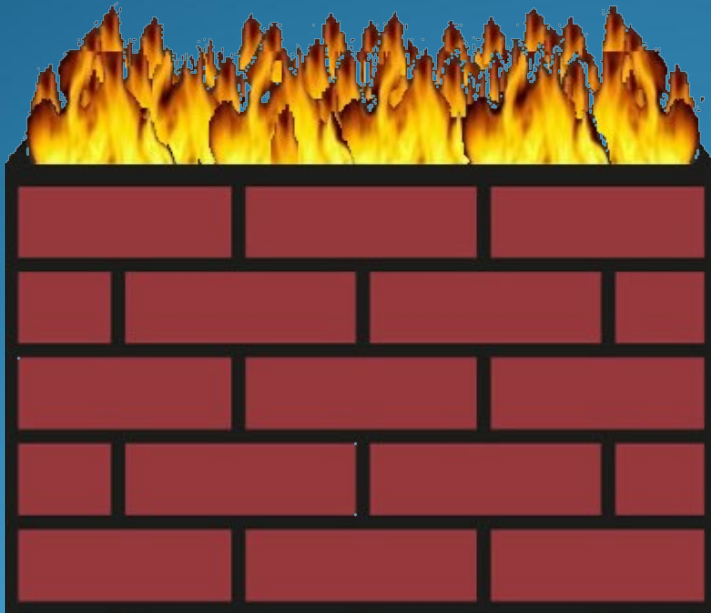


Firewall

Porty, NAT, rozdělení

- Lukáš Jakubík



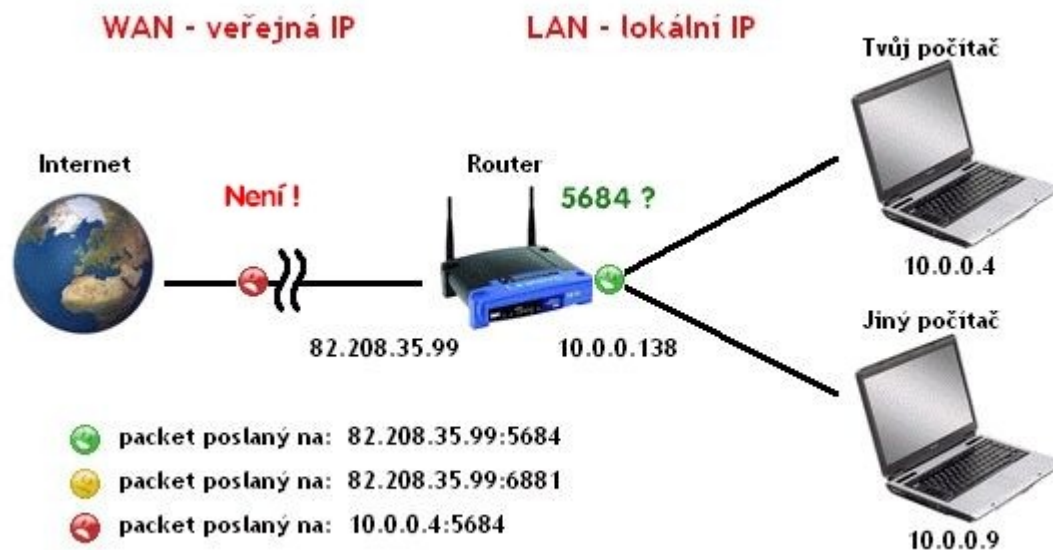
Port

- **Síťový port** je číslo, které slouží u protokolů TCP, UDP k rozlišení komunikace na dané IP adrese
 - portem se rozumí "dveře" nebo "brána" do počítače
 - na portu aplikace poslouchá a čeká na komunikaci
 - je daný číslem v rozsahu 0-65535
 - *IP adresa:port* 192.168.0.1:80
- typické porty
 - pro **ssh** 22, pro **smtp** 25, pro **web** 80, pro **https** 443
 - od 50000 volné, jinak rozdělení a registraci určuje IANA (Internet Assigned Numbers Authority)

NAT

- **NAT** (network address translation) je proces překladu vnější adresy na adresu z vnitřní sítě
 - nastavuje se v směrovači, NAT tabulka, pravidla typu *vnější IP adresa směrovače:port » vnitřní IP adresa:port*
 - typicky je potřeba
 - pro přístup k nějaké službě vevnitř sítě (web, mail, ssh)
 - pro přímý download (utorrent)
 - pro spojení počítačových her v síti apod.
 - v minulosti se pomocí NAT řešil nedostatek IPv4 adres

NAT tabulka



<http://www.utorrent.cz/help/img/portfrwd.gif>

25 - ADVANCED PORT FORWARDING RULES

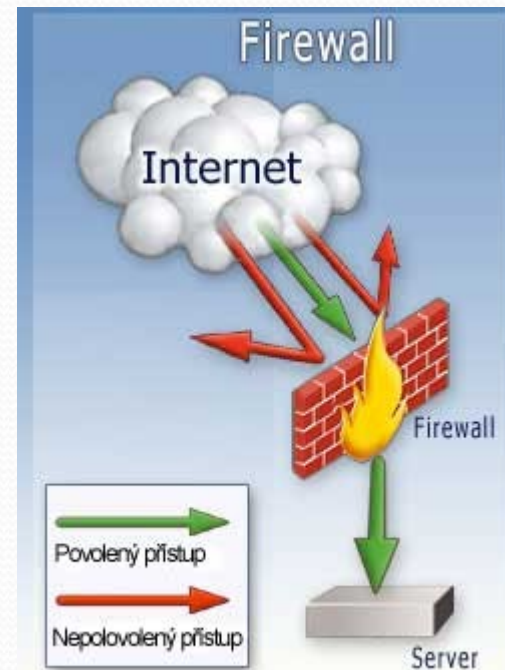
Remaining number of rules that can be created: 25

			Port	Traffic Type
<input checked="" type="checkbox"/>	Name utorrent	<< Application Name	Public Port 5684 ~ 5684	TCP
	IP Address 10.0.0.4	<< Computer Name	Private Port 10000 ~ 10000	

- první paket se směrovačem podle NAT tabulky doručí na tvůj počítač
- druhý paket směrovač zahodí jako nedoručitelný, protože pro něj nemá pravidlo v NAT
- třetí paket je ztracen již po cestě jako nesmyslný (má neveřejnou adresu)

Co to je firewall?

- Ohnivzdorná zeď, ale propustná, síto, co stojí mezi místní sítí (LAN) a světem (WAN)
- **Kontrolní bod**, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje
- Typy firewallů
 - hardwarově samostatné zařízení (i počítač) / **síťový**
 - softwarový nástroj v OS koncového počítače / **osobní**



<http://pctuning.tyden.cz/ilustrace3/zombux/firewall/firewall.jpg>

Principy firewallu

- Základním posláním je chránit počítače umístěné v síti za firewallem **před útokem zvenčí** pomocí
 - zavíráním portů, skrýváním počítačů (NAT tabulka)
 - aktivní kontrolou hlaviček paketů
 - aktivní kontrolou dat v paketech
- Některé pokročilejší firewally dokážou chránit i vnitřní počítače před únikem dat zevnitř ven
- Firewall **je řízen pravidly**, které bývají přednastaveny, ale nakonec vždy záleží na obsluze, co zakáže, nebo co (omylem) povolí

Historie vývoje firewallů

- 1. Nestavové paketové filtry
- 2. Stavové paketové filtry
- 3. Aplikační brány (proxy firewally)
- 4. UTM (Unified Threat Managment)

Paketové filtry

- **Paket** je blok dat přenášených v počítačových sítích, obsahuje hlavičku (režijní informace) a data
- **Paketový filtr** kontroluje pakety, z jaké adresy a portu přicházejí a na jakou adresu a port jdou
 - doručení paketu ovlivňují striktní pravidla v firewallu
 - výhodou je rychlá kontrola paketů
 - nevýhoda je nízká bezpečnost a často minimální přizpůsobitelnost, omezena jen na IP adresy a porty

Stavové paketové filtry

- **Stavové paketový filtry** navíc dokážou uchovat stav
 - po ustavení komunikace *IP:port <>> IP:port* si uloží stav a tuto komunikaci dále nekontrolují
 - mají režim, který nepovolí jinou komunikaci
 - výhodou může být ještě rychlejší kontrola
 - nevýhodou zůstává malá nastavitelnost a práce s pakety jen na síťové vrstvě

Aplikační brány

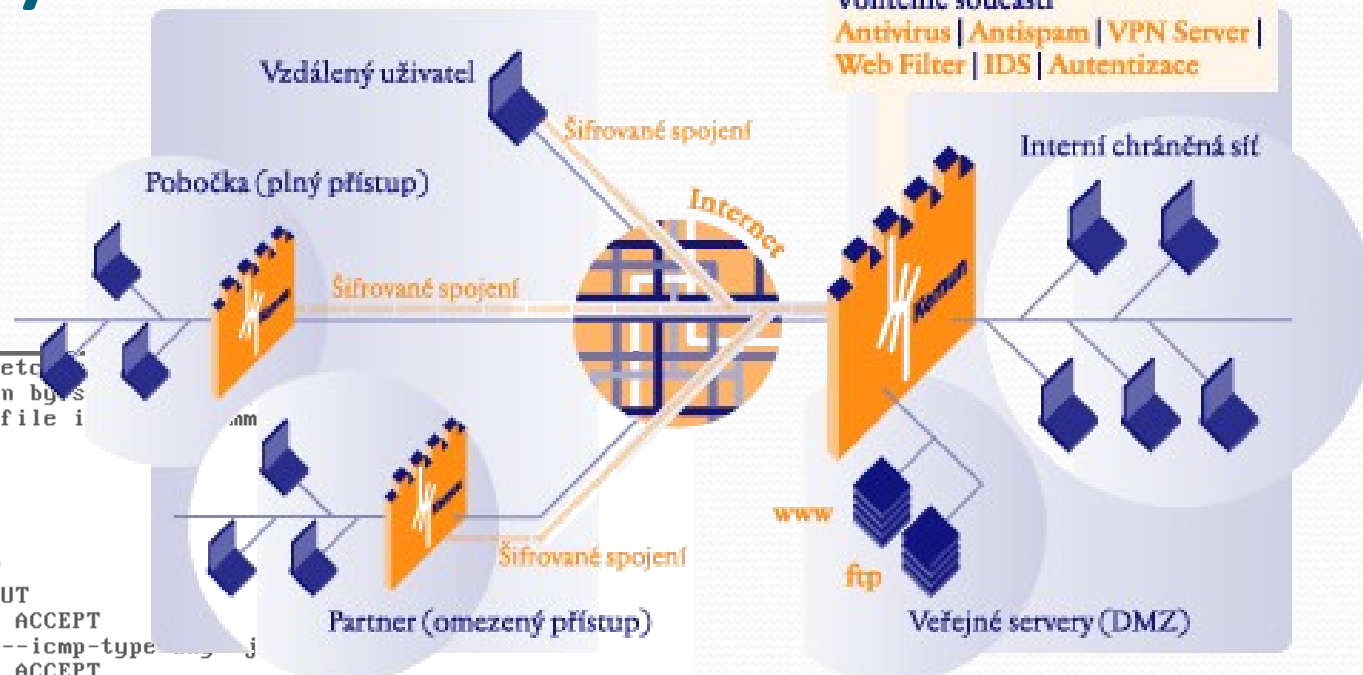
- **Proxy** je server, přes který jsou směrována data klientů
 - za účelem ochrany anonymity, nebo bezpečnosti
 - často i kvůli agregaci dat a filtrování obsahu
- **Aplikační brána** je firewall, který kontroluje pakety již na aplikační vrstvě pomocí svojí proxy
 - vynucená kontrola jdoucí až do vnitřku paketů, na data
 - možno zakázat jednotlivé příkazy, nebo akce uživatele
 - výhodou je vysoké zabezpečení, mnoho možností nastavení a filtrování
 - nevýhodou jsou vysoké požadavky jak na hardware, software, tak i na obsluhu

UTM

- **UTM (Unified Threat Management)**
 - komplexní řešení pro korporace, sjednocující vícero bezpečnostních prvků v jednom balíku
 - firewall
 - antivirus
 - anti-spam
 - antispyware
 - filtrování obsahu
 - detekce (IDS nebo IPS)
 - QoS (quality of service)
 - DMZ (demilitarized zone)
 - VPN...

Firewally na serverech

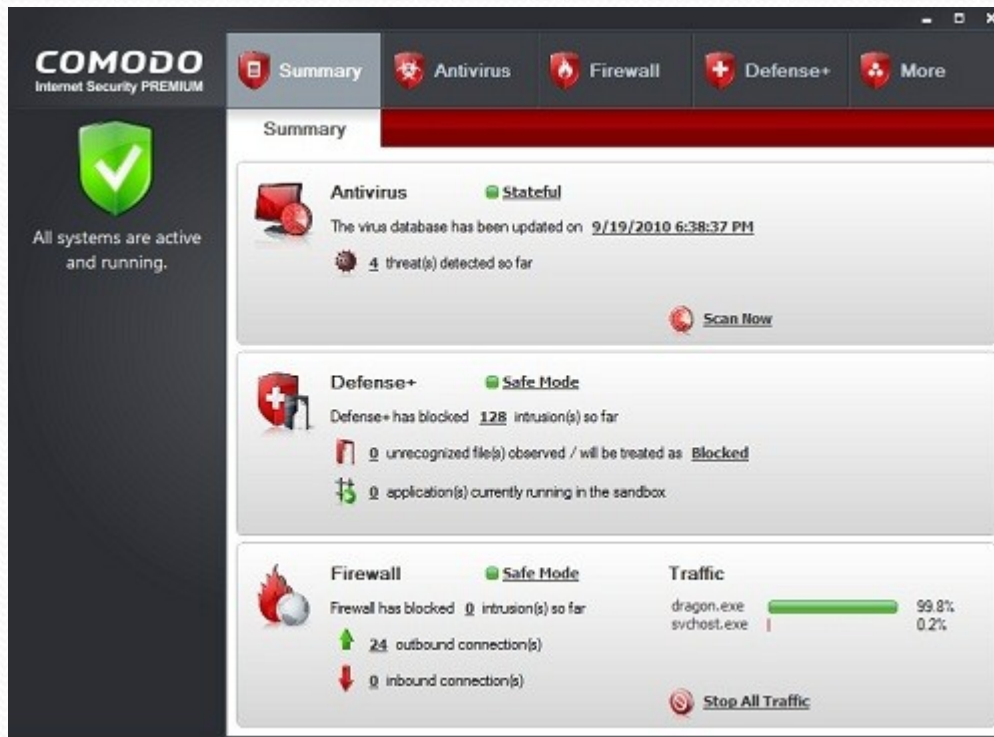
```
[root@localhost package]# cat /etc/passwd
# Firewall configuration written by s
# Manual customization of this file i
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@localhost package]# _
```



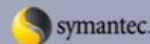
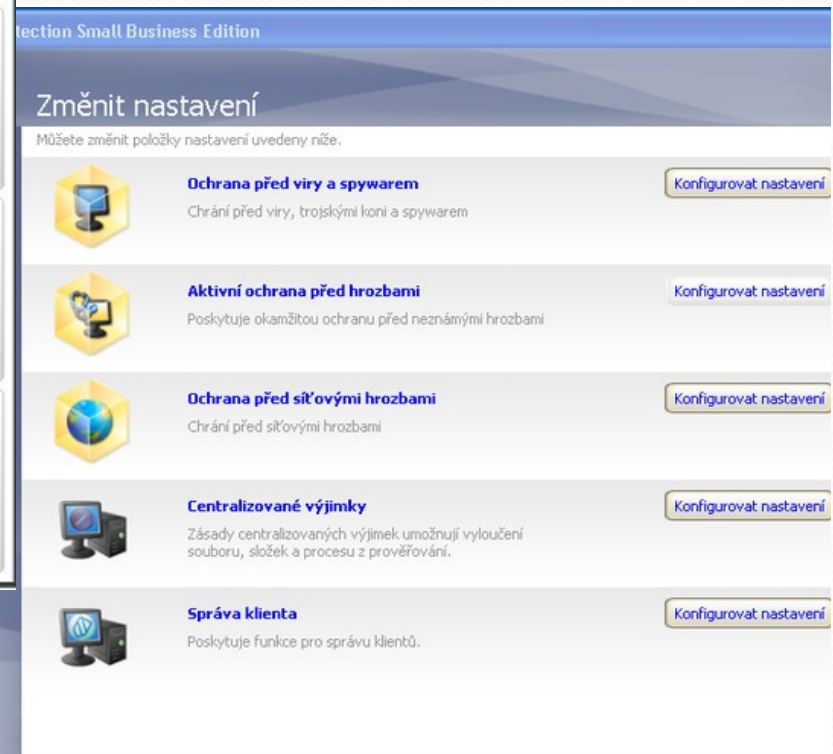
UTM Kernun

Paketový filter iptables

Firewally na stanicích



Osobní bezpečnostní balík Comodo



Klientská část firewallu Symantec Endpoint Protection



























































Symantec Endpoint Protection

- Jde o firewall s antivirem, byznys řešení na vícero PC, z dálky nastavitelný
- Obsahuje i IDS, který může kromě detekce útoků zvnějška zamezit i odnosu citlivých dat z firmy

Konfigurovat pravidla brány firewall

Pravidla brány firewall povolují, blokují a protokolují provoz sítě.

