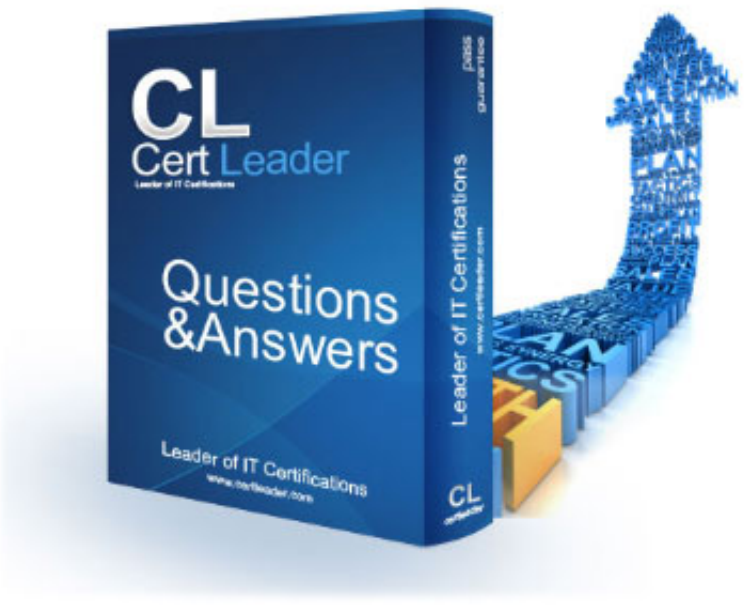
NSE6_FNC-7.2 Dumps

Fortinet NSE 6 - FortiNAC 7.2

https://www.certleader.com/NSE6_FNC-7.2-dumps.html



NEW QUESTION 1
Where do you look to determine when and why the FortiNAC made an automated network access change?

A. The Event view
B. The Port Changes view
C. The Connections view
D. The Admin Auditing view

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/536166/viewing- event-logs
Study Guide p. 356: Any time FortiNAC changes network access for an endpoint, the change is documented on the Port Changes view. This provides an administrator with valuable information when validating control configurations and enforcement.

NEW QUESTION 2
Which three of the following are components of a security rule? (Choose three.)

A. Security String
B. Methods
C. Action
D. User or host profile
E. Trigger

Answer: CDE

Explanation:
Reference: https://docs.fortinet.com/document/fortinac/8.8.0/administration-guide/167668/add-or-modify-a-rule

NEW QUESTION 3
When configuring isolation networks in the configuration wizard, why does a Layer 3 network type allow for more than one DHCP scope for each isolation network type?

A. There can be more than one isolation network of each type.
B. Any scopes beyond the first scope are used if the Initial scope runs out of IP addresses.
C. Configuring more than one DHCP scope allows for DHCP server redundancy.
D. The Layer 3 network type allows for one scope for each possible host status.

Answer: A

NEW QUESTION 4
What method of communication does FortiNAC use to control VPN host access on FortiGate?

A. RSSO
B. Security Fabric
C. RADIUS accounting
D. SAMLSSO

Answer: B

NEW QUESTION 5
When FortiNAC is managing VPN clients connecting through FortiGate. why must the clients run a FortiNAC agent?

A. To collect user authentication details
B. To meet the client security profile rule for scanning connecting clients
C. To collect the client IP address and MAC address
D. To transparently update the client IP address upon successful authentication

Answer: B

NEW QUESTION 6
Which three circumstances trigger Layer 2 polling of infrastructure devices? (Choose three.)

A. Manual polling
B. Scheduled poll timings
C. A failed Layer 3 poll
D. A matched security policy
E. Linkup and Linkdown traps

Answer: ABE

Explanation:
A. Manual Polling: This is when an administrator or network operator initiates a poll manually to gather information or check the status of the network devices. This can be done for immediate troubleshooting or assessment.
* B. Scheduled Poll Timings: Network management systems often have the capability to schedule regular polls of devices to check their status or monitor their

performance. These scheduled polls can be set at regular intervals (such as every few minutes, hours, or daily) depending on the requirements of the network.
* E. Linkup and Linkdown Traps: SNMP (Simple Network Management Protocol) traps, like Linkup and Linkdown, are automated notifications sent from network devices to a management system. A Linkup trap indicates that a particular interface has become active (up), while a Linkdown trap indicates that an interface has become inactive (down). These traps can trigger Layer 2 polling to ascertain the current status of network interfaces and devices.

NEW QUESTION 7
Where are logical network values defined?

A. In the model configuration view of each infrastructure device
B. In the port properties view of each port
C. On the profiled devices view
D. In the security and access field of each host record

Answer: A

Explanation:
In FortiNAC, logical networks are an integral part of device management and network segmentation. These logical networks are defined and appear within the model configuration of each infrastructure device that is modeled in the topology tree. The configuration allows for the assignment of unique names and, optionally, descriptions to each logical network, thereby clarifying their purpose or use within the network infrastructure.
References: FortiNAC 7.2 Study Guide, Logical Networks Security Fabric and Firewall Tags section.

NEW QUESTION 8
Two FortiNAC devices have been configured in an HA configuration. After five failed heartbeats between the primary device and secondary device, the primary device fail to ping the designated gateway. What happens next?

A. The primary device continues to operate as the in-control device and changes the status or secondary device to contact lost.
B. The primary device changes its designation to secondary, and the secondary device changes to primary.
C. The primary device shuts down NAC processes and changes to a management down status.
D. The primary device waits 3 minutes and attempts to re-establish the HA heartbeat before attempting a second ping of the gateway.

Answer: C

NEW QUESTION 9
An administrator is configuring FortiNAC to manage FortiGate VPN users. As part of the configuration, the administrator must configure a few FortiGate firewall policies.
What is the purpose of the FortiGate firewall policy that applies to unauthorized VPN clients?

A. To deny access to only the production DNS server
B. To allow access to only the FortiNAC VPN interface
C. To allow access to only the production DNS server
D. To deny access to only the FortiNAC VPN interface

Answer: B

NEW QUESTION 10
When FortiNAC passes a firewall tag to FortiGate, what determines the value that is passed?

A. Security rule
B. Device profiling rule
C. RADIUS group attribute
D. Logical network

Answer: B

NEW QUESTION 10
In which view would you find who made modifications to a Group?

A. The Event Management view
B. The Security Events view
C. The Alarms view
D. The Admin Auditing view

Answer: D

Explanation:
It’s important to audit Group Policy changes in order to determine the details of changes made to Group Policies by delegated users.
Reference: https://www.lepide.com/how-to/audit-chnages-made-to-group-policy- objects.html

NEW QUESTION 14
View the command and output.

```
>hsIsSlaveActive Host FortiNAC-Secondary
Host fortinac-primary
SQL version 5.6.31,
Slave is active
```

What is the state of database replication?

A. Secondary to primary synchronization failed.
B. Primary to secondary synchronization failed.
C. Secondary to primary synchronization was successful.
D. Primary to secondary database synchronization was successful.

Answer: D

Explanation:
The command and output shown in the exhibit indicate that the host FortiNAC-Secondary is referencing FortiNAC-Primary, and it states "Slave is active." In database replication terminology within a high availability setup, the term "Slave is active" typically means that the secondary server (slave) is actively receiving data from the primary server (master). This implies that the synchronization process from the primary to the secondary database has been successful and is currently active.
References
? FortiNAC 7.2 Study Guide, Security Policies section

NEW QUESTION 19
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE6_FNC-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE6_FNC-7.2-dumps.html