✓ 200 XP ▶

Understand firewalls and network security

10 minutes

A vulnerable network can be exploited by attackers to steal information and render services and resources inaccessible. Such an attack on your organization can lead to reputational and financial loss.

In this unit, we'll get an overview of network security and some of the different types available. We'll also learn about network security zones and firewalls. Finally, we'll explore the network security tools used to strengthen network protection in Azure.

Overview of network security

You need robust security to diagnose and prevent suspicious events, attacks, and weaknesses in your network. There are many reasons why security-related issues arise and several ways you can deal with them. Here we'll explore the different types of network security strategies that you can employ to deal with these issues.

Access control

You use access control to scrutinize every user and client to determine whether they have permission to access your network or its resources. Access control is implemented by configuring security policies that ensure the user has the right level of permissions assigned to do specific actions on your network. For example, you might want to deny read access for some resources when the user is connecting from outside your on-premises location.

Antimalware tools

Antimalware tools protect your network from malicious software (malware). Malware comes in different forms, including:

- Ransomware
- Viruses
- Spyware
- Trojans

Use antimalware and antivirus tools to monitor and remedy malware. These tools can detect anomalies in your files, taking actions to remove malicious pieces of code, and repairing affected resources and devices on your network.

Application security

Attackers can compromise applications whether they are your own or owned by a third party. The software may inadvertently contain security vulnerabilities that an attacker might use to access devices and network resources. If an application is developed in-house, you'll need to actively find and fix vulnerabilities that attackers could abuse. One solution is to test your application during its development lifecycle, and implement whatever changes are needed to fix a potential vulnerability. If you're dealing with an application development elsewhere, it's a good practice to apply updates as soon as they're available.

Behavioral analytics

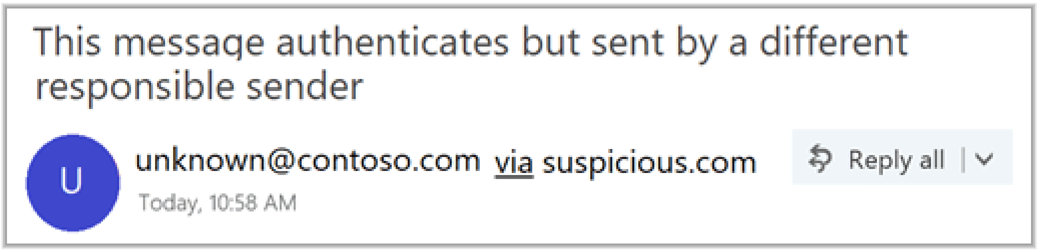
Use behavioral analytics tools to establish regular usage and behavior across your network and identify any suspicious changes.

For example, let's assume that you detect a user who starts accessing your network outside their standard usage patterns. Usually, the user accesses the network from one location in the United States during work hours. If their credentials are suddenly used to attempt access from Australia at midnight, the attempt is flagged as suspicious.

To address this problem, you can create security policies based on these analytics. You can deny access pending additional verification, like a secret code sent to the user's work mobile device.

Email security

Attackers often use email to access your network. An email that looks genuine might ask users to select a link and provide details that the attacker uses to access resources and devices on your network. Email applications like Microsoft Outlook help us identify suspicious messages and senders.



This message authenticates but sent by a different responsible sender

unknown@contoso.com via suspicious.com

Today, 10:58 AM

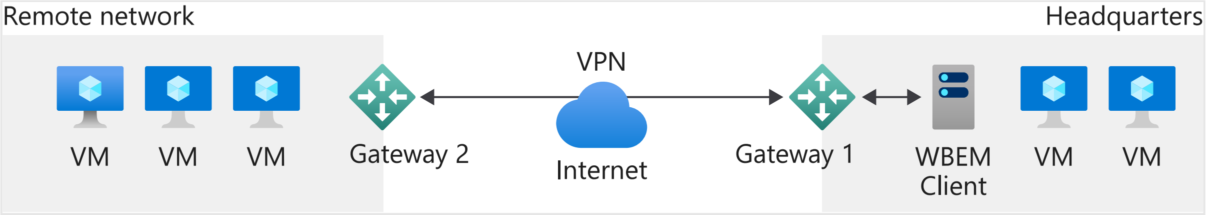
Intrusion detection and prevention

You want to take a proactive and preventative security posture for your network. The earlier you can identify intrusion, the better. You can use intrusion prevention and detection tools together to monitor all your network traffic.

For example, Azure Network Watcher can provide data to an open-source intrusion detection system. From this system traffic is analyzed across your network on Azure, and you're alerted about intrusions.

VPN

A virtual private network (VPN) can establish an encrypted connection from one network to another over the internet. The VPN configures an encrypted tunnel that either uses TLS or IPSec to provide secure communication and remote access capabilities across your networks.



Web security

You can employ tools that secure how your people use the web. For example, you use a web filter to prevent users from accessing certain types of sites that have been red-flagged. These web security tools also enable you to set up policies that help you decide how you want to handle different types of web requests in your network.

Wireless security

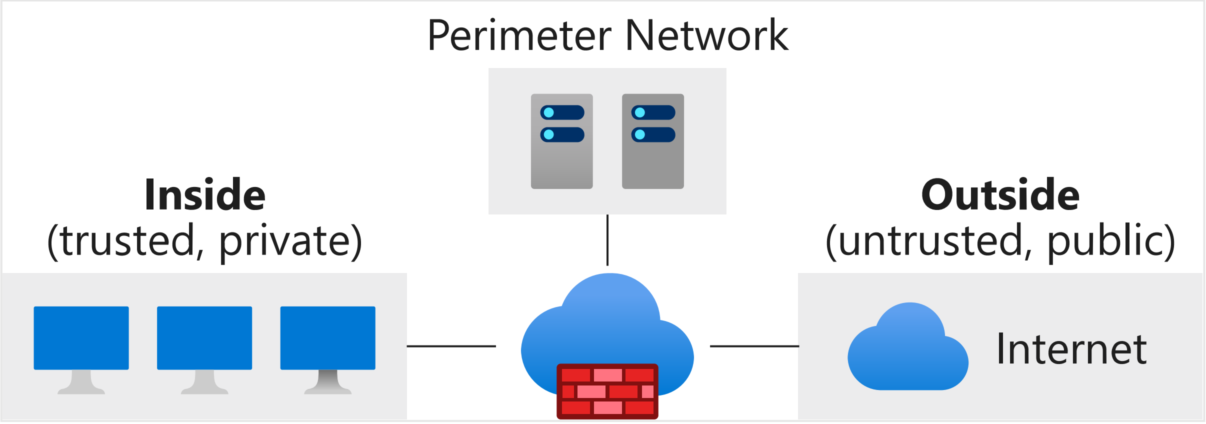
The wireless portions of your network aren't as secure as the wired portions. A wireless network is accessible from outside your organization, depending on the strength of the wireless signal. Different tools are available to scan and monitor activity on the wireless portions of your network. The first step to securing a wireless network is to use the strongest type of encryption available on wireless devices. Second, configure a separate wireless network for guests to prevent visitors from using the wireless network intended for internal users.

Network security zones

A network security zone is a network segment that has specific security policies applied to it and is often separated from other network segments by firewalls. There are three different types of security zones.

Trusted or private zones

A trusted or private zone contains the resources and devices that should never be accessible to anyone who's outside your organization. Examples include printers, workstations used by internal users, and internal servers. In this zone, you'll configure the devices with private IP addresses.



Public zones

A public zone contains everything outside the organization. This zone is part of the internet or another network and not in the control of the organization.

Perimeter network

The perimeter network (also known as DMZ, demilitarized zone, and screened subnet) is a zone where resources and services accessible from outside the organization are available. For example, you can use a perimeter network to provide access to an application, a partnering organization, or a supplier.

Zone filtering policies

Zone filtering policies handle the flow of traffic as it travels between different zones. These policies include:

- **Inside-to-outside** and **inside-to-perimeter-network**. This type of filter scrutinizes all traffic that originates from the inside and is headed to the perimeter network. For example, your internal staff members may want to access a public website. The traffic would be inspected to check whether the website is trustworthy.

- **Outside-to-inside**. This type of filter blocks traffic coming from outside into your network. The only traffic permitted will be traffic that is a direct response to a request that originated from the inside zone. For example, when an internal staff member requests a webpage from a server, the response is allowed (if it's a trusted source), so the user can browse the site.
- **Outside-to-perimeter-network**. This type of filter inspects all traffic coming from the outside and going to the perimeter network. The traffic will either be permitted or denied permission. The types of traffic that may be allowed to pass through include email and HTTPS traffic.
- **Perimeter-network-to-outside**. This type of filter inspects traffic that comes from the perimeter network and leaves your network. Traffic is permitted to travel outside the network based on firewall rules and the resource or client starting the request. For example, a mail server in the perimeter network might need to sync with another server that's outside the network. In this case, you'll configure firewall rules to decide what should happen.

