VMware

Exam Questions 2V0-41.24

VMware NSX 4.X Professional V2

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
When deploying an NSX Edge Transport Node, what two valid IP address assignment options should be specified for the TEP IP addresses? (Choose two.)

A. Use an IP Pool
B. Use RADIUS
C. Use a Static IP List
D. Use BootP
E. Use a DHCP Server

Answer: AE

Explanation:
IP Pool: This allows you to define a range of IP addresses within NSX that the TEPs can use.
DHCP Server: This enables the TEPs to automatically obtain IP addresses from a DHCP server configured in the network.

NEW QUESTION 3
Which tool could be used to configure BGP on a Tier-0 Gateway?

A. ESX CLI
B. NSX CLI
C. API
D. iPerf3

Answer: BC

NEW QUESTION 4
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.

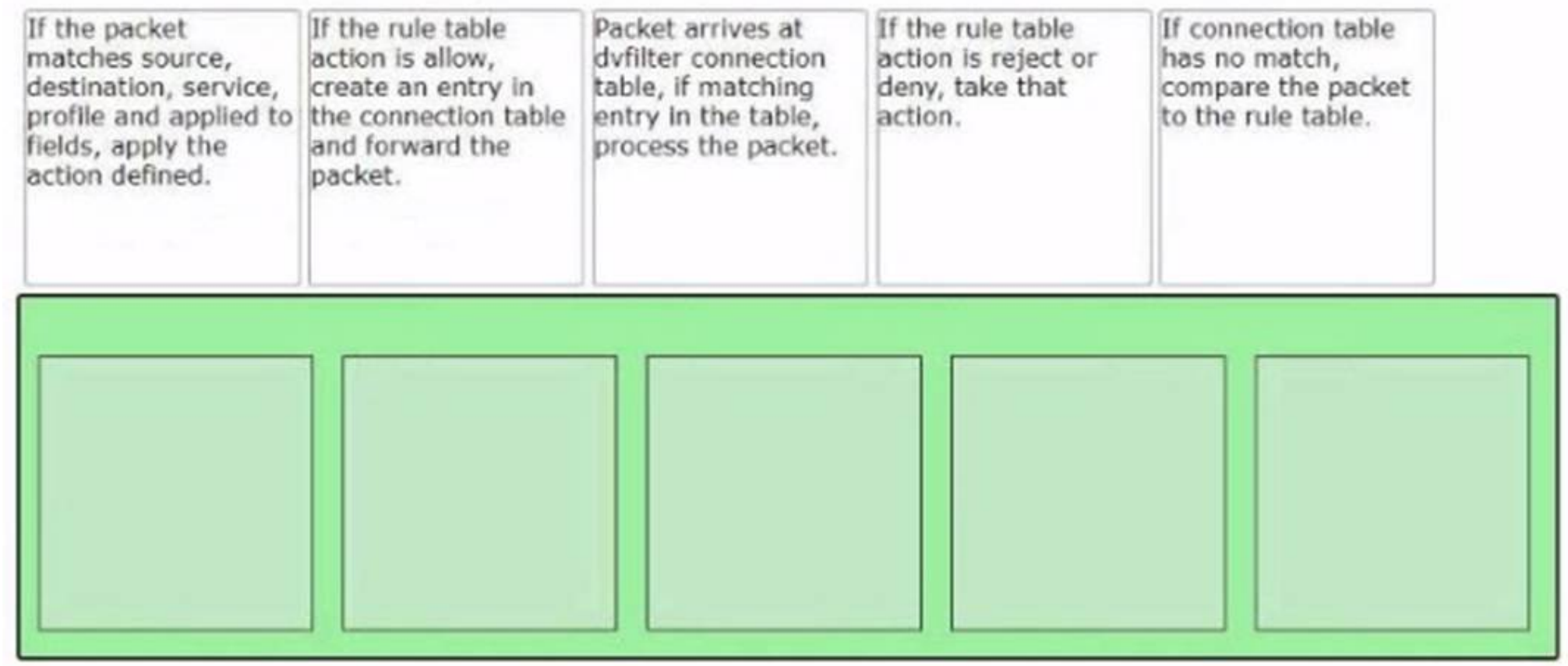
NEW QUESTION 5
When configuring OSPF on Tier-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

