Microsoft

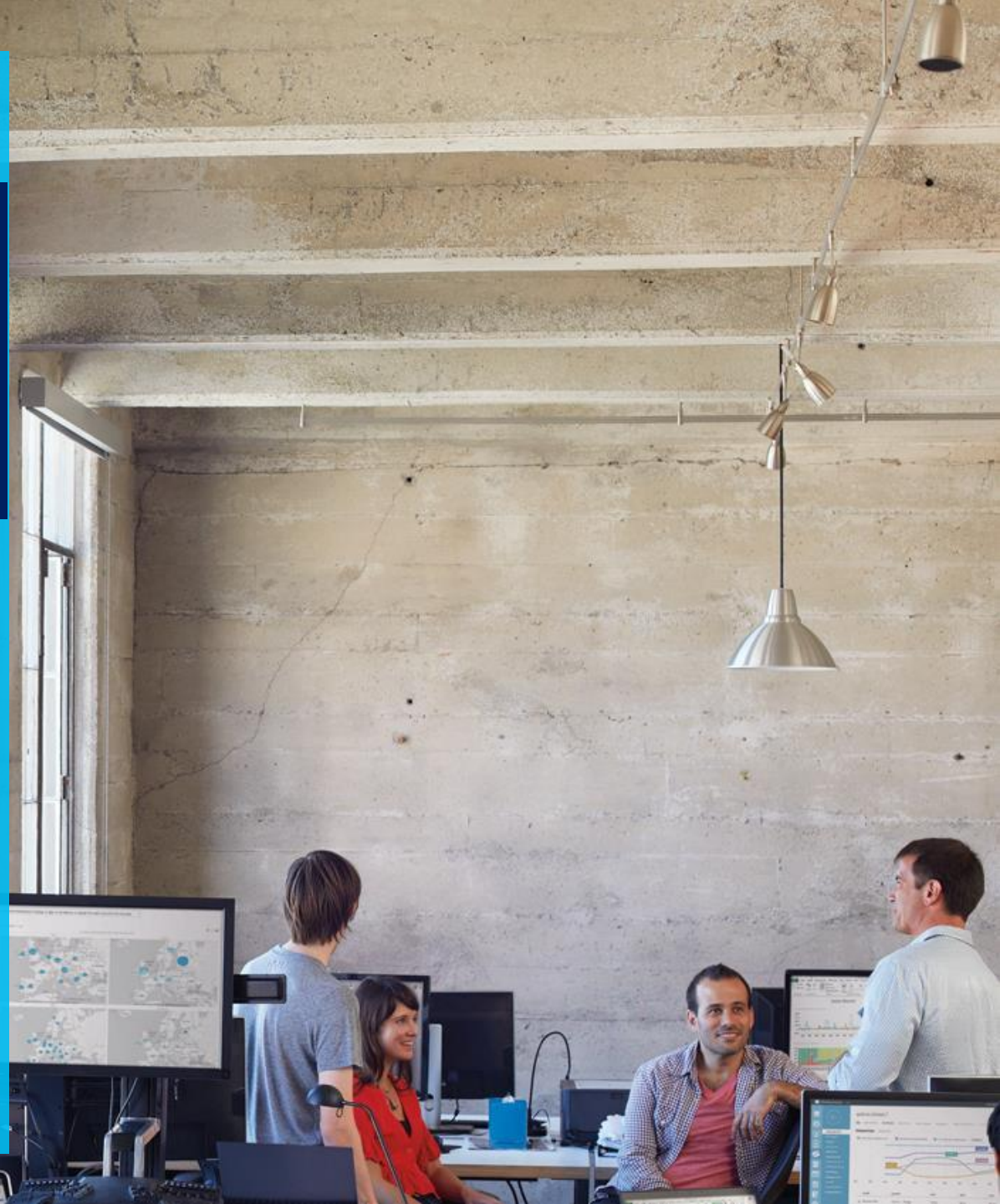
Microsoft Azure Power Lunch

Secure your APIs with Azure Application Gateway and Azure API Management

Series website: http://azurepowerlunch.com/

On-Demand Session Information (Recordings) are available here: Azure Power Lunch YouTube Channel

Date: 25th June, 2021



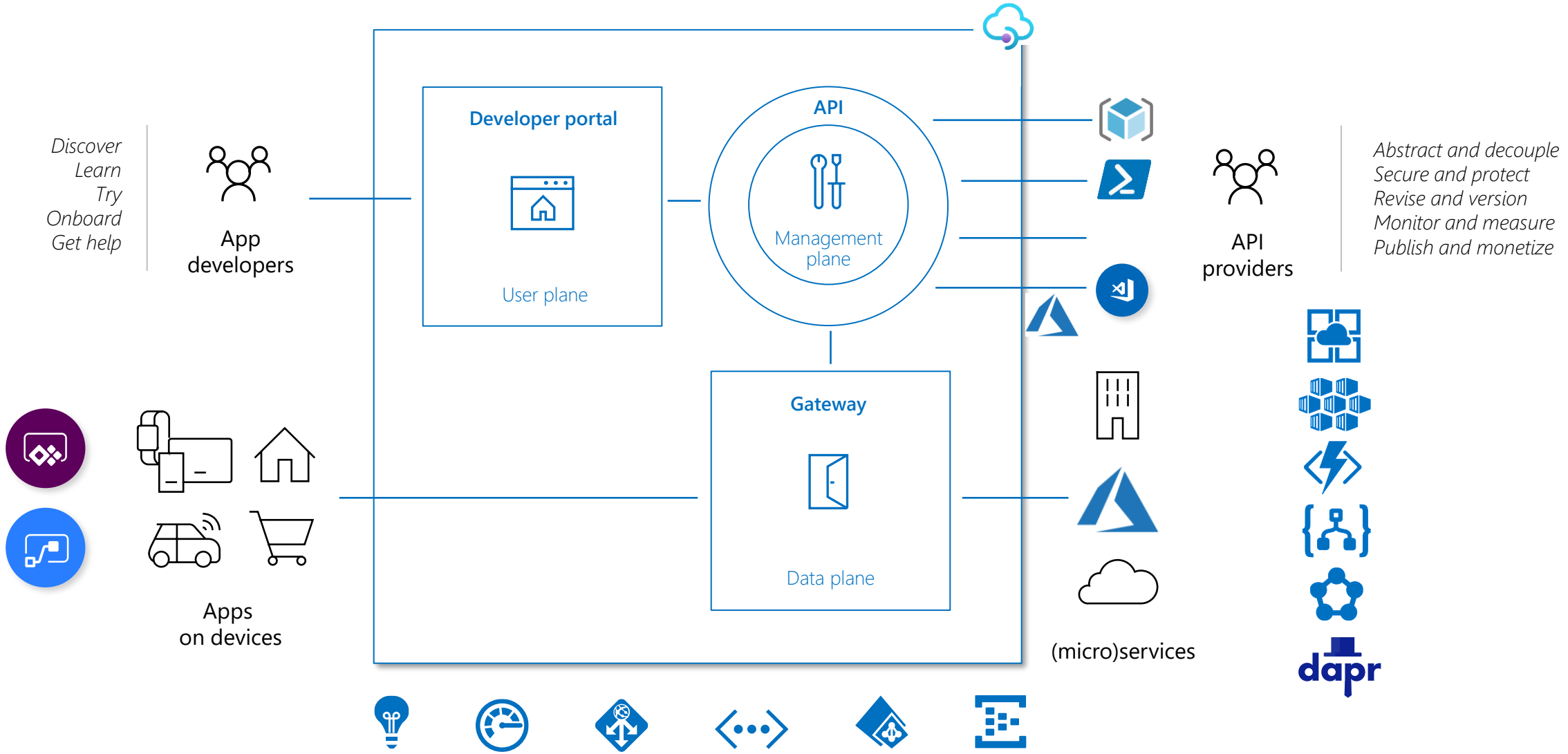
Naveed Zaheer – Cloud Solution Architect

- Been with Microsoft for more than 16 years and in software industry for more than 24 years
- Spent 10+ years with Microsoft Consulting Services in areas such as AppDev, Distributed Applications, SOA and Cloud Applications
- Working with Azure since its inception
- Currently in a Cloud Solution Architect role

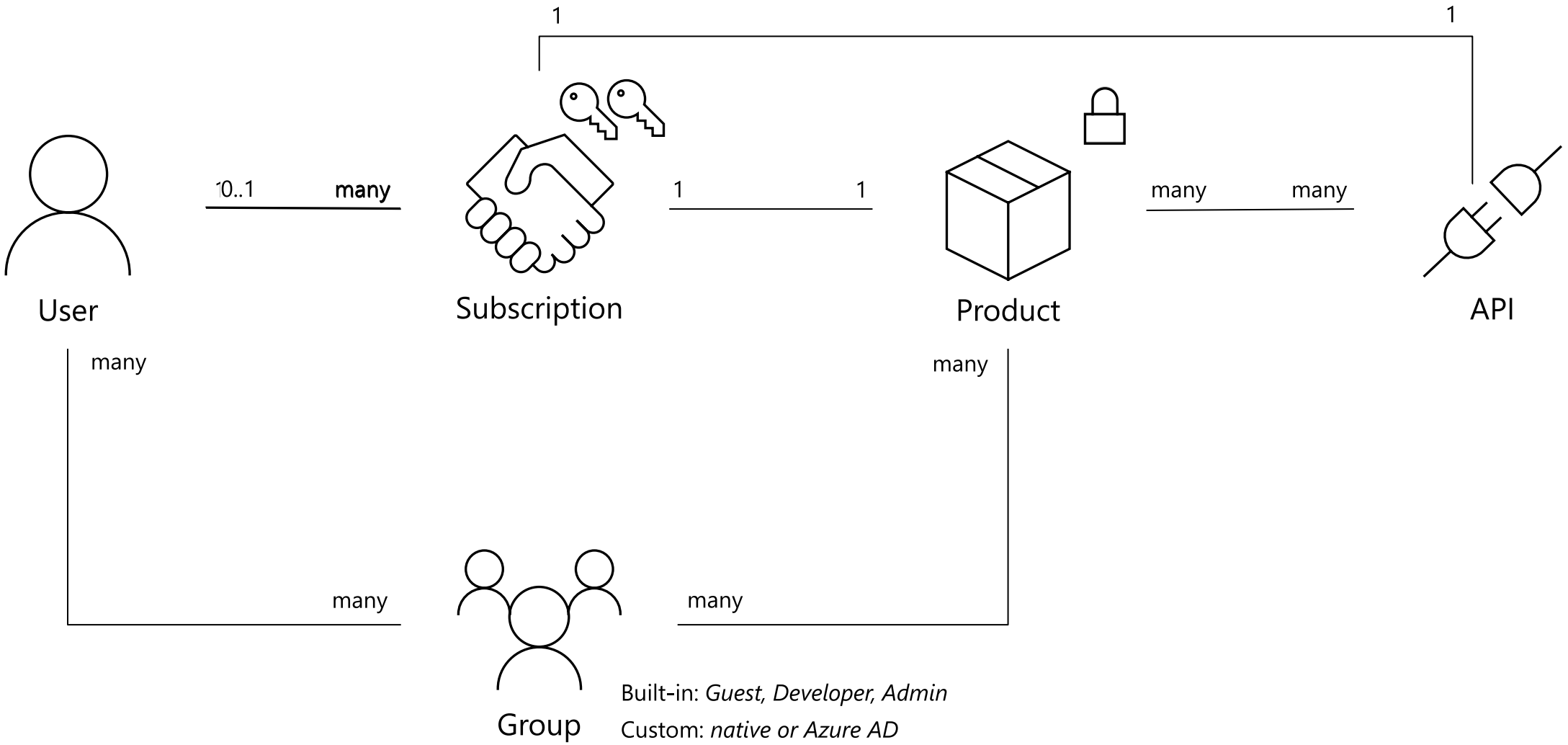
Agenda

- Overview of the services
- Problem Statement
- Reference Architecture
- Demo

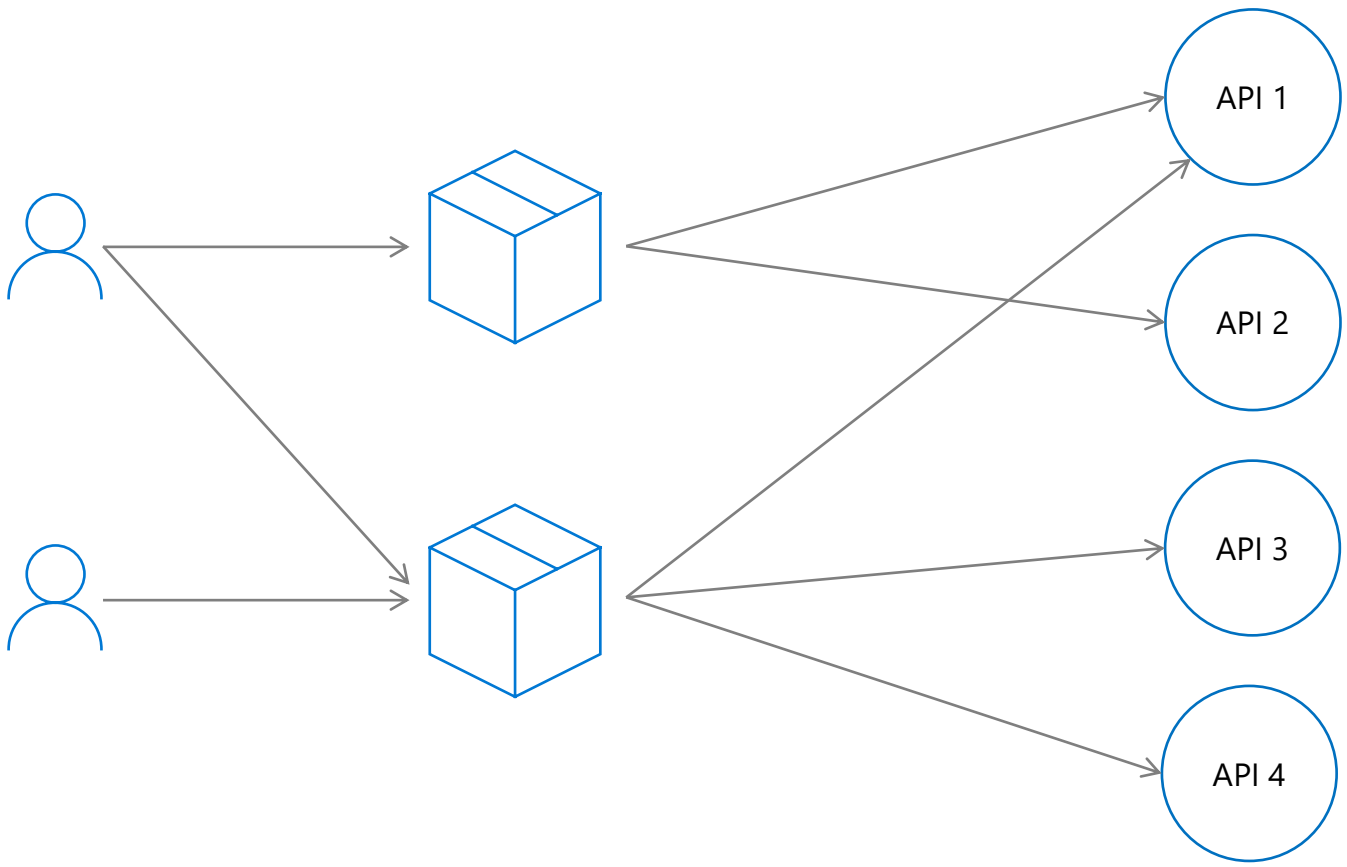
Azure API Management



Users, groups, products, APIs and subscriptions



Expose APIs via products



Developer portal

Browse products and associated APIs
Subscribe to products
Manage subscriptions and keys

Management plane

Manage products and API associations
Define product-scoped policies
Approve and manage subscriptions
Collect and analyze usage data
Monetize access

Gateway

Authenticate API requests with keys
Execute product-scoped policies

Azure App Gateway

- **Build secure, scalable, and highly available web front ends in Azure**

Platform-managed, scalable, and highly available application delivery controller as a service

Centralized SSL offload and SSL policy

99.95 percent uptime service-level agreement for multi-instance deployments

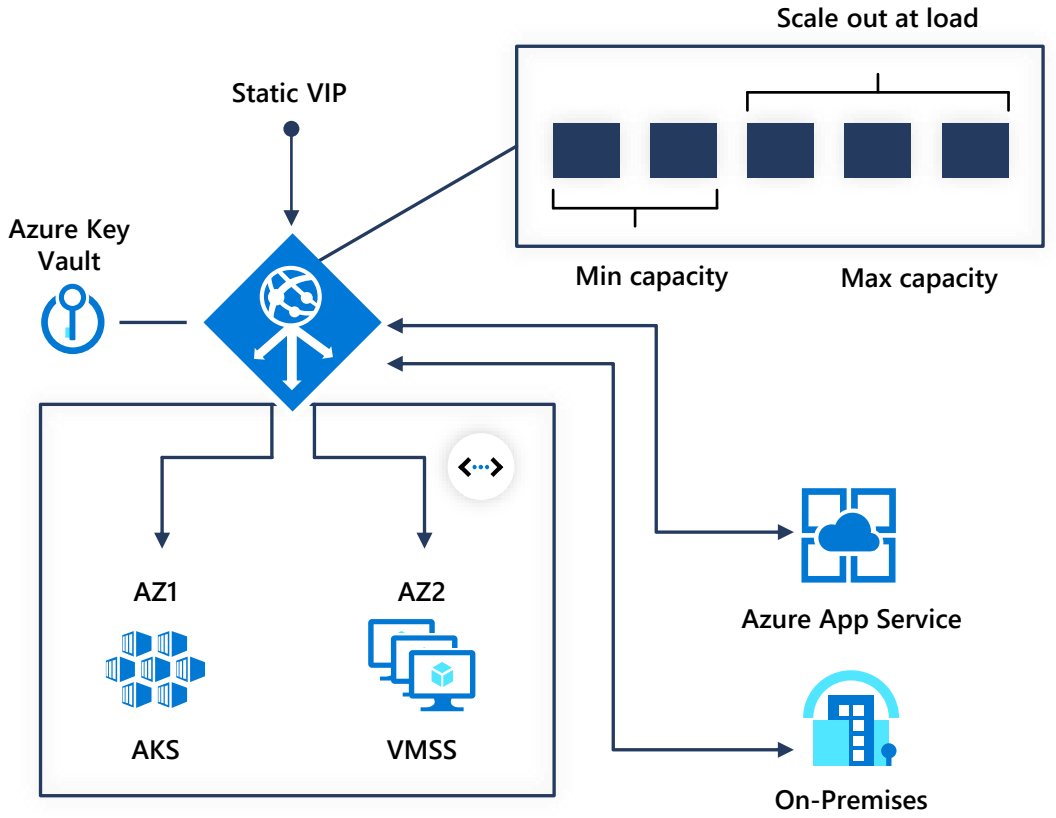
Support for cookie-based session affinity

Customizable layer 7 load-balancing solution

Support for public, private, and hybrid websites

Integrated web application firewall

Management through Azure APIs



Autoscaling, improved performance and faster provisioning

Azure Web Application Firewall

- **A cloud-native web application firewall (WAF) service that provides powerful protection for web apps**

Highly available, autoscaling, fully platform managed

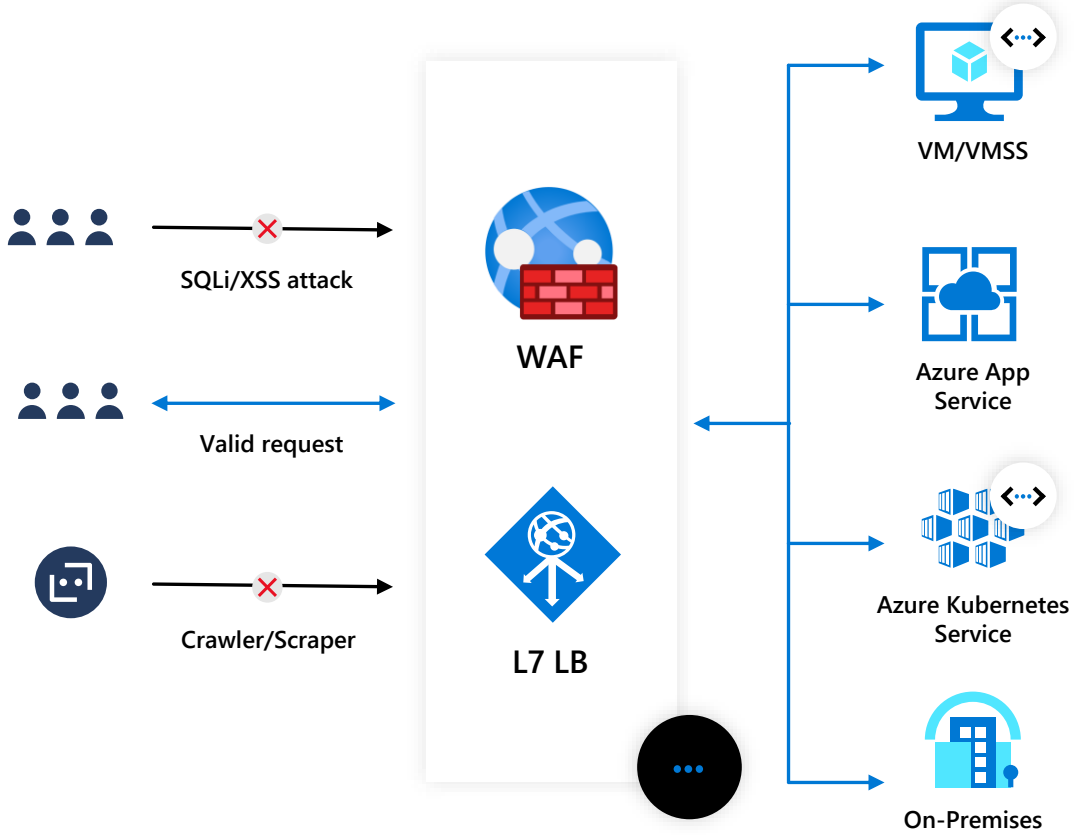
Native in region and intra-VNet/hybrid integration

Support public IP, private IPs, cross region, or on-premises backend pools

OWASP top 10 out of box protection
CRS 2.2.9, CRS 3.0, CRS 3.1 (upcoming)
Custom Rules supported

Rule configurability, exclusion lists, different rules sets, anomaly scoring

Near real time monitoring/alerting with Azure Monitor, Azure Security Center integration, Azure Sentinel integration



Application Gateway & WAF

Problem Statement

- Securing mobile infrastructure
  - Gating access with API keys
  - Preventing DOS attacks by using throttling,
  - Using advanced security policies like JWT token validation.
- Enabling ISV partner ecosystems
  - Offering fast partner onboarding through the developer portal
  - Building an API facade to decouple from internal implementations that are not ripe for partner consumption.
- Running an internal API program
  - Offering a centralized location for the organization to communicate about the availability and latest changes to APIs
  - Gating access based on organizational accounts, all based on a secured channel between the API gateway and the backend.

Step# 1 – Prerequisites

- Create certificates for your custom domain
  - For using self signed certificates in non-production environments, please see this link to know more about how create the root certs
  - Create the self signed certificates for Proxy, Portal and Management endpoints by using this script as reference
  - For certificates in production environment, please content your IT team
- Create the Virtual Network
  - Create a subnet for API Management
  - Create a subnet for App Gateway
  - Create a subnet for Jump server for testing
  - (Optional) Create a subnet for the forwarding proxy & PLS service
- Create an Azure Key Vault to store keys
  - Upload the Proxy, Portal and Management certificates to Key Vault
- Create a User Managed Identity for App Gateway to access Key Vault
  - Give that User Managed Identity access to Key Vault certificates using Access Policies

Step# 2 – Create APIM Instance (Internal VNET)

- Create API Management Instance
  - Use the Subnet/VNET created in the last step
  - Enable System Managed Identity for the APIM instance
    - Give that Managed Identity access to Key Vault certificates using Access Policies
- Create custom domains for
  - Gateway
  - Portal
  - Management
- Setup Private DNS Zone to resolve custom domain names
- For reference, please follow this link:
  - Connect to an internal virtual network using Azure API Management
  - Connect to a virtual network using Azure API Management

Step# 2a – APIM Network Configuration

API Management requires network configuration to support the control of the API Management service.

Custom DNS requirements

- The API Management service depends on several Azure services. When API Management is hosted in a VNET with a custom DNS server, it needs to resolve the hostnames of those Azure services. Otherwise, if using standard Azure DNS resolution will be successful.

Ports (see table)

- You can control inbound and outbound traffic into the subnet in which API Management is deployed by using NSGs. If any of the following ports are unavailable, API Management may not operate properly and may become inaccessible. Blocked ports are another common misconfiguration issue when using API Management with a VNET.

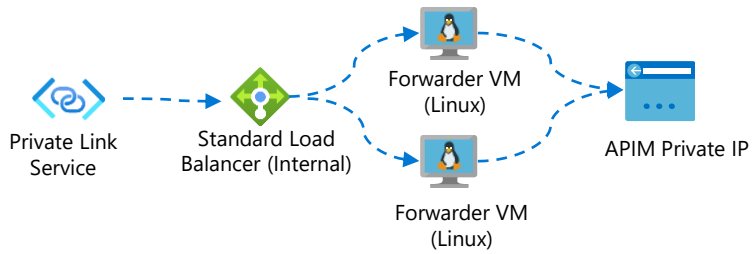
Source / Destination Port(s)	Direction	Transport protocol	Source / Destination	Purpose (*)
* / 3443	Inbound	TCP	ApiManagement / VIRTUAL_NETWORK	Management endpoint for Azure portal and PowerShell
* / 443	Outbound	TCP	VIRTUAL_NETWORK / Storage	Dependency on Azure Storage
* / 443	Outbound	TCP	VIRTUAL_NETWORK / AzureActiveDirectory	Azure Active Directory and Azure KeyVault dependency
* / 1433	Outbound	TCP	VIRTUAL_NETWORK / SQL	Access to Azure SQL endpoints
* / 443	Outbound	TCP	VIRTUAL_NETWORK / AzureKeyVault	Access to Azure KeyVault
* / 5671, 5672, 443	Outbound	TCP	VIRTUAL_NETWORK / EventHub	Dependency for Log to Event Hub policy and monitoring agent
* / 445	Outbound	TCP	VIRTUAL_NETWORK / Storage	Dependency on Azure File Share for GIT
* / 443, 12000	Outbound	TCP	VIRTUAL_NETWORK / AzureCloud	Health and Monitoring Extension
* / 1886, 443	Outbound	TCP	VIRTUAL_NETWORK / AzureMonitor	Publish Diagnostics Logs and Metrics, Resource Health, and Application Insights
* / 25, 587, 25028	Outbound	TCP	VIRTUAL_NETWORK / INTERNET	Connect to SMTP Relay for sending e-mails
* / 6381 - 6383	Inbound & Outbound	TCP	VIRTUAL_NETWORK / VIRTUAL_NETWORK	Access Redis Service for Cache policies between machines
* / 4290	Inbound & Outbound	UDP	VIRTUAL_NETWORK / VIRTUAL_NETWORK	Sync Counters for Rate Limit policies between machines
* / *	Inbound	TCP	AZURE_LOAD_BALANCER / VIRTUAL_NETWORK	Azure Infrastructure Load Balancer

Step# 3 – Create Application Gateway

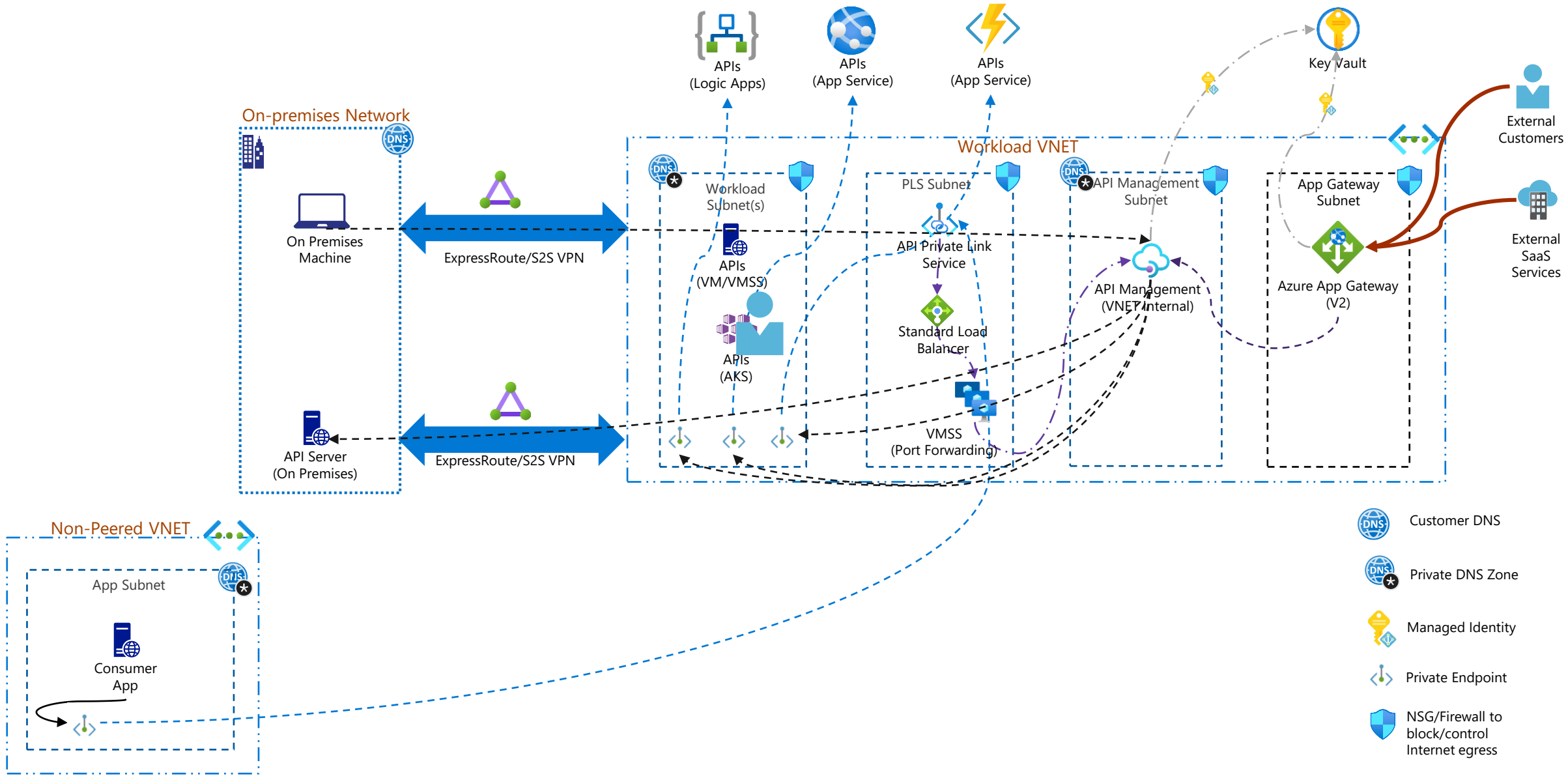
- Create App Gateway
  - Create a public IP for App Gateway
  - Use this PowerShell script here as reference to create the App Gateway
- Please see these link for further details abut this topic
  - Integrate API Management in an internal virtual network with Application Gateway
  - Integrating API Management with App Gateway V2

Step# 4 – Setup Private Link Service (Optional)

- Create Linux VM or VMSS to forward requests
  - Enable IP Forwarding.
    - Use this link for details
    - Here is the sample script to forward requests to IP address 10.3.0.5 and port 443
      - `sudo firewall-cmd --permanent --add-service=https`
      - `sudo firewall-cmd --permanent --add-forward port=port=443:proto=tcp:toport=443:toaddr=10.3.0.5`
      - `sudo firewall-cmd --permanent --add-forward-port=port=443:proto=tcp:toaddr=10.3.0.5:toport=443`
      - `sudo firewall-cmd --reload`
  - Create an Internal Standard Load Balancer and assign the VM(s) to its backend pool
    - See this link for more details
  - Create a Private Link Service using this Standard Load Balancer
    - See this link for details
    - Reference Architecture



Reference Architecture



Demo

© Copyright Microsoft Corporation. All rights reserved.