

ИНФОРМАЦИЯ О ПРОДУКТЕ

CISCO RUSSIA VPN NETWORK MODULE

Компания Cisco Systems представляет модуль NME-RVPN (Russia VPN Network Module) для маршрутизаторов серии Cisco® 2800 и 3800 Integrated Services Routers. Модуль представляет собой инновационное решение, интегрированное именно с маршрутизаторами Cisco и специально разработанное для обеспечения российского рынка высокотехнологичным сертифицированным решением VPN (виртуальные частные сети, ВЧС) с передовыми технологиями Cisco и удовлетворяющим современным требованиям эффективной защиты всех видов сетевых взаимодействий. Модуль NME-RVPN использует программное обеспечение CSP VPN Gate компании «С-Терра СиЭсПи», реализующее стандарт IPsec (RFC 2401-2412), имеющее сертификат ФСТЭК РФ как шлюз безопасности и использующее встроенную библиотеку криптографических алгоритмов ГОСТ, сертифицированную ФСБ РФ.

ОБЗОР ПРОДУКТА

Модуль NME-RVPN в составе маршрутизаторов серии Cisco® 2800 и 3800 Integrated Services Routers предлагает российским потребителям уникальное устройство, позволяющее обеспечить как эффективную маршрутизацию, так и защиту трафика данных, голоса, видео. При этом устройство управляется как единое целое, используя интерфейс Cisco для формирования правил маршрутизации и защиты сетевых взаимодействий. Подобная глубокая интеграция позволяет существенно уменьшить сложность сети, не предъявлять дополнительных требований к квалификации персонала и, как результат, снизить затраты на развертывание и поддержку, а также сроки развертывания подсистемы информационной безопасности.

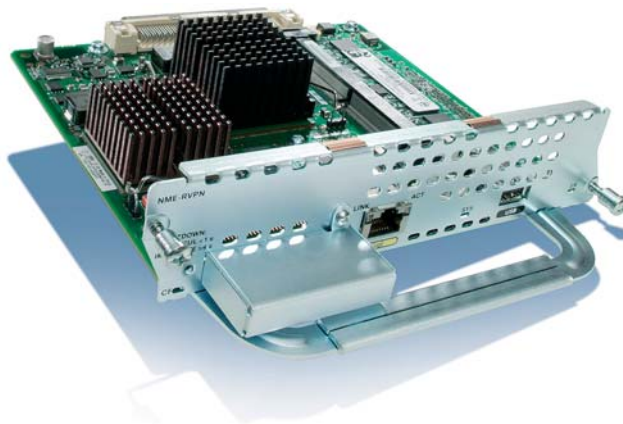


Рисунок 1. Модуль NME-RVPN

ПРЕИМУЩЕСТВА И ВОЗМОЖНОСТИ ПРОДУКТА

Защищенность сетевых взаимодействий

В связи с широкой интеграцией корпоративных коммуникаций с публичными сетями для обеспечения взаимодействий компаний с филиалами, удаленными пользователями, заказчиками и партнерами первостепенное значение приобретает вопрос обеспечения российских пользователей высокотехнологичным сертифицированным VPN-решением в сочетании с передовыми технологиями Cisco Systems и удовлетворяющим современным требованиям эффективной защиты всех видов сетевых взаимодействий. При этом необходимо не только решить вопросы защиты внешнего обмена данными, но и предоставить современные решения по защищенным беспроводным коммуникациям, защите голоса и видео с обеспечением качества обслуживания, максимально эффективно защитить взаимодействие клиентов в сетях операторов связи и услуг.

Включение модуля NME-RVPN в маршрутизаторы серии Cisco 2800 или 3800 Integrated Services Router позволяет потребителям получить единое решение, обеспечивающее, в том числе, организацию сетевой защиты, использующей российскую сертифицированную криптографию, развитую маршрутизацию, качество обслуживания приоритетного трафика (QoS), сервисы видео и голоса, коммутацию сетей. Подобные качества совместно с управляемостью и надежностью технологий Cisco IOS практически полностью закрывают потребность современного бизнеса в организации и защите ответственных, критически важных сетевых взаимодействий.

Программное обеспечение CSP VPN Gate

Программное обеспечение CSP VPN Gate, входящее в состав модуля NME-RVPN, является еще одним элементом семейства продуктов CSP VPN Client, CSP VPN Server и масштабируемой серии шлюзов безопасности CSP VPN Gate 100/1000/3000/7000/10000.

