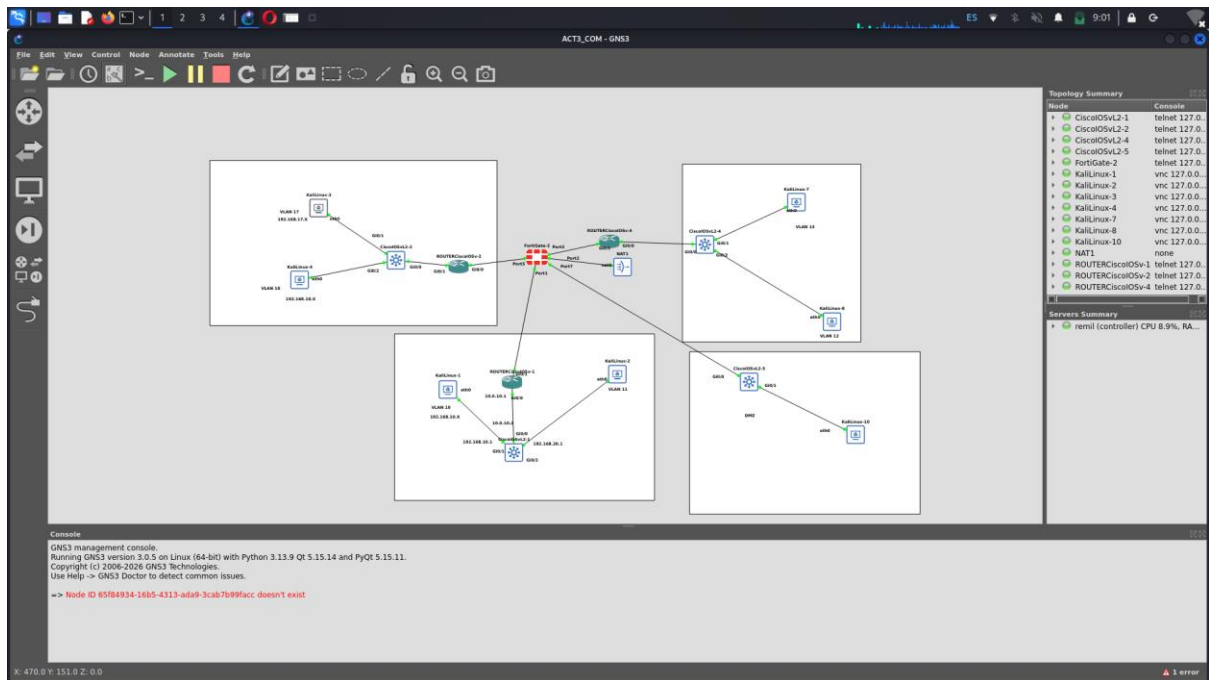


ACT3 – DMZ



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
DMZ_WAN	DMZ	WAN_TO_NAT1 (port2)	all	all	always	DNS HTTP HTTPS PING	ACCEPT	Enabled	no-inspection	All	0 B
DMZ_LAN	DMZ	LAN_BLOQUE4 (port3) LAN_BLOQUE3 (port4) LAN_BLOQUE2 (port5) LAN_BLOQUE1 (port1)	all	all	always	ALL	DENY	Disabled		Disabled	756 B
LAN1_DMZ	LAN_BLOQUE1 (port1) LAN_BLOQUE4 (port3) LAN_BLOQUE3 (port4) LAN_BLOQUE2 (port5)	DMZ	all	all	always	HTTP PING	ACCEPT	Disabled	no-inspection	All	13.93 kB
DENY_BLOQUE_TO_OTHER_LANS	LAN_BLOQUE1 (port1)	LAN_BLOQUE4 (port3) LAN_BLOQUE3 (port4) LAN_BLOQUE2 (port5)	all	all	always	ALL	DENY	Enabled		All	1.18 kB
	LAN_BLOQUE2 (port5)	LAN_BLOQUE1 (port1) LAN_BLOQUE4 (port3) LAN_BLOQUE3 (port4)	all	all	always	ALL	DENY	Enabled		All	168 B
	LAN_BLOQUE4 (port3)	LAN_BLOQUE1 (port1) LAN_BLOQUE3 (port4) LAN_BLOQUE2 (port5)	all	all	always	ALL	DENY	Enabled		All	0 B
WAN_TO_DMZ_HTTP	WAN_TO_NAT1 (port2)	DMZ	all	VIP_HTTP_DMZ	always	HTTP	ACCEPT	Disabled	no-inspection	All	13.13 kB
	LAN_BLOQUE1 (port1)	WAN_TO_NAT1 (port2)	all	all	always	PING DNS HTTP HTTPS	ACCEPT	Enabled	no-inspection	All	4.79 kB
	LAN_BLOQUE2 (port5)	WAN_TO_NAT1 (port2)	all	all	always	PING DNS HTTP HTTPS	ACCEPT	Enabled	no-inspection	All	2.02 kB
	LAN_BLOQUE4 (port3)	WAN_TO_NAT1 (port2)	all	all	always	PING DNS HTTP HTTPS	ACCEPT	Enabled	no-inspection	All	2.18 kB

<-- IMPORTANTE! YA NO EXISTE EL BOQUE DE ARRIBA PORQUE NECESITABA POLITICAS, YA ESTABA EN MAXIMO

FW:

config firewall policy

edit 12

set srcintf "port1" "port3" "port4" "port5"

set dstintf "DMZ"

set srcaddr "all"

set dstaddr "all"

set schedule "always"

set service "HTTP" "PING"

set nat disable

set logtraffic all

next

end

config firewall policy

edit 210

set name "DMZ_to_LAN_DENY"

set srcintf DMZ

set dstintf "port1" "port3" "port4" "port5"

set srcaddr "all"

set dstaddr "all"

set action deny

set schedule "always"

set service "ALL"

```
    set logtraffic all
next
end
```

```
config system interface
    edit "port7"
        set alias "DMZ"
        set ip 172.16.50.1/24
        set allowaccess ping
    next
end
```

```
config firewall vip
    edit "VIP_HTTP_DMZ"
        set extintf "port2"
        set extip <IP_PORT2_FORTI>
        set mappedip "172.16.50.10"
        set portforward enable
        set extport 80
        set mappedport 80
    next
end
```

```
config firewall policy
    edit 300
        set name "WAN_to_DMZ_HTTP"
        set srcintf "port2"
```

```
set dstintf "DMZ"  
set srcaddr "all"  
set dstaddr "VIP_HTTP_DMZ"  
set action accept  
set schedule "always"  
set service "HTTP"  
set nat disable  
set logtraffic all  
next  
end
```

SW:

```
enable
```

```
conf t
```

```
vlan 50
```

```
name DMZ
```

```
exit
```

```
interface gi0/0
```

```
description TO_FORTI_port7
```

```
switchport mode access
```

```
switchport access vlan 50
```

```
no shutdown
```

exit

interface gi0/1

description DMZ_PC

switchport mode access

switchport access vlan 50

no shutdown

exit

end

wr