

l2tp

Original file



NETSHe Lab

1. - - - - - Настройка L2TP соединений средствами NETSHe OS

© 2020, NETSHeLabLtd

Ярославль

Данное руководство не включает в себя описания настройки подключений к сети Интернет или иным IP-сетям, теоретические вопросы протокола L2TP и настройку маршрутизации. Предполагается, что данные вопросы известны пользователю по соответствующим разделам документации NETSHe OS, а так же прочим общедоступным источникам.

Теоретическая часть

NETSHe OS, поддерживает возможность организации L2TP сервера, а так же клиентского подключения к серверам L2TP, в том числе реализованных на серверах под управлением других операционных систем или на телекоммуникационном оборудовании других производителей.

Традиционно наиболее часто L2TP применяется для туннелирования соединений через публичную сеть Интернет с целью безопасной передачи приватного трафика между сегментами своей сети или дружественными локальными сетями. Приятным бонусом в этой схеме является то, что со стороны клиента L2TP не требует статического и даже динамического публичного IP адреса, успешно устанавливая соединение из-за NAT (NetworkAddressTranslation), применяемого на оборудовании периметра частной сети или на оборудовании оператора связи.

Фактически, L2TPсоединение - это туннель для передачи пакетов третьего уровня модели OSI поверх четвертого уровня (UDP). Для каждого такого туннеля существует нижележащий локальный интерфейс и удаленный серверный интерфейс, образующие пару внешних адресов туннеля.

L2TP соединение может быть установлено только после получения IP-адреса нижележащим интерфейсом, и только при наличии рабочего маршрута до серверного адреса через нижележащий интерфейс (случай с прохождением маршрута по-умолчанию через L2TP интерфейс будет рассмотрен ниже).

L2TP соединение не может автоматически устанавливать маршруты:

- на клиенте за исключением маршрута по-умолчанию
- на сервере — маршрут по-умолчанию; иные маршруты могут быть установлены через специальный RADIUS-аттрибут для конкретного соединения.

Пожалуйста, обратите внимание! Для нормального функционирования L2TP соединения адрес удаленной стороны туннеля (сервера для клиента; клиента для сервера) должен быть доступен через нижележащий интерфейс.

Возможности авторизации подключения к серверу, автоматической замены маршрута по умолчанию на новый сделали L2TP (наряду с PPTP) популярным средством подключения к сетям Интернет сервис провайдеров.

Довольно быстро подключения к серверам L2TP стали использоваться как сервисы в Интернете и использоваться для разных нужд: как VPN туннели для обхода корпоративных или национальных стандартов, в целях сокрытия источника трафика от сервисов GeoIP и прочих.

Клиентские L2TP соединения в NETSHe OS имеют названия l2tp, l2tp1 и т. д.

Серверные L2TP соединения имеют имена типа rrrX, где X- положительное целое число.

В другом руководстве от нашей лаборатории «Настройка объединения сегментов Ethernet-сетей через IP-сети средствами NETSHe OS» рассматривается более сложный пример применения L2TP в качестве одной ступени в каскаде последовательного применения разных сетевых протоколов.

Ограничения реализации

1. Применение L2TP в серверной части требует наличия центрального устройства (сервера или шлюза), имеющего постоянное подключение к IP сети (например, Интернет) и постоянный IP-адрес (либо настроенное разрешение символического имени в IP-адрес).

Общие программно-аппаратные требования

Требования, предъявляемые к серверу

Серверная часть L2TP может быть настроена почти во всех реализациях NETSHeOS: на физическом сервере, в облачном окружении на виртуальной машине, в составе встроенного программного обеспечения большинства телекоммуникационных устройств с ролью маршрутизатора. Единственным обязательным условием является наличие соответствующего программного пакета в составе прошивки.

Сервер должен иметь, как минимум, один внешний интерфейс, соединенный с IP сетью, через которую осуществляется соединение с конечными устройствами, например, Интернет. Настройки внешнего интерфейса (встроенного МСЭ) должны допускать UDP пакеты на порт 1701.

При планировании аппаратной или виртуальной части стоит исходить из:

- минимальных нагрузок в части дисковой подсистемы;
- незначительных запросов в части оперативной памяти (один активный клиент — примерно 1 мегабайт памяти);
- значительной нагрузки в процессорной части (не менее 1 процессорного ядра на 50-100 активных клиентов (зависит от объема трафика) и одно дополнительное ядро на каждые 200 пользователей. Рекомендуются производительные процессорные ядра).

Требования, предъявляемые к клиенту

Клиентское L2TP-соединение не является ресурсоемким и не предъявляет каких-либо существенных требований.

Единственным требованием является наличие маршрута до сервера через нижележащий интерфейс при использовании маршрута по-умолчанию через L2TP соединение.

При использовании L2TP для клиентского доступа в Интернет операторами связи, указанное выше требование реализуется передачей маршрутов до L2TP сервера(ов) в составе DHCP настроек.

В ином случае следует озаботиться настройкой такого маршрута самостоятельно, согласно руководства по статической маршрутизации NETShe.

Пожалуйста, обратите внимание! В случае использования символьного имени для L2TP сервера и разрешении имени в более чем один IP-адрес, **следует настроить маршруты до каждого адреса**.

Настройка клиента L2TP

Настройка интерфейса

Перейдите в меню «Сеть→Интерфейсы / Network→Interfaces», введите имя нового интерфейса l2tp, как показано ниже, и нажмите кнопку «Новый/New».

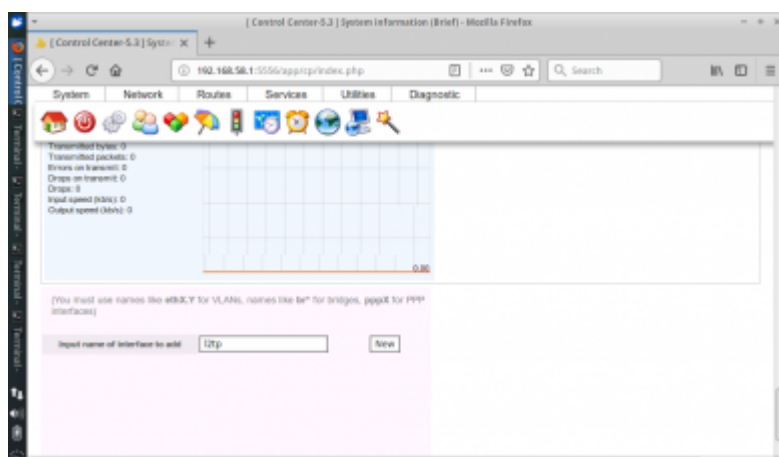


Рисунок 3. Создание нового интерфейса

Встроенное программное обеспечение некоторых устройств с NETSHe OS может иметь шаблон конфигурации, имеющий предварительно (полностью или частично) настроенные L2TP-соединение и Ethernet-порт (интерфейс), что может облегчить настройку. Также, подобные настройки могут быть автоматически установлены на устройство через NETSHe NMMS. Тем не менее, рассмотрим настройку режима в полном объеме.

На данном этапе мы рассматриваем наличие проводного подключения к сети Интернет через вышестоящий маршрутизатор; доступность настроенного сервера L2TP, адресуемого по символьному имени или IP-адресу; наличия у пользователя пары «имя пользователя/пароль» для L2TP подключения. Чуть позже опишем, какие коррективы нужно внести, чтоб использовать вариант непосредственного подключения к Интернет через сотовую сеть.

После нажатия кнопки «New» Вы будете переадресованы на страницу ввода настроек L2TP-подключения, как показано на рисунке ниже.

[Настроить интерфейс l2tp]

Разрешить интерфейс ? : ☐

Базовые настройки | Дополнительно | Подробная информация | Маршруты через интерфейс

Тип соединения: *

Логин:

Пароль:

Устройство (например, identity5) или интерфейс, который будет использован(о) для установки соединения:

PPPoE/L2TP Сервер/Имя службы PPPoE:

Использовать интерфейс как резервный?: ☐

Не заменять текущий маршрут по умолчанию?: ☐

Не использовать серверы имен от провайдера?: ☐

Разрешить IPv6?: ☐

Использовать безопасный PPP?: ☐

Запретить буферизацию?: ☐

Включить прозрачный IP режим?: ☐

MTU:

Статический IP для интерфейса. Обычно провайдер назначает его автоматически. Оставьте поле пустым, если не уверены:

Внешний адрес для проверки состояния соединения:

Перезагрузить сервис(ы) после сохранения ? : ☐ Сохранить

Сохраните изменения, а затем перейдите по этой ссылке, чтобы настроить CoS для интерфейса

* Заполнение выделенных полей обязательно!

Рисунок 4. Пример настройки L2TP соединения

Заполните:

- поля «Имя пользователя / Username», «Пароль / Password»;
- поле «L2TP сервер / L2TP server» именем или адресом L2TP сервера;
- поле «Устройство или интерфейс, который будет использован(о) для установки соединения / Device or interface used to establish connection» именем WAN интерфейса клиентского устройства.
- Если Вам необходимо, чтобы весь трафик шел от устройства через L2TP сервер, очистите поля «Не заменять текущий маршрут по умолчанию / Do not replace existing default route» и «Не заменять серверы имен от провайдера» и не забудьте настроить (проверить получение) маршрут до сервера через нижележащий интерфейс.

Перейдите на вкладку «Дополнительно / Additional » и выберите зону WAN для интерфейса, как показано ниже, и нажмите кнопку «Сохранить / Save».

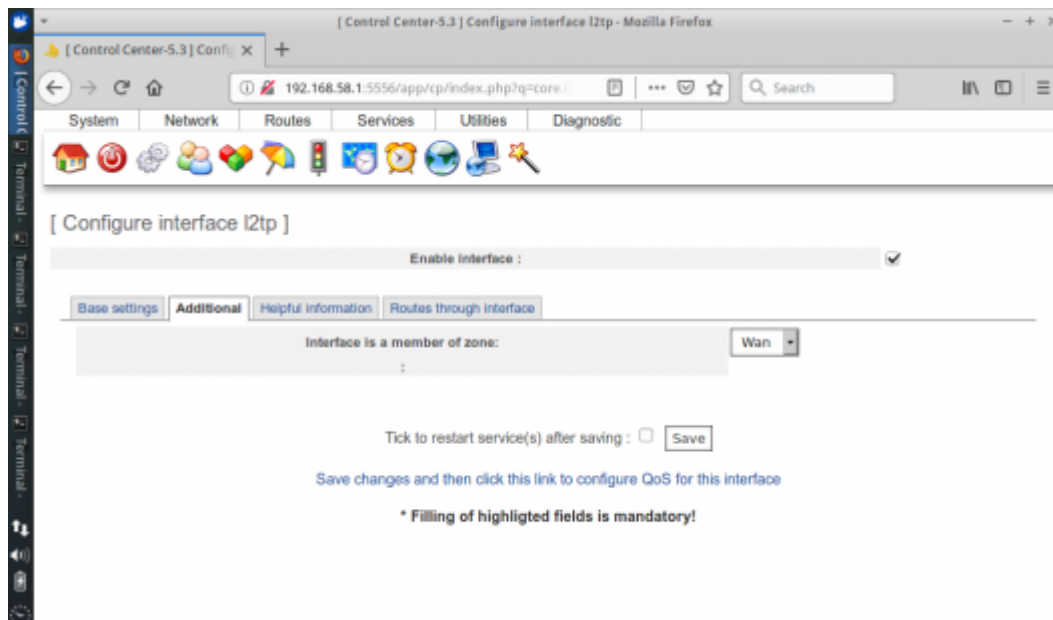


Рисунок 5. Задание зоны WAN для L2TP-соединения.

Настройка маршрута до L2TP-сервера

Еще раз отметим, что существует два варианта построения маршрутизации через L2TP туннель: направление в туннель маршрута по умолчанию либо создание на обеих сторонах туннеля маршрутов в удаленную сеть. Если по условиям задачи, нам необходимо направить маршрут по-умолчанию через L2TP соединение, а маршрут до сервера не получен автоматически, нам предстоит озаботиться этим самостоятельно.

Маршрут по-умолчанию будет устанавливаться после снятия галки «Не заменять текущий маршрут по умолчанию» в настройках интерфейса l2tp.

Создадим статический маршрут до сервера.

Для этого нужно выбрать пункт меню «Маршрутизация→Статические маршруты / Routing→Staticroutes», и добавить соответствующую строку с маршрутом.

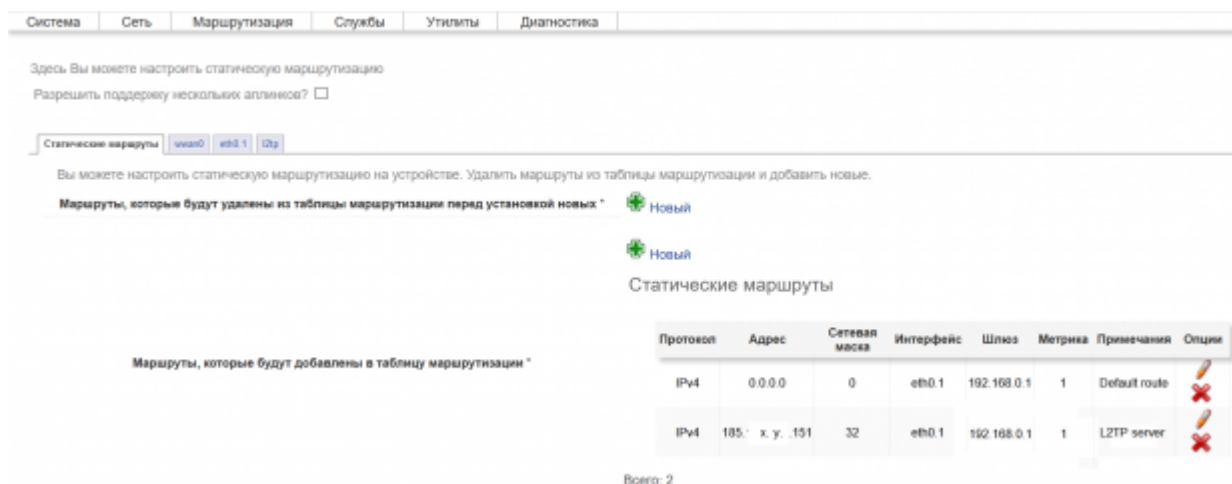


Рисунок 6. Задание статического маршрута до L2TP-сервера.

- В настройках интерфейса l2tp следует указать имя интерфейса, используемого для соединения, как `wwan0` или `cellular`.
- Маршрут по умолчанию и статический маршрут до сервера L2TP должны проходить через сотовый интерфейс. Отметим, что интерфейсы `wwan0` и `cellular` не оперируют ARP-запросами, а адрес шлюза в такой сети определить не представляется возможным. Следовательно, поле «шлюз» у маршрутов должно быть пустым.

[illegible]

Базовые настройки

Дополнительно

Панель информации

Маршруты через интерфейс

Настройка интерфейса [2tr]

Разрешить интерфейс ? :

Тип соединения: *

Логин:

Пароль:

Устройство (например, identity5) или интерфейс, который будет использован(о) для установки соединения:

PPTP/L2TP Сервер/Шлюз службы PPPoE:

Использовать интерфейс как резервный? :

Не заменять текущий маршрут по умолчанию ? :

Не использовать серверы имен от провайдера ? :

Разрешить IPv6? :

Использовать синхронный PPP? :

Запретить буферизацию? :

Включить прозрачный IP режим? :

MTU:

Статический IP для интерфейса. Обычно провайдер назначает его автоматически. Оставьте поле пустым, если не уверены:

Внешний адрес для проверки состояния соединения:

L2TP ▾

15090233

wan0

185 x, y, 101

☐

☐

☐

☐

☐

☐

☐

0

Перезагрузить сервис(ы) после сохранения ? : ☐

Сохранить

Сохраните изменения, а затем перейдите по этой ссылке, чтобы настроить QoS для интерфейса

* Заполнение выделенных полей обязательно!

Printed on 2020/11/04 05:10

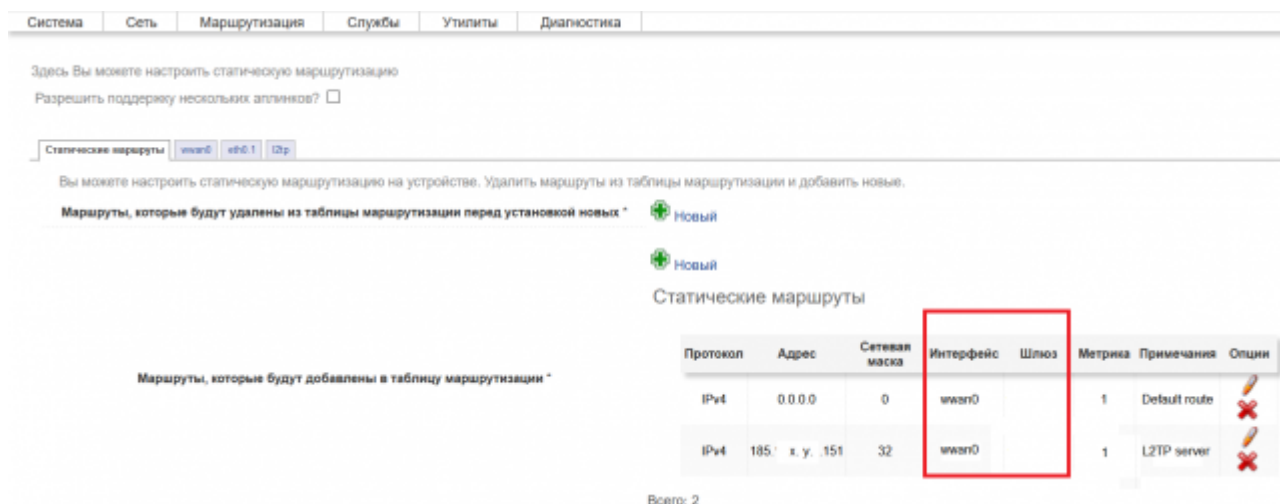


Рисунок 9. Статические маршруты.

Результат. Проверка работоспособности.

В качестве проверки работоспособности туннеля L2TP решим две задачи доступа:

- к веб-интерфейсу для управления клиентским устройством,
- к удаленному рабочему столу компьютера, находящемуся в LAN клиентского устройства.

После проведенных настроек туннель L2TP должен подняться, а у интерфейса l2tp должны быть показаны текущий выданный туннельный адрес и статистика трафика.

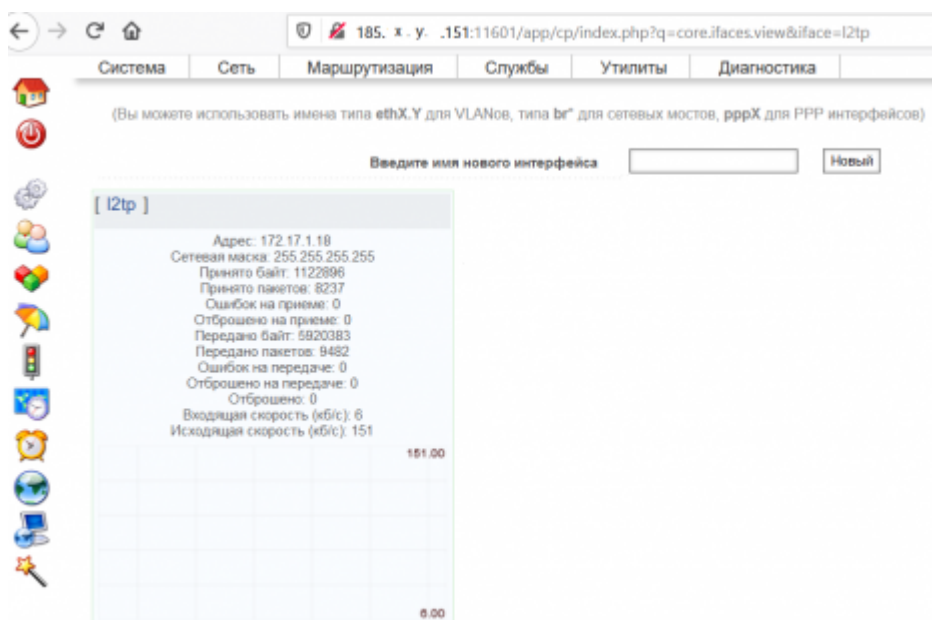


Рисунок 10. Интерфейс l2tp в активном состоянии.

Пример. Доступ к WebUI устройства, подключенного

Для интерфейса l2tp требуется установить галки «Не заменять маршрут по-умолчанию» и «Не использовать сервера имен провайдера». Задавать маршрут до сервера не нужно.

Останется на любом компьютере, имеющем доступ в Интернет, открыть WebUI устройства, находящегося за туннелем L2TP. Для этого в браузере следует ввести URL-адрес:

<http://185.x.y.151:11601> , где 185.x.y.151 адрес L2TP-сервера.

Пример. Доступ к компьютеру за туннелем L2TP

Задача доступа к любым устройствам за туннелем решается пробросом портов (DNAT или PAT в разных терминологиях) на устройстве – клиенте L2TP. В данном случае нам придется для проброса использовать TCP-порт 11602, который в процессе сопоставления NAT будет заменен на 3389 (стандартный порт MicrosoftRDP).

Для этого в пункте меню «Сеть→Межсетевой экран/ Network→Firewall» нужно настроить правило пересылки и разрешить пропуск TCP:11602 для зоны WAN. После чего перезагрузить службу МСЭ, выставив соответствующую галку рядом с кнопкой «Сохранить / Save».

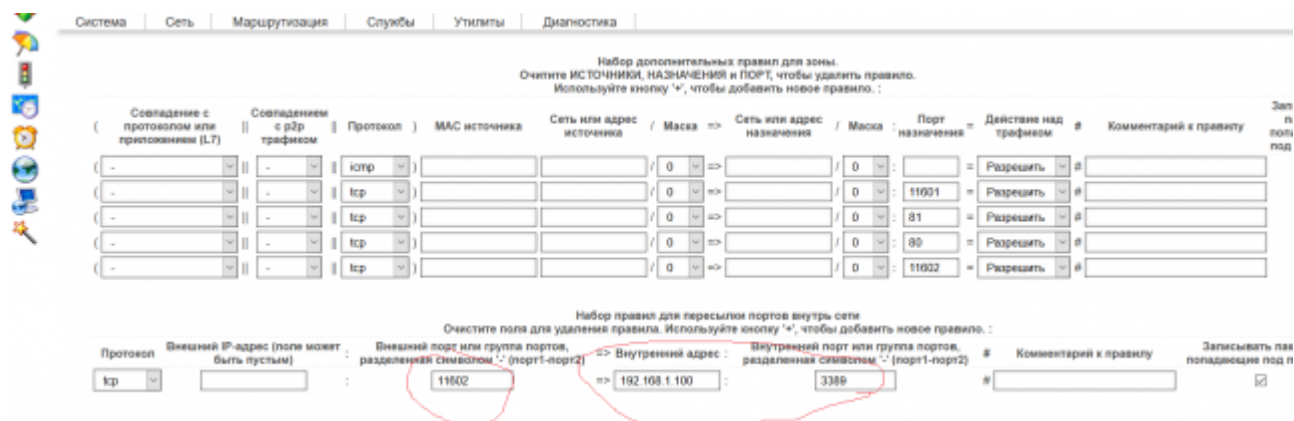


Рисунок 13. Настройка сетевого экрана.

Далее мы можем убедиться, что проброс порта 11602 внутрь сети за клиентским устройством работает:

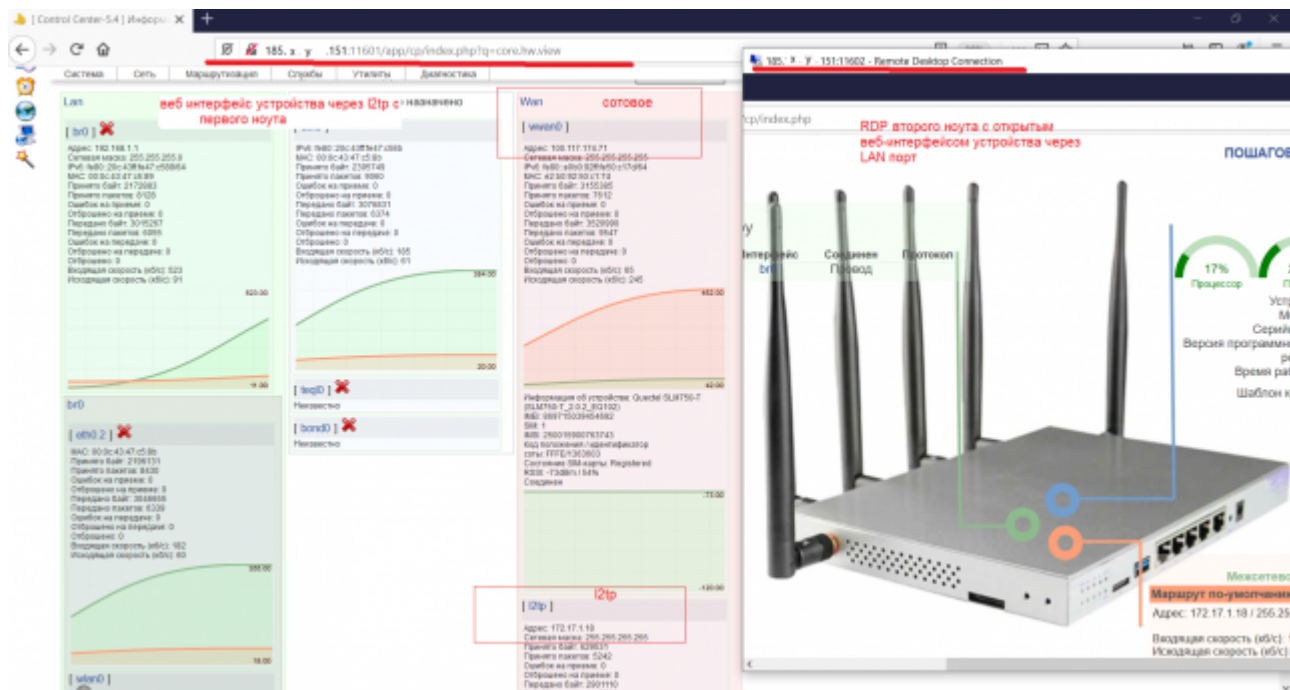


Рисунок 14. Два работающих подключения к WebUI клиента-L2TP и RDP к удаленному компьютеру.

Заключение.

В виду очевидной простоты и удобства в работе, L2TP может использоваться в комбинации с различными протоколами качестве средства обхода NAT, туннелирования трафика уровней L2-L7, а так же во многих других случаях. Для выяснения всех деталей применения пользователю следует обратиться в нашу техподдержку или на сайт «Нетше лаб»: <http://www.netshe-lab.ru/>

Специалисты нашей компании помогут Вам по любым вопросам, в том числе связанным с криптографической защитой L2TP соединений, если такое предусмотрено и урегулировано в ваших проектах.

From: <http://docs.netshe-lab.ru/> - Документация по NETSHe

Permanent link: http://docs.netshe-lab.ru/docs.php?id=%D0%BD%D0%80%D1%81%D1%82%D1%80%D0%8E%D0%89%D0%8A%D0%80%D2%D1%81%D0%8E%D0%85%D0%84%D0%8B%D0%8D%D0%85%D0%80%D0%8F%D0%89_%D0%82_netshe_%D1%81_%D0%8F%D1%80%D0%8B%D0%8C%D0%85%D1%80%D0%80%D0%8C%D0%8B

Last update: 2020/10/11 08:19

