Межсетевым экранам свойственен определенный набор функций. Основная функция любого межсетевого экрана — это фильтрация пакетов на основании определенного набора правил. Эту функцию поддерживают все брандмауэры. Также все рассматриваемые брандмауэры поддерживают NAT. Но есть довольно специфические функции, например, маскировка портов, регулирование нагрузки, многопользовательских режим работы, контроль целостности, развертывание программы в ActiveDirectory и удаленное администрирование извне. Когда программа поддерживает развертывание в ActiveDirectory — не нужно вручную устанавливать ее на каждом компьютере сети. Также удобно, если межсетевой экран поддерживает удаленное администрирование извне — можно администрировать сеть, не выходя из дому, что будет актуально для администраторов, привыкших выполнять свои функции удаленно.

Основная задача межсетевых экранов при защите персональных — это защита информационной системы персональных данных. Поэтому администратору часто все равно, какими дополнительными функциями будет обладать межсетевой экран. Ему важны следующие факторы:

- Время защиты. Здесь понятно, чем быстрее, тем лучше.
- Удобство использования. Не все межсетевые экраны одинаково удобны, что и будет показано в обзоре.
- Стоимость. Часто финансовая сторона является решающей.
- Срок поставки. Нередко срок поставки оставляет желать лучшего, а защитить данные нужно уже сейчас.[4]

Брандмауэр TrustAccess — это распределенный межсетевой экран с централизованным управлением, предназначенный для защиты серверов и рабочих станций от несанкционированного доступа, разграничения сетевого доступа к ИС предприятия.
Киберсейф Межсетевой экран — мощный межсетевой экран, разработанный для защиты компьютерных систем и локальной сети от внешних вредоносных воздействий.
ViPNet Office Firewall 4.1 — программный межсетевой экран, предназначенный для контроля и управления трафиком и преобразования трафика (NAT) между сегментов локальных сетей при их взаимодействии, а также при взаимодействии

узлов локальных сетей с ресурсами сетей общего пользования.

Время защиты. Все три межсетевых экрана распространяются в виде пакетов MSI, а это означает, что можно использовать средства развертывания ActiveDirectory для их централизованной установки.

На предприятии, как правило, используется централизованное управление межсетевыми экранами. А это означает, что на какой-то компьютер устанавливается сервер управления брандмауэрами, а на остальные устанавливаются программы-клиенты или как их еще называют агенты. Проблема вся в том, что при установке агента нужно задать определенные параметры — как минимум IP-адрес сервера управления, а может еще и пароль и т.д.
Следовательно, даже если вы развернете MSI-файлы на все компьютеры сети, настраивать их все равно придется вручную. А этого бы не очень хотелось, учитывая, что сеть большая. Даже если у вас всего 50 компьютеров вы только вдумайтесь — подойти к каждому ПК и настроить его.
Как решить проблему? А проблему можно решить путем создания файла трансформации (MST-файла), он же файл ответов, для MSI-файла. Вот только ни VipNet Office Firewall, ни TrustAccess этого не умеют. Развернуть эти программы в домене можно, но требуется ручная работа администратора.
Киберсейф Межсетевой экран самостоятельно создает MST-файл, нужно лишь установить его на один компьютер, получить заветный MST-файл и указать его в групповой политике. За какие-то полсача (а то и меньше) вы сможете развернуть межсетевой экран на все компьютеры сети.
Именно поэтому Киберсейф Межсетевой экран актуальнее в факторе времени защиты.

Удобство использования. Брандмауэр — это не текстовый процессор. Это довольно специфический программный продукт, использование которого сводится к принципу «установил, настроил, забыл». С одной стороны, удобство использования — второстепенный фактор. Например, iptables в Linux нельзя назвать удобным, но ведь им же пользуются? С другой — чем удобнее брандмауэр, тем быстрее получится защитить ИСПДн и выполнять некоторые функции по ее администрированию.
VipNet Office Firewall, не очень удобный. Выделить компьютеры в группы можно только по IP-адресам. Другими словами, есть привязка к IP-адресам и вам нужно или выделять различные ИСПДн в разные подсети, или же разбивать одну подсеть на диапазоны IP-адресов. Например, есть три ИСПДн: Управление, Бухгалтерия, IT.

Вам нужно настроить DHCP-сервер так, чтобы компьютерам из группы Управление «раздавались» IP-адреса из диапазона 192.168.1.10 — 192.168.1.20, Бухгалтерия 192.168.1.21 — 192.168.1.31 и т.д. Это не очень удобно.

В межсетевом экране Киберсейф, наоборот, нет никакой привязки к IP-адресу. Компьютеры, входящие в состав группы, могут находиться в разных подсетях, в разных диапазонах одной подсети и даже находиться за пределами сети. Филиалы компании расположены в разных городах (Ростов, Новороссийск и т.д.). Создать группы очень просто — достаточно перетащить имена компьютеров в нужную группу и нажать кнопку «Применить». После этого можно нажать кнопку «Установить правила» для формирования специфических для каждой группы правил.

Что касается TrustAccess, то нужно отметить тесную интеграцию с самой системой. В конфигурацию брандмауэра импортируются уже созданные системные группы пользователей и компьютеров, что облегчает управление межсетевым экраном в среде ActiveDirectory. Вы можете не создавать ИСПДн в самом брандмауэре, а использовать уже имеющиеся группы компьютеров в домене Active Directory.

Стоимость. Обойти финансовую сторону вопроса просто невозможно, ведь часто она становится решающей при выборе того или иного продукта. Так, стоимость одной лицензии ViPNet Office Firewall 4.1 (лицензия на 1 год на 1 компьютер) составляет 15 710 р. А стоимость лицензии на 1 сервер и 5 рабочих станций TrustAccess обойдется в 23 925 р. За эти деньги можно купить лицензию на 25 узлов Киберсейф Межсетевой экран (15178 р.) или немного добавить и будет вполне достаточно на лицензию на 50 узлов (24025 р.). Но самое главное в этом продукте — это не стоимость. Самое главное — это срок действия лицензии и технической поддержки. Лицензия на Киберсейф Межсетевой экран — без срока действия, как и техническая поддержка. То есть вы платите один раз и получаете программный продукт с пожизненной лицензией и технической поддержкой.

Срок поставки. Время поставки VipNet Office Firewall составляет около 2-3 недель после обращения в ОАО «Инфотекс». Честно говоря, это довольно долго, учитывая, что покупается программный продукт, а не ПАК.
Время поставки TrustAccess, если заказывать через «Софтлайн», составляет от 1 дня. Более реальный срок — 3 дня, учитывая некоторую задержку «Софтлайна». Хотя могут поставить и за 1 день, здесь все зависит от загруженности «Софтлайна». Опять-таки — это личный опыт, реальный срок конкретному заказчику может отличаться. Но в любом случае срок поставки довольно низкий,

что нельзя не отметить.
Что касается программного продукта КиберСейф Межсетевой экран, то производитель гарантирует поставку электронной версии в течение 15 минут после оплаты.

Заключение. Если ориентироваться только по стоимости продукта и технической поддержки, то выбор очевиден — Киберсейф Межсетевой экран. Киберсейф Межсетевой экран обладает оптимальным соотношением функционал/цена. С другой стороны, если вам нужна поддержка Secret Net, то нужно смотреть в сторону TrustAccess. А вот VipNet Office Firewall можем порекомендовать разве что как хороший персональный брандмауэр, но для этих целей существует множество других и к тому же бесплатных решений.

Список литературы:

1.https://www.securitycode.ru/company/news/mezhsetevoy_ekran_trustaccess_razrabotki_komp

2. https://habr.com/company/cybersafe/blog/250127/

3. http://www.cisco-lan.ru/vipnet_safedisk_version_4_1_reliable_data_protection_and_network_hard_disks_memory_

4. https://habr.com/company/cybersafe/blog/268049/