Записки IT специалиста
Технический блог специалистов ООО"Интерфейс"

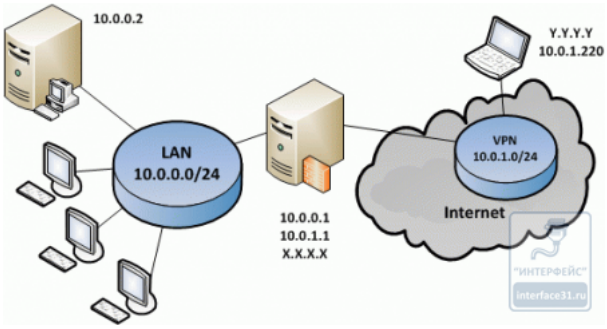
# Настраиваем VPN сервер. Часть 3 - PPTP. Платформа Linux.

Автор: Уваров А.С. — 14.09.2010 21:07 | **201 Comments**


Рассмотрев в предыдущих частях теоретические вопросы перейдем к практической реализации. Сегодня мы рассмотрим создание VPN сервера PPTP на платформе Ubuntu Server. Данный материал рассчитан на читателей, имеющих навыки работы с Linux, поэтому мы не будем отвлекаться на вещи описанные нами в других статьях, таких как настройку сети и т.п. Если вы испытываете затруднения - предварительно изучите другие наши материалы.

Практическое знакомство с VPN мы начнем с PPTP, как наиболее простого в реализации. Однако следует помнить о том, что это слабозащищенный протокол и его не следует использовать для доступа к критически важным данным.

Рассмотрим схему, которую мы создали в нашей тестовой лаборатории для практического знакомства с данной технологией:




У нас имеется локальная сеть 10.0.0.0/24 с сервером терминалов 10.0.0.2 и **роутером**10.0.0.1, который будет выполнять функции VPN сервера, для VPN мы зарезервировали сеть 10.0.1.0/24. Внешний интерфейс сервера имеет условный выделенный IP адрес X.X.X.X. Наша цель - предоставить удаленным клиентам доступ к терминальному серверу и общим ресурсам на нем.

## Настройка сервера PPTP

Установим пакет pptpd реализующий функционал PPTP VPN:

```
sudo apt-get install pptpd
```

Теперь откроем файл **/etc/pptpd.conf** и зададим основные настройки VPN сервера. Перейдем в самый конец файла, где укажем адрес сервера в VPN сети:

```
localip 10.0.1.1
```

И диапазон адресов для выдачи клиентам:

```
remoteip 10.0.1.200-250
```

Адресов нужно выделить не меньше, чем возможных одновременных соединений, лучше с небольшим запасом, так как их увеличение без перезапуска pptpd невозможно. Также находим и раскомментируем строку:

```
bcrelay eth1
```

Это позволит передавать VPN клиентам широковещательные пакеты внутренней сети.

Также можно использовать опции **listen** и **speed**, первая позволяет указать IP адрес локального интерфейса для прослушивания входящих PPTP соединений, второй указать скорость VPN соединений в бит/с. Например разрешим серверу принимать PPTP соединения только с внешнего интерфейса:

```
listen X.X.X.X
```

Более тонкие настройки находятся в файле **/etc/ppp/pptpd-options**. Настройки по умолчанию вполне соответствуют нашим требованиям, однако кратко рассмотрим некоторые из них, чтобы вы имели представление о их назначении.

Секция **#Encryption** отвечает за шифрование данных и проверку подлинности. Данные опции запрещают использование устаревших и небезопасных протоколов PAP, CHAP и MS-CHAP:

```
refuse-pap
refuse-chap
refuse-mschap
```

Форум
Подписка на блог
YouTube

Категории
1С Предприятие 7.7 (13)
1С Предприятие 8.x (52)
Linux - начинающим (9)
OS-обзор (16)
Ubuntu Server и Debian (91)
UNIX-like (16)
Windows 7 (22)
Windows 8 (16)
Windows 10 (9)
Windows Server (73)
Windows XP (9)
Админу на заметку (20)
Антивирусы и безопасность в сети (28)
Виртуализация (15)
Для дома, для семьи (11)
Железо (54)
За рубежом (8)
Общие вопросы (6)
Сайтостроение (16)
Сети и интернет (113)
Системному администратору (195)
Службы каталогов (22)
Страницы истории (4)
Тестовая лаборатория (50)
Хранение и защита данных (71)
Форум

