Zscaler for Users – Essentials (EDU-200) for ZDTA Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What two probe types are configured when setting up an application in the ZDX Administrator portal?

A. HTML and Network Probes.

B. Web Probe and Cloudpath Probes.

C. MTR and HTTP POST Probes.

D. Traceroute Probe and Network Auth Probes.

2. Which method is better suited for controlling access to specific web applications?

A. URL Filtering

B. VPN Access

C. Firewalls

D. Cloud App Control

3. What functionality does the Access Control Services Suite offer?

A. Network Monitoring

B. DNS

C. Cloud Based Firewall

D. Application Monitoring

4. What is an Application Segment?

A. A mechanism to append DNS Suffixes to short names

B. A list of FQDNs or IP Addresses

C. A list of TCP or UDP Ports

D. Segments define the network subnets applications exist on

5. In Zero Trust architecture, what is emphasized regarding user access?

A. Access based solely on user credentials

B. Access based on location and time

C. Access based on user, device, and application context

D. Access based on random selection

6. What options for TLS Inspection Certificates are available? (Select 2)

- **A. Zscaler Root Certificate Authority**
- **B. Customer Root Certificate Authority**
- **C. Verisign Root CA**
- **D. Microsoft Azure Certificate Authority**

7. What unique features does Zscaler's mobile app offer?

- **A. Voice recognition and biometric authentication**
- **B. Secure access and simplified user experience**
- **C. Offline browsing capabilities and ad-blocking features**
- **D. Customizable themes and backgrounds**

8. What stage follows after the initial compromise in a typical cyber attack?

- **A. Data encryption**
- **B. Lateral movement**
- **C. Finding the attack surface**
- **D. Extortion attempts**

9. What role does Zscaler ThreatLabZ serve?

- **A. A team that monitors network traffic in real-time**
- **B. A research team that analyzes security trends and updates databases**
- **C. A group dedicated to public relations for Zscaler**
- **D. A team specializing in customer support**

10. Which address translation options are available in the Firewall policy? (Select 3)

- **A. Destination Port Translation**
- **B. Source IP Translation to static IP**
- **C. Destination IP Translation to static IP**
- **D. Source Port Translation**
- **E. Destination IP Translation to FQDN**

Answers

1. B
2. D
3. B
4. B
5. C
6. A
7. B
8. B
9. B
10. A

Explanations

1. What two probe types are configured when setting up an application in the ZDX Administrator portal?

A. HTML and Network Probes.

B. Web Probe and Cloudpath Probes.

C. MTR and HTTP POST Probes.

D. Traceroute Probe and Network Auth Probes.

When setting up an application in the ZDX Administrator portal, the Web Probe and Cloudpath Probes are essential for the application's performance monitoring. The Web Probe allows the monitoring of application performance and user experience by simulating user interactions through synthetic transactions. This type of probe captures data such as response time, availability, and other metrics critical for understanding how the application performs from various locations. Cloudpath Probes complement this by offering insights into connectivity and access performance through authentication processes, typically related to how end-users connect to the application in the cloud. These probes work together to give a comprehensive view of both the application's performance and the user experience, ensuring that any issues can be detected and addressed proactively. Understanding these probe types is important for effectively managing and optimizing application performance in the cloud, which is a key focus of Zscaler's ZDX platform.

2. Which method is better suited for controlling access to specific web applications?

A. URL Filtering

B. VPN Access

C. Firewalls

D. Cloud App Control

The most suitable method for controlling access to specific web applications is through Cloud App Control. This approach allows organizations to enforce policies specifically tailored to various cloud applications, providing granular control over who can access which applications and under what conditions. Cloud App Control allows administrators to monitor usage, set permissions, manage user access rights, and apply specific security measures such as data loss prevention (DLP) policies directly to the cloud applications being utilized. This targeted control ensures that only authorized users have access to sensitive applications, thus enhancing overall security. While URL Filtering, VPN Access, and Firewalls provide different levels of web access control and security, they do not offer the same level of specificity needed for individual web applications attributed to Cloud App Control. URL Filtering focuses on blocking or allowing access based on URLs, but does not offer in-depth management of specific applications. VPN Access provides a secure connection for users but does not inherently manage which applications can be accessed. Firewalls protect networks from unauthorized access but generally operate at a broader level than the application-specific controls provided by Cloud App Control. Therefore, for precise management of access to cloud applications, Cloud App Control stands out as the preferred method.

3. What functionality does the Access Control Services Suite offer?

A. Network Monitoring

B. DNS

C. Cloud Based Firewall

D. Application Monitoring

The correct answer highlights the role of DNS (Domain Name System) in the context of the Access Control Services Suite. DNS functionality is crucial for translating human-readable domain names into IP addresses that machines use to identify each other on the network. When it comes to security, DNS services can also include features such as DNS filtering, which helps in blocking access to malicious sites, enhancing overall network security. The Access Control Services Suite incorporates DNS capabilities as part of its broader functionality to ensure that users can efficiently access allowed applications while also protecting against threats. This integration streamlines access control and improves user experience by ensuring that requests are appropriately routed and filtered according to security policies. The other options, while potentially relevant in the context of a broader security strategy, do not specifically encapsulate the primary functionality offered by the Access Control Services Suite regarding direct user and application interaction through domain resolution and management. Network monitoring, cloud-based firewalls, and application monitoring may be components of a comprehensive security posture but do not represent the core features associated explicitly with the DNS functionality in this suite.

4. What is an Application Segment?

A. A mechanism to append DNS Suffixes to short names

B. A list of FQDNs or IP Addresses

C. A list of TCP or UDP Ports

D. Segments define the network subnets applications exist on

An Application Segment refers specifically to a list of Fully Qualified Domain Names (FQDNs) or IP Addresses that group together applications, allowing for more effective policy management and traffic steering. By identifying applications through their specific FQDNs or IP addresses, organizations can apply security policies, access controls, and enable proper monitoring of application traffic. This concept is pivotal within Zscaler's framework as it enables organizations to ensure that security and access policies are applied based on the application context rather than simply on IP addresses or ports. This method enhances the granularity and precision of the security measures while managing user access based on the applications used. Other options, while related to networking and application management, do not accurately represent what an Application Segment is. For example, appending DNS suffixes or listing ports are specific technical configurations that do not capture the broader strategic grouping of applications by their FQDNs or IP addresses, which is the fundamental aspect of application segmentation in the context of Zscaler.

5. In Zero Trust architecture, what is emphasized regarding user access?

A. Access based solely on user credentials

B. Access based on location and time

C. Access based on user, device, and application context

D. Access based on random selection

In Zero Trust architecture, user access is primarily emphasized based on context. This means that access decisions take into account not only the user's identity but also the context in which the access request is being made. This includes variables like the user's device, the specific application being accessed, and the overall environment, including factors such as security posture and risk assessment at the time of the request. This contextual approach allows organizations to minimize potential vulnerabilities by enforcing security policies that are dynamically assessed rather than relying on static criteria like user credentials alone or factors like location and time. This adaptability and context-awareness are central to the Zero Trust model, as it assumes that threats could be present both outside and inside the network perimeter, requiring continuous verification and assessment of access rights.

6. What options for TLS Inspection Certificates are available? (Select 2)

A. Zscaler Root Certificate Authority

B. Customer Root Certificate Authority

C. Verisign Root CA

D. Microsoft Azure Certificate Authority

The correct choice concerning options for TLS Inspection Certificates includes the Zscaler Root Certificate Authority. This certificate is fundamental to Zscaler's architecture, as it is utilized to create secure connections while maintaining the ability to inspect encrypted traffic. By deploying the Zscaler Root Certificate Authority within your organization, you enable the Zscaler platform to decrypt and inspect legitimate SSL/TLS traffic for threats and policy violations without disrupting users' experiences. In addition to the Zscaler Root Certificate Authority, the Customer Root Certificate Authority is often used in scenarios where organizations want to leverage their internal infrastructure. By using their own Root CA, customers can manage their certificate lifecycle, trust hierarchies, and enforce specific security policies tailored to their organizational needs. While other options such as Verisign Root CA and Microsoft Azure Certificate Authority are well-known, they do not align with the specific TLS Inspection requirements established by Zscaler, which relies on its Root CA or the option to utilize a Customer CA for customized deployments.

7. What unique features does Zscaler's mobile app offer?

A. Voice recognition and biometric authentication

B. Secure access and simplified user experience

C. Offline browsing capabilities and ad-blocking features

D. Customizable themes and backgrounds

Zscaler's mobile app is designed to provide secure access while maintaining a simplified user experience, which is crucial for users who need reliable and efficient connectivity while on the go. This emphasis on secure access ensures that users can safely connect to resources and applications over the internet without compromising on security. The simplified user experience is achieved through an intuitive interface that allows users to navigate easily, maximizing productivity without unnecessary complexity. Other options, while they may sound appealing, do not reflect the core offerings of Zscaler's mobile app. Voice recognition and biometric authentication, for instance, are common in many mobile applications but are not specifically highlighted as unique features of Zscaler's app. Offline browsing capabilities and ad-blocking features could enhance user experience but are not central to Zscaler's primary focus on secure access. Customizable themes and backgrounds pertain more to aesthetic choices and user personalization rather than the functional security aspects that Zscaler prioritizes. Thus, the correct choice emphasizes the essential capabilities of the app that align with Zscaler's mission to deliver secure cloud access.

8. What stage follows after the initial compromise in a typical cyber attack?

A. Data encryption

B. Lateral movement

C. Finding the attack surface

D. Extortion attempts

In the context of a typical cyber attack, the stage that follows the initial compromise is lateral movement. After an attacker successfully gains initial access to a system or network, their next objective is often to explore the environment and move across different systems to escalate privileges and gain broader access to valuable resources. This lateral movement involves navigating the internal network, discovering additional vulnerabilities, and leveraging compromised accounts to infiltrate other devices, systems, or applications. This process is critical for the attacker, as it allows them to strategically position themselves to access sensitive data or deploy additional harmful payloads. The attackers may perform reconnaissance during this stage to identify key servers, databases, and other valuable assets, greatly increasing their ability to inflict damage or exfiltrate data before the attack is detected. The other stages mentioned, such as data encryption, finding the attack surface, and extortion attempts, do not occur immediately after the compromise and typically follow other steps in a cyber attack lifecycle. Data encryption is often related to ransomware attacks that come after lateral movement has enabled the attacker to gain access to critical systems. Finding the attack surface is part of the initial planning and reconnaissance process before any networks are compromised, while extortion attempts usually happen later, often as a result of successful data theft or

9. What role does Zscaler ThreatLabZ serve?

A. A team that monitors network traffic in real-time

B. A research team that analyzes security trends and updates databases

C. A group dedicated to public relations for Zscaler

D. A team specializing in customer support

Zscaler ThreatLabZ serves as a research team that focuses on analyzing security trends and updating databases with their findings. This is crucial for maintaining the platform's effectiveness against emerging threats. The team conducts extensive research into malware, vulnerabilities, and attack patterns, allowing them to provide timely updates to the Zscaler security infrastructure. This proactive approach ensures that Zscaler's customers are protected against the latest threats, contributing to a robust security environment. The contributions of ThreatLabZ are integral to the overall mission of Zscaler, which is to provide secure internet access and optimize user experience while minimizing risks. By continuously analyzing security data and trends, ThreatLabZ helps enhance the intelligence behind Zscaler's security measures, thereby reinforcing its position in the cybersecurity landscape.

10. Which address translation options are available in the Firewall policy? (Select 3)

A. Destination Port Translation

B. Source IP Translation to static IP

C. Destination IP Translation to static IP

D. Source Port Translation

E. Destination IP Translation to FQDN

In the context of a Firewall policy, address translation options are crucial for managing how IP addresses are modified as packets pass through. The question focuses on the types of address translation that can be configured within the policy. Destination Port Translation allows the firewall to change the port number of a packet destined for a specific IP address. This is particularly useful when multiple services are hosted on the same IP but need to be accessed through different ports. By altering the destination port, the firewall helps direct traffic to the appropriate internal service based on the port requested. Source IP Translation to static IP refers to the ability of the firewall to change the outgoing IP address of packets originating from the internal network. This is essential for ensuring that internal IP addresses remain private while still allowing communication with external networks. By translating the source IP to a static IP, organizations can maintain a consistent public-facing address. Destination IP Translation to static IP allows the firewall to map incoming traffic to a specific internal IP address. This means that even if the request comes to a public IP, the firewall can ensure it reaches the correct internal destination by translating the incoming IP to a designated internal IP, which is vital for services that may be hosted behind a firewall. The other options, such as Destination IP Translation to