



ОФИЦИАЛЬНЫЙ ДОКУМЕНТ

ПЯТЬ ВАЖНЕЙШИХ ПРОБЛЕМ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Компания Cisco предлагает стратегию самозащищающейся сети **Self-Defending Network**, разработанную для предприятий малого и среднего бизнеса.

РЕЗЮМЕ

Предприятия малого и среднего бизнеса используют Интернет и сетевые прикладные системы для привлечения новых клиентов и более эффективного обслуживания существующих пользователей. В то же время непрерывно появляющиеся угрозы безопасности и проблемы законодательного порядка оказывают возрастающее давление на бизнес-ориентированные сети, требуя от них повышенной надежности и безопасности. Компания Cisco® предлагает эффективные, доступные и интегрированные решения по безопасности, предназначенные для предприятий малого и среднего бизнеса, которые должны помочь обеспечить информационную целостность бизнеса, сохранить конфиденциальность информации клиента и снизить эксплуатационные расходы. В результате предприниматели смогут уделять больше времени развитию своего бизнеса, сокращая временные затраты на решение проблем сетевой безопасности.

ЗАДАЧИ БИЗНЕСА

Охваченный глобальной конкурентной борьбой современный деловой мир в лице предприятий малого и среднего бизнеса нацелен на расширение своей коммерческой деятельности и повышение степени удовлетворенности своих клиентов при одновременном контроле уровня расходов. К счастью, Интернет и сетевые приложения выровняли условия для действующих на рынке игроков. Предприятия малого и среднего бизнеса используют свои сети для расширения рыночных возможностей и организации взаимодействия со своими клиентами и партнерами, действуя при этом оперативно и экономно. Однако быстрый и динамичный электронный бизнес — это палка о двух концах, доступ к этим средствам вскрывает дорогостоящие проблемы обеспечения информационной безопасности. Вследствие этого необходимость иметь надежную, безопасную и доступную сеть ощущается очень остро.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Согласно последним исследованиям, безопасность — это самая серьезная проблема, с которой столкнулись предприятия малого и среднего бизнеса. Непрерывно меняющиеся угрозы безопасности как с внешней, так и с внутренней стороны бизнес-ориентированной сети могут внести хаос в деловые операции, отрицательно воздействуя на прибыльность сделок и удовлетворенность клиентов. Кроме того, предприятия малого и среднего бизнеса должны отвечать требованиям новых нормативных актов и законов, разработанных для защиты частной собственности потребителя и обеспечения безопасности электронной информации.

Проблема безопасности 1: черви и вирусы

Компьютерные черви и вирусы остаются наиболее распространенной угрозой безопасности — ежегодно 75% предприятий малого и среднего бизнеса испытывают атаку хотя бы одного вируса*. Черви и вирусы способны оказать разрушающее воздействие на целостность коммерческой информации и эффективность бизнеса. Наделенные мощным интеллектом вредоносные «щупальца» распространяются гораздо быстрее, чем раньше, в секунды заражая весь офис. Очистка зараженных компьютеров требует гораздо большего времени. Катастрофические последствия выливаются в потерянные заказы, разрушенные базы данных и разгневанных клиентов. Поскольку предприниматели стремятся обновить свои компьютеры за счет установки последних версий операционных систем и антивирусных программ, новые вирусы могут в любой день недели проникнуть через их защитные барьеры. В то же время сотрудники непреднамеренно распространяют вирусы и программы-шпионы, обращаясь к зараженным web-сайтам, загружая непроверенные файлы или открывая инфицированные сообщения электронной почты.

* По результатам Maritz Research, 2005 г.

Подобные атаки, реализуемые зачастую без всякого умысла, вместе с тем наносят организациям заметный финансовый ущерб. Системы безопасности должны обнаруживать и уничтожать червей, вирусы и программы-шпионы во всех точках сети.

Проблема безопасности 2: хищение информации

Сегодня хищение информации представляется серьезной проблемой. Злостные хакеры проникают в коммерческие сети с целью снятия средств по кредитным карточкам или кражи средств, используя номера страховых полисов. Предприятия малого и среднего бизнеса находятся в зоне риска, поскольку на фоне больших корпораций они выглядят этакими простаками. Защита сети по всему периметру представляется толковым первым шагом, но этого недостаточно, поскольку многие киберворы имеют доверенных сообщников внутри сети в лице сотрудников или подрядчиков.

Утечки информации могут дорого обойтись предприятиям малого и среднего бизнеса, поскольку главное, что двигает их бизнес, – это удовлетворенные клиенты и незапятнанная репутация. Предприниматели, которые в недостаточной степени защищают свою информацию, могут столкнуться с такими проблемами, как разглашение конфиденциальной для них информации, наложение штрафов со стороны государственных органов и даже судебное преследование. Так, например, новые законы в защиту интересов потребителей, принятые в штате Калифорния, требуют от любого предпринимателя, который подозревает, что информация его клиента стала известна посторонним людям, уведомить об этом ВСЕХ своих клиентов. В России также существуют законы, предусматривающие наказание за нарушение правил обработки конфиденциальной информации или персональных данных. Любая стратегия безопасности должна предотвращать кражу электронной информации как снаружи, так и внутри сети.

Проблема безопасности 3: угроза эффективности бизнеса

Компьютерные черви и вирусы могут существенно снизить надежность сетевых ресурсов, которые, в свою очередь, сказываются на способности предпринимателей оперативно реагировать на запросы своих клиентов, хотя черви и вирусы представляют угрозу не только для эффективности бизнеса. Имея дело с сетями, которые столь критичны к современным коммерческим операциям, кибертеррористы занялись шантажом предпринимателей, угрожая выведением из строя web-сайтов и операций электронной коммерции, если их требования не будут удовлетворены. Подобные атаки, приводящие к отказу от обслуживания (Denial of Service, DoS), посылают большие объемы трафика на критический элемент сети, вызывая выход его из строя или лишая его возможности обработать нормальный трафик. И опять последствия катастрофичны: информация и заказы теряются, а запросы клиентов остаются без ответа. Если данные атаки становятся достоянием общественности, то это отрицательно сказывается на кредите доверия компании и ее репутации.

В то время как основное внимание защите от последствий DoS-атак уделяется в крупных банках и крупных компаниях, предприятия малого и среднего бизнеса остаются пока незащищенными. Можно без труда увидеть, что они гораздо хуже подготовлены к атакам, чем крупные корпорации. Известно много других, менее опасных, но более реальных атак, которые угрожают эффективности работы предприятий малого и среднего бизнеса и, соответственно, их доходности и взаимоотношениям с клиентами. К примеру, атака, связанная с кражей ресурсов, проникает в коммерческие компьютеры и сети, используя их для незаконного совместного просмотра музыкальных программ, фильмов или программных средств. Чаще всего предприниматели и не подозревают о происходящем. А в это время их компьютеры и сети не в состоянии быстро ответить клиентам, а их невольное участие в совместном использовании запрещенных файлов может стать причиной судебного разбирательства.

Проблема безопасности 4: неизвестность

С каждым новым открытием в сферах компьютерной техники и коммуникаций всегда найдется искусный хакер, который отыщет способы использовать эту технологию для своей выгоды или из озорства. Вновь появляющиеся аппаратные и программные средства предоставляют новые возможности. Одноранговые коммуникации (P2P) и передача мгновенных сообщений по Интернету (Instant Messaging, IM) продолжали оставаться сравнительно новыми приложениями, когда их пользователи были атакованы специально написанной для них программой. А с недавних пор вирусы выбрали для себя новую цель – мобильные телефоны. Никто не знает, что будет следующим, но лучше всех будет защищен тот, кто сможет легко приспособиться к будущим угрозам, не ломая при этом свой бизнес.

Проблема безопасности 5: законодательная база

Помимо перечисленных злонамеренных угроз безопасности, новые законы и нормативные акты требуют, чтобы предприятия малого и среднего бизнеса обеспечивали конфиденциальность и целостность доверенной им информации. Страны Европейского Союза и многие отдельные страны, в т. ч. и Россия, приняли или примут в ближайшем времени законы, которые

определяют условия защиты персональных данных, которыми располагают организации. Кроме того, страны приняли дополнительные законодательные акты, касающиеся защиты специализированной информации типа сведений о состоянии здоровья населения. Так, например, принятый в США Закон об отчетности и использовании данных в сфере медицинского страхования (HIPAA) требует от организаций здравоохранения, вплоть до каждого медицинского учреждения, применять меры по защите сведений о состоянии здоровья их пациентов и исключения несанкционированного доступа к ним. Аналогичные требования есть и в России для защиты врачебной тайны. Ответственность за соблюдение законов и нормативных актов, касающихся их бизнеса и рынков, ложится на предпринимателей. К сожалению, многие мелкие предприниматели находят, что средства, которыми они располагают, не позволяют им пойти так далеко.

Между тем клиенты хотят иметь гарантию, что информация, которую они доверили предпринимателям, сохраняется в тайне. Все бизнесмены должны принимать меры по защите своих коммерческих инфраструктур, но именно предприятия малого и среднего бизнеса в первую очередь нуждаются в простых, компактных и приемлемых решениях. Cisco разработала решение по безопасности специально для предприятий малого и среднего бизнеса (SMB), которое построено на стратегии самозащищающейся сети Cisco Self-Defending Network.

САМОЗАЩИЩАЮЩАЯСЯ СЕТЬ CISCO

Самозащищающаяся сеть Cisco (Self-Defending Network, SDN) – это долгосрочная стратегия компании по защите бизнес-процессов путем выявления, предотвращения и адаптации к внешним и внутренним угрозам. Самозащищающаяся сеть Cisco позволяет обезопасить сегодняшний бизнес и адаптироваться к грядущим требованиям. С компанией Cisco предприниматели могут защитить не только свои сети, но и свои инвестиции в сетевую инфраструктуру. В результате они получают улучшенные бизнес-процессы и реальную экономию средств.

Самозащищающаяся сеть Cisco обладает тремя уникальными свойствами, это: интеграция, взаимодействие и адаптируемость. Во-первых, она интегрирует средства безопасности во все элементы сети, гарантируя, что каждая точка в сети будет защищать себя как от внешних, так и от внутренних угроз. Во-вторых, такие сетевые элементы работают совместно, обмениваясь информацией и обеспечивая тем самым дополнительную защиту. В-третьих, сеть использует новейшие средства распознавания по поведенческим признакам для адаптации к новым угрозам по мере их нарастания.

Концепция Cisco Secure Network Foundation представляет собой упрощенное, но при этом эффективное и экономичное решение по безопасности для предприятий малого и среднего бизнеса, которое создает надежные и самозащищающиеся сети.

ОБЗОР КОНЦЕПЦИИ SECURE NETWORK FOUNDATION

Решение Cisco Secure Network Foundation позволяет предприятиям малого и среднего бизнеса сосредоточить свои усилия на вопросах получения прибыли, а не на проблемах сети. Решение включает необходимые механизмы безопасности для всех пользователей – и проводных, и беспроводных. Эти механизмы безопасности встраиваются в маршрутизаторы, коммутаторы и выделенные устройства защиты Cisco, помогая предприятиям малого и среднего бизнеса упрощать операции и снижать расходы.

Решение Cisco Secure Network Foundation основано на стратегии самозащищающейся сети Cisco, которая позволяет обезопасить современные сети и учитывает требования по безопасности завтрашнего дня. Предприниматели могут продолжать работать даже под давлением атак и выполнять требования как клиентов, так и законодательных актов относительно защиты данных и сохранения их конфиденциальности.

Быть открытым для бизнеса, даже находясь под прицелом атак

С ростом угрозы атак предприниматели и клиенты нуждаются в гарантиях, что они защищены от потрясений и нарушений возможности оказывать платные услуги или от искаженных обрабатываемых данных. Опробованное на практике решение Cisco Self-Defending Network представляет собой многофункциональный и эшелонированный подход, который защищает предпринимателей от губительных эффектов воздействия червей, вирусов, кибертеррористов и прочих угроз.

Компьютерные вирусы, черви и программы-шпионы обычно проникают в компьютерные сети через электронную почту или Интернет-пейджеры в результате загрузки с web-сайтов или пересылки файлов, а более хитроумные атаки могут проникать через беспроводные сети или средства мобильной связи. Наиболее прогрессивные в отрасли системы предотвращения атак (Cisco Intrusion Prevention Systems) просматривают и проверяют любой входящий трафик в реальном времени, стараясь обнаружить известные атаки или иные аномалии, которые могут свидетельствовать об атаке. При обнаружении несанкционированной активности устройство защиты Cisco оценивает степень опасности и оповещает о ней все остальные средства обеспечения сетевой безопасности. Таким способом они могут приостановить угрозу в самом зародыше, не допуская ее распространения по сети.

Черви, вирусы и программы-шпионы – это не единственные способы атаки коммерческих сетей. Для обнаружения и ликвидации DoS-атак и прочих вторжений, настолько новых, что даже не имеющих название, устройства защиты Cisco используют специальные возможности по проверке трафика и приложений в поисках еще неизвестных нападений.

Интегрированные в бизнес средства обеспечения безопасности останавливают в реальном времени известные и неизвестные атаки, а существующая между сетевыми компонентами связь позволяет им адаптироваться к изменяющимся условиям безопасности. Данное решение позволяет предприятиям малого и среднего бизнеса продолжать оперативно обслуживать клиентов и оставаться открытыми для бизнеса даже под прицелом атак.

Сохранение конфиденциальности информации клиента

Решение Cisco Secure Network Foundation использует множество средств для защиты информации клиента от доступа несанкционированных пользователей, находящихся как внутри, так и снаружи сети. Виртуальные частные сети (VPN) дают возможность небольшим офисам и мобильным сотрудникам взаимодействовать между собой и со своим головным офисом в условиях полной конфиденциальности, даже используя для передачи сообщений открытую сеть Интернет. Наилучшие в отрасли стандарты аутентификации гарантируют доступ к сети VPN только проверенных пользователей и устройств. Мощные средства криптографической защиты делают информацию непонятной для любого, кто пытается проникнуть в каналы связи VPN через сети общего пользования.

Межсетевые экраны и средства предотвращения атак (IPS) на каждой сетевой точке входа помогают остановить червей, программы-шпионы или попытки хакеров проникнуть в коммерческие сети с целью кражи информации. Кроме того, межсетевые экраны очень эффективны в вопросах предотвращения доступа внутренних пользователей к важной информации. Так, например, использование межсетевых экранов для внутренних целей может предотвратить доступ несанкционированных лиц к финансовой информации, данным отдела кадров или компьютерам бухгалтерии, либо к просмотру этих типов трафиков. Виртуальные локальные сети (VLAN) позволяют предпринимателям продолжать сегментировать внутренние каналы связи в пределах своих организаций. Важная финансовая или клиентская информация может быть помещена в собственную сеть VLAN, логически отделенную от рабочих локальных сетей.

Решение Cisco Secure Network Foundation помогает предпринимателям соблюдать законодательные требования относительно безопасности и конфиденциальности клиентской информации за счет защиты сети от нарушений безопасности или несанкционированных вторжений в сеть как изнутри, так и снаружи.

Контроль расходов

Решение Cisco Secure Network Foundation помогает предприятиям малого и среднего бизнеса контролировать расходы двумя способами: во-первых, путем исключения ненужных расходов, связанных с нарушениями требований безопасности, и во-вторых, за счет использования многофункциональных, эффективно интегрируемых элементов обеспечения безопасности, которые наращиваются и масштабируются по мере изменения требований. Интегрированная безопасность упрощает затраты на управление и сопровождение сети, снижая суммарные расходы на владение сетью.

За решением проблем обеспечения сетевой безопасности стоят как очевидные, так и скрытые расходы. К примеру, многие угрозы безопасности, такие как относительно безобидные вирусы, наносят незначительный вред, и связанные с ними очевидные расходы определяются временными и людскими затратами на очистку инфицированных коммерческих систем. Расходы растут с увеличением количества инфицированных систем, что делает их защиту и быстрое обнаружение источником экономии средств. Менее очевидные расходы связаны с рабочим временем, потерянным пользователями инфицированных компьютеров из-за их чистки. В качестве примеров скрытых расходов можно привести упущенные возможности, потерю клиентов, ухудшение деловой репутации или судебные издержки, связанные с несоблюдением требований безопасности. Подобные расходы, хотя и не столь частые, могут быть очень значительными. В прошлом 2005 году компьютерные преступления стоили Великобритании 2,4 млрд фунтов стерлингов (по данным National Hi-Tech Crime Unit).

Решение Cisco Secure Network Foundation помогает предпринимателям избежать как очевидных, так и скрытых расходов, связанных с решением проблем безопасности, снижая коммерческий риск и повышая доверие и приверженность со стороны своих клиентов. Предприятия малого и среднего бизнеса не располагают людскими ресурсами или финансовыми возможностями для развертывания и сопровождения сложных решений по безопасности. Решение Cisco Secure Network Foundation представляется безопасным, надежным и простым средством, снижающим общие затраты на владение сетью, так что организации могут сосредоточить свои усилия на решении проблем бизнеса, а не сетевых проблем. Это решение легко адаптируется к изменяющимся коммерческим требованиям и условиям безопасности, обеспечивая пропорциональность роста расходов темпам развития бизнеса.

Реализация решения Secure Network Foundation

Решение Cisco Secure Network Foundation построено на базе двух основных товарных семейств – семейства маршрутизаторов с интегрированными сервисами (Cisco Integrated Services Router, ISR) и семейства многофункциональных защитных устройств Cisco ASA 5500 (Cisco ASA 5500 Series Adaptive Security Appliance). Данные решения закладывают основы самозащищающихся сетей Cisco для предприятий малого и среднего бизнеса.

Как следует из их названия, устройства Cisco ISR объединяют множество функций в отдельной надежной и эффективной платформе маршрутизации, ориентированной на домашние офисы или сети малого и среднего размера. Маршрутизатор Cisco ISR выполняет функции маршрутизатора широкополосного доступа DSL и обладает встроенными функциями резервирования каналов связи, коммутатора ЛВС, беспроводной точки доступа и коммутатора беспроводной ЛВС – и все это в одном устройстве. Поскольку эти функциональные возможности могут добавляться в устройства Cisco ISR по мере необходимости, они могут без труда настраиваться под изменяющиеся требования предприятия малого и среднего бизнеса. Кроме того, они охватывают многие основные функции безопасности, включая возможности межсетевых средств защиты, систем предотвращения атак и сетей VPN.

Решение Cisco ASA 5500 Series Adaptive Security Appliance представляет собой семейство высокопроизводительных, интегрированных устройств безопасности, построенное на апробированной технологии безопасности Cisco, которая оперативно реагирует на известные и неизвестные угрозы и адаптируется к требованиям защиты от них. Устройство Cisco ASA 5500 Series объединяет в себе наиболее эффективные функции межсетевых экранов Cisco Pix, систем отражения вторжений Cisco IPS, сетевых антивирусов, а также проверку приложений и построение VPN для удаленного доступа или межофисного взаимодействия. Устройство Cisco ASA 5500 обеспечивает высочайший уровень защиты от несанкционированного доступа пользователей, червей, вирусов, программ-шпионов, а также от опасных или вредоносных приложений. Данное компактное устройство, объединяющее в себе проверенные рынком технологии безопасности, предназначено для современных сетей предприятий малого и среднего бизнеса. Оно экономически эффективно в эксплуатации, легко устанавливается, сопровождается и допускает модернизацию. По мере возрастания угроз сетевой безопасности устанавливаемые пользователем расширения и модификации позволяют продуктам Cisco ASA адаптироваться к новым условиям и продолжать успешно защищать коммерческие сети.

Устройство Cisco ASA 5500 Series – отличный вариант для установки в главном офисе или в офисе филиала, где требуется высокий уровень информационной безопасности. Дополнительным компонентом в решении Cisco Secure Network Foundation является коммутатор Cisco Catalyst® Express 500 Series – простое и эффективное устройство безопасности, специально разработанное для предприятий малого и среднего бизнеса. Все коммутаторы Cisco Catalyst содержат функции безопасности, которые обнаруживают аномалии трафика и защищают сети от превышения их коммутационных или маршрутизирующих возможностей. Оптимизированный для работы с информационными, беспроводными и голосовыми каналами связи, коммутатор Cisco Catalyst Express 500 предлагает надежность и безопасность коммутаторов Catalyst в более доступной форме, которая требует для установки всего лишь несколько минут. Каждый коммутатор Cisco Catalyst Express 500 поступает в комплекте с модулем Cisco Network Assistant – средством, которое помогает сконфигурировать коммутатор, распознавая остальные компоненты в сети.

Еще одним дополнительным компонентом являются точки беспроводного доступа Cisco Aironet®, которые обеспечивают безопасный доступ к беспроводным ЛВС для офисов предприятий малого и среднего бизнеса. Беспроводные продукты Cisco расширяют возможности по обеспечению безопасности, масштабируемости и управляемости проводных ЛВС аналогичного класса. Точки беспроводного доступа Cisco Aironet поддерживают скоростной, безопасный роуминг при совместном использовании с устройствами Cisco или совместимыми устройствами, имеющимися у клиента, позволяя аутентифицированным пользователям безопасно переходить с одной точки доступа на другую.

Сведение всех вместе

Для продолжительного успеха любого сетевого решения важное значение имеет организация высококлассного его обслуживания и сопровождения. Решение Cisco SMB Support Assistant разработано с учетом требований предприятий малого и среднего бизнеса. Эта простая в использовании, высокоэффективная программа поддержки решает типичные для SMB проблемы, обеспечивая доступность и безопасность сети. Предприниматели могут получать результаты своевременной диагностики, рекомендации по поиску и устранению неисправностей и проводить упреждающую замену деталей. Основным компонентом программы является Cisco SMB Support Assistant Portal – набор интерактивных средств обеспечения безопасности, которые позволяют пользователям восстанавливать пароли, получать доступ к справочной документации, выполнять проверки состояния сети, загружать программные обновления и инициировать запросы к службе технической поддержки там, где это необходимо.

ПОЧЕМУ CISCO?

Решение Cisco Secure Network Foundation для предприятий малого и среднего бизнеса поддерживает работу бизнес-процессов, гарантирует конфиденциальность информации клиента и контролирует расходы, связанные с сопровождением доступной и безопасной самозащищающейся сети. В свою очередь, это повышает доверие клиентов, поддерживает или повышает эффективность работы персонала, помогает предпринимателям соблюдать законодательные требования и снижает общие расходы на владение сетью.

Решение Cisco Secure Network Foundation — это одна из составляющих интеллектуальных решений Cisco SMB Class, разработанных для повышения производительности труда сотрудников, поддержки новейших сервисов, повышения удовлетворенности клиентов и снижения эксплуатационных расходов. Располагая улучшенными возможностями в сферах голосовой связи, обеспечения безопасности и мобильности сетей, а также защиты инвестиций, решения Cisco SMB Class отвечают требованиям бизнеса сегодняшнего дня и ближайшего будущего.

Cisco и ее торговые партнеры в состоянии поделиться с предприятиями малого и среднего бизнеса максимально богатым опытом, накопленным за долгое время работы с клиентами. Различные варианты финансирования (аренда, лизинг и т. п.), отмеченные международными премиями первоклассные обслуживание и поддержка, а также персональное обучение способствуют получению предпринимателями максимальной выгоды от решения Cisco SMB Class.

Cisco — лидер на рынке маршрутизации, коммутации и безопасности — предлагает гибкие решения, способные отвечать требованиям бизнеса сегодняшнего дня и ближайшего будущего, позволяя ему развиваться и совершенствоваться. Стратегия безопасности Cisco Self-Defending Network обеспечивает безопасность каждой точки сетевой инфраструктуры, взаимодействует с сетевым окружением для получения дополнительного уровня защищенности и адаптируется к изменяющимся сетевым условиям, чтобы противостоять новым угрозам безопасности.

ПОСЛЕДУЮЩИЕ ШАГИ

Для получения более подробной информации о решении Cisco Secure Network Foundation обращайтесь к своему партнеру Cisco или посетите сайт: <http://www.cisco.com/go/smbclass>

Для поиска торговых партнеров Cisco посетите сайт: <http://www.cisco.com/go/partnerlocator>

Для получения дополнительной информации по вопросам финансирования решения Secure Network Foundation посетите сайт: <http://www.cisco.com/go/ciscocapital>



Cisco Systems
Россия, 115054 МОСКВА
бизнес центр «Риверсайд Тауерс»
Космодамианская наб., 52
стр. 1, этаж 4
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 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. Addresses, phone numbers, and fax numbers are listed on the
Cisco Connection Online Web site at <http://www.cisco.com>.
[//www.cisco.ru](http://www.cisco.ru).

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark
England • Finland • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxemburg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore
South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • Turkey • United Arab Emirates • United States • Venezuela

Copyright © 2005 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco IOS is the trademark; and Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.