Безопасность IP-сетей нового поколения для провайдеров услуг

В архитектуре IP-сетей нового поколения (NGN) Cisco® функции безопасности могут быть интегрированы в инфраструктуру сети на всех уровнях. Вопросы информационной безопасности учтены в технологиях, политиках, средствах мониторинга и дополнительных функциях защиты на всем пути передачи данных – от сетей провайдеров услуг до устройств конечных пользователей. Эволюционно развивающиеся решения в области обеспечения безопасности, предлагаемые компанией Cisco, позволяют провайдерам услуг расширить существующие коммерческие предложения, внедрить новые услуги для получения дополнительных доходов, а также обеспечить клиентам ту степень защиты и уверенности, которая необходимы при работе в сетевой среде, в которой присутствуют разноплановые и смешанные угрозы безопасности, комбинируются и совместно используются различные методы проведения атак. Средства обеспечения безопасности интегрированы в фундамент архитектуры Cisco IP NGN и предназначены для нейтрализации широкого спектра сетевых угроз, которые существуют уже сегодня или обрушатся на сети завтра.

В этом документе рассмотрен ряд наиболее распространенных угроз, способных препятствовать стабильному предоставлению сервисов и непрерывному осуществлению деловой активности, а также описана роль средств обеспечения безопасности Cisco IP NGN в защите от этих угроз. Архитектура безопасности Cisco IP NGN включает модель процесса функционирования сети для решения задач комплексной экспертизы безопасности, разработки и внедрения средств обеспечения безопасности. Эта модель также помогает оценить экономическую и функциональную эффективность сервисов безопасности. Кроме того, такую модель можно использовать для стимулирования внедрения аутсорсинговых услуг безопасности с использованием технологий, внедряющих средства обеспечения безопасности в инфраструктуру сети и решения системного уровня для реализации интегрированной объединенной и адаптивной системы обеспечения безопасности.

Введение

Основная проблема, с которой сталкиваются сегодня провайдеры услуг, - это поддержание предсказуемости предоставления сервисов в условиях лавинного трафика злоумышленников, источниками которого служат различные оконечные точки, разбросанные по различным границам сети. В современной терминологии этот тип поведения ассоциируется, в частности, с такими угрозами, как распределенные атаки типа «отказ в обслуживании» (DDoS), современные Интернет-черви, почтовый спам, фишинг и вирусы. То количество трафика, которое генерируется вследствие инфицирования, и последующие всплески трафика могут нарушить нормальную работу сети и создают дополнительный риск для сетевых устройств, которые ответственны за выполнение базовых функций маршрутизации и коммутации пакетов.

В настоящее время безопасность становится критической характеристикой всех сервисов и играет исключительно важную роль в прибыльности работы провайдеров услуг. Сегодня для поддержания более высокого уровня сетевой безопасности провайдерам услуг необходимо перейти от традиционного реактивного подхода к поэтапному проактивному подходу, уменьшая количество существующих уязвимостей, улучшая показатели времени реакции и эффективно подавляя атаки. Вместе с тем существует определенный кадровый дефицит квалифицированных специалистов в сфере информационной безопасности и дефицит систем обеспечения безопасности, использующих механизмы корреляции, для формирования комплексного представления состояния сети в целом.

Время совершенствовать операции по обеспечению безопасности уже настало. Наиболее передовые средства и решения по обеспечению безопасности будут переживать эволюционное развитие по мере перестройки IP-сетей провайдеров. Эффективное обеспечение безопасности сетей – сложная и многогранная задача. Для решения этой задачи в рамках архитектуры IP NGN компания Cisco Systems® разработала формализованное описание и подходы, заложенные в методологию, стандарты, технологии, продукты и технические решения.

Задача

Объемы трафика злоумышленников постоянно растут, поскольку существуют легкодоступные и все более совершенные инструменты атак, а мотивы проведения атак становятся все более разнообразными. Мы стали свидетелями перестройки в криминальной экономике – в сообществе, которое совершает преступления в сфере информационной безопасности ради получения финансовой выгоды. Эта перестройка и ее финансовые отголоски требуют от провайдеров услуг четко определенных и экономически эффективных предложений по защите сетей и сервисов. Провайдерам услуг необходимо воздействовать на основные сервисы, существующие на рынке, смещая их в направлении услуг с учетом требований безопасности, а также предоставлять клиентам новые, более эффективные гарантии сервисов с учетом их стоимости.

