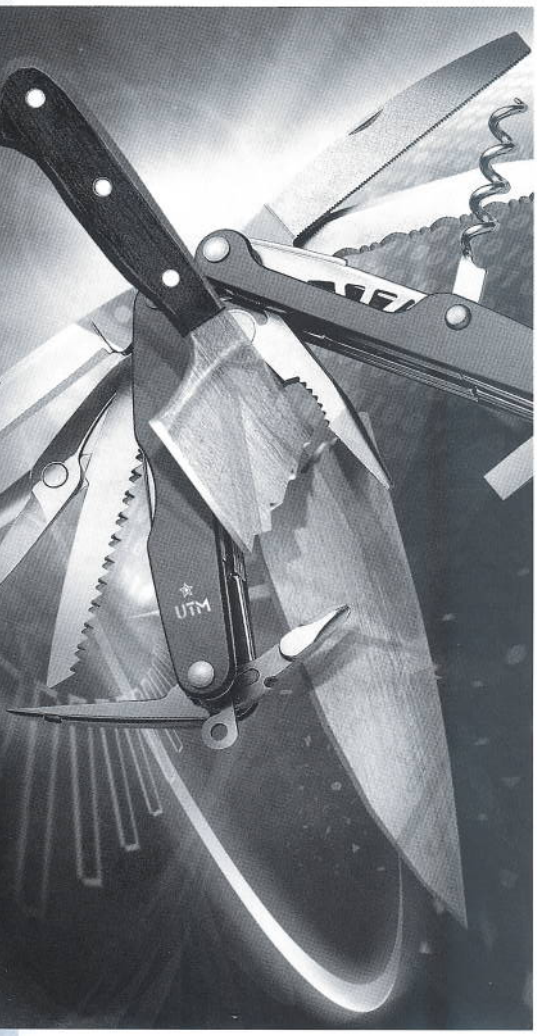
Специализированные устройства против UTM – битва проиграна?

А. В. Комаров, *начальник отдела маркетинга*

Компания SafeLine

Термин UTM (Unified Threat Management – унифицированное управление угрозами) был введен исследовательской компанией IDC для обозначения многофункциональных сетевых устройств, являющихся многоуровневыми системами защиты и способных обезопасить сеть компании от самых различных видов угроз. Первоначально такие продукты содержали минимальный набор функций: межсетевое экранирование, антиспам, антивирус, систему предотвращения/обнаружения вторжений (IDS/IPS), контентную фильтрацию и средства для построения защищенных виртуальных частных сетей (VPN). Современные UTM-устройства позволяют эффективно защищаться от гораздо более широкого спектра угроз и представляют собой более чем великолепную альтернативу традиционным узкоспециализированным решениям.



Бизнес-эффективность

Подавляющее большинство современных компаний ежедневно подвергается многочисленным угрозам, связанным со все большим проникновением всемирной сети Интернет в их бизнес-процессы. Желание упростить и облегчить доступ к информационным ресурсам и системам для клиентов, партнеров и собственных сотрудников неизбежно вступает в противоречие с необходимостью уменьшить риск неавторизованного доступа. Пренебрегающие первым рискуют проиграть конкурентную борьбу, а вторым – потерять ценную информацию и, в конечном итоге, опять-таки долю рынка или даже весь бизнес. Таким образом, необходимость в надежной и эффективной защите от потенциальных угроз сегодня, пожалуй, уже никем не оспаривается, а вот способы и методы построения такой защиты пока еще выбираются разные.

Классический подход предполагает использование набора разных решений для обеспечения защиты от разных угроз. Основным аргументом в его пользу принято считать тезис, что специализированный продукт лучше справляется со своей задачей, чем «многофункциональный комбайн», за счет более узкой направленности и ориентированности всех своих компонентов на конкретный аспект обеспечения безопасности. Однако с учетом нынешнего уровня развития технологий противопоставление качества и универсальности утратило свою актуальность. Подробнее об этом будет рассказано ниже.

Важно заметить, что технические свойства (производительность, надежность и т. д.) для продуктов информационной безопасности крайне важны, но не стоит забывать, что с точки зрения эффективности бизнеса любое внедряемое решение также должно как минимум соответствовать следующим требованиям:

- увеличение эффективности существующих ресурсов и инвестиций;
- уменьшение сложности инфраструктуры безопасности;
- снижение эксплуатационных и капитальных затрат.

Использование единой платформы комплексной безопасности как нельзя лучше соответствует данным требованиям, и, в частности, именно по этой причине UTM-устройства по праву завоевывают популярность у все большего числа клиентов. Рассмотрим оба похода более детально.

Эволюция традиционного подхода

Исторически для комплексной защиты сетей (рис. 1) первыми повсеместно начали использоваться межсетевые экраны. Появляющиеся же со временем все новые и новые угрозы привели к необходимости существенного расширения спектра решений, обеспечивающих сетевую безопасность.

Так, для безопасного удаленного доступа потребовалось внедрение технологий виртуальных частных сетей (VPN), а совершенствование хакерских техник и рост сложности корпоративного программного обеспечения вынудило разработать принципиально новые методы защиты, такие как системы предотвращения/обнаружения вторжений.

Решения по борьбе со спамом и защиты от вирусов в настоящее время также активно используются на периметре сети организации, разгружая ресурсы рабочих станций и серверов и останавливая вредоносный код еще «на пороге».

Усложнение содержимого html-кода web-страниц, тенденция к повсеместному использованию интерактивности и применение скриптовых языков программирования вызвало необходимость внедрения web-фильтров, которые теперь не столько блокируют доступ сотрудников к нежелательным сайтам, сколько активно защищают корпоративные сети от вторжений извне.

Ориентация большинства современных приложений на сетевое взаимодействие выявило потребность

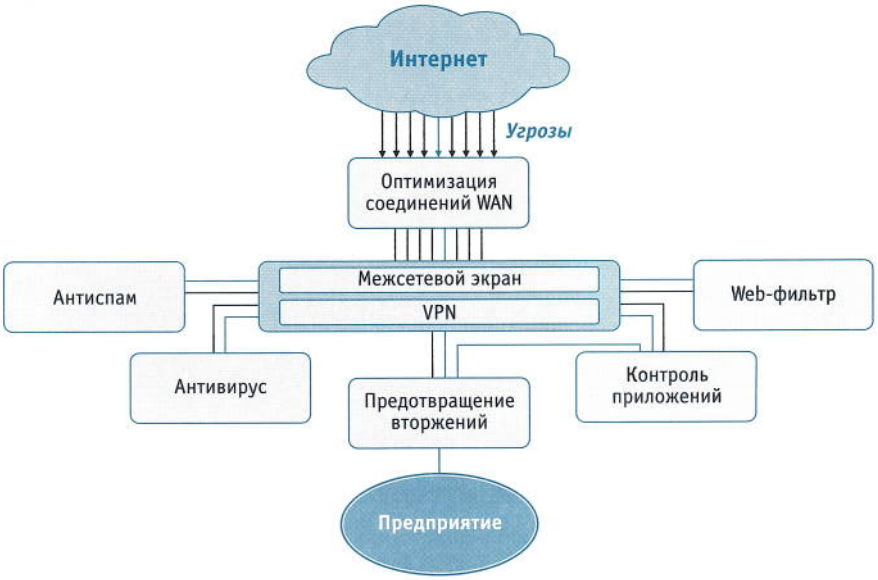


Рис. 1. ***Традиционный подход к защите сети***

в контроле передаваемого ими контента, невидимого классическими средствами межсетевого экранирования.

Наконец, необходимость повышения надежности соединений и эффективности использования пропускной способности канала, напрямую связанная с повышением уровня доступности, толкает компании на установку WAN-оптимизаторов.

На практике продукты для обеспечения информационной безопасности помимо своего основного предназначения, как правило, имеют тот или иной дополнительный функционал. Встраивание элементов системы предотвращения/обнаружения вторжений в межсетевые экраны, контентный анализ с одновременной проверкой на наличие вредоносного кода, комплексная защита электронной почты от спама и вирусов – явления на сегодняшний день вполне обычные. Таким образом, построенная по традиционной схеме система безопасности зачастую имеет множество дублирующих компонентов, что, в частности, снижает быстродействие и увеличивает стоимость.

Можно выделить следующие характерные признаки традиционного подхода:

- использование автономных, не интегрированных между собой средств защиты;
- применение смеси из аппаратных (коробочных) решений и программных продуктов (приложений);
- высокая совокупная стоимость владения за счет дублирования функций;
- сложность внедрения, управления и обслуживания;
- большие эксплуатационные трудозатраты.

Секрет успеха современных UTM-устройств

В противовес традиционному подходу, производители UTM-решений предлагают использование единой комплексной платформы безопасности (рис. 2), объединяющей в себе все функции по обеспечению безопасности.

Вместо постоянного внедрения новых элементов системы защиты, призванных отвечать вновь возникающим угрозам и опасностям, применяется одно-единственное устройство, целиком осуществляющее всесторонний контроль и обеспечивающее безопасность сразу на всех уровнях.

Огромным экономическим плюсом от такого подхода является снижение издержек на содержание парка различных устройств, для обслуживания которых требуется штат квалифицированных специалистов. Не секрет, что даже при несложной процедуре конфигурации самих устройств по отдельности основные проблемы внедрения и последующего использования решений от нескольких вендоров возникают как

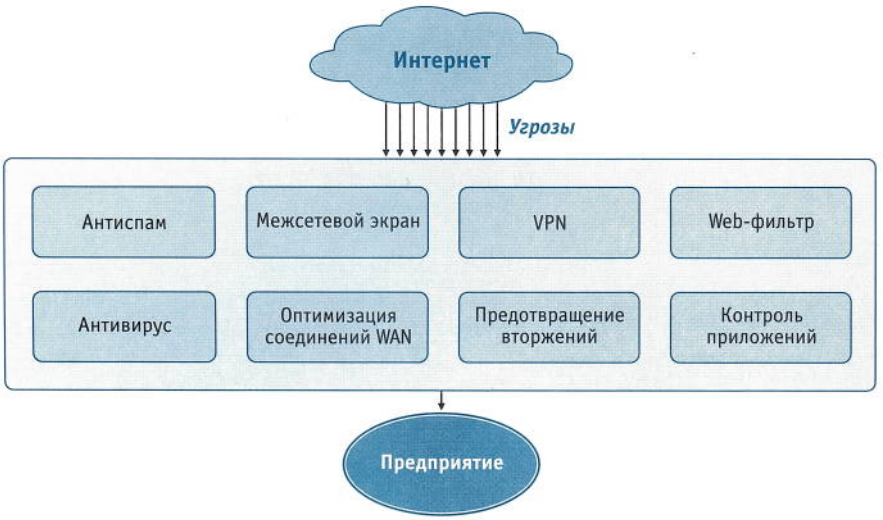


Рис. 2. ***Защита сети с помощью UTM-устройства***

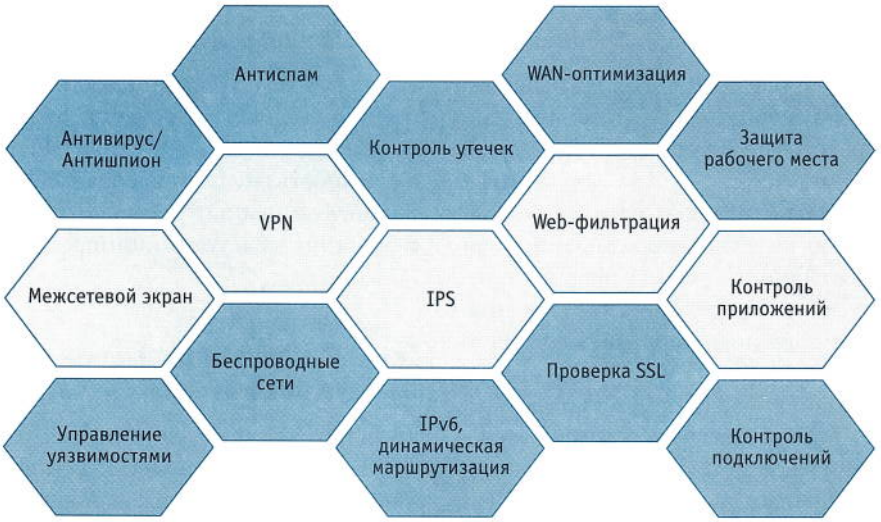


Рис. 3. ***Функционал UTM-устройства***

раз при настройке их взаимодействия между собой. Различная логика подхода производителей к построению систем управления, корреляции событий, анализа и отчетности еще больше затрудняет конфигурирование и требует от специалистов дополнительных знаний и практических навыков. Использование UTM-устройств снимает необходимость конфигурации взаимодействия различных компонентов защиты между собой, так как это уже сделано самим вендором, причем оптимальным образом.

Столь тесная интеграция средств защиты между собой позволяет более эффективно бороться с угрозами, поскольку результаты проверок могут в полном объеме использоваться на последующих уровнях для достижения максимально глубокого анализа сетевого трафика. Таким образом, комбинация и корреляция подсистем, работающих на одном устройстве, существенно повышает общий уровень обеспечиваемой безопасности.

Ключевыми признаками данного подхода к построению системы безопасности являются:

- интегрированные сервисы безопасности;
- использование специализированных платформ и высокая общая производительность;
- низкая совокупная стоимость владения;
- простота внедрения, управления и эксплуатации.

Тенденция к расширению функционала классических устройств сетевой безопасности, о которой уже говорилось выше, достаточно ярко свидетельствует о том, что подход, предложенный производителями UTM-устройств, действительно эффективен.

Принципиально нужно отметить, что просто оснастить устройство дополнительными модулями или подсистемами, приближающими его к «чистокровным» UTM, не достаточно. Такая реализация будет иметь низкие показатели как производительности, так и обеспечиваемого уровня безопасности. Для того чтобы быть настоящим UTM, необходимо изначально быть спроектированным и построенным как UTM.

Важной особенностью UTM-устройств является использование при их построении специально разработанных аппаратных платформ, дополнительных ускоряющих анализ и обработку сетевого трафика процессоров (ASIC) и специализированной операционной системы, тонко оптимизированной под специфические требования всего решения.

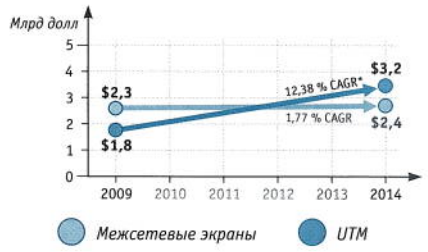
Именно появление таких новых платформ и обусловливает текущую тенденцию к вытеснению целого полка отдельных специализированных устройств у все большего круга компаний.

Тенденции

Наряду с термином UTM можно встретить такое понятие, как Next Generation Firewall (NGFW – межсетевые экраны нового поколения), используемое, в частности, компанией Gartner. По своей сути NGFW являются подмножеством UTM-устройств, так как обычно предоставляют существенно более ограниченный набор функций.

Помимо уже упоминавшихся выше классических средств защиты (межсетевой экран, VPN, IPS/IDS, web-фильтрация и пр.), UTM-устройства лидеров этого рынка предлагают все больше и больше дополнительных функций (рис. 3), реализуемых на базе единого устройства: предотвращение утечек информации, контроль и управление уязвимостями, анализ шифрованного SSL-трафика, контроль подключений, безопасность беспроводных сетей и многое другое.

Оценив рыночные перспективы UTM-устройств, исследовательская



* CAGR – совокупный среднегодовой темп роста (Compound Annual Growth Rate)

Рис. 4. ***Прогноз изменения объемов рынков UTM-устройств и межсетевых экранов с VPN***

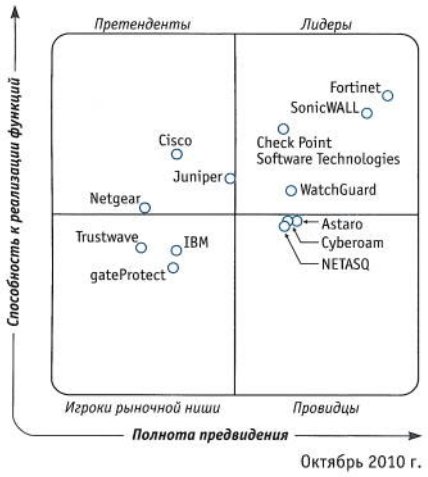


Рис. 5. ***Магический квадрат Gartner для UTM-устройств***

компания IDC в 2010 году выпустила отчет «Worldwide Network Security 2009-2014 Forecast and 2009 Vendor Shares» (рис. 4), согласно которому в 2009 году объем рынка классических межсетвых экранов составил 2,3 млрд долларов, а UTM-устройств не намного меньше – около 1,8 млрд долларов. При этом совокупный среднегодовой темп роста (CAGR) оценивается специалистами компаний как 1,77 % и 12,38 % соответсвенно, что, по их мнению, обеспечит существенный рост рынка UTM-решений в течение нескольких последующих лет.

В заключение приведем магический квадрат Gartner «Magic Quadrant for Unified Threat Management» (рис. 5) от октября 2010 года, наглядно показывающий текущую расстановку сил в сегменте UTM-устройств между компаниями, изначально ориентировавшихся на традиционный подход, и вендоров, избравших путь унификации управления угроз в качестве своей основной бизнес-модели.

Российская прописка инновационного решения Cisco

С 24 мая по 20 июля в 12 городах России (Астрахани, Владивостоке, Казани, Краснодаре, Красноярске, Москве, Омске, Самаре, Санкт-Петербурге, Тюмени, Челябинске и Ханты-Мансийске) прошло road show «Российская криптография в решениях Cisco».

Масштабное мероприятие, организуемое корпорацией Cisco Systems совместно с ее технологическим партнером – компанией «С-Терра СиЭсПи», состоялось на базе и при технической поддержке Сетевых академий Cisco. Это уже второе road show, которое проводится в рамках программы Cisco Expo Learning Club – самого крупномасштабного института повышения квалификации ИТ-специалистов, действующего на территории СНГ.

Основная цель предстоящего мероприятия состояла в том, чтобы познакомить участников с инновационным аппаратным VPN-модулем – первым устройством, производимым в России по лицензии Cisco с использованием многоуровневой высокотехнологичной цепочки поставок, в которую входят российские партнеры Cisco. Речь идет о VPN-модуле NME-RVPN в исполнении MCM (модуль сетевой модернизированный). Российским организациям самых разных типов все чаще требуются решения для обеспечения надежных коммуникаций внутри организации, для связи с филиалами и мобильными сотрудниками. Чтобы повысить эффективность работы и гибкость рабочих процессов, удаленным сотрудникам необходимо предоставлять доступ во внутреннюю сеть и к внутренним приложениям, соблюдая при этом конфиденциальность и целостность передаваемой информации. Упомянутый VPN-модуль дает заказчикам возможность защищать конфиденциальную информацию, персональные данные, финансовые транзакции и данные других типов, а маршрутизаторы Cisco, оборудованные таким устройством, могут использоваться для создания географически распределенных сетей.

VPN-модуль Cisco производится в России в соответствии с согласованным с ФСБ России «Порядком организации производства изделия „Модуль сетевой модернизированный (MCM)" в рамках подконтрольного технологического процесса на территории Российской Федерации» и сертифицирован ФСБ России и ФСТЭК России. Таким образом, он соответствует всем требованиям российского законодательства в области криптографической защиты.

В компании особо отмечают уникально высокую степень локализации этого производства: на территории России будет осуществляться как монтаж печатных плат, так и финишная сборка и тестирование. Серийный выпуск оборудования Cisco будет осуществляться на мощностях ООО «ПК Альтоника», которое инвестировало существенные средства как в новое оборудование, так и в систему организации производства, чтобы они соответствовали строгим требованиям мирового уровня, которые предъявляет новый заказчик.

В программу прошедших семинаров входил ряд презентаций специалистов Cisco и «С-Терра СиЭсПи», а также лабораторные работы. На лабораторном стенде было представлено решение, работающее с программным обеспечением шлюза безопасности CSP VPN Gate 3.1. Оно сертифицировано в соответствии с требованиями ФСТЭК России и ФСБ России к устройствам криптографической защиты информации (СКЗИ КС1, КС2), что позволяет использовать его в государственных организациях и органах власти, в том числе и для защиты информационных систем персональных данных (ИСПДн) до класса К1.

Кроме того, в компании «С-Терра СиЭсПи» подчеркнули, что демонстрируемое решение из разряда «все на одном шасси», так как оно в полной мере использует функционал маршрутизаторов Cisco ISR G2, позволяя не только решить вопросы, связанные с требованиями российских регуляторов, но и при этом существенно сократить расходы.