Exam Questions 2V0-41.24

VMware NSX 4.X Professional V2

https://www.2passeasy.com/dumps/2V0-41.24/

NEW QUESTION 1
An administrator has connected two virtual machines on the same overlay segment. Ping between both virtual machines is successful.
What type of network boundary does this represent?

A. Layer 2 bridge
B. Layer 2 broadcast domain
C. Layer 2 VPN
D. Layer 3 route

Answer: B

Explanation:
When two virtual machines are connected on the same overlay segment, they are part of the same Layer 2 broadcast domain. In this case, the communication between the two VMs is happening within the same broadcast domain, which means that broadcast traffic can be sent to all devices on the segment. Since the ping is successful, the two VMs can communicate directly over Layer 2 without needing routing.

NEW QUESTION 2
Which of the following settings must be configured in an NSX environment before enabling stateful active-active SNAT?

A. Tier-1 gateway in active-standby mode
B. A Punting Traffic Group for the NSX Edge uplinks
C. An Interface Group for the NSX Edge uplinks
D. Tier-1 gateway in distributed only mode

Answer: B

Explanation:
In an NSX environment, a Punting Traffic Group for the NSX Edge uplinks must be configured before enabling stateful active-active Source NAT (SNAT). This configuration ensures that traffic is appropriately handled and forwarded between the NSX Edge nodes in an active-active setup, allowing stateful connections to be maintained across multiple Edge nodes.

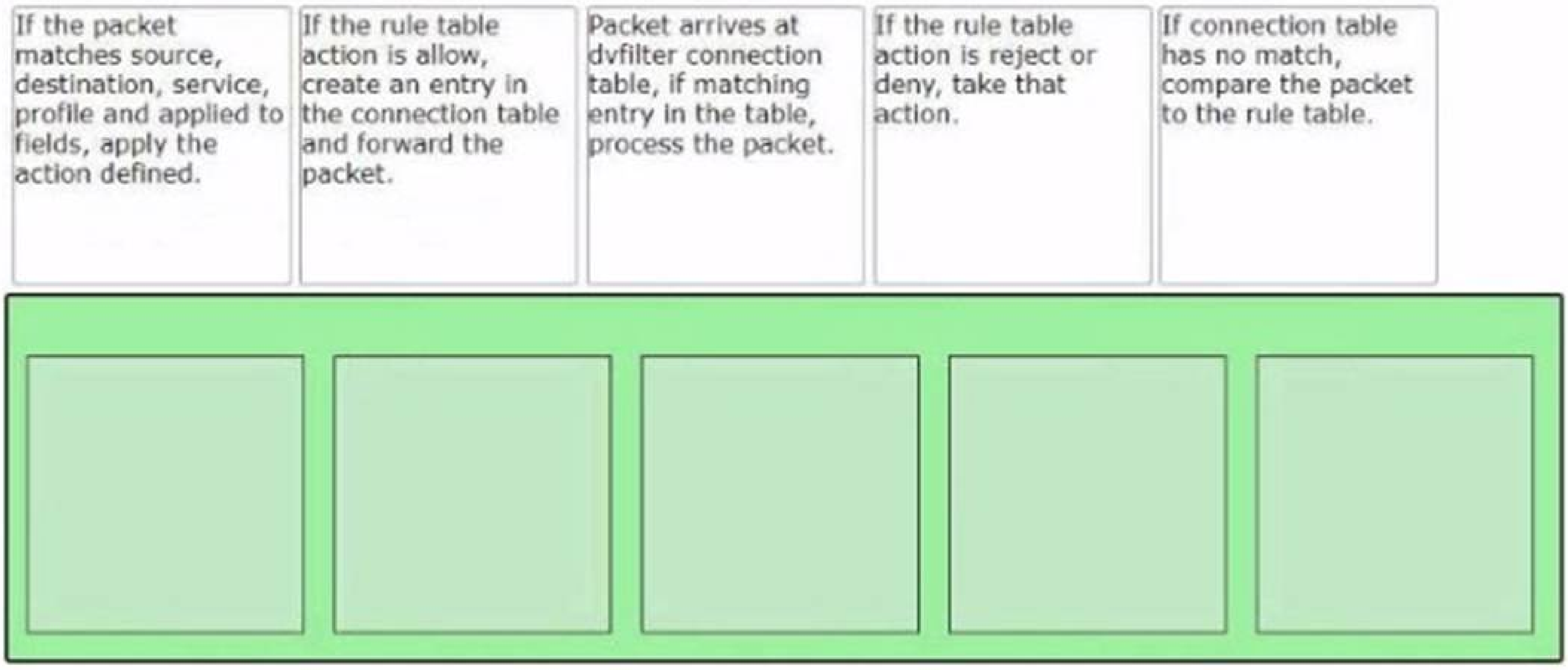
NEW QUESTION 3
An NSX administrator is creating a NAT rule on a Tier-0 Gateway configured in active- standby high availability mode.
Which two NAT rule types are supported for this configuration? (Choose two.)

A. Port NAT
B. 1:1 NAT
C. Destination NAT
D. Reflexive NAT
E. Source NAT

Answer: C

Explanation:
In an NSX environment with a Tier-0 Gateway configured in active-standby high availability mode, Destination NAT (DNAT) and Source NAT (SNAT) are supported NAT rule types. These allow for traffic redirection by modifying the destination or source IP addresses as needed, which is commonly used in configurations involving external access and internal IP address translation.

NEW QUESTION 4
DRAG DROP
Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct order of the rule processing steps of the Distributed Firewall is as follows:
? Packet arrives at vfilter connection table. If matching entry in the table, process the packet.
? If connection table has no match, compare the packet to the rule table.
? If the packet matches source, destination, service, profile and applied to fields, apply the action defined.
? If the rule table action is allow, create an entry in the connection table and forward the packet.
? If the rule table action is reject or deny, take that action.
This order is based on the description of how the Distributed Firewall works in the web search results1. The first step is to check if there is an existing connection entry for the packet in the vfilter connection table, which is a cache of flow entries for rules with an allow action. If there is a match, the packet is processed according to the connection entry. If there is no match, the packet is compared to the rule table, which contains all the security policy rules. The rules are evaluated from top to bottom until a match is found. The match criteria include source, destination, service, profile and applied to fields. The action defined by the matching rule is applied to the packet. The action can be allow, reject or deny. If the action is allow, a new connection entry is created for the packet and the packet is forwarded to its destination. If the action is reject or deny, the packet is dropped and an ICMP message or a TCP reset message is sent back to the source.

NEW QUESTION 5
Which troubleshooting step will resolve an error with code 1001 during the configuration of a time-based firewall rule?

A. Restarting the NTPservice on the ESXi host.
B. Reconfiguring the ESXi host with a local NTP server.
C. Re-installing the NSX VIBs on the ESXi host.
D. Changing the time zone on the ESXi host.

Answer: A

Explanation:
An error with code 1001 during the configuration of a time-based firewall rule often indicates a time synchronization issue. Restarting the NTP service on the ESXi host can resolve this issue by ensuring that the host??s time is synchronized correctly, which is essential for time-based rules to function accurately.

NEW QUESTION 6
Which two BGP configuration parameters can be configured in the VRF Lite gateways? (Choose two.)

A. Route Aggregation
B. Route Distribution
C. BGP Neighbors
D. Graceful Restart
E. Local AS

Answer: CE

Explanation:
BGP Neighbors: This parameter is essential for establishing BGP sessions with other routers. Configuring BGP neighbors allows VRF Lite gateways to exchange routing information with adjacent BGP-enabled devices.
Local AS: The Local Autonomous System (AS) number can be set for the VRF Lite gateway, which is necessary for BGP operations within a specific routing domain.

NEW QUESTION 7
Which CLI command on NSX Manager and NSX Edge is used to change NTP settings?

A. set timezone
B. set ntp-server
C. get timezone
D. get time-server

Answer: B

Explanation:
The set ntp-server command is used on NSX Manager and NSX Edge to configure the NTP (Network Time Protocol) settings. This command allows administrators to specify the NTP server, ensuring that the NSX components synchronize their time accurately with the designated time server.

