Настройка ІРІР-туннеля.

Если в вашей компании имеется удаленный филиал, то для объединения локальных сетей безопасным способом наиболее подходящим решением будет являться настройка шифрованного туннеля между ними.



Для настройки IPIP или GRE-туннеля между двумя ИКС необходимо выполнить следующие действия:

- 1. Добавить новый туннель IPIP или GRE
- 2. Указать список локальных и удаленных сетей для маршрутизации между ними
- 3. Настроить параметры шифрования
- 4. Добавить в межсетевой экран необходимые разрешающие правила.

После чего все действия необходимо произвести на втором конце туннеля.

В нашем примере мы создадим туннель между двумя серверами.

	Сервер 1	Сервер 2
Внешний адрес	192.168.17.145	192.168.17.245
Адрес локальной сети	192.168.84.1/24	192.168.55.1/24



Сначала добавим новый IPIP-туннель в модуле «Провайдере и сети».

Добавление туннеля IPIP	\boxtimes
Общие настройки Настройки I	шифрования
Название:	Новый туннель ІРІР
Внешний интерфейс:	Связьинтерком 🛛 💙
Внешний ір-адрес удаленного сервера:	192.168.17.245
Локальные сети:	🚠 Зоопарк 🗶 📟
Удаленные сети:	192.168.55.1/24 ×
Автоматически создавать маршрут для удаленных сетей:	✓
	Добавить Отмена

Добавление туннеля IPIP	×
Общие настройки Настройки и	иифрования
Использовать шифрование:	☑
Ключ шифрования:	
Настройки для фазы 1:	
Режим работы:	main 🛛 💙
Алгоритм шифрования:	3des 🛛 🗸
Алгоритм хеширования:	sha1 💎
DH-группа:	2 💎
Время жизни:	28800 сек.
Настройки для фазы 2:	
Протокол:	ESP 🛛
PFS:	1 💎
Алгоритм аутентификации:	hmac_sha1 💟 🗸
	Добавить Отмена

Выбираем в качестве исходящего интерфейса нашего провайдера, указываем внешний адрес Сервера 2, выбираем локальную сеть и прописываем в удаленной сети сеть Сервера 2. Чтобы пользователи автоматически могли получить доступ к хостам в локальной сети Сервера 2, устанавливаем флажок «Автоматически создавать маршрут для удаленных сетей».

Затем переходим во вкладку «Шифрование», включаем его и устанавливаем pre-shared key. Остальные параметры имеют оптимальные настройки, их можно оставить по умолчанию.



Красный статус «нет пинга до внутреннего адреса на удаленном сервере» сигнализирует о том, что туннель создан, но не установлен. Продолжаем настройку.

Чтобы разрешить Серверу 1 принимать пакеты через туннель от Сервера 2, необходимо создать разрешающее правило. Для этого нужно перейти в модуль «Межсетевой экран» и добавить новое разрешающее правило.

Last update: 2020/01/27 16:28 en:пример_ipip https://doc.a-real.ru/doku.php?id=en:%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80_ipip

Добавление разрешающего правила 🛛 🔀			
Описание:	Тестовый туннель		
Направление:	Входящий и исходящий 🛛		
Источник:	• 192.168.17.245 × 🚥		
Назначение:	(любой) 🚥		
Протокол:	(любой) 🛛		
Порт источника:	(любой) 🚥		
Порт назначения:	(любой) 🚥		
Интерфейс:	(любой) 🚥		
Время действия:	(всегда) 🚥		
B Manum	Добавить		

В правиле достаточно указать ip-адрес Сервера 2 в качестве источника. Остальные параметры указывать не обязательно. Также необходимо проверить, что в списке правил присутствует и включено правило по умолчанию «Доступ к серверу через GRE тоннели», разрешающее прохождение GRE-трафика.

Теперь всю процедуру необходимо повторить на Сервере 2.

Добавление туннеля IPIP	×
Общие настройки Настройки шифрования	
Название:	Тестовый туннель
Внешний интерфейс:	Провайдерко 💎
Внешний ір-адрес удаленного сервера:	192.168.17.145
Локальные сети:	器 Новая локальная сеть 🗱 🚥
Удаленные сети:	◎ 192.168.84.1/24 ×
Автоматически создавать маршрут для удаленных сетей:	
	Добавить Отмена

Добавление туннеля IPIP	\mathbf{X}
Общие настройки Настройки шифрования	
Использовать шифрование: 🗹	^
Ключ шифрования: •••••	
Настройки для фазы 1:	
Режим работы: 🛛 main 🛛 🔗	
Алгоритм шифрования: <mark>3des </mark> 💎	=
Алгоритм хеширования: sha1 🔗	
DH-группа: 2 😒	
Время жизни: 28800 сек.	
— Настройки для фазы 2:	
Протокол: ЕЅР 😒	
PFS: 1 🔝	
Алгоритм аутентификации: hmac_sha1 🛛 💎	~
Добавить	на

Добавление разрешающего правила 🛛 🔀			
Описание:	Тестовый туннель		
Направление:	Входящий и исходящий 🛛		
Источник:	• 192.168.17.145 × 🚥		
Назначение:	(любой) 🚥		
Протокол:	(любой)		
Порт источника:	(любой) 🚥		
Порт назначения:	(любой) 🚥		
Интерфейс:	(любой) 🚥		
Время действия:	(всегда) 🚥		
	оступ для пассивного Бть апрешить ТСР трафик, входищ Добавить Отмена о		

Теперь, если все настроено верно, в статусе созданного туннеля на каждом сервере должна появиться надпись «подключен».



Проверить работу туннеля можно с помощью модуля «Сетевые утилиты», запустив пинг с Сервера 1 на внутренний интерфейс Сервера 2.

🗲 Пинг	Трейс	Onpoc Dns	Информация о домене	Дамп	Сетевые интерфейсы 🔶
	Адр	ec: 192.168	.55.1		🞯 Запустить 🔵
Количес	тво пакет	ов: 4			
DING 10	22.1.0	FF 4 2400		1	
64 byte	92.168. 93 from	55.1 (192 192.168.)	.168.55.1): 56 0 55.1: icmn seg=0	ata byt 1 ttl=64	es time=0.836 ms
64 byte	es from	192.168.	55.1: icmp seq=1	l tt1=64	time=0.499 ms
64 byte	es from	192.168.	55.1: icmp_seq=2	ttl=64	time=0.426 ms
64 byte	es from	192.168.	55.1: icmp_seq=3	6 ttl=64	time=0.421 ms
192.168.55.1 ping statistics					
4 packets transmitted, 4 packets received, 0.0% packet loss					
round-t	trip mi	n/avg/max,	/stddev = 0.421/	0.545/0	.836/0.171 ms

Ваш туннель настроен и работает. Теперь вы можете использовать ресурсы обоих филиалов одновременно.

