

Ответы на часто задаваемые вопросы о модуле NME-RVPN в исполнении MCM

Информация о продукте

В1. Что такое модуль NME-RVPN в исполнении MCM?

О1. Модуль NME-RVPN в исполнении MCM (модуль сетевой модернизированный) представляет собой модуль для маршрутизаторов Cisco ISR первого и второго поколения (Cisco® ISR серий 2800/3800 и Cisco® ISR серий 2900/3900), предназначенный для обеспечения российского рынка сертифицированным VPN-решением.

В2. В чем заключается исполнение MCM модуля NME-RVPN?

О2. Модуль NME-RVPN в исполнении MCM является функциональным аналогом модуля NME-RVPN. Технологический процесс производства модуля в исполнении MCM согласован с ФСБ России. Программное обеспечение (шлюз безопасности) CSP VPN Gate 3.1 при работе на платформе NME-RVPN (MCM) сертифицировано в соответствии с требованиями ФСТЭК и ФСБ России к устройствам криптографической защиты информации.

В3. Для каких маршрутизаторов предназначен модуль NME-RVPN (MCM)?

О3. Модуль NME-RVPN (MCM) можно устанавливать в маршрутизаторы Cisco ISR первого поколения (2811, 2821, 2851, 3825 и 3845) и второго поколения (2911, 2921, 2951, 3925 и 3945) с IOS версии 12.4(11)T или более поздней версии. Модуль может работать с любым функциональным набором IOS, начиная с «IP base». При этом устанавливать какие-либо дополнительные устройства (память и т. п.) в маршрутизатор не требуется.

В4. Сколько модулей NME-RVPN (MCM) можно одновременно установить в маршрутизатор Cisco ISR?

О4. В маршрутизаторы моделей 2811, 2821 2851, 2911 и 2921 может устанавливаться один модуль, моделей 3825, 2951 и 3925 – два, моделей 3845 и 3945 – до четырех модулей одновременно.

В5. Можно ли выполнять обновление ПО модуля и маршрутизатора независимо?

О5. Да, можно. Необходимое условие: операционная система Cisco IOS должна поддерживать данный модуль (IOS версии 12.4(11)T или более поздней версии).

В6. Какова аппаратная архитектура модуля?

О6. Модуль представляет собой вычислительную платформу на базе процессора Intel Celeron-M с тактовой частотой 1,0 ГГц, объем оперативной памяти – 512 Мбайт, емкость карты Compact Flash – 512 Мбайт. На лицевой панели присутствуют порты USB и Ethernet.

В7. Как модуль NME-RVPN (MCM) взаимодействует с IOS маршрутизатора и внешней сетью?

О7. Модуль NME-RVPN (MCM) работает полностью независимо от IOS маршрутизатора, получая от маршрутизатора только питание. Взаимодействие модуля с маршрутизатором осуществляется по сети посредством интерфейса Gigabit Ethernet. Для подключения к внешней сети модуль оборудован внешним интерфейсом Gigabit Ethernet.

В Cisco IOS внутренний интерфейс связи с модулем обозначается как `interface Special-Services-Engine x/0`.

В8. Для чего нужен разъем USB на передней панели модуля NME-RVPN (MCM)?

О8. Разъем USB служит для двух целей.

1. Для организации резервного канала связи благодаря подключению внешних GSM-, CDMA- или WiMAX-модемов. Модуль с программным обеспечением CSP VPN Gate 3.1 поддерживает работу с модемами GSM, CDMA и WiMAX. Модем подключается непосредственно к модулю NME-RVPN. При отказе основного канала происходит автоматическое обнаружение резервного канала и переключение на него. При восстановлении основного канала переключение на него также происходит автоматически.
2. Подключение устройства-носителя ключевого материала. К порту USB может подключаться USB-ключ eToken PRO (32 или 64 К) - средство для защищенного хранения и доставки ключевого материала. Использование eToken позволяет обеспечить более безопасный процесс распространения ключевых пар. Подробное описание процедуры взаимодействия с этими устройствами можно найти в документации на продукт CSP VPN Gate 3.1 на сайте www.s-terra.com.

Сертификация

В9. Каковы особенности производства модуля NME-RVPN (MCM)?

О9. Технологический процесс производства модуля согласован с ФСБ России и определен документом «Порядок организации производства изделия «Модуль Сетевой Модернизированный (MCM)» в рамках подконтрольного технологического процесса на территории Российской Федерации». Изготовление продукта в рамках подконтрольного технологического процесса гарантирует отсутствие в вычислительной среде недокументированных аппаратно-программных элементов.

В10. Может ли модуль NME-RVPN (MCM) использоваться как СКЗИ?

О10. При использовании на модуле программного обеспечения CSP VPN Gate 3.1 этот программно-аппаратный комплекс может использоваться как средство криптографической информации, т. к. СКЗИ CSP VPN Gate 3.1 при работе на платформе NME-RVPN (MCM) имеет сертификат ФСБ России №СФ/114-1411 и сертифицировано по классу защиты КС1.

В11. Какие сертификаты ФСТЭК имеются для модуля NME-RVPN в исполнении MCM при использовании CSP VPN Gate версии 3.1?

О11. Сертификат ФСТЭК России подтверждает для этого продукта оценочный уровень доверия ОУД 3+, соответствие 3 уровню контроля отсутствия недеklarированных возможностей и возможность использования при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1 класса включительно.

В12. Возможно ли использование модуля NME-RVPN в исполнении MCM для защиты персональных данных?

О12. В результате сертификации в ФСТЭК России получен сертификат, разрешающий использование комплекса CSP VPN Gate версии 3.1 на платформе NME-RVPN для защиты персональных данных до 1 класса включительно.

В13. Возможно ли использование модуля NME-RVPN в исполнении MCM в государственных организациях и органах власти Российской Федерации?

О13. Модуль NME-RVPN (MCM) с программным обеспечением CSP VPN Gate 3.1 (шлюз безопасности) сертифицирован в соответствии с требованиями ФСТЭК и ФСБ России к устройствам криптографической защиты информации. Все это позволяет использовать решение в целом (модуль NME-RVPN в исполнении MCM совместно с ПО CSP VPN Gate 3.1) в государственных организациях и органах власти Российской Федерации для передачи сведений, не составляющих государственную тайну.

Возможности программного обеспечения

В14. Какое программное обеспечение используется в модуле?

О14. Модуль NME-RVPN (MCM) работает независимо от IOS маршрутизатора, используя программное обеспечение CSP VPN Gate 3.1 компании «С-Терра СиЭсПи». Это программное обеспечение предустановлено на карте Compact Flash модуля.

В15. Какова производительность модуля?

О15. Производительность при использовании наиболее популярного алгоритма для создания IPsec-туннелей, включающего шифрование с проверкой целостности (ESP+HMAC), составила 40 Мбит/с (измерения производились на больших UDP-пакетах – 1400 байт). Если же проверка целостности не важна, то в режиме ESP без проверки целостности модуль может обеспечить скорость шифрования до 95 Мбит/с.

В16. Какие протоколы используются для построения защищенных VPN-туннелей?

О16. Для построения защищенных туннелей на модуле NME-RVPN (MCM) используются стандартные протоколы IKE/IPsec в соответствии с RFC 2401-2412. При использовании западных криптоалгоритмов это обеспечивает совместимость с любыми устройствами, поддерживающими протокол IPsec, например Cisco ISR или Cisco ASA. При использовании российских криптоалгоритмов обеспечена совместимость со всеми продуктами линейки CSP VPN.

В17. Какие алгоритмы шифрования, хэширования и электронно-цифровой подписи используются при работе модуля?

О17. В продуктах CSP VPN Gate могут использоваться алгоритмы шифрования ГОСТ 28147-89, DES, 3DES, IDEA, AES; алгоритмы хэширования ГОСТ Р 34.11-94, MD5, SHA1; алгоритмы электронно-цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, DSA, RSA.

В18. Q. Можно ли одновременно использовать на одном устройстве отечественные (ГОСТ) и западные криптоалгоритмы для создания разных туннелей?

О18. Можно.

В19. Каковы основные программные возможности модуля NME-RVPN (MCM)?

О19. Модуль NME-RVPN (MCM) компании «С-Терра СиЭсПи» работает, используя стандартные протоколы IKE/IPsec (RFC 2401 – RFC 2412), западные криптографические алгоритмы (DES, 3DES, AES) и отечественные криптографические алгоритмы.

В20. Каким образом может выполняться аутентификация?

О20. Аутентификация может выполняться как на основе предопределенных ключей (pre-shared key), так и с помощью цифровых сертификатов.

В21. Как выполняется управление (администрирование) шлюза с программным обеспечением CSP VPN Gate 3.1?

О21. Предусмотрены следующие способы управления.

- Из командной строки CLI (аналогично командной строке Cisco IOS). Данный способ является основным.
- С помощью CSM (Cisco Security Manager), используя графический интерфейс.
- Специфические функции CSP VPN Gate можно задействовать, настраивая “native configuration” (способ, рекомендуемый только для специальных настроек и только для опытных пользователей).

В22. Как получить доступ к консоли модуля NME-RVPN (MCM)?

О22. Для подключения к консоли модуля необходимо использовать команду IOS `service-module special-services-engine slot/0 session`. Поддерживается доступ к CLI или командному интерпретатору Linux по протоколу SSH.

- V23.** Как модуль NME-RVPN (MCM) идентифицируется в Cisco Security Manager?
- O23.** В CSM модуль NME-RVPN (MCM) определяется как «Cisco Router 2811».
- V24.** Как происходит взаимодействие модуля NME-RVPN (MCM) с Cisco Security Manager?
- O24.** Модуль NME-RVPN (MCM) взаимодействует с CSM по протоколу SSH.
- V25.** Чем процедуры управления модулем NME-RVPN (MCM) с помощью команд CLI отличаются от процедур управления с использованием командной строки Cisco IOS?
- O25.** Консоль CLI модуля предоставляет пользователю интерфейс в стиле командной строки Cisco IOS. Набор команд консоли является подмножеством команд IOS с некоторыми ограничениями функциональности и небольшими дополнительными возможностями. Как и у IOS, у консоли есть привилегированный и конфигурационный режимы (`configure terminal`). В отличие от IOS, изменения настроек вступают в действие не сразу, а только после выхода из конфигурационного режима. Дополнительную информацию можно найти в документации на продукт CSP VPN Gate на сайте www.s-terra.com.
- V26.** Каковы особенности работы Crypto ACL?
- O26.** Основные особенности заключаются в следующем:
- допустимо использование протоколов TCP и UDP;
 - при указании "range" портов будут создаваться множественные SA;
 - при использовании фильтрующих ACL используется один ACL на интерфейс, но он применяется в обоих направлениях;
 - нет необходимости явным образом разрешать протоколы IKE, AH, ESP.
- Дополнительную информацию можно найти в документации на продукт CSP VPN Gate на сайте www.s-terra.com.
- V27.** Каковы ограничения на использование интерфейса командной строки и планируется ли расширять список команд, доступных в продуктах CSP VPN?
- O27.** В продукте CSP VPN Gate 3.1 реализован ограниченный набор команд, совместимых с Cisco IOS версии 12.2(13)T. Этот набор команд непрерывно расширяется по мере выхода новых версий продукта.
- V28.** Есть ли поддержка syslog?
- O28.** Да, можно настроить один syslog-сервер.
- V29.** С какими удостоверяющими центрами (в рамках инфраструктуры PKI) совместимо ПО CSP VPN Gate?
- O29.** Шлюз CSP VPN Gate совместим со следующими удостоверяющими центрами: Microsoft Certificate Authority с криптопровайдером CryptoPro; Notary-PRO компании Сигнал-Ком; RSA Keon.
- V30.** Поддерживает ли CSP VPN Gate работу с сертификатами, содержащими символы кириллицы?
- O30.** Да. Начиная с версии 2.1, введена поддержка кириллицы в сертификатах.
- V31.** Что необходимо для построения системы удаленного доступа по протоколу IPSec с российскими криптоалгоритмами?
- O31.** Для обеспечения удаленного доступа компания «С-Терра СиЭсПи» поставляет клиент CSP VPN Client версии 3.1, поддерживающий российские криптоалгоритмы. Этот клиент может быть установлен на компьютеры, работающие под управлением операционных систем Windows 2000, XP, Vista. Продукт CSP VPN Client версии 3.1 сертифицирован как средство криптографической защиты информации (сертификат ФСБ России №СФ/114-1411).

- В32. Можно ли на один компьютер установить CSP VPN Client и Cisco Security Agent (CSA)?**
- О32.** Можно. При установке CSP VPN Client после CSA возникают запросы последнего на разрешение установки Client. При проверке совместимости использовалась политика по умолчанию CSA Desktop. Если первым на компьютер установлен CSP VPN Client, то следует убедиться, что его политика не блокирует доступ к серверу с установленным MC CSA.
- В33. Поддерживает ли CSP VPN Gate 3.1 функциональность GRE?**
- О33.** Текущая версия CSP VPN Gate не поддерживает создание GRE-туннелей, при необходимости данную функциональность следует настраивать в базовом маршрутизаторе Cisco.
- В34. Не удалось установить защищенное соединение между шлюзами CSP VPN Gate, между которыми включен NAT. В чем может быть причина?**
- О34.** Скорее всего, проблема в том, что производится попытка настроить туннель IPSec(AH+ESP)- или IPSec(AH)-туннель. Иными словами, в используемых наборах преобразований задан алгоритм проверки целостности AH (AH_GOST_HMAC или AH_SHA_HMAC).
- Однако AH не работает через NAT, можно использовать только ESP или ESP+HMAC.
- В35. С какими продуктами компании С-Терра СиЭсПи совместим модуль NME-RVPN (MCM)?**
- О35.** Модуль NME-RVPN (MCM) совместим с любыми другими продуктами серии CSP VPN Gate, Client, Server компании «С-Терра СиЭсПи». Более подробная информация о продуктах серии CSP VPN доступна на сайте <http://www.s-terra.com>.

ЗАКАЗЫ И ПОДДЕРЖКА

- В36. Какие гарантии предоставляются на модуль NME-RVPN (MCM)?**
- О36.** Техническая поддержка модуля NME-RVPN (MCM) с программным обеспечением CSP VPN Gate осуществляется в течение одного года с момента приобретения решения. Она включает в себя услуги гарантированного технического сопровождения, включая исправление вновь найденных дефектов. При необходимости контракт на услуги по техническому сопровождению может быть приобретен и на более длительный срок. Поддержка осуществляется компанией «С-Терра СиЭсПи» и ее партнерами.
- В37. Как можно приобрести модуль NME-RVPN (MCM)?**
- О37.** Модуль NME-RVPN (MCM) можно заказать у бизнес-партнеров компании «С-Терра СиЭсПи», список и контактная информация представлены на сайте: <http://www.s-terra.com>.
- В38. Где можно найти техническую документацию по решению на модуле NME-RVPN (MCM)?**
- О38.** Все информация представлена на сайте: <http://www.s-terra.com>. Отправить запрос на инструкции по установке и конфигурированию можно по адресам presale@s-terra.com или support@s-terra.com.
- В39. Каковы экспортные ограничения на модуль NME-RVPN (MCM)?**
- О39.** А. Программное обеспечение модуля NME-RVPN (MCM) компании «С-Терра СиЭсПи» содержит криптографические функции (алгоритмы шифрования ГОСТ 28147-89; алгоритмы хэширования ГОСТ Р 34.11-94; алгоритмы электронно-цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001), подлежащие экспортному контролю согласно российскому законодательству. Сам по себе аппаратный модуль не содержит данных функций.
- В40. Кто оказывает техническую поддержку по установке и конфигурированию модуля NME-RVPN (MCM)?**
- О40.** Техническая поддержка решений на базе модуля NME-RVPN (MCM) для конечных пользователей оказывается системными интеграторами, являющимися партнерами компании «С-Терра СиЭсПи». Вы также можете обратиться в компанию «С-Терра СиЭсПи» по телефону + 7 (495) 536-99-58 или отправить сообщение на адрес support@s-terra.com.

Примечание. Пожалуйста, не обращайтесь в центр технической поддержки Cisco (TAC) по вопросам, связанным с этим сетевым модулем.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Для получения дополнительной информации по продуктам компании Cisco зайдите на страницу <http://www.cisco.com/web/RU/> или свяжитесь с региональным представителем Cisco.

Для получения дополнительной информации по модулю NME-RVPN (MCM) зайдите на сайт «С-Терра СиЭсПи» <http://www.s-terra.com>, отправьте запрос на адреса presale@s-terra.com, support@s-terra.com или свяжитесь с партнерами «С-Терра СиЭсПи».



Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., 52, стр. 1, 4-й этаж.
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск,
бизнес-центр «Росэнергогаз»,
Димитрова пр-т, 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Alronet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)