Technical Note: Inter-VDOM routing

Product: Fortigate 5.0 Onwards

Requirement:

Traffic routing between 2 VDOMs

ROOT and ERP_Users VDOM network design is as below

WAN1 > 172.31.16.196 -- root vdom

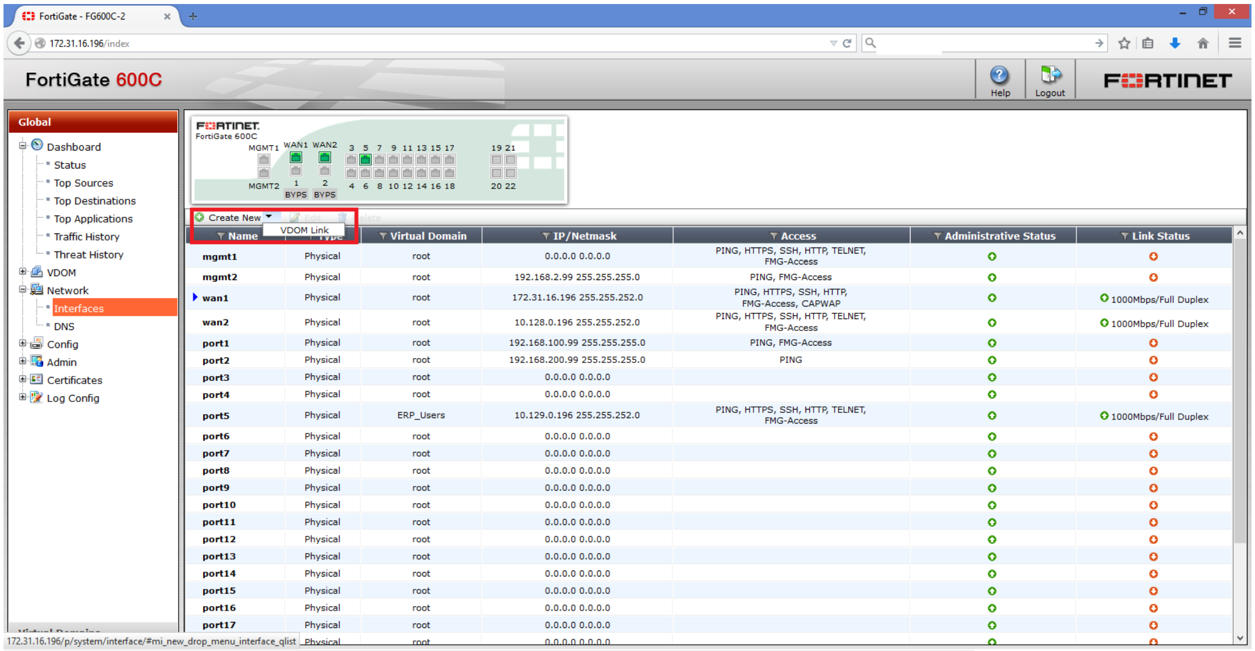
WAN2 > 10.128.0.196/23 -- root VDOM internal interface