На заре киберпреступности квалифицированные системные администраторы нередко разрабатывали и выпускали инструменты выявления и проверки существования уязвимостей. Этими инструментами пользовались и сами администраторы, стремившиеся устранить конкретные уязвимости, и злоумышленники, которые приспосабливали эти инструменты для проведения своих атак. Но, как правило, эти инструменты рассматривались как положительный вклад в обеспечение безопасности. Однако позднее многие злоумышленники стали пользоваться таким инструментами для автоматизации проведения стандартных атак. За последние несколько лет эти методы усовершенствовались, в них появились интеллектуальные алгоритмы, служащие для создания действительно комплексных смешанных угроз, которые распространяются автоматизированным путем с высокой степенью резервирования. Эта эволюция показана на рисунке 1. Сегодня задача злоумышленника становится проще, а задача специалиста по защите сетей, напротив, усложняется.

Рисунок 1. Сетевые атаки становятся все более изощренными и легко организуемыми

Если раньше атаки в первую очередь проводили злоумышленники, которые хотели временно вывести из строя хорошо известные сайты, чтобы привлечь внимание СМИ, на сегодняшний день атаки все больше используются как фундамент для реализации сложных схем шантажа или приобретают политическую или экономическую подоплеку. Ежегодно это приносит предприятиям и провайдерам услуг многомиллионные убытки.

Эволюция систем обеспечения безопасности провайдеров услуг

Сегодня клиенты хотят, чтобы провайдеры внедряли средства обеспечения безопасности, позволяющие эффективно бороться со злоумышленным трафиком и Интернет-червями. Клиенты нуждаются в полномасштабной защите, функционирующей в автоматическом режиме. Решения, для реализации которых требуется развернуть большое количество выделенного оборудования, устанавливаемого на площадях клиента (CPE), и существенно переработать топологии сетей, нереализуемы на практике из-за высокой стоимости, увеличивающихся затрат на обслуживание, росту использования средств шифрования для маскировки атак, дополнительной сложности системы и растущих рисков, а также проблем масштабируемости. Клиенты хотят, чтобы провайдеры несли ответственность за функционирование оконечных устройств, но на сегодняшний день провайдеры услуг не обладают адекватными инструментами для наглядного представления состояния оконечных устройств и управления ими. Кроме того, провайдеры услуг не располагают надлежащей инфраструктурой для распространения, сопровождения и отладки программного обеспечения для оконечных устройств.

Сегодня безопасность уже не ограничивается установкой отдельного устройства или предоставлением отдельной услуги. Безопасность – это краеугольный камень сетей будущего. Мы перешли от концепции сети Интернет, построенной на подразумеваемом доверии, к концепции сети Интернет, основанной на всеобщем недоверии, в рамках которой политики безопасности носят обязательный характер, и ни один пакет, сервис и устройство не могут считаться надежными, до тех пор пока они не пройдут проверку. Поэтому обеспечение безопасности перестает быть специализированным направлением работы или выделенной функцией. Средства защиты должны распределиться по всей рабочей среде провайдера и процессам ее эксплуатации, и их необходимо воспринимать как критически

важные элементы, за счет которых поддерживаются:

- доступность и надежность сервисов,
- непрерывность деловой активности,
- соблюдение условий договоров об уровне обслуживания (SLA),
- доверие и лояльность клиентов.

Для интеграции средств обеспечения безопасности требуется фундаментальная модель процессов функционирования и надежная инфраструктура, составляющая фундамент обеспечения непрерывной деловой активности и предоставления сервисов. Требуется, чтобы все элементы сетевой структуры обладали информацией о значимых аспектах функционирования сети в целом. Требуется, чтобы сама сетевая структура стала повсеместно распространенной проактивной средой мониторинга и реализации политики безопасности. Это подразумевает тесное сотрудничество, как по вопросам ведения деловой активности, так и вопросам используемых технологий, между провайдерами услугами и их клиентами-предприятиями и создает возможности для внедрения сервисов обеспечения безопасности, управляемых провайдерами услуг.

Решение

Архитектуры комплексного обеспечения безопасности

Специалисты компании Cisco рассматривают безопасность как основной опорный элемент архитектуры IP NGN и одно из наиболее важных требований для надежного предоставления сервисов и обеспечения непрерывности деловой активности. Комплексная методология обеспечения безопасности Cisco служит эффективным руководством по разработке архитектуры системы обеспечения безопасности, помогая создать план определения характеристик, сопровождения и внедрения процессов обеспечения безопасности во всей сети. Созданную таким образом архитектуру можно затем применить в рамках программы действия провайдера услуг по обеспечению безопасности путем использования политик, процедур и технологий. Компания Cisco выработала соответствующие сегодняшним реалиям определения угроз в IP-сетях и предлагает проверенную на практике модель для создания услуг провайдеров, приносящих прибыль. По определению компании Cisco на сегодняшний день существуют следующие типы угроз:

- **Информационная разведка.** Злоумышленники сканируют сеть для обнаружения уязвимых устройств (например, это могут быть открытые порты, отсутствие парольной защиты, уязвимости ОС) и атакуют обнаруженные жертвы.
- **Распределенные атаки типа «отказ в обслуживании» (DDoS) и атаки на инфраструктуру.** Это атаки с использованием большого количества IP-пакетов, передаваемых в сеть. Целями атаки являются снижение быстродействия и надежности работы сети.
- **Взлом и захват сетевых устройств.** Как правило, такие действия следуют за этапом информационной разведки и представляют собой несанкционированный доступ к тому или иному устройству с намерением нарушить его безопасность.
- **Кража сервисов и мошенничество.** Угрозы данного типа заключаются в несанкционированном использовании сетевых ресурсов.

После идентификации угрозы необходимо приступать к ее нейтрализации. Для эффективной борьбы с угрозами необходимо понимание трех базовых принципов, а именно:

- **Предотвращение.** Реализация известных защитных мер для предотвращения известных угроз. Средства предотвращения включают установку “заплат” в уязвимые системы, внедрение стандартных и усиленных образов системного программного обеспечения, использование межсетевых экранов или иных технологий разграничения доступа.
- **Мониторинг.** Выявление потенциально опасных действий и действий, связанных с использованием известных уязвимостей; разграничение реальных действий злоумышленника и неадекватных действий пользователей с целью выделения реальных угроз, которые обнаруживаются в ключевых точках агрегации. Для выявления таких действия используются методы развертывания средств мониторинга вторжений, проведение анализа журналов серверов и межсетевых экранов, а также активный мониторинг вызовов операционной системы.
- **Ответные меры.** Способность действовать на основании полученной информации с целью ограничить последствия подтвержденной реальной угрозы в режиме, приближенном к режиму реального времени. В числе применяемых методов – динамическое разграничение доступа, сброс пакетов, изменение конфигурации сетевого устройства, прерывание сеансов работы и блокирование некорректных системных вызовов.

Важно осознавать, что эти принципы должны реализовываться на всех уровнях функционирования сети, приложений и инфраструктуры в целом.

Когда скорость передачи трафика достигает уровня нескольких гигабит, для подавления возникающих угроз к провайдерам предъявляются иные требования: происходит переход от автономных устройств обеспечения безопасности к интеграции средств обеспечения безопасности в инфраструктуру сети. Интегрированная безопасность обеспечивает:

- защиту, которая не затрагивает быстродействие сети в целом,
- использование существующих сервисов, которые обладают высокой степенью доступности,
- способность идентифицировать, классифицировать и отслеживать аномальное поведение в сети,
- возможность улучшать общее состояние безопасности сети,
- способность распространять контрмеры на большое количество узлов сети.

Компания Cisco помогает провайдерам в создании таких программ обеспечения безопасности, которые распространяются на различные точки агрегирования трафика и охватывают как все известные угрозы, так и угрозы, появление которых вероятно в ближайшем будущем.

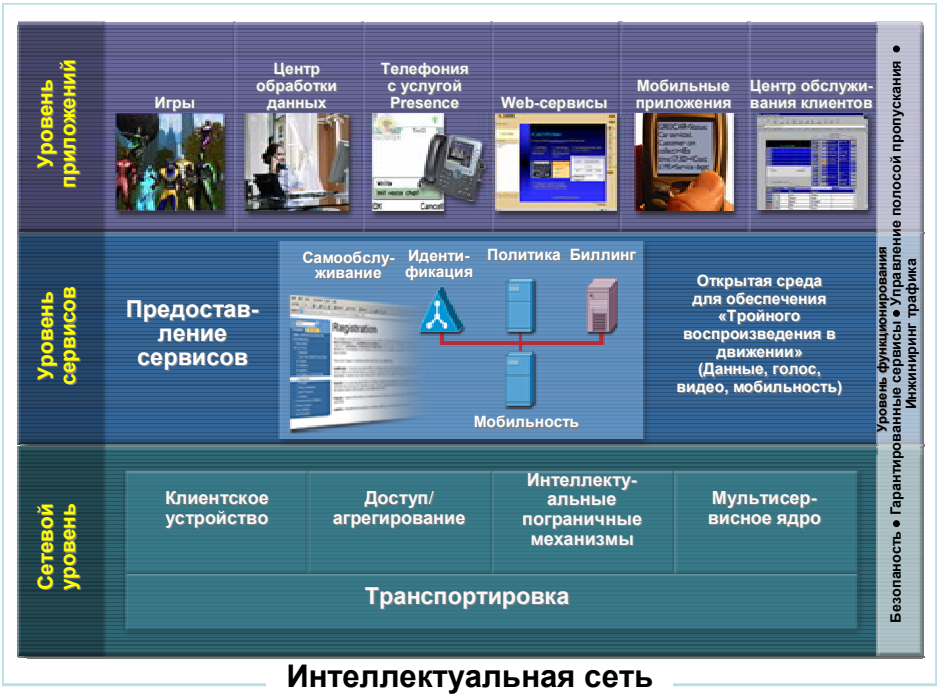
Ресурсы обеспечения безопасности Cisco IP NGN

Cisco IP NGN – это концепция и архитектура, предназначенные для проведения широкой полномасштабной перестройки сетей провайдеров услуг и предприятий. Это решение предоставляет существенные конкурентные преимущества и прибыли, помогая провайдерам услуг развивать и планировать на будущее свою организационную структуру, архитектуру сети и соответствующие бизнес-модели.

В архитектуре IP NGN безопасность – основной фактор способности провайдера услуг защитить инфраструктуру сети, предоставить сервисы в соответствии с требованиями конкретных уровней обслуживания и контролировать свою работу. Средства обеспечения

безопасности постоянно присутствуют на всех четырех уровнях архитектуры IP NGN (см. рис. 2). Решения в области обеспечения безопасности Cisco IP NGN помогают создать такую рабочую среду, в которой провайдеры могут предложить дополнительные услуги с целью привлечения дополнительных доходов и дифференциации, повышения показателей эффективности благодаря сервисам с высокой степенью доступности и минимальными показателями времени простоя, а так же более эффективно управлять успешным функционированием сети и предприятием в целом.

Рисунок 2. Архитектура Cisco IP NGN



Средства обеспечения безопасности распространены по всей архитектуре IP NGN, обеспечивая защиту сервисов в масштабах всей сети для поддержания доступности сервисов в случае атаки. На сетевом уровне средства обеспечения безопасности заложены в фундамент инфраструктуры, ее аппаратуру и операционные системы для обеспечения безопасной передачи данных сервисов на транспортном уровне. На уровне сервисов – это часть инфраструктуры обмена сервисами Cisco Service Exchange Framework – средства обеспечения безопасности вовлечены в создание сервисов и сервисных функций с целью привлечения доходов и дифференциации сервисов. На уровне приложений средства обеспечения безопасности постоянно присутствуют в самих приложениях и в ссылках на уровень сервисов для обеспечения целостности приложений при их взаимодействии с сетью.

Интеллектуальный уровень функционирования работает при посредстве трех уровней конвергенции IP NGN – сеть, сервис и приложение - и помогает устанавливать соединения между ними, обеспечивая максимальную эффективность и производительность работы в интранет-сетях и в сети Интернет. Механизмы интеллектуальной сетевой интеграции упрощают функционирование IP NGN, повышая надежность, интегрированность и адаптивность системы. Совместная работа трех уровней конвергенции, связующего уровня функционирования и средств интеллектуальной сетевой интеграции позволяют компании Cisco создавать интегрированные функции, гармонизированные в различных линейках

продукции и обеспечивающие функционирование продуктов как глобальной системы – IP-сети нового поколения. Безопасность является фундаментальной составляющей IP NGN, она реализуется за счет объединения *процессов*, *технологий* и *решений*.

Модель процессов функционирования Cisco для рассмотрения вопросов обеспечения безопасности провайдеров услуг

Модель процессов функционирования Cisco для рассмотрения вопросов обеспечения безопасности провайдеров услуг определяет, каким образом провайдер может результативно предложить больший объем сервисов при более высокой эффективности с большей степенью управляемости. Эта модель может применяться как для коммерческих, так и для технологических подразделений в организационной структуре провайдера; основной акцент сделан на обеспечении доступности и надежности сервисов, а также на создании новых возможностей для получения доходов.

