Firewally a aplikační filtry

Bezpečnost ICT 2

Lukáš Malina

Vysoké učení technické v Brně
malina@vut.cz
axe.vut.cz

2022

Informační bezpečnost

Firewall - definice

Definice:

- **Síťový bezpečnostní systém (zařízení/program), který monitoruje a kontroluje síťový provoz na základě definovaných pravidel.**
- FW zajišťuje bezpečnost sítě či síťových prvků (serverů, klientských PC atd.) pomocí **omezení** příchozího a odchozího provozu podle pravidel.

Základní funkce:

- Identifikuje zdroje a cíle provozu (IP adresy, porty).
- **Prosazuje filtrační pravidla** na jednotlivé spojení/uživatele.
- Vyhodnocuje informace o stavu spojení, kontroluje protokoly (i data).
- Chrání před útoky a neoprávněnými průniky do sítě.

Firewall - další pojmy

DMZ (demitilarizovaná zóna):

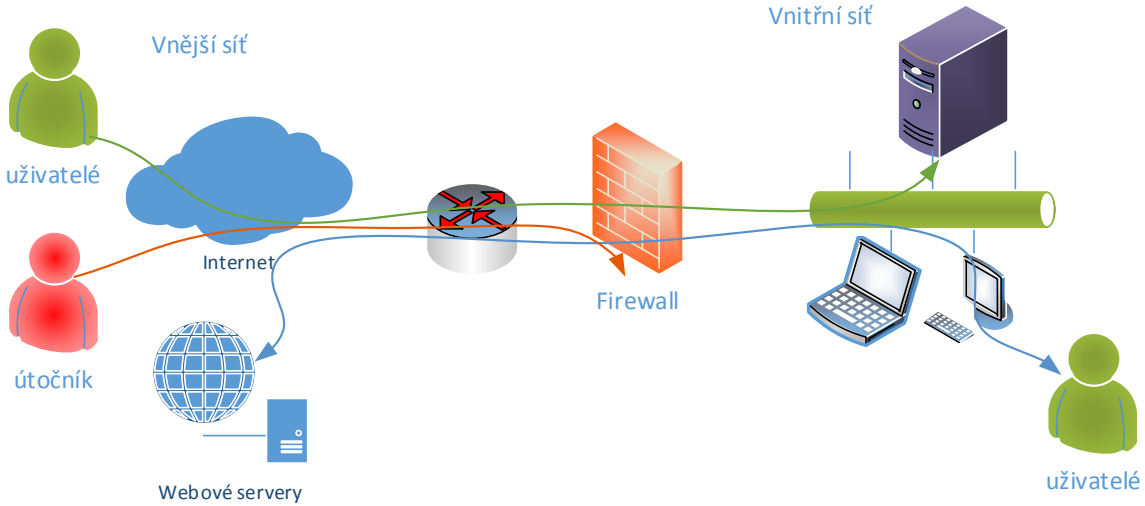
- **Část sítě na perimetru mezi vnitřní a vnější sítí**.
- Pro **bezpečnější umístění serverů a služeb poskytované směrem do vnější sítě** (Internet).
- Pro FW je to třetí rozhraní se **stupněm důvěrnosti mezi vnitřní a vnější sítí**.

Honeypot:

- Systém nebo SW na serveru, který vypadá zranitelně a má za cíl přitáhnout na sebe útoky.
- Slouží jako **falešná návnada**.
- Bývá často součástí IDS (Intrusion Detection System).

Základní rozdělení firewallů

- Softwarový vs hardwarový.
- Paketový; stavový paketový; stavový paketový s kontrolou síťových protokolů; aplikační; Next generation FW (NGFW)...



Historie firewallů

- První typy od 1987 [1]
- 1. generace: **Paketové filtry (IP a porty), 3. + 4. ISO/OSI vrstva**, Digital Equipment Corporation DEC 1988.
- 2. generace: **Stavové paketové filtry, stavová inspekce (stateful packet inspection)**, ATT Bell laboratories 1989-1990.
- 3. generace: **Aplikační** brány/Proxy **firewally**, taky známé jako Firewall Toolkit (FWTK), pracuje jako NAT, od roku 1994.
- **Moderní** firewally: **firewall + hloubková inspekce na aplikační vrstvě** (*deep packet inspection*), Next-Generation Firewall (NGFW) od 2012.
- Rozšíření dnešních firewallů: Intrusion Prevention Systems (IPS), integrace uživatelských identit (IDs s IP a MAC adresami), Web Application Firewall (WAF) - otisky používající časové postranní kanály.

Paketový firewall

- Pracují na **(3) síťové a (4) transportní vrstvě** (ISO/OSI).
- Zkoumají zdrojovou a cílovou **IP adresu**, **hlavičku** paketu/datagramu (např. FLAGS, TTL), zdrojový a cílový **port**, rozhraní.
- Využívání tzv. ACL (Access Control Lists) u Cisco IOS - L3 přepínače/směrovače, starší varianty linux firewallů, tzv. bezstavové, ...
- Výhody: vysoká rychlost, jednoduchost, nižší cena u HW řešení.
- Nevýhody: nižší úroveň zabezpečení, nechrání proti spoofování IP adres a škodlivému obsahu dat, problémy s protokoly např. aktivní režim FTP atd.

Stavový paketový firewall

- Pracují na (3) síťové a (4) transportní vrstvě (ISO/OSI).
- Zkoumají data jako paketový firewall/ACL a rozhoduje se i podle stavu (nové spojení, existující), **ukládají info o stavu jednotlivých spojení do paměti** a pak např. povolit jen odpovědi atp.
- Ukládá **info o socketech** do tab (**src IP, dest IP, src port, dest port, TCP/UDP**).
- FireWall-1 (Check Point), starší verze Cisco PIX, Cisco IOS Firewall, iptables v linuxovém jádře, ipfw v *BSD...
- Výhody: rychlost (např. náročný rozhodovací proces jen u 1. paketu, další jsou již zpracovány rychleji), jednoduchost, vyšší bezpečnost než u paketového filtru, možnost virtuálních stavů u bezestavových protokolů (UDP, ICMP).
- Nevýhody: nižší úroveň zabezpečení než aplikační filtry (nechrání proti některým útokům, náchylnost na DDoS,...).

Aplikační firewall

- Pracují **3. 4. a na 7. (aplikační) vrstvě** (ISO/OSI).
- Zkoumají data pro nebo od konkrétních aplikací a porovnávají vzorce (signatury) útoků a malwaru.
- Rozeznají i pokus aplikace obejít kontrolu na FW přes jiný port (tzv. bypass).
- Blokují celé procesy (několik dat/paketů najednou).
- Od 2012 tzv. **Next Generation FW (NGFW)** které poskytují **deep packet inspection** - mimo hlavičky se zkoumá i obsah dat (práce s bloky paketů), filtrace na 3 - 7 vrstvě, Identity management, strojové učení, Web app. FW atp.
- Např. Palo Alto FWs, FireWall-1 od verze 4.1 (Check Point), Netscreen/ISG/SSG (Juniper). Experimentální modul v iptables u linuxu.
- Výhody: vyšší bezpečnost, prevence proti počítačovým červům, trojanům, mitigace DDoS.
- Nevýhody: vyšší zpoždění, výpočetní náročnost, složitost může způsobit chybu či vznik zranitelnosti, vyžaduje periodický update a revizi.
- Pozn. v minulosti se nasazoval až ke koncovém uzlu (jako osobní FW).

Virtuální firewall

- Vznikl jako bezpečnostní záplata při rozmachu virtualizace a virtuálních sítí.
- FW na virtuálním rozhraní kontrolující provoz mezi virtuálními stroji.
- Pracuje s daty a protokoly na L2 - L7.
- Dva režimy:
  - Bridge mode - pracuje jako fyz. FW kdy bývá umístěn mezi síťovými rozhraními.
  - Hypervisor mode - dohlíží na chod a data z/do virtuálního stroje, nejčastěji v cloudu.
- Výhody jsou jednoduchá migrace a přenos nastaveného FW.
- Nevýhodou je snížený výkon - tj. nenahradí plně fyz. FW, ale dokáže jej zastoupit.