Port5 > 10.129.0.196/23 -- ERP_Users VDOM internal interface

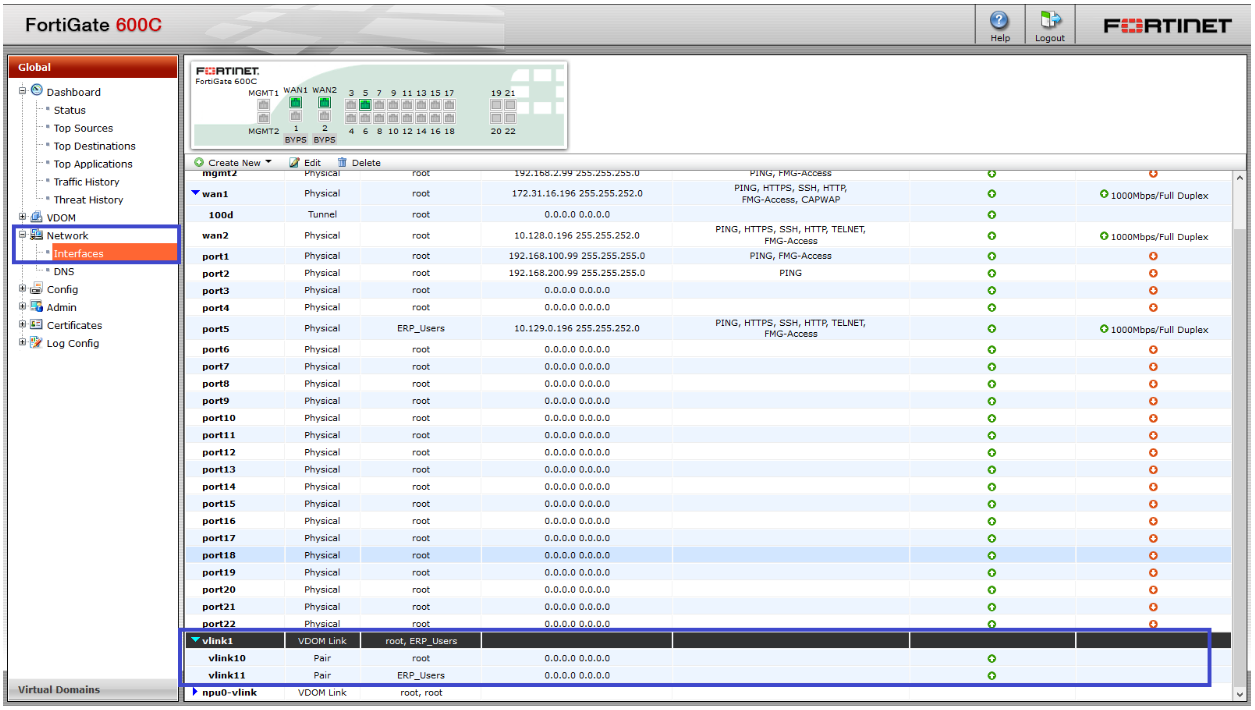
User should be able to communicate from ERP_Users Port5 to WAN2 subnet and vice-verse

On Global Settings:

Creating VDOM Link under System > Network > Interface >



Name	Type	Virtual Domain	IP/Netmask	Access	Administrative Status	Link Status
mgmt1	Physical	root	0.0.0.0 0.0.0.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	▲	▼
mgmt2	Physical	root	192.168.2.99 255.255.255.0	PING, FMG-Access	▲	▼
wan1	Physical	root	172.31.16.196 255.255.252.0	PING, HTTPS, SSH, HTTP, FMG-Access, CAPWAP	▲	▲ 1000Mbps/Full Duplex
wan2	Physical	root	10.128.0.196 255.255.252.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	▲	▲ 1000Mbps/Full Duplex
port1	Physical	root	192.168.100.99 255.255.255.0	PING, FMG-Access	▲	▼
port2	Physical	root	192.168.200.99 255.255.255.0	PING	▲	▼
port3	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port4	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port5	Physical	ERP_Users	10.129.0.196 255.255.252.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	▲	▲ 1000Mbps/Full Duplex
port6	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port7	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port8	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port9	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port10	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port11	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port12	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port13	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port14	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port15	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port16	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port17	Physical	root	0.0.0.0 0.0.0.0		▲	▼
	Physical	root	0.0.0.0 0.0.0.0		▲	▼

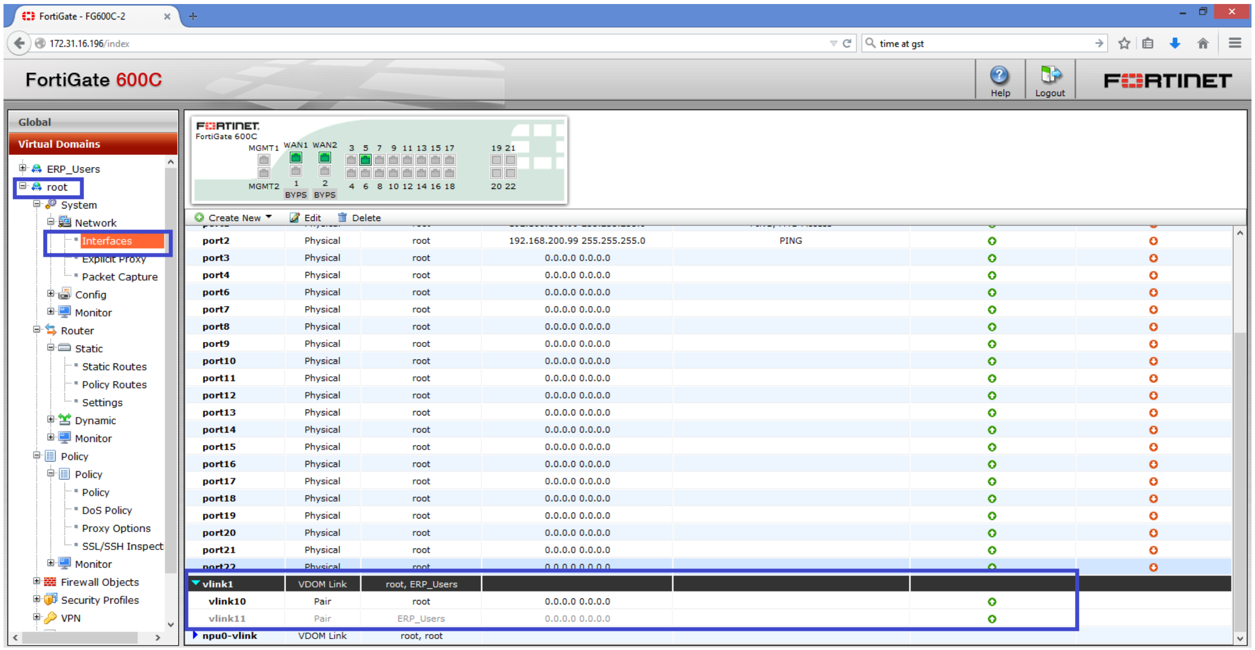


mgmt2	Physical	root	192.168.2.99 255.255.255.0	PING, FMG-Access	▲	▼
wan1	Physical	root	172.31.16.196 255.255.252.0	PING, HTTPS, SSH, HTTP, FMG-Access, CAPWAP	▲	▲ 1000Mbps/Full Duplex
100d	Tunnel	root	0.0.0.0 0.0.0.0		▲	
wan2	Physical	root	10.128.0.196 255.255.252.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	▲	▲ 1000Mbps/Full Duplex
port1	Physical	root	192.168.100.99 255.255.255.0	PING, FMG-Access	▲	▼
port2	Physical	root	192.168.200.99 255.255.255.0	PING	▲	▼
port3	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port4	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port5	Physical	ERP_Users	10.129.0.196 255.255.252.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	▲	▲ 1000Mbps/Full Duplex
port6	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port7	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port8	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port9	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port10	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port11	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port12	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port13	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port14	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port15	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port16	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port17	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port18	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port19	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port20	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port21	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port22	Physical	root	0.0.0.0 0.0.0.0		▲	▼
vlink1	VDOM Link	root, ERP_Users				
vlink10	Pair	root	0.0.0.0 0.0.0.0		▲	
vlink11	Pair	ERP_Users	0.0.0.0 0.0.0.0		▲	
npu0-vlink	VDOM Link	root, root				

After creating the vdom-interlink need to pair the correct VDOMs

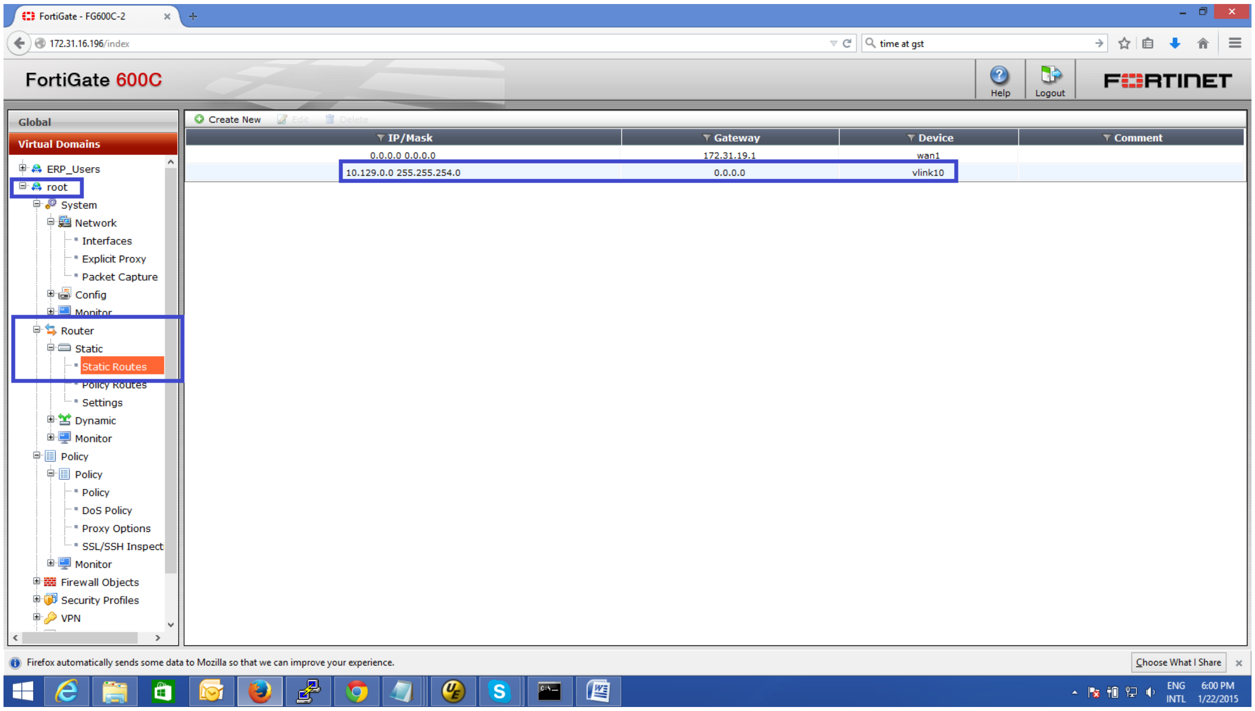
ROOT VDOM settings:

VDOM Interface on 'root' vdom



port2	Physical	root	192.168.200.99 255.255.255.0	PING	▲	▼
port3	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port4	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port6	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port7	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port8	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port9	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port10	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port11	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port12	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port13	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port14	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port15	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port16	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port17	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port18	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port19	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port20	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port21	Physical	root	0.0.0.0 0.0.0.0		▲	▼
port22	Physical	root	0.0.0.0 0.0.0.0		▲	▼
vlink1	VDOM Link	root, ERP_Users				
vlink10	Pair	root	0.0.0.0 0.0.0.0		▲	
vlink11	Pair	ERP_Users	0.0.0.0 0.0.0.0		▲	
npu0-vlink	VDOM Link	root, root				

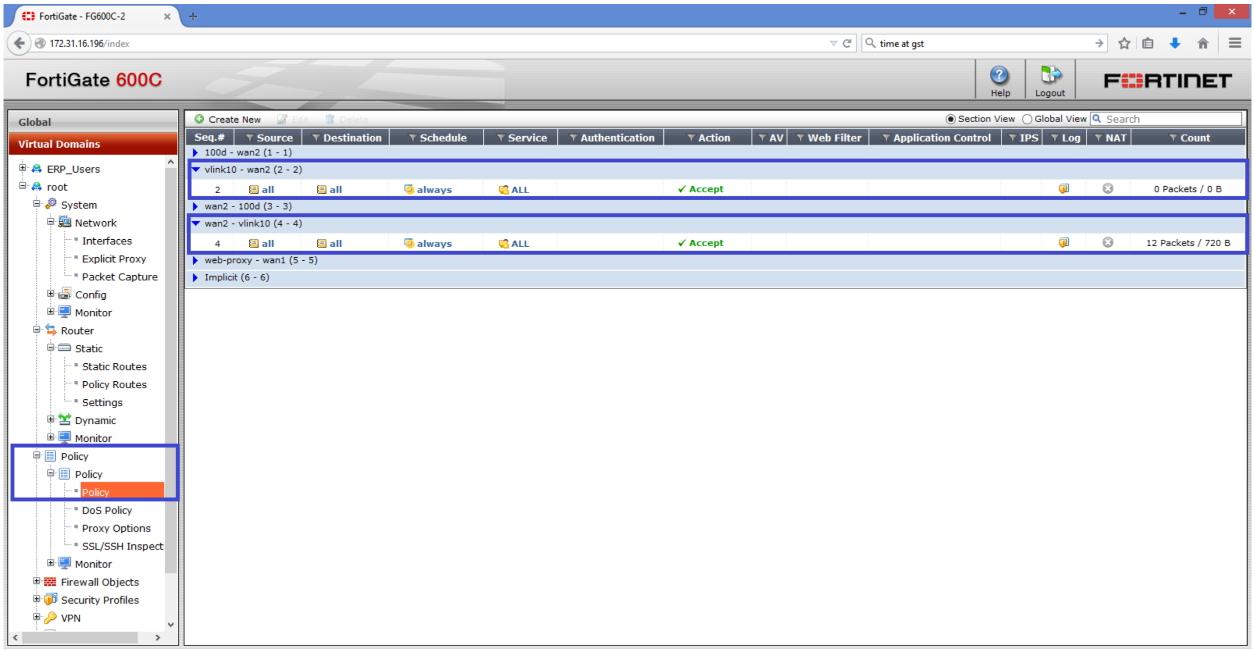
Configuring route to ERP_Users port5 subnet



IP/Mask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	172.31.19.1	wan1	
10.129.0.0 255.255.254.0	0.0.0.0	vlink10	

Need to select the correct vlink interface (which is paired)

Configuring firewall policies

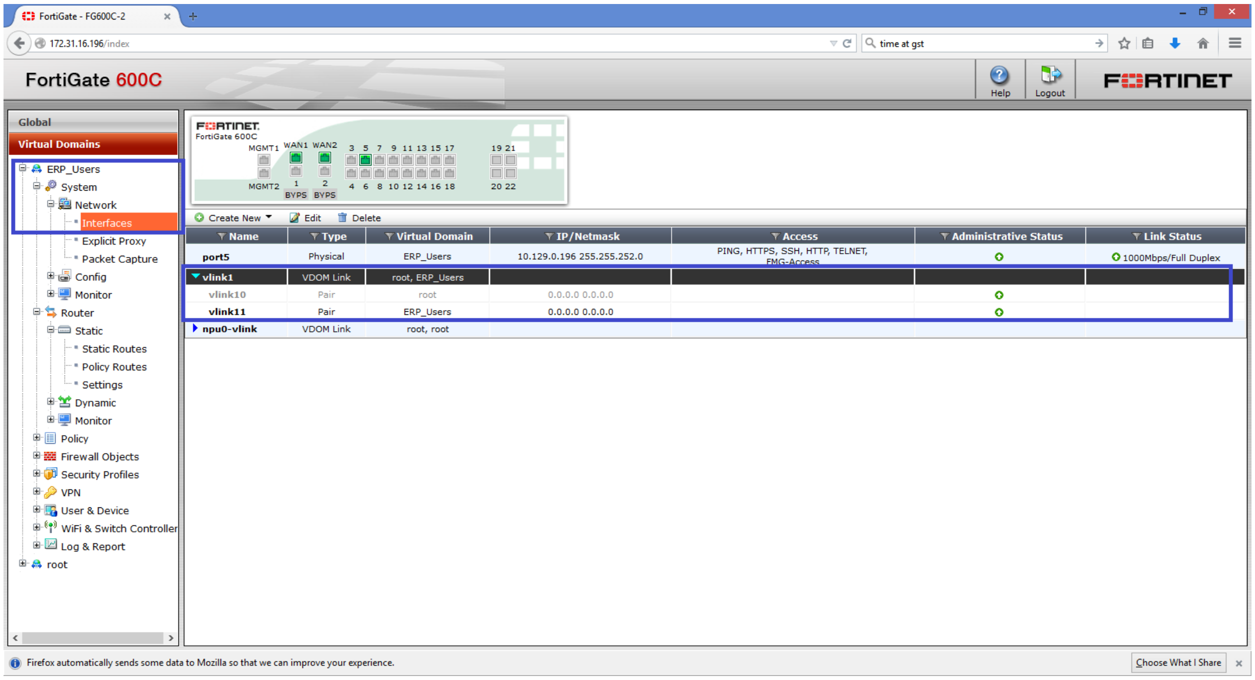


Seq.#	Source	Destination	Schedule	Service	Authentication	Action	AV	Web Filter	Application Control	IPS	Log	NAT	Count
100d - wan2 (1 - 1)													
vlink10 - wan2 (2 - 2)													
2	all	all	always	ALL		✓ Accept							0 Packets / 0 B
wan2 - 100d (3 - 3)													
wan2 - vlink10 (4 - 4)													
4	all	all	always	ALL		✓ Accept							12 Packets / 720 B
web-proxy - wan1 (5 - 5)													
Implicit (6 - 6)													

Need to configure policy from vlink10 to wan2 and vice-verse

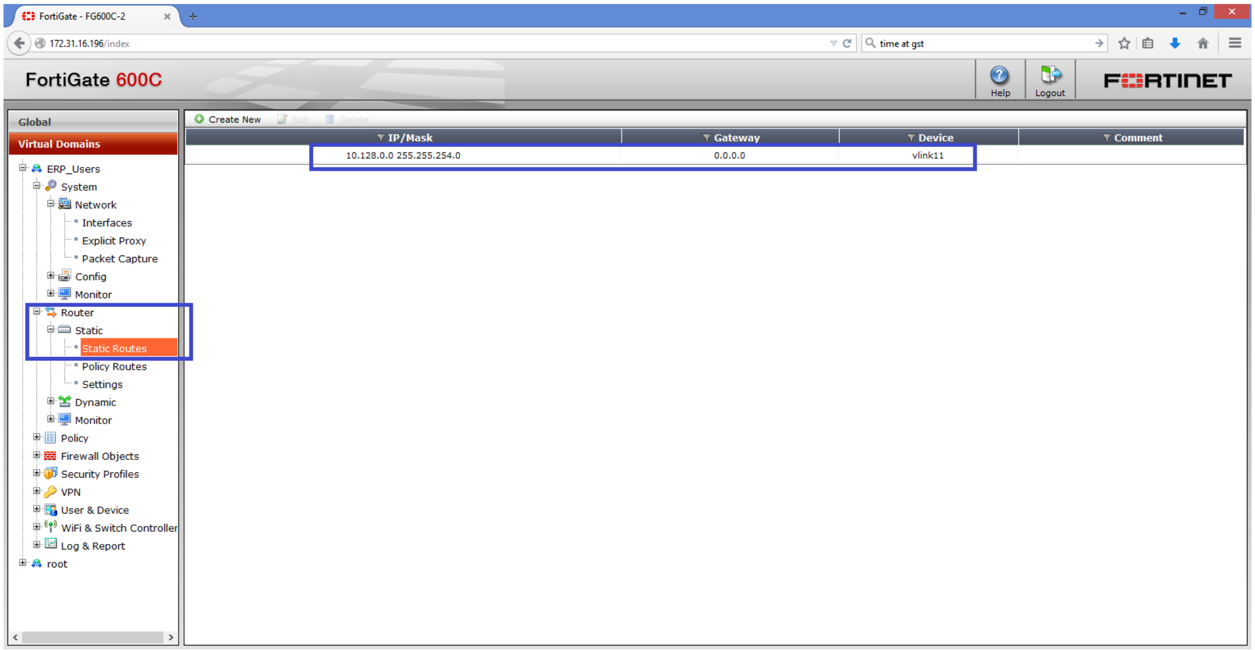
Configuration on ERP_Users VDOM

Interfaces on ERP_Users VDOM



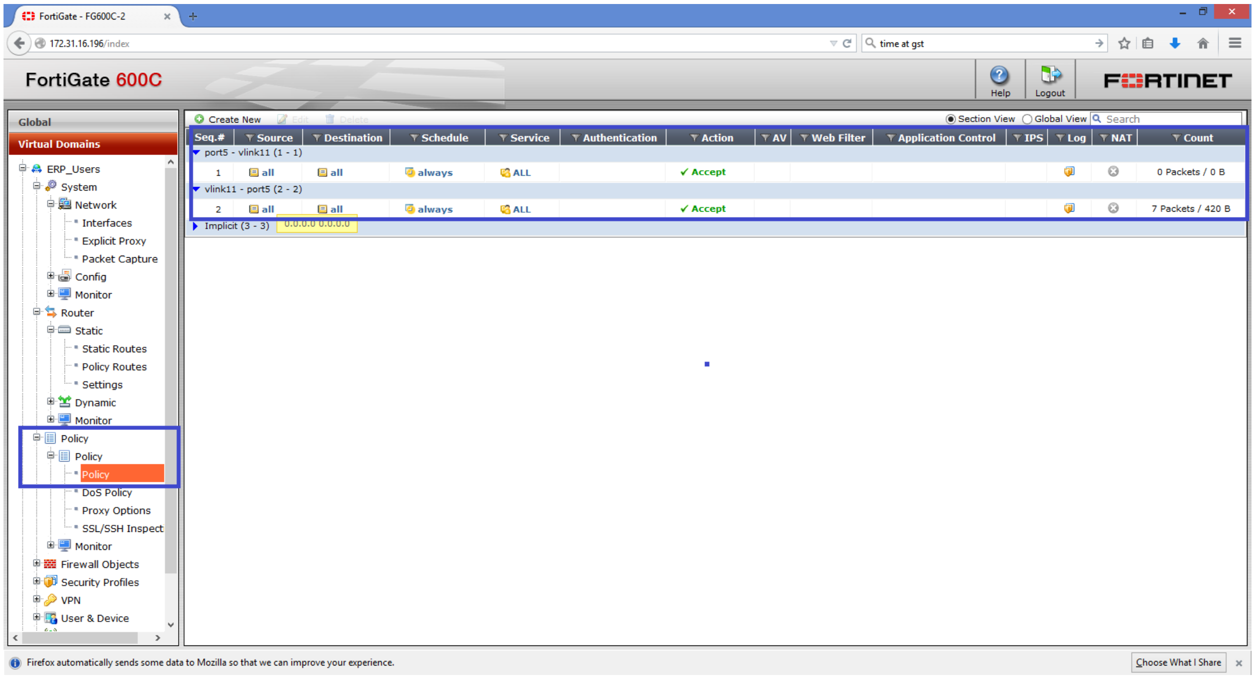
Name	Type	Virtual Domain	IP/Netmask	Access	Administrative Status	Link Status
port5	Physical	ERP_Users	10.129.0.196 255.255.252.0	PING, HTTPS, SSH, HTTP, TELNET, FMG-Access	●	● 1000Mbps/Full Duplex
vlink1	VDOM Link	root, ERP_Users				
vlink10	Pair	root	0.0.0.0 0.0.0.0		●	
vlink11	Pair	ERP_Users	0.0.0.0 0.0.0.0		●	
npu0-vlink	VDOM Link	root, root				

Configuring route for 10.128.0.0/23 (for root vdom) via vlink11 interface



IP/Mask	Gateway	Device	Comment
10.128.0.0 255.255.254.0	0.0.0.0	vlink11	

Configuring Firewall policies



Seq.#	Source	Destination	Schedule	Service	Authentication	Action	AV	Web Filter	Application Control	IPS	Log	NAT	Count
port5 - vlink11 (1 - 1)													
1	all	all	always	ALL		✓ Accept						⊗	0 Packets / 0 B
vlink11 - port5 (2 - 2)													
2	all	all	always	ALL		✓ Accept						⊗	7 Packets / 420 B
Implicit (3 - 3)	0.0.0.0 0.0.0.0												

Policies from vlink11 to port5 and vice-verse

Configuration on CLI

```
config global
config system vdom-link
    edit "vlink1"
        set type ppp
    next
end
```

config vdom

```
edit root
config system  interface
    edit "wan2"
        set vdom "root"
        set ip 10.128.0.196 255.255.252.0
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set explicit-web-proxy enable
        set snmp-index 6
    next
    edit "vlink10"
        set vdom "root"
        set type vdom-link
        set snmp-index 32
    next
    edit "vlink11"
        set vdom "ERP_Users"
        set type vdom-link
        set snmp-index 33
    next
end

config router static
    edit 3
        set device "vlink10"
        set dst 10.129.0.0 255.255.254.0
    next
end

config firewall policy

config firewall policy
    edit 1
        set srcintf "vlink10"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set srcintf "wan2"
        set dstintf "vlink10"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

On ERP_Users VDOM

```
config vdom

edit ERP_Users
config system interface
    edit "vlink11"
        set vdom "ERP_Users"
        set type vdom-link
        set snmp-index 33
    next
    edit "port5"
        set vdom "ERP_Users"
        set ip 10.129.0.196 255.255.252.0
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set snmp-index 10
    next
end


config router static
    edit 1
        set device "vlink11"
        set dst 10.128.0.0 255.255.254.0
    next
end


config firewall policy
    edit 1
        set srcintf "port5"
        set dstintf "vlink11"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set srcintf "vlink11"
        set dstintf "port5"
            set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Test Result:

Debug flow:

```
id=13 trace_id=60 func=print_pkt_detail line=4307 msg="vd-ERP_Users received a packet(proto=1, 10.129.0.67:1->10.128.0.196:8) from port5. code=8, type=0, id=1, seq=68."

id=13 trace_id=60 func=init_ip_session_common line=4463 msg="allocate a new session-000b88fc"

id=13 trace_id=60 func=vf_ip4_route_input line=1605 msg="find a route: flags=00000000 gw-10.128.0.196 via vlink11"

id=13 trace_id=60 func=__iprope_tree_check line=534 msg="use addr/intf hash, len=2"

id=13 trace_id=60 func=fw_forward_handler line=667 msg="Allowed by Policy-1:"
```

Sniffer output

```
diagnose sniffer packet any 'host 10.128.0.196 and icmp ' 4

interfaces=[any]

filters=[host 10.128.0.196 and icmp ]

5.659014 port5 in 10.129.0.67 -> 10.128.0.196: icmp: echo request
5.659078 vlink11 out 10.129.0.67 -> 10.128.0.196: icmp: echo request
5.659078 vlink10 in 10.129.0.67 -> 10.128.0.196: icmp: echo request
5.659138 vlink10 out 10.128.0.196 -> 10.129.0.67: icmp: echo reply
5.659138 vlink11 in 10.128.0.196 -> 10.129.0.67: icmp: echo reply
5.659169 port5 out 10.128.0.196 -> 10.129.0.67: icmp: echo reply
```