

Настройка сети центрального офиса

1. Настройте административный доступ ко всем сетевым устройствам в центральном офисе.

i. Для обеспечения административного доступа создайте интерфейс Loopback1 на HQ1, HQ2, D1, D2. На коммутаторах A1 и A2 используйте интерфейс Vlan 14.

HQ1, HQ2, D1, D2:

Int lo1

Ip addr x.x.x.x x.x.x.x (адрес придумываем сами)

A1, A2:

Int vlan 14

Ip addr x.x.x.x x.x.x.x (адрес придумываем сами)

!!Адреса не забыть добавить в dns, проверка только по именам!!

!!Не забыть попробовать подключиться по именам!!

ii. Используйте SSH версии 2 и ключ длиной 4096 бит.

Ip domain name AS21.local

Crypto key gen rsa mod 4096

Ip ssh ver 2

Line vty 0 15

Tr in ssh

!!Проверить подключение по SSH по доменному имени!!

iii. Используйте для аутентификации по SSH NPS-сервер, но предусмотрите локальный вход в случае недоступности сервера.

!!Сначала создаем юзера, например а с 15 привилегиями и паролем а, чтоб не потерять доступ!!

Aaa new-model

aaa authentication login SSH group radius local //Создаем отдельный лист, чтобы освободить дефолт и не терять доступ к консоли

aaa authorization exec SSH group radius local

aaa authorization console

//Это была настройка AAA, теперь настраиваем коннект к NPS.

!!Предварительно развернуть и настроить NPS на ДК!!

radius server RAD

address ipv4 1.1.1.1 auth-port 1812 acct-port 1813

key cisco //ключ такой же как на NPS для клиента

timeout 5 //делать не обязательно, но можно, чтоб меньше ждать, если сдохнет сервак. Совсем маленькие значения ставить не рекомендуется, 3-5 норм

line ty 0 15

login authentication SSH

authorization exec SSH // Список SSH в AAA мы делали выше, теперь надо указать его на линии.

!!На line con 0 оставляем default, там RADIUS не просят!!

iv. Используйте локальную аутентификацию для консоли.

```
aaa authentication login default local
```

```
aaa authorization exec default local
```

!!больше настраивать ничего не надо, default висит везде по умолчанию!!

v. Создайте локальную учётную запись tech с паролем easy на маршрутизаторах HQ1 и HQ2 с возможностью просматривать настройки IP на интерфейсах и таблицу маршрутизации, но исключите возможность вводить другие команды.

```
Parser view tech
```

```
Secret easy
```

```
commands exec include sh ip int br
```

```
commands exec include sh ip route
```

```
username tech privilege 0 view tech algorithm-type scrypt secret easy
```

!!Проверка: логинимся под этим юзером по SSH, смотрим доступные команды.

Должны быть доступны sh ip int br и sh ip route, а так же все вариации sh ip route (sh ip route ospf и так далее)!!

vi. Создайте учётную запись atom с защищённым паролем skills и максимальными привилегиями на тех устройствах, где её ещё нет.

!!Не важно, есть она или нет, создаем везде, чтоб точно не накосячить!!

```
username atom privilege 15 algorithm-type scrypt secret skills
```

!!Создай на одном устройстве, попробуй залогиниться туда по ssh и через консоль. После того, как успешно залогинился – копируй команду везде!!

vii. При входе в систему по SSH или через консоль с учётной записью atom пользователю должны автоматически передаваться максимальные полномочия.

!!Уже настроили это в AAA, но лучше проверь. Прямо по каждому устройству пройди!!

viii. Настройте хешированный пароль as на режим enable.

```
enable algorithm-type scrypt secret as
```

!!disable – выйти из enable. Выйди везде и попробуй зайти в en под этим паролем, прямо на каждом устройстве.!!

ix. Все пароли должны храниться в защищённом виде с использованием алгоритма scrypt.

!!Просто к каждому паролю подписываем algorithm-type scrypt!!

x. В случае попытки подбора пароля на маршрутизаторах HQ1 и HQ2 (не менее 3 раз за 15 секунд) они должны временно блокировать доступ по SSH со стороны интернета на 2 минуты. Доступ со стороны локальной сети должен сохраняться.

```
ip access-list standard LOGIN
permit x.x.x.x x.x.x.x // Пермитим в этот ацл ВСЕ локальные сетки ЦО
login block-for 120 attempts 3 within 15 // 120 – на сколько секунд лочим, 3 – сколько
попыток на вход, 15 – в течении сколько секунд
login quiet-mode access-class LOGIN //разрешаем доступ со стороны локальной
сети
!!Проверка: sh login. Брутфорсить сидеть не надо!!
```

2. Настройте маршрутизатор HQ2 и коммутатор D2 согласно топологии L3.

i. Создайте необходимые SVI на D2.

```
Int vlan x
Ip address x.x.x.x x.x.x.x // тут думаю все понятно
!!D1 и HQ1 настраивать тоже надо, разумеется. Не забываем проверять
пингами со всех машин ЦО. Должно пинговаться. int Vlan делаем 11-14!!
```

ii. Настройте IP-адреса на внутреннем интерфейсе маршрутизатора HQ2 и интерфейсах коммутатора D2 на ваше усмотрение.

```
D2:
Int g1/2
No switchport
Ip address x.x.x.x x.x.x.x
HQ2:
Int g0/1
No sh
Ip address x.x.x.x x.x.x.x
```

iii. Настройте IP-адрес на маршрутизаторе HQ2, выдаваемый провайдером.

```
int g0/0
no sh
ip address 77.34.141.141 255.255.252.0
ip route add 0.0.0.0 0.0.0.0 77.34.140.1
```

3. Настройте L2-Etherchannel между коммутаторами D1, D2, A1 и A2.

i. Используйте протокол LACP.

ii. Коммутаторы D1 и D2 должны инициировать согласование канала.

```
D1:
Int range g0/0-1
Sh
Channel-group 1 mode active
No sh
Int range g0/2-3
Sh
```

Channel-group 2 mode active
No sh

D2:
Int range g0/0-1
Sh
Channel-group 3 mode active
No sh
Int range g0/2-3
Sh
Channel-group 4 mode active
No sh

A1:
Int range g0/0-1
Sh
Channel-group 1 mode passive
No sh
Int range g0/2-3
Sh
Channel-group 4 mode passive
No sh

A2:
Int range g0/0-1
Sh
Channel-group 3 mode passive
No sh
Int range g0/2-3
Sh
Channel-group 2 mode passive
No sh

!!Проверка: sh etherchannel summary, везде должно быть SU. Если не SU – идем на интерфейсы и делаем sh; no sh!!

iii. Используйте балансировку по MAC-адресам источника и назначения.

!!На всех коммутерах!!

port-channel load-balance src-dst-mac

!!Проверка: sh port-channel load-balance. Везде должно быть написано Source XOR Destination MAC address!!

****Примечание**:** для корректной настройки LACP возможно потребуется предварительно выключить физические порты с двух сторон Etherchannel, произвести настройку и затем включить физические порты.

4. Настройте L3-Etherchannel между коммутаторами D1 и D2.

i. Используйте протокол PAgP. Коммутатор D1 должен инициировать создание канала.

D1:
Int range g1/0-1
Sh
No switchport
Channel-group 5 mode desirable
Ip address x.x.x.x x.x.x.x //придумай что-нибудь свое
No sh

D2:
Int range g1/0-1
Sh
No switchport
Channel-group 5 mode auto
Ip address x.x.x.x x.x.x.x // очевидно из подсети, которую ты сделал на D1
No sh

!!Проверка: sh etherchannel sum Po5 Должен быть RU. Так же попробуй пингануть, пинги должны быть. Если не работает sh; no sh интерфейсы!!

5. Настройте транки между коммутаторами D1, D2, A1 и A2 поверх Etherchannel.

i. Транки должны устанавливаться принудительным образом. В явном виде отключите протокол DTP.

!!На всех коммутерах!!

Int range g0/0-3
Switchport trunk encap dot1q
Switchport mode trunk
Switchport none

!!Проверка: sh int trunk!!

ii. Вручную ограничьте список VLAN, разрешённых на этих транках таким образом, чтобы в него входили только фактически используемые сети VLAN.

!!На всех коммутерах!!

Int range g0/0-3
Switchport trunk allowed vlan 11-14

!!Проверка: s hint trunk. Allowed vlan должны быть ТОЛЬКО 11-14!!

6. Настройте VRRP на коммутаторах D1 и D2 для сетей WINA, WINB и LINA.

i. Используйте версию 2.

fhrp version vrrp v2

!!Проверка: sh fhrp version!!

ii. Используйте номер группы, совпадающий с номером VLAN.

iii. Все устройства из соответствующих сетей должны использовать адрес виртуального маршрутизатора в качестве шлюза.

!!Настрой в DHCP и статикой нормальный шлюз на VRRP адрес!!

iv. В сетях WINA и WINB должен по умолчанию предпочитаться шлюз D1, а в сети LINA - шлюз D2.

D1:

Int vlan 11

Vrrp 11 ip x.x.x.x //на D2 пишешь такой же

Vrrp 11 priority 100

Vrrp 11 preempt

Int vlan 12

Vrrp 12 ip x.x.x.x //на D2 пишешь такой же

Vrrp 12 priority 100

Vrrp 12 preempt

Int vlan 13

Vrrp 13 ip x.x.x.x //На D2 пишешь такой же

Vrrp 13 priority 99

Vrrp 13 preempt

D2:

Int vlan 11

Vrrp 11 ip x.x.x.x

Vrrp 11 priority 99

Vrrp 11 preempt

Int vlan 12

Vrrp 12 ip x.x.x.x

Vrrp 12 priority 99

Vrrp 12 preempt

Int vlan 13

Vrrp 13 ip x.x.x.x

Vrrp 13 priority 100

Vrrp 13 preempt

7. Настройте службу DHCP в центральном офисе.

i. Сделайте необходимые настройки, чтобы устройства в сети WINA могли получить адрес по DHCP от сервера DC.

!!Делаем на D1 и D2!!

Int vlan 11

Ip helper-address x.x.x.x //тут адрес DC

ii. Настройте DHCP Snooping на коммутаторах A1 и A2.

A1:

Ip dhcp snooping vlan 11-14

Ip dhcp snooping
Int range g1/1, g0/0-3
Ip dhcp snooping trust
No ip dhcp snooping verify mac-address
No ip dhcp snooping information option

A2:

Ip dhcl snooping vlan 11-14
Ip dhcp snooping
Int range g0/0-3
Ip dhcp snooping trust
No ip dhcp snooping verify mac-address
No ip dhcp snooping information option

**!!Если не работает – no ip dhcp snooping и забей. Проверка –
получить адрес по DHCP. Еще можно s hip dhcp snooping!!**

8. Настройте протокол STP на коммутаторах D1, D2, A1, A2.

i. Коммутатор D1 должен быть корнем в VLAN 11 и 12. Коммутатор D2
должен быть корнем в VLAN 13.

D1:

Spanning-tree vlan 11-12 priority 4096
Spanning-tree vlan 13 priority 8192

D2:

Spanning-tree vlan 11-12 priority 8192
Spanning-tree vlan 13 priority 4096

!!проверка: sh spanning-tree!!

ii. Используйте протокол 802.1w.

!!на всех коммутерах!!

Spanning-tree mode rapid-pvst

!!проверка: sh spanning-tree!!

9. Настройте порты доступа на коммутаторах A1 и A2.

i. Порты в сторону клиентских устройств и серверов должны сразу
переходить в состояние Forwarding, но блокироваться, если на них приходит
BPDU.

A1:

Int range g1/0-1
Spanning-tree portfast

Spanning-tree bpduguard enable

A2:

Int range g1/0-3

Spanning-tree portfast

Spanning-tree bpduguard enable

ii. Принудительно переведите их в режим доступа и отключите в явном виде протокол DTP.

A1:

Int g1/0

Switchport none

Switchport mode access

Switchport access vlan 11

Int g1/1

Switchport none

Switchport mode access

Switchport access vlan 12

A2:

Int g1/0

Switchport none

Switchport mode access

Switchport access vlan 12

Int g1/1-3

Switchport none

Switchport mode access

Switchport access vlan 13

!!Проверка: sh vlan!!

10. Включите протокол LLDP на всех сетевых устройствах центрального офиса.

i. Отключите отправку LLDP-сообщений в сторону клиентов и серверов, а также провайдера, но оставьте их получение.

!!На всех в ЦО!!

Lldp run

HQ1:

Int g0/0

Lldp recive

No lldp trans

HQ2:

Int g0/0

Lldp recive

No lldp trans

A1:

Int range g1/0-1

Lldp recive

No lldp trans

A2:

Int range g1/0-3

Lldp recive

No lldp trans

!!проверка: sh lldp int!!

11. Настройте динамическую маршрутизацию с помощью протокола OSPF.

- i. Используйте область 0.
- ii. Коммутаторы D1 и D2 должны использовать маршрут по умолчанию типа 1, полученный по OSPF.
- iii. Все сети центрального офиса должны быть объявлены в OSPF.
- iv. Все интерфейсы, через которые не предусмотрено соседство, должны находиться в пассивном режиме.

HQ1:

Router ospf 1

Network x.x.x.x x.x.x.x area 0 //тут вписываешь сетку которая на g0/1

Network x.x.x.x x.x.x.x area 0 // тут вписываешь сетку lo

Default-information originate mtrix-type 1

Passive-interface default

No passive-interface g0/1

HQ2:

Router ospf 1

Network x.x.x.x x.x.x.x area 0 //тут вписываешь сетку которая на g0/1

Network x.x.x.x x.x.x.x area 0 // тут вписываешь сетку lo

Default-information originate mtrix-type 1 metric 16777214 //метрику бери через ?(Знак вопроса (Справку (встроенную документацию)))

Passive-interface default

No passive-interface g0/1

D1:

Router ospf 1

Network 0.0.0.0 0.0.0.0 area 0

Passive-interface default

No passive-interface Po5 // L3 etherchannel между D1 и D2

No passive-interface g1/2

D2:

Router ospf 1

Network 0.0.0.0 0.0.0.0 area 0

Passive-interface default //ОБЯЗАТЕЛЬНО ДЕЛАЙ ТАК

No passive-interface Po5 // L3 etherchannel между D1 и D2

No passive-interface g1/2

!!проверка: sh ip ospf nei; sh ip route ospf!!

v. Настройте BFD для быстрого определения состояния каналов между HQ1, HQ2, D1 и D2.

!!На всех!!

Bfd slow-timers 1200

bfd-template single-hop OSPF

interval min-tx 120 min-rx 100 multiplier 3

!!Заходим на интерфейсы между девайсами!!

Bfd template OSPF

12. Настройте второй интернет-канал в центральном офисе через маршрутизатор HQ2.

i. Второй канал должен использоваться в качестве резервного.

Ip access-list st NAT

Permit x.x.x.x x.x.x.x //Тут пермит все локальные сетки ЦО

Ip nat inside source list NAT interface g0/0 overload

Int g0/0

Ip nat inside

Int g0/1

Ip nat outside

!!проверка: Должны появятся пинги до 8.8.8.8 из внутренних сетей через HQ2!!

13. Настройте на маршрутизаторах HQ1 и HQ2 проверку связи со шлюзом провайдера по ICMP. В случае недоступности шлюза провайдера с маршрутизатора HQ1 должно автоматически происходить переключение на резервный канал связи.

!!На всех устройствах!!

ip sla 1

```
icmp-echo 178.207.179.25 //для HQ2 указать свой шлюз
threshold 5000
timeout 6000
frequency 7
ip sla schedule 1 life forever start-time now
```

```
track 1 ip sla 1 reachability
```

```
event manager applet INET_DOWN
event track 1 state down
action 001 syslog msg "INET IS DOWN"
action 002 cli command "en"
action 003 cli command "conf t"
action 004 cli command "no ip route 0.0.0.0 0.0.0.0 178.207.179.25" //На HQ2
роут в сторону ISP HQ2
action 005 cli command "end"
```

```
event manager applet INET_UP
event track 1 state up
action 001 syslog msg "INET UP"
action 002 cli command "en"
action 003 cli command "conf t"
action 004 cli command "ip route 0.0.0.0 0.0.0.0 178.207.179.25" //На HQ2
роут в сторону ISP HQ2
action 005 cli command "end"
```

14. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.

i. В качестве сервера должен выступать маршрутизатор HQ1 со стратум 5

ii. Используйте на маршрутизаторе HQ1 интерфейс Loopback1 в качестве источника.

```
ntp master 5
Ntp source lo1
```

iii. Все остальные сетевые устройства должны синхронизировать своё время с маршрутизатором HQ1.

```
!!на всех кроме HQ1!!
Ntp server x.x.x.x x.x.x.x //Тут адрес lo1 на HQ1
```

iv. Используйте на всех устройствах московский часовой пояс.

```
!!Везде!!
Clock timezone MSK +3
```

!!Проверка: sh clock; sh ntp ass!!

15. Настройте мониторинг, журналирование и архивирование конфигураций на сетевых устройствах HQ1, HQ2, D1, D2, A1, A2.

- i. Используйте SNMPv2c и строку сообщества atomskills2021
- ii. Опрос по SNMP нужно разрешить для сервера SRV.

!!на всех устройствах!!

Ip access-list st SNMP

Permit host x.x.x.x //тут адрес SRV

Snmp-server community atomskills 2021 SNMP

Snmp-server enable traps

Snmp-server source-interface informs lo1 // на A1 и A2 vlan14

Snmp-server source-interface traps lo1 // На A1 и A2 vlan14

iii. Архив конфигурации необходимо при каждом сохранении отправлять на TFTP-сервер на SRV.

- iii. Имя архива должно содержать имя устройства, дату и время.

!!На всех устройствах!!

Archive

Path tftp://x.x.x.x/\$H-\$T.cfg

Write-memory

v. Syslog уровня важности 5 и более важные необходимо отправлять на сервер SRV.

vi. В сообщениях журнала необходимо указывать дату, время и часовой пояс.

!!На всех устройствах!!

Logging host x.x.x.x //тут адрес SRV

Logging x.x.x.x // тут адрес SRV

Logging facility local5

Logging source-interface lo1 // На A1 и A2 vlan14

Service timestamps log datetime show-timezone localtime

Logging on

vii. В качестве источника трафика на сетевых устройствах D1, D2, HQ, HQ2 используйте интерфейс Loopback1. На устройствах A1 и A2 используйте интерфейс VLAN13

!!Уже сделано!!

16. Настройте DMVPN между центральным офисом и ЦОД.

i. Используйте CR1 и CR2 в качестве хабов.

ii. Используйте номер интерфейса 101 для связи между CR1, HQ1 и HQ2.

iii. Используйте номер интерфейса 102 для связи между CR2, HQ1 и

HQ2.

iv. На CR1 используйте интерфейс в сторону провайдера LVL80.

CR1:

Int tun 101

Ip address x.x.x.x x.x.x.x //Адрес внутри туннеля придумай сам

Ip nhrp network-id 101

Ip nhrp map multicast dynamic

Tunnel key 101

Tunnel source g0/2

Tunnel mode gre multipoint

Ip nhrp redirect

CR2:

Int tun 102

Ip address x.x.x.x x.x.x.x //Адрес внутри туннеля придумай сам

Ip nhrp network-id 102

Ip nhrp map multicast dynamic

Tunnel key 102

Tunnel source g0/0

Tunnel mode gre multipoint

Ip nhrp redirect

HQ1:

Int tun 101

Ip address x.x.x.x x.x.x.x //Адрес из подсети как на CR1

Ip nhrp network-id 101

Ip nhrp map 138.12.12.5 x.x.x.x //тут внешний адрес CR1

Ip nhrp map multicast x.x.x.x //тут внешний адрес CR1

Ip nhrp nhs x.x.x.x //тут адрес внутри туннеля CR1

Tunnel key 101

Tunnel source g0/0

Tunnel mode gre multipoint

Ip nhrp redirect

Ip nhrp shortcut

Int tun 102

```
Ip address x.x.x.x x.x.x.x //Адрес из подсети как на CR2
Ip nhrp network-id 102
Ip nhrp map 178.207.179.4 x.x.x.x // тут внешний адрес CR2
Ip nhrp map multicast x.x.x.x // тут внешний адрес CR2
Ip nhrp nhs x.x.x.x //тут адрес внутри туннеля CR2
Tunnel key 102
Tunnel source g0/0
Tunnel mode gre multipoint
Ip nhrp redirect
Ip nhrp shortcut
```

HQ2:

```
Int tun 101
Ip address x.x.x.x x.x.x.x //Адрес из подсети как на CR1
Ip nhrp network-id 101
Ip nhrp map 138.12.12.5 x.x.x.x // тут внешний адрес CR1
Ip nhrp map multicast x.x.x.x // тут внешний адрес CR1
Ip nhrp nhs x.x.x.x //тут адрес внутри туннеля CR1
Tunnel key 101
Tunnel source g0/0
Tunnel mode gre multipoint
Ip nhrp redirect
Ip nhrp shortcut
```

```
Int tun 102
Ip address x.x.x.x x.x.x.x //Адрес из подсети как на CR2
Ip nhrp network-id 102
Ip nhrp map 178.207.179.4 x.x.x.x // тут внешний адрес CR2
Ip nhrp map multicast x.x.x.x // тут внешний адрес CR2
Ip nhrp nhs x.x.x.x //тут адрес внутри туннеля CR2
Tunnel key 102
Tunnel source g0/0
Tunnel mode gre multipoint
Ip nhrp redirect
Ip nhrp shortcut
```

!!Проверка: sh dmvrn; пинги через туннель до всего отовсюду должны ходить!!

v. Используйте следующие параметры для защиты туннеля:

- a. IKEv1 с параметрами AES128, SHA, DH14
- b. IPsec с помощью протокола ESP с шифрованием AES128 и хешем SHA.

!!На всех устройствах!!

```
Crypto isakmp policy 1
Encryption aes
Hash sha
```

Group 14

Authentication pre-share

Crypto isakmp key cisco address 0.0.0.0

Crypto ipsec transform-set IPSEC esp-aes esp-sha-hmac

Mode tunnel

Crypto ipsec profile IPSEC

Set transform-set IPSEC

Int tun 101

Tunnel protection ipsec profile IPSEC shared

Int tun 102

Tunnel protection ipsec profile IPSEC shared

!!Проверка: sh crypto isakmp sa; sh crypto ipsec sa!!

!!Дописывай слово shared в конце обязательно!!

17. Настройте маршрутизацию EIGRP поверх DMVPN

i. Используйте номер автономной системы 65000.

!!На всех устройствах!!

Router eigrp 65000

Network x.x.x.x x.x.x.x //анонсим все внутренние сети, сеть туннеля,

lo

!!проверка: sh ip eigrp nei; sh ip route eigrp!!

ii. Для связи между ЦОД и центральным офисом должен предпочитаться маршрут через CR2 и HQ2.

!!На HQ1 и CR1!!

Int tun 101

Bandwidth 10000000 //Значение берем через ?

Настройка ЦОД

1. Настройте административный доступ ко всем устройствам в центре обработки данных.

i. Создайте для этого интерфейс Loopback1 на CR1, CR2, CSW1, CSW2.

Int lo1

Ip address x.x.x.x x.x.x.x //адрес придумай сам, чтоб не совпадал с тем, что в HQ

ii. Используйте SSH версии 2 и ключ длиной 4096 бит.

Ip domain name AS21.local

Crypto key gen rsa mod 4096

Ip ssh ver 2

Line vty 0 15

Tr in ssh

!!Проверить подключение по SSH по доменному имени!!

iv. Используйте для аутентификации локальные базы учётных записей.

!!Сначала создай юзера!!

Username a priv 15 alghoritm-type scrypt secret a

Aaa new-model

Aaa authentication login default local

Aaa authorization console

Aaa authorization exec default local

v. Используйте локальную аутентификацию для консоли.

!!Уже работает, default висит везде по умолчанию!!

vi. Создайте учётную запись atom с защищённым паролем skills и максимальными привилегиями на тех устройствах, где её ещё нет.

!!Создавай везде!!

Username atom priv 15 algorithm-type scrypt secret skills

vii. При входе в систему по SSH или через консоль с учётной записью atom пользователю должны автоматически передаваться максимальные полномочия.

!!Работает по умолчанию!!

viii. Настройте хешированный пароль as на режим enable.

Enable alghoritm-type scrypt secret as

- ix. Все пароли должны храниться в защищённом виде с использованием алгоритма scrypt.

!!При создании ВСЕХ юзеров юзаем scrypt

2. Настройте все сети VLAN согласно топологии.

- i. Создайте недостающие VLAN и укажите их имена согласно топологии.
- ii. На всех транках должны быть разрешены только используемые в топологии VLAN.

!!Не забудь сделать порты access, которые в сторону вм!!

Vlan 100

Name DMZ1

Vlan 200

Name VMMGMT

Vlan 300

Name DCNET

Vlan 50

Name ROUTING

Int g0/1, g0/3, g1/0 //На CSW1 только g0/1

Switchport trunk encap dot1q

Switchport mode trunk

Switchport none

Switchport trunk allowed vlan 100,200,300,50 // перечисление именно через запятую

3. Настройте IP-адресацию на CR1, CR2, CSW1, CSW2.

Int vlan 50

Ip address x.x.x.x x.x.x.x // придумай сам на обоих свичах

Int vlan 100

Ip address 203.0.113.x 255.255.255.0 //Подсеть бери именно эту, так по заданию

Int vlan 200

Ip address x.x.x.x x.x.x.x //тут придумай сам

Int vlan 300

Ip address x.x.x.x x.x.x.x //тоже сам

Int g1/1 //На csw2 g0/2

No switchport

Ip address 203.0.117.x 255.255.255.0 //Адрес именно из этой подсети по заданию

Int g0/0 //на CR1 и CR2 g0/1
No switchport //На CR1 и CR2 не надо
No switchport
Ip address x.x.x.x x.x.x.x

4. Настройте выход в интернет в ЦОД
- i. Настройте подключение через LVL80 на CR1.
 - ii. Настройте подключение через GIGAFON на CR2.

CR1:
Int g0/2
Ip address 138.12.12.5 255.255.255.0

CR2:
Int g0/0
Ip address 178.207.179.4 255.255.255.248

5. Настройте BGP на CR1, CR2, CSW1, CSW2, LINDMZ.
- i. Настройте соседство с провайдерами на CR1 и CR2.

CR1:
Router bgp 64500
Network 172.217.35.0 mask 255.255.255.0
Network 138.12.12.0 mask 255.255.255.0
Neighbor 172.217.35.1 remote-as 15169
Neighbor 138.12.12.1 remote-as 3356

CR2:
Router bgp 64500
Network 178.207.179.0 mask 255.255.255.248
Neighbor 178.207.179.1 remote-as 31133

- ii. Настройте iBGP между всеми сетевыми устройствами ЦОД.

CR1:
Router bgp 64500
Neighbor x.x.x.x remote-as 64500 //Соседем с CSW1

CR2:
Router bgp 64500
Neighbor x.x.x.x remote-as 64500 //соседем с CSW2

CSW1:
Router bgp 64500
Network 203.0.113.0 mask 255.255.255.0
Network 203.0.117.0 mask 255.255.255.0

Neighbor x.x.x.x remote-as 64500 // соседим с CR1
Neighbor x.x.x.x remote-as 64500 // соседим с CSW2 через VLAN50

CSW2:

Router bgp 64500

Network 203.0.113.0 mask 255.255.255.0

Network 203.0.117.0 mask 255.255.255.0

Neighbor x.x.x.x remote-as 64500 // соседим с CR2

Neighbor x.x.x.x remote-as 64500 // соседим с CSW1 через VLAN50

iii. Используйте CSW1 и CSW2 в качестве Route Reflector.

Router bgp 64500

Neighbor x.x.x.x route-reflector-client // На CSW1 делаем клиентом CR1,
на CSW2 делаем CR2

iv. Сделайте необходимые настройки, чтобы для выхода в Интернет и входящего трафика предпочитался канал LVL80, однако сети MOOGLE и GIGAFON были доступны напрямую через соответствующие автономные системы.

CR1:

Route-map BGP

Set as-path prepend 3356 3356 3356 3356

Router bgp 64500

Neighbor 172.217.35.1 route-map BGP

Neighbor 138.12.12.1 weight 65535

CSW1:

Route-map BGP

Set as-path prepend 64500 64500 64500 64500

Router bgp 64500

Neighbor x.x.x.x route-map BGP out // адрес CR1

Neighbor x.x.x.x weight 65535 // адрес CR1

#ИТОГОВЫЕ КОНФИГИ BGP ПОД ВСЕ ЗАДАНИЕ

---CR1---

router bgp 64500

neighbor 138.12.12.1 remote-as 3356

neighbor 138.12.12.1 weight 65000

neighbor 172.16.1.10 remote-as 64500 \ 172.16.1.10 - адрес CSW1 на g0/0

neighbor 172.16.1.10 default-originate

neighbor 172.217.35.1 remote-as 15169

neighbor 172.217.35.1 route-map BGP out

route-map BGP

set as-path prepend 3356 3356 3356 3356

---CR2---

router bgp 64500

```
neighbor 172.16.1.20 remote-as 64500 \\ 172.16.1.20 - адрес CSW2 на g0/0
neighbor 172.16.1.20 default-originate
neighbor 178.208.179.1 remote-as 31133
neighbor 178.208.179.1 route-map BGP1 out
    route-map BGP1
        set as-path prepend 31133 31133 31133 31133
```

---CSW1---

```
router bgp 64500
neighbor 172.16.1.1 remote-as 64500
neighbor 172.16.50.2 remote-as 64500 \\ сеть VLAN 50
neighbor 203.0.117.20 remote-as 64500
    address-family ipv4
        network 203.0.113.0 mask 255.255.255.0
        network 203.0.117.0 mask 255.255.255.0
        neighbor 172.16.1.1 activate
        neighbor 172.16.1.1 route-reflector-client
        neighbor 172.16.1.1 weight 65535
        neighbor 172.16.1.1 route-map BGP out
        neighbor 172.16.50.2 activate \\ сосед CSW2 во влане 50
        neighbor 172.16.50.2 default-originate
        neighbor 203.0.117.20 default-originate \\ шлюз для LINDMZ
    route-map BGP
        set as-path prepend 64500 64500 64500
```

---CSW2---

```
router bgp 64500
neighbor 172.16.1.2 remote-as 64500
neighbor 172.16.50.1 remote-as 64500
neighbor 203.0.117.20 remote-as 64500
    address-family ipv4
        network 203.0.113.0 mask 255.255.255.0
        network 203.0.117.0 mask 255.255.255.0
        neighbor 172.16.1.2 activate
        neighbor 172.16.1.2 route-reflector-client
        neighbor 172.16.50.1 activate
        neighbor 172.16.50.1 weight 65000
        neighbor 203.0.117.20 activate
        neighbor 203.0.117.20 default-originate
```

По итогу важно добиться, чтобы трафик шел - CSW2,CSW1,CR1 ,ISP - это в здоровом ключе!

**В случае неполадок в ЦОДе, BGP сам тебя спасет, но нужно поиграться с таймерами -
#КАК ИГРАТЬ С ТАЙМЕРОМ БГП**

6. Настройте EIGRP на CR1, CR2, CSW1 и CSW2.
- i. Используйте номер автономной системы 65000.
 - ii. Все интерфейсы, через которые не предусмотрено соседство, должны быть в режиме Passive. Соседство между CSW1 и CSW2 должно быть только через VLAN 50.

CR1:

Router eigrp 65000

Network x.x.x.x x.x.x.x //Анонсим сеть между CR1 и CSW1 а еще lo

Passive-interface default //ОБЯЗАТЕЛЬНО ДЕЛАЙ ТАК

No passive-interface g0/1

No passive-interface tun101

CR2:

Router eigrp 65000

Network x.x.x.x x.x.x.x //Анонсим сеть между CR2 и CSW2 а еще lo

Passive-interface default //ОБЯЗАТЕЛЬНО ДЕЛАЙ ТАК

No passive-interface g0/1

No passive-interface tun102

CSW1:

Router eigrp 65000

Network x.x.x.x x.x.x.x //Анонсим сеть до роутера, vlan50, vlan 200, vlan 300 и lo. ТОЛЬКО ИХ

Passive-interface default //ОБЯЗАТЕЛЬНО ДЕЛАЙ ТАК

No passive-interface vlan 50

No passive-interface g0/0

CSW1:

Router eigrp 65000

Network x.x.x.x x.x.x.x //Анонсим сеть до роутера, vlan50, vlan 200, vlan 300 и lo. ТОЛЬКО ИХ

Passive-interface default //ОБЯЗАТЕЛЬНО ДЕЛАЙ ТАК

No passive-interface vlan 50

No passive-interface g0/0

- iii. Настройте редистрибуцию сетей из EIGRP в OSPF и обратно. Не используйте статические маршруты для обеспечения маршрутизации между центральным офисом и ЦОД.

HQ1:

Router ospf 1

Redistribute eigrp 65000 metric 10000

Router eigrp 65000

**redistribute ospf 1 metric 10000 10000 1 1 1400 //метрику прописывать
обязательно всю, иначе не взлетит**

HQ2:

Router ospf 1

Redistribute eigrp 65000

Router eigrp 65000

**redistribute ospf 1 metric 10000 10000 255 1 1400 //метрику прописывать
обязательно всю, иначе не взлетит**

**!!Обязательно удали статические маршруты, они могут там быть.
Проверь и удали!!**

7. Сервер LINDMZ должен получать только маршрут по умолчанию по протоколу BGP от CSW1 и CSW2. Все остальные префиксы должны быть отфильтрованы.

!!Ставим frr и погнали!!

ip prefix-list FILTER permit 0.0.0.0/0

ip prefix-list FILTER deny 0.0.0.0/0 ge 32

Router bgp 64500

Network 203.0.117.0 mask 255.255.255.0

Neighbor x.x.x.x remote-as 64500 //соседемся с CSW1

Neighbor x.x.x.x remote-as 64500 //соседемся с CSW2

Neighbor x.x.x.x prefix-list FILTER in // фильтруем роуты с CSW1

Neighbor x.x.x.x prefix-list FILTER in //фильтруем роуты с CSW2

- i. Входящий трафик из интернета до сервера LINDMZ должен приходить через CSW1 и переключаться на CSW2 только в случае проблем со связью на CSW1, CR1 или у провайдера.

Route-map LP

Set local-preference 1000

Router bgp 64500

Neighbor x.x.x.x route-map LP out // ставим local preference на CSW2

Настройка сети филиала 1

!!Включаем ASDM если надо. Будет лежать на флешке, называться может как угодно!!

```
http server enable
http 0.0.0.0 0.0.0.0 inside //Должен быть интерфейс с таким именем,
на котором стоит адрес. Можно заводить на внешнем интф
asdm image flash:/asd,.bin //выбраем изображение, лежит на флешке
с расширением .bin. Назваться может по другому!!!
```

1. Настройте межсетевой экран ASA для обеспечения доступа в интернет для клиентов локальной сети.

i. Используйте в качестве имени внешнего интерфейса название провайдера.

ii. Настройте IP-адреса на внешнем и внутреннем интерфейсах.

```
Int g0/0
Nameif WATERFONE
Ip address 84.64.44.24 255.255.255.240
No sh
```

```
Int g0/1
Nameif inside
Ip address x.x.x.x x.x.x.x // придумай сам
No sh
```

```
Route WATERFONE 0.0.0.0 0.0.0.0 84.64.44.17
```

iii. Настройте службу DHCP для локальной сети. Используйте MOOGLE в качестве DNS-сервера.

```
dhcpd address x.x.x.x-x.x.x.x inside // inside – название внутреннего
интерфейса
dhcpd dns 8.8.8.8
dhcpd enable inside
```

!!не забудь проверить, что DHCP работает и перевести комп на получение адреса по DHCP!!

iv. Настройте NAT для адресов в локальной сети.

```
object network INSIDE
subnet 172.16.0.0 255.255.255.0
nat (inside,WATERFONE) dynamic interface
```

!!Чтобы работали пинги:

```
policy-map global_policy
class inspection_default
inspect icmp
```

можно это найти через sh run policy-map!!

2. Настройте административный доступ к межсетевому экрану ASA.

i. Используйте SSH версии 2 и ключ длиной 4096 бит.

```
crypto key generate rsa modulus 4096
ssh version 2
ssh 0.0.0.0 0.0.0.0 inside
ssh key-exchange group dh-group14-sha1 //чтобы норм работал SSH
```

ii. Используйте локальную аутентификацию для консольного доступа.

```
aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL auto-enable
```

iii. Создайте учётную запись atom с паролем skills и максимальными привилегиями на тех устройствах, где её ещё нет.

```
username atom password skills privilege 15 //последовательность
параметров именно такая
```

iv. При входе в систему по SSH или через консоль с учётной записью atom пользователю должны автоматически передаваться максимальные полномочия.

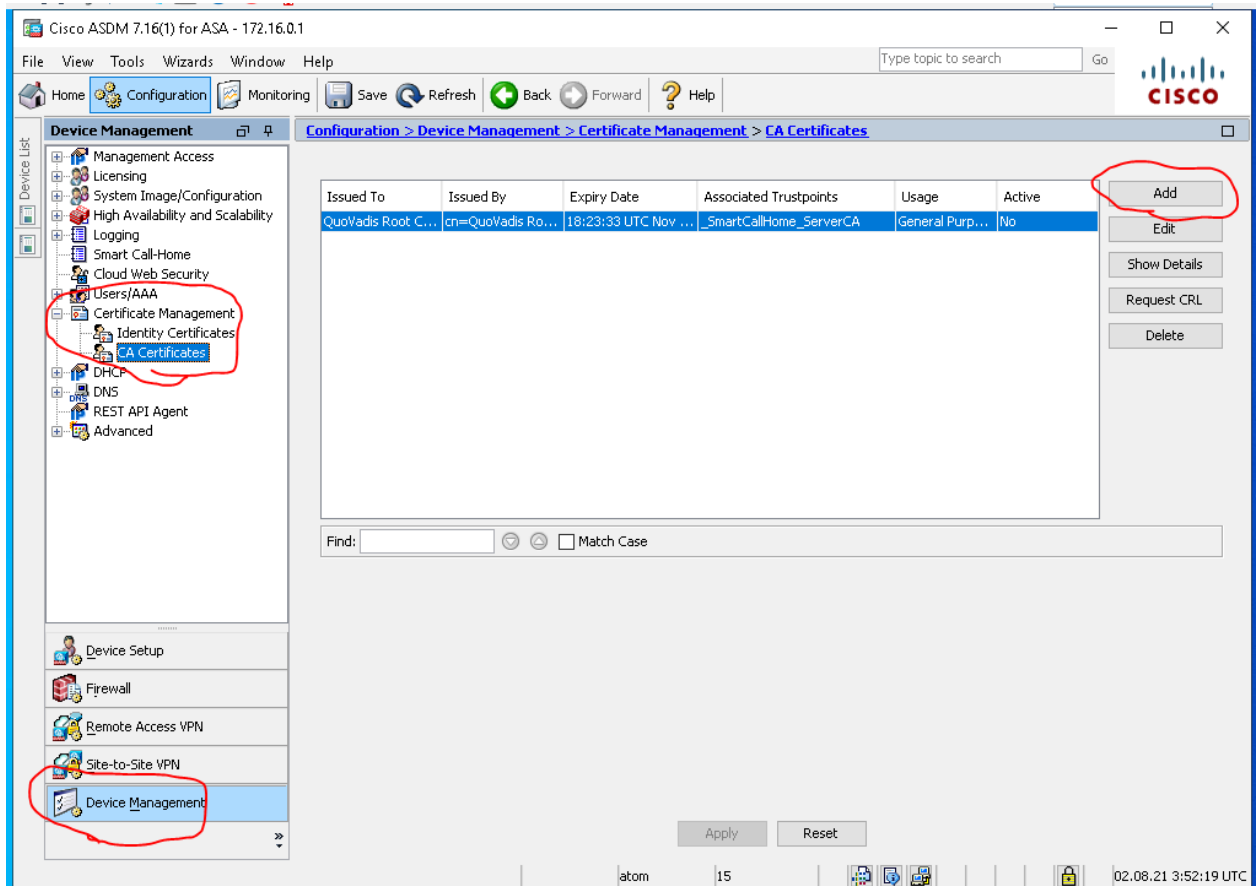
```
!!Делается вот этой командой
aaa authorization exec LOCAL auto-enable
Но при входе через консоль он всегда будет давать 1 уровень
привилегий
Проверка будет через команду login, так что все норм!!
```

v. Настройте пароль asa на режим enable.

```
Enable password asa
```

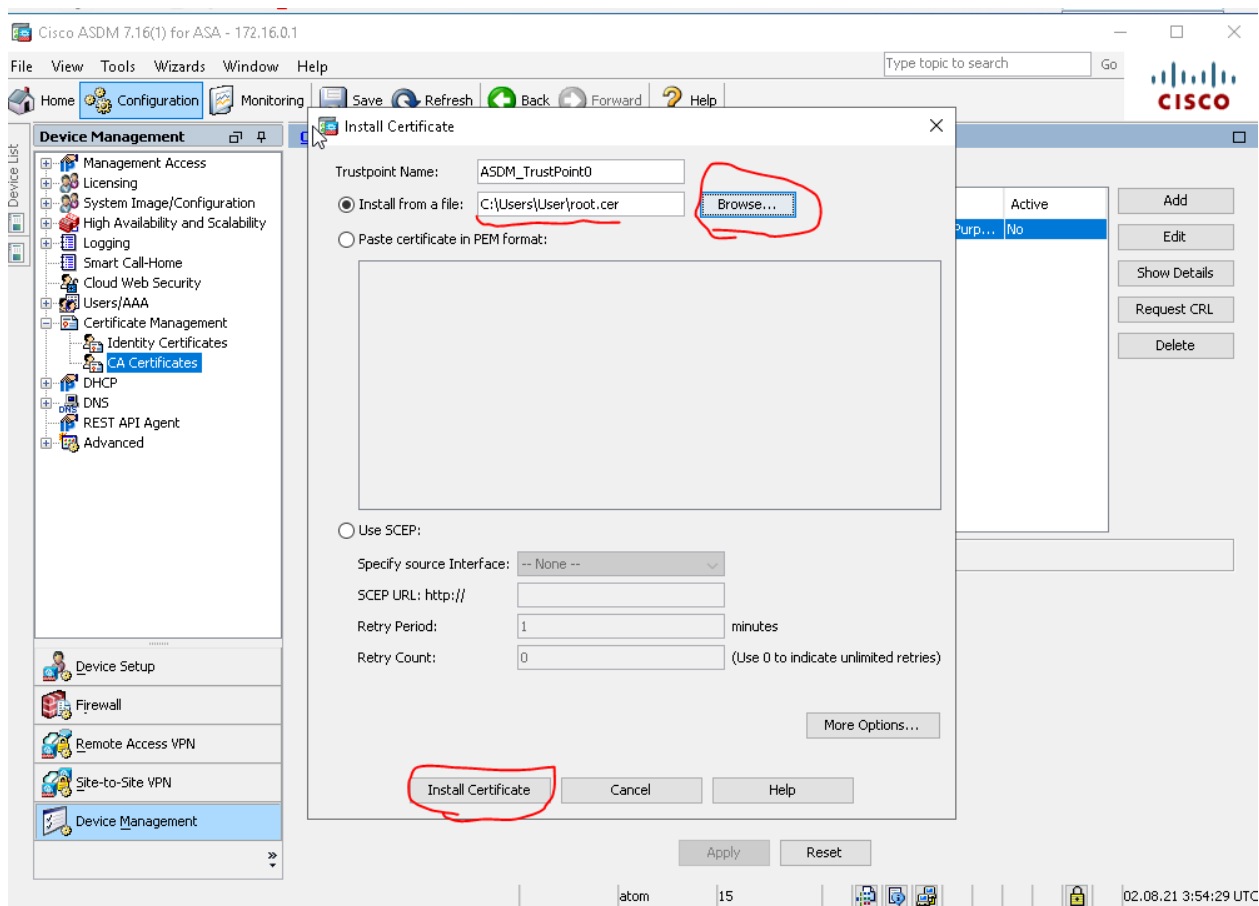

3. Настройте технологию SSL VPN с помощью Cisco AnyConnect.
- i. Используйте пакет openconnect на LINNET для проверки соединения.
 - ii. Настройте автоматическое подключение с проверкой пользователя по сертификатам.
 - iii. Весь трафик от клиента должен передаваться через это соединение.

