Microsoft

Jak postavit Enterprise grade síťovou infrastrukturu z pohledu bezpečnosti, správy a integrace s on-premises prostředím

Tomáš Kubica

3. – 5. 4. 2019

Microsoft

Kompletní lab si můžete vyzkoušet sami

https://github.com/tkubica12/azure-networking-lab

Microsoft

Enterprise networking v Azure (1)

- Propojte svoji síť s Azure s využitím Azure VPN nebo Azure Virtual WAN
- Segmentujte prostředky s Network Security Group
- Vytvořte privilegovanou pracovní stanici (jump server) pro vyšší bezpečnost
- Balancujte provoz na servery s Azure Load Balancer Standard

Microsoft

Enterprise networking v Azure (2)

- Oddělte projekty do separátních subskripcí a VNETů. Vytvořte sdílenou subskripci s VPN, AD, firewall, reverse proxy a připojte ostatní subskripce přes VNET peering
- Filtrujte provoz mezi projekty a řiďte outbound pravidla do Internetu centrálně s Azure Firewall
- Vystavujte aplikace do Internetu přes Azure Application Gateway (reverse proxy a WAF)

Microsoft

Enterprise networking v Azure (3)

- Globální aplikace vystavujte přes Azure Front Door
- Pokud potřebujete, použijte appliance třetích stran (Linux, Cisco, Palo Alto, Checkpoint, Barracuda, F5, Fortinet, …)
- Spravujte síť a analyzujte provoz s Azure Monitor včetně packet capture, traffic analytics nebo network performance monitoring

Microsoft

Jak na PaaS služby (1)

- Některé PaaS služby se nasazují ve VNETu a můžete nejen mluvit z nich, ale i připojovat se na ně, nicméně management je public – Azure Kubernetes Service, Azure Container Instances, Application Service Environment, API Management Premium, Integration Services Environment, Azure SQL Managed Instance, …
- Platí pro ně tedy stejná pravidla jako pro IaaS, ale musíte povolit přístup cloudu do nich pro management
- Mohou znamenat vyšší náklady, protože jsou single-tenant (nevyužijete výnosy z rozsahu – například ASE vs App Service)
- Mohou komunikovat s VNETem a dá se k nim přistupovat přes VPN

Microsoft

Jak na PaaS služby (2)

- Některé PaaS služby nasazují worker nody ve VNETu, ale frontend a management je public – Application Services
- WebApp worker je ve VNETu a může přímo komunikovat s prostředky ve VNETu, za VPN nebo připojené servisní endpointy (o tom později)
- Náhrada předchozího řešení s P2S VPN
- Nicméně přístup uživatelů (frontend) je na public endpointu

Microsoft

Jak na PaaS služby (3)

- Většina PaaS služeb sice běží na public endpointu, ale umožňuje vytvořit tunel mezi VNETem a službou pro privátní přístup a vypnout či omezit přístup z Internetu – to se jmenuje Service Endpoint
- Azure SQL, Azure Key Vault, Cosmos DB, Azure MySQL, Azure PostgreSQL, Azure Service Bus, …
- Adresa je ale i nadále public, nicméně nereaguje na přístup zvenku, pokud nechcete
- Toto řešení nefunguje přes VPN! Z onpremises musíte zvenku.

