Azure DDoS Protection

Background on DDoS Attacks

The aim of a Distrubuted Denial of Service (DDoS) attack is to overwhelm resources on applications and servers rendering them unusable. The three most common types of DDoS attacks are:

- Volumetric: volume-based attacks that flood the network with what seems to be genuine traffic to consume all available bandwith
- Protocol: render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. Measured in packets per second.
- Resource (application) layer: Target web application packets to distrupt the transmission of data between hosts.

What is Azure DDoS Protection?

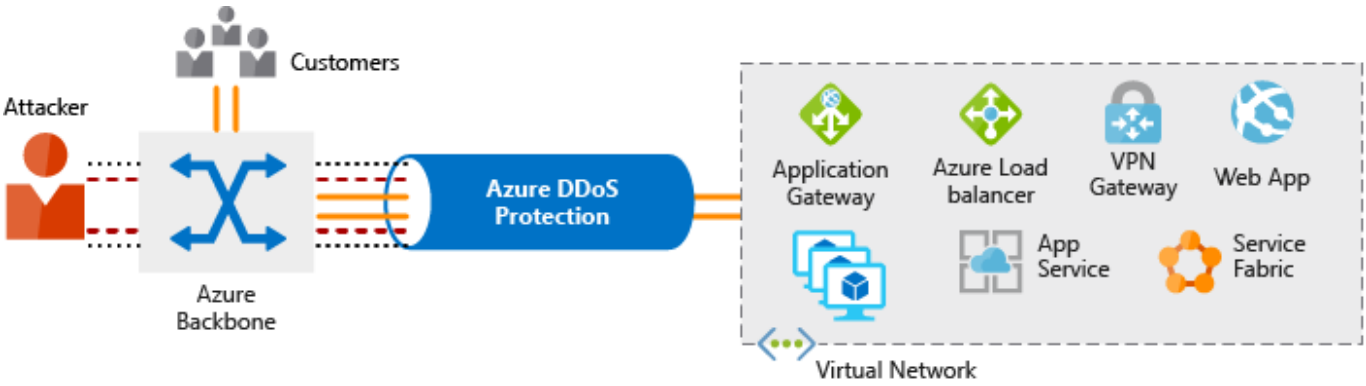

Diagram above shows Azure DDoS Protection blocking traffic, but still letting legitimate traffic from customers through.

Azure DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. Azure DDoS Protection comes in two tiers:

- Basic: is enabled for every property in Azure at no extra cost as part of the Azure platform. Always-on traffic monitoring and real time mitigation of common network level attacks provide the same defences that Microsoft's own services use.
- Standard: provides extra mitigation capabilities that are tuned specifically to Mcirosfot Azure Virtual Network resources. It is simple to enable and does not require any application chabnges. Protection policies are tuned through dedicated traffic monitoring and machine

learning algorithms - applied to public IP addresses associated with resources deployed in virtual networks such as Azure Load Balancer and Application gateway.

Azure Firewall

Is a managed, cloud-based network security device that protects your Azure virtual network (Vnet) resources from attackers. Although it can be deployed on any virtual network it is best to use on a centralised virtual network.

Key features

- Built in high availability and availability zones: HA built in so there's nothing to configure. Azure Firewall can be configured to span multiple availability zones.
- Network and application level filtering: Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic
- Outbound SNAT and inbound DNAT: Translate the private IP address of networ kresources to an Azure public IP address (source network address translation) to identify and allow traffic originating from the virtual network to internet destinations. Inbound traffic to the firewall public IP is translated (Destination Network Address Translation) and filtered to the private IP addressses of resources.
- Multiple public IP addresses: can be associated with Azure Firewall
- Threat intelligence: can be enabled on your firewall to alert and deny traffic from/to known malicious IP addresses and domains
- Integration with Azure Monitor: Integrated with Azure Monitor to enable collecting, analysing and acting on telemetry from logs.

Web Application Firewall

Web applications are increasingly targeted by malicious attacks that exploit common vulnerabilities. Web Application Firewall (WAF) provides centralised protection of your web applications from tcommon exploits and vulns. to make security management simpler. This improves response times and alows patching in one place.

Network Segmentation

Main reasons for network segmentation are:

- Ability to group related assets

- Isolation of resources
- Governance policies set by the organisation

Network segmentation also supports the Zero Trust model and a layered approach to security that is part of a defence in depth strategy.

Azure Virtual Network

VNet is the fundamental building block for your orgs private network in Azure. VNet is similar to a traditional network that you would operate in your own datacenter but has additional benefits like scale, availability and isolation.

Azure Network Security Groups

Network Security Groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network e.g. a virtual machine. An NSG consists of rules that define how traffic is filtered.

Inbound and outbound security rules

NSGs are made up of inbound and outbound security rules, which are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic.

What is the difference between NSGs and Azure Firewall?

Azure Firewall service compliments the NSG functionality. NSG provide distributed network layer traffic filtering to limit traffic to within virutal networks in each subscription. Azure Firewall is fully stateful and provides network and application level protection accross different subscriptions and virtual networks.

Azure Bastion and JIT Access

Azure Bastion

A service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The key features are:

- RDP and SSH directly in Azure Portal
- Remote session over TLS and firewall traversal for RDP/SSH
- No Public IP required on the Azure VM required

- No hassle of managing NSGs
- Protection against Port Scanning
- Hardening in once place to protect against zero-day exploits

Just-in-time Access

Allows lock down of inbound traffic to VMs, reducing exposure to attacks whilst providing easy access to connect to VMs when needed.

JIT requires Microsoft Defender for servers to be enabled on the subscription

Ways Azure Encrypts Data

Azure provides many different ways to secure your data, each depending on the service or usage required.

- Azure Storage Service Encryption: helps protect data at rest by automatically encrypting before persisting it to Azure Managed disks, Azure Blob storage, Azure files, or Azure Queue Storage - and decrypts data before retrieval.
- Azure Disk Encryption: helps you encrypt Windows and Linux IaaS virtual machine disks. Uses BitLocker of windows and the dm-crypt feature of Linux.
- Transparent Data Encryption (TDE): protects Azure SQL Database and Azure Data Warehouse against the threat of malicious activity

Azure Key Vault

Azure Key Vault is a centralised cloud service for storing application secrets. Key vault helps control your app secrets by keeping them in one location and providing secure access, permission control, land access logging capabilities. Useful for different scenarios:

- Secrets management: store and tightly control access to tokens, passwords, certificates, API keys and other
- Key management: makes it easier to create and control encryption keys that encrypt your data
- Certificate management: lets you provision, manage, and deploy publich adn private Secure Sockets Layer/ Transport Layer Security (SSL/TLS) certificates for Azure
- Store secrets based by hardware security modules (HSM): can be protected by software or FIPS 140-2 Level 2 validated HSMs