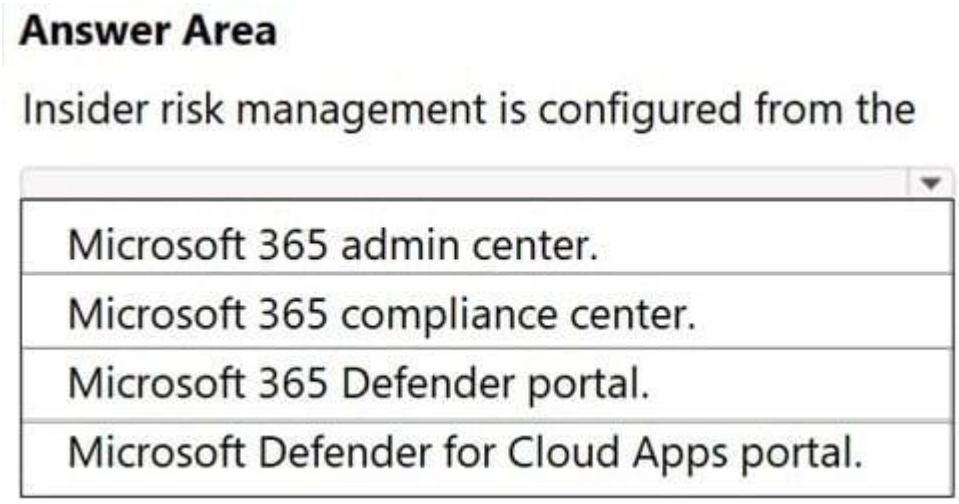
Vendor: Microsoft
Exam Code: SC-900
Exam Name: Microsoft Security Compliance and Identity Fundamentals
Certification: Microsoft Certifications
Total Questions: 267 Q&A (View Details)

https://www.leads4pass.com/sc-900.html

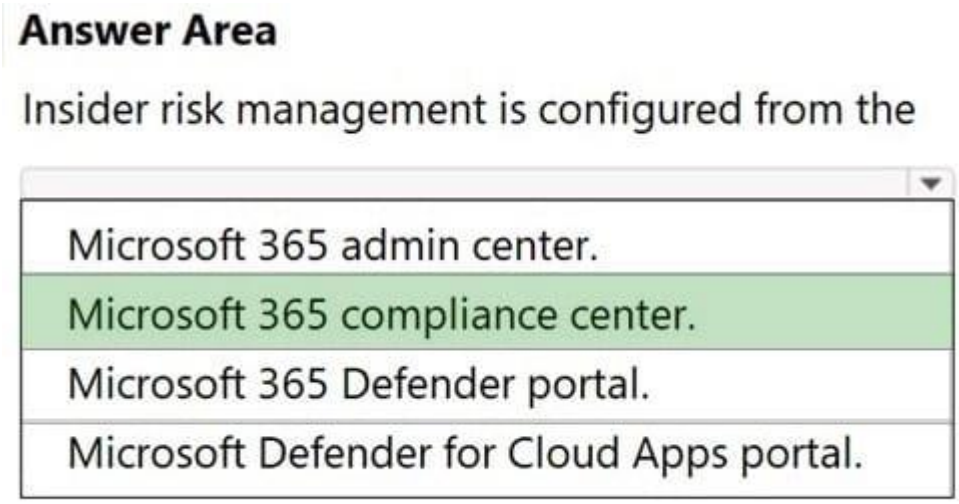
Question 1:
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Correct Answer:



Microsoft 365 Compliance center.

Add users to an insider risk management role group

Complete the following steps to add users to an insider risk management role group:

1.

Sign into Microsoft Purview compliance portal using credentials for an admin account in your Microsoft 365 organization.

2.

In the Security and Compliance Center, go to Permissions. Select the link to view and manage roles in Office 365.

3.

Select the insider risk management role group you want to add users to, then select Edit role group.

4.

Select Choose members from the left navigation pane, then select Edit.

5.

Select Add and then select the checkbox for all users you want to add to the role group.

6.

Select Add, then select Done.

7.

Select Save to add the users to the role group. Select Close to complete the steps.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide

---

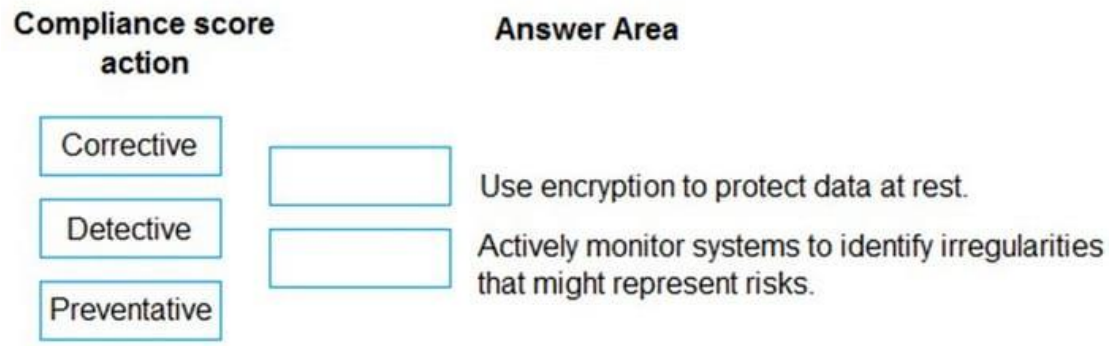
Question 2:
DRAG DROP

Match the types of compliance score actions to the appropriate tasks.

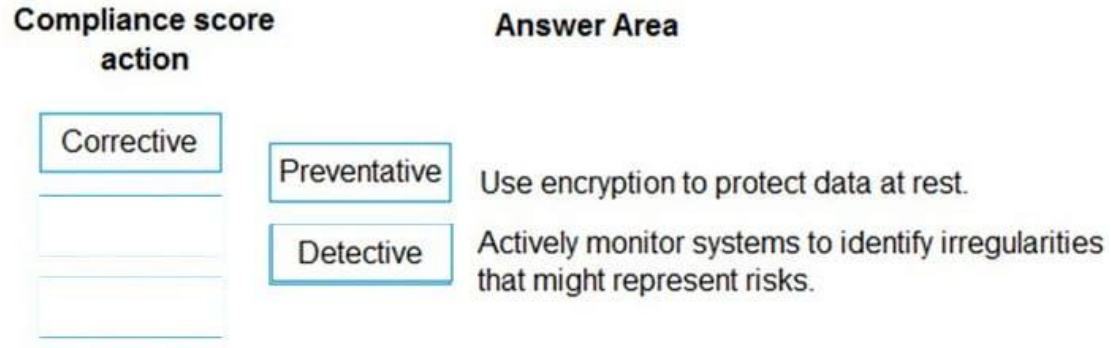
To answer, drag the appropriate action type from the column on the left to its task on the right. Each type may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Correct Answer:



Box 1: Preventative

Preventative actions address specific risks. For example, protecting information at rest using encryption is a preventative action against attacks and breaches. Separation of duties is a preventative action to manage conflict of interest and

guard against fraud.

Box 2: Detective

Detective actions actively monitor systems to identify irregular conditions or behaviors that represent risk, or that can be used to detect intrusions or breaches. Examples include system access auditing and privileged administrative actions.

Regulatory compliance audits are a type of detective action used to find process issues.

Incorrect:

Corrective actions try to keep the adverse effects of a security incident to a minimum, take corrective action to reduce the immediate effect, and reverse the damage if possible. Privacy incident response is a corrective action to limit damage

and restore systems to an operational state after a breach.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide

Question 3:
HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

Question 4:
Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.

B. Use identity as the primary security boundary.

C. Always verify the permissions of a user explicitly.

D. Always assume that the user system can be breached.

E. Use the network as the primary security boundary.

Correct Answer: BCD

Reference: https://docs.microsoft.com/en-us/security/zero-trust/

Question 5:
Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. fingerprint

B. facial recognition

C. PIN

D. email verification

E. security question

Correct Answer: ABC

Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

---

Question 6:
HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	○	○

Correct Answer:

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	○	○

Question 7:
HOTSPOT

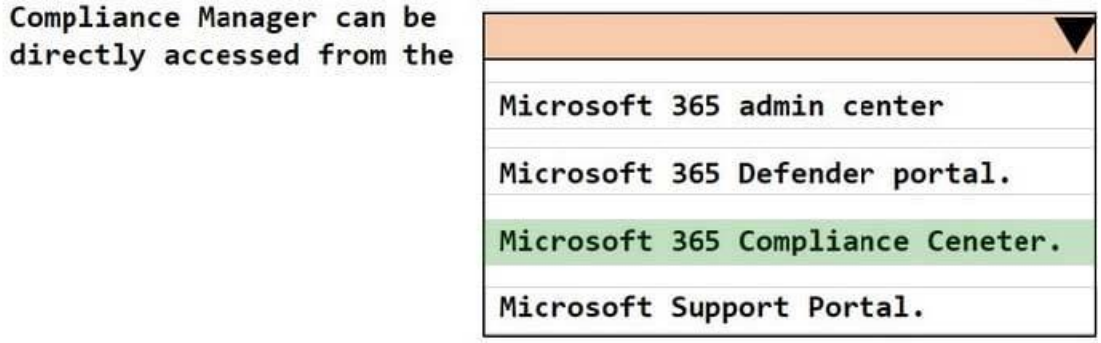
Select the answer that correctly completes the sentence.

Hot Area:

Compliance Manager can be directly accessed from the

- Microsoft 365 admin center
- Microsoft 365 Defender portal.
- Microsoft 365 Compliance Ceneter.
- Microsoft Support Portal.

Correct Answer:



Sign in to Compliance Manager

Go to the Microsoft Purview compliance portal and sign in with your Microsoft 365 global administrator account.

Select Compliance Manager on the left navigation pane. You\'ll arrive at your Compliance Manager dashboard.

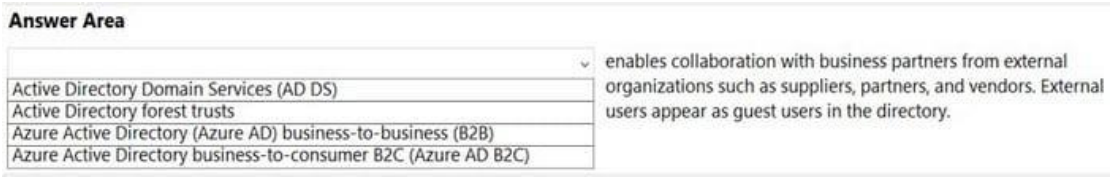
The direct link to access Compliance Manager is https://compliance.microsoft.com/compliancemanager Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup

---

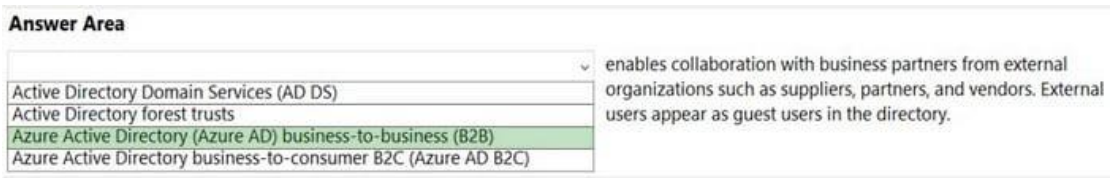
Question 8:
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Correct Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

Question 9:
HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Box 1: Yes

Box 2: No

Conditional Access policies are enforced after first-factor authentication is completed.

Box 3: Yes

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question 10:

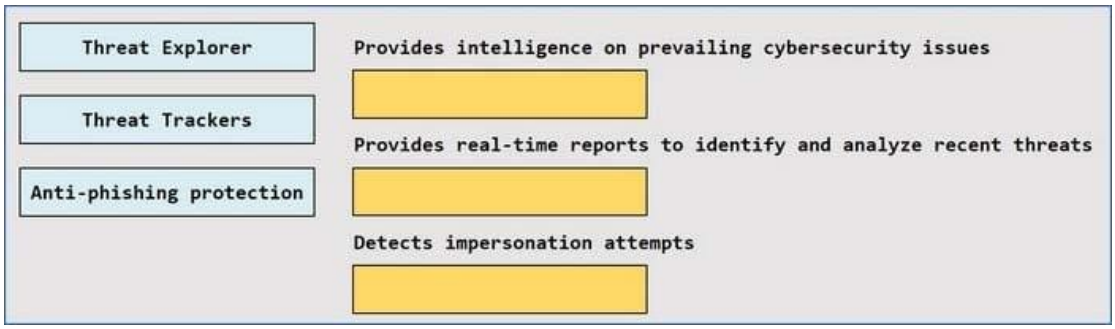
DRAG DROP

Match the Microsoft Defender for Office 365 feature to the correct description.

To answer, drag the appropriate feature from the column on the left to its description on the right. Each feature may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Correct Answer:

Question 11:
Which Microsoft 365 compliance center feature can you use to identify all the documents on a Microsoft SharePoint Online site that contain a specific key word?

A. Audit

B. Compliance Manager

C. Content Search

D. Alerts

Correct Answer: C

The Content Search tool in the Security and Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business.

The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide

---

Question 12:
Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune-managed devices from accessing corporate resources?

A. network security groups (NSGs)

B. Azure AD Privileged Identity Management (PIM)

C. conditional access policies

D. resource locks

Correct Answer: C

Question 13:
HOTSPOT

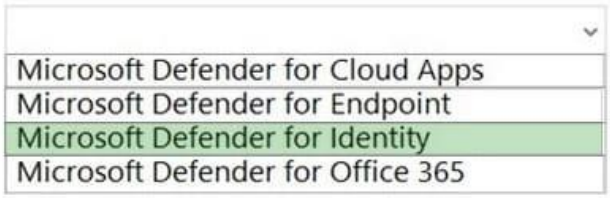
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Correct Answer:

Answer Area



is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Reference: https://docs.microsoft.com/en-us/defender-for-identity/what-is

---

Question 14:
HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Correct Answer:

Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	○	○
Microsoft Sentinel is a data lifecycle management solution.	○	○
Microsoft Purview can only discover data that is stored in Azure.	○	○

Box 1: Yes

Microsoft Purview allows you to apply sensitivity labels to assets, enabling you to classify and protect your data.

Box 2: Yes

Microsoft Sentinel content is Security Information and Event Management (SIEM) content that enables customers to ingest data, monitor, alert, hunt, investigate, respond, and connect with different products, platforms, and services in

Microsoft Sentinel.

Content sources for Microsoft Sentinel content and solutions

Each piece of content or solution has one of the following content sources:

Content hub - Content or solutions deployed by the content hub that support lifecycle management

Custom - Content or solutions you\'ve customized in your workspace

Gallery content- Content or solutions from the gallery that don\'t support lifecycle management

Repositories - Content or solutions from a repository connected to your workspace

Box 3: No

Microsoft Purview provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data.

Reference:

https://docs.microsoft.com/en-us/azure/purview/create-sensitivity-label

https://docs.microsoft.com/en-us/azure/sentinel/sentinel-solutions

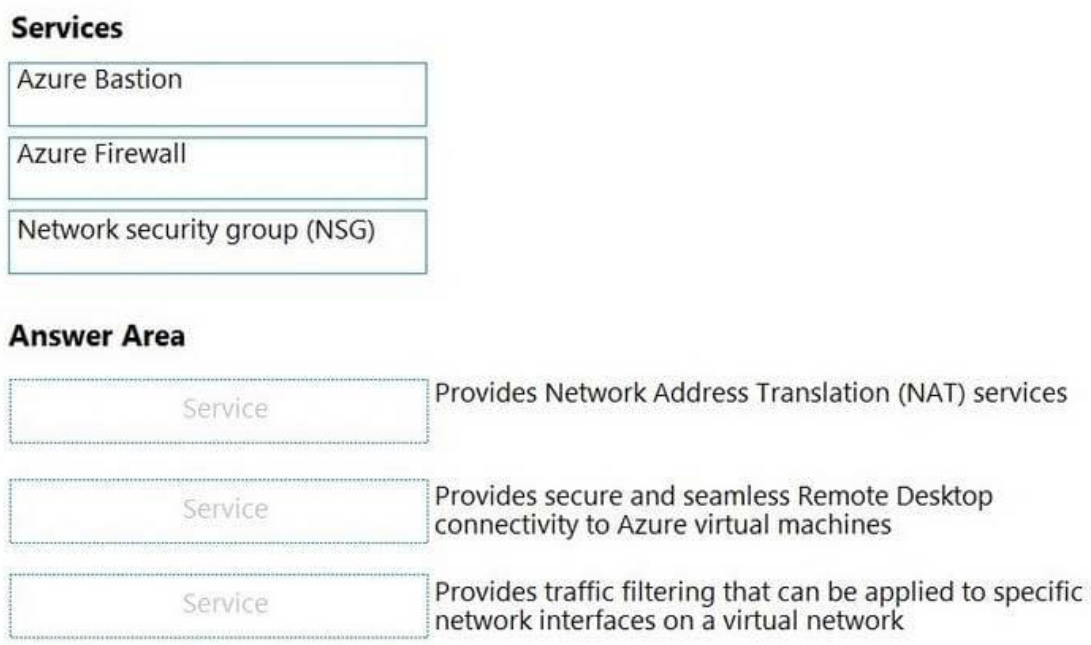
Question 15:
DRAG DROP

Match the Azure networking service to the appropriate description.

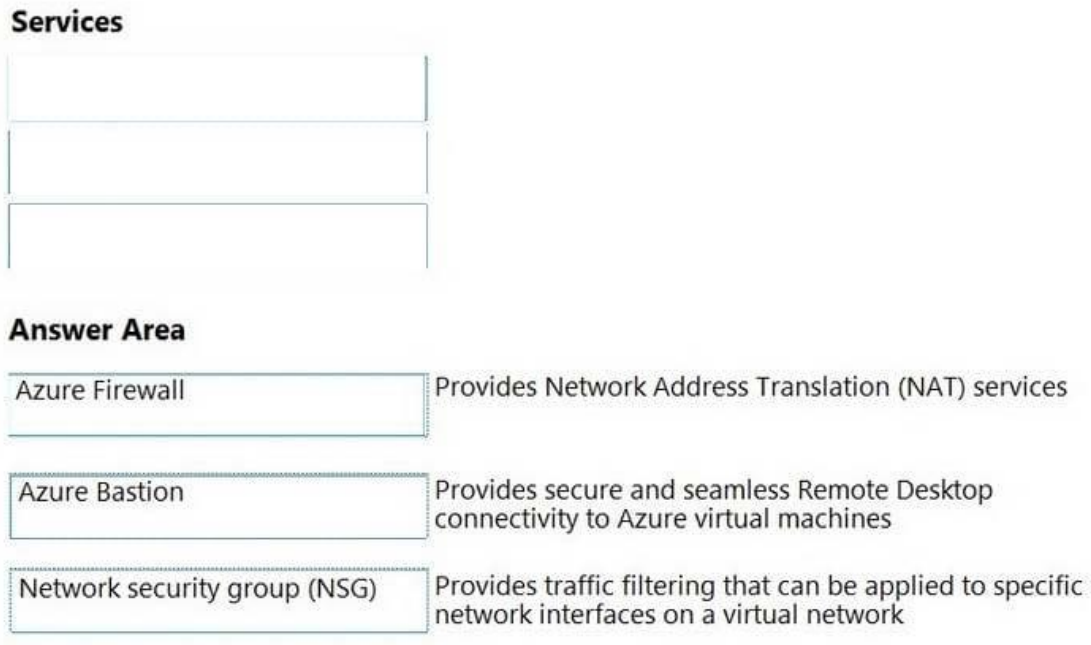
To answer, drag the appropriate service from the column on the left to its description on the right. Each service may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Correct Answer:



Box 1: Azure Firewall

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

Reference:

https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview

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

https://docs.microsoft.com/en-us/azure/firewall/features

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview