ОСНОВНЫЕ ЭЛЕМЕНТЫ СТРАТЕГИИ САМОЗАЩИЩАЮЩЕЙСЯ СЕТИ CISCO

Отчасти благодаря деятельности Cisco®, представляющей стратегию самозащищающейся сети Cisco (Self-Defending Network), многие начинают осознавать необходимость интегрированных средств сетевой защиты.

Но неужели сеть может защищать сама себя?

Кратким ответом на этот вопрос будет: «Да, может». Механизмы обеспечения сетевой безопасности эволюционировали от независимо используемых «точечных» продуктов, таких как межсетевые экраны или средства обнаружения вторжений, в область интегрированных и целостных решений. Cisco Systems® является ведущей компанией по разработке технологии, позволяющей сделать самозащищающиеся сети реальностью.

Идея решения достаточно проста: в настоящее время поддержание целостности, конфиденциальности и доступности корпоративной информации является ключом к успеху любой компании. Значение информации и надежных механизмов контроля доступа к ней еще никогда не было так велико. Таким образом, назначение IT-инфраструктуры заключается в создании систем, предоставляющих возможность обнаружения нарушений безопасности и защиты от несанкционированного доступа с одновременным предоставлением оперативного доступа легальным пользователям. Простой отказ в доступе уже не является подходящей реакцией на атаку. Современные сети должны реагировать на атаки, сохраняя свою доступность, надежность и работоспособность. Во многих отношениях, целью обеспечения безопасности становится повышение степени отказоустойчивости сетей. Вместо того, чтобы становиться жертвами, сети должны стать способными «поглощать» атаки и сохранять работоспособность, подобно иммунной системе человека, позволяющей организму функционировать при наличии в нем вирусов и бактериальных инфекций.

В данном документе описывается целесообразность использования стратегии самозащищающейся сети Cisco (Cisco Self-Defending Network, SDN), ее основы и предлагаемые Cisco Systems поэтапные действия, позволяющие обеспечить такие возможности.

РАЗВИТИЕ СИТУАЦИИ В СФЕРЕ БЕЗОПАСНОСТИ

За последние три года технологии обеспечения безопасности изменились больше, чем за все предшествующее десятилетие. Объем и темп этих изменений усложнили возложенную на IT-специалистов задачу поддержания должного уровня защищенности. Перед тем, как продолжить рассказ о Cisco SDN, необходимо получить представление о сути этих изменений.

Защита периметра сети. Пожалуй, наиболее существенным фактором, повлиявшим на изменение подхода к обеспечению безопасности сетей, стало изменение самой сущности сети. Уже не представляется возможным обеспечить безопасность сети только за счет организации защиты ее периметра; после того, как корпорации стали консолидировать

центры обработки данных, использовать конвергированные внутренние сети и активно использовать сеть Интернет, среда, которая ранее считалась изолированной и контролируемой, теперь является открытой для партнеров за счет сетей "экстранет", подключений пунктов розничной продажи, надомных работников и пр. Расширение корпоративной сети, таким образом, приводит к необходимости взаимодействия через ненадежные промежуточные сети и неконтролируемые среды. Устройства, подключающиеся к корпоративной сети через эти промежуточные сети, зачастую не соответствуют требованиям корпоративных политик безопасности. А устройства, соответствующие требованиям корпоративных политик, часто используются для доступа к другим неконтролируемым сетям до соединения с корпоративной сетью. В результате, устройства, подключенные к внешним сетям, могут стать «перевалочным пунктом» для атак и связанных с ними несанкционированных действий.

Беспроводные сети и сети мобильной связи. Привязанные к понятию периметра защиты беспроводные сети и сети мобильной связи предприятий теперь обеспечивают поддержку ноутбуков, карманных компьютеров (PDA) и мобильных телефонов, которые подключены к нескольким сетям. Эти устройства с несколькими сетевыми интерфейсами поддерживают возможность установления одноранговых беспроводных соединений для работы в сети "точка-точка". Кроме того, пакеты могут эффективно передаваться между устройствами на прикладном уровне. В результате понятие границ сети становится все более размытым. Для управления системой обеспечения безопасности и поддержания доступности сети корпорациям необходимо иметь возможность управления такими мобильными устройствами.

Электронная коммерция, сети "экстранет" и проведение деловых операций в глобальной сети. Появление общих прикладных интерфейсов на основе протоколов передачи сообщений, таких как XML и SOAP, оказало благотворное влияние на электронную коммерцию и производительность работы предприятий. Но, как и в большинстве случаев появления новых технологий, появление новых протоколов передачи сообщений привело к возникновению совершенно новых уязвимостей и источников атак, с которыми приходится бороться. Данные, которые раньше передавались с помощью множества сетевых протоколов и проходили фильтрацию на межсетевых экранах, теперь передаются с помощью нескольких или всего одного транспортного протокола (например, HTTP с использованием порта 80 TCP). В результате, большая часть данных, которая раньше помещалась в заголовках пакетов, теперь располагается в теле пакетов. Это существенно облегчает злоумышленнику задачу обхода классической системы защиты сети (см. рис. 1). Более того, для обеспечения конфиденциальности и целостности корпоративных данных все чаще используется шифрование трафика прикладного уровня с помощью протоколов SSL/TLS и HTTPS. При этом возникает побочный эффект, связанный с усложнением контроля доступа на границе сети из-за невозможности проверки пакетов в зашифрованных потоках данных.

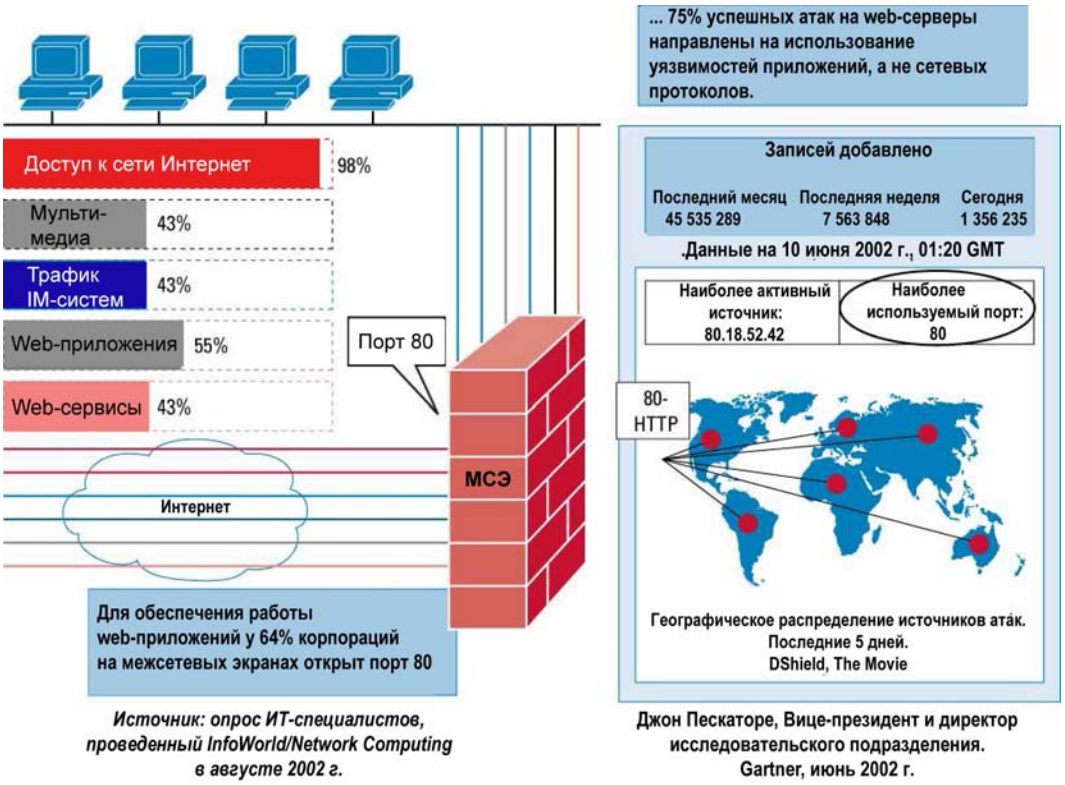

Рисунок 1. Новые уязвимости, связанные с портом 80

Вирусы, Интернет-черви и скорость их распространения. Количество и многообразие появившихся за последние три года вирусов и Интернет-червей само по себе является устрашающим. Чудовищное воздействие этих Интернет-червей и вирусов на сети предприятий и их производительность было обусловлено наличием двух факторов: короткого промежутка времени между обнаружением уязвимости и появлением атаки с ее использованием, а также скорости, с которой большинство атак распространялось по сети. При этом число нарушений работы сетей достигало недопустимого уровня, а для устранения последствий приходилось идти на незапланированные траты человеческих, временных и материальных ресурсов.

Соблюдение установленных норм. Получившие широкую огласку факты нарушений и неправомерные действия внутри корпораций подтолкнули управляющие органы многих отраслей к созданию норм по регулированию рисков в отношении корпоративной информации. В США эти нормы, наиболее известными из которых являются закон Сарбейнса-Оксли, закон Грэмма-Лича-Блили и закон о соблюдении конфиденциальности информации о здравоохранении и личных данных пациентов (HIPAA), привели к коренным изменениям способов организации корпоративных сетей, серверов, баз данных и хостов. Аналогичная тенденция наблюдается и в России.

Хотя многие организации полагают, что соблюдение норм обеспечивает более надежную защиту их инфраструктуры, данное мнение зачастую является ошибочным. Сам процесс следования установленным нормам может привести к возникновению новых уязвимостей. Например, Интернет-черви и вирусы могут более эффективно распространяться в сети, поддерживающей сквозные VPN-соединения, в связи с тем, что проходящие по ним потоки данных являются невидимыми для промежуточных узлов. Такие потоки данных могут

переносить Интернет-червей на критически важные корпоративные серверы посредством надежно зашифрованных пакетов. Кроме того, что на обнаружение такой атаки уходит много времени, сквозные VPN-соединения усложняют процесс устранения ее последствий.

ПРИНЦИПЫ ПОСТРОЕНИЯ СОВРЕМЕННЫХ БЕЗОПАСНЫХ СЕТЕЙ

Корпорации не могут бесконечно следовать изменяющимся направлениям в области безопасности. В идеале, совершенствование системы безопасности должно оказывать минимальное воздействие на существующую инфраструктуру маршрутизации и коммутации, методы разграничения и контроля доступа и смежные организационные структуры, обеспечивающие поддержку этих систем. В данном параграфе описываются основные элементы самозащищающейся сети: *присутствие*, *контекст*, *взаимосвязи* и *доверие*.

Присутствие. Фундаментальным понятием защищенной системы является понятие контрольных точек, которое мы определим как присутствие (см. рис. 2). Подобно иммунной системе человека, полагающейся на клетки, рассредоточенные по всему телу человека и выполняющие функции обнаружения инфекции и выполнения ответных действий, сеть полагается на наличие определенных возможностей у отдельных узлов. К таким возможностям относятся классические методы идентификации, контроля доступа, проверки данных и защиты взаимодействия, а также новые возможности анализа действий приложений, связанные с расширением областей использования клиентов файлообменных сетей, web-сервисов, а также голосовых сервисов и сервисов передачи динамического контента по мобильным сетям.

