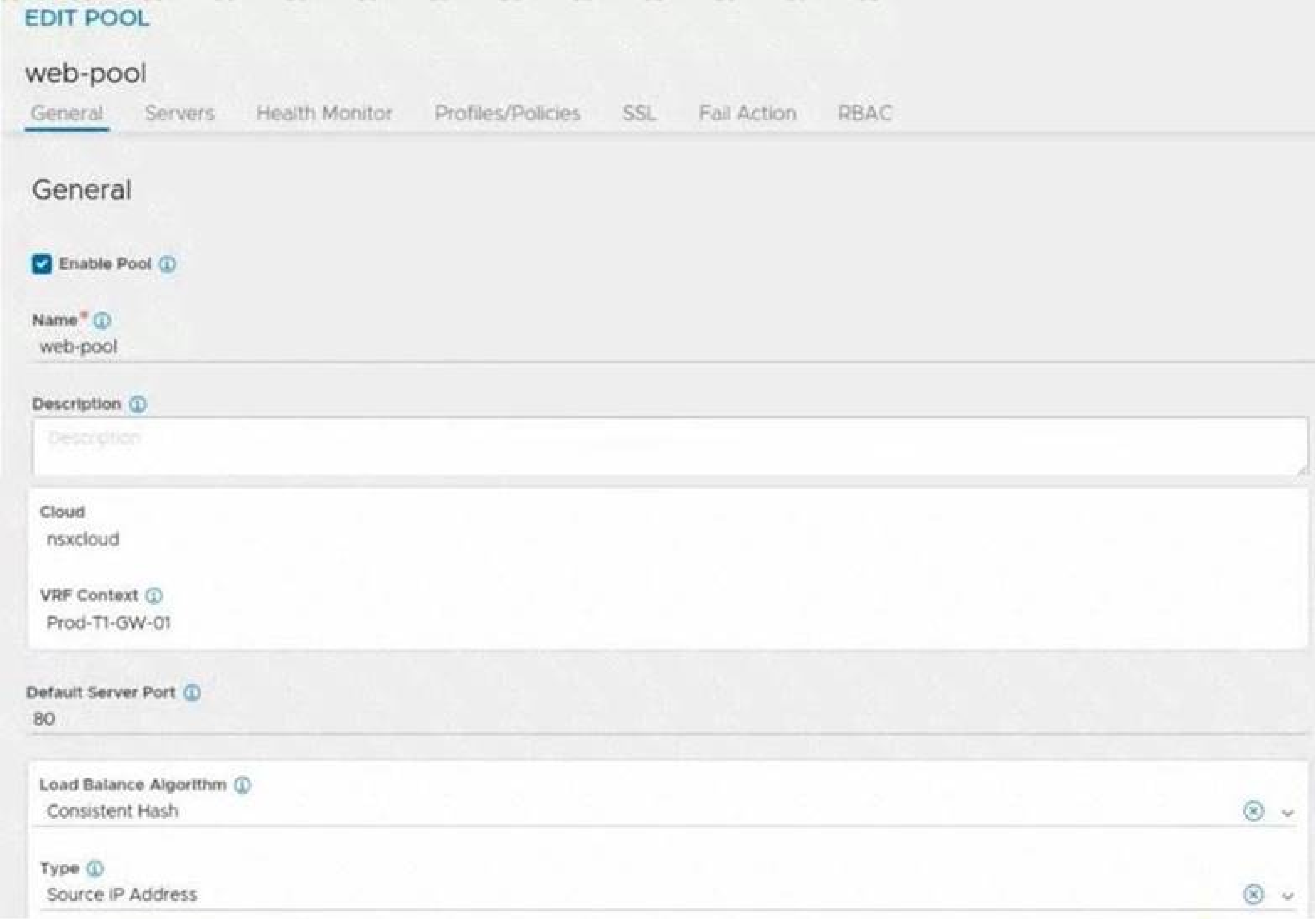
VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

NEW QUESTION 1
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.



web-pool

General

☑ Enable Pool

Name*
web-pool

Description
Description

Cloud
nsxcloud

VRF Context
Prod-T1-GW-01

Default Server Port
80

Load Balance Algorithm
Consistent Hash

Type
Source IP Address

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Load Balancing Algorithm

NEW QUESTION 2
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

Answer: CD

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/

NEW QUESTION 3
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.

