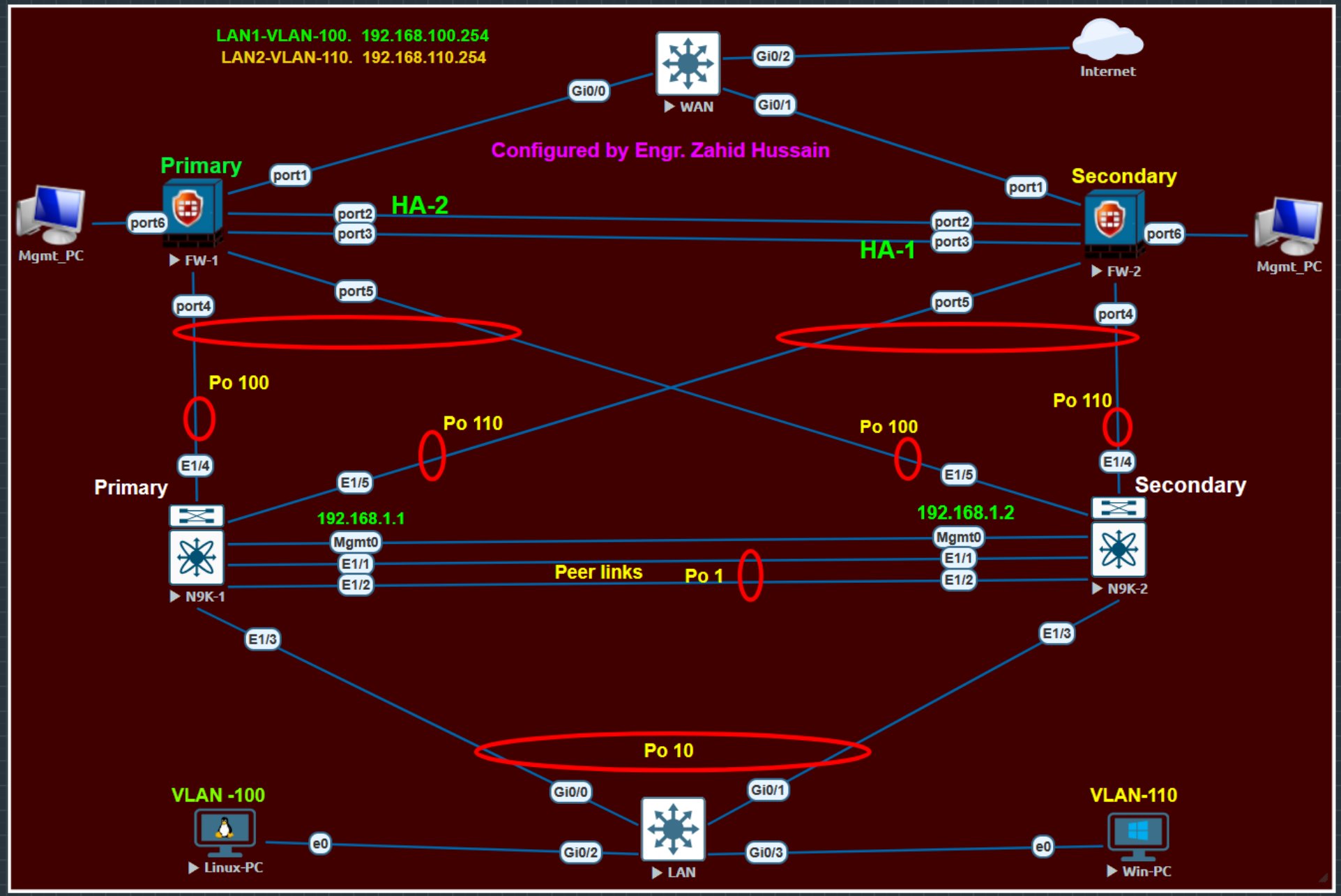
# FortiGate Project

I have configured High Availability (HA) on FortiGate with two firewalls and established fully redundant back links using two Nexus 9000 switches.




Notifications

N9K-1

```
Primary# show running-config

!Command: show running-config
!Running configuration last done at: Thu Jun 12 12:38:50 2025
!Time: Thu Jun 12 12:42:27 2025

version 9.3(1) Bios:version
hostname Primary
vdc Primary id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute
feature lacp
feature vpc

no password strength-check
username admin password 5 $5$39CUYLoV$Dj4XCrVv6aDa47.dRdE1X85oH0TRINovtdCBqdtKgm
5  role network-admin
username zahid password 5 $5$nxbknpcG$qm/58/GIM.0v8M2s/1pFgJbtEJoiULlQU5olQr/NCP
B  role network-operator
username zahid passphrase  lifetime 99999 warntime 14 gracetime 3
```

```
vlan 1,100,110

vrf context management
vpc domain 1
  role priority 20
  peer-keepalive destination 192.168.1.2 source 192.168.1.1

interface port-channel1
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  vpc peer-link

interface port-channel10
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 10

interface port-channel100
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 100

interface port-channel110
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 110
```

```
interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  channel-group 1 mode active

interface Ethernet1/2
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  channel-group 1 mode active

interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 10 mode active

interface Ethernet1/4
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 100 mode active

interface Ethernet1/5
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 110 mode active
```

N9K-2

```
Secondary# show running-config

!Command: show running-config
!No configuration change since last restart
!Time: Thu Jun 12 12:31:19 2025

version 9.3(1) Bios:version
hostname Secondary
vdc Secondary id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute
feature lacp
feature vpc
```

```
vlan 1,100,110

vrf context management
vpc domain 1
  role priority 30
  peer-keepalive destination 192.168.1.1 source 192.168.1.2

interface port-channel1
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  vpc peer-link

interface port-channel10
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 10

interface port-channel100
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 100

interface port-channel110
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  vpc 110
```

