Free Questions for 5V0-41.21 by braindumpscollection

Shared by Mayo on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.)

Options:

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

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. 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

Question 2

Question Type: MultipleChoice

An administrator is creating the first distributed firewall rules for a company's salts department. What is the first object that must be created in the distributed firewall'

Options:

A- firewall policy

B- firewall file

C- firewall folder

D- firewall service

Answer:

A

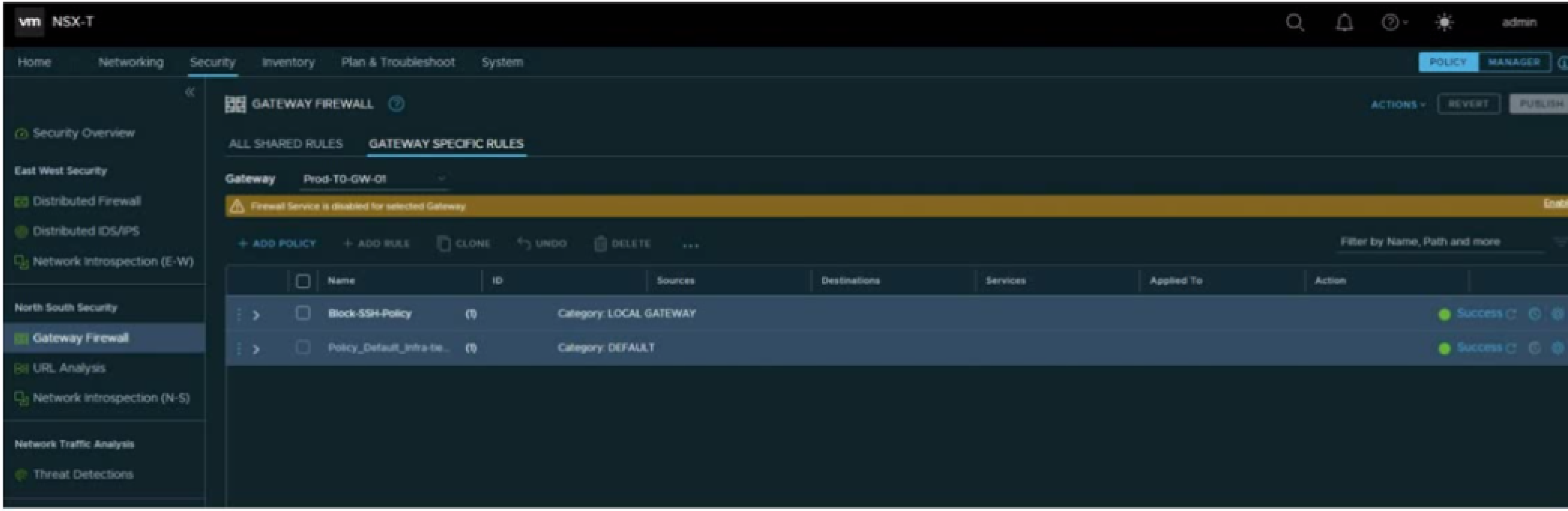
Explanation:

The first object that must be created in the distributed firewall is a firewall policy. A firewall policy is a set of rules that define what traffic is allowed or blocked on a given network. When creating a policy, the administrator must specify the source and destination address and port, as well as the type of traffic that is allowed or blocked. The policy will then be applied to the distributed firewall, allowing it to enforce the rules specified in the policy. Reference: [1]https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-4CAF59C8-13F3-4F3E-B53E-D8F1E03FBE7B.html[2]https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-nsx-data-center-for-vsphere-distributed-firewall-deployment-guide.pdf

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



Gateway Prod-T0-GW-01

⚠ Firewall Service is disabled for selected Gateway

□ Name	ID	Sources	Destinations	Services	Applied To	Action
□ Block-SSH-Policy (1)	Category: LOCAL GATEWAY					● Success
□ Policy_Default_Infra-tie... (1)	Category: DEFAULT					● Success

An administrator configured a firewall rule on their Edge Gateway to allow access to web servers.

What is missing in the Gateway Firewall policy to have the firewall rule applied?

Options:

A- Firewall service needs to be enabled on gateway.

B- Firewall rule needs to be moved to Default category.

C- Firewall rule needs to be enabled.

D- Firewall rule needs to be published

Answer:

B

Question 4

Question Type: MultipleChoice

Which are the four use cases for NSX Tags?

Options:

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:

C

Explanation:

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

Question 5

Question Type: MultipleChoice

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

Options:

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. Reference: [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 6

Question Type: MultipleChoice

What component in a transport node receives the firewall configuration from the central control plane?

