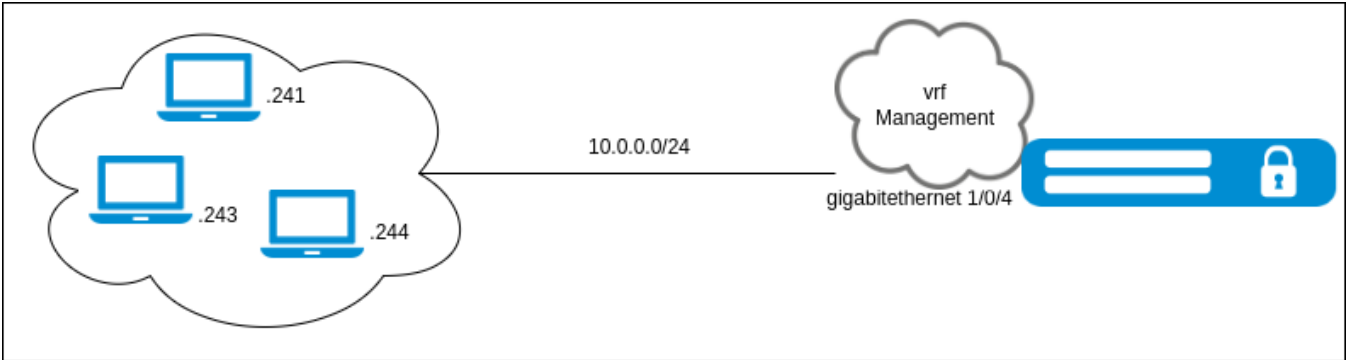


SSH, Telnet VRF

-
-
-
- VRF
- object-group
-
- SSH, Telnet
- SSH Telnet vrf
-

SSH Telnet VRF (virtual routing and forwarding).



SSH Telnet VRF zone-based firewall

- i** zone-based firewall :
- Zone-Based StateFull Firewall
 -

i zone-based firewall. - , SSH Telnet, firewall zone-based firewall , SSH, Telnet, ssh/telnet Firewall

, SSH Telnet VRF , VRF. vrf Management. zone-based firewall Trusted. vrf. vrf Management IP-, -
Trusted self. SSH Telnet , VRF.

VRF

VRF Management:

```
esr# configure
esr(config)# ip vrf Management
esr(config-vrf)# exit
```

Trusted VRF:

```

esr(config)# security zone Trusted
esr(config-security-zone)# ip vrf forwarding Management
esr(config-security-zone)# exit

```

, . vrf Management, Trusted IP:-

```

esr# configure
esr(config)# interface gigabitethernet 1/0/4
esr(config-if-sub)# ip vrf forwarding Management
esr(config-if-sub)# security-zone Trusted
esr(config-if-sub)# ip address 10.0.0.1/24
esr(config-if-sub)# exit

```

object-group

object-group , .

object-group network Remote_admin. IP-, . IP- 10.0.0.241, 10.0.0.243 - 10.0.0.244:

```

esr(config)# object-group network Remote_admin
esr(config-object-group-network)# ip address-range 10.0.0.241
esr(config-object-group-network)# ip address-range 10.0.0.243-10.0.0.244
esr(config-object-group-network)# exit

```

object-group network Router_management. IP- , . IP- 10.0.0.1:

```

esr(config)# object-group network Router_management
esr(config-object-group-network)# ip address-range 10.0.0.1
esr(config-object-group-network)# exit

```

object-group service TCP- (SSH,Telnet), , SSH_port Telnet_port. , :

```

esr(config)# object-group service SSH_port
esr(config-object-group-network)# port-range 33221
esr(config-object-group-network)# exit
esr(config)# object-group service Telnet_port
esr(config-object-group-network)# port-range 24221
esr(config-object-group-network)# exit

```

Trusted self. SSH Telnet :

- - TCP
- IP-, object-group network Remote_admin
- IP-, object-group network Router_management
- TCP-, object-group service SSH_port object-group service Telnet_port

```

security zone-pair Trusted self
rule 1
    description "SSH"
    action permit
    match protocol tcp
    match source-address Remote_admin
    match destination-address Router_management
    match destination-port SSH_port
    enable
exit
rule 2
    description "Telnet"
    action permit
    match protocol tcp
    match source-address Remote_admin
    match destination-address Router_management
    match destination-port Telnet_port
    enable
exit
exit

```

SSH, Telnet

SSH Telnet, . object-group . , :

```

esr(config)# ip ssh port 33221
esr(config)# ip telnet port 24221

```

SSH Telnet vrf

SSH Telnet vrf:

```

esr(config)# ip ssh server vrf Management
esr(config)# ip telnet server vrf Management

```

SSH Telnet :

```

user@PC-1:~# telnet 10.0.0.1 24221
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.

```

esr login:

```

user@PC-2:~# ssh -l admin -p 33221 10.0.0.1
Password:

```

show ip firewall sessions vrf Management :

```
esr# show ip firewall sessions vrf Management
Codes: E - expected, U - unreplied,
       A - assured, C - confirmed
```

Prot	Inside source		Inside destination	Outside source	Outside destination
Pkts	Bytes	Status			
-----	-----	-----	-----	-----	-----
tcp	10.0.0.243:50296		10.0.0.1:33221	10.0.0.243:50296	10.0.0.1:33221
--	--	AC			
tcp	10.0.0.244:50174		10.0.0.1:24221	10.0.0.244:50174	10.0.0.1:24221
--	--	AC			