

Установка Cisco VPN Client

1. Требования
2. Где взять Cisco VPN Client
3. Установка Cisco VPN Client
4. Создание нового подключения
5. Вторичная авторизация
6. Диагностика и устранение проблем при установлении крипто-туннеля
7. Контакты

Требования

1. Cisco VPN Client работает на любой операционной системе семейства Microsoft Windows. Может работать нестабильно в Windows 8.
2. Для установки Cisco VPN Client необходимо иметь права администратора.
3. Для работы Cisco VPN Client использует порты UDP 500, 4500, протокол ESP они должны пропускаться через Firewall на вход и на выход.
4. Cisco VPN Client НЕ работает через Proxy.

Где взять

Файл для установки cisco vpn клиента можно взять с ftp:

<ftp://ftp.nprts.ru/net/vpn/>

рекомендуем использовать последнюю версию программы
файл для скачивания:

для 32-х битных Windows: vpnclient-win-msi-5.0.07.0410-k9.exe,

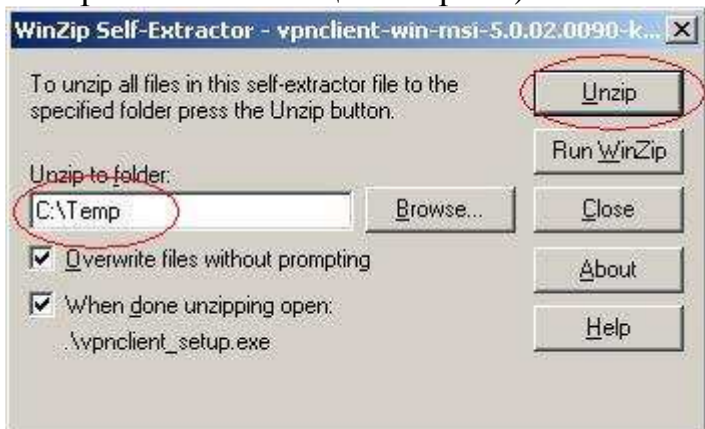
для 64-х битных Windows: vpnclient-winx64-msi-5.0.07.0440-k9.exe

Содержание /net/vpn/

Имя	Размер	Последнее изменение
 [родительский каталог]		
 archive/		13.01.14 11:13:00
 vpnclient-darwin-4.9.01.0180-universal-k9.dmg	14.5 MB	13.01.14 11:13:00
 vpnclient-linux-x86_64-4.8.02.0030-k9.tar.gz	2.0 MB	13.01.14 11:13:00
 vpnclient-win-msi-5.0.07.0410-k9.exe	7.6 MB	13.01.14 11:13:00
 vpnclient-winx64-msi-5.0.07.0440-k9.exe	4.8 MB	13.01.14 11:13:00
 VPN_installation_guide.pdf	928 kB	13.01.14 11:13:00
 VPN_installation_guide_ENG.pdf	830 kB	13.01.14 11:13:00

Установка Cisco VPN Client

После сохранения необходимо запустить файл .exe на выполнение (это самораспаковывающийся архив)



