Azure Firewall

Ghid complet zero-to-hero pentru ingineri de rețea și arhitecți Azure

VERSIUNE 2026

PREDARE PRACTICĂ ÎN AZURE PORTAL

Despre acest curs

Ce vei învăța astăzi

01

Fundamente

De ce există Azure Firewall, comparație cu NSG, App Gateway, Load Balancer și concepte de rețea esențiale.

02

SKU-uri și Arhitecturi

Basic vs Standard vs Premium, modele Hub-and-Spoke, Secured Virtual Hub și Forced Tunneling.

03

Deploy & Configurare

Laborator zero-to-hero în Azure Portal: VNet, subnets, Firewall Policy, reguli, UDR și DNS.

04

Operare & Troubleshooting

Monitorizare, metrici, logging, cele mai frecvente probleme și bune practici de inginerie.

Nivel

De la concepte de bază până la design și operare avansată în producție.

Public țintă

Studenți Azure, administratori, ingineri de rețea, DevOps/SRE, arhitecți cloud.

De ce există Azure Firewall și de ce contează

În orice infrastructură există un moment în care nu mai este suficient să spui că ai o rețea, câteva VM-uri și niște NSG-uri. Ai nevoie de un **punct central** prin care poți controla, jurnaliza și securiza traficul. Exact aici intră Azure Firewall.

Analogia cu campusul de birouri

NSG

Agentul de pază de la ușa fiecărei clădiri. Controlează accesul local, la nivel de NIC sau subnet.

Application Gateway

Recepția web pentru vizitatorii HTTP și HTTPS. Se ocupă de routing, WAF și TLS termination.

Load Balancer

Dirijorul care împarte mașinile spre mai multe intrări. Distribuie trafic L4 eficient.

Azure Firewall

Postul central de control care vede fluxurile importante, aplică reguli unificate și ține jurnalul tuturor deciziilor.

Mesaj cheie: Azure Firewall nu înlocuiește toate celelalte servicii de rețea. El **completează** NSG, Application Gateway, Load Balancer și gateway-urile de VPN/ExpressRoute, oferind control și inspecție centralizată.

Ce oferă Azure Firewall concret

Control centralizat est-vest și nord-sud

Controlează traficul dintr-un singur punct, indiferent dacă fluxul este între subnets, între VNet-uri sau spre internet.

Reguli L3–L7

Aplică reguli de rețea (IP, port, protocol), reguli de aplicație (FQDN, URL categories) și reguli NAT (SNAT, DNAT).

Jurnalizare și observabilitate nativă

Integrare nativă cu Azure Monitor, Log Analytics și Workbooks pentru vizibilitate completă asupra traficului.

Serviciu PaaS, scalare automată

Nu administrezi appliance-uri, patch-uri sau HA manual. Azure Firewall se scalează automat după cerere.

Comparație: Azure Firewall vs alte servicii Azure

Serviciu	Nivel	Scop principal	Când îl folosești	Ce nu face
Azure Firewall	L3–L7	Control centralizat, NAT, filtrare, logging	Politică unificată pentru trafic inbound, outbound și inter-subnet/inter-VNet	Nu este reverse proxy web dedicat ca App Gateway
NSG	L3–L4	Allow/deny pe NIC sau subnet	Micro-segmentare locală, reguli simple bazate pe IP, port, protocol	Nu oferă policy centrală, NAT, TLS inspection sau web categories
Application Gateway	L7	Load balancing și protecție pentru trafic web HTTP/HTTPS	Aplicații web cu path-based routing, WAF, TLS termination	Nu gestionează generic tot traficul TCP/UDP
Load Balancer	L4	Distribuție de trafic TCP/UDP	Load balancing simplu și performant	Nu face filtrare aplicativă sau analiză avansată a fluxurilor
VPN/ExpressRoute Gateway	L3	Conectivitate între Azure și on-prem sau alte rețele	Transport privat/hibrid	Nu este firewall și nu înlocuiește regulile de securitate

În practică, o arhitectură matură le **combină**: NSG pentru segmentare locală, Azure Firewall pentru control centralizat, Application Gateway pentru web, iar Gateway-urile pentru conectivitate hibridă.

Concepte de rețea esențiale

Concepte fundamentale

- **Allow și Deny**

  Azure Firewall pornește cu **deny implicit**. Permiți explicit fluxurile dorite; tot restul este blocat.

- **Stateful Firewall**

  Dacă permiți o conexiune inițiată dintr-o parte, răspunsurile asociate sunt înțelese și permise fără reguli separate.

- **Layer 3 / Layer 4 / Layer 7**

  L3 = IP sursă/destinație. L4 = porturi și protocoale (TCP 443, UDP 53). L7 = FQDN, URL category, TLS inspection, IDPS.

Concepte de rutare și NAT

- **SNAT**

  Firewall-ul schimbă IP-ul sursă la ieșire pentru a reprezenta resursa outbound.

- **DNAT**

  Firewall-ul publică un serviciu intern pe baza unei adrese IP publice și port.

- **UDR (User Defined Route)**

  Route table cu next hop definit astfel încât traficul să treacă obligatoriu prin firewall.

- **DNS Proxy**

  Foarte important pentru filtrarea corectă pe FQDN în network rules. Fără DNS Proxy, regulile FQDN pot fi inconsistente.

Real life: Dacă NSG-ul este semaforul local dintr-o intersecție, Azure Firewall este centrul de control al traficului din tot orașul. El nu doar spune stop sau merge; știe și pe unde ar trebui să meargă traficul și de ce.

SKU-uri: Basic vs Standard vs Premium

Capabilitate	Basic	Standard	Premium	Observații practice
Scalare	Până la 250 Mbps	Până la 30 Gbps	Până la 100 Gbps	Alege după cerințe de throughput și complexitate
Threat Intelligence	Nu	Da	Da	Util pentru deny/alert către IP-uri și domenii malițioase
DNS Proxy și Custom DNS	Nu	Da	Da	Important pentru filtrare robustă pe FQDN
Web Categories	Nu	Da	Da	Util pentru control outbound web în enterprise
TLS Inspection și IDPS	Nu	Nu	Da	Necesare pentru medii sensibile și inspecție avansată
Cost	Mai mic	Mediu	Mai mare	Standard = punct de pornire corect pentru enterprise

Regulă practică: Pentru majoritatea mediilor enterprise, **Standard** este punctul de pornire corect. **Premium** este justificat când ai nevoie de TLS inspection, IDPS și control mai profund. **Basic** este pentru scenarii mici, simple sau cu constrângeri de cost.

Modele arhitecturale

Single VNet simplu

Bun pentru laboratoare sau medii mici. Firewall-ul stă în același VNet cu workload-urile. Simplu de configurat și de înțeles.

Hub-and-Spoke

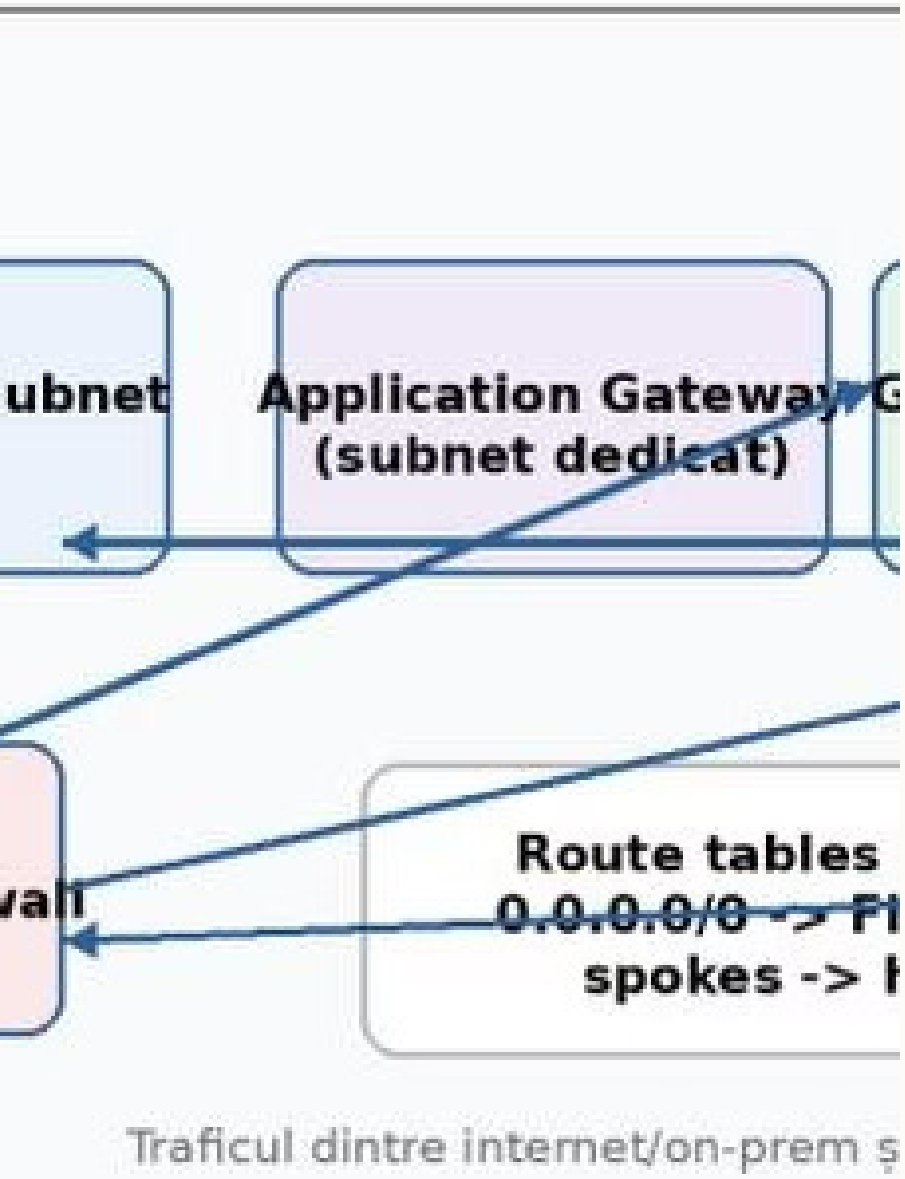
Modelul enterprise clasic. Firewall-ul stă în hub și protejează mai multe spoke-uri. Route tables direcționează tot traficul prin hub.

Secured Virtual Hub / Virtual WAN

Variantă managed când vrei integrare strânsă cu topologii mari și conectivitate globală. Azure gestionează infrastructura hub-ului.

Forced Tunneling

Folosit când vrei ca traficul de ieșire să meargă mai departe spre alt dispozitiv sau spre on-premises pentru control suplimentar. Necesită Management NIC în anumite scenarii.



Arhitectură de referință: Hub-and-Spoke

Figura 1. Exemplu de hub-and-spoke în care Azure Firewall devine punct central pentru fluxul de trafic și deciziile de securitate. Hub VNet conține AzureFirewallSubnet /26, Application Gateway, GatewaySubnet VPN/ER și Azure Firewall. Route tables / UDR cu regula `0.0.0.0/0 → Firewall` forțează tot traficul din spoke-uri prin hub. Spoke VNet conține App subnet și workload-uri AKS/VM/App.

Ce trebuie să știe un network engineer înainte de deployment

1

Subnet dedicat obligatoriu

Azure Firewall se deployează într-un subnet denumit exact `AzureFirewallSubnet`. Nu pune alte resurse în acest subnet.

2

Dimensionare minimă /26

AzureFirewallSubnet trebuie dimensionat la minimum **/26**. Serviciul are nevoie de spațiu pentru scalare și operațiuni interne. Nu micșora acest subnet.

3

Management Subnet opțional

`AzureFirewallManagementSubnet` este necesar pentru forced tunneling și anumite funcții de management. De asemenea minimum /26.

4

Planifică rutarea de la început

Definește clar ce subnets și ce spoke-uri vor trimite traficul prin firewall. Fără această claritate, regulile devin greu de întreținut.

5

Design DNS înainte de reguli FQDN

Custom DNS și DNS Proxy trebuie tratate explicit înainte de a scrie reguli bazate pe FQDN. Altfel, filtrarea va fi inconsistentă.

6

Definește inbound, outbound și east-west

Claritatea direcțiilor de trafic este esențială pentru un set de reguli curat și ușor de auditat.

LABORATOR ZERO-TO-HERO

Setul minim de resurse recomandat

Resurse de infrastructură

- **Resource Group:** rg-lab-firewall-001
- **Region:** West Europe sau regiunea aprobată de politica ta
- **VNet:** vnet-hub-lab-001
- **Address Space:** 10.20.0.0/16

Subnets și resurse Firewall

- **AzureFirewallSubnet:** 10.20.0.0/26
- **AzureFirewallManagementSubnet:** 10.20.0.64/26 (opțional, util pentru demo)
- **VM test subnet:** 10.20.1.0/24
- **Firewall Policy:** fwpol-lab-001
- **Firewall:** azfw-lab-001
- **VM de test:** Windows sau Linux

Un /16 pentru VNet îți oferă spațiu să adaugi ulterior spoke-uri, subnets pentru AKS, Application Gateway, Bastion sau alte workload-uri fără să refaci planul IP. Gândește creșterea de la început.

Deploy zero-to-hero în Azure Portal

Urmărim pașii în ordine logică: Resource Group → VNet și Subnets → Firewall Policy → Azure Firewall → DNS și Threat Intelligence → Route Table (UDR).

Pașii 1–3: Resource Group, VNet și Firewall Policy

1

8.1 Resource Group

Portal → Resource groups → Create. Introdu `rg-lab-firewall-001`, alege subscription-ul și region-ul. Review + create.

2

8.2 VNet și Subnets

Virtual networks → Create. Name = `vnet-hub-lab-001`, address space = `10.20.0.0/16`. Adaugă cele 3 subnets: AzureFirewallSubnet /26, AzureFirewallManagementSubnet /26 și snet-workload /24.

3

8.3 Firewall Policy

Firewall Policy → Create. Name = `fwpol-lab-001`. Alege SKU **Standard** pentru echilibrul corect între funcții și cost. Asociază policy cu aceeași regiune ca firewall-ul.

Pasul 4: Creează Azure Firewall

Setări de bază

Firewalls → Create. Name = `azfw-lab-001`. Region = aceeași cu VNet-ul. Virtual network = `vnet-hub-lab-001`.

Firewall Policy

Selectează `fwpol-lab-001`. Firewall Policy este modelul recomandat pentru management centralizat, reutilizare și guvernanță.

Firewall Management NIC

Enable dacă vrei demo de forced tunneling sau separare clară a traficului de management. Nu este obligatoriu în toate scenariile.

Public IP

Creează un Public IP nou pentru firewall. În multe scenarii ai nevoie de IP public pentru servicii inbound și management.

Pașii 5–6: DNS, Threat Intelligence și UDR

8.5 DNS și Threat Intelligence

În **Firewall Policy → DNS Settings** poți alege Azure DNS sau Custom DNS servers. Activează **DNS Proxy** dacă vrei filtrare robustă pe FQDN în network rules.

În **Threat Intelligence**, setează *Alert* sau *Alert and Deny* în funcție de maturitatea operațională. În laboratoare, începe cu *Alert* pentru a evita blocări neașteptate.

8.6 Route Table (UDR)

Route tables → Create. Name = `rt-workload-to-fw`. Adaugă rută `0.0.0.0/0` cu Next hop type = **Virtual appliance**. Introdu ca next hop **IP-ul privat al Azure Firewall**. Asociază route table la subnetul `snet-workload`.

De ce? Fără UDR, workload-urile ar ieși direct la internet prin ruta implicită Azure. UDR-ul forțează traficul prin Azure Firewall, unde îl poți inspecta, filtra și jurnaliza.

Ordinea de procesare a regulilor

Ordinea logică de evaluare: **DNAT → Network Rules → Application Rules**. Regula este *terminating*: la primul match, procesarea se oprește imediat.

> **Greșeală comună:** Inginerii creează o regulă broad de allow prea sus și apoi se întreabă de ce o regulă de deny mai specifică nu mai contează. Într-un firewall, ordinea și granularitatea sunt la fel de importante ca regula în sine.

Creează regulile de bază

9.1 Network Rule Collection (L3/L4)

Folosește pentru trafic bazat pe IP, port și protocol. Exemple tipice:

- Permite DNS din workload subnet către 168.63.129.16 sau DNS custom, UDP/TCP 53.
- Permite outbound HTTPS generic TCP 443 pentru update-uri, dacă strategia permite.
- Permite SSH sau RDP doar dintr-un subnet de management către subnets administrative.

9.2 Application Rule Collection (L7)

Folosește pentru control la nivel de FQDN și categorii web. Exemple tipice:

- Permite doar *.microsoft.com și *.windowsupdate.com pentru update-uri.
- Permite registry-uri și endpoint-uri necesare AKS sau containere.
- Blochează categorii web nepotrivite în medii enterprise.

9.3 DNAT Rule Collection

Publică un serviciu intern către exterior pe baza IP-ului și portului. Exemplu: mapare PublicIP:8443 → 10.20.1.4:443.

- Folosește DNAT doar când chiar ai nevoie de expunere inbound.
- Pentru web modern, App Gateway sau Front Door este deseori o alegere mai bună.
- Expunerea prin DNAT cere igienă excelentă de NSG, hardening și logging.

Prioritatea și ordinea regulilor

1 Deny implicit

Azure Firewall pornește cu **deny implicit**. Dacă nu permiți explicit, traficul este blocat. Aceasta este baza oricărei politici sănătoase.

2 Reguli terminating

La primul match, procesarea se oprește. Tipurile de reguli sunt evaluate în ordinea: **DNAT → Network → Application**.

3 Priorități numerice

În Firewall Policy, rule collection groups și rule collections au priorități numerice. **Numărul mai mic = prioritate mai mare.**

4 Politici ierarhice

Politica părinte are prioritate față de politica copil pentru colecțiile evaluate înaintea acestora. Util pentru guvernanță centralizată în organizații mari.

DNS, FQDN, Service Tags și IP Groups

DNS Proxy și Custom DNS

DNS Proxy este critic pentru filtrare FQDN în network rules. Fără el, rezoluția DNS poate fi inconsistentă și regulile FQDN nu funcționează corect.

Custom DNS trebuie ales dacă organizația folosește rezoluție internă sau split-horizon DNS. Gândește design-ul DNS înainte de a scrie orice regulă FQDN.

Service Tags și IP Groups

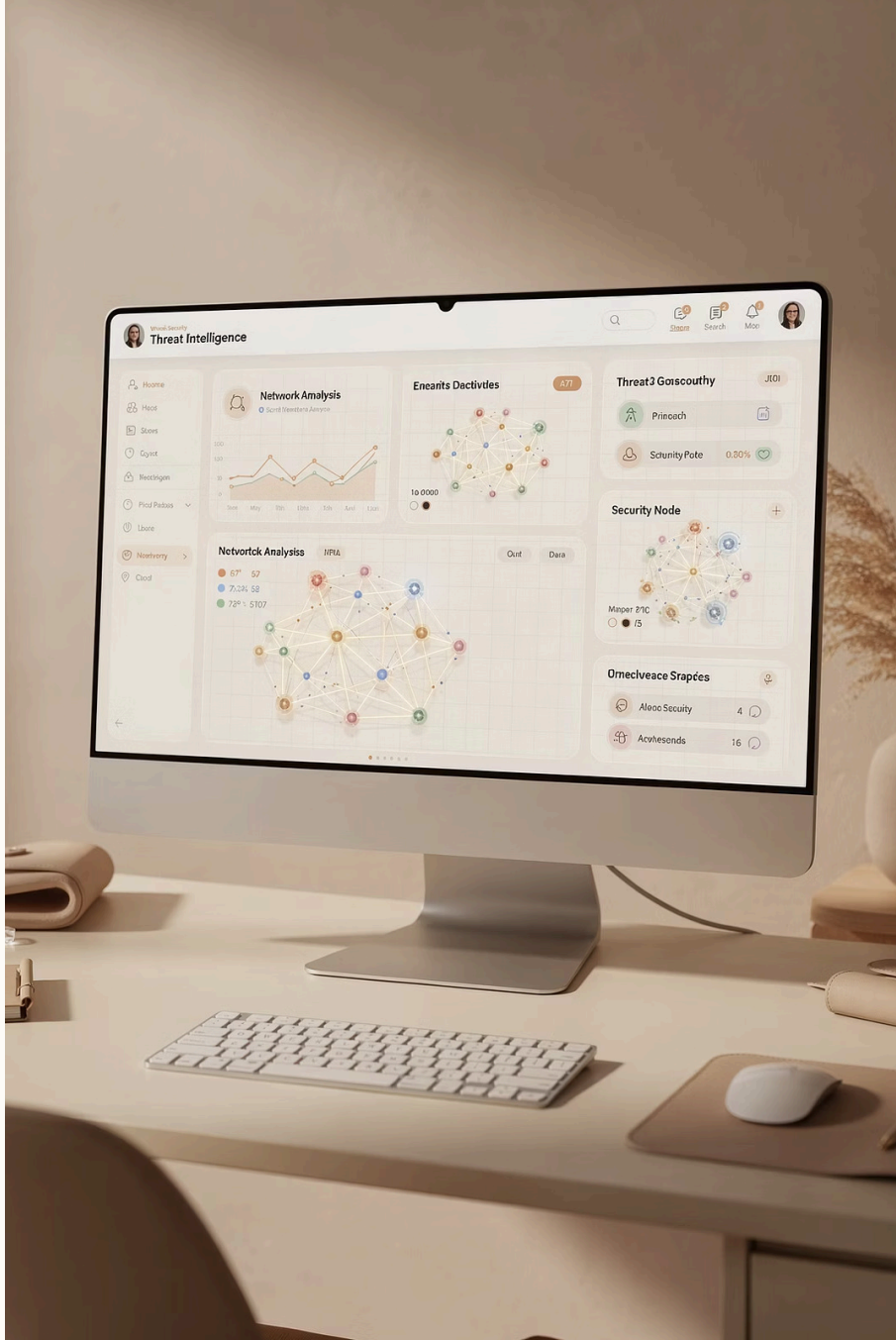
Service Tags simplifică regulile pentru servicii Azure și reduc numărul de IP-uri hardcodate. Exemple: `AzureMonitor`, `Storage`, `Sql`.

IP Groups simplifică managementul adreselor și fac regulile mai curate și reutilizabile. Grupezi surse interne o singură dată și le referențiezi în mai multe reguli.

> Pattern bun enterprise: IP Groups pentru surse interne + Application rules pentru destinații web + DNS Proxy pentru consistență.

Threat Intelligence, TLS Inspection și IDPS

Aici apare diferența mare dintre **Standard** și **Premium**. Aceste funcții sunt relevante pentru organizații cu cerințe de securitate avansate.



Funcții avansate de securitate (Premium)

Threat Intelligence Filtering

Compară traficul cu feed-ul Microsoft de IP-uri și domenii cunoscute malițioase. Disponibil în Standard și Premium. Poate funcționa în modul *Alert* sau *Alert and Deny*.

TLS Inspection (Premium)

Permite decriptarea controlată a traficului TLS pentru inspecție mai profundă. Necesită certificate gestionate corect și o politică clară de privacy și compliance.

IDPS — Intrusion Detection and Prevention (Premium)

Inspectează fluxuri pentru semnături și comportamente suspecte. Poate funcționa în *Alert* sau *Alert and Deny*. Oferă vizibilitate profundă asupra amenințărilor active.

Real life: Într-o organizație mare, Standard poate fi suficient pentru filtrare de bază și control egress. Premium apare în discuție când ai de apărat date sensibile, segmentare strictă sau când vrei vizibilitate mai profundă asupra traficului criptat.

Monitorizare, Metrici și Logging

Un firewall fără observabilitate este doar pe jumătate operat. Pentru operare sănătoasă ai nevoie de diagnostic settings, metrici, logs și alerte configurate din ziua zero.

Cum configurezi observabilitatea

Log Analytics Workspace

Trimite jurnalele în Log Analytics Workspace pentru interogări avansate cu KQL. Activează Diagnostic Settings pe firewall și policy.

Metrici cheie

Urmărește: **Throughput**, **Data processed**, **Rule hit count** și **Latency**. Acestea îți spun dacă firewall-ul funcționează sănătos.

Alerte operaționale

Construiește alerte pentru ThreatIntel, firewall health, deployment failures și anomalii de trafic. Integrează cu Azure Monitor Alerts.

Corelarea jurnalelor

Corelează jurnalele firewall cu NSG flow logs, VM logs, Application Gateway logs și activitate de schimbare pentru context complet.

Întrebări utile în operare zilnică

→ Surge de trafic neobișnuit?

Există surge de trafic neobișnuit într-un anumit subnet? Verifică metrici de throughput și corelează cu schimbările recente de configurație sau de workload.

→ Throughput crescut brusc?

A crescut brusc throughput-ul după o schimbare de rută sau după deschiderea unui nou serviciu? Poate indica o rută greșită sau un serviciu neașteptat expus.

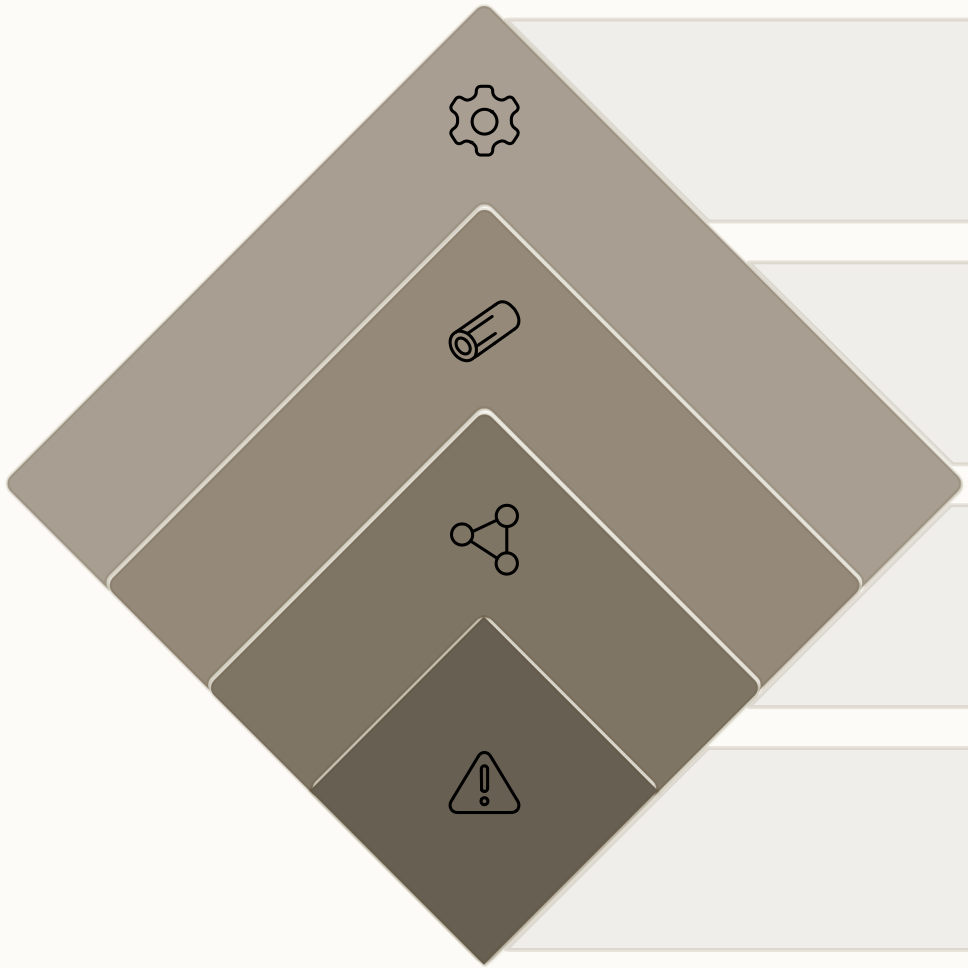
→ Reguli cu hit count zero?

Ce reguli au hit count zero și pot fi optimizate sau eliminate? Un firewall matur este și un firewall curat — regulile neutilizate adaugă complexitate fără valoare.

→ Latență anormală?

Există latență anormală sau blocaje locale care afectează un serviciu critic? Verifică dacă există asimetrie de rutare sau reguli care procesează volume mari.

Flux operațional: exemplu practic



Analiză Configurații

Revizuiește RuleCollectionGroups și Route Tables

Inspectare Loguri

Caută deny pe FQDN, IP sau port

Verificare Conectivitate

Outbound 443 și DNS rezolvă corect

Raportare Probleme

Utilizatorii semnalează update-uri eșuate

Acesta este un exemplu tipic de flux operațional. Urmând acești pași în ordine, poți identifica rapid cauza majorității problemelor de conectivitate raportate de utilizatori.

Cum se combină Azure Firewall cu alte servicii

Azure Firewall + NSG

Combinația normală și recomandată. Firewall-ul oferă control central și inspecție L7; NSG oferă micro-segmentare locală la nivel de NIC și subnet. Se completează, nu se exclud.

Azure Firewall + Application Gateway

Foarte des întâlnit pentru aplicații web. App Gateway se ocupă de web și WAF; Azure Firewall de control central, trafic non-web și egress. Fiecare la stratul lui.

Azure Firewall + Load Balancer

Load Balancer distribuie traficul L4 eficient; firewall-ul îl inspectează și îl jurnalizează. Combinație utilă pentru servicii interne cu volum mare.

Azure Firewall + VPN/ExpressRoute Gateway

Design-ul clasic pentru hub-and-spoke și conectivitate hibridă. Gateway-ul aduce traficul on-prem în hub; firewall-ul îl inspectează înainte de a-l trimite spre spoke-uri.

Nu încerca să convertești aceste servicii într-un singur produs. Fiecare are rolul lui. Designul matur le combină după stratul de rețea și după responsabilitate.

Troubleshooting: cele mai frecvente probleme

Simptom	Cauza probabilă	Ce verifici
Traficul outbound ocolește firewall-ul	UDR lipsă sau neasociat la subnet	Route table pe subnet, next hop IP firewall, effective routes
DNS nu merge din workload	DNS proxy / custom DNS greșit sau blocat	Setările DNS din policy și regulile UDP/TCP 53
Aplicația publică nu răspunde	DNAT sau NSG sau routing greșit	NAT rules, public IP, rule hit counts, NSG, backend reachability
Asymmetry / trafic instabil	Route return path greșite, mai ales în hub-and-spoke	UDR pe subnetul aplicației și traseul de întoarcere
FQDN rule nu funcționează	DNS Proxy dezactivat sau rezoluție inconsistentă	DNS settings, logs, cache și tipul corect de regulă

Bune practici de inginerie

Un deployment sănătos de Azure Firewall nu înseamnă doar că funcționează — înseamnă că este ușor de operat, de auditat și de extins în timp.

16 bune practici esențiale

1 Deploy prin Firewall Policy

Folosește Firewall Policy în locul regulilor clasice atunci când consistența și guvernanța sunt importante. Policy permite reutilizare și management centralizat.

2 Deny by default, documentează fiecare allow

Pornește cu deny implicit și adaugă reguli de allow explicit, documentate. Fiecare regulă trebuie să aibă un motiv business clar.

3 IP Groups și Application Rules

Folosește IP Groups pentru surse și Application rules pentru destinații web. Fac regulile mai curate, mai reutilizabile și mai ușor de auditat.

4 Evită DNAT când există alternative

Nu publica servicii prin DNAT dacă există alternative mai potrivite, de exemplu App Gateway sau Private Access patterns.

Observabilitate din ziua zero

Planifică metrici, logs, alerte și workbook-uri înainte de prima regulă. Un firewall fără observabilitate este pe jumătate operat.

DNS coerent și testare incrementală

Păstrează DNS-ul coerent între firewall, workload-uri și automatizări. Testează schimbările de rutare incremental, cu plan de rollback. Revizuiește periodic regulile — un firewall matur este și un firewall curat.

Studiu de caz real

Contextul

O companie cu aplicații interne și ieșire controlată la internet are mai multe spoke-uri și workload-uri sensibile. Nevoia: control centralizat al tuturor ieșirilor, protecție web și conectivitate hibridă.

Soluția aleasă

Hub-and-spoke cu Azure Firewall Standard, route tables și Application Gateway pentru web devine modelul natural.

Deciziile cheie de implementare

Control total al ieșirilor

Se impune controlul tuturor ieșirilor prin firewall. UDR pe toate spoke-urile cu next hop = Azure Firewall.

Application Rules pentru update-uri

Se folosesc Application rules pentru update-uri și endpoint-uri aprobate. Lista albă explicită, nu allow-all.

DNAT minim

Se păstrează DNAT minim și doar pentru servicii absolut necesare. Restul traficului inbound merge prin App Gateway.

Integrare cu Azure Monitor

Firewall-ul este integrat cu Azure Monitor și cu alertele operaționale din prima zi de producție.

Checklist final — ce trebuie să știi

1

Problema rezolvată

Știi ce problemă rezolvă Azure Firewall și de ce nu înlocuiește NSG, Load Balancer și App Gateway.

2

Design VNet și Route Tables

Poți proiecta un VNet, subnets și route tables pentru un deployment sănătos, inclusiv AzureFirewallSubnet /26.

3

Alegerea SKU-ului

Știi când alegi Basic, Standard sau Premium în funcție de cerințele de throughput, funcții și cost.

4

Deploy din Azure Portal

Știi să deployezi firewall-ul din Azure Portal și să îl legi de o Firewall Policy cu toți pașii din laborator.

5

Configurarea regulilor

Știi să configurezi network, application și DNAT rules, inclusiv ordinea de procesare și prioritatea.

6

Observabilitate și Troubleshooting

Știi să activezi și să interpretezi logs, metrici și alerte. Știi să citești simptomele clasice de rutare, DNS și procesare a regulilor.

Referințe oficiale Microsoft recomandate

Deploy și configurare

Deploy and configure Azure Firewall using the Azure portal Deploy and configure Azure Firewall and policy using the Azure portal

Alegerea SKU-ului și FAQ

Choose the right Azure Firewall SKU to meet your needs Azure Firewall FAQ Azure Firewall Management NIC

Reguli și FQDN

Azure Firewall rule processing logic Azure Firewall FQDN filtering in network rules

Monitorizare și arhitectură

Monitor Azure Firewall Architecture Best Practices for Azure Firewall Azure Firewall and Application Gateway for Virtual Networks

Toate documentele sunt disponibile pe **learn.microsoft.com**. Recomandăm parcurgerea lor în ordinea de mai sus, în paralel cu laboratorul practic.

Mulțumim pentru participare!

Ai parcurs ghidul complet zero-to-hero pentru Azure Firewall — de la concepte fundamentale, prin deploy practic în Azure Portal, până la operare, troubleshooting și bune practici de inginerie.

Pasul următor

Parcurge laboratorul practic în Azure Portal folosind resursele din secțiunea 7 și deployează primul tău Azure Firewall.

Întrebări?

Folosește secțiunea de Q&A sau referințele oficiale Microsoft pentru aprofundare. Comunitatea Azure este activă și bine documentată.

VERSIUNE 2026

CONSTRUIT PENTRU PREDARE PRACTICĂ ÎN AZURE PORTAL