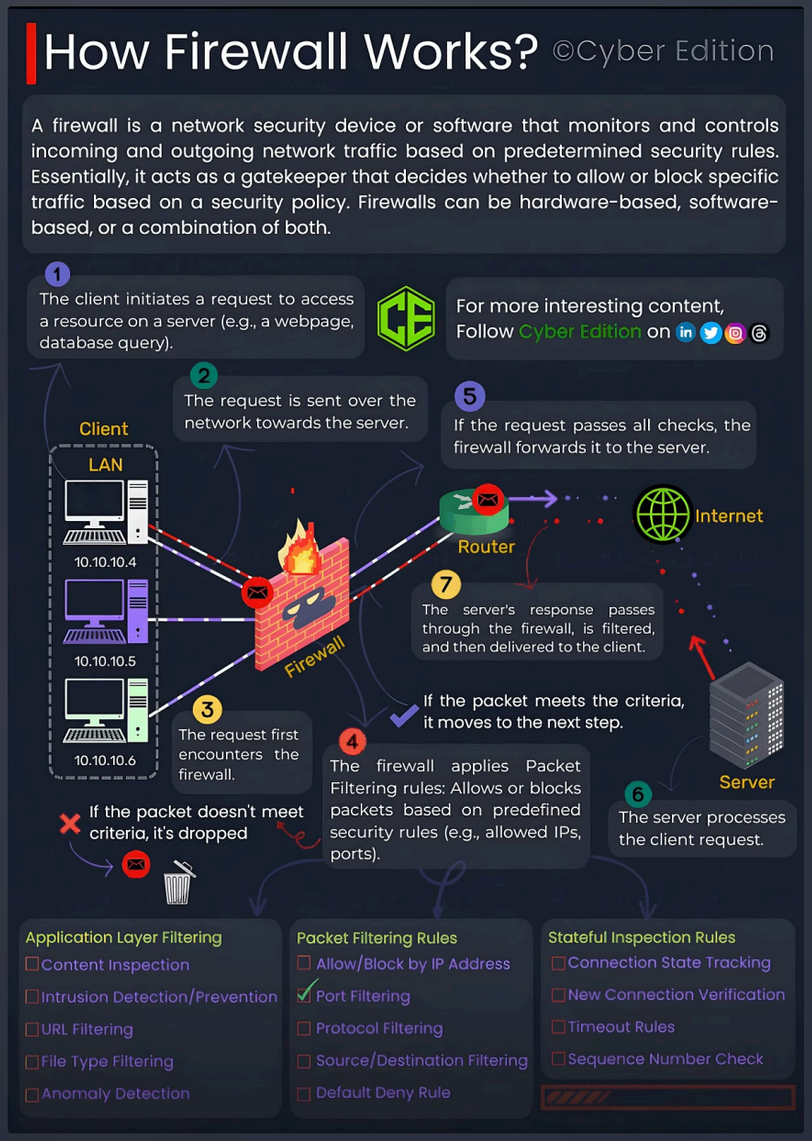


Ako funguje firewall

Komplexný sprievodca sieťovou bezpečnosťou pre IT administrátorov a študentov. Od základných princípov až po pokročilé techniky filtrovania, segmentáciu siete a prácu s Windows Serverom.

KYBERNETICKÁ BEZPEČNOSŤ | IT ADMINISTRÁCIA | SIEŤOVÉ TECHNOLÓGIE

Obsah prezentácie

Čo sa naučíme

01

Základy firewallu

Čo je firewall, typy firewallov, základná myšlienka a kľúčové pojmy ako klient, server, LAN, router a paket.

02

Filtrovacie techniky

Packet filtering, filtrovanie podľa IP adresy, portu, protokolu a princíp Default Deny Rule.

03

Pokročilé funkcie

Stateful inspection, application layer filtering, IDS/IPS, URL filtering a detekcia anomálií.

04

Prax a troubleshooting

Firemné scenáre, Windows Server, Active Directory, firewall logy, SIEM a riešenie bežných problémov.

Čo je firewall?

