VMware.Premium.5V0-41.21.30q - DEMO

Number: 5V0-41.21
Passing Score: 800
Time Limit: 120 min

Exam Code: 5V0-41.21
Exam Name: VMware NSX-T Data Center 3.1 Security
Website: https://VCEup.com/
Team-Support: Support@VCEup.com

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.
Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.5/nsxt_25_admin_guide/GUID-E0CC7D8A-F9E6-4A6F-A6F8-6A3D7B3DC3EF.html#GUIDE0CC7D8A- F9E6-4A6F-A6F8-6A3D7B3DC3EF

QUESTION 2
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 3
Which is an insertion point for East-West service insertion?

A. tier-1 gateway
B. Partner SVM
C. Guest VM vNIC
D. transport node

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-TData-Center/3.1/com.vmware.nsxt.security.doc/GUID-8F7C8B70-F1A6-4F31-8D6CA0A9B9C9A9D3.html

QUESTION 4
An NSX administrator has been tasked with configuring a remote logging server (192.168.110.60) to send FW connections and packets logs to a remote logging server. The administrator is using this command syntax found in the NSX-T 3.1 documentation:

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level
[clientca <filename>] [certificate <filename>] [key <filename>] [struct
```

Which of the following commands does the administrator use to complete the configuration task?

A. set logging-server 192.168.110.60 proto udp level info facility syslog message Id FIREWALLCONNECTION
B. set logging-server 192.168.110.60 proto udp level info facility syslog message!- monitor. Firewall
C. set logging-server 192.168.110.60 proto udp level info facility syslog message Id FIREWALLPKTLOG
D. set logging-server 192.168.110.60 proto udp level info facility syslog message Id system, fabric

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The administrator is using the command syntax found in the NSX-T 3.1 documentation to configure a remote logging server to send firewall connections and packets logs. In order to complete the configuration task, the administrator needs to use the correct options for the command.
The options used in the command are: logging-server: This option specifies the IP address or hostname of the remote logging server. In this case, the IP address of the remote logging server is 192.168.110.60. proto: This option specifies the protocol to be used to send the logs to the remote server. In this case, the protocol used is UDP. level: This option specifies the level of logging to be sent to the remote server. In this case, the level of logging is "info" facility: This option specifies the facility to be used for syslog messages. In this case, the facility used is "syslog" message Id: This option specifies the message Id that will be used for the logs. In this case, the message Id used is "FIREWALL-PKTLOG"
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Logging documentation
https://docs.vmware.com/en/VMware-NSX-TData-Center/3.1/com.vmware.nsxt.logging.doc/GUID-2B9E9F8D-6CA9-4A1E-B7B1-8B8C7F0C2B2E.html

QUESTION 5
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin_guide/GUID-A8FAC8A1-F9F9-43EC-A822-F2F2CB5C5E5A.html#GUIDA8FAC8A1- 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.
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.

Reference:
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/GUIDC4ED1F4D-4E4B-4A9C-9F5C-7AC081A5C5D5.html

QUESTION 6
An administrator needs to send FW connections logs to a remote server.
Which sequence of commands does the administrator need to apply on their ESXi Host?

A.
```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

B.
```
esxcli network firewall ruleset set -r syslog -e true
esxcli network syslog config set --loghost=udp://<log server IP>:<port>
esxcli network syslog reload
```

C.
```
esxcli security firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

D.
```
esxcli system firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.
Reference: https://docs.vmware.com/en/VMwarevSphere/7.0/com.vmware.vsphere.security.doc/GUID-2AAB1D7A-E6A6-47F7-9B28-F9C9DED1C6B7.html

QUESTION 8
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-NSXT-Data-Center/3.1/com.vmware.nsxt.intelligence.config.doc/GUID-7F44F3D3-3A3C-4EBE-A5D5-F1E3E3F59A8B.html

QUESTION 9
Which of the following describes the main concept of Zero-Trust Networks for network connected devices?

A. Network connected devices should only be trusted if they are issued by the organization.
B. Network connected devices should only be trusted if the user can be successfully authenticated.
C. Network connected devices should only be trusted if their identity and integrity can be verified continually.
D. Network connected devices should only be trusted if they are within the organizational boundary.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Zero-Trust Networks is a security concept that assumes that all devices, users, and networks are untrusted until they can be verified. This means that all network-connected devices must be verified for their identity and integrity before they are granted access to resources. This is done continually, meaning that devices are verified every time they try to access a resource, rather than being trusted permanently.
1. Network connected devices should only be trusted if their identity and integrity can be verified continually. This is the main concept of Zero-Trust Networks, every device that wants to access the network should be authenticated and verified its identity and integrity.
Reference:
Zero Trust Networks, Forrester Research https://www.forrester.com/report/Zero+Trust+Networks/-/E-RES146810
Zero Trust Security: From Theory to Practice, NIST
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800

QUESTION 10
Which three security objects are provided as an output in a recommendation session in NSX Intelligence? (Choose three.)

A. context profiles
B. distributed firewall rules
C. security service
D. gateway firewall rules
E. security groups

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NSX Intelligence uses machine learning algorithms to analyze network traffic and provide recommendations for security and compliance. These recommendations include the following security objects:
Distributed Firewall Rules: Distributed firewall rules are used to control traffic between virtual machines within a logical network. NSX Intelligence can recommend new distributed firewall rules based on traffic patterns it observes in the network.
Security Service: Security services are used to protect virtual machines and networks from threats.
NSX Intelligence can recommend new security services to be deployed based on traffic patterns it observes in the network.
Security Groups: Security groups are used to group virtual machines and networks together for security and management purposes. NSX Intelligence can recommend new security groups to be created based on traffic patterns it observes in the network.
A. context profiles are not an output from a recommendation session in NSX Intelligence. It is used to define the context of the network traffic that is being analyzed, such as the type of device, the network location, or the user.
D. gateway firewall rules are not an output from a recommendation session in NSX Intelligence.
Gateway firewall rules are used to control traffic between logical networks, such as between a VLAN and a VXLAN, or between a logical network and the physical network.
Reference:

VMware NSX Intelligence documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.intelligence.doc/GUID-F2F1D7E8-F6B2-4870-9E
Top of Form
Bottom of Form

QUESTION 11
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-TData-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

QUESTION 12
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. Large amounts of log information can fill up the vSphere Server database.
B. Logging can only be enabled for sections and not for single rules.
C. Once logging is enabled for all rules it cannot be disabled afterwards.
D. Large amounts of log information will likely affect performance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
An administrator has configured a new firewall rule but needs to change the Applied-To parameter.
Which two are valid options that the administrator can configure? (Choose two.)

A. DFW
B. rule
C. services
D. profiles
E. groups

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-704E1B2F-1E43-4E7F-97F2-59BBF8F6C9F6.html) for more information on configuring firewall rules.

QUESTION 14
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 andpermissions in NSX-T Data Center.

QUESTION 15
As part of an audit, an administrator is required to demonstrate that measures have been taken to prevent critical vulnerabilities from being exploited. Which Distributed IDS/IPS event filter can the administrator show as proof?

A. Attack Type
B. CVSS
C. CVE
D. Signature ID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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/GUIDA1A7F233-5F9F-4B2E-B3D3-0F8B593032F6.html) for more information on configuring theas the CVE filter can be used to filter out any events which are related to a specific vulnerability

QUESTION 16
Which two are used to define dynamic groups for an NSX Distributed Firewall? (Choose two.)

A. segment
B. physical servers
C. machine name
D. tags
E. segment's port

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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/GUIDBEDA8D9F-ACBC-42B1-B7F5-FEEF0E0D899C.html) for more information on configuring dynamicgroups.

QUESTION 17
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: 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/GUIDQuestionsand Answers PDF 16/38D9A6B1E7-FFCD-47A7-8E0C-FDD3DE6AC2B6.html) for more information on configuring an IDS/IPS system.

QUESTION 18
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.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
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 19
Which vCenter component is used by the NSX Manager to deploy the Partner Service VM on every host of a cluster configured for guest introspection?

A. ESXi Agent Manager (EAM)
B. Auto Deploy
C. Update Manager (VUM)
D. Component Manager

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Component Manager is used to deploy the Partner Service VM on every host of a cluster configured for guest introspection.
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/GUIDACB4CE1E-4F6E-4B4F-96BF-9FA9DFFF9229.html) for more information on configuring guestintrospection.

QUESTION 20
To which object can time based rules be applied?

A. Gateway Firewall only
B. DFW and Gateway Firewall both
C. DFW only
D. DFW or Gateway Firewall, but not both at the same time

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-8F9C6E9E-9C83-4CAD-BB3A-F4E4A25C6FE7.html) for more information on configuring time basedrules.

QUESTION 21
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 22
Refer to the exhibit.

An administrator needs to configure a security policy with a firewall rule allowing a group of applications to retrieve the correct time from an NTP server. Which is the category to configure thissecurity policy and firewall rule?

A. Emergency
B. Application
C. Infrastructure
D. Environment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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/GUIDD12A8AE7-B9E9-4C79-8FE4-7F4BECD4F71B.html) for more information on configuring firewall rules.

QUESTION 23
Which two statements are true about IDS/IPS signatures? (Choose two.)

A. Users can upload their own IDS signature definitions from the NSX UI.
B. IDS Signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
C. Users can create their own IDS signature definitions from the NSX UI.
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.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUIDAFAF58DB-E661-4A7D-A8C9-70A3F3A3A3D3.html)

QUESTION 24
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 25
Which three criteria help to determine the severity for a Distributed IDS/IPS? (Choose three.)

A. The type-rating associated with the classification type.
B. The Common Vulnerability Scoring System score specified in the signature.
C. The load balancer deployment type.
D. The Distributed Intrusion Detection and Intrusion Prevention rules.
E. The severity specified in the signature itself

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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/GUIDE6B25C6F-1F25-4B0F-B8AF-6B8C00F9C3A3.html) for more information on configuring the Distributed IDS/IPS.

QUESTION 26
Which is the port number used by transport nodes to export firewall statistics to NSX Manager?

A. 1235
B. 4789
C. 6081
D. 1234

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The port number used by transport nodes to export firewall statistics to NSX Manager is 4789.
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-15A2EBC2-C39D-45F3-B847-DC18F7B1E9B9.html) for more information on transport nodes and firewall statistics.

QUESTION 27
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
[1] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmwarensx-data-center-for-vsphere-partner-svm-security-deploymentguide.pdf [2] https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-A2A6B7F6-9020-4D4F-AFC6-7E6D2E6194DF.html
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.

QUESTION 28
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

QUESTION 29
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

Correct Answer: AD
Section: (none)

Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 30
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: