Организация VPN доступа к ресурсам Компании

Руководство пользователя

Листов 22

Дата:

Версия:

СОДЕРЖАНИЕ

1. История изменений документа 2

1.1 Список изменений 2

1.2 Список согласований и ревью 3

1.3 Список утверждений 3

2. Список сокращений 4

3. Цель и границы документа 4

4. Описание деятельности 4

4.1 Предназначение системы 4

4.2 Описание протокола 4

4.3 Описание системы удаленного доступа к проектным ресурсам 5

4.4 Виды VPN доступа к сети Luxoft 5

4.5 Порядок предоставления доступа к VPN. 6

4.6 Получение прав на удаленное подключение к проектным ресурсам 6

4.7 Использование прав доступа 6

4.8 Схема подключения при использовании VPN клиента 6

4.9 Стандартные проблемы 7

Приложение 1. Результат ipconfig /all со своего рабочего ПК 8

Приложение 2. Получение VPN клиента. 10

Приложение 3. Установка VPN клиента. 12

Приложение 4. Настройка VPN клиента. 14

Приложение 5. Схема подключения при использовании VPN клиента 17

Приложение 6. Решение проблем с удалением VPN клиента. 19

# История изменений документа

## Список изменений

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Версия | Дата | Предмет изменения | Причина изменений | Кем сделано |
| 001 | 12.07.2002 | 0.1 | Создание документа | В. Егорин |
| 002 | 15.07.2002 | 0.7 | Изменение структуры документа в соответствии с замечаниями И. Гаврилюка | В. Егорин |
| 003 | 06.08.2002 | 1.0 | Внесены изменения в п.3.1. Добавлены п.3.2 и приложение 2 | И. Гаврилюк |
| 004 | 14.06.2005 | 1.1 | Добавлены приложение 4 и имена новых VPN серверов | Д. Мозжерин |
| 005 | 22.06.2005 | 1.2 | Дополнения к п.4.2 | Д. Мозжерин |
| 006 | 27.06.2005 | 1.3 | Убран список доступа сотрудников.  Добавлена Форма 1.(Приложение 1)  Убрана инструкция настройки VPN подключения в Windows 2000.  Добавлено описание системы доступа к проектным ресурсам.(Приложение 3). | Д. Мозжерин |
| 007 | 24.11.2005 | 1.4 | Добавлен п 4.2 Порядок предоставления доступа к VPN. | А.Ковалёв |
| 008 | 06.12.2010 | 1.5 | Редактирование документа | И. Кузьменков |
| 009 | 10.12.2010 | 1.6 | Внесение изменений в структуру документа | И. Кузьменков |
| 010 | 10.12.2010 | 1.7 | Форматирование документа согласно регламентам компании | И. Кузьменков |
| 011 | 26.01.2011 | 1.8 | Изменение структуры документа в соответствии с замечаниями Quality Engineer | И. Кузьменков |
| 012 | 06.06.2011 | 2.0 | Актуализация инструкции. | Ф. Тарасенко |
|  |  |  |  |  |

## Список согласований и ревью

|  |  |  |  |
| --- | --- | --- | --- |
| Версия | Дата | Ревьюер | Результат ревью (ссылка на документ) |
|  |  |  |  |
|  |  |  |  |

## Список утверждений

|  |  |  |  |
| --- | --- | --- | --- |
| Версия | Дата | Кто утвердил | Ссылка на документ (или подпись) |
|  |  |  |  |
|  |  |  |  |

# Список сокращений

VPN — Virtual Private Network, система защищенного доступа к ресурсам сети Компании удаленных пользователей через Интернет.

# Цель и границы документа

Настоящий документ описывает систему удаленного доступа к сети Компании и правила ее использования.

# Описание деятельности

## Предназначение системы

Система VPN доступа предназначена для доступа сотрудников, находящихся вне офиса Компании к ресурсам локальной сети Компании. Для осуществления доступа необходимо иметь компьютер, подключенный к Интернет и обладать соответствующими полномочиями.

VPN обеспечивает защищенное присоединение к сети Компании и двустороннюю передачу данных. После осуществления подключения между сторонами устанавливается виртуальный туннель, внутри которого осуществляется передача зашифрованных данных. То есть обеспечивается двойная защита — инкапсуляция пакетов данных в пакеты туннеля, обратное раскрытие которых возможно только участниками установленного соединения + шифрование данных.

