# Introduction

Every system, architecture, and application needs to be designed with security in mind, whether on-premises or in the cloud. There's too much at risk. For example, a denial of service attack could prevent your customer from reaching your web site or services and block you from doing business. Or, your website could be defaced, causing damage to your reputation. A data breach could be even worse, as it can ruin hard-earned trust, while causing significant personal and financial harm. We must all work to guarantee the security of our systems.

**Tip**

### Contoso Shipping Case Study

You are working for Contoso Shipping, leading the development program of drone deliveries in rural areas, all while having truck drivers leverage mobile apps to deliver to urban areas. You're in the process of moving a large quantity of Contoso Shipping's infrastructure to the cloud in order to maximize efficiency. You are also moving several physical servers in the company's data center to Azure virtual machines. Your team plans on creating a hybrid solution, with some of the servers remaining on-premises. To do this, you'll need a secure, high-quality connection between the new virtual machines and the existing network.

In this module, you will explore the available network security capabilities in Azure and review how they help you build secure solutions in the cloud, based on your business needs. We will use the Contoso Shipping example to show real-world examples.

By the end of this module, you will be able to discuss the basic concepts for protecting your infrastructure and data when you work in the cloud. You will also, understand the responsibilities that are yours and what Azure takes care of for you.

**Level**:

Beginner

**Learning Objectives**

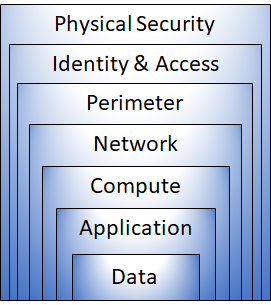
* Learn how security responsibility is shared with Azure
* Learn how identity management provides protection, even outside your network
* Learn how encryption capabilities built into Azure can protect your data
* Learn how to protect your network and virtual networks
* Learn about advanced services and features Azure provides to keep your services and data secure and safe

**Explore defense in depth**

**Defense in depth** is a strategy that employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to data. The objective of defense in depth is to protect and prevent information from being stolen by individuals not authorized to access it. The common principles used to define a security posture are **confidentiality**, **integrity**, and **availability**, known collectively as CIA.

* **Confidentiality** - The Principle of least privilege restricts access to information only to individuals explicitly granted access. This information includes protection of user passwords, remote access certificates, and email content.
* **Integrity** - The prevention of unauthorized changes to information at rest or in transit. A common approach used in data transmission is for the sender to create a unique fingerprint of the data using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The data's hash is recalculated and compared to the original by the receiver to ensure the data wasn't lost or modified in transit.
* **Availability** - Ensure services are available to authorized users. Denial of service attacks are a prevalent cause of loss of availability to users.

Defense in depth can be visualized as a set of layers, with the Data to be secured at the center. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection and acts to slow down an attack and provide alert telemetry that can be acted upon, either automatically or manually.



* **Physical security** is the first line of defense to protect computing hardware in the datacenter.
* **Identity & access** controls access to infrastructure and change control.
* **Perimeter** layer uses distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
* **Networking** layer limits communication between resources through segmentation and access controls.
* **Compute** layer secures access to virtual machines.
* **Application** layer ensures applications are secure and free of vulnerabilities.



**Data**

In almost all cases, attackers are after data:

* Stored in a database
* Stored on disk inside virtual machines
* Stored on a SaaS application such as Microsoft 365
* Stored in cloud storage

It's the responsibility of those storing and controlling access to data to ensure that it's properly secured. Often, there are regulatory requirements that dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.



**Application**

* Ensure applications are secure and free of vulnerabilities.
* Store sensitive application secrets in a secure storage medium.
* Make security a design requirement for all application development.

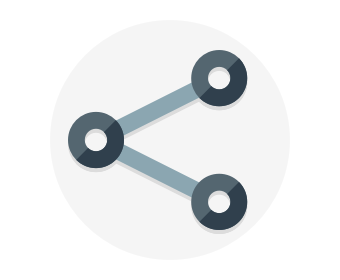
Integrating security into the application development life cycle will help reduce the number of vulnerabilities introduced in code. We encourage all development teams to ensure their applications are secure by default, and that they're making security requirements non-negotiable.



**Compute**

* Secure access to virtual machines.
* Implement endpoint protection and keep systems patched and current.

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure your compute resources are secure, and that you have the proper controls in place to minimize security issues.



**Networking**

* Limit communication between resources.
* Deny by default.
* Restrict inbound internet access and limit outbound, where appropriate.
* Implement secure connectivity to on-premises networks.

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what is required. By limiting this communication, you reduce the risk of lateral movement throughout your network.



**Perimeter**

* Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
* Use perimeter firewalls to identify and alert on malicious attacks against your network.

At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.



**Identity and access**

* Control access to infrastructure and change control.
* Use single sign-on and multi-factor authentication.
* Audit events and changes.

The identity and access layer is all about ensuring identities are secure, access granted is only what is needed, and changes are logged.



**Physical security**

* Physical building security and controlling access to computing hardware within the data center is the first line of defense.

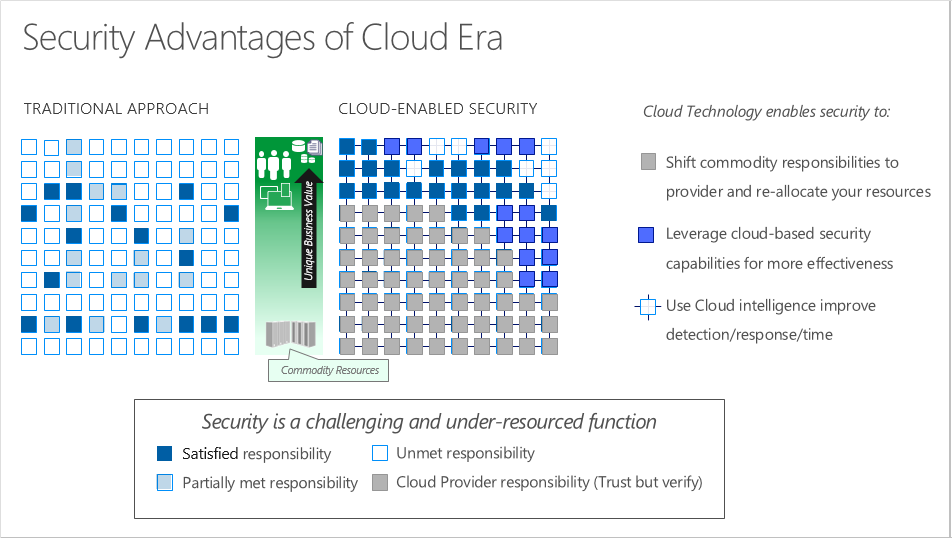
With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately.

Azure helps alleviate your security concerns. But security is still a **shared responsibility**. How much of that responsibility falls on us depends on which model we use with Azure. We use the *defense in depth* rings as a guideline for considering what protections are adequate for our data and environments.

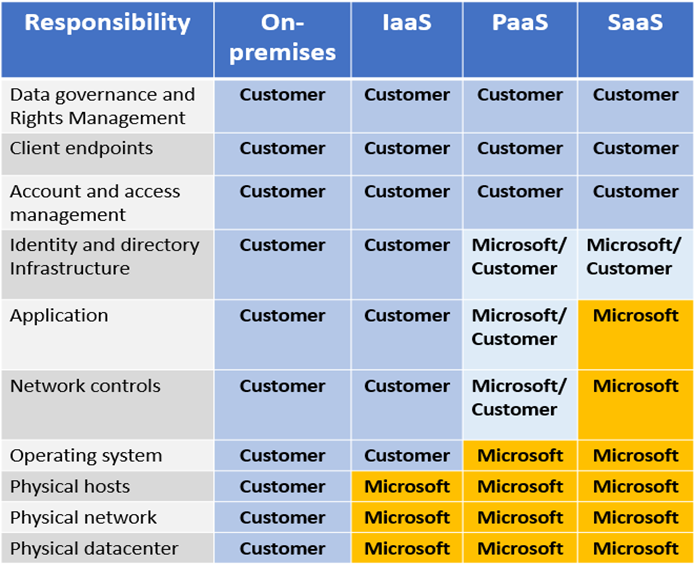
* Microsoft applies a layered approach to security, both in our physical datacenters and across Azure services.

# Define shared security

Organizations face many challenges with securing their datacenters, including recruiting and keeping security experts, using many security tools, and keeping pace with the volume and complexity of threats.



As computing environments move from customer-controlled datacenters to the cloud, the responsibility of security also shifts. Security of the operational environment is now a concern shared by both cloud providers and customers. By shifting these responsibilities to a cloud service like Azure, organizations can reduce focus on activities that aren't core business competencies. Depending on the specific technology choices, some security protections will be built into the particular service, while addressing others will remain the customer's responsibility. To ensure that the proper security controls are provided, a careful evaluation of the services and technology choices becomes necessary.



**Tip**

### Contoso Shipping - Security is a shared responsibility

One of the first shifts Contoso Shipping makes is from on-premises data centers to infrastructure as a service (IaaS). With IaaS, you are leveraging the lowest-level service and asking Azure to create virtual machines (VMs) and virtual networks. At this level, it's still your responsibility to patch and secure your operating systems and software, as well as configure your network to be secure. At Contoso Shipping, you are taking advantage of IaaS when you start using Azure virtual machines instead of your on-premises physical servers. In addition to the operational advantages, you receive the security advantage of having outsourced concern over protecting the physical parts of the network.

Next, it is time to build your drone app in the cloud. Moving to platform as a service (PaaS) outsources several security concerns. At this level, Azure is taking care of the operating system and of most foundational software like database management systems. Everything is updated with the latest security patches and can be integrated with Azure Active Directory for access controls. PaaS also comes with many operational advantages. Rather than building whole infrastructures and subnets for your environments by hand, you can "point and click" within the Azure portal or run automated scripts to bring complex, secured systems up and down, and scale them as needed. Contoso Shipping uses an app built on Azure for tracking telemetry data from drones and trucks — as well as a web app — which are both examples of PaaS.

With software as a service (SaaS), you outsource almost everything. SaaS is software that runs with an internet infrastructure. The code is controlled by the vendor but configured to be used by the customer. Like so many companies, Contoso Shipping uses Microsoft 365, which is a great example of SaaS!

# Explore Azure Firewall

A **Firewall** is a service that grants server access based on the originating IP address of each request. You create firewall rules that specify ranges of IP addresses. Only clients from these granted IP addresses will be allowed to access the server. Firewall rules also include specific network protocol and port information.

Azure Firewall icon.

[Azure Firewall](https://azure.microsoft.com/services/azure-firewall) is a managed, cloud-based, network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can create, enforce, and log, application and network connectivity policies across subscriptions, and virtual networks, centrally. Azure Firewall uses a static public IP address for your virtual network resources, which allows outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Azure Firewall provides many features, including:

* Built-in high availability.
* Unrestricted cloud scalability.
* Inbound and outbound filtering rules.
* Azure Monitor logging.

### Common usage scenarios

You typically deploy Azure Firewall on a central virtual network to control general network access. With Azure Firewall you can configure:

* Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
* Network rules that define source address, protocol, destination port, and destination address.
* [Azure Application Gateway](https://azure.microsoft.com/services/application-gateway) also provides a firewall, called the [**Web Application Firewall** (WAF)](https://azure.microsoft.com/services/web-application-firewall/). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities

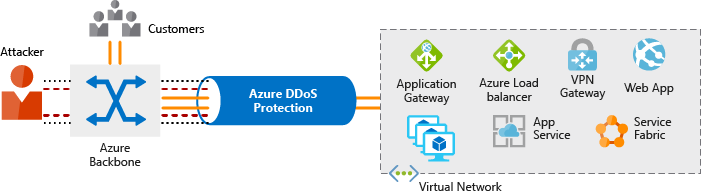
**Explore Azure Distributed Denial of Service protection**



[Distributed Denial of Service (DDoS)](https://azure.microsoft.com/services/ddos-protection) attacks attempt to overwhelm and exhaust an application’s resources, making the application slow or unresponsive to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Thus, any resource exposed to the internet, such as a website, is potentially at risk from a DDoS attack.

When you combine Azure DDoS Protection with application design best practices, you help provide defense against DDoS attacks. DDoS Protection leverages the scale and elasticity of Microsoft’s global network to bring DDoS mitigation capacity to every Azure region. The Azure DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.

This diagram shows network traffic flowing into Azure from both customers and an attacker. Azure DDoS protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from reaching Azure services. Legitimate traffic from customers still flows into Azure without any interruption of service.



**Azure Distributed Denial of Service (DDoS) protection service tiers**

Azure DDoS Protection provides the following service tiers:

* **Basic**. The Basic service tier is automatically enabled as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft’s online services use. Azure’s global network is used to distribute and mitigate attack traffic across regions.
* **Standard**. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway.

**Distributed Denial of Service (DDoS) standard protection**

DDoS standard protection can mitigate the following types of attacks:

* **Volumetric attacks**. The attack's goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
* **Protocol attacks**. These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
* **Resource (application) layer attacks**. These attacks target web application packets to disrupt the transmission of data between hosts.

**Define Network Security Groups**

[Network Security Groups (NSG)](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups?azure-portal=true) allow you to filter network traffic to and from Azure resources in an Azure virtual network. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

**Network security rule properties**

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies the following properties:

| **DEFINE NETWORK SECURITY GROUPS** | |
| --- | --- |
| **Property** | **Explanation** |
| Name | Unique name of the Network Security Group (NSG). |
| Priority | A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers. |
| Source or Destination | Individual IP address or IP address range, service tag, or application security group. |
| Protocol | TCP, UDP, or Any. |
| Direction | Whether the rule applies to inbound or outbound traffic. |
| Port Range | An individual port or range of ports. |
| Action | Allow or Deny. |

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

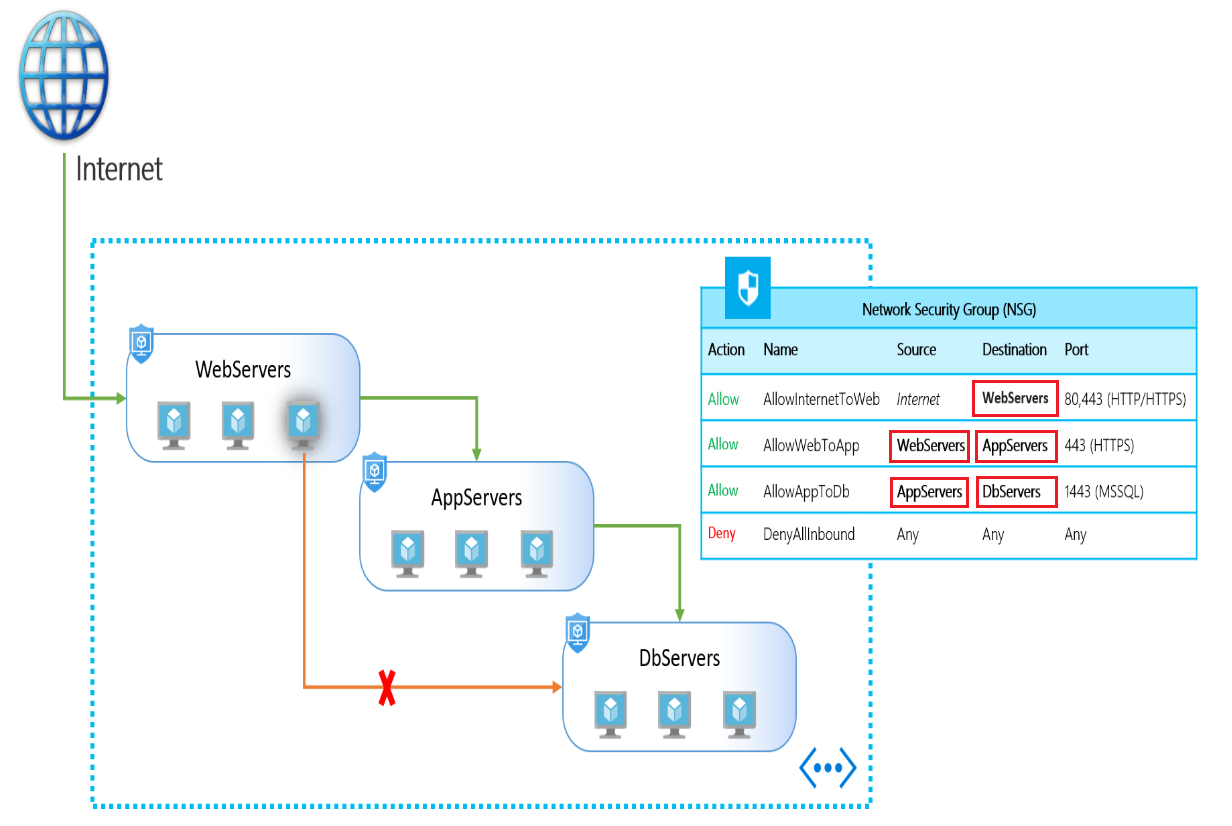
# Define Application Security Groups

[Application security groups (ASG)](https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups) enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

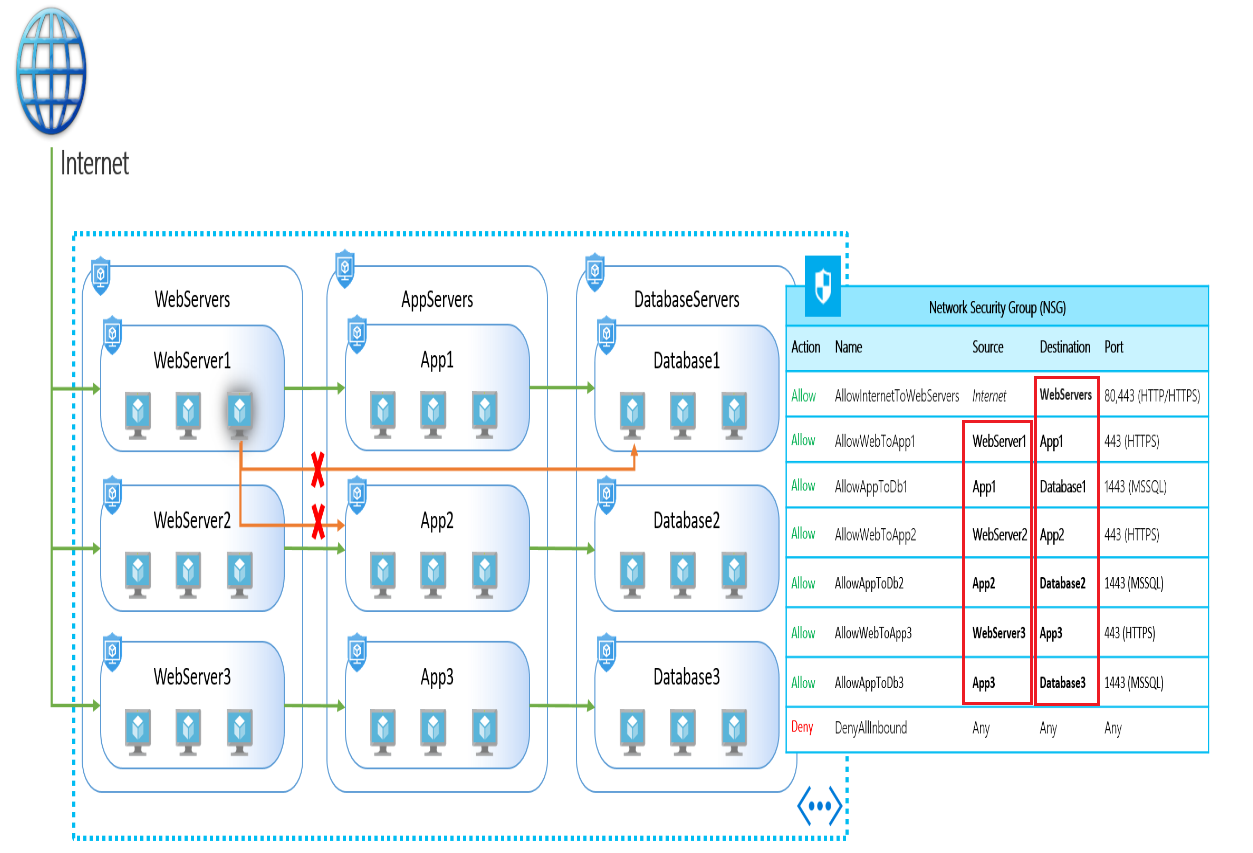
This feature allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

## Example

An Application Security Group enables you to group servers with similar port filtering requirements, and group together servers with similar functions, such as web servers. In the below example, we have ASGs defined for Web Servers, App Servers, and DB Servers and green and red arrows indicating which network traffic paths are allowable and which are not.



In the below example, multiple applications are deployed into the same virtual network. Based on the security rules described, workloads are isolated from each other. If a virtual machine from one of the applications is compromised, lateral exploration is limited, minimizing the potential impact of an attacker. In this example, let’s assume one of the web server virtual machines from application1 is compromised, the rest of the application will continue to be protected, even access to critical workloads like database servers will still be unreachable. This implementation provides multiple extra layers of security to your network, making this intrusion less harmful and easy to react on such events.



Application Security Groups help simplify how you can filter and control network traffic coming into your organization and how that network traffic is allowed to move. They allow you to isolate multiple workloads and provide additional levels of protection for your virtual network in a more easily manageable way.

# Choose Azure network security solutions

When considering your Azure security solution consider all the elements of defense in depth.

## Perimeter layer

The network perimeter layer is about protecting organizations from network-based attacks against your resources. Identifying these attacks, alerting, and eliminating their impact is important to keep your network secure. To do this:

* Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for end users.
* Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

## Network layer

At this layer, the focus is on limiting network connectivity across all your resources to only allow what is required. Segment your resources and use network-level controls to restrict communication to only what is needed. By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack. Use NSGs to create rules about inbound and outbound communication at this layer. As best practices:

* Limit communication between resources through segmenting your network and configuring access controls.
* Deny by default.
* Restrict inbound internet access and limit outbound where appropriate.
* Implement secure connectivity to on-premises networks.

## Combine services

You can also combine multiple Azure networking and security services to manage your network security and provide increased layered protection. The following are examples of combined services:

* **Network security groups and Azure Firewall**. Azure Firewall complements network security group functionality. Together, they provide better defense-in-depth network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall-as-a-service, which provides network and application-level protection across different subscriptions and virtual networks.
* **Application Gateway WAF and Azure Firewall**. WAF is a feature of Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities. Azure Firewall provides inbound protection for non-HTTP/S protocols (for example, RDP, SSH, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S. Combining both provides additional layers of protection.