УДК 004

АРХИТЕКТУРА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Слесаренко Ю.В. ИТб-181, IV курс, Фурман Н.В., старший преподаватель, кафедра ИиАПС
Научный руководитель: Протодьяконов А. В., доцент (к.н.) кафедры ИиАПС
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, филиал в г. Кемерово
г. Кемерово

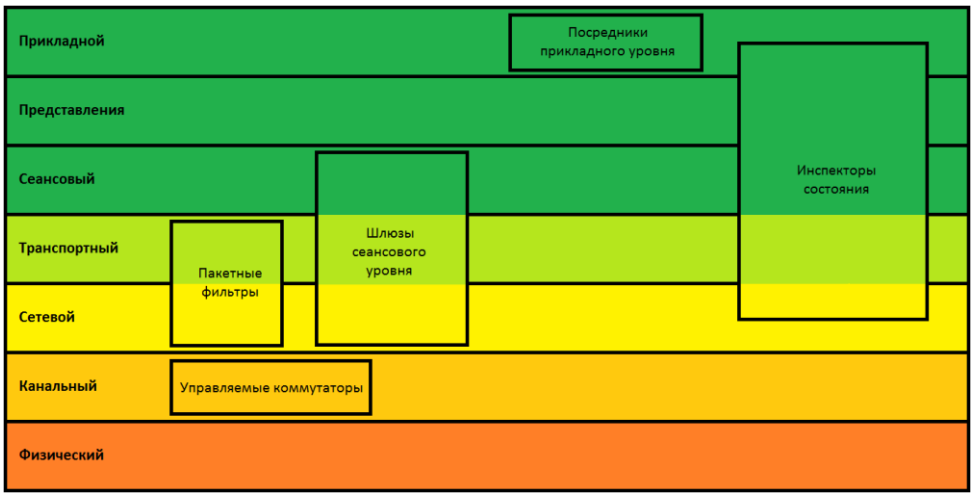
Архитектура системы информационной безопасности (Архитектура СИБ) - комплекс технических средств для защиты информационных данных от сторонних воздействий.

Для всех компаний информационные данные является ключевой ресурс, поэтому защитить информацию, от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения, является основной задачей. В данной работе мы рассмотрим основные компоненты, которые предоставляет архитектура СИБ Cisco SAFE для безопасности предприятий.

1. Межсетевой экран.

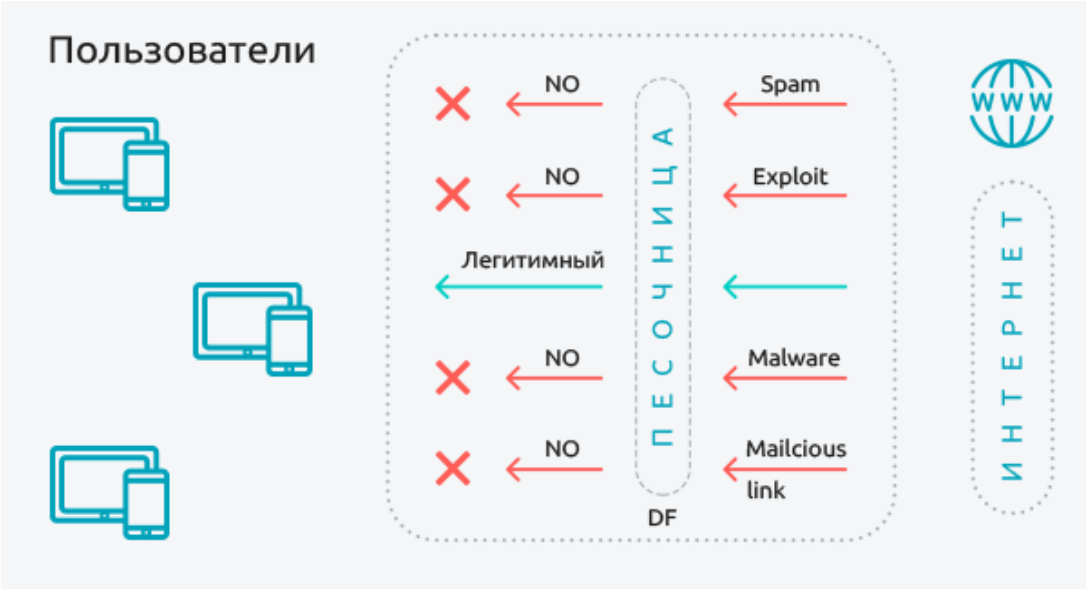
Проблема, которую решает межсетевой экран заключается в защите сети по установленным правила (ruleset), как правило это набор фильтров посредством который проходит поток информации. Есть два способа интеграции в бизнес процесс программное и программно-аппаратное решение, для применение программного решение необходим свободный компьютер с высокими требованиями, как правило у организаций такого не находится, поэтому популярны решения программно-аппаратное решение, достоинствами такого подхода является, проста установки и использования, а также производительность и отказа устойчивость. Ограничениями межсетевой экран является, не способность принять решение что делать с не распознанным трафиком которые, например, используют криптографию или с шифровку данных прикладного уровня, во всех этих случая правила, которые установлены межсетевой экран, должны явно, куда отправлять такой (не распознанный) трафик. Еще в кратко коснемся классификации сетевого экрана:

1) Управляемые коммутаторы - фильтруют трафик в рамках локальной сети.
2) Пакетные фильтры – рассматривает параметры заголовка сетевого пакета.
3) Шлюзы сеансового уровня – Блокирует взаимодействия внешних хостов с узлом локальной сети.
4) Посредники прикладного уровня - Может определить тип полученной информации и запрещать использовать некоторые команды
5) Инспекторы состояния – объединяет все выше перечисленные уровни



2. Песочница.

Это совокупность мер направленных на выявление целевых атак в изолированной среде. Комплекс использует виртуальную машину или сервер, оснащению разными инструментами, которые эмитируют обычную работу операционной системы или ПО, в которой производиться проверка файлов, после этого трафик попадает на рабочие машин. Простой способ интеграции песочницы представляет собой подключение к SPAN – портам коммутатора.



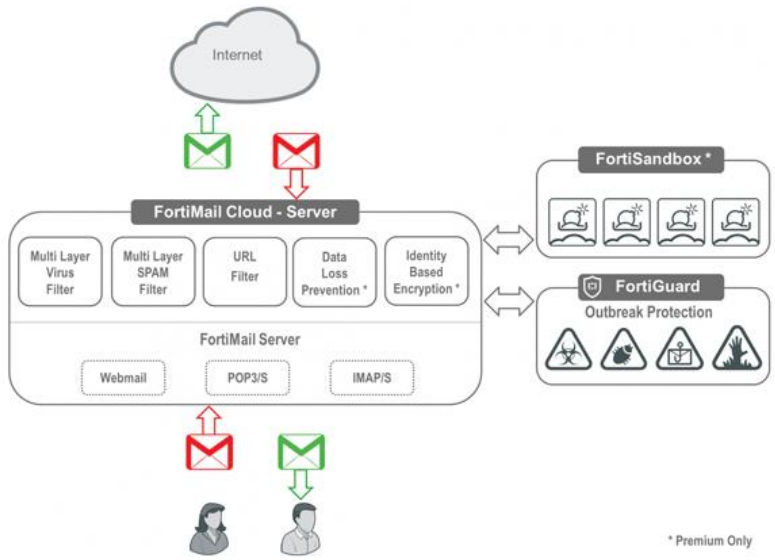
3. Защита электронной почты.

Существует три варианта реализации защиты физического или виртуального устройства, а также в качестве облачного сервиса. Принцип проверки, сначала отправленное адресатом письмо, проходит проверку на специально

выделенном сервере или виртуальной машине, а потом доходит до адресата. Проверка письма включает в себя:

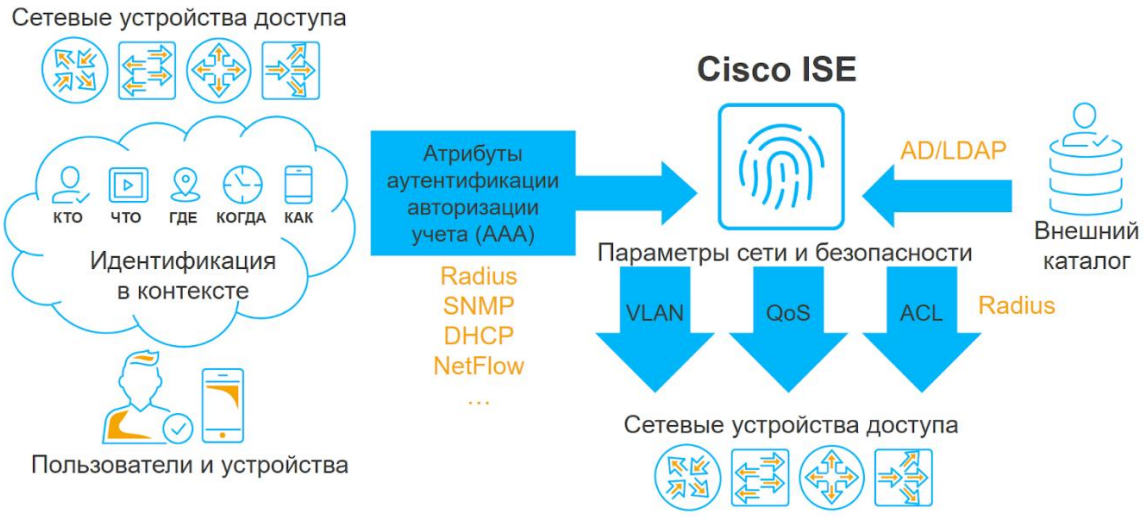
- Проверку IP-адресата
- Домена отправителя
- Репутации отправителя
- Проверка подлинности получателя
- Проверка по ключевым словам
- Анализ изображений
- Проверка URL ссылок

Рисунок 4. Схема обеспечения безопасности электронной почты при FortiMail Cloud (Server)



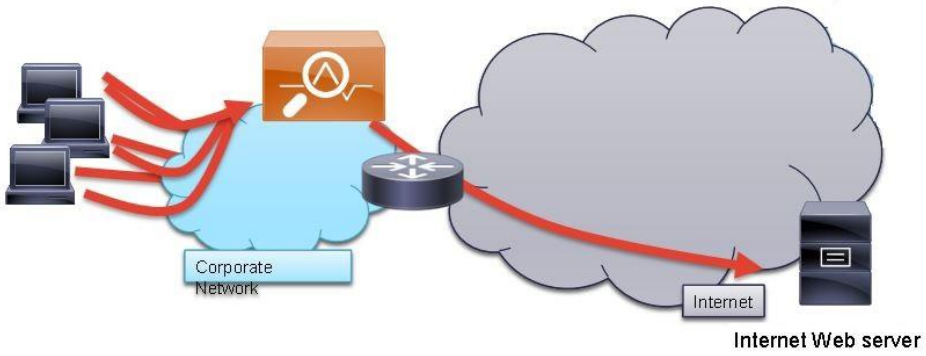
4. Контроль доступа к сети.

Контроль доступа к сети может быть установлен, как и большинство современных решений виртуально или физически как отдельный сервер. Контроль объединяет в себя, сервисы аутентификации, авторизации и учета событий (AAA), оценки состояния, профилированием и управлением гостевым доступом в раках единой платформы.



5. Защита веб-приложений

Самый проверенный способ защиты доступа в интернет. Принцип работы прост прокси сервер принимает на себя запросы пользователей, проверяет на соответствие безопасности и уже через себя устанавливает соединение с интернетом.



Заключение

В данном работе рассмотрены основные технологии, которые направлены на сохранение и защиту информационных данных предприятия. Описаны средства создания архитектуры информационной безопасности предприятия.