

Manual Azure Networking - Ediția Gamificată (Partea a IV-a)

Despre Acest Manual (Partea a IV-a)

Bun venit la a patra parte a călătoriei tale în Azure! Ai explorat fundamentele, ai stăpânit serviciile de calcul și ai devenit un gardian al datelor. Acum, este timpul să devii un arhitect de rețea, învățând cum să construiești autostrăzile digitale care conectează totul în cloud. Rețelistica este coloana vertebrală a oricărei soluții cloud, iar în acest manual vei învăța cum să o proiectezi, să o securizezi și să o gestionezi în Azure.

Ce vei învăța:

-  Virtual Networks (VNet) și Subnets - Izolarea și organizarea resurselor
-  Adrese IP Publice și Private - Conectarea la lume și comunicarea internă
-  Network Security Groups (NSG) - Firewall-ul tău virtual
-  Azure Load Balancer - Asigurarea disponibilității și scalabilității
-  Laborator practic: Construirea unei arhitecturi de rețea sigure

Sistem de Gamification:

-  **XP Points** - Câștigă experiență pentru fiecare capitol și laborator
-  **Achievement-uri Noi** - Deblochează medalii pentru competențe de rețelistică
-  **Nivele de Dificultate** - De la Beginner la Advanced
-  **Laborator Hands-on** - Construiește infrastructură de rețea reală în Azure

Total XP Posibil (Partea a IV-a): 1,300 puncte

CAPITOLUL 11: Virtual Networks - Rețeaua Ta Privată În Cloud

Tema Gamification: “Arhitectul de Rețea”

Nivel: Beginner-Intermediate (★★)

Orice oraș are nevoie de străzi și autostrăzi pentru ca mașinile să poată circula. În mod similar, orice aplicație cloud are nevoie de o rețea pentru ca datele să poată circula. În acest capitol, vei învăța cum să construiești fundația rețelei tale în Azure: **Virtual Network (VNet)**. Vei învăța cum să-ți creezi propria rețea privată și izolată în cloud, cum să împărți în segmente logice numite **subnets** și cum funcționează adresarea IP. La final, vei debloca achievement-ul **Network Architect**!

11.1 Ce este o Rețea Virtuală (VNet)?

O **Azure Virtual Network (VNet)** este reprezentarea rețelei tale private în cloud. Este un mediu izolat logic în care poți lansa resurse Azure precum mașini virtuale, baze de date și aplicații. Gândește-te la VNet ca la o extensie a proprietății tale rețele locale (on-premises) în cloud, dar cu beneficiile de scalabilitate, disponibilitate și izolare ale infrastructurii Azure.

Analogie: Un VNet este ca un teren privat pe care l-ai cumpărat într-un oraș mare (Azure). Pe acest teren, tu decizi cum construiești drumurile, unde plasezi casele (VM-urile) și cum le conectezi între ele. Nimeni din afara terenului tău nu poate intra fără permisiunea ta.

Caracteristici Cheie ale unui VNet:

- Izolare:** Resursele dintr-un VNet pot comunica între ele în mod implicit, dar sunt izolate de internet și de alte VNet-uri.
- Adresare IP Proprie:** Tu definești spațiul de adrese IP privat pentru VNet-ul tău (ex: 10.0.0.0/16), la fel ca într-o rețea tradițională.
- Conectivitate:** Poți conecta VNet-ul la internet, la alte VNet-uri (VNet Peering) sau la rețeaua ta on-premises (VPN/ExpressRoute).
- Gratuitate:** Crearea unui VNet este gratuită. Plătești doar pentru resursele pe care le implementezi în el.

11.2 Subnets: Segmentarea Rețelei

Un **subnet** (subrețea) este o diviziune a spațiului de adrese al VNet-ului tău. Împărțirea unui VNet în subnets îți permite să organizezi și să securizezi resursele mai eficient.

Analogie: Dacă VNet-ul este terenul tău privat, subnets-urile sunt cartierele pe care le construiești pe acel teren. Poți avea un cartier rezidențial (pentru serverele de aplicații), un cartier de afaceri (pentru bazele de date) și un cartier industrial (pentru alte servicii). Fiecare cartier are propriul său set de reguli de acces.

De ce să folosești subnets?

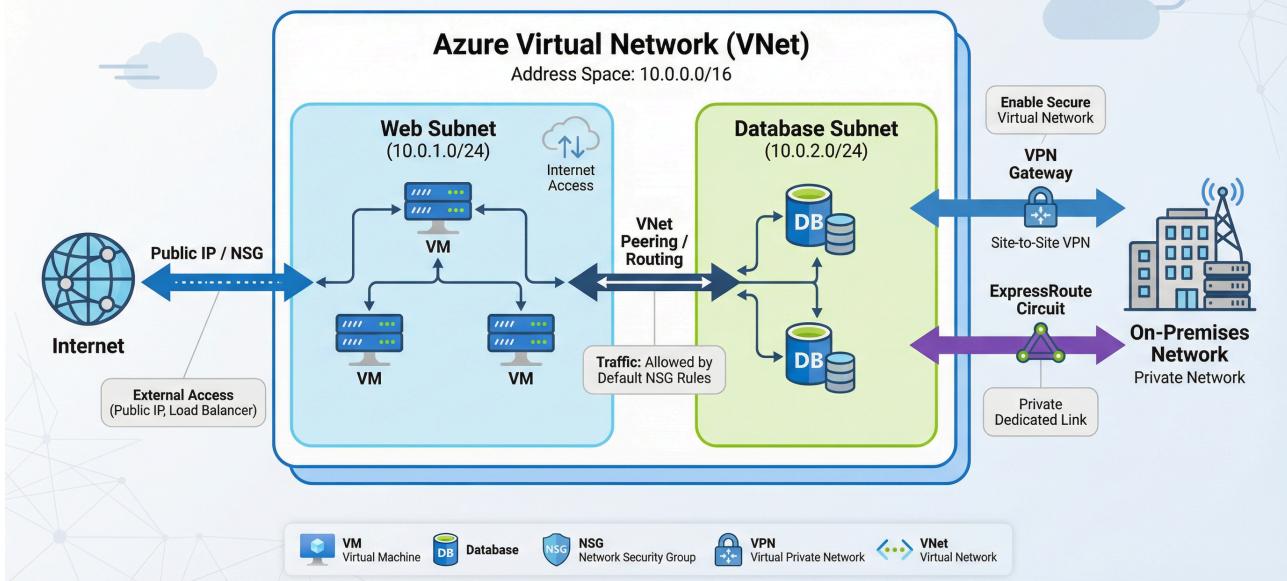
- **Organizare:** Grupezi resurse similare (ex: toate serverele web într-un subnet, toate bazele de date în altul).
- **Securitate:** Poți aplica reguli de securitate diferite pentru fiecare subnet. De exemplu, poți permite accesul din internet doar la subnet-ul serverelor web, în timp ce subnet-ul bazelor de date rămâne complet izolat.
- **Managementul Adreselor IP:** Aloci o parte din spațiul de adrese al VNet-ului pentru fiecare subnet.

Exemplu de Arhitectură:

- **VNet Address Space:** 10.1.0.0/16 (oferă 65,536 de adrese IP)
- **Web Subnet:** 10.1.1.0/24 (oferă 251 de adrese IP disponibile pentru serverele web)
- **Database Subnet:** 10.1.2.0/24 (oferă 251 de adrese IP disponibile pentru bazele de date)

Notă: Azure rezervă primele patru adrese și ultima adresă din fiecare subnet pentru utilizare internă.

Azure VNet Architecture Diagram



11.3 Adrese IP Publice și Private

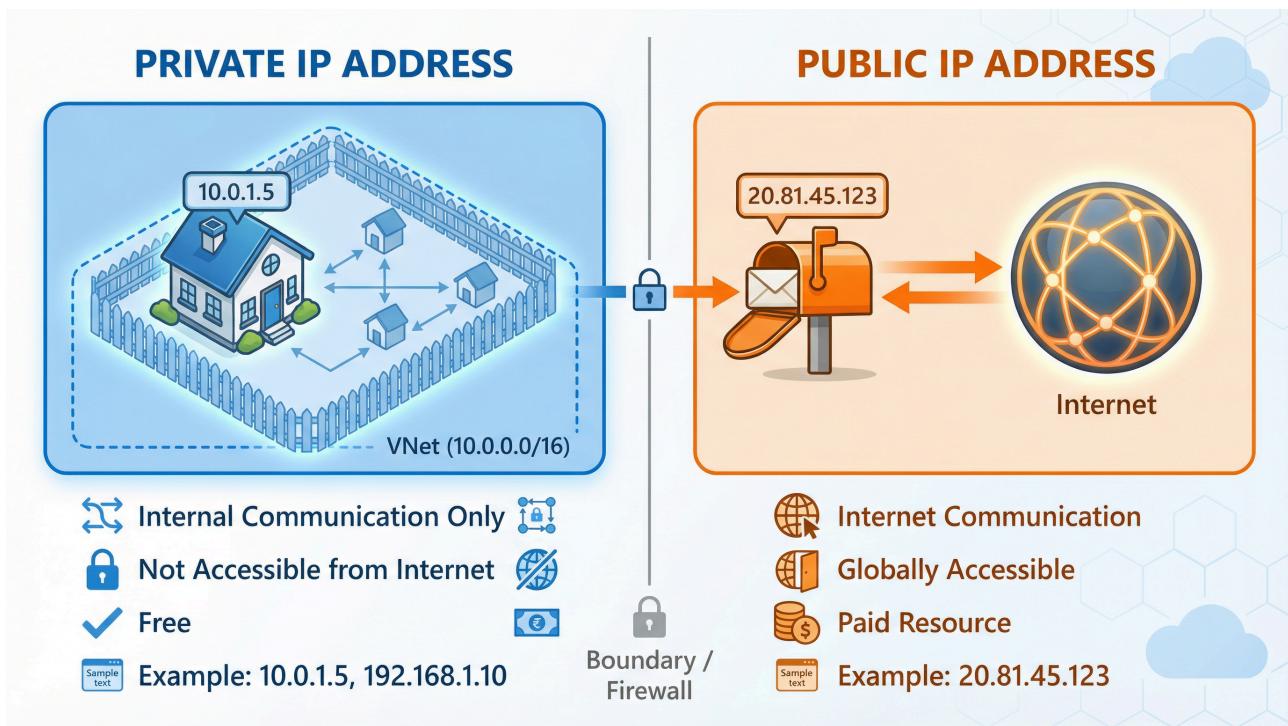
În Azure, resursele pot avea două tipuri de adrese IP:

Adrese IP Private:

- Scop:** Pentru comunicare **în interiorul** unui VNet și cu rețelele on-premises conectate.
- Alocare:** Sunt alocate din spațiul de adrese al subnet-ului în care se află resursa.
- Accesibilitate:** Nu sunt accesibile direct din internet.
- Analogie:** Este adresa poștală a unei case din cartierul tău privat. Doar cei din interiorul cartierului o pot folosi pentru a trimite corespondență.

Adrese IP Publice:

- Scop:** Pentru comunicare **cu internetul**.
- Alocare:** Sunt alocate de Azure și sunt unice la nivel global.
- Accesibilitate:** Permit resurselor să fie accesibile din internet (inbound) și să comunice cu internetul (outbound).
- Asociere:** Pot fi asociate cu mașini virtuale, load balancere, gateway-uri VPN etc.
- Analogie:** Este o cutie poștală publică pe care o instalezi în fața casei tale. Oricine de pe glob poate trimite scrisori la acea cutie poștală.



Tip IP	Utilizare	Accesibilitate	Cost
Privat	Comunicare internă (VNet)	Doar din VNet / rețele conectate	Gratuit
Public	Comunicare cu internetul	Accesibil global	Taxabil (există un nivel gratuit)

Metode de Alocare:

- Dinamică:** Adresa IP este alocată automat și se poate schimba dacă resursa este oprită și pornită (deallocated).
- Statică:** Adresa IP este rezervată și rămâne aceeași pe totă durata de viață a resursei. Este recomandată pentru servere care trebuie să fie accesibile constant la aceeași adresă (ex: controlere de domeniu, servere DNS).

★ QUIZ TIME! ★

1. Ce este un Azure Virtual Network (VNet)?
 - O rețea publică pentru oricine.
 - O rețea privată și izolată în Azure pentru resursele tale.
 - Un tip de mașină virtuală.

2. Care este principalul motiv pentru a împărți un VNet în subnets?
 - a) Pentru a crește viteza internetului.
 - b) Pentru a organiza și securiza resursele mai eficient.
 - c) Pentru a reduce costurile.
3. Ce tip de adresă IP ai folosi pentru a permite unei mașini virtuale să fie accesibilă din internet?
 - a) Adresă IP Privată
 - b) Adresă IP Publică
 - c) Adresă MAC
4. Câte adrese IP rezervă Azure în fiecare subnet?
 - a) 2
 - b) 3
 - c) 5
5. Când este recomandat să folosești o adresă IP statică?
 - a) Pentru stații de lucru temporare.
 - b) Pentru servere care trebuie să fie accesibile constant la aceeași adresă.
 - c) Nu este niciodată recomandat.

(Răspunsuri la finalul manualului)

Ai pus fundația. Acum știi cum să-ți construiești propria rețea privată în cloud. Ești gata să înveți cum să o protejezi.

 Achievement Deblocat: Network Architect 

+250 XP

CAPITOLUL 12: Network Security Groups - Paznicul Rețelei Tale

Tema Gamification: “Gardianul Porților”

Nivel: Intermediate (★★★)

Ai construit drumurile, dar acum trebuie să instalezi porți și paznici pentru a controla cine intră și cine ieșe. În acest capitol, vei învăța despre **Network Security Groups**

(NSG), firewall-ul tău virtual în Azure. Vei învăța cum să creezi reguli pentru a permite sau a bloca traficul de rețea către resursele tale, asigurând un nivel fundamental de securitate. Stăpânirea NSG-urilor îți va aduce achievement-ul **Gatekeeper!**

12.1 Ce este un Network Security Group (NSG)?

Un **Network Security Group (NSG)** este un set de reguli de securitate care filtrează traficul de rețea către și de la resursele Azure dintr-un VNet. Un NSG poate fi asociat cu un **subnet** sau cu o **interfață de rețea (NIC)** a unei mașini virtuale.

Analogie: Un NSG este ca un paznic la poarta unui cartier (subnet) sau la ușa unei case (NIC). Paznicul are o listă de reguli (o listă de invitați). Dacă cineva se prezintă la poartă, paznicul verifică lista. Dacă persoana este pe listă (regula Allow), i se permite accesul. Dacă nu este pe listă sau este pe o listă de interdicție (regula Deny), accesul este refuzat.

Cum funcționează?

- Un NSG conține o listă de **reguli de securitate**.
- Fiecare regulă specifică dacă traficul este **permis (Allow)** sau **blocat (Deny)**.
- Regulile sunt evaluate în funcție de **prioritate** (un număr între 100 și 4096). Cu cât numărul este mai mic, cu atât prioritatea este mai mare.
- Procesarea se oprește la prima regulă care se potrivește cu traficul.

12.2 Anatomia unei Reguli NSG

Fiecare regulă dintr-un NSG are următoarele proprietăți:

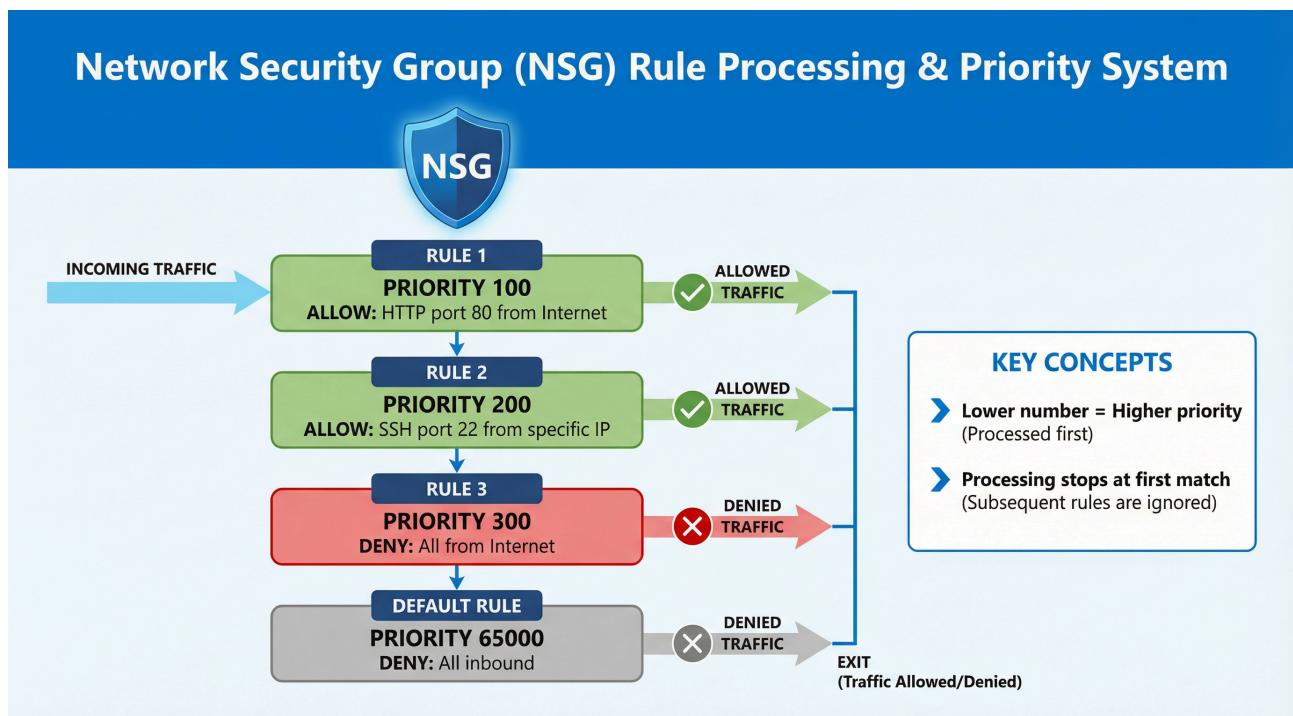
- **Name:** Un nume descriptiv pentru regulă (ex: Allow-HTTP-Inbound).
- **Priority:** Un număr între 100 și 4096. Regulile cu prioritate mai mică sunt procesate primele.
- **Source / Destination:** Adresa IP, range-ul de adrese (CIDR), sau un **Service Tag** (ex: Internet, VirtualNetwork, Storage) de unde provine sau către care se duce traficul.
- **Protocol:** TCP, UDP, ICMP, sau Any.
- **Direction:** Inbound (trafic care intră în resursă) sau Outbound (trafic careiese din resursă).

- **Port Range:** Portul sau intervalul de porturi (ex: 80 , 443 , 1000-2000 , * pentru toate).
- **Action:** Allow sau Deny.

Exemplu de Regulă:

- **Name:** Allow-SSH-From-My-IP
- **Priority:** 200
- **Source:** Adresa ta IP publică (ex: 86.12.34.56)
- **Destination:** Any
- **Protocol:** TCP
- **Direction:** Inbound
- **Port Range:** 22
- **Action:** Allow

Această regulă permite traficul SSH (port 22) să ajungă la resursa asociată, dar **numai** de la adresa ta IP. Orice altă încercare de conectare SSH de la o altă adresă IP va fi blocată (presupunând că nu există o altă regulă cu prioritate mai mare care să o permită).



12.3 Reguli Implicite (Default Rules)

Fiecare NSG nou creat vine cu un set de **reguli implicite**. Aceste reguli au prioritate foarte mare (peste 65000) și nu pot fi șterse, dar pot fi suprascrise de reguli create de tine cu prioritate mai mică.

Reguli Inbound Implicite:

- 1. AllowVnetInBound:** Permite traficul din interiorul VNet-ului.
- 2. AllowAzureLoadBalancerInBound:** Permite traficul de la Azure Load Balancer (pentru health probes).
- 3. DenyAllInBound:** Blochează tot restul traficului inbound.

Reguli Outbound Implicite:

- 1. AllowVnetOutBound:** Permite traficul către orice resursă din VNet.
- 2. AllowInternetOutBound:** Permite tot traficul outbound către internet.
- 3. DenyAllOutBound:** Blochează tot restul traficului outbound.

Important: Regula `DenyAllInBound` este motivul pentru care, în mod implicit, nu poți accesa o mașină virtuală din internet. Trebuie să creezi o regulă nouă cu prioritate mai mică (ex: prioritate 200) care să permită traficul pe portul dorit (ex: RDP pe 3389 sau SSH pe 22).

12.4 Asocierea NSG-urilor: Subnet vs. NIC

Un NSG poate fi asociat cu:

- **Un Subnet:** Regulile se aplică **tuturor** resurselor din acel subnet. Aceasta este metoda recomandată pentru a gestiona securitatea la scară.
- **O Interfață de Rețea (NIC):** Regulile se aplică **doar** acelei mașini virtuale. Este util pentru a crea excepții pentru o anumită mașină.

Cum se combină regulile?

- **Trafic Inbound:** Mai întâi se evaluatează regulile NSG-ului de la nivel de **subnet**, apoi cele de la nivel de **NIC**. Traficul trebuie să fie permis la ambele niveluri pentru a ajunge la VM.

- **Trafic Outbound:** Mai întâi se evaluează regulile de la nivel de **NIC**, apoi cele de la nivel de **subnet**. Traficul trebuie să fie permis la ambele niveluri pentru a ieși din VM.

Best Practice: Folosește NSG-uri la nivel de subnet pentru reguli generale (ex: permite HTTP/HTTPS către subnet-ul web) și NSG-uri la nivel de NIC pentru excepții specifice (ex: permite SSH către o singură mașină de management de la IP-ul tău).

12.5 Service Tags

Service Tags sunt etichete create de Microsoft care reprezintă un grup de adrese IP pentru un anumit serviciu Azure. Folosirea lor simplifică enorm crearea regulilor.

Exemple de Service Tags:

- `Internet` : Reprezintă tot spațiul de adrese IP publice.
- `VirtualNetwork` : Reprezintă tot spațiul de adrese al VNet-ului tău.
- `Storage.WestEurope` : Reprezintă toate adresele IP ale serviciului Azure Storage din regiunea West Europe.
- `Sql.EastUS` : Reprezintă toate adresele IP ale serviciului Azure SQL din regiunea East US.

În loc să cauți și să adaugi manual zeci sau sute de adrese IP pentru un serviciu, poți folosi pur și simplu service tag-ul corespunzător în regulile tale NSG.

★ QUIZ TIME! ★

1. Ce face un Network Security Group (NSG)?
 - a) Accelerează viteza rețelei.
 - b) Filtrează traficul de rețea pe baza unor reguli de securitate.
 - c) Distribuie traficul între mai multe mașini virtuale.
2. O regulă NSG cu prioritatea 100 este procesată înainte sau după o regulă cu prioritatea 200?
 - a) După
 - b) Înainte
 - c) În același timp

3. Ce face regula implicită `DenyAllInBound` ?
- a) Permite tot traficul care intră.
 - b) Blochează tot traficul care intră, cu excepția cazului în care este permis de o regulă cu prioritate mai mare.
 - c) Permite doar traficul de la Azure Load Balancer.
4. Care este metoda recomandată de a aplica NSG-uri pentru a gestiona securitatea la scară?
- a) Asocierea cu fiecare mașină virtuală individual.
 - b) Asocierea cu subnet-ul.
 - c) Nu se recomandă folosirea NSG-urilor.
5. Ce este un Service Tag?
- a) Un nume pentru mașina ta virtuală.
 - b) O etichetă care reprezintă un grup de adrese IP pentru un serviciu Azure.
 - c) O regulă de securitate.

(Răspunsuri la finalul manualului)

Ai devenit un paznic vigilant. Știi cum să controlezi fiecare punct de acces în rețeaua ta. Acum ești gata să gestionezi fluxul de trafic la scară mare.

 Achievement Deblocat: Gatekeeper 

+300 XP

CAPITOLUL 13: Azure Load Balancer - Dirijorul Traficului

Tema Gamification: “Maestrul Scalabilității”

Nivel: Intermediate-Advanced (

Ai construit rețeaua și ai securizat porțile. Dar ce se întâmplă când mii de utilizatori încearcă să-ți accesese aplicația în același timp? Un singur server nu va face față. Aici intervine **Azure Load Balancer**, dirijorul care distribuie intelligent traficul între mai multe servere pentru a asigura disponibilitate și performanță. Stăpânirea acestui serviciu te va transforma într-un maestru al scalabilității și îți va aduce achievement-ul **Scaling Maestro!**

13.1 Ce este un Load Balancer?

Un **Azure Load Balancer** este un serviciu care distribuie traficul de rețea de intrare (inbound) către un grup de resurse sau servere backend. Acesta acționează ca un singur punct de contact pentru clienți, distribuind cererile în mod egal sau conform unor reguli specifice către mașinile virtuale din spate.

Analogie: Un Load Balancer este ca un dispecer la un centru de apeluri. Când sună un client, dispecerul nu răspunde el însuși la întrebare. În schimb, el direcționează apelul către unul dintre mulții operatori disponibili și liberi. Dacă un operator este bolnav sau într-o pauză (unhealthy), dispecerul nu-i va mai trimite apeluri până când acesta nu devine din nou disponibil.

De ce să folosești un Load Balancer?

- **High Availability (Disponibilitate Ridicată):** Dacă o mașină virtuală cade, Load Balancer-ul încețează să-i mai trimită trafic și îl redirecționează către celelalte mașini sănătoase. Aplicația ta rămâne online.
- **Scalability (Scalabilitate):** Poți adăuga sau elimina mașini virtuale din grupul de backend fără a întrerupe serviciul. Load Balancer-ul se adaptează automat.
- **Performance (Performanță):** Distribuind încărcarea, te asiguri că niciun server nu este suprasolicitat, ceea ce duce la timpi de răspuns mai buni pentru utilizatori.

13.2 Tipuri de Azure Load Balancer

Azure oferă mai multe servicii de load balancing, dar cel fundamental, care operează la **Layer 4 (Transport - TCP/UDP)**, este Azure Load Balancer. Acesta vine în două variante principale:

- **Public Load Balancer:**
 - **Scop:** Distribuie traficul provenit din **internet** către mașinile virtuale din VNet-ul tău.
 - **Frontend IP:** Are o adresă IP publică.
 - **Scenariu:** Folosit pentru a expune aplicații web, API-uri sau alte servicii către publicul larg.
- **Internal (Private) Load Balancer:**

- **Scop:** Distribuie traficul provenit din **interiorul VNet-ului** tău.
- **Frontend IP:** Are o adresă IP privată.
- **Scenariu:** Folosit pentru a distribui traficul între diferitele niveluri ale unei aplicații (ex: de la serverele web la serverele de baze de date) fără a expune serviciile interne la internet.

Tip	Sursă Trafic	IP Frontend	Scenariu Tipic
Public	Internet	Public	Aplicație web publică
Internal	VNet / On-premises	Privat	Servicii backend (ex: baze de date)

SKU-uri (Stock Keeping Units):

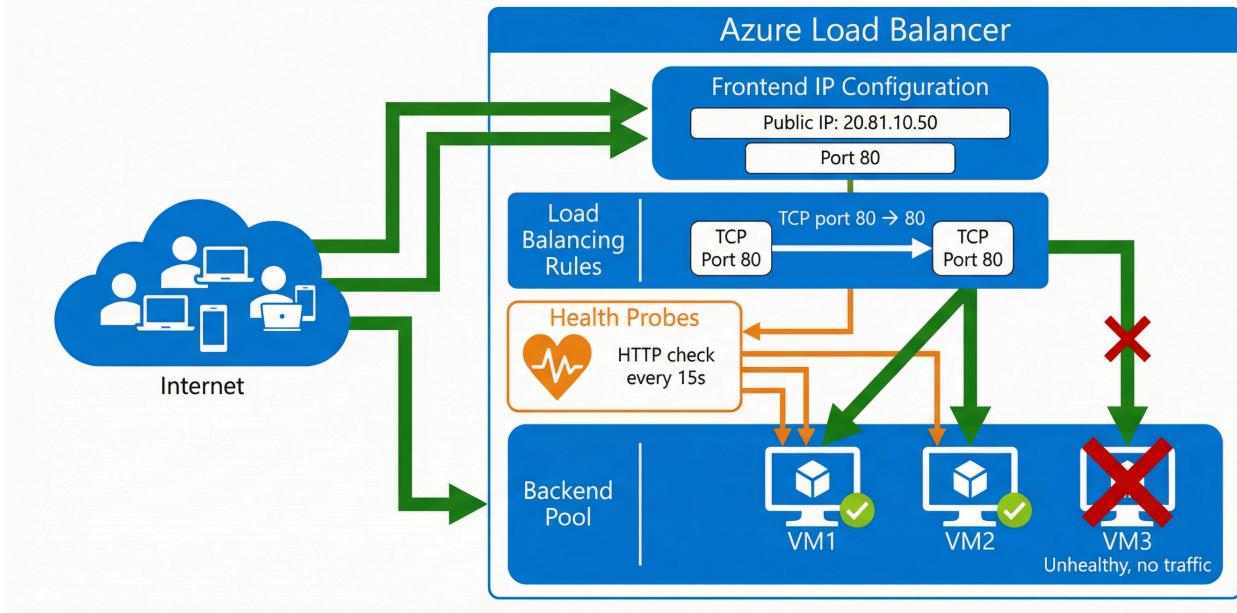
- **Basic (în curs de retragere):** Varianta veche, cu funcționalități limitate. Nu este recomandată pentru aplicații noi.
- **Standard:** Varianta modernă, recomandată pentru toate aplicațiile de producție. Oferă securitate sporită (închis la internet în mod implicit), scalabilitate mai mare și monitorizare avansată.

13.3 Componentele unui Load Balancer

Configurarea unui Load Balancer implică definirea a patru componente principale:

1. **Frontend IP Configuration:** Adresa IP a Load Balancer-ului, punctul de intrare pentru trafic.
2. **Backend Pool:** Grupul de mașini virtuale (sau interfețe de rețea) care vor primi traficul.
3. **Health Probes:** Mecanismul prin care Load Balancer-ul verifică starea de sănătate a mașinilor din backend pool. Poate fi o verificare TCP (dacă un port este deschis) sau HTTP/HTTPS (dacă o pagină web returnează un cod de succes, ex: 200 OK).
4. **Load Balancing Rules:** Regulile care leagă totul împreună. O regulă definește: “Traficul care vine pe **portul X** al **frontend IP-ului** va fi trimis pe **portul Y** al mașinilor din **backend pool**, folosind **protocolul Z**.”

Azure Load Balancer Traffic Flow and Components



Exemplu de Regulă:

- **Frontend IP:** 20.81.10.50
- **Protocol:** TCP
- **Port (Frontend):** 80
- **Backend Port:** 80
- **Backend Pool:** web-server-pool
- **Health Probe:** http-probe

Această regulă spune: “Orice trafic HTTP (TCP port 80) care ajunge la IP-ul public al load balancer-ului va fi redirecționat către portul 80 al uneia dintre mașinile sănătoase din web-server-pool.”

13.4 Cum funcționează Health Probes?

Health Probes sunt esențiale pentru disponibilitatea ridicată. Load Balancer-ul trimite periodic o cerere de verificare (sondă) către fiecare mașină din backend pool.

- **Interval:** Cât de des se trimit sonda (ex: la fiecare 15 secunde).
- **Unhealthy Threshold:** Câte sonde consecutive trebuie să eșueze pentru ca mașina să fie marcată ca “nesănătoasă” (unhealthy).

Când o mașină este marcată ca unhealthy, Load Balancer-ul **încetează să-i mai trimítă trafic nou**. Va continua să o verifice, iar de îndată ce mașina începe să răspundă din nou corect la sonde, o va marca din nou ca “sănătoasă” (healthy) și o va reintroduce în rotație pentru a primi trafic.

Best Practice: Configurează o pagină de health check dedicată în aplicația ta (ex: `/health`) care returnează un cod 200 OK doar dacă aplicația funcționează corect (ex: are conexiune la baza de date). Folosește această pagină pentru health probe-ul HTTP al Load Balancer-ului. Acest lucru asigură o verificare mult mai precisă a stării de sănătate decât o simplă verificare a portului.

13.5 Load Balancer vs. Alte Servicii Azure

Este important să nu confunzi Azure Load Balancer cu alte servicii de distribuție a traficului:

- **Application Gateway:** Este un load balancer de **Layer 7 (Aplicație)**. Înțelege protocolul HTTP/HTTPS și poate lua decizii de rutare bazate pe URL, headere HTTP etc. (ex: trimită traficul pentru `/imagini` la un set de servere și cel pentru `/video` la alt set). Include și un Web Application Firewall (WAF).
- **Front Door:** Este un serviciu de load balancing **global**, care operează la Layer 7. Distribuie traficul între diferite regiuni Azure pentru a oferi cea mai mică latență utilizatorilor din întreaga lume și pentru a asigura failover la nivel de regiune.
- **Traffic Manager:** Este un load balancer bazat pe **DNS**. Direcționează clienții către diferite endpoint-uri (care pot fi în Azure sau în afara lui) pe baza unor metode de rutare DNS (ex: performanță, geografic, prioritate).

Serviciu	Layer OSI	Scop	Scenariu Tipic
Load Balancer	Layer 4 (TCP/UDP)	Load balancing regional, non-HTTP	Orice aplicație TCP/UDP
Application Gateway	Layer 7 (HTTP/S)	Load balancing HTTP/S regional, WAF	Aplicații web complexe
Front Door	Layer 7 (HTTP/S)	Load balancing HTTP/S global	Aplicații web globale
Traffic Manager	DNS	Rutare DNS globală	Disaster recovery, hibrid

★ QUIZ TIME! ★

1. Care este principalul beneficiu al utilizării unui Load Balancer?
 - Creșterea spațiului de stocare.
 - Asigurarea disponibilității ridicate și a scalabilității.
 - Criptarea datelor.
2. Ce tip de Load Balancer ai folosi pentru a distribui traficul între serverele web și serverele de baze de date, fără a expune bazele de date la internet?
 - Public Load Balancer
 - Internal Load Balancer
 - Nu se poate face acest lucru.
3. Ce componentă a Load Balancer-ului verifică dacă mașinile virtuale din backend sunt funcționale?
 - Frontend IP Configuration
 - Backend Pool
 - Health Probes
4. La ce nivel al modelului OSI operează Azure Load Balancer (Standard/Basic)?
 - Layer 2 (Data Link)
 - Layer 4 (Transport)
 - Layer 7 (Application)
5. Ce serviciu de load balancing ai folosi pentru a distribui traficul unei aplicații web către utilizatori din Europa și America, direcționându-i către cea mai apropiată

- regiune Azure?
- a) Internal Load Balancer
 - b) Azure Load Balancer (Public)
 - c) Azure Front Door

(Răspunsuri la finalul manualului)

Ești un adevărat dirijor al traficului cloud. Știi cum să gestionezi fluxuri masive de date și să menții aplicațiile online, indiferent de situație.

 Achievement Deblocat: Scaling Maestro 

+350 XP

CAPITOLUL 14: Laborator Practic - Construirea unei Rețele Secure

Tema Gamification: “Fortăreața Digitală”

Nivel: Intermediate-Advanced (

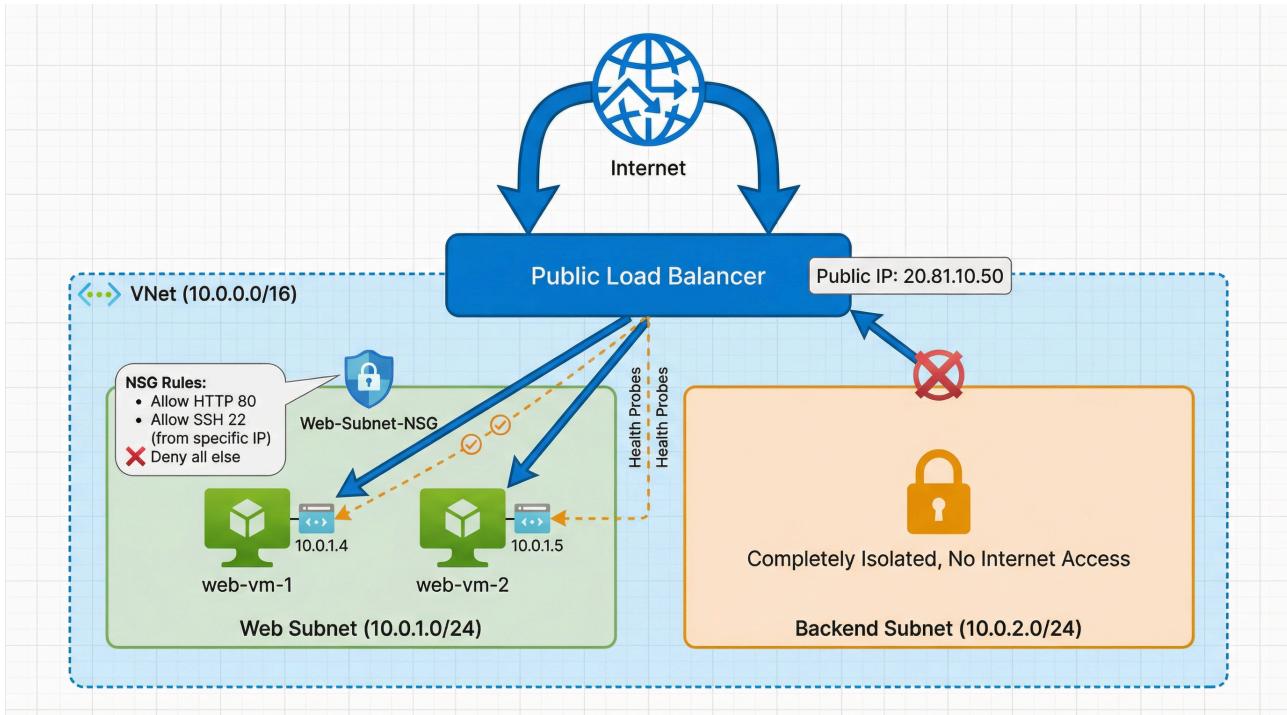
Acum este momentul să combini toate cunoștințele acumulate. În acest laborator final, vei construi o arhitectură de rețea clasică și sigură, cu două niveluri (two-tier): un nivel web expus la internet și un nivel de backend complet izolat. Vei folosi VNet, subnets, NSG-uri și un Load Balancer pentru a crea o fortăreață digitală. Finalizarea acestui laborator îți va aduce achievement-ul suprem de rețelistică: **Network Master**.

14.1 Obiectivul Laboratorului

Vei construi următoarea arhitectură:

- Un **VNet** cu două **subnets**: web-subnet și backend-subnet .
- Două mașini virtuale **Linux** în web-subnet , care vor acționa ca servere web.
- Un **Public Load Balancer** care distribuie traficul HTTP către cele două servere web.
- Un **Network Security Group (NSG)** care:
 - Permite traficul HTTP (port 80) din internet către web-subnet .

- Permite traficul SSH (port 22) doar de la adresa ta IP către web-subnet .
- Blochează orice alt trafic din internet.
- Izolează complet backend-subnet de internet.



14.2 Pașii Laboratorului

Challenge: “Construiește Fortăreața” (400 XP)

Urmează cu atenție pașii de mai jos în Azure Portal.

Pasul 1: Creează Rețeaua Virtuală și Subnet-urile

1. În Azure Portal, caută “Virtual networks” și apasă “Create”.
2. **Resource Group:** Creează unul nou, numit `Network - Lab - RG` .
3. **Name:** `Lab-VNet` .
4. **Region:** Alege o regiune (ex: West Europe).
5. Mergi la tab-ul **IP Addresses**.
6. **IPv4 address space:** Lasă valoarea implicită (ex: `10.0.0.0/16`).
7. Sub **Subnets**, apasă pe `default` . Redenumește-l în `web-subnet` și lasă address range-ul implicit (ex: `10.0.0.0/24`). Apasă “Save”.

8. Apasă “+ Add subnet”. Numește-l backend-subnet și setează un address range, de exemplu 10.0.1.0/24 . Apasă “Add”.
9. Apasă “Review + create” și apoi “Create”.

Pasul 2: Creează Network Security Group (NSG)

1. Caută “Network security groups” și apasă “Create”.
2. **Resource Group:** Selectează Network-Lab-RG .
3. **Name:** Web-Subnet-NSG .
4. **Region:** Alege aceeași regiune ca VNet-ul.
5. Apasă “Review + create” și apoi “Create”.
6. Mergi la resursa Web-Subnet-NSG și selectează **Inbound security rules**.
7. Apasă “+ Add”. Creează următoarele două reguli:
 - **Regula 1 (HTTP):**
 - Source: Any
 - Source port ranges: *
 - Destination: Any
 - Destination port ranges: 80
 - Protocol: TCP
 - Action: Allow
 - Priority: 100
 - Name: Allow-HTTP-Inbound
 - **Regula 2 (SSH):**
 - Source: IP Addresses
 - Source IP addresses/CIDR ranges: **Introdu adresa ta IP publică** (caută “what is my ip” pe Google).
 - Source port ranges: *
 - Destination: Any
 - Destination port ranges: 22
 - Protocol: TCP

- Action: Allow
- Priority: 110
- Name: Allow-SSH-From-My-IP

8. Acum, asociază NSG-ul cu subnet-ul. Mergi la `Web-Subnet-NSG`, selectează **Subnets** și apasă “+ Associate”.
9. Selectează `Lab-VNet` și apoi `web-subnet`. Apasă “OK”.

Pasul 3: Creează Mașinile Virtuale

1. Vei crea două mașini virtuale identice. Caută “Virtual machines” și apasă “Create”.
2. **Resource Group:** `Network-Lab-RG`.
3. **Virtual machine name:** `web-vm-1`.
4. **Region:** Aceeași regiune.
5. **Image:** Ubuntu Server 20.04 LTS.
6. **Size:** Alege o dimensiune mică, gratuită (ex: `Standard_B1s`).
7. **Authentication type:** Password. Alege un username și o parolă.
8. **Public inbound ports:** Selectează `None`. Vom controla accesul prin Load Balancer și NSG.
9. Mergi la tab-ul **Networking**.
10. **Virtual network:** `Lab-VNet`.
11. **Subnet:** `web-subnet`.
12. **Public IP:** `None`. VM-urile nu vor avea IP-uri publice individuale.
13. **NIC network security group:** `None`. Folosim NSG-ul de la nivel de subnet.
14. Apasă “Review + create” și apoi “Create”.
15. **Repetă pașii 1-14** pentru a crea a doua mașină virtuală, numită `web-vm-2`.

Pasul 4: Creează Load Balancer-ul

1. Caută “Load balancers” și apasă “Create”.
2. **Resource Group:** `Network-Lab-RG`.
3. **Name:** `Public-LB`.

4. **Region:** Aceeași regiune.
5. **SKU:** Standard .
6. **Type:** Public .
7. **Public IP address:** Apasă “Create new”. Numește-l LB-Public-IP și apasă “OK”.
8. Mergi la tab-ul **Frontend IP configuration** și apasă “+ Add a frontend IP configuration”.
9. **Name:** LB-Frontend .
10. **IP address:** Selectează LB-Public-IP pe care l-ai creat.
11. Apasă “Add”.
12. Mergi la tab-ul **Backend pools** și apasă “+ Add a backend pool”.
13. **Name:** LB-Backend-Pool .
14. **Virtual network:** Lab-VNet .
15. Sub **Virtual machines**, apasă “+ Add”. Selectează web-vm-1 și web-vm-2 și apasă “Add”.
16. Apasă “Save”.
17. Mergi la tab-ul **Health probes** și apasă “+ Add”.
18. **Name:** HTTP-Probe .
19. **Protocol:** TCP .
20. **Port:** 80 .
21. **Interval:** 5 (pentru testare rapidă).
22. Apasă “Add”.
23. Mergi la tab-ul **Load balancing rules** și apasă “+ Add a load balancing rule”.
24. **Name:** HTTP-Rule .
25. **Frontend IP address:** LB-Frontend .
26. **Backend pool:** LB-Backend-Pool .
27. **Protocol:** TCP .
28. **Port:** 80 .
29. **Backend port:** 80 .

30. **Health probe:** HTTP-Probe .

31. Apasă “Add”.

32. Apasă “Review + create” și apoi “Create”.

Pasul 5: Configurează și Testează Serverele Web

1. Trebuie să te conectezi la fiecare VM pentru a instala un server web. Dar cum, dacă nu au IP public? Vei folosi o resursă numită **Azure Bastion** sau o metodă mai simplă pentru acest laborator: alocarea temporară a unui IP public.
2. Mergi la `web-vm-1`, selectează **Networking**, apasă pe interfața de rețea (NIC), apoi pe **IP configurations**. Apasă pe `ipconfig1`, selectează **Associate public IP address**, creează unul nou și salvează. Notează IP-ul.
3. Conectează-te prin SSH la `web-vm-1` folosind IP-ul public temporar.
4. În terminalul SSH, rulează următoarele comenzi pentru a instala un server web simplu:

```
sudo apt-get update
sudo apt-get install -y nginx
echo "Hello from web-vm-1" | sudo tee /var/www/html/index.html
```

5. Deconectează-te. Mergi înapoi la configurația IP a VM-ului și **disociază** IP-ul public.
6. **Repetă pașii 2-5** pentru `web-vm-2`, dar schimbă textul în `echo "Hello from web-vm-2"`.
7. Acum, găsește IP-ul public al Load Balancer-ului (mergi la resursa `Public-LB` și uită-te în Overview).
8. Deschide un browser și accesează `http://<IP-ul_Public_al_LB-ului>`.
9. Ar trebui să vezi mesajul “Hello from web-vm-1” sau “Hello from web-vm-2”. Dacă dai refresh de mai multe ori, mesajul ar trebui să se schimbe, demonstrând că Load Balancer-ul distribuie traficul!

Pasul 6: Curățenie (Foarte Important!)

1. Mergi la Resource Group-ul `Network-Lab-RG`.

2. Apasă “Delete resource group” și confirmă ștergerea.

★ QUIZ TIME! ★

1. De ce nu am alocat IP-uri publice direct mașinilor virtuale în arhitectura finală?
 - a) Pentru că este mai scump.
 - b) Pentru a le securiza, expunându-le doar prin Load Balancer, care este un singur punct de intrare controlat.
 - c) Pentru că Ubuntu nu suportă IP-uri publice.
2. Ce rol a avut NSG-ul în acest laborator?
 - a) A distribuit traficul între cele două VM-uri.
 - b) A acționat ca un firewall, permitând doar traficul HTTP și SSH de la surse autorizate.
 - c) A crescut viteza de procesare a VM-urilor.
3. Dacă ai fi vrut să permiti accesul la o bază de date pe backend-subnet de la web-subnet, dar nu și de pe internet, ce ai fi făcut?
 - a) Ai fi creat o regulă NSG care permite traficul de la web-subnet la backend-subnet pe portul bazei de date.
 - b) Ai fi alocat un IP public bazei de date.
 - c) Ai fi mutat baza de date în web-subnet.
4. De ce este importantă curățenia (ștergerea Resource Group-ului) după laborator?
 - a) Pentru a elibera adresele IP private.
 - b) Pentru a opri toate costurile asociate cu resursele create (VM-uri, IP-uri publice, Load Balancer).
 - c) Pentru a reseta parolele VM-urilor.
5. Ce componentă a Load Balancer-ului a fost responsabilă pentru a decide dacă o VM este aptă să primească trafic?
 - a) Backend Pool
 - b) Health Probe
 - c) Load Balancing Rule

(Răspunsuri la finalul manualului)

Felicitări, Arhitect de Rețea! Ai construit o fortăreață digitală funcțională și sigură în Azure. Ai demonstrat măiestrie în utilizarea VNet-urilor, NSG-urilor și a Load Balancer-ului.

 Achievement Deblocat: Network Master 

+400 XP



SECȚIUNEA FINALĂ (Partea a IV-a)

Răspunsuri Quiz-uri

Capitolul 11:

1. b) O rețea privată și izolată în Azure pentru resursele tale.
2. b) Pentru a organiza și securiza resursele mai eficient.
3. b) Adresă IP Publică
4. c) 5
5. b) Pentru servere care trebuie să fie accesibile constant la aceeași adresă.

Capitolul 12:

1. b) Filtrează traficul de rețea pe baza unor reguli de securitate.
2. b) Înainte
3. b) Blochează tot traficul care intră, cu excepția cazului în care este permis de o regulă cu prioritate mai mare.
4. b) Asocierea cu subnet-ul.
5. b) O etichetă care reprezintă un grup de adrese IP pentru un serviciu Azure.

Capitolul 13:

1. b) Asigurarea disponibilității ridicate și a scalabilității.
2. b) Internal Load Balancer
3. c) Health Probes
4. b) Layer 4 (Transport)
5. c) Azure Front Door

Capitolul 14:

1. b) Pentru a le securiza, expunându-le doar prin Load Balancer, care este un singur punct de intrare controlat.
 2. b) A acționat ca un firewall, permitând doar traficul HTTP și SSH de la surse autorizate.
 3. a) Ai fi creat o regulă NSG care permite traficul de la web-subnet la backend-subnet pe portul bazei de date.
 4. b) Pentru a opri toate costurile asociate cu resursele create (VM-uri, IP-uri publice, Load Balancer).
 5. b) Health Probe
-

Glosar de Termeni (Partea a IV-a)

Termen	Definiție
VNet (Virtual Network)	O rețea privată și izolată în Azure.
Subnet	O diviziune a spațiului de adrese al unui VNet.
CIDR	Classless Inter-Domain Routing. Notația folosită pentru a defini un range de adrese IP (ex: 10.0.0.0/16).
NIC (Network Interface)	O componentă virtuală care permite unei mașini virtuale să comunice în rețea.
NSG (Network Security Group)	Un firewall virtual care filtrează traficul la nivel de subnet sau NIC.
Service Tag	O etichetă predefinită de Microsoft care reprezintă un grup de adrese IP pentru un serviciu Azure.
Load Balancer	Un serviciu care distribuie traficul de rețea către un grup de servere backend.
Backend Pool	Grupul de resurse (ex: VM-uri) care primesc trafic de la un Load Balancer.
Health Probe	O verificare periodică a stării de sănătate a resurselor dintr-un backend pool.
VNet Peering	Conectarea a două VNet-uri pentru a permite comunicarea între ele.
VPN Gateway	Un serviciu care permite conectarea securizată a unei rețele on-premises la un VNet prin internet.
ExpressRoute	Un serviciu care oferă o conexiune privată, dedicată, între o rețea on-premises și Azure.

Resurse pentru Aprofundare (Networking)

Documentație Oficială Microsoft:

- [Azure Virtual Network Documentation](#)

- [Azure Load Balancer Documentation](#)
- [Network Security Groups](#)
- [Choose the right load-balancing service for your application](#)

Certificări Recomandate:

- **AZ-104: Azure Administrator** - Include managementul complet al rețelelor virtuale.
- **AZ-700: Designing and Implementing Azure Networking Solutions** - Certificarea specializată pentru ingineri de rețea.
- **AZ-305: Azure Solutions Architect** - Design de arhitecturi de rețea complexe.

Hands-on Labs:

- [Microsoft Learn - Introduction to Azure Virtual Networks](#)
- [Microsoft Learn - Load balance web traffic with Azure Application Gateway](#)

Tabelul Final de Achievement-uri (Partea a IV-a)

Achievement	Descriere	XP
Network Architect	Completează Capitolul 11 și înțelege VNet-urile	250
Gatekeeper	Completează Capitolul 12 și stăpânește NSG-urile	300
Scaling Maestro	Completează Capitolul 13 și înțelege Load Balancer-ul	350
Network Master	Completează Laboratorul și construiește o rețea sigură	400

Total XP Posibil (Partea a IV-a): 1,300 XP

Mesaj Final (Partea a IV-a)

Felicitări pentru finalizarea acestui modul crucial! Ai devenit un arhitect de rețea capabil să proiecteze, să securizeze și să scaleze infrastructura care stă la baza oricărei aplicații cloud. Aceste competențe sunt printre cele mai căutate în industrie.

Ai parcurs o călătorie impresionantă, de la fundamentele cloud, la calcul, stocare și acum rețelistică. Ai adunat o colecție impresionantă de achievement-uri și ai acumulat cunoștințe practice valoroase.

Drumul tău în Azure nu se oprește aici. Acesta este doar începutul!  