Архивы по месяцам
Выберите месяц…

Реклама

Найти
Найти

Похожие запи
Настраиваем огран скорости для польз Squid
Введение в сеть To
Организация канал офисами при помо OpenVPN на платф
Zimbra. Обновляем установленную вер
Настройка iSCSI-хр Ubuntu Server/Debi
Настраиваем веб-с Nginx как front-end
Zimbra. Обновляем операционную сис (Ubuntu Server)
Linux - начинающи такое Load Average информацию он не
WPAD или автомат настройка парамет прокси
DansGuardian. Наст передачу IP-адреса Squid
Настраиваем веб-с базе Nginx + PHP-FI Debian / Ubuntu Se

Реклама


Облако тегов

Далее предписывается использовать безопасный протокол проверки подлинности MS-CHAP v2 и 128-битное шифрование MPPE-128:

```
require-mschap-v2
require-mppe-128
```

Следующая секция **#Network and Routing**, здесь следует обратить внимание на опцию **ms-dns**, которая позволяет использовать DNS сервер во внутренней сети. Это может быть полезно при доменной структуре сети или наличия в ней DNS сервера который содержит имена всех ПК сети, что дает возможность обращаться к компьютерам по их именам, а не только по IP. В нашем случае данная опция бесполезна и закомментирована. Подобным образом можно задать и адрес WINS сервера опцией **ms-wins**.

Здесь же находится опция **proxyarp**, включающая, как несложно догадаться из названия, поддержку сервером **Proxy ARP.**

В секции **#Miscellaneous** содержится опция **lock**, которая ограничивает клиента одним подключением.

На этом настройку сервера можно считать законченной, осталось создать пользователей. Для этого внесем необходимые записи в **/etc/ppp/chap-secrets**. Записи должны иметь вид:

```
ivanov * 123 *
petrov * 456 10.0.1.201
```

Первая запись позволяет подключаться к серверу пользователю ivanov с паролем 123 и присваивает ему произвольный IP адрес, вторая создает пользователя petrov с паролем 456, которому при подключении будет присваиваться постоянный адрес 10.0.1.201.

Перезапускаем **pptpd**:

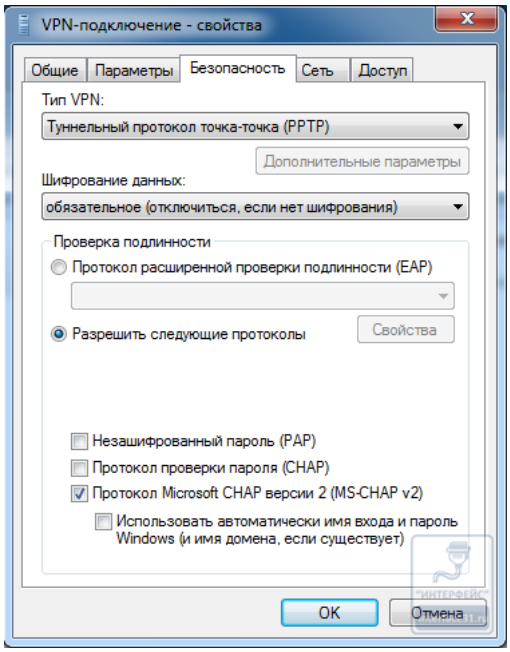
```
sudo /etc/init.d/pptpd restart
```

Важное замечание! Если **pptpd** не хочет перезапускаться, зависая на старте, а в **/var/log/syslog** добавляя строку **long config file line ignored** обязательно добавьте в конец файла **/etc/pptpd.conf** перенос строки.

Наш сервер готов к работе.

## Настройка клиентских ПК

В общем случае достаточно настроить VPN соединение с опциями по умолчанию. Однако мы советуем явно указать тип соединения и отключить лишние протоколы шифрования.




Далее, в зависимости от структуры сети, необходимо указать статические маршруты и основной шлюз. Эти вопросы подробно разбирались в предыдущих частях.

Устанавливаем VPN соединение и пробуем пропинговать какой либо ПК в локальной сети, мы без каких либо затруднений получили доступ к терминальному серверу:



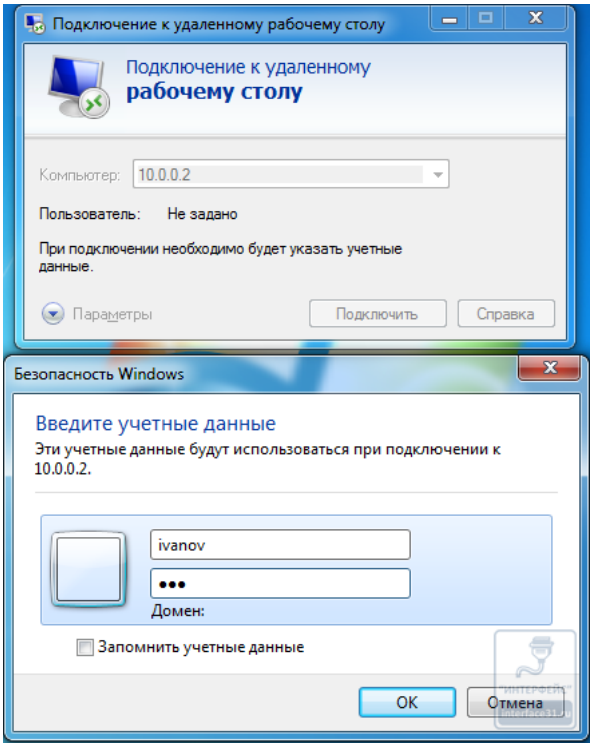
Страницы

Авторам
О блоге
Правила перепечатки

Статистика

География


Ubuntu Ser
Windows Se
Сетевые
технологии
Предприят
HDD Файлов
сервер Activ
Directory Wi
7 Безопасно
DNS Squid
Производите
Debian Диагн
Службы катал
mail Антивир
Linux Window
Автоматизаци
Предприятие
Web-сервер
Развертывани
SSD Ubuntu V
Windows Serv
Виртуализаци
Планировани
iptables DHCP
RAID Wi-Fi Zim
Dnsmasq Micro
Samba SSL Wir
Update
Лицензирован
Рабочее место
Резервное
копирование T
оборудование
PostgreSQL We
Digital Window
Windows XP
Персонализаци
V Kaspersky RDF
Восстановление
Сайт ClamAV Hi
availability LDAP
MySQL PHP PKI
PowerShell Seag
Штрих-код Com
DansGuardian D
NAT SMB USB
Автообмен Внед
Сервер термина
avast IIS Jabber li
mdadm NAS PPTP
WSUS Дедупликац
Apache AVG Avira
HASP HGST iSCSI
Kerberos NOD 32
Openfire OpenVPN
Smartbuy Sysinter
Sysprep torrent El
Удаленое
администрирован
cacher-ng Bitdefend
DLNA Emsisoft Exc
Fedora FreeBSD HT
McAfee Nginx Outl
Outpost Phison PP
Privacy PXE Remov
Toshiba TRIM WAI
WPAD Архивация




Теперь еще одно важное дополнение. В большинстве случаев доступ к компьютерам локальной сети будет возможен только по IP адресам, т.е. путь \\10.0.0.2 будет работать, а \\SERVER - нет. Это может оказаться неудобным и непривычным для пользователей. Существует несколько способов решения данной проблемы. Если локальная сеть имеет доменную структуру, достаточно указать DNS сервером для VPN подключения DNS сервер контроллера домена. Воспользуйтесь опцией **ms-dns** в **/etc/ppp/pptpd-options** сервера и данные настройки будут получены клиентом автоматически. Если DNS сервер в локальной сети отсутствует, то можно создать и использовать WINS сервер, информацию о нем также можно автоматически передавать клиентам при помощи опции **ms-wins**. И наконец, если удаленных клиентов немного, использовать на клиентских ПК файлы **hosts** (C:\Windows\System32\drivers\etc\hosts), куда следует добавить строки вида:

```
10.0.0.2        SERVER
```

По одной для каждого ПК в локальной сети к ресурсам которого требуется доступ.

Дополнительные материалы:

**Категории:** Ubuntu Server и Debian, Сети и интернет, Системному администратору
**Теги:** PPTP, Ubuntu Server, VPN, Сетевые технологии





## Об этой записи

Сообщение опубликовано *14.09.2010 21:07*. Автор — Уваров А.С..

Предыдущая запись — Ubuntu Server. Можно ли эффективно заблокировать торренты?

Следующая запись — Ubuntu Server. Антивирусная защита для файлового сервера (Samba + ClamAV).

Смотрите новые записи на главной странице или загляните в архив, где есть ссылки на все сообщения.

Маршрутизация M
клавиатуры Перев
360 Total ACL Adpre
BeOS BSOD Celeron
Driver FastCGI fetch
GnuPG GPO Haiku
L2TP Let's Encrypt l
Marvell MBAM MS C
MultiSSID NANO NE
Framework Netsh n
NTLM NTP OpenSUS
Panda PC-BSD PHP-
RegExp rktools SAM
SandForce SiliconPo
StarWind Starwind s
TeamViewer TFTP Tr
Inspector Trend Micr
VLAN Windows Serve
Wordpress xCore Zo
Архитектура систем
Клиент-банк Эквайр

**201 Комментариев** **Записки IT специалиста** **Войти**

**Рекомендовать** 2 **Поделиться** **Лучшее в начале**

Присоединиться к обсуждению...

**Sergei** • 2 года назад

Добрый день, как реализовать vpn сервер чтобы клиенты получали статические адреса внутри сети, vpn используется для доступа из вне.

например:
/etc/ppp/chap-secrets
andrey1 pptpd andrey1 172.16.20.20
andrey2 pptpd andrey2 172.16.20.21
andrey3 pptpd andrey3 172.16.20.23

при этом все работают в локалке через адрес 192.168.22.10, а как сделать чтобы пользователи работали в локалке под статичными адресами, например:

172.16.20.20 --> 192.168.22.12
172.16.20.21 --> 192.168.22.13
172.16.20.22 --> 192.168.22.14

1 • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Sergei • 2 года назад

Сразу выдавайте клиентам адреса из диапазона вашей сети.

1 • Ответить • Поделиться ›

**Sergei** ➚ Уваров А.С. • 2 года назад

тоесть здесь /etc/ppp/chap-secrets я прописываю адреса локальной сети ?
а как быть в /etc/ppp/pptpd-options с этим
localip 172.16.20.1
remoteip 172.16.20.100-150

поменять их на
localip 192.168.22.10
remoteip 192.168.22.100-150

так ?

в сети 192.168.22.0/24 у меня никто не живет, там нет dhcp и никаких станций кроме шлюза на 192.168.22.5

1 • Ответить • Поделиться ›

**Roman Pavlovsky** ➚ Sergei • 2 года назад

Да, правильно.

1 • Ответить • Поделиться ›

**Всеволод Пушкарёв** ➚ Уваров А.С. • 3 месяца назад

Сергей! Как с вами связаться? Нужен совет по настройке VPN.

• Ответить • Поделиться ›

**Владимир** • 4 месяца назад

Добрый день. Давно меня интересует вопрос в настройке pptpd, никак не могу найти на

него ответ. Как передать статические маршруты клиенту автоматически во время pptp подключения? В openvpn это реализуется очень просто, либо в конфигурации сервера, либо в конфигурации конкретного пользователя указывается, какие маршруты ему передать. Он подключается и получает все маршруты автоматом с сервера.

А с pptpd на линуксе не могу понять, можно ли это в принципе сделать, или нет. Добавлять вручную или скриптами маршруты клиенту уже после подключения не очень удобно. В openvp это реализовано, думаю, что в pptpd тоже должна быть такая возможность. Это же очень удобно.

• Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Владимир • 4 месяца назад

PPTPD не умеет, но это и не надо, существуют специальные DHCP-опции которые предназначены передавать маршрут: 121 и 249.

• Ответить • Поделиться ›

**Владимир** ➚ Уваров А.С. • 4 месяца назад

Спасибо за информацию. Жаль, что сам pptpd не умеет, я надеялся на простое решение. Придется пробовать с dhcp.

• Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Владимир • 4 месяца назад

А он и не должен, зачем изобретать велосипед, если все уже давно придумано. И с DHCP нет ничего сложного, тот-же dnsmasq настраивается буквально в несколько строк:

```
listen-address=10.8.0.1
dhcp-range=vpn,10.8.0.100,10.8.0.199,255.255.255.0,1h
dhcp-option=tag:vpn,vendor:MSFT,2,1i
dhcp-option=tag:vpn,249,192.168.0.0/24,10.8.0.1
dhcp-option=tag:vpn,121,192.168.0.0/24,10.8.0.1
```

В данном случае добавляется маршрут к 192.168.0.0/24

Также должен быть включен proxyarp в pptpd.

• Ответить • Поделиться ›

**Владимир** ➚ Уваров А.С. • 4 месяца назад

В данном случае 10.8.0.1 адрес pptp интерфейса на сервере?

• Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Владимир • 4 месяца назад

Да

• Ответить • Поделиться ›

**Владимир** ➚ Уваров А.С. • 4 месяца назад

Спасибо за помощь. Настроил я все с помощью dhcpd, так как он уже был в сети. Конечно я бы не сказал, что это очень просто, пришлось повозиться с некоторыми настройками. Для тех, кто будет настраивать, делюсь ссылкой http://www.linux.org.ru/for... Вариант рабочий, только что настроил. Пришлось в обязательном порядке назначать второй ip на физический интерфейс и указывать параметр bcrelay eth0:1 на этот интерфейс. Без этого не работала выдача маршрута по pptp.

• Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Владимир • 4 месяца назад

Ну тонкости уже зависят от конкретной реализации DHCP-сервера.

• Ответить • Поделиться ›

**Иван Гришин** • 6 месяцев назад

Здравствуйте! Прочитал вашу инструкцию, очень содержательный материал для таких как я ). Столкнулся с проблемой: имею сервер с PPTP(192.168.2.0-100 255.255.255.255) к которому должны подключаться удаленно сотрудники, к этому серверу через роутер подключена сеть(192.168.1.0-50 255.255.254.0) из сети с роутера пингуется ккак сам сервер так и удаленные клиенты, а в обратном порядке нет( как с самого сервера не пингуется сеть так и с клиентских машин). Возможно у Вас есть варианты решения?

• Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Иван Гришин • 6 месяцев назад

Вариант решения один - правильно настроить маршрутизацию:
http://interface31.ru/tech_...

• Ответить • Поделиться ›

**Иван Гришин** → Уваров А.С. • 6 месяцев назад
На удаленном VPN сервере при подключении у каждого пользователя появляется свой интерфейс ppp0, ppp1 и т.д. При добавлении нового маршрута он цепляется только к ppp0, при попытке указать другой интерфейс вылетает ошибка: siocaddrt: no such process
Ответить • Поделиться ›

**Уваров А.С.** Модератор → Иван Гришин • 6 месяцев назад
Значит неправильно добавляете, в случае с туннелями надо:

route add -net XXX.XXX.XXX.XXX netmask XXX.XXX.XXX.XXX dev pppX
Ответить • Поделиться ›

**DEN** • год назад
Добрый день! Подскажите куда смотреть, есть домашний ПК за роутером, на ПК поднят pptp-сервер Ubuntu 14.04, клиенты подключаются без проблем, но есть проблема или недопонимания всего процесса, есть желание при создания допустим каким нибудь клиентом соединения с сервером иметь возможность с сервера (с ПК) заходить на расшариные ресурсы клиентского ПК то есть иметь обычную возможность обмена файлами как в локальной сети, на данный момент на сервере (ПК) можно при подключении какого либо клиента в наутилусе в раскладке "сеть" появляется значок машины клиента, но при попытке открыть для просмотра расшариных ресурсом выдает ошибку, что то типо связанное с не возможностью определить местоположение, а в тоже время со стороны клиента , клиент имеет нормальный доступ к открытым ресурсам сервера.
Спасибо.
Ответить • Поделиться ›

**Уваров А.С.** Модератор → DEN • год назад
К удаленным ПК, кроме случаев, когда VPN сеть имеет общее адресное пространство с локальной сетью, следует подключаться через IP. Затем следует проверять настройки брандмауэра на клиенте и права доступа на общие ресурсы.
Ответить • Поделиться ›

**DEN** → Уваров А.С. • год назад
Спасибо что ответили!
В данном случаи адресное пространство совпадают, на сервере видны машины клиентов, но зайти на них не получается , вылетает ошибка, а сами клиенты между собой и с сервером свободно обмениваются данными.
Может что нибудь с маршрутом надо подправить?
Ответить • Поделиться ›

