

Решение CSP VPN Gate на платформе Cisco UCS C-200

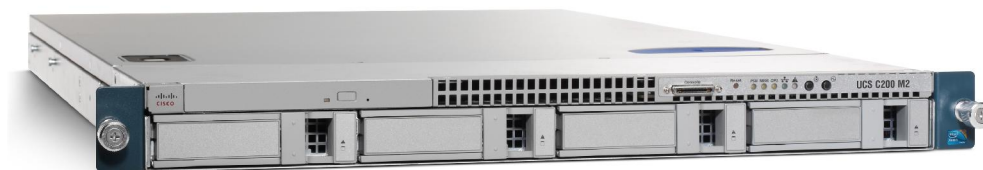
Решение CSP VPN Gate на платформе Cisco UCS C-200 представляет собой VPN-шлюз, реализующий стандартные механизмы защищенной передачи данных в сетях TCP/IP (IPSec) с применением российской криптографии.

Продукт разработан специально для обеспечения российского рынка высокотехнологичным решением в области интеграции приложений сетевой безопасности. Программное обеспечение CSP VPN Gate версии 3.1 сертифицировано ФСБ России как СКЗИ по классу КС1 или КС2 в зависимости от комплектации. 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, а также информационных систем персональных данных (ИСПДн) до 1 класса включительно. Таким образом, решение CSP VPN Gate версии 3.1 на платформе Cisco UCS C-200 применимо при работе с персональными данными и может использоваться как в корпоративном, так и в государственном секторе.

Обзор продукта

Решение CSP VPN Gate на платформе Cisco UCS C-200 предлагается для использования в средних и крупных организациях, для компаний с территориально распределенной структурой и для защиты каналов связи в современных центрах обработки данных. Оно отвечает требованиям потребителей, которым необходимы высокопроизводительные VPN-шлюзы для защиты каналов связи. Аппаратная платформа Cisco UCS позволяет существенно повысить производительность решения, сохранить компактность и обеспечить низкое энергопотребление. На платформе Cisco UCS C-200 представлены шлюзы CSP VPN Gate серий 3000 и 7000. Разные модели шлюзов отличаются уровнем производительности и функциональными возможностями. Это обеспечивает заказчикам возможность выбора оптимальной комплектации, в том числе и по критерию «цена/производительность».

Рисунок 1. Сервер Cisco UCS C200 M2



Преимущества и функциональные возможности продукта

Шлюз безопасности CSP VPN Gate на платформе Cisco UCS C-200 призван обеспечить российский рынок высокотехнологичным и высокопроизводительным VPN-решением, в котором сочетаются передовые технологии Cisco и российское сертифицированное программное обеспечение. Решение обеспечивает защиту данных при взаимодействии с внешними абонентами, беспроводных коммуникаций, передачу голоса и видео с обеспечением качества обслуживания, а также обеспечивает безопасность взаимодействия клиентов в сетях операторов связи и провайдеров услуг. Представленное решение предназначено для использования не только в корпоративном, но и в государственном секторе, т. к. программное обеспечение сертифицировано ФСБ России как средство криптографической защиты информации по классу КС1 или КС2 в зависимости от комплектации.

В решение интегрированы российские криптографические стандарты, развитые средства маршрутизации, средства поддержки механизмов качества обслуживания приоритетного трафика

(QoS), сервисы IP-телефонии и видео, средства коммутации сетей. Серверы Cisco UCS C-200 являются оптимальной платформой для применения в качестве выделенных высокопроизводительных устройств для защиты канала связи в распределенных центрах обработки данных и построения отказоустойчивых систем и систем с балансировкой нагрузки. Компактность и высокая производительность оборудования, богатая функциональность, управляемость и надежность технологий отвечает требованиям современных организаций к защите критически важных сетевых взаимодействий.

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.

Высокая производительность наряду с поддержкой непрерывности бизнес-процессов и механизмами обеспечения качества обслуживания (QoS), отказоустойчивость, возможность использования конфигураций с резервированием и балансировкой нагрузки, а также средства создания RAID-массивов (в конфигурации G-7000-S-9104-6-RED-CP) позволяют использовать решение для обеспечения защищенного взаимодействия между центрами обработки данных (ЦОД).

Защита беспроводных и мультисервисных сетей

В современных экономических условиях для успешного ведения бизнеса необходимо оперативно взаимодействовать с коллегами, партнерами и заказчиками вне зависимости от их местонахождения. При этом немаловажным фактором является само качество связи. Рассматриваемые решения поддерживают сценарии защиты как выделенных мультисервисных, так и смешанных сетей. При этом высокий уровень производительности решения позволяет избежать задержек при обработке трафика, т. е. сохраняется высокое качество обслуживания (QoS). Это особенно важно при защите мультисервисного трафика, когда одновременно передаются обычные данные, видео- и голосовые данные, а также обрабатываются сеансы видеоконференцсвязи. Данные решения могут также использоваться для защиты каналов связи платформы Cisco TelePresence.

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).

В качестве клиента для организации удаленного доступа пользователей может применяться CSP VPN Client версии 3.1, который, как и CSP VPN Gate версии 3.1, является сертифицированным средством криптографической защиты информации (СКЗИ) класса КС1.

Архитектура шлюза

Решение представлено в пяти комплектациях. Подробное описание каждой комплектации (характеристики аппаратной платформы) представлено в таблице 1.

Таблица 1. Комплектации решения

Артикул	Аппаратная платформа Cisco UCS C200 M2
G-3000-S-9100-2-CP	<ul style="list-style-type: none"> Процессор Intel Xeon E5504, частота 2,0 ГГц 2 Гбайт оперативной памяти 1 диск SATA 2 порта Gigabit Ethernet Установка в стойку, форм-фактор 1U
G-3000-S-9101-2-CP	<ul style="list-style-type: none"> Процессор Intel Xeon E5520, частота 2,26 ГГц 2 Гбайт оперативной памяти 1 диск SATA 2 порта Gigabit Ethernet Установка в стойку, форм-фактор 1U
G-3000-S-9102-2-CP	<ul style="list-style-type: none"> Процессор Intel Xeon E5540, частота 2,53 ГГц 2 Гбайт оперативной памяти 1 диск SATA 2 порта Gigabit Ethernet Установка в стойку, форм-фактор 1U
G-7000-S-9103-2-CP	<ul style="list-style-type: none"> 2 процессора Intel Xeon E5520, частота 2,26 ГГц 4 Гбайт оперативной памяти 1 диск SATA 2 порта Gigabit Ethernet Установка в стойку, форм-фактор 1U
G-7000-S-9104-6-RED-CP	<ul style="list-style-type: none"> 2 процессора Intel Xeon X5570, частота 2,93 ГГц 4 Гбайт оперативной памяти 6 портов Gigabit Ethernet 2 диска SATA (в RAID 1) 2 блока питания Установка в стойку, форм-фактор 1U

Аппаратная платформа

Серверы серии Cisco UCS C-200 отличаются высокой производительностью. Платформа оборудована дополнительными устройствами, позволяющими расширить ее функциональность (блоки питания, сетевые карты, включая матрицу коммутации с пропускной способностью 10 Гбит/с). Следует также отметить низкий уровень энергопотребления и компактность серверов Cisco UCS C-200.

Более подробное описание возможностей и преимуществ аппаратной платформы приведено в таблице 2.

Таблица 2. Преимущества платформы Cisco UCS C-200

Возможности	Преимущества
Унифицированная матрица коммутации (10 Гбит/с)	<ul style="list-style-type: none"> Матрица коммутации, поддерживающая технологии Fibre Channel over Ethernet (FCoE) и Ethernet 10 Гбит/с, с малыми задержками и без потерь пакетов. Простое подключение к сети, для которого требуется меньшее количество кабелей и портов.
2 встроенных порта Gigabit Ethernet	<ul style="list-style-type: none"> Высокая производительность, увеличенная эффективность и гибкость сетевых функций. Высокая доступность сети при настройке отказоустойчивой конфигурации.
Шестиядерные процессоры Intel Xeon 5600	<ul style="list-style-type: none"> Автоматическое управление производительностью и энергопотреблением в соответствии с требованиями приложений. Автоматический перевод процессора и оперативной памяти в режим наименьшего энергопотребления при сохранении необходимого быстродействия.
Поддержка до 2 слотов PCIe 2.0	<ul style="list-style-type: none"> Гибкость, повышенная пропускная способность и совместимость с отраслевыми стандартами. Слоты PCIe 2.0 предоставляют удвоенную пропускную способность при сохранении совместимости с PCIe 1.1. Имеет в составе 2 слота PCIe x8: 1 низкопрофильный слот половинной длины и 1 слот полной высоты половинной длины.

Таблица 2. Преимущества платформы Cisco UCS C-200 (продолжение)

Возможности	Преимущества
Унификация управления (при интеграции с Cisco Unified Computing System)	<ul style="list-style-type: none"> Единое эффективное и гибкое управление всем решением с помощью Cisco UCS Manager. Сервисные профили и шаблоны для управления с использованием ролевой модели контроля доступа и политик позволяют эффективно работать администраторам сетей, серверов и хранилищ данных. Процедуры автоматизации установки позволяют разворачивать приложения за считанные минуты вместо нескольких дней.
Диски SAS и SATA с возможностью "горячей" замены	<ul style="list-style-type: none"> До 4 внутренних 3,5 дюймовых дисков SAS или SATA, доступных с передней панели сервера, с возможностью "горячей" замены. Возможность выбора дисков для обеспечения баланса производительности и емкости: <ul style="list-style-type: none"> диски SAS 15 000 об/мин: максимальная производительность; диски SAS 7 200 об/мин: большая емкость, высокая производительность; недорогие диски SATA II 7 200 об/мин: максимальная емкость.
Поддержка RAID 0, 1, 5, 6, и 10	<ul style="list-style-type: none"> Выбор из 3 типов RAID-контроллеров с поддержкой до 4 дисков SAS или SATA: <ul style="list-style-type: none"> встроенный контроллер для дисков SATA в режиме RAID 0, 1; RAID 0, 1 для дисков SAS или SATA с использованием мезанинного контроллера; контроллер PCIe LSI MegaRAID для дисков SAS с поддержкой RAID 0, 1, 5, 6 и 10.
Встроенный контроллер управления Cisco UCS	<ul style="list-style-type: none"> Web-интерфейс для управления серверами, виртуализированным окружением, поддержка удаленной работы с клавиатурой, монитором и мышью (KVM). Удаленная поддержка CD- и DVD-дисков при работе через KVM. Поддержка Intelligent Platform Management Interface (IPMI) 2.0 для внеполосного управления с использованием продуктов сторонних поставщиков. Интерфейс командной строки (CLI) для управления серверами.
Поддержка скоростных модулей DRAM	12 слотов для модулей DIMM, позволяющих сформировать подсистему оперативной памяти общим объемом до 96 Гбайт памяти (1333 МГц) для оптимальной производительности.
Резервируемые вентиляторы и источники питания	Резервирование вентиляторов и источников питания для обеспечения высокой надежности

Функциональные возможности

Шлюзы безопасности CSP VPN Gate версии 3.1 предоставляют уникальное сочетание работы в сетях IPsec и создания защищенных каналов с помощью российских криптографических стандартов. Решение сертифицировано: в системе сертификации ФСБ России как средство криптографической защиты информации (СКЗИ) по классам КС1 и КС2; в системе сертификации ФСТЭК России как программное средство общего назначения со встроенными средствами защиты от несанкционированного доступа, которое может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1 класса включительно. Сертификация позволяет использовать решение в качестве средства защиты персональных данных.

На платформе Cisco UCS C-200 используются шлюзы CSP VPN Gate различной производительности, что позволяет заказчику гибко подойти к решению своих задач. Программное обеспечение поддерживает различное количество туннелей (CSP VPN Gate 3000 – от 500 до 1000 туннелей одновременно; CSP VPN Gate 7000 – неограниченное количество туннелей) и демонстрирует разную производительность – от 800 до 3100 Мбит/с (измерения производились при использовании потока UDP-пакетов размером 1400 байт). Кроме того, решение может предоставить расширенную функциональность — зеркалирование жестких дисков и дублирование блоков питания для обеспечения отказоустойчивой конфигурации.

В результате заказчик получает возможность внедрить продукт именно в той комплектации, которая наиболее эффективна для организации защиты сетей в его компании. При этом он не несет дополнительных расходов.

Функциональные возможности решения в целом обусловлены функциональными возможностями программного обеспечения CSP VPN Gate 3.1. Они представлены в таблице 3.

Таблица 3. Функциональные возможности решения

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	<ul style="list-style-type: none"> • 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 (base64, bin), CRL
Маршрутизация	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • IP-адрес (диапазон IP, сайт) источника и назначения • Порт и тип протокола • Обработка фрагментированных пакетов
Настройка и управление	<ul style="list-style-type: none"> • 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 приоритизация очередей QoS для обеспечения работы IP-телефонии и видео
Высокая доступность	<ul style="list-style-type: none"> • Распределение нагрузки, псевдокластер (n+1), поддержка IPsec-соединений. • Обнаружение потери соединения (draft-ietf-ipsec-dpd-04), восстановление соединения • Поддержка протокола RRI
Управление	<ul style="list-style-type: none"> • Интерфейс командной строки CLI • Графический интерфейс Cisco Security Manager (CSM)

Производительность

Производительность при использовании наиболее популярного алгоритма для создания IPsec-туннелей, включающего шифрование с проверкой целостности (ESP+HMAC), составляет от 800 до 1300 Мбит/с (измерения производились на больших UDP-пакетах длиной 1400 байт) в зависимости от применяемой аппаратной платформы.

Таблица 4. Производительность решения в зависимости от аппаратной платформы

Используемый алгоритм	Значение*
G-3000-S-9100-2-CP	800 Мбит/с
G-3000-S-9101-2-CP	1520 Мбит/с
G-3000-S-9102-2-CP	1700 Мбит/с
G-3000-S-9103-2-CP	2480 Мбит/с
G-3000-S-9104-6-RED-CP	3100 Мбит/с

* Измерено при использовании потока UDP-пакетов размером 1400 байт.

Технические характеристики

Технические характеристики решения определяются характеристиками, присущими аппаратной платформе.

Таблица 5. Технические характеристики решения

Характеристика	Описание
Физические размеры (В x Ш x Д)	1RU: 4,32 x 42,93 x 70,61 см
Температура эксплуатации	От +10 до +35 °C
Температура хранения	От -40 °C до +65 °C
Относительная влажность при эксплуатации	От 5% до 93%, без конденсации
Относительная влажность при хранении	От 5% до 93%, без конденсации
Высота над уровнем моря при эксплуатации	До 3 000 м
Высота над уровнем моря при хранении	До 12 000 м
Сертификаты по электробезопасности	<ul style="list-style-type: none"> • UL 60950-1 No. 21CFR1040 • CAN/CSA-C22.2 No. 60950-1 • IRAM IEC60950-1 • CB IEC60950-1 • EN 60950-1 • IEC 60950-1 • ГОСТ IEC60950-1 • SABS/CB IEC6095-1 • CCC*/CB GB4943-1995 • CNS14336 • CB IEC60950-1 • AS/NZS 60950-1 • GB4943
Сертификаты по электромагнитной совместимости	<ul style="list-style-type: none"> • 47CFR Part 15 (CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR2 2 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A
Сертификаты по электромагнитной помехоустойчивости	<ul style="list-style-type: none"> • EN55024 • CISPR24 • KN 610000-4 Series, KN 24
Соответствие российским требованиям по электробезопасности	<ul style="list-style-type: none"> • ГОСТ Р МЭК 60950-1-2005
Соответствие российским требованиям к допустимому уровню шума	<ul style="list-style-type: none"> • ГОСТ 26329-84
Соответствие российским требованиям к электромагнитной совместимости	<ul style="list-style-type: none"> • ГОСТ Р 51318.22-99 • ГОСТ Р 51318.24-99 • ГОСТ Р 51317.3.2-2006 • ГОСТ Р 51317.3.3-2008

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.s-terra.com/CSP/RU/licenses/licenses.htm>

Шлюз безопасности 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 СКЗИ и имеет сертификат соответствия СФ/114-1411 от 20 марта 2010 г.

Сертификат подтверждает, что средство криптографической защиты информации CSP VPN Gate версии 3.1 соответствует классу защиты КС1. Такой же класс защиты имеет продукт CSP VPN Client версии 3.1, который может применяться совместно с CSP VPN Gate для организации удаленного доступа пользователей. При использовании в составе решения аппаратно-программного средства защиты информации от несанкционированного доступа решение соответствует классу защиты КС2.

Программное обеспечение CSP VPN Gate 3.1 обладает сертификатом соответствия ФСТЭК России № 2103, CSP VPN Server 3.1 — № 2102, CSP VPN Client 3.1 — № 2104. Сертификаты подтверждают для этих продуктов оценочный уровень доверия ОУД 3+, соответствие 3 уровню контроля отсутствия недеklarированных возможностей и возможность использования этих продуктов при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1 класса включительно.

Сертифицированное программное обеспечение CSP VPN Gate версии 3.1 может применяться как в коммерческих структурах, так и в государственных органах.

ЗАКАЗЫ

Для бизнес-партнеров «С-Терра СиЭсПи» решение CSP VPN Gate версии 3.1 на платформе UCS C-200 доступно для заказа со склада этой компании. Конечные заказчики могут приобрести решение 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 решения, обращайтесь по адресу sales@s-terra.com.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка шлюзов безопасности CSP VPN Gate версии 3.1 для конечных пользователей оказывается системными интеграторами, являющимися партнерами компании «С-Терра СиЭсПи».

По вопросам технической поддержки CSP VPN Gate версии 3.1 на платформе Cisco UCS C-200 вы можете обратиться в компанию «С-Терра СиЭсПи» по телефону +7 (499) 720 6958 или отправить сообщение на e-mail: support@s-terra.com.

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

РЕЗЮМЕ

Решение CSP VPN Gate версии 3.1 на платформе Cisco UCS C-200 имеет функциональность VPN-шлюза, работающего по протоколу IPSec с российскими криптографическими алгоритмами. Продукт сертифицирован ФСБ России как средство криптографической защиты информации (СКЗИ) по классам КС1 и КС2. В системе сертификации ФСТЭК России получены сертификаты, устанавливающие 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.

Решение предназначено для использования на российских предприятиях, а также в государственных учреждениях и органах государственных власти. Оно 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 решению CSP VPN Gate отправьте запрос по адресу info@s-terra.com или sales@s-terra.com.



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, Altonet, 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)