Answer: D

NEW QUESTION 4
Which TraceFlow traffic type should an NSX administrator use tor validating connectivity between App and DB virtual machines that reside on different segments?

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

Answer: B

Explanation:
Unicast is the traffic type that an NSX administrator should use for validating connectivity between App and DB virtual machines that reside on different segments. According to the VMware documentation1, unicast traffic is the traffic type that is used to send a packet from one source to one destination. Unicast traffic is the most common type of traffic in a network, and it is used for applications such as web browsing, email, file transfer, and so on2. To perform a traceflow with unicast traffic, the NSX administrator needs to specify the source and destination IP addresses, and optionally the protocol and related parameters1. The traceflow will show the path of the packet across the network and any observations or errors along the way3. The other options are incorrect because they are not suitable for validating connectivity between two specific virtual machines. Multicast traffic is the traffic type that is used to send a packet from one source to multiple destinations simultaneously2. Multicast traffic is used for applications such as video streaming, online gaming and group communication4. To perform a traceflow with multicast traffic, the NSX administrator needs to specify the source IP address and the destination multicast IP address1. Broadcast traffic is the traffic type that is used to send a packet from one source to all devices on the same subnet2. Broadcast traffic is used for applications such as ARP, DHCP, and network discovery. To perform a traceflow with broadcast traffic, the NSX administrator needs to specify the source IP address and the destination MAC address as FF:FF:FF:FF:FF:FF1. Anycast traffic is not a valid option, as it is not supported by NSX Traceflow. Anycast traffic is a traffic type that is used to send a packet from one source to the nearest or best destination among a group of devices that share the same IP address. Anycast traffic is used for applications such as DNS, CDN, and load balancing.

NEW QUESTION 5
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. RADII 2.0
B. Keyoen Enterprise
C. RSA SecurelD
D. LDAP and OpenLDAP based on Active Directory (AD)
E. SecureDAP

Answer: CD

Explanation:
NSX supports two types of authentication, authorization, and accounting (AAA) systems when integrating with VMware Identity Manager: RSA SecurID and LDAP and OpenLDAP based on Active Directory (AD). RSA SecurID is a two-factor authentication system that uses a token-based approach to verify the identity of users. LDAP and OpenLDAP based on AD are directory services that store and manage user information and credentials. Both systems can be used to provide centralized authentication for users who want to access applications in an NSX environment .
https://blogs.vmware.com/networkvirtualization/2017/11/remote-user-authentication-and-rbac-with-nsx-t.html

NEW QUESTION 6
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.

NEW QUESTION 7
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.

Answer: D

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.

NEW QUESTION 8
When configuring OSPF on a Tler-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

Answer: BCF

Explanation:
ccording 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.

NEW QUESTION 9
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 10
Which is an advantages of a L2 VPN In an NSX 4.x environment?

A. Enables Multi-Cloud solutions
B. Achieve better performance
C. Enables VM mobility with re-IP
D. Use the same broadcast domain

Answer: D

Explanation:
L2 VPN is a feature of NSX that allows extending Layer 2 networks across different sites or clouds over an IPsec tunnel. L2 VPN has an advantage of enabling VM mobility with re-IP, which means that VMs can be moved from one site to another without changing their IP addresses or network configurations. This is possible because L2 VPN allows both sites to use the same broadcast domain, which means that they share the same subnet and VLAN .

NEW QUESTION 10
Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

A. HTTPS

B. TCP
C. SSH
D. UDP
E. TLS
F. SSL

Answer: BDE

Explanation:
An NSX administrator can use TCP, UDP, or TLS protocols to transfer log messages to a remote log server. These protocols are supported by NSX Manager, NSX Edge, and hypervisors for remote logging. A Log Insight log server supports all these protocols, as well as LI and LI-TLS, which are specific to Log Insight and optimize network usage. HTTPS, SSH, and SSL are not valid protocols for remote logging in NSX-T Data Center. References: : VMware NSX-T Data Center Administration Guide, page 102. : VMware Docs: Configure Remote Logging

NEW QUESTION 14
An NSX administrator Is treating a NAT rule on a Tler-0 Gateway configured In active-standby high availability mode. Which two NAT rule types are supported for this configuration? (Choose two.)

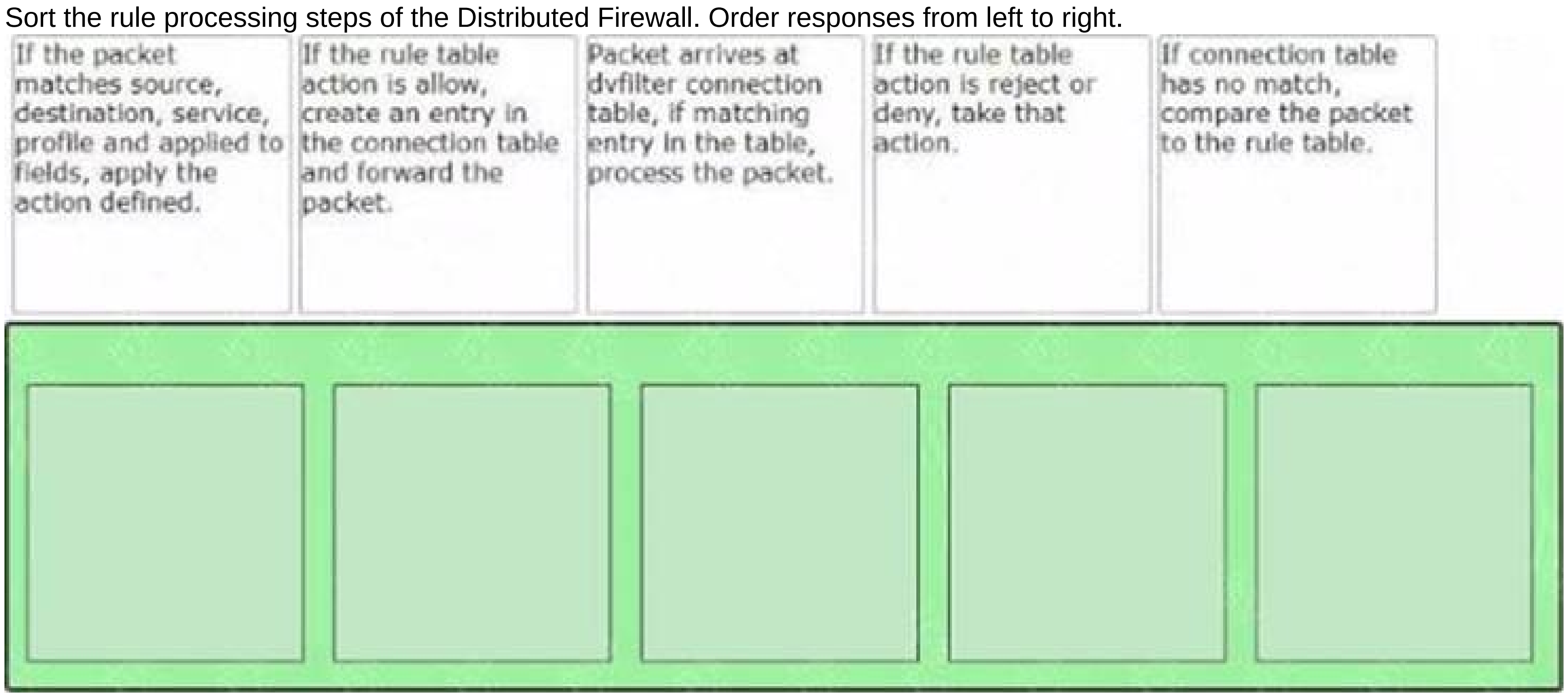
A. Reflexive NAT
B. Destination NAT
C. 1:1 NAT
D. Port NAT
E. Source NAT

Answer: BE

Explanation:
According to the VMware NSX Documentation, these are two NAT rule types that are supported for a tier-0 gateway configured in active-standby high availability mode. NAT stands for Network Address Translation and is a feature that allows you to modify the source or destination IP address of a packet as it passes through a gateway.

- Destination NAT: This rule type allows you to change the destination IP address of a packet from an external IP address to an internal IP address. You can use this rule type to provide access to your internal servers from external networks using public IP addresses.
- Source NAT: This rule type allows you to change the source IP address of a packet from an internal IP address to an external IP address. You can use this rule type to provide access to external networks from your internal servers using public IP addresses.

NEW QUESTION 19
Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.



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.

A. Mastered
B. Not Mastered

Answer: A

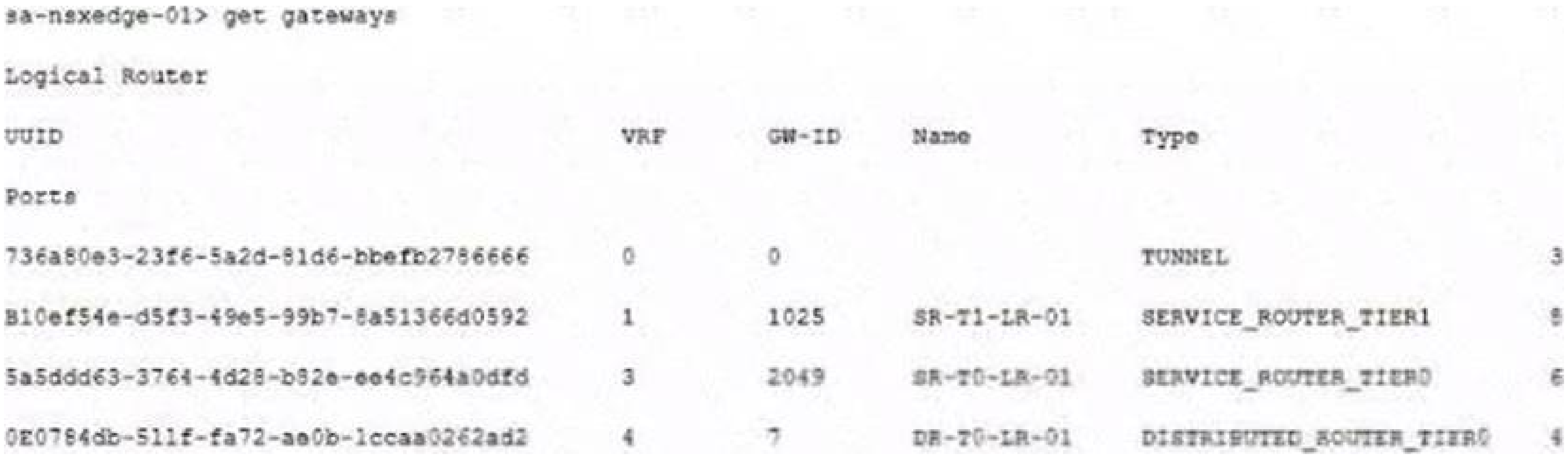
Explanation:
The correct order of the rule processing steps of the Distributed Firewall is as follows:

- 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 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 24
A customer has a network where BGP has been enabled and the BGP neighbor is configured on the Tier-0 Gateway. An NSX administrator used the get gateways

command to retrieve this Information:



```
sa-nsxedge-01> get gateways

Logical Router

UUID                                    VRF     GW-ID    Name           Type

Ports

736a80e3-23f6-5a2d-81d6-bbefb2786666    0       0                       TUNNEL                       3

810ef54e-d5f3-49e5-99b7-8a51366d0592    1       1025     SR-T1-LR-01    SERVICE_ROUTER_TIER1         8

5a5ddd63-3764-4d28-b82e-ee4c964a0dfd    3       2049     SR-T0-LR-01    SERVICE_ROUTER_TIER0         6

0E0784db-511f-fa72-ae0b-1ccaa0262ad2    4       7        DR-T0-LR-01    DISTRIBUTED_ROUTER_TIER0     4
```

Which two commands must be executed to check BGP neighbor status? (Choose two.)

A. vrf 1
B. vrf 4
C. sa-nexedge-01(tier1_sr> get bgp neighbor
D. sa-nexedge-01(tier0_sr> get bgp neighbor
E. sa-nexedge-01(tier1_dr)> get bgp neighbor
F. vrf 3

Answer: DF

Explanation:
BGP will be configured on the T0 SR. Connect to the VRF for the T0 SR and run get bgp neighbor once connected to it.
https://docs.vmware.com/en/VMware-Validated-Design/5.1/sddc-deployment-of-vmware-nsx-t-workload-doma
For the BGP configuration on NSX-T, the Tier-0 Service Router (SR) is typically where BGP is configured. To check the BGP neighbor status:
Connect to the VRF for the T0 SR, which is VRF 3 based on the provided output. Run the command to get BGP neighbor status once connected to it.

NEW QUESTION 26
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.

Answer: B

Explanation:
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.

NEW QUESTION 31
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

Answer: AB

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

NEW QUESTION 35
Which two are requirements for FQDN Analysis? (Choose two.)

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

E. A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Answer: AD

Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-C5CD87FD-8095-49F3-97CE-E606AB89

NEW QUESTION 36
NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

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

Answer: A

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

NEW QUESTION 37
Which Is the only supported mode In NSX Global Manager when using Federation?

A. Controller
B. Policy
C. Proxy
D. Proton

Answer: B

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.

NEW QUESTION 38
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

Answer: B

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-D5B6DC79-6733-44

NEW QUESTION 43
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

Answer: B

Explanation:
To make NSX Edge Services available to a VM on a VLAN-backed logical switch, you need to configure
a VLAN Uplink on the Tier-0 Gateway. A VLAN Uplink is a logical interface that connects the Tier-0 Gateway to the physical network and provides external connectivity for the NSX Edge Services1. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface1.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266

NEW QUESTION 45
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.

Answer: DE

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.

NEW QUESTION 50
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.

Answer: D

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.

NEW QUESTION 55
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.

Answer: AE

Explanation:
East-West Malware Prevention is a feature of NSX Advanced Threat Prevention that can detect and prevent malicious files in the network traffic between virtual machines (east-west) and between the data center and the external network (north-south). To enable this feature, a Service Virtual Machine (SVM) is deployed on every ESXi host to intercept and analyze the files in the east-west traffic. An agent must also be installed on every NSX Edge node to intercept and analyze the files in the north-south traffic. The NSX Application Platform is a cloud-based service that provides threat intelligence and analysis for the NSX Malware Prevention feature. The NSX Application Platform must have Internet access to receive updates and send files for analysis. The NSX Edge nodes must also have Internet access to communicate with the NSX Application Platform.
References:

- Overview of NSX IDS/IPS and NSX Malware Prevention
- Administering NSX Malware Prevention

NEW QUESTION 59
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

Answer: D

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-133650FD

NEW QUESTION 64
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 VPN
B. Layer 2 bridge
C. Layer 2 broadcast domain
D. Layer 3 route

Answer: C

Explanation:
An overlay segment is a logical construct that provides Layer 2 connectivity between virtual machines that are attached to it. An overlay segment can span multiple hosts and can be extended across different subnets or locations using Geneve encapsulation3. Therefore, two virtual machines on the same overlay segment belong to the same Layer 2 broadcast domain, which means they can communicate with each other using their MAC addresses without requiring any routing. The other options are incorrect because they involve Layer 3 or higher network boundaries, which require routing or tunneling to connect different segments. References: VMware NSX Documentation

NEW QUESTION 66
Which steps are required to activate Malware Prevention on the NSX Application Platform?

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

Answer: D

Explanation:
To activate Malware Prevention on the NSX Application Platform, the steps are:

- In the NSX Manager UI, select System and in the Configuration section, select NSX Application Platform.
- Navigate to the Features section, locate the NSX Malware Prevention feature card, and click Activate or anywhere in the card.
- In the NSX Malware Prevention activation window, select one of the available cloud regions from which you can access the NSX Advanced Threat Prevention cloud service.
- Click Run Prechecks. This precheck process can take some time as the system validates that the minimum license requirement is met and that it is eligible for use with the NSX Advanced Threat Prevention cloud service. The system also validates that the selected cloud region is reachable.
- Click Activate. This step can take some time1. Therefore, the correct answer is D. The other options are incorrect because they involve activating or deploying NSX Network Detection and Response, which is a different feature from Malware Prevention. References: Activate NSX Malware Prevention

NEW QUESTION 67
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

Answer: AB

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
```

NEW QUESTION 68
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.

Answer: D

Explanation:
The answer is D. 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-

NEW QUESTION 72

......