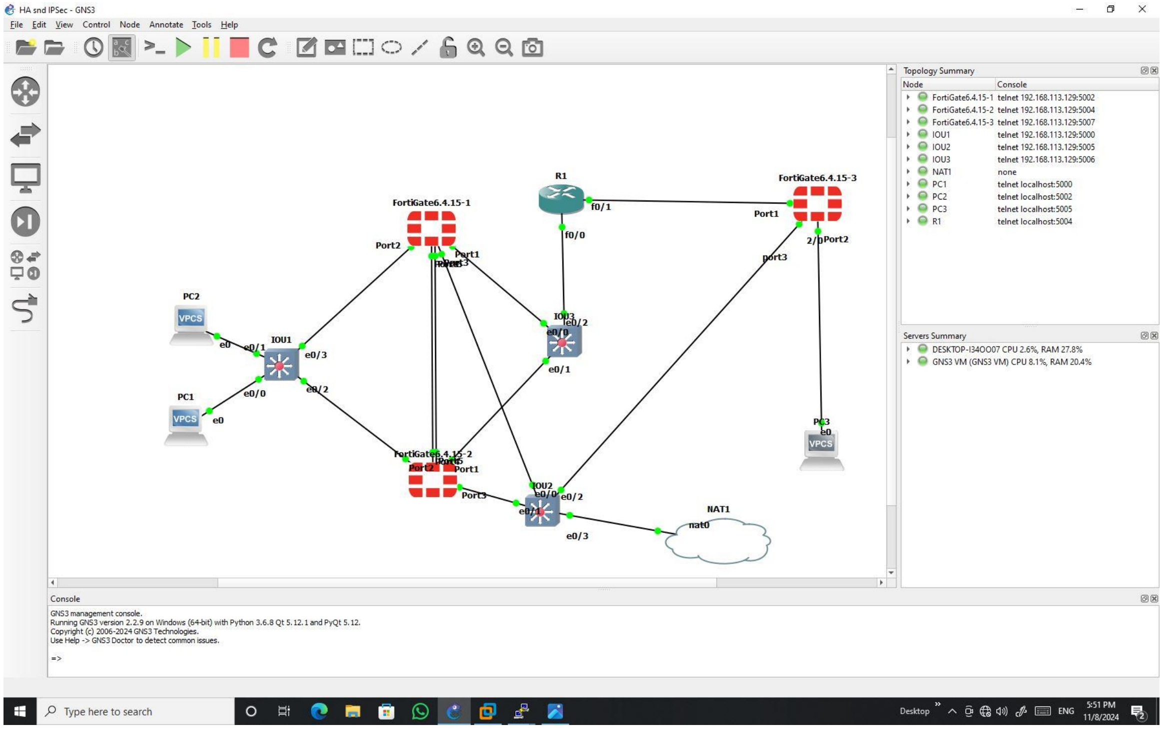
HA Task

Topology:



Topology Summary

Node	Console
FortiGate6.4.15-1	telnet 192.168.113.129:5002
FortiGate6.4.15-2	telnet 192.168.113.129:5004
FortiGate6.4.15-3	telnet 192.168.113.129:5007
IOU1	telnet 192.168.113.129:5000
IOU2	telnet 192.168.113.129:5005
IOU3	telnet 192.168.113.129:5006
NAT1	none
PC1	telnet localhost:5000
PC2	telnet localhost:5002
PC3	telnet localhost:5005
R1	telnet localhost:5004

