SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure Security Benchmark compliance controls in Defender for Cloud

Correct Answer: A

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software.

Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.

When you\\'ve enabled and configured adaptive application controls, you\\'ll get security alerts if any application runs other than the ones you\\'ve defined as safe.

Incorrect:

Not B: App protection policies (APP) are rules that ensure an organization\\'s data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of

actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Not C: Cloud Discovery anomaly detection policy reference. A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded

data, uploaded data, transactions, and users are considered for each cloud application.

Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy

https://docs.microsoft.com/en-us/security/benchmark/azure/overview

QUESTION 2

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 subscription, and an Azure subscription.

The company\\'s on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

1.

Prevent the remote users from accessing any other resources on the network.

2.

Support Azure Active Directory (Azure AD) Conditional Access.

3.

Simplify the end-user experience. What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN

Correct Answer: A

Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal

application portal.

Azure AD Application Proxy is:

Secure. On-premises applications can use Azure\\'s authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application Proxy doesn\\'t require you to open inbound connections through your firewall.

Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don\\'t need to change or update your applications to work with Application Proxy.

Incorrect:

Not D: Azure Virtual WAN

Azure Virtual WAN is for end users, not for applications.

Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).

Site-to-site VPN connectivity.

Remote user VPN connectivity (point-to-site).

Private connectivity (ExpressRoute).

Intra-cloud connectivity (transitive connectivity for virtual networks).

VPN ExpressRoute inter-connectivity.

Routing, Azure Firewall, and encryption for private connectivity.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

QUESTION 3

Your company has an office in Seattle.

The company has two Azure virtual machine scales sets hosted on different virtual networks.

The company plans to contract developers in India.

You need to recommend a solution to provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

1.

Prevent exposing the public IP addresses of the virtual machines.

2.

Provide the ability to connect without using a VPN.

3.

Minimize costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a hub and spoke network by using virtual network peering.

B. Deploy Azure Bastion to each virtual network.

C. Enable just-in-time VM access on the virtual machines.

D. Create NAT rules and network rules in Azure Firewall.

E. Deploy Azure Bastion to one virtual network.

Correct Answer: AE

Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

Provision the service directly in your local or peered virtual network to get support for all the VMs within it.

Connect to your virtual machines in your local and peered virtual networks over SSL, port 443, directly in the Azure portal.

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don\\'t have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it

can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

Architecture

When VNet peering is configured, Azure Bastion can be deployed in hub-and-spoke or full-mesh topologies.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

https://azure.microsoft.com/en-us/products/azure-bastion/#features

QUESTION 4

Your company develops several applications that are accessed as custom enterprise applications in Azure AD.

You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications.

What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps

B. sign-in risk policies in Azure AD Identity Protection

C. Azure AD Conditional Access policies

D. device compliance policies in Microsoft Endpoint Manager

E. user risk policies in Azure AD Identity Protection

Correct Answer: A

Microsoft Defender for Cloud Apps Activity policies.

Activity policies allow you to enforce a wide range of automated processes using the app provider\\'s APIs. These policies enable you to monitor specific activities carried out by various users, or follow unexpectedly high rates of one certain

type of activity.

After you set an activity detection policy, it starts to generate alerts - alerts are only generated on activities that occur after you create the policy.

Each policy is composed of the following parts:

Activity filters – Enable you to create granular conditions based on metadata.

Activity match parameters – Enable you to set a threshold for the number of times an activity repeats to be considered to match the policy.

Actions – The policy provides a set of governance actions that can be automatically applied when violations are detected.

Incorrect:

Not C: Azure AD Conditional Access policies applies to users, not to applications.

Note: Blocking user logins by location can be an added layer of security to your environment. The following process will use Azure Active Directory conditional access to block access based on geographical location. For example, you are

positive that nobody in your organization should be trying to login to select cloud applications from specific countries.

Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/user-activity-policies
https://cloudcompanyapps.com/2019/04/18/block-users-by-location-in-azure-o365/

QUESTION 5

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware.

The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. The client access tokens are refreshed.

B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. Microsoft Defender for Endpoint reports the endpoints as compliant.

Correct Answer: AC

A: When a client acquires an access token to access a protected resource, the client also receives a refresh token. The refresh token is used to obtain new access/refresh token pairs when the current access token expires. Refresh tokens

are also used to acquire extra access tokens for other resources.

Refresh token expiration

Refresh tokens can be revoked at any time, because of timeouts and revocations.

C: Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. It uses a combination of endpoint behavioral sensors, cloud

security analytics, and threat intelligence.

The interviewees said that “by implementing Zero Trust architecture, their organizations improved employee experience (EX) and increased productivity.” They also noted, “increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager.” This had a bonus effect of reducing the number of agents installed on a user\\'s device, thereby increasing device stability and performance. “For some organizations, this can reduce boot times from 30 minutes to less than a minute,” the study states. Moreover, shifting to Zero Trust moved the burden of security away from users. Implementing single sign-on (SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.

Note: Azure AD at the heart of your Zero Trust strategy Azure AD provides critical functionality for your Zero Trust strategy. It enables strong authentication, a point of integration for device security, and the core of your user-centric policies to guarantee least-privileged access. Azure AD\\'s Conditional Access capabilities are the policy decision point for access to resource

Reference: https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/ https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens