есть машина не настроенная (интерфейсы не настроены ) Linux Debian, требуется Создание маршрутизатор который объединяет локальные сети к нему подключены следующие локальные сети :

|  |
| --- |
| 1:linuxClient interface = eth3  2:WindowsClient interface = eth2  3:srv interface = eth1  4:Network interface = eth0 |

В сети номер 3 находится контроллер доменов на базе windows server 2019

И машина с веб сайтом

В сети номер 4 сеть подключённая к интернету

В сети номер 2 клиенты на windows

В сети номер 1 клиенты на linux

Необходимо настроить DHSP , NAT , Site to site vpn ,настроить интерфейсы

Для настройки маршрутизатора на Linux Debian для объединения четырех локальных сетей (linuxClient, WindowsClient, srv, Network) и обеспечения доступа к контроллеру домена и веб-сайту на машине, а также доступу в Интернет, следует выполнить следующие шаги:

1 Настройте интерфейсы для каждой локальной сети, чтобы машина могла связываться с устройствами в каждой сети. Для этого в файле /etc/network/interfaces нужно добавить секции для каждого интерфейса с настройками IP-адреса, маски подсети и шлюза по умолчанию. Например, для интерфейса, подключенного к локальной сети linuxClient:

|  |
| --- |
| auto eth3  iface eth3 inet static  address 10.0.4.1  netmask 255.255.255.0 |

Аналогично настройте оставшиеся интерфейсы.

Или sudo ifconfig имя ip-адрес netmask 255.255.255.0

**Назначьте адрес основного шлюза.** Введите route add default gw 192.168.1.1

2 Установите DHCP-сервер, чтобы автоматически назначать IP-адреса устройствам в каждой локальной сети. Для этого можно использовать пакет isc-dhcp-server. В файле /etc/dhcp/dhcpd.conf нужно добавить конфигурацию для каждой сети. Например, для сети linuxClient:

subnet 10.0.4.0 netmask 255.255.255.0 {

range 10.0.4.100 10.0.4.200;

option routers 10.0.4.1;

option domain-name-servers 8.8.8.8, 8.8.4.4;

}

|  |
| --- |
|  |

После того как вы отредактировали основной файл конфигурации и объявили  диапазоны IP, откройте файл **/etc/default/isc-dhcp-server** и замените параметр **INTERFACESv4** на имя сетевого интерфейса, который смотрит внутрь сети. Чтобы узнать его имя воспользуйтесь командами  **ipconfig** или **ip.**

**Или etc/dhsp/dhcpd.conf**

3 Настройте NAT (Network Address Translation) для обеспечения доступа к Интернету для устройств в каждой локальной сети. Для этого можно использовать утилиту iptables. В файле /etc/sysctl.conf нужно разрешить пересылку пакетов между интерфейсами с помощью строки:

net.ipv4.ip\_forward=1

Затем в терминале выполните следующие команды:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables-save > /etc/iptables/rules.v4

4 Настройте Site-to-Site VPN для объединения сетей. Для этого можно использовать пакет OpenVPN. Создайте сервер OpenVPN на маршрутизаторе и добавьте клиентов с других машин, которые будут подключаться к серверу. Подробные инструкции по настройке OpenVPN можно найти в официальной документации.

Для настройки Site-to-Site VPN с помощью OpenVPN на маршрутизаторе Debian, следуйте этим инструкциям:

Установите пакет OpenVPN на маршрутизатор Debian:

sudo apt-get update

sudo apt-get install openvpn

Создайте каталог для конфигурационных файлов OpenVPN:

sudo mkdir /etc/openvpn/server

Скопируйте файл конфигурации по умолчанию в каталог сервера OpenVPN:

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/server/

sudo gzip -d /etc/openvpn/server/server.conf.gz

Отредактируйте файл конфигурации сервера /etc/openvpn/server/server.conf. Некоторые настройки, которые вам может потребоваться изменить, приведены ниже:

local <IP-адрес маршрутизатора> # IP-адрес маршрутизатора

port 1194 # порт, на котором будет работать сервер OpenVPN

proto udp # протокол, используемый для соединения

dev tun # тип устройства для туннеля (TUN или TAP)

ca /etc/openvpn/server/ca.crt # путь к сертификату авторизации

cert /etc/openvpn/server/server.crt # путь к сертификату сервера

key /etc/openvpn/server/server.key # путь к ключу сервера

dh /etc/openvpn/server/dh.pem # путь к файлу DH-параметров

server 10.8.0.0 255.255.255.0 # сеть и маска подсети VPN

push "route 10.0.1.0 255.255.255.0" # маршрут до сети linuxClient

push "route 10.0.2.0 255.255.255.0" # маршрут до сети WindowsClient

push "route 10.0.3.0 255.255.255.0" # маршрут до сети srv

push "redirect-gateway def1" # перенаправление трафика клиента через VPN

Создайте файл DH-параметров:

sudo openssl dhparam -out /etc/openvpn/server/dh.pem 2048

Создайте сертификат авторизации и сертификат сервера для OpenVPN:

cd /etc/openvpn/easy-rsa/

sudo ./easyrsa init-pki

sudo ./easyrsa build-ca

sudo ./easyrsa gen-req server nopass

sudo ./easyrsa sign-req server server

sudo cp pki/ca.crt /etc/openvpn/server/

sudo cp pki/issued/server.crt /etc/openvpn/server/

sudo cp pki/private/server.key /etc/openvpn/server/

Создайте клиентские сертификаты на других машинах, которые будут подключаться к серверу OpenVPN. Для этого можно использовать утилиту easy-rsa, как и в предыдущем шаге.

Запустите сервер OpenVPN:

sudo systemctl start openvpn-server@server

5 Настройте доступ к контроллеру домена и веб-сайту. Для этого можно использовать прямой маршрут (без NAT )

6 Настройте статические маршруты для доступа к контроллеру домена и веб-сайту из каждой локальной сети. Например, для доступа к контроллеру домена с IP-адресом 192.168.0.10:

Для сети linuxClient:

route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.4.1

Для сети WindowsClient:

route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.3.1

Для сети srv:

route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.2.1

Для сети Network:

route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.1.1

7 Проверьте доступность контроллера домена и веб-сайта из каждой локальной сети.

8 Настройте DNS-сервер, чтобы устройства в каждой локальной сети могли разрешать имена хостов. Для этого можно использовать пакет bind9. В файле /etc/bind/named.conf.local нужно добавить зоны для каждой локальной сети. Например, для сети linuxClient:

zone "linuxclient.local" {

type master;

file "/etc/bind/db.linuxclient.local";

};

Создайте файл /etc/bind/db.linuxclient.local с записями DNS для сети linuxClient.

Аналогично настройте DNS для остальных локальных сетей.

9 Проверьте разрешение имен хостов из каждой локальной сети.

10 Дополнительно можно настроить брандмауэр (например, утилиту ufw) для обеспечения безопасности маршрутизатора.

11 запуск всех служб

1. Остановите службу **isc-dhcp-server**:

sudo systemctl stop isc-dhcp-server.service

Если не пингует

Настройте правила маршрутизации для пересылки пакетов между сетями. Для этого используйте команду iptables. Например, чтобы разрешить доступ из сети 1 (192.168.4.0/24) к сети

2 (192.168.3.0/24), выполните следующую команду:

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -d 192.168.3.0/24 -j MASQUERADE