

Использование VPN с базовой станцией Cisco Aironet

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Установите VPN](#)

[IP-безопасность](#)

[Отрегулируйте MTU](#)

[Дополнительные сведения](#)

Введение

Базовые станции Cisco Aironet (BSM и модели BSE) предоставляют домашним пользователям и малым офисам с возможностью беспроводного подключения к интранет или Интернету. Модель базовой станции Ethernet (BSE) (BSE), с портом RJ-45 Ethernet, может подсоединяться к интернету через цифровую абонентскую линию (DSL) или кабельный модем. Модель модема базовой станции (BSM) оборудована интегрированным модемом коммутируемой линии передачи v.90 56k, который позволяет нескольким компьютерам подсоединяться к интернету через традиционную телефонную систему.

Типичное использование Устройства Базовая Станция должно обратиться к Интернету или по кабелю или по подключению DSL в сочетании с технологией Virtual Private Networking (VPN) для обеспечения быстрого и безопасного доступа к сети компании.

Базовую станцию легко настроить с помощью Base Station Client Utility (BSCU). Этот документ показывает, как установить модуль для использования с VPN.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- Работа сети VPN
- Конфигурация базовой станции

Используемые компоненты

Сведения в этом документе основываются на Базовой станции Cisco Aironet (BSM и модели BSE).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Установите VPN

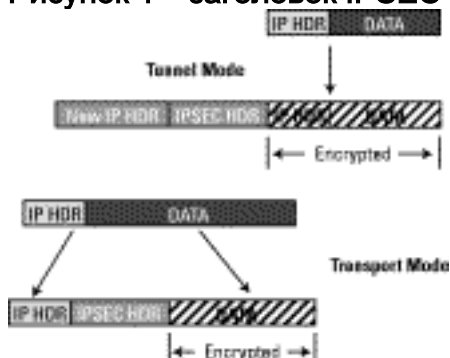
IP-безопасность

Первый шаг в Настройках VPN должен принять для использования IP-безопасности (IPSec) технологию, которая включена в технологии VPN. IPSec использует технологию шифрования для обеспечения конфиденциальности данных, целостности и подлинности между взаимодействующими одноранговыми узлами в частной сети.

IPSec определяет новый набор заголовков, которые добавлены к датаграммам IP. Эти заголовки размещены после IP - заголовка и перед протоколом Уровня 4 (как правило, Протокол управления передачей [TCP] или Протокол датаграммы пользователя [UDP]). Результат состоит в том, что пакеты идут от локальной сети, где ПК установлен через к Интернету. Эти пакеты являются большим размером, чем незашифрованные пакеты. Увеличение размера может вызвать проблемы к устройствам, которые ожидают пакеты нормального размера, потому что принимающие устройства рассматривают их как пакеты с превышением размера.

Рисунок 1 показывает, как Заголовок IPSEC соответствует в стандартном пакете.

Рисунок 1 – заголовок IPSEC



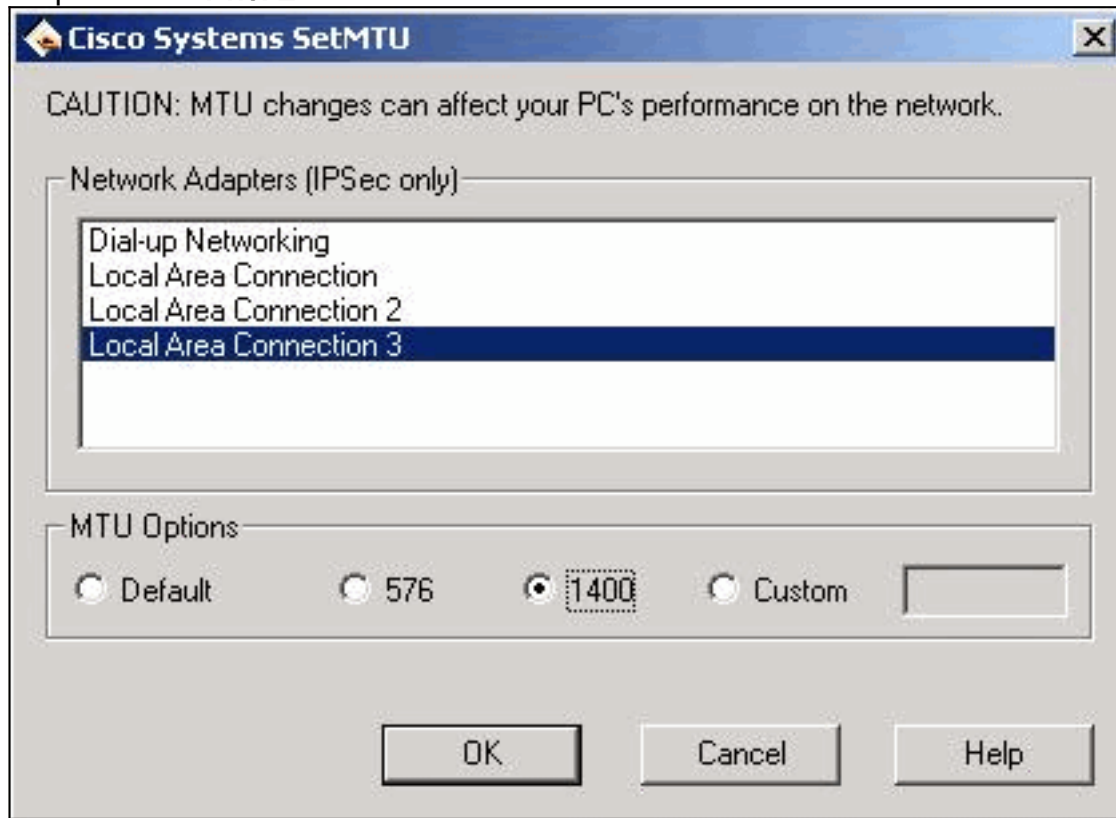
Отрегулируйте MTU

Чтобы убедиться, что принимающие устройства не воспринимают пакеты как слишком большие, необходимо отрегулировать значение максимального размера передаваемого блока банных (MTU) на стороне PC/host. Отрегулируйте общий максимальный размер, который может взять пакет так, чтобы это не превышало нормальный размер

зашифрованного Пакета Ethernet non. Приложения VPN, как правило, предоставляют возможность настраивать максимальный размер передаваемого блока данных.

Выполните эти шаги для регулировки MTU в клиенте VPN Cisco Systems в Microsoft Windows:

1. Выберите **Start> Programs> Cisco Systems VPN Client> Set MTU**. Это окно открывается:**Рис. 2**



2. Выберите беспроводной клиентский адаптер, который вы используете для соединения с Устройством Базовая Станция (в примере, показанном на рисунке 2, Подключение по локальной сети 3).
3. Под **Параметрами MTU** нажмите кнопку с зависимой фиксацией **1400** года, и затем нажмите **ОК**. Это заставляет ваш ПК передавать пакеты с 1400 байтами как максимум. Поэтому дополнительный Заголовок IPSEC принят, но не превышен 1518-байтовый стандартный максимальный размер Пакета Ethernet.

Примечание: Оператор, что "изменения MTU могут влиять на производительность вашего ПК в сети", обращается к факту, что из-за меньшего максимального размера передаваемого блока данных, два пакета требуются, чтобы передать данные, ранее содержащиеся в одиночном незашифрованном кадре.

Для получения дополнительной информации о том, как настроить ваше Устройство Базовая Станция для PPP over Ethernet (PPPoE) и Кабель/DSL, обратитесь к [Настройке Базовые станции BSM342 и BSE342](#).

Примечание: Протокол PPTP не поддерживается

Примечание: Установите беспроводную карту, *прежде чем* будет установлен клиент VPN. Если необходимо удалите обоих, то повторно установите карту, придерживавшуюся VPN. Несмотря на то, что это было проблемой в выпуске Cisco 2.x клиента VPN, он был исправлен в более поздних пересмотрах.

Дополнительные сведения

- [Настройка базовых станций BSE342 и BSM342](#)
- [Технические примечания Cisco Aironet серии 340](#)
- [Техническая поддержка - Cisco Systems](#)