МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей

3-курс

Занятие 14

Принципы организации VPN

Что такое VPN соединение?

VPN (**Virtual Private Network**) – это виртуальная частная сеть, которая используются для обеспечения защищенного подключения к сети.

Технология, позволяющая **объединить** любое количество устройств в частную сеть.

Как правило, через интернет.

Хотя это технология не новая, но за последнее время она приобрела актуальность из-за желания пользователей сохранить целостность данных или приватность в режиме реального времени.

Что такое VPN соединение?

Такой способ соединения называется **VPN туннель**.

Подключится к VPN можно с любого **компьютера**, с любой **операционной системой**, которая поддерживает VPN соединение.

Либо установлен **VPN-Client**, который способен делать проброс портов с использованием TCP/IP в виртуальную сеть.

Что такое VPN соединение?

Предположим, что имеются **головной офис**, который находится в Москве и сотрудник, который по служебным делам находится, например в Самаре.

В процессе работы ему необходим доступ к внутренним ресурсам сети, такие как:

- серверы,
- корпоративный чат,
- различные приложения,
- какие-то другие сервисы,

которые **недоступны** пользователям данной сети.

Что такое VPN соединение?

Как же быть в такой ситуации?

Можно, конечно, «вынести» серверы в зону **DMZ** и предоставлять доступ по паролю, но это не решает всех задач.

Однако есть другое решение.

Достаточно просто идентифицировать пользователя как «своего» и предоставить ему полный доступ во внутреннюю сеть.

Причем пользователь может иметь IP-адрес из диапазона родной сети, хотя это не является обязательным.

Что такое VPN соединение?

Вроде бы все просто – ввел логин и пароль и работай.

Но проблема заключается в том, что **логин с паролем** могут **перехватить** и преспокойно подключиться к сеансу связи и ко всей корпоративной сети.

Так вот, чтобы этого не произошло весь канал связи **шифруется**.

Удаленные пользователи проходят сложную процедуру **идентификации**, чтобы наверняка знать кто подключается к сети.

Таким образом создается логический **виртуальный канал** или **туннель**, который надежно защищен.

Что делает VPN

VPN обеспечивает удалённое подключение к частным

Что делает VPN

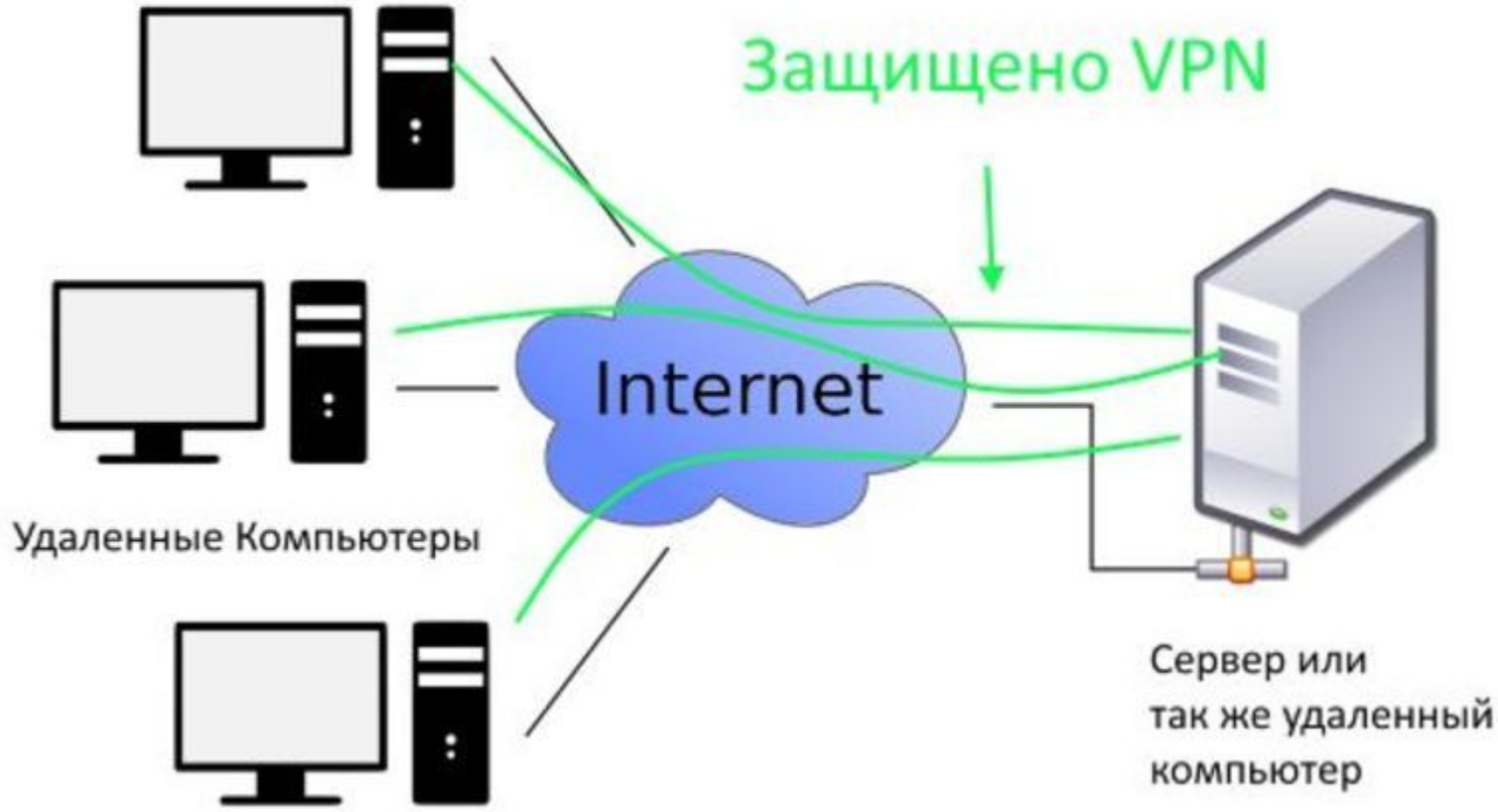
Все участники связи физически подключены к интернету и разным подсетям.

Логически же они находятся в одной сети.

Эта сеть называется **Виртуальная Частная Сеть** (Virtual Private Network, VPN).

Что делает VPN

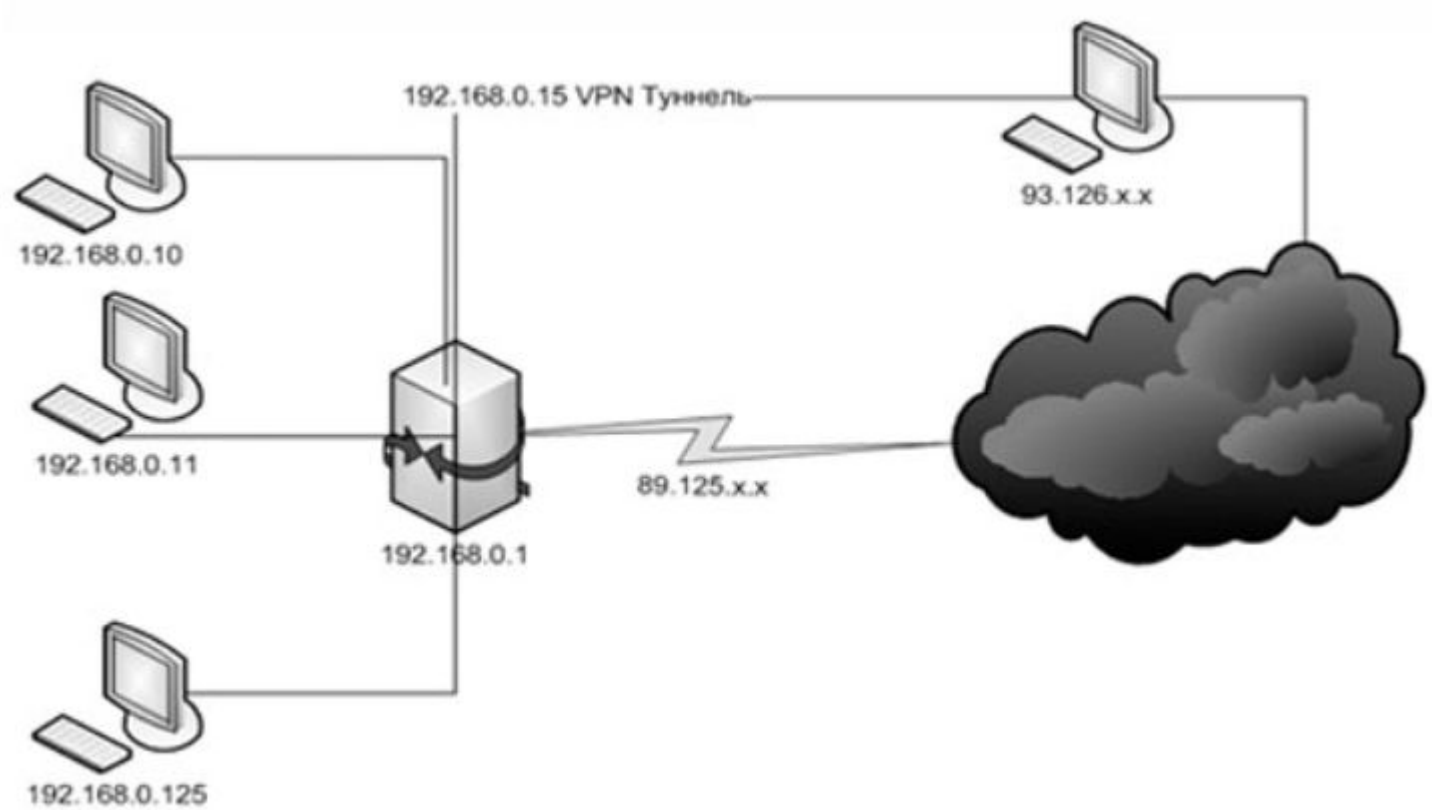
Так же вы можете безопасно объединить несколько компьютеров и серверов



Что делает VPN

Компьютеры с ip адресами с 192.168.0.10 по 192.168.0.125 подключается через сетевой шлюз, который выполняет роль VPN-сервера.

Предварительно на сервер
и маршрутизаторе должны
быть прописаны правила
для соединений по
каналу VPN.



Что делает VPN

VPN позволяет спокойно использовать интернет при подключении даже к открытым wi-fi сетям в общедоступных зонах, таких как:

- торговые центры,
- отели,
- вокзалы,
- аэропорты,
- другие общественные места.

Основные принципы VPN

Основными принципами VPN являются:

- **Аутентификация** участников (маршрутизаторов, компьютеров).
- **Шифрование** данных.
- Периодическая **смена** всех криптографических **ключей**.
- **Обеспечение** и **контроль** целостности передаваемых данных (то есть пакеты не были модифицированы перехватывающей стороной).

Для этого используется хэширование неизменяемых полей пакета.

Хеширование — это преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

Основные принципы VPN

Затем этот хэш добавляется в заголовок.

Принимающая сторона тоже **вычисляет** хэш и **сравнивает** его с принятым.

Если в пакете был **изменен** хотя бы один бит, то вычисленный хэш будет **кардинально отличаться** от переданного в заголовке.

Типы VPN

Существует несколько типов VPN:

Intranet – удаленные филиалы подключены к головному офису и используют ресурсы его сети.

Причем абсолютно все пользователи могут обмениваться данными друг с другом вне зависимости от географического нахождения.

Туннель устанавливается между пограничными маршрутизаторами сетей.

Extranet – к корпоративной сети компании могут также подключаться:

- различные партнёры,
- поставщики,
- клиенты.

Типы VPN

Все эти категории могут получить возможность пользоваться общими ресурсами.

Причем степень доступа регулируется политикой безопасности. Туннель устанавливается между пограничными маршрутизаторами сетей.

Коммутируемые – сотрудники компании могут подключиться к головному офису с любой точки Земли с помощью своего ноутбука.

В компьютере пользователя устанавливается специальная программа для создания VPN либо используются встроенные функции самой операционной системы.

Туннель создается от самого ноутбука до пограничного маршрутизатора корпоративной сети.

Принцип работы VPN

Если кратко, то принцип работы заключается в следующем.

Отправитель **шифрует** исходный IP-пакет (ничего не меняя в самом пакете) заранее согласованным алгоритмом шифрования.

Затем **добавляет** дополнительную информацию в виде заголовков.

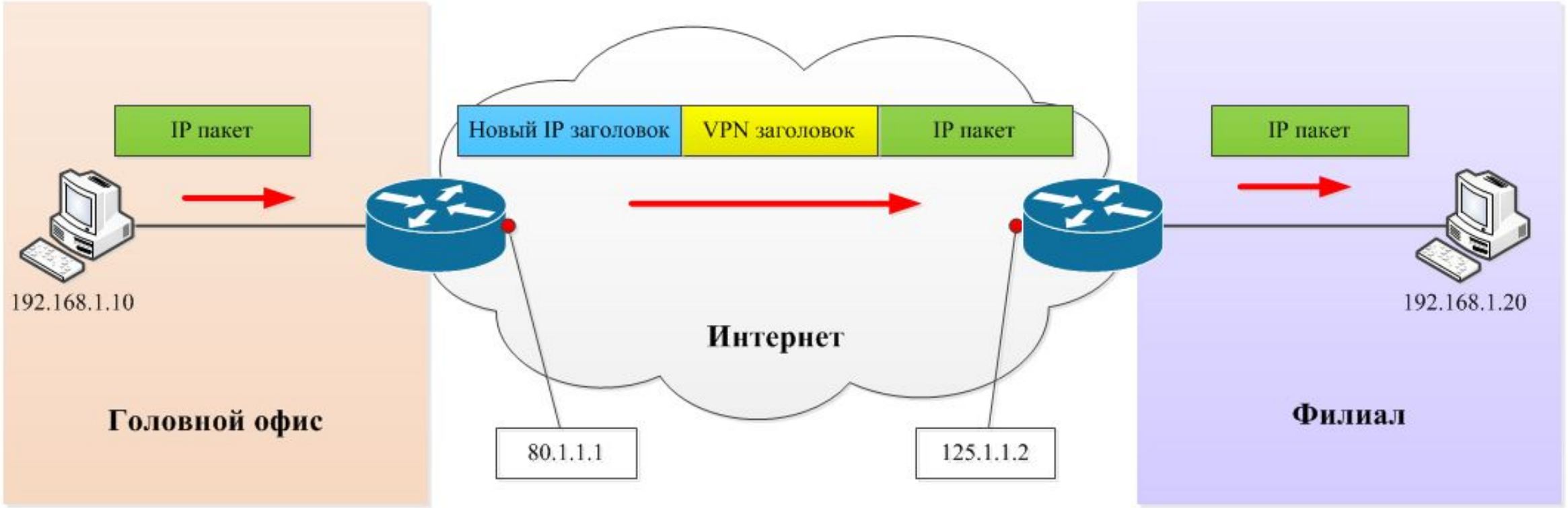
После этого данный пакет **инкапсулируется** в новый IP-пакет с новыми IP-адресами.

Получатель совершает **обратную процедуру**.

Извлекает зашифрованный пакет с VPN заголовком.

Затем **удаляет** сам VPN заголовок и **дешифрует** исходный пакет.

Принцип работы VPN



Вот как выглядит инкапсулируемый пакет:

Адрес отправителя 80.1.1.1	Адрес получателя 125.1.1.2	VPN заголовок	Адрес отправителя 192.168.1.10	Адрес получателя 192.168.1.20	Данные

Принцип работы VPN

На сегодняшний день существует множество протоколов и стандартов для создания VPN.

К ним относят:

- GRE - Generic Routing Encapsulation
- IPsec - IP Security
- Easy Cisco VPN
- Web VPN
- L2/L3 VPN

Наиболее популярными являются GRE и IPSec.

Принцип работы VPN

В туннеле обычно используется **три** прослойки протоколов:

1. **Транспортный протокол** (например, IP).

Это протокол, на котором построена существующая реальная сеть, то есть, он изначально не связан с VPN-ом, но используется для транспортировки инкапсулированных пакетов, содержащих внутри себя зашифрованную, или открытую информацию, относящуюся ко внутренней сети туннеля.

Принцип работы VPN

2. **Протокол инкапсуляции** (например, GRE) – используется как прослойка между **транспортным** протоколом и **внутренним транспортируемым** протоколом.

3. **Инкапсулированный** (транспортируемый) протокол (например, IP, IPX, IPSec) – это собственно пакеты внутритуннельной сети.

Пользователь, подключенный к VPN-у отправляет пакеты, которые на входе в туннель становятся инкапсулированными, например, в GRE, который, в свою очередь, инкапсулируется в транспортный протокол.

Принцип работы VPN

Таким образом, общий порядок инкапсуляции, в случае использования site-to-site VPN следующий: пользователь **отправляет** обычный пакет, пакет **доходит** до устройства, на котором поднят туннель.

Устройство **заворачивает** этот полезный пакет в поле «data» протокола инкапсуляции, который, в свою очередь заворачивается в поле «data» транспортного протокола.

После чего из устройства выходит с виду обычный, например, ip-пакет, в котором, на самом деле, в поле с полезными данными содержится GRE-пакет, в котором, в свою очередь, содержится другой внутренний IP-пакет.