Продукты CSP VPN обеспечивают базовую функциональность современного VPN-устройства:

- Шифрование (конфиденциальность) и ЭЦП (целостность, аутентификация) IP-пакетов, целостность потока пакетов.
- Маскировку топологии сети за счет инкапсуляции трафика в защищенный туннель.
- Прозрачность для NAT (поддержка инкапсуляции пакета ESP в UDP).
- Аутентификацию узлов сети и пользователей, контроль доступа на уровне компьютеров, пользователей и приложений, интегрированный межсетевой экран 4-го класса (CSP VPN Gate удовлетворяет требованиям к межсетевому экрану по 4-му классу защищенности).
- Обеспечение надежности с выравниванием нагрузки в схеме резервирования N+1 (Dead Peer Detection protocol).
- Унификацию политики безопасности для мобильных и «внутренних» пользователей (динамическое конфигурирование корпоративных IP-адресов для удаленных пользователей «внутри VPN»).
- Сохранение классификации трафика для защищенных пакетов (мапирование ToS поверх IPsec), приоритетную обработку трафика голоса и видео (поддержка QoS), отсутствие потери пакетов при регенерации сессионных ключей (smooth IKE re-keying).
- Гибкое, централизованное и событийное ведение журнала с возможностью вторичной обработки на основе протокола Syslog.

Как результат, применение модуля NME-RVPN в составе маршрутизатора Cisco Integrated Services Router 2800/3800 обеспечивает эффективную реализацию множества сценариев сертифицированной защиты, включая:

- межсетевые взаимодействия;
- защищенный доступ удаленных и мобильных пользователей;
- защиту беспроводных сетей;
- защиту мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь);
- защиту платежных систем и систем управления технологическими процессами в производстве и на транспорте.

Межсетевые взаимодействия

Сценарии защиты межсетевых взаимодействий (Site-to-Site VPN) применяются для защиты коммуникаций территориально распределенных корпоративных сетей через публичные (открытые, не заслуживающие доверия) сети/каналы связи.

По сути применение VPN-решений для этих целей не должно приводить к понижению требований к характеристикам непосредственно канала передачи данных, таких как поддержка множественности протоколов, высокая надежность, большая масштабируемость. Наоборот, современные VPN-решения должны обеспечивать высокую ценовую эффективность и большую гибкость в реализации таких требований. Высокую ценовую эффективность можно получить, например, за счет возможности использовать публичные каналы для передачи информации, что ранее было недоступно.

Использование для этой цели маршрутизаторов Cisco ISR (рисунок 2) в полной мере выполняет поставленную выше задачу.

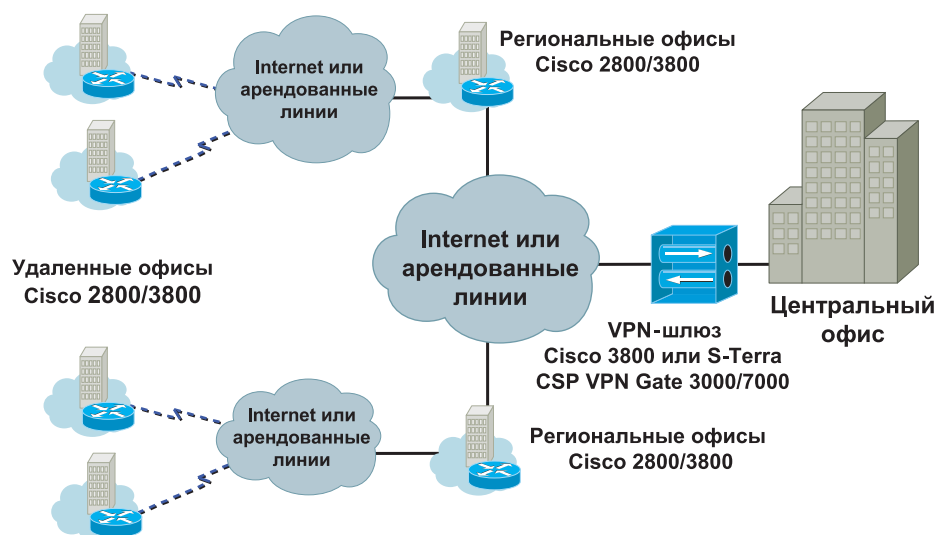


Рисунок 2. Использование VPN-туннелей для создания защищенной корпоративной сети

Для выполнения требований повышенной надежности сетевых взаимодействий крупных сетей (обеспечивающей непрерывность бизнес-процессов в них) в дополнение к приведенному выше примеру могут использоваться решения с резервированием и балансировкой нагрузки.

Защита беспроводных и мультисервисных сетей

Продукты CSP VPN поддерживают сценарии защиты как выделенных мультимедийных сетей, так и «смешанных» сетей, обеспечивая:

- поддержку качества сетевого обслуживания;
- защиту качества сервиса в голосовой VPN при перегрузке трафика данных.

Модуль NME-RVPN в составе маршрутизаторов Cisco 2800 или Cisco 3800, обеспечивающих дополнительную функциональность CallManager Express и беспроводной точки доступа, предоставляет для удаленных офисов всю необходимую функциональность обработки и защиты беспроводных мультимедийных и мультисервисных сетей в едином устройстве.

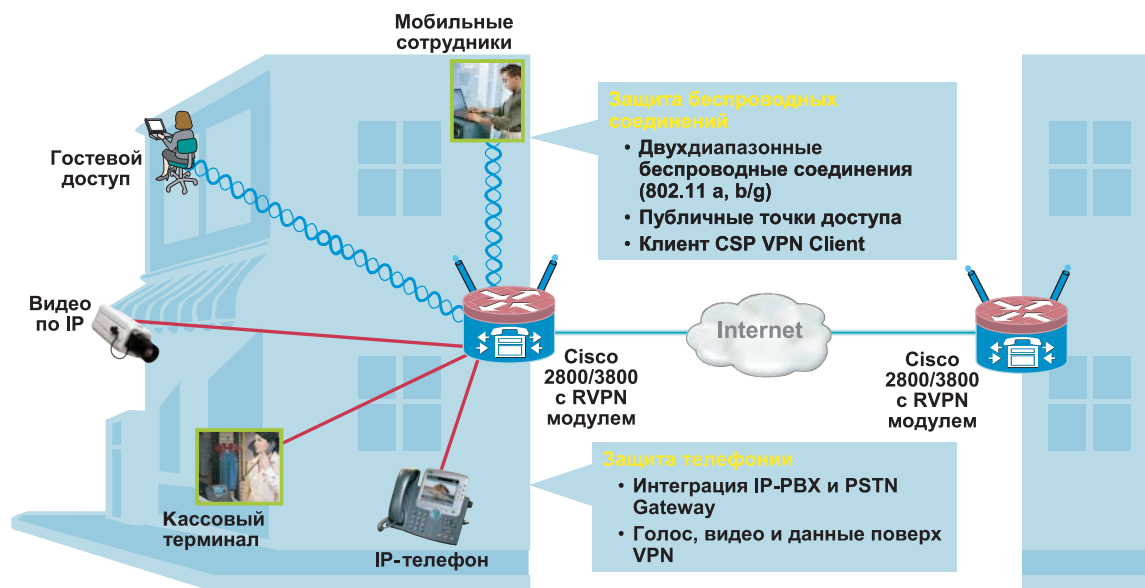


Рисунок 3. Защита беспроводных и мультисервисных сетей

Основным средством защиты трафика в беспроводной сети является IPsec. При этом обеспечивается не только аутентификация устройств (что делается на канальном уровне), но и аутентификация пользователей (рисунок 3).

Применение в радиосегменте выделенного адресного пространства и IPsec VPN обеспечивает:

- возможность изолировать проводной сегмент от открытого IP-трафика;
- пропускать внутрь проводной корпоративной сети (к ресурсам локальной сети) только IPsec-трафик, причем только в «домашние» сети.

Защита удаленных и мобильных пользователей

Сценарии удаленного доступа пользователей (Remote Access VPN) применяются для защиты доступа удаленных или мобильных пользователей в корпоративную сеть через публичные (открытые, не заслуживающие доверия) сети или каналы связи.

- Политика безопасности клиента доступа CSP VPN Client определяется только системным администратором (администратором безопасности) и не может быть изменена пользователем.
- Права доступа пользователя определяются в корпоративной сети, и информация о правах доступа в корпоративной сети отсутствует на клиенте доступа CSP VPN Client.
- Клиент доступа CSP VPN Client не требует от пользователя никаких технических операций кроме установки и ввода ключа, предоставленного администратором безопасности.

CSP VPN Client поддерживает защищенную связь практически из любой точки, где присутствует какой-либо коммуникационный ресурс. Используются специальные меры в обеспечении мобильности пользователя:

- адаптивность к адресному пространству (IPsec автоматически включается в зонах, где требуется защищенное соединение);
- поддержка различных сред передачи, в том числе мобильных (GPRS, CDMA, Wi-Fi, WiMAX и др.);
- обеспечение прозрачной передачи IKE/IPsec трафика через шлюзы с трансляцией адресов (NAT).

ВОЗМОЖНОСТИ И ПРЕИМУЩЕСТВА

По сравнению с другими отдельными подобными устройствами модуль NME-RVPN при использовании в сетевой инфраструктуре центрального офиса имеет ряд преимуществ:

- Общий с другими устройствами интерфейс управления. Для управления и конфигурирования модуля можно применять интерфейс командной строки (CLI) с использованием команд, аналогичных Cisco IOS. Модулем можно также управлять с помощью графического web-интерфейса.
- Снижение потребления и простота коммутации. Модуль получает питание от маршрутизатора, не нуждается в коммутации и не занимает места в стойке с сетевым оборудованием.

АРХИТЕКТУРА МОДУЛЯ

Модуль NME-RVPN можно установить в маршрутизаторы Cisco ISR 2811, 2821, 2851, 3825 и 3845 с версией IOS 12.4(11)T или выше. При этом модуль NME-RVPN работает независимо от IOS маршрутизатора, используя программное обеспечение CSP VPN Gate v 2.1 компании «С-Терра СиЭсПи», установленное на компакт-флэш-карте (Compact Flash) модуля. Программное обеспечение модуля функционирует под управлением адаптированной OS Linux.

Аппаратно модуль NME-RVPN представляет собой вычислительную платформу на базе процессора Intel Celeron-M 1.0ГГц с 512 МБ оперативной памяти и 512 МБ Compact Flash (рисунок 4). Для подключения к локальной сети модуль имеет внешний интерфейс Gigabit Ethernet. Аналогичный внутренний интерфейс осуществляет взаимодействие и передачу данных между модулем и маршрутизатором.

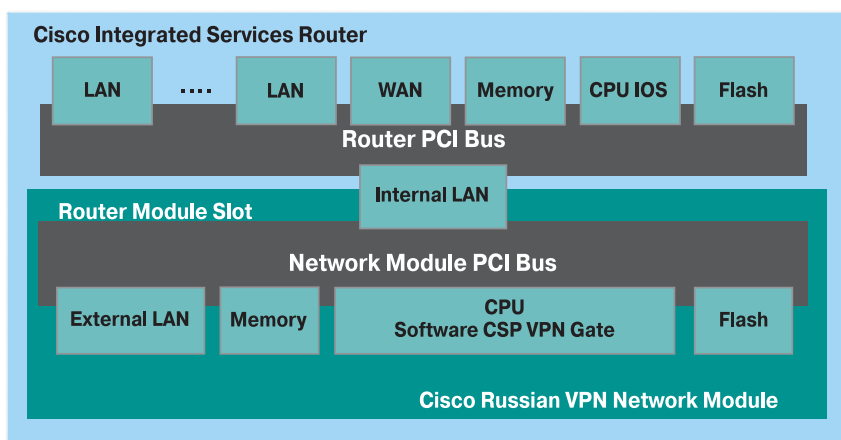


Рисунок 4. Архитектура модуля NME-RVPN и Cisco Integrated Services Router

СПЕЦИФИКАЦИЯ ПРОДУКТА

Спецификация модуля NME-RVPN представлена в таблице 1.

Таблица 1. Спецификация продукта

Характеристики	Описание
Аппаратные характеристики модуля	
Процессор	1 ГГц Intel Celeron-M
Память DRAM	512 МБ DDR2
Сетевые интерфейсы	<ul style="list-style-type: none"> • 1 внутренний интерфейс 1000 Мбит/с Ethernet • 1 внешний интерфейс 10/100/1000 Мбит/с Ethernet
Память Flash	512 МБ Compact Flash
Физические характеристики модуля	
Физические размеры (В x Ш x Д)	3,9 x 18,0 x 18,3 см (1,55 x 7,10 x 7,2 дюймов)
Вес	1,25 фунтов (567 грамм)
Рабочая влажность	от 5% до 95%, без конденсата
Рабочая температура	0–40 °C (32–104 °F)
Температура хранения	-25 °C до 70 °C
Рабочая высота над уровнем моря	10 000 футов (3048 м) при 25 °C
Мощность	21 Вт

Сертификаты по безопасности	<ul style="list-style-type: none"> • Underwriters Laboratory 1950 • CSA-C22.2 No. 950 • EN 60950 • IEC 60950
Сертификаты по электромагнитной совместимости	<ul style="list-style-type: none"> • 47 CFR Part 15 Class A • CISPR22 Class A • EN300386 Class A • EN55022 Class A • EN61000-3-2 • EN61000-3-3 • VCCI Class I • AS/NZS CISPR 22 Class A
Сертификаты по электромагнитной помехоустойчивости	<ul style="list-style-type: none"> • CISPR24 • EN300386 • EN50082-1 • EN55024 • EN61000-6-1

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Функциональные возможности модуля NME-RVPN представлены в таблице 2.

Таблица 2.

Программная совместимость	Любые продукты, поддерживающие протоколы IKE/IPSec (RFC 2401 – RFC 2412)
Протоколы туннелирования	IPSec, NAT Transparent IPSec (UDP инкапсуляция – draft-huttunen-ipsec-esp-in-udp-01.txt)
Шифрование/аутентификация	IPSec Encapsulating Security Payload (ESP) и/или IPSec Authentication Header (AH) при использовании ГОСТ 28147-89 (256 бит), DES/3DES (56/168 бит) или AES (128/192/256 бит) с ГОСТ Р 34.11-94, MD5 или SHA
Управление ключами	IKE (Internet Key Exchange) IKE exchanges: Main mode, Aggressive mode, Quick mode, Transaction Exchanges, Informational Exchanges. IKE: ГОСТ Р 34.10-94, ГОСТ Р 31.10-2001, RSA, DSA, Pre-shared key Поддержка Smooth IKE/IPSec rekeying
Работа с сертификатами	LDAP v.3, x509 v.3, PKCS #7 (base64, bin), PKCS #10 (base64, bin), PKCS #12 (base 64, bin), base 64, bin, CRL
Маршрутизация	Статическая маршрутизация Управляемый политикой IPSec контроль фрагментации пакетов в канале Обнаружения отказов удаленных узлов: IKE keep-alive extension – Dead Peer Detection (draft-huang-dpd-00.txt) Удаленный клиент IP, назначение IP из локального пула адресов (IKE-CFG)
Фильтрация	IP-адрес (диапазон IP, сайт) источника и назначения Порты и тип протокола Обработка фрагментированных пакетов
Настройка и управление	Протоколы управления: Telnet, SSH, HTTP или они же в режиме защиты IPSec Ведение журнала событий: syslog (локально или на удаленный сервер) Протокол SNMP, поддержка MIB-II SNMP traps (CISCO-IPSECFLOW- MONITOR-MIB, CISCO-IPSECMIB, CISCO-CONFIG-MAN-MIB)
Поддержка QoS	Отображение битов TOS поверх IPSec и приоритизация очередей QoS для обеспечения работы IP-телефонии и видео
Высокая доступность	Распределение нагрузки, псевдокластер (n+1), поддержка IPSec соединений Обнаружение потери соединения (draft-huang-dpd-00.txt), восстановление соединения
Управление политиками	Интерфейс командной строки CLI Графический пользовательский интерфейс на основе Web

СЕРТИФИКАЦИЯ И ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ

Решение на базе продуктов CSP VPN Gate/Client с использованием модуля NME-RVPN удовлетворяет необходимым требованиям регулирующих органов Российской Федерации по защите конфиденциальной информации и может применяться как в коммерческих структурах, так и в государственных органах. В частности, согласно Специальным требованиям СТР-К модуль NME-RVPN со встроенным шлюзом CSP VPN Gate может быть использован для защиты конфиденциальной информации при ее передаче по каналам связи в автоматизированных системах класса 1Г.

Компания «С-Терра СиЭсПи» обладает всеми необходимыми лицензиями ФСБ РФ и Государственной Технической комиссии http://www.s-terra.com/CSP/RU/licenses/licenses.htm#security_targets

Таблица 3. Выполнение сертификационных требований

Сертификат	Описание
Сертификат ФСТЭК	Сертификат соответствия ФСТЭК РФ № 1205 от 07 июля 2006 года, подтверждающий, что программный комплекс «CSP VPN Gate. Версия 2.1» является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует заданию по безопасности (оценочный уровень доверия ОУД 3, ГОСТ Р ИСО/МЭК 15408) http://www.s-terra.com/CSP/RU/licenses/licenses.htm#certificates
	Сертификат соответствия ФСТЭК РФ № 1206 от 07 июля 2006 года, подтверждающий, что программный комплекс «CSP VPN Client. Версия 2.1» является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует заданию по безопасности (оценочный уровень доверия ОУД 3, ГОСТ Р ИСО/МЭК 15408) http://www.s-terra.com/CSP/RU/licenses/licenses.htm#certificates
Выполнение требований РД Гостехкомиссии к МЭ	CSP VPN Gate удовлетворяет требованиям РД Гостехкомиссии РФ к межсетевым экранам по 4-му классу защищенности (ГОСТ Р ИСО/МЭК 15408–2002, Шлюз безопасности CSP VPN Gate версии 2.1, Задание по Безопасности, Приложение А http://www.s-terra.com/CSP/documents/ST_CSP_VPN_Gate_21.pdf)
Сертификат ФСБ	Для модулей NME-RVPN и удаленных продуктов CSP VPN Gate/Client: встроенная криптобиблиотека СКЗИ от компании «Сиграл-Ком», имеющая сертификат ФСБ по уровням KC1, KC2 http://www.signal-com.ru/ru/about/cert/index.php
	Только для удаленных продуктов CSP VPN Gate/Client: встроенная криптобиблиотека СКЗИ от компании «Крипто-Про», имеющая сертификат ФСБ по уровням KC1, KC2 http://www.cryptopro.ru/CryptoPro/products/csp/conformance.htm

ПРОИЗВОДИТЕЛЬНОСТЬ

Наиболее часто используемый алгоритм для IPsec-туннелей, включающий шифрование с проверкой целостности (ESP+HMAC), показывает производительность, равную 40 Мбит/с (измерено на больших пакетах –1400 байт). Если же проверка целостности не важна, то в режиме «ESP only» модуль может обеспечить скорость шифрования до 95 Мбит/с. Подробные характеристики производительности модуля NME-RVPN представлены в таблице 4.

Таблица 4. Характеристики производительности модуля NME-RVPN

Используемый алгоритм	Значение*
ESP с проверкой целостности	40 Мбит/с
ESP без проверки целостности	95 Мбит/с
AH	57 Мбит/с
AH+ESP	40 Мбит/с

* Измерено при использовании потока UDP пакетов размером 1400 байт.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Системные требования для модуля NME-RVPN представлены в таблице 5.

Таблица 5. Системные требования

Требования	Описание
Оборудование	Cisco 2811, 2821 или 2851 Integrated Series Routers
	Cisco 3825 или 3845 Integrated Series Routers
Программное обеспечение	Cisco IOS® Software Release 12.4(11)T или более поздний, установленный на маршрутизаторе

ЗАКАЗЫ

Модуль NME-RVPN можно заказать у бизнес-партнеров компании «С-Терра СиЭсПи», список которых и контактная информация по которым доступны на странице: http://www.s-terra.com/CSP/RU/partners/business_partners.htm

Модуль NME-RVPN имеет номенклатурный номер NME-RVPN=.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка решений на базе модуля NME-RVPN для конечных пользователей оказывается системными интеграторами, являющимися бизнес-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 e-mail: support@s-terra.com

Примечание.

Пожалуйста, не обращайтесь в Cisco Technical Assistance Center (ТАС) по вопросам, связанным с этим сетевым модулем.

РЕЗЮМЕ

Модуль NME-RVPN предлагает конечному пользователю сочетание некриптографических средств защиты информации от компании Cisco и сертифицированных продуктов сетевой защиты CSP VPN от компании «С-Терра СиЭсПи». Решение CSP VPN характеризуется высокой масштабируемостью, что, наряду с корректным техническим балансом надежности и производительности, обеспечивает высокую экономическую эффективность для конечного заказчика.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

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

Для получения дополнительной информации по модулю NME-RVPN зайдите на страницу «С-Терра СиЭсПи» <http://www.s-terra.com/CSP/RU/products/products.htm> или свяжитесь с партнерами «С-Терра СиЭсПи».



Cisco Systems
Россия, 115054, Москва
бизнес центр «Риверсайд Тауерс»
Космодамианская наб., 52
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186, Санкт-Петербург,
бизнес центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр «Самал 2»
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр «Горайзон Тауерс»
Ул. Шовковична, 42-44, этаж 9
Тел.: +7 (38044) 490 36 00
Факс: +7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or 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. (0406R)