IPSec умер?!
Да здравствует SSL!

Корпоративная сетевая инфраструктура становится все более сложной, требующей для обеспечения ее информационной безопасности перехода на более современные методы шифрования трафика, персонификации пользователей и управления конечными устройствами. Тема публикации – особенности нового класса защищенных сетей – SSL VPN – в сравнении с распространенными сейчас – IPSec VPN, а также краткий обзор состояния рынка SSL VPN.

Введение

Традиционно для обеспечения доступа к корпоративным серверам и ресурсам использовались сети IPSec VPN. Для связи между сайтами IPSec остается пока единственным приемлемым решением, но для соединений типа client-to-enterprise использование IPSec в последнее время резко сокращается. Прежде всего, это происходит из-за необходимости развертывания большого числа экземпляров клиентского IPSec ПО, что стало ограничивающим фактором масштабируемости этого типа сетей по количеству поддерживаемых клиентов. К этому добавляется еще и то, что IPSec-туннелирование не позволяет полностью исключить возможность непосредственного вторжения в сеть "сомнительных" устройств, "пробивших бреши" в системе сетевой защиты.

При использовании сетей SSL VPNs, в отличие от IPSec, нет необходимости вообще в установке какого-либо клиентского ПО, не говоря уже о его поддержке. Это не только сокращает затраты на IT-персонал, но и снимает какие-либо ограничения на подключение удаленных клиентов – публичные интернет-киоски, партнерские сайты, ноутбуки и т.д. Что еще более важно, при использовании SSL VPN нет никакого открытого туннеля в соединении client-to-enterprise. SSL VPNs определяет политику защиты по каждому подключению, разрешая доступ только к определенным ресурсам, на основании установленного профиля доступа для конкретного пользователя, его местоположении и данных о том устройстве, с которого осуществляется доступ (наличие антивируса, файервола, обновлений и т.д.). И как с любой хорошо управляемой защитой – все запрещено, если не разрешено администратором.

В соответствии с прогнозами IDC, количество мобильных и удаленных работающих пользователей к концу 2006 г. вырастет до более чем 150 млн. Это предъявляет гораздо более жесткие требования к безопасности подключения. Время, когда вручную прописывались условия для каждого типа соединения, безвозвратно уходит. На смену приходят решения, обеспечивающие полную автоматизацию условий подключения и защиту критических ресурсов для любых групп пользователей, независимо от места их соединения.

По данным исследования Forrester-Reserch, 2005 г.:

- ✔ В **2008** г. SSL VPN "де-факто" займет большую часть рынка как защищенный стандарт при удаленном доступе
- ✔ **44%** американского бизнеса уже имеют развернутые SSL VPNs
- ✔ **$97 млн** было потрачено на технологию SSL VPN в 2003 г.
- ✔ **$1,2 млрд** было потрачено на технологию SSL VPN в 2004 г.

Интерес к рынку SSL VPN резко возрос за последние 3 года. Это было "подогрето" и прогнозом Frost & Sullivan, в соответствии с которым рынок SSL VPN ежегодно увеличивается на 49% и к 2010 г. его объем превысит более $2,46 млрд.

Почему такой интерес к SSL VPN? Во-первых, как уже отмечалось, SSL VPN, давая возможность подключения по интернету (через 443 TCP-порт), предоставляет пользователям использовать любой web-браузер вместо того, чтобы требовать установленного клиентского ПО, как в случае с IPsec. При этом уровень сетевой защиты не сокращается. SSL VPNs может преодолевать системы сетевой защиты и управлять NAT (network address translation – трансляция сетевого адреса). IPsec VPNs может управлять NAT, используя дополнительную компоненту IKE (Internet Key Exchange) версии 2 и добавляя еще некоторый уровень сложности. Кроме того, с SSL VPNs доступ происходит на уровне приложений, допуская поэтапное управление и являясь при этом высокомасштабируемым решением.