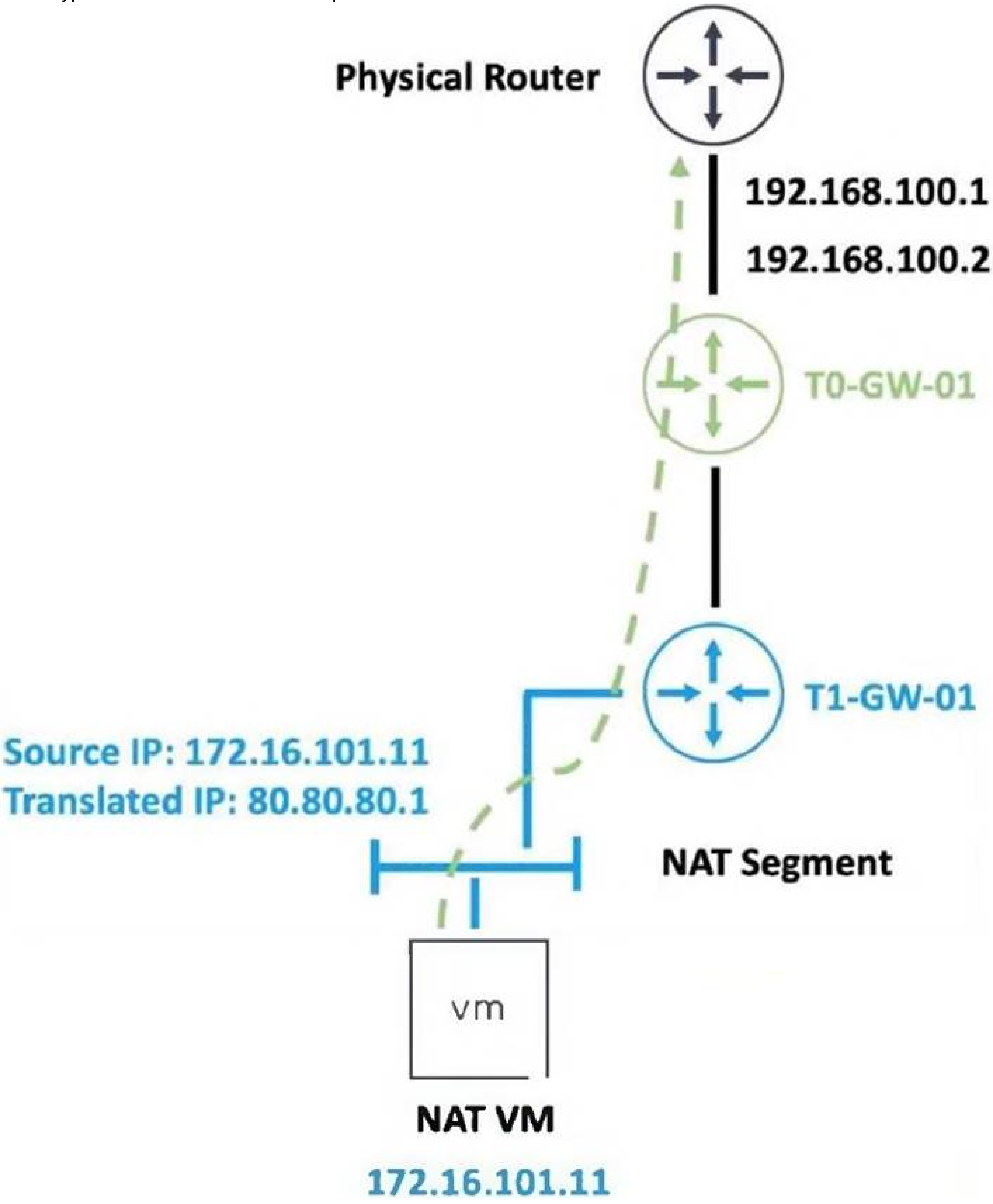
NEW QUESTION 8
What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

A. It collects real-time analytics from application traffic flows.
B. It stores the configuration and policies related to load-balancing services.
C. It performs application load-balancing operations.
D. It deploys web servers to perform load-balancing operations.
E. It provides a user interface to perform configuration and management tasks.

Answer: AC

Explanation:
Reference: https://docs.vmware.com/en/VMware-NSX-Advanced-Load- Balancer/22.1/Administration_Guide/GUID-84139C37-0129-40A7-A7AB-5A93E1F65B6D.html

NEW QUESTION 9
Refer to the exhibit.
An administrator would like to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network.
Which type of NAT solution should be implemented to achieve this?

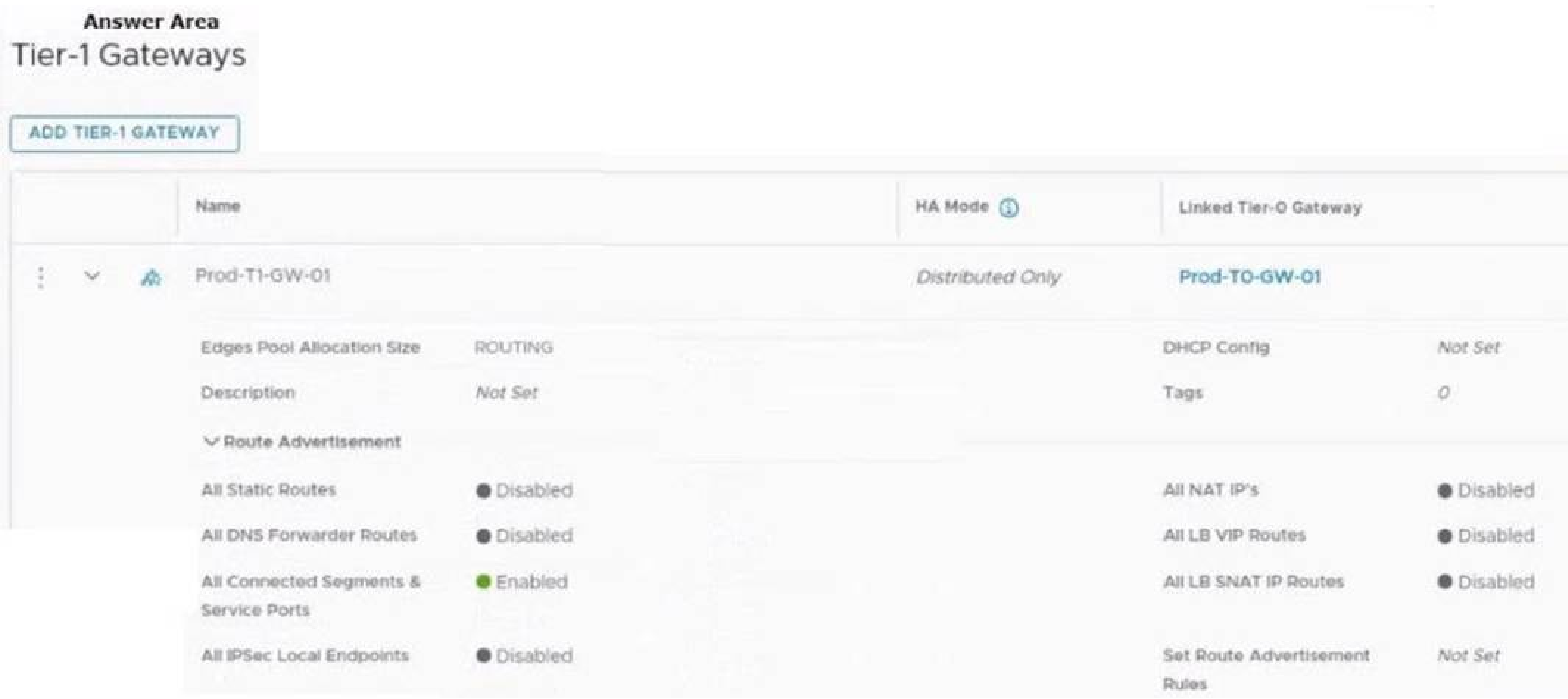


A. NAT64
B. Reflexive NAT
C. DNAT
D. SNAT

Answer: D

Explanation:
Source NAT (SNAT) is used to translate the private IP address (172.16.101.11) of the NAT VM to a public IP address (80.80.80.1) as the packets leave the NAT-Segment network. SNAT changes the source IP of outbound packets, allowing private IP addresses within the internal network to be mapped to public IP addresses for communication with external networks.

NEW QUESTION 10
HOTSPOT
Refer to the exhibit.
An administrator configured NSX Advanced Load Balancer to load balance the production web server traffic, but the end users are unable to access the production website by using the VIP address.
Which of the following Tier-1 gateway route advertisement settings needs to be enabled to resolve the problem? Mark the correct answer by clicking on the image.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct answer is to enable the option All LB VIP Routes on the Tier-1 gateway route advertisement settings. This option allows the Tier-1 gateway to advertise the NSX Advanced Load Balancer LB VIP routes to the Tier-0 gateway and other peer routers, so that the end users can reach the production website by using the VIP address1. The other options are not relevant for this scenario.
To mark the correct answer by clicking on the image, you can click on the toggle switch next to All LB VIP Routes to turn it on. The switch should change from gray to blue, indicating that the option is enabled. See the image below for reference:

NEW QUESTION 10
Which NSX CLI command is used to change the authentication policy for local users?

A. set hardening-policy
B. get auth-policy minimum-password-length
C. set cli-timeout
D. set auth-policy

Answer: D

Explanation:
The set auth-policy command in the NSX CLI is used to configure the authentication policy for local users. This command allows administrators to adjust settings related to password policies, lockout policies, and other authentication-related parameters for local user accounts on NSX Manager.

NEW QUESTION 13
Which NSX feature can be leveraged to achieve consistent policy configuration and simplicity across sites?

A. VRF Lite
B. Ethernet VPN
C. NSX MTML5 UI
D. NSX Federation

Answer: D

Explanation:
According to the VMware NSX Documentation, this is the NSX feature that can be leveraged to achieve consistent policy configuration and simplicity across sites:
? NSX Federation: This feature allows you to create and manage a global network infrastructure that spans across multiple sites using a single pane of glass. You can use this feature to synchronize policies, segments, gateways, firewalls, VPNs, load balancers, and other network services across sites.

NEW QUESTION 16
What are three NSX Manager roles? (Choose three.)

A. master
B. manager
C. controller
D. cloud
E. policy
F. zookeeper

Answer: ACF

Explanation:
master: The master role in NSX Manager is responsible for managing and coordinating the other NSX Manager nodes in the cluster.
policy: The policy role handles the policy-driven API and configuration, allowing administrators to define and manage network and security policies.
controller: The controller role in NSX Manager manages control plane functions and handles routing, switching, and other network state information required for NSX operations.

NEW QUESTION 20
The security administrator turns on logging for a firewall rule. Where is the log stored on an ESXi transport node?

A. /var/log/messages.log
B. /var/log/vmware/nsx/firewall.log
C. /var/log/fw.log
D. /var/log/dfwpktlogs.log

Answer: D

Explanation:
When logging is enabled for a firewall rule in NSX, the logs are stored on the ESXi transport node in the /var/log/vmware/nsx/firewall.log file. This file contains information about firewall rule hits and is useful for monitoring and troubleshooting firewall activity on the transport node.

NEW QUESTION 23
An NSX administrator is troubleshooting a connectivity issue with virtual machines running on an ESXi transport node.
Which feature in the NSX UI shows the mapping between the virtual NIC and the host??s physical adapter?

A. Port Mirroring
B. Activity Monitoring
C. IPF1X
D. Switch Visualization

Answer: D

Explanation:
Switch Visualization in the NSX UI provides a clear mapping between virtual NICs (vNICs) and the physical adapters on the host. This feature allows administrators to see how virtual network interfaces connect to the underlying physical network infrastructure, which is essential for troubleshooting connectivity issues on transport nodes.

NEW QUESTION 28
Which two are requirements for FQDN Analysis? (Choose two.)

A. The NSX Edge nodes require access to the Internet to download category and reputation definitions.
B. ESXi control panel requires access to the Internet to download category and reputation definitions.
C. The NSX Manager requires access to the Internet to download category and reputation definitions.
D. A layer 7 gateway firewall rule must be configured on the Tier-1 gateway uplink.
E. A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Answer: AD

Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-C5CD87FD-8095-49F3-97CE-E606AB89162E.html?hWord=N4IghgNiBcIGYEcAmA7ABGFkCeBnAlriAL5A

NEW QUESTION 32
Which two statements are true for IPSec VPN? (Choose two.)

A. IPSec VPN services can be configured at Tier-0 and Tier-1 gateways.
B. Dynamic routing is supported for any IPSec mode in NSX.
C. IPSec VPNs use the DPDK accelerated performance library.
D. VPNs can be configured on the command line interface on the NSX manager.

Answer: AC

Explanation:
IPSec VPN services can be configured at Tier-0 and Tier-1 gateways: In NSX, IPSec VPN services can be applied to both Tier-0 and Tier-1 gateways, allowing secure site-to-site connections from these gateway levels.
IPSec VPNs use the DPDK accelerated performance library: NSX leverages the Data Plane Development Kit (DPDK) for optimized performance, which accelerates packet processing for IPSec VPNs and improves throughput.

NEW QUESTION 36
Which of the two following characteristics about NAT64 are true? (Choose two.)

A. NAT64 requires the Tier-1 gateway to be configured in active-active mode.
B. NAT64 is stateless and requires gateways to be deployed in active-standby mode.
C. NAT64 is supported on Tier-0 and Tier-1 gateways.
D. NAT64 is supported on Tier-1 gateways only.
E. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.

Answer: CE

Explanation:
NAT64 is supported on both Tier-0 and Tier-1 gateways, allowing for IPv6-to-IPv4 address translation at different gateway levels within NSX.
NAT64 requires the Tier-1 gateway to be configured in active-standby mode, as this configuration ensures stateful translation and consistency for IPv6-to-IPv4 traffic handling.

NEW QUESTION 40
NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

A. Network Segmentation
B. Virtual Security Zones
C. Edge Firewalling
D. Dynamic Routing

Answer: A

Explanation:
According to the web search results, network segmentation is a feature of NSX that improves the security of today??s modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting vulnerabilities or credentials . Network segmentation prevents lateral movement by dividing a network into smaller segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot access other segments or resources . NSX enables network segmentation by using micro-segmentation, which applies granular firewall rules at the virtual machine level, regardless of the physical network topology .

NEW QUESTION 45
An administrator is configuring service insertion for Network Introspection. Which two places can the Network Introspection be configured? (Choose two.)

A. Edge Node
B. Host pNIC
C. Tier-0 gateway
D. Tier-1 gateway
E. Partner SVM

Answer: DE

Explanation:
Tier-1 gateway: Network introspection services can be configured at the Tier-1 gateway level to inspect and control East-West traffic between workloads.
Partner SVM (Service Virtual Machine): Network introspection is often implemented through integration with a Partner SVM, which is a virtual machine provided by a third-party security partner to perform deep packet inspection and other security functions.

NEW QUESTION 47
An NSX administrator is reviewing syslog and notices that Distributed Firewall Rules hit counts are not being logged.
What could cause this issue?

A. Zero Trust Security is not enabled.
B. Syslog is not configured on the NSX Manager.
C. Syslog is not configured on the ESXi transport node.
D. Distributed Firewall Rule logging is not enabled.

Answer: D

Explanation:
If Distributed Firewall Rule hit counts are not being logged, it is likely because Distributed Firewall Rule logging is not enabled. For hit counts to appear in the logs, logging must be explicitly enabled on each firewall rule where tracking is required. Without enabling logging at the rule level, no hit count information will be recorded in syslog.

NEW QUESTION 52
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events.
Which message ID (msgid) should be used in the syslog export configuration command as a filter?

A. FABRIC
B. SYSTEM
C. GROUPING
D. MONITORING

Answer: A

Explanation:
In NSX, the FABRIC message ID is used to capture and export syslog events related to host preparation and other fabric-related activities. These events are important for tracking and troubleshooting the setup and configuration of NSX components across the fabric, including host preparation events.

NEW QUESTION 57
Which three security features are dependent on the NSX Application Platform? (Choose three.)

A. NSX Intelligence
B. NSX Firewall
C. NSX Network Detection and Response
D. NSX TLS Inspection
E. NSX Distributed IDS/IPS

F. NSX Malware Prevention

Answer: ACF

Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-42EDE0AD-CD65-41AC-9694-AD0CCEC35969.html

NEW QUESTION 62
What are the four types of role-based access control (RBAC) permissions? (Choose four.)

A. Auditor
B. Full access
C. Enterprise Admin
D. None
E. Execute
F. Read
G. Network Admin

Answer: ABDF

Explanation:
Auditor: Allows users to view settings and logs without making changes.
Full access: Provides complete control over all NSX settings and configurations. None: No permissions are granted, restricting access completely.
Read: Allows users to view configurations and settings without editing capabilities.

NEW QUESTION 64
In an NSX environment, an administrator is observing low throughput and congestion between the Tier-0 Gateway and the upstream physical routers.
Which two actions could address low throughput and congestion? (Choose two.)

A. Configure ECMP on the Tier-0 gateway.
B. Configure a Tier-1 gateway and connect it directly to the physical routers.
C. Deploy Large size Edge node/s.
D. Configure NAT on the Tier-0 gateway.
E. Add an additional vNIC to the NSX Edge node.

Answer: AC

Explanation:
Configure ECMP on the Tier-0 gateway: ECMP (Equal-Cost Multi-Path) allows multiple paths for traffic between the Tier-0 Gateway and the upstream physical routers, effectively distributing the traffic load and improving throughput. By enabling ECMP, you can reduce congestion and increase bandwidth utilization, thus addressing performance issues. Deploy Large size Edge node/s: Deploying larger Edge nodes can provide more resources (CPU, memory, and network interfaces) to handle higher throughput and reduce congestion. This is especially important if the existing Edge node is overwhelmed by the amount of traffic.

NEW QUESTION 67
What are four NSX built-in role-based access control (RBAC) roles? (Choose four.)

A. None
B. Read
C. Auditor
D. Full Access
E. Network Admin
F. Enterprise Admin
G. Operator

Answer: ABCD

Explanation:
None: No permissions are granted, restricting the user??s access entirely.
Read: Grants read-only access, allowing the user to view configurations and settings without making changes.
Auditor: Similar to Read, but typically includes access to audit logs and more detailed viewing permissions for compliance purposes.
Full Access: Grants complete control over all NSX configurations and settings, allowing unrestricted access.

NEW QUESTION 72
Which steps are required to activate Malware Prevention on the NSX Application Platform?

A. Select Cloud Region and Deploy Network Detection and Response.
B. Activate NSX Network Detection and Response and run Pre-checks.
C. Activate NSX Network Detection and Response and Deploy Malware Prevention.
D. Select Cloud Region and run Pre-checks.

Answer: D

Explanation:
To activate Malware Prevention on the NSX Application Platform, the steps are:
? In the NSX Manager UI, select System and in the Configuration section, select NSX Application Platform.
? Navigate to the Features section, locate the NSX Malware Prevention feature card, and click Activate or anywhere in the card.
? In the NSX Malware Prevention activation window, select one of the available cloud regions from which you can access the NSX Advanced Threat Prevention cloud service.

? Click Run Prechecks. This precheck process can take some time as the system validates that the minimum license requirement is met and that it is eligible for use with the NSX Advanced Threat Prevention cloud service. The system also validates that the selected cloud region is reachable.
? Click Activate. This step can take some time1. Therefore, the correct answer is D. The other options are incorrect because they involve activating or deploying NSX Network Detection and Response, which is a different feature from Malware Prevention. References: Activate NSX Malware Prevention

NEW QUESTION 74
What are two valid BGP Attributes that can be used to influence the route path traffic will take? (Choose two.)

A. AS-Path Prepend
B. BFD
C. Cost
D. MED

Answer: AD

Explanation:
? AS-Path Prepend: This attribute allows you to prepend one or more AS numbers to the AS path of a route, making it appear longer and less preferable to other BGP routers. You can use this attribute to manipulate the inbound traffic from your BGP peers by advertising a longer AS path for some routes and a shorter AS path for others.
? MED: This attribute stands for Multi-Exit Discriminator and allows you to specify a preference value for a route among multiple exit points from an AS. You can use this attribute to manipulate the outbound traffic to your BGP peers by advertising a lower MED value for some routes and a higher MED value for others.

NEW QUESTION 79
Which two are supported by L2 VPN clients? (Choose two.)

A. NSX Autonomous Edge
B. NSX Edge
C. NSX for vSphere Edge
D. 3rd party Hardware VPN Device

Answer: BD

Explanation:
The NSX Edge supports L2 VPN (Layer 2 VPN) functionality, which allows it to connect different Layer 2 networks over an IP transport.
Third-party hardware VPN devices can also be used as L2 VPN clients, providing connectivity between different Layer 2 networks through an external device.

NEW QUESTION 80
Which CLI command is used for packet capture on the ESXi Node?

A. tcpdump
B. set capture
C. pktcap-uw
D. debug

Answer: C

Explanation:
The pktcap-uw command is specifically used on ESXi hosts for packet capture. It provides a detailed packet capture utility that allows administrators to capture traffic at various points on the ESXi host, such as virtual switches, uplinks, and VMkernel interfaces, making it a powerful tool for network troubleshooting on ESXi nodes.

NEW QUESTION 83
Which VMware NSX Portfolio product can be described as a distributed analysis solution that provides visibility and dynamic security policy enforcement for NSX environments?

A. NSX Manager
B. NSX Distributed IDS/IPS
C. NSX Intelligence
D. NSX Cloud

Answer: C

Explanation:
NSX Intelligence is a distributed analytics solution within the VMware NSX Portfolio that provides visibility and dynamic security policy enforcement in NSX environments. It enables detailed traffic analysis, identifies security threats, and helps in the automated creation and enforcement of security policies based on observed network traffic patterns and behaviors.

NEW QUESTION 85
Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

A. The option to set time-based rule is a clock Icon in the rule.
B. The option to set time based rule is a field in the rule Itself.
C. There Is no option in the NSX U
D. It must be done via command line interface.
E. The option to set time-based rule is a clock Icon in the policy.

Answer:

D

Explanation:
According to the VMware documentation1, the clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time- based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface. https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC80BE7.html

NEW QUESTION 87
What are four NSX built-in rote-based access control (RBAC) roles? (Choose four.)

A. Network Admin
B. Enterprise Admin
C. Full Access
D. Read
E. LB Operator
F. None
G. Auditor

Answer: ABEG

Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-26C44DE8-1854-4B06-B6DA-A2FD426CDF44.html

NEW QUESTION 89
An NSX administrator is creating a Tier-1 Gateway configured in Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original failed node to become the Active node upon recovery.
Which failover policy meets this requirement?

A. Enable Preemptive
B. Non-Preemptive
C. Preemptive
D. Disable Preemptive

Answer: B

Explanation:
In Non-Preemptive failover policy, once a failover occurs and a new Active node is designated, the original failed node will not automatically become the Active node upon recovery. This setting ensures that the failover does not revert to the original node after it comes back online, maintaining the stability of the network by keeping the current Active node as is.

NEW QUESTION 94
Which TraceFlow traffic type should an NSX administrator use for validating connectivity between App and DB virtual machines that reside on different segments?

A. Anycast
B. Multicast
C. Broadcast
D. Unicast

Answer: B

Explanation:
In NSX, Unicast traffic type should be used in TraceFlow when validating connectivity between two specific virtual machines, such as App and DB VMs, that reside on different segments. Unicast traffic is directed from one source to a single destination, making it suitable for testing direct connectivity between two VMs.

NEW QUESTION 98
When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

A. Core Files
B. Controller Files
C. Audit Files
D. Management Files

Answer: A

Explanation:
Core Files should be excluded when collecting support bundles through NSX Manager because they may contain sensitive information, such as memory dumps that could reveal sensitive data from processes at the time of an issue. Excluding core files helps ensure that potentially sensitive data is not unintentionally shared.

NEW QUESTION 101
In which VPN type are the Virtual Tunnel interfaces (VTI) used?

A. SSL-based VPN
B. Route & SSL based VPNs
C. Policy & Route based VPNs

D. Route-based VPN

Answer: D

Explanation:
Virtual Tunnel Interfaces (VTI) are used in route-based VPNs. In this type of VPN, the tunnel is treated like a regular interface on the router. This allows for the configuration of routing protocols and the application of routing decisions to the traffic flowing through the VPN tunnel. VTIs simplify the management of routing and make it more flexible in VPN scenarios.

NEW QUESTION 104
When running nsxcli on an ESXi host, which command will show the Replication mode?

A. get logical-switch <Local-Switch-UUID> status
B. get logical-switch <Logical-Switch-UUID>
C. get logical-switches
D. get logical-switch status

Answer: C

Explanation:
https://vdc-download.vmware.com/vmwb-repository/dcr-public/c3fd9cef-6b2b-4772-93be-3fe60ce064a1/1f67b9e1-b111-4de7-9ea1-39931d28f560/NSX-T%20Command-Line%20Interface%20Reference.html#get%20logical- switch%20%3Clogical-switch-id%3E

NEW QUESTION 109
Which two steps must an NSX administrator take to integrate VMware Identity Manager in NSX to support role-based access control? (Choose two.)

A. Create a SAML authentication in VMware Identity Manager using the NSX Manager FQDN.
B. Add NSX Manager as a Service Provider (SP) in VMware Identity Manager.
C. Enter the Identity Provider (IdP) metadata URL in NSX Manager.
D. Enter the service URL, Client Secret, and SSL thumbprint in NSX Manager.
E. Create an OAuth 2.0 client in VMware Identity Manager.

Answer: BC

Explanation:
Adding NSX Manager as a Service Provider (SP) in VMware Identity Manager is necessary to enable SAML-based single sign-on (SSO), which allows VMware Identity Manager to manage and authenticate users accessing NSX.
Entering the Identity Provider (IdP) metadata URL in NSX Manager is required to establish a connection between NSX and VMware Identity Manager, enabling NSX to use VMware Identity Manager as the IdP for authentication.

NEW QUESTION 111
When a stateful service is enabled for the first time on a Tier-0 Gateway, what happens on the NSX Edge node?

A. DR is instantiated and automatically connected with SR.
B. SR is instantiated and automatically connected with DR.
C. SR and DR doesn??t need to be connected to provide any stateful services.
D. SR and DR is instantiated but requires manual connection.

Answer: B

Explanation:
When a stateful service (such as NAT or firewall) is enabled for the first time on a Tier-0 Gateway, the Service Router (SR) is instantiated on the NSX Edge node and automatically connected with the Distributed Router (DR). This connection enables the Tier-0 Gateway to handle stateful services by routing traffic through the SR, which manages stateful packet processing, while the DR provides distributed routing functionality.

NEW QUESTION 113
Where can an administrator see a visual overview of network connections between different VMs and different networks, within the NSX domain?

A. Network Intelligence
B. NSX Intelligence
C. VMware Aria Operations
D. VMware Aria Operations for Networks

Answer: B

Explanation:
NSX Intelligence provides a visual overview of network connections within the NSX domain, allowing administrators to see the traffic flows between different VMs and networks. It offers detailed visibility into network traffic patterns, application dependencies, and security posture, making it a valuable tool for monitoring and troubleshooting within NSX environments.

NEW QUESTION 118
What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

A. TEP
B. STT
C. VXLAN
D. UDP

Answer: A

Explanation:
TEP (Tunnel Endpoint): TEPs (Tunnel Endpoints) are configured on transport nodes to handle the encapsulation and decapsulation of the Geneve protocol. TEPs are responsible for creating the overlay network by encapsulating traffic in the Geneve protocol when it moves between transport nodes and decapsulating it upon arrival.

NEW QUESTION 122
......