

Get started with Azure Firewall

Stefan Ivemo

Technical Architect – Advania – Knowledge Factory

 @StefanIvemo

Stefan Ivemo

Introduction



Technical Architect @ Advania – Knowledge Factory



In love with Azure since 2014



Azure Bicep fanboy!



Frequent contributor to docs.microsoft.com



Creator of community projects:

☁ Azure Virtual WAN Playground



Bicep PowerShell Module



blog.ivemo.se



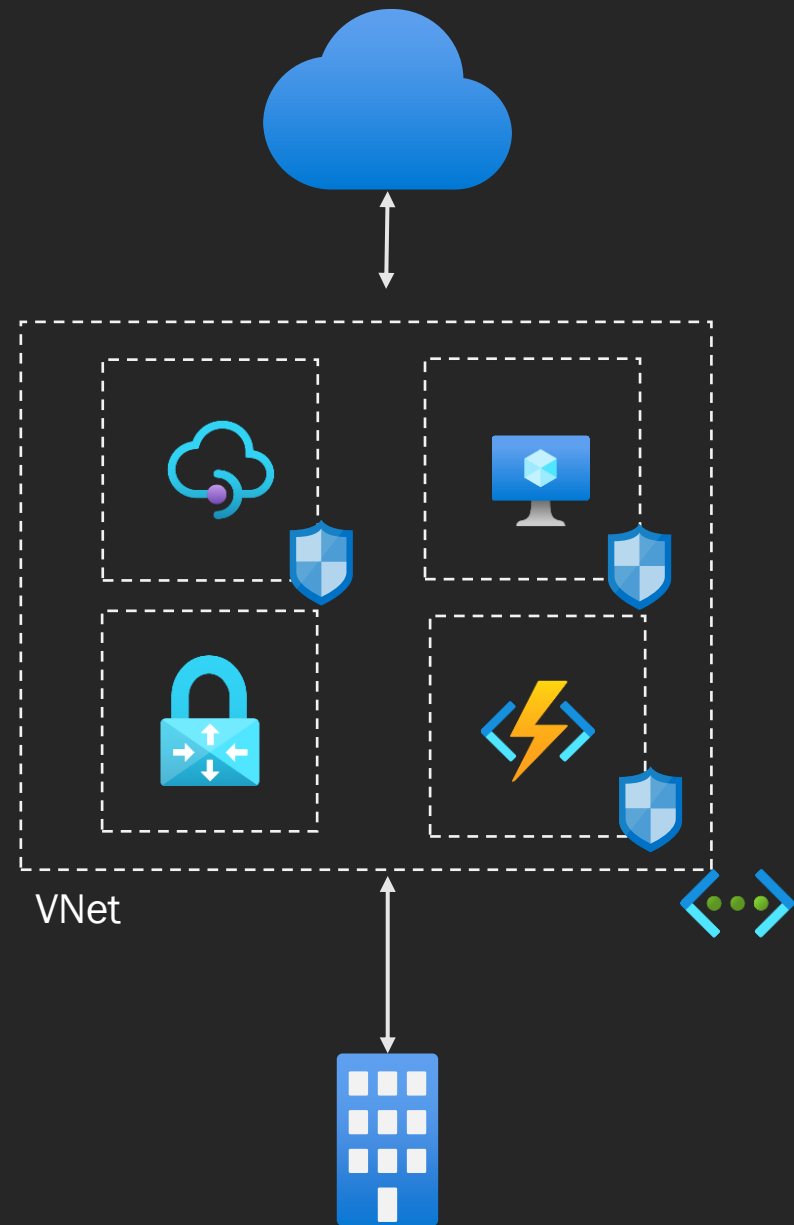
StefanIvemo



@StefanIvemo

What is a Virtual Network?

Virtual Network



Why do we need a Firewall?

Why do we need a Firewall?



Security is not
just happening in the cloud



Inbound & outbound
traffic



More and more VNet
connected services



Wrong people doing
Network Security



NSGs

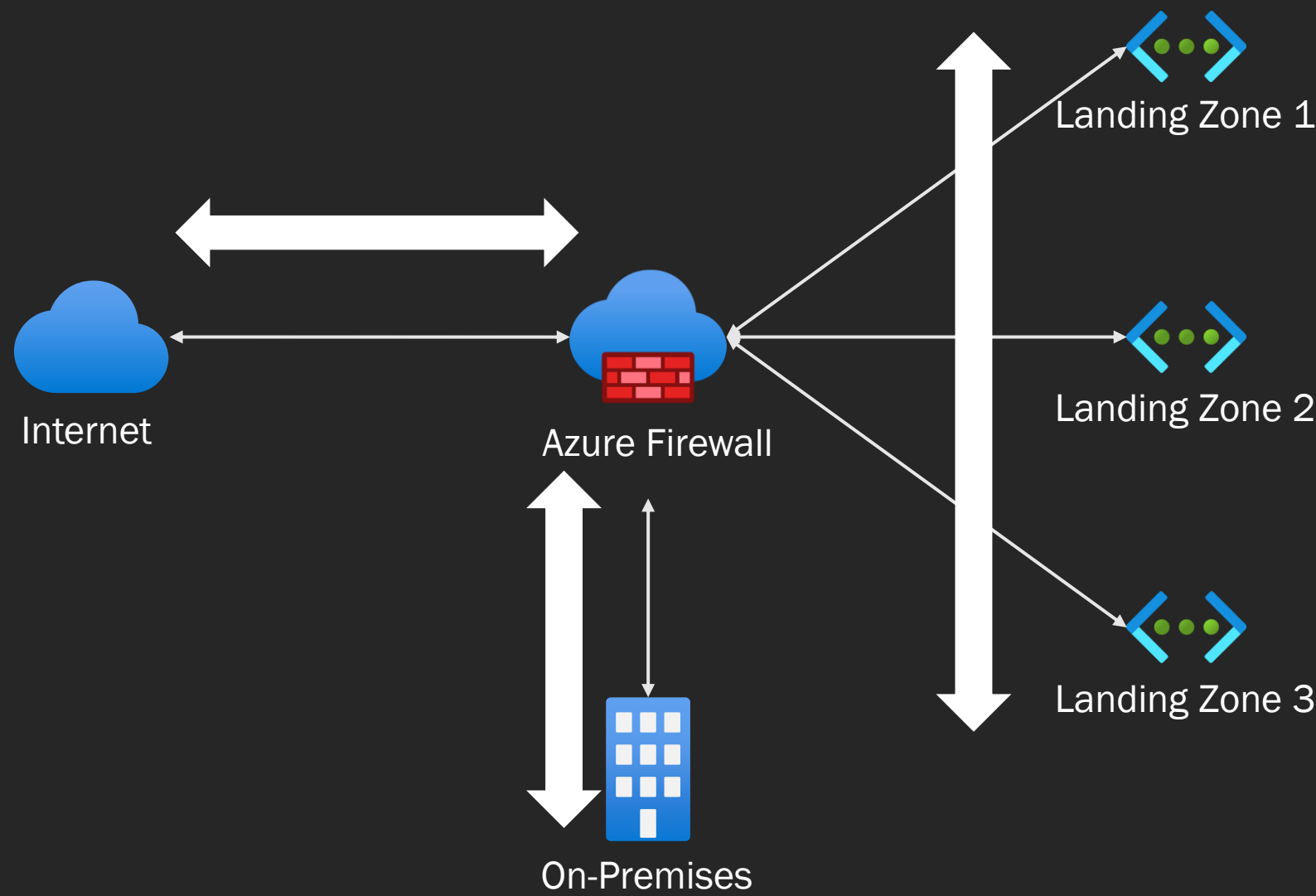


Application GW
+ WAF



Central logs

Central Firewall



What is Azure Firewall?

Azure Firewall



Built-in HA



Scalability



Up to 30 Gbps
throughput



Deploy/Manage
as Code



Azure Support

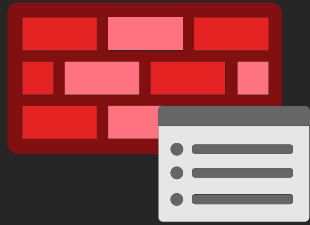


Certifications



Multiple Public IPs

Features – Standard SKU



Traffic Filtering



Threat Intelligence



DNS Proxy



Logs & Monitoring

Features – Premium SKU (Preview)



TLS Inspection



IDPS

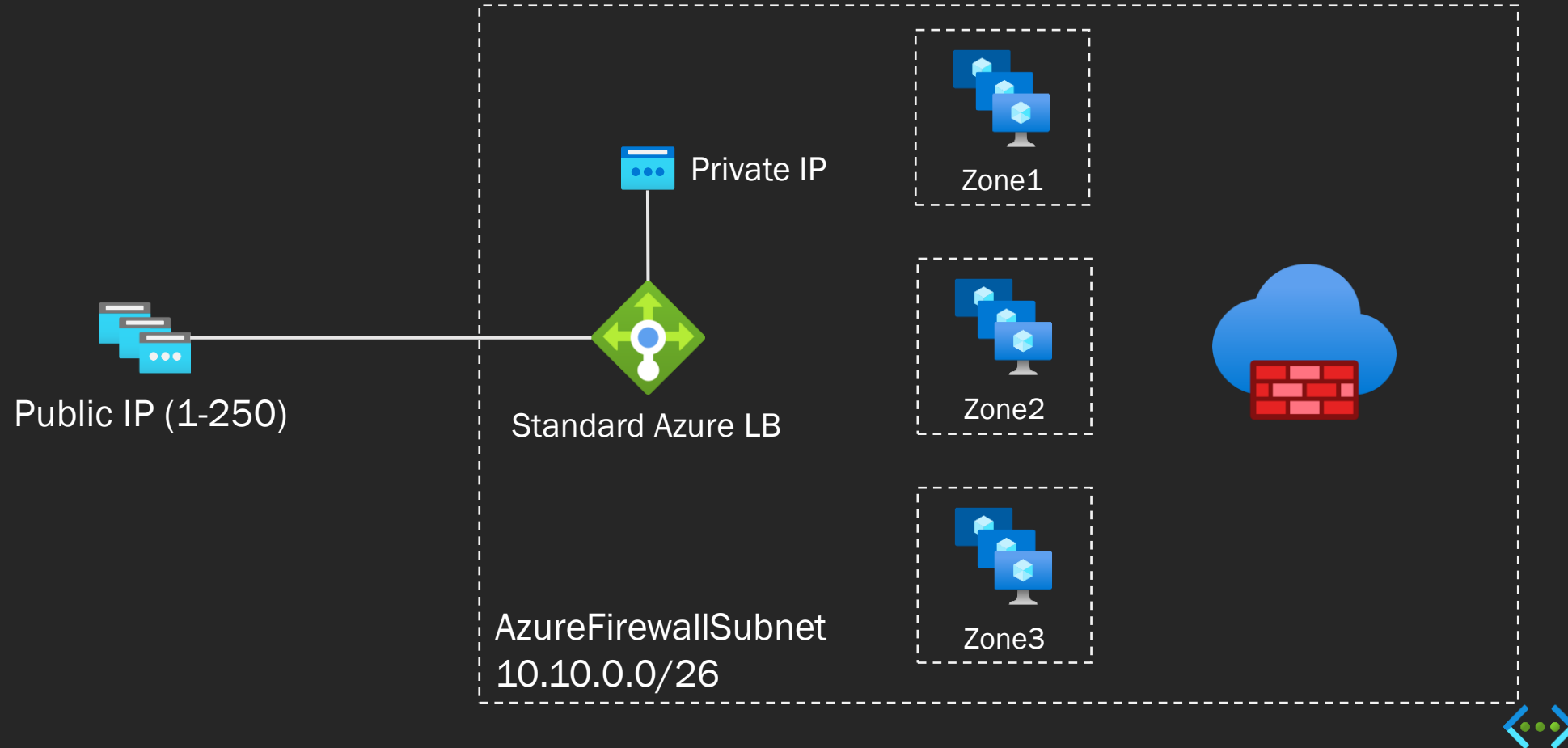


URL Filtering



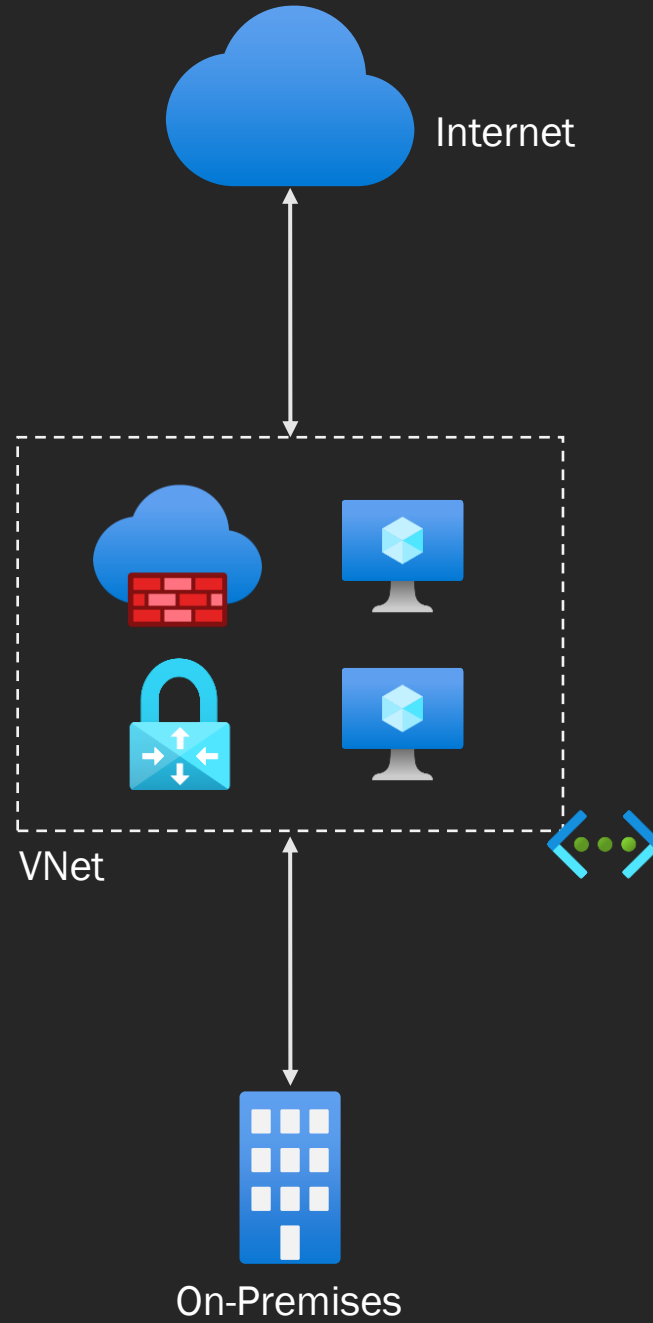
Web Categories

Under the hood

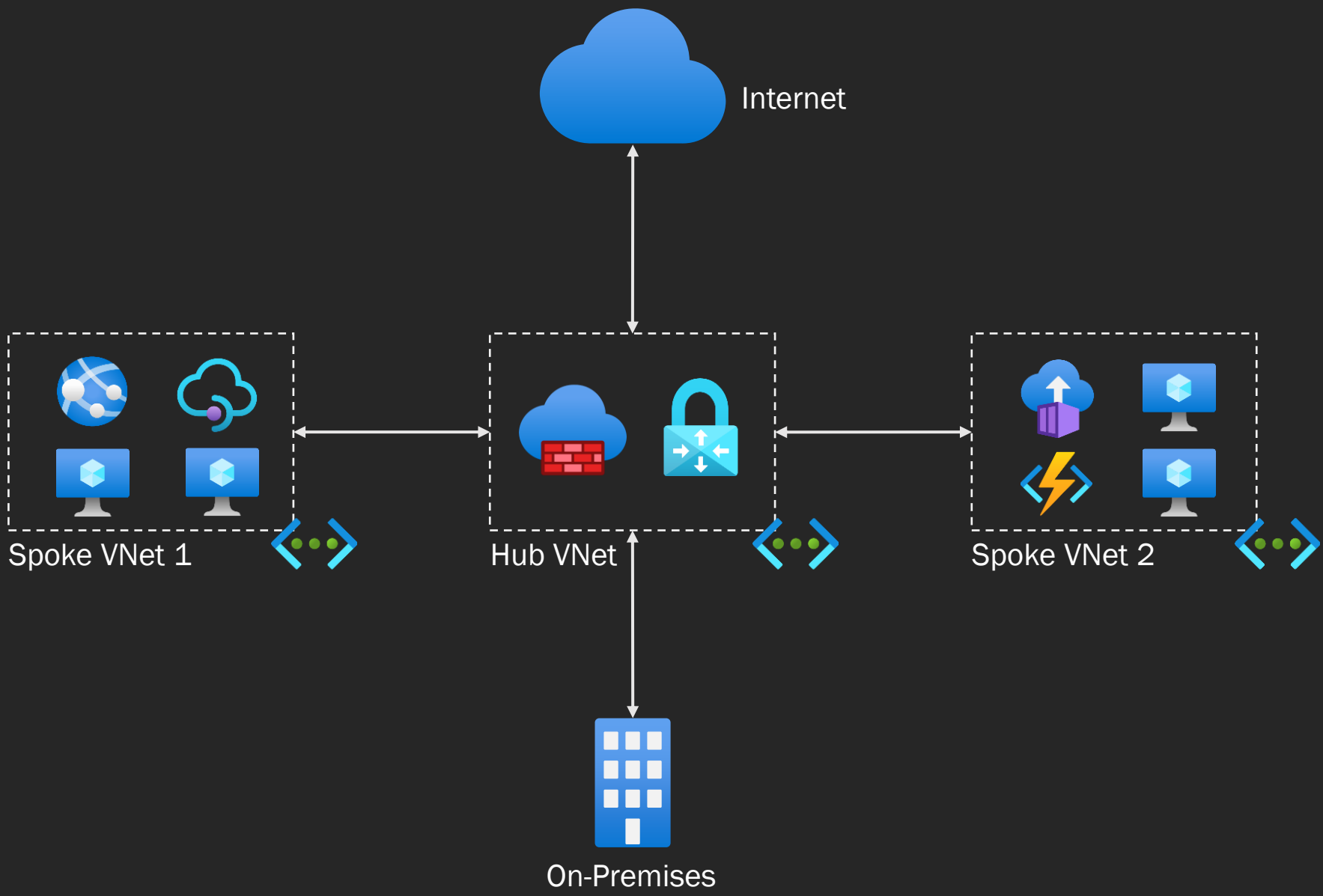


Azure Firewall Topologies

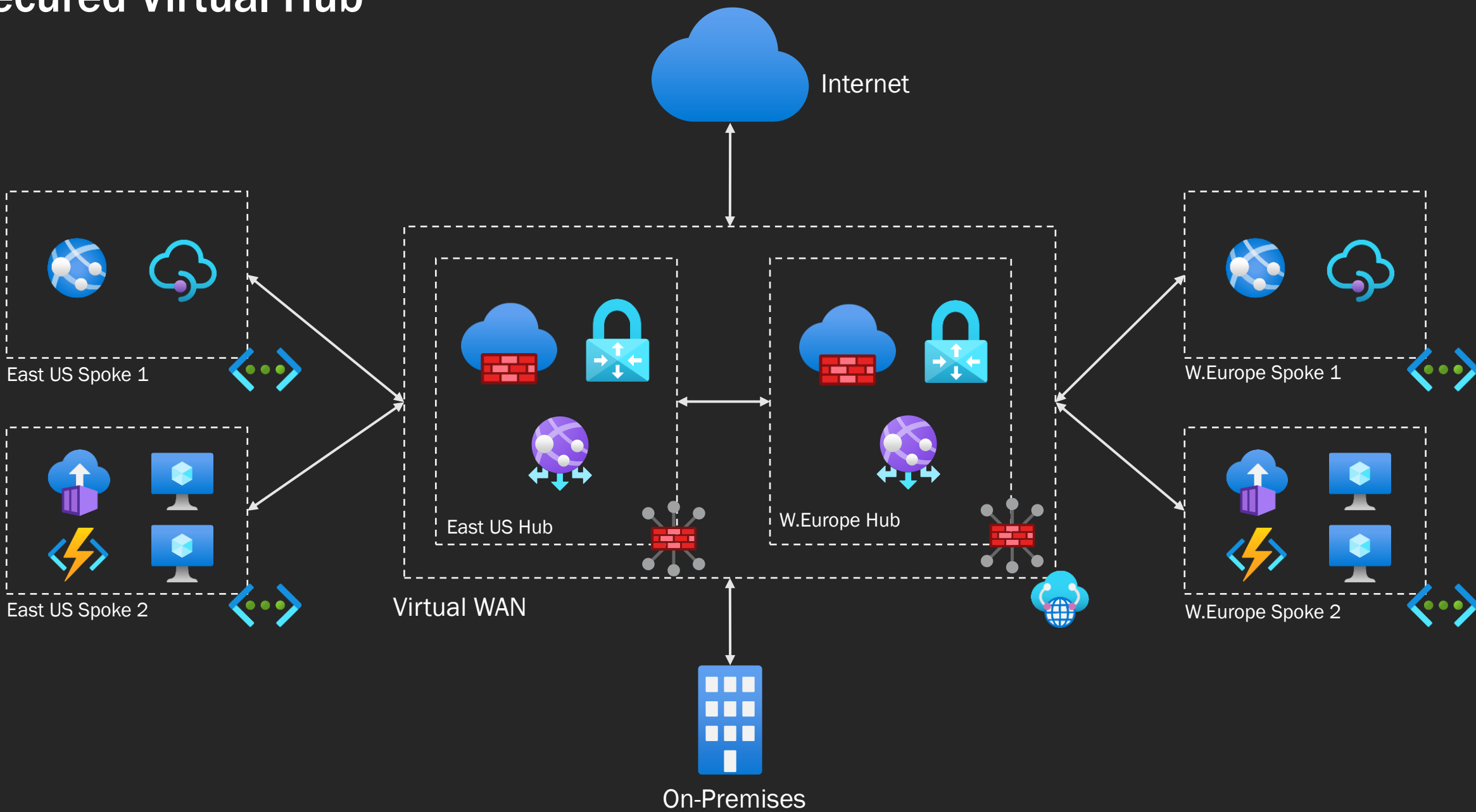
Single VNet



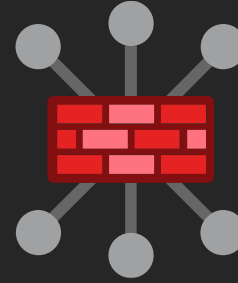
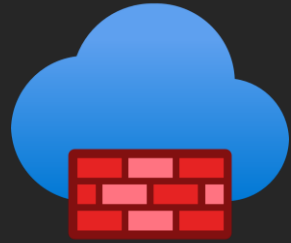
Hub & Spoke



Secured Virtual Hub



VNet FW vs. Secured Virtual Hub



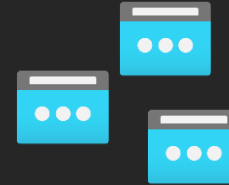
Availability Zones supported



Availability Zones not yet available



Customer managed Public IPs



Auto generated Public IPs



DDoS Protection standard support



No DDoS Protection standard support




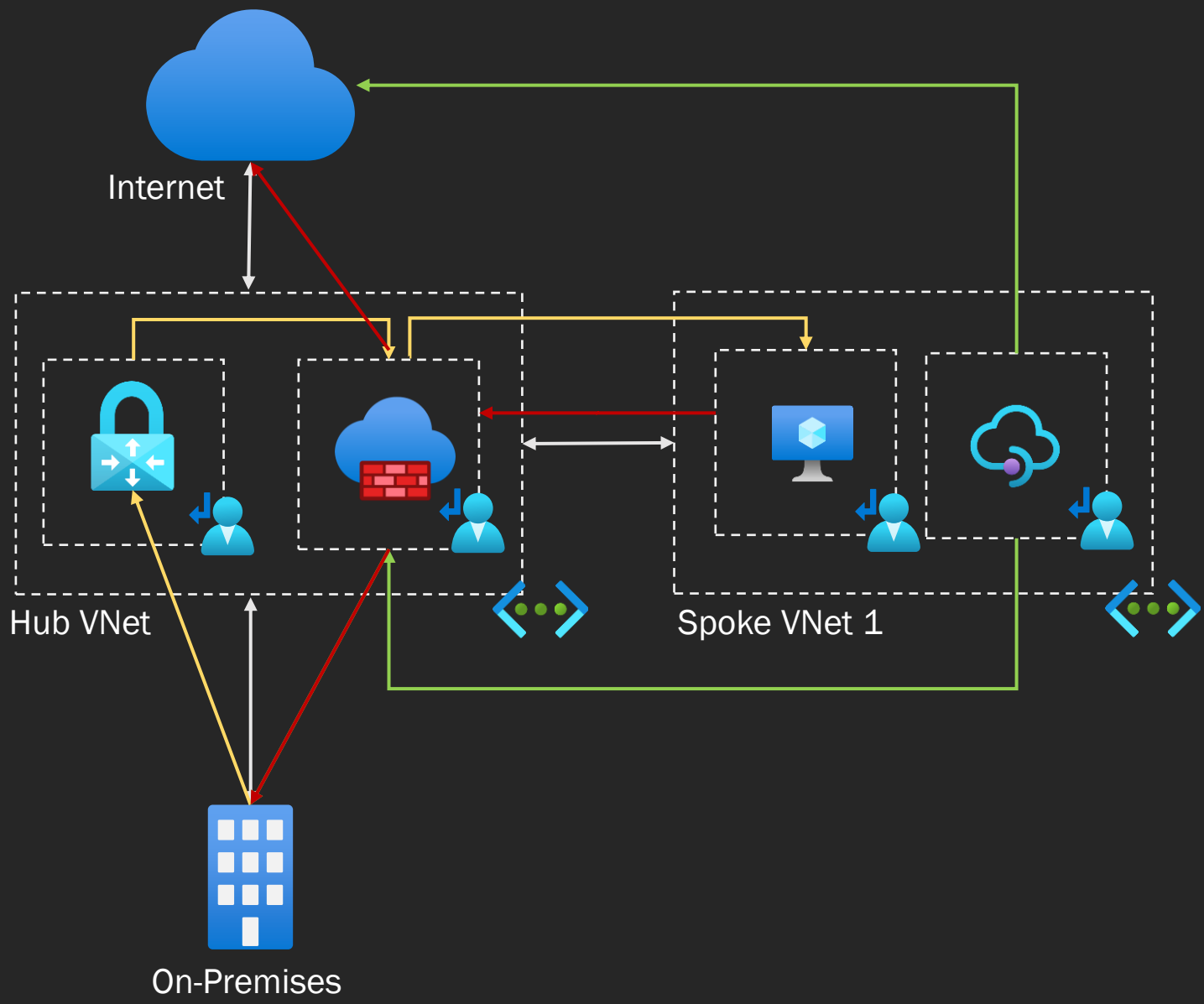
Subnet level routing



Simplified routing

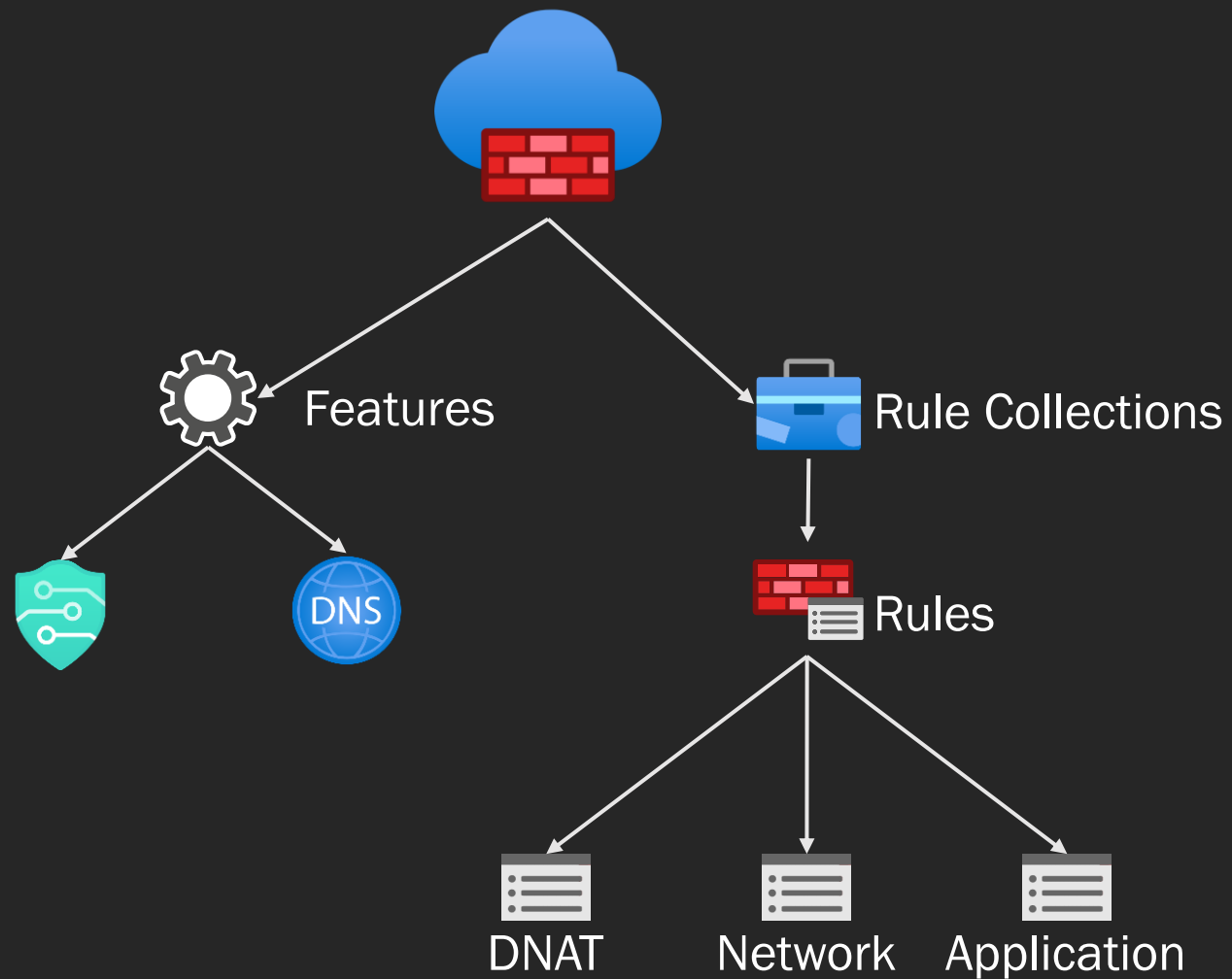
Routing

 User-defined routes

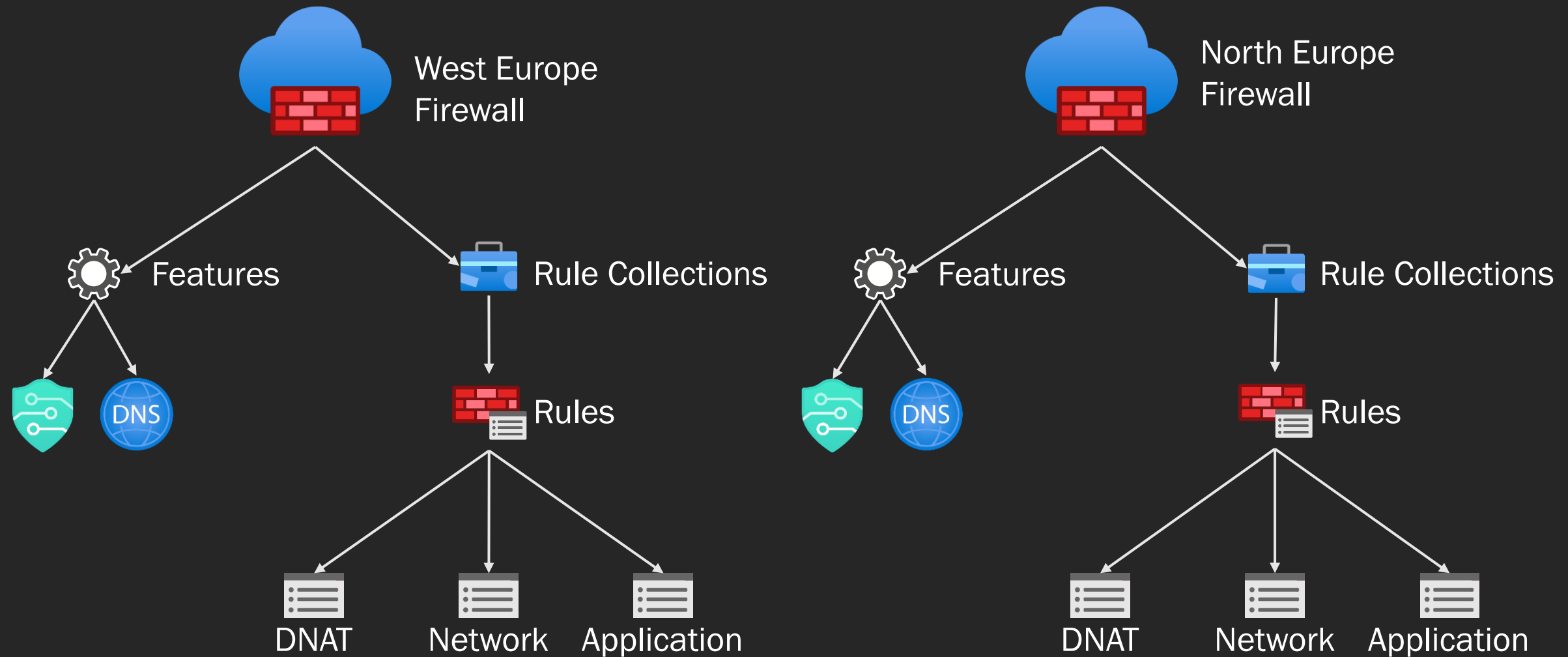


Administrative Models

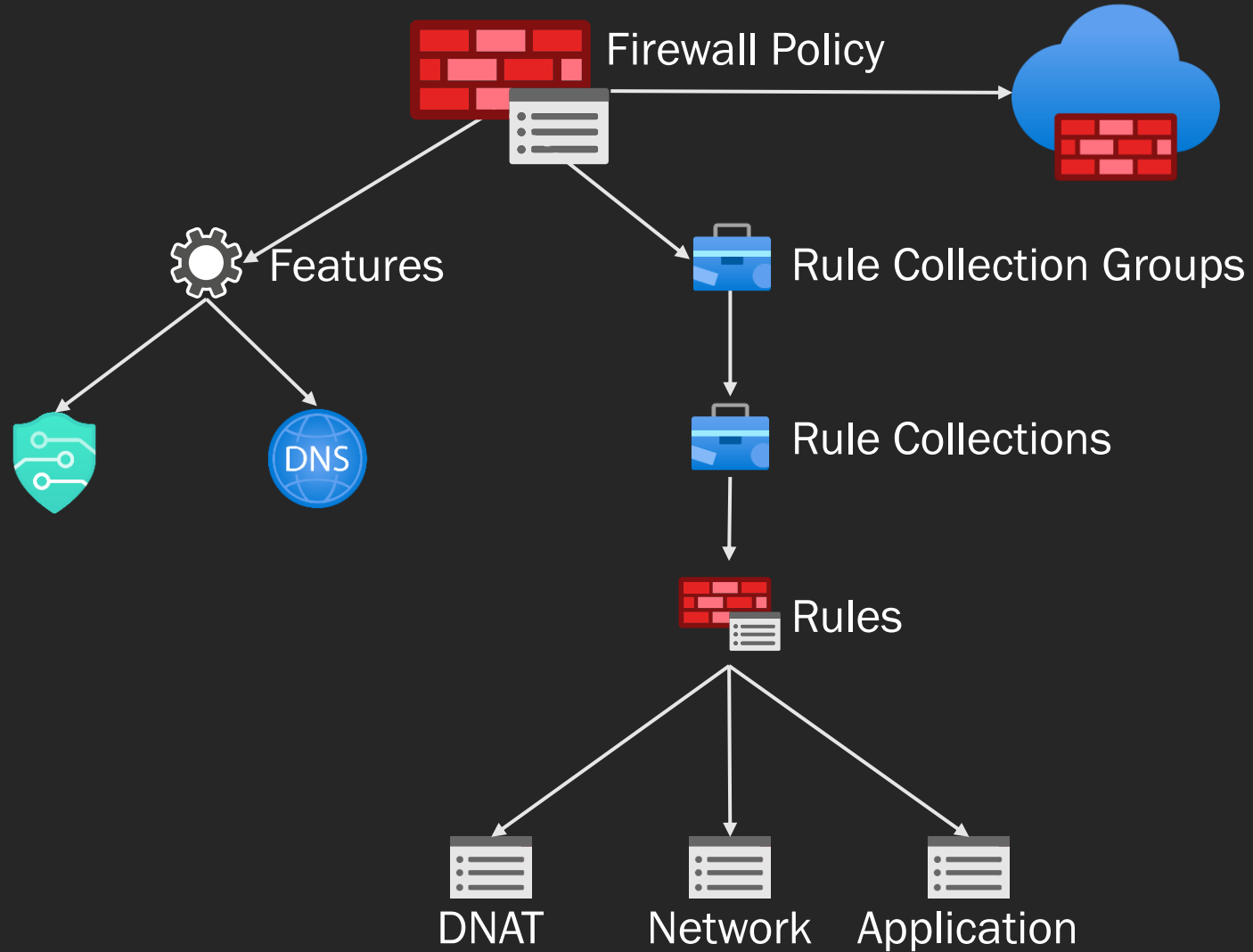
Standalone Management



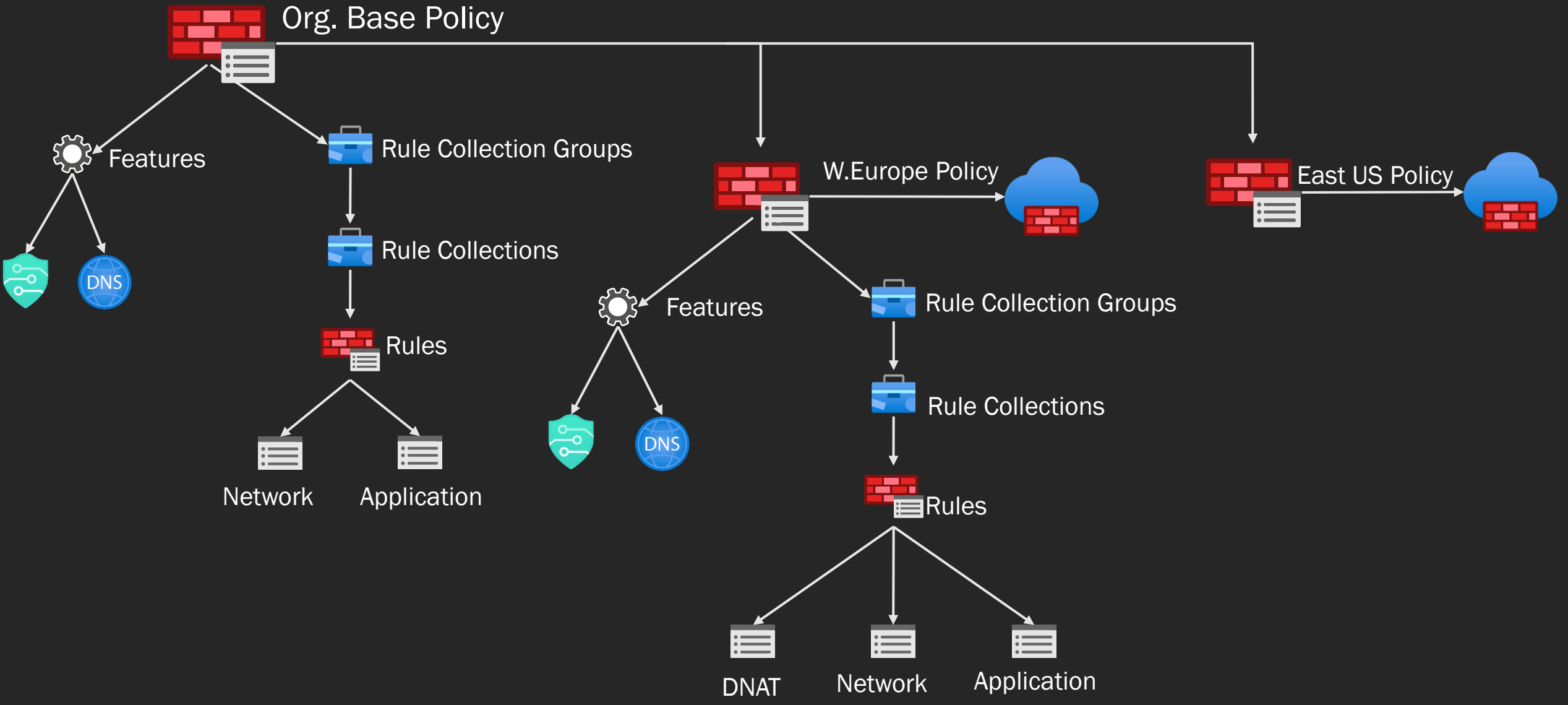
Standalone Management



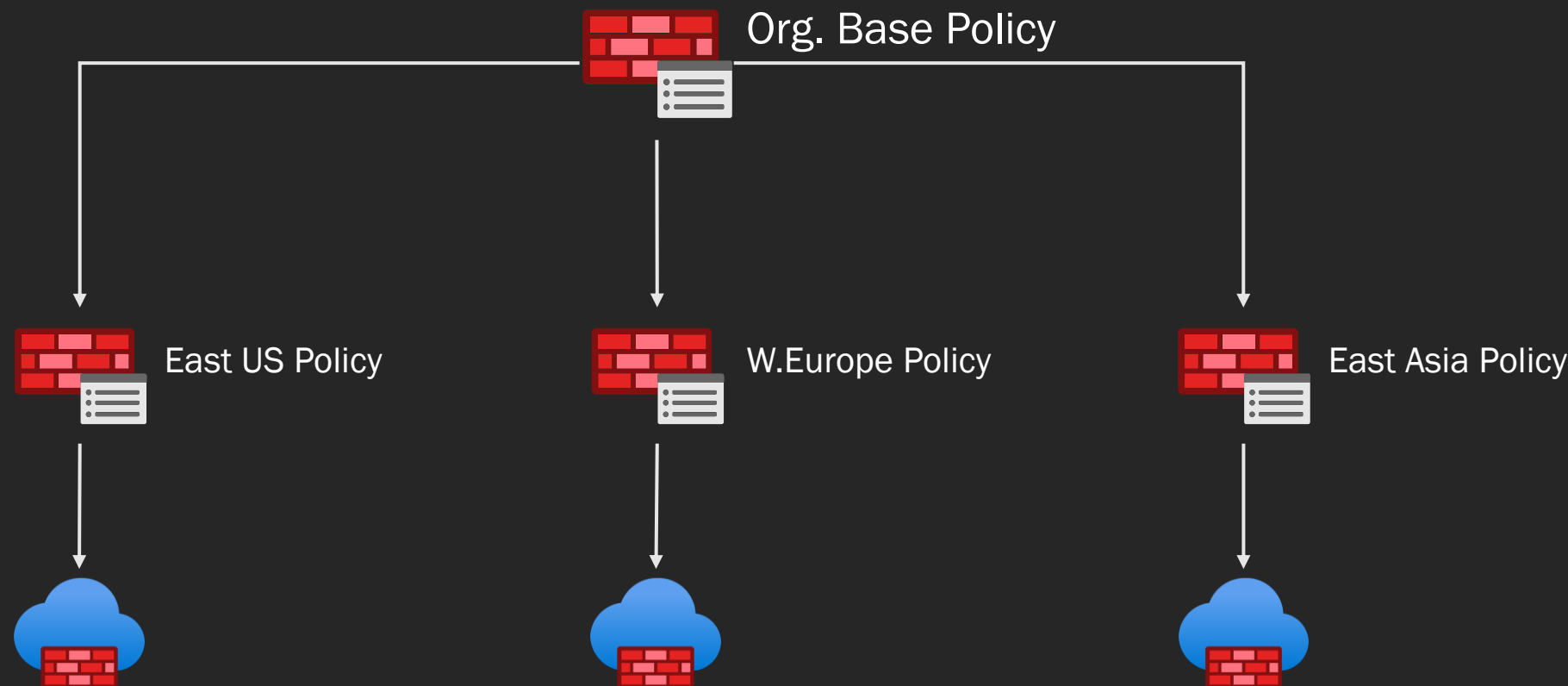
Firewall Manager



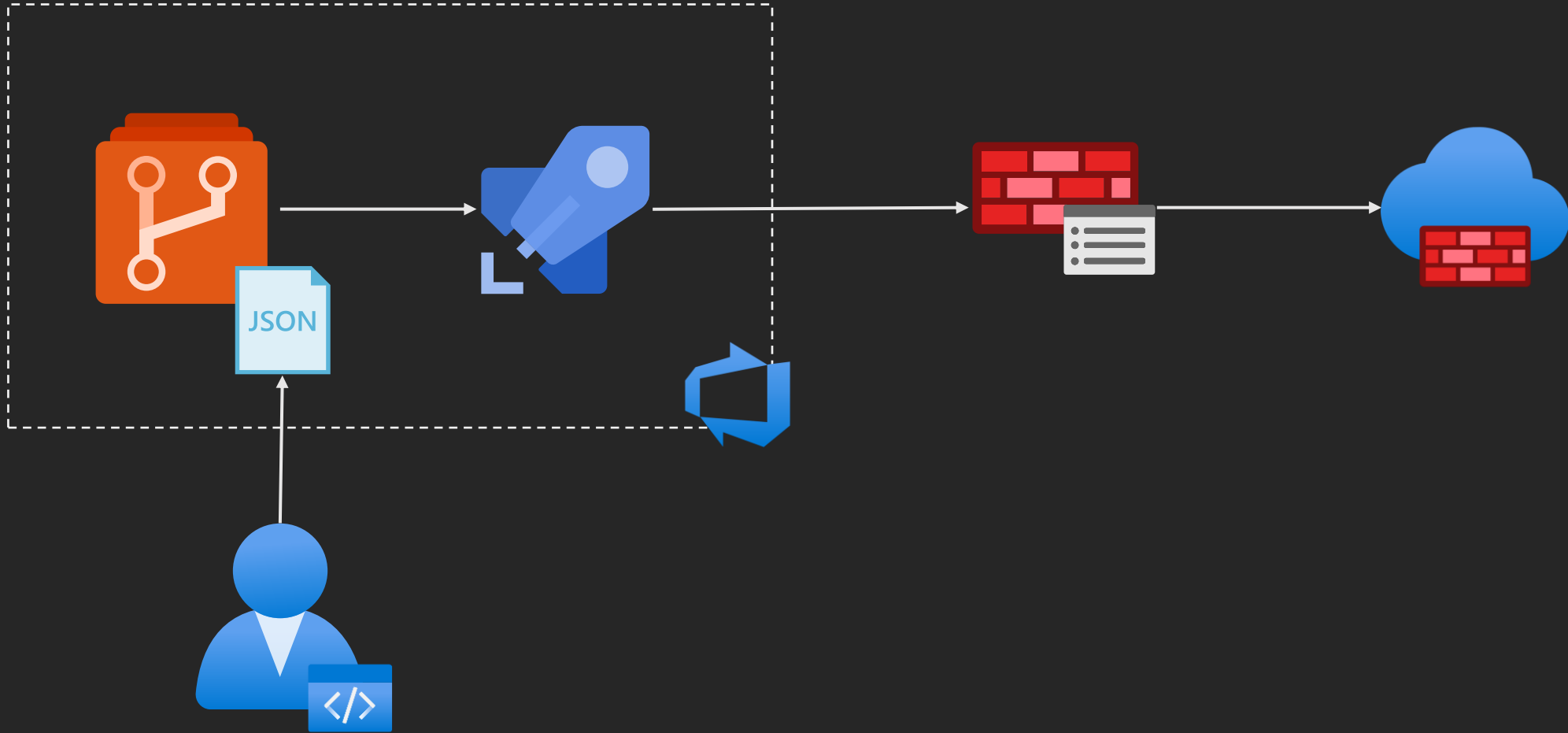
Firewall Manager



Firewall Policy Hierarchy



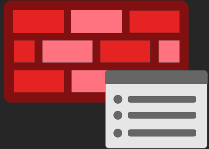
DevOps



Firewall Rules

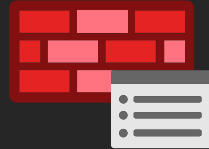
Rule Types

DNAT



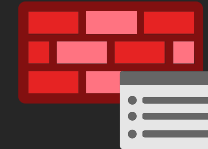
-
- Translate and filter inbound Internet traffic.
 - Implicitly adds a corresponding network rule.

Network



-
- TCP, UDP, ICMP, ANY
 - Destinations – IP Address, IP Groups, ServiceTag, FQDN
 - Inbound & Outbound

Application



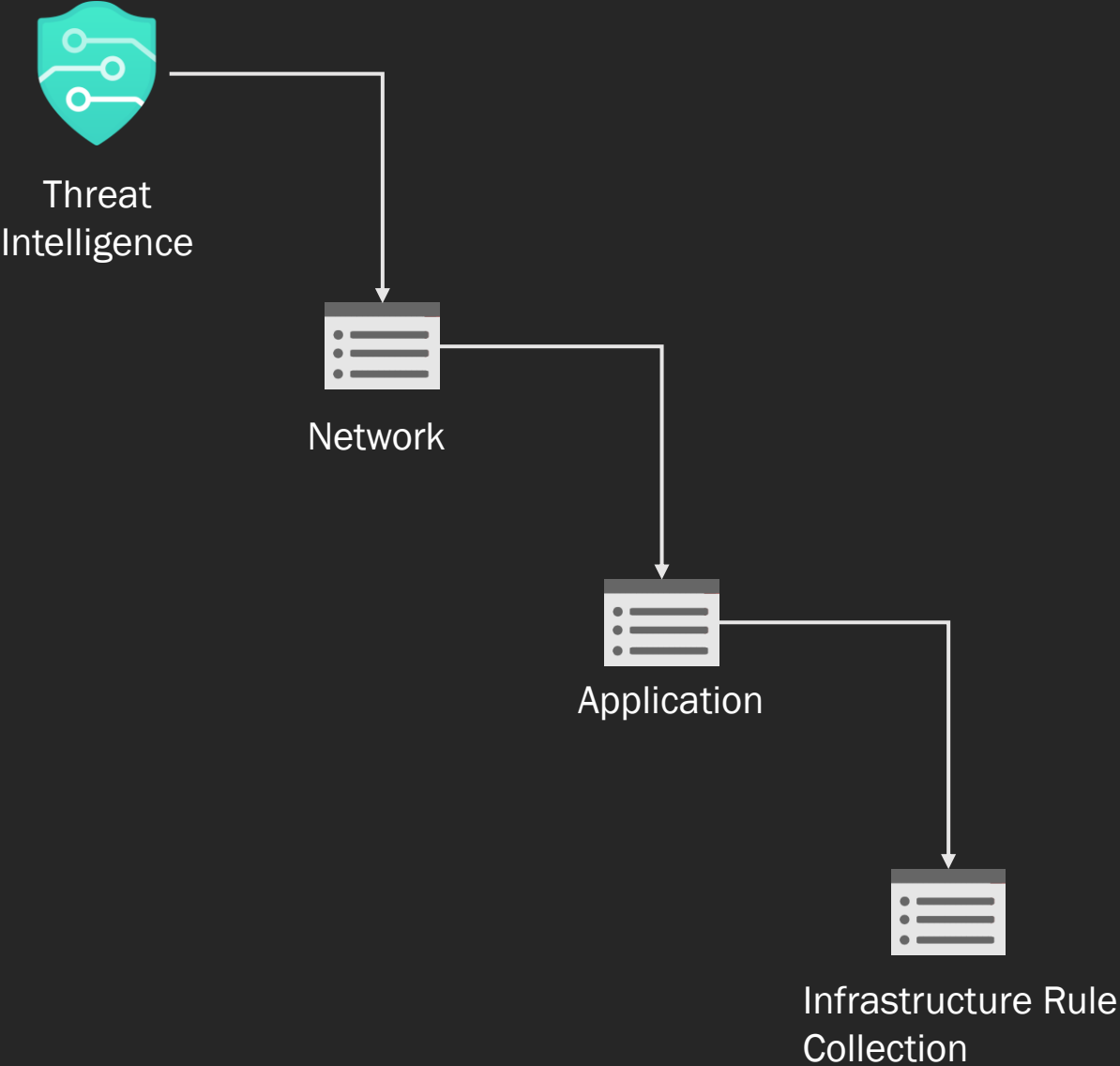
-
- HTTP, HTTPS, MSSQL
 - Destinations – FQDN, FQDN Tags
 - Outbound Only

IP Groups



```
1  resource ipGroup 'Microsoft.Network/ipGroups@2020-11-01' = {  
2      name: 'OnPremises-IpGroup'  
3      location: resourceGroup().location  
4      properties:{  
5          ipAddresses:[  
6              '192.168.0.0/24'  
7              '172.16.0.0/12'  
8          ]  
9      }  
10 }
```

Outbound - Rule processing order



Outbound - Rule processing logic

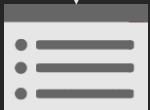
Rule
Collection



Name	Allow-web
Type	Network
Priority	200
Action	Allow

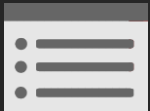


Rules

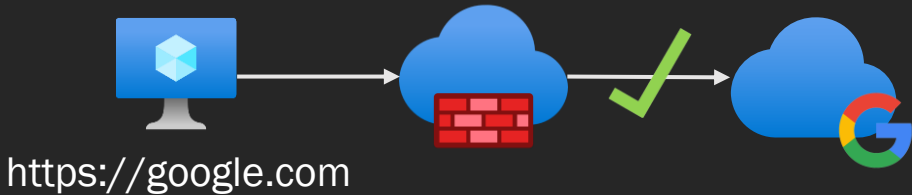


Name	Source	Protocol	Destination ports	Destination
HTTP	10.10.0.0/24	TCP	80	*
HTTPS	10.10.0.0/24	TCP	443	*

Rule
Collection



Name	Deny-google
Type	Application
Priority	100
Action	Deny

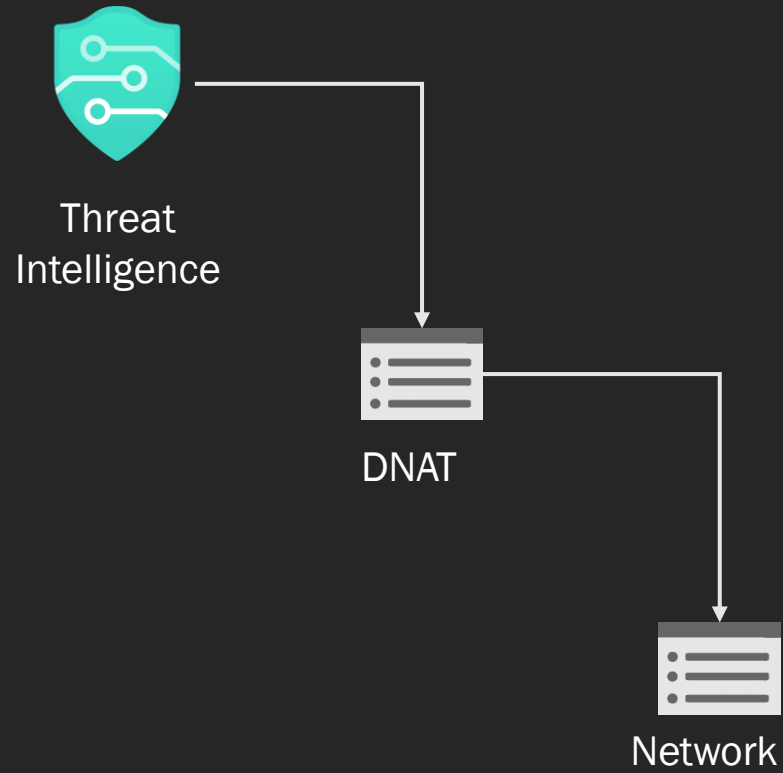


Rules



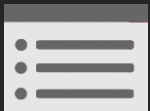
Name	Source	Protocol:Port	Target FQDNs
HTTP	10.10.0.0/24	http:80,https:443	google.com

Inbound - Rule processing order



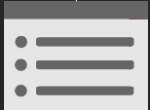
Inbound - Rule processing logic

Rule
Collection



Name	Allow-FTP
Type	DNAT
Priority	100

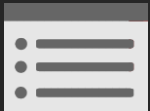
Rules



Name	Source	Protocol	Dest. ports	Destination	Translated address	Translated port
FTP	*	TCP	21	FW PiP	10.10.0.8	21



Rule
Collection

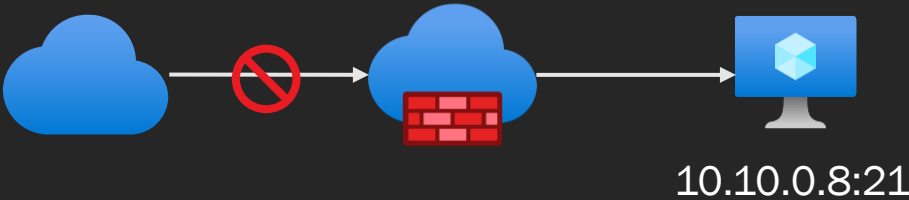


Name	Override-FTP-NAT
Type	Network
Priority	100
Action	Deny

Rules

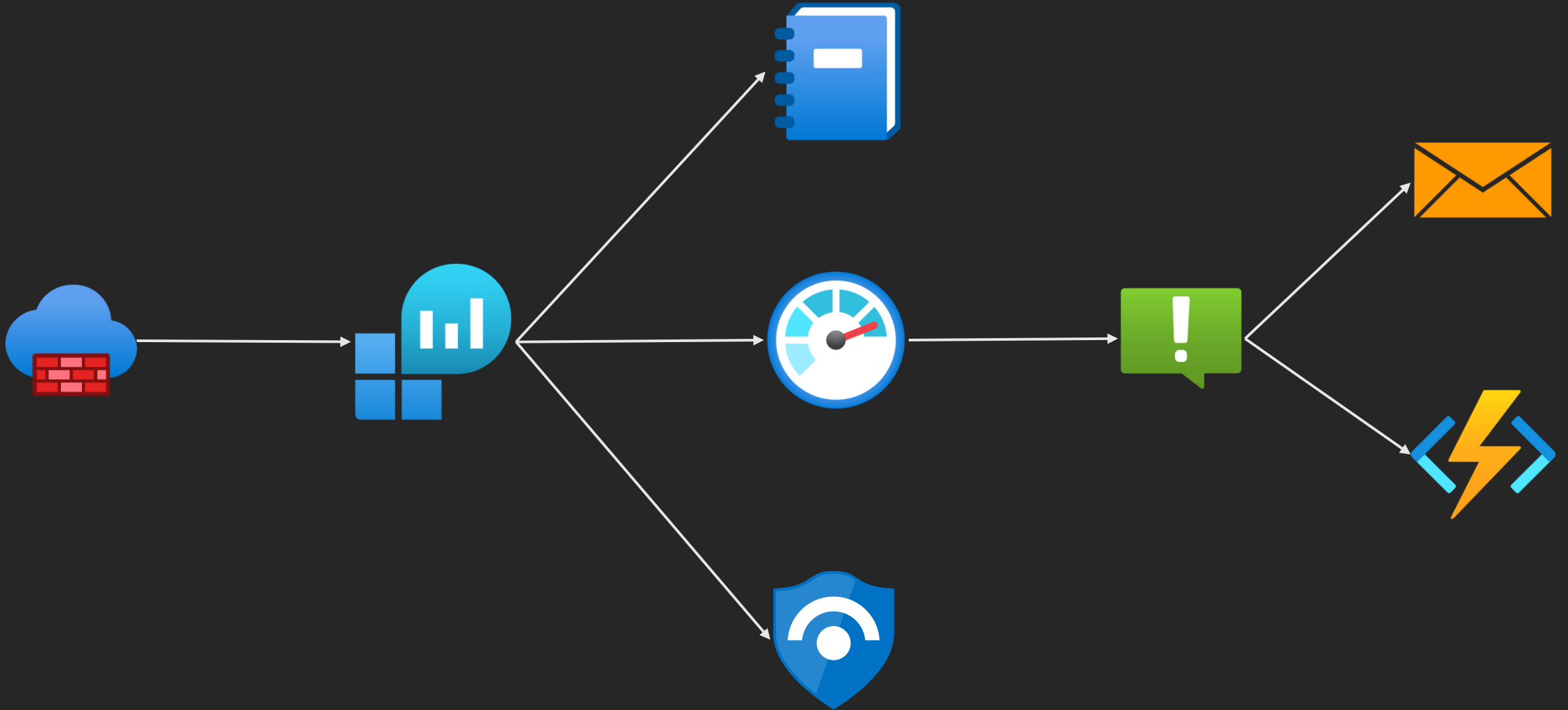


Name	Source	Protocol	Destination ports	Destination
FTP	*	TCP	21	10.10.0.8

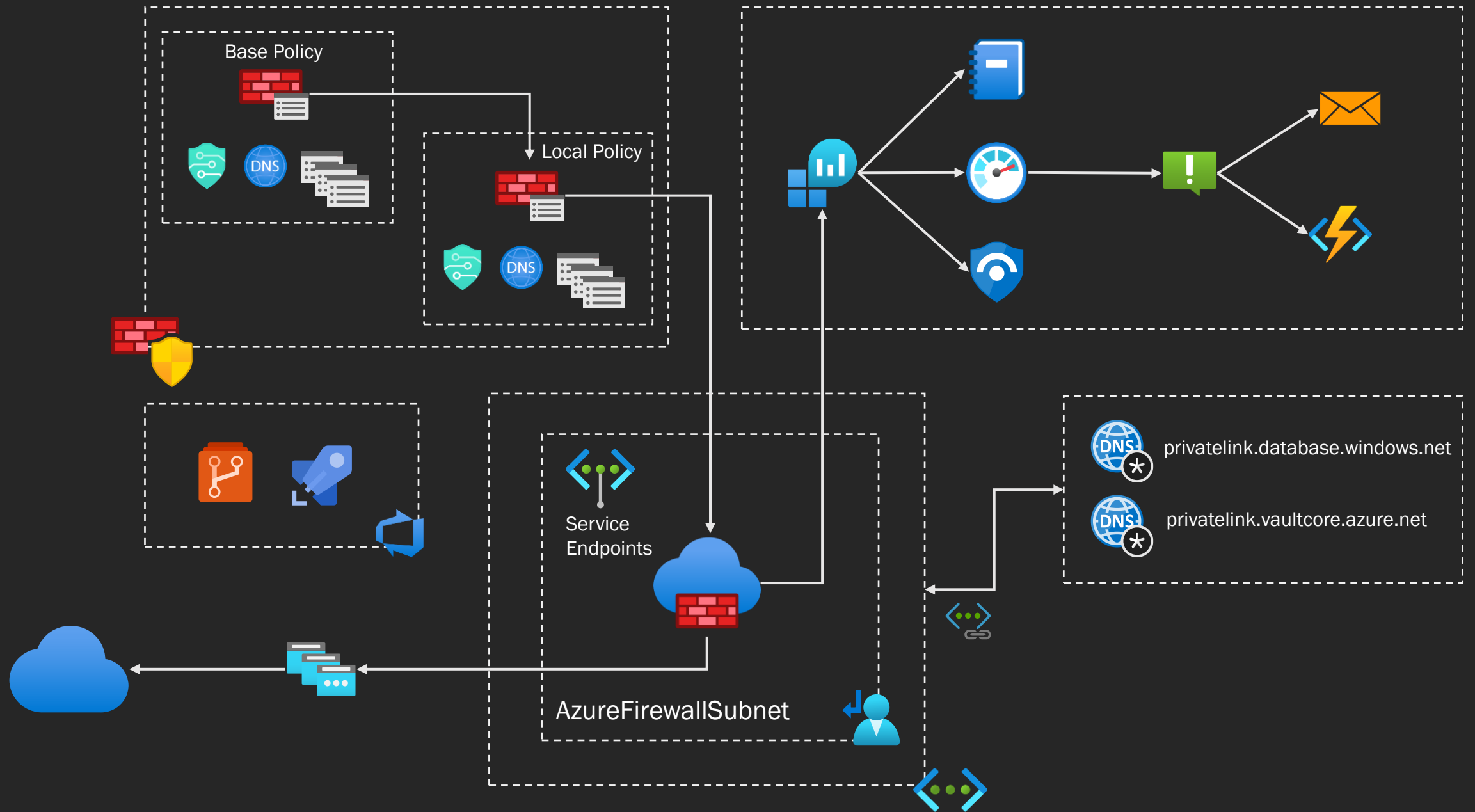


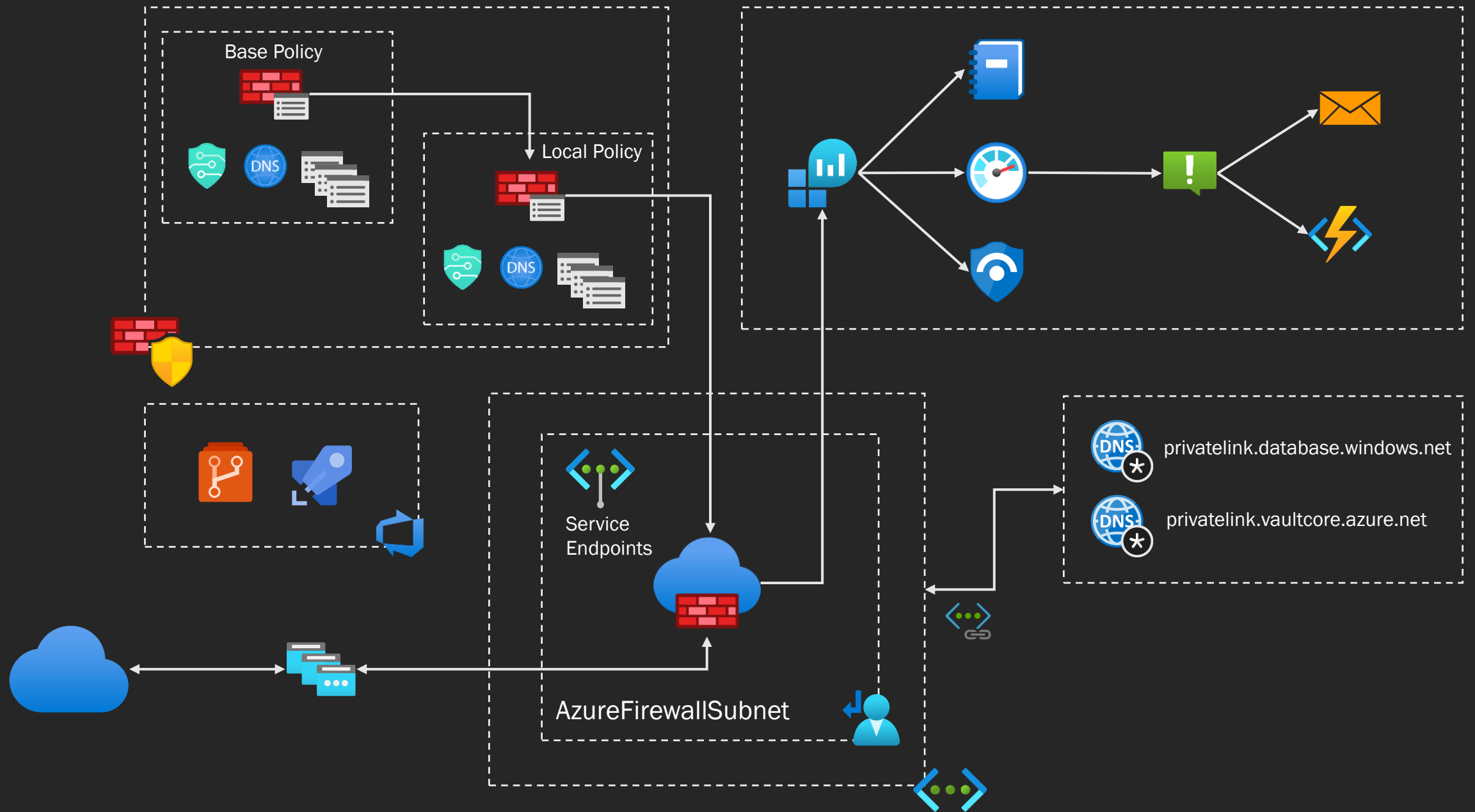
Monitoring

Monitoring and logs



Putting it all together!





Template Deployment

Navigating the docs

Questions?

Thank you!

 stefan@ivemo.se

 blog.ivemo.se

 StefanIvemo

 @StefanIvemo