VMware.5V0-41.21.v2023-05-08.q32

Exam Code:	5V0-41.21
Exam Name:	VMware NSX-T Data Center 3.1 Security
Certification Provider:	VMware
Free Question Number:	32
Version:	v2023-05-08
# of views:	847
# of Questions views:	320
https://www.freeqas.com/qa/VMware/5V0-41.21/VMware.5V0-41.21.v2023-05-08.q32.html	

NEW QUESTION: 1
Which two are requirements for URL Analysis? (Choose two.)
A. The ESXi hosts require access to the Internet to download category and reputation definitions.
B. A layer 7 gateway firewall rule must be configured on the tier-0 gateway uplink to capture DNS traffic.
C. A layer 7 gateway firewall rule must be configured on the tier-1 gateway uplink to capture DNS traffic,
D. The NSX Edge nodes require access to the Internet to download category and reputation definitions.
E. The NSX Manager requires access to the Internet to download category and reputation definitions.
Answer: (SHOW ANSWER)
The NSX Edge nodes require access to the Internet to download category and reputation definitions, and a layer 7 gateway firewall rule must be configured on the tier-1 gateway uplink to capture DNS traffic. This will allow the URL Analysis service to analyze incoming DNS traffic and block malicious requests. 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

NEW QUESTION: 2
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 vNIC.
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: D,E (LEAVE A REPLY)

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:

1. 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.
2. 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.

NEW QUESTION: 3

Which 3 CU commands ant required to configure remote logging on an ESXI host? (Choose three.)

A. esxcl; systex syslcg -sx firewall enable

B. esxcli network services restart --firewall

C. esxcli systex syslcg reload

D. esxcli systex syslog config set "loghost-udp://<log server IP>:<port>

E. esxcli network firewall ruleset set -r syslog -e true

Answer: C,D,E (LEAVE A REPLY)

The three CU commands required to configure remote logging on an ESXi host are esxcli syslog config set "loghost-udp://<log server IP>:<port>", esxcli network firewall ruleset set -r syslog -e true, and esxcli system syslog reload. The first command sets the remote log server IP address and port for the ESXi host, the second command enables the syslog ruleset, and the third command reloads the syslog configuration. This will ensure that all syslog messages generated by the ESXi host will be sent to the remote log server. Reference: [1] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-CFE0E8FC-7C27-4F45-A037-CACCD8A1E9A2.html [2] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-A2F2A3D2-076A-4FE6-

NEW QUESTION: 4

What type of IDS/IPS system deployment allows an administrator to block a known attack?

A. A system deployed in SPAN port mode.

B. A system deployed inline with ALERT and DROP action.

C. A system deployed inline with ALERT action.

D. A system deployed in TERM mode.

Answer: B (LEAVE A REPLY)

as a system deployed inline with both ALERT and DROP action will provide the ability to block attacks when a match is found For further reading, see the VMware NSX-T Data Center Administration Guide (https://pubs.vmware.com/NSX-T-Data-

Center/index.html#com.vmware.nsxt.admin.doc/GUID-D9A6B1E7-FFCD-47A7-8E0C-FDD3DE6AC2B6.html) for more information on configuring an IDS/IPS system.

NEW QUESTION: 5
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 (LEAVE A REPLY)
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.
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html 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

NEW QUESTION: 6
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: (SHOW ANSWER)
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. Reference: [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

NEW QUESTION: 7
An organization wants to add security controls for contractor virtual desktops. Which statement Is true when configuring an NSX Identity firewall rule?
A. User Identity can be used in the both the Source and the Destination sections of the firewall rule.
B. User Identity can only be used in the Source section of the firewall rule.
C. User Identity cannot be used in Source or Destination sections of the firewall rule.
D. User Identity can only be used in the Destination Section of the firewall rule.
Answer: B (LEAVE A REPLY)
In NSX-T, Identity firewall rules allow you to specify security controls based on the identity of the user, rather than the IP address or other network-based attributes. User identity can be used as a source in the firewall rule.

NEW QUESTION: 8
There has been a confirmed case of virus infection on multiple VMs managed by Endpoint Protection. A security administrator wants to create a group to quarantine infected VMs in the future.
What criteria will be used to build this group?
A. NSX Tags
B. Segment
C. vSphere Tags
D. VM Name
Answer: C (LEAVE A REPLY)
vSphere Tags are labels that can be used to group and categorize virtual machines and other objects. The security administrator can create a tag for quarantined VMs and assign it to any VMs that are confirmed to be infected. This will help identify and isolate the infected VMs more quickly and easily in the future.

NEW QUESTION: 9
What is the NSX feature that allows a user to block ICMP between 192.168.1.100 and 192.168.1.101?
A. NSX Distributed Switch Agent
B. NSX Distributed IDS/IPS
C. NSX Distributed Routing
D. NSX Distributed Firewall
Answer: D (LEAVE A REPLY)
NSX Distributed Firewall is used to create firewall rules to control traffic between networks.

For further reading, see the VMware NSX-T Data Center Administration Guide (https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUID-4B6A4A87-F9C7-4AAB-923F-C6B84C33AF7D.html) for more information on configuring firewall rules.

NEW QUESTION: 10
To which network operations does a user with the Security Engineer role have full access permission?
A. Networking IP Address Pools, Networking NAT, Networking DHCP
B. Networking Forwarding Policies, Networking NAT, Networking VPN
C. Networking Load Balancing, Networking DNS, Networking Forwarding Policies
D. Networking DHCP, Networking NAT, Networking Segments
Answer: A (LEAVE A REPLY)
A user with the Security Engineer role has full access permission to Networking IP Address Pools, Networking NAT, Networking DHCP, Networking Forwarding Policies, Networking VPN, Networking Load Balancing, Networking DNS, and Networking Segments. These operations allow the Security Engineer to configure and manage the necessary networking components to ensure a secure network environment. For example, Networking IP Address Pools allows the Security Engineer to create and manage IP address pools for assigning IP addresses to nodes on the network, Networking NAT allows the Security Engineer to configure Network Address Translation to improve security and privacy, and Networking Forwarding Policies allows the Security Engineer to configure policies for routing traffic between different networks. Reference: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-ACA9C0F2-2F2E-43E3-A3C3-DEEECB7CFE8F.html [2] https://docs.vmware.com/en/VMware-NSX-T/2.5/vmware-nsx-t-25

NEW QUESTION: 11
What component in a transport node receives the firewall configuration from the central control plane?
A. nsx-ccp
B. nsx-appl-proxy
C. nsx-mpa
D. nsx-proxy
Answer: C (LEAVE A REPLY)
The component in a transport node that receives the firewall configuration from the central control plane is the NSX-MPA (Management Plane Agent). The NSX-MPA runs on each transport node and is responsible for connecting to the NSX-T central control plane and receiving the configuration for the transport node. It is also responsible for pushing the configuration down to the other components on the transport node, such as the NSX-Proxy, NSX-Appl-Proxy, and NSX-CCP. Reference: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-8C33F5B5-1B98-4A5F-B5B1-D70BE45F9FAD.html [2]

https://docs.vmware.com/en/VMware-NSX-T/3.0/com.vmware.nsxt.install.doc/GUID-C129F7F0-E6F8-4A14-B2B0-9D6F3A7A3F62.

NEW QUESTION: 12
Which two are true of the NSX Gateway Firewall? (Choose two.)
A. Firewall rules in System category cannot be edited.
B. Firewall rules in Pre Rule category are applied to all gateways.
C. NAT service can be configured in NSX Gateway Firewall policy.
D. Security Groups can be used in Applied-To column.
E. Applied-To can be configured at Firewall Policy level.
Answer: B,D (LEAVE A REPLY)
NSX Gateway Firewall is a distributed firewall that provides security for east-west traffic within a virtual environment.
1. Firewall rules in Pre Rule category are applied to all gateways. This category contains system-defined rules that are always applied first to all gateways and cannot be modified. These rules include the default deny all rule and others that control basic connectivity.
2. Security Groups can be used in Applied-To column. Security groups allow you to group together VMs that have similar security requirements and then apply firewall policies to those groups. This way you can apply the same security rules to multiple VMs at once, instead of configuring the rules on each individual VM.
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html VMware NSX-T Data Center Gateway Firewall documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.firewall.doc/GUID-4C5D5A5F-8FDF-4F2A-9C5A-2C1903A3E5A5.html