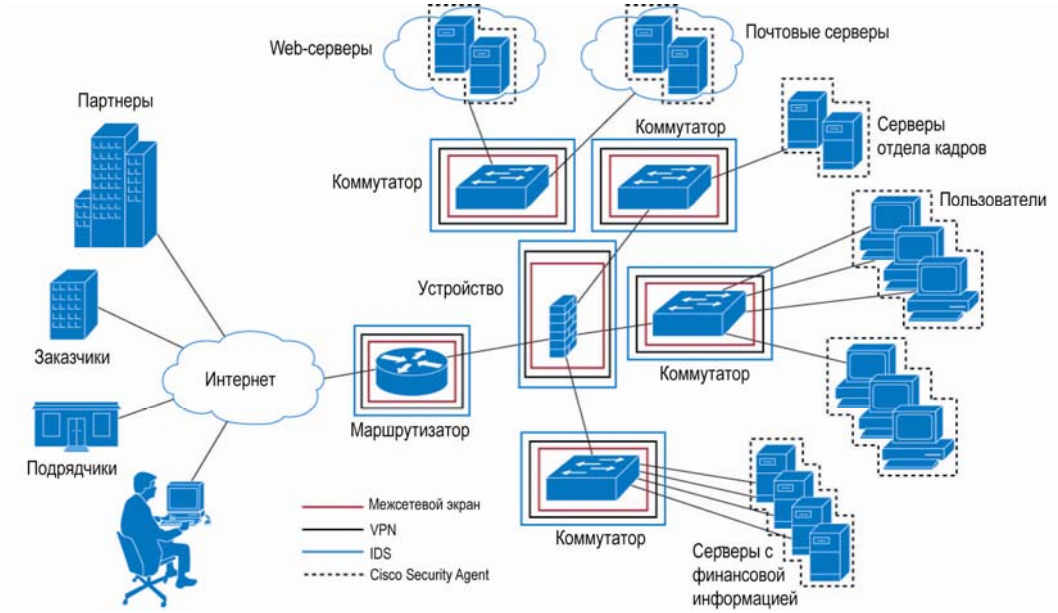

Рисунок 2. Присутствие в самозащищающейся сети

Контекст. При входе пользователя в систему сеть запрашивает и получает доступ к набору реквизитов доступа пользователя и хоста, представляющих собой конечную *сущность*. Полномочия могут изменяться с течением времени в зависимости от действий подключенного к сети хоста. Совокупность этих данных представляют собой *контекст*. В отличие от существующих систем сетевой безопасности, в которых большое внимание уделяется только проверке полномочий пользователя при входе в сеть, самозащищающаяся

сеть принимает решения о предоставлении или отмене полномочий на основе изменений поведения и соответствующего ему контекста за все время соединения сущности с сетью. Например, если сеть обнаруживает, что хост заражен вирусом (при этом пользователь может обладать всеми полномочиями на доступ), она изолирует этот хост в карантинный сегмент сети. Поскольку данные могут быть подменены, в процессе обеспечения безопасности системы может понадобиться получение контекста от других систем для точного и своевременного определения прав хоста и привилегий в конкретный момент времени.

Взаимосвязи. Взаимосвязи между отдельными сущностями позволяют обмениваться контекстом и создавать «систему». Традиционно, взаимосвязи между устройствами сети устанавливались с помощью протоколов маршрутизации, такими как протокол BGP. Для того чтобы противостоять самым современным видам угроз и несанкционированных действий, теперь необходимо расширять эти взаимосвязи по всему маршруту от источника к получателю сетевого трафика. Кроме того, из-за растущего числа мобильных устройств, подключенных к разным линиям, взаимосвязи вышли за пределы границ, которые до недавнего времени рассматривались как внешние границы сетей в традиционном понимании. Привилегии, которые сущность получает при доступе к сети, а также характер их изменения в процессе сеанса работы определяются на основе контекста этой сущности и ее взаимосвязей в сети или сетях.

Доверие. Безопасность системы определяется безопасностью поступающей в нее информации; система функционирует гораздо эффективнее, если в ней присутствуют *доверительные* отношения. Ранее степень доверия определялась главным образом на основе идентификации устройства или пользователя. Результаты последних исследований показали, что в концепцию защищенных систем должны быть включены понятия *состояния* и месторасположения устройства.

По многим параметрам действия, выполняемые пользователями или устройствами в сети, можно сравнить с управлением автомобилем. Подобно тому, как человек получает водительские права, позволяющие ему управлять определенным классом транспортных средств, пользователи должны обладать некоторой идентификационной информацией для того, чтобы выполнить вход в сеть. Кроме того, у каждого автомобиля есть идентификационный номер, который должен быть зарегистрирован в местных органах управления, - сети и конечные узлы в скором времени будут иметь цифровые сертификаты, создаваемые во время выпуска и требующие выполнения определенного типа регистрации при использовании в рамках компании. Но поскольку сущностям не всегда удается вовремя предоставлять идентификационные данные, соответствующие заданному месторасположению или точке, самозащищающаяся сеть использует передовые методы *косвенного доверия* и *максимальных усилий* для аутентификации и авторизации сущностей. Самозащищающаяся сеть должна как минимум уметь запрашивать идентификационные данные каждого устройства и пользователя, выполнять анализ состояния устройства и устанавливать местоположение устройства в сети (см. рис. 3). Технология, позволяющая реализовать эти возможности, будет повсеместно распространена и задействована с помощью четко определенных стандартных форматов сообщений и протоколов, таких как протокол 802.1x и протокол аутентификации EAP.

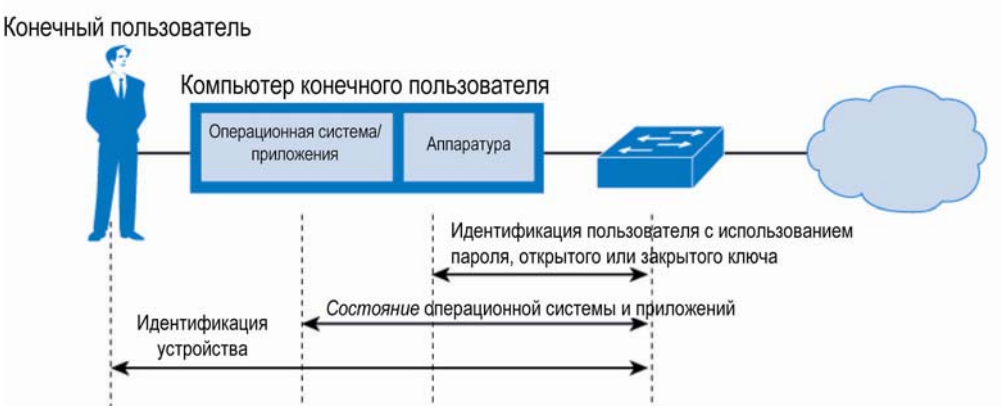

Рисунок 3. Идентификационные данные, как основа сетевой безопасности

Само по себе каждое из этих понятий не особенно примечательно. Но они приобретают силу при объединении в самозащищающейся сети Cisco. В оставшейся части данного документа описываются некоторые способы использования этих понятий в рамках самозащищающейся сети.

НЕОБХОДИМОСТЬ ПОСТРОЕНИЯ САМОЗАЩИЩАЮЩЕЙСЯ СЕТИ

Корпоративные сети, как и атаки на них, в настоящее время достигли такого уровня сложности, что полностью полагаться на один 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, компания Cisco полагает, что существует способ построения лучших адаптивных решений. В результате, специалисты 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 общине. Общей чертой 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:

- непрерывность функционирования,
- ненавязчивость,
- минимизация возможности распространения атак,
- быстрая реакция на еще неизвестные атаки.

Эти системы построены на концепции ограниченности ресурсов и необходимости их бережного использования во избежание их истощения. Также в этих системах используются все преимущества существующей инфраструктуры с минимальным воздействием на IT-операции потребителей.

Самозащищающаяся сеть Cisco предоставляет решения на основе систем, предоставляющие потребителям новые возможности использования существующей инфраструктуры для сокращения количества источников уязвимостей, минимизации ущерба от атак и повышения доступности и надежности инфраструктуры в целом. Самозащищающаяся сеть также позволяет создавать автономные системы, способные быстро реагировать на вторжения, практически не требуя вмешательства оператора в этот процесс. Такая быстрая ответная реакция необходима для пресечения самых последних видов несанкционированных действий, которые гораздо опаснее своих предшественников.

Самозащищающаяся сеть Cisco продолжает совершенствовать механизм реакции на новые угрозы. На первом этапе (**интегрированная защита)** выполняется включение механизмов обеспечения безопасности в состав сетевых устройств, таких как коммутаторы и маршрутизаторы. Второй этап (**коллективная защита**) включает построение связей между элементами сетевой защиты и распространение присутствия сети на оконечные устройства, подключенные 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 Anti-X.

СТРУКТУРНЫЕ ЭЛЕМЕНТЫ САМОЗАЩИЩАЮЩЕЙСЯ СЕТИ CISCO

Поскольку одновременная перестройка всех подсистем без нарушения целостности IT-сервисов может оказаться сложной задачей, большинство потребителей не сможет внедрить все компоненты стратегии Cisco SDN одновременно. Некоторые потребители могут медлить с передачей функций контроля безопасности автоматизированной системе до тех пор, пока они не убедятся в том, что эта система будет работать надежно. Стратегия самозащищающейся сети Cisco позволяет решать эти задачи за счет предоставления продуктов, которые могут использоваться независимо друг от друга, и решений, позволяющих связать эти продукты между собой после того, как у потребителя появится доверие к каждому продукту и подсистеме – успешный подход основан на объединении процессов разработки продуктов, приобретения продуктов, разработки систем и установления партнерских отношений. Поэтому имеет смысл рассмотреть основные этапы проектирования самозащищающейся сети Cisco.

Защита оконечных узлов. Вирусы и Интернет-черви, заражающие оконечные узлы, часто приводят и к побочному эффекту, - перегрузке сети, являющейся следствием быстрого распространения. Cisco предлагает средство предотвращения вторжений на оконечные узлы – Cisco Security Agent, позволяющее решить обе проблемы. Используемые в Cisco Security Agent передовые методы защиты на основе анализа поведения позволяют обнаруживать вирусы и Интернет-черви, а также предотвращать их проникновение на оконечные системы и распространения по сети. Фактически, Cisco Security Agent является первой линией обороны для предотвращения распространения вирусов и Интернет-червей.

Вторым очевидным аргументом в пользу применения Cisco Security Agent является то, что он используется на оконечных узлах, что позволяет создать цепь ответной реакции между оконечным узлом и сетью; в результате получается сеть, способная быстро адаптироваться к возникающим угрозам.