A. Area ID
B. MTU of the Uplink C Naming convention
C. Address of the neighbor
D. Subnet mask
E. Protocol and Port

Answer: ABE

Explanation:
Area ID: Both routers must belong to the same OSPF area for a neighbor relationship to form.
MTU of the Uplink: Mismatched MTU settings can prevent the OSPF adjacency from forming, as OSPF packets may be dropped if they exceed the MTU size.
Subnet mask: Both routers must have the same subnet mask on the interface where OSPF is configured to establish a neighbor relationship.

NEW QUESTION 6
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 7
How is the RouterLink port created between a Tier-1 Gateway and Tier-0 Gateway?

A. Automatically created when Tier-1 is created.
B. Manually create a Logical Switch and connect to bother Tier-1 and Tier-0 Gateways.
C. Manually create a Segment and connect to both Tier-1 and Tier-0 Gateways.
D. Automatically created when Tier-1 is connected with Tier-0 from NSX UI.

Answer: D

Explanation:
The RouterLink port between a Tier-1 Gateway and a Tier-0 Gateway is automatically created when the Tier-1 Gateway is connected to the Tier-0 Gateway through the NSX UI. This link enables routing between the Tier-1 and Tier-0 gateways without the need for manual configuration of segments or logical switches.

NEW QUESTION 8
Which VMware GUI tool is used to identify problems in a physical network?

A. VMware Aria Operations Networks
B. VMware Aria Automation
C. VMware Site Recovery Manager
D. VMware Aria Orchestrator

Answer: A

Explanation:
VMware Aria Operations Networks (formerly known as vRealize Network Insight) is a tool specifically designed for network visibility and troubleshooting. It provides insights into both virtual and physical network infrastructures, making it ideal for identifying problems in a physical network.

NEW QUESTION 9
A company security policy requires all users to log into applications using a centralized authentication system.
Which two authentication, authorization, and accounting (AAA) systems are available when integrating NSX with VMware Identity Manager? (Choose two.)

A. RSA SecureID
B. SecureDAP
C. RADII 2.0
D. LDAP and OpenLDAP based on Active Directory (AD)
E. Keygen Enterprise

Answer: AD

Explanation:
RSA SecureID: RSA SecureID is a commonly used two-factor authentication (2FA) system that can integrate with VMware Identity Manager for enhanced security during authentication, making it a suitable AAA system for user authentication.
LDAP and OpenLDAP based on Active Directory (AD): VMware Identity Manager can integrate with LDAP and OpenLDAP directories, including Active Directory (AD), for
centralized user authentication. This allows users to authenticate against an organization's directory service.

NEW QUESTION 10
An NSX administrator wants to create a Tier-0 Gateway to support equal cost multi-path (ECMP) routing.
Which failover detection protocol must be used to meet this requirement?

A. Host Standby Router Protocol (HSRP)
B. Beacon Probing (BP)
C. Virtual Router Redundancy Protocol (VRRP)
D. Bidirectional Forwarding Detection (BFD)

Answer: D

Explanation:
To support Equal-Cost Multi-Path (ECMP) routing in an NSX environment, Bidirectional Forwarding Detection (BFD) must be used for failover detection. BFD is a rapid failure detection protocol that works with ECMP to provide fast failure detection between routers. It helps in detecting link failures more quickly than traditional protocols, ensuring that traffic is routed through available paths as quickly as possible.

NEW QUESTION 10
An NSX administrator would like to create an L2 segment with the following requirements:
• L2 domain should not exist on the physical switches.
• East/West communication must be maximized as much as possible. Which type of segment must the administrator choose?

A. VLAN
B. Overlay
C. Bridge
D. Hybrid

Answer: B

Explanation:
An overlay segment is a layer 2 broadcast domain that is implemented as a logical construct in the NSX-T Data Center software. Overlay segments do not require any configuration on the physical switches, and they allow for optimal east/west communication between workloads on different ESXi hosts. Overlay segments use the Geneve protocol to encapsulate and decapsulate traffic between the hosts. Overlay segments are created and managed by the NSX Manager.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID- 316E5027-E588-455C-88AD-A7DA930A4F0B.html

NEW QUESTION 14
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 16
What is the VMware recommended way to deploy a virtual NSX Edge Node?

A. Through the NSX Ul
B. Through automated or interactive mode using an ISO
C. Through the vSphere Web Client
D. Through the OVF command line tool

Answer: B

Explanation:
VMware recommends deploying a virtual NSX Edge Node using an ISO in either automated or interactive mode. This method provides flexibility and ensures that the NSX Edge node is deployed properly with all the necessary configurations. Using an ISO allows
for a more streamlined and controlled deployment process, especially in larger environments.

NEW QUESTION 19
Which two choices are use cases for Distributed Intrusion Detection? (Choose two.)

A. Use agentless antivirus with Guest Introspection.
B. Quarantine workloads based on vulnerabilities.
C. Identify risk and reputation of accessed websites.
D. Gain Insight about micro-segmentation traffic flows.
E. Identify security vulnerabilities in the workloads.

Answer: BE

Explanation:
According to the VMware NSX Documentation, these are two of the use cases for Distributed Intrusion Detection, which is a feature of NSX Network Detection and Response:
? Quarantine workloads based on vulnerabilities: You can use Distributed Intrusion
Detection to detect vulnerabilities in your workloads and apply quarantine actions to isolate them from the network until they are remediated.
? Identify security vulnerabilities in the workloads: You can use Distributed Intrusion
Detection to scan your workloads for known vulnerabilities and generate reports that show the severity, impact, and remediation steps for each vulnerability.

NEW QUESTION 24
Which table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision?

A. Routing Table
B. ARP Table
C. TEP Table
D. MAC Table

Answer: D

Explanation:
The MAC Table on an ESXi host is used to determine the location of a particular workload for frame-forwarding decisions. This table maps MAC addresses to specific interfaces, enabling the ESXi host to forward frames to the correct destination based on the MAC address of the workload. This is crucial for efficient Layer 2 forwarding decisions within the host.

NEW QUESTION 29
Where is the insertion point for East-West network introspection?

A. Tier-0 router
B. Guest VM vNIC
C. Partner SVM
D. Host Physical NIC

Answer: B

Explanation:
The insertion point for East-West network introspection in NSX is at the Guest VM vNIC (virtual Network Interface Card). By inspecting traffic at the vNIC level, NSX can monitor and apply security policies to traffic between virtual machines (East-West traffic) within the same network segment or data center, providing detailed security controls for VM-to-VM communication.

NEW QUESTION 33
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 38
A security administrator needs to configure a firewall rule based on the domain name of a specific application.
Which field in a distributed firewall rule does the administrator configure?

A. Profile
B. Service
C. Policy
D. Source

Answer: A

Explanation:
To configure a firewall rule based on the domain name of a specific application, the administrator needs to use the Profile field in a distributed firewall rule. The Profile field allows the administrator to select a context profile that contains one or more attributes for filtering traffic. One of the attributes that can be used is Domain (FQDN) Name, which specifies the fully qualified domain name of the application. For example, if the administrator wants to filter traffic to *.office365.com,

they can create a context profile with the Domain (FQDN) Name attribute set to *.office365.com and use it in the Profile field of the firewall rule.
References:
? Filtering Specific Domains (FQDN/URLs)
? FQDN Filtering

NEW QUESTION 39
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.

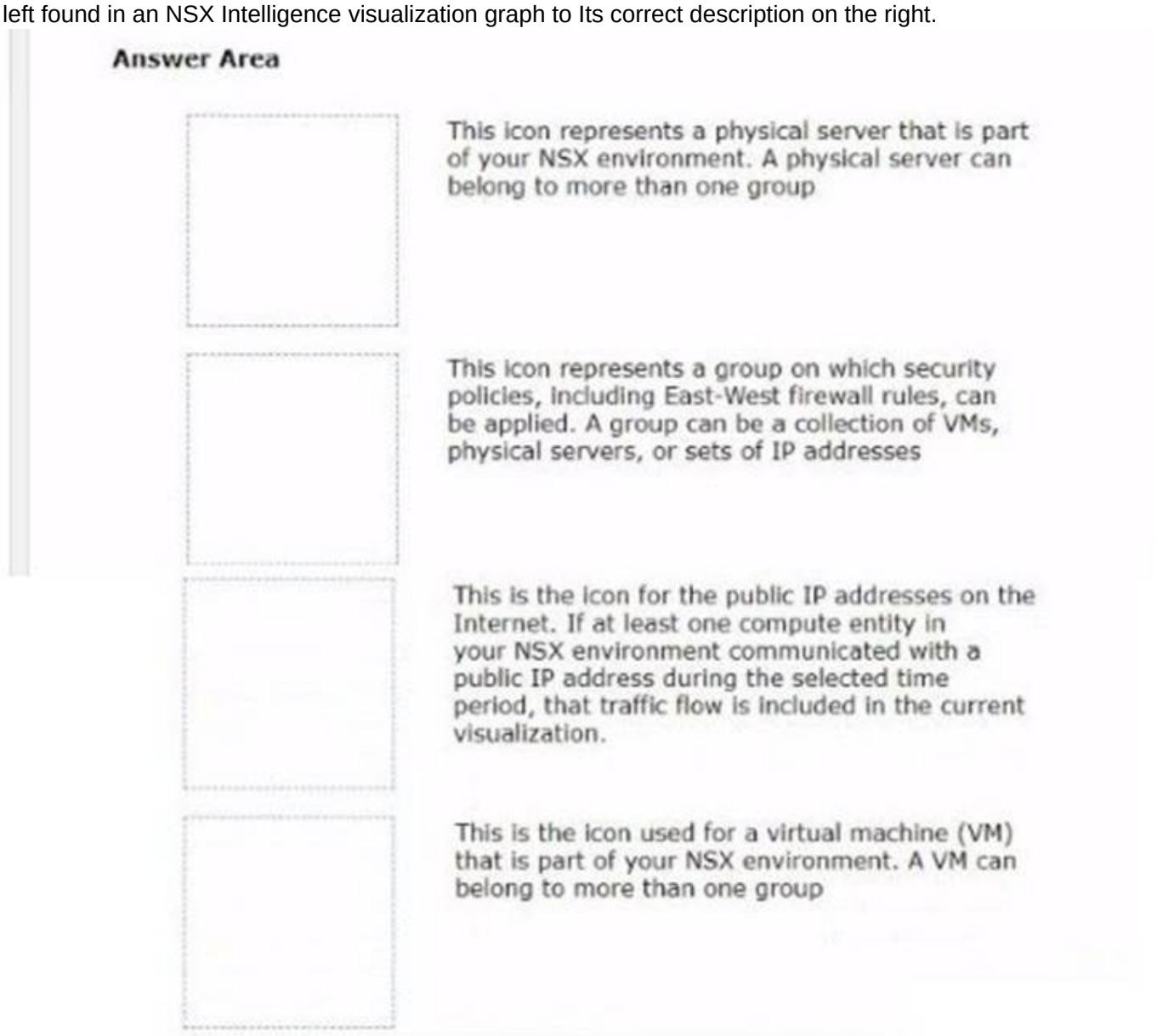
NEW QUESTION 44
An administrator wants to validate the BGP connection status between the Tier-0 Gateway and the upstream physical router.
What sequence of commands could be used to check this status on NSX Edge node?

