SECR

Software Engineering Conference Russia

November 14-15, 2019. Saint-Petersburg

Using Azure Front Door to deliver fast, scalable and secure web applications

Stamo Petkov

Information Services Plc

Contact

Stamo Petkov

Information services Plc.

Head of Microsoft Technologies department

s.g.petkov@is-bg.net
stamo.petkov@gmail.com

https://github.com/stamo
http://bg.linkedin.com/in/stamopetkov
https://www.facebook.com/stamo.petkov
@stamo_petkov

ИНФОРМАЦИОННО
ОБСЛУЖВАНЕ

SECR

MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSD
App Builder
Earned 2016

MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSA
Web Applications
Earned 2016

MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSE
Cloud Platform and Infrastructure
Earned 2018

MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSA
Windows Server 2012
Earned 2018

MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2019 - 2020

Agenda

- Azure Front Door Service
  - Anycast
  - Split TCP
  - Health probes
  - Caching
  - Architecture
- Azure Front Door application protection
  - Azure web application firewall (WAF)
- Demo
- Summary
- Q&A

Azure Front Door Service

Application Delivery Network

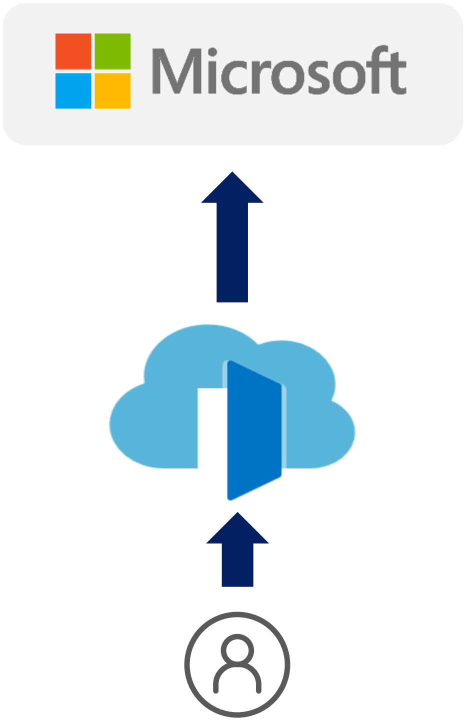
Azure Front Door Service

Build on the "battle-tested" platform used to power reliable and fast global services at Microsoft

"Azure DevOps has onboarded all of its microservices to the Azure Front Door Service over the past year. It provides us with significant benefits in terms of both performance and reliability."

Front Door enables Bing to operate at scale with competitive performance while also scaling agile development across many independent microservices.

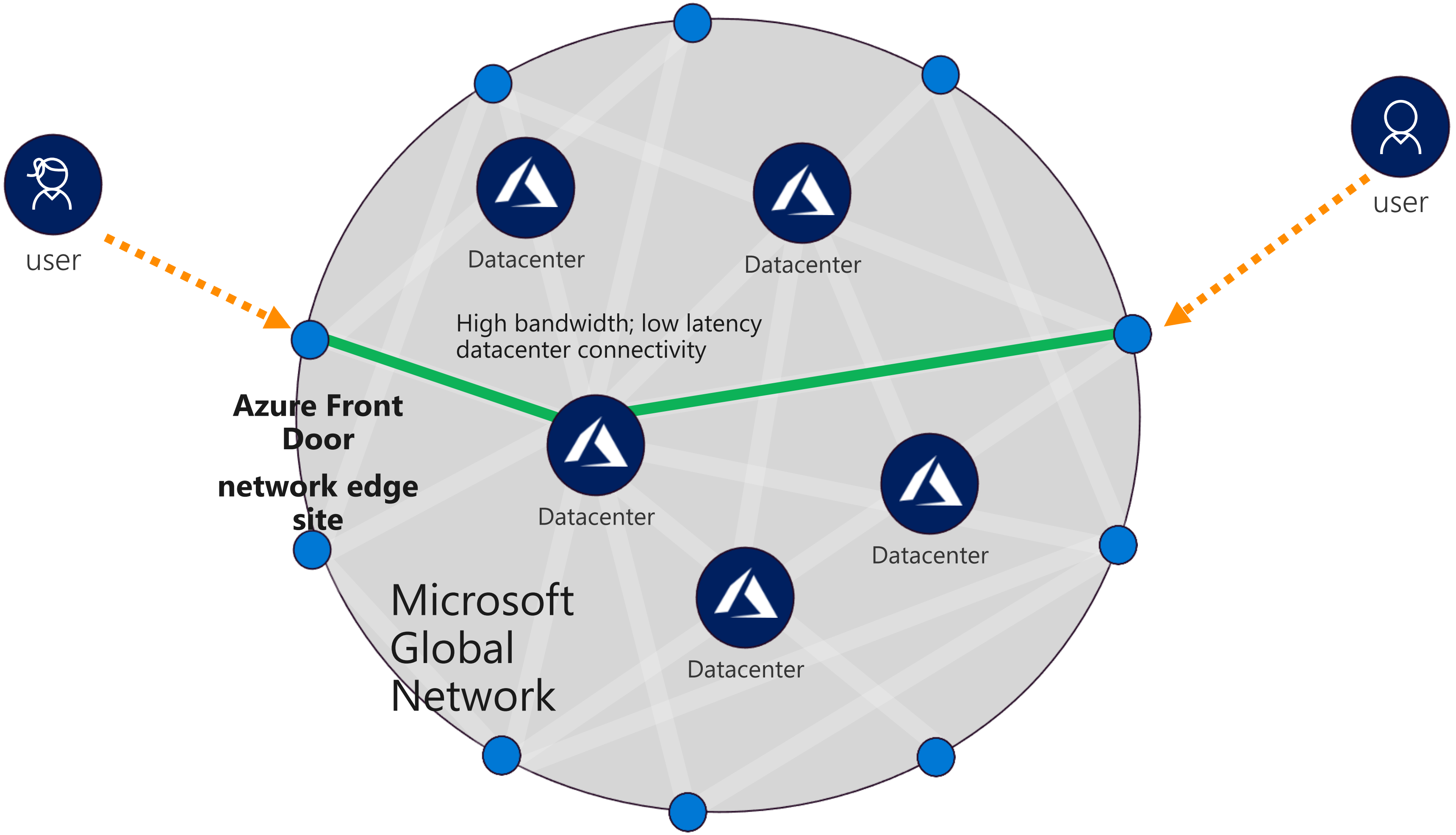
Office 365 Azure Skype Bing
Azure DevOps MSN OneDrive
Xbox Cortana Windows Teams



Selecting the Front Door environment for traffic routing (Anycast)

- Routing to the Azure Front Door environments leverages Anycast for both DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol) traffic, so user traffic will go to the closest environment in terms of network topology (fewest hops)
- Front Door organizes its environments into primary and fallback "rings“
- The outer ring has environments that are closer to users
- The inner ring has environments that can handle the failover for the outer ring environment in case an issue happens
- The outer ring is the preferred target for all traffic, but the inner ring is necessary to handle traffic overflow from the outer ring

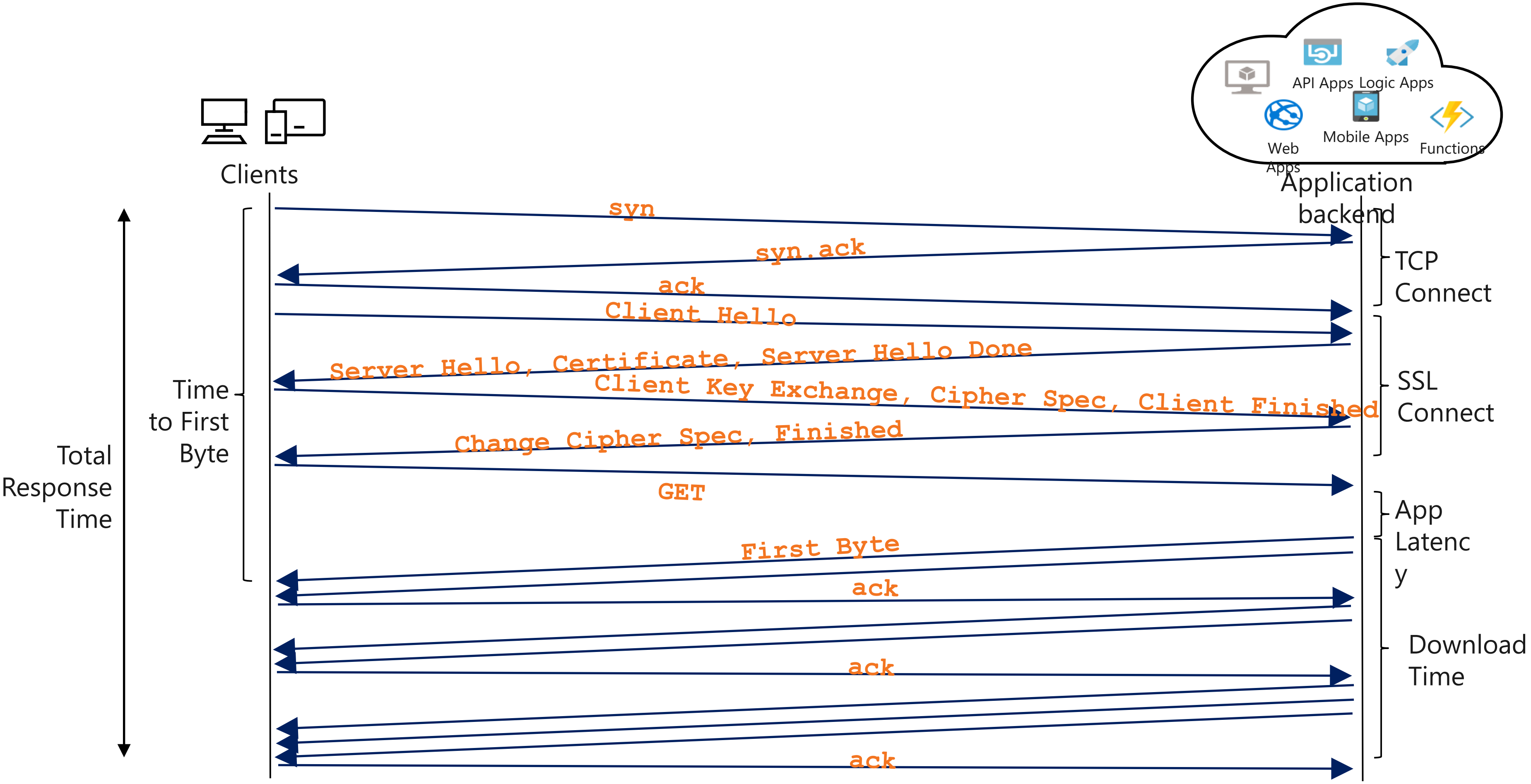
Global application delivery



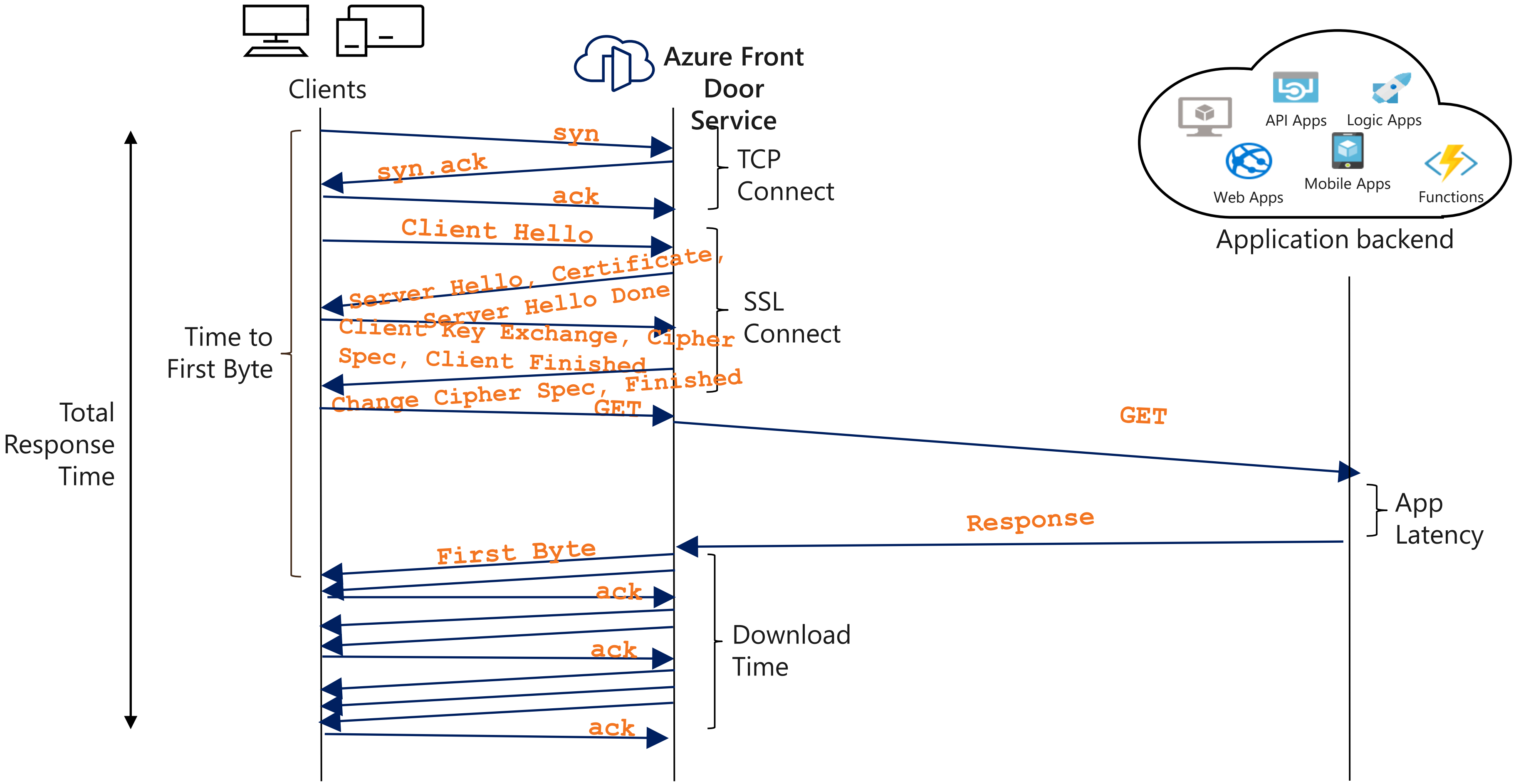
Connecting to Front Door environment

- Split TCP is a technique to reduce latencies and TCP problems by breaking a connection that would incur a high round-trip time into smaller pieces
- One TCP connection with a large round-trip time (RTT) to application backend is split into two TCP connections
- The short connection between the end user and the Front Door environment gets established over three short round trips
- The long connection between the Front Door environment and the backend can be pre-established and reused across multiple end-user calls
- The effect is multiplied when establishing a SSL/TLS (Transport Layer Security) connection as there are more round trips to secure the connection