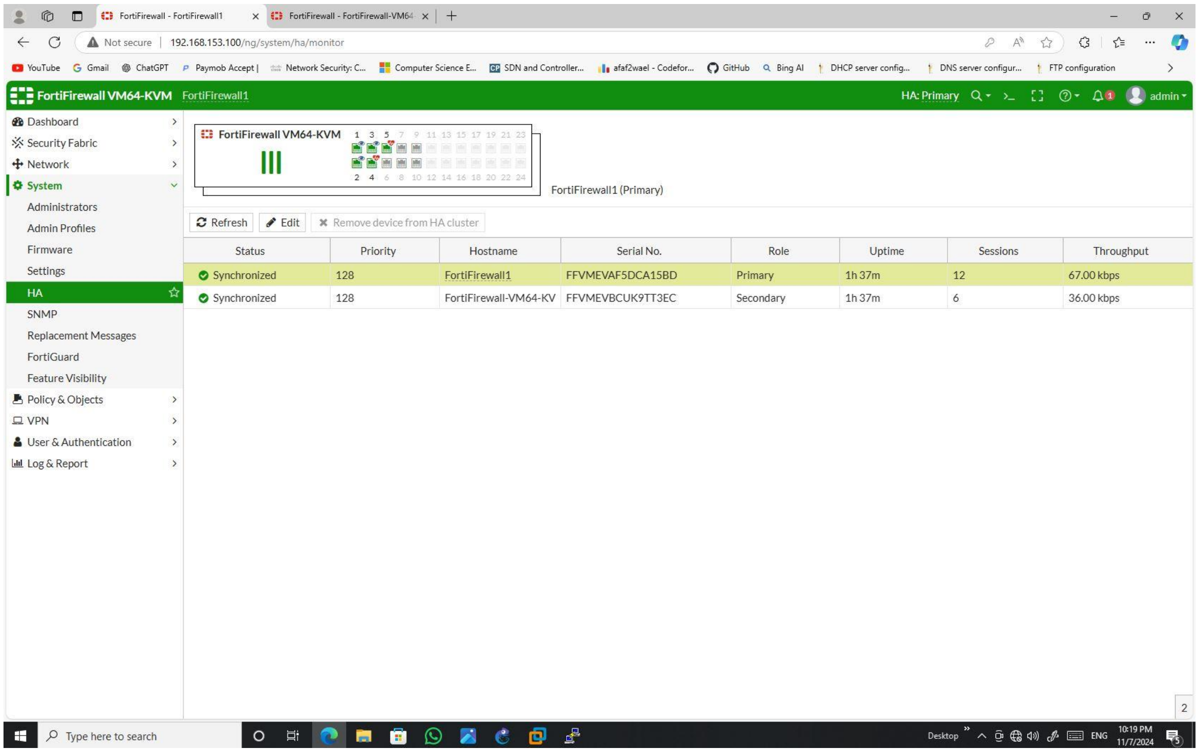
Servers Summary

- DESKTOP-I34OO07 CPU 2.6%, RAM 27.8%
- GNS3 VM (GNS3 VM) CPU 8.1%, RAM 20.4%

Console

```
GNS3 management console.
Running GNS3 version 2.2.9 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2024 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Primary & Secondary HA:

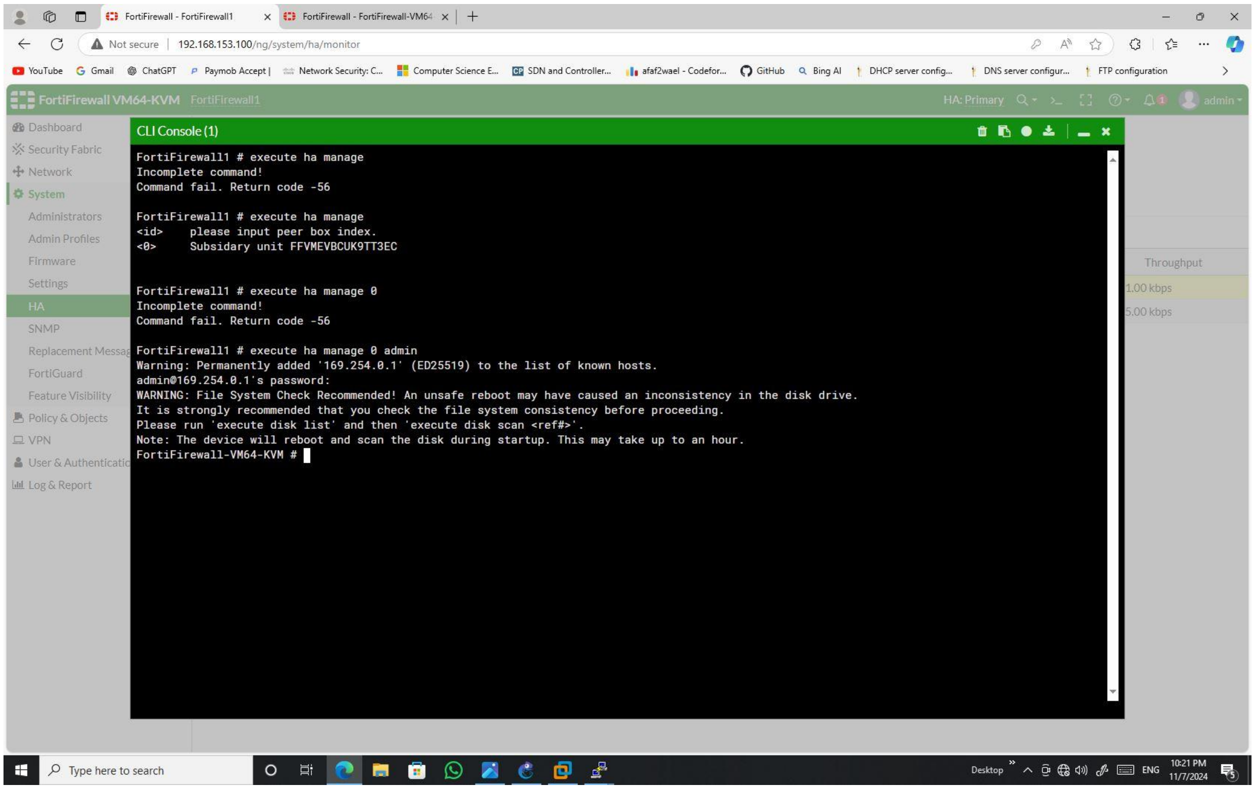


192.168.153.100/ng/system/ha/monitor

FortiFirewall1 (Primary)

Status	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
✓ Synchronized	128	FortiFirewall1	FFVMEVAF5DCA15BD	Primary	1h 37m	12	67.00 kbps
✓ Synchronized	128	FortiFirewall-VM64-KV	FFVMEVBCUK9TT3EC	Secondary	1h 37m	6	36.00 kbps

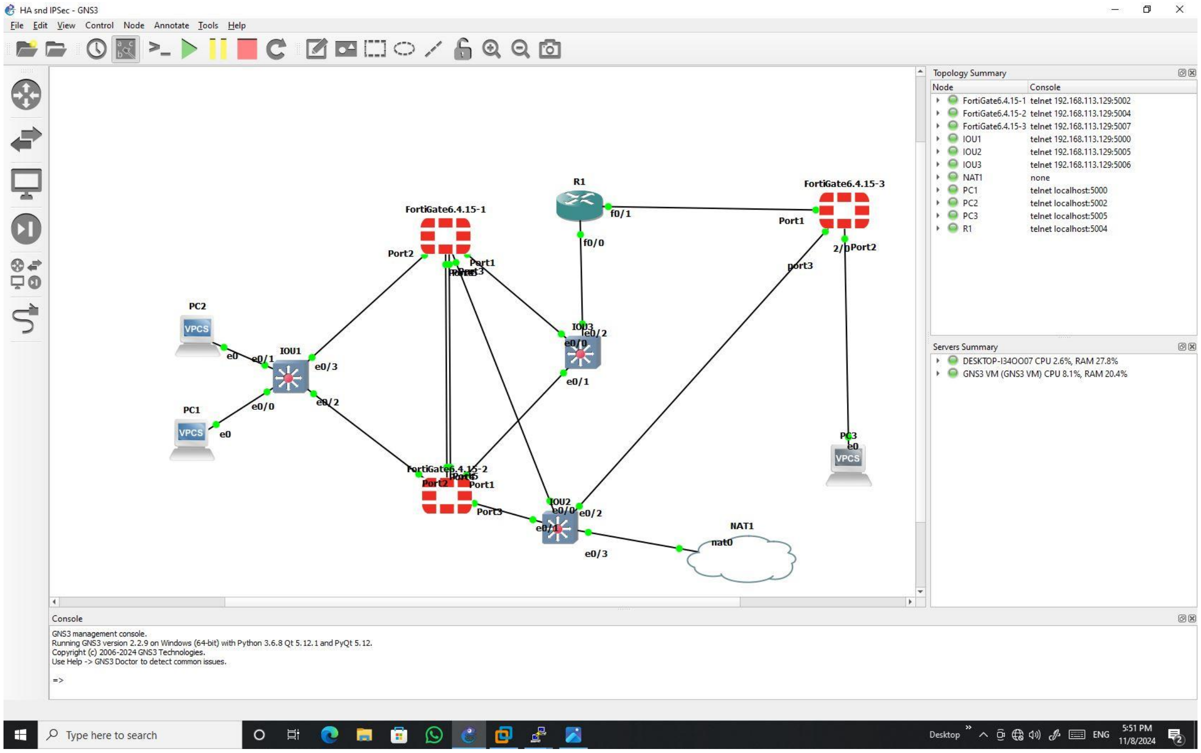
Connect to Secondary with CLI:



```
FortiFirewall1 # execute ha manage
Incomplete command!
Command fail. Return code -56

FortiFirewall1 # execute ha manage
<id>    please input peer box index.
<0>     Subsidary unit FFVMEVBCUK9TT3EC


FortiFirewall1 # execute ha manage 0
Incomplete command!
Command fail. Return code -56

FortiFirewall1 # execute ha manage 0 admin
Warning: Permanently added '169.254.0.1' (ED25519) to the list of known hosts.
admin@169.254.0.1's password:
WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiFirewall-VM64-KVM #
```

IPSec Task

Topology:



Topology Summary

Node	Console
FortiGate6.4.15-1	telnet 192.168.113.129:5002
FortiGate6.4.15-2	telnet 192.168.113.129:5004
FortiGate6.4.15-3	telnet 192.168.113.129:5007
IOU1	telnet 192.168.113.129:5000
IOU2	telnet 192.168.113.129:5005
IOU3	telnet 192.168.113.129:5006
NAT1	none
PC1	telnet localhost:5000
PC2	telnet localhost:5002
PC3	telnet localhost:5005
R1	telnet localhost:5004

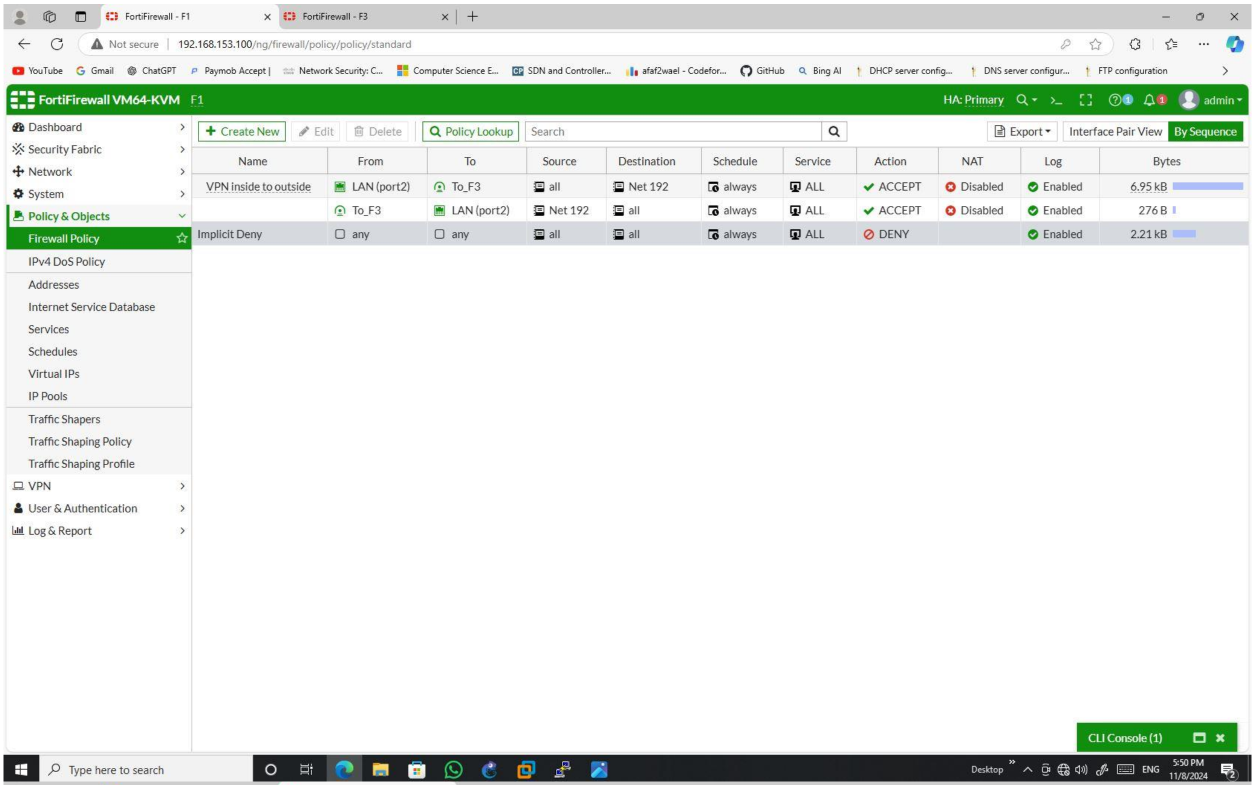
Servers Summary

DESKTOP-I34OO07 CPU 2.6%, RAM 27.8%
GNS3 VM (GNS3 VM) CPU 8.1%, RAM 20.4%

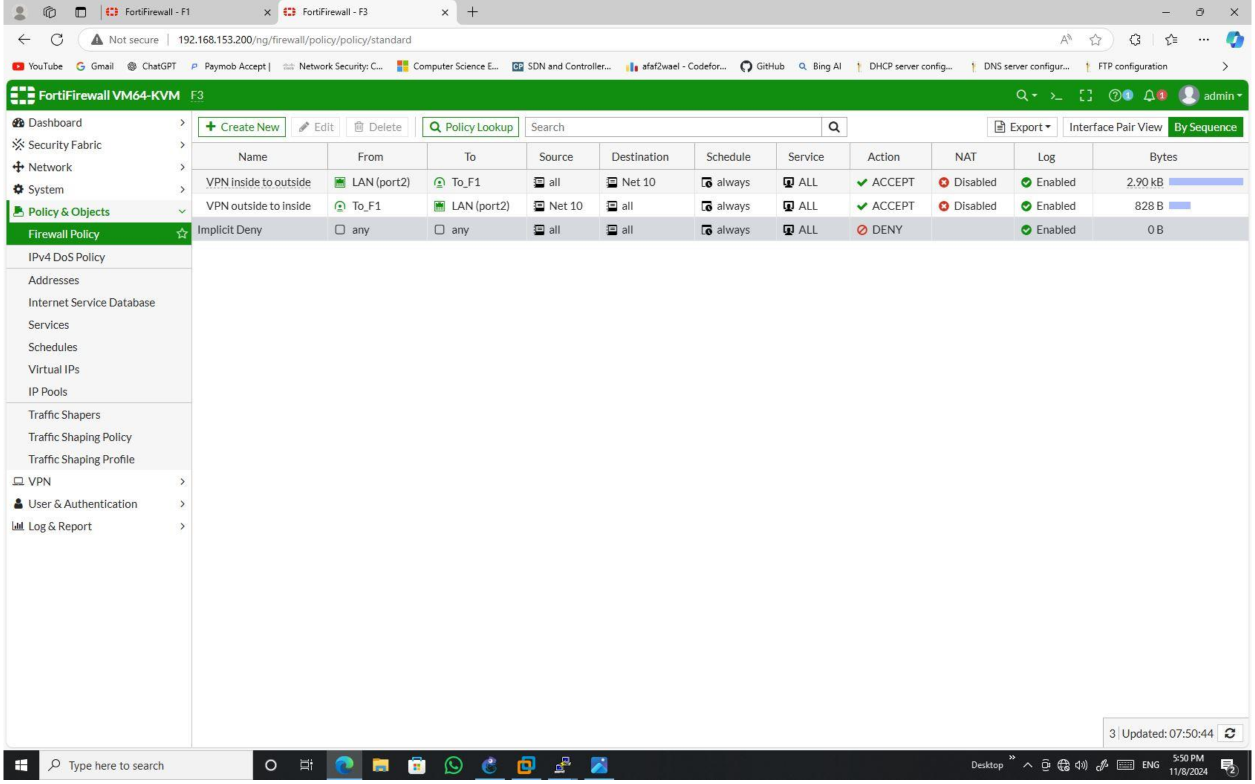
Console

```
GNS3 management console.
Running GNS3 version 2.2.9 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2024 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Firewall Policies on both devices:

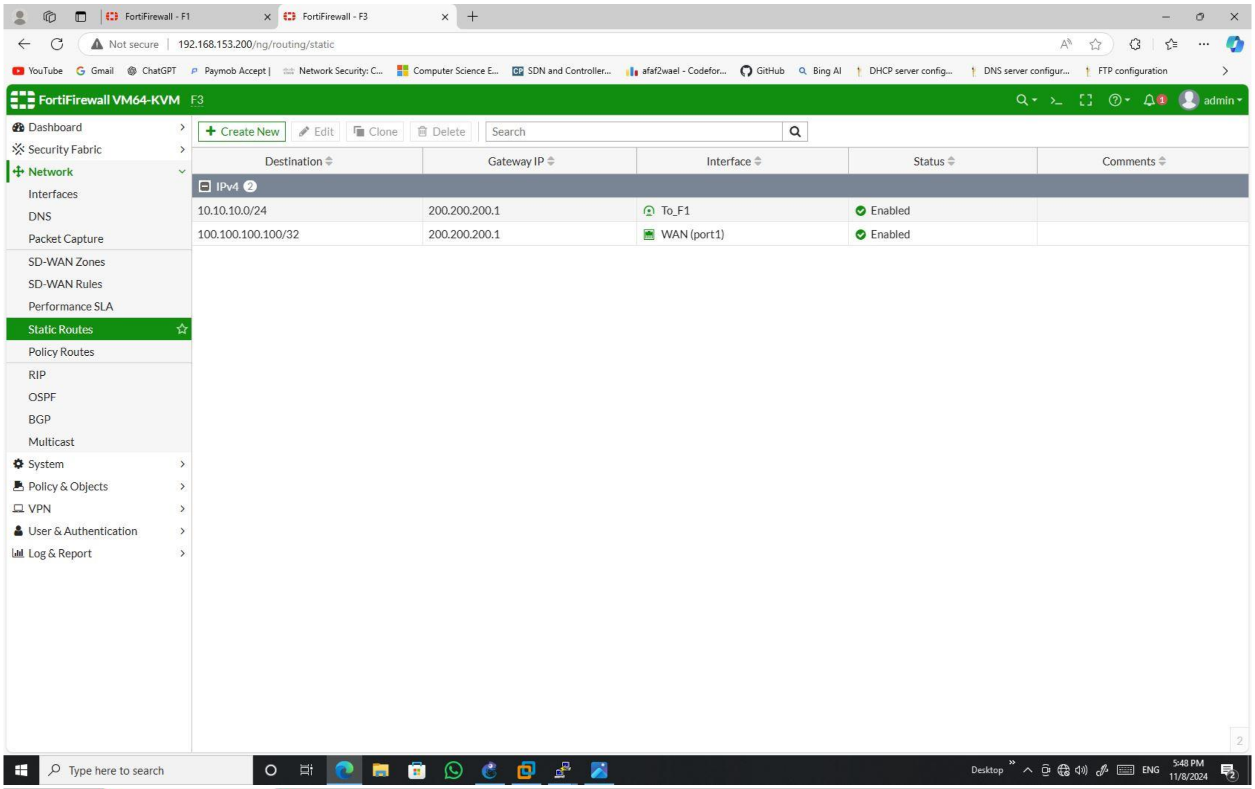


Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Log	Bytes
VPN inside to outside	LAN (port2)	To_F3	all	Net 192	always	ALL	✓ ACCEPT	Disabled	Enabled	6.95 kB
	To_F3	LAN (port2)	Net 192	all	always	ALL	✓ ACCEPT	Disabled	Enabled	276 B
Implicit Deny	any	any	all	all	always	ALL	DENY		Enabled	2.21 kB



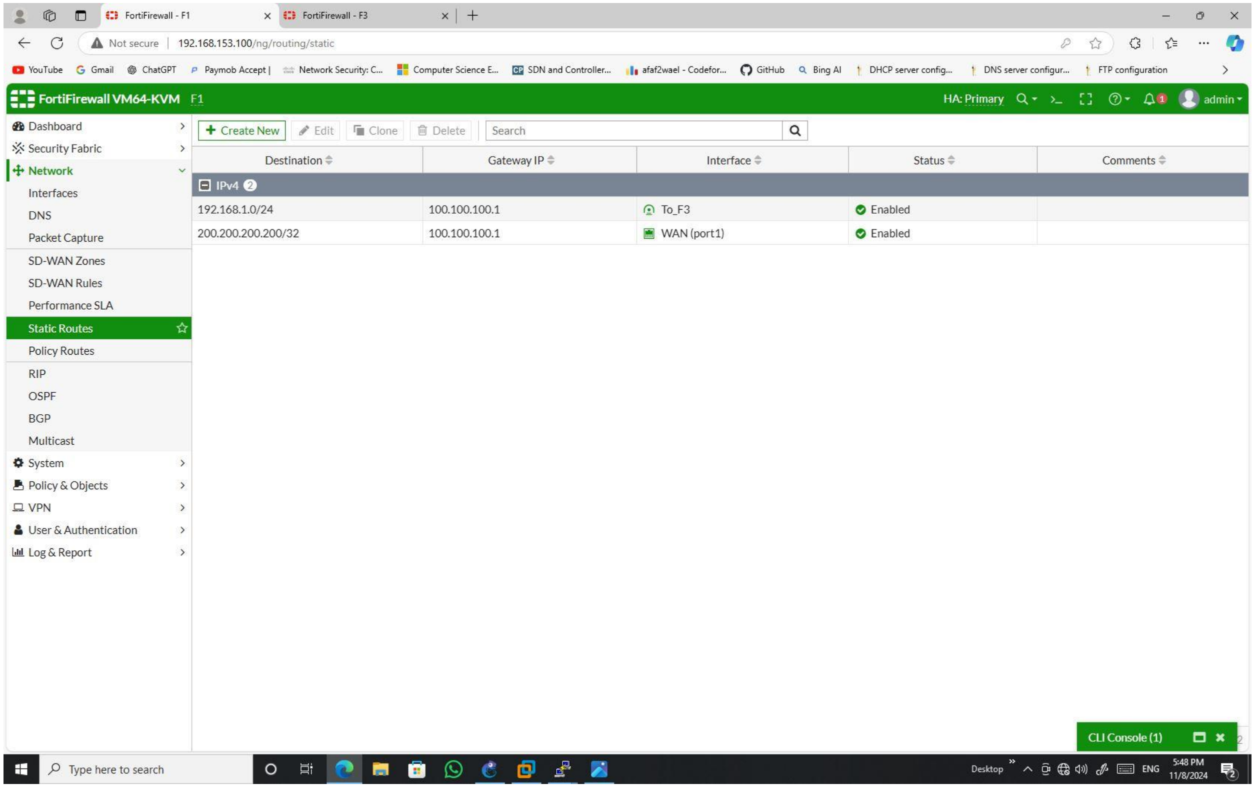
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Log	Bytes
VPN inside to outside	LAN (port2)	To_F1	all	Net 10	always	ALL	✓ ACCEPT	Disabled	Enabled	2.90 kB
VPN outside to inside	To_F1	LAN (port2)	Net 10	all	always	ALL	✓ ACCEPT	Disabled	Enabled	828 B
Implicit Deny	any	any	all	all	always	ALL	DENY		Enabled	0 B

