Оглавление

[Базовая конфигурация 3](#_Toc529259577)

[Общая (кроме FW1): 3](#_Toc529259578)

[Дополнительно на HQ1: 3](#_Toc529259579)

[На FW1: 3](#_Toc529259580)

[Пункт 6 – Интерфейсы (часть настроек интерфейсов в др. секциях): 4](#_Toc529259581)

[SW1-3 (после настройки VTP): 4](#_Toc529259582)

[HQ1: 4](#_Toc529259583)

[FW1: 4](#_Toc529259584)

[BR1: 5](#_Toc529259585)

[Настройка коммутации 6](#_Toc529259586)

[1: VTP-сервер SW1 : 6](#_Toc529259587)

[1: VTP клиенты: 6](#_Toc529259588)

[3: EtherChannel: 6](#_Toc529259589)

[2: Транки: 7](#_Toc529259590)

[4: Spanning-tree: 7](#_Toc529259591)

[5: Настройка портов: 8](#_Toc529259592)

[6: Отключение CDP на маршрутизаторах HQ1 и BR1: 8](#_Toc529259593)

[Настройка подключений к глобальным сетям 9](#_Toc529259594)

[1: PPPoE между ISP1 и BR1: 9](#_Toc529259595)

[2: Multilink PPP между HQ1 и ISP1: 9](#_Toc529259596)

[3: IPoE на FW1: сделана в базовых настройках, 6: интерфейсы 9](#_Toc529259597)

[Настройка маршрутизации 10](#_Toc529259598)

[3: EIGRP на BR1: 10](#_Toc529259599)

[4: BGB HQ1: 10](#_Toc529259600)

[4: BGB FW1: 10](#_Toc529259601)

[1 и 2: OSPF HQ1 (после настройки ip GRE туннеля, хотя бы без защиты туннеля): 11](#_Toc529259602)

[1: OSPF FW1: 11](#_Toc529259603)

[2: OSPF BR1 (после настройки ip GRE туннеля, хотя бы без защиты туннеля): 11](#_Toc529259604)

[5: OSPFv3 HQ1 и BR1 (после настройки ipv6 GRE туннеля, хотя бы без защиты туннеля): 11](#_Toc529259605)

[Настройка служб 12](#_Toc529259606)

[1: Cервер времени HQ1: 12](#_Toc529259607)

[1: Cервер времени HQ1 + клиенты NTP: 12](#_Toc529259608)

[2: BR1 PAT: 12](#_Toc529259609)

[3: DHCP на HQ1: !! нужно проверить !! 12](#_Toc529259610)

[Настройка механизмов безопасности 13](#_Toc529259611)

[1: Пользователи на HQ1: 13](#_Toc529259612)

[2: Port Security на SW3: 13](#_Toc529259613)

[3: DHCP Snooping на SW3: 14](#_Toc529259614)

[4: ARP inspection на SW3: 14](#_Toc529259615)

[Настройка параметров мониторинга и резервного копирования 15](#_Toc529259616)

[1: Журналирование HQ1 и FW1: 15](#_Toc529259617)

[2: SNMPv3 на HQ1 и FW1: 15](#_Toc529259618)

[3: Резервное копирование на HQ1: 15](#_Toc529259619)

[Конфигурация виртуальных частных сетей 16](#_Toc529259620)

[1: DMVPN на HQ1 и BR1: 16](#_Toc529259621)

[2: DMVPN protection на HQ1 и BR1: 16](#_Toc529259622)

[3: AnyConnect SSL на FW1: 16](#_Toc529259623)

# Базовая конфигурация

## Общая (кроме FW1):

(config)# hostname <host>

(config)# ip domain-name wsr2018.ru

(config)# username wsr2018 privilege 15 secret cisco

(config)# enable password wsr

(config)# service password-encryption

(config)# crypto key generate rsa modulus 1024

(config)# ip ssh version 2

(config)# aaa new-model

(config)# aaa authentication login default local

(config)# aaa authorization exec default local

(config)# aaa authorization console

(config-line)# line vty 0 15

(config-line)# transport input ssh telnet

## Дополнительно на HQ1:

HQ1(config)# radius-server host 172.16.20.2 auth-port 1812 acc-port 1813 key cisco

HQ1(config)# aaa authentication login method\_man group radius local

HQ1(config)# aaa authorization exec method\_man if-authenticated

HQ1(config)# line vty 0 4

HQ1(config)# login authentication method\_man

HQ1(config)# authorization exec method\_man

## На FW1:

FW1(config)# hostname FW1

FW1(config)# domain-name wsr2018.ru

FW1(config)# username wsr2018 password cisco privilege 15

FW1(config)# enable password wsr #!!хеширует пароль!!а не надо!

FW1(config)# password encryption aes

FW1(config)# crypto key generate rsa modulus 1024 # Необязательно

FW1(config)# ip ssh version 2

FW1(config)# aaa authentication serial console LOCAL

FW1(config)# aaa authentication ssh LOCAL

FW1(config)# aaa authentication http console LOCAL

FW1(config)# aaa authorization http console LOCAL

FW1(config)# aaa authorization exec LOCAL auto-enable

## Пункт 6 – Интерфейсы (часть настроек интерфейсов в др. секциях):

### SW1-3 (после настройки VTP):

SW(config)# interface vlan 100

SW(config-if)# ip address 172.16.10.<11-13> 255.255.255.0

SW(config-if)# no shutdown

### HQ1:

HQ1(config)# ipv6 unicast-routing

HQ1(config)# ipv6 multicast-routing

HQ1(config)# interface GigabitEthernet 0/0/1.100

HQ1(config-if)# encapsulation dot1Q 100

HQ1(config-if)# ip address 172.16.10.1 255.255.255.0

HQ1(config-if)# interface GigabitEthernet 0/0/1.200

HQ1(config-if)# encapsulation dot1Q 200

HQ1(config-if)# ip address 172.16.20.1 255.255.255.252

HQ1(config-if)# interface GigabitEthernet 0/0/1.300

HQ1(config-if)# encapsulation dot1Q 300

HQ1(config-if)# ip address 30.30.30.1 255.255.255.0

HQ1(config-if)# interface GigabitEthernet 0/0/0

HQ1(config-if)# ip address 172.16.0.13 255.255.255.252

HQ1(config-if)# no shutdown

HQ1(config-if)# interface Loopback 0

HQ1(config-if)# ip address 1.1.1.1 255.255.255.255

HQ1(config-if)# ipv6 address 2001:A:B:1::1/64

### FW1:

FW1(config)# interface GigabitEthernet 1/3

FW1(config-if)# ip address 30.30.30.2 255.255.255.0

FW1(config-if)# nameif OFFICE

FW1(config-if)# security-level 100

FW1(config-if)# no shutdown

FW1(config-if)# interface GigabitEthernet 1/2

FW1(config-if)# ip address 172.16.0.14 255.255.255.252

FW1(config-if)# nameif HQ1

FW1(config-if)# security-level 100

FW1(config-if)# no shutdown

FW1(config-if)# interface GigabitEthernet 1/1

FW1(config-if)# ip address 40.15.5.2 255.255.255.252

FW1(config-if)# nameif ISP

FW1(config-if)# no shutdown

### BR1:

HQ1(config)# ipv6 unicast-routing

HQ1(config)# ipv6 multicast-routing

BR1(config)# interface Loopback 0

BR1(config-if)# ip address 11.11.11.11 255.255.255.255

BR1(config-if)# ipv6 address 2001:A:B:11::1/64

# Настройка коммутации

## 1: VTP-сервер SW1 :

SW1(config)# vtp domain wsr2018.ru

SW1(config)# vtp password VTPPass

SW1(config)# vtp mode server vlan # Необязательно

SW1(config)# vtp version 3

SW1# vtp primary vlan force

SW1(config)# vlan 100

SW1(config-vlan)# name MGT

SW1(config-vlan)# vlan 200

SW1(config-vlan)# name DATA

SW1(config-vlan)# vlan 300

SW1(config-vlan)# name OFFICE

SW1(config-vlan)# vlan 400

## 1: VTP клиенты:

SW(config)# vtp domain wsr2018.ru

SW(config)# vtp password VTPPass

SW(config)# vtp mode client

SW(config)# vtp version 3

## 3: EtherChannel:

SW1(config)# interface range FastEthernet 0/1-3

SW1(config-if-range)# channel-group 1 mode active

SW2(config)# interface range FastEthernet 0/1-3

SW2(config-if-range)# channel-group 1 mode passive

SW2(config)# interface range FastEthernet 0/6-7

SW2(config-if-range)# channel-group 2 mode desirable

SW3(config)# interface range FastEthernet 0/6-7

SW3(config-if-range)# channel-group 2 mode auto

## 2: Режимы портов:

SW1(config)# interface FastEthernet 0/5

SW1(config-if)# switchport mode dynamic desirable

SW1(config-if)# interface Port-channel 1

SW1(config-if)# switchport mode dynamic desirable

SW1(config-if)# interface FastEthernet 0/10

SW1(config-if)# switchport mode access

SW1(config-if)# interface FastEthernet 0/24

SW1(config-if)# switchport mode tunk

SW2(config)# interface Port-channel 2

SW2(config-if)# switchport mode trunk

SW2(config-if)# interface FastEthernet 0/24

SW2(config-if)# switchport mode access

SW3(config)# interface Port-channel 2

SW3(config-if)# switchport mode trunk

SW3(config-if)# interface FastEthernet 0/10

SW3(config-if)# switchport mode access

## 4: Spanning-tree:

SW1(config)# spanning-tree mode rapid-pvst

SW1(config)# spanning-tree vlan 100,200,300 root primary

SW1(config)# interface FastEthernet 0/5

SW1(config-if)# spanning-tree guard root

SW2(config)# spanning-tree mode rapid-pvst

SW2(config)# spanning-tree vlan 100,200,300 root secondary

SW2(config-if)# interface Port-channel 2

SW2(config-if)# spanning-tree guard root

SW2(config-if)# interface FastEthernet 0/10

SW2(config-if)# spanning-tree portfast

SW2(config-if)# spanning-tree bpduguard enable

SW3(config)# spanning-tree mode rapid-pvst

## 5: Настройка портов:

SW1(config)# interface FastEthernet 0/10

SW1(config-if)# switchport access vlan 200

SW3(config)# interface FastEthernet 0/24

SW3(config-if)# switchport access vlan 300

SW1(config)# interface FastEthernet 0/10

SW1(config-if)# switchport access vlan 300

## 6: Отключение CDP на маршрутизаторах HQ1 и BR1:

HQ1(config)# interface Serial 0/1/0

HQ1(config)# no cdp enable

HQ1(config)# interface Serial 0/1/1

HQ1(config)# no cdp enable

BR1(config)# interface GigabitEthernet 0/0/0

BR1(config)# no cdp enable

# Настройка подключений к глобальным сетям

## 1: PPPoE между ISP1 и BR1:

BR1(config)# ip route 0.0.0.0 0.0.0.0 Dialer 0

BR1(config)# interface Dialer 0

BR1(config-if)# encapsulation ppp

BR1(config-if)# ip address negotiated

BR1(config-if)# ppp authentication chap callin

BR1(config-if)# ppp chap hostname cisco

BR1(config-if)# ppp chap password cisco

BR1(config-if)# dialer pool 1

BR1(config-if)# interface GigabitEthernet 0/0/0

BR1(config-if)# pppoe enable group global

BR1(config-if)# pppoe-client dial-pool-number 1

BR1(config-if)# no shutdown

## 2: Multilink PPP между HQ1 и ISP1:

HQ1(config)# interface Multilink 1

HQ1(config-if)# ip address negotiated

HQ1(config-if)# interface Serial 0/1/0

HQ1(config-if)# encapsulation ppp

HQ1(config-if)# ppp multilink group 1

HQ1(config-if)# no shutdown

HQ1(config-if)# interface Serial 0/1/1

HQ1(config-if)# encapsulation ppp

HQ1(config-if)# ppp multilink group 1

HQ1(config-if)# no shutdown

## 3: IPoE на FW1: сделана в базовых настройках, 6: интерфейсы

# Настройка маршрутизации

## 3: EIGRP на BR1:

BR1(config)# router eigrp 2018

BR1(config-router)# network 11.11.11.11 0.0.0.0

BR1(config-router)# network 33.33.33.0 0.0.0.3

BR1(config-router)# no auto-summary

BR1(config)# key chain EIGRP

BR1(config-keychain)# key 2

BR1(config-keychain-key)# key-string WSR

BR1(config)# interface Dialer 0

BR1(config-if)#ip authentication mode eigrp 2018 md5

BR1(config-if)#ip authentication key-chain eigrp 2018 EIGRP

## 4: BGB HQ1:

HQ1(config)# router bgp 65000

HQ1(config-router)# neighbor 40.15.7.1 remote-as 65001

HQ1(config-router)# neighbor 172.16.0.14 remote-as 65000  
 HQ1(config-router)# network 1.1.1.1 mask 255.255.255.255

HQ1(config-router)# network 30.30.30.0 mask 255.255.255.0

HQ1(config-router)# network 40.15.7.0 mask 255.255.255.252

## 4: BGB FW1:

FW1(config)# router bgp 65000

FW1(config-router)# address-family ipv4

FW1(config-router-af)# neighbor 40.15.7.1 remote-as 65001

FW1(config-router-af)# neighbor 172.16.0.13 remote-as 65000

FW1(config-router-af)# network 30.30.30.0 mask 255.255.255.0

FW1(config-router-af)# network 40.15.5.0 mask 255.255.255.252

## 1 и 2: OSPF HQ1 (после настройки ip GRE туннеля, хотя бы без защиты туннеля):

HQ1(config)# router ospf 1

HQ1(config-router)# network 172.16.0.12 0.0.0.3 area 51

HQ1(config-router)# network 172.16.10.0 0.0.0.255 area 51

HQ1(config-router)# network 172.16.20.0 0.0.0.3 area 51

HQ1(config-router)# network 5.5.5.0 0.0.0.255 area 0

HQ1(config-router)# passive-interface default

HQ1(config-router)# no passive-interface Tunnel 1

HQ1(config-router)# no passive-interface GigabitEthernet 0/0/0

## 1: OSPF FW1:

FW1(config)# router ospf 1

FW1(config-router)# network 172.16.0.12 255.255.255.252 area 51

!# невозможно объявить пассивные интерфейсы на ASA!

## 2: OSPF BR1 (после настройки ip GRE туннеля, хотя бы без защиты туннеля):

HQ1(config)# router ospf 1

HQ1(config-router)# network 192.168.1.0 0.0.0.255 area 1

HQ1(config-router)# network 5.5.5.0 0.0.0.255 area 0

HQ1(config-router)# passive-interface default

HQ1(config-router)# no passive-interface Tunnel 1

## 5: OSPFv3 HQ1 и BR1 (после настройки ipv6 GRE туннеля, хотя бы без защиты туннеля):

(config)# ipv6 router ospf 1

(config-rtr)# interface Loopback 0

(config-if)# ipv6 ospf 1 area 0

(config-if)# interface GigabitEthernet 0/0/1

(config-if)# ipv6 ospf 1 area 0

(config-if)# interface Tunnel 1

(config-if)# ipv6 ospf 1 area 0

(config-if)# ipv6 ospf authentication ipsec spi 555 md5 ->

-> 11111111111111111111111111111111

!# **spi 555** это 32 бит код, индетификатор, индекс параметров защиты

!# **md5 11...11** (32 hex-цифры, 0-f) это ключ. Все это может быть

!# любым набором цифр, главное, чтобы они совпадали на обеих

!# маршрутизаторах

!# Либо в настройках самого OSPFv3:

(config)# ipv6 router ospf 1

(config-rtr)# area 0 authentication ipsec spi 555 md5 <numbers>

# Дополнительно на BR1

(config-if)# interface GigabitEthernet 0/0/1

(config-if)# ipv6 ospf 1 area 0

Примечание к динамическим маршрутам: не будут появляться маршруты OSPFv2 и OSPFv3 с BR1 интерфейса на PC2, если интерфейс не активен!

# Настройка служб

## 1: Cервер времени HQ1:

HQ1(config)# ntp server 172.16.20.2

HQ1(config)# ntp update-calendar

HQ1(config)# ntp master 2

## 1: Cервер времени HQ1 + клиенты NTP:

(config)# clock timezone MSK 3

(config)# ntp authenticate

(config)# ntp authentication-key 1 md5 WSR

(config)# ntp trusted-key 1

!# только клиенты NTP:

(config)# ntp server 172.16.10.1 key 1

## 2: BR1 PAT:

BR1(config)# access-list 1 permit 192.168.1.0 /24

BR1(config)# ip nat inside source list 1 interface Loopback 0

BR1(config)# interface GigabitEthernet 0/0/0

BR1(config)# ip nat inside

BR1(config)# interface Dialer 0

BR1(config)# ip nat outside

## 3: DHCP на HQ1:

HQ1(config)# ip dhcp excluded-address 30.30.30.1 30.30.30.10

HQ1(config)# ip dhcp pool OFFICE

HQ1(dhcp-config)# network 30.30.30.0 /24

HQ1(dhcp-config)# default-router 30.30.30.1

HQ1(dhcp-config)# option 150 ip 172.16.20.2 !# TFTP сервер

HQ1(config)# ip dhcp pool PC1

HQ1(dhcp-config)# host 30.30.30.30

HQ1(dhcp-config)# client-identifier 01<MAC-адрес интерфейса PC1>

# Настройка механизмов безопасности

## 1: Пользователи на HQ1:

BR1# enable view

BR1(config)# username user1 privilege 5 password cisco

BR1(config)# privilege exec all level 5 debug

BR1(config)# privilege exec level 5 reload

BR1(config)# parser view sh\_view

BR1(config-view)# secret cisco

BR1(config-view)# commands exec include show cdp neighbor

BR1(config-view)# commands exec include all show ip

BR1(config-view)# commands exec include who

BR1(config-view)# parser view ping\_view

BR1(config-view)# secret cisco

BR1(config-view)# commands exec include all ping

BR1(config-view)# commands exec include all traceroute

BR1(config-view)# parser view wan\_view

BR1(config-view)# secret cisco

BR1(config-view)# commands exec include configure

BR1(config-view)# commands exec include configure terminal

BR1(config-view)# commands configure include interface Dialer 0

BR1(config-view)# commands interface include all encapsulation

BR1(config-view)# commands interface include all ppp authentication

BR1(config-view)# commands interface include all ip address

BR1(config-view)# commands interface include all shutdown

BR1(config-view)# commands interface include no

BR1(config-view)# parser view super superview

BR1(config-view)# secret cisco

BR1(config-view)# view sh\_view

BR1(config-view)# view ping\_view

BR1(config-view)# view wan\_view

BR1(config)# username user2 view super password cisco

## 2: Port Security на SW3:

SW3(config)# interface FastEthernet 0/10

SW3(config-if)# switchport port-security maximum 2

SW3(config-if)# switchport port-security violation restrict

SW3(config-if)# switchport port-security

## 3: DHCP Snooping на SW3:

SW3(config)# ip dhcp snooping database flash:/DHCPSnoop.DB

SW3(config)# ip dhcp snooping vlan 300

## 4: ARP inspection на SW3:

SW3(config)# ip arp inspection vlan 300

SW3(config)# interface FastEthernet 0/11

SW3(config-if)# ip arp inspection trust

