Информационный бюллетень

Модуль сетевой модернизированный NME-RVPN (MCM)

Модуль сетевой модернизированный NME-RVPN (MCM)

Модуль NME-RVPN в исполнении MCM может использоваться в составе маршрутизаторов Cisco ISR первого и второго поколения (Cisco® ISR серий 2800/3800 и Cisco® ISR серий 2900/3900). Этот модуль разработан специально для обеспечения российского рынка высокотехнологичным решением в области интеграции приложений сетевой безопасности: в модуле, основанном на передовых технологиях Cisco, используется российское сертифицированное программное обеспечение. Технологический процесс производства модуля NME-RVPN в исполнении MCM определен документом «Порядок организации производства изделия «Модуль Сетевой Модернизированный (MCM)» в рамках подконтрольного технологического процесса на территории Российской Федерации» и согласован с регулятором (ФСБ России).

Обзор продукта

Модуль NME-RVPN в исполнении MCM для применения в составе маршрутизаторов Cisco® ISR серий 2800/3800 и 2900/3900 представляет собой уникальное устройство, позволяющее обеспечить как эффективную маршрутизацию, так и защиту трафика данных, голоса и видео. Устройство управляется как единое целое, используя интерфейс Cisco IOS как для формирования правил маршрутизации, так для управления защитой сетевых взаимодействий. Такая интеграция позволяет существенно снизить сложность сетевой инфраструктуры, не предъявлять дополнительных требований к квалификации персонала и в итоге понизить затраты на развертывание и поддержку, а также уменьшить сроки развертывания подсистемы обеспечения информационной безопасности.

Преимущества и функциональные возможности продукта

Защищенность сетевых взаимодействий
В связи с глубокой интеграцией современных корпоративных сетей с сетями общего доступа (для обеспечения взаимодействия центральных офисов с филиалами, удаленными пользователями, заказчиками и партнерами) первостепенное значение приобретает вопрос обеспечения российских пользователей высокотехнологичным сертифицированным VPN-решением на базе передовых технологий Cisco. Такое решение должно не только соответствовать самым современным требованиям эффективной защиты всех видов сетевых взаимодействий, но и удовлетворять требованиям российского технического регулирования в сфере информационной безопасности. При этом необходимо решить вопросы защиты обмена данными с внешними абонентами, обезопасить беспроводные коммуникации, защитить передачу голоса и видео с обеспечением качества обслуживания, а также обеспечить максимально эффективную защиту взаимодействия клиентов в сетях операторов связи и провайдеров услуг.

Интеграция модуля NME-RVPN в исполнении MCM в маршрутизаторы Cisco ISR серий 2800/3800 и 2900/3900 позволяет потребителям получить единое решение, обеспечивающее защиту передаваемой информации в соответствии с требованиями российских стандартов, развитую маршрутизацию, поддержку механизмов качества обслуживания приоритетного трафика (QoS), а также сервисы IP-телефонии и передачи видео. Подобные качества, дополненные управляемостью и надежностью платформ на базе операционной системы

Модуль NME-RVPN (MCM)

Cisco IOS, практически полностью закрывают потребности современных организаций в защите критически важных сетевых взаимодействий и обеспечивают возможность успешного применения модуля как в корпоративном, так и в государственном секторе.

Защита межсетевых взаимодействий
Сети VPN типа «сеть-сеть» применяются для защиты взаимодействия в рамках распределенной корпоративной сети по публичным (открытым, не заслуживающим доверия) сетям/каналам связи.

Применение VPN-решений для этих целей не приводит к понижению требований к характеристикам непосредственно канала передачи данных, таких как набор поддерживаемых протоколов, высокая надежность, большая масштабируемость. Напротив, современные VPN-решения обеспечивают высокую экономическую эффективность и большую гибкость в реализации таких требований, в том числе и за счет возможности использовать публичные каналы для передачи информации.

Использование для этой цели маршрутизаторов Cisco ISR первого и второго поколений (см. рис. 2) позволяет решить поставленную задачу в полной мере.

Для соблюдения требований по повышению надежности и производительности сетевых взаимодействий крупных сетей (включая требования по обеспечению непрерывности бизнес-процессов) в дополнение к приведенному выше примеру могут использоваться решения с резервированием и балансировкой нагрузки.

Защита беспроводных и мультисервисных сетей
Рассматриваемые решения поддерживают сценарии защиты как выделенных мультисервисных, так и смешанных сетей, обеспечивая:

- поддержку механизмов качества обслуживания;
- защиту качества обслуживания в голосовой; защищенной сети при перегрузке сетевых каналов трафиком данных.

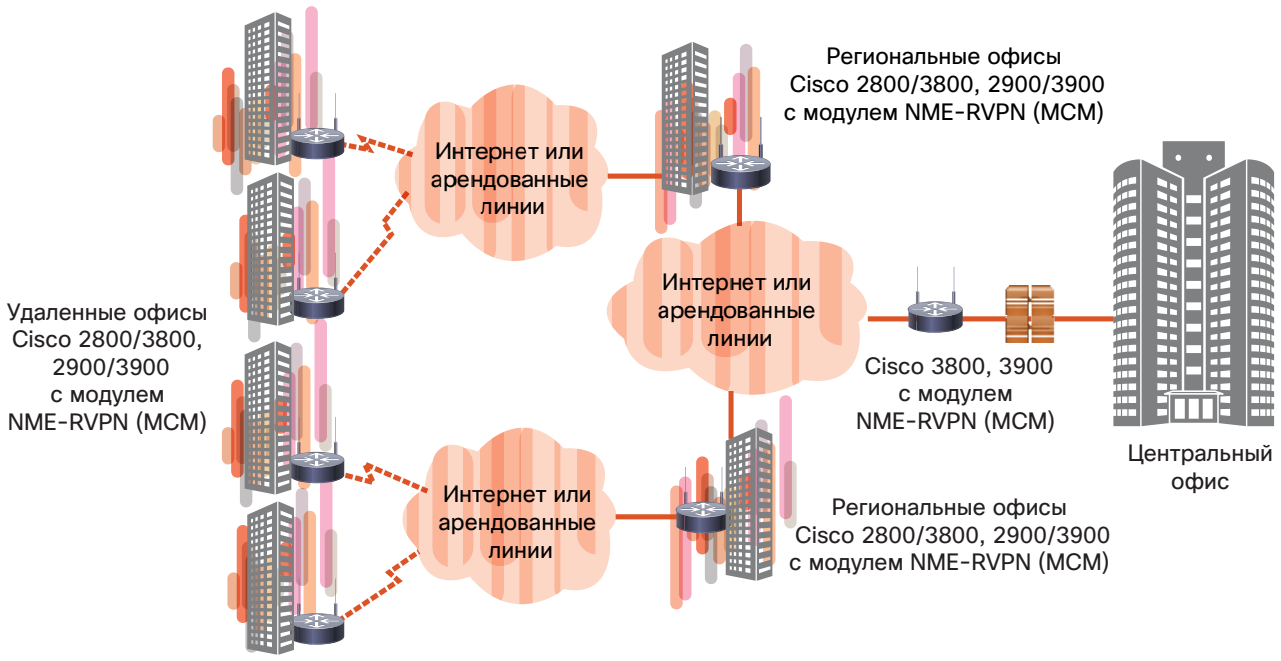

Рисунок 2. Использование VPN-туннелей для создания защищенной корпоративной сети

Модуль сетевой модернизированный NME-RVPN (MCM)

Защита удаленных и мобильных пользователей

Сети VPN удаленного доступа применяются для защиты доступа удаленных или мобильных пользователей в корпоративную сеть через публичные сети или каналы связи. Использование сетей VPN удаленного доступа характеризуется следующими особенностями:

- VPN-клиент не требует от пользователя никаких технических операций, кроме ввода учетных данных, предоставленных администратором безопасности.
- Политика безопасности VPN-клиента доступа определяется только системным администратором (администратором безопасности) и не может быть изменена пользователем.
- Права доступа пользователя определяются в корпоративной сети, информация о правах доступа в корпоративной сети отсутствует на VPN-клиенте.

Предлагаемые VPN-клиенты обеспечивают защищенную связь практически из любой точки мира, где присутствует какой-либо коммуникационный ресурс. Для обеспечения мобильности пользователя используются следующие механизмы:

- адаптивность к адресному пространству;
- поддержка различных сред передачи данных, в том числе мобильных (GPRS, CDMA, Wi-Fi, WiMAX и др.);
- обеспечение прозрачной передачи трафика через шлюзы, выполняющие трансляцию адресов (NAT).

Возможности и преимущества

По сравнению с другими неинтегрированными сетевыми устройствами со сходной функциональностью модуль NME-RVPN в исполнении MCM имеет ряд преимуществ, среди которых можно выделить следующие:

- Простота администрирования и единый с другими устройствами интерфейс управления. Для управления и конфигурирования модуля можно использовать интерфейс командной строки (CLI) или систему управления устройствами безопасности Cisco Security Manager, имеющую графический интерфейс.
- Снижение энергопотребления и простота коммутации. При использовании модуля не занимаются дополнительные интерфейсы маршрутизатора. Модуль получает питание от маршрутизатора, не нуждается в коммутации и не занимает места в стойке с сетевым оборудованием.
- Повышение мобильности и простоты установки. Предварительно настроенный в центральном офисе маршрутизатор с модулем можно передать в филиал для установки в стойке с другим оборудованием. При этом не требуется наличие квалифицированных специалистов в филиале. Дополнительные настройки модуля можно выполнять удаленно.

Технологический процесс производства модуля NME-RVPN в исполнении MCM согласован с ФСБ России.

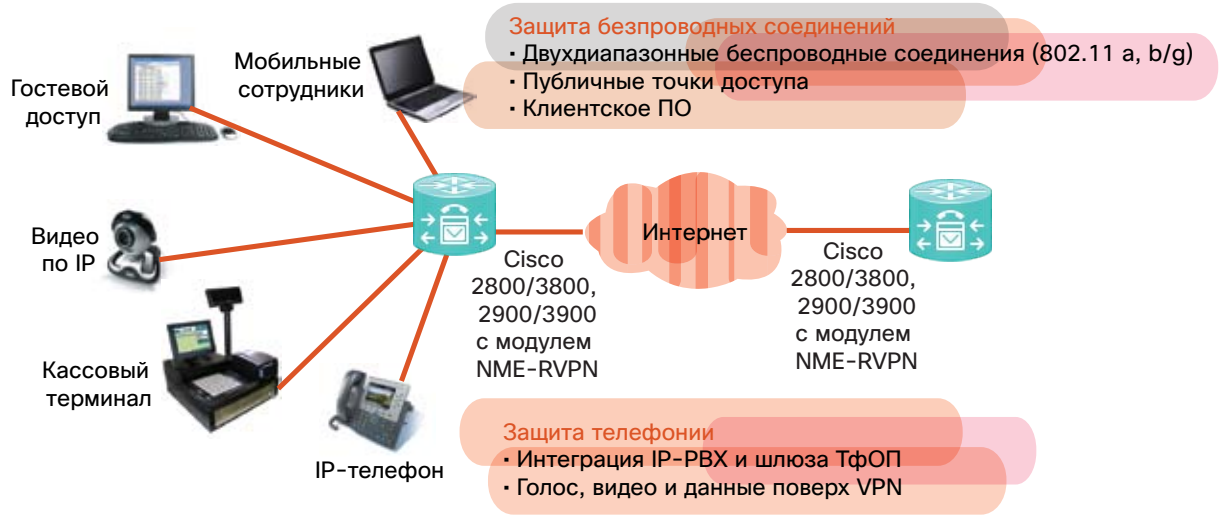

Рисунок 3. Защита беспроводных и мультисервисных сетей

Архитектура модуля

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 версией IOS 12.4(11)T или выше. Модуль поддерживается любым функциональным набором (feature set) операционной системы Cisco IOS, начиная с «IP base». При этом устройство работает независимо от ОС IOS-маршрутизатора, используя программное обеспечение, установленное на CF-карте модуля. Программное обеспечение устройства функционирует под управлением адаптированной ОС Linux.

Аппаратно модуль NME-RVPN (MCM) представляет собой вычислительную платформу на базе процессора Intel Celeron-M с тактовой частотой 1,0 ГГц, 512 Мбайт оперативной памяти и 512 Мбайт Compact Flash (см. рис. 4). Для подключения к локальной сети модуль оборудован внешним интерфейсом Gigabit Ethernet. Аналогичный внутренний интерфейс осуществляет взаимодействие и передачу данных между модулем и маршрутизатором.

Технические характеристики

Технические характеристики модуля NME-RVPN в исполнении MCM приведены в таблице 1.

Функциональные возможности

Функциональные возможности определяются установленным на модуле программным обеспечением. Функциональные возможности модуля NME-RVPN в исполнении MCM, использующего программный комплекс CSP VPN Gate 3.1 компании «С-Терра СиЭсПи», приведены в таблице 2.

Производительность

Производительность при использовании наиболее популярного алгоритма для создания IPsec-туннелей, включающего шифрование с проверкой целостности (ESP+HMAC), составляет 40 Мбит/с (измерения производились на больших UDP-пакетах длиной 1400 байт). Прочие значения показателей производительности для различных режимов работы IPSec см. в таблице 3.

Сертификация и государственное регулирование

Компания «С-Терра СиЭсПи» – технологический партнер компании Cisco Systems (Cisco Solution Technology Integrator). «С-Терра СиЭсПи» является производителем модуля NME-RVPN (MCM), а также разработчиком ПО CSP VPN Gate 3.1. Компания обладает необходимыми лицензиями ФСБ и ФСТЭК России, подробная информация доступна на странице http://www.sterra.com/CSP/RU/licenses/licenses.htm

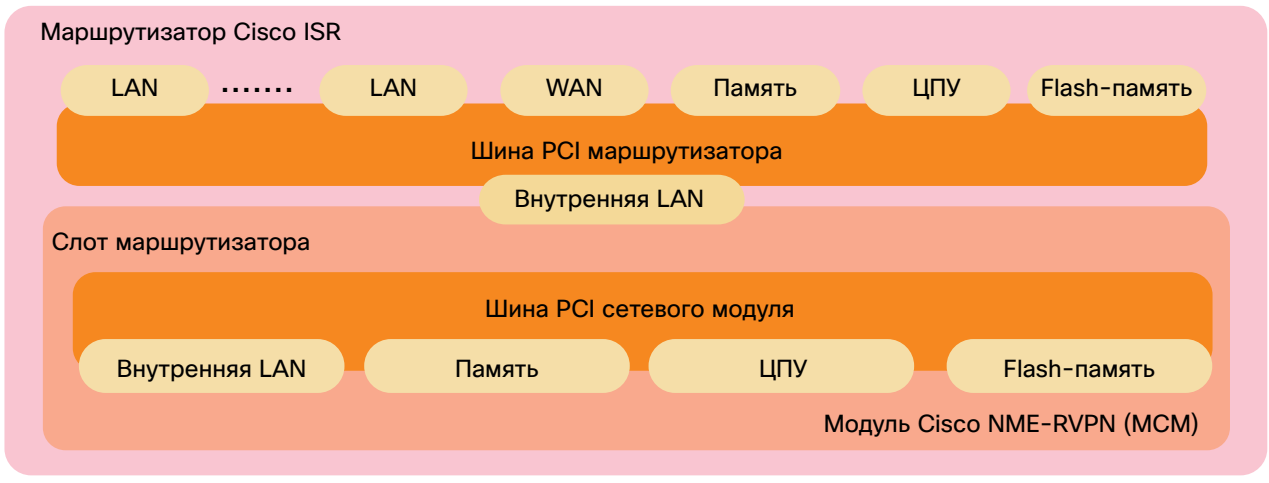

Рисунок 4. Архитектура модуля NME-RVPN (MCM) и маршрутизатора Cisco ISR

Модуль сетевой модернизированный NME-RVPN (MCM)

Модуль NME-RVPN (MCM) с программным обеспечением CSP VPN Gate версии 3.1 сертифицирован как средство криптографической защиты информации (СКЗИ) и удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» ФСБ России. Решение соответствует требованиям к средствам криптографической защиты информации класса КС1/КС2 и имеет сертификаты соответствия ФСБ СФ/114-1622 и СФ/114-1624 от 28 февраля 2011 г. Программное обеспечение CSP VPN Gate 3.1 обладает сертификатом соответствия ФСТЭК России № 2103. Сертификат подтверждает оценочный уровень доверия ОУД 3+, соответствие 3-му уровню контроля отсутствия недекларированных возможностей и возможность использования при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1-го класса включительно.

Сертифицированное программное обеспечение, работающее на базе модуля NME-RVPN (MCM), может применяться как в коммерческих структурах, так и в государственных органах.

Таблица 1. Технические характеристики модуля NME-RVPN (MCM)

Характеристика	Описание
Аппаратные характеристики модуля	
Процессор	Intel Celeron-M 1 ГГц
Память DRAM	512 Мбайт DDR2
Сетевые интерфейсы	• 1 внутренний интерфейс Ethernet 1000 Мбит/с • 1 внешний интерфейс Ethernet 10/100/1000 Мбит/с
Память Flash	512 Мбайт Compact Flash
Физические характеристики модуля	
Физические размеры (В x Ш x Д)	3,9 x 18,0 x 18,3 см
Вес	567 г
Относительная влажность при эксплуатации	от 5% до 95%, без конденсации
Температура эксплуатации	От 0 до 40 °C
Температура хранения	От -25 °C до 70 °C
Высота над уровнем моря при эксплуатации	До 3048 м при 25 °C
Потребляемая мощность	21 Вт
Сертификаты по электробезопасности	• Underwriters Laboratory 1950 • CSA-C22.2 No. 950 • EN 60950 • IEC 60950

Характеристика	Описание
Сертификаты по электромагнитной совместимости	• 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	• CISPR24 • EN300386 • EN50082-1 • EN55024 • EN61000-6-1
Соответствие российским требованиям по электробезопасности	• ГОСТ Р МЭК 60950-2002 (сертификат № РОСС US.ME61.B03697)
Соответствие российским требованиям к допустимому уровню шума	• ГОСТ 26329-84 (сертификат № РОСС US.ME61.B03697)
Соответствие российским требованиям к электромагнитной совместимости	• ГОСТ Р 51318.22-99 (сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51318.24-99 (сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51317.3.2-99 (сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51317.3.3-99 (сертификат № РОСС US.ME61.B03697)

Системные требования

Системные требования для модуля NME-RVPN (MCM) представлены в таблице 4.

Для установки модуля в маршрутизаторы Cisco ISR второго поколения требуется специальный адаптер (номенклатурный номер SM-NM-ADPTR). 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.

Заказы

Для бизнес-партнеров компании «С-Терра СиЭсПи» модуль NME-RVPN (MCM) доступен для заказа со склада этой компании. Конечные заказчики могут приобрести модуль у партнеров «С-Терра СиЭсПи», список которых представлен на следующей web-странице: http://www.s-terra.com/CSP/RU/partners/business_partners.htm.

По всем вопросам, связанным с приобретением модуля NME-RVPN (MCM), обращайтесь по адресу sales@s-terra.com.

Таблица 2. Функциональные возможности модуля NME-RVPN (MCM) при использовании CSP VPN Gate 3.1

Характеристика	Описание
Программная совместимость	Любые продукты, поддерживающие протоколы IKE/IPsec (RFC 2401 – RFC 2412)
Протоколы туннелирования	IPsec, NAT Traversal IPsec (NAT-T по draft-ietf-ipsec-nat-t-ike-03(02) и draft-ietf-ipsec-udp-encaps-03(02))
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, Preshared 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 (base64, bin), CRL
Маршрутизация	• Статическая маршрутизация • Управляемый политикой IPsec контроль фрагментации пакетов в канале • Обнаружение отказа удаленных узлов: IKE keep-alive extension - Dead Peer Detection (draft-ietf-ipsec-dpd-04) • Удаленный клиент IP, назначение IP из локального пула адресов (IKECFG)
Фильтрация	• IP-адрес (диапазон IP, сайт) источника и назначения • Порт 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 • Сообщения SNMP trap
Поддержка QoS	Отображение битов TOS поверх IPsec и приоритезация
Высокая доступность	• Распределение нагрузки, псевдокластер (n+1), поддержка
Управление	• Интерфейс командной строки CLI • Графический интерфейс Cisco Security Manager (CSM)

Таблица 3. Характеристики производительности модуля NME-RVPN (MCM) при использовании CSP VPN Gate 3.1

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.

Модуль сетевой модернизированный NME-RVPN (MCM)

Техническая поддержка

Техническая поддержка решений на базе модуля NME-RVPN (MCM) для конечных пользователей оказывается системными интеграторами, являющимися партнерами компании «С-Терра СиЭсПи».

По вопросам технической поддержки модуля NME-RVPN (MCM) вы можете обратиться в компанию «С-Терра СиЭсПи» по телефону +7 (499) 720 6958 или отправить сообщение на e-mail: support@sterra.com.

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

Резюме

Модуль NME-RVPN (MCM) с программным обеспечением CSP VPN Gate версии 3.1 имеет функциональность VPN-шлюза, работающего по протоколу IPSec с российскими криптографическими алгоритмами. Продукт сертифицирован как средство криптографической защиты информации (СКЗИ) класса КС2. Технологический процесс производства модуля согласован с ФСБ России. В системе сертификации ФСТЭК России получен сертификат, устанавливающий для продукта оценочный уровень доверия ОУД 3+, соответствие 3-му уровню контроля отсутствия недекларированных возможностей и возможность использования при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1-го класса включительно.

Модуль NME-RVPN (MCM) предназначен для использования на российских предприятиях, а также в государственных учреждениях и органах государственной власти. Решение обеспечивает оптимальный баланс надежности и производительности при высокой степени экономической эффективности.

Дополнительная информация

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

Для получения дополнительной информации по модулю NME-RVPN (MCM) отправьте запрос по адресу info@s-terra.com или sales@s-terra.com.

Таблица 4. Системные требования

Требование	Значение
Оборудование	• Маршрутизаторы Cisco ISR первого поколения (модели 2811, 2821, 2851, 3825 и 3845) • Маршрутизаторы Cisco ISR второго поколения (модели 2911, 2921, 2951, 3925 и 3945)
Программное обеспечение	Операционная система маршрутизатора Cisco IOS® версии 12.4(11)T или более поздней

Cisco
Россия,115054, Москва
бизнес-центр «Риверсайд Тауерс»
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, 197198, Санкт-Петербург
бизнес-центр «Арена Холл»
пр. Добролюбова, 16, лит. А, кор. 2
Телефон: +7 (812) 313 6230
Факс: +7 (812) 313 6280
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск
бизнес-центр «Росевроплаза»
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.**