KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **FCSS_EFW_AD-7.6**

Title : Fortinet NSE 7 - Enterprise Firewall 7.6 Administrator

Version : DEMO

1.A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)
A. Use metadata variables to dynamically assign values according to each FortiGate device.
B. Use provisioning templates and install configuration settings at the device layer.
C. Use the Global ADOM to deploy global object configurations to each FortiGate device.
D. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.
E. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.
Answer: A,B,E
Explanation:
Use metadata variables to dynamically assign values according to each FortiGate device:
Metadata variables in FortiManager allow device-specific configurations to be dynamically assigned without manually configuring each FortiGate. This is especially useful when deploying multiple devices with similar base configurations.
Use provisioning templates and install configuration settings at the device layer:
Provisioning templates in FortiManager provide a structured way to configure FortiGate devices. These templates can define interfaces, policies, and settings, ensuring that each device is correctly configured upon deployment.
Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices:
Zero-Touch Provisioning (ZTP) and Local Touch Provisioning (LTP) help automate the deployment of FortiGate devices. By adding devices as model devices in FortiManager, configurations can be pushed automatically when devices connect for the first time, reducing manual effort.

2.An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.
What two conclusions can the administrator draw? (Choose two.)
A. The suspicious packet is related to a cluster that has VDOMs enabled.
B. The network includes FortiGate devices configured with the FGSP protocol.
C. The suspicious packet is related to a cluster with a group-id value lower than 255.
D. The suspicious packet corresponds to port 7 on a FortiGate device.
Answer: A,D
Explanation:
According to the FortiOS 7.6 Infrastructure study guide and High Availability (HA) documentation, FortiGate units in an HA cluster use a virtual MAC address to ensure seamless failover. The structure of this virtual MAC address is strictly defined by the Fortinet HA protocol.
For a standard HA cluster, the virtual MAC address format is 00:09:0f:09:<group-id_hex>:<vcluster_port_hex>. However, when VDOMs are enabled, the virtual MAC address prefix changes to e0:23:ff to accommodate the additional complexity of multiple virtual domains. Therefore, the prefix e0:23:ff in the suspicious MAC address e0:23:ff:fc:00:86 confirms that the packet originated from a cluster with VDOMs enabled (Option A).

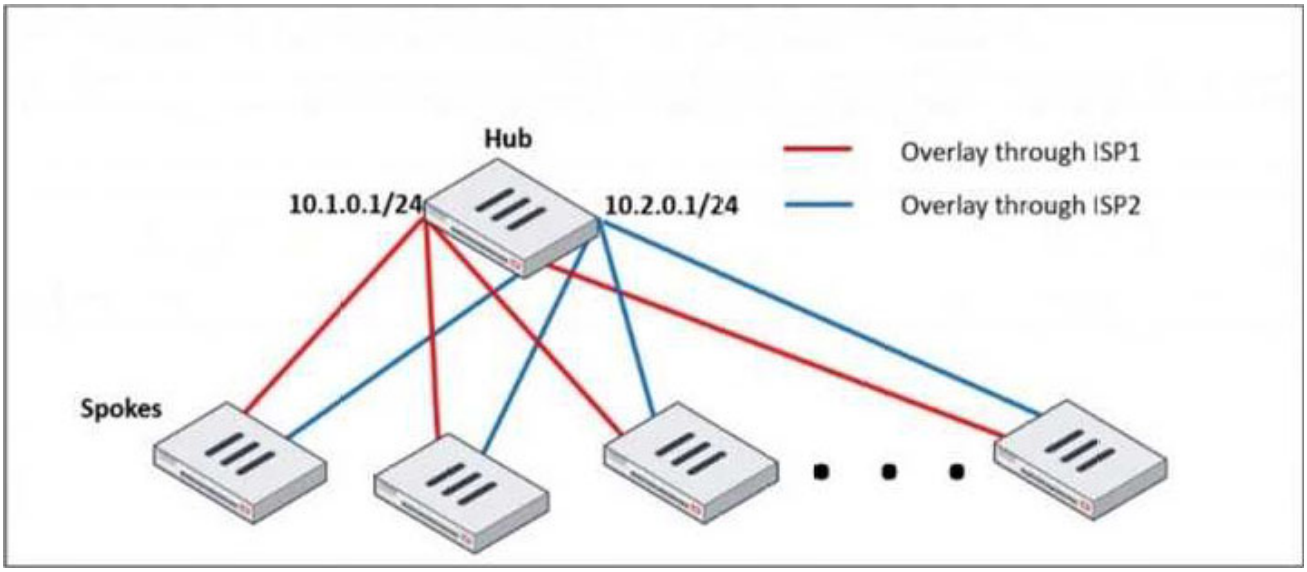
Regarding the interface identification, the last byte (86) is calculated as follows:
The 0x80 bit indicates virtual-cluster 2 (vcluster 2). Since $0x86 = 0x80 + 0x06$, we know the packet is from vcluster 2.
The remaining value 0x06 represents the interface index. In FortiOS, the index starts at 0 (port1 = 0, port2 = 1, port3 = 2, port4 = 3, port5 = 4, port6 = 5, port7 = 6). Therefore, the index 6 corresponds exactly to port 7 (Option D).
The fourth byte (fc) represents the HA Group ID (252 in decimal). While this is indeed lower than 255, the specific logic of the virtual MAC composition in a VDOM-enabled environment points specifically to the port identification and vcluster status as the primary diagnostic conclusions.

3.A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.
Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?
A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.
Answer: B
Explanation:
When FortiGate is operating in proxy mode with full SSL inspection enabled, it inspects encrypted HTTPS traffic by default on port 443. However, some websites may use non-standard HTTPS ports (such as 8443), which FortiGate does not inspect unless explicitly configured.
To ensure that FortiGate inspects HTTPS traffic on port 8443, administrators must manually add port 8443 in the Protocol Port Mapping section of the SSL/SSH Inspection Profile. This allows FortiGate to treat HTTPS traffic on port 8443 the same as traffic on port 443, enabling proper inspection and enforcement of FortiGuard category-based web filtering.

4.An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow.
Which action can the administrator take to prevent false positives on IPS analysis?
A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.
B. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.
C. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.
D. Install missing or expired SSUTLS certificates on the client PC to prevent expected false positives.
Answer: A
Explanation:
False positives in Intrusion Prevention System (IPS) analysis can disrupt legitimate traffic and negatively

impact user experience.
To reduce false positives while maintaining security, administrators can:
● Use IPS profile extensions to fine-tune the settings based on the organization's environment.
● Select the correct operating system, protocol, and application types to ensure that IPS signatures match the network's actual traffic patterns, reducing false positives.
● Customize signature selection based on the network's specific services, filtering out unnecessary or irrelevant signatures.

5.Refer to the exhibit, which shows a hub and spokes deployment.



An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.
Which two commands allow the administrator to minimize the configuration? (Choose two.)
A. neighbor-group
B. route-reflector-client
C. neighbor-range
D. ibgp-enforce-multihop
Answer: A,C
Explanation:
neighbor-group:
● This command is used to group multiple BGP neighbors with the same configuration, reducing redundant configuration.
● Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-group and apply the same policies, reducing manual work.
neighbor-range:
● This command allows the configuration of a range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.
● It automatically adds BGP neighbors that match a given prefix, simplifying deployment.