VMware.2V0-41.23.by.Hung.61q

Number: 2V0-41.23
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: 2V0-41.23

Exam Name: VMware NSX 4.x Professional

Exam A

QUESTION 1

Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

A. Can have a maximum of 10 edge nodes

B. Can have a maximum of 8 edge nodes

C. Can contain multiple types of edge nodes (VM or bare metal)

D. Must contain only one type of edge nodes (VM or bare metal)

E. Must have only active-active edge nodes

Correct Answer: A, C
Section:
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/installation/GUID-14183A62-8E8D-43CC-92E0-E8D72E198D5A.html

QUESTION 2

Which two tools are used for centralized logging in VMware NSX? (Choose two.)

A. VMware Aria Operations

B. Syslog Server

C. VMware Aria Automation

D. VMware Aria Operations for Logs

E. VMware Aria Operations for Networks

Correct Answer: B, D
Section:
Explanation:
Two tools that are used for centralized logging in VMware NSX areSyslog ServerandVMware Aria Operations for Logs.Syslog Server is a standard protocol for sending log messages from various network devices to a centralized server1.VMware NSX supports syslog for long term retention of logs and all NSX components can send syslog messages to a configured syslog server2.VMware Aria Operations for Logs is a VMware product that provides intelligent log analytics for NSX3.It provides monitoring and troubleshooting capabilities and customizable dashboards for network virtualization, flow analysis, and alerts3. The other options are incorrect because they are not tools for centralized logging in VMware NSX.VMware Aria Operations is a VMware product that provides operations management and automation for NSX4, but it is not the same as VMware Aria Operations for Logs.VMware Aria Automation is a VMware product that provides automation and orchestration for NSX5, but it is not related to logging. VMware Aria Operations for Networks is not a valid product name.References:Syslog,NSX Logging and System Events,VMware vRealize Log Insight for NSX,VMware vRealize Operations Management Pack for NSX,VMware vRealize Automation

QUESTION 3

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

A. set vrf <ID> show logical-routers show <LR-D> bgp

B. show logical-routers get vrf show ip route bgp

C. get gateways vrf <number> get bgp neighbor

D. enable <LR-D> get vrf <ID> show bgp neighbor

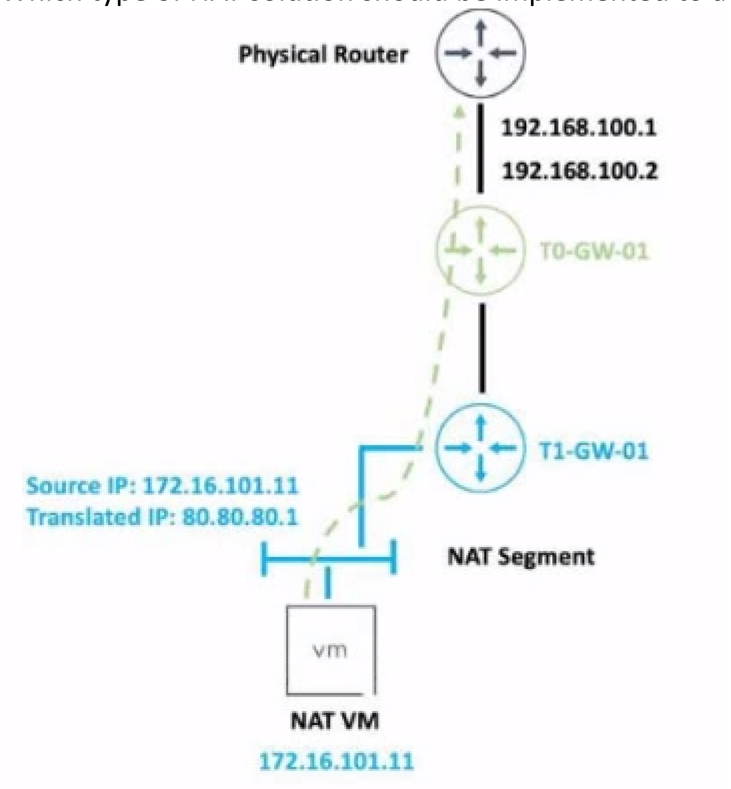
Correct Answer: C
Section:
Explanation:
The sequence of commands that could be used to check the BGP connection status between the Tier-O Gateway and the upstream physical router on NSX Edge node isget gateways, vrf <number>, get bgp neighbor.These commands can be executed on the NSX Edge node CLI after logging in as admin6.The first command,get gateways, displays the list of logical routers (gateways) configured on the Edge node, along with their IDs and VRF numbers7.The second command,vrf <number>, switches to the VRF context of the desired Tier-O Gateway, where <number> is the VRF number obtained from the previous command7.The third command,get bgp neighbor, displays the BGP neighbor summary for the selected VRF, including the neighbor IP address, AS number, state, uptime, and prefixes received8. The other options are incorrect because they either use invalid or incomplete commands or do not switch to the correct VRF context.References:NSX-T Command-Line Interface Reference,NSX Edge Node CLI Commands,Troubleshooting BGP on NSX-T Edge Nodes

QUESTION 4
Which command is used to set the NSX Manager's logging-level to debug mode for troubleshooting?

A. Set service manager log-level debug
B. Set service manager logging-level debug
C. Set service nsx-manager log-level debug
D. Set service nsx-manager logging-level debug

Correct Answer: B
Section:
Explanation:
According to the VMware Knowledge Base article1, the CLI command to set the log level of the NSX Manager to debug mode is set service manager logging-level debug.This command can be used when the NSX UI is inaccessible or when troubleshooting issues with the NSX Manager1. The other commands are incorrect because they either use a wrong syntax or a wrong service name.The NSX Manager service name is manager, not nsx-manager2.The log level parameter is logging-level, not log-level3.
https://kb.vmware.com/s/article/55868

QUESTION 5
Refer to the exhibit.
An administrator would like to change the private IP address of the NAT VM I72.l6.101.il 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. DNAT
B. SNAT
C. Reflexive NAT
D. NAT64

Correct Answer: B
Section:
Explanation:
SNAT stands for Source Network Address Translation. It is a type of NAT that translates the source IP address of outgoing packets from a private address to a public address.SNAT is used to allow hosts in a private network to access the internet or other public networks1
In the exhibit, the administrator wants 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. This is an example of SNAT, as the source IP address is modified before the packets are sent to an external network.
According to the VMware NSX 4.x Professional Exam Guide, SNAT is one of the topics covered in the exam objectives2
To learn more about SNAT and how to configure it in VMware NSX, you can refer to the following resources:
VMware NSX Documentation: NAT3
VMware NSX 4.x Professional: NAT Configuration4
VMware NSX 4.x Professional: NAT Troubleshooting5
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-7AD2C384-4303-4D6C-A44A-DEF45AA18A92.html

QUESTION 6
When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

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

Correct Answer: C
Section:
Explanation:
According to the VMware NSX Documentation1, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information.
Core files and Audit logs might contain sensitive information such as passwords or encryption keys. https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-73D9AF0D-4000-4EF2-AC66-6572AD1A0B30.html

QUESTION 7
Which three of the following describe the Border Gateway Routing Protocol (BGP) configuration on a Tier-0 Gateway? (Choose three.)

A. Can be used as an Exterior Gateway Protocol.
B. It supports a 4-byte autonomous system number.
C. The network is divided into areas that are logical groups.
D. EIGRP Is disabled by default.
E. BGP is enabled by default.

Correct Answer: A, B, D
Section:
Explanation:
A) Can be used as an Exterior Gateway Protocol. This is correct. BGP is a protocol that can be used to exchange routing information between different autonomous systems (AS). An AS is a network or a group of networks

under a single administrative control. BGP can be used as an Exterior Gateway Protocol (EGP) to connect an AS to other ASes on the internet or other external networks1
B) It supports a 4-byte autonomous system number. This is correct. BGP supports both 2-byte and 4-byte AS numbers. A 2-byte AS number can range from 1 to 65535, while a 4-byte AS number can range from 65536 to 4294967295. NSX supports both 2-byte and 4-byte AS numbers for BGP configuration on a Tier-0 Gateway2
C) The network is divided into areas that are logical groups. This is incorrect. This statement describes OSPF, not BGP. OSPF is another routing protocol that operates within a single AS and divides the network into areas to reduce routing overhead and improve scalability. BGP does not use the concept of areas, but rather uses attributes, policies, and filters to control the routing decisions and traffic flow3
D) FIGRP Is disabled by default. This is correct. FIGRP stands for Fast Interior Gateway Routing Protocol, which is an enhanced version of IGRP, an obsolete routing protocol developed by Cisco. FIGRP is not supported by NSX and is disabled by default on a Tier-0 Gateway.
E) BGP is enabled by default. This is incorrect. BGP is not enabled by default on a Tier-0 Gateway. To enable BGP, you need to configure the local AS number and the BGP neighbors on the Tier-0 Gateway using the NSX Manager UI or API.
To learn more about BGP configuration on a Tier-0 Gateway in NSX, you can refer to the following resources:
VMware NSX Documentation: Configure BGP 1
VMware NSX 4.x Professional: BGP Configuration
VMware NSX 4.x Professional: BGP Troubleshooting

QUESTION 8
Which three NSX Edge components are used for North-South Malware Prevention? (Choose three.)

A. Thin Agent
B. RAPID
C. Security Hub
D. IDS/IPS
E. Security Analyzer
F. Reputation Service

Correct Answer: B, C, D
Section:
Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED08F0.html#:~:text=On%20the%20north%2Dsouth%20traffic,Guest%20Introspection%20(GI)%20platform.
The main components on the edge node for north-south malware prevention perform the following functions:
* IDS/IPS engine: Extracts files and relays events and data to the security hub
North-south malware prevention uses the file extraction features of the IDS/IPS engine that runs on NSX Edge for north-south traffic.
* Security hub: Collects file events, obtains verdicts for known files, sends files for local and cloud-based analysis, and sends information to the security analyzer
* RAPID: Provides local analysis of the file
* ASDS Cache: Caches reputation and verdicts of known files

QUESTION 9
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.

Correct Answer: B, E
Section:
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.

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

A. Set cli-timeout
B. Get auth-policy minimum-password-length
C. Set hardening- policy
D. Set auth-policy

Correct Answer: D
Section:
Explanation:
According to the VMware NSX Documentation4, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings .
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-99BAED85-D754-4589-9050-72A1AB528C10.html

QUESTION 11
Which statement is true about an alarm in a Suppressed state?

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

Correct Answer: D
Section:
Explanation:
An alarm can be suppressed for a specific duration in hours.
According to the VMware NSX documentation, an alarm can be in one of the following states: Open, Acknowledged, Suppressed, or Resolved12
An alarm in a Suppressed state means that the status reporting for this alarm has been disabled by the user for a user-specified duration12
When a user moves an alarm into a Suppressed state, they are prompted to specify the duration in hours. After the specified duration passes, the alarm state reverts to Open. However, if the system determines the condition has been corrected, the alarm state changes to Resolved13
To learn more about how to manage alarm states in NSX, you can refer to the following resources:
VMware NSX Documentation: Managing Alarm States 1
VMware NSX Documentation: View Alarm Information 2
VMware NSX Intelligence Documentation: Manage NSX Intelligence Alarm States 3
https://docs.vmware.com/en/VMware-NSX-Intelligence/1.2/user-guide/GUID-EBD3C5A8-F9AB-4A22-BA40-92D61850C1E6.html

QUESTION 12
How is the RouterLink port created between a Tier-1 Gateway and Tler-0 Gateway?

A. Manually create a Logical Switch and connect to bother Tler-1 and Tier-0 Gateways.
B. Automatically created when Tler-1 is created.
C. Manually create a Segment and connect to both Titrr-1 and Tier-0 Gateways.

D. Automatically created when Tier-t Is connected with Tier-0 from NSX UI.

Correct Answer: D
Section:
Explanation:
According to the VMware NSX 4.x Professional documents and tutorials, a RouterLink port is a logical port that connects a Tier-1 gateway to a Tier-0 gateway. This port is automatically created when a Tier-1 gateway is associated with a Tier-0 gateway from the NSX UI or API. The RouterLink port enables routing between the two gateways and carries all the routing protocols and traffic.There is no need to manually create a logical switch or segment for this purpose1.

QUESTION 13
What are three NSX Manager roles? (Choose three.)

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

Correct Answer: D, E, F
Section:
Explanation:
According to the VMware NSX 4.x Professional documents and tutorials, an NSX Manager is a standalone appliance that hosts the API services, the management plane, control plane, and policy management.The NSX Manager has three built-in roles: policy, manager, and controller2. The policy role handles the declarative configuration of the system and translates it into desired state for the manager role. The manager role receives and validates the configuration from the policy role and stores it in a distributed persistent database. The manager role also publishes the configuration to the central control plane.The controller role implements the central control plane that computes the network state based on the configuration and topology information3. The other roles (master, cloud, and zookeeper) are not valid NSX Manager roles.

QUESTION 14
What are two valid options when configuring the scope of a distributed firewall rule? (Choose two.)

A. DFW
B. Tier-1 Gateway
C. Segment
D. Segment Port
E. Group

Correct Answer: A, E
Section:
Explanation:
A group is a logical construct that represents a collection of objects in NSX, such as segments, segment ports, virtual machines, IP addresses, MAC addresses, tags, or security policies. A group can be used to define dynamic membership criteria based on various attributes or filters.A group can also be used as the scope of a distributed firewall rule, which means that the rule will apply to all the traffic that matches the group membership criteria32

QUESTION 15
Which two statements are true for IPSec VPN? (Choose two.)

A. VPNs can be configured on the command line Interface on the NSX manager.
B. IPSec VPN services can be configured at Tler-0 and Tler-1 gateways.

C. IPSec VPNs use the DPDK accelerated performance library.
D. Dynamic routing Is supported for any IPSec mode In NSX.

Correct Answer: B, C
Section:
Explanation:
According to the VMware NSX 4.x Professional documents and tutorials, IPSec VPN secures traffic flowing between two networks connected over a public network through IPSec gateways called endpoints. NSX Edge supports a policy-based or a route-based IPSec VPN.Beginning with NSX-T Data Center 2.5, IPSec VPN services are supported on both Tier-0 and Tier-1 gateways1.NSX Edge also leverages the DPDK accelerated performance library to optimize the performance of IPSec VPN2.
https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-7D9F7199-E51B-478B-A8BC-58AD5BBAA0F6.html

QUESTION 16
Which two built-in VMware tools will help Identify the cause of packet loss on VLAN Segments? (Choose two.)

A. Flow Monitoring
B. Packet Capture
C. Live Flow
D. Activity Monitoring
E. Traceflow

Correct Answer: B, E
Section:
Explanation:
According to the VMware NSX Documentation1, Packet Capture and Traceflow are two built-in VMware tools that can help identify the cause of packet loss on VLAN segments.
Packet Capture allows you to capture packets on a specific interface or segment and analyze them using tools such as Wireshark or tcpdump. Packet Capture can help you diagnose network issues such as misconfigured MTU, incorrect VLAN tags, or firewall drops.
Traceflow allows you to inject synthetic packets into the network and trace their path from source to destination. Traceflow can help you verify connectivity, routing, and firewall rules between virtual machines or segments. Traceflow can also show you where packets are dropped or modified along the way.

QUESTION 17
What should an NSX administrator check to verify that VMware Identity Manager Integration Is successful?

A. From VMware Identity Manager the status of the remote access application must be green.
B. From the NSX UI the status of the VMware Identity Manager Integration must be 'Enabled'.
C. From the NSX CLI the status of the VMware Identity Manager Integration must be 'Configured'.
D. From the NSX UI the URI in the address bar must have 'locaNfatse' part of it.

Correct Answer: B
Section:
Explanation:
From the NSX UI the status of the VMware Identity Manager Integration must be ''Enabled''.According to the VMware NSX Documentation1, after configuring VMware Identity Manager integration, you can validate the functionality by checking the status of the integration in the NSX UI. The status should be ''Enabled'' if the integration is successful. The other options are either incorrect or not relevant.

QUESTION 18
What is the VMware recommended way to deploy a virtual NSX Edge Node?

A. Through the OVF command line tool
B. Through the vSphere Web Client

C. Through automated or Interactive mode using an ISO
D. Through the NSXUI

Correct Answer: D
Section:
Explanation:
Through the NSX UI.According to the VMware NSX Documentation2, you can deploy NSX Edge nodes as virtual appliances through the NSX UI by clicking Add Edge Node and providing the required information. The other options are either outdated or not applicable for virtual NSX Edge nodes.
https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199F.html

QUESTION 19
Which three DHCP Services are supported by NSX? (Choose three.)

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

Correct Answer: A, C, E
Section:
Explanation:
According to the VMware NSX Documentation1, NSX-T Data Center supports the following types of DHCP configuration on a segment:
Local DHCP server: This option creates a local DHCP server that has an IP address on the segment and provides dynamic IP assignment service only to the VMs that are attached to the segment.
Gateway DHCP server: This option is attached to a tier-0 or tier-1 gateway and provides DHCP service to the networks (overlay segments) that are directly connected to the gateway and configured to use a gateway DHCP server.
DHCP Relay: This option relays the DHCP client requests to the external DHCP servers that can be in any subnet, outside the SDDC, or in the physical network.
https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-486C1281-C6CF-47EC-B2A2-0ECFCC4A68CE.html

QUESTION 20
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 UI. It must be done via command line interface.
D. The option to set time-based rule is a clock Icon in the policy.

Correct Answer: D
Section:
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

QUESTION 21
What can the administrator use to identify overlay segments in an NSX environment if troubleshooting is required?

A. VNI ID
B. Segment ID
C. Geneve ID
D. VIAN ID

Correct Answer: A
Section:
Explanation:
According to the VMware NSX Documentation1, a segment is mapped to a unique Geneve segment that is distributed across the ESXi hosts in a transport zone. The Geneve segment uses a virtual network identifier (VNI) as an overlay network identifier. The VNI ID can be used to identify overlay segments in an NSX environment if troubleshooting is required.

QUESTION 22
Which two BGP configuration parameters can be configured in the VRF Lite gateways? (Choose two.)

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

Correct Answer: B, E
Section:
Explanation:
Route Aggregation and and D) BGP neighbours are available when configuring BGP in a VRF. 'Route distribution' does not exist, what you can do is a 'Route Re-Distribution' via BGP. https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-4CB5796A-1CED-4F0E-ADE0-72BF7B3F762C.html

QUESTION 23
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events. Which message ID (msgld) should be used in the syslog export configuration command as a filler?

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

Correct Answer: D
Section:
Explanation:
According to the VMware NSX Documentation2, the FABRIC message ID (msgld) captures messages related to NSX host preparation events, such as installation, upgrade, or uninstallation of NSX components on ESXi hosts.
The syslog export configuration command for NSX host preparation events would look something like this:
set service syslog export FABRIC
The other options are either incorrect or not relevant for NSX host preparation events.MONITORING captures messages related to NSX monitoring features, such as alarms and system events2.SYSTEM captures messages related to NSX system events, such as login, logout, or configuration changes2.GROUPING captures messages related to NSX grouping objects, such as security groups, security tags, or IP sets2.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-CC18C0E3-D076-41AA-8B8C-133650FDC2E7.html

QUESTION 24
Which three data collection sources are used by NSX Network Detection and Response to create correlations/Intrusion campaigns? (Choose three.)

A. Files and anti-malware (lie events from the NSX Edge nodes and the Security Analyzer

B. East-West anti-malware events from the ESXi hosts

C. Distributed Firewall flow data from the ESXi hosts

D. IDS/IPS events from the ESXi hosts and NSX Edge nodes

E. Suspicious Traffic Detection events from NSX Intelligence

Correct Answer: A, D, E
Section:
Explanation:
The correct answers are A. Files and anti-malware (file) events from the NSX Edge nodes and the Security Analyzer, D. IDS/IPS events from the ESXi hosts and NSX Edge nodes, and E. Suspicious Traffic Detection events from NSX Intelligence.According to the VMware NSX Documentation3, these are the three data collection sources that are used by NSX Network Detection and Response to create correlations/intrusion campaigns.
The other options are incorrect or not supported by NSX Network Detection and Response.East-West anti-malware events from the ESXi hosts are not collected by NSX Network Detection and Response3.Distributed Firewall flow data from the ESXi hosts are not used for correlation/intrusion campaigns by NSX Network Detection and Response3.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-14BBE50D-9931-4719-8FA7-884539C0D277.html

QUESTION 25
Which VMware GUI tool is used to identify problems in a physical network?

A. VMware Aria Automation

B. VMware Aria Orchestrator

C. VMware Site Recovery Manager

D. VMware Aria Operations Networks

Correct Answer: D
Section:
Explanation:
According to the web search results, VMware Aria Operations Networks (formerly vRealize Network Insight) is a network monitoring tool that can help monitor, discover and analyze networks and applications across clouds1.It can also provide enhanced troubleshooting and visibility for physical and virtual networks2.
The other options are either incorrect or not relevant for identifying problems in a physical network. VMware Aria Automation is a cloud automation platform that can help automate the delivery of IT services. VMware Aria Orchestrator is a cloud orchestration tool that can help automate workflows and integrate with other systems. VMware Site Recovery Manager is a disaster recovery solution that can help protect and recover virtual machines from site failures.

QUESTION 26
An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two additional nodes and Cluster VIP using the NSX UI.
What two are the prerequisites for this configuration? (Choose two.)

A. All nodes must be in separate subnets.

B. The cluster configuration must be completed using API.

C. NSX Manager must reside on a Windows Server.

D. All nodes must be in the same subnet.

E. A compute manager must be configured.

Correct Answer: D, E
Section:
Explanation:
According to the VMware NSX Documentation, these are the prerequisites for adding nodes to an NSX Management Cluster using the NSX UI:
All nodes must be in the same subnet and have IP connectivity with each other.
A compute manager must be configured and associated with the NSX Manager node.

The NSX Manager node must have a valid license.
The NSX Manager node must have a valid certificate.

QUESTION 27
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.

Correct Answer: B, E
Section:
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.

QUESTION 28
When configuring OSPF on a TIer-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

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

Correct Answer: B, C, F
Section:
Explanation:
according to the VMware NSX Documentation, these are the three parameters that must match in order to establish an OSPF neighbor relationship with an upstream router on a tier-0 gateway:
MTU of the Uplink: The maximum transmission unit (MTU) of the uplink interface must match the MTU of the upstream router interface. Otherwise, OSPF packets may be fragmented or dropped, causing neighbor adjacency issues.
Subnet mask: The subnet mask of the uplink interface must match the subnet mask of the upstream router interface. Otherwise, OSPF packets may not reach the correct destination or be rejected by the upstream router.
Area ID: The area ID of the uplink interface must match the area ID of the upstream router interface. Otherwise, OSPF packets may be ignored or discarded by the upstream router.
https://www.computernetworkingnotes.com/ccna-study-guide/ospf-neighborship-condition-and-requirement.html

QUESTION 29
Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

A. NSX Intrusion Detection and Prevention
B. NSX Intelligence
C. NSX Network Detection and Response
D. NSX Malware Prevention Metrics

E. NSX Intrinsic Security

Correct Answer: C, D
Section:
Explanation:
The NSX Application Platform Deployment features are divided into three form factors: Evaluation, Standard, and Advanced.Each form factor determines which NSX features can be activated or installed on the platform1.The Evaluation form factor supports only NSX Intelligence, which provides network visibility and analytics for NSX-T environments2.The Standard form factor supports both NSX Intelligence and NSX Network Detection and Response, which provides network threat detection and response capabilities for NSX-T environments3.The Advanced form factor supports all four features: NSX Intelligence, NSX Network Detection and Response, NSX Malware Prevention, and NSX Metrics1.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-85CD2728-8081-45CE-9A4A-D72F49779D6A.html

QUESTION 30
What needs to be configured on a Tler-0 Gateway lo make NSX Edge Services available to a VM on a VLAN-backed logical switch?

A. Downlink Interface
B. VLAN Uplink
C. Loopback Router Port
D. Service Interface

Correct Answer: D
Section:
Explanation:
The service interface is a special-purpose port to enable services for mainly VLAN-based networks. North-south service insertion is another use case that requires a service interface to connect a partner appliance and redirect north-south traffic for partner services. Service interfaces are supported on both active-standby Tier-0 logical routers and Tier-1 routers. Firewall, NAT, and VPNs are supported on this interface. The service interface is also a downlink

QUESTION 31
Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

A. Source
B. Profiles -> Context Profiles
C. Destination
D. Profiles -> L7 Access Profile

Correct Answer: D
Section:
Explanation:
The field in a Tier-1 Gateway Firewall that would be used to allow access for a collection of trustworthy web sites isProfiles -> L7 Access Profile.This field allows the user to create a Layer 7 access profile that defines a list of allowed or blocked URLs based on categories, reputation, or custom entries1.The user can then apply the L7 access profile to a firewall rule to control the traffic based on the URL filtering criteria1. The other options are incorrect because they are not related to URL filtering.The Source field specifies the source IP address or group of the firewall rule1.The Destination field specifies the destination IP address or group of the firewall rule1.The Profiles -> Context Profiles field allows the user to create a context profile that defines a list of application signatures or attributes that can be used to identify and classify network traffic1.References:Gateway Firewall

QUESTION 32
An NSX administrator is reviewing syslog and notices that Distributed Firewall Rules hit counts are not being logged.
What could cause this issue?

A. Syslog is not configured on the ESXi transport node.
B. Zero Trust Security is not enabled.

C. Syslog is not configured on the NSX Manager.
D. Distributed Firewall Rule logging is not enabled.

Correct Answer: D
Section:
Explanation:
https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-D57429A1-A0A9-42BE-A299-0C3C3546ABF3.html

QUESTION 33
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

Correct Answer: C
Section:
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

QUESTION 34
An administrator is configuring service insertion for Network Introspection.
Which two places can the Network Introspection be configured? (Choose two.)

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

Correct Answer: A, B
Section:
Explanation:
Network Introspection is a service insertion feature that allows third-party network security services to monitor and analyze the traffic between virtual machines. Network Introspection can be configured on the host pNIC or on the partner SVM, depending on the type of service and the deployment model. The host pNIC configuration is used for services that require traffic redirection from the physical network to the service virtual machine. The partner SVM configuration is used for services that require traffic redirection from the virtual network to the service virtual machine. Network Introspection cannot be configured on the Tier-0 or Tier-1 gateways, as they are not part of the data plane where the service insertion occurs. Network Introspection also cannot be configured on the edge node, as it is a logical construct that hosts the Tier-0 and Tier-1 gateways.References:Distributed Service Insertion,NSX Securing ''Anywhere'' Part IV

QUESTION 35
Which CLI command would an administrator use to allow syslog on an ESXi transport node when using the esxcli utility?

A. esxcli network firewall ruleset set -r syslog -e true
B. esxcli network firewall ruleset -e syslog
C. esxcli network firewall ruleset set -r syslog -e false

D. esxcli network firewall ruleset set -a -e false

Correct Answer: A
Section:
Explanation:
To allow syslog on an ESXi transport node, the administrator needs to use the esxcli utility to enable the syslog ruleset in the ESXi firewall. The correct syntax for this command isesxcli network firewall ruleset set -r syslog -e true, where-rspecifies the ruleset name and-especifies whether to enable or disable it. The other options are incorrect because they either use an invalid syntax, such as omitting the ruleset name or using-ainstead of-r, or they disable the syslog ruleset instead of enabling it, which is the opposite of what the question asks.References: [ESXi Firewall Command-Line Interface], [Configure Syslog on ESXi Hosts]

QUESTION 36
An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances.
What feature of NSX fulfills this requirement?

A. Load balancer
B. Federation
C. Multi-hypervisor support
D. Policy-driven configuration

Correct Answer: B
Section:
Explanation:
Federation is a feature of NSX that allows the administrator to manage multiple NSX instances with a single pane of glass view, create gateways and segments that span one or more locations, and configure and enforce firewall rules consistently across locations1.Federation provides centralized policy management for security and networking services for all locations and pushes it down to NSX Local Managers at the respective sites for enforcement1.Federation also enables disaster recovery and workload mobility scenarios by providing consistent network and security policies across different sites1.References:1: NSX Federation - VMware Docs(https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D5B6DC79-6733-44A7-8072-50221CF2122A.html)

QUESTION 37
In an NSX environment, an administrator is observing low throughput and congestion between the Tier-O Gateway and the upstream physical routers.
Which two actions could address low throughput and congestion? (Choose two.)

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

Correct Answer: B, C
Section:
Explanation:
ECMP (Equal Cost Multi-Path) is a routing protocol that increases the north and south communication bandwidth by adding an uplink to the tier-0 logical router and configure it for each Edge node in an NSX Edge cluster2.The ECMP routing paths are used to load balance traffic and provide fault tolerance for failed paths2.The tier-0 logical router must be in active-active mode for ECMP to be available2.A maximum of eight ECMP paths are supported2. Configuring ECMP on the tier-0 gateway can address low throughput and congestion by distributing the traffic among multiple paths and avoiding bottlenecks.
Deploying Large size Edge node/s can also address low throughput and congestion by providing more resources (memory, CPU, disk) for the Edge node to handle the network traffic.The NSX Edge VM system requirements vary depending on the appliance size, which affects the bandwidth, NAT/firewall, load balancer, and VPN capabilities of the Edge node1.A Large size Edge node has 32 GB memory, 8 vCPU, 200 GB disk space, and can support 2-10 Gbps bandwidth, L2-L4 features, and L7 load balancer1.An Extra Large size Edge node has 64 GB memory, 16 vCPU, 200 GB disk space, and can support more than 10 Gbps bandwidth, L2-L4 features, L7 load balancer, and VPN1.Deploying a larger size Edge node can improve the performance and capacity of the tier-0 gateway.References:2: Understanding ECMP Routing - VMware Docs(https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-443B6B0D-F179-429E-83F3-E136038332E0.html)1: NSX Edge VM System Requirements - VMware Docs(https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/installation/GUID-22F87CA8-01A9-4F2E-B7DB-9350CA60EA4E.html)

QUESTION 38
How does the Traceflow tool identify issues in a network?

A. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
C. Injects ICMP traffic into the data plane and observes the results in the control plane.
D. Injects synthetic traffic into the data plane and observes the results in the control plane.

Correct Answer: D
Section:
Explanation:
The Traceflow tool identifies issues in a network by injecting synthetic traffic into the data plane and observing the results in the control plane. This allows the tool to identify any issues in the network and provide a detailed report on the problem. You can use the Traceflow tool to test connectivity between any two endpoints in your NSX-T Data Center environment.

QUESTION 39
Which two statements are correct about East-West Malware Prevention? (Choose two.)

A. A SVM is deployed on every ESXi host.
B. NSX Application Platform must have Internet access.
C. An agent must be installed on every ESXi host.
D. An agent must be installed on every NSX Edge node.
E. NSX Edge nodes must have Internet access.

Correct Answer: A, B
Section:

QUESTION 40
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

Correct Answer: A
Section:
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

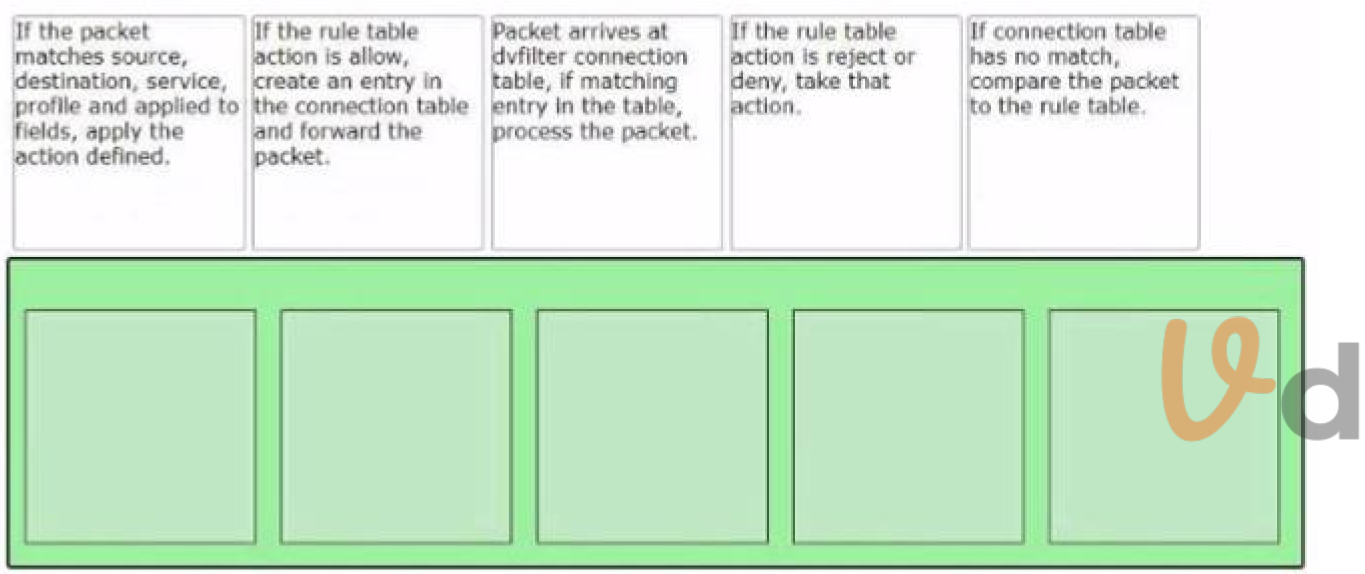
QUESTION 41
What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

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.

Correct Answer: A, C
Section:

QUESTION 42
DRAG DROP
Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.

Select and Place:



If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

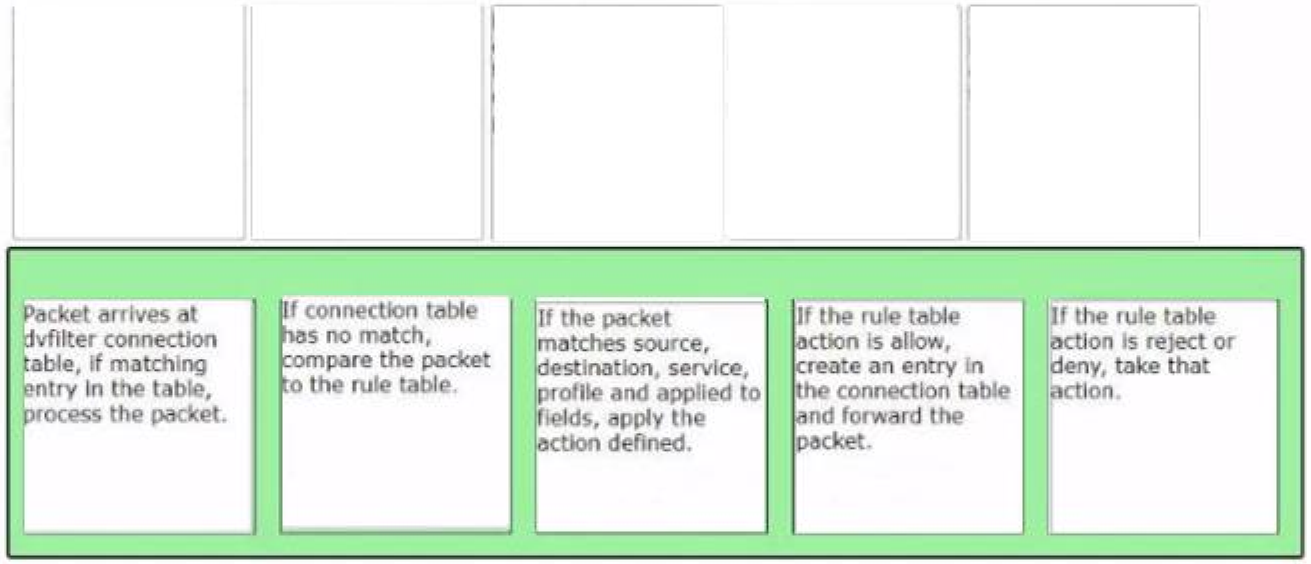
If the rule table action is allow, create an entry in the connection table and forward the packet.

Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.

If the rule table action is reject or deny, take that action.

If connection table has no match, compare the packet to the rule table.

Correct Answer:



Packet arrives at dvfilter 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.

Section:
Explanation:

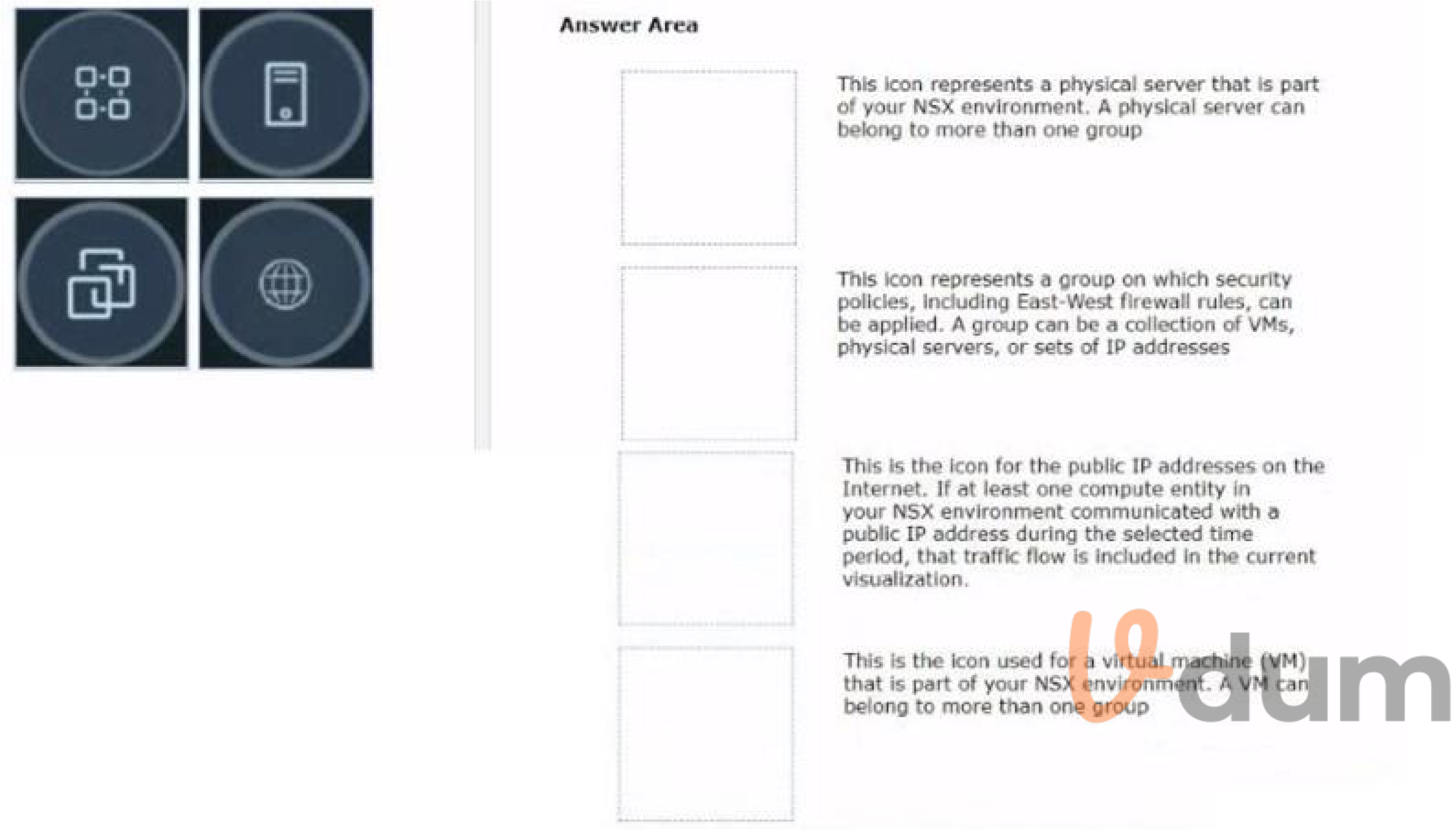
QUESTION 43

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.

Select and Place:



Answer Area

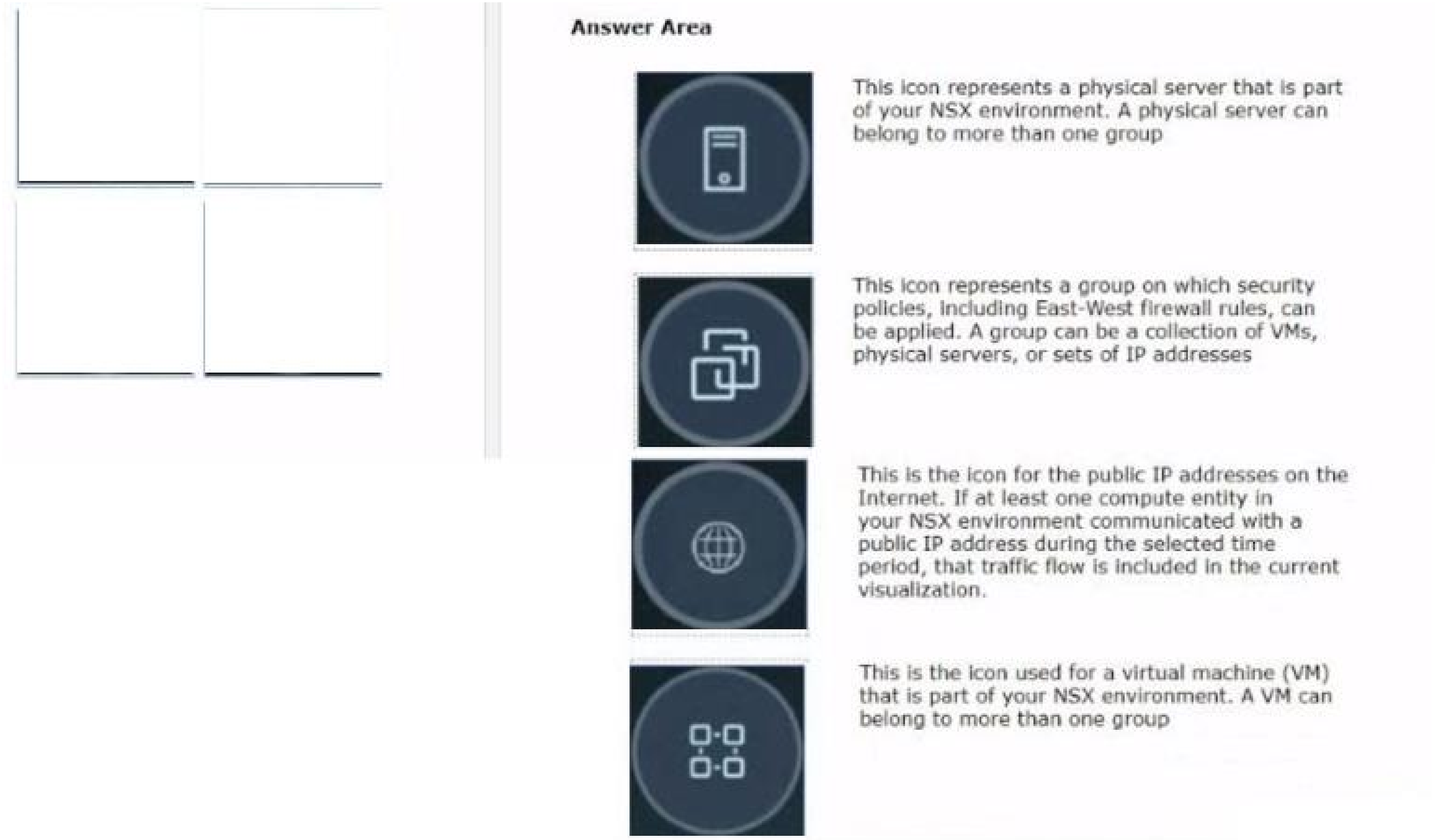
This icon represents a physical server that is part of your NSX environment. A physical server can belong to more than one group

This icon represents a group on which security policies, including East-West firewall rules, can be applied. A group can be a collection of VMs, physical servers, or sets of IP addresses

This is the icon for the public IP addresses on the Internet. If at least one compute entity in your NSX environment communicated with a public IP address during the selected time period, that traffic flow is included in the current visualization.

This is the icon used for a virtual machine (VM) that is part of your NSX environment. A VM can belong to more than one group

Correct Answer:



Answer Area

This icon represents a physical server that is part of your NSX environment. A physical server can belong to more than one group

This icon represents a group on which security policies, including East-West firewall rules, can be applied. A group can be a collection of VMs, physical servers, or sets of IP addresses

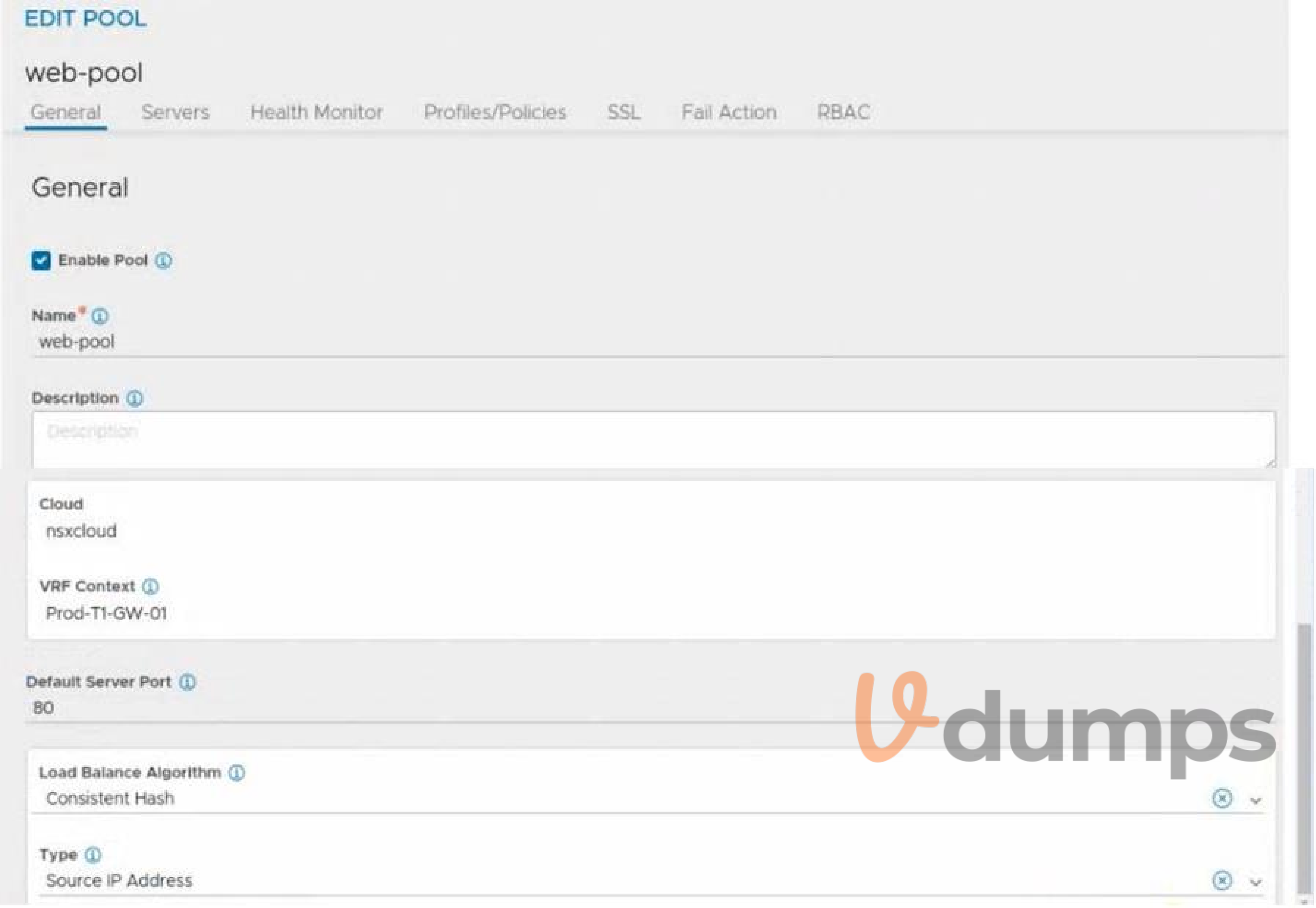
This is the icon for the public IP addresses on the Internet. If at least one compute entity in your NSX environment communicated with a public IP address during the selected time period, that traffic flow is included in the current visualization.

This is the icon used for a virtual machine (VM) that is part of your NSX environment. A VM can belong to more than one group

Section:
Explanation:

QUESTION 44
HOTSPOT
Refer to the exhibit.
An administrator configured NSX Advanced Load Balancer to redistribute the traffic between the web servers. However, requests are sent to only one server
Which of the following pool configuration settings needs to be adjusted to resolve the problem? Mark the correct answer by clicking on the image.

Hot Area:



EDIT POOL

web-pool

General

☑ Enable Pool

Name* web-pool

Description

Cloud nsxcloud

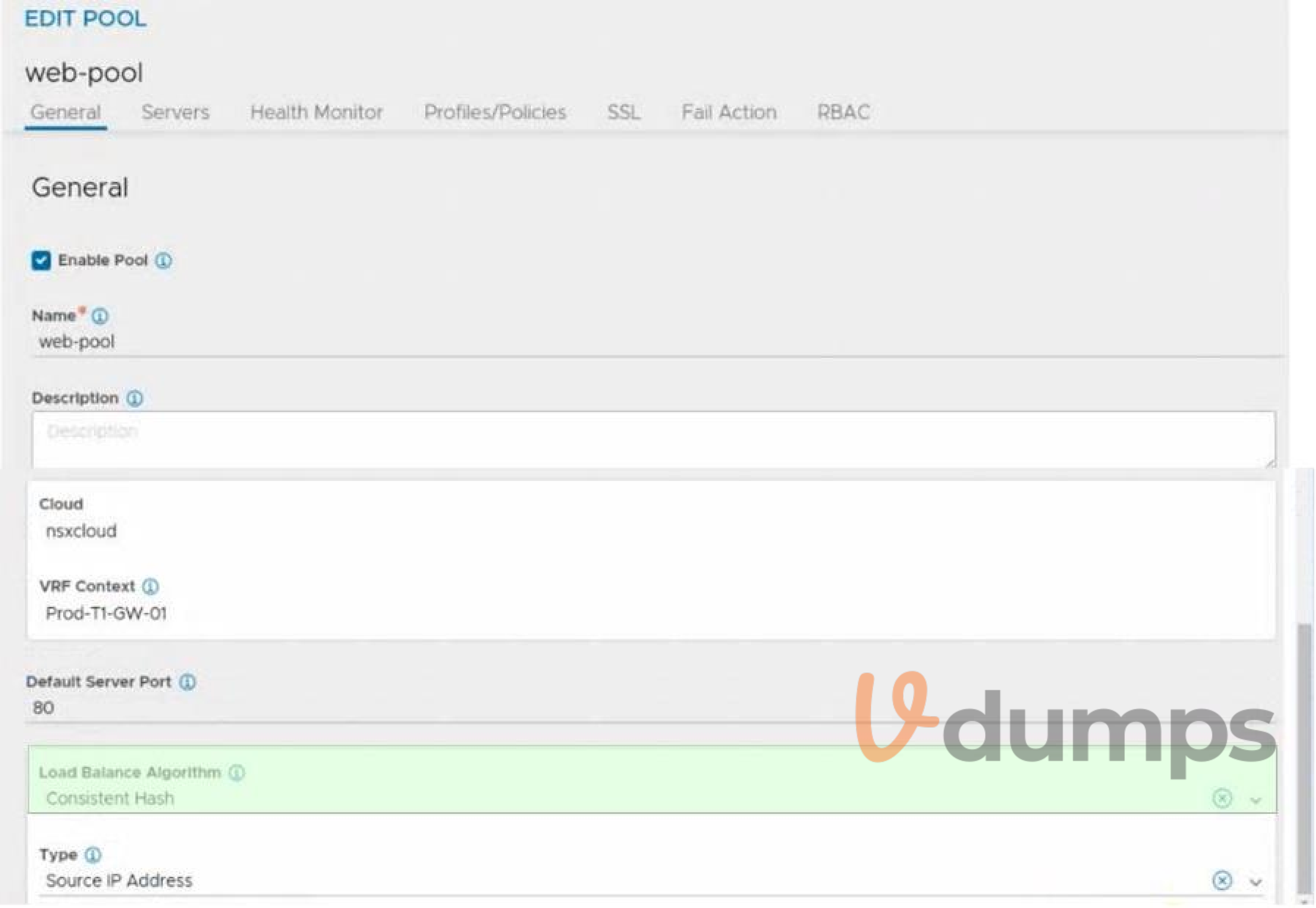
VRF Context Prod-T1-GW-01

Default Server Port 80

Load Balance Algorithm Consistent Hash

Type Source IP Address

Answer Area:



EDIT POOL

web-pool

General

☑ Enable Pool

Name* web-pool

Description

Cloud nsxcloud

VRF Context Prod-T1-GW-01

Default Server Port 80

Load Balance Algorithm Consistent Hash

Type Source IP Address

Section:
Explanation:

QUESTION 45
Which VPN type must be configured before enabling a L2VPN?

A. Route-based IPSec VPN
B. Policy based IPSec VPN
C. SSL-bosed IPSec VPN
D. Port-based IPSec VPN

Correct Answer: A
Section:
Explanation:
According to the VMware NSX Documentation, this VPN type must be configured before enabling a L2VPN. L2VPN stands for Layer 2 VPN and is a feature that allows you to extend your layer 2 network across different sites using an IPSec tunnel. Route-based IPSec VPN is a VPN type that uses logical router ports to establish IPSec tunnels between sites.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-86C8D6BB-F185-46DC-828C-1E1876B854E8.html

QUESTION 46
Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

A. esxcfg-nics -1

B. excli network nic list

C. esxcli network vswitch dvs wmare list

D. esxcfg-vmknic -1

E. esxcfg-vmsvc/get.network

Correct Answer: A, B
Section:
Explanation:
esxcfg-nics -l and esxcli network nic list are two CLI commands that can be used to see the vmnic link status on an ESXi host. Both commands display information such as the vmnic name, driver, link state, speed, and duplex mode. The link state can be either Up or Down, indicating whether the vmnic is connected or not. For example, the output of esxcfg-nics -l can look like this:

```
Name PCI Driver Link Speed Duplex MAC Address MTU Description
vmnic0 0000:02:00.0 igbn Up 1000Mbps Full 00:50:56:01:2a:3b 1500 Intel Corporation I350 Gigabit Network Connection
vmnic1 0000:02:00.1 igbn Down 0Mbps Half 00:50:56:01:2a:3c 1500 Intel Corporation I350 Gigabit Network Connection
```

QUESTION 47
Which two of the following will be used for Ingress traffic on the Edge node supporting a Single Tier topology? (Choose two.)

A. Inter-Tier interface on the Tier-0 gateway

B. Tier-0 Uplink interface

C. Downlink Interface for the Tier-0 DR

D. Tier-1 SR Router Port

E. Downlink Interface for the Tier-1 DR

Correct Answer: B, C
Section:
Explanation:
The two interfaces that will be used for ingress traffic on the Edge node supporting a Single Tier topology are:
B) Tier-0 Uplink interface
C) Downlink Interface for the Tier-0 DR
The Tier-0 Uplink interface is the interface that connects the Tier-0 gateway to the external network. It is used to receive traffic from the physical router or switch that is the next hop for the Tier-0 gateway. The Tier-0 Uplink interface can be configured with a static IP address or use BGP to exchange routes with the external network.
The Downlink Interface for the Tier-0 DR is the interface that connects the Tier-0 gateway to the workload segments. It is used to receive traffic from the VMs or containers that are attached to the segments. The Downlink Interface for the Tier-0 DR is a logical interface (LIF) that is distributed across all transport nodes that host the segments. The Downlink Interface for the Tier-0 DR has an IP address that acts as the default gateway for the VMs or containers on the segments.

QUESTION 48
Which Is the only supported mode In NSX Global Manager when using Federation?

A. Controller

B. Policy

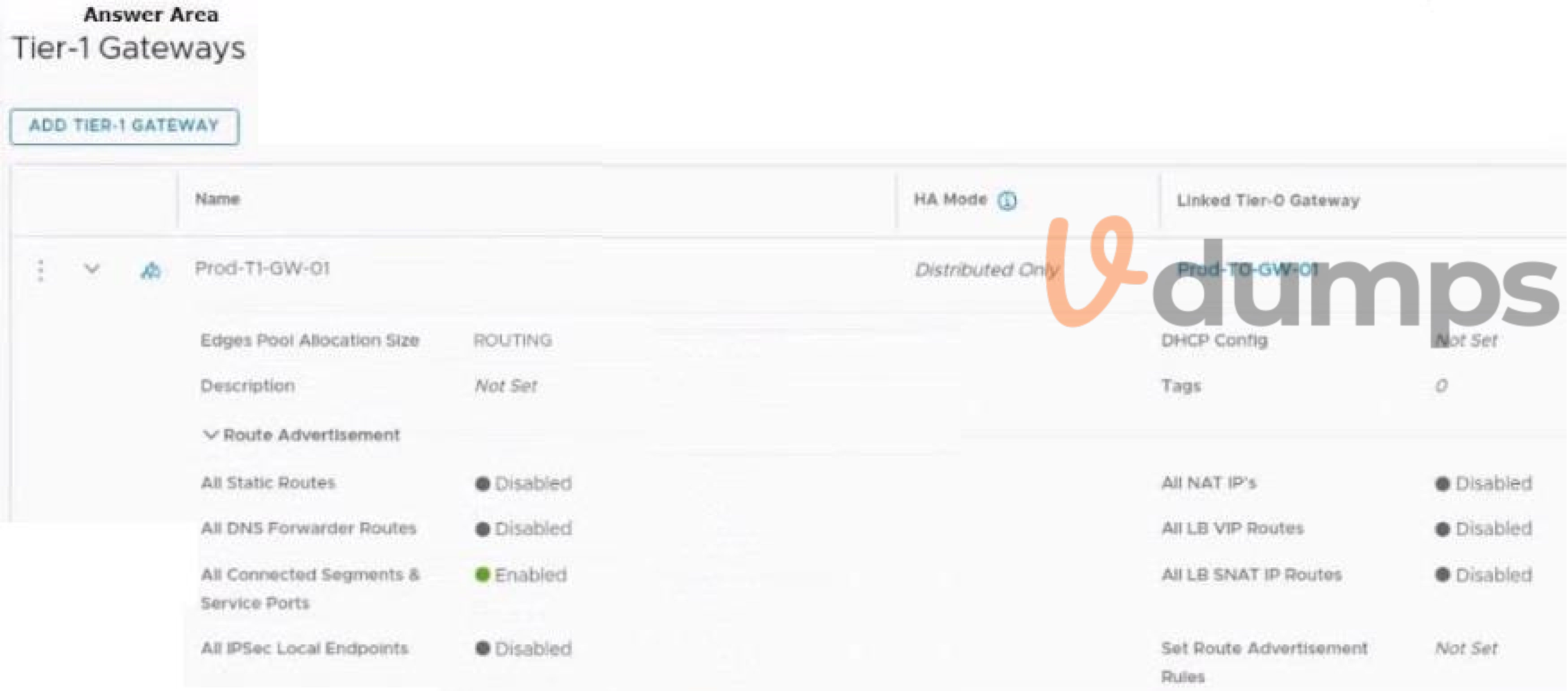
C. Proxy

D. Proton

Correct Answer: B
Section:
Explanation:
NSX Global Manager is a feature of NSX that allows managing multiple NSX domains across different sites or clouds from a single pane of glass. NSX Global Manager supports Federation, which is a capability that enables synchronizing configuration and policy across multiple NSX domains. Federation has many benefits such as simplifying operations, improving resiliency, and enabling disaster recovery.
The only supported mode in NSX Global Manager when using Federation is Policy mode. Policy mode means that NSX Global Manager acts as a policy manager that defines and distributes global policies to local NSX managers in different domains. Policy mode also allows local NSX managers to have their own local policies that can override or merge with global policies.
https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-29998FC5-C1AB-40BC-B669-6E8E9937F345.html

QUESTION 49
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.

Hot Area:



Answer Area
Tier-1 Gateways

ADD TIER-1 GATEWAY

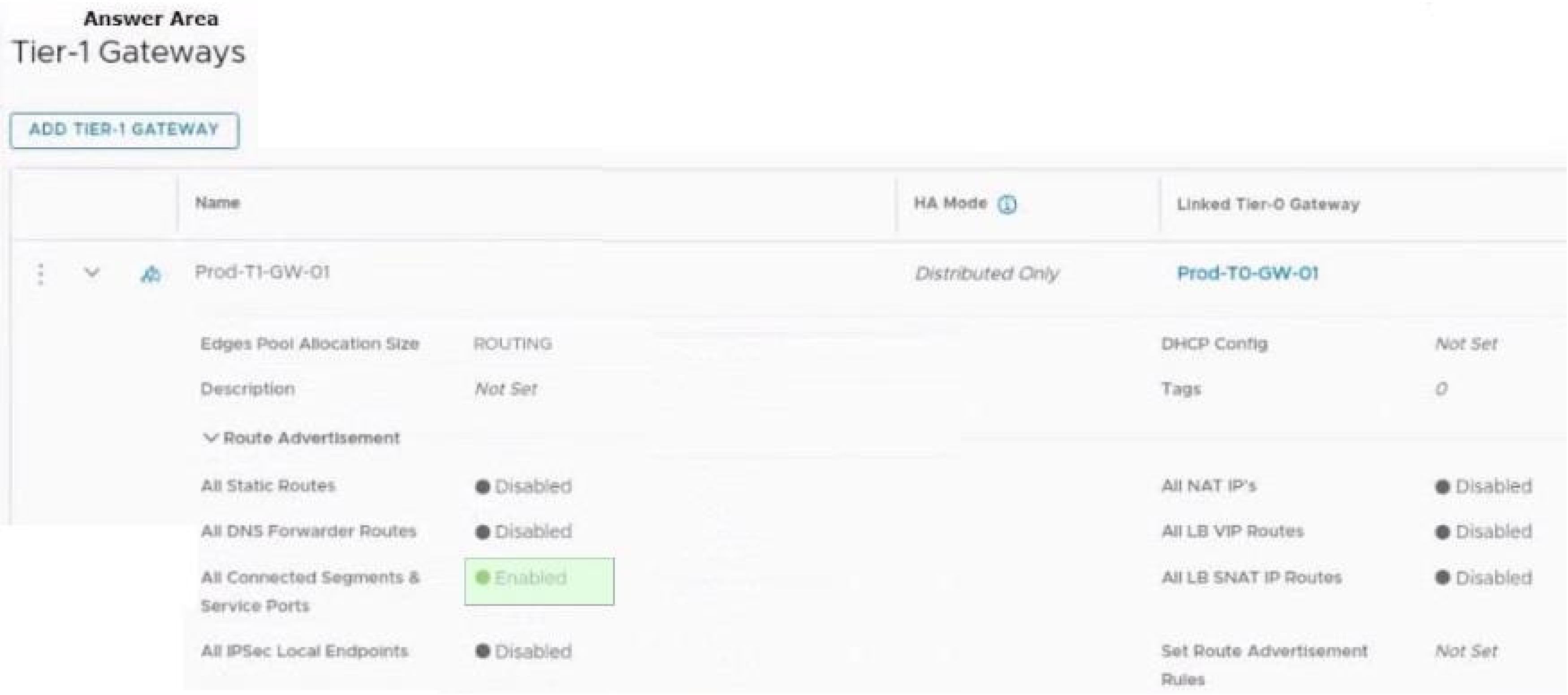
Name	HA Mode	Linked Tier-0 Gateway
Prod-T1-GW-01	Distributed Only	Prod-T0-GW-01

Edges Pool Allocation Size	ROUTING	DHCP Config	Not Set
Description	Not Set	Tags	0

Route Advertisement

All Static Routes	● Disabled	All NAT IP's	● Disabled
All DNS Forwarder Routes	● Disabled	All LB VIP Routes	● Disabled
All Connected Segments & Service Ports	● Enabled	All LB SNAT IP Routes	● Disabled
All IPSec Local Endpoints	● Disabled	Set Route Advertisement Rules	Not Set

Answer Area:



Answer Area

Tier-1 Gateways

Name	HA Mode	Linked Tier-0 Gateway
Prod-T1-GW-01	*Distributed Only*	Prod-T0-GW-01

Edges Pool Allocation Size	ROUTING	DHCP Config	*Not Set*
Description	*Not Set*	Tags	*0*

Route Advertisement

All Static Routes	● Disabled	All NAT IP's	● Disabled
All DNS Forwarder Routes	● Disabled	All LB VIP Routes	● Disabled
All Connected Segments & Service Ports	● Enabled	All LB SNAT IP Routes	● Disabled
All IPSec Local Endpoints	● Disabled	Set Route Advertisement Rules	*Not Set*

Section:

Explanation:

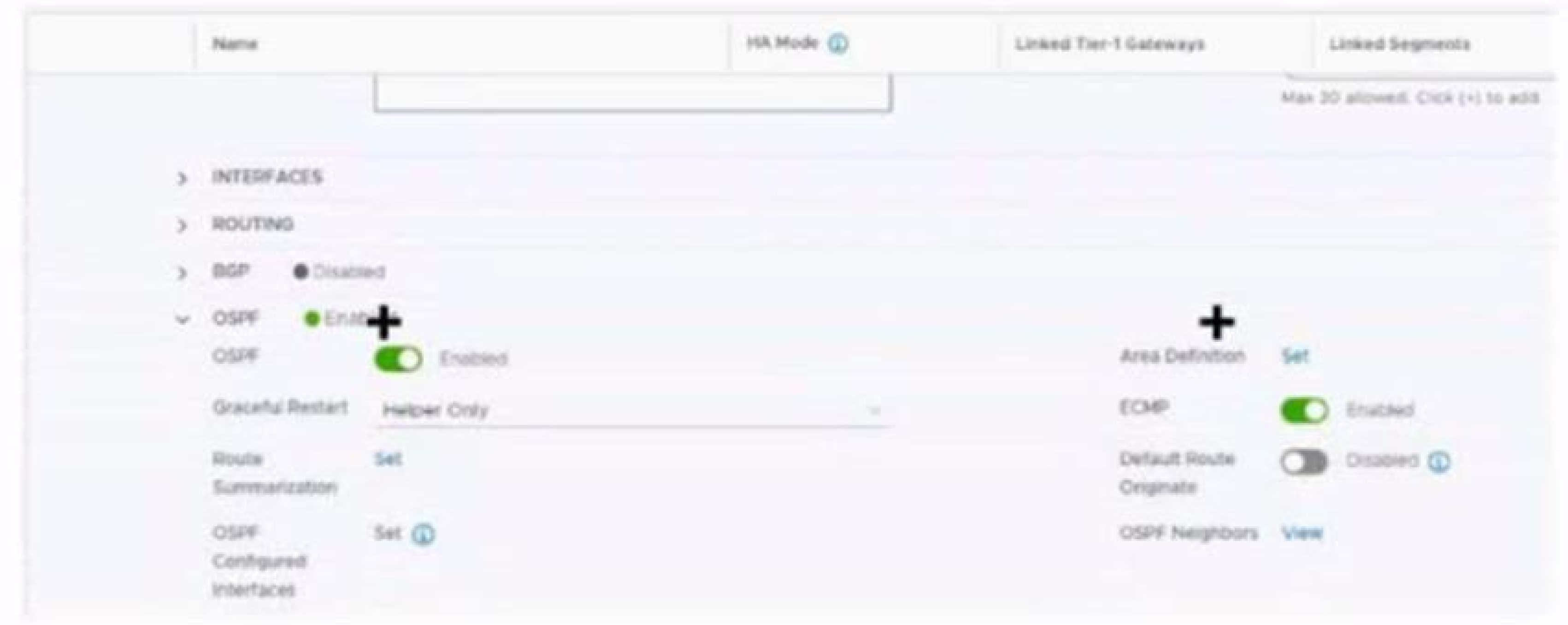
QUESTION 50

HOTSPOT

Refer to the exhibit.

Which two items must be configured to enable OSPF for the Tler-0 Gateway in the Image? Mark your answers by clicking twice on the image.

Hot Area:



Name	HA Mode	Linked Tier-1 Gateways	Linked Segments

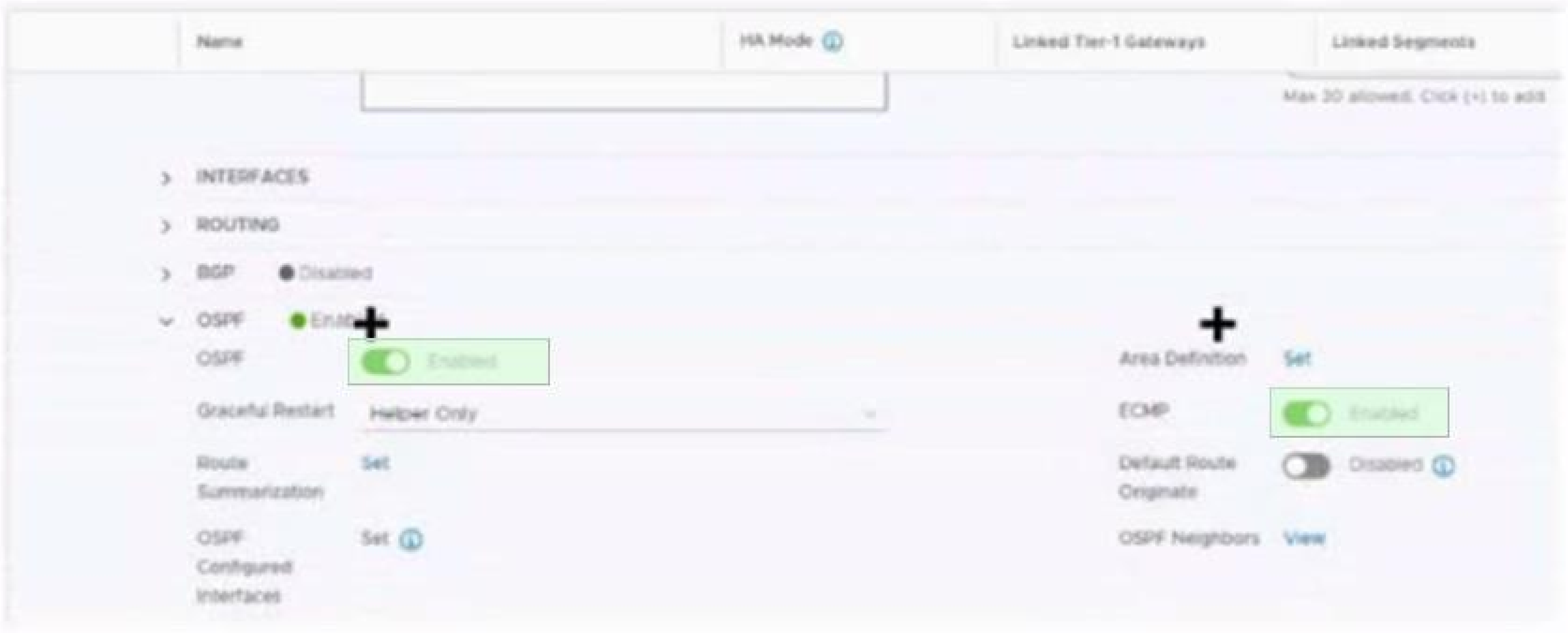
Max 20 allowed. Click (+) to add

BGP ● Disabled

OSPF ● Enabled

OSPF	Enabled	Area Definition	Set
Graceful Restart	Helper Only	ECMP	Enabled
Route Summarization	Set	Default Route Originate	Disabled
OSPF Configured Interfaces	Set	OSPF Neighbors	View

Answer Area:



Name | HA Mode | Linked Tier-1 Gateways | Linked Segments

Max 30 allowed. Click (+) to add

› INTERFACES

› ROUTING

› BGP ● Disabled

⌄ OSPF ● Enabled

OSPF: Enabled

Graceful Restart: Helper Only

Route Summarization: Set

OSPF Configured Interfaces: Set

Area Definition: Set

ECMP: Enabled

Default Route Originate: Disabled

OSPF Neighbors: View

Section:
Explanation:

QUESTION 51
The security administrator turns on logging for a firewall rule.
Where is the log stored on an ESXi transport node?

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

Correct Answer: C
Section:
Explanation:
The log for a firewall rule on an ESXi transport node is stored in the /var/log/dfwpktlogs.log file. This file contains information about the packets that match or do not match the firewall rules, such as the source and destination IP addresses, ports, protocols, actions, and rule IDs. The log file can be viewed using the esxcli network firewall get command or the vSphere Client.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D57429A1-A0A9-42BE-A299-0C3C3546ABF3.html

QUESTION 52
An architect receives a request to apply distributed firewall in a customer environment without making changes to the network and vSphere environment. The architect decides to use Distributed Firewall on VDS.
Which two of the following requirements must be met in the environment? (Choose two.)

A. vCenter 8.0 and later
B. NSX version must be 3.2 and later
C. NSX version must be 3.0 and later
D. VDS version 6.6.0 and later

Correct Answer: B, D
Section:
Explanation:
Distributed Firewall on VDS is a feature of NSX-T Data Center that allows users to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This feature provides NSX security capabilities such as Distributed Firewall (DFW), Distributed IDS/IPS, Identity Firewall, L7 App ID, FQDN Filtering, NSX Intelligence, and NSX Malware Prevention. To enable this feature, the following requirements must be met in the environment:
The NSX version must be3.2 and later1. This is the minimum version that supports Distributed Security for VDS.
The VDS version must be6.6.0 and later1. This is the minimum version that supports the NSX host preparation operation that activates the DFW with the default rule set to allow.
References:
Overview of NSX IDS/IPS and NSX Malware Prevention

QUESTION 53
Which command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

A. tepconfig
B. ifconfig
C. tcpdump
D. debug

Correct Answer: B
Section:
Explanation:
The commandifconfigis used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node2. The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. Theifconfigcommand can show the IP address, netmask, broadcast address, and other information of the network interface. For example, the following command shows the network configuration of the TEP IP on a bare metal transport node with interface name ens192:

```
ifconfig ens192
```

The output of the command would look something like this:

```
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.10.10 netmask 255.255.255.0 broadcast 10.10.10.255 inet6 fe80::250:56ff:fe9a:1b8c prefixlen 64 scopeid 0x20<link> ether 00:50:56:9a:1b:8c
txqueuelen 1000 (Ethernet) RX packets 123456 bytes 123456789 (123.4 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 234567 bytes 234567890 (234.5 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The TEP IP in this example is10.10.10.10.
References:
IBM Cloud Docs

QUESTION 54
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

Correct Answer: B
Section:
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

QUESTION 55
Which table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision?

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

Correct Answer: B
Section:
Explanation:
The MAC table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision. The MAC table maps the MAC addresses of the workloads to their corresponding tunnel endpoint (TEP) IP addresses. The TEP IP address identifies the ESXi host where the workload resides. The MAC table is populated by learning the source MAC addresses of the incoming frames from the workloads. The MAC table is also synchronized with other ESXi hosts in the same transport zone by using the NSX Controller.
https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide

QUESTION 56
Which two choices are solutions offered by the VMware NSX portfolio? (Choose two.)

A. VMware Tanzu Kubernetes Grid
B. VMware Tanzu Kubernetes Cluster
C. VMware NSX Advanced Load Balancer
D. VMware NSX Distributed IDS/IPS
E. VMware Aria Automation

Correct Answer: C, D
Section:
Explanation:
VMware NSX is a portfolio of networking and security solutions that enables consistent policy, operations, and automation across multiple cloud environments1
The VMware NSX portfolio includes the following solutions:
VMware NSX Data Center: A platform for data center network virtualization and security that delivers a complete L2-L7 networking stack and overlay services for any workload1
VMware NSX Cloud: A service that extends consistent networking and security to public clouds such as AWS and Azure1
VMware NSX Advanced Load Balancer: A solution that provides load balancing, web application firewall, analytics, and monitoring for applications across any cloud12
VMware NSX Distributed IDS/IPS: A feature that provides distributed intrusion detection and prevention for workloads across any cloud12
VMware NSX Intelligence: A service that provides planning, observability, and intelligence for network and micro-segmentation1
VMware NSX Federation: A capability that enables multi-site networking and security management with consistent policy and operational state synchronization1
VMware NSX Service Mesh: A service that connects, secures, and monitors microservices across multiple clusters and clouds1
VMware NSX for Horizon: A solution that delivers secure desktops and applications across any device, location, or network1
VMware NSX for vSphere: A solution that provides network agility and security for vSphere environments with a built-in console in vCenter1
VMware NSX-T Data Center: A platform for cloud-native applications that supports containers, Kubernetes, bare metal hosts, and multi-hypervisor environments1
VMware Tanzu Kubernetes Grid and VMware Tanzu Kubernetes Cluster are not part of the VMware NSX portfolio. They are solutions for running Kubernetes clusters on any cloud3
VMware Aria Automation is not a real product name. It is a fictional name that does not exist in the VMware portfolio.
https://blogs.vmware.com/networkvirtualization/2020/01/nsx-hero.html/

QUESTION 57

When a stateful service is enabled for the first lime on a Tier-0 Gateway, what happens on the NSX Edge node'

A. SR is instantiated and automatically connected with DR.
B. DR Is instantiated and automatically connected with SR.
C. SR and DR Is instantiated but requites manual connection.
D. SR and DR doesn't need to be connected to provide any stateful services.

Correct Answer: A
Section:
Explanation:
The answer is A. SR is instantiated and automatically connected with DR.
SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions1
The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network1
When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR2
According to the VMware NSX 4.x Professional Exam Guide, understanding the SR and DR components and their functions is one of the exam objectives3
To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources:
VMware NSX Documentation: NSX Edge Components 1
VMware NSX 4.x Professional: NSX Edge Architecture
VMware NSX 4.x Professional: NSX Edge Routing

QUESTION 58
A company Is deploying NSX micro-segmentation in their vSphere environment to secure a simple application composed of web. app, and database tiers.
The naming convention will be:
* WKS-WEB-SRV-XXX
* WKY-APP-SRR-XXX
* WKI-DB-SRR-XXX
What is the optimal way to group them to enforce security policies from NSX?

A. Use Edge as a firewall between tiers.
B. Do a service insertion to accomplish the task.
C. Group all by means of tags membership.
D. Create an Ethernet based security policy.

Correct Answer: C
Section:
Explanation:
The answer is C. Group all by means of tags membership.
Tags are metadata that can be applied to physical servers, virtual machines, logical ports, and logical segments in NSX. Tags can be used for dynamic security group membership, which allows for granular and flexible enforcement of security policies based on various criteria1
In the scenario, the company is deploying NSX micro-segmentation to secure a simple application composed of web, app, and database tiers. The naming convention will be:
WKS-WEB-SRV-XXX
WKY-APP-SRR-XXX
WKI-DB-SRR-XXX
The optimal way to group them to enforce security policies from NSX is to use tags membership. For example, the company can create three tags: Web, App, and DB, and assign them to the corresponding VMs based on their names. Then, the company can create three security groups: Web-SG, App-SG, and DB-SG, and use the tags as the membership criteria. Finally, the company can create and apply security policies to the security groups based on the desired rules and actions2
Using tags membership has several advantages over the other options:

It is more scalable and dynamic than using Edge as a firewall between tiers. Edge firewall is a centralized solution that can create bottlenecks and performance issues when handling large amounts of traffic3
It is more simple and efficient than doing a service insertion to accomplish the task. Service insertion is a feature that allows for integrating third-party services with NSX, such as antivirus or intrusion prevention systems. Service insertion is not necessary for basic micro-segmentation and can introduce additional complexity and overhead.
It is more flexible and granular than creating an Ethernet based security policy. Ethernet based security policy is a type of policy that uses MAC addresses as the source or destination criteria. Ethernet based security policy is limited by the scope of layer 2 domains and does not support logical constructs such as segments or groups.
To learn more about tags membership and how to use it for micro-segmentation in NSX, you can refer to the following resources:
VMware NSX Documentation: Security Tag 1
VMware NSX Micro-segmentation Day 1: Chapter 4 - Security Policy Design 2
VMware NSX 4.x Professional: Security Groups
VMware NSX 4.x Professional: Security Policies

QUESTION 59
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. Tier-1 gateway in distributed only mode
C. An Interface Group for the NSX Edge uplinks
D. A Punting Traffic Group for the NSX Edge uplinks

Correct Answer: C
Section:
Explanation:
To enable stateful active-active SNAT on a Tier-0 or Tier-1 gateway, you must configure an Interface Group for the NSX Edge uplinks. An Interface Group is a logical grouping of NSX Edge interfaces that belong to the same failure domain. A failure domain is a set of NSX Edge nodes that share the same physical network infrastructure and are subject to the same network failures.By configuring an Interface Group, you can ensure that the stateful services are distributed across different failure domains and can recover from network failures1

QUESTION 60
Which two are supported by L2 VPN clients? (Choose two.)

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

Correct Answer: C, D
Section:
Explanation:
The following L2 VPN clients are recommended:
1. NSX Managed NSX Edge in a separate NSX Managed environment.
* Overlay and VLAN segments can be extended.
2. Autonomous Edge:
* Enables L2 VPN access from a non-a NSX environment to NSX environments.
* Deployed by using an OVF file on a host that is not managed by NSX.
* Only VLAN segments can be extended.

QUESTION 61
As part of an organization's IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication).
What should an NSX administrator have ready before the integration can be configured? O

A. Active Directory LDAP integration with OAuth Client added

B. VMware Identity Manager with an OAuth Client added

C. Active Directory LDAP integration with ADFS

D. VMware Identity Manager with NSX added as a Web Application

Correct Answer: B
Section:
Explanation:
To configure NSX Manager for two-factor authentication (2FA), an NSX administrator must have VMware Identity Manager (vIDM) with an OAuth Client added. vIDM provides identity management services and supports various 2FA methods, such as VMware Verify, RSA SecurID, and RADIUS. An OAuth Client is a configuration entity in vIDM that represents an application that can use vIDM for authentication and authorization. NSX Manager must be registered as an OAuth Client in vIDM before it can use 2FA.References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware NSX-T Data Center Administration Guide, page 102.: VMware Blogs: Two-Factor Authentication with VMware NSX-T