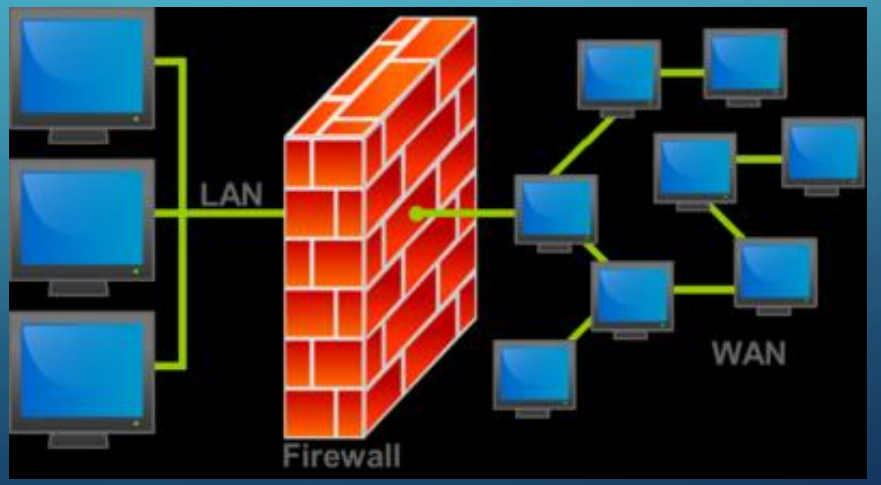
# FIREWALL (МЕЖСЕТЕВЫЕ ЭКРАНЫ)

АВТОР:

ШНАЙДЕР А.В.

# О ТЕХНОЛОГИИ FIREWALL

Firewall (межсетевой экран) - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

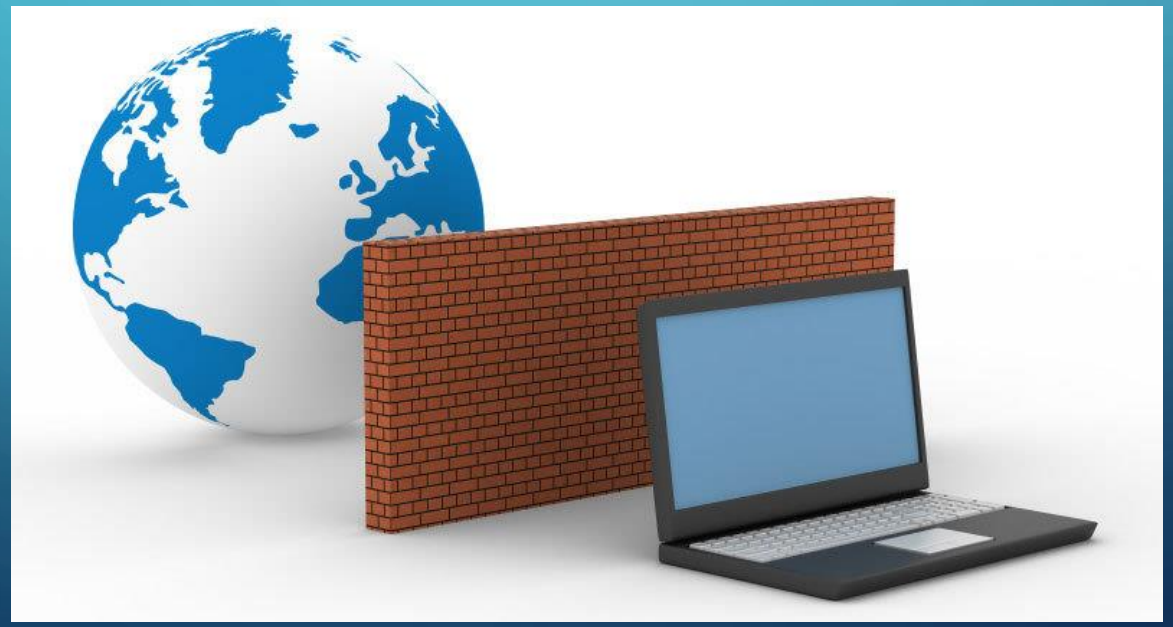


# ИСТОРИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х, когда Интернет был новшеством и не использовался в глобальных масштабах. Этими устройствами были маршрутизаторы, инспектирующие трафик на основании данных, содержащихся в заголовках протоколов сетевого уровня. Впоследствии, с развитием сетевых технологий, данные устройства получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого, транспортного уровня. Маршрутизаторы можно считать первой программно-аппаратной реализацией межсетевого экрана.

# ИСТОРИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Программные межсетевые экраны появились существенно позже и были гораздо моложе, чем антивирусные программы. Например, проект Netfilter/iptables (один из первых программных межсетевых экранов, встраиваемых в ядро Linux с версии 2.4) был основан в 1998 году. Такое позднее появление вполне объяснимо, так как долгое время антивирус решал проблему защиты персональных компьютеров от вредоносных программ. Однако в конце 1990-х вирусы стали активно использовать отсутствие межсетевых экранов на компьютерах, что привело к повышению интереса пользователей к данному классу устройств

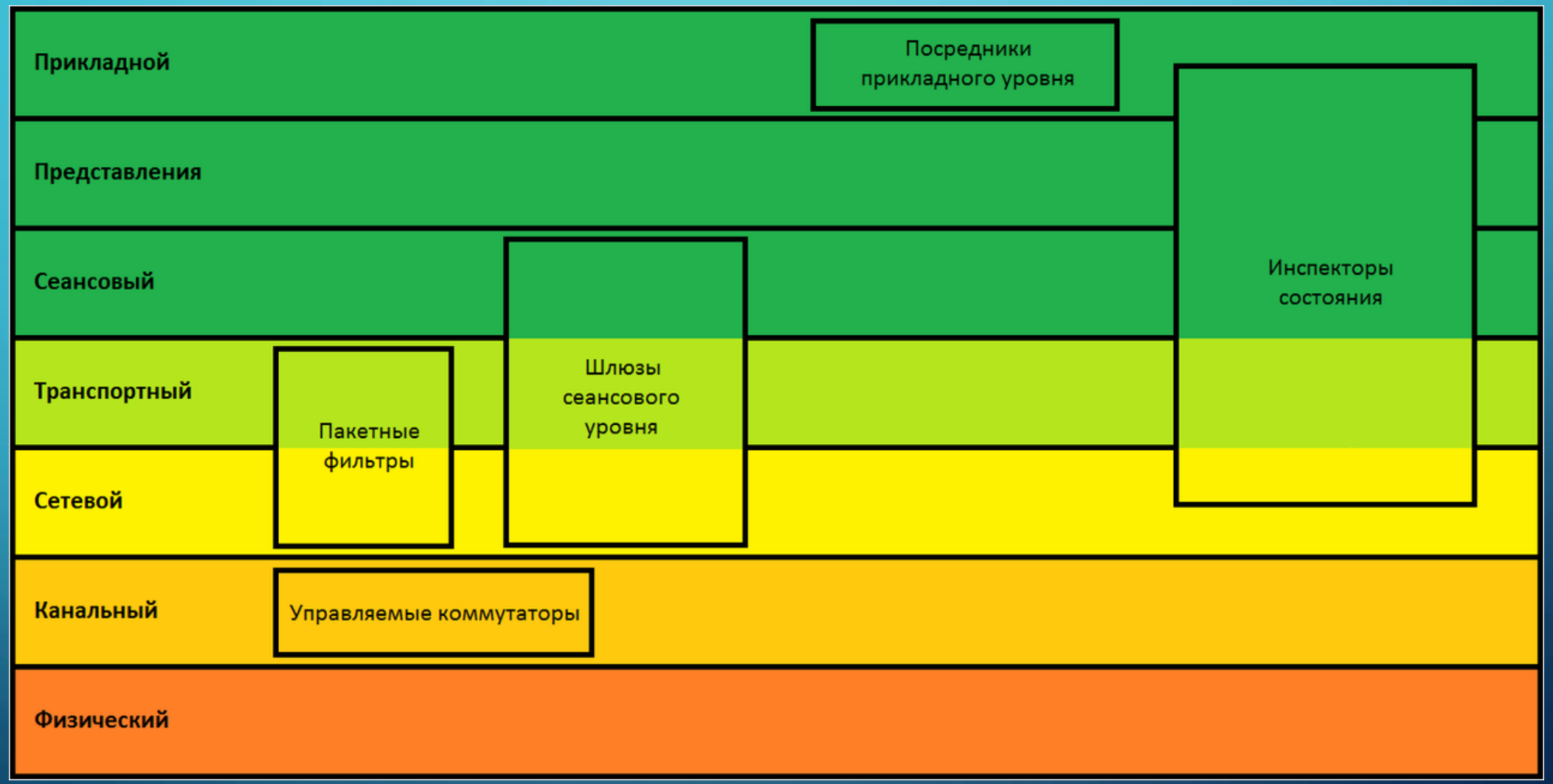


# КЛАССИФИКАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Однако в большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при их классификации. Учитывая данную модель, различают следующие типы межсетевых экранов:

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.

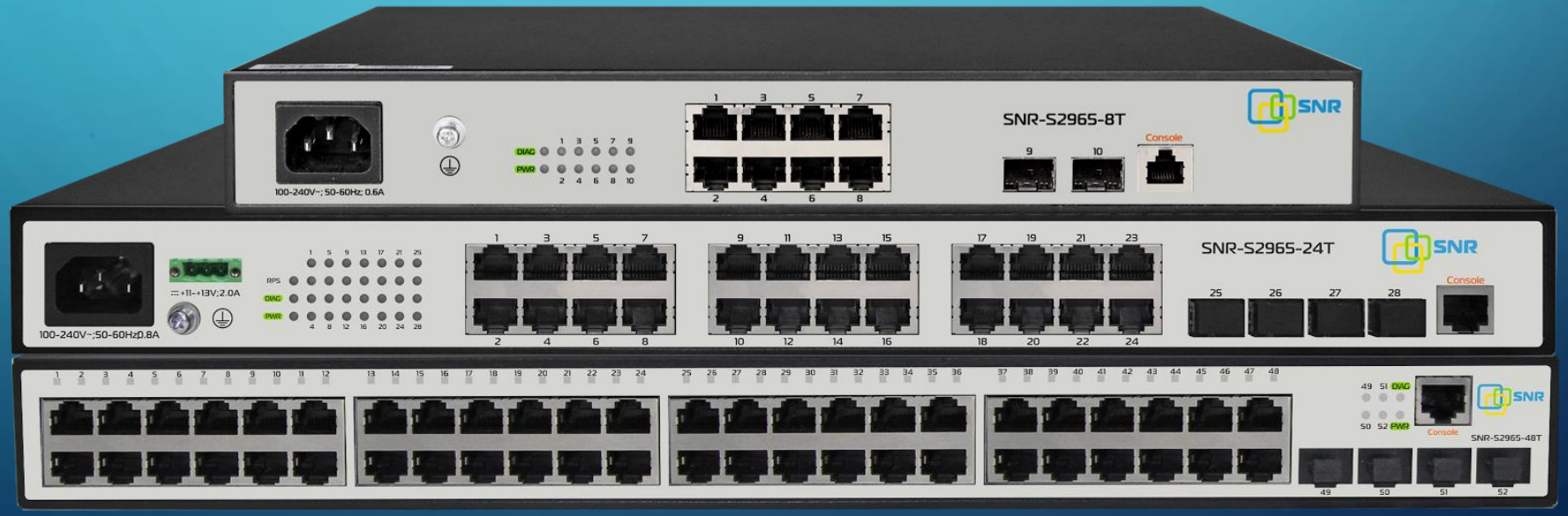
# КЛАССИФИКАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ




Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

# УПРАВЛЯЕМЫЕ КОММУТАТОРЫ

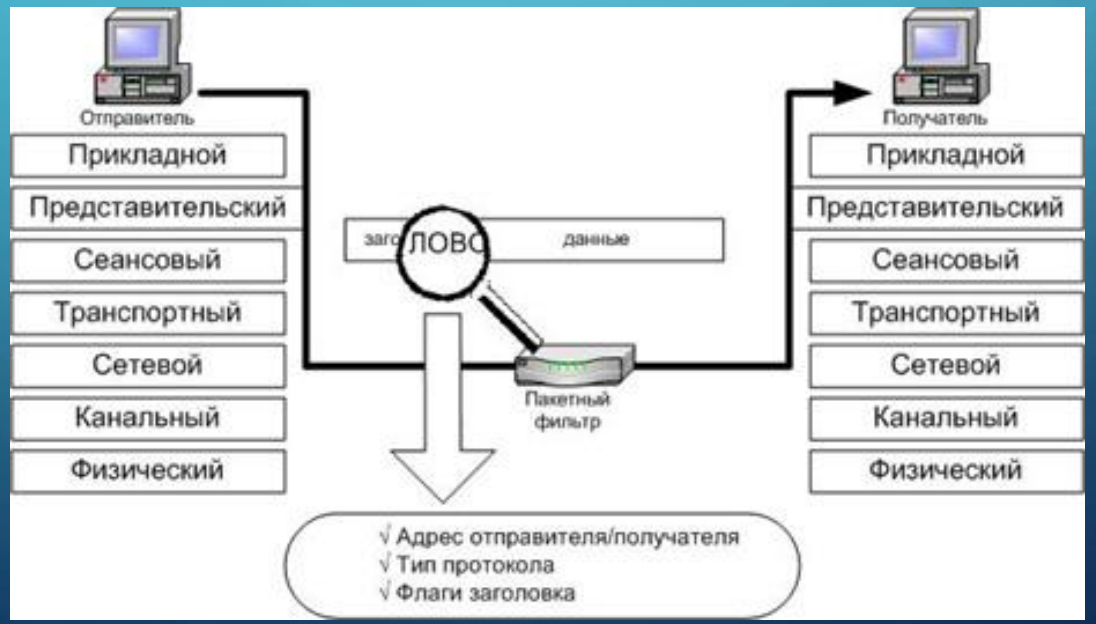
Управляемые коммутаторы иногда причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они работают на канальном уровне и разделяют трафик в рамках локальной сети, а значит не могут быть использованы для обработки трафика из внешних сетей (например, из Интернета)




Управляемый коммутатор доступа SNR-S2965

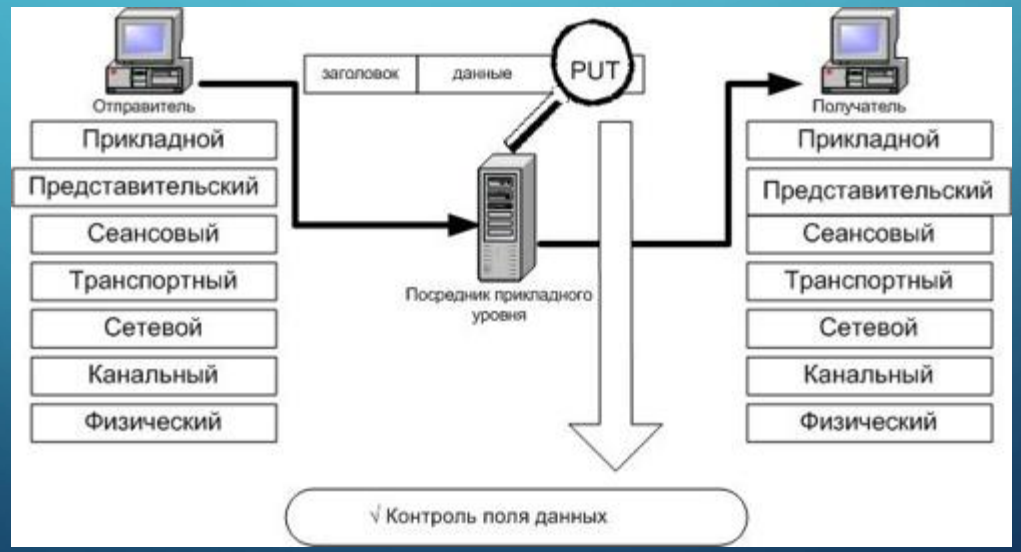
# ПАКЕТНЫЕ ФИЛЬТРЫ

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP или UDP). Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространённым их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах.



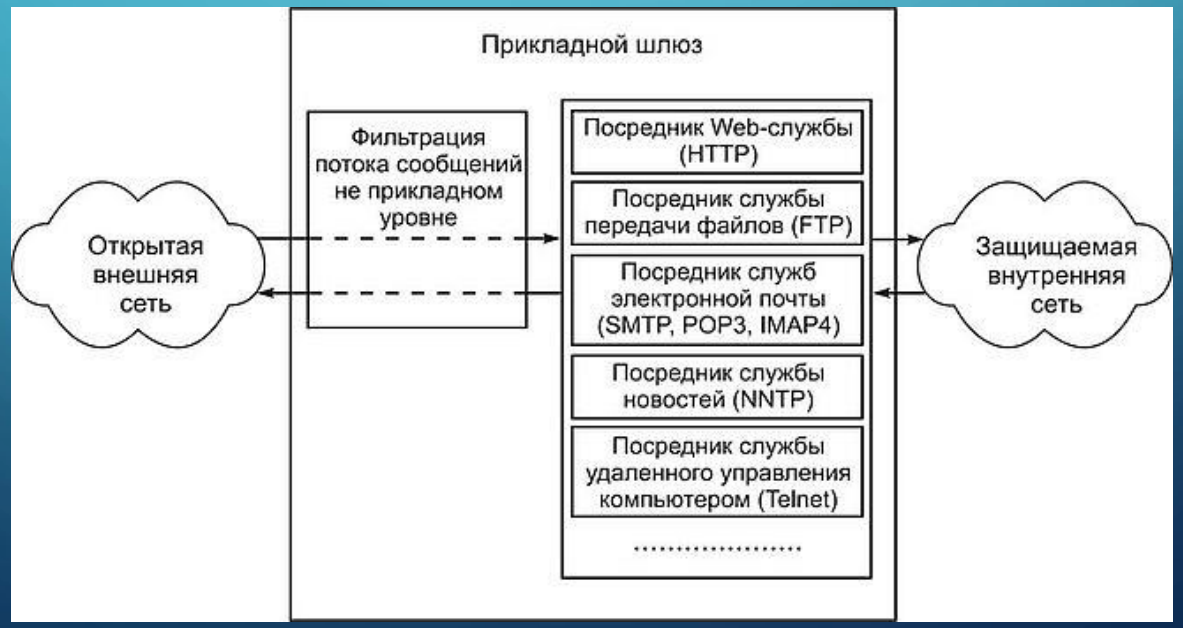
# ШЛЮЗЫ СЕАНСОВОГО УРОВНЯ

Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Как только приходит запрос на установление соединения, в специальную таблицу помещается соответствующая информация. В случае, если соединение установлено, пакеты, передаваемые в рамках данной сессии, будут просто копироваться в локальную сеть без дополнительной фильтрации. Когда сеанс связи завершается, сведения о нём удаляются из данной таблицы. Поэтому все последующие пакеты, «притворяющиеся» пакетами уже завершённого соединения, отбрасываются.



# ПОСРЕДНИКИ ПРИКЛАДНОГО УРОВНЯ

Межсетевые экраны прикладного уровня, к которым, в частности, относится файрвол веб-приложений, как и шлюзы сеансового уровня, исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников, каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, что зачастую означает DoS-атаку, либо запрещать использование некоторых команд.



# ИНСПЕКТОРЫ СОСТОЯНИЯ

Каждый из вышеперечисленных типов межсетевых экранов используется для защиты корпоративных сетей и обладает рядом преимуществ. Однако, куда эффективней было бы собрать все эти преимущества в одном устройстве и получить межсетевой экран, осуществляющий фильтрацию трафика с сетевого по прикладной уровень. Данная идея была реализована в инспекторах состояний, совмещающих в себе высокую производительность и защищённость. Данный класс межсетевых экранов позволяет контролировать:

- каждый передаваемый пакет — на основе таблицы правил;
- каждую сессию — на основе таблицы состояний;
- каждое приложение — на основе разработанных посредников.

# РЕАЛИЗАЦИЯ

Существует два варианта исполнения межсетевых экранов — программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности — в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

Логотип брандмауэра Windows


Маршрутизатор со встроенным межсетевым экраном


Специализированное устройство с межсетевым экраном (security appliance)

# ПРОГРАММНЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это вызвано тем, что для его применения достаточно, казалось бы, всего лишь приобрести программное обеспечение межсетевого экрана и установить на любой имеющийся в организации компьютер. Однако, как показывает практика, в организации далеко не всегда находится свободный компьютер, да ещё и удовлетворяющий достаточно высоким требованиям по системным ресурсам. После того, как компьютер всё-таки найден (чаще всего — куплен), следует процесс установки и настройки операционной системы, а также, непосредственно, программного обеспечения межсетевого экрана.

# ПРОГРАММНО-АППАРАТНЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

всё большее распространение стали получать специализированные программно-аппаратные комплексы, называемые security appliance, на основе, как правило, FreeBSD или Linux, «урезанные» для выполнения только необходимых функций. Достоинствами данных решений являются:

- Простота внедрения: данные устройства имеют предустановленную и настроенную операционную систему и требуют минимум настроек после внедрения в сеть.
- Простота управления: данными устройствами можно управлять откуда угодно по стандартным протоколам, таким как SNMP или Telnet, либо посредством защищённых протоколов, таких как SSH или SSL.
- Производительность: данные устройства работают более эффективно, так как из их операционной системы исключены все неиспользуемые сервисы.
- Отказоустойчивость и высокая доступность: данные устройства созданы выполнять конкретные задачи с высокой доступностью.


Спасибо за внимание