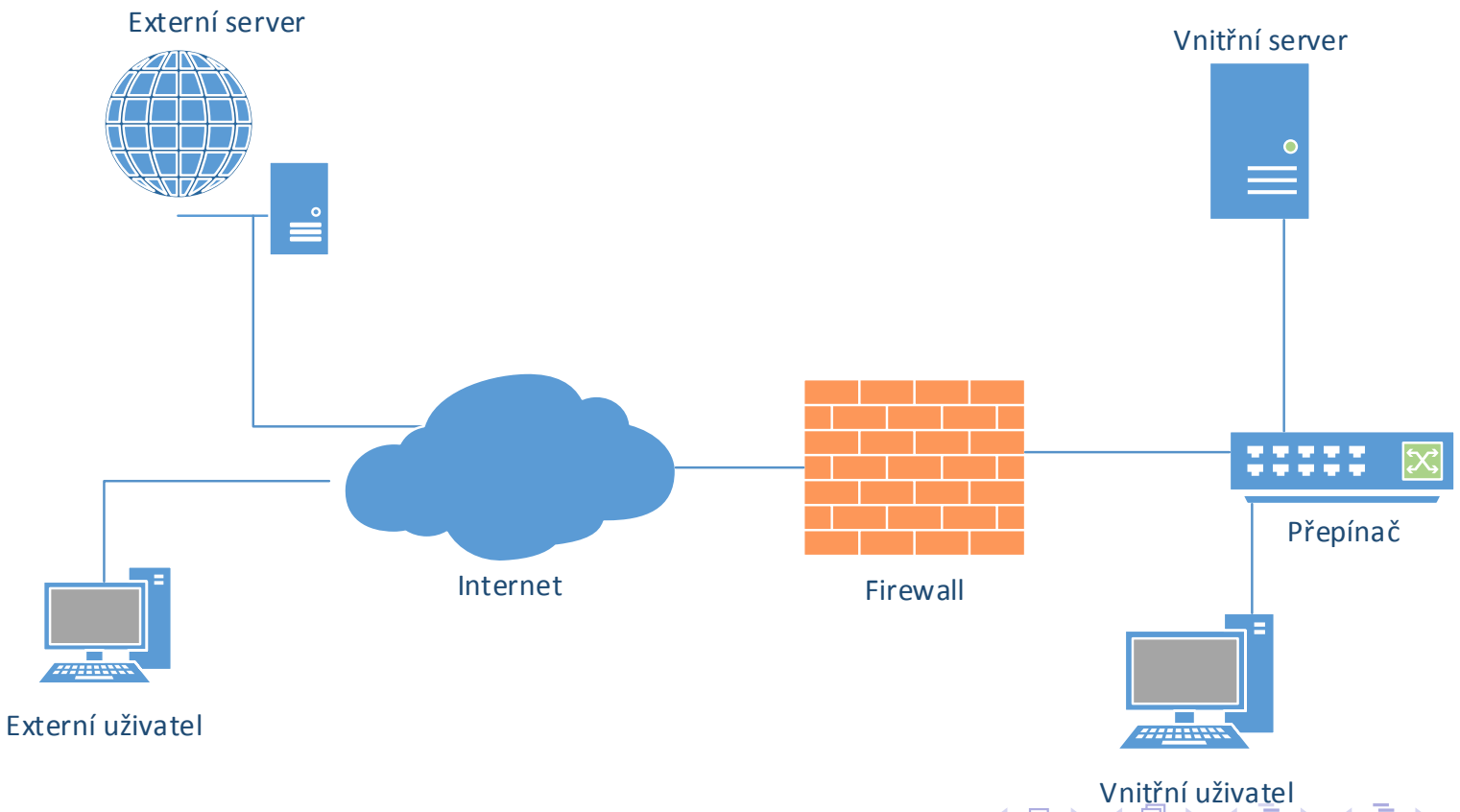
Osobní firewall/Aplikační proxy server

- **Osobní FW ve OS pracují na (2-7) vrstvě (ISO/OSI)**.
- Dnes součástí OS + IPS/IDS, antispyware funkce.
- Jednoduché nastavení, dotazy při nových službách (povolit/zakázat).

- Aplikační **proxy server** - **prostředník** v komunikaci v rámci služeb.
- Proxy server sám vystupuje jako klient - není zajištěna end-to-end konektivita.
- Web proxy server - řízení uživ. přístupu na web.stránky, filtrace obsahu, blokace reklamy.

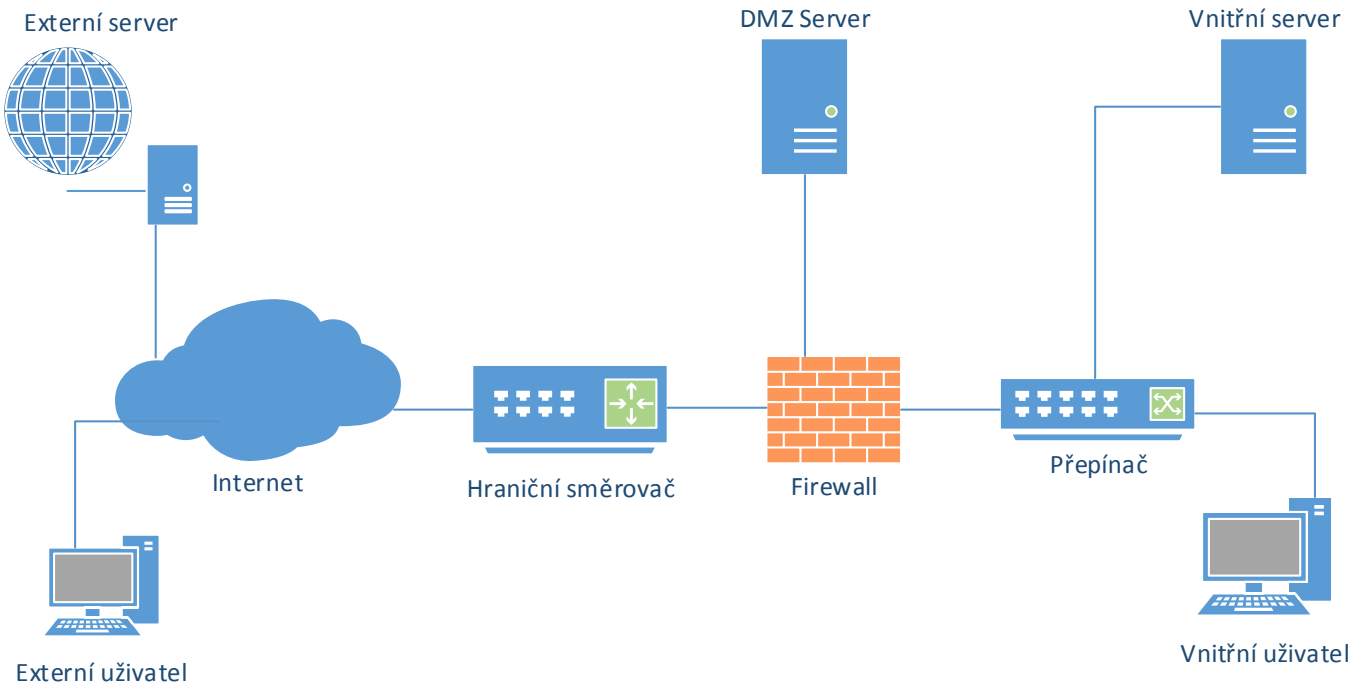
Firewall - umístění I.

- Mezi vnitřní (intranet) a vnější sítí (Internet), často jako součást směrovače nebo jako samostatné zařízení.



Firewall - umístění II.

- Ve vnitřní síti u hraničního směrovače.
- Mezi vnitřní sítí, vnější sítí a **demilitarizovanou zónou** (DMZ), FW s min. 3 rozhraními.



