Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Síťová bezpečnost – Firewally

Autor práce: Bc. Bohuslav Nepovím

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra informačního inženýrství | Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bohuslav Nepovím

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Síťová bezpečnost – Firewally**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Teoretická část - počítačové sítě, síťová bezpečnost
4. Popis jednotlivých firewallů - HW, SW
5. Klady, zápory a cenová kalkulace jednotlivých řešení
6. Praktický příklad SW řešení
7. Závěr
8. Seznam použitých zdrojů
9. Přílohy

Rozsah hlavní textové části: 60 - 80 stran

Doporučené zdroje:

STREBE, Matthew, PERKINS, Charles. Firewally a proxy-servery : praktický průvodce. 1. vyd. Brno : Computer Press, 2003. 472 s. ISBN 80-7226-983-6

BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno : Computer Press, 2004. 992 s. ISBN 80-251-0178-9

NORTHCUTT, Stephen, ZELTSER Lenny, WINTERS Scott, FREDERICK Karen Kent, RITCHEY Ronald W. Bezpečnost počítačových sítí. 1. vyd. Brno: CP Books, 2005. 592s. ISBN 80-251-0697-7

THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. 1. vyd. Brno: CP Books, 2005. 338 s. ISBN 80-251-0417-6

PETERKA, Jiří. E-archiv Jiřího Peterky : Počítačové sítě, verze 3.4 [online]. [2009]. Dostupný z WWW: <http://www.earchiv.cz/l220/index.php3>.

Vedoucí diplomové práce: **Ing. Martin Papík**

Termín odevzdání diplomové práce: duben 2011

L.S.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 3. 2. 2010

Evidováno děkanátem PEF pod č.j.: KII-057-10D

Prohlášení autora práce

Prohlašuji, že jsem diplomovou práci na téma „Síťová bezpečnost – Firewally“ vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Pardubice 18. března 2011

_____

Bc. Bohuslav Nepovím

Poděkování

Děkuji vedoucímu diplomové práce panu Ing. Martinovi Papíkovi, Ph.D. za všechny rady a připomínky, které mi pomáhaly při tvorbě této diplomové práce.

Síťová bezpečnost – Firewally

Network security - Firewalls

Souhrn:

Tato diplomová práce se zabývá bezpečností počítačových sítí. V teoretické části postupně popisuji základní principy počítačových sítí, bezpečnost počítačových sítí, možné síťové útoky a ochranu proti nim, sociální inženýrství, funkce firewallů a různá zapojení firewallů v síti. V praktické části pak popisuji testování zranitelnosti osobních firewallů programem Nessus a pomocí utilit, tzv. leak testů. Nessus hledá zranitelná místa, leak testy prověřují zdatnost firewallu detekovat neoprávněnou odchozí komunikaci do Internetu. Všechny výsledky testů jsou pak vzájemně porovnány a vyhodnoceny.

Klíčová slova:

Autentizace, Autorizace, DMZ, DNS, Firewall, IDS, IPS, NAT, PROXY, VPN

Summary:

This thesis deals with the security of computer networks. A theoretical part gradually provides the description of fundamental principles of computer networks, computer network security, possible network attacks and protection against them, social engineering, functions of firewalls and various integration of the firewalls in the network. The practical part consequently describes personal firewall tests by means of the Nessus program, and utilities, so-called the leak tests. Whereas the Nessus searches for vulnerable places, the leak tests verify the efficiency of firewall in detecting unauthorized outbound communication to the Internet. Afterwards, all the test results are mutually compared, and evaluated.

Key words:

Authentication, Authorization, DMZ, DNS, Firewall, IDS, IPS, NAT, PROXY, VPN

Obsah

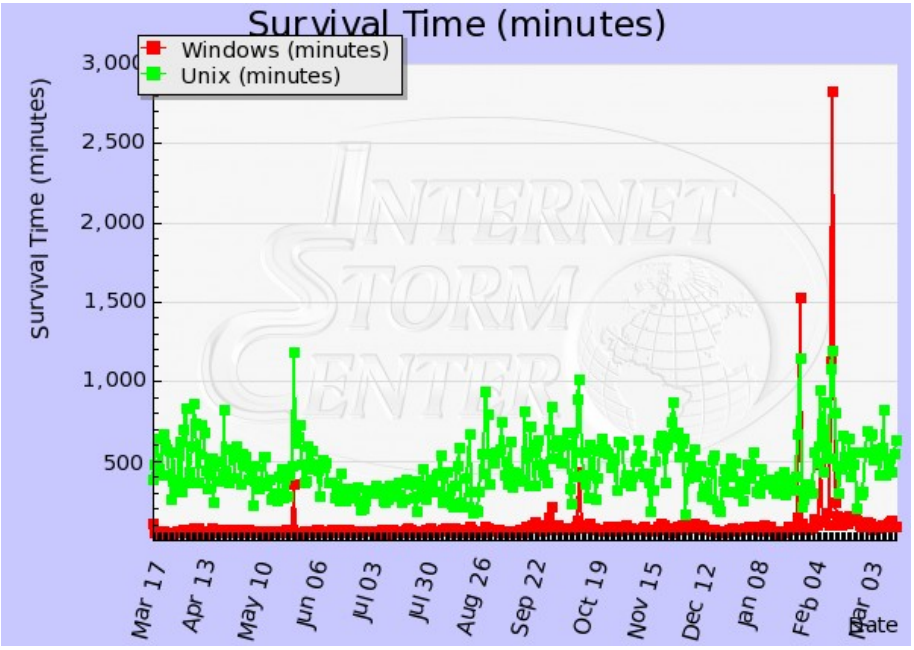
Seznam obrázků

Seznam tabulek

Úvod

Téma diplomové práce jsem si vybral na základě mého dlouhodobého zájmu o počítačové sítě a mé praxe v oboru, neboť pracuji ve školství jako správce počítačové sítě. Informatika jako taková nám pomáhá zjednodušovat, urychlovat a automatizovat práci, ať pracujeme v kterémkoliv oboru. V posledních několika letech se většina papírových formulářů digitalizuje, využívají se více informační systémy obsahující citlivé informace a v neposlední řadě narůstá i komunikace s veřejnou správou pomocí různých internetových portálů. Bohužel všechny tyto výhody, kterých využíváme nebo můžeme využívat, nesou s sebou i bezpečnostní rizika. Ať už se to týká virů, trojských koní, nevyžádaných e-mailů či přímých útoků na počítače či počítačové sítě, vždy se jedná o závažný problém, který nám může způsobit nevratné škody. Proto je zapotřebí těmto rizikům předcházet, a to nejen zabezpečením počítačové sítě, ale také dodržováním bezpečnostních pravidel od uživatelů, kteří v této síti pracují. Bezpečnostní uvědomění uživatelů se především vyplatí při útocích typu takzvaného sociálního inženýrství.

V současnosti je k Internetu připojeno na miliony serverů a stanic, které jsou potencionálními cíli pro útočníky. Podle studie Internet Storm Centrum (ISC) spadající pod SANS institut zabere útočníkům méně než pět minut najít a kompromitovat počítač s operačním systémem Windows bez potřebných záplat a aktualizací systému, u systému Unix je zapotřebí několika hodin.



Obrázek 1 - Životnost instalací operačních systémů bez záplat a aktualizací; zdroj [9]

Obrázek (Obrázek 1) ukazuje statistiku životnosti operačních systémů (Windows, Unix) v minutách (osa y), přičemž se jedná o údaje za posledních 12 měsíců (osa x, březen 2010 – březen 2011). ISC ve svém výzkumu zaznamenávalo časy mezi připojením do sítě a úspěšným průnikem hackera do systému, který pak tento systém kompromitoval programem typu exploit či worm.

Řada domácích uživatelů a jejich systémů připojených k Internetu je vystavena neustálému nebezpečí, za uvedenou dobu není schopný uživatel stáhnout z Internetu ani potřebné aktualizace. Výsledek studie ISC údajně věrně reprezentuje skutečnou situaci, kterou řada lidí stále podceňuje.

1 Cíl práce a metodika

Cílem mé diplomové práce je vysvětlit každému zájemci základní informace o bezpečnosti počítačových sítí, jak síť funguje, jaké hrozby nám hrozí a jak se jim můžeme bránit. Čtenář tedy nemusí být žádným IT profesionálem, a přesto věřím, že má práce bude přínosem opravdu každému. Svým jednoduchým výkladem podávám vysvětlení nejdůležitějších pojmů z oblasti bezpečnosti, na kterých se dá dále stavět. Po přečtení mé práce by si měl čtenář uvědomit, že skutečná bezpečnost se nedá koupit v nějakém jednom produktu, ale že je to celá řada procesů, do nichž jsou kromě produktů zapojeni také zaměstnanci organizace.

V teoretické části, v kapitole *Počítačové sítě* vysvětluji základní pojmy a principy počítačových sítí, jak komunikace na síti vůbec funguje. Popisuji také jednotlivé vrstvy modelu TCP/IP. V další kapitole *Síťová bezpečnost* vysvětluji průběh útoku, jednotlivé možnosti síťových útoků a techniky sociálního inženýrství. V této kapitole se také zmiňuji o různých možnostech prevence a ochrany proti těmto hrozbám. V kapitole *Firewally* vysvětluji základní funkce firewallů, různá zapojení firewallů v síti, členění dnešních firewallů a pro porovnání uvádím i cenu SW a HW řešení.

Po praktické stránce pak otestuji, porovnám a vyhodnotím kvalitu několika osobních firewallů. Pro toto testování jsem vybral samostatné firewally bez antivirové ochrany, které jsou na Internetu zdarma ke stažení. Tyto osobní firewally jsou určené především pro domácí použití, licencované jako freeware. Testování zranitelnosti osobních firewallů provedu programem Nessus a za pomocí utilit, tzv. leak testů. Nessus hledá zranitelná místa, leak testy prověřují zdatnost firewallu detekovat neoprávněnou odchozí komunikaci do Internetu.

2 Počítačové sítě

Počítačová síť je skupina propojených počítačů a používá se ke sdílení informací mezi lidmi, správě prostředků a zabezpečení. Počítače v počítačových sítích používají pro vzájemnou komunikaci síťové protokoly. Síťovým protokolem rozumíme soustavu předpisů definující pravidla pro vzájemnou spolupráci dvou sítí. Síťových protokolů existuje celá řada. V Internetu se používají síťové protokoly TCP/IP (Transmission Control Protocol / Internet Protocol), které tvoří rozsáhlou soustavu protokolů. TCP/IP je v dnešní době standardní sada protokolů určená pro propojení a komunikaci rozlehlých sítí WAN. Byla vyvinuta v roce 1969 americkou agenturou DARPA (Defense Advanced Research Projects Agency) jako výsledek experimentu se sdílením prostředků nazvaného ARPANET (Advanced Research Projects Agency Network).
Informace pro tuto kapitolu jsem čerpal ze zdroje [1], [3], [10].

2.1 Základní pojmy

Ze všeho nejdříve si vysvětlíme základní pojmy, na které budu později odkazovat. Vysvětlíme si a sjednotíme definice základních prvků jako směrovač, firewall, VPN a další.

Obvod sítě představuje zabezpečené hranice sítě, do nichž mohou patřit: směrovače, firewally, IDS, VPN, demilitarizované zóny a podsítě.

Směrovač je zařízení, které vzájemně propojuje dvě nebo více sítí. Řídí provoz vedoucí dovnitř sítě a ven z ní. Často se stává ústředním bodem zabezpečení sítě.

Hraniční směrovač je pak poslední námi řízený směrovač před vstupem do Internetu. Prochází přes něj veškerý internetový provoz dané organizace, a proto se svým prvotním a závěrečným filtrováním často slouží jako první a zároveň poslední linie sítě.[1]

Firewall je síťové zařízení, které pomocí množiny pravidel povoluje či zamítá síťový provoz. Filtrování provozu je v něm mnohem důkladnější než ve směrovači. Firewally dle funkce dělíme na statické paketové filtry, stavové firewally a proxy firewally. Firewally slouží k ochraně síťových počítačů před operacemi, které by mohly vést k napadení interních počítačů, a tím pádem poškození jejich dat, nebo odepření služeb pro oprávněné uživatele.

[1] NORTHCUTT, Stephen a kol. *Bezpečnost počítačových sítí*, s. 12

NAT (překládání síťových adres) překládá IP adresy interních hostitelských počítačů a skrývá je před monitorováním zvenčí. Funkci NAT se někdy také říká maskování IP adres.[2]

DMZ (demilitarizovaná zóna) je rozhraní, umístěné mezi důvěryhodným a nedůvěryhodným segmentem sítě (mezi firemní sítí a Internetem). Funguje jako „nárazníkové pásmo“ pro ochranu serverů a služeb, dostupných z veřejného internetu.

VPN (virtuální privátní síť) je v podstatě zabezpečené připojení, které je pomocí šifrovacích nebo autentizačních technologií zavedeno nad existující veřejnou infrastrukturou, čímž se vytvoří „virtuální“ segment mezi dvěma entitami, které k sobě mají přístup. VPN lze vytvářet přes sdílenou infrastrukturu místní sítě LAN, WAN nebo přes veřejnou infrastrukturu internetu.

IDS (systém detekce vniknutí) funguje jako poplašný systém, který detekuje síťové narušení. Jeho úkolem je identifikování útoků a bezpečnostních incidentů, a tím může enormně zlepšit celkovou bezpečnost sítě.

2.2 Model TCP/IP

Abychom mohli popsat, jak firewally fungují, musíme si nejdříve vysvětlit, jak probíhá komunikace na síti, v Internetu. Proto se budeme zajímat o protokol TCP/IP. Příčiny úspěchu rozšíření tohoto protokolu jsou:

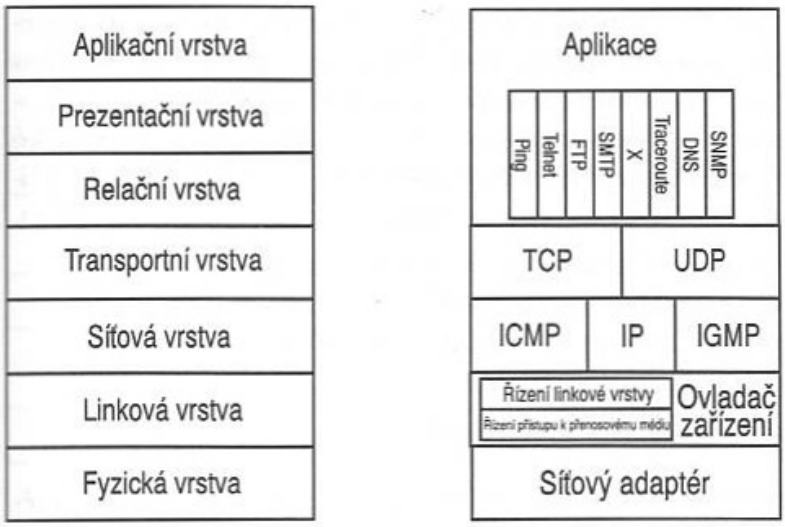
- Je založený na paketech, může přes jedno síťové propojení posílat data na více komunikujících počítačů. Sítě založené na paketech jsou levnější a snadněji se implementují.
- Umožňuje decentralizované řízení. Každá síť komunikující přes protokol TCP/IP má svůj interval adres, jež může přidělit počítačům v uvedené síti.
- Zařízení, která spolu komunikují, jsou na stejné úrovni. Každý počítač může iniciovat nebo přijímat síťová připojení nezávisle na ostatních počítačích.
- Je směrovatelný. Pomocí směrovače lze přenášet data mezi dvěma nebo více LAN.
- Je nezávislý na konkrétním přenosovém médiu, funguje na Ethernetu, Token Ringu, ARCNetu, USB, sériových spojích nebo jiném mechanismu, který umožňuje mezi dvěma a více počítačům vyměňovat signály.
- Je otevřený standard publikovaný zdarma na Internetu a každý ho může použít.

[2] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce,* s. 4

- Nic nestojí, protokol může implementovat kdokoli.
- Je robustní, protokol zjišťuje a opravuje chyby při přenosu, dokonce umí při směrování obcházet poškozené části Internetu.

Protokol TCP/IP není ale ve všem dokonalý, mezi zásadní nedostatky patří adresace a zabezpečení. Původně bylo navrženo 32 bitové adresování, které v dnešní době již nedostačuje a nevěnovala se také žádná pozornost proti rizikům zabezpečení sítě. Nedostatek adresování se vyřešil zavedením IPv6, používá adresování o délce 128 bitů.

TCP/IP je vystavěn na vrstvách, z nichž každá vrstva spoléhá na služby, které poskytuje vrstva pod ní, a zároveň poskytuje vyspělejší služby vrstvě umístěné nad ní. Na obrázku (Obrázek 2) je grafické znázornění vrstev v sadě protokolů TCP/IP. Obsahuje fyzickou, linkovou, síťovou a aplikační vrstvu.



Obrázek 2 - Síťový model OSI, TCP/IP; zdroj [3]

Jednotlivé vrstvy plní konkrétní funkce, které si dále rozepíšeme. OSI (Open system Interconnect) je referenční model pro srovnávání síťových protokolů, který vyvinula mezinárodní normalizační organizace (ISO – International Standards Organization).

2.2.1 Vrstva síťového rozhraní

Tato vrstva obsahuje fyzické zařízení (ethernetová karta, modem) zajišťující propojování počítačů do sítí. Protokol TCP/IP se nezajímá, o jaké konkrétní zařízení se jedná, záleží mu pouze na tom, jestli takové zařízení existuje, a zda lze po něm vyměňovat data. Tato vrstva tedy zodpovídá za předávání TCP/IP paketů síťovému médiu a přijímání TCP/IP paketů

z tohoto média. Vrstva síťového rozhraní zahrnuje linkovou a fyzickou vrstvu referenčního modelu OSI.

2.2.2 Síťová vrstva

Tato vrstva se stará o doručování dat od jejich zdroje až k jejich koncovým adresátům. Za tímto účelem vyhledává optimální cesty k cílovému uzlu (směrování), zajišťuje přenesení přes mezilehlé uzly (forwarding) a předchází zahlcení. V síťové vrstvě jsou zabudovány síťové 32-bitové abstraktní adresy, převodní mechanismy (ARP, RARP) a protokoly na podporu fungování síťové vrstvy (ICMP, IGMP):

- Protokol IP (Internet Protocol) je směrovatelný protokol odpovědný za adresaci, směrování, rozdělování a opětovné skládání paketů.
- Protokol ARP (Address Resolution Protocol) je odpovědný za překlad adres internetové vrstvy (IP adres) na adresy pro vrstvu síťového rozhraní, jako jsou hardwarové adresy MAC.
- Protokol RARP (Reverse ARP) plní opačnou funkci protokolu ARP.
- Protokol ICMP (Internet Control Message Protocol) je odpovědný za poskytování diagnostických funkcí a hlášení o problémech s doručením IP paketů.
- Protokol IGMP (Internet Group Management Protocol) je odpovědný za správu skupin pro vícesměrové vysílání.

2.2.3 Transportní vrstva

Hlavním úkolem této vrstvy je zajišťovat end-to-end komunikaci, rozlišovat mezi více odesilateli a příjemci v rámci daného uzlu, měnit spojový/nespojový charakter, zajišťovat spolehlivost, kvalitu služeb, přecházet zahlcení a řídit tok. Tato vrstva obsahuje dva alternativní transportní protokoly:

- Protokol TCP (Transmission Control Protocol) poskytuje spolehlivé komunikační služby pro dvoubodové spojení. TCP odpovídá za ustavení TCP spojení, seřazení a potvrzení posílaných paketů a obnovení paketů ztracených během přenosu.
- Protokol UDP (User Datagram Protocol) poskytuje nespolehlivé komunikační služby pro dvou či vícebodové spojení. Rychlost přenosu paketu je vyšší, spolehlivost doručování není ovšem zaručena.

Vyšší vrstvy si mohou samy vybrat, který transportní protokol využijí.

2.2.4 Aplikační vrstva

Tato vrstva zahrnuje relační, prezentační a aplikační vrstvu referenčního modelu OSI. TCP/IP vychází z toho, že relační a prezentační vrstvy potřebují jen některé aplikace. Tak pokud nějaká aplikace tuto službu potřebuje, musí si ji realizovat sama. Nejznámější protokoly této vrstvy jsou:

- Protokol SNMP (Simple Network Management Protocol) umožňuje získávat, sbírat a vyhodnocovat informace o stavu sítě pro potřeby její správy.
- Protokol DNS (Domain Name System) se používá k překladu doménových názvů na konkrétní IP adresy, které se používají k adresaci v Internetu.
- Protokol HTTP (Hyper Text Transfer Protocol) se používá k přenosu souborů tvořících webové stránky na Internetu.
- Protokol SMTP (Simple Mail Transfer Protocol) se používá k přenosu poštovních zpráv.
- Protokol FTP (File Transfer Protocol) se používá k interaktivnímu přenosu souborů.
- Protokol Telnet (Telnet Protocol) emuluje terminál a používá se ke vzdálenému přístupu k hostitelům v sítích.

Obvykle všechny aplikace v rámci TCP/IP jsou založeny na architektuře klient/server.

3 Síťová bezpečnost

Bezpečnost počítačových sítí a aplikací je v současnosti jedním z nejdiskutovanějších problémů. Bezpečnost označuje ochranu počítačových prostředků proti náhodnému nebo úmyslnému prozrazení důvěrných dat, neoprávněné modifikaci dat nebo programů, zničení dat, softwaru nebo hardwaru a neoprávněnému zabránění v použití počítačových prostředků.

V dnešní době, kdy je internet využíván jako hlavní komunikační prostředek pro přenosy dat i k obchodním transakcím, je stále důležitější data a jejich přenosy maximálně zabezpečit. Nejdříve si vysvětlíme, jakým hrozbám můžeme čelit.

Informace pro tuto kapitolu jsem čerpal ze zdroje [2], [11].

3.1 Hacker - průběh útoku

Abychom mohli důkladně zabezpečit náš systém, měli bychom si také vysvětlit a pochopit, jak takový hacker (útočník) postupuje. Hacker může získat přístup do systému několika způsoby. Objektem jeho zájmu může být přitom jen jeden domácí počítač anebo celá podniková síť. Bez ohledu na velikost cíle hacker provádí základní kroky:

- obhlídka a průzkum terénu
- sledování
- soupis prostředí
- získání přístupu
- rozšíření oprávnění
- vytvoření zadních vrátek a zahlazování stop

3.1.1 Obhlídka a průzkum terénu

Hackeři provádějí nejdříve obhlídku vyhlídnutého cíle. Aby hacker zůstal neodhalen, používá během této fáze obhlídky neinvazivní a opatrné metody. Jen díky jednoduchým dotazům (třeba nslookup, ping) či jednoduchým nástrojům (whois, WhatRoute) se dá zjistit plno základních informací. Pokud je vyhlídnutá firma připojená k internetu, útočník může zjistit:

- doménový název a servery DNS
- IP adresy dostupné z internetu

- hardware a operační systém, na kterém běží síťové služby
- přítomnost firewallu či detekčního systému IDS
- fyzické umístění zařízení
- používané síťové protokoly
- používaný typ vzdáleného přístupu a cíl připojovaných uživatelů
- způsob kontroly přístupu k síti

3.1.2 Sledování

V této fázi má hacker dokončenou obhlídku a na základě získaných informací si může vytvořit jednoduchou mapu sítě. Od této doby ovšem jeho útoky jsou zpravidla invazivní a mohou se objevit zaznamenané v systémových protokolech. V této fázi provádí aktivní sledování či prohledávání sítě, třeba pomocí nástroje nmap (www.insecure.org) lze aktivně sledovat porty, pomocí nástroje TigerSuite (www.tigertools.net) dostupné služby na daném serveru.

3.1.3 Soupis prostředí

Aby útočník mohl definovat síťové prostředí, musí provést obhlídku a průzkum, sledování a také soupis prostředí. Útočník volí nejsnadnější cestu k prolomení zranitelných míst, proto sleduje, jaké porty jsou v systému otevřené a jaké služby na něm běží. Pomocí soupisu prostředí útočník zjišťuje různé informace o platných účtech, ovšem musí již vytvářet aktivní spojení. V tomto kroku útočník zjišťuje:

- síťové prostředky a sdílené složky
- uživatelé a skupiny
- aplikace
- úvodní zprávy zařízení

3.1.4 Získání přístupu

V této fázi útočník uplatňuje invazivnější metody zkoumání, kde vyhledává platné uživatelské účty a nedostatečně chráněné sdílené prostředky. Útočník zde může provádět tyto typy útoků:

Útoky na operační systém – díky nabízeným síťovým službám musí mít systém otevřené porty a aktivní služby, které jsou zvenčí pro útočníky viditelné.

Útoky na aplikace – útočníci využívají nezabezpečené funkce těchto aplikací.
Útoky na nesprávnou konfiguraci – útočníci zde třeba hledají spuštěné služby, u nichž není pozměněno výchozí uživatelské jméno a heslo administrátora.
Skriptové útoky – útočníci v systémech Unix a Linux mohou najít již od výrobce množství ukázkových skriptů a programů, které se dají přímo spustit. Proto je potřeba tyto přednastavené skripty a programy deaktivovat nebo sledovat. Útočníci během této fáze útoku zkoušejí následující typy zásahů:

- přetečení paměťového bufferu
- uhodnutí hesla metodou hrubé síly
- odposlech hesla
- zachycení souboru hesel

3.1.5 Rozšíření oprávnění

V této fázi již útočník získal přístup do cílového systému prolomením hesla některého uživatele, které ovšem nemusí mít požadované oprávnění pro jeho další kroky, a proto se snaží tyto oprávnění rozšířit. K tomu využívají možnosti chyb či zranitelných míst v operačních systémech.

3.1.6 Zahlazení stop a zadní vrátka

Zkušený útočník po úspěšném proniknutí do systému za sebou zahlazuje stopy, což je jeden z nejobtížnějších úkolů. Hacker musí vyčistit protokol událostí a položky systémového registru, aby nebyl administrátorem odhalen. Pokud se později útočník hodlá vrátit, tak si v systému vytváří zadní vrátka buď vytvářením zvláštního účtu, nebo zapíná různé služby, nebo instaluje aplikace pro vzdálené řízení.

3.2 Přehled nejčastějších útoků

Zde uvádím nejčastěji používané typy útoků, jejich výčet není úplný, protože jich každým dnem mnoho přibývá.

- *Odepření služeb (Denial of Service, DoS)* – při tomto útoku se hacker snaží dostat systém do poruchového stavu, v němž odepírá běžné služby ostatním i právoplatným uživatelům.

- *Distribuované odepření služeb (Distributed Denial of Service, DDoS)* – tento typ operace útočí na vyhlédnutou oběť z většího množství různých napadených nic netušících systémů.
- *Útok se záplavou paketů SYN* – pomocí tohoto útoku se síť zahltí pakety SYN, které normálně znamenají zahájení požadavku o spojení. Výsledkem je pak takové obsazení procesoru, paměti a síťového rozhraní, že systém již nemůže obsluhovat právoplatné požadavky spojení a vzniká odepření služeb (Dos).
- *Útok se záplavou paketů UDP* – při tomto útoku dochází k záplavě paketů v takovém množství, že se cílový systém výrazně zpomalí a nedokáže zpracovávat platná spojení.
- *Prohledávání portů* – znamená vysílání paketů s různými čísly portů a jeho cílem je nalezení dostupných služeb k možnému zneužití.
- *Falšování IP adres* – pomocí tohoto útoku se hacker snaží obejít bezpečnostní kontroly firewallu tím, že napodobuje IP adresu, e-mailovou adresu nebo uživatelský ID platného klienta.
- *Prohledávání s dotazy ping* – hacker při této operaci zasílá požadavky opakování echo ICMP (ping) na různé cílové adresy a přitom sleduje, jestli mu některý z cílů odpoví, a on se tak dozví IP adresu potenciální oběti.
- *Hrubá síla* – hacker se pokouší uhodnout hesla do systému pomocí primitivních technik, jako je opakované přihlašování pod určitý účet s výrazy převzatými ze slovníku možných hesel.
- *Záplava paketů ICMP* – hacker pomocí dotazů ICMP (ping) přetíží cílový systém takovým množstvím požadavků na opakování (echo), že systém zcela vyčerpá své prostředky na odpovědi a nemůže zpracovávat normální provoz.
- *Odposlech paketů* – je pasivní metodou útoku. Hacker pomocí dokonalejších odposlechových nástrojů umí dekódovat data z paketů všech sedmi vrstev referenčního modelu OSI. Díky tomu se mohou útočníci snadno zmocnit uživatelských jmen a hesel, pomocí kterých pak vedou další útoky.

3.3 Sociální inženýrství

Sociální inženýrství je moderní metoda počítačového útoku na nejslabší článek těchto systémů, a tím je člověk. Psychologie a umění ovládat lidi, neboli využívání lidských

slabin v jednání, jsou nejmocnější zbraní sociotechnika. Sociotechnika v pojetí informační bezpečnosti znamená přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili, že útočník je někdo jiný, a zmanipulovat je k vyzrazení informací nebo provedení určitých úkonů.

Lidé jsou v principu důvěřiví a věří jeden druhému, a proto jsou vůči sociálnímu inženýrství hodně zranitelní. I zdánlivě nevinné informace je třeba chránit, proto by zaměstnanci v organizacích měli dodržovat jednoduché pravidlo: veškeré firemní údaje musí považovat za citlivé a nikomu je nesmí prozrazovat. Mezi nejpoužívanější metody útoku patří Trashing, Phishing, Pharming a Vishing.

3.3.1 Trashing

Trashing je nejstarší technikou a znamená prosévání firemního či bytového odpadu za účelem získání cenných informací. Útočník hledá jakékoli dokumenty spojené s výpisy z účtu, telefonních karet a jiné cennosti. Řada společností i domácností má kontejnery umístěny v nestřeženém okolí svých budov, a tím se stávají snadno dostupné pro útočníka. Tato metoda je velmi účinná, ale u sociotechnika méně oblíbená, protože ne každý má žaludek na prohrabávání popelnic. V poslední době ale útočníkům napomáhá třídění odpadu, prohledávají pouze kontejnery na papír a nemusí se prohrabávat veškerým hnijícím odpadem.

Obranou proti této technice je přejít na elektronickou formu citlivých dokumentů nebo zbavovat se důležitých dokumentů fyzickým zničením, nejlépe zpopelněním. Ani skartace papírových dokumentů není bezpečná, protože pokud si dá někdo tu práci, dokáže rozřezané papíry složit zpět jako puzzle.

3.3.2 Phishing

Phishing nebo-li „rybaření“ je podvodná technika používaná na Internetu k získávání citlivých a užitečných údajů od obětí, jako jsou hesla, čísla kreditních karet, PIN a podobně. Využívá se k tomu rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce s odkazem na podvodné stránky, kde vyzývají adresáta k zadání jeho přihlašovacích údajů. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni s jeho účtem libovolně manipulovat. Phishing především čerpá z:

- nepozornosti samotných obětí

- důvěřivosti a sociálního inženýrství - autoři phishingových zpráv velmi výrazně využívají právě důvěřivosti uživatelů
- neznalosti problematiky

Obranou před touto technikou je nepovažovat Internet za zdroj pouze důvěryhodných informací, nepoužívat hypertextové odkazy zahrnuté přímo v e-mailu, nikomu nesvěřovat důvěrné informace. Je vhodné používat aktualizovaný antivirový software a prohlížeče či doplňky, které umějí phishing rozpoznat (z prohlížečů např. IE7, My Internet Browser, Firefox, Opera, z doplňků třeba Netcraft Toolbar).

3.3.3 Pharming

Pharming označuje činnost, při které útočníci přesměrují internetovou komunikaci z jednoho webu na jiný. Pharming spočívá v modifikaci DNS záznamů. To lze docílit dvěma způsoby, buď metodou napadnutím vybraného DNS serveru, a nebo druhou metodou, a to změnou záznamů v souboru hosts u jednotlivých počítačů s operačními systémy Windows. Nic netušící uživatel je pak i při zadání správné adresy internetového bankovnictví přesměrován díky změněným DNS záznamům na podvodnou stránku. Jestliže je tato falešná stránka dobře vypracovaná, pak je nízká šance, že by uživatel na podvod přišel. Jediná možnost ověření správné adresy je podrobná kontrola certifikátu, kterým je tato stránka podepsána. První metoda je sice nezávislá na klientských počítačích, ale je mnohem složitější zdolat ochranu DNS serveru, proto se útočníci více zaměřují na metodu druhou. Pharming je už mnohem nebezpečnější než phishing.

Obranou proti tomuto útoku je zajistit ochranu samotného souboru s názvy hostitelů a mít správně nastavený a aktuální antivirový program kontrolující nejen všechny soubory posílané elektronickou poštou, ale také vše, co je spouštěno a stahováno z webu. Další možností je používání nástrojů, které zobrazují doplňující informace o právě zobrazovaných webových stránkách. Jedním z těchto nástrojů je například produkt Netcraft Toolbar .

3.3.4 Vishing

Vishing těží z důvěry v telefonní služby, je to zneužívání VoIP technologie (Voice over Internet Protocol) pro vylákání osobních a finančních informací za účelem osobního obohacení. Vishing napodobuje obvyklý způsob komunikace lidí s jejich finančními

institucemi. Oběti jsou dotazovány na čísla účtů, hesla nebo čísla sociálního zabezpečení. Tyto údaje jsou poté prodávány v Internetu a používány k podvodům se získanou identitou. S příchodem VoIP již nemusí být na konci telefonního spojení pevná linka, ale třeba i počítač, který lze snadno pro tyto účely zneužít. Technologie VoIP je relativně nová, a tak vývoj bezpečnostních řešení má za jejím nástupem zpoždění. Bezpečnostní experti varují, že vishing může být daleko efektivnější a nebezpečnější než phishing technologie.
Obrana proti vishingu zůstává pouze na uživateli a vždy, když přijde na identifikační údaje, je vhodné používat zdravý rozum. V případě finančních institucí je vhodné žádat o ověření totožnosti například požádáním, jakou transakci jsme naposledy provedli. Zloděj k takovým informacím nebude mít pravděpodobně přístup.

3.4 Obrana

V současné době musí každý uživatel, připojený do jakýkoli sítě, klást vysoký důraz na bezpečnost. Nejlepší obranou je prevence, a proto si v dalších podkapitolách popíšeme základní principy návrhu zabezpečení, bezpečnostní protokoly a systémy na detekci vniknutí.

3.4.1 Základní principy návrhu zabezpečení

Vrstvená bezpečnost - bezpečnost musí být vrstvená. Potřebujeme firewall jako základní bránu pro filtrování mezi bezpečnostními zónami, potřebujeme antivirus a antispam, potřebujeme VPN pro bezpečný přístup zaměstnanců, popř. pro propojení korporace s jejími partnery, a potřebujeme další ochrany v závislosti na službách a jejich důležitosti.
Řízení přístupu – musíme určit a nastavit, kdo bude mít povolen přístup do sítě. Jedním z doporučovaných postupů je všechno zablokovat a potom výslovně povolit jen to, co daný uživatel potřebuje ke své práci.
Uvědomění uživatelů – školení uživatelů a posílení jejich uvědomělosti v otázkách bezpečnosti je velmi důležité, jen tak pochopí její význam a budou spolupracovat a podporovat zásady zabezpečení.
Monitorování – je zapotřebí systémy průběžně monitorovat a ověřovat, jestli jsou stále bezpečné a odolné vůči útokům. Sledování provádíme pomocí detekčních systémů IDS (Intrusion Detection System).

Aktualizace systémů – je potřeba sledovat, jestli pro daný systém nejsou k dispozici nějaké aktualizace či záplaty. Mnohé novější operační systémy dokáží automaticky připomínat stahování aktualizací.
Obranný tým – s bezpečnostními problémy se dříve nebo později setká každý, a proto je potřeba stanovit způsob reakce na útoky a přijmout příslušná opatření v jakékoli situaci.

3.4.2 Bezpečnostní protokoly

V oblasti informačních technologií, zejména v oblasti zabezpečení počítačů, bezpečnostní protokol definujeme jako bezpečný postup regulace datového přenosu mezi počítači. V této podkapitole si vysvětlíme některé metody šifrování dat pro bezpečný přenos po síti. Ochrana dat pomocí šifrování se dá považovat za jednu z vrstev síťové bezpečnosti. Pro ochranu dat se běžně používají různé šifrovací algoritmy se symetrickým nebo asymetrickým klíčem.
V případě, že se k zašifrování a dešifrování používá stejný klíč, říká se, že šifra používá symetrickou funkci. Odesílatel i příjemce musí vlastnit stejný klíč. Symetrické šifry jsou rychlé a bezpečné.
V případě asymetrického šifrování se používají dva klíče, veřejný a privátní klíč. Veřejný klíč slouží k šifrování prostého textu a privátní klíč k jeho dešifrování. Problémem u šifer s veřejnými klíči je jejich pomalost, jsou mnohem pomalejší než symetrické šifrování, někdy až tisíckrát.

- *Šifrování DES* - tuto šifru vyvinulo IBM ve spolupráci s Národní agenturou pro bezpečnost (NSA). V roce 1974 předložila firma IBM svůj algoritmus *Lucifer*, který pracoval s klíči o délce 128 bitů. Dne 23. listopadu 1976 přijal americký národní úřad NIST upravený algoritmus *Lucifer* za americký federální standard a změnil jeho název na Data Encryption Standard (DES). NIST na příkaz Národního bezpečnostního úřadu NSA z bezpečnostních důvodů zkrátil 128 bitový klíč na pouhých 56 bitů, čímž se bohužel ochranná síla šifrování výrazně oslabila. Dnes dokáže algoritmus DES prolomit libovolná organizace i s průměrným vybavením.
- *Šifrování Triple DES* - algoritmus DES byl překonaný, a proto se z něj vyvinul algoritmus Triple DES (3DES). Algoritmus 3DES používá při šifrování tři samostatné klíče, a tím prodlužuje efektivní délku klíče z 8 na 24 znaků,

tedy na 168 bitů. Vlastní postup šifrování v algoritmu 3DES je stejný jako v DES, jen se 3x opakuje. Původní data se zašifrují pomocí prvního klíče, výsledek pomocí druhého klíče a tento výsledek pak pomocí třetího klíče. Nevýhodou pak tohoto algoritmu je, že je pomalejší díky trojitému šifrování než algoritmus DES.

- *Algoritmus MD5* - s vývojem Internetu, potřebou práce s daty a s počítačovými sítěmi je nutné se zabývat bezpečností, autenticitou (pravost) a integritou dat (celistvost) Algoritmus otisku zprávy MD5 (Message Digest 5) je jednou z nejlepších metod zajištění zabezpečení datové komunikace. Algoritmus MD5 žádná data nijak nešifruje ani je nepozměňuje, místo toho vytváří jen otisk, pomocí kterého lze poznat autenticitu a integritu přijatých dat. Za zdrojem algoritmu stojí Ron Rivest, který jej vytvořil v roce 1994. Algoritmus generuje ze vstupních dat libovolné délky jistý výstup o pevné délce, který se nazývá *haš* (hash) neboli otisk. Tento otisk je nevratný a žádnou jeho zpětnou analýzou nelze odvodit původní obsah dat. Hash ověřuje, že se soubor během přenosu nezměnil, a je třeba vhodný pro distribuci softwaru nebo k zajištění integrity systémových souborů.

Dále si také vysvětlíme něco o běžných implementací VPN, tunelování provozu v síti a jeho ochranu zabezpečením pomocí dvou protokolů PPTP a L2TP.

- *Protokol PPTP* - tento protokol společně vyvinuly firmy Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics a U.S. Robotics. Protokol PPTP (Point-to-Point Tuneling Protocol) vychází z protokolu PPP (Point-to-Point Protocol), který je standardem pro dvoubodové vytáčené připojení k síti. PPTP je množina komunikačních pravidel, pomocí nichž může firma rozšířit svoji podnikovou síť o privátní tunely vedené po veřejném Internetu. Protokol PPTP přebírá data paketů PPP a dále je zapouzdří do paketů IP, které nakonec přenese přes tunel sítě VPN v běžném Internetu. V tomto protokolu se tedy šifrování zahajuje až po dokončení procesu spojení PPP a tedy až po její autentizaci. Bohužel PPTP funguje jen přes TCP/IP a další nevýhodou je, že nedefinuje způsob autentizace a šifrování dat. Proto se klidně může stát, že dva různí výrobci, kteří vyrábějí zařízení či klienty podporující stejný protokol PPTP, se nakonec stejně „nedomluví“.
- *Protokol L2TP* – L2TP (Layer 2 Tuneling Protocol) je také rozšířením protokolu pro propojení typu PPP (Point-to-Point Protocol) a slouží k zajištění činnosti

virtuální privátní sítě VPN nad veřejným Internetem. Je postaven na standardech, což znamená podstatně lepší spolupráci různých zařízení od různých výrobců. U tohoto protokolu nastupuje šifrování dat již před procesem spojení PPP. Toto spojení využívá šifrovací algoritmus DES nebo 3DES. L2TP vyžaduje jak autentizaci na úrovni uživatele, tak autentizaci počítače definovanou jeho certifikátem. Navíc tento protokol je konstruován tak, aby fungoval na libovolném protokolu, jako je IP, IPX a AppleTalk.

Dalšími dvěma běžnými metodami, kterými administrátoři unixových a open-source operačních systémů vytvářejí VPN, jsou PPP přes SSL nebo SSH.

- *SSL (Secure Socket Layer)* – je protokol založený na asymetrickém šifrování. Vytvořila ho společnost Netscape na podporu bezpečného surfování na Internetu. SSL neprovádí autentizaci, jen šifruje obsah mezi klientem a veřejným serverem, takže SSL provádí jen výměnu veřejných klíčů.
- SSH (Secure Shell) – provádí bezpečné autentizované přihlašování pomocí PFS (Perfect Forward Secrecy) a pak šifruje komunikační relaci mezi klientem a hostitelským počítačem Na rozdíl od SSL používá SSH šifrování pomocí tajného klíče, takže obě strany ho musí znát před ustanovením spojení.

3.4.3 Detekce vniknutí

V této podkapitole si vysvětlíme, jak zabránit útokům, kterým nedokáže zabránit firewall, anebo jak vůbec zjistit, že se někomu podařil průnik do naší sítě.

Zatímco firewall zamezuje útokům tím, že blokuje připojení na nepoužívané porty, systémy IDS (Intrusion Detection System) a IPS (Intrusion Prevention System) zajišťují bezpečnost portů, na kterých jsou provozovány aktivní služby – tedy portů otevřených. Systémy IDS/IPS se nejčastěji vyskytují v podobě hardwarového zařízení, ale existují i varianty softwarové určené k instalaci na koncové klientské stanice. Zařízení IDS (systém detekce útoku) sleduje toky dat a snaží se v nich nalézt jakýkoli pokus o útok na službu. Toto zařízení nijak nezasahuje do chodu monitorované sítě a lze ho zapojit přímo na síťový rozbočovač. Oproti tomu IPS (systém zamezení útoku) tyto útoky nejen dokáže identifikovat, ale umí na ně i patřičně zareagovat – tzn. buď útok zastavit, nebo automaticky změnit konfiguraci směrovače či firewallu a v něm vytvořit přístupový seznam pro blokování IP adresa útočníka..

Detekční systém IDS je možné provozovat v různých místech sítě. Rozlišujeme dva základní typy systémů: NIDS (síťové) a HIDS (hostitelské).

- *Síťový detekční systém NIDS* je umístěn přímo v chráněné síti a sleduje v ní veškerý provoz. Tyto systémy bývají většinou provozovány před a za firewallem či bránou sítě VPN. Zde pak účinně sledují příchozí, odchozí provoz a vnitřní provoz mezi jednotlivými hostitelskými systémy i lokálními segmenty sítě.
- *Hostitelský detekční systém HIDS* je speciální softwarová aplikace nainstalovaná na serveru. Systém zde pak sleduje příchozí, odchozí provoz a změny souborového systému. Systémy HIDS jsou účinné zejména u aplikačních serverů, jako jsou webové a poštovní servery.

Ideální je provozovat systémy NIDS a HIDS současně, jen tak získáme důkladný přehled o komunikaci uvnitř sítě.

Systémy detekce vniknutí nabízejí obrovskou množinu funkcí a možností:

- Závislost mezi událostmi – při provozování několika IDS v hodně zatížené síti lze díky vymezení závislosti přesně stanovit, které události spolu souvisí, i když jsou hlášeny z různých senzorů z různých podsítí.
- Centralizovaná správa senzorů – umožňuje zjištění závislosti mezi událostmi, kontrolu reakcí senzorů a vytváření podrobných zpráv o bezpečnosti sítě.
- Možnost přizpůsobení projevů útoků a prahových hodnot – díky veškerým aktualizacím aplikací a systémů dochází mezi objevením zranitelného místa a vytvořením nového projevu příslušného časového útoku systému IDS k určité časové prodlevě. Proto je vhodné nabídnout administrátorům možnost libovolného projevu útoku, v němž může ošetřit jakýkoli možný případ.
- Vyloučení falešných poplachů – v továrním nastavení má zařízení IDS všechny funkce standardně zapnuté. Tím jsou zbytečně citlivé a dávají velké množství falešných poplachů. Proto je žádoucí mít možnost jednotlivé falešné poplachy vypnout.
- Implementace postavená na standardech – pro správu systému IDS je nejdůležitější funkce zasílání zpráv. Proto vznikl jistý standard z databáze CVE (Common Vulnerabilities and Exposures), která klasifikuje jednotlivá zranitelná místa do přehledného systému, a tím jsou oznamovací události podstatně lépe čitelné.

- Funkce pro prevenci vniknutí – znamená schopnost aktivní reakce na vniknutí a nežádoucí provoz.
- Kontrola projevů – systém IDS porovnává každý paket či posloupnost paketů procházející sítí se známými vzory útoků. Na základě pozitivní shody pak systém může vyvolat výstrahu SNMP, odeslat varovnou e-mailovou zprávu nebo v případě IPS aktivně zabránit v dokončení útoků.
- Detekce anomálií – v systému se vytvoří srovnávací databáze se vzorkem normálního provozu. Při překročení normálních hodnot, třeba při detekci nového protokolu v síti, detekční systém zareaguje. Tento mechanismus tak reaguje na veškeré abnormální příkazy a požadavky.

Detekční systém ovšem neumí detekovat úplně vše, a proto je jen jednou vrstvou v celkovém plánu vrstveného zabezpečení sítě.

4 Firewally

Internet nabízí výkonný způsob komunikace, proto se do ní privátní sítě připojují. Když se privátní síť připojí k internetu, propojí se tím s dalšími privátními sítěmi, které jsou na internet napojené. Tím se privátní síť stává zranitelnou vůči útokům z internetu. Obecně neexistuje centrální bod zabezpečení, a proto by měl každý na hranici své privátní sítě instalovat firewall, který vytváří kontrolní bod zabezpečení. Firewall pak kontroluje všechny pakety, které mezi privátní sítí a internetem probíhají a podle nastavených pravidel buď pakety propouští, a nebo blokuje. Na trhu existuje několik typů firewallů, se kterými se postupně seznámíme. Dále v následujících kapitolách si také vysvětlíme, jak obecně firewally fungují.

Informace pro tuto kapitolu jsem čerpal ze zdroje [3], [12], [13].

4.1 Funkce firewallu

Díky firewallům můžeme bezpečně připojit privátní síť k internetu. Dokonalejší firewally chrání síť na všech vrstvách: linkové, síťové, aplikační.

Firewally fungují primárně na základě tří metod:[3]

Filtrování paketů – Odmítá pakety TCP/IP od neautorizovaných uživatelů a odmítá pokusy o připojení k neautorizovaným službám.

Překládání síťových adres (NAT) – Překládá IP adresy interních hostitelských počítačů a skrývá je před monitorováním zvenčí. Funkcí NAT se někdy také říká maskování adres IP.

Služby proxy – Vytváří na základě požadavků interních hostitelských počítačů připojení na aplikační vrstvě. Tím úplně ruší propojení mezi interními a externími hostiteli na síťové vrstvě.

A dále provádí další 2 služby zabezpečení:

Šifrovaná autentizace – Umožňuje uživatelům veřejných sítí prokazovat firewallu svou totožnost, a získávat tak přístup k privátní síti z externích lokalit.

Propojování virtuálních privátních sítí – Ustavuje bezpečné propojení mezi dvěma privátními sítěmi přes veřejné prostředí, např. internet. Fyzicky oddělené sítě tak

[3] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce*, s. 4

mohou ke komunikaci místo pronajatých linek používat internet. VPN se také říká zašifrované tunely.

Některé firewally také nabízejí dodatečné služby, které se přímo nevztahují přímo k zabezpečení, ale jež mnoho uživatelů ocení:[4]

Skenování virů – Prohledává příchozí datové toky a zjišťuje, zda neobsahuje signatury virů. Chcete-li mít k dispozici nejaktuálnější signatury, musíte si objednat službu aktualizace virů, kterou poskytuje dodavatel firewallu.

Filtrování obsahu – Umožňuje blokovat interním uživatelům přístup k určitým typům obsahu podle kategorií, např. pornografie, propaganda rasistických organizací, a informace o hackerství. Aktualizace seznamů blokovaných webových stránek pro určitou kategorii je k dispozici také pouze po registraci služby.

4.1.1 Paketové filtry

První internetové firewally byly založeny na filtrování paketů a toto zůstává i nadále jako jedna z klíčových funkcí dnešních firewallů. Podle určitých identifikačních údajů v hlavičce paketu stanovíme, zda paket může vstoupit či vystoupit ze sítě. Filtry mohou být implementovány v operačních systémech, softwarových i hardwarových firewallech a jsou také součástí směrovačů. Filtry instalované ve směrovačích nepropouštějí žádný podezřelý provoz do cílové sítě. Kdežto filtrovací moduly na serverech pouze brání tomu, aby konkrétní zařízení na podezřelý provoz reagovalo. Proto by se mělo filtrování v implemetaci TCP/IP protokolů na serverech používat jen jako doplnění filtrování pomocí směrovače. Pomocí operačního systému by se měly nastavit filtry pouze pro protokoly, které jsou potřeba obsluhovat. U standardních serverů jsou služby nastavené tak, aby poslouchaly jen na některých portech. Seznamy nejčastěji používaných portů a služeb jsou uvedeny v příloze (Příloha P1).

Pravidla zabezpečení pro filtrování paketů lze nastavit dvěma základními způsoby:

Optimistický – povolí se veškerý provoz a blokuje se jen zaručeně škodlivý.

Pesimistický – zakáže se veškerý provoz a povoluje se jen ten, který je nezbytný.

Při filtrování paketů je třeba vzít v úvahu tato všeobecná pravidla:[5]

- V původním nastavení deaktivujte všechny protokoly a adresy a pak výslovně povolte služby a hostitele, které si přejete podporovat.

[4] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce,* s. 4
[5] Tamtéž, s. 9

- Deaktivujte všechny pokusy o připojení k hostitelům v síti. Kdybyste povolili příchozí připojení, umožníte hackerům, aby se připojovali k k trojským koním nebo zneužívali chyby v softwaru pro služby.
- Odfiltrujte zprávy s přesměrováním ICMP a zprávy typu „ozvěna“ (ping) a „neodpovídejte na ně“. Blokujte všechny pakety, které používají přímé směrování TCP. Přímé směrování se používá pro legitimní účely jen málokdy.
- Blokujte všechny aktualizace externích směrovacích protokolů (RIP, OSPF), které jsou určeny interním směrovačům. Vně interní sítě by nikdo neměl přenášet aktualizace protokolů RIP.
- Zvažte deaktivaci fragmentů po nultém fragmentu. Tato funkce je většinou už zastaralá a často přes ni dochází k napadení.
- Pro hostitelské počítače, které obsahují veřejné služby, jako jsou webové servery a servery SMTP, neotevírejte průchody paketovými filtry. Umístěte je raději před paketové filtry.
- Nespoléhejte se při obraně sítě pouze na filtrování paketů.

4.1.2 NAT - Překládání síťových adres

Pomocí překladu síťových adres NAT organizace především řeší nedostatek veřejných IP adres ve své síti, připojené do internetu. Překlady síťových adres NAT provozujeme na vhodném zařízení (firewallu, směrovači nebo počítači) umístěném mezi vnitřní síti s privátními IP adresami a vnějším internetem s veřejnými IP adresami. Zařízení pak provádí překlady adres z privátních na veřejné, a tím řeší problém skrývání interních hostitelů.

Funkce NAT je v podstatě proxy na síťové vrstvě. Funkce NAT skrývá interní IP adresy tak, že všechny adresy interních hostitelů zkonvertuje na adresu zařízení poskytující funkci NAT. Toto zařízení potom pomocí čísla portu TCP odešle datovou část z interního hostitelského počítače z jeho vlastní adresy. Tím monitoruje, jaká připojení z veřejné sítě se přiřazují ke kterým hostitelům v privátní síti. Pro Internet se pak jeví, že veškerý provoz v interní síti pochází od jednoho velmi zaneprázdněného počítače.

NAT působí problémy administrátorům chtějícím se připojit ke klientům za NAT za účelem správy. Je to způsobeno tím, že NAT má pouze jednu IP adresu, a proto nelze upřesnit interního klienta, ke kterému se chce administrátor připojit. Proto většina

novějších zařízení umožňuje vytvářet pravidla pro přenášení (forwardování) portů, pomocí nichž se lze k interním hostitelským počítačům dostat.

Další omezení mechanismu NAT jsou:

- Problémy s protokolem UDP, protože mechanismus NAT sleduje a kontroluje stav spojení a protokol UDP je nespojovaný, proto nelze stav spojení nějak určit.
- Některé protokoly skrývají nebo pozměňují pakety, které NAT potřebuje ke správnému překladu adres. Jedná se o protokoly Kerberos, X Windows a vzdálený shell.
- Vzájemné vlivy systémů šifrování a autentizace díky principu mechanismu NAT, který pakety pozměňuje. Systémy šifrování dat ovšem vyžadují integritu dat, a kontrolují tak jejich neporušenost při přenosu. Proto šifrovací a autentizační technologie s funkcí NAT nedokážou pracovat.
- Komplikovaný záznam do systémových protokolů právě kvůli překladům adres. Složitě a těžce se zjišťuje, který z interních systémů vlastně dané události zaznamenal.

4.1.3 Proxy

Firewally na aplikační úrovni zajišťují nejbezpečnější typ datových spojení díky zkoumání všech vrstev modelu TCP/IP v komunikačním procesu. Proxy firewally umožňují úplné přerušení toku protokolů na síťové úrovni a omezení protokolů vyšší úrovně – HTTP, FTP a SMTP. Proxy kontrolují každé spojení a fungují na hranicích mezi dvěma sítěmi, které jsou propojeny pomocí směrovačů. Jakmile provede klient v chráněné síti připojení na server ve veřejné síti, obdrží proxy žádost o připojení a připojí se jménem původního klienta. Pak proxy postoupí požadavek z veřejného serveru do interní sítě.

Aplikační proxy nemusí být nainstalovaný nutně jen na firewallech, tuto roli může vykonávat jakýkoli server. Bez firewallu ale není žádné skutečné zabezpečení, a tak jsou zapotřebí oba komponenty. Ideálním způsobem pak je, aby firewall prováděl funkce proxy. Některé firewallové proxy jsou sofistikovanější a umožňují funkci filtrování a maskování IP adres.

Omezení možnosti proxy jsou:

- Pomalejší činnost způsobená důkladným zkoumáním a pečlivým zpracováním paketů. Protože se na této úrovni zabezpečení kontrolují v podstatě všechny části všech paketů, bývá činnost proxy firewallů opravdu pomalá.
- Nejsou vždy aktuální, protože vyvinout a otestovat nové proxy servery na nové protokoly a aplikace nějakou dobu trvá. Po tuto dobu je příslušné bezpečnostní zařízení neaktuální.

Z bezpečnostního pohledu se za nejbezpečnější firewall dá považovat standardní proxy firewall, který provádí inspekci veškerého provozu na aplikační vrstvě. Solidní základ vrstvené bezpečnosti sítě dosáhneme, pokud v navrhované síti v rámci vrstveného zabezpečení použijeme proxy server, na hranovém směrovači paketový filtr a ve firewallovým zařízení překlady adres NAT.

4.1.4 Virtuální privátní sítě

Virtuální privátní sítě (VPN) umožňují bezpečné propojení dvou fyzicky oddělených sítí prostřednictvím Internetu, aniž by přenášená data byla odhalena někým cizím. Po dobu, co je VPN ustavena a zabezpečena šifrováním, odolává veškerým napadením. Problém ale vzniká v okamžiku vytváření zašifrovaného tunelu ve vlastních VPN. Zde pak může docházet k pokusům o přesměrování a všem možným hackerským útokům, proto se privátní síť implementuje jako nedílná součást firewallu. Pak mohou napadání VPN během vytváření zašifrovaného tunelu zabránit autentizace firewallu a služby zabezpečení.

4.1.5 Šifrovaná autentizace

Šifrovaná autentizace umožňuje externím uživatelům na Internetu prokázat firewallu, že jsou autorizovaní uživatelé s oprávněním provést připojení k interní síti. Šifrovaná autentizace může využívat bezpečné autentizační protokoly. Při navázání spojení může nebo nemusí být toto spojení šifrované. Využití šifrované autentizace je výhodné, protože k němu dochází na transportní úrovni mezi softwarem klienta a firewallem a nemusí se řešit pak zvláštním softwarem, který podporuje konkrétní nainstalované firewally.
Šifrovaná autentizace ale bohužel snižuje zabezpečení firewallu. Svou podstatou vyvolává tyto problémy:[6]

[6] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce*, s. 14

- Firewall musí na nějakém portu reagovat, protože naslouchá pokusům o připojení. Hackeři se tak mohou dozvědět, že firewall existuje.
- Připojení může být po ustavení pomocí ICMP přesměrováno, obzvláště pokud není šifrované.
- Hacker, který by sledoval ustavení připojení, může zfalšovat adresu autorizovaného klienta, a získat tak přístup do sítě, aniž by musel stávající připojení přesměrovávat.
- Přístup do sítě lze získat zneužitím ukradeného laptopu s příslušnými klíči.
- Zaměstnanci, kteří pracují doma, se mohou stát cílem napadení, protože jejich počítače mají přístup do privátní sítě.
- Postup autentizace může obsahovat mnoho chyb nebo nemusí být úplně bezpečný, takže kdokoliv na Internetu má možnost ověřit průchody přes firewall.

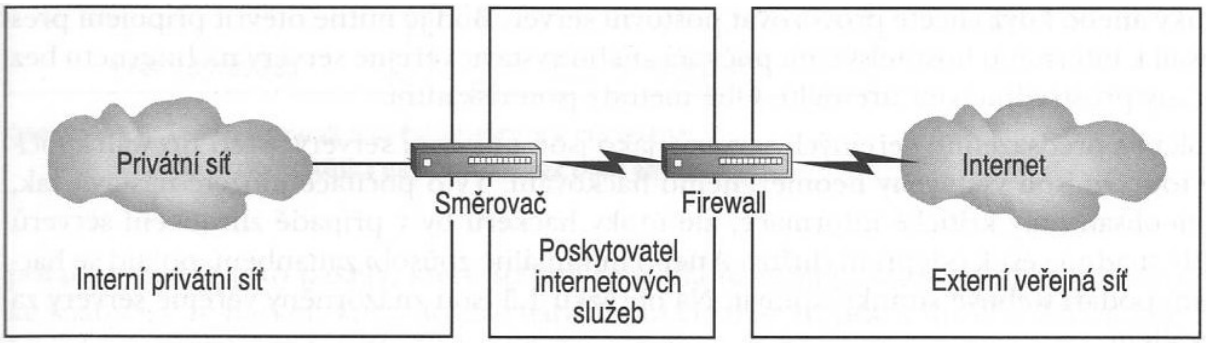
4.2 Možnosti zabezpečení

Při připojení firewallu mezi privátní sítí a Internetem vzniká problém, jak poskytovat veřejné služby zákazníkům a zároveň zabezpečit interní síť. Metody, které společnosti používají k ochraně sítí, je hned několik. Mezi tyto metody patří:

- služby filtrování paketů
- jeden firewall s veřejnými servery umístěnými v síti
- jeden firewall s s veřejnými servery umístěný mimo síť
- dvojitý firewall nebo firewall s demilitarizovanými zónami
- podnikové firewally
- odpojení

4.2.1 Služby filtrování paketů

Většina poskytovatelů internetových služeb poskytuje zákazníkům službu filtrování paketů. Za měsíční poplatek ISP firewall nastaví na filtrování do sítě a z ní. Někteří ISP také poskytují servery proxy a funkce NAT. Na obrázku (Obrázek 3) je znázorněno, jak služba filtrování paketů funguje.

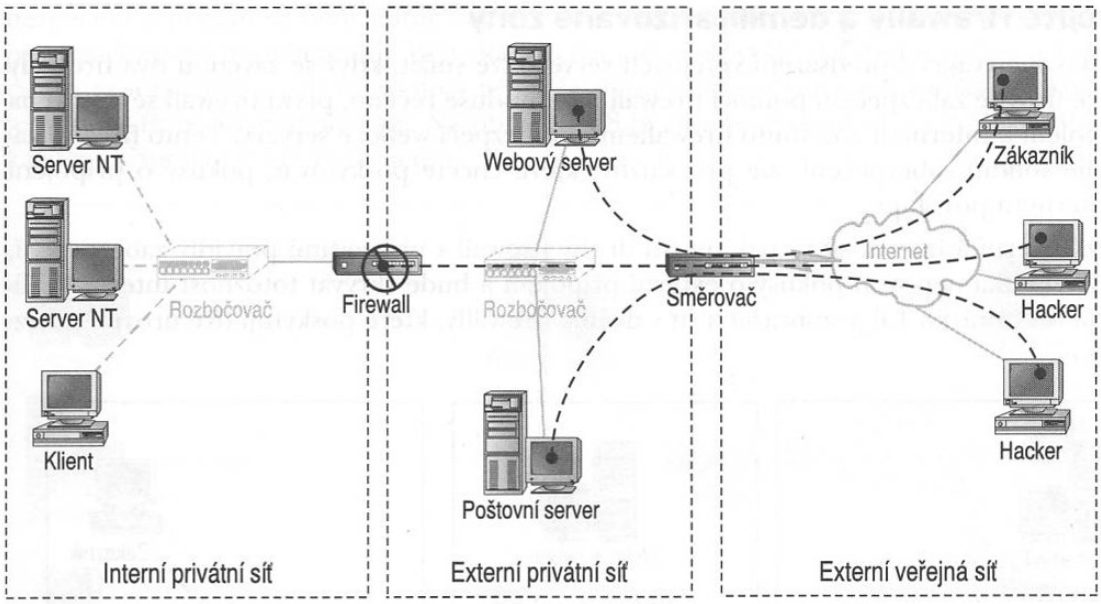


Obrázek 3 - Služba filtrování paketů; zdroj [3]

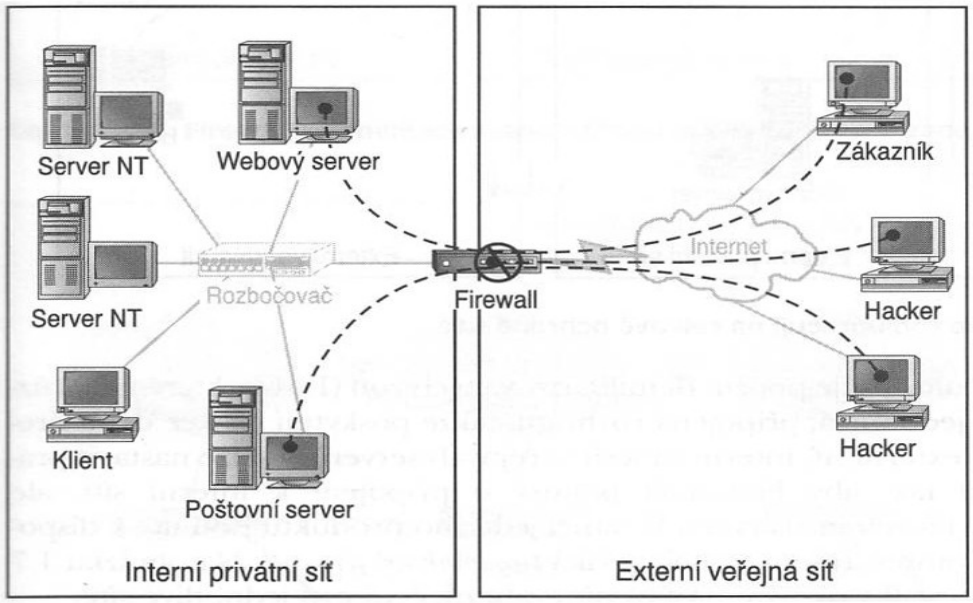
I kdyby byly služby firewallu poskytované ISP komplexní, přesto není nikdy dobré svěřovat zabezpečení sítě do rukou externí organizace.

4.2.2 Použití jednoho firewallu

Použitím jednoho firewallu je nejjednodušším zabezpečením hranic sítě. S jedním firewallem a jedním připojením k Internetu lze vytvořit jediný bod správy a řízení. Zapojení lze provést dvěma způsoby. Buď vystavíme veřejné servery na Internetu bez ochrany prostřednictvím firewallu (Obrázek 4), anebo veřejné servery umístíme za firewall do interní sítě (Obrázek 5).



Obrázek 4 - Jeden firewall a veřejné servery vystavené internetu; zdroj [3]



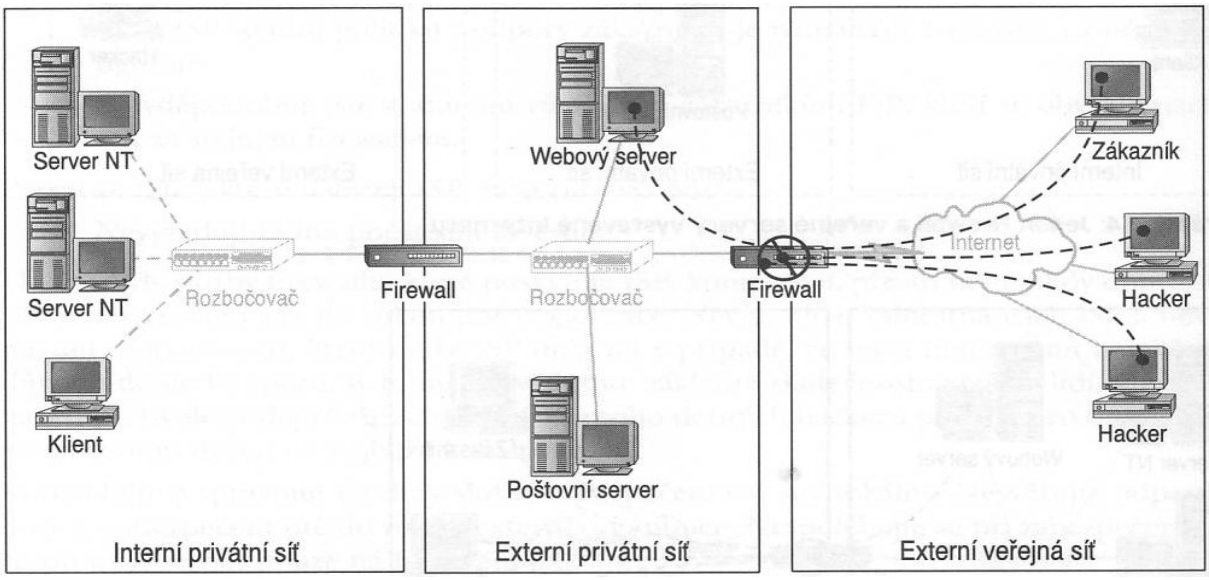
Obrázek 5 - Jeden firewall a veřejné servery umístěné za firewallem; zdroj [3]

Nevýhoda umístění veřejných serverů na Internetu spočívá v možnosti napadení těchto serverů hackery, proto musí být proti těmto útokům odolný a neměly by obsahovat žádné kritické informace.

Nevýhoda umístění veřejných serverů v interní síti spočívá v možnosti napadení chyby v softwaru služeb vyšší úrovně, a tím hacker ovládne počítač umístěný v interní síti. Z tohoto důvodu většina organizací instaluje servery před firewall, a přes firewall nepouští žádná externí připojení.

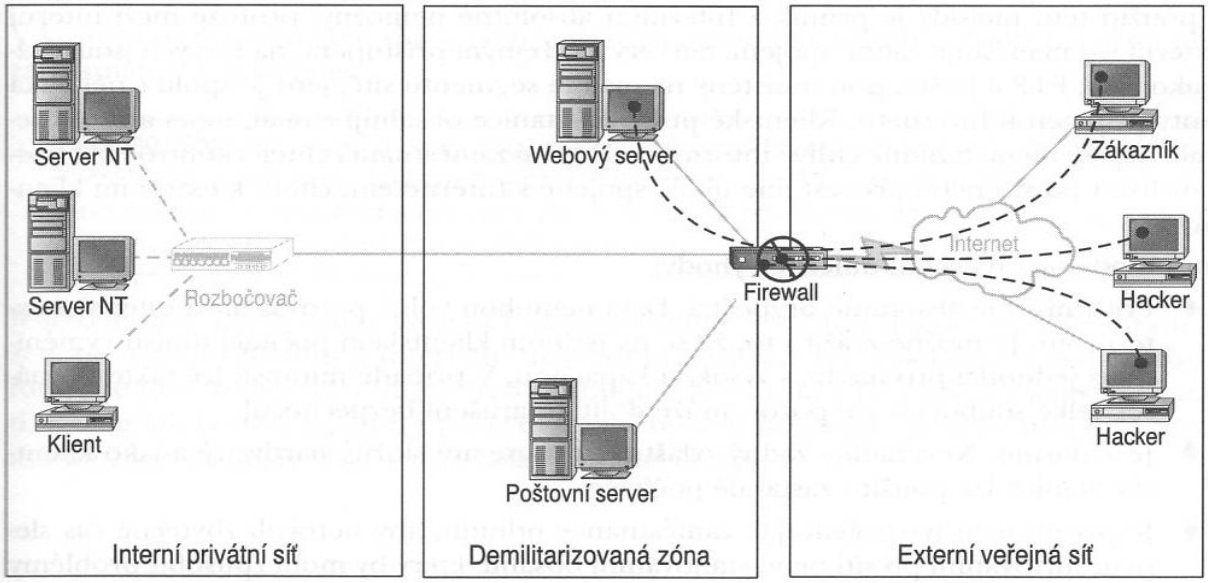
4.2.3 Dvojité firewally a demilitarizované zóny

Riziko napadení veřejných serverů lze snížit zavedením dvou firewallů. První firewall se umístí na připojení k Internetu, druhý firewall s přísnějšími zabezpečeními mezi externí a privátní sítí a veřejné servery jsou pak umístěné v externí síti (Obrázek 6).



Obrázek 6 - Dva firewally, které spolupracují na celkové ochraně sítě; zdroj [3]

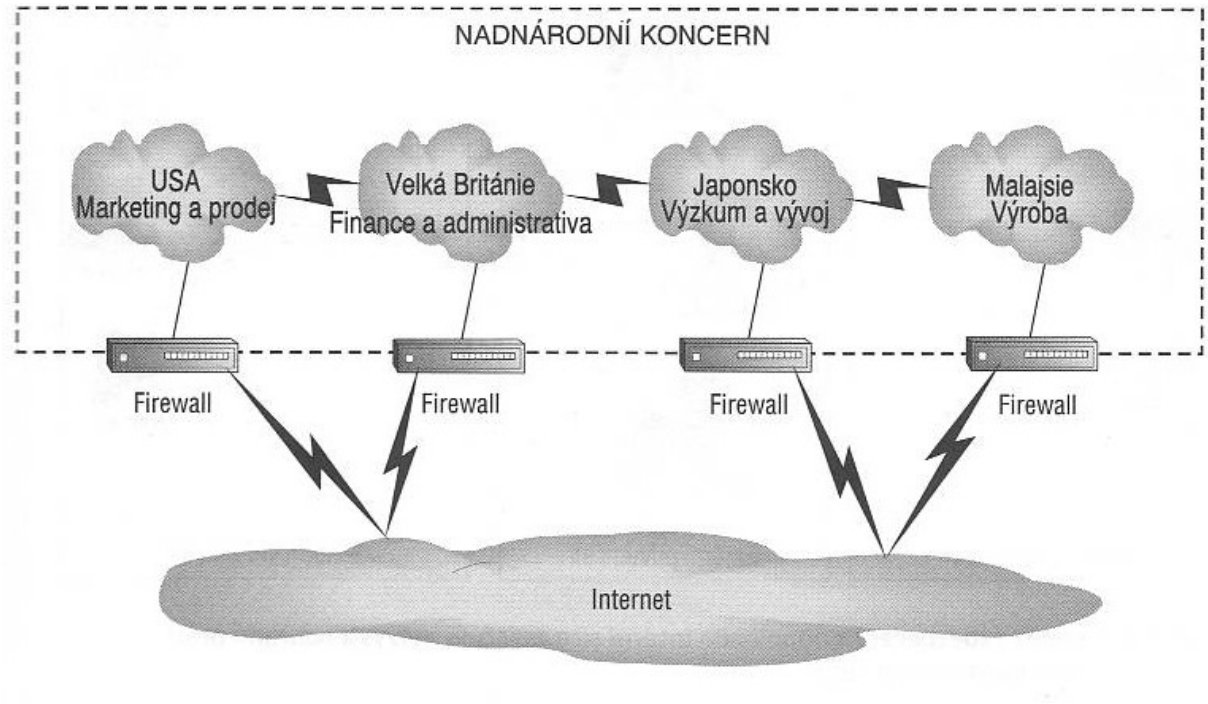
Většina novějších firewallů umožňuje použití demilitarizovaných zón (DMZ). Tyto firewally mají tři rozhraní – interní síť, externí síť a síť veřejných serverů. Pro jednotlivá rozhraní mají pak nastavená různá pravidla například tak, aby blokovala pokusy o připojení k interní síti, ale propouštěla určité protokoly na veřejné servery. V rámci jediného produktu jsou tak k dispozici funkce dvou firewallů, schéma tohoto zapojení je vidět na následujícím obrázku (Obrázek 7).



Obrázek 7 - Firewall s demilitarizovanou zónou; zdroj [3]

4.2.4 Podnikové firewally

Podnikové firewally sdílejí jeden centralizovaný soubor pravidel pro více firewallů. Pravidla pro firewall se definují na pracovní stanici pro zabezpečení a pak s pomocí zabezpečené autentizace replikují na jednotlivé firewally v organizaci. Takovéto schéma zapojení je vidět na následujícím obrázku (Obrázek 8).

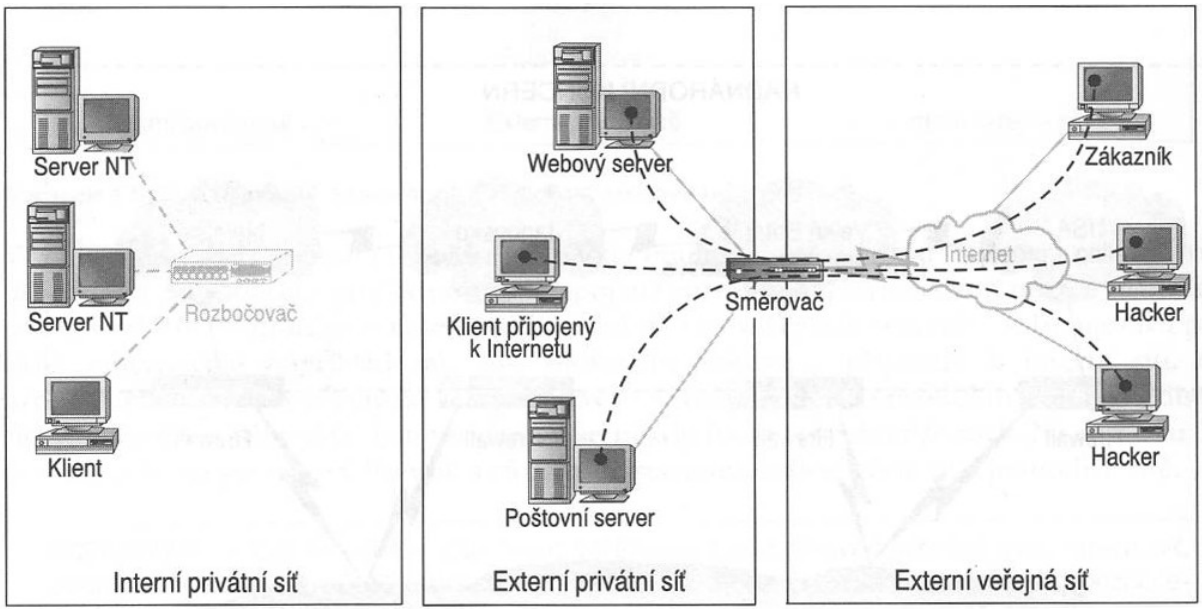


Obrázek 8 - Vícečetné firewally v podniku; zdroj [3]

4.2.5 Odpojení

Nejbezpečnější metodou je nepřipojovat interní síť k Internetu vůbec. Místo toho máme vytvořenou samostatnou síť, která se využívá pouze pro služby nějak spojené s Internetem. Jsou zde umístěné veřejné servery a několik klientů určených pro práci s Internetem. Při použití této metody je průnik do interní sítě zcela nemožný, protože mezi interní a externí síti neexistuje žádné spojení. Pokud zaměstnanci potřebují pracovat s internetovými službami, chodí ke klientům umístěným v externí privátní síti. Na obrázku (Obrázek 9) je zobrazeno schéma tohoto návrhu.

Výhodou tohoto zapojení je zajištění toho, aby zaměstnanci netrávili během pracovní doby žádný čas na Internetu a nedocházelo ke stahování nebezpečného obsahu působící problémy s právní odpovědností.



Obrázek 9 - Model zabezpečení s odpojením interní sítě; zdroj [3]

Nevýhodou je přecházení ke stanicím s přístupem k Internetu, které jsou většinou umístěné v jednom centrálním prostoru. Přenášení souborů se většinou pak provádí pomocí médií s vysokou kapacitou.

Oblíbenost této metody není u zaměstnanců moc velká.

4.3 Členění dnešních firewallů

Současné firewally můžeme rozdělit do těchto kategorií:

- osobní firewally
- vestavěné firewally
- SOHO softwarové firewally
- SOHO hardwarové firewally
- Enterprise softwarové firewally
- Enterprise hardwarové firewally
- speciální firewally

Softwarové i hardwarové firewally se vyskytují ve verzích SOHO a Enterprise. Rozdílem je zejména maximální propustnost, bezpečnost, počet současných spojení, počet uživatelů a kvalita služeb (QoS).

4.3.1 Osobní firewally

Osobní firewally jsou nejvíce rozšířené a jde o aplikace určené převážně pro ochranu uživatelských stanic s operačními systémy Windows. Tyto firewally jsou umístěné mezi operační systém a uživatelskými aplikacemi. Dokáží omezovat komunikaci nejen na základě služeb, portů a IP adres, ale také odlišují konkrétní aplikace. V poslední době se tento druh firewallů integruje také s antiviry, antispamy a dalšími nástroji pro bezpečnost. Příkladem osobního firewallu je Comodo Firewall, Online Armor Free, PC Tools Firewall Plus, Sunbelt Personal Firewall, ZoneAlarm Free a další.

4.3.2 Vestavěné firewally

Vestavěné firewally pracují na principu paketových filtrů a jsou často implementovány do směrovačů, přepínačů, nebo také WiFi přístupových bodů. Oproti pokročilejším řešením však vestavěné firewally poskytují pouze omezenou funkčnost, právě kvůli omezeným výpočetním prostředkům. Pokud tento typ firewallu disponuje i s rozšiřující funkcí IDS/IPS, pak se označují jako firewally s hloubkovou inspekcí.

4.3.3 Softwarové firewally

Softwarový firewall je specializovaný software s netriviálním nastavením, určený pro serverové operační systémy, není tedy vhodný pro laického uživatele, jako např. osobní firewall. Toto řešení zabezpečení je vhodné, když na daném serveru běží mimo služeb firewallu také další služby. Příkladem tohoto řešení jsou Astaro Security Gateway a Oracle SunScreen.

4.3.4 Hardwarové firewally

Hardwarové firewally se používají pro zabezpečení velkých sítí. Tyto firewally můhou být založeny na vlastní architektuře s aplikačně specifickými integrovanými obvody, nebo také na standardní PC architektuře, kde mnohá z řešení jsou založena na standardním unixovém operačním systému**,** nebo využívají tyto systémy po vlastních úpravách. Výrobci se rozhodli poskytovat tato řešení z důvodu lepší optimalizace softwaru na cílový hardware a také pro možnost garance propustnosti. Jako příklad je možné uvést Kernun UTM a Fortinet Fortigate vyvinuté nad FreeBSD, Gauntlet vyvinutý nad Solarisem nebo Secure SnapGear vyvinutý nad embedded verzí Linuxu.

4.3.5 Speciální firewally

Speciální firewall je zaměřený na konkrétní aplikaci. Jde o firewally pro ochranu webových aplikací, databázových serverů, e-mailových serverů nebo filtrování webového obsahu. Omezená funkčnost aplikačních firewallů je nahrazena možností pokročilé konfigurace pravidel pro kontrolu a filtrování přesně definovaných služeb, což je možné právě díky jejich úzkému zaměření.

4.4 Klady, zápory a cenová kalkulace SW a HW řešení

Zde bych rád uvedl popis jednotlivých řešení, jejich klady, zápory a v neposlední řadě jejich cenovou kalkulaci. Pro porovnání cen jsem uvedl SW a HW řešení od firmy Kerio a v příloze (Příloha P2) je uvedena cenová nabídka dalších firewallů, kterou zpracovala firma Autocont.

4.4.1 Softwarové produkty

Jedná se o programy určené zejména k instalaci na servery nebo klientské stanice. Výhodou je jejich nižší pořizovací cena vzhledem k možnosti využití stávajícího hardware zákazníka a snadnější aktualizace systému. Nevýhodou je zase o něco větší časová náročnost při implementaci, nutnost prověření kompatibility se stávajícími aplikacemi a vytěžování stávajícího serveru. Také je nutné počítat s náklady na údržbu a správu systému.

Příkladem serverové instalace je třeba produkt Kerio Control 7. Ceník je uveden v následující tabulce (Tabulka 1).

Tabulka 1 - Kerio Control pro nového uživatele, platnost licence 1 rok; zdroj [15]

Produkt	Cena bez DPH	Další uživatelé (lze zakoupit v blocích po 5)
Server (včetně 5 uživatelů)	5 000 Kč	480 Kč / uživatel

4.4.2 Hardwarové produkty

Jedná se o samostatná zařízení, která jsou dodávána zákazníkovi dle jeho požadavků a jsou dále konfigurována. Hardwarový firewall je obecně považovaný za výkonnější a bezpečnější, protože se o počítač nedělí s dalšími aplikacemi, které jej mohou ohrozit. Výhodou tohoto řešení je, že zákazník získává samostatné dostatečně dimenzované

zařízení, jež lze snadno umístit třeba do klimatizovaného rozvaděče a ve většině případů nevyžaduje další údržbu. Nevýhodou je poněkud vyšší pořizovací cena oproti řešení softwarovému. Většinou toto zařízení také nemá vyřešeno zálohování dat a aktualizaci systému.

Příkladem je produkt Kerio Control Box. Pro malé prostředí je určený Kerio Control Box 1110, pro větší a náročnější prostředí je Kerio Control Box 3110 s licencí pro 40 uživatelů a osmi ethernetovými porty 1Gbps. Ceník je uveden v následující tabulce (Tabulka 2).

Tabulka 2 - Kerio Control Box pro nového uživatele, platnost licence 1 rok; zdroj [15]

Produkt	Cena bez DPH	Další uživatelé (lze zakoupit v blocích po 5)
Kerio Control Box 1110 (včetně 20 uživatelů)	29 600 Kč	734 Kč / uživatel
Kerio Control Box 3110 (včetně 40 uživatelů)	53 300 Kč	734 Kč / uživatel

Dalším příkladem HW řešení je Fortinet Fortigate, nabízí několik modelů pro různou velikost počítačové sítě. Pro malé firmy, kanceláře / domácí kanceláře (SOHO) je vhodný model FortiGate-50B, pro podniky středních rozměrů je vhodné výkonnější řešení, a to model FortiGate-110C. Cena těchto produktů je uvedena v příloze (Příloha P2).

5 Praktický příklad – způsob testování

Z praktického hlediska bych chtěl otestovat funkčnost osobních firewallů. Testování jsem rozdělil do dvou částí. V první části otestuji dva připravené stolní počítače, jeden s čistou instalací systému Windows XP a druhý s již nainstalovanými běžnými aplikacemi, pomocí programu Nessus – skener zranitelných míst. V druhé části pak otestuji tyto počítače pomocí leak-testů, na kterých postupně otestuji zdatnost pěti osobních firewallů. Pro testování jsem si vybral pouze osobní firewally bez antivirové ochrany, určené především pro domácí použití, licencované jako freeware. Ty lze na internetu získat zdarma a nebo jako trial verze až na 30 zkušebních dnů, které se po uplynutí této doby přepnou do bezplatné verze. Tento produkt je určen pro širokou cílovou skupinu, protože osobní firewally nalézají uplatnění zpravidla u uživatelů v domácnostech. Osobní firewally by měly nabízet jednoduchou obsluhu a intuitivní nastavení pravidel i pro nepříliš znalé uživatele.

HW specifikace testovaných počítačů: starší značkový počítač HP D530S SFF s CPU Intel Pentium 4 HT 2.66GHz, 1GB RAM, HDD 40GB, integrovaná VGA, zvuková a síťová karta.

SW specifikace testovaných počítačů:

PC-pokus1 – čistá instalace Windows XP Professional se SP3 a veškerými dostupnými aktualizacemi k únoru 2011 a Internet Explorer verze 8.0.6001.18702.

PC-pokus2 – instalace Windows XP Professional se SP3 a veškerými dostupnými aktualizacemi k únoru 2011, Internet Explorer verze 8.0.6001.18702, Adobe Flash Player 10 ActivX, Adobe Reader 9.4.2, Adobe Shockwave Player 11.5, ICQ 7.4, Microsoft Office Professional Edition 2003 se SP3, Microsoft Silverlight, Skype ™ 5.1, Total Commander 7.55a a Windows Media Player 11.

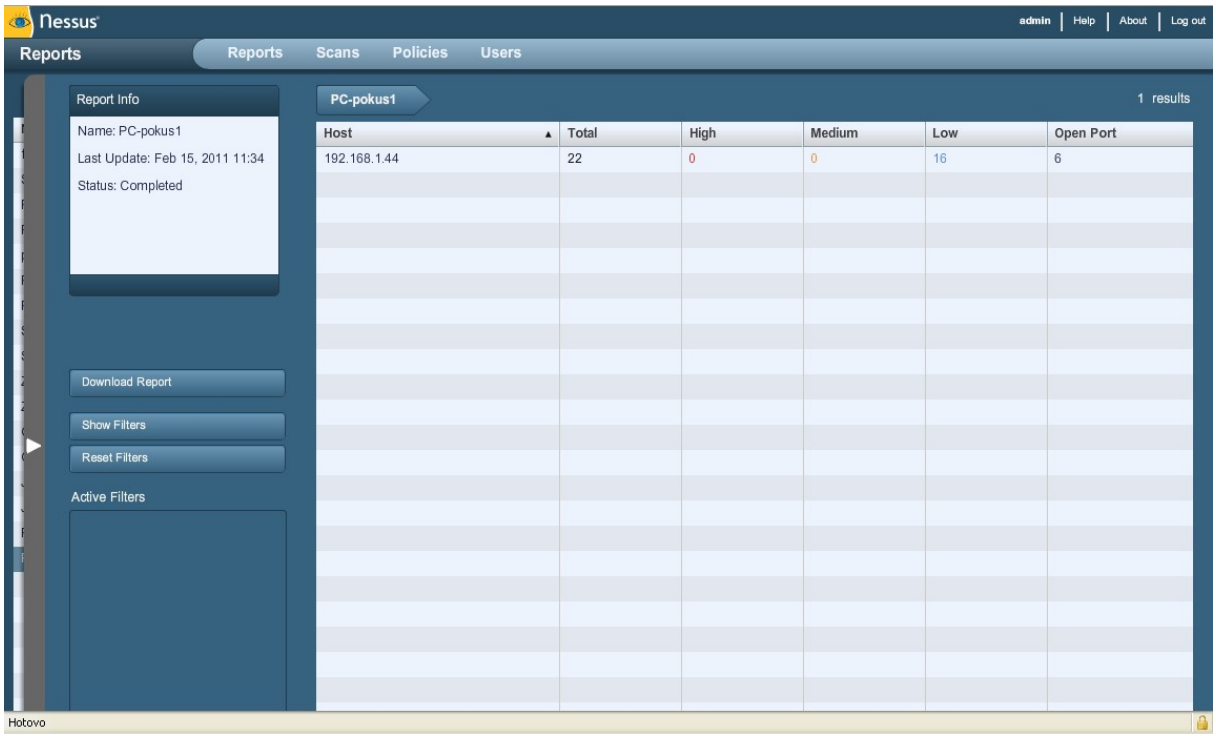
Po nainstalování pokusných počítačů bez instalovaných osobních firewallů jsem si vytvořil bod obnovy, ke kterému jsem se pokaždé vracel, když jsem instaloval nový firewall. Tímto způsobem jsem se snažil zajistit stejné výchozí podmínky pro každý testovaný osobní firewall.

Informace pro tuto kapitolu jsem čerpal ze zdroje [14].

5.1 Odhalování zranitelných míst – Nessus

Program Nessus (http://www.nessus.org/) je kvalitní skener zranitelných míst, který vyhledává dostupné porty služeb a provádí ověření bezpečnosti tak, abychom se dozvěděli, zda by na objevené systémy mohly být použity nějaké známé postupy pro zneužití zranitelných míst. Součástí programu Nessus jsou stovky různých pluginů, pomocí nichž lze zhodnotit mnoho typu zařízení. Pluginy jsou seskupeny do kategorií typu *backdoors, small services, Microsoft Windows a CGI abuses*, tedy skupina pluginů pro hledání zadních vrátek, malých služeb, Microsoft Windows, a skupina pluginů zaměřující se na zranitelnosti pomocí skriptů CGI.

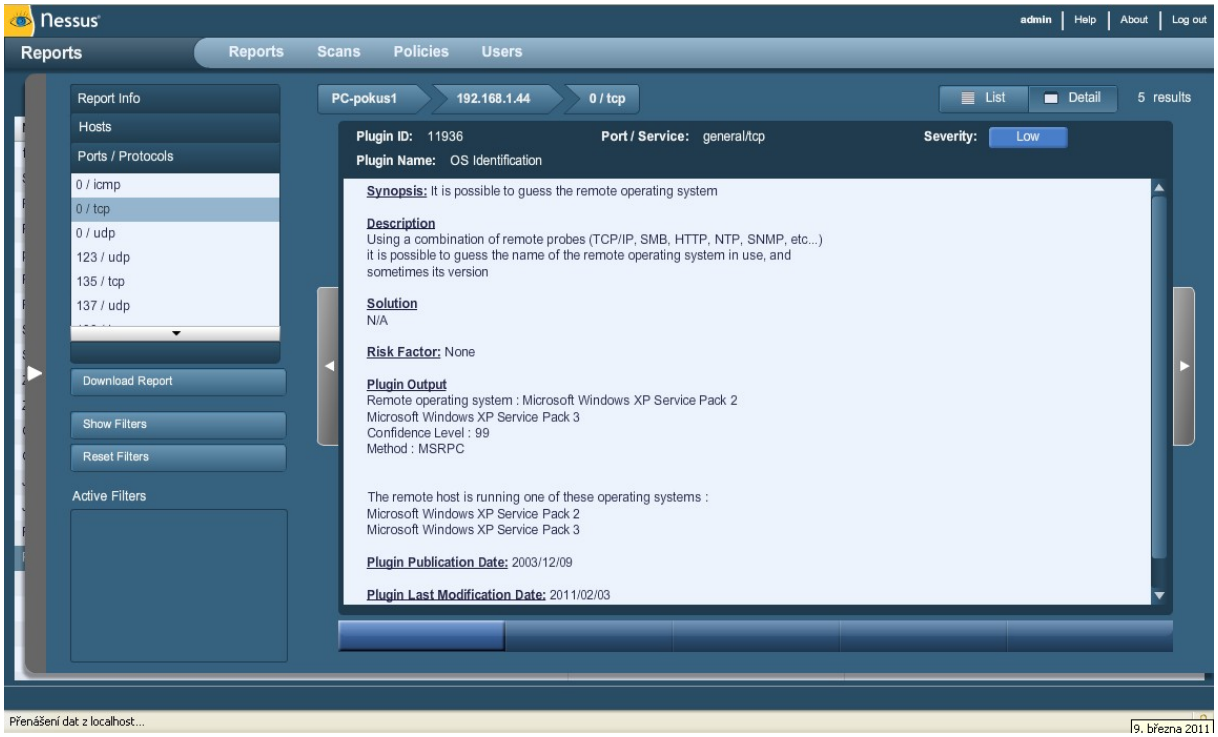
Po provedení skenování zranitelných míst, program Nessus sestaví souhrnnou tabulku (Obrázek 10) s počtem otevřených portů a s rozdělením do tří úrovní bezpečnostních rizik: nízké, střední a vysoké riziko. Testování otevřenosti portů zkoumá napadnutelnost počítače z Internetu. Kontrolují se především porty nejpoužívanějších a nejzneužívanějších služeb, jako například ftp, telnet, smtp, pop3, www a jiné. Tento způsob vzdáleně otestuje, je-li příslušný port otevřen, a tím pádem i napadnutelný.



Obrázek 10 - Výsledek skenování; zdroj vlastní

Pak už můžeme začít rozklikávat a prohlížet bezpečnostní trhliny, které jsou seřazeny podle závažnosti v tříbodové stupnici. Nejtěžší (High) trhliny doporučuji co nejdříve

vyřešit. Z Nessusu se dozvíme název a popis chyby. Na obrázku (Obrázek 11) vidíme popis bezpečnostního rizika identifikace operačního systému, která je kvalifikována jako riziko s nízkou úrovní. U některých chyb vám dokonce Nessus sám navrhne řešení nebo na ně odkáže.



Obrázek 11 - Identifikace OS; zdroj vlastní

Celkový výsledek obou testovaných stanic je uveden v tabulce (Tabulka 3):

Tabulka 3 - Počty nalezených bezpečnostních rizik; zdroj vlastní

	IP adresa	Total	High	Medium	Low	Open port
PC-pokus1	192.168.1.44	22	0	0	16	6
PC-pokus2	192.168.1.29	40	0	0	28	12

Na testování nemělo žádný vliv, jaký osobní firewall byl na pracovní stanici zrovna nainstalovaný. Z tabulky je patrné, že čím více aplikací je na počítači nainstalováno (především aplikací vyžadující komunikaci s Internetem), tím více vzniká otevřených portů a následných bezpečnostních rizik.

5.2 Leak testy

Další pomůckou pro testování osobních firewallů jsou tzv. leak testy. To jsou malé neškodné programy vytvořené odborníky pro testování síťové bezpečnosti, které prověřují

zdatnost firewallu detekovat neoprávněnou odchozí komunikaci do Internetu. Každý tento prográmek se o to snaží odlišným způsobem. Správný firewall by měl nabízet jednoduchou filtraci a zároveň odolat útokům z internetu na chráněný počítač. Na internetu lze nalézt několik projektů, které se těmito testy zabývají. Najdeme je na stránkách: http://www.pcflank.com, http://www.testmypcsecurity.com/ a nebo nejzajímavější na http://www.matousec.com/projects/proactive-security-challenge/. O posledním zmíněném projektu lze říci, že je nejznámější a jedná se o projekt Davida Matouška, který s týmem lidí zveřejnil testy nazvané Firewall Challenge. Cílem testů je spojit hloubkovou analýzu spolu s jednoduchostí leak testů. Testuje se i pokus o obejití ochrany nebo ukončení běhu firewallu, což je test zaměřený na obranné mechanismy firewallu. Analýza se také zaměřuje na výkonnostní testy a aplikace špionážního softwaru, mezi kterými nalezneme keyloggery a paket sniffery. Já jsem z tohoto projektu vybral pro testování firewallů tyto leak testy:

Awft	Utilita, která zkouší různé možnosti a techniky, jak se dostat z testovaného počítače bez vědomí firewallu.
Bitstest	Pokouší se využít BITS (Background Intelligent Transfer Service) služby systému Windows XP ke stažení souboru ze vzdáleného serveru.
Breakout	Test prohlížeče Internet Explorer a jeho zneužití pomocí Windows Active Desktop.
Coat	Pomocí substituce o sobě mění informace a poté se snaží navázat internetové spojení.
Copycat	Používá konkrétní službu Windows API (Advanced Program Interface) k převzetí kontroly nad vláknem procesu, který je povolen v nastavení firewallu.
CPIL	Comodo Parent Injection Leak testovací souprava obsahuje testy k obelhání firewallu pomocí manipulace se spouštěcím souborem prohlížeče explorer.exe.
Cpilsuite	Tento program obsahuje tři testy, jež jsou variací na CPIL test a navíc tento program testuje také útok pomocí OLE protokolu a práce s pamětí.
Ddetest	Testuje, zda firewall chrání Internet Explorer před manipulací nedůvěryhodnou aplikací pomocí protokolu DDE.
Dnstest	Testuje, zda firewall dokáže rozlišit čistý a infikovaný Service Host proces.

Dnstester	Tato metoda využívá v systémech Windows DNS klienta, jehož prostřednictvím se snaží odeslat informace z vašeho počítače.
Echotest	Testuje, zda firewall filtruje ICMP pakety tak, že se snaží zaslat vzdálenému serveru pakety ve formě ICMP ECHO požadavku.
Firehole	Tento test se pokusí o procesní injekci internetového prohlížeče.
Flank	Testuje, zda firewall zabraňuje manipulaci Internet Exploreru za použití rozhraní IWebBrowser2.
Jumper	Pokusí se infikovat soubor prohlížeče svým vlastním kódem a po násilném restartu prohlížeče se načte do systému a zkusí odeslat informace na internet.
Leaktest	Jeden z nejstarších leak-testů, který zaměňuje název spuštěného procesu.
Newclass	Testuje, zda firewall správně chrání před zneužitím OLE objektu.
Osfwbypass	Zkusí načíst HTML stránku s Java skriptem, který přesměruje prohlížeč na vzdálený server.
Runner	Zkusí nabourat integritu spouštěcího souboru prohlížeče.
Schedtest	Testuje, zda firewall umožňuje nedůvěryhodným aplikacím vytvářet události přes rozhraní Task Scheduler COM.
Thermite	Testuje, zda firewall blokuje pokusy manipulovat s pamětí běžící instance výchozího prohlížeče.
Tooleaky	Spustí skrytě prohlížeč s parametry příkazového řádku.
Vbstest	Testuje, zda je možné obejít firewall pomocí skriptu Visual Basic.
Wallbreaker	Cílem těchto testů je různými způsoby spustit originál nebo kopii spouštěcího souboru prohlížeče.
Yalta	Během testu se pokusí odeslat několik UDP paketů prostřednictvím portů jako 53 (DNS), 21 (FTP) apod. a zkouší, zda jsou otevřeny.

Po dohodě s vedoucím diplomové práce jsme vybrali pro testování tyto osobní firewally: Comodo Firewall, Online Armor Free, PC Tools Firewall Plus, Sunbelt Personal Firewall a ZoneAlarm Free. Popis jednotlivých osobních firewallů, průběh a výsledek jejich testování je rozsáhlejší, a proto je popsán v následující kapitole.

6 Testování osobních firewallů

V této kapitole popisuji jednotlivé produkty osobních firewallů, tzn. co nabízejí, jakým způsobem se instalují, jejich vzhled, možnosti nastavení a v neposlední řadě i přehledný souhrn výsledků jednotlivých leak testů.

6.1 Comodo Firewall

Pro testovací účely jsem použil Comodo Firewall, verze 5.3.176757.1236 vydaná dne 29. 12. 2010. Comodo Firewall je poskytován zcela zdarma.

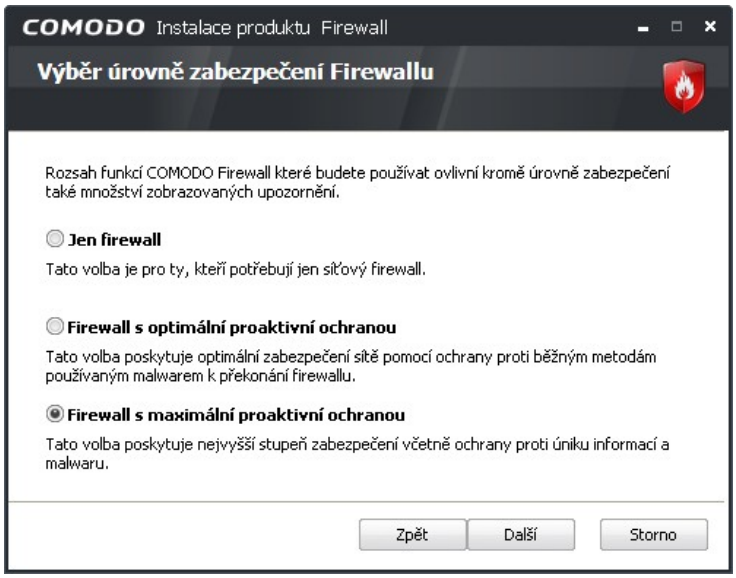
6.1.1 O produktu

Společnost Comodo (http://comodo.com) nabízí uživatelské produkty týkající se internetové bezpečnosti, jako jsou firewall, antispam, antivirus, e-mailové zabezpečení a jiné. V programu Comodo Firewall lze velice podrobně definovat stupeň zabezpečení. Možné je zvolit z několika stupňů bezpečnosti i provést konfiguraci pro jednotlivé typy souborů. Samozřejmostí je blokování portů nebo nastavení způsobu upozorňování na jednotlivé bezpečnostní hrozby. Manuálně lze přidávat aplikace, které jsou za všech okolností povolené, nebo naopak programy, k jejichž spuštění nedojde nikdy. V případě jakýchkoli nesnází je možné využít fórum internetové komunity programu, odeslat lze i podezřelá data na analýzu vývojářům aplikace.

6.1.2 Instalace

Samotná instalace je úplně bezproblémová a standardní. Instalací firewallu provází grafický průvodce, který pomáhá uživateli s jejím průběhem. Hned po spuštění průvodce jsme dotázáni na jazyk instalace, kde lze vybrat i češtinu. Po odsouhlasení podmínek licence se můžeme bezplatně registrovat pro odběr novinek a aktualizací. Tato registrace je nepovinná. V dalším okně průvodce je možnost vybrat produkty k instalaci, a to samotný Comodo Firewall a Comodo GeekBuddy (60-ti denní zkušební verze). Produkt Comodo GeekBuddy poskytuje neomezenou pomoc prostřednictvím živé vzdálené podpory pomáhající odstraňovat problémy, vylepšovat výkon počítače, optimalizovat nastavení Windowsu, nastavovat e-maily, tiskárny a další. V dalším okně volíme úroveň zabezpečení firewallu (Obrázek 12), zda jen samotný firewall, nebo s optimální či maximální proaktivní ochranou. V další nabídce volíme zda chceme, nebo nechceme využívat Comodo Secure

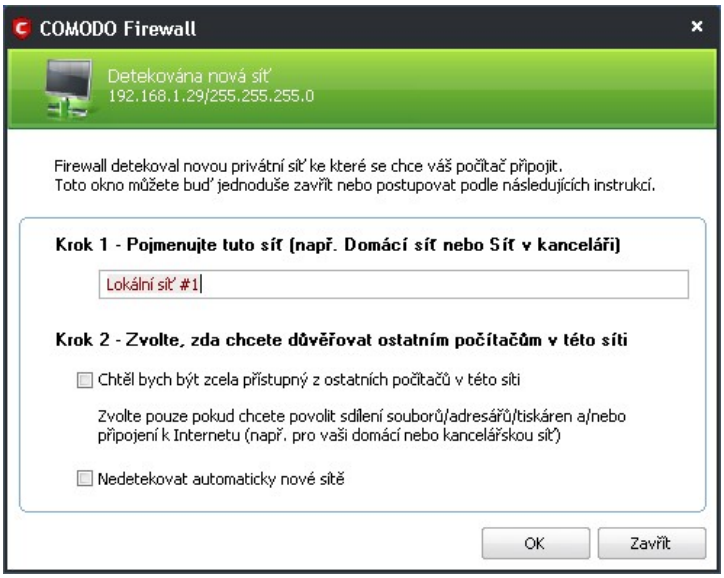
DNS. Pak už nás průvodce upozorňuje na úspěšné dokončení instalace. Po nainstalování se musí restartovat počítač.



Obrázek 12 - Výběr úrovně zabezpečení; zdroj vlastní

6.1.3 První spuštění

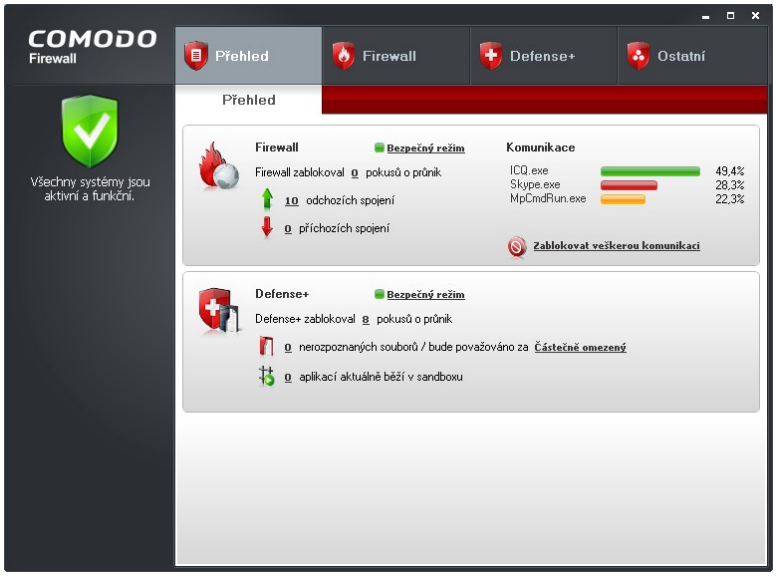
Při prvním spuštění firewall automaticky detekuje novou síť a následně se dotazuje ohledně procesů, které již v počítači běží, zda je přijmout, nebo blokovat. U každého takové okna je krátký popis upozornění**.** Jedná se například o systémové procesy, různé komunikátory, prohlížeče, poštovní klienty apod.



Obrázek 13 - Detekce nové sítě; zdroj vlastní

6.1.4 Popis nastavení a vzhledu

Úvodní okno (Obrázek 14) obsahuje levý panel informující o stavu systému a čtyři záložky, mezi kterými se lze přepínat: *Přehled*, *Firewall*, *Defense+* a *Ostatní*.



Obrázek 14 - Vzhled programu; zdroj vlastní

Záložka *Přehled* zobrazuje informace ve dvou oddílech. V prvním oddíle se graficky signalizují události firewallu typu příchozí a odchozí spojení, úroveň zabezpečení firewallu a probíhající síťová komunikace. V druhém oddíle jsme informováni o událostech Defense+. Tato součást aplikace kontroluje chování systému a procesů**.** Pokud se spouští nějaký spustitelný soubor**,** pak je uživatel upozorněn.

Záložka *Firewall* umožňuje prohlížet události, které firewall zaznamenal, zablokovat určitou aplikaci, nebo ji naopak přidat do důvěryhodných aplikací, nastavovat síťová pravidla pro paketové filtry, prohlížet si aktivní spojení, maskovat porty a měnit další nastavení chování firewallu jako je například úroveň zabezpečení, podrobnost a četnost upozornění.

Záložka *Defense+* umožňuje prohlížet události, které tato služba zaznamenala, nastavovat důvěryhodné soubory, u nerozpoznaných souborů nastavit, zda jsou důvěryhodné a naopak, nastavovat pravidla zabezpečení (chráněné soubory a adresáře, klíče registru, COM rozhraní a další), sledovat aktivní procesy, možnost spuštění programu v sandboxu (izolované prostředí) a další nastavení jako je například úroveň zabezpečení, nastavení sandboxu a nastavení sledování.

Záložka *Ostatní* umožňuje nastavovat samotnou aplikaci. Do toho spadá například jazyk, vzhled, rodičovská ochrana, způsob připojení, diagnostika, nápověda, informace o programu ale i odkaz na diskusní fórum.

6.1.5 Průběh při testování

Během práce na počítači firewall upozorňuje uživatele na jednotlivé události pomocí vyskakujících oken. V oknech upozornění Firewallu se zobrazuje název aplikace pokoušející se navázat spojení, cílová IP adresa s portem, bezpečnostní doporučení a nabídku odpovědi, zda spojení povolit nebo zakázat.

V oknech upozornění Defense+ (Obrázek 15) se zobrazuje název spuštěného souboru a jeho činnost, kterou chce provádět. Podle informací v oddíle Bezpečnostní doporučení se pak můžeme rozhodnout, zda akci povolíme, nebo zamítneme, a zatržením volby můžeme ještě upřesnit, zda se má vytvořit bod obnovení systému, odeslat soubory k analýze, nebo si zapamatovat odpověď.

Obrázek 15 - Upozornění Defense+; zdroj vlastní

6.1.6 Hodnocení

Pracuje spolehlivě, jeho ovládání je velice jednoduché, velkou výhodou je databáze důvěryhodných aplikací. Program byl testován v úrovni zabezpečení s maximální proaktivní ochranou. Úspěšnost tohoto programu v testování je zobrazena v tabulce

(Tabulka 5), kde jsou porovnány výsledky všech testovaných osobních firewallů. Odinstalace proběhla v pořádku.

6.2 Online Armor Free

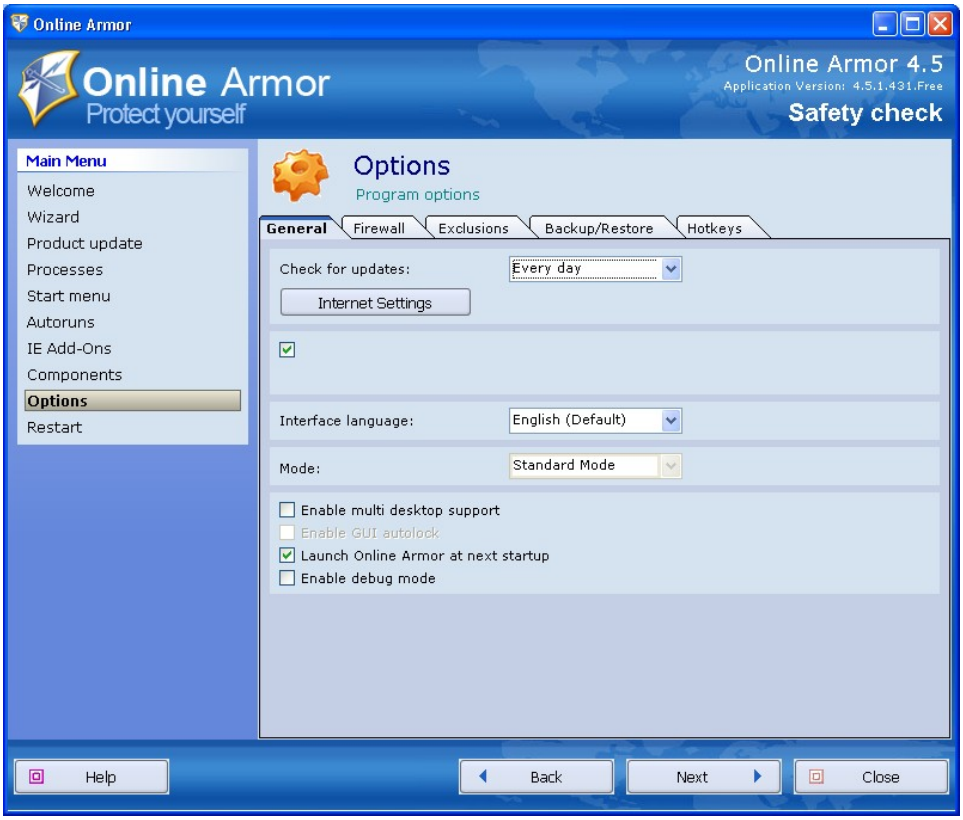
Pro testovací účely jsem použil Online Armor Free, verze 4.5.1.431 vydaná dne 28. 10. 2010. Online Armor Free je poskytován zcela zdarma.

6.2.1 O produktu

Společnost Emsi Software GmbH (http://www.online-armor.com) nabízí uživatelské produkty týkající se internetové bezpečnosti jako jsou firewall, antispam, antivirus, e-mailové zabezpečení a jiné. Firma nabízí tři verze tohoto produktu, Online Armor Free nabízí samozřejmě nejméně funkcí. Kromě standardních funkcí firewallu nabízí i pravidelné aktualizace, webový štít, ochranu proti shození, detekci keyloggerů i obranu proti červům. Při spokojenosti s programem je možné zakoupit pokročilejší verzi buď Online Armor Premium, nebo Online Armor ++, který má v sobě i antivirus.

6.2.2 Instalace

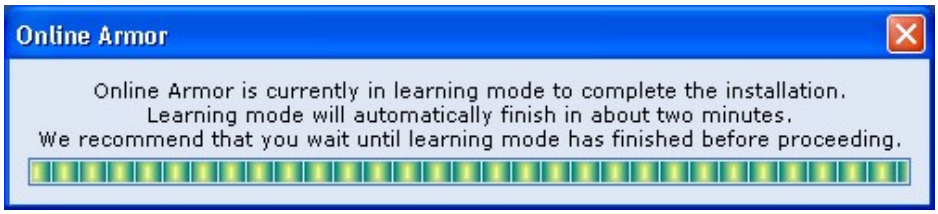
Samotná instalace je úplně bezproblémová a standardní. Instalací firewallu provází grafický průvodce, který pomáhá uživateli s jejím průběhem. Hned po spuštění průvodce jsme dotázáni na jazyk instalace, bohužel tento produkt není lokalizován do češtiny. Po uvítací stránce se nás průvodce ptá, jakou verzi chceme instalovat. Zde máme právě na výběr, zda zvolíme verzi zdarma, a nebo nějakou z dalších placených. Na dalších stránkách musíme postupně zadat registrační e-mail, odsouhlasit licenční podmínky, zadat cílový adresář instalace a název složky v nabídce Start. Hned po nainstalování se spouští průvodce bezpečnostního nastavení (Obrázek 16), který provádí nastavením už samotného programu. Většina voleb proběhne automaticky, u placené verze může zkušenější uživatel jednotlivé položky sám nastavovat. V této konfiguraci probíhá skenování systému, aktualizace produktu a samotné nastavení firewallu. Bohužel v této verzi můžeme nastavit pouze standardní mód. Po této konfiguraci se musí restartovat počítač.



Obrázek 16 - Průvodce bezpečnostního nastavení; zdroj vlastní

6.2.3 První spuštění

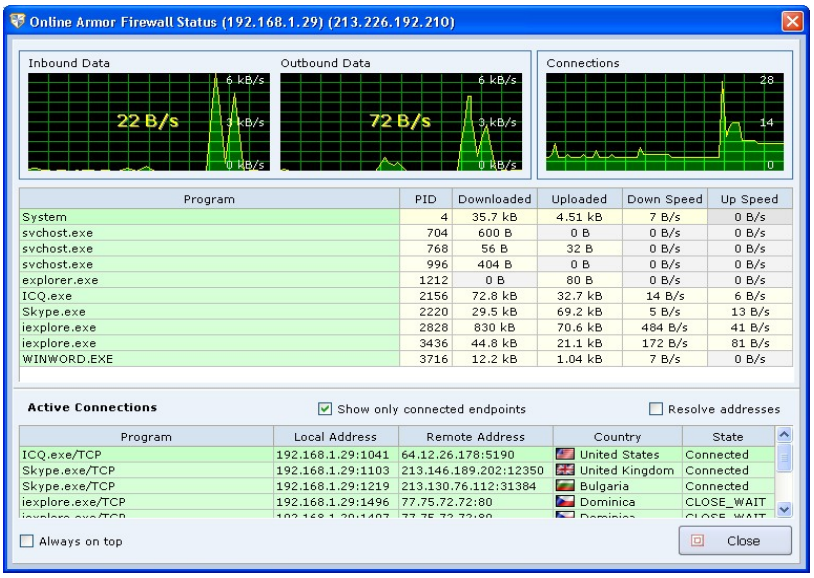
Po prvním spuštění se firewall ještě automaticky donastavuje v režimu učení (Obrázek 17).



Obrázek 17 - Učící se režim; zdroj vlastní

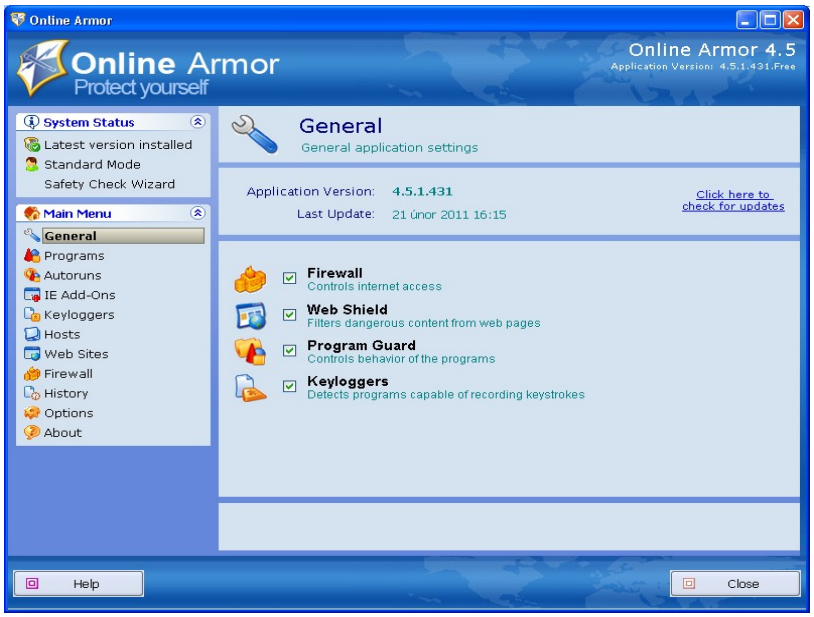
6.2.4 Popis nastavení a vzhledu

Po instalaci a restartu se v taskbaru objeví dvě signalizační ikonky, první signalizuje síťový provoz (Obrázek 18). Je rozdělen do tří oddílů, ve kterých jsme informováni o aktuální síťové komunikaci a jejích detailech jako objem přenesených dat, rychlost stahování a seznam IP adres aktivních spojení.



Obrázek 18 - Síťový provoz; zdroj vlastní

Druhá ikonka v taskbaru slouží pro samotné nastavování programu. Online Armor má příjemné a přehledné grafické rozhraní (GUI – Graphical User Interface) (Obrázek 19).



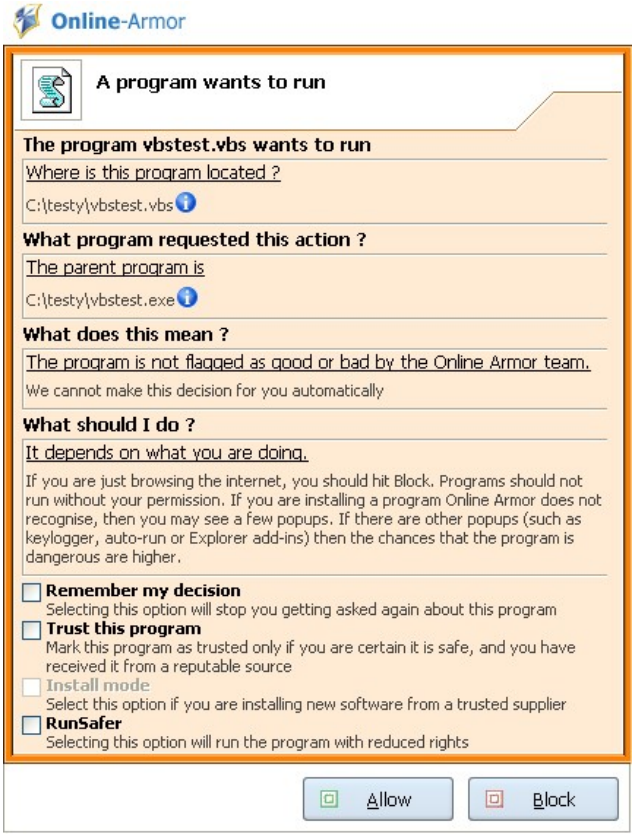
Obrázek 19 - Vzhled programu; zdroj vlastní

V horní liště jsme informováni o verzi programu. Levá lišta je rozdělena na dva oddíly. V horním oddíle jsou zobrazeny systémové informace o stavu aktualizace, v jakém módu firewall běží a průvodce bezpečnostního nastavení. V dolním oddíle je samotná hlavní nabídka, pomocí které konfigurujeme samotný firewall. Každá položka v nabídce zobrazuje v hlavním okně příslušné informace a možnost nastavení. V těchto nabídkách

zapínáme a nastavujeme hlavní funkce programu jako je firewall, webový štít, ochranu před manipulací a ochranu před keyloggery. Díky ořezané verzi nelze vše konfigurovat. Dále můžeme zobrazit historii upozornění a akci, kterou jsme provedli.

6.2.5 Průběh při testování

Během práce na počítači firewall upozorňuje uživatele na jednotlivé události pomocí vyskakujících oken (Obrázek 20), kde buď vytváříme pravidla pro aplikace přistupující k internetu, anebo pravidla pro aplikace spouštěné na tomto počítači. V pop-up oknech se zobrazuje název spuštěného souboru a kde se soubor nachází. Podle zobrazených informací se pak můžeme rozhodnout, zda akci povolíme, nebo zamítneme, a zatržením dalších voleb můžeme své rozhodnutí upřesnit.



Obrázek 20 - Upozornění; zdroj vlastní

6.2.6 Hodnocení

Jeho ovládání je velice jednoduché a intuitivní. Program byl konfigurován v automatickém režimu. Úspěšnost tohoto programu v testování je zobrazena v tabulce

(Tabulka 5), kde jsou porovnány výsledky všech testovaných osobních firewallů. Odinstalování programu proběhlo v pořádku.

6.3 PC Tools Firewall Plus

Pro testovací účely jsem použil PC Tools Firewall Plus, verze 7.0.0.111 vydaná 30. 11. 2010, je poskytována zcela zdarma.

6.3.1 O produktu

Společnost PC Tools™ (http://www.pctools.com/) vydává software a poskytuje technické zdroje pro zabezpečení, ochranu a údržbu operačních systémů Windows® a Macintosh. PC Tools Firewall Plus je osobní firewall, který můžeme nastavit dvěma způsoby, prvním z nich je povolení či zakázání přístupu k jednotlivým aplikacím. Druhý způsob funguje na bázi TCP/IP protokolu, což vyžaduje pokročilé znalosti. Zde můžeme nastavit použitý protokol, port a IP adresu.

6.3.2 Instalace

Samotná instalace je úplně bezproblémová a standardní. Instalací firewallu provází grafický průvodce, který pomáhá uživateli s jejím průběhem. Hned po spuštění průvodce jsme dotázáni na jazyk instalace, bohužel zde ale není na výběr český jazyk. To ovšem nevadí, protože pak samotný program po nainstalování lze přepnout do české lokalizace. Po uvítací stránce pak v jednotlivých krocích musíme souhlasit s licenčními podmínkami, nastavit cílový adresář a potvrdit úspěšnost instalace. Tento produkt jako jediný nevyžadoval restart systému, program se okamžitě spustil.

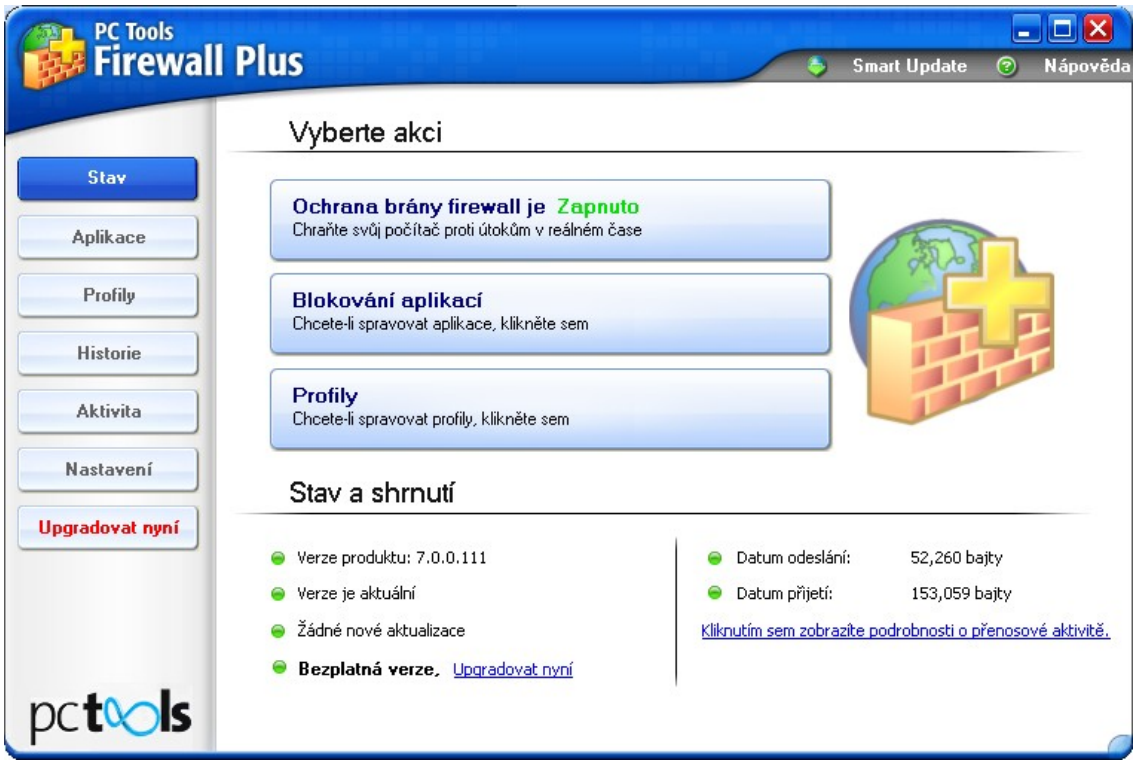
6.3.3 První spuštění

Hned po instalaci a spuštění firewallu bez nutnosti restartování systému jsme upozorněni na detekci nové sítě (Obrázek 21), kde můžeme zvolit důvěryhodná, nebo nedůvěryhodná síť. Tuto volbu