Современные системы предотвращения вторжений

ТЕКСТ: **Наталья Павлюк**

В центре внимания – решения, обеспечивающие передовую линию обороны в составе защищенных сетей, высокую доступность информационных активов и их устойчивость.

В сегменте информационной безопасности уже довольно давно существует подкласс систем, именующихся системами предотвращения вторжений – IPS. Зачастую, агрессивный маркетинг производителей систем безопасности смешивает схожие по направленности понятия, и определить наверняка, что же такое система предотвращения вторжений бывает нелегко. Постараемся определить для начала механизмы и типы угроз, от которых защищают системы предотвращения вторжений, затем – свойства и существующие типы систем данного класса.

Итак, системы предотвращения вторжений бывают четырех типов: сетевые системы, системы поведенческого анализа, системы предотвращения атак на беспроводные сети, а также хостовые системы.

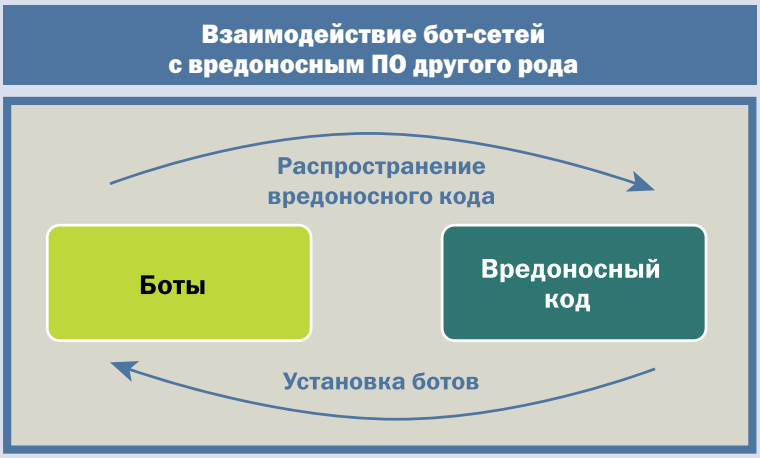
Ликбез: методы обнаружения

Процесс обнаружения и предотвращения атак на уязвимости, как таковой, подразумевает анализ и реакции на события: нарушения политик безопасности, политик использования ресурсов, политик стандартизации. Инциденты могут иметь любую природу, например, вредоносный код, неавторизованный доступ или попытки получения дополнительных прав. Системы предотвращения вторжения умеют непосредственно воздействовать на такие компоненты атаки, как

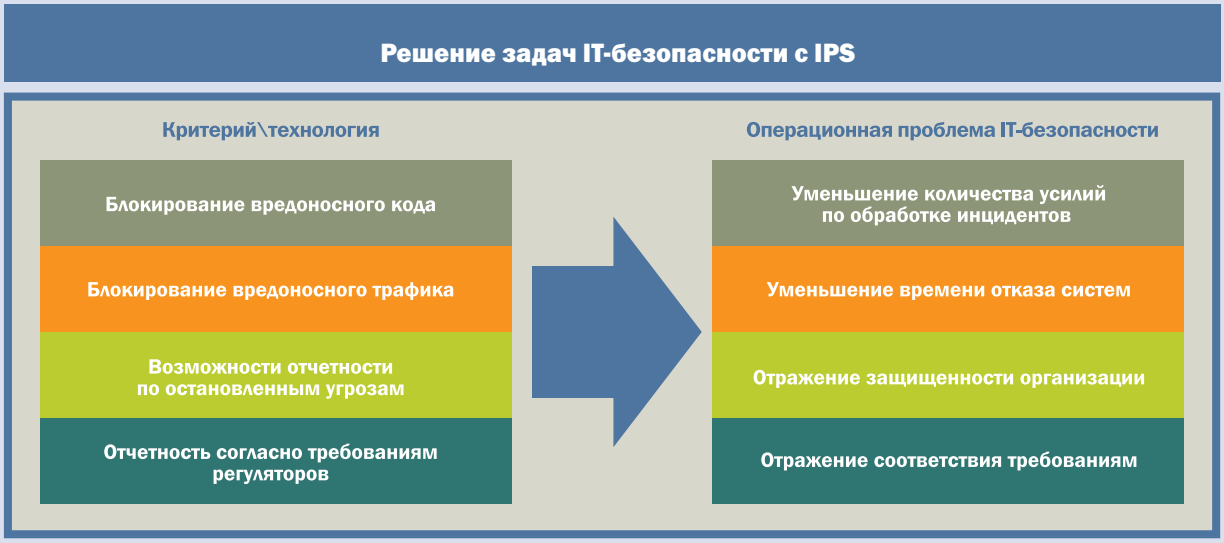
тело атаки, например, обрыв соединения; среда безопасности, например, переконфигурирование файерволла для запрета сетевого доступа в сегмент; содержимое атаки, или удаление вредного аттачмента. Среди общих методов обнаружения можно выделить три основных.

Сигнатурное обнаружение, как метод, основывается на сопоставлении шаблонов событий, соответствующих паттернам известных атак. Например, подключение telnet к ресурсу с помощью root может являться нарушением политик безопасности. Надо понимать, что сигнатурное обнаружение является эффективным для уже известных атак, когда возможно точное сопоставление события существующего в системе паттерна, защита по принципу: есть сигнатура – есть защита. Его преимуществом является высокая скорость реагирования и анализа, в силу использования локальных сканирующих ресурсов. Но важно понимать, что сигнатурный метод обнаружения не оснащен механизмами сопоставления нескольких последовательных событий, а также сопоставления ответов ресурсов запросам, например ответ ВЕБ-сервера с кодом 403 необходимо сопоставить с невозможностью выполнить запрос, порой даже переименование исполняемого файла в составе атаки может обойти сигнатурный модуль.

Обнаружение аномалий – это механизм, работающий по принципу сопоставления паттернов активности соединений, пользователей, хостов или приложений. Паттерны, в свою очередь, являются неким слепком поведения того или иного объекта за определенный промежуток времени. Паттерны состоят из отдельных атрибутов, примером которых могут быть: ширина полосы использования ВЕБ-трафика, количество входов пользователя в систему, количество отосланных сообщений электронной почты, процент использования ресурсов процессора и т д. Данный механизм является высокоэффективным для использования против неизвестных угроз, когда мы обладаем набором



Источник: Reading Room SANS Intrusion Detection & Response – Leveraging Next Generation Firewall Technology



Источник: Forrester Market Overview: Intrusion Prevention Systems 2011

ТОЧКА ЗРЕНИЯ

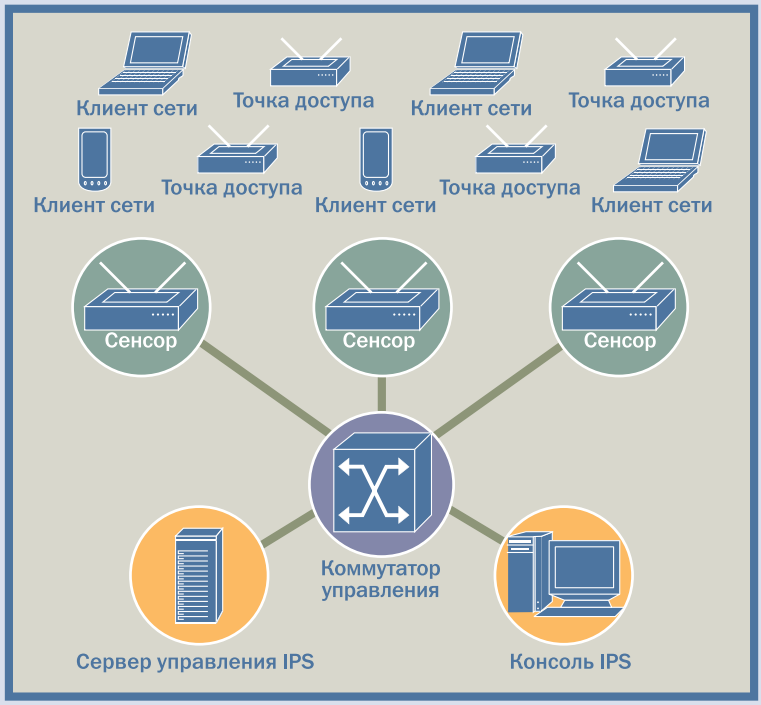
Сергей Дугарев,
руководитель направления компании Headtechnology

Нельзя недооценивать угрозы безопасности для беспроводных сетей

У нас есть основания утверждать, что 2012-й будет годом наибольшей востребованности решений защиты беспроводных точек подключения. В частности, для решений компании AirTight Networks, позволяющих обеспечить уникальную безопасность гетерогенных информационных сред. Если говорить о типах компаний клиентов в сегменте решений защиты беспроводных точек, прежде всего, это банковский сектор, где есть необходимость подтверждения соответствия требованиям PCI DSS, а также компании с уже выстроенной инфраструктурой. Самой серьезной угрозой безопасности для этой сферы является недооценка существующих угроз для беспроводных сетей. Зачастую IT-руководство компании уверено в защищенности простейших беспроводных решений, на которых построена сеть. Второй по значимости можно рассматривать угрозу некачественного конфигурирования уже используемых точек подключения. Затем идут угрозы, связанные с отсутствием должного контроля за размещением точек доступа.

Возвращаясь к нашему продукту WIPS AirTight Networks, нужно отметить, что основным преимуществом решения является возможность развертывания над существующей инфраструктурой заказчика (OVERLAY), то есть мы не зависим от того, насколько гетерогенна сеть заказчика. Решение интегрируется с оборудованием всех основных производителей сетевого оборудования и в качестве компонента включено в систему Hewlett Packard ProCurve Open Networking Ecosystem (ProCurve ONE). Закупка решения WIPS AirTight Networks осуществляется по схеме «бессрочная лицензия с подпиской».

Пример архитектуры беспроводного IPS



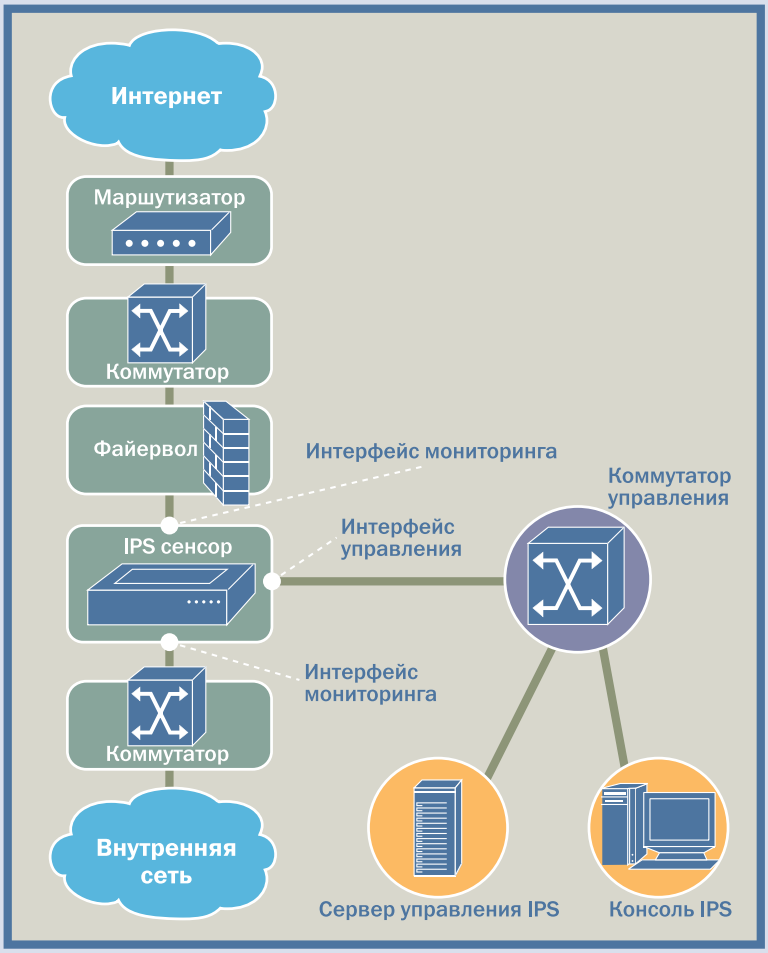
Источник: NIST Guide to Intrusion Detection and Prevention Systems

параметров, свойственных нормальному функционирования среды, но не известны сигнатуры атаки непосредственно. Системы, оснащенные механизмами анализа аномалий, зачастую требуют обязательный период обучения для захвата паттернов нормального функционирования защищаемой среды, такой период может длиться от нескольких дней до нескольких недель. Паттерны могут быть как статичными, так и динамическими. Одна из проблем поведенческих систем предотвращения заключается в том, что зачастую «нормальность» функционирования инфраструктуры меняется от времени к времени, и системы приходится «переучивать». Например, конец квартала в отделе продаж увеличивает нагрузку на все используемые средства связи, что является вполне нормальным. Примером может также быть передача резервных копий на месячной основе, потребляющая большой объем трафика. Таким образом, для большинства инфраструктур динамические паттерны являются рекомендованной формой поведен-

ческой защиты. Несмотря на красоту данного сценария, существует риск медленной атаки, когда злоумышленник постепенно наращивает потребление атакованных ресурсов и так попадает в динамически меняющееся окно обновления. Таким образом, важным этапом при использовании систем поведенческого анализа является определение правильных расписаний для обучения, которые будут включать в себя наибольшее множество событий нормального функционирования вашей сети.

Устойчивый анализ протокола является алгоритмом сопоставления и обнаружения отклонений в приемлемой активности протоколов на каждой стадии взаимодействия. Это означает, что сенсоры работают на трех уровнях: сетевом, транспортном, а также уровне приложений. Например, пользователь начинает FTP-сессию, на стадии использования возможностей аутентификации протокола может быть использован ряд команд, сенсор отслеживает их появление, после перехода в аутентифицированную часть сессии сенсор будет отслеживать последующие ожидаемые сессионные команды взаимодействия, в то же время обнаружение команд, не свойственных определенному этапу взаимодействия будет свидетельствовать о подозрительности поведения внутри сессии. Анализ протокола подразумевает проверки количества команд, а также количества аргументов, используемых в составе команд. У метода есть и ряд ограничений: высокое потребление системных ресурсов, за счет сложности алгоритмов проверки. Также необходимо отметить, что метод анализа протокола не умеет обнаруживать атаки, не выходящие за рамки стандартного использования протоколов, например, когда устанавливается большое количество одновременных сессий в рамках правильного использования протокола, но, тем не менее, вызывающие отказ в обслуживании систем (DoS). Иногда также возникает потребность доводки механизмов анализа для работы с отдельными версиями протоколов в приложениях, поведение протоколов может меняться от версии к версии.

Пример архитектуры IPS, подключаемого в разрез сети



Источник: NIST Guide to Intrusion Detection and Prevention Systems

Никаких сетевых атак!

Сетевые системы анализируют трафик для отдельных сетевых сегментов и устройств и работают на трех уровнях: сетевом, транспортном и уровне приложений.

Архитектурно сетевые системы подразделяются на подключаемые в разрез сети, обычно они ставятся за файерволлами, такие системы могут обнаруживать атаки на уровне разных подсетей. Также существует отдельный класс пассивных систем обнаружения вторжений – IDS, они подключаются через зеркальный SPAN-порт к граничному свичу, через который проходит трафик подсетей. Кроме того, такие системы могут подключаться посредством TAP-устройств. В принципе, тип пассивных систем предотвращения вторжений является наиболее актуальным для компаний, которые настроенны использовать бесплатные продукты с открытым кодом. Активные системы предотвращения вторжений

ТОЧКА ЗРЕНИЯ

Андрей Пастушенко,
специалист отдела технической поддержки проектов группы компаний «БАКОТЕК»

Основные заказчики – финансовый сектор и представительства зарубежных компаний

В основном IPS и NBA интересуются компании средних и больших размеров с распределенной ИТ-инфраструктурой. Как правило, это компании финансового сектора или зарубежного происхождения. Наиболее актуальными для компаний в сегменте систем IPS и NBA являются вредоносные программы, угрозы «нулевого дня», атаки отказа в обслуживании, бот-сети, несанкционированное использование приложений. Прежде всего, для заказчиков подобных систем важна эффективность предотвращения вторжений в сеть как за счет технологий «на борту» решения, так и за счет глобальных исследований производителя, важна приоритезация приложений, их контроль, идентификация пользователей, гибкая интеграция в существующую инфраструктуру, максимально возможный уровень мониторинга и отчетности. Одно из решений, которое представляет «БАКОТЕК», IPS McAfee Network Security Platform, ранее известное под названием IntruShield, произведено в 2000 году компанией IntruVert Network, которая в свою очередь была поглощена McAfee в 2003 году. В Украине продажи McAfee NSP начались уже в 2006 году. Среди решений McAfee стоит отметить шлюзы поведенческого анализа, McAfee – Network Threat Behavior Analysis и Network User Behavior Analysis, ранее известные как Securify. Упомянутые решения являются доступными на Украине.

Поставляемые «БАКОТЕК, продукты McAfee оснащены уникальными механизмами контроля трафика с сохранением состояния соединений, реагирования на ранее неизвестные угрозы от Global Threat Intelligence (центр реагирования на основании информации миллионов датчиков со всего мира), механизмов идентификации новых бот-сетей на основании поведения трафика. Технология Application Prism дает возможность точного определения и контроля более 1100 приложений, а также их отдельных функций.

Если же говорить о денежном вопросе, закупка и продление перечисленных решений осуществляется по схеме «аппаратная платформа + лицензия на ПО и поддержку».

в своей архитектуре подключаются в разрез сети и блокируют атаки непосредственно. Если система не обеспечивает блокирование атак сама по себе, она должна уметь отдавать инструкцию блокирования коммутатору на сетевом уровне. Такой подход является в некотором роде устаревшей методикой предотвращения. Если говорить о платных сетевые системах предотвращения вторжений, то они зачастую требуют внимания к настройке и расширенное конфигурирование. Так, например, полезной является настройка пороговых значений, а также профилей сканирования по разным портам устройств. В свою очередь, привязка сервисов к пулам IP-адресов может значительно оптимизировать работу сетевой системы. Некоторые решения дают доступ даже к редактированию кода сигнатур, что требует от пользователя данных систем высокого уровня подготовки, но при этом появляется несравнимый уровень гибкости настройки такой системы предотвращения вторжений.

Для сетевых систем предотвращения вторжений существует ряд технологических ограничений, которые надо учитывать. Основные ограничения это: невозможность непосредственного анализа шифрованного трафика, а также невозможность полного анализа при высоких нагрузках. Проблема шифрованного трафика решается размещением систем за VPN-шлюзами, таким образом, весь поступающий на вход трафик уже будет являться расшифрованным и доступным для анализа. Проблема высоких нагрузок решается на этапе выбора устройства, производитель указывает рекомендуемую пропускную способность каждой системы и количество одновременных соединений. Превышение рекомендуемых параметров при использовании чревато потерей пакетов или высокой задержкой при прохождении.

Ваше поведение будет проанализировано

Системы поведенческого анализа ориентированы на мониторинг необычных отклонений в палитре проходящего трафика, а также событий и атак, которые можно отследить сбором статистики с множества распределенных шлюзовых точек. Например, к таким событиям относятся DDOS-атаки, распространение червей, предоставление сетевых сервисов неавторизованным сетям. Архитектура решений поведенческого анализа обычно подразумевает наличие двух типов устройств: сенсоров, собирающих данные, и серверов управления, эти данные консолидирующих. Существующие поведенческие

ТОЧКА ЗРЕНИЯ

Сергей Маковец,
директор по технологиям компании ISSP

Наблюдается тенденция сближения технологий предотвращения сетевых вторжений с межсетевыми экранами

На сегодняшний день IPS и NBA решениями интересуются большие компании. SMB-сектор использует устройства класса UTM. В данном направлении есть огромное количество угроз. Корпоративный веб-сервер может подвергаться DOS-атакам или специализированным sql-инъекциям. Для финансовых институтов характерно наличие атак, которые характеризуются точечностью воздействия и невозможностью обнаружения стандартными средствами. Сейчас наблюдается тенденция сближения технологий предотвращения сетевых вторжений с межсетевыми экранами. Использование ранее различных функций в рамках одного устройства позволяет уменьшить количество занятых мест в ЦОД, время реакции на атаки, а также нагрузку на файервол. Необходимо отметить, что многие заказчики сейчас желают иметь в составе решений этого класса также полноценный контроль приложений и контроль URL.