Options:

A- nsx-ccp

B- nsx-appl-proxy

C- nsx-mpa

D- nsx-proxy

Answer:

C

Explanation:

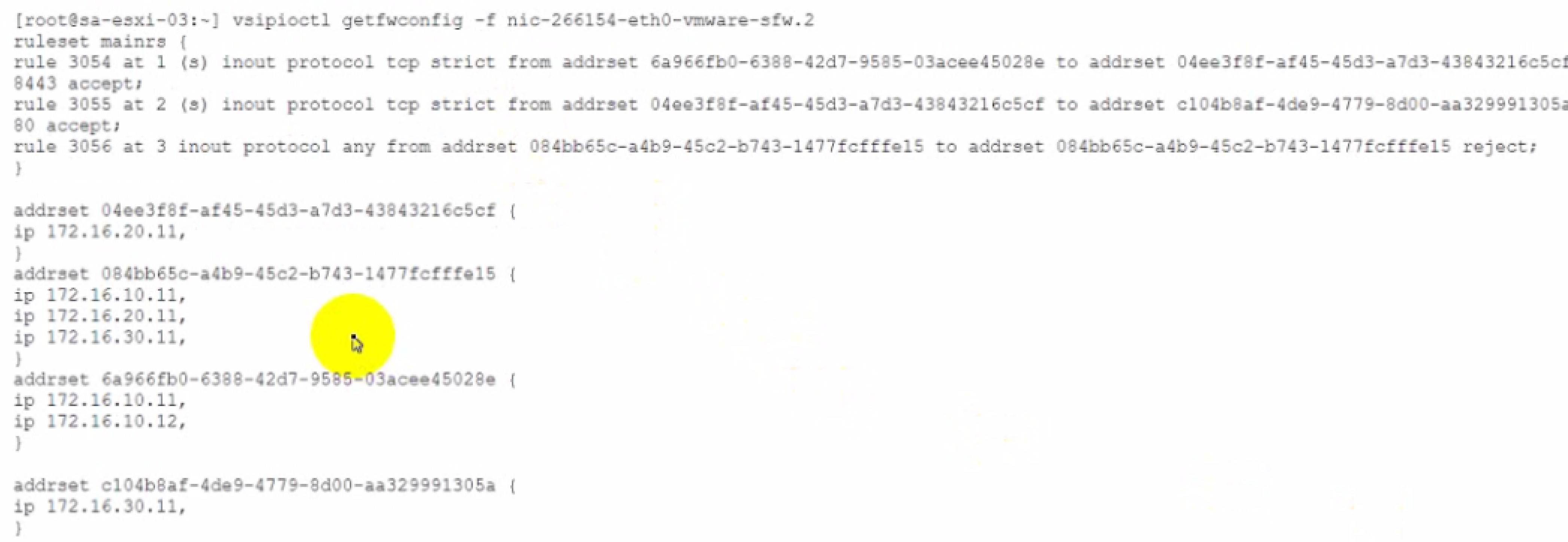
The component in a transport node that receives the firewall configuration from the central control plane is the NSX-MPA (Management Plane Agent). The NSX-MPA runs on each transport node and is responsible for connecting to the NSX-T central control plane and receiving the configuration for the transport 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.

Question 7

Question Type: MultipleChoice

Reference the CLI output.



```
[root@sa-esxi-03:~] vsipioctl getfwconfig -f nic-266154-eth0-vmware-sfw.2
ruleset mainrs {
rule 3054 at 1 (s) inout protocol tcp strict from addrset 6a966fb0-6388-42d7-9585-03acee45028e to addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf
8443 accept;
rule 3055 at 2 (s) inout protocol tcp strict from addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf to addrset c104b8af-4de9-4779-8d00-aa329991305a
80 accept;
rule 3056 at 3 inout protocol any from addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 to addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 reject;
}

addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf {
ip 172.16.20.11,
}
addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 {
ip 172.16.10.11,
ip 172.16.20.11,
ip 172.16.30.11,
}
addrset 6a966fb0-6388-42d7-9585-03acee45028e {
ip 172.16.10.11,
ip 172.16.10.12,
}

addrset c104b8af-4de9-4779-8d00-aa329991305a {
ip 172.16.30.11,
}
```

What is the source IP address in the distributed firewall rule to accept HTTP traffic?

Options:

A- 172.16.30.11

B- 172.16.10.12

C- 172.16.10.11

D- 172.16.20.11

Answer:

C

Question 8

Question Type: **MultipleChoice**

An administrator wants to use Distributed Intrusion Detection. How is this implemented in an NSX-T Data Center?

Options:

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

Explanation:

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

Question 9

Question Type: MultipleChoice

Which two statements are true about NSX Intelligence? (Choose two.)

Options:

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:

A, E

Explanation:

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.

Question 10

Question Type: MultipleChoice

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

Options:

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:

D

Question 11

Question Type: MultipleChoice

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?

Options:

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:

A

Question 12

Question Type: **MultipleChoice**

Which two Guest OS drivers are required for the Identity Firewall to operate? (Choose two.)

Options:

A- NSX Network Introspection

B- vmxnet3

C- NSX File Introspection

D- Guest Introspection

E- e1000e

Answer:

A, D

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.

To Get Premium Files for 5V0-41.21 Visit

https://www.p2pexams.com/products/5v0-41.21

For More Free Questions Visit

https://www.p2pexams.com/vmware/pdf/5v0-41.21

20%
DISCOUNT