NEW QUESTION: 13
At which OSI Layer do Next Generation Firewalls capable of analyzing application traffic operate?
A. Layer 4
B. Layer 3
C. Layer 7
D. Layer 2
Answer: (SHOW ANSWER)
Next Generation Firewalls are capable of analyzing application traffic at Layer 7 of the OSI model. Layer 7 is the Application Layer, which is where the application-level protocols, such as HTTP and FTP, are implemented. Next Generation Firewalls are able to inspect the application traffic and apply rules based on the content of the application-level packets.
For more information on the OSI model and Next Generation Firewalls, please refer to the following resources:
* OSI Model: https://en.wikipedia.org/wiki/OSI_model * Next Generation Firewalls: https://en.wikipedia.org/wiki/Next-generation_firewall

NEW QUESTION: 14
A customer has a requirement to achieve Zero-Trust Security and minimize operational overhead. Which VMware solution can be used by the customer to achieve the requirement?
A. NSX Manager
B. Tanzu Kubernetes Grid
C. Carbon Black Anti-Virus
D. NSX Intelligence
Answer: D (LEAVE A REPLY)
NSX Intelligence is a security analytics solution from VMware that can be used to achieve Zero-Trust Security and minimize operational overhead. It provides an AI-driven security analytics platform that can detect and respond to threats in real-time, allowing organizations to quickly identify threats and respond to them before they can cause damage. Additionally, it also provides automated security operations and orchestration capabilities that can help reduce manual overhead and free up resources for more important tasks.
For more information on NSX Intelligence and how it can help achieve Zero-Trust Security and minimize operational overhead, 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

NEW QUESTION: 15
Which two statements are true about NSX Intelligence? (Choose two.)
A. NSX Intelligence assists to build service insertion with Partner SVM.
B. NSX Intelligence supports planning of distributed firewall rules and policy.
C. NSX Intelligence can help to visualize network physical infrastructure.
D. NSX Intelligence can be used in conjunction with vRealize Network Insight.
E. NSX Intelligence supports planning of NSX-T Edge Firewall rules and policy.
Answer: (SHOW ANSWER)
The two statements that are true about NSX Intelligence are that it assists to build service insertion with Partner SVM and that it supports planning of NSX-T Edge Firewall rules and policy. NSX Intelligence can be used in conjunction with vRealize Network Insight to provide visibility and insights into the network, but it cannot be used to visualize the physical infrastructure. Additionally, while it can help to plan firewall rules and policy, it does not support planning of distributed firewall rules and policy.

NEW QUESTION: 16
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: D (LEAVE A REPLY)
An administrator can implement Distributed Intrusion Detection as a distributed solution across multiple NSX Edge nodes in an NSX-T Data Center. This allows for real-time monitoring of network traffic, as well as detection and prevention of malicious activity. Additionally, it can be used to identify, investigate, and respond to potential security threats. Reference: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-1F8741C0-D1CD-4EA3-A2BB-98CEF7F8D1DA.html [2] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-nsx-data-center-for-vsphere-distributed-intrusion-detection-deployment-guide.pdf