Это позволяет использовать независимую адресацию внутри туннеля и снаружи туннеля.

Принцип работы VPN

Когда целевое устройство **получает** такой пакет, оно **разворачивает** его, **декапсулируя** из него GRE и потом внутренний IP-пакет.

После чего внутренний пакет **направляется** получателю.

В данной ситуации, как не сложно догадаться, отправитель и получатель ничего не знают о наличии туннеля, и работают так, как будто бы его нет.

При этом в транспортном протоколе используется **одна адресация** (например, публичные IP адреса), а в транспортируемом протоколе могут использоваться **приватные адреса**, что не мешает ему транспортироваться через интернет (так как маршрутизация осуществляется для внешнего, транспортного пакета).

Принцип работы VPN

Виртуальная частная сеть базируется на трех китах:

- туннелирование,
- шифрование,
- аутентификация.

Туннелирование обеспечивает передачу данных между двумя точками — окончаниями туннеля — таким образом, что для источника и приемника данных оказывается скрытой вся сетевая инфраструктура, лежащая между ними.

Транспортная среда туннеля, как паром, подхватывает пакеты используемого сетевого протокола у входа в туннель и без изменений доставляет их к выходу.

Принцип работы VPN

Построения туннеля **достаточно** для того, чтобы соединить два сетевых узла так, что с точки зрения работающего на них программного обеспечения они выглядят подключенными к одной (локальной) сети.

Однако нельзя забывать, что на самом деле «паром» с данными проходит через множество промежуточных узлов (маршрутизаторов) открытой публичной сети.

Принцип работы VPN

Такое положение дел таит в себе **две** проблемы.

Первая заключается в том, что передаваемая через туннель информация может быть **перехвачена** злоумышленниками.

Если она конфиденциальна (номера банковских карточек, финансовые отчеты, сведения личного характера), то вполне реальна угроза ее компрометации, что уже само по себе неприятно.

Хуже того, злоумышленники имеют возможность **модифицировать** передаваемые через туннель данные так, что получатель не сможет проверить их достоверность.

Последствия могут быть самыми плачевными.

Принцип работы VPN

Учитывая сказанное, мы приходим к выводу, что туннель **в чистом виде** пригоден разве что для некоторых типов сетевых компьютерных игр и **не может претендовать** на более серьёзное применение.

К счастью, обе проблемы решаются современными средствами **криптографической** защиты информации.

Чтобы воспрепятствовать внесению несанкционированных изменений в пакет с данными на пути его следования по туннелю, используется метод **электронной цифровой подписи** (ЭЦП).

Принцип работы VPN

Суть метода состоит в том, что каждый передаваемый пакет снабжается **дополнительным блоком информации**, который вырабатывается в соответствии с асимметричным криптографическим алгоритмом и уникален для содержимого пакета и секретного ключа ЭЦП отправителя.

Этот блок информации является ЭЦП пакета и позволяет выполнить **аутентификацию** данных получателем, которому известен открытый ключ ЭЦП отправителя.

Защита передаваемых через туннель данных от несанкционированного просмотра достигается путем использования сильных **алгоритмов шифрования**.

Принцип работы VPN

Таким образом, связка «**туннелирование** + **аутентификация** + **шифрование**» позволяет передавать данные между двумя точками через сеть общего пользования, моделируя работу частной (локальной) сети.

Иными словами, рассмотренные средства позволяют построить **виртуальную частную сеть**.

Дополнительным приятным эффектом VPN-соединения является возможность (и даже необходимость) использования **системы адресации**, принятой в локальной сети.

Принцип работы VPN

Реализация виртуальной частной сети на практике выглядит следующим образом.

В локальной вычислительной сети офиса фирмы устанавливается **сервер VPN**.

Удаленный пользователь (или маршрутизатор, если осуществляется соединение двух офисов) с использованием клиентского программного обеспечения VPN **инициирует** процедуру соединения с сервером.

Происходит **аутентификация** пользователя — **первая фаза** установления VPN-соединения.

Принцип работы VPN

В случае подтверждения полномочий наступает **вторая фаза** — между клиентом и сервером выполняется согласование деталей обеспечения **безопасности** соединения.

После этого организуется VPN-соединение, обеспечивающее **обмен** информацией между клиентом и сервером в форме, когда каждый пакет с данными проходит через процедуры:

- шифрования/дешифрования и
- проверки целостности — аутентификации данных.

Принцип работы VPN

Чтобы обеспечить совместимость различных реализаций VPN, были приняты **стандарты**, наиболее распространенными среди которых являются протоколы PPTP и L2TP.

Оба эти стандарта обеспечивают схожий уровень функциональности.

Однако поскольку L2TP использует протокол UDP для организации туннеля, он может работать через сети ATM (Asynchroneus Transfer Mode), Frame Relay и X.25.

Кроме того, L2TP предлагает **более высокую защищенность** соединения за счет использования протокола обеспечения безопасности IPSec.

Принцип работы VPN

Существует **два** типа VPN туннелей:

1. Remote access VPN – означает, что туннель организуется между **приложением** на компьютере клиента и каким-либо устройством, которое выступает в качестве сервера и организовывает подключения от различных клиентов (например, VPN-концентратор, маршрутизатор, Cisco ASA и т. п.)

2. Site-to-site VPN – подразумевает наличие **двух устройств** (например, маршрутизаторов), между которыми имеется перманентный туннель.

В этом случае, пользователи находятся за устройствами, в локальный сетях и на их компьютерах не требуется установки какого-либо специального программного обеспечения

Принцип работы VPN

Первый тип используется для подключения, например, **удалённых** работников в корпоративную сеть предприятия по защищённому каналу.

В этом случае работник может находиться в **любом месте**, где есть интернет.

Программное обеспечение на его компьютере **построит туннель** до маршрутизатора компании, по которому будут передаваться полезные данные.

Принцип работы VPN

Второй тип используется в случае необходимости стационарного соединения между двумя удалёнными **филиалами**, или филиалом и центральным офисом.

В этом случае сотрудники без специального ПО работают в локальной сети офиса.

На границе этой сети стоит **маршрутизатор**, который незаметно для пользователя создаёт **туннель** с удалённым **маршрутизатором** и передаёт на него полезный трафик.

Средства для реализации VPN

Приступая к построению VPN, прежде всего необходимо определиться со **средствами**, которые будут выделены на реализацию проекта.

VPN-соединения могут быть организованы как с помощью **программного обеспечения** (коммерческого или свободно распространяемого), так и с помощью **аппаратных средств**, в изобилии появившихся на рынке.

Крупная фирма в случае необходимости обеспечить безопасное соединение нескольких офисов (по схеме route-to-route) и дать возможность удаленной работы (remote access) с ресурсами локальной сети своим сотрудникам скорее всего предпочтет оборудование **Cisco** как наиболее мощный и гибкий вариант.

Средства для реализации VPN

Если фирма **только развивается** и ей требуется подключить к главному офису одно региональное представительство, можно ограничиться маршрутизаторами-брандмауэрами производства ZyXEL или D-Link.

Это решение существенно **дешевле**, а главное, не предъявляет таких **высоких требований** к профессиональному уровню системных администраторов, как настройка маршрутизаторов Cisco.

Обе компании предоставляют подробную документацию, описывающую как возможности своих продуктов, так и процедуру их настройки с вариантами использования.

Средства для реализации VPN

Нужно отметить, что **аппаратные** устройства, как правило, являются **комплексными** решениями и предлагают целый набор смежных технологий, которые облегчают интеграцию вычислительных устройств через VPN-соединение и увеличивают уровень безопасности.

Обращаясь к **программным** реализациям VPN, нужно вспомнить о том, что операционные системы Microsoft имеют встроенную поддержку VPN-соединений по протоколам PPTP или L2TP.

Если построение **VPN-сервера** на базе серверной операционной системы этого производителя может вызывать споры и дискуссии, то наличие интегрированного **VPN-клиента** безусловно является удобством и позволяет организовывать удаленные рабочие места сотрудников с минимальными затратами.

Средства для реализации VPN

Если же в фирме используется **другая** операционная система или по каким-то причинам интегрированные средства признаны неудовлетворительными, стоит обратить внимание на свободную **кросс-платформенную** реализацию VPN-сервера **OpenVPN**.

При использовании оборудования или программного обеспечения **различных производителей** нужно убедиться, что устройства поддерживают одинаковые протоколы для VPN.

В противном случае их совместное функционирование будет либо **невозможным**, либо **малоэффективным** из-за необходимости применения некоторого подмножества поддерживаемых протоколов, что может существенно снизить уровень информационной безопасности.

Протоколы PPTP и L2TP с IPSec

Сетевая технология **PPTP** (Point-to-Point Tunneling Protocol) — развитие протокола удаленного доступа PPP (Point-to-Point Protocol).

PPTP, относящаяся к стеку протоколов TCP/IP, была создана для организации работы многопротокольных сетей через Интернет.

Для функционирования PPTP необходимо установить два TCP-соединения:

- для **управления** VPN-соединением и
- для **передачи** данных.

Конфиденциальность передаваемой информации обеспечивается шифрованием по схеме RC4 с ключом до 128 бит.

Протоколы PPTP и L2TP с IPSec

Улучшенная версия протокола PPTP — индустриальный стандарт **L2TP** (Layer Two Tunneling Protocol), представляющий собой комбинацию технологий PPTP и L2F (Layer Two Forwarding).

Транспортная среда для протокола L2TP — UDP.

Шифрование данных обеспечивает комплекс средств, предлагаемых протоколом безопасности **IPSec**.

Доступны следующие методы шифрования: DES (Data Encryption Standard) с 56-бит ключом и 3DES (Triple DES) с тремя 56-бит ключами.

Кроме того, IPSec предоставляет механизм согласования ключей IKE (Internet Key Exchange), аутентификацию Kerberos и другие технологии информационной безопасности.

Протоколы PPTP и L2TP с IPSec

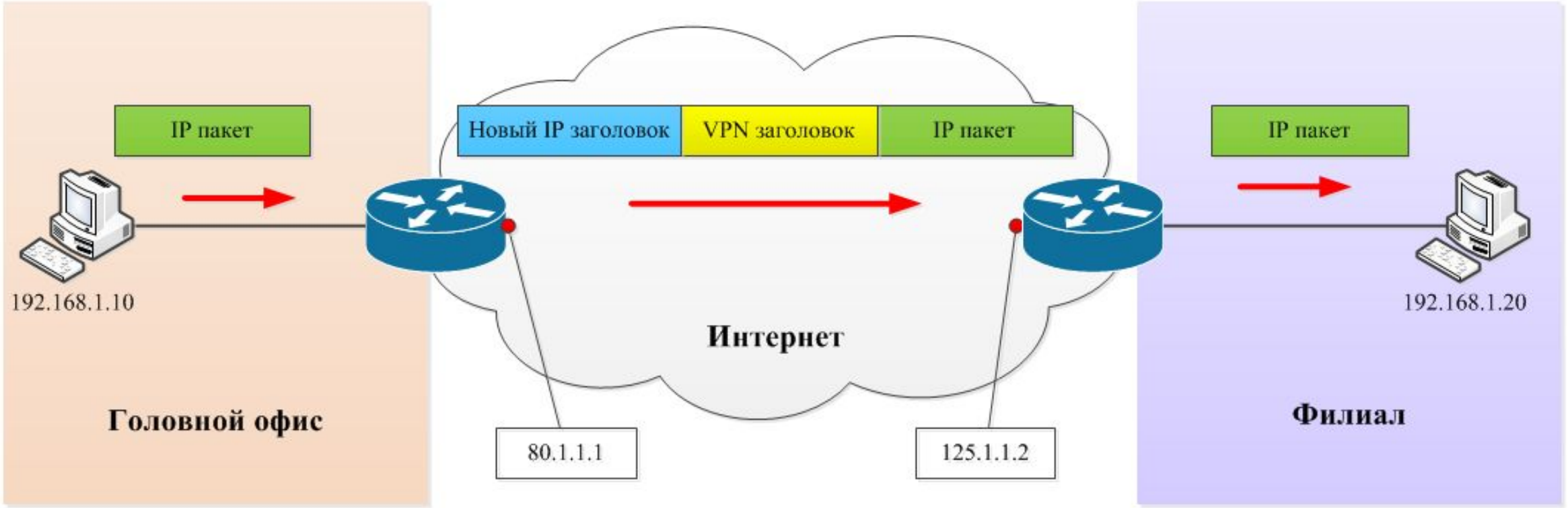
В основе работы обоих рассмотренных протоколов туннелирования лежит **инкапсуляция** пакетов протокола сетевого уровня, используемого в локальной сети, в PPP-пакеты.

На рисунках представлен вид структуры информации, передаваемой по туннелю.

Полезные данные, заключенные в пакеты протоколов сетевого уровня (IP, IPX или NetBEUI), снабжены PPP-заголовками, содержащими информацию о протоколе.

Они необходимы для того, чтобы полученные данные направлялись соответствующему драйверу.

Принцип работы VPN



Вот как выглядит инкапсулируемый пакет:

Адрес отправителя 80.1.1.1	Адрес получателя 125.1.1.2	VPN заголовок	Адрес отправителя 192.168.1.10	Адрес получателя 192.168.1.20	Данные

Протоколы PPTP и L2TP с IPSec

Протокол PPTP шифрует пришедшую информацию и снабжает ее заголовком, требующимся для доставки получателю — шлюзу VPN.

В отличие от него, L2TP добавляет заголовки L2TP и UDP.

После этого модуль обеспечения безопасности IPSec выполняет **шифрование** данных.

Затем они, сопровожденные IPSec-заголовком, **дополняются** адресной информацией, необходимой для доставки.

Аппаратные устройства VPN

Поскольку стоимость **аппаратных** решений для организации VPN приемлема даже для малых фирм или индивидуальных предпринимателей, а в эксплуатации они гораздо удобнее и надежнее, нежели **программные средства** на базе ПК, имеет смысл обратить внимание на некоторые из них.

Создать точку доступа для нескольких VPN-соединений можно на основе **VPN-маршрутизатора** DI-804HV/DI-808HV (позволяет организовать до **40 соединений**) производства D-Link или брандмауэра ZyWALL (от 1 до **100 соединений** в зависимости от модификации) компании ZyXEL.

Аппаратные устройства VPN

Конфигурирование обоих устройств может быть выполнено через удобный веб-интерфейс.

Продукты ZyXEL, кроме того, позволяют получить доступ к ZyNOS (сетевой операционной системе ZyXEL) в режиме командной строки по протоколу **Telnet**.

Это дает возможность **более тонкой настройки** и отладки соединений.

Интересным и недорогим решением для объединения локальных сетей является использование ADSL модема-маршрутизатора-брандмауэра ZyXEL Prestige P661H.

Аппаратные устройства VPN

Это устройство позволяет организовать **два** VPN-соединения.

Помимо того может:

- **служить мостом** между тремя IP-подсетями, разделяющими общую среду Ethernet (с возможностью фильтрации трафика между ними),
- **направлять IP-трафик** в соответствии с таблицей статических маршрутов,
- **реализовать фирменную технологию Any-IP**, которая позволяет задействовать его в качестве шлюза по умолчанию компьютерам, сконфигурированным в расчете на работу в другой подсети.

Аппаратные устройства VPN

При настройке описанных устройств нужно внимательно прописывать **параметры VPN-соединений**, так как в случае даже небольшой ошибки туннели не установятся.

Например, **предопределенные ключи** (Preshared Key) должны быть одинаковыми на обоих окончаниях туннеля.

Для одного и того же VPN-соединения **не могут** различаться:

- **механизмы согласования** ключей (Manual или IKE) и
- **криптографические алгоритмы** шифрования и аутентификации.

Аппаратные устройства VPN

Если что-то отказывается работать, необходимо:

- **обратиться** к сопроводительной документации,
- **понять принцип**, в соответствии с которым должен функционировать проблемный участок,
- **определить круг возможных причин** неработоспособности.

Выбирая **параметры** туннеля, следует внимательно ознакомиться с возможными вариантами его реализации.

Это нужно для того, чтобы быть **уверенным** в получении должной функциональности.

Аппаратные устройства VPN

Так, например, протокол AH (Authentication Header) организации SA (Security Association) обеспечивает только **аутентификацию** передаваемых данных **без** их шифрования.

Для получения **полной** защиты следует выбирать протокол **ESP** (Encapsulating Security Payload).

Настройка VPN сервера

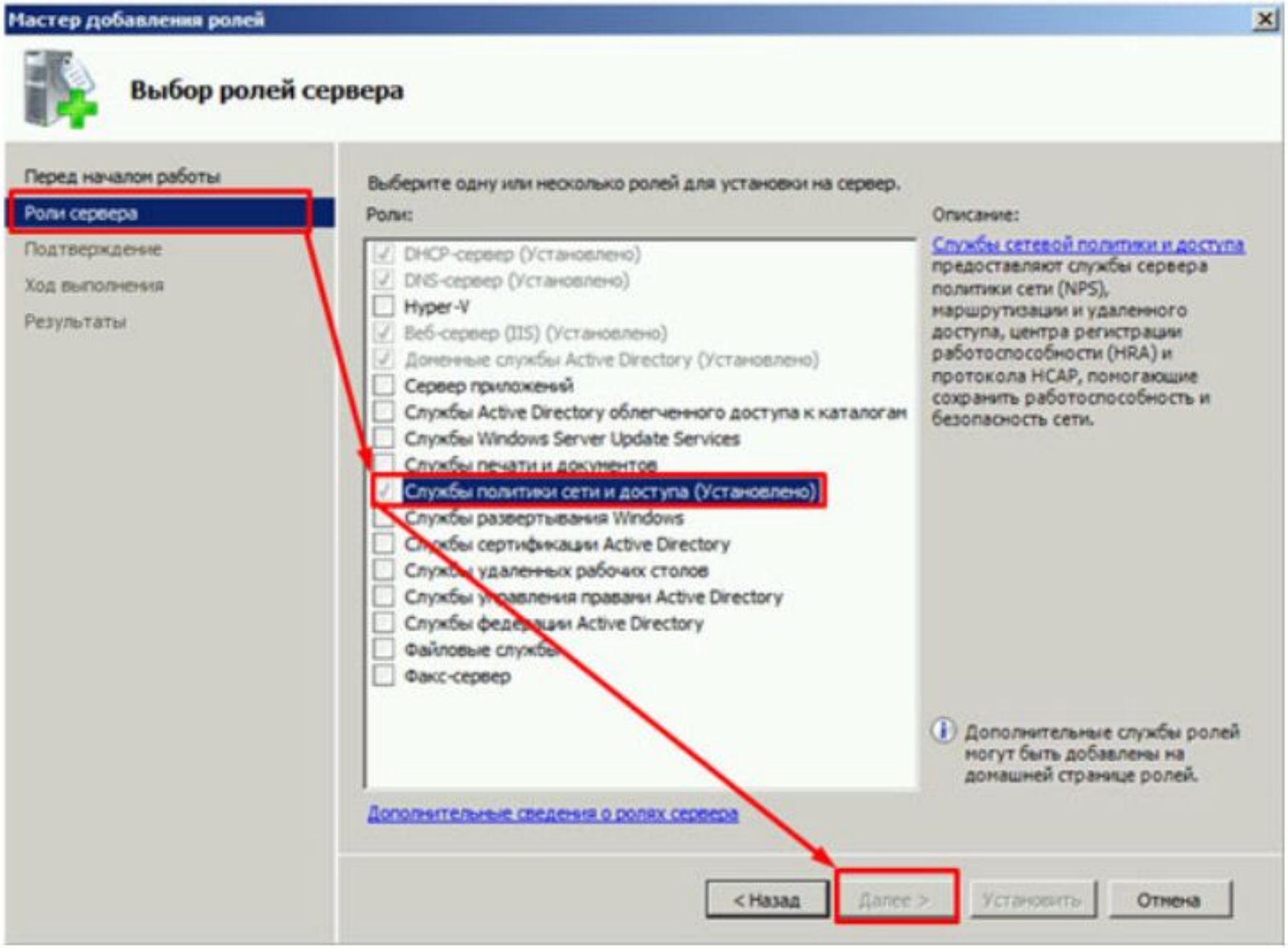
Настройка VPN сервера

Если вы хотите установить и использовать VPN сервер на базе семейства Windows , то необходимо понимать, что клиенские машины Windows XP/7/8/10 данную функцию не поддерживают, вам необходима система виртуализации, либо физический сервер на платформе Windows 2000/2003/2008/2012/2016, но мы рассмотрим данную функцию на Windows Server 2008 R2.

1. Для начала необходимо установить роль сервера «**Службы политики сети и доступа**».

Для этого открываем **Диспетчер сервера** и нажимаем на ссылку «**Добавить роль**»:

Выбираем роль «**Службы политики сети и доступа**» и нажимаем «**Далее**».

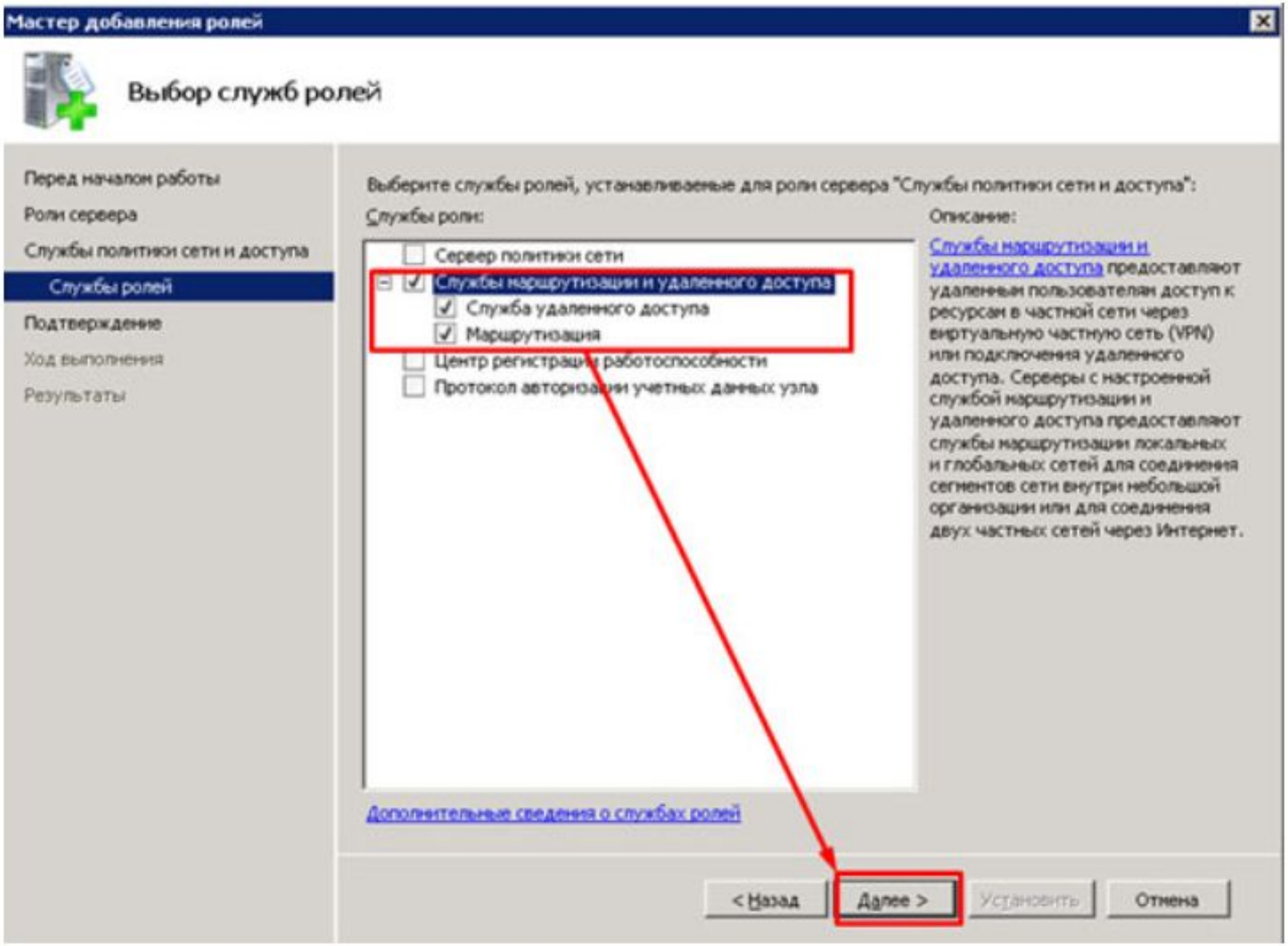

Мастер добавления ролей
Выбор ролей сервера
Перед началом работы
Роли сервера
Подтверждение
Ход выполнения
Результаты
Выберите одну или несколько ролей для установки на сервер.
Роли:
DHCP-сервер (Установлено)
DNS-сервер (Установлено)
Hyper-V
Веб-сервер (IIS) (Установлено)
Доменные службы Active Directory (Установлено)
Сервер приложений
Службы Active Directory облегченного доступа к каталогам
Службы Windows Server Update Services
Службы печати и документов
Службы политики сети и доступа (Установлено)
Службы развертывания Windows
Службы сертификации Active Directory
Службы удаленных рабочих столов
Службы управления правами Active Directory
Службы федерации Active Directory
Файловые службы
Факс-сервер
Описание:
Службы сетевой политики и доступа предоставляют службы сервера политики сети (NPS), маршрутизации и удаленного доступа, центра регистрации работоспособности (HRA) и протокола HCAP, помогающие сохранить работоспособность и безопасность сети.
Дополнительные службы ролей могут быть добавлены на домашней странице ролей.
Дополнительные сведения о ролях сервера
< Назад
Далее >
Установить
Отмена

Настройка VPN сервера

Выбираем «**Службы маршрутизации и удаленного доступа**» и

нажимаем «**Далее**» и

«**Установить**».


Мастер добавления ролей
Выбор служб ролей
Перед началом работы
Роли сервера
Службы политики сети и доступа
Службы ролей
Подтверждение
Ход выполнения
Результаты
Выберите службы ролей, устанавливаемые для роли сервера "Службы политики сети и доступа":
Службы роли:
Сервер политики сети
Службы маршрутизации и удаленного доступа
Служба удаленного доступа
Маршрутизация
Центр регистрации работоспособности
Протокол авторизации учетных данных узла
Описание:
Службы маршрутизации и удаленного доступа предоставляют удаленным пользователям доступ к ресурсам в частной сети через виртуальную частную сеть (VPN) или подключения удаленного доступа. Серверы с настроенной службой маршрутизации и удаленного доступа предоставляют службы маршрутизации локальных и глобальных сетей для соединения сегментов сети внутри небольшой организации или для соединения двух частных сетей через Интернет.
Дополнительные сведения о службах ролей
< Назад
Далее >
Установить
Отмена

Настройка VPN сервера

2. После установки роли необходимо настроить ее.

Переходим в **Диспетчер сервера**, раскрываем ветку «**Роли**»,

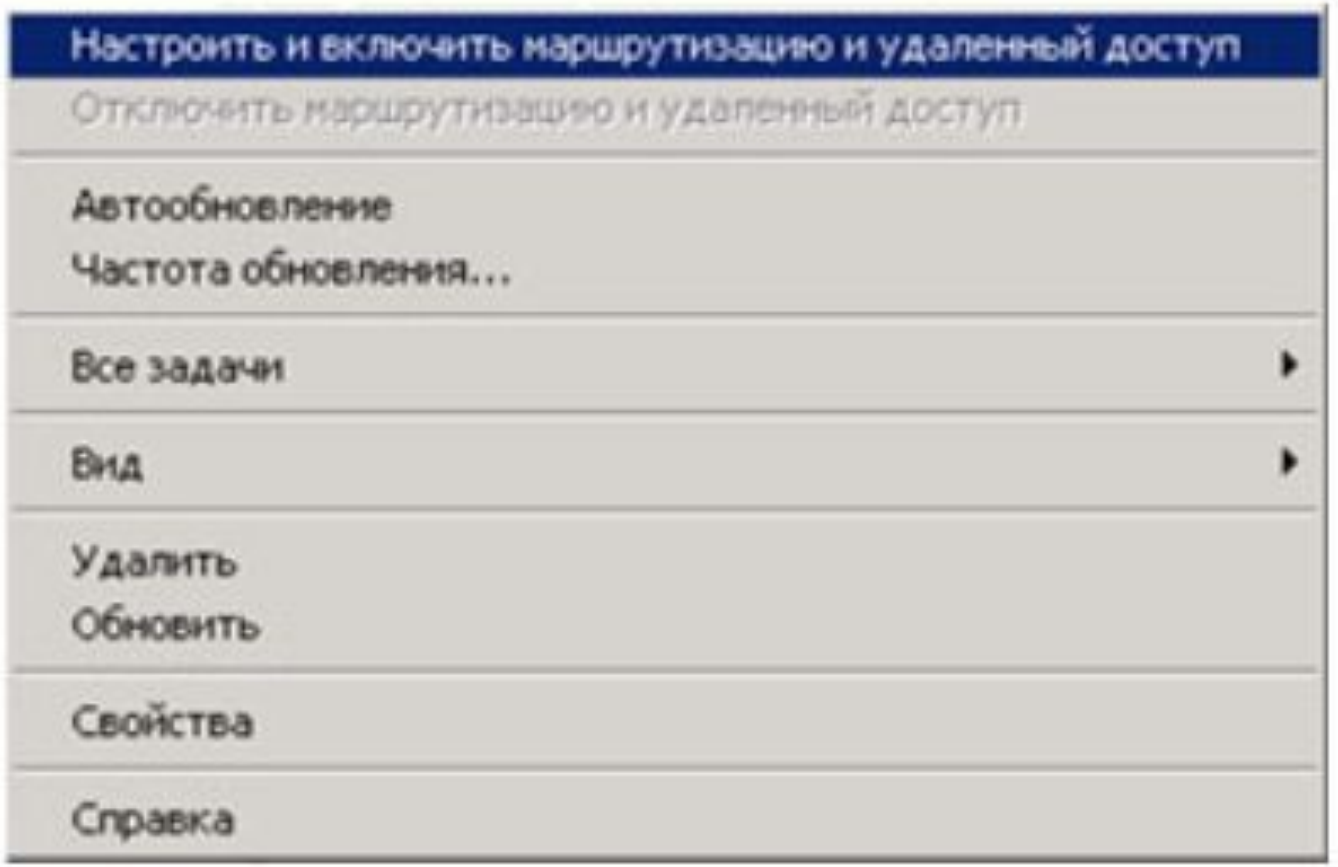
выбираем роль «**Службы политики сети и доступа**»,

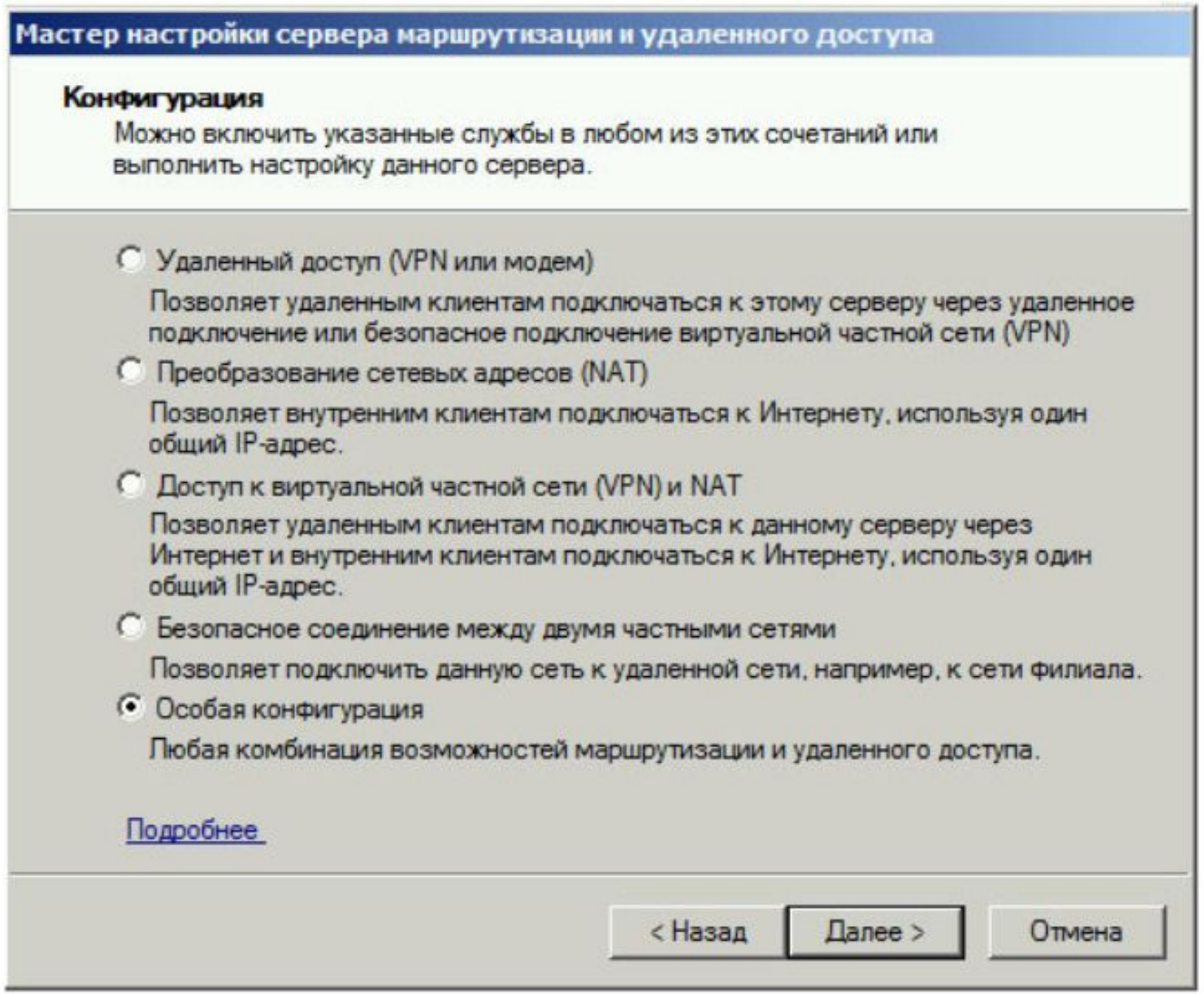
разворачиваем, кликаем правой кнопкой по

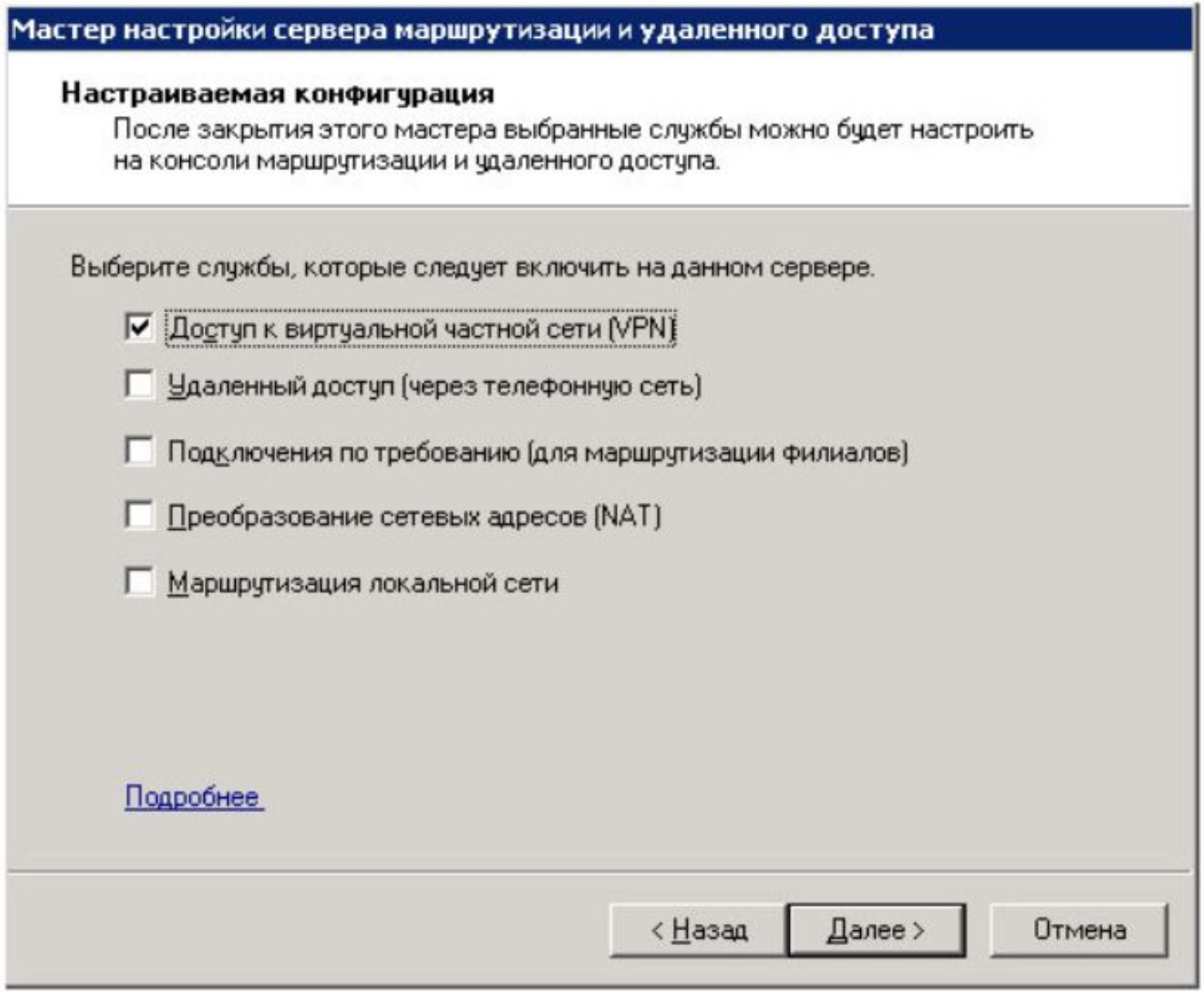
«**Маршрутизация и удаленный доступ**» и

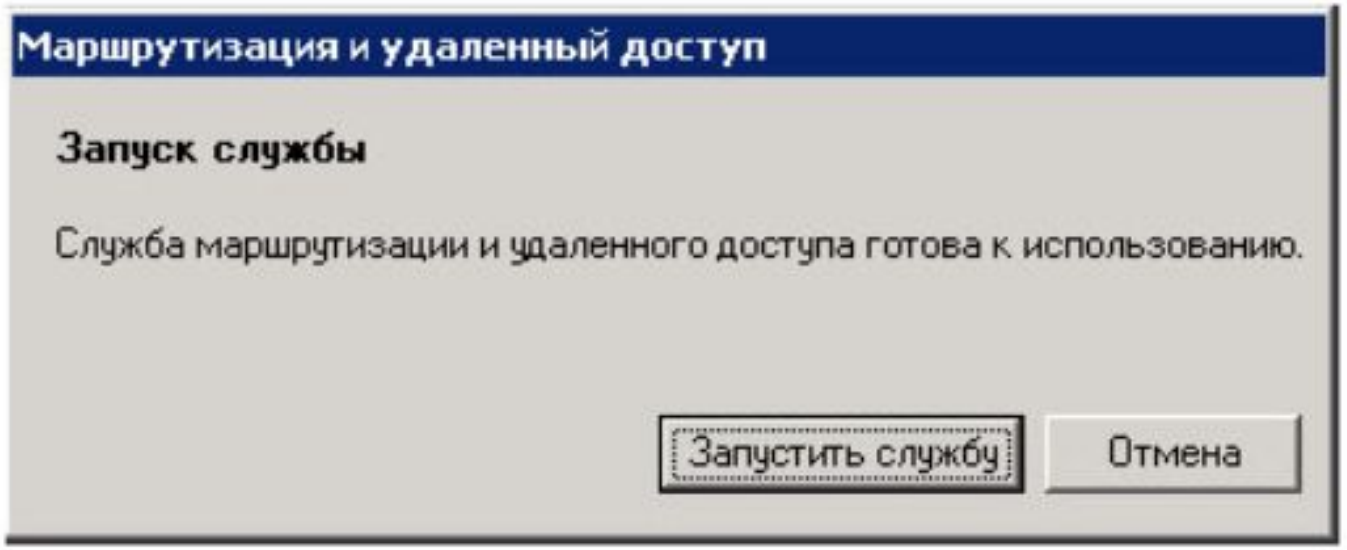
выбираем

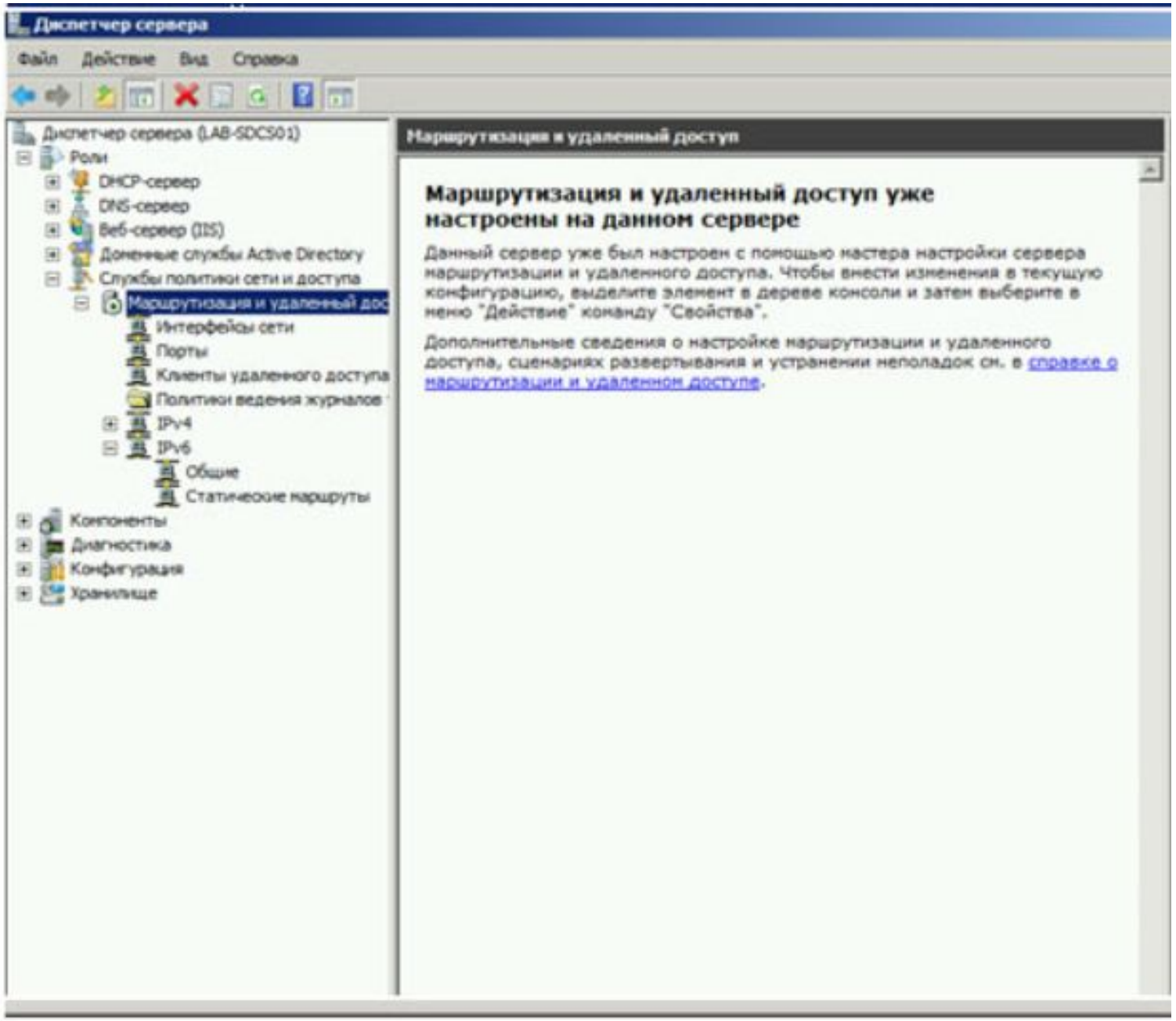
«**Настроить и включить маршрутизацию и удаленный доступ**».


Настроить и включить маршрутизацию и удаленный доступ
Отключить маршрутизацию и удаленный доступ
Автообновление
Частота обновления...
Все задачи
Вид
Удалить
Обновить
Свойства
Справка


Мастер настройки сервера маршрутизации и удаленного доступа
Конфигурация
Можно включить указанные службы в любом из этих сочетаний или выполнить настройку данного сервера.
Удаленный доступ (VPN или модем)
Позволяет удаленным клиентам подключаться к этому серверу через удаленное подключение или безопасное подключение виртуальной частной сети (VPN)
Преобразование сетевых адресов (NAT)
Позволяет внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.
Доступ к виртуальной частной сети (VPN) и NAT
Позволяет удаленным клиентам подключаться к данному серверу через Интернет и внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.
Безопасное соединение между двумя частными сетями
Позволяет подключить данную сеть к удаленной сети, например, к сети филиала.
Особая конфигурация
Любая комбинация возможностей маршрутизации и удаленного доступа.
Подробнее
< Назад
Далее >
Отмена


Мастер настройки сервера маршрутизации и удаленного доступа
Настраиваемая конфигурация
После закрытия этого мастера выбранные службы можно будет настроить на консоли маршрутизации и удаленного доступа.
Выберите службы, которые следует включить на данном сервере.
Доступ к виртуальной частной сети (VPN)
Удаленный доступ (через телефонную сеть)
Подключения по требованию (для маршрутизации филиалов)
Преобразование сетевых адресов (NAT)
Маршрутизация локальной сети
Подробнее
< Назад
Далее >
Отмена


Маршрутизация и удаленный доступ
Запуск службы
Служба маршрутизации и удаленного доступа готова к использованию.
Запустить службу
Отмена


Диспетчер сервера
Файл
Действие
Вид
Справка
Диспетчер сервера (LAB-SDCS01)
Роли
DHCP-сервер
DNS-сервер
Веб-сервер (IIS)
Доменные службы Active Directory
Службы политики сети и доступа
Маршрутизация и удаленный дос
Интерфейсы сети
Порты
Клиенты удаленного доступа
Политики ведения журналов
IPv4
IPv6
Общие
Статические маршруты
Компоненты
Диагностика
Конфигурация
Хранилище
Маршрутизация и удаленный доступ
Маршрутизация и удаленный доступ уже настроены на данном сервере
Данный сервер уже был настроен с помощью мастера настройки сервера маршрутизации и удаленного доступа. Чтобы внести изменения в текущую конфигурацию, выделите элемент в дереве консоли и затем выберите в меню "Действие" команду "Свойства".
Дополнительные сведения о настройке маршрутизации и удаленного доступа, сценариях развертывания и устранении неполадок см. в справке о маршрутизации и удаленном доступе.

Настройка VPN сервера

После запуска службы считаем настройку роли **законченной**. Теперь необходимо **разрешить** пользователям доступ до сервера и настроить выдачу ip-адресов клиентам.

Порты которые поддерживает VPN.

После поднятие службы они открываются в брендмауэре.

Для PPTP: 1723 (TCP);

Для L2TP: 1701 (TCP)

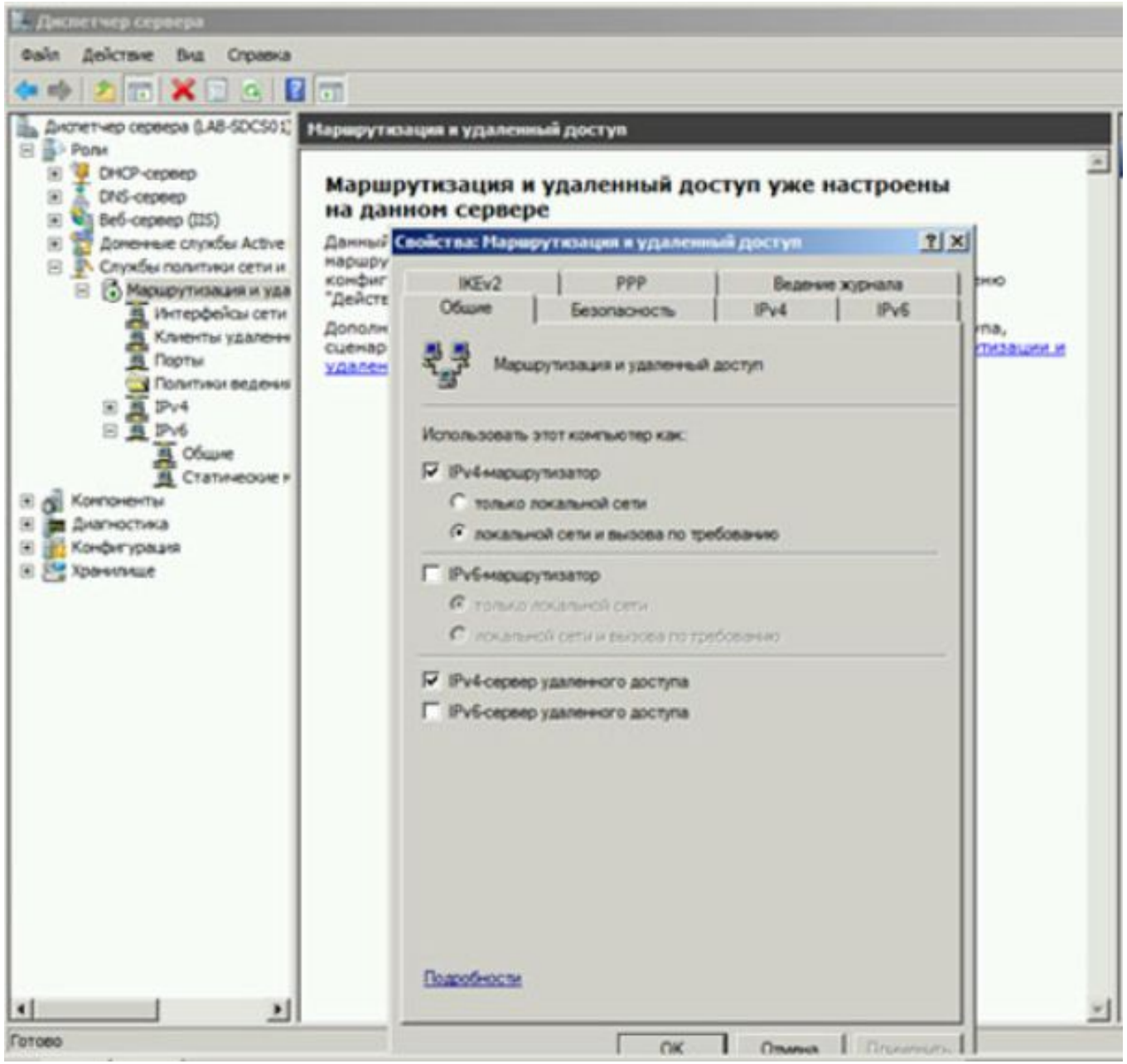
Для SSTP: 443 (TCP).

Настройка VPN сервера

Протокол **L2TP/IpSec** является более **предпочтительным** для построения VPN-сетей, в основном это касается **безопасности** и более высокой **доступности**, благодаря тому, что для каналов данных и управления используется одна UDP-сессия.

Рассмотрим настройку **L2TP/IpSec** VPN-сервера на платформе Windows Server 2008 r2.

Переходим в Диспетчер сервера: **Роли – Маршрутизация и удалённый доступ**, щелкаем по этой роли правой кнопкой мыши и выбираем «**Свойства**», на вкладке «**Общие**» ставим галочку в полях IPv4-маршрутизатор, выбираем «**локальной сети и вызова по требованию**», и «**IPv4-сервер удаленного доступа**».


Диспетчер сервера
Файл Действие Вид Справка
Диспетчер сервера (LAB-SDC50
Роли
DHCP-сервер
DNS-сервер
Веб-сервер (IIS)
Доменные службы Active
Службы политики сети и
Маршрутизация и уда
Интерфейсы сети
Клиенты удаленн
Порты
Политики ведения
IPv4
IPv6
Общие
Статические м
Компоненты
Диагностика
Конфигурация
Хранилище
Маршрутизация и удаленный доступ
Маршрутизация и удаленный доступ уже настроены на данном сервере
Данный маршру конфиг "Дейст
Дополн сценар удален
Свойства: Маршрутизация и удаленный доступ
IKEv2
PPP
Ведение журнала
Общие
Безопасность
IPv4
IPv6
Маршрутизация и удаленный доступ
Использовать этот компьютер как:
IPv4-маршрутизатор
только локальной сети
локальной сети и вызова по требованию
IPv6-маршрутизатор
только локальной сети
локальной сети и вызова по требованию
IPv4-сервер удаленного доступа
IPv6-сервер удаленного доступа
Подробности
OK
Отмена
Применить
Готово

Настройка VPN сервера

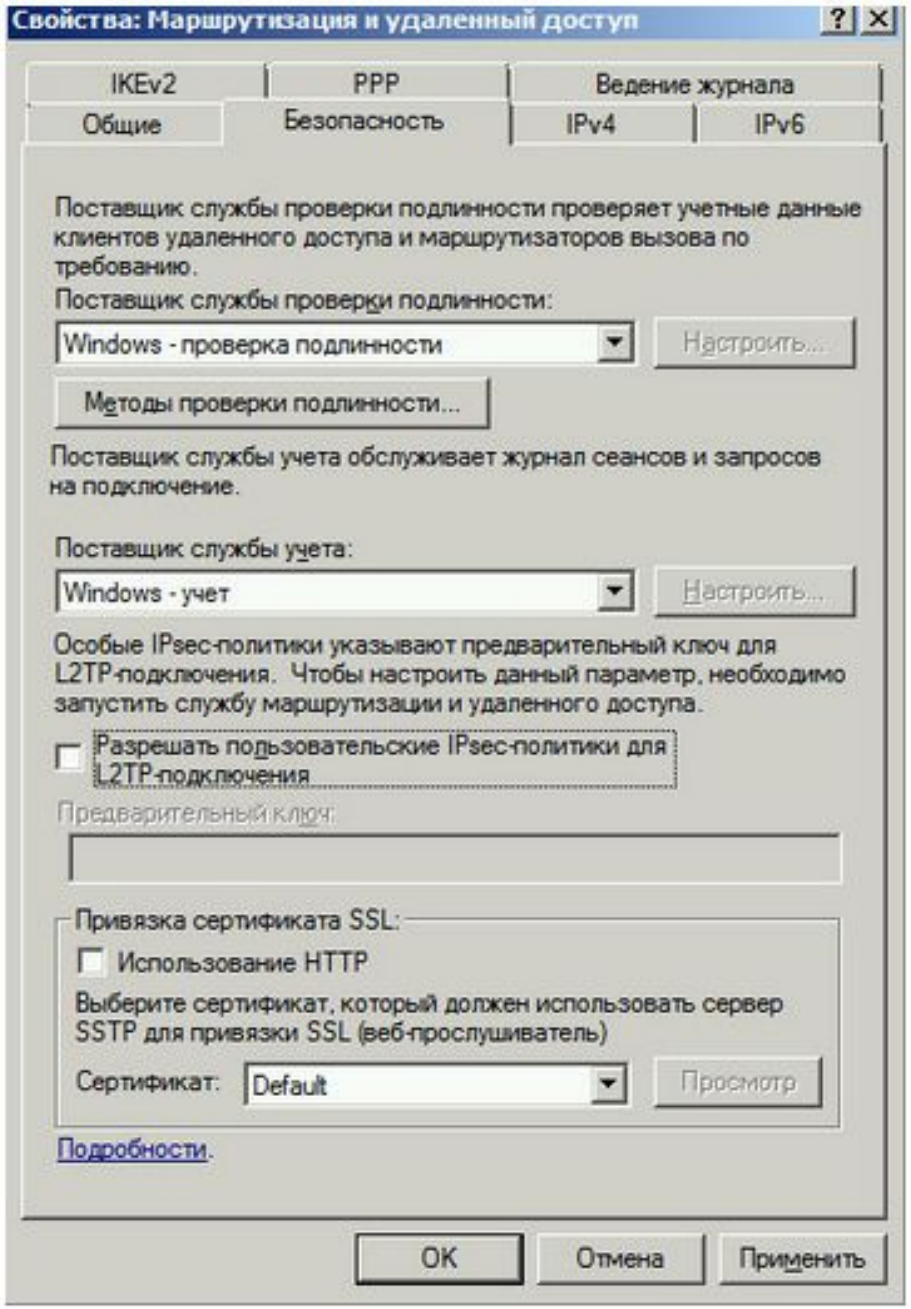
Теперь нам необходимо ввести предварительный ключ.

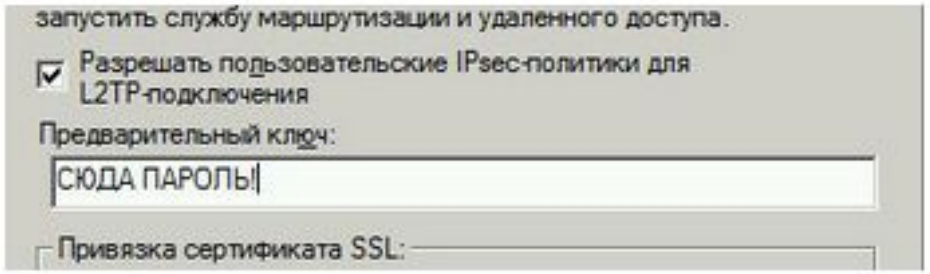
Переходим на вкладку **Безопасность** и в поле **Разрешить особые IPSec-политики для L2TP-подключения** поставьте галочку и введите Ваш ключ.

Вы можете ввести туда произвольную **комбинацию** букв и цифр главный принцип, чем сложнее комбинация – тем безопаснее, и еще запомните или запишите эту комбинацию она нам еще понадобиться.

Во вкладке «**Поставщик службы проверки подлинности**»

выберите «**Windows — проверка подлинности**».


Свойства: Маршрутизация и удаленный доступ
IKEv2
PPP
Ведение журнала
Общие
Безопасность
IPv4
IPv6
Поставщик службы проверки подлинности проверяет учетные данные клиентов удаленного доступа и маршрутизаторов вызова по требованию.
Поставщик службы проверки подлинности:
Windows - проверка подлинности
Настроить...
Методы проверки подлинности...
Поставщик службы учета обслуживает журнал сеансов и запросов на подключение.
Поставщик службы учета:
Windows - учет
Настроить...
Особые IPsec-политики указывают предварительный ключ для L2TP-подключения. Чтобы настроить данный параметр, необходимо запустить службу маршрутизации и удаленного доступа.
Разрешать пользовательские IPsec-политики для L2TP-подключения
Предварительный ключ:
Привязка сертификата SSL:
Использование HTTP
Выберите сертификат, который должен использовать сервер SSTP для привязки SSL (веб-прослушиватель)
Сертификат:
Default
Просмотр
Подробности.
OK
Отмена
Применить


запустить службу маршрутизации и удаленного доступа.
Разрешать пользовательские IPsec-политики для L2TP-подключения
Предварительный ключ:
СЮДА ПАРОЛЬ!
Привязка сертификата SSL:

Настройка VPN сервера

Теперь нам необходимо настроить **Безопасность подключений**.

Для этого на вкладке **Безопасность** выберем

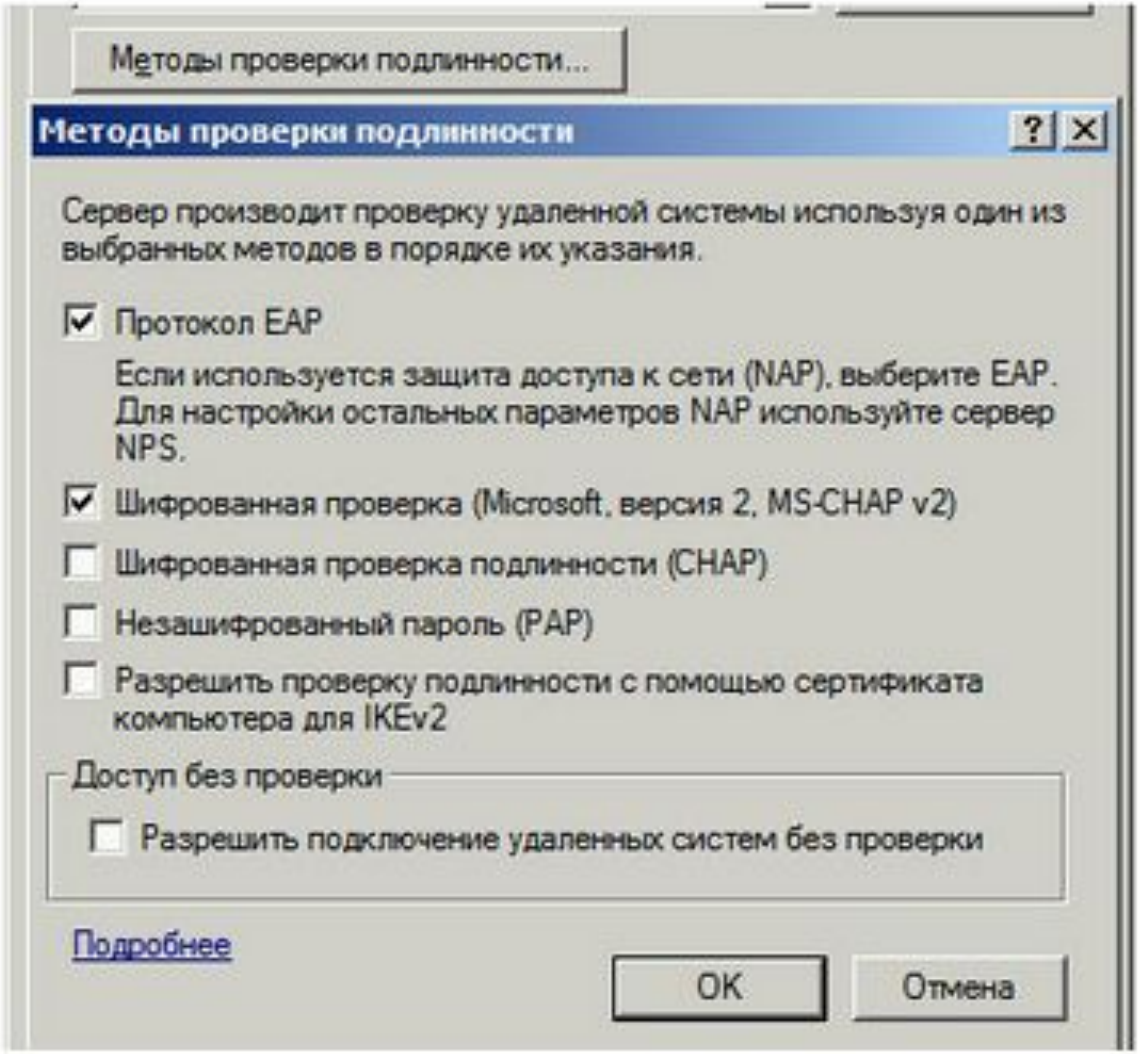
Методы проверки подлинности,

поставьте галочки на

Протокол EAP

и

Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2).

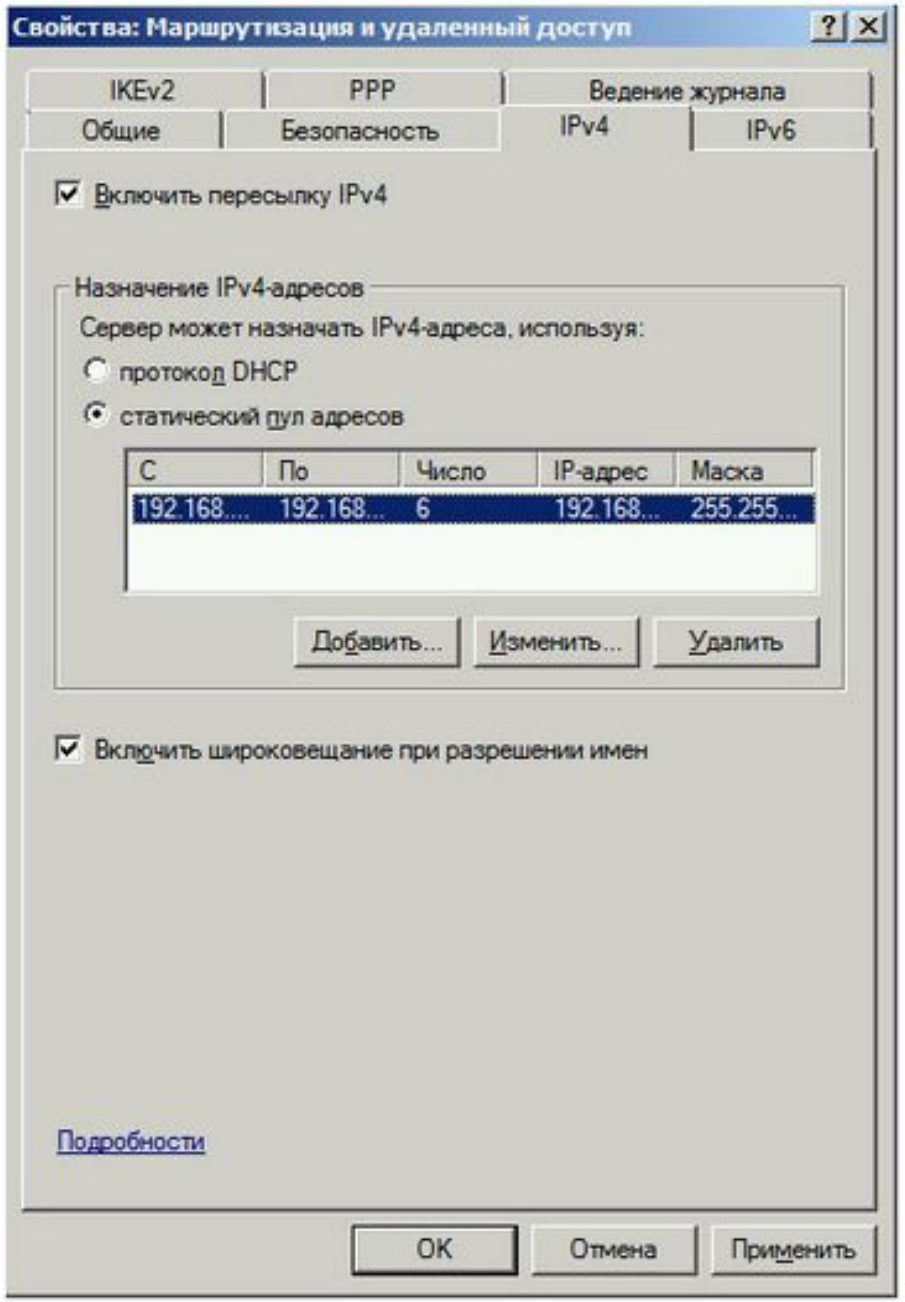

Методы проверки подлинности...
Методы проверки подлинности
Сервер производит проверку удаленной системы используя один из выбранных методов в порядке их указания.
Протокол EAP
Если используется защита доступа к сети (NAP), выберите EAP. Для настройки остальных параметров NAP используйте сервер NPS.
Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2)
Шифрованная проверка подлинности (CHAP)
Незашифрованный пароль (PAP)
Разрешить проверку подлинности с помощью сертификата компьютера для IKEv2
Доступ без проверки
Разрешить подключение удаленных систем без проверки
Подробнее
OK
Отмена

Настройка VPN сервера

Далее перейдем на вкладку **IPv4**.

Там укажем какой интерфейс будет принимать подключения VPN, а так же настроим пул выдаваемых адресов клиентам L2TP VPN на вкладке **IPv4**.

Интерфейсом выставьте «**Разрешить RAS выбирать адаптер**».


Свойства: Маршрутизация и удаленный доступ
IKEv2
PPP
Ведение журнала
Общие
Безопасность
IPv4
IPv6
Включить пересылку IPv4
Назначение IPv4-адресов
Сервер может назначать IPv4-адреса, используя:
протокол DHCP
статический пул адресов
С
По
Число
IP-адрес
Маска
192.168....
192.168...
6
192.168...
255.255...
Добавить...
Изменить...
Удалить
Включить широковещание при разрешении имен
Подробности
OK
Отмена
Применить

Настройка VPN сервера

Теперь перейдем на появившуюся вкладку **Порты**,

нажмем правой кнопкой мыши и **Свойства**,

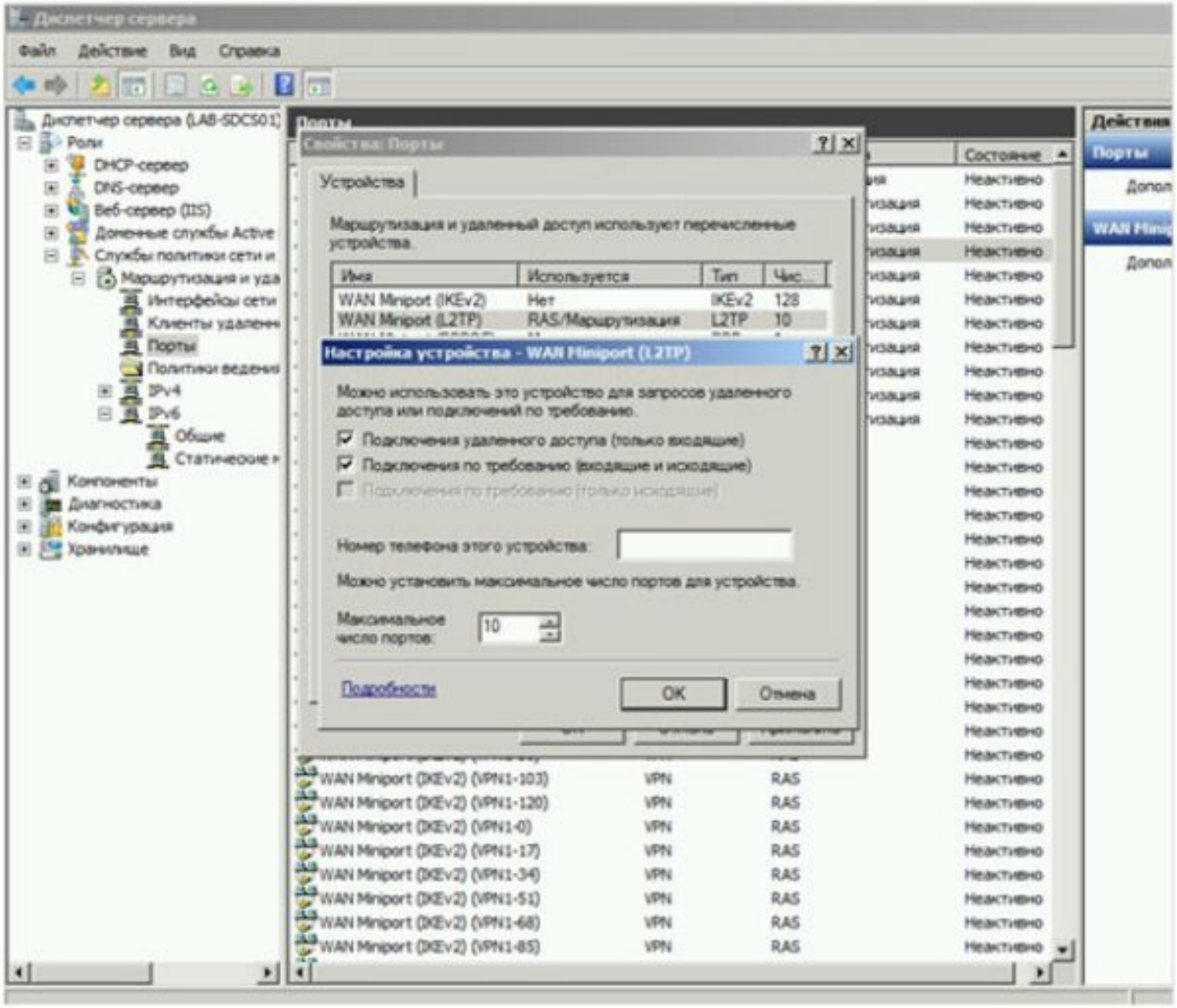
выберем подключение **L2TP** и нажмем **Настроить**,

в новом окне выставим **Подключение удаленного доступа (только входящие)** и

Подключение по требованию (входящие и исходящие) и

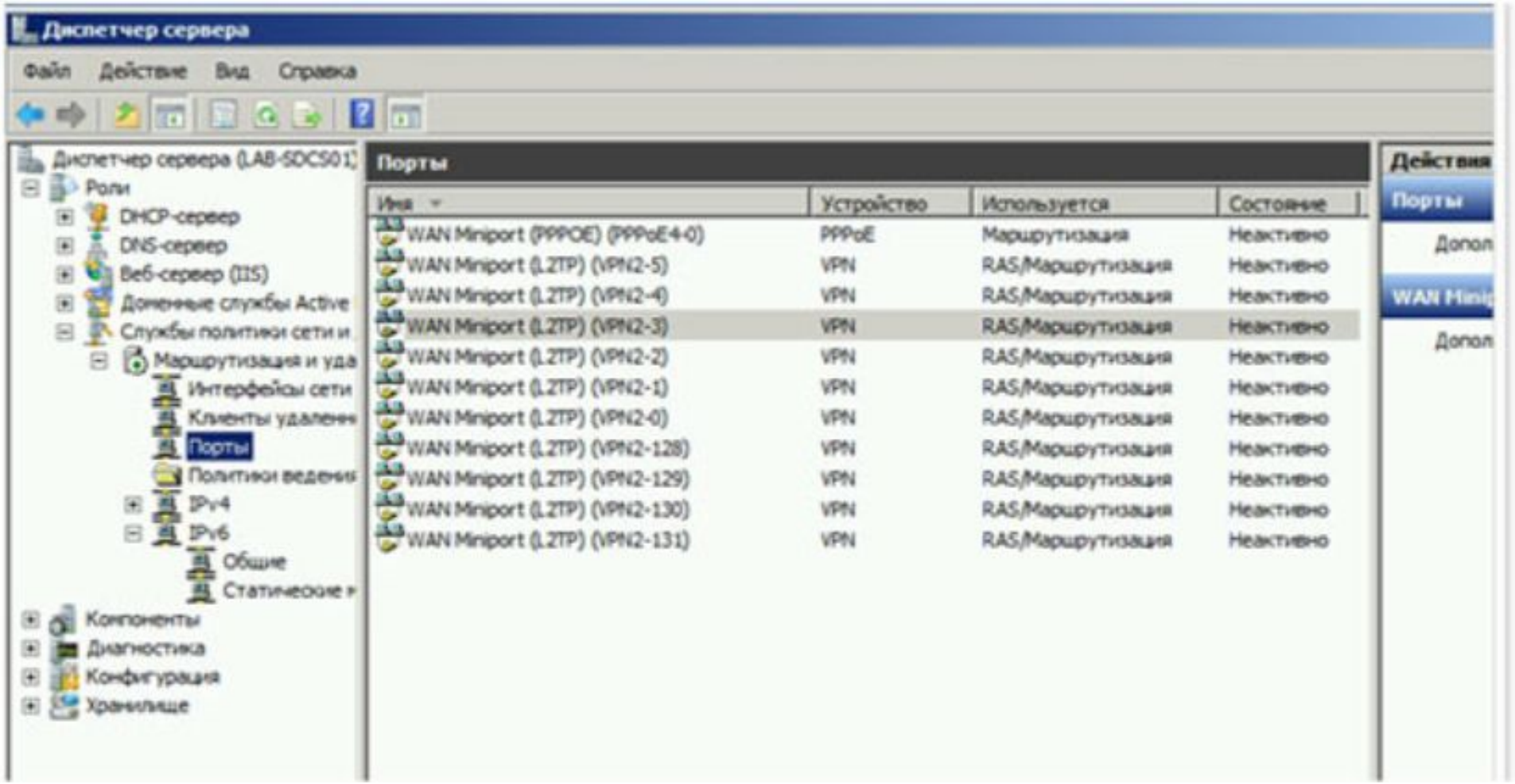
выставим максимальное количество портов, число портов должно соответствовать или превышать предполагаемое количество клиентов.

Неиспользуемые протоколы лучше отключить, убрав в их свойствах обе галочки.


Диспетчер сервера
Файл Действие Вид Справка
Диспетчер сервера (LAB-SDCS01)
Роли
DHCP-сервер
DNS-сервер
Веб-сервер (IIS)
Доменные службы Active
Службы политики сети и
Маршрутизация и уда
Интерфейсы сети
Клиенты удаленн
Порты
Политики ведения
IPv4
IPv6
Общие
Статические
Компоненты
Диагностика
Конфигурация
Хранилище
Порты
Свойства: Порты
Устройства
Маршрутизация и удаленный доступ используют перечисленные устройства.
Имя
Используется
Тип
Час...
WAN Miniport (IKEv2)
Нет
IKEv2
128
WAN Miniport (L2TP)
RAS/Маршрутизация
L2TP
10
Настройка устройства - WAN Miniport (L2TP)
Можно использовать это устройство для запросов удаленного доступа или подключений по требованию.
Подключения удаленного доступа (только входящие)
Подключения по требованию (входящие и исходящие)
Подключения по требованию (только исходящие)
Номер телефона этого устройства:
Можно установить максимальное число портов для устройства.
Максимальное число портов:
10
Подробности
OK
Отмена
Состояние
Неактивно
WAN Miniport (IKEv2) (VPN1-103)
WAN Miniport (IKEv2) (VPN1-120)
WAN Miniport (IKEv2) (VPN1-0)
WAN Miniport (IKEv2) (VPN1-17)
WAN Miniport (IKEv2) (VPN1-34)
WAN Miniport (IKEv2) (VPN1-51)
WAN Miniport (IKEv2) (VPN1-68)
WAN Miniport (IKEv2) (VPN1-85)
VPN
RAS
Действия
Порты
Допол
WAN Miniport
Допол

Настройка VPN сервера

Список портов, которые у нас остались в указанном кол



Настройка VPN сервера

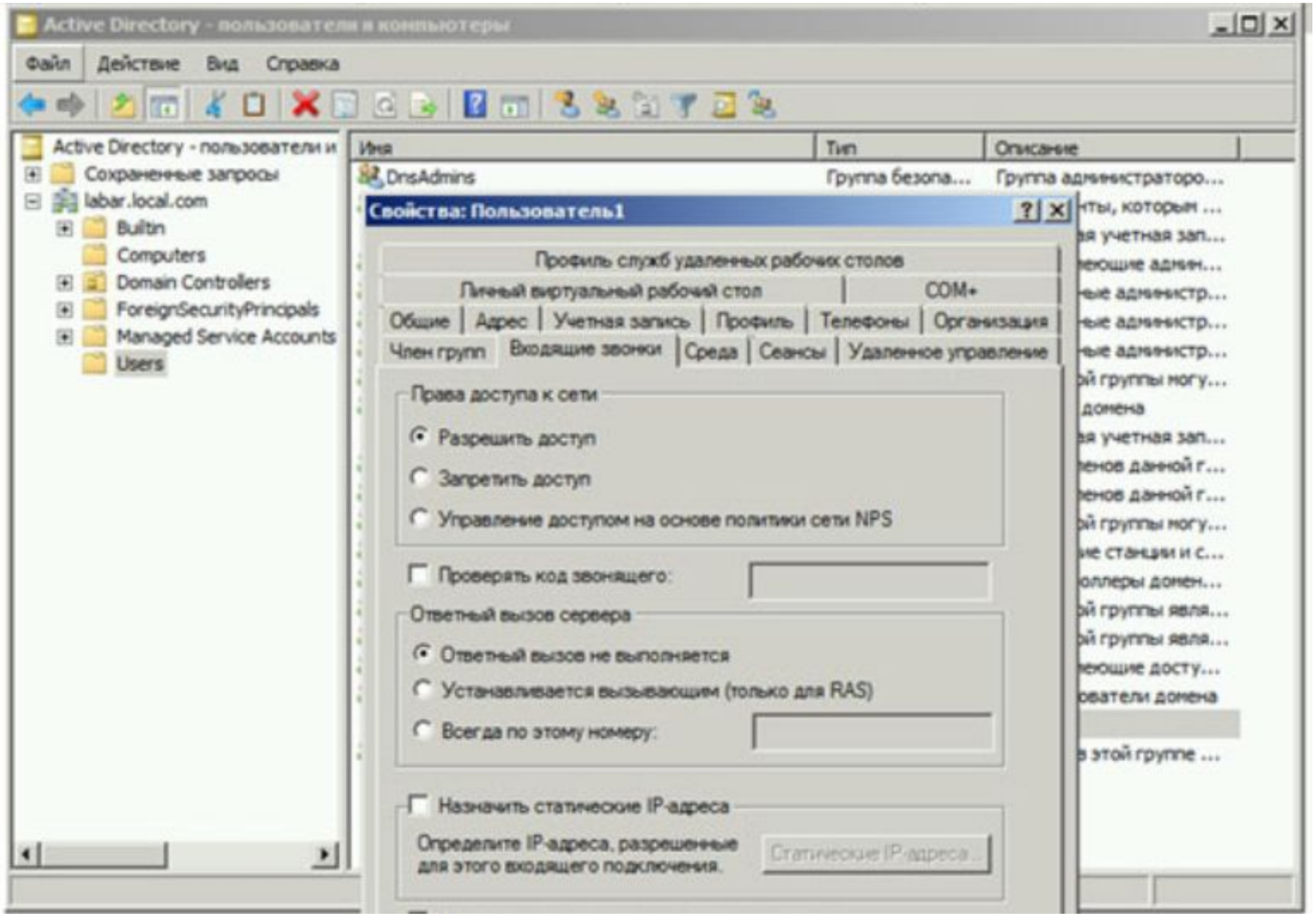
На этом настройка сервера **закончена**.

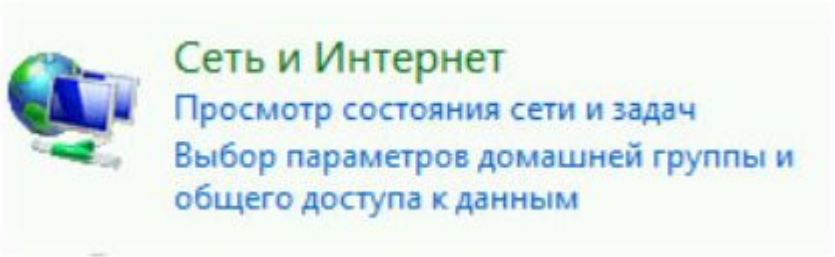
Осталось только **разрешить** пользователям подключатся к серверу.

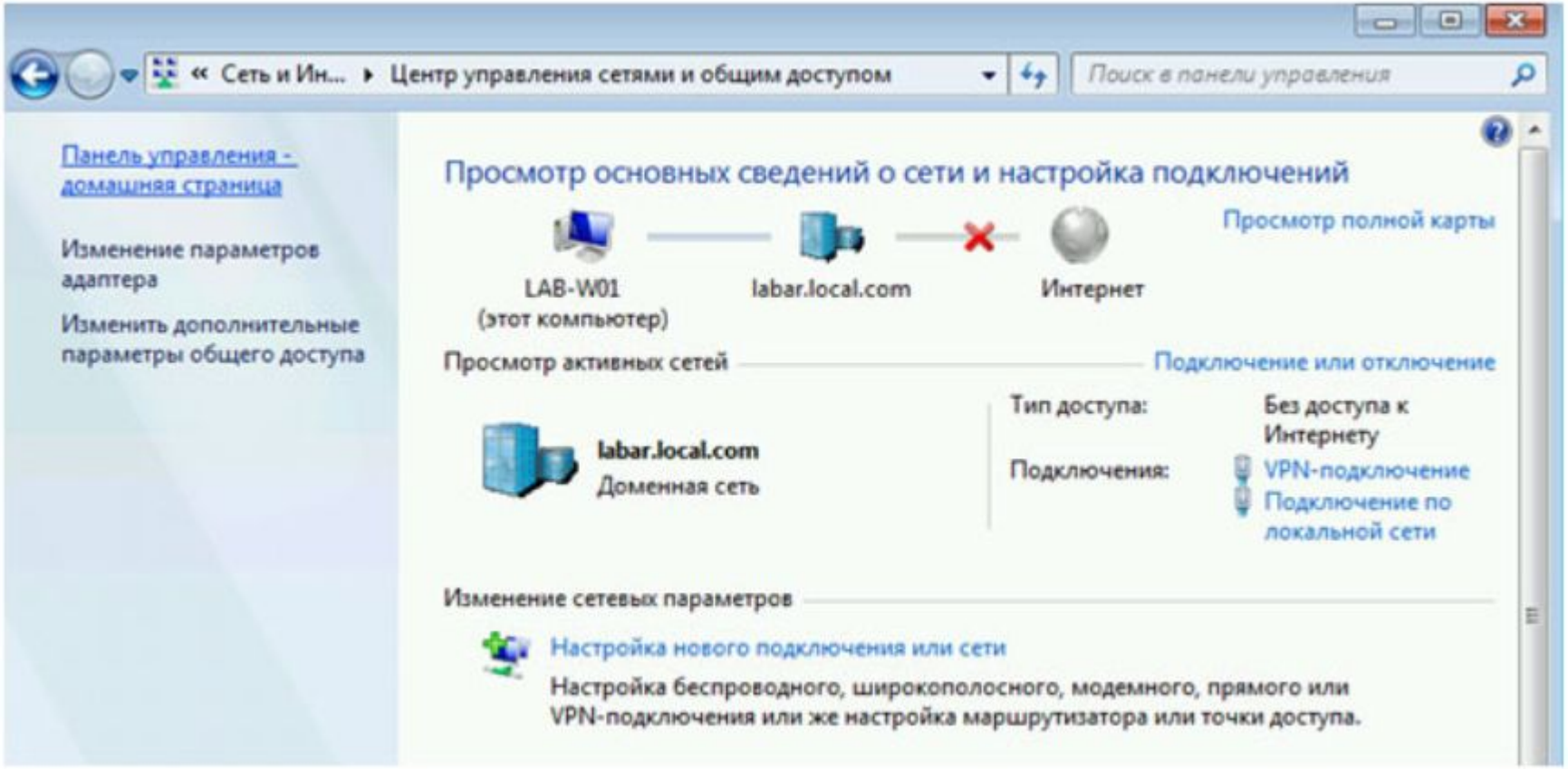
Перейдите в

Диспетчере сервера Active Directory – пользователи – находим пользователя которому хотим **разрешить доступ** нажимаем

«**Свойства**», заходим в закладку входящие звонки.


Active Directory - пользователи и компьютеры
Файл
Действие
Вид
Справка
Active Directory - пользователи и
Сохраненные запросы
labar.local.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Имя
Тип
Описание
DnsAdmins
Группа безопа...
Свойства: Пользователь1
Профиль служб удаленных рабочих столов
Личный виртуальный рабочий стол
COM+
Общие
Адрес
Учетная запись
Профиль
Телефоны
Организация
Член групп
Входящие звонки
Среда
Сеансы
Удаленное управление
Права доступа к сети
Разрешить доступ
Запретить доступ
Управление доступом на основе политики сети NPS
Проверять код звонящего:
Ответный вызов сервера
Ответный вызов не выполняется
Устанавливается вызывающим (только для RAS)
Всегда по этому номеру:
Назначить статические IP-адреса
Определите IP-адреса, разрешенные для этого входящего подключения.
Статические IP-адреса...


Сеть и Интернет
Просмотр состояния сети и задач
Выбор параметров домашней группы и общего доступа к данным


« Сеть и Ин... ▸ Центр управления сетями и общим доступом
Поиск в панели управления
Панель управления - домашняя страница
Изменение параметров адаптера
Изменить дополнительные параметры общего доступа
Просмотр основных сведений о сети и настройка подключений
Просмотр полной карты
LAB-W01
(этот компьютер)
labar.local.com
Интернет
Просмотр активных сетей
Подключение или отключение
labar.local.com
Доменная сеть
Тип доступа:
Без доступа к Интернету
Подключения:
VPN-подключение
Подключение по локальной сети
Изменение сетевых параметров
Настройка нового подключения или сети
Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа.

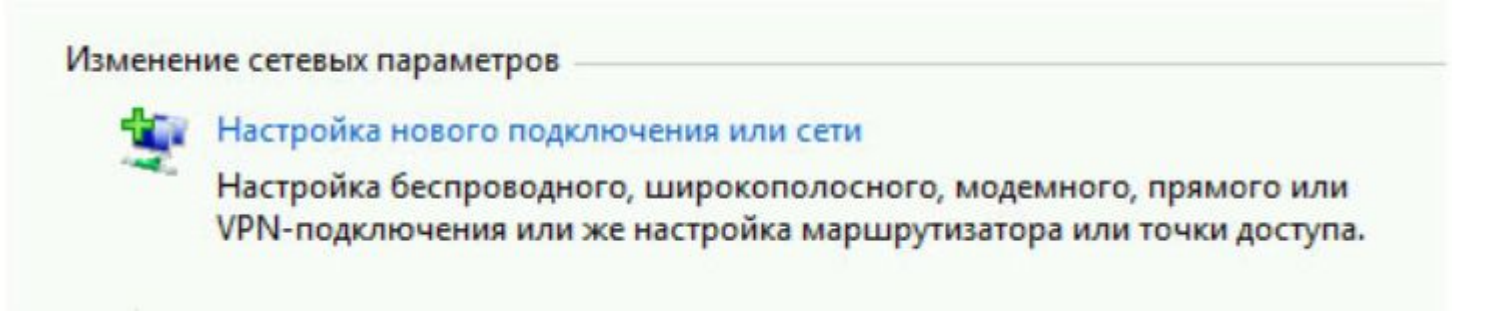
Настройка VPN соединения для Windows

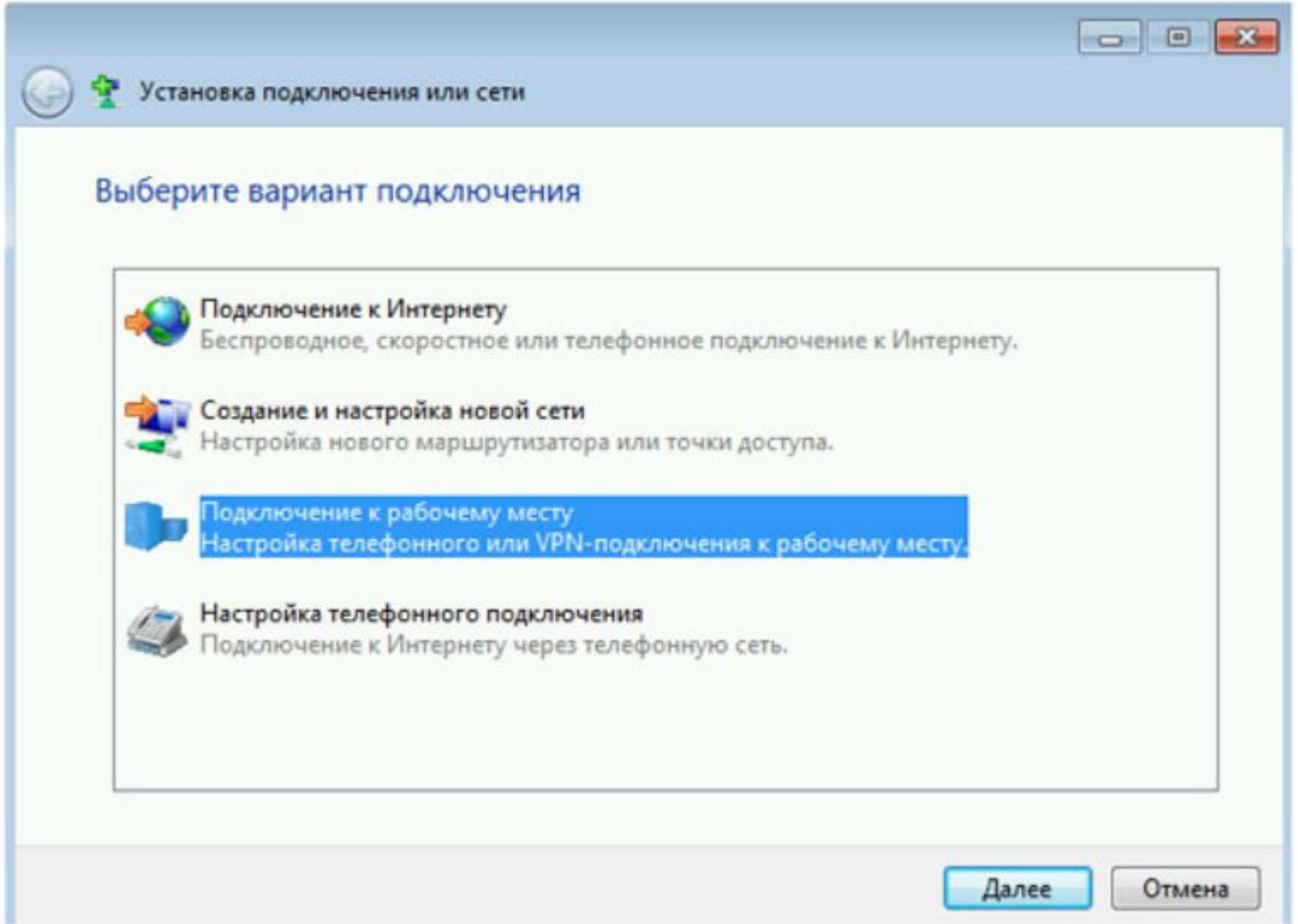
Настройка VPN соединения для Windows

Теперь необходимо настроить **пользовательскую машину** для подключения к серверу через VPN

Для этого последовательно выбираем:

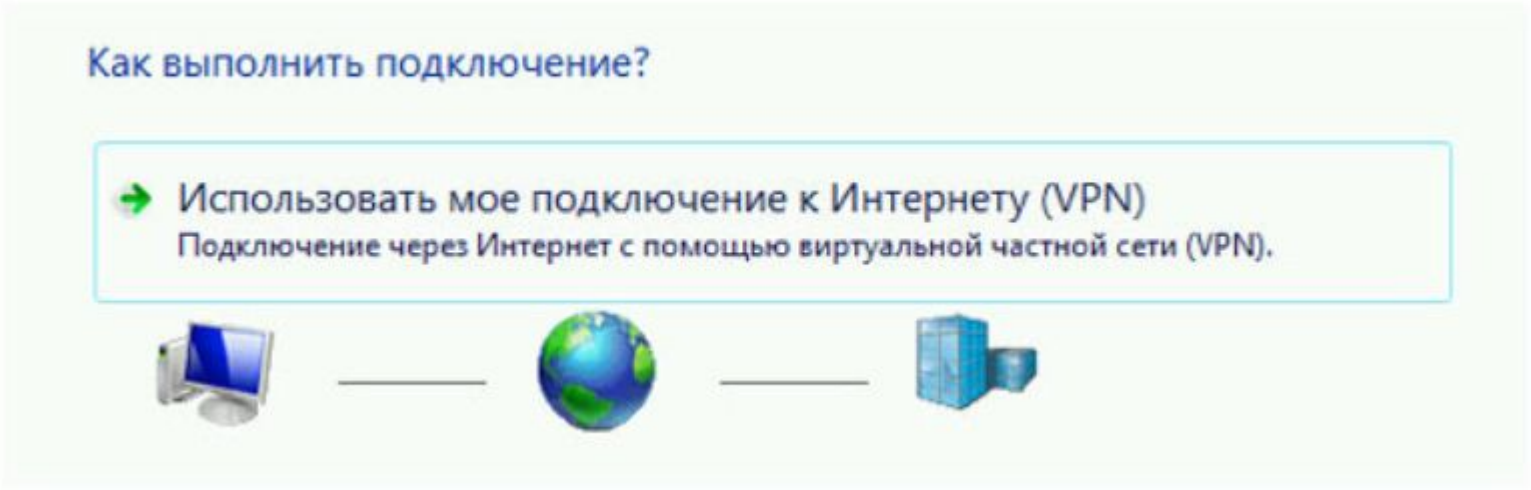
Пуск – Панель управления – Сеть интернет – Просмотр состояния сети и задач


Изменение сетевых параметров
Настройка нового подключения или сети
Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа.


Установка подключения или сети
Выберите вариант подключения
Подключение к Интернету
Беспроводное, скоростное или телефонное подключение к Интернету.
Создание и настройка новой сети
Настройка нового маршрутизатора или точки доступа.
Подключение к рабочему месту
Настройка телефонного или VPN-подключения к рабочему месту.
Настройка телефонного подключения
Подключение к Интернету через телефонную сеть.
Далее
Отмена

Настройка VPN соединения для Windows

Выбираем мастера подключения к сети



Настройка VPN соединения для Windows

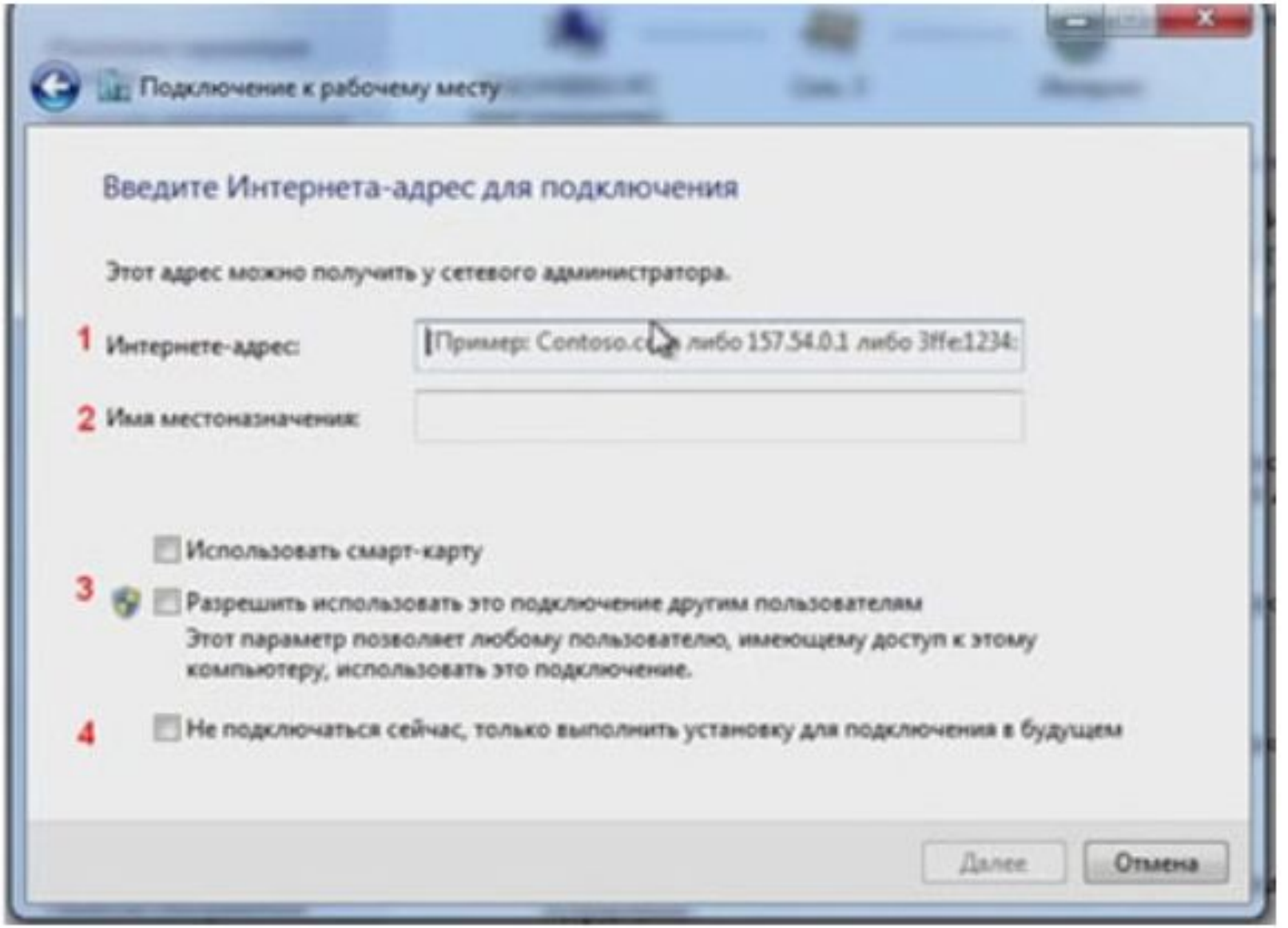
Указываем:

1. Имя VPN Сервера.

2. Имя можно указать любое.

3. Галочку поставить необходим с правами **администратора**.

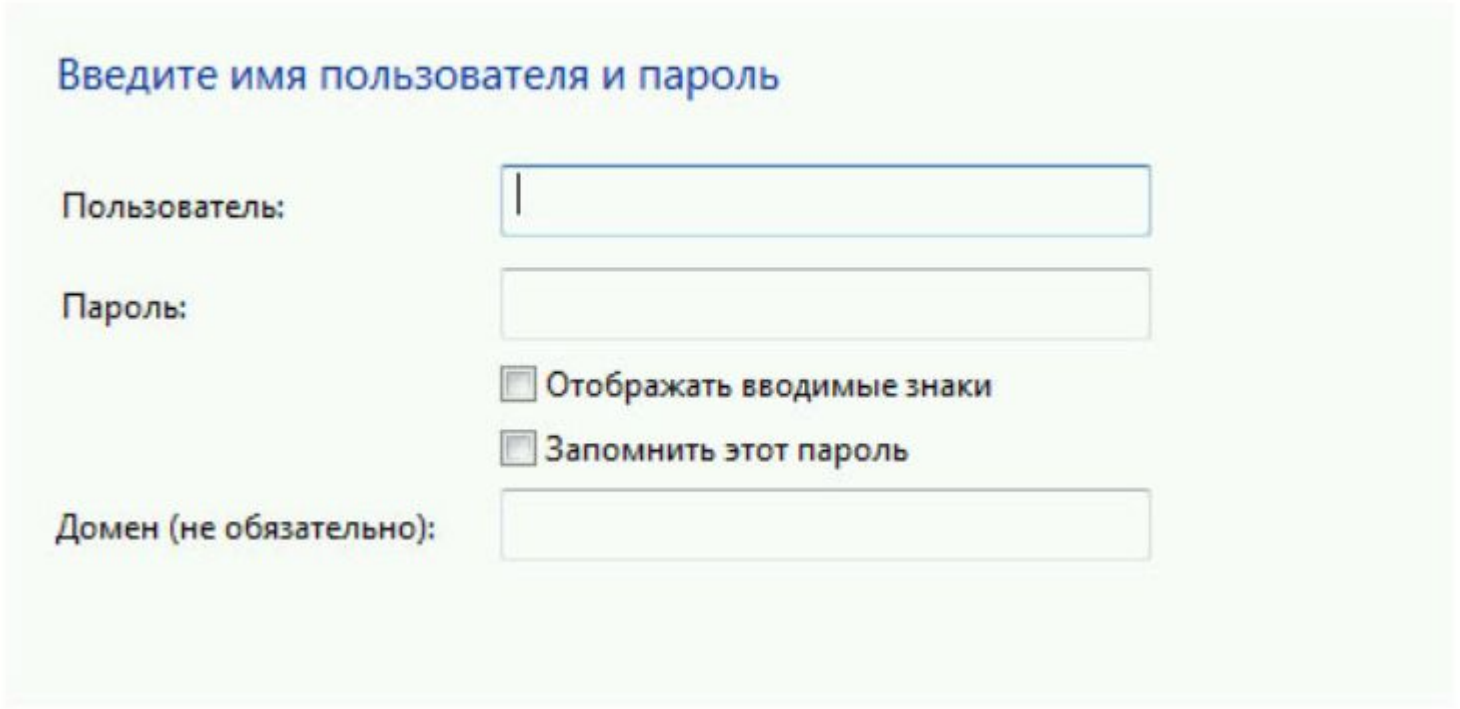
4. Галочку поставить «**Не подключаться сейчас…**».


Подключение к рабочему месту
Введите Интернета-адрес для подключения
Этот адрес можно получить у сетевого администратора.
1 Интернете-адрес:
Пример: Contoso.com либо 157.54.0.1 либо 3ffe:1234:
2 Имя местоназначения:
Использовать смарт-карту
3 Разрешить использовать это подключение другим пользователям
Этот параметр позволяет любому пользователю, имеющему доступ к этому компьютеру, использовать это подключение.
4 Не подключаться сейчас, только выполнить установку для подключения в будущем
Далее
Отмена

Настройка VPN соединения для Windows

Указываем доменные учётные записи пользователя под которым хотим подключиться:

- **имя** пользователя,
- **пароль**.


Введите имя пользователя и пароль
Пользователь:
Пароль:
Отображать вводимые знаки
Запомнить этот пароль
Домен (не обязательно):

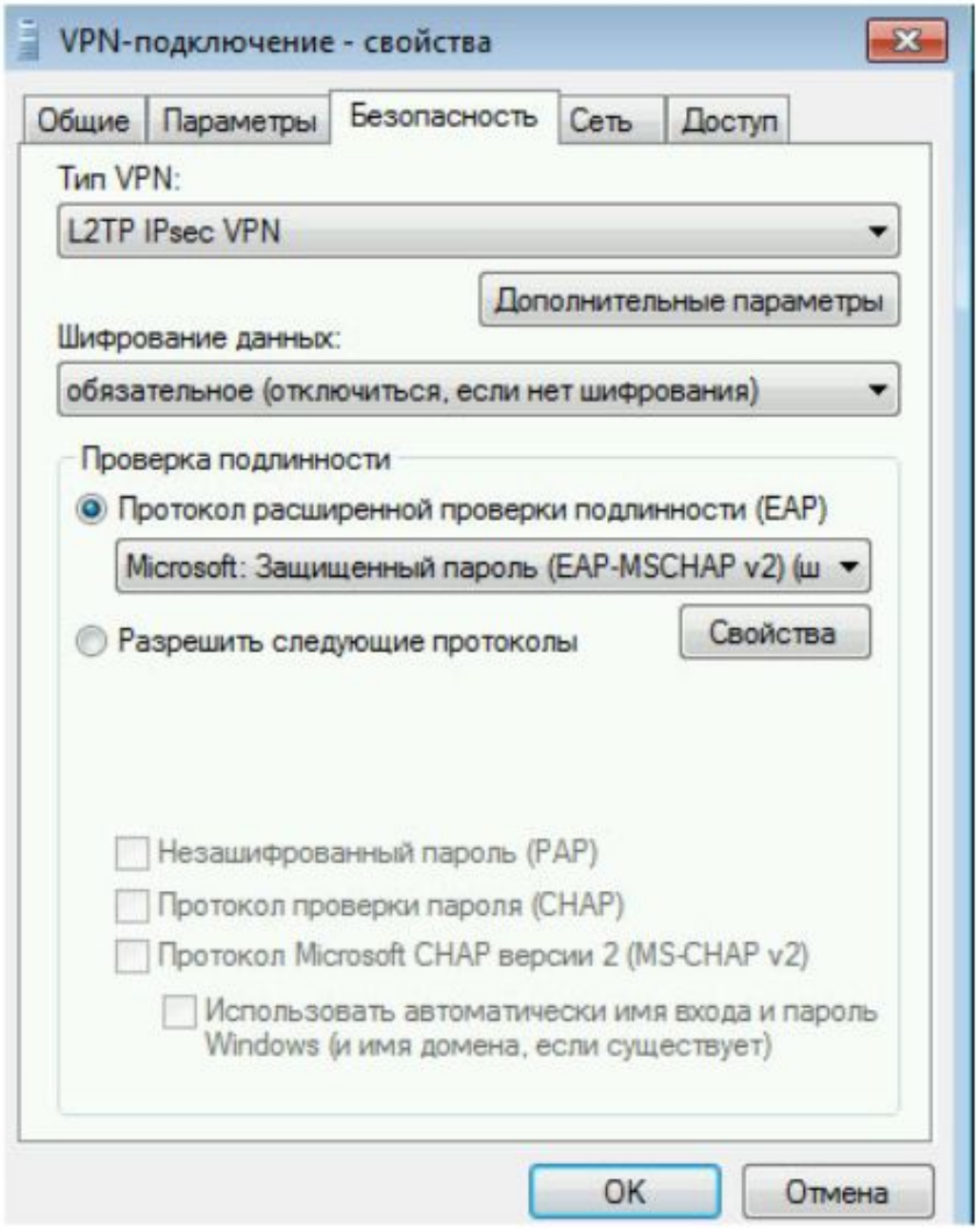
Настройка VPN соединения для Windows

После подключения зайдем в **свойства VPN** соединения на вкладку:

«**Безопасность**».

В разделе «**Проверка подлинности**» указать

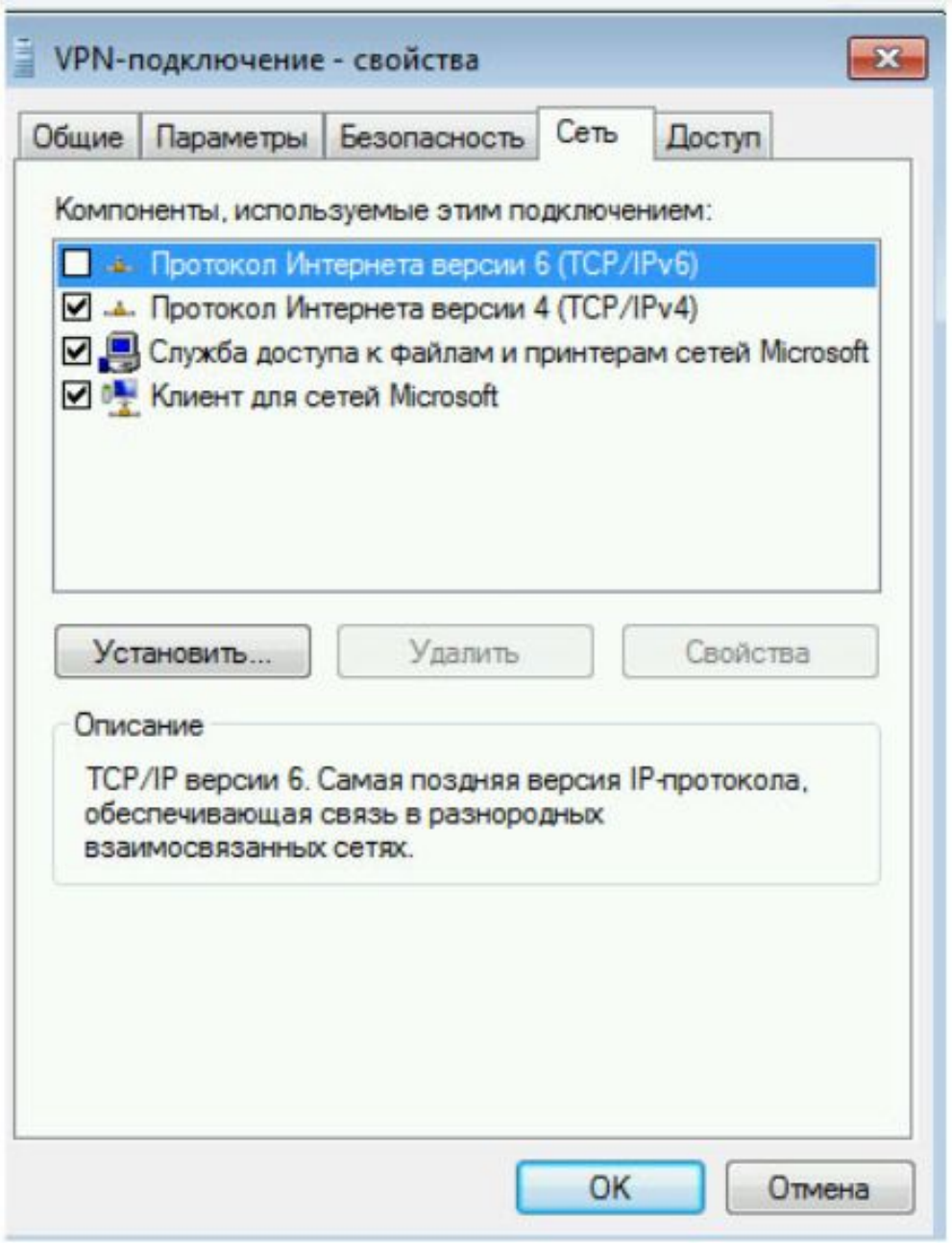
«**Протокол расширенной проверки подлинности (EAP)**».


VPN-подключение - свойства
Общие
Параметры
Безопасность
Сеть
Доступ
Тип VPN:
L2TP IPsec VPN
Дополнительные параметры
Шифрование данных:
обязательное (отключиться, если нет шифрования)
Проверка подлинности
Протокол расширенной проверки подлинности (EAP)
Microsoft: Защищенный пароль (EAP-MSCHAP v2) (ш
Разрешить следующие протоколы
Свойства
Незашифрованный пароль (PAP)
Протокол проверки пароля (CHAP)
Протокол Microsoft CHAP версии 2 (MS-CHAP v2)
Использовать автоматически имя входа и пароль Windows (и имя домена, если существует)
OK
Отмена

Настройка VPN соединения для Windows

Далее зайдём в **свойства VPN** соединения на вкладку «**Сеть**».

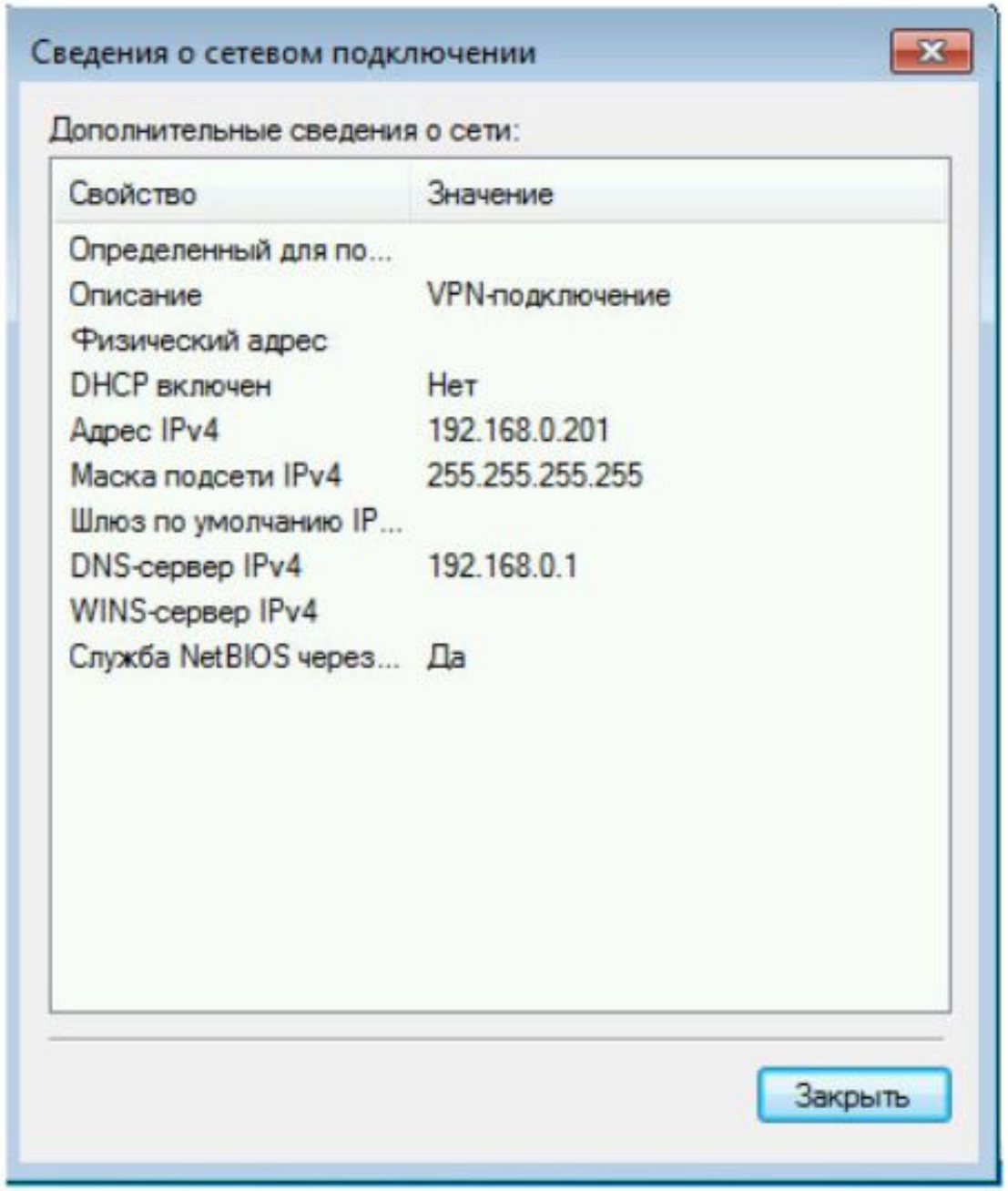
Убираем поддержку **VPN IPv6**.


VPN-подключение - свойства
Общие
Параметры
Безопасность
Сеть
Доступ
Компоненты, используемые этим подключением:
Протокол Интернета версии 6 (TCP/IPv6)
Протокол Интернета версии 4 (TCP/IPv4)
Служба доступа к файлам и принтерам сетей Microsoft
Клиент для сетей Microsoft
Установить...
Удалить
Свойства
Описание
TCP/IP версии 6. Самая поздняя версия IP-протокола, обеспечивающая связь в разнородных взаимосвязанных сетях.
OK
Отмена

Настройка VPN соединения для Windows

Проверяем настройки VPN совпадают ли они с нашими настройками

Теперь мы видим, что настройка прошла **успешно** и можно **пользоваться** ресурсами локальной сети, к которой подключились через VPN соединение!!!


Сведения о сетевом подключении
Дополнительные сведения о сети:
Свойство
Значение
Определенный для по...
Описание
VPN-подключение
Физический адрес
DHCP включен
Нет
Адрес IPv4
192.168.0.201
Маска подсети IPv4
255.255.255.255
Шлюз по умолчанию IP...
DNS-сервер IPv4
192.168.0.1
WINS-сервер IPv4
Служба NetBIOS через...
Да
Закрыть

Список литературы:

1. Беленькая М. Н., Малиновский С. Т., Яковенко Н. В. Администрирование в информационных системах. Учебное пособие. - Москва, Горячая линия - Телеком, 2011.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.

Список ссылок:

https://sys-team-admin.ru/stati/bezopasnost/155-chto-delaet-vpn-kak-nastroit-vpn-soedinenie-dlya-windows-nastrojka-vpn-servera.html
https://easy-network.ru/93-urok-45-vpn-operation.html
http://ciscotips.ru/vpn
https://www.osp.ru/pcworld/2008/09/5650787
https://youtube-lessons.ru/wp-content/auploads/798372/tehnologiya_vpn-soedineniya.jpg
https://slide-share.ru/image/5810862.jpeg

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru