We offer free update service for one year!
https://www.certqueen.com

Exam : **250-583**

Title : Symantec ZTNA Complete R1 Technical Specialist

Version : DEMO

1.A Security Solutions Architect is presenting the scaling strategy for an enterprise anticipating a 300% increase in ZTNA traffic over the next fiscal quarter due to a corporate merger. The organization relies entirely on virtual VMware OVA Site Connectors.
Which THREE statements represent the architectural best practices and inherent realities of horizontally scaling Site Connector capacity within the Symantec ZTNA framework? (Select all that apply.)
A. Because the Site Connectors operate strictly outbound, adding ten new nodes to a single datacenter Site does not consume any additional public inbound IP addresses or require external firewall NAT rule modifications.
B. The architecture scales horizontally; the architect easily accommodates the growth by deploying additional virtual Site Connectors and simply registering them to the existing logical Sites.
C. The Symantec cloud edge handles the complex algorithmic load balancing across the clustered connectors natively, completely eliminating the need for the customer to purchase and deploy expensive internal hardware load balancers.
D. Scaling up individual connector VM resources (e.g., from 2 vCPUs to 16 vCPUs) is the only supported scaling methodology; horizontal clustering is strictly limited to two nodes per Site.
E. Adding new connectors to an active Site requires a mandatory, scheduled 15-minute maintenance window where the entire logical Site must be taken offline to allow the cloud routing tables to recalculate.
Answer: A, B, C

2.A Network Security Analyst is granted Read-Only access to the Symantec ZTNA Admin Portal to review the organization's infrastructure layout. The analyst needs to view the geographic locations where connectors are deployed.
Which primary navigation section within the console architecture must the analyst access to find this specific infrastructure grouping?
A. It is located in the Reports section, which provides live maps of active user connections.
B. It is located in the Identity section, which manages both user locations and authentication.
C. It is located in the Sites section, which centralizes the logical deployment of connectors.
D. It is located in the Policies section, which groups network locations alongside access rules.
Answer: C

3.A ZTNA Administrator is tasked with restricting access to the 'Prod_DB' application. The offshore development team ('Offshore_Devs' group) must only access the database using corporate-issued, compliant devices during their authorized shift (08:00 to 17:00 UTC).
Requested Constraints:
Target: Prod_DB
Target Group: Offshore_Devs
Device Requirement: Corporate_Compliant_Profile
Time Window: 08:00 - 17:00 UTC
Which Access Policy configuration accurately enforces these exact constraints without inadvertently granting broader access?
A. Action: Allow | Group: Any_User | Posture: Corporate_Compliant_Profile | Time: 08:00-17:00 UTC
B. Action: Block Rule | Group: Offshore_Devs | Posture: Any_Profile | Time: 17:01-07:59 UTC
C. Action: Bypass | Group: Offshore_Devs | Posture: Corporate_Compliant_Profile | Time: Always_Active
D. Allow | Group: Offshore_Devs | Posture: Corporate_Compliant_Profile | Time: 08:00-17:00 UTC

Answer: D

4.A Network Security Analyst is troubleshooting an integration failure between Symantec ZTNA and a custom SAML Identity Provider. Users are successfully redirected to the IdP, authenticate successfully, but receive an error when their browser returns to the ZTNA platform. (Choose 2.)
SAML Configuration Snippet (IdP Side):
Entity ID (Audience URI): https://saml.ztna.symantec.com
Single Sign-On URL: https://idp.custom.local/sso/saml
Assertion Consumer Service (ACS) URL: https://portal.ztna.symantec.com/consume
NameID Format: Unspecified
Which TWO configuration mismatches or errors in the provided snippet are likely causing the authentication flow to fail upon returning to the ZTNA platform?
A. The NameID Format is set to Unspecified, which explicitly prevents the ZTNA platform from reading the user's email address.
B. The Single Sign-On URL points to an internal .local domain, which the Symantec cloud edge cannot resolve or route to.
C. The Entity ID (Audience URI) configured on the IdP does not match the exact ZTNA Tenant Entity ID provided in the ZTNA Admin Portal.
D. The Assertion Consumer Service (ACS) URL configured on the IdP does not match the specific tenant ACS URL generated by Symantec ZTNA.
Answer: C, D

5.A Network Security Analyst is investigating a performance issue. An internal application is mapped to the "HQ_Datacenter" Site. The Site is configured as an HA cluster containing two Site Connectors (Connector-A and Connector-B). The analyst notices a severe load imbalance. (Choose 2.)
Health Status Report Snippet:
Connector-A: Online | Active Connections: 4,500 | CPU: 80%
Connector-B: Degraded | Active Connections: 15 | CPU: 95%
What are TWO potential architectural reasons for this severe load imbalance within the ZTNA HA cluster?
A. Connector-B is experiencing significant internal packet loss on the corporate network, causing its outbound health telemetry to report poor performance to the load balancer.
B. The ZTNA Access Policy governing the application was manually configured to bind the "Finance_Users" group explicitly to the hardware MAC address of Connector-A.
C. The ZTNA cloud edge strictly utilizes an active/passive failover algorithm by default, explicitly keeping Connector-B idle until Connector-A suffers a total heartbeat loss.
D. The local hypervisor hosting Connector-B is severely under-provisioned (lacking adequate vCPU or RAM), resulting in a "Degraded" health status that forces the cloud edge to actively steer new traffic away from it.
Answer: A, D