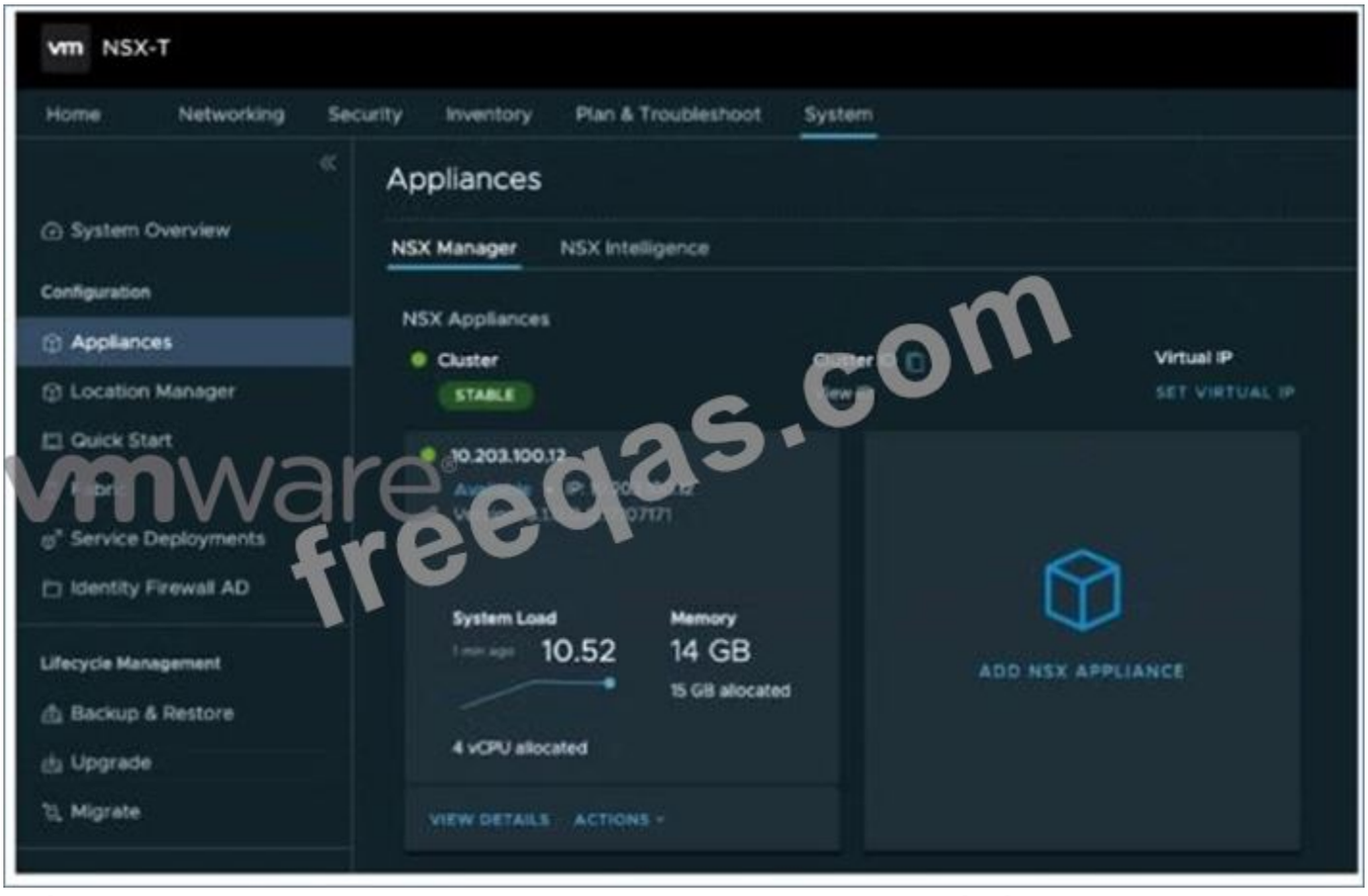
NEW QUESTION: 17
Which two Guest OS drivers are required for the Identity Firewall to operate? (Choose two.)
A. NSX Network Introspection
B. vmxnet3
C. NSX File Introspection
D. Guest Introspection
E. e1000e
Answer: (SHOW ANSWER)
The two Guest OS drivers that are required for the Identity Firewall to operate are NSX Network Introspection and Guest Introspection. NSX Network Introspection provides network-level visibility and control, while Guest Introspection provides kernel-level visibility and control. The other drivers listed, vmxnet3, NSX File Introspection, and e1000e, are not required for the Identity Firewall to operate.

NEW QUESTION: 18
Which is an insertion point for East-West service insertion?
A. tier-1 gateway
B. Partner SVM
C. Guest VM vNIC
D. transport node
Answer: C (LEAVE A REPLY)

East-West service insertion refers to the ability to insert security services, such as firewall and intrusion detection and prevention, between virtual machines (VMs) that are communicating within the same logical network.
One of the insertion points for East-West service insertion is the virtual network interface card (vNIC) of the guest VM. The vNIC is the virtual representation of a physical NIC on a VM, and it connects the VM to the virtual network. By inserting security services at the vNIC level, traffic between VMs can be inspected and secured before it reaches the virtual switch.
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html VMware NSX-T Data Center Security documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.security.doc/GUID-8F7C8B70-F1A6-4F31-8D6C-A0A9B9C9A9D3.html

NEW QUESTION: 19
Where is a partner security virtual machine (Partner SVM) deployed to process the redirected North-South traffic in an efficient manner?
A. Deployed close to the Partner Manager.
B. Deployed close to the NSX Edge nodes.
C. Deployed close to the VMware vCenter Server.
D. Deployed close to the compute nodes.
Answer: B (LEAVE A REPLY)
Reference:
This allows for the Partner SVM to be close to the compute nodes, allowing for faster processing of the traffic and improved security. Additionally, the Partner SVM is also deployed close to the Partner Manager for added security and ease of management.

NEW QUESTION: 20
Refer to the exhibit.



Referencing the exhibit, what is the VMware recommended number of NSX Manager Nodes to additionally deploy to form an NSX-T Manager Cluster?

A. 2

B. 5

C. 4

D. 3

Answer: D (LEAVE A REPLY)

NEW QUESTION: 21

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: D,E (LEAVE A REPLY)

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. Reference: [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

NEW QUESTION: 22
A security administrator has configured NSX Intelligence for discovery. They would like to get recommendations based on the changes in the scope of the input entities every hour.
What needs to be configured to achieve the requirement?
A. Start a new recommendation.
B. Publish the recommendations.
C. Toggle the monitoring option on.
D. Adjust the time range to 1 hour.
Answer: D (LEAVE A REPLY)
NSX Intelligence uses machine learning algorithms to analyze network traffic and provide recommendations for security and compliance. The administrator can configure the time range of the input entities to be analyzed, so that the recommendations are based on changes in the scope of the input entities over that period of time.
To achieve the requirement of getting recommendations based on the changes in the scope of the input entities every hour, the administrator needs to adjust the time range to 1 hour. This will ensure that the analysis and recommendations are based on the most recent hour of network traffic.
Reference:
VMware NSX Intelligence documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.intelligence.doc/GUID-F2F1D7E8-F6B2-4870-9E38-7C8D3D3F9B1E.html VMware NSX Intelligence Configuration documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.intelligence.config.doc/GUID-7F44F3D3-3A3C-4EBE-A5D5-F1E3E3F59A8B.html

NEW QUESTION: 23
A Security Administrator needs to update their NSX Distributed IDS/IPS policy to detect new attacks with critical CVSS scoring that leads to credential theft from targeted systems.
Which actions should you take?
A. * Update Distributed IDS/IPS signature database
* Edit your profile from Security > Distributed IDS > Profiles
* Select Critical severity, filter on attack type and select Successful Credential Theft Detected
* Check the profile is applied in Distributed IDS rules
B. * Edit your Distributed IDS rule from Security > Distributed IDS/IPS > Rules
* Filter on attack type and select Successful Credential Theft Detected

* Update Mode to detect and prevent
* Click on gear icon and change direction to OUT

C. * Create a new profile from Security > Distributed IDS > Profiles
* Select Critical severity, filter on attack type and select Successful Credential Theft Detected
* Check the profile is applied In Distributed IDS rules
* Monitor Distributed IDS alerts to validate changes are applied

D. * Edit your Distributed IDS rule from Security > Distributed IDS/IPS > Rules
* Filter on attack type and select Successful Credential Theft Detected
* Update Mode to detect and prevent
* Click on gear icon and change direction to IN-OUT

Answer: A (LEAVE A REPLY)

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_ids_ips/GUID-B2D6A7F6-

NEW QUESTION: 24

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: (SHOW ANSWER)

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

NEW QUESTION: 25

When using URL Analysis In NSX-T, which two services must be set in the URL rule to capture traffic over TCP and UDP? (Choose two.)
A. DNS-TSIG
B. DNS
C. DHCPv6
D. DNS-UDP
E. DHCP
Answer: (SHOW ANSWER)

NEW QUESTION: 26
An NSX administrator has turned on logging for the distributed firewall rule. On an ESXi host, where will the logs be stored?
A. /var/log/esxupdate.log
B. /var/log/dfwpktlogs.log
C. /var/log/hostd.log
D. /var/log/vmkerntl.log
Answer: B (LEAVE A REPLY)
The NSX administrator has enabled logging for the distributed firewall rule, and the logs are stored in the /var/log/dfwpktlogs.log file on the ESXi host. This log file stores the packet logs for the distributed firewall rules, and the logs can be used for auditing and troubleshooting the distributed firewall.

NEW QUESTION: 27
What is one of the main use-cases of NSX-T Endpoint Protection?
A. Use Network Security Services of a third party vendor
B. Agentless Antivirus
C. East-West Firewalling
D. North-South Firewalling
Answer: B (LEAVE A REPLY)
NSX-T Endpoint Protection provides agentless antivirus protection for virtual machines running on VMware ESXi hosts. It uses the VMware vShield Endpoint API to scan the virtual machines without requiring the installation of antivirus agents. The service is integrated with third-party antivirus solutions, such as McAfee and Symantec, to provide real-time protection against malware and other threats.
For more information on NSX-T Endpoint Protection, 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-endpoint-protection/GUID-25C22F02-4B30-47D4-8F0C-3BC9F9C3AFD3.html

NEW QUESTION: 28
What must an administrator deploy to provide Linux based VMs with antivirus protection?
A. Antivirus Agent in NSX

B. Antivirus Agent in vCenter
C. Guest Introspection Thin Agent
D. Guest Customization Agent
Answer: C (LEAVE A REPLY)
NSX provides a feature called Guest Introspection that allows administrators to provide security services to virtual machines, including antivirus protection. One of the components of Guest Introspection is the Guest Introspection Thin Agent, which must be deployed to provide Linux-based VMs with antivirus protection. The Thin Agent is a lightweight agent that runs inside the guest operating system of virtual machines and communicates with the NSX Manager to provide security services.
Once the Guest Introspection Thin Agent is deployed, the administrator can configure the antivirus service to scan virtual machines for malware and take action on any threats that are detected.
Reference:
VMware NSX Guest Introspection documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.guest_introspection.doc/GUID-A86FBAF1-A8D9-4E12-8F3D-04B3D89B8F7E.html VMware NSX Guest Introspection Thin Agent documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.guest_introspection.doc/GUID-A86FBAF1-A8D9-4E12-8F3D-04B3D89B8F7E.html

NEW QUESTION: 29
Which of the following are the local user accounts used to administer NSX-T Data Center?
A. operator, admin, audit
B. admin, super, read-only
C. operator, admin, root
D. admin, audit, root
Answer: A (LEAVE A REPLY)
For further reading, see the VMware NSX-T Data Center Administration Guide (https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.admin.doc/GUID-4A4E9FBE-50B3-4F8F-B6C4-8527E7A08A67.html) for more information on user accounts and permissions in NSX-T Data Center.

NEW QUESTION: 30
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 (LEAVE A REPLY)

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.
Reference:
In the IDS/IPS events tab of NSX-T Data Center, different colors of dots are used to indicate the severity of an attack.
A solid red dot indicates a critical attack, which is the highest severity level.
A solid orange dot indicates a medium attack, which is a moderate severity level.
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.
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html 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

NEW QUESTION: 31
Which are the four use cases for NSX Tags?
A. Accountability, Third-party sharing/context sharing. Security, and Logging
B. Manageability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability)
C. Accountability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability)
D. Manageability, Third-party sharing/context sharing. Security, and Logging
Answer: (SHOW ANSWER)
The four use cases for NSX Tags are Manageability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability). NSX Tags provide an easy way to organize, document, and manage virtual networks and can be used to track changes and enforce security policies. They can also be used to share context between third-party providers, such as cloud service providers, to ensure that security policies are adhered to. Additionally, NSX Tags can be used for logging and troubleshooting by providing traceability and making it easier to debug network issues.
Reference: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-2F3E7A3F-3C85-48E1-8F7E-2A2F7C2F8FCC.html [2] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-data-center-for-vsphere-tag-based-security-guide.pdf

NEW QUESTION: 32
A company's CTO has requested that all logging should be enabled for all NSX-T Data Center Distributed Firewall rules. What should be considered prior to executing this request?
A. Once logging is enabled for all rules it cannot be disabled afterwards.
B. Logging can only be enabled for sections and not for single rules.
C. Large amounts of log information can fill up the vSphere Server database.
D. Large amounts of log information will likely affect performance.
Answer: C (LEAVE A REPLY)