Важнейшие элементы этой модели доступны уже сегодня, они позволяют предотвращать сбой в работе сервисов и нейтрализовывать атаки, нацеленные на инфраструктуру провайдера. Для реализации и масштабирования модели функционирования требуется комплексная интеграция различных систем безопасности в структуру сети провайдера. Компания Cisco прилагает существенные усилия для интеграции и адаптации всей модели в целом, а не только применительно к сфере безопасности, вопросам функционирования устройств или внедрения подсистемы, нацеленной на борьбу с проблемами одного конкретного типа.

Модель процессов функционирования Cisco для обеспечения безопасности провайдеров услуг разработана специально для провайдеров услуг. Такой проактивный подход к нейтрализации угроз выходит за рамки одного устройства или технологии, учитывает возможный недостаток профессиональных навыков в области обеспечения безопасности функционирования, помогает свести к минимуму количество угроз, которые невозможно полностью проконтролировать, и установить контроль над теми, которые поддаются контролю. Этот подход также направлен на снижение эксплуатационных расходов как для провайдера услуг, так и для корпоративного клиента.

В соответствии с принятой стратегией функционирования для обеспечения непрерывности предоставления сервисов и ведения деловой активности в рабочей среде, в которой постоянно присутствуют угрозы нарушения безопасности, используются собранные данные телеметрии, которые позволяют обеспечить полный контроль состояния сети и полное управление сетью и элементами системы. Модель применяется для внедрения средств безопасности в масштабах всей сети без упора на какую-либо одну технологию. При этом в сети применяются различные технологии и функции для получения наглядной картины поведения сети и установления контроля над нестандартными ситуациями в сети.

Модель служит для реализации средств контроля состояния IP-инфраструктуры и управления ей (см. рис. 3). Архитектура IP NGN используется в рамках надежной модели функционирования, поддерживая работоспособность сети операции и операции обеспечения безопасности. Все основные элементы этой модели действуют как единое целое, формируя надежную систему защиты.

Рисунок 3. Модель процессов функционирования Cisco для обеспечения безопасности провайдеров услуг

Понятие безопасности в IP NGN подразумевает полная контроль состояния и полное управление, в основе которых лежат следующие элементы:

- **Идентификация и доверие.** Идентификация устройств, получающих доступ в сеть, и контроль данных,используемых для аутентификации, требуются для того, чтобы определить степень доверия.
- **Телеметрия.** Мониторинг эффективности функционирования политики безопасности.
- **Механизмы корреляционного анализа и интеллектуальные механизмы.** Интерпретация и преобразование больших объемов данных в значимую информацию, пригодную для анализа. Сюда относятся контекстуализация несвязанных на первый взгляд изменений в состоянии безопасности, методы выявления нарушений политики безопасности или обнаружение комбинации изменений состояния безопасности, которая может помешать гарантированному предоставлению сервисов.
- **Инструментарий.** Введение механизмов интеллектуальной логики, анализирующих журналы аудита, результаты мониторинга событий, сведения о неполадках, функциональном состоянии элементов системы и корректности их функционирования, а также соответствующее графическое представление в режиме, приближенном к режиму реального времени.
- **Виртуализация.** Определение и реализация политик для логических устройств и требуемого состояния безопасности.
- **Обеспечение выполнения политик.** Обеспечение выполнения политик по результатам контроля состояние системы; присутствие в политиках описания действий, которые необходимы при контекстуализации результатов наблюдений.

В числе основных преимуществ, предоставляемых моделью процессов функционирования Cisco для обеспечения безопасности провайдеров услуг, – интеграция собранной телеметрической информации, интеллектуальные объединенные системы управления, обеспечение рентабельности затрат за счет виртуализации, а также проактивная и адаптивная структура, готовая к нейтрализации угроз. Такой подход ускоряет развертывание сервисов и обеспечивают надлежащую степень масштабирования.

Технологии безопасности, интегрированные в продуктах

В маршрутизаторах и коммутаторах Cisco предусмотрены встроенные средства обеспечения безопасности, позволяющие защитить и обеспечить надежное функционирование сети провайдера услуг на сетевом уровне. Эти средства – Cisco NetFlow и система обеспечения

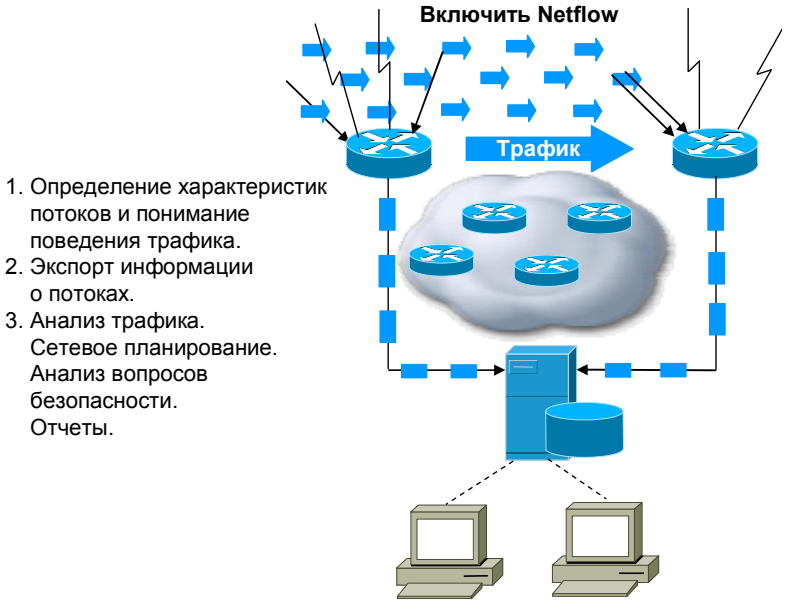
безопасности сети Cisco Network Foundation Protection – работают совместно с целью нейтрализации самых распространенных угроз, отражения распространенных атак и обеспечения основных функций безопасности.

Cisco NetFlow

Технология Cisco NetFlow, заложенная в программном обеспечении Cisco IOS®, эффективно предоставляет ряд сервисов для IP-приложений, в том числе учет сетевого трафика, сетевой биллинг, основанный на показателях использования, планирование сети, обеспечение безопасности, средства мониторинга DoS, средства общего мониторинга сети и трафика (см. рис. 4).

Средства NetFlow предоставляют ценную телеметрическую информацию о пользователях сети и сетевых приложениях, о пиковых периодах загрузки и о маршрутизации трафика. Компания Cisco создала NetFlow и является лидером в технологиях обработки потоков IP-трафика, введя NetFlow как стандартное средство получения данных о состоянии IP-сетей и их функционировании.

Рисунок 4. Принципы работы Cisco NetFlow



Cisco NetFlow помогает сетевым администраторам выявлять и классифицировать инциденты в сфере информационной безопасности, а также понимать, какое влияние оказывают на работу сети изменения в структуре сети и введение сервисов, обеспечивать более эффективное использование сети и повышать быстродействие приложений. Кроме того, с помощью Cisco NetFlow провайдеры услуг могут снизить стоимость пользования IP-сервисами и приложениями и провести дополнительную оптимизацию затрат на сеть.

Система Cisco Network Foundation Protection

Система Cisco Network Foundation Protection (NFP) входящая в состав программного обеспечения Cisco IOS, обеспечивает защиту сетевых устройств, механизмов маршрутизации и передачи управляющей информации, а также управление трафиком, поступающим на сетевые устройства (см. рис. 5). Система Cisco NFP заложена в основные механизмы маршрутизаторов и коммутаторов Cisco.

Рисунок 5. Система Cisco Network Foundation Protection

Аббревиатуры:
ACL – список управления доступом.
RTBH – сброс в “черные дыры” с удаленной инициацией.
uRPF – однонаправленная проверка передачи по обратному пути.
PE – граница зоны провайдера.

Cisco NFP обеспечивает защиту уровней данных, контроля и управления сетевой инфраструктуры от широкого спектра угроз безопасности. Эта система помогает обезопасить сетевые устройства не только от DDoS-атак, но и от таких типов атак, как информационная разведка, взлом и захват сетевых устройств и кража сервисов. Система помогает свести к минимуму количество уязвимостей критически важных сервисов, в том числе, системы DNS, системы обработки электронной почты, средства web-доступа и механизмов IP-телефонии (VoIP). Используя средства сбора телеметрической информации, в частности, данные NetFlow, система NFP анализирует шаблоны трафика в режиме реального времени, устанавливает базовые характеристики трафика, выявляет аномалии и злоупотребления и указывает интерфейсы, затронутые атакой. Предусмотрена возможность сопоставления аномалий в пределах сети для обратного отслеживания и определения точки проникновения. Дополняя решение Cisco по обеспечению защиты от DDoS-атак, система NFP также отражает примитивные DDoS-атаки, высвобождая ресурсы механизма Cisco Guard – одного из важнейших элементов решения Cisco по защите от DDoS-атак – для борьбы с более изощренными атаками.

Решения по обеспечению безопасности на системной основе

В семейство решения для обеспечения безопасности Cisco входят заложенные в систему

решения по обеспечению безопасности, которые уже успешно внедрены ведущими провайдерами услуг и принесли им дополнительные доходы. Описанные ниже решения открывают перед провайдерами услуг широкие возможности по созданию аутсорсинговых услуг в сфере информационной безопасности, которые могут быть предложены клиентам.

Защита от DDoS-атак и защита входящего трафика

Решения Cisco по защите от DDoS-атак предоставляют провайдерам услуг возможность обеспечить безопасность каналов передачи информации. В этих решениях используются заложенные в программное обеспечение Cisco IOS ресурсы NetFlow и NFP, которые реализуют комплексные функции обеспечения безопасности на коммутаторах и маршрутизаторах Cisco. Тем самым, на коммутаторах и маршрутизаторах обеспечиваются фиксация сервисов и протоколов маршрутизации, защищенный доступ к средствам управления, а также защита данных, пересылаемых через устройства. Кроме того, в решении используются средства Cisco для защиты от DDoS-атак и продукты сторонних производителей, которые обеспечивают выявление, подавление, перенаправление и обратную вставку трафика для защиты сеть от все более усложняющихся DDoS-атак. Решения Cisco по защите от DDoS-атак помогают провайдерам услуг обеспечить продажу клиентам услуг подключения и заданной полосы пропускания «последней мили» при одновременном повышении надежности собственной сетевой инфраструктуры поставщика услуг.

Управление сервисами и защита исходящего трафика

Набор решений Cisco для управления сервисами обеспечивает защиту трафика, исходящего от клиентов провайдера услуг, и предоставляет возможность изоляции определенных пользователей в карантин. Сетевой карантин – прием, используемый для выявления и сдерживания распространения потенциальных угроз в пределах домена провайдера услуг путем выделения всего трафика, поступающего от инфицированных хостов, и его отправки в изолированную сеть, которая специально предназначена для того, чтобы дать конечному пользователю возможность самостоятельно выявить и устранить угрозы. Сетевой карантин не является мерой обеспечения безопасности, которая позволяла бы изолировать злоумышленников. Это отказоустойчивый инструмент, обеспечивающий соблюдение политик провайдера услуг законопослушными пользователями, и обеспечивающий отсутствие угроз другим пользователям или сетевым ресурсам со стороны конечного пользователя. Основная задача механизмов управления сервисами – значительно сократить затраты на поддержку клиентов и службу сопровождения, предоставив клиентам возможность подавлять атаки самостоятельно. Этого можно добиться с помощью своевременного обновления программного обеспечения или применения выделенного программного обеспечения для удаления с хоста вирусов, червей и другого вредоносного кода.

Виртуальные частные сети

Решения Cisco в сфере IP VPN предоставляют провайдерам услуг возможность предлагать корпорациям, а также малым и средним предприятиям (SMB) надежный, универсальный и полностью интегрированный сервис IP VPN. Это экономичное масштабируемое решение в сфере VPN, которое использует все преимущества имеющейся у провайдера сети MPLS для введения новых вариантов услуг, приносящих прибыль, в том числе, механизмы приоритетов класса обслуживания (CoS) для конкретных приложений и пользователей и договоры об уровне обслуживания (SLA). Для добавления новых клиентов сети VPN не требуется установка дополнительных интерфейсов и реконфигурация маршрутизаторов на

границах клиентской зоны. Основная возможность извлечения доходов для провайдеров состоит в том, чтобы предлагать управляемый доступ к таким сетям VPN. Например, услуга управляемого удаленного доступа к сети VPN для клиентов, работающих в сети Интернет, с использованием протокола IPSec или SSL, или услуга управляемого надежного доступа к сети Интернет из сети VPN с дополнительной защитой с помощью межсетевого экрана.

Управление оборудованием, установленным на площадях клиента, и обеспечение безопасности на границе сети клиента

Комплект решений в сфере обеспечения безопасности управляемого оборудования, устанавливаемого на площадях клиента/клиентского оборудования Cisco (CPE/CE) – это набор лучших из известных методик работы на рынке и управления сервисами в формате решения, готового к представлению рынке. Этот комплект помогает провайдерам услуг создавать, разрабатывать и внедрять сервисы удаленного управления, используя технологии Cisco, на площадках своих клиентов. Набор методик служит инструкцией по разработке поддерживающей инфраструктуры и планированию в создании функциональной, ориентированной на реальный рынок, стратегии для внедрения управляемых элементов CPE с применением технологий Cisco. В числе аспектов удаленного управления, рассмотренных в методиках, – системное управление, приемы выявления, обнаружение, изоляция и разрешение инцидентов в сфере информационной безопасности; приемы управления конфигурированием и изменениями конфигурации; концепции формирования отчетов об инцидентах в сфере информационной безопасности, анализе таких инцидентов и нейтрализации угроз. Все приемы и концепции удаленного управления разработаны для оптимизации доступности и надежности функционирования сервисов, предлагаемых конечным пользователям, и обеспечения устойчивости к сбоям, даже в условиях технологических неполадок или атак злоумышленников.

Управление пограничными устройствами

В архитектурах систем обмена трафиком между провайдерами нового поколения особое внимание уделено внедрению новых уровней обеспечения безопасности для беспрепятственного предоставления голосовых, видео- и мультимедийных сервисов. Функции управления пограничными устройствами предназначены для обеспечения безопасности, гарантии предоставления сервисов и соблюдения требований нормативных документов, например, требований по легальному протоколированию взаимодействий на границах IP-сетей, содержащихся в законодательных требованиях многих стран. Функции пограничных устройств подчиняются многоуровневой модели обмена трафиком между провайдерами услуг, которая обеспечивает разделение функций устройств с целью улучшения контроля и получения новых доходов за счет соединений между провайдерами. В числе этих функций – функции поддержки QoS на уровне обмена между провайдерами, функции обеспечения безопасности на границе между провайдерами, а также функции контроля над соблюдением условий договоров SLA между провайдерами.

Заключение

Интегрированная объединенная адаптивная система обеспечения безопасности в эволюционно развивающейся архитектуре Cisco IP NGN встраивается в сетевую инфраструктуру провайдера услуг и интегрируется с остальными элементами сети. Интеграция означает, что в каждом элементе сети реализованы технологии обеспечения безопасности, и он является одним из рубежей обороны. Объединение ресурсов безопасности означает, что элементы сети совместно обеспечивают новые виды защиты, в том числе, безопасное взаимодействие между оконечными устройствами, элементами сети и

реализацию политики безопасности. Адаптивность системы заключается во введении методы анализа поведения системы, которые позволяют распознавать новые виды угроз по мере их появления. Благодаря этому, расширяются возможности выявления угроз и борьба с ними ведется на разных уровнях сети.

Cisco Systems не только предлагает широкий спектр продуктов в области обеспечения безопасности, но и оказывает провайдерам услуг содействие в разработке управляемых сервисов безопасности, приносящих дополнительный доход: от концепции до внедрения и проведения маркетинга. С точки зрения специалистов компании Cisco безопасность представляет собой не побочный аспект, а краеугольный камень работы провайдера услуг, который распространяется на все сервисы. Компания Cisco разработала модульный подход к созданию управляемых сервисов обеспечения безопасности для корпораций, а также для малых и средных предприятий. Такой подход предоставляет провайдерам услуг возможность быстро и легко формировать персонифицированные наборы сервисов в соответствии с потребностями различных категорий клиентов и требованиями вертикалей рынка. Широкий спектр функций и модульный характер платформ Cisco обеспечивают реальную универсальность управляемых сервисов безопасности, которые могут приносить провайдерам немалые доходы и гарантировать надежную защиту конечных клиентов.

Концепция IP NGN подразумевает формирование интеллектуальной инфраструктуры, на базе которой сети, в которых реализованы динамические функции работы с сервисами, обеспечивают надежную доставку сервисов, в которых реализованы динамические функции работы с приложениями. Эти интеллектуальные механизмы обеспечивают непосредственную поддержку усилий по проактивной защите сетей от существующих и постоянно меняющихся угроз и, одновременно с этим, предоставляют провайдерам услуг ощутимые конкурентные преимущества.

Дополнительная информация

Система Cisco Network Foundation Protection: http://www.cisco.com/go/nfp

Cisco NetFlow: http://www.cisco.com/go/netflow

Решения Cisco в сфере VPN:
http://www.cisco.com/en/US/netsol/ns587/networking_solutions_sub_solution.html

Решение Cisco по защите от DDoS-атак: http://www.cisco.com/go/cleanpipes

