PassQueen
a.k.a dumpsqueen.com

Nutanix Certified ProfessionalNetwork and Security (NCP-NS) 7.5

Nutanix NCP-NS-7.5

Version Demo

Total Demo Questions: 11

Total Premium Questions: 118

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Fundamentals	4
Topic 2, Network Configuration	40
Topic 3, Network Security	57
Topic 4, Network Troubleshooting	16
Topic 5, Mix Questions	1
Total	118

QUESTION NO: 1

An administrator has been tasked with configuring virtual switches and setting the appropriate MTU size for a Nutanix cluster to optimize network performance. The cluster needs to support high-throughput traffic between VMs and ensure compatibility with external networks. The administrator needs to configure the virtual switches and MTU size to enable jumbo frames while ensuring that all nodes and network components are properly aligned to prevent packet loss or fragmentation. What is the first step to configure the virtual switches and MTU size in a Nutanix cluster for optimal network performance?

A. Enable multicast filtering on the virtual switches to optimize MTU configuration.

B. Set the MTU size to 1500 on the Nutanix virtual switches and configure a separate VLAN for MTU traffic.

C. Set the MTU size to 1500 on all nodes and virtual switches for compatibility with external networks.

D. Configure the MTU size to 9000 on all nodes and virtual switches, and verify that all physical network switches support jumbo frames.

ANSWER: D

Explanation:

Configure the MTU size to 9000 on all nodes and virtual switches, and verify that all physical network switches support jumbo frames. This establishes a consistent end-to-end jumbo-frame configuration for the VM data path, which is essential before relying on larger Ethernet frames for high-throughput workloads. In a Nutanix AHV environment, the virtual switch configuration alone is insufficient: the AHV hosts' relevant interfaces and every physical-switch port, uplink, and intermediate network device on the path must support the selected MTU. A single lower-MTU segment can cause oversized packets to be dropped or fragmented, reducing throughput and producing difficult-to-diagnose connectivity symptoms. Using an MTU of 9000 is a common jumbo-frame setting and leaves room for networking overhead where applicable while enabling efficient transfer of large payloads. The administrator should also validate the complete path, including external connectivity where jumbo frames are expected to traverse it, rather than assuming that a setting applied in the cluster automatically changes the physical network. Nutanix AHV networking documentation describes virtual-switch and host-network configuration concepts, while Nutanix support guidance covers MTU consistency and jumbo-frame considerations. See the Nutanix AHV Administration Guide networking documentation and Nutanix knowledge base guidance on jumbo frames.

QUESTION NO: 2

An administrator assigns a Floating IP to a web server VM in a VPC overlay subnet. The VPC has an external subnet connection and a default route to that external subnet. External clients can reach the Floating IP, but TCP port 443 connections to the web server are blocked after a Flow Network Security policy is enforced. What should the administrator do?

A. Add an inbound rule permitting TCP port 443 from the intended external client network to the Web secured entity.

B. Assign a second Floating IP to the web server VM.

C. Change the VPC default route to use an internal overlay subnet.

D. Restart the web server VM after assigning the Floating IP.

ANSWER: A

Explanation:

The administrator should add an inbound rule that permits TCP port 443 from the intended external client network to the Web secured entity. A Floating IP provides address translation and external reachability, but it does not bypass Flow Network Security policy enforcement. When the web VM is covered by an enforced policy, inbound traffic must match an explicit permitted rule.

Changing the Floating IP, rebooting the VM, or adding another default route does not address a Flow policy deny. The rule should be scoped to the required source network and HTTPS service to preserve least-privilege access.

QUESTION NO: 3

An administrator plans to enable Flow Network Security Next-Gen microsegmentation for workloads deployed on an on-premises overlay network. Which two prerequisites must be satisfied? (Choose two.)

A. Enable Network Controller in Prism Central.

B. Attach the protected workloads to an overlay network.

C. Convert every workload subnet to a VLAN Basic network.

D. Configure a Floating IP for every protected workload.

E. Create static routes for all workload IP addresses.

ANSWER: A B

Explanation:

Flow Network Security Next-Gen requires the Network Controller service to be enabled in Prism Central. The workload network must also be a supported overlay network because Next-Gen security is supported for on-premises overlay networking.

A VLAN Basic network is not a supported deployment environment for Flow Network Security Next-Gen. Creating static routes or assigning Floating IPs can be required for particular connectivity designs, but neither action enables Next-Gen microsegmentation.

QUESTION NO: 4

An administrator is implementing Flow Network Security user-based security for Windows virtual desktops. Policies use a dynamic category that is applied when a user belonging to an Active Directory group signs in. Which two conditions are required for the expected dynamic user category to be assigned? (Choose two.)

A. Configure a functioning Active Directory integration in Prism Central.

B. Install, enable, and run Nutanix Guest Tools on the virtual desktop.

C. Assign a Floating IP to each virtual desktop.

D. Configure a default route through a NAT external subnet.

E. Place the security policy in Enforce mode before users sign in.

ANSWER: A B

Explanation:

User-based security requires a functioning Active Directory integration so that Prism Central can evaluate the logged-in user's group membership. Nutanix Guest Tools must also be installed, enabled, and running on the virtual desktop so that user logon information can be reported for dynamic category assignment.