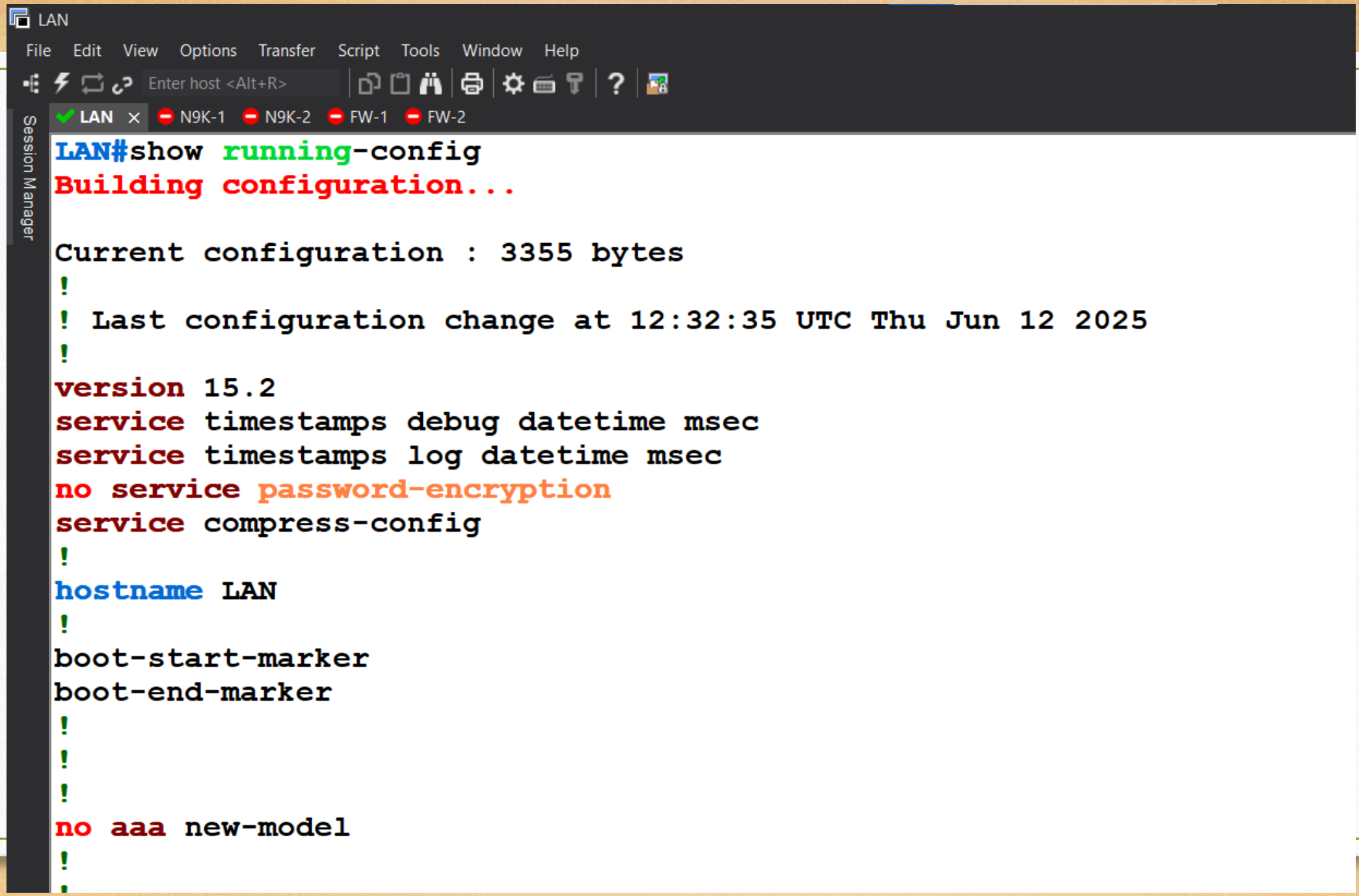
Enter host <Alt+R>

LAN | N9K-1 | N9K-2 | FW-1 | FW-2

Session Manager

```
interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  channel-group 1 mode active

interface Ethernet1/2
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  spanning-tree port type network
  channel-group 1 mode active

interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 10 mode active

interface Ethernet1/4
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 110 mode active

interface Ethernet1/5
  switchport mode trunk
  switchport trunk allowed vlan 100,110
  channel-group 100 mode active
```

```
Primary# show running-config interface mgmt 0

!Command: show running-config interface mgmt0
!Running configuration last done at: Thu Jun 12 11:02:31 2025
!Time: Thu Jun 12 11:05:47 2025

version 9.3(1) Bios:version

interface mgmt0
  vrf member management
  ip address 192.168.1.1/24

Primary# copy running-config startup-config
[####################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
Primary# ping 192.168.1.2 vrf management
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=5.367 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=3.621 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=6.58 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=6.22 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=3.673 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.621/5.092/6.58 ms
Primary#
```


LAN
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
Session Manager
LAN
N9K-1
N9K-2
FW-1
FW-2
LAN#show running-config
Building configuration...
Current configuration : 3355 bytes
!
! Last configuration change at 12:32:35 UTC Thu Jun 12 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname LAN
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!

# LAN side Internal Switch Config

Enter host <Alt+R>

LAN | N9K-1 | N9K-2 | FW-1 | FW-2

```
interface Port-channel10
 switchport trunk allowed vlan 100,110
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 100,110
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-protocol lacp
 channel-group 10 mode active
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 100,110
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-protocol lacp
 channel-group 10 mode active
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
 negotiation auto
!
interface GigabitEthernet0/3
 switchport access vlan 110
 switchport mode access
```

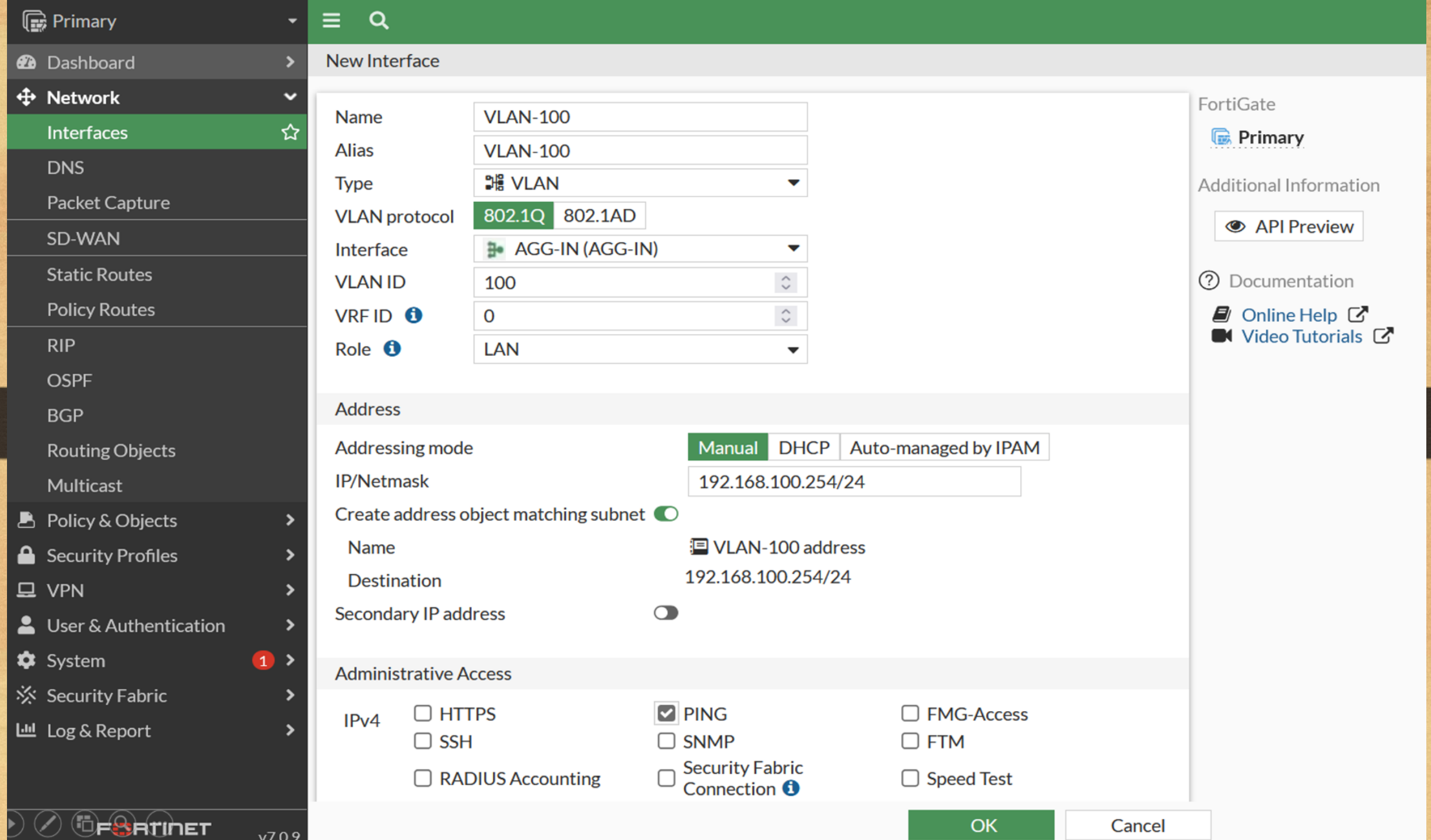
FW-1

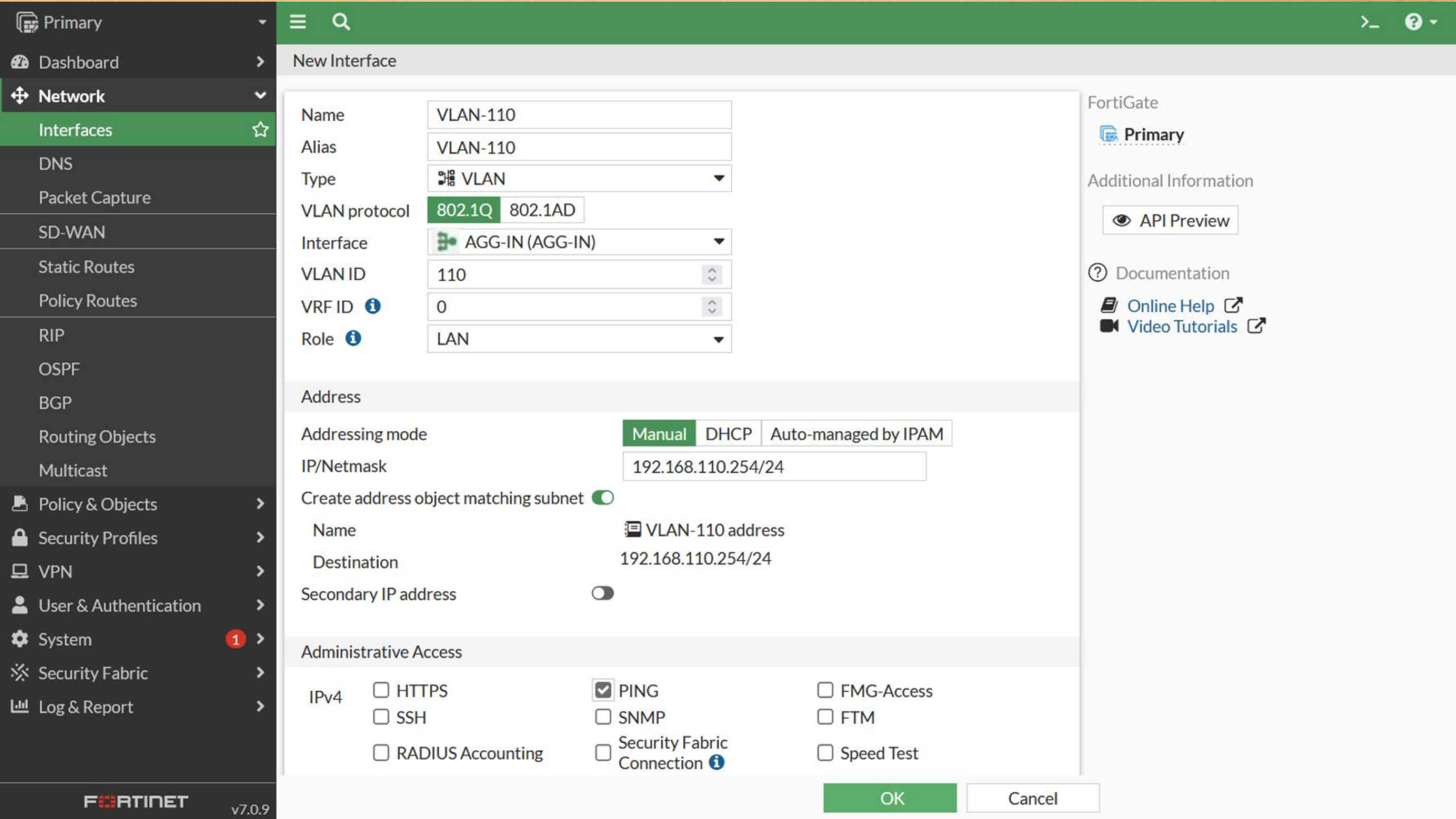
```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port6

FortiGate-VM64-KVM (port6) # set ip 192.168.79.100/24

FortiGate-VM64-KVM (port6) # set allowaccess https http ssh ping

FortiGate-VM64-KVM (port6) # end

Primary #
```

