**Networking is a critical component of any cloud infrastructure. Developers need to connect Cloud resources and optimize application performance -- all of which depends on solid network architecture.**

**Microsoft Azure networking offer various capabilities to connect and manage cloud resources.**

**Beyond virtual networks**

**and a number of connectivity options,**

**Azure offers services**

**to monitor and manage traffic, perform load balancing and ensure secure user connections.**

**A reliable cloud network provides centralized management which allows to deliver faster content in a secured way.**

**Now we will discuss Why does performance of Web application matter?**

Whether it’s the bank, in restaurant, in traffic, nobody likes to wait.

The same is true with online web application – a website’s load and response times have a major impact on the user experience.

Some of the web’s busiest sites have found the impact to be significant:

Google found that a 500ms slowdown equals 20% decrease in ad revenue.

Amazon finds a 100ms slowdown - can decrease 1% in revenue.

Yahoo! found that a 400ms improvement in load time translated to a 9% increase in traffic.

These findings show how much speed can impact the bottom line. More speed means more visits, longer visits, and more revenue. WebSite speed is not an abstraction that only few care about…. –

According to one survey:

**27% of users**

**Say that**

**visiting a slow site**

**makes them more likely to visit a**

**competitor!**

Speed & performance really…. matters! it has become a significant factor in how well your site sells your services and represents your brand…..

<https://www.fengqi.asia/wp-content/uploads/2015/04/EdgeCast_Speed_Matters.pdf>

**How can we speed up Sitecore Managed Cloud instances?**

Sitecore offers the customers to integrate their application with Azure CDN. CDN servers are usually distributed across different physical locations. Having distributed nodes across different geographical locations increases availability. The CDN servers also store cached contents and act as a mediator between the origin of the web application and clients.

If your Sitecore application is heavy on content from the Sitecore media library, you can offload your Sitecore instances by allowing images to be retrieved from a CDN and helps to reduce the load on application. This reduction in load can help to increase the performance and scalability of the application, as well as minimizing hosting costs by reducing the processing resources required to achieve a specific level of performance and availability.

It is easy to integrate & deploy CDN with Sitecore existing environment. CDN can deployed via Marketplace or ARM templates in Sitecore Managed Cloud.

When a user requests a media item, the CDN responds to the request

by utilizing the closest CDN server to the user.

First, the CDN attempts to use the cache of the CDN server.

If the cache is available and valid, the CDN server responds directly to the user,

otherwise it sends a request to Sitecore for the content.

The CDN server then stores the content in cache and responds to the user.

Sitecore supports the Azure CDN service in its integration with standard Sitecore Managed Cloud topologies. Currently the only Sitecore feature that supports a CDN is the Sitecore Media Library. However, developers can customize the media library to use a CDN for static resources or other assets. For example, instead of using relative URLs to link to .css or .js files , you can use absolute URLs to connect to a CDN endpoint.

In next slide, my colleague Gurveen will discuss more about security and how can we secure Sitecore managed Cloud from cyber attacks?

WAF

Security issues are becoming a day-to-day struggle for online web applications. The number of security attacks occurring each year has been increased. In one of the recent security research suggests that most companies have poor networking infrastructure in place which make them vulnerable to security issues.

There are various technologies available which can mitigate the risk of security attacks. One of the most effective is the Web Application Firewall (WAF). Sitecore also offers and provides support for Azure Application Gateway WAF which provides centralized protection for your web applications. Azure Application Gateway is a web traffic load balancer that provides application layer (OSI level 7) load balancing and includes the Web Application Firewall (WAF).

WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application. The WAF sits on the outside of your network in front of the public side of the web application and monitors incoming traffic which helps protect you from cyber-attacks. It is a useful technology for preventing attacks relating to common cyber-attacks such as SQL injection, brute force attacks, and cross-site scripting (XSS).

Microsoft has released Azure Application Gateway V2 and Web Application Firewall (WAF) V2 which offer significant improvements and additional capabilities to customers for their instances. So let’s discuss new features of WAF v2:

**Scalability:** It allows you to perform scaling of the number of instances on the traffic.

**Static VIP:** The VIP assigned to the Application Gateway can be static which will not change over its lifecycle.

**Header Rewrite:** It allows you to add, remove or update HTTP request and response headers on application gateway.

**Zone redundancy:** It enables application gateway to survive zonal failures which allows increasing the resilience of applications.

**Improved Performance:** Improvement in performance during the provisioning and during the configuration update activities.

**Cost:** V2 SKU may work out to be overall cheaper for you relative to V1 SKU.

Now Sitecore is also supporting WAF v2. In case you have WAF v1 then you can raise request to migrate WAF v1 to WAF v2, Sitecore will be responsible to migrate your existing WAF configuration to WAF v2.

Front Door:

There are several services available within Microsoft Azure that focus on traffic management and load balancing workloads. Azure Front Door is another member of Azure load balancers and traffic routers which provides a great service for commercial web sites with more complex topology, fault tolerance or geo-distribution.

Azure Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure.

1. AFD uses Anycast protocol & Split TCP which accelerate application performance.

2. AFD uses reverse proxy which provides faster failover support.

3. It allows URL-based routing.

4. It offers Multiple-site hosting which means you can have two different domains www.abc.com and www.xyz.com configured on the same Front Door.

5. Session affinity: Useful to keep a user session on the same application backend.

6. It provides TLS protocol termination (SSL offload) which means it take load off from the Web Front Ends, which do not have to encrypt or decrypt the request.

7. It provides features like Caching & WAF.

8. Allows URL rewrite feature.

9. It supports IPv6 & HTTP/2 traffic

In the past, one would need to use three Azure services to meet these requirements: a combination of Azure Traffic Manager, Content Delivery Manager (CDN) and Web Application Firewall. Let’s assume we have Sitecore Managed Cloud in two different regions, then we might need CDN for caching,

WAF for security and Traffic manager for global traffic distribution.

Just imagine other ways to build up something like this on Azure. It would be complex work and I am sure it will be more expensive. Delivering this functionality can now be simplified by using Azure Front Door Service, which delivers all those Azure services into one unified solution.

I was surprised how easy it is to get Azure Front Door up and running. It took just few hours to integrate with Sitecore Managed Cloud. WAF works well and stops most of malicious requests. I think for global critical sites Azure Front Door is perfect choice. With the help of AFD, we can

monitor and manage traffic, perform load balancing, and ensure secure user connections for Sitecore managed Cloud.

Now let’s have a quick look into different azure load balancers:

AFD & Traffic Manager are distributing traffic globally while Application gateway & load balancer distribute regionally.

AFD & Application gateway uses reverse proxy to route traffic. TM uses DNS routing

and load balancer provides network level distribution.

The features like SSL offloading & Web application Firewall

is available in AFD & application gateway while these features are not available in TM & Load balancer.

One additional benefit of AFD is ….it also supports Caching while no other load balancer supports caching.

When we compare Azure front door and Azure CDN capabilities,

We found that the performance of caching of both the services are quite same. AFD is not just a CDN but it also has more features. Hence, I would recommend if your goal is to use AFD as a content delivery network, then Azure CDN makes more sense.