200 XP

Network security

10 minutes

Securing your network from attacks and unauthorized access is an important part of any architecture. As part of the planning for its cloud migration, Lamna Healthcare took the time to plan out its network infrastructure to ensure it had the proper network security controls in place to protect its network infrastructure from attack. Here, we'll take a look at what network security looks like, how to integrate a layered approach into your architecture, and how Azure can help you provide network security for your environment.

What is network security

Network security is protecting the communication of resources within and outside of your network. The goal is to limit exposure at the network layer across your services and systems. By limiting this exposure, you decrease the likelihood that your resources can be attacked. In the focus on network security, efforts can be focused on the following areas:

- Securing traffic flow between applications and the internet
- Securing traffic flow amongst applications
- Securing traffic flow between users and the application

Securing traffic flow between applications and the internet focuses on limiting exposure outside your network. Network attacks will most frequently start outside your network, so by limiting the internet exposure and securing the perimeter, the risk of being attacked can be reduced.

Securing traffic flow amongst applications focuses on data between applications and their tiers, between different environments, and in other services within your network. By limiting exposure between these resources, you reduce the effect a compromised resource can have. This can help reduce further propagation within a network.

Securing traffic flow between users and the application focuses on securing the network flow for your end users. This limits the exposure your resources have to outside attacks, and provides a secure mechanism for users to utilize your resources.

A layered approach to network security

A common thread throughout this module has been taking a layered approach to security, and this approach is no different at the network layer. It's not enough to just focus on securing the

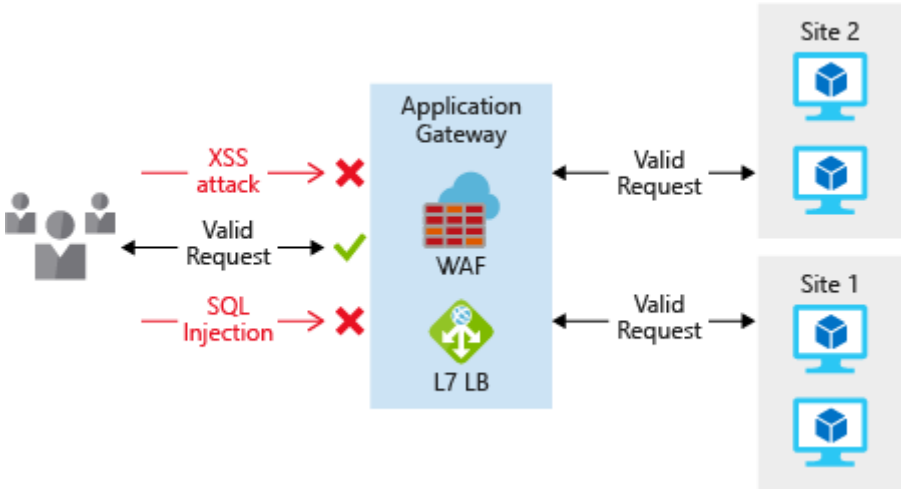
network perimeter, or focusing on the network security between services inside a network. A layered approach provides multiple levels of protection, so that if an attacker gets through one layer, there are further protections in place to limit further attack.

Let's take a look at how Azure can provide the tools for a layered approach to securing your network footprint.

Internet protection

If we start on the perimeter of the network, we're focused on limiting and eliminating attacks from the internet. A great first place to start is to assess the resources that are internet-facing, and only allow inbound and outbound communication where necessary. Identify all resources that are allowing inbound network traffic of any type, and ensure they are necessary and restricted to only the ports/protocols required. Azure Security Center is a great place to look for this information, as it will identify internet-facing resources that don't have network security groups (NSG) associated with them, as well as resources that are not secured behind a firewall.

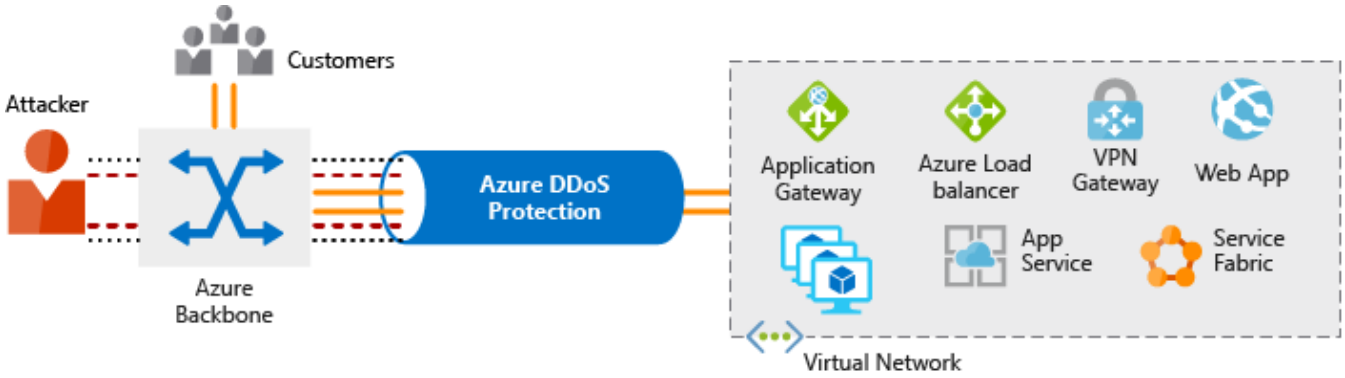
To provide inbound protection at the perimeter, there are a couple of ways to do this. Application Gateway is a Layer 7 load balancer that also includes a web application firewall (WAF) to provide advanced security for your HTTP-based services. The WAF is based on rules from the OWASP 3.0 or 2.2.9 core rule sets, and provides protection from commonly-known vulnerabilities such as cross-site scripting and SQL injection.



For protection of non-HTTP-based services or for increased customization, network virtual appliances (NVA) can be used to secure your network resources. NVAs are similar to firewall appliances you might find in on-premises networks, and are available from many of the most popular network security vendors. NVAs can provide greater customization of security for those applications that require it, but can come with increased complexity, so careful consideration of requirements is advised.

Any resource exposed to the internet is at risk of being attacked by a denial-of-service attack. These types of attacks attempt to overwhelm a network resource by sending so many requests

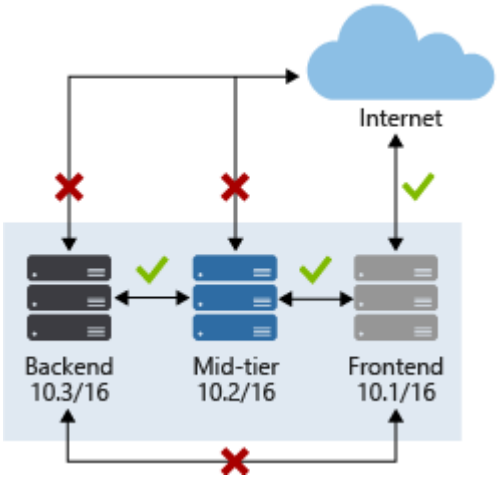
that the resource becomes slow or unresponsive. To mitigate these attacks, Azure DDoS provides basic protection across all Azure services and enhanced protection for further customization for your resources. DDoS protection blocks attack traffic and forwards the remaining traffic to its intended destination. Within a few minutes of attack detection, you are notified using Azure Monitor metrics.



Virtual network security

Once inside a virtual network (VNet), it's important to limit communication between resources to only what is required.

For communication between virtual machines, network security groups (NSG) are a critical piece to restrict unnecessary communication. NSGs operate at layers 3 & 4, and provide a list of allowed and denied communication to and from network interfaces and subnets. NSGs are fully customizable, and give you the ability to fully lock down network communication to and from your virtual machines. By using NSGs, you can isolate applications between environments, tiers, and services.



To isolate Azure services to only allow communication from virtual networks, use VNet service endpoints. With service endpoints, Azure service resources can be secured to your virtual network. Securing service resources to a virtual network provides improved security by fully removing public internet access to resources, and allowing traffic only from your virtual

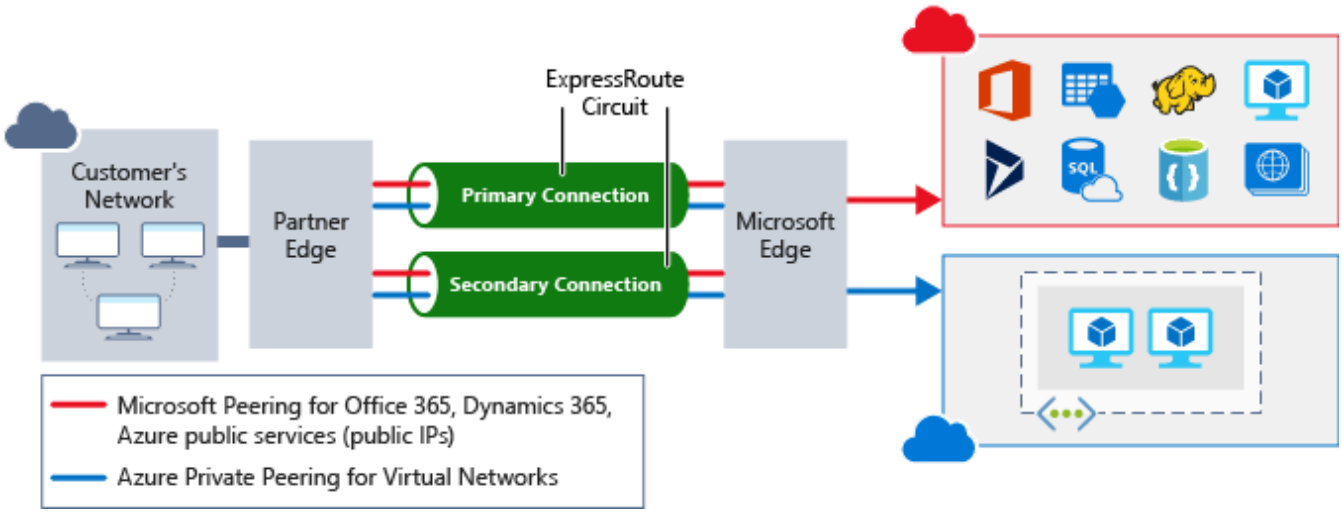
network. This reduces the attack surface for your environment, reduces the administration required to limit communication between your VNet and Azure services, and provides optimal routing for this communication.

Network integration

It's common to have existing network infrastructure that needs to be integrated to provide communication from on-premises networks, or to provide improved communication between services in Azure. There are a few key ways to handle this integration and improve the security of your network.

Virtual private network (VPN) connections are a common way of establishing secure communication channels between networks, and this is no different when working with virtual networking on Azure. Connection between Azure VNets and an on-premises VPN device is a great way to provide secure communication between your network and your virtual machines on Azure.

To provide a dedicated, private connection between your network and Azure, you can use ExpressRoute. ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365. This improves the security of your on-premises communication by sending this traffic over the private circuit instead of over the internet. You don't need to allow access to these services for your end users over the internet, and you can send this traffic through appliances for further traffic inspection.



To easily integrate multiple VNets in Azure, VNet peering establishes a direct connection between designated VNets. Once established, you can use NSGs to provide isolation between resources in the same way you secure resources within a VNet. This integration gives you the ability to provide the same fundamental layer of security across any peered VNets. Communication is only allowed between directly connected VNets.

Network security at Lamna Healthcare

Lamna Healthcare has taken advantage of many of these services to build out a secure network infrastructure. Communication between resources is denied by default, and allowed only when required. Inbound connectivity from the internet is enabled only for services that require it; RDP and SSH are not permitted from internet endpoints, only from trusted internal resources.

To secure their internet-facing web services, they place them behind Application Gateways with WAF enabled. This is true both for services running on virtual machines as well as on App Service. By using Application Gateways, they have protection from many of the common vulnerabilities.

They have DDoS standard enabled, to provide protection for their internet-facing endpoints from denial-of-service attacks.

Through the use of NSGs, they are able to fully isolate communication between application services and between environments. They only allow the necessary communication between services within an environment, and no access is allowed between production and non-production environments.

To provide dedicated connectivity between their end users and applications in Azure, they have provisioned an ExpressRoute circuit with connectivity to their on-premises network. This keeps their traffic to Azure off the internet and a private connection for their services in Azure to communicate with systems remaining on-premises.

With this approach, Lamna Healthcare has leveraged Azure services to provide security at multiple layers of their network infrastructure.

Summary

A layered approach to network security helps reduce your risk of exposure through network-based attacks. Azure provides several services and capabilities to secure your internet-facing resource, internal resources, and communication between on-premises networks. These features make it possible to create secure solutions on Azure.

Check your knowledge

1. Azure network security groups can be used to secure communication between which of the following?

- ○ Communication between Azure virtual machines and the internet

- ○ Communication between Azure virtual machines within a VNet
- ○ Communication between Azure virtual machines and systems in an on-premises network
- ○ All of the above

2. Which of the following is not a method for protecting internet facing services from network attacks?

- ○ Azure DDoS
- ○ Azure Application Gateway WAF
- ○ Azure Disk Encryption
- ○ A network virtual appliance

Check your answers