Современные темпы ИТ- технологий, особенно сегмента широкополосного доступа в Интернет приводит к естественному процессу- размещению важных компонентов бизнес- решений в среду Web. Например, системы типа банк-клиент, публичные сайты организаций, интернет-магазины, новостные, развлекательные и торговые площадки являются обязательной составляющей всемирной сети. Однако прогрессу в этой области мешает как раз та доступность, которая и является главным достоинством WEB-технологий. Из-за своей толерантности к обращениям Web- приложения подвергаются различным атакам, становясь уязвимой целью для хакеров, поэтому не мудрено, что решения по сетевой защите очень актуально и будет еще долго необходимо.

В последнее время обозначилась тенденция к тому, чтобы Web- приложения проектировать в виде межплатформенных сервисов, при этом сам функционал таких приложений распределен между тонким и толстым клиентом, при этом БД, как правило, располагается на сервере.

Таким образом, важнейшая задача- построить основы безопасного применения в такой среде, по крайней мере с аппаратной точки зрения. На рис.1. Показан пример типичной конфигурации для портала iBiomatics, который доступен в Интернете. При этом надо обратить внимание, что соединение браузера к веб - серверу всегда выполняется с помощью протокола https:\\. Это гарантирует, что вся информация, передаваемая между браузером и сервером шифруются. При чем, везде, где это возможно, используется 128-битное шифрование.

Между браузером и веб-сервером, брандмауэр осуществляет фильтрацию портов. Браузер должен запросить подключение к определенному порту или же брандмауэр заблокирует соединение. Тут надо отметить, что если портал iBiomatics будет развертываться только на отдельных участках, то этот брандмауэр должен быть настроен на IP-фильтрацию. Например, если в некой многонациональной фармацевтической компании был установлен ряд сайтов, которые были открыты для доступа, то

IP-адреса корпоративных машин будут сконфигурированы в брандмауэр так, чтобы в их узлы блокировался доступ со всех других подключений к Интернету.

На обратной стороне брандмауэра находится узел с внутренним IP-адресом для Web –сервера и только брандмауэр знает этот IP-адрес, при этом веб-сервер будет отвечать только на запрос от брандмауэра. Это гарантирует, что никто не может соединиться с веб-сервер, минуя брандмауэр.

Затем веб-сервер делает запросы в другие устройства в сети, но только через второй брандмауэр. Этот брандмауэр, как обычно, настроен на осуществление IP-фильтрации и фильтрации портов. На IP-адрес веб-сервера будет разрешено проходить только через брандмауэр. И еще раз, только брандмауэр знает внутренние IP-адреса других машин в сети.

И межсетевой экран будет реагировать только на запросы на одном порту. Таким образом, все это гарантирует, что все взаимодействия с внутренней сетью будут брать свое начало на веб-сервере, а весь трафик будет проходит через второй брандмауэр.

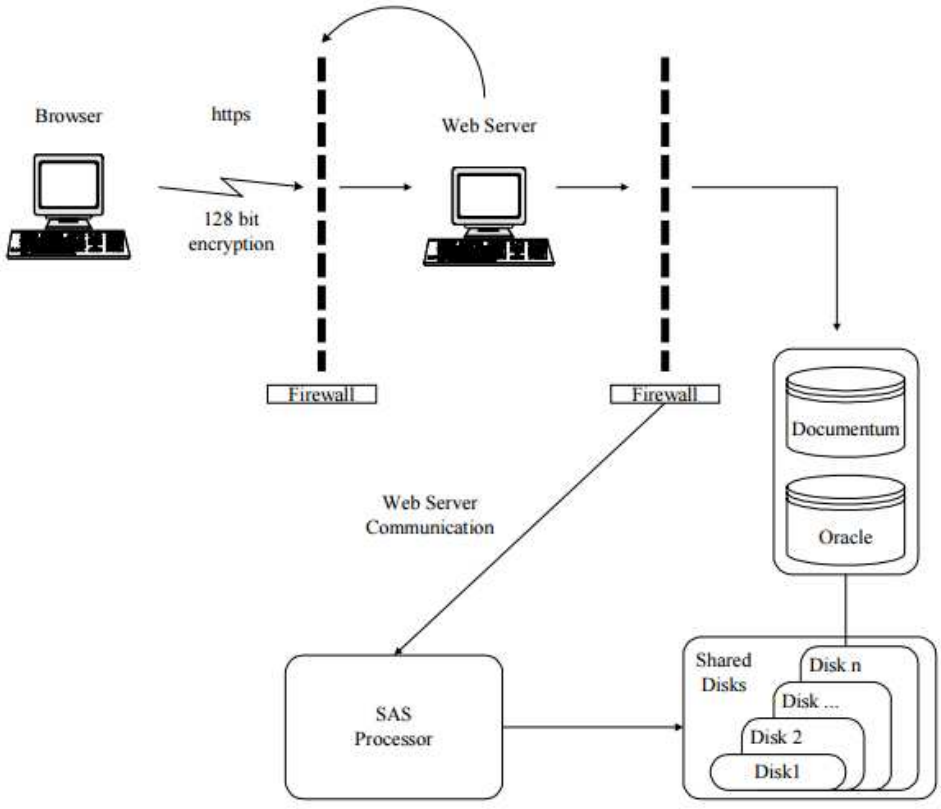

Рис.1. базовая аппаратная конфигурация портала iBiomatics

В своей повседневной работе всегда надо учитывать, что Веб-приложения могут быть последней преградой между злоумышленниками и уязвимыми внутренними ресурсами предприятий. Соответственно, надо очень внимательно отнестись к защите внутренних систем компании.

http://www.yildiz.edu.tr/~naydin/I2B/docs/ComputerGiants.pdf

http://www.zoominfo.com/Search/ReferencesView.aspx?PersonID=-131820

IBiomatics http://www.iBiomatics.com