Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

killexams.com

Vmware

5V0-41.21

VMware NSX-T Data Center 3.1 Security

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/5V0-41.21

Question: 1

Which three are required by URL Analysis? (Choose three.)

A. NSX Enterprise or higher license key
B. Tier-1 gateway
C. Tier-0 gateway
D. OFW rule allowing traffic OUT to Internet
E. Medium-sized edge node (or higher), or a physical form factor edge
F. Layer 7 DNS firewall rule on NSX Edge cluster

Answer: A,B,D,F

Explanation:

To use URL Analysis, you will need to have a Tier-1 gateway and a Layer 7 DNS firewall rule on the NSX Edge cluster. Additionally, you will need to configure an OFW rule allowing traffic OUT to the Internet. Lastly, a medium-sized edge node (or higher), or a physical form factor edge is also required as the URL Analysis service will run on the edge node. For more information, please see this VMware Documentation article[1], which explains how to configure URL Analysis on NSX.

[1] https://docs.vmware.com/en/VMware-NSX-T-Data-

Center/3.1/nsxt_31_url_analysis/GUID-46BC65F3-7A45-4A9F-B444-E4A1A7E0AC4A.html

Question: 2

What needs to be configured on each transport node prior to using NSX-T Data Center Distributed Firewall time-based rule publishing?

A. DNS
B. NTP
C. PAT
D. NAT

Answer: B

Explanation:

In order to use NSX-T Data Center Distributed Firewall time-based rule publishing, the NTP (Network Time Protocol) needs to be configured on each transport node. This ensures that the transport nodes have accurate time synchronization, which is required for time-based rule publishing. Additionally, DNS (Domain Name System) and PAT (Port Address Translation) may also need to be configured on each transport node, depending on the desired configuration. References:

[1] https://docs.vmware.com/en/VMware-NSX-T/2.5/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-

6A17A6F39A6C.html [2] https://docs.vmware.com/en/VMware-NSX-T/2.4/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-6A17A6F39A6C.html

Question: 3

An NSX administrator is trying to find the dvfilter name of the sa-web-01 virtual machine to capture the sa-web-01 VM traffic.

What could be a reason the sa-web-01 VM dvfilter name is missing from the command output?

A. sa-web-01 VM has the no firewall rules configured.
B. ESXi host has 5SH disabled.
C. sa-web-01 is powered Off on ESXi host.
D. ESXi host has the firewall turned off.

Answer: C

Explanation:

The most likely reason the sa-web-01 VM dvfilter name is missing from the command output is that the sa-web-01 VM is powered off on the ESXi host. The dvfilter name is associated with the VM when it is powered on, and is removed when the VM is powered off. Therefore, if the VM is powered off, then the dvfilter name will not be visible in the command output. Other possible reasons could be that the ESXi host has the firewall turned off, the ESXi host has 5SH disabled, or that the sa-web-01 VM has no firewall rules configured.

References: [1] https://kb.vmware.com/s/article/2143718 [2] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-AC3CC8A3-B2DE-4A53-8F09-B8EEE3E3C7D1.html

Question: 4

Which two statements are true about IDS/IPS signatures? (Choose two.)

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

Answer: A,C

Explanation:

(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUID-AFAF58DB-E661-4A7D-A8C9-70A3F3A3A3D3.html)

Question: 5

An organization is using VMware Identity Manager (vIDM) to authenticate NSX-T Data Center users Which two selections are prerequisites before configuring the service? (Choose two.)

A. Validate vIDM functionality
B. Assign a role to users
C. Time Synchronization
D. Configure vIDM Integration
E. Certificate Thumbprint from vIDM

Answer: A,D,E

Explanation:

The two prerequisites before configuring the VMware Identity Manager (vIDM) service for NSX-T Data Center are Configure vIDM Integration and Certificate Thumbprint from vIDM. In order to use vIDM for authentication, it must be integrated with NSX-T Data Center, which will involve configuring the vIDM integration service. Additionally, a certificate thumbprint from vIDM must be provided to NSX-T Data Center to enable secure communication between the two services. Time synchronization and assigning roles to users are not necessary prerequisites for configuring the vIDM service.

