Настройка Cisco VPN 3000 Concentrator с Microsoft RADIUS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Установите и настройте сервер RADIUS на Windows 2000 и Windows 2003
Установите сервер RADIUS
Настройте сервер Microsoft Windows 2000 с IAS
Настройте Microsoft Windows 2003 Server с IAS
Настройте Cisco VPN 3000 Concentrator для проверки подлинности RADIUS
Проверка
Устранение неполадок
Сбои аутентификации WebVPN
Сбои проверки подлинности пользователя против Active Directory
Дополнительные сведения

Введение

Сервер аутентификации Microsoft Internet Authentication Server (IAS) и Microsoft Commercial Internet System (MCIS 2.0) в настоящее время доступен. Сервер Microsoft RADIUS удобен, потому что он использует Active Directory на Primary Domain Controller для его базы данных пользователей. Вы больше не должны поддерживать отдельную базу данных. Это также поддерживает 40-разрядное и 128-разрядное шифрование для VPN-подключений Протокола PPTP. См. контрольный список Microsoft: IAS Настройки для модемной связи и документации доступа к VPN для получения дополнительной информации.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Установите и настройте сервер RADIUS на Windows 2000 и Windows 2003

Установите сервер RADIUS

Если вы не имеете сервера RADIUS (IAS) уже установленный, выполняете эти шаги для установки. Если вам уже установили сервер RADIUS, продолжаете к действиям настройки.

1. Вставьте компакт-диск Windows Server и запустите программу установки.
2. Нажмите **Install Add-On Components**, и затем нажмите **Add/Remove Windows Components**.
3. В Компонентах нажмите **Networking Services** (но не выбирайте или снимайте флажок), и затем нажмите **Details**.
4. Проверьте **интернет-Сервис проверки подлинности** и нажмите **OK**.
5. **Нажмите кнопку Next.**

Настройте сервер Microsoft Windows 2000 с IAS

Выполните эти шаги для настройки сервера RADIUS (IAS) и запустить сервис для предоставления доступа к нему доступным для аутентификации пользователей на Концентраторе VPN.

1. Выберите **Start> Programs> Administrative Tools> Internet Authentication Service**.
2. Щелкните правой кнопкой мыши **интернет-Сервис проверки подлинности** и нажмите **Properties** от подменю, которое появляется.
3. Перейдите к вкладке RADIUS для исследования параметров настройки на порты.Если ваша Проверка подлинности RADIUS и Протокол передачи дэйтаграмм пользователя учета RADIUS (UDP) вводят ваши параметры порта, порты отличаются от предоставленных значений по умолчанию (1812 и 1645 для аутентификации, 1813 и 1646 для учета) на Аутентификации и Учете. **Закончив все действия, нажмите кнопку OK.Примечание:** Не изменяйте порты по умолчанию. Разделите порты при помощи запятых для использования параметров настройки множественных портов для аутентификации или бухгалтерских запросов.
4. Щелкните правой кнопкой мыши **Клиентов** и выберите **New Client** для добавления Концентратора VPN как клиент аутентификации, авторизации и учета (AAA) к серверу RADIUS (IAS).**Примечание:** Если резервирование настроено между двумя Cisco VPN 3000 Concentrator, резервный Cisco VPN 3000 Concentrator должен также быть добавлен к серверу RADIUS как Клиент RADIUS.
5. Введите дружественное имя и выберите как **Протокол RADIUS**.
6. Определите Концентратор VPN с IP-адресом или именем DNS на следующем окне.
7. Выберите **Cisco** из полосы прокрутки Клиента - поставщика.
8. Введите общий секретный ключ.**Примечание:** Необходимо помнить *точную* тайну,

которую вы используете. Вам нужна эта информация для настройки Концентратора VPN.

