Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

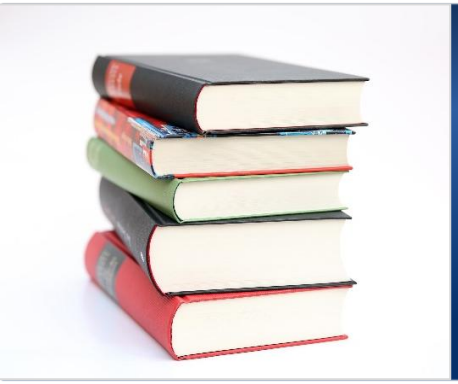
Sieťové topológie, bezpečnostné zariadenia a služby

Sieťová bezpečnostná architektúra
Kurz: Špecialista kybernetickej bezpečnosti

prof. Ing. Pavel Segeč, PhD.

KC KYB UNIZA, https://kc.uniza.sk

pavel.segec@fri.uniza.sk



Obsah

- Blok 1: Úvod a základné pojmy
- Blok 2: Plánovanie, metodiky a rámce
- Blok 3: Princípy návrhu
- Blok 4: Bezpečnostné opatrenia

- Literatúra
  - Cisco Netacad Security Essentials
  - Cisco Netacad Network Security
  - Cisco Netacad CCNA/CCNP
  - Fortinet NS4
  - CCNP Security CORE 701
  - CISP

Blok 1 - Úvod a základné pojmy

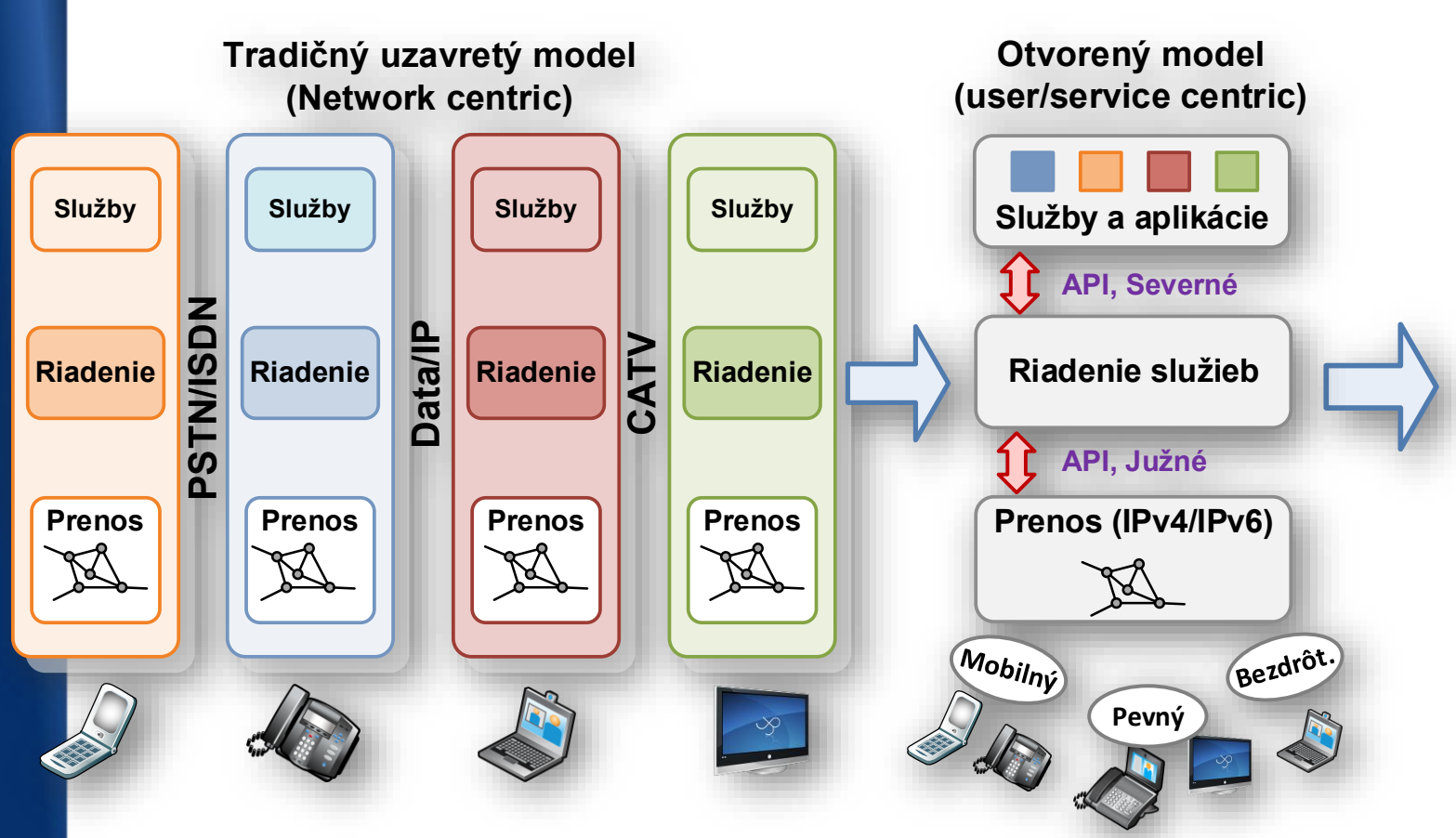
Obsah (Úvod + hrozby + základné pojmy a koncepty,):

- Pochopiť význam sieťovej bezpečnostnej architektúry
- Poznať základné sieťové a bezpečnostné pojmy
- Vedieť identifikovať základné zariadenia a ich úlohy
- Príklady hrozieb a útokov podľa vrstiev a mitigácie

IP siete – krátke pripomenutie a kontext

Východiská

Konvergencia – komplexnosť sietí



Konvergencia vo všetkých oblastiach (Evrything over IP)

(služby, siete, technológie, koncové zariadenia, IT)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

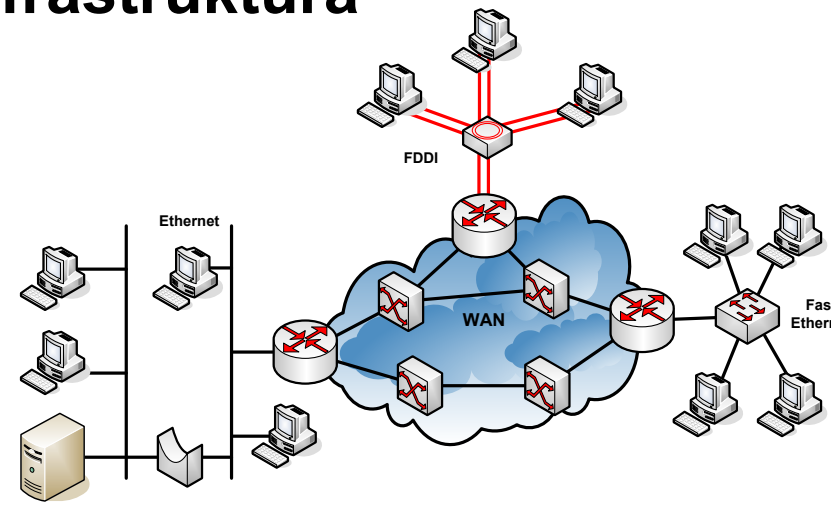
Prečo nás zaujíma sieť

- Voľná definícia pojmu „Komunikačná sieť (KS):

  Súbor koncových staníc a sieťových uzlov prepojených komunikačnými linkami, ktoré umožňujú vzdialenú elektronickú komunikáciu medzi používateľmi alebo koncovými stanicami

  - Poskytuje komunikačnú službu

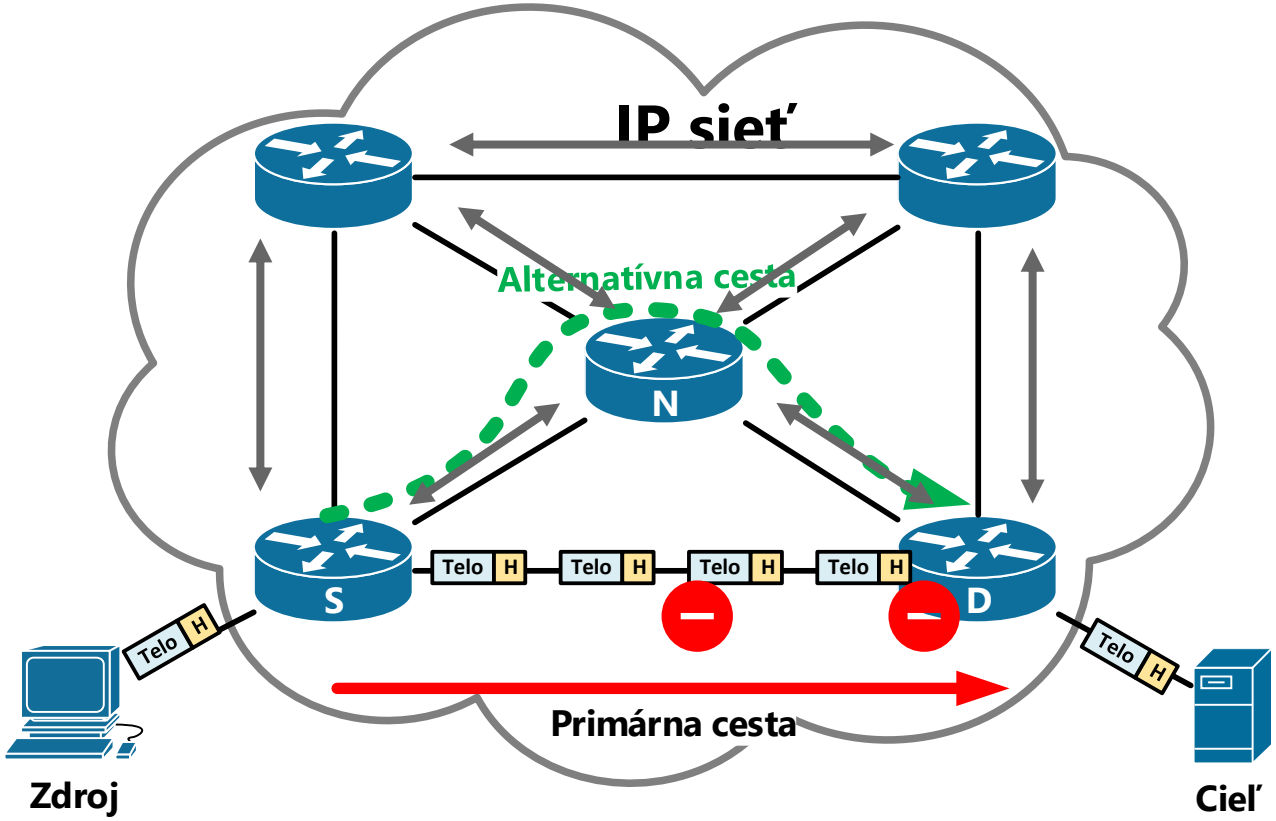
- Pozícia komunikačnej siete dnes = **Sieť je kritická infraštruktúra**
  - Spája ľudí, dáta, aplikácie a cloud
    - „*all-is-connected*“, IoT, BYOD, IoE
  - V digitálnej ekonomike => Sieť je chrbtová kosť biznisu
  - Vstupná brána ku všetkým aktívam
    - *Assets (aktíva) v sieti: Dáta, servery, aplikácie, zariadenia*



- Výpadok alebo kompromitácia siete → okamžitý dopad na služby, výrobu, financie

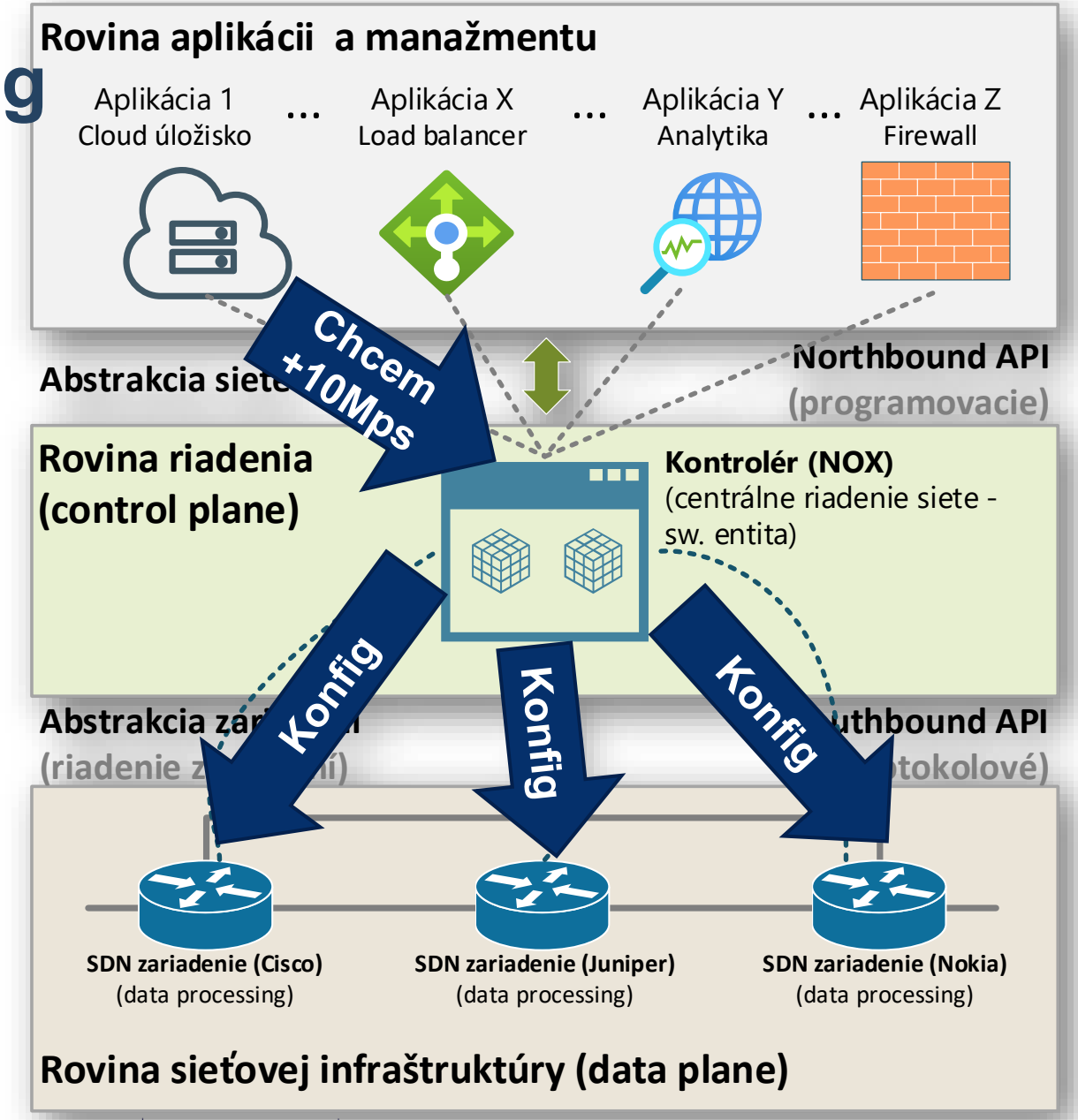
IP siete – princípy a charakteristiky

- Adresovanie (IP adresy)
  - Každé zariadenie/rozhranie má jedinečnú adresu pre komunikáciu v sieti (IPv4/IPv6)
- Paketové prepínanie (Data plane)
  - Dáta vo forme paketov, posielané nezávisle
- Smerovanie (Routing / Control plane)
  - Základný proces, rozhoduje, kadiaľ sa dáta dostanú k cieľu
- Doručenie bez garancie
  - Sieť sa snaží pakety doručiť, ale negarantuje ich spoľahlivosť ani poradie
- Kľúčové vlastnosti IP sietí
  - Decentralizácia
    - Bez centrálneho bodu, čo zvyšuje odolnosť voči výpadkom
  - Škálovateľnosť
    - Fungujú rovnako dobre v malej domácej sieti aj v obrovskom globálnom internete
  - Všadeprítomnosť
    - IP je univerzálny štandard prepojenia



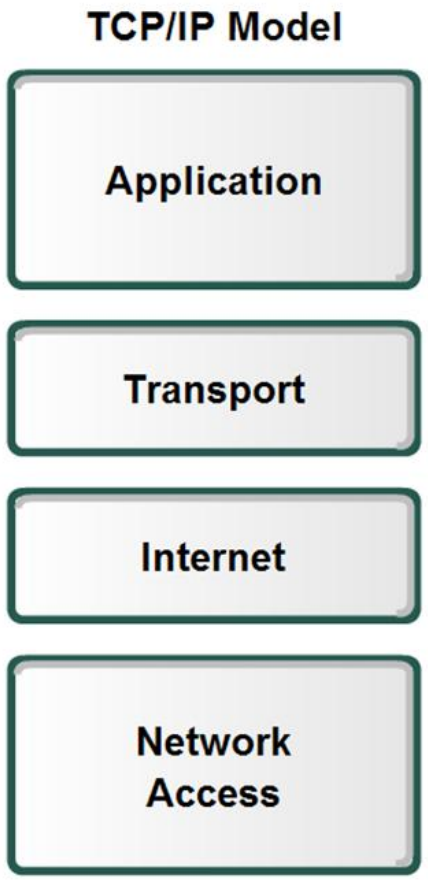
Software Defined Networking

- Zmena prístupu: **Od distribuovaného k centralizovanému riadeniu IP sietí**
  - Oddelenie funkcií riadenia od preposielania
  - Oddelenie služieb od sieťovej infraštruktúry
  - Roviny prepojené otvorenými rozhraniami (API)
- SDN prináša
  - **Na službu orientované sieťové architektúry**
  - Dynamika a flexibilita cez sieťovú automatizáciu a programovateľnosť

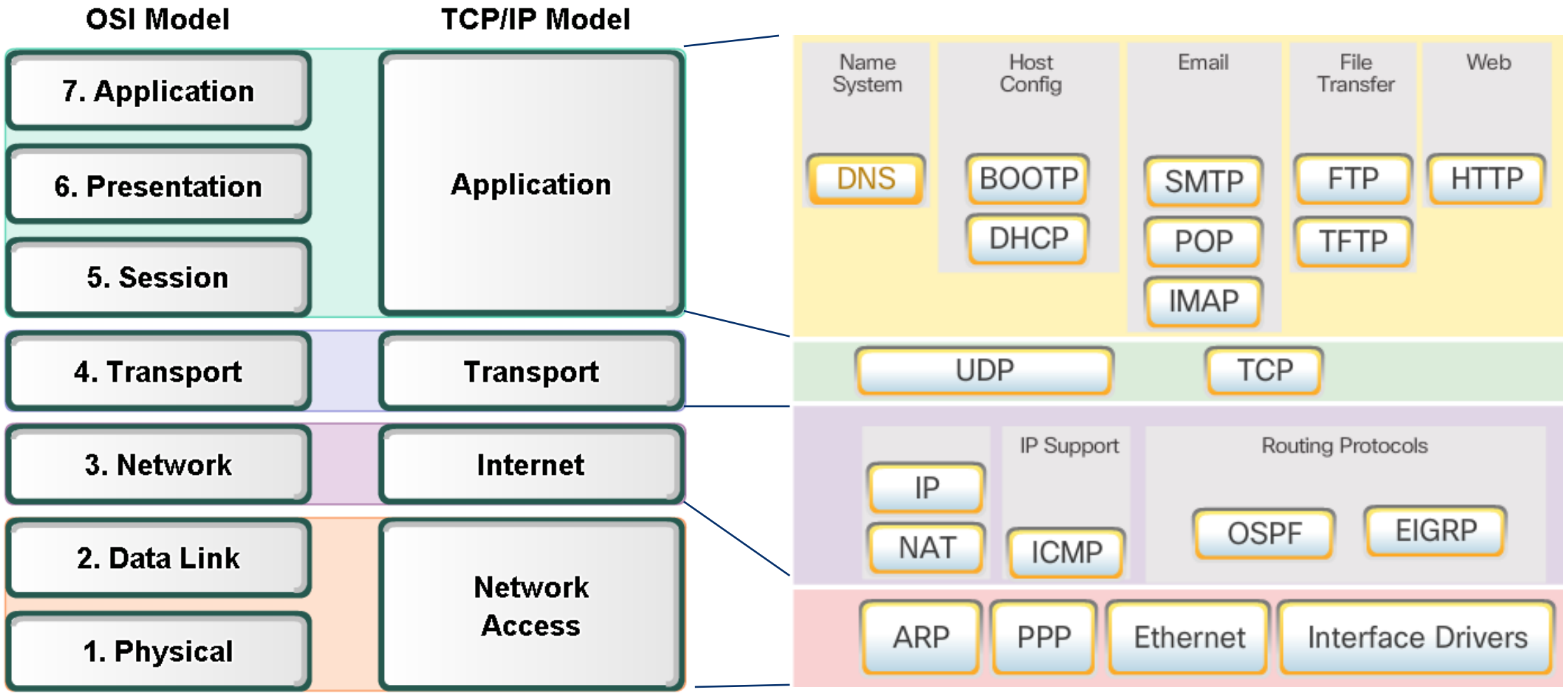


Popis činnosti siete - Protokolový model TCP/IP

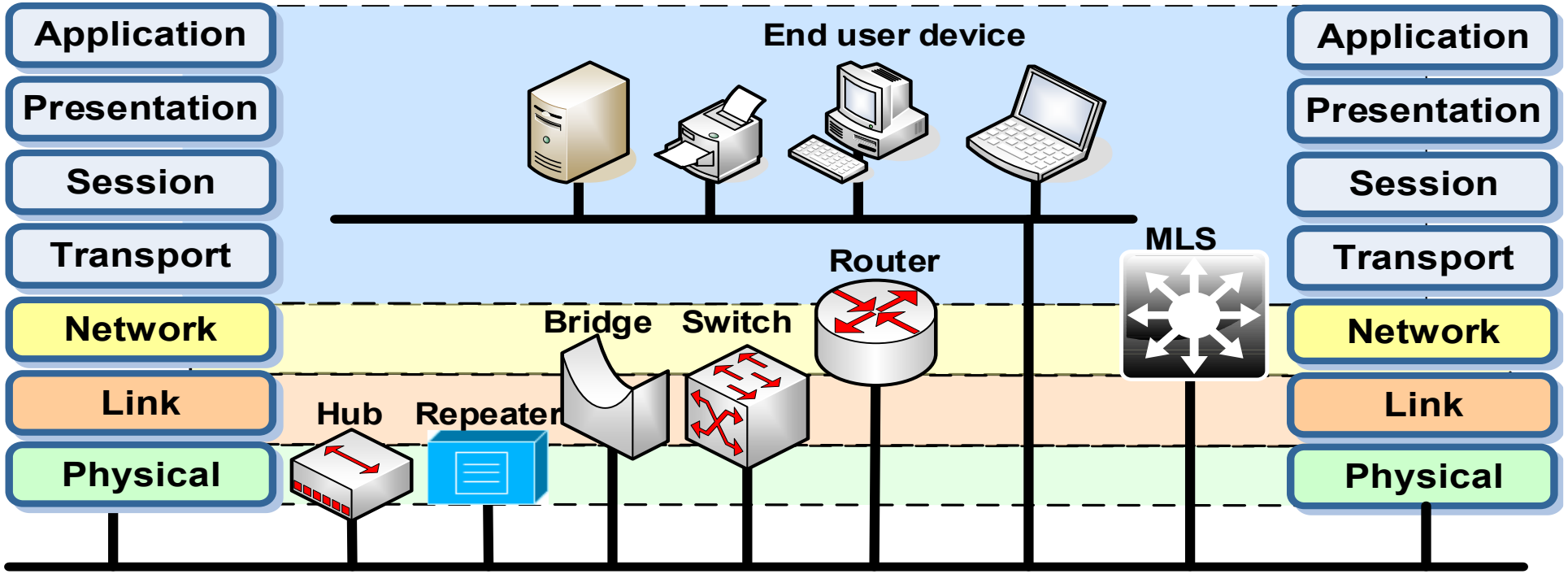
- **Aplikačná vrstva**:
  - Poskytuje nástroje na tvorbu sieťových aplikácií a služieb vrátane identifikácie spoločného formátu prenášaných dát, kódovania a riadenie dialógov medzi komunikujúcimi procesmi
  - Zariadenia: gateway (brána), **host**
  - PDU: správa
- **Transportná vrstva**:
  - Doplnkové služby prenosu dát, riešenie adresovania vhodnému na cieľovom počítači,
  - Rieši otázky spoľahlivosti, spojovanosti a riadenia toku dát
  - Zariadenia: gateway (brána), **host**
  - PDU: datagram (UDP), segment (TCP)
- **Internetová vrstva**:
  - Tvorba internetwork, prenáša pakety medzi vzdialenými koncovými uzlami, určuje vhodnú cestu pre paket idúci sieťou (smerovanie)
  - Zariadenie: smerovač
  - PDU: paket
- **Vrstva prístupu k sieti**:
  - Zabezpečuje funkcie spojené s prenosom rámcov medzi fyzicky susediacimi zariadeniami prepojenými daným médiom, kontroluje prenosové médium a prístup naň
  - Zariadenie: hub, opakovač, bridge, prepínač,
  - PDU: rámec (frame)



Vzťah ISO OSI a TCP/IP a jej protokolová sada



Základné sieťové zariadenia IP sietí



- Medziľahlé sieťové zariadenia
  - Repeater, Hub
    - Pracujú na fyzickej vrstve (L1)
  - Bridge (Most), Switch (Prepínač), NIC (Sieťová karta)
    - Pracujú na linkovej vrstve (L2)
  - MLS prepínač (L2 až L7 prepínač)
  - Smerovač
    - Pracuje na sieťovej vrstve (L3)

- Koncové uzly
  - Slúžia ako vstupné body
  - PC, servery, pracovné stanice, tlačiarne
  - VoIP, IP kamery atď.
  - Pracuje na všetkých 7 vrstvách (L7)

Delenie sietí podľa oblasti nasadenia

- **SOHO (Small Office / Home Office)**
  - Jednoduchá architektúra, často „all-in-one“ zariadenia (Wi-Fi router s NAT, základný FW)
  - Priorita: nízke náklady, jednoduchá správa
  - Typické slabiny: používateľ, default nastavenia, nízka segmentácia, slabé zabezpečenie Wi-Fi
- **Enterprise network (Podnikové siete)**
  - Viacvrstvová architektúra (core–distribution–access)
  - Segmentácia na LAN, WAN, DMZ, VPN, cloudové integrácie
  - Dedikované bezpečnostné zariadenia a monitoring
  - Priorita: komplexná segmentácia, viacero úrovní ochrany
- **Telco/Service Provider Network (Siete poskytovateľov)**
  - Veľkoplošné WAN a backbone siete, BGP, MPLS, 5G/FTTH infraštruktúra
  - Priorita: dostupnosť, redundancia, ochrana proti DDoS, SLA garantované služby
- **Datacenter Networks (Siete dátových centier)**
  - Vysoká hustota serverov, virtualizácia (VM, kontajnery), East-West traffic
  - Interný traffic East-West je dôležitejší než perimetrový (South-North)
  - Priority: mikrosegmentácia, rýchle prepínanie, hardening hypervisorov
- **Cloud Networks (Virutálne siete Cloud prostredí)**
  - Public (AWS, Azure, GCP), Private, Hybrid
  - Model **shared responsibility** – časť zabezpečuje provider, časť zákazník
    - „Provider zabezpečuje cloud, ale zákazník zabezpečuje V CLOUDE “

Sieťové hrozby a útoky

Prečo nás zaujíma sieť z pohľadu bezpečnosti

Problém?

- Siete
  - Sami sú ako aj prepájajú aktíva (Assets)
  - Sú konvergované a komplexné (hlas, video, dáta, IoT, cloud)
    - Tvoria ich rôzne HW + SW komponenty
  - => Každý prvok potencionálne obsahuje zraniteľnosti (vulnerabilities)
- Útočníci cielia na tieto slabiny sietí
  - => vznikajú hrozby a riziká

Pojmy

- Assets:
  - *Čokoľvek hodnotné v organizácii (dáta, servery, aplikácie, zariadenia, služby)*
- Vulnerabilities (zraniteľnosti)
  - *Slabiny v HW, SW, konfigurácii alebo procese, ktoré možno zneužiť*
- Hrozba (Threat / Hrozba)
  - *Potenciálna udalosť, ktorá môže zneužiť zraniteľnosť konkrétneho aktíva a spôsobiť škodu*
  - *Potenciálna nebezpečná udalosť*
- Riziko (Risk)
  - *Pravdepodobnosť, že hrozba zneužije zraniteľnosť aktíva*
  - *Vyjadruje pravdepodobnosť výskytu incidentu*

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady kybernetických hrozieb

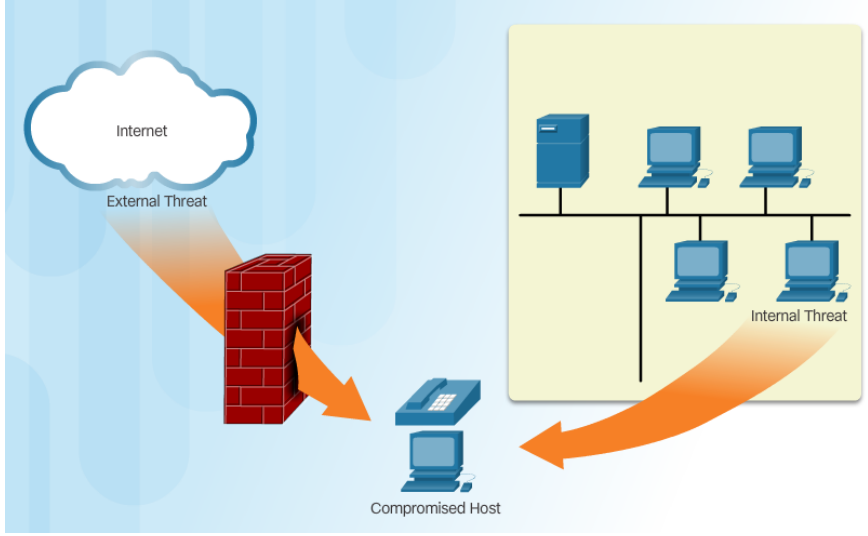
- Softvérové útoky
  - Malware, DoS/DDoS, exploitácia zraniteľností
- Softvérové chyby
  - Bugy, výpadky služieb, chybné skripty
- Sabotáž
  - Úmyselné poškodenie systémov oprávneným používateľom
- Ľudské chyby
  - Misconfigurations, slabé heslá, neúmyselné chyby
- Krádež
  - Odcudzenie HW alebo citlivých dát
- HW zlyhania
  - Poruchy zariadení, diskov, sieťových prvkov
- Prerušenie služieb
  - Výpadky elektriny, zlyhanie chladenia, požiarne systémy
- Prírodné katastrofy
  - Povodne, zemetrasenia, požiare, búrky

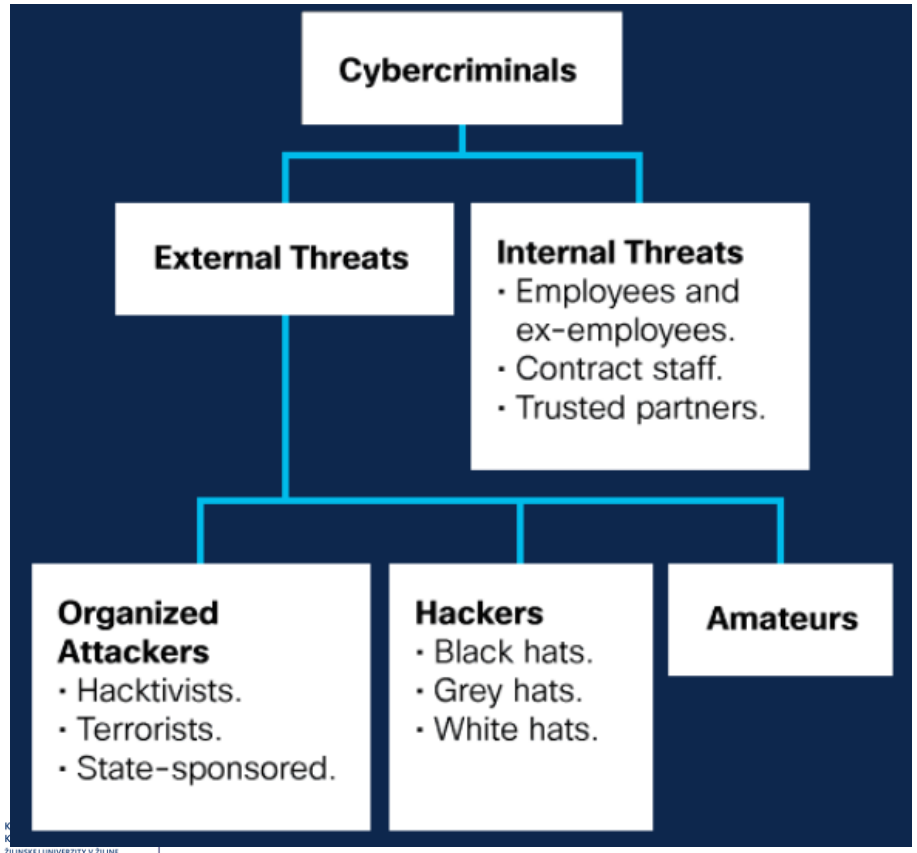
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Východiská a základné pojmy

Interné vs Externé hrozby

- **Interné (vnútorné) hrozby**
  - Zvyčajne ich spôsobujú **súčasní alebo bývalí zamestnanci** a **zmluvní partneri**
  - Môžu byť **neúmyselné alebo úmyselné**
    - Neúmyselné
      - Nesprávne narábanie s dôvernými dátami
      - Pripojenie infikovaných médií
      - Otváranie škodlivých e-mailov alebo webov
      - Zlé rozhodnutia
    - **Úmyselné činy**
      - **P**odvod, sabotáž, špionáž, krádež majetku
  - **Potenciálne väčšie škody ako externé hrozby**.
  - **Dôvody:** priame prístupy, znalosť siete, infraštruktúry, dát, služieb, ľudí, procesov, bezpečnostných opatrení
  - **Trend:** tieto hrozby získavajú na význame
- **Externé hrozby**
  - Pochádzajú od **osôb mimo organizácie**
  - Útočníci môžu byť:
    - **Amatéri** (script kiddies)
    - **Skúsení** útočníci
  - Cieľ: **získať prístup k interným zdrojom organizácie**





Prečo nás zaujíma sieť z pohľadu bezpečnosti

Problém?

- Slabiny sieti a systémov
  - *Attack surface*
- Útočníci cieliaci na tieto slabiny sietí
  - => Vykonávajú kybernetický útok
- Ako?
  - Realizáciou vektoru útoku cez exploit
- **Cieľ bezpečnosti** = znížiť útočnú plochu potláčaním a protiopatreniami (mitigation)

Pojmy

- Attack surface
  - *Celkový súčet zraniteľností v danom systéme, ktoré môže útočník využiť*
- Útok (Attack)
  - *Konanie, ktorým sa entita snaží obísť bezpečnostné služby a porušiť politiku*
  - *Môže byť zvonka/zvnútra, pasívny/aktívny*
- Attack vector
  - *Cesta alebo metóda, ktorou sa útočník snaží získať prístup*
  - *Spôsob realizácie útoku*
- Exploit
  - *Mechanizmus, ktorý využíva konkrétnu zraniteľnosť na kompromitáciu aktíva*
- Mitigácia (Mitigation / Zmiernenie)
  - *Opatrenie na zníženie závažnosti alebo pravdepodobnosti zneužitia zraniteľnosti*
  - *Často označované ako countermeasures (protiopatrenia)*

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kto útočí

- **Hacker**
  - Teraz (žijeme v zjednodušenom svete)
    - Spravidla ide o kybernetického útočníka cez sieť
      - Využíva zraniteľné miesta
  - Predtým alebo lepšia definícia
    - Kvalifikovaný počítačový expert, ktorý využíva svoje technické znalosti na prekonanie problému
- Typy hackerov
  - **White** Hat (the good one)
    - Zručnosti v mene dobra
    - Ethical hackers, pentesters, skill testers, vulnerability researchers ☺, admins
  - **Black** Hat (the bad one)
    - Neeticky hacking
    - Hackuje pre osobný zisk alebo iných zlých dôvodov
    - Slovensky: Lotor, oplan, niktoš, galgan, paskuda., pľuha, gauner....(viac slov. Ľ. Štúra)
  - **Gray** Hat (the … last one)
    - Robte neetické veci, ale nie pre zisk
  - Green, Red, Blue Hat
- Ďalšie moderné pomenovanie:
  - Script Kiddies (blue one)
    - Tínedžeri or používatelia s menšími vedomosťami
    - Používajú predripravené skripy či nástroje (Kali?)
  - Vulnerability Brokers (grey)
    - Objav a nahlás
  - Hacktivists (grey)
    - Vyjadrenie prostestu(anonymous)
  - Cyber Criminals (black)
    - Operate in underground economy (Lone volwes)
      - buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, private information, intellectual property, and much more.
  - Štátom sponzorovaný hacker (? ? ??)
    - Najnovší typ, veľmi pokročilý
      - Útočníci financovaní vládou (stuxnet)
    - Nie sú oficiálne priznaný

Kategórie bezpečnostných / útočných nástrojov

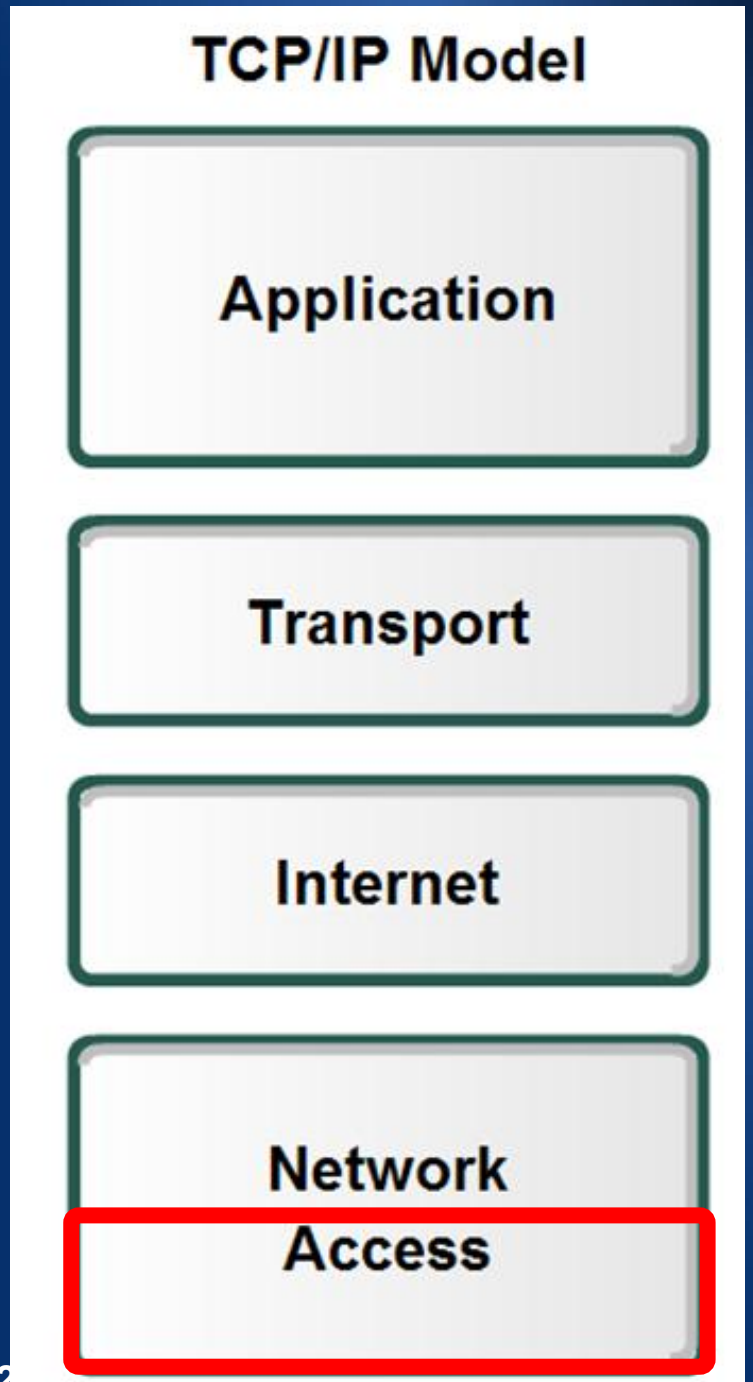
- Penetration testing tools and toolkits:
  - Password crackers
    - Also called password recovery tool ☺
    - Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, Meduse
  - Wireless hacking
    - Kismet, Aircrack-ng, KisMAC, Firesheep
  - Network scanning and hacking
    - Network probing
    - Nmap, SuperScan, Angry IP Scanner, hping3
  - Packet crafting
    - Firewall test tools, packet generators
    - Hping, scapy, Socat, Netcat, Nemesis …
  - Packet sniffers
    - Capture and analyze
    - Wireshark, tcpdump, Ettercap, Paros, Dsniff, Fiddler, EtherApe. SSLstrip …
  - Rootkit detectors
    - Directory and file integrity checkers
    - AIDE, NetFilter …
- Fuzzers to search vulnerabilities
  - Fuzzing = assurance technique used to discover coding errors and security loopholes in software, operating systems or networks
  - Fuzzer, Social Engineering Toolkit (SET), Skipfish, Wapitti, W3af, wfuzz …
- Forensic
  - computer investigation and analysis techniques in the interests of determining potential legal evidence.
  - Kit, Helix, Maltego, Encase
- Debuggers
  - Reverse engineering
  - GDB, WinDog, IDA, Imunity Debugger
- Encryption
- Vulnerability exploitation
  - Metasploit, Netsparker, Sqlmap, Core Impact
- Vulnerability Scanners
  - Network and system identity scans
  - OpenVAS, Nessus, Nipper, Secuma PSI
- … many of them *nix based

Čím útočí /

Kali, BlackBox, Parrot Security, BlackArch, Fedora security, Network security toolkit …

Útoky po vrstvách - prehľad

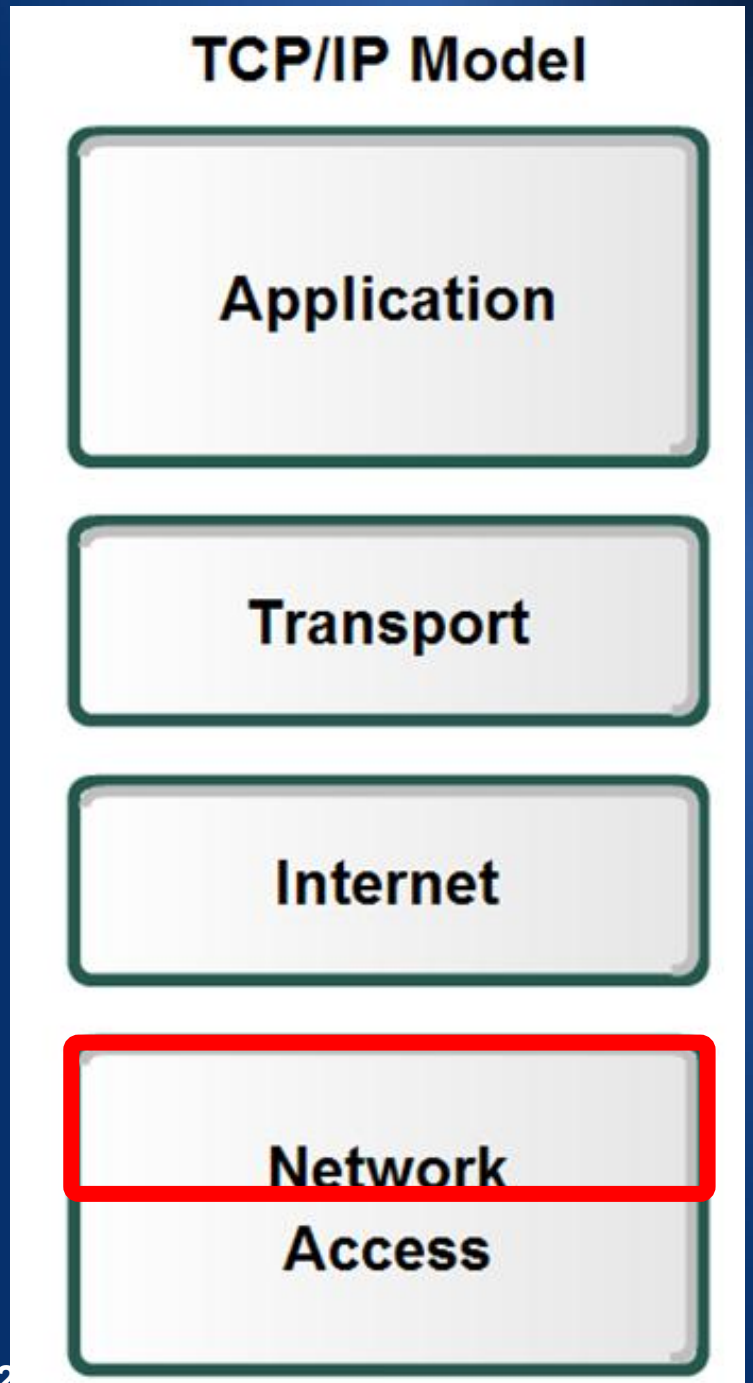
Vrstva (L)	Typ útoku	Príklady útokov	Dopady na podnikovú sieť	Kľúčová mitigácia/Ochrana
L1 (Fyzická)	Pasívne, Aktívne, Fyzické	Odpočúvanie (TAPs), Rušenie (Jamming), Poškodenie káblov	Únik dát, výpadok služieb, kompromitácia zariadení	Fyzická bezpečnosť, MACsec šifrovanie, monitorovanie integrity
L2 (Linková)	Pasívne, Aktívne	MAC spoofing, ARP poisoning, VLAN hopping	Únik dát (MITM), narušenie segmentácie	Port security, ARP inspection, DHCP snooping, privátne VLAN
L3 (Sieťová)	Manipulácia, Zahltenie, Smerovanie	IP spoofing, ICMP flood, BGP hijacking	Výpadok služieb, presmerovanie dát, únik dát	Anti-spoofing filtre (uRPF), rate limiting, autentifikácia smerovacích protokolov
L4 (Transportná)	Zahltenie, Zber info, Manipulácia	TCP SYN flood, UDP flood, Port scanning, Session hijacking	Výpadok služieb (zahltenie), únik dát (hijacking)	TCP SYN cookies, firewall pravidlá, šifrovanie relácií (TLS)
L5-7 (Aplikačná)	Exploitácia, Sociálne inžinierstvo, Malvér, Zahltenie	SQL injection, Phishing, Ransomware, DNS poisoning, HTTP flood	Únik dát, kompromitácia používateľov, výpadok služieb	WAF, IPS, emailové filtre, Antimalware, DNSSEC, bot detekcia



Útoky na fyzickej vrstve (L1)

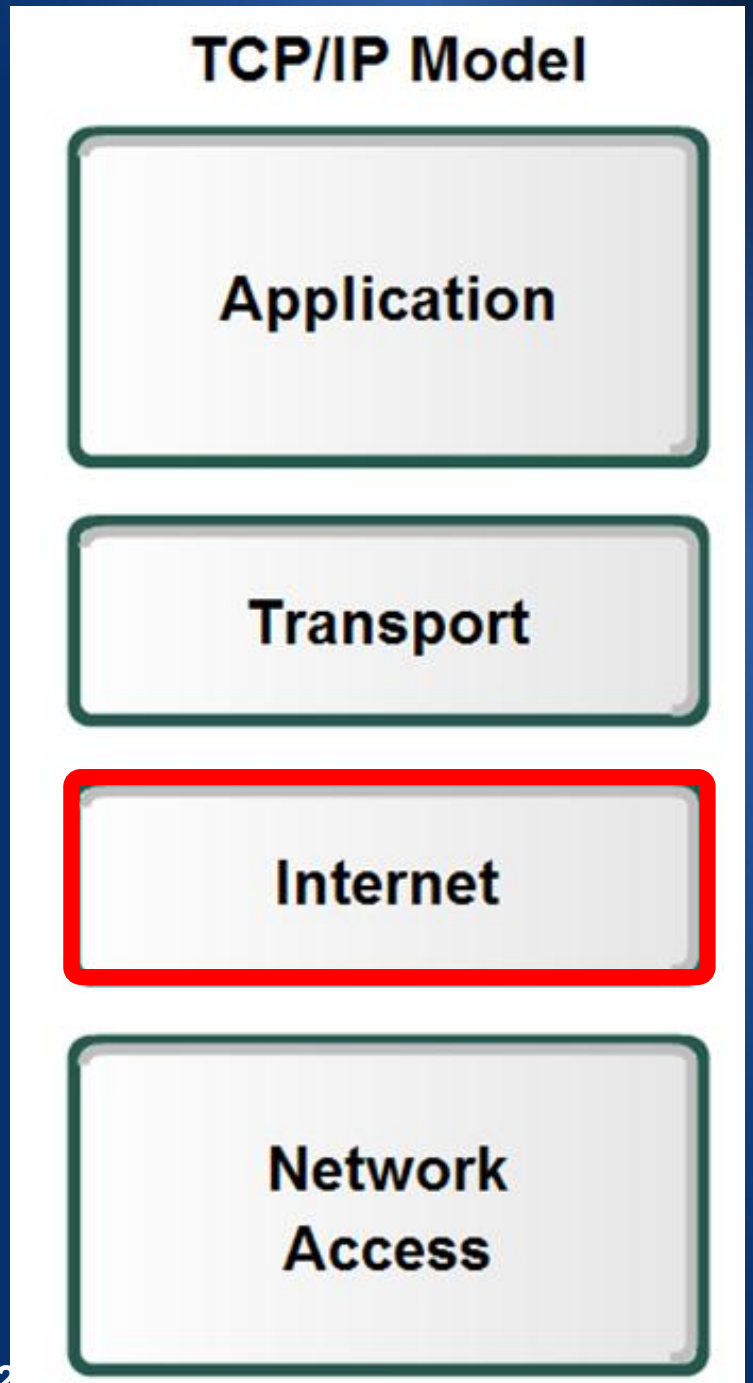
- **Klasifikácia útokov**
  - **Pasívne (odpočúvanie):** Získavanie dát bez zásahu do prenosu
    - **Príklady:** Káblové odbočenie (TAPs), RF monitoring (Wi-Fi sniffing)
  - **Aktívne (rušenie):** Narušenie funkčnosti siete
    - **Príklady:** Jamming Wi-Fi/Bluetooth, elektromagnetické rušenie (EMP)
  - **Fyzické (manipulácia):** Priamy zásah do zariadení/médií
    - **Príklady:** Poškodenie optiky, neoprávnený prístup k switchu/routeru, krádež zariadenia
- **Dopady v enterprise sieťach**
  - Únik dát (odpočúvanie nezabezpečených liniek)
  - Výpadok služieb (prerušené káble, jamming)
  - Kompromitácia zariadení (napr. inštalácia škodlivého firmvéru, loaderov ...)
- **Ochrana**
  - Fyzická bezpečnosť (zámky, prístupové systémy, IPTV)
  - Šifrovanie prenosu (napr. MACsec na L1)
  - Monitorovanie integrity (detekcia výpadkov, alarmy)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



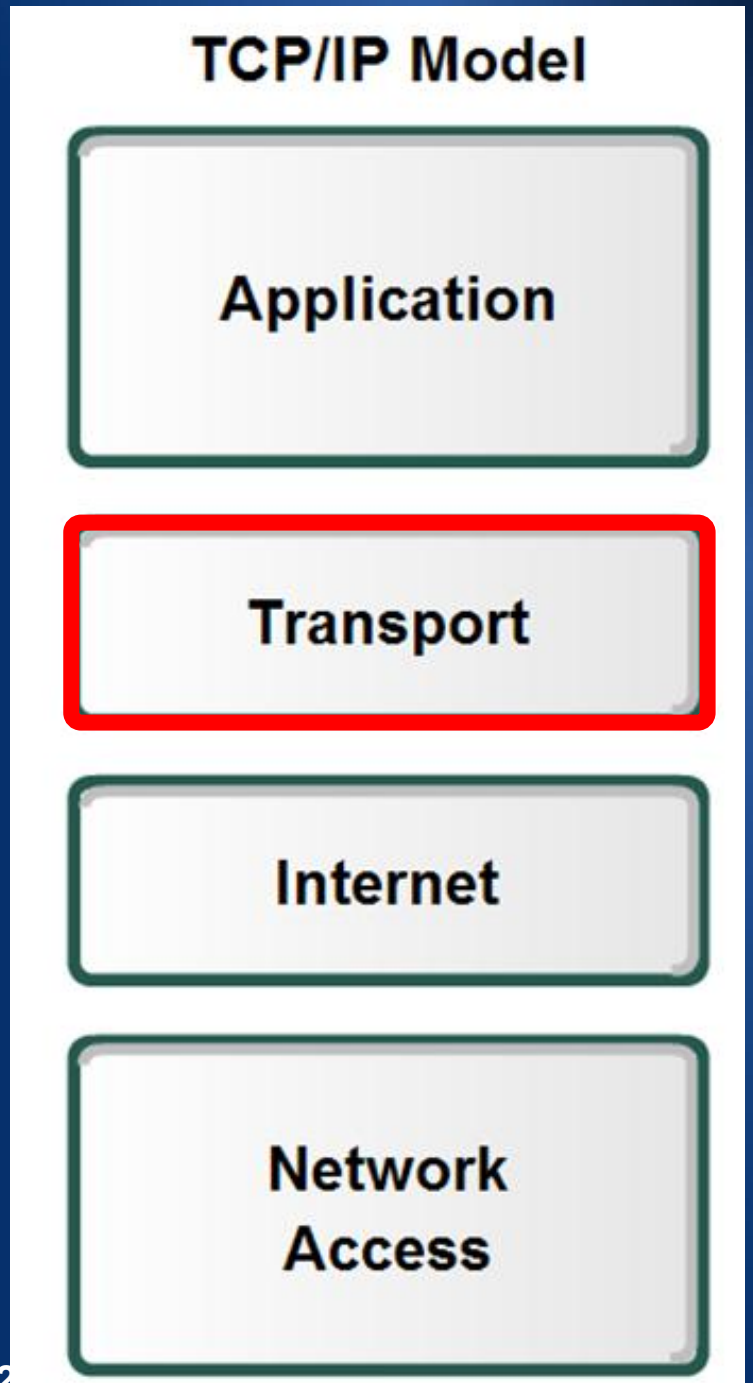
Útoky na linkovej vrstve (L2)

- **Klasifikácia útokov**
  - **Pasívne (odpočúvanie):** Získavanie dát cez manipuláciu L2 protokolov
    - **Príklad:** MAC spoofing (falšovanie MAC adresy na obídenie filtrov)
  - **Aktívne (manipulácia):** Narušenie L2 protokolov na MITM alebo manipulácia s tokom dát
    - **Príklady**
      - ARP poisoning/spoofing (falošné ARP odpovede → MITM útok)
      - DHCP spoofing (útočník vydáva IP adresy, mení gateway/DNS.
  - **Obídenie segmentácie:** Prelomenie L2 segmentácie siete
    - **Príklad:** VLAN hopping (obídenie VLAN segmentácie cez double-tagging)
- **Dopady v enterprise**
  - Únik dát (MITM cez ARP poisoning)
  - Presmerovanie prenosu (DHCP spoofing → falošný DNS)
  - Narušenie segmentácie (prístup do chránených VLAN)
- **Ochrana:**
  - Port security (obmedzenie MAC adries na prepínači)
  - ARP inspection, DHCP snooping (overovanie L2 protokolov)
  - VLAN izolácia, privátne VLAN (zamedzenie hoppingu)



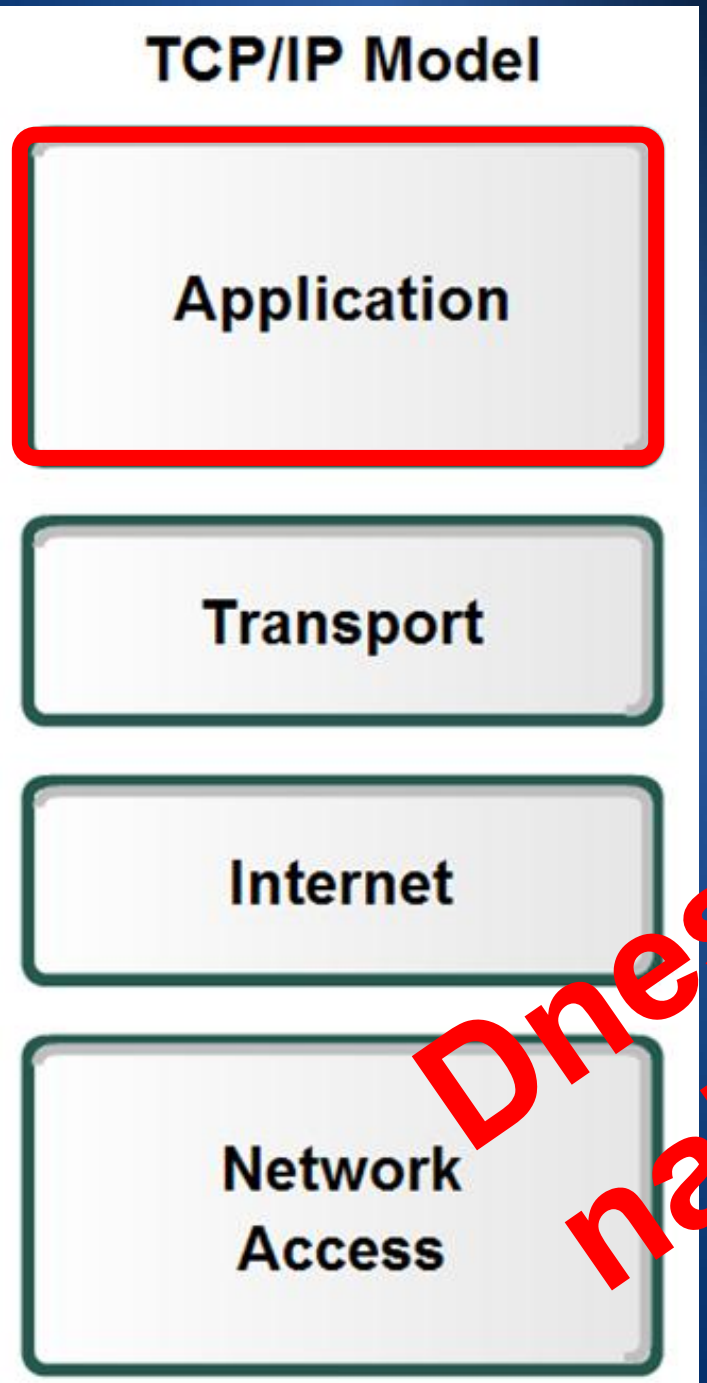
Útoky na sieťovej vrstve (L3)

- **Klasifikácia útokov**
  - **Manipulácia identity:** Falšovanie odosielateľa
    - **Príklad:** IP spoofing (falšovanie IP adresy na obídenie filtrov)
  - **Zahltenie siete:** Vytvorenie preťaženia na L3
    - **Príklady:**
      - ICMP flood (zahltenie siete ICMP požiadavkami)
      - Ping of Death (poškodenie cieľa chybnými ICMP paketmi)
      - Smurf attack (zosilnený ICMP útok cez broadcast)
  - **Útoky na smerovanie:** Narušenie routovacích protokolov
    - **Príklady:** RIP poisoning, OSPF LSA injection, BGP hijacking (manipulácia smerovacích tabuliek)
- **Dopady v enterprise:**
  - Únik dát alebo MITM (spoofing umožňuje obísť ACL)
  - Výpadok služieb (ICMP flood/Smurf zahlcuje linky)
  - Presmerovanie prenosu (BGP hijacking → nesprávne cesty)
- **Ochrana:**
  - Anti-spoofing filtre (uRPF na routeroch)
  - Rate limiting ICMP (ochrana pred floodom)
  - Autentifikácia smerovacích protokolov (MD5 pre OSPF/BGP)



Útoky na transportnej vrstve (L4)

- **Klasifikácia útokov**
  - **Zahltenie služieb:** Vytvorenie preťaženia na L4 protokoloch
    - **Príklady**
      - TCP SYN flood (zahltenie polootvorenými spojeniami)
      - UDP flood (zahltenie servera UDP prevádzkou)
  - **Zber informácií:** Prieskum siete na zraniteľnosti
    - **Príklad:** Port scanning (zisťovanie otvorených portov)
  - **Manipulácia relácií:** Narušenie existujúcich spojení
    - **Príklad:** Session hijacking (prevzatie TCP relácie)
- **Dopady v enterprise**
  - Výpadok služieb (SYN/UDP flood zahltenie serverov)
  - Únik dát (session hijacking a únik dát)
  - Prieskum pre ďalšie útoky (port scanning a ďalšie zraniteľnosti)
- **Ochrana**
  - TCP SYN cookies, rate limiting (proti flood útokom)
  - Firewall pravidlá (blokovanie nevyžiadaného UDP/portov)
  - Šifrovanie relácií (TLS proti hijackingu)



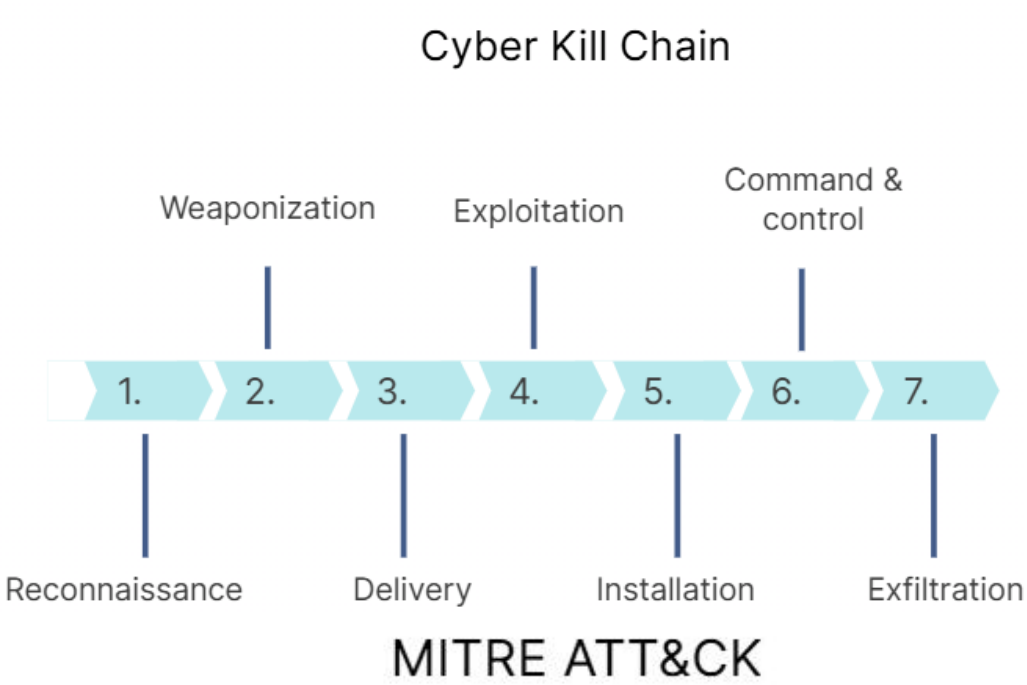
Útoky na aplikačnej vrstve (L5-7)

- **Klasifikácia útokov**
  - **Exploitovanie zraniteľností:** Zneužitie slabín v aplikáciách
    - **Príklady:** SQL injection, XSS, command injection
  - **Sociálne inžinierstvo:** Manipulácia používateľov
    - **Príklady:** Phishing, spear phishing, social engineering
  - **Malvér a ransomware:** Šírenie škodlivého kódu
    - **Príklady:** Malware cez HTTP, e-mail, drive-by download
  - **DNS útoky:** Narušenie alebo zneužitie DNS služieb
    - **Príklady:** DNS poisoning, DNS tunneling
  - **Zahltenie aplikácií:** Aplikačný DDoS útok
    - **Príklad:** HTTP flood (zahltenie servera požiadavkami)
- **Dopady v enterprise**
  - Únik dát (SQL injection odhalí databázy)
  - Kompromitácia používateľov (phishing ukradne prihlasovacie údaje)
  - Výpadok služieb (HTTP flood, ransomware zastaví operácie)
  - Presmerovanie prenosu (DNS poisoning)
- **Ochrana**
  - WAF (ochrana proti SQL injection, XSS)
  - E-mailové filtre, SPF/DKIM/DMARC (proti phishingu)
  - Antimalware a sandboxing (proti ransomware)
  - DNSSEC, DNS monitoring (proti poisoning/tunneling)
  - Rate limiting, bot detekcia (proti HTTP flood)

Dnes najčastejšie a najnebezpečnejšie

Typy sieťových útokov

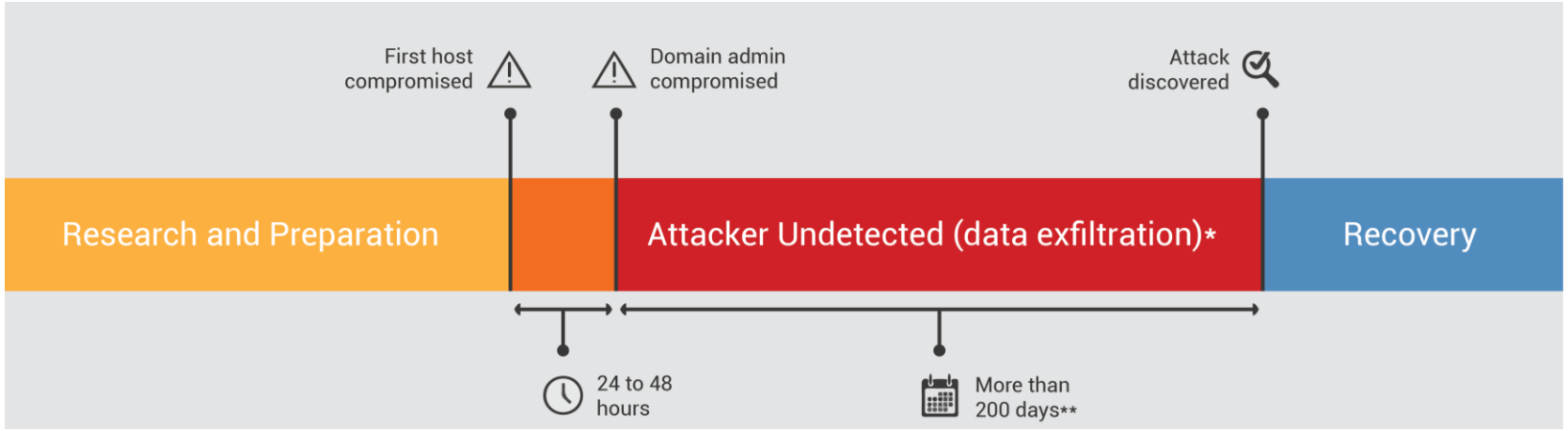
- Sieťový / bezpečnostný profesionál
  - **Musí vedieť zmierňovať útoky** → to znamená **rozumieť sieťovým (a systémovým) útokom**
- **Problém =>** existuje veľké množstvo typov útokov
- **Riešenie**
  - **Klasifikácia útokov a postupov**
  - Lepšie je chápať **generické typy** než sa učiť každý útok zvlášť (inak to môže byť zahlcujúce)
- **Frameworky útokov**:
  - Existuje viacero rámcov, ktoré pomáhajú:
    - pochopiť **útoky, taktiky, fázy, dopady**
  - **Príklady**
    - Lockheed Martin Cyber Kill Chain
    - MITRE ATT&CK
    - …



Source: https://attack.mitre.org/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Attack Timeline (časová os útoku)



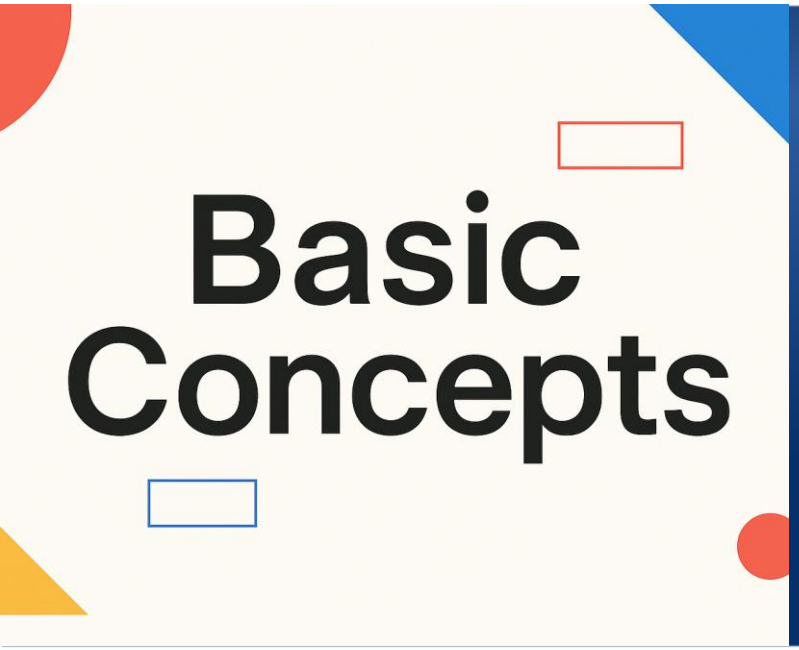
- Príprava útoku (Research & Preparation)
  - Zber informácií, skenovanie, phishing, príprava exploitov
- Prvotná kompromitácia (24–48 hod.)
  - Infekcia prvého hosta alebo účtu
- Eskalácia oprávnení
  - Získanie doménového administrátora, laterálne pohyby
- Útočník neodhalený (200+ dní)
  - Dlhodobá prítomnosť v sieti, exfiltrácia dát, špehovanie
  - => problém dlhá fáza neodhalenia
- Detekcia útoku
  - Incident response, forenzná analýza
- Obnova (Recovery)
  - Čistenie, patchovanie, lessons learned

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Trendy v sieťovej bezpečnosti - 2025

- **AI Phishing a Generatívne útoky**
  - Deepfake hovory, AI-generované e-maily a malvér – útočníci používajú gen AI na sofistikované phishingové kampane
  - Zvýšené využitie AI na personalizované útoky zvyšuje úspešnosť o 20-30% (https://deepstrike.io/blog/top-cybersecurity-threats-2025)
- **Quantum threats**
  - Ohrozenie asymetrických šifier (RSA, ECC) kvôli quantum computing – potreba prechodu na post-quantum kryptografiu
  - NIST odporúča migráciu, ako útoky na šifrovanie sa stávajú realitou do 2030
- **Supply chain útoky**
  - Kompromitácia dodávateľov a softvéru (napr. SolarWinds 2020, MOVEit 2023) – zameranie na third-party riziká
  - Rast o 15% v 2025, s dôrazom na edge devices a open-source knižnice
- **Cloud & remote work**
  - Rozplývanie perimetra – shift k SASE a Zero Trust pre hybridné prostredia
  - 72% organizácií hlási zvýšené riziká kvôli cloud migrácii a remote access (https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/)
- **Ďalšie kľúčové trendy**
  - **Ransomware evolution:** Sofistikovanejšie taktiky, vrátane double extortion a AI-assisted šírenia
  - **OT cyber threats:** Zvýšené útoky na operačné technológie (IoT, ICS) v kritických sektoroch
  - **Regulačné zmeny:** Prísnejšie normy (NIS2, DORA) nútia k compliance a resilience
  - **AI v obrane:** Použitie gen AI na automatizovanú detekciu a odpoveď na hrozby

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

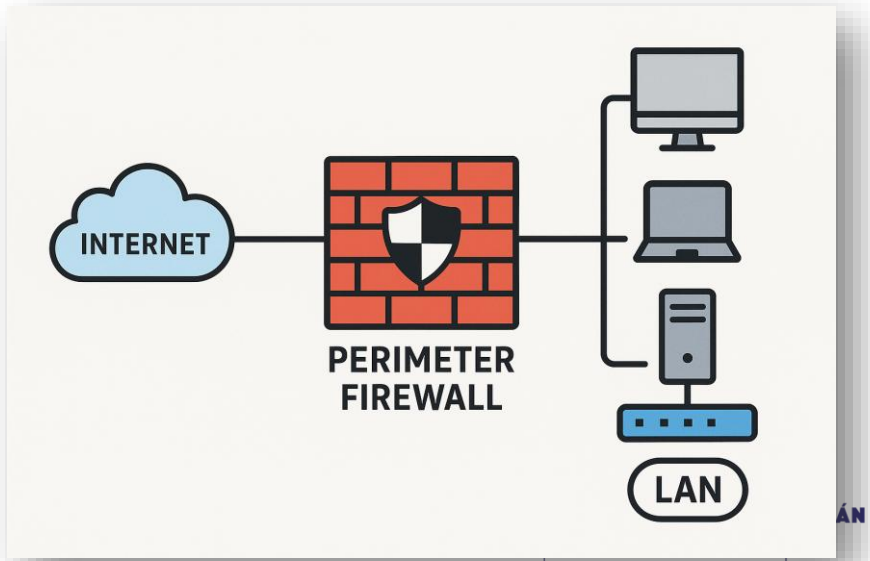


Základné bezpečnostné koncepty a pojmy v sieťovej architektúre

Základné pojmy: Perimeter, Trust zone

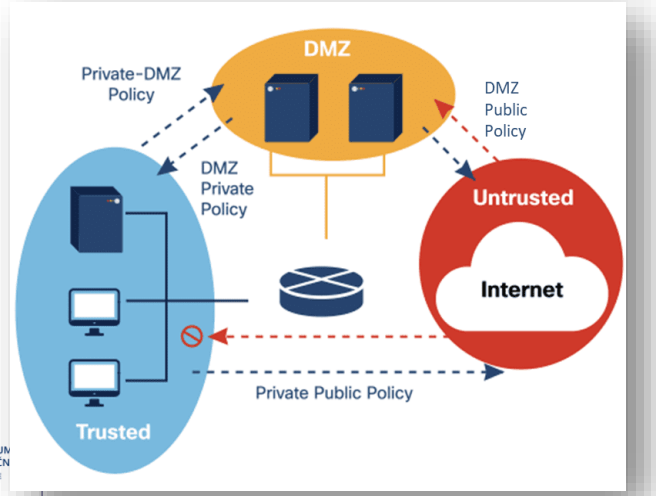
Perimeter (sieťová hranica)

- Hranica medzi internou a externou sieťou
- Tradične definovaný firewallom alebo hraničným routerom
- Dnes sa koncept perimetra rozplýva
  - cloud, remote access, mobilita, BYOD...
- Stále základ bezpečnostného dizajnu



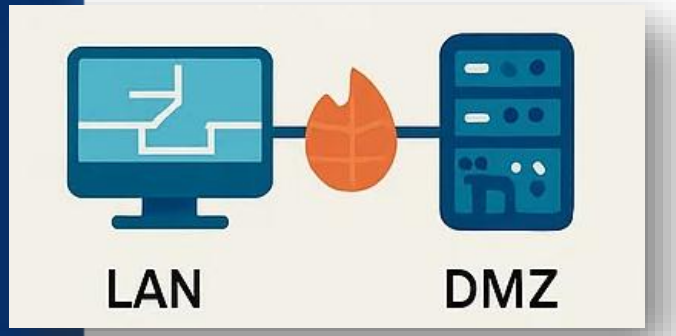
Trust Zones (Zóny dôvery)

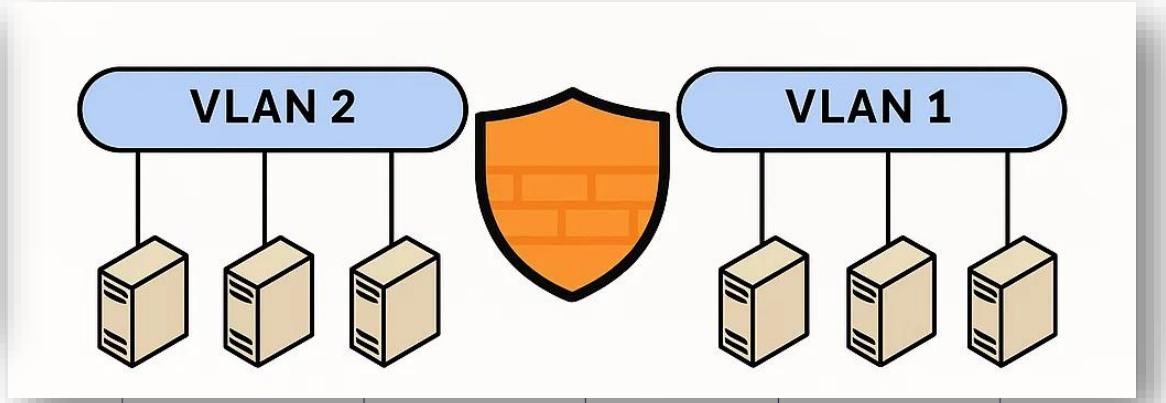
- Rozdelenie siete do zón
  - Interná sieť (LAN) – vysoká dôveryhodnosť
  - DMZ – polodôveryhodná zóna, nárazník pre verejné služby (webserver)
  - Internet/Outside – nedôveryhodné prostredie
  - Cloud – zóna s čiastočnou kontrolou (shared responsibility)



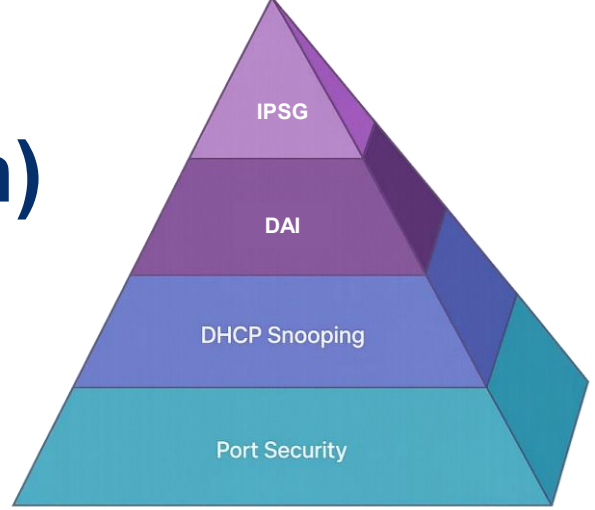
Základné pojmy: Segmentácia siete

- **Izolácia ako ochrana v IP sieťach**
  - Základ bezpečnostnej architektúry v enterprise
- **Definícia segmentácie**
  - Rozdelenie siete na menšie, izolované segmenty (zóny) na zníženie rizika šírenia útokov
- **Typy segmentácie**
  - **Fyzická:** Oddelené zariadenia/siete (napr. samostatný switch pre DMZ)
  - **Logická:** VLAN (L2), VRF (L3), mikrosegmentácia (softvérové oddelenie v rámci siete,napr. VxLAN, Ipsec, ...)
- **Príklady v praxi**
  - **LAN vs. DMZ:** Interná sieť oddelená od verejných služieb
  - **Oddelenie oddelení:** HR, IT, financie – každé s vlastným VLAN
  - **Cloud:** Virtuálne siete (VPC) pre izoláciu workloads
- **Výhody**
  - Obmedzenie pohybu útočníka („lateral movement“)
  - Kontrola prístupu (ACL, firewall pravidlá medzi segmentmi)
  - Zníženie dopadu útokov (napr. ransomware izolovaný v jednom segmente).





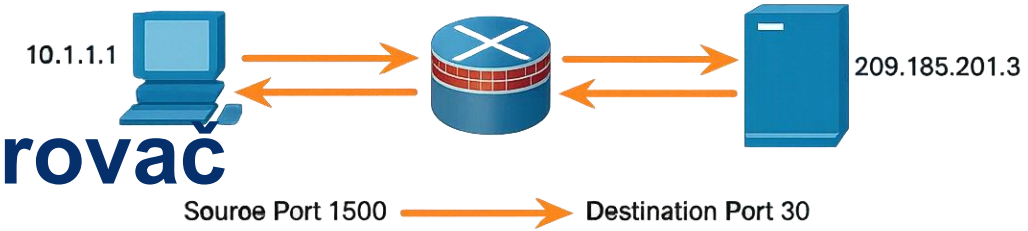
Bezpečnostné zariadenia – Prepínač (Switch)



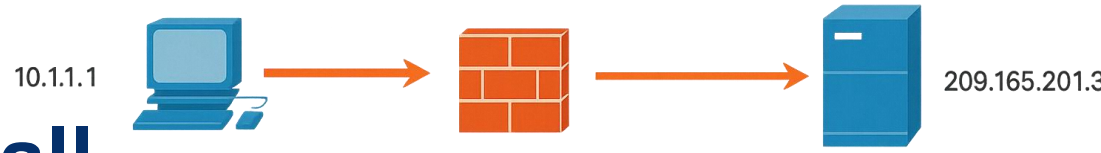
- **Úloha prepínača** v sieťovej bezpečnosti
  - Nie je *primárne* bezpečnostné zariadenie
  - Ale
    - Riadi L2 konektivitu, chráni pred útokmi ako MAC spoofing, ARP poisoning
    - Základ segmentácie siete (VLAN)
    - Prevencia pred „rogue" zariadeniami
- **Kľúčové bezpečnostné funkcie**
  - **Port Security:** Obmedzenie MAC adries na porte
  - **STP ochrana (Spanning Tree Protection):** Prevencia proti manipulácii STP
    - BPDU guard, BPDU Filter, Root Guard, ...
  - **DHCP Snooping**: Filtrovanie neautorizovaných DHCP serverov či DHCP útokov
  - **VLAN / Private VLAN** segmentácia
- **Iné**
  - **MAC ACL:** Jednoduchý filter na základe MAC adries
- **Dopady v enterprise**
  - Zabezpečuje integritu siete (kontrola prístupu, zariadení a protokolov)
  - Znižuje riziko MITM útokov (ARP poisoning)
  - Zníženie laterálneho pohybu
- **Význam**
  - Switch ako **prvá línia ochrany** na L2 access

Smerovač ako základná hranica medzi sieťami

Bezpečnostné zariadenia – Smerovač



- **Úloha smerovača v bezpečnosti**
  - Riadi L3 smerovanie, filtruje prenos a chráni pred útokmi (napr. IP spoofing)
  - Kľúčový prvok na perimetri alebo medzi segmentmi siete
- **Bezpečnostné funkcie**
  - **ACL (Access Control List):** Filtruje prenos podľa IP, portov, protokolov
  - **NAT (Network Address Translation):** Preklad a maskovanie interných IP adries
  - **Routing Filters:** Kontrola obsahu smerovacích protokolov (RIP, OSPF, BGP)
    - Napr. Filtrovanie neplatných ciest (zamedzenie BGP hijackingu)
  - **Control Plane Protection (CoPP):** Chráni riadiacu rovinu smerovača záťaže od DoS útokov na riadiace protokoly
  - **IP Spoofing Ochrana (uRPF):** Overuje zdrojové IP adresy
  - **Reverse Path Check:** Kontroluje spätnú cestu paketov.
- **Dopady v enterprise**
  - Znižuje riziko únikov dát a neautorizovaného prístupu
  - Zabezpečuje integritu a dostupnosť smerovania
- **Význam:**
  - Internet edge router, NAT, route filter, route ACL
  - Router ako L3 screening filter
    - Chráni toky dát a bráni šíreniu útokov

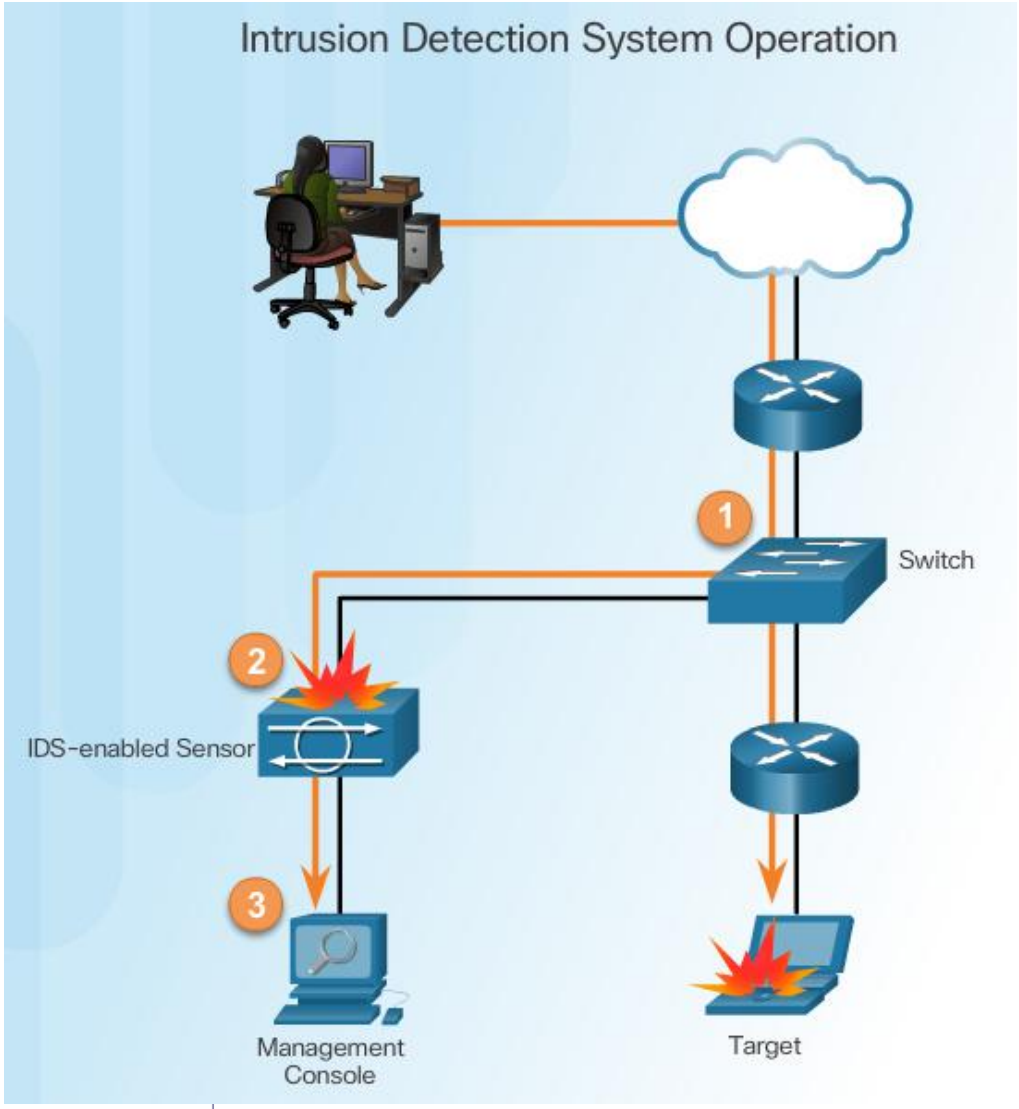


Bezpečnostné zariadenia: Firewall

- **Definícia**
  - Firewall je hardvérové alebo softvérové bezpečnostné zariadenie
  - Monitoruje prichádzajúcu a odchádzajúcu sieťovú premávku a na základe jemu definovaných pravidiel ju povolí alebo zakáže
- **Úloha firewallu v bezpečnosti**
  - Filtruje sieťový prenos na L3/L4 (až L7 u NGFW), chráni pred neautorizovaným prístupom
  - Kľúčový prvok na perimetri, v DMZ alebo medzi internými segmentmi
- **Kľúčové typy a funkcie**
  - **Packet Filter:** Filtrovanie podľa IP, portov, protokolov (statické pravidlá).
  - **Stateful Inspection:** Sleduje stav spojení (TCP handshake)
  - **NGFW (Next-Generation Firewall):** Aplikačná kontrola, IPS, hlboká inšpekcia
- **Dopady v enterprise**
  - Zabraňuje útokom (DDoS, IP spoofing, neautorizovaný prístup)
  - Zabezpečuje dôvernosť a dostupnosť služieb
  - Poskytuje Advanced kontrolné funkcie
- **Význam:**
  - Firewall ako hlavná bariéra – chráni zóny a riadi prenos podľa bezpečnostných politík
  - Centrálna kontrola toku dát
  - Znižuje riziko prieniku z nedôveryhodných sietí
  - Možnosť aplikácie politiky „least privilege“
- Príklady nasadenia
  - Personálny / Perimetrový / Zónový / Cloudový firewall
  - Segmentačný firewall medzi rôznymi oddeleniami v enterprise

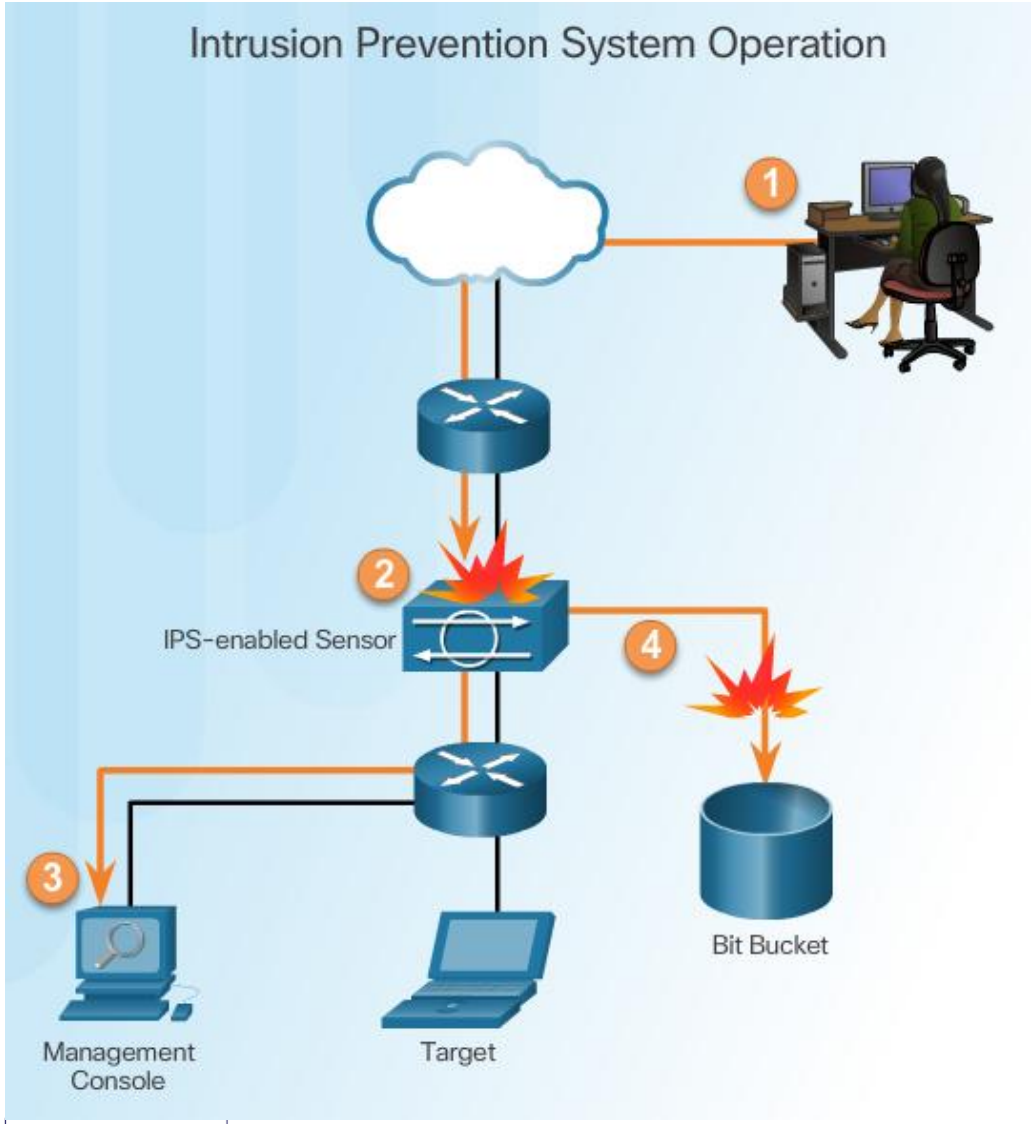
Bezpečnostné zariadenia: IDS – základný koncept

- **IDS (Intrusion Detection System)**
  - Bezpečnostné zariadenie alebo softvér, ktorý **pasívne monitoruje sieťovú alebo systémovú prevádzku**, aby identifikoval podozrivé aktivity, zaznamenával ich a upozornil administrátora.
  - IDS **nezasahuje priamo do toku dát**.
- **Charakteristika**
  - Pasívny monitorovací senzor, prevádzka neprechádza cez zariadenie
  - Analyzuje od L2 po L7
  - **Pasívny prístup**
    - Nezasahuje do prevádzky
    - Identifikuje podozrivú aktivitu a možné incidenty
    - Loguje a reportuje udalosti
  - Primárne orientovaný na viditeľnosť a upozornenie
- **Nasadenie**: SPAN port, TAP mirror
  - Vyžaduje kópiu prevádzky (packets copy)
- **Limity**
  - IDS nemôže zastaviť útok
  - Vie však poslať inštrukciu smerovaču/FW, aby aplikoval politiky (napr. ACL)



Bezpečnostné zariadenia: IPS – základný koncept

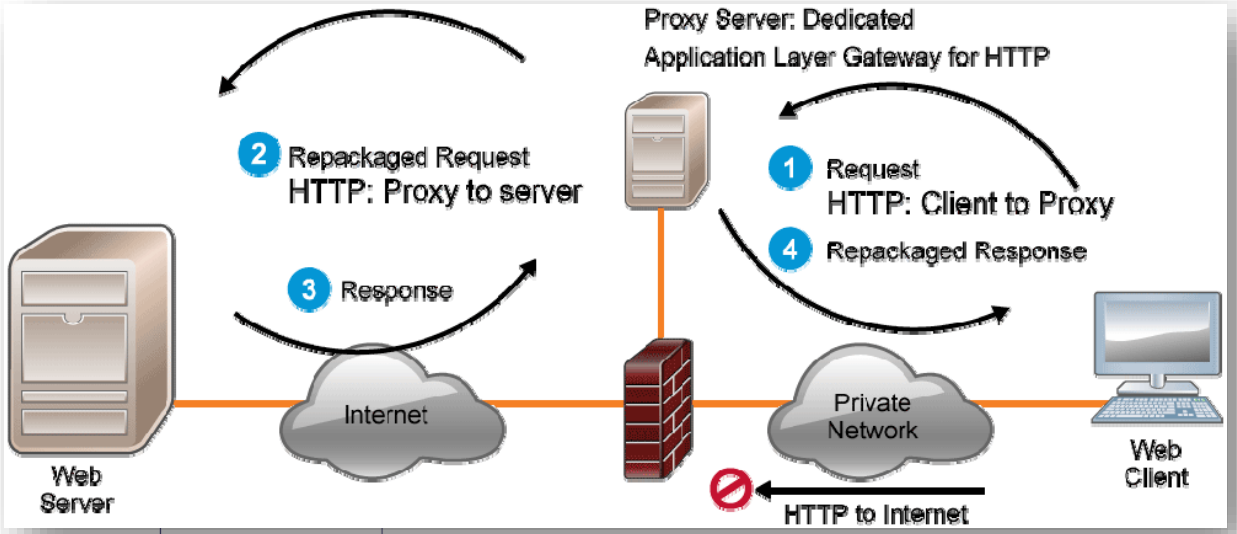
- **Intrusion Prevention System - IPS**
  - Bezpečnostné zariadenie alebo softvér ktorý dokáže **aktívne blokovať alebo meniť sieťovú prevádzku** na základe detegovaných hrozieb
  - Evolúcia IDS - kombinuje detekciu s prevenciou
- **Charakteristika**
  - Detekuje útoky od L2 po L7 (signatúry, anomálie, policy-based)
  - Aktívne blokuje podozrivú alebo škodlivú prevádzku
  - Vie resetovať spojenia, dropnúť pakety, aplikovať politiky
  - Umožňuje okamžitú reakciu (automatická prevencia)
  - Spolupracuje s ďalšími bezpečnostnými technológiami (FW, NGFW)
- Nasadenie: inline
  - Inline nasadenie – všetka prevádzka prechádza cez IPS
- **Výhody**
  - Okamžite zastaví známe aj niektoré neznáme útoky – Zero Day
  - Znižuje riziko kompromitácie serverov a služieb
  - Často sa integruje do NGFW ako IPS modul
- **Nevýhody**
  - Môže znižovať výkon siete (latencia)
  - Pri nesprávnej konfigurácii → false positives a blokovanie legitímnej prevádzky



Bezpečnostné zariadenia (aplikačné): Web proxy / WSA

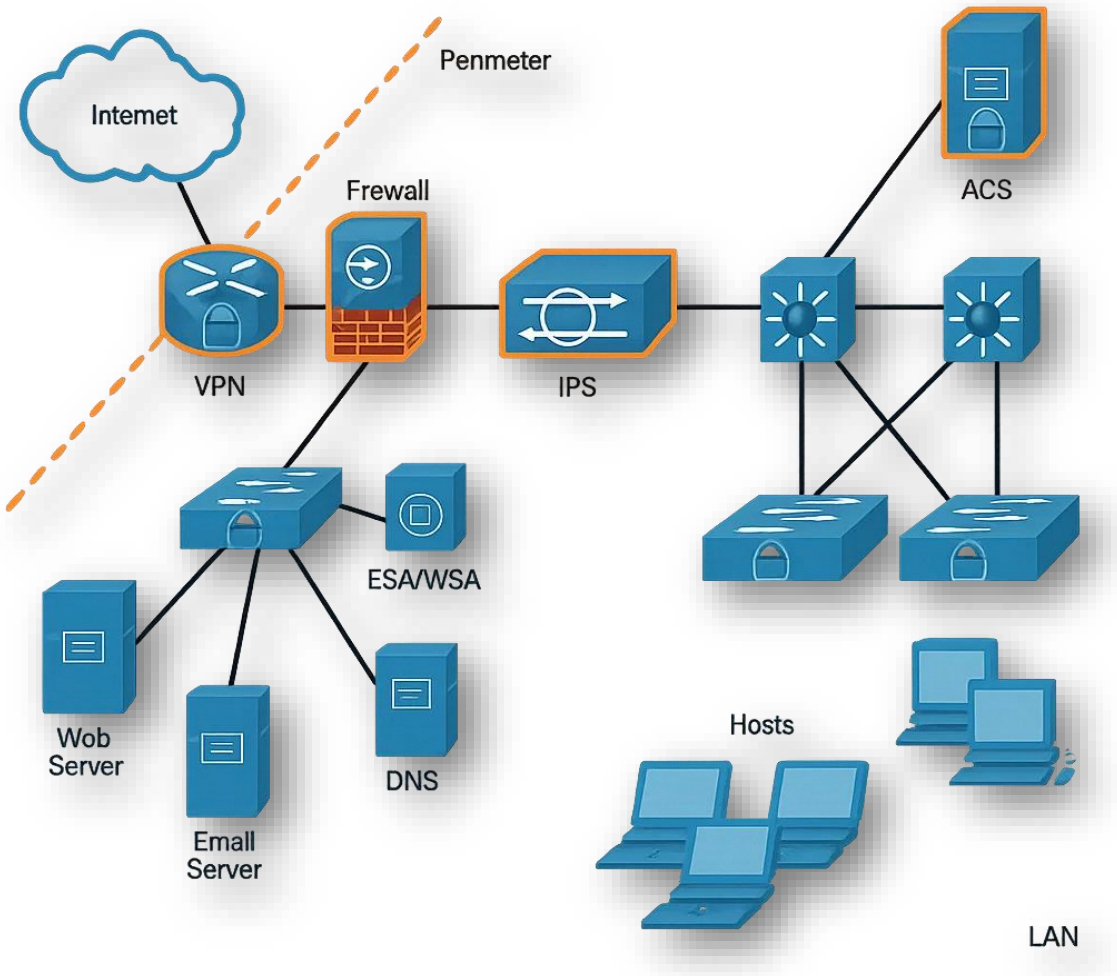
- **Web Proxy/WSA (Web Security Appliance)**
  - Kategória aplikačná kontrola
  - Filtruje a kontroluje HTTP/HTTPS premávku
  - Chráni pred webovými hrozbami a riadi prístup používateľov
- **Kľúčové funkcie:**
  - **Filtrácia obsahu / URL filtering:** Blokuje škodlivé stránky (malware, phishing)
    - **Príklad:** Zablokuje prístup na podozrivé URL
  - **Autentifikácia a politika:** Obmedzuje prístup podľa rolí (napr. zamestnanci vs. hostia)
    - **Príklad:** Povolí iba podnikovú schválené stránky
  - **SSL inšpekcia:** Analyzuje šifrovanú prevádzku (HTTPS)
    - **Príklad:** Detekcia skrytého malvéru v šifrovanej komunikácii
  - **Reportovanie:** Monitoruje webové aktivity pre audit
    - **Príklad:** Zaznamená pokusy o prístup na neautorizované stránky
  - **DLP (Data Loss Prevention):** prevencia pred únikom dát cez web
  - **Sandboxing:** testovanie súborov v izolovanom prostredí pred sprístupnením

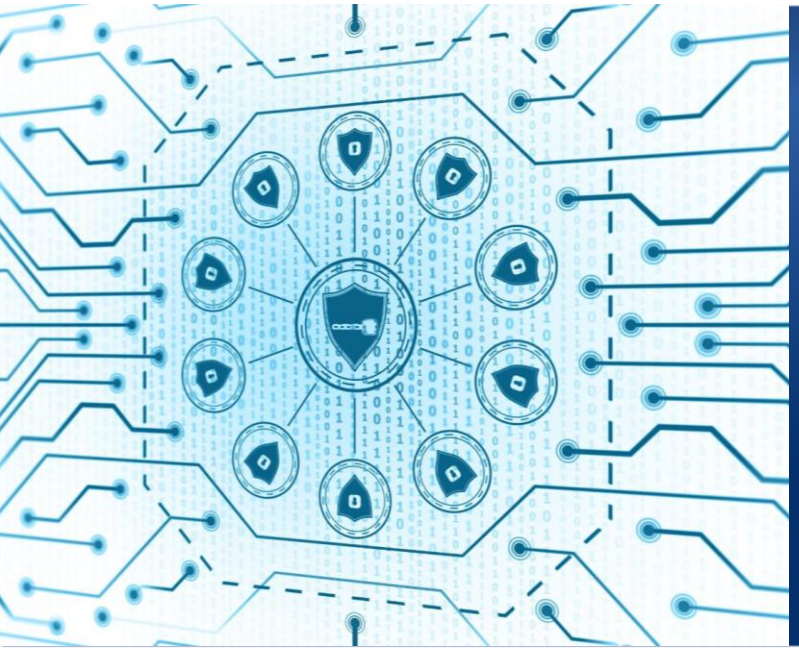
- **Dopady v enterprise:**
  - Znižuje riziko malvéru a phishingu cez web.
  - Zabezpečuje súlad s bezpečnostnými politikami
  - Web Proxy/WSA je ochranná vrstva pre L7
    - Chráni používateľov a služby pred webovými hrozbami



Rekapitulácia základných pojmov a zariadení

- **Základné koncepty:**
  - **Perimeter** – hranica medzi internou a externou sieťou
  - **Trust zones** – úrovne dôveryhodnosti (LAN, DMZ, Internet, Cloud)
  - **Segmentácia** – oddelenie sietí pre obmedzenie rizík
- **Zariadenia a ich úloha:**
  - **Router** – ACL, NAT, routing filters → prvá línia ochrany
  - **Switch** – port security, STP guard, DHCP snooping → ochrana prístupovej vrstvy
  - **Firewall** – filtrácia paketov, stavová inšpekcia, NGFW → základ perimeter security
  - **IDS** – pasívna detekcia, monitoring, alerty
  - **IPS** – inline prevencia, blokovanie útokov v reálnom čase
  - **Proxy/WSA** – filtrácia webovej komunikácie, URL filtering, sandboxing





Blok 2 – Plánovanie, rámce, architektúra

Prečo potrebujeme plánovať bezpečnostnú architektúru

- Ad-hoc riešenia → chaos
  - Slabá odolnosť, ťažšia správa, vyššie riziko incidentov
  - Príklad: WannaCry 2017 – nesegmentovaná sieť viedla k globálnemu výpadku
- Systematický dizajn → konzistentnosť
  - Predvídateľnosť správania / reakcie na útok
  - Auditovateľnosť pre regulácie (NIS2)
  - Jednoduchšia správa siete
- Plánovanie = základ pre:
  - **Bezpečnosť** – minimalizácia rizík (napr. segmentácia proti šíreniu)
  - **Škálovateľnosť** – pripravenosť na rast, rozšírenie
  - **Spoľahlivosť siete** – stabilná prevádzka, stabilita služieb
  - Inak len reaktívne hasenie incidentov
- Frameworky a metodiky pomáhajú
  - Určiť priority
  - Zjednotiť prístup (NIST CSF, SABSA, TOGAF)

Architektúry sieťovej bezpečnosti ako stavebný princíp

- Architektúra ≠ produkt
  - Systematický princíp budovania bezpečnosti a plán
    - Nejde o konkrétne zariadenie (napr. firewall, IDS), ale o **koncept, plán a princípy**
    - Určuje ***čo, kde a ako***
  - Výsledok ➔ Konzistentný a odolný dizajn siete namiesto ad-hoc riešení
- **Tradičné architektúry (modely) sieťovej bezpečnosti**
  - Perimeter-based security
  - Defense in Depth (Viacvrstvová obrana)
- **Moderné architektúry (modely)**
  - Zero Trust Architecture (ZTA)
  - SASE (Secure Access Service Edge)
  - Iné
    - Cyber Resiliency / Adaptive Security, SAFE ...
- Viac v Bloku III: detailné princípy (Defense in Depth, Zero Trust)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Top-down vs. bottom-up prístup k implementácií

Top-down (zhora nadol)

- Vychádza z biznis požiadaviek, procesov a regulácií
- Strategický a systematický prístup
  - Od cieľov po technológie
    - Biznis ciele → analýza aktív → analýza rizík → návrh bezpečnostných zón a politík → výber technológií
- Výhody
  - Zhoda s podnikovými prioritami, komplexný pohľad
  - Konzistentnosť naprieč celou organizáciou
- Nevýhody
  - Časovo náročné, vyžaduje manažérsku podporu

Bottom-up (zdola nahor)

- Iniciované technickými tímami (admins)
  - Začína od **konkrétnych technických riešení** (FW, IDS, ACL)
  - Postupne sa ad-hoc rozširuje
- Reaktívny prístup v praxi
  - Incident → kúpa technológie
    - Orientované na rýchle riešenia („kúpme firewall, lebo bol incident“)
- Výhody
  - Rýchla implementácia, technická presnosť
- Nevýhody
  - Riziko nesúladu s biznis potrebami, riziko nekonzistencie a slabých miest

Best practice => kombinácia

- **Top-Down**: strategické projekty, enterprise architektúra, compliance
- **Bottom-Up**: rýchle reakcie na incidenty, pilotné projekty.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Risk-based prístup – hodnotenie rizík

- **Rizikovo-orientovaný prístup** = základ plánovania bezpečnostnej architektúry
  - Top-down či bottom-up – v oboch prípadoch potrebujeme systematicky hodnotiť riziká
    - => **to určí priority**
- Kľúčové kroky hodnotenia rizík
  - **Identifikácia aktív** (asset inventory)
    - Čo chránime?
      - Dáta, systémy, služby, servery
  - **Identifikácia hrozieb a zraniteľností**
    - Čo ich ohrozuje? (phishing, misconfig).
  - **Odhad pravdepodobnosti a dopadu** (risk matrix)
    - Aké je riziko?
    - Riziko = dopad × pravdepodobnosť
  - **Prioritizácia rizík** (high impact/high likelihood)
    - Podľa rizika a biznis dopadov
  - **Mitigácia - výber a implementácia kontrol**
    - Ako znížiť riziko?
      - FW, IDS/IPS, segmentácia, zálohy
  - **Kontinuálne monitorovanie a revízia**
- **Výhody**
  - Efektívne využitie zdrojov
    - Fokus na najväčšie hrozby
  - Prispôsobenie sa špecifickým potrebám
    - Napr. úradov, školám
  - Lepšia komunikácia s manažmentom
  - Podpora súladu (ISO 27001, NIST CSF)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kľúčové pojmy a ich rola

Kategória	Príklady	Úloha v plánovaní
Metodiky	Top-down, Bottom-up	Spôsob implementácie. Ako implementujeme bezpečnostné opatrenia.
Prístupy	Risk-based approach	Ako rozhodujeme, čo má prioritu. Logika rozhodovania.
Frameworky	NIST CSF, ISO/IEC 27001, SABSA, TOGAF	Čo pokrývame a ako meriame pokrok. Štruktúra a kontrolný zoznam.
Architektúry	Zero Trust, SASE, Defense-in-Depth	Aký cieľový stav chceme dosiahnuť. Výsledok celého procesu.

- Implentácia bezpečnosti
  - [Risk-based approach]
    ↓ (dáva logiku rozhodovania – čo riešiť skôr)
  - [Framework (NIST CSF, ISO, SABSA)]
    ↓ (dáva štruktúru a jazyk – čo pokrývať a merať)
  - [Metodika (Top-down / Bottom-up)]
    ↓ (určuje implementačný spôsob – ako uviesť do praxe)
  - [Architektúra (Zero Trust, DiD, SASE)]
    ↓ (cieľový stav – výsledná podoba siete)

Frameworky pre riadenie rizík a bezpečnostnej architektúry

- Frameworky = **štruktúrované metodiky** pre plánovanie a riadenie bezpečnosti
  - Poskytujú systematický prístup k ochrane sietí a dát
  - Menia **risk-based prístup** na konkrétne systémové kroky
  - Prekladajú riziká do akčných plánov
- Zabezpečujú
  - Konzistentnosť
  - Auditovateľnosť
  - Súlad (compliance)
- Príklady rámcov:
  - **NIST CSF** – riadenie rizík, 5 funkcií
  - **ISO/IEC 27001** – normatívny systém riadenia ISMS
  - **CIS Controls v8** – praktické technické opatrenia
  - **TOGAF** (**SABSA?**) – väzba bezpečnosti na biznis architektúru

Ovplyvňujú riešenie sieťovej bezpečnosti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

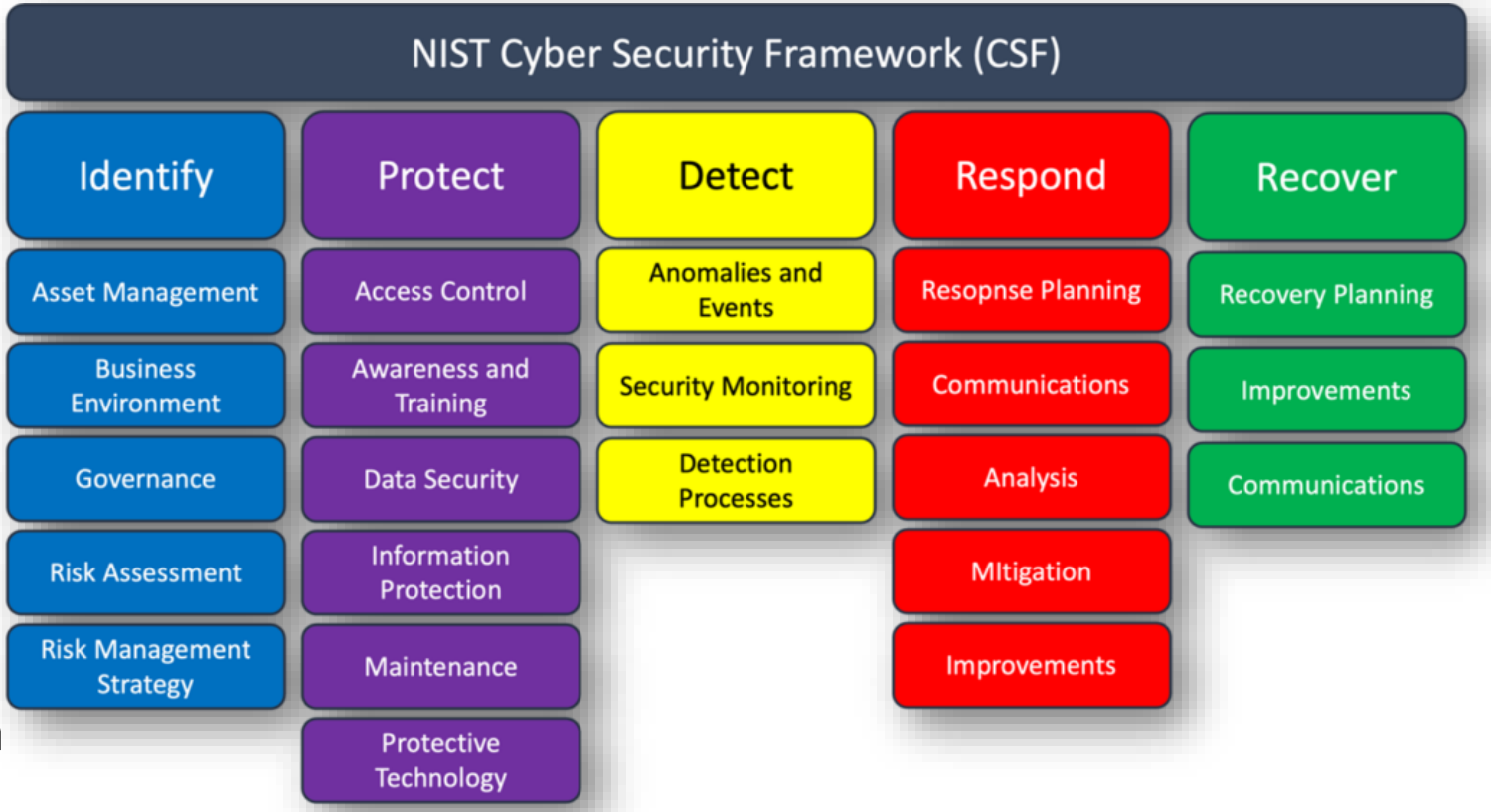
Framework – NIST CSF - Základ proaktívnej bezpečnostnej architektúry

- **NIST C**ybersecurity **F**ramework **(CSF) =** medzinárodne uznávaný rámec/metodika na riadenie **kyber rizík**
  - Vyvinutý americkým National Institute of Standards and Technology
  - Reakcia na potrebu **systematického riadenia kybernetickej bezpečnosti**
- **Prečo je vhodný?**
  - **Flexibilita:** Prispôsobiteľný pre SOHO, enterprise aj úradné siete
  - Súlad s legislatívou (**Compliance):** Podpora NIS2, GDPR, ISO 27001
  - **Praktickosť:** Jednoduché 5 krokov – Identify, Protect, Detect, Respond, Recover
- **Výhody NIST CSF**
  - Nezávislý od technológie → *čo dosiahnuť*, nie *aký produkt kúpiť*
  - Konzistentnosť → jednotný jazyk pre IT, bezpečnosť a manažment
  - Kompatibilný s inými normami (napr. ISO/IEC 27001) – dopĺňa, kombinuje
  - Univerzálny - vhodný pre malé aj veľké organizácie (vyberiem čo je vhodné)
  - Podporuje neustále zlepšovanie bezpečnosti - Cyklický prístup (plan → implement → review → improve)
  - Prepája **technické opatrenia s biznis cieľmi**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

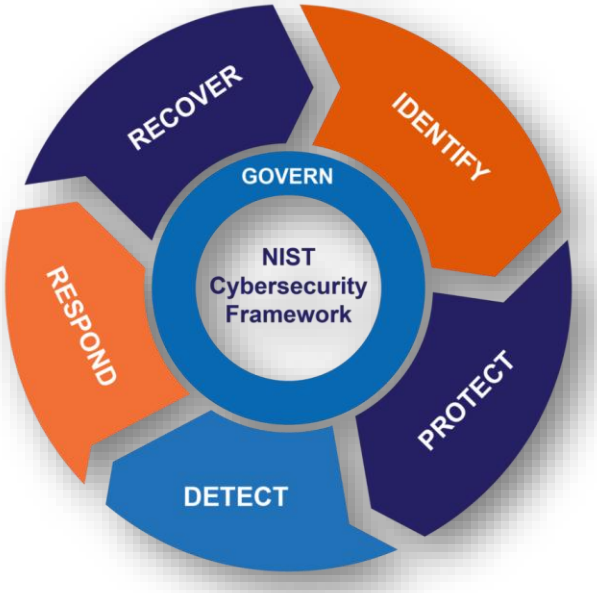
NIST CSF: Kroky

- **Identify (Identifikovať)**
  - Porozumenie rizikám, aktívam, dátam, systémom a procesom
  - Inventarizácia HW/SW, zodpovednosti, risk register
- **Protect (Chrániť)**
  - Implementácia bezpečnostných opatrení na ochranu kritických služieb
  - IAM, segmentácia, firewally, hardening, školenia
- **Detect (Detekovať)**
  - Včasné odhalenie kybernetických incidentov
  - IDS/IPS, SIEM, monitoring, XDR
- **Respond (Reagovať)**
  - Reakcia na incidenty a minimalizácia ich dopadu
- **Recover (Obnoviť)**
  - Obnovenie služieb po incidente a zlepšenie odolnosti
  - BCP, DRP, redundancia, zálohy, lessons learned



NIST CSF: Identify (Identifikovať)

- Identifikácia a porozumenie aktív, rizík, dát, systémov a procesov v sieti
- Základ pre ďalšie kroky plánovania
  - Kľúčová fáza
- **Cieľ:** poznať **aktíva, systémy, ľudí, dáta a procesy**, ktoré treba chrániť
- Obsahuje/pokrýva
  - Asset Management – inventarizácia HW, SW, dát, služieb
  - Business Environment – úloha aktív v biznis procesoch
  - Governance – pravidlá, politiky, zodpovednosti
  - Risk Assessment – analýza hrozieb, zraniteľností, dopadov
  - Risk Management Strategy – definovanie prahov rizík, tolerancie
  - **Súčasť** ➔ Definovanie Trust Zones
    - Definícia zón (LAN, DMZ, Cloud) a ich ochrany



- Identifikovať prepojenie aktív s biznis procesmi
- Príklad
  - Univerzita → kritické aktíva = študijný informačný systém, e-mail, sieťová infraštruktúra
  - pre biznis (vzdelávanie) sú kľúčové → musia byť v prvej línii ochrany

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Identify (Identifikovať)

NIST CSF: Protect (Chrániť)

- Implementácia bezpečnostných opatrení na ochranu kritických služieb
- Obsahuje **technické aj organizačné opatrenia**
- **Cieľ:** znížiť dopad incidentu
- Kategórie:
  - Access Control (IAM, MFA, least privilege)
  - Awareness & Training – používatelia ako prvá línia obrany
  - Data Security – šifrovanie, DLP, zálohovanie
  - Information Protection Processes & Procedures – politiky, hardening
  - Maintenance – pravidelné aktualizácie a správa zariadení
  - Protective Technology – FW, segmentácia, IDS/IPS, EDR

- Fokus na prevenciu útokov
  - Firewall (FW)
    - Filtrácia prenosu (napr. blokovanie neautorizovaného prístupu)
  - Segmentácia
    - Rozdelenie siete na zóny (VLAN, DMZ).
      - Príklad: Izolácia databáz od verejného prístupu
  - Identity and Access Management (IAM)
    - Kontrola prístupu (napr. MFA pre admins)
  - Hardening
    - Posilnenie zariadení (napr. vypnutie nepotrebných služieb)

NIST CSF: Respond (Reagovať)

- **Cieľ**: zvládnuť incident a minimalizovať škody
- Zameranie:
  - **Incident Response Planning** – pripravený plán reakcie
  - **Communications** – jasné oznamovanie (interné + externé)
  - **Analysis** – hodnotenie dopadu, koreňová príčina
  - **Mitigation** – okamžité opatrenia na zastavenie útoku
  - **Improvements** – lessons learned, aktualizácia procesov
- Typické kroky reakcie:
  - **Detekcia a potvrdenie incidentu** (alert z IDS/SIEM, hlásenie používateľa)
  - **Obsiahnutie (containment)** – izolácia napadnutého segmentu alebo zariadenia
  - **Eradikácia** – odstránenie malvéru, zatvorenie zraniteľnosti
  - **Obnova služby** – návrat systémov do prevádzky
  - **Lessons learned** – vyhodnotenie, čo zlyhalo a čo zlepšiť
- Technológie a nástroje:
  - **SOAR** (Security Orchestration, Automation and Response) – automatizácia reakcií
  - **Playbooks** – vopred pripravené postupy pre typické incidenty (napr. phishing, ransomware)
  - **Forenzné nástroje** – analýza logov, zachytenie dôkazov
  - **Komunikačné kanály** – interné (SOC → IT → manažment), externé (CERT, regulátori, zákazníci)
- Prínosy Respond fázy:
  - **Minimalizácia dopadu** incidentu na biznis (skrátenie „dwell time“)
  - **Zachovanie dôvery** zákazníkov a partnerov
  - **Pripravenosť na regulácie** (NIS2, GDPR – povinnosť ohlásiť incident do 72 hodín)
  - Zlepšovanie bezpečnostnej architektúry po každom incidente

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

NIST CSF: Recover (Obnoviť)

- **Cieľ**: obnovenie systémov a služieb po incidente
- Zameranie:
  - Recovery Planning – pripravené plány obnovy služieb
  - Improvements – poučenie sa z incidentov, úprava procesov
  - Communications – informovanie zákazníkov, partnerov, regulátorov
- Kľúčové procesy:
  - Business Continuity (BCP) – zachovanie kritických procesov počas incidentu
  - Disaster Recovery (DRP) – obnova systémov po havárii alebo útoku
  - Redundancia a HA – záložné linky, servery, datacentrá
  - Zálohovanie a obnova dát – 3-2-1 princíp (3 kópie, 2 médiá, 1 offsite)
  - Testovanie plánov – pravidelné cvičenia obnovy, tabletop exercises
- Výhody fázy Recover:
  - Minimalizuje čas výpadku (downtime) a finančné straty
  - Posilňuje dôveru klientov - transparentná komunikácia po incidente
  - Zabezpečuje compliance (NIS2, ISO 22301 – Business Continuity Management)
  - Umožňuje zlepšiť architektúru – každý incident = príležitosť na zvýšenie odolnosti
- Príklady opatrení:
  - Geo-redundantné cloud riešenia (Azure, AWS – multi-region)
  - Automatizovaná obnova konfigurácií (network device backup, AutoSecure baseline)
  - Incident report → update bezpečnostných politík a architektúry

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prepojenie frameworku s bezpečnostnou architektúrou

- **NIST CSF ≠ bezpečnostná architektúra**
  - **NIST CSF je rámec -** podporuje systematické riadenie kybernetickej bezpečnosti
  - **Bezpečnostná architektúra** - technický návrh **ako sa bezpečnosť implementuje**
    - Siete, segmentácia, firewall, IAM, monitoring atď.

Funkcia CSF	Výstupy (framework)	Opatrenia a dopad na sieťovú architektúru
Identify	Asset inventory, klasifikácia dát, risk register	Segmentácia siete (LAN, DMZ, Cloud), definovanie trust zones, firewall politiky, požiadavky na HA, výber technológií
Protect	Prístupové politiky, hardening, šifrovanie	IAM/AAA (802.1X, NAC), VPN, firewall ACL, port security, hardening, endpoint hardening and protection, DLP
Detect	Monitoring, logovanie, detekcia anomálií	IDS/IPS senzory, NetFlow/sFlow, TAP/SPAN porty, ACL s logovaním
Respond	Incident response plán, containment	Karanténne VLAN, dynamické ACL/FW pravidlá, izolácia segmentov, sinkhole DNS
Recover	Plán obnovy služieb, lessons learned	Zálohy konfigurácií, redundancia (HA firewally, HSRP/VRRP), záložné linky, cloud failover

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Blok III. – Princípy, modely a sieťové bezpečnostné architektúry

- Základné bezpečnostné princípy
- Architektonické modely (HMS, perimeter)
- Moderný dizajn (DiD, ZTA, ZTNA, SASE)

Princípy sieťovej bezpečnosti - prehľad

- Architektonické princípy
  - Pravidlá a zásady pre návrh bezpečnej siete
  - => základ dizajnu
- Princípy
  - Premosťujú frameworky (napr. NIST CSF) do technických rozhodnutí
  - Zaisťujú konzistentnosť, odolnosť, škálovateľnosť, auditovateľnosť
  - Umožňujú predvídateľné reakcie siete na incidenty (izolácia, fallback vrstvy)
  - Zabraňujú ad-hoc riešeniam a chybám

- **Od klasiky k moderným princípom**
  - **Klasické princípy - ciele sieťovej bezpečnosti**
    - CIA Triáda:
      - Confidentiality (Dôvernosť), Integrity (Integrita), Availability (Dostupnosť)
      - + Authenticity, Accountability, Privacy, Resilience
  - **Tradičné princípy - riadenie prístupu – ako rozhodujeme o prístupe**
    - Authentication (Autentifikácia), Authorization (Autorizácia)
    - Modely: RBAC, DAC, MAC, ABAC/PBAC (atribúty/politiky

Moderné princípy sieťovej bezpečnosti

- **Architektonické princípy (ako sieť navrhujeme)**
  - Least Privilege (LP) – iba nevyhnutné oprávnenia
  - Segmentation & Isolation (SEG) – rozdelenie na zóny
  - Zero Trust (ZT) – „Never trust, always verify“
  - Defense-in-Depth (DiD) – vrstvená ochrana
- **Dizajnové a prevádzkové zásady (ako bezpečne prevádzkujeme)**
  - Fail-Safe Defaults (FSD) – implicitné deny
  - Accountability & Auditing (ACC) – logovanie a audit
  - Separation of Duties (SoD) – rozdelenie kompetencií

Princípy - CIA triáda v bezpečnosti sietí

- **Confidentiality (Dôvernosť)**
  - Ochrana pred neoprávneným prístupom k dátam v IP sieťach
  - Príklady
    - Šifrovanie (TLS, IPsec, VPN), Autentifikácia (MFA, 802.1X), prístupové politiky (ACL, firewall pravidlá) a riadenie prístupu
- **Integrity (Integrita)**
  - Zabezpečenie, že dáta v sieťovom prenose nie sú neoprávnene zmenené
  - Príklady
    - Hashovanie (SHA-256 na kontrolu dát), digitálne podpisy (overenie zdroja), kontrolné súčty (detekcia chýb v paketoch).
- **Availability (Dostupnosť)**
  - Zabezpečenie funkčnosti sietí a služieb, keď sú potrebné
  - Príklady
    - Redundancia (viacnásobné linky, HA zariadenia), DDoS ochrana (rate limiting, cloud scrubbing), zálohovanie (siete, konfigurácie, dáta)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Princípy - CIA triáda - Rozšírené atribúty

- **Authenticity (Autentickosť)**
  - Overenie identity zdroja dát alebo používateľa.
  - **Príklad:** Digitálne certifikáty, protokoly ako 802.1X a NAC
- **Resilience (Odolnosť)**
  - Schopnosť siete / systému prežiť incident/udalosť a pokračovať v činnosti
  - Príklady: redundancia, failover, rýchla obnova
- **Accountability (Zodpovednosť)**
  - Sledovanie a auditovanie sieťových aktivít
  - Možnosť vystopovať, kto čo vykonal
  - Príklad: SIEM systémy, syslog pre analýzu incidentov

Moderné princípy sieťovej bezpečnosti (1.)

- **LP – Least Privilege**
  - Povoľ iba minimálne nutné oprávnenia, blokuj nepotrebné
  - Príklad v sieti: **inter-VLAN default deny**, **ACL whitelist**, **egress** filtre (napr. 445/135/25), oddelený mgmt
  - **Anti-vzor:** permit ip any any, zdieľané admin účty
- **SEG - Segmentation & Isolation** – zóny
  - Delenie do zón/mikrosegmentov s riadenými prechodmi (east-west kontrola), izoluj kritické časti
  - **Príklad v sieti:** VLAN/VRF, DMZ, ISFW/NGFW medzi zónami, SDN mikrosegmentácia (napr. tagy/SGT)
  - **Anti-vzor:** „Flat“ sieť, trunking všade, shared VLAN pre všetko
- **DiD – Defense-in-Depth -** viac vrstiev ochrany
  - Viacvrstvová obrana; ak jedna vrstva zlyhá, ďalšia zachytí nezávislé, komplementárne kontroly
  - **Príklady v sieti:** Perimeter FW → interný FW/ACL → IDS/IPS (east-west) → mikrosegmentácia → EDR/HIPS → zálohy/DR
  - **Anti-vzor:** Spoliehať sa na „jednu krabicu“ (NGFW) v jedinom chokepointe
- **ZT – Zero Trust -** „Never trust, always verify“
  - Žiadna implicitná dôvera; priebežné overovanie identity, zariadenia a kontextu pri každom prístupe
  - Rozšírenie konceptu zón a z perimetra na jednu identitu a plošne
  - **Príklad v sieti:** 802.1X/NAC na vstupe, ZTNA, prístup, identity-based FW; dynamická VLAN
  - **Anti-vzor:** „VPN = dôvera všade“ (full-tunnel bez ďalšej verifikácie)
- *Pozn. Tieto dve sú aj modelom či architektúrou, nielen princípom*

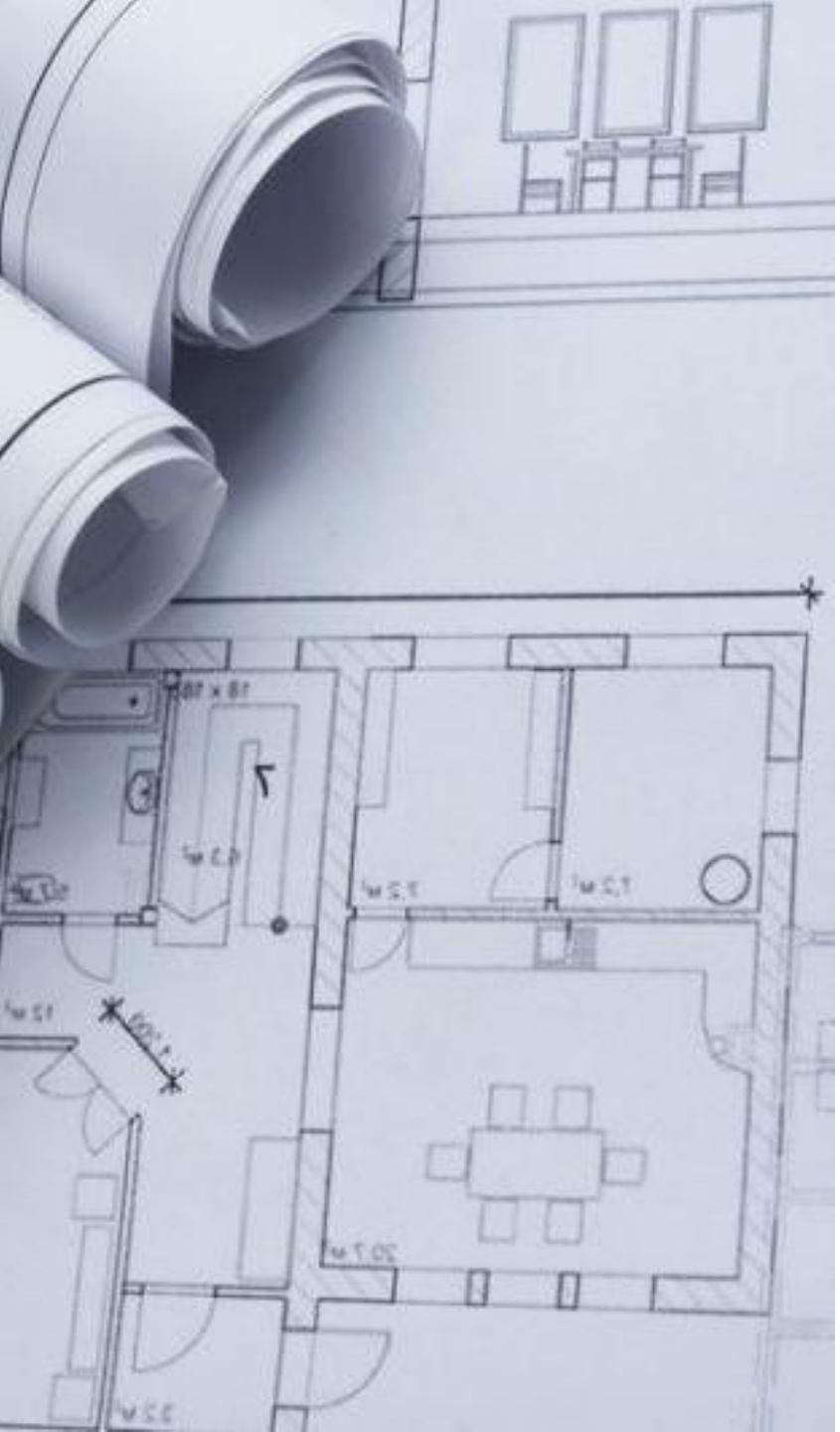
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Moderné princípy sieťovej bezpečnosti (2.)

- **FSD - Fail-Safe Defaults** – handling chybových stavov
  - Bezpečný default = deny (implicitné odmietnutie); povoľuj len výnimky (whitelist)
  - **Príklad v sieti:** FW implicit deny all, inter-VLAN deny, egress filter
  - **Anti-vzor:** „Dočasné“ výnimky bez expirácie; „allow all outbound“
- **ACC – Accountability & Auditing (or TbV – Trust but verify) -** logovanie, korelácia
  - Dohľadateľnosť akcií a integrita logov
  - „**Trust but verify**“ – všetko musí byť podložené audit trailom
  - **Príklad v sieti:** Syslog+NetFlow+NTP, TACACS+/RADIUS accounting, SIEM korelácia, verzionovanie konfigurácií
  - **Anti-vzor:** Lokálne logy bez odoslania; zdieľané účty → neauditovateľné zmeny
- **SoD – Separation of Duties** – delenie úloh
  - Rozdelenie úloh na zníženie rizika zneužitia právomocí
  - Kritické úlohy nemá držať jedna rola
  - **Príklad v sieti:** tím routing ≠ tím FW policy; schvaľovanie zmien oddeleným tímom; oddelené mgmt domény;
  - **Anti-vzor:** „Jeden superadmin na všetko“

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné sieťové architektúry



Sieťové bezpečnostne architektúry

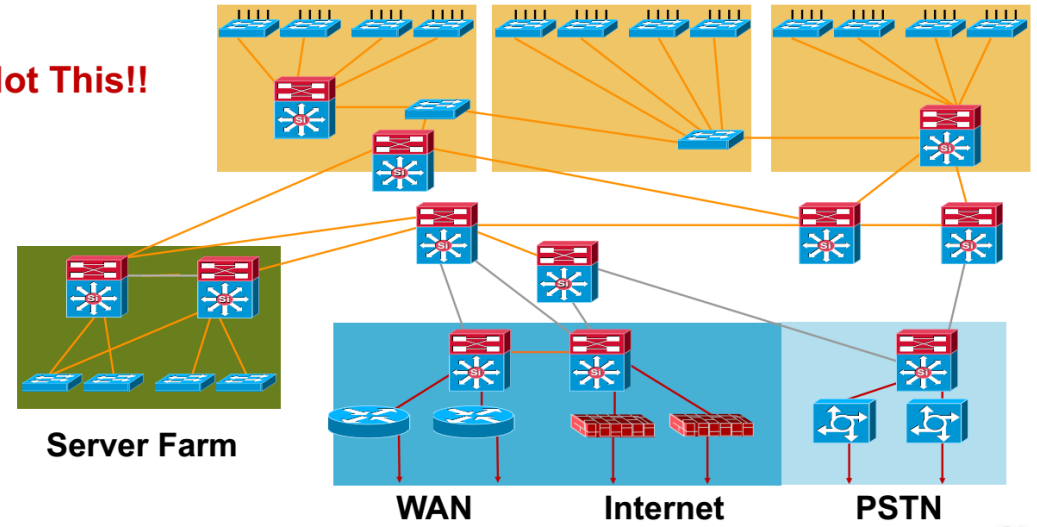
- Architektúra ≠ produkt
  - Plán a princíp budovania bezpečnosti
  - Nejde o konkrétne zariadenie (napr. firewall, IDS)

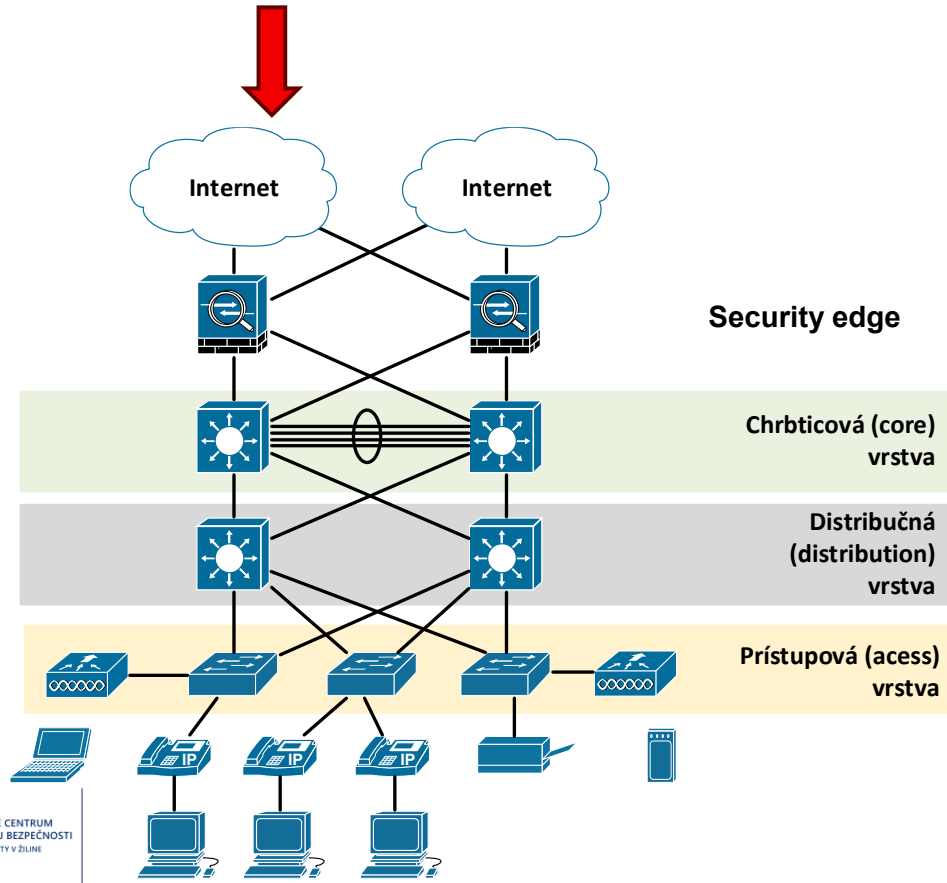
- **Architektúra sieťového dizajnu – security basement**
  - Hierarchická architektúra siete (Trojvrstvový model siete)
- **Tradičné architektúry sieťovej bezpečnosti**
  - Perimeter-based security
  - Defense in Depth (Viacvrstvová obrana)
- **Moderné prístupy**
  - Zero Trust Architecture (ZTA)
  - SASE (Secure Access Service Edge)
  - Cyber Resiliency / Adaptive Security
  - Iné (Cisco SAFE, ...)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hierarchický model siete (HMS)

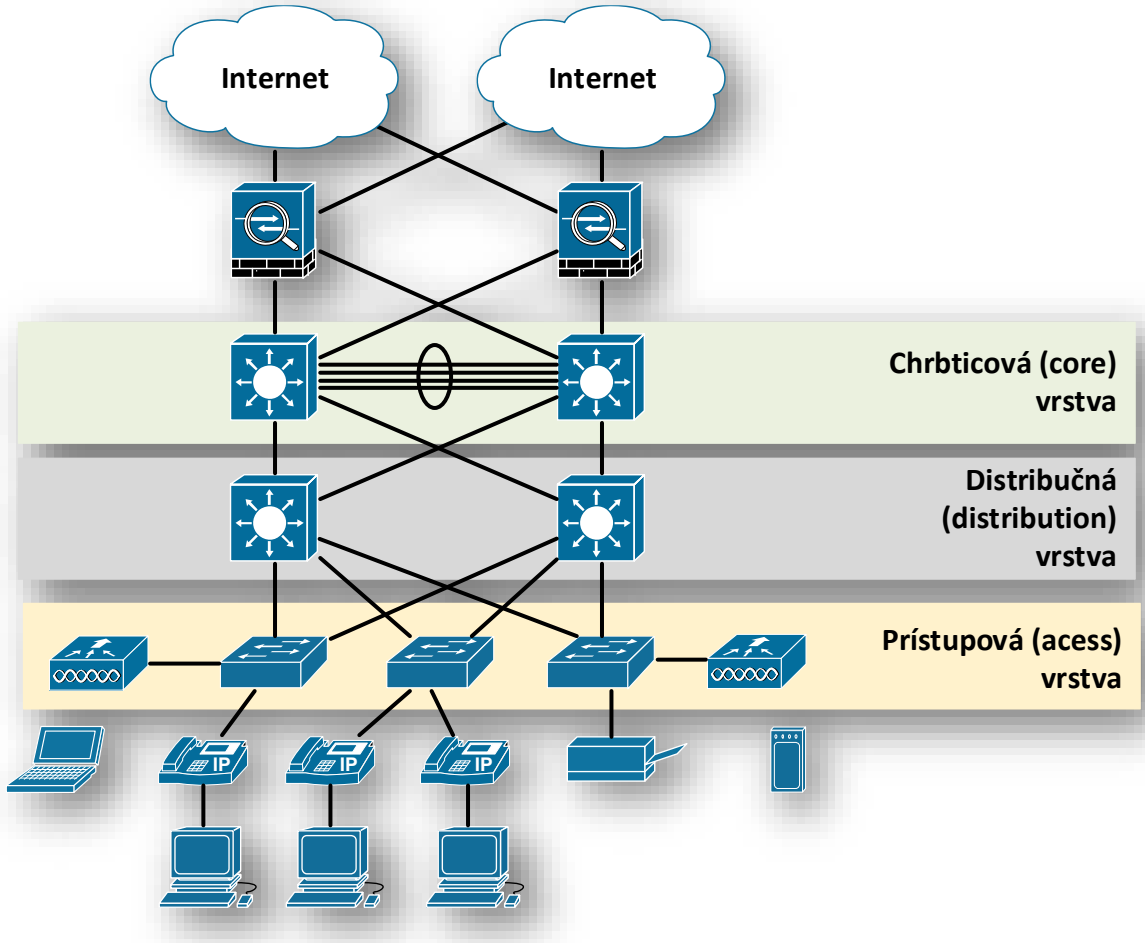
- Model
  - Základ pre enterprise siete a hybridné prostredia
  - Prechod od plochých k štruktúrovaným dizajnom
- Cieľ
  - Zvýšenie škálovateľnosti a správy
  - Oddelenie funkcií pre lepšiu kontrolu
- Výhody - prevádzka
  - Vyššia priepustnosť a lepšie riadenie prevádzky
  - Jednoduchšia údržba a troubleshootovanie
  - Vyššia odolnosť a spoľahlivosť
  - Škálovateľnosť a modularita
  - Ohraničuje veľkosť chybových domén segmentáciou
- Výhody - bezpečnosť
  - Jasné body, kde nasadiť bezpečnostné opatrenia
  - Lepšia segmentácia → granularity access control
  - Politiky presadzované v správnych bodoch siete
  - Rýchlejšia reakcia na incidenty – izolácia problému do konkrétnej vrstvy



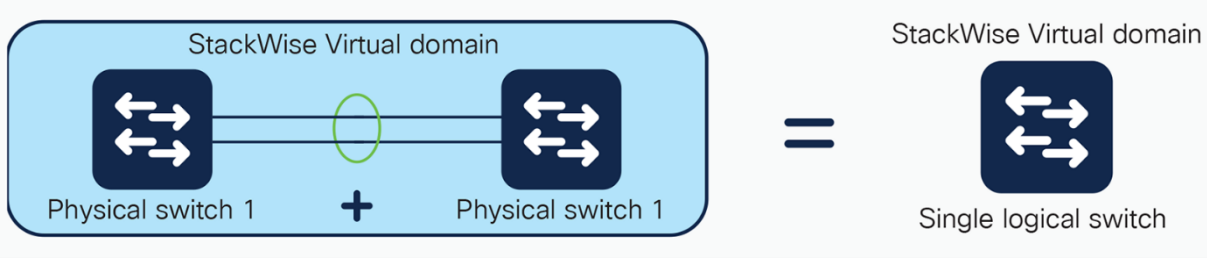


Hierarchický model siete (HMS)

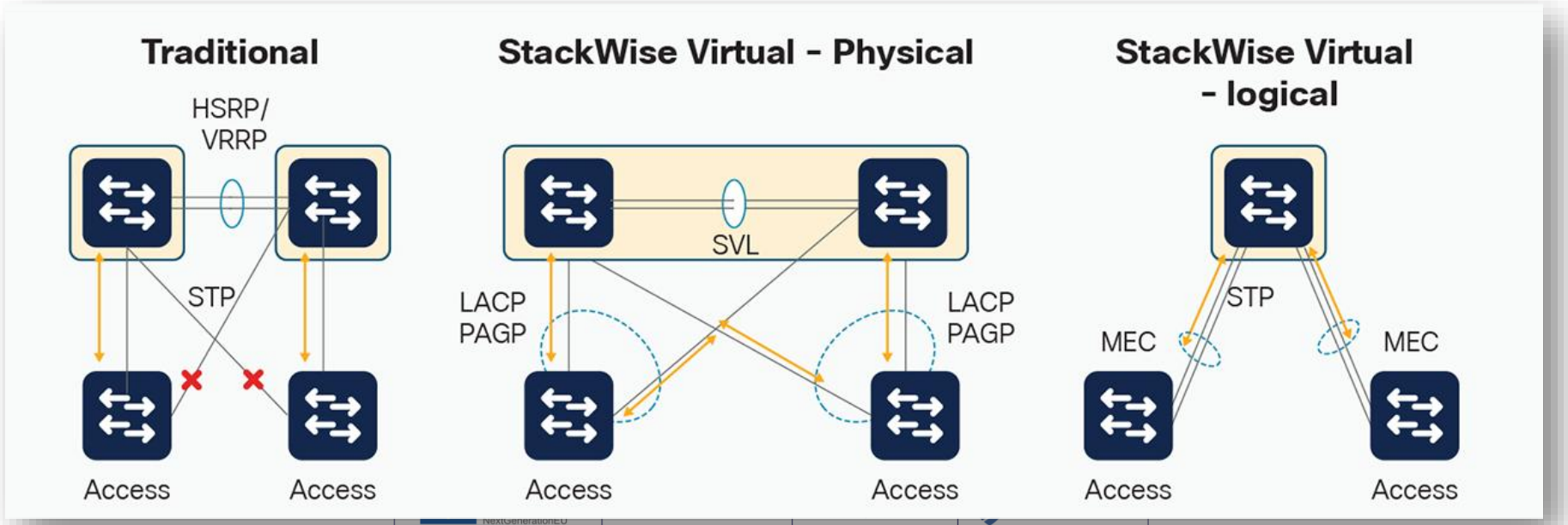
- Rozdeľuje sieť podľa funkcionality do troch vrstiev
- **Core**
  - Tvorí **vysokorýchlostnú** chrbticu siete
  - Musí zvládať spracovávať veľké objemy dát a veľmi rýchlo
  - Agreguje dáta od distribučných prepínačov
  - Musí byť **vysokodostupná** a **redundantná**
- **Distribution**
  - Agreguje dáta z prístupovej vrstvy
  - Optimalizuje smerovanie medzi nimi
  - Riadi tok dát (smerovacie a ACL politiky)
  - Musí byť vysokorýchlostná a redundantná
  - Segmentácia L2/L3
- **Access**
  - Poskytuje prostriedky na prístup do siete
  - Riadi kto môže komunikovať cez sieť
  - Segmentácia L2
  - Definuje bezpečnostnú hranicu



Trendy - StackWise prístup

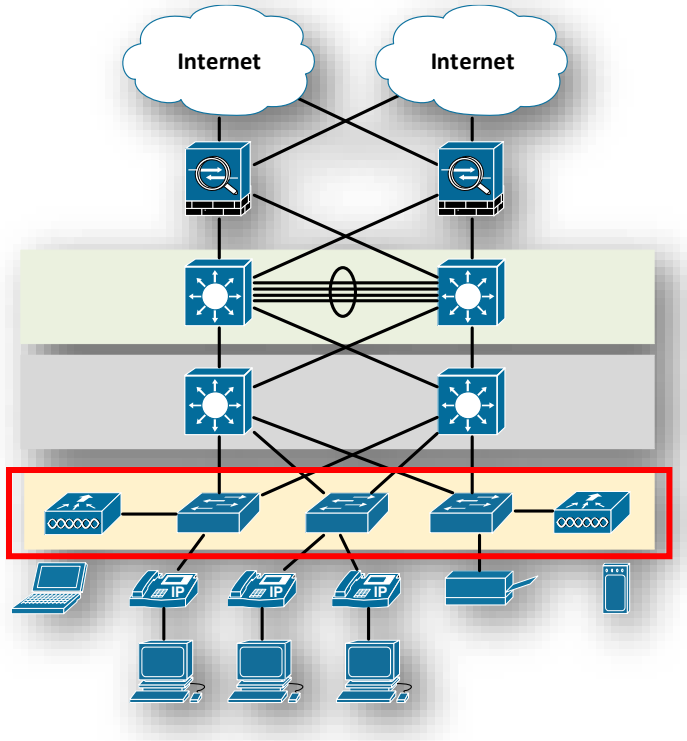


- Cisco StackWise Virtual Pair (SVP)
  - Viaceré fyzické prepínače sa javia a konfigurujú ako jeden
  - Stackwise je dátový aj napájací
  - Dopad na dizajn:



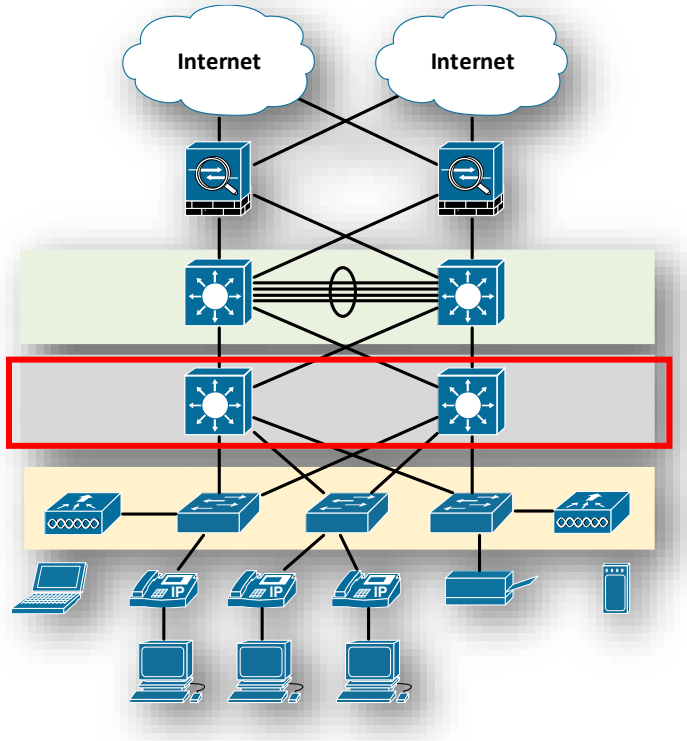
HMS vrstvy a ich bezpečnostná rola - access

- Hierarchický model = pevný základ bezpečnostnej architektúry
  - Jasné body pre riadenie prístupu, kontrolu a vynucovanie politík
- **Access Layer → detailná granularita**
  - Pripájanie autorizovaných koncových zariadení (PC, IoT, tlačiarne) + WiFi
  - **Bezpečnostný cieľ:** prvá línia obrany → First Hop Security
  - **Princípy**: Zero Trust/Never Trust, Least Privilege, Segmentation, NAC (802.1X), Accountability (telemetria/flow)...
  - **Opatrenia:** VLAN segmentácia, Guest/Quarantine VLAN, Private VLANs, Port Security, DHCP Snooping, ARP Inspection, IP soruce guard, BPDU Guard, MAC ACL...
  - **Hrozby & mitigácie (L2)**
    - MAC flooding → Port security; Rogue DHCP → DHCP Snooping/NAC; ARP spoofing → DAII; IP Spoofing → Source Guard; BYOD/IoT → segmentácia
  - **Prevádzka a správa**
    - „Deny by default“ medzi VLAN (inter-VLAN povolujeme až vyššie).
    - Logovanie 802.1X/porušení portov, baseline hardening (SSH, AAA, vypnúť nepoužité služby)



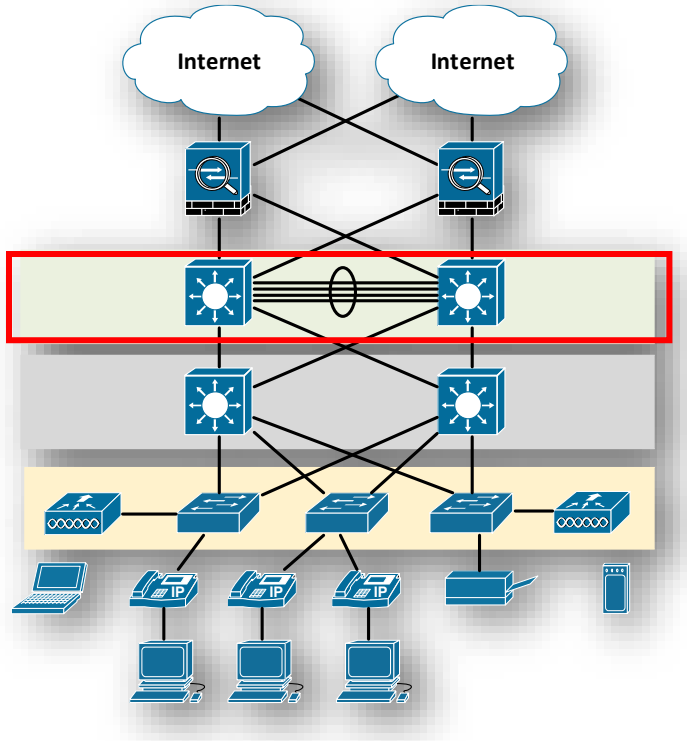
HMS vrstvy a ich bezpečnostná rola - distro

- **Distribution Layer – zóna politík a segmentácie**
  - Agregácia prevádzky, enforcement bod pre politiky
  - **Bezpečnostný cieľ:** segmentácia a kontrola tokov medzi zónami/oddeleniami
  - **Princípy:** Defense in Depth, Trust Zones, Segmentation & Isolation, Least Privilege, Accountability (telemetria/flow).
  - **Opatrenia**
    - Kontrola dátových tokov medzi segmentmi → Firewally (segmentačné), IDS/IPS, ACL, Route protection → uRPF, routing filters, QoS/Rate limiters
  - **HA & odolnosť**
    - Redundantné distribučné prvky, ECMP, FHRP (HSRP/VRRP/GLBP)
    - Jasné L3 hranice (SVI na distribúcii, nie v core)
  - **Monitorovanie**
    - Flow telemetry (NetFlow/sFlow), logovanie match-hit z ACL/FW



HMS vrstvy a ich bezpečnostná rola - core

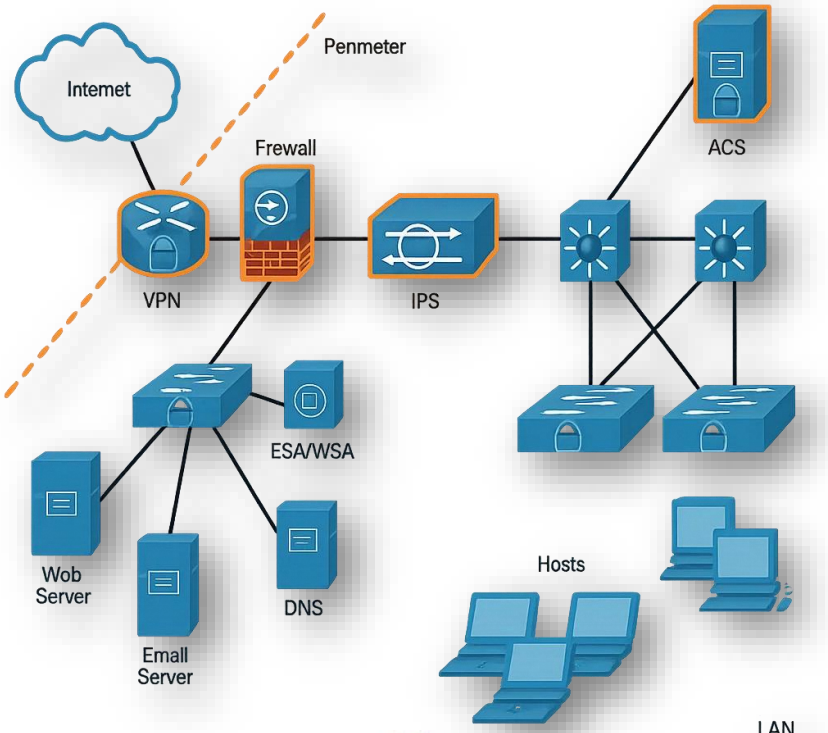
- **Core Layer – chrbtica siete** → rýchlosť a dostupnosť
  - Vysokorýchlostná, minimálna latencia, rýchla konvergencia
  - **Bezpečnostný cieľ:** dostupnosť a odolnosť
    - Ochrana infraštruktúry, nie aplikovanie detailných politík
  - **Princípy:** Availability, Resilience, DoS ochrana, Accountability (telemetria/flow)
  - **Opatrenia**
    - Redundancia (duálny core, link aggregation, rýchly failover)
    - Control-Plane Protection (CoPP/CPPr), iACL (infrastructure ACL) – chrániť samotné prvky
    - Autentifikácia routingu (OSPF/BGP keychain/TLS podľa možností), TTL-security, max-prefix
    - DDoS/DoS tlmenie na infra vrstvách (policers, rate-limits)
  - **Nepatria sem** L7 politiky – policy sa rieši v distribúcii alebo NGFW

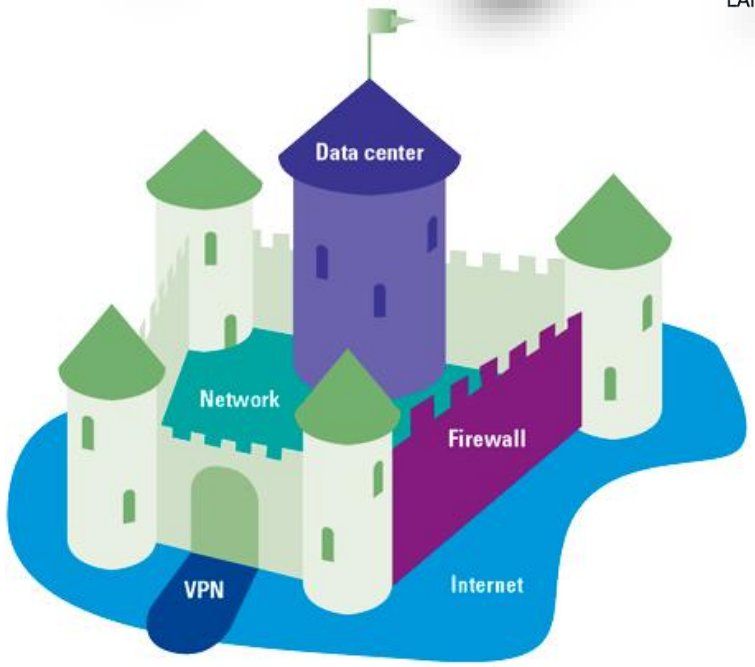


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Perimetrový model (Castle-and-Moat)

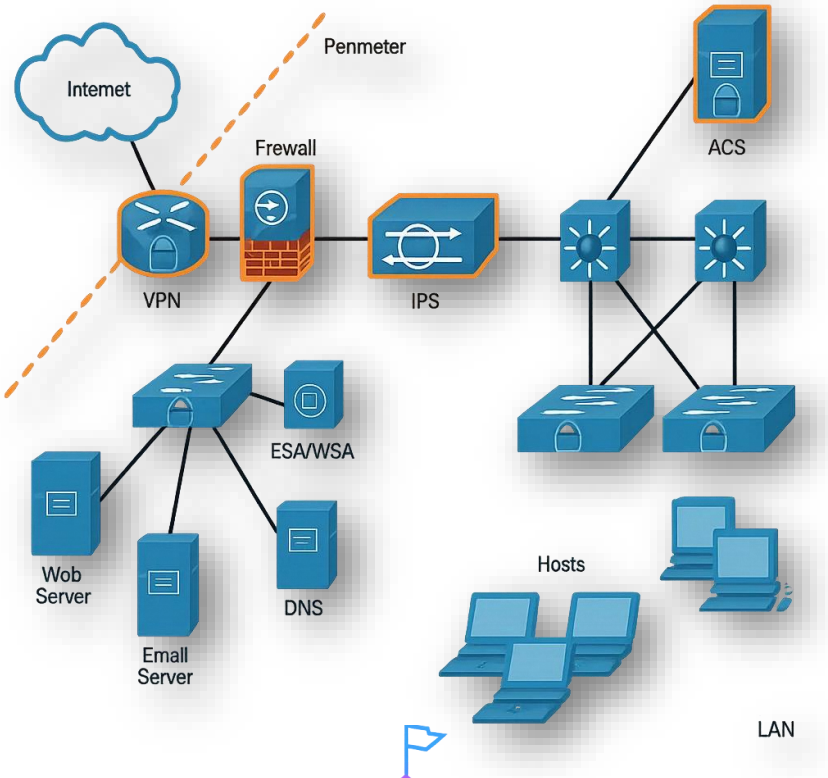
- **Dôvod vzniku**
  - Vnútro: uzavreté prostredie, dôveryhodné / „bezpečné“
  - Vonkajšok: nedôveryhodný
  - Perimeter: oddelenie dôveryhodné vs. nedôveryhodné
- Bezpečnostný cieľ = **Ochrániť hranicu** medzi nedôveryhodným a interným prostredím
- **Nástroje a opatrenia**
  - NGFW (L3–L7): aplikačná a obsahová kontrola, IPS integrácia, dešifrácia TLS podľa politiky
  - Anti-spoofing: uRPF, ingress ACL
  - DDoS ochrana: on-prem mitigation, cloud scrubbing služby,IDS/IPS: inline (prevencia) alebo one-arm (detekcia)
  - **Traffic Control:** pravidlá určujúce, čo smie dnu/von;
- **Politiky**
  - „deny by default“ - povoliť len publikované služby, **geofencing**, **rate limiting**, SSL/TLS inšpekcia podľa politiky, **explicitné povolenia** pre remote access / VPN.
- **Viditeľnosť / monitoring**
  - NetFlow/sFlow, FW/IPS logy → SIEM
- **DMZ** ako buffer: publikované služby oddeliť od LAN

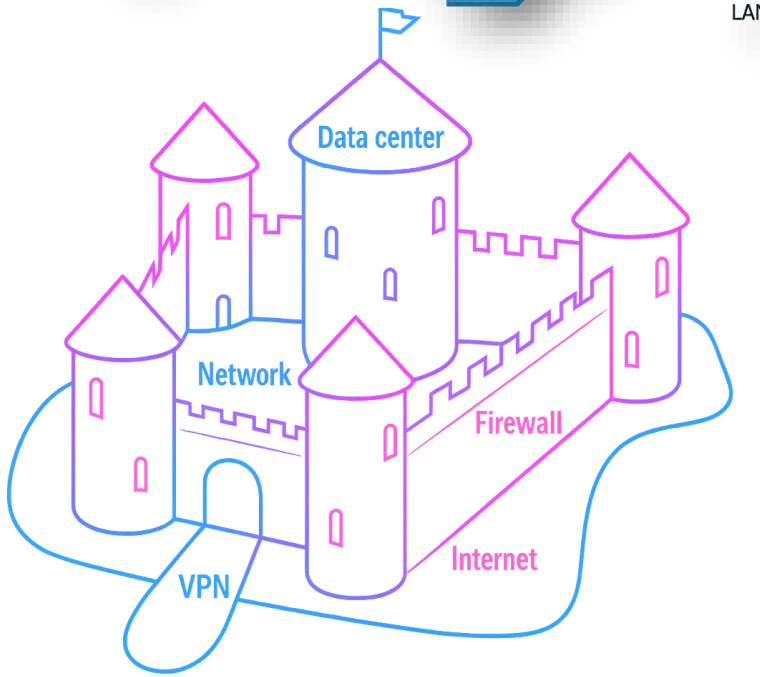




Perimetrový model (Castle-and-Moat)

- **Silné stránky**
  - **Prvá línia obrany**
    - **Z**ákladná bariéra proti externým hrozbám
  - **Jednoduchý koncept**
    - implementácia a pochopenie
  - Vhodný pre legacy a tradičné on-prem siete
  - Súčasť aj súčasných dizajnov - Perimeter s FW je **stále dôležitý**
- **Slabé stránky:**
  - **Internal Blindness:**
    - nedostatočná viditeľnosť vo vnútri siete → laterálny pohyb útočníka
  - **Assumes Internal Trust:**
    - všetko vo vnútri sa považuje za bezpečné → falošný pocit istoty
  - **Insider threats:**
    - perimeter model neadresuje riziká zo strany zamestnancov alebo kompromitovaných účtov
  - **Jedno miesto zlyhania:**
    - ak perimeter padne, útočník má voľný prístup k vnútorným systémom
  - **Nedostatočné pre moderné architektúry:**
    - cloud, mobilita, remote work → perimeter sa rozmazáva





Porovnanie: Perimeter vs. Hierarchický model

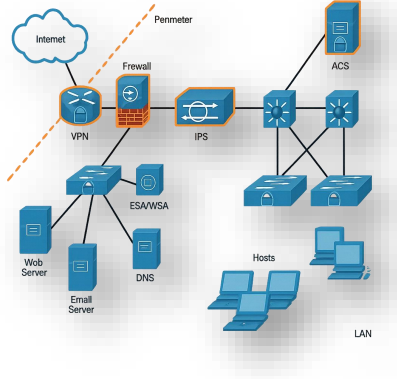
Perimeter security

- **Princíp**
  - Jedna hranica
    - dnu = dôveryhodné
    - vonku = hrozba
- **Nástroje:** FW, IDS/IPS, VPN, DMZ
- **Výhody**
  - Jednoduchý koncept, rýchla implementácia
  - Dobrá prvá línia obrany (Internet ↔ LAN)
- **Slabiny:**
  - Interná “slepota”, implicitná dôvera vo vnútri
  - Slabé pre cloud a mobilitu

Hierarchický model

- **Princíp**
  - Viac vrstiev siete → prirodzené body kontroly
- **Nástroje:** NAC v Access, FW/ACL/IDS v Distribution, redundancia a CoPP v Core …
- **Výhody**
  - Modularita, škálovateľnosť, jasné hranice
  - prirodzene podporuje Defense-in-Depth
- **Slabiny:**
  - Potrebuje dobrý návrh a dôsledné uplatnenie princípov

Bezpečnosť v Enterprise vs. SOHO



- **Enterprise (veľká organizácia):**
  - **Ciele:** bezpečnosť, škálovateľnosť, odolnosť, compliance (ISO 27001, NIS2, GDPR)
  - **Architektúra:** hierarchický model (Access–Dist–Core) + perimeter + DMZ + mikrosegmentácia
  - **Procesy:** riadené zmeny (change management), pravidelné testy, monitoring 24/7, **plánovanie**
  - **Investície:** dedikované tímy (NetOps, SecOps)

- Kľúčové oblasti návrhu
  - **High Availability (HA):**
    - redundantné FW, load balancer, dual-homed ISP, FHRP (HSRP, VRRP, GLBP)
  - **Resilience & Odolnosť:**
    - segmentácia služieb, fallback linky, zálohovanie konfigurácií, „Design for failure“
  - **Monitoring & Visibility:**
    - NTP sync, NetFlow/sFlow/IPFIX, SIEM korelácia, NMS (SNMPv3, Syslog, NetConf), baseline monitoring
  - **Change Management & Testing:**
    - testovanie failover scenárov, chaos engineering light, SoD (4-eyes) kontrola
  - **Bezpečnostné prvky:**
    - NGFW, IDS/IPS, WAF, NAC+AAA, ESA/WSA, SIEM, HA clustre

Cvičenie

Cvičenie: Návrh zón pre e-shop infraštruktúru

- **Scenár:**
  - Malá firma prevádzkuje e-shop
  - Infraštruktúra
    - Webserver publikovaný na internete
    - Interný aplikačný server
    - Databázový server
    - Interná LAN pre zamestnancov
- **Cieľ:**
  - Navrhnúť **zónovú architektúru**, ktorá minimalizuje riziko kompromitácie
- **Úloha**
  - Rozhodnite, **koľko zón** navrhnete (minimálne 3, možno viac)
  - Rozmiestnite jednotlivé komponenty (web, app, DB, LAN) do zón
  - Určte **pravidlá komunikácie** medzi zónami (čo môže s kým hovoriť, na akom porte)

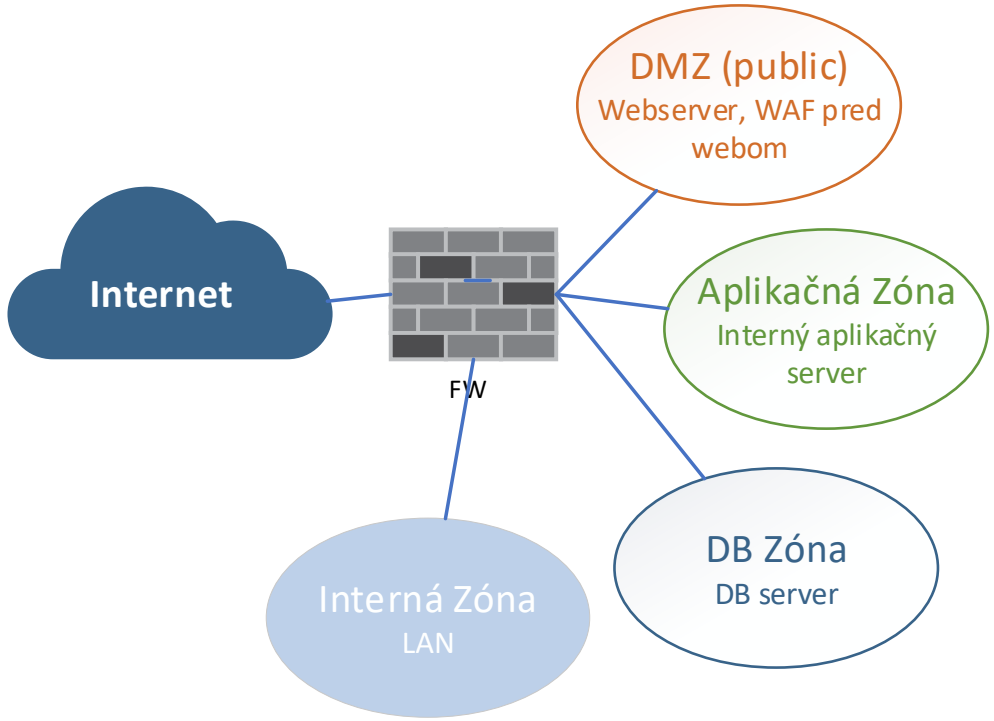
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Možné riešenie - zóny

Koľko zón?

- **Zóny**
  - **DMZ (Public)**
    - Webserver, WAF pred webom;
    - Žiadny priamy prístup do LAN
  - **Application Zone**
    - Interný aplikačný server (API, business logika)
  - **Database Zone**
    - Databázový server izolovaný, bez priameho prístupu z DMZ ani z LAN
  - **Internal LAN (Users)**
    - Používateľské stanice, kancelária, tlačiarne (oddelené VLAN)
  - *(Voliteľná)* **Management Zone**
    - Jump host, nástroje správy, zálohovací server; oddelené od Users

Koľko zón?



Možné riešenie – policy

Aké policy? Ktorá zóna s ktorou a ako bude komunikovať?

Zóna → Zóna	Smer	Služby (príklad)	Poznámka
Internet → DMZ/Web	IN	TCP/80,443	WAF pred webom
DMZ → App	IN	TCP/8443 (API)	Len Web → App, ak je vôbec potrebné
App → DB	IN	TCP/5432/3306	Len App → DB
LAN → App/DB	IN	—	**Deny**
LAN → DMZ	In	—	**Deny -** Typicky žiadny
Mgmt → všetky servery	IN	SSH/HTTPS/RDP	cez **jump host**, časové JIT
Všetky → Internet (egress)	OUT	len HTTPS (updates)	blok 25/135/445 atď.

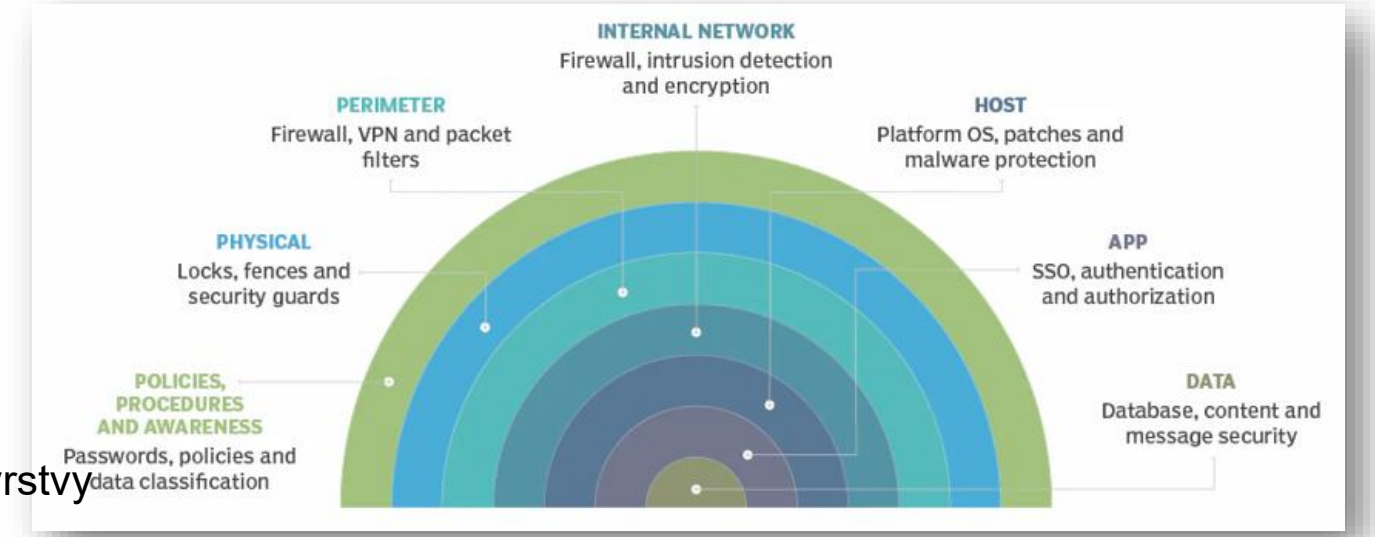
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Moderný dizajn – bližší pohľad

- DiD
- ZTN/ZTNA
- SDN / SD-WAN / SDA

Defense-in-Depth (DiD)

- **Cieľ:**
  - Zníženie rizika prieniku a šírenia hrozieb
  - Chráni pred zlyhaním jednej vrstvy
- **Stratégia** viacerých obranných vrstiev sústredných okolo aktíva
  - Žiadna „jedna“ zložka ochrany nie je dostatočná
    - Vrstvy spolupracujú
  - Predpoklad => Útočník musí penetrovať všetky vrstvy
- Vrstvy
  - **Administratívna vr.**
    - Politiky a postupy: silné heslá, data classification, incident response
    - Awareness: školenia, simulované phishing kampane
    - Compliance: ISO 27001, NIS2, audit
  - **Fyzická vr.**
    - Access control: biometria, RFID karty
    - Monitoring: CCTV, alarmy, senzory.
    - Ochrana prostredia: požiarna ochrana, klimatizácia, UPS
  - **Technická vr.** => ďalši slajd

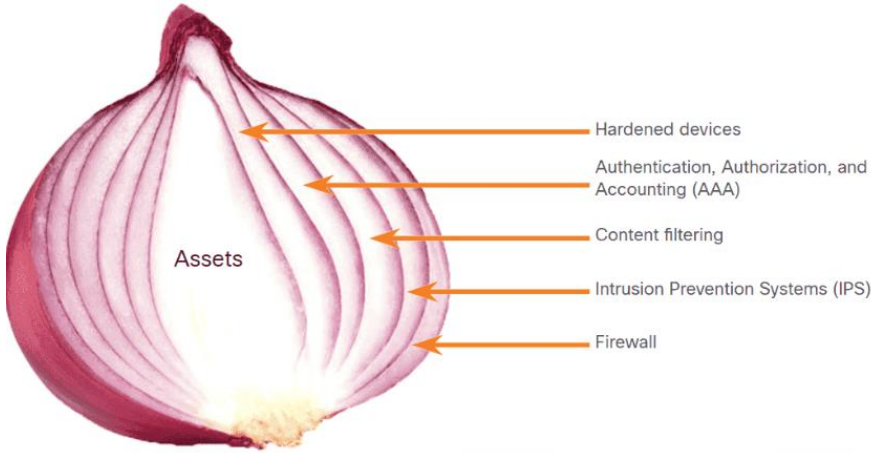


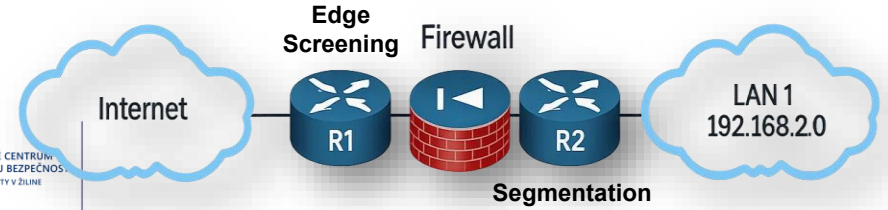
- **Implementácia**
  - Kombinácia technológií (NGFW, EDR) a procesov (politiky, školenia)
  - Security framework (napr. NIST NCF) => pomáha identifikovať kritické vrstvy (posilnenie ochrany)
- **Historický kontext** => Štandardná prax v enterprise sieťach už od konca 90. rokov
- **Súčasnosť** => stále relevantná, no dopĺňa sa o Zero Trust a moderné prístupy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

DiD – siete a technická aplikácia

- **Perimeter Security**
  - Prvá vrstva ochrany, ktorá chráni sieť pred vonkajšími hrozbami
  - NGFW, DMZ, Screening FW, IPS, anti-DDoS
  - Príklad: Blokovanie DDoS z internetu
- **Sieťová Segmentácia**
  - Rozdelenie flat siete na menšie, izolované časti
  - Segmentácia VLAN/VRF, NSG, mikrosegmentácia, IDS/NDR
  - Príklad: VLAN per DMZ, internal VLAN, ...
- **Endpoint Security**
  - Ochrana jednotlivých koncových zariadení
  - Antivírus, EDR, patch management, hardening, application whitelisting
  - Príklad: Detekcia ransomware na PC
- **Aplikačná Bezpečnosť**
  - Zabezpečenie aplikácií, aby sa predišlo útokom zraniteľností v kóde
  - WAF, API gateways, Secure SDLC
  - Príklad: WAF zastavenie SQL injection na e-shope.
- **Dátová Bezpečnosť**
  - Priama ochrana samotných dát
  - Šifrovanie (at rest & in transit), HSM/Key Vault, DLP, zálohy
  - Príklad: Zálohy obnovaia dát po útoku šifrovacím softvérom
- **Zálohovanie a obnova:** Možnosť obnovy dát a služieb v prípade zlyhania





Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Posúdenie Defense in Depth

Výhody

- **Viacvrstvová ochrana**
  - *„Dôveruj ale preveruj (Trust but Verify)“*
  - Znižuje riziko prieniku jednou vrstvou pri jej zlyhaní
  - Chráni pred rôznymi typmi útokov
- **Flexibilita**
  - Možno kombinovať rôzne technológie podľa potrieb organizácie
  - Funguje v tradičných aj hybridných prostrediach
    - Vhodný aj pre **hybridné prostredia**
    - Kombinuje on-prem a cloud ochranu
- **Jednoduché vysvetlenie**
  - Koncept je intuitívny a ľahko komunikovateľný manažmentu.
- **Komplementárny k moderným prístupom**
  - DiD sa dobre dopĺňa s ZTA, SASE, ASA – nie je v konflikte

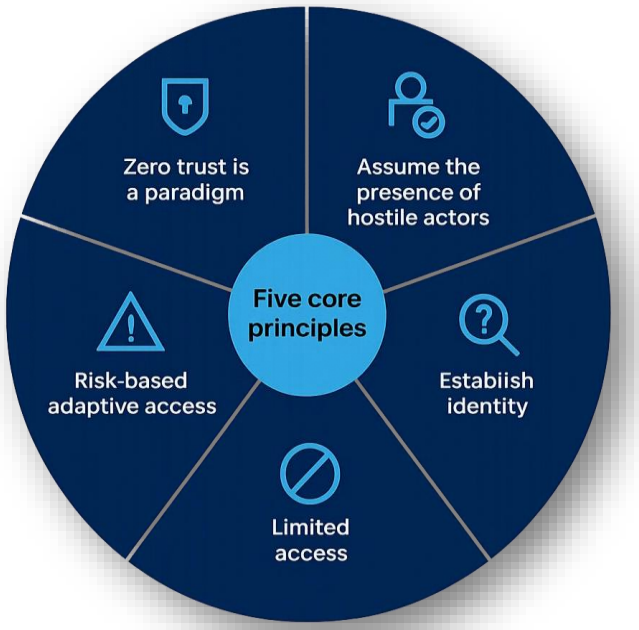
Výzvy a riziká

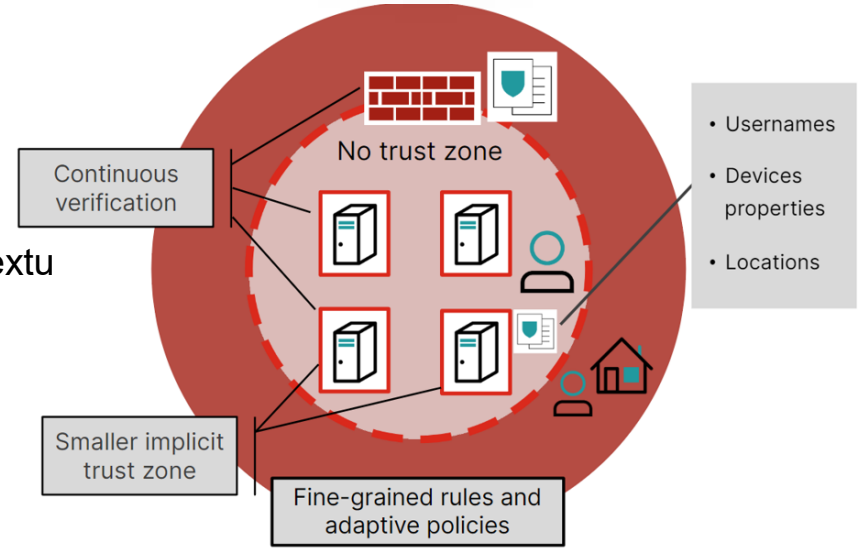
- **Statický model**
  - Na sieť zamerané / IP oriented
  - Neadaptuje sa na kontext alebo riziko v reálnom čase
  - Môže byť neefektívny proti moderným hrozbám
- **Implicitná dôvera**
  - Raz overený zdroj (používateľ, zariadenie) je dôveryhodné
- **Technické výzvy**
  - Komplexita integrácie viacerých technológií
  - Náročnosť na správu a monitoring vrstiev
- **Náklady**
  - Vyžaduje investície do viacerých technológií a tímov
- **Organizačné výzvy**
  - Koordinácia medzi tímami (SecOps, NetOps)
  - Nedostatok školení a času pre správu vrstiev
  - Príklad: Chyba v konfigurácii firewallu kvôli nejasným rolám
- **Riziká**
  - Možné prestoje pri zlúčení vrstiev

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ A INFORMATIZÁCIE SLOVENSKA

Zero Trust Architektúra (ZTA) – princípy

- ZTA
  - Moderný architektonický model pre sieťovú a aplikačnú bezpečnosť
  - Postavený na princípe **„Never trust, always verify“**
  - Žiadna implicitná dôvera, ani vo vnútri siete
  - Posúva ochranu z perimeteru na **identitu, kontext a dáta**
- **ZTA ≠ iba princípy, ale celá architektúra**
  - **Logické komponenty**: identita, zariadenia, aplikácie, dátové toky
  - **Technické opatrenia**: IAM, MFA, NAC, segmentácia siete, šifrovanie
  - Zero Trust stavia na
    - **Least Privilege (LP) Access**
      - Prístup iba k potrebným zdrojom, minimálne oprávnenia
      - Prístupy sú udeľované len v rozsahu nevyhnutnom na vykonanie úlohy (modely RBAC, ABAC)
    - **Continuous Verification**
      - Neustále overovanie identity a integrity zariadení
      - Každá požiadavka je validovaná podľa identity, stavu zariadenia, polohy a kontextu
    - **Microsegmentation**
      - Rozdelenie siete na malé zóny s prísnou kontrolou a politikami
    - **Assume Breach**
      - Predpoklad, že v sieti je prienik / je už kompromitovaná
    - **Hostile environment**
      - Všetci používatelia, zariadenia a siete sú považované za nedôveryhodné





Prečo vznikol Zero Trust

- **Perimeter a Zero Trust**
  - **Perimeter model prestáva stačiť** – kolaps perimetra
    - Stieranie hraníc siete (cloud, SaaS, hybrid infra, outsourcing)
    - Implicitná dôvera vo vnútri → útočník po prieniku má voľný pohyb
    - Perimeter FW/VPN chránia len „okraj“, nie vnútro
    - Laterálny pohyb
  - Nové trendy a výzvy
    - **BYOD & mobilita** – vlastné zariadenia, rôzne OS a bezpečnostné úrovne
    - **Remote work** – home office, kontraktori, partneri
    - **Cloud služby** – aplikácie a dáta mimo firemného datacentra
    - **Moderné hrozby** – phishing → kradnuté identity, ransomvér → lateral movement, insider threats
  - **Výsledok**
    - Potrebný posun k **Zero Trust**:
      - **identita + kontext = nový perimeter**

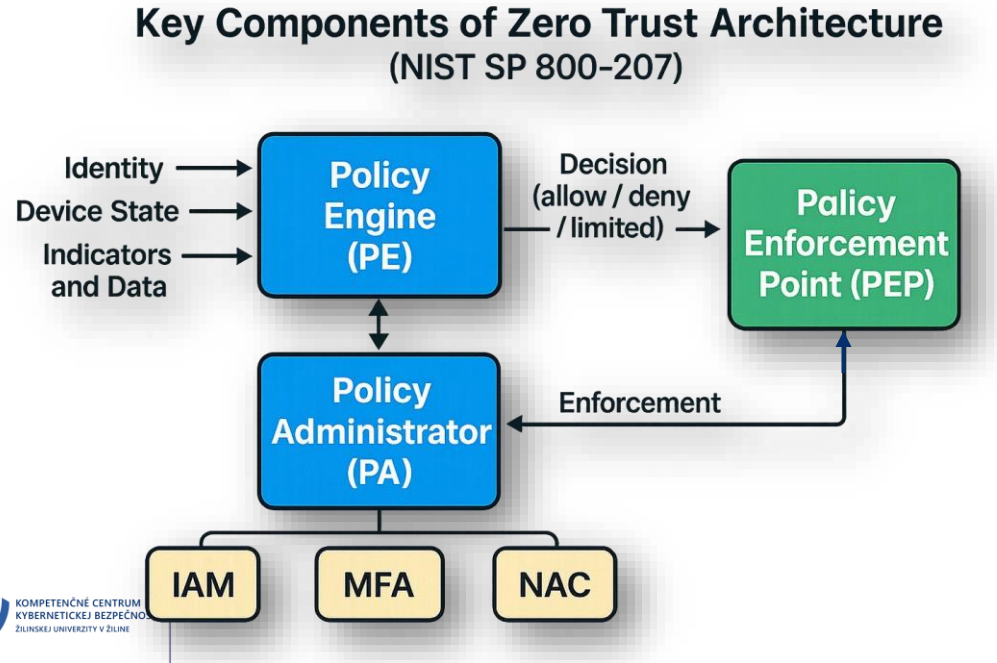
- **DiD a Zero trust**
  - DiD ≠ zastarané
    - Stále základný stavebný princíp
- Zero Trust
  - Posúva DiD od network policy (IP based) k identity-based prístupu
  - Zohľadnenie na cloud, mobilitu a BYOD
  - DiD sa integruje so ZT
- **DiD + Zero Trust = Moderná komplexná a adaptívna** architektúra
  - **viacvrstvová ochrana + neustála verifikácia**

Sedem princípov ZTA (NIST SP 800-207)

Princíp	Opis
1. Zdroje	Všetky dátové zdroje a služby sú považované za zdroje, ktoré si vyžadujú ochranu
2. Komunikácia	Všetka komunikácia (interná či externá) je zabezpečená, bez ohľadu na jej umiestnenie v sieti (šifrovanie)
3. Prístup	Prístup k zdrojom je udeľovaný na základe jednej transakcie v relácii (nie celej relácie) a na základe potreby
4. Dynamická politika	Rozhodnutia o prístupe sú riadené dynamickými politikami, ktoré berú do úvahy kontext a riziko (poloha v reálnom čase, identita používateľa, stav zariadenia a environmentálne atribúty)
5. Integrita	Integrita a stav zabezpečenia všetkých aktív sú neustále monitorované na prítomnosť zraniteľností a narušení
6. Overenie a autorizácia	Overenie a autorizácia sú dynamické a prísne vynucované pred každým prístupom
7. Zber údajov	Zberajú sa komplexné informácie na neustále zlepšovanie bezpečnostného stavu (komplexná telemetria)

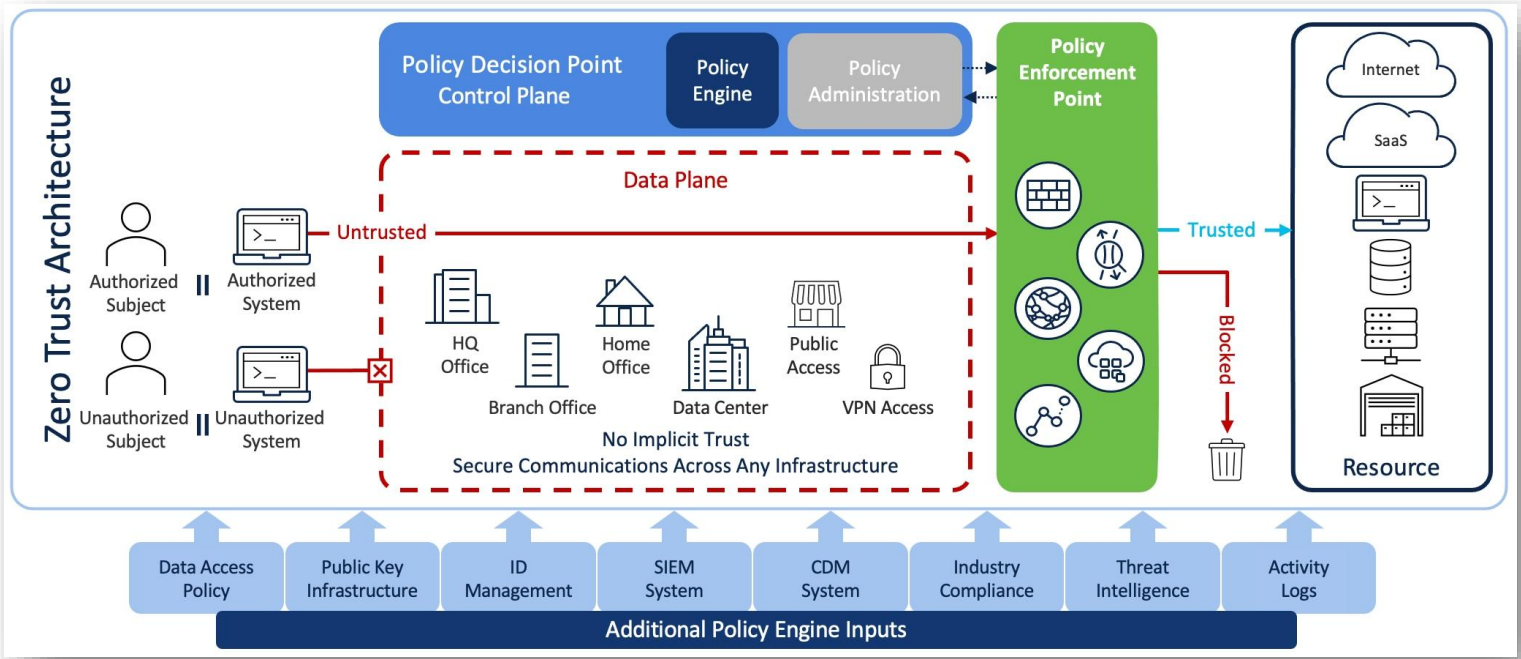
Zero Trust Architektúra – logické komponenty

- **Policy Engine (PE) - mozog**
  - Rozhoduje o udelení/odmietnutí prístupu
  - Vstupy z PIP: identita (IAM), stav zariadenia (NAC, EDR), rizikové skóre (UEBA), threat intel (SIEM dáta), kontext (čas, miesto, typ požiadavky)
  - Výstup: rozhodnutie „allow / deny / limited“ do PEP
- **Policy Administrator (PA) - správca**
  - Vytvára, udržiava a spravuje pravidlá pre PE
  - Prekladá rozhodnutie PE do konkrétnych akcií
  - Vydáva tokeny, certifikáty alebo session keys
  - Distribuuje politiky do enforcement bodov
  - Jednoducho: konfiguruje PE a PIP
- **Policy Enforcement Point (PEP)**
  - Reálne uplatňuje rozhodnutie z PE
  - Príklad: ZTNA agent na koncovom zariadení, sieťová brána, FW, proxy, VPN GW
  - Overuje každý request a povoľuje len schválenú komunikáciu
- **Policy Information Point (PIP)**
  - Podporné dátové zdroje a telemetria pre PE
    - Identity provider (IdP) – AD, LDAP, Azure AD
    - Device posture – MDM (MobDevManag), EDR (stav zariadenia, patching, AV)
    - Threat intelligence – IOC, reputačné feedy
    - Logging & SIEM – spätná väzba pre kontinuálne učenie



Zero Trust Architektúra – workflow

- **Príklad workflow NIST SP 800-207:**
  - Používateľ žiada o prístup k aplikácii
  - PEP → zachytí a posiela request do PA/PE na rozhodnutie
  - PE
    - Číta dáta z PIP (telemetria)
    - Vyhodnotí identitu, device posture, riziko
    - Príjme rozhodnutie na základe rizika
  - PA vydá relačný token /session key
  - PEP vynúti rozhodnutie PE
    - Povoľuje len autorizovaný prístup
- Nedeje sa jednorazovo ale nepretržite a cyklicky
  - PIP monitoruje situáciu
  - Zmena kontextu
    - Informácia do PE => nový workflow

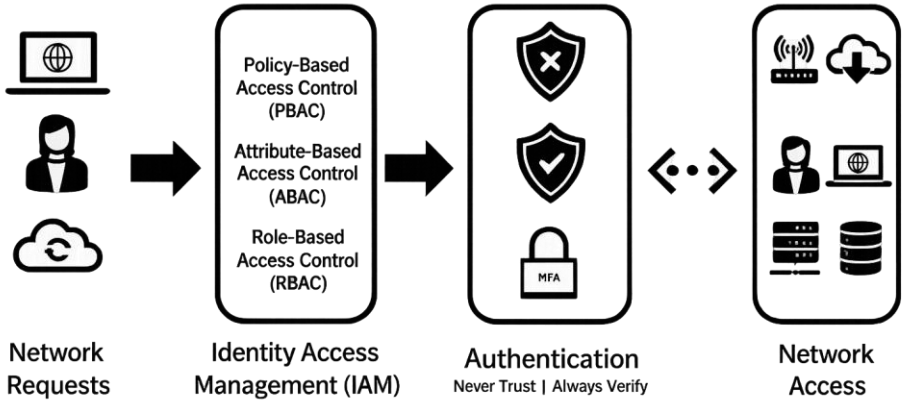


Základné technológie pre implementáciu ZT

Identita = IAM + MFA

- Identity v ZTA => nový perimeter
  - Identita používateľa a zariadenia je kľučová => posun od adries k používateľovi
  - Každá požiadavka sa autorizuje na základe identity + kontextu
- Identita a autenticita
  - **IAM** (Identity & Access Management) => **SSO**
    - IAM = centrálny zdroj „pravdy“ o tom, kto je kto a čo môže
    - Identity Provider (IdP): Active Directory, Azure AD, Okta, Keycloak
    - Politiky prístupu: RBAC, ABAC, just-in-time (JIT) prístupy
    - Lifecycle: provisioning, deprovisioning, správa privilegovaných účtov
    - Audit: všetky zmeny prístupov musia byť logované a auditovateľné
  - **MFA** (Multi-Factor Authentication)
    - Viac faktorová autentifikácia
      - Kombinuje čo viem (heslo), čo mám (token/app), čo som (biometria)
    - Risk based MFA - úroveň autentifikácie sa prispôsobuje rizikovému kontextu

- ZT => **Continuous authentication => Continuous verification**
  - CA → session risk scoring (lokácia, device health)
  - CV → používateľ sa znova verifikuje pri zmenách kontextu (nové zariadenie, iná lokácia)
  - Príklad: prístup do DB povolený len pri MFA + zariadenie v compliance stave
- Anti-príklad
  - Jednorazové prihlásenie s heslom → neobmedzený prístup k celej sieti
  - Zdieľané administrátorské účty bez MFA

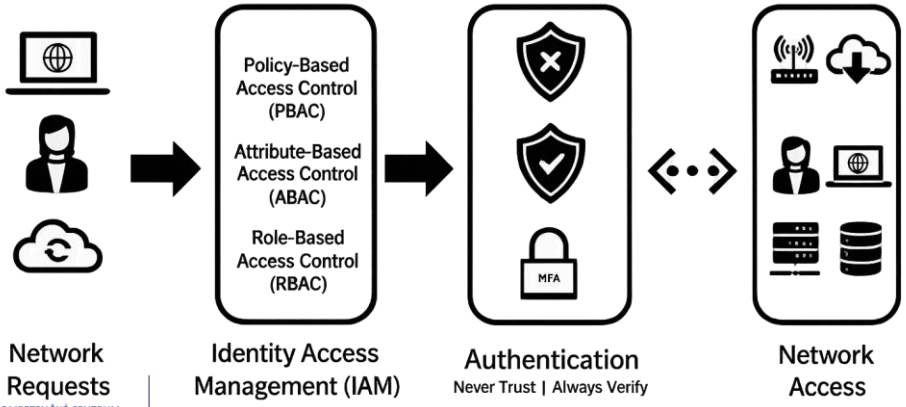


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie prístupu k sieti

- ZTA = **Posilnenie kontroly prístupu**
  - Žiadná implicitná dôvera
- **NAC (Network Access Control):**
  - **Prvá línia verifikácie** => overovanie a autorizácia zariadení pred pripojením
  - Vrátane „*device compliance*“
  - Integrácia s IdP pre overenie stavu zariadenia (napr. patch level)
  - **Mechanizmy:** IEEE 802.1X (port-based), posture assessment (AV, patch, konfigurácia)
  - **Príklad**: Blokovanie neaktualizovaného PC od prístupu k sieti
- **Mikrosegmentácia:**
  - Rozdelenie siete na malé zóny s prísnym prístupom
  - + zabezpečenie kontroly a obmedzenia pohybu
    - Vrátane East-West prevádzky
  - **Mechanizmy:** SDN (Cisco ACI, VMware NSX), identity-based firewally, host-based FW, ...
  - – každá komunikácia medzi servermi alebo aplikáciami je overovaná
  - Znižuje šírenie hrozieb po kompromitácii / laterálneho pohybu

- **Výzvy:**
  - Komplexita implementácie a správy
  - Náklady na sofistikované riešenia
- **Príklad v praxi:**
  - Notebook sa pripája do LAN → NAC overí cez 802.1X a posture check
  - Notebook dostane prístup len do VLAN pre bežných používateľov
  - Pokus o prístup na DB server je blokovaný, ak používateľ nemá rolu *DB admin*
- **Anti-vzor:**
  - Všetky zariadenia v LAN = rovnaká dôvera
  - Jeden kompromitovaný klient → útočník má voľný pohyb v celej sieti



Výhody ZTA

- **Lepšia reakcia na hrozby a útoky**
  - Zastavuje **lateral movement** → útočník sa nedostane ďalej, ani keď kompromituje jedno konto
  - Chráni pred **insider threats** (žiadna implicitná dôvera)
- **Lepšia kontrola a audit**
  - Každý prístup je **overený a logovaný**
  - Umožňuje detailný **audit trail** pre NIS2, GDPR, ISO 27001
- **Podpora princípu Least Privilege**
  - Dynamické politiky na základe identity, kontextu a rizika
  - Minimalizácia prístupov = menší útokový povrch
- **Škálovateľnosť a budúca pripravenosť**
  - Kompatibilné s **SASE, IAM, ZTNA** riešeniami
  - Architektúra pripravená na **AI-driven bezpečnostné systémy**
- **Adaptácia na moderné prostredia**

  Funguje v **hybridných infraštruktúrach** (cloud + on-prem)
  - **Výhody pre Cloud**
    - Chráni distribuované prostredia (IaaS, PaaS, SaaS).
    - Mikrosegmentácia izoluje cloudové zdroje.
    - Príklad: ZT zabezpečí Office 365 pred neautorizovaným prístupom.
  - **Výhody pre Remote Workforce**
    - Bezpečný prístup z ľubovoľného miesta.
    - Continuous verification zvláda dynamické lokácie.
    - Príklad: Zamestnanec z domu pristupuje k CRM s MFA
  - Podporuje **mobilitu, BYOD, remote work**

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výzvy pri ZTA

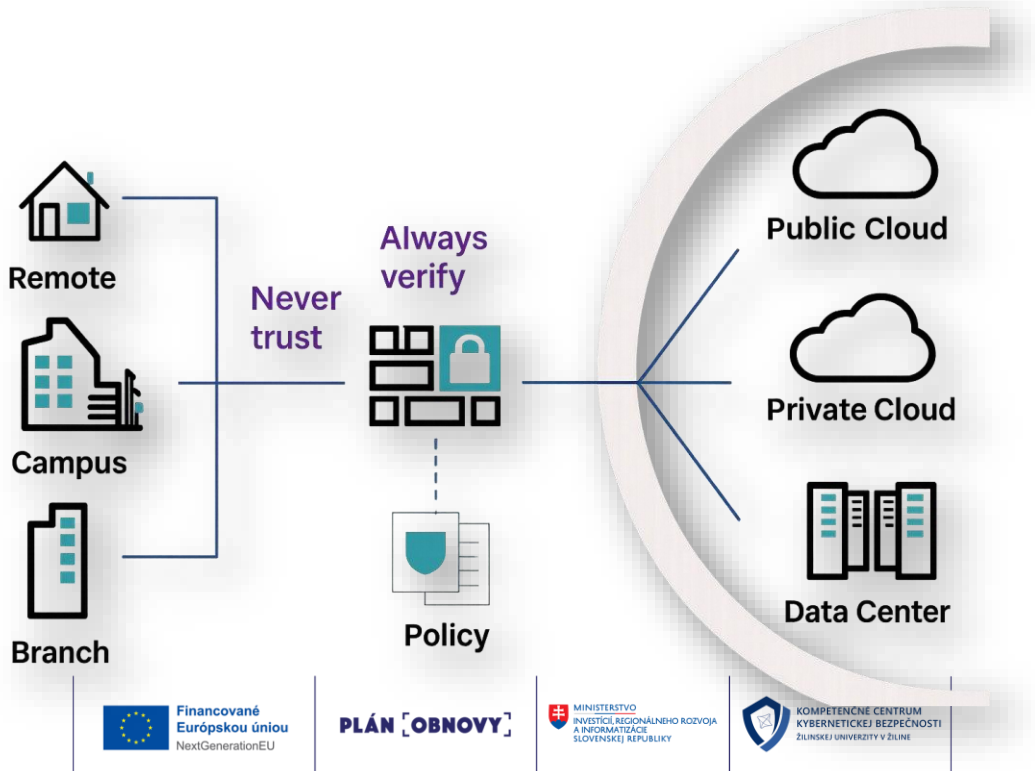
- **Technické výzvy**
  - **Zásadné zmeny v infaštuktúre**
  - **Komplexná integrácia** – prepojenie IAM, FW, NAC, SIEM, EDR, cloud security
  - **Legacy systémy** – staré aplikácie a protokoly nemusia podporovať moderné IAM/MFA
  - **Výkon a latencia** – každé overenie môže zvyšovať oneskorenie pri prístupe
  - **Viditeľnosť a monitoring** – nutnosť centralizovaného dohľadu nad identitami, zariadeniami a dátovými tokmi
  - **Správa politik -** Veľké množstvo mikro-politík môže byť náročné na správu a audit
    - Potreba centralizovaného Policy Engine a automatizácie
- **Organizačné výzvy**
  - **Kultúrna zmena** – zmena myslenia z „*dôveruj vo vnútri*“ na „*never trust, always verify*“
  - **Odpor používateľov** – viac autentifikácií (MFA) môže znižovať komfort
  - **Náklady** – investícia do nových riešení, školení a prevádzky
  - **Zodpovednosti** – zmena rolí v tímoch (sieť vs. bezpečnosť vs. identity management)
- **Bezpečnostné výzvy**
  - **Falošný pocit bezpečia -** ZTA nie je „silver bullet“
    - Stále je potrebné riešiť patching, insider threats, phishing.
    - Overenie identity ≠ bezpečný používateľ.
  - **Dynamické hrozby -** Útočníci sa prispôsobujú
    - napr. kradnutie tokenov, manipulácia s kontextom.
    - Potreba neustáleho risk scoringu a adaptívnych reakcií
- **Externé faktory**
  - **Compliance & regulácie** – zosúladenie ZT s GDPR, NIS2, ISO 27001
  - **Multi-cloud prostredie** – rozdielne IAM a bezpečnostné politiky poskytovateľov
- **Riziká:**
  - Vysoké počiatočné náklady na implementáciu
  - Možné prestoje počas prechodu
- **Riešenia**
  - Postupná migrácia s pilotným projektom
  - Investícia do školení a nástrojov (napr. SIEM)

ZTA štandardizácia

Rámec	Pôvod	Primárne zameranie	Kľúčové piliere/komponenty
NIST SP 800-207	NIST (National Institute of Standards and Technology)	Poskytuje základné, od dodávateľov nezávislé princípy a architektonické komponenty.	Sedem základných princípov, komponenty PE, PA, PEP.
CISA ZTMM	CISA (Cybersecurity and Infrastructure Security Agency)	Poskytuje postupný plán na implementáciu princípov ZT.	Päť pilierov (Identita, Zariadenia, Siete, Aplikácie a pracovné zaťaženie, Dáta) a tri možnosti (Viditeľnosť, Automatizácia, Riadenie).
Forrester ZTX	Forrester Research	Rozširuje ZT na celopodnikovú architektúru a zahŕňa všetky vrstvy.	Piliere zahŕňajú bezpečnosť ľudí/pracovnej sily, zariadení, siete, pracovného zaťaženia/aplikácií a dát.

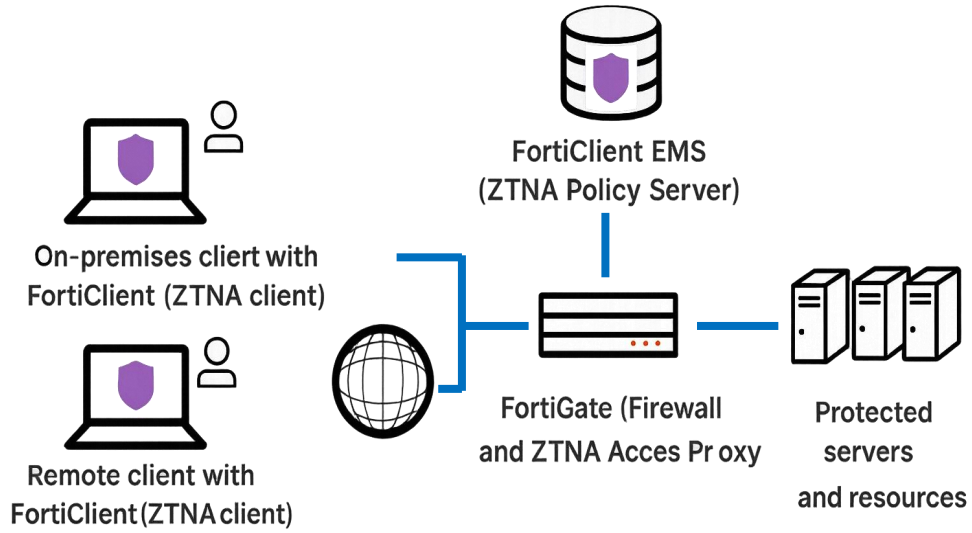
Aplikácia Zero Trust – Zero Trust Network Access architektúra

- **ZTNA – Zero Trust Network Access**
  - Aplikácia ZTA pre zabezpečený vzdialený prístup
  - Nahrádza alebo dopĺňa tradičné VPN s dynamickým overovaním
  - Vytvára dynamické, šifrované tunely medzi používateľom a konkrétnym zdrojom
  - Granulárny prístup na základe **identity a kontextu**



Aplikácia Zero Trust – ZTNA Fortinet

- Komponenty (príklad Fortinet)
  - **ZTNA Klient / Agent – FortiClient**
    - Spustený na zariadení používateľa, kt. zbiera a posiela
    - Autentifikácia s cert a MFA
  - **ZTNA Policy Server - FortiClient Endpoint Management Server - EMS**
    - Pravidlá (policies) pre prístup podľa identity a stavu zariadenia
    - Generuje certifikáty klientov a „posture tags“ (značky podľa stavu zariadenia)
  - **ZTNA Broker/Gateway (Proxy & Firewall) – FortiGate FW**
    - Overuje klienta a jeho certifikát
    - Aplikuje politiky (Least Privilege, Continuous Verification) z EMS
    - Rozhoduje, či a k čomu bude mať klient prístup



- **Chránené zdroje (servery/aplikácie)**
  - Sú dostupné iba cez FortiGate proxy
  - Klient nikdy nepristupuje priamo do celej siete
    - **Len granularny prístup** – nie do celej siete, ale k špecifickej službe
- **Monitoring – FortiAnalyzer**
- **Identity Provider - FortiAuthenticator alebo priamo Azure AD / AD**

ZTNA Fortinet – Zjednodušený príklad činnosti

1 **Client (FortiClient) → posiela identitu a stav → EMS**
Používateľ (on-prem alebo remote) spustí FortiClient
FortiClient: odosiela do FortiClient EMS:
- Atribúty zariadenia (typ operačného systému)
- Informácie o používateľovi (ID používateľa)
- Bezpečnostný stav zariadenia

2 **EMS → vydá certifikát + tagy → Client**
FortiClient EMS generuje:
- Posture Tag (Compliant/non compliant)
- Digitálny certifikát klienta

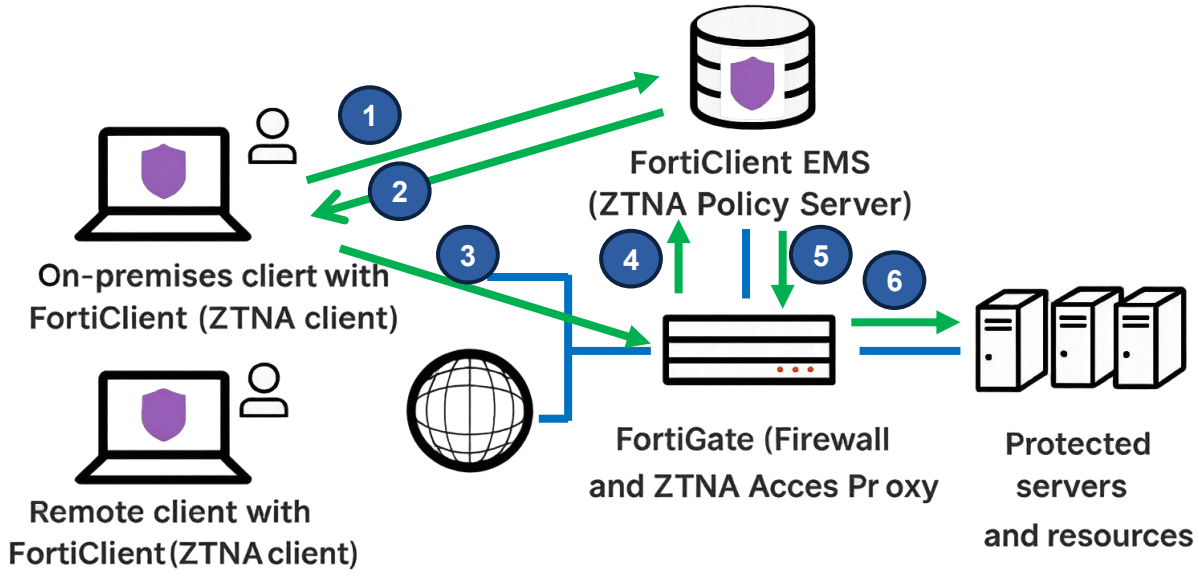
3 **Client → pripojenie na FortiGate Proxy → požiadavka na zdroj**

4 **FortiGate ↔ EMS → kontrola politiky (Allow/Deny/Limite**

5
- **F**ortiGate si vyžiada rozhodnutie od EMS: Allow / Deny / Limited access.
- Politika je založená na: identite, stave zariadenia, kontexte (lokalita, čas, riziko).

6 **FortiGate → vytvorí šifrovaný tunel → Protected Server**
- Ak je zariadenie a používateľ v súlade s politikami:
  - FortiGate vytvorí **šifrovaný tunel** (TLS/DTLS) medzi klientom a cieľovým serverom/aplikáciou
  - Používateľ má prístup len k schváleným aplikáciám/zdrojom (microsegmentation).

7 **Monitoring → Logy/Analyzer**
Všetky udalosti sú logované v **FortiAnalyzer / SIEM**



SDN – SD-WAN – SD Access

- **SDN = technický enabler pre ZTA / ZTNA v sieťovej infraštruktúre**
- **Software-Defined Networking (SDN)**
  - Architektonický prístup k návrhu siete
  - Oddelenie **Control Plane** a **Data Plane**
  - Centralizované riadenie a presadzovanie politík
  - Programovateľnosť siete (API, automatizácia)
  - Umožňuje konzistentnú a škálovateľnú implementáciu bezpečnostných princípov
  - **Abstrakcia sieťovej infraštruktúry**
    - Politiky definované logicky, nie na úrovni jednotlivých zariadení
    - Dynamická reakcia siete na zmeny kontextu (identity, aplikácie, stav)
    - Zníženie závislosti na IP adresách a statických konfiguráciách
- **SD-WAN – realizácia SDN princípov vo WAN**
  - Centrálne riadený WAN dizajn (hub-and-spoke / full-mesh overlay)
  - Bezpečný overlay (IPsec) nad rôznymi transportmi (MPLS, Internet, LTE/5G)
  - Politiky založené na:
    - Aplikácii, kvalite linky (latencia, jitter, loss), kontexte komunikácie
  - Bezpečnostný význam:
    - šifrovanie a izolácia prevádzky
    - kontrola tokov medzi lokalitami
    - podpora Zero Trust prístupu k aplikáciám
- **SD-Access – realizácia SDN princípov v LAN / campuse**
  - Software-defined campus architektúra
  - Oddelenie **identity od IP adresy**
  - Automatizovaná segmentácia (overlay siete, mikrosegmentácia)
  - Centrálne definované politiky prístupu
  - Bezpečnostný význam:
    - identity-based access control
    - obmedzenie laterálneho pohybu útočníka
    - presadzovanie princípov **Least Privilege** a **Segmentation**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Secure Access Service Edge (SASE) - Úvod

- SASE
  - **Cloud-native architektonický rámec => poskytovaný ako cloudová služba** (vendor-neutral koncept)
  - Spája **sieťové a bezpečnostné služby** do jednej platformy
  - Koncept definovaný spoločnosťou **Gartner** v roku 2019
    - Nie je štandardizovaný
- Cieľ
  - **Bezpečný a optimalizovaný prístup** ku všetkým aplikáciám a dátam – kdekoľvek a kedykoľvek

- **Kľúčové komponenty:**
  - **SD-WAN** (Software Defined WAN) – optimalizácia sieťového pripojenia
    - Dynamický výber ciest, QoS, redundancia
  - Bezpečnostné služby
    - **ZTNA** - Zero Trust Network Access
      - Bezpečný prístup na základe identity a kontextu
    - **CASB** – Cloud Access Security Broker
      - Kontrola prístupu k cloudovým aplikáciám, DLP, compliance
    - **SWG -** Secure Web Gateway
      - Ochrana pri prístupe na web
      - Web filtering, malware protection, URL kategorizácia
    - **FWaaS** – Firewall as a Service
      - Firewall ako služba
    - **DLP** – ochrana dát pred únikom

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SASE

- **Výhody:**
  - Jednotná bezpečnostná politika pre všetky lokality a používateľov
  - Zníženie komplexity a nákladov na infraštruktúru
  - Lepšia viditeľnosť a kontrola nad dátovými tokmi – aplikačná0
  - Škálovateľnosť pre hybridný pracovný model
  - Zjednodušená správa bezpečnosti a siete
- **Výzvy:**
  - Neexistuje formálna štandardizácia (napr. NIST, ISO)
  - Závislosť na dodávateľovi – rôzne implementácie, vendor lock-in
  - Komplexná migrácia z tradičnej infraštruktúry
  - Integrácia s existujúcimi systémami (IAM, SIEM, monitoring)

Iné architekturálne prístupy

- **Adaptive Security Architecture (ASA)**
  - Dynamická a cyklická bezpečnostná architektúra,
  - Neustále sa prispôsobuje aktuálnym hrozbám
  - Úloha: Zabezpečiť nepretržitú ochranu prostredníctvom adaptívneho rozhodovania a automatizácie
  - **Fázy**: Predict / Prevent / Detect / Respond
  - **Technológie**: SIEM, SOAR, UEBA, threat intelligence, machine learning
- **SSE – Security Service Edge**
  - Podmnožina SASE, zameraná čisto na **bezpečnostné služby** bez sieťovej vrstvy.
  - **Zahŕňa**: ZTNA, DLP
  - Vhodné pre organizácie, ktoré už majú SD-WAN
- **CARTA – Continuous Adaptive Risk and Trust Assessment (Gartner)**
  - Dynamické hodnotenie dôvery a rizika v reálnom čase.
  - Princíp: „never trust, always verify“ + „always monitor and adapt“
  - **Využíva:** UEBA, SIEM, threat intelligence
- **SDP – Software Defined Perimeter**
  - Skryje aplikácie pred verejným internetom, prístup je možný len po overení identity.
  - Zabraňuje skenovaniu portov a útokom typu reconnaissance.
  - Príklady: Appgate SDP, Google BeyondCorp
- **CNAPP – Cloud-Native Application Protection Platform**
  - Komplexná ochrana cloudových aplikácií: od vývoja po produkciu.
  - Príklady: Wiz, Orca Security, Palo Alto Prisma Cloud
- Cisco SAFE
- ...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sumarizácia

- **Bezpečnostné princípy**
  - CIA triáda (Confidentiality, Integrity, Availability)
  - Moderné princípy: Least Privilege, Segmentation, Fail-Safe Defaults, Accountability, Separation of Duties, Defense-in-Depth, Zero Trust
- **Architektonické modely** sú základom bezpečného návrhu
  - **Hierarchický model siete** → organizácia, škálovateľnosť, „pevný základ“ pre bezpečnosť
  - **Klasické modely**: perimeter security a jeho limity
- **Moderné prístupy**
  - **Defense-in-Depth** → vrstvená ochrana
  - **Zero Trust** → overovanie identity a kontextu vždy, všade
- **Kľúčové memento -** Perimeter už nestačí
  - Moderná bezpečnostná architektúra kombinuje viac vrstiev (DiD) a filozofiu Zero Trust

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Blok IV. – Technologické opatrenia

Perimeter & Sieťová vrstva

Access & Endpoint Layer

Core & Infrastructure Hardening

Technické opatrenia

Endpoint Protection - ochrana koncových zariadení

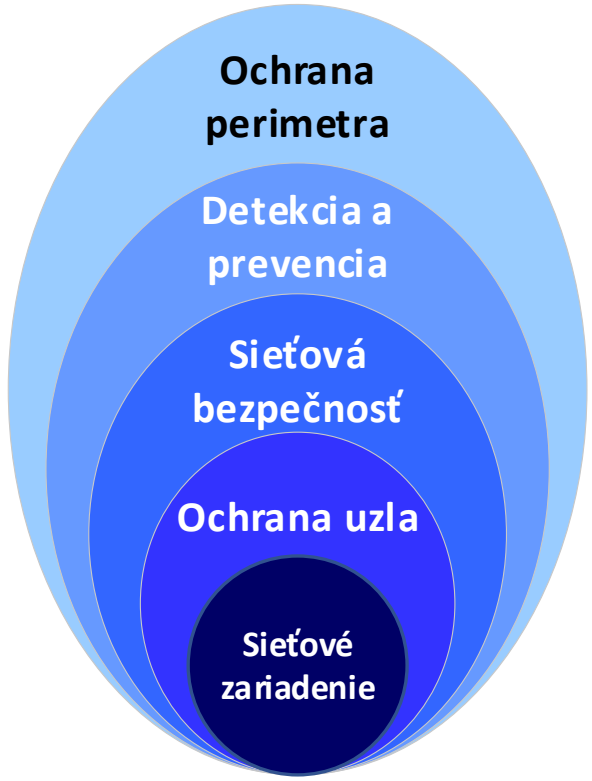
- **Základná preventívna ochrana**
  - Antivírus / Antimalware (signature + heuristika)
    - Tradičná signatúrová ochrana proti známym hrozbám
    - Dnes len základná vrstva
  - Endpoint/Personal Firewall
  - Network Intrusion Prevention (NIPS)
  - Anti-Spyware
  - Endpoint Hardening - vypnutie nepotrebných služie
  - Patch Management - aktualizácie OS/softvér
- **Pokročilá preventívna ochrana**
  - Blokovanie hrozieb ešte predtým, ako stihnú spustiť škodlivý kód:
  - Exploit Prevention
  - Anti-Ransomware – súborové aktivity
  - Application Control (Whitelisting) – zoznamy spustiteľných apps
  - End point Protection (EPP) - analýza správania, sandboxing, správa FW
- **Detekcia a reakcia**
  - Endpoint Detection and Response (EDR)
    - Zbieranie dát, Detekcia hrozieb, Vyhľadávanie (Threat Hunting), Náprava
  - Rozšírená detekcia a reakcia (XDR) – evolúcia EDR
  - Managed Detection and Response (MDR) - outsourcovaná služba
  - Logovanie a audit (zaznamenávanie aktivít)
- **Ochrana dát**
  - Zálohovanie dát
  - Šifrovanie disku (Full Disk Encryption - FDE) - Šifruj celý disk (BitLocker, FileVault)
  - Šifrovanie súborov - Šifrovanie na úrovni jednotlivých súborov alebo priečinkov
  - Data Loss Prevention (DLP) - Ochrana pred únikom citlivých dát
- **Kontrola integrity**
  - Aplikačný Sandbox – testovanie súborov pred spustením
  - Code Integrity Control (napr. CI Policy v Windows)
- **Špecializované riešenia**
  - Mobile Device Management (MDM) / Mobile Threat Defense (MTD): Ochrana pre smartfóny a tablety (Android, iOS)
  - Browser Security: Izolácia prehliadania (Browser Sandboxing) do cloudu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Technické opatrenia

Ochrana siete

- **Perimeter security - Ochrana perimetra a obvodu**
  - Firewally – ACL packet filter, stateful, NGFW (app control, URL filtering)
  - Zónová segmentácia – LAN/DMZ/Internet, mikrosegmentácia v DC
  - NAT – maskovanie, PAT, load-sharing
  - Anti-DDoS
- **Detection and prevention - Detekcia a prevencia (Hĺbková inšpekcia)**
  - IDS/IPS – detekcia a prevencia útokov
  - NDR – Network Detection & Response
  - SIEM (Security Information and Event Management)
- **Network Security - Sieťová bezpečnosť**
  - Segmentácia VLAN/VRF
  - Mikrosegmentácia
  - **Access Layer Security – Zabezpečenie prístupu**
    - 802.1X, Port Security, DHCP snooping
    - Wi-Fi šifrovanie (WPA3, certifikáty)
- **Node protection – Ochrana sieťového uzla**
  - Patch management a Zálohy
  - Device hardening
  - DDoS protection
  - Control plane protection



- **Ochrana aplikácií a služieb**
  - WAF – ochrana web aplikácií (SQLi, XSS, OWASP Top 10)
  - ESA – Email Security Appliance (spam, phishing, malware)
  - WSA – Web Security Appliance (URL filtering, sandboxing)
- **Remore access and management - Vzdialený prístup a manažment**
  - VPN – Site-to-Site, Remote Access, SSL, Ipsec
  - In-band vs. Out-of-band management
  - Bezpečný manažment – SSH, SNMPv3, syslog

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

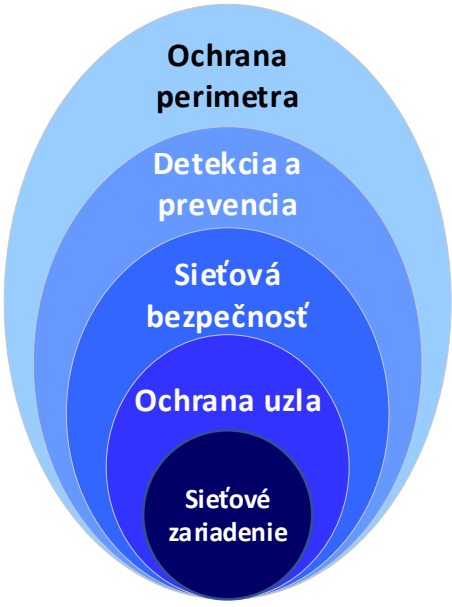
Perimeter security - Ochrana perimetra a obvodu

FW

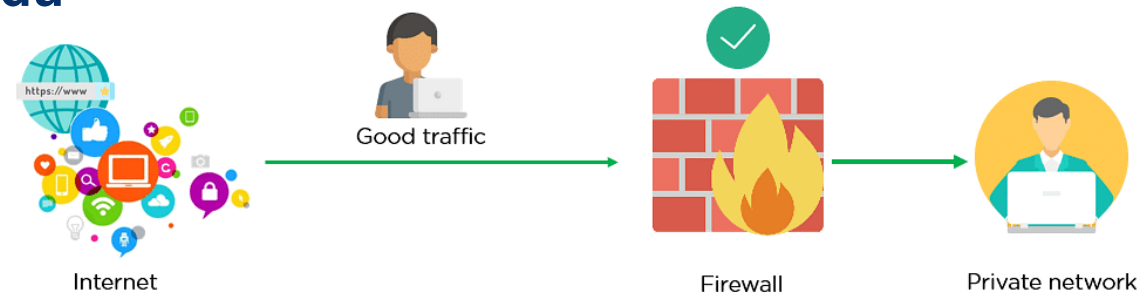
ACL

Zóny

NAT



Firewall

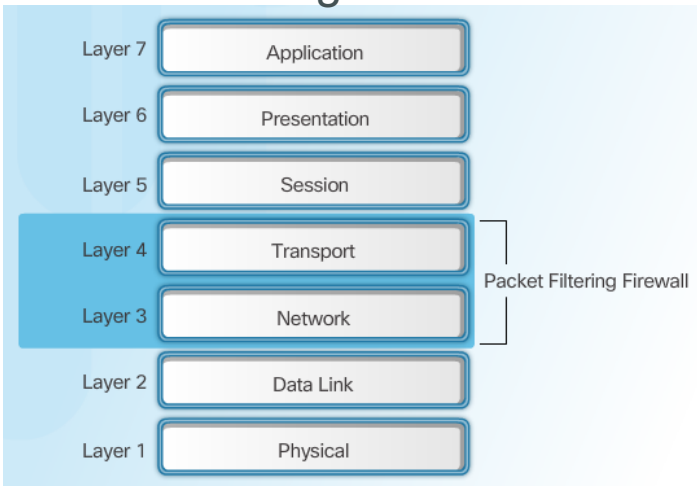


- Firewall
  - Hardvérové alebo softvérové zariadenie na kontrolu sieťovej komunikácie
  - Monitoruje prichádzajúcu a odchádzajúcu sieťovú premávku
  - Základný stavebný prvok Defense in Depth (DiD) architektúry
- Primárna úloha
  - Prvá línia obrany – „gatekeeper“ pre sieťové zdroje
  - Povoliť/zakázať premávku podľa bezpečnostných politík/pravidiel
- Typy pravidiel/politík
  - Zdroj/cieľová IP adresa, zdroj/cieľ rozhranie, port, protokol, stav spojenia, aplikačné dáta
  - Líši sa per vendor a per typ FW
- Limity
  - Neochráni pred všetkými hrozbami - insider threats, šifrovaná prevádzka
- Predpoklady správnej funkcie FW
  - Odolnosť voči útokom na seba
  - Zabezpečený OS a FW politika
  - Jediný tranzitný bod medzi sieťami (všetok traffic cez FW)
  - Implicitné blokovanie – povolené je len definované
- Realizácia
  - Hardvérový – najvyšší výkon a stabilita
  - Virtuálny – SW verzia ako VM
  - FWaaS – FW ako cloud služba
  - Softvérový/host – SW na servery / endpoint

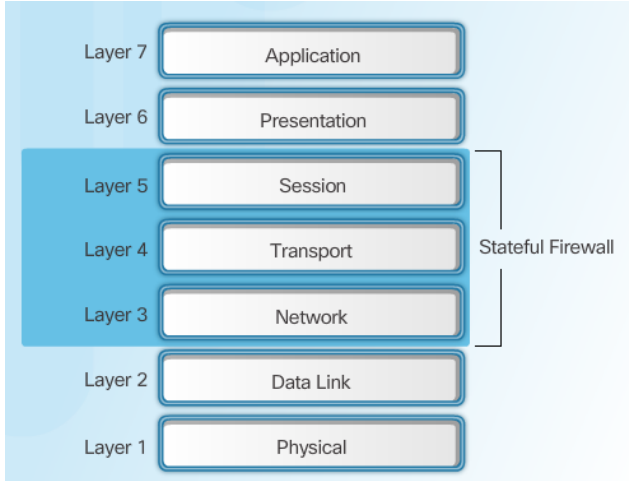
Typy sieťových Firewall-ov – základné členenie

- **Packet Filtering Firewall (stateless)**
  - Prvá generácia FW (80. roky)
  - Kontrola hlavičiek paketov (IP, port, protokol – 5-tuple)
  - Každý paket vyhodnocuje samostatne
  - Implementácia: ACL na routeroch, jednoduché firewally
  - Výhody
    - Nízka cena, vysoký výkon, jednoduchá konfigurácia
    - Stále v úlohe Edge/Screening FW
  - Nevýhody
    - Žiadny kontext spojenia, problémy s fragmentáciou, dynamickými portami
- **Statefull Firewall**
  - Druhá generácia FW (90. roky)
  - Sleduje stav spojenia (TCP 3-way handshake, UDP pseudo-session)
  - Udržiava *state table* pre každé spojenie
  - Automaticky povoľuje návratový traffic
  - Stále pomerne rozšírený
  - Výhody:
    - Vyššia bezpečnosť, ochrana pred spoofingom/DoS, jednoduchšie pravidlá
  - Nevýhody
    - Nevidí do aplikácií, problémy s niektorými protokolmi (VoIP, FTP), vyššie nároky na výkon

Packet Filtering Firewall

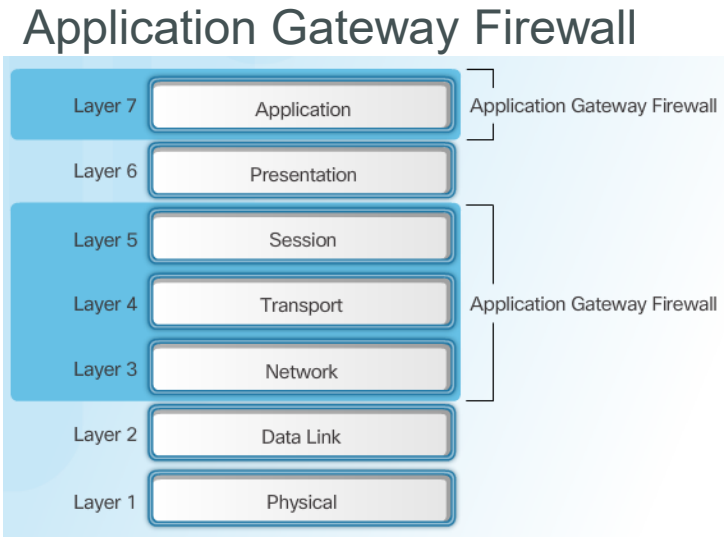


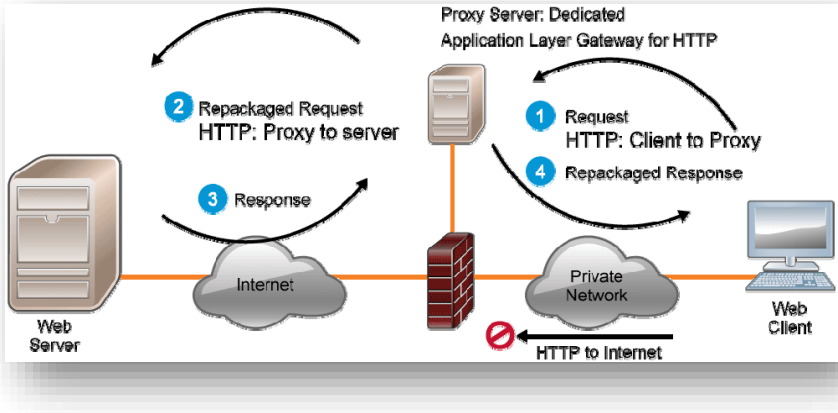
Stateful Firewall



Typy sieťových Firewall-ov – základné členenie

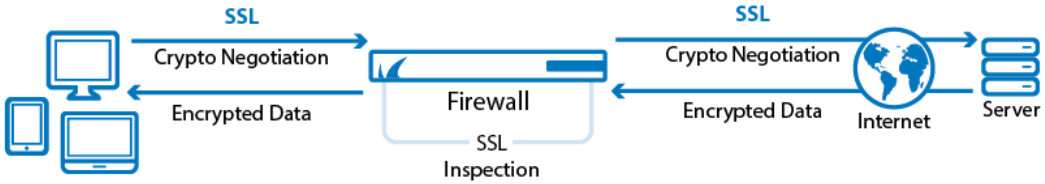
- **Application Gateway Firewall (Proxy, ALG. WAF):**
  - Tretia generácia FW – aplikačná vrstva (L7) – per protokol
  - Známy ako Proxy model: klient ↔ FW ↔ server
  - Detailná inšpekcia protokolov (HTTP, DNS, SMTP)
  - Podpora autentifikácie používateľov
  - **Výhody:** vysoká bezpečnosť, blokuje aplikačné útoky
  - **Nevýhody:** vysoká latencia, náročnejšie na výkon
- **Next-Generation Firewall (NGFW):**
  - L3-L7
  - Evolúcia stateful + application firewallov
  - Granulárna kontrola: používateľ, aplikácia, zariadenie, čas
  - **Výhody:** vysoká úroveň viditeľnosti a prevencie útokov
  - **Nevýhody:** cena, komplexná konfigurácia a správa





Funkcie Next Gen FW

- Funkcie moderného NGFW
  - Stateful inspection + packet filtering (základ FW)
  - Aplikačná viditeľnosť a kontrola (App-ID, User-ID, Device-ID)
  - IPS/IDS integrácia – detekcia a prevencia útokov
  - Deep Packet Inspection (DPI) – analýza obsahu paketov
  - SSL/TLS dešifrovanie a inspekcia (viditeľnosť do šifrovaného trafficu)
  - URL/DNS filtering – reputácia, kategórie domén, anti-phishing
  - Antimalware & sandboxing – ochrana proti zero-day hrozbám
  - Segmentácia a podpora VRF / mikrosegmentácia
  - Centralizovaný management a reporting (FMC, Panorama, FortiManager, …)
  - HA, clustering, cloud FW (AWS, Azure, GCP)
  - SandBoxing: izolované prostredie na nalýzu podozrivých súborov alebo kódu



- Botnet IP/Domain: blokovanie prístupu na známe škodlivé IP adresy a domény na základe reputačných databáz
- VPN koncentrátor: centralizované zariadenie/služba pre termináciu a správu veľkého počtu VPN spojení
- AntiVirus: kontrola na prítomnosť známeho malvéru
- GeoProtection: filtrovanie alebo blokovanie podľa geografického pôvodu IP adresy
- WebFirewall (WAF): ochrana webových aplikácií pred útokmi na aplikačnej vrstve (napr. SQLi, XSS)

NextGen Firewall Magic Quadrant - 2022

Source: Gartner (December 2022)

- Gartner Magic Quadrant
  - Grafický nástroj a analýza, publikovaná typicky ročne.
  - Používa sa na hodnotenie a porovnávanie spoločností v rôznych trhových odvetviach na základe ich schopnosti preukázaných výsledkov a stratégie v danej oblasti.
  - Používa sa v mnohých odvetviach
    - Aj technických, ale skôr investovanie
- Kvadranty
  - **Leaders (Líderi)**
    - Spoločnosti v tomto štvorci majú silný výkon a silnú schopnosť plniť budúce požiadavky trhu.
    - Obvykle inovatívny lídri v danej oblasti.
  - **Challengers (Vyzývatelia)**
    - Títo hráči majú silný výkon, ale možno im chýba inovácia alebo stratégia na výrazné posunutie na trhu.
  - **Visionaries (Víziári)**
    - Spoločnosti v tejto kategórii majú výraznú výhľadovú stratégiu a často inovujú, ale môžu mať problémy s aktuálnym výkonom.
  - **Niche Players (Špecialisti)**
    - **T**íto hráči sa zameriavajú na konkrétnu časť trhu a môžu mať silný výkon v obmedzenom kontexte, ale nie sú vo všetkom trhu konkurencieschopní.

Firewall riešenia - Open Source

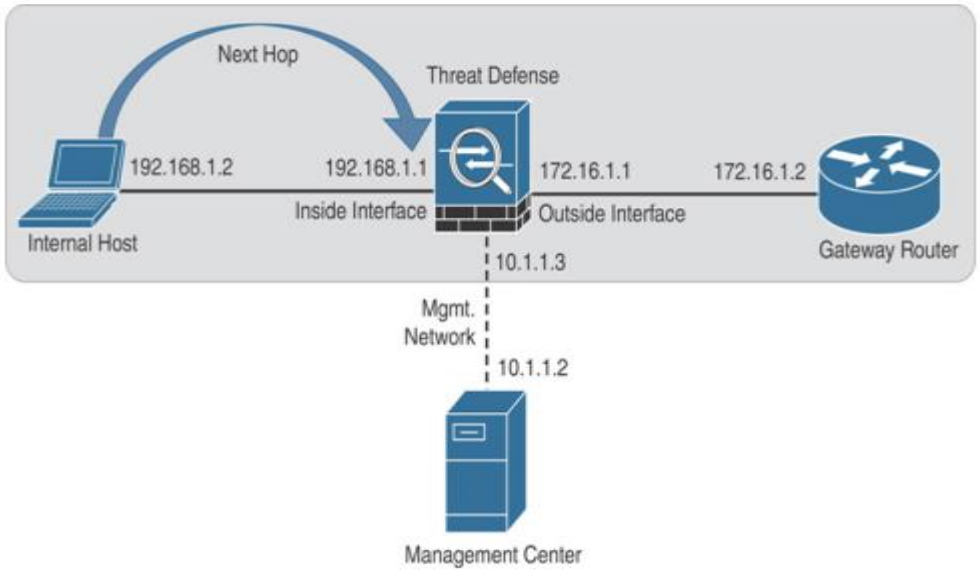
- pfSense https://www.pfsense.org/
  - open-source firewall a router riešenie založené na FreeBSD
  - ponúka aj HW
- OPNsense https://opnsense.org/
  - open-source firewall a bezpečnostná platforma postavená na FreeBSD
  - fork pfSense
  - ponúka rozsiahle bezpečnostné funkcie a používateľské rozhranie
  - GUI, dual stack, Multi WAN (LB a failover), HW failover (CARP protokol), VPN (OpenVPN, WireGuard), SD-WAN (ZeroTier), IDS/IPS (Suricata), dvojfaktorová autentifikácia, routing, web filtering, viacjazyčnosť
- iptables
  - klasický firewall nástroj pre Linux, umožňuje detailnú konfiguráciu spracovania sieťovej prevádzky
- Other (ostatné)
  - IPFire https://www.ipfire.org/
    - open-source firewall riešenie založené na Linux kerneli
    - známe pre svoju rýchlosť a jednoduchosť nasadenia
  - Untangle
    - open-source firewall riešenie s grafickým užívateľským rozhraním
    - poskytuje široký rozsah bezpečnostných funkcií
  - Smoothwall
    - open-source firewall a sieťová bezpečnostná platforma postavená na Linuxe
    - navrhnuté najmä pre malé a stredne veľké firmy
  - Firewalld
    - správca firewallu pre Linux
    - ponúka jednoduchú správu firewallu cez príkazový riadok alebo grafické rozhranie

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Firewall – módy nasadenia

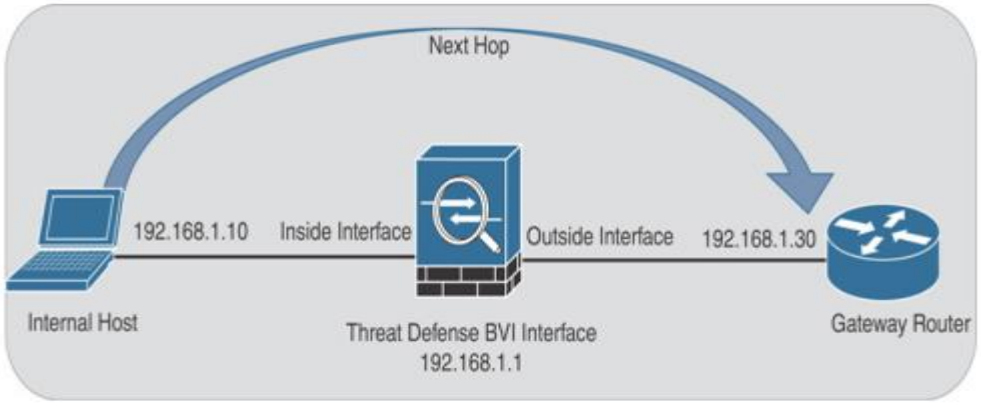
Routed mode

- Firewall pracuje na 3. vrstve (IP)
- Správa sa ako default gateway z pohľadu hostov
- Oddeluje podsiete (rôzne IP rozsahy)
- Často sa kombinuje s NAT (preklad adries)

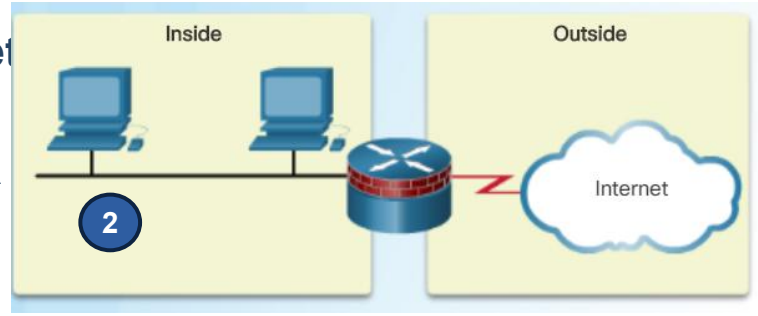


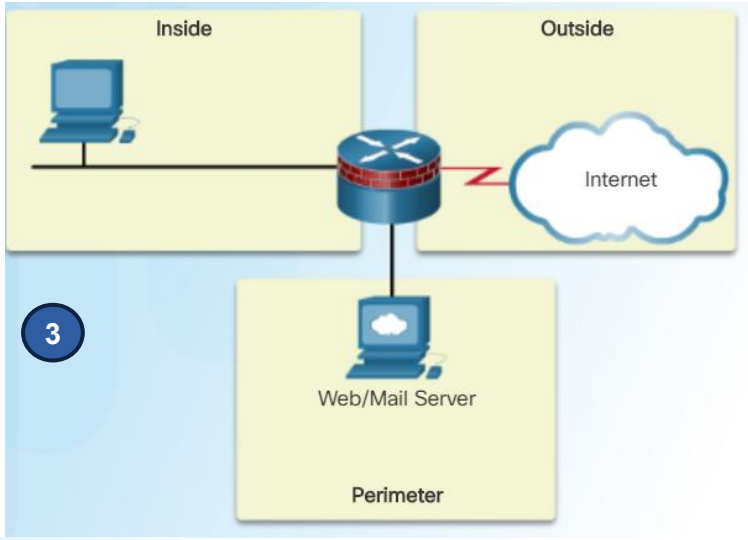
Transparent mode

- Firewall pracuje na 2. vrstve (Ethernet)
- Je „priehľadný“ – hosty ho nevnímajú ako gateway
- Preklenuje vnútornú a vonkajšiu sieť transparentne
- Nasadenie nevyžaduje preadresovanie siete

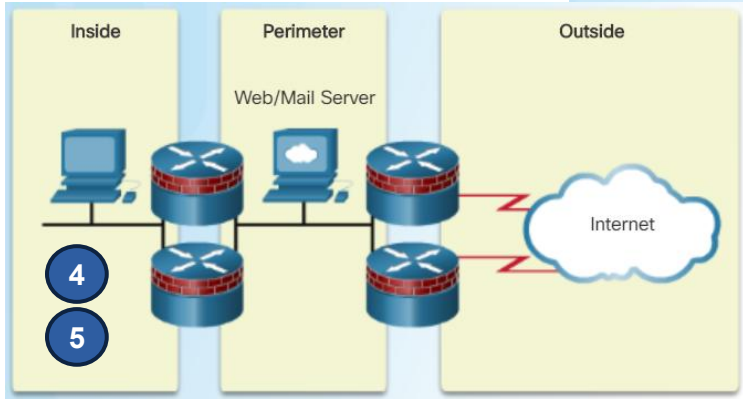


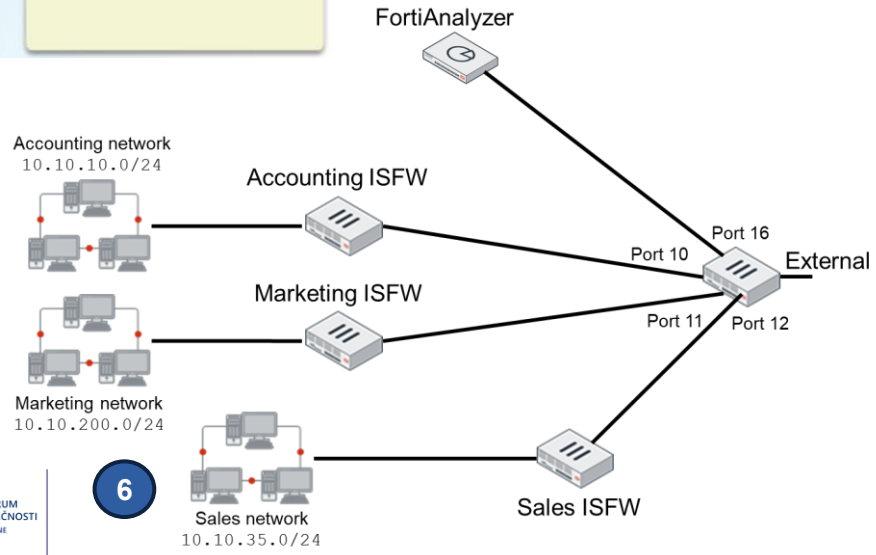
Modely nasadenia





1. **Model router on Stick**
2. **Jednoduchý Inside / outside**
3. **Klasický perimetrový model -** TrojZónový firewall s DMZ
4. **Obrana do Hĺbky: Dvojvrstvové Nasadenie (Back-to-Back Firewall)**
   - Ochrana na viacerých hraničných bodoch siete
5. **Redundantný firewall**
   - HA, clustering, failover pre dostupnosť a odolnosť
6. **Segmentation firewall (interný)**
   - oddelenie LAN/VLAN segmentov, mikrosegmentácia





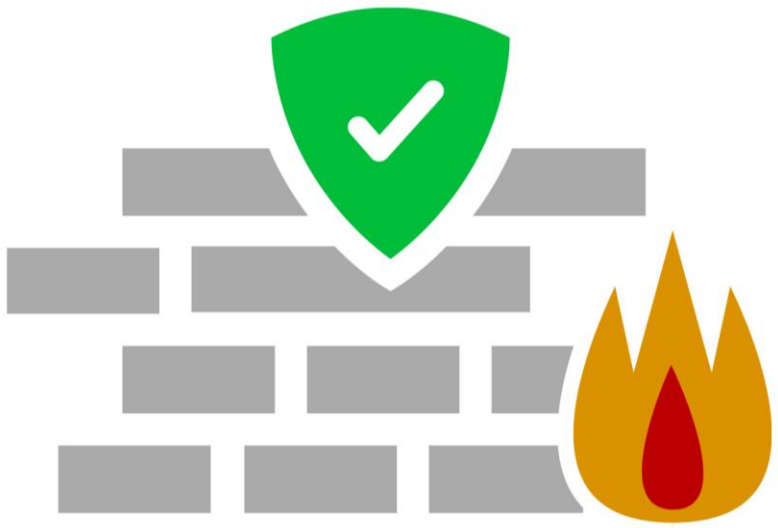
Benefity a obmedzenia FW

Benefity

- Sanitizácia protokolov – prevencia zneužitia chýb protokolov
- Ochrana citlivých hostov, zdrojov a aplikácií pred nedôveryhodnými používateľmi
- Blokovanie škodlivej prevádzky medzi servermi a klientmi
- Zníženie komplexity bezpečnostného manažmentu (centralizované riadenie prístupu)
- Platforma pre ďalšie perimeter funkcie (NAT, VPN, IPsec GW)
- Možnosť integrácie s inými bezpečnostnými technológiami (IDS/IPS, WAF, SIEM)

Obmedzenia

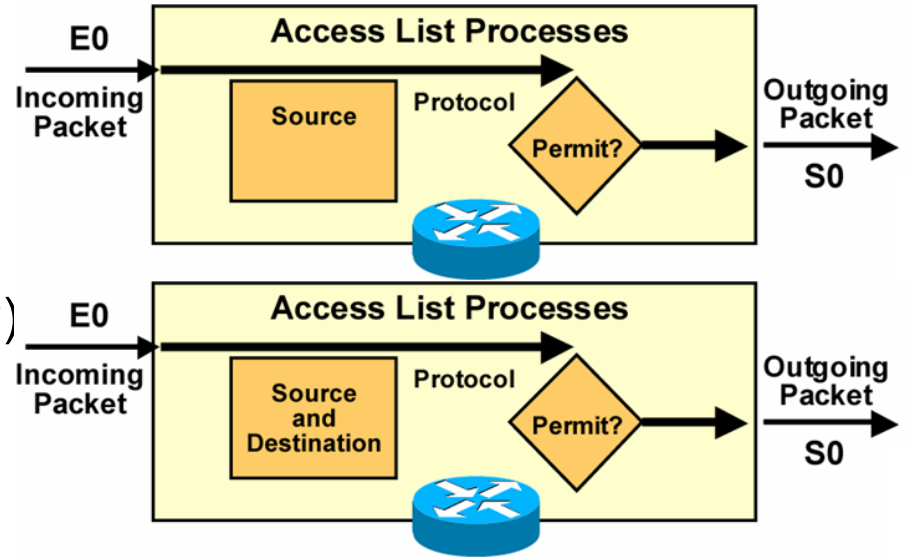
- Koncentrácia bezpečnostných funkcií – chybná konfigurácia má kritické dôsledky
- Single Point of Failure – bez HA môže výpadok zastaviť komunikáciu
- Zraniteľnosti softvéru – firewall je počítač, môže obsahovať CVE
- Výkonnostné limity – firewall môže byť bottleneck siete (priepustnosť, latencia)
- Nepokrýva všetky hrozby:
  - insider threats (útoky zvnútra)
  - obchádzanie pravidiel (tunneling, šifrovanie, proxy)
  - zámerné pokusy používateľov obísť blokovanie obsahu



Prístupové zoznamy ACL

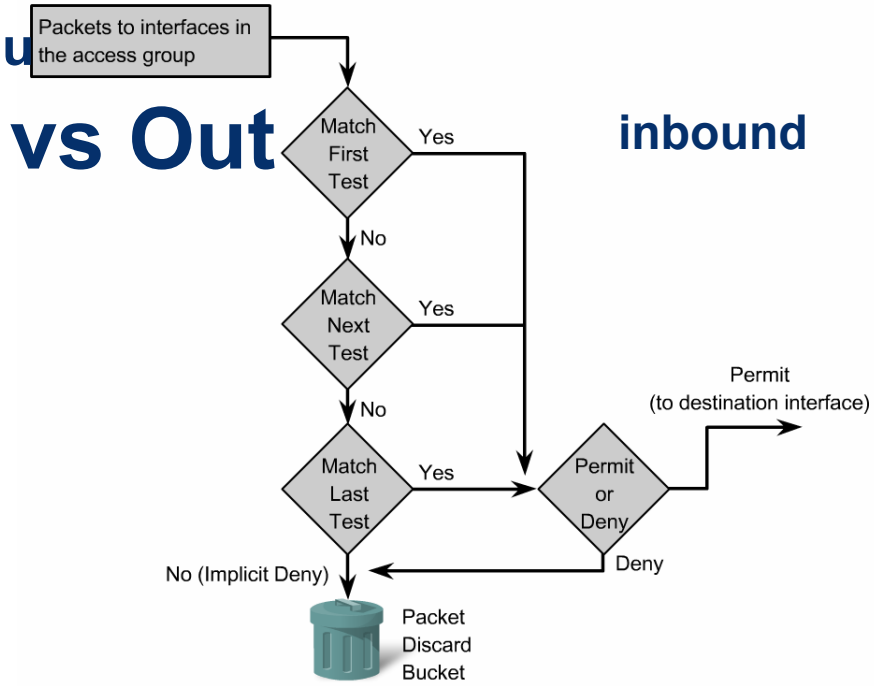
Prístupové zoznamy ACL - štandardné a rozšírené

- **ACL = základný firewall mechanizmus**
  - Najstarší a zároveň najpoužívanejší bezpečnostný mechanizmus
  - Veľmi rozšírený, často súčasť moderných security policies na NGFW
  - Sada pravidiel *permit/deny* pre sieťovú prevádzku
- **Štandardné ACL – L3**
  - filtrujú podľa zdrojovej IP adresy
  - jednoduché, menej flexibilné, typicky stateless
- **Rozšírené ACL – L3/L4**
  - filtrujú podľa: zdroj/cieľová IP, protokol (TCP/UDP/ICMP) porty
  - vyššia granularita a kontrola
  - Podľa implementácie stateless aj statefull
- **Použitie ACL**
  - routery a L3 switche (Cisco IOS, Juniper, Huawei)
  - OS firewally (Linux iptables/nftables, Windows Firewall)
  - cloud security groups (AWS, Azure, GCP)
  - dokonca aplikácie (AppLockers)
- **Výhody:** rýchle, jednoduché, efektívne, široká podpora
- **Limity:** manuálna správa, komplexnosť vo veľkých prostrediach

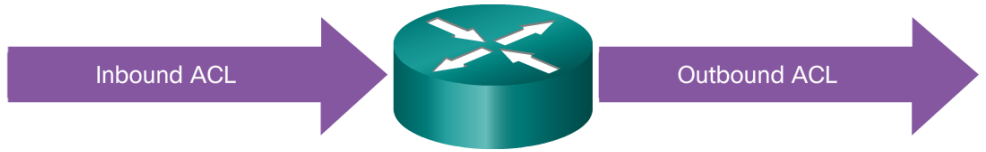


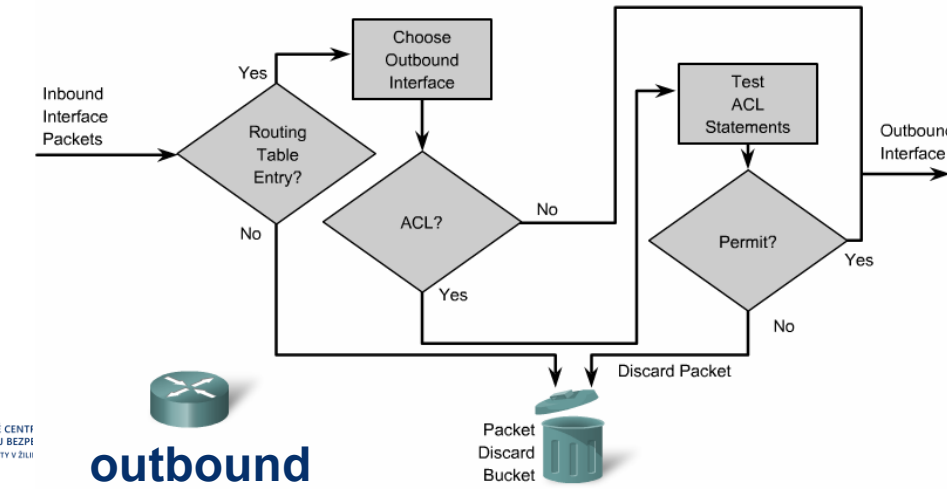
Prístupové zoznamy ACL – In vs Out

- ACL = zoznam podmienok (ACEs Access Control Entries = ACL statements)
  - Aplikujú sa na IP prevádzku prechádzajúcu rozhraniami smerovača/FW
- Každý záznam obsahuje **testovaciu podmienku** a **akciu**, ktorá sa má vykonať
- Zoznam je prehľadávaný sekvenčne
  - Ak je zhoda na podmienku vykoná sa akcia
    - paket je povolený (permit)
    - alebo zahodený (deny)
- Pri zhode podmienky už ďalej nepokračujem
- Ak nenájdem ani jednu podmienku
  - Použije sa default akcia na konci ACL
    deny any



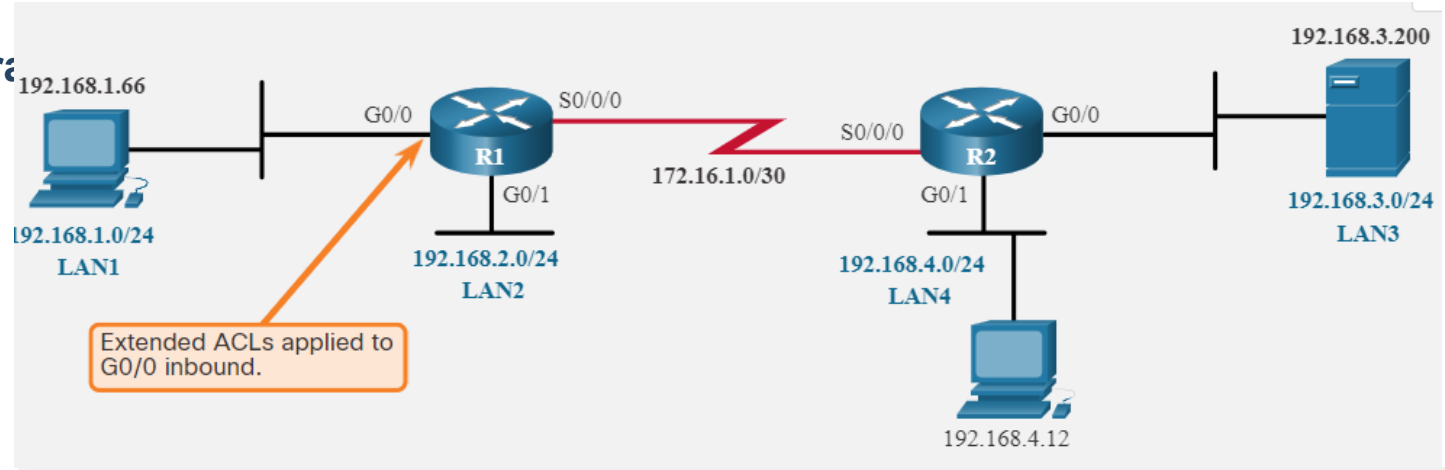
inbound





outbound

Aktivita




```
access-list 105 permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.200 eq 80
access-list 105 permit ip host 192.168.1.66 host 192.168.3.200
access-list 105 permit tcp 192.168.1.0 0.0.0.255 host 192.168.4.12 eq 22
access-list 105 permit tcp host 192.168.1.66 192.168.2.0 0.0.0.255 eq 23
```

Source	Destination	Protocol
192.168.1.67	192.168.2.88	http
192.168.1.66	192.168.4.12	ssh
192.168.1.77	192.168.3.75	http
192.168.1.66	192.168.2.75	telnet
192.168.1.77	192.168.2.75	telnet
192.168.1.66	192.168.3.200	telnet

Permit or deny?

Best practise ACL a FW Rules (security policies)

- **Implicitné "Zakáž všetko" (Implicit Deny All**
  - Každé ACL má na konci implicitné *deny all* – teda čo nie je povolené, je blokované
  - Ak nie, tak to zabezpeč
- **Sekvenčné vyhodnocovanie (Top-Down Processing)**
  - Pravidlá sa spracovávajú **zhora nadol**
  - Prvé zhodné sa uplatní a ďalej sa nepokračuje
  - => Umiestňuj **najšpecifickejšie podmienky na vrchu ACL**
- **Umiestnenie a smer (Placement and Direction)**
  - Štandardné ACL – bližšie k cieľu, aby sa znížilo riziko blokovania iných komunikácií
  - Rozšírené ACL – bližšie k zdroju, aby sa blokovaná komunikácia odfiltrovala čo najskôr
- Nové pravidlá sa defaultne pridávajú na koniec zoznamu
- **Cisco špecifiká**
  - Prevádzka generovaná samotným routerom (napr. ICMP echo reply, OSPF hello) sa outbound ACL nefiltruje
  - **Jedno pravidlo pre jednu vec**
    - Na danom rozhraní (fyzickom, virtuálnom) a v danom smere (inbound/outbound) platí v jeden moment len jedna sada pravidiel pre daný protokol

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

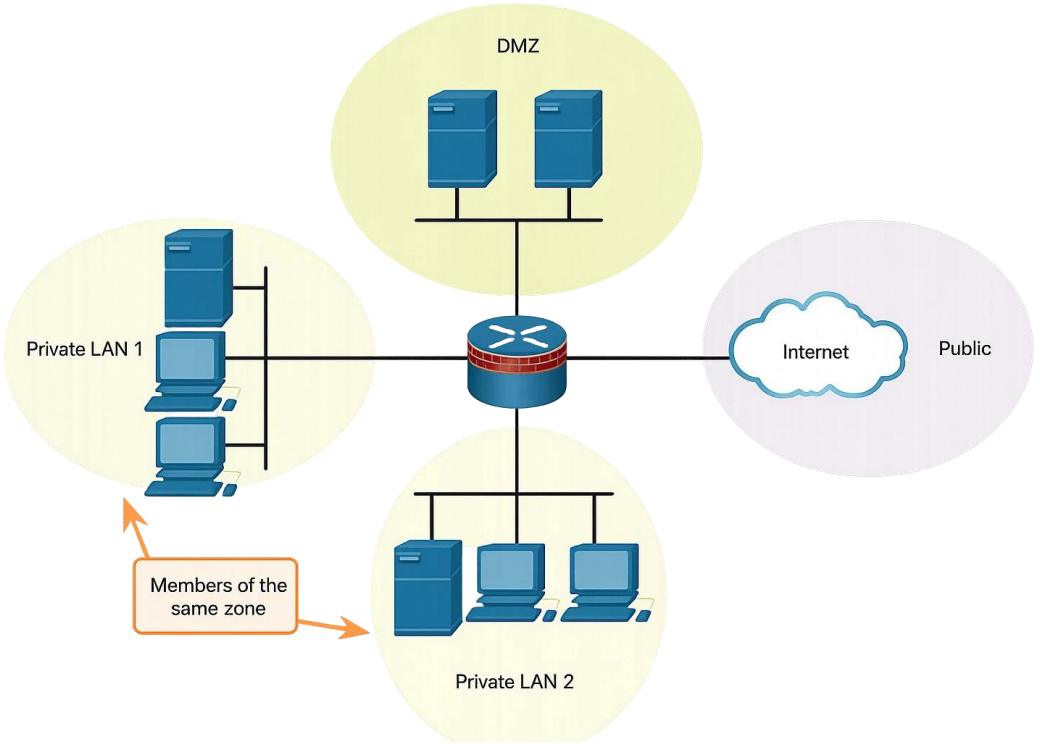
Riziká nekonzistentných ACL (router/FW)

- **ACL Inconsistency =** Nezhody v pravidlách
- **Riziká:**
  - Neautorizovaný prístup kvôli chybám
  - Zníženie dostupnosti služieb (falošné blokovanie)
  - Zraniteľnosť voči útokom (napr. bypass)
- **Príčiny:**
  - Ručná konfigurácia bez synchronizácie
  - Nedostatočné testovanie zmien
- **Prevencia:**
  - Centralizovaná správa (napr. FortiManager)
  - Automatické testovanie pravidiel pred nasadením
  - Pravidelné audity a logovanie zmien

- **Kategórie**
  - **Príliš voľné pravidlá (promiscuous rules)**
    - `permit ip any any` → umožní viac prístupu než je potrebné
  - **Redundantné pravidlá**
    - duplicitné alebo zbytočné položky, predlžujú ACL a komplikujú správu
  - **Shadowed rules (zatienené pravidlá)**
    - špecifické pravidlo nikdy neplatí, lebo je prepísané všeobecnejším pravidlom vyššie
  - **Orphaned rules (sirotské pravidlá)**
    - odkazujú na IP/protokoly, ktoré v sieti neexistujú → nikdy sa neuplatnia
  - **Nesprávne plánované pravidlá**
    - nepresný preklad biznis požiadaviek na technické ACL, chýbajúca analýza protokolov/portov
  - **Nesprávne implementované pravidlá**
    - chyba administrátora pri zadávaní IP, portu alebo protokolu

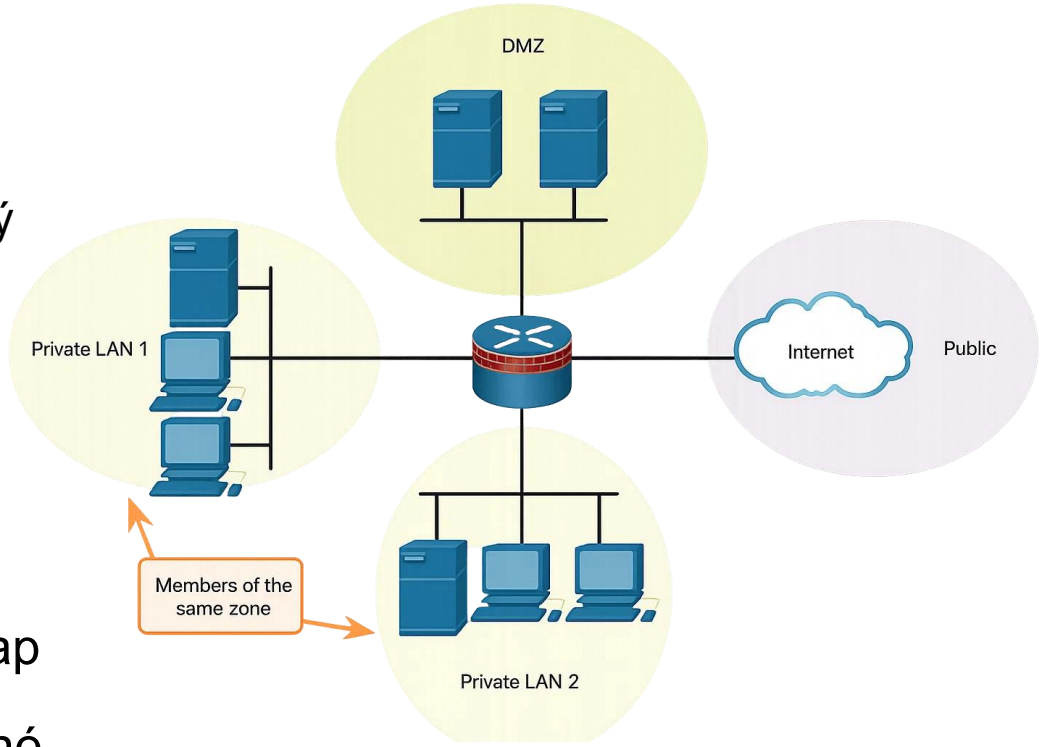
Zone-Based Firewall (ZBF): Koncept zón a vendor prístup

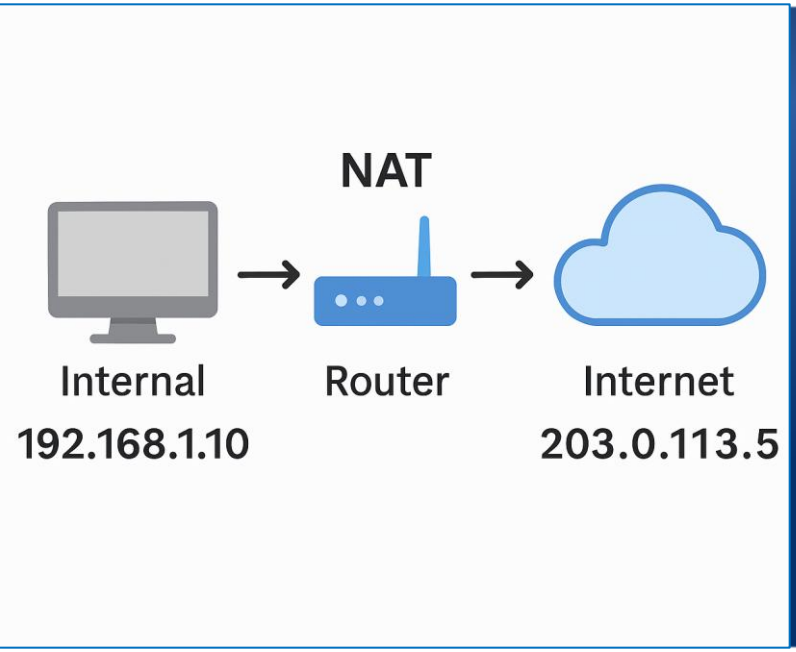
- **Cisco IOS/IOS-XE feature** – Zone-Based Policy Firewall
  - Evolúcia ACL a CBAC (Context-Based Access Control) k plnému stavovému FW
  - Namiesto manuál priradenia ACL => bezpečnostná zóna
- **Logika zón**
  - Rozhrania priradené do zón (Inside, Outside, DMZ, Self)
  - Prevádzka v rámci zóny = voľná
  - Prevádzka medzi zónami = blokovaná, kým nie je definované zónový pár a policy
  - Handling paketov je Statefull
- **Princíp zón je generický** – používajú ho všetci veľkí vendori:
  - Cisco IOS: Zone-Based Firewall (class-map/policy-map/zone-pair)
  - Juniper SRX: security zones + policies
  - Palo Alto: zones + security policies (App-ID, User-ID)
  - Fortinet: interface groups + policies



ZBF: Policies a výhody (cisco)

- **Filozofia**
  - Class-map: vyber prevádzku (ACL or proto)
  - Policy-maps: vykonaj akciu
    - **inspect** – stavová kontrola, dynamicky povoľuje návratový traffic
    - **pass** – povolí bez inšpekcie
    - **drop** – zablokuje (implicit default)
    - **log** – zapisuje udalosti
  - Service-map: aplikuj na zónový pař
- **Výhody ZBF oproti ACL/CBAC:**
  - default *deny* medzi zónami (bezpečnejšie)
  - jednoduchšia konfigurácia a troubleshooting (class-map / policy-map / service-policy)
  - lepšia granularita (protocol ID, L7 inšpekcia pre vybrané služby)
  - podpora VRF, transparentný mód, integrácia so QoS a policy routing
- **Príklady zón:** Inside, Outside, DMZ, Self-zone (prevádzka smerom na router)

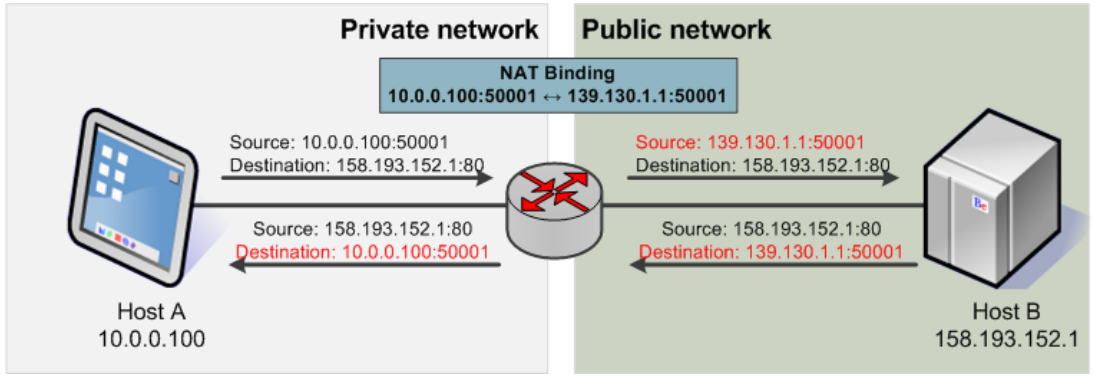




Network Address Translation (NAT)

NAT (Network Address Translation)

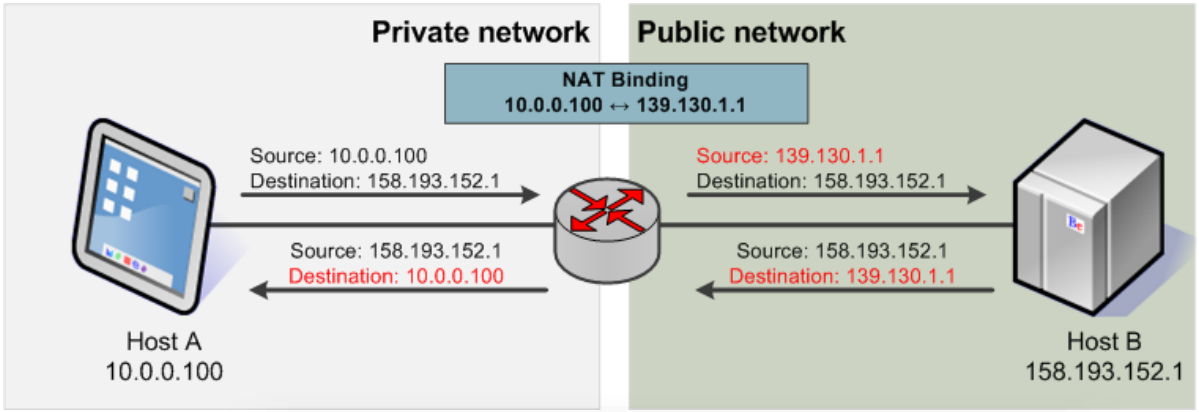
- **NAT (Network Address Translation)**
  - Preklad privátnych IP adries na verejné pri prechode medzi privátnou a verejnou sieťou
  - Vznikol ako riešenie nedostatku IPv4 adries
  - Typicky súčasť **perimeter dizajnu** (router / firewall)
- **Princíp činnosti**
  - Odchádzajúci paket z privátnej siete
  - Preklad zdrojovej IP (a portu) na verejnú adresu
  - Stavové mapovanie v NAT tabuľke
- **Typy NAT**
  - **Static NAT (1:1)** – publikovanie serverov (DMZ)
  - **Dynamic NAT (pool)** – dočasné mapovanie
  - **PAT / NAPT** – zdieľanie jednej verejnej IP viacerými hostmi

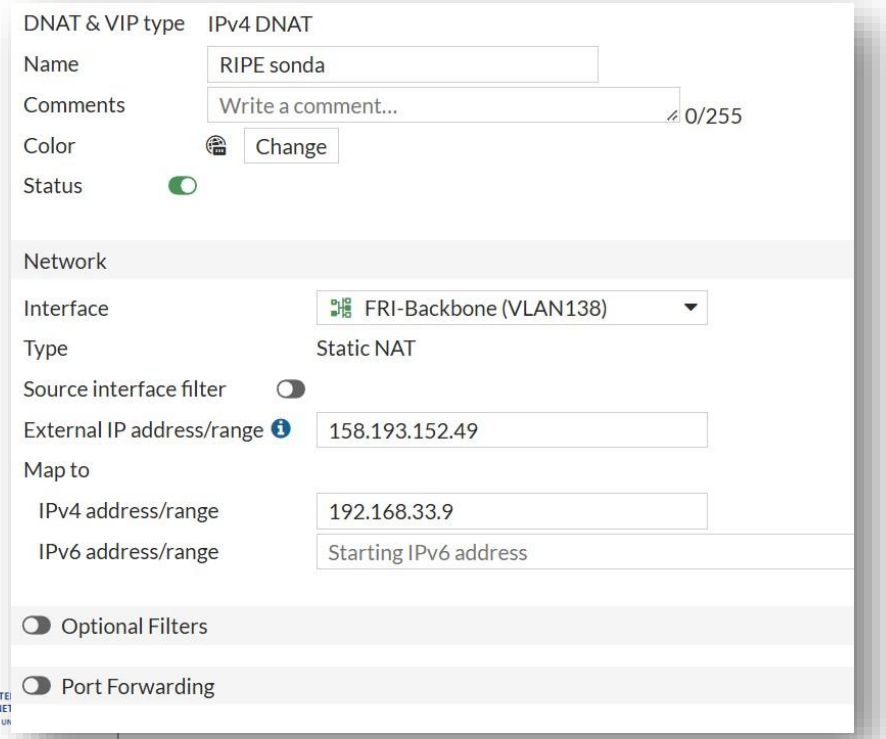


- **Kľúčové pojmy**
  - Inside/Outside, Local/Global (Cisco)
  - SNAT (Source NAT), DNAT (Destination NAT) – vendor-neutral

Statický NAT (1:1) / DNAT – použitie v perimeter dizajne

- Pevné mapovanie privátnej ↔ verejnej IP adresy
- **Vlastnosti**
  - transparentné pre klientov aj servery
  - preklad je **trvalý a predvídateľný**
- **Použitie**
  - publikovanie serverov v DMZ (web, mail, VPN)
  - prístup zvonku na konkrétny vnútorný host aj obrátene
- **Vendor-neutral pojmy**
  - DNAT (Destination NAT): preklad cieľovej adresy (publikovanie služieb, inbound) (linux, Forti)
  - Bi-directional NAT or Two-way NAT (RFC)
- **Výhody**
  - konzistentná adresa – vhodná pre DNS a služby
  - jednoduché na pochopenie a troubleshooting
- **Nevýhody:**
  - spotreba verejných IP (1:1)
  - neškáluje vo veľkých sieťach





NAT a bezpečnosť / problémy

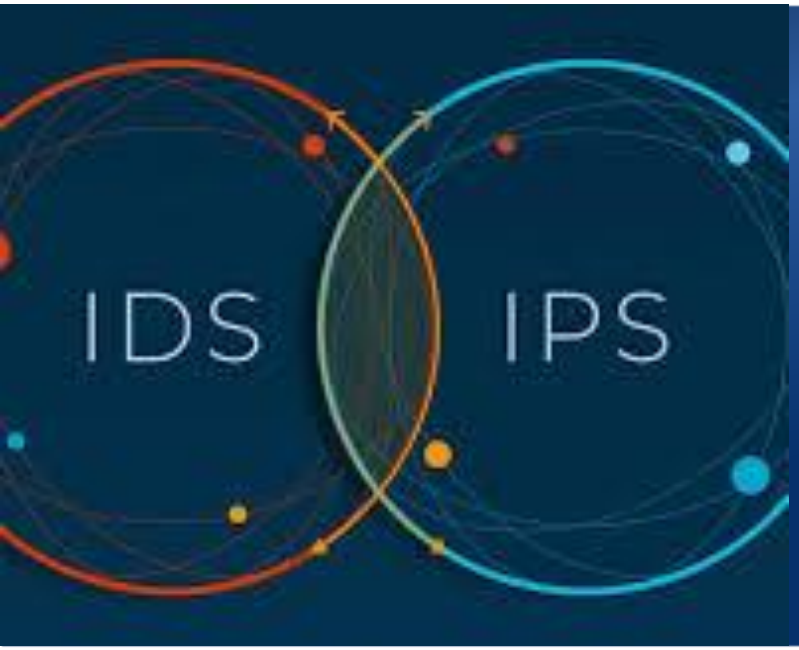
Výhody NAT

- Maskovanie vnútorných adries (topology hiding)
- Úspora verejných IPv4 adries
- Flexibilita pri zmene ISP alebo adresného plánu
- Považovaný za light security mechanizmus
- Môže byť súčasť FW policy

- **IPv6 pohľad:**
  - NAT nie je potrebný (dostatok adries)
  - NAT64/NAT46 ako prechodová technika medzi IPv6 ↔ IPv4
  - NAT66 - NAT medzi dvomi IPv6 sieťami

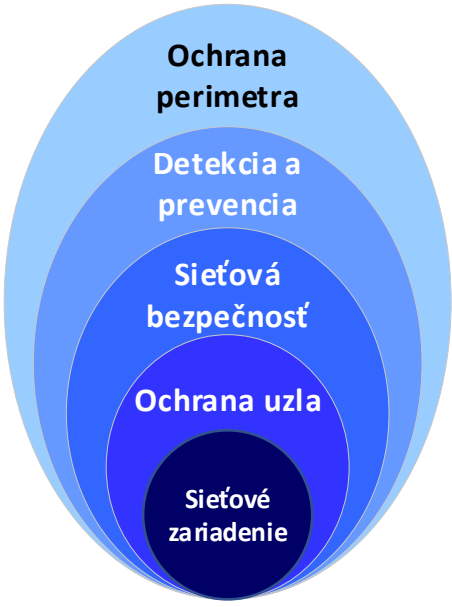
Nevýhody a problémy

- Narúša **end-to-end princíp** internetu (RFC 1958)
- Inbound spojenia nefungujú bez DNAT / statických mapovaní
- **Časovo obmedzené dynamické mapovania** – po vypršaní spojenie padá
- Komplikácie s protokolmi, ktoré vkladajú IP adresu do payloadu (SIP, FTP, H.323)
- Problémy s multimédiami a VoIP pri symetrickej implementácii NAT → potreba NAT traversal (STUN, TURN, ICE, ALG, SBC)
- Vyššia latencia a záťaž na NAT zariadenie (checksum recompute, port allocation)
- Treba riešiť v IPsec



Detekcia a prevencia (Hĺbková inšpekcia) - Intrusion Detection and Prevention System (IDS/IPS)

IDS/IPS



Zerodays útoky

- **Hrozby mimo dosahu firewallu**
  - Zero-day útoky, neznáme exploity zneužívajúce zraniteľnosti aplikácií (nemajú signatúru)
  - Timeline (potencionálny)
- **Vydanie antivírusovej signatúry – typický priebeh**
  - **Zachytenie malvéru (Day 0–1)**
    - Malvér využívajúci zero-day je zachytený v honeypotoch, sandboxoch alebo od používateľov
  - **Reverzná analýza (1–3 dni)**
    - Bezpečnostní analytici skúmajú binárny kód, správanie, C2 komunikáciu.
    - Identifikujú unikátne znaky (hash, heuristika, správanie) / IOC
  - **Vytvorenie signatúry (1–5 dní)**
    - Vzniká signatúra pre AV engine (napr. hash, YARA pravidlo, heuristická detekcia).
    - V prípade polymorfného malvéru sa používajú **behaviorálne alebo AI-based detekcie**.
  - **Distribúcia signatúry**
    - Aktualizácia AV databáz (často **do 24 hodín** od identifikácie).
    - Cloudové AV systémy (napr. Microsoft Defender, CrowdStrike) reagujú **takmer okamžite**
- **Vydanie patch-u**
  - **Objavenie zraniteľnosti (Day 0)**
    - Môže ju objaviť výskumník, bezpečnostná firma alebo útočník
    - Ak je zodpovedne nahlásená, ide o tzv. **responsible disclosure**
    - Ak je zneužívaná bez vedomia výrobcu, ide o **true zero-day exploit**
  - **Analýza a potvrdenie (1–7 dní)**
    - Výrobca softvéru analyzuje chybu, overuje jej dopad
    - Paralelne môže prebiehať **reverzná analýza malvéru** bezpečnostnými firmami
  - **Vývoj opravy (patchu) (7–90 dní)**
    - Kritické chyby: patch do niekoľkých dní (napr. 24–72 hodín)
    - Menej závažné: patch v rámci pravidelného cyklu (napr. Patch Tuesday)
    - Testovanie je kľúčové – zlá oprava môže spôsobiť nové problémy
  - **Vydanie patchu**
    - Výrobca vydá aktualizáciu softvéru
    - Zraniteľnosť je často zverejnená (CVE ID) spolu s patchom

Zerodays útoky - prístupy a riešenia

- **Monitorovanie a log analýza**
  - Zber a korelácia udalostí (FW, servery, aplikácie)
  - Časovo náročné, manuálne, menej škálovateľné
  - **=> SIEM** pomáha pri automatizácii a korelácii
- **Tradičné AV (signatúrne)**
  - Neúčinné proti zero-day útokom, kým nevznikne a nerozšíri sa signatúra
- **Moderné riešenia (EDR/XDR)**
  - **Behaviorálna analýza** – blokovanie typických činností malvéru (šifrovanie, zmena boot sektora)
  - **Machine Learning / AI** – detekcia podozrivých vzorcov v kóde a správaní
  - **Cloudová analýza** – rýchle zdieľanie hrozieb a ochrana celej základne
- **Zero Trust prístup**
  - Minimalizuje škody aj pri prelomení ochrany
  - Kontinuálne overovanie identity a integrity zariadení
- **IDS/IPS v kontexte**
  - IDS/IPS = dôležitá vrstva (ale nie všeliek)
- Reálna ochrana = kombinácia AV/EDR, IDS/IPS, SIEM, Zero Trust

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

IDS vs IPS

IDS – Intrusion Detection System	IPS – Intrusion Prevention System
Pasívne zariadenie, traffic len monitoruje	Inline zariadenie, traffic cez neho prechádza
Analyzuje kópiu prevádzky (SPAN, TAP)	Kontroluje reálnu prevádzku v reálnom čase. Vie zastaviť init paket útoku.
Deteguje podozrivé vzorce. Vykonáva Deep packet inspection (DPI).	
Generuje **alerty, logy, SNMP trapy.**	Aktívne reaguje: **Drop, Reset, Deny flow, Log**
Žiadny vplyv na latenciu a dostupnosť	Môže zvýšiť latenciu a byť bottleneck
Žiadny vplyv na sieť v prípade zlyhania	
Poskytuje viditeľnosť, ale neblokuje priamo útok. Môže spolupracovať s FW na blokovaní.	Znižuje riziko útokov, ale prináša výkonovú záťaž
Vhodné na **monitoring, forenznú analýzu**	Vhodné na **prevenciu, blokovanie útokov**
Riziko: ignorovanie alertov (alert fatigue)	Riziko: falošné pozitíva = blokovanie legitímnej prevádzky

Typy IDS/IPS: Host vs. Net

HIDS (Host-based IDS)

- Nasadené priamo na hostovi (server, PC)
- Monitoruje logy, súbory, systémové volania, procesy, zmeny v registroch, spúšťanie inštalátorov
- Deteguje podozrivé zmeny v OS alebo aplikáciách
- **Výhody**: detailná aplikačná viditeľnosť, detekcia insider útokov, podpora špecifického OS, ochrana OS aj app
- **Nevýhody**: závislé na OS, vysoké nároky na hosta, musí byť na každom hostovy, menej efektívne pri sieťových útokoch

NIDS (Network-based IDS)

- Nasadené v sieti (senzory na segmentoch, SPAN/TAP)
- Monitoruje sieťovú prevádzku v reálnom čase
- Deteguje útoky, scanning, DoS/DDoS, exploity
- **Výhody**: centrálna viditeľnosť, detekcia sieťových hrozieb, nezávislý od OS hosta
- **Nevýhody**: nevidí do šifrovanej prevádzky (nové AI prístupy), možnosť preťaženia pri vysokých rýchlostiach

Techniky detekcie v moderných IPS

Detekčné prístupy (čo hľadám?)

- **Signatúrová detekcia (Signature-based or Pattern-Based)**
  - porovnávanie paketov/sekvencií so signatúrami (napr. HTTP payload)
  - + rýchla, presná, nízke false-positive
  - – slabá proti zero-day (kým nevznikne signatúra)
- **Heuristická analýza (Anomaly-Based)**
  - normálny profil + štatistika + kontrola „či je komunikácia legit“
  - hľadá neštandardné hlavičky/payloady/sekvencie príkazov
  - **+** odhalí aj varianty známych útokov
  - **–** vyššie riziko false-positive → tuning
- **Behaviorálna (Behavior-based)**
  - sleduje správanie systémov a aplikácií v čase (sekvencie akcií)
  - anomálie: neobvyklé prístupy, zmeny súborov, spúšťanie procesov
  - **+** vie zachytiť „nové“ útoky podľa správania
- **Policy / Rule-based**
  - povolené správanie definované politikou; mimo politiky = alarm
  - využíva prahy/historické dáta (napr. počet skenovaných portov)
  - **–** náročné na návrh pravidiel a znalosť prevádzky

Pokročilé mechanizmy (ako zvýšim pokrytie?)

- **DPI – Deep Packet Inspection (L7)**
  - analýza celého obsahu (nielen hlavičiek)
  - detekcia aplikačných útokov (SQLi, XSS)
  - často vyžaduje **SSL/TLS inšpekciu**
- **Sandboxing**
  - izolované spustenie podozrivého kódu
  - sleduje správanie typické pre malvér (exfiltrácia, zmeny v registri)
  - najmä pre súbory a e-mail prílohy
- **Strojové učenie / AI (NGIPS)**
  - tréning na veľkých datasetoch, adaptácia na nové hrozby
  - detekcia „podobností vzorcov“ mimo klasických signatúr
- **Threat Intelligence integrácia**
  - napojenie na databázy hrozieb (Talos, VirusTotal, MISP)
  - rýchle aktualizácie signatúr a IOC
  - lepšia reakcia na zero-day, ktorý sa objaví inde

Výhody a nevýhody IDS/IPS

Výhody IDS/IPS:

- Detekcia útokov, ktoré firewall nevidí (napr. aplikačné exploity, zero-day)
- Analýza na úrovni paketu (atomic) či toku (composite)
- Možnosť reagovať na hrozby v reálnom čase (IPS)
- Forenzná hodnota – logy, alerty, korelácia so SIEM
- Zvyšuje úroveň viditeľnosti v sieti
- Dopĺňa model *Defense in Depth*

Nevýhody IDS/IPS:

- IDS: detekcia bez prevencie → riziko ignorovania alertov (alert fatigue)
- IPS: riziko falošných pozitív → blokovanie legitímnej prevádzky
- Výkonová záťaž pri vysokých rýchlostiach siete (latencia, throughput)
- Potreba pravidelných aktualizácií signatúr a tuningu

- **Samostatné vs. integrované riešenia:**
  - **Samostatné IDS/IPS:** vyššia flexibilita, špecializovaná funkčnosť, možnosť nasadenia len ako monitoring, vhodné pre väčšie siete
  - **FW s IDS/IPS modulom (NGFW/UTM):** jednoduchšia správa, ale zdieľa výkonové zdroje s firewallom
  - IDS/IPS sú efektívne **ako doplnok k firewallu**, nie jeho náhrada

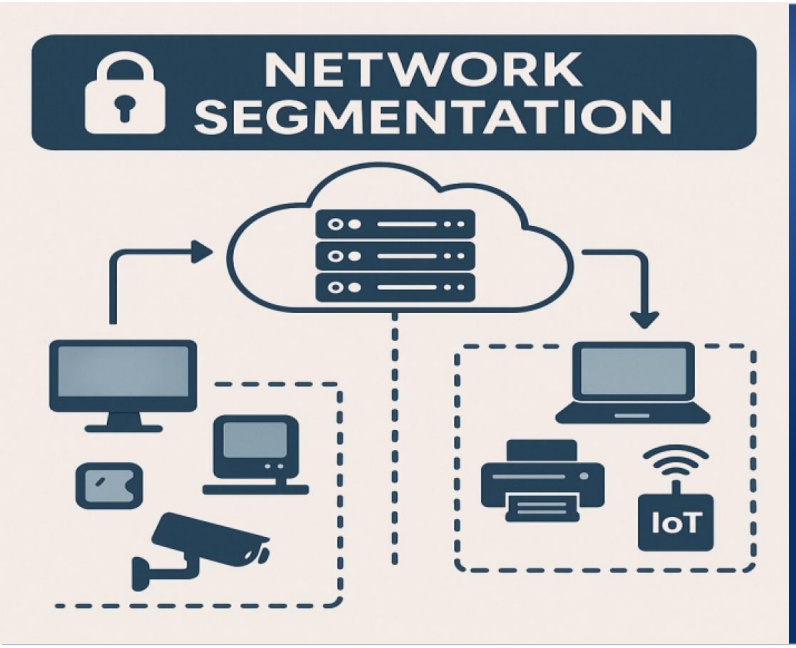
IDS/IPS v sieťovej ochrane DiD - best practise

- **Sieť (NIDS/NIPS):** Pohľad zhora na celok/celú sieť
  - *Hranica (Internet Edge), Interná segmentácia, Core (span port)*
  - IDS senzory: Perimeter, core, DMZ (napr. TAP porty)
  - IPS inline: Pred kritickými systémami (DC, externé služby)
  - Cloud: Flow-based monitoring (napr. AWS VPC)
  - **Detekuje:** Scans, DDoS, známy malware premávku
- **Hostiteľ (HIDS/HIPS):** Pohľad zvnútra - detail
  - *Servery, kritické workstations.*
  - **Detekuje:** Rootkity, zmeny súborov, privilege escalation. **Vidí zašifrovanú premávku**
- **Aplikácia (WAF):** Pohľad na transakcie
  - *Inline pred webovými aplikáciami*
  - **Detekuje:** Špecializuje sa na útoky na aplikačnej vrstve, ako napríklad SQLi alebo XSS

- **Aktualizácie a tuning**
  - Signatúry: Vendor/komunitné feedy (Snort)
  - Tuning: Minimalizácia falošných pozitív Automatizácia: SOAR, testovanie v sandboxe
- **Integrácia so SIEM**
  - Centralizovaný zber logov, korelácia
  - Real-time analytics a XDR integrácia
  - Playbooky pre incident response
- **Výkonnostné aspekty**
  - Dimenzovanie: Throughput, latencia
  - Redundancia: HA cluster, bypass mode (s monitoringom)
  - Škálovateľnosť: Load balancing

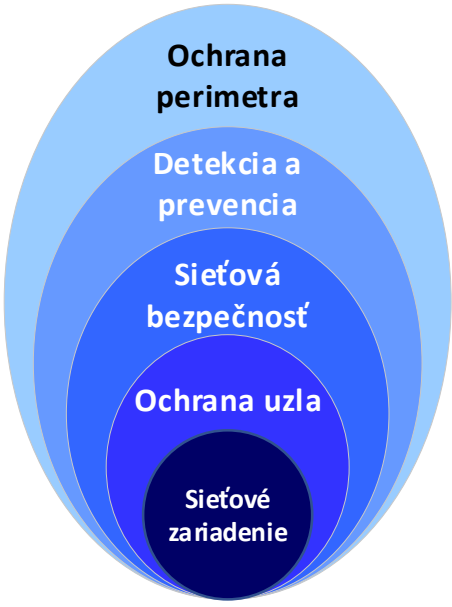
IDS/IPS: Open-source vs. Komerčné riešenia

- **Open-source riešenia:**
  - **Snort (Cisco Talos):** Najznámejší open-source NIDS/IPS, signatúry + heuristika, komunitné a komerčné pravidlá.
  - **Suricata (OISF):** Moderný IDS/IPS, multithreading, DPI, JSON logy, integrácia so SIEM (ELK, Splunk).
  - **Wazuh/OSSEC:** HIDS pre logy, súbory a procesy, vhodné na host monitoring a compliance.
- **Komerčné riešenia:**
  - **Cisco Firepower / Secure IPS (NGIPS):** Inline IPS, Snort engine, signatúry od Talos, centralizovaná správa.
  - **Palo Alto Threat Prevention:** IPS funkcie v NGFW, App-ID, User-ID, cloud sandboxing (WildFire).
  - **Fortinet FortiGate IPS:** IPS modul v NGFW, správa cez FortiManager, HW akcelerácia.
  - **Trend Micro TippingPoint:** Špecializovaný IPS, silný v enterprise a telco prostrediach
  - TripWire



Network Security - Sieťová bezpečnosť

Segmentácia VLAN/VRF
Mikrosegmentácia
Access Layer Security

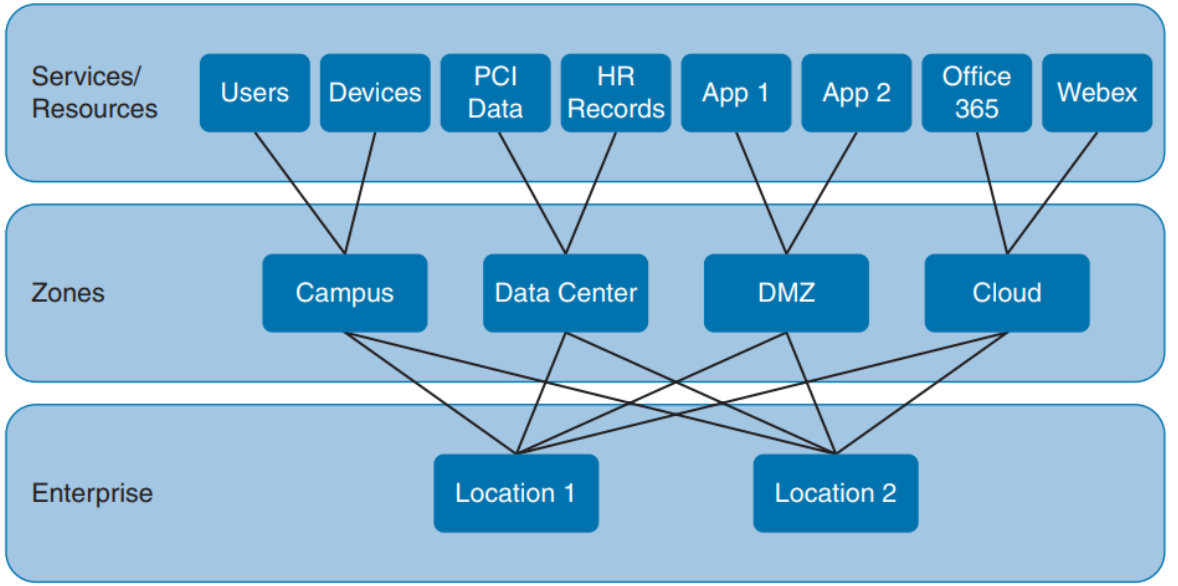


Segmentácia

- Segmentácia =
  - logické zgrupovanie aktív/zdrojov
  - riadenie komunikácie medzi zónami a objektmi,
- Ponúka flexibilitu
  - Implementácia rôznych služieb
  - S rôznymi autentifikačnými požiadavkami
  - A bezpečnostnými kontrolami
- Bežné zóny/segmenty
  - **Untrusted Network (Internet)**
    - Externá sieť mimo kontroly organizácie. Najvyššie riziko.
  - **DMZ (Semi-Trusted)**
    - Obsahuje servery prístupné z Internetu (web, mail)
    - Chránená perimeter firwallom
  - **Trusted Network**
    - Interná LAN pre zamestnancov
    - Prístup len pre autorizovaných používateľov
  - **Enclave Network**
    - Izolovaná zóna pre citlivé systémy a dáta
    - Prístup len cez VPN + MFA
  - **Guest Network**
    - Pre návštevníkov, iba Internet prístup, žiadny prístup do internej siete

Ako segmentovať

- **Zber dát (viditeľnosť)**
  - Identifikuj používateľov, aplikácie, systémy a zdroje, ktoré potrebujú komunikovať
  - Zisti aké toky sú nutné (kto ↔ čo ↔ port/protokol ↔ smer)
- **Začni zhora – logické zóny**
  - Choď od lokalít
  - Definuj hlavné zóny podľa funkcie a rizika:
    - Campus · Data Center · DMZ · Cloud · Internet Edge
  - Zóny definuj podľa funkcie a rizika (nie len podľa IP/VLAN)
- **Postupné spresňovanie (refinement)**
  - Rozdeľuj zóny až po úroveň aplikácií / dát / služieb
  - Cieľ: minimalizovať „flat“ prístup medzi zónami (east–west)



- **Objekty a kontext**
  - Politika musí vychádzať z typu objektu (user/device/server/app) a umiestnenia (campus/DC/DMZ/cloud)
  - Rovnaký objekt v inej zóne = často iné pravidlá
- **Kontrola prístupu (Zero Trust)**
  - Zohľadni, kto žiada prístup, ku ktorým zdrojom a prečo
  - Nastav „deny by default“ + povoľ len nevyhnutné (least privilege)

Segmentácia na L2 (VLAN) a L3 (VRF)

- **L2 Segmentácia – VLAN:**
  - Oddelenie broadcast domén na prepínači
  - Použitie pre oddelenie používateľov/služieb (Admin, Výroba, Hostia).
  - Pri router-on-stick vytváranie aj perimetrových zón, DMZ
  - **Bezpečnostný prínos:** obmedzenie broadcastov, izolácia hostí, základ pre ACL/802.1X
  - **VLAN segmentácia (L2):** útočník vo VLAN 20 sa môže pohybovať laterálne v rámci VLAN
- **L3 Segmentácia – VRF:**
  - Virtuálne routing inštancie (oddelené smerovacie tabuľky)
  - Umožňuje izoláciu sietí aj s rovnakými IP rozsahmi (overlapping IP)
  - **Bezpečnostný prínos:** izolácia kritických aplikácií (napr. HR, Finance), rozdielne routing politiky, menšia útočná plocha

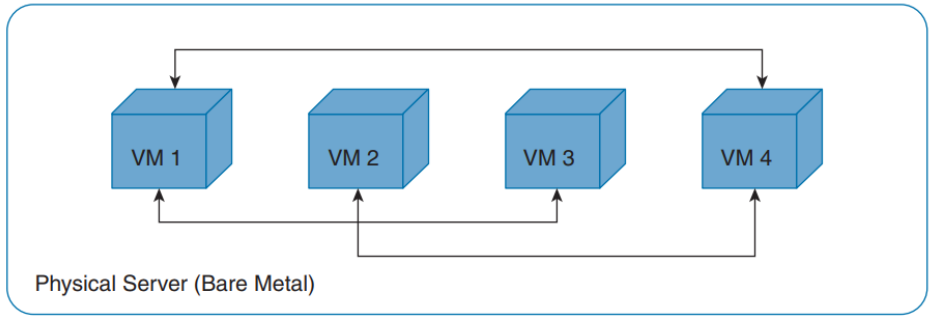
```
Switch# show vlan brief

VLAN Name         Status   Ports

10   ADMIN        active   Gi0/3, Gi0/4

20   PROD         active   Gi0/5, Gi0/6

30   GUEST        active   Gi0/7
```

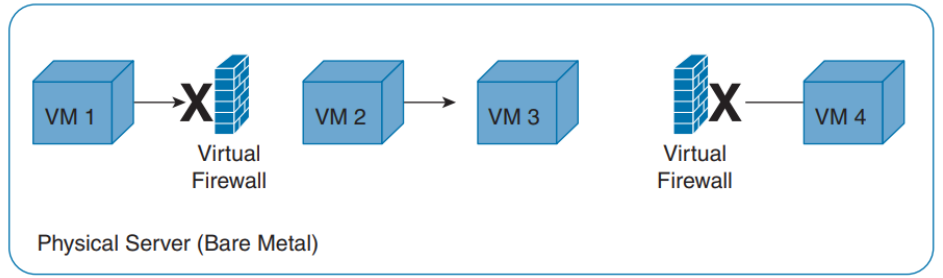
```
Router# show ip route vrf HR

Routing Table: HR

10.0.0.0/24 is directly connected,
GigabitEthernet0/0

172.16.0.0/16 [110/2] via 10.10.10.2, 00:00:12,
Gi0/0
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Mikrosegmentácia: Jemná izolácia v sieti

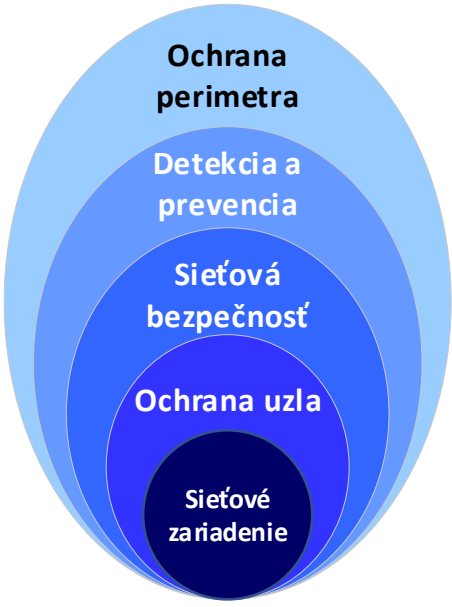
- Mikrosegmentácia
  - Jemná segmentácia na úrovni jednotlivých VM, aplikácií alebo procesov
  - Politiky založené na identite, kontexte, aplikácii – nie len na IP/VLAN
- **Princíp:**
  - Každý workload má vlastné pravidlá komunikácie („least privilege“)
  - Politiky aplikované softvérovo – distribuovaný firewall/agent
  - Nezávislé od fyzickej topológie siete
- **Príklady implementácie:**
  - AWS / OpenStack security groups (na úrovni inštancie VM)
  - VMware NSX – Distributed Firewall pre VM
  - Cisco ACI – Endpoint Groups (EPG) s microsegmentation policies
- **Výhody:**
  - Zastavenie laterálneho pohybu útočníka (ransomware, APT)
    - Útočník je izolovaný, povolené sú iba explicitne definované komunikácie (napr. App ↔ DB).
  - Granulárna kontrola: povolená iba nevyhnutná komunikácia
  - Podpora Zero Trust Network Access (ZTNA)
- **Výzvy:**
  - Vyššia komplexita návrhu a správy
  - Potreba integrácie s IAM a monitoringom

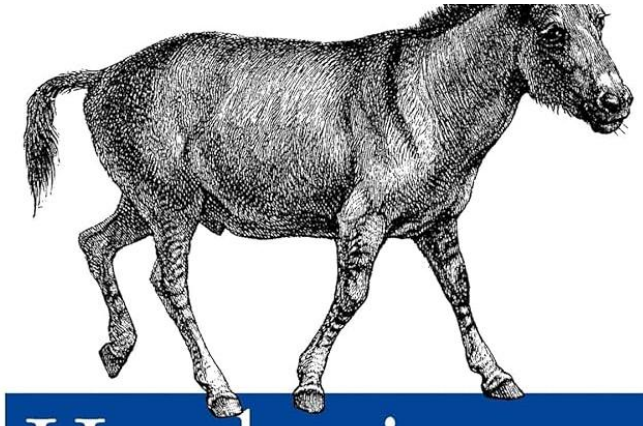




Access Layer Security – Zabezpečenie prístupu

NAC, 802.1X, Access layer Security,
=> samostatná prednáška





Network device protection

Network Device Hardening

Patch management a zálohy

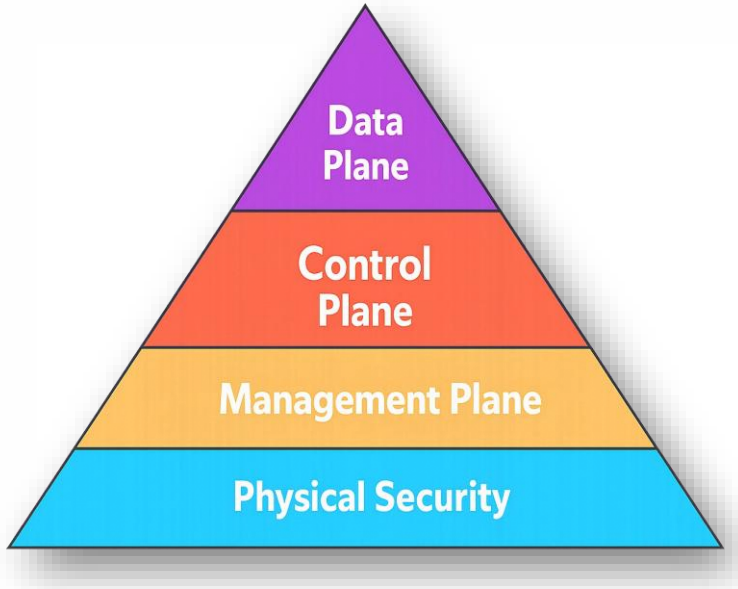
AutoSecure – baseline hardening

Logging and monitoring

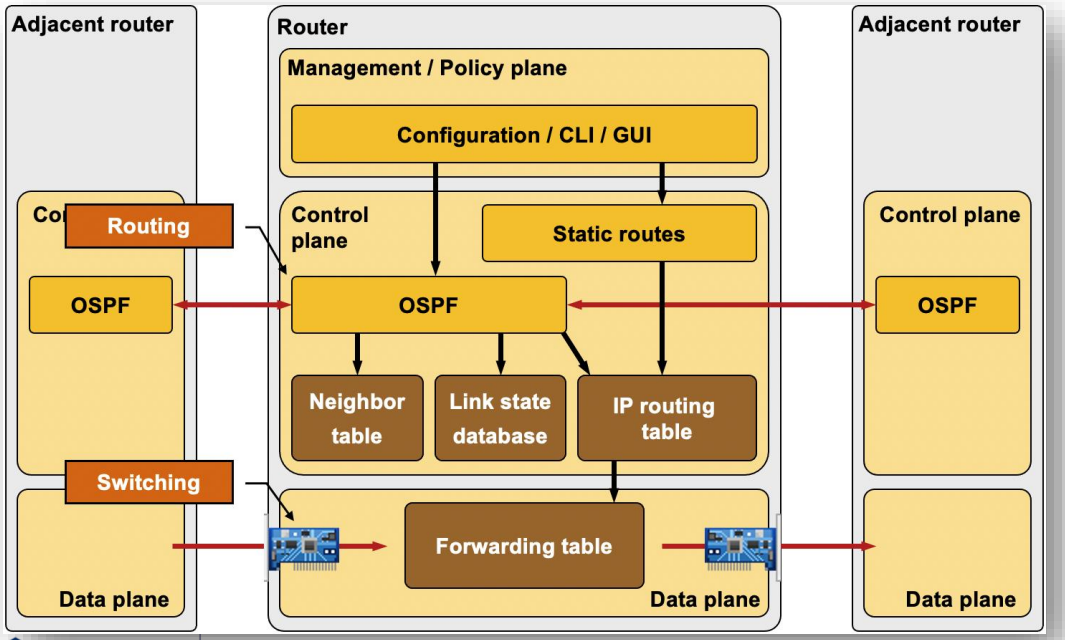
Ochrana aplikácií a služieb

Cisco pohľad (CIS, NSA, CISA pohľad)

Network node Hardening: Úvod



- **Router/ switch / firewall hardening**
  - Systematické vyladenie konfigurácie a prostredia zariadenia
- **Cieľ**
  - Minimalizovať útočnú plochu, zvýšiť odolnosť a dostupnosť
- **Prečo je to dôležité:**
  - Router = kritický uzol → ak padne, padá celá sieť
  - Častý cieľ útokov (DDoS, spoofing, brute-force na management)
  - Nespevnené zariadenie môže byť pivotom pre útočníka
- **Hlavné oblasti hardeningu:**
  - Physical & OS Security (prístup, patching, zálohy)
  - Management Plane (bezpečná správa, AAA, ACL, logging)
  - Control Plane (ochrana CPU, routing protokolov)
  - Data Plane (ACL, uRPF, port security, storm-control)
- **Best Practice rámce:**
  - Cisco hardening guides
  - CIS Benchmark for Cisco IOS/IOS-XE
  - NSA/CISA odporúčania pre sieťové uzly



Physical & OS Security (prístup, patching, zálohy)

- **Physical Security & Availability**
  - **Zabezpečená miestnosť**, kontrolovaný fyzický prístup (badge, CCTV, logovanie vstupov)
  - **EMI/ESD ochrana**, protipožiarne systémy (Inergen, FM200), klimatizácia redundantná (N+1)
  - **Napájanie:** UPS + diesel generátor, pravidelné testy failoveru
  - **RACK bezpečnosť:** uzamykateľné racky, plombovanie, označenie zariadení
  - **Inventarizácia HW:** CMDB záznamy, sledovanie životného cyklu zariadení
- **Operating System Security**
  - **Patch management:** pravidelné aktualizácie IOS/IOS-XE podľa Cisco PSIRT advisories, testovanie pred nasadením
  - **Verifikácia image:** používať digitálne podpísané LTS verzie (image integrity validation)
  - **Resilience & Recovery:** zabezpečený boot-config, recovery režim chránený heslom, záložné image v flash (secure-boot)
  - **Configuration Compliance:** pravidelné porovnanie s „golden config“ pomocou napr. Ansible

Physical & OS Security - Patch Management a Zálohy

- **Patch Management:**
  - Pravidelný upgrade FW/OS (Cisco IOS, Junos, FortiOS, PAN-OS) na bezpečnostné verzie
  - Sledovanie PSIRT advisories, CVE databáz, vendor bulletins
  - Testovanie updatov v lab prostredí pred produkciou
  - Odstraňovanie zastaraných/zraniteľných obrazov
- **Zálohy konfigurácií a image:**
  - Automatizované zálohy cez SCP/SFTP/HTTPS/REST API (nie TFTP)
  - Verzionovanie záloh – timestamp, commit ID, rollback možný
  - Centralizované a zabezpečené uloženie mimo produkčnej siete
  - *Resilient Config* alebo ekvivalent (secure boot-image & boot-config)
- **Infra as Code (IaC):**
  - Source of Truth - NetBox
  - Git ako úložisko konfigurácií (audit, diff, revert)
  - Automatizačné nástroje: Ansible, Salt, Puppet, Chef, Terraform
  - Podpora multivendor prostredí (Cisco, Juniper, Fortinet, Palo Alto)
  - CI/CD pipeline pre testovanie a nasadzovanie konfigurácií
- **Best Practices:**
  - Zaviesť change management a review proces
  - Overovať digitálne podpisy vendor obrazov
  - Testovať obnovu záloh → záloha má hodnotu len ak funguje

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Management Plane (bezpečná správa, AAA, ACL, logging)

- Politika hesiel
  - Komplexné heslá, minimálna dĺžka, pravidelná rotácia, zakázať opakované použitie
- Role-Based CLI Access
  - Privilege levels, AAA authorization, logging príkazov (TACACS+)
- AAA (TACACS+/RADIUS)
  - Centralizovaná autentifikácia, autorizácia a audit príkazov
- Len bezpečné protokoly: SSHv2, HTTPS, SNMPv3
  - Zakázať Telnet/HTTP
- ACL pre prístup k manažmentu
- Session management
  - Časový limit (timeout), login block-for po neúspešných pokusoch (ochrana pred brute-force), Bannery s právnym upozornením
- OS Hardening
  - Vypnutie nepoužívaných služieb (HTTP, CDP, LLDP, SNMPv1/v2), Finger / Source-Route
- Out-of-Band (OOB) Management
  - Separovaná VLAN / fyzická sieť pre management

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Logging & Monitoring

- NTP synchronizácia
  - Zabezpečené časové zdroje (NTPv4 + authentication key) – nutné pre koreláciu v SIEM
- Syslog
  - Odosielať logy na centralizovaný Syslog server cez TLS (TCP/6514)
- SNMPv3 + traps
  - Len šifrovaná komunikácia (authPriv), zber metrik a alarmov
- Integrácia do SIEM
  - Korelácia udalostí (prihlásenia, príkazy, ACL zmeny, systémové chyby)
- AAA accounting
  - Detailné logovanie prístupov a príkazov používateľov
- Baseline + Alertovanie
  - Prahové hodnoty CPU/memory, fail login pokusy, konfigurácia trapov
- Zálohy logov
  - Pravidelné exporty, ochrana pred manipuláciou (write-once storage)

- **SIEM Integrácia**
  - Splunk, ELK/Graylog, QRadar, Cisco SecureX
  - Korelácia logov zo sieťových a bezpečnostných uzlov
  - Incident response playbooky a alerting
- **Best Practices**
  - Uchovávať logy mimo produkčnej siete
  - Monitorovať trendové metriky
    - Zariadenie: CPU load, RAM usage, teplota, stav napájania/ventilátorov
    - Sieť: Interface errors/discards, utilization %, packet drops
    - Bezpečnosť: počty ACL deny, IPS/IDS alertov, VPN session failures
    - Trendové ukazovatele: rast objemu logov, zvýšená latencia, neobvyklý traffic pattern
  - Testovať alerty → aby neboli ignorované

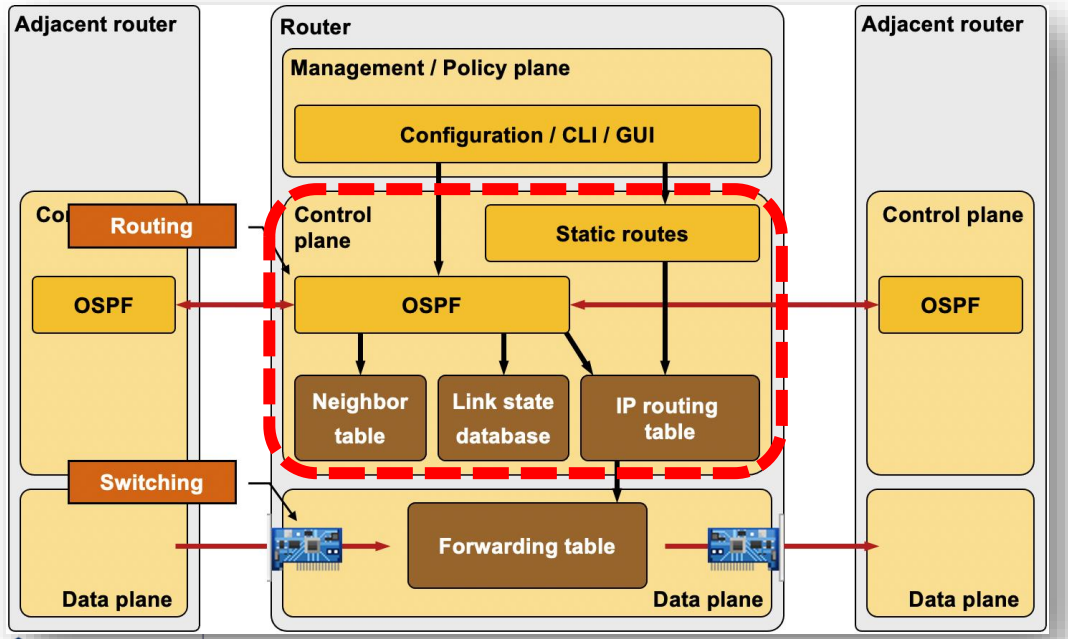
AutoSecure: Baseline Hardening

- **AutoSecure**
  - Automatizovaný sprievodca pre spevnenie konfigurácie zariadenia
  - V Cisco IOS/IOS-XE: príkaz auto secure
- **Funkcie (Cisco):**
  - Zakáže nepotrebné služby (CDP, Finger, PAD, Source Routing)
  - Zapne SSH, AAA, bannery a logging
  - Vytvorí základné ACL pre management
  - Povinné silné heslá a časové limity
- **Výhody:**
  - Rýchla aplikácia baseline nastavení
  - Redukuje útočnú plochu od začiatku
- **Nevýhody:**
  - Cisco-špecifické (nie univerzálne)
  - Menej flexibilné → vyžaduje následný manuálny tuning

- **Univerzálne alternatívy:**
  - Juniper: *Junos EZ Security Templates*
  - Fortinet: *Security Fabric Initial Hardening*
  - Palo Alto: *CIS baseline config*
  - Open štandardy: **CIS Benchmarks, NIST SP 800-53** ako „baseline hardening“

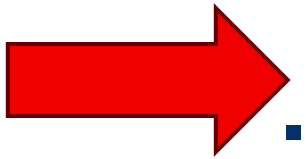
Control Plane Security

- Ochrana CPU, pamäte a riadiacej roviny zariadenia
- **Hrozby**
  - Flood ICMP, spoofing routing protokolov (OSPF, BGP, EIGRP), DoS/DDoS
- **Control Plane Policing (CoPP)**
  - Bráni zahlteniu CPU, nastavuje limity na ICMP, SSH, BGP či OSPF
  - Class-map & Policy-map → policing/rate-limit pre CPU traffic
  - Povoliť iba potrebné protokoly, ostatné dropnúť
- **Routing Protocol Protection**
  - Zabraňuje podvrhom v smerovaní
    - Autentifikácia (MD5/SHA) v OSPF, EIGRP, BGP
    - TTL Security (OSPF = TTL=1, BGP GTSM)
    - Filtre pre susedov (neighbor ACLs)
- **Best practices**
  - Oddeliť management → Out-of-Band ak je možné
  - Rate-limit ICMP a traceroute
  - Nepoužívané routing protokoly zakázať

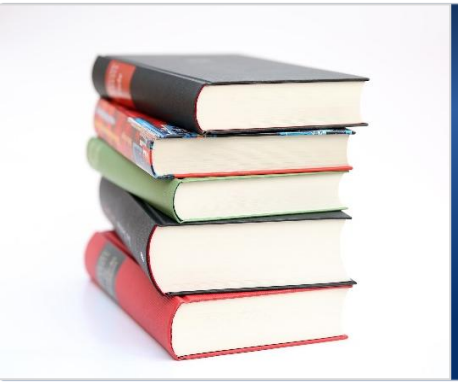


Data Plane Security

- **Opatrenia ktoré preberáme**



- **Access Control Lists (ACLs):**
  - Filtrácia dátovej prevádzky podľa zdroja/cieľa/portu
  - Vynútenie politiky „default deny“
- **Unicast Reverse Path Forwarding (uRPF):**
  - Overuje, či zdrojová adresa má platnú cestu v routovacej tabuľke
  - Blokuje spoofing zdrojových adries
- **Port Security (na switchi):**
  - Obmedzenie počtu MAC adries na porte
  - Akcia pri porušení: shutdown / restrict / protect
- **Storm Control:**
  - Ochrana pred broadcast, multicast a unicast stormami
  - Rate-limiting na prístupových portoch
- **IPS/NGFW integrácia:**
  - Detekcia a blokovanie škodlivej prevádzky
- **Best practices:**
  - Implicit deny, segmentácia VLAN/VRF
  - Kombinovať ACL + uRPF + Port Security



Zdroje

- Cisco IOS/IOS-XE Hardening Guide
- NSA Network Infrastructure Security Guide – best practices
- Cisco IOS (17.x/16.x) – kontrolný zoznam bezpečnej konfigurácie (zakázanie služieb, šifry, management ACL)
- CISA hardening guidance pre sieťové zariadenia

Ochrana aplikácií a služieb

WAF, ESA, WSA

WAF (Web Application Firewall)

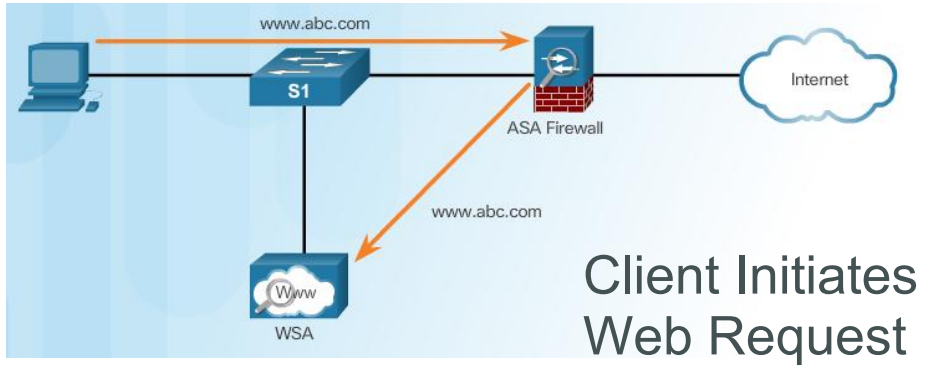
- Ochrana webových aplikácií pred útokmi na L7
- **Typické hrozby:** SQL Injection, XSS, CSRF, Command Injection (OWASP Top 10)
- **Mechanizmus:**
  - Analýza HTTP/HTTPS requestov a odpovedí
  - Aplikačné signatúry, pravidlá, pozitívny bezpečnostný model
- **Nasadenie:**
  - Reverse proxy pred webserverom
  - Integrované v NGFW alebo cloud (AWS WAF, Azure WAF)
- **Výhody:** Špecializovaná ochrana aplikácií, detekcia aplikačných útokov
- **Nevýhody:** Možnosť falošných pozitív, potreba údržby pravidiel
- Príklad
  - Open-source:ModSecurity (OWASP CRS) – modul pre Apache/Nginx/IIS, najrozšírenejší open-source WAF
  - Komerčné:F5 Advanced WAF alebo Imperva WAF

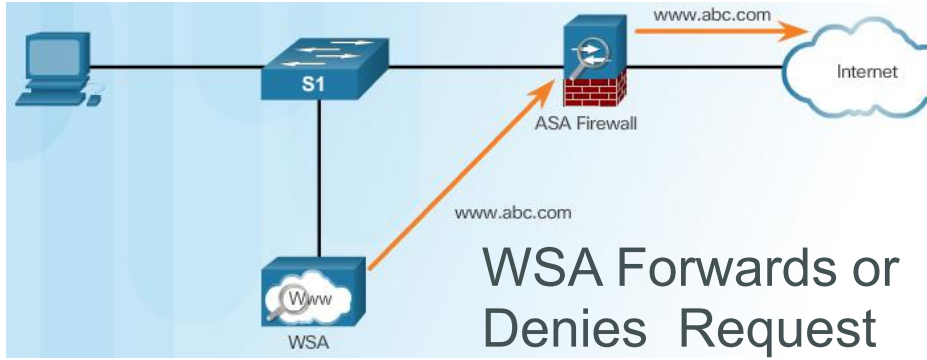
ESA (Email Security Appliance)

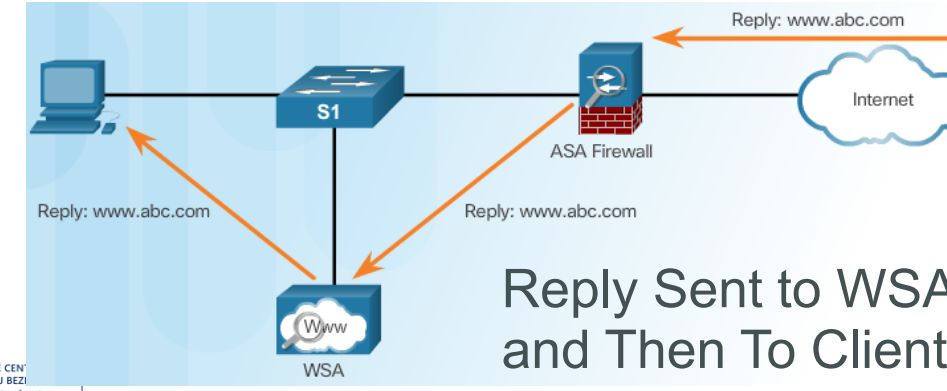
- **Obsah snímky**
- **Cieľ:** Ochrana e-mailovej komunikácie
- **Typické hrozby:** Spam, phishing, malware v prílohách, BEC útoky
- **Funkcie:**
  - Antispam filtre (blacklist, reputácia, content filter)
  - Antivírus + sandboxing príloh
  - Link protection (prehľad URL v e-maile)
  - DLP (Data Loss Prevention) pre e-maily
- **Nasadenie:**
  - Gateway medzi interným mail serverom a internetom
  - Cloud (Microsoft 365 Defender, Proofpoint, Cisco ESA)
- **Výhody:** Špecializovaná ochrana pred e-mailovými hrozbami
- **Nevýhody:** Dodatočná latencia, potreba priebežného ladenia filtrov
- Príklad:
  - Open-source:
    - MailScanner alebo Rspamd – open-source brány pre antispam/antimalware filtering
      - SpamAssasin, ClamAV, Amavis
  - Komerčné: Proofpoint Email Protection, Cisco Secure Email (ESA IronPort)

WSA (Web Security Appliance) – Web proxy

- Ochrana používateľov pri prístupe na web
- **Typické hrozby:** Malware zo škodlivých webov, phishing, drive-by downloads
- **Funkcie:**
  - URL filtering (kategórie, reputácia)
  - Malware scanning, sandboxing sťahovaných súborov
  - SSL inspection pre HTTPS traffic
  - CASB integrácia (kontrola SaaS aplikácií)
- **Nasadenie:**
  - Proxy brána medzi klientom a internetom
  - Cloud Secure Web Gateway (SWG, Zscaler, Cisco Umbrella)
- **Výhody:** Viditeľnosť a kontrola webovej prevádzky
- **Nevýhody:** Latencia pri inspekcii SSL, potreba certifikátov na klientoch
- Príklad:
  - Open-source: Squid Proxy (s ACL a URL filtermi) + ClamAV
  - Komerčné: Zscaler Internet Access (SWG), Cisco Umbrella (SWG)







Remote access and management - Vzdialený prístup a manažment

VPN – Site-to-Site, Remote Access, SSL, Ipsec

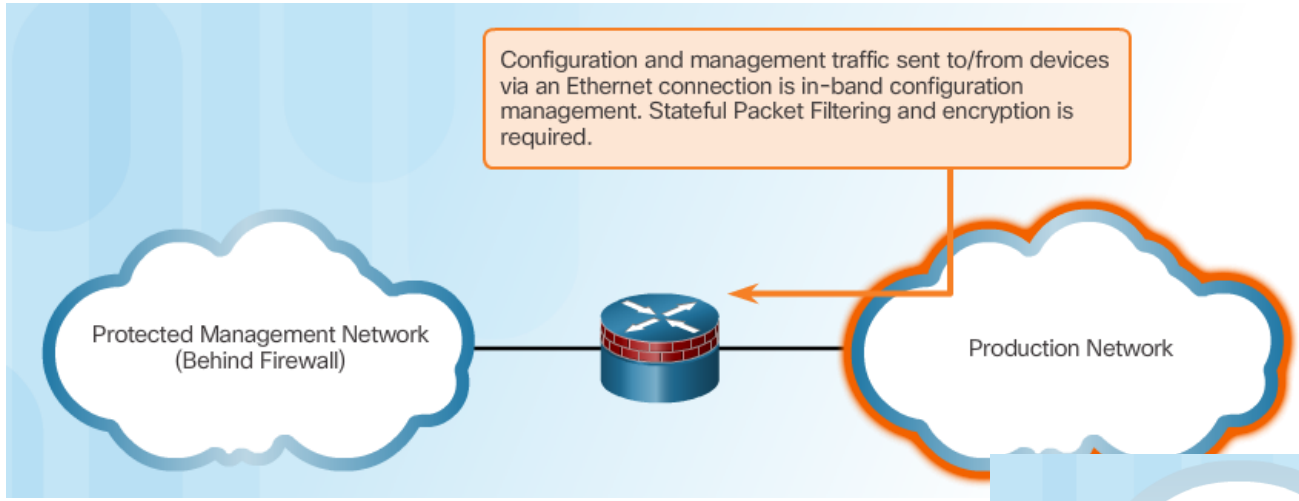
=> samostatná prednáška

In-band vs. Out-of-band management

Bezpečný manažment – SSH, SNMPv3, syslog

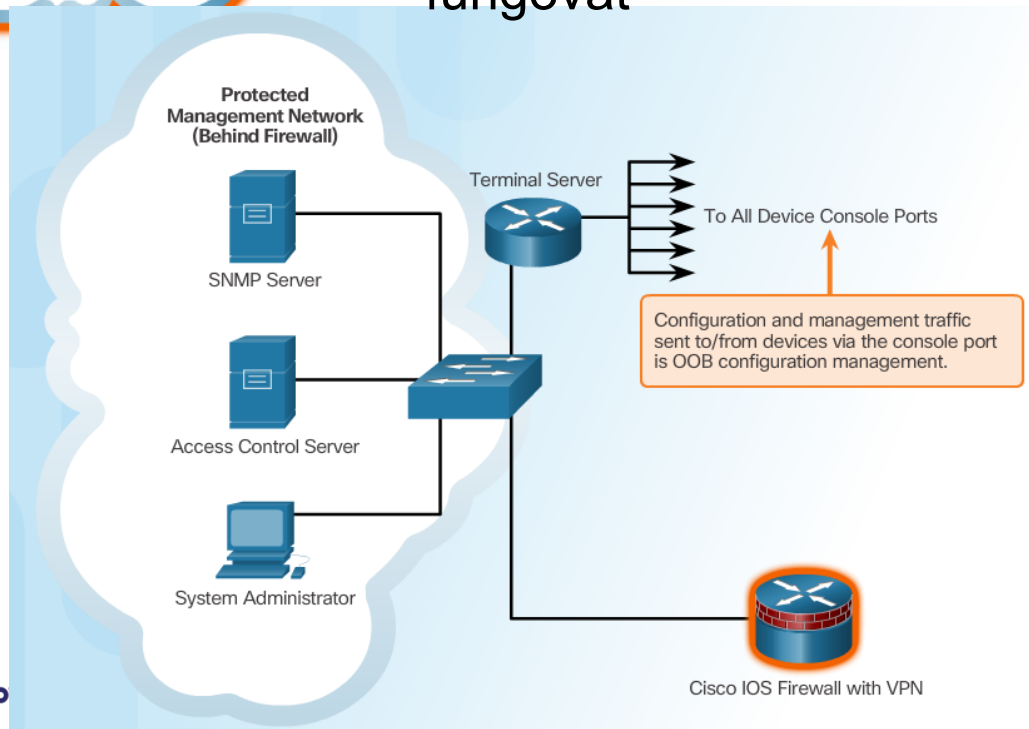
=> mimo čas

In-band vs. Out-of-Band Management

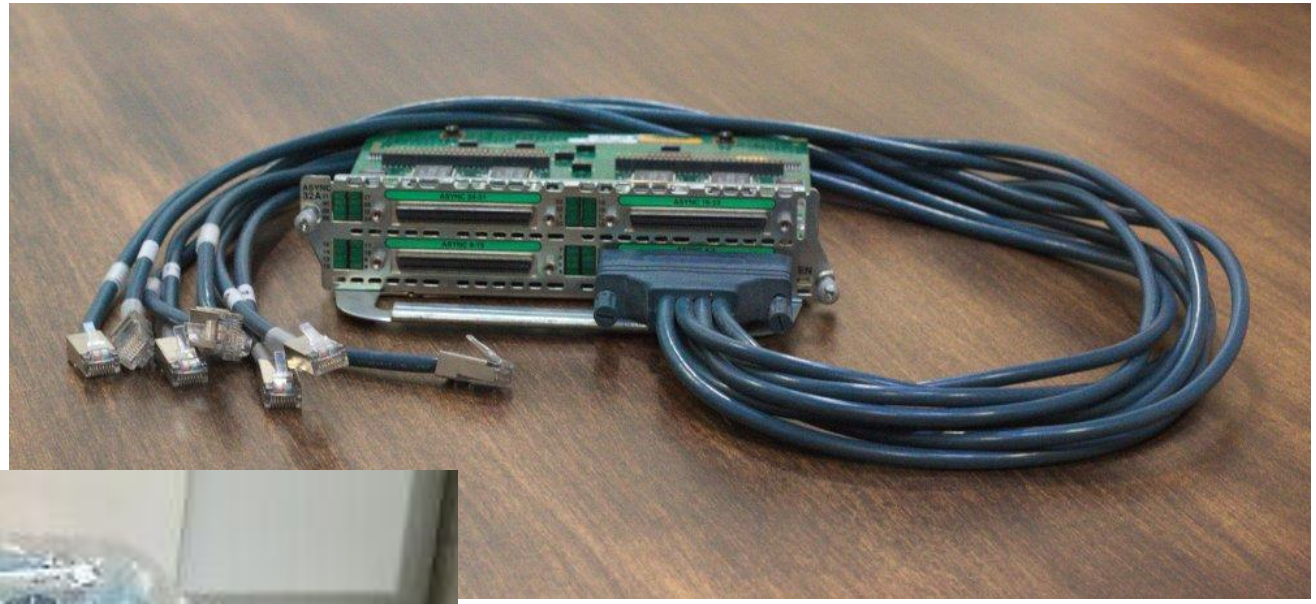


- **In-band Management (IB):**
  - Manažment cez produkčnú dátovú sieť (rovnaká infraštruktúra pre používateľov aj adminov)
    - Jednoduchšie a lacnejšie (nepotrebuje extra infraštruktúru)
  - – Ak je dátová sieť kompromitovaná alebo zahltená, manažment prestáva fungovať

- **Out-of-Band Management (OOB):**
  - Oddelená sieťová infraštruktúra pre manažment (dedikované rozhrania, konzolové servery)
    - Nezávislé od produkčnej prevádzky → dostupné aj počas útoku/výpadku
    - Väčšia bezpečnosť (segmentácia, ACL, VPN prístup)
  - – Vyššie náklady a komplexita



Cisco “octopus” RAS/console server



Other example

Kvíz

- **Aký je hlavný cieľ Control Plane Policing (CoPP) na routeri alebo switchi?**
  - A) Zabezpečiť šifrovaný prístup k management rozhraniu
  - **B) Ochraniť CPU zariadenia pred zahltením škodlivou alebo nadmernou prevádzkou**
  - C) Znížiť broadcast traffic v rámci VLAN
  - D) Monitorovať logy a posielať ich do SIEM

- **Ktoré z nasledujúcich tvrdení je *najlepším postupom* pri segmentácii siete?**
  - A) Povoliť všetku komunikáciu medzi VLAN segmentmi, aby bola sieť flexibilná
  - B) Spoliehať sa len na VLAN segmentáciu, bez ACL alebo firewallu
  - **C) Použiť „default deny“ medzi segmentmi a povoľovať iba potrebné spojenia**
  - D) Rozdeliť sieť na čo najviac VLAN (over-segmentation)

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Sieťová bezpečnostná architektúra

prof. Ing. Pavel Segeč, PhD.

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk