1. Настройка NAT(SNAT) для доступа в Интернет в маршрутизаторе vESR.

**NAT (Network Address Translation) — это механизм преобразования локальных (частных) IP-адресов в глобальные (публичные) и наоборот**. Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз и обеспечивает безопасность сети.

**Процесс работы NAT**:

1. **Устройство отправляет запрос в интернет**. Оно использует внутренний IP-адрес, который уникален только внутри локальной сети.
2. **Когда пакет данных достигает маршрутизатора**, NAT заменяет внутренний IP-адрес на внешний IP-адрес маршрутизатора. При этом маршрутизатор запоминает, какой внутренний IP-адрес связан с каким внешним IP-адресом и портом.
3. **Когда ответ от сервера приходит обратно в сеть**, маршрутизатор использует свои таблицы NAT, чтобы направить пакет данных к правильному устройству в локальной сети, заменяя внешний IP-адрес обратно на внутренний.

Типы NAT

**Существует несколько типов NAT**:

* **Статический NAT (Static NAT)**. Создаёт постоянное соответствие между внутренним и внешним IP-адресами. Обычно используется для серверов, которые должны быть доступными из внешнего интернета, например, веб-серверов или почтовых серверов.
* **Динамический NAT (Dynamic NAT)**. Присваивает внутренним IP-адресам временные внешние IP-адреса из пула доступных адресов. Это позволяет множеству устройств в локальной сети использовать один внешний IP-адрес, но при этом адреса могут изменяться.
* **PAT (Port Address Translation), также известный как NAT Overload**. Позволяет множеству устройств использовать один внешний IP-адрес, отличая их по номерам портов. Это наиболее распространённый тип NAT.

Преимущества и недостатки NAT

**Преимущества NAT**:

* **Экономия IP-адресов**. NAT позволяет сократить потребность в публичных IP-адресах, так как несколько устройств в локальной сети могут использовать один и тот же публичный IP-адрес.
* **Повышение безопасности**. NAT скрывает внутреннюю структуру сети от внешних пользователей, что затрудняет несанкционированный доступ извне.
* **Управление трафиком**. NAT помогает управлять трафиком, направляя запросы к правильным устройствам в локальной сети.

**Недостатки NAT**:

* **Задержки в пути из-за преобразования**. Каждый сетевой пакет, покидающий локальную сеть и направляющийся в Интернет, должен пройти процесс перевода адресов на граничном маршрутизаторе.
* **Некоторые приложения не функционируют при включённом NAT**. Например, приложения, которые применяют передачу данных с использованием определённых портов или требуют прямого взаимодействия с уникальными IP-адресами.
* **Сложности с туннелированием протоколов, таких как IPsec**. NAT изменяет заголовки пакетов, а это может привести к проблемам с корректной передачей зашифрованных данных.

Используем схему подключения сетевых устройств , рассмотренную в предыдущей главе для настройки доступа с PC1 (172.16.1.100/24) и **PC2** (172.16.1.200/24) к публичной сети с использованием функции Source NAT, через ip-адрес виртуальный маршрутизатор vesr-1 который смотрит в настоящую сеть Интернет. Работу по настройке интерфейсов , назначение адресов и мэжсетевого экрана мы уже проделали в предыдущей главе, но сказано неоднократно было : «Повторение-мать учения», поэтому не будет нарушать традицию ( вводить снова эти команды в консоли маршрутизатора не обязательно):

Проверяем доступ к сети с устройства PC2:

PC2> ping 8.8.8.8

8.8.8.8 icmp\_seq=1 timeout

8.8.8.8 icmp\_seq=2 timeout

8.8.8.8 icmp\_seq=3 timeout

8.8.8.8 icmp\_seq=4 timeout

8.8.8.8 icmp\_seq=5 timeout

1. Назначаем IP-адреса на интерфейсы командами:

configure

* на интерфейс смотрящий в сторону глобальной сети получаем сетевые параметры по DHCP

interface gi1/0/1

description connection\_WAN

ip address dhcp

exit

* на интерфейс смотрящий в сторону PC1 и PC2 назначаем статический адрес из подсети 172.16.1.0/24

interface gi1/0/2

description connection\_LAN\_GATEWAY

ip address 172.16.1.1/24

exit

1. Создадим зону безопасности **«trusted»** и установим принадлежность интерфейса **gi1/0/2** (смотрящего в подсеть PC1 и PC2) командами:

security zone trusted

exit

interface gi1/0/2

security-zone trusted

exit

1. Создадим зону безопасности **«untrusted»** и установим принадлежность интерфейса **gi1/0/1** (смотрящего в настоящую сеть Интернет) командами:

security zone untrusted

exit

interface gi1/0/1

security-zone untrusted

exit

do commit

1. Для конфигурирования SNAT и настройки правил зон безопасности потребуется создать профиль адресов сети «LAN\_GATEWAY», включающий адреса, которым разрешен выход в публичную сеть, и профиль адреса публичной сети «WAN».

object-group network LAN\_GATEWAY

ip address-range 172.16.1.1-172.16.1.254 # указываем всю локальную сеть

exit

Вышеприведенные команды уже должны быть в конфигурационном файле виртуального маршрутизатора, поскольку мы их вводили ранее в предыдущей главе при настройке сервера DHCP. Проверить их наличие можно еоандой show run.

Для настройки NAT необходимо знать IP адрес интерфейса , «смотрящего» в Интернет. Для этого даем команду:

vesr-1# sh ip interfaces gigabitethernet 1/0/1

IP address Interface Adm in Link Type Precedence

--------------------------------------------------- -------------------- --- -- ----- ------- -----------

**192.168.10.74**/24 gi1/0/1 Up Up DHCP --

И копируем IP адрес.

А вот эту команду мы еще не вводили, открываем консоль и вводим команды:

configure

object-group network WAN

ip address-range 192.168.10.74 # IP-адрес - смотрящий в настоящую сеть Интернет

exit

do commit

do confirm

vesr-1# config

vesr-1(config)# object-group network WAN

vesr-1(config-object-group-network)# ip address-range 192.168.10.74

vesr-1(config-object-group-network)# exit

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-30T06:58:49+00:00 %CLI-I-CRIT: user admin from console input: do commit

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-30T06:58:58+00:00 %CLI-I-CRIT: user admin from console input: do confirm

vesr-1(config)#

1. Для пропуска трафика из зоны **trusted** в зону **untrusted** создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов LAN\_GATEWAY для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой enable:

security zone-pair trusted untrusted

rule 1

match source-address LAN\_GATEWAY

action permit

enable

exit

exit

do commit

do confirm

vesr-1(config)# security zone-pair trusted untrusted

vesr-1(config-security-zone-pair)# rule 1

vesr-1(config-security-zone-pair-rule)# match source-address object-group LAN\_GATEWAY

vesr-1(config-security-zone-pair-rule)# action permit

vesr-1(config-security-zone-pair-rule)# enable

vesr-1(config-security-zone-pair-rule)# exit

vesr-1(config-security-zone-pair)# exit

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-30T07:05:53+00:00 %CLI-I-CRIT: user admin from console input: do commit

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-30T07:05:59+00:00 %CLI-I-CRIT: user admin from console input: do confirm

vesr-1(config)#

1. Конфигурируем сервис SNAT. Первым шагом задаётся IP-адрес публичной сети (WAN), используемых для сервиса SNAT:

nat sourсe

pool WAN

ip address-range 192.168.10.74 # IP-адрес isp - смотрящий в настоящую сеть Интернет

exit

1. Создаём набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону **untrusted**. Правила включают проверку адреса источника данных на принадлежность к пулу **LAN\_GATEWAY**:

ruleset SNAT

to zone untrusted

rule 1

match source-address LAN\_GATEWAY

action source-nat pool WAN

enable

exit

exit

do commit

do confirm

vesr-1(config)#

vesr-1(config)# nat source

vesr-1(config-snat)# pool WAN

vesr-1(config-snat-pool)# ip address-range 192.168.10.74

vesr-1(config-snat-pool)# exit

vesr-1(config-snat)# ruleset SNAT

vesr-1(config-snat-ruleset)# to zone trusted

vesr-1(config-snat-ruleset)# rule 1

vesr-1(config-snat-rule)# match source-address object-group LAN\_GATEWAY

vesr-1(config-snat-rule)# action source-nat pool WAN

vesr-1(config-snat-rule)# enable

vesr-1(config-snat-rule)# exit

vesr-1(config-snat-ruleset)# exit

vesr-1(config-snat)# exit

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-30T07:09:54+00:00 %CLI-I-CRIT: user admin from console input: do commit

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-30T07:09:59+00:00 %CLI-I-CRIT: user admin from console input: do confirm

vesr-1(config)# exit

vesr-1#

**Проверяем с PC1 и PC2 доступ в Интернет**

PC1> ping ya.ru

ya.ru resolved to 77.88.44.242

84 bytes from 77.88.44.242 icmp\_seq=1 ttl=56 time=9.907 ms

84 bytes from 77.88.44.242 icmp\_seq=2 ttl=56 time=10.354 ms

84 bytes from 77.88.44.242 icmp\_seq=3 ttl=56 time=13.094 ms

84 bytes from 77.88.44.242 icmp\_seq=4 ttl=56 time=16.578 ms

84 bytes from 77.88.44.242 icmp\_seq=5 ttl=56 time=12.613 ms

**PC2> ping cisco.com**

**cisco.com resolved to 72.163.4.185**

**84 bytes from 72.163.4.185 icmp\_seq=1 ttl=46 time=163.881 ms**

**84 bytes from 72.163.4.185 icmp\_seq=2 ttl=46 time=163.377 ms**

**84 bytes from 72.163.4.185 icmp\_seq=3 ttl=46 time=164.746 ms**

**84 bytes from 72.163.4.185 icmp\_seq=4 ttl=46 time=164.599 ms**

**84 bytes from 72.163.4.185 icmp\_seq=5 ttl=46 time=163.202 ms**

**Проверяем таблицу преобразований адресов на vesr-1**

show ip nat translation

vesr-1# sh ip nat translations

Prot Inside source Inside destination Outside source Outside destination Pkts Bytes

---- --------------------- --------------------- --------------------- --------------------- ---------- ----------

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.100 77.88.55.242 192.168.10.74 77.88.55.242 -- --

icmp 172.16.1.100 77.88.55.242 192.168.10.74 77.88.55.242 -- --

icmp 172.16.1.100 77.88.55.242 192.168.10.74 77.88.55.242 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.100 77.88.55.242 192.168.10.74 77.88.55.242 -- --

icmp 172.16.1.100 77.88.55.242 192.168.10.74 77.88.55.242 -- --

udp 172.16.1.200:14503 77.88.8.8:53 192.168.10.74:14503 77.88.8.8:53 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

udp 172.16.1.100:28458 77.88.8.8:53 192.168.10.74:28458 77.88.8.8:53 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

icmp 172.16.1.200 72.163.4.185 192.168.10.74 72.163.4.185 -- --

В итоге такая конфигурация виртуального маршрутизатора достаточна для обеспечения минимально защищенного доступа в сеть Интернет сети домашнего офиса.