Сеть в Linux. Удаленный доступ.

SKILLFACTORY

Содержание

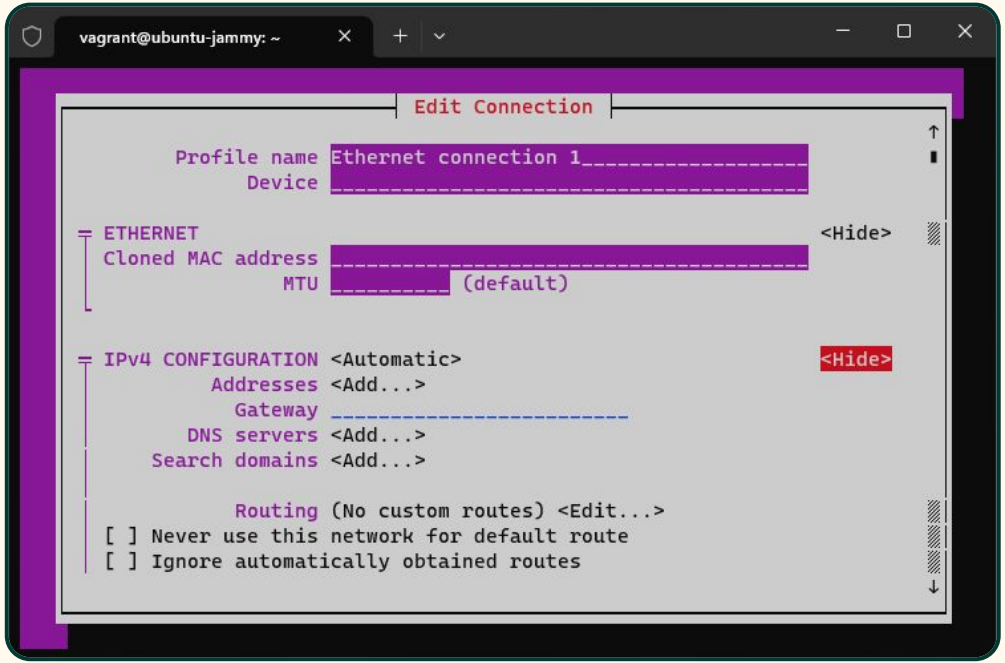
- Network-manager — управление сетью
- VPN — Wireguard, OpenVPN
- Удаленный доступ — SSH, XRDP, VNC
- Межсетевой экран — Iptables и ufw

Управление сетью

Network–manager – системная сетевая служба для управления сетевыми устройствами.

Функции:

- ➔ Wi–Fi подключение.
- ➔ Подключение к WWAN.
- ➔ Ethernet–подключение.
- ➔ Создание точки доступа.
- ➔ Общее подключение.



Работа с сетью

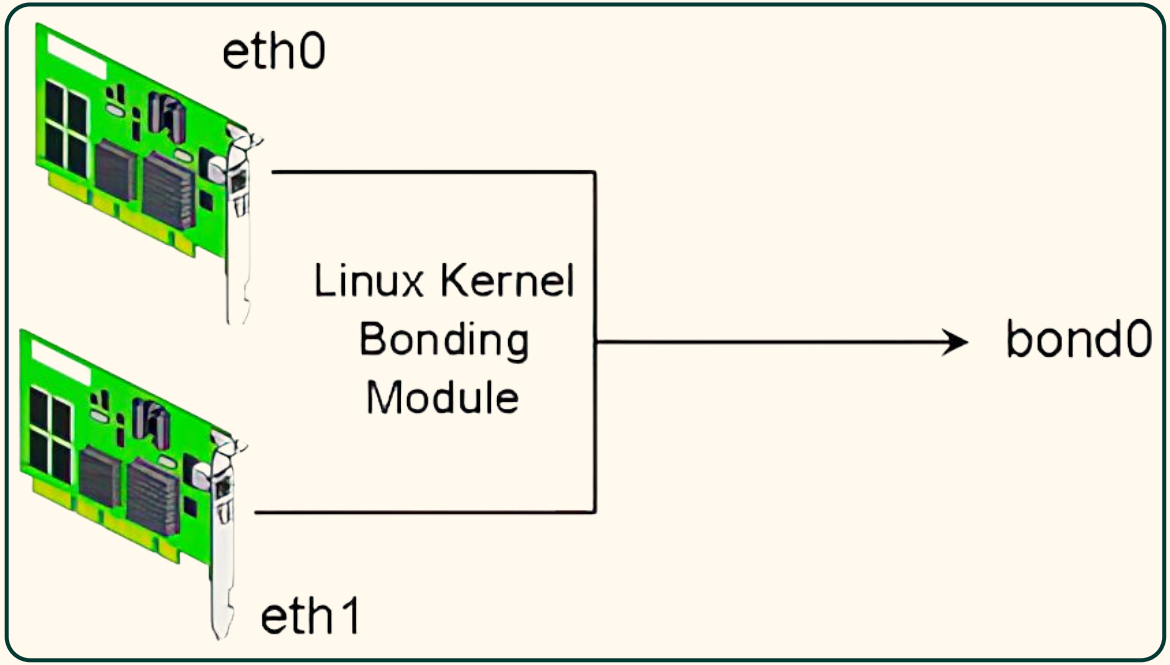
- **ping** – проверка доступности хоста.
- **traceroute** – трассировка маршрута до определенного хоста.
- **ip** – базовая утилита для управления сетью.
- **nslookup** – интерактивные запросы к DNS.
- **nmap** – сканирование сети и портов.
- **dig** – запрос информации о домене.
- **mtr** – отображение статистики трассировки.
- **tcpdump** – анализатор заголовков пакетов.
- **wget** – скачать файл.
- **netstat** – отображение статистики сети.
- **host** – информация о домене.
- **nc** – прослушивание порта, создание соединения TCP/UDP.

Конфигурационные файлы

- **/etc/hosts** – перечень IP адресов и соответствующих им имен.
- **/etc/networks –** определяет порядок поиска имени хоста/сети.
- **/etc/resolv.conf** – содержит список DNS серверов.
- **/etc/nsswitch.conf –** определяет порядок поиска имени хоста/сети.
- **/etc/netplan/*** – конфигурационные файлы сетевых интерфейсов.
- **/etc/network/interface** – конфигурации сетевых интерфейсов (используется в предыдущих версиях и Debian).

Linux Bond

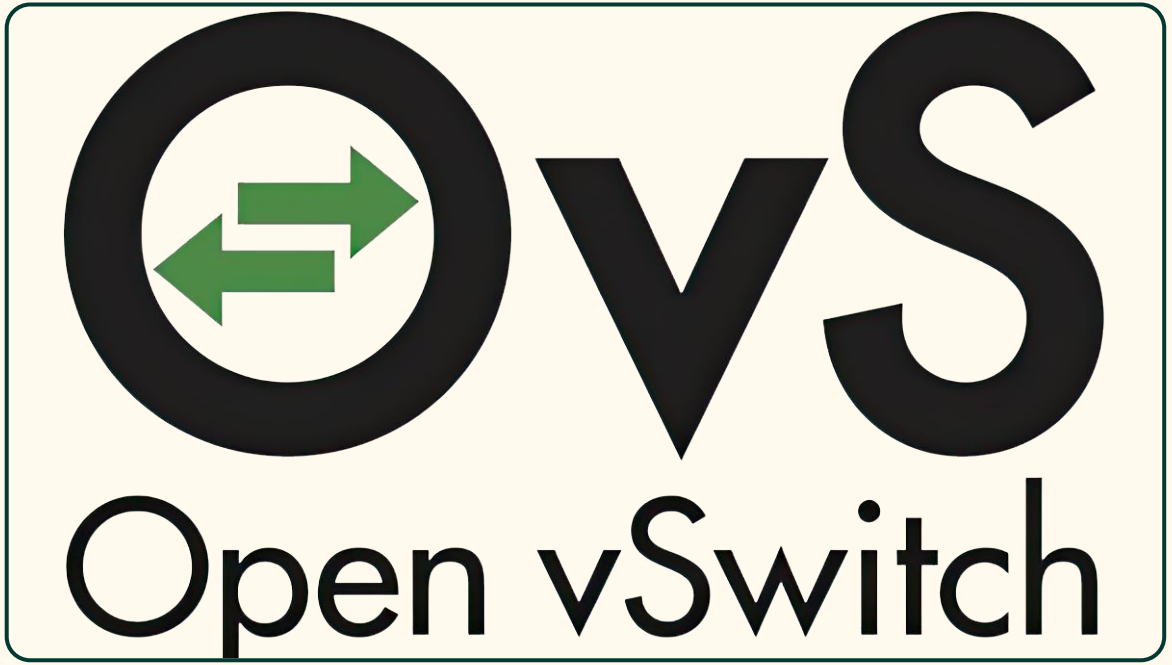
Механизм объединения сетевых интерфейсов в Linux для повышения пропускной способности и отказоустойчивости сети.



OpenSwitch

Возможности:

- ➔ LACP (IEEE 802.1AX–2008)
- ➔ 802.1Q VLAN
- ➔ IPv6 support
- ➔ Per VM interface traffic policing
- ➔ Multicast snooping
- ➔ .....



Содержание

- Network-manager — управление сетью
- VPN — Wireguard, OpenVPN
- Удаленный доступ — SSH, XRDP, VNC
- Межсетевой экран — Iptables и ufw

OpenVPN

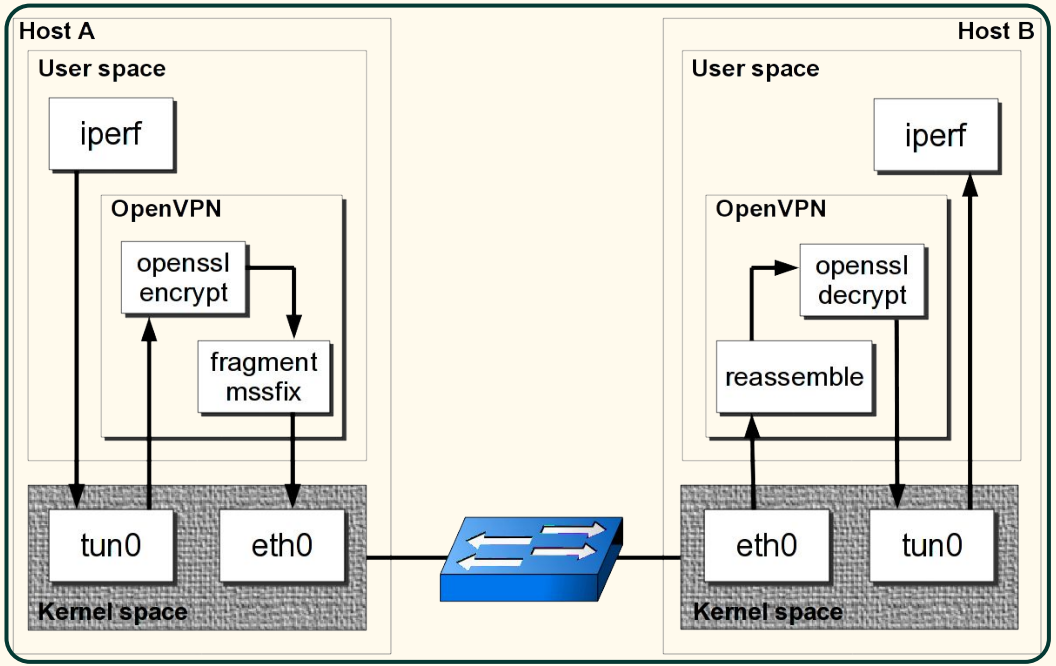
Свободная реализация технологии виртуальной частной сети с открытым исходным кодом для создания зашифрованных каналов типа точка–точка или сервер–клиенты между компьютерами.

Работает на уровнях 2 и 3 модели OSI

OpenVPN

Возможности:

- ➔ шифрование с использованием TLS.
- ➔ поддержка 802.11Q.
- ➔ гибкая настройка системы аутентификации.
- ➔ работа через UDP или TCP.
- ➔ мультиплатформенность.

