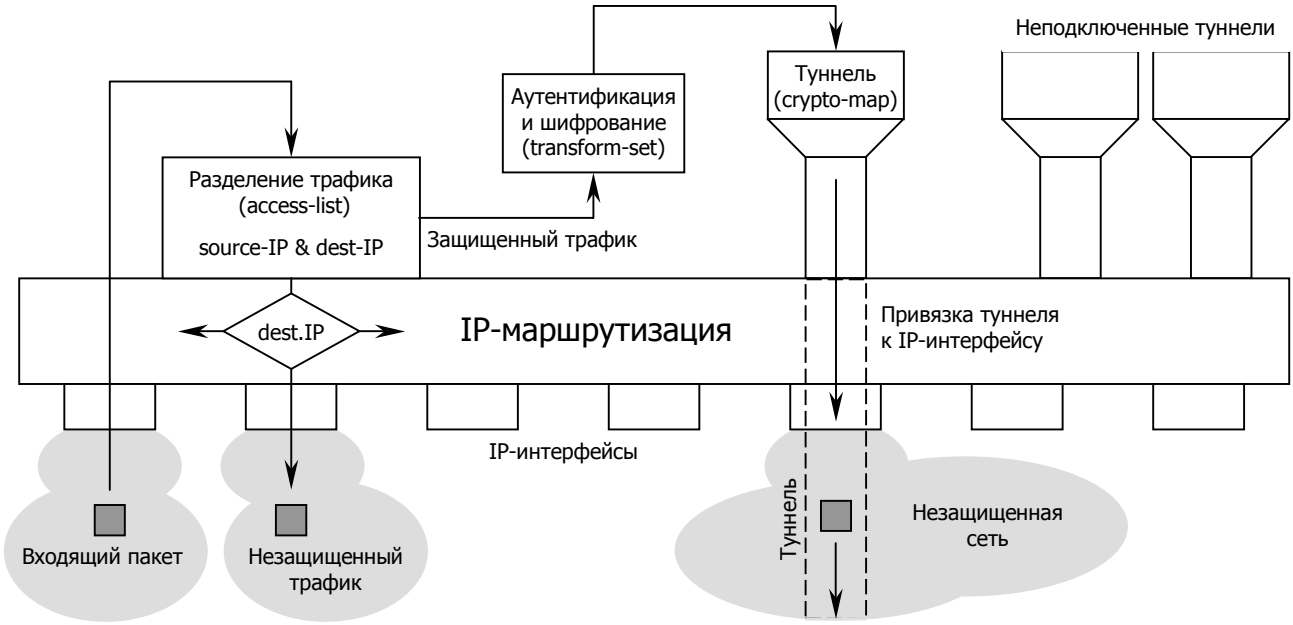
— Определение трафика, который должен быть защищен. Производится с помощью списков доступа (*access lists*), каждый из которых имеет свой уникальный номер.
— Определение правила преобразования для этого трафика. Производится с помощью описаний правил (*transform sets*), каждое из которых также имеет уникальный номер.
— Настройка туннеля для передачи указанного трафика с указанным преобразованием. Совокупность параметров туннеля (*crypto map*) включает номер списка доступа и номер правила преобразования, а также параметры, относящиеся к собственно соединению между двумя шлюзами VPN. Туннель может быть создан одним из двух способов:
  — Постоянно существующий туннель. Для создания постоянного туннеля используется ручное согласование ключей, используемых обоими шлюзами.
  — Динамически создаваемый туннель. Для создания такого туннеля используется процедура автоматического согласования ключей, определенная протоколом IKE (Internet Key Exchange).
— Подключение созданного туннеля к одному из IP-интерфейсов маршрутизатора.

Постоянный и динамически создаваемый туннели имеют следующие отличия:

Постоянный	Динамический
Создается в результате ручного конфигурирования и существует до тех порт, пока не будет удален из конфигурации устройства.	Подготавливается (!) в результате конфигурирования устройства. Создается автоматически по инициативе какой-либо из участвующих сторон (VPN-шлюзов), если на этом устройстве имеется пакет, который должен быть направлен в данный туннель.
Ключи аутентификации и/или шифрования, индекс туннеля (SPI) и правило преобразования выбираются администратором и должны быть строго согласованы (одинаковы) с удаленной стороной.	Ключи аутентификации и/или шифрования, индекс туннеля (SPI) и конкретное правило преобразования выбираются VPN-шлюзами автоматически.
Удаляется из конфигурации устройства вручную администратором. Никакие способы автоматического разрыва туннеля или изменения его параметров (ключи аутентификации и/или шифрования, индекс туннеля) в процессе его работы невозможны.	Созданный туннель может быть разорван любой из участвующих сторон в произвольный момент времени. Разрыв туннеля может происходить, в частности, в следующих случаях: — Истечение установленного времени неактивности; — Истечение установленного срока жизни (по времени или объему переданного трафика); — Вручную по инициативе администратора одного из VPN-шлюзов, при помощи соответствующей команды. После разрыва туннель остается в состоянии готовности и может быть автоматически создан снова по инициативе одной из сторон. После восстановления туннель будет обладать другими параметрами (ключи аутентификации и/или шифрования, индекс туннеля).

Этапы обработки обычного и защищенного трафика в VPN-маршрутизаторе показаны на рисунке на следующей странице. Уместно заметить, что с теоретической точки зрения работа VPN представляет собой расширенный, двухступенчатый вариант маршрутизации, внутрь которого дополнительно вставлено шифрование. Именно, разделение пакетов на трафик VPN и обычный трафик можно рассматривать как статическую маршрутизацию по совокупности IP-адресов источника и назначения; если пакет не подпадает под правила, определенные в *access-list*, то далее к нему применяется обычная маршрутизация по IP-адресу назначения. Защищенный трафик шифруется и передается на вход туннеля; привязка туннеля к IP-интерфейсу есть не что иное, как совокупность двух правил маршрутизации: для исходящих пакетов — фиксированной, для входящих — по номеру интерфейса и IP-адресу источника. Эти два правила являются статическими для постоянных туннелей и динамическими — для динамических туннелей.

ВНИМАНИЕ Весь механизм VPN и структура команд VPN существенно переработаны, начиная с версии NSG Linux 1.0.0 beta 1. Пользователям более ранних версий NSG Linux настоятельно рекомендуется перейти на актуальную версию и при настройке руководствоваться данным документом.



Этапы обработки трафика в VPN-маршрутизаторе

§4.1.2. Поддерживаемые стандарты и спецификации

Технология VPN реализована в устройствах NSG на основании следующих документов IETF:

Архитектура безопасности для протокола IP:

Security Architecture for the Internet Protocol	RFC 2401 (RFC 1825)

Описание протокола AH (Authentication Header):

IP Authentication Header	RFC 2402 (RFC 1826)
Вспомогательные рекомендации:	
IP Authentication using Keyed MD5	RFC 1828
The Use of HMAC-MD5-96 within ESP and AH	RFC 2403
The Use of HMAC-SHA-1-96 within ESP and AH	RFC 2404
HMAC: Keyed-Hashing for Message Authentication	RFC 2104
HMAC-MD5 IP Authentication with Replay Prevention	RFC 2085
The Use of HMAC-RIPEMD-160-96 within ESP and AH	RFC 2857

Описание протокола ESP (Encapsulating Security Payload):

IP Encapsulating Security Payload (ESP)	RFC 2406 (RFC 1827)
Вспомогательные рекомендации:	
The ESP DES-CBC Transform	RFC 1829
The ESP DES-CBC Cipher Algorithm With Explicit IV	RFC 2405
The ESP CBC-Mode Cipher Algorithms	RFC 2451
The NULL Encryption Algorithm and Its Use With IPsec	RFC 2410

Описание протокола IKE Internet Key Exchange):

The Internet Key Exchange (IKE)	RFC 2409
Вспомогательные рекомендации:	
The Internet IP Security Domain of Interpretation for ISAKMP	RFC 2407
Internet Security Association and Key Management Protocol (ISAKMP)	RFC 2408
The OAKLEY Key Determination Protocol	RFC 2412

Взаимосвязь между стандартами и спецификациями:

IP Security Document Roadmap	RFC 2411

Реализация VPN в устройствах NSG совместима с аппаратными и программными решениями других производителей, соответствующей указанным стандартам.

§4.2. Настройка VPN

§4.2.1. Определение трафика, который должен быть защищен (*access list*)

Пакеты направляются в безопасный туннель в том случае, если их IP-адреса источника и назначения находятся в заданных диапазонах. Для такой сортировки трафика в NSG Linux используются расширенные списки доступа (*access lists*) NSG, которые назначаются и удаляются при помощи следующих команд в меню (config-nsg)#:

access-list ext-ip <номер>
no access-list ext-ip <номер>
Создать *access list* и войти в меню его редактирования, и удалить *access list*, соответственно. Номер расширенного *access list* может находиться в диапазоне 100...199 или 2000...2699.

Редактирование списка производится в меню (config-access-...-NN)# при помощи команд:

add <приоритет> { permit | deny } ip <источник> <назначение> ...
Добавить запись в *access list*. Запись относится ко всем IP-пакетам независимо от протокола, инкапсулируемого в IP. При этом параметры <источник> и <назначение> определяют два множества IP-адресов (*source addresses* и *destination addresses*, соответственно), на которые должна действовать данная запись. Оба эти параметра могут быть записаны в одном из следующих форматов:

<ip-адрес> <шаблон>	совокупность базового IP-адреса и шаблона (*wildcard bits)*
host <ip-адрес>	одиночный IP-адрес
any	любой IP-адрес

delete < приоритет>
Удалить запись с заданным номером из *access list*.

description <комментарий>
Ввести текстовое описание (строка) для данного *access list*. Если строка содержит пробелы, она должна быть заключена в кавычки. Максимальная длина описания — 255 символов.

ПРИМЕЧАНИЕ Шаблон адреса (*wildcard bits*) содержит единицы в тех битах, значения которых могут варьироваться. Иногда он называется также *инверсией маски*; однако в общем случае это более широкое понятие, поскольку нулевые/ненулевые биты могут чередоваться в нем произвольным образом. Примеры:
— шаблон 0.0.0.7 соответствует маске длиной 29 бит (255.255.255.248);
— шаблон 0.0.0.3 соответствует маске длиной 30 бит (255.255.255.252);
— шаблон 0.0.0.5 не может быть описан никакой маской (в последнем байте допускается изменение 0 и 2 битов, но не допускается изменение битов 1 и 3…7).

Подробнее о списках доступа см. Часть 3 данного руководства. Пример:

```
access-list ext-ip 151
   add 1 permit ip 11.0.0.0 0.255.255.255 12.0.0.0 0.255.255.255
```

Под данное правило (номер 151) подпадает любой трафик, посылаемый из сети 11.0.0.0 с маской 255.0.0.0 в сеть 12.0.0.0 с маской 255.0.0.0.

ВНИМАНИЕ *Access-list*, предназначенный для отбора трафика в безопасный туннель, может содержать только одну запись. Это принципиальная особенность реализации VPN в NSG Linux. Если требуется защитить трафик для нескольких пар "источник — назначение", то для каждой из них следует создать отдельный *access-list* и отдельную *crypto map* (см. ниже.)

§4.2.2. Определение правила преобразования трафика (*transform set*)

На данном шаге устанавливается тип протокола, который применяется для организации туннеля, вариант используемой аутентификации и размер ключа шифрования. В данной версии NSG Linux реализован только протокол ESP с шифрованием 3DES (с аутентификацией либо без нее). Правила преобразования трафика создаются и удаляются в меню (config-nsg)# следующими командами:

crypto transform-set <имя> esp { 3des-md5-hmac | 3des-sha-hmac }
no crypto transform-set <имя>

Имя правила преобразования — текстовая строка длиной до 15 символов. esp является в данной реализации ключевым словом, поскольку это единственный выбор. Последний параметр определяет только алгоритм аутентификации:

3des-md5-hmac	Шифрование Triple DES (168 бит) с аутентификацией MD5
3des-sha-hmac	Шифрование Triple DES (168 бит) с аутентификацией SHA

Другие алгоритмы туннелирования, предусмотренные IPsec, не поддерживаются ввиду их неактуальности.

§4.2.3. Настройка туннеля (*crypto map, crypto isakmp*)

Процедура создания постоянного туннеля включает в себя: назначение индекса туннеля (SPI) и определение секретного ключа; установку ссылок на соответствующие правило преобразования и диапазон адресов защищаемого трафика; определение IP-адреса конечной точки туннеля (интерфейса маршрутизатора, работающего в паре с данным) и маршрута к нему. Описание туннеля создается и удаляется в меню (config-nsg)# следующими командами:

crypto map <имя> <1...10>
no crypto map <имя> <1...10>

Создать или подготовить туннель с указанными именем и приоритетом (от 1 до 10) и войти в меню его настройки, и удалить туннель, соответственно.

ПРИМЕЧАНИЕ Если некоторый интерфейс устройства является точкой начала нескольких туннелей, то все описания этих туннелей должны иметь одинаковое имя. Все описания туннелей рассматриваются в порядке убывания приоритета. Меньший номер соответствует более высокому приоритету.

ПРИМЕЧАНИЕ Данная версия NSG Linux содержит 4 интерфейса IPsec, на каждом из которых возможно создать до 10 туннелей. Таким образом, максимальное число удаленных узлов, которые могут быть обслужены одним устройством, составляет 40, причем через различные физические интерфейсы или суб-интерфейсы (DLCI, VLAN). Данные ограничения являются временными и могут быть изменены в последующих версиях NSG Linux.

Дальнейшая настройка туннеля осуществляется в подменю (config-crypto-map-XXX)#.

method { ipsec-manual | ipsec-isakmp }

Установить тип создаваемого туннеля:

ipsec-manual	Постоянный туннель с ручным назначением ключей (устанавливается по умолчанию).
ipsec-isakmp	Динамически создаваемый туннель с автоматическим согласованием ключей.

match address <номер access-list>

Определить закрываемый трафик при помощи соответствующего *access-list* (см. п.4.2.1).

set peer <ip-адрес>

Установить IP-адрес маршрутизатора, работающего в паре с данным. Между двумя пограничными маршрутизаторами образуется безопасный туннель через сеть общего пользования, по которому передается закрываемый трафик. Чтобы отменить установленный адрес парного маршрутизатора , следует установить его в значение 0.0.0.0.

set transform-set <имя правила>

Для постоянного туннеля — установить правило преобразования трафика с заданным номером (протокол ESP, шифрование 3DES, аутентификация MD5, SHA либо отсутствует).
Для динамически создаваемого туннеля — установить набор алгоритмов, которые будут предлагаться удаленной стороне (или выбираться из предложенных) при создании туннелей. При этом, если задан туннель без аутентификации, то только такой туннель и может быть установлен. Если задана аутентификация, то два VPN-шлюза выбирают алгоритм MD5 или SHA, исходя из перечней разрешенных алгоритмов и их приоритетов, установленных на каждой из сторон. Если в двух этих списках не найдется ни одного алгоритма, который было бы разрешено использовать обоим устройствам, туннель не будет создан.

set lifetime <120...86400>

Только для динамически создаваемых туннелей: установить ограничение на время жизни туннеля, в секундах. По истечении указанного времени туннель принудительно разрывается и может быть установлен заново по инициативе любой из сторон. После переустановления туннель будет использовать другие ключи шифрования и может получить другой индекс.

set nexthop <ip-адрес>

Установить/отменить IP-адрес следующего маршрутизатора в открытой сети на пути следования туннеля. Именно через него будут отправляться пакеты, принадлежащие к данному туннелю (де-факто при этом создается маршрут к удаленной стороне туннеля с длиной маски 32 бита). Чтобы удалить этот маршрут, следует установить nexthop равным 0.0.0.0.

Параметр является обязательным, если создаваемый туннель должен работать через широковещательный интерфейс (Ethernet, VLAN и т.п.), а удаленный VPN-шлюз находится в другой сети за одним или несколькими маршрутизаторами.

Если удаленный VPN-шлюз расположен в непосредственно подключенной сети, то указание nexthop не требуется.

Если создаваемый туннель должен работать на интерфейсе типа "точка-точка" (например, на PPP-интерфейсе сотового соединения CDMA или GPRS), то nexthop должен быть установлен в значение 0.0.0.0. Вместо него безусловно используется адрес удаленной стороны этого соединения.

Следующие команды относятся только к постоянному туннелю:

set session-key esp <256...4294967295> cipher <ключ-C> authenticator <ключ-A>

Установить параметры для протокола ESP с аутентификацией (т.е. 3des-md5-hmac или 3des-sha-hmac):

<256...4294967295>	Индекс туннеля (Security Parameter Index, SPI)
<ключ-C>	Ключ, используемый для шифрования
<ключ-A>	Ключ, используемый для аутентификации

Все три указанные параметра должны быть установлены одинаковыми на обеих сторонах туннеля.

Правила назначения ключей для постоянного туннеля:

а) SPI и каждый из ключей устанавливаются в одинаковое значение на обоих концах туннеля.

б) Для задания ключа используются шестнадцатеричные цифры 0..9, A..F.

в) Размер ключа, используемого для вычисления хэш-функции при аутентификации (<ключ-A>):
для варианта MD5 — 32 шестнадцатеричные цифры (128 бит)
для варианта SHA–1 — 40 шестнадцатеричных цифр (160 бит)

г) Размер ключа, используемого для шифрования (<ключ-C>) — 48 шестнадцатеричных цифр (используется 168 бит)

ПРИМЕЧАНИЕ Если какой-либо из вышеперечисленных параметров описания туннеля (за исключением set nexthop) не определен, то данное описание туннеля будет неработоспособно, о чем будет сообщено при включении на интерфейсе режима туннелирования (см. следующий параграф).

Для динамически создаваемого туннеля, вместо назначения ключей, необходимо определить динамически же создаваемую ассоциацию безопасности — *security association* (SA). В рамках этой ассоциации осуществляется согласование SPI, ключей, алгоритмов и других параметров создаваемого туннеля между пограничными маршрутизаторами (шлюзами). Ассоциация описывается следующими атрибутами:

— Способ взаимной аутентификации двух сторон. В данной версии NSG Linux поддерживается только механизм разделяемого секрета — *preshared key* (PSK).
— Стойкость шифра для обмена ключами (группа Диффи-Хелмана) — 2 либо 5 (1024 и 1536 бит, соответственно)
— Шифрование — обязательное, 3DES
— Аутентификация — обязательная, SHA–1 либо MD5

При этом единственный параметр, задаваемый на устройстве NSG административно — это собственно PSK (разделяемый секрет). Команда определения PSK для конкретной SA находится в меню конфигурирования (config-nsg)# и имеет вид:

crypto isakmp key <psk> address <удаленный_ip> <локальный_ip>
no crypto isakmp key <psk>

Создать/удалить PSK со следующими параметрами:

<psk>	Произвольный набор символов (строка) — разделяемый секрет. Он должен быть установлен одинаковым на обоих маршрутизаторах.
<удаленный_ip>	IP-адрес интерфейса удаленного маршрутизатора, с которым образуется SA.
<локальный_ip>	IP-адрес интерфейса данного маршрутизатора, который будет участвовать в создании SA.

§4.2.4. Включение и выключение режима туннелирования на интерфейсе

После того, как определены параметры туннеля (постоянного) или правила для его создания (динамического), туннель может быть подключен к некоторому интерфейсу маршрутизатора. Для включения/выключения туннеля необходимо войти в подменю порта, VLAN или DLCI, на котором начинается туннель.

crypto map <имя>
: Включить на интерфейсе режим туннелирования и определить для него все туннели с указанным именем *crypto map*. При этом будут созданы все туннели, определяемые *crypto maps* типа ipsec-manual. Все туннели, определяемые *crypto maps* типа ipsec-isakmp, окончательно подготовлены для создания и будут реально создаваться либо при поступлении данных, предназначенных для отправки в этот туннель, либо по инициативе удаленной стороны.

no crypto map
: Выключить на интерфейсе режим туннелирования. При этом разрываются все существующие на нем туннели — как статические, так и динамические. Кроме того, от интерфейса отключаются также все определенные для него правила создания динамических туннелей. (Однако сами правила при этом сохраняются в конфигурации устройства.)

crypto show
: Показать состояние и статистику всех туннелей (как статических, так и динамических) и SA, установленных на данном порту, VLAN или DLCI.

crypto clear
: Разорвать все SA, установленные на данном порту, VLAN или DLCI. Динамически созданная безопасная ассоциация (SA) может быть разорвана по инициативе любой из участвующих сторон. В дальнейшем она может быть создана вновь.
Данная команда разрыва воздействует только на динамически созданные SA. Туннели, созданные вручную (ipsec-manual) сохраняются до тех пор, пока не будут удалены вручную же командой no crypto map.

Де-факто при подключении туннелей выполняется следующая процедура. Все туннели с одним именем подключены к внутреннему служебному интерфейсу IPsec (таких в системе 4 с именами ipsec0, ...). Обратно, один интерфейс IPsec позволяет определить только одну *crypto map*. Сами по себе эти интерфейсы являются служебными и напрямую средствами основной командной оболочки не настраиваются, но их можно просмотреть командой show interface или средствами ОС Linux. Команда привязывает crypto map интерфейс IPsec к выбранному небезопасному IP-интерфейсу для подключения к внешней сети. Таким образом, одно устройство NSG может обслуживать до 40 удаленных VPN-шлюзов через 4 различных физических интерфейса или суб-интерфейса (DLCI, VLAN) по 10 на каждом.

§4.2.5. Просмотр информации о туннелях

Для просмотра сводной информации обо всех туннелях и безопасных ассоциациях, определенных в устройстве, предусмотрена следующая команда в меню (config-nsg)#:

crypto show Вход в меню просмотра информации IPsec.

Внутри данного узла меню имеются команды:

running Вывести информацию обо всех существующих статических и динамических туннелях и безопасных ассоциациях, в т.ч. о тех SA, в которых в данный момент нет действующих туннелей.

eroute Вывести информацию о маршрутах, уходящих в удаленные сети через безопасные туннели.

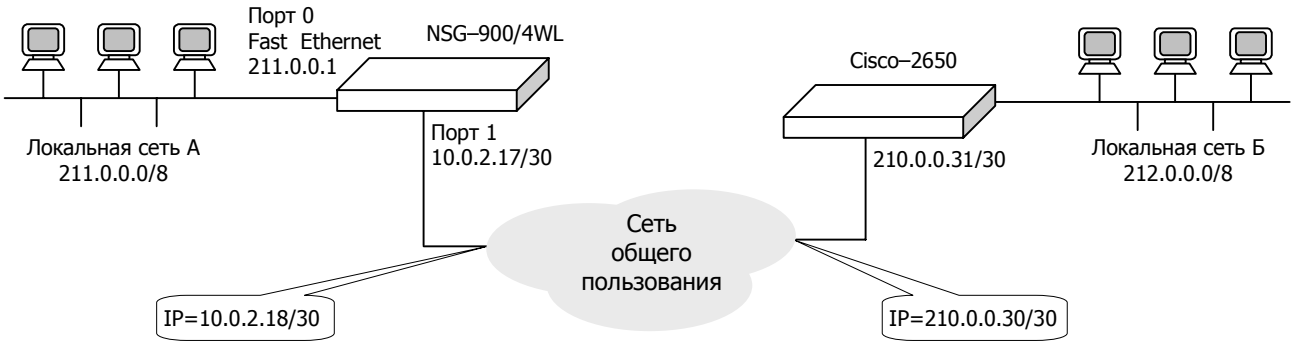
spi Вывести информацию о реально существующих туннелях (статических и динамических) и их индексы (SPI).

tncfg Вывести информацию о соответствии туннелей реальным физическим интерфейсам.

Все перечисленные команды не имеют параметров.

§4.2.6. Пример ручной настройки защищенных туннелей на базе IPSec

Схема стенда показана на рисунке. Стенд состоит из двух пограничных маршрутизаторов, соединенных через сеть общего пользования. Интерфейсы соседних маршрутизаторов в этой сети имеют IP-адреса 10.0.2.18 и 210.0.0.30. Для наглядности на одной стороне используется устройство NSG–900, на другой — Cisco–2650.



Через маршрутизаторы связаны две приватные сети 211.0.0.0/8 и 212.0.0.0/8. Трафик этих сетей передается в безопасном туннеле между интерфейсами пограничных маршрутизаторов NSG–900 (10.0.2.17) и Cisco–2650 (210.0.0.31). При этом весь пакет, включая заголовок, шифруется по алгоритму 3DES (длина ключа 168 бит) и передается как данные в IP-пакете между двумя маршрутизаторами. Дополнительно передается аутентификационный заголовок (вариант MD5), обеспечивающий аутентичность и целостность. На противоположной стороне туннеля данные пакета расшифровываются и передаются в приватную сеть. Весь остальной трафик принимается и отсылается указанными интерфейсами без какой-либо обработки.

Настройка NSG–900

Конфигурирование диапазона адресов, трафик которых нужно отсылать в защищенном туннеле:

```
!
nsg
    access-list  ext-ip 154
        add 1 permit  ip  211.0.0.0  0.255.255.255  212.0.0.0  0.255.255.255
        exit
```

Создание правила преобразования трафика, направляемого и получаемого из туннеля. Выбор механизма аутентификации MD5:

```
        crypto  transform-set  tun4  esp  3des-md5-hmac
```

Описание туннеля. Назначение индекса (SPI) и определение секретного ключа. Установка ссылок на соответствующие правило преобразования и диапазон адресов защищаемого трафика. Определение IP-адреса конечной точки туннеля (интерфейс маршрутизатора, работающего в паре с данным):

```
        crypto  map  tunnel_nsg  1
            method  ipsec-manual
            match  address  154
            set  transform-set  tun4
            set  peer  210.0.0.31
            set nexthop 10.0.2.18
            set  session-key  esp  4000  cipher  11223344556677889900112233445566778899001122334 ↵
4 authenticator  1122334455667788990011223344556677889900
            exit
```

Включение механизма туннелирования на интерфейсе, от которого начинается защищенный туннель:

```
        port  s1
            ip address 10.0.2.17/30
            crypto  map  tunnel_nsg
            exit
        exit
!
```

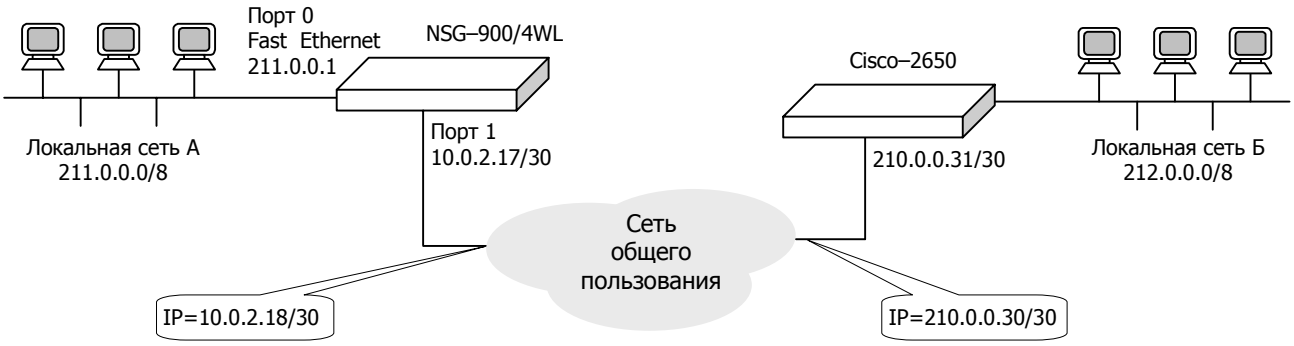
Настройка Cisco–2650

```
!
crypto ipsec transform-set ts4 esp-3des esp-md5-hmac
!
crypto map tunnel_cisco 40 ipsec-manual
    set peer 10.0.2.17
    set session-key inbound esp 4000 cipher 1122334455667788990011223344556677889900112233 44 ↵
authenticator 11223344556677889900112233445566778899001122334400
    set session-key outbound esp 4000 cipher 1122334455667788990011223344556677889900112233 44 ↵
authenticator 11223344556677889900112233445566778899001122334400
    set transform-set ts4
    match address 154
!
access-list 154 permit ip 212.0.0.0 0.255.255.255 211.0.0.0 0.255.255.255
!
interface FastEthernet0/0
    ip address 210.0.0.31 255.255.255.252
    crypto map tunnel_cisco
!
ip route 211.0.0.0 255.0.0.0 10.0.2.17
ip route 10.0.2.17 255.255.255.255 210.0.0.30
!
```

(Строки, начинающиеся от левого поля, являются продолжением предыдущей строки.)

§4.2.7. Пример создания защищенных туннелей на базе IPSec с использованием IKE

Схема стенда показана на рисунке. Стенд состоит из двух пограничных маршрутизаторов, соединенных через сеть общего пользования. Интерфейсы соседних маршрутизаторов в этой сети имеют IP-адреса 10.0.2.18 и 210.0.0.30. Для наглядности на одной стороне используется устройство NSG–900, на другой — Cisco–2650.



Через маршрутизаторы связаны две приватные сети 211.0.0.0/8 и 212.0.0.0/8. Трафик этих сетей передается в безопасном туннеле между интерфейсами пограничных маршрутизаторов NSG–900 (10.0.2.17) и Cisco–2650 (210.0.0.31). При этом весь пакет, включая заголовок, шифруется по алгоритму 3DES (длина ключа 168 бит) и передается как данные в IP-пакете между двумя маршрутизаторами. Дополнительно передается аутентификационный заголовок (вариант SHA–1), обеспечивающий аутентичность и целостность. На противоположной стороне туннеля данные пакета расшифровываются и передаются в приватную сеть. Весь остальной трафик принимается и отсылается указанными интерфейсами без какой-либо обработки.

Настройка NSG–900

Конфигурирование диапазона адресов, трафик которых нужно отсылать в защищенном туннеле:

```
!
nsg
    access-list ext-ip 153
        add 1 permit ip 211.0.0.0 0.255.255.255 212.0.0.0 0.255.255.255
        exit
```

Создание правила преобразования трафика, направляемого и получаемого из туннеля:

```
crypto transform-set tun3 esp 3des-sha-hmac
```

Описание туннеля. Установка ссылки на соответствующие правило преобразования и диапазон адресов защищаемого трафика. Определение IP-адресов конечной точки туннеля (интерфейс маршрутизатора Cisco) и следующего шлюза на этом маршруте (узел 10.0.2.16):

```
    crypto  map  tunnel_nsg  1
        method  ipsec-isakmp
        match  address  153
        set  transform-set  tun3
        set  peer  210.0.0.31
        set nexthop 10.0.2.18
        set lifetime 3600
        exit
```

Определение разделяемого секрета — *preshared key* (PSK). В данном примере разделяемый секрет — строка из двух символов aa.

```
    crypto isakmp key aa address 210.0.0.31 10.0.2.17
```

Включение механизма туннелирования на интерфейсе, от которого начинается защищенный туннель:

```
    port  s1
        ip address 10.0.2.17/30
        crypto  map  tunnel_nsg
        exit
    exit
!
```

Настройка Cisco–2650

```
access-list 153 permit ip 212.0.0.0 0.255.255.255 211.0.0.0 0.255.255.255
crypto ipsec transform-set ts3 esp-3des esp-sha-hmac
!
crypto map M1 3 ipsec-isakmp
    set peer 10.0.2.17
    set transform-set ts3
    match address 153
!
crypto isakmp key aa address 10.0.2.17
!
```

Дополнительно требуется определить *policy* с указанием использования механизма PreShared Key (поскольку *default policy* использует RSA):

```
!
crypto isakmp policy 1
    encr 3des
    authentication pre-share
    group 2
    lifetime 3600
!
```

В заключение конфигурируется IP-интерфейс и маршрутизация:

```
!
interface FastEthernet0/0
    ip address 210.0.0.31 255.255.255.252
    crypto map M1
!
ip  route  211.0.0.0  255.0.0.0  10.0.2.17
ip  route  10.0.2.17  255.255.255.255  210.0.0.30
!
```

§4.3. Особые случаи VPN

§4.3.1. Особенности реализации VPN в устройствах различных производителей

Стандарты и спецификации VPN допускают неоднозначное толкование некоторых деталей. Кроме того, они не определяют некоторые смежные вопросы функционирования устройства. Различные производители могут по-разному интерпретировать эти моменты, и возникающие отличия следует взаимно учитывать при установлении туннелей между их устройствами. В частности, в устройствах NSG имеются следующие особенности по сравнению с реализацией, предлагаемой компанией Cisco Systems.

а) Маршрутизация при использовании туннелей

Данная особенность относится как к статическим, так и к динамически создаваемым туннелям. В маршрутизаторах Cisco наличие туннеля само по себе не оказывает никакого влияния на таблицу маршрутизации. Иначе говоря, помимо создания туннеля, необходимо вручную сконфигурировать маршрут в удаленную сеть, находящуюся на другой стороне туннеля (обычный статический маршрут). Пример конфигурации (фрагмент, непосредственно связанный с маршрутизацией):

```
!
interface FastEthernet0/0
ip address 10.0.0.31 255.0.0.0
!
crypto map test1 1 ipsec-manual
set peer 10.0.2.11
.....
!
ip route 192.168.1.0 255.255.255.0 10.0.2.11
!
```

Здесь 10.0.0.31 — IP-адрес интерфейса Cisco, 10.0.2.11 — IP-адрес удаленного маршрутизатора. Последняя строка означает, что неизвестная для данного устройства сеть 192.168.1.0 с маской 255.255.255.0 находится за точкой 10.0.2.11.

При удалении туннеля (или правила для установления динамического туннеля) следует удалить и статические маршруты, проходящие через этот туннель.

В устройствах NSG, напротив, настройка статических маршрутов в удаленные сегменты приватной сети не является обязательной. При установлении и удалении туннелей автоматически создаются/удаляются и соответствующие записи в таблице маршрутизации.

б) Организация туннеля ISAKMP SA (стадия MAIN MODE) между пограничными маршрутизаторами

1. При инициализации туннеля со стороны NSG предлагается сразу весь (!) пакет предложений, в следующем составе:

   PSK, group5 (1536), 3DES, SHA
   PSK, group5 (1536), 3DES, MD5
   PSK, group2 (1024), 3DES, SHA
   PSK, group2 (1024), 3DES, MD5

2. При получении запроса на установление туннеля список предложений, поступивший от удаленной стороны, поочередно сравнивается в приведенным выше списком. Совпавший вариант отсылается в качестве подтверждения (выбора).
3. В Cisco все варианты туннелей ISAKMP образуют приоритетное множество предложений (*policies*), которые при посылке отсылаются в порядке, определяемом приоритетом *policy*, а при приеме предложений начинают проверяться в соответствии с приоритетом.

в) Организация туннеля IPSEC SA (стадия QUICK MODE) для защищенной передачи трафика

1. При инициализации туннеля со стороны NSG предлагается (или выбирается из предложенных) пакет из двух предложений с использованием Encapsulation Secure Payload (ESP) и обязательной аутентификацией. Выбор варианта MD5 либо SHA–1 оставляется на усмотрение удаленной стороны.
2. В маршрутизаторах Cisco конкретное множество правил преобразования и их приоритет определяются в самом описании crypto-map (тип ipsec-isakmp). Это устанавливается перечислением в параметре

   (config-crypto-map)# transform-set <предложение_1> <предложение_2> <предложение_3> ...

   Если инициатором соединения был удаленный маршрутизатор, то для устройства NSG предпочтительным является алгоритм ESP_3DES + SHA, а если он не предложен удаленной стороной — тогда ESP_3DES + MD5.

§4.3.2. Совместное использование VPN и NAT

При совместном использовании VPN и NAT на одном интерфейсе возникает конфликт между двумя этими механизмами. Типичным примером является подключение офисной сети к Интернет, когда один и тот же интерфейс с единственным реальным IP-адресом используется и для доступа к хостам Интернет, и для установления защищенного соединения с удалённым офисом. Для нормальной работы необходимо исключить пакеты VPN (с номером протокола 50) из числа пакетов, подлежащих преобразованию адресов.

Для Source NAT (IP-маскарадинга) корректная настройка в этом случае имеет вид:

```
!
nsg
    access-list ext-ip 100
        add 1 deny 50 <ip-адрес интерфейса> <ip-адрес удалённого шлюза>
        add 2 permit ip any any
        exit
    port s1
        nat source access-list 100 masquerade
        exit
    !
```

Настройка в аналогичной задаче для Destination NAT (виртуальных серверов):

```
!
nsg
    access-list ext-ip 101
        add 1 deny 50 <ip-адрес удалённого шлюза> <ip-адрес интерфейса>
        add 2 permit ip any any
        exit
    port s1
        nat destination access-list 101 <ip-адрес сервера во внутренней сети>
        exit
!
```

§4.4. Туннелирование протоколов

Программное обеспечение NSG Linux позволяет организовывать туннели для передачи пакетов с одним протоколом через сеть с таким же или другим протоколом. Как правило, в прикладных задачах трафик корпоративной сети туннелируется через сеть общего пользования. Данная версия NSG Linux поддерживает следующие типы туннелей:

— IP-over-IP (GRE)
— IP-over-IP (совместимая с Linux)
— IP-over-PPTP клиент
— Ethernet bridge-over-IP (GRE)
— Generic HDLC-over-IP (GRE)
— IP-over-X.25
— X.25-over-IP

§4.4.1. Туннели GRE и IP-over-IP

Управление туннелями GRE и IP-over-IP производится в меню (config-nsg)# следующими командами:

tunnel ip <1...255>
no tunnel ip <1...255>
Создание/изменение и удаление туннеля с указанным номером, соответственно. Номер туннеля используется только как локальный идентификатор в устройстве NSG и никак не связан с номером, присвоенным этому туннелю на удаленной стороне.

ПРИМЕЧАНИЕ Протокол GRE является самостоятельным протоколом транспортного уровня (в терминах модели OSI), работающим не поверх общеизвестных протоколов TCP или UDP, а параллельно с ними. Идентификатор протокола GRE, указываемый в заголовке IP-пакетов — 47. Для нормальной работы GRE-туннелей в системах с брандмауэрами и фильтрами необходимо разрешить прохождение пакетов IP с данным идентификатором.

Для каждого создаваемого туннеля в системе создается IP-интерфейс с именем вида tuniN. Дальнейшая настройка производится меню туннеля (config-tunnel-N)#. Меню содержит следующие команды:

description "<комментарий>"
Административное описание данного туннеля. Если строка содержит пробелы, она должна быть заключена в кавычки. Максимальная длина описания — 255 символов.

adm-state { up | down }
Административное состояние интерфейса.

destination-ip <ip-адрес>
Адрес удаленной стороны туннеля. В некоторых специальных случаях (при использовании параметра device) адрес может быть не указан, т.е. установлен в значение 0.0.0.0. Это же значение устанавливается по умолчанию.

source-ip <ip-адрес>
IP-адрес, который будет указываться в качестве источника в пакетах, отправляемых в сеть общего пользования. Этот же адрес должен быть указан в качестве назначения в пакетах, получаемых из сети общего пользования и относящихся к данному туннелю.
Если адрес не указан (значение 0.0.0.0, оно же установлено по умолчанию), то в исходящих пакетах в качестве источника указывается адрес того IP-интерфейса, с которого отправляются пакеты. Во входящих пакетах в этом случае в качестве назначения может быть указан IP-адрес любого IP-интерфейса данного устройства NSG; принадлежность пакета тому или иному туннелю (если их несколько) определяется при помощи ключа.

device use {<интерфейс> | none }
Жесткая привязка туннеля к IP-интерфейсу с указанным именем. При этом, если указанный интерфейс отсутствует или находится в состоянии down, то туннель работать не будет.
Если для туннеля не задан destination-ip, то интерфейс должен иметь тип "точка-точка".
Если для туннеля установлено значение device none (оно же установлено по умолчанию), то для него необходимо указать destination-ip. В этом случае выходной интерфейс выбирается согласно текущей таблице маршрутизации.

ПРИМЕЧАНИЕ В качестве транспорта для туннеля может использоваться любой IP-интерфейс, в т.ч. другой туннельный интерфейс, виртуальный многоканальный интерфейс teql, и т.п.

key { use < 0...4294967295> | A.B.C.D | none }

Ключ туннеля — число длиной 32 бита. Для удобства ввода ключ может быть задан как в виде обычного десятичного числа, так и в десятично-точечной нотации. При помощи ключа реализуется слабый метод защиты туннеля, а также выбор туннеля, если их в данном устройстве несколько с совпадающими (или не определенными) IP-адресами.
По умолчанию ключ не задан (установлен в значение none).

Как можно видеть, в общем случае для туннеля должно быть установлено хотя бы одно из двух значений destination-ip и device. Если туннелей более одного, то должно быть также установлено хотя бы одно из двух значений source-ip и key.

ПРИМЕЧАНИЕ В ряде программных и аппаратных продуктов, в т.ч. в некоторых продуктах Cisco Systems, возможна работа только одного туннеля с одинаковыми IP-адресами сторон. В программном обеспечении NSG Linux такая ситуация допускается, а туннели в этом случае различаются по ключу.

checksum { no | yes }

Обработка контрольной суммы. При установленном значении yes контрольная сумма исходящих пакетов вычисляется и указывается в заголовке GRE. Во входящих пакетах проверяется контрольная сумма, поврежденные пакеты уничтожаются.
По умолчанию проверка отключена.

pmtudisc { yes | no }

Включение/выключение функции Path MTU Discovery в туннеле. По умолчанию, а также при использовании параметра TTL, данная функция включена.

sequence-datagrams { yes | no }

Включение/выключение контроля последовательности пакетов. Данный механизм предназначен для уничтожения всех "запоздавших" пакетов. Если он включен, то в исходящие GRE пакеты добавляются порядковые номера, а во входящих — проверяются их номер и пакеты, выпадающие из последовательности, уничтожаются. Например, если пакеты получены в такой последовательности:

1 2 3 5 6 4 7 8

то пакет 4 будет удален.
По умолчанию контроль последовательности выключен. Если он включен, то включать его необходимо на обеих сторонах туннеля.

tos use { <0...255> | none }

Установка поля Type of Service для пакетов GRE-туннеля в сети общего пользования. По умолчанию принудительная установка поля TOS выключена; в этом случае поле TOS туннеля берется из туннелируемых пакетов корпоративной сети.

ttl use { <0...255> | none }

Установка поля TTL для туннелируемых пакетов корпоративной сети. Поскольку туннель сокращает количество шагов маршрутизации (*hops*) для этих пакетов, рекомендуется использовать небольшие значения — обычно 64. По умолчанию принудительная установка TTL выключена.

encapsulation { ip-over-gre | ip-over-ip | eth-br-over-ip | hdlc-over-gre }

Выбор инкапсулируемого протокола, т.е. "полезной нагрузки" туннеля, и способа инкапсуляции. В данной версии NSG Linux поддерживаются следующие варианты туннелей:

ip-over-gre	Инкапсуляция GRE, передаются пакеты IP. Туннель участвует в IP-маршрутизации наравне с остальными IP-интерфейсами.
ip-over-ip	Простая инкапсуляция IP-over-IP, используемая в Linux. (Не тождественна GRE!) Совместима с другими программными и аппаратными Linux-системами. Туннель участвует в IP-маршрутизации наравне с остальными IP-интерфейсами.
eth-br-over-gre	Инкапсуляция GRE, передаются пакеты Ethernet. Туннель должен быть включен в состав Bridge Group.
hdlc-over-gre	Инкапсуляция GRE, передаются пакеты HDLC общего вида. Как частные случаи, это могут быть пакеты Frame Relay, X.25, PPP или Cisco-HDLC.

По умолчанию используется инкапсуляция IP-over-GRE.

keepalive { <1...32000> retry <1...32000> | no }

Настройка механизма *keepalive* для туннеля. Об особенностях реализации данного механизма см. следующий параграф. Первый параметр определяет периодичность отсылки запросов *keepalive*, второй — максимально допустимое число неудачных попыток.

Далее для туннеля с инкапсуляцией ip-over-gre или ip-over-ip в меню включаются команды, общие для всех IP-интерфейсов (физических портов, Frame Relay DLCI, Ethernet VLAN и т.п.). В данном случае они определяют характеристики интерфейса, представляющего туннель с точки зрения наложенной сети:

[no] access-group ...
: Настройка фильтрации IP-пакетов на данном интерфейсе. Подробно см. Часть 3.

[no] crypto ...
: Настройка защищенных туннелей VPN, создаваемых на данном IP-интерфейсе. В данном случае трафик частной сети IP передается внутри защищенного туннеля VPN, который, в свою очередь, проходит по туннелю IP-over-IP. Подробно о настройке VPN см. раздел 4.2.

[no] ip ... Настройка параметров протокола IP. Подробно см. Часть 3.

mtu <64...18000>
: Установка размера MTU для IP-пакета. Подробно см. Часть 3.

nat ... Настройка трансляции сетевых IP-адресов (NAT) для данного интерфейса. Подробно см. Часть 3.

[no] service-policy ...
: Выбор и настройка политики управления IP-трафиком для данного интерфейса. Подробно см. Часть 3.

show ... Просмотр состояния и статистики интерфейса. Подробно см. Часть 3.

Для туннеля с инкапсуляцией eth-br-over-gre в меню добавляется пункт для включения его в состав Ethernet-моста:

bridge-group { <номер> | no }
: Включение данного туннеля в программный мост (*bridge group*) Ethernet и исключение из него. Помимо туннелей GRE, в состав моста могут входить физические порты Ethernet, VLAN и виртуальные каналы Frame Relay. Подробно об использовании Bridge Group см. Часть 2.

Для туннеля с инкапсуляцией hdlc-over-gre создается отдельный настраиваемый объект — виртуальный порт с именем вида tN, где N — номер туннеля. Данный объект обладает всеми протокольными параметрами, присущими синхронному порту. В частности, ему может быть назначена инкапсуляция Frame Relay, X.25, PPP Cisco-HDLC, либо Raw-HDLC. Для туннеля Frame Relay-over-IP создаются виртуальные каналы Frame Relay и т.п. В целом настройка такого виртуального порта полностью аналогична протокольной настройке физического синхронного порта, описанной в Части 2.

ПРИМЕЧАНИЕ Для всех протоколов HDLC-семейства в заголовке пакета GRE указывается, в данной версии NSG Linux, идентификатор протокола Frame Relay. Реализация Frame Relay-over-IP в устройствах NSG совместима с продуктами других производителей.

§4.4.2. Механизм *keepalive* для туннелей GRE

Протокол GRE не предусматривает встроенного механизма *keepalive*, однако у различных производителей имеются собственные реализации этого механизма. В программном обеспечении NSG Linux используется механизм, предложенный компанией Cisco Systems; подробное описание этого алгоритма приведено в документе Cisco Systems: *GRE Tunnel Keepalives* (Document ID: 64565) и доступно по адресу: http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a008048cffc.shtml.

Суть данного механизма состоит в том, что на удаленную сторону посылается специально сформированный пакет GRE с инкапсулируемым протоколом IP. Внутри него, однако, находится не просто IP-пакет, а еще один GRE-пакет, имеющий адресом назначения IP-адрес системы, инициирующей запрос. Такая конструкция не противоречит спецификации GRE, поскольку пакет GRE является частным случаем IP-пакета. В качестве идентификатора протокола в этом пакете указан 0, что позволяет отличить его от остальных пакетов GRE-туннеля.

Инициатор посылает запросы GRE *keepalive* через установленные промежутки времени. Удаленная сторона туннеля разбирает внешний пакет GRE, извлекает из них вложенный пакет и обрабатывает его в соответствии со своей таблицей маршрутизации. Поскольку этот пакет представляет собой готовый пакет GRE-туннеля, он маршрутизируется обратно инициатору. Тот, получив пакет, разбирает его заголовок, по идентификатору протокола определяет, что это не пакет с полезными данными, а ответ на *keepalive*, и считает запрос отвеченным.

При отключенном механизме *keepalive* интерфейс посылает данные в туннель "наугад", не имея никакой информации о доступности и работоспособности удаленной стороны. В этом случае реализация GRE совместима с продуктами любых других сторонних производителей. Однако, чтобы туннель не превратился в "черную дыру", для контроля целостности данных следует использовать механизмы вложенных протоколов.

ПРИМЕЧАНИЕ Механизм *keepalive* не реализован для туннелей типа IP-over-IP (Linux).

Пример конфигурации.

```
!
nsg
    tunnel ip 1
        destination-ip 10.0.52.34
        source-ip 10.0.52.33
        keepalive 3 retry 5
        encapsulation hdlc-over-gre
        exit
!
```

В данном случае запрос посылается каждые 3 секунды. В случае 5 неудачных запросов интерфейс tuni1 переходит в состояние DOWN. При этом удаляются маршруты через этот интерфейс и др. Пакеты с данными, поступающие от удаленной стороны туннеля, сбрасываются с сообщением "proto unreachable" (как если бы туннеля не было вовсе).

Независимо от состояния интерфейса запросы продолжают посылаться; при получении первого ответа, т.е. при восстановлении работоспособности туннеля, интерфейс переходит в состояние UP, для него восстанавливаются все маршруты и дополнительные службы.

Из сути данного механизма следует, что запрос *keepalive* формируется в рамках туннеля и ответить на него может только вторая сторона туннеля, в рамках которого он создан. При этом наличие потока данных (в любую сторону) никак не влияет на алгоритм поднятия опускания туннеля, т.е. если ответы на *keepalive* не приходят, то интерфейс перейдет в состояние DOWN независимо от того, что данные вроде как идут.

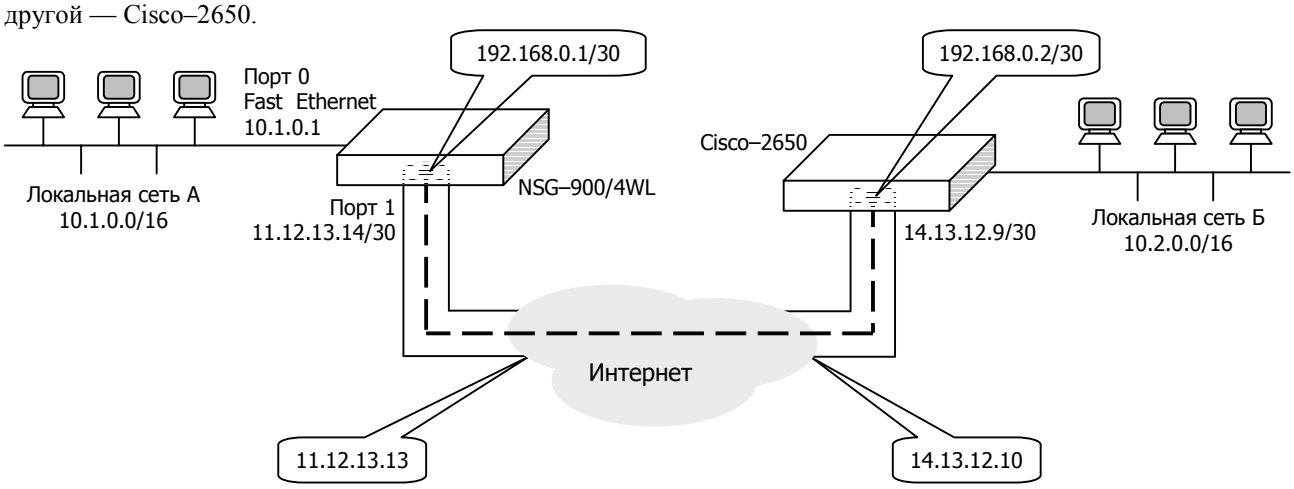
В частности, для того, чтобы система отвечала на запросы удаленной стороны, в ней должен быть создан туннельный интерфейс, для него указано административное состояние UP и указан адрес удаленной стороны. На входящие запросы туннель отвечает всегда, даже если сам он находится в состоянии DOWN по причине неполучения ответов *keepalive* от удаленной стороны, или на нём выставлен флаг DOWN вручную (командой ifconfig tuni1 down в командной оболочке Linux). Кроме того, прохождение пакетов GRE keepalive должно быть не запрещено фильтрами на обеих сторонах:

```
add 1 permit 47 <источник> <назначение>
```

ВНИМАНИЕ Обычные Linux-системы не поддерживают *keepalive* и не отвечают на него, несмотря на то, что туннели поддерживаются. Это следует из общего правила, гласящего, что система не может принимать пакеты, которые якобы исходят от неё самой (а именно такой прием используется в данном случае).
Маршрутизаторы Cisco Systems поддерживают ответ на *keepalive* даже в том случае, если сами не умеют его посылать, но умеют создавать туннели.
Для продуктов других производителей возможна одна из двух вышеописанных ситуаций, в также иные фирменные реализации GRE *keepalive*.

§4.4.3. Пример построения туннеля IP-over-GRE

Схема стенда показана на рисунке. Стенд состоит из двух пограничных маршрутизаторов, соединенных через сеть общего пользования. Для наглядности на одной стороне используется устройство NSG–900, на другой — Cisco–2650.



Через маршрутизаторы связаны две приватные сети 10.1.0.0/16 и 10.2.0.0/16. Трафик этих сетей передается в туннеле между интерфейсами пограничных маршрутизаторов NSG–900 (11.12.13.14) и Cisco–2650 (14.13.12.9). При этом весь IP-пакет приватной сети, включая заголовок, передается как данные в новом пакете между двумя маршрутизаторами. На противоположной стороне пакеты корпоративной сети извлекаются из пакетов туннеля и передаются в приватную сеть. Для простоты приведены минимальные настройки, необходимые для работы туннеля. (Параметры, не относящиеся непосредственно к туннелю, опущены.)

Настройка NSG–900

```
!
nsg
    port eth0
        ip address 10.1.0.1/16
    tunnel ip 1
        description "tunnel  NSG - CISCO"
        adm-state up
        destination-ip 14.13.12.9
        source-ip 11.12.13.14
        ip address 192.168.0.1/30
        exit
    exit
!
ip route 10.2.0.0/16  tuni1
ip route 14.13.12.9/32  11.12.13.13
!
```

Настройка Cisco–2650

```
!
interface FastEthernet0/0
    ip address 10.2.0.1 255.255.0.0
!
interface tunnel 0
    description "tunnel  CISCO - NSG"
    tunnel  mode gre ip
    tunnel destination 11.12.13.14
    tunnel source 14.13.12.9
    ip address 192.168.0.2/30
!
ip route 10.1.0.0/16  192.168.0.1
ip route 11.12.13.14  255.255.255.255  14.13.12.10
!
```

§4.4.4. Клиент PPTP

Протокол PPTP предназначен для передачи пакетов PPP через сеть IP при помощи общего механизма GRE. Для работы этого протокола, помимо потока датаграмм, содержащих "полезную нагрузку", организуется управляющее соединение, устанавливаемое от клиента к серверу на номер порта TCP 1723. Для работы PPTP необходимо, чтобы на стороне сервера было разрешено принимать входящие TCP-пакеты и запросы на установление соединений по данному порту.

Создание туннелей PPTP производится в меню (config-nsg)# следующими командами:

tunnel pptp <1…255>
no tunnel pptp <1…255>
: Создание/изменение и удаление туннеля с указанным номером, соответственно. Номер туннеля используется только как локальный идентификатор в устройстве NSG и никак не связан с номером, присвоенным этому туннелю на удаленной стороне.

Для каждого создаваемого туннеля в системе создается IP-интерфейс с именем вида pptpN. Дальнейшая настройка производится меню туннеля (config-tunnel-N)#. Меню содержит следующие команды:

description "<комментарий>"
: Административное описание данного туннеля. Если строка содержит пробелы, она должна быть заключена в кавычки. Максимальная длина описания — 255 символов.

adm-state { up | down }
: Административное состояние интерфейса.

server-address <ip-адрес>
: Адрес удаленной стороны (сервера PPTP). Параметр обязательный.

source-address <ip-адрес>
: Адрес, указываемый в качестве адреса источника в пакетах, относящихся к данному туннелю. Если параметр не задан (0.0.0.0 — значение по умолчанию), в качестве адреса источника указывается адрес того IP-интерфейса, через который пакеты уходят в сеть общего пользования. В специфических сетевых решениях, требующих некоторого определенного значения адреса источника (например, для фильтрации), данный параметр позволяет принудительно установить любой IP-адрес, принадлежащий какому-либо интерфейсу устройства.

virtual-template <1…25>
: Указатель на шаблон интерфейса. Содержит полную информацию о настройках виртуального интерфейса PPP: IP-адреса и способ их назначения, способ аутентификации и т.п. Подробно о *virtual-template* см. Часть 2.

ppp-log { previous | current }
: Просмотр журнала сеанса PPTP. Ключевое слово previuos выводит журнал последней завершенной попытки, current — текущей попытки. Во втором случае, повторяя ввод команды, можно проследить ход сеанса по мере его выполнения.
В ходе сеанса PPTP весь вывод направляется также на сервер Syslog, если он включен. Для этого необходимо предварительно перейти в командную оболочку ОС Linux и выполнить команду:
    syslogd
либо включить syslogd при помощи сценария, см. Часть 1. Просмотреть файл системного журнала можно также в командной оболочке ОС Linux следующей командой:
    cat /var/log/messages

keepalive { no | <0…3600> [retry {<1…100> | no }] }

Проверка целостности управляющего TCP-соединения с помощью механизма Echo Request/Reply. Первый параметр определяет интервал (в секундах) между посылкой контрольных пакетов; если значение параметра равно нулю или no, запросы не посылаются. При этом ответы на приходящие запросы отсылаются в любом случае (в т.ч. и при keepalive no).

Второй параметр устанавливает максимальное количество запросов. Если на указанное число запросов подряд не получено ни одного ответа, соединение разрывается. Суммарное время, по истечении которого интерфейс сочтет соединение неработающим и рестартует, равно произведению этих двух параметров. Значение retry no показывает, что разрыв соединения не производится, независимо от отсутствия ответов на запросы; такая установка целесообразна, например, если пакеты *keepalive* посылаются с единственной целью предотвратить разрыв соединения на физическом уровне из-за отсутствия трафика (переход сотовых модемов в "спящий" режим и т.п.).

При изменении параметра keepalive параметр retry автоматически принимает значение no. Таким образом, чтобы использовать механизм зондирования и разрыва соединения, данную команду необходимо вводить полностью.

По умолчанию установлены следующие значения параметров: keepalive no retry no.

show … Просмотр состояния и статистики интерфейса. Подробно см. Часть 3.

Особо стоит остановиться на контроле целостности соединения PPTP, поскольку он может осуществляться в трех местах: на уровне несущего соединения PPP или SLIP в сети общего пользования, на уровне соединения PPTP и в управляющем соединении PPTP. Рекомендуется использовать контроль только на одном объекте, представляющем собой наиболее слабое звено стека, а именно:

— Для соединений через сотовые сети, коммутируемые модемные линии и другие типы подключений, которые могут быть потенциально ненадежны и неустойчивы — в шаблоне несущего соединения PPP.

— Для соединений через сети Ethernet, IP-over-X.25 и т.п. надежные среды — в управляющем соединении PPTP.

Пример настройки соединения PPTP через сотовую сеть CDMA (SkyLink). Используется устройство NSG–700/4AU с интерфейсным модулем UIM–EVDO.

```
!
nsg
    virtual-template 2
        keepalive no retry no
        ppp ipcp accept-address yes
        ppp set-default-route yes
        ppp sent-username basile
        exit
    virtual-template 1
        keepalive 10 retry 3
        ppp ipcp accept-address yes
        ppp sent-username mobile
        exit
    tunnel pptp 1
        server-address 123.145.167.189
        virtual-template 2
        exit
    chat-script CDMA "TIMEOUT 10 XXX-AT-OK ATD#777 CONNECT ' '"
    card s1 uim-cdma
    port eth0
        ip address 10.0.2.16/8 anycast 0.0.0.0
        exit
    port s1
        encapsulation ppp
        virtual-template 1
        chat-script CDMA
        exit
!
username basile  password P0uPkiNe
username mobile password internet
!
ip route 123.145.167.189/32 s1
!
```

Здесь mobile и internet — имя и пароль для доступа к услуге CDMA, 123.145.167.189 — адрес удаленного сервера в Интернет, basile P0uPkine — имя и пароль для PPTP-соединения с этим сервером. В случае некорректного отсоединения от сети CDMA (пропадание сигнала и т.п.) отказ будет детектирован через 30 сек (3 попытки по 10 сек). После этого PPP-интерфейс рестартует и попытается снова установить соединение с

сетью. Если соединение будет восстановлено успешно и с прежним IP-адресом, а по туннелю в течение всего этого времени никакие данные не посылались, то туннель PPTP продолжит работу, так что переустановление физического соединения и PPP-соединения останется незамеченным для пользователей сети. Если же соединение не восстановлено, а PPTP-интерфейс попытается передать данные по туннелю, то управляющее соединение обнаружит, что интерфейс сети общего пользования находится в состоянии DOWN (или снова в UP, но с иным IP-адресом), и туннель будет разорван.

§4.4.5. IP-over-X.25 и X.25-over-TCP/IP

Туннели, связанные с протоколом X.25 (либо в качестве полезной нагрузки, либо в качестве транспорта), рассматриваются в Части 5 данного документа.