ADFS Powered By Windows Azure

Sameera Perera
October 2015

Agenda:

AD FS in Azure

- On-Premises AD FS Deployment Architecture
- Azure AD FS Deployment Architecture
- Azure Deployment Components

Topology Options:

- ADFS All in Azure simulating a “DMZ”
- ADFS All in Azure
- Proxy Hybrid
- Failover Hybrid
- Load Balanced Hybrid

Monitoring AD FS

Open Q & A

What is AD FS?

- AD FS provide authentication to claim based applications

Traditional Methods of Authentication

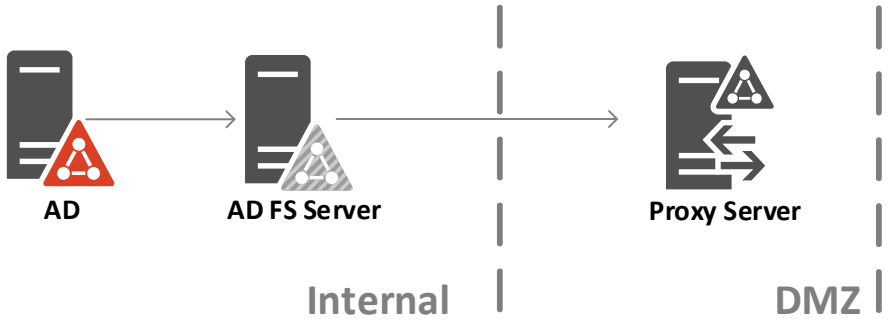
- Kerberos authentication – Username Password
- NTLM authentication – Username Password

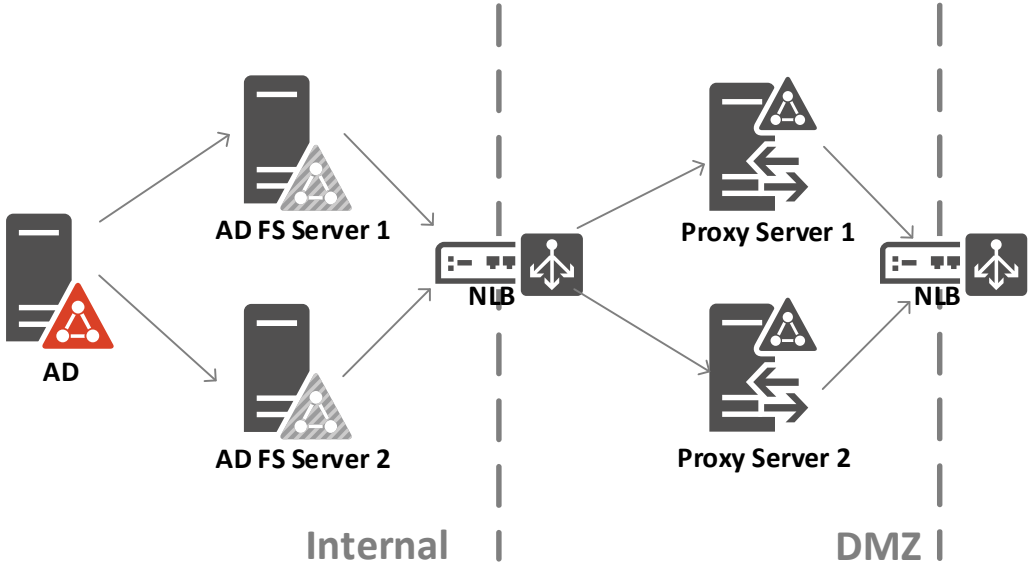
Why is it popular?

- Cloud Integration
- SaaS Applications – Web based applications
- Single Sign on - Best end user login experience

Standard AD FS deployments

On-premises



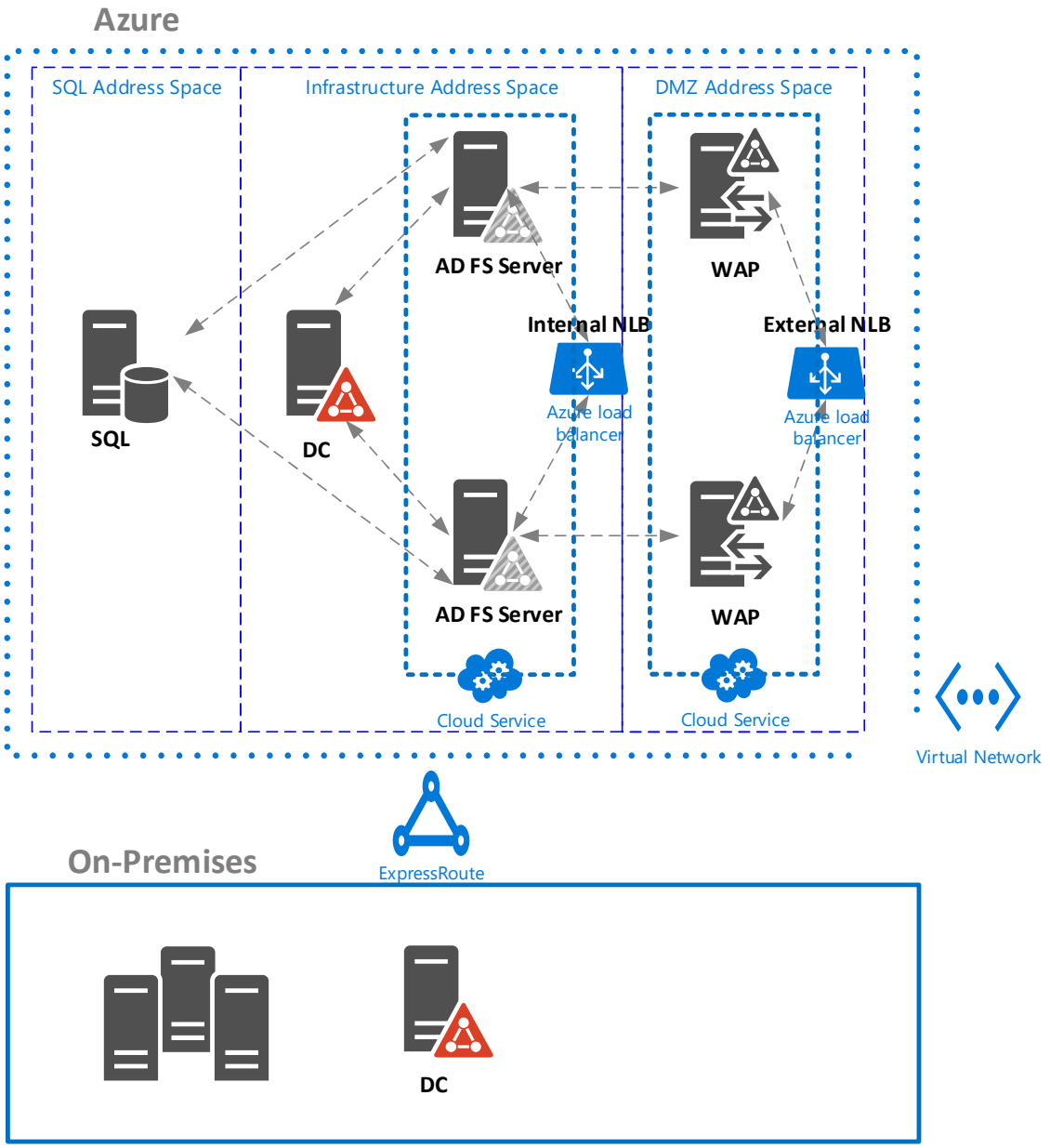


AD FS in Azure Components

- Azure VM
- Cloud Services
- Availability Sets

- Network and Connectivity
  - ExpressRoute
  - Load balancing
  - Network Security Groups
  - Address Spaces