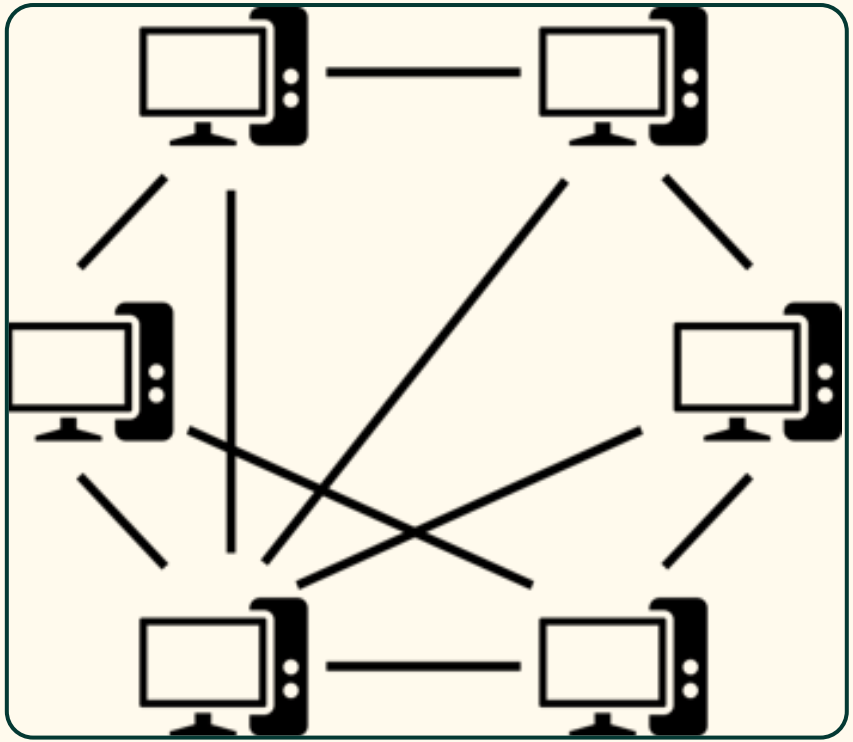


Wireguard

Возможности:

- ➔ простой в настройке;
- ➔ маленький объем кодой базы;
- ➔ мультиплатформенность;
- ➔ высокая скорость работы.

Работает на 3 уровне модели OSI.



Содержание

- Network-manager — управление сетью
- VPN — Wireguard, OpenVPN
- Удаленный доступ — SSH, XRDP, VNC
- Межсетевой экран — Iptables и ufw

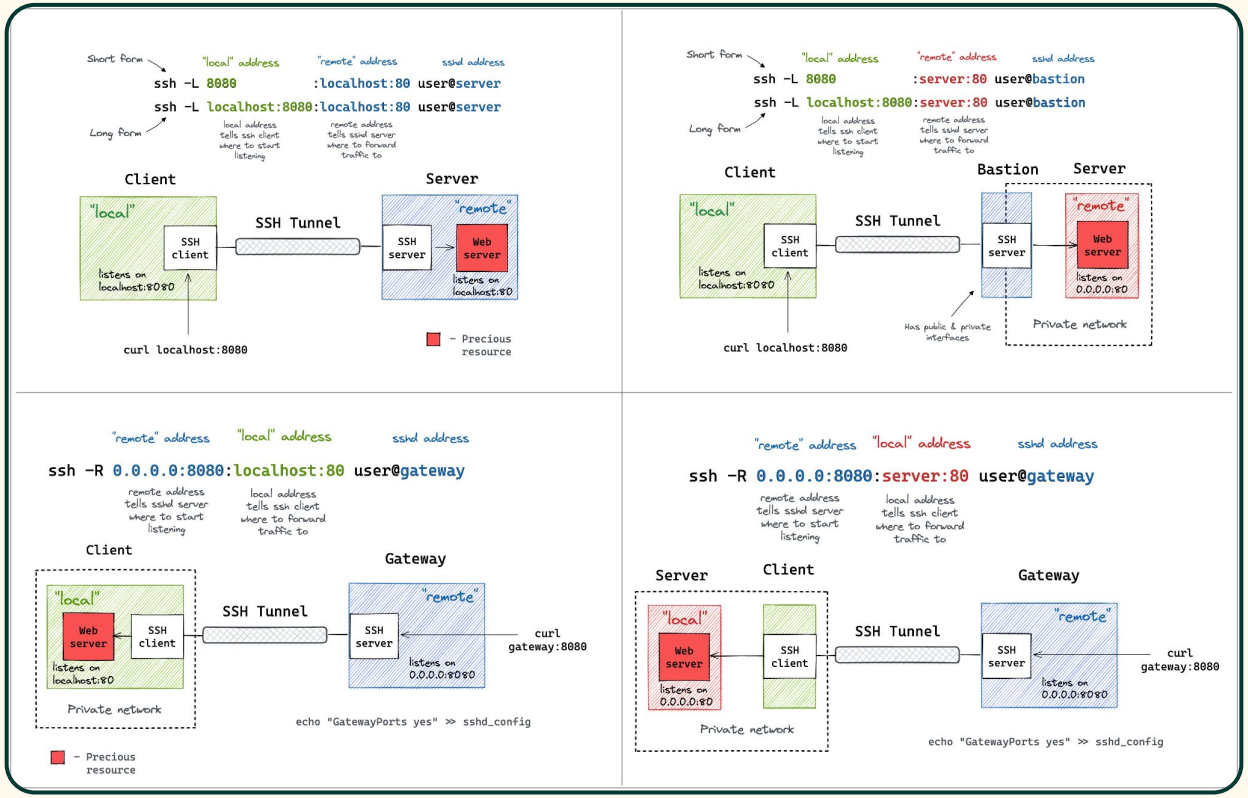
SSH

Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP–соединений.

Возможности:

- ➔ Безопасный удаленный вход в систему
- ➔ Безопасная передача файлов
- ➔ Безопасное удаленное выполнение команд
- ➔ Гибкая система аутентификации
- ➔ Контроль доступа
- ➔ Проброс портов

SSH туннелирование



RDP, VNC

RDP - протокол удаленного рабочего стола.

FreeRDP – реализация с открытым исходным кодом.

Хорошо совместим с ОС семейства Windows.

VNC - система удалённого доступа к рабочему столу компьютера, использующая протокол RFB.

Легковесное программное обеспечение для задач администрирования с открытым исходным кодом.

Содержание

- Network-manager — управление сетью
- VPN — Wireguard, OpenVPN
- Удаленный доступ — SSH, XRDP, VNC
- Межсетевой экран — Iptables и ufw

Iptables

Встроенный межсетевой экран в Linux. Обеспечивает проверку пакетов и их обработку в соответствии с заданными цепочками правил в системе.

Виды правил:

- ➔ input – входящие пакеты и подключения.
- ➔ forward – пересылаемые пакеты
- ➔ output – исходящие пакеты и сведения.
- ➔ prerouting – предобработка пакета.
- ➔ postrouting – все пакеты после цепочки forward.

Iptables

Действия:

- ➔ ACCEPT – разрешить пакет.
- ➔ DROP – отбросить пакет.
- ➔ REJECT – отклонить пакет и вывести сообщение пользователю.
- ➔ LOG – сделать запись о пакете в лог файл.
- ➔ QUEUE – отправить пакет пользовательскому приложению.

Таблицы – уровень абстракции выше уровня цепочки правил. Используются для выполнения действий над пакетами.

Виды таблиц:

- ➔ **raw** – для обработки сырых пакетов;
- ➔ **mangle** – для модификации пакетов;
- ➔ **nat** – преобразование сетевых адресов;
- ➔ **filter** – фильтрация пакетов.

Iptables

$ iptables –t таблица действие цепочка дополнительные_параметры

Действие:

- **–A** – добавить правило в цепочку
- **–C** – проверить все правила
- **–D** – удалить правило
- **–I** – вставить правило с нужным номером
- **–L** – вывести все правила в текущей цепочке
- **–S** – вывести все правила
- **–F** – очистить все правила
- **–N** – создать цепочку
- **–X** – удалить цепочку
- **–P** – установить действие по умолчанию

Доп. параметры:

- **–p** – указать протокол, один из tcp, udp, udplite, icmp, icmpv6, esp, ah, sctp, mh
- **–s** – указать ip адрес устройства–отправителя пакета
- **–d** – указать ip адрес получателя
- **–i** – входной сетевой интерфейс
- **–o** – исходящий сетевой интерфейс
- **–j** – выбрать действие, если правило подошло

UFW

Uncomplicated FireWall – надстройка над Iptables для простой работы с правилами.

$ ufw опции действие параметры

Опции:

- ➔ **—version** – вывести версию брандмауэра
- ➔ **—dry–run** – тестовый запуск, никакие реальные действия не выполняются

Действия:

- ➔ **enable** – включить фаервол и добавить его в автозагрузку
- ➔ **disable** – отключить фаервол и удалить его из автозагрузки
- ➔ **reload** – перезагрузить файервол
- ➔ **default** – задать политику по умолчанию
- ➔ **logging** – включить журналирование или изменить уровень подробности
- ➔ **reset** – сбросить все настройки до состояния по умолчанию
- ➔ **status** – посмотреть состояние фаервола
- ➔ **show** – посмотреть один из отчётов о работе
- ➔ **allow** – добавить разрешающее правило
- ➔ **deny** – добавить запрещающее правило
- ➔ **reject** – добавить отбрасывающее правило
- ➔ **limit** – добавить лимитирующее правило
- ➔ **delete** – удалить правило

UFW

$ ufw allow имя_службы
$ ufw allow порт

$ ufw allow порт/протокол
$ ufw allow направление порт

$ ufw allow in on ethin out on ethout from ip_источника

$ ufw allow proto протокол from ip_источника to ip_назначения port порт_назначения

Ссылки

- Сетевые адаптеры VirtualBox
- Управление сетью в Ubuntu
- OpenvSwitch
- Ubuntu Bonding
- Настройка UFW
- Настройка Iptables
- Установка Freerdp
- Настройка VNC
- Настройка Wireguard
- Безопасная настройка SSH