Název pravidla	Hostitelé	Porty a protokoly	Akce	Síťové adaptéry
<input checked="" type="checkbox"/> Povolit ovladač NDISUIO.SYS	Všichni hostitelé	Všechny porty a protokoly	Povolit	Všechny síťové a...
<input checked="" type="checkbox"/> Povolit protokol RDP (Remote Desktop Protocol)	Všichni hostitelé	Místní porty TCP 3389; příchozí prov...	Povolit	Všechny síťové a...
<input checked="" type="checkbox"/> Blokovat protokol IPv6 (sít Ethernet typu 0x86dd)	Všichni hostitelé	typ sítě Ethernet 34525; příchozí i od...	Blokovat	Všechny síťové a...
<input checked="" type="checkbox"/> Blokovat vzdálený port UDP 3544 protokolu IPv6 over IPv4 (Tere...	Všichni hostitelé	Vzdálené porty UDP 3544; příchozí i ...	Blokovat	Všechny síťové a...
<input checked="" type="checkbox"/> Povolit bezdrátový provoz protokolu EAPOL	Všichni hostitelé	typ sítě Ethernet 0x888E; příchozí i o...	Povolit	Všechny síťové a...

	Product	Product score	Level reached	Protection level	Recommendation	Report	Award
	Comodo Internet Security 4.0.141842.828 <small>FREE</small>	100 %	10+	Excellent – 100 %	GET IT NOW!		
	Online Solutions Security Suite 1.5.14905.0	99 %	10+	Excellent	GET IT NOW!		
	Outpost Security Suite Free 7.0.4.3418.520.1245.401 <small>FREE</small>	97 %	10+	Excellent	GET IT NOW!		
	Outpost Security Suite Pro 7.0.1.3376.514.1234.401	97 %	10+	Excellent	GET IT NOW!		
	Kaspersky Internet Security 2011 11.0.1.400	92 %	10+	Excellent	GET IT NOW!		
	Malware Defender 2.6.0	90 %	10	Very good	N/A		
	Privatefirewall 7.0.21.1 <small>FREE</small>	86 %	9	Very good	N/A		
	BitDefender Internet Security 2011 14.0.24.330	84 %	10+	Very good	GET IT NOW!		
	ZoneAlarm Extreme Security 9.1.008.000	59 %	7	Poor	Not recommended		–
	Rising Internet Security 2010 22.33.00.01	55 %	8	Poor	Not recommended		–
	PC Tools Firewall Plus 6.0.0.88 <small>FREE</small>	51 %	7	Poor	Not recommended		–
	Norton Internet Security 2011 18.1.0.37	40 %	6	Very poor	Not recommended		–
	Jetico Personal Firewall 2.1.0.7.2412	28 %	4	None	Not recommended		–
	Dr.Web Security Space Pro 6.0.2.07290	14 %	3	None	Not recommended		–
	CA Internet Security Suite Plus 2010 6.0.0.285	12 %	3	None	Not recommended		–
	F-Secure Internet Security 2010 10.00.246	9 %	2	None	Not recommended		–
	Trend Micro Internet Security Pro 2010 17.50.1647.0000	9 %	2	None	Not recommended		–
	FortKnox Personal Firewall 6.0.205.0	7 %	2	None	Not recommended		–
	ZoneAlarm Free Firewall 9.2.076.000 <small>FREE</small>	7 %	2	None	Not recommended		–
	ESET Smart Security 4.2.64.12	6 %	2	None	Not recommended		–
	avast! Internet Security 5.0.418.0	3 %	1	None	Not recommended		–
	Avira Premium Security Suite 10.0.0.542	3 %	1	None	Not recommended		–
	AVG Internet Security 2011 10.0.1153	3 %	1	None	Not recommended		–
	McAfee Internet Security 2010 11.0.378	3 %	1	None	Not recommended		–
	G Data Internet Security 2011 21.1.1.0	2 %	1	None	Not recommended		–

<http://www.matousec.com/projects/proactive-security-challenge/results.php>

Zdroje

- Wikipedia contributors. *Port number* [Internet]. Wikipedia, The Free Encyclopedia; 2011-01-13, 15:52 UTC [cit. 2011-01-17].
http://en.wikipedia.org/w/index.php?title=Port_number&oldid=407674054
- Příspěvatelé Wikipedie. *Firewall* [Internet]. Wikipedie: Otevřená encyklopedie; 2011-01-15, 01:34 UTC [cit. 2011-01-17]. Dostupné na:
<http://cs.wikipedia.org/w/index.php?title=Firewall&oldid=6351294>
- Řešení pro prostředí s vysokými požadavky na bezpečnost [Internet]. TNS, aktualizované 2008-07-17 [cit. 2011-01-17]. Dostupné na:
<http://www.tns.sk/prod/firewall.html>
- Wikipedia contributors. Symantec Endpoint Protection [Internet]. Wikipedia, 2011-01-12, 18:55 UTC [cit. 2011-01-17].
http://en.wikipedia.org/w/index.php?title=Symantec_Endpoint_Protection&oldid=407514757