References: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-1B4EA3C9-8F43-4C4F-A86A-BFB0DB6D1A6C.html [2] https://docs.vmware.com/en/VMware-Identity-Manager/3.3/com.vmware.identity.install.doc/GUID-D56A0C0A-52F

Question: 6

Which esxcli command lists the firewall configuration on ESXi hosts?

A. esxcli network firewall ruleset list
B. vsipioct1 getrules -filter <filter-name>
C. esxcli network firewall rules
D. vsipioct1 getrules -f <filter-name>

Answer: A

Explanation:

This command allows you to display the current firewall ruleset configuration on an ESXi host.

It will show the ruleset names, whether they are enabled or disabled, and the services and ports that the ruleset applies to.

For example, you can use the command "esxcli network firewall ruleset list" to list all the firewall rulesets on the host.

You can also use the command "esxcli network firewall ruleset rule list -r <ruleset_name>" to display detailed information of the specific ruleset, where <ruleset_name> is the name of the ruleset you want to display.

It's important to note that you need to have access to the ESXi host's command-line interface (CLI) and have appropriate permissions to run this command.

https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcli.ref.doc/esxcli_network_firewall_ruleset.html

Question: 7

Which three are required to configure a firewall rule on a getaway to allow traffic from the internal to web servers? (Choose three.)

A. Create a URL analysis profile for web hosting category.
B. Create a firewall rule in System category.
C. Enable Firewall Service for gateway.
D. Create a firewall policy in Local Gateway category.
E. Add a firewall rule in Local Gateway category.
F. Disable the firewall rule in Default category.

Answer: A,C,D,E

Explanation:

In order to configure a firewall rule on a gateway to allow traffic from the internal to web servers, the administrator needs to enable the Firewall Service for the gateway, create a firewall policy in the Local Gateway category, and add a firewall rule in the Local Gateway category. This firewall rule should specify the web servers as the destination and the internal network as the source.

For more information on how to configure firewall rules on a gateway, please refer to the NSX-T Data Center documentation: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-firewall/GUID-3A79CA7A-9D5E-4F2B-8F75-4EA298E4A4D5.html

Question: 8

Which are two use-cases for the NSX Distributed Firewall'(Choose two.)

A. Zero-Trust with segmentation
B. Security Analytics
C. Lateral Movement of Attacks prevention
D. Software defined networking
E. Network Visualization

Answer: A,C

Explanation:

Zero-Trust with segmentation is a security strategy that uses micro-segmentation to protect a network from malicious actors. By breaking down the network into smaller segments, the NSX Distributed Firewall can create a zero-trust architecture which limits access to only users and devices that have been authorized. This reduces the risk of a malicious actor gaining access to sensitive data and systems.

Lateral Movement of Attacks prevention is another use-case for the NSX Distributed Firewall. Lateral movement of attacks are when an attacker is already inside the network and attempts to move laterally between systems. The NSX Distributed Firewall can help protect the network from these attacks by controlling the flow of traffic between systems and preventing unauthorized access.

References: https://www.vmware.com/products/nsx/distributed-firewall.html
https://searchsecurity.techtarget.com/definition/zero-trust-network

Question: 9

A security administrator is required to protect East-West virtual machine traffic with the NSX Distributed Firewall.

What must be completed with the virtual machine's vNIC before applying the rules?

A. It is connected to the underlay.
B. It must be connected to a vSphere Standard Switch.
C. It is connected to an NSX managed segment.
D. It is connected to a transport zone.

Answer: C

Explanation:

In order to apply the rules, the vNIC of the virtual machine must be connected to an NSX managed segment. The NSX managed segment is a logical representation of the virtual network, and all rules are applied at this level.

For more information on NSX Distributed Firewall and how to configure it, please refer to the NSX-T Data Center documentation: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-firewall/GUID-B6B835F2-B6F2-4468-8F8E-6F7B9B9D6E91.html

Question: 10

An administrator wants to use Distributed Intrusion Detection.

How is this implemented in an NSX-T Data Center?

A. As a distributed solution across multiple ESXi hosts.
B. As a distributed solution across multiple KVM hosts.
C. As a distributed solution across multiple NSX Managers.
D. As a distributed solution across multiple NSX Edge nodes.

Answer: A

Explanation:

Distributed Intrusion Detection System (IDS) is part of the NSX-T data center and operates on multiple ESXi hosts.

Question: 11

An administrator wants to configure NSX-T Security Groups inside a distributed firewall rule.

Which menu item would the administrator select to configure the Security Groups?

A. System
B. Inventory
C. Security

D. Networking

Answer: C

Explanation:

To configure NSX-T Security Groups inside a distributed firewall rule, the administrator would select the "Security" menu item in the NSX-T Manager user interface. Within the Security menu, the administrator would navigate to the "Groups" option, where they can create, edit, and manage security groups. These groups can then be used in the "Applied To" column when creating or editing firewall rules.

In the Security menu, administrator can also configure other security features such as firewall, micro-segmentation, intrusion detection and prevention, and endpoint protection. References:

â VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html

â VMware NSX-T Data Center Security Groups documentation

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.groups.doc/GUID-8C8DDC52-0B91-4E9F-8D8E-E1649D3C3BBD.html

Question: 12

An administrator has enabled the "logging" option on a specific firewall rule. The administrator does not see messages on the Logging Server related to this firewall rule.

What could be causing the issue?

A. The logging on the firewall policy needs to be enabled.
B. Firewall Rule Logging is only supported in Gateway Firewalls.
C. NSX Manager must have Firewall Logging enabled.
D. The logging server on the transport nodes is not configured.

Answer: D

Question: 13

An NSX administrator has been tasked with deploying a NSX Edge Virtual machine through an ISO image.

Which virtual network interface card (vNIC) type must be selected while creating the NSX Edge VM allow participation in overlay and VLAN transport zones?

A. e1000
B. VMXNET2
C. VMXNET3
D. Flexible

Answer: C

Explanation:

When deploying an NSX Edge Virtual Machine through an ISO image, the virtual network interface card (vNIC) type that must be selected is VMXNET3 in order to allow participation in overlay and VLAN transport zones. VMXNET3 is a high-performance and feature-rich paravirtualized NIC that provides a significant performance boost over other vNIC types, as well as support for both overlay and VLAN transport zones.

For more information on deploying an NSX Edge Virtual Machine through an ISO image, please refer to the NSX-T Data Center documentation: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-deploy-config/GUID-A782558B-A72B-4848-B6DB-7A8A9E71FFD6.html

Question: 14

A security administrator is verifying the health status of an NSX Service Instance.

Which two parameters must be functioning for the health status to show as Up? (Choose two.)

A. VMs must have at least one vNI
B. VMs must not have existing endpoint protection rules.
C. VMs must have virtual hardware version 9 or higher.
D. VMs must be available on the host.
E. VMs must be powered on.

Answer: A,C,D

Explanation:

The health status of an NSX Service Instance is an indicator of the overall health and functionality of the service.

For an NSX Service Instance to show as Up, the following two parameters must be functioning:

D. VMs must be available on the host - The VMs that are associated with the service must be present on the host and able to communicate with the NSX Manager. If a VM is not available on the host, the service will not be able to function properly.

E. VMs must be powered on - The VMs that are associated with the service must be powered on and running. If a VM is not powered on, the service will not be able to function properly.

Question: 15

In a brownfield environment with NSX-T Data Center deployed and configured, a customer is interested in Endpoint Protection integrations.

What recommendation should be provided to the customer when it comes to their existing virtual machines?

A. Virtual machine must be protected by vSphere H
B. Virtual machine hardware should be version 10 or higher.
C. A minimum installation of VMware tools is required.
D. A custom install of VMware tools is required to select the drivers.

Answer: B

Explanation:

VMware Tools is a suite of utilities that enhances the performance of a virtual machine â s guest operating system. It is required for endpoint protection integrations in a NSX-T Data Center environment.

Question: 16

Which dot color indicates an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center?

A. blinking yellow dot
B. solid red dot
C. solid orange dot
D. blinking orange dot

Answer: C

Explanation:

The dot color that indicates an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center is a solid orange dot. This indicates that the attack has been detected and is ongoing at a medium severity level.

References: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin_guide/GUID-A8FAC8A1-F9F9-43EC-A822-F2F2CB5C5E5A.html#GUID-A8FAC8A1-F9F9-43EC-A822-F2F2CB5C5E5A

In the IDS/IPS events tab of NSX-T Data Center, different colors of dots are used to indicate the severity of an attack.

â A solid red dot indicates a critical attack, which is the highest severity level.

â A solid orange dot indicates a medium attack, which is a moderate severity level.

â A solid yellow dot indicates a low attack, which is the lowest severity level.

In this case, a solid orange dot is used to indicate an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center.

It's worth noting that there is no blinking dots in this context, all the dots are solid.

References:

â VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html

â VMware NSX-T Data Center Intrusion Detection and Prevention documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.ids.doc/GUID-C4ED1F4D-4E4B-4A9C-9F5C-7AC081A5C5D5.html

Question: 17

How does N5X Distributed IDS/IPS keep up to date with signatures?

A. NSX Edge uses manually uploaded signatures by the security administrator.
B. NSX-T Data Center is using a cloud based database to download the IDS/IPS signatures.
C. NSX Manager has a local IDS/IPS signatures database that does not need to be updated.

D. NSX Distributed IDS/IPS signatures are retrieved from updates.vmware.com.

Answer: B

Question: 18

What is the default action of the Default Layer 3 distributed firewall rule?

A. Drop
B. Allow
C. Forward
D. Reject

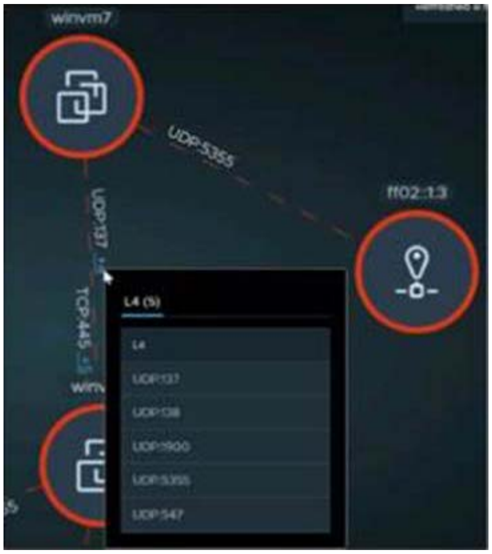
Answer: B

Explanation:

The default action of the Default Layer 3 distributed firewall rule in NSX-T Data Center is to allow. This default policy is to allow all unless otherwise specified, ensuring network connectivity isn't lost when the distributed firewall is enabled. However, in a production environment, this default policy is typically overridden to be more secure.

Question: 19

Refer to the exhibit.



An administrator is reviewing NSX Intelligence information as shown in the exhibit.

What does the red dashed line for the UDP: 137 flow represent?

A. Discovered communication
B. Allowed communication
C. Blocked communication
D. Unprotected communication

Answer: C

Explanation:

The red dashed line for the UDP:137 flow in the NSX Intelligence information represents blocked communication. This indicates that the NSX Distributed Firewall has blocked the communication between the source and destination IP addresses on port 137. For more information on NSX Intelligence and how to use it, please refer to the NSX-T Data Center documentation: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-intelligence/GUID-C2B2AF2E-A76A-46B8-A67A-42D7A9E924A9.html

Question: 20

When configuring members of a Security Group, which membership criteria art permitted?

A. Virtual Machine, Physical Machine, Cloud Native Service Instance, and IP Set
B. Segment Port, Segment, Virtual Machine, and IP Set
C. Virtual Interface, Segment, Cloud Native Service Instance, and IP Set.
D. Virtual Interface, Segment, Physical Machine, and IP Set

Answer: B

Explanation:

When configuring members of a Security Group in NSX-T Data Center, membership criteria can include Segment Port, Segment, Virtual Machine, and IP Set.