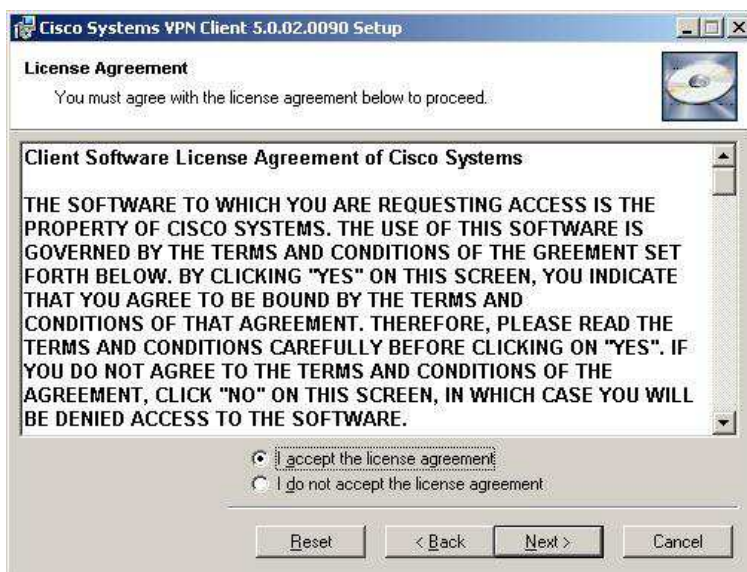
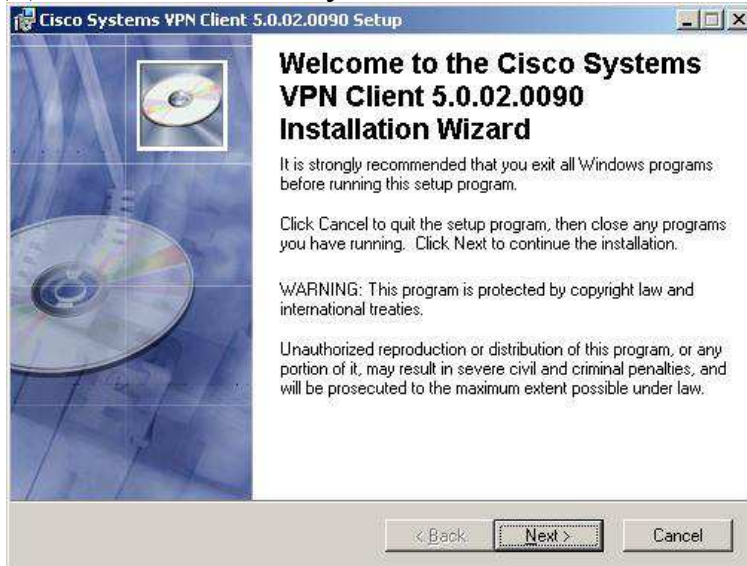
Выбрать папку для распаковки, нажать кнопку Unzip и дождаться сообщения:



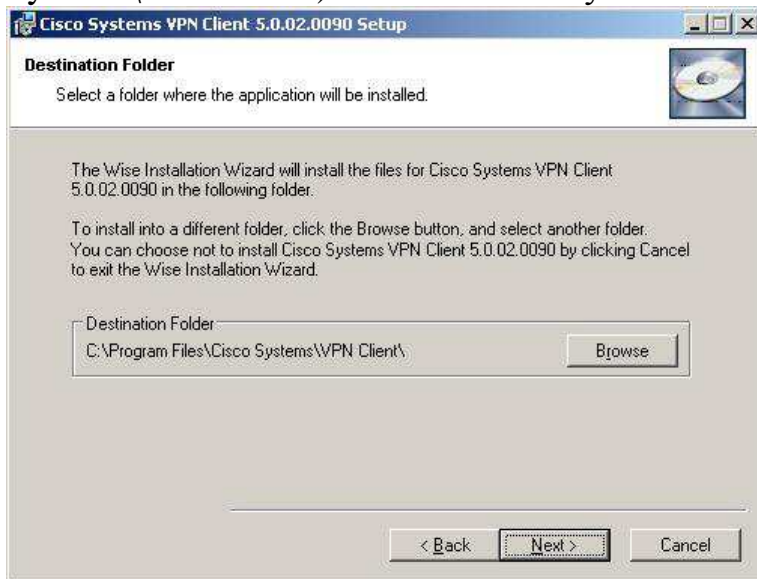
После этого, автоматически, запустится программа установки
Выбираем язык интерфейса программы и нажать кнопку «ОК»



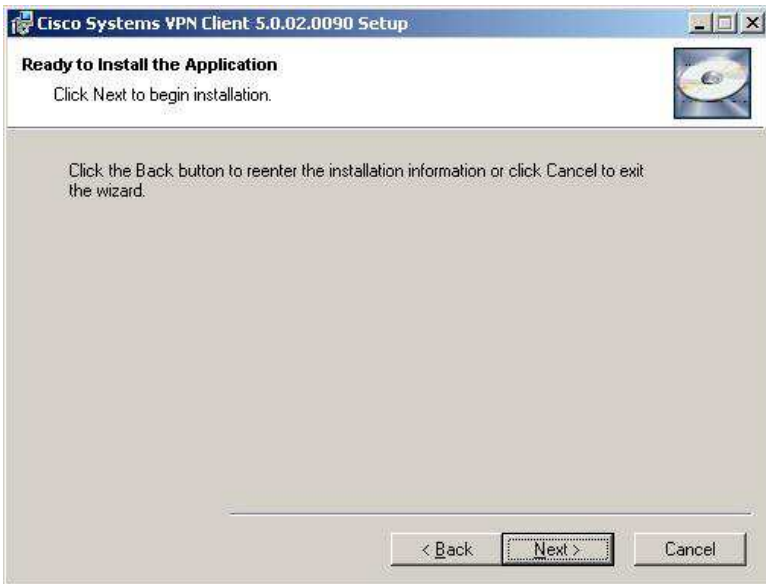
Далее нажать кнопку «Next»



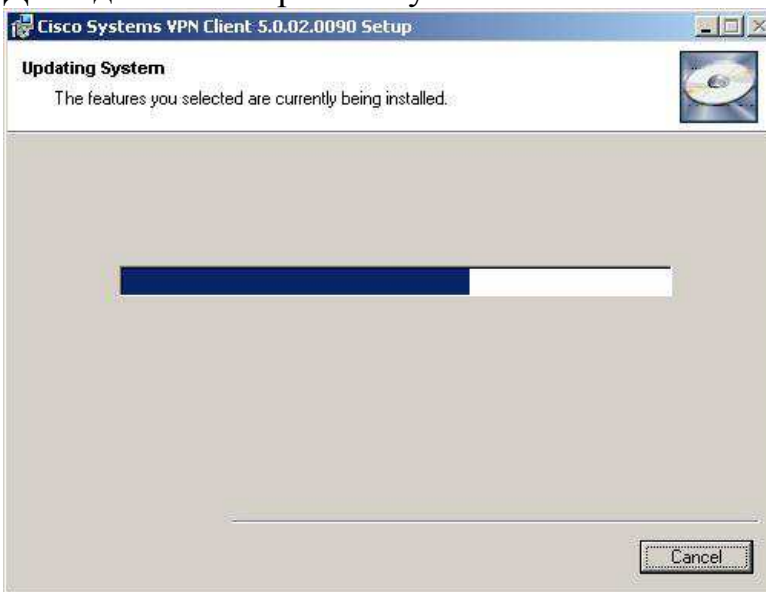
Выбрать путь для установки программы (по умолчанию C:\Program Files\Cisco Systems\VPN Client) и нажать кнопку «Next»



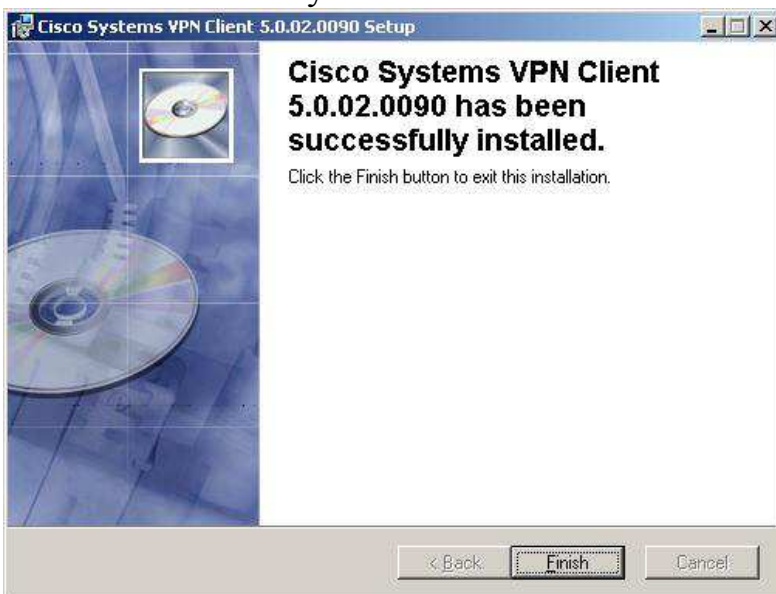
Последняя возможность поправить данные, которые вводились при установке



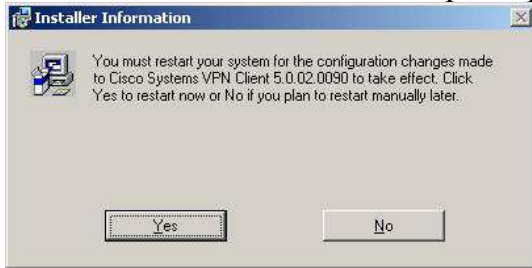
Дожидаемся завершения установки



И нажимаем кнопку «Finish»



После этого необходимо перезагрузить операционную систему, нажав кнопку «Yes».

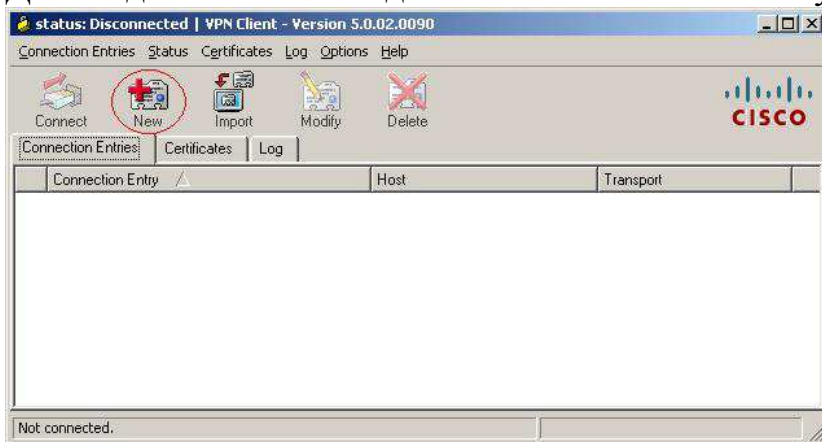


Создание нового подключения

После перезагрузки системы нужно найти на рабочем столе (или в меню «Start -> Programs -> Cisco Systems VPN Client -> VPN Client») ярлык «VPN Client» и запустить программу.



Для создания нового подключения нажмите кнопку «New»



В поле «Connection Entry» - введите имя вашего подключения (например РТС)

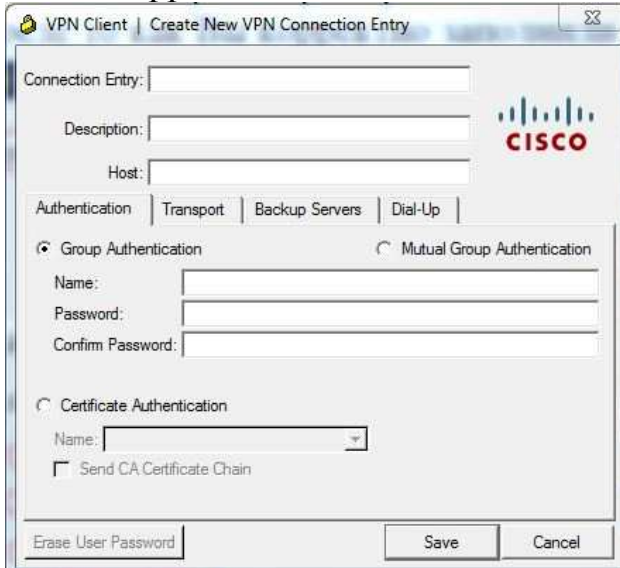
В поле «Host» - IP адрес VPN шлюза на стороне РТС, присланный Вам в письме

В поле «Name» - групповой логин, присланный Вам в письме

В полях «Password» и «Confirm Password» - групповой пароль, присланный Вам в письме.

Соблюдение регистра строго обязательно.

После корректного заполнения всех полей, нажимаете кнопку «Save».



VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

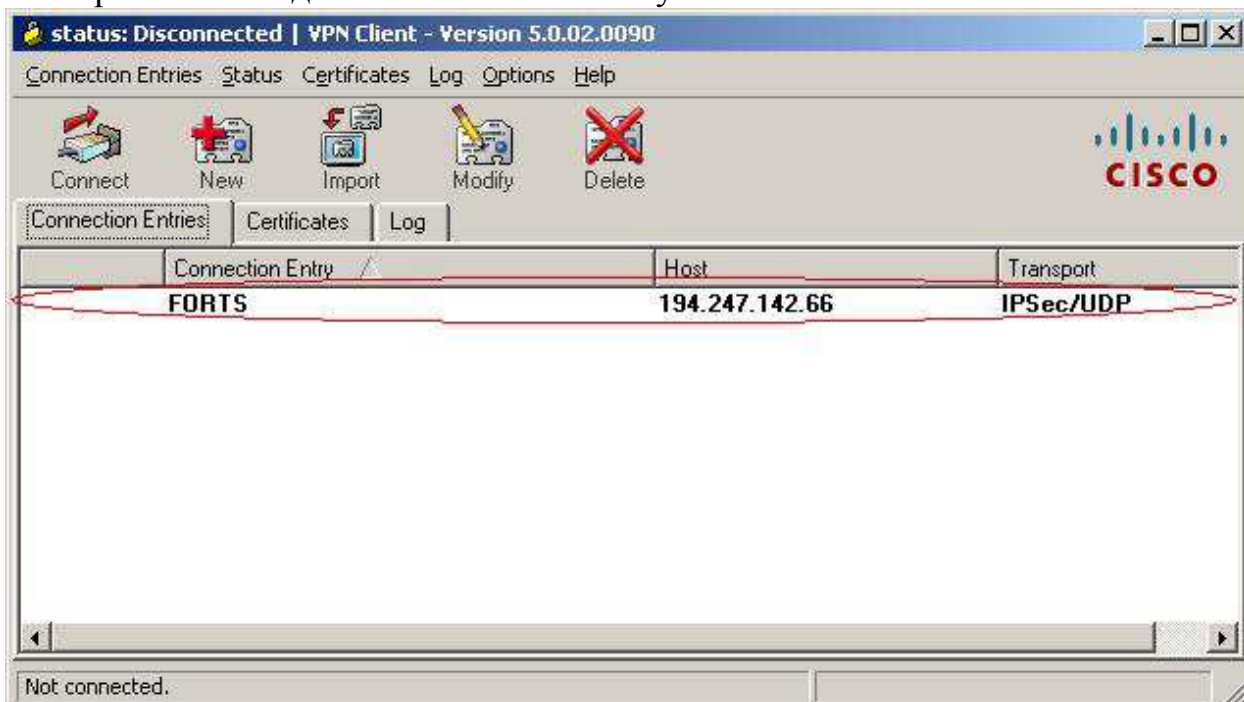
Name:

Send CA Certificate Chain

Erase User Password Save Cancel

В главном окне программы появляется строчка с заданным Вами «Connection Entries».

Выбираем это соединение и ждем кнопку «Connect»



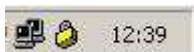
Вторичная авторизация

После прохождения первичной авторизации под групповым аккаунтом, VPN клиент попросит ввести Ваш личный Логин (поле Username) и Пароль (поле Password), посланный Вам в письме с настройками.



При повторном подключении появится возможность для сохранения пароля.

Результатом нормально установившегося соединения является пиктограмма Cisco VPN Client в трее около часов, при наведении на пиктограмму появляется надпись «VPN Client – Connected»



При нажатии правой кнопкой мыши на пиктограмме можно увидеть пункт меню «Statistics», войдя в которую, можно увидеть статистику VPN соединения.

