Основные настройки

|  |  |
| --- | --- |
| Router(config)# | line con 0 |
| Router(config-line)# | logging synchronous |
| Router(config-line)# | exec-timeout 0 0 |
| Router(config-line)# | exit |
| Router(config)# | no ip domain lookup |
| Router(config)# | hostname |

Loopback interface

|  |  |
| --- | --- |
| Router(config)# | int lo0 |
| Router(config-if)# | ip add 50.0.1.1 255.255.255.0 |
| Router(config-if)# | no shutdown |

VLANs access - trunk

|  |  |
| --- | --- |
| AccSW(config-if)# | switch mode access |
| AccSW(config-if)# | switch access vlan (№) |
| AccSW(config-if)# | switch trunk encapsulation dot1q |
| AccSW(config-if)# | switch mode trunk |

Port-channel

|  |  |
| --- | --- |
| DistSW(config)# | int ra fa 1/4 – 1/5 |
| DistSW(config-if-range)# | switch trunk enc dot1q |
| DistSW(config-if-range)# | switch mode trunk |
| DistSW(config-if-range)# | channel-group 1 mode on |
| DistSW(config)# | port-channel load-balance src-dst-mac |

show etherchannel summary

Spanning-tree

|  |  |
| --- | --- |
| DistSW(config)# | spanning-tree vlan 2 root primary |
| DistSW(config)# | spanning-tree vlan 3 root secondary |

show spanning-tree brief

OSPF

|  |  |
| --- | --- |
| Router(config)# | router ospf 1 |
| Router(config-router)# | router-id 1.1.1.1 |
| Router(config-router)# | network 10.0.1.0 0.0.0.255 area 0 |
| Router(config-router)# | area 1 range 192.168.0.0 255.255.0.0 |

SSH

|  |  |
| --- | --- |
| Router(config)# | ip domain-name geteway |
| Router(config)# | hostname gateway |
| Router(config)# | crypto key generate rsa |
| Router(config)# | service password-encryption |
| Router(config)# | username (user) privilege 15 secret (password) |
| Router(config)# | aaa new-model |
| Router(config)# | aaa authorization exec default local |
| Router(config)# | line vty 0 4 |
| Router(config-line)# | transport input ssh |
| Router(config-line)# | logging synchronous |
| Router(config-line)# | exec-timeout 60 0 |

DHCP

|  |  |
| --- | --- |
| Router(config)# | ip dhcp pool VLAN2POOL |
| Router(dhcp-config)# | network 192.168.2.0 255.255.255.0 |
| Router(dhcp-config)# | default-router 192.168.2.1 |
| Router(dhcp-config)# | dns-server 192.168.0.50 |
| Router(config)# | ip dhcp excluded-address 192.168.2.1 |
| DistSW(config-if)# | ip helper-address 60.0.1.1 |

HSRP

**Настройка HSRP root заходим в vlan:**

|  |  |
| --- | --- |
| Router(config)# | int vlan (№ vlan) |
| Router(config-if)# | standby (№ vlan) ip 123.10.10.1 |
| Router(config-if)# | standby (№ vlan) priority 110 |
| Router(config-if)# | standby (№ vlan) preempt |
| Router(config-if)# | ip add 123.10.10.50 255.255.255.0 |
| Router(config-if)# | exit |
| Router(config)# | spanning-tree vlan 20 root primary |

**Настройка HSRP secondary заходим в vlan:**

|  |  |
| --- | --- |
| Router(config)# | int vlan (№ vlan) |
| Router(config-if)# | standby (№ vlan) ip 123.10.10.1 |
| Router(config-if)# | standby (№ vlan) preempt |
| Router(config-if)# | ip add 123.10.10.51 255.255.255.0 |
| Router(config-if)# | exit |
| Router(config)# | spanning-tree vlan 20 root secondary |

**Осмотреть hsrp:** show standby brief

GLBP

**Настройка GLBP балансировки трафика**

|  |  |
| --- | --- |
| Router(config)# | int vlan (№ vlan) |
| Router(config-in)# | glbp (№ vlan) ip (vIP) |
| Router(config-in)# | glbp (№ vlan) priority 110 |
| Router(config)# | glbp (№ vlan) preempt |
| Router(config-in)# | ip add 123.10.10.50 255.255.255.0 |

**Осмотреть hsrp:** show glbp brief

BVI

**Настройка HSRP root заходим в vlan:**

|  |  |
| --- | --- |
| Router(config)# | interface ra g0/1-2 |
| Router(config-if)# | bridge-group 1 |
| Router(config)# | bridge irb |
| Router(config)# | bridge 1 protocol ieee |
| Router(config)# | bridge 1 priority 0 |
| Router(config)# | bridge 1 route ip |
| Router(config-if)# | interface bvi 1 |
| Router(config-if)# | ip address 192.168.1.254 255.255.255.0 |

ACL extended

**Настройка ACL на оборудовании**

|  |  |
| --- | --- |
| Router(config)# | ip access-list extended 100 |
| Router(config-ext-nacl)# | permit ip any (subnet) |
| Router(config-ext-nacl)# | deny ip any (subnet) |
| Router(config)# | int vlan 10 |
| Router(config-in)# | ip access-group 100 in |

Самая простая конфигурация для настройки разрешения и запрета.

Но что делать если у нас множество подсетей, которые могут увеличиться?

Для этого мы будем использовать запрет на все адреса, которые не разрешены.

|  |  |
| --- | --- |
| Router(config)# | ip access-list extended 100 |
| Router(config-ext-nacl)# | permit ip any (subnet) |
| Router(config-ext-nacl)# | deny ip any any |
| Router(config)# | int vlan 10 |
| Router(config-in)# | ip access-group 100 in |

Если нам необходимо разрешить выходить нашей подсети до определенного ip адреса или определенного порта, для этого мы можем использовать отдельную команду.

|  |  |
| --- | --- |
| Router(config)# | ip access-list extended 100 |
| Router(config-ext-nacl)# | permit ip any (subnet) |
| Router(config-ext-nacl)# | permit ip any host 10.10.10.1 |
| Router(config-ext-nacl)# | permit tcp any host 10.10.10.2 eq 22 |
| Router(config-ext-nacl)# | deny ip any any |
| Router(config)# | int vlan 10 |
| Router(config-in)# | ip access-group 100 in |

NAT

**Настройка интерфейсов входов выходов:**

**Интерфейс смотрящий в интернет:**

|  |  |
| --- | --- |
| Router(config)# | int fa 0/0 |
| Router(config-if)# | ip nat outside |

**Интерфейс смотрящий в локаль:**

|  |  |
| --- | --- |
| Router(config)# | int fa 1/0 |
| Router(config-if)# | ip nat inside |

**Создание access-list для завертывания трафика:**

|  |  |
| --- | --- |
| Router(config)# | access-list 7 permit 192.168.0.0 0.0.255.255 |

**Создание NAT:**

|  |  |
| --- | --- |
| Router(config)# | ip nat inside source list 7 interface fa0/0 overload |

**Команда что говорит, что у этого роутера есть выход в 8 нулей.**

|  |  |
| --- | --- |
| Router(config)# | router ospf 1 |
| Router(config-router)# | default-information originate metric 10 |

**Команда выкида пакетов наружу:**

|  |  |
| --- | --- |
| Router(config)# | ip route 0.0.0.0 0.0.0.0 218.56.23.1 |

ASA 5506 v9.6>

**Настройка ASA как border оборудование:**

|  |  |
| --- | --- |
| ASA(config)# | int Gi0/0 |
| ASA(config-if)# | nameif INTERNET |
| ASA(config-if)# | ip add 10.11.1.1 255.255.255.0 |
| ASA(config-if)# | no shutdown |
| ASA(config-if)# | int Gi0/1 |
| ASA(config-if)# | nameif LOCAL |
| ASA(config-if)# | security-level 100 |
| ASA(config-if)# | ip add 10.12.1.254 255.255.255.0 |
| ASA(config-if)# | no shutdown |
| ASA(config)# | route ospf 100 |
| ASA(config-router)# | network 10.12.1.254 255.255.255.0 area 0 |
| ASA(config-router)# | default-information originate |
| ASA(config)# | route INTERNET 0.0.0.0 0.0.0.0 (next-hope) |
| ASA(config)# | policy-map global\_policy |
| ASA(config-pmap)# | class inspection\_default |
| ASA(config-pmap-c)# | inspect icmp |
| ASA(config)# | object network VLANLOCAL |
| ASA(config-network-object)# | subnet 10.12.1.254 255.255.255.0 |
| ASA(config-network-object)# | nat (LOCAL,INTERNET) dynamic interface |
| ASA(config)# | access-list SPLIT-ACL extended permit ip 10.12.1.254 255.255.255.0 any |
| ASA(config)# | access-group SPLIT-ACL in interface LOCAL |

Event manager

**Перезагрузка интерфейсов vlan после загрузки оборудования:**

|  |  |
| --- | --- |
| Router(config)# | event manager applet SHUT\_SVI\_VLANS |
| Router(config-applet)# | event timer countdown time 100 |
| Router(config-applet)# | action 1.0 cli command "enable" |
| Router(config-applet)# | action 2.0 cli command "conf ter" |
| Router(config-applet)# | action 3.0 cli command "int vlan 20" |
| Router(config-applet)# | action 4.0 cli command "shutdown" |
| Router(config-applet)# | action 5.0 cli command "end" |
| Router(config-applet)# | action 6.0 cli command "exit" |
| Router(config-applet)# | exit |
| Router(config)# | event manager applet NO\_SHUT\_SVI\_VLANS |
| Router(config-applet)# | event timer countdown time 150 |
| Router(config-applet)# | action 1.0 cli command "enable" |
| Router(config-applet)# | action 2.0 cli command "conf ter" |
| Router(config-applet)# | action 3.0 cli command "int vlan 20" |
| Router(config-applet)# | action 4.0 cli command "no shutdown" |
| Router(config-applet)# | action 5.0 cli command "end" |
| Router(config-applet)# | action 6.0 cli command "exit" |
| Router(config-applet)# | end |
| Router# | copy r s |

IP SLA

**Настройка ip sla для пинга с интерфейса оборудования, на другой ip-адрес, для остановки анонса выкида в интернет этим роутером:**

|  |  |
| --- | --- |
| Router(config)# | ip sla 1 |
| Router(config-ip-sla)# | icmp-echo 8.8.8.8 source-interface lo1 |
| Router(config-ip-sla-echo)# | frequency 10 |
| Router(config ip-sla-echo)# | ip sla schedule 1 life forever start now |
| Router(config)# | track 1 ip sla 1 reachability |
| Internet(config)# | ip route 172.40.40.1 255.255.255.0 192.168.1.1 |

show track

**Остановка анонса выкида в интернет этим роутером:**

|  |  |
| --- | --- |
| Router(config)# | ip route 1.1.1.1 255.255.255.255 null 0 track 1 |
| Router(config)# | ip prefix-list CONTROL\_ROUTE seq 10 permit 1.1.1.1/32 |
| Router(config)# | route-map DEFAULT-INFORMATION permit 10 |
| Router(config-route-map)# | match ip address prefix-list control\_route |
| Router(config-route-map)# | router ospf 1 |
| Router(config-router)# | default-information originate always route-map DEFAULT-INFORMATION |

Команда default-information originate отвечает за анонс маршрута в инет по умолчанию, после привязки route-map DEFAULT-INFORMATION анонс будет происходить только когда будет работать route-map, route-map будет работать только если будет работать prefix-list control\_route, а prefix-list control\_route будет работать только когда в таблице будет маршрут 1.1.1.1 255.255.255.255 null 0, а этот маршрут там будет если состояние track 1 будет в состоянии up. (-\_-).

SLA ASA

**Настройка sla для пинга с интерфейса оборудования, на другой ip-адрес, для остановки анонса выкида в интернет ASA:**

|  |  |
| --- | --- |
| Ciscoasa(config)# | object network local-network |
| Ciscoasa(config-network-object)# | subnet 192.168.0.1 255.255.255.0 |
| Ciscoasa(config)# | int gi 0/0 |
| Ciscoasa(config-if)# | nameif outside1 |
| Ciscoasa(config-if)# | ip add 101.0.0.1 255.255.255.0 |
| Ciscoasa(config)# | int gi 0/1 |
| Ciscoasa(config-if)# | nameif outside2 |
| Ciscoasa(config-if)# | ip add 102.0.0.1 255.255.255.0 |

Далее нам необходимо установить мониторинг, который будет отменять маршрут выхода в интернет, если с этого интерфейса не будет доступен интернет.

|  |  |
| --- | --- |
| Ciscoasa(config)# | sla monitor 99 |
| Ciscoasa(config-sla-monitor-echo)# | type echo protocol ipIcmpEcho 8.8.8.8 interface outside1 |
| Ciscoasa(config-sla-monitor-echo)# | num-packets 3 |
| Ciscoasa(config-sla-monitor-echo)# | frequency 10 |
| Ciscoasa(config)# | sla monitor schedule 99 life forever start-time now |
| Ciscoasa(config)# | track 99 rtr 99 reachability |

Далее необходимо написать наши маршруты для выхода в интернет, а также доработать NAT.

|  |  |
| --- | --- |
| Ciscoasa(config)# | route outside1 0.0.0.0 0.0.0.0 101.0.0.2 100 track 99 |
| Ciscoasa(config)# | route outside2 0.0.0.0 0.0.0.0 102.0.0.2 200 |
| Ciscoasa(config)# | nat (inside,outside1) source dynamic any interface |
| Ciscoasa(config)# | nat (inside,outside2) source dynamic any interface |

FTP Backups server IOS

Install HomeFtpServerInstall.exe

Settings HomeFtpServerInstall and running server FTP.

|  |  |
| --- | --- |
| CoreSW1(config)# | archive |
| CoreSW1(config-archive)# | path ftp://FTPUser:g7#h5)1F@123.20.20.5/$H |
| CoreSW1(config-archive)# | time-period 360 |
| CoreSW1(config-archive)# | write-memory |
| CoreSW1(config-archive)# | ip ftp source-interface lo0 |
| CoreSW1# | configure replace ftp://FTPUser:g7#h5)1F@123.20.20.5/name |
| CoreSW1# | reload in 1 |

CLOCK (ЧАСЫ СИНХРОНИЗАЦИЯ)

show clock

show ntp associations

|  |  |
| --- | --- |
| EdgeRT1(config)# | clock timezone KURGAN +5 |
| EdgeRT1(config)# | service timestamps debug datetime localtime |
| EdgeRT1(config)# | service timestamps log datetime localtime |
| EdgeRT1# | clock set 12:13:00 24 Apr 2020 |
| EdgeRT1(config)# | ntp source fa0/0 |
| EdgeRT1(config)# | ntp update-calendar |
| EdgeRT1(config)# | ntp server 1.ru.pool.ntp.org prefer |
| EdgeRT1(config)# | ntp server ntp3.stratum2.ru |
| EdgeRT1(config)# | ntp master 3 |
| EdgeRT1(config)# | clock calendar-valid |
| CoreSW1(config)# | ntp peer 50.0.1.1 и на другом ntp peer 50.0.2.1 |

**Защита NTP:**

|  |  |
| --- | --- |
| EdgeRT1(config)# | access-list 1 permit host 88.147.254.232 |
| EdgeRT1(config)# | ntp access-group peer 1 |
| EdgeRT1(config)# | access-list 2 permit host 50.0.5.1 |
| EdgeRT1(config)# | ntp access-group serve-only 2 |
| Windows Server | net stop w32time  w32tm /config /syncfromflags:manual /manualpeerlist:”123.20.20.1  (настройка NTP на Windows Server через CMD)  w32tm /config /reliable:yes  net start w32time  w32tm /query /status |