Static routes on both devices:



IPv4 2

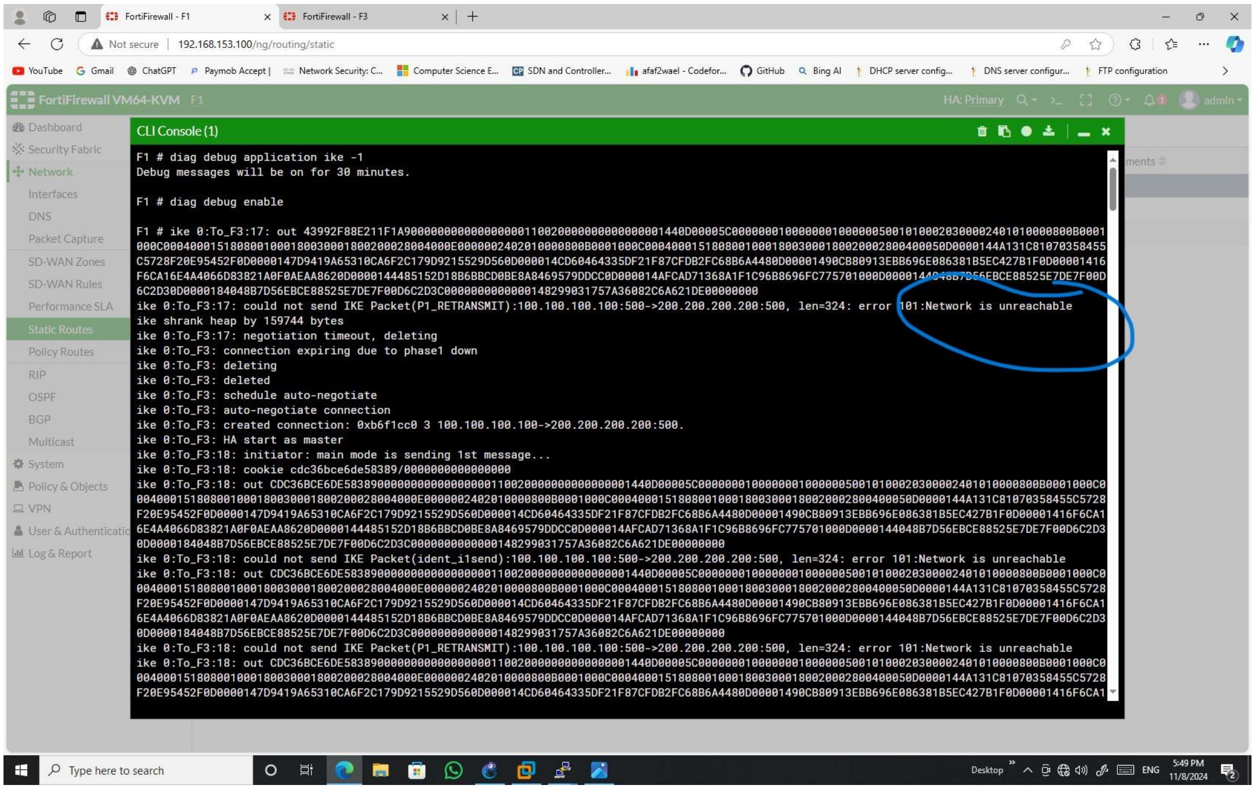
Destination	Gateway IP	Interface	Status	Comments
10.10.10.0/24	200.200.200.1	To_F1	Enabled	
100.100.100.100/32	200.200.200.1	WAN (port1)	Enabled	



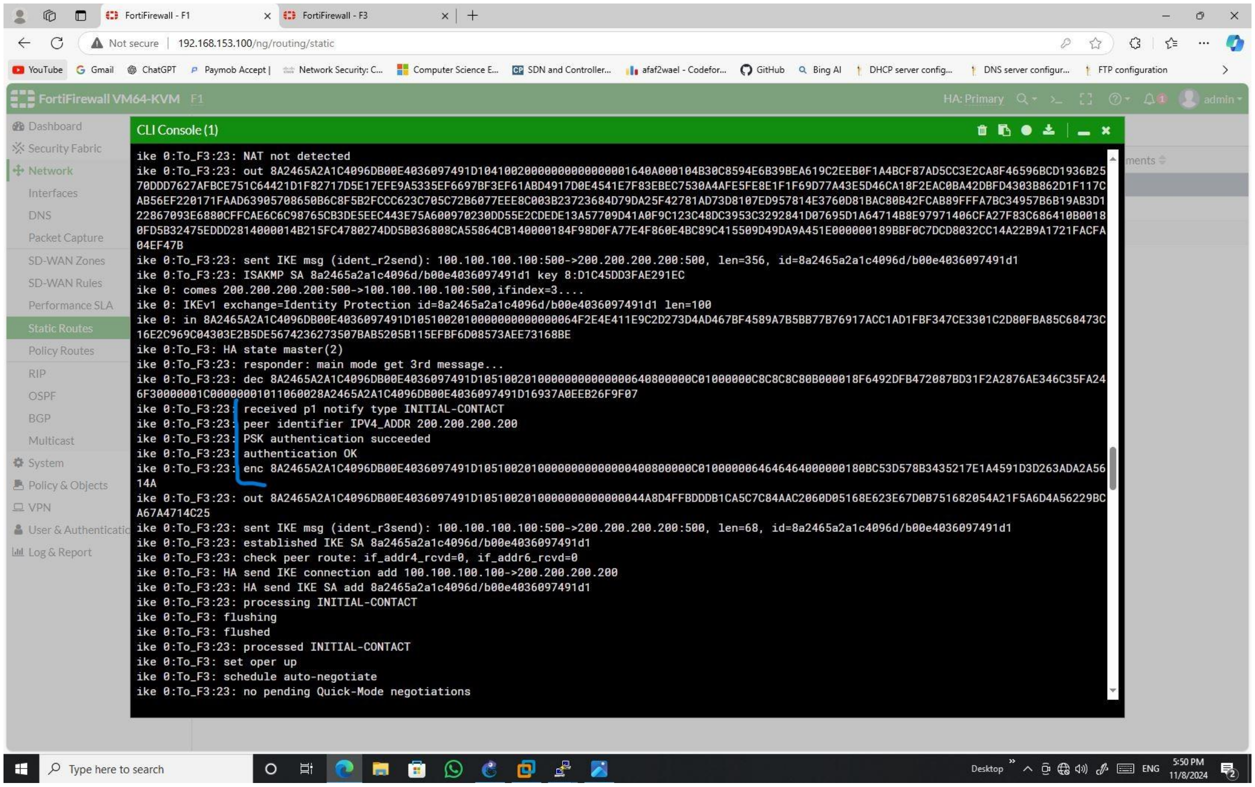
IPv4 2

Destination	Gateway IP	Interface	Status	Comments
192.168.1.0/24	100.100.100.1	To_F3	Enabled	
200.200.200.200/32	100.100.100.1	WAN (port1)	Enabled	

Some Troublshooting:

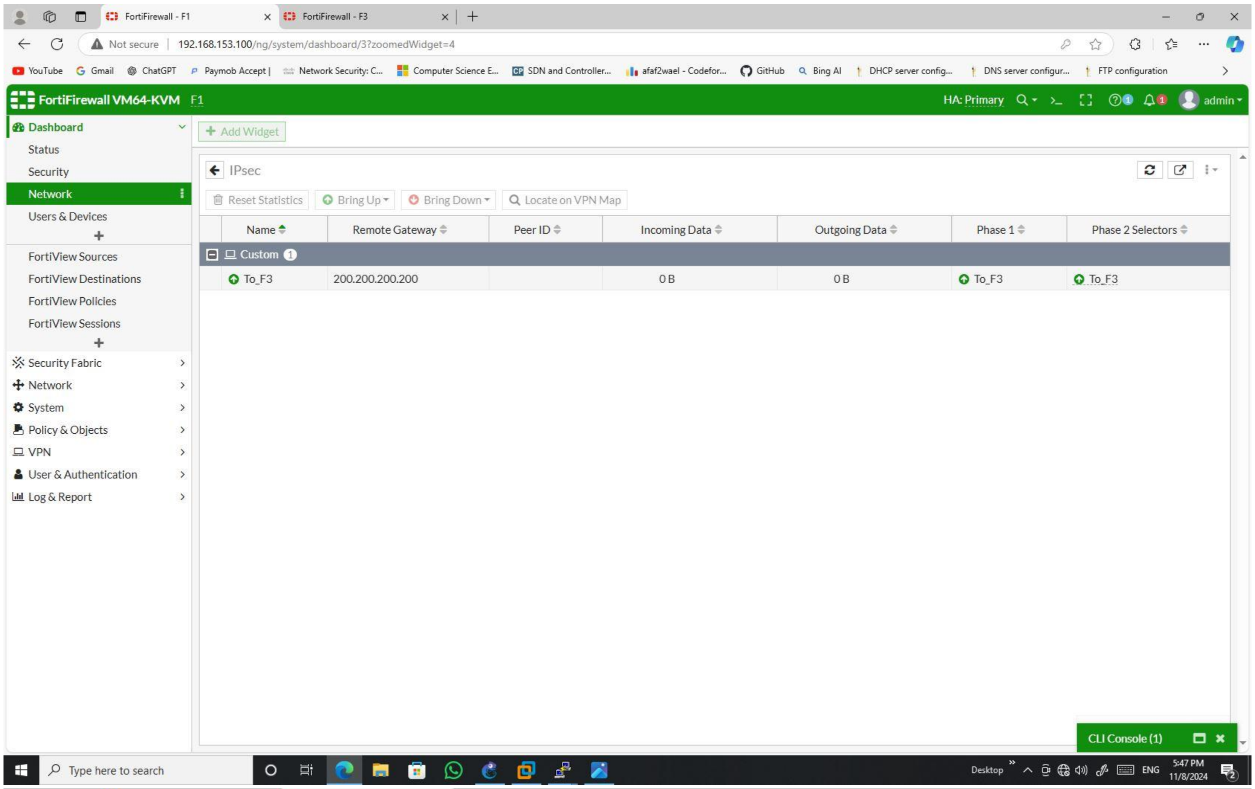


```
F1 # diag debug application ike -1
Debug messages will be on for 30 minutes.

F1 # diag debug enable

F1 # ike 0:To_F3:17: out 43992F88E211F1A900000000000000000110020000000000000001440D00005C00000001000000010000005001010002030000240101000800B0001
000C00040001518080010001800300018002000280040000E0000002402010000800B0001000C00040001518080010001800300018002000280040050D0000144A131C81070358455
C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416
F6CA16E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D
6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3C0000000000000148299031757A36082C6A621DE00000000
ike 0:To_F3:17: could not send IKE Packet(P1_RETRANSMIT):100.100.100.100:500->200.200.200.200:500, len=324: error 101:Network is unreachable
ike shrank heap by 159744 bytes
ike 0:To_F3:17: negotiation timeout, deleting
ike 0:To_F3: connection expiring due to phase1 down
ike 0:To_F3: deleting
ike 0:To_F3: deleted
ike 0:To_F3: schedule auto-negotiate
ike 0:To_F3: auto-negotiate connection
ike 0:To_F3: created connection: 0xb6f1cc0 3 100.100.100.100->200.200.200.200:500.
ike 0:To_F3: HA start as master
ike 0:To_F3:18: initiator: main mode is sending 1st message...
ike 0:To_F3:18: cookie cdc36bce6de58389/0000000000000000
ike 0:To_F3:18: out CDC36BCE6DE58389000000000000000001100200000000000000001440D00005C00000001000000010000005001010002030000240101000800B0001000C0
0040001518080010001800300018002000280040000E0000002402010000800B0001000C00040001518080010001800300018002000280040050D0000144A131C81070358455C5728
F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA1
6E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D3
0D0000184048B7D56EBCE88525E7DE7F00D6C2D3C0000000000000148299031757A36082C6A621DE00000000
ike 0:To_F3:18: could not send IKE Packet(ident_i1send):100.100.100.100:500->200.200.200.200:500, len=324: error 101:Network is unreachable
ike 0:To_F3:18: out CDC36BCE6DE58389000000000000000001100200000000000000001440D00005C00000001000000010000005001010002030000240101000800B0001000C0
0040001518080010001800300018002000280040000E0000002402010000800B0001000C00040001518080010001800300018002000280040050D0000144A131C81070358455C5728
F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA1
6E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D3
0D0000184048B7D56EBCE88525E7DE7F00D6C2D3C0000000000000148299031757A36082C6A621DE00000000
ike 0:To_F3:18: could not send IKE Packet(P1_RETRANSMIT):100.100.100.100:500->200.200.200.200:500, len=324: error 101:Network is unreachable
ike 0:To_F3:18: out CDC36BCE6DE58389000000000000000001100200000000000000001440D00005C00000001000000010000005001010002030000240101000800B0001000C0
0040001518080010001800300018002000280040000E0000002402010000800B0001000C00040001518080010001800300018002000280040050D0000144A131C81070358455C5728
F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA1
```

