Что такое «современный межсетевой экран»?

Игорь Шитов

Менеджер продукта «ЗАСТАВА»

Прежде чем начать рассуждения на тему продуктивного использования межсетевых экранов, необходимо определиться с понятиями. Так что такое «межсетевой экран»? Наиболее кратким, но в то же время понятным определением будет то, которое дано в Википедии: «Межсетевой экран или сетевой экран (а также firewall, FW, файрволл, брандмауэр, МЭ) — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами». Это определение буквально и относится к МЭ в классическом понимании стоящих перед ними задач. Ещё десяток лет назад такое определение было бы исчерпывающим. Однако в настоящий момент его можно смело расширить, используя для описания понятия те задачи, которые решаются современными межсетевыми экранами. Давайте поговорим о задачах подробнее.

Задачи, решаемые современными VPN/FW-продуктами

Практика разработки и, прежде всего, использования современных систем распределённого межсетевого экранирования показывает, что потребителем наиболее востребованы решения, совмещающие в себе функции файрволла и средства построения виртуальных частных сетей (VPN). И подавляющие их большинство из представленных на рынке позволяет нам сделать вывод — именно такое решение имеет право на существование. Поэтому в дальнейшем мы будем исходить из аксиомы, что современный МЭ — это FW и VPN. Тогда решаемые им задачи будут такими:

- Организация доверенных и защищённых каналов связи в рамках единой, территориально распределённой информационной системы.
- Сегментирование информационных систем.
- Защита корпоративной информационной системы от внешних угроз.
- Организация защищённого доступа удалённых (мобильных) пользователей к корпоративным ресурсам.
- Обеспечение надёжности и отказоустойчивости защищаемой информационной системы.

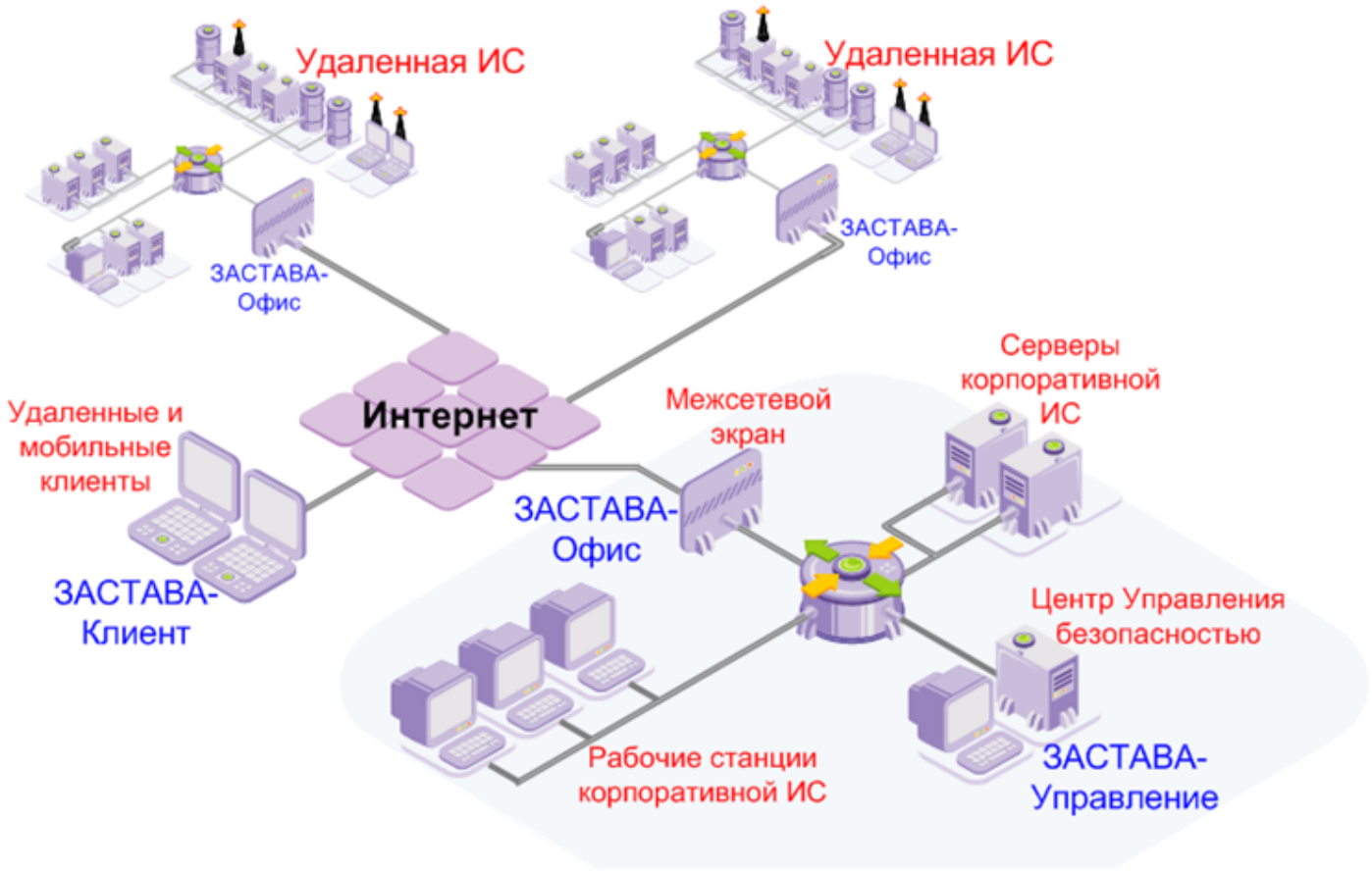

Рис. 1. Архитектура корпоративной ИС

Какие критерии используются для выбора межсетевого экрана?

Некоторое время назад заказчикам было достаточно того, чтобы определённое решение обладало необходимыми сертификатами регуляторов, и это было одним из основных критериев выбора. Но сейчас сертификаты есть у всех ведущих производителей. Современному заказчику гораздо интереснее получить решение, которое не только закроет требования по наличию сертифицированного межсетевого экрана (МЭ) в его ИС, но и будет выполнять реальные защитные функции.

Продукты линейки ЗАСТАВА сертифицированы ФСТЭК (МЭ 2, НДВ 3), ФСБ (КС1, КС2) и Министерством обороны Российской Федерации (МЭ 2, НДВ 2).

Немаловажным фактором при выборе того или иного решения является его стоимость. В 2012 году компанией ЭЛВИС-ПЛЮС было проведено исследования, согласно которому продукты под маркой ЗАСТАВА не проигрывают по стоимости ближайшим аналогам при закупке небольшого количества лицензий, и значительно дешевле конкурентов при применении в больших проектах. Прайс-лист на наши решения был доработан и сейчас, в нашем понимании, он как никогда интересен заказчику любого ранга.

Масштабируемость и производительность — больше значит лучше?

Утверждение, вынесенное в заголовок этого раздела может показаться очень спорным. Действительно, производительность межсетевого экрана должна коррелировать с решаемыми задачами. Предприятиям СМБ нет необходимости использовать производительные решения на базе многоядерных серверных систем — им для выполнения требований регуляторов по защите персональных данных достаточно установить на границе своего информационной системы программно-аппаратный комплекс мини-ПК — ЗАСТАВА.

Для больших, территориально-распределённых организаций с большими объёмами защищаемого сетевого трафика компания ЭЛВИС-ПЛЮС предлагает специализированные решения на высокопроизводительных

аппаратных платформах. Также важна адаптация под современные аппаратные сетевые решения. Например, недавно были завершены тестирования на платформе Crossbeam, и некоторые наши заказчики уже сделали выбор в пользу этого высокопроизводительного решения нового поколения.

Ключевые особенности ПАК «ЗАСТАВА»:

- Требуют минимальных усилий по настройке и установке.
- Скорость шифрования от 30 Мбит/сек (мини-компьютер) до 10 Гбит/с (производительный сервер, Crossbeam).
- Неограниченное количество туннелей.
- Неограниченное количество защищаемых рабочих мест в сегменте.

Соблюдение международных стандартов — единственный подход, гарантирующий совместимость продуктов

Нередки случаи, когда появляется необходимость расширения или модернизации уже существующей информационной инфраструктуры. При этом она может быть построена на программном и аппаратном обеспечении разных вендоров, у неё могут быть различные требования по «железу» конкретных производителей, на всё это накладываются видение и практика использования такой системы CIO, обслуживающим персоналом и рядовыми пользователями. Ребром встаёт вопрос совместимости решений и продуктов! Для разработчика единственный способ её обеспечить — опираться на признанные международные стандарты при создании своего продукта. К сожалению, очень часто ситуацию со стандартами можно проиллюстрировать комиксом:

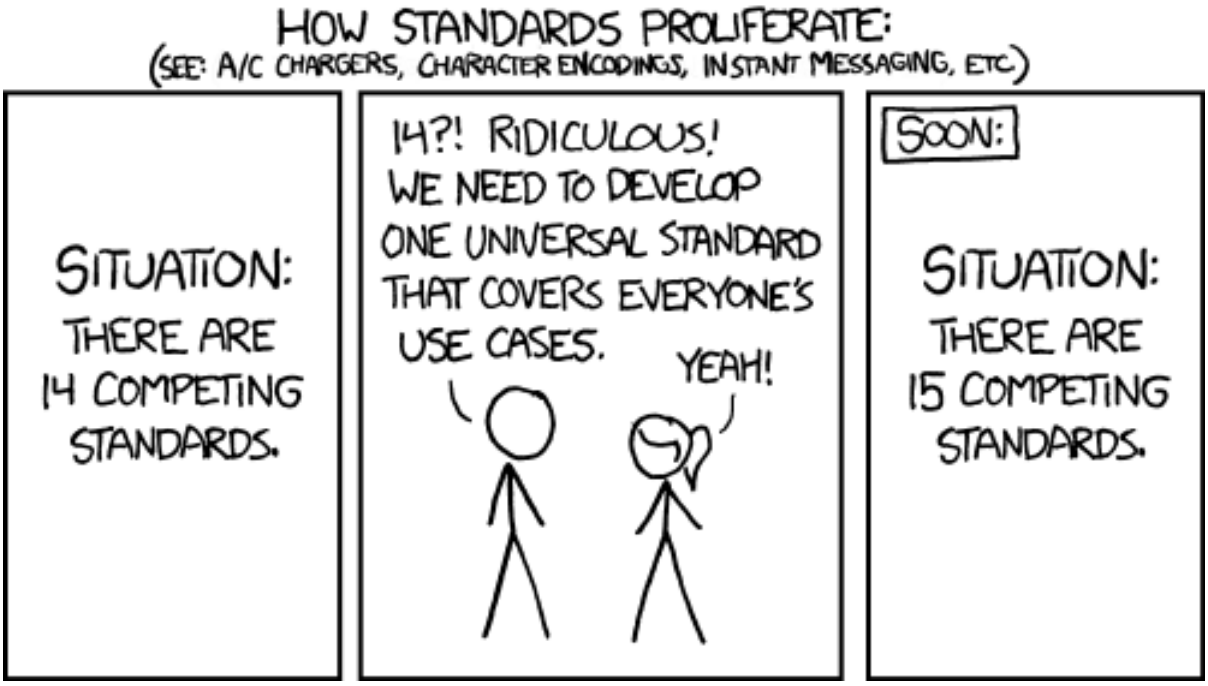

Рис. 2. Как распространяются стандарты

К счастью, для разработчиков и производителей VPN/FW есть международный стандарт IPsec. IPsec это набор протоколов (protocol suite), созданный The Internet Engineering Task Force(IETF) для обеспечения безопасности в IPv4 и IPv6. Семейство протоколов IPsec можно изобразить так:

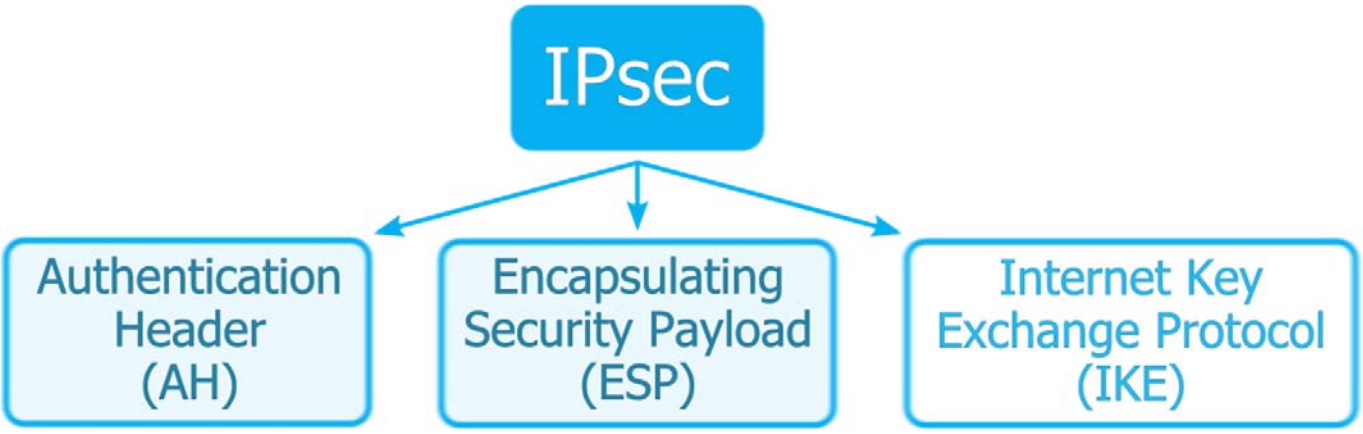

Рис. 3. Семейство протоколов IPsec

AH и ESP — протоколы непосредственной защиты данных. Роль IKE совсем другая — он не занимается непосредственно защитой данных пользователя, но обеспечивает AH и ESP аутентифицированными ключами. Именно поэтому на схеме они выделены разными цветами.

Семейство продуктов «ЗАСТАВА» создаётся на базе именно этих стандартов. Что это нам даёт на практике? Во-первых, это обеспечивает совместимость продуктов различных производителей. Решения линейки «ЗАСТАВА» могут работать в сетях, построенных с использованием оборудования и ПО, например, Cisco Systems, Checkpoint и других вендоров, ориентирующихся на IPsec. В отличие от проприетарных протоколов и стандартов, несовместимых с другими решениями (к сожалению, такой подход исповедуют и некоторые отечественные разработчики), использование IPsec обеспечивает столь необходимую для современных систем межсетевого экранирования гибкость и адаптируемость к различным требованиям. Второе значимое преимущество — большая надёжность и устойчивость к атакам. Новые версии продуктов «ЗАСТАВА» уже используют последнюю версию протокола обмена аутентифицированными ключами — IKEv2. И это открывает перед нами как разработчиками собственного продукта и перед нашими заказчиками очень серьёзные возможности:

1. **Более гибкое использование криптографических алгоритмов**. Использование IKEv2 позволяет применять в конечном продукте разнообразные криптоалгоритмы, в зависимости от требований политики информационной безопасности заказчика.
2. **Лучшая защита от DoS-атак.** Сокращение числа сетевых взаимодействий для обмена ключами по сравнению с IKEv1 даёт значительный запас производительности (при прочих равных условиях), поэтому провести DoS-атаку на VPN/FW становится сложнее.
3. **Повышение эффективности использования ресурсов.** Применение IKEv2 влияет как на загрузку сетевой инфраструктуры (снижается количество сетевых взаимодействий между узлами сети), так и на аппаратное обеспечение («криптографические cookies»).
4. **Повышенная надёжность работы протокола в условиях, когда велика вероятность потери сетевых пакетов.** Все операции требуют подтверждения от другой стороны VPN-соединения.

Централизованное управление — необходимость

Если посмотреть на список крупнейших проектов, где использовались решения на базе линейки продуктов ЗАСТАВА

- ФСТЭК России и её региональные управления
- Информационные системы Минобороны
- Единый Информационный Расчетный Центр города Москвы
- Росреестр
- ЕМТС (Правительство Санкт-Петербурга)
- Республика Татарстан
- ФСК ЕЭС
- Российский Союз Автостраховщиков

- ФМБА Крови
- ОАО «Газпром»

то можно выявить одну интересную и очень важную закономерность. Все эти организации территориально распределены. ЗАСТАВА не только надёжно защищает каналы передачи данных, но и обеспечивает удалённое управление и администрирование всего парка ЗАСТАВА-Агентов. Это реализуется благодаря использованию уникального для российского рынка продукта — ЗАСТАВА-Управление. Наши продукты популярны по нескольким причинам: это дружелюбный к администратору сети GUI, визуализация правил распределённого межсетевого экранирования и точечного шифрования трафика, возможность управления не только продуктами ЗАСТАВА, но и продуктами других производителей (если они построены на IPsec), на практике — неограниченный размер управляемой сети (существуют внедрения на 8 000 Застава-Агентов), мониторинг в режиме реального времени, возможность диагностировать проблемы у удалённых агентов.

Таким образом, современный межсетевой экран — это комплекс программных и аппаратных решений, выполняющий функции распределённого межсетевого экранирования и построения виртуальных частных сетей, обладающий необходимой гибкостью и масштабируемостью, простой в настройке и обслуживании.

Подробное описание линейки продуктов ЗАСТАВА — zastava.ru

Сайт системного интегратора информационной безопасности ЭЛВИС-ПЛЮС — elvis.ru

Есть что сказать? Появились вопросы? Пишите нам в твиттер — twitter.com/ELVIS_PLUS