Firewall - umístění III.

- Na koncových uzlech - PC, server, atd.
- Softwarový firewall, osobní firewall.

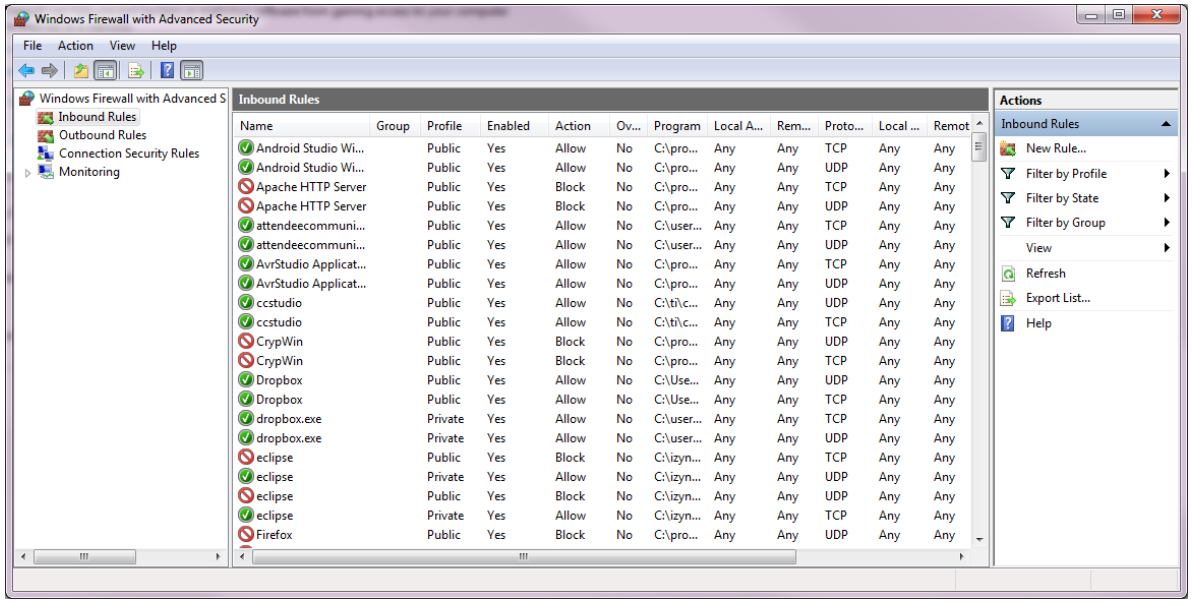


Figure: Windows firewall

Možnosti konfigurace firewallu

- Možnost **přímé** nebo **vzdálené** konfigurace přes **CLI** nebo **WebUI**.
- Moderní NGFW mají přístup přes webový prohlížeč (často https://192.168.1.1).
- **WebUI** $\approx$ **dashboard** $\approx$ **GUI** pro konfiguraci k FW.
- Console (např. RS-232, USB), Telnet, SSH, HTTP, HTTPS.
- Používat pouze **SSH** nebo **HTTPS**, ostatní přístupy zakázat!
- Různé úrovně konfigurace (uživatelský, privilegovaný/exekuční, globální konfigurační, konkrétní konfigurační - např. pro 1 interface).

Pracovní režimy firewallu

- **Směrovací režim** (routing mode - L3) - pracuje **jako směrovač**. FW **propojuje** rozhraní představující **podsítě** a pakety jsou mezi nimi směrovány na základě definovaných **pravidel** a NAT.
- **Transparentní režim** (transparent/bridging mode - L2) - transparentní most, všechna rozhraní patří do jedné podsítě. Firewall pracuje **jako L2 přepínač**. Není nutná konfigurace IP, NAT a routingu. Pouze **kontroluje bezpečnostní pravidla**.
- **Tap režim** - **pouze monitoring provozu**, který je přiváděn (mirroring) od přepínače.
- **Režim Virtual Wire** - **monitoring** provozu přímo na spojení + bezp. **pravidla**.

Základní funkce firewallu

- Zabezpečení komunikace/**filtrace** (povolení, blokování, zahazování) podle pravidel.
  - Pravidla rozlišují příchozí, odchozí, směrovaný provoz.
  - Pravidla rozlišují provoz dle IP adres, stavů, portů, aplikací, uživatelů a zón.
- **Logování** událostí a paketů.
- Zajišťuje další služby např. překlady adres (Network Address Translation - **NAT, PAT**), šifrovaná spojení (Virtual Private Network - **VPN**), Intrusion Detection System - **IDS**, autentizaci a autorizaci uživatelů, správa šířky pásma, atd.
- NGFW funkce - **detekce malware**, **ochrana proti útokům na L3-L7** (signatur útoků, behaviorální analýza - sledování prahů, UI - strojové učení, DDoS ochrany atp.).

Základní funkce filtrace firewallu

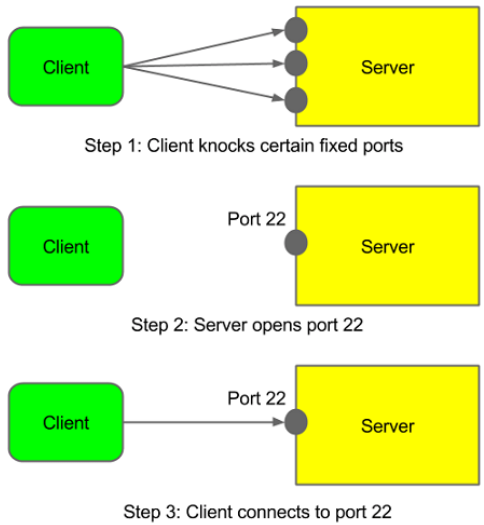
- Pravidla se mohou uplatnit podle zdr. nebo cíl. **IP adresy**, typu **protokolu** (ICMP,TCP,UDP,FTP...), typu **provozu** (ingress - příchozí, engress - odchozí, směrovaný - forwarded), **uživatele** atp.
- Dalším kritériem jsou **zóny** původu a cíle (**trusted, untrusted, DMZ**).
- Definovaná pravidla se mohou uplatnit v seznamu **zhora dolů** (např. iptables), podle definicí **priorit**, ...
- **Akce** s daty/pakety: **povolit**/allow/accept, **zakázat**/**reject a poslat ICMP**, **zahodit**/deny/**drop bez ICMP** a další (např. Reset client, Reset Server, tarpit).
- Odlišné nastavení u různých FW.

Metody filtrace firewallu

- Základní filtrace sleduje parametry ve zprávách na L2 (EtherTypes), L3 (IP adresy), L4 (TCP, UDP, porty, služby) a L7 (detekce podle služeb) a filtruje zprávy na základě definovaných pravidel.
- Práce s 1 až *n* zprávami/pakety/rámci.
- **Pokročilá detekce a filtrace** využívá metody jako např.:
  - Znalost **signatur útoků** (databáze příznaků),
  - Budování statistického modelu - **behaviorální analýza** - sledování prahů a jejich zadávání, sledování anomálií.
  - Využíti **umělé inteligence UI** - strojové učení (řízené/supervised a neřízené/unsupervised), neuronové sítě, perceptron.
- U pokročilých metod vzniká mnoho false positive nálezů (tj. některý legitimní provoz je filtrován).

Port knocking - klepání na porty

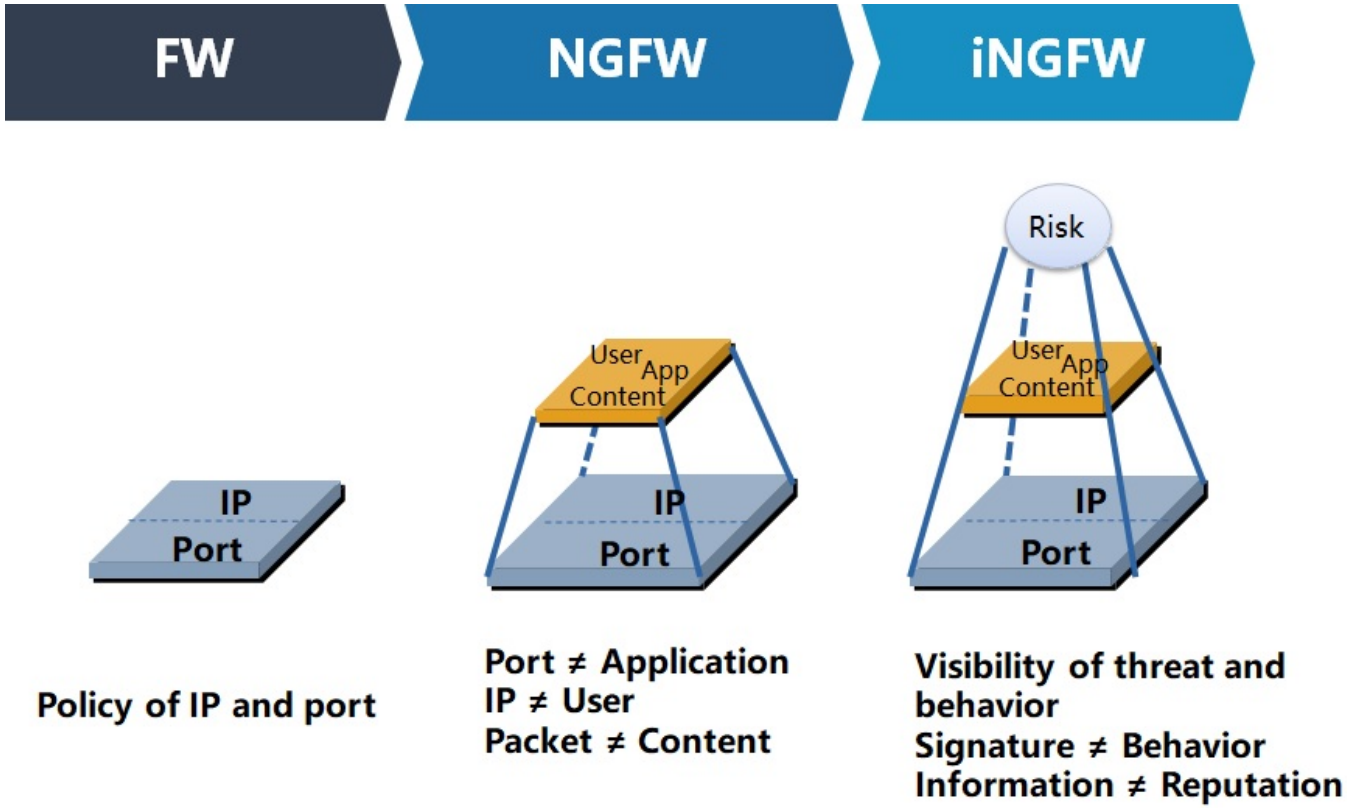
- Metoda jak si z nedůvěryhodného externího uzlu **otevřít přístup**/službu do uzlu nebo sítě chráněné firewallem.
- Přístup na port služby se na FW otevře po zaslání správných pokusů (**sekvence**) o připojení na skupinu předem specifikovaných portů.
- Sekvenci hlídá **démon**, vyhodnocuje se i pasivní **autentizace** (např. hash tagy zabraňují replay útokům).
- Cílem je **předcházet** využívání **exploitů na** permanentně **otevřených portech**.



Strategie konfigurace a životní cyklus FW

- Udělat si podrobný **přehled služeb a zařízení** v síti.
- **Nastavit pravidla**:
  - Začít s **Zakázat vše a pak povolit málo** - výhodou je **vyšší bezpečnost** a nevýhodou je vyšší omezení provozu a **složitější** donastavování a povolování provozu.
  - Začít s **Povolit vše a pak zakázat málo** - výhodou **jednoduší** nastavování a nižší omezení provozu, nevýhodou je **nižší bezpečnost**.
- Pravidelně **testovat konfiguraci** a FW v síti (např. pomocí nmap).
- Využít pokročilé metody detekce a filtrace a sledovat jejich dopad na provoz.
- Sledovat aktuální hrozby, **aktualizovat** a včasně implementovat záplaty a ochrany do konfigurace FW (NGFW řešení automaticky informují adminy).

Evoluce firewallů



Hardwarové firewally

Hardwarové firewally

- **Samostatná síťová zařízení**, která **slouží v síti jako firewall**, umístění v racku (1U).
- **Stavové** a paketové firewally (starší zařízení), **aplikační** firewally (novější zařízení).
- Různý počet **rozhraní**, spojení, datové rychlosti, velikost RAM, CPU, počet VPN atd.
- Výkonnost (HW) je přímo uzpůsobena činnosti firewallu.

Figure: CISCO ASA 5510 Firewall

Bezpečnostní zařízení - Security appliance

- **Bezpečnostní zařízení** pro ochranu sítí - kombinace monitoringu, FW filtrace, detekce IPS/IDS a AV modulů.
- Ochrana proti nechtěnému provozu (filtrace), škodlivému kódu (AV moduly), kyber-útokům (behaviorální analýzy, strojové učení).
- Podpora bezpečného přenosu - VPN brány, AAA servery.

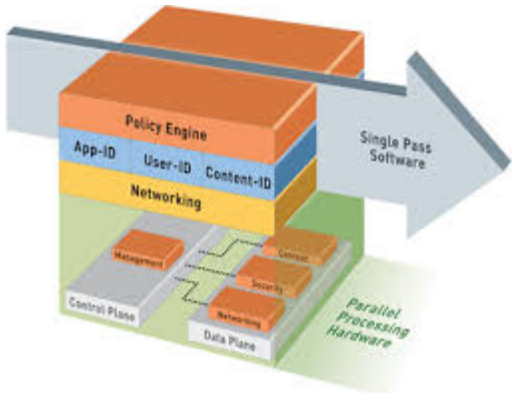
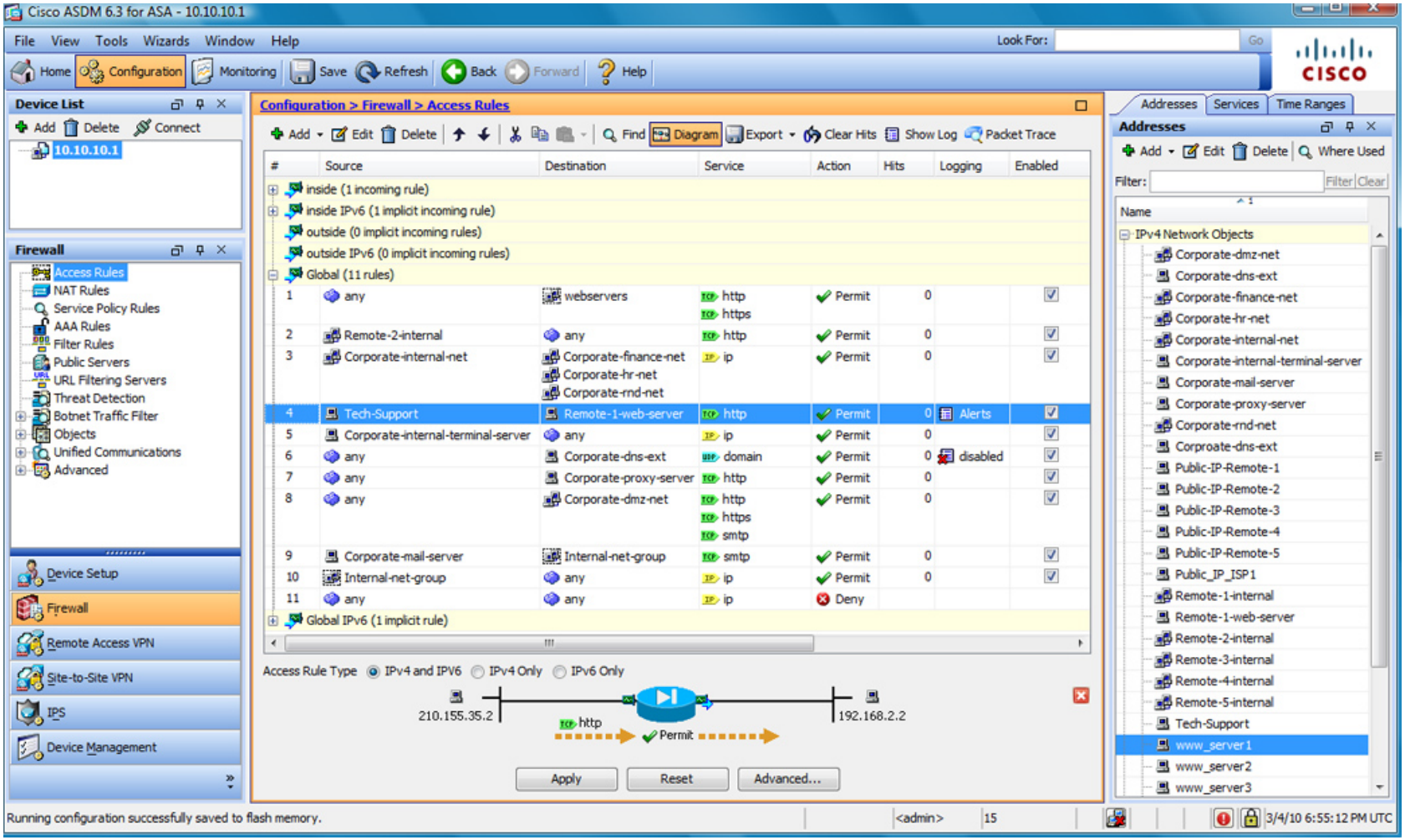