Microsoft

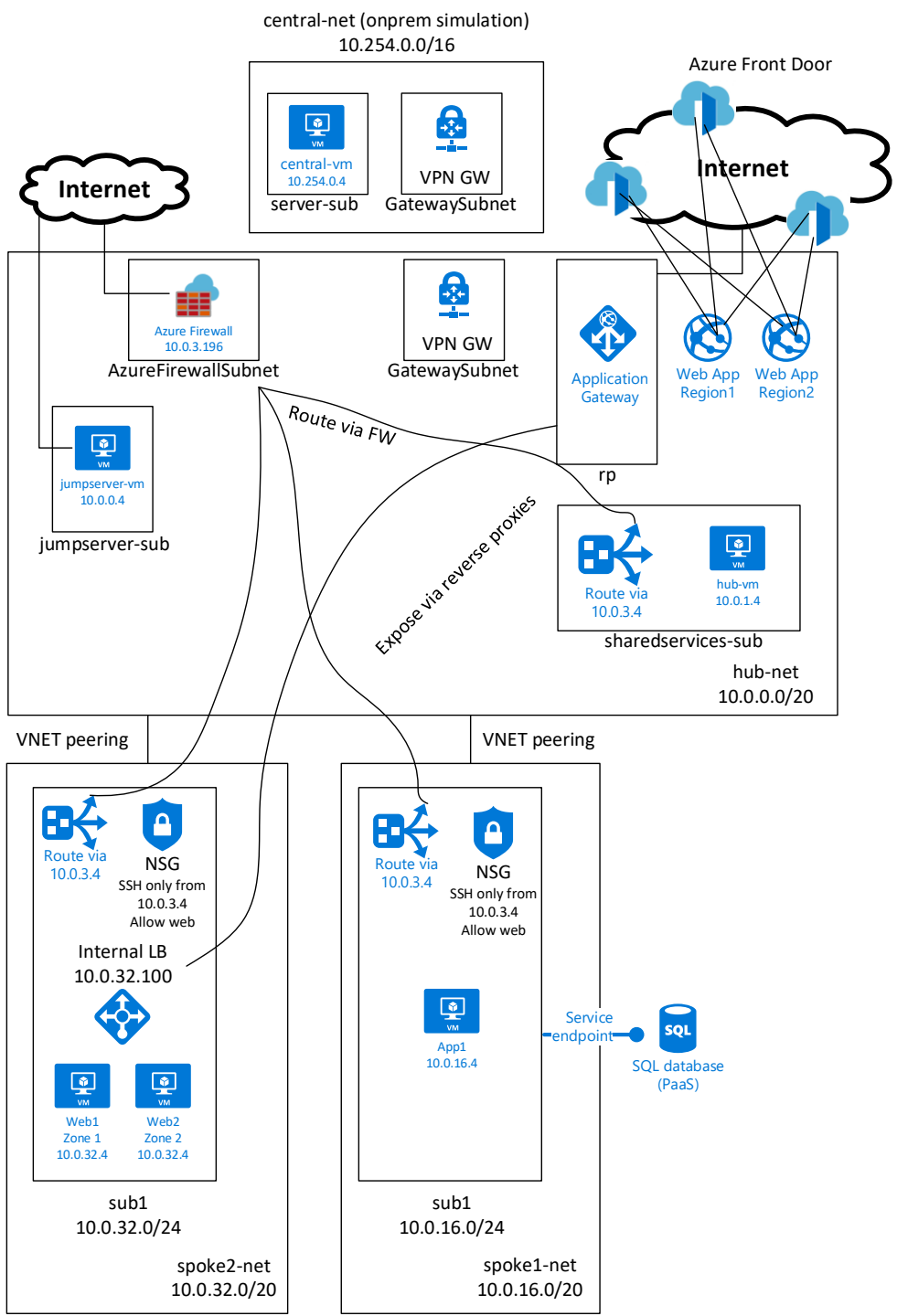
Express Route

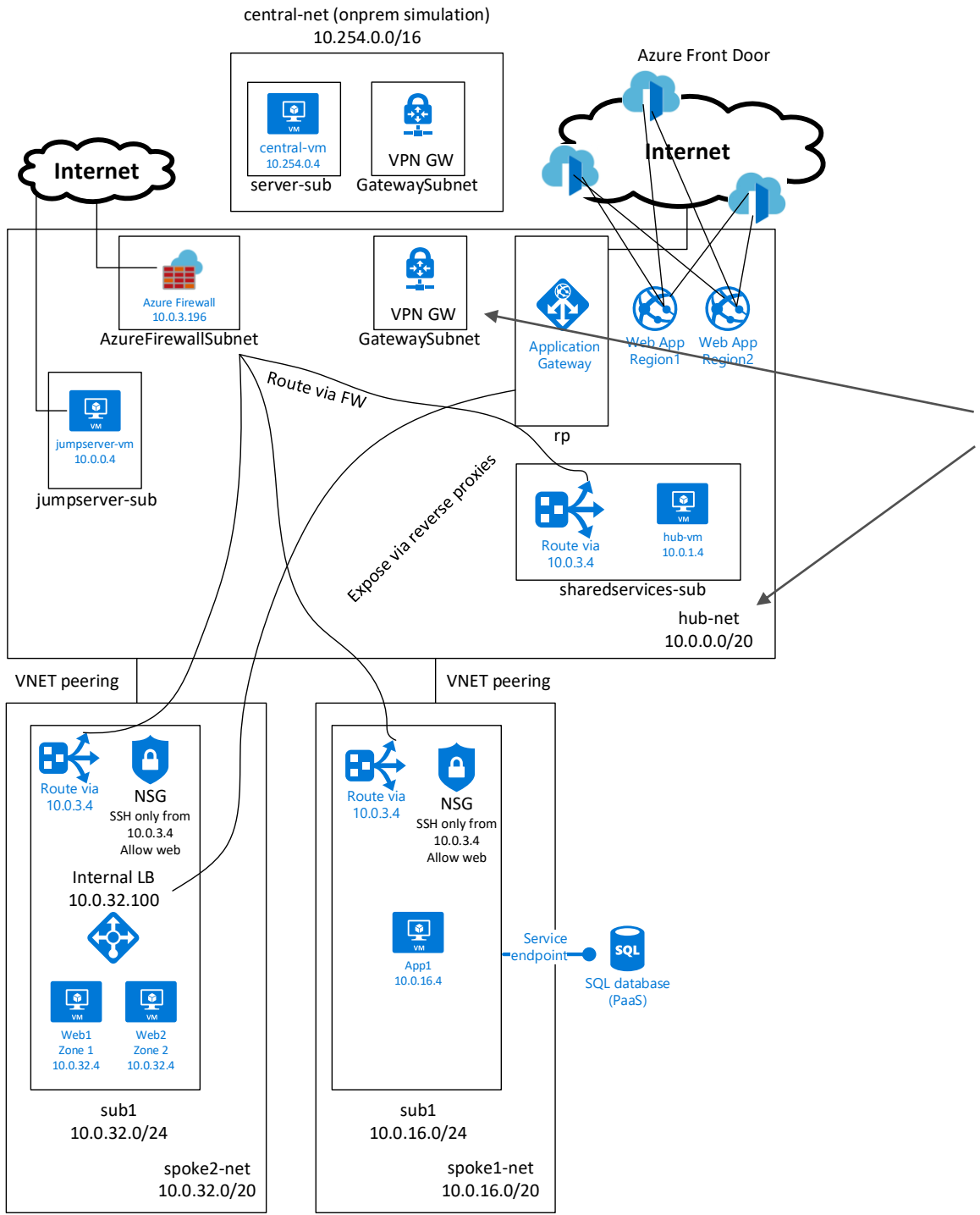
- Pronajatý okruh pro přímé spojení vás s Microsoft sítí přes operátora
- Private peering – alternativa k VPN (můžete použít Azure VPN pro zálohu)
- Microsoft peering – komunikace na úrovni public IP adres, řešení pro poslání PaaS služeb přes privátní linku (nepoužívejte pro Office365!)

Microsoft

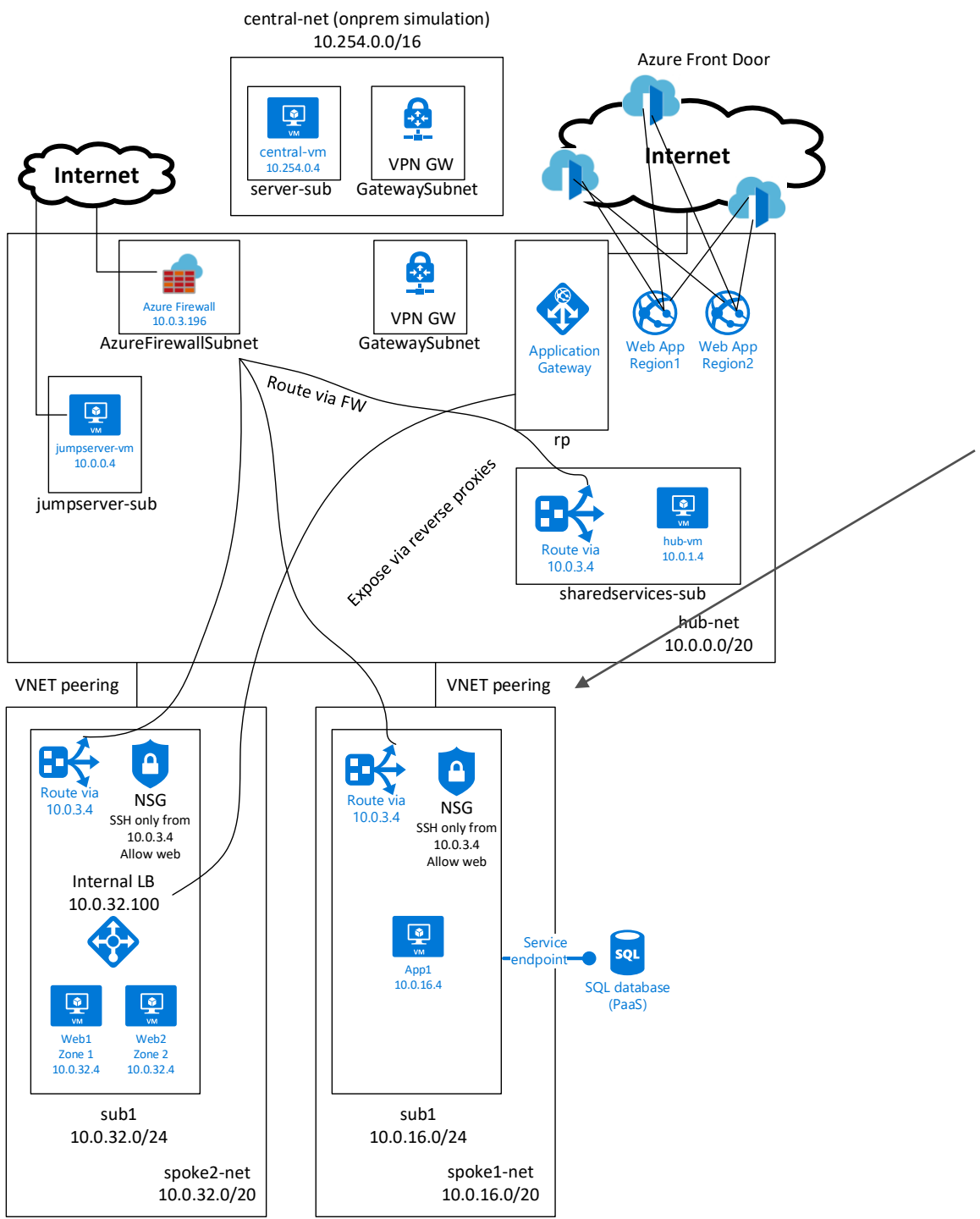
Express Route

- ER je bránou do Microsoft sítě – jedna ER vám dá přístup do celé Evropy a s Premium SKU do celého světa
- ER můžete namapovat na vícero VNETů i v různých tenantech
- Azure Virtual WAN je alternativou nebo doplňkem ER pro rozsáhlé celoplanetární sítě postavené na SD-WAN

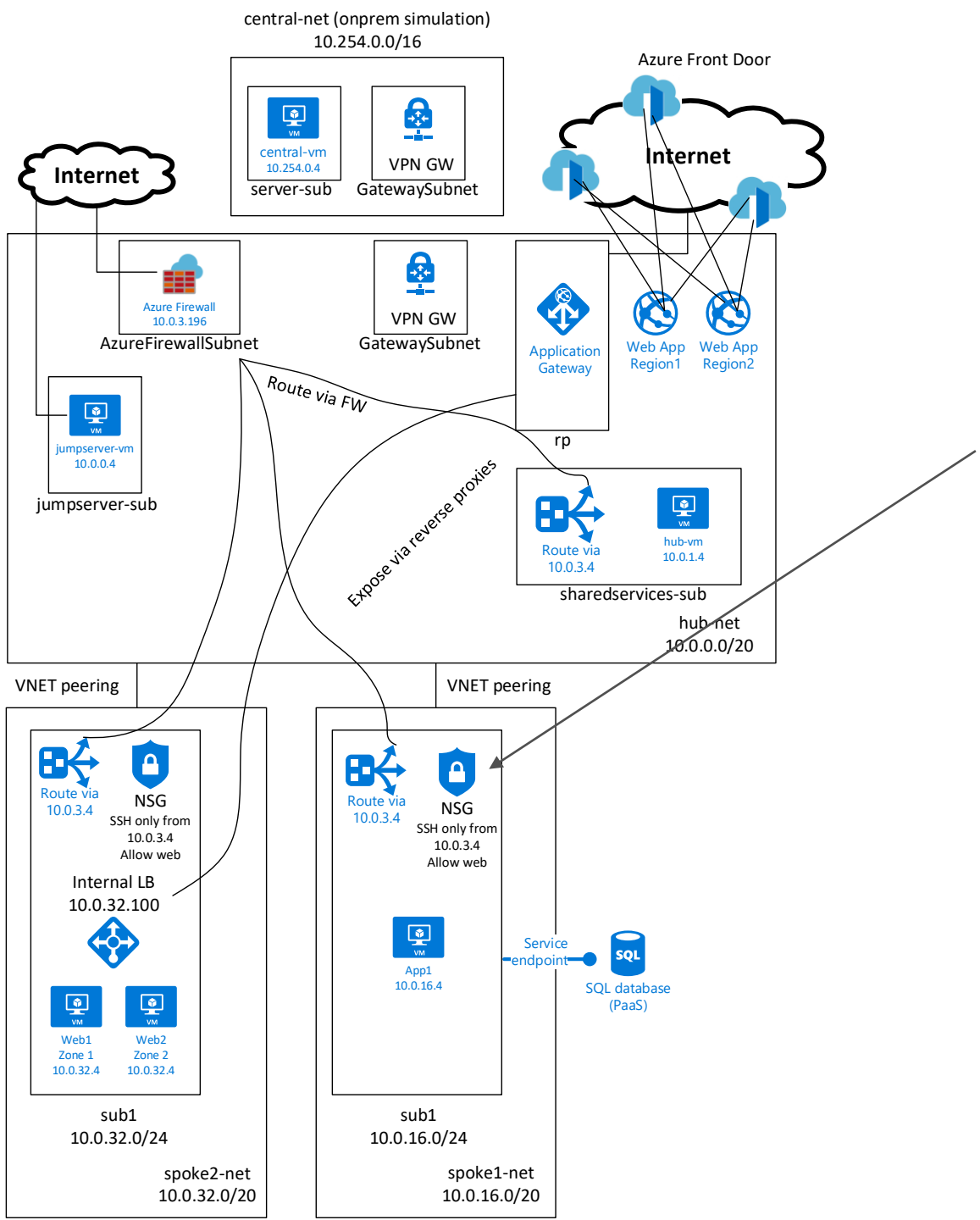

central-net (onprem simulation)
10.254.0.0/16
central-vm
10.254.0.4
server-sub
VPN GW
GatewaySubnet
Azure Front Door
Internet
Internet
Azure Firewall
10.0.3.196
AzureFirewallSubnet
VPN GW
GatewaySubnet
Application Gateway
Web App Region1
Web App Region2
jumpserver-vm
10.0.0.4
jumpserver-sub
Route via FW
rp
Expose via reverse proxies
Route via
10.0.3.4
hub-vm
10.0.1.4
sharedservices-sub
hub-net
10.0.0.0/20
VNET peering
VNET peering
Route via
10.0.3.4
NSG
SSH only from
10.0.3.4
Allow web
Internal LB
10.0.32.100
Web1
Zone 1
10.0.32.4
Web2
Zone 2
10.0.32.4
sub1
10.0.32.0/24
spoke2-net
10.0.32.0/20
Route via
10.0.3.4
NSG
SSH only from
10.0.3.4
Allow web
App1
10.0.16.4
Service endpoint
SQL
SQL database
(PaaS)
sub1
10.0.16.0/24
spoke1-net
10.0.16.0/20



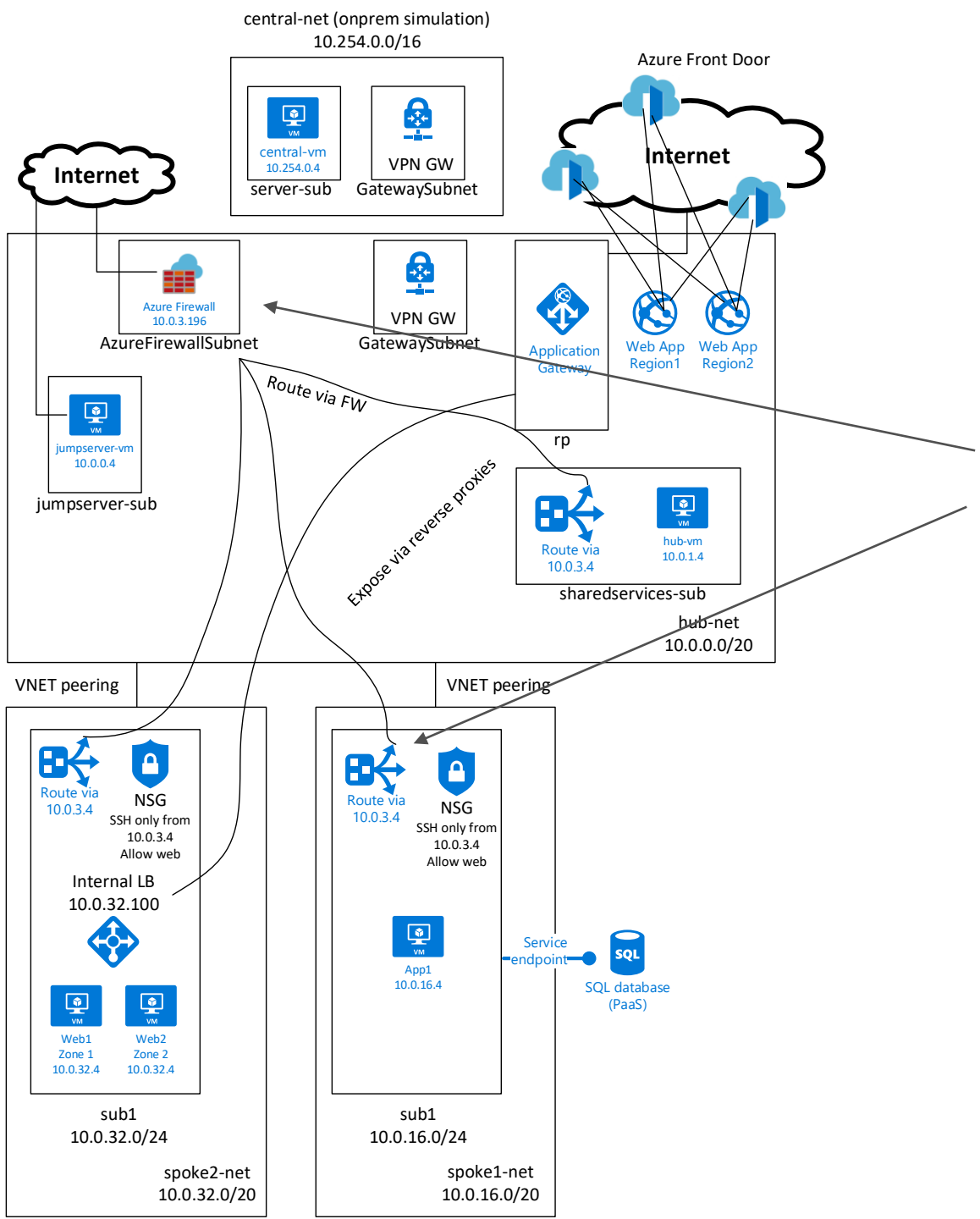
Máme VNET a připojení do on-premises přes zone-redundant VPN



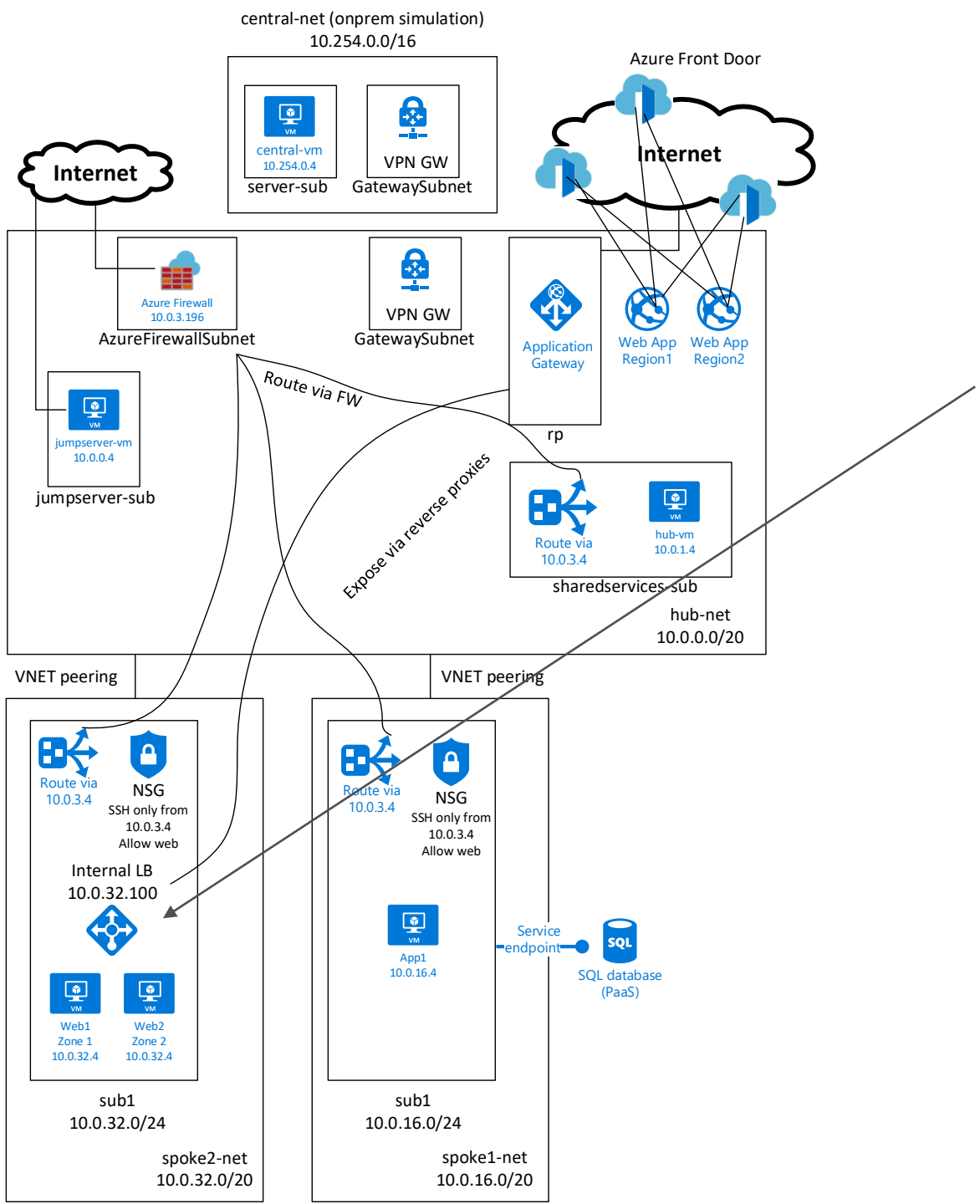
Hub-and-spoke topologie



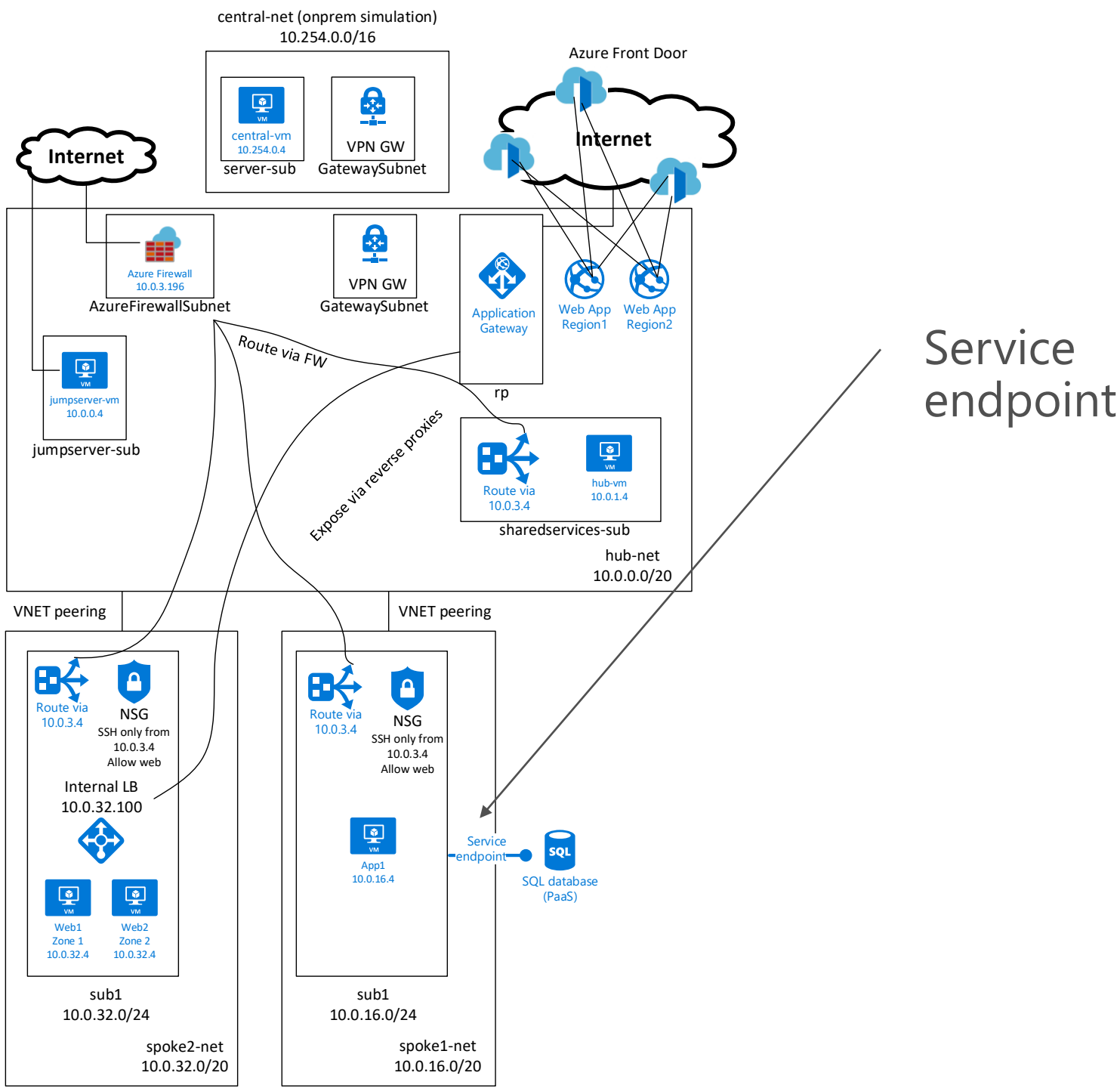
Network Security Group pro segmentaci

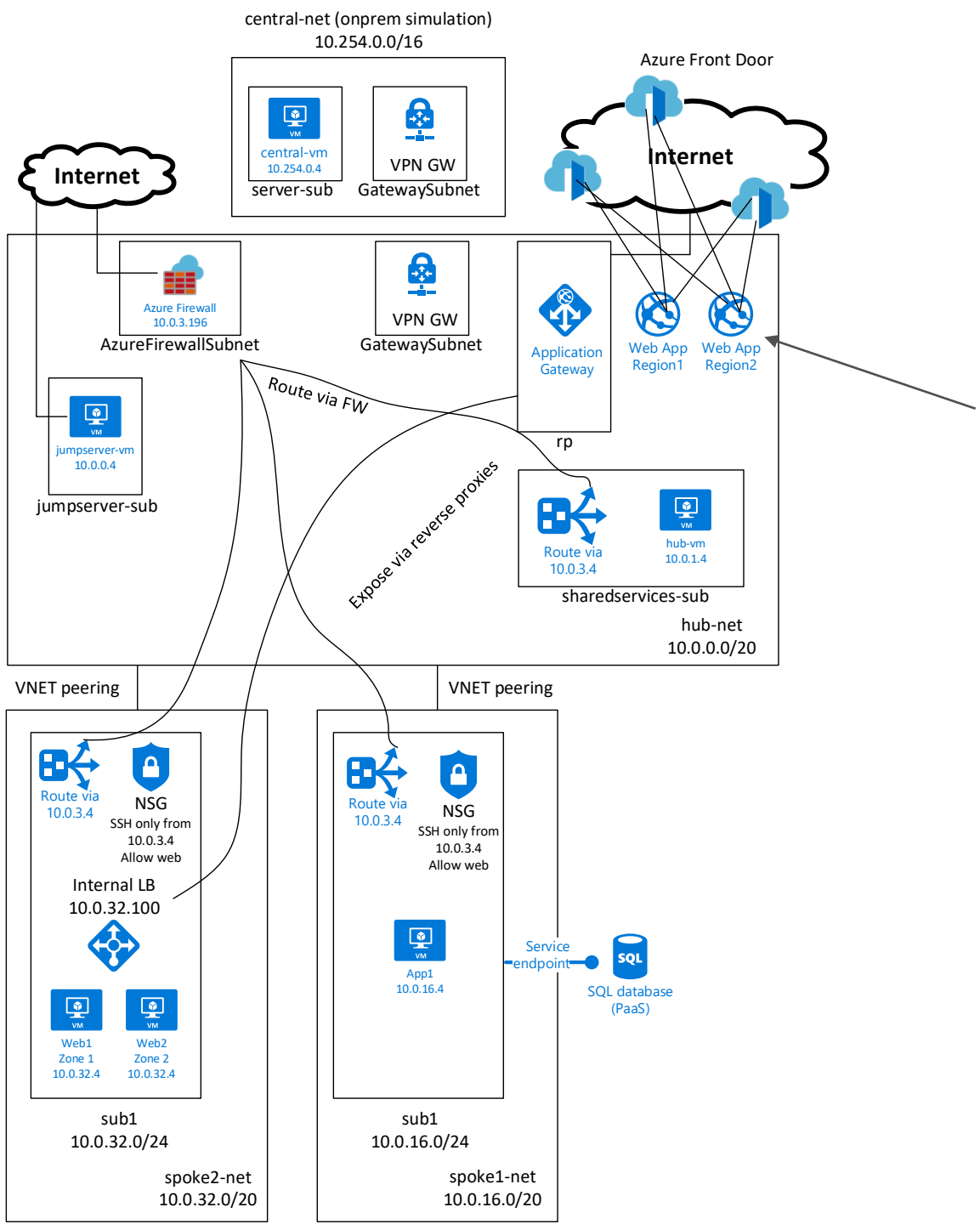


Centrální firewall pro outbound

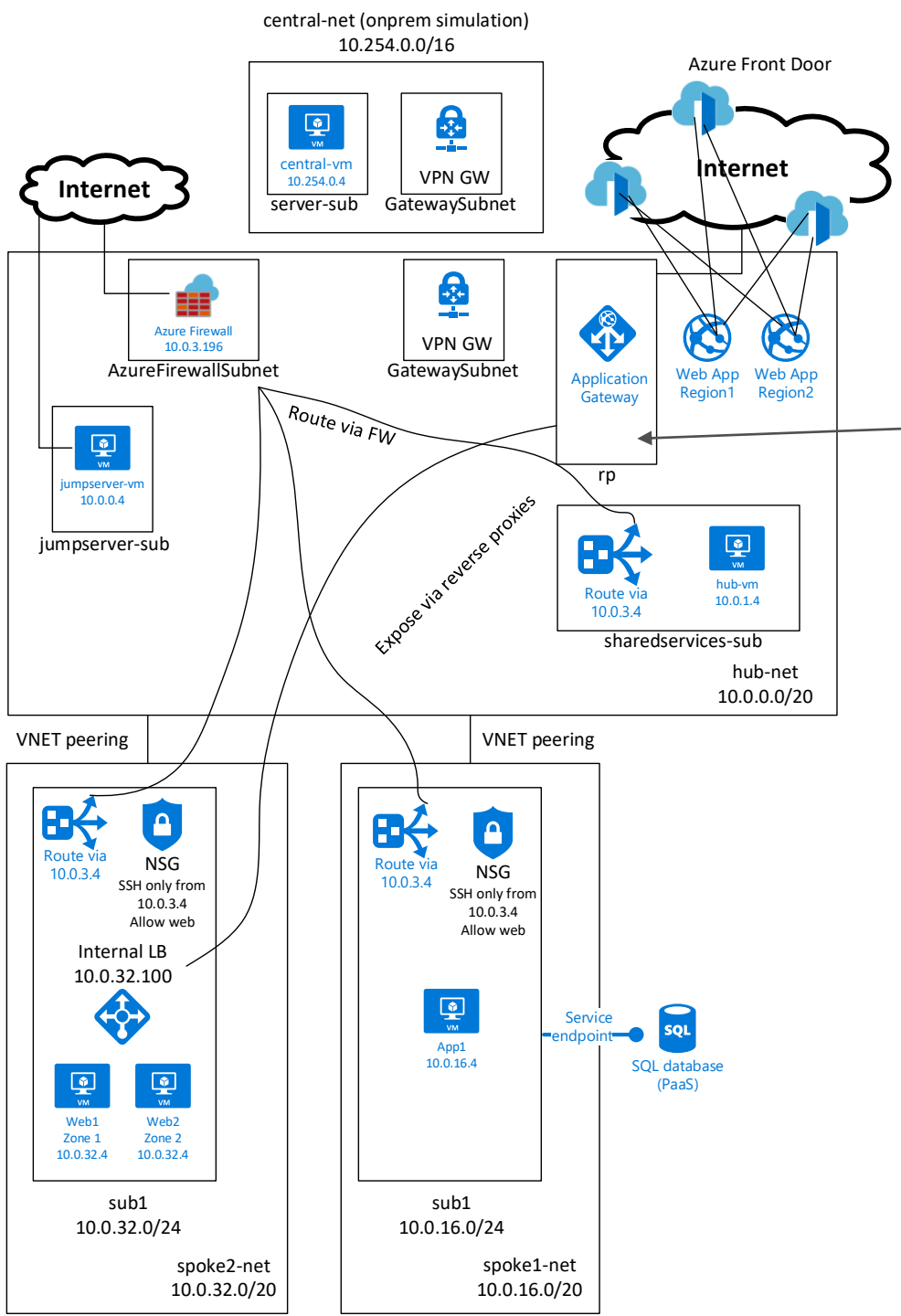


Load balancer, zone redundant

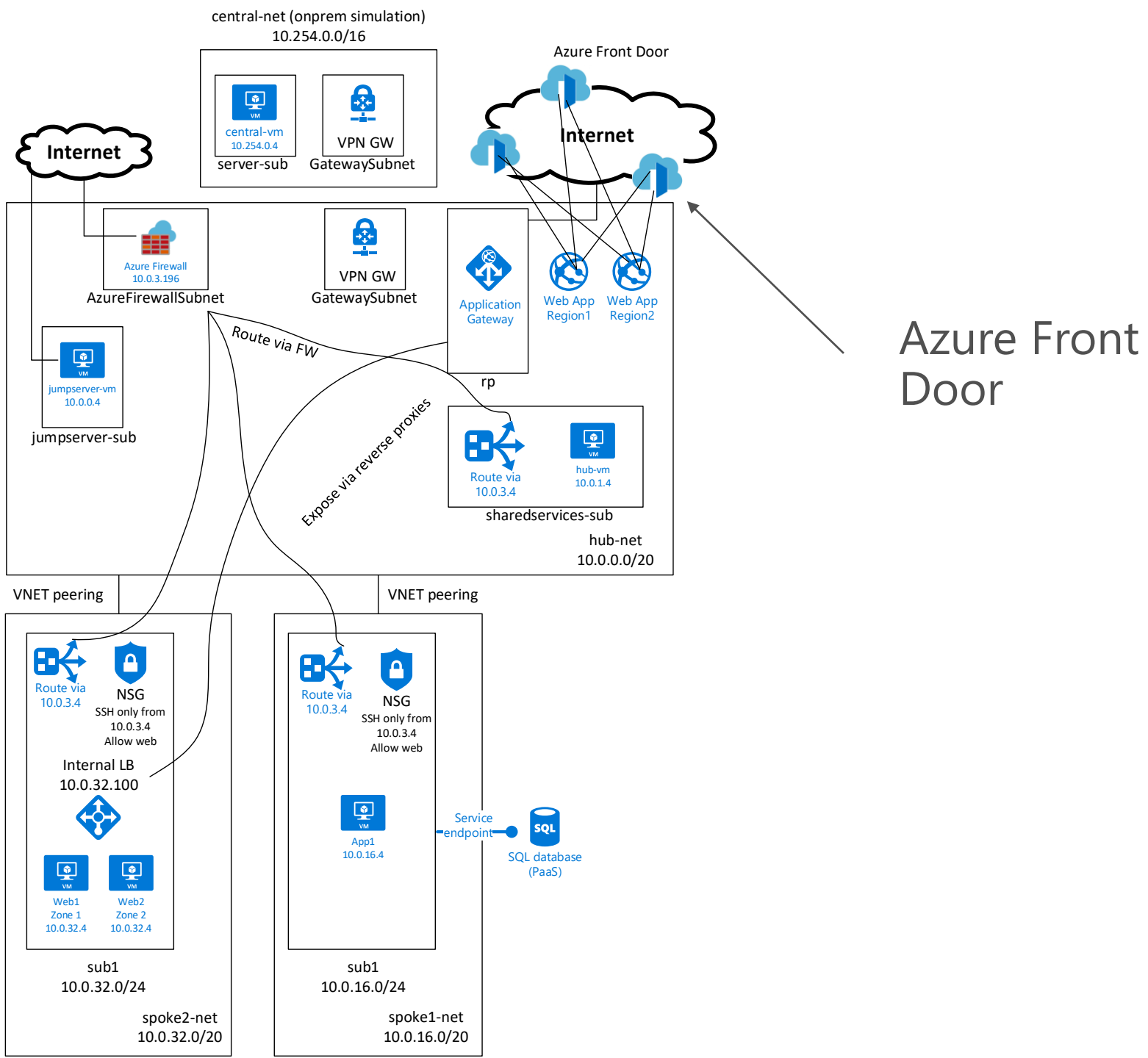

central-net (onprem simulation)
10.254.0.0/16
central-vm
10.254.0.4
server-sub
VPN GW
GatewaySubnet
Azure Front Door
Internet
Internet
Azure Firewall
10.0.3.196
AzureFirewallSubnet
VPN GW
GatewaySubnet
Application Gateway
Web App Region1
Web App Region2
jumpserver-vm
10.0.0.4
jumpserver-sub
Route via FW
rp
Expose via reverse proxies
Route via
10.0.3.4
hub-vm
10.0.1.4
sharedservices-sub
hub-net
10.0.0.0/20
VNET peering
VNET peering
Route via
10.0.3.4
NSG
SSH only from
10.0.3.4
Allow web
Internal LB
10.0.32.100
Web1
Zone 1
10.0.32.4
Web2
Zone 2
10.0.32.4
sub1
10.0.32.0/24
spoke2-net
10.0.32.0/20
Route via
10.0.3.4
NSG
SSH only from
10.0.3.4
Allow web
App1
10.0.16.4
Service endpoint
SQL
SQL database
(PaaS)
sub1
10.0.16.0/24
spoke1-net
10.0.16.0/20
Service endpoint



App Service VNET integration



Reverse proxy
s WAF



Azure Front Door

Microsoft

Azure vám umožňuje postavit komplexní Enterprise-grade networking, pokud to potřebujete.