1.4.1 ESR OTT

-
- ESR

EoGRE 1.4.1 ESR1200/1700 , GRE . GRE, IPsec , ESR . IPsec VRF, , , GRE VRF IPsec, VRF ESR. .. - ESR1200 /1700 OTT EoGRE. 1.4.0-OTT IPsec VRF, ESR 1.4.1 - .

, te1/0/1, SoftWLC, OTT . IPsec OTT te1/0/1.4000, po2, VRF ipsec. po2 (te1/0/2 te1/0/6, te1/0/3 te1/0/7) po6, VRF. , GRE VRF ipsec connected .

ESR

:

```
object-group service telnet
 port-range 23
exit
object-group service ssh
 port-range 22
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service ntp
 port-range 123
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 COA
 port-range 3799
 port-range 31812-31813
exit
object-group network SoftWLC
 ip address-range 101.0.0.24
exit
object-group network ipsec_remote_address
 ip prefix 172.31.0.0/21
exit
object-group network gre_termination
 ip prefix 192.168.7.0/29
exit
object-group network mgmt_AP
 ip prefix 10.2.0.0/21
exit
```

VRF ipsec1:

```
ip vrf ipsec1
exit
```

-:

```
radius-server timeout 10
radius-server retransmit 5
radius-server host 101.0.0.24
 key ascii-text encrypted 88B11079B9014FAAF7B9
 timeout 11
 priority 20
 source-address 10.255.0.2
 auth-port 31812
 acct-port 31813
 retransmit 10
 dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 101.0.0.24
exit
das-server COA
 key ascii-text encrypted 88B11079B9014FAAF7B9
 port 3799
 clients object-group SoftWLC
exit
aaa das-profile COA
 das-server COA
exit
```

vlan:

```
vlan 5
 force-up
exit
vlan 6
 force-up
exit
vlan 7
 force-up
exit
```

:

```
security zone trusted
exit
security zone user
exit
security zone gre
exit
security zone ipsec
 ip vrf forwarding ipsec1
exit
security zone untrusted
exit
security zone gre-vrf1
 ip vrf forwarding ipsec1
exit
security zone trusted1
 ip vrf forwarding ipsec1
exit
```

BGP:

```
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 64534
 address-family ipv4
  neighbor 10.255.0.1
   remote-as 64512
   route-map out_BGP_AP out
   update-source 10.255.0.2
   enable
  exit
  neighbor 10.255.0.5
   remote-as 64512
   route-map out_BGP_NAT out
   update-source 10.255.0.6
   enable
  exit
  enable
 exit
exit
```

SNMP-:

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

snmp-server host 101.0.0.24
exit
```

VRF GRE, , :

```
bridge 5
 vlan 5
 security-zone gre
 ip address 192.168.7.1/29
 ip address 192.168.7.2/29
 enable
exit
bridge 6
 vlan 6
 security-zone trusted
 ip address 10.2.0.1/21
 ip helper-address 101.0.0.24
 ip tcp adjust-mss 1312
 protected-ports
 protected-ports exclude vlan
 enable
exit
bridge 7
 vlan 7
 security-zone user
 ip address 172.31.236.1/22
 ip helper-address 101.0.0.24
 ip tcp adjust-mss 1312
 location AP1
 protected-ports
 protected-ports exclude vlan
 enable
exit
```

VRF ipsec1, , GRE :

```
interface port-channel 2
 ip vrf forwarding ipsec1
 speed 10G
 security-zone gre-vrf1
 ip address 192.168.7.3/29
exit
```

VRF, GRE bridge 5, GRE:

```
interface port-channel 6
 speed 10G
 switchport forbidden default-vlan
 switchport general pvid 5
 switchport general allowed vlan add 5 untagged
exit
```

:

```
interface tengigabitethernet 1/0/1

 switchport forbidden default-vlan
 switchport general acceptable-frame-type tagged-only
exit
```

SoftWLC:

```
interface tengigabitethernet 1/0/1.601
 description "mgmt_SoftWLC"
 security-zone trusted
 ip address 10.255.0.2/30
exit
```

NAT, :

```
interface tengigabitethernet 1/0/1.602
 description "clients_to_inet"
 security-zone untrusted
 ip address 10.255.0.6/30
exit
```

IP OTT , VRF ipsec1:

```
interface tengigabitethernet 1/0/1.4000
 ip vrf forwarding ipsec1
 security-zone ipsec
 ip address 188.237.154.25/31
exit
```

PO 2 :

```
interface tengigabitethernet 1/0/2
 channel-group 2 mode auto
exit
interface tengigabitethernet 1/0/3
 channel-group 2 mode auto
exit
```

PO 6 :

```
interface tengigabitethernet 1/0/6
 channel-group 6 mode auto
exit
interface tengigabitethernet 1/0/7
 channel-group 6 mode auto
exit
```

softgre :

```
tunnel softgre 1
 description "mgmt"
 mode management
 local address 192.168.7.1
 default-profile
 enable
exit
tunnel softgre 1.1
 bridge-group 6
 enable
exit
tunnel softgre 2
 description "data"
 mode data
 local address 192.168.7.2
 default-profile
 enable
exit
```

port-channel ip src, dst, port:

```
port-channel load-balance src-dst-ip-port
```

:

```
security zone-pair trusted self
  rule 100
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair user self
  rule 10
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port redirect
    enable
  exit
exit
security zone-pair gre self
  rule 10
    action permit
    match protocol any
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
exit
security zone-pair user trusted
  rule 10
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
exit
security zone-pair ipsec self
  rule 1
    action permit
    match protocol icmp
    match source-address any
    match destination-address any
    enable
  exit
  rule 11
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port ipsec_ports
    enable
  exit
  rule 12
    action permit
    match protocol esp
    match source-address any
    match destination-address any
    enable
  exit
```

```
  rule 13
    action permit
    match protocol gre
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
  rule 14
    action permit
    match protocol icmp
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
exit
security zone-pair trusted trusted
  rule 100
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair user untrusted
  rule 100
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair untrusted self
  rule 10
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol icmp
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair ipsec gre-vrf1
  rule 10
    action permit
    match protocol any
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
exit
security zone-pair gre-vrf1 ipsec
  rule 10
    action permit
    match protocol any
    match source-address gre_termination
    match destination-address ipsec_remote_address
    enable
  exit
exit
security zone-pair gre-vrf1 self
  rule 100
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair trusted untrusted
```

```
 rule 100
  action permit
  match protocol any
  match source-address any
  match destination-address any
  enable
 exit
exit
```

, mode config:

```
address-assignment pool ipsec_pool_1
 ip prefix 172.31.0.0/21
 data-tunnel address 192.168.7.2
 management-tunnel address 192.168.7.1
exit
```

IKE , , :

```
security ike proposal dh1_md5_aes128
 authentication algorithm md5
 encryption algorithm aes128
exit
security ike policy psk_xauth1
 lifetime seconds 86400
 pre-shared-key ascii-text encrypted 88B11079B9014FAAF7B9
 authentication method xauth-psk-key
 authentication mode radius
 proposal dh1_md5_aes128
exit
        security ike gateway ike1_from_inet
 ike-policy psk_xauth1
 local address 188.237.154.25
 local network 192.168.7.0/29
 remote address any
 remote network dynamic pool ipsec_pool_1
 mode policy-based
 dead-peer-detection action clear
 dead-peer-detection interval 10
exit
```

IPsec , VPN. VPN , VRF ipsec1:

```
security ipsec proposal md5_aes128_esp
 authentication algorithm md5
 encryption algorithm aes128
exit
security ipsec policy vpn1_pol1
 proposal md5_aes128_esp
exit
security ipsec vpn for_INET_1
 mode ike
 ip vrf forwarding ipsec1
 ike establish-tunnel by-request
 ike gateway ike1_from_inet
 ike ipsec-policy vpn1_pol1

 enable
exit
```

DHCP-:

```
ip dhcp-relay
```

:

```
ip route 172.31.0.0/21 192.168.7.3              # VRF IP , VRF ipsec1

ip route 188.237.154.24/31 192.168.7.3          # VRF IPsec VRF ipsec1

ip route vrf ipsec1 0.0.0.0/0 188.237.154.24    # VRF ipsec1
```

softgre:

```
wireless-controller
  nas-ip-address 10.255.0.2
  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 101.0.0.24
  prefer
exit
```