Контроль доступа. Одной из наиболее важных возможностей самозащищающейся сети Cisco является механизм контроля доступа к сети Cisco Network Admission Control (NAC).

NAC позволяет определить, какой уровень доступа следует предоставить оконечному узлу, исходя из соответствия *состояния узла* политике безопасности компании, которое определяется путем анализа состояния безопасности операционной системы и установленных приложений. В дополнение к функциям контроля и разграничения доступа NAC предоставляет IT-администраторам возможность автоматического перевода в карантин и лечения оконечных узлов, не прошедших проверку соответствия. Проверка соответствия конечных узлов политике безопасности (список установленных обновлений операционной системы, список обновлений антивирусного программного обеспечения и т.п.) является эффективной *второй линией обороны* для предотвращения распространения вирусов и Интернет-червей. NAC можно также рассматривать как инструментальное средство анализа уязвимостей и управления установкой «заплат» по требованию.

Отличительной особенностью NAC является предоставление как клиентского, так и административного интерфейса AAA, позволяющих потребителям устанавливать продукты большого числа разработчиков средств защиты оконечных узлов и политик безопасности с помощью средств NAC.

В настоящее время более 250 лидирующих на рынке разработчиков интенсивно внедряют или уже внедрили механизмы NAC в свои продукты.

Рисунок 4. Контроль доступа к сети

Важно предоставить возможность использования NAC в системах малых и средних предприятиям. Для этого Cisco несколько лет назад приобрела корпорацию Perfigo, областью деятельности которой является разработка комплексных решений контроля доступа к сети. Основными функциями решений являются анализ политик оконечных узлов, проверка соответствия состояния узлов установленным требованиям и обеспечение работоспособности средств контроля и разграничения доступа. Теперь в рамках инициативы Network Admission Control компания Cisco предлагает решение под названием Cisco NAC Appliance (Cisco Clean Access).

Ограничение области заражения. Усиленные политики доступа не являются панацеей и не устраняют необходимость мониторинга устройств после их входа в сеть. Квалифицированные злоумышленники в состоянии обойти практически любую проверку прав доступа, а сети не могут постоянно полагаться на зараженный элемент или *доверять* ему. Устройства, прошедшие проверку соответствия, также могут быть инфицированы с помощью разнообразных источников заражения после входа в сеть – например, может использоваться USB-диск с вредоносным содержимым. Самозащищающаяся сеть Cisco спроектирована для выполнения проверок безопасности не только во время получения узлом доступа к сети, но и в течение всего сеанса соединения, что позволяет еще больше усилить защиту сети. Кроме того, самозащищающаяся сеть может полагаться на другие элементы сети, включая оконечные узлы для определения компрометации других узлов, по аналогии с тем, как полиция контролирует уровень преступности путем анализа звонков на номер 911. Cisco рассматривает средства ограничения области заражения как *третью линию обороны* для предотвращения распространения вирусов и Интернет-червей.

К сожалению, существующие протоколы аутентификации не разрабатывались для работы после начального обмена информацией. Таким образом, самозащищающаяся сеть должна обеспечивать новые способы обмена информацией о состоянии устройств (контекст), а также способы оценки достоверности этой информации на основе как косвенного, так и прямого доверия. Например, администратор может создать правило, в соответствии с которым уведомление, полученное от оконечного узла с установленным агентом Cisco Security Agent, заслуживает большего доверия, чем уведомление, пришедшее от незащищенного оконечного узла. В результате компания Cisco начала разработку новых механизмов корреляционного анализа и ответной реакции на основе косвенных атрибутов.

Интеллектуальные средства корреляционного анализа и реагирования на инциденты. Для обеспечения эффективной работы методов ответной реакции, таких как ограничение области заражения, необходимо, чтобы самозащищающаяся сеть предоставляла сервисы корреляционного анализа событий в сфере безопасности в режиме реального времени, быстрой оценки воздействия события на систему безопасности, выбора конкретного действия, определения ближайшего средства защиты для ответной реакции и пр. Для решения этой задачи компания Cisco приобрела компанию Protego Networks, которая разработала семейство продуктов MARS, предоставляющих методы связывания ответной реакции от различных сетевых устройств (межсетевые экраны, системы обнаружения вторжений, маршрутизаторы, коммутаторы и хосты) с контекстом, получаемым в результате изучения топологии сети на уровне 2 и 3. Это позволяет группе реакции на нарушения в сфере безопасности быстро определить место появления атак в сети.

Cisco также сотрудничает с компанией netForensics и другими партнерами для расширения возможностей корреляционного анализа с целью улучшения процесса проверки самозащищающейся сети.

Интегрированные системы обнаружения вторжений и механизмы обнаружения аномалий. Проектирование эффективных систем обнаружения сетевых вторжений (NIDS) всегда было важным направлением в области постоянно ведущихся исследований и разработок Cisco. Одним из первых новшеств Cisco в этой области было внедрение NIDS в маршрутизаторы и коммутаторы. Но для того чтобы система NIDS обладала полной функциональностью, ее необходимо преобразовать в систему предотвращения вторжений (IPS) с встроенными возможностями фильтрации трафика. Механизм фильтрации трафика

позволяет отбрасывать ненужные пакеты с помощью тонко настраиваемых подсистем классификации трафика.

К сожалению, большинство NIDS выдают слишком много ложных срабатываний и не могут надежно выполнять задачу предотвращения атак при установке системы на промежуточном устройстве. Отчасти проблема заключается в необходимости сбора и обработки большого объема информации (контекста) в течение довольно короткого промежутка времени. В особенности это касается приложений, которые очень чувствительны к задержкам передачи (например, IP-телефония). Для решения этой задачи Cisco разрабатывает несколько методов, обеспечивающих высококачественную и эффективную обработку и классификацию контролируемого трафика.

Многие легальные действия могут быть ошибочно восприняты сетью как аномальные; главным образом, это касается сетей со значительным числом переменных факторов. В результате компания Cisco стала следовать консервативному поэтапному подходу к обнаружению аномалий, начиная с Cisco Security Agent, поскольку было установлено, что операционные системы моделировать проще, чем сетевые среды. После этого компанией Cisco была приобретена эффективная система предотвращения вторжений Riverhead, характеризующаяся низким числом ложных срабатываний за счет четкого разделения действий, направленных на проведение атак типа «отказ в обслуживании», и другой сетевой активности. Технология, которая была получена Cisco при приобретении Riverhead, позволяет обнаруживать атаки типа «отказ в обслуживании» с высокой точностью, количество ложных срабатываний чрезвычайно мало.

На базе опыта работы с Cisco Security Agent и возможностей четкого разделения сетевой активности, предоставляемых семейством продуктов Cisco Guard и Cisco Traffic Anomaly Detector, компания Cisco разработала систему предотвращения вторжений, которая сокращает число ложных срабатываний за счет использования передовых методов обнаружения аномалий и обмена состояниями (контекстами) между оконечными узлами и элементами (связями) сети. Эта система предотвращения вторжений также предоставляет механизм многовекторного обнаружения угроз и корреляционного анализа событий для быстрого обнаружения уязвимостей и оценки возможных последствий их использования. Поэтапное представление этих технологий на рынке позволяет Cisco поднять уверенность потребителей в своих возможностях и, следовательно, повысить доверие к концепции Cisco Self-Defending Network.

Безопасность приложений и защита от вредоносных программ (Anti-X). За последние несколько лет появились новые сетевые приложения, обеспечивающие защиту от новых видов угроз, – включая *вирусы, Интернет-червей, спам, шпионские программы, злонамеренное использование web-сервисов и средств IP-телефонии, а также несанкционированное использование клиентов файлообменных сетей*, – защита от которых не обеспечивалась в полной мере классическими межсетевыми экранами и продуктами NIDS (см. рис. 5). В целях защиты от этих угроз специалистами Cisco были разработаны сервисы защиты нового поколения, выполняющие проверку заголовков пакетов и их содержимого. Это позволяет обеспечить тщательную проверку трафика в критически важных точках сети и обрабатывать злонамеренный трафик до попадания в корпоративную сеть.

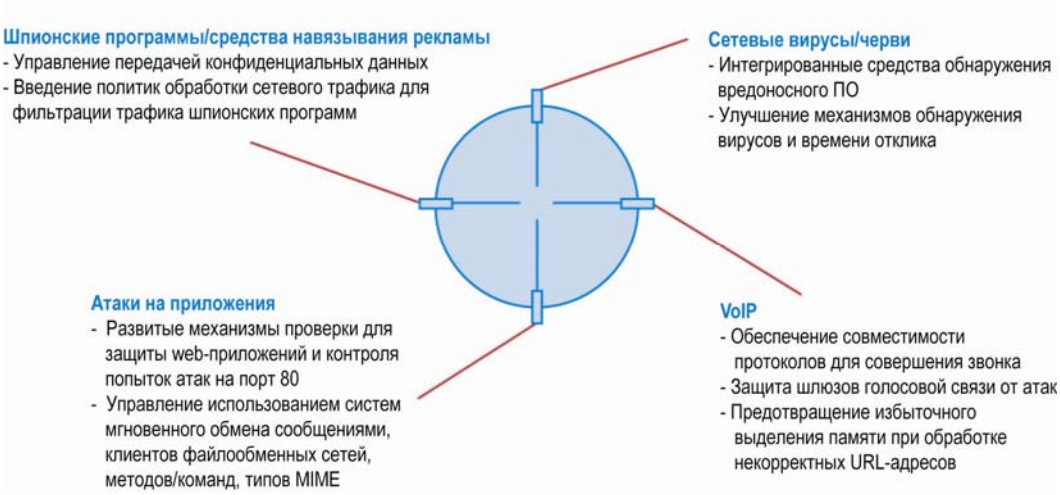

Рисунок 5. Улучшение защиты с помощью механизма многовекторного обнаружения неизвестных угроз

Объединение этих сервисов в многофункциональные платформы позволяет расширить возможности разработчиков, а также снизить совокупную стоимость владения для потребителя. Кроме того, интеграция этих механизмов позволит расширить возможности самозащищающейся сети по контролю приложений.

Если в приложениях используется сквозное шифрование, самозащищающаяся сеть может собирать информацию с конечных узлов, компенсируя потери, связанные с невозможностью контроля данных на границе сети.

СЛЕДУЮЩИЕ ШАГИ

Cisco будет продолжать увеличивать капиталовложения в построение самозащищающихся сетей, позволяющих создавать взаимосвязи между средствами обеспечения безопасности сети, включая оконечные системы (см. рис6). Таким образом, Cisco предоставляет организациям более широкие возможности по контролю и управлению устройствами, пользователями и приложениями, взаимодействующими в рамках инфраструктуры сети предприятия. Это знаменует необходимый и важный этап развития сетей, сравнимый с ведение интеллектуальных протоколов маршрутизации.

Рисунок 6. Cisco продолжает расширять возможности самозащищающейся сети

Основные понятия самозащищающейся сети Cisco Self-Defending Network, кратко изложенные в рамках данного документа, заслуживают более подробного рассмотрения. Предложенный подход позволяет обеспечить безопасность сетей сегодня и заложить основу для проектирования безопасных сетей в будущем. Выбор каждой организации зависит от конкретных требований к системе защиты, приемлемых рисков и других задач:

- Сотрудникам, ответственным за безопасность периметра, стоит познакомиться с представленными недавно платформой межсетевого экрана Cisco PIX® 7.0 и платформой маршрутизаторов с интегрированными сервисами. Эти решения предоставляют множество механизмов обеспечения безопасности и функционирования сети, включая тщательную проверку данных и контроль широкого спектра протоколов и присущих им атак.
- Группам информационной безопасности, которые прилагают невероятные усилия для поиска способов отражения нарушений безопасности, следует освоить технологию Cisco MARS, а также расширить свои знания о новых возможностях системы предотвращения вторжений, встроенной в инфраструктуру и устройства защиты.
- Сотрудникам, отвечающим за данные критической важности, которым часто приходится иметь дело с атаками DoS и DDoS, следует ознакомиться с технологией Cisco Guard и Cisco Traffic Anomaly Detector.
- Сотрудникам, которым постоянно приходится бороться с Интернет червями и вирусами, или сотрудникам, которым необходимы решения для проверки соответствия конечных узлов требованиям политики безопасности, следует освоить технологии Cisco Security Agent, Network Admission Control и Cisco Clean Access.
- Аудиторам, ответственным за оценку соответствия узлов нормативным документам, следует освоить технологии NAC, средство CiscoWorks Security Information Management System (SIMS), которое предоставляет подробную информацию об использовании инфраструктуры коммуникаций в целом, а также систему аудита Cisco Security Auditor.

И, наконец, IT-специалистам, отвечающим за проектирование и развертывание систем безопасности и сетевой инфраструктуры, следует обращаться к представителю партнера Cisco для получения дополнительной информации о самозащищающейся сети.

Cisco Systems
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб., 52,
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004, Киев,
бизнес-центр
«Горайзон Тауерс»
Ул. Шовковична, 42-44,
этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

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