1. Как настроить в Linux прием и передачу тегированного трафика?

– Сначала необходимо установить утилиту vlan, затем указать в

/etc/network/interfaces VLAN ID, IP-адрес, маску подсети и физический сетевой

интерфейс для виртуального сетевого интерфейса, затем необходимо

перезапустить устройство для сохранения настроек.

2. Какие есть варианты разграничения компьютеров в сети?

– Настройка правил доступа к каждому узлу на всех узлах сети,

физическое разделить общей сеть на несколько сетей, настройка VLAN

3. Что такое VLAN? Для чего он нужен?

– (Виртуальная локальная сеть) - логическая группа узлов сети, трафик

которой, в том числе и широковещательный, полностью изолирован от других

узлов сети на канальном уровне. Служит VLAN для разграничения

компьютеров в сети, ограничения распространения широковещательного

трафика, повышения безопасности сети.

4. Как выполняется маршрутизация между разными VLAN?

– Через виртуальные сетевые интерфейсы, настроенные на

маршрутизаторе.

5. На каких узлах может быть настроен VLAN?

– VLAN может быть настроен как на маршрутизаторах и коммутаторах,

так и на отдельных ПК, оргтехнике и т.д.

6. Как настроить обмен данными между разными подсетями?

– Для обмена данными между разными VLAN, необходимо настроить

виртуальные сетевые интерфейсы на маршрутизаторе, через которые и будут

проходить пакеты.

1. Что позволяет делать сетевой экран?

– Сетевой экран осуществляет контроль и фильтрацию проходящего

через него сетевого трафика в соответствии с заданными правилами. Это

необходимо для того, чтобы блокировать вредоносный трафик, направленный

на различные сервисы, для обеспечения их бесперебойной работы и

своевременного ответа на легитимные запросы

2. Какие бывают типы сетевых экранов и чем они различаются?

– Типы сетевых экранов по их местоположению. Существует два

основных варианта расположения сетевого экрана: host-based и network-based.

Host-based сетевой экран – это экран, который располагается на самой системе,

где необходимо фильтровать трафик. Network-based-экран устанавливается на

промежуточных узлах между защищаемыми ресурсами и другими узлами.

Типы сетевых экранов по глубине анализа трафика. Первый анализирует

только заголовки пакетов и может работать на транспортном, сетевом и

канальном уровнях иерархии DoD (TCP/IP). Второй тип межсетевого экрана

может анализировать данные в пакете и работает на прикладном уровне

иерархии DoD (TCP/IP).

3. Приведите примеры, когда лучше использовать сетевые экраны host-

based.

– Host-based сетевые экраны позволяют гибко и удобно настраивать

правила на конкретном компьютере, упрощая тем самым процесс настройки и

обслуживания системы фильтрации. Примером может послужить домашний

персональный компьютер.

4. Каким типом сетевого экрана является iptables?

– Типом, который анализирует только заголовки пакетов и может

работать на транспортном, сетевом и канальном уровнях иерархии DoD

(TCP/IP).

5. Каковы минусы использования proxy-сервера в качестве сетевого

экрана?

– Внешние узлы proxy-сервера обычно предоставляются сторонними

компаниями, предлагающими «очистку данных». Такой подход позволяет

снизить нагрузку на администрирование и настройку сетевого экрана, однако

конфиденциальные данные при передаче их через внешний proxy-сервер могут

быть перехвачены.

6. Для чего нужна таблица NAT в iptables?

– nat – просматривает только пакеты, создающие новое соединение

(согласно системе определения состояний). Поддерживает действия DNAT,

SNAT, MASQUERADE, REDIRECT. Содержит цепочки PREROUTING,

OUTPUT и POSTROUTING

7. Чем DROP отличается от REJECT?

– Действие DROP просто останавливает дальнейшую работу с пакетом.

REJECT генерирует ответ отправителю о блокировке пакета.

8. Какую цепочку лучше использовать, чтобы заблокировать доступ с

ПК на ресурс во внешней сети?

– Лучше использовать цепочку OUTPUT – для пакетов, генерируемых

локальными процессами

9. Можно ли использовать несколько типов сетевых экранов для защиты

корпоративных сетей и узлов и почему/для чего?

– Можно, например для того чтобы защитить все узлы корпоративной

сети от DDoS атак, можно применить Network–based тип сетевых экранов, а

для конкретных узлов в корпоративной сети настроить Host–based тип,

например на узлах работников запретить доступ к социальным сетям, а на

узлах руководства не запрещать.