Туннели

Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру.

Статические туннели используются для объединения нескольких локальных сетей в одну: например при объединении нескольких удалённых офисов в одну локальную сеть таким образом, чтобы пользователи одной сети могли обращаться к ресурсам других.

Туннели настраиваются на пограничных маршрутизаторах этих сетей и весь промежуточный трафик передаётся через интернет инкапсулированным в IP или GRE-пакеты.

В ИКС вы можете настроить подключение между серверами статическим туннелем по IPIP или GRE протоколу.

Провайдеры и сети	Внешние устройства	Монитор пров	зайдеров Журнал
Добавить - Удалити	выключить 👻	Редактировать	🌮 Мастер настройки сети
Сети 🕨			
🚠 Локальная сеть			
Провайдеры			
🌐 Провайдер			
Туннели 🕨	Туннель IPIP		
	🌐 Туннель GRE		
	😡 Туннель OpenVPN		

Обычно выбор типа туннеля зависит от промежуточных провайдеров, которые по каким-либо причинам могут блокировать траффик GRE или IPIP, что приводит к невозможности использования какого-то одного типа туннеля. Принципиальной разницы между этими типами туннелей нет.

		Добавление туннеля GRE	
Общие настройки Настройки шифрования Название* Ламповый туннель Внешний интерфейс* Внешний ір-адрес удаленного сервера* Ф Мошный провайлер		Общие настройки Настройки шифрования Название* Классный туннель GRE Внешний интерфейс* Внешний ір-адрес удаленного сервера* (192.168.170.134/24) ▼	
(192.168.170.134/24) ×	Удаленный ір-адрес туннеля *	Локальный ір-адрес туннеля * 10.0.0.1	Удаленный ір-адрес туннеля* 10.0.0.2
10.0.0.1	10.0.2	Локальные сети	Удаленные сети
Локальные сети	Удаленные сети	Локальные сети 🝷	Удаленные сети
Локальные сети 🔸	Удаленные сети	мти	
мти		Автоопределение	*
	*	Автоматически создавать маршрут для удаленных	сетей
Автоматически создавать маршрут для удаленны:	< сетей	Использовать NAT	
Использовать NAT		Ключ GRE	
		(не использовать)	^
	Добавить Отмена		Лобавить Отмена

Настройки туннелей также не отличаются. Вам необходимо указать, на каком интерфейсе будет настроен данный туннель и прописать параметры маршрутизации:

- 1. внешний адрес удаленного сервера
- 2. адрес локальной сети
- 3. адрес удаленной сети

Аналогичные настройки необходимо произвести на другом конце тоннеля.

Важно: для того, чтобы туннель работал корректно, необходимо, чтобы в межсетевом экране ИКС был разрешен GRE-трафик, а также разрешены входящие соединения с ip-адреса удаленного сервера.

IP Security

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.

3/10

Добавление туннеля IPIP

Общие настройки	Настройки шифров	ания	
🕑 Использовать шифро	ование		
Ключ шифрования			
Настройки для фазы 1:			Настройки для фазы 2:
Режим работы			Протокол
main		•	ESP -
Алгоритм шифрования			PFS
aes256		•	15 - modp3072 -
Алгоритм хеширования			Алгоритм аутентификации *
sha2_384		•	hmac_sha2_384 🗱
DH-группа			Алгоритм шифрования
15 - modp3072		•	aes256 🛪 🔹
Время жизни *			Время жизни *
28800	^	сек.	1200 🗘 сек.
			Лобавить Отмена
			200ability Clinicia

Защита передачи данным по туннелям позволяет избежать многих проблем, связанных с утечкой информации и получения ложных данных. Вы можете защитить туннельный трафик, перейдя на вкладку «Шифрование» и установив флажок «Использовать шифрование». После этого вы можете произвести необходимые настройки параметров.

Внимание! Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.

Внимание! При использовании IPsec шифрования в туннелях IPIP и GRE трафик будет проходить через интерфейс **enc0**. Статистика на данном интерфейсе не собирается!

OpenVPN

OpenVPN - свободная реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она

позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall, без необходимости изменения их настроек.

Добавление туннеля OpenVPN

Основные настройки Шифрован	ие и сертификаты
Название *	Адрес сервера *
Лучший туннель OpenVPN	10.100.0.0
Протокол	Порт сервера *
UDP	• 1194
Использовать NAT	
	Добавить Отмена

Система туннелей OpenVPN построена таким образом: что одна из машин выбирается сервером, в рамках «ИКС» настраивается OpenVPN-сеть; а все остальные - клиентами, в рамках «ИКС» OpenVPN туннели.

На сервере прописывается адресация пространства внутри OpenVPN-сети (рекомендуется оставить значение по умолчанию) и размещаются SSL-сертификаты, а на клиентах указывается внешний IP-адрес сервера. Также, указывается порт обмена данными, что позволяет подключаться к серверу, который находится за межсетевым экраном или NAT, при помощи перенаправления портов.

Чтобы прописать необходимые сертификаты от сервера клиентам, сделайте следующее:

1. На сервере необходимо создать OpenVPN-сеть

ОреnVPN-се	VPN (10.8.0.0/24) ^{гть}					
Ір-адрес/Преф Прото Порт серв Корневой сертифи Сертификат серв	икс: 10.8.0.0/24 кол: udp ера: 1194 ікат: 🏶 Корневой сертификат ера: 🏶 Муми-OpenVpn	г				
Подробнее	Настройки авторизации	🛓 Выгрузить сертификаты	Удалить	Редактировать	Выключить	•

2. Создать пользователя для подключения и открыть ему доступ в модуле OpenVPN

2025/	09/02 01:41				5/10		Туннели
V	'PN-сервер	Настройки	Пользователи	Текущие сеан	сы События Журна	л	
Д	ļобавить 👻	Удалить	Выключить 👻	Редактировать			
Им	19			Логин 🔺	Ip-адреса из Vpn-сетей	Vpn- доступ	OpenVPN-доступ
Ξ	🖿 Корневая гр	руппа					-
	🕀 🖿 Семья						
	🗉 🖿 Долина						
	🕀 🖿 Друзья						
	💄 Туве Янс	сон		root			
	💄 Муми-ту	инель		tunnel			✓

3. Выгрузить сертификат в индивидуальном модуле пользователя, с расширением *.ovpn

OpenVPN-доступ для польз	ователя включен в 😭) Новая OpenVPN-сеть (10.8.0.0/24)	
Передать клиенту марц IP клиента (опционально)	ірут по умолчанию		
Передать клиентам маршрут	ы до сетей	Удаленные сети	
Передать клиентам марц	іруты до сетей 🔹	• Удаленные сети	
Сертификат клиента *			
🜻 Новая ОрепVPN-сеть	Администратор 🗙		-
Сохранить Обновить	Выгрузить серти	іфикаты	

4. Информацию из скаченного файла (*.ovpn) необходимо разбить на 3 файла (ca.crt, client.crt, client.key). В файл ca.crt поместить информацию содержащуюся между тегами <ca></ca>. Аналогично и для файлов client.crt и client.key помещаем информацию между тегами <cert></cert> и <key></key> соответственно. Далее импортируем корневой сертификат, а затем клиентский с указанием ключа на клиентском сервере.

*	Защита								🚨 Адми	нистратор	1 37 🔁 🛓
2						1					
		Добавить	Удалить	Просмотр сертификата	🛓 Импорт 🏦 Экспорт 👻				Q, No		C
đà		Haanauura			Turn contraction on the	2000 00 10 10	au Coorou	Пойстон	or no Muquan and	C 100770	
0	Веб-фильтр Касперского	пазвание =			тип сертификата	Закрытый ют	Создан	деиству	ет до имя или адре	C XUCIA	
-	Веб-фильтр SkyDNS	🗆 🏶 Сертиф	икаты								
	Межсетевой экран	🖂 🌞 Корн	евой сертифик	ат (зашифрован)	CA	зашифрован	21.11.20	21.11.20	20 test.ru		
	Web Application Firewall	🜻 O1	penVpnNetwork	(1_tunnel	Конечный сертификат	не зашифрова	н 21.11.20	21.11.20	20 tunnel		
0	Application Firewall	🗰 Autor	generated Aster	isk_5dd662397b8cd0.69169904	Конечный сертификат	не зашифрова	н 21.11.20	22.11.20	29 ics-asterisk		
•	Летектор атак Suricata	🌻 Auto	generated GUI_	5dd6623855b1d3.90975404	Конечный сертификат	не зашифрова	н 21.11.20	22.11.20	29 ics-gui		
2		🗰 Auto	generated MailS	Server_5dd66238932e16.61893	393Конечный сертификат	не зашифрова	н 21.11.20	22.11.20	29 ics-mail-server		
۶											
	Сертификаты										
•											
- T											
<											

5. После этого импортированные сертификаты можно будет выбрать на вкладке «Шифрование» при создании туннеля OpenVPN (поле «Ключ TLS авторизации» необходимо заполнить, содержимым файла *.ovpn, а именно информацией между тегами <tls-auth></tls-auth>)

Основные настройки Шифрова	ие и сертификаты	
Алгоритм шифрования	Алгоритм хеширования	
AES-256-CBC	- SHA256	-
Включить сжатие LZO		
ink-MTU *		
1500		~
Корневой сертификат	Сертификат клиента	
🌞 Корневой сертификат 🛪	OpenVpnNetwork1	_tunnel ×
(люч TLS авторизации		
# # 2048 bit OpenVPN static key #		,
BEGIN OpenVPN Static key V1 7dbb7d87c3b7e3b9745211888bcbb9ef 9524ae4cc6876bf37255ef390a339c48		

Туннель IPsec

В ИКС можно настроить подключение между серверами IPsec-туннелем, в котором IPsec

работает в туннельном режиме. Особенностью данного туннеля является то, что он считается активным только до тех пор, пока между локальными и удаленными сетями туннеля происходит обмен трафиком. При отсутствии такого трафика в течение 8 часов туннель объявляется неактивным, с соответствующим статусом туннеля.

Чтобы добавить туннель IPsec, выполните следующие действия:

1. Нажмите кнопку «Добавить» и выберите «Сети > Туннели > Туннель IPsec».

â	Сеть	ООО "Организация" > Провайдеры и сети	💄 Администратор 🏦 🔤 1 🤪
<u>۹</u>	Мастер настройки сети Провайдеры и сети	Провайдеры и сети Внешние устройства	Монитор провайдеров Журнал
•	Сетевые утилиты	Добавить - Удалить Выключить -	Редактировать Q Поиск
-	Межсетевой экран	Сети 🕨	
	маршруты Перенаправление портов	Локальная сеть (.170.187/24)	выбран по умолчанию, основной, подключен
°.	DNS	Провайдеры • еть (192.168.1.1/24)	
ŗ	Прокси VPN	Туннели 에 Туннель IPSec	кабель подключен
	ARP-таблица		
\$	Удалённое управление	Новая ОрепVPN-се ОрепVPN-се ОрепVPN-сеть ОрепVPN-сеть	
<			

2. На вкладке «Общие настройки» введите название туннеля.

3. Выберите внешний интерфейс.

4. Введите в соответствующих полях следующие **адреса**: внешний IP-адрес удаленного сервера, локальные сети, удаленные сети.

Добавление туннеля IPSec

Общие настройки	Настройки шифрования	Настройки мониторинга
Название *		
Новый туннель IPSec		
Внешний интерфейс*		Внешний ір-адрес удаленного сервера*
🌐 Новый провайдер	(192.168.17.108/24) ×	192.168.1.1
Локальные сети *		Удаленные сети *
192.168.17.187 ×	•	192.168.17.108/24 🗙
		Добавить Отмена

5. На вкладке «Настройки шифрования» можно установить параметры шифрования IPsec.

Внимание! Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.

9/10

Добавление туннеля IPSec

Общие настройки	Настройки шифровани	ия Настройки мониторинга	
Ключ шифрования *			
•••••			\$
Настройки для фазы 1:		Настройки для фазы 2:	
Режим работы		Протокол	
main	-	ESP	•
Алгоритм шифрования		PFS	
aes256	-	15 - modp3072	•
Алгоритм хеширования		Алгоритм аутентификации *	
sha2_384	-	hmac_sha2_384 🗙	-
DH-группа		Алгоритм шифрования	
15 - modp3072	-	aes256 🗶	-
Время жизни *		Время жизни *	
28800	🔷 сек.	1200	сек.
		Добавить	Отмена

6. На вкладке «Настройки мониторинга» можно установить флаги:

- «Проверять наличие пинга внешнего IP-адреса удаленного сервера» проверка, отвечает ли на ICMP-запросы внешний адрес удаленного сервера, который указан в общих настройках туннеля. Если пинг не будет проходить, в статусе туннеля отобразится соответствующее уведомление;
- «Проверять наличие пинга удаленной сети» позволяет задать пинг до IP-адреса в удаленной сети с указанием в качестве источника IP-адрес ИКС из локальной сети. Таким образом, если пинг будет проходить успешно, статус туннеля всегда будет «Подключен». При установке флага выберите локальную сеть и введите IP-адрес удаленной локальной сети;
- «Проверять доступность серверов» при установке флага укажите серверы, доступность которых будет проверяться.

По умолчанию все флаги сняты.

Добавление туннеля IPSec

Общие настройки	Настройки шифрования	Настройки мониторинга
 Проверять наличие г 	пинга внешнего ір-адреса удале	нного сервера
Проверять наличие г	пинга удаленной сети	
Локальная сеть *		Ір-адрес удаленной локальной сети *
	Ψ	
Проверять доступно	сть серверов	
		Добавить Отмен

7. Нажмите «Добавить» — новый туннель появится в списке.

8. Аналогичные настройки необходимо произвести на другом конце туннеля.

Внимание! Для корректной работы туннеля необходимо, чтобы в межсетевом экране ИКС был разрешен трафик от внешнего удаленного адреса, а также разрешен трафик от локальных удаленных сетей, если это необходимо.

From: https://doc-old.a-real.ru/ - **Документация**

Permanent link: https://doc-old.a-real.ru/doku.php?id=ics70:tunnels&rev=1594819728



Last update: 2020/07/15 16:28