Boost up Your Certification Score

Nutanix

NCP-NS-7.5

Nutanix Certified Professional - Network and Security (NCP-NS) 7.5

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

During a security review, the administrator confirms that the existing security policy does not explicitly allow traffic from Environment: Development to Environment: Production. A VM in the Development category was still able to reach a Production VM over IPv6. What is the most likely cause of this behavior?

A. An isolation policy was incorrectly applied instead of an application policy.
B. The Allow All IPv6 option in the policy was selected.
C. The policy was misconfigured and allowed all Layer 2 broadcast traffic.
D. The VM was using a static IPv6 address.

Answer: B

Explanation:
From a Nutanix exam perspective, this question is really testing whether the administrator understands the control point that actually governs the behavior shown in the scenario. The correct response is B, meaning “The Allow All IPv6 option in the policy was selected.”. An Isolation Policy is built to stop communication between defined groups. Unlike an application policy, it is intended to create a hard boundary, making it the correct choice when the requirement is “no traffic between these entities.” Application Policies are the most appropriate way to model legitimate workload communication in a tiered application. They allow administrators to express which sources, destinations, and services are required instead of relying on broad network access. This is a Flow policy design question, so categories, secured entities, rule direction, policy mode, and policy precedence matter more than simple IP connectivity assumptions. Seen from a design perspective, the correct answer is the least ambiguous and most supportable implementation path inside Prism Central and AHV. Notice that A sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. C sounds plausible, but it does not align with the specific.

Question: 2

An administrator has two user VPCs connected via a Transit VPC. Routing works for most subnets, but one overlay subnet cannot reach external networks. What is the most probable cause?

A. Incorrect ASN in the BGP configuration in the Transit VPC
B. Mismatch in ERP configuration in user and Transit VPC
C. Floating IP not assigned to the gateway
D. DHCP configuration is disabled on the overlay subnet in the user VPC

Answer: B

Explanation:

What makes this a strong certification question is that several answers look technically related, but only one aligns with the exact behavior of Flow networking or Flow security. The correct response is B, meaning “Mismatch in ERP configuration in user and Transit VPC”. A Floating IP is the normal mechanism for exposing a workload in an overlay-backed VPC to external clients. It preserves internal VM addressing while publishing a reachable external address through the VPC’s north-south path. Externally Routable Prefixes determine which overlay prefixes are advertised beyond the VPC. If the ERP does not cover the workload subnet, upstream devices never learn a valid return path, even when the local VPC appears healthy. Operationally, Flow Virtual Networking should be checked from the control plane outward: gateway health, peering state, route advertisement, ERP coverage, external path, and MTU when encapsulation is involved. By contrast, A does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. C addresses exposure of a single VM, not the broader routing or security behavior under discussion. Seen operationally, the correct response is the least disruptive and most deterministic.

Question: 3

While configuring a new security policy in a Nutanix microsegmentation environment, an administrator wants the policy to remain flexible even if virtual machines change subnets or obtain new IP addresses. Which configuration approach should the administrator use when defining the policy scope?

A. Configure the policy only on specific VLAN IDs.
B. Use VM categories to define the secured and allowed entities.
C. Apply the policy after setting static routes for each VM.
D. Assign IP addresses manually to all VMs included in the policy.

Answer: B

Explanation:
This item is best solved by thinking like an operator in Prism Central: first identify whether the problem is design, control-plane state, or policy logic, then pick the option tied to that layer. The correct response is B, meaning “Use VM categories to define the secured and allowed entities.”. The winning option is the one tied to the native Nutanix object or control that governs the outcome described in the scenario. This is a Flow policy design question, so categories, secured entities, rule direction, policy mode, and policy precedence matter more than simple IP connectivity assumptions. A strong exam habit is to ask which Nutanix construct would have to change for the symptom or requirement to change. That mental shortcut usually separates the real answer from distractors that mention generic networking steps, disruptive resets, or unrelated configuration objects. Notice that A sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. C sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. In practice, administrators who anchor their decisions to Prism Central constructs—such as VPCs,.

Question: 4

An administrator has observed the following message: Which two statements most accurately describe the security hitlog captured above? (Choose two.)

A. This is a security hit log on the rule name "Production-External-WebTier".
B. The source ip address is 10.38.174.5 and source port is TCP/123.
C. 86.108.190.23 is sending a packet on UDP 123.
D. 10.38.174.57 is sending a packet destined to UDP 123.

Answer: B, D

Explanation:
What makes this a strong certification question is that several answers look technically related, but only one aligns with the exact behavior of Flow networking or Flow security. The correct response is BD, which corresponds to The source ip address is 10.38.174.5 and source port is TCP/123. and 10.38.174.57 is sending a packet destined to UDP 123.. Policy hitlogs provide precise evidence of what Flow evaluated, including source, destination, protocol, and rule outcome. In troubleshooting, that makes hitlogs one of the best places to confirm whether traffic matched an allow or deny decision. From a troubleshooting standpoint, the validation path is policy scope first, then categories or identity mapping, then hitlog evidence, service definition, and finally policy precedence. Seen from a design perspective, the correct answer is the least ambiguous and most supportable implementation path inside Prism Central and AHV. Notice that A does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. C does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. The key takeaway is that.

Question: 5

While configuring third-party services (Service Insertion) in Flow Network Security Next-Gen, an administrator notices dropped packets when redirecting traffic through a network function. Which configuration change would address this issue?

A. Reduce the MTU size to 1400 to match Geneve encapsulation.
B. Disable Geneve tunneling on the virtual switch.
C. Increase the MTU by an additional 58 bytes for the Geneve header.
D. Keep the default MTU at 1500. Encapsulation is handled automatically.

Answer: C

Explanation:
The most professional way to evaluate this question is to map the symptom to the Nutanix feature responsible for that function rather than reacting to secondary details in the prompt. The correct response is C, meaning “Increase the MTU by an additional 58 bytes for the Geneve header.”. MTU planning matters because encapsulation adds overhead. When overlay, Geneve, VXLAN, or IPSec is present, a path that looks healthy at 1500 bytes can still fragment or drop larger frames unless the underlay and endpoints are sized correctly. Service insertion introduces an additional dataplane hop through a network function VM. That makes correct vNIC pairing, health monitoring, and MTU sizing essential, because steering can fail even when the firewall appliance itself appears powered on. This is a Flow policy design question, so categories, secured entities, rule direction, policy mode, and policy

precedence matter more than simple IP connectivity assumptions. In other words, this is less about broad infrastructure suspicion and more about finding the exact Nutanix decision point that explains the behavior. Notice that A does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome.

Question: 6

What happens when a monitored policy is enforced?

A. Stops logging traffic
B. Blocks all traffic that is not allowed
C. Deletes the policy hitlogs
D. Removes all discovered flows

Answer: B

Explanation:
What makes this a strong certification question is that several answers look technically related, but only one aligns with the exact behavior of Flow networking or Flow security. The correct response is B, meaning “Blocks all traffic that is not allowed”. Policy hitlogs provide precise evidence of what Flow evaluated, including source, destination, protocol, and rule outcome. In troubleshooting, that makes hitlogs one of the best places to confirm whether traffic matched an allow or deny decision. This is a Flow policy design question, so categories, secured entities, rule direction, policy mode, and policy precedence matter more than simple IP connectivity assumptions. By contrast, A does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. C does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. The key takeaway is that Flow is intentionally modular. Networking objects determine reachability, security objects determine permission, and lifecycle steps determine supportability. Mixing those layers usually produces the distractor answers. A strong exam habit is to ask which Nutanix construct would have to.

Question: 7

In Nutanix Flow, which action transitions a security policy from observing traffic to actively enforcing the rules?

A. Disable Traffic Visualization for the policy.
B. Enforce policy by setting its scope.
C. Change policy mode from Monitor to Save.
D. Change policy mode from Monitor to Enforce.

Answer: D

Explanation:
The clean way to read this scenario is to separate what is merely present in the environment from the single Nutanix construct that actually satisfies the requirement. The correct response is D, meaning

“Change policy mode from Monitor to Enforce.”. The winning option is the one tied to the native Nutanix object or control that governs the outcome described in the scenario. This is a Flow policy design question, so categories, secured entities, rule direction, policy mode, and policy precedence matter more than simple IP connectivity assumptions.
Seen from a design perspective, the correct answer is the least ambiguous and most supportable implementation path inside Prism Central and AHV. Notice that A sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. B sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. For exam preparation, remember that Nutanix usually separates discovery from enforcement, routing from NAT, and access policy from identity mapping. Choosing the layer that truly owns the function is what leads to the right answer.

Question: 8

How can the administrator discover the root cause of the issue?

A. Confirm that Inter-VM connectivity is enabled within the VM networking settings and that VMs in the Database tier are configured correctly to accept inbound traffic.
B. Check if traffic isolation has been configured on the Database tier and ensure that there is no policy preventing App tier communication with the Database tier.
C. Check the security policies again to ensure that the rule allowing port 3306 from Web - > Database is applied and active, then check the policy enforcement mode to ensure it is in Enforcement Mode.
D. Verify that the port 3306 is open on the external gateway and that SNAT is not being applied for internal communication.

Answer: C

Explanation:
A reliable method here is to translate the scenario into Nutanix terms—VPC routing, external connectivity, policy scope, identity mapping, or upgrade readiness—and then choose the answer that directly addresses that domain. The correct response is C, meaning “Check the security policies again to ensure that the rule allowing port 3306 from Web - > Database is applied and active, then check the policy enforcement mode to ensure it is in Enforcement Mode.”. The winning option is the one tied to the native Nutanix object or control that governs the outcome described in the scenario. From a troubleshooting standpoint, the validation path is policy scope first, then categories or identity mapping, then hitlog evidence, service definition, and finally policy precedence. Seen from a design perspective, the correct answer is the least ambiguous and most supportable implementation path inside Prism Central and AHV. Notice that A does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. B sounds plausible, but it does not align with the specific Flow policy object or precedence rule that controls this case. The key takeaway is that Flow is intentionally.

Question: 9

An administrator is building a VPC... VPC CIDR: 10.10.0.0/16 Subnet CIDR: 10.10.10.0/24 "Ext_Net_Ext" (NAT): 192.168.1.0/24 "Ext_Net_Internal" (Routed): 172.16.1.0/24 The on-premises application server

has an IP address of 172.16.2.50/24. A VM (10.10.10.100) in the VPC Subnet can reach the internet but cannot reach the on-premises server. Which static route needs to be added to the VPC route table to resolve this?

A. Destination prefix: 172.16.2.0/24, Next-Hop: Ext_Net_Ext
B. Destination Prefix: 10.10.0.0/16, Next-Hop: Ext_Net_Internal
C. Destination prefix: 192.168.1.0/24 Next-Hop: Ext_Net_Ext
D. Destination prefix: 172.16.2.0/24, Next-Hop: Ext_Net_Internal

Answer: D

Explanation:
The most professional way to evaluate this question is to map the symptom to the Nutanix feature responsible for that function rather than reacting to secondary details in the prompt. The correct response is D, meaning “Destination prefix: 172.16.2.0/24, Next-Hop: Ext_Net_Internal”. The winning option is the one tied to the native Nutanix object or control that governs the outcome described in the scenario. Operationally, Flow Virtual Networking should be checked from the control plane outward: gateway health, peering state, route advertisement, ERP coverage, external path, and MTU when encapsulation is involved.
Seen from a design perspective, the correct answer is the least ambiguous and most supportable implementation path inside Prism Central and AHV. Notice that A is not appropriate because NAT changes addressing behavior and does not solve the routing or policy condition described in the scenario. B is not appropriate because NAT changes addressing behavior and does not solve the routing or policy condition described in the scenario. Seen operationally, the correct response is the least disruptive and most deterministic one. It changes the exact Nutanix setting that governs the outcome instead of introducing workarounds elsewhere in the stack.

Question: 10

An administrator notices that several VMs in a Nutanix AHV cluster are intermittently losing network connectivity. In Prism Central, a critical alert appears: "Network Function VM (NFVM) packet processing delays" What is the next step that the administrator should take for this issue?

A. Review the Alerts and Events in Prism Central to confirm if the affected host shows NIC or uplink errors.
B. Reboot the affected VMs to re-establish virtual NIC connections.
C. Increase the MTU size on all virtual switches to improve packet throughput.
D. Disable all Flow policies on the cluster to eliminate microsegmentation as the cause.

Answer: A

Explanation:
A reliable method here is to translate the scenario into Nutanix terms—VPC routing, external connectivity, policy scope, identity mapping, or upgrade readiness—and then choose the answer that directly addresses that domain. The correct response is A, meaning “Review the Alerts and Events in Prism Central to confirm if the affected host shows NIC or uplink errors.”. MTU planning matters

because encapsulation adds overhead. When overlay, Geneve, VXLAN, or IPSec is present, a path that looks healthy at 1500 bytes can still fragment or drop larger frames unless the underlay and endpoints are sized correctly. Operationally, Flow Virtual Networking should be checked from the control plane outward: gateway health, peering state, route advertisement, ERP coverage, external path, and MTU when encapsulation is involved.

Notice that B is a disruptive action and does not address the actual control-plane or policy requirement being tested. C does not fit because it targets a different layer of the Nutanix networking and security stack than the one causing the outcome here. The key takeaway is that Flow is intentionally modular. Networking objects determine reachability, security objects determine permission, and lifecycle steps determine supportability. Mixing those layers usually produces the distractor answers.

Visit us at: https://www.examsboost.com/test/ncp-ns-7-5

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer