ИНТЕГРИРОВАННЫЕ UTM-УСТРОЙСТВА – НА СТРАЖЕ КОМПЬЮТЕРНОЙ СЕТИ

Р. Косичкин, технический специалист Rainbow Technologies,
О. Коваленко, PR-менеджер Rainbow Technologies

Все чаще в последнее время, говоря об информационной безопасности, СМИ используют термин «UTM-устройства». Понятие «Unified Threat Management» (UTM), обозначающее отдельный класс оборудования для защиты сетевых ресурсов, было введено международным агентством IDC, исследующим ИТ-рынок. По его классификации, UTM-устройства – это многофункциональные программно-аппаратные комплексы, в которых интегрированы функции межсетевого экрана, системы обнаружения и предотвращения вторжений в сеть, а также функции антивирусного шлюза.

Однако у специалистов по информационной безопасности, работающих на российском рынке, много вопросов вызывает то, какие же решения всё-таки являются UTM-устройствами, а какие – нет. Полноценные UTM-устройства производят такие всемирно известные компании, как Symantec, WatchGuard Technologies и Fortress. Вот уже несколько лет эти фирмы входят в первую пятерку по объемам продаж. В конце 2005 года, по данным все того же IDC, WatchGuadr Technologies уверенно заняла позиции лидера по объему продаж UTM-устройств в сегменте SMB (малый и средний бизнес).

Так что же в себе таит аббревиатура UTM (в дословном переводе – «объединенное управление угрозами»)? Тут же возникают дополнительные вопросы: какими угрозами и как нужно управлять, и каким образом должно функционировать устройство, чтобы считаться полноценным UTM?

УГРОЗЫ СРЕДИ НАС

Защита локальных сетей предприятий с каждым годом становится все более сложной задачей, и сегодня является одним из основополагающих факторов, с которым сталкивается бизнес. Новые и постоянно изменяющиеся угрозы появляются с пугающей регулярностью, и ни одна организация от них не застрахована.

Каждый раз при появлении новых, более опасных угроз изменяется само понятие «безопасная сеть». По данным SANS Institute, только за первый квартал 2005 года было обнаружено более 600 сетевых уязвимостей [1].

Когда сеть подвергается вторжению, DoS-атаке или вирусной эпидемии, под угрозой оказывается деятельность всей организации. Это происходит вследствие увеличения опасности для операционных ресурсов, пользовательских данных, собственных средств и технологий. Интеллектуальная собственность может быть украдена и неправомерно использована третьей стороной.

Разновидности сетевых атак

Сетевое вторжение. В случае использования сетевого вторжения хакер, не имеющий прав доступа, пытается удаленно проникнуть в сеть для осуществления враждебных действий.

DoS/DDoS-атаки. В случае DoS-атаки подвергнутые нападению системы становятся недоступными зачастую из-за монопольного захвата сетевых ресурсов. Распределенные DoS-атаки (DDoS) используют множество компьютерных систем (возможно, сотни) для посылки трафика на выбранные адреса.

Вирусы. Вирус – это компьютерная программа, которая «заражает» другие программы своими копиями, клонируя себя с диска на диск или от одной системы к другой по компьютерным сетям. Вирус запускается и производит свои разрушительные действия при работе «зараженной» программы.

Рекламное и шпионское программное обеспечение. Рекламное ПО – это программы, которые при запуске демонстрируют рекламные баннеры. Они могут проявляться в виде выскакивающих окон или полоски на экране компьютера. Шпионское ПО используется для получения сведений о персональных данных пользователя и передачи их третьей стороне.

Rootkits. Rootkit – это программа, внедряющаяся в операционную систему и перехватывающая команды доступа к файлам на жестком диске, которые другие программы используют для осуществления основных функций. Rootkit маскируется среди ОС и сервисных программ и контролирует все их действия.

DNS Poisoning. Серверы системы доменных имен перенаправляют трафик с нормальных ресурсов на «зараженные», с которых вредоносное и шпионское программное обеспечение скрытно проникает на компьютер жертвы.

Сеть также может стать уязвимой во время расширения или изменения структуры организации. Когда сети становятся более сложными и должны решать больше задач по поддержке и развитию различных видов деловой активности, лучшей защитой от вредоносных атак и растущих уязвимостей может стать мощное, многоуровневое решение безопасности.

Сигнатуры – это только часть решения...

Решения, основанные на сигнатурах, в течение многих лет являются основой арсенала безопасности и используют базу данных известных шаблонов для обнаружения и блокирования вредоносного трафика прежде, чем он попадет внутрь сети. Эти решения обеспечивают защиту против таких угроз и нарушений политики безопасности, как: троянские программы, переполнение буфера, случайное исполнение вредоносного SQL-кода, службы мгновенных сообщений и общения типа «точка – точка» (используемого в Napster, Gnutella и Kazaa).

В то же время после выявления и идентификации предполагаемой угрозы до создания соответствующих файлов сигнатур, доступных для

Рис. 1. Жизненный цикл атаки и окно уязвимости

скачивания, может пройти от нескольких часов до нескольких недель. Этот лаг создает окно уязвимости (рис. 1), в течение которого сети открыты для атаки.

Таким образом, возникает вопрос: что необходимо предпринять, если сигнатуры в одиночку не могут справиться с угрозами? Ответом является – Unified Threat Management. В UTM-устройствах многоуровневая система безопасности работает совместно с решениями, основанными на сигнатурах, и другими службами, обеспечивая мощную, всеобъемлющую защиту от сложных угроз.

ПОЧЕМУ УСТРОЙСТВА НАЗЫВАЮТ UNIFIED THREAT MANAGEMENT?

Финансовая выгода

Интегрированные системы, в отличие от решений многоуровневой безопасности, которые строятся с помощью множества отдельных устройств, используют намного меньше оборудования. Это отражается на итоговой стоимости. Полностью интегрированное решение может включать в себя межсетевой экран, VPN, многоуровневую систему безопасности, антивирусный фильтр, системы предотвращения вторжений и защиты от шпионского ПО, фильтр URL и системы централизованного мониторинга и управления.

Остановка атак на сетевом шлюзе без прерывания рабочего процесса

Многоуровневый подход позволяет избежать катастрофы, блокируя сетевые атаки там, где они пытаются проникнуть в сеть. Вредоносный код не сможет нарушить защиту на уровне рабочей станции или сервера, поскольку уровни производят защиту совместно. Осуществив один раз функцию проверки, те же ресурсы UTM-устройства на следующем уровне повторно не используются. Поэтому скорость трафика не снижается и реагирующие на нее приложения остаются доступными для работы.

Простота установки и использования

Являетесь вы экспертом или новичком в ИТ-технологиях безопасности, интегрированные системы с централизованным управлением позволяют легко формировать, а также управлять устройствами и службами. Это значительно упрощает работу администраторов и снижает операционные расходы.

Возможность с легкостью установить и развернуть системы, используя помощь «мастеров», оптимальные настройки «по умолчанию» и другие автоматизированные средства, снимает многие технические барьеры на пути быстрого создания системы безопасности сети. Система управления наглядно демонстрирует способы отображения сетевой активности. Ясная и лаконичная программа отчетности держит вас в курсе всех событий безопасности, что позволяет быстро определить возможные проблемы и предпринять необходимые предупреждающие или корректирующие шаги.

КАК ВЫГЛЯДЯТ РЕШЕНИЯ UNIFIED THREAT MANAGEMENT?

Чтобы добиться действительно эффективной защиты, которая называется UTM, устройство должно быть активным, интегрированным и многоуровневым и выполнять следующие функции:

- многоуровневая защита в сети;
- антивирусный фильтр, система предотвращения вторжений и защита от шпионского ПО, расположенные на сетевом шлюзе;
- защита от небезопасных URL и спама, зависящая от источника атаки.

Многоуровневая защита

Многоуровневая защита обеспечивает активный и глубокий анализ потока данных и передает информацию о подозрительном трафике различным уровням устройства.

- Обнаружение аномалий протокола – стандарты Интернета применительно к потоку данных используются для определения некорректного трафика и изолирования угроз.
- Анализ поведения – хосты, которые ведут себя подозрительно, обнаруживаются и блокируются.
- Проверка на совпадение шаблонов – опасные файлы, о которых известно, что через них могут распространяться вирусы или атаки, помечаются и удаляются из системы.

Трафик постоянно проверяется на вирусы, черви, шпионское ПО, троянцы и другой нежелательный код, который при обнаружении активно блокируется устройством. В то же время остальной поток данных проходит в сеть, не задерживаясь в нем. При использовании многоуровневой системы безопасности нет необходимости дожидаться доступности файлов сигнатур. Поэтому вы всегда защищены от новых, еще неизвестных атак.

Антивирусы и системы, основанные на сигнатурах

Антивирусные сигнатурные фильтры совместно с другими способами защиты образуют на сетевом шлюзе уровень защиты от угроз, реализуемых через электронную почту. Это вирусы, черви и смешанные угрозы. Опасный трафик, маскирующийся под нормальный, определяется и останавливается в режиме on-line прежде чем сможет внедрить свои вложения и повредить вашу сеть.

Системы защиты от вторжений и шпионского ПО обеспечивают постоянную защиту от известных угроз на уровне сети и приложений. При этом входящий трафик соответствует стандартам, но его содержимое может представлять собой нежелательный код, атакующий системы, используя уязвимости в протоколах и приложениях.

Защита от небезопасных URL и спама

Бесконтрольное перемещение сотрудников компании по web-сайтам увеличивает вероятность подвернуться заражению опасным шпионским ПО, троянскими программами и вирусами. Вдобавок к этому снижается производительность труда, уменьшается пропускная способность сети и может даже случиться, что вашей компании придется отвечать перед законом за допущенные нарушения. Служба URL-фильтрации позволяет наложить запрет на

сайты с небезопасным или нежелательным содержимым. Можно упорядочить доступ к web-ресурсам в зависимости от дня недели, потребностей подразделения или индивидуальных запросов пользователя.

Спам может полностью заполнить почтовый сервер, перегрузить сетевые ресурсы и отрицательно сказаться на производительности труда сотрудников. Он также может являться носителем различных видов опасных атак, включая вирусы, уловки социальной инженерии при использовании web или фишинг. Используя выделенную службу блокирования спама, вы сможете эффективно остановить лишний трафик на сетевом шлюзе, прежде чем он попадет в сеть и нанесет вред.

UTM-УСТРОЙСТВА ОТ WATCHGUARD

Чтобы разобраться, как функционируют UTM-устройства, рассмотрим довольно известные решения производства компании WatchGuard. Из мировых лидеров в производстве и разработке аналогичных устройств сегодня только эта компания имеет на территории России своего дистрибьютора (Rainbow Technologies) и продвигает оборудование на нашем рынке.

Firebox® X и Intelligent Layered Security

Архитектура Intelligent Layered Security (ILS) является сердцевиной линейки UTM-устройств Firebox® X компании WatchGuard® и обеспечивает эффективную защиту для развивающихся предприятий. Используя динамическое взаимодействие между уровнями, ILS обеспечивает безопасность при оптимальной производительности устройства.

Архитектура ILS состоит из шести слоев защиты, взаимодействующих друг с другом (рис. 2). Благодаря этому подозрительный трафик динамически выявляется и блокируется, а нормальный – пропускается внутрь сети. Это позволяет противостоять как известным, так и неизвестным атакам, обеспечивая максимальную защиту при минимальных затратах.

Рассмотрим подробнее каждый уровень.

- «Внешние службы безопасности» предлагают технологии, расширяющие защиту сети за межсетевой экран.
- «Целостность данных» проверяет целостность пакетов и их соответствие протоколам.
- «VPN» проверяет зашифрованные внешние соединения организации.
- Межсетевой экран с динамическим анализом ограничивает трафик от источников до тех пунктов назначения и портов, которые разрешены в соответствии с политикой безопасности.
- «Глубокий анализ приложений» обеспечивает их соответствие уровню приложений модели ISO, отсекает опасные файлы по шаблону или по типу файла, блокирует опасные команды и преобразует данные для избежания утечки.
- «Безопасность содержимого» анализирует и упорядочивает трафик для соответствующего приложения. Примером этого являются технологии, основанные на применении сигнатур, службы блокирования спама и фильтрации URL.

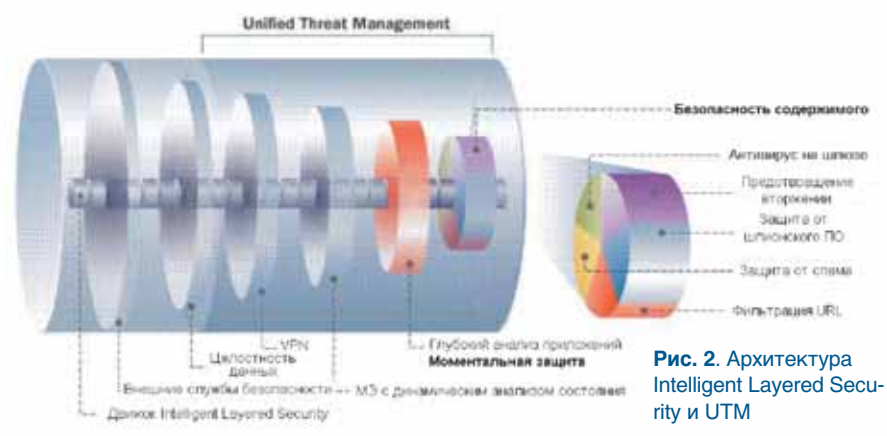

Рис. 2. Архитектура Intelligent Layered Security и UTM

Защита с использованием технологий сигнатур

Антивирус/система предотвращения вторжений на шлюзе является встроенной службой безопасности, основанной на использовании сигнатур. Она в режиме on-line вычисляет и блокирует опасный трафик и код. При использовании в многоуровневой системе безопасности антивируса и системы предотвращения вторжений обеспечивается надежная защита от шпионского ПО, вирусов и опасных приложений.

Встроенное программное обеспечение URL-фильтрации

WebBlocker обеспечивает гибкость в настройке доступа пользователей в Интернет. При его использовании можно снизить загрузку сети, значительно увеличить производительность труда сотрудников и уменьшить возможные угрозы безопасности.

Блокирование спама

SpamBlocker, разработанный компанией WatchGuard, является лучшим решением в области разделения нормального содержимого от спамерских атак. Благодаря ему в режиме on-line блокируется до 97 % нежелательных почтовых сообщений.

ВЫВОДЫ

Объединение и преобразование традиционных средств безопасности в интегрированные UTM-устройства позволяет предприятиям перейти на новый, более высокий уровень защиты своих локальных сетей. Подход компании WatchGuard, основанный на объединении нескольких уровней защиты (ILS; службы, основанные на сигнатурах; фильтрация URL и пр.) в одном устройстве, обеспечивает надежную защиту для любой развивающейся сетевой инфраструктуры. Это особенно важно сегодня, когда с увеличивающейся частотой появляются все более изощренные сетевые угрозы.

Более подробно о решениях WatchGuard, представленных на российском рынке, можно узнать у дистрибьютора – компании Rainbow Technologies (www. rainbow. msk. ru).

Использованные источники

www. sans. org
Информация от компании WatchGuard

(Подготовлено Rainbow Technologies по материалам компании WatchGuard)