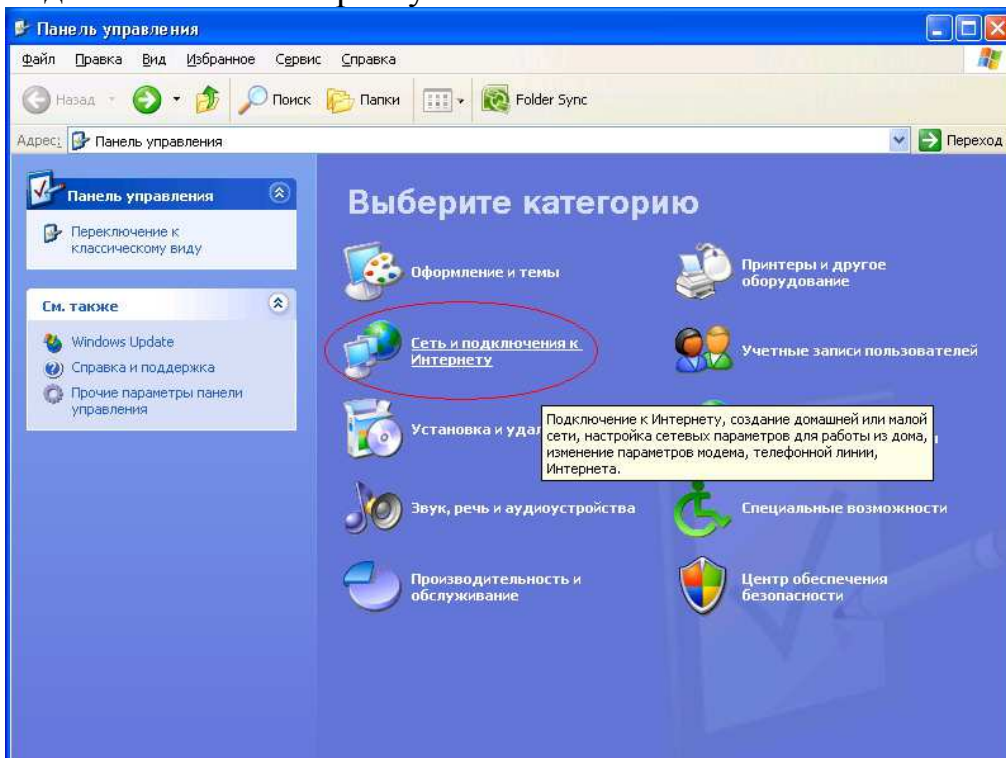
При нормальной работе VPN клиента в статистике его работы можно увидеть количество пакетов уходящих (Encrypted) и входящих (Decrypted) через крипто-туннель.



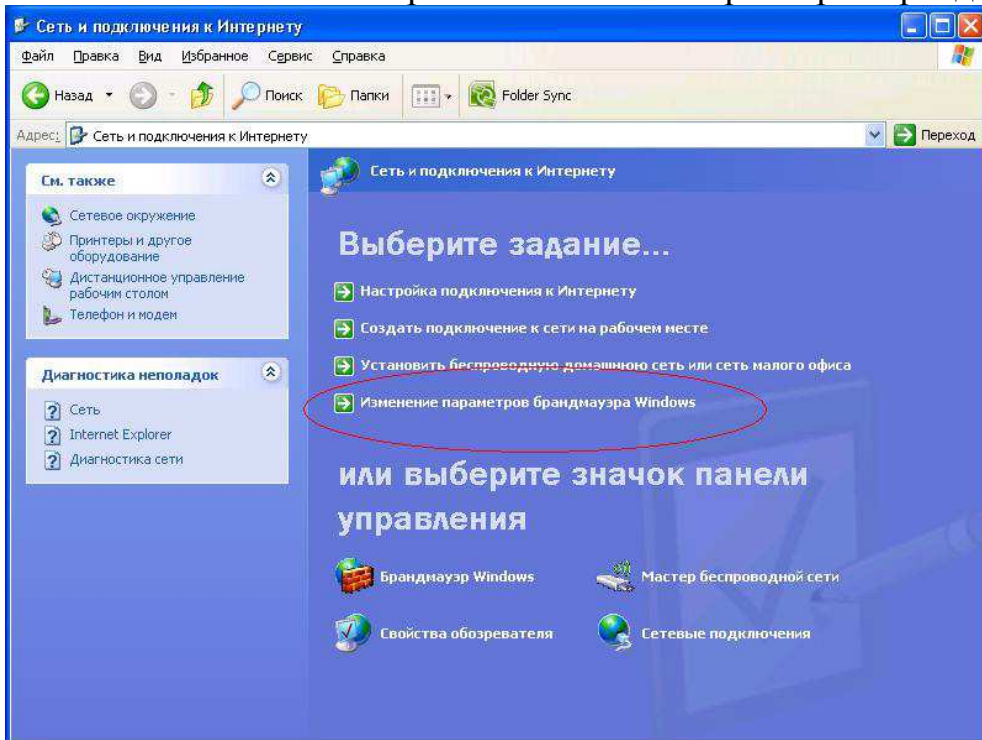
Отключение Брандмауэра в Windows XP

Для исключения ошибок в работе VPN клиента, на стадии настройки, желательно отключить брандмауэр (встроенный Firewall).