VPN

**Простой VPN без шифрования (GRE тунель):**

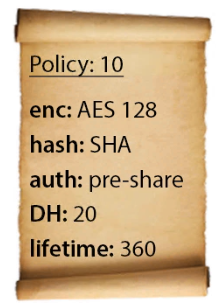
|  |  |
| --- | --- |
| EdgeRT1(config)# | ip add 217.23.145.23 255.255.255.0 |
| EdgeRT1(config)# | ip route 0.0.0.0 0.0.0.0 10.1.1.1 |
| EdgeRT1(config)# | int Tunnel0 |
| EdgeRT1(config-if)# | tunnel mode gre ip |
| EdgeRT1(config-if)# | ip add 192.168.2.1 255.255.255.0 |
| EdgeRT1(config-if)# | tunnel source fa0/1 |
| EdgeRT1(config-if)# | tunnel destination 156.213.54.76 |
| EdgeRT2(config)# | ip add 156.213.54.76 255.255.255.0 |
| EdgeRT2(config)# | ip route 0.0.0.0 0.0.0.0 10.1.2.1 |
| EdgeRT2(config)# | int Tunnel0 |
| EdgeRT2(config-if)# | tunnel mode gre ip |
| EdgeRT2(config-if)# | ip add 192.168.2.2 255.255.255.0 |
| EdgeRT2(config-if)# | tunnel source fa0/1 |
| EdgeRT2(config-if)# | tunnel destination 217.23.145.23 |

**Снятие флага DF с приходящих пакетов (когда не грузятся страницы церез VPN):**

|  |  |
| --- | --- |
| EdgeRT1(config)# | access-list 120 permit ip any any |
| EdgeRT1(config)# | route-map clear-df permit 10 |
| EdgeRT1(config-route-map)# | match ip address 120 |
| EdgeRT1(config-route-map)# | set ip df 0 |
| EdgeRT1(config)# | int fa 0/0 |
| EdgeRT1(config-if)# | ip policy route-map clear-df |

**Или:**

|  |  |
| --- | --- |
| EdgeRT1(config)# | int tunnel 0 |
| EdgeRT1(config)# | ip mtu 1500 |
| 1 | |

Создание политики - это настройка 1 фазы VPN (настройка протокола IKE (построение мини-туннеля ISAKMP) определяется как будут шифроваться данные аутентификации роутеров (фаза 2)

|  |  |
| --- | --- |
| RT(config)# | crypto isakmp policy 10 |
| RT(config-isakmp)# | encryption aes 128 |
| RT(config-isakmp)# | hash sha |
| RT(config-isakmp)# | authentication pre-share |
| RT(config-isakmp)# | group (№) |
| RT(config-isakmp)# | lifetime 120 |

Создание профиля - это дополнительная настройка первой фазы VPN

|  |  |
| --- | --- |
| RT(config)# | crypto isakmp profile MYPROF |
| RT(conf-isa-prof)# | initiate mode aggressive (не рекомендуется) |
| RT(conf-isa-prof)# | match identity address 0.0.0.0 |
| RT(conf-isa-prof)# | keyring default |
| RT(conf-isa-prof)# | crypto map PEER2 10 ipsec-isakmp |
| RT(conf-isa-prof)# | set isakmp-profile MYPROF |

|  |
| --- |
| 2 |

Построение основного туннеля IPSec – это настройка фазы 2, которая отвечает за определение как будут шифроваться пользовательские «боевые» данные

Настройка политики 2 фазы

|  |  |
| --- | --- |
| EdgeRT1(config)# | crypto ipsec transform-set TO\_PEERS esp-aes esp-sha-hmac |
| EdgeRT1(cfg-crypto-trans)# | mode tunnel |
| EdgeRT1(config)# | crypto isakmp key lait address 172.20.20.76 |

Настройка crypto-map

|  |  |
| --- | --- |
| EdgeRT(config)# | access-list 102 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 |
| EdgeRT(config)# | crypto map PEER2 10 ipsec-isakmp |
| EdgeRT(config-crypto-map)# | set peer 172.20.20.76 |
| EdgeRT(config-crypto-map)# | set transform-set TO\_PEERS |
| EdgeRT(config-crypto-map)# | match address 102 |
| EdgeRT(config-crypto-map)# | set pfs group16 |
| EdgeRT(config)# | crypto ipsec security-association lifetime kilobytes disable |
| EdgeRT(config)# | crypto ipsec security-association lifetime idle-time 1800 |
| EdgeRT(config-if)# | crypto map PEER2 |

show crypto isakmp sa detail

show crypto isakmp sa (state)

show crypto isakmp key

do clear cry sess

**IKEv2 (IPSec v2):**

Настройка атрибутов первой фазы IKEv2:

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto ikev2 proposal PHASE\_1 |
| EdgeRT(config-ikev2-proposal)# | encryption aes-cbc-256 |
| EdgeRT(config-ikev2-proposal)# | integrity sha512 |
| EdgeRT(config-ikev2-proposal)# | group № |

Определение политик IKEv2:

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto ikev2 policy POL1 |
| EdgeRT(config-ikev2-policy)# | proposal PHASE\_1 |

Определение используемых ключей:

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto ikev2 keyring RING\_1 |
| EdgeRT(config-ikev2-keyring)# | peer branch |
| EdgeRT(config-ikev2-keyring-peer)# | address 150.150.150.1 |
| EdgeRT(config-ikev2-keyring-peer)# | pre-shared-key grep |

Определение IKEv2 профиля:

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto ikev2 profile PROF |
| EdgeRT(config-ikev2-profile)# | match identity remote address 150.150.150.1 255.255.255.255 |
| EdgeRT(config-ikev2-profile)# | authentication local pre-share |
| EdgeRT(config-ikev2-profile)# | authentication remote pre-share |
| EdgeRT(config-ikev2-profile)# | keyring local RING\_1 |

Настройка политика IPSec (фазы 2)

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto ipsec transform-set PEER\_BRANCH esp-aes 256 esp-sha512-hmac |
| EdgeRT(cfg-crypto-trans)# | mode tunnel |

Настройка списков доступа:

|  |  |
| --- | --- |
| EdgeRT(config)# | ip access-list extended LIST\_FOR\_IKEv2 |
| EdgeRT(config-ext-nacl)# | permit ip 150.150.140.0 0.0.0.255 150.150.150.0 0.0.0.255 |

Настройка crypto-map:

|  |  |
| --- | --- |
| EdgeRT(config)# | crypto map IKEv2\_MAP 10 ipsec-isakmp |
| EdgeRT(config-crypto-map)# | set peer 150.150.150.1 |
| EdgeRT(config-crypto-map)# | set pfs group24 |
| EdgeRT(config-crypto-map)# | set transform-set PEER\_BRANCH |
| EdgeRT(config-crypto-map)# | match address LIST\_FOR\_IKEv2 |
| EdgeRT(config-crypto-map)# | set ikev2-profile PROF |
| EdgeRT(config-if)# | crypto map IKEv2\_MAP |

DMVPN (динамическое построение VPN туннелей):



Конечная настройка VPN

|  |  |
| --- | --- |
| 1(совпадает) | |
| R(config)# | crypto isakmp policy 10 |
| R(config-router)# | encryption aes 256 |
| R(config-router)# | hash sha |
| R(config-router)# | group 16 |
| R(config-router)# | lifetime 21600 |
| R(config-router)# | authentication pre-share |
| R(config)# | crypto isakmp key 12345 address 0.0.0.0 0.0.0.0 |
| 2(совпадает) | |
| R(config)# | crypto ipsec transform-set SetForDMVPN esp-aes 256 esp-sha-hmac |
| R(cfg-crypto-trans)# | mode transport |
| Профиль(совпадает) | |
| R(config)# | crypto ipsec profile DMVPN |
| R(ipsec-profile)# | set transform-set SetForDMVPN |
| R(ipsec-profile)# | set pfs group14 |
| R(ipsec-profile)# | set security-association lifetime seconds 10800 |
| Настройка интерфейса главного | |
| R(config)# | int tunnel1 |
| R(config-if)# | ip add 100.0.1.1 255.255.255.0 |
| R(config-if)# | ip nhrp authentication 123456 |
| R(config-if)# | tunnel key 12345 |
| R(config-if)# | ip nhrp map multicast dynamic |
| R(config-if)# | ip nhrp network-id 100 |
| R(config-if)# | tunnel source fa3/0 |
| R(config-if)# | tunnel mode gre multipoint |
| R(config-if)# | ip nhrp redirect |
| R(config-if)# | tunnel protection ipsec profile DMVPN |
| R(config-if)# | ip nhrp registration no-unique |
| R(config-if)# | crypto isakmp keepalive 10 periodic |
| Настройка интерфейса филиала | |
| R(config)# | int tunnel1 |
| R(config-if)# | ip add 100.0.1.10 255.255.255.0 |
| R(config-if)# | ip nhrp authentication 123456 |
| R(config-if)# | ip nhrp map multicast 145.145.12.1 |
| R(config-if)# | ip nhrp map 100.0.1.1 145.145.12.1 |
| R(config-if)# | ip nhrp network-id 100 |
| R(config-if)# | ip nhrp nhs 100.0.1.1 |
| R(config-if)# | ip nhrp shortcut |
| R(config-if)# | tunnel source fa0/0 |
| R(config-if)# | tunnel mode gre multipoint |
| R(config-if)# | tunnel key 12345 |
| R(config-if)# | tunnel protection ipsec profile DMVPN |
| R(config)# | crypto isakmp keepalive 10 periodic |

show ip nhrp br

**eBGP(65010) and iBGP(65020)**

Настройка динамической маршрутизации на головном-офисе:

|  |  |
| --- | --- |
| R(config)# | router bgp 65010 |
| R(config-router)# | neighbor 100.0.1.2 remote-as 65020 |
| R(config-router)# | network 134.50.10.0 mask 255.255.255.0 |
| R(config-router)# | neighbor 100.0.1.2 route-reflector-client |
| R(config-router)# | neighbor 100.0.1.2 next-hop-self |
| R(config-router)# | aggregate-address 134.50.0.0 255.255.0.0 summary-only |

Настройка динамической маршрутизации на филиале:

|  |  |
| --- | --- |
| R2(config)# | router bgp 65020 |
| R2(config-router)# | neighbor 100.0.1.1 remote-as 65010 |
| R2(config-router)# | network 134.50.13.0 mask 255.255.255.0 |
| R2(config-router)# | neighbor 100.0.1.1 allowas-in |

Настройка PKI на Cisco IOS (центр сертификации)

Конфигурация PKI-сервера (центр сертификации) Cisco:

|  |  |
| --- | --- |
| CA(config)# | crypto key generate rsa label CS-KEYS modulus 2048 exportable |
| CA(config)# | crypto pki trustpoint MY-CS |
| CA(ca-trustpoint)# | rsakeypair CS-KEYS |
| CA(config)# | ip http server |
| CA(config)# | crypto pki server MY-HTTP-CS |
| CA(ca-server)# | issuer-name CN=CA,OU=VPN,O=BTI,C=RU |
| CA(ca-server)# | database url nvram:/certbase |
| CA(ca-server)# | database url crl publish ftp://123.20.20.5/ username CA password @$@$ |
| CA(ca-server)# | database level complete |
| CA(ca-server)# | hash sha1 |
| CA(ca-server)# | lifetime certificate 365 |
| CA(ca-server)# | lifetime ca-certificate 730 |
| CA(ca-server)# | lifetime crl 24 |
| CA(ca-server)# | grant auto |
| CA(ca-server)# | no shut |

**Настройка клиентской части:**

|  |  |
| --- | --- |
| RT (config)# | ip domain name bti.local |
| RT (config)# | crypto key generate rsa label VPN-KEYS modulus 2048 |
| RT (config)# | crypto pki trustpoint VPN-PKI |
| RT (ca-trustpoint)# | enrollment url http://122.122.122.1 |
| RT (ca-trustpoint)# | fqdn nameIOS.bti.local |
| RT (ca-trustpoint)# | subject-name CN=nameIOS,OU=VPN,O=BTI,C=RU |
| RT (ca-trustpoint)# | rsakeypair VPN-KEYS |
| RT (config)# | crypto pki authenticate VPN-PKI |
| CA(config)# | crypto pki enroll VPN-PKI |

Настройка VPN с аутентификацией по сертификатам:

|  |  |
| --- | --- |
| RT(config)# | crypto isakmp policy 10 |
| RT(config-isakmp)# | encryption aes 128 |
| RT(config-isakmp)# | hash sha |
| RT(config-isakmp)# | authentication rsa-sig |
| RT(config-isakmp)# | group (№) |
| RT(config-isakmp)# | lifetime 3600 |