Sesiunea 05: Pregătire pentru VM Deployment

Azure Fundamentals · Sesiunea 5 din 10

Astăzi nu creăm încă mașini virtuale — dar după această oră, veți înțelege exact ce se întâmplă în spatele lor: porturi, protocoale de acces și reguli de securitate.

WEBINAR · CURS INTRODUCTIV AZURE

Agenda sesiunii de astăzi

Parcurgem șase capitole esențiale care pregătesc terenul pentru sesiunea viitoare, când vom crea primele mașini virtuale.

01

Ce este un Port?

Diferența dintre IP și Port — analogia clădirii cu apartamente

02

RDP versus SSH

Cele două protocoale cu care veți lucra cel mai mult în Azure

03

Structura unei reguli NSG

Cele șase elemente ale unui Network Security Group

04

Exercițiu Practic

Creăm Resource Group, VNet și NSG cu o regulă reală

05

Greșeli Clasice & Security Mindset

Ce să NU faceți niciodată în producție și cum gândește un arhitect de securitate

PARTEA 1 · PORTURI

Ce este un Port?

Hai să începem cu o întrebare simplă. Dacă adresa IP este adresa unei clădiri... **cum ajungi la apartamentul corect?** Știți strada, știți numărul. Dar clădirea are zece etaje și cincizeci de apartamente. Unde bați la ușă?

> **IP-ul este adresa clădirii. Portul este apartamentul.** Un server poate avea un singur IP, dar poate asculta pe sute sau chiar mii de porturi simultan. Portul îți spune ce serviciu răspunde.

PARTEA 1 · PORTURI

Porturile cele mai importante

Același server, același IP — dar în interior, servicii diferite ascultă pe porturi diferite. Iată cele mai importante porturi pe care le veți întâlni în Azure:

Port 80 — HTTP

Traficul web obișnuit, nesecurizat. Browserul dvs. accesează site-uri prin acest port când adresa începe cu `http://`. În producție modernă, traficul pe portul 80 este de obicei redirecționat automat spre portul 443.

Port 443 — HTTPS

Traficul web securizat, criptat cu TLS/SSL. Orice site serios folosește HTTPS. Browserul afișează lacătul verde. Acesta este portul pe care îl deschideți pentru utilizatorii publici ai unui server web.

Port 3389 — RDP

Remote Desktop Protocol — pentru conexiuni vizuale la mașini Windows. Vă permite să vedeți desktopul și să lucrați de la distanță exact ca și cum ați sta în fața calculatorului.

Port 22 — SSH

Secure Shell — pentru conexiuni în terminal la servere Linux. Nu există interfață grafică: introduceți comenzi text, eficient și sigur. Conexiunea este criptată end-to-end.

> 💡 **Rețineți:** Fără port, IP-ul singur nu vă spune nimic despre ce puteți face cu serverul respectiv. Portul este cel care direcționează traficul către serviciul corect.

PARTEA 2 · RDP VS SSH

RDP versus SSH: Cum accesăm serverele?

Acestea sunt cele două protocoale cu care veți lucra cel mai des în sesiunile viitoare de Azure. Înțelegerea diferenței dintre ele este esențială.

RDP — Remote Desktop Protocol

Port: 3389 · **Sistem:** Windows

Când te conectezi prin RDP la o mașină Windows, ai parte de o **interfață grafică completă**. Vedeți desktopul, puteți da click, puteți deschide aplicații, puteți naviga în File Explorer. Este exact ca și cum ați sta fizic în fața calculatorului respectiv, dar de la distanță, prin internet.

Se folosește clientul **mstsc.exe** pe Windows sau aplicația "Microsoft Remote Desktop" pe Mac/iOS/Android. Introduceți IP-ul serverului, username și parolă — și sunteți conectat.

- Interfață grafică completă
- Ideal pentru utilizatori Windows
- Ușor de folosit de oricine
- Consum mai mare de bandă

SSH — Secure Shell

Port: 22 · **Sistem:** Linux

SSH este conexiunea pentru servere Linux. **Nu există interfață grafică** — aveți un terminal, un ecran cu text, și introduceți comenzi. Sună intimidant la început, dar este mult mai eficient pentru administrarea serverelor: mai rapid, mai puțin consumator de resurse, complet scriptabil.

Se folosește clientul **ssh** din terminal (disponibil nativ pe Mac, Linux și Windows 10+) sau aplicații precum **PuTTY**. Autentificarea se face cu parolă sau, mai sigur, cu chei SSH.

- Terminal text, fără GUI
- Standard pentru servere Linux
- Eficient și ușor scriptabil
- Consum minim de bandă

PARTEA 2 · RDP VS SSH

De ce contează alegerea protocolului?

Săptămâna viitoare vom crea împreună două mașini virtuale în Azure. Iată exact ce vom face și de ce cunoașterea de astăzi este fundamentul pentru acea sesiune.

VM Windows → RDP

Vom crea o mașină virtuală cu Windows Server. Ne vom conecta prin portul 3389 folosind Remote Desktop. Vom vedea desktopul și vom configura serverul vizual.

VM Linux → SSH

Vom crea o mașină virtuală cu Ubuntu Linux. Ne vom conecta prin portul 22 folosind SSH. Vom rula comenzi în terminal și vom administra serverul eficient.

NSG → Securitate

Ambele conexiuni vor fi protejate de reguli NSG pe care le vom configura corect. Numai IP-ul nostru va putea accesa porturile de management.

⚠️ **Gândiți-vă la asta:** Dacă deschid portul 3389 pentru toată lumea pe internet, oricine — orice bot, orice atacator — ar putea încerca să se conecteze la desktopul vostru. Acesta este exact motivul pentru care există NSG-urile.

PARTEA 3 · NSG

Ce este un Network Security Group (NSG)?

Network Security Group este portarul de la intrarea în clubul vostru. Un NSG este o resursă Azure care conține o listă de reguli de securitate — fiecare regulă specifică ce trafic este permis sau blocat. NSG-ul poate fi asociat unui subnet sau direct unei plăci de rețea (NIC) a unei mașini virtuale.

Ce face un NSG?

- Filtrează traficul de intrare (**Inbound**) și de ieșire (**Outbound**)
- Evaluează regulile în ordinea priorității, de la numărul cel mai mic la cel mai mare
- Aplică **prima regulă care se potrivește** și ignoră restul
- Are reguli implicite (default) care nu pot fi șterse, dar pot fi suprascrise

Unde se poate atașa un NSG?

- **Subnet** — protejează toate resursele dintr-un subnet
- **NIC (Network Interface Card)** — protejează o singură mașină virtuală
- Puteți aplica NSG-uri la ambele niveluri simultan pentru dublă protecție
- Recomandat: NSG la nivel de subnet + NSG specific per VM critică

PARTEA 3 · NSG

Cele 6 Elemente ale unei Reguli NSG

Fiecare regulă NSG este definită prin șase câmpuri. Înțelegerea fiecărui câmp este esențială pentru configurarea corectă a securității rețelei voastre.

1

Source

De unde vine traficul? Poate fi un IP specific (ex: `85.120.45.10`), un range CIDR (ex: `192.168.1.0/24`), un Service Tag (ex: `Internet`, `VirtualNetwork`) sau `Any`.

2

Source Port

Portul de pe care pleacă cererea. În general se lasă pe `*` (Any), deoarece portul sursă este ales aleatoriu de sistemul de operare al clientului și nu poate fi controlat.

3

Destination

Unde merge traficul? De obicei mașina voastră virtuală, un subnet specific, sau un Service Tag. Poate fi un IP, un range CIDR, sau `Any`.

4

Destination Port

Portul la care bate traficul. Aici specifici exact: `3389` pentru RDP, `22` pentru SSH, `443` pentru HTTPS. Poți specifica un range: `8000-8080`.

5

Protocol

TCP, UDP, sau Any. RDP și SSH folosesc TCP. Unele servicii (DNS, VoIP) folosesc UDP. Pentru majority serviciilor web, specificați TCP.

6

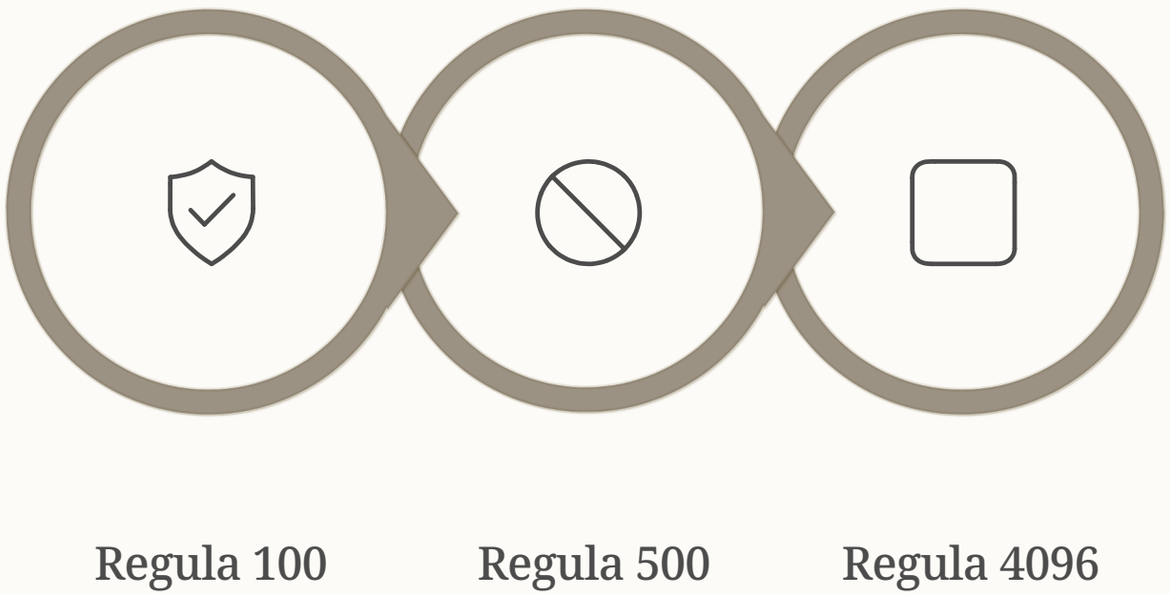
Action + Priority

Allow sau Deny — lași să treacă sau blochezi. **Priority** — număr între 100 și 4096. Regulile sunt evaluate de la cel mai mic număr la cel mai mare. Prima regulă care se potrivește câștigă.

PARTEA 3 · NSG

Cum funcționează Prioritatea în NSG?

Portarul verifică lista de sus în jos și aplică **prima regulă care se potrivește**. Regulile cu număr de prioritate mai mic sunt verificate primele. Odată ce o regulă se potrivește, restul regulilor sunt ignorate pentru acea conexiune.



Exemplul de mai sus ilustrează o configurație corectă: regula cu prioritate 100 permite SSH doar de la IP-ul tău specific. Dacă cineva altcineva încearcă SSH, regula 100 nu se potrivește (IP-ul sursă e diferit), regula 500 se potrivește și blochează conexiunea. Regula default 65500 `DenyAllInBound` există întotdeauna și nu poate fi ștearsă — este plasa de siguranță.

> 💡 **Regulă de aur:** Numerotați regulile cu salturi — 100, 200, 300 — nu 1, 2, 3. Astfel puteți insera reguli noi între ele fără să renumerotați totul.

PARTEA 4 · EXERCIȚIU PRACTIC

Exercițiu Practic — Pasul 1 și 2

Acum punem în practică tot ce am discutat. Urmați pașii în ordinea indicată. Durată estimată: 15–20 minute.

1 Creați un Resource Group

Navigați în Azure Portal la `Resource Groups` → `+ Create`. Numiți-l `rg-s05-[prenumele_vostru]` (ex: `rg-s05-andrei`). Alegeți regiunea `West Europe` sau `North Europe`. Dați click pe **Review** + **Create**, apoi **Create**. Resource Group-ul este containerul care va ține toate resursele exercițiului de astăzi.

2 Creați o Rețea Virtuală (VNet)

În interiorul Resource Group-ului creat, adăugați o nouă resursă: `Virtual Network`. Numiți-o `s05-vnet-[prenumele_vostru]`. Lăsați valorile default pentru spațiul de adrese (`10.0.0.0/16`) și subnet-ul default (`10.0.0.0/24`). VNet-ul este rețeaua privată în care vor trăi mașinile voastre virtuale.

PARTEA 4 · EXERCIȚIU PRACTIC

Exercițiu Practic — Pasul 3 și 4

1 Creați un Network Security Group

Adăugați o nouă resursă în Resource Group: `Network Security Group`. Numiți-l `s05-nsg-[prenumele_vostru]`. Același Resource Group, aceeași regiune. După creare, navigați în NSG și explorați tab-urile **Inbound security rules** și **Outbound security rules**. Observați că există deja câteva reguli default — acestea sunt generate automat de Azure și nu pot fi șterse.

2 Adăugați o Regulă Inbound pentru RDP

În NSG-ul vostru, mergeți la **Inbound security rules** → + **Add** și completați astfel:

- **Name:** `Allow-RDP-MyIP`
- **Source:** `My IP address` — Azure completează automat IP-ul vostru public
- **Source port ranges:** `*` (Any)
- **Destination:** `Any`
- **Destination port ranges:** `3389`
- **Protocol:** `TCP`
- **Action:** `Allow`
- **Priority:** `1000`

🔑 **Diferența crucială:** Source este `My IP Address`, nu `Any`. Aceasta înseamnă că **doar voi** vă puteți conecta prin RDP. Nimeni altcineva din întreaga lume nu poate accesa portul 3389. Aceasta este securitatea de bază.

PARTEA 4 · EXERCIȚIU PRACTIC

Ce ar trebui să vedeți după exercițiu

Dacă ați urmat toți pașii corect, NSG-ul vostru ar trebui să arate astfel. Verificați fiecare element înainte de a continua.

Câmp	Valoarea corectă	De ce?
Name	`Allow-RDP-MyIP`	Numele regulii este descriptiv — știți imediat ce face
Source	IP-ul vostru public (ex: 85.x.x.x)	Numai voi puteți accesa — securitate maximă
Destination Port	3389	Portul RDP — exact ce trebuie, nimic în plus
Protocol	TCP	RDP folosește TCP, nu UDP
Action	Allow	Permitem conexiunea de la sursa specificată
Priority	1000	Lăsăm spațiu pentru reguli mai urgente (100–900)

PARTEA 5 · GREȘELI CLASICE

Cea mai periculoasă regulă pe care o puteți crea

> Source: **Any** · Destination: **Any** · Port: **Any** · Action: **Allow**

Ce ați făcut cu această regulă? Ați deschis serverul **complet**. Oricine, de oriunde în lume, pe orice port, poate să intre. Este ca și cum ați lăsa ușa casei deschisă, ați stinge lumina și ați pleca în vacanță două săptămâni.

Aceasta este **greșeala numărul unu** pe care o întâlnim în producție. NSG-uri cu reguli Any-Any-Allow create în grabă, pentru că ceva nu mergea, și uitate acolo pentru luni de zile. În acel timp, boți automatizați scanează internetul 24/7 și încearcă să se conecteze pe portul 3389 cu parole comune.

❌ Niciodată în Producție

Source: Any Port: Any Action: Allow **Aceasta este o invitație pentru atacatori.**

✅ Practica Corectă

Source: IP-ul tău specific Port: exact portul necesar Action: Allow **Principiul least privilege.**

🔒 Regula de Aur

Never Any-Any-Allow în producție. Niciodată. Fără excepții. Nu există o situație care să justifice această configurație.

PARTEA 5 · GREȘELI CLASICE

Greșeli frecvente — Lista completă

Dincolo de Any-Any-Allow, există și alte greșeli comune pe care studenții (și uneori profesioniștii) le fac cu NSG-urile:

→ Deschiderea portului 22 sau 3389 din Any

Chiar dacă aveți parolă puternică, expunerea porturilor de management la internet înseamnă că serverul vostru va fi atacat constant prin brute force. Soluția: restricționați la IP-ul vostru sau folosiți Azure Bastion.

→ Folosirea priorităților consecutive (1, 2, 3...)

Dacă trebuie să inserați o regulă nouă între prioritatea 1 și 2, nu mai aveți unde. Folosiți întotdeauna salturi: 100, 200, 300. Lăsați spațiu pentru viitor.

→ Uitarea că IP-ul vostru de acasă se schimbă

IP-urile rezidențiale sunt de obicei dinamice — se pot schimba după restart de router. Dacă v-ați restricționat accesul la IP-ul vechi, nu vă mai puteți conecta. Verificați și actualizați regula NSG când e necesar.

→ NSG atașat la NIC, nu la subnet

Dacă aveți mai multe VM-uri într-un subnet, atașați NSG-ul la subnet pentru a proteja toate VM-urile simultan. Un NSG atașat doar la o NIC protejează o singură mașină.

PARTEA 6 · SECURITY MINDSET

Jocul Security Consultant

Sunteți consultantul de securitate al unui client. Clientul are un **server web** care trebuie să fie accesibil utilizatorilor din toată lumea. Ce reguli NSG configurați? Gândiți-vă înainte să citiți răspunsul.

> Portul 443 (HTTPS) din **Any** — *Allow* · Portul 80 (HTTP) din **Any** — *Allow* (sau Deny dacă redirecționați spre 443) · Portul 3389 și 22 din **Any** — *niciodată*

De ce deschideți 443 din Any?

Website-ul trebuie să fie public. Utilizatorii din toată lumea trebuie să îl acceseze. Nu puteți ști dinainte IP-urile lor. Prin urmare, Source = Any este corect și necesar pentru portul 443. Aceasta este o decizie de business, nu o greșeală de securitate.

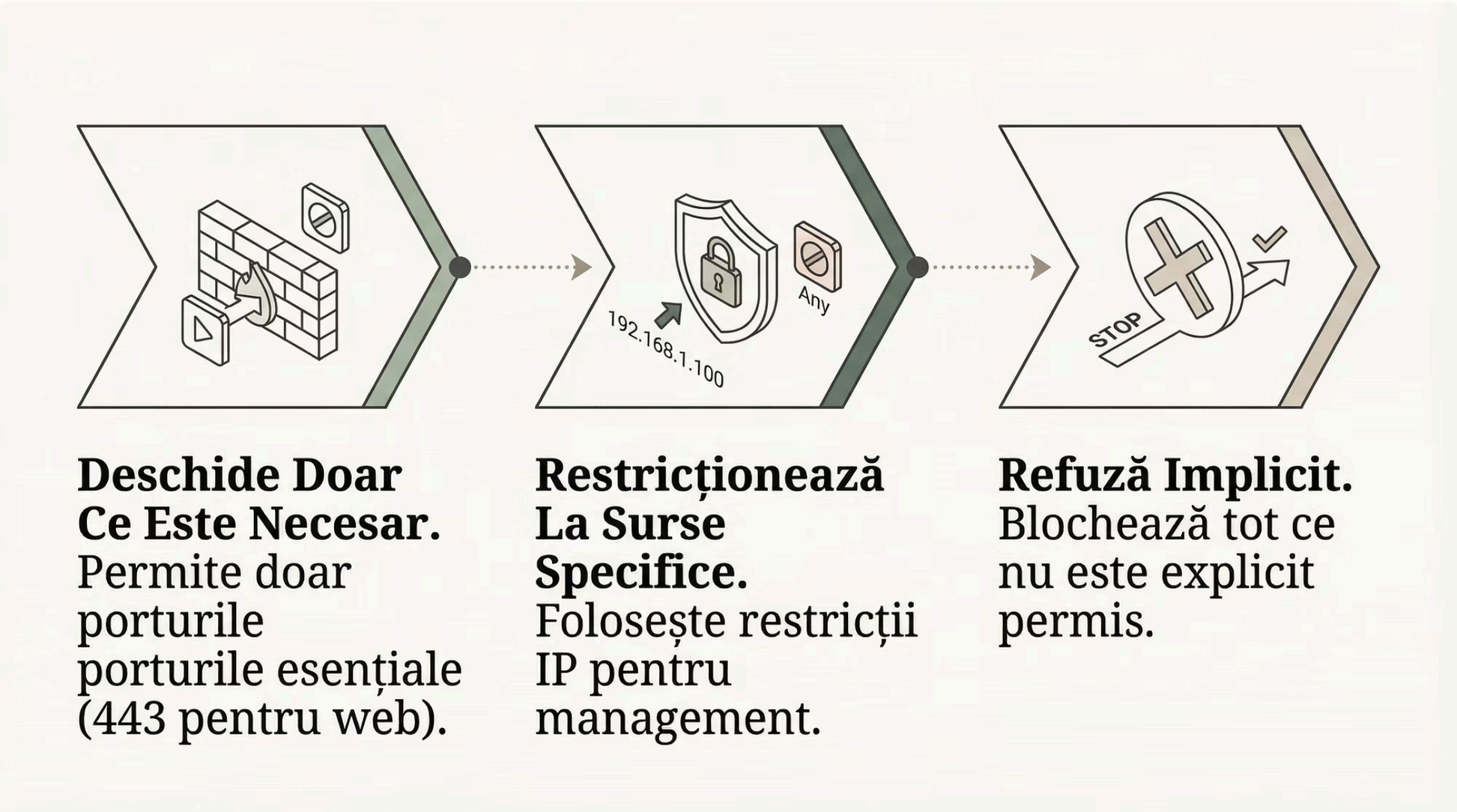
De ce NU deschideți 3389/22 din Any?

Porturile de management (RDP, SSH) nu trebuie să fie niciodată publice. Numai administratorii se conectează — și aceștia au IP-uri cunoscute sau folosesc VPN/Bastion. Deschiderea acestor porturi public este o vulnerabilitate critică, nu o comoditate.

PARTEA 6 · SECURITY MINDSET

Gândirea unui Arhitect de Securitate

Securitatea nu înseamnă să blocați totul. Și nu înseamnă să deschideți totul. Înseamnă să **deschideți exact ce trebuie, pentru exact cine trebuie**. Aceasta este esența principiului *Least Privilege*.



Fiecare regulă NSG pe care o creați trebuie să răspundă la trei întrebări: **Cine?** (Source), **Ce?** (Destination Port), **De ce?** (există o justificare de business documentată). Dacă nu puteți răspunde la toate trei, nu creați regula.

RECAPITULARE

Ce am învățat astăzi — Rezumat

Înainte să trecem la curățenie și temă, să recapitulăm rapid tot ce am acoperit în această sesiune.

Porturi

IP = adresa clădirii. Port = apartamentul. Un server ascultă simultan pe sute de porturi. Porturile cheie: 80 (HTTP), 443 (HTTPS), 3389 (RDP), 22 (SSH).

RDP vs SSH

RDP (3389) = acces vizual la Windows. SSH (22) = terminal text pentru Linux. Ambele sunt protocoale de management și trebuie protejate corespunzător.

NSG

6 elemente: Source, Source Port, Destination, Destination Port, Protocol, Action + Priority. Prima regulă care se potrivește câștigă. Evaluare de la prioritate mică la mare.

Securitate

Never Any-Any-Allow. Deschideți exact ce trebuie, pentru exact cine trebuie. Porturile de management (RDP, SSH) niciodată publice. Least Privilege mereu.

CURĂȚENIE AZURE

Important: Ștergeți Resursele după Exercițiu

Înainte să închidem sesiunea, o regulă importantă de igienă Azure pe care o vom respecta la fiecare sesiune de curs.

> Ștergeți Resource Group-ul `rg-s05-[prenumele_vostru]`. Ștergând Resource Group-ul, ștergeți automat **tot ce este în el**: VNet, Subnet, NSG, și orice altă resursă creată în el.

01

Navigați la Resource Groups

În Azure Portal, căutați `Resource Groups` în bara de search de sus.

02

Selectați rg-s05-[prenumele]

Click pe Resource Group-ul creat la exercițiu.

03

Delete Resource Group

Click pe **Delete resource group**, introduceți numele pentru confirmare, și confirmați ștergerea.

04

Așteptați confirmarea

Ștergerea durează 2–5 minute. Veți primi o notificare când s-a finalizat.

💰 **De ce?** Azure taxează pentru resursele care rulează. O bună practică este să curățați după fiecare exercițiu. Vă economisiți credite și mențineți contul ordonat. Mașinile virtuale (pe care le vom crea în sesiunea 6) costă bani chiar și când sunt oprite — de aceea sunt importante regulile de curățenie.

TEME

Tema pentru Sesiunea 05

Tema are două puncte și trebuie trimisă înainte de sesiunea viitoare. Scopul temei nu este să copiați din documentație — ci să înțelegeți și să puteți explica cu propriile cuvinte.

1

Punctul 1 — Explicație în cuvinte proprii

Explicați în **cinci propoziții** ce este un port și ce este un NSG. Nu copiați din documentație. Scrieți ca și cum ați explica unui coleg care nu știe nimic despre Azure sau rețele.

Întrebări ghid: Ce face un port? De ce avem nevoie de el? Ce face un NSG? Cum funcționează regulile lui? De ce e important să îl configurăm corect?

2

Punctul 2 — Analiză de securitate

Care este mai sigur și **de ce**?

- Varianta A: Allow port 3389 din `Any`
- Varianta B: Allow port 3389 din `My IP Address`

Răspunsul trebuie să includă o justificare clară, nu doar "B este mai sigur". Explicați ce risc concret există în varianta A și cum îl elimină varianta B.

Sesiunea Viitoare: Prima Mașină Virtuală!

Tot ce am discutat astăzi va prinde viață în sesiunea 6. Veți ști exact de ce funcționează, pentru că înțelegeți rețeaua și regulile care o guvernează.

🖥️ VM Windows

Creăm prima mașină virtuală cu Windows Server în Azure și ne conectăm prin RDP

🐧 VM Linux

Creăm o mașină virtuală cu Ubuntu Linux și ne conectăm prin SSH din terminal

🔒 NSG Live

Configurăm regulile NSG în timp real și vedem cum protejează mașinile noastre

Vă mulțumim pentru atenție! Ne vedem la Sesiunea 06. 🚀

AZURE.MICROSOFT.COM/LEARN

PORTAL.AZURE.COM