

ESMART Token Защищенное VPN-соединение

на примере Microsoft Windows Server 2003 и клиента Windows 7 Professional



Содержание

1.	Установка VPN-соединений по сертификату	3
1.1	Требования к клиентским компьютерам	3
1.2	Требования к оборудованию VPN-сервера	3
1.3	Требования к программному обеспечению VPN-сервера	3
2.	Подготовительные этапы	3
2.1	Установка центра сертификации	3
2.2	Выдача клиентских сертификатов	4
3.	Настройка VPN-сервера	4
3.1	Настройка политик удаленного доступа	4
4.	Настройка VPN-клиента	6



1. Установка VPN-соединений по сертификату

При настройке удаленного VPN-доступа к сетевым ресурсам нежелательно использовать параметры учетной записи, защищенной только паролем. Двухфакторная авторизация по смарт-карте является более защищенным вариантом. Требование предоставить смарт-карту с соответствующим сертификатом и ввести ПИН-код значительно уменьшает вероятность несанкционированного доступа к сети организации.

VPN обеспечивает безопасность благодаря защищенному туннельному подключению и шифрованию данных. Доступ к корпоративной сети предоставляется только пользователям, предоставившим верный сертификат на смарт-карте или USB-ключе и ПИН-код, подбор которого не возможен.

1.1 Требования к клиентским компьютерам

Для работы со смарт-картами требуется OC Windows не ниже XP SP2. На каждом клиентском компьютере должен быть установлен криптопровайдер ESMART Token CSP. При использовании Windows XP также требуется установка пакета Microsoft Base CSP. Установка подробно описана в руководстве **ESMART Token - CSP**.

На клиентском ПК должен быть установлен драйвер для считывателя смарт-карт или драйвер USBключа ESMART Token.

1.2 Требования к оборудованию VPN-сервера

VPN-подключения увеличивают загрузку процессора на сервере удаленного доступа. Вход в систему с помощью смарт-карты или USB-ключа не вносит существенного вклада в эту загрузку. VPN-сервера удаленного доступа, обслуживающие большой объем входящих подключений, требуют использования быстрых процессоров (желательно в многопроцессорной конфигурации), а также поддержки высокой пропускной способности сети.

1.3 Требования к программному обеспечению VPN-сервера

Требования к программному обеспечению VPN-сервера для доступа на основе смарт-карт довольно просты. На серверах удаленного доступа может использоваться ОС Windows 2003 Server или более поздняя версия с включенной поддержкой маршрутизации и удаленного доступа и поддержкой EAP-TLS.

EAP-TLS представляет собой механизм взаимной проверки подлинности, разработанный для использования совместно с устройствами безопасности, например смарт-картами. EAP-TLS поддерживает подключения по протоколу PPP (Point-to-Point Protocol) и VPN и позволяет обмениваться общими секретными ключами для MPPE в дополнение к IPsec.

Основными преимуществами EAP-TLS являются устойчивость к атакам методом прямого подбора паролей и поддержка взаимной проверки подлинности. При взаимной проверке подлинности и клиент, и сервер должны подтвердить друг другу свои учетные данные. Если клиент или сервер не отправят сертификат для проверки своих учетных данных, подключение будет прервано.

Microsoft Windows Server 2003 и выше поддерживает EAP-TLS для коммутируемых и VPN-подключений, что позволяет удаленным пользователям использовать смарт-карты.

2. Подготовительные этапы

2.1 Установка центра сертификации

Установка и настройка корпоративного центра сертификации описана в руководствах по развертыванию центра сертификации Windows Server 2003 и Windows Server 2008.



2.2 Выдача клиентских сертификатов

Процедура выдачи клиентских сертификатов и записи сертификатов на смарт-карту или USB-ключ описана в руководствах по развертыванию центра сертификации Windows Server 2003 и Windows Server 2008 и выше.

3. Настройка VPN-сервера

Добавьте оснастку Маршрутизация и удаленный доступ.

В контекстном меню сервера выберите Свойства, перейдите на вкладку Безопасность.

Выберите пункт Методы проверки подлинности.

Установите флажок Протокол расширенной проверки подлинности (ЕАР) и нажмите кнопку ОК.



3.1 Настройка политик удаленного доступа

В оснастке **Маршрутизация и удаленный доступ** выберите **Политики удаленного доступа** > **Подключения к серверу маршрутизации и удаленного доступа.**

Нажмите Изменить профиль, выберите вкладку Проверка подлинности и нажмите Методы ЕАР.

Если в списке **Типы EAP** не появится элемент **Смарт-карта или иной сертификат**, нажмите кнопку **Добавить**, укажите **Смарт-карта или иной сертификат** и нажмите кнопку **OK**.

Отметьте опцию Предоставить право удаленного доступа.



Консоль Дейстение №и Справка Марирутизация и удаленный доступ Состояние сереера Марирутизация и удаленный доступ Состояние сереера Состояние удаленного доступа Сихазать в праве удаленного доступа Сихазать в праве удаленного доступа Сихазать в праве удаленного доступа	🚊 Маршрутизация и удаленный доступ		
 Сойства: Подключения к серверу маршрутизации и удалени. Состояние сервера ОС (покалью) Киенты удаленного доступа (0) Порты Пенаршрутизация Собще Собще Сотатические маршруты Агент DHCP-ретрансляции Цоменить Ведение журнала удаленного доступа Ведение журнала удаленного доступа Политика удаленного доступа Сополтика управляет досталочение довлетворять запросы на подключение. Добавить Изменить Удалить Ведение журнала удаленного доступа Ведение журнала удаленного доступа Сополтика управляет досталочение удовлетворят условиям, указанным в той политике, то к подключение удовлетворят условиям, указанным в профиль. Изменить профиль Эта политика управляет доступа к сети, если только индивидуальные разрешения на доступ не указываются явно в профиле пользователа. Сли запрос на подключение удовлетворяет указанным условиям: Предеставить право удаленного доступа Тиказать в праве удаленного доступа 	<u>К</u> онсоль <u>Д</u> ействие <u>В</u> ид <u>С</u> правка		
Маршутизация и даленный доступ Состояние сервера DC1 (локально) Кленты удаленный доступа (0) порты P-наршутизация Общие Сатические маршуты д Агент DHCP-ретранслации Добае итв			
	Маршрутизация и удаленный доступ Состояние сервера DC1 (локально) Порты IP-маршрутизация Общие Статические маршруты Areнt DHCP-ретрансляции IGMP Политика удаленного доступа Ведение журнала удаленного доступа	Свойства: Подключения к серверу маршрутизации и удале ? Х Параметры Укажите условия, которым должны удовлетворять запросы на подключение. Условия политики: МS-RAS-Vendor соответствует "^З11\$" Добавить Изменить Удадить Если запросы на подключение удовлетворяют условиям, указанным в этой политике, то к подключению применяется соответствующий профиль. Изменить профиль Эта политика управляет доступом к сети, если только индивидуальные разрешения на доступ не указанным условиям: если запрос на подключение удовлетворяет указанным условиям: © Предоставить право удаленного доступа ОК Отмена Применить	

🚊 Маршрутизация и удаленный доступ		- 🗆 🗵
<u>К</u> онсоль <u>Д</u> ействие <u>В</u> ид <u>С</u> правка		
	Изменение профиля коммутируемых подключений	
Маршрутизация и удаленный доступ Состояние сервера DCI (локально) Клиенты удаленного доступа (0) Порты IP-маршрутизация Политика удаленного доступа Beдение журнала удаленного доступа	Изменение профила конмутируемых подключения IP Многоканальное подключение Ограничения по входящим звонкам Проверка подлинности Шифрование Дополнительно Выбрать поставщиков ЕАР Типы ЕАР согласуются в перечисленном порядке. Ципы ЕАР: Смарт-карта или иной сертификат Вверх Вина Добавить Изменить Удалить ОК Отмена	
	ОК Отмена Применить	

Выберите пункт Смарт-карта или иной сертификат и нажмите кнопку Изменить.



🚊 Маршрутизация и удаленный доступ			
<u>К</u> онсоль <u>Д</u> ействие <u>В</u> ид <u>С</u> правка	<u>Консоль Действие Вид Справка</u>		
$\leftarrow \rightarrow \textcircled{\ } \blacksquare \leftthreetimes \textcircled{\ } \blacksquare \biguplus \textcircled{\ } \Rightarrow + \bullet$	Изменение профиля коммутируемых подключений		
 Даршрутизация и удаленный доступ Состояние сервера С	ІР Многоканальное подключение Ограничения по входящим звонкам Проверка подлинности Шифрование Дополнительно D: Как со целиности Шифрование Дополнительно Выбрать поставщиков ЕАР Сеойства смарт-карты или другого сертификата Зтот сервер должен идентифицировать себя для успешного подключения. Выберите для сервера сертификат как доказательство его подлинности. Сертификат выдан для: dc1. МуСотрану.com Понятное имя: Поставщик: dc1 Срок действия: 31.10.2007 21:11:25 ОК Отмена тмена		
	ОК Отмена Применить		
-			

Укажите сертификат для проверки подлинности ЕАР и подтвердите изменения.

4. Настройка VPN-клиента

Процедура настройки клиентов для проверки подлинности с использованием смарт-карт может отличаться в зависимости от установленной операционной системы. Далее показана настройка VPNсоединения для Windows 7 Professional.

Откройте Панель управления. Выберите **Сеть и Интернет > Центр управления сетями и общим до**ступом. В разделе **Изменение сетевых параметров** выберите **Настройка нового подключения или се***т*и.

🍚 🙅 Установка подключения или сети		
Выберите вариант подключения		
Подключение к Интернету Беспроводное, скоростное или телефонное подключение к Интернету.		
Создание и настройка новой сети Настройка нового маршрутизатора или точки доступа.		
Подключение к рабочему месту Настройка телефонного или VPN-подключения к рабочему месту.		
Кастройка телефонного подключения Подключение к Интернету через телефонную сеть.		
Далее	Отмена	



Выберите Подключение к рабочему месту > Использовать мое подключение к Интернету (VPN).

	- • •
🚱 🔚 Подключение к рабочему месту	
Как выполнить подключение?	
 Использовать мое подключение к Интернету (VPN) Подключение через Интернет с помощью виртуальной частной сети (VPN). 	
🔍 — 🎱 — 🕪	
Использовать прямой набор номера Прямое подключение к телефонному номеру без выхода в Интернет.	
i i i i i i i i i i i i i i i i i i i	
Что такое VPN-подключение?	
	Отмена

Задайте параметры подключения и отметьте Использовать смарт-карту.

🚱 🌆 Подключение к рабоче	🕝 🌆 Подключение к рабочему месту			
Введите Интернета-а	Введите Интернета-адрес для подключения			
Этот адрес можно получит	ъ у сетевого администратора.			
Интернете-адрес:	157.54.0.01]		
Имя местоназначения:	VPN-подключение			
🔽 Использовать смарт-карту				
🌚 🔲 Разрешить использовать это подключение другим пользователям				
Этот параметр позволяет любому пользователю, имеющему доступ к этому компьютеру, использовать это подключение.				
🔲 Не подключаться с	ейчас, только выполнить установку для подключения в	будущем		
	Подключит	гь Отмена		

Выберите в списке созданное подключение и откройте в контекстном меню Свойства.



	Свойства смарт-карты или другого сертификата 🛛 💌
УРN-подключение - свойства Общие Параметры Безопасность Сеть Доступ Тип VPN: L2TP IPsec VPN ▼ Дополнительные параметры Шифрование данных:	При подключении: использовать мою смарт-карту использовать сертификат на этом компьютере Использовать выбор простого сертификата (рек.) Проверять сертификат сервера Подключение к серверам:
Проверка подлинности Протокол расширенной проверки подлинности (EAP) Мicrosoft: Смарт-карта или иной сертификат (шифро Разрешить следующие протоколы Свойства	Доверенные корневые центры сертификации AAA Cettficate Services AC Raíz Ceticámara S.A. AC RAIZ DNIE AC RAIZ FNMT-RCM AC1 RAIZ MTIN ACEDICOM Root
 Незашифрованный пароль (РАР) Протокол проверки пароля (СНАР) Протокол Microsoft СНАР версии 2 (MS-CHAP v2) Использовать автоматически имя входа и пароль Windows (и имя домена, если существует) 	Аслыв Аctalis Authentication CA G1 К Просмотреть сертификат Не запрашивать пользователя авторизовать новые серверы или доверенные Центры Сертификации.
ОК Отмена	Использовать для подключения другое имя пользователя ОК Отмена

При установлении VPN-соединения откроется окно ввода ПИН-кода.



Если смарт-карта не вставлена, соединение не будет установлено:



