1.6.2 ESR OTT

-
-
-
- ESR

EoGRE 1.4.1 ESR1200/1700 , GRE . GRE, IPsec , ESR . IPsec VRF, , , GRE VRF IPsec, VRF ESR.

, te1/0/1, SoftWLC, OTT . IPsec OTT te1/0/1.4092, port-channel 2, VRF ipsec. po2 (te1/0/2 te1/0/6, te1/0/3 te1/0/7) port-channel 1, VRF. , GRE VRF ipsec connected .

ESR, .

1.6.2, BGP, ESR, EoGRE (ESR 1200/1700). :

1) te1/0/1.4092: 10.12.20.3/28 - , , IPsec, VRF ipsec;

2) port-channel 2: 192.168.200.35./28 - , GRE ;

3) te1/0/1.4081: 10.255.255.6/30 - , VRF backbone SoftWLC, DHCP DNS ;

4) te1/0/1.4082: 10.255.255.10/30 - , VRF nat ;

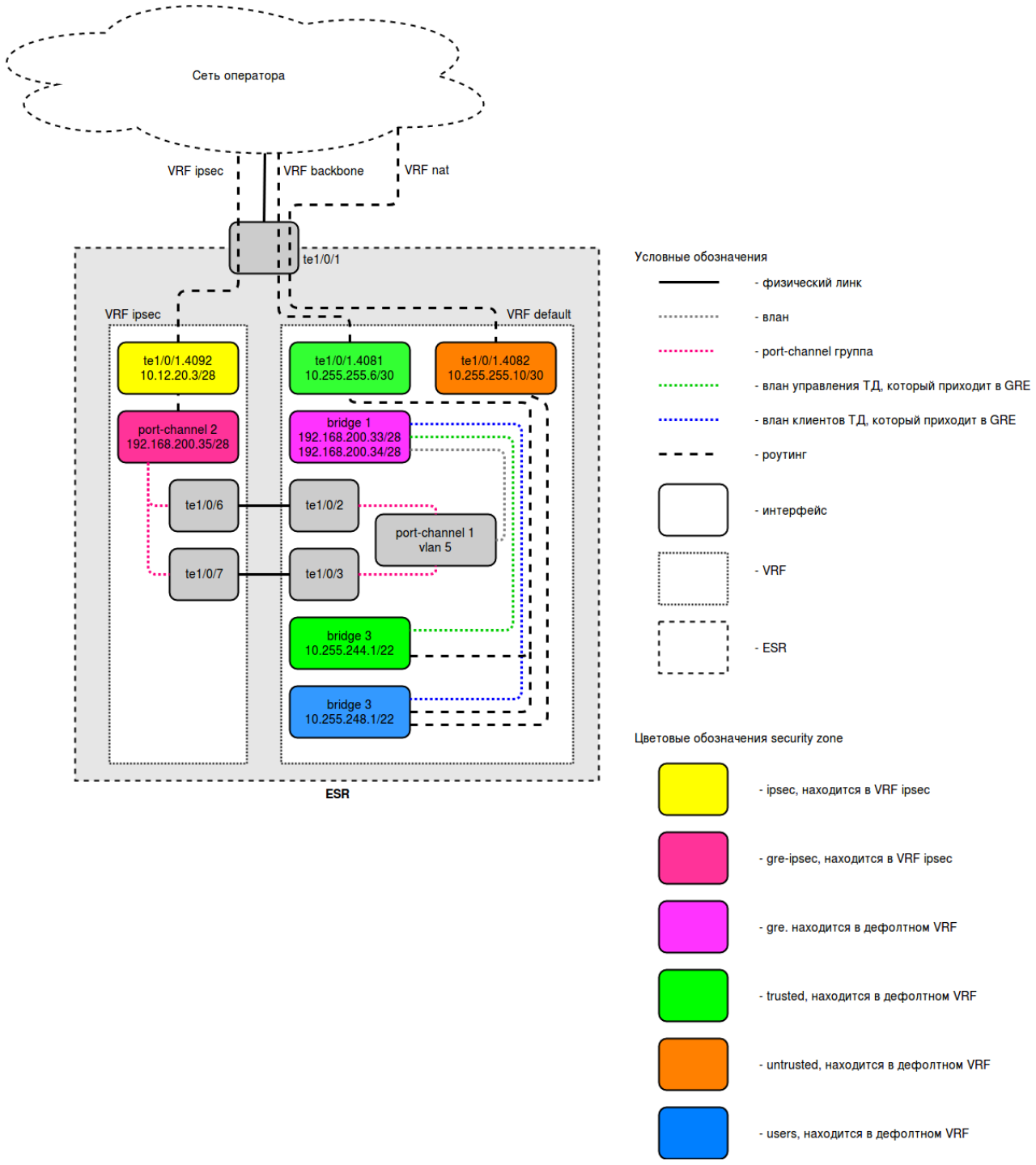
4) bridge 1: 192.168.200.33/28 192.168.200.34/28 - EoGRE , ;

5) bridge 3: 10.255.244.0/22 - . 10.255.244.1 ESR SoftWLC;

6) bridge 10: 10.255.244.0/22 - . - 10.255.244.1, DNS 100.123.0.2;

7) 172.31.0.0/21 - , mode config, EoGRE ;

8) 100.110.123.0/24 - . 100.123.0.2 - SoftWLC, DHCP, DNS.



ESR

```
hostname esr-ipsec

ip firewall sessions classification enable
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ipsec_ports
```

```
  port-range 500
  port-range 4500
exit
object-group service snmp
  port-range 161-162
exit
object-group service dns
  port-range 53
exit
object-group service bgp
  port-range 179
exit

object-group network SoftWLC
  ip prefix 100.123.0.0/24
exit
object-group network ipsec_remote_address
  ip prefix 172.31.0.0/21
exit
object-group network gre_termination
  ip prefix 192.168.200.32/28
exit
object-group network mgmt_AP
  ip prefix 10.255.244.0/22
  ip prefix 10.255.248.0/22
exit
object-group network clients_AP
  ip prefix 10.255.244.0/22
  ip prefix 10.255.248.0/22
exit

ip vrf ipsec
exit

syslog console none

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 10.255.255.6
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text testing123
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

vlan 3
  force-up
exit
vlan 10
  force-up
exit
vlan 5
exit

security zone trusted
exit
```

```
security zone gre
exit
security zone ipsec
  ip vrf forwarding ipsec
exit
security zone untrusted
exit
security zone gre-ipsec
  ip vrf forwarding ipsec
exit
security zone users
exit


ip protocols bgp max-routes 256
route-map out_BGP_AP
  rule 10
    match ip address object-group mgmt_AP
    action permit
  exit
exit
route-map out_BGP_NAT
  rule 10
    match ip address object-group clients_AP
    action permit
  exit
exit
router bgp 64601
  address-family ipv4
    router-id 10.255.255.6
    redistribute connected
    neighbor 10.255.255.5
      remote-as 65001
      route-map out_BGP_AP out
      update-source 10.255.255.6
      enable
    exit
    neighbor 10.255.255.9
      remote-as 65001
      route-map out_BGP_NAT out
      update-source 10.255.255.10
      enable
    exit
    enable
  exit
exit

snmp-server
snmp-server system-shutdown
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 100.123.0.2
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment pwrin
snmp-server enable traps environment pwrin-insert
snmp-server enable traps environment fan
snmp-server enable traps environment fan-speed-changed
snmp-server enable traps environment fan-speed-high
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
```

```
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps environment board-overheat-temp
snmp-server enable traps environment board-supercooling-temp
snmp-server enable traps environment sfp-overheat-temp
snmp-server enable traps environment sfp-supercooling-temp
snmp-server enable traps environment switch-overheat-temp
snmp-server enable traps environment switch-supercooling-temp
snmp-server enable traps wifi
snmp-server enable traps wifi wifi-tunnels-number-in-bridge-high
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon fan
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon supply
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
  vlan 5
  security-zone gre
  ip address 192.168.200.33/28
  ip address 192.168.200.34/28
  enable
```

```
exit
bridge 3
  vlan 3
  security-zone trusted
  ip address 10.255.244.1/22
  ip helper-address 100.123.0.2
  ip tcp adjust-mss 1312
  protected-ports
  protected-ports exclude vlan
  enable
exit
bridge 10
  vlan 10
  security-zone users
  ip address 10.255.248.1/22
  ip helper-address 100.123.0.2
  ip tcp adjust-mss 1312
  location AP1
  protected-ports
  protected-ports exclude vlan
  enable
exit

interface port-channel 1
  mode hybrid
  speed 10G
  switchport forbidden default-vlan
  switchport general pvid 5
  switchport general allowed vlan add 5 untagged
exit
interface port-channel 2
  ip vrf forwarding ipsec
  mode hybrid
  speed 10G
  security-zone gre-ipsec
  ip address 192.168.200.35/28
exit
interface tengigabitethernet 1/0/1
  description "UpLink"
exit
interface tengigabitethernet 1/0/1.4081
  description "VRF_backbone"
  security-zone trusted
  ip address 10.255.255.6/30
  ip tcp adjust-mss 1312
exit
interface tengigabitethernet 1/0/1.4082
  description "VRF_nat"
  security-zone untrusted
  ip address 10.255.255.10/30
exit
interface tengigabitethernet 1/0/1.4092
  ip vrf forwarding ipsec
  description "VRF_ipsec"
  security-zone ipsec
  ip address 10.12.20.3/28
exit
interface tengigabitethernet 1/0/2
  mode hybrid
  channel-group 1 mode auto
exit
interface tengigabitethernet 1/0/3
  mode hybrid
  channel-group 1 mode auto
exit
interface tengigabitethernet 1/0/6
  mode hybrid
  channel-group 2 mode auto
exit
interface tengigabitethernet 1/0/7
  mode hybrid
```

```
  channel-group 2 mode auto
exit
interface service-port 1
  service-policy dynamic
exit
tunnel softgre 1
  description "managment_AP"
  mode management
  local address 192.168.200.33
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 3
  enable
exit
tunnel softgre 2
  description "data_AP"
  mode data
  local address 192.168.200.34
  default-profile
  enable
exit

port-channel load-balance src-dst-ip

security zone-pair trusted self
  rule 10
    action permit
    enable
  exit
exit
security zone-pair users self
  rule 10
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port redirect
    enable
  exit
exit
security zone-pair gre self
  rule 10
    action permit
    match protocol gre
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
  rule 20
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair users trusted
  rule 10
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
```

```
    match protocol udp
    match destination-port dns
    enable
  exit
exit
security zone-pair ipsec self
  rule 10
    action permit
    match protocol udp
    match destination-port ipsec_ports
    enable
  exit
  rule 20
    action permit
    match protocol esp
    enable
  exit
  rule 30
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted trusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair users untrusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair untrusted self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port bgp
    enable
  exit
exit
security zone-pair ipsec gre-ipsec
  rule 10
    action permit
    match protocol gre
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
exit
security zone-pair gre-ipsec ipsec
  rule 10
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair gre-ipsec self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
exit
```

```
address-assignment pool ipsec_pool_1
  ip prefix 172.31.0.0/21
  data-tunnel address 192.168.200.34
  management-tunnel address 192.168.200.33
exit

security ike proposal dh1_md5_aes128
  authentication algorithm md5
  encryption algorithm aes128
exit

security ike policy psk_xauth
  lifetime seconds 86400
  pre-shared-key ascii-text testing123
  authentication method xauth-psk-key
  authentication mode radius
  proposal dh1_md5_aes128
exit

security ike gateway xauth_ike
  ike-policy psk_xauth
  local address 10.12.20.3
  local network 192.168.200.32/28
  remote address any
  remote network dynamic pool ipsec_pool_1
  mode policy-based
  dead-peer-detection action clear
  dead-peer-detection interval 60
  dead-peer-detection timeout 180
exit

security ipsec proposal md5_aes128_esp
  authentication algorithm md5
  encryption algorithm aes128
exit

security ipsec policy ipsec_pol
  proposal md5_aes128_esp
exit

security ipsec vpn xauth_ipsec
  mode ike
  ip vrf forwarding ipsec
  ike establish-tunnel by-request
  ike gateway xauth_ike
  ike ipsec-policy ipsec_pol
  enable
exit

security passwords history 0
ip dhcp-relay

ip route 172.31.0.0/21 192.168.200.35
ip route vrf ipsec 0.0.0.0 10.12.20.2

wireless-controller
  nas-ip-address 10.255.255.6
  resp-time 3
  failure-count 3
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
```

```
ntp server 100.123.0.2
exit
```