What is a network firewall?

A network firewall is a security appliance that blocks or remedy unauthorized access into your network. Network firewalls also monitor and make logs of all traffic across your network. Use security policies to configure your network firewalls to take appropriate action on all traffic across your network. Network firewalls can be hardware or software implementations.

A **hardware firewall** can be a standalone physical device or form part of another device on your network. Physical devices like routers, for example, already have a built-in firewall. Hardware firewalls are expensive to operate and typically found in large organizations.

A **software firewall** is installed and configured on a device, like a workstation or a server. Software firewalls have flexible features and can be run on many devices more cost-effectively than hardware firewalls. However, certain sophisticated breaches can more easily compromise these types of firewalls.

Firewall types

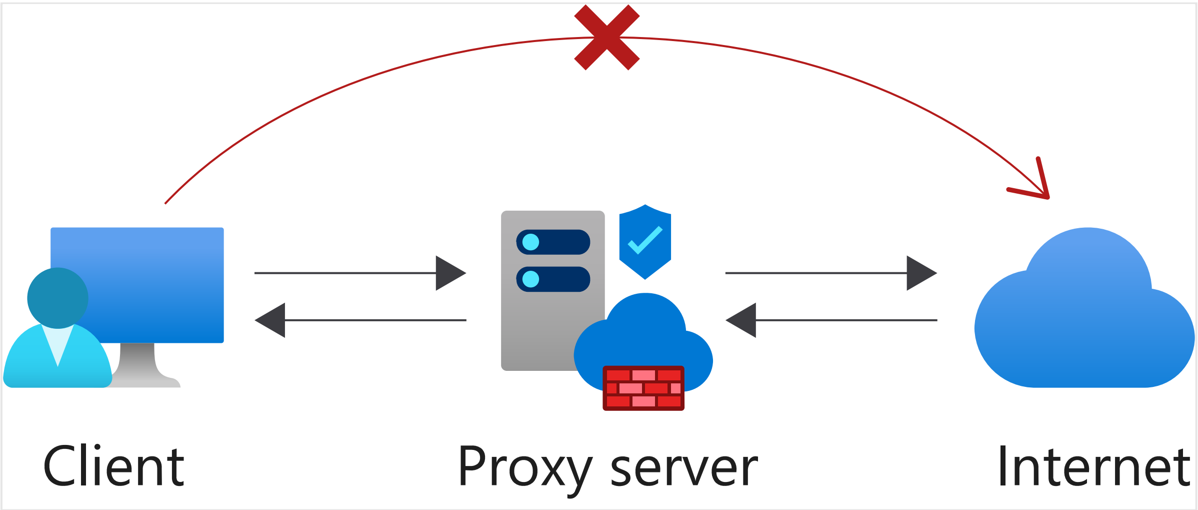
Firewalls can perform several different functions across your network:

- **Application-layer firewalls** can be a physical appliance, or software-based, like a plug-in or a filter. These types of firewalls target your applications. For example, they could affect how requests for HTTP connections are inspected across each of your applications.

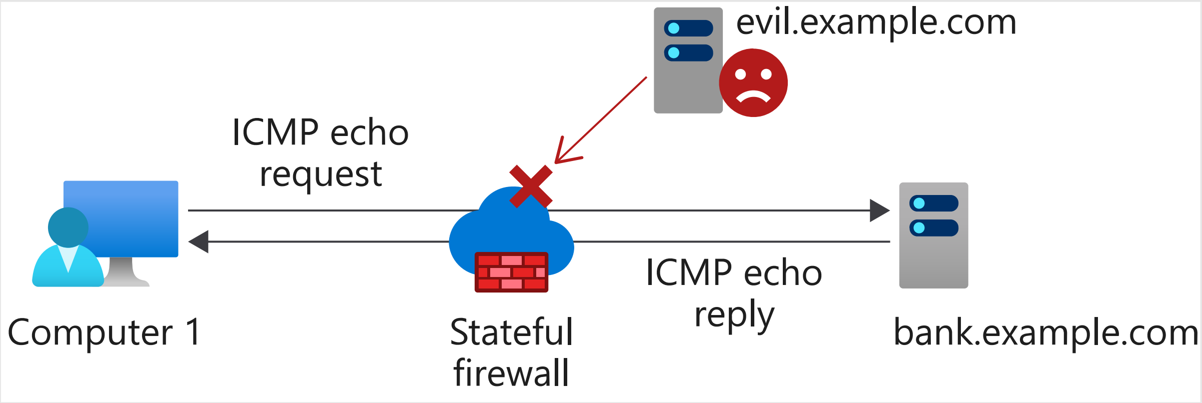
- **Packet filtering firewalls** scrutinize each data packet as it travels through your network. Based on rules you configure, they decide whether to block the specific packet or not.

- **Circuit-level firewalls** check whether TCP and UDP connections across your network are valid before data is exchanged. For example, this type of firewall might first check whether the source and destination addresses, the user, the time, and date meet certain defined rules. When these checks pass and a session starts, data is exchanged between parties without further scrutiny.

- **Proxy server firewalls** control the information that goes into and out of a network. Firewall proxy servers provide safety and security by providing internet access to all devices on a network. This ability means the server can monitor, filter, and cache data requests to and from the network.



- **Stateful firewalls** inspect characteristics about the connections on your network. The firewall also monitors packets over time and stores a combination of this information in a state table. When a connection and packet match aren't recognized, based on the information held in the table, traffic is blocked.



- **Next-generation firewalls** perform many of the same functions as stateful firewalls, but they can encompass more functions from other types of firewalls, such as packet filtering and VPN support. This type of firewall also investigates packets more thoroughly when compared to stateful firewalls. For example, a next-generation firewall could look at the payload for each packet and inspect it for suspicious characteristics and malware.

The importance of firewalls

Firewalls help protect your network from the outside world. If you don't have a firewall set up:

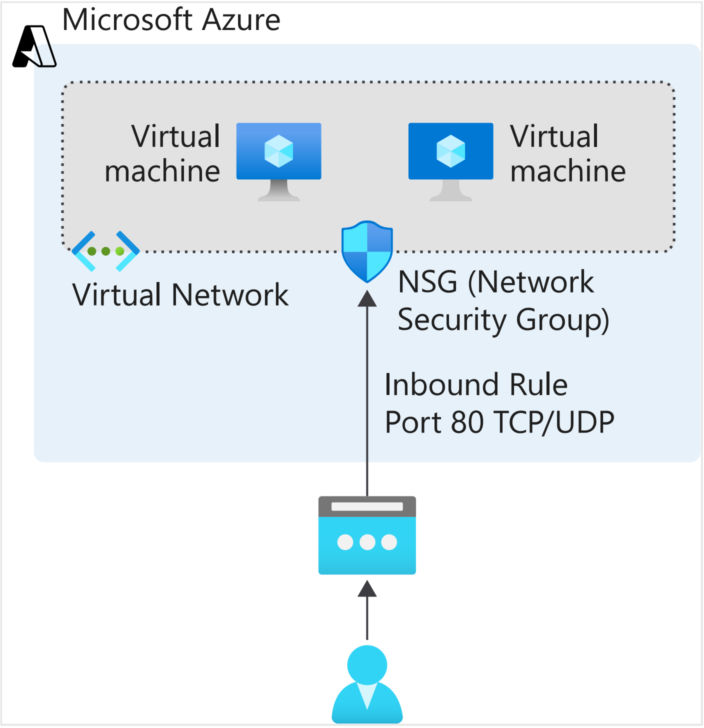
- An attacker could employ malware and take advantage of your bandwidth to use it for themselves.
- Sensitive and private information about employees and clients could be stolen.
- Your resources, devices, and the entire network could be held to ransom.

It's important to place firewalls between your network and any outside connection. You can combine different types of firewalls to achieve the most robust network security.

Azure network security tools

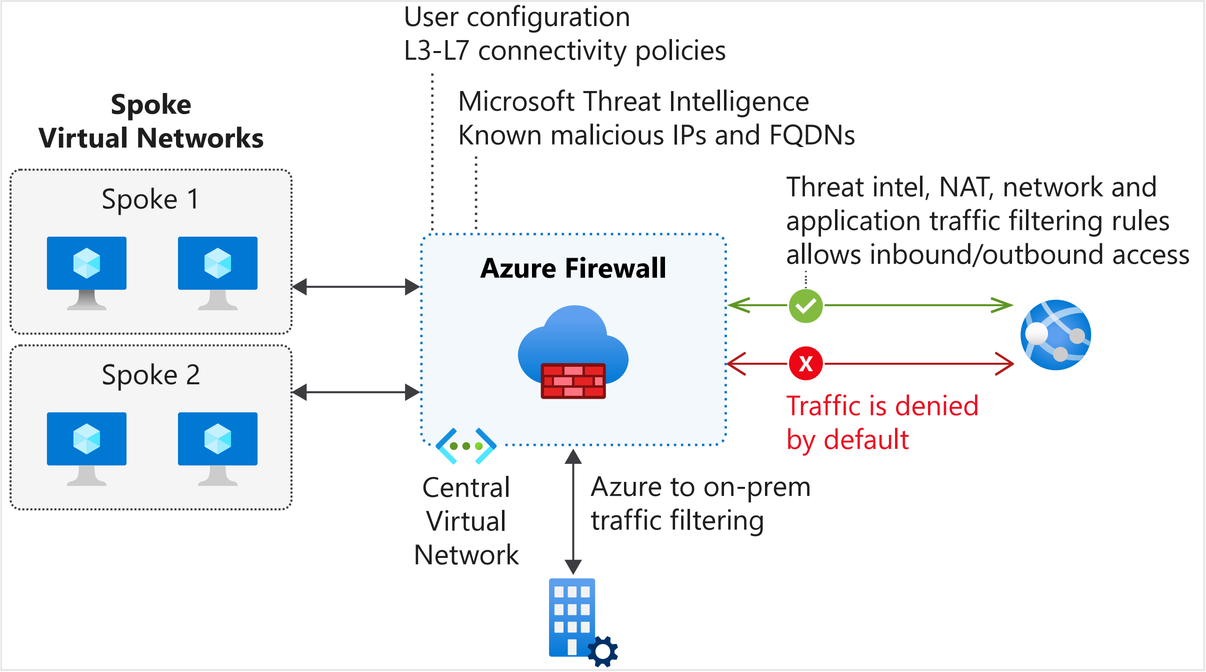
Azure provides several tools that you can use as part of your network security. Each of these tools is designed to address a different aspect of your network's security.

You can build your networks through Azure Virtual Network. Use **Network Security Groups** to filter traffic from Azure and on-premises resources to, and from, resources that form part of your virtual networks. A Network Security Group filters traffic through security rules that you specify to deny or permit different types of traffic across your networks.

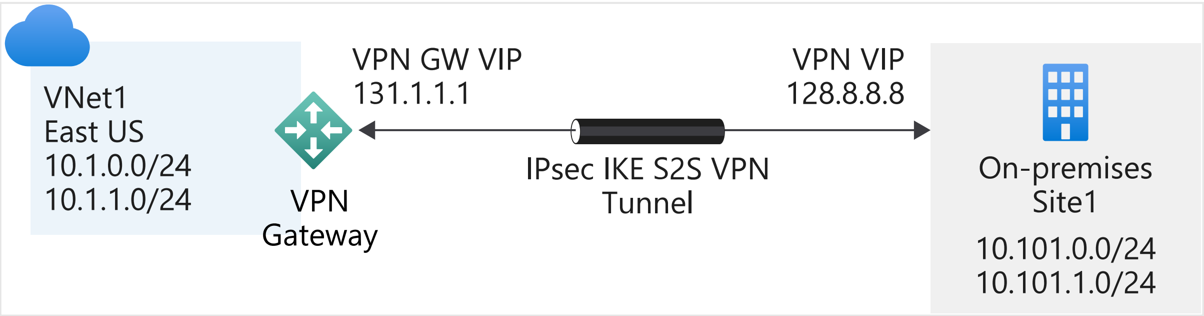


You can also log all the traffic flowing through your network security groups for analysis. Use the Azure Network Watcher service and enable NSG flow logs. Your logs will then be stored for use in a JSON file in a storage account.

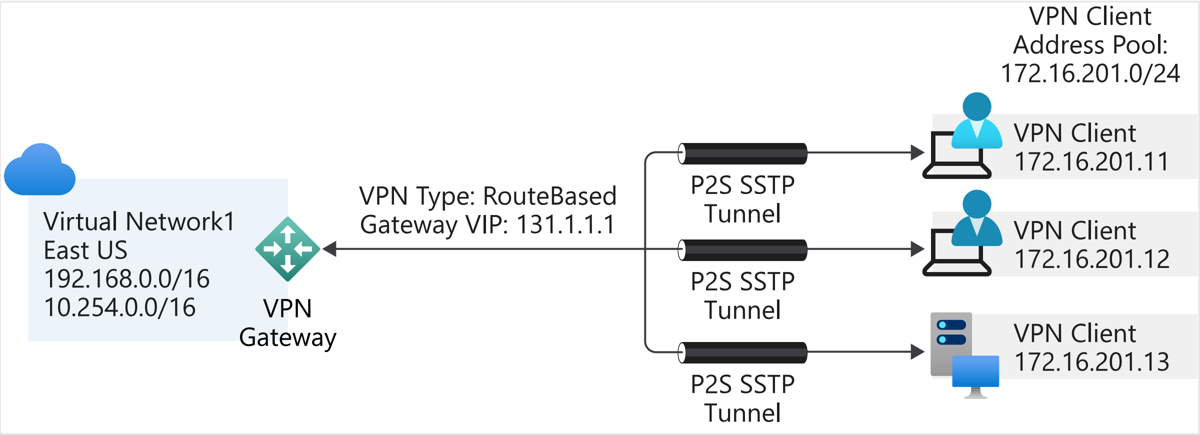
Azure Firewall is a fully managed firewall that you can use to protect the resources that are inside your Azure virtual networks. Because Azure Firewall is cloud-based, it comes with certain advantages. You won't have to worry about whether Azure Firewall can scale to the number of resources on your networks. It comes preconfigured with high availability to prevent your firewall from going down.


User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke Virtual Networks
Spoke 1
Spoke 2
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central Virtual Network
Azure to on-prem traffic filtering

You connect your on-premises network to your Azure virtual networks by configuring a **site-to-site VPN** connection with Azure. Use a VPN gateway (which is a VPN appliance from Azure), along with your local VPN device, to establish a VPN tunnel for communication. Your cloud and on-premises resources then communicate across the VPN tunnel.



You can also set up a **point-to-site VPN** connection between Azure and your on-premises network. Here, individual users and clients can connect to your Azure resources through a secure tunnel.



Azure network security considerations

There's much you can do to improve network security on Azure. Here are a few things you should consider implementing:

Use **Azure network security appliances**, developed by Microsoft partners on Azure Marketplace, to improve network security. This range of appliances provides a number of functions, including:

- Detecting anomalies on your network.
- Identifying and rectifying vulnerabilities.
- Web filtering.
- Antivirus protection.

Configure **Azure virtual network service endpoints** so that critical Azure services only connect to your Azure virtual networks, and not to the public internet. These services include:

- Azure SQL Database.
- Azure Storage.

- Azure App Service.
- Azure Key Vault.

Disable SSH/RDP access whenever possible. These protocols are used to manage your virtual machines from a remote location, but attackers could attempt brute-force attacks if no proper protections are in place. Create a point-to-site VPN connection before enabling SSH/RDP for remote management.

Use **load balancing** to improve the performance and availability of your network. When you use a load balancer, you distribute network traffic across the machines in your network. For example, if you have a couple of web servers that look after a website as part of your network, you can configure a load balancer to distribute the traffic between them. This way, you improve the performance and availability of the website.

A distributed denial-of-service (DDoS) attack overloads resources or services across your network so that they become unusable or inaccessible. **Azure DDoS Protection** provides automatic traffic monitoring and mitigating for DDoS attacks. You can interact with the service and enable additional features, like having access to DDoS experts, by upgrading to the Standard tier.

Check your knowledge

1. Which of the following best practices should you implement for your network security on Azure?

○ Disable load balancing of traffic.

● Disable SSH/RDP protocols.

✓ **You can enable it again once you've established a VPN tunnel for your connections.**

○ Disable network service endpoints.

2. You need to prevent users' devices from directly requesting web pages from the internet. Which tool would you use to do this?

○ Packet filtering firewall.

○ Circuit-level firewall.

● Proxy server firewall.

✓ **A proxy server helps you hide details about the requesting client.**

Next unit: Network monitoring

Continue >