MANAGING ADMITANCE TO AZURE-LAND

TONY BJERSTEDT, CISSP, AZURE CERTIFIED SA, AWS CSAA

AGENDA

The CIA Triad

OSI Network Model Refresher

- DNS Routing
- Layer 4 Routing
- Layer 7 Routing

Azure Tools

- Traffic Manager
- Load Balancer
- App Gateway
- Azure Front Door
- WAF

Third Party Tools

- NGINX
- CloudFlare

ABOUT ME

Email:
tony@bjerstedttechnologies.com
anthony.bjerstedt@sogeti.com

LinkedIn: linkedin.com/in/tbjerstedt
Twitter: @tbjerstedt

sogeti
Part of Capgemini

CISSP®

Microsoft CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

aws certified
Solutions Architect
Associate

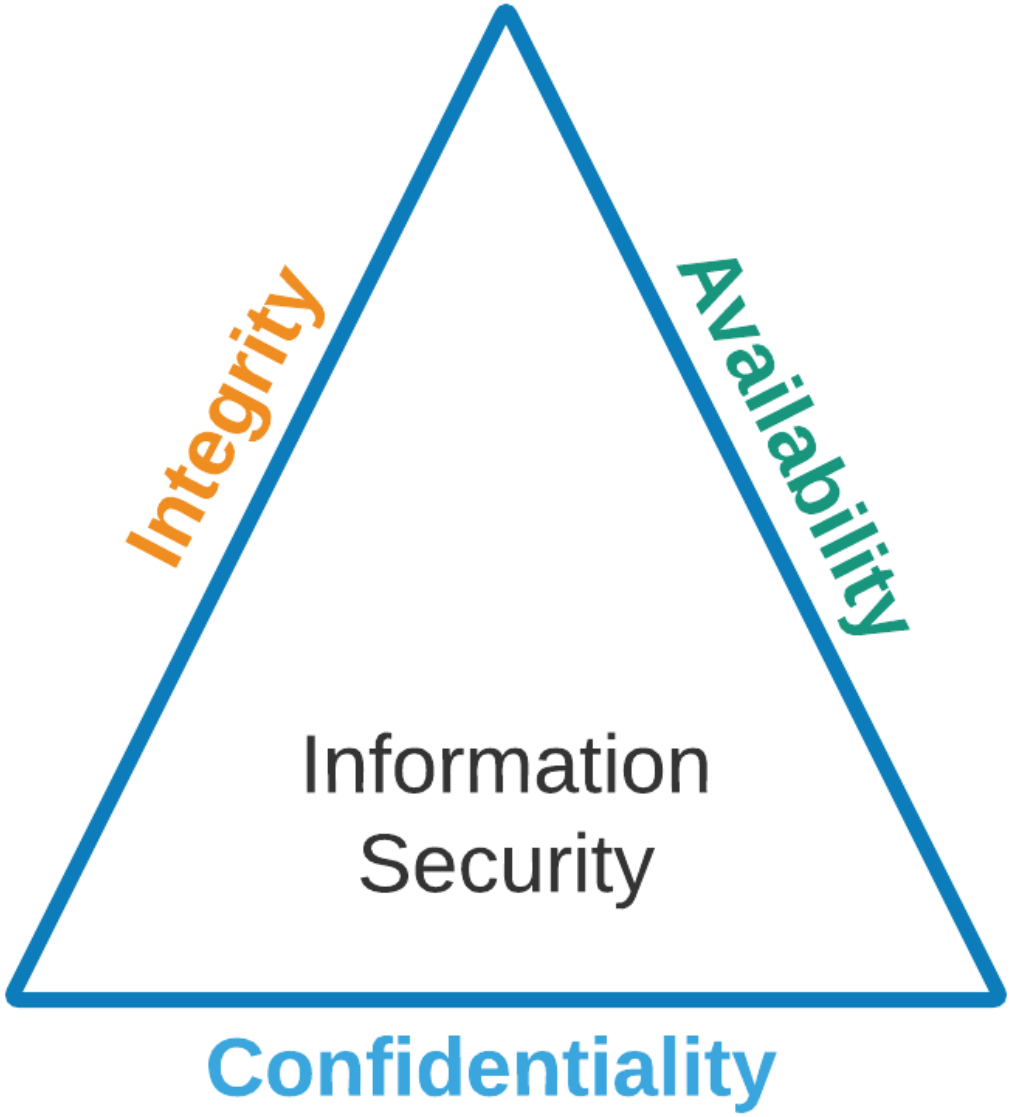
TOASTMASTERS INTERNATIONAL

AEA
Association of Enterprise Architects
Minnesota Chapter

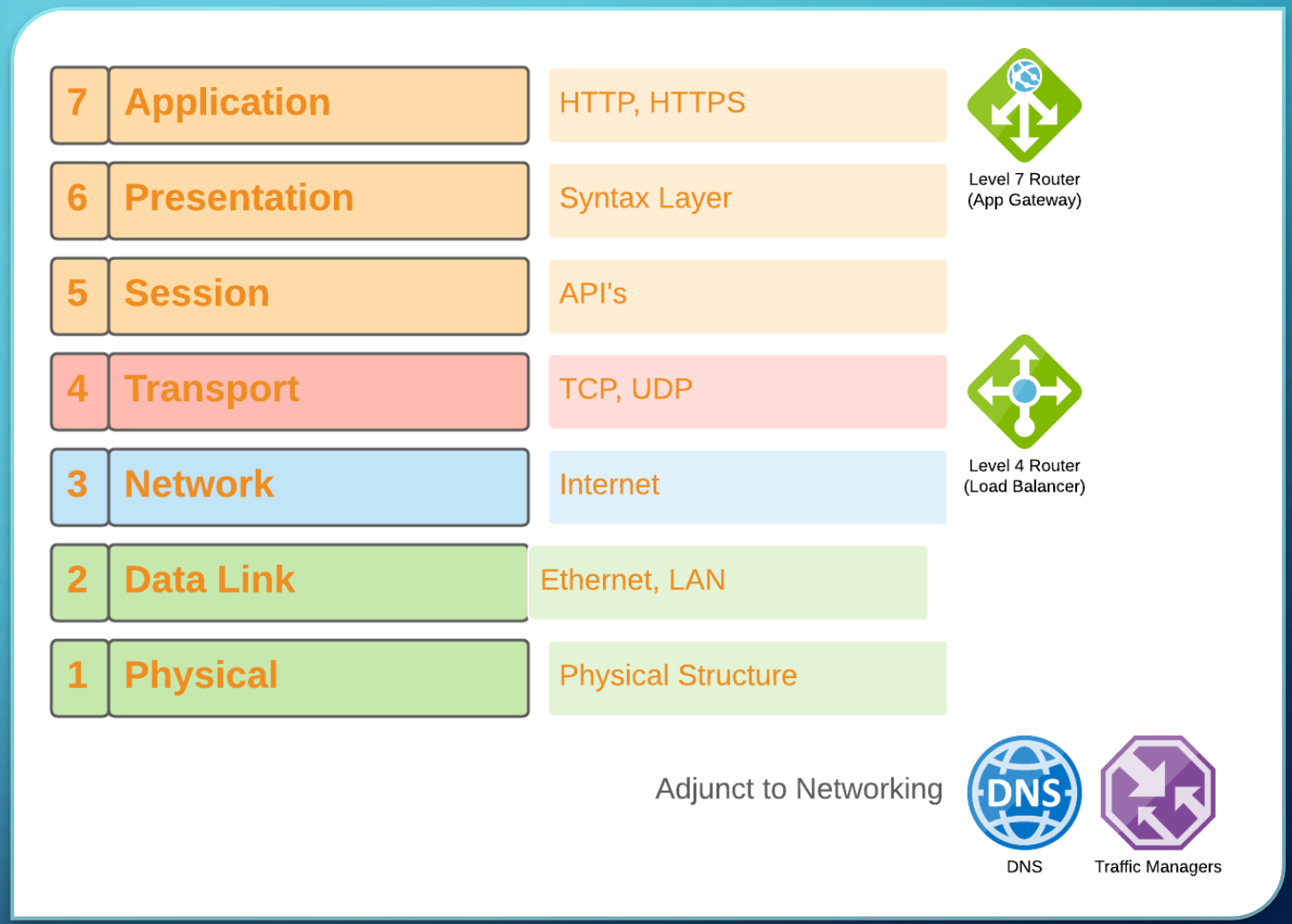
THE IMPORTANCE OF GOOD ARCHITECTURE

When your security gate is a ladder

THE CIA TRIAD



OSI NETWORKING MODEL



LAYER 4 ROUTING

Entire request is opaque

- URL Path not visible
- Headers not visible

Back end handles

- HTTPS
- Authentication

Use for

- Simple sites
- Single, uniform backend
- Lower security needed
- Main concern is load balancing

SSL Certificate installed everywhere

AZURE LOAD BALANCER

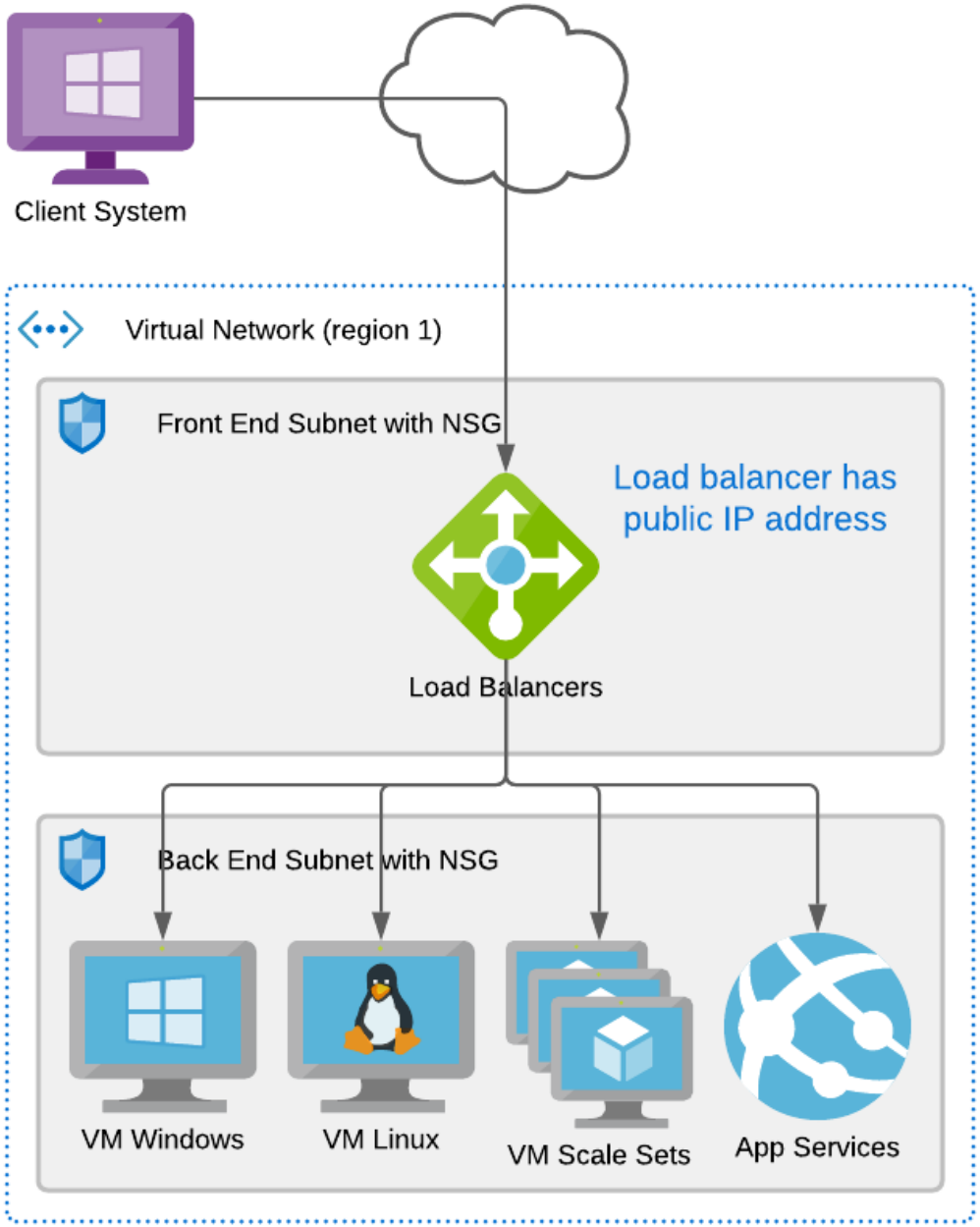
Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

AZURE LOAD BALANCER

Routes all messages to single pool of uniform back end services

AKS Ingress is **not** integrated

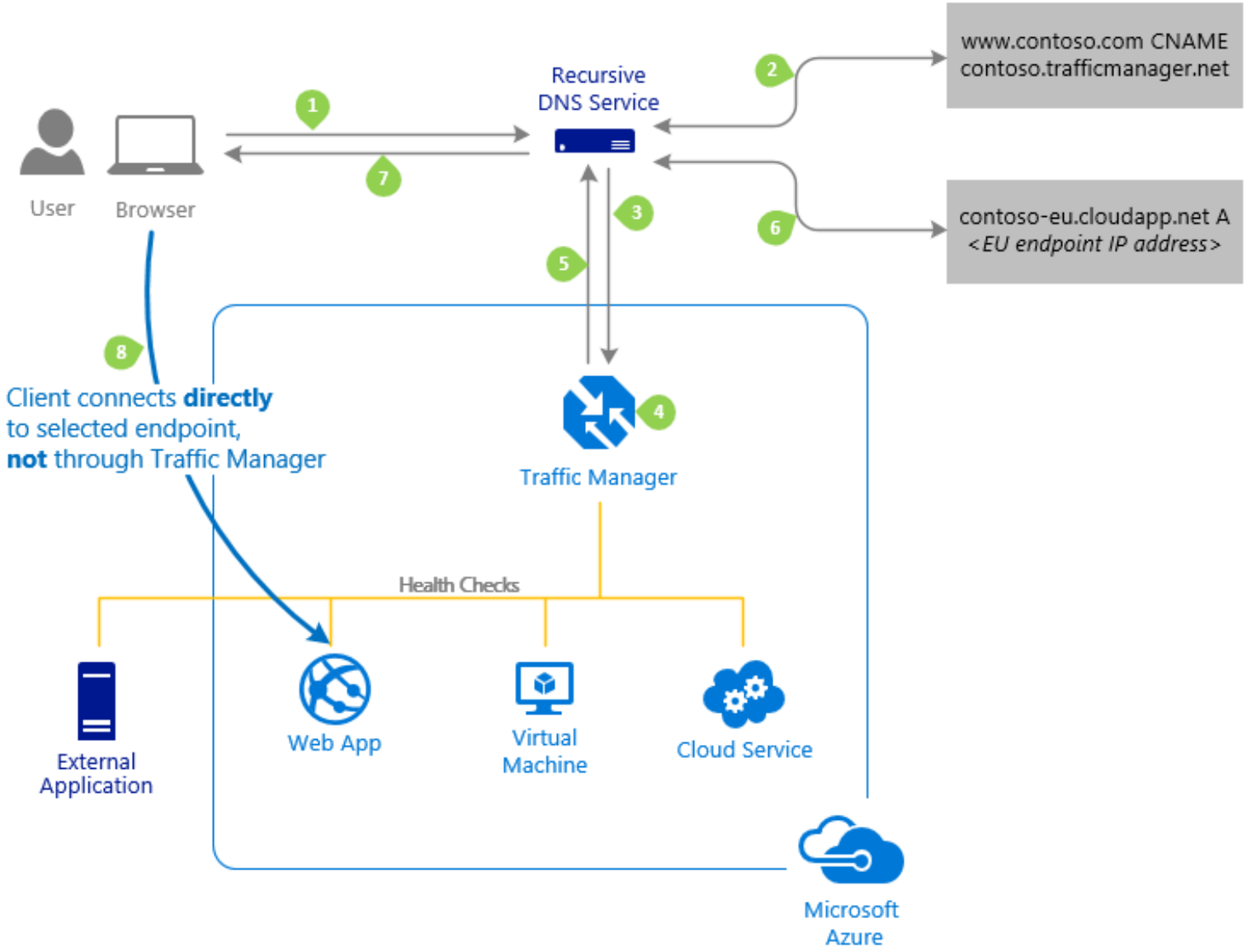


TRAFFIC MANAGER

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

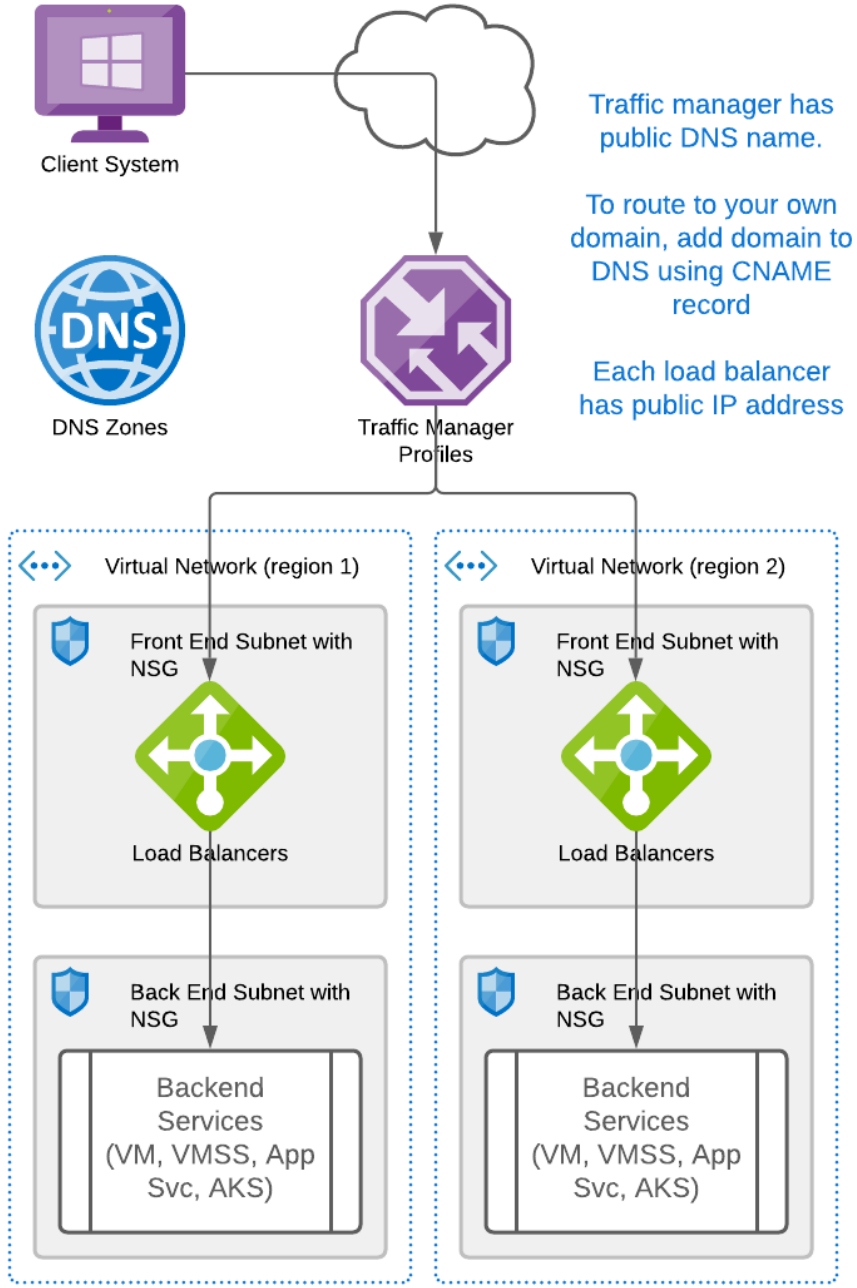
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

TRAFFIC MANAGER FLOW



https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works

MULTI-REGION LOAD BALANCER



LAYER 7 ROUTERS

- Router can handle SSL
- Router can handle certificates
- Router can handle authentication
- Router has full visibility
  - Router can use URL Path
  - Router can use headers
- WAF Support

Use for

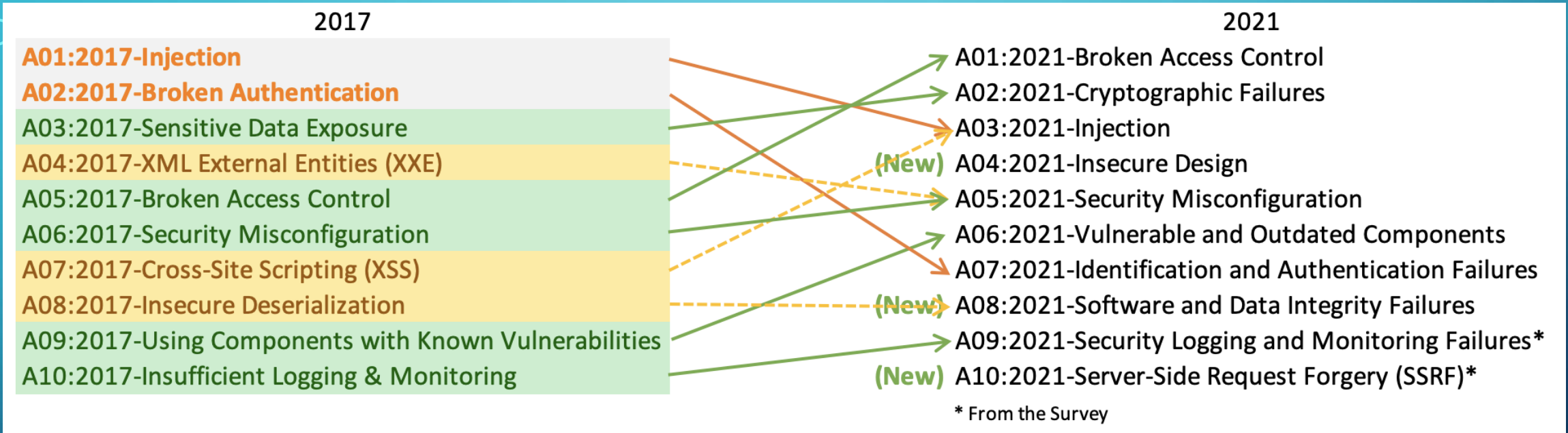
- Complex sites
- Multiple back ends.
  - Image storage
  - Application Servers

WAF (WEB APPLICATION FIREWALL)

"A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors."

https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

OWASP TOP 10



https://owasp.org/Top10/

AZURE APPLICATION GATEWAY

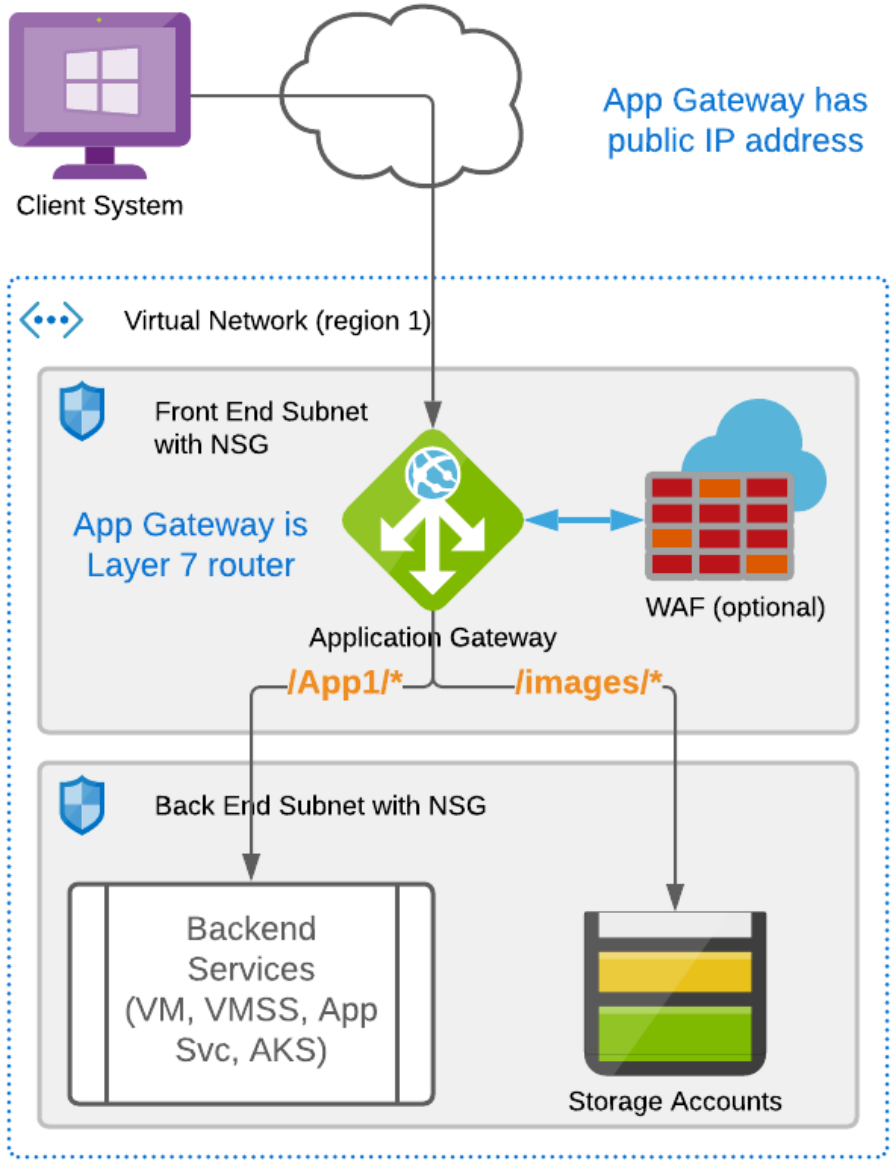
Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.

https://docs.microsoft.com/en-us/azure/application-gateway/overview

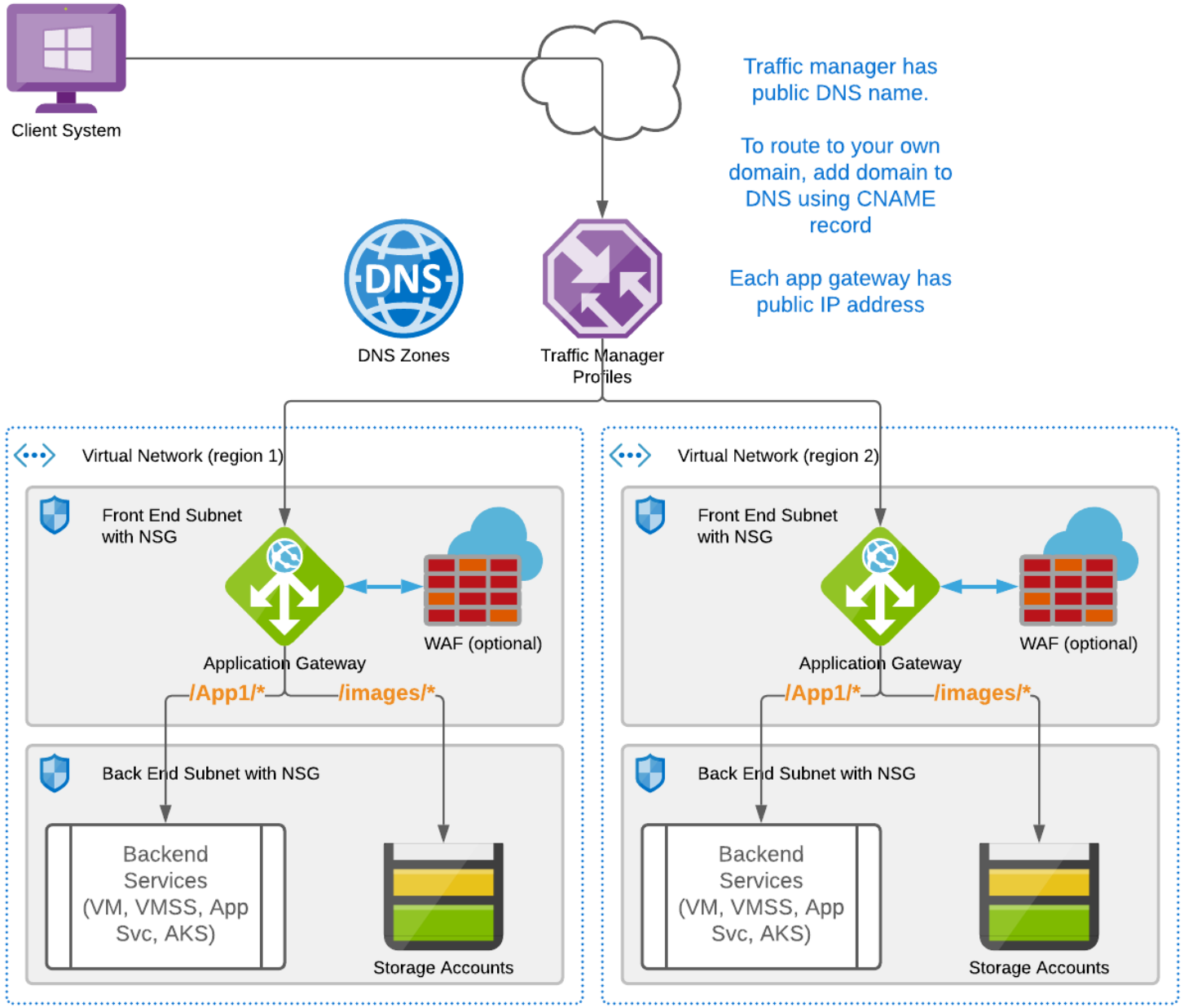
APPLICATION GATEWAY

- High traffic support
- Routing
  - Multiple site hosting
  - URL and Headers
  - Rewrite headers/URL
- SSL
- Ingress for AKS
- WebSockets



Multiple backend applications and storage accounts can be used

MULTI-REGION APP GATEWAY



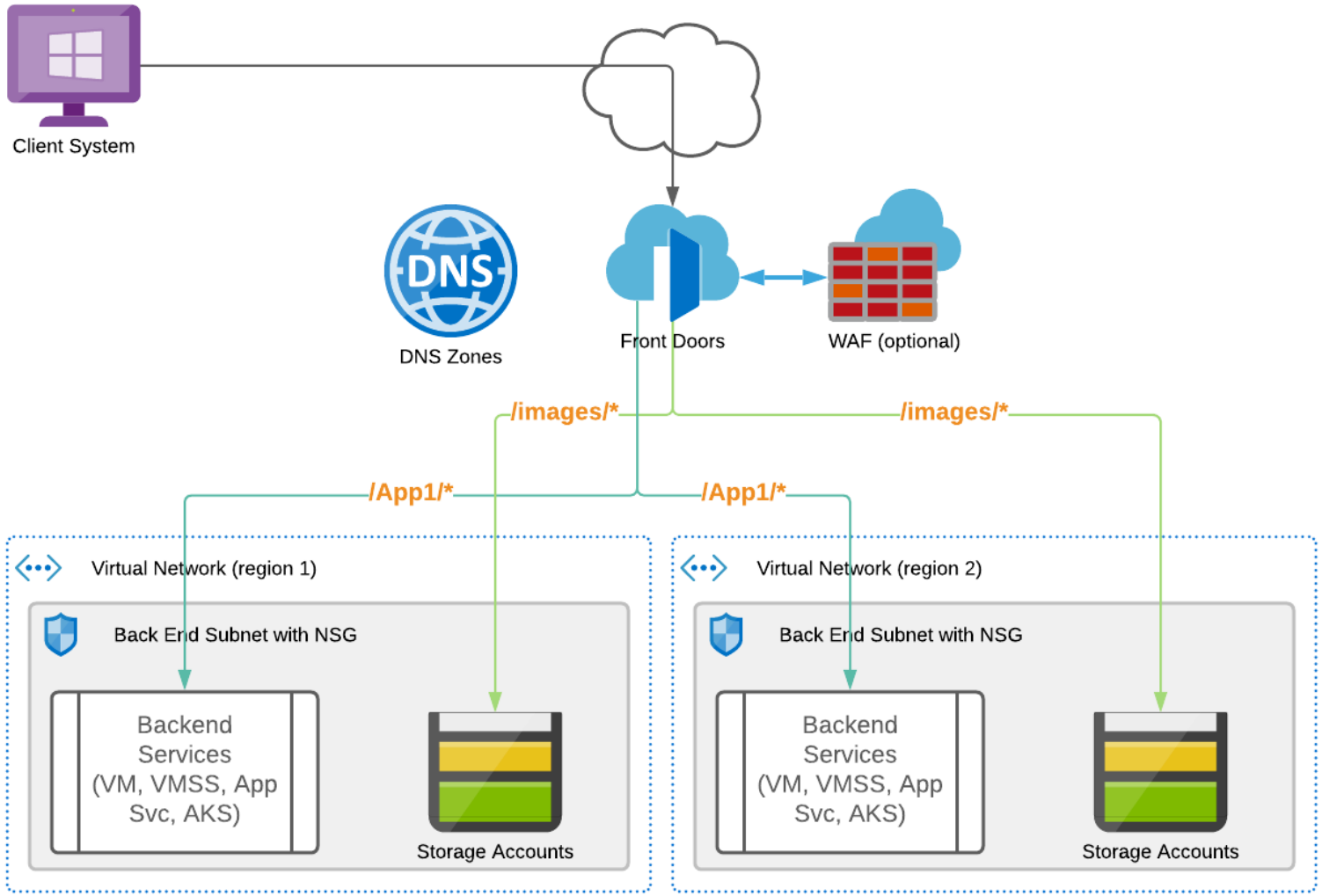
AZURE FRONT DOOR

Azure Front Door is a secure cloud CDN service that cyber security teams can use to accelerate content delivery while protecting apps, APIs, and websites from cyberthreats. It combines intelligent threat protection and modern CDN technology in a tightly integrated service that's easy to setup, deploy and manage.

https://redmondmag.com/articles/2021/02/18/azure-front-door-and-azure-firewall.aspx

AZURE FRONT DOOR

Consider this when you need to support multiple regions at Layer 7.



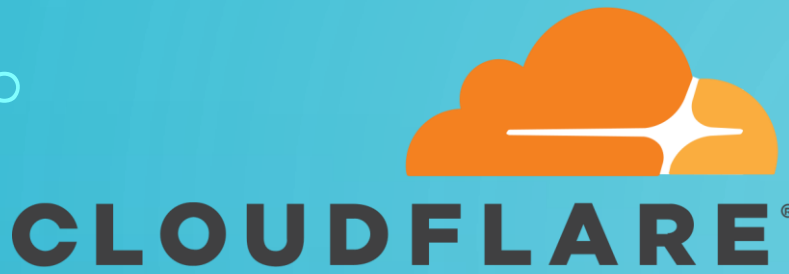
THIRD PARTY TOOLS

NGINX (engine X)

Your All-in-One Load Balancer, Reverse Proxy, API Gateway – and Much More

NGINX is open source software for web serving, reverse proxying, caching, load balancing, media streaming, and more. It started out as a web server designed for maximum performance and stability. In addition to its HTTP server capabilities, NGINX can also function as a proxy server for email (IMAP, POP3, and SMTP) and a reverse proxy and load balancer for HTTP, TCP, and UDP servers.

https://www.nginx.com/resources/glossary/nginx/
https://www.nginx.com/products/nginx/



Cloudflare is a global network designed to make everything you connect to the Internet secure, private, fast, and reliable.

https://www.cloudflare.com/what-is-cloudflare/

- Global Network
- Layer 7 WAF and Routing
- DDoS Protection
- CDN capabilities

OTHER CONSIDERATIONS

Maintain Zero Trust

Use:

- HTTPS inside you VNet (mutual certificate authentication)
- Whitelist Client IP
  - Many Azure Services allow public endpoints, lock then down

SUMMARY

- Many ways to secure entry
  - DNS vs Layer 4 vs Layer 7 vs CDN
  - Azure internal vs Third Party
- Which to use when – it depends
  - Your Use Case
  - Cost vs Benefit

UPCOMING EVENTS

AEA Minnesota:

Pivoting in the Noise: Event-Driven Architecture

Friday, Oct 15, 2021 10:30 AM – 12:00

MACC 2021: Virtual Conference

Surviving The Crisis: What Changed and What Didn't?

Thursday, Nov 4 2021 (All Day)

(MACC = Midwest Architecture Community Collaboration)