Для пользователя это выглядит это как работа в сети Компании. Единственное отличие — более низкая скорость соединения (в зависимости от используемого канала передачи данных), чем при работе в локальной сети. **Также для этого соединения не разрешен доступ к серверам высшего уровня конфиденциальности.**

Таким образом, в рамках виртуальной частной сети, пользователь получает единую среду информационного окружения. Он может обращаться к ресурсам Компании независимо от своего местонахождения, имея только доступ в Интернет. Ему не нужно запоминать множество паролей — достаточно лишь учетной записи в домене. При этом, **он должен четко следовать рекомендациям по регулярной смене паролей и обеспечения их недоступности для третьих лиц.**

## Описание протокола

Соединение устанавливается по протоколам IKE (UDP port 500) и IPSEC (IP protocol 51).

Если между VPN шлюзом и вами осуществляется трансляция адресов (NAT), то для IKE используются UDP port 500 , а для IPSEC UDP или TCP port 4500.

## Описание системы удаленного доступа к проектным ресурсам

Для организации доступа удаленных пользователей к сети компании необходимо выполнение следующих операций:

* аутентификация пользователя
* авторизация пользователя
* политика ведения учетных записей

Пользователь, соединяясь с VPN шлюзом, пересылает свои данные — логин и пароль. VPN шлюз посылает запрос на аутентификацию и авторизацию RADIUS серверу, который в свою очередь обращается к базе пользователей контроллера домена. После согласования всех необходимых параметров и выполнения настроек политик доступа, между компьютером клиента и VPN шлюзом устанавливается шифрованное соединение. При этом согласно политикам, заданным пользователю на контроллере домена и firewall, пользователь получает доступ к ресурсам локальной сети компании.

В качестве VPN шлюзов выступают устройства Cisco ASA/PIX.

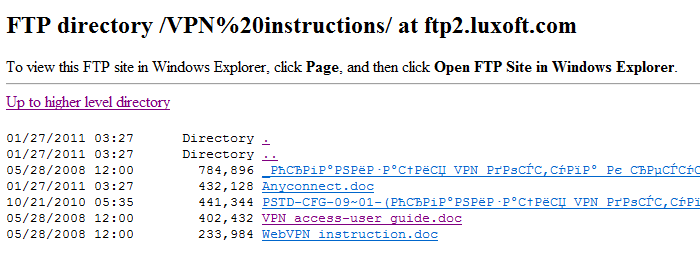
Используются следующие профили подключений:

|  |  |
| --- | --- |
| **Локация** | **Название профиля** |
| Москва, Дубна, Санкт-Петербург | LUXOFT Remote Access (Moscow).pcf |
| Омск | LUXOFT Remote Access (Omsk).pcf |
| Украина | LUXOFT Remote Access (Kiev).pcf |
| Румыния | LUXOFT Remote Access (Moscow).pcf |
| Америка | LUXOFT Remote Access (New York).pcf |
| Вьетнам | LUXOFT Remote Access (Vietnam).pcf |

## Виды VPN доступа к сети Luxoft

Существует два основных вида VPN доступа к сети Luxoft:

1. С использованием VPN клиента (Cisco VPN client или Cisco Anyconnect )
2. С использованием сервиса WebVPN ( <https://webvpn.luxoft.com> )



## Порядок предоставления доступа к VPN.

Порядок предоставления доступа к VPN устанавливается следующий:

1. VPN доступ для сотрудников выдается в рамках производственной необходимости при подтверждении начальника отдела и описанием необходимости. В частности, если в проекте сотруднику необходим доступ из дома – должно быть приведено обоснование такой необходимости и по окончание проекта доступ должен быть отключен.
2. Доступ по VPN предоставляется до: проектных серверов по всем портам, корпоративных ресурсов кроме серверов высшего уровня конфиденциальности, и персональных компьютеров только по портам 3389 (RDC).

## Получение прав на удаленное подключение к проектным ресурсам

Для предоставления доступа по VPN до сети компании необходимо создать заявку в системе ServiceDesk (<https://servicedesk.luxoft.com>), в которой приложить аттачем следующую информацию:

* подтверждение руководителя сотрудника (в том случае если запрашивающий сам является руководителем группы или направления, то подтверждение не нужно). Приложением или комментарием к заявке.
* результат ipconfig /all со своего рабочего ПК. Как узнать ipconfig своего ПК можно посмотреть в Приложении 1 настоящей инструкции.

## Использование прав доступа

Реализация удаленного подключения осуществляется посредством создания и настройки специального вида подключения — VPN-клиента, на персональной рабочей станции (ноутбуке) сотрудника.

Процедура получения, установки и настройки VPN клиента, входящего в состав Windows описана в Приложении 2, Приложении 3 и Приложении 4 соответственно.

## Схема подключения при использовании VPN клиента

Пользователь через VPN клиент подключается к сети Luxoft. Далее пользователю необходимо подключиться, используя RDC ([Remote Desktop Connection](http://ru.wikipedia.org/w/index.php?title=Remote_Desktop_Connection&action=edit&redlink=1" \o "Remote Desktop Connection (страница отсутствует)) Client) , к своему рабочему ПК, откуда он имеет свой стандартный рабочий доступ. Для этого необходимо выполнить действия, описанные в Приложении 5.

## Стандартные проблемы

Основные проблемы, возникающие у пользователя, можно разделить на три вида :

1. Проблемы с установкой и настройкой VPN клиента

Не запускается VPN клиент – первое что надо проверить запушен ли сервис Cisco AnyConnect VPN Agent или Cisco Systems, Inc. VPN Service (в зависимости от клиента), проверить выключен ли сервис Internet Connection Sharing в свойствах сетевой карты. Error 440: Driver Failure – обычно это происходить из за отсутствия DNE (Deterministic Network Enhancer), его можно вручную добавить на NIC :

* Открыть Network and Sharing Center
* Открыть Manage Network Connection
* Правый клик на Local Area Connection
* Выбрать Install
* Выбрать Service
* Выбрать Have Disk
* Выбрать путь c:\program files\common\Deterministic Networks\DNE\dne2000
* Выбрать Open

Reason 440: Cannot start the driver - убедитесь что DNE установлен правильно . Откройте CMD выполните следующие команды «net stop dne» вы должны получить ответ, что он не может быть остановлен, если же вы получили ошибку cannot be found значит DNE не установлен (см. выше). Если он установлен, то выполните следующие команды «net stop cvpndrva», затем «net start cvpndrva». Если все выше описанное не помогло, переустановите VPN клиент ( удалите старый, перезагрузитесь и установить новый ).

1. *Проблемы с подключением VPN клиента*

При возникновении проблем с подключением VPN клиента в первую очередь необходимо проверить правильность вводимого пароля или учтенной записи. Или обратиться в службу Service Desk

1. *Проблемы с удалением VPN клиента*

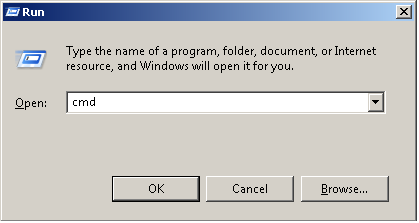
При возникновении сложностей с удалением VPN клиента, необходимо удалить некоторые ключи реестра. Как это сделать описано в Приложении 6.

# Приложение 1. Результат ipconfig /all со своего рабочего ПК

Для того чтобы узнать ipconfig своего ПК , необходимо выполнить следующие действия :

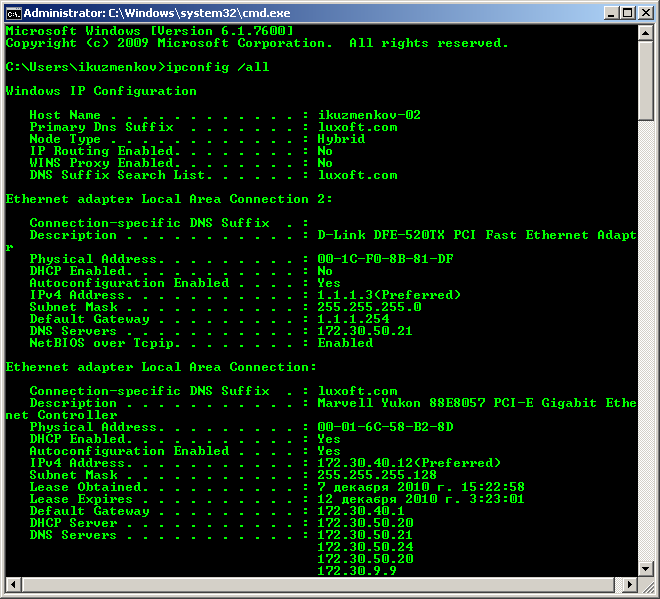
1. Пуск – Выполнить – cmd (Рис. 1.1)

Рис 1. 1.



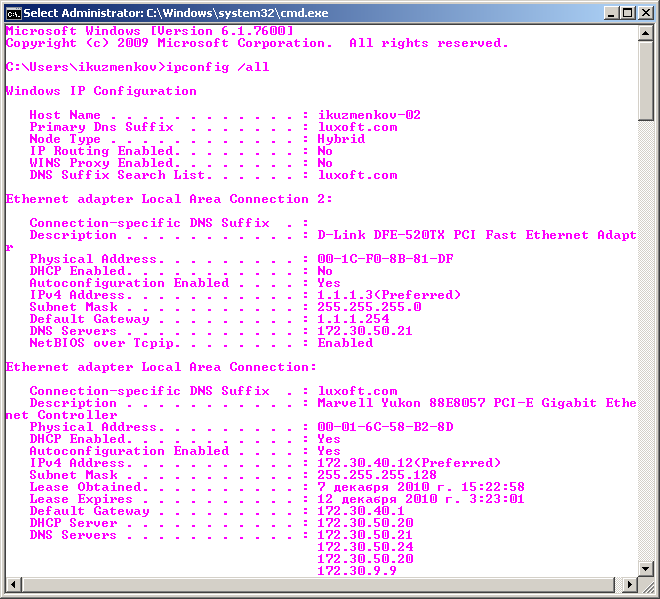
1. В появившемся окне набрать команду ipconfig /all (Рис. 1.2)

Рис 1.2.



1. Затем нажать правой кнопкой мыши на консоли в контекстном меню выбрать Select All, после чего нажать на правую кнопку мыши (текст скопируется на клипборд) (Рис.1.3)

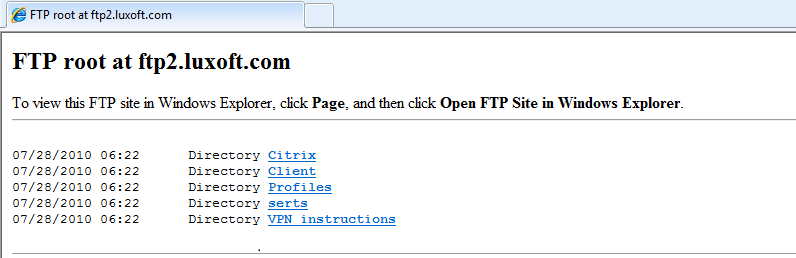
Рис 1. 3.



1. Далее текст можно вставить в комментарий к заявке, кликнув правой клавишей мыши и нажав Paste в теле заявки.

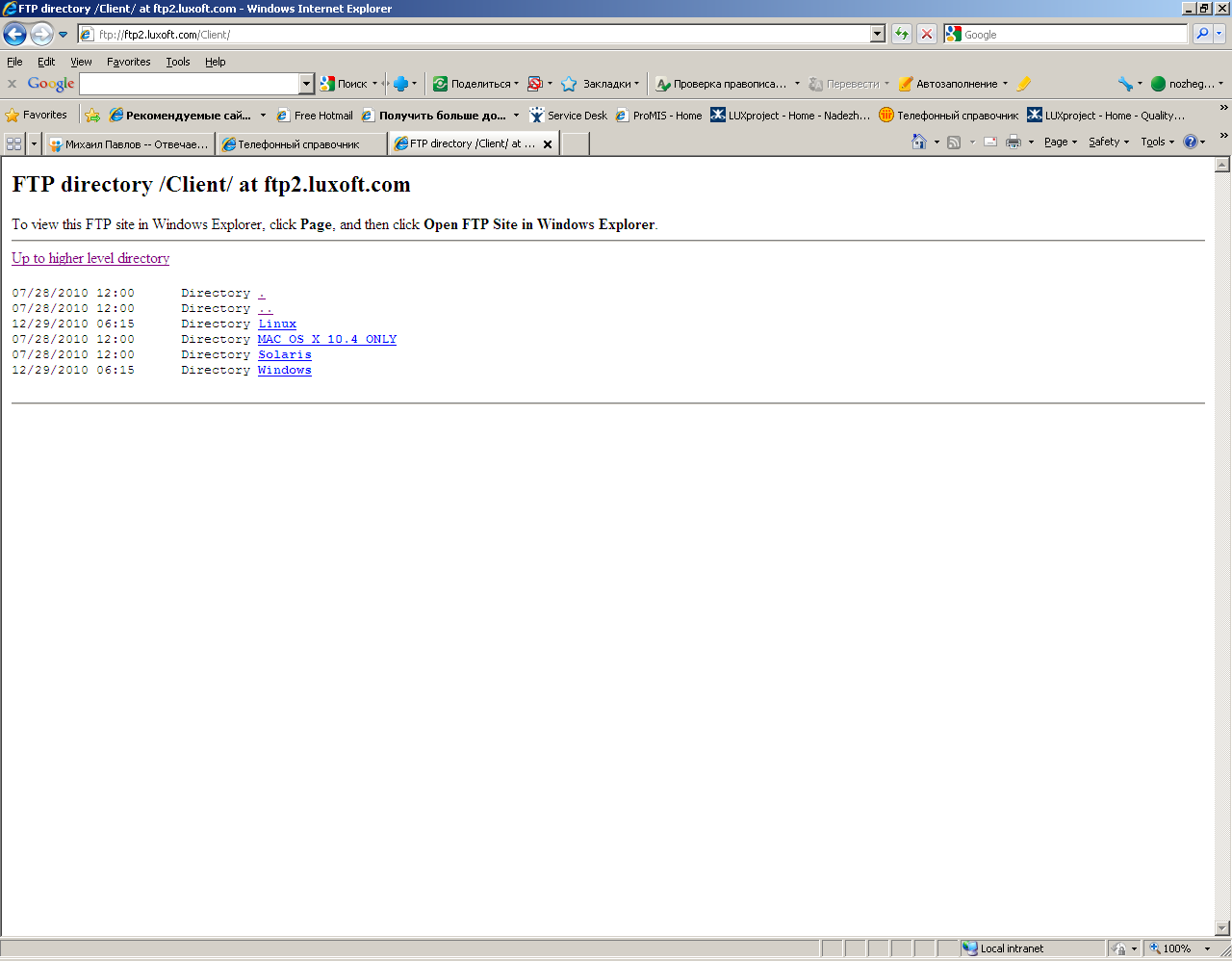
# Приложение 2. Получение VPN клиента.

Для получения дистрибутива VPN клиента пройдите по адресу <ftp://ftp2.luxoft.com/>. При входе видны папки (Рис. 1.4). Для установки VPN клиента необходимы папки Client и Profiles.

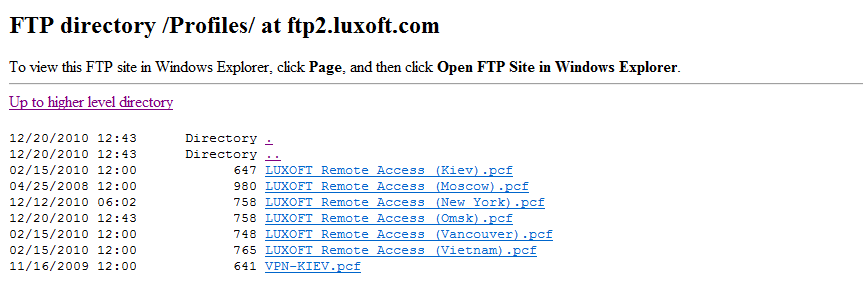
Рис 1.4. 