Firewall je bezpečnostné zariadenie alebo softvér, ktorý sleduje a riadi sieťovú komunikáciu medzi počítačom, lokálnou sieťou a vonkajším svetom — napríklad internetom. Jednoducho povedané: firewall je **bezpečnostná brána** medzi tvojím počítačom a internetom.

Povolí

Komunikácia spĺňa bezpečnostné pravidlá a môže pokračovať ďalej.

Zablokuje

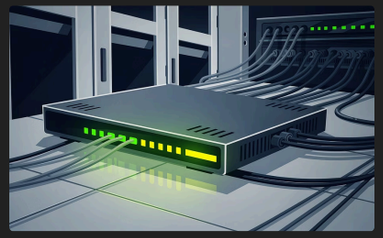
Komunikácia nie je povolená a firewall ju odmietne alebo zahodí.

Prepustí po kontrole

Pokročilý firewall obsah preskúma a až potom rozhodne o ďalšom postupe.

Typy firewallov

Firewally existujú v rôznych formách — od fyzických zariadení až po softvérové riešenia. Každý typ má svoje výhody a typické použitie.



Hardvérový firewall

Samostatné fyzické zariadenie, ktoré je často súčasťou routera alebo podnikovej bezpečnostnej brány. Používa sa najmä vo firmách a dátových centrách.

Softvérový firewall

Program bežiaci v počítači alebo serveri. Príkladom je **Windows Defender Firewall**. Vhodný pre jednotlivých používateľov aj servery.

Kombinovaný firewall

Spojenie hardvérového aj softvérového riešenia. Poskytuje najvyššiu úroveň ochrany a používa sa v kritických podnikových prostrediach.

Dôležité pojmy

Predtým ako pochopíme fungovanie firewallu, je potrebné poznať základné sieťové pojmy, ktoré sa objavujú v každom scenári komunikácie.

Client (Klient)

Zariadenie, ktoré žiada o prístup k nejakej službe alebo serveru. Napríklad počítač, notebook alebo mobil. V LAN môžu mať klienti IP adresy ako 10.10.10.4, 10.10.10.5 alebo 10.10.10.6.

Router

Zariadenie, ktoré smeruje komunikáciu medzi rôznymi sieťami — napríklad medzi domácou LAN a internetom. Router rieši **smerovanie**, firewall rieši **bezpečnosť**. V praxi router často obsahuje aj firewallové funkcie.

Server

Počítač alebo systém, ktorý poskytuje službu klientovi — webový server, databázový server, e-mailový alebo aplikačný server. Keď otvoríš webovú stránku, tvoj počítač je klient a stránka beží na serveri.

Paket (Packet)

Malý kus dát posielaný cez sieť. Dáta sa rozdelia na pakety, každý obsahuje zdrojovú a cieľovú IP adresu, zdrojový a cieľový port, protokol a časť prenášaných dát.

Lokálna sieť – LAN

Čo je LAN?

LAN znamená **Local Area Network** — lokálna sieť v rámci jednej domácnosti, školy, úradu alebo firmy.

Príklady zariadení v LAN:

- Počítače v kancelárii alebo škole
- Servery v serverovej miestnosti
- Tlačiarne a interné zariadenia
- Sieťové ukladacie zariadenia (NAS)

Typické IP rozsahy v LAN

Rozsah	Použitie
10.0.0.0/8	Veľké firemné siete
172.16.0.0/12	Stredné podnikové siete
192.168.0.0/16	Domácnosti a malé firmy

