

## Значимость интегрированной безопасности

За последние двадцать лет сети из закрытых инфраструктур превратились в интегрированные системы, благодаря которым организации могут более тесно взаимодействовать с сотрудниками, партнерами, заказчиками и поставщиками, находящимися по всему миру, за счет подключения и автоматизации бизнес-процессов и приложений. Современная сеть представляет собой платформу делового общения между организациями и удаленными рабочими местами. К сожалению, одновременно идет и развитие угроз безопасности: периметр корпоративной сети размывается, угрозы все сложнее обнаруживать и устранять, фокусировка атак меняется с всеобщего охвата в «пользу» конкретной организации.

Нарушения безопасности могут настичь компанию из разнообразных источников, включая объединенные в сеть компьютеры и серверы компании. Пользовательские устройства сети подвергаются атакам новых червей и вирусов, поэтому перед небольшими предприятиями или офисами филиалов с ограниченным объемом ИТ-ресурсов стоит задача по нейтрализации этих проблем. Происходящие в результате этого потери данных, несоблюдение нормативных требований, связанные с отсутствием или неполной защитой информации ограниченного доступа, а также потеря доходов и производительности из-за простоев, побуждают организации вкладывать средства в системы обеспечения безопасности...<sup>1</sup>

В настоящее время в основе стратегии самозащищающейся сети Cisco Self Defending Network® лежат передовые системы защиты сети и оконечных устройств, объединяющие инновационные технологии безопасности приложений, контента, мониторинг средств защиты и соблюдения политик. Возможности набора продуктов Cisco со встроенными функциями безопасности, разработанного с помощью системного подхода к защите данных, предлагают комплексное решение для устранения современных угроз безопасности.

Компания Cisco помогает организациям создавать самозащищающиеся сети, обладающие ключевыми возможностями по обнаружению и предотвращению угроз, а также способные на них реагировать. Важной составляющей этой платформы являются маршрутизаторы с интеграцией сервисов Cisco ISR G2. Эти маршрутизаторы первыми стали осуществлять высокоскоростную, защищенную и интегрированную передачу различных видов трафика — голосовых, видео и обычных данных, а также обеспечивать развертывание других дополнительных сервисов на предприятиях малого и среднего бизнеса (SMB) и в филиалах корпораций.

В этом обзоре основное внимание уделяется меняющейся сфере обеспечения безопасности и встроенным функциям защиты маршрутизаторов с интеграцией сервисов Cisco ISR серий 800, 1900, 2900 и 3900. Наряду с тенденциями рынка, указывающими на растущие требования заказчиков к параллельному выполнению интегрированных сервисов в ИТ-инфраструктурах малых предприятий и филиалов, в этом документе рассмотрена значимость включения механизмов защиты в маршрутизатор. Кроме того, продемонстрировано эффективное решение современных и будущих проблем безопасности с помощью уникального системного подхода, разработанного компанией Cisco.

Данный материал не предназначен для использования в качестве руководства по техническому развертыванию. В нем представлены сведения о том, каким образом Cisco объединяет современные технологии обеспечения безопасности сети с двадцатилетним опытом в области маршрутизации, изменяя само понятия сетевой безопасности и предоставляя заказчикам комплексные решения по защите сети.

<sup>1</sup> Infonetics Research, Устройства и программное обеспечение для обеспечения сетевой безопасности, ежеквартальная доля на мировом рынке и прогнозы на 1 квартал 2008 года.

## Появление более изощренных угроз

В прошлом распространение угроз, исходящих из внутренних и внешних источников, было довольно медленным. В 1980-е годы эпидемии первого поколения вирусов (загрузочных вирусов, поражавших отдельные компьютеры) осуществлялись в течение нескольких недель. В 1990-е годы второе поколение угроз могло поражать свои жертвы уже за несколько дней. Они включали макровирусы, вирусы, заражавшие электронную почту, DoS-атаки и хакерские вторжения.

В современных условиях организации все еще вынуждены решать целый ряд сложных проблем, касающихся безопасности бизнеса, — от предотвращения потери и утечки данных до защиты от ботнетов и необходимости соответствия нормативным требованиям. Угрозы, общие для Web-трафика и трафика электронной почты, вредоносное ПО, программы-шпионы, Интернет-черви, вирусы и троянские программы распространяются по информационным сетям за считанные минуты, приводя к широкомасштабным заражениям и дорогостоящим повреждениям, не говоря уже о снижении производительности и расходах, вызванными простоями.

Согласно исследованию 2008 CSI Computer Crime and Security Survey, основной причиной материального ущерба являются финансовые махинации, обусловленные нарушениями системы безопасности. Потери в результате каждого подобного случая составляют около 500 000 долларов США. Немного меньше — около 350 000 долларов США — компании теряют из-за атак вредоносных программ и программ-ботов. Ущерб, вызванный потерей информации, являющейся собственностью компании, или утечкой конфиденциальных данных заказчиков или сотрудников, составляет в среднем 250 000 долларов США. Вполне очевидно, что об ослаблении сетевых атак не может быть и речи. В этом исследовании CSI также были установлены следующие факты<sup>22</sup>:

- по сравнению с другими типами угроз организации наиболее часто сталкиваются с атаками вирусов;
- Неправомерное использование сетей лицами внутри организации является второй наиболее часто возникающей ситуацией, за которой следуют кражи ноутбуков и других мобильных устройств;
- Количество атак на системы DNS с 2007 года выросло на 2%, затронув 10% всех компаний;
- Наблюдается рост направленных атак (вредоносного ПО, программных роботов и т. д.), охват этих атак составляет примерно 27% компаний;
- Свыше 68% компаний занимается разработкой и внедрением политик информационной безопасности ;
- Более 50% компаний считают, что их потери связаны с атаками, которые проводятся из-за пределов организации.

## Соблюдение нормативных требований требует должной проверки безопасности

Современные условия оказывают возрастающее давление на организации, требуя от них соблюдения отраслевых, государственных и федеральных требований, которые предназначены для обеспечения конфиденциальности, национальной безопасности и, во многих случаях, корпоративной ответственности. К примерам подобных нормативных актов можно отнести стандарт защиты данных для отрасли платежных карт PCI DSS, действующий для всех организаций, получающих, хранящих или передающих данные владельцев платежных карт.

В России можно выделить СТР-К — требования по защите данных в государственных учреждениях, стандарт Банка России по информационной безопасности СТО БР ИББС-1.0-2008 в банковской отрасли и требования ФСФР в сфере корпоративной отчетности. В соответствии с федеральным законом «О персональных данных», принятым в России,

<sup>22</sup> Исследование «2008 CSI Computer Crime and Security Survey»

обработка таких личных данных, осуществляется только при соблюдении заданного уровня обеспечения безопасности.

Штрафы, взыскания, судебные разбирательства — это лишь часть того, через что может пройти компания в случае нарушения системы безопасности и несоблюдения нормативных требований. Невыполнение нормативных актов наносит вред имиджу компании и ее репутации, которые иногда невозможно восстановить.

### **Продолжающийся рост требований к безопасности маршрутизаторов**

Мировой рынок интегрированных средств безопасности продолжает развиваться. "Рост в этой области можно приписать продажам высокопроизводительных продуктов, поддерживающих маршрутизацию, для филиалов; с течением времени мы ожидаем увеличения прибыли в филиалах в результате перехода от изолированных устройств к маршрутизаторам с интегрированными функциями безопасности".<sup>3</sup> Infonetics прогнозирует, что в течение следующих четырех лет развитие рынка маршрутизации будет вполне успешным. В начале 2008 года прибыль от продажи продуктов ценового диапазона от 1 500 до 29 999 долларов США составляла более трети в секторе интегрированных устройств безопасности, но большая часть этого рынка уже теряет часть своей популярности, уступая предназначенным для филиалов маршрутизаторам с интегрированным межсетевым экраном и VPN.

Согласно Infonetics, "многие мультипротокольные маршрутизаторы были приобретены до и во время Интернет-бума (1996-2001) и в настоящее время их жизненный цикл завершается", поэтому компании, стремящиеся заменить старые мультипротокольные маршрутизаторы новыми, будут искать продукты, поддерживающие широкий ряд IP-сервисов, в т. ч. и направленных на поддержку развитых механизмов обеспечения безопасности.

Развитие решений по безопасности необходимо для соответствия меняющимся в этой области требованиям, и компания Cisco продолжает устанавливать стандарты, разрабатывая инновационные решения по безопасности, удовлетворяющие постоянно меняющимся запросам предприятий в реальном мире. Благодаря таким возможностям, как Cisco Group Encrypted Transport (GET VPN), фильтрация контента средствами Cisco IOS и усовершенствованные средства передачи голосовых данных через межсетевой экран Cisco IOS, предприятия могут сконцентрироваться на выполнении современных требований безопасности при одновременном формировании будущих требований к сети.

Компания Cisco придерживается системного подхода в обеспечении информационной безопасности, при котором меры, принимаемые для защиты ресурсов, должны соответствовать требованиям к полосе пропускания. И как результат, Cisco встраивает функции сетевой защиты во все маршрутизаторы с интеграцией сервисов и маршрутизаторы агрегации сервисов Cisco ASR.

### **Значимость средств обеспечения безопасности, интегрированных в маршрутизаторы**

Прямая интеграция средств безопасности в ПО Cisco IOS, под управлением которого функционируют маршрутизаторы, имеет ряд преимуществ. Во-первых, используются все преимущества существующей сетевой инфраструктуры; для установки новых функций безопасности в маршрутизатор с помощью ПО Cisco IOS не требуется развертывать дополнительное оборудование. В этом случае происходит экономия времени и средств, поскольку сокращается количество устройств в сети, снижаются расходы на обучение и управление, а также снижается совокупная стоимость владения (TCO). Дополнительные сведения см. в публикации "[Оптимизация TCO инфраструктуры сети офиса филиала с помощью Cisco ISR](#)".

Во-вторых, благодаря интеграции происходит гибкое применение средств обеспечения безопасности, например межсетевого экрана, системы предотвращения вторжений и VPN, в любой точке сети для максимальной защиты от угроз безопасности. Сочетание

<sup>3</sup> Infonetics Research, Устройства и программное обеспечение для обеспечения сетевой безопасности, ежеквартальная доля на мировом рынке и прогнозы на 1 квартал 2008 года.

функций безопасности на основе маршрутизаторов и коммутаторов представляет собой комплексную систему безопасности в масштабах всей сети.

В-третьих, интеграция средств безопасности непосредственно в ПО Cisco IOS маршрутизатора обеспечивает защиту сетевых шлюзов, поскольку маршрутизаторы Cisco ISR G2 являются первыми точками входа в сеть, а маршрутизатор Cisco ASR — точкой входа в центр обработки данных. Таким образом, лучшие в своем классе функции обеспечения безопасности развертываются на всех точках входа в сеть, представляющих собой логические пункты для защиты сети. Средства безопасности, встроенные в маршрутизатор, не только защищают первую точку входа в сеть, но и используют преимущество интеллекта маршрутизатора как "надежного устройства обработки" трафика, объединяющего больше дополнительных возможностей защиты, качества обслуживания и маршрутизации.

В этом случае средства безопасности могут пользоваться общими данными и координировать быстрые и точные ответные действия на угрозы, обеспечивая при этом высокую доступность сети. Интегрированные средства защищают и сам маршрутизатор, создавая линию обороны от атак, направленных непосредственно на инфраструктуру сети, например DDoS-атак. Многие доступные специализированные решения по безопасности защищают отдельные компоненты сети, и лишь небольшая часть решений может защитить всю инфраструктуру, обеспечив безопасность всех элементов сети так, как это можно сделать с помощью набора решений по безопасности от компании Cisco.

### **Экологичность**

Местные и глобальные инициативы по охране окружающей среды приобретают серьезное коммерческое значение на рынке. Все больше и больше руководители говорят о проблемах, связанных с охраной окружающей среды, и выносят их на первые места при реализации определенных корпоративных программ. В ряде отчетов Межправительственной группы по климатическим изменениям при ООН (U.N. Intergovernmental Panel on Climate Change) представлены факты, свидетельствующие о том, что деятельность человека — в особенности, выбросы диоксида углерода — является основной причиной глобального изменения климата. Эти тенденции оказывают возрастающее давление на высшее руководство компании, требуя сокращения выбросов углерода во время производства.

Очень важно решать проблемы, касающиеся защиты окружающей среды, которые могут быть разными в зависимости от размеров компании. Основными моментами, на которые обращается внимание в любой организации, являются потребности в энергоснабжении, расходы на командировки сотрудников и неоправданный расход электроэнергии. Компания Cisco подтверждает свои притязания на отраслевое лидерство в сфере сохранения ресурсов.

Одним из способов сокращения потребления энергии и ресурсов на охлаждения в офисе филиала является объединение возможностей и функций и использование в результате этого меньшего количества систем. Средства обеспечения безопасности, реализованные в маршрутизаторах, служат примером того, что компания Cisco прилагает значительные усилия по обеспечению эффективной и рациональной работы ИТ-систем в офисах филиалов. Дополнительные сведения см. в документе ["Сокращение потребления энергии за счет интегрированного предоставления услуг"](#).

### **Высокая доступность в офисе филиала**

Cisco предлагает поистине огромный набор возможностей для обеспечения высокой степени готовности и доступности дополнительных офисов и филиалов. Изначально разработанная для постоянно доступных сетей, сквозная концепция Cisco предоставляет ИТ-подразделениям архитектуру самозащищающейся сети, которая проста в развертывании и обслуживании. Маршрутизатор Cisco ISR G2 еще больше укрепляет этот подход за счет одновременного использования нескольких интерфейсов и функций, повышая при этом производительность нескольких параллельно выполняющихся сервисов безопасности, управления и интеграции.

Маршрутизатор Cisco ISR G2 является комплексным решением для обеспечения высокой готовности допфилиалов и филиалов, которое сокращает простои сети и

обеспечивает постоянный доступ к самым необходимым для предприятия приложениям. Внимание, уделяемое компанией интеграции новых сервисов инфраструктуры и производительности, позволяет предприятиям создавать более интеллектуальные, гибкие и надежные сети. Дополнительные сведения о решении Cisco в области высокой доступности для офисов филиалов и небольших компаний см. в официальном документе "[Обеспечение максимальной доступности в филиале с помощью маршрутизатора с интеграцией сервисов](#)".

### Производительность

Маршрутизаторы Cisco ISR G2, использующие системный подход, должны обеспечивать производительность, соответствующую пропускной способности канала подключения к глобальной сети. Это значит, что если заказчики включают дополнительные сервисы, например передачу голосовых данных или защиту, производительность не падает ниже скорости соответствующего интерфейса WAN. Маршрутизаторы с интеграцией сервисов оптимизированы для параллельного выполнения разных сервисов с определенной мощностью центрального процесса (ЦП), а сервисы с высокой интенсивностью использования ЦП, переводятся на выделенные акселераторы.

Cisco пригласила компанию Mier Communications, Inc. для независимой проверки настройки, эксплуатации и производительности маршрутизаторов с интеграцией сервисов. Miercom подтвердила производительность этих систем во время одновременного предоставления важных высокоуровневых сетевых сервисов для филиала организации, включая межсетевой экран Cisco IOS, технологию преобразования сетевых адресов (NAT), систему предотвращения вторжений (IPS), связь VoIP и услуги аналоговой телефонии, причем это было сделано в условиях интенсивной передачи данных. Тесты также подтвердили гарантированное качество голосовых служб во время сильной транспортной нагрузки. Итоговые отчеты Miercom см. на странице <http://www.miercom.com>.

### Интеллект

Системный подход начинается с единой гибкой платформы, такой как маршрутизаторы Cisco ISR G2, который затем выходит за рамки принципа "все в одном". Системный подход сочетает пакет с интеллектуальными сервисами внутри служб и между ними. Совместная работа сервисов предоставляет реальные преимущества, например динамически меняющуюся связную сеть VPN (Dynamic Multipoint VPN, DMVPN) для функционирования динамических туннелей или VPN с поддержкой голоса и видео (V3PN), как показано на рисунке 1.

Рисунок 1. Безопасная качественная IP-телефония с использованием DMVPN



#### Требования

- Шифрование на скорости передачи
- Полносвязная конфигурация, уровень сложности соответствует звезде
- Приоритезация голоса/видео
- Экономия пропускной способности
- VPN с поддержкой нескольких сервисов
- Поддержка SRTP

#### Преимущества

- Простота управления и настройки
- Передача трафика с шифрованием
- Высокое качество голосовой и видеосвязи
- DMVPN обеспечивает динамическое создание туннелей
- Защита в глобальной сети, снижение затрат
- Защита в локальной сети

Системный подход объединяет сервисы по передаче голосовых данных, службы безопасности и маршрутизации, а также службы приложений, поэтому процессы становятся более автоматизированными и интеллектуальными. Результатами являются

всеохватывающая безопасность сети и приложений, более высокое качество обслуживания (QoS) трафика голосовых, видео- и обычных данных, высокая доступность сети и, соответственно, повышенная производительность. Благодаря этому подходу можно выполнять следующие задачи:

- быстрее разворачивать базовые и дополнительные сервисы;
- управлять этими сервисами с помощью общих средств и интерфейсов, упрощающих выполнение операций;
- укреплять сетевую безопасность путем сокращения количества отдельных блоков, которые должны быть заблокированы;
- пользоваться преимуществами существующих и будущих интерфейсов и сетевых модулей, ускоряющих доставку данных и высвобождающих оборудование для новых приложений;
- быстрее устранять неполадки, проще устанавливать запасные части, более эффективно обучать сотрудников, т. е. способствовать сокращению эксплуатационных затрат;
- пользоваться преимуществами сформированных наборов решений и соглашений об обслуживании для снижения капитальных затрат.

### Отличительные функции безопасности маршрутизатора

Основанные на двадцатилетнем лидерстве компании и поддерживающие инновации, маршрутизаторы Cisco с интеграцией сервисов Cisco ISR G2 и маршрутизаторы агрегации Cisco ASR поставляются с комплексным набором сервисов безопасности, интеллектуально встраивая данные, безопасность и голос в единую надежную систему для быстрой и масштабируемой доставки критически важных бизнес-приложений.

При разработке семейств маршрутизаторов Cisco ISR G2 и маршрутизаторов Cisco ASR в качестве основного компонента была принята безопасность, при этом аппаратное шифрование стало стандартной функцией. Встроенные аппаратные механизмы ускорения шифрования снимают нагрузку с VPN-процессов, обеспечивая повышенную пропускную способность VPN с минимальным воздействием на ЦП маршрутизатора. Если требуется дополнительная пропускная способность VPN или масштабируемость (например, больше туннелей VPN), можно воспользоваться дополнительными модулями AIM для шифрования трафика и организации VPN. Безопасность маршрутизации касается не только VPN. ПО Cisco IOS предлагает набор интегрированных технологий управления угрозами, а также другие средства для нейтрализации угроз и защиты бизнеса (см. рис. 2).

Рисунок 2. Технологии безопасности, реализованные в маршрутизаторах



### VPN для безопасного взаимодействия

"Большинство конечных пользователей все еще переходит от модели централизованного подключения к Интернету к распределенному подключению, которое будет продолжаться как минимум еще пять лет; широкополосный доступ к Интернету требует минимальных расходов и широко доступен, поэтому имеет смысл воспользоваться экономией средств и функциями безопасности, предлагаемыми сетями VPN и распределенным Интернет-подключением."<sup>4</sup>

Гарантия конфиденциальности и целостности всех данных имеет очень важное значение для бизнеса. Поскольку для расширения единого информационного пространства до допозисов и филиалов, удаленных работников, заказчиков и партнеров компании используют гибкость и экономичность Интернета, обеспечение безопасности является главным вопросом. Создание защищенной, управляемой и экономически эффективной инфраструктуры имеет следующие преимущества:

- улучшение производительности;
- повышение эффективности бизнеса;
- соблюдение нормативных требований о конфиденциальности данных.

### Cisco VPN: туннелирование и шифрование

Сети VPN — это наиболее быстро развивающаяся форма соединения сетей. Во все маршрутизаторы Cisco с интеграцией сервисов и агрегации входят встроенные аппаратные механизмы ускорения шифрования VPN, которые снимают нагрузку при шифровании IPSec и обеспечивая VPN-процессам повышенную пропускную способность с минимальным воздействием на ЦП. Эта возможность поддерживает для протокола IPSec такие стандарты шифрования как Advanced Encryption Standard (AES), Digital Encryption Standard (DES) и Triple DES (3DES) без использования слота AIM.

Компании, которым требуется дополнительная пропускная способность или масштабируемость VPN, могут воспользоваться дополнительными модулями AIM для шифрования VPN. В результате повышается производительность VPN и снижается общее использование ЦП маршрутизатора. По сравнению с предыдущими моделями дополнительный модуль повышает производительность шифрования почти в 10 раз.