Connection establishment and response



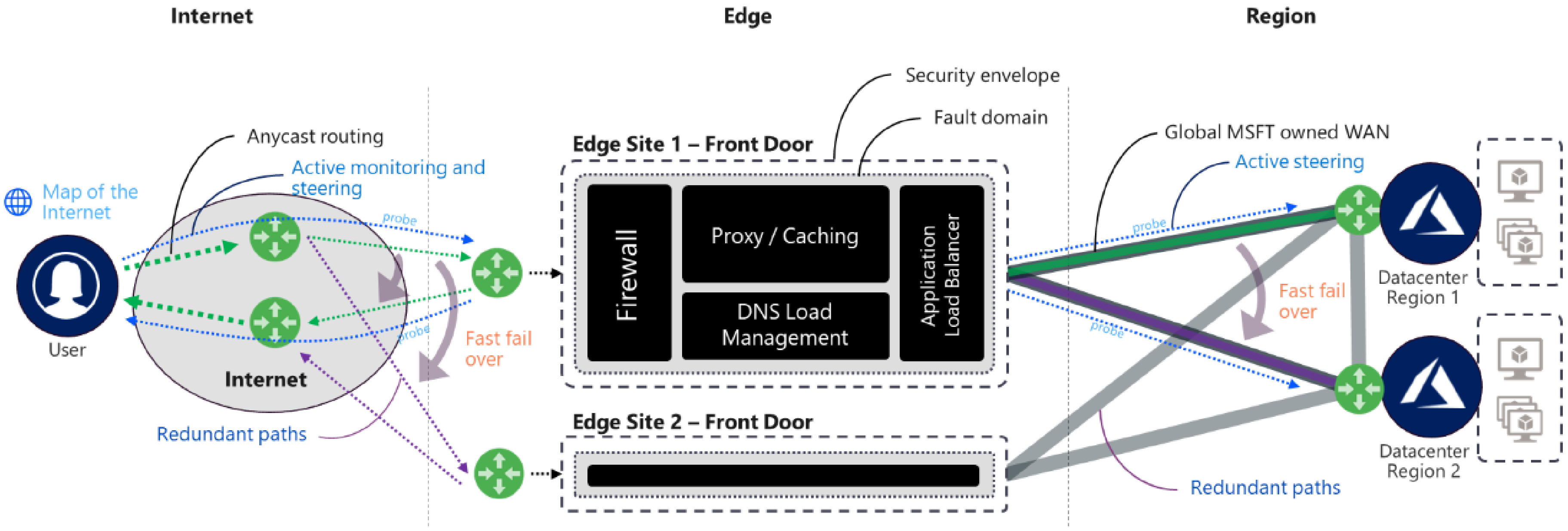
Make your apps faster, reduce backend load



Identifying available backends in the backend pool

- In order to determine the health of each backend, each Front Door environment periodically sends a synthetic HTTP/HTTPS request to each of your configured backends
- Front Door uses responses from these probes to determine the "best" backends to which it should route real client requests
- A 200 OK status code indicates the backend is healthy. Everything else is considered a failure
- Azure Front Door Service uses the same three-step process across all algorithms to determine health
  - Exclude disabled backends
  - Exclude backends that have health probes errors
  - Out of the set of healthy backends in the backend pool, Front Door additionally measures and maintains the latency (round-trip time) for each backend
- If health probes fail for every backend in a backend pool, then Front Door considers all backends healthy and routes traffic in a round robin distribution across all of them

Enterprise grade architecture



Azure Front Door application protection

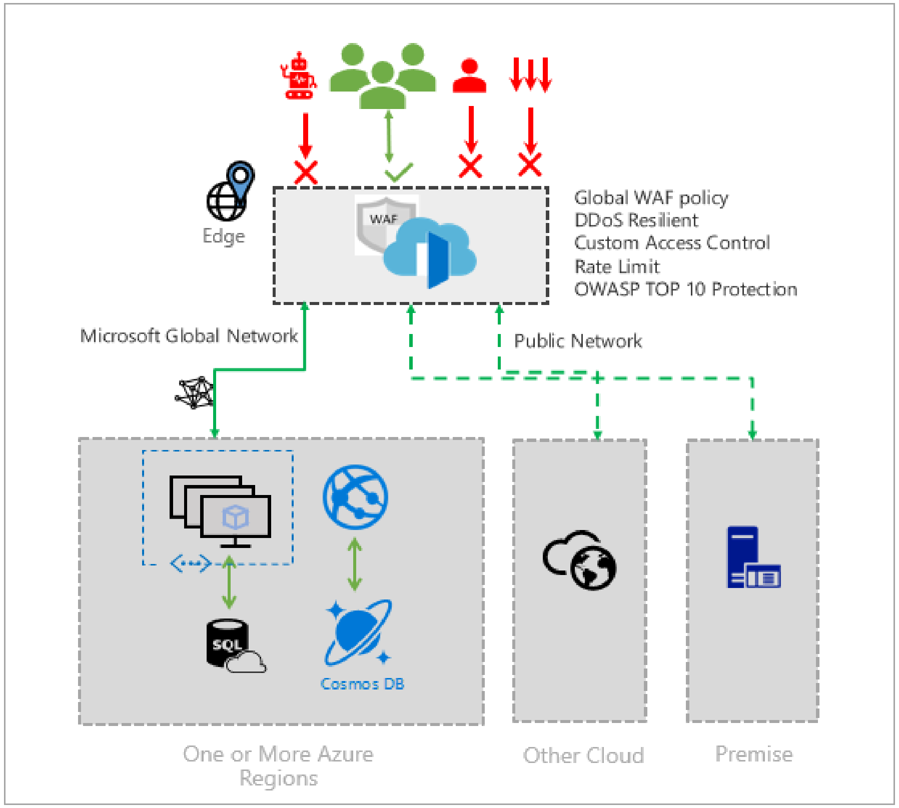
Azure web application firewall (WAF)

Azure Front Door application protection

- Web applications are increasingly the targets of malicious attacks such as denial of service floods, SQL injection attacks, and cross-site scripting attacks
- These malicious attacks may cause service outage and data loss, pose a significant threat to web application owners
- Preventing such attacks in application code can be challenging and may require rigorous maintenance, patching and monitoring at multiple layers of the application topology
- A centralized web application firewall helps make security management much simpler and gives better assurance to application administrators

Azure web application firewall

- WAF for Front Door is a global and centralized solution
- Provides centralized protection for your web applications that are globally delivered using Azure Front Door
- Every incoming request for a WAF enabled web application delivered by Front Door is inspected at the network edge
- Prevents malicious attacks close to the attack sources, before they enter virtual network and offers global protection at scale without sacrificing performance



Azure Front Door application protection

Network DDoS protection

- Built in with platform. Block attacks at Azure edge,
  only allow http(s) workloads to reach web sites behind Azure Front Door

IP blacklists and whitelists

- Configure custom rules to control access based on list of IP addresses

Geo filtering

- Configure custom access control based on client's country code

Flexible actions

- Configure action to allow, block, or log only when a rule is triggered

Custom http(s) access rules

- Configure custom access rules based on matching
  http(s) request parameters including headers, URL,
  and query strings

Rate limiting

- Configure limit on number of web requests allowed
  by a client IP in a one minute duration

Azure managed ruleset

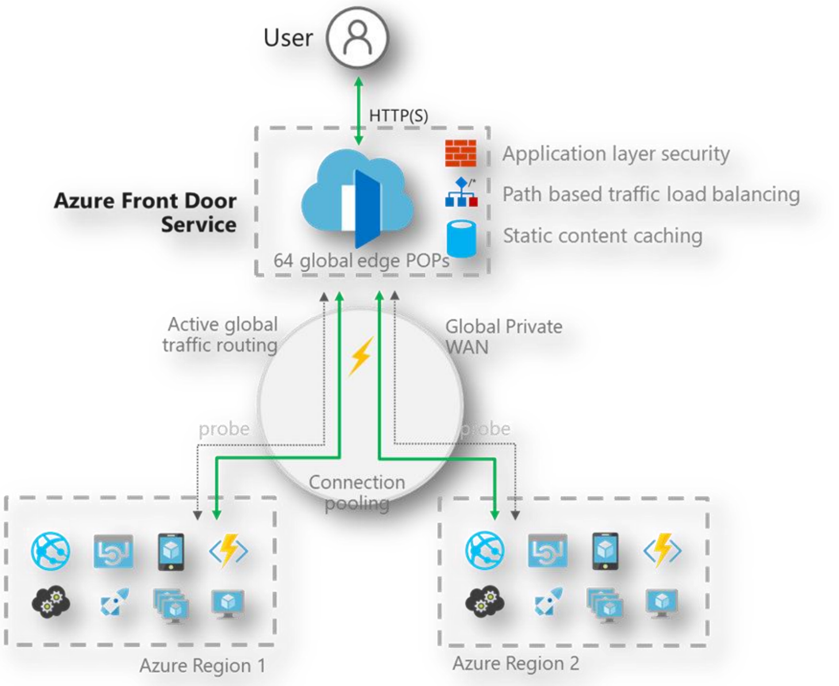
- Enable pre–configured SQL injection
- Cross–site scripting checking on request parameters

Demo

See Azure Front Door service in action

Azure Front Door Service Summary

- SSL offload and application acceleration at the edge close to end users
- Global HTTP load balancing with instant failover
- Actionable insights about your users and back ends
- Web Application Firewall (WAF) and DDoS Protection
- Central control plane for traffic orchestration



Questions & Answers

ИНФОРМАЦИОННО
ОБСЛУЖВАНЕ

SECR