eot ver2

Original file

NETSHe Lab

1. - - - - - - - **Настройка объединения сегментов Ethernet-сетей через IP-сети средствами NETSHe OS**

© 2019-2020, NETSHe Lab Ltd

Ярославль

Оглавление

Настройка объединения сегментов Ethernet-сетей через IP-сети средствами NETSHe OS, L2TP и GRETAP

Данное руководство не включает в себя аспекты настройки подключений к сети Интернет или иным IP-сетям, общие вопросы создания L2TP соединения, выделения Ethernet-портов, настройки сетевого моста и включения порта в сетевой мост.

Предполагается, что данные вопросы известны пользователю по соответствующим разделам документации NETSHe OS.

Теоретическая часть

NETSHe OS (начиная с версии 5.2) имеет возможность объединения Ethernet-сетей (L2) поверх IP-сетей (L3).

Допускается как объединение двух или более удаленных сегментов одной сети, так и объединение удаленных сегментов с внутренним (по отношению к серверу или шлюзу) сегментом.

Кроме того, поддерживается возможность изолированного объединения различных сетей, используя технику VLAN.

Для передачи L2 кадров по IP сети используется инкапсуляция кадров в пакеты GRE (GRE-туннель). Поскольку GRE протокол не может функционировать при нахождении какого-либо конца туннеля за NAT, а также для решения проблемы с фиксированными (предсказуемыми) адресами концов туннеля, в NETSHe OS дополнительно используется инкапсуляция GRE

пакетов в пакеты L2TP соединения.

Использование L2TP соединений снимает проблему работы оконечных устройств за NAT, реализует возможность авторизации и управления системой в целом за счет использования RADIUS.

Тем не менее, применение L2TP требует наличия центрального устройства (сервера или шлюза), имеющего постоянное подключение к IP сети (например, Интернет) и постоянный IP-адрес (либо настроенное разрешение символьного имени в IP-адрес).

Соответственно, настройка объединения Ethernet сетей сводится к задачам настройки оконечного устройства и сервера (шлюза). На рисунке 1 показан простейший случай объединения двух сегментов Ethernet-сети.

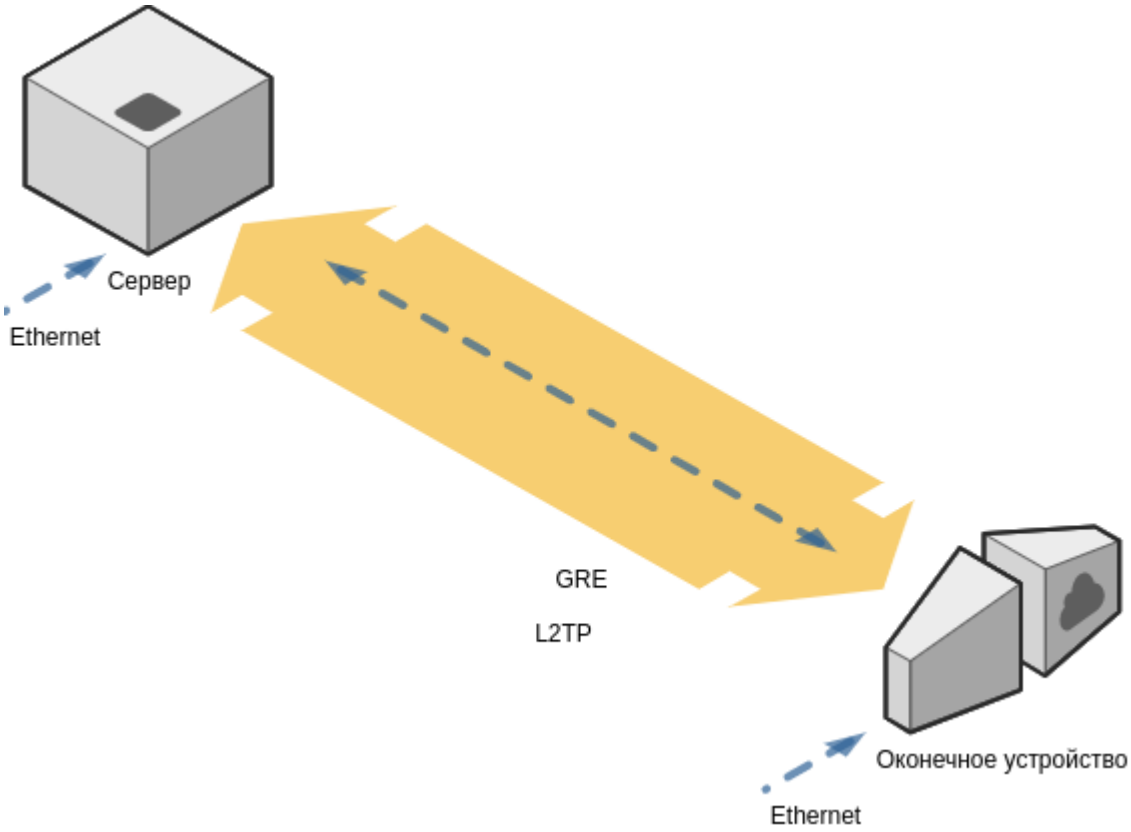


Рисунок 1. Объединение двух сегментов одной Ethernet-сети.

Сервер принимает входящие L2TP соединения от конечных устройств на своем внешнем интерфейсе, авторизует их (например, на RADIUS-сервере), создает соответствующий GRE-туннель и подключает к необходимому сетевому мосту.
Данный сетевой мост служит как для объединения двух и более Ethernet-сетей, находящихся за конечными устройствами, так и для объединения (в том числе с использованием VLAN) с сетями, находящимися за вторым интерфейсом сервера.

При объединении фрагментов одной сети настройка и использование VLAN 802.1Q тэгирования может не потребоваться.

На рисунке 2 показан пример объединения трех сегментов одной Ethernet-сети

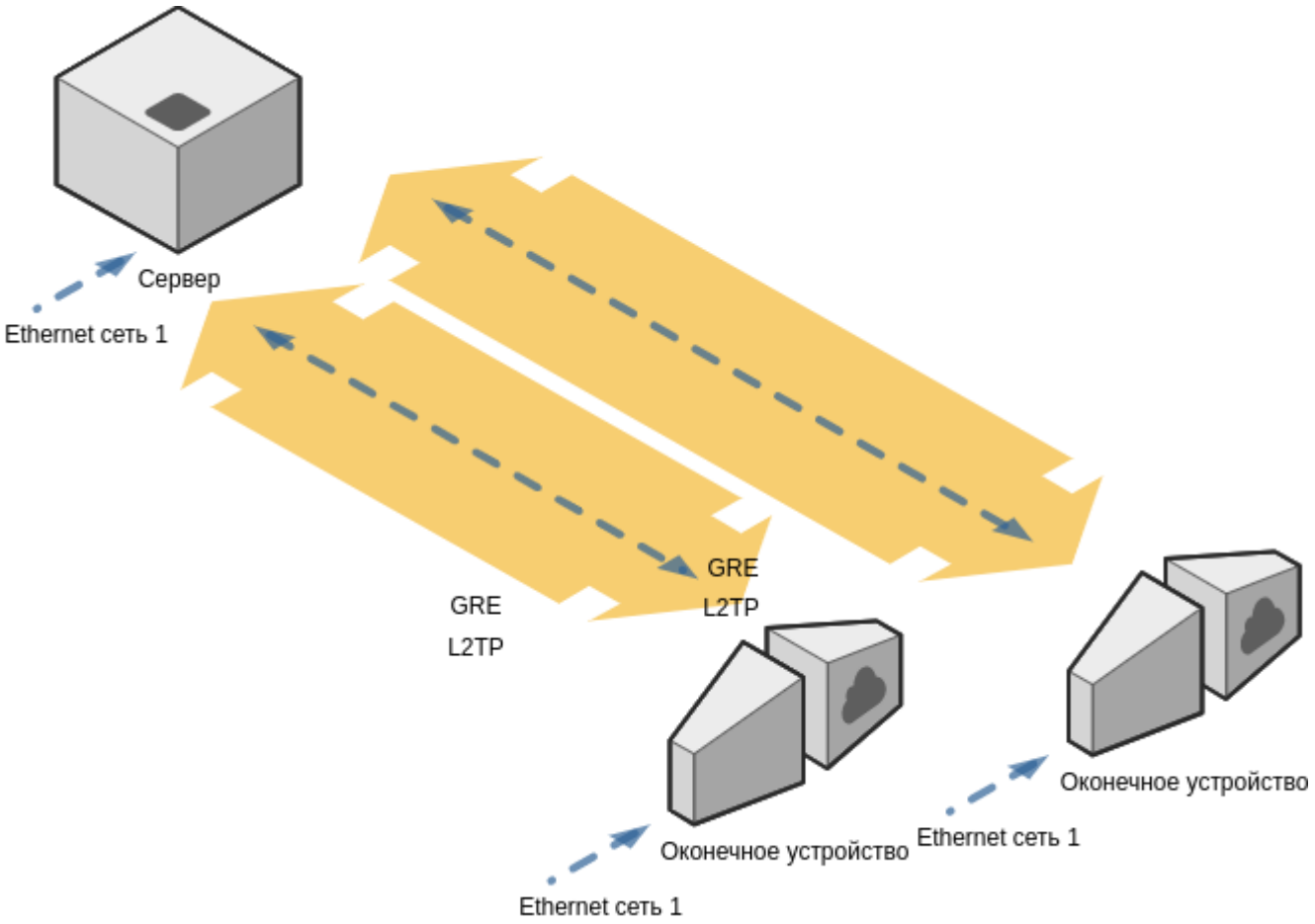


Рисунок 2. Объединение двух и более сегментов одной Ethernet-сети

При объединении только удаленных сегментов сетей настройка и использование второго интерфейса на сервере не требуется.

А на рисунке 3 показан пример объединения сегментов разных сетей.

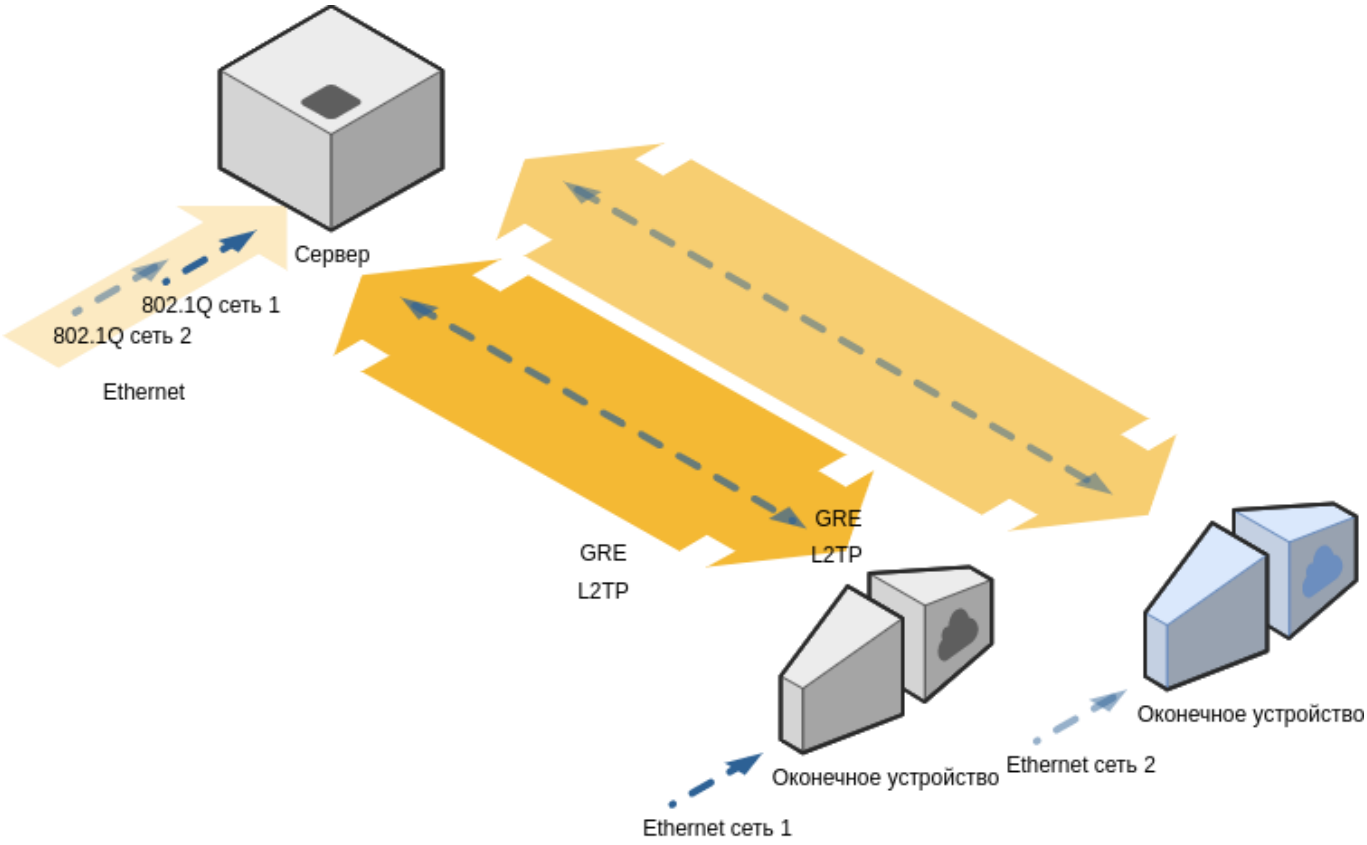


Рисунок 3. Объединение сегментов разных сетей.

Каждой Ethernet-сети на сервере будет соответствовать свой сетевой мост. Такие сетевые мосты на сервере создаются автоматически. В каждый такой мост входят только определенные туннели и VLAN интерфейсы (при подключении внутренних сегментов).

Определение того, какой туннель, сетевой мост и VLAN интерфейс использовать, производится на основе атрибута VLAN-EgressID в ответе RADIUS-сервера.

Два L2TP-соединения, для которых получены ответы RADIUS-сервера с одинаковыми VLAN-EgressID, будут включены в один сетевой мост и фактически объединены.

Два L2TP-соединения, для которых получены ответы RADIUS-сервера с разными VLAN-EgressID, будут включены в разные сетевые мосты и фактически изолированы друг от друга.

Таким образом, изоляция разных Ethernet-сетей внутри сервера осуществляется за счет включения туннелей в разные сетевые мосты, а изоляция Ethernet-кадров внутри второго интерфейса сервера — за счет разных меток 802.1Q.

Ограничения реализации

Ограничениями реализации являются:

1. Обязательное наличие RADIUS-сервера, выдающего ответ с атрибутом VLAN-EgressID.
2. Поддержка только одного L2TP-соединения между оконечным устройством и сервером (следует как из ограничений самого протокола L2TP, так и из требования единого удаленного IP-адреса для L2TP соединений).
3. Невозможность поддержки двух и более VLAN со стороны оконечного устройства

(следует из предыдущего пункта, а также невозможности создания двух и более GRETAP туннелей между двумя IP-адресами).
4. Один VLAN-EgressID — одна Ethernet-сеть (следствие авторизации и управления через RADIUS-сервер); один 802.1Q тэг на выходе с сервера в сторону коммутатора.
5. Реализация не содержит каких-либо активированных средств для ограничения передачи широковещательного и группового L2 трафика по соединениям. Данный вопрос предлагается решать (при необходимости) средствами Ethernet-коммутаторов (предпочтительнее) или настройкой правил фильтрации на сетевых мостах оконечных устройств.
6. Накладные расходы (служебное использование пропускной способности IP-соединения) на передачу каждого кадра Ethernet-сети составляют более 6% и растут с уменьшением размера передаваемого кадра.
7. Размер Ethernet-кадра в 1360 байт и более (с высокой вероятностью, более 1450 — гарантированно) приведет к передаче двух пакетов на каждый кадр. Что влечет за собой увеличение нагрузки на процессор до двух раз.

Стоит отметить, что пункты 3 и 4 приводят к одному итоговому ограничению: одно оконечное устройство может участвовать в объединении только одной Ethernet-сети.

Общие требования к программно-аппаратному обеспечению

Общие требования, предъявляемые к серверу системы

Серверная часть может быть установлена как на физический сервер, так и запущена в облачном окружении.

Для использования в облачном окружении, серверная часть поставляется в виде образа виртуальной машины в файле формата .vmdk со встроенной поддержкой систем виртуализации VMWare/KVM.

Сервер должен иметь 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 (L2TP подключения).

При необходимости объединения внешних и внутренних Ethernet-сетей сервер должен иметь второй (внутренний) Ethernet-интерфейс, который будет принимать/отправлять кадры с метками 802.1Q.

Настройки МСЭ (межсетевого экрана) на внешнем или внутреннем интерфейсе должны обеспечивать беспрепятственный обмен пакетами с RADIUS-сервером.

При планировании аппаратной или виртуальной части стоит исходить из:

1. минимальных нагрузок в части дисковой подсистемы;
2. незначительных запросов в части оперативной памяти (один активный клиент — примерно 1 мегабайт памяти);
3. 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). При отключении межсетевого экрана (обеспечивается специализированным устройством) на сервере и использовании высокопроизводительных ядер, следует исходить из правила: 1 ядро на 300 пользователей и 1 дополнительное ядро на каждые 400 пользователей.

Система, в целях обеспечения отказоустойчивости и балансировки нагрузки, может содержать более одного сервера при условии помещения перед серверной частью соответствующего балансировщика нагрузки.

Вопросы настройки балансировщика, облачного окружения и (или) сетевых коммутаторов для обработки тэгированных кадров не являются предметом настоящего руководства.

Рекомендуемая архитектура серверной части приведена на рисунке 4.

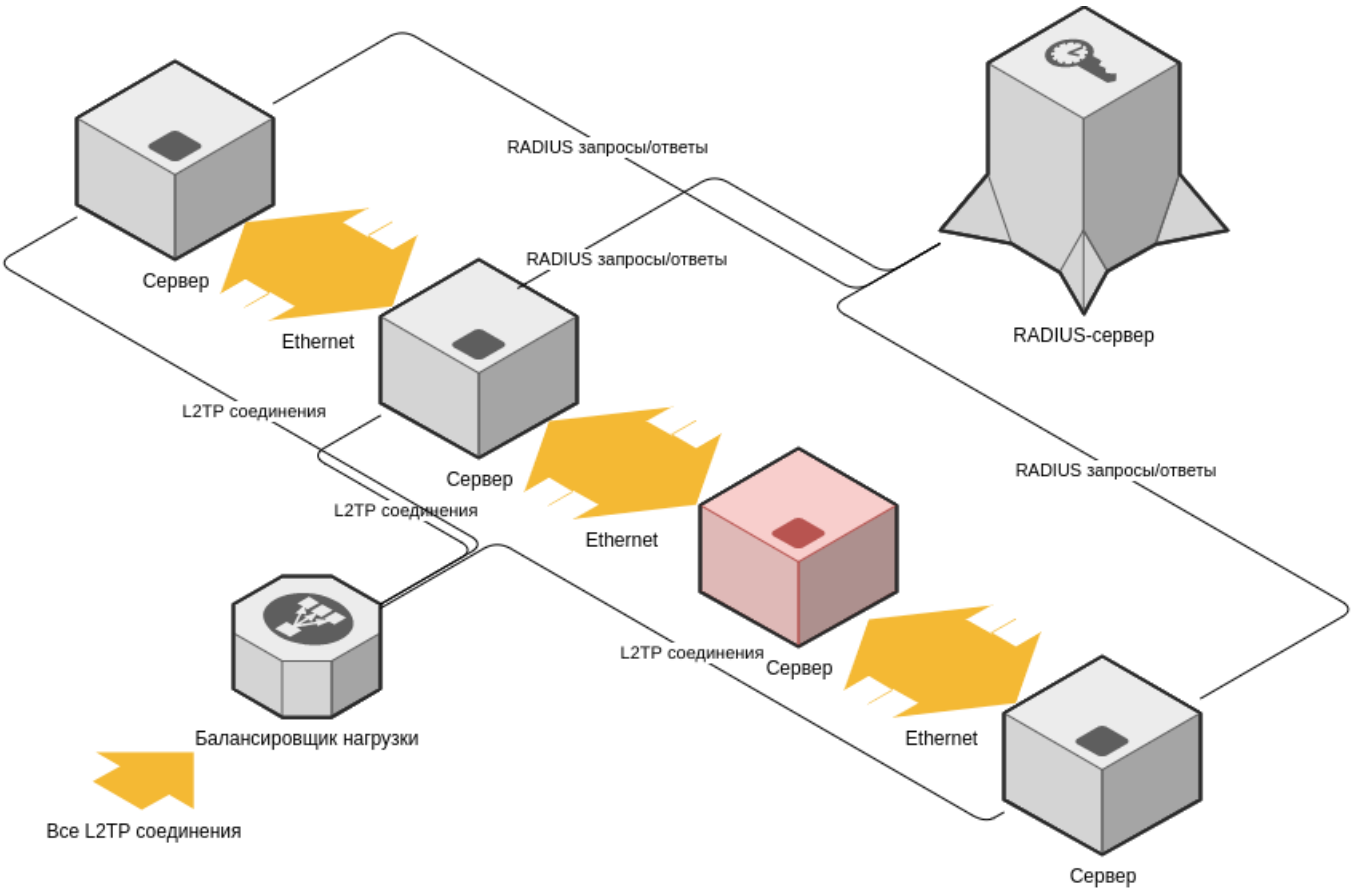


Рисунок 4. Пример рекомендуемой архитектуры серверной части.

На рисунке 5 показан пример минимально возможной серверной части.

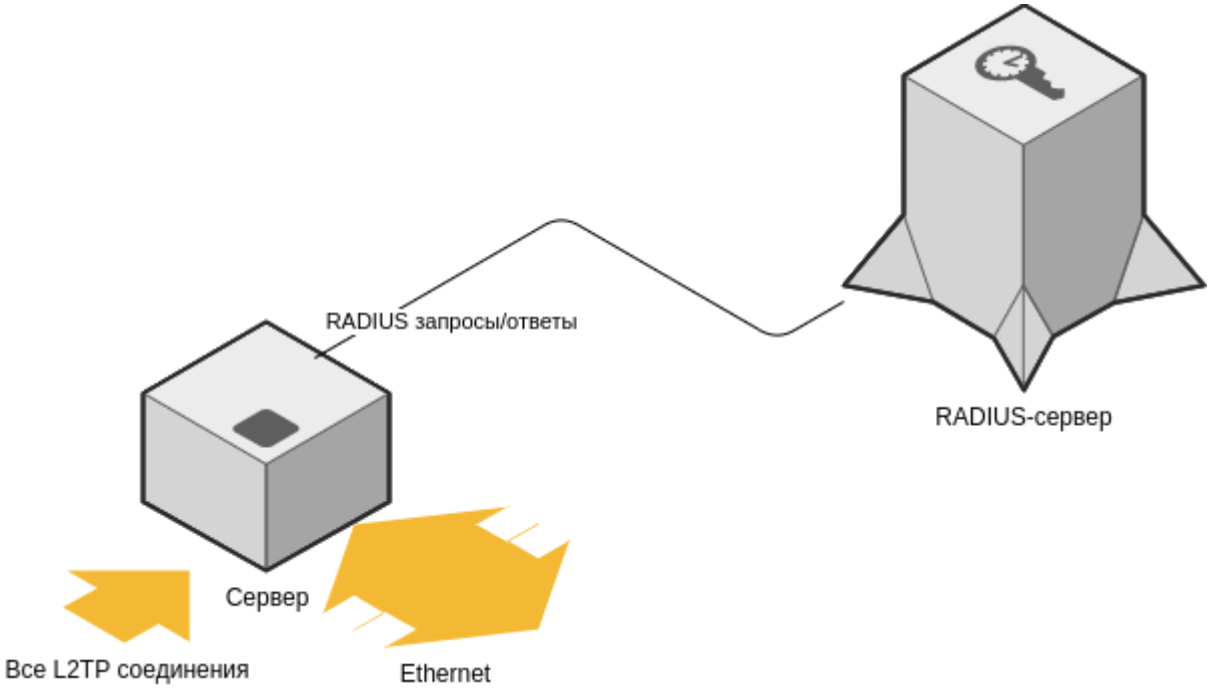


Рисунок 5. Пример минимальной архитектуры серверной части.

Обязательным условием в настройке всех серверов является использование единого локального адреса L2TP соединений. Для предотвращения конфликтов с возможными адресами, мы рекомендуем использовать адрес из Link Local адресов (169.254.0.0/16).

Общие требования, предъявляемые к RADIUS-серверу

В системе может использоваться любой RADIUS-сервер умеющий:

1. авторизовать соединения с CHAP,
2. выдать для авторизованного соединения атрибут VLAN-EgressID с номером VLAN.

Одним из таких RADIUS-серверов является сервер, входящий в состав NETSHe NMMS.

Вопросы настройки RADIUS-сервера не являются предметом настоящего руководства.

Общие требования, предъявляемые к оконечным устройствам и их подключению для объединения Ethernet-сетей

Конечное устройство должно иметь:

1. Встроенное программное обеспечение NETSHe версии не ниже 5.2;
2. Иметь настроенное подключение к сети Интернет или иной IP-сети, через которую осуществляется объединение сегментов;
3. Иметь минимум один доступный Ethernet-порт;
4. Иметь общую производительность и пропускную способность подключения к IP-сети адекватную требуемой пропускной способности для Ethernet-сети.

Настройка системы

Общий план настройки серверной части

Для настройки серверной части необходимо выполнить следующий набор действий:

1. Настроить адрес внешнего интерфейса сервера и маршрут по умолчанию в соответствии с выбранной архитектурой.
2. Настроить второй интерфейс и все необходимые VLAN интерфейсы на нем в случае объединения внутренних сегментов сети, удаленного доступа к серверу и т. п.
3. Настроить встроенный межсетевой экран для пропуска UDP пакетов на порт 1701 внешнего интерфейса, пропуска RADIUS пакетов на внешний или один из внутренних интерфейсов (зависит от конкретной архитектуры), удаленного доступа и взаимодействия с балансировщиком (при необходимости).
4. Указать адреса, порты и секретные фразы основного и резервного RADIUS-серверов.
5. Настроить L2TP-сервер, указав внешний интерфейс для приема соединений, внутренний/локальный адрес соединений (ДОЛЖЕН БЫТЬ ОДИНАКОВ ДЛЯ ВСЕХ СЕРВЕРОВ), пул адресов для удаленных клиентов.
6. Перезапустить сервер.
7. Проверить работоспособность сервера и перепроверить все настройки.

Настройка сервера

Настройка подключения сервера к IP-сети не является предметом настоящего руководства.

Настройка внутреннего Ethernet-интерфейса

Настройка внутреннего Ethernet-интерфейса может осуществляться либо вручную, посредством создания соответствующих VLAN интерфейсов, как это описано в документации к NETSHe OS, либо автоматически.

При предварительной настройке интерфейса (например, eth1), последний должен быть исключен из каких-либо существующих мостов, с него требуется убрать назначенный ранее IP-адрес.

В случае ручной настройки, для данного интерфейса должны быть созданы необходимые VLAN интерфейсы (например, eth1.2 (управление), eth1.10, eth1.11, eth1.12 ... eth1.102 — для объединяемых сетей).

В случае автоматического создания VLAN для объединяемых сетей следует выбрать пункт меню «Services→Access concentrator→Ethernet over tunnel server / Службы → Концентратор доступа → Ethernet поверх туннелей».

В открывшемся диалоге нужно выбрать соответствующий физический интерфейс (например, eth1), указать размер MTU для выбранного интерфейса и нажать кнопку «Save / Сохранить», как показано на рисунке ниже.

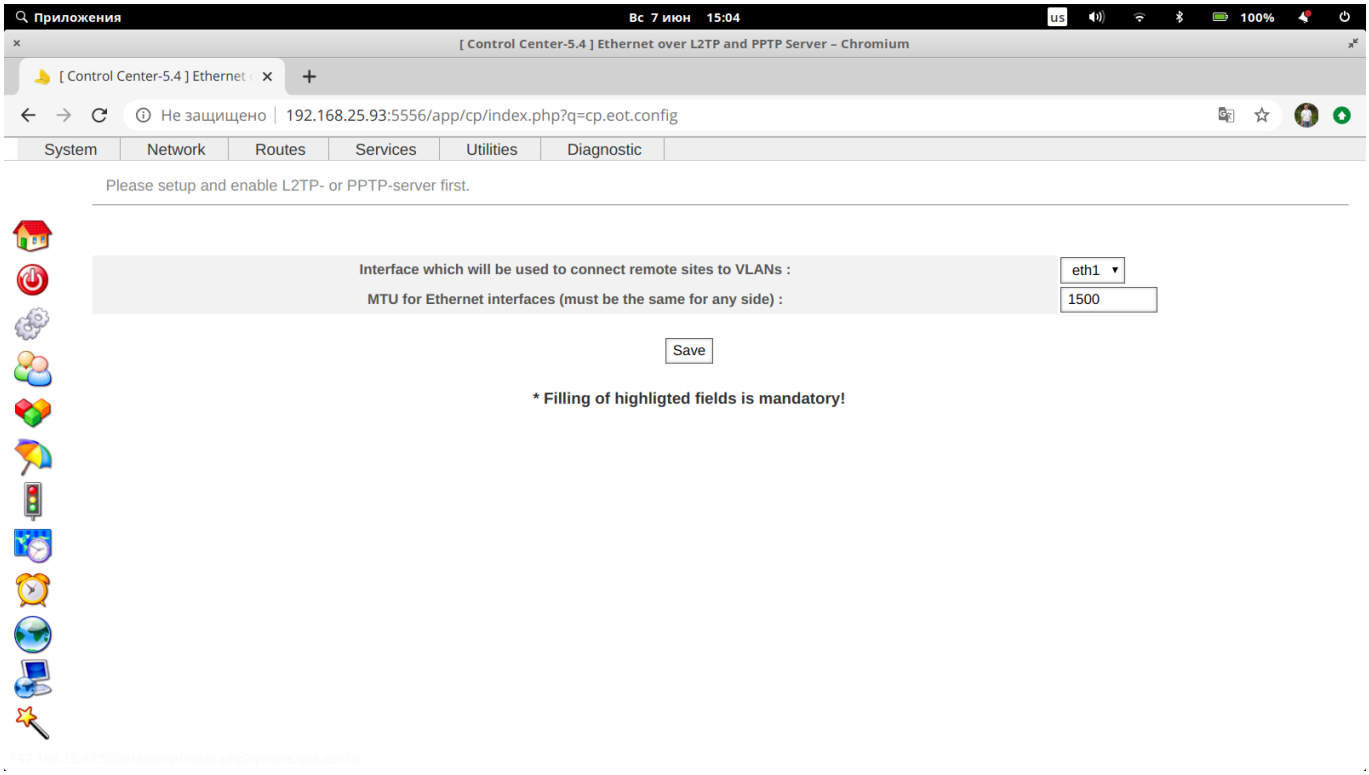


Рисунок 6. Настройка интерфейса, для которого будут автоматически создаваться VLAN

Настройка межсетевого экрана

Разрешите прием входящих L2TP-соединений в МСЭ, добавив правило для зоны WAN, как показано на рисунке ниже:

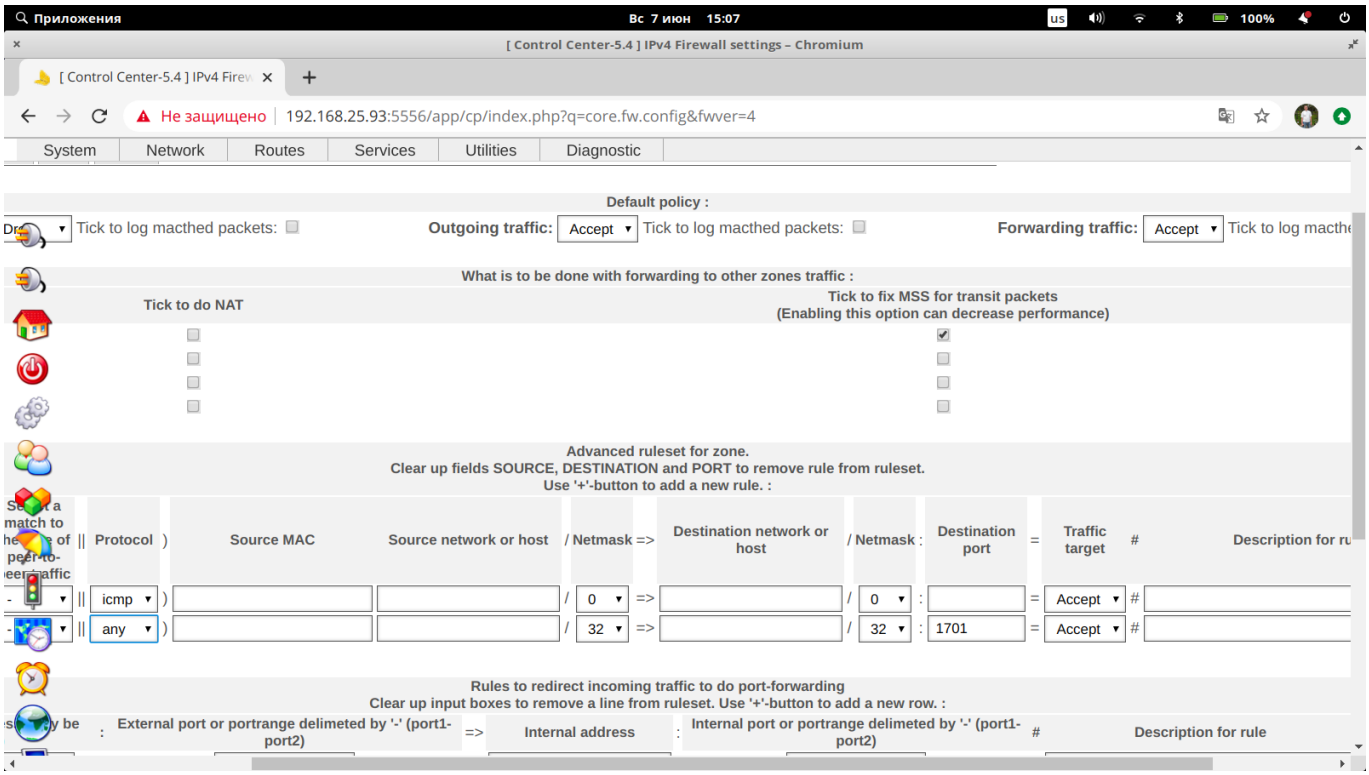


Рисунок 7. Правило для приема L2TP-соединений

В случае если сервер отделен от общедоступных сетей (Интернет) специализированным устройством, рекомендуем отключить встроенный межсетевой экран для снижения нагрузки

на центральный процессор.

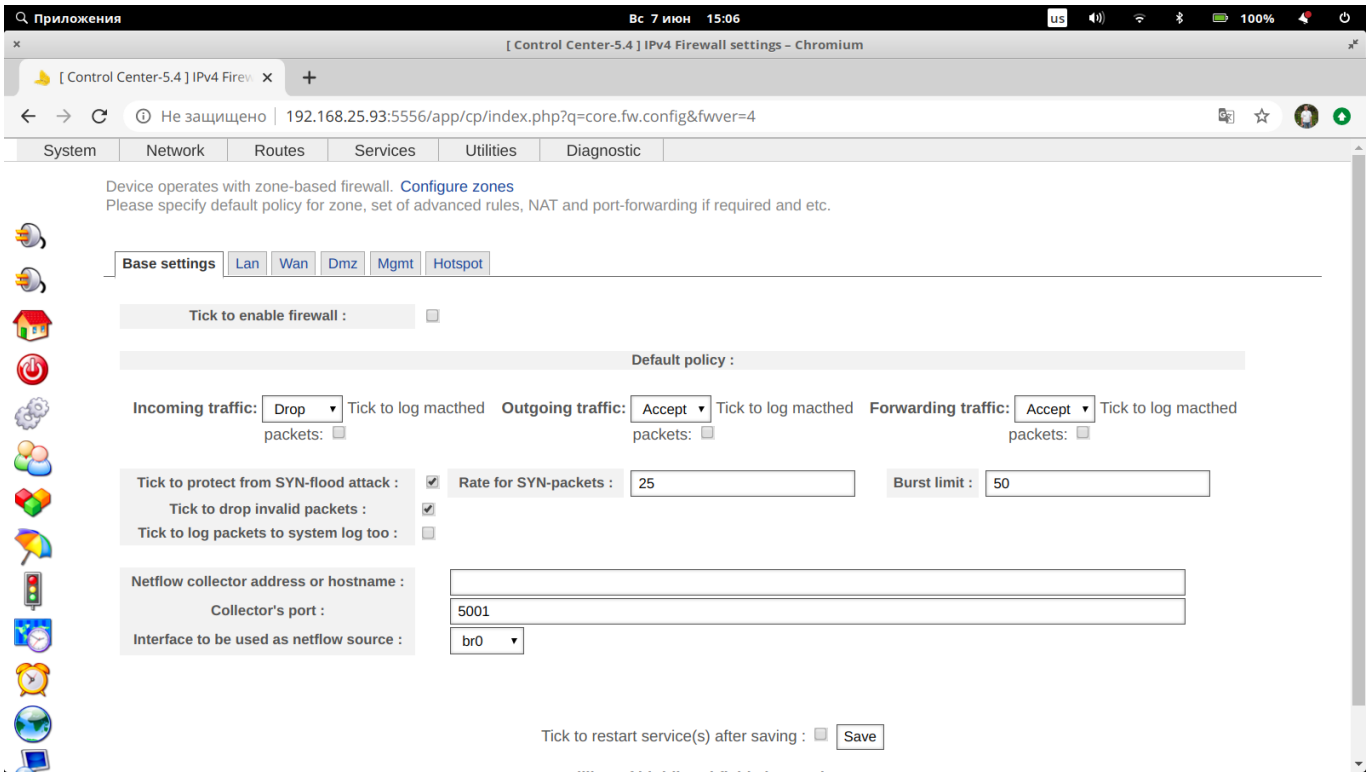


Рисунок 8. Отключение МСЭ

Настройка RADIUS

Выберите пункт меню «System → Base settings / Система→ Базовые настройки» и перейдите на вкладку RADIUS-клиент.

Введите имена / адреса, секретные фразы и порты основного и резервного RADIUS-серверов, как показано на рисунке ниже.

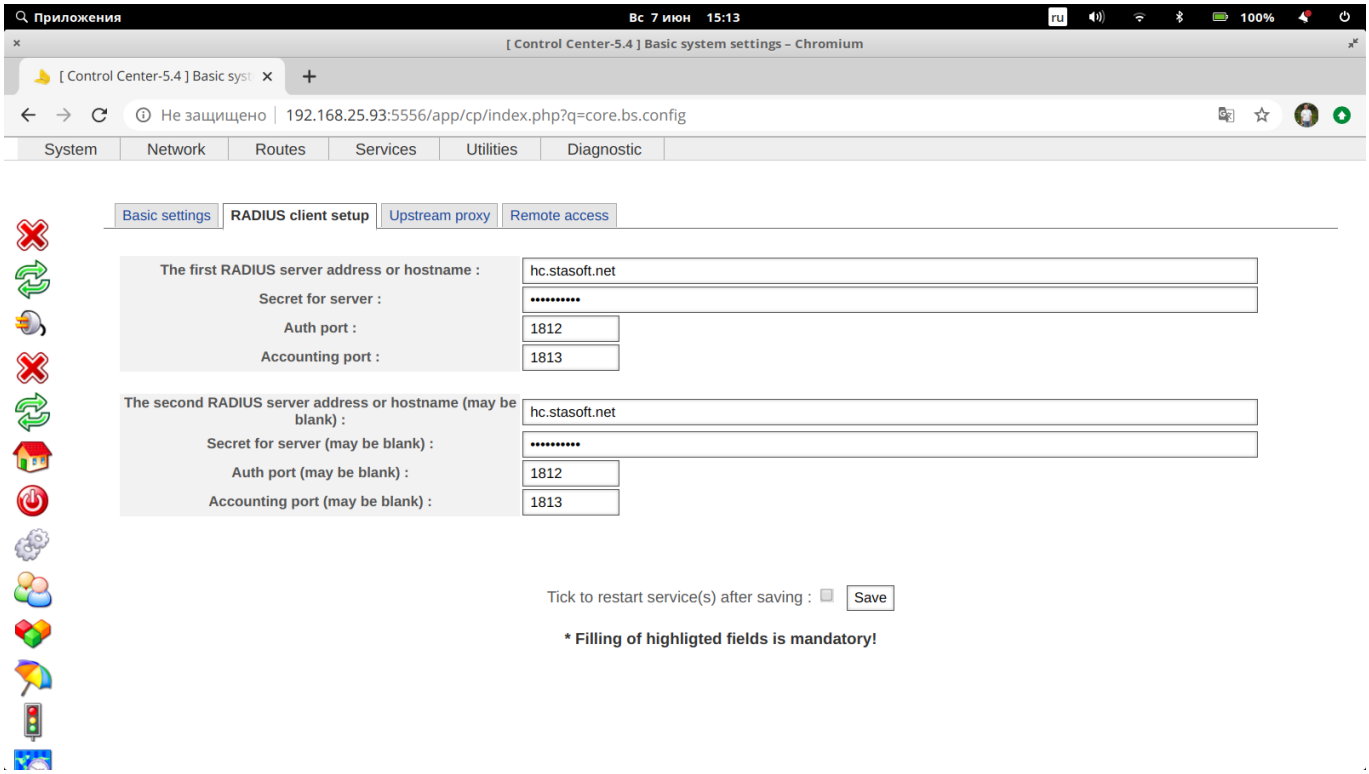


Рисунок 9. Настройка RADIUS

Настройка L2TP-сервера

Для настройки L2TP-сервера выберите пункт меню «Services→Access concentrator→L2TP server / Службы → Концентратор доступа → L2TP сервер», далее:

1. Включите сервер.
2. Выберите внешний интерфейс (обычно eth0).
3. Укажите локальный IP-адрес для L2TP-соединений (ДОЛЖЕН БЫТЬ ОДИНАКОВ ДЛЯ ВСЕХ СЕРВЕРОВ).
4. Укажите первый и последний адреса для назначения клиентам.
5. Указывать адреса серверов имен не требуется.

Для обеспечения уникальности используемых адресов, исключения конфликтов с адресами, применяющимися на оконечных устройствах, мы рекомендуем использовать адреса из диапазона 169.254.0.0/16.

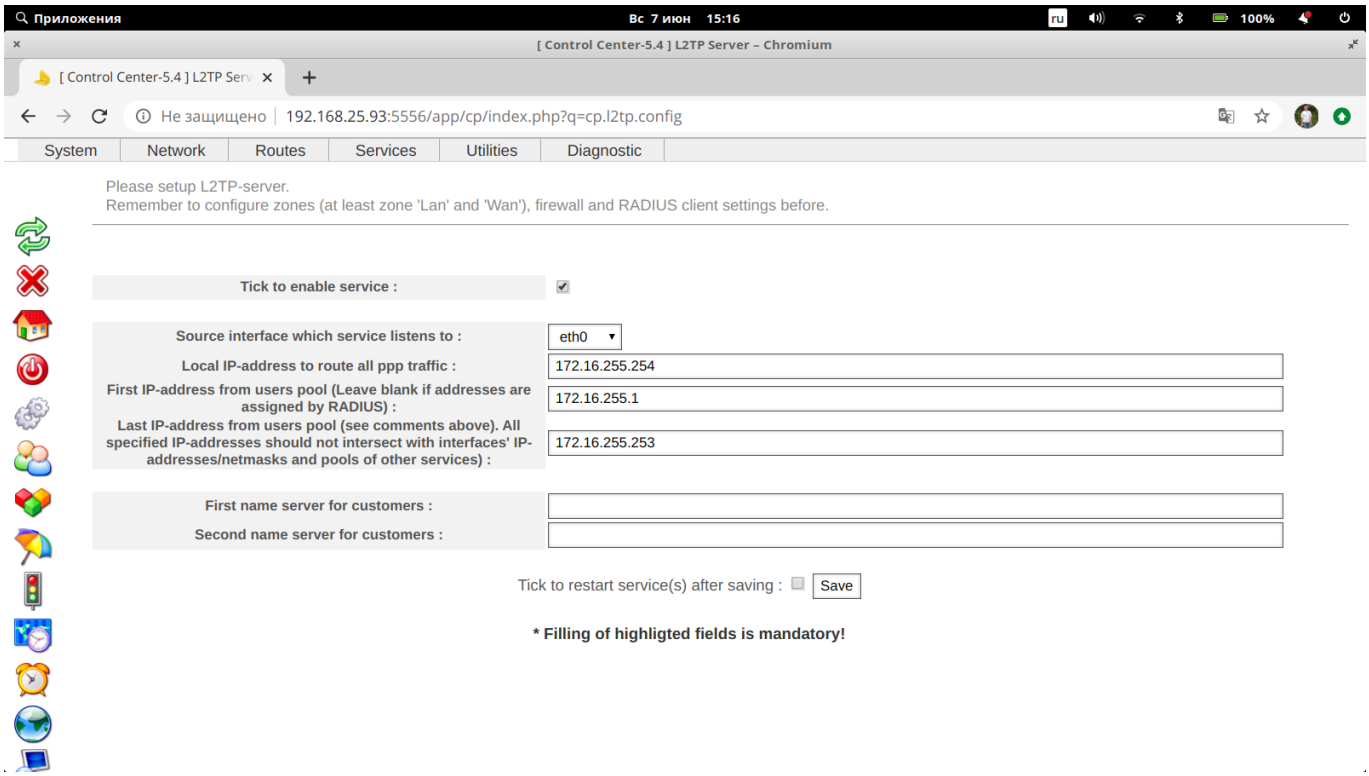


Рисунок 10. Настройка L2TP сервера.

Сохраните изменения и перезапустите сервер.

Проверка сделанных настроек

Для проверки работоспособности, убедитесь, что в списке процессов после перезагрузки присутствует процесс с именем xl2tpd; проверьте настройки межсетевого экрана, прохождение RADIUS-пакетов к серверу RADIUS.

Общий план настройки оконечного устройства

Для оконечного устройства необходимо выполнить следующий набор действий:

1. Настроить подключение устройства к внешней сети.
2. Настроить L2TP-подключение к серверу, указав его адрес или доменное имя, интерфейс подключения к внешней сети в качестве основного, выданные имя пользователя и пароль. Указать MTU согласно рекомендациям из настоящего руководства (1538).
3. Создать и настроить туннель типа GRETAP, указав в качестве удаленного адреса локальный адрес L2TP-сервера, а в качестве основного интерфейса — l2tp. Указать MTU согласно рекомендациям настоящего руководства (1514).
4. Создать сетевой мост без назначения ему IP-адреса и отключенным STP.
5. Включить туннельный интерфейс в состав этого сетевого моста.
6. Высвободить и (или) создать (при отсутствии) или включить имеющийся Ethernet-интерфейс в состав нового сетевого моста.
7. Перезагрузить устройство и проверить работоспособность.

Настройка конечного устройства

Встроенное программное обеспечение некоторых устройств с NETSHe OS может иметь шаблон конфигурации, имеющий предварительно (полностью или частично) настроенные L2TP-соединение, GRETAP туннель, сетевой мост 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.

Данное руководство исходит из наличия сотового подключения к сети Интернет; доступности настроенного сервера, адресуемого по символьному имени или IP-адресу; наличия у пользователя пары «имя пользователя/пароль» для L2TP подключения, указывающего на VLAN, к которому будет осуществляться подключение Ethernet-порта.

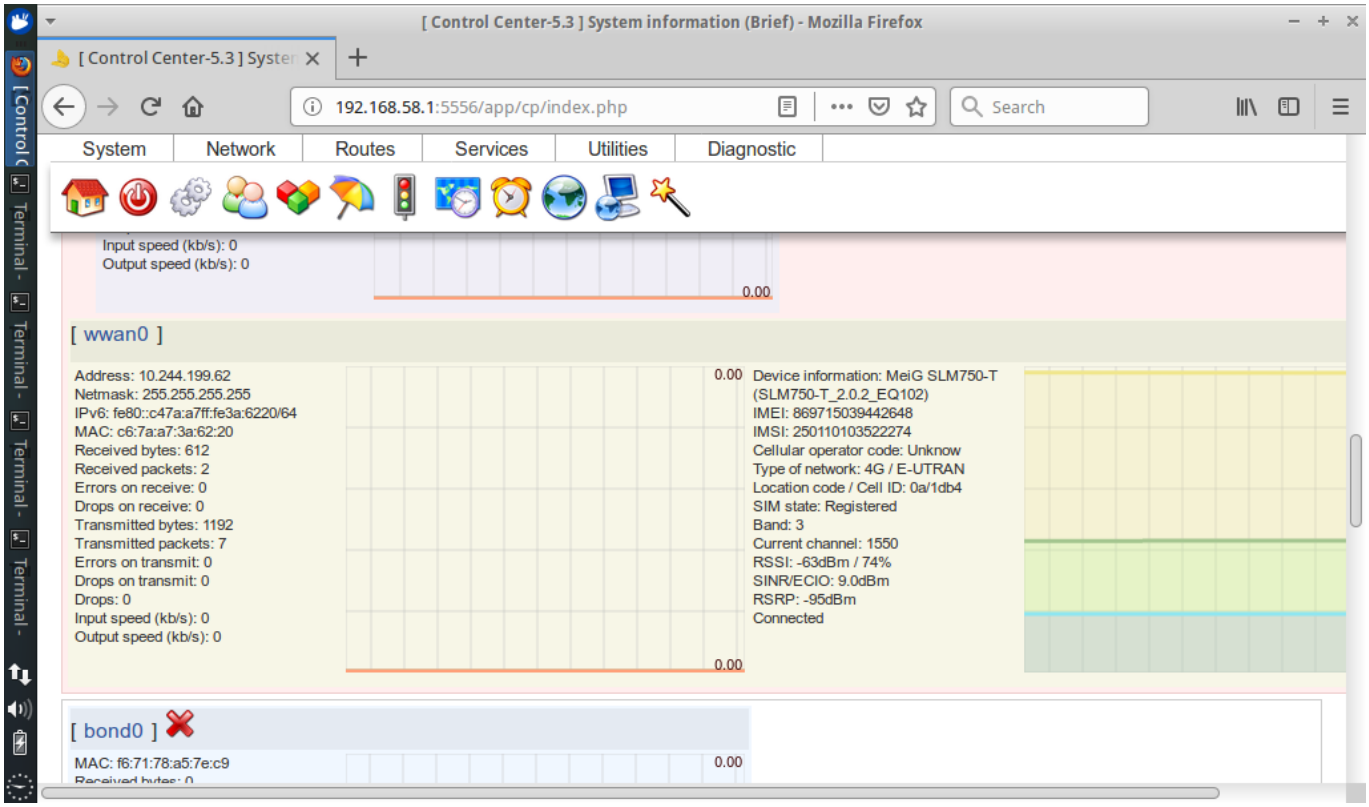


Рисунок 11. Работающее сотовое подключение через интерфейс wwan0

1. Настройка l2tp подключения

Перейдите в меню «Сеть→Интерфейсы / Network→Interfaces», пролистайте страницу до конца (или найдите вверху страницу), введите имя нового интерфейса l2tp, как показано ниже и нажмите кнопку «Новый/New».

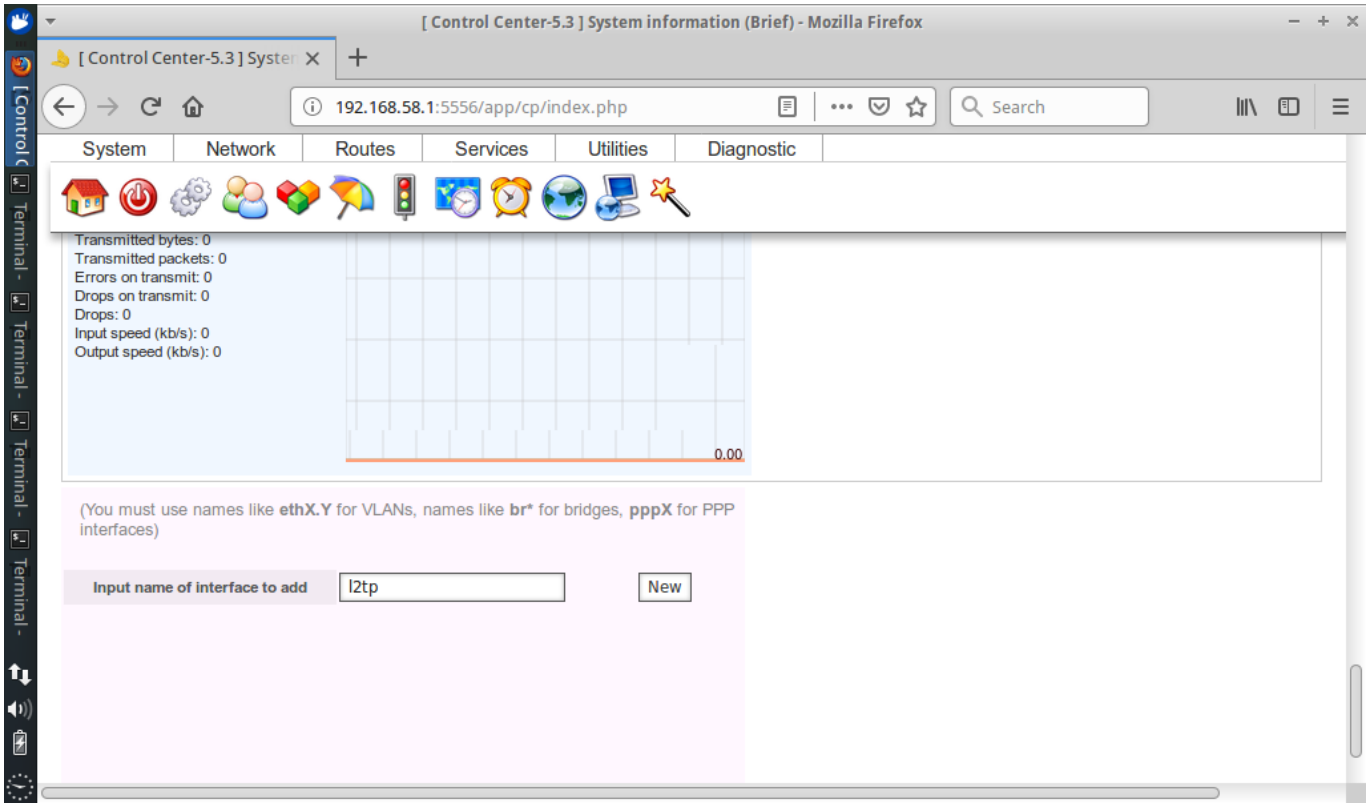


Рисунок 12. Создание нового интерфейса

Вы будете переадресованы на страницу ввода настроек L2TP подключения, как показано на рисунке ниже.

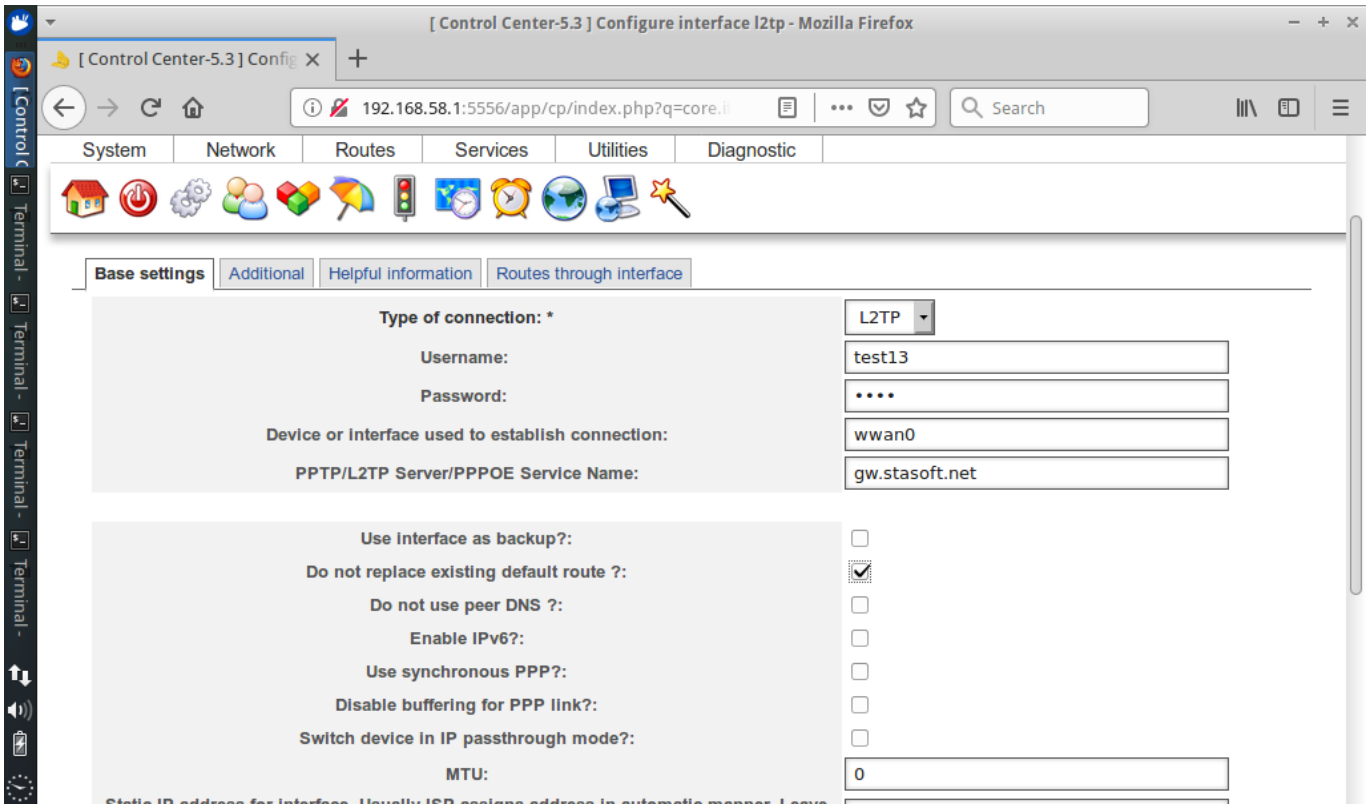


Рисунок 13. Пример настройки L2TP соединения

Заполните:

1. поля «Имя пользователя / Username», «Пароль / Password» назначенной для устройства парой;
2. поле «L2TP сервер / L2TP server» именем или адресом L2TP сервера;
3. поле «Устройство или интерфейс, который будет использован(о) для установки соединения / Device or interface used to establish connection» именем сотового интерфейса (wwan0).
4. Отметьте поле «Не заменять текущий маршрут по умолчанию / Do not replace existing default route».
5. Укажите MTU для интерфейса, рассчитанный по формуле: MTU l2tp = MTUethernet + 38. Для стандартного случая, это 1538.

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

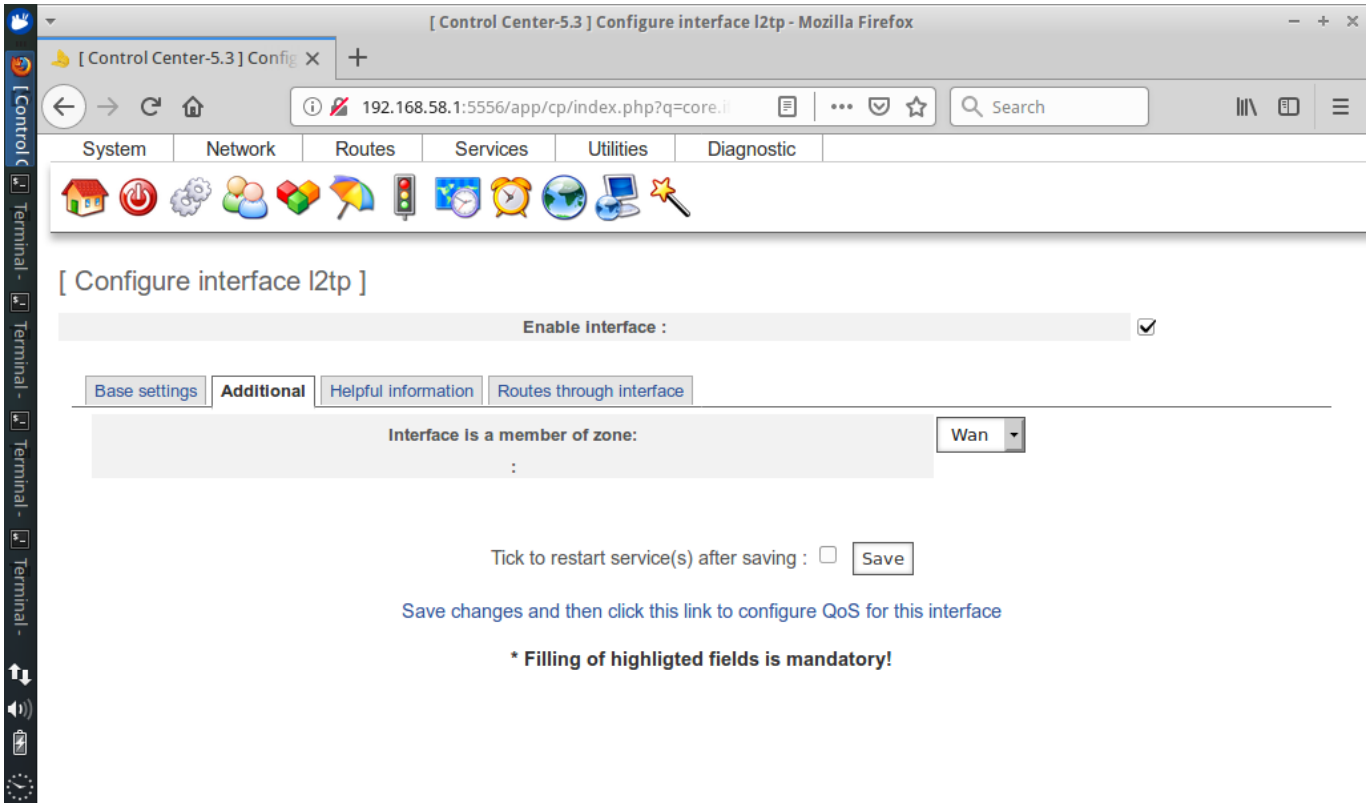


Рисунок 14. Задание зоны WAN для L2TP соединения.

1. Создание GRE туннеля

Вернитесь в список интерфейсов и перейдите к полю ввода нового интерфейса, как показано на рисунке 2.

Введите имя интерфейса (например, int-gretap) и нажмите кнопку «Новый / New».

Внимание! Имя интерфейса должно содержать слово «gretap».

Вы будете перенаправлены на страницу ввода параметров туннеля:

1. Выберите l2tp из списка интерфейсов, как локальный интерфейс для политики/туннеля;
2. Введите адрес внутренний адрес L2TP-сервера в поле ниже (Например, 172.16.255.254);
3. Введите MTU, вычисленный по формуле MTU = MTU ethernet + 14. Для стандартного случая, это 1514.

Нажмите кнопку «Сохранить / Save».

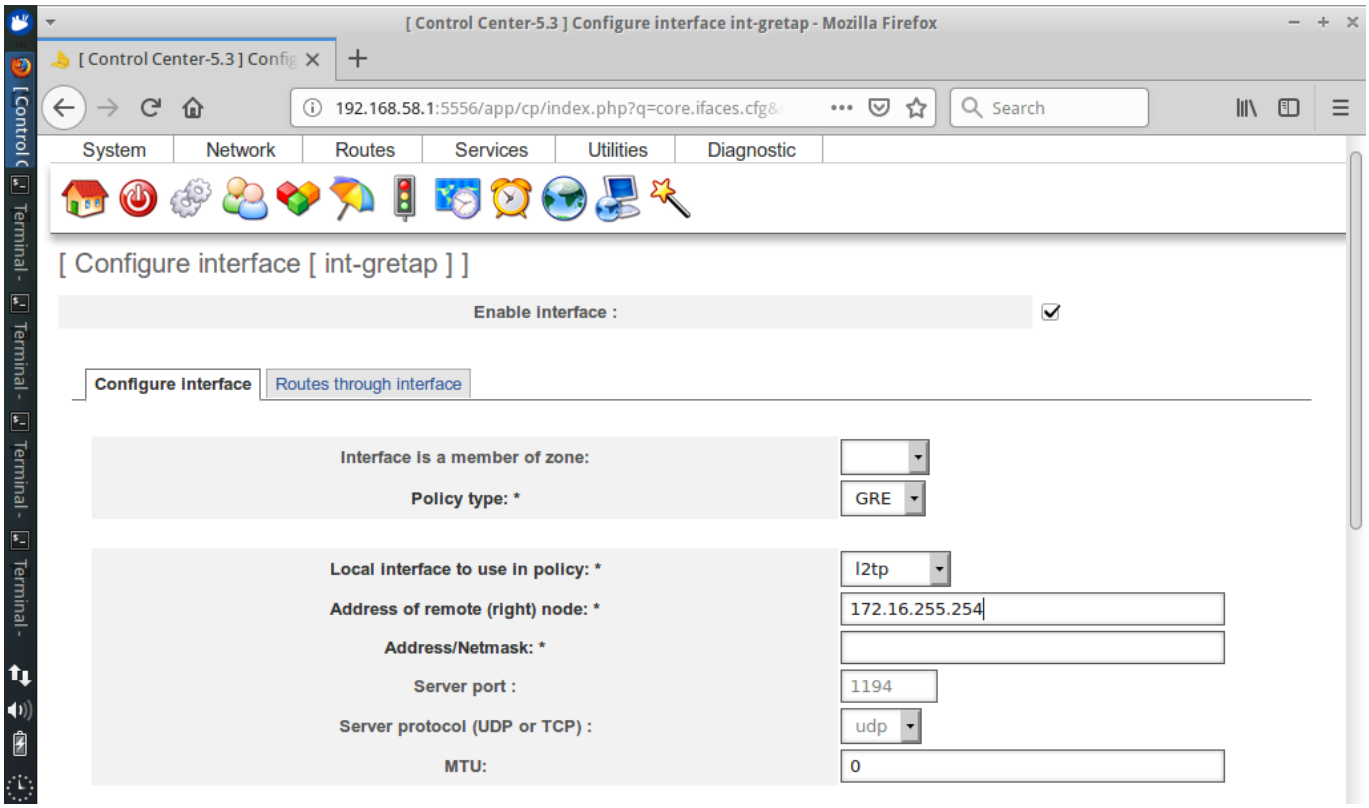


Рисунок 15. Создание GRETAP туннеля.

1. Создание сетевого моста

Данный шаг необходим в случае, если функция объединения сегментов Ethernet-сетей не является единственной. В противном случае переходите к следующему пункту.

Вернитесь в список интерфейсов и перейдите к полю ввода нового интерфейса, как показано на рисунке 2.

Введите имя интерфейса, например br-int и нажмите кнопку «Новый / New».

Внимание! Имя интерфейса должно содержать слово «br».

В открывшемся окне включите интерфейс, убедитесь в отключении STP и включении моста в зону LAN. Нажмите кнопку «Сохранить/Save».

1. Включение GRETAP туннеля в сетевой мост

Выберите пункт меню «Сеть-Сетевые мосты / Network-Bridges».

Найдите только что созданный интерфейс туннеля в списке неназначенных интерфейсов. Найдите прямоугольник подходящего сетевого моста (например, введенного на предыдущем шаге). Перетащите интерфейс в прямоугольник моста, как показано на рисунке ниже, и нажмите кнопку «Сохранить / Save».

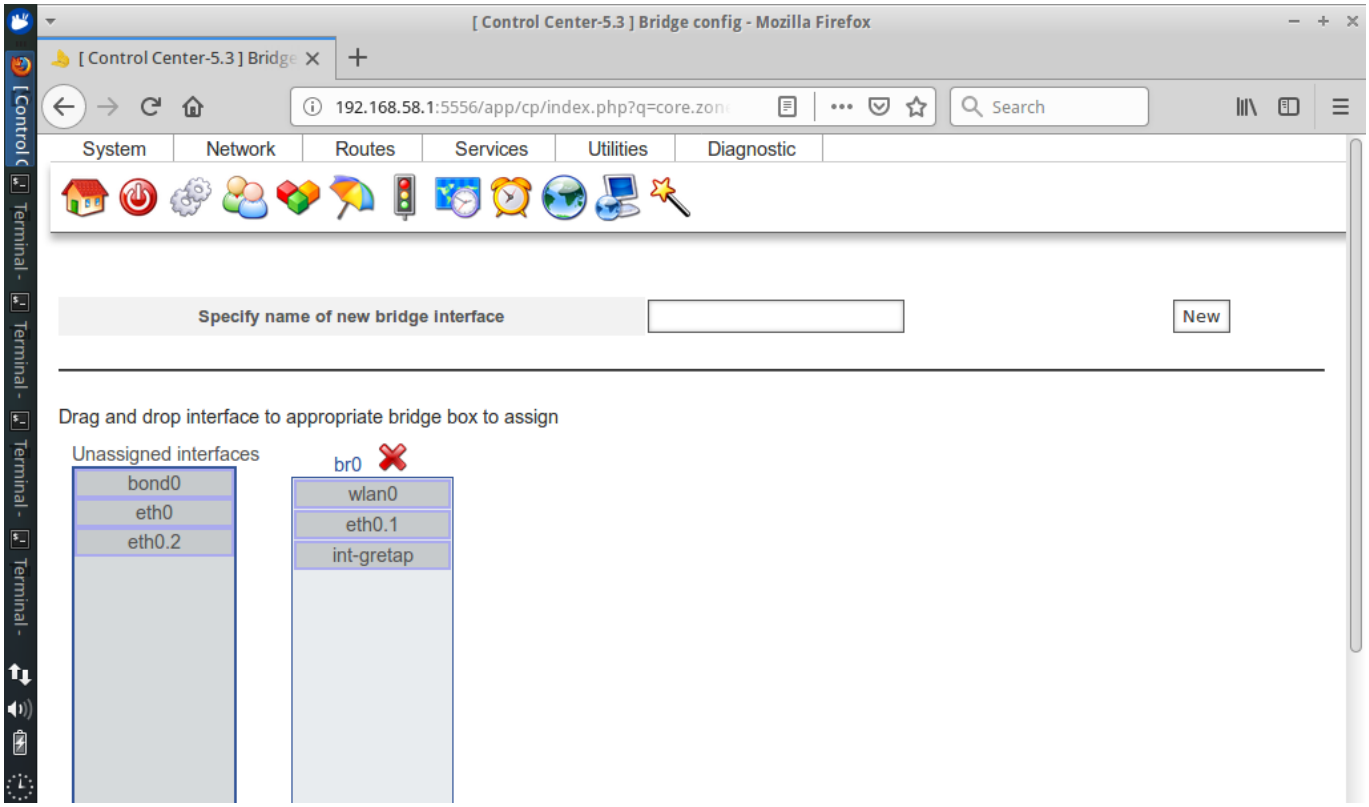


Рисунок 16. Помещение интерфейса int-gretap в мост br0

Включение свободного/нового Ethernet-интерфейса

Включение отдельного Ethernet-интерфейса необходимо в случае, когда функция проброса осуществляется для какого-то отдельного сегмента сети, а другой необходимой функцией оконечного устройства является, например, предоставление доступа в Интернет.

Работа с отдельным интерфейсом требует создания отдельного сетевого моста, как указано двумя шагами выше.

Помещение интерфейса в сетевой мост описано шагом выше.

Создание нового интерфейса описано в основной документации NETSHe или в документации к конкретному устройству.

1. Применение настроек

Процесс настройки завершен. Перезагрузите терминал

Результат. Проверка работоспособности

После нормальной загрузки устройства, в списке сетевых интерфейсов должны присутствовать два интерфейса с IP-адресами:

1. wwan0 — сотовое подключение. Внешний адрес L2TP сервера должен быть доступен через сотовое подключение. Проверить можно подобным образом: ping gw.stasoft.net -Iwwan0;
2. l2tp — туннельное подключение к удаленному серверу. Внутренний адрес L2TP сервера

должен быть доступен подобным образом: ping 172.16.255.254 -I l2tp;

и один интерфейс без IP-адреса — int-gretap.

Интерфейс int-gretap должен присутствовать в списке портов сетевого моста. Проверить можно подобным образом: brctl show br0 (или указав иной сетевой мост).

Все Ethernet-кадры, поступившие на сетевой мост br0 одного устройства, будут переданы через сервер на сетевой мост другого (других) устройств, подключенных к серверу.

Вопросы безопасности

Предлагаемое решение в достаточной степени безопасно, что обеспечено следующими мерами:

1. На оконечном устройстве:
    1. Для второго уровня:
        1. разные Ethernet-сети (при наличии) изолированы друг от друга на уровне отдельных портов, интерфейсов, сетевых мостов. В туннель попадают кадры только указанной сети.
    2. Для третьего уровня:
        1. l2tp соединение не устанавливает и (или) изменяет каких-либо маршрутов на оконечном устройстве.
        2. При создании нового сетевого моста/Ethernet-интерфейса без назначения адресов (что является рекомендуемым), последние также не изменяют/устанавливают каких-либо маршрутов на оконечном устройстве.
        3. Никакие службы оконечного устройства недоступны со стороны L2TP сервера, если иное не определено настройками зоны WAN межсетевого экрана.
2. На сервере / шлюзе:
    1. Для второго уровня:
        1. разные Ethernet-сети изолированы друг от друга на уровне отдельных сетевых мостов и соответствующих им VLAN-интерфейсов. В конкретный туннель попадают кадры только указанной сети.
    2. Для третьего уровня:
        1. Сервер принимает извне только L2TP соединения и авторизует их на RADIUS-сервере. При правильной настройке межсетевого экрана, доступ к каким-либо службам на сервере и сетям за сервером/шлюзом невозможен.

Очевидным и доступным способом повысить безопасность системы является использование IPSec для защиты L2TP соединений между оконечным устройством и шлюзом.

Настройка IPSec, как и альтернативный вариант объединения сегментов — DM EVPN, не являются предметом настоящего руководства.

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

Permanent link:
http://docs.netshe-lab.ru/doku.php?id=%D0%BE%D0%B1%D1%8A%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_ethernet-%D1%81%D0%B5%D1%82%D0%B5%D0%B9

Last update: **2020/07/15 11:56**