Если организация планирует передавать по каналам связи информацию, требующую защиты в соответствие с российским законодательством, то для этой цели компания Cisco совместно с двумя российскими компаниями С-Терра СиЭсПи и ИнфоТеКС разработала специализированные аппаратные модули NME-RVPN и NME-RVPN VipNet, которые используют отечественные алгоритмы криптографической защиты информации, в частности, ГОСТ 28147-89. При этом криптографическое ядро, использованное в данном модуле, интегрируемое в маршрутизаторы Cisco ISR G2, имеет сертификат Федеральной службы безопасности России (ФСБ). Аналогичные модули были разработаны для выполнения украинских (модуль «Булава» - совместно с НПО «Криптон») и казахских (модуль KazVPN – совместно с компанией ZorSoft) регулятивных требований. В 2010 году модуль NME-RVPN (в варианте исполнения "модуль сетевой модернизированный" или MCM) получил сертификат ФСБ России по классу КС1 (сертификат № СФ/114-1411 от 20 марта 2010 г.).

Маршрутизаторы Cisco поддерживают различные решения для VPN, предназначенные для удовлетворения уникальных потребностей современных организаций, включая следующие:

- **IPSec на основе стандартов.** Поддерживает простые подключения типа "сеть-сеть" для связи удаленных расположений и головных офисов, при которой отсутствует необходимость в динамической маршрутизации или QoS
- **Easy VPN.** Предлагает высокомасштабируемые топологии типа "звезда" с использованием технологии "проталкивания политики" (policy-push) для упрощения

<sup>4</sup> Infonetics Research, Устройства и программное обеспечение для обеспечения сетевой безопасности, ежеквартальная доля на мировом рынке и прогнозы на 1 квартал 2008 года.

управления, при этом сохраняется широкий спектр настроек и контроль над соблюдением политик

- **DMVPN.** Использование VPN по требованию и масштабируемой полносвязной сети VPN для сохранения полосы пропускания и упрощения развертывания VPN
- **Group Encrypted Transport VPN.** Предоставляет простое в управлении шифрование для частных сетей WAN с использованием общих способов защиты, а не межточечных туннелей IPSec.

#### **Безопасная передача голосовых и видеоданных**

Функции проверки подлинности и шифрования данных в маршрутизаторах Cisco ISRG2 обеспечивают защиту голосовой связи, осуществляющуюся либо на портах TDM, либо на портах аналогового голосового шлюза, от прослушивания. Эти надежные и масштабируемые возможности создают безопасные условия для IP-связи по сетям LAN или WAN. При шифровании данных мультимедиа с помощью протокола SRTP выполняется шифрование голосовой связи, которая становится непонятной для внутренних или внешних злоумышленников, которые проникли в сеть и получили доступ к голосовому домену. Являясь стандартом IETF RFC 3711, протокол SRTP разработан специально для передачи голосовых пакетов, он поддерживает алгоритм шифрования AES. При шифровании медиаданных с помощью SRTP полоса пропускания используется более эффективно, чем при использовании IPSec.

Для передачи высококачественных голосовых и видео данных через IPSec или SSL VPN требуется не просто шифрование трафика, необходимо сочетание передовых сетевых технологий, к числу которых можно отнести мультисервис-центрическое QoS, поддержка различных типов и приоритезация трафика, поддержка многофункциональных сетевых топологий и улучшенные возможности переключения при отказах сети.

#### **Аспекты безопасности Multi-VRF и MPLS для операторов связи**

Multi-Virtual Route Forwarding (VRF) является расширением IPSec VPN типа "сеть-сеть". Предприятия вправе ожидать, что передаваемый через сеть оператора связи трафик будет защищен и сохранит конфиденциальность. Однако отделение трафика в обычной сети LAN становится все сложнее. Этот процесс особенно важен при развертывании в нескольких офисах филиалов. Multi-VRF сохраняет конфиденциальность между сегментами приемлемым и удобным способом.

Дополнительные сведения о VPN IOS Cisco см. по адресу <http://www.cisco.com/go/vpn>.

#### **Управление угрозами**

Система интегрированного управления угрозами Cisco предлагает комплексную защиту сети с помощью упрощенного управления политиками и упреждающей системы защиты системы. Она предназначена для выполнения следующих задач:

- защита сети, серверов, оконечных устройств и данных от широкого спектра угроз;
- контроль доступа в сеть, изоляция инфицированных систем, предотвращение вторжений, защита важных бизнес-активов;
- нейтрализация вредоносного трафика, например червей, вирусов, и вредоносного ПО, прежде чем они окажут негативное влияние на бизнес.

#### **Межсетевой экран Cisco IOS Firewall**

Межсетевой экран (МСЭ) Cisco IOS Firewall, получивший наряду с сертификатом Common Criteria (EAL4) еще и сертификат ФСТЭК по 4-му классу защищенности для МСЭ, является средством защиты с технологией инспекции пакетов с учетом состояния, интегрированным в маршрутизаторы Cisco. Используя преимущества тех же самых технологий межсетевой защиты с учетом состояния, применяемых в межсетевом экране Cisco PIX® и адаптивных устройств безопасности Cisco ASA 5500, он обеспечивает высокую доступность сети и безопасность информационных активов компании за счет защиты инфраструктуры сети от атак сетевого и прикладного уровней, а также от вирусов и червей. Межсетевой экран Cisco IOS Firewall не только является надежной

точкой защиты в периметре сети, но и делает соблюдение политики безопасности неотъемлемым компонентом самой сети. Он защищает систему унифицированных коммуникаций, обеспечивая безопасность оконечных устройств, поддерживающих протокол SIP, и ресурсов управления вызовами. Межсетевой экран Cisco IOS реализует следующие ключевые функции:

- Межсетевой экран приложений. Контролирует трафик, инкапсулирует в HTTP, и гарантирует, что он является допустимым и соответствующим политике безопасности организации, а не трафиком систем обмена мгновенными сообщениями или сходным с ним, который пытается проникнуть через межсетевой экран.
- Прозрачный межсетевой экран 2-го уровня. Обеспечивает высокий уровень защиты на канальном уровне, что позволяет реализовать прозрачное внедрение МСЭ в сеть, не требующее изменение топологии и не видимое злоумышленниками.
- Межсетевой экран на основе зон. Предоставляет понятный интерфейс для настройки детализированных политик межсетевого экрана, соответствующих политикам безопасности информации для бизнеса, за счет строгого контроля доступа к сетевым службам.

Дополнительные сведения о межсетевом экране Cisco IOS см. по адресу <http://www.cisco.com/go/iosfw>.

### **Система предотвращения вторжений Cisco IOS IPS**

Компания Cisco первой в отрасли предложила маршрутизаторы с встроенной системой предотвращения атак (IPS). Cisco IOS IPS — это решение, основанное на глубокой проверке пакетов, которое расширяет функциональность межсетевого экрана Cisco IOS Firewall, помогая ему эффективно нейтрализовывать сетевые атаки. Cisco IOS IPS применяется для предотвращения вторжений и оповещения о событиях, могущих негативно повлиять на защищенность сети. В этой системе используются технологии, реализованные в продуктах системы предотвращения вторжений (IPS) компании Cisco, в числе которых сенсоры Cisco IPS 4200, модуль системы обнаружения вторжений Cisco CatalystDSM-2 и модули системы предотвращения атак для маршрутизаторов Cisco AIM-IPS и многофункциональных защитных устройств Cisco ASA 5500 – Cisco AIP-SSM.

Поскольку система Cisco IOS IPS включается в разрыв сети, она может блокировать трафик, помогая маршрутизатору мгновенно реагировать на угрозы безопасности и защищать сетевые ресурсы. За счет взаимодействия с IPSec VPN, механизмами инкапсуляции GRE и межсетевым экраном Cisco IOS Firewall система Cisco IOS IPS может эффективно бороться с атаками в зашифрованном трафике, выполняя его расшифрование, терминование VPN-туннелей, использовать средства межсетевой защиты и проверять трафик в первой точке входа в сеть (в сегменте или концентраторе).

Система Cisco IOS IPS помогает блокировать трафик атаки как можно ближе к источнику его возникновения. Дополнительные сведения о системе IPS Cisco IOS см. по адресу <http://www.cisco.com/go/iosips>.

### **Средства фильтрации контента Cisco IOS**

Средства фильтрации контента Cisco IOS помогают предприятиям организовать защиту от известных и новых Интернет-угроз, повысить производительность сотрудников и обеспечить выполнение политик по соблюдению нормативных требований. Средства фильтрации контента в Cisco IOS выполняют следующие задачи:

- мониторинг и контроль действий сотрудников в Интернете путем блокировки или ограничения доступа к определенным web-узлам;
- обеспечение защиты от узлов, с которых могут распространяться вредоносные, рекламные программы, программы-шпионы, фишинг и т.п.;
- помощь организациям в эффективном управлении сетевыми ресурсами с простым развертыванием.

### **Дополнительные возможности безопасности**

По Cisco IOS предлагает дополнительные технологии безопасности для интеллектуальной защиты оконечных устройств сети.

- NAC (Network Admission Control) — это общепромышленная разработка под руководством Cisco, которая обеспечивает проверку соответствия каждого конечного узла политикам сетевой безопасности и ИТ-политикам до того, как этому узлу будет предоставлен доступ в сеть. NAC ограничивает ущерб, причиняемый вирусами и червями, путем опроса устройств, пытающихся получить доступ к сетевым ресурсам, для проверки их соответствия последним корпоративным политикам безопасности. Только после этого устройства получают доступ в сеть. Уязвимые и не отвечающие требованиям хосты изолируются или получают ограниченный сетевой доступ до тех пор, пока не будут внесены обновления и обеспечена их безопасность. Так исключается риск того, что эти хосты могут стать источником распространения эпидемий или мишенью для червей и вирусов.
- В приложениях, соответствующих стандарту 802.1x, неавторизованный доступ к защищенным информационным ресурсам затруднен, поскольку для этого требуются действующие учетные данные доступа. Развертывая приложения, соответствующие стандарту 802.1x, администраторы сетей также могут фактически исключить возможность создания пользователями незащищенных точек беспроводного доступа, т.е. решить одну из важнейших проблем в применении легко развертываемого оборудования беспроводных сетей (WLAN).
- Network Foundation Protection (NFP) защищает сам маршрутизатор от атак на него. В качестве примеров можно назвать реализацию политик на уровне управления (Control Plane Policing), функцию автоматического отключения ненужных сервисов AutoSecure, распознавание сетевых приложений (Network-Based Application Recognition, NBAR) и т.п.
- Механизмы гибкого анализа пакетов FPM дополняют систему IPS Cisco IOS, поддерживая настраиваемые фильтры, которые можно определить и развернуть быстрее, чем будет выполнено обновление сигнатур IPS или антивирусных шаблонов. Благодаря этому администраторы безопасности сети получают мощные средства для выявления вредоносного трафика, его сброса или регистрации с целью проверки.

### **Сервисы безопасности в модулях безопасности маршрутизаторов Cisco**

Заказчики, которым требуется дополнительная производительность для ряда защитных функций, могут воспользоваться специальными аппаратными модулями для маршрутизаторов с интеграцией сервисов Cisco 1900, Cisco 2900 и 3900 Series: сервисный модуль AIM для Cisco IPSec VPN, модуль AIM системы предотвращения вторжений (IPS) Cisco, сетевой модуль Cisco NAC, а также сетевой модуль для реализации отечественных криптографических алгоритмов NME-RVPN.

### **Управление безопасностью маршрутизации**

Для управления небольшим количеством устройств существуют встроенные системы — Router and Security Device Manager (SDM) и Cisco Configuration Professional. Они сочетают управление службами маршрутизации и безопасности и простоту использования, интеллектуальные мастера настройки и широкие возможности устранения неполадок, предоставляя единое средство управления, поддерживающее преимущества интеграции сервисов в маршрутизатор. Заказчики могут синхронизировать политики маршрутизации и безопасности во всей сети, пользоваться более полным представлением состояния сервисов маршрутизатора и сокращать эксплуатационные расходы.

Для управления функциями безопасности в масштабах всего предприятия Cisco предлагает семейство Security Management Suite, представляющее собой систему управления Cisco Security Manager и систему мониторинга безопасности Cisco MARS.

Дополнительные сведения о системе управления Cisco Security Manager и системе мониторинга Cisco Security MARS см. на странице <http://www.cisco.com/go/mars>.

### **Выделенные устройства обеспечения безопасности или маршрутизатор с интеграцией сервисов?**

Компания Cisco предлагает как функции защиты, встроенные в маршрутизаторы, так и специальные выделенные устройства безопасности, чтобы заказчики смогли сделать выбор относительно оптимальной защиты сетей. Несмотря на то что, грань между интегрированной безопасностью и отдельными устройствами становится все менее заметной, существует несколько причин, по которым заказчик может предпочесть одно решение другому или выбрать комбинацию решений.

### **Интегрированные функции безопасности идеально подходят для предприятий малого бизнеса и офисов филиалов**

Согласно предположениям большинства исследований отраслевого рынка одним из важных условий является расположение сети, безопасность которой необходимо обеспечить. Многие компании принимают решение об интеграции средств безопасности в пограничные маршрутизаторы агрегации. Однако более крупные предприятия могут выбрать защиту головных узлов или центров обработки данных с помощью отдельных устройств, поскольку для этих областей сети требуется высокая пропускная способность. Эти же организации могут остановить свой выбор на защите всех компонентов сети за счет установки маршрутизаторов со встроенными функциями безопасности в допотофисах и филиалах.

Перед офисами небольших и средних предприятий и офисами филиалов стоят те же самые проблемы безопасности, что и перед головными офисами корпораций, однако они обычно располагают небольшим количеством локальных ИТ-ресурсов для управления решениями по безопасности либо эти ресурсы отсутствуют вообще. Развертывание и управление несколькими устройствами с помощью ограниченных ИТ-ресурсов может не соответствовать модели поддержки предприятия.

Для таких моделей интеграция нескольких функций в одну платформу с центральным управлением может решить вопросы, связанные с устранением неполадок и обслуживанием устройств в небольших офисах, и привести к сокращению совокупной стоимости владения.

Маршрутизаторы с интеграцией сервисов Cisco серий 800, 1900, 2900 и 3900 идеально подходят для предприятий малого бизнеса и офисов филиалов, являясь многофункциональным интегрированным решением для подключения дополнительных сетей удаленных офисов, мобильных пользователей и партнеров или оборудования, которое устанавливается на территории абонента и управляется поставщиком услуг. Имея в своем распоряжении ПО VPN, межсетевой экран, систему предотвращения атак, систему фильтрации контента, а также дополнительное аппаратное шифрование и модули IPS (для маршрутизаторов Cisco серий 2900 и 3900), Cisco предлагает самое надежное и адаптируемое в отрасли решение безопасности для маршрутизаторов уровня филиала.

### **Предпочтения компаний**

На выбор между решениями интегрированной безопасности и специализированными решениями может оказать влияние желание воспользоваться преимуществами существующей инфраструктуры, развертывания, эксплуатационной архитектуры или отличиями определенных функций. Некоторые компании просто предпочитают, чтобы "маршрутизаторы маршрутизировали, а коммутаторы коммутировали". Или с точки зрения управления, компания может решить отделить инфраструктуру обеспечения безопасности и VPN от сетевых инфраструктур, поскольку в ней данные задачи разнесены по разным подразделениям – ИТ и безопасности.

### **Оценка будущих расходов**

Использование существующих маршрутизаторов или коммутаторов для обеспечения безопасности путем добавления или простого включения подсистем безопасности Cisco IOS является экономически выгодным вариантом продления периода развертывания

инфраструктуры. В этом случае обеспечивается высокий уровень возврата первоначальных инвестиций, значительно сокращаются будущие расходы и исключается остановка бизнеса, связанная с непродуманной заменой устройств. Самым значимым фактором при оценке будущих расходов могут стать расходы, относящиеся к запланированным и внеплановым простоям. Усовершенствованные возможности интегрированных сервисов усиливают общую гибкость и доступность сети, подготавливая сеть к дальнейшим развертываниям конвергентных мультимедийных технологий. Благодаря этому организации смогут быстрее реагировать и не упускать возможности для бизнеса, сократить общее время развертывания новых сервисов, исключить ненужные обновления устройств и снизить ТСО.

### Отличия функций

В связи с тем, что Cisco интегрирует технологию из устройств безопасности в программное обеспечение для безопасности Cisco IOS, наборы функций стали очень похожими. Однако при этом существуют и характерные для технологии различия. Прежде чем принимать какие-либо решения, организации должны понимать свои потребности в обеспечении безопасности и уровне производительности.

### Соответствие требованиям

Информационная безопасность – это тема, которая по-разному регулируется в разных странах мира. Именно поэтому Cisco старается учитывать локальные требования в области информационной безопасности. В России функции безопасности, интегрированные в маршрутизаторы Cisco ISR G2, были многократно проверены Федеральной службой по техническому и экспортному контролю (ФСТЭК России), которая выдала несколько десятков сертификатов соответствия требованиям отечественным нормативных документов в области безопасности информации. В частности, Cisco ISR были сертифицированы по 4-му классу защищенности для межсетевых экранов по схеме «сертификация производства». Также необходимо отметить, что модуль построения VPN NME-RVPN, разработанный совместно с компанией С-Терра СиЭсПи, получил признание ФСБ России, выраженное в сертификате соответствия по классу КС1.

### Резюме

Сфера обеспечения безопасности переживает период быстрого развития, связанный с возникновением новых угроз, поэтому очень сложно точно предсказать, что произойдет в ближайшие несколько лет, однако "когда речь идет о безопасности, мы верим в то, что пользователи всегда будут использовать функции безопасности в разнообразных представлениях, и в то время как расходы могут меняться между категориями и типами устройств, основные тенденции роста не изменяются"<sup>5</sup>.

В списке приоритетов руководителей ИТ-отделов сетевая безопасность занимает одно из ведущих мест, что связано с реальным ростом угроз безопасности. В связи с ростом требований безопасности компания Cisco, располагая интегрированными решениями по безопасности, которые защищают все точки входа в сеть, модернизирует набор продуктов защиты для значительного улучшения возможностей сети по обнаружению, предотвращению угроз и реагирования на них. Построенные с использованием аппаратного ускорения, маршрутизаторы Cisco ISR G2 с интеграцией сервисов объединяют службы VPN, межсетевого экрана, системы IPS, а также средства фильтрации контента в рамках набора продуктов маршрутизации Cisco, предоставляя самые комплексные и адаптивные в отрасли решения по безопасности. Эти маршрутизаторы удовлетворяют требованиям офисов филиалов, которым интегрированная безопасность необходима для сокращения числа операционных систем и устройств, управляемых с использованием ограниченных ИТ-ресурсов.

Благодаря сочетанию надежных функций ПО Cisco IOS и широкого ряда возможностей подключения LAN и WAN с инновационными функциями безопасности, интегрированные решения безопасности Cisco позволяют компаниям воспользоваться преимуществами существующей сетевой инфраструктуры и развертывать решения там, где они наиболее

<sup>5</sup> Infonetics Research, Устройства и программное обеспечение для обеспечения сетевой безопасности, ежеквартальная доля на мировом рынке и прогнозы на 1 квартал 2008 года.

необходимы. Вместо добавления оборудования ПО Cisco IOS позволяет заказчикам просто "включить" функции безопасности в маршрутизаторах и применить их в любой точке сети.

#### **Получение дополнительной информации**

Дополнительные сведения об интегрированных функциях обеспечения безопасности в модульных маршрутизаторах с интеграцией сервисов Cisco серий 1900, 2900 и 3900 см. в следующих документах в Интернете:

- Брошюра о самозащищающейся сети Cisco

[http://www.cisco.com/web/RU/downloads/Core\\_SDN\\_elements\\_wp.pdf](http://www.cisco.com/web/RU/downloads/Core_SDN_elements_wp.pdf)

- Функции безопасности в маршрутизаторах Cisco с интеграцией сервисов

[http://www.cisco.com/en/US/products/ps5854/products\\_data\\_sheet0900aecd80169b0a.html](http://www.cisco.com/en/US/products/ps5854/products_data_sheet0900aecd80169b0a.html)

Сведения о дополнительных решениях для безопасности маршрутизаторов и сопутствующих продуктах см. на странице по адресу

<http://www.cisco.com/go/routersecurity>.



Cisco  
Россия, 115054, Москва,  
бизнес-центр «Риверсайд Тауерс»,  
Космодамианская наб., 52, стр. 1, 4-й этаж.  
Телефон: +7 (495) 961 1410  
Факс: +7 (495) 961 1469  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://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](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Россия, 630099, Новосибирск,  
бизнес-центр «Росевроплаза»,  
Димитрова пр-т, 2, 5-й этаж.  
Телефон: +7 (383) 230 2670  
Факс: +7 (383) 230 1795  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://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](http://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, Aironet, 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, PowerPanels, 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)