Интерфейс виртуальных туннелей IPsec

Содержание

Интерфейс виртуальных туннелей IPsec

Содержание

Ограничения для интерфейса виртуальных туннелей IPsec

Сведения об интерфейсе виртуальных туннелей IPsec

Преимущества использования интерфейса виртуальных туннелей IPsec

Маршрутизация при использовании интерфейса виртуальных туннелей IPsec

Статические интерфейсы виртуальных туннелей

Динамические интерфейсы виртуальных туннелей

Жизненный цикл динамического интерфейса виртуальных туннелей

Шифрование трафика в интерфейсе виртуальных туннелей IPsec

Поддержка атрибутов пользователей в серверах Easy VPN

Как настроить интерфейс виртуальных туннелей IPsec

Настройка статических интерфейсов виртуальных туннелей IPsec

Настройка динамических интерфейсов виртуальных туннелей IPsec

Настройка атрибутов пользователей на локальном сервере Easy VPN AAA

Примеры конфигурации интерфейсов виртуальных туннелей IPsec

Статический интерфейс виртуальных туннелей с IPsec: пример

Статический интерфейс виртуальных туннелей с поддержкой VRF: пример

Статический интерфейс виртуальных туннелей с QoS: пример

Статический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример

Сервер Easy VPN с динамическим интерфейсом виртуальных туннелей: пример

Клиент Easy VPN с ди=амическим интерфейсом виртуальных туннелей: пример

IPsec с поддержкой VRF с динамическим интерфейсом VTI: пример

Динамический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример

Динамический интерфейс виртуальных туннелей с QoS: пример

Атрибуты пользователей на сервере Easy VPN: пример

Дополнительные ссылки

Дополнительная документация

Стандарты

Базы данных MIB

Документы RFC

Техническая поддержка

Справочник по командам

crypto aaa attribute list

crypto isakmp client configuration group

crypto isakmp profile

interface virtual-template

show vtemplate

tunnel mode

virtual-template

Информация о функциональных возможностях интерфейсов виртуальных туннелей IPsec

Интерфейс виртуальных туннелей IPsec

Первая публикация: 18 октября 2004 г.

Последнее обновление: 1 августа 2006 г.

Интерфейсы виртуальных туннелей (virtual tunnel interfaces, VTI) IPsec представляют собой тип маршрутизируемых интерфейсов на концах туннелей IPsec. Это простой способ установки защиты между узлами для образования перекрывающихся сетей. Интерфейсы VTI IPsec упрощают настройку IPsec для защиты удаленных каналов, поддерживают мультиадресную рассылку, делают проще управления сетью и балансировку нагрузки.

Поиск сведений о функциональных возможностях в данном модуле

Некоторые версии программного обеспечения Cisco IOS могут поддерживать не все функции, описанные в данном модуле. Ссылки на документацию по специальным функциям для данного модуля, а также список версий, поддерживающих все перечисленные функции, можно найти в разделе «Информация о функциональных возможностях интерфейсов виртуальных туннелей IPsec».

Получение информации о поддержке платформ и образов программного обеспечения Cisco IOS

Для поиска информации о поддержке платформ и образов программного обеспечения Cisco IOS воспользуйтесь инструментом Cisco Feature Navigator. Доступ к инструменту Cisco Feature Navigator можно получить по адресу http://www.cisco.com/go/fn. Необходимо наличие учетной записи на веб-сайте cisco.com. Если у вас нет учетной записи, вы забыли имя пользователя или пароль, то в диалоговом окне входа в систему нажмите кнопку Cancel (Отмена) и следуйте дальнейшим указаниям.

Содержание

- Ограничения для интерфейса виртуальных туннелей IPsec
- Сведения об интерфейсе виртуальных туннелей IPsec
- Как настроить интерфейс виртуальных туннелей IPsec
- Примеры конфигурации интерфейсов виртуальных туннелей IPsec
- Дополнительные ссылки
- Справочник по командам
- Информация о функциональных возможностях интерфейсов виртуальных туннелей IPsec

Ограничения для интерфейса виртуальных туннелей IPsec

Набор для преобразования IPsec

Набор для преобразования IPsec должен настраиваться только в режиме туннеля.

Сопоставления безопасности IKE

Сопоставления безопасности (security association, SA) протокола обмена интернет-ключами (Internet Key Exchange, IKE) привязаны к интерфейсу виртуальных туннелей. Поскольку сопоставления SA IKE привязаны к интерфейсу виртуальных туннелей, для криптокарты не могут использоваться одинаковые сопоставления SA IKE.

Селекторы трафика сопоставлений безопасности(SA) IPsec

Статические интерфейсы виртуальных туннелей поддерживают только одно сопоставление SA IPsec, присоединенную к интерфейсу VTI. Селектор трафика для SA IPsec всегда имеет вид «IP any any».

Динамический интерфейс VTI является также интерфейсом «точка-точка», который поддерживает одно сопоставление SA IPsec, однако динамический VTI более гибок в том, что обеспечивает доступ к селекторам IPsec, предоставляемым инициатором.

Прокси

Статические интерфейсы VTI поддерживают только прокси вида «IP any any».

Динамические интерфейсы VTI поддерживают только один прокси, который имеет вид «IP any any», или любое его подмножество.

Формирование трафика QoS

Формируемый трафик коммутируется по процессам.

Восстановление после отказа с отслеживанием состояния

В интерфейсе VTI IPsec не поддерживается восстановление после отказа с отслеживанием состояния IPsec.

Защита туннеля

Ключевое слово **shared** не используется и не должно задаваться при использовании команды **tunnel mode ipsec ipv4** в режиме IPv4 IPsec.

Сравнение статических интерфейсов VTI и туннелей GRE

Интерфейсы VTI с использованием IPsec ограничены одноадресным и мультиадресным IP-трафиком, в противоположность туннелям GRE, которые имеют более широкую схему применения для реализации IPsec.

Конфигурация IPsec с поддержкой VRF

В конфигурациях IPsec с поддержкой маршрутизации и переадресации в виртуальных частных сетях (Virtual Private Network routing and forwarding, VRF) в статических или динамических интерфейсах VTI (dynamic VTI, DVTI) VRF *не должен* настраиваться в профиле протокола управления сопоставлениями безопасности и ключами в Интернете (Internet Security Association and Key Management Protocol, ISAKMP). Вместо этого VRF необходимо настраивать в туннельном интерфейсе статических интерфейсов VTI. В DVTI необходимо применить VRF к шаблону vtemplate с помощью команды **ip vrf forwarding**.

Сведения об интерфейсе виртуальных туннелей IPsec

Использование виртуальных туннельных интерфейсов IPsec одновременно значительно упрощает процесс конфигурации в случае необходимости защиты удаленного доступа и обеспечивает более простую альтернативу использованию общей инкапсуляции маршрутов (generic routing encapsulation, GRE) или протоколов туннелирования уровня 2 (Layer 2 Tunneling Protocol, L2TP) для инкапсуляции и криптокарт IPsec. Основное преимущество, связанное с интерфейсом VTI IPsec состоит в том, что настройка не требует статического сопоставления сеансов IPsec с физическим интерфейсом. Конечная точка туннеля IPsec связывается с реальным (виртуальным) интерфейсом. Поскольку в конечной точке туннеля имеется маршрутизируемый интерфейс, для туннеля IPsec можно применять множество общих возможностей интерфейса.

Интерфейс VTI IPsec обеспечивает гибкость отправки и приема одноадресного и мультиадресного шифрованного трафика IP на любой физический интерфейс, например, в случае наличия множества путей. Трафик шифруется или дешифруется при пересылке в туннельный интерфейс или из него и управляется с помощью таблицы маршрутизации IP. Для

маршрутизации трафика через виртуальный интерфейс можно использовать динамическую или статическую IP-маршрутизацию. Использование IP-маршрутизации для пересылки трафика через туннельный интерфейс упрощает настройку VPN IPsec по сравнению с более сложным процессом использования списков управления доступом (ACL) с криптокартой в стандартных конфигурациях IPsec. Функции DVTI схожи с другими реальными интерфейсами, так что, пока туннель активен, с ними можно использовать средства обеспечения качества обслуживания (QoS), брандмауэр и другие службы безопасности.

Без модуля ускорения виртуальных частных сетей (VPN) 2+ (VAM2+), ускоряющего виртуальные интерфейсы, пакет, проходящий по виртуальному интерфейсу IPsec, направляется на процессор маршрутизации (RP) для инкапсуляции. Этот метод имеет тенденцию к снижению скорости работы и обладает ограниченной масштабируемостью. В аппаратном режиме шифрования все интерфейсы VTI IPsec ускоряются с помощью криптографического модуля VAM2+. Весь трафик, проходящий через туннель, шифруется и расшифровывается с помощью VAM2+.

Дополнительная информация о интерфейсе VTI IPsec содержится в следующих разделах:

- Преимущества использования интерфейса виртуальных туннелей IPsec
- Маршрутизация при использовании интерфейса виртуальных туннелей IPsec
- Статические интерфейсы виртуальных туннелей
- Динамические интерфейсы виртуальных туннелей
- Жизненный цикл динамического интерфейса виртуальных туннелей
- Шифрование трафика в интерфейсе виртуальных туннелей IPsec
- Поддержка атрибутов пользователей в серверах Easy VPN

Преимущества использования интерфейса виртуальных туннелей IPsec

Интерфейс VTI IPsec позволяют настраивать виртуальный интерфейс, в котором можно использовать различные функциональные возможности. Функциональные возможности для нешифрованных пакетов настраиваются в интерфейсе VTI. Функциональные возможности для шифрованных пакетов используются во внешнем физическом интерфейсе. При использовании VTI IPsec можно разделить использование таких функций, как NAT, ACL и QoS, и применять их для нешифрованных или шифрованных пакетов, или для обоих видов. При использовании криптокарт не существует простого способа использовать средства шифрования для туннеля IPsec.

Маршрутизация при использовании интерфейса виртуальных туннелей IPsec

Поскольку VTI являются маршрутизируемыми интерфейсами, маршрутизация играет важную роль в процессе шифрования. Трафик шифруется только при пересылке из VTI, трафик, поступающий в VTI, расшифровывается и маршрутизируется соответствующим образом. Интерфейсы VTI позволяют организовать зашифрованный туннель, используя в качестве конечной точки туннеля реальный интерфейс. Можно осуществлять маршрутизацию на интерфейс или использовать службы, такие как QoS, брандмауэры, трансляция сетевых адресов и статистика Netflow, как это делается для других интерфейсов. Можно отслеживать интерфейс или осуществлять маршрутизацию на него, имея преимущество перед криптокартами за счет того, что реальный интерфейс обеспечивает возможности, присущие всем типовым интерфейсам Cisco IOS. Кроме того, интерфейс VTI шифрует передаваемый ему трафик.

В туннельном интерфейсе можно использовать протоколы маршрутизации, так что информация о маршрутах будет распространяться через виртуальный туннель. Маршрутизатор может установить отношения с соседними узлами через VTI. Может производиться шифрование мультиадресных пакетов и взаимодействие со стандартными установками IPsec, поскольку статический интерфейс VTI IPsec будет согласовывать и принимать прокси **permit IP ANY ANY**.

Существует два типа интерфейсов VTI: статические VTI (SVTI) и динамические VTI (DVTI).

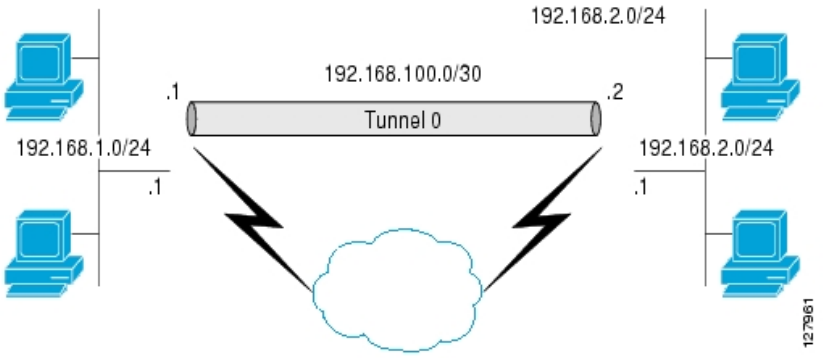
Статические интерфейсы виртуальных туннелей

Конфигурации интефейса SVTI могут использоваться для связи между узлами, при которой туннель обеспечивает постоянную связь между двумя узлами. Преимущество использования SVTI по сравнению с конфигурациями с криптокартой состоит в том, что пользователи могут применять для туннельного интерфейса динамические протоколы маршрутизации, не используя дополнительные 4 байта, необходимые для заголовков GRE, что уменьшает полосу пропускания для передачи шифрованных данных.

Кроме того, можно настроить различные функции ПО Cisco IOS непосредственно для туннельного интерфейса и выходного физического интерфейса туннельного интерфейса. Такая прямая настройка позволяет пользователям надежно контролировать использование функций на пути до и после шифрования.

Рис. 1 иллюстрирует использование статического VTI.

Рис. 1. Статический интерфейс VTI IPsec



VTI IPsec поддерживает стандартное туннелирование IPsec и реализует большинство свойств физического интерфейса.

Динамические интерфейсы виртуальных туннелей

Интерфейсы DVTI могут обеспечить более безопасное и масштабируемое соединение для сетей VPN с удаленным доступом. Технология DVTI заменяет такие методы создания туннелей, как динамические криптокарты и динамические сети с топологией «звезда».

Динамические VTI могут использоваться как для конфигурации с сервером, так и для конфигурации с удаленным доступом. Туннели по требованию предоставляют

отдельные виртуальные интерфейсы доступа для каждого сеанса VPN. Конфигурации виртуальных интерфейсов доступа клонируются из шаблона конфигурации виртуального доступа, который включает в себя конфигурацию IPsec и функции Cisco IOS, настроенные для шаблона виртуального интерфейса, такие как QoS, NetFlow или ACL.

Функции DVTI схожи с другими реальными интерфейсами, так что, пока туннель активен, с ними можно использовать средства обеспечения качества обслуживания (QoS), брандмауэр и другие службы безопасности. Функции QoS можно использовать для повышения производительности различных приложений в сети. Любые сочетания функций QoS, предоставляемых в ПО Cisco IOS, можно использовать в приложениях передачи голоса, видео и данных.

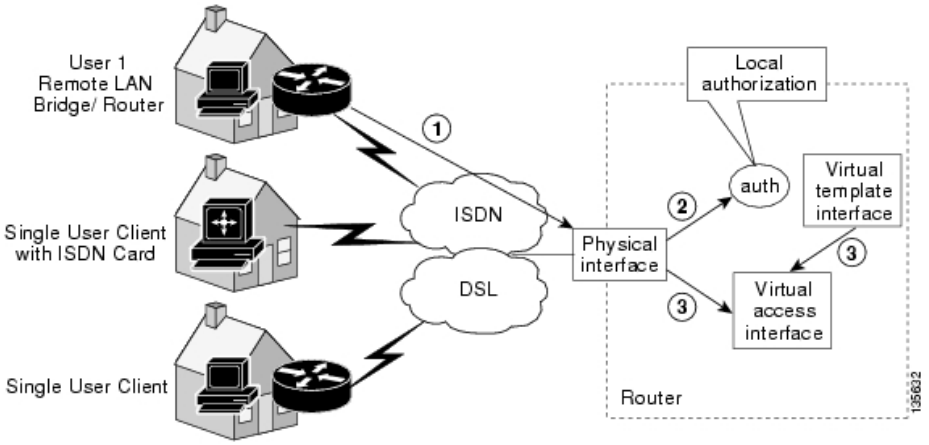
Динамические интерфейсы VTI обеспечивают эффективное использование IP-адресов и защиту соединений. Динамические интерфейсы VTI позволяют использовать динамически загружаемые политики пользователей и групп, настроенные на сервере RADIUS. Определения пользователей и групп можно создавать, используя расширенную аутентификацию (Xauth) группы User или Unity, или извлекать из сертификата. Динамические интерфейсы VTI основаны на стандартах, так что они совместимы с оборудованием различных производителей. Динамические интерфейсы VTI IPsec позволяют создавать

хорошо защищенные соединения для VPN удаленного доступа и могут использоваться в сочетании с архитектурой Cisco для голосовых, видео и интегрированных данных (AVVID) для объединенной доставки голоса, видео и данных по IP-сетям. Динамические интерфейсы VTI упрощают развертывание IPsec с поддержкой маршрутизации и переадресации в виртуальных частных сетях (Virtual Private Network routing and forwarding, VRF). Функция VRF настраивается на интерфейсе.

Динамические интерфейсы VTI требуют минимальных настроек маршрутизатора. Можно настраивать и клонировать один виртуальный шаблон.

Динамический VTI создает интерфейс для сеансов IPsec и использует инфраструктуру виртуального шаблона для динамического создания и управления динамическими VTI IPsec. Инфраструктура виртуального шаблона расширяется для создания динамических интерфейсов туннелей с виртуальным доступом. Динамические интерфейсы VTI используются в конфигурации сети с топологией «звезда». Один динамический VTI может поддерживать несколько статических VTI. Решения принимаются через обновления маршрутизации. Рис. 2 иллюстрирует путь аутентификации динамического VTI.

Рис 2. Динамический VTI IPsec



Аутентификация, показанная на рис. 2, происходит следующим образом:

1. Пользователь 1 вызывает маршрутизатор.

2. Маршрутизатор 1 производит аутентификацию пользователя 1.

3. IPsec клонирует интерфейс виртуального доступа из шаблона виртуального интерфейса.

Жизненный цикл динамического интерфейса виртуальных туннелей

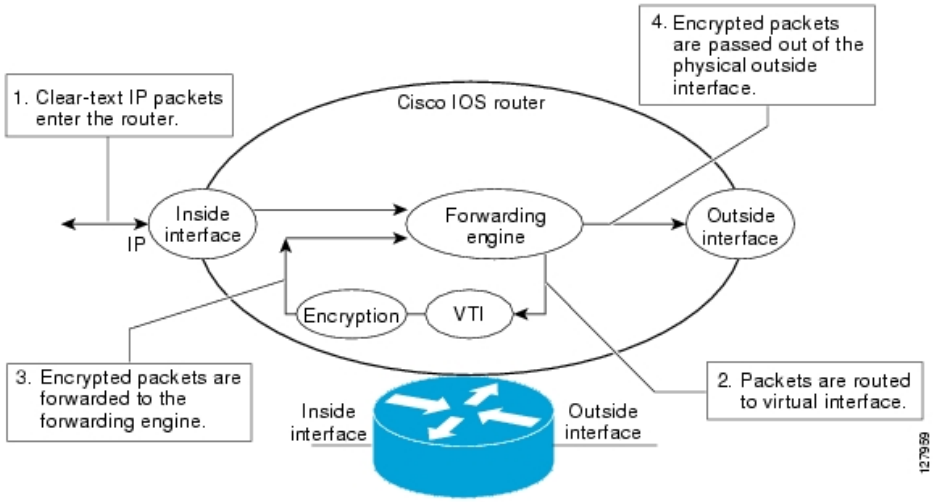
Профили IPsec определяют политики для динамических VTI. Динамический интерфейс создается в конце фазы 1 IKE и фазы 1.5 IKE. Интерфейс удаляется, когда закрывается сеанс IPsec с одноранговым узлом. Сеанс IPsec закрывается, когда IKE и SA IPsec с одноразовым узлом удаляются.

Шифрование трафика в интерфейсе виртуальных туннелей IPsec

При настройке VTI IPsec в туннеле производится шифрование. Трафик шифруется при передаче в туннельный интерфейс. Передача трафика осуществляется в соответствии с таблицей маршрутизации IP, для маршрутизации трафика в VTI может использоваться динамическая или статическая маршрутизация IP. Использование маршрутизации IP для пересылки трафика на шифрование упрощает настройку VPN IPsec, поскольку использование ACL с криптокартой в стандартной настройке IPsec становится ненужным. Виртуальный туннель IPsec также позволяет шифровать трафик мультиадресной рассылки с IPsec.

Поток пакетов IPsec, входящих в туннель IPsec, показан на рис. 3.

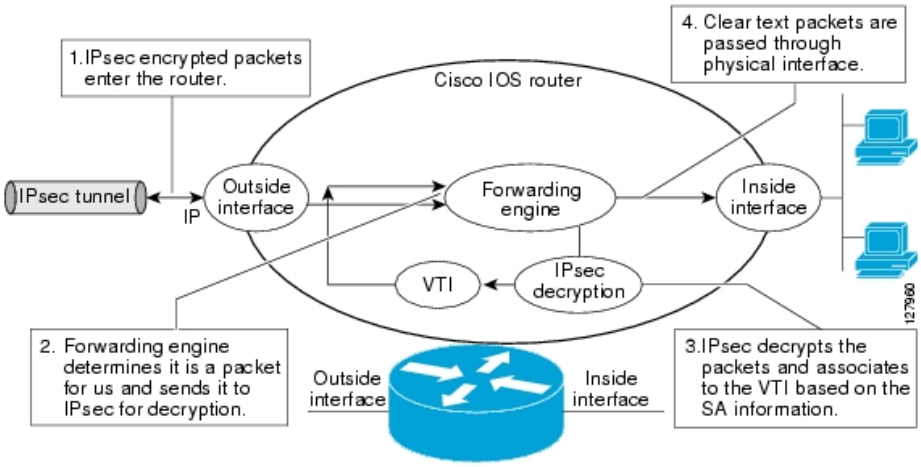
Рис 3. Поток пакетов в туннеле IPsec



После поступления пакетов на внутренний интерфейс механизм пересылки коммутирует пакеты на VTI, где они шифруются. Шифрованные пакеты передаются обратно в механизм пересылки, где они коммутируются через внешний интерфейс.

На рис. 4 показан поток пакетов, исходящих из туннеля IPsec.

Рис 4. Поток пакетов, исходящих из туннеля IPsec



Поддержка атрибутов пользователей в серверах Easy VPN

Функция поддержки атрибутов пользователей на серверах Easy VPN дает пользователям возможность поддерживать атрибуты пользователей на серверах Easy VPN. Эти атрибуты относятся к виртуальным интерфейсам доступа.

Локальный сервер Easy VPN AAA

Для локального сервера Easy VPN AAA пользовательские атрибуты используются на уровне групп или на уровне пользователей с помощью интерфейса командной строки.

Сведения о настройке атрибутов пользователей на локальном сервере Easy VPN см. в разделе «Настройка атрибутов пользователей на локальном сервере Easy VPN AAA».

Удаленный сервер Easy VPN AAA

Пары атрибут-значение (AV) могут определяться на удаленном сервере Easy VPN AAA, как показано в следующем примере:

cisco-avpair = «ip:outacl#101=permit tcp any any established

Атрибуты пользователей

В настоящее время для сервера AAA определены следующие атрибуты пользователей, которые используются в IPsec:

- inacl
- interface-config
- outacl
- route
- rte-fltr-in
- rte-fltr-out
- sub-policy-In
- sub-policy-Out
- policy-route
- prefix

Настройка интерфейса виртуальных туннелей IPsec

- Настройка статических интерфейсов виртуальных туннелей IPsec
- Настройка динамических интерфейсов виртуальных туннелей IPsec
- Настройка атрибутов пользователей на локальном сервере Easy VPN AAA

Настройка статических интерфейсов виртуальных туннелей IPsec

Данная конфигурация показывает, как настроить статический VTI IPsec.

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface** *type number*
6. **ip address** *address mask*
7. **tunnel mode ipsec ipv4**
8. **tunnel source** *interface*
9. **tunnel destination** *ip-address*
10. **tunnel protection IPsec profile** *profile-name* [**shared**]

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или действие	Назначение
Шаг 1	**enable** Пример. Router> enable	Включение привилегированного режима EXEC. • При запросе введите пароль.
Шаг 2	**configure terminal** Пример. Router# configure terminal	Вход в режим глобальной конфигурации.
Шаг 3	**crypto IPsec profile** *profile-name* Пример. Router(config)# crypto IPsec profile PROF	Определение параметров IPsec, которые будут использоваться для шифрования IPsec между двумя маршрутизаторами IPsec.
Шаг 4	**set transform-set** transform-set-name [*transform-set-name2... transform-set-name6*] Пример. Router(config)# set transform-set tset	Определение наборов преобразования, используемых в записи криптокарты.
Шаг 5	**interface** *type number* Пример.	Определение интерфейса, для которого будет настраиваться туннель, и вход в режим настройки интерфейса.

	Router(config)# interface tunnel0	
Шаг 6	**ip address** *address mask* Пример. Router(config-if)# ip address 10.1.1.1 255.255.255.0	Установка IP-адреса и маски.
Шаг 7	**tunnel mode ipsec ipv4** Пример. Router(config-if)# tunnel mode ipsec ipv4	Определение режима туннеля.
Шаг 8	**tunnel source** *interface* Пример. Router(config-if)# tunnel source loopback0	Определение начальной точки туннеля как петлевого интерфейса.
Шаг 9	**tunnel destination** *ip-address* Пример. Router(config-if)# tunnel destination 172.16.1.1	Определение IP-адреса конечной точки туннеля.
Шаг 10	**tunnel protection IPsec profile** *profile-name* [shared] Пример. Router(config-if)# tunnel protection IPsec profile PROF	Связывание туннельный интерфейс с профилем IPsec.

Настройка динамических интерфейсов виртуальных туннелей IPsec

Данная конфигурация показывает, как настроить динамический VTI IPsec.

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface virtual-template** *number*

6. **tunnel mode** *mode*

7. **tunnel protection IPsec profile** *profile-name* [**shared**]

8. **exit**

9. **crypto isakamp profile** *profile-name*

10. **virtual-template** *template-number*

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или действие	Назначение
Шаг 1	**enable** Пример. Router> enable	Включение привилегированного режима EXEC. • При запросе введите пароль.
Шаг 2	**configure terminal** Пример. Router# configure terminal	Вход в режим глобальной конфигурации.
Шаг 3	**crypto IPsec profile** *profile-name* Пример. Router(config)# crypto IPsec profile PROF	Определение параметров IPsec, которые будут использоваться для шифрования IPsec между двумя маршрутизаторами IPsec.
Шаг 4	**set transform-set** transform-set-name [*transform-set-name2... transform-set-name6*] Пример. Router(config)# set transform-set tset	Определение наборов преобразования, используемых в записи криптокарты.
Шаг 5	**interface virtual-template** number Пример. Router(config)# interface virtual-template 2	Определение виртуального шаблона туннельного интерфейса и вход в режим настройки интерфейса.
Шаг 6	**tunnel mode ipsec ipv4** Пример. Router(config-if)# tunnel mode ipsec ipv4	Определение режима туннеля.
Шаг 7	**tunnel protection IPsec profile**	Связывание туннельного интерфейса с профилем

	profile-name [shared] Пример. Router(config-if)# tunnel protection IPsec profile PROF	IPsec.
Шаг 8	**exit** Пример. Router(config-if)# exit	Выход из режима настройки интерфейса.
Шаг 9	**crypto isakamp profile** *profile-name* Пример. Router(config)# crypto isakamp profile red	Определение профиля ISAKAMP, который будет использоваться в виртуальном шаблоне.
Шаг 10	**virtual-template** *template-number* Пример. Router(config)# virtual-template 1	Определение виртуального шаблона, присоединенного к профилю ISAKAMP.

Настройка атрибутов пользователей на локальном сервере Easy VPN AAA

Для настройки атрибутов пользователей на локальном сервере Easy VPN AAA выполните следующие действия.

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. aaa attribute list *list-name*
4. attribute type ***name value*** [**service *service***] [**protocol *protocol***]
5. **exit**
6. **crypto isakmp client configuration group** *group-name*
7. **crypto aaa attribute list** *list-name*

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или действие	Назначение
Шаг 1	**enable** Пример.	Включение привилегированного режима EXEC.

	Router> enable	• При запросе введите пароль.
Шаг 2	**configure terminal** Пример. Router# configure terminal	Вход в режим глобальной конфигурации.
Шаг 3	**aaa attribute list** *list-name* Пример. Router(config)# aaa attribute list list1	Определение списка атрибутов AAA локально на маршрутизаторе и вход в режим настройки списка атрибутов.
Шаг 4	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*] Пример. Router(config-attr-list)# attribute type attribute xxxx service ike protocol ip	Определение списка атрибутов, который добавляется к локальному списку атрибутов на маршрутизаторе.
Шаг 5	**exit** Пример. Router(config-attr-list)# exit	Выход из режима настройки списка атрибутов.
Шаг 6	**crypto isakmp client configuration group** *group-name* Пример. Router (config)# crypto isakmp client configuration group group1	Указание группы, для которой будет определен профиль политики, и переход в режим настройки группы ISAKMP.
Шаг 7	**crypto aaa attribute list** *list-name* Пример. Router (config-isakmp-group)# crypto aaa attribute list listname1	Определение списка атрибутов AAA локально на маршрутизаторе.

Примеры конфигурации интерфейсов виртуальных туннелей IPsec

Следующие примеры приведены для иллюстрации сценариев настройки для IPsec VTI:

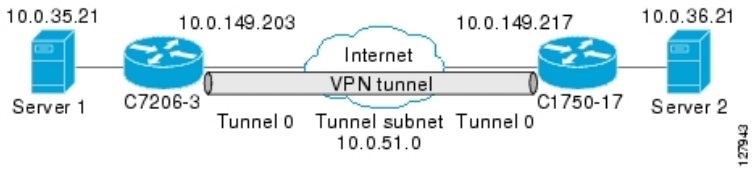
- Статический интерфейс виртуальных туннелей с IPsec: пример
- Статический интерфейс виртуальных туннелей с поддержкой VRF: пример
- Статический интерфейс виртуальных туннелей с QoS: пример

- Статический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример
- Сервер Easy VPN с динамическим интерфейсом виртуальных туннелей: пример
- Клиент Easy VPN с динамическим интерфейсом виртуальных туннелей: пример
- IPsec с поддержкой VRF с динамическим интерфейсом VTI: пример
- Динамический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример
- Динамический интерфейс виртуальных туннелей с QoS: пример
- Атрибуты пользователей на сервере Easy VPN: пример

Статический интерфейс виртуальных туннелей с IPsec: пример

Следующие примеры настроек используют для аутентификации между узлами предварительный ключ. Трафик VPN передается в VTI IPsec для шифрования, после чего пересылается на физический интерфейс. Туннель в подсети 10 проверяет пакеты на соответствие политике IPsec и пересылает их в механизм шифрования (Crypto Engine, CE) для инкапсуляции IPsec. Рис. 5 иллюстрирует конфигурацию VTI IPsec.

Рис 5. VTI с IPsec



Конфигурация маршрутизатора C7206

```
version 12.3


service timestamps debug datetime

service timestamps log datetime

hostname 7200-3

no aaa new-model

ip subnet-zero

ip cef

controller ISA 6/1

!
```

```
crypto isakmp policy 1

encr 3des

authentication pre-share

group 2

crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0

crypto IPsec transform-set T1 esp-3des esp-sha-hmac

crypto IPsec profile P1

set transform-set T1

!


interface Tunnel0

ip address 10.0.51.203 255.255.255.0

ip ospf mtu-ignore

load-interval 30

tunnel source 10.0.149.203

tunnel destination 10.0.149.217

tunnel mode IPsec ipv4

tunnel protection IPsec profile P1

!

interface Ethernet3/0

ip address 10.0.149.203 255.255.255.0

duplex full

!

interface Ethernet3/3

ip address 10.0.35.203 255.255.255.0

duplex full

!

ip classless
```

```
ip route 10.0.36.0 255.255.255.0 Tunnel0

line con 0

line aux 0

line vty 0 4

end
```

Конфигурация маршрутизатора C1750

```
version 12.3


hostname c1750-17

no aaa new-model

ip subnet-zero

ip cef

crypto isakmp policy 1

encr 3des

authentication pre-share

group 2


crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0

crypto IPsec transform-set T1 esp-3des esp-sha-hmac

crypto IPsec profile P1

set transform-set T1

!

interface Tunnel0

ip address 10.0.51.217 255.255.255.0

ip ospf mtu-ignore

tunnel source 10.0.149.217

tunnel destination 10.0.149.203

tunnel mode ipsec ipv4

tunnel protection ipsec profile P1
```

```
!

interface FastEthernet0/0

ip address 10.0.149.217 255.255.255.0

speed 100

full-duplex

!

interface Ethernet1/0

ip address 10.0.36.217 255.255.255.0

load-interval 30

full-duplex

!



ip classless

ip route 10.0.35.0 255.255.255.0 Tunnel0

line con 0

line aux 0

line vty 0 4

end
```

Проверка результатов статического виртуального туннельного интерфейса IPsec: пример

В этом разделе содержатся сведения, которые можно использовать для подтверждения правильности работы конфигурации. В приведенном ниже примере туннель 0 включен, и протокол линии передачи данных также включен. Если протокол линии передачи данных отключен, сеанс неактивен.

Проверка состояния C7206

```
Router# show interface tunnel 0



Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 10.0.51.203/24

MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
```

```
reliability 255/255, txload 103/255, rxload 110/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.0.149.203, destination 10.0.149.217

Tunnel protocol/transport IPsec/IP, key disabled, sequencing disabled

Tunnel TTL 255


Checksumming of packets disabled, fast tunneling enabled

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Tunnel protection via IPsec (profile "P1")

Last input never, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

30 second input rate 13000 bits/sec, 34 packets/sec

30 second output rate 36000 bits/sec, 34 packets/sec

191320 packets input, 30129126 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

59968 packets output, 15369696 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 output buffer failures, 0 output buffers swapped out


Router# show crypto session


Crypto session current status

Interface: Tunnel0
```

```
Session status: UP-ACTIVE

Peer: 10.0.149.217 port 500

IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active

IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0

Active SAs: 4, origin: crypto map


Router# show ip route


Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.35.0/24 is directly connected, Ethernet3/3

S 10.0.36.0/24 is directly connected, Tunnel0

C 10.0.51.0/24 is directly connected, Tunnel0

C 10.0.149.0/24 is directly connected, Ethernet3/0
```

Статический интерфейс виртуальных туннелей с поддержкой VRF: пример

Чтобы добавить VRF к статическому VTI, включите в настройку команды **ipvrf** и **ip vrf forwarding**, как показано в следующем примере.

Конфигурация маршрутизатора C7206

```
hostname c7206

.

.

ip vrf sample-vti1
```

```
rd 1:1

route-target export 1:1

route-target import 1:1

!

.

.

interface Tunnel0

ip vrf forwarding sample-vti1

ip address 10.0.51.217 255.255.255.0

tunnel source 10.0.149.217

tunnel destination 10.0.149.203

tunnel mode ipsec ipv4

tunnel protection ipsec profile P1

.

.

!

end
```

Статический интерфейс виртуальных туннелей с QoS: пример

На конечной точке туннеля можно применить политику QoS , включив в туннельный интерфейс инструкцию **service-policy**. В следующем примере к исходящему трафику туннельного интерфейса применяется политика.

Конфигурация маршрутизатора C7206

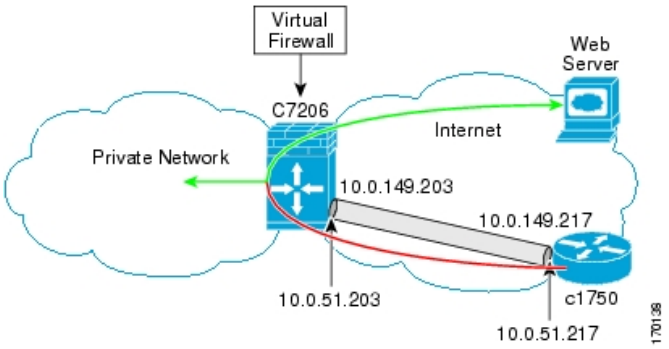
```
hostname c7206

.

.

class-map match-all VTI

match any

!

policy-map VTI
```

```
 class VTI

 police cir 2000000

   conform-action transmit

   exceed-action drop

!

.

.

interface Tunnel0

ip address 10.0.51.217 255.255.255.0

tunnel source 10.0.149.217

tunnel destination 10.0.149.203

tunnel mode ipsec ipv4

tunnel protection ipsec profile P1

service-policy output VTI

!

.

.

!

end
```

Статический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример

Использование виртуального брандмауэра в статическом туннеле VTI позволяет трафику оконечных устройств проходить через концентратор в Интернет. На рис. 6 показан статический VTI с оконечным устройством, защищенный корпоративным брандмауэром.

Рис 6. Статический VTI с виртуальным брандмауэром



Базовые настройки статического VTI можно изменить, включив в них описание виртуального брандмауэра.

Конфигурация маршрутизатора C7206

```
hostname c7206

.

.

ip inspect max-incomplete high 1000000

ip inspect max-incomplete low 800000

ip inspect one-minute high 1000000

ip inspect one-minute low 800000

ip inspect tcp synwait-time 60

ip inspect tcp max-incomplete host 100000 block-time 2

ip inspect name IOSFW1 tcp timeout 300

ip inspect name IOSFW1 udp

!

.

.

interface GigabitEthernet0/1

description Internet Connection

ip address 172.18.143.246 255.255.255.0

ip access-group 100 in

ip nat outside

!
```

```
interface Tunnel0

ip address 10.0.51.217 255.255.255.0

ip nat inside

ip inspect IOSFW1 in

tunnel source 10.0.149.217

tunnel destination 10.0.149.203

tunnel mode ipsec ipv4

tunnel protection ipsec profile P1

!

ip classless

ip route 0.0.0.0 0.0.0.0 172.18.143.1

!

ip nat translation timeout 120

ip nat translation finrst-timeout 2

ip nat translation max-entries 300000

ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0

ip nat inside source list 110 pool test1 vrf test-vti1 overload

!

access-list 100 permit esp any any

access-list 100 permit udp any eq isakmp any

access-list 100 permit udp any eq non500-isakmp any

access-list 100 permit icmp any any

access-list 110 deny   esp any any

access-list 110 deny   udp any eq isakmp any

access-list 110 permit ip any any

access-list 110 deny   udp any eq non500-isakmp any

!

end
```

Сервер Easy VPN с динамическим интерфейсом виртуальных туннелей: пример

В следующем примере показано использование сервера Easy VPN с DVTI, который работает как концентратор удаленного доступа IPsec. Клиент может быть домашним пользователем, запустившим клиент Cisco VPN, или маршрутизатором Cisco IOS, настроенным как клиент Easy VPN.

Конфигурация маршрутизатора C7206

```
hostname c7206

!

aaa new-model

aaa authentication login local_list local

aaa authorization network local_list local

aaa session-id common

!

ip subnet-zero

ip cef

!

username cisco password 0 cisco123

!

controller ISA 1/1

!

crypto isakmp policy 1

encr 3des

authentication pre-share

group 2

!

crypto isakmp client configuration group group1

key cisco123

pool group1pool

save-password
```

```
!
crypto isakmp profile vpn1-ra
  match identity group group1
  client authentication list local_list
  isakmp authorization list local_list
  client configuration address respond
  virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-3des esp-sha-hmac
!
crypto ipsec profile test-vti1
set transform-set VTI-TS
!
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
!
interface GigabitEthernet0/2
description Internal Network
ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/1
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
```

```
ip classless

ip route 0.0.0.0 0.0.0.0 172.18.143.1

!

end
```

Проверка результатов для сервера Easy VPN с динамическим интерфейсом виртуальных туннелей: пример

В следующих примерах показано, как можно настроить динамический VTI для сервера Easy VPN.

```
Router# show running-config interface Virtual-Access2


Building configuration...


Current configuration : 250 bytes

!

interface Virtual-Access2

ip unnumbered GigabitEthernet0/1

ip virtual-reassembly

tunnel source 172.18.143.246

tunnel destination 172.18.143.208

tunnel mode ipsec ipv4

tunnel protection ipsec profile test-vti1

no tunnel protection ipsec initiate

end


Router# show ip route


Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

      E1 - OSPF external type 1, E2 - OSPF external type 2

      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
      ia - IS-IS inter area, * - candidate default, U - per-user static route

      o - ODR, P - periodic downloaded static route


Gateway of last resort is 10.2.1.10 to network 0.0.0.0


    172.18.0.0/24 is subnetted, 1 subnets

C       172.18.143.0 is directly connected, GigabitEthernet0/1

    192.168.1.0/32 is subnetted, 1 subnets

S       192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2

    10.0.0.0/24 is subnetted, 1 subnets

C       10.2.1.0 is directly connected, GigabitEthernet0/2

S*   0.0.0.0/0 [1/0] via 172.18.143.1
```

Клиент Easy VPN с динамическим интерфейсом виртуальных туннелей: пример

В следующем примере показано, как можно настроить маршрутизатор в качестве клиента Easy VPN. В примере используются в основном те же принципы, что и для клиента Easy VPN, который можно запустить на ПК для организации связи. Фактически конфигурация сервера Easy VPN будет работать и для программного клиента, и для клиента — Cisco IOS.

```
hostname c1841

!

no aaa new-model

!

ip cef

!

username cisco password 0 cisco123

!

crypto ipsec client ezvpn CLIENT

connect manual

group group1 key cisco123

mode client

peer 172.18.143.246
```

```
virtual-interface 1

username cisco password cisco123

xauth userid mode local

!

interface Loopback0

ip address 10.1.1.1 255.255.255.255

!

interface FastEthernet0/0

description Internet Connection

ip address 172.18.143.208 255.255.255.0

crypto ipsec client ezvpn CLIENT

!

interface FastEthernet0/1

ip address 10.1.1.252 255.255.255.0

crypto ipsec client ezvpn CLIENT inside

!

interface Virtual-Template1 type tunnel

ip unnumbered Loopback0

!

ip route 0.0.0.0 0.0.0.0 172.18.143.1

!

end
```

Определить клиент можно различными способами. Режим, определяемый командой **connect**, может быть автоматическим или ручным. Если установлен ручной режим, туннель IPsec инициируется пользователем вручную.

Также обратите внимание на использование команды **mode**. Возможные режимы: клиент (client), расширение сети (network-extension) или дополнительное расширение сети (network-extension-plus). В этом примере демонстрируется режим клиента; это означает, что сервер передает клиенту частный адрес. Режим расширения сети отличается от режима клиента тем, что клиент определяет для сервера присоединенную частную подсеть. В зависимости от режима таблицы маршрутизации на каждом из концов будут немного отличаться друг от друга. Основные операции с туннелем IPSec остаются одинаковыми вне зависимости от режима.

Проверка результатов для сервера Easy VPN с динамическим интерфейсом виртуальных туннелей: пример

Следующие примеры иллюстрируют различные способы отображения состояния интерфейса DVTI.

```
Router# show running-config interface Virtual-Access2

Building configuration...

Current configuration : 148 bytes
!
interface Virtual-Access2
ip unnumbered Loopback1
tunnel source FastEthernet0/0
tunnel destination 172.18.143.246
tunnel mode ipsec ipv4
end

Router# show running-config interface Loopback1

Building configuration...

Current configuration : 65 bytes
!
interface Loopback1
ip address 192.168.1.1 255.255.255.255
end

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
      E1 - OSPF external type 1, E2 - OSPF external type 2

      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

      ia - IS-IS inter area, * - candidate default, U - per-user static route

      o - ODR, P - periodic downloaded static route


Gateway of last resort is 172.18.143.1 to network 0.0.0.0


    10.0.0.0/32 is subnetted, 1 subnets

C       10.1.1.1 is directly connected, Loopback0

    172.18.0.0/24 is subnetted, 1 subnets

C       172.18.143.0 is directly connected, FastEthernet0/0

    192.168.1.0/32 is subnetted, 1 subnets

C       192.168.1.1 is directly connected, Loopback1

S*   0.0.0.0/0 [1/0] via 172.18.143.1

               [1/0] via 0.0.0.0, Virtual-Access2


Router# show crypto ipsec client ezvpn


Easy VPN Remote Phase: 6


Tunnel name : CLIENT

Inside interface list: FastEthernet0/1

Outside interface: Virtual-Access2 (bound to FastEthernet0/0)

Current State: IPSEC_ACTIVE

Last Event: SOCKET_UP

Address: 192.168.1.1

Mask: 255.255.255.255

Save Password: Allowed

Current EzVPN Peer: 172.18.143.246
```

IPsec с поддержкой VRF с динамическим интерфейсом VTI: пример

В этом примере показано, как настраивать IPsec с поддержкой VRF, чтобы воспользоваться преимуществами динамического VTI:

```
hostname c7206

.

.

ip vrf test-vti1

rd 1:1

route-target export 1:1

route-target import 1:1

!

.

.

interface Virtual-Template1 type tunnel

ip vrf forwarding test-vti1

ip unnumbered Loopback0

ip virtual-reassembly

tunnel mode ipsec ipv4

tunnel protection ipsec profile test-vti1

!

.

.

end
```

Динамический интерфейс виртуальных туннелей с виртуальным брандмауэром: пример

Сервер Easy VPN с DVTI может настраиваться за виртуальным брандмауэром. Конфигурация с брандмауэром позволяет пользователям входить в сеть, когда сетевой брандмауэр защищен от неавторизованного доступа. По отношению к интерфейсу Интернета и виртуальным шаблонам виртуальный брандмауэр использует контроль доступа на основе контекста (Context-Based Access Control, CBAC) и NAT.

```
hostname c7206
```

```
.

.

ip inspect max-incomplete high 1000000

ip inspect max-incomplete low 800000

ip inspect one-minute high 1000000

ip inspect one-minute low 800000

ip inspect tcp synwait-time 60

ip inspect tcp max-incomplete host 100000 block-time 2

ip inspect name IOSFW1 tcp timeout 300

ip inspect name IOSFW1 udp

!

.

.

interface GigabitEthernet0/1

description Internet Connection

ip address 172.18.143.246 255.255.255.0

ip access-group 100 in

ip nat outside

!

interface GigabitEthernet0/2

description Internal Network

ip address 10.2.1.1 255.255.255.0

!

interface Virtual-Template1 type tunnel

ip unnumbered Loopback0

ip nat inside

ip inspect IOSFW1 in

tunnel mode ipsec ipv4
```

```
tunnel protection ipsec profile test-vti1

!

ip classless

ip route 0.0.0.0 0.0.0.0 172.18.143.1

!

ip nat translation timeout 120

ip nat translation finrst-timeout 2

ip nat translation max-entries 300000

ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0

ip nat inside source list 110 pool test1 vrf test-vti1 overload

!

access-list 100 permit esp any any

access-list 100 permit udp any eq isakmp any

access-list 100 permit udp any eq non500-isakmp any

access-list 100 permit icmp any any

access-list 110 deny   esp any any

access-list 110 deny   udp any eq isakmp any

access-list 110 permit ip any any

access-list 110 deny   udp any eq non500-isakmp any

!

end
```

Динамический интерфейс виртуальных туннелей с QoS: пример

Существует возможность добавить QoS к туннелям DVTI, применив политику служб к виртуальному шаблону. При клонировании шаблона для создания виртуального интерфейса доступа к нему применяется политика служб. В следующем примере показана базовая конфигурация DVTI с добавленным механизмом QoS.

```
hostname c7206

.

.

class-map match-all VTI
```

```
match any

!

policy-map VTI

 class VTI

 police cir 2000000

   conform-action transmit

   exceed-action drop

!

.

.

interface Virtual-Template1 type tunnel

ip vrf forwarding test-vti1

ip unnumbered Loopback0

ip virtual-reassembly

tunnel mode ipsec ipv4

tunnel protection ipsec profile test-vti1

service-policy output VTI

!

.

.

!

end
```

Атрибуты пользователей на сервере Easy VPN: пример

В следующем примере показана настройка атрибутов пользователей на сервере Easy VPN.

```
!


aaa new-model
```

```
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
username example password 0 example
!
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
```

```
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny   icmp any any
logging alarm informational
logging trap debugging
!
control-plane
!
gatekeeper
```

```
 shutdown
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end
```

Дополнительные ссылки

В следующем разделе приведены ссылки, относящиеся к интерфейсам виртуальных туннелей с IPsec.

Дополнительная документация

Смежные темы	Название документа
IPsec, вопросы безопасности	*Руководство по конфигурации системы безопасности Cisco IOS*
Команды системы безопасности	*Справочник по командам системы безопасности Cisco IOS*
Конфигурация VPN	*Cisco IOS для сервера Easy VPN* Cisco IOS для удаленного устройства Easy VPN

Стандарты

Стандарт	Название
Эта функциональная возможность не поддерживает новые или измененные стандарты и не изменила поддержки существующих стандартов.	—

Базы данных MIB

База данных MIB	Ссылка на базы данных MIB
Эта функциональная возможность не поддерживает новые или измененные базы данных MIB и не изменила поддержки существующих баз данных MIB.	Для поиска и загрузки баз данных управляющей информации (Management Information Base, MIB) для выбранных платформ, версий программного обеспечения Cisco IOS и наборов характеристик воспользуйтесь страницей поиска баз данных Cisco MIB Locator по следующему адресу:

	http://www.cisco.com/go/mibs

Документы RFC

Документ RFC	Наименование
RFC 2401	*Архитектура безопасности для протокола IP*
RFC 2408	*Протокол управления сопоставлениями безопасности и ключами в Интернете*
RFC 2409	*Обмен ключами в Интернете (IKE)*

Техническая поддержка

Описание	Ссылка
Веб-сайт технической поддержки и документации компании Cisco содержит тысячи страниц технической информации с возможностью поиска, включая ссылки на продукты, технологии, решения, технические советы, инструменты и техническую документацию. Зарегистрированные пользователи веб-сайта cisco.com могут войти в систему с этой страницы и получить еще более обширную информацию.	http://www.cisco.com/techsupport

Справочник по командам

В этом разделе описаны только новые и измененные команды.

- **crypto aaa attribute list**
- crypto isakmp client configuration group
- **show vtemplate**
- interface virtual-template
- tunnel mode
- tunnel mode
- **virtual-template**

crypto aaa attribute list

Для определения списка атрибутов для аутентификации, авторизации и работы с учетными записями (AAA) для пользователя на локальном сервере Easy VPN используйте команду **crypto aaa attribute list** в режиме настройки группы crypto isakmp. Чтобы удалить список атрибутов AAA, используйте форму **no** этой команды.

crypto aaa attribute list *list-name*

no crypto aaa attribute list *list-name*

Описание синтаксиса

list-name	Имя локального списка атрибутов.

По умолчанию:

Локальный список атрибутов не определен.

Командные режимы

Конфигурация группы crypto isakmp

История команды

Версия	Изменение
12.4(9)T	Команда включена впервые.

Инструкции по использованию

Число списков, которые можно определить, не ограничено (за исключением пределов емкости памяти NVRAM).

Примеры

Следующий пример демонстрирует настройку атрибутов пользователей на локальном сервере Easy VPN AAA:

```
!



aaa new-model

!

!

aaa authentication login default local

aaa authentication login noAAA none
```

```
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
username example password 0 example
!
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
```

```
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
```

```
 speed auto
 media-type rj45
 no negotiation auto

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny   icmp any any
logging alarm informational
logging trap debugging
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
```

```
line aux 0

 stopbits 1

line vty 0 4

!

!

end
```

Связанные команды

Команда	Описание
crypto isakmp client configuration group	Указывает, для какой группы будет определен профиль политики.

crypto isakmp client configuration group

Чтобы определить, для какой группы будет определен профиль политики, и войти в режим настройки группы crypto ISAKMP, используйте команду **crypto isakmp client configuration group** в режиме глобальной конфигурации. Чтобы удалить эту команду и все связанные с ней подкоманды, используйте форму **no** этой команды.

crypto isakmp client configuration group {*group-name* | **default**}

no **crypto isakmp client configuration group**

Описание синтаксиса

group-name	Определение группы, которое идентифицирует политику, проводимую пользователями.
По умолчанию	Политика, осуществляемая для всех пользователей, не принадлежащих к группе, имя которой совпадает с аргументом *group-name* . Ключевое слово **default** может настраиваться только локально.

По умолчанию

Нет поведения или значений по умолчанию.

Командные режимы

Глобальная конфигурация

История команды

Версия	Изменение
12.2(8)T	Команда включена впервые.
12.3(2)T	Добавлены команды **access-restrict**, **firewall are-u-there**, **group-lock**, **include-local-lan** и **save-password**. Эти команды добавлены в ходе настройки режимов. Кроме того, эти команды изменены так, что вывод этих команд будет показывать, зашифрован ли предварительный ключ.
12.3(4)T	Добавлены команды **backup-gateway**, **max-logins**, **max-users** и **pfs**.
12.2(18)SXD	Эта команда была добавлена в Cisco IOS версии 12.2(18)SXD.
12.4(2)T	Добавлена команда **browser-proxy**.
12.4(6)T	Добавлена команда **firewall policy**.
12.2(33)SRA	Эта команда была добавлена в Cisco IOS версии 12.2(33)SRA.
12.4(9)T	Добавлены команды **crypto aaa attribute list**, **dhcp-server** и **dhcp-timeout**.

Инструкции по использованию

Используйте команду **crypto isakmp client configuration group** для определения информации о групповой политике, которую необходимо определить или изменить. Может потребоваться изменение групповой политики маршрутизатора для связи с клиентом с использованием ID группы, который не совпадает с аргументом *group-name* .

После выполнения этой команды, которая помещает пользователя в режим настройки протокола управления сопоставлениями безопасности и ключами в Интернете (ISAKMP) для группы, можно определять характеристики групповой политики с использованием следующих команд:

- **access-restrict** — связывает указанную группу виртуальной частной сети (VPN) с указанным интерфейсом для доступа к шлюзу Cisco IOS и службам, которые он защищает.
- **acl** — настраивает раздельное туннелирование.
- **auto-update-client** — настраивает автоматическое обновление.
- **backup-gateway** — настраивает сервер для передачи клиенту очередного списка резервных шлюзов. Эти шлюзы используются по порядку списка в случае сбоя предыдущего шлюза. Шлюзы можно определять с помощью IP-адресов или имен узлов.
- **banner** — определяет заголовок режима настройки.
- **browser-proxy** — использует для группы отображение browser-proxy.
- **configuration url** — определяет для сервера URL-адрес, который удаленное устройство Easy VPN использует для получения конфигурации при смене режима конфигурации.

- **configuration version** — определяет для сервера версию, которую должно использовать удаленное устройство Cisco Easy VPN для получения конкретной конфигурации при смене режима конфигурации.

- **crypto aaa attribute list** — определяет список атрибутов AAA для атрибутов пользователей локального сервера Easy VPN.

- **dhcp server** — настраивает несколько записей сервера DHCP.

- **dhcp timeout** — управляет временем ожидания до вызова следующего сервера DHCP в списке.

- **dns** — определяет первичный и вторичный DNS-серверы для группы.

- **domain** — определяет членство в домене группы.

- **firewall are-u-there —** добавляет атрибут Firewall-Are-U-There в группу сервера, если на ПК работает брандмауэр Black Ice или Zone Alarm.

- **firewall policy** — определяет политику брандмауэра по помещению имен в стек CPP для группы конфигурации клиентов с крипто-ISAKMP локального сервера AAA.

- **group-lock** — используется, если в управлении ключами в Интернете (IKE) применяется аутентификация по предварительному ключу. Позволяет вводить имя пользователя для расширенной аутентификации (Xauth). Разделитель группы сравнивается с идентификатором группы, посылаемым в энергичном режиме IKE.

- **include-local-lan** — настраивает атрибут Include-Local-LAN, позволяющий производить соединение туннелями без разделения для доступа к локальной подсети одновременно с клиентом.

- **key** — определяет предварительный ключ IKE при определении информации о групповой политике для помещения в стек настроек режима.

- **max-logins** — ограничивает число одновременных подключений пользователей к системе для указанной группы пользователей.

- **max-users** — ограничивает число соединений с указанной серверной группой.

- **netmask** — маска подсети, используемая клиентом для локального соединения.

- **pfs** — настраивает сервер так, чтобы он уведомлял клиента о политике центрального узла относительно необходимости PFS для каждой SA IPsec. Поскольку клиентское устройство не имеет параметра интерфейса пользователя, позволяющего включать или отключать согласование PFS, сервер будет уведомлять клиентское устройство о политике центрального узла через этот параметр. Группа Диффи-Хеллмана (D-H), предоставляемая для PFS, будет той же самой, что обсуждалась в фазе 1 согласования IKE.

- **pool** — указывает на адрес локального пула IP, используемого для выделения клиентам внутренних IP-адресов.

- **save-password** — сохраняет пароль Xauth локально на ПК пользователя.

- **split-dns** — определяет список доменных имен, которые необходимо туннелировать или разрешать в частную сеть.

- **wins** — определяет первичный и вторичный серверы Windows-службы имен Интернет (WINS) для группы.

Вывод команды **crypto isakmp client configuration group** (при использовании подкоманды **key**) покажет, зашифрован ли предварительный ключ. Пример вывода для нешифрованного предварительного ключа:

```
crypto isakmp client configuration group key test
```

Пример вывода зашифрованного предварительного ключа типа 6:

crypto isakmp client configuration group

```
 key 6 JK_JHZPeJV_XFZTKCQFYAAB
```

Отслеживание и ограничения сеанса для клиента Easy VPN

Существует возможность моделирования предоставляемой некоторыми серверами RADIUS функциональности по ограничению числа соединений с указанной группой сервера, а также ограничению числа одновременных подключений для пользователей в этой группе.

Для ограничения числа соединений с указанной группой сервера используйте подкоманду **max-users**. Для ограничения одновременного входа в систему пользователей в серверной группе используйте подкоманду **max-logins**.

Следующие примеры показывают пары атрибут-значение (AV) RADIUS для максимального числа пользователей и подключений:

```
ipsec:max-users=1000
```

```
ipsec:max-logins=1
```

Команды **max-users** и **max-logins** могут использоваться вместе или по отдельности для управления использованием ресурсов любыми группами или отдельными пользователями.

При использовании сервера RADIUS, например, сервера контроля доступа (ACS) CiscoSecure, рекомендуется активировать контроль над сеансами на сервере RADIUS, если он предлагает такую функциональность. Таким образом можно управлять использованием нескольких серверов при помощи одного центрального хранилища. При включении этой функции на самом маршрутизаторе отслеживаются только подключения к группам на данном устройстве, поэтому для него невозможно точно рассчитать сценарии разделения загрузки.

Примеры

В следующем примере показано, как определить информацию о групповой политике для помещения в стек настроек режима. В этом примере имя первой группы — «cisco», второй группы — «default». Таким образом, политика по умолчанию будет применяться для всех пользователей, не относящихся к группе, имя которой не соответствует «cisco».

```
crypto isakmp client configuration group cisco
```

```
key cisco
```

```
dns 10.2.2.2 10.2.2.3
```

```
wins 10.6.6.6
```

```
domain cisco.com
```

```
pool fred

acl 199

!

crypto isakmp client configuration group default

key cisco

dns 10.2.2.2 10.3.2.3

pool fred

acl 199
```

Связанные команды

Команда	Описание
access-restrict	Связывает указанную группу виртуальной частной сети (VPN) с указанным интерфейсом для доступа к шлюзу Cisco IOS и службам, которые он защищает.
acl	Настраивает раздельное туннелирование.
backup-gateway	Настраивает сервер для передачи клиенту очередного списка резервных шлюзов.
browser-proxy	Использует значение параметра browser-proxy для группы.
crypto isakmp keepalive	Добавляет атрибут Firewall-Are-U-There в группу сервера, если на ПК работает брандмауэр Black Ice или Zone Alarm.
dns	Определяет первичный и вторичный DNS-серверы.
domain (isakmp-group)	Определяет домен DNS, к которому принадлежит группа.
firewall are-u-there	Добавляет атрибут Firewall-Are-U-There в группу сервера, если на ПК работает брандмауэр Black Ice или Zone Alarm.
firewall policy	Определяет политику брандмауэра по помещению имен в стек CPP для группы конфигурации клиентов с крипто-ISAKMP локального сервера AAA.
group-lock	Позволяет ввести имя пользователя Xauth, в том числе имя группы, если в IKE используется аутентификация с предварительным ключом.
include-local-lan	Настраивает атрибут Include-Local-LAN, позволяющий производить соединение туннелями без разделения для доступа к локальной подсети одновременно с клиентом.

key (isakmp-group)	Определяет предварительный ключ IKE для определения атрибута Group-Policy.
max-logins	Ограничивает число одновременных подключений пользователей к системе для указанной серверной группы.
max-users	Ограничивает число соединений с указанной серверной группой.
pool (isakmp-group)	Определяет адрес локального пула.
save-password	Сохраняет пароль Xauth локально на ПК пользователя.
set aggressive-mode client-endpoint	Определяет атрибут Tunnel-Client-Endpoint для конфигурации узлов ISAKMP.

crypto isakmp profile

Для определения профиля протокола управления сопоставлениями безопасности и ключами в Интернете (ISAKMP) и аудита пользовательских сеансов IPsec используйте команду **crypto isakmp profile** в режиме глобальной конфигурации. Чтобы удалить профиль крипто-ISAKMP используйте форму **no** этой команды.

crypto isakmp profile *profile-name* [**accounting** *aaa-list*]

no crypto isakmp profile *profile-name* [**accounting** *aaa-list*]

Описание синтаксиса

profile-name	Имя профиля пользователя. Чтобы ассоциировать профиль пользователя с сервером RADIUS необходимо идентифицировать имя профиля пользователя.
accounting *aaa-list*	(Необязательно) Имя списка учетных записей клиентов.

По умолчанию

Если команда не использована, профили отсутствуют.

Командные режимы

Глобальная конфигурация

История команды

Версия	Изменение
12.2(15)T	Команда включена впервые.
12.2(18)SXD	Эта команда была добавлена в Cisco IOS версии 12.2(18)SXD.
12.4(2)T	Добавлена поддержка динамических виртуальных туннельных интерфейсов.
12.4(4)T	Добавлена поддержка IPv6.
12.2(33)SRA	Эта команда была добавлена в Cisco IOS версии 12.2(33)SRA.

Инструкции по использованию

Определение профиля ISAKMP

Профиль ISAKMP можно рассматривать как хранилище команд фазы 1 и фазы 1.5 для набора одноранговых узлов. Конфигурация фазы 1 включает команды для настройки таких вещей, как поддержка установленного соединения, сопоставление идентичности и список авторизации. Конфигурация фазы 1.5 включает команды для настройки таких вещей, как расширенная аутентификация (Xauth) и настройка режима.

Узлы отображаются на профиль ISAKMP, если их идентификаторы (указанные в полезной нагрузке идентификации [ID] обмена ключами в Интернете [IKE]) совпадают с идентификаторами, определенными в профиле ISAKMP. Для однозначного отображения на профиль ISAKMP два профиля ISAKMP не должны содержать одинаковые идентификаторы. Если идентификаторы узла в двух профилях ISAKMP совпадают, конфигурация недействительна. Кроме того, чтобы профиль ISAKMP был полным, в нем должно быть не менее одной команды **match identity**.

После выполнения этой команды и входа в режим настройки профиля ISAKMP можно настраивать следующие команды:

- **accounting** — включает аутентификацию, авторизацию и учет (AAA).
- **ca trust-point** — определяет центры сертификации.
- **client** — определяет параметры конфигурации клиента.
- **default** — выводит подкоманды для команды **crypto isakmp profile**.
- **description** — задает описание этого профиля.
- **initiate mode** — инициирует режим.
- **isakmp authorization** — параметры авторизации ISAKMP.
- **keepalive** — устанавливает интервал поддержки установленного соединения.
- **keyring** — задает хранилище ключей.
- **local-address** — определяет интерфейс, используемый в качестве локального адреса в данном профиле ISAKMP.

- **match** — сопоставляет значения узла.
- **qos-group** — использует для данного профиля карту класса политики качества обслуживания (QoS).
- **self-identity** — определяет идентификатор.
- **virtual-template** — определяет виртуальный шаблон динамического интерфейса.
- **vrf** — определяет экземпляр маршрутизации и пересылки в виртуальной частной сети (VRF), к которой относится профиль.

Проверка пользовательских сеансов IPSec

Используйте эту команду для проверки различных пользовательских сеансов, заканчивающихся на шлюзе IPSec.

Примечание. Команды **crypto isakmp profile** и **crypto map (global IPSec)** являются взаимоисключающими. Если имеется профиль (была использована команда **crypto isakmp profile)** без учетных записей, но с глобальной командой (команда **crypto isakmp profile** без ключевого слова **accounting**), учет будет производиться с использованием атрибутов глобальной команды.

Динамические интерфейсы виртуальных туннелей

Поддержка динамических виртуальных туннельных интерфейсов позволяет отображать виртуальный профиль на определенные виртуальные шаблоны.

Примеры

Пример сопоставления профиля ISAKAMP и идентификаторов узлов

В следующем примере показано, как определить профиль ISAKMP и сопоставить идентификаторы узлов:

```
crypto isakmp profile vpnprofile

match identity address 10.76.11.53
```

Пример профиля ISAKAMP с учетом

В следующем примере учета показано, что настроен профиль ISAKMP:

```
aaa new-model

!

!

aaa authentication login cisco-client group radius
```

```
aaa authorization network cisco-client group radius

aaa accounting network acc start-stop broadcast group radius

aaa session-id common

!

crypto isakmp profile cisco

vrf cisco

match identity group cclient

 client authentication list cisco-client

 isakmp authorization list cisco-client

 client configuration address respond

 accounting acc

!

crypto dynamic-map dynamic 1

set transform-set aswan

set isakmp-profile cisco

reverse-route

!

!

radius-server host 172.16.1.4 auth-port 1645 acct-port 1646

radius-server key nsite
```

Связанные команды

Команда	Описание
crypto map (global IPsec)	Входит в режим настройки криптокарты и создает или изменяет запись криптокарты, создает криптопрофиль, который содержит шаблон для настройки динамически создаваемых криптокарт, либо настраивает список учетных записей клиентов.
debug crypto isakmp	Выводит сообщения о событиях IKE.
match identity	Ищет идентификатор узла в профиле ISAKMP.
tunnel	Связывает туннельный интерфейс с профилем IPsec.

protection	
virtual template	Указывает, какой виртуальный шаблон будет использоваться для клонирования интерфейсов виртуального доступа.

interface virtual-template

Для создания шаблона виртуального интерфейса, который можно динамически настраивать и использовать для создания интерфейса виртуального доступа используйте команду **interface virtual-template** в режиме глобальной конфигурации. Для удаления шаблона виртуального интерфейса используйте форму **no** этой команды.

interface virtual-template number

no **interface virtual-template** *number*

Описание синтаксиса

number	Номер, используемый для идентификации шаблона виртуального интерфейса. Можно настраивать до 200 шаблонов виртуального интерфейса.

По умолчанию:

Определенные шаблоны виртуальных интерфейсов отсутствуют.

Командные режимы

Глобальная конфигурация

История команды

Версия	Изменение
11.2F	Команда включена впервые.
12.2(4)T	Команда расширена для увеличения максимального числа шаблонов виртуальных интерфейсов с 25 до 200.
12.2(28)SB	Эта команда была добавлена в Cisco IOS версии 12.2(28)SB.
12.2(33)SRA	Эта команда была добавлена в Cisco IOS версии 12.2(33)SRA.

Инструкции по использованию

Шаблон виртуального интерфейса используется для настройки динамически создаваемых интерфейсов виртуального доступа. Он создается пользователями и может сохраняться в памяти NVRAM.

После создания шаблона виртуального интерфейса его можно настроить так же, как последовательный интерфейс.

Шаблоны виртуальных интерфейсов могут создаваться и использоваться в различных целях, например, как виртуальные профили, в виртуальных частных сетях с коммутируемым доступом (VPDN), PPP через ATM, трансляции протоколов и многоблочного многоканального PPP (MMP).

Примеры

Пример виртуального шаблона с аутентификацией PPP

В следующем примере создается и настраивается шаблон виртуального интерфейса 1:

```
interface virtual-template 1 type ethernet

ip unnumbered ethernet 0

ppp multilink

ppp authentication chap
```

Пример виртуального шаблона IPsec

В следующем примере показано, как настраивать виртуальный шаблон для виртуального туннельного интерфейса IPsec.

```
interface virtual-template1 type tunnel

 ip unnumbered Loopback1

 tunnel mode ipsec ipv4

 tunnel protection ipsec profile virtualtunnelinterface
```

Связанные команды

Команда	Описание
tunnel protection	Связывание туннельного интерфейса с профилем IPsec.
virtual interface	Устанавливает имя зоны для присоединенной сети AppleTalk.
virtual template	Определяет точку назначения туннельного интерфейса.

show vtemplate

Для вывода информации обо всех настроенных виртуальных шаблонах используйте команду **show vtemplate** в привилегированном режиме EXEC.

show vtemplate

Описание синтаксиса

У команды нет аргументов и ключевых слов.

Командные режимы

Привилегированный режим EXEC

История команды

Версия	Изменение
12.0(7)DC	Эта команда была введена на серии Cisco 6400 NRP.
12.2(13)T	Эта команда была добавлена в Cisco IOS Release 12.2(13)SRA.
12.3(14)T	Представление вывода было изменено для вывода типа интерфейса виртуального шаблона и счетчиков интерфейсов по их типам для виртуальных туннельных интерфейсов IPsec.
12.2(33)SRA	Эта команда была добавлена в Cisco IOS Release 12.2(33)SRA.

Примеры

Ниже приводится пример вывода для команды **show vtemplate**:

```
Router# show vtemplate


Virtual access subinterface creation is globally enabled


        Active     Active    Subint  Pre-clone Pre-clone Interface

      Interface Subinterface Capable Available   Limit     Type

      --------- ------------ ------- --------- --------- ---------

Vt1           0            0   Yes          --        --   Serial

Vt2           0            0   Yes          --        --   Serial

Vt4           0            0   Yes          --        --   Serial

Vt21          0            0    No          --        --   Tunnel
```

```
Vt22           0            0   Yes          --        --   Ether

Vt23           0            0   Yes          --        --   Serial

Vt24           0            0   Yes          --        --   Serial


Usage Summary

                            Interface   Subinterface

                            ---------   ------------

Current Serial  in use                1              0

Current Serial  free                  0              3

Current Ether   in use                0              0

Current Ether   free                  0              0

Current Tunnel  in use                0              0

Current Tunnel  free                  0              0

Total                                 1              3


Cumulative created                    8              4

Cumulative freed                      0              4


Base virtual access interfaces: 1

Total create or clone requests: 0

Current request queue size: 0

Current free pending: 0


Maximum request duration: 0 msec

Average request duration: 0 msec

Last request duration: 0 msec


Maximum processing duration: 0 msec

Average processing duration: 0 msec

Last processing duration: 0 msec
```

```
Last processing duration:0 msec
```

Таблица 1 описывает важные поля, имеющиеся в примере.

Поле	Описание
Virtual access subinterface creation is globally...	Настроенные параметры команды **virtual-template**. Создание субинтерфейсов виртуального доступа можно включить или отключить.
Active Interface	Число интерфейсов виртуального доступа, клонированных из указанного виртуального шаблона.
Active Subinterface	Число субинтерфейсов виртуального доступа, клонированных из указанного виртуального шаблона.
Subint Capable	Указывает, допускает ли конфигурация виртуального шаблона поддержку субинтерфейсов виртуального доступа.
Pre-clone Available	Число предварительно клонированных интерфейсов виртуального доступа, которые можно использовать в данный момент в конкретном виртуальном шаблоне.
Pre-clone Limit	Число предварительно клонированных интерфейсов виртуального доступа, которые можно использовать в конкретном виртуальном шаблоне.
Current in use	Число используемых в настоящий момент интерфейсов и субинтерфейсов виртуального доступа.
Current free	Число не используемых более интерфейсов и субинтерфейсов виртуального доступа.
Total	Общее число созданных интерфейсов и субинтерфейсов виртуального доступа.
Cumulative created	Число удовлетворенных запросов к интерфейсам и субинтерфейсам виртуального доступа.
Cumulative freed	Число освобождений приложений, использовавших интерфейсы и субинтерфейсы виртуального доступа.
Base virtual-access interfaces	Это поле содержит число базовых интерфейсов виртуального доступа. Базовый интерфейс виртуального доступа используется для создания субинтерфейсов виртуального доступа. На приложение, поддерживающее субинтерфейсы, имеется один базовый интерфейс виртуального доступа. Базовый интерфейс виртуального доступа можно идентифицировать из вывода результатов работы команды **show interfaces virtual-access**.

Total create or clone requests	Число запросов, сделанных через API асинхронных запросов диспетчера виртуальных шаблонов.
Current request queue size	Число элементов в рабочей очереди диспетчера виртуальных шаблонов.
Current free pending	Число интерфейсов виртуального доступа, ожидающих окончательного освобождения. Эти интерфейсы виртуального доступа не могут быть освобождены в настоящий момент, потому что они продолжают использоваться.
Maximum request duration	Максимальное время, прошедшее с момента создания асинхронного запроса до прихода уведомления о выполнении запроса от приложения.
Average request duration	Среднее время, прошедшее с момента создания асинхронного запроса до прихода уведомления о выполнении запроса от приложения.
Last request duration	Время, прошедшее с момента создания асинхронного запроса до прихода уведомления о выполнении запроса от приложения для последнего запроса.
Maximum processing duration	Максимальное время, потраченное диспетчером виртуальных запросов на удовлетворение запроса.
Average processing duration	Среднее время, требуемое диспетчеру виртуальных запросов для удовлетворения запроса.
Last processing duration	Время, потраченное диспетчером виртуальных запросов на удовлетворение последнего запроса.

Связанные команды

Команда	Описание
show interfaces virtual-access	Выводит состояние, данные о трафике и сведения о конфигурации указанного интерфейса виртуального доступа.
virtual-template	Указывает, какой виртуальный шаблон был использован для клонирования интерфейсов виртуального доступа.

tunnel mode

Для задания режима инкапсуляции для туннельного интерфейса используйте команду **tunnel mode** в режиме настройки интерфейса. Для восстановления режима по умолчанию воспользуйтесь формой **no** этой команды.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** |

ipsec ipv6 | **mpls** | **nos** | **rbscp**}

no tunnel mode

Описание синтаксиса

aurp	Протокол маршрутизации на основе обновления AppleTalk
cayman	Инкапсуляция Cayman TunnelTalk для протокола AppleTalk.
dvmrp	Протокол мультиадресной маршрутизации по методу вектора расстояния.
eon	Туннель совместимого с EON сетевого протокола без предварительного соединения (CLNS).
gre	Протокол общей инкапсуляции маршрутов (GRE). Это значение используется по умолчанию.
gre multipoint	Многоточечный GRE (mGRE).
gre ipv6	Туннелирование GRE с использованием IPv6 в качестве протокола доставки.
ipip	Инкапсуляция IP-по-IP.
decapsulate-any	(Необязательно) Разъединяет любое количество туннелей IP-в-IP, построенных на основе одного туннельного интерфейса. По такому туннелю не будет передаваться исходящий трафик, однако любое количество удаленных конечных точек могут использовать настроенный таким образом туннель в качестве своей точки назначения.
ipsec ipv4	Туннельный режим — IPSec, транспортный протокол — IPv4.
iptalk	Инкапсуляция Apple IPTalk.
ipv6	Статический туннельный интерфейс, настроенный на инкапсуляцию пакетов IPv6 или IPv4 в IPv6.
ipsec ipv6	Туннельный режим — IPSec, транспортный протокол — IPv6.
mpls	Инкапсуляция с помощью многопротокольной коммутации по меткам (MPLS):
nos	KA9Q/NOS-совместимая IP через IP:
rbscp	Протокол управления на базе скорости передачи для спутниковой связи (RBSCP).

По умолчанию

Туннелирование GRE

Командные режимы

Настройка интерфейса

История команды

Версия	Изменение
10.0	Команда включена впервые.
10.3	Добавлены ключевые слова **aurp**, **dvmrp** и **ipip**.
11.2	Добавлено необязательное ключевое слово **decapsulate-any**.
12.2(13)T	Добавлено ключевое слово **gre multipoint**.
12.3(7)T	Добавлены следующие ключевые слова: • **gre ipv6** для поддержки туннелирования GRE с использованием IPv6 в качестве протокола доставки. • **ipv6** для настройки статических туннельных интерфейсов на инкапсуляцию пакетов IPv6 и IPv4 в IPv6. • **rbscp** для поддержки RBSCP.
12.3(14)T	Добавлено ключевое слово **ipsec ipv4**.
12.2(18)SXE	Добавлено ключевое слово **gre multipoint**.
12.2(30)S	Эта команда была добавлена в Cisco IOS Release 12.2(30)S.
12.4(4)T	Добавлено ключевое слово **ipsec ipv6**.
12.2(33)SRA	Эта команда была добавлена в Cisco IOS версии 12.2(33)SRA.

Инструкции по использованию

Адрес узла-источника и узла назначения

Нельзя иметь два туннеля с одинаковым режимом инкапсуляции, которые имеют одинаковые адреса узла-источника и узла назначения. Обходным путем эту проблему можно решить при помощи создания петлевого интерфейса и выхода пакетов из петлевого интерфейса.

Туннелирование Cayman

Разработанное компанией Cayman Systems туннелирование Cayman реализует туннелирование, позволяющее маршрутизаторам Cisco работать с устройствами Cayman GatorBox. При туннелировании Cayman можно организовывать туннели между двумя маршрутизаторами или между маршрутизатором Cisco и GatorBox. При использовании туннелирования Cayman нет необходимости настраивать туннель с использованием сетевого адреса AppleTalk.

DVMRP

Используйте DVMRP, когда маршрутизатор соединяется с mrouted (мультиадресным) маршрутизатором для запуска DVMRP через туннель. Необходимо настраивать протокол мультиадресной передачи PIM (мультиадресная передача, не зависящая от протокола) и IP-адрес туннеля DVMRP.

GRE с AppleTalk

Туннелирование GRE может выполняться только между маршрутизаторами Cisco. При использовании туннелирования GRE для AppleTalk туннель настраивается с использованием сетевого адреса AppleTalk. Используя сетевой адрес AppleTalk, можно послать эхо-запрос на другой конец туннеля, чтобы проверить соединение.

Многоточечный GRE

После включения туннелирования mGRE можно выполнить команду **tunnel protection**, что позволит связать туннель mGRE с профилем IPSec. Сочетание туннелей mGRE с шифрованием IPSec позволяет использовать один интерфейс mGRE для поддержки нескольких туннелей IPSec, что уменьшает размер конфигурации и сложность настройки.

Примечание. Поддержка установленного соединения по туннелю GRE настраивается с использованием команды **keepalive** в интерфейсе GRE, который поддерживается только в туннелях GRE «точка-точка».

RBSCP

Туннелирование RBSCP создавалось для беспроводных каналов или каналов с задержкой дальней связи с высоким уровнем ошибок, например, спутниковых каналов. Благодаря использованию туннелей RBSCP может повысить производительность некоторых протоколов IP, например, TCP и IPSec, с помощью спутниковых каналов с моделью сквозного соединения без разрывов.

Транспорт IPSec с помощью IPv6

Инкапсуляция IPSec в IPv6 обеспечивает защиту IPSec между узлами для одноадресного и мультиадресного трафика IPv6. Эта возможность позволяет маршрутизаторам IPv6 работать в качестве защищенных шлюзов, организуя туннели IPSec между другими защищенными шлюзами-маршрутизаторами, и обеспечивать криптозащиту IPSec для трафика во внутренней сети при его передаче через общедоступный Интернет IPv6. IPSec IPv6 очень похож на модель защищенных шлюзов, использующую защиту IPsec IPv4.

Примеры

Туннелирование Cayman

В следующем примере показано, как включить туннелирование Cayman:

```
Router(config)# interface tunnel 0

Router(config-if)# tunnel source ethernet 0

Router(config-if)# tunnel destination 10.108.164.19

Router(config-if)# tunnel mode cayman
```

Туннелирование GRE

В следующем примере показано, как включить туннелирование GRE:

```
Router(config)# interface tunnel 0

Router(config-if)# appletalk cable-range 4160-4160 4160.19

Router(config-if)# appletalk zone Engineering

Router(config-if)# tunnel source ethernet0

Router(config-if)# tunnel destination 10.108.164.19

Router(config-if)# tunnel mode gre
```

Транспорт IPSec с помощью IPv4

В следующем примере показано, как настроить туннель с использованием инкапсуляции IPSec с IPv4 в качестве транспортного механизма:

Router(config)# crypto ipsec profile PROF

Router(config`crypto isakmp profile vpnprofile` # set transform tset

`match identity address 10.76.11.53`

Router(config`aaa new-model` # interface Tunnel0

Router(config ! # ip address 10.1.1.1 255.255.255.0

Router(config ! # tunnel mode ipsec ipv4

Router(config`aaa authentication login cisco-client group radius` # tunnel source Loopback0

Router(config`aaa authorization network cisco-client group radius` # tunnel destination 172.16.1.1

Router(config`aaa accounting network acc start-stop broadcast group radius` # tunnel protection ipsec profile PROF

Транспорт IPSec с помощью IPv6

В следующем примере показано, как настроить туннельный интерфейс IPSec IPv6:

```
Router(config)# interface tunnel 0

Router(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64

Router(config-if)# tunnel destination 10.0.0.1

Router(config-if)# tunnel source Ethernet 0/0

Router(config-if)# tunnel mode ipsec ipv6
```

Router(config-if)# **tunnel protection ipsec profile profile1**

Многоточечное туннелирование GRE

В следующем примере показано, как включить туннелирование mGRE:

```
interface Tunnel0

 bandwidth 1000

 ip address 10.0.0.1 255.255.255.0

! Ensures longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.

 ip mtu 1416

! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.

 no ip split-horizon eigrp 1

 no ip next-hop-self eigrp 1

 delay 1000

! Sets IPSec peer address to Ethernet interface's public address.

 tunnel source Ethernet0

 tunnel mode gre multipoint

! The following line must match on all nodes that want to use this mGRE tunnel.

 tunnel key 100000

 tunnel protection ipsec profile vpnprof
```

Туннелирование RBSCP

В следующем примере показано, как включить туннелирование RBSCP:

```
Router(config)# interface tunnel 0

Router(config-if)# tunnel source ethernet 0

Router(config-if)# tunnel destination 10.108.164.19

Router(config-if)# tunnel mode rbscp
```

Связанные команды

Команда	Описание
appletalk cable-range	Включает расширенную сеть AppleTalk.
appletalk zone	Устанавливает имя зоны для присоединенной сети AppleTalk.
tunnel destination	Определяет точку назначения туннельного интерфейса.
tunnel protection	Связывает туннельный интерфейс с профилем IPSec.
tunnel source	Устанавливает адрес узла-источника туннельного интерфейса.

virtual-template

Для указания виртуального шаблона, который будет использоваться для клонирования интерфейсов виртуального доступа, используйте команду **virtual-template** в режиме конфигурации группы VPDN. Для удаления виртуального шаблона из группы виртуальной частной коммутируемой сети (VPDN) используйте форму **no** этой команды.

virtual-template *template-number*

no virtual-template

Описание синтаксиса

template-number	Номер виртуального шаблона, который будет использоваться для клонирования интерфейсов виртуального доступа.

По умолчанию

Нет включенных виртуальных шаблонов.

Командные режимы

История команды

Версия	Изменение
12.0(5)T	Команда включена впервые.
12.1(1)T	Команда расширена для поддержки PPPoE по ATM для работы с входящими сеансами коммутируемого PPP через Ethernet (PPPoE).
12.2(15)T	Команда расширена для поддержки пользовательских атрибутов IP, используемых в исходящих сеансах туннельного протокола уровня 2 (L2TP).

Рекомендации по использованию

Сначала необходимо включить туннельный протокол группы VPDN, используя команду **protocol (VPDN)**, только после этого можно выполнять команду **virtual-template**. Удаление или изменение команды **protocol** приведет к удалению команды **virtual-template** из группы VPDN.

Каждая группа VPDN может клонировать интерфейсы виртуального доступа, используя только один виртуальный шаблон. Если ввести в группу VPDN вторую команду **virtual-template**, она заменит первую команду **virtual-template**.

В таблице 2 содержатся команды группы VPDN, в которых можно ввести команду **virtual-template**. Ввод команды группы VPDN запускает режим настройки группы VPDN. Таблица содержит приглашение командной строки для режима настройки группы VPDN и тип настраиваемой службы.

Команда группы VPDN	Приглашение командной строки	Тип службы
accept-dialin	`aaa session-id common`	Туннельный сервер
request-dialout	!	Сервер сети L2TP (LNS)

Если команда **virtual-template** вводится в подгруппе VPDN **request-dialout** , IP и другие пользовательские атрибуты могут использоваться для коммутируемого сеанса L2TP из LNS. Перед тем, как эта команда была расширена, настройки IP пользователей для серверов аутентификации, авторизации и учета (AAA) не поддерживались; конфигурация IP бралась из интерфейса номеронабирателя, определенного в маршрутизаторе.

Расширенная команда **virtual-template** работает аналогично настройке виртуальных профилей и удаленного доступа в L2TP. Интерфейс виртуального доступа L2TP первым клонируется из виртуального шаблона, это значит, что конфигурации интерфейса виртуального шаблона используются в интерфейсе виртуального доступа L2TP. После аутентификации конфигурация AAA пользователей используется в интерфейсе виртуального доступа. Поскольку атрибуты AAA пользователей используются только после аутентификации пользователя, LNS необходимо настроить так, чтобы она могла производить аутентификацию исходящего пользователя (для этой команды необходима настройка аутентификации).

Благодаря расширенной команде **virtual-template** все программные компоненты теперь могут использовать конфигурацию, присутствующую в интерфейсе виртуального доступа, а не в интерфейсе номеронабирателя. Например, согласование адреса протокола управления IP (IPCP) при согласовании адреса узла использует локальный адрес интерфейса виртуального доступа в качестве адреса маршрутизатора.

Примеры

В следующем примере LNS используется для работы с туннелем L2TP от концентратора доступа L2TP (LAC) с именем LAC2. Интерфейс виртуального доступа будет клонирован от виртуального шаблона 1.

```
vpdn-group 1

 accept-dialin

  protocol l2tp

  virtual-template 1

 terminate-from hostname LAC2
```

В следующем примере PPPoE по ATM используется для работы с коммутируемыми сеансами PPPoE. Интерфейс виртуального доступа для сеансов PPP будет клонирован от виртуального шаблона 1.

```
vpdn-group 1

 accept-dialin

  protocol pppoe

  virtual-template 1
```

В следующем примере показано, как настроить LNS для поддержки пользовательских конфигураций IP с сервера AAA:

```
!

vpdn enable

vpdn search-order domain

!

vpdn-group 1

.

.

.

 request-dialout

  protocol l2tp

  rotary-group 1

  virtual-template 1

 initiate-to ip 10.0.1.194.2
```

```
 local name lns

 l2tp tunnel password 7094F3$!5^3

 source-ip 10.0.194.53

!
```

Предыдущая конфигурация требует профиля AAA, такого, как в следующем примере, для описания пользовательских атрибутов:

```
5300-Router1-out  Password = "cisco"

     Service-Type = Outbound

     cisco-avpair = "outbound:dial-number=5550121"

7200-Router1-1  Password = "cisco"

     Service-Type = Outbound

     cisco-avpair = "ip:route=10.17.17.1 255.255.255.255 Dialer1 100 name 5300-Router1"

5300-Router1 Password = "cisco"

     Service-Type = Framed

     Framed-Protocol = PPP

     cisco-avpair = "lcp:interface-config=ip unnumbered loopback 0"

     cisco-avpair = "ip:outacl#1=deny ip host 10.5.5.5 any log"

     cisco-avpair = "ip:outacl#2=permit ip any any"

     cisco-avpair = "ip:inacl#1=deny ip host 10.5.5.5 any log"

     cisco-avpair = "ip:inacl#2=permit ip any any"

     cisco-avpair = "multilink:min-links=2"

     Framed-Route = "10.5.5.6/32 Ethernet4/0"

     Framed-Route = "10.5.5.5/32 Ethernet4/0"

     Idle-Timeout = 100
```

Связанные команды

Команда	Описание
accept-dialin	Настраивает LNS для доступа к туннелированным соединениям PPP от LAC и создания подгруппы VPDN accept-dialin.

protocol (VPDN)	Определяет туннельный протокол уровня 2, который будет использовать подгруппа VPDN.
request-dialout	Позволяет LNS запрашивать исходящие вызовы VPDN с помощью L2TP и создавать подгруппу VPDN request-dialout.
vpdn-group	Определяет локальный уникальный числовой идентификатор номера группы.

Информация о функциональных возможностях интерфейсов виртуальных туннелей IPsec

Таблица 3 содержит историю версий для этой функции.

Не все команды могут быть доступны в вашей версии программного обеспечения Cisco IOS. Информацию о версиях, в которых поддерживается определенная команда, можно найти в справочнике по командам.

Образы программного обеспечения Cisco IOS зависят от версии Cisco IOS, набора функций и используемой платформы. Для поиска информации о поддержке платформ и образов программного обеспечения Cisco IOS воспользуйтесь инструментом Cisco Feature Navigator. Доступ к инструменту Cisco Feature Navigator можно получить по адресу http://www.cisco.com/go/fn. Необходимо наличие учетной записи на веб-сайте cisco.com. Если у вас нет учетной записи, вы забыли имя пользователя или пароль, то в диалоговом окне входа в систему нажмите кнопку Cancel (Отмена) и следуйте дальнейшим указаниям.

Примечание. В таблице 3 перечислены только те версии программного обеспечения Cisco IOS, в которых вводилась поддержка данной функции в данной группе версий программного обеспечения Cisco IOS. Если не указано обратное, последующие версии группы версий программного обеспечения Cisco IOS также поддерживают эту функцию.

Таблица 3. Информация о возможностях виртуальных туннельных интерфейсов IPsec

Название функции	Версии	Информация о настройке функциональных возможностей
Статические VTI IPsec	12.3(7)T 12.3(14)T 12.2(33)SRA	Интерфейсы виртуальных туннелей (VTI) IPsec представляют собой тип маршрутизируемых интерфейсов на концах туннелей IPsec. Это простой способ установки защиты между узлами для образования перекрывающихся сетей. Интерфейсы VTI IPsec упрощают настройку IPsec для защиты удаленных каналов, поддерживают мультиадресную рассылку, делают проще управления сетью и балансировку нагрузки. Статические туннельные интерфейсы могут настраиваться на инкапсуляцию пакетов IPv6 или IPv4 в IPv6.
Динамические интерфейсы VTI IPsec	12.3(7)T 12.3(14)T	Динамические интерфейсы VTI обеспечивают эффективное использование IP-адресов и защиту соединений. Динамические интерфейсы VTI позволяют использовать динамически загружаемые политики пользователей и групп, настроенные на сервере RADIUS. Определения пользователей и групп можно создавать, используя расширенную аутентификацию (Xauth) группы User или Unity, или извлекать из сертификата. Динамические интерфейсы VTI основаны на стандартах, так что они совместимы с оборудованием различных производителей.

		Динамические интерфейсы VTI IPsec позволяют создавать хорошо защищенные соединения для VPN удаленного доступа и могут использоваться в сочетании с архитектурой Cisco для голосовых, видео и интегрированных данных (AVVID) для объединенной доставки голоса, видео и данных по IP-сетям. Динамические интерфейсы VTI упрощают развертывание IPsec с поддержкой VRF. Функция VRF настраивается на интерфейсе.
Поддержка атрибутов пользователей в серверах Easy VPN	12.4(9)T	Эта функциональная возможность обеспечивает поддержку атрибутов пользователей на серверах Easy VPN. Сведения об этой функциональной возможности содержатся в разделе «Поддержка пользовательских атрибутов в серверах Easy VPN» Для этой функции были добавлены или изменены команды **crypto aaa attribute list** и **crypto isakmp client configuration group**.

Все IP-адреса, использованные в данном документе, являются вымышленными. Все примеры, выходные данные команд, а также рисунки, включенные в данный документ, приведены только в пояснительных целях. Любое совпадение IP-адресов, приведенных в качестве иллюстрации, с реальными IP-адресами является случайным и непреднамеренным.