Однако, несмотря на существенные отличия, IPsec и SSL могут успешно сосуществовать и SSL может развиваться параллельно, сохраняя инвестиции в IPsec. Фактически IPsec VPNs является идеальным решением для долгосрочных, статических соединений между удаленными сайтами, а также для управляемого способа предоставить небольшим группам пользователей безопасный удаленный доступ. В свою очередь, SSL VPN – основной выбор для обеспечения доступа большого числа мобильных служащих в extranet-среде.

Эксперты группы компаний ЛАНИТ всегда внимательно следят за тенденциями рынка информационной безопасности. ЛАНИТ одним из первых предложил своим клиентам решения ведущих и надежных производителей, основанные на использовании технологии SSL VPN. Сегодня ЛАНИТ решает для своих клиентов весь комплекс задач, связанных с внедрением

подобных решений, включая разработку и реализацию политик доступа для различных групп пользователей. Специалисты ЛАНИТ делятся своим опытом и рассказывают о том, какая ситуация сегодня складывается на российском рынке решений SSL VPN, и какие игроки на нем присутствуют.

Особенности SSL VPN

Многие из продуктов, которые появляются на рынке SSL VPN, – по сути разработки уже в третьем поколении и, как технические решения, достигли определенной технологической зрелости. Основные характеристики, которыми они отличаются друг от друга: способ реализации политики защиты; способ управления удаленными конечными устройствами и степень "прозрачности" используемых технологий для конечного пользователя.

Степень детализации политик доступа в SSL VPN позволяет администраторам осуществлять доступ не только на основании того, что (какая информация) загружается, но также и откуда она загружается. Кроме того, каждое SSL-устройство может самостоятельно поддерживать некоторое ПО защиты "конечной точки" (которое также имеет отличительные особенности в зависимости от вендора). Данное ПО анализирует доступные ему параметры клиентского устройства, определяет уровень его защищенности и применяет к нему права доступа, основанные на предопределенных "трастовых зонах". Например, данное ПО может обнаружить, что на пользовательском ноутбуке установлено антивирусное ПО и личная система сетевой защиты. В этом случае пользователь напрямую (через Wi-Fi) осуществляет соединение, а SSL-устройство только предоставляет proxy-доступ, а не полный сетевой доступ по IPSec-style уровня 3 туннелю. В настоящее время не существует никакого широко распространившегося стандарта для управления защиты "конечной точки", но такие компании, как Cisco и Microsoft, в ближайшее время должны изменить эту ситуацию.

Вне зоны управления доступом все SSL-устройства используют дополнительные меры защиты. Они поддерживают "безопасный просмотр" на основе клиентов типа Symantec Sygate Secure Desktop. Эти клиенты создают виртуальные sandboxes, в которых выполняются SSL-сессии. Когда пользователь закрывает безопасный браузер, его временные файлы и информация сеанса помещаются в binary black hole. К тому же, большинство SSL VPNs включает ПО, чистящее кэш, которое вычищает следы пользователя (временные файлы, cookies и другую информацию сеанса от браузера). Эти меры

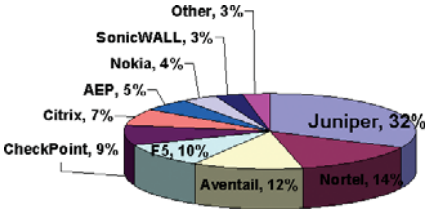

Рис. 1. Распределение долей рынка между основными производителями SSL VPN оборудования по региону Северная Америка.

Ист.: Gartner (December 2005).

Рис. 2. "Магический квадрат" Gartner – производителей SSL VPN оборудования по региону Северная Америка по итогам 3 кв. 2005 г.

очень важны для пользователей, соединяющихся с помощью публично доступных PC, но они не столь же эффективны, как использование безопасного браузера, потому что удаленные файлы чаще всего можно восстановить.

Другие особенности, которые также интересны, включают поддержку VLAN и кластеризацию. VLANs позволяют сегрегировать трафик на одной и той же физической сети – удобная особенность для сервис-провайдеров или больших компаний. Кластеризация дает возможность SSL VPN устройствам поддерживать высокую доступность за счет автоматических средств восстановления после сбоев/отказов и балансировки загрузки, а также может расширять до тысяч число параллельно работающих пользователей, поддерживаемых SSL-устройством.

Средняя рыночная (мировая) цена одного устройства SSL VPNs в пересчете на одного пользователя и при 500 параллельно работающих колеблется в диапазоне от $50–120. Также, хотя каждый продукт предлагает некоторый уровень проверки хост-целостности, он часто ограничен. При расширенной функциональности SSL-устройство включает защиту конечной точки типа Symantec Sygate OnDemand или Symantec WholeSecurity Confidence Online Enterprise Edition.

Основные игроки на рынке устройств для SSL VPN на конец 3 кв. 2005 г. и распределение рынка между производителями по региону Северная Америка представлены на рис. 1, 2.

Что хотят пользователи?

Удаленные пользователи нуждаются в доступе ко многим приложениям, которые не доступны по web, включая те, которые используют общие почтовые протоколы типа SMTP, POP3 и MAPI, а также к удаленным программным оболочкам, подобно telnet и VNC. Этот доступ требует удаленной поддержки компьютеров и вызывает сетевые проблемы. Типичные VPNs как IPsec и SSL позволяют запрещать внешний доступ к таким приложениям или использовать технологию кодирования, чтобы защитить трафик, передающийся по неконтролируемым сетям.

Утверждение, что SSL является бесклиентской сетью правильно только частично. Обеспечение доступа к не-web-приложениям требует клиентской программы или того, что загружается на компьютер удаленного пользователя как элемент управления ActiveX или Java-аплет, который переадресовывает сетевой трафик от его предназначенного адресата на SSL VPN шлюз. Таким образом, требуется ActiveX или Java-поддержка наряду с установленными привилегиями для их выполнения.

Ожидалось, что SSL-продукты поддержат существующие Active Directory (AD) и RSA ACE/Server для идентификации, но реальность преподнесла несколько неожиданностей. Идентификация вместо AD была реализована через Microsoft NTLM (NT LanMan) или через LDAP. Идентификация вместо ACE/Server, используя SecurID-маркеры, была реализована через "родной" ACE-клиент или RADIUS. Удивительно, системы от Caymas и Check Point не поддерживают NTLM и Permeo Base5, используя внедренную конфигурацию RADIUS/AD.

Как только пользователь достигает безопасного соединения, он должен быть "связан" ограничениями доступа. Все протестированные продукты обеспечили основные функциональные возможности, используя членство в группе и идентификацию. Но, что касалось управления доступом в части степени детализации (на основе предопределенных переменных, таких, как IP-адреса – источник или назначение, URL, имя пользователя или членство в группе, время дня и другие элементы, касающиеся сеанса), показало отличие многих продуктов. Так, устройства от Juniper и Nortel действительно обеспечивали эту функциональность. Наоборот, система от Check Point не поддерживала варианты доступа по времени дня, а Check Point Connectra 6000 не поддерживала еще IP-адрес.

Обзор рынка SSL VPNs

Участники данного обзора были выбраны не случайно. Хотя не трудно заметить, что на мировом рынке, даже в числе лидеров отрасли SSL VPN, тот же Gartner предлагает нашему вниманию другие имена, реалии нашего российского рынка диктуют нам свои предпочтения. Выбранные производители и их решения – это весомые и ощутимые игроки российского рынка Information Security. ЛАНИТ с ними знакомы давно и, может быть, для кого-то эти производители выступят в новом амплуа, демонстрируя свои успехи в области SSL VPN решений.

Juniper Networks Secure Access 5000 с IVE 5.0

Устройство SA-5000 работает на платформе Juniper Instant Virtual Extranet. Продукт имеет хорошо продуманный дизайн и предлагает большое число вариантов конфигурации – от сетевой инсталляции или предустановленных проверок аутотентификации до портального дизайна. Имеется очень большое число параметров для идентификации пользователя или группы, что дает возможность реализации любой методологии для центра данных и неоспоримые преимущества в сравнении с другими продуктами в этой части. Расширения в рамках концепции Juniper End Point Defense Initiative (JEDI), вместе с возможно-

стью создания поэтапного доступа на основе политик, дают большие возможности. Одна из самых интересных особенностей этой версии продукта – Network Connect – загружаемый агент с особенностью двойного режима, который может переключать транспортные режимы между IPsec и SSL автоматически.

Только продукты от Juniper и Array требовали частичную начальную инициализацию (используя порт консоли). В обоих случаях это требовало соединения с последовательным портом для начальной конфигурации внутреннего порта. Как только это было сделано, можно было конфигурировать все остальное через web-интерфейс. Все другие протестированные продукты уже имели встроенный порт управления с определенным IP-адресом или соединение для инициализации через eth0-порт, используя устройство в той же самой сети.

Чтобы подключить AD-сервер, необходимо было "кликнуть" на "Authorization Servers" -> "Active Directory" -> "Новый Сервер" и затем вводились имя, IP-адрес сервера и NT-домен, что не вызывало сложностей. Массив также имеет простой метод для соединения с AD.

Далее создавались две роли: "telecommuter" – для тех, кто регистрируется с известных IP-адресов, и "киоска" – для остальных. Для "telecommuter" ограничивался доступ к разделяемым web- и Windows-файлам и e-mail. После определения ролей устанавливались ограничения, основанные на исходном IP, цифровых атрибутах сертификата, политике проверки хоста, типе браузера, ОС, дне/времени недели и внутреннем/внешнем интерфейсе. Политика проверки хоста давала возможность выполнить сканирование удаленной системы перед идентификацией, например, можно было определить, что PC должен выполнять антивирусное ПО, являются ли конкретные порты открытыми, а также проверить определенный файл или выполняемый процесс.

Конфигурирование политик проверки хоста на SA-5000 было простым, но "check-box" опции были ограничены Symantec Sygate Universal Enforcement API, Symantec Sygate Security Agent, Zone Labs ZoneAlarm Pro и Zone Labs Integrity, McAfee Desktop Firewall 8.0 и InfoExpress CyberGatekeeper Agent. Также было возможно конфигурирование правил предоставления или отказа в доступе на основании выполнения определенного процесса, наличия открытых портов или присутствия файлов (например, было установлено правило пользователей "киоска", которое запрещает доступ, если 80-й порт является открытым).

Далее, роли "telecommuter" (удаленного сотрудника) и "киоска" были уточнены на основе использования правил, таких как: имя пользователя, атрибуты пользователя и "пользовательское выражение" (custom expression). Последние позволяют назначать пользователей на различные роли, основываясь на атрибуте местоположения в пределах AD. Например, можно создать "правило отображения" (mapping rule), которое назначает роль пользователя "киоска" тем, которые используют Internet Explorer, и роль удаленного сотрудника – всем другим.

Области определяют, к какому URL пользователь обращается в течение регистрации. Например, чтобы разрешить OWA (Outlook Web Access) соединения, конфигурируется новая регистрация URL/exchange. Администратор также может добавить закладку или URL-ссылку к портальной странице для определенных пользователей. Совместное использование файлов (Windows/NFS) определяется подобным же способом. Также расширяется и IVE-портал. Например, можно управлять форматом новых закладок панели – в виде одной или двух колонок.

Тем компаниям, которые пытаются устранить любые варианты удаленной комбинации web-сервисов, сервисов по общему использованию файлов, а также telnet-сервисов для пользователей Apple Macintosh OS 10.4 и/или Sun Solaris 8/9, решение SA-5000 позволяет это обеспечить. Также пользователи могут выполнять клиент-серверные приложения через SA-5000, не устанавливая VPN клиента, использующего JSAM (Juniper Secure Application Manager), но это требует лицензии. Например, можно создать роль "Макинтоша" для тех, кто зарегистрируются с известного IP-адреса. После создания роли назначаются права доступа к telnet к Extreme коммутатору и соотнести эту роль с правилом идентификации к AD-серверу.

Nortel Networks Nortel VPN Gateway 3070 5.0

Nortel 3070 – корпоративного класса SSL VPN устройство, которое обеспечивает и IPsec и SSL VPN поддержку в одном блоке.

Nortel предлагает 3 безопасных варианта доступа: бесклиентский (clientless), усовершенствованный бесклиентский и Net Direct. Режим clientless использует браузер для доступа к web-приложениям и файлам. Усовершенствованный clientless-режим требует Java-port-forwarding для доступа к неweb TCP-приложениям. При выходе из системы, Java-агент деинсталлируется с "машины" клиента. В режиме Net Direct загружается ActiveX-агент (только для Windows-платформ), который обеспечивает устройству пользователя полный сетевой доступ, сам агент удаляется с клиентского ПК при выходе из системы. Этот режим предусматривает полный двунаправленный трафик TCP и поддерживает как полное, так и split-туннелирование.

Основной интерфейс (подобный Windows Explorer), предлагает 3 уровня для работы: Setup, Normal и Expert. Гарантию целостности установок SSL VPN можно обеспечить за счет блокировки GUI при проведении изменений (возможность блокировки VPN – параметр профиля пользователя). Эта особенность отсутствовала на большинстве протестированных SSL VPN. В устройствах Juniper и Caymas предлагался только уровень доступа администратора. Конфигурирование связности (connectivity) к AD-серверу требовало установок в профиле пользователя, что являлось частью Schema Admin группы. Nortel действительно обеспечивает опцию подтверждения подлинности. При работе в режимах Expert/VPN Gateways/Auth Order можно видеть доступные методы идентификации и затем выбирать соответствующий.

Пользователи отображаются в одной или более группах доступа, и правила доступа, связанные с группой, определяют права доступа пользователя на интранет. Один из трех пользовательских типов определяет, какая портальная позиция будет отображена: для "новичка" – позиция "home"; для "среднего" добавляются позиции Files и Access (если допускается); для "профи" высвечиваются все позиции. При определении портального набора связей пользователь будет видеть только текст связи, а не его URL.

Защита конечной точки как для SSL, так и для IPsec VPNs, основана на приложении Nortel Tunnel Guard (туннельная защита). При инициировании опции для создания правил защиты была представлена системная конфигурация устройства, из которой была возможность выбрать опцию, позволяющую обеспечивать гранулированные AND/OR выражения для выбора компонент и выполняемых программ, которые являются или активными, или выполняющимися на удаленном компьютере. Например, для тестируемого компьютера, выполняющего Symantec Corporate Edition 10, можно привязать политику конечной точки к антивирусному ПО. Также, например, можно захватить информацию от другого устройства в сети, чтобы добавить ее к нашей политике конечной точки. Однако можно ограничиться и встроенными списками, объединенными с возможностью для администратора добавлять собственные процедуры проверки целостности без необходимости пересылки информации от другой машины.

Функции посредничества позволяют разрешить или запретить доступ к ограниченному сайту. После завершения сессии в этом случае "чистильщик" кэша удаляет proxy-загрузки и временные файлы.

Check Point Software Technologies Connectra Web Security Gateway

Check Point старается усилить свою позицию как тяжеловеса в области сетевой защиты, чтобы увеличить свою долю на рынке SSL VPN. Хотя ряд добавленных в версии 2.0 Connectra особенностей типа – очистка кэша, кодирование данных сеанса и проверка хост-целостности конечной точки – быстро становятся стандартными, ряд функционала отсутствует. Так, Connectra не имеет детального управления доступом, и Check Point не поддерживает идентификацию через ActivCard Pack или Windows Domain Login (NTLM).

Административный интерфейс не загружен вариантами. Connectra предлагает 2 режима удаленного доступа: "естественный" (native) доступ к web-приложениям, разделяемым файлам/электронной почте и TCP-, UDP- или ICMP-сервисы через Check Point SSL Network Extender Active-X-based VPN клиента. "Check-box" опция позволяет задать разрешение запуска SSL Network Extender автоматически или нет.

По умолчанию, опция для использования Integrity Secure Browser, который шифрует "следы" сеанса на удаленной

конечной точке и удаляет все на выходе из системы, выключена. Но даже после того, как эта опция активировалась, пользователям все равно предлагается использовать этот безопасный браузер, и требуются достаточно профессиональные усилия для его активизации.

Тестирование было проведено с различными браузерами. Выяснилось, что web-приложения типа OWA работают с Internet Explorer, Mozilla Firefox и Apple Safari, однако, совместное использование файлов и сервисов на основе SSL Network Extender (расширитель сети SSL) требует последней версии Internet Explorer на удаленном клиенте. Работа с более поздней версией IE (5.0) была невозможна.

Connectra имеет встроенную защиту против DoS-атак; возможности системы сетевой защиты предоставить или запретить подключение с портами для определенных услуг, а также встроенный интеллект уровня приложений для защиты файлов Microsoft и ресурсов печати от саморазмножающегося вируса, подобно Nimda и opaserv. Есть также защита для DNS (UDP Protocol Enforcement).

Средства защиты конечной точки используют Check Point Zone Labs технологию, которые при тестировании демонстрировали детальность и перестраиваемую конфигурацию. Можно было выбрать антивирусные правила и "malware"-поведение, а также проверить для клиента целостность системы сетевой защиты. Администратор может расширить возможности перепосредничества, добавляя текст пользователя или адресуя попытку обращения к определенному URL.

При включенной опции Integrity Clientless Security для Connectra не поддерживалась (на Macintosh) версия браузера Safari 2.0. То же самое было и для Linux клиента, выполняющего Mozilla's Firefox 1.0.3. Также отсутствуют возможности добавления каких-либо пользовательских проверок. Для проверок хост-целостности можно использовать только ZoneLabs Integrity. Некоторые трудности были и с AD-интеграцией.

К плюсам устройства можно отнести поддержку для Citrix и Lotus iNotes и то, что SSL Extender поддерживает TCP-приложения, дополнительный язык и статистику в реальном масштабе времени.

Citrix Access Gateway 4.0

Access Gateway – дополнительный модуль устройства корпоративного класса, на своей аппаратной платформе – Citrix Access Suite. Это относительно новая линейка устройств от Citrix, на которую возлагаются большие надежды, как на сильного игрока на рынке SSL VPN.

Весь стандартный уже сейчас функционал подобных устройств, конечно, присутствует. А именно: кодирование сеансов связи, очистка кэша, проверка конечной точки доступа. Помимо прочего, стоит отметить возможность сокрытия IP-адресов и DNS-имен. В случае разрыва сеанса связи устройство может автоматически переподключаться и восстанавливать рабочие сессии. Как и некоторые его "коллеги", это устройство поддерживает как полное, так и Split-тунеллирование.

Табл. 1. Сравнение VPN SSL от пяти производителей.

	Citrix	Juniper Networks	Herrtel	Symantec	CheckPoint
Наименование продукта	Citrix Access Gateway	Netscreen Secure Access Series	VPN Gateway 30x0	Symantec Gateway Security 5600 Series	Connectra
Тип продукта	SSL VPN Gateway Appliance	Hybrid VPN Gateway Appliance	Multi-Function Hybrid VPN Gateway Appliance	Multi-Function Secure Access Gateway (Hybrid)	Secure Access Gateway (SSL) Appliance & Software
Позиционирование вендора	SSL VPN Appliance	SSL VPN Appliance	SSL VPN Appliance	Multi-Function Security Appliance	Web Security Gateway
Возможные типы VPN					
SSL Remote/Local Access	Да	Да	Да	Да	Да
IPSec Remote/Local Access	Нет	Да	Да	Да	
IPSec Site-to-Site Protection	Нет		Да	Да	
Способы доступа к ресурсам (с помощью SSL если не указано другое)					
Web Applications	L2 Net Connector (at client)	HTTP Proxy/URL Rewriter	HTTP Proxy/URL Rewriter	HTTP Proxy/URL Rewriter	HTTP Proxy/URL Rewriter
Client-Server	L2 Net Connector (at client)	Port Forwarder	Port Forwarder	Port Forwarder	Application & Level 3 Net Connector
Terminal-Server	L2 Net Connector (at client)	Port Forwarder	Port Forwarder	Port Forwarder	Application & Level 3 Net Connector
Full Net Access	L2 Net Connector (at client)	Level 3 Net Connector	Level 3 Net Connector	Level 3 Net Connector	Level 3 Net Connector
Поддержка Методов Доступа SSL для конечных устройств (Web/Client-Server/Terminal Server/Full Net Access) Важно: Да/Нет/Нет/Да указывает на то, что это осуществляется стандартными средствами; специальные агенты для клиент-серверных приложений не используются					
Windows XP	Нет/Нет/Нет/Да	Да/Да/Да/Да	Да/Да/Да/Да	Да/Да/Да/Да	Да/Да/Да/Да
Linux	Нет/Нет/Нет/Нет	Да/Да/Да/Да	Да/Нет/Нет/Нет	Да/Нет/Нет/Нет	Да/Да/Да/Да
Macintosh	Нет/Нет/Нет/Нет	Да/Да/Да/Да	Да/Нет/Нет/Нет	Да/Нет/Нет/Нет	Да/Нет/Нет/Нет
Unix	Нет/Нет/Нет/Нет	Да/Да/Да/Да	Да/Нет/Нет/Нет	Да/Нет/Нет/Нет	Да/Да/Да/Да
Other		Pocket PC: Да/Да/Да/Да	Pocket PC: Да/Да/Да/Да	Pocket PC: Да/Нет/Нет/Нет	
Клиентское шлюзовое ПО					
Browser	IE, FireFox	IE, FireFox, Navigator, Safari	IE, FireFox, Navigator, Safari	IE, FireFox, Navigator, Safari	IE, FireFox, Navigator, Safari
ActiveX or Java Agent	ActiveX	ActiveX & Java.	ActiveX (IE Only)	ActiveX (IE Only)	ActiveX - App Conn. Java - App & Net Conn.
Proprietary Security Client	Да	Level 3 Net Connector		Level 3 Net Connector	Level 3 Net Connector (SSL)
Шлюзовой пользовательский интерфейс					
Web Portal	Нет	Да	Да	Да	Да
Native Application Clients	Да	Да	Да		Application & Level 3 Net Connector
Детальность политики авторизации					
Applications & File Servers	Да	Да	Да	Да	Да
Subnetworks	Да	Да	Да	Да	Да
Web Pages (URLs)	Да	Да	Да	Да	Да
Identity-based Granular Access Control		Да	Да	Да	Да
Предустановленная защита конечной точки доступа					
Session-level Security	Да	Да	Да	TBD	Да
Compliance Enforcemen	TBD	Да	Да	Symantec Anti-Virus Only	Да
Personal Security Software	Нет			Personal FW, Anti-Virus, Spyware Protection	Spyware/malicious code protection (IE only)
Device OS Controls					
Встроенная защита периметра					
Network Firewall	Нет		Да	Да	Да
IDS/IPS	Нет			Да	Да
Web (HTTP) Firewall	Нет		Да	?	Advanced
Denial-of-Service Defense	Да	Да	Да	Да	Да
Other				Anti-Virus, Anti-Spam	
Другие преимущества					
Service Provider Feature Set	Нет	Да	Да		
NIST-Certified FIPS-140	Нет	Да			
High Performance Platform	Нет	Да	Да		
Pre-Packaged Strong Authentication	Нет				
Other					Real-time Upates for Endpoint & Perimeter Security

Пользовательский интерфейс позволяет администратору реализовать некоторые возможности по изменению дизайна, а администраторский интерфейс предоставляет способы для удобного, интегрированного управления.

Особое внимание Citrix уделила вопросу централизованного развертывания приложений, чтобы упростить процесс внешнего доступа, кроме того, хочется отметить, что сканирование конечной точки доступа происходит в режиме online, а не только во время подключения и установления соединения.

Symantec™ Gateway Security 5600 Series

Symantec Gateway Security 5600 – это доступный, надежный и простой в управлении программно-аппаратный комплекс для универсального управления угрозами, использующий различные технологии Symantec, в том числе технологии антивирусной защиты и обнаружения/предотвращения

вторжений. За счет использования восьми функций обеспечения безопасности, тесно интегрированных друг с другом, этот программно-аппаратный шлюз обеспечивает эффективную и простую в управлении защиту. Программно-аппаратный комплекс SGS5660 позволяет обеспечить для автономных офисов и офисов ROBO (Remote Office/Branch Office – удаленный офис или филиал), до 5000 пользователей.

Функция Symantec Clientless VPN дает возможность клиенту безопасно и защищенно расширить свою корпоративную сеть для удаленных пользователей, партнеров и покупателей через интернет. Эта функция использует проверенные технологии безопасности и доступа, широко применяемые в интернет: Secure Socket Layer (SSL) и web-браузеры. Комплекс Symantec Gateway Security 5600 Series, помимо организации безопасного удаленного доступа, предоставляет законченное решение по защите периметра.

Мастер Windows помогает с интеграцией с Windows Active Directories (и NT Domains) для аутентификации пользователей и применения групповых политик. Среди прочего, можно выделить поддержку на стороне клиента Microsoft Windows Mobile 2003 и Palm OS 5.x based PDAs. L3VPN второго поколения предоставляют возможность двунаправленного обмена для всех IP-приложений, основанных на unicast.

Заключение

Мировые тенденции рынка решений SSL VPN все же находят отражение в тенденциях и нашего, российского рынка. Но, в любом случае, размах, конечно, не тот. Это связано, в первую очередь, со спецификой построения корпоративных информационных сетей и организации рабочего процесса российских компаний. В подавляющем большинстве случаев и то, и другое строится по "классическим" канонам. Информационная инфраструктура, равно как и рабочий процесс, "заточены" под стационарное ведение бизнеса. Пока что трудно себе представить среднестатистическую российскую компанию, сотрудники которой проводят, если не значительную, то значимую часть своего рабочего времени вне стен "родного" офиса. А уж если и уезжают в командировки или отпуск, то пользуются чем-нибудь, но не MS Outlook Web Access. Слово "мобильность" для обычного пользователя пока что – один из рекламных слоганов всевозможных производителей. Помимо этого, ценовой вопрос также остается для многих камнем преткновения.

Но, несмотря на все эти аспекты, многие российские компании уже "вкусили плоды цивилизации" и оценили, что значит слово "мобильность", в отношении использования трудовых ресурсов, на самом деле. Правда, опыт внедрения подобных решений специалистами группы компаний ЛАНИТ говорит о том, что пионерами, впрочем, как и основными участниками на данный момент, являлись и являются крупные иностранные компании и крупные российские компании с участием иностранного капитала и управления. Но на сегодняшний день уже многие руководители понимают, что обеспечение действительно мобильной работы своих сотрудников благотворно влияет на их производительность и в итоге – на благосостояние самой компании в целом. И вот тут при выборе технологии, обеспечивающей эту мобильность, более выгодное положение, несомненно, оказывается у SSL VPN, в отличие от IPSec. Кроме того, это самое благосостояние компании растет еще и за счет снижения общей стоимости владения такого решения. В итоге в выигрыше остаются все: и пользователи, которым нет необходимости таскать везде свой ноутбук и перед отъездом каждый раз ломать голову, какие же данные с корпоративных ресурсов им могут понадобиться, и работодатель, который, помимо экономии на поддержке и администрировании такой мобильности и повышения производительности своих сотрудников, увеличивает защищенность своей корпоративной информационной системы, что, в принципе, ставится во главу угла в подобного рода решениях.

IPSec, конечно, еще рано хоронить, но его "родственник" нам по душе. Да здравствует SSL VPN!

Поборцев Николай,
менеджер по развитию направления информационной безопасности,
ДСИ ЛАНИТ