Сначала надо установить сертификаты. Забираем рут, саб и энроллим серт для асы.

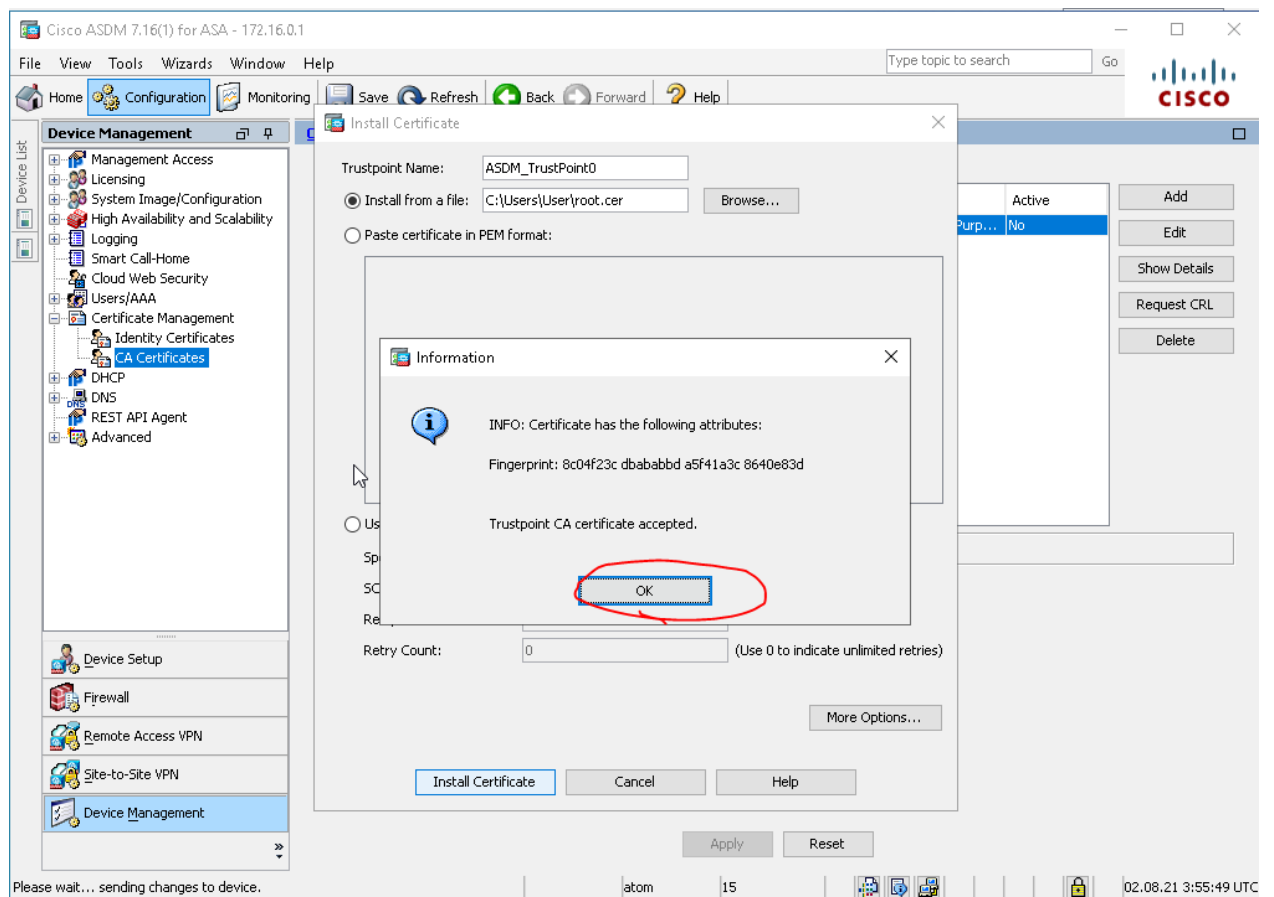


!!Убедись, что на асе нормальное время!!

Идем сюда и нажимаем add



Выбираем серт и устанавливаем



Точно так же ставим сабовый

Cisco ASDM 7.16(1) for ASA - 172.16.0.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
SubCA	cn=RootCA, dc=...	04:13:53 UTC Jul 3...	ASDM_TrustPoint1	Signature	Yes
RootCA	cn=RootCA, dc=...	10:12:15 UTC Jul 3...	ASDM_TrustPoint0	Signature	Yes
QuoVadis Root C...	cn=QuoVadis Ro...	18:23:33 UTC Nov ...	_SmartCallHome_ServerCA	General Purp...	No

Find: ☐ Match Case

Apply Reset

Configuration changes saved successfully.

atom 15 02.08.21 3:57:59 UTC

Серт на винде делаем как обычно, из шаблона Web server.
Экспортируем в PFX, шифруем обязательно в TripleDES-sha1 (по умолчанию.) Загоняем этот серт в Identity.

Cisco ASDM 7.16(1) for ASA - 172.16.0.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

- Management Access
- Licensing
- System Image/Configuration
- High Availability and Scalability
- Logging
- Smart Call-Home
- Cloud Web Security
- Users/AAA
- Certificate Management
 - Identity Certificates
 - CA Certificates
- DHCP
- DNS
- REST API Agent
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.AS21.local]	Not Available	Pending...	ASDM_TrustPoint0	Unknown	

Add

Show Details

Delete

Export

Install

Install Identity certificate

Identity Certificate

☒ Install from a file: C:\Users\User\certnew.cer Browse

☐ Paste the certificate data in base-64 format:

Install Certificate Cancel Help

Repeat Alert Interval : 7 (days)

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Enroll ASA SSL certificate with Entrust

Using a previously saved certificate signing request, [enroll with Entrust](#).

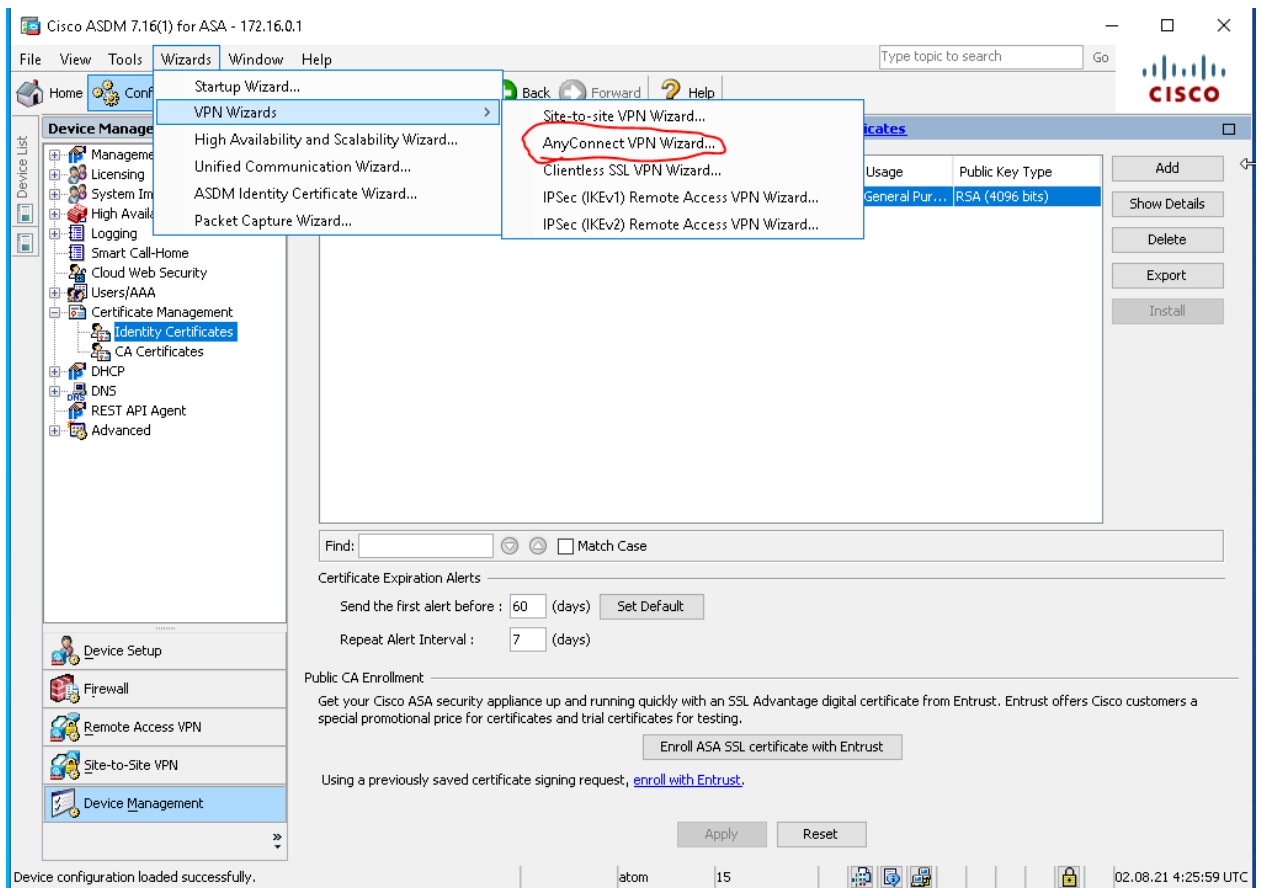
Apply Reset

Configuration changes saved successfully.

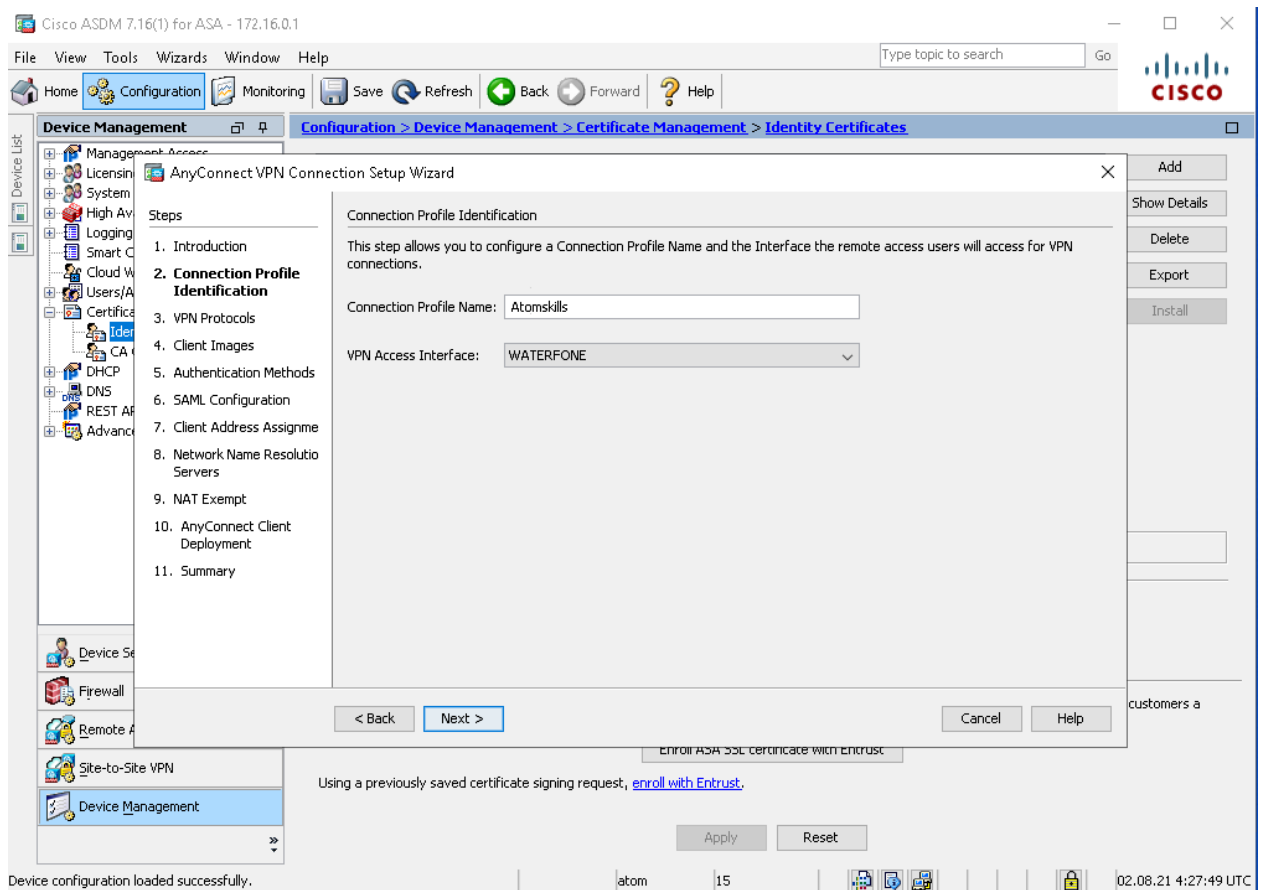
atom 15

02.08.21 4:23:39 UTC

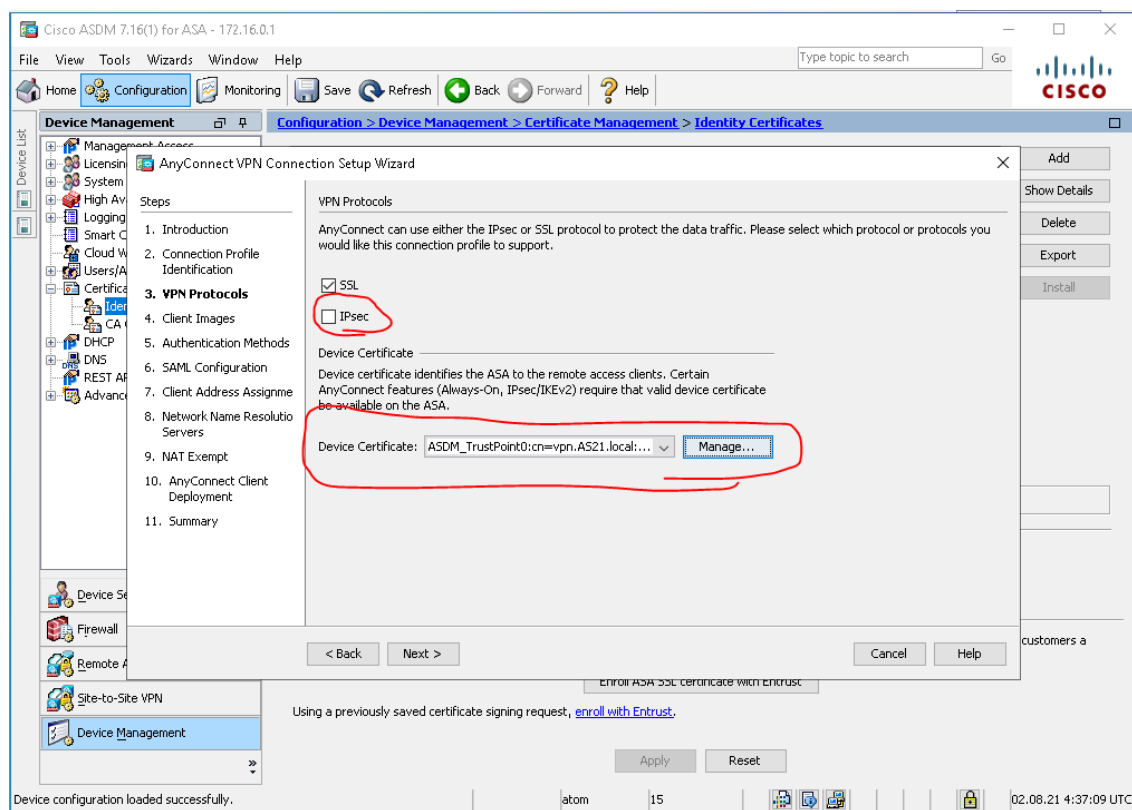
Выбираем серт и снова нажимаем Install



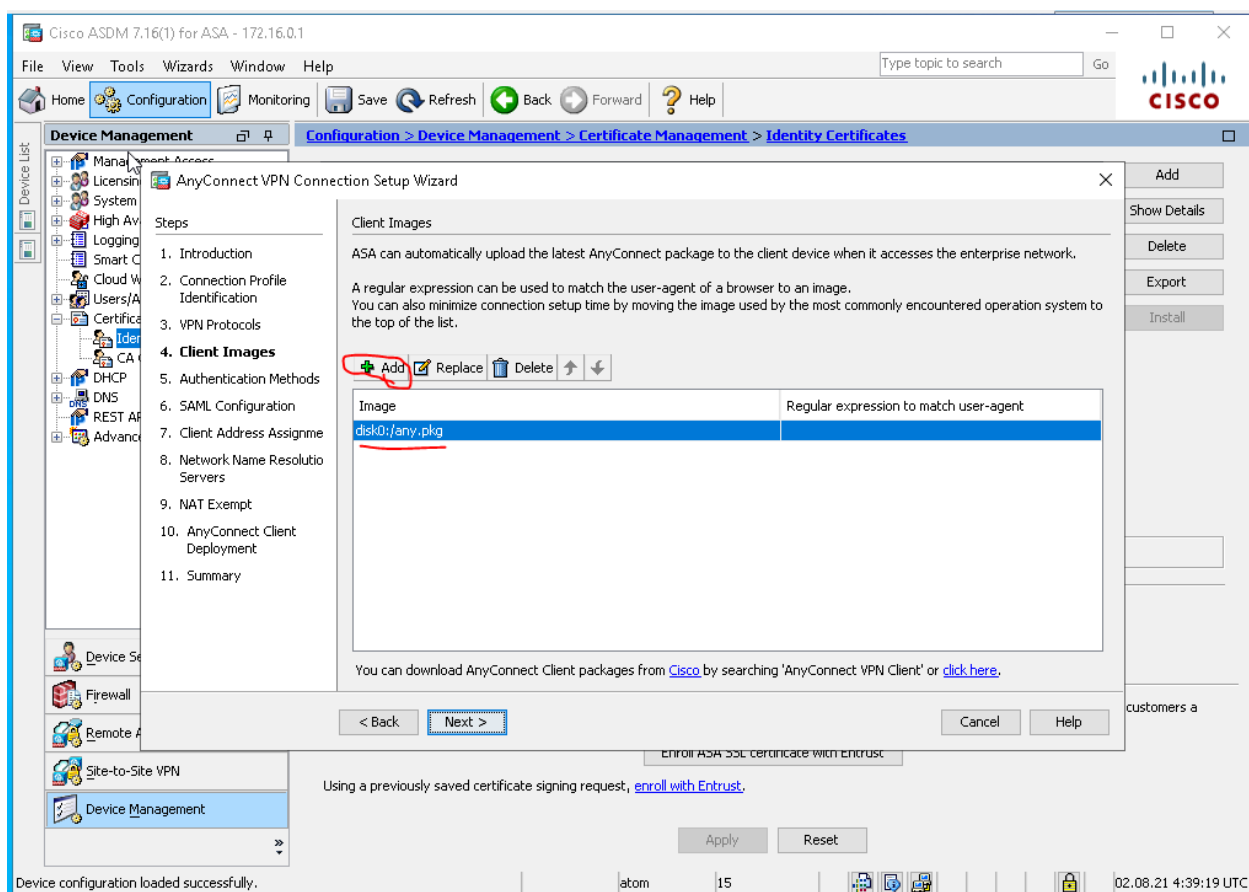
Теперь идем в Anyconnect wizard



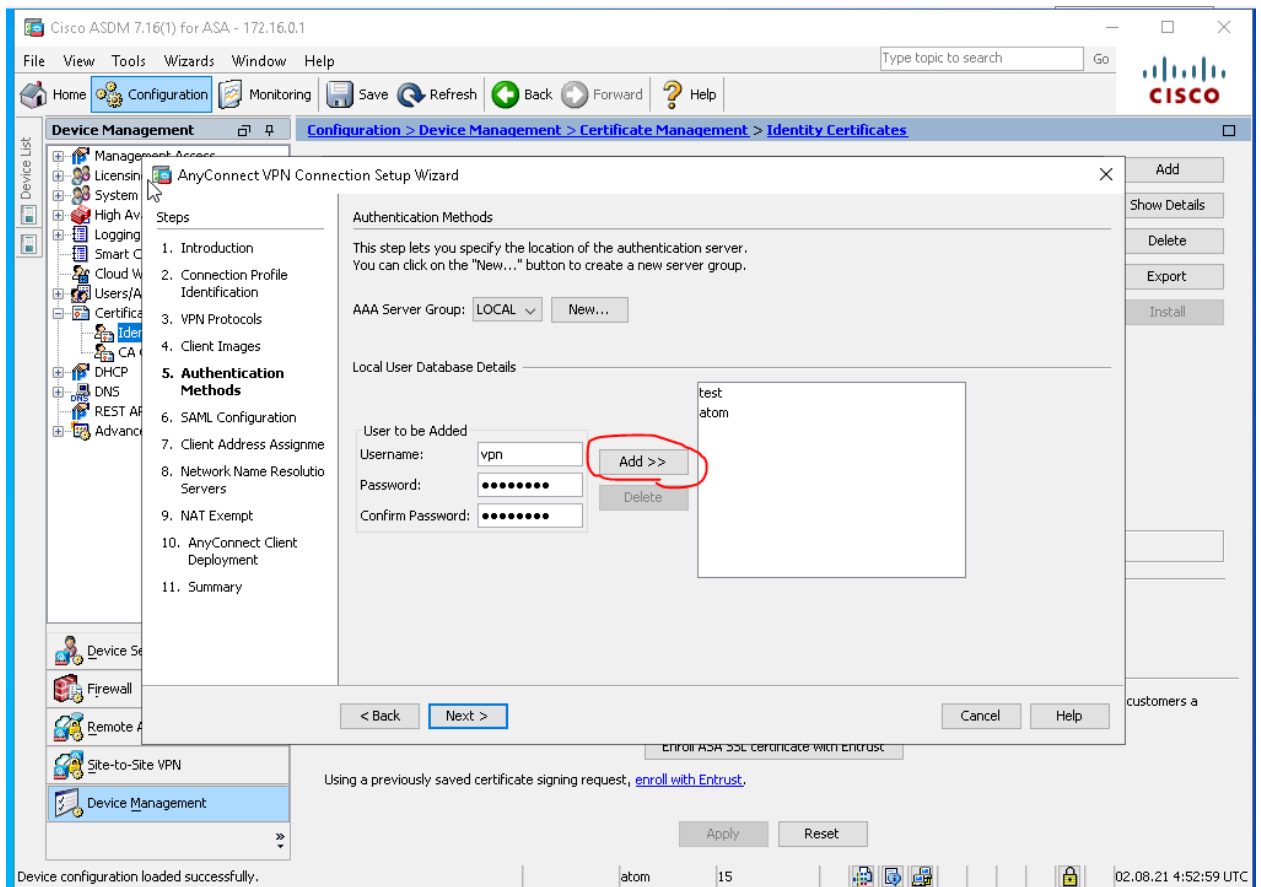
Пишем любое название профиля и выбираем внешний интерфейс