9. **Нажмите кнопку Finish.**
10. Дважды нажмите **Remote Access Policies** и дважды нажмите политику, которая появляется в правой части окна.**Примечание:** После установки IAS политика удаленного доступа должна уже существовать.В Windows 2000 авторизацию предоставляют на основе свойств наборного (телефонный) доступа политики удаленного доступа и учетной записи пользователя. Политика удаленного доступа является рядом условий и настроек соединения, которые дают администраторам сети большую гибкость в авторизации попыток подключения. Сервис маршрутизации Windows 2000 и Служба удаленного доступа и IAS Windows 2000 обе политики удаленного доступа использования, чтобы определить, принять ли или отклонить попытки подключения. В обоих случаях политика удаленного доступа сохранена локально. См. документацию IAS Windows 2000 для получения дополнительной информации о том, как обработаны попытки подключения.
11. Выберите **дают разрешение удаленного доступа** и нажимают **Edit Profile** для настройки свойств наборного (телефонный) доступа.
12. Выберите протокол для использования для аутентификации на вкладке Authentication. Проверьте **версию 2 Microsoft Encrypted Authentication** и снимите флажок со всеми другими протоколами аутентификации.**Примечание:** Параметры настройки в этом Профиле Наборного (телефонный) доступа должны совпасть с параметрами настройки в конфигурации VPN 3000 Concentrator и Клиенте с наборным (телефонным) доступом. На аутентификации MSCHAPv2 данного примера без шифрования PPTP используется.
13. На вкладке Encryption не проверяют **Шифрования** только.
14. Нажмите **OK** для закрытия профиля Наборного (телефонный) доступа, затем нажмите **OK** для закрытия окна политики удаленного доступа.
15. Щелкните правой кнопкой мыши **интернет-Сервис проверки подлинности** и нажмите **Start Service** в дереве консоли.**Примечание:** Можно также использовать эту функцию для остановки сервиса.
16. Выполните эти шаги для изменения пользователей для разрешения соединения.Выберите **Console> Add/Remove Snap-in**.**Нажмите Add** и выберите **Local Users и моментальный снимок Groups - в**.**Нажмите Add.**Удостоверьтесь, что выбрали **Local Computer**Нажмите **Finish** и **OK**.
17. **Разверните Local User and Groups и щелкните папку Users в левой панели.** В правой панели дважды нажмите пользователя (Пользователь VPN), вы хотите предоставить доступ.
18. Перейдите к Вкладке наборный (телефонный) доступ и выберите **Allow Access** в соответствии с Разрешениями Удаленного доступа (Наборный (телефонный) доступ или VPN).
19. Нажмите **Apply** и **OK** для завершения действия. Можно закрыть Консольное Окно управления и сохранить сеанс при желании.Пользователи, которых вы модифицировали, теперь в состоянии обратиться к Концентратору VPN с Клиентом VPN. Следует иметь в виду, что сервер IAS только аутентифицирует сведения о пользователе. Концентратор VPN все еще делает групповую аутентификацию.

Настройте Microsoft Windows 2003 Server с IAS

Чтобы настроить Microsoft Windows 2003 server с IAS, выполните следующие действия.

Примечание: Эти шаги предполагают, что IAS уже установлен на локальном компьютере. В противном случае добавьте это через **Панель управления> Добавления/удаления программы**.

1. **Выберите Administrative Tools > Internet Authentication Service и нажмите правой кнопкой мыши RADIUS Client, чтобы добавить нового клиента RADIUS. После ввода данных нажмите OK.**
2. Введите дружественное имя.
3. Определите Концентратор VPN с IP-адресом или именем DNS на следующем окне.
4. Выберите **Cisco** из полосы прокрутки Клиента - поставщика.
5. Введите общий секретный ключ.**Примечание:** Необходимо помнить *точную* тайну, которую вы используете. Вам нужна эта информация для настройки Концентратора VPN.
6. **Нажмите OK для завершения.**
7. Перейдите **к Политике Удаленного доступа**, щелкните правой кнопкой мыши на **Соединениях с Другими Серверами доступа** и выберите **Properties**.
8. Выберите **дают разрешение удаленного доступа** и нажимают **Edit Profile** для настройки свойств Dial-In.
9. Выберите протокол для использования для аутентификации на вкладке Authentication. Проверьте **версию 2 Microsoft Encrypted Authentication** и снимите флажок со всеми другими протоколами аутентификации.**Примечание:** Параметры настройки в этом Профиле Наборного (телефонный) доступа должны совпасть с параметрами настройки в конфигурации VPN 3000 Concentrator и Клиенте с наборным (телефонным) доступом. На аутентификации MSCHAPv2 данного примера без шифрования PPTP используется.
10. На вкладке Encryption не проверяют **Шифрования** только.
11. **Закончив все действия, нажмите кнопку OK.**
12. Щелкните правой кнопкой мыши **интернет-Сервис проверки подлинности** и нажмите **Start Service** в дереве консоли.**Примечание:** Можно также использовать эту функцию для остановки сервиса.
13. Выберите **Administrative Tools> Computer Management> System Tools> Local Users и Groups**, щелкните правой кнопкой мыши на **Пользователях** и выберите **New Users** для добавления пользователя в учетную запись локального компьютера.
14. Добавьте пользователя с Паролем Cisco "vpnpassword" и проверьте эти данные профиля.**Убедитесь, что на вкладке General выбран параметр Password Never Expired вместо параметра User Must Change Password.**На Вкладке наборный (телефонный) доступ выберите, опция для **Предоставляют доступ** (или настройка по умолчанию выхода доступа Контроля через Политику Удаленного доступа).**Закончив все действия, нажмите кнопку OK.**

Настройте Cisco VPN 3000 Concentrator для проверки подлинности RADIUS

Выполните эти шаги для настройки Cisco VPN 3000 Concentrator для Проверки подлинности RADIUS.

1. Соединитесь с Концентратором VPN с вашим Web-браузером и выберите

Configuration> System> Servers> Authentication из левого кадрового меню.
2. **Нажмите Add** и настройте эти параметры настройки.Тип сервера = RADIUSСервер проверки подлинности = IP-адрес или имя хоста вашего сервера RADIUS (IAS)Порт сервера = 0 (0=default=1645)Секретный сервер = то же как в шаге 8 в раздел по Настраивает сервер RADIUS
3. **Нажмите Add** для добавления изменений к рабочей конфигурации.
4. **Нажмите Add**, выберите **Internal Server for Server Type** и нажмите **Apply**.Вам нужно это позже для настройки Группы IPSec (Вам нужен только Тип сервера = Внутренний сервер).
5. Настройте Концентратор VPN для пользователей PPTP или для Пользователей VPN-клиента.**PPTP**Выполните эти шаги для настройки для пользователей PPTP.Выберите **Configuration> User Management> Base Group** и нажмите вкладку **PPTP/L2TP**.Выберите **MSCHAPv2** и снимите флажок с другими протоколами аутентификации в разделе Протоколов Аутентификации PPTP.Нажмите **Apply** внизу страницы для добавления изменений к рабочей конфигурации.Теперь, когда пользователи PPTP соединяются, они аутентифицируются сервером RADIUS (IAS).**VPN-клиент**Выполните эти шаги для настройки для Пользователей VPN-клиента.**Choose Configuration> User Management> Groups** и **нажмите Add** для добавления новой группы.Введите имя группы (например, IPsecUsers) и пароль.Этот пароль используется в качестве предварительного общего ключа для согласования туннеля.Перейдите к вкладке IPSec и установите Аутентификацию в **RADIUS**.Это позволяет Клиентам IPSEC аутентифицироваться через Сервер проверки подлинности RADIUS.**Нажмите Add** внизу страницы для добавления изменений к рабочей конфигурации.Теперь, когда Клиенты IPSEC подключают и используют группу, вы настроили, они аутентифицируются сервером RADIUS.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Сбои аутентификации WebVPN

В последующих подразделах описан процесс устранения неполадок конфигурации.

- **Проблема:** Пользователи WebVPN не в состоянии аутентифицироваться против сервера RADIUS, но могут аутентифицироваться успешно с локальной базой данных Концентратора VPN. Они получают ошибки, такие как "Вход в систему, подведенный" и это сообщение.**Причина**: Когда любая база данных кроме внутренней базы данных Концентратора используется, эти типы проблем часто происходят. Пользователи WebVPN поражают Базовую группу, когда они сначала соединяются с Концентратором и должны использовать метод проверки подлинности по умолчанию. Часто этот метод установлен во внутреннюю базу данных Концентратора и не является настроенным RADIUS или другим сервером.**Решение:** Когда пользователь WebVPN аутентифицируется, Концентратор проверяет список серверов, определенных при **Configuration> System> Servers> Authentication**, и использует лучший. Удостоверьтесь,

что переместили сервер, с которым вы хотите, чтобы пользователи WebVPN аутентифицировались на вершине этого списка. Например, если RADIUS должен быть методом аутентификации, необходимо переместить сервер RADIUS в вершину списка для продвижения аутентификации к нему.**Примечание:** Просто, потому что пользователи WebVPN первоначально совершают нападки, Базовая группа не означает, что они ограничены Базовой группой. Дополнительные группы WebVPN могут быть настроены на Концентраторе, и пользователей может назначить на них сервер RADIUS с населением атрибута 25 с ***OU=groupname***. См. Блокировку Пользователей в Группу концентратора VPN 3000 Использование сервера RADIUS для большего количества подробного объяснения.

Сбои проверки подлинности пользователя против Active Directory

В Сервере Active Directory, на вкладке Account Свойств пользователя отказывающего пользователя, вы видите этот флажок:

[x] Не требуйте процедур, предшествующих аутентификации

Если флажок не установлен, установите его и повторите аутентификацию пользователя заново.

Дополнительные сведения

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Client
- Согласование IPsec/Протоколы IKE
- Страница технической поддержки RADIUS (Служба Проверки Подлинности Удаленного Наборного Телефонного Доступа Пользователя)
- Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)
- Cisco Systems – техническая поддержка и документация