**Уваров А.С.** Модератор → DEN • год назад
Если машина пингуется, то попробуйте обратиться по ip-адресу.
Ответить • Поделиться ›

**DEN** → Уваров А.С. • год назад
Пинг есть! Спасибо будем побывать.
Ответить • Поделиться ›

**arastegaev** • 2 года назад
Hi!
Вы случаем VPN при помощи IPsec не поднимали?
Пытаюсь подружить Zyxell Zywall USG-100 и Ubuntu 14.04
при проверке ipsec verify выдает:
Checking that pluto is running [FAILED]
whack: Pluto is not running (no "/var/run/pluto/pluto.ctl") - и что с ним делать не понятно
Ответить • Поделиться ›

**Уваров А.С.** Модератор → arastegaev • 2 года назад
Смотрите /var/log/auth.log или вывод ipsec barf, там должна быть более подробная информация.
Ответить • Поделиться ›

**PatyHard** • 2 года назад
Как поднять несколько vpn серверов с выделенными статистическими ip на выделенном сервере?
Ответить • Поделиться ›

**Уваров А.С.** Модератор → PatyHard • 2 года назад
Что значит "несколько серверов"? Один сервер может принимать подключения на

разных адресах.

Ответить • Поделиться ›

**PatyHard** ➚ Уваров А.С. • 2 года назад

да вот такое надо чтоб сервер принимал подключения на разные статичные ip и отсылал с тогоже ип с которым с впн сервером соединились.НУ или принимал с разных портов но в интернете спредствлялся разными статичными ip в зависимости от порта.Возможно такое?Если да то как такое реализовать?

Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ PatyHard • 2 года назад

Давайте начнем с того, что вы вообще хотите получить, какая задача стоит?

Ответить • Поделиться ›

**PatyHard** ➚ Уваров А.С. • 2 года назад

Сама задача:для серфинга в интернете нужно 12 индивидуальных ip адресов.

Ответить • Поделиться ›

**gena** • 2 года назад

Добрый день, подскажите какой командой можно посмотреть кто подключен в данное время????

Ответить • Поделиться ›

**vladimir** ➚ gena • 2 года назад

ifconfig, дальше смотри в строке с указанием номера интерфейса ip адрес, а потом сверяй полученный ip адрес с логином из /etc/ppp/chap-secrets.

Ответить • Поделиться ›

**Igor Ilin** • 2 года назад

Добрый день. У меня такая проблема. Настроил VPN сервер на работе. Коннекчусь с дома. Есть коннект, но вот интернет сразу пропадает. Локальную сеть как бы вижу) подскажите в каком направлении копать?) Спасибо)

Ответить • Поделиться ›

**Roman Pavlovsky** ➚ Igor Ilin • 2 года назад

Правой кнопкой мышки на VPN-подключении -> Свойства -> Закладка "Сеть" -> Пункт "Протокол Интернета версии 4 (TCP/IPv4)" - > Свойства -> Закладка "Общие" -> Кнопка "Дополнительно" -> Закладка "Параметры IP" и снимаем галочку с пункта "Использовать основной шлюз в удаленной сети". Потом на всех окнах нажимаем "ОК" и переподключаемся.

1 Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Roman Pavlovsky • 2 года назад

Правильно, первая часть в самом конце, тоже самое в картниках: http://interface31.ru/tech_...

Ответить • Поделиться ›

**Igor Ilin** ➚ Уваров А.С. • 2 года назад

Спасибо за ответ! но вот хотелось бы, что бы и интернет шел так же через VPN. В качестве файрволла стоит Траффик инспектор на работе. Дома только доступ доступ по на сайтам находящимся в нашей доменной зоне страны. А вот выход в мир, мне не доступен. Приходится вот так выкручиваться. Да и еще вопрос. Стат IP обязателен для VPN клиента?

Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Igor Ilin • 2 года назад

Настраивайте на работе маршрутизацию интернета в туннель, насколько я помню, в Траффик-инспекторе нужно еще разрешить RAS-клиентов. Выделенный IP для клиента не нужен.

1 Ответить • Поделиться ›

**Igor Ilin** ➚ Уваров А.С. • 2 года назад

Спасибо большое за консультацию) вы внесли последнюю ясность в моем непростом деле) оказалось, да, надо было в траффик инспекторе накрутить для RAS клиентов) теперь все работает и я очень доволен) спасибо вам, Уважаемый А.С)

Ответить • Поделиться ›

**Андрей** • 3 года назад

Добрый вечер.
Подскажите, возникла необходимость организовать доступ к домашней локальной сети, т.е. к серверу, настроенному по вашим статьям и к принтерам расположенным в локальной сети, из внешних сетей. Т.е. предвидится что я перемещаясь с мобильным устройством (смартфон, ноутбук, планшет) могу зайти на домашний сервер и загрузить, распечатать и т.д. документы и фотографии.
Как бы Вы порекомендовали организовать доступ из вне, реализовать через pptpd или через openvpn или как нибудь иначе ?
Спасибо.

^ | v • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Андрей • 3 года назад

Может вам лучше использовать режим Удаленного рабочего стола? VPN - просто канал между двумя хостами или сетями, который позволяет им работать в одной сети. А там смотрите по задачам и приложениям.

^ | v • Ответить • Поделиться ›

**Андрей** ➚ Уваров А.С. • 3 года назад

Я знаю что VPN это просто туннель, но "оказавшись" в одной сети с домашним сервером я могу получить доступ к samba-ресурсам и т.д. как будто нахожусь дома. А как "прикрутить" удаленный рабочий стол к серверу на Ubuntu для меня если честно полная загадка.

^ | v • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Андрей • 3 года назад

Удаленный рабочий стол, это для Windows машин. По VPN вы конечно сможете получить доступ к ресурсам домашней сети, но не забывайте, что пропускная способность будет ограничена шириной канала.

^ | v • Ответить • Поделиться ›

**Андрей** ➚ Уваров А.С. • 3 года назад

Да, я понимаю про ограничения накладываемые шириной канала; но так как ставящиеся задачи не подразумевают интенсивного и постоянного использование канала из вне, а будут носить скорее эпизодический характер, то шириной канала можно пренебречь.

^ | v • Ответить • Поделиться ›

**Sergio** • 3 года назад

Пол дня убил, пол интернета перерыл, пока сам не догадался открыть порт 1723, могли бы и написать...

^ | v • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ Sergio • 3 года назад

Ну это азы, если вы беретесь настраивать VPN, то должны иметь представление о iptables и что и зачем там надо настраивать.

^ | v • Ответить • Поделиться ›

**gena** • 3 года назад

добрый вечер, подскажите как можно ограничить подключение, что бы человек мог подключаться только с определенного айпи провайдера, а с других не пускало, например у сотрудника есть ноутбук он на работе подключается все нормально работает, а если он его забирает домой, что бы с его домашней сети не пускало??

^ | v • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ gena • 3 года назад

Закройте доступ к порту 1723 через iptables. Например так:

iptables -A INPUT -p tcp ! -s 192.168.0.0/24 --dport 1723 -j DROP

Данная строка запретит подключения к 1723 для всех, кроме подсети 192.168.0.0/24

^ | v • Ответить • Поделиться ›

**gena** ➚ Уваров А.С. • 3 года назад

подскажите еще, а если нужно разрешит 2 или 3 подсетям как тогда правильно записать????

^ | v • Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ gena • 3 года назад

Тогда делаете так:

iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 1723 -j ACCEPT

iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 1723 -j ACCEPT

iptables -A INPUT -p tcp --dport 1723 -j DROP

T.e. вначале разрешаете доступ нужным адресам / подсетям, потом запрещаете остальным. Помните, что правила в цепочке обрабатываются последовательно, до первого срабатывания.

Ответить • Поделиться ›

**gena** ➚ Уваров А.С. • 3 года назад

то есть если одна подсеть подключилась то другая уже не сможет подключиться?

Ответить • Поделиться ›

**Уваров А.С.** Модератор ➚ gena • 3 года назад

Почему? Просто если вы первым поставите запрещающее правило, то подключиться не сможет никто.

Пришедший пакет последовательно сравнивается с правилами в цепочке, если какое-то правило сработало - остальные не применятся. Далее пакет либо идет дальше, либо убивается, в зависимости от правил.

Ответить • Поделиться ›