



Q&A

РЕШЕНИЯ CISCO SYSTEMS ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ В ВОПРОСАХ И ОТВЕТАХ

О КОМПАНИИ CISCO SYSTEMS И ЕЕ СТРАТЕГИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Q. Разве компания Cisco занимается информационной безопасностью?

A. Интернет, отцом которого часто называют компанию Cisco, радикально изменил отношение к ведению бизнеса. Компании выводят возможности установления взаимоотношений с заказчиками, поставщиками, партнерами, своими сотрудниками на качественно новый уровень. Стремление компаний стать лидерами в своем сегменте рынка привело к появлению новых приложений для управления предприятием (ERP), цепочками поставок (SCM), взаимодействия с заказчиками (CRM), дистанционного обучения и т.п., – приложений, которые снижают издержки на выполнение транзакций, ускоряют многие бизнес-процессы, увеличивают удовлетворенность пользователей и снижают совокупную стоимость владения информационной системой.

Безопасность является фундаментальным элементом любой стратегии электронного ведения бизнеса. Открытие своих сетей для большего числа пользователей и приложений приводит к росту опасностей для информационных ресурсов. За ростом риска растет важность задачи их управления и повышения уровня защищенности компании к внешним и внутренним несанкционированным информационным воздействиям.

Компания Cisco Systems, помогая своим заказчикам в их бизнесе, не может обойти вниманием область информационной безопасности и предлагает уникальную стратегию защиты корпоративных сетей – Cisco Self-Defending Network. Решения, являющиеся составной частью данной стратегии, за время их существования получили признание специалистов разных стран и занимают лидирующие позиции в своих сегментах рынка. Компания Cisco предлагает своим заказчикам не только встроенные в сетевое оборудование (коммутаторы, маршрутизаторы, точки беспроводного доступа, IP-телефоны и т.п.) механизмы защиты, но и специализированные программные и программно-аппаратные решения:

- межсетевые экраны и системы предотвращения атак,
- средства построения VPN и системы аутентификации,
- средства защиты содержимого (антиспам, антивирус, блокирование URL, антифишинг, защита от шпионского ПО и т.п.) и управления безопасностью,
- системы персональной защиты ПК, серверов и ноутбуков и т.д.

Эти решения комбинируются с продуктами наших эко-партнеров в рамках стратегии построения безопасной сети SAFE, что позволяет создать всесторонне защищенную инфраструктуру для ведения бизнеса.

Дополнительная информация доступна по адресу: <http://www.cisco.com/security/>

Q. Что такое Self-Defending Network?

A. Идея Self-Defending Network (SDN) достаточно проста: в настоящее время поддержание целостности, конфиденциальности и контроля доступа в течение всего жизненного цикла информационной системы является ключом к успеху любой компании. Значение информации и контроля доступа к ней еще никогда не было так велико. Таким образом, задачей IT-инфраструктуры является предоставление своевременного доступа законным пользователям с одновременной возможностью обнаружения нарушений безопасности и защиты от несанкционированного доступа. Просто запрет доступа уже не является подходящим действием в ответ на обнаружение атаки. Современные сети должны реагировать на атаки, сохраняя свою доступность, надежность и работоспособность. Во многих отношениях, целью процесса обеспечения безопасности является повышение отказоустойчивости сетей. Вместо того, чтобы становиться жертвами, сети должны быть способными «поглощать» атаки и сохранять работоспособность, подобно иммунной системе человека, позволяющей организму функционировать при наличии в нем вирусов и бактериальных инфекций.

Стратегия Self-Defending Network построена на концепции ограниченности ресурсов (финансовых, человеческих, временных и т.п.) и необходимости их бережного использования во избежание их истощения. Также эти системы используют все преимущества существующей инфраструктуры, оказывая минимальное воздействие на IT-операции и бизнес-процессы потребителей.

Механизмы реакции на новые угрозы в рамках стратегия самозащищающейся сети Cisco продолжают непрерывно совершенствоваться. На первом этапе – **Интегрированная защита** – выполняется включение элементов защиты в состав элементов сети, таких как коммутаторы и маршрутизаторы. Второй этап – **Совместная защита** – включает построение связей между элементами сетевой защиты и распространение присутствия сети на конечные узлы, которые подключаются к сети. На **последнем** (на данный момент) **этапе** построения самозащищающейся сети Cisco происходит внедрение механизма **адаптивной защиты от угроз (Adaptive Threat Defense, ATD)**, позволяющего расширить возможности ответной реакции сети на угрозы на основе новейших технологий защиты от вредоносного контента *Anti-X*.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/sdn>

Q. Чем Self-Defending Network (SDN) отличается от Adaptive Threat Defense (ATD)?

A. Adaptive Threat Defense – это очередной (третий) этап развития стратегии компании Cisco в области информационной безопасности Self-Defending Network.

Корпоративные сети, как и атаки на них, в настоящее время достигли такого уровня сложности, что полностью полагаться на какой либо метод поддержания их безопасности стало невозможно. Это привело к возникновению идеи «глубокой эшелонированной обороны». До недавнего времени эта идея была основана на концепции *упреждающей* или проактивной защиты. Но, учитывая типы уязвимостей и атак, сопровождающих непрерывно меняющиеся сети, Cisco Systems полагает, что существует способ построения лучших *адаптивных* решений. В результате, специалисты компании Cisco начали поиск других, на вид не имеющих отношения к делу, примеров из реального мира, таких как иммунная система человека в качестве модели для самозащищающейся сети. Другие системы из реального мира, в ходе изучения которых были получены наглядные результаты, можно найти в эпидемиологии, а также при рассмотрении процесса обеспечения общественного порядка в группе населения. Общим для всех этих систем является использование средств как *адаптивной*, так и *упреждающей* защиты.

В ходе дальнейшего наблюдения можно увидеть, что средства защиты систем такой природы встроены в каждый функциональный блок. Ключевыми возможностями этих средств адаптивной защиты являются:

- Непрерывное функционирование
- Ненавязчивость

- Минимизация возможности распространения атак
- Быстрая реакция на еще неизвестные атаки.

Q. Что такое интегрированная безопасность в понимании Cisco?

A. Тенденции последних лет убедительно показывают, что мало выпустить систему безопасности – она должна быть очень тесно связана с защищаемыми бизнес-процессами. А это значит, что каким бы хорошим не был «навесной» продукт в области защиты информации, он остается не более чем придатком к основной информационной системе предприятия. Он не учитывает сложившуюся практику использования информационных технологий, не «понимает» бизнес-процессов и даже не всегда корректно работает с ранее внедренными ИТ-решениями.

Это приводит к необходимости интеграции защитных механизмов в инфраструктуру корпоративной сети или сети оператора связи. Как только межсетевой экран, система предотвращения атак, модули построения VPN становятся неотъемлемой частью сети, их эффективность возрастает на порядок; не говоря уже о снижении совокупной стоимости владения таким целостным решением.

Именно поэтому компания Cisco уделяет такое большое внимание интеграции своих защитных технологий в весь спектр своего оборудования и программных решений. Любой наш коммутатор или маршрутизатор, IP-телефон или точка беспроводного доступа содержат большое количество встроенных механизмов защиты. Достаточно только посмотреть на маршрутизаторы Cisco Integrated Service Router (ISR), Cisco Wireless LAN Controller и т.п. Заказчики, сделавшие выбор в пользу нашего оборудования, сделали хорошие инвестиции и в свою информационную безопасность. Им не приходится заниматься внедрением и интеграцией «навесных» средств защиты в уже работающую инфраструктуру – им достаточно просто настроить уже существующие в сетевом оборудовании механизмы защиты и не бояться, что принятая технология обработки информации будет нарушена.

Q. Какие новые продукты и технологии по безопасности у вас появились за прошедший год?

A. За прошедший год компания Cisco выпустила следующие новые продукты и технологии по информационной безопасности:

- Cisco Russian VPN Module
- Cisco Pix 7.2
- Cisco IPS 5.2 (и новую платформу IPS 4260)
- Cisco Security Agent (CSA) 5.1
- Cisco MARS 4.1
- Cisco Configuration Assurance Solution
- Cisco AVS 3120 Application Velocity System
- Cisco ASA 7.2 (и новые платформы ASA 5505 и 5550)
- Cisco NAC Appliance (бывший Cisco Clean Access)
- Cisco Secure Services Client
- Cisco IntelliShield Alert Manager

Дополнительная информация доступна в каталоге продуктов Cisco Systems по информационной безопасности по адресу:
<http://www.cisco.com/global/RU/broch.shtml>

Q. Вы называете себя лидером в области информационной безопасности не только в мире, но и в России. Как вы можете это доказать?

A. Оборот Cisco Systems в области информационной безопасности за 2005 календарный год только на территории России составил 40 миллионов долларов США. Данные цифры включают ТОЛЬКО межсетевые экраны, системы обнаружения и предотвращения атак, модули безопасности для коммутаторов Catalyst 6500 и маршрутизаторов Cisco 7600 и security bundles на их основе. Эти показатели по данным обзора CNews «Средства защиты информации и бизнеса 2006» (<http://www.cnews.ru/reviews/free/security2006/>) позволили нашей компании в очередной раз позволили занять первое место в России среди игроков рынка информационной безопасности.

Q. Кто ваши конкуренты? А в России?

A. Согласно последнему отчету компании Synergy (за 2-ий квартал 2006 года) доля производителей средств информационной безопасности распределяется следующим образом (учитывались и межсетевые экраны, и VPN, и системы обнаружения и предотвращения атак):

Производитель	Место	Доля рынка
Cisco	1	33.8%
CheckPoint	2	10.7%
Juniper	3	9.1%
Symantec	4	6.5%
Nokia	5	5.5%

На рынке гибридных и многофункциональных средств защиты компания Cisco по данным компании Synergy также занимает первое место:

Производитель	Место	Доля рынка
Cisco	1	39.4%
CheckPoint	2	13.5%
Juniper	3	8.0%
Nokia	4	7.0%
Symantec	5	5.5%

Аналогичные лидирующие позиции у компании Cisco и на рынке средств обнаружения и предотвращения атак:

Производитель	Место	Доля рынка
Cisco	1	17.9%
ISS (была куплена IBM)	2	14.4%
Symantec	3	13.4%
3Com	4	10.8%

Juniper	5	7.8%
---------	---	------

Q. Чем вы отличаетесь от других международных компаний, работающих в России и выпускающих средства защиты наряду с сетевым оборудованием?

A. В первую очередь мы отличаемся четкой стратегией в области информационной безопасности – Cisco Self-Defending Network. Данная стратегия не стоит на месте и продолжает непрерывно совершенствоваться. Однако стратегия Cisco SDN – это не просто красивые слова, за ней стоят серьезные исследования, на которые ежегодно инвестируется свыше 300 миллионов долларов, позволившие выпустить нам не менее 50 продуктов по защите от широкого спектра угроз (и список этих продуктов постоянно расширяется). Все эти продукты ориентированы не только на защиту крупных предприятий, но и позволяют обезопасить ресурсы операторов связи. Немалое внимание Cisco уделяет и сегменту малого и среднего бизнеса, выпустив целый ряд специализированных решений по безопасности, удовлетворяющих техническим и финансовым требованиям небольших предприятий. Одним из ключевых отличий Cisco от других сетевых производителей является выпуск системы защиты персональных компьютеров, серверов и ноутбуков – Cisco Security Agent. Эта система позволяет построить действительно многоуровневую и эшелонированную оборону корпоративных ресурсов от различных известных и неизвестных угроз.

Помимо выделенных решений компания Cisco серьезное внимание уделяет интегрированным решениям, которые «встроены» в любые технологии и оборудование нашей компании – сети хранения данных и оптические сети, коммутаторы и маршрутизаторы, беспроводные сети и IP-телефония и т.п.; все они обладают механизмами отражения различных несанкционированных действий и атак, аутентификации пользователей и устройств и т.д. При этом никакого негативного влияния на циркулирующий трафик не оказывается. Более того, все технологии разрабатывались для эффективной защиты не только обычных данных, но и других типов трафика в конвергентных сетях – голосовых, мультимедиа, видео и т.п. В качестве примера такой интеграции можно назвать индустриальную инициативу Network Admission Control (NAC), которая помимо Cisco поддерживается почти 70 различных производителей – IBM, Intel, HP, Microsoft, Trend Micro, McAfee, Symantec, CA, Check Point, ISS и т.д. Эта технология позволяет не только локализовывать эпидемии вредоносных программ и обнаруживать любые отклонения от политики безопасности, но и блокировать доступ несоответствующих узлов к важным информационным ресурсам, а также автоматически устранять обнаруженные нарушения.

