Записки IT специалиста
Технический блог специалистов ООО"Интерфейс"

Настраиваем VPN сервер. Часть 1 - Общие вопросы.

Автор: Уваров А.С. — 07.08.2010 13:07 | **48 Comments**

Развертывание VPN сервера в сети предприятия является более сложной задачей, чем настройка базовых служб - NAT, DHCP и файловых серверов. Перед тем как браться за дело необходимо четко представлять структуру будущей сети и задачи которые должны решаться с ее помощью. В этой статье мы затронем основные вопросы ответы на которые вы должны твердо знать еще до того, как подойдете к серверу. Такой подход позволит избежать множества типовых проблем и бездумного копирования настроек из примера, а также позволит правильно настроить VPN именно для своих задач и потребностей.

Что такое VPN?

VPN (*Virtual Private Network*) - виртуальная частная сеть, под этой аббревиатурой скрывается группа технологий и протоколов позволяющих организовать логическую (виртуальную) сеть поверх обычной сети. Широко применяется для разграничения доступа и повышения безопасности корпоративных сетей, организации безопасного доступа к ресурсам корпоративной сети извне (через интернет) и, в последнее время, провайдерами городских сетей для организации доступа в интернет.

Какие типы VPN бывают?

В зависимости от применяемого протокола VPN подразделяются на:

- **PPTP** (Point-to-point tunneling protocol) -- туннельный протокол типа точка-точка, позволяет организовать защищенное соединение за счет создания специального туннеля поверх обычной сети. На сегодняшний день это наименее безопасный из всех протоколов и его не рекомендуется применять во внешних сетях для работы с информацией доступ к которой для посторонних лиц нежелателен. Для организации соединения используется две сетевых сессии: для передачи данных устанавливается PPP сессия с помощью протокола GRE, и соединение на TCP порту 1723 для инициализации и управления соединением. В связи с этим нередко возникают сложности с установлением подобного соединения в некоторых сетях, например гостиничных или мобильных операторов.
- **L2TP** (*Layer 2 Tunneling Protocol*) -- протокол туннелирования второго уровня, более совершенный протокол, созданный на базе PPTP и L2F (протокол эстафетной передачи второго уровня от Cisco). К его достоинствам относится гораздо более высокая безопасность за счет шифрования средствами протокола IPSec и объединения канала данных и канала управления в одну UDP сессию.
- **SSTP** *(Secure Socket Tunneling Protocol)* -- протокол безопасного туннелирования сокетов, основан на SSL и позволяет создавать защищенные VPN соединения посредством HTTPS. Требует для своей работы открытого порта 443, что позволяет устанавливать соединения из любого места, даже находясь за цепочкой прокси.

Для чего обычно применяют VPN?

Рассмотрим несколько наиболее часто используемые применения VPN:

- **Доступ в интернет.** Чаще всего применяется провайдерами городских сетей, но также весьма распространенный способ и в сетях предприятий. Основным достоинством является более высокий уровень безопасности, так как доступ в локальную сеть и интернет осуществляется через две разные сети, что позволяет задать для них разные уровни безопасности. При классическом решении - раздача интернета в корпоративную сеть - выдержать разные уровни безопасности для локального и интернет трафика практически не представляется возможным.
- **Доступ в корпоративную сеть извне,** также возможно объединение сетей филиалов в единую сеть. Это собственно то, для чего и задумывали VPN, позволяет организовать безопасную работу в единой корпоративной сети для клиентов находящихся вне предприятия. Широко используется для объединения территориально разнесенных подразделений, обеспечения доступа в сеть для сотрудников находящихся в командировке или на отдыхе, дает возможность работать из дома.
- **Объединение сегментов корпоративной сети.** Зачастую сеть предприятия состоит из нескольких сегментов с различным уровнем безопасности и доверия. В этом случае для взаимодействия между сегментами можно использовать VPN, это гораздо более безопасное решение, нежели простое объединение сетей. Например, таким образом можно организовать доступ сети складов к отдельным ресурсам сети отдела продаж. Так как это отдельная логическая сеть, для нее можно задать все необходимые требования безопасности не влияя на работу отдельных сетей.