# Настройка параметров мониторинга и резервного копирования

## 1: Журналирование HQ1 и FW1:

(config)# logging on

(config)# logging trap informational

!# на HQ1

HQ1(config)#logging host 172.16.20.2

!# на FW1

FW1(config)# logging host HQ1 172.16.20.2

## 2: SNMPv3 на HQ1 и FW1:

(config)# snmp-server contact admin@wsr.ru

(config)# snmp-server location MSK, Russia

!# на HQ1

HQ1(config)# snmp-server view RO 1 included

HQ1(config)# snmp-server group WSR v3 priv read RO

HQ1(config)# snmp-server user snmpuser WSR v3 auth sha snmppass priv aes 128 snmppass

HQ1(config)# snmp-server host 172.16.20.2 version 3 priv snmpuser # Необязательно

!# на FW1

FW1(config)# snmp-server enable # Необязательно

FW1(config)# snmp-server group WSR v3 priv

FW1(config)# snmp-server user snmpuser WSR v3 engineID .1 auth sha snmppass priv aes 128 snmppass

FW1(config)# snmp-server host HQ1 172.16.20.2 version 3 snmpuser

## 3: Резервное копирование на HQ1:

HQ1(config)# archive

HQ1(config-archive)# path tftp://172.16.20.2/<$H><$T>.cfg

HQ1(config-archive)# write-memory

# Конфигурация виртуальных частных сетей

## 1: DMVPN на HQ1 и BR1:

#!HQ1 + BR1:

(config)# int Tunnel 1

(config-if)# tunnel source Loopback 0

(config-if)# tunnel mode gre multipoint

(config-if)# ip address 5.5.5.<1-2> 255.255.255.0

(config-if)# ip mtu 1416

(config-if)# ip nhrp network-id 1

(config-if)# ipv6 address 2001::<1-2>/64

(config-if)# ipv6 mtu 1416

(config-if)# ipv6 nhrp network-id 1

#!HQ1 (HUB)

HQ1(config-if)# ip nhrp map multicast dynamic

HQ1(config-if)# ipv6 nhrp map multicast dynamic

#!BR1 (spoke) !! это работает, но не уверен, что это так нужно настроить !!

BR1(config-if)# ip nhrp nhs 5.5.5.1

BR1(config-if)# ip nhrp map 5.5.5.1 1.1.1.1

BR1(config-if)# ip nhrp map multicast 1.1.1.1

BR1(config-if)# ipv6 nhrp nhs 2001::1

BR1(config-if)# ipv6 nhrp map 2001::1/64 1.1.1.1

BR1(config-if)# ipv6 nhrp map multicast 1.1.1.1

## 2: DMVPN protection на HQ1 и BR1:

(config)# crypto isakmp policy 10

(config-isakmp)# hash sha384

(config-isakmp)# encryption aes 192

(config-isakmp)# group 14

(config-isakmp)# authentication pre-share

(config)# crypto isakmp key wsr address 0.0.0.0 0.0.0.0

(config)# crypto ipsec transform-set TS esp-aes 192 esp-md5-hmac

(cfg-crypto-trans)# mode transport

(config)# crypto ipsec profile VPN

(ipsec-profile)# set transform-set TS

(config)# interface Tunnel 1

(config-if)# tunnel protection ipsec profile VPN

## 3: AnyConnect SSL на FW1:

!# Для настройки AnyConnect через ASDM необходимо включить HTTP сервер:

FW1(config)# http server enable

FW1(config)# http 0 0 OFFICE

FW1(config)# http redirect OFFICE !# для удобства

FW1(config)# asdm image flash:/asdm-792-152.bin !# если не указан образ

!# Далее через ASDM в Wisard’ах выбираем AnyConnect Wisard -> Next -> Снимаем галку с IPSec, создаем новый сертификат ... и далее по ситуации ))

!# Также делаем статический маршрут на HQ1 для сети 10.0.0.0/24 в сторону FW1