Помимо программных, аппаратных и программно-аппаратных средств защиты компания Cisco предлагает своим заказчикам широкий набор сервисов и услуг, позволяющих охватить весь жизненный цикл информационной системы предприятия – анализ требований по защите бизнес-процессов, создание концепции информационной безопасности и планов защиты, внедрение средств защиты и их интеграция с существующей инфраструктурой, эксплуатация и регулярная проверка соответствия текущего состояния заданным в политике безопасности требованиям и т.п. Все эти услуги базируются на архитектуре защищенной корпоративной сети SAFE, ознакомиться с которой свободно можно на сайте Cisco. Для более эффективного использования решений по информационной безопасности компания Cisco предлагает своим заказчикам пройти авторизованное обучение по большому числу программ и курсов. После обучения и сдачи соответствующих экзаменов специалист может получить признанный во всем мире сертификат по безопасности Cisco.

Еще одним важным отличием является участие Cisco в форуме FIRST – First of Incident Response and Security Teams (<http://www.first.org/about/organization/teams/index.html>), объединяющем компании и организации, занимающиеся реагированием на регулярно обнаруживаемые уязвимости. FIRST дает возможность всем его участникам не только самостоятельно заниматься тестированием безопасности своих решений (как это делает Cisco PSIRT), но и получать аналогичную информацию от десятков других участников, что существенно повышает вероятность обнаружения и устранения дыр *до того*, как они будут обнаружены злоумышленниками.

В России и странах СНГ компания Cisco предлагает все продукты и услуги в области информационной безопасности. При этом число инженеров, консультирующих заказчиков и помогающих им внедрять наши решения по безопасности превышает 50.

Российским специалистам доступны книги по информационной безопасности Cisco на русском языке. Компания Cisco, соблюдая российское законодательство в области информационной безопасности, сертифицировала в Федеральной службе по техническому и экспортному контролю (ФСТЭК) многие свои решения на соответствие российским требованиям в области информационной безопасности – общее число сертификатов превышает на данный момент 240. И, наконец, в октябре 2006 года компания Cisco и российская компания «С-Терра» объявили о создании модуля шифрования для маршрутизаторов Cisco ISR, построенного на базе сертифицированной ФСБ криптографической библиотеки.

Q. Чем вы отличаетесь от других международных компаний, работающих в России и называющих себя лидерами рынка информационной безопасности?

A. Помимо вышеназванных отличий преимущество компании Cisco опирается на знание сетевых технологий, используемых у заказчика и возможность тесной интеграции механизмов безопасности в сетевое оборудование. В этом случае, заказчик получает изначально защищенную инфраструктуру для своего бизнеса и не должен заниматься внедрением в уже работающую сеть «навесных» средств защиты.

Q. Чем вы отличаетесь от российских компаний, работающих на рынке информационной безопасности?

A. Помимо вышеназванных отличий преимущество компании Cisco опирается на круглосуточно работающий центр поддержки, отработанную логистику и эффективную защиту самых современных технологий, используемых российскими заказчиками.

Q. Значит ли это, что вы в состоянии «закрыть» все потребности заказчика в области информационной безопасности?

A. Мы стараемся предлагать нашим заказчикам те решения, в области которых мы являемся специалистами и обладаем большой квалификацией и опытом. Те задачи, которые не «закрывают» наши собственные разработки, решаются с помощью наших эко-партнеров. Таким образом мы создаем целую экосистему, позволяющую удовлетворить даже самые неожиданные и взыскательные потребности наших заказчиков.

Например, мы очень тесно сотрудничаем с компанией Trend Micro – мировым лидером в области антивирусной защиты и контроля вредоносного контента. Наш альянс уже позволил нам предложить заказчикам ряд совместных решений. Например, систему снижения ущерба от эпидемий вредоносных программ Cisco Incident Control System или специальный модуль Content Security Module для многоцелевого защитного устройства Cisco ASA 5500. Другой пример связан с российской компанией S-Terra CSP, с которой мы выпустили совместное решение по организации виртуальных частных сетей (VPN), использующее сертифицированное в ФСБ криптографическое ядро и интегрируемое в маршрутизаторы Cisco ISR.

Q. Я слышал, что рекомендуется приобретать все решения у одного производителя. Почему?

A. При выборе разработчика средств защиты небольшие организации зачастую придают слишком большое значение экономии непосредственных затрат, не принимая во внимание расходы по эксплуатации. Например, приобретение комбинированного оборудования разных разработчиков позволяет иногда снизить первоначальные капитальные затраты, но приводит к увеличению затрат на интеграцию и, в большинстве случаев, к снижению уровня безопасности.

Это происходит потому, что обеспечение безопасности является глобальной проблемой, проблемой «нестыковок между компонентами», а также самих компонентов. Собирая систему безопасности из компонентов разных разработчиков, организации приходится выступать в роли интегратора систем безопасности. Это очень трудная задача, которую еще больше усложняют различные протоколы, интерфейсы управления, а также договоры поддержки и другие документы разных разработчиков, которые потребуется изучить. Кроме того, при неизбежных нарушениях системы безопасности обращение по телефону к множеству разработчиков и согласование их ответов является не самым оптимальным вариантом отражения атаки.

Более надежная защита и низкие расходы по эксплуатации могут быть достигнуты за счет выбора разработчика, предлагающего полностью совместимое оборудование и программное обеспечение для всех областей сети, включая межсетевые экраны, компоненты внутренней сети, настольные станции, сети VPN и пр.

Q. Сколько ваша компания тратит на исследования в области информационной безопасности?

A. Год от года эта цифра меняется. В 2003 финансовом году компания Cisco потратила на исследования и разработки в области информационной безопасности 300 миллионов долларов. Это больше, чем годовой оборот многих зарубежных компаний работающих на рынке информационной безопасности. Такой подход позволяет нам лидировать практически во всех сегментах рынка средств защиты информации, на которых представлены решения компании Cisco.

Q. Зачем вы так много тратите на исследования информационной безопасности?

A. Без исследований невозможно разрабатывать решения, которые бы удовлетворяли как требованиям заказчиков, так и рекомендациями различных регулирующих органов и нормативных документов. Именно поэтому компания Cisco инвестирует около 10% своего общего бюджета на исследования и разработки на нужды, связанные с информационной безопасностью. И такой подход оправдал себя – наша компания является лидером во всех сегментах, в которых представлены решения Cisco по защите информации.

Не будет преувеличением сказать, что на наших исследованиях «построен» Интернет и его безопасность - эксперты Cisco участвовали в разработке многих общепризнанных стандартов в области защиты информации. Но наша компания не останавливается на достигнутом (топтанье на месте равносильно смерти) и продолжает активно участвовать в разработке различных стандартов по информационной безопасности.

В приложении приведен список из почти 60 стандартов, в разработке которых принимала участие компания Cisco.

Q. Что вы предлагаете кроме оборудования и программных решений в области информационной безопасности?

A. В первую очередь все наши решения базируются на архитектуре построения защищенной сети SAFE, которая позволяет построить из отдельных фрагментов целостную картину. Грамотное внедрение средств защиты может быть осуществлено заказчиком как самостоятельно, так и с помощью экспертов компании Cisco. В первом случае помочь могут книги по информационной безопасности и проектированию сетей, выпущенные издательством CiscoPress (<http://www.ciscopress.com/>). Во втором – можно обратиться в консалтинговое подразделение Cisco, которое готово предложить свыше 40 различных сервисов и услуг по информационной безопасности – от разработки концепций безопасности и заканчивая реагирование на инциденты.

Q. Что такое SAFE?

A. Главная цель архитектуры Cisco Systems для безопасности корпоративных сетей (SAFE) состоит в том, чтобы предоставить заинтересованным сторонам информацию о современном опыте проектирования и развертывания защищенных сетей. SAFE призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. SAFE исходит из принципа глубоко эшелонированной обороны сетей от внешних атак. Этот подход нацелен не на механическую установку межсетевого экрана и системы обнаружения атак, а на анализ ожидаемых угроз и разработку методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности. SAFE основывается на продуктах компании Cisco Systems и ее партнеров.

Архитектура Cisco SAFE с максимальной точностью моделирует функциональные потребности современных корпоративных сетей и решает следующие задачи (в порядке приоритетности):

- Безопасность и борьба с атаками на основе политик.
- Внедрение мер безопасности по всей инфраструктуре (а не только на специализированных устройствах защиты).
- Безопасное управление и отчетность.
- Аутентификация и авторизация пользователей и администраторов для доступа к критически важным сетевым ресурсам.
- Обнаружение атак на критически важные ресурсы и подсети.

- Поддержка новых сетевых приложений.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/safe>

Q. Какие преимущества дает SAFE?

A. Внедряя SAFE, заказчики получают множество преимуществ, т.к. SAFE:

- Обеспечивает основу для построения безопасных, доступных, интегрированных сетей.
- Открытая модульная структура.
- Упрощает разработку, внедрение и управление сетевой безопасностью.
- Обеспечивает масштабируемость решений.
- Позволяет эффективное поэтапное внедрение.
- Использует лучшие продукты и услуги сетевой безопасности благодаря интеграции решений экосистемных партнеров.

Q. Что такое NAC?

A. Технология Network Admission Control (NAC) позволяет предотвратить доступ к корпоративным ресурсам или сети оператора связи устройства, не соответствующие политике безопасности (заражен вредоносной программой, отсутствует или устарел антивирус, отсутствуют патчи и Service Pack'и, отсутствуют средства защиты и иное программное обеспечение). В случае обнаружения такого несоответствия доступ узла либо блокируется, либо он перенаправляется в карантинную сеть, в которой на узел может быть установлено отсутствующее программное обеспечение.

Cisco была первой компанией, выпустившей работающее решение пару лет назад. Оно было представлено сразу в двух ипостасях – в виде подсистемы NAC Framework, интегрированной в сетевое оборудование, и в виде отдельного устройства NAC Appliance (бывший Cisco Clean Access). В первом случае в качестве устройства, через которое проходили все запросы мог выступать любой маршрутизатор, коммутатор, точка беспроводного доступа, межсетевой экран или многофункциональное защитное устройство компании Cisco. Во втором случае, технология контроля сетевого доступа была реализована в виде NAC Appliance, который мог быть установлен на сети, построенной на оборудовании любого производителя.

Решение Cisco NAC поддерживается несколькими десятками производителей, выступающих в качестве поставщиком систем для конечных устройств. В качестве таких производителей можно назвать Check Point, ISS, Trend Micro, Symantec, McAfee, Лаборатория Касперского, Intel, Microsoft и т.д. При этом конечные устройства могут работать под управлением Windows, Linux, Solaris и т.д. Наличие открытого API позволяет подключаться к данной инициативе любому разработчику.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/nac>

Q. Чем Cisco NAC отличается от инициатив других компаний?

A. Поддержка NAC встроена в сетевое оборудование и не требует смены топологии и приобретения дополнительного оборудования, что позволяет начать использовать возможности Network Admission Control практически сразу после подключения маршрутизаторов, коммутаторов или точек беспроводного доступа. Другим отличием NAC является ее поддержка ведущими производителями программного и программно-аппаратного обеспечения, к числу которых можно отнести IBM, Trend Micro, Symantec, LANDesk и т.д. О своей поддержке индустриальной инициативы NAC объявили компании Intel, Microsoft, HP, VMWare, Check Point, ISS, eEye, WebSense, Computer Associates и т.д. Технология NAC также совместима с технологией NAP компании Microsoft.

Q. Я хочу использовать технологию NAC, но моя сеть построена не на оборудовании Cisco. Что мне делать?

A. Вы можете заменить ваше оборудование на решения Cisco по программе Trade-In. Если это невозможно, то вы можете обратить свое внимание на специальное программно-аппаратное решение NAC Appliance (Cisco Clean Access), которое позволяет реализовать весь функционал NAC в сетях, построенных на сетевом оборудовании других производителей.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/cca>

Q. Кто из российских разработчиков поддерживает Network Admission Control (NAC)?

A. Компания «Лаборатория Касперского» подписала соглашение о начале работе по поддержке технологии NAC Framework в своих решениях. Кроме того решения компании «Лаборатория Касперского» уже сейчас поддерживаются в NAC Appliance (бывший Cisco Clean Access). Сейчас мы также ведем переговоры с рядом других российских производителей по поводу интеграции их средств защиты с индустриальной инициативой NAC.

Q. Что вас связывает с компанией Positive Technologies (разработчиками XSpider)?

A. С компанией Positive Technologies мы организовали совместную акцию «Проверь здоровье своей сети» (<http://www.freescan.ru/>), предназначенную для бесплатной проверки защищенности сетей наших заказчиков и их защиты от современных угроз.

О СЕРТИФИКАЦИИ ПО РОССИЙСКИМ ТРЕБОВАНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Q. Какие сертификаты ФСТЭК (Гостехкомиссии) у вас есть?

A. По данным на середину 2006 года наша компания получила 242 сертификата Федеральной службы по техническому и экспортному контролю (бывшая Гостехкомиссия). Сертификаты выданы как на единичные экземпляры, так и на партии изделий. В зависимости от типа средства защиты сертификация проводилась по техническим условиям (ТУ), Руководящим документам или заданию по безопасности. Полный список всех сертификатов вы можете получить, сделав запрос по адресу: security-request@cisco.com.

Q. Есть ли у вас сертификаты ФСБ/ФАПСИ?

A. Нет. Однако криптографическое ядро, входящее в наш VPN-модуль, разработанный вместе с компанией «С-Терра», имеет сертификат ФСБ.

Q. Есть ли у вас сертификаты по недеklarированным возможностям?

A. На данный момент нет.

Q. Сертифицированы ли вы по «Общим критериям» (ISO 15408 или ГОСТ Р ИСО/МЭК 15408)?

A. Да, наши решения сертифицированы как по международному стандарту ISO 15408. В России мы проводим сертификацию наших решений в соответствие со стандартом ГОСТ Р ИСО/МЭК 15408, базирующемся на ISO 15408.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/securitycert>

Q. Можно ли использовать ваши решения для защиты гостайны?

A. На данный момент полученные нами сертификаты не позволяют использовать наши решений в автоматизированных системах, обрабатывающих сведения, составляющие государственную тайну.

Q. Соответствуют ли ваши решения требованиям СТР-К или нового стандарта Банка России по информационной безопасности?

A. Да, соответствуют. На сайте www.cisco.ru (<http://www.cisco.com/global/RU/broch.shtml>) доступны документы, описывающие, как решения компании Cisco выполняют требования СТР-К или стандарта Банка России по информационной безопасности.

О СРЕДСТВАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Q. Можем ли мы официально использовать ваши решения VPN?

A. Да, при условии официального их ввоза на территорию российской федерации. Из этого правила есть ряд исключений, описанных в федеральном законодательстве.

Q. Что делать, если мы не можем получить разрешение на эксплуатацию ваших средств построения VPN?

A. Вы можете использовать совместное решение Cisco и российской компании S-Terra CSP, которое, с одной стороны построено на базе сертифицированного в России криптографического ядра, а с другой стороны является составной частью сетевого оборудования Cisco.

Q. Планируете ли вы встраивать отечественные алгоритмы шифрования (по ГОСТ) в ваши VPN-решения?

A. Да. Такие работы были проведены и их результатом стал VPN-модуль для маршрутизаторов Cisco ISR, использующий отечественные алгоритмы шифрования.

Q. Что вы можете сказать по поводу того, что Nortel встроила в свои решения отечественные алгоритмы шифрования (по ГОСТ)?

A. С точки зрения отечественного законодательства любые импортируемые на территорию России средства, содержащие функции шифрования, должны ввозиться только по лицензии Министерства по экономическому развитию и торговле. Поэтому решения Nortel с российскими алгоритмами шифрования и решения Cisco с международными стандартами в области шифрования (DES, 3DES, AES и т.д.) находятся для российских потребителей в одинаковых с точки зрения законодательства условиях, даже при условии, что интеграция оборудования Nortel с российскими криптоалгоритмами будет происходить на территории Российской Федерации.

Кроме того, совместно с российской компанией S-Terra CSP мы предложили нашим заказчикам совместное решение по построению VPN на базе сертифицированного в России криптографического ядра.

Дополнительная информация доступна по адресу: <http://www.cisco.com/global/RU/products/hw/vpndevc/rvpn/index.shtml>

Q. Есть ли у вас проблемы с таможней с ввозом оборудования, поддерживающего криптографические механизмы?

A. Нет. По Российскому законодательству, ввоз продукции, содержащей шифрование, требует получения лицензии Министерства Экономического Развития и Торговли РФ, оформляемой на основании решения ФСБ России на каждую конкретную партию товаров. Так же существуют разрешительные списки, куда могут включаться продукты, которые так же могут ввозиться без получения лицензий. В настоящий момент в отношении продукции компании Cisco Systems действуют следующие документы:

- Письмом номер 8/ЛЗ/2/3-1656 от 01.07.2005 Центр по Лицензированию, Сертификации и защите Государственной Тайны ФСБ РФ сообщил, что оборудование и программное обеспечение компании Cisco Systems, в обозначении которого не содержатся коды "K8" и "K9" не требует для своего ввоза получения лицензии Министерства Экономического Развития и Торговли РФ.
- Письмом номер 8/ЛЗ/2/3-1788 от 15.07.2005 Центр по Лицензированию, Сертификации и защите Государственной Тайны ФСБ РФ сообщил, что ввоз модулей ускорения шифрования (AIM-VPN*, NM-VPN/MP, MOD1700-VPN*, PIX-VPN-ACCEL*, PIX-VAC-PLUS*) должен осуществляться по лицензии МЭРТ.
- Так же существует письмо, в котором Центр по Лицензированию дает указание таможне при определении, необходима лицензия или нет, руководствоваться информацией о том, какой вариант IOS установлен на устройство.

Компания Cisco также находится в процессе согласования с Центром по Лицензированию ФСБ списков продукции, которая содержит криптографические функции, но не может использоваться для шифрования непосредственно данных. Это, например, системы сетевого управления. Так же не должно быть проблем с ввозом беспроводного оборудования.

ОБ ОТДЕЛЬНЫХ РЕШЕНИЯХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Q. Заменит ли Cisco ASA 5500 Cisco Pix, Cisco IPS или Cisco VPN 3000?

A. Cisco ASA 5500 – это многофункциональные защитные устройства, включающие в себя и межсетевой экран Cisco Pix, и систему предотвращения атак Cisco IPS и систему построения VPN – Cisco VPN 3000 Concentrator. При этом используемая архитектура позволяет легко расширять функционал устройства новыми возможностями – антивирусной защитой, контролем содержимого и т.п. В тех условиях, где требуется комбинация защитных технологий, мы рекомендуем использовать интегрированные решения, такие как Cisco ASA 5500. Если же в защищаемой сети уже внедрен межсетевой экран или система предотвращения атак, то применение выделенного устройства, решающего оставшуюся задачу, является более предпочтительным.

Дополнительная информация по Cisco ASA доступна по адресу: <http://www.cisco.com/go/asa>

Q. Могут ли ваши решения по информационной безопасности быть интегрированы с решениями других фирм?

A. Да. В рамках специализированных программ Cisco Technology Developer Program и Network Admission Control Program наши решения по информационной безопасности могут быть интегрированы с решениями таких компаний, как Aladdin Knowledge Systems, Arbor Networks, SurfControl, Trend Micro, Websense, С-Терра СиЭсПи, Лаборатория Касперского, Altiris, Computer Associates, IBM, McAfee, Symantec, Panda Software, Check Point, eEye Digital, Sophos, Intel, Internet Security Systems и др.

Полный список компаний, с которыми интегрируются наши решения по безопасности, может быть найден по адресам <http://www.cisco-partners.info> и <http://www.cisco.com/en/US/partners/pr46/nac/partners.html>.

Q. Может ли Cisco Pix анализировать трафик приложений на прикладном уровне?

A. Да. Такая возможность существует в межсетевом экране Cisco Pix, системах предотвращения атак Cisco IPS, многофункциональных устройствах Cisco ASA и т.д.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/pix>

Q. Предлагает ли компания Cisco решения по контролю содержимого?

A. Да. Исторически в межсетевом экране Cisco Pix и устройства кэширования Content Engine входили решения по контролю и блокированию URL – WebSense, N2H2 или SmartFilter. Кроме того, с помощью механизма Network-based Application Recognition (NBAR), встроенного в операционную систему IOS, можно осуществлять контроль содержимого для различных сетевых и прикладных протоколов. Еще одним решением поставленной задачи является модуль Anti-X, разработанный совместно с компанией Trend Micro, который позволяет контролировать SMTP-, POP3-, HTTP- и FTP-трафика.

Q. Cisco Secure ACS – это обычный RADIUS-сервер?

A. Нет. Это ключевой элемент инфраструктуры управления доступом и доверием компании Cisco, который поддерживает протоколы RADIUS, TACACS+, архитектуру IBNS (802.1x), Network Admission Control, а также интегрируется с внешними серверами контроля доступа (например, RSA Keon или IBM Tivoli Identity Manager), хранилищами идентификационной информации (Active Directory, LDAP и т.п.).

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/acs>

Q. Cisco предлагает только сетевые средства защиты?

A. Нет. Большое внимание мы уделяем и защите конечных устройств (Endpoint Security), таких как сервера, рабочие станции, ноутбуки, IP-телефоны и т.п. Для решения этой задачи компания предлагает специальное программное решение – Cisco Security Agent, которое позволяет обнаруживать и блокировать известные и неизвестные угрозы, направленные против конечных устройств. С целью локализации узлов, несоответствующих корпоративной политике безопасности мы разработали технологию Network Admission Control, о поддержке которой объявили многие компании, предлагающие средства защиты рабочих станций и серверов – IBM, Trend Micro, McAfee, Symantec, Check Point, ISS и т.п.

Q. Cisco Pix поддерживает механизм Stateful Inspection?

A. Да. Этот механизм поддерживает также Cisco IOS Firewall и Cisco ASA 5500.

Q. Ваши конкуренты говорят, что у вас нет Stateful Inspection.

A. Заявлять можно все. Рассудит потребитель. Если посмотреть на независимые тесты, а также доли рынка сетевой безопасности, занимаемые нами и другими компаниями, то можно сразу видеть, кто прав, а кто нет.

УСЛУГИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Q. Можете ли вы помочь в разработке концепции, политики или плана информационной безопасности?

A. Да. В компании существует специальное подразделение, занимающееся разработкой организационно-распорядительной документацией в области информационной безопасности, в т.ч. концепций или планов информационной безопасности.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/securityconsulting>

Q. Можете ли вы помочь нам в развертывании официально приобретенных у вас решений по информационной безопасности?

A. Да. Эта задача может быть реализована как специалистами компании Cisco, так и ее партнерами, специализирующимися на информационной безопасности и имеющих соответствующий статус.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/securityconsulting>

Q. Что мне делать, если я хочу использовать ваши решения по информационной безопасности, но у меня нет людей, которые будут ими управлять?

A. Эта распространенная проблема во всем мире, когда заказчики выводят все непрофильные активы и подразделения за рамки компании, концентрируясь на основном бизнесе. Управление информационными технологиями и информационной безопасностью в таком случае передается внешней организации на аутсорсинг (т.н. Managed Security Service). Эта организация занимается настройкой, мониторингом и обновлением средств защиты, установленных у заказчика в круглосуточном режиме с привлечением высококвалифицированных специалистов. Компания Cisco предлагает своим заказчикам помощь в переходе на использование аутсорсинговых услуг информационной безопасности.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/securityconsulting>

Q. С помощью ваших решений по информационной безопасности я обнаружил атаку. Что мне теперь делать?

A. Мы предлагаем набор специальных услуг Cisco Incident Readiness and Response Services, помогающих нашим заказчикам быть готовыми к обнаружению, предотвращению и реагированию на аномальную и подозрительную активность, фиксируемую внедренными средствами защиты. Данный набор услуг включает в себя 3 основных компонента:

- Incident Readiness Assessment – оценка готовности компании к реагированию на атаки.
- Incident Readiness Design Development – разработка технических мер и процедур для эффективного реагирования на атаки.

- Incident Response – круглосуточные консультации экспертов Cisco в момент атаки на ваши ресурсы.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/securityconsulting>

Q. Есть ли у вас услуга, которая позволяет получать мне уведомления об уязвимостях в программно-аппаратном обеспечении разных производителей?

A. Да, такая услуга носит название Cisco IntelliShield Alert Manager. Она подразумевает доступ к специально созданной инфраструктуре, которая содержит свыше 15 тысяч описаний уязвимостей по 18500 версий 5500 продуктов 1700 известных разработчиков программного и программно-аппаратного обеспечения различных производителей. Основное отличие Cisco Security IntelliShield Alert Manager Service от множества других сервисов – уведомление только о тех уязвимостях, которые присущи именно вашему программному обеспечению.

ОБ ОБУЧЕНИИ И СЕРТИФИКАЦИИ СПЕЦИАЛИСТОВ

Q. Можно ли пройти обучение по вашим решениям? Где?

A. Обучение по курсам, подготовленным компанией Cisco Systems в области информационной безопасности, можно пройти в авторизованных учебных центрах – Cisco Training Center, Комптек и REDCENTER и десятках других, разбросанных по территории Российской Федерации и стран СНГ.

Более подробная информация по ним может быть найдена по адресу: <http://www.cisco.com/go/securitytraining>

Q. Какие сертификации специалистов по информационной безопасности предлагает компания Cisco?

A. По информационной безопасности компания Cisco Systems предлагает две схемы сертификации, ценящиеся во всем мире:

- Основная сертификация
 - Cisco Certified Internetwork Expert (CCIE Security)
 - Cisco Certified Security Professional (CCSP)
- Специализированные сертификации по основным технологиям, в т.ч. и информационной безопасности
 - Cisco Advances Security Field Specialist
 - Cisco Firewall Specialist
 - Cisco IPS Specialist
 - Cisco Security Sales Specialist
 - Cisco Security Solutions and Design Specialist
 - Cisco VPN Specialist.

Более подробная информация по ним может быть найдена по адресам: <http://www.cisco.com/go/ccsp>,

<http://www.cisco.com/en/US/learning/le3/ccie/security/index.html> и

http://www.cisco.com/web/learning/le3/le2/le41/le85/learning_certification_type_home.html.

Q. Какие книги вы порекомендуете по вашим решениям в области информационной безопасности?

A. С целью обучения наших заказчиков нами было организовано специальное подразделение CiscoPress

(<http://www.ciscopress.com/>), в задачи которого входит публикация книг по различным аспектам деятельности нашей компании. В

т.ч. издательство CiscoPress опубликовало множество книг и по информационной безопасности, ориентированных как на технических специалистов, так и на людей, принимающих решения.

Некоторые из этих книг были переведены на русский язык (<http://www.ciscopress.ru/>) и их можно приобрести во многих традиционных или электронных книжных магазинах России и стран СНГ.

ОБ ИНЦИДЕНТАХ БЕЗОПАСНОСТИ И РЕШЕНИЯХ CISCO

Q. Я приобрел у официального поставщика ваше оборудование. В нем была обнаружена уязвимость? Как мне ее устранить?

A. Вся информация об уязвимостях, подверженных им версиях продуктов и способах устранения доступна по адресу: http://www.cisco.com/en/US/products/products_security_advisories_listing.html. В том случае если вы заключили сервисный контракт на поддержку приобретенного вами оборудования, вы можете загрузить с сайта Cisco все необходимые обновления, устраняющие обнаруженную уязвимость.

Дополнительная информация доступна по адресу: <http://www.cisco.com/go/psirt>

Q. Как вы боретесь с уязвимостями в вашем оборудовании?

A. Любое программное или программно-аппаратное обеспечение компании Cisco проходит жесткий контроль качества. Дополнительную проверку с точки зрения безопасности проводит специальное подразделение Cisco Product Security Incident Response Team (PSIRT).

Помимо собственного подразделения PSIRT наша компания также входит в альянс FIRST. Это позволяет нам своевременно получать информацию о различных уязвимостях от других участников FIRST, что многократно увеличивает вероятность обнаружения и устранения уязвимостей еще до того, как об этом станет известно широкой общественности. Другие производители вынуждены «вариться в собственном соку» и рассчитывать только на свои силы.

Дополнительную информацию о процессе поиска и устранения уязвимостей в оборудовании Cisco, вы можете узнать по адресу: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.

Q. Говорят сайт Cisco в августе 2005 года взломали. Это правда?

A. Нет, это неправда. Этот слух связан со сменой паролей пользователей на сайте cisco.com. Некоторые СМИ посчитали это следствием взлома нашего сайта, что не соответствует действительности.

Q. Почему в августе 2005 года были сменены пароли всех пользователей cisco.com?

A. В процессе тестирования защищенности Web-сервера cisco.com независимой организацией была обнаружена уязвимость в системе поиска нашего сайта, которая могла негативным образом сказаться на паролях всех зарегистрированных на сайте пользователей – заказчиков, партнеров, сотрудников Cisco и др. Уязвимость была своевременно устранена, но в рамках защиты персональных данных пользователей сайта мы приняли соответствующие меры, в т.ч. и по смене всех паролей.

Компания Cisco очень серьезно относится к защите своих ресурсов, а также к защите своих клиентов и партнеров. Данный инцидент не является следствием слабостей в наших продуктах, технологиях и инфраструктуры. Мы благодарим вас за понимание и просим извинений за некоторые неудобства связанные со сменой паролей.

Дополнительная информация доступна по адресу: <http://www.cisco.com/security/security-alerts.html>

Q. На конференции BlackHat 2005 был сделан доклад о дырах в Cisco IOS. Как вы это прокомментируете?

A. В представленном докладе не говорится ни о НОВЫХ уязвимых местах, ни о недостатках в IOS. Оригинальный доклад был результатом исследований, проводившихся компанией Internet Security Systems в области анализа атак на сетевое оборудование

(маршрутизаторы). Однако представленная в нем информация могла способствовать обнаружению новых уязвимостей, что привело бы к росту атак на сетевую инфраструктуру пользователей по всему миру, что, разумеется, было не в интересах компании Cisco. Проанализировав последствия опубликования доклада, компании Cisco и ISS приняли решение о снятии доклада с программы конференции.

При этом компания Cisco всегда была и остается сторонником проактивного подхода в защите бизнес-процессов наших заказчиков. Только своевременное обновление программного обеспечения (в т.ч. и для сетевого оборудования), а также активное внедрение решений и технологий в рамках стратегии Self-Defending Network поможет свести последствия от существующих и будущих атак к минимуму.

Дополнительная информация доступна по адресу: <http://www.cisco.com/security/security-alerts.html>

Q. Прокомментируйте сообщения прессы об утечке из Cisco исходных кодов. Были ли зафиксированы случаи взлома сетей ваших заказчиков вследствие данной утечки?

A. Больше года назад действительно был зафиксирован случай утечки части исходных кодов операционной системы Cisco IOS. Однако это произошло не из компании Cisco, а из сети одного из университетов, проводивших работы по контракту с Cisco. За прошедшие с момента инцидента больше года роста атак на наше сетевое оборудование не зафиксировано, что служит гарантией того, что в украденных фрагментах исходного кода не было обнаружено уязвимостей.

При этом компания Cisco всегда была и остается сторонником проактивного подхода в защите бизнес-процессов наших заказчиков. Только своевременное обновление программного обеспечения (в т.ч. и для сетевого оборудования), а также активное внедрение решений и технологий в рамках стратегии Self-Defending Network поможет свести последствия от существующих и будущих атак к минимуму.

Дополнительная информация доступна по адресу: <http://www.cisco.com/security/security-alerts.html>

Q. Существует ли связь между утечкой из Cisco исходных кодов и докладом на конференции Black Hat?

A. Никакой связи между утечкой части исходных кодов и докладом на конференции Black Hat нет.

Q. Прокомментируйте сообщения о разработке червя и большого числа других атак для IOS.

A. Данные новости не подтверждены никакими фактами. Любые спекуляции на эту тему до подтверждения факта якобы обнаруженных в Cisco IOS уязвимостях, позволяющих выполнять несанкционированные действия в сетях, построенных на нашем оборудовании беспочвенны.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Для получения дополнительной информации о решениях Cisco Systems в области информационной безопасности вы можете обратиться по электронной почте security-request@cisco.com.

ПРИЛОЖЕНИЕ 1. СПИСОК RFC, В СОЗДАНИИ КОТОРЫХ УЧАСТВОВАЛА КОМПАНИЯ CISCO

RFC 985

RFC 1858 (Security Considerations for IP Fragment Filtering)

RFC 1910 (User-based Security Model for SNMPv2)

RFC 1918 (Address Allocation for Private Networks)

RFC 1969 (The PPP DES Encryption Protocol (DESE))

RFC 2082 (RIPv2 MD5 Authentication)

RFC 2154 (OSPF with Digital Signatures)

RFC 2264, RFC 2274, RFC 2574 и RFC 3414 (User-based Security Model for SNMPv3)

RFC 2265, RFC 2275, RFC 2575 и RFC 3415 (View-based Access Control Model for the SNMP)

RFC 2267 и RFC 2827 (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)

RFC 2341 (Layer Two Forwarding)

RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH)

RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH)

RFC 2405 (The ESP DES-CBC Cipher Algorithm With Explicit IV)

RFC 2408 (Internet Security Association and Key Management Protocol, ISAKMP)

RFC 2409 (The Internet Key Exchange, IKE)

RFC 2410 (The NULL Encryption Algorithm and Its Use With IPsec)

RFC 2419 (The PPP DES Encryption Protocol, Version 2, DESE-bis)

RFC 2451 (The ESP CBC-Mode Cipher Algorithms)

RFC 2661 (Layer Two Tunneling Protocol, L2TP)

RFC 2725 (Routing Policy System Security)

RFC 2747 (RSVP Cryptographic Authentication)

RFC 2809 (Implementation of L2TP Compulsory Tunneling via RADIUS)

RFC 2867 (RADIUS Accounting Modifications for Tunnel Protocol Support)

RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)

RFC 2989 (Criteria for Evaluating AAA Protocols for Network Access)

RFC 3078 (Microsoft Point-To-Point Encryption Protocol, MPPE)



RFC 3079 (Deriving Keys for use with Microsoft Point-to-Point Encryption)

RFC 3118 (Authentication for DHCP Messages)

RFC 3129 (Requirements for Kerberized Internet Negotiation of Keys)

RFC 3130 (Notes from the State-Of-The-Technology: DNSSEC)

RFC 3156 (MIME Security with OpenPGP)

RFC 3162 (RADIUS and IPv6)

RFC 3174 (US Secure Hash Algorithm 1, SHA1)

RFC 3193 (Securing L2TP using IPsec)

RFC 3489 (Simple Traversal of User Datagram Protocol Through Network Address Translators)

RFC 3576 (Dynamic Authorization Extensions to RADIUS)

RFC 3579 (RADIUS Support For EAP)

RFC 3580 (IEEE 802.1X RADIUS Usage Guidelines)

RFC 3585 (IPsec Configuration Policy Information Model)

RFC 3711 (The Secure Real-time Transport Protocol, SRTP)

RFC 3740 (The Multicast Group Security Architecture)

RFC 3748 (EAP)

RFC 3826 (AES in the SNMP User-based Security Model)

RFC 3931 (L2TPv3)

RFC 3947 (Negotiation of NAT-Traversal in the IKE)

RFC 3948 (UDP Encapsulation of IPsec ESP Packets)

RFC 4017 (EAP Method Requirements for Wireless LANs)

RFC 4046 (Multicast Security Group Key Management Architecture)

RFC 4106 (The Use of Galois/Counter Mode (GCM) in IPsec ESP)

RFC 4176 (Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management)

SDEE, и другие.



Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: 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
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: 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
**Cisco Connection Online Web site at <http://www.cisco.com/>
<http://www.cisco.ru/>**

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