Код ошибки: 800

Описание

Удаленное подключение не было установлено, потому что попытка установить VPN подключения завершилась с ошибкой. Сервер VPN возможно не достижим. Если данное подключение пытается использовать L2TP/IPsec протокол, параметры безопасности необходимые для IPsec согласования возможно указаны не верно.

Причина

Данная ошибка возникает, когда тип VPN установлен в «Автоматически» и подключение не устанавливается ни для одного из типов.

Решение

Если известен тип VPN подключения, который должен быть использован, следует указать его в настройках подключения (открыть свойства VPN подключения – вкладка «Безопасность» – «Тип VPN»).
После указания конкретного типа VPN подключения, попытка подключения будет по-прежнему, завершаться с ошибкой, но будет возвращаться конкретный код ошибки.
Данная ошибка обычно возникает, когда VPN сервер не достижим или подключение устанавливается с ошибкой. Убедитесь в доступности сервера. Запустите командную строку и введите команду – *ping 10.13.0.1*. Убедитесь, что с сервером удачно проходит обмен пакетами. Если используется PPTP протокол, убедитесь что TCP порт 1723 (протокол PPTP) или порт 47 (протокол GRE) не блокируется брандмауэром.

Если используется протокол L2TP, убедитесь что:

1. Введен правильный предварительный ключ (открыть свойства VPN подключения, выбрать вкладку «Безопасность», нажать кнопку «Дополнительные параметры»);
2. Порт UDP 1701 не блокируется брандмауэром.

Если используется протокол IKE, убедитесь что:

1. Порт UDP 500 и UDP 4500 не блокируется брандмауэром;
2. Правильный сертификат компьютера для IKE присутствует на стороне клиента и сервера.

Код ошибки: 609, 633

Описание

609 – указанный тип устройства не существует
633 – подключаемое устройство уже используется или не корректно сконфигурировано

Причина

Указанная ошибка обычно происходит, когда подключаемое устройство (т.н. miniport) не сконфигурировано корректно. Чтобы убедиться в причине, нужно запустить командную строку от имени администратора и выполнить следующую команду:

netcfg.exe –q <miniport>, где miniport

PPTP протокол: MS_PPTP
L2TP протокол: MS_L2TP
SSTP протокол: MS_SSTP
IKEv2 протокол: MS_AGILEVPN

Решение

1. В системе Windows 7 нужно воспользоваться встроенной утилитой диагностики и решения проблем. Для этого в окне, где отображается ошибка подключения нажать кнопку «Диагностика» и следовать дальнейшим инструкциям.
2. В более ранних версиях Windows нужно запустить командную от администратора и выполнить команду:

```
netcfg.exe -e -c p -i <miniport>
netstop rasman
netstart rasman
```

Код ошибки: 732, 734, 812

Описание

732
Не удается произвести согласование протокола управления PPP
734
Соединение по протоколу управления PPP была оборвана
812
Соединение было запрещено политикой сконфигурированной на RAS/VPN сервере. Метод идентификации, который используется сервером для проверки имени пользователя и пароля может не соответствовать методу идентификации, сконфигурированному в настройках подключения.

Причина

Одной из основных причин возникновения данной ошибки, является запрет на использование протоколов идентификации отличного от MS-CHAP на сервере VPN (или RADIUS сервере). Данный протокол по соображениям безопасности был удален из Microsoft Windows Vista и более поздних версиях Windows. По этой причине соединение не может быть установлено.
Ошибка 812 возникает, когда протокол идентификации задан через NPS (Network Policy and Access Services), в противном случае возникает ошибка 732/734.
Системное событие с кодом 20276 регистрируется в системе, когда настроенный протокол идентификации в службе маршрутизации и удаленного доступа (RRAS) на VPN сервере не соответствует с протоколом, который используется на клиентском компьютере.

Решение

Настройте более безопасный прокол идентификации, например MS-CHAPv2 или EAP на сервере, который будет соответствовать с выбранным протоколом на клиентском компьютере.

Код ошибки: 806

Описание

Соединение VPN между клиентским компьютером и сервером VPN не может быть установлено. Наиболее распространенной причиной данной ошибки, является то, что протокол GRE запрещен, по крайней мере, на одном из устройств (маршрутизаторе) на пути следования пакета между клиентским компьютером и VPN сервером. Если ошибка происходит повторно нужно обратиться к сетевому администратору или провайдеру интернета.

Причина

Туннельный протокол PPTP использует протокол GRE (Generic Route Encapsulation) для того, чтобы инкапсулировать полезную нагрузку в безопасном режиме. Данная ошибка обычно возникает, когда некоторые брандмауэры или сетевые устройства на пути следования пакетов между клиентом и сервером блокируют GRE протокол (т.н. IP протокол с номером 47).

Решение

Нужно разрешить протокол GRE в обоих направлениях на брандмауэре и на каждом из устройств на пути следования пакетов между клиентом и VPN сервером. Если это невозможно, нужно организовать SSTP (Secure Socket Tunneling Protocol) на основе VPN туннеля на VPN сервере и клиенте. Это позволит установить VPN подключение через брандмауэр, прокси-сервер или NAT.

Код ошибки: 789, 835

Описание

789
Соединение L2TP не может быть установлено из-за ошибки, произошедшей на уровне безопасности во время согласований с удаленным компьютером.
835
Соединение L2TP не может быть установлено, потому что на уровне безопасности не удалось проверить подлинность удаленного компьютера. Это может возникать из-за того, что одно или более полей сертификата представленное удаленным сервером не может быть проверено как принадлежащее цели назначения.

Причина

Данная ошибка является общей и возникает, когда согласование IPSec заканчивается неудачей для L2TP/IPSec соединений. Возможные причины:

1. Клиент, использующий протокол L2TP для VPN подключения находится за сервером NAT;
2. Не правильный сертификат или предварительный ключ, который задан в настройках подключения;
3. Сертификат клиентского компьютера или корневой сертификат клиента отсутствует на VPN сервере;
4. Сертификат клиентского компьютера на VPN сервере не имеет «Server Authentication» (EKU) в расширении сертификата.

Решение

Убедитесь, что на стороне клиента и сервера используется правильный сертификат. В случае, если используется предварительный ключ, убедитесь в его правильном значении.

Код ошибки: 766

Описание

Сертификат не может быть найден. Подключение, которое использует L2TP протокол через IPSec, требует установки сертификата для компьютера.

Причина

Данная ошибка обычно происходит, когда нет правильного сертификата компьютера на компьютере клиента.

Решение

Нужно убедиться, что правильный сертификат компьютера для L2TP установлен на компьютере клиента.

Код ошибки: 691

Описание

Удаленное подключение было отклонено, потому что комбинация имени и пароля не принята или выбранный протокол идентификации не разрешен на сервере.

Причина

Данная ошибка происходит, когда фаза идентификации завершается с ошибкой из-за неверных данных.

Решение

1. Проверить правильность имени пользователя и пароля.
2. Проверить выключена ли кнопка CapsLock при вводе имения пользователя и пароля.
3. Выбрать правильный протокол идентификации, который разрешен на сервере.

Код ошибки: 809

Описание

Сетевое подключение не может быть установлено между компьютеров клиента и VPN сервером, потому что сервер VPN не отвечает на запрос.

Причина

Данная ошибка часто возникает, когда брандмауэр или промежуточный маршрутизатор между клиентом и сервером блокирует порты, которые требуются для организации VPN туннеля:

- Протокол PPTP: 1723 (TCP)
- Протокол L2TP или IKEv2: 500 (UDP) и 4500 (UDP)

Решение

Разрешить требуемые порты на брандмауэре или маршрутизаторе. Если это невозможно, нужно организовать SSTP (Secure Socket Tunneling Protocol) на основе VPN туннеля на VPN сервере и клиенте. Это позволит установить VPN подключение через брандмауэр, прокси-сервер или NAT.

Код ошибки: 13806

Описание

Не найден правильный сертификат компьютера, который требуется для протокола IKE (Internet Key Exchange). Обратитесь к вашему администратору для установки правильного сертификата в хранилище сертификатов.

Причина

Данная ошибка обычно происходит, когда сертификат компьютера отсутствует или отсутствует корневой сертификат компьютера на VPN сервере.

Решение

Обратитесь к администратору для решения данной проблемы.

Код ошибки: 13801

Описание

Данные использованные при идентификации по протоколу IKE были неправильными.

Причина

Данная ошибка возникает обычно в следующих случаях:

1. Сертификат компьютера, который используется для проверки подлинности по протоколу IKEv2 на RAS сервере, не имеет «Server Authentication» в расширении;
2. Истек срок действия сертификата компьютера на RAS сервере;
3. Корневой сертификат, который используется для проверки подлинности сертификата RAS сервера, отсутствует на стороне клиента;
4. Имя VPN сервера полученное от клиента не соответствует значению в поле «subjectName» сертифіката сервера.

Решение

Обратитесь к администратору для решения данной проблемы.