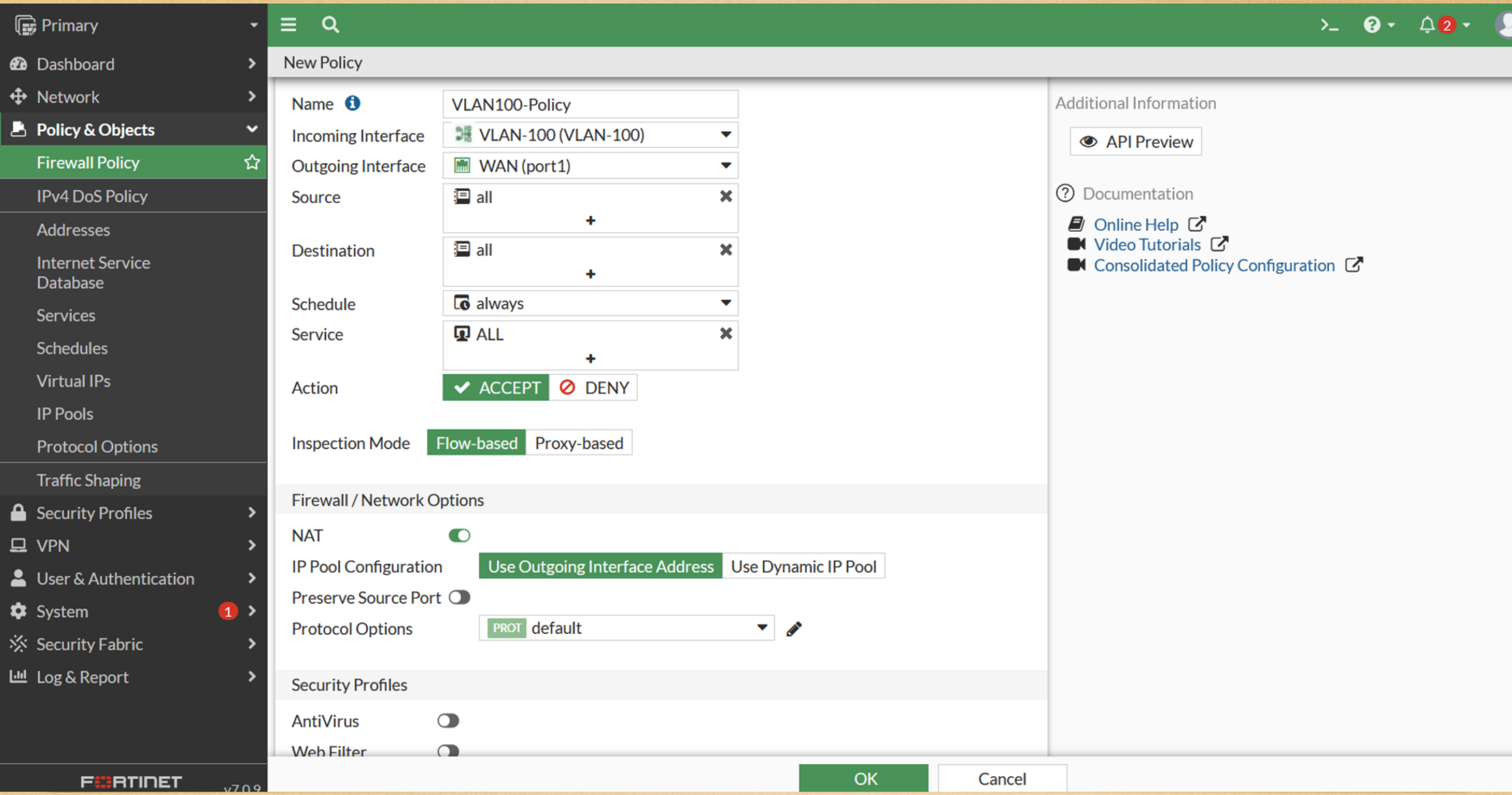
FW-2

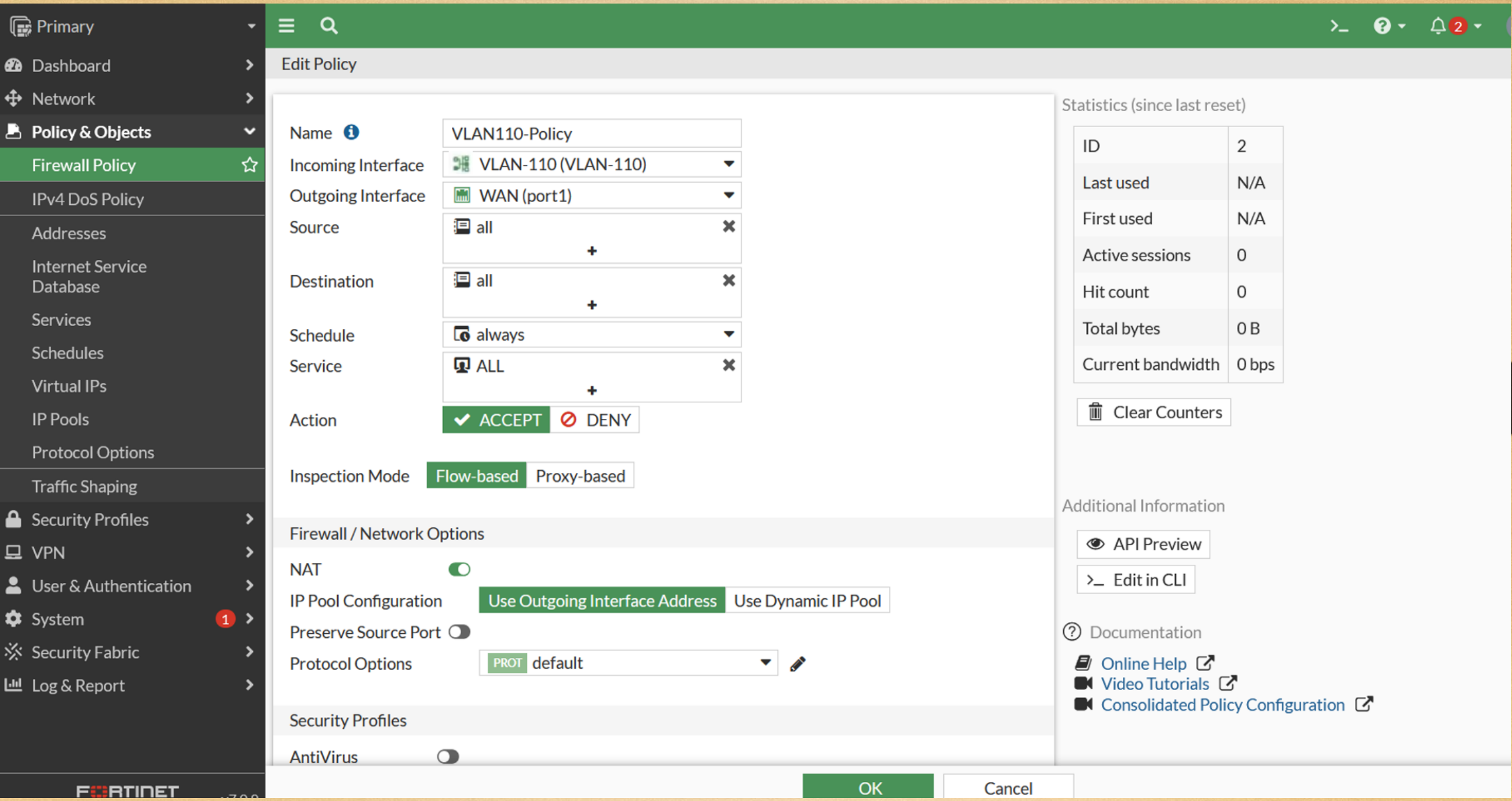
```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port6

FortiGate-VM64-KVM (port6) # set ip 192.168.79.110/24

FortiGate-VM64-KVM (port6) # set allowaccess https http ssh ping

FortiGate-VM64-KVM (port6) # end
```

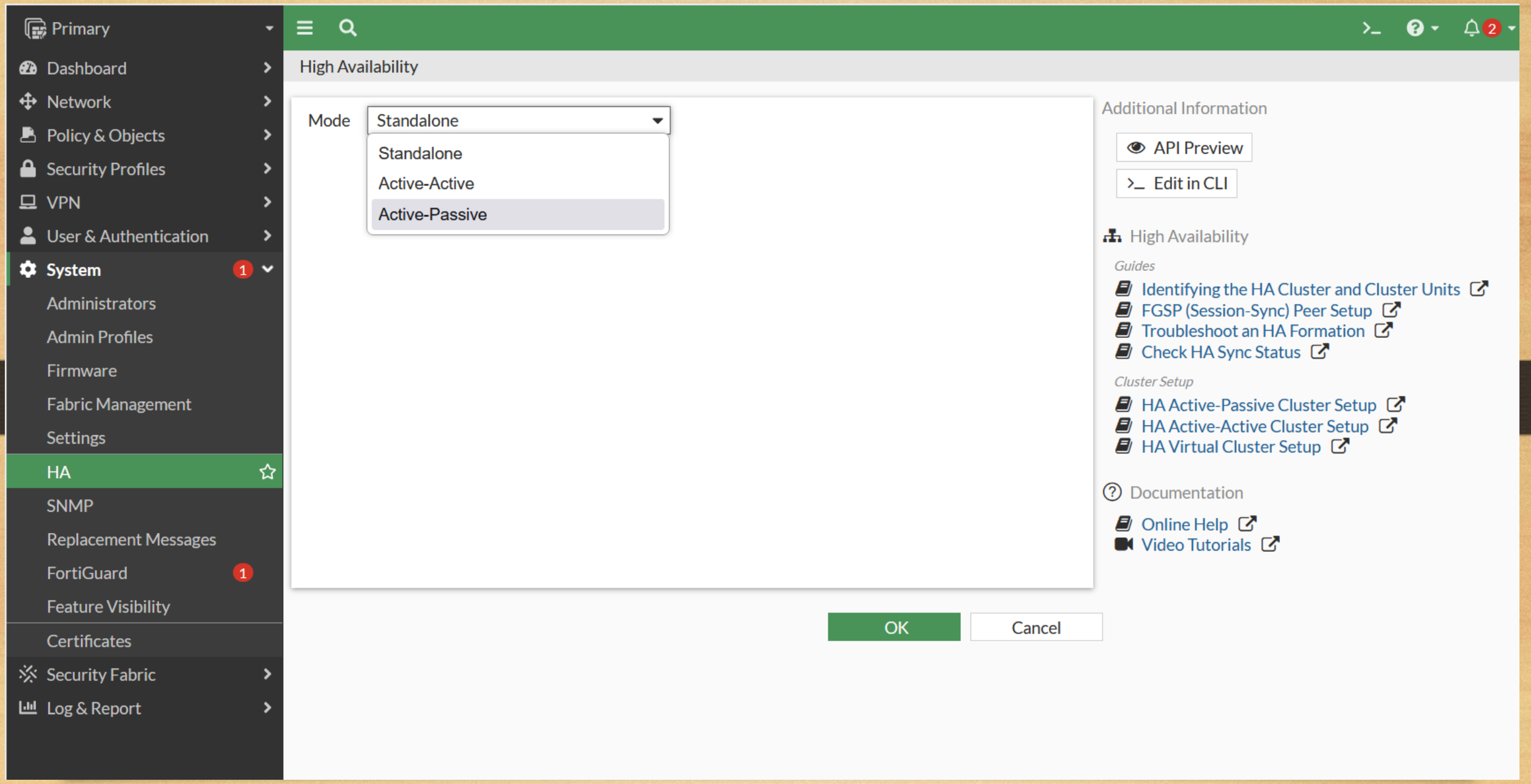
```
Secondary #
Secondary #
```

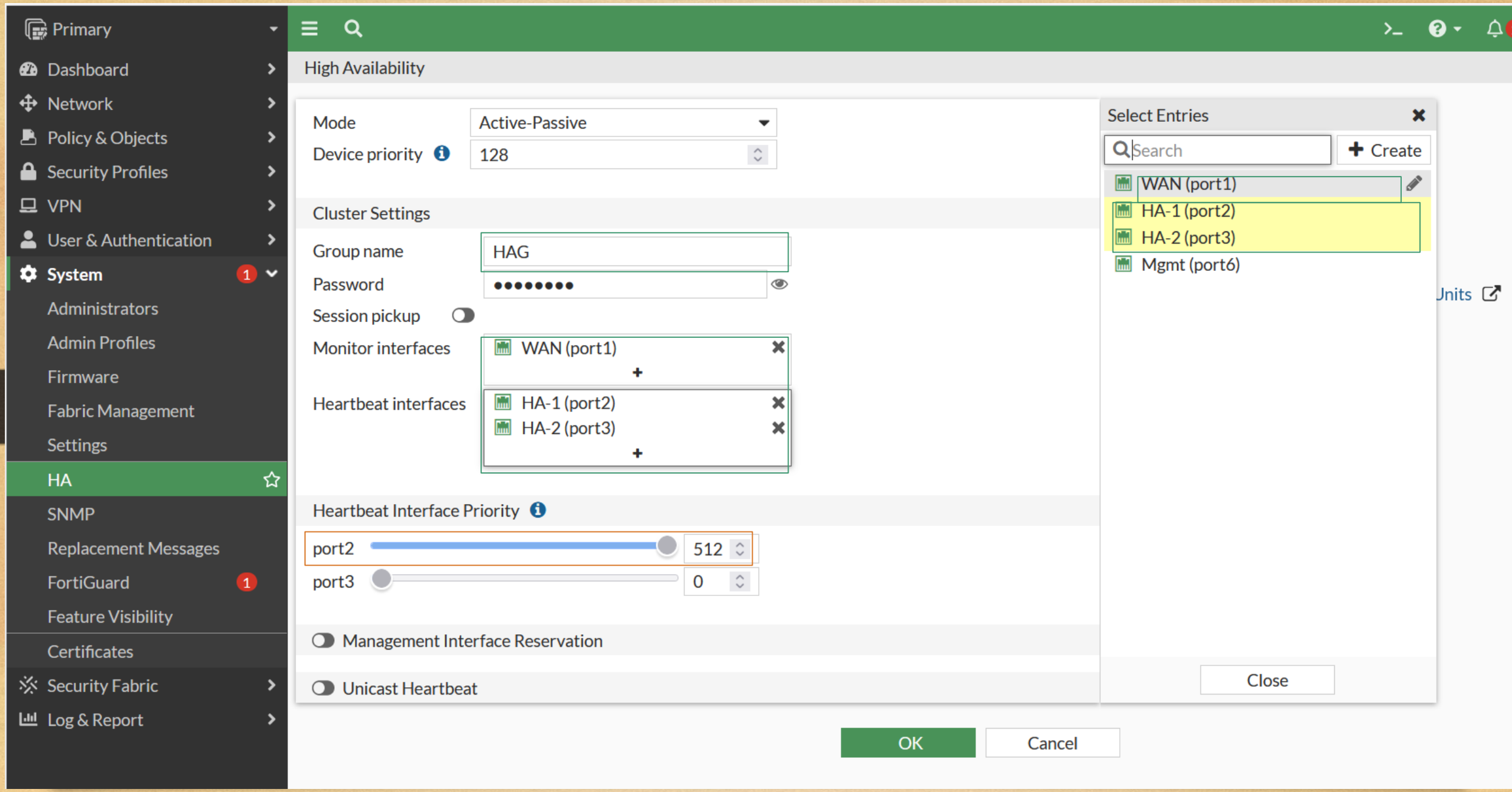

Primary
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
1
Security Fabric
Log & Report
FORTINET
v7.0.8
New Interface
Name
VLAN-100
Alias
VLAN-100
Type
VLAN
VLAN protocol
802.1Q
802.1AD
Interface
AGG-IN (AGG-IN)
VLAN ID
100
VRF ID
0
Role
LAN
Address
Addressing mode
Manual
DHCP
Auto-managed by IPAM
IP/Netmask
192.168.100.254/24
Create address object matching subnet
Name
VLAN-100 address
Destination
192.168.100.254/24
Secondary IP address
Administrative Access
IPv4
HTTPS
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Speed Test
FortiGate
Primary
Additional Information
API Preview
Documentation
Online Help
Video Tutorials
OK
Cancel

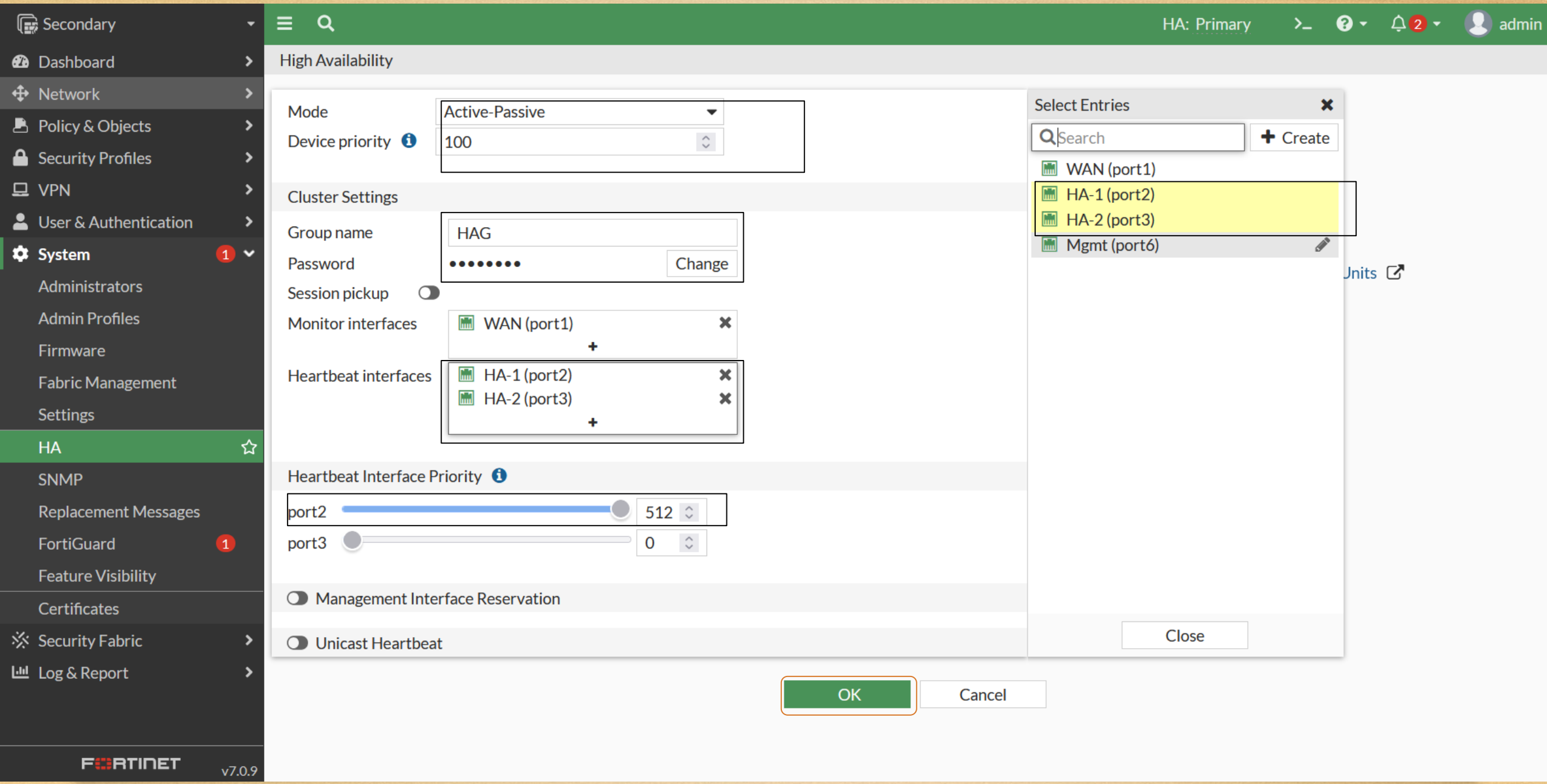

Primary
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
1
Security Fabric
Log & Report
FORTINET
v7.0.9
New Interface
Name
VLAN-110
Alias
VLAN-110
Type
VLAN
VLAN protocol
802.1Q
802.1AD
Interface
AGG-IN (AGG-IN)
VLAN ID
110
VRF ID
0
Role
LAN
Address
Addressing mode
Manual
DHCP
Auto-managed by IPAM
IP/Netmask
192.168.110.254/24
Create address object matching subnet
Name
VLAN-110 address
Destination
192.168.110.254/24
Secondary IP address
Administrative Access
IPv4
HTTPS
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Speed Test
OK
Cancel
FortiGate
Primary
Additional Information
API Preview
Documentation
Online Help
Video Tutorials

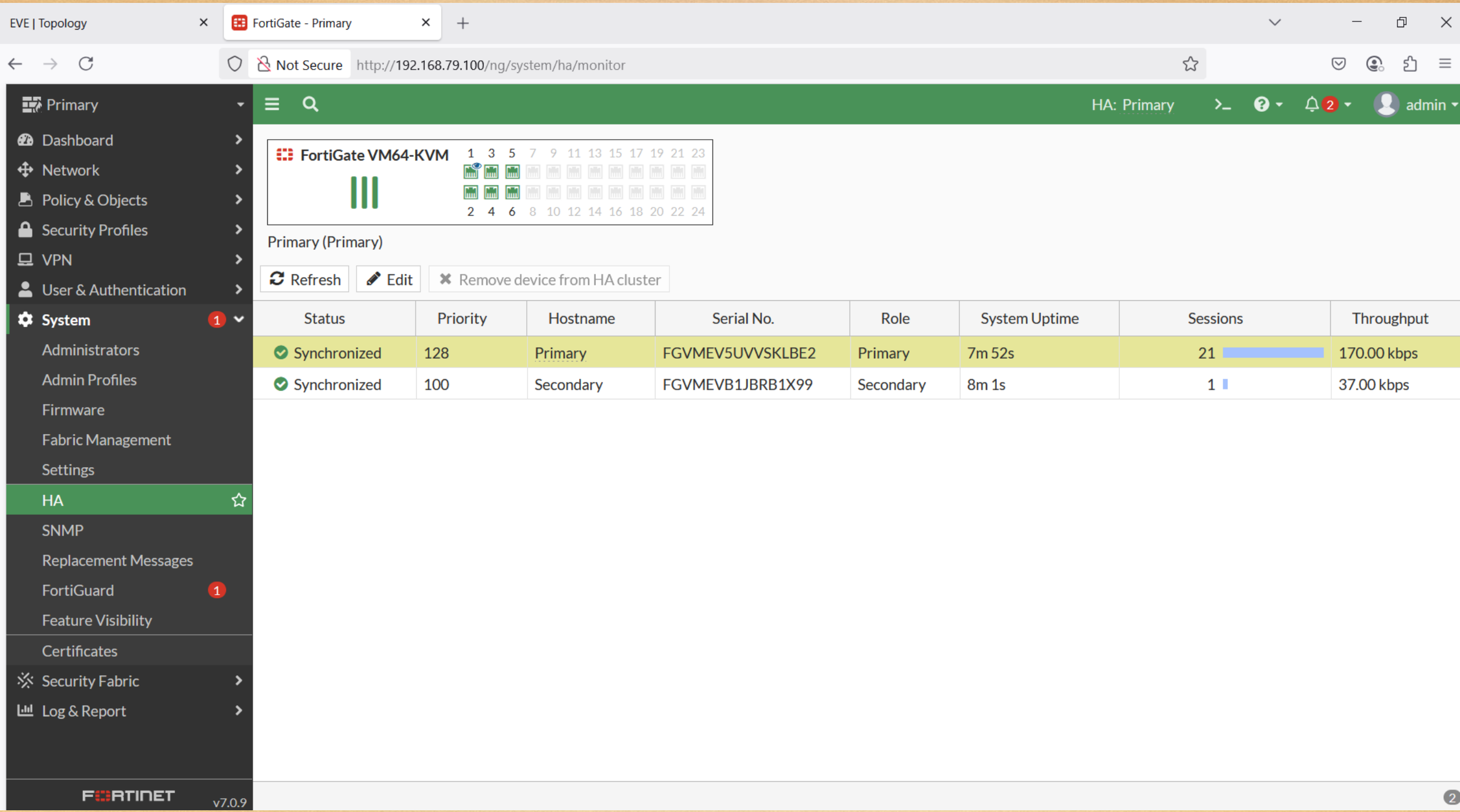

Primary
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.9
New Policy
Name
VLAN100-Policy
Incoming Interface
VLAN-100 (VLAN-100)
Outgoing Interface
WAN (port1)
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default
Security Profiles
AntiVirus
Web Filter
Additional Information
API Preview
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
OK
Cancel


Primary
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Edit Policy
Name
VLAN110-Policy
Incoming Interface
VLAN-110 (VLAN-110)
Outgoing Interface
WAN (port1)
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default
Security Profiles
AntiVirus
Statistics (since last reset)
ID
2
Last used
N/A
First used
N/A
Active sessions
0
Hit count
0
Total bytes
0 B
Current bandwidth
0 bps
Clear Counters
Additional Information
API Preview
Edit in CLI
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
OK
Cancel


Primary
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
1
Administrators
Admin Profiles
Firmware
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
1
Feature Visibility
Certificates
Security Fabric
Log & Report
2
High Availability
Mode
Standalone
Standalone
Active-Active
Active-Passive
Additional Information
API Preview
Edit in CLI
High Availability
Guides
Identifying the HA Cluster and Cluster Units
FGSP (Session-Sync) Peer Setup
Troubleshoot an HA Formation
Check HA Sync Status
Cluster Setup
HA Active-Passive Cluster Setup
HA Active-Active Cluster Setup
HA Virtual Cluster Setup
Documentation
Online Help
Video Tutorials
OK
Cancel


Primary
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Administrators
Admin Profiles
Firmware
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
High Availability
Mode
Active-Passive
Device priority
128
Cluster Settings
Group name
HAG
Password
Session pickup
Monitor interfaces
WAN (port1)
Heartbeat interfaces
HA-1 (port2)
HA-2 (port3)
Heartbeat Interface Priority
port2
512
port3
0
Management Interface Reservation
Unicast Heartbeat
Select Entries
Search
Create
WAN (port1)
HA-1 (port2)
HA-2 (port3)
Mgmt (port6)
Units
Close
OK
Cancel


Secondary
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
1
Administrators
Admin Profiles
Firmware
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
1
Feature Visibility
Certificates
Security Fabric
Log & Report
FORTINET
v7.0.9
HA: Primary
2
admin
High Availability
Mode
Active-Passive
Device priority
100
Cluster Settings
Group name
HAG
Password
Change
Session pickup
Monitor interfaces
WAN (port1)
Heartbeat interfaces
HA-1 (port2)
HA-2 (port3)
Heartbeat Interface Priority
port2
512
port3
0
Management Interface Reservation
Unicast Heartbeat
Select Entries
Search
Create
WAN (port1)
HA-1 (port2)
HA-2 (port3)
Mgmt (port6)
Units
Close
OK
Cancel


EVE | Topology
FortiGate - Primary
Not Secure
http://192.168.79.100/ng/system/ha/monitor
Primary
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Administrators
Admin Profiles
Firmware
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
FORTINET
v7.0.9
HA: Primary
admin
FortiGate VM64-KVM
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Primary (Primary)
Refresh
Edit
Remove device from HA cluster
Status
Priority
Hostname
Serial No.
Role
System Uptime
Sessions
Throughput
Synchronized
128
Primary
FGVMEV5UVVSKLBE2
Primary
7m 52s
21
170.00 kbps
Synchronized
100
Secondary
FGVMEVB1JBRB1X99
Secondary
8m 1s
1
37.00 kbps

EVE | Topology

FortiGate - Secondary

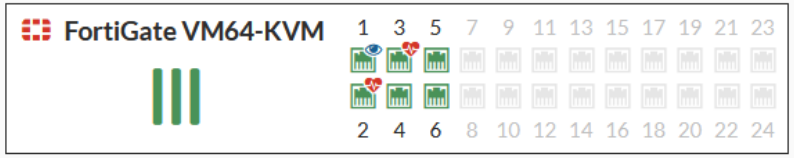
Not Secure http://192.168.79.100/ng/system/ha/monitor

Secondary

HA: Primary admin

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- System 1
  - Administrators
  - Admin Profiles
  - Firmware
  - Fabric Management
  - Settings
  - HA
  - SNMP
  - Replacement Messages
  - FortiGuard 1
  - Feature Visibility
  - Certificates
- Security Fabric
- Log & Report

FORTINET v7.0.9




Secondary (Primary)

Refresh Edit Remove device from HA cluster

| Status | Priority | Hostname | Serial No. | Role | System Uptime | Sessions | Throughput |
|---|---|---|---|---|---|---|---|
| Synchronized | 100 | Secondary | FGVMEVB1JBRB1X99 | Primary | 19m 56s | 13 | 62.00 kbps |
| Synchronized | 128 | Primary | FGVMEV5UVVSKLBE2 | Secondary | 2m 20s | 18 | 45.00 kbps |