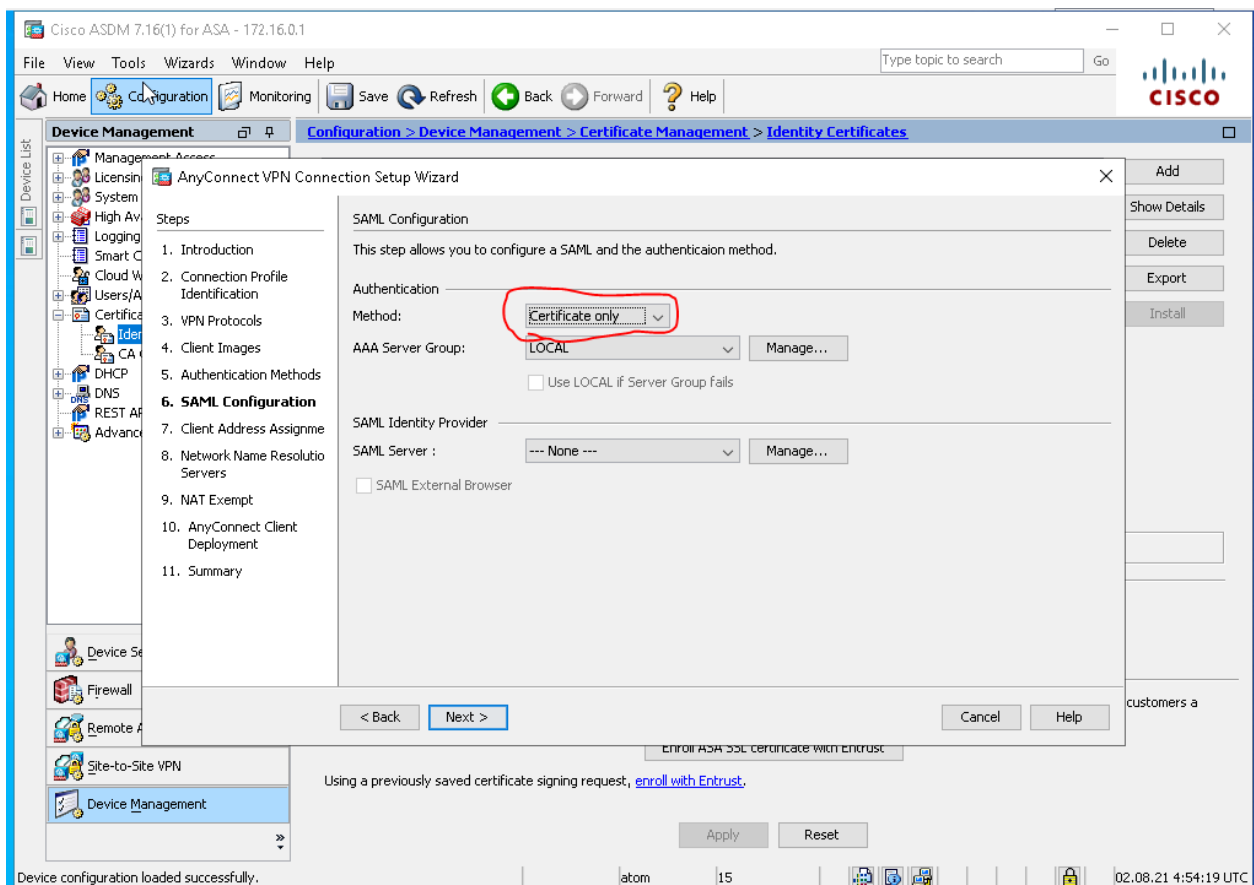
Выбираем серт, который мы залили ранее и отключаем IPSEC



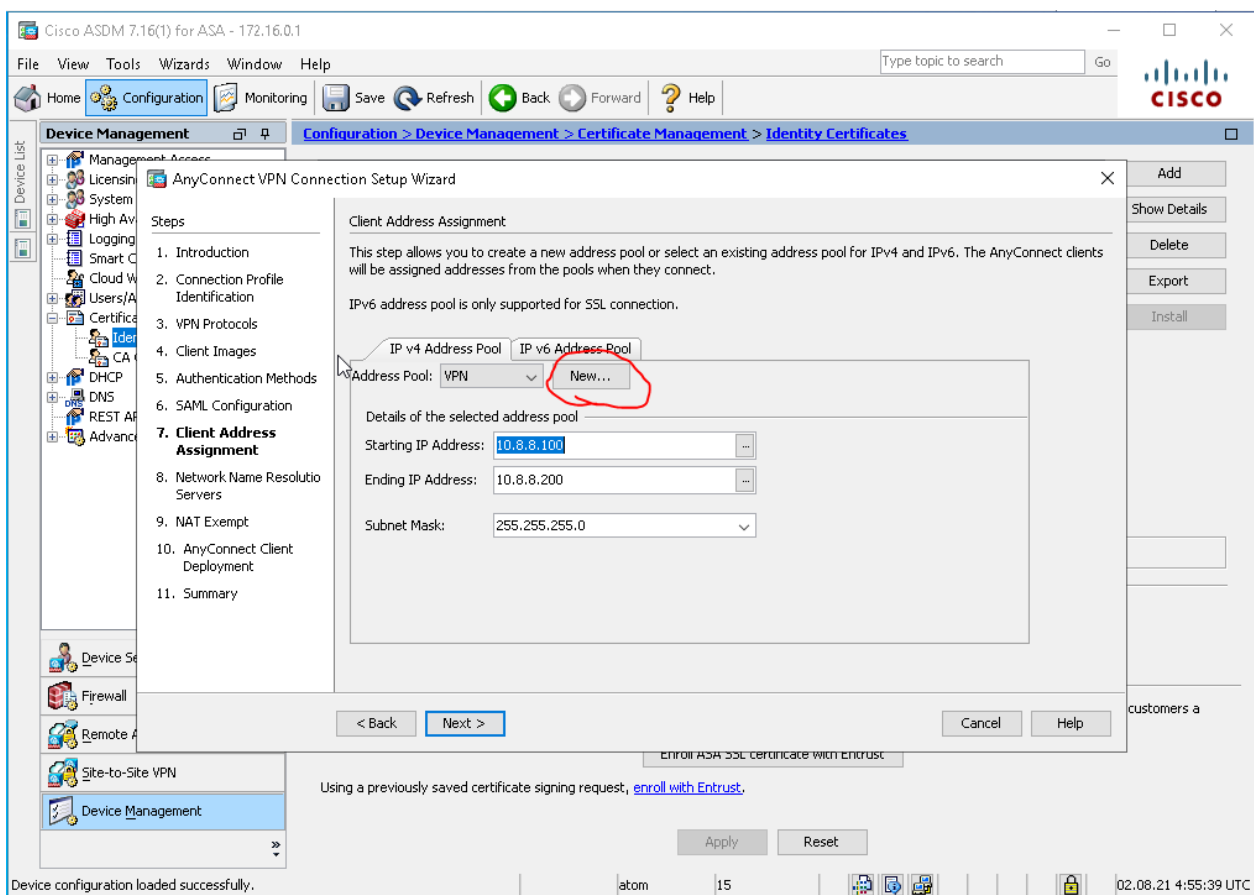
Тут выбираем клиентское изображение через add. Оно на флешке



Добавляем какого-нибудь юзера



Выбираем метод аутентификации только по сертам



Добавляем VPN подсеть

Cisco ASDM 7.16(1) for ASA - 172.16.0.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Certificate Management > Identity Certificates

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignment
8. Network Name Resolution Servers
9. NAT Exempt
10. AnyConnect Client Deployment
11. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 8.8.8.8

WINS Servers:

Domain Name:

< Back Next > Cancel Help

Enroll ASA SSL certificate with Entrust

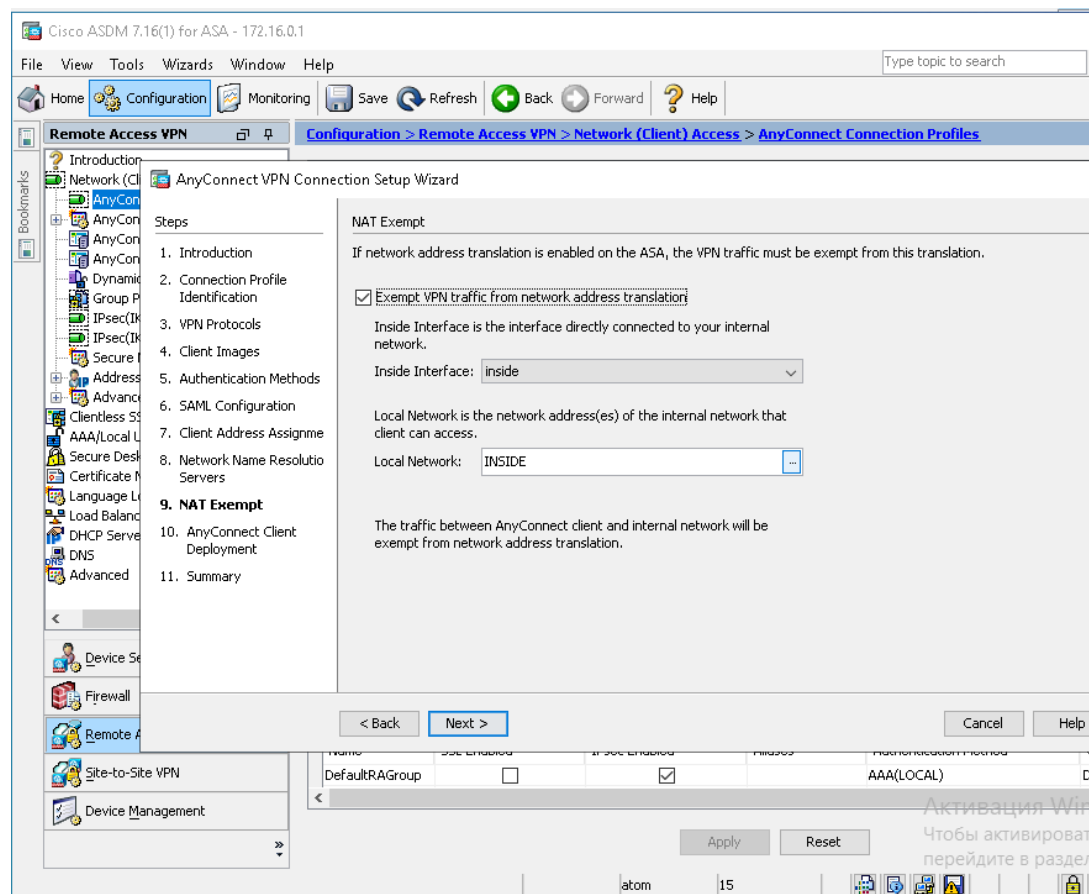
Using a previously saved certificate signing request, [enroll with Entrust](#).

Apply Reset

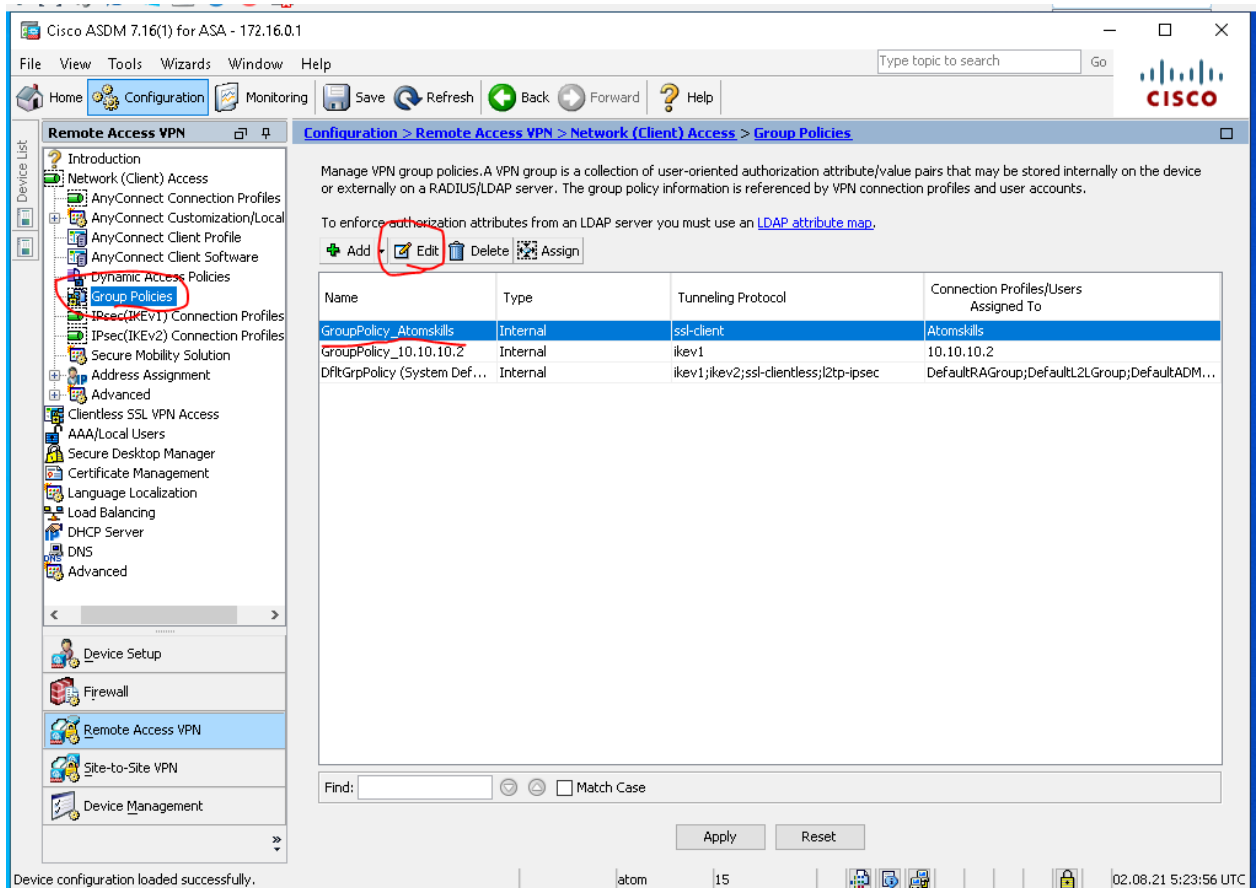
Device configuration loaded successfully.

Обращение к Корпане atom 15 02.08.21 4:56:59 UTC

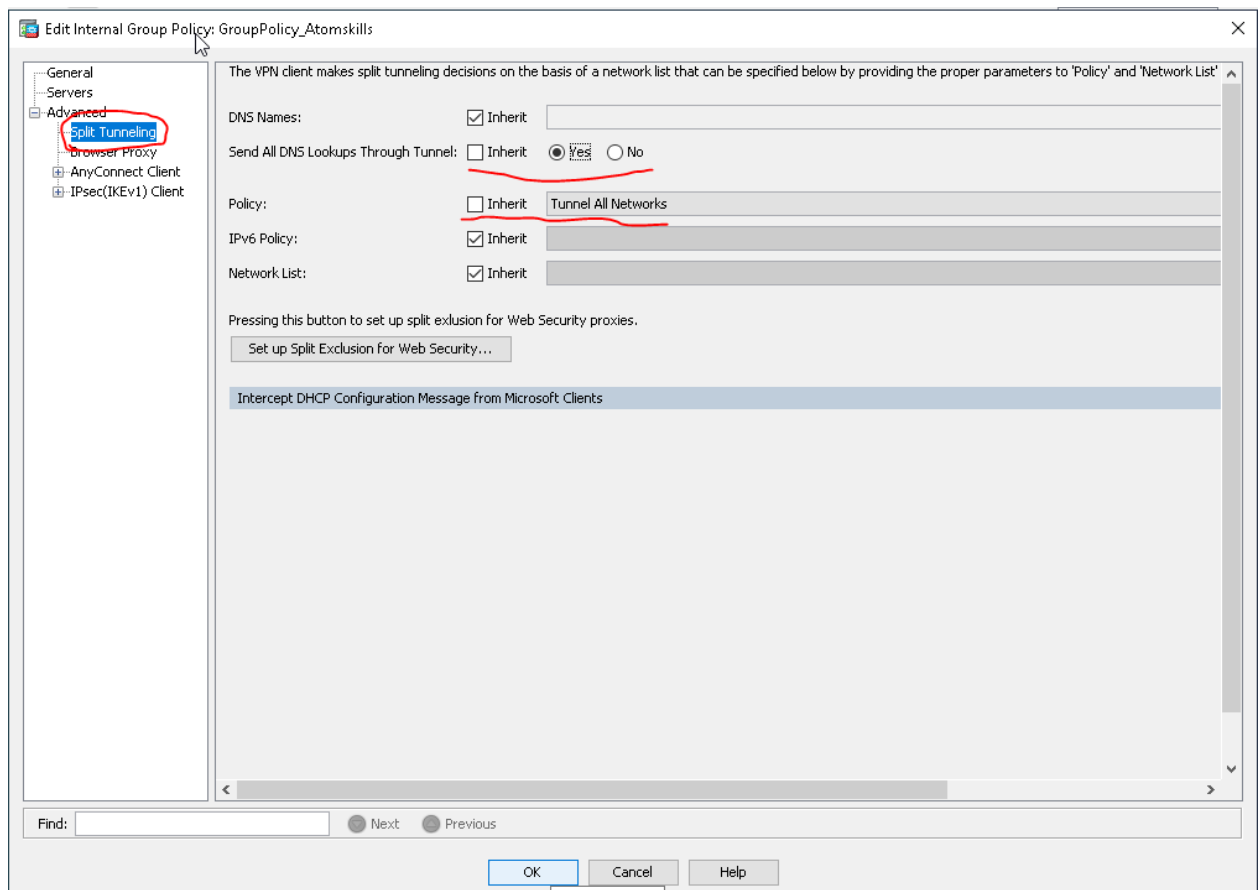
Добавляем DNS сервер



Делаем исключения из ната как на картинке
!!Сделай еще sh run nat и пропиши исключение из ната, чтоб
клиенты могли стучатся до LINA!!



Теперь идем в групповые политики и выбираем нашу



Делаем так, чтобы весь трафик ходил через туннель.

Забираем серт, переносим его на клиента, так же забираем рут и саб

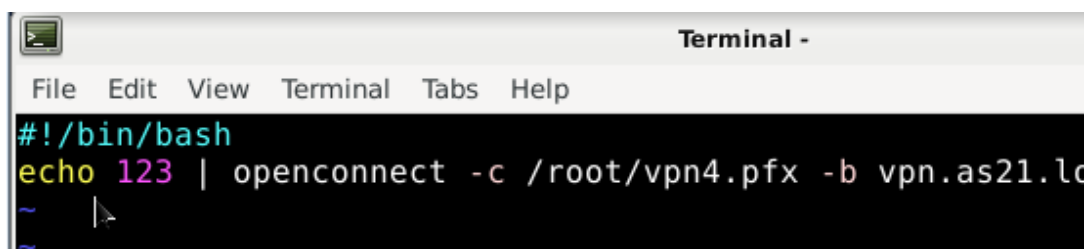
Копируем рут и саб в /usr/local/share/ca-certificates и делаем update-ca-trust

!!МИША МОКШАНЦЕВ, делать надо так, а не как ты обычно. У меня не взлетело.!!

После этого добавляем в hosts vpn.as21.local ну или для чего ты там выпустил серт (смотри CN серта на асе). Пробуем через curl или wget пойти на vpn.as21.local (то, что ты прибил в хостс). Если ошибок нет – тестим подключение

Openconnect –с cert.pfx vpn.as21.local

Если все норм подключилось – автоматизируем

A screenshot of a terminal window titled "Terminal -". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows a prompt "#!/bin/bash" followed by the command "echo 123 | openconnect -c /root/vpn4.pfx -b vpn.as21.local". The cursor is positioned at the end of the command line.

```
#!/bin/bash
echo 123 | openconnect -c /root/vpn4.pfx -b vpn.as21.local
```

123 это пароль от серта. Даем права на выполнение, загоняем в кронтаб и готово

4. Настройте соединение IPsec с помощью IKEv1 между ASA и HQ1

i. Используйте следующие параметры защиты IKEv1: аутентификация по общему ключу, AES128, SHA, DH5

ii. Используйте IPsec с помощью протокола ESP с шифрованием AES128 и хешем SHA.

iii. Необходимо защитить трафик между локальной сетью филиала и сетью LINA в центральном офисе, а также трафик от клиентов AnyConnect.

HQ1:

crypto isakmp policy 2 //Обрати внимание POLICY 2, если редачить первую – разнесешь DMVPN.

encryption aes 128

hash sha

group 5

authentication pre-share

crypto isakmp key cisco address 0.0.0.0 //просто бери ключ с DMVPN и не парься

ip access-list extended IPSEC //да да, именно extended, чтоб мы могли сделать NAT exemption

permit ip x.x.x.x x.x.x.x x.x.x.x x.x.x.x //пермитим из сетки LINA до сетки за асой. Так же пермитим из LINA до сетки Anyconnect

ip access-list extended NAT //если до этого юзал стандартный список – удали и сделай по новой

deny ip x.x.x.x x.x.x.x x.x.x.x x.x.x.x //Запрети трафик из сетки LINA в сетку за асой. Так же запрети из сети LINA в сетку anyconnect. Надо чтобы он не натился.

Permit ip x.x.x.x x.x.x.x any //тут разрешай все внутренние подсети до any, они будут натиться

Crypto ipsec transform-set IPSEC2 esp-aes 128 esp-sha-hmac //обрати внимание, название трансформ сета другое!!

Mode tunnel

Crypto map IPSEC2 1 ipsec-isakmp //внимательно смотри коммент, который высирает циска, там написано, что надо конфигурировать

Set peer 84.64.44.24 //соседемся с асой по ее внешнему адресу

Set transform-set IPSEC2 //тут название трансформсета

Match address IPSEC //тут название ацл

Int g0/0

Crypto map IPSEC2

Ip route x.x.x.x x.x.x.x 84.64.44.24 //пишем роут до сетки за асой через внешний адрес асы. Такой же роут делаем для anyconnect подсети.

ASA:

Crypto ikev1 policy 1

Encryption aes

Hash sha

Group 5

Authentication pre-share

Crypto ikev1 enable WATERPHONE //включаем ikev1 на внешнем интф

Tunnel-group 178.207.179.29 type ipsec-l2l //Обязательно пиши внешний HQ1

Tunnel-group 178.207.179.29 ipsec-attributes

Ikev1 pre-shared-key cisco //Такой же как на HQ1

Object network SRCNET

Subnet x.x.x.x x.x.x.x //тут надо написать адрес сети за асой

Object network DSTNET

Subnet x.x.x.x x.x.x.x //тут надо написать адрес сети LINA

Object network ANYNET

Subnet x.x.x.x x.x.x.x //тут надо написать адрес anyconnect сети

Access-list 100 extended permit ip object SRCNET object DSTNET

//разрешаем трафик из сети за асой до LINA

Access-list 100 extended permit ip object ANYNET object DSTNET

//разрешаем трафик от anyconnect сети до сети LINA

nat (inside,WATERFONE) source static SRCNET SRCNET destination static DSTNET DSTNET no-proxy-arp route-lookup //делаем исключение из ната для сети за асой

nat (inside,WATERFONE) source static ANYNET ANYNET destination static DSTNET DSTNET no-proxy-arp route-lookup //делаем исключение для сетки anyconnect

!!NAT из сетки асы до провайдера после этого сломаться не должен! Проверь, если он сломался – удали эти правила и сделай нормально!!

Crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac

Crypto map IPSEC 1 set peer 178.207.179.29 //соседемся по внешнему HQ1

Crypto map IPSEC 1 match address 100 //матчим по ацл который мы создали выше

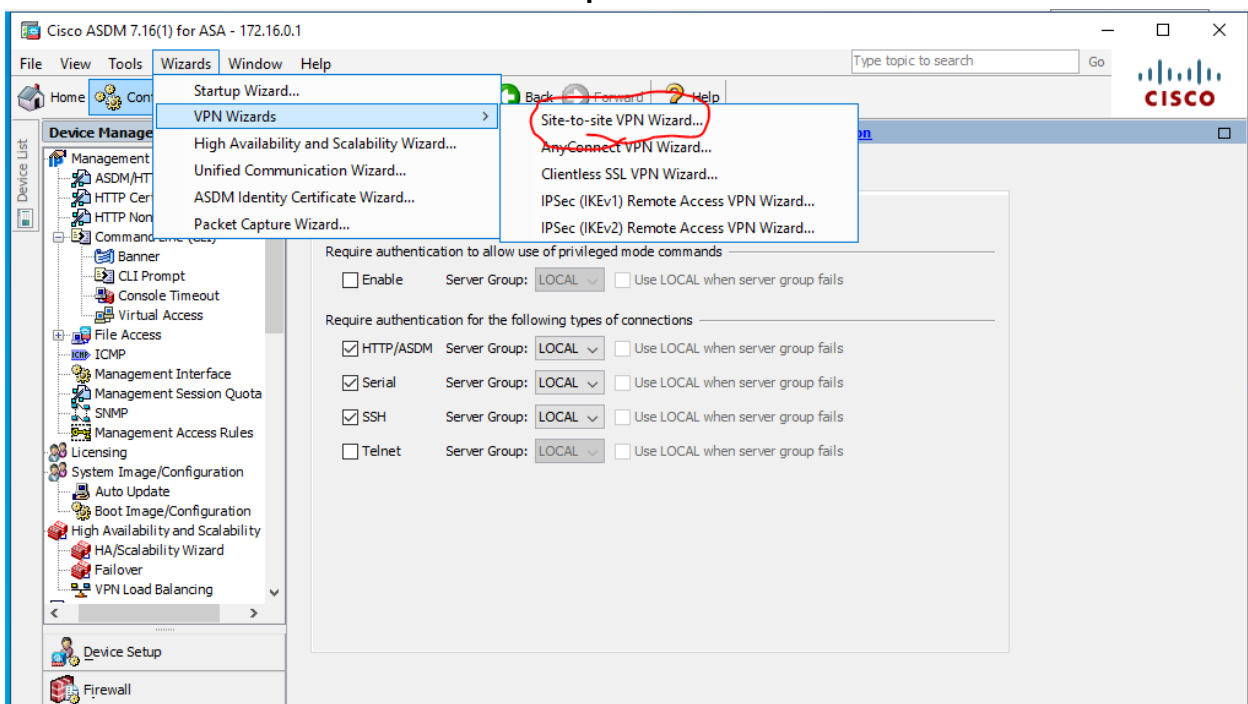
Crypto map IPSEC 1 ikev1 transform-set IPSEC //трансформсет который мы создали выше

Crypto map IPSEC interface WATERFONE //включаем карту на внешний интерфейс

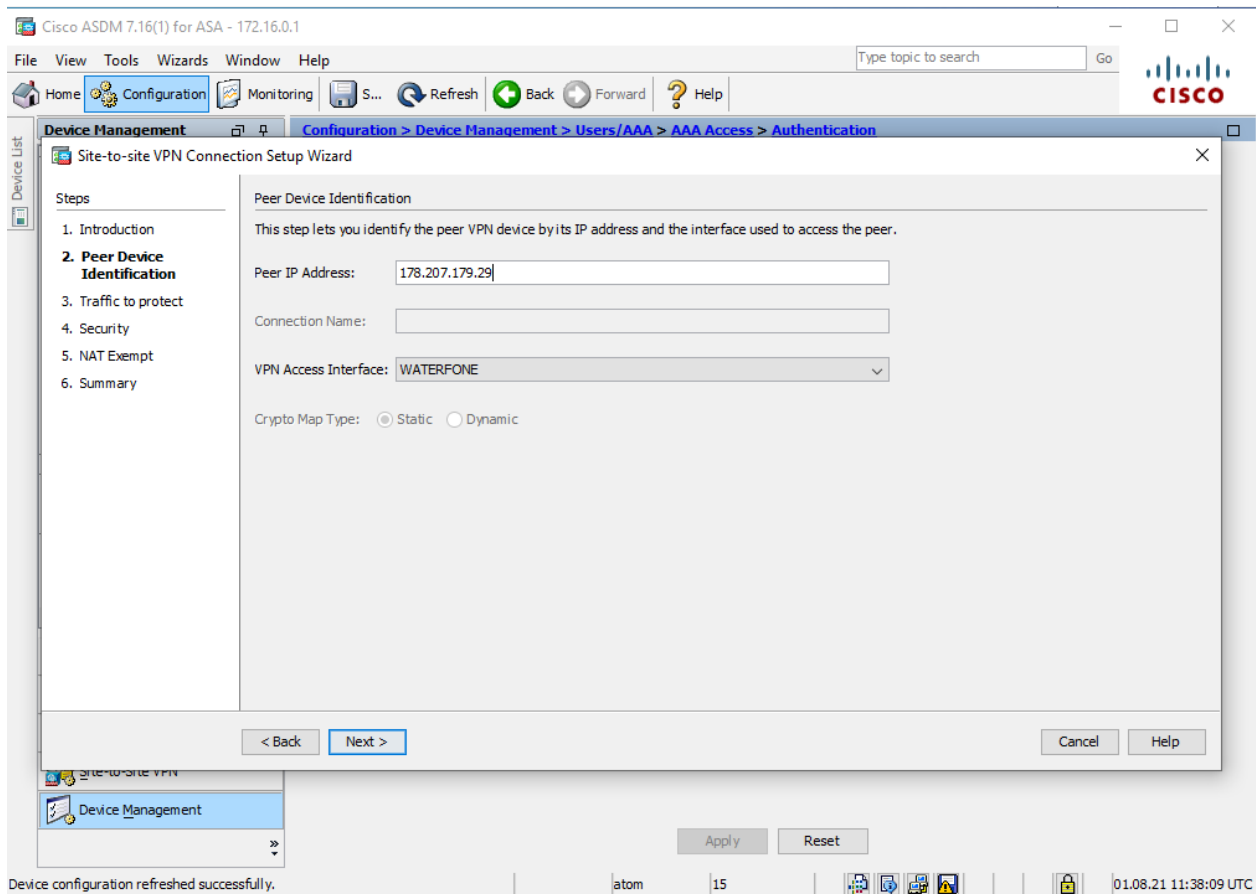
Route WATERFONE x.x.x.x x.x.x.x 178.207.179.29 //Пишем роут до сети LINA через внешний HQ1

!!Если все сделано правильно – пинги будут ходить в инет, в сеть LINA из сети за асой и через anyconnect!!

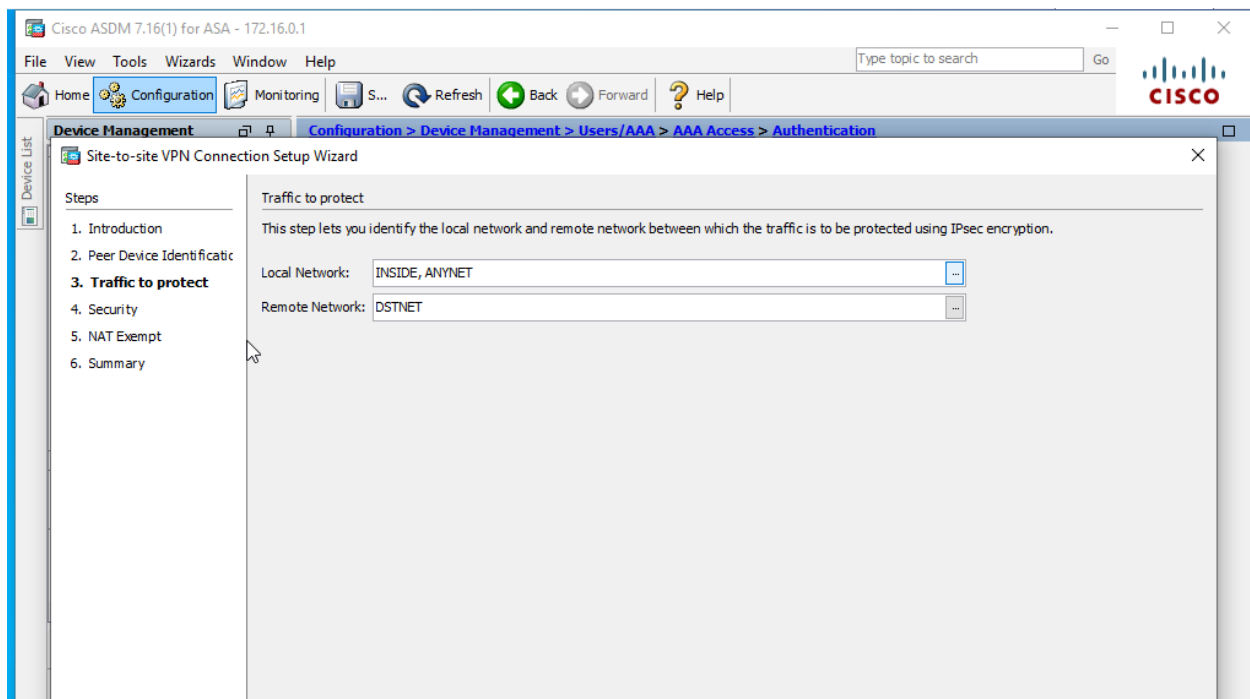
!!То же самое через ASDM!!



Идем как на картинке



Пишем внешний адрес HQ1. Интерфейс тоже внешний.



Указывает объекты локальной и удаленной сети

Cisco ASDM 7.16(1) for ASA - 172.16.0.1

File View Tools Wizards Window Help

Home Configuration Monitoring S... Refresh Back Forward Help

Device Management Configuration > Device Management > Users/AAA > AAA Access > Authentication

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. **Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

☐ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

☒ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy

☒ IKE version 1

☐ IKE version 2

< Back Next > Cancel Help

Ставим custom configuration, убираем ikev2

Cisco ASDM 7.16(1) for ASA - 172.16.0.1

File View Tools Wizards Window Help

Home Configuration Monitoring S... Refresh Back Forward Help

Device Management Configuration > Device Management > Users/AAA > AAA Access > Authentication

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. **Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

☐ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

☒ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy

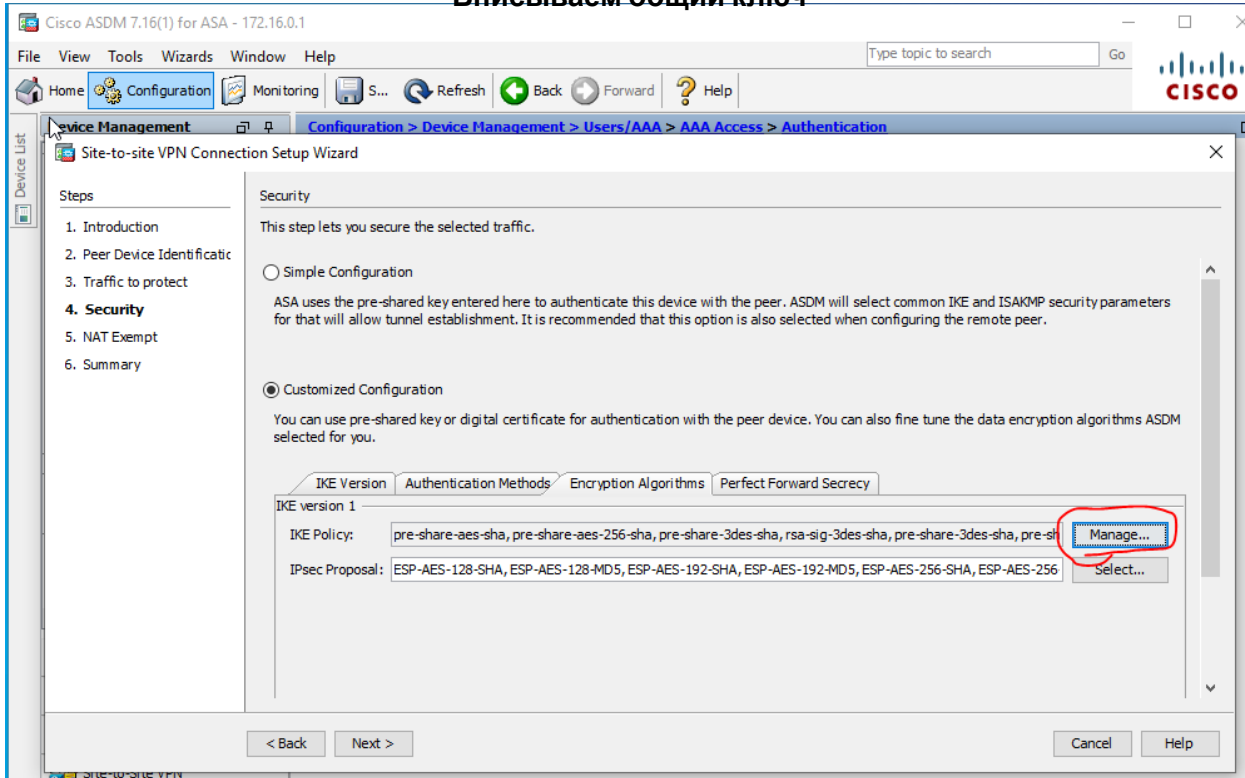
IKE version 1

Pre-shared Key:

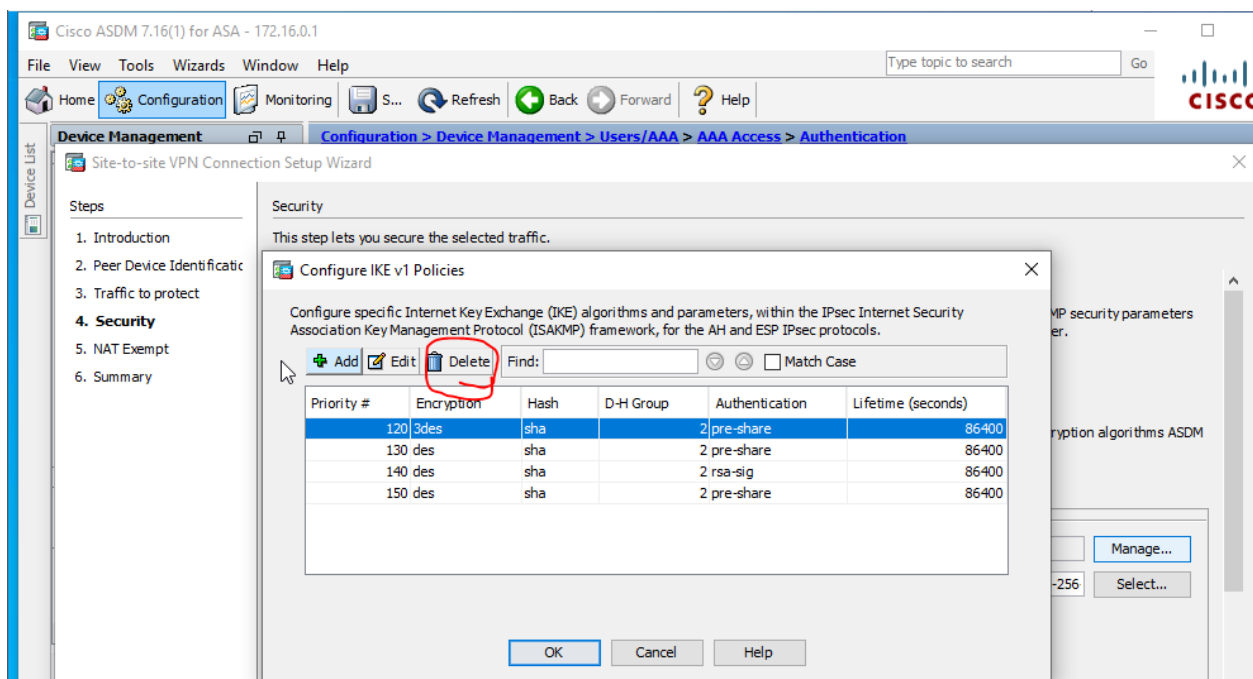
Device Certificate: -- None -- Manage...

