رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

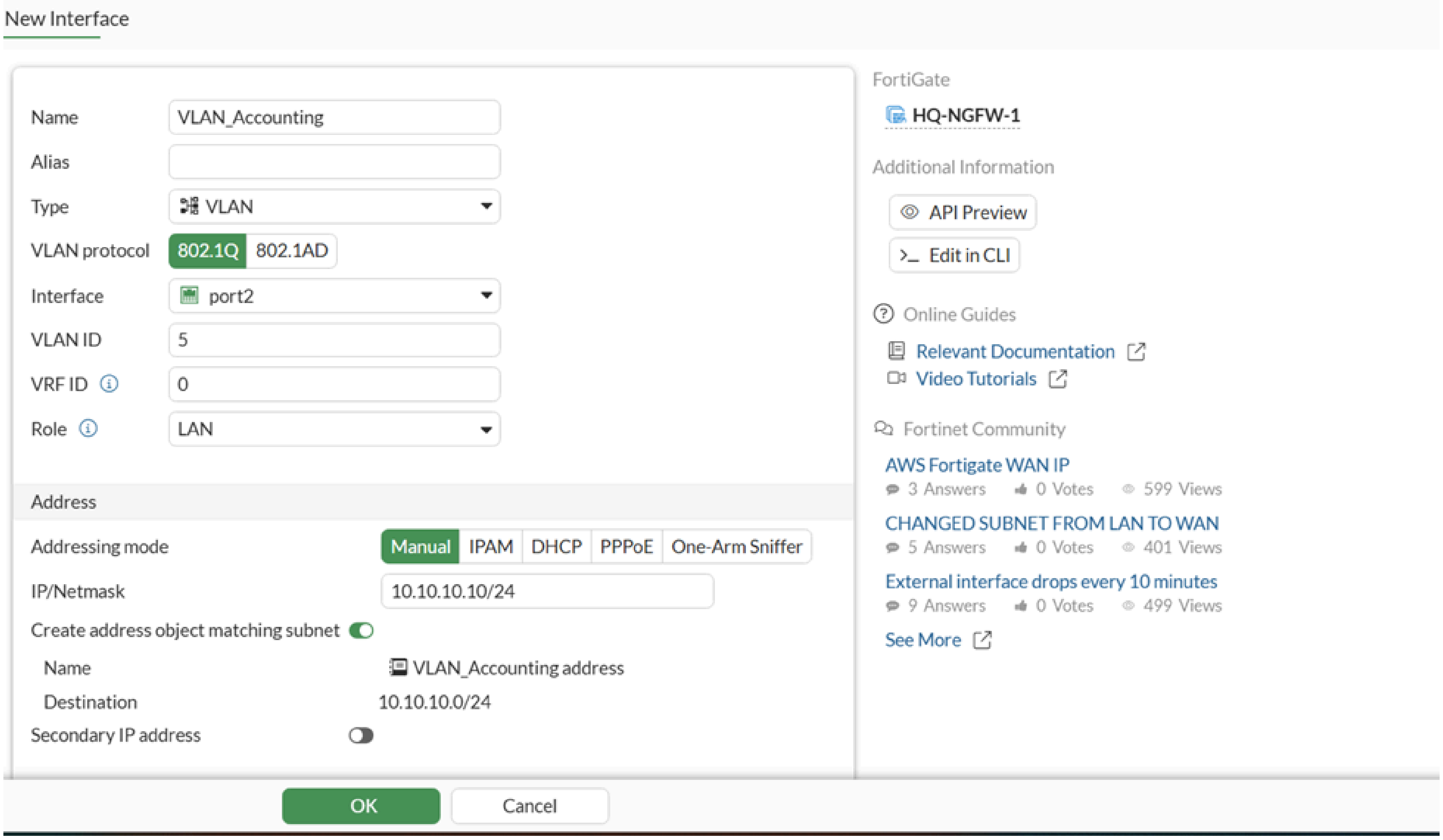
FortiGate VLAN configuration and policy documentation

INTRODUCTION

In Week 2 of the project, the goal was to integrate the FortiGate firewall with the VLANs created in Week 1 and enable inter-VLAN routing. We Created VLAN subinterfaces on the FortiGate, assigning gateway addresses, configuring administrative access, and adding firewall policies to control traffic between the VLANs.

Fortigate Vlan Configuration:

VLAN_Accouting



New Interface

Name	VLAN_Accounting
Alias	
Type	VLAN
VLAN protocol	[✓ 802.1Q] 802.1AD
Interface	port2
VLAN ID	5
VRF ID ⓘ	0
Role ⓘ	LAN

Address

Addressing mode	[✓ Manual] IPAM DHCP PPPoE One-Arm Sniffer
IP/Netmask	10.10.10.10/24
Create address object matching subnet	●
Name	VLAN_Accounting address
Destination	10.10.10.0/24
Secondary IP address	○

FortiGate

HQ-NGFW-1

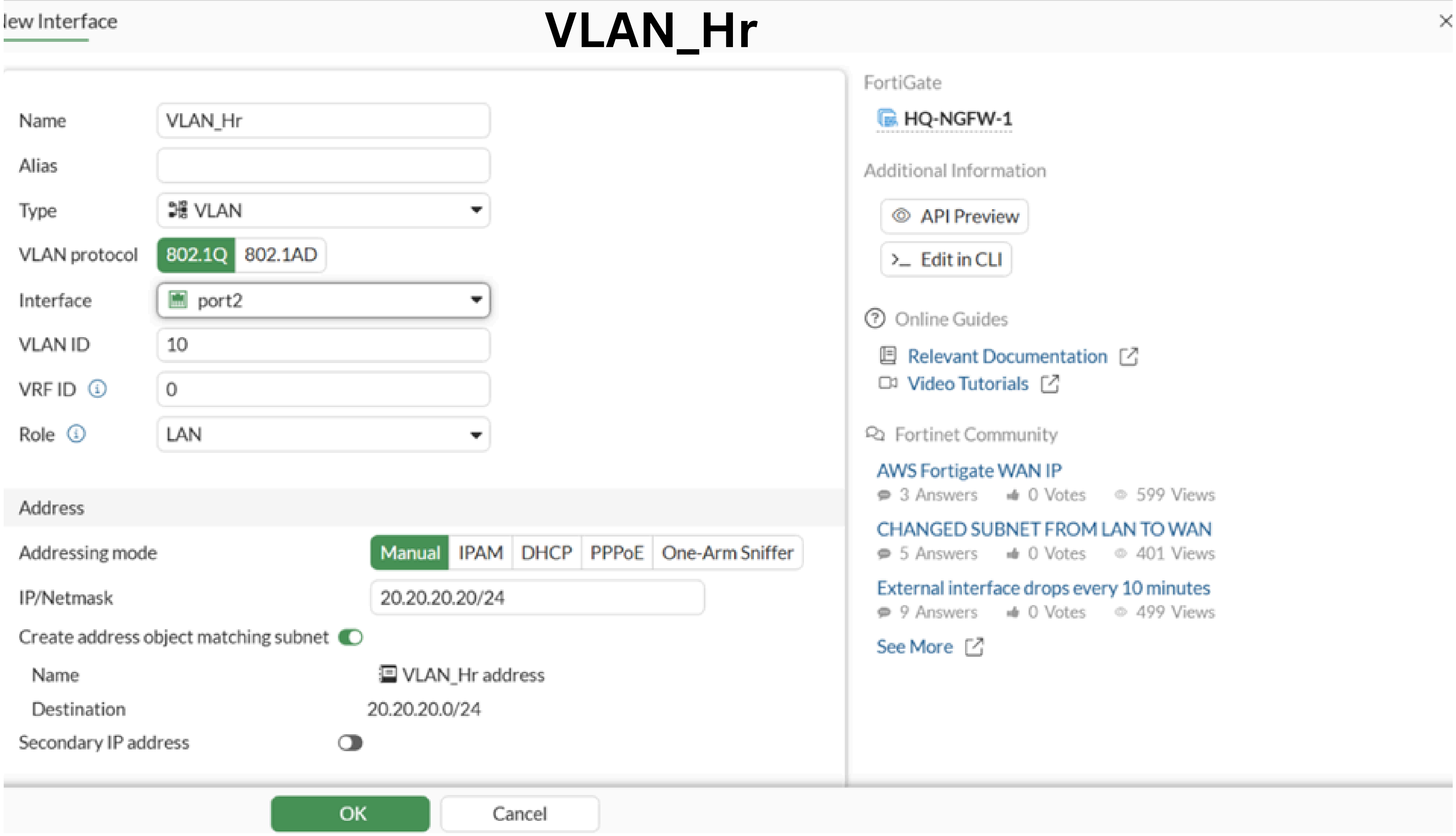
Additional Information

AWS Fortigate WAN IP
3 Answers 0 Votes 599 Views

CHANGED SUBNET FROM LAN TO WAN
5 Answers 0 Votes 401 Views

External interface drops every 10 minutes
9 Answers 0 Votes 499 Views

VLAN_Hr



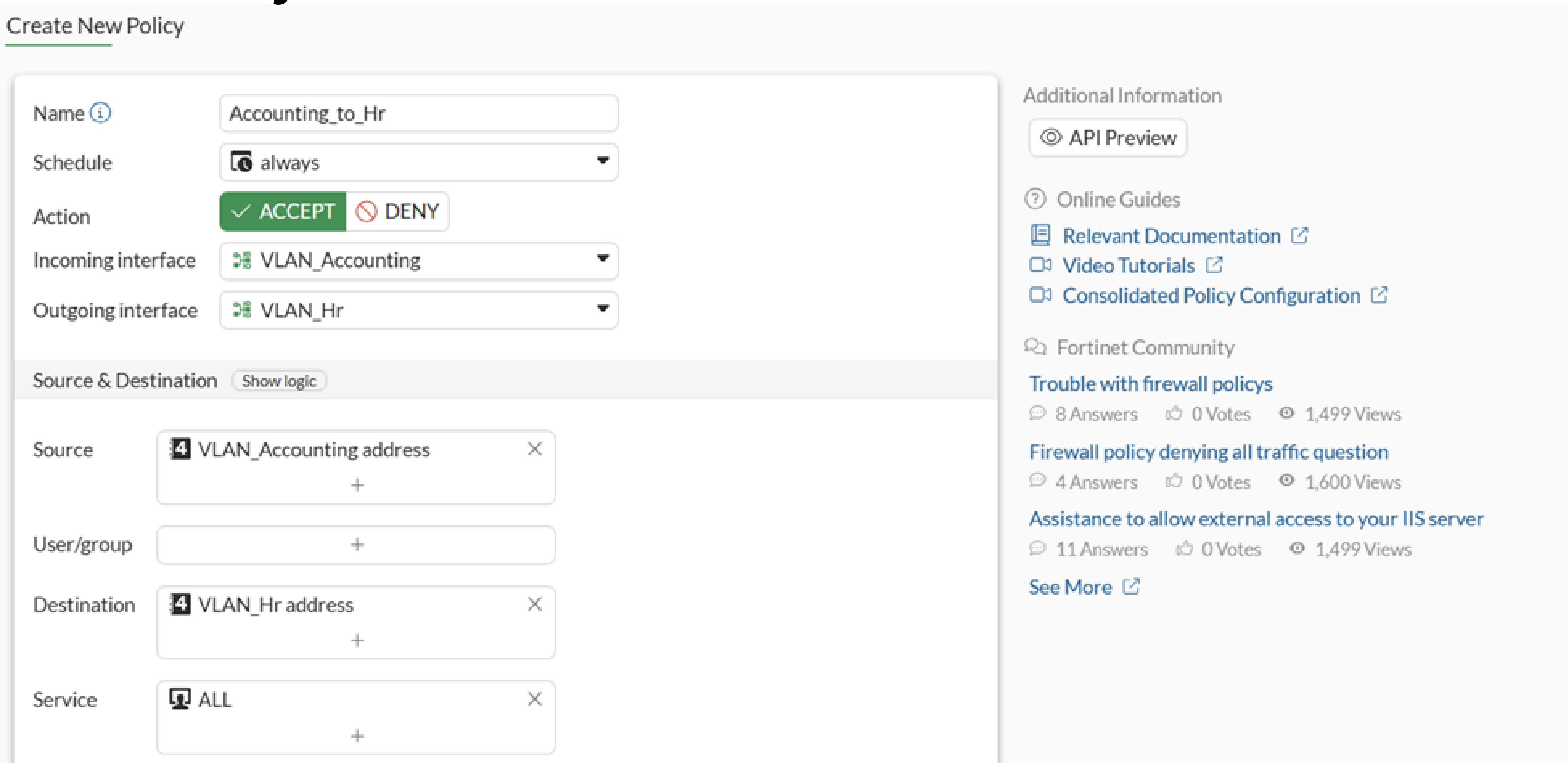
lew Interface

Name: VLAN_Hr
Alias:
Type: VLAN
VLAN protocol: 802.1Q | 802.1AD (802.1Q selected)
Interface: port2
VLAN ID: 10
VRF ID: 0
Role: LAN

Address
Addressing mode: Manual | IPAM | DHCP | PPPoE | One-Arm Sniffer (Manual selected)
IP/Netmask: 20.20.20.20/24
Create address object matching subnet: enabled
Name: VLAN_Hr address
Destination: 20.20.20.0/24
Secondary IP address: disabled

Both of these VLANs were implemented on port 2 , with 2 separate Ips as shown in attached pictures

Firewall Policy:

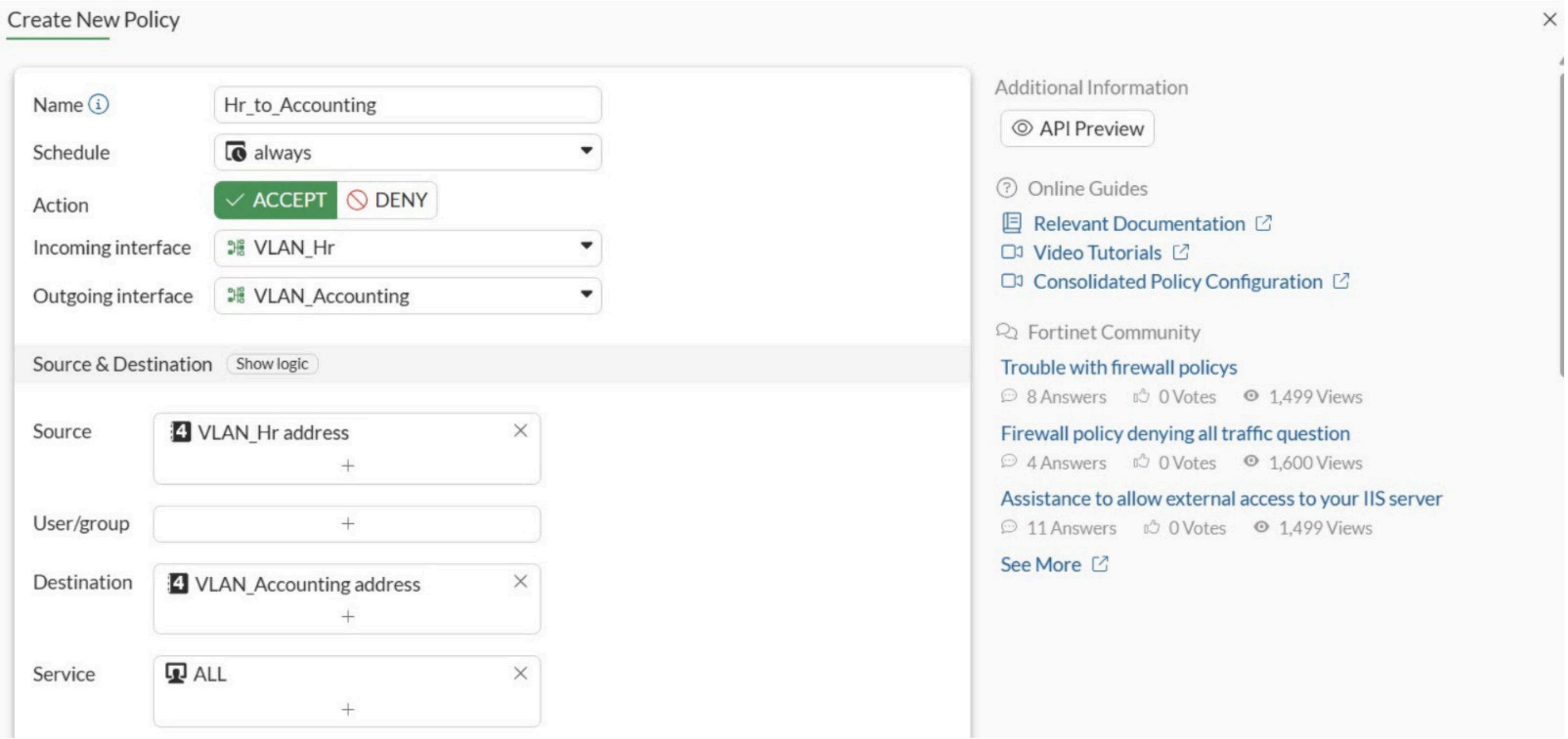


Create New Policy

Name: Accounting_to_Hr
Schedule: always
Action: ACCEPT | DENY (ACCEPT selected)
Incoming interface: VLAN_Accounting
Outgoing interface: VLAN_Hr

Source & Destination
Source: VLAN_Accounting address
User/group:
Destination: VLAN_Hr address
Service: ALL

Show logic
+
×
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Trouble with firewall policys
8 Answers 0 Votes 1,499 Views
Firewall policy denying all traffic question
4 Answers 0 Votes 1,600 Views
Assistance to allow external access to your IIS server
11 Answers 0 Votes 1,499 Views
See More



Create New Policy

Name: Hr_to_Accounting

Schedule: always

Action: [✓ ACCEPT] DENY

Incoming interface: VLAN_Hr

Outgoing interface: VLAN_Accounting

Source & Destination

Source: VLAN_Hr address

User/group:

Destination: VLAN_Accounting address

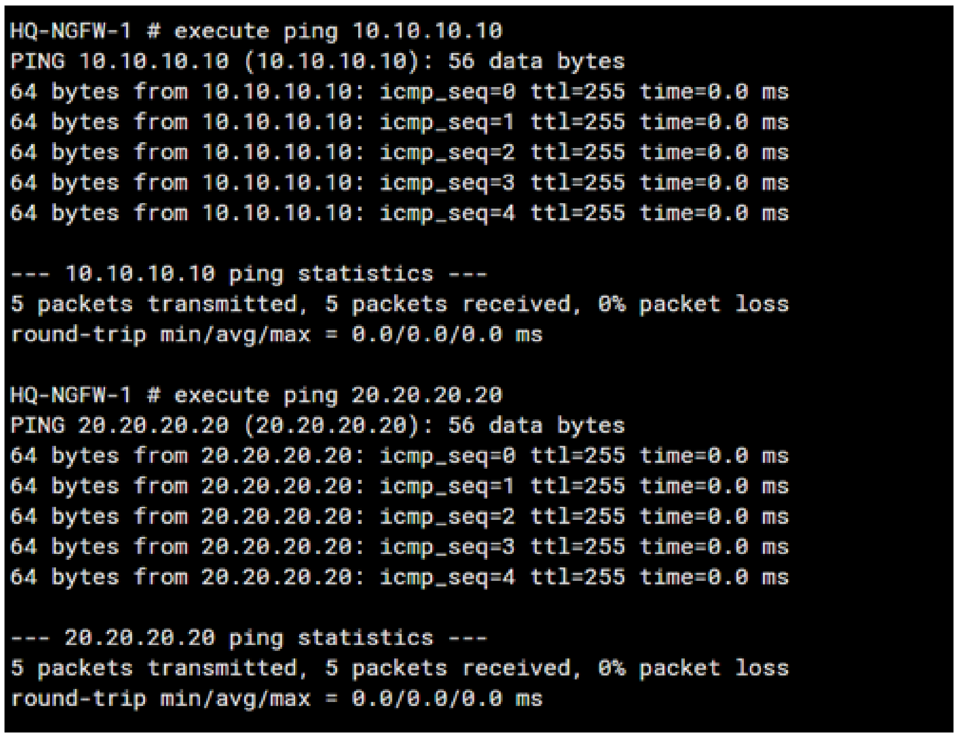
Service: ALL

Show logic
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Trouble with firewall policys
8 Answers 0 Votes 1,499 Views
Firewall policy denying all traffic question
4 Answers 0 Votes 1,600 Views
Assistance to allow external access to your IIS server
11 Answers 0 Votes 1,499 Views
See More

These policies ensure that traffic can flow freely between the two VLANs, while still allowing the firewall to enforce inspection, logging, or security profiles if needed.

Verification:

To make sure that the vlans were implemented correctly independently of each other , and to then prove that they could communicate with each other the following tests were preformed



```
HQ-NGFW-1 # execute ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

HQ-NGFW-1 # execute ping 20.20.20.20
PING 20.20.20.20 (20.20.20.20): 56 data bytes
64 bytes from 20.20.20.20: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=4 ttl=255 time=0.0 ms

--- 20.20.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

This confirms that inter-VLAN routing is working properly and that firewall policies allow communication in both directions.