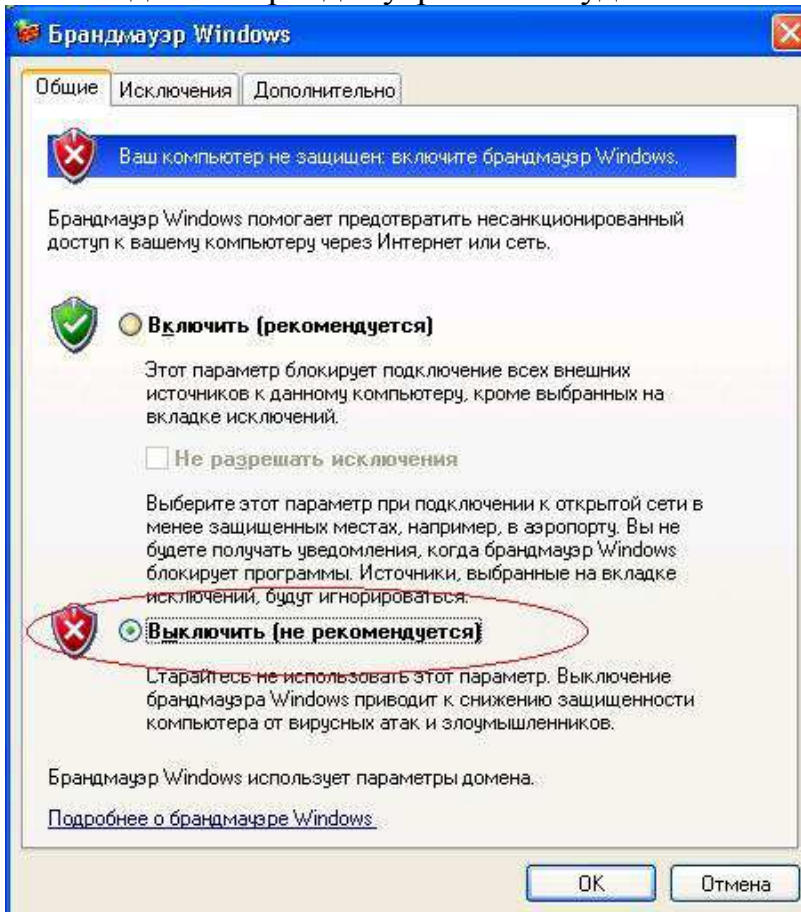
Для этого в панели управления (Start -> Settings -> Control Panel) выбрать «Сеть и подключение к Интернету»



В появившемся окне выбрать «Изменение параметров брандмауэра Windows»



Поставить отметку на пункте «Выключить» и нажать кнопку «ОК»
В последствии брандмауэр можно будет включить и настроить.



Что делать если VPN клиент не соединяется.

1. Проверить настройки VPN клиента, которые Вы вносили при создании нового подключения. Name и Password не должны содержать русских букв и пробелов. Адрес Host должен соответствовать указанному в письме.
2. Проверить правильность настройки Firewall`а, он должен пропускать порты UDP 500 и 4500 в обе стороны. Желательно открыть на Firewall`е ICMP для проверки доступности VPN шлюза через Интернет.
3. Отключить брандмауэр Windows (в случае использования Windows XP).
4. Для проверки работоспособности связки «операционная система – VPN клиент» можно предоставить компьютеру внешний IP адрес, тем самым ФИЗИЧЕСКИ исключив Firewall, Proxy и т.п.
5. Некоторые Firewall`ы требуют дополнительной настройки. Дополнительные порты UDP с 62514 по 62524.

Подробнее об этом можно прочитать на сайте Cisco Systems

http://cisco.com/en/US/products/hw/vpndevc/ps2284/products_qanda_item09186a0080094cf4.shtml

Контакты

7(495)899-01-73

Отдел эксплуатации сети net@rts.ru

Отдел информационной безопасности sin@rts.ru