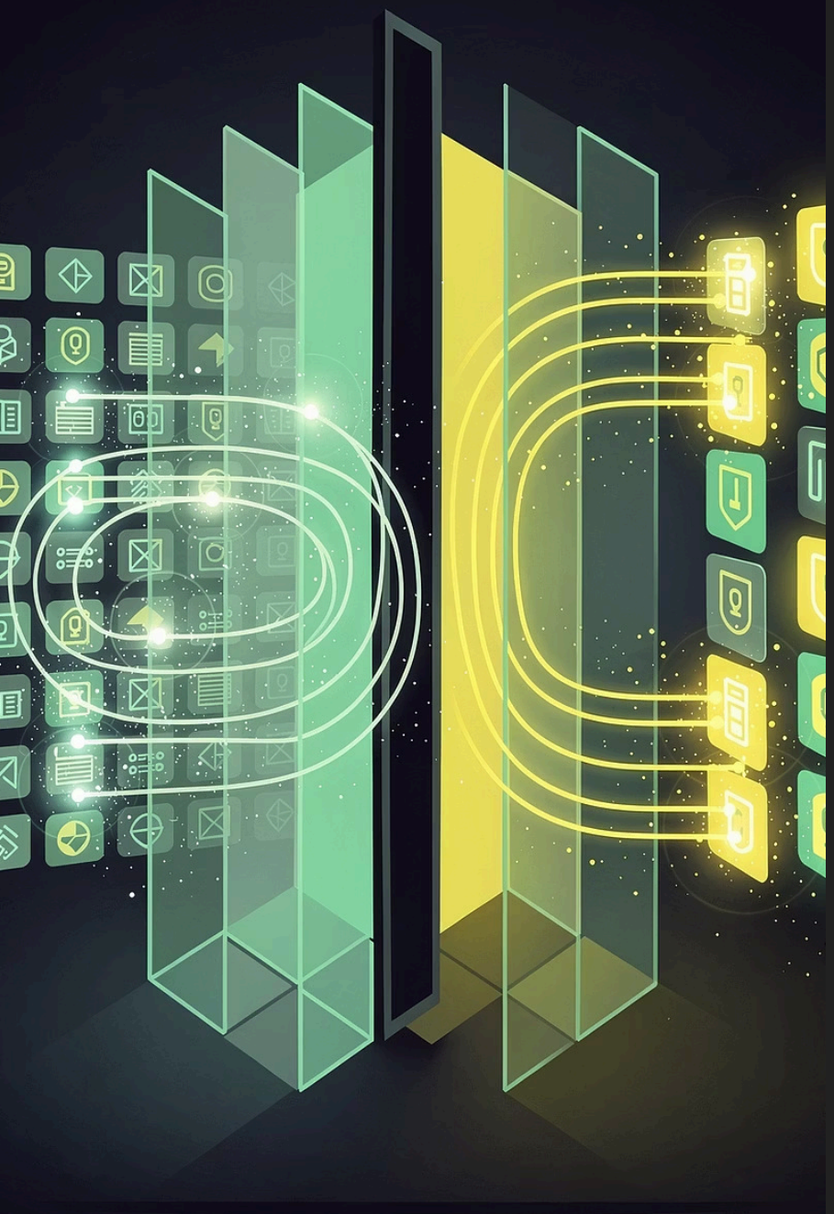
Firewall stojí na rozhraní medzi LAN a vonkajšou sieťou (internetom) a kontroluje všetku prechádzajúcu komunikáciu.

Komunikácia cez firewall – krok za krokom

Nasledujúci diagram znázorňuje základný proces komunikácie medzi klientom a serverom cez firewall v siedmich krokoch.

Klient štartuje | Požiadavka v LAN | Dotyk s firewallom | Firewall pravidlá | Paket pokračuje

Každý paket prechádza firewallovými pravidlami **obojsmerne** — tak požiadavka od klienta, ako aj odpoveď servera musia spĺňať bezpečnostné kritériá. Ak paket nespĺňa pravidlá, firewall ho zahodí alebo zablokuje.



Packet Filtering – základná technika

Packet filtering je základná technika firewallu. Firewall kontroluje jednotlivé pakety podľa jednoduchých, vopred definovaných pravidiel. Je to prvá línia obrany v každej sieti.

Čo firewall kontroluje

- IP adresu odosielateľa (source IP)
- IP adresu príjemcu (destination IP)
- Port — zdrojový aj cieľový
- Protokol — TCP, UDP, ICMP
- Smer komunikácie — inbound / outbound

Príklad pravidiel

- Povoliť TCP port 443 → HTTPS komunikácia
- Blokovať TCP port 23 → zakázaný Telnet
- Povoliť len IP 10.10.10.5 → konkrétny počítač
- Blokovať všetko ostatné → Default Deny

Najčastejšie kontrolované porty

Porty sú číselné identifikátory sieťových služieb. Firewall ich používa na rozhodovanie, ktorá komunikácia je povolená a ktorá nie. Toto sú porty, ktoré musí poznať každý IT administrátor.

Port	Služba	Význam	Odporúčanie
80	HTTP	Nešifrovaný web	Obmedziť, preferovať 443
443	HTTPS	Šifrovaný web	Povoliť
22	SSH	Vzdialená správa Linux	Len z internej siete
3389	RDP	Vzdialená plocha Windows	Nikdy z internetu!
25	SMTP	Odosielanie e-mailov	Len pre mail servery
53	DNS	Preklad domén na IP	Povoliť TCP/UDP
445	SMB	Windows zdieľanie súborov	Len v LAN, blokovať z internetu
1433	MS SQL	Microsoft SQL Server	Len z app servera
3306	MySQL	MySQL databáza	Len z app servera

Filtrovanie podľa IP, portu a protokolu

Filtrovanie podľa IP

Firewall môže rozhodovať podľa IP adresy — povolí alebo zablokuje konkrétne zariadenie.

Allow: 10.10.10.5 → server

Block: 10.10.10.100 → server

Užitočné vo firmách, kde len niektoré zariadenia majú prístup k citlivým systémom.

Filtrovanie podľa portu

Firewall povoľuje alebo blokuje komunikáciu podľa čísla portu. Veľa útokov sa zameriava práve na otvorené porty.

Allow TCP 443 (HTTPS)

Block TCP 23 (Telnet)

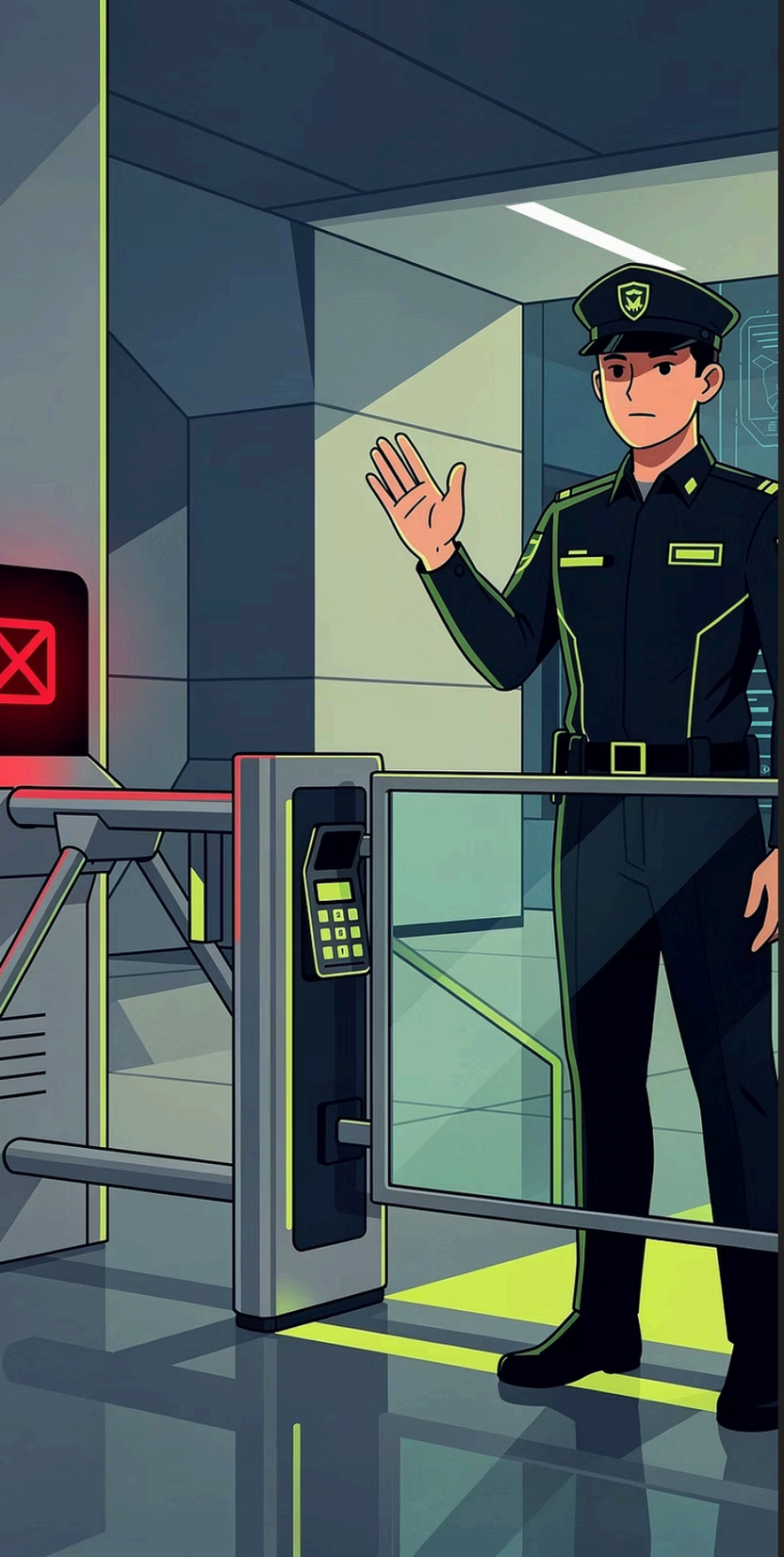
Block TCP 3389 from Internet

Filtrovanie podľa protokolu

Firewall môže filtrovať aj podľa sieťového protokolu.

Protokol	Použitie
TCP	Web, e-mail, DB
UDP	DNS, VoIP, streaming
ICMP	Ping, diagnostika

Block ICMP from Internet — zabraňuje sieťovej diagnostike zvonka.



Default Deny Rule

> Čo nie je výslovne povolené, je zakázané.

Toto je jeden z najdôležitejších bezpečnostných princípov. Default Deny Rule znamená, že firewall blokuje **všetku komunikáciu**, ktorá nie je explicitne uvedená v povolených pravidlách. Je to oveľa bezpečnejší prístup ako opačný model, kde je všetko povolené a blokujú sa len známe hrozby.

✅ Allow HTTPS

Povoliť TCP 443 pre šifrovaný web

✅ Allow DNS

Povoliť UDP/TCP 53 pre preklad domén

🚫 Block all other traffic

Všetka ostatná komunikácia je automaticky zakázaná

Stateful Inspection

Stateful inspection je pokročilejší spôsob, akým firewall kontroluje komunikáciu. Na rozdiel od jednoduchého packet filteringu si firewall **pamätá stav spojenia** — nekontroluje iba jednotlivý paket izolovane, ale pozerá sa aj na to, či paket patrí k existujúcej relácii.

Stavy spojenia (Connection States)

Stav	Význam
New	Nové, doteraz neznáme spojenie
Established	Už existujúce, povolené spojenie
Related	Súvisiace spojenie (napr. FTP dáta)
Invalid	Neplatné alebo podozrivé spojenie

Firewall tiež používa **Timeout Rules** — ak spojenie dlho nič nerobí, automaticky ho ukončí, čo šetrí zdroje a znižuje bezpečnostné riziká.

Príklad stateful inspection

1. Klient otvorí webovú stránku
2. Firewall dovolí odchádzajúcu HTTPS požiadavku
3. Server odpovie
4. Firewall vie, že odpoveď patrí k požiadavke
5. Odpoveď pustí späť ku klientovi

Náhodná komunikácia z internetu bez predchádzajúcej požiadavky je **automaticky zablokovaná**.

Application Layer Filtering

Application layer filtering je pokročilejšia kontrola komunikácie. Firewall sa nepozerá iba na IP adresy a porty, ale snaží sa pochopiť **obsah a typ aplikácie**. Ide o funkciu Next-Generation Firewallov (NGFW).

Content Inspection

Kontrola obsahu komunikácie — škodlivý kód, nebezpečné súbory, zakázané vzory, únik citlivých dát.

IDS / IPS

IDS deteguje útok a upozorní správcu. IPS útok nielen deteguje, ale ho aj **automaticky zablokuje**.

URL Filtering

Blokovanie webových stránok podľa adresy alebo kategórie — phishing, malware, hazard, sociálne siete.

File Type Filtering

Blokovanie nebezpečných typov súborov — .exe, .bat, .ps1, .zip, .rar — znižuje riziko ransomvéru.

Anomaly Detection

Hľadanie neobvyklého správania — tisíce požiadaviek za sekundu, pripojenie z neobvyklej krajiny, komunikácia s podozrivou IP adresou.

Inbound vs. Outbound komunikácia

⬇️ Inbound Traffic

Komunikácia smerom **dovnútra siete**. Napríklad: niekto z internetu sa chce pripojiť na firemný server.

Táto komunikácia je **rizikovejšia**, pretože prichádza zvonka. Firewally typicky venujú inbound pravidlám najväčšiu pozornosť.

- Blokovať RDP z internetu
- Blokovať SMB z internetu
- Povoliť len HTTPS na webový server

⬆️ Outbound Traffic

Komunikácia smerom **von zo siete**. Napríklad: zamestnanec otvorí webovú stránku.

Mnoho ľudí si myslí, že outbound komunikácia je automaticky bezpečná. **Nie je to pravda.** Infikovaný počítač sa môže pokúšať komunikovať s útočníkom cez internet.

- Sledovať neobvyklú odchádzajúcu komunikáciu
- Blokovať prístup na škodlivé domény
- Obmedziť nepovolené protokoly

Firewall v praxi – firemné prostredie

Predstav si firmu so zamestnanci, servermi, databázou a prístupom na internet. Firewall môže byť nastavený nasledovne:

Pravidlo	Akcia	Dôvod
Zamestnanci → Internet TCP 443	✅ Povoliť	Šifrovaný web
Zamestnanci → DNS UDP/TCP 53	✅ Povoliť	Preklad domén
TCP 23 (Telnet)	🚫 Blokovať	Nezabezpečený protokol
RDP z internetu	🚫 Blokovať	Vysoké riziko útoku
Databáza ← App Server	✅ Len konkrétna IP	Segmentácia prístupu
Internet → LAN	🚫 Blokovať	Ochrana internej siete
Všetko ostatné	🚫 Default Deny	Bezpečnostný princíp

ⓘ V praxi sa odporúča každé pravidlo zdokumentovať — uviesť dôvod, dátum vytvorenia a zodpovednú osobu.

Firewall a Windows Server

Pre IT prax je kľúčové rozumieť firewallu aj v prostredí Windows Server. **Windows Defender Firewall with Advanced Security** umožňuje nastavovanie podrobných inbound a outbound pravidiel.

Profily Windows Firewallu

Profil	Použitie
Domain	Počítač je členom domény
Private	Dôveryhodná súkromná sieť
Public	Verejná / nedôveryhodná sieť

Vo firme sa najčastejšie používa **Domain profile**.

Príklad: povolenie RDP len z internej siete

```
Allow TCP 3389 from 10.10.10.0/24
Block TCP 3389 from Internet
```

Toto znamená: správca vo firme sa môže pripojiť na server cez RDP, útočník z internetu nie. Ide o typický príklad **source/destination filtering**.

Povolenia firewallu zahŕňajú:

- Inbound a outbound rules
- Connection security rules
- Pravidlá podľa portov a aplikácií

Firewall a Active Directory

V prostredí Active Directory je správne nastavenie firewallu kriticky dôležité. Ak firewall zablokuje nesprávny port, môžu nastať vážne problémy s prihlasovaním, Group Policy alebo replikáciou.

Porty vyžadované doménovým radičom

Služba	Port
DNS	53 TCP/UDP
Kerberos	88 TCP/UDP
LDAP	389 TCP/UDP
LDAPS	636 TCP
SMB	445 TCP
Global Catalog	3268 TCP
RPC Endpoint Mapper	135 TCP
NTP	123 UDP

Dôsledky zlého nastavenia

Prihlásenie do domény

Počítač sa neprihlási do domény, ak je blokovaný Kerberos (88) alebo LDAP (389).

Group Policy

GPO sa neaplikujú bez funkčného SMB (445) a LDAP (389).

Replikácia

Replikácia medzi radičmi zlyhá bez RPC (135) a SMB (445).

Troubleshooting – riešenie problémov s firewallom

Keď niečo v sieti nefunguje, firewall je jedna z prvých vecí, ktoré treba skontrolovať. Nasleduje praktický postup riešenia scenára: *"Neviem sa pripojiť na internú webovú aplikáciu."*

1

Overiť IP adresu

`ipconfig` — zistiť IP klienta

2

Overiť dostupnosť

`ping webserver01` — test ICMP

3

Overiť port

`Test-NetConnection webserver01 -Port 443`

4

Skontrolovať pravidlá

`Get-NetFirewallRule` — zobraziť pravidlá

5

Skontrolovať logy

Event Viewer → Windows Defender Firewall logs

6

Opraviť pravidlo

`New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow`

Firewall logy a SIEM

Na čo slúžia firewall logy?

Firewall zaznamenáva udalosti do logov — čo bolo povolené, čo zablokované, odkiaľ komunikácia prišla, na aký port smerovala a kedy sa udalosť stala.

Logy sú vo firemnej praxi kľúčové pre:

- Bezpečnostný audit a compliance
- Vyšetrovanie bezpečnostných incidentov
- Detekciu opakovaných pokusov o útok
- Integráciu so SIEM systémami

Čo je SIEM?

SIEM (Security Information and Event Management) zbiera logy z firewallov, serverov, klientov a cloudových služieb a hľadá podozrivé vzory.

Populárne SIEM nástroje:

- Microsoft Sentinel
- Splunk
- QRadar (IBM)
- Elastic Security
- Wazuh (open-source)

> ⚠ Príklad: Jedna IP adresa sa pokúsi počas 5 minút pripojiť na 500 rôznych portov → možný port scan → SIEM upozorní správcu.

Segmentácia siete a Zero Trust

Segmentácia siete

Firewall môže deliť sieť na izolované časti, čím znižuje riziko šírenia útoku.

Segment	Prístup
Guest Wi-Fi	Len internet, nie LAN
Admin sieť	Prístup na servery
Užívatelia	Bez prístupu na DB
App Server	Prístup na DB povolený
IoT zariadenia	Izolovaná sieť

Zero Trust princíp

> Nikomu automaticky never. Vždy overuj.

Moderný bezpečnostný princíp Zero Trust predpokladá, že žiadna komunikácia — ani interná — nie je automaticky dôveryhodná.

Vždy overuj identitu

Minimálne oprávnenia

Nepretržitá kontrola

Najčastejšie chyby pri konfigurácii firewallu

Chyba	Riziko
Povolené všetko (allow all)	Sieť je príliš otvorená — žiadna ochrana
RDP otvorené do internetu	Vysoké riziko brute-force a ransomvér útokov
Chýba Default Deny pravidlo	Nepovolená komunikácia môže prejsť
Nepoužívajú sa logy	Správca nevie, čo sa v sieti deje
Príliš staré neaktualizované pravidlá	Bezpečnostné diery zostávajú nezaplátané
Pravidlá bez popisu a dokumentácie	Ťažká správa a audit
Rovnaké pravidlá pre všetkých	Slabá segmentácia, šírenie útokov
Žiadna kontrola outbound traffic	Malware môže voľne komunikovať s útočníkom

Dobré bezpečnostné zásady

Dodržiavanie týchto zásad výrazne zvyšuje bezpečnosť každej siete — bez ohľadu na jej veľkosť.

→ Princíp Least Privilege

Povoľuj len to, čo je skutočne potrebné. Každý prístup navyše je potenciálne riziko.

→ Default Deny + dokumentácia pravidiel

Blokuj všetko, čo nie je výslovne povolené. Každé pravidlo musí mať popis, dôvod a dátum.

→ Pravidelný audit a kontrola logov

Staré pravidlá môžu obsahovať bezpečnostné diery. Logy odhalia pokusy o útok skôr, ako spôsobia škodu.

→ Segmentácia siete a VPN pre správu

Nepovoľuj RDP, SMB a databázové porty priamo z internetu. Administráciu vykonávaj cez VPN.

→ Testovanie po každej zmene

Každá zmena pravidiel môže neúmyselne narušiť funkčnosť alebo bezpečnosť. Vždy otestuj výsledok.

Praktická úloha: Firewall pre školskú sieť

Navrhni firewall pravidlá pre školskú sieť so žiackymi počítačmi, učiteľskými počítačmi, serverom, hosťovským Wi-Fi a prístupom na internet.

#	Pravidlo	Protokol / Port	Akcia
1	Žiaci → Internet	TCP 443	✅ Allow
2	Žiaci → DNS	UDP/TCP 53	✅ Allow
3	Učitelia → Súborový server	TCP 445	✅ Allow
4	Admini → Servery (RDP)	TCP 3389	✅ Allow (len interná sieť)
5	Hosťovská Wi-Fi → Interná LAN	Všetky	🚫 Block
6	Hosťovská Wi-Fi → Internet	TCP 443	✅ Allow
7	Internet → LAN (RDP)	TCP 3389	🚫 Block
8	App Server → Databázový server	TCP 1433	✅ Allow
9	Všetko ostatné	—	🚫 Default Deny

Prirovnanie: Firewall ako vrátnik

Firewall si môžeš predstaviť ako vrátnika v budove. Klient je človek, ktorý chce niekam ísť. Server je miestnosť, do ktorej sa chce dostať. Firewall je vrátnik, ktorý každého skontroluje.

Kto si?

Aká je tvoja IP adresa? Si v zozname povolených zariadení?

Kam ideš?

Aká je cieľová IP adresa a port? Je tento cieľ povolený?

Máš povolenie?

Existuje pravidlo, ktoré ti dovoľuje prejsť? Ak nie, si zastavený.

Patrí odpoveď k požiadavke?

Stateful inspection — vrátnik si pamätá, kto bol vpustený, a overí, či odpoveď zodpovedá požiadavke.

Mini test — otestuj svoje vedomosti

1

Otázka 1

Firewall je: **B — Bezpečnostný systém na kontrolu sieťovej komunikácie**

2

Otázka 2

Port 443 sa najčastejšie používa pre: **A — HTTPS (šifrovaný web)**

3

Otázka 3

Default Deny znamená: **B — Všetko je zakázané, ak to nie je výslovne povolené**

4

Otázka 4

Stateful inspection znamená, že firewall: **B — Pamätá si stav spojenia**

5

Otázka 5

RDP používa port: **C — 3389**

Zhrnutie – čo sme sa naučili

Firewall je základný a nenahraditeľný prvok kybernetickej bezpečnosti každej siete. Tu je rýchle zhrnutie kľúčových poznatkov.

🔍 Kontroluje komunikáciu

Povolí alebo blokuje pakety podľa pravidiel — IP adresy, porty, protokoly, smer.

🧠 Pamätá si stav

Stateful inspection sleduje existujúce spojenia a blokuje náhodné komunikácie zvonka.

🔎 Kontroluje obsah

Next-gen firewally vykonávajú URL filtering, content inspection, IDS/IPS a detekciu anomálií.

🏢 Je súčasťou ekosystému

Spolupracuje so SIEM, VPN, Active Directory, segmentáciou siete a Zero Trust princípmi.

> Firewall nerozhoduje podľa pocitu, ale podľa pravidiel: kto komunikuje, kam komunikuje, cez aký port, akým protokolom a či je táto komunikácia povolená.