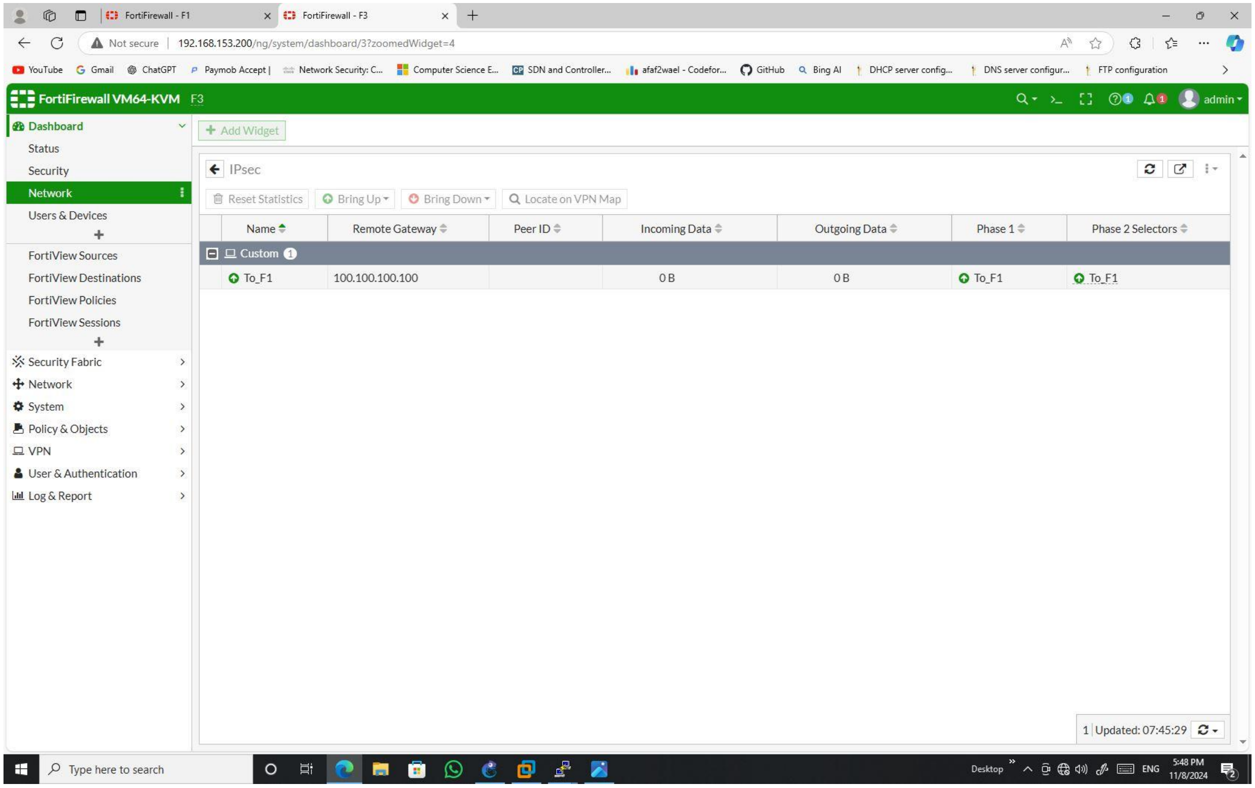


```
ike 0:To_F3:23: NAT not detected
ike 0:To_F3:23: out 8A2465A2A1C4096DB00E4036097491D1041002000000000000000001640A000104B30C8594E6B39BEA619C2EEB0F1A4BCF87AD5CC3E2CA8F46596BCD1936B25
70DDD7627AFBCE751C64421D1F82717D5E17EFE9A5335EF6697BF3EF61ABD4917D0E4541E7F83EBEC7530A4AFE5FE8E1F1F69D77A43E5D46CA18F2EAC0BA42DBFD4303B862D1F117C
AB56EF220171FAAD6390570865 0B6C8F5B2FCCC623C705C72B6077EEE8C003B23723684D79DA25F42781AD73D8107ED957814E3760D81BAC80B42FCAB89FFFA7BC34957B6B19AB3D1
22867093E6880CFFCAE6C6C98765CB3DE5EEC443E75A600970230DD55E2CDEDE13A57709D41A0F9C123C48DC3953C3292841D07695D1A64714B8E97971406CFA27F83C686410B0018
0FD5B32475EDDD2814000014B215FC4780274DD5B036808CA55864CB140000184F98D0FA77E4F860E4BC89C415509D49DA9A451E000000189BBF0C7DCD8032CC14A22B9A1721FACFA
04EF47B
ike 0:To_F3:23: sent IKE msg (ident_r2send): 100.100.100.100:500->200.200.200.200:500, len=356, id=8a2465a2a1c4096d/b00e4036097491d1
ike 0:To_F3:23: ISAKMP SA 8a2465a2a1c4096d/b00e4036097491d1 key 8:D1C45DD3FAE291EC
ike 0: comes 200.200.200.200:500->100.100.100.100:500,ifindex=3....
ike 0: IKEv1 exchange=Identity Protection id=8a2465a2a1c4096d/b00e4036097491d1 len=100
ike 0: in 8A2465A2A1C4096DB00E4036097491D10510020100000000000000064F2E4E411E9C2D273D4AD467BF4589A7B5BB77B76917ACC1AD1FBF347CE3301C2D80FBA85C68473C
16E2C969C04303E2B5DE5674236273507BAB5205B115EFBF6D08573AEE73168BE
ike 0:To_F3: HA state master(2)
ike 0:To_F3:23: responder: main mode get 3rd message...
ike 0:To_F3:23: dec 8A2465A2A1C4096DB00E4036097491D1051002010000000000000000640800000C01000000C8C8C8C80B000018F6492DFB472087BD31F2A2876AE346C35FA24
6F30000001C000000001011060028A2465A2A1C4096DB00E4036097491D16937A0EEB26F9F07
ike 0:To_F3:23: received p1 notify type INITIAL-CONTACT
ike 0:To_F3:23: peer identifier IPV4_ADDR 200.200.200.200
ike 0:To_F3:23: PSK authentication succeeded
ike 0:To_F3:23: authentication OK
ike 0:To_F3:23: enc 8A2465A2A1C4096DB00E4036097491D1051002010000000000000000400800000C010000006464646400000180BC53D578B3435217E1A4591D3D263ADA2A56
14A
ike 0:To_F3:23: out 8A2465A2A1C4096DB00E4036097491D10510020100000000000000044A8D4FFBDDDB1CA5C7C84AAC2060D05168E623E67D0B751682054A21F5A6D4A56229BC
A67A4714C25
ike 0:To_F3:23: sent IKE msg (ident_r3send): 100.100.100.100:500->200.200.200.200:500, len=68, id=8a2465a2a1c4096d/b00e4036097491d1
ike 0:To_F3:23: established IKE SA 8a2465a2a1c4096d/b00e4036097491d1
ike 0:To_F3:23: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0
ike 0:To_F3: HA send IKE connection add 100.100.100.100->200.200.200.200
ike 0:To_F3:23: HA send IKE SA add 8a2465a2a1c4096d/b00e4036097491d1
ike 0:To_F3:23: processing INITIAL-CONTACT
ike 0:To_F3: flushing
ike 0:To_F3: flushed
ike 0:To_F3:23: processed INITIAL-CONTACT
ike 0:To_F3: set oper up
ike 0:To_F3: schedule auto-negotiate
ike 0:To_F3:23: no pending Quick-Mode negotiations
```

IPSec established on both devices:

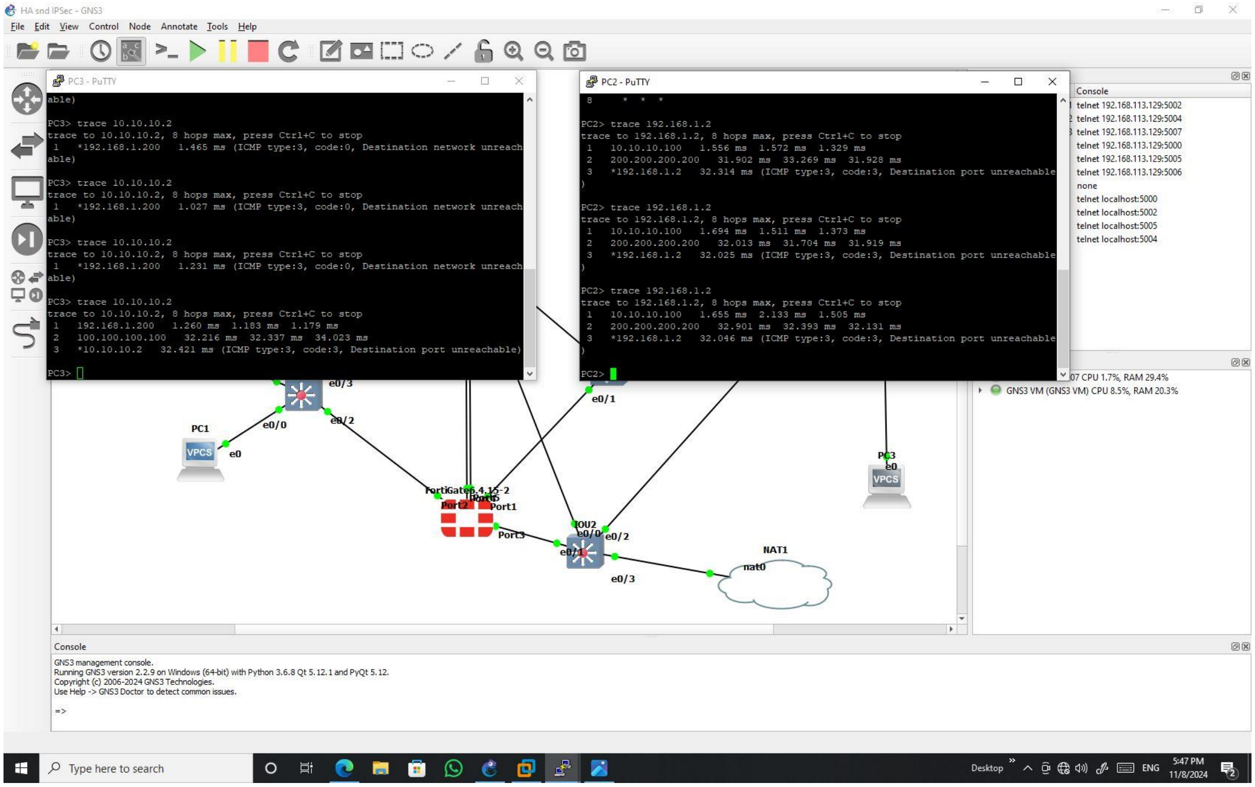


Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
To_F3	200.200.200.200		0 B	0 B	To_F3	To_F3



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
To_F1	100.100.100.100		0 B	0 B	To_F1	To_F1

Ping is allowed between both networks:



```
able)

PC3> trace 10.10.10.2
trace to 10.10.10.2, 8 hops max, press Ctrl+C to stop
 1   *192.168.1.200   1.465 ms (ICMP type:3, code:0, Destination network unreach
able)

PC3> trace 10.10.10.2
trace to 10.10.10.2, 8 hops max, press Ctrl+C to stop
 1   *192.168.1.200   1.027 ms (ICMP type:3, code:0, Destination network unreach
able)

PC3> trace 10.10.10.2
trace to 10.10.10.2, 8 hops max, press Ctrl+C to stop
 1   *192.168.1.200   1.231 ms (ICMP type:3, code:0, Destination network unreach
able)

PC3> trace 10.10.10.2
trace to 10.10.10.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.200   1.260 ms  1.183 ms  1.179 ms
 2   100.100.100.100   32.216 ms  32.337 ms  34.023 ms
 3   *10.10.10.2   32.421 ms (ICMP type:3, code:3, Destination port unreachable)

PC3> 
```

```
 8     *  *  *

PC2> trace 192.168.1.2
trace to 192.168.1.2, 8 hops max, press Ctrl+C to stop
 1   10.10.10.100   1.556 ms  1.572 ms  1.329 ms
 2   200.200.200.200   31.902 ms  33.269 ms  31.928 ms
 3   *192.168.1.2   32.314 ms (ICMP type:3, code:3, Destination port unreachable
)

PC2> trace 192.168.1.2
trace to 192.168.1.2, 8 hops max, press Ctrl+C to stop
 1   10.10.10.100   1.694 ms  1.511 ms  1.373 ms
 2   200.200.200.200   32.013 ms  31.704 ms  31.919 ms
 3   *192.168.1.2   32.025 ms (ICMP type:3, code:3, Destination port unreachable
)

PC2> trace 192.168.1.2
trace to 192.168.1.2, 8 hops max, press Ctrl+C to stop
 1   10.10.10.100   1.655 ms  2.133 ms  1.505 ms
 2   200.200.200.200   32.901 ms  32.393 ms  32.131 ms
 3   *192.168.1.2   32.046 ms (ICMP type:3, code:3, Destination port unreachable
)

PC2> 
```

Console

```
telnet 192.168.113.129:5002
telnet 192.168.113.129:5004
telnet 192.168.113.129:5007
telnet 192.168.113.129:5000
telnet 192.168.113.129:5005
telnet 192.168.113.129:5006
none
telnet localhost:5000
telnet localhost:5002
telnet localhost:5005
telnet localhost:5004
```

Console

```
GNS3 management console.
Running GNS3 version 2.2.9 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2024 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```