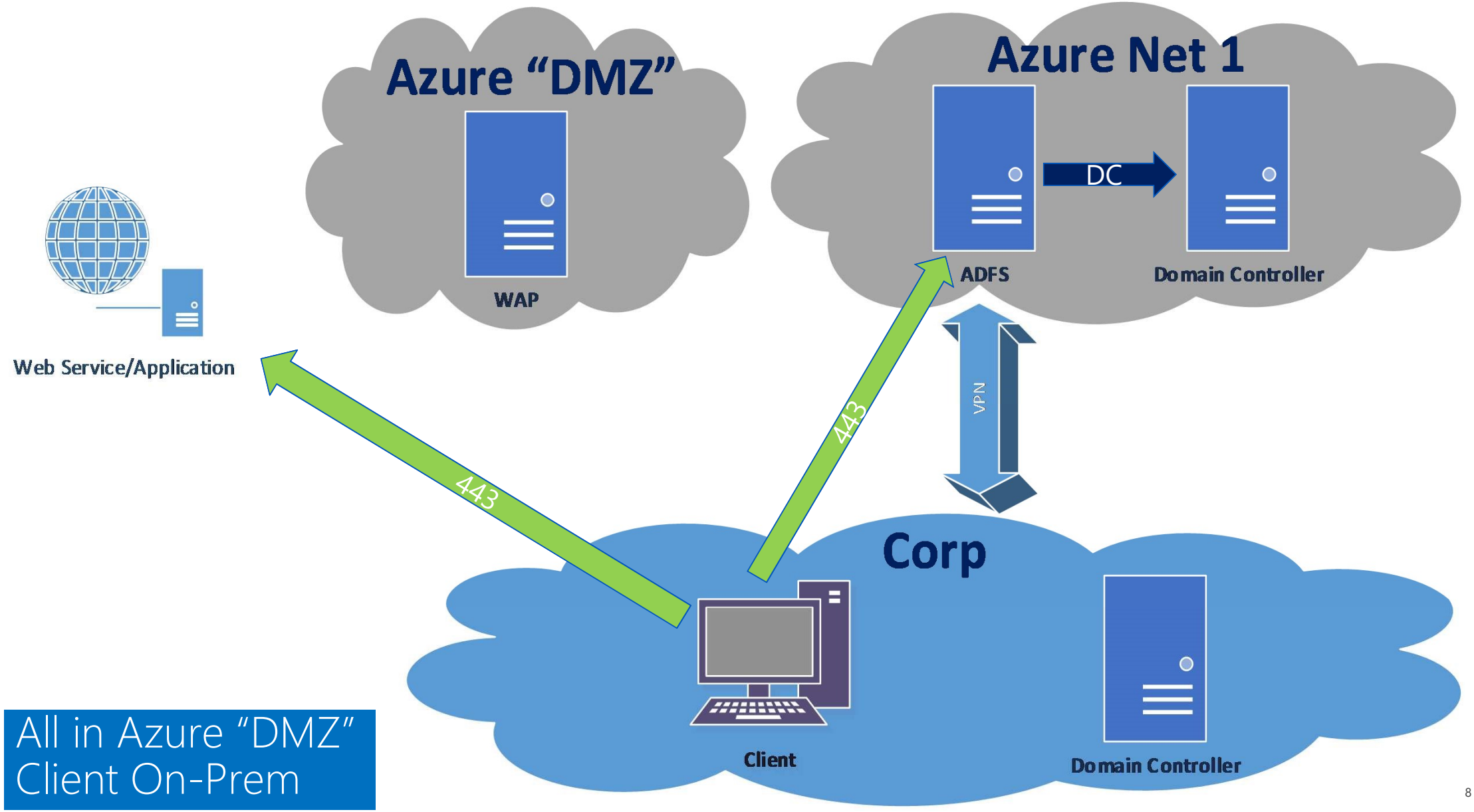
- Published End point



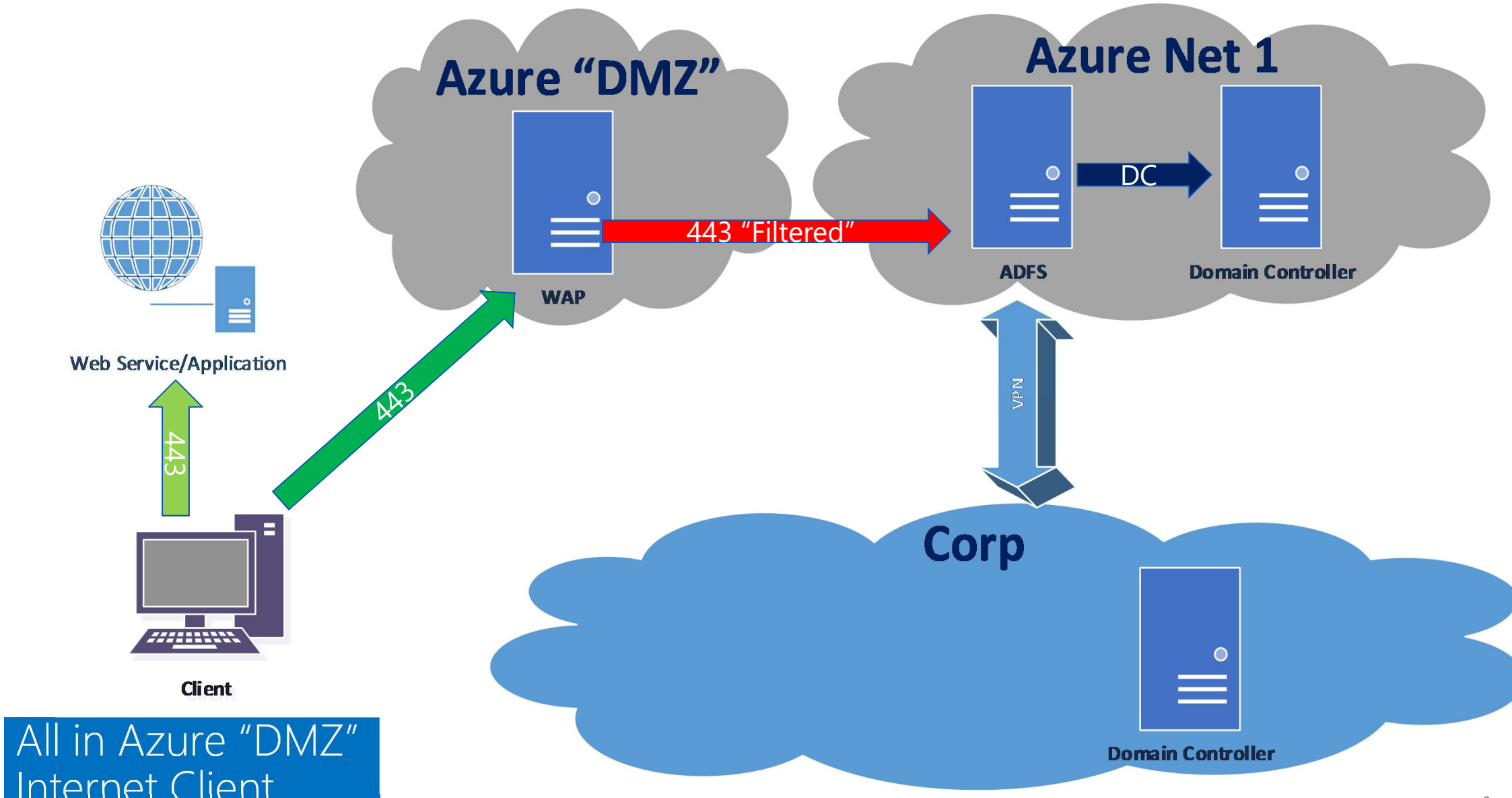
Azure AD FS Deployment Topologies

ADFS all in Azure

Separate the “DMZ” Network



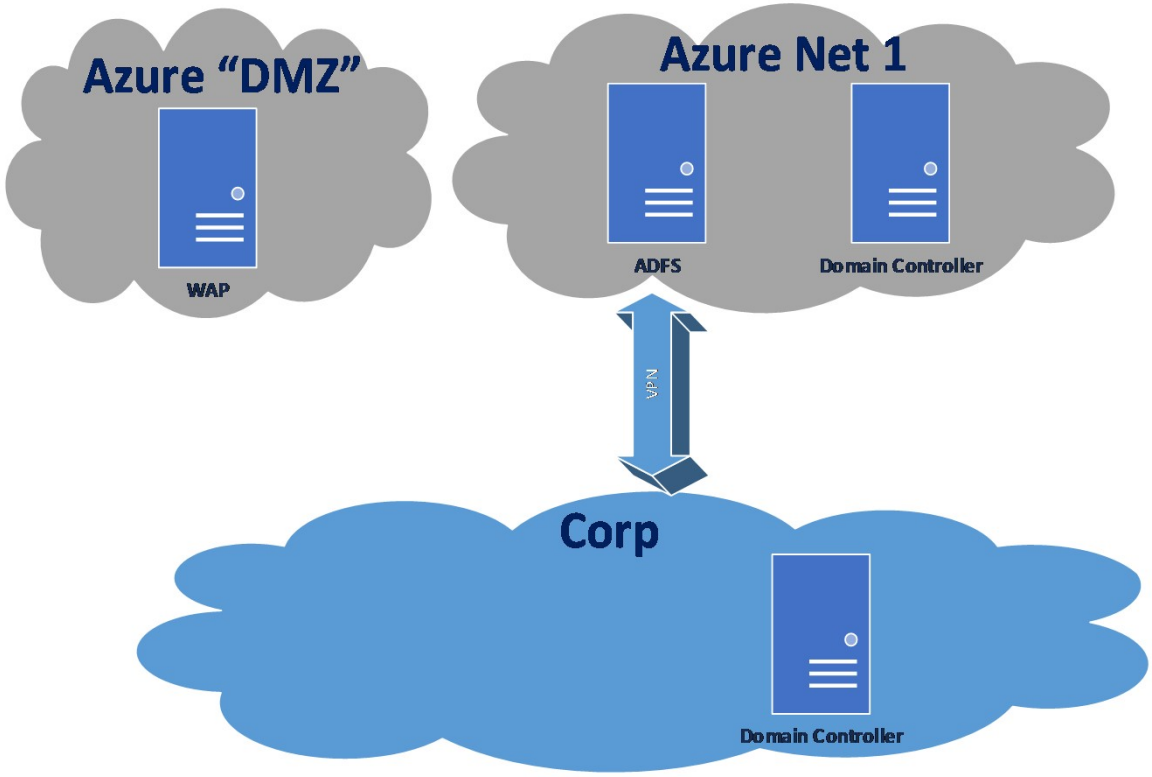
All in Azure "DMZ" Client On-Prem



All in Azure "DMZ"
Internet Client

All in Azure "DMZ"

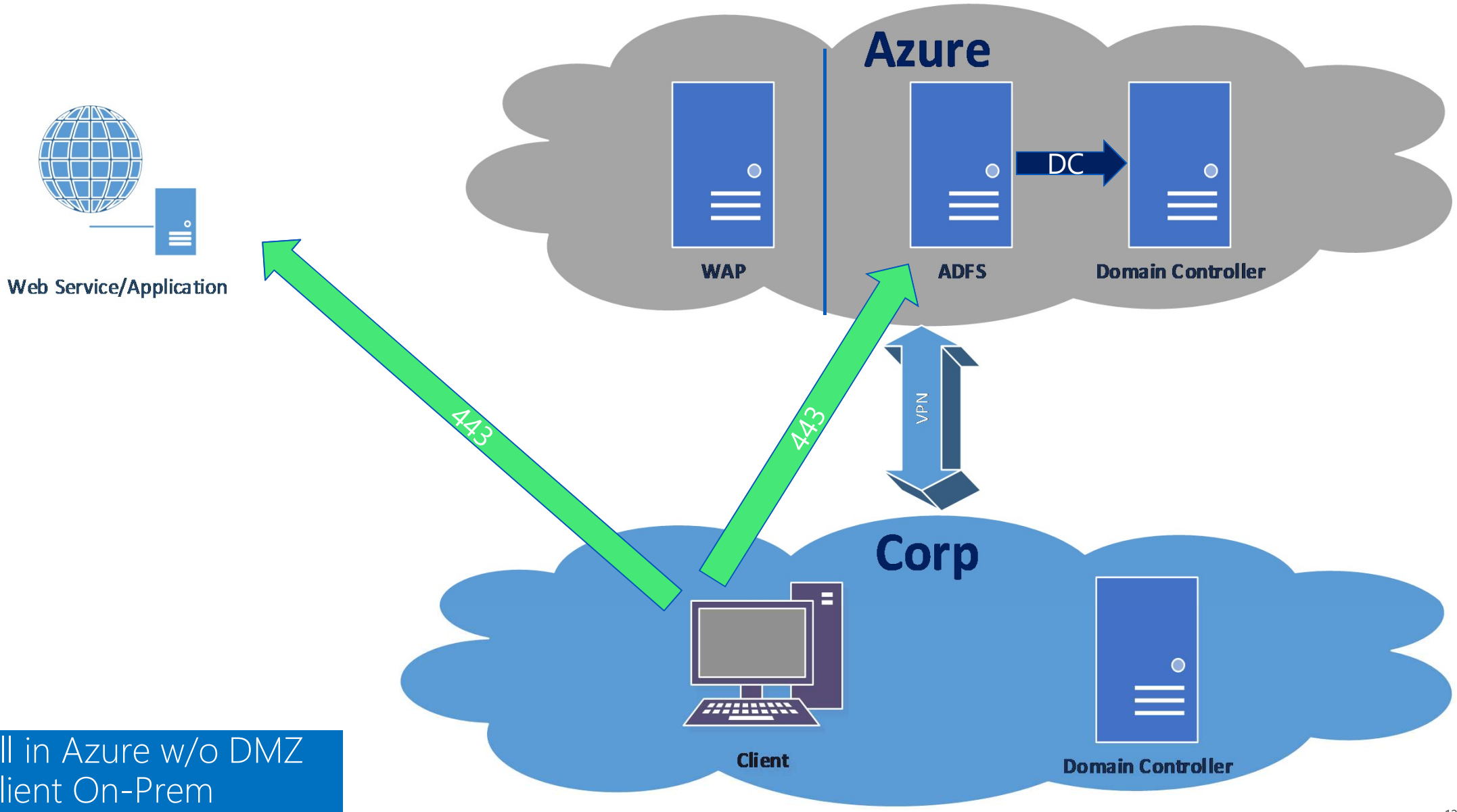
Pros and Cons



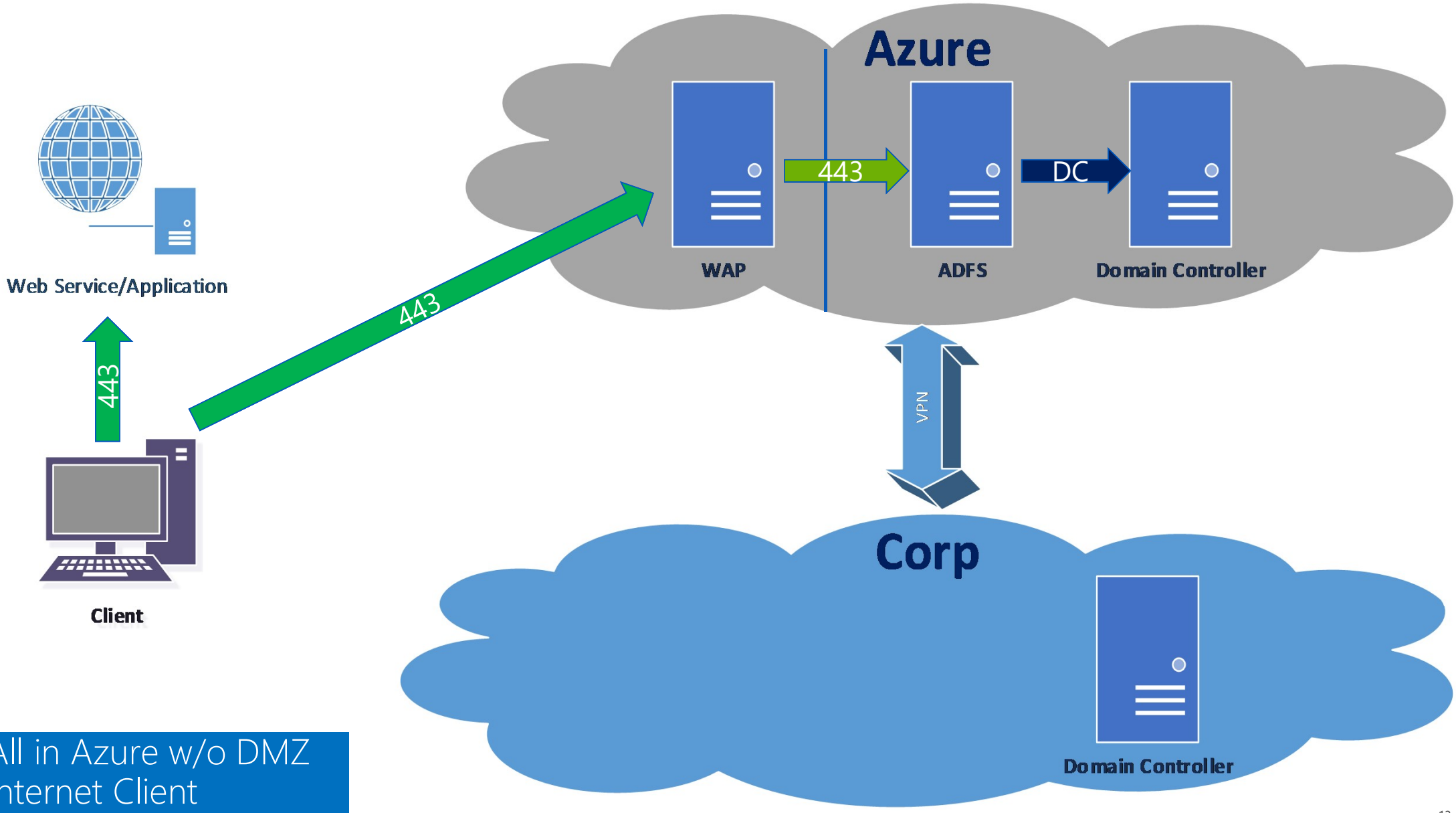
Pro	Con
WAP servers are on an isolated network	More Complex network configuration
If VPN/Express route is down ADFS will still function externally	ADFS Servers are exposed to the internet (ACL for 443)
If On-Prem datacenter is down, ADFS still function externally	If VPN/Express route is down ADFS will not function internally

ADFS all in Azure

Without the “DMZ”



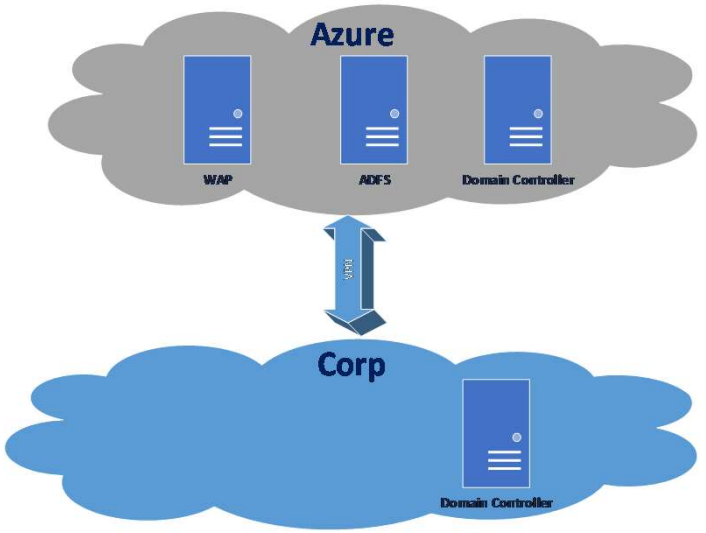
All in Azure w/o DMZ
Client On-Prem



All in Azure w/o DMZ
Internet Client

All in Azure

Pros and Cons

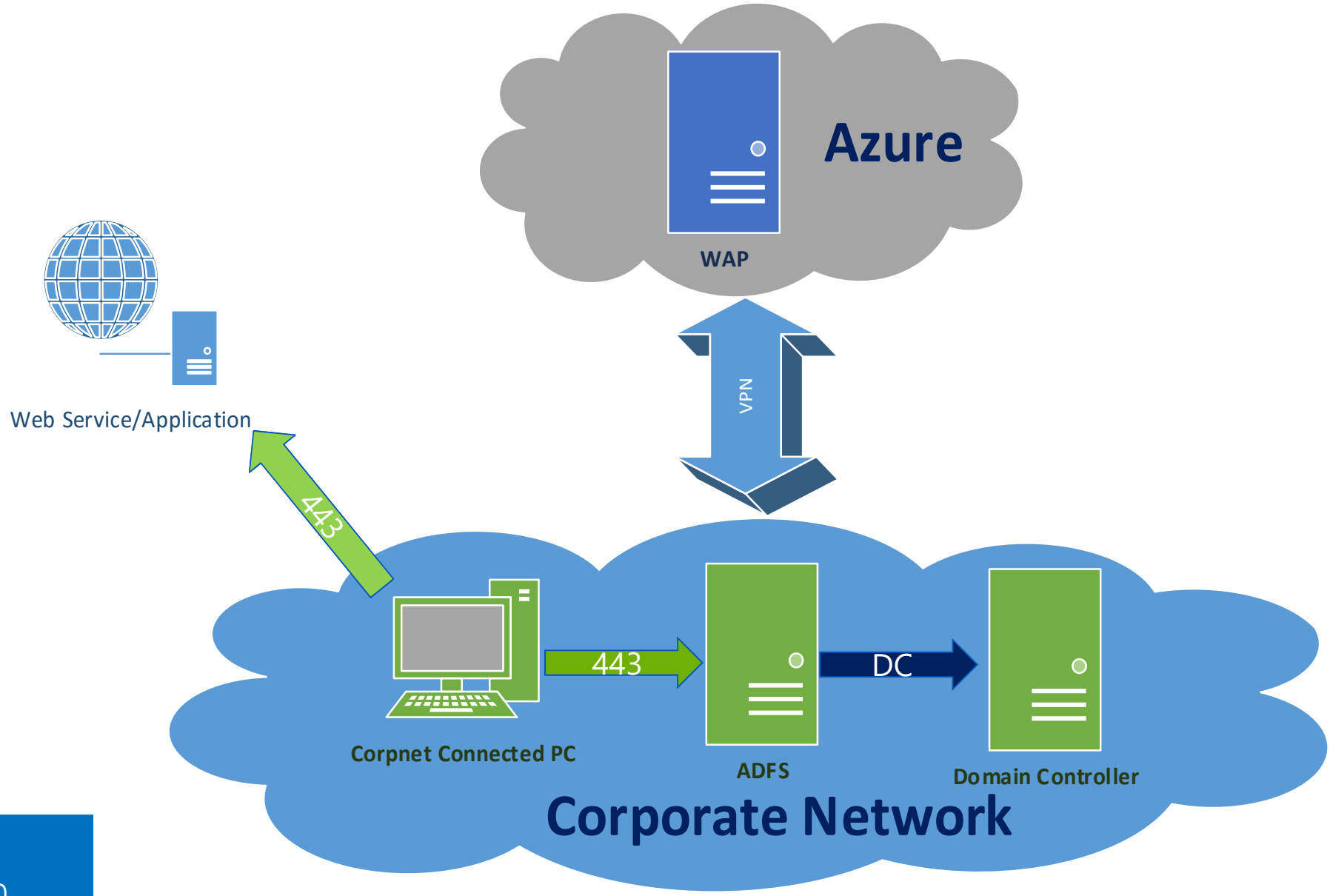


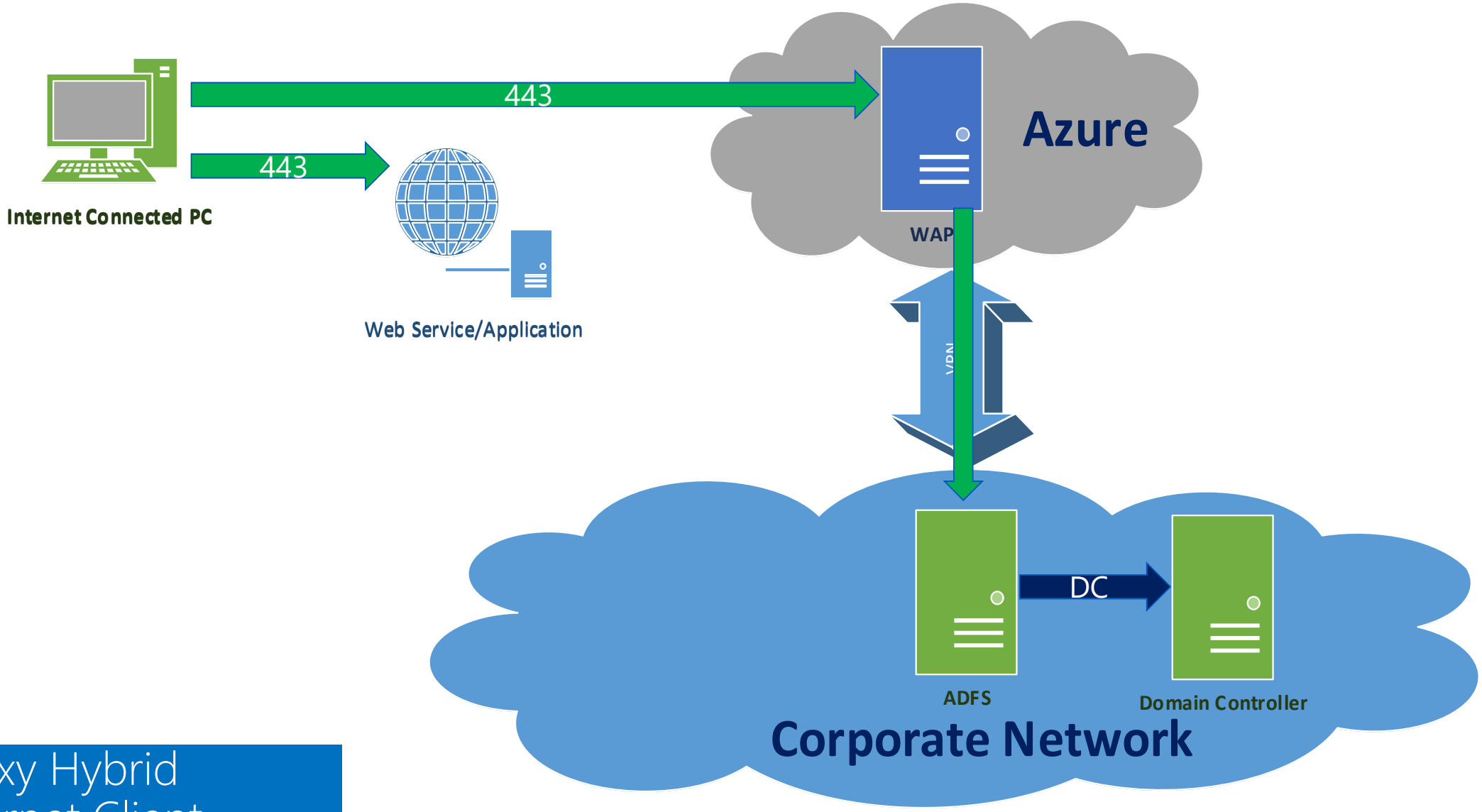
Complex network configuration	Con
ADFS servers not exposed to the internet	Complex network configuration
If VPN/Express route / on-prem DC is down ADFS will still function externally	If VPN/Express route is down ADFS will not function internally
All AD FS infrastructure is hosted in Azure.	Network level troubleshooting complexity
More secure deployment Only allowing necessary ports.	

Proxy in Azure Hybrid

Topology Overview

Proxy Hybrid Client On-Prem

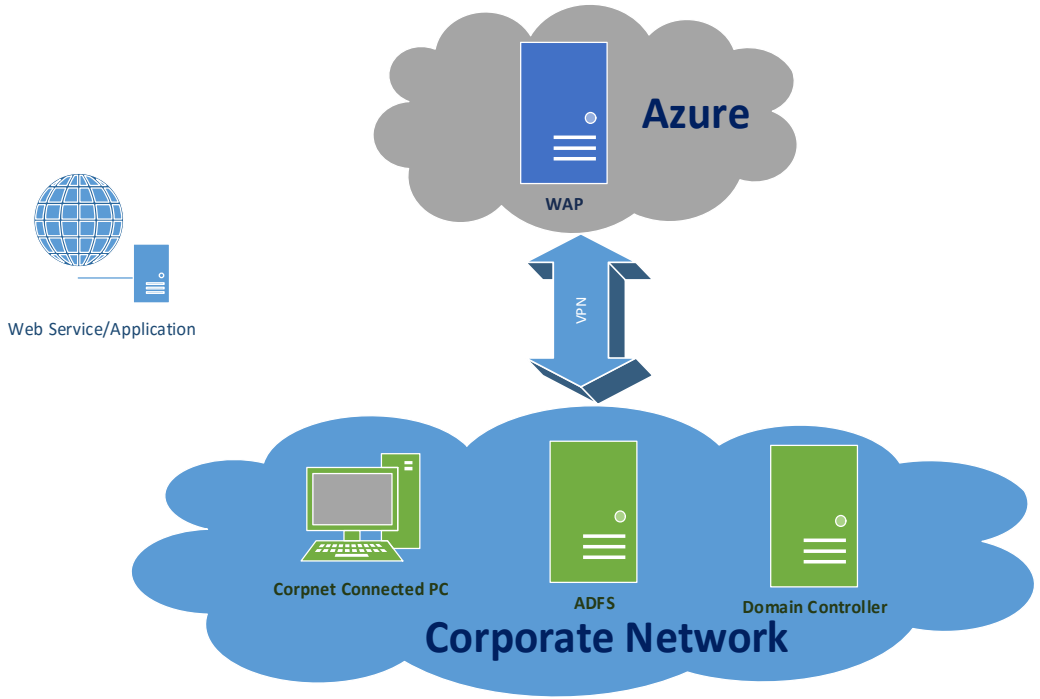




Proxy Hybrid Internet Client

Proxy in Azure

Pros and Cons

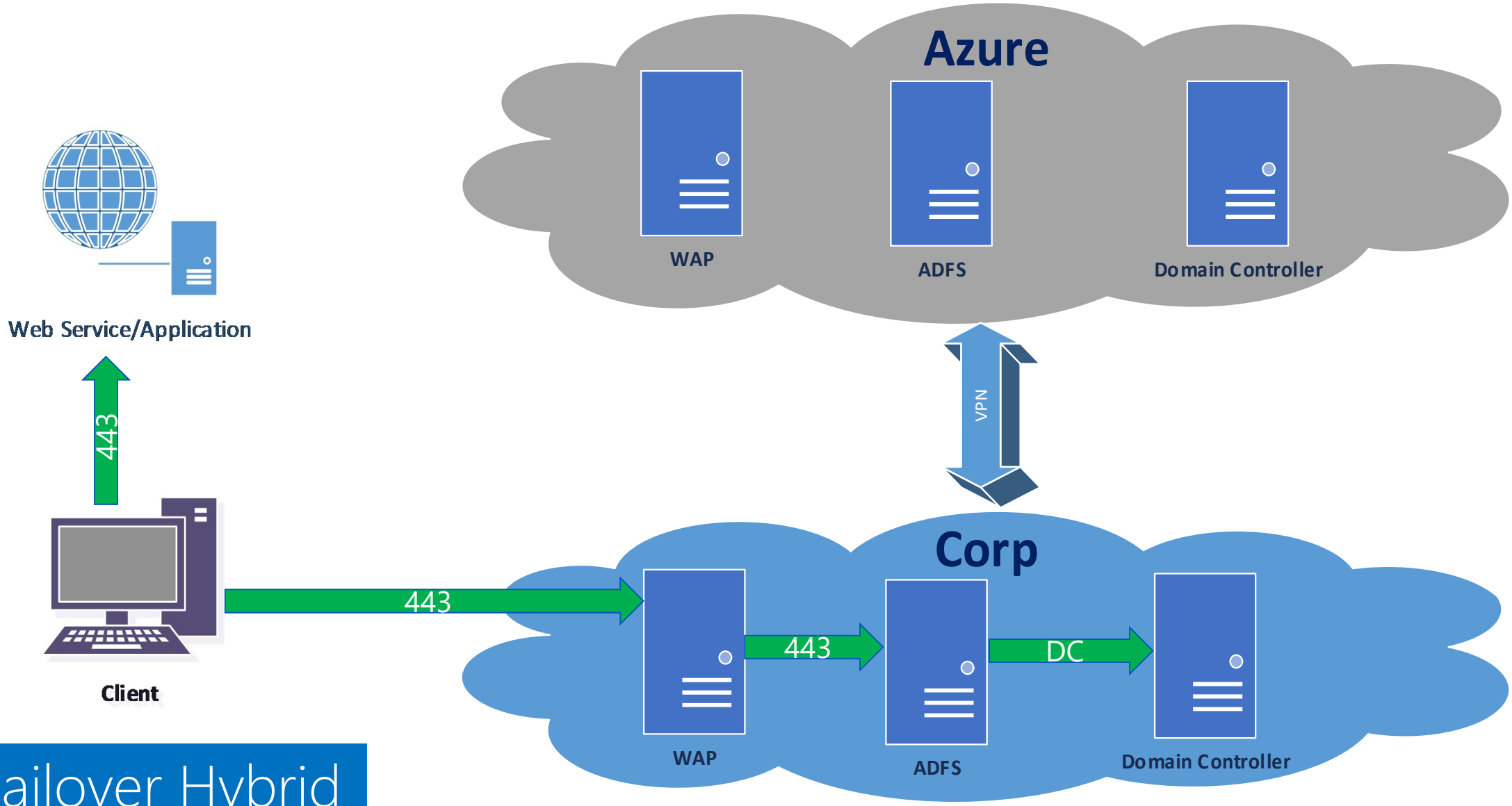


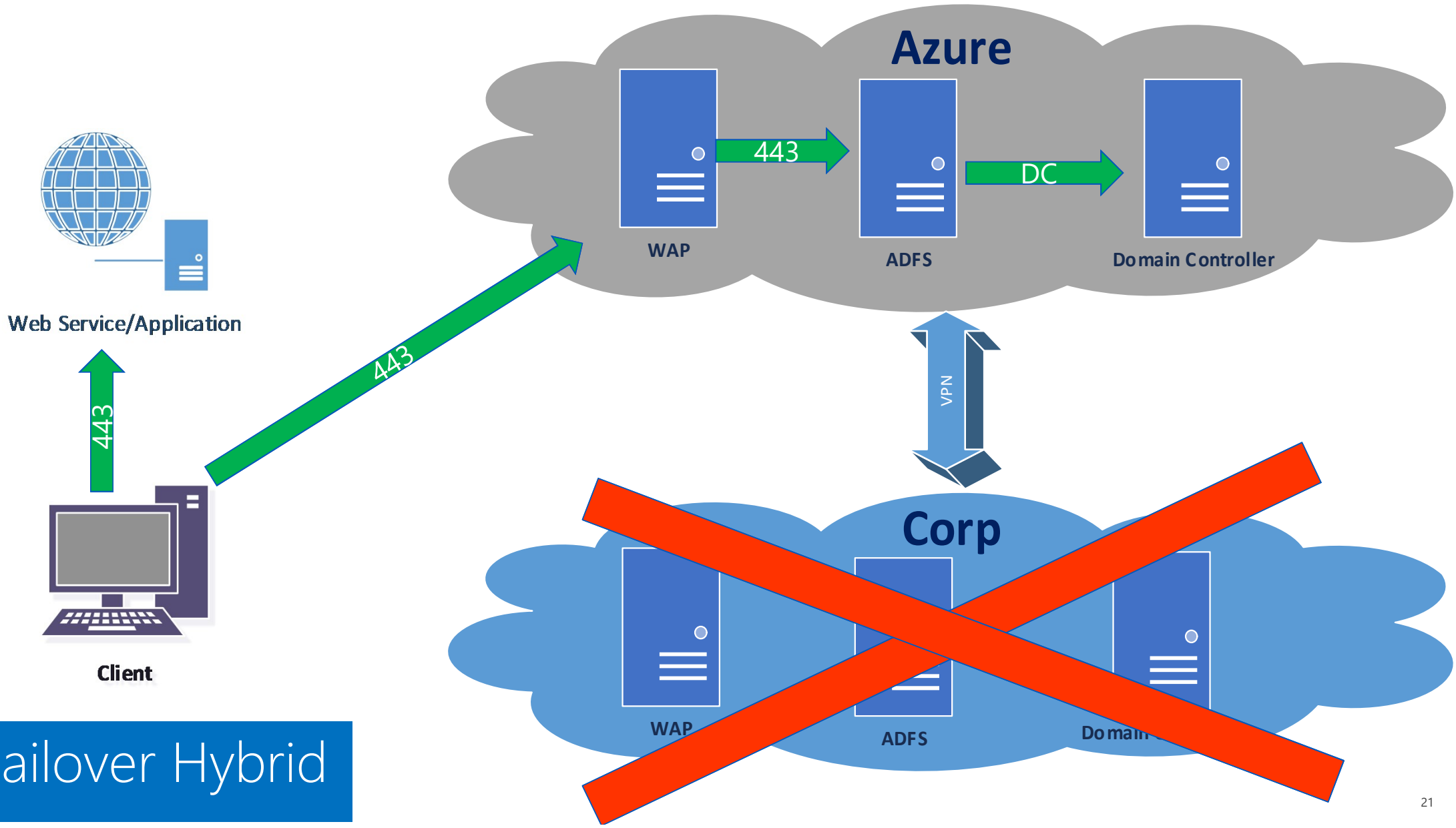
Pro	Con
Minimal Azure configuration	Solution dependent on VPN/ExpressRoute and On-prem servers
Enhanced security	
Can use public IPv4 from Azure	

ADFS Hybrid Configuration

Manual DNS Failover

Failover Hybrid





Failover Hybrid

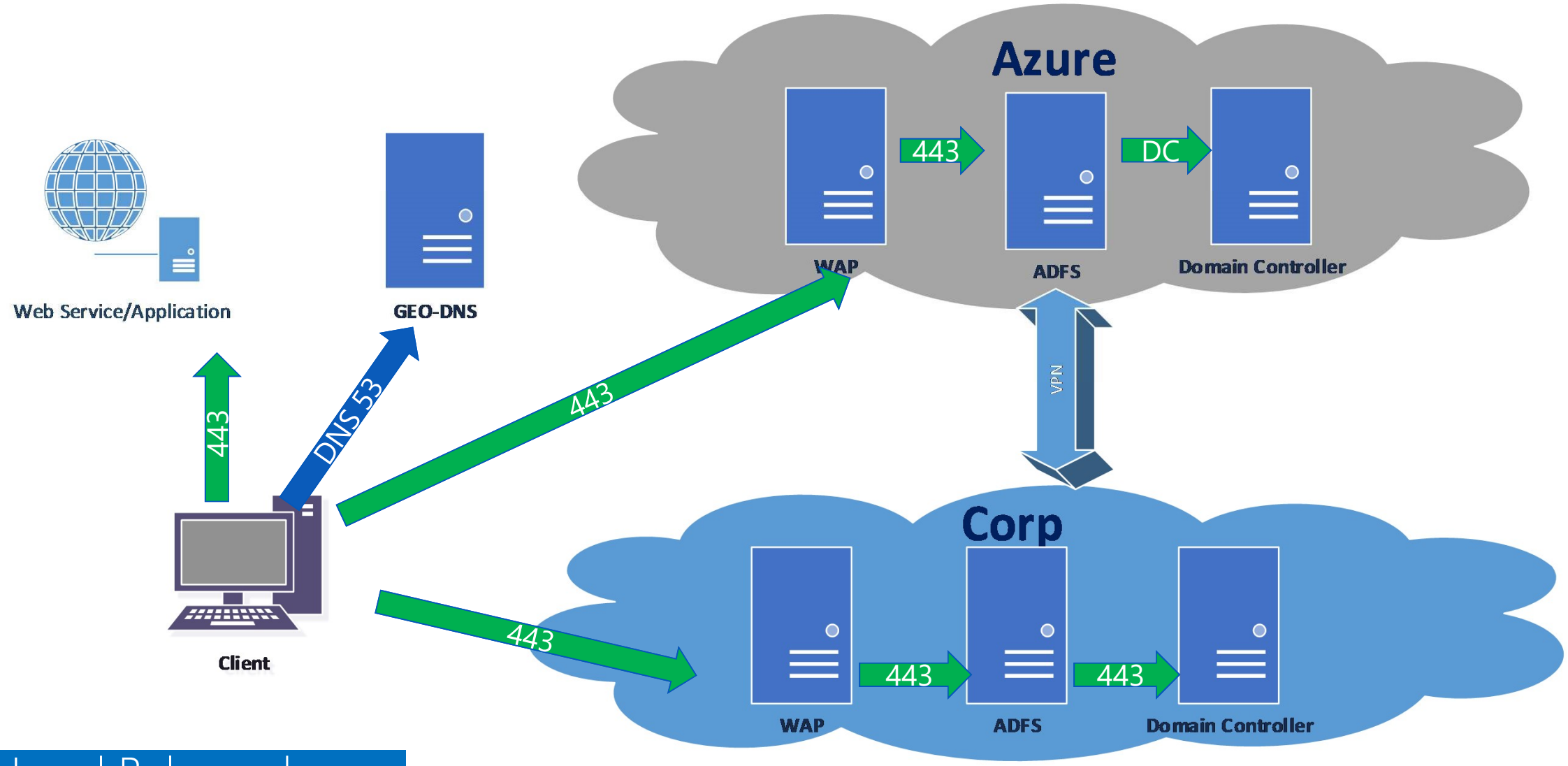
ADFS Hybrid Configuration – Manual Failover

Pros and Cons

Pro	Con
HA AD FS	Manual action must be taken for failover
On-Prem clients do not need to traverse Azure network	DNS TTL must expire for clients to failover
DR Solution for AD FS	Active Passive scenario

ADFS Hybrid Configuration

Load Balancer Configuration



Load Balanced Hybrid

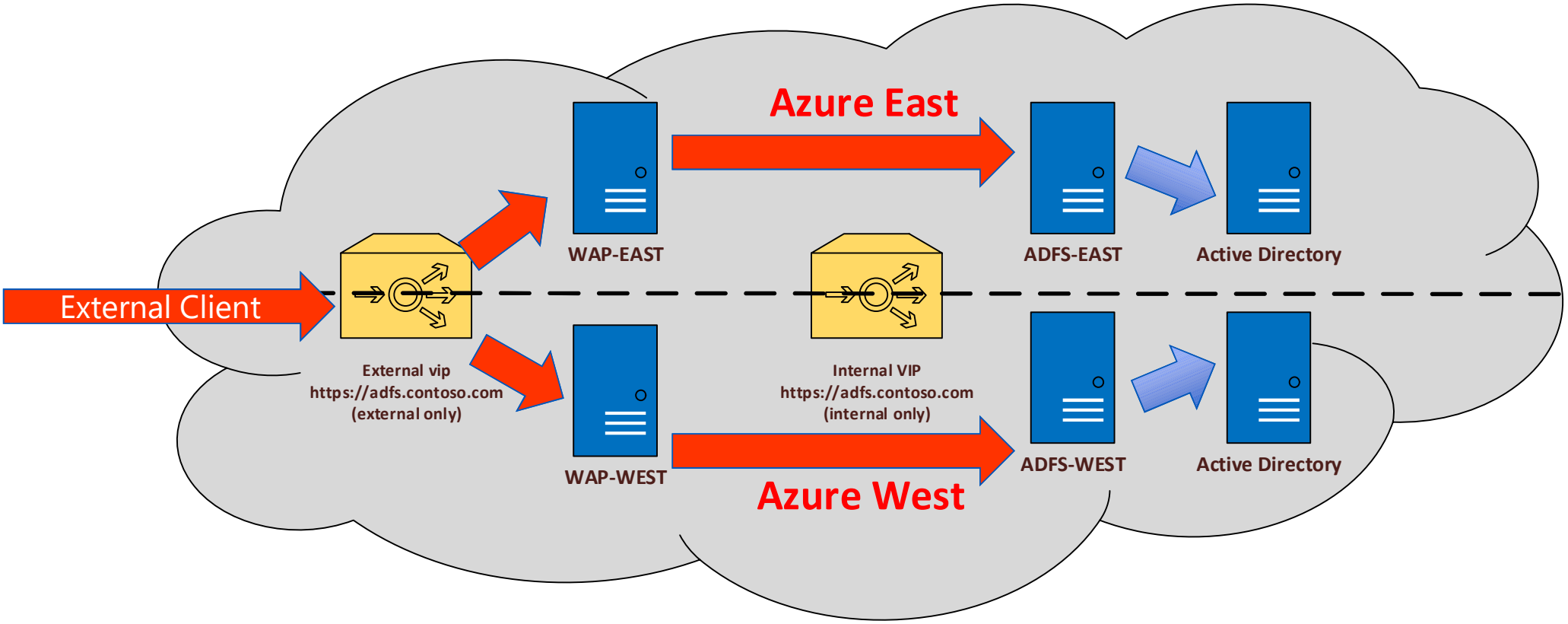
ADFS Hybrid Configuration – Load Balancer Configuration

Pros and Cons

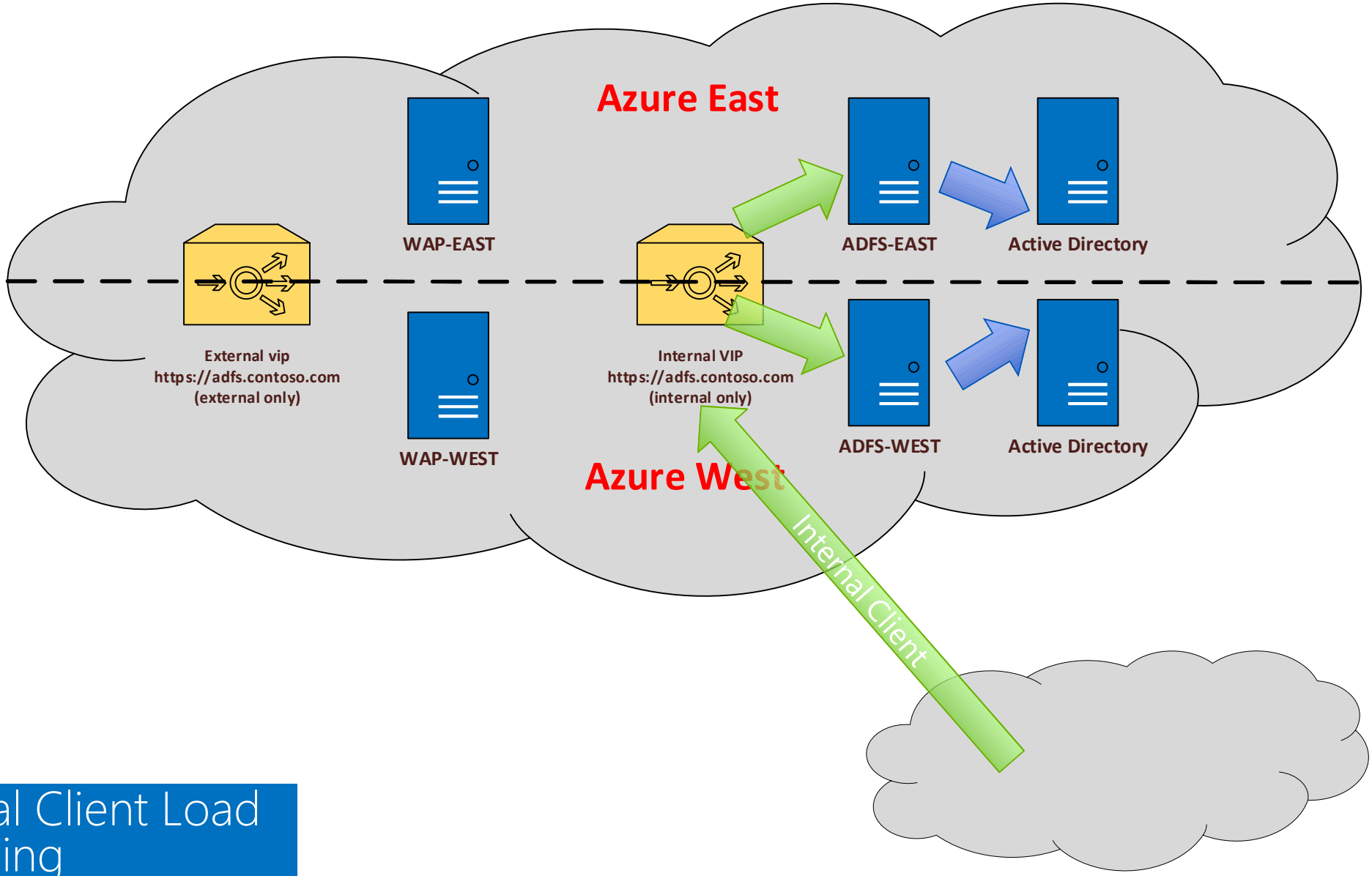
Pro	Con
Duplicate configurations for HA	3rd Party geo-load balancer or Hardware load balancer required
On-Prem clients do not need to traverse Azure network	More resources involved
Automatic Failover if On-prem or Azure fails	
Active - Active Scenario	

Load Balancing Scenario

All in Azure



External Client Load Balancing



Internal Client Load Balancing

ADFS Monitoring

ADFS Monitoring

AAD Connect Health

- Requires Azure AD Premium License
- Monitor you AD FS Servers from the Azure Portal.
- Detailed Logging
- Email Notification to Critical Alerts
- Graphical Presentation of login activities – Capacity Planning

AD FS Monitoring – DEMO

AD Connect Health

Q & A

Thank you!