2V0-41.23^Q&As^

VMware NSX 4.x Professional

Pass VMware 2V0-41.23 Exam with 100% Guarantee

Following Questions and Answers are all new published by VMware Official Exam Center

QUESTION 1

An NSX administrator is using ping to check connectivity between VM1 running on ESXi1 to VM2 running on ESXi2. The ping tests fails. The administrator knows the maximum transmission unit size on the physical switch is 1600.

Which command does the administrator use to check the VMware kernel ports for tunnel end point communication?

A. esxcli network diag ping-I vmk0O-H

B. vmkping ++netstack=geneve-d-s 1572

C. esxcli network diag ping-H

D. vmkping ++netstack=vxlan-d-s 1572

Correct Answer: B

The command vmkping ++netstack=geneve-d-s 1572 is used to check the VMware kernel ports for tunnel end point communication. This command uses the geneve netstack, which is the default netstack for NSX-T. The-d option sets the DF (Don\\'t Fragment) bit in the IP header, which prevents the packet from being fragmented by intermediate routers. The-s 1572 option sets the packet size to 1572 bytes, which is the maximum payload size for a geneve encapsulated packet with an MTU of 1600 bytes. The is the IP address of the remote ESXi host or VM. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware Knowledge Base: Testing MTU with the vmkping command (1003728). : VMware NSX-T Data Center Administration Guide, page 102.

QUESTION 2

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

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

QUESTION 3

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: BC

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 4

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: ACE

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.

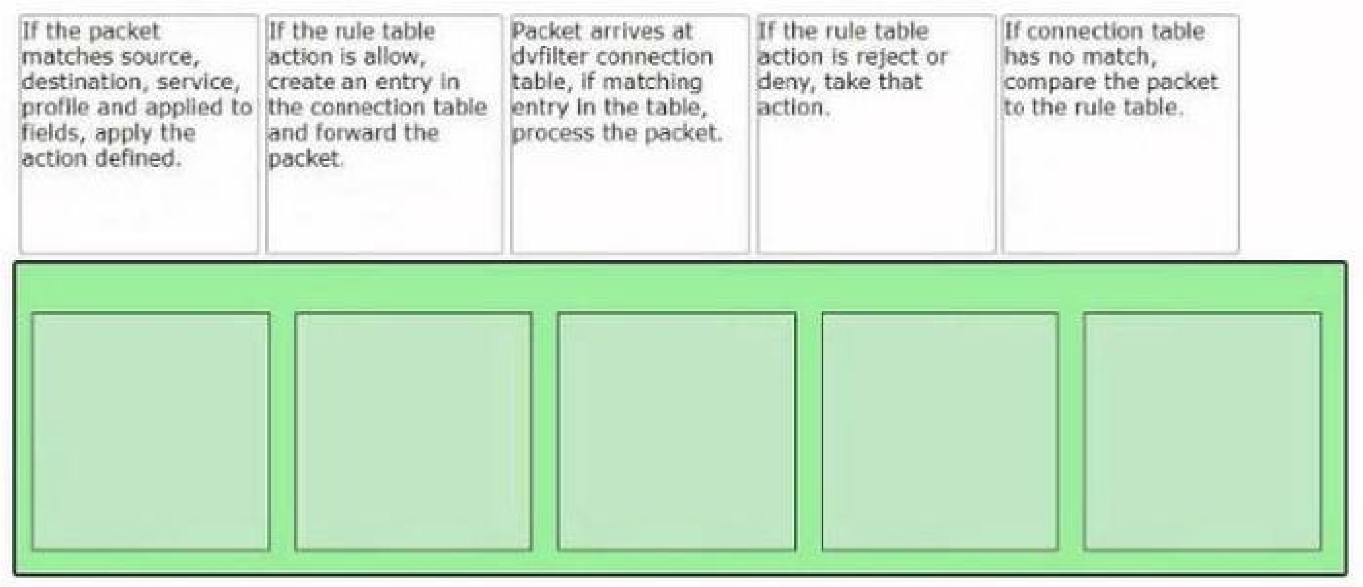
https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-486C1281-C6CF-47EC-B2A2-0ECFCC4A68CE.html

QUESTION 5

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.

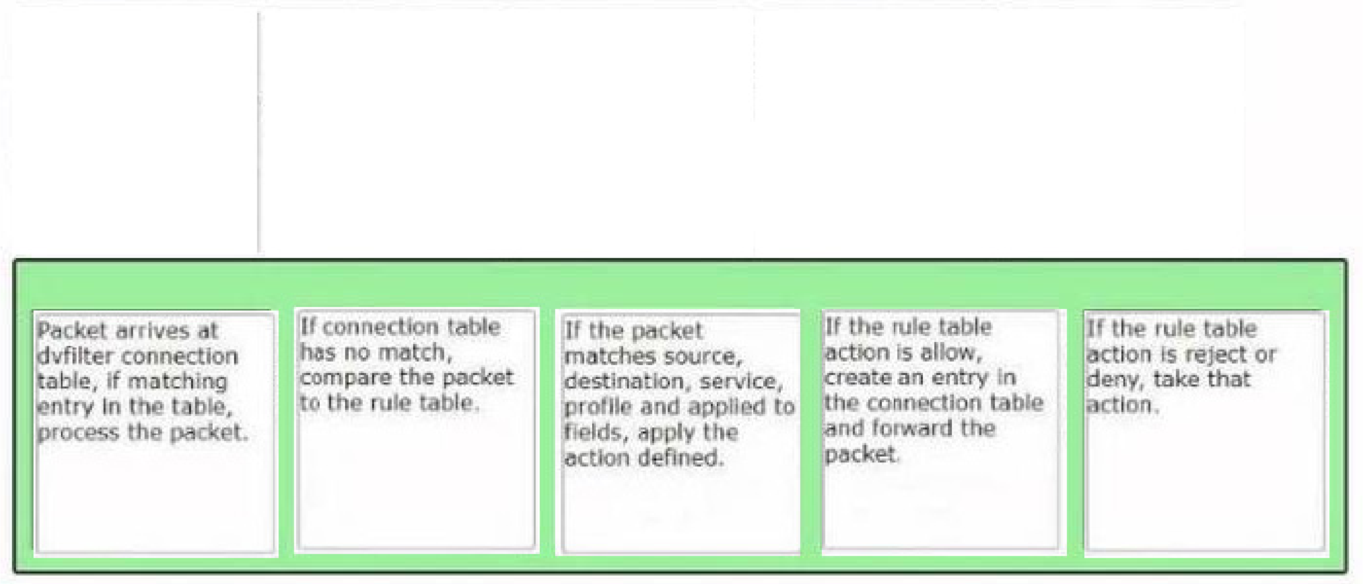
If the rule table action is allow, create an entry in the connection table and forward the packet.

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.

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.

QUESTION 6

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: BD

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 be 3.2 and later1. This is the minimum version that supports Distributed Security for VDS.

The VDS version must be 6.6.0 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 7

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: AE

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 Reference: https ://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-41CC06DF-1CD4-4233-B43E-492A9A3AD5F6.html https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/ com.vmware.nsx.admin.doc/GUID-D44C8923-992F-4695-B9C0-5CC271679D09.html

QUESTION 8

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: ABD

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 9

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

A. Reinstalling the NSX VIBs on the ESXi host.

B. Restarting the NTPservice on the ESXi host.

C. Changing the lime zone on the ESXi host.

D. Reconfiguring the ESXI host with a local NTP server.

Correct Answer: B

According to the web search results, error code 1001 is related to a time synchronization issue between the ESXi host and the NSX Manager. This can cause problems when configuring a time-based firewall rule, which requires the ESXi host

and the NSX Manager to have the same time zone and NTP server settings . To resolve this error, you need to restart the NTP service on the ESXi host to synchronize the time with the NSX Manager. You can use the following command to

restart the NTP service on the ESXi host:

```
/etc/init.d/ntpd restart
```

The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager.

Reconfiguring the ESXi host with a local NTP server may not be compatible with the NSX Manager\\'s NTP server.

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

Correct Answer: B

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 11

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

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 12

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: ADE

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 13

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

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 uide, 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 14

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

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 15

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

A. Network Segmentation

B. Virtual Security Zones

C. Edge Firewalling

D. Dynamic Routing

Correct Answer: A

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