Визитка

СТАНИСЛАВ ШПАК, более пяти лет занимается сопровождением Active Directory и Windows-серверов. Имеет сертификаты MCSE по Windows Server 2000/2003

UserGate Proxy&Firewall

Сертифицированный защитник сетей*

Необходимость организации безопасного межсетевого взаимодействия, ограничений на доступ пользователей к внешним ресурсам и мониторинга их активности — задача, знакомая многим системным администраторам

Кроме того, организации, обрабатывающие персональные данные (ПДн), согласно закону 152-ФЗ обязаны защищать свои информационные системы и сети в соответствии с требованиями нормативно-методической базы Регуляторов. При взаимодействии информационных систем с внешними сетями или информационно-телекоммуникационными сетями международного информационного обмена (Интернет) одним из основных способов защиты является межсетевое экранирование в целях управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы.

В качестве одного из решений по межсетевому экранированию рассмотрим российскую разработку компании Entensys – продукт UserGate Proxy&Firewall 5.2.F. Семейство средств защиты этой компании уже давно известно в профессиональной среде и зарекомендовало себя с положительной стороны. Данный продукт позиционируется для сегмента малого и среднего бизнеса, хотя функциональность его приближается к решениям корпоративного уровня, а в чем-то, возможно, и превосходит их.

Требования законодательства в области защиты ПДн

Если обратиться к закону 152-ФЗ «О персональных данных» и статье 19 закона, становится ясно, что защищать ПДн необходимо в соответствии с требованиями Регулирующих органов. Основным органом, устанавливающим методы и способы защиты информации в информационных системах, является Федеральная служба по техническому и экспортному контролю (ФСТЭК России). 5 февраля 2010 года она выпустила приказ №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». В соответствии с утвержденным документом межсетевые экраны организаций должны обеспечивать выполнение ряда требований предъявляемых к фильтрации, регистрации и учету сетевой информации, контролю доступа и обеспечению целостности.

Казалось бы, теперь операторам ПДн нужно просто найти способ выполнить требования методических указаний. Но все не так просто. Есть еще Постановление Правительства РФ от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», в п. 5 которого читаем следующее: «Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия».

В соответствии со статьей 20 Федерального закона от 27 декабря 2002 года №184-ФЗ «О техническом регулировании» подтверждение соответствия осуществляется в формах: принятия декларации о соответствии (декларирование соответствия) или обязательной сертификации. В настоящее время ФСТЭК России и ФСБ России, которые в соответствии с п. 3 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Постановление Правительства РФ 2007 года №781) получили право устанавливать методы и способы защиты информации в информационных системах, имеют только действующие системы сертификации средств защиты информации, а системы декларирования соответствия ими еще не созданы. Отсюда следует, что в настоящее время для защиты ПДн необходимо применение сертифицированных средств. Кроме того, наличие у продукта сертификата ФСТЭК России – гарантированное подтверждение того, что он отвечает требованиям методических указаний, приведенных в приказе №58.

В апреле 2010 года UserGate Proxy&Firewall 5.2.F стал первым российским программным межсетевым экраном, прошедшим сертификацию ФСТЭК России на соответствие:

Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» – по ОУД2.

Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» (РД МЭ) – по четвертому классу защищенности.

Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств

защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» – по четвертому уровню контроля.

На основании полученного сертификата, продукт может использоваться для защиты:

- конфиденциальной информации в автоматизированных системах до класса защищенности 1Г включительно;
- персональных данных в ИСПДН до первого класса включительно.

Не надо задумываться о применимости или классе информационной системы, которую можно защищать сертифицированной версией UserGate, так как первый класс ИСПДн является максимальным.

Примечательно, что UserGate Proxy&Firewall 5.2.F, помимо соответствия требованиям РД МЭ, проходил сертификацию по «Общим критериям», так как его функциональные возможности, в том числе касающиеся безопасности, шире требований Руководящего документа к данным классам межсетевых экранов.

Приемущества UserGate Proxy & Firewall

Наличие сертификата соответствия – лишь одно из преимуществ. UserGate Proxy&Firewall – это комплексное решение по обеспечению разделения внутренних подсетей компании от внешних, организации доступа сотрудников в Интернет, контролю и статистике использования ресурсов Интернета. Также его можно использоваться и для сегментирования внутри сети, разделив сеть ИСПДн на несколько сегментов, снизив тем самым требования и упростив защиту ПДн.

Системные требования зависят от размера обслуживаемой внутренней подсети, но по нынешним временам вполне скромные: от Pentium4 1GHZ/512Mb RAM на Windows 2000 до Pentium4 2GHz/1Gb RAM на Windows 2003 (если станут использоваться дополнительные модули, то системные требования могут быть выше). Поддерживается вся линейка операционных систем от Microsoft начиная с Windows 2000, причем важной особенностью является отсутствие необходимости обязательного использования серверных ОС.

Интерфейс управления достаточно прост и интуитивно понятен (см. рис. 1). Давайте кратко рассмотрим основные возможности программы: те, которые очевидны из скриншота консоли администрирования, и те, которые скрыты более глубоко, но не менее приятны для системного администратора. Сразу оговорюсь, что специально для тех, кому с первого взгляда продукт покажется слишком сложным, существует мастер пошаговой настройки.

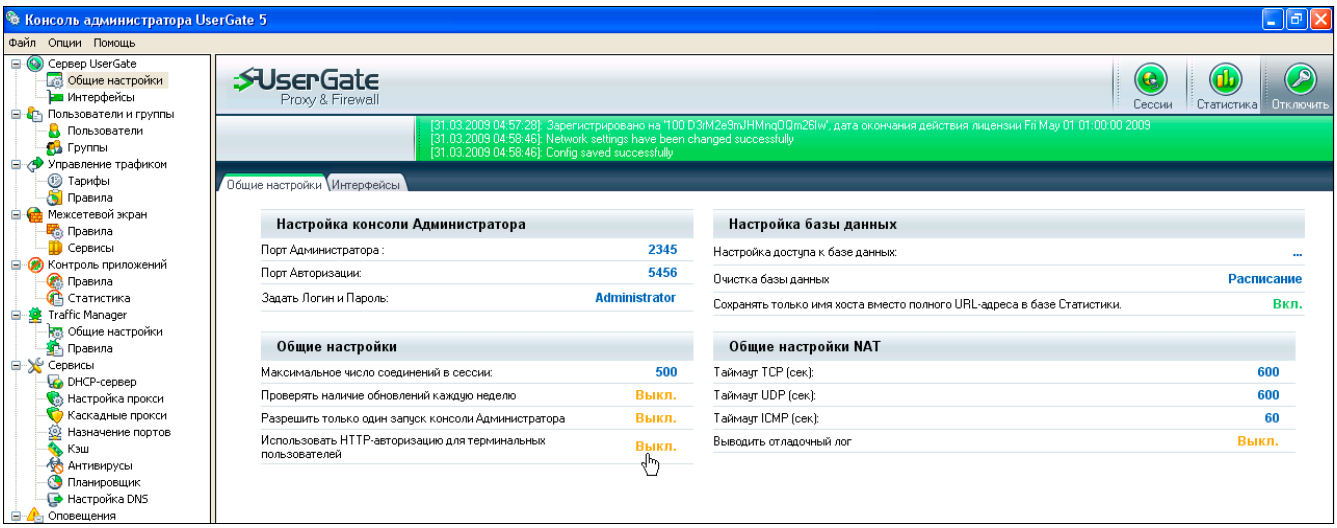
Итак, основная функция программы – межсетевое экранирование. Реализована эта функция через собственный расширенный драйвер NAT, отличный от стандартного в Windows. Благодаря ему можно создавать локальные маршрутизируемые подсети, делать публикацию внутренних серверов для использования «снаружи», поддерживать VPN-соединения и протоколы IP-телефонии, создавать различные правила по доступу к внешним ресурсам либо их блокировке.

Применяются правила к пользователям либо компьютерам – последние могут быть представлены как IP-, так и MAC-адресом. Учетные записи пользователей UserGate могут быть синхронизированы с Active Directory, поддерживаются NTLM-аутентификация и объединение пользователей в группы.

UserGate умеет работать с несколькими провайдерами и осуществлять переключение на лету между ними, когда один из каналов «падает». После восстановления работоспособности канала произойдет обратное переключение. Также можно связать определенных пользователей с определенным каналом. Таким образом, без труда можно сделать так, что начальство будет пользоваться быстрым, стабильным и дорогим каналом, в то время как рядовые пользователи – дешевым и медленным.

Впрочем, распределить ширину канала между пользователями можно и при наличии только одного внешнего канала. UserGate умеет работать с шейпингом трафика, позволяя задавать ограничения для пользователей или их групп по скорости канала или по объему скачанной информации, уменьшая скорость канала вплоть до полной блокировки доступа. Кроме того, можно назначать разный приоритет для разных типов трафика.

Рисунок 1. Консоль администрирования UserGate Proxy&Firewall



Кстати, о разных видах трафика. UserGate имеет различные прокси-серверы для различных протоколов (HTTP, FTP, SOCKS, POP3, SMTP), работающие в прозрачном или непрозрачном режимах. Кроме того, поддерживается каскадирование прокси-серверов.

Сегодня мало разграничить правила, разрешающие и запрещающие доступ в Интернет, зачастую нужно постараться предотвратить нецелевое его использование. Существует два принципиальных подхода к этой проблеме – предварительная фильтрация либо административный запрет. Во втором случае выпускается административное распоряжение, запрещающее пользоваться определенными ресурсами, например, сайтами социальных сетей. В конце отчетного периода администратор готовит руководству отчет по работе пользователей в Интернете, на основании этого происходит разбор полетов и наказание нарушителей.

Для первого подхода существует база данных адресов сайтов, отсортированных по различным категориям, в рамках которой запрещается или разрешается доступ определенным пользователям к определенным категориям. Такие решения – не редкость, однако их обычное узкое место – это поддержание базы в актуальном состоянии и наличие в ней регионально значимых сайтов. Например, база для пользователей из США будет не очень актуальна для России и наоборот. Очевидно, это понимали и разработчики UserGate, потому что в рамках продукта предлагается специально адаптированная для использования русскоязычными пользователями база, содержащая 500 миллионов сайтов (из которых до 10 миллионов – русскоязычные) в 82 категориях.

Контроль за приложениями на пользовательских компьютерах также возможен. Для этого на клиентских компьютерах разворачивается бесплатная программа-агент, которая будет связываться с сервером UserGate, блокировать или разрешать работу приложения в Интернете. Кроме того, подход за контролем приложений позволит получить наиболее полную статистику использования интернет-ресурсов. Построение наглядных отчетов по различным критериям – это то, что помогает системному администратору в общении с руководством. Используя статистику и отчеты UserGate, можно без труда перевести трафик в деньги и показать руководству реальную экономию от внедрения программы. Кроме того, в UserGate существует возможность доступа к веб-статистике, причем доступ может быть трех уровней – пользователь, директор и администратор. Пользователь видит только свою статистику и может следить за тем, как он расходует интернет-трафик. Директорский уровень доступа позволяет следить за статистикой всех пользователей, администратор, кроме того, может еще и создавать шаблоны отчетов для получения статистических данных (см. рис. 2).

Антивирусная защита в UserGate

Да-да, все правильно – есть возможность приобрести UserGate с антивирусным модулем. Это вполне логичное решение – сейчас большинство вирусов попадает на компьютер пользователя через Интернет. Так почему бы не перехватывать вредоносные программы на шлюзе, не допуская такой трафик до клиентского компьютера? Разумеется, отказываться от антивирусного ПО на компьютерах пользователей не нужно, так как есть и другие пути заражения компьютера вирусом – например, через флешки.

***

На этом я завершу краткий обзор российского межсетевого экрана UserGate Proxy&Wirewall. Думаю, функционал программы не оставит равнодушным никого, кто заинтересован в надежной защите периметра и гибкости настроек. А сертификацию ФСТЭК оценят организации, которые всерьез озабочены защитой персональных данных в своих сетях. EOF

** На правах рекламы*

Рисунок 2. Веб-статистика в UserGate