A Floating IP and a VPC default route affect external connectivity, not user identity detection. The policy can be monitored or enforced, but the policy mode does not create the dynamic category.

QUESTION NO: 5

A service-insertion firewall VM protects user VMs access to the internet. The virtual and physical switches, as well as all user VMs, currently use the default MTU size of 1500. Everything functions normally until a user VM is migrated to another host. After the migration, the user reports that some websites fail to load while ping to those same sites still succeeds. Routing and security policies appear normal. Which two configuration changes could resolve the issue? (Choose two.)

A. Increase the MTU across all vSwitch and physical uplinks on the relevant network path to 1558 or greater.

B. Lower the MTU across all vSwitch and physical uplinks on the relevant network path to 1442 or lower.

C. Decrease the MTU on the user VM's vNIC to 1442 or lower.

D. Increase the MTU on the user VM's vNIC to 1558 or greater.

ANSWER: A C

Explanation:

“Increase the MTU across all vSwitch and physical uplinks on the relevant network path to 1558 or greater” is correct because service insertion uses overlay encapsulation between the workload host and the firewall service VM. Encapsulation adds headers to the original Ethernet frame. A 1500-byte guest packet can therefore become approximately 1558 bytes on the underlay. Configuring every vSwitch and physical link in that path for at least 1558 bytes permits those encapsulated frames to traverse the network without fragmentation or drops.

“Decrease the MTU on the user VM's vNIC to 1442 or lower” is also correct as an alternative remediation when the underlay must remain at 1500. Reducing the guest MTU reserves sufficient room for the encapsulation overhead, allowing the resulting outer packet to remain within the 1500-byte underlay limit. It also causes TCP endpoints to negotiate a smaller effective payload size, which addresses the common symptom in which ICMP succeeds but larger TCP responses, such as web content, fail after migration. Nutanix networking documentation and product guides are available through the Nutanix Product Documentation page and the Nutanix Support Portal documentation library.

QUESTION NO: 6

In a Nutanix deployment, when is the Network Controller automatically enabled?

A. When the Small Prism Central deployment is scaled out to three PCVM's

B. When the Network Controller is manually configured from the Prism Central settings page

C. When the Network Controller is enabled on a Hyper-V cluster

D. When the X-Large Prism Central deployment is installed or upgraded

ANSWER: D

Explanation:

When the X-Large Prism Central deployment is installed or upgraded, Nutanix automatically enables the Network Controller service. The Network Controller is the Prism Central control-plane component used by Flow Virtual Networking to manage virtual networking constructs centrally, including VPC-related networking services and the required overlay-network control functions. Its automatic enablement is tied to the X-Large Prism Central deployment size because that sizing provides the capacity and resilient multi-VM Prism Central architecture expected for this service. Administrators planning to use Flow Virtual Networking should therefore account for the Prism Central sizing requirement as part of the design, rather than treating Network Controller activation as a separate routine configuration step. This behavior also means that moving an existing Prism Central deployment to X-Large can activate the service as part of the supported scale-up or upgrade workflow. Nutanix documents Flow Virtual Networking and its Prism Central service requirements in the Flow Virtual Networking documentation. Additional product and architecture context is available on the Nutanix Flow Virtual Networking product page.

QUESTION NO: 7

An administrator is troubleshooting a web server VM that is published through a Floating IP. The external network connection and the Floating IP assignment are healthy, but external HTTPS clients cannot establish a session. Which two items should the administrator verify next? (Choose two.)

A. Verify that the VPC route table includes a route through the applicable external subnet.

B. Verify that an enforced security policy permits inbound TCP port 443 to the web VM.

C. Verify that the web VM has Nutanix Guest Tools installed.

D. Verify that the external client uses the same DNS server as Prism Central.

E. Verify that the web VM is attached to a VLAN Basic subnet.

ANSWER: A B

Explanation:

The VPC must have a route, normally a default route, through the appropriate external subnet so that return traffic can leave the VPC through the external connectivity path. A Floating IP association alone does not provide complete bidirectional forwarding.

The administrator must also verify that an enforced Flow Network Security policy permits the required inbound HTTPS traffic to the web VM. A policy can block the connection even when external addressing, translation, and routing are correctly configured. DNS configuration and guest-tools installation do not determine whether the VPC can forward and permit the HTTPS session.

QUESTION NO: 8

An administrator recently deployed a new set of virtual machines... 3-tier web application... restricted as follows: Only application VMs can talk to database VMs on port 3306 Frontend VMs should only communicate with application VMs on port 8080 Which action will correctly create and configure the Security Policies in Nutanix Flow to satisfy this task?

A. Create VLANs for each tier and configure ACLs to restrict communication.

B. Create IP-based rules for each VM category within a Security Policy.

C. Configure a global "Allow All" Security Policy and rely on guest OS firewalls for tier-based restrictions.

D. Create categories for each tier then define an Application Policy allowing specific ports between them.

ANSWER: D

Explanation:

Create categories for each tier then define an Application Policy allowing specific ports between them. Nutanix Flow Network Security uses categories to identify groups of workloads independently of IP addresses or VLAN placement. Assigning the frontend, application, and database virtual machines to distinct tier categories creates reusable, intent-based workload groups. An Application Policy can then use those categories as the source and destination of explicit allow rules: frontend workloads may reach application workloads using TCP port 8080, and application workloads may reach database workloads using TCP port 3306. This implements microsegmentation at the virtual-machine level and preserves the intended communication path as workloads are added, moved, or renumbered. The policy is centrally managed in Prism Central and enforced by Flow on the participating AHV hosts, rather than requiring each workload's network identity to be maintained manually. Category-based policies are therefore the appropriate mechanism for defining the application's permitted east-west traffic according to its tiers and required services. Nutanix describes Flow Network Security as a native, policy-driven microsegmentation capability in its Nutanix Flow overview; administrators can also access the applicable product documentation through the Nutanix Support Portal.

QUESTION NO: 9

An administrator needs to make a web server VM, which is inside a private VPC overlay subnet, accessible from the external network. The administrator assigns a Floating IP to the VM, but the service is still unreachable from the outside. What is a likely reason for this failure?

A. A Floating IP was assigned from a different external subnet than the one used by the VP

B. The VPC has no default route configured to use the external subnet.

C. The VM was not rebooted after the Floating IP was assigned.

D. The web server VM is not running the latest version of NGT.

ANSWER: B

Explanation:

The VPC has no default route configured to use the external subnet. A Floating IP provides a public-to-private address association for the VM, but it does not by itself establish complete VPC-to-external-network forwarding. The VPC routing configuration must provide a route for external-bound traffic, normally a default route for `0.0.0.0/0` that uses the appropriate external subnet as its next hop. This route is particularly important for the VM's return traffic: after an external client reaches the VM through the Floating IP, the response must be routed back through the VPC's external connectivity so that the flow can be correctly translated and delivered to the originating client. Without that default route, the VM can receive the translated inbound connection attempt but lacks the required VPC forwarding path for a successful end-to-end session. When publishing services with Floating IPs, administrators should therefore confirm that the external subnet is connected to the VPC and that the VPC route table includes the applicable default route. Nutanix Flow Virtual Networking documentation describes VPC external connectivity, route tables, and Floating IP-based access in the Flow Virtual Networking Administration Guide. Additional Nutanix networking documentation is available through the Nutanix Documentation portal.

QUESTION NO: 10

What does placing a policy in Monitor mode accomplish?

A. Visualizes discovered traffic that matches the policy.

B. Blocks traffic that does not match the policy.

C. Enables hitlogs for traffic that matches the policy.

D. Redirects discovered traffic to a monitoring device.

ANSWER: A

Explanation:

Visualizes discovered traffic that matches the policy. is correct because Monitor mode in Nutanix Flow Network Security is intended to evaluate a policy without enforcing its rules on live workloads. Flow observes communications that meet the policy criteria and presents the discovered matching traffic, allowing an administrator to understand actual application dependencies before applying enforcement. This is particularly useful when building segmentation policies for an application whose required inbound and outbound flows have not yet been fully validated.

Using Monitor mode supports a safe policy-development workflow: define the intended application boundaries, observe the traffic that the policy identifies, review the discovered flows, and then refine the policy as needed before switching it to an enforcement mode. The observation is based on the policy's matching conditions, including the protected entities and rule criteria. It therefore provides visibility into relevant traffic behavior while avoiding disruption to application connectivity during assessment and tuning. Nutanix describes Flow Network Security as providing application-centric microsegmentation and visibility for workload communication. See the Nutanix Flow Network Security product page and the Flow Network Security Administration Guide for product and policy-management details.

QUESTION NO: 11

An administrator has a requirement to capture application flow data for a policy in Monitor mode and export those events to an external SIEM for correlation with other logs. Which two actions are required to achieve this? (Choose two.)

A. Enable IPFIX export on the monitored policy.

B. Enable Policy Hit Logging on the monitored policy.

C. Create a Flow Audit Policy on the monitored policy.

D. Configure a remote syslog destination in Prism Central.

ANSWER: B D

Explanation:

Enable Policy Hit Logging on the monitored policy and configure a remote syslog destination in Prism Central. A Flow Network Security policy operating in Monitor mode observes traffic that matches its rules without enforcing a drop action, making it suitable for validating application communication before enforcement. Policy Hit Logging supplies the required policy-level event records, including details that identify the policy/rule match and the traffic observed. This logging must be enabled on the policy being monitored; Monitor mode by itself does not provide an external SIEM feed.

Prism Central must also have a remote syslog destination configured so that generated Flow policy-hit events are forwarded from the Nutanix environment to the organization's SIEM or log collector. The SIEM can then retain, search, and correlate those Flow events with information from other infrastructure and application sources. Together, policy hit logging creates the relevant security-policy telemetry, while remote syslog configuration provides the export path required for central correlation. Nutanix documents Flow Network Security policy monitoring and logging in the Flow Network Security Administration Guide and describes external syslog configuration in the Prism Central Guide.