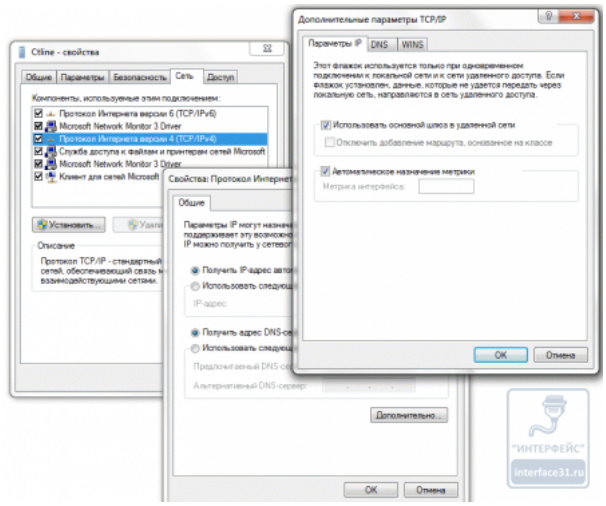
Настройка VPN соединения.

В качестве клиентов VPN сервера с большой болей вероятности будут выступать рабочие станции под управлением Windows, в то время как сервер может работать как под Windows, так и под Linux или BSD, поэтому будем рассматривать настройки соединения на примере Windows 7. Мы не будем останавливаться на базовых настройках, они просты и понятны, Остановимся на одном тонком моменте.

При подключении обычного VPN соединения основной шлюз будет указан для VPN сети, то есть интернет на клиентской машине пропадет или будет использоваться через подключение в удаленной сети.

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
WPAD или автомат настройка парамет прокси
DansGuardian. Наст передачу IP-адреса Squid
Настраиваем проб в Windows при пом командной строки
Настраиваем FTP-с виртуальными пользователями на vsftpd
Организация VPN м между офисами. Маршрутизация
Настраиваем Squid работы с Active Dire Часть 3 - Авторизац основе групп AD
Настраиваем Squid работы с Active Dire Часть 2 - Kerberos-аутентификация
Настраиваем Squid работы с Active Dire Часть 1 - базовые н
Реклама

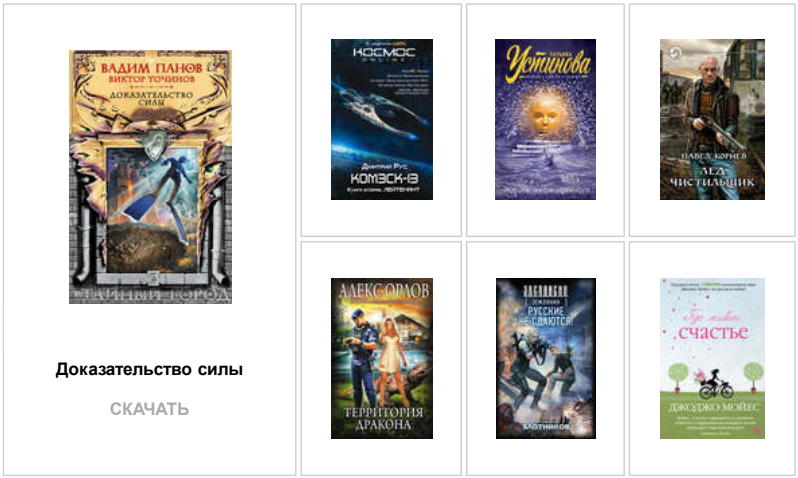
Понятно, что это как минимум неудобно, а в ряде случаев способно привести к двойной оплате трафика (один раз в удаленной сети, второй раз в сети провайдера). Для исключения этого момента на закладке **Сеть** в свойствах протокола **TCP/IPv4** нажимаем кнопку **Дополнительно** и в открывшемся окне снимаем галочку **Использовать основной шлюз в удаленной сети**.



Мы бы не останавливались на этом вопросе столь подробно, если бы не массовое возникновение проблем и отсутствие элементарных знаний о причинах такого поведения VPN соединения у многих системных администраторов.

В **следующей части** нашей статьи мы рассмотрим другую актуальную проблему - правильную настройку маршрутизации для VPN клиентов, что является основой грамотного построения VPN сетей уровня предприятия.

Дополнительные материалы:



Доказательство силы

СКАЧАТЬ

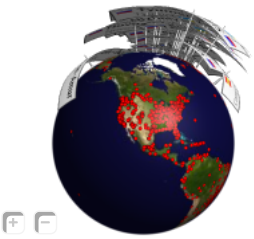
Категории: Сети и интернет, Системному администратору
Теги: VPN, Сетевые технологии

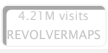
Страницы

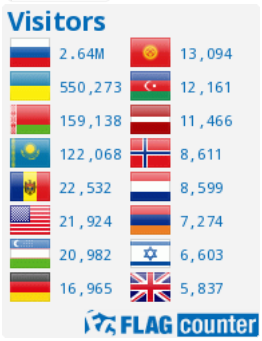
Авторам
О блоге
Правила перепечатки

Статистика

География







Облако тегов

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 Wi
Update
Лицензирован
Рабочее место
Резервное копирование
оборудование
PostgreSQL We

48 Комментариев **Записки IT специалиста** **Войти**

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

Присоединиться к обсуждению...

Уваров А.С. Модератор • 6 лет назад
Если можно поподробнее с адресацией, если адреса домашней и рабочей сети лежат в одном диапазоне то можно попробовать активировать режим proxy ARP на VPN сервере, что позволит обойтись без маршрутизации.

Автоматически получать маршрут клиент не может, однако вы можете запускать соединение пакетным файлом, который будет добавлять маршрут или смотрите в сторону OpenVPN.
1 • Ответить • Поделиться ›

Игорь • год назад
Кто мне сможет обьяснить как защитить свойсмартфон или планшет отпроникновения в него инами лицами по удалёному доступу? Моя подруга наблюдала как её смартфон работал независимо от её действий ,. Удалялись файлы , просматривались фото и переписки в сетях
• Ответить • Поделиться ›

Уваров А.С. Модератор ➦ Игорь • год назад
Вы какие-то чудеса тут рассказываете. На самом деле все просто: не ставить неизвестные приложения, даже из маркета, а если ставите - смотреть на требуемые разрешения и думать. Ну и хороший коммерческий антивирус не помешает.
1 • Ответить • Поделиться ›

Рома • 2 года назад
Какие основные причины нестабильной работы канала (периодическое пропадание связи) ? Если провайдер предоставляет интернет, а поверх интернета поднять VPN ?
• Ответить • Поделиться ›

Уваров А.С. Модератор ➦ Рома • 2 года назад
Причин может быть много, от нестабильной работы сервера или клиента, до сбоя на любом этапе прохождения пакетов.

По второму вопросу: с какой целью это планируете?
• Ответить • Поделиться ›

arch • 2 года назад
Здравствуйте.
Ещё не рассмотрен вид VPN-SSTP детально. Как определить какой алгоритм шифрования (битность) после установления соединения по данному протоколу? Если при использовании PPTP или например L2TP (L2TP/IPSec) это можно узнать из свойств соединения - подробно, то каким образом это можно сделать при использовании SSTP? И как вообще должна выглядеть эта вкладка SSTP-соединения при адекватном подключении? На одном англоязычном сайте видел скрин, где на этой вкладке наряду с другими параметрами (проверка подлинности и т.д.) был указан тип соединения - PPP. У себя подобного не наблюдаю.
• Ответить • Поделиться ›

Об этой записи

Сообщение опубликовано *07.08.2010 13:07*. Автор — Уваров А.С..

Предыдущая запись — 1С Предприятие 7.7 Тестирование производительности в различных режимах.

Следующая запись — Настраиваем VPN сервер. Часть 2 - Маршрутизация и структура сети.

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

Digital Windows
Windows XP
Персонализаци
V Kaspersky RDP
Восстановление
Сайт ClamAV Hig
availability LDAP
MySQL PHP PKI
PowerShell Seaga
Штрих-код Com
DansGuardian Di
NAT SMB USB
Автообмен Внед
Сервер термина
avast IIS Jabber lig
mdadm NAS PPTP
WSUS Дедуплика
Apache AVG Avira
HASP HGST iSCSI
Kerberos NOD 32
Openfire OpenVPN
Smartbuy Sysinter
Sysprep torrent EF
Удаленое
администрирован
cacher-ng Bitdefend
DLNA Emsisoft Exc
Fedora FreeBSD HT
McAfee Nginx Outl
Outpost Phison PP
Privacy PXE Remov
Toshiba TRIM WAIK
WPAD Архивация
Маршрутизация M
клавиатуры Перев
360 Total ACL Adpre
BeOS BSOD Celeron
Driver FastCGI fetch
GnuPG GPO Haiku
L2TP Let's Encrypt lo
Marvell MBAM MS C
MultiSSID NANO NE
Framework Netsh n
NTLM NTP OpenSUS
Panda PC-BSD PHP-
RegExp rktools SAM
SandForce SiliconPow
StarWind Starwind s
TeamViewer TFTP Tr
Inspector Trend Micr
VLAN Windows Serve
Wordpress xCore Zo
Архитектура системь
Клиент-банк Эквайр

Уваров А.С. Модератор ➚ arch • 2 года назад

Вообще должно быть все на вкладке соединения, к сожалению сейчас негде посмотреть, как оно выглядит.\

А тип соединения PPP у вас будет и так, любой VPN - это соеднинеие точка-точка, т.е. PPP (Point-to-Point Protocol), а во что он завернут - это уже зависит от технологии установления соединения.

^ | v • Ответить • Поделиться ›

arch ➚ Уваров А.С. • 2 года назад

При создании vpn-соединения на вкладке Безопасность есть возможность выбора проверки подлинности:
*Протокол расширенной проверки подлинности
где в выпадающем меню можно выбрать
Microsoft: Защищённый пароль (EAP-MSCHAPv2)(шифрование включено)
и др.
В каких случаях эти протоколы проверки уместно использовать и что для этого необходимо, в случае подключения по SSTP?

^ | v • Ответить • Поделиться ›

Уваров А.С. Модератор ➚ arch • 2 года назад

Данные протоколы используются в зависимости от настройки вашего сервера и относятся к PPP части соединения, к типу подключения они отношения не имеют.

^ | v • Ответить • Поделиться ›

arch ➚ Уваров А.С. • 2 года назад

Насколько понимаю, для использования протоколов расширенной проверки подлинности необходима установка сертификата на клиенте?
Вообще, объясните пожалуйста, что это и в каких случаях использовать эти три установки (скрин)?
P.S. удалите лишний.

^ | v • Ответить • Поделиться ›

Уваров А.С. Модератор ➚ arch • 2 года назад

Не нужно. Данные настройки выбираются в зависимости от настроек сервера. Как норма жизни используется MSCHAP-2, EAP на сегодня слаб, смарт-карта - удел корпоративных сетей и т.п.

Но в любом случае проверка подлинности будет работать не та, которую вы выбрали на этой вкладке, а та, которую поддерживает сервер. Если вы установили что-то другое - подключиться не получится.

^ | v • Ответить • Поделиться ›

arch ➚ Уваров А.С. • 2 года назад

Сертификат не нужен совсем. Понял.
То что на сервере и клиенте должены быть устанрвлены одинаковые параметры для протоколов аутентификации догадывался. Ну это в общем и понятно - иначе коннект должен быть неудачным.
Вот моя вкладка состояние - подробно SSTP.
MSCHAP-v2 самодостаточный уровень проверки подлинности?
В настройках указал уровень шифрования: максимальный иначе отключаться (скрин).
Вот вопрос).
Если в настройках указываю без шифрования, иначе отключаться, то коннект всё равно успешен и соединение с сервером устанавливается. Причём эта указанная вкладка (что на скрине) абсолютно идентична.
Если использовать PPTP или L2TP/IPSec, то соединение не устанавливается с выводом сообщения о соответствующих ошибках.

Если указываю максимальный уровень шифрования, то в свойствах

показать больше

Ответить • Поделиться ›

Уваров А.С. Модератор → arch • 2 года назад

Вы не путайте проверку подлинности и настройки шифования PPP сессии. Сейчас специально посмотрел спецификации, PPP внутри SSTP не шифруется, так как уже зашифрован SSL.

Ответить • Поделиться ›

arch → Уваров А.С. • 2 года назад

И не путаю. Просто вопросы плавно перетекли в другое русло. Вот хотел узнать, как при SSTP узнать уровень шифрования сессии передачи самих данных? Почему присутствуют вышеуказанные нюансы означенного протокола?
Знать надо, а информации нигде нет и не найдёшь.

Сервис утверждает("Протокол SSTP использует 2048 бит SSL / TLS сертификаты для проверки подлинности и 256-битным ключ SSL для шифрования."), что шифрование по передачи данных SSL - AES-256bit. В случае с L2TP или PPTP (128bit - MPPE) в этом убедиться легко на вкладке состояния. А как это проверить при SSTP?

Ответить • Поделиться ›

Уваров А.С. Модератор → arch • 2 года назад

Еще раз, L2TP или PPTP предусматривают шифрование PPP-сессии, что отображается на вкладке соединения. SSTP не шифрует PPP-пакеты, так как они находятся внутри SSTP-пакетов и зашифрованы SSL.

T.e. SSTP канал по любому зашифрован на уровне SSL, как минимум это 128-битный AES, чего вполне достаточно для защиты данных.

1 Ответить • Поделиться ›

arch → Уваров А.С. • 2 года назад

С шифрованием понятно. Спасибо.

Ответить • Поделиться ›

Roman Pavlovsky • 3 года назад

Здравствуйте.
Подскажите, что нужно анализировать в tcpdump, чтобы выявить причину отвала VPN, когда на клиенте прописываешь маршрут либо в браузере пытаешься открыть IP адрес сервера VPN?
Либо может есть какой-то "фирменный" анализатор пакетов, который ведет лог в реальном времени и покажет причину отвала VPN?

Ответить • Поделиться ›

Уваров А.С. Модератор → Roman Pavlovsky • 3 года назад

Попробуйте Wireshark, а причин отвала может быть множество, надо смотреть и думать.

Ответить • Поделиться ›

Roman Pavlovsky → Уваров А.С. • 3 года назад

Так я дамп сделал, открыл его в Wireshark, а дальше не знаю что именно нужно искать, так как с чистым VPN не приходилось работать.

Ответить • Поделиться ›

Уваров А.С. Модератор → Roman Pavlovsky • 3 года назад

Отфильтруйте трафик к VPN серверу и смотрите что происходило в течении сессии. Тип VPN какой?

Ответить • Поделиться ›

Roman Pavlovsky → Уваров А.С. • 3 года назад

PPTP.

Безопасность:
CHAP
MS-CHAP v2

Шифрование:
обязательное (если нет шифрования, отключиться)

Ответить • Поделиться ›

Уваров А.С. Модератор → Roman Pavlovsky • 3 года назад

Смотрите управляющее соединение на порт 1723

Ответить • Поделиться ›

Roman Pavlovsky ➚ Уваров А.С. • 3 года назад

Можно Вам отправить куда-то tcpdump, чтобы Вы посмотрели?

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Roman Pavlovsky • 3 года назад

Ответил на почту

Ответить • Поделиться ›

nenene • 4 года назад

Добрый день!
Спасибо Вам огромное за Вашу работу, читать статьи можно как художественную литературу. С упоением).
В последнем абзаце данной статьи есть ссылка " следующей части ", она ведет на, видимо старую статью, которую судя по комментариям переписали...

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ nenene • 4 года назад

Спасибо, поправили.

Ответить • Поделиться ›

Djovani • 5 лет назад

У IIS хорошие возможности и плюс бесплатен. Пробовал его один раз впечатлений побольше, чем у Денвер. Между PHP и ASP.NET согласитесь ASP.NET получше. У IIS имеется хорошая поддержка ASP.NET. Сайты, которые работают под PHP, оставляют желать лучшего (Internet Explorer глючит на этих сайтах).

С Денвер - ом, когда то сталкивался, и он мне тоже понравился. Думаю нужно заострить внимание на IIS. Если IIS меня не устроит, то перейти на Денвер.

Большое спасибо за добрый совет. Если мне нужен будет Ваш совет, могу ли я ещё побеспокоить Вас?

До встречи (в Интернете).

Ответить • Поделиться ›

Roman Pavlovsky ➚ Djovani • 3 года назад

IIS бесплатен, если у Вас ломаная Windows установлена =)
Разницы между ASP.NET и PHP не вижу при работе в IE. Все зависит от того, как и кто разрабатывал дизайн для сайта, а код ASP.NET и PHP выполняются только на сервере, а в браузер выдают результаты, а не браузер их выгружает и обрабатывает)

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Roman Pavlovsky • 3 года назад

Вообще-то IIS таки бесплатен и для клиентских версий
http://www.microsoft.com/we...

А все остальное - на любителя, на вкус и цвет все фломастеры разные.

Ответить • Поделиться ›

Roman Pavlovsky ➚ Уваров А.С. • 3 года назад

Спасибо за информацию - не знал.

Ответить • Поделиться ›

Djovani • 5 лет назад

Исходя из теории, я хотел установить VPN, потом через VPN установить Windows server 2008 r2 и уже в нём обучатся. Если я что, то напорчу и не смогу исправить, то потом мне достаточно будет удалить папку с Системой и т.д. То есть потрясений меньше.

Ваши ответы решили мои некоторые вопросы. Думаю последовать Вашим советам.

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Djovani • 5 лет назад

Если вам нужен сайт - поставьте Денвер , даже если накосячите - удалили папку с сайтом и сделали новую.

Если хотите экспериментировать с системами - ставьте виртуальную машину:

VirtualBox или VMWare. Получите "компьютер в компьтере", сможете ставить, настраивать, удалять различные ОС, настраивать сеть между виртуальными машинами и много еще чего интересного не затрагивая основной компьютер,

Ответить • Поделиться ›

Djovani • 5 лет назад

Пока занят. Чуть позже я подключусь.

Ответить • Поделиться ›

Уваров А.С. Модератор • 5 лет назад

Я спрошу еще раз, зачем вам VPN сервер? Какие функции он будет выполнять? С размещением сайта на сервере VPN никак не связан.

Ответить • Поделиться ›

Djovani • 5 лет назад

Один раз я пробовал активировать VPN-сервер и у меня (на этом комп.) перестала работать внешняя связь. Сетевое подключение видело только локальную сеть. Тогда я понял, что вопрос упирался в сетевой адаптер. То есть если бы я подключил Интернет, минуя маршрутизатор сразу на комп. Он бы работал. Потом я разобрался в своих ошибках, но так и не до конца. Читая одну информацию, там говорилось про два сетевых адаптера.

Уже потом читая Вашу статью: «Windows Server. Настройка NAT + DHCP» я тоже увидел в сетевом интерфейсе два сетевых адаптера. Вот и решил спросить.

Ваш совет я приму во внимание. Спасибо.

Ответить • Поделиться ›

Djovani • 5 лет назад

Сайт мне нужен на моем компьютере. Пока мои запросы не нуждаются в хостинге. (Преимущества и недостатки хостинга мне известны). А что Windows server 2008 r2 Enterprise не в состояние справится с такими задачами?

Я хотел услышать от Вас, что то по поводу сетевого адаптера. Завтра понедельник и я вообще-то уже спланировал идти в магазин за сетевым адаптером. Надеюсь, мой ответ не грубый и если что, то не так-то извините.

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Djovani • 5 лет назад

Зачем вам сетевой адаптер? Поднимаете на W2K8 IIS7 + MSSQL, если планируете делать сайт на платформе Windows, или Apache + PHP + MySQL, затем на маршрутизаторе пробрасываете наружу 80 порт, к внешнему IP привязываете доменное имя и работайте.

1 Ответить • Поделиться ›

Djovani • 5 лет назад

Я пока с VPN знаком только теоретически.

Моя цель установить VPN сервер и на нём сделать свой личный сайт с возможностью работы в Интернете.

На данный момент схема моей сети такая: два компьютера (на одном установлен Windows server 2008 r2 на другом Windows 7 max), Wan приходит на маршрутизатор от него подключаются эти компьютеры. VPN активирую на Windows server 2008 r2 но на нём только один сетевой адаптер. И если я не ошибаюсь, для нормальной работы VPN нужны два сетевых адаптера (естественно, чтобы хотя бы один из них имел поддержку VPN технологии).

Мне нужно купить сетевой адаптер для VPN?

Ответить • Поделиться ›

Roman Pavlovsky ➚ Djovani • 3 года назад

Сетевая карта для VPN здесь не причем.
У меня на одной сетевой карте работал Интернет, Локальная Сеть и VPN с другим компьютером, который имел свой IP по VPN сети от основного ПК и получал выход в Интернет через VPN

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Djovani • 5 лет назад

Похоже что незнакомы. Каким образом VPN-сервер связан с сайтом? Может быть

вам нужен веб-сервер? Тогда купите хостинг, он нынче дешев как никогда.

Ответить • Поделиться ›

Салават • 6 лет назад

Здравствуйте. Такой вопрос по настройке доступа по VPN.

Схема доступа такая LAN_home -> VPN_to_Internet -> VPN_to_work (основной шлюз в настройках отключен) -> LAN_work.

Дело в том, что когда диапазон ip LAN-home перекрывает LAN-work, то при подключении, доступ к ресурсам LAN-home закрывается. Это можно обойти, если поставить галку "Отключить добавление маршрута, основанное на классе", при этом прописав статический маршрут до LAN-work вручную, через "ip vpn-client", сохранив при этом практически полностью доступ к домашней сети, т.к. пул адресов рабочей очень мал по сравнению с ней. Для стационарного удаленного клиента этот маршрут можно прописать постоянно, а вот для ноутбука, который подключается удаленно через разных провайдеров и непосредственно на работе, такой маршрут придется постоянно, то включать, то отключать.

Возможно ли, чтобы VPN-клиент получая ip-адрес из диапазона LAN-work, еще и получал бы маршрут к его ресурсам через шлюз="ip vpn-client"?

Ответить • Поделиться ›

Сергей • 7 лет назад

Согласен... реально нуна статья по настройке сервака VPN на гигтег в уже имеющейся схеме на основе прошлых статей...

Но к огромному сожалению думаю, что статья не выйдет :((((хотя кто знает...

Ответить • Поделиться ›

Уваров А.С. Модератор ➚ Сергей • 7 лет назад

> Но к огромному сожалению думаю, что статья не выйдет

И чего вы так решили? Просто нужно запастись терпением. Каждый наш материал проходит 100% проверку. Т.е. берется стенд и на нем воспроизводятся все действия, затем все еще раз повторяется на чистой системе, что позволяет проверить повторяемость и полноту материала. И только потом появляется статья. А свободного времени, увы, не так и много. Выдавать материал без проверки мы не хотим, такого хлама в интернете предостаточно.

Кстати, полностью переписали вторую часть:
http://interface31.ru/tech_it/2010/08/nastraivaem-vpn-server-chast-2-marshrutizaciya.html

Ответить • Поделиться ›

Владимир • 7 лет назад

ну когда же будет опубликована третья часть?! очень надо=)

Ответить • Поделиться ›

Уваров А.С. Модератор • 7 лет назад

Начав писать третью часть выяснилось, что вторая не полностью раскрывает вопрос и нужно либо делать пространные отсупления в третьей или переписывать вторую. Сейчас полностью перерабатываем материал второй, после чего будет сразу опубликована практически готовая третья и четвертая (платформа Windows Server).

Ответить • Поделиться ›

Сергей • 7 лет назад

Вопрос - а куда пропала вторая часть?

и ещё вопрос - а когда будет опубликованна часть про настройку самого VPN сервера? :)

заранее спасибки вам за пояснения :)

удачи вам в ващем не лёгком и крайне необходимом многим людям деле :)

Ответить • Поделиться ›

Уваров А.С. Модератор • 7 лет назад

К сожалению жара сбила все планы, прошедшую неделю с семьей провел на отдыхе, что не располагало к написанию статей. Теперь, набравшись сил, буду наверстывать упущенное.

Ответить • Поделиться ›

Сергей • 7 лет назад

вот цикл статей про VPN очень и очень ждали!!!!

спасибо всё скачали и распечатали :) подшили в папочку и ожидаем продолжения :)

• Ответить • Поделиться ›