Take Networking to the Next Level

ExpressRoute, VPN Gateway, Private Link și arhitecturi hub-spoke — Ghid didactic zero-to-hero pentru Azure Portal

Material complet pentru cursanți și ingineri de rețea care vor să înțeleagă nu doar cum se face deploy, ci și **de ce fiecare serviciu există, când se alege și cum se combină** într-o arhitectură enterprise.

WEBINAR 2026 | MICROSOFT AZURE | ZERO-TO-HERO

Arhitectură de referință: Hub-Spoke cu ExpressRoute

Model didactic pentru organizații care combină conectivitate hibridă, izolare și acces privat la servicii.

Hub = nod central

Conectivitate, securitate și servicii comune centralizate într-un singur VNet.

Spoke-uri = workload-uri

Găzduiesc aplicațiile și pot folosi gateway-ul din hub prin **gateway transit**.

Private Endpoint

Publică un IP privat în subnetul ales; traficul **nu iese pe internet**.

Reziliență hibridă

ExpressRoute și VPN pot coexista pentru reziliență sau pentru site-uri diferite.

De ce contează acest material

Analogia orașului

Dacă Azure Firewall este paznicul central al traficului, atunci ExpressRoute, VPN Gateway, Private Link și hub-spoke sunt **drumurile, tunelurile, intrările private și planul orașului**. Fără ele, o infrastructură cloud poate funcționa, dar nu este ușor de extins, securizat și operat la scară.

Analogii simple

- **ExpressRoute** — autostradă privată închiriată între compania ta și cloud.
- **VPN Gateway** — tunel securizat prin drumurile publice ale internetului.
- **Private Link** — ușă laterală privată direct în clădirea unui serviciu Azure, fără intrarea publică.
- **Hub-spoke** — aeroport central cu terminale: un hub comun și mai multe zone specializate.

Un serviciu poate fi perfect implementat la nivel de aplicație, dar dacă rutarea, DNS-ul, conectivitatea hibridă și izolarea de rețea sunt proiectate slab, apar exact problemele care dor în viața reală: **latență, downtime, timeouts, rezolvare DNS inconsistentă, troubleshooting dificil și costuri operaționale inutile.**

Ce problemă rezolvă fiecare serviciu

Înainte de a intra în detalii tehnice, este esențial să înțelegi rolul fiecărui serviciu și când îl alegi.

Serviciu	Analogie	Ce face bine	Când îl alegi
ExpressRoute	Autostradă privată	Conectivitate privată, stabilă, predictibilă, BGP, latență mai bună	Ai datacenter / MPLS și vrei conectivitate enterprise
VPN Gateway	Tunel securizat	Criptează traficul IPsec; bun pentru filiale și backup	Vrei timp rapid de implementare și cost mai mic
Private Link	Intrare privată dedicată	Expune un serviciu PaaS prin IP privat în VNet	Vrei acces privat la Storage, SQL, Key Vault, App Service
Hub-Spoke	Aeroport central	Centralizează gateway, firewall, DNS, monitorizare și politici	Ai mai multe workload-uri și vrei guvernanță clară
App Gateway	Recepție inteligentă	Reverse proxy, WAF, TLS, routing HTTP/S	Ai trafic web L7 și vrei WAF / routing pe URL
NSG	Paznic la ușa clădirii	Allow/Deny statul pentru conexiuni; micro-segmentare	Vrei micro-segmentare la nivel de VM sau subnet

Roluri principale — privire de ansamblu

ExpressRoute

Conectivitate privată între on-prem și Azure. Folosește provider și BGP; **nu este internet VPN**. Nivel: Hibrid / WAN.

VPN Gateway

Tuneluri IPsec între Azure și alte rețele. Excelent pentru filiale, backup și scenarii rapide. Nivel: L3.

Private Endpoint

IP privat în VNet pentru un serviciu. **Nu conectează rețele întregi**; conectează consumatorul la un serviciu concret.

Hub-Spoke

Model de arhitectură și guvernare. Centralizează gateway, firewall, DNS și controale comune. Nivel: Topologie.

Private Link Service

Publici propriul tău serviciu în mod privat. Necesită **Standard Load Balancer** în fața serviciului tău.

Concepte fundamentale de rețea

Înainte de orice deploy, trebuie să stăpânești aceste concepte de bază. Ele sunt fundația pe care se construiesc toate serviciile discutate.

CIDR și adresare

Alege spații de adrese care **nu se suprapun** cu on-premises sau cu alte VNets. Un design bun începe cu IP plan-ul. Dacă două rețele au prefixe care se suprapun, vei avea probleme garantate.

Subnet

Porțiune a VNet-ului. Unele servicii Azure cer subneturi dedicate — de exemplu **GatewaySubnet** pentru VPN/ExpressRoute.

Routing

Traficul urmează cea mai specifică rută. Azure combină **system routes, peering routes, BGP routes și UDR-uri**.

BGP

Protocol de rutare dinamică folosit intens de ExpressRoute și, opțional, de VPN Gateway. Permite schimb automat de rute.

Gateway transit

Permite spoke-urilor să folosească gateway-ul din hub **fără a crea gateway în fiecare spoke**. Economie și simplitate.

DNS pentru Private Endpoint

Private Endpoint fără DNS bine gândit devine rapid o sursă de confuzie. Numele trebuie să rezolve către **IP-ul privat**, nu către endpoint-ul public.

Regulă de aur: Proiectarea adresării este primul exercițiu de disciplină, nu un detaliu administrativ. Fă-o corect de la început.

Arhitectura Hub-Spoke explicată ușor

Hub — centrul de comandă

Hub-ul este locul central pentru servicii comune: gateway-uri, firewall, DNS, monitorizare, bastion, instrumente de ops. Tot ce este partajat stă aici.

Spoke — zona de workload

Spoke-urile sunt rețele separate pentru workload-uri: aplicații, date, integrare, sandbox sau medii dev/test/prod. Fiecare spoke este izolat logic.

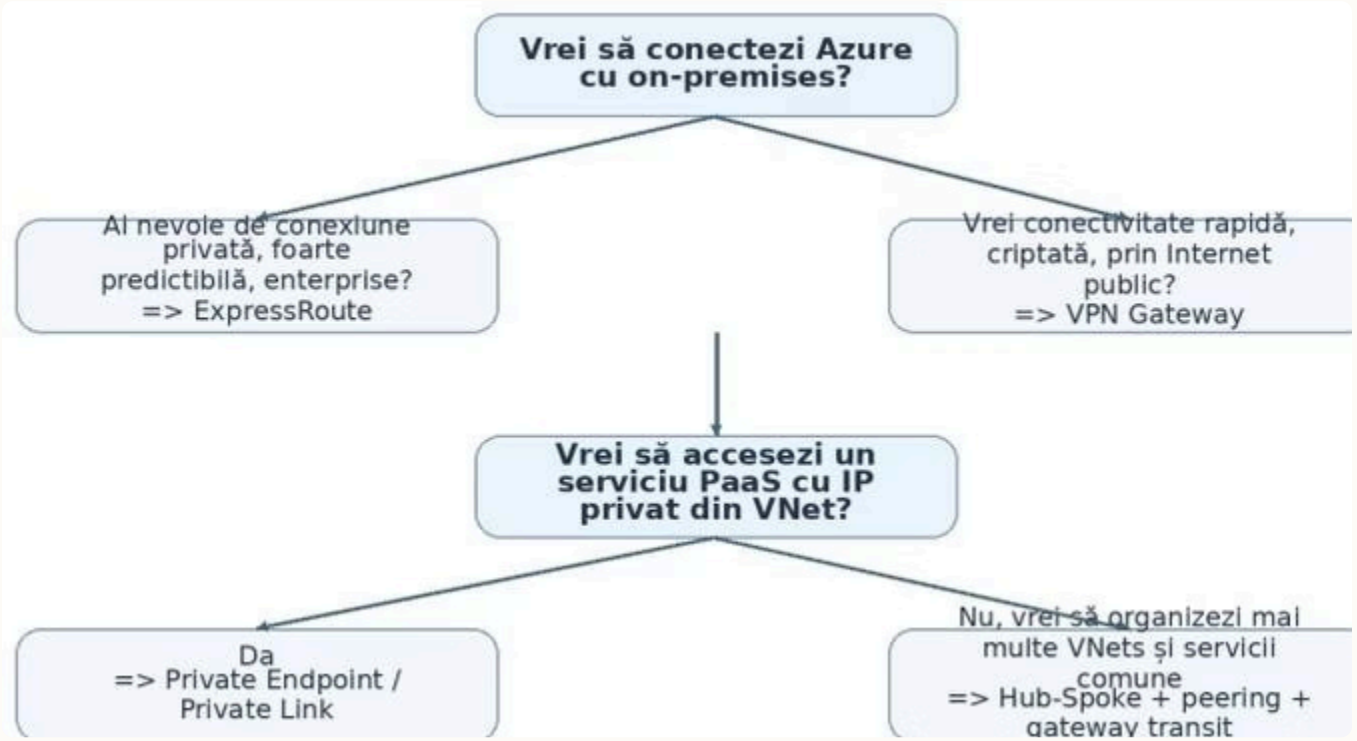
Principii cheie

- **Hub** = centralizare și guvernare
- **Spoke** = izolare logică și limitarea blast radius-ului
- **Peering** = legătura de mare viteză între VNETs
- **Allow gateway transit** pe hub + **Use remote gateways** pe spoke = spoke-ul învață rutele din gateway-ul hub-ului
- Poți adăuga **Azure Firewall sau NVA** în hub și folosi UDR pentru a direcționa traficul prin el

Întrebări frecvente

Pui gateway în fiecare spoke?	De regulă nu. De aceea există hub-ul.
Peering-ul este tranzitiv?	Nu. Dacă A peered cu B și B cu C, A nu vede automat C.
Private Endpoint în hub sau spoke?	Cât mai aproape de consumatorul principal și de zona de guvernare DNS.
Virtual WAN vs hub-spoke self-managed?	Virtual WAN când ai multe site-uri globale și vrei model gestionat de Microsoft.

Decision Flow: Ce alegi și când



1

Conectezi Azure cu on-prem?

Primul pas: determini dacă ai nevoie de conectivitate hibridă.

2

Privat și enterprise?

ExpressRoute — conexiune privată, predictibilă, cu SLA și BGP prin provider dedicat.

3

Rapid și criptat?

VPN Gateway — tunel IPsec prin internet public, ideal pentru filiale și bootstrap.

4

Acces privat la PaaS?

Private Endpoint / **Private Link** — IP privat în VNet pentru servicii specifice.

5

Organizare multi-VNet?

Hub-Spoke + **peering** + **gateway transit** — guvernanță clară pentru mai multe workload-uri.

ExpressRoute în profunzime

ExpressRoute extinde rețeaua ta în Microsoft cloud peste o **conexiune privată** oferită printr-un provider. Nu traversezi internetul public pentru traficul de date către Azure. De aceea este ales când vrei stabilitate, latență mai predictibilă, SLA și integrare serioasă cu rețeaua enterprise.

ExpressRoute — cele 4 componente

1

Circuitul ExpressRoute

Legătura contractuală și tehnică cu providerul. Definește bandwidth-ul, locația de peering și SLA-ul.

2

Peering-ul

Private peering pentru VNETs și, dacă este cazul, **Microsoft peering** pentru anumite servicii Microsoft (Office 365, Dynamics).

3

ExpressRoute Gateway în VNet

Aduce VNet-ul în conversație cu circuitul. Se creează în GatewaySubnet. SKU-ul determină capacitatea și funcționalitățile disponibile.

4

BGP

Schimb automat de rute între mediile tale și Azure. Fără BGP, rutele nu se propagă dinamic între on-prem și cloud.

Aspect	Explicație practică
Private peering	Peering-ul folosit pentru conectivitate către VNETs prin gateway.
Gateway subnet	Se recomandă /27 sau mai mare; pentru 16 circuite trebuie /26 sau mai mare.
Scale units (ErGwScale)	Gateway-ul scalabil permite ajustarea capacității în funcție de trafic.
Coexistență cu VPN	Suportată; se folosește des pentru backup sau pentru site-uri care nu intră pe ExpressRoute.

Când NU alegi ExpressRoute: Dacă ai doar un site mic, un buget limitat sau ai nevoie de conectivitate rapidă de tip bootstrap, VPN Gateway este adesea alegerea mai pragmatică. ExpressRoute strălucește când contextul este enterprise.

Deploy ExpressRoute — pas cu pas

01

Creează Resource Group-ul

Portal > Resource groups > Create. Alege subscription, nume și regiune coerentă cu restul designului.

02

Creează circuitul

Caută ExpressRoute > Create. Completează subscription, resource group, region, **provider, peering location și bandwidth**.

03

Notează Service Key-ul

Acesta este codul pe care îl dai providerului pentru a activa circuitul. Fără el, providerul nu poate face nimic.

04

Configurează peering-ul

După ce providerul activează circuitul, intri la Peerings și creezi **Private peering**; dacă ai cerință specifică, adaugi și Microsoft peering.

05

Pregătește VNET-ul cu GatewaySubnet

VNET-ul care va consuma ExpressRoute trebuie să aibă un **GatewaySubnet**. Proiectează-l cel puțin /27.

06

Creează ExpressRoute Virtual Network Gateway

Alege gateway type = **ExpressRoute** și SKU-ul potrivit. Dacă folosești gateway-ul scalabil, ajustezi scale units după trafic.

07

Leagă VNET-ul la circuit

Creezi Connection / Link către virtual network gateway. Verifici că starea devine **Connected**.

08

Verifică BGP routes și conectivitatea

Verifici effective routes și conectivitatea reală din VM sau workload. Validarea este obligatorie după orice schimbare.

De ce contează provider și peering location: Nu sunt simple câmpuri administrative — ele determină unde și prin cine intri în ecosistemul ExpressRoute. Gateway type trebuie să fie **ExpressRoute**, nu VPN. GatewaySubnet mai mare îți lasă spațiu pentru scenarii de creștere și coexistență.

VPN Gateway în profunzime

VPN Gateway trimite trafic criptat între Azure și alte rețele prin internetul public, folosind **IPsec/IKE**. Este una dintre cele mai utile unelte pentru conectivitate rapidă, pentru filiale, laboratoare, parteneri sau pentru fallback față de ExpressRoute.

Site-to-Site (S2S)

Conectează sediul on-premises la Azure. Ideal pentru filiale și birouri cu echipament de rețea dedicat.

Point-to-Site (P2S)

Acces individual securizat pentru admini și utilizatori remote. Fiecare utilizator se conectează cu un client VPN.

VNet-to-VNet

Leagă două VNET-uri aflate în regiuni diferite dacă nu folosești peering sau ai cerințe specifice de criptare.

Scenariu	De ce VPN Gateway este potrivit
Branch office către Azure	Cost și timp de implementare mai bune decât un circuit privat dedicat.
Remote admins sau utilizatori	Point-to-Site pentru acces individual securizat.
Fallback pentru ExpressRoute	Asigură o cale alternativă dacă traseul principal cade.
VNETs în regiuni diferite	VNet-to-VNet dacă nu folosești peering sau ai cerințe specifice de criptare.

Modele de disponibilitate: **active-standby** sau **active-active**. Active-active înseamnă două instanțe gateway și două IP-uri publice. Toate tunelurile partajează bandwidth-ul disponibil al gateway-ului ales.

Deploy VPN Gateway — pas cu pas

01

Pregătește VNet-ul

Asigură-te că spațiul de adresare **nu se suprapune** cu on-premises. Aceasta este condiția de bază.

02

Creează GatewaySubnet

Recomandarea uzuală este **/27 sau mai mare** pentru flexibilitate și compatibilitate viitoare.

03

Caută Virtual network gateway > Create

Pornești procesul de creare din portal. Alege subscription și resource group corect.

04

Alege Gateway type = VPN

VPN type = **Route-based** în majoritatea scenariilor moderne. Policy-based rămâne o excepție sau constrângere impusă.

05

Alege SKU-ul și opțiunile

Dacă designul o cere, activezi **active-active** și **zone-redundant**. Folosești SKU Standard pentru IP public.

06

Creează Local Network Gateway

Definești **IP-ul public al echipamentului on-prem** și prefixele rețelei locale. Aceasta reprezintă sediul tău în Azure.

07

Creează Connection

Între VPN gateway și Local network gateway. Introduci **pre-shared key** și, opțional, BGP settings.

08

Configurează echipamentul on-prem

Configurezi tunelul cu parametrii compatibili Azure. Validezi conectivitatea și verifici **diagnostic logs, connection health și effective routes**.

Private Link și Private Endpoint explicate clar

Aici apare una dintre cele mai importante diferențe conceptuale din Azure networking: **VPN și ExpressRoute conectează rețele. Private Link conectează consumatorul la un serviciu specific**, printr-un IP privat în subnetul tău.

Componentele Private Link

Private Endpoint

Interfață de rețea cu IP privat în subnetul tău, asociată unui serviciu precum Storage, SQL, Key Vault, App Service sau alt serviciu compatibil. Modelul preferat pentru izolare maximă.

Private Link Service

Modul în care publici propriul tău serviciu, de obicei în spatele unui **Standard Load Balancer**, pentru a fi consumat privat de alte VNETs sau chiar alte organizații.

Private DNS Zone

Componenta care face ca **numele serviciului să rezolve către IP-ul privat corect**. Fără aceasta, aplicația continuă să rezolve endpoint-ul public.

DNS Private Resolver

Util când ai nevoie de rezolvare între Azure și on-prem **fără să menții propriile VM DNS forwarders**. Simplifică arhitectura DNS hibridă.

Private Endpoint

Adaugă un IP privat în subnetul tău. Accesul la serviciu rămâne pe rețea privată. **Modelul preferat** când vrei izolare maximă.

Service Endpoint

Optimizează accesul către un serviciu Azure pe backbone-ul Microsoft, dar serviciul rămâne tot cu endpoint public. **Mai puțin izolat** decât Private Endpoint.

Greșeala clasică: Administratorul creează Private Endpoint, dar uită DNS. Rezultatul: aplicația continuă să rezolve numele public și pare că Private Link "nu merge". De fapt, conectivitatea există, dar **numele nu indică IP-ul privat**.

Deploy Private Endpoint — pas cu pas

01

Alege serviciul țintă

Selectezi serviciul pe care vrei să-l expui privat: **Storage Account, SQL Server, Key Vault sau App Service**.

02

Pornește crearea

Caută Private endpoint > Create sau pornești din resursa respectivă din secțiunea **Networking / Private endpoint connections**.

03

Completează detaliile

Selectezi subscription, resource group, **nume, regiune și resursa țintă**. Fiecare câmp are impact asupra localizării și rutării.

04

Alege VNET-ul și subnetul

Subnetul trebuie să aibă **spațiu IP disponibil** și să fie ales intenționat — de obicei aproape de consumatorul principal.

05

Activează integrarea cu Private DNS Zone

În cele mai multe cazuri, aceasta este **alegerea corectă** pentru laborator și pentru majoritatea mediilor enterprise. Nu sări peste acest pas!

06

Verifică conexiunea aprobată

Resursa primește o conexiune aprobată, iar în subnet apare noul **NIC cu IP privat**.

07

Testează DNS și conectivitatea

Dintr-o VM sau aplicație din VNet, verifici că **numele rezolvă către IP-ul privat**, nu către endpoint-ul public.

Deploy Hub-Spoke — pas cu pas

01

Creează Hub VNet

De exemplu **10.0.0.0/16**. Rezervi GatewaySubnet și, dacă este cazul, subneturi pentru Firewall, Bastion, DNS Resolver, management.

02

Creează Spoke VNETs

De exemplu **10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16**. Păstrezi prefixele distincte și documentate. Nicio suprapunere!

03

Creează VNet peering

Peering între hub și fiecare spoke. Peering-ul **nu este tranzitiv** — fiecare spoke trebuie peered direct cu hub-ul.

04

Activează Allow gateway transit pe hub

Dacă spoke-urile trebuie să folosească gateway-ul din hub, activezi această opțiune pe peering-ul din hub.

05

Activează Use remote gateways pe spoke

Pe peering-ul din spoke activezi această opțiune. Verifici și **Allow forwarded traffic** unde este necesar pentru trafic forțat prin firewall/NVA.

06

Configurează UDR-uri pentru Azure Firewall

Dacă vrei centralizare de trafic, creezi UDR-uri în spoke-uri și trimiți prefixele dorite către **IP-ul privat al firewall-ului**.

07

Configurează DNS links

Dacă spoke-urile consumă Private Endpoints sau zone private, configurezi corect **DNS links și DNS Private Resolver**.

08

Verifică effective routes și connectivity

Folosești **Network Watcher** sau direct workload-urile pentru a valida că rutele și conectivitatea sunt corecte.

De ce hub-spoke este atât de popular: Reduce haosul. În loc să pui gateway, firewall, DNS și reguli în fiecare VNet, le concentrezi într-un hub și lași spoke-urile curate, dedicate aplicațiilor lor.

Cum se leagă între ele aceste servicii

Într-o arhitectură reală, serviciile nu funcționează izolat. Fiecare are un rol precis și colaborează cu celelalte pentru a forma un întreg coerent.

Colaborarea dintre servicii

ExpressRoute / VPN Gateway

Aduc compania în Azure. Sunt **poarta de intrare hibridă**. Fără ele, on-premises nu vede Azure în mod privat.

Hub-Spoke

Organizează VNETs și centralizează punctele comune: gateway, firewall, DNS, monitorizare. **Structura de bază** a oricărei arhitecturi enterprise.

Azure Firewall / NVA

Controlează și inspectează traficul centralizat în hub. Lucrează cu **UDR-uri** pentru a forța traficul prin el.

Private Link

Duce serviciile PaaS în spațiul privat al rețelei tale. Completează hub-spoke cu **acces privat la servicii** fără expunere publică.

App Gateway / WAF

Stă în fața aplicațiilor web. **Nu înlocuiește** gateway-ul de rețea — este complementar, nu alternativ.

NSG-uri

Fac micro-segmentare la subnet sau NIC. **Completează** celelalte servicii, nu le anulează. Sunt ultimul strat de control.

Serviciu	Cu ce colaborează natural
ExpressRoute	Hub-spoke, ExpressRoute gateway, BGP, Firewall, Private DNS Resolver
VPN Gateway	Gateway transit, on-prem routers, P2S users, Firewall/NVA, DNS
Private Endpoint	Private DNS Zones, DNS Resolver, spoke workloads, NSG policy
Hub-Spoke	Peering, UDR, Firewall, shared services, monitoring
NSG	Toate subneturile și NIC-urile relevante

Greșeli clasice și cum le eviți

Adrese suprapuse între Azure și on-premises

Soluție: IP plan serios înainte de deployment. Aceasta este prima disciplină, nu un detaliu administrativ.

GatewaySubnet prea mic

Soluție: Proiectează de la început /27 sau mai mare pentru flexibilitate; verifică nevoile de coexistență și scale.

Private Endpoint fără DNS privat

Soluție: Leagă Private DNS Zone și testează rezolvarea numelui. Fără DNS corect, Private Link "nu merge" aparent.

Confuzie App Gateway vs VPN Gateway

Unul este pentru **trafic web L7**, celălalt pentru **conectivitate de rețea**. Sunt instrumente complet diferite.

Confuzie Private Link vs Peering

Private Link expune un serviciu; **peering conectează VNETs**. Sunt concepte fundamental diferite.

Lipsa verificării effective routes

Soluție: După orice schimbare de peering, UDR, BGP sau gateway, validează rutele efective. Nu presupune că funcționează.

Prea multă logică distribuită în fiecare spoke

Soluție: Centralizează cât are sens în hub. Spoke-urile trebuie să rămână curate și dedicate workload-urilor lor.

Scenarii reale de utilizare

Fiecare organizație are nevoi diferite. Iată cum se mapează cerințele reale pe designul recomandat.

Companie cu datacenter principal

Cerințe stricte de performanță și SLA. Design recomandat: **ExpressRoute** + **hub-spoke** + **Firewall** + **Private Endpoints** pentru PaaS critice.

Firmă medie cu 2-3 sedii

Buget atent controlat. Design recomandat: **VPN Gateway S2S** + **hub-spoke simplu** + **Private Endpoints** pentru servicii sensibile.

Admini și dezvoltatori remote

Acces individual securizat. Design recomandat: **P2S VPN** + **Private Link** + **DNS Resolver** unde este nevoie.

Migrare treptată spre cloud

Tranziție graduală. Design recomandat: **VPN Gateway inițial, apoi coexistență cu ExpressRoute** pentru traseu principal și VPN ca backup.

Platformă multi-workload

Multe echipe și workload-uri. Design recomandat: **Hub-spoke cu gateway transit, firewall central** și standarde clare de peering, DNS și UDR.

Checklist practic pentru Network Engineer

Înainte de a considera un design complet, verifică fiecare punct din această listă. Fiecare item nerezolvat este un risc potențial în producție.

Design și planificare

- Am un **IP plan fără suprapuneri** între on-prem, hub, spoke și eventuale medii viitoare?
- Știu clar ce conectez: **rețele întregi, utilizatori individuali sau doar servicii specifice**?
- Am ales corect între **ExpressRoute și VPN** pe baza cerințelor reale, nu din reflex?
- Am proiectat **GatewaySubnet corect** și am verificat cerințele pentru coexistență / scale?

Implementare și validare

- Am gândit **DNS-ul pentru Private Link** și rezolvarea hibridă?
- Am documentat peering settings: **Allow gateway transit, Use remote gateways, Allow forwarded traffic**?
- Am verificat **effective routes, NSG-uri, UDR-uri** și health-ul conexiunilor?
- Am plan de **monitorizare și alerte** pentru gateway, conexiuni, DNS și availability?

Laborator recomandat pentru curs

Lab 1 — Hub-Spoke de bază

Creează un hub VNet și două spoke VNETs cu peering corect. Validează că peering-ul funcționează și că rutele sunt propagate.

Lab 2 — VPN Gateway cu gateway transit

Adaugă un VPN Gateway în hub și validează **gateway transit** către spoke. Verifică effective routes din spoke.

Lab 3 — Private Endpoint și DNS privat

Creează un Storage Account cu Private Endpoint și rezolvă DNS-ul privat. Testează că numele rezolvă IP privat, nu public.

Lab 4 — Design enterprise pe hârtie

Desenează varianta enterprise: **ExpressRoute** + **VPN backup** + **hub-spoke** + **Private Link** + **Firewall**. Exercițiu de arhitectură.

Lab 5 — Troubleshooting

Schimbă o setare de peering sau DNS și cere cursantului să identifice de ce nu mai merge. Cel mai valoros exercițiu practic.

Formulă simplă de memorat

Rețele întregi ExpressRoute sau VPN Gateway	**Servicii specifice** Private Link
Organizare și guvernare Hub-Spoke	**Segmentare locală** NSG
Protecție centralizată Firewall / NVA	**Trafic web inteligent** Application Gateway / WAF

> Dacă reții un singur lucru din acest ghid, să fie acesta: în Azure networking nu câștigi doar când "merge", ci când designul este suficient de clar încât să poți explica **de ce merge, cum se scalează și unde va ceda dacă apar schimbări**. ExpressRoute, VPN Gateway, Private Link și hub-spoke nu sunt servicii concurente. Sunt piese complementare ale aceleiași discipline.

Surse oficiale recomandate pentru aprofundare

ExpressRoute

Microsoft Learn — ExpressRoute overview, peerings și virtual network gateway. Documentația oficială pentru circuite, SKU-uri și BGP.

VPN Gateway

Microsoft Learn — VPN Gateway tutorials, about gateway settings, gateway transit și highly available design. Include ghiduri pentru S2S, P2S și active-active.

Private Link

Microsoft Learn — Private Link overview, private endpoint overview și private endpoint DNS. Esențial pentru înțelegerea integrării DNS.

Hub-Spoke Architecture

Microsoft Learn — Hub-spoke architecture în **Azure Architecture Center**. Conține diagrame de referință și bune practici actualizate.

DNS Private Resolver

Microsoft Learn — DNS Private Resolver overview pentru scenarii hibride. Util pentru înțelegerea rezolvării DNS între Azure și on-prem.

Versiune 2026 — structură bazată pe documentația Microsoft Learn și pe bune practici de arhitectură Azure. Verificați întotdeauna documentația oficială pentru cele mai recente actualizări de SKU-uri și funcționalități.