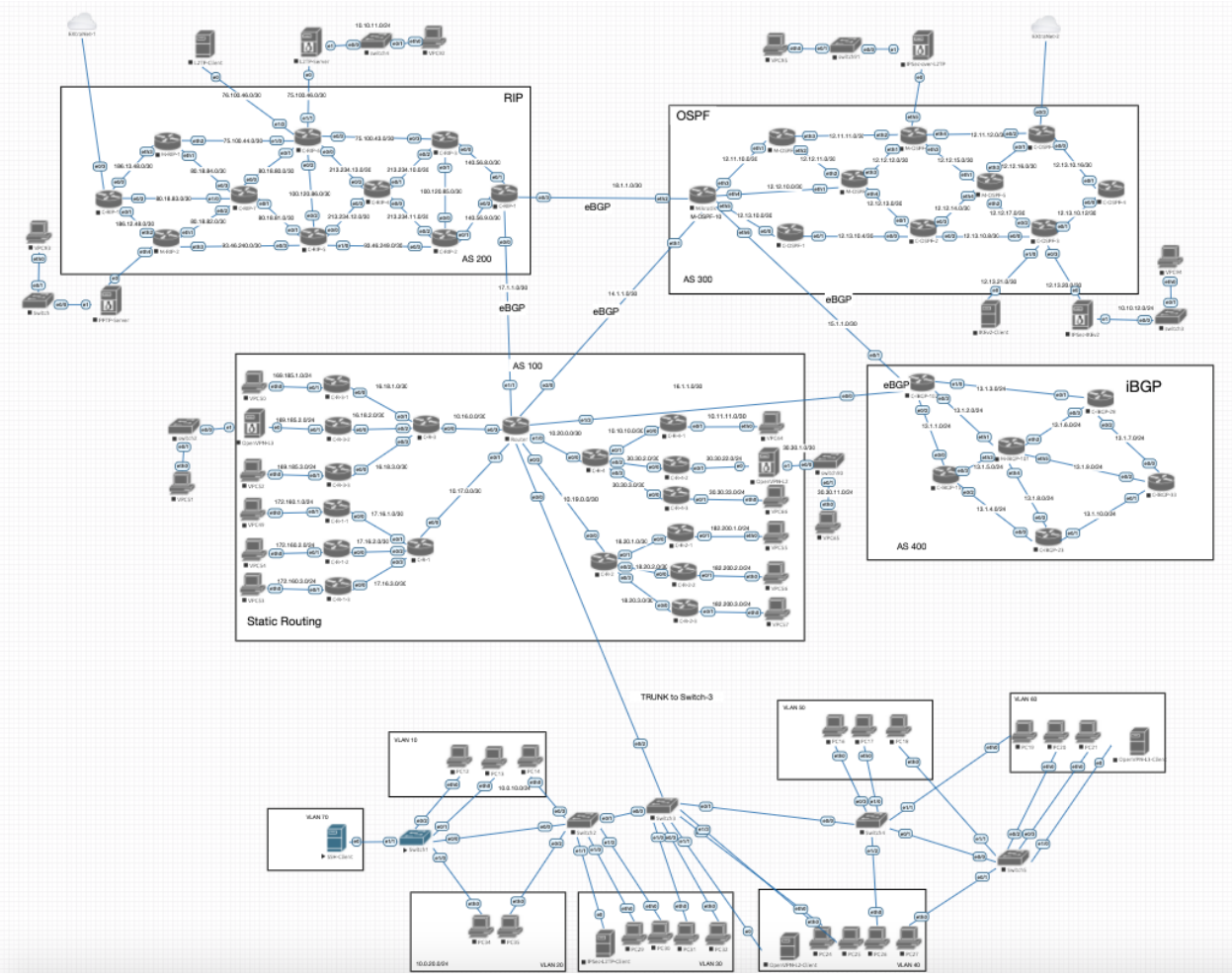
Отчёт по практической работе №4

Главная цель практической работы: научиться конфигурировать защищенный протокол удаленного управления SSH на оборудовании Cisco и Mikrotik, а также давать доступ оборудованию в интернет, используя технологию NAT.

Топология сети практической работы №4



Задание:

1. Настроить SSH на каждом сетевом устройстве таким образом, чтобы с устройства SSH-Client можно было подключиться по SSH к любому устройству в рамках всех лабораторных работ.

> Коммутаторы, которые представлены в лаборатории EVE-NG, имеют прошивку, не поддерживающую SSH. Как решение - можно воспользоваться протоколом telnet или заменить образ cisco_L2 на поддерживающий SSH (скачать образ можно тут).

2. Настроить технологию NAT на роутерах C-RIP-10 и C-OSPF-5.

Далее Настроить ACL на main роутере по следующим условиям:

1. Устройства из VLAN 10 **не доступны** по сети для устройств из VLAN 20,30…60.

2. Устройства из VLAN 10 **не могут** обращаться ни к одному ip адресу из чужих подсетей (изолированная сеть).

> Исключение: VLAN-70 может обращаться к устройствам из VLAN 10 по TCP портам 3389, 80, 22, 443, 445, а так же по icmp.

3. Устройства из VLAN 20 **могут** только **пинговать** (icmp) VLAN 30…70 (другие протоколы недоступны). До остальных сетей из vlan 20 доступ без ограничений.

4. Устройства из VLAN 30 **не имеют** сетевого доступа до AS400. До остальных сетей без ограничений.

5. Устройства из VLAN 50 **имеют** полный доступ на уровне коммутации (то есть до всех vlan, если выше не сказано иначе), а так же имеют доступ к домену статической маршрутизации. Соответственно сети RIP, OSPF, iBGP, Интернет оттуда не доступны.

6. Предусмотреть, что все VPC получают адреса по DHCP.

> Пояснения: К каждому пункту добавляйте фразу “если выше по пунктам не сказано иначе”. Это означает, что, например, первый пункт выполняется так, как написан. А вот задача по

> пункту 3 не должна нарушить правило 1, то есть остается без доступа к vlan 10, хоть там и написано, что без ограничений.

Если что-то не работает - Перепроверь всё еще раз и прочитай документацию!!!

> В случае, если не включается сетевое устройство cisco - заменить данное устройство на микротик и настроить его.

> Чтобы выполнить проверку доступности по портам, замените virtual pc в проверяемой сети на debian, kali или windows. С помощью nmap/telnet можно проверить доступность порта.

Характеристики оборудования для самостоятельного построения стенда:

- **Cisco IOL: Router** - L3 образ. 512mb RAM;
- **Cisco IOL: Switch** - L2 образ. 256mb RAM;
- **Mikrotik** - Mikrotik ver.6.39;
- **Linux**: Debian 12 SRV. 1024mb RAM, Ethernet 2;
- **VPC.**

Методы проверки ЛР №4:

1. Каждое устройство может достучаться до любого другого устройства в рамках выполненных лабораторных работ.
2. Трассировка между всеми компьютерами должна показать путь прохождения трафика.
3. Подключение по SSH возможно осуществить к любому сетевому устройству, по SSH или telnet рамках лабораторных работ № 1, 2, 3.

1. Настроить SSH на каждом сетевом устройстве таким образом, чтобы с устройства SSH-Client можно было подключиться по SSH к любому устройству в рамках всех лабораторных работ.

Подключение по TELNET с SSH-Client’а к коммутатору Switch-3:

```
root@debian-11:~# ssh -l admin 10.0.70.254
kex_exchange_identification: Connection closed by remote host
Connection closed by 10.0.70.254 port 22
root@debian-11:~# telnet 10.0.70.3
Trying 10.0.70.3...
Connected to 10.0.70.3.
Escape character is '^]'.


User Access Verification

Username: admin
Password:

SW-3-Mikhauluk>
SW-3-Mikhauluk>
SW-3-Mikhauluk>
SW-3-Mikhauluk>
SW-3-Mikhauluk>_
```

Подключение по SSH с SSH-Client’а к роутеру Main-Router:

```
root@debian-11:/home/user# ssh -l admin 10.20.0.2
The authenticity of host '10.20.0.2 (10.20.0.2)' can't be established.
RSA key fingerprint is SHA256:Mx+jm4g/skRAN+u6L2/kZ/l8dmUAzNxKWvDszU9go7A.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.20.0.2' (RSA) to the list of known hosts.
(admin@10.20.0.2) Password:
Dmikhauluk-Main-Router>
```

Подключение по SSH с SSH-Client’а к роутеру C-RIP-10:

```
root@debian-11:/home/user# ssh -l admin 186.12.48.2
The authenticity of host '186.12.48.2 (186.12.48.2)' can't be established.
RSA key fingerprint is SHA256:Ek736vqlaY7j/Coh0KXUd7Fw84kWRjB6lgBbsLqbbMc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '186.12.48.2' (RSA) to the list of known hosts.
(admin@186.12.48.2) Password:
Dmikhauluk-C-RIP-10>_
```

Подключение по SSH с SSH-Client’a к роутеру C-OSPF-5:

```
root@debian-11:/home/user# ssh -l admin 12.12.16.2
The authenticity of host '12.12.16.2 (12.12.16.2)' can't be established.
RSA key fingerprint is SHA256:ECyX2zqni1YCaV2KkKN6cxmTRQ6mbXEjMsjPAMYnAbK
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '12.12.16.2' (RSA) to the list of known hosts.
(admin@12.12.16.2) Password:
Dmikhauluk-OSPF-5>_
```

Подключение по SSH с SSH-Client’a к роутеру M-iBGP-101:

```
root@debian-11:/home/user# ssh -l admin 13.1.9.101
The authenticity of host '13.1.9.101 (13.1.9.101)' can't be established.
RSA key fingerprint is SHA256:sAxyiaQkvHjbpVKrrOS17FiWrRt8lZxo+A7Np0+gXpc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.1.9.101' (RSA) to the list of known hosts.
admin@13.1.9.101's password:




  MMM       MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM     MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.39rc68 (c) 1999-2017       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@DMikhauluk-IBGP-101] > _
```

2. Настроить технологию NAT на роутерах C-RIP-10 и C-OSPF-5.

Пинг 8.8.8.8 с коммутатора Switch-1:

```
DMikhauluk-Switch-1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 26/26/26 ms
DMikhauluk-Switch-1#
*Nov  7 17:03:52.500: %SYS-5-CONFIG_I: Configured from console by console
DMikhauluk-Switch-1#
```

Пинг 8.8.8.8 с роутера C-R-2-2:

```
DMikhauluk-C-R-2-2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 29/30/31 ms
DMikhauluk-C-R-2-2#
```

Пинг 8.8.8.8 с роутера C-RIP-2:

```
DMikhauluk-C-RIP-2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/25/26 ms
DMikhauluk-C-RIP-2#
```

Пинг 8.8.8.8 с роутера M-OSPF-2:

```
[admin@DMikhauluk-M-OSPF-2] >> ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56  55 19ms
    1 8.8.8.8                                    56  55 20ms
    2 8.8.8.8                                    56  55 19ms
    3 8.8.8.8                                    56  55 20ms
    4 8.8.8.8                                    56  55 20ms
    sent=5 received=5 packet-loss=0% min-rtt=19ms avg-rtt=19ms max-rtt=20ms
```

Пинг 8.8.8.8 с роутера C-iBGP-33:

```
DMikhauluk-IBGP-33#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 26/31/40 ms
DMikhauluk-IBGP-33#
```