Решения компании Sourcefire, представляемые нашей компанией, известны за рубежом с 2002 года, но распространение получили за последние 6 лет. Использование Sourcefire в качестве защиты от сетевых вторжений силовыми структурами США говорит о многом. В Украине продукция Sourcefire появилась в 2009 году. А созданная собственником компании Sourcefire Мартином Роешом бесплатная сетевая система предотвращения вторжений Snort известна миллионам пользователей с 1998 года. Запатентованное пассивное сканирование трафика RNA позволяет построить полную карту ИТ-активов (ОС, используемые сетевые протоколы и сервисы). Используя знания о сети, можно резко снизить нагрузку на IPS-сенсоры и всегда защищать ИТ-активы от целевых атак. Автоматическая подстройка правил оптимизирует стоимость сопровождения, а карта сети в реальном масштабе времени позволяет создавать правила для обнаружения несоответствия политикам безопасности, принятым в компании. Сетевой процессор FirePOWER позволяет обрабатывать трафик со скоростью до 40 Гбит/с. FirePOWER обеспечивает модульную архитектуру и позволяет определять трафик от сотен пользовательских приложений с минимальной на рынке задержкой(latency) в 150 микросекунд. Использование RNA существенно сокращает время установки в инфраструктуру, в результате внедрение IPS можно провести в течение одного дня.

системы могут мониторить трафик по аналогии с сетевыми системами предотвращения – то есть по принципу снифера, перехватывая трафик сегментов сети, либо анализируя поток. Под потоком в данном случае подразумевается отдельная сессия, устанавливающаяся между хостами (например, netFlow, sFlow). Зачастую системы поведенческого анализа являются пассивными сетевыми устройствами и подключаются через SPAN, TAP-порты. Особенность в том, что решения данного класса должны мониторить трафик с целых сетевых сегментов, поэтому рекомендуется размещать их в DMZ, или непосредственной близости с периметральными файерволами.

Доводка систем поведенческого анализа подразумевает сбор статистики так называемых паттернов трафика, свойственных инфраструктуре пользователя, а также дальнейшее определение значений для срабатывания оповещения по паттернам. Основным ограничением систем поведенческого анализа является их зависимость от непосредственных источников событий: таких как свичи и сетевые системы предотвращения. Как результат задержек передачи событий, некоторые типы атак, такие как DOS и вирусная инвазия, могут быть обнаружены уже после их осуществления. Причиной задержек может быть также использование перехвата пакетов вместо анализа потока, как такового. Если организация намерена использовать средства перехвата пакетов, необходимо уделить внимание расчету адекватного быстродействия выбранных решений поведенческого анализа.

Защита без провода

Беспроводные системы предотвращения ориентированы на анализ протоколов беспроводной связи IEEE 802.11a, b, g, идентификации и предотвращения подозрительной активности. Необходимо сразу обозначить, что данный класс систем не работает на более высоких уровнях модели OSI. Спецификой атак на беспроводные сети является тот факт, что для их успешности атакующий должен находиться в непосредственной близости от точки доступа, в случае с проводными сетями, атака фактически может осуществляться из любой точки.

В основе атак на беспроводные сети лежит перехват трафика точки доступа или между двумя станциями, а также внедрение дополнительных

ТОЧКА ЗРЕНИЯ

Иван Белевцов,
начальник отдела продаж System Integration Service

Беспроводной широковещательный доступ тесно связан с необходимостью контроля и защиты от возможных угроз при доступе к ресурсам сети

В современных условиях системы предотвращения вторжений используются компаниями в рамках общей стратегии обеспечения сетевой безопасности, которая уже давно не ограничивается только защитой периметра сети. Необходимость в более глубоком анализе передаваемых в сети данных и их природе определяется не только критичностью самих корпоративных сервисов, но и унификацией доступа к ним. Так, например, широкое распространение, которое сейчас получили мобильные устройства (смартфоны, планшеты, ПК), используемые для работы с корпоративными данными и приложениями, обусловило необходимость внедрения беспроводных сетей корпоративных масштабов. Беспроводной широковещательный доступ очень тесно связан с необходимостью контроля доступа и защиты от возможных угроз при доступе к ресурсам сети. Выходом может послужить внедрение системы обнаружения атак в беспроводной среде передачи данных. Системы обнаружения беспроводных атак пока не настолько популярны, как их проводные аналоги, но тенденции роста угроз неутешительны. К примеру, решение от Cisco под названием Adaptive Wireless Intrusion Prevention System является расширением функционала компонентов беспроводной сети, позволяющим обеспечивать защиту, специфичную именно для беспроводного доступа, работая совместно со стандартными системами сигнатурного анализа и другими средствами защиты.

Что касается классических систем предотвращения вторжений, то все чаще их приходится сравнивать с брандмауэрами уровня приложений (Web Application Firewall). Обычно системы предотвращения вторжений являются статическими анализаторами исходного кода (Static Application Security Testing). Эти системы можно рассматривать как сканеры приложений – просматривающие его байт-код или двоичные файлы, целью систем является поиск индикаторов уязвимости. Однако многие из этих систем также обеспечивают динамическое тестирование безопасности на уровне приложений (Dynamic Application Security Testing). Наиболее эффективно системы работают, используя обе эти технологии одновременно. К таким системам можно отнести решения компании IBM Proventia Network IPS, Server IPS и Virtual Server IPS, обеспечивающие защиту сетевой инфраструктуры, виртуализированных и аппаратных серверов. Как правило, выбор решений данного сегмента основывается на общей стратегии и политиках безопасности компании, вырабатываемых в ходе аудита, проводимого сертифицированными специалистами SIS совместно с сотрудниками клиента.

данных в состав сеанса беспроводной связи. В отличие от кабельных систем предотвращения, получающих все пакеты сети, беспроводные системы делают выборку трафика. Существует два основных диапазона частот 2,4 Ггц и 5 Ггц, которые в свою очередь делятся на каналы. Системы обеспечивают поочередное сканирование каналов на предмет атак. Полезным функционалом беспроводных систем предотвращения является возможность обнаружения атакующего с помощью метода триангуляции, и, как последующий метод реагирования, может использоваться физическая безопасность. Использование метода триангуляции вместе с планами зданий позволяет качественно приоритезировать беспроводные угрозы. Обсуждаемые беспроводные сенсоры умеют осуществлять воздействия 2-х типов при обнаружении атаки: беспроводное воздействие – когда обрывается соединение между клиентом и точкой доступа посредством отсылки сообщения о диссоциации сессии, после чего сенсор отказывает в восстановлении соединения; сетевой тип воздействия – сенсор передает кабельному свичу команду блокировать соединение с заданного клиента сети на основании порта или MAC. Необходимо заметить, что для систем беспроводного предотвращения атак свойственны такие ограничения: невозможность отлавливания пассивных атак, когда атакующий собирает пакеты без подключения к сети, а, следовательно, не обозначает свое присутствие. Как средство защиты от данных атак рекомендуется использовать криптостойкие методы аутентификации пользователей сети и при необходимости – средства жесткой аутентификации.

«Персональная» система защиты от вторжений

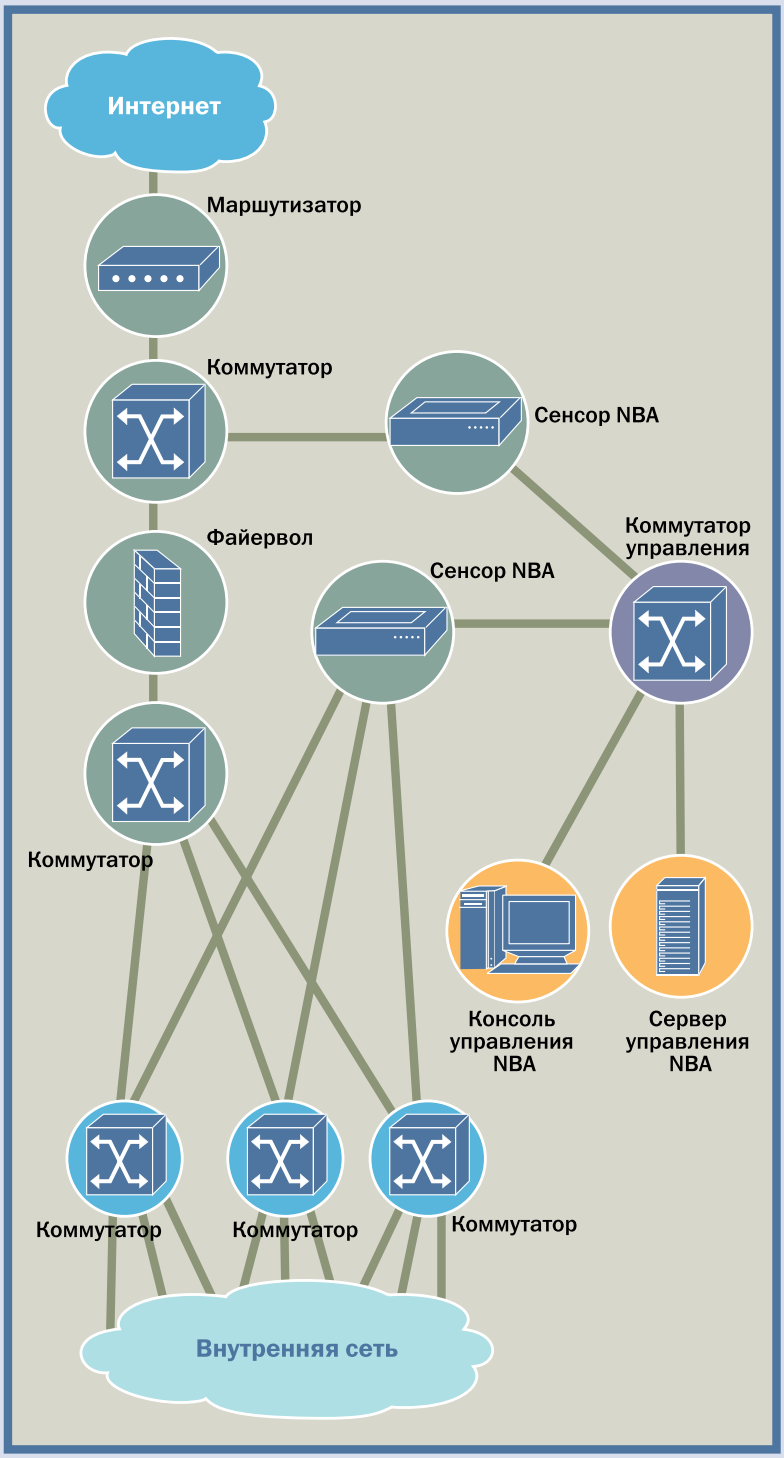
Хостовые системы предотвращения атак обеспечивают защиту отдельной платформы как от сетевых, так и от беспроводных атак, а также

могут обеспечивать мониторинг выполнения процессов, изменения конфигураций и доступ к файлам, и даже доступ к съемным устройствам. Особенностью хостовых систем является необходимость установки программного компонента на каждую защищаемую платформу. Зачастую такой компонент рассчитан на защиту отдельного сервера, рабочего места или отдельного выполняемого процесса. Архитектура подобных решений является двухуровневой, а также клиент-серверной, компоненты, установленные на конечные точки, управляются из единого центра управления, на котором также консолидируется вся информация о событиях и политиках. Установка компонентов хостовых систем предотвращения осуществляется на ресурсы высокой критичности или ресурсы, расположенные публично. С одной стороны, хостовые системы обладают более широким охватом угроз, с другой стороны, их использование подразумевает более сложное сопровождение, в силу того, что необходимо определить совместимость с платформами, сервисами, а также наладить процедуры сопровождения модулей на каждой из защищенных точек. К ограничениям, касающимся хостовых систем предотвращения вторжений, относятся следующие: задержки при передаче уведомлений об атаках в силу использования расписаний в клиент-серверной архитектуре, использование аппаратных ресурсов защищаемой платформы, необходимость тщательного тестирования на предмет совместимости с используемым прикладным программным обеспечением.

Тестируйте одновременно

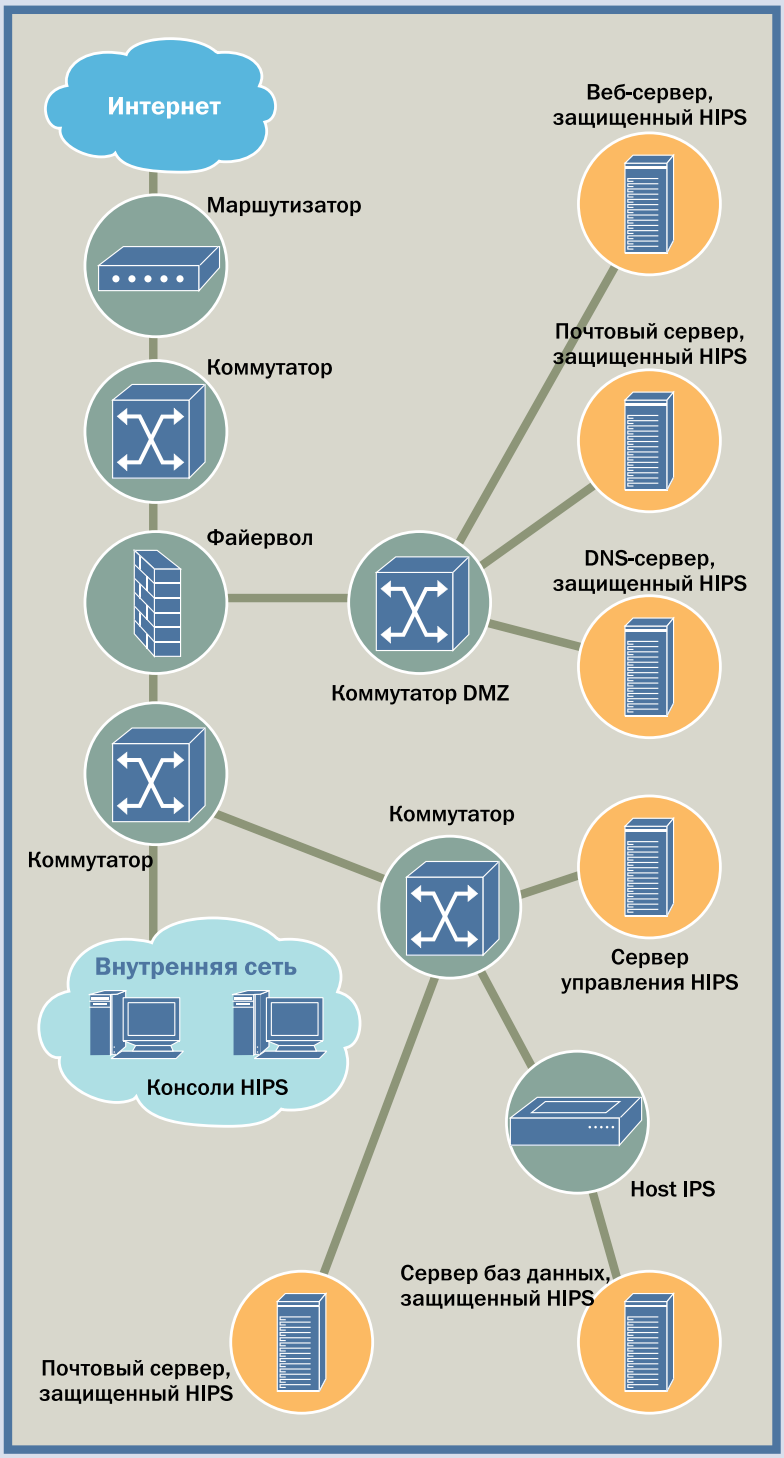
Во время выбора продукта по предотвращению сетевых атак хорошей практикой является тестирование нескольких вендоров параллельно. Такую схему тестирования можно

Пример архитектуры поведенческого IPS (Network Behavior Analysis)



Источник: NIST Guide to Intrusion Detection and Prevention Systems

Пример архитектуры хостового IPS(HIPS)



Источник: NIST Guide to Intrusion Detection and Prevention Systems

реализовать в случае установки решений на разные наименее критичные сегменты сети. Таким образом, устройства будут одновременно обрабатывать реальный трафик реальной инфраструктуры, что облегчит анализ эффективности. При тестировании систем предотвращения атак пользователю стоит обратить внимание на ряд пунктов, позволяющих ускорить и сделать более эффективным процесс проверки продукта на соответствие инфраструктурным требованиям. А именно, необходимо оценить:

1. Время на установку решения.
2. Время для конфигурирования среды до установки решения. Важно учитывать поправки на совместимость с гетерогенными средами, а также возможности мультиплатформенной защиты.
3. Какой процент уязвимостей покрывается при использовании «из коробки».
4. Простота использования. Возможности управления такими объектами, как приложение, пользователь, группа пользователей, агент.
5. Интеграция с сетевыми устройствами других производителей.
6. Управление устройствами, сложность развертывания, частота обновлений сигнатур безопасности. Величина окна между появлением уязвимости и выпуском обновления для того или иного механизма IPS является важным фактором эффективности работы системы, данное временное окно должно быть значительно меньше, чем время выпуска патча производителем атакуемого программного обеспечения.
7. Эффективность защиты в штатном режиме, а также режиме предотвращения атаки. Как уже было сказано ранее, при блокировании атак пропускная способность полезного трафика у систем предотвращения атак может резко снижаться.

ТОЧКА ЗРЕНИЯ

Андрей Ротач,
директор по развитию компании NetWave

Решения IPS на сегодня являются в большей степени «облачными» системами

В последние годы довольно популярными стали IPS-системы, включенные в функционал UTM (unified threat management) устройств, которые включают в себя разнообразный функционал обеспечения сетевой безопасности. Такие IPS-системы менее гибкие, по сравнению с отдельными IPS устройствами, и, тем не менее, они зачастую проще в освоении и дешевле, поэтому доступны для малого и среднего бизнеса.

Наша компания предлагает различные решения для различных сегментов рынка, например решения Cisco и McAfee – это зрелые системы, которые прошли испытание временем. Также UTM-системы от Fortinet, которые имеют функционал IPS и предназначены для малого и среднего бизнеса, данные системы просты в настройке, что уменьшает затраты на эксплуатацию. Интересные решения представлены новичком рынка сетевой безопасности, компанией PaloAlto networks, эти устройства имеют комплексный функционал, позволяющий идентифицировать и управлять трафиком в разрезе пользователь, приложение, контент. Решения IPS на сегодня являются в большей степени «облачными» системами, ведь они состоят из программно-аппаратной платформы, работающей на стороне заказчика и «облачного» сервиса производителя, с которым взаимодействует платформа для определения атак, репутаций и обновления своих сигнатурных баз. Программно-аппаратная платформа оптимизирована для максимально эффективного выполнения задач, в IPS McAfee, например, используются специализированные микросхемы, что обеспечивает высокую производительность на уровне железных компонентов. Сессии соединений анализируются несколькими программными модулями, которые работают с отдельными пакетами, последовательностями, всей сессией в целом или протоколами уровня приложений. При работе с данным типом средств предотвращения наша компания NetWave предлагает своим заказчикам квалифицированную консультацию и возможности бесплатного тестирования выбранного решения на период проработки проектного решения, чтобы заказчик мог познакомиться с продуктом и убедиться в правильности выбора.

8. Эффективность работы системы с ложными срабатываниями. Гибкость обнаружения и доводки настроек являются залогом эффективного сопровождения.
9. Возможности отказоустойчивости и высокой доступности. Модельный ряд и возможности масштабирования на разные архитектуры сети могут быть решающими при выборе унифицированного решения на всю компанию.
10. Возможности отчетности. Степень детализации отчетов, избыточность для расследования инцидентов.
11. Возможности и стоимость поддержки со стороны производителя.
12. Доступность и стоимость специализированных тренингов по системам.
13. Наличие истории удачных внедрений, а также оценок независимых тестовых лабораторий. Знание, где уже используется тестируемое вами решение, может уберечь заказчика от покупки еще сырого продукта. Независимые лаборатории также проводят тесты в «живой среде» и в значительной степени могут оценить адекватность поставляемого продукта.

Выводы

Хочется отметить высокую важность контекстной ориентации разрабатываемых систем безопасности. Контекст систем в данном случае означает детализированную возможность анализа условий, атрибутов и объектов, в которых происходит использование информационных ресурсов. Функционал анализа событий защищаемой информационной среды может включать множество параметров обмена данными: версию используемого программного обеспечения и его компонентов, время соединения, региональное размещение подключаемого клиента, используемые протоколы, используемые методы аутентификации, наличие одновременных сессий и запущенных процессов и их количество, обнаруженные уязвимости системы и программного обеспечения на подключаемых системах, типы передаваемых данных, классификацию самих подключаемых клиентов виртуальные или физические. Адаптивная защита, построенная на подобных факторах, в перспективе позволит добиться высокого уровня безопасности и гибкости защищаемых информационных сред и, как результат, стойкого функционирования бизнеса.