< Back Next > Cancel Help

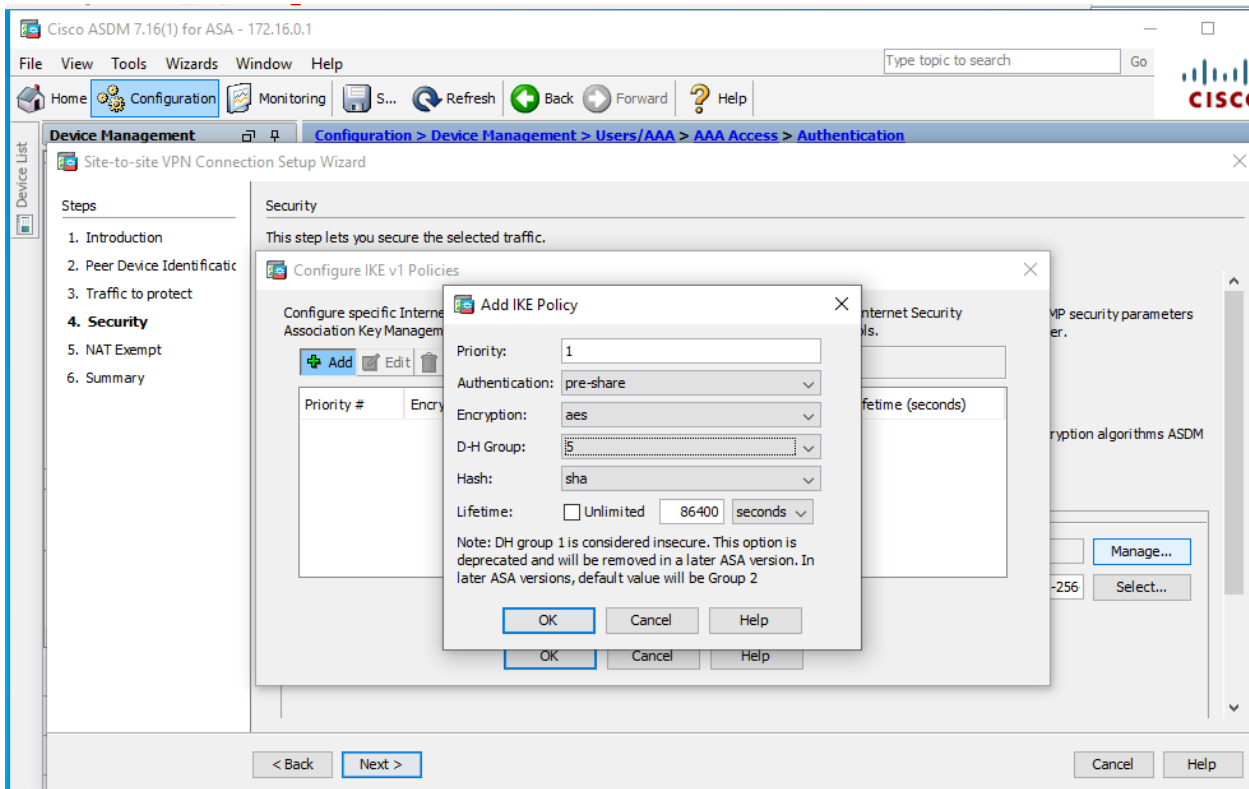
Вписываем общий ключ



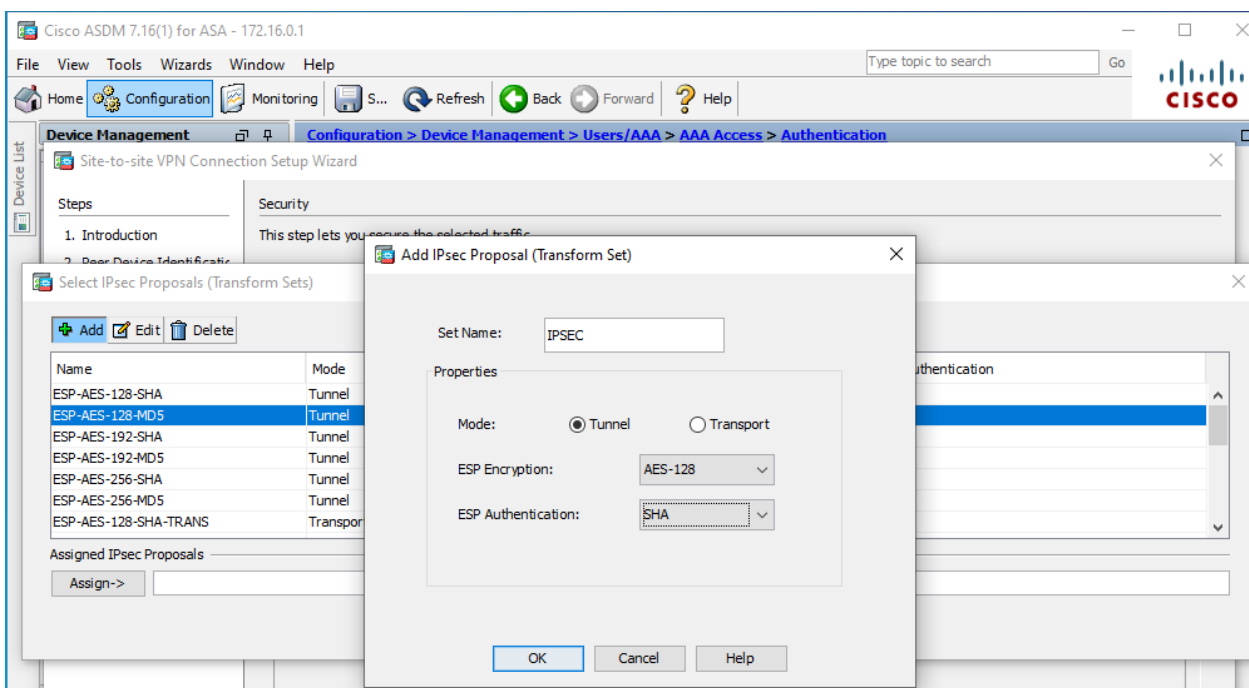
Тут нажимаем Manage



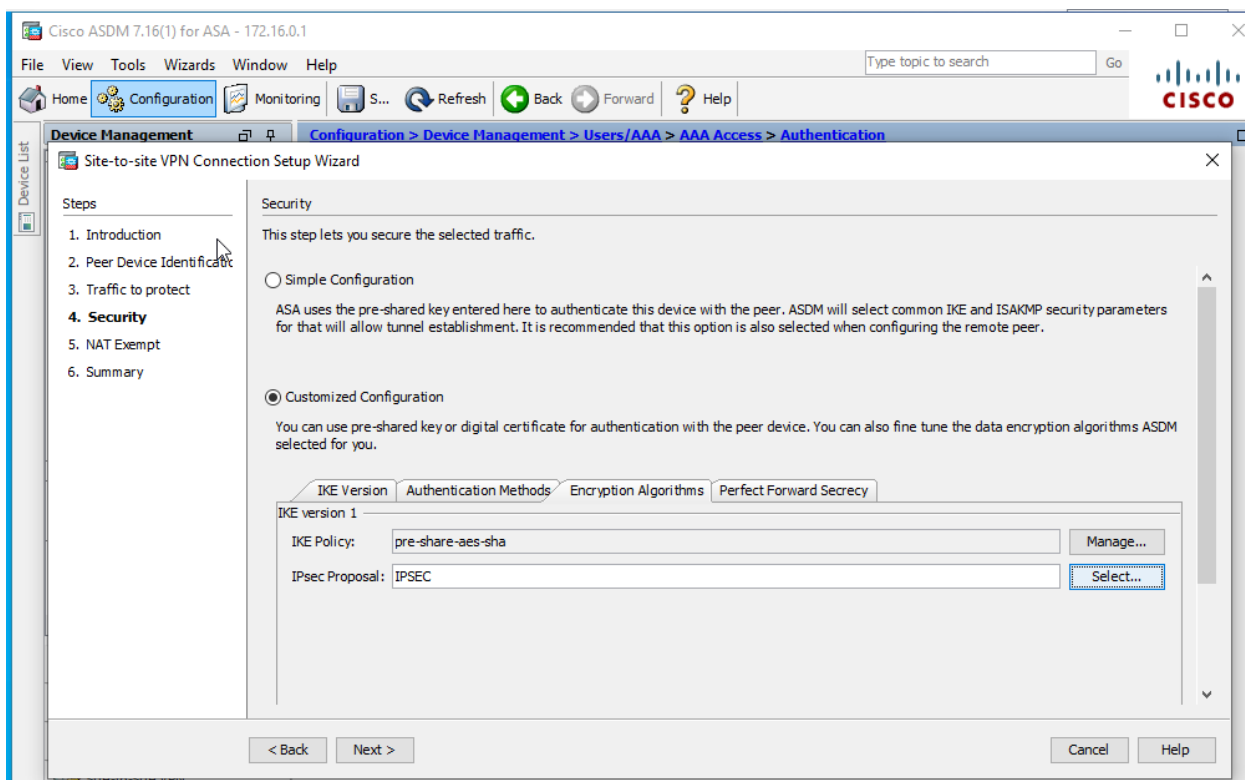
Удаляем все, что есть и нажимаем add



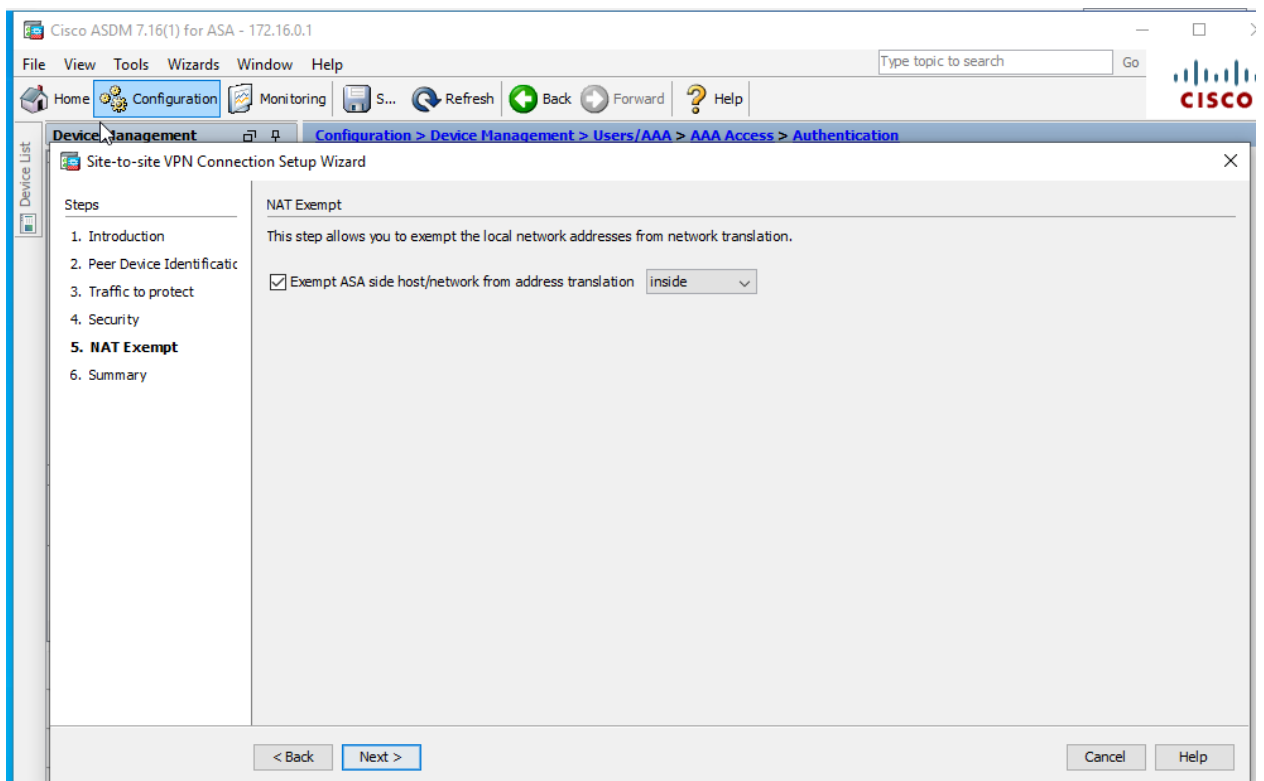
Вписываем параметры как по заданию, такие же как на HQ1 и нажимаем OK



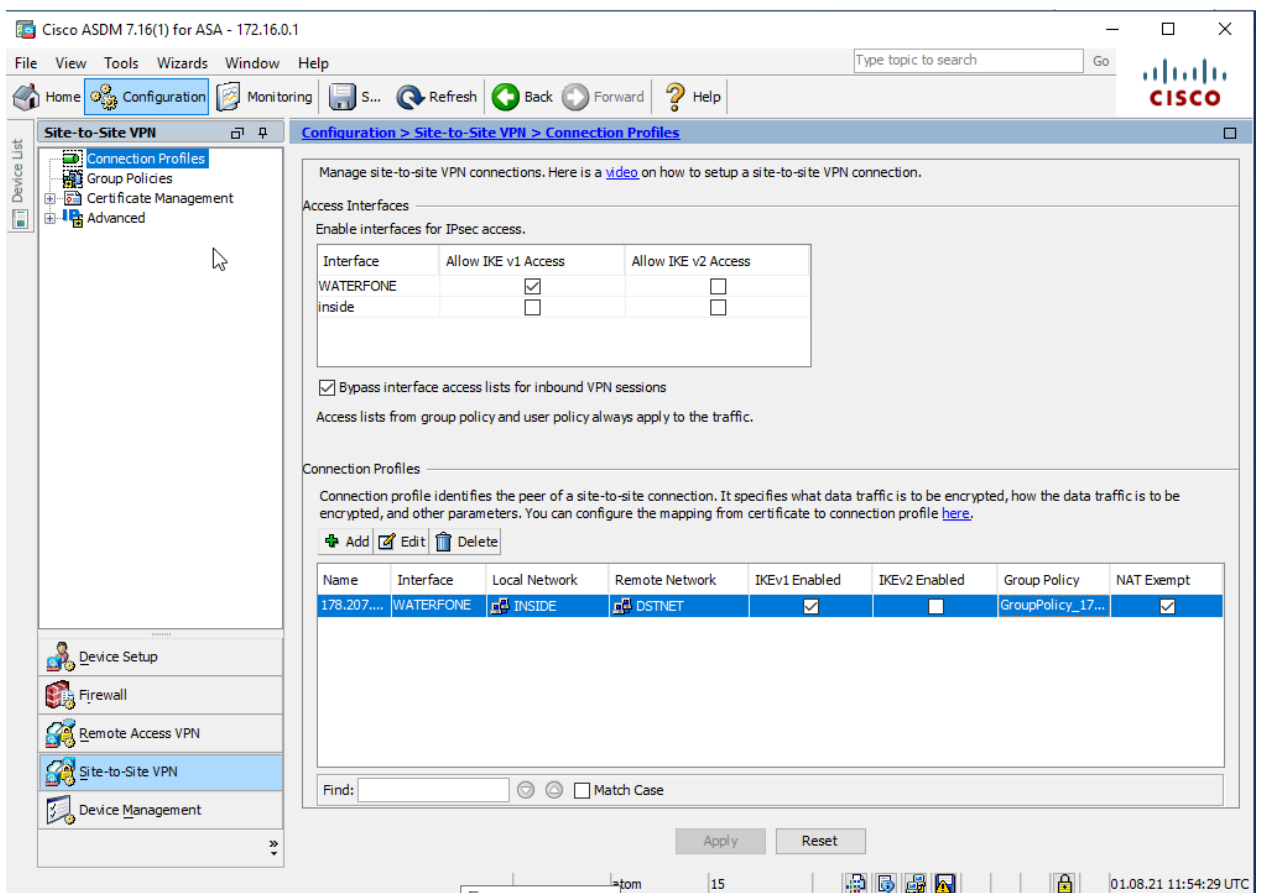
На IPSEC тоже жмем Manage и сразу жмем ADD, удалять там ничего не надо.
Прописываем параметры по заданию и добавляем



В конце должно получиться так



NAT exempt вешаем на inside
!!Второй exempt добавляем руками!!



Собсна все, идем проверять.
!!не забудь руками добавить роут!!

Настройка сети филиала 3

!!Дефолтные креды: admin/Admin@123!!

!!Для входа в en пиши system-view!!

!!Для сохранения конфиги выходим в unprivileged (quit) и пишем save!!

1. Настройте на межсетевом экране USG IP-адреса для связи с провайдером и для локальной сети филиала.

int g1/0/1

ip address x.x.x.x xx //В хвавей можно маску по пацански писать e.g. 172.16.0.1 24. Адрес придумай сам

service-manage enable //Включаем менеджмент разрешаем все

service-manage http permit

service-manage https permit

service-manage ping permit

service-manage ssh permit

security-policy

default-action permit //чтоб пинги норм ходили

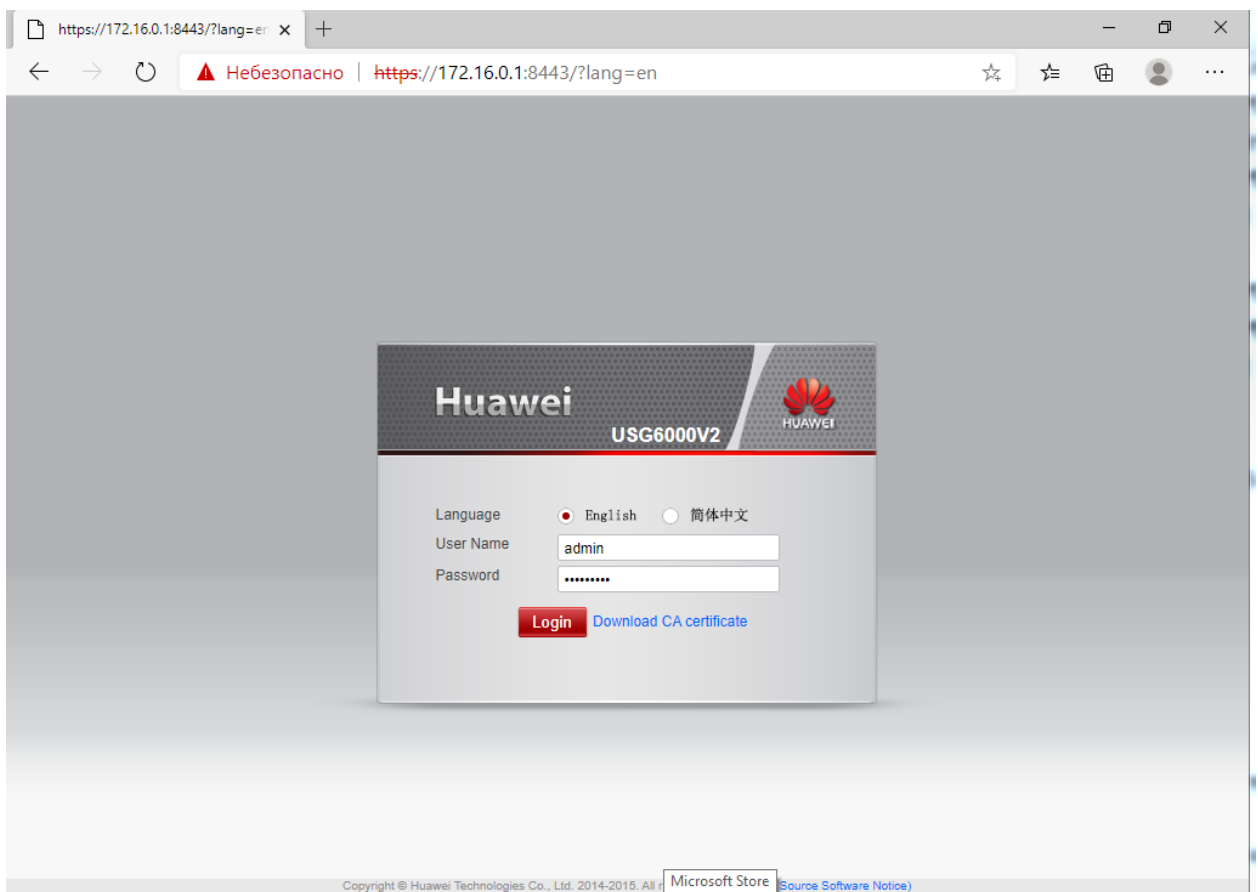
firewall zone trust

add interface g1/0/1

!!После этого идем на веб морду

<https://x.x.x.x:8443>

Через edge работает прекрасно!!



2. Настройте на межсетевом экране USG DHCP-сервер. Клиент WINCLIZ должен автоматически получать адрес по DHCP.
- i. Используйте адрес MOOGLE в качестве адреса DNS сервера для клиентов сети.

После логина откроется стартап визард – его не стоит скипать

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

Welcome to Startup Wizard

This wizard will guide you to complete the basic firewall configurations and to connect to the Internet.

☐ Do not display this page upon the next login

< Back Next > Cancel

Нажимаем далее

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

Basic Configuration

Enter the host name.

Host Name USG

You are advised to change the administrator password upon your first login.

☐ Change Administrator Password

Old Password

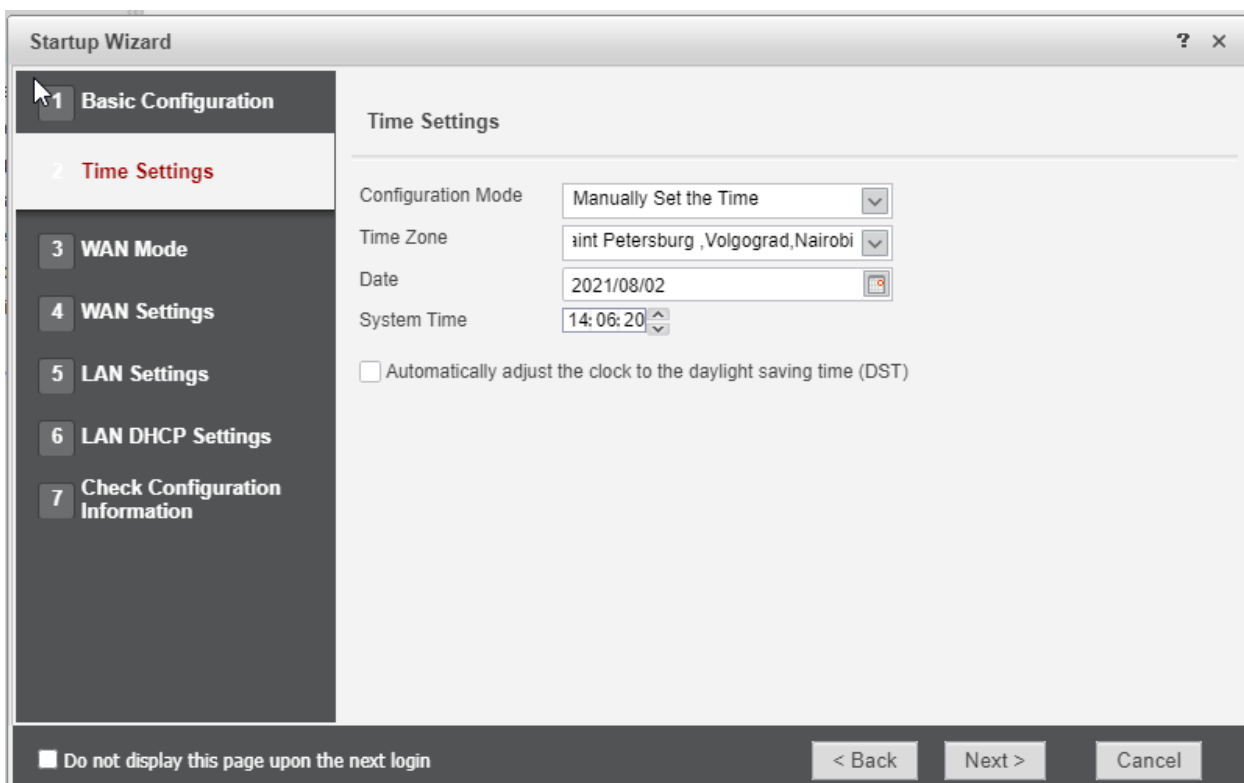
New Password

Confirm

☐ Do not display this page upon the next login

< Back Next > Cancel

Меняем хостнейм. Щербинин сказал, что пароль по умолчанию будет P@ssw0rd и его можно будет оставить, по этому пасс не меняем.



The image shows the 'Startup Wizard' window, specifically the 'Time Settings' step. On the left, a sidebar lists seven steps: 1 Basic Configuration, 2 Time Settings (highlighted in red), 3 WAN Mode, 4 WAN Settings, 5 LAN Settings, 6 LAN DHCP Settings, and 7 Check Configuration Information. The main area is titled 'Time Settings' and contains the following fields: 'Configuration Mode' set to 'Manually Set the Time', 'Time Zone' set to 'Saint Petersburg, Volgograd, Nairobi', 'Date' set to '2021/08/02', and 'System Time' set to '14:06:20'. There is an unchecked checkbox for 'Automatically adjust the clock to the daylight saving time (DST)'. At the bottom, there is a checkbox 'Do not display this page upon the next login' and three buttons: '< Back', 'Next >', and 'Cancel'.

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

Time Settings

Configuration Mode: Manually Set the Time

Time Zone: Saint Petersburg, Volgograd, Nairobi

Date: 2021/08/02

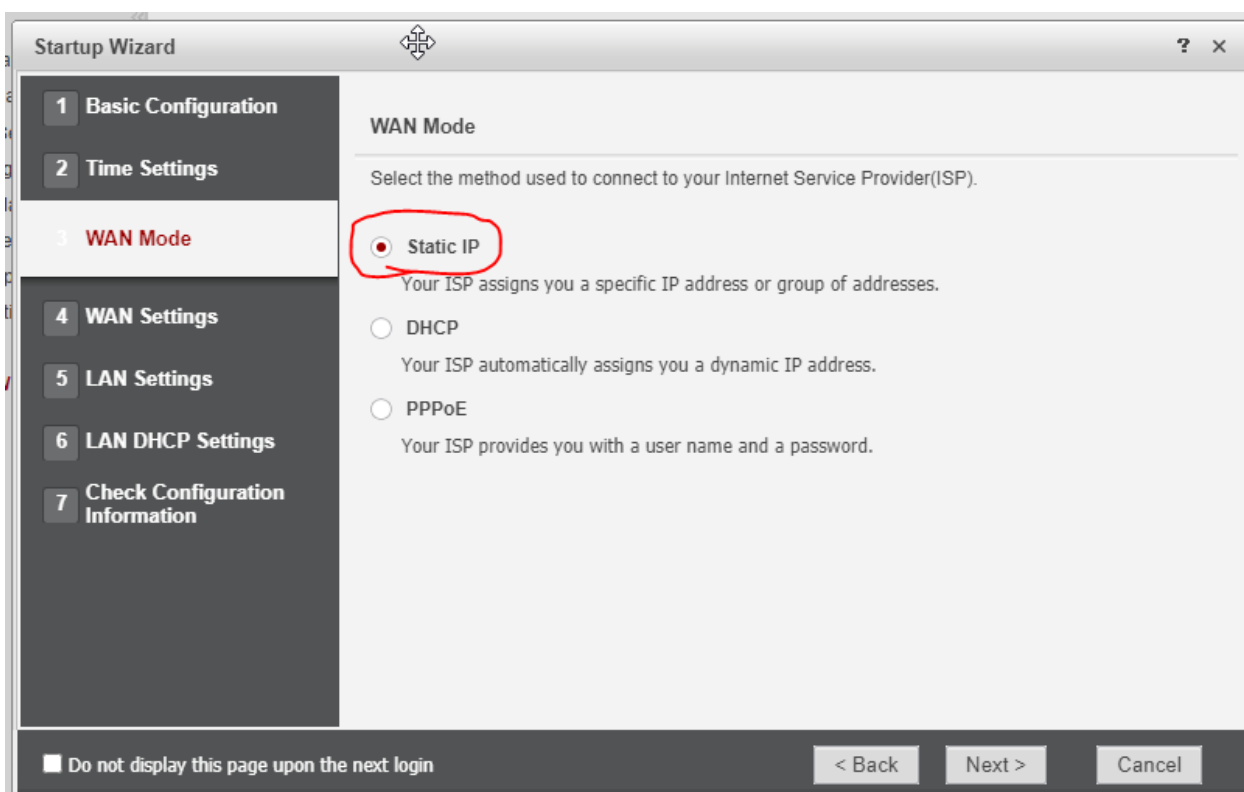
System Time: 14:06:20

☐ Automatically adjust the clock to the daylight saving time (DST)

☐ Do not display this page upon the next login

< Back Next > Cancel

Выставляем правильное время, это важно



The image shows the 'Startup Wizard' window, specifically the 'WAN Mode' step. On the left, the sidebar lists the same seven steps as the previous screen, but 'WAN Mode' (step 3) is now highlighted in red. The main area is titled 'WAN Mode' and contains the text 'Select the method used to connect to your Internet Service Provider(ISP)'. There are three radio button options: 'Static IP' (which is selected and circled in red), 'DHCP', and 'PPPoE'. Below each option is a descriptive sentence: 'Your ISP assigns you a specific IP address or group of addresses.' for Static IP, 'Your ISP automatically assigns you a dynamic IP address.' for DHCP, and 'Your ISP provides you with a user name and a password.' for PPPoE. At the bottom, there is a checkbox 'Do not display this page upon the next login' and three buttons: '< Back', 'Next >', and 'Cancel'.

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

WAN Mode

Select the method used to connect to your Internet Service Provider(ISP).

☒ Static IP
Your ISP assigns you a specific IP address or group of addresses.

☐ DHCP
Your ISP automatically assigns you a dynamic IP address.

☐ PPPoE
Your ISP provides you with a user name and a password.

☐ Do not display this page upon the next login

< Back Next > Cancel

Тут ставим static IP

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 **WAN Settings**

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

WAN Settings -- Static IP

Set the following parameters to connect to the Internet.

Contact your ISP for the information.

Interface	GE1/0/0 *
IP Address	62.33.111.111 *
Subnet Mask	255.255.255.128 *
Default Gateway	62.33.111.1 *
Primary DNS Server	8.8.8.8 *
Secondary DNS Server	

☐ Do not display this page upon the next login

< Back Next > Cancel

Заполняем настройки подключения к провайдеру как по заданию

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 **LAN Settings**

6 LAN DHCP Settings

7 Check Configuration Information

LAN Settings

Enter the information about the LAN interface.

You are advised to use a "private" address (such as 10.0.0.1 or 192.168.0.1). The default values below will work well for most networks.

Interface	GE1/0/1 *
IP Address	172.16.20.1 *
Subnet Mask	255.255.255.0 *

☐ Do not display this page upon the next login

< Back Next > Cancel

Указываем LAN интерфейс, сеть придумай сам !!НЕ КАК НА АСЕ!!

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

LAN DHCP Settings

☒ Enable DHCP Server on LAN

Enter the IP address range assigned to devices on the LAN.

Start IP Address: 172.16.0.100

End IP Address: 172.16.0.200

☐ Do not display this page upon the next login

< Back Next > Cancel

Включаем DHCP

Startup Wizard

1 Basic Configuration

2 Time Settings

3 WAN Mode

4 WAN Settings

5 LAN Settings

6 LAN DHCP Settings

7 Check Configuration Information

Check Configuration Information

Internet

Outside

Interface: GE1/0/0
 IP Address: 20.20.20.2
 Subnet Mask: 255.255.255.252
 Default Gateway: 20.20.20.1
 Primary DNS Server: 8.8.8.8
 Secondary DNS Server:

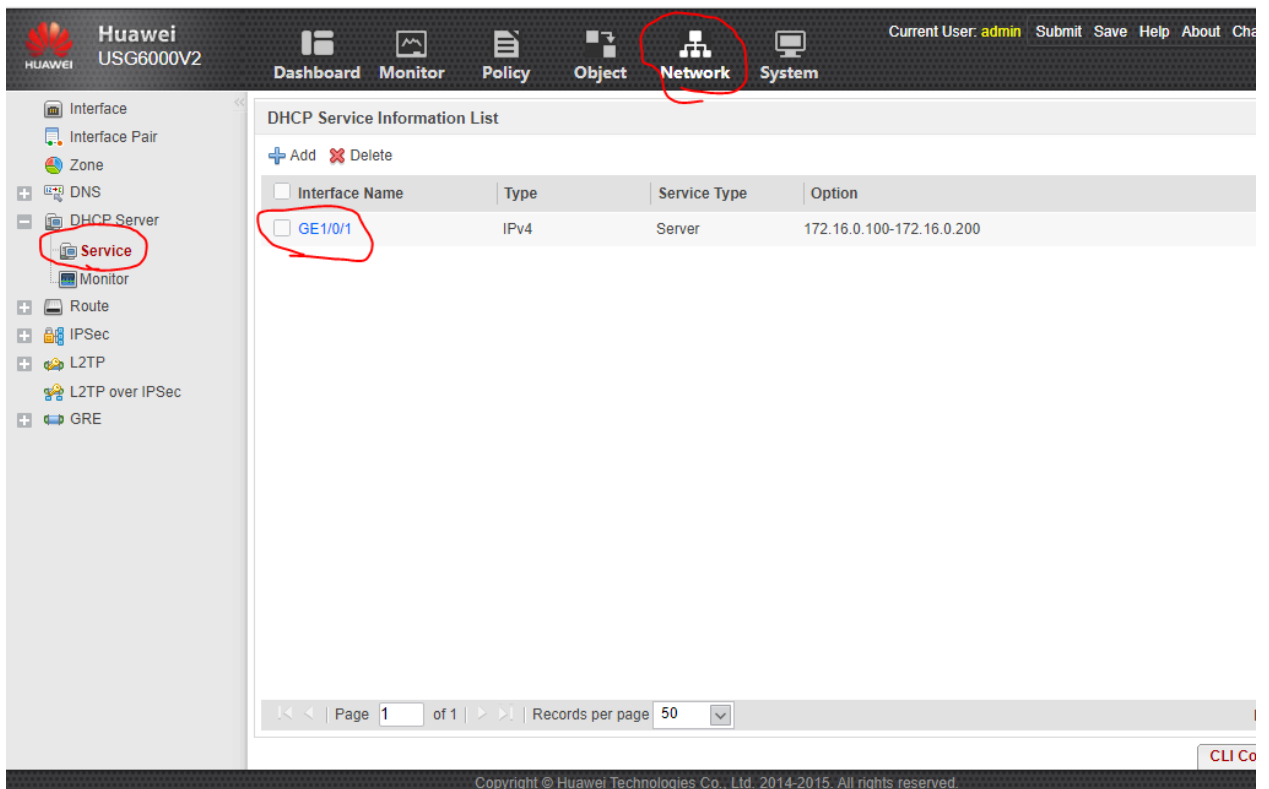
Inside

Interface: GE1/0/1
 IP Address: 172.16.0.1
 Subnet Mask: 255.255.255.0
 Enable DHCP Server on LAN:
 172.16.0.100_172.16.0.200

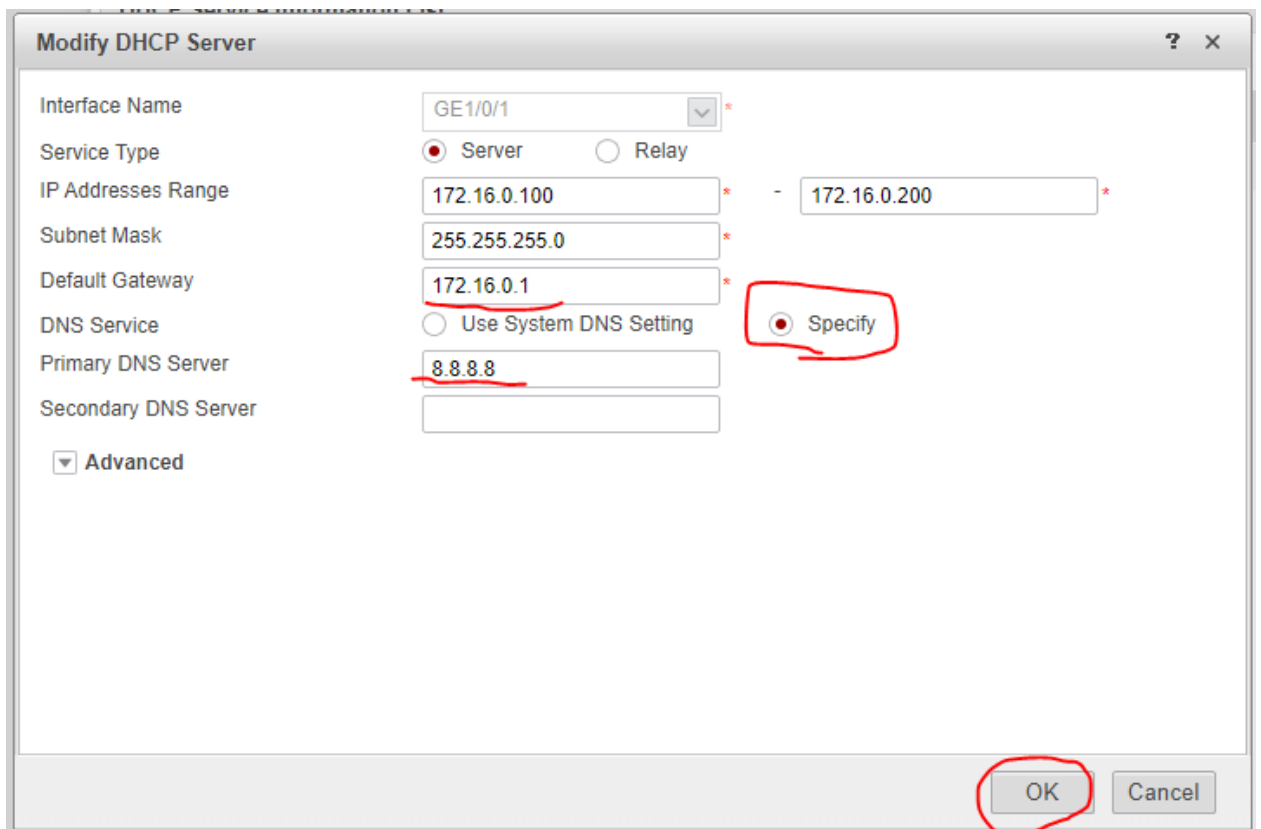
☒ Do not display this page upon the next login

< Back Apply Cancel

Проверяй, что все норм, ставь галку и жми apply. DHCP настроится сильно базовый, по этому его надо отредачить.



Нажимаешь на Network, идешь в DHCP, нажимаешь на интерфейс



Дописываем шлюз, указываем DNS и жмем ОК.

!!Не забудь проверить, что DHCP работает и переключить комп на получение адреса по DHCP!!

3. Настройте NAT и обеспечьте доступ в интернет для клиентов локальной сети.

Если ты протыкал визард, то у тебя уже будет нат. Не забудь проверить, что он работает.

4. Настройте GRE-туннель между межсетевым экраном USG и маршрутизатором HQ2 в центральном офисе.

i. На маршрутизаторе HQ2 используйте туннельный интерфейс с номером 3.

HQ2:

Int tun 3

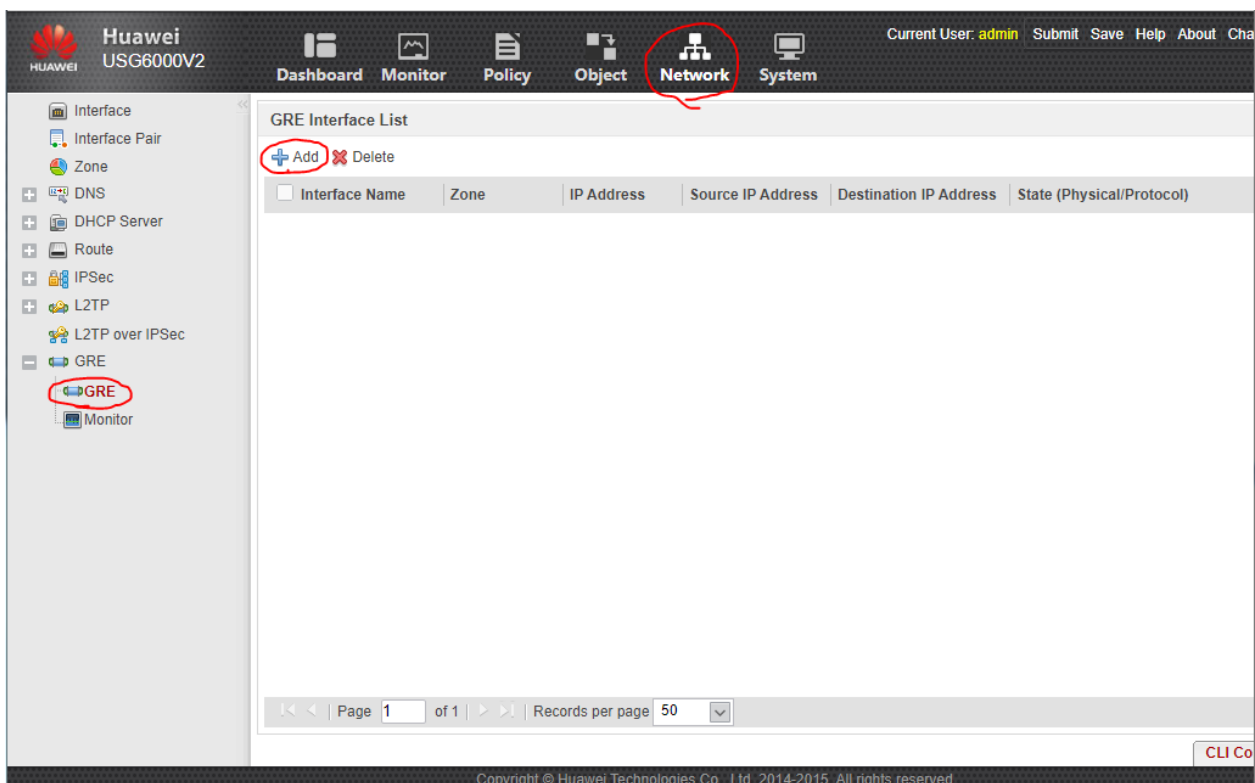
Ip address x.x.x.x x.x.x.x //придумай сам

Tun source g0/0

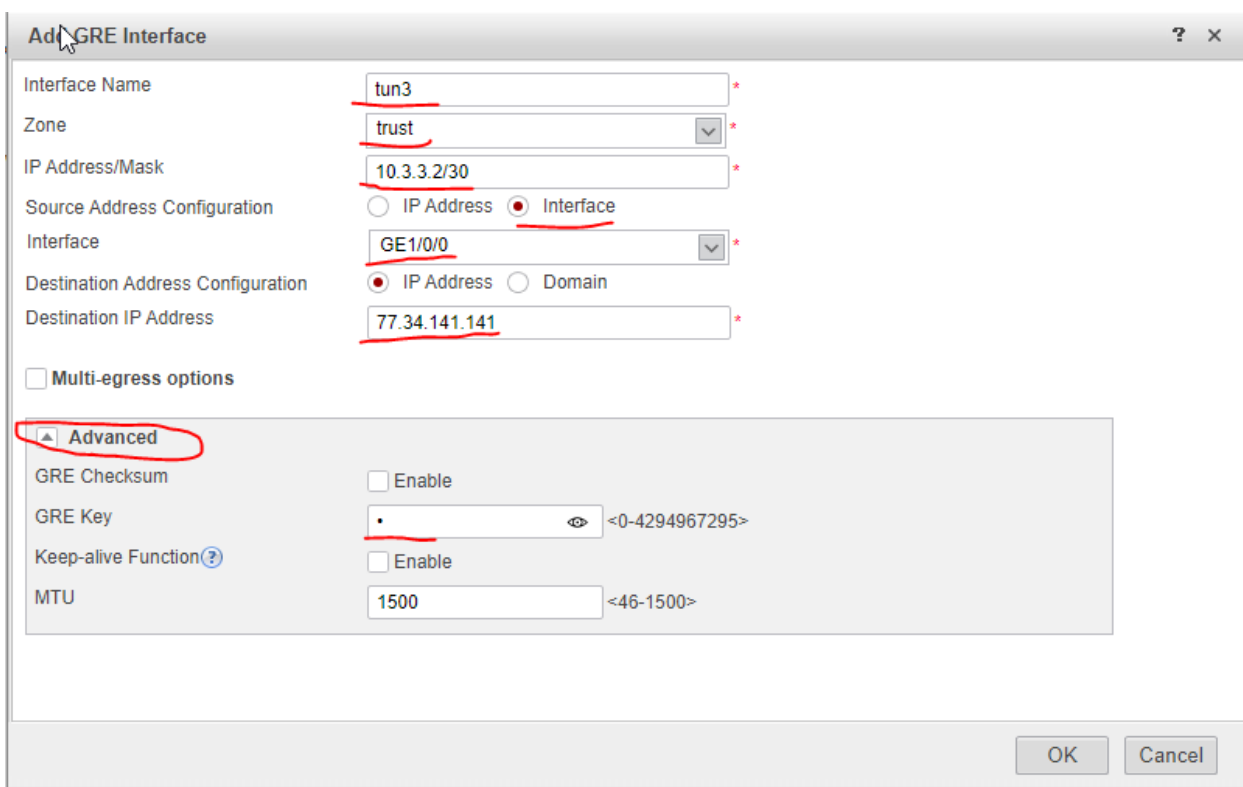
Tun dest 62.33.111.111

Tunnel key 3

USG:



Идем в Network – GRE – Add



Заполняем параметры туннеля, не забываем в advanced указать tunnel key

5. Настройте защиту GRE-туннеля с помощью IPsec.

i. Используйте IKEv2 с общим ключом.

ii. Используйте шифрование AES256, хеширование SHA256, группу DH15.

HQ2:

Crypto ikev2 proposal IPSEC2

Encryption aes-cbc-256

Integrity sha256

Group 15

Prf sha256

Crypto ikev2 policy IPSEC2

Proposal IPSEC2

Crypto ikev2 profile IPSEC2

Authentication local pre-share key cisco

Authentication remote pre-share key cisco

Match address local interface g0/1

Identity local address 77.34.141.141

Match identity remote any

Crypto ipsec transform-set IPSEC2 esp-aes256 esp-sha256-hmac

Mode tunnel

Crypto ipsec profile IPSEC2

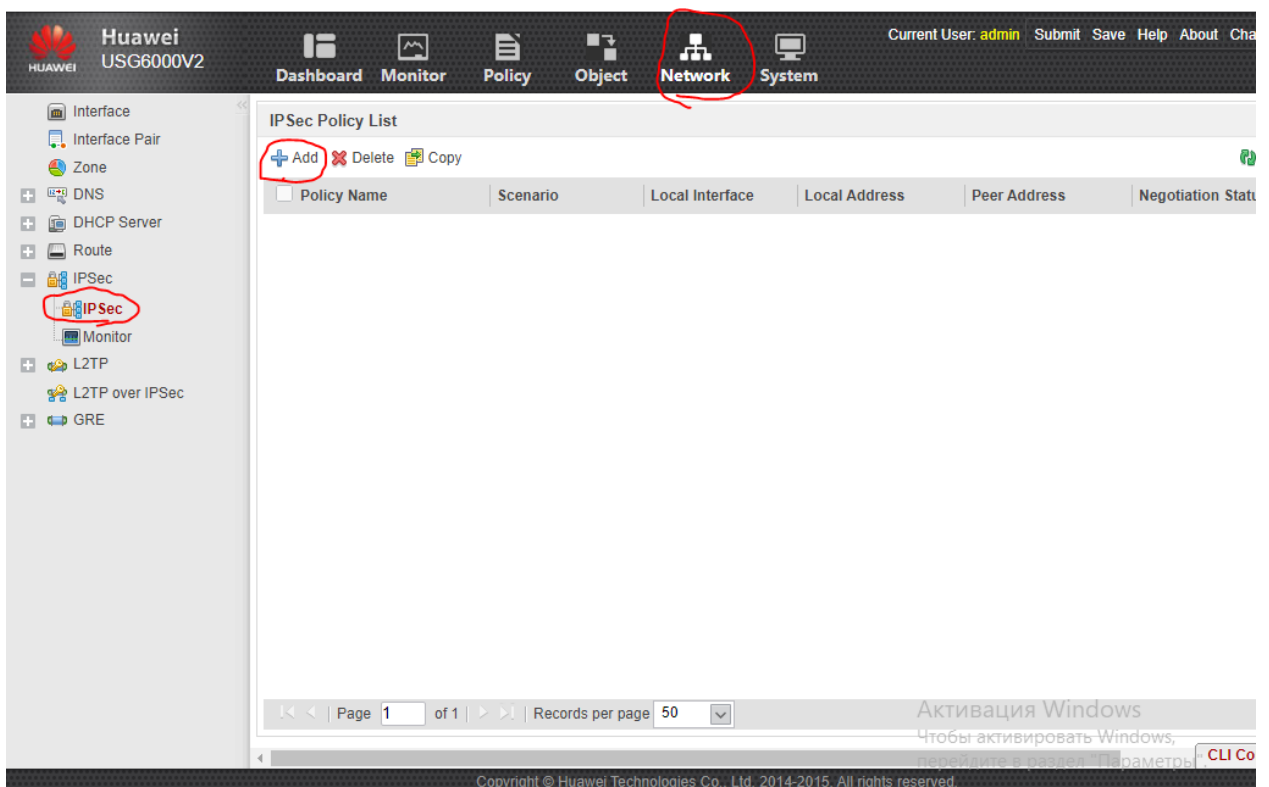
Set ikev2-profile IPSEC2

Set transform-set IPSEC2

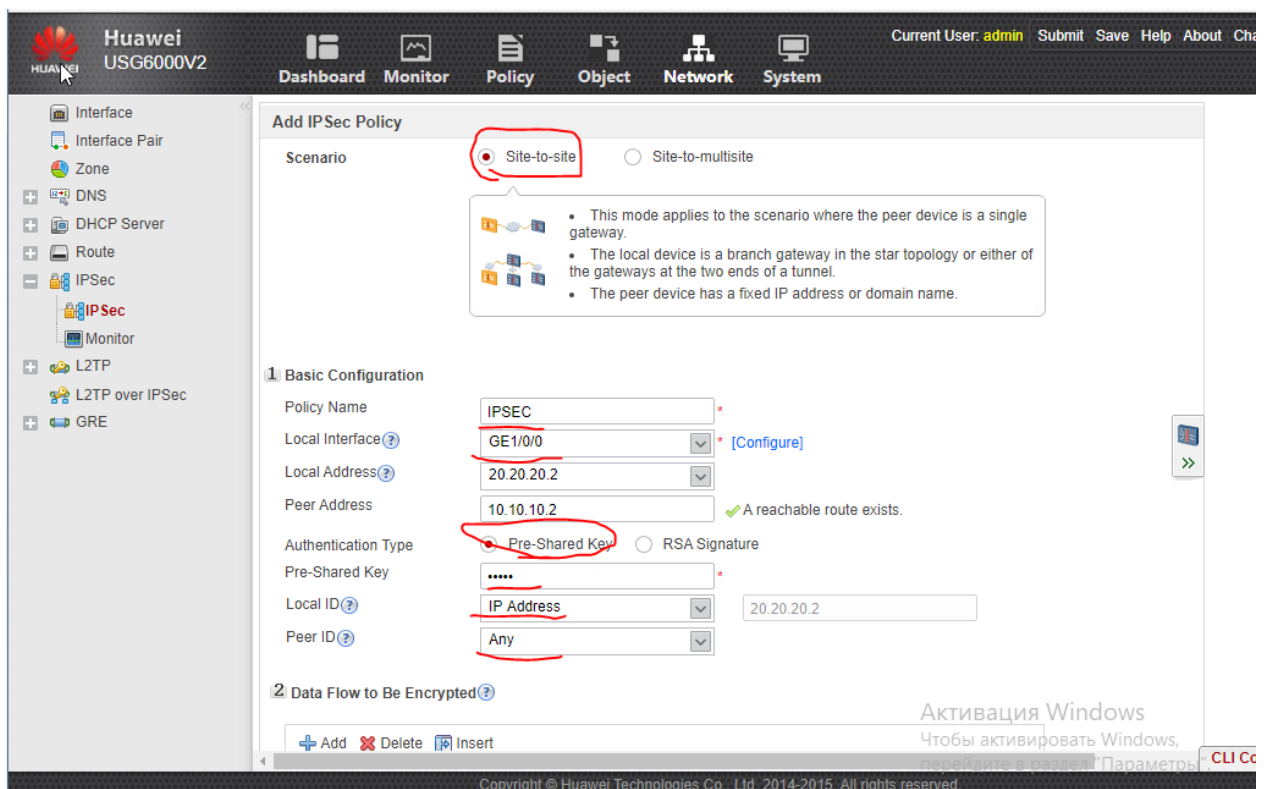
Int tun 3

Tunnel protection ipsec profile IPSEC2

USG:



Идем в network – IPSEC нажимаем add



Делаем как на картинке. Адреса очевидно по заданию. Ключ как на HQ2.

Huawei
USG6000V2

Current User: **admin** Submit Save Help About Ch...

Dashboard Monitor Policy Object Network System

Interface
Interface Pair
Zone
DNS
DHCP Server
Route
IPSec
IPSec
Monitor
L2TP
L2TP over IPSec
GRE

Policy Name: **IPSEC**

Local Interface: **GE 1/0/0** [Configure]

Local Address: **20.20.20.2**

Peer Address: **10.10.10.2** A reachable route exists.

Authentication Type: ☒ Pre-Shared Key ☐ RSA Signature

Pre-Shared Key: *********

Local ID: **IP Address** **20.20.20.2**

Peer ID: **Any**

2 Data Flow to Be Encrypted

+ Add - Delete Insert

ID	Source Address	Destination Address	Prot...	Source Port	Destination Port	Action	Edit
<input type="checkbox"/>	Implicit	any	any	any	any	Not Enc	

Displaying 1

3 IKE/IPSec Proposal

☒ Advanced

Apply Return

Активация Windows
Чтобы активировать Windows,
перейдите в раздел "Параметры".

Copyright © Huawei Technologies Co., Ltd. 2014-2015. All rights reserved.

Modify Data Flow to Be Encrypted

Define packets on which IPSec encryption is to be implemented. [Configuration Example]

Source Address: **20.20.20.2**

Destination Address: **10.10.10.2**

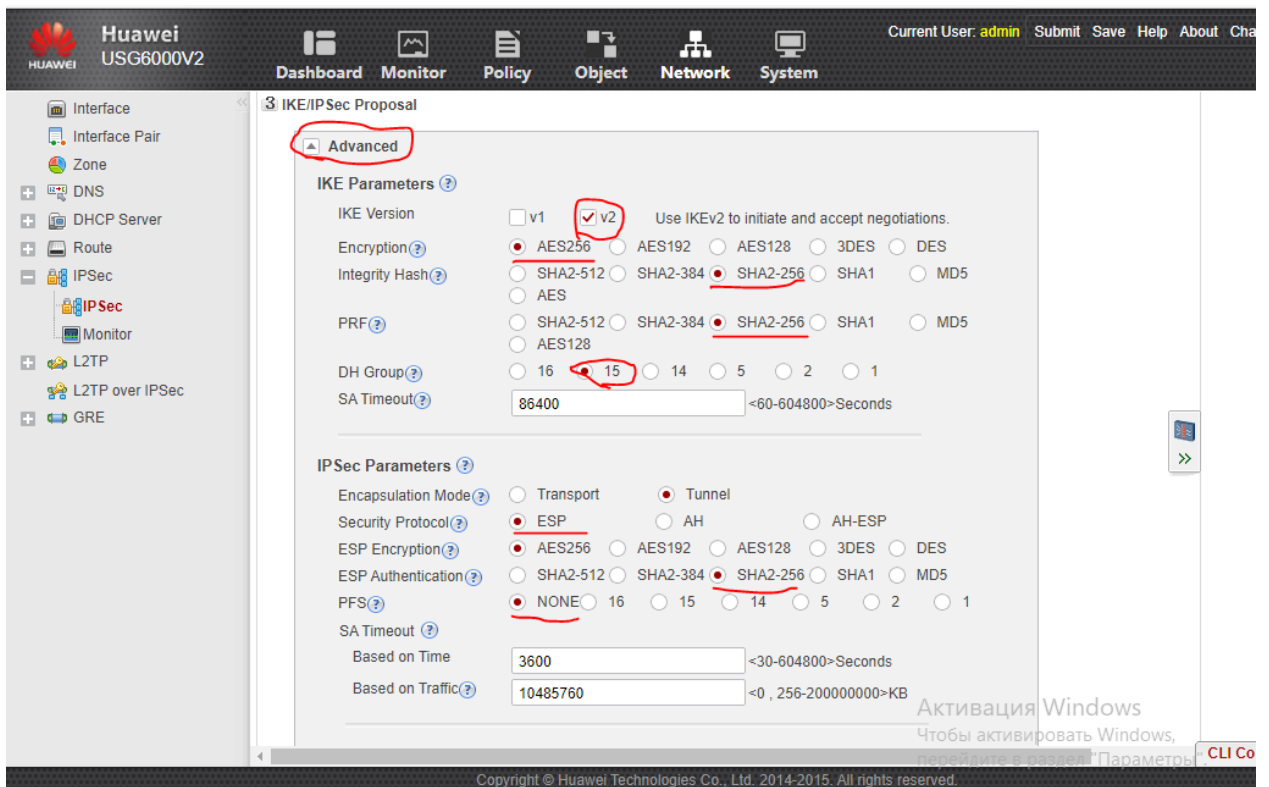
Protocol: **any**

Action: **Encrypt**

Enter a private IP address of the local device, for example, 192.168.1.1.
Enter an address range, for example, 192.168.1.0/24 or 192.168.1.0/255.255.255.0.

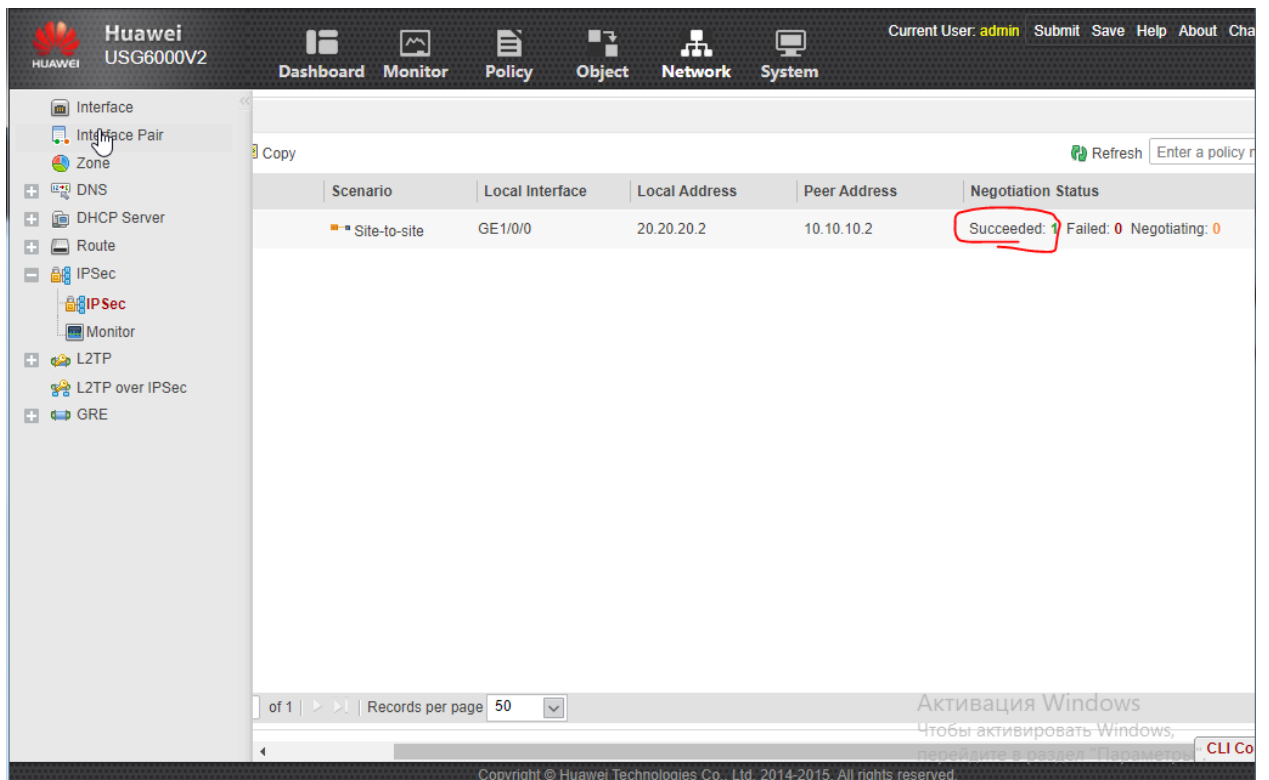
OK Cancel

Настраиваем адреса, которые необходимо шифровать. Адреса пиши внешние, по которым соседится туннель.



Открываем Advanced и настраиваем все как делали на роутере. Больше ничего делать не надо.

Пингуем туннель, на циске смотрим `sh crypto ikev2 sa`



На хвавец выглядит так

6. Настройте протокол динамической маршрутизации OSPF для обмена маршрутами между филиалом и центральным офисом.

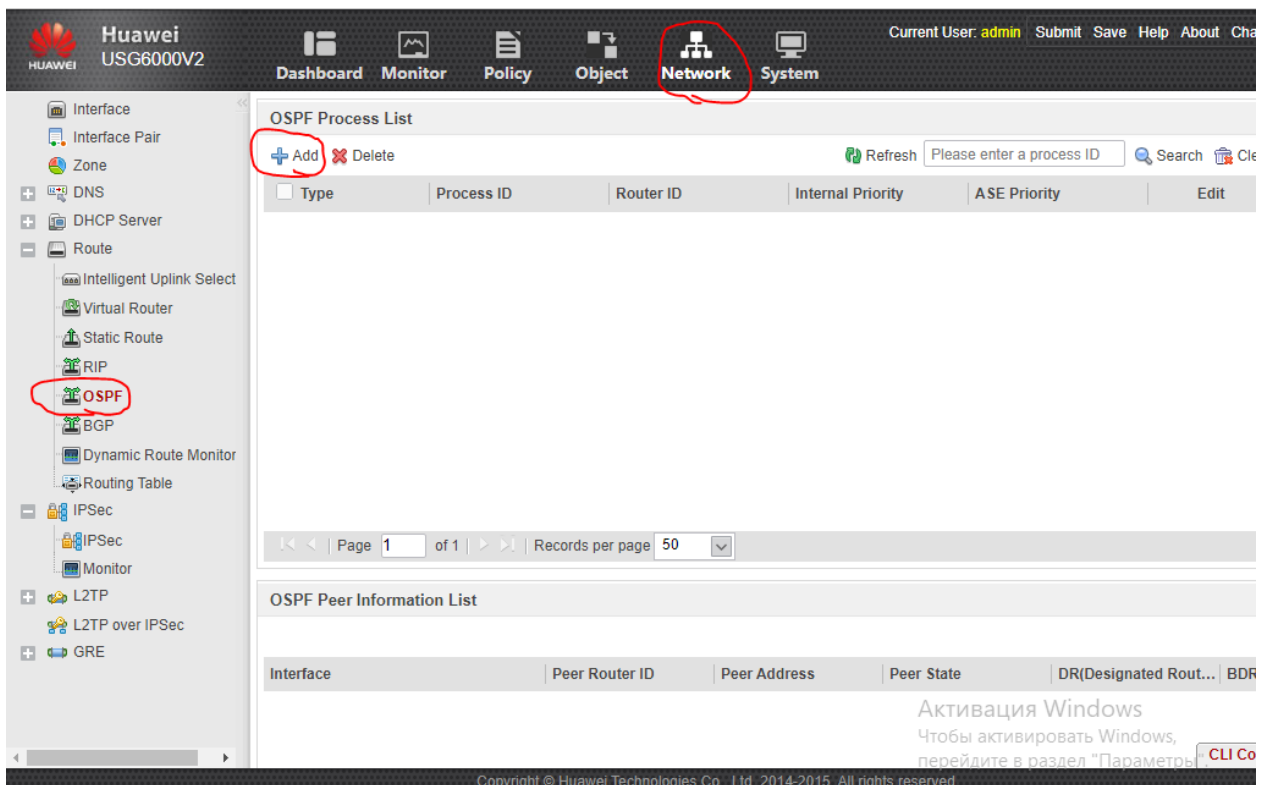
i. Используйте область 3.

ii. Объявите сеть филиала в OSPF.

HQ2:

Все уже должно быть настроено если ты делал DMVPN. Заанонси только сетку туннеля до хвавея в area 0.

USG:



Идем в network – OSPF и нажимаем add

Add OSPF Process

Type: ☒ OSPF v2 ☐ OSPF v3

Process ID: * <1-65535>

Router ID:

Virtual Router: ▼

SPF Calculation Interval: <1-10000>ms

Internal Priority: <1-255>

ASE Priority: <1-255>

BFD Function : ☐ Enable

Local Detection Multiple: <3-50>

Sending Interval: <100-1000>ms

Receiving Interval: <100-1000>ms

☐ Default Route

OK **Cancel**

Не меняй ничего, просто жми ОК

IV2 Dashboard Monitor Policy Object Network System Current User: admin Submit Save Help About Change Password Logout

OSPF Process List

+ Add - Delete Refresh Please enter a process ID Search Clear Search Condition

Type	Process ID	Router ID	Internal Priority	ASE Priority	Edit	Advanced Set...
OSPF v2	1	172.16.0.1	10	150		

Page 1 of 1 Records per page 50 Displaying 1 - 1 of 1

OSPF Peer Information List

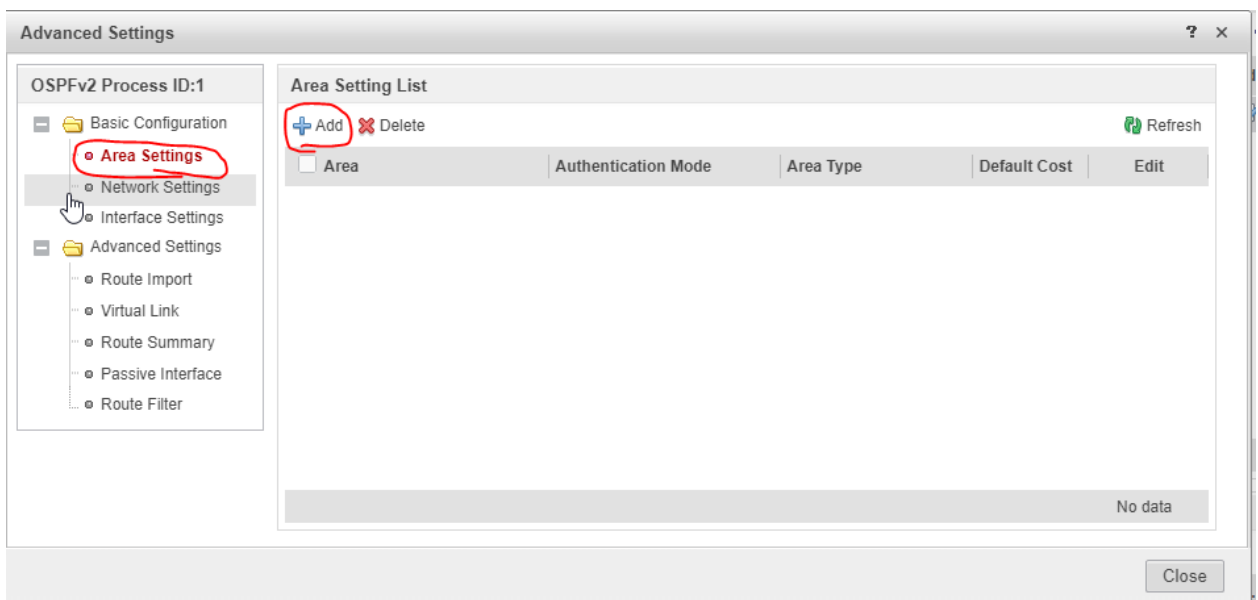
Refresh

Interface	Peer Router ID	Peer Address	Peer State	DR(Designated Rout...	BDR(Backup Design...
-----------	----------------	--------------	------------	-----------------------	----------------------

Активация Windows
Чтобы активировать Windows, перейдите в [настройки](#) или введите ключ активации.

Copyright © Huawei Technologies Co., Ltd. 2014-2015. All rights reserved.

Двигай полосу снизу чуть вправо и жми на Advanced settings



Тут жми ADD

Add Area

Area 0 *

IP Network 10.3.3.0 *

Mask/Wildcard Mask 255.255.255.252 *

Authentication Mode -- NONE --

Area Type -- NONE --

OK Cancel

Добавляй сетку туннеля в Area 0 и еще раз жми add

Add Area

Area 3 *

IP Network 172.16.0.0 *

Mask/Wildcard Mask 255.255.255.0 *

Authentication Mode -- NONE --

Area Type -- NONE --

OK Cancel

Добавляем сетку за хвавец в area 3

