

OS - Bezpečnost 1

Firewall

Firewall

► Firewall:

- zařízení - ochrana počítače nebo **lokální počítačové sítě**
 - před škodlivými útoky zvenčí (WAN - internet)

► **Vnější útoky**

- U připojení počítačových sítí do Internetu
 - zabezpečení přístupové cesty do počítačové sítě
- Spojeno s monitoringem vstupních cest:
 - Získáme včas informaci:
 - někdo se pokouší prolomit naši ochranu

Firewall

► FIREWALL NENÍ ANTIVIR:

- Antivirový program: - kontroluje obsah dat/souborů/programů
 - Hledá škodlivý kód (řetězec dat) a porovnává se vzorky v databázi
 - Databáze musí být aktuální
 - Zpomaluje činnost počítače
- FireWall: - kontroluje komunikaci
 - kdo s kým a jak komunikuje (kdo posílá/přijímá data)
 - Kontroluje IPAdresy, porty (služby)...

Firewall

▶ **Vnitřní útoky**

- ▶ Vyřešení vnějších útoků:
 - není zdaleka vyhráno
- ▶ Je možné škodit i uvnitř počítačové sítě
 - Př. nevhodná práce se samotnými daty
 - Viry - zasílání informací / dat na cizí servery v internetu
- ▶ Navrhnout opatření:
 - K minimalizaci případné ztráty / odesílání dat

Firewall

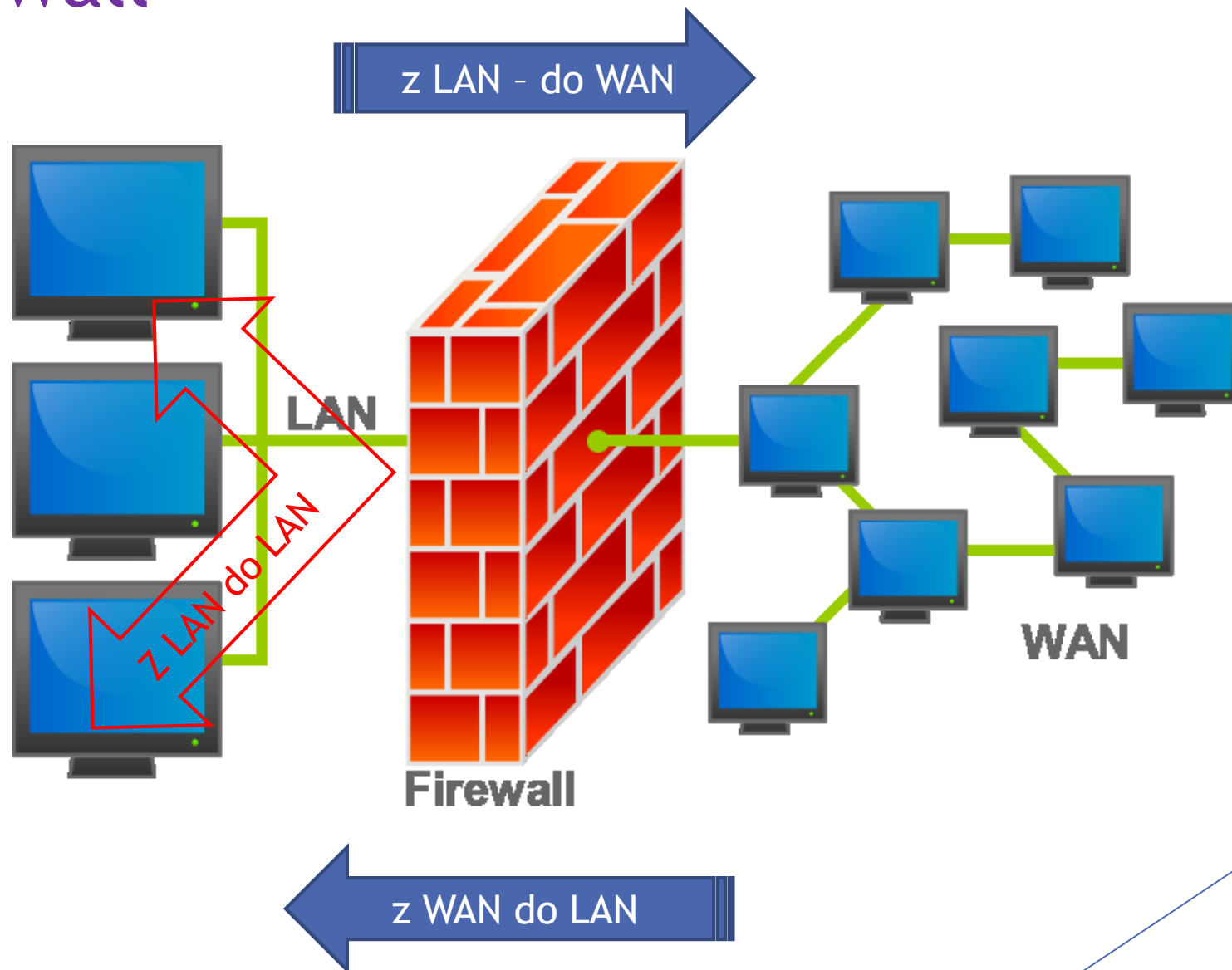
1) Ochrana jednoho počítače *(1.sít'.karta)*:

- ▶ jednoduchý osobní (personal) firewall
 - Instalován na koncovém zařízení

2) Ochrana LAN *(min. 2.sít'.karty)*

- ▶ odděluje LAN1 od LAN2 (LAN - WAN)
 - kontroluje tok **(ne obsah)** dat **mezi sítěmi**
 - může ale vykonávat i jiné složitější úkoly

Firewall

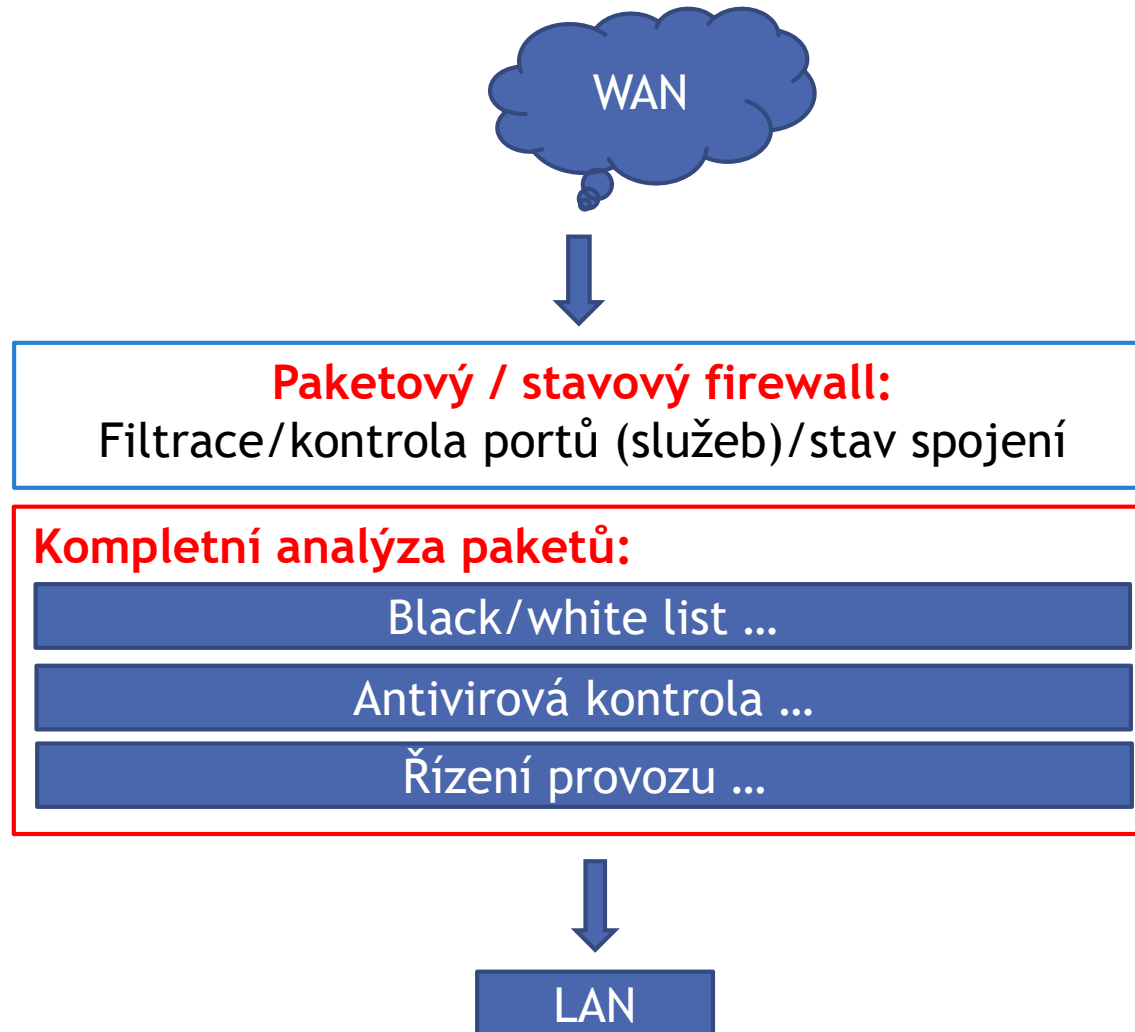


Firewall - druhy firewallů

1. Aplikační proxy server - proxy brána:

- ▶ Plnohodnotný „průchozí“ PC (2 sít'.karty)
 - Pro hloubkový dohled nad přenášenými daty
 - Včetně **antivirové ochrany**/ analýzy škodlivého obsahu
 - filtrování dat
 - řízení přístupu do LAN/WAN: autentizace/autorizace uživatele
 - Vyhrazen pro konkrétní/více služeb (DNS, Cache ...)
- ▶ Nevýhoda aplikačního proxy serveru:
 - **zpomalení** síťového provozu,

Aplikační proxy server - proxy brána:

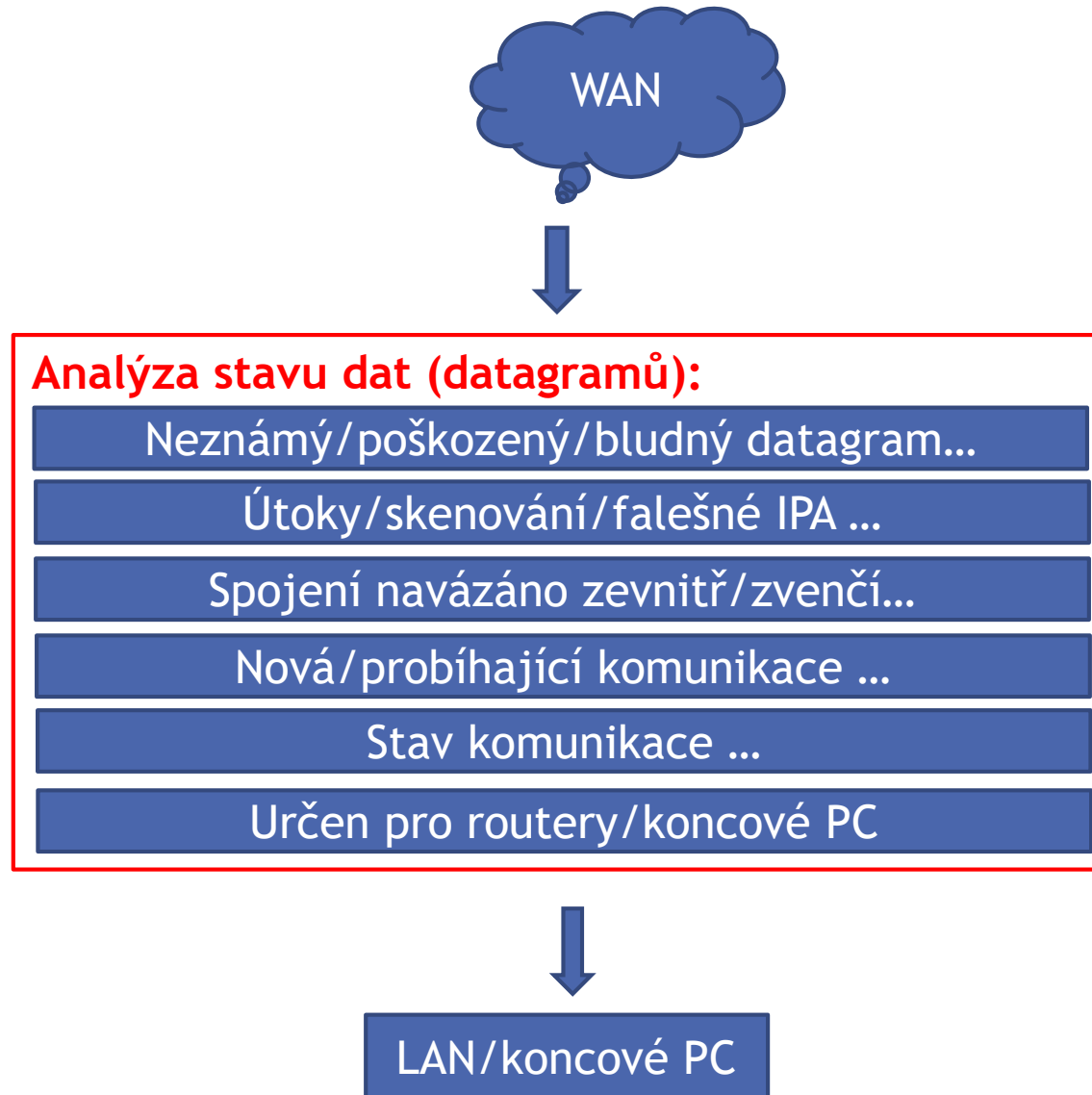


Stavový Firewall:

2. Stavový firewall:

- ▶ Speciální varianta filtru
- ▶ Sleduje spojení - **relační/transportní** vrstva OSI/ISO
 - Dokáže filtrovat datagramy podle stavu spojení
 - Zachovat probíhající spojení
 - Omezit nové relace

Stavový Firewall:



Stavový Firewall:

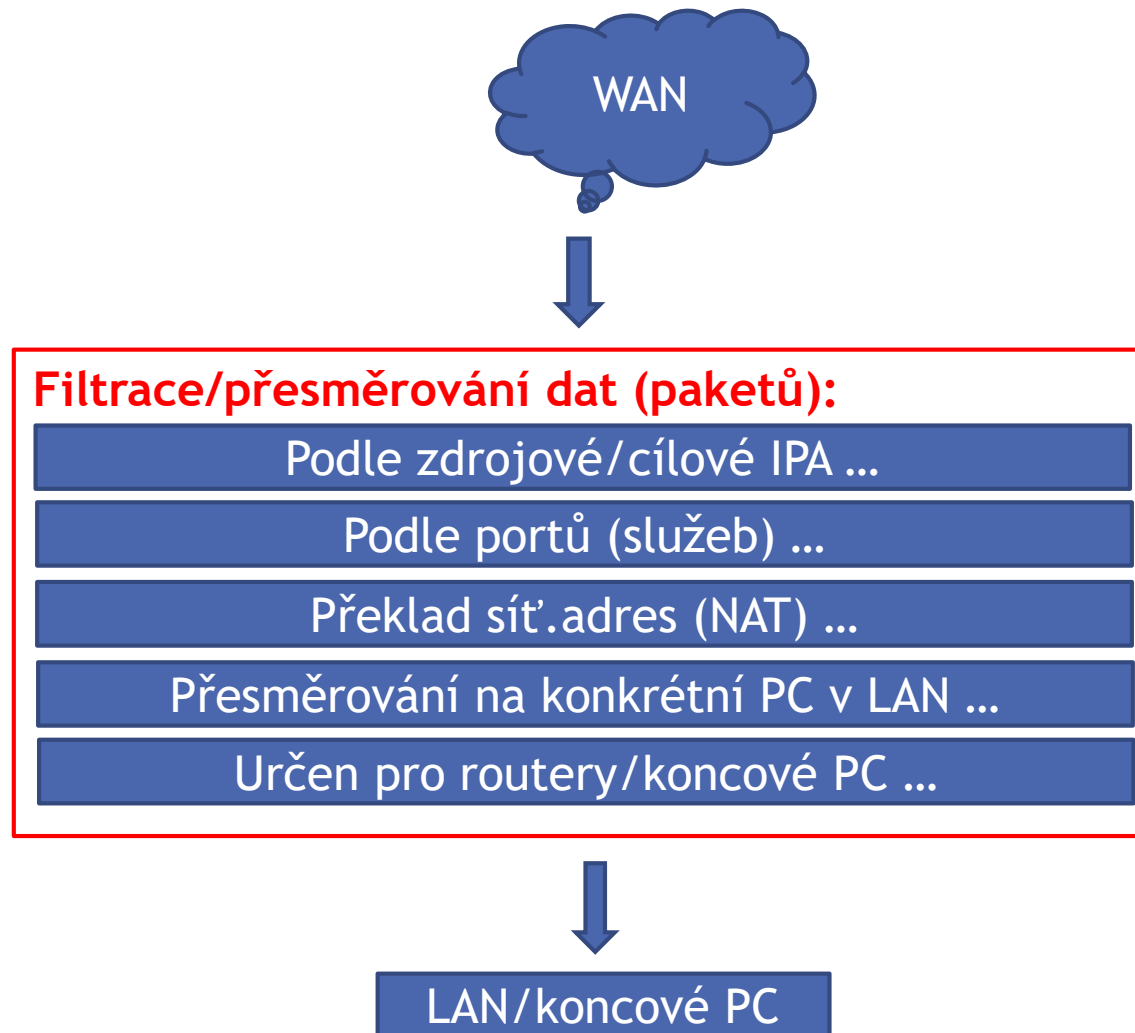
► Ochrana:

- proti skenování portů (programů, běžících v OSW)
- zjišťování typu OS
- falšování zdrojové IP adresy
- DoS/DDoS (Denial of Service) útoky
- ...

Paketový filtr Firewall

- ▶ sleduje síťový provoz,
 - IP adresy,
 - porty (služby - běžící programy),
- ▶ mnohem rychlejší než proxy
 - jeho správa je komplikovanější
 - nemá tolik možností jako aplikační/stavové proxy servery

Paketový filtr Firewall



Sítový firewall

► Realizace sítového firewallu:

► Na společném počítači - server

- již běží konkrétní služby - poštovní, web. a proxy server
- řešení je levnější, ale nebezpečné
- **ovládnutím serveru** - ovládnutí celé LAN

► Firewall na samostatném počítači

- Oddělení LAN od WAN
- vysoká bezpečnost - aplikační úroveň

Sítový Firewall - DMZ

► Demilitarizovaná zóna DMZ

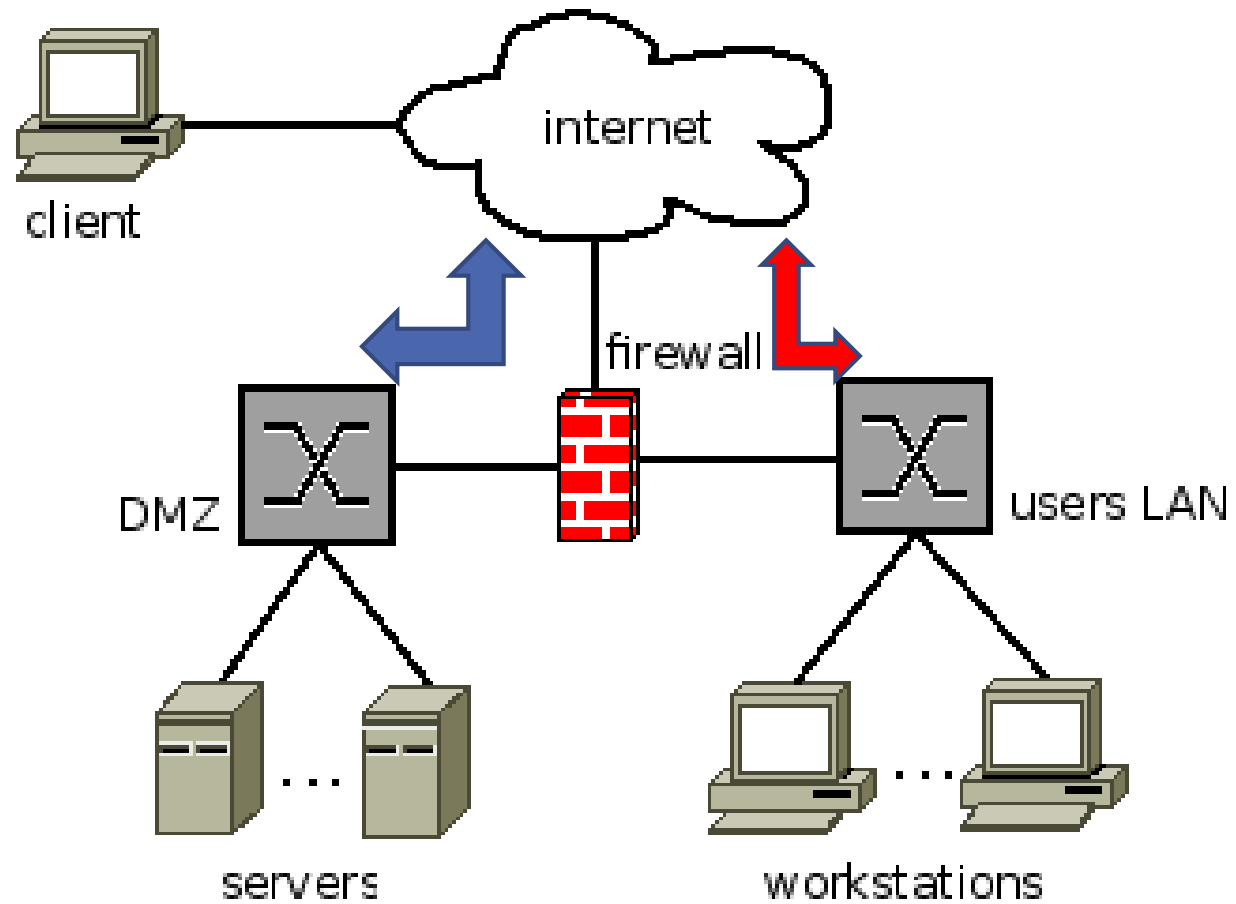
► Firewall na samostatném počítači pro 3 sítě

► 1. LAN, 2. WAN a 3. síť DMZ

- **DMZ** - jen pro přístup z WAN (**oddělena od LAN**)
 - Pro služby dostupné z WAN - Web, mail, ftp
- LAN server (LAN síť) - zcela odříznut od DMZ - ochráněn

► **Zvýšená bezpečnost** - aplikační úroveň

Firewall



Princip činnosti firewallu

► Princip firewall

- Realizuje **naše pravidla** co dělat s pakety
- **pravidla** pro manipulaci s pakety:
 - Obsahují **podmínky**
 - Obsahují **akce** (co s pakety)
 - 1) Propustit paket
 - 2) Zahodit paket
 - 3) Zahodit paket **s oznámením**

Princip činnosti firewallu

► Pravidla firewallu

► Potřebné informace pro pravidla z **headeru**:

- Zdrojová IP Adresa
 - **Source** (0.0.0.0 - od všech serverů/klientů)
- Cílová adresa IP Adresa
 - **Destination** (0.0.0.0 - všem serverům/klientům)
- Čísla Portů (kterých služeb se pravidla týkají),
- Příznaky - doplňující informace z paketu...

Princip činnosti firewallu

► Pravidla firewallu

- Pravidla se ukládají do tzv. **řetězů** (chain)
 - Jako „pole pravidel - zásobník pravidel“
- Pravidla se vybírají a realizují:
 - v definovaném pořadí (**od prvního uloženého ...**)

Princip činnosti firewallu

► Řetězce pravidel firewallu

- **INPUT** - pravidla pro příchozí pakety (z WAN -> do LAN)
 - do PC/routeru
- **OUTPUT** - pravidla pro odchozí pakety (z LAN -> do WAN)
 - z PC/routeru

► Implicitní nastavení:

- řetězce **prázdné - bez pravidel !!!**
- **Skoro vše dovoleno !!!**

Princip činnosti firewallu

► Řetězce pravidel firewallu

- **FORWARD** - pakety přeposílá (Router)
 - Pakety **nejsou** určeny pro toto zařízení - Router ale pro PC
 - pravidla **INPUT a OUTPUT se jich netýkají !!!**
 - Např.: LAN1 přeposílá pakety do LAN2
 - Co s nimi - se řeší **až v LAN2** (další FW)

► Implicitně je řetězec **prázdný - bez pravidel !!!**

Princip činnosti firewallu

► Akce pro pravidla:

► Definovány dvě základní akce pro pravidla:

1. povolit paket (**ACCEPT** - paket propustí)
2. zamítnout paket (**DROP/DENY** - paket zahodí)
 - zamítnout paket (**REJECT** - typ_hlášky)
 - zamítnutí se zdvořilou odpovědí

Příklad pravidel firewallu - script

► Pravidla pro zdrojovou/cílovou adresu paketu:

- parametr **-s** adresa/maska (**s**ource)
- parametr **-d** adresa/maska (**d**estination)

Př.: INPUT **-s** 10.6.6.6/24 -j DROP

Pakety pro 10.6.6.6 budou
zahozeny

► Podobně:

FORWARD **udp ! -d** 10.0.0.1 -j DROP

„!**!**“ neguje podmínku

Pouze pakety protokolu
UDP pro 10.0.0.1 budou
propuštěny

Filtrování portů - Router

Service Name		VideoIP			
No	Source Port		Destination Port		Transport
	Low	High	Low	High	
1	0	65535	1503	1503	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
2	0	65535	1720	1720	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
3	0	65535	3603	3603	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
4	0	65535	3230	3235	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other 17
5	0	65535	3230	3235	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
6	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
7	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6
8	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6

Filtrování portů - Router

Port Filtering

This page allows configuration of port filters in order to block specific internet services to all devices on the LAN. [Show more rows](#)

Start Port	End Port	Protocol	Enabled
<input type="text" value="0"/>	<input type="text" value="0"/>	Both ▾	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	Both ▾	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	Both ▾	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	Both ▾	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	Both ▾	<input type="checkbox"/>

APPLY

Firewall - Router

◉ Filtrace paketů

Př.:

- IP 0.0.0.0 - jakákoliv IP Adresa

• Zdroj IP	Port	Cíl IP	Akce
• 0.0.0.0	80	0.0.0.0	povolit
• 0.0.0.0	8989	0.0.0.0	zakázat

Firewall - Router

The screenshot shows the ASUS RT-N16 web interface. The left sidebar contains a menu with options: Network Map, UPnP Media Server, AiDisk, EzQoS Bandwidth Management, Advanced Setting, Wireless, LAN, WAN, USB Application, **Firewall**, Administration, and System Log. The main content area is titled 'Firewall - General' and includes a sub-header 'General' with tabs for 'URL Filter', 'MAC Filter', and 'LAN to WAN Filter'. The settings are as follows:

- Enable Firewall?**: ☒ Yes ☐ No
- Enable DoS protection?**: ☐ Yes ☒ No
- Logged packets type:**: None
- Enable Web Access from WAN?**: ☒ Yes ☐ No
- Port of Web Access from WAN:**: 8080
- Respond LPR Request from WAN?**: ☐ Yes ☒ No
- Respond Ping Request from WAN?**: ☐ Yes ☒ No

Red callout boxes with arrows point to specific settings:

- Zapnutí firewallu**: Points to 'Enable Firewall? Yes'.
- Ochrana proti DoS Denial of Service**: Points to 'Enable DoS protection? No'.
- Přístup do routeru z WAN IPAdresa:8080**: Points to 'Enable Web Access from WAN? Yes' and 'Port of Web Access from WAN: 8080'.
- Odpovídat na požadavky z WAN LPR – tisk, ping...**: Points to 'Respond LPR Request from WAN? No' and 'Respond Ping Request from WAN? No'.

Firewall - Router

The screenshot shows the ASUS RT-N16 web interface. The left sidebar contains a menu with items like Network Map, UPnP Media Server, AiDisk, EzQoS Bandwidth Management, and Firewall (highlighted). The main content area is titled 'Firewall - URL Filter' and includes tabs for General, URL Filter, MAC Filter, and LAN to WAN Filter. The 'URL Filter' tab is active, showing options to 'Enable URL Filter?' (Yes/No), 'Date to Enable URL Filter' (checkboxes for days of the week), and 'Time of Day to Enable URL Filter' (time range). Below these is a 'URL Keyword List' table with a 'Delete' button. Red arrows point from callout boxes to specific elements: 'Zapnutí filtrování adres' points to the 'Enable URL Filter?' section; 'Časový plán' points to the 'Date to Enable URL Filter' section; 'URL adresa: **www.aaa.bbb**' points to the 'URL Keyword List' table; and 'Seznam blokovanych adres' points to the 'Delete' button.

ASUS
RT-N16

Time: 02:29:16
SSID: ASUS
Firmware Version: 9.9.3.7

Language: English

General URL Filter MAC Filter LAN to WAN Filter

Firewall - URL Filter

To specify keyword, URL filter will block specific URL access from clients.

Enable URL Filter? ☐ Yes ☒ No

Date to Enable URL Filter: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time of Day to Enable URL Filter: 00 : 00 - 23 : 59

URL Keyword List

Delete

Apply

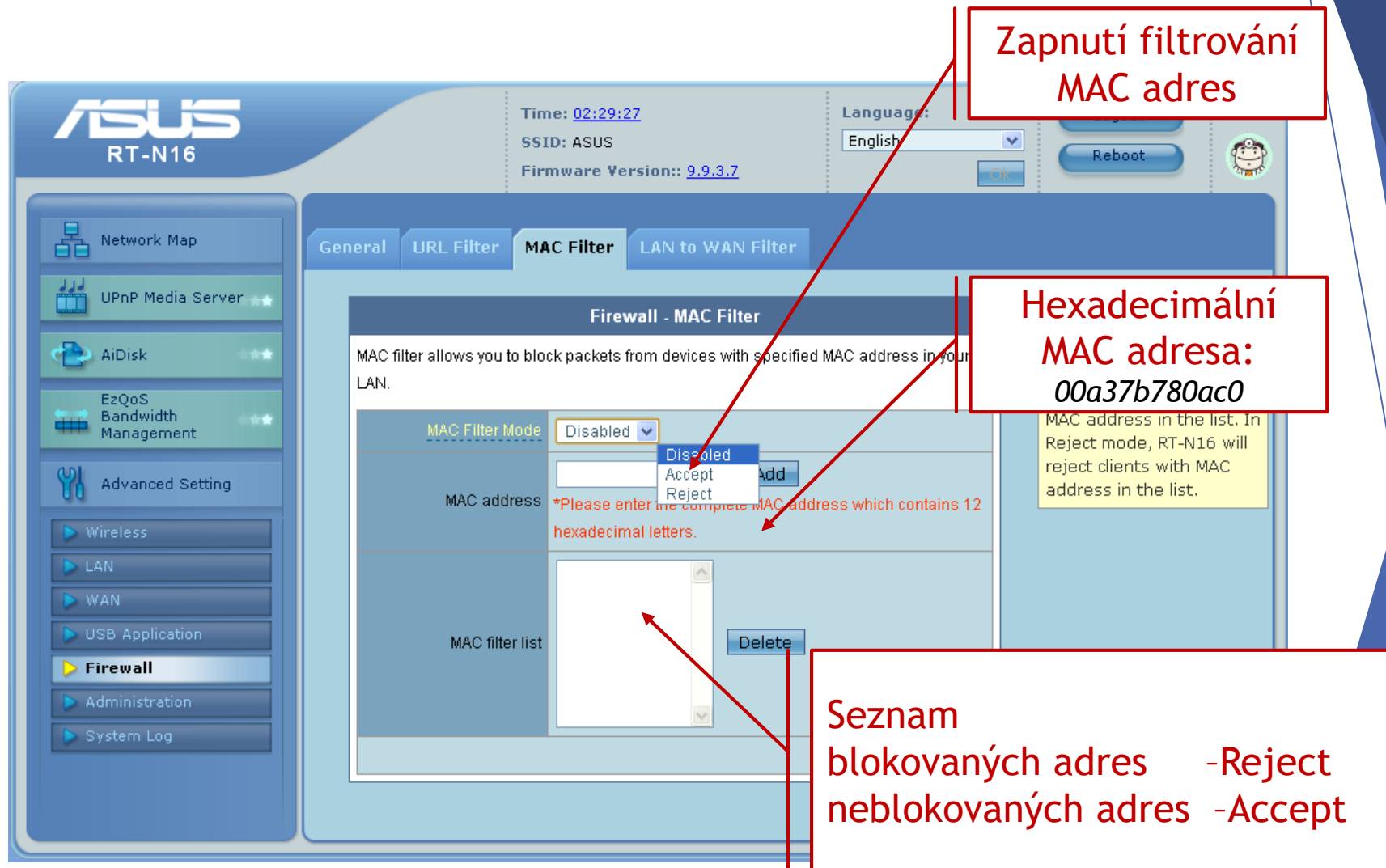
Zapnutí filtrování adres

Časový plán

URL adresa: **www.aaa.bbb**

Seznam blokovanych adres

Firewall - Router



ASUS RT-N16

Time: 02:29:27
SSID: ASUS
Firmware Version: 9.9.3.7

Language: English

Reboot

Network Map

UPnP Media Server

AiDisk

EzQoS Bandwidth Management

Advanced Setting

Wireless

LAN

WAN

USB Application

Firewall

Administration

System Log

General URL Filter **MAC Filter** LAN to WAN Filter

Firewall - MAC Filter

MAC filter allows you to block packets from devices with specified MAC address in your LAN.

MAC Filter Mode: Disabled

MAC address: *Please enter the complete MAC address which contains 12 hexadecimal letters.

MAC filter list

Delete

Disabled
Accept
Reject

MAC address in the list. In Reject mode, RT-N16 will reject clients with MAC address in the list.

Zapnutí filtrování MAC adres

Hexadecimální MAC adresa: 00a37b780ac0

Seznam blokovanych adres -Reject
neblokovanych adres -Accept

Firewall - Router

ASUS RT-N16

Time: 02:44:23
SSID: ASUS
Firmware Version: 9.9.3.7

Language: English

General URL Filter MAC Filter LAN to WAN Filter

Firewall - LAN to WAN Filter

LAN to WAN filter allows you to block specified packets between LAN and WAN. For example, if you want to prevent clients from surfing the web from 8:00 to 23:59 from Monday to Friday, you can check the date options from Mon to Fri and input time period 08:00-23:59 and selecting Black List as table type. Then, Add the rule which port range is 80 and Apply the setting.

Enable LAN to WAN Filter? ☐ Yes ☒ No

Filter table type: Black List

Date to Enable LAN to WAN Filter: White List Black List ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time of Day to Enable LAN to WAN Filter: 00 : 00 - 23 : 59

Filtered ICMP packet types:

LAN to WAN Filter Table

Well-Known Applications: WWW

Source IP	Port Range	Destination IP	Port Range	Protocol
			80	TCP

Add

Seznam filtrovaných adres:
Př.
Zdroj/port: 0.0.0.0:12345 (všechny)
10.11.10.11:54321 - na konkrétní PC

Časový plán
filtrace adres

Zapnutí filtrování
IP adres
BlackList - co není
v tabulce -
zahozeno