Figure: Palo alto NGFW schéma

CISCO firewally

- Součástí CISCO směrovačů a přepínačů - **ACL moduly**.
- Staré řady do roku 2008: CISCO **PIX** (Private Internet eXchange) - IP Firewally s NAT modulem, CPU 133 až 1000 MHz, RAM 16 až 1024 MB, počet rozhraní 2 až 14, Fast Ethernet, stavová inspekce, DoS ochrana, AAA, NAT/PAT, VPN.
- **Novější** řady od roku 2005: CISCO **ASA** (Adaptive Security Appliance) - funkce zděděny od řad PIX + IPS, IDS, aplikační filtry, ochrana proti malware, mitigace DDoS, Gigabit Ethernet rozhraní, X GB RAM, vhodné pro ochranu větších sítí, data center,...

CISCO firewally - ASA 5505 GUI



Check Point firewally

- Zařízení Check Point Security Appliances.
- IPS, aplikační firewall, filtrace web služeb, ochrana proti DoS, NAT a podpora QoS (Quality of Service).
- Široká škála zařízení s propustností pro malé sítě až po velké datové centra.
- Propustnost firewallů 750 Mbps až 400 Gbps.
- IPS propustnost 50 Mbps až 130 Gbps

Check Point firewall - dashboard

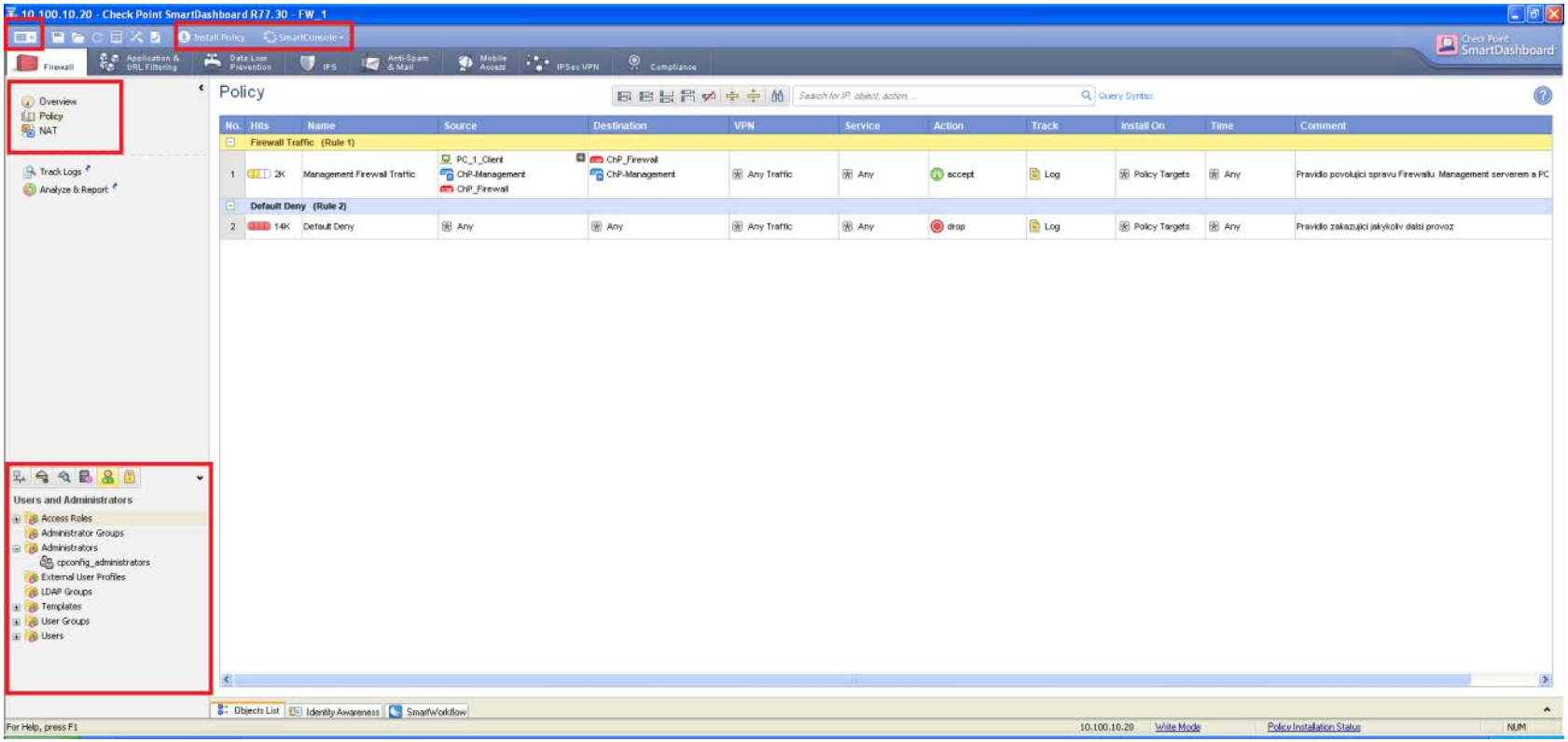


Figure: Check Point Firewall - GUI

Juniper firewally

- Firewally řady SSG a SRX.
- IPS, aplikační firewall, filtrace webu, ochrana proti DoS, NAT a podpora QoS.
- Široká škála zařízení s propustností pro jednotlivé stanice, malé sítě až po velké datové centra.
- Propustnost firewallů 700 Mbps - 320 Gbps.
- IPS propustnost 75 Mbps až 100 Gbp
- Počet pravidel od 384, přes tisíce až neomezeně.

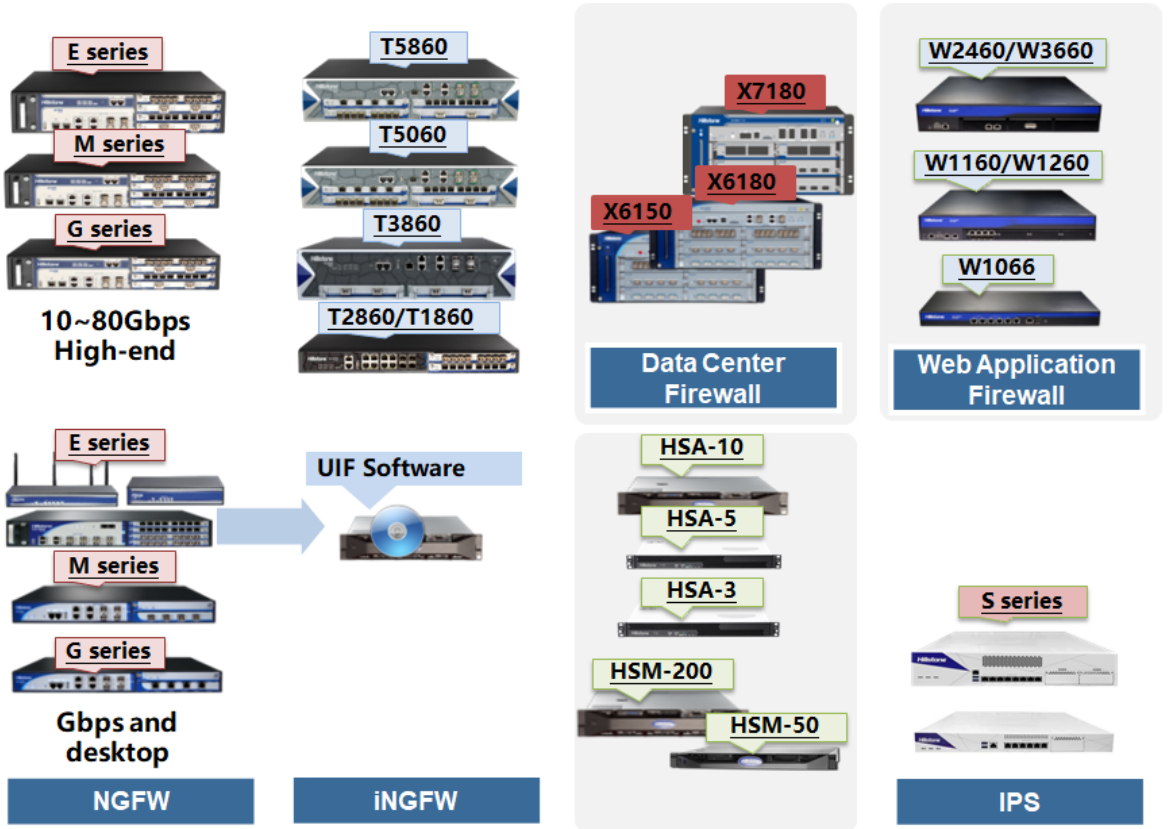
Palo Alto firewally

- Firewally NGFW, HW firewally, VM FW.
- Kombinace **NGFW** - Ochrana koncových prvků (Traps - sledování procesů Cyber Kill Chain a ochrana proti útokům) - Automatická cloud ochrana (**Wildfire** - **proti malware** a zero-day útokům, Autofocus - korelace bezpečnostních služeb, databází a údajů o útocích v rámci cloudu a upozorňování na útoky v síti).

Figure: Palo Alto Firewally

Hillstone firewally

- Firewally NGFW a iNGFW, DC FW, virt. FW a IPS.



Další HW firewally

- FortiGate (Fortinet).
- Mikrotik (založeno na iptables).
- Dell SonicWall (Dell).
- Barracuda Spam & Virus Firewall 100 (Barracuda).
- WatchGuard XTM (WatchGuard).
- ZyWALL (ZyXel).
- ...

HW firewally - vývoj podle Gartner 2020

Figure 1. Magic Quadrant for Network Firewalls

Softwarové firewally

Osobní firewally

- **Firewally běžící** na **operačních systémech** Windows, Linux, Mac OS.
- Firewally bežící **na platformách** chytrých zařízení (Android, iOS).
- Menší počet pravidel na L3 (jeden koncový bod).
- Větší stupeň ochrany na aplikační vrstvě (využívá výkonu hostitele).
- Lehká konfigurace (musí zvládnout běžný uživatel).
- Samoučící nebo manuální konfigurace.

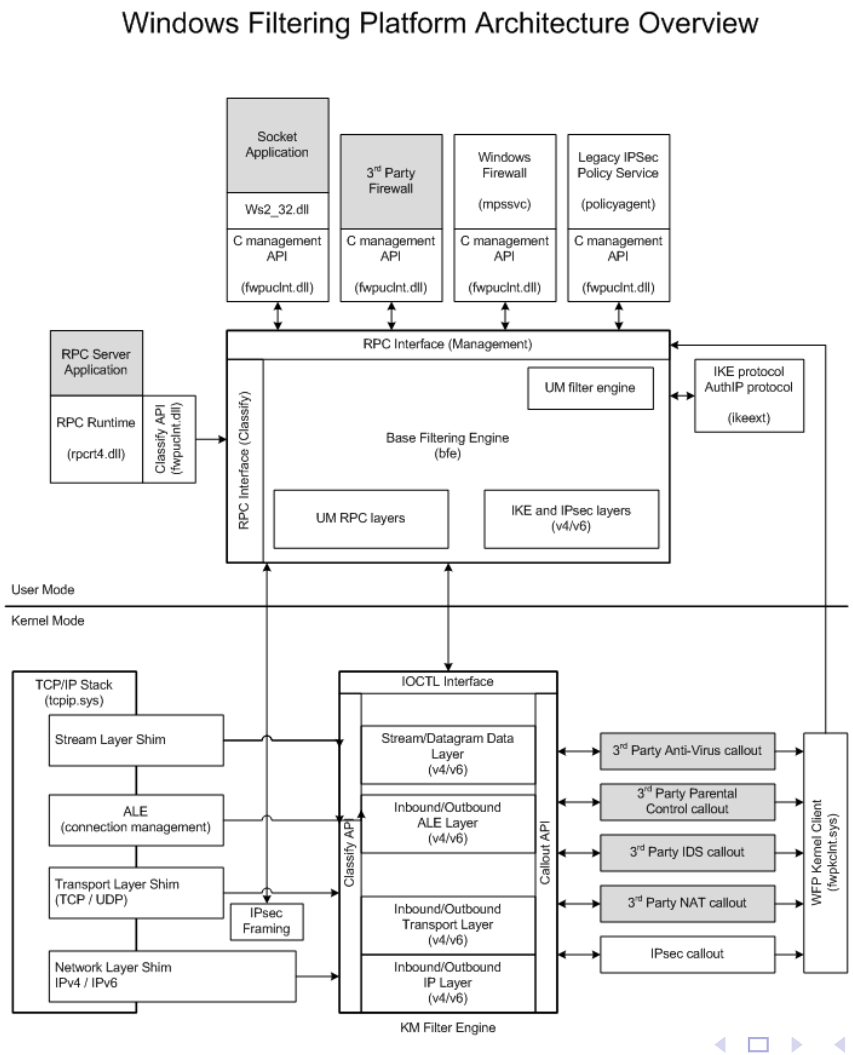
Osobní firewally pro OS Windows

- Nativní firewally jako komponenty operačních systémů Windows XP, Vista, 7, 8, 10 (rozdíly ve funkcionalitě).
- Komerční FW aplikace (McAfee Personal Firewall Plus, Norton Personal Firewall, ...), Freeware (Comodo Internet Security, Glasswire, ...), Open-source (PeerBlock, PeerGuardian,...).
- Konfigurace je většinou přes GUI.
- Komerční firewally přidávají další funkce jako IDS/IPS, Spyware detection, Malware blocking,...

Windows Firewall

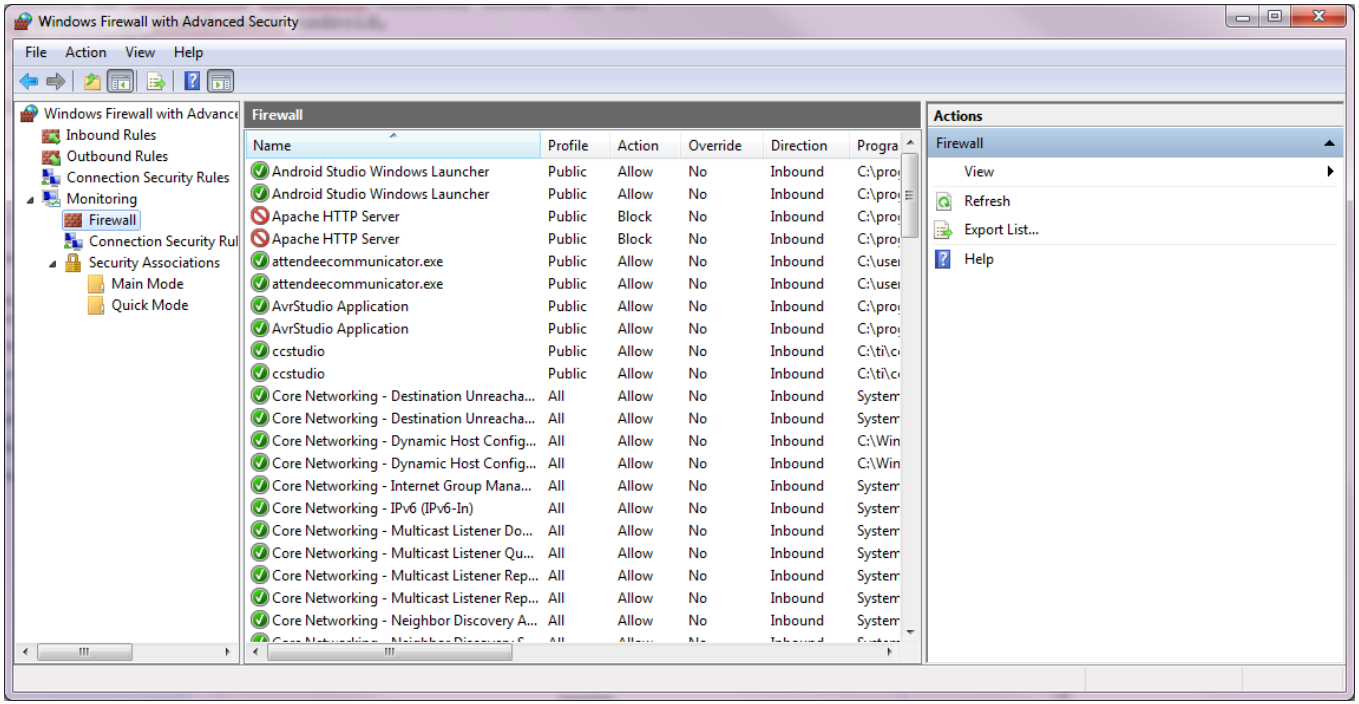
- Dostupné (u W7 a W10) pod Control Panel: System and Security: Windows Firewall.
- Změna názvu na Windows Defender Firewall (ve MS W10).
- **Windows Filtering Platform** (WFP) pracuje se stackem TCP/IP. Na vrstvách Layers pomocí pravidel (filters) a pomocí shims (malé knihovny, které přerušují volaní API) prohledává vnitřní strukturu paketů klasifikuje a filtruje provoz. Dále používají i funkce callouts pro NAT, IDS a malware detekce.
- 3 profily: Public (přísné pravidla), Private (méně přísné), Domain (nejméně přísné).
- Odchozí filtr proti malwaru, paketový filtry, filtr služeb, IPSec, Kerberos,...

Windows Filtering Platform Architecture



Windows Firewall na W7 a W10

Rozhraní pro Firewall na OS Windows 7 a 10:



Firewally pro UNIX a Linux systémy

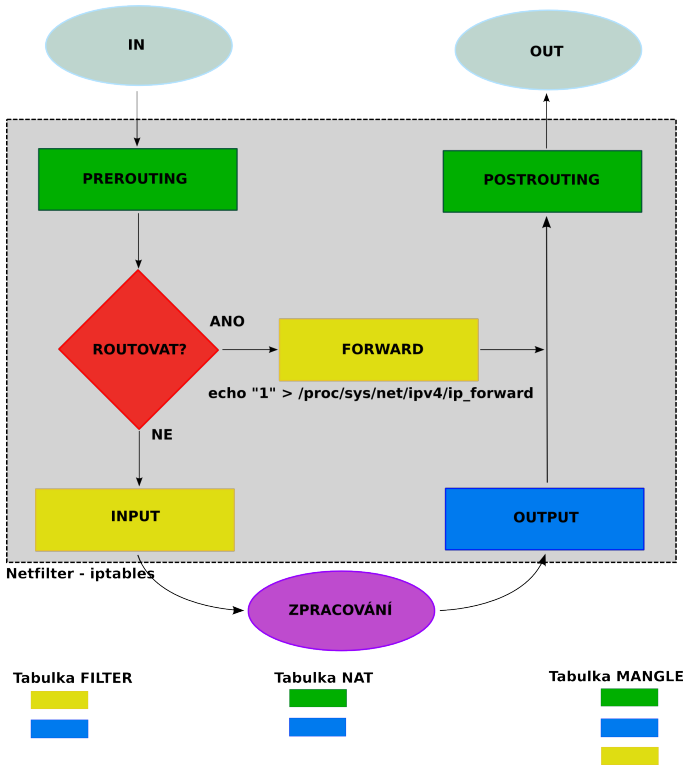
- **IPFilter** (ipf) je open source softwarový balíček poskytující **stavový firewall** a překladač adres (NAT) na UNIX-like OSs (např. Solaris, FreeBSD, UnixWare atd.).
- NPF je stavový paketový filtr pod BSD licencí (2012).
- **PF (Packet Filter, pf)** je stavový paketový filtr pod BSD licencí tvořící hlavní část programu u firewallů na OS: FreeBSD, Debian GNU, Mac OS X 10.7 a další.
- NetFilter/**iptables** filtrují příchozí, odchozí a přesměrovávaný provoz, součástí od Linux Kernel v 2.4.
- **nftables** je následníkem iptables (Linux Kernel v 3.13 - 2014) poskytující filtraci paketů a jejich klasifikaci.
- **ipfirewall** (**ipfw**) je FreeBSD IP paketový filtr (byl nasazen na **Mac OS X**).
- Další firewally na Unix/Linux: FireHOL, Firestarter, Shorewall, MoBlock, m0n0wall, SmallWall, Squid,....

SW Firewally pro nasazení do sítě

- **SW firewally** bežící na klasickém HW (PC, Server) mající **min. 2 síťová rozhraní**.
- NetFilter/iptables využity jako core v mnoha HW firewallech (např. Mikrotik).
- iptables - kolekce tabulek (5 typů), které obsahují dále řetězce (chains), což jsou sady pravidel (rules) v pořadí pro jednotlivé směry.

Princip Netfilter/iptables

- Základní chainy: **INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING**.
- Tabulky: **filter - pro filtraci, nat - pro změnu IP, mangle - pro změny parametru, jako např. TOS/QoS/TTL**.



Konfigurace firewallu iptables

Zápis ve formě:
iptables [tabulka] [akce] [chain] [ip_část] [match] [target/jumps] [target_info]
Základní příkazy [akce] s chainy:

- `-A chain` přidá pravidlo na konec chainu,
- `-I chain` přidá pravidlo do chainu na začátek nebo na určené místo,
- `-D chain` zmaže pravidlo,
- `-N chain` vytvoří nový chain,
- `-P chain` nastaví defaultní politiku firewallu.

Parametry [match]: -p (protokol), -s (zdroj - adresa/maska), -d (cíl), -i (in-interface), -o (out-interface), ...
[target/jumps]: -j ACCEPT/DROP/REJECT/LOG...

Příklady konfigurace iptables

Example

```
iptables -P INPUT ACCEPT
iptables -P INPUT DROP
```

Example

```
iptables -A INPUT -s 192.168.1.2 -p tcp --dport 23 -j ACCEPT
iptables -D INPUT -s 192.168.1.2 -p tcp --dport 23 -j ACCEPT
iptables -I OUTPUT -o eth1 -p !  udp -j DROP
iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 23 -j DROP
iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A PREROUTING -t nat -o eth1 -j DNAT --to-adress 124.56.34.5-124.56.34.8
```

Example

```
iptables -A INPUT -p tcp --tcp-flags ALL FIN,URG,PSH -m limit --limit 5/h --limit-burst 3 -j LOG
--log-prefix "Firewall:Weird_packets-- "
```

Virtuální firewally

- Využívají běžně dostupný HW.
- 2 síťové rozhraní pro příchozí/odchozí provoz.
- **Vyatta** - virtuální stavový firewall a router pro IPv4/6, konzolová nebo webová konfigurace, Debian, běžící na x86-46 serverech, lze i do VMware. Přerušen vývoj, poslední verze 2012. Pokračování jako **DANOS** vR od 2018.
- pfSense - open source firewall/router (FreeBSD), který lze instalovat na PC nebo virtuální stroj pro filtraci v síti.

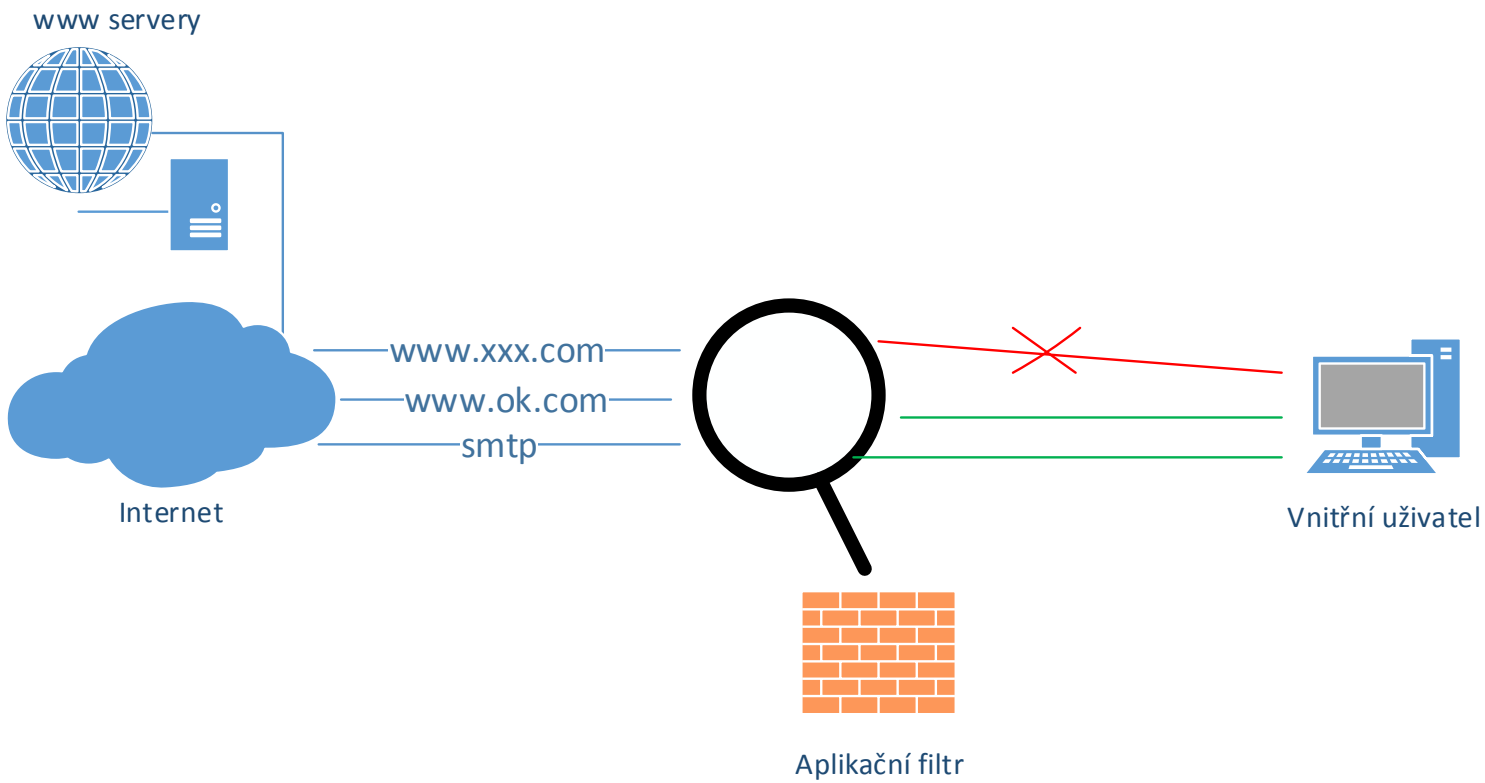
Aplikační filtry

Aplikační filtry

- Filtry na aplikační úrovni (7 vrstva ISO/OSI).
- Bývají **součástí mnoha firewallů**, ale také mohou fungovat **samostatně**.
- Náročné na výpočetní výkon zařízení, na HW filtru/firewallu.
- Sofistikovaná analýza aplikačních protokolů (HTTP, FTP, SMTP,...).
- Testování socketů (dat) i procesů - vyhodnocení - **větší zpoždění**.
- **Mitigace a blokace malwaru** (worms, trojans), web.stránek, exploitů a kyber-útoků.

Aplikační filtry - dělení

- Aplikační filtry pro sítě.
- Aplikační filtry pro hosty.



Aplikační filtry pro sítě

- **Monitorují provoz** na aplikační vrstvě v rámci sítí.
- Chrání uživatele v síti, více hostů.
- Často se zaměřují na web služby a emaily.
- Další funkce poskytují blokaci malware, pokusů o zneužití chyb v aplikacích, a nebo závadného nebo nepovoleného obsahu.
- Např. A10 Networks Web Application Firewall, Citrix Netscaler, Wildfire Palo Alto, F5 ASM, Fortinet FortiWeb, Imperva,...

Aplikační filtry pro hosty

- Monitorují u aplikací vstupní, výstupní a systémové volání.
- Poskytují **ochranu aplikacím** běžící na konkrétním hostu (PC, Server).
- Umí filtrovat aplikace podle ID procesu.
- Běží obvykle na klasickém OS (Windows, Linux, Mac OS X).
- Náročnější na výkon.
- Neumí zabránit útokům, kdy dojde k zneužití a modifikaci procesů.
- Mandatory Access Control (MAC), Sandboxing, omezená působnost pro zranitelné služby.
- např. Kerio Control, AppArmor, Zorp, WinGate, WebKnight,...

Speciální filtry a firewally

- Specializované firewally, zaměřující se na konkretní aplikace (např. webové aplikace).
- **Webové aplikační filtry** - chrání aplikační/web servery před uživateli, čistí dotazy.
- **Distribuované firewally** (Distributed Web Application Firewall - dWAF) - separované části fyzicky rozmístěny na více místech v síti, lepší vlastnosti detekce a management, lepší ochrana v případě selhání jednoho zařízení.
- **Cloud-based web application firewall** - monitorování a filtrace provozu na požádání, nezávislost na HW a SW, detekce hrozby je navíc sdílena, silnější filtrace (např. u DDoS), např. Imperva, Ghaim, Wallarm, Autofocus PA, Cisco Stealthwatch + Cisco Security Packet Analyzer ...

Děkuji za pozornost!
Dotazy ?

malina@vut.cz

Reference I


Ingham, Kenneth a Stephanie, Forrest.
A history and survey of network firewalls.
University of New Mexico, Tech. Rep (2002).


Cheswick, William R., Steven M. Bellovin a Aviel D. Rubin.
Firewalls and Internet security: repelling the wily hacker.
Addison-Wesley Longman Publishing Co., Inc., 2003.


Lawrence C. Miller
CYBERSECURITY SURVIVAL GUIDE, Principles Best Practices.
Palo Alto Networks, Inc., 2016.