В папке «Client» находятся версии VPN клиентов под разные ОС (есть клиенты для MAC OS 10.4, Linux, Solaris и Windows). Описание установки VPN клиента под имеющуюся ОС (например, Windows) приводится в Приложении 3.

Рис 1.5 Содержание папки Client



В папке «Profiles» находятся .pcf файлы настройки подключения для VPN клиента. Выбор нужного файла зависит от вашего физического места расположения. Описание как импортировать выбранный файл в VPN клиент приводится в пункте 3.2.

Рис 1.6. Содержимое папки Profiles 

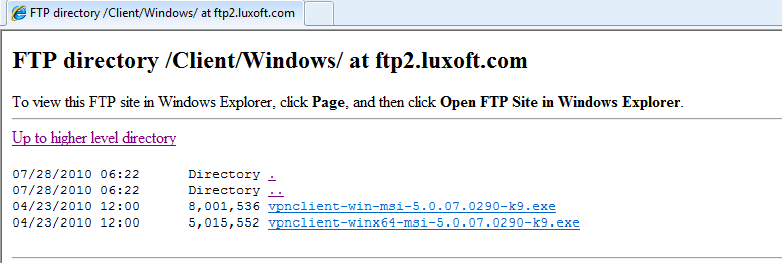
# Приложение 3. Установка VPN клиента.

Перед тем, как начать установку VPN клиента, скачайте, к примеру, в папку С:\Temp\ папку Profile и соответствующую вашей ОС (например, Windows) папку Client/Windows.

В папке «Windows» находится 2 файла клиента для Windows OC (Win XP, Win Vista, Win 7)

* vpnclient-win-msi – клиент для 32 битной ОС;
* vpnclient-winх64-msi – клиент для 64 битной ОС.

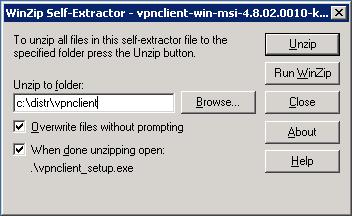
Рис 1.7.



Откройте папку C:\Temp\Windows и запустите необходимую под вашу ОС установку клиента vpnclient-win-msi-5.0.00.0340-k9.exe

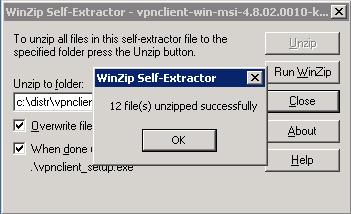
Разверните клиент (например, в папку c:\distr\vpnclient). Нажмите Unzip

Рис 1.8

****

Нажмите OK (рис. ниже)

Рис 1. 9.

****

Далее по шагам:

Нажмите Next .

Выбирете I accept the license agreement и нажмите Next.

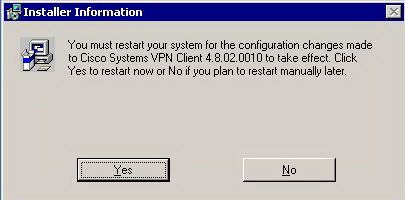
Нажмите Next.

Нажмите Next.

После окончания установки нажмите Finish.

Далее перезагрузите ПК выбрав Yes (рис. ниже)

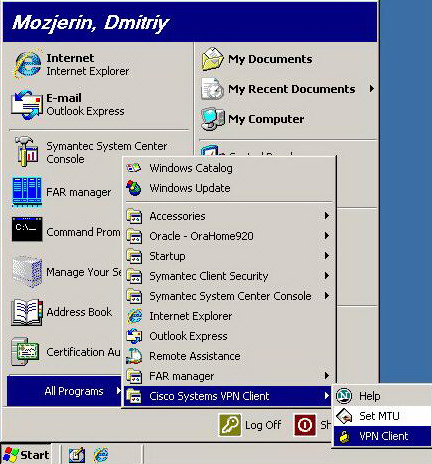
Рис 1.10

****

# Приложение 4. Настройка VPN клиента.

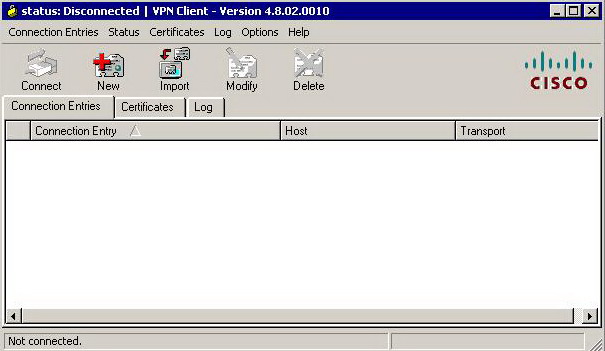
После перезагрузки запустите VPNClient.

Рис 1. 11

****

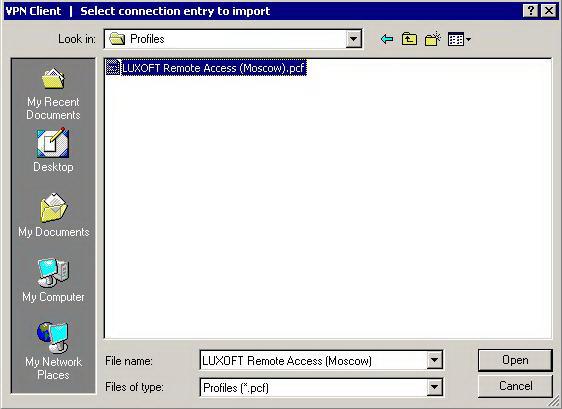
В появившемся ниже окне нажмите на иконку Import

Рис 1.12.

****

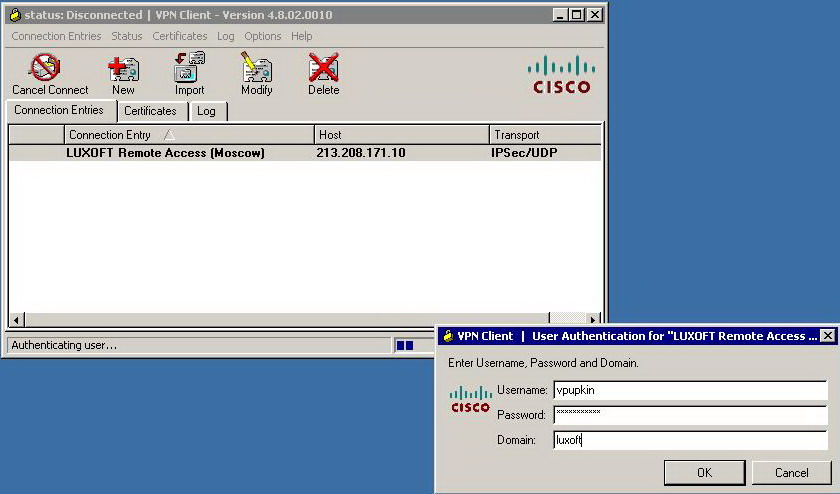
Зайдите в папку C:\Temp\Profiles , выберите профиль и нажмите Open. (Профилей может быть несколько. В имени профиля в скобках указан филиал ,через который вы входите в корпоративную сеть: Москва, Питер, Киев и т.д. Выбирать желательно ближайший к вам город)

Рис 1.13



Вернитесь к закладке Connection Entries, выберите соединение и нажмите на иконку Connect. Введите доменную учётную информацию и жмите OK.

Рис 1.14

****

После успешного соединения вы увидите окно с приветствием. Нажмите Continue. Появится жёлтая иконка на панели инструментов.

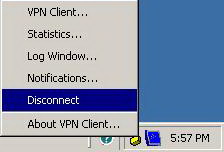
Рис 1.15

**993**

Теперь Вы можете работать с корпоративной сетью.

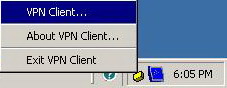
Чтобы прервать VPN соединение нажмите на значок и выберете Disconnect.

Рис 1.16

****

Чтобы возобновить соединение, нажмите на значок и активируйте главное окно выбрав в меню VPN Client . Далее снова выбираете нужное соединение и нажимаете Connect.

Рис 1.17

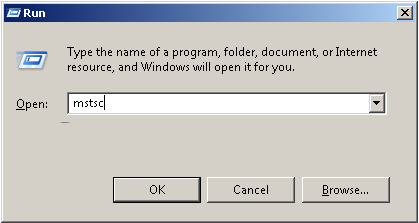
****

# Приложение 5. Схема подключения при использовании VPN клиента

Для подключения к сети Luxoft через VPN выполнить следующие действия:

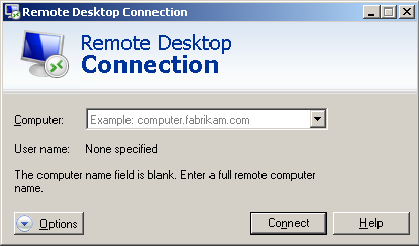
1. Пуск – Выполнить – mstsc

Рис 1. 18



1. В появившемся окне вводим IP адрес или имя удаленного ПК

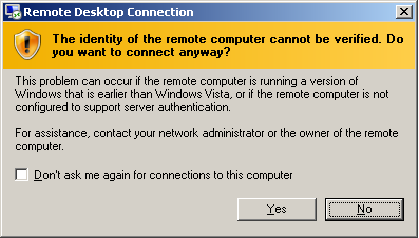
Рис 1.19



1. Нажимаете Connect

Примечание. Если вы используете Windows 7 или Windows Vista при подключение к более ранним OC, то появится предупреждение

Рис 1.20



Поставьте галочку «Don’t ask me again» и нажмите «Yes»

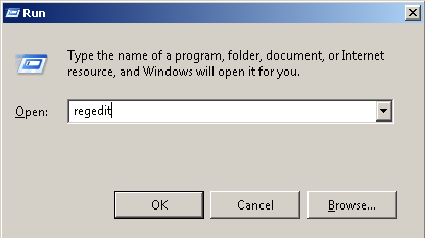
Далее введите ваши доменные учтенные данные (Логин\Пароль)

# Приложение 6. Решение проблем с удалением VPN клиента.

При возникновении сложностей с удалением VPN клиента, необходимо удалить некоторые ключи реестра.

* Открываем редактор реестра Пуск – Выполнить – regedit

Рис 1. 21



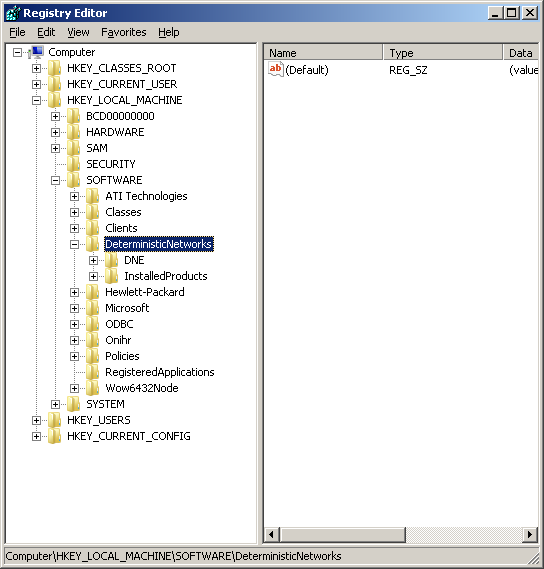
* Находим необходимые ветки реестра:

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Cisco Systems \ VPN Client

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Deterministic Networks

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ {5624c000-b109-11d4-9db4-00e0290fcac5}

Рис 1. 22



* Также проверяем другие ключи на предмет упоминания о VPN Client (с помощью поиска)

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ CISCOREBOOTFLAG

Теперь удаляем некоторые каталоги и файлы (часть может оказаться заблокированной - для их удаления можно воспользоваться FAR'ом или удалить все незаблокированные, а потом удалить остальных после перезагрузки ПК) .

?С\Program Files\Cisco Systems\VPN Client

?С\Program Files\Common Files\Deterministic Networks

?Windows\system32\drivers\dne2000.sys

?Windows\inf\dne2000m.inf и dne2000m.pnf

?Windows\system32\dneinobj.dll

?Windows\system32\drivers\cvpndrv.sys или cvpndrva.sys

переименуем файл ?Windows\system32\CSGina.dll в CSGina.old

Теперь можно перезагрузиться и убедиться, что в системе больше нет Cisco VPN интерфейса.