Сетевая безопасность

Защита информации
компьютерных систем и сетей

Интернет

это всемирная сеть сетей, которая использует для взаимодействия стек протоколов TCP/IP.

Типовые сервисы

- SMTP

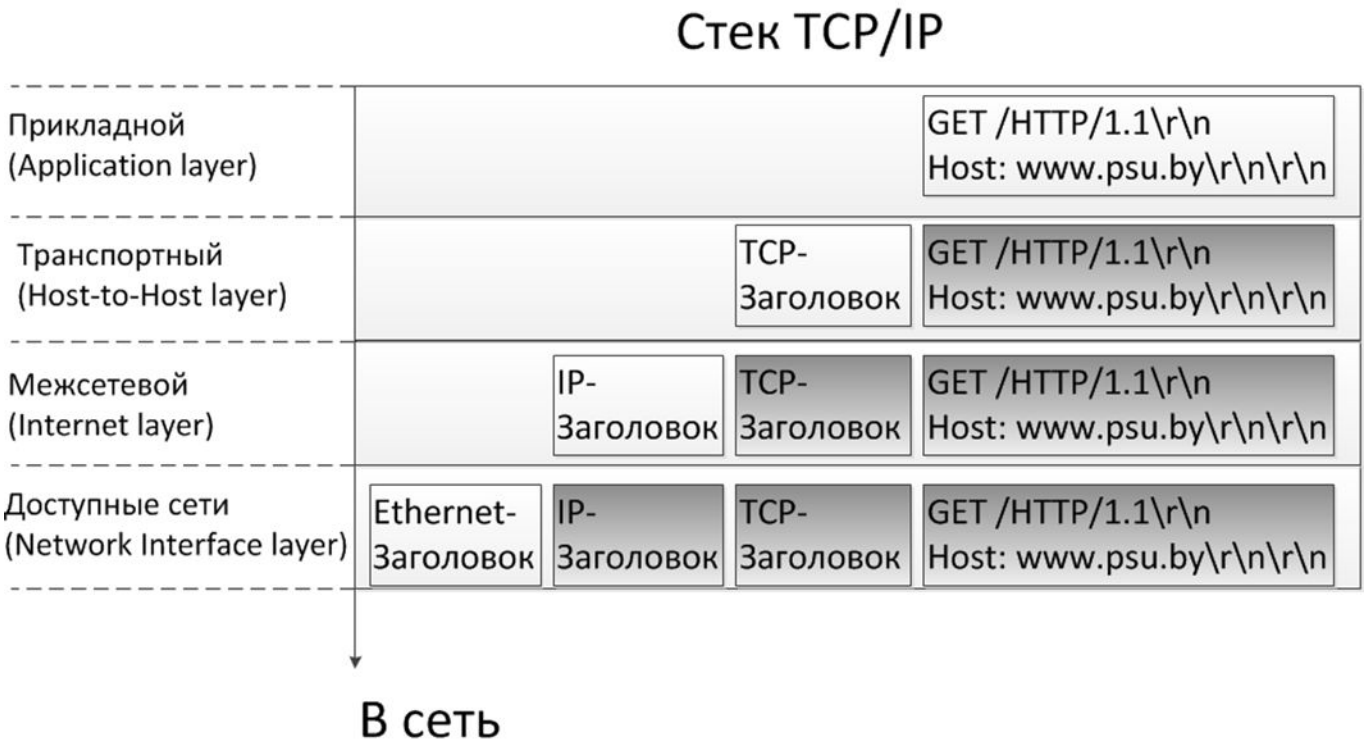
- TELNET

- FTP

- DNS

- WWW

Инкапсуляция



Инциденты с безопасностью в Интернете

- Внутренний инцидент - инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом

- Внешний инцидент - инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом

Внутренний инцидент

- утечка конфиденциальной информации;
- неправомерный доступ к информации;
- удаление информации;
- компрометация информации;
- саботаж;
- мошенничество с помощью ИТ;
- аномальная сетевая активность;
- аномальное поведение бизнес-приложений;
- использование активов компании в личных целях или в мошеннических операциях.

Внешний инцидент

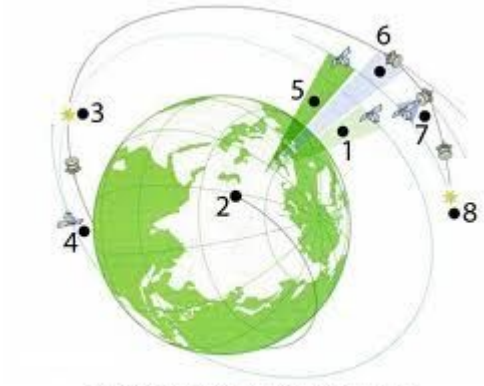
- мошенничество в системах ДБО;
- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- неправомерное использование корпоративного бренда в сети Интернет;
- фишинг;
- размещение конфиденциальной/провокационной информации в сети
- Интернет;
- взлом, попытка взлома, сканирование портала компании;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации;
- анонимные письма (письма с угрозами).

Способы аутентификации

- Аутентификация по многоразовым паролям
- Аутентификация по одноразовым паролям
- Многофакторная аутентификац

Наблюдения за передаваемыми данными

- Сетевой снифинг
- Ложные запросы ARP
- Ложная маршрутизация
- Перехват TCP-соединения

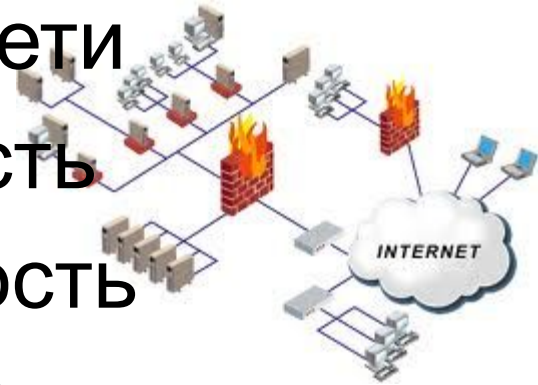


Брандмауэр

это подход к безопасности; он помогает реализовать политику безопасности, которая определяет разрешенные службы и типы доступа к ним, и является реализацией этой политики в терминах сетевой конфигурации

Целесообразность использование брандмауэра

- Защита от уязвимых мест в службах
- Управляемый доступ к систем сети
- Концентрированная безопасность
- Повышенная конфиденциальность
- Протоколирование и статистика использования сети и попыток проникновения
- Претворение в жизнь политики



Прокси-сервер

служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам

VPN

обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)

Классификация VPN