A. - enable <LR-D>- get vrf <ID>- show bgp neighbor
B. - get gateways- vrf <number>- get bgp neighbor
C. - set vrf <ID>- show logical-routers- show <LR-D> bgp
D. - show logical-routers- get vrf- show ip route bgp

Answer: A

Explanation:
To validate the BGP connection status between the Tier-0 Gateway and the upstream physical router on an NSX Edge node, the correct sequence involves enabling the specific logical router (Tier-0 Gateway), checking the VRF (Virtual Routing and Forwarding) context, and then using the show bgp neighbor command to view the BGP session status. enable <LR-D>: This command enables the logical router interface (Tier-0 Gateway) to access its configuration.
get vrf <ID>: This command checks the specific VRF (used for routing separation) to see the associated routing table.
show bgp neighbor: This command displays the status of the BGP connection, including details about the neighbor relationships and their state.

NEW QUESTION 47
DRAG DROP
Refer to the exhibits.
Drag and drop the NSX graphic element icons on the left found in an NSX Intelligence visualization graph to Its correct description on the right.



A. Mastered

B. Not Mastered

Answer: A

Explanation:
https://docs.vmware.com/en/VMware-NSX-Intelligence/4.0/user-guide/GUID-DC78552B-2CC4-410D-A6C9-3FE0DCEE545B.html

NEW QUESTION 52
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 55
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 58
Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

A. esxcfg-nics -l
B. esxcli network nic list
C. esxcfg-vmknic -l
D. esxcfg-vmsvc/get.networks
E. esxcli network vswitch dvs vmware list

Answer: AB

Explanation:
esxcfg-nics -l: This command lists all physical NICs on the ESXi host along with their link status, allowing you to check if any vmnic link status is down.
esxcli network nic list: This command provides a list of network interfaces with their details, including link status, making it useful for verifying if the link status of a vmnic is down.

NEW QUESTION 63
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 65
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 67
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 70
Which two statements are true about IDS Signatures? (Choose two.)

A. Users can upload their own IDS signature definitions.
B. An IDS signature contains data used to identify known exploits and vulnerabilities.
C. An IDS signature contains data used to identify the creator of known exploits and vulnerabilities.
D. IDS signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
E. An IDS signature contains a set of instructions that determine which traffic is analyzed.

Answer: BE

Explanation:
According to the Network Bachelor article1, an IDS signature contains data used to identify an attacker??s attempt to exploit a known vulnerability in both the operating system and applications. This implies that statement B is true. According to the VMware NSX Documentation2, IDS/IPS Profiles are used to group signatures, which can then be applied to select applications and traffic. This implies that statement E is true. Statement A is false because users cannot upload their own IDS signature definitions, they have to use the ones provided by VMware or Trustwave3. Statement C is false because an IDS signature does not contain data used to identify the creator of known exploits and vulnerabilities, only the exploits and vulnerabilities themselves. Statement D is false because IDS signatures are classified into one of the following severity categories: Critical, High, Medium, Low, or Informational1.
Reference: 3: Distributed IDS/IPS Settings and Signatures - VMware Docs 2: Distributed IDS/IPS - VMware Docs 1: NSX-T: Exploring Distributed IDS - Network Bachelor https://docs.vmware.com/en/VMware-SD-WAN/5.4/VMware-SD-WAN-Administration- Guide/GUID-0BB81F8D-70EB-42D4-ABAF-F80C8F77A4CB.html

NEW QUESTION 73
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 77
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 81
Which statement is true about an alarm in a Suppressed state?

A. An alarm can be suppressed for a specific duration in hours.
B. An alarm can be suppressed for a specific duration in seconds.
C. An alarm can be suppressed for a specific duration in days.
D. An alarm can be suppressed for a specific duration in minutes

Answer: A

Explanation:
In NSX and VMware environments, an alarm in a suppressed state can typically be set to remain suppressed for a specific duration measured in hours. This allows administrators to temporarily ignore the alarm for a set period while working on a resolution without continuous alerts.

NEW QUESTION 85
An administrator has been tasked with implementing the SSL certificates for the NSX Manager Cluster VIP.
Which is the correct way to implement this change?

A. Send an API call to https://<nsx-mgr>/api/vl/cluster/api- certificate?action=set_cluster_certificate&certificate_id=<certificate_id>
B. Send an API call to https://<nsx- mgr>/api/vl/node/services/http?action=apply_certificate&certificate_id=<certificate_id>
C. SSH as admin into the NSX manager with the cluster VIP IP and run nsxcli cluster certificate node install <certificate_id>
D. SSH as admin into the NSX manager with the cluster VIP IP and run nsxcli cluster certificate vip install <certificate_id>

Answer: D

Explanation:
To implement SSL certificates for the NSX Manager Cluster VIP, the correct method is to SSH into the NSX Manager (using the Cluster VIP IP) and run the nsxcli cluster certificate vip install <certificate_id> command. This command installs the SSL certificate for the VIP, ensuring that the cluster's SSL certificate is properly configured for secure communications.

NEW QUESTION 87
Which of the following statements is true regarding the use of a Dynamic Routing Protocol on a Tier-1 Gateway?

A. Both BGP and OSPF can be used on a Tier-1 Gateway.
B. You can only use OSPF on the Tier-1 Gateway
C. A Dynamic Routing Protocol cannot be used on a Tier-1 Gateway.
D. You can only use BGP on the Tier-1 Gateway.

Answer: D

Explanation:
In NSX, BGP is the only supported dynamic routing protocol on a Tier-1 Gateway. OSPF is not supported at the Tier-1 level; it is only available on Tier-0 Gateways. This limitation means that for dynamic routing on a Tier-1 Gateway, administrators can configure BGP to exchange routing information with connected Tier-0 Gateways.

NEW QUESTION 88
Which two logical router components span across all transport nodes? (Choose two.)

A. SERVICE_ROUTER_TIER0
B. TIER0_DISTRIBUTED_ROUTER
C. DISTRIBUTED_ROUTER_TIER0
D. DISTRIBUTED_ROUTER_TIER1
E. SERVICE_ROUTER_TIER1

Answer: BD

Explanation:
TIER0_DISTRIBUTED_ROUTER: The Tier-0 Distributed Router spans all transport nodes, providing distributed routing capabilities across the NSX environment at the Tier-0 level. DISTRIBUTED_ROUTER_TIER1: Similarly, the Tier-1 Distributed Router spans all transport nodes, enabling distributed routing at the Tier-1 level, which allows routing functions to occur closer to the workload VMs across the transport nodes.

NEW QUESTION 89
Which three DHCP Services are supported by NSX? (Choose three.)

A. Gateway DHCP
B. Segment DHCP
C. DHCP Relay
D. Port DHCP per VNF
E. VRF DHCP Server

Answer: ABC

Explanation:
Gateway DHCP: NSX supports DHCP services configured on the gateway, allowing it to provide IP addresses to clients within the network.
Segment DHCP: NSX can provide DHCP services at the segment level, where DHCP is configured directly on a network segment to assign IP addresses to

connected clients. DHCP Relay: NSX supports DHCP Relay, which allows forwarding of DHCP requests to an external DHCP server for IP address assignment.

NEW QUESTION 94

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

2V0-41.24 Practice Exam Features:

* 2V0-41.24 Questions and Answers Updated Frequently

* 2V0-41.24 Practice Questions Verified by Expert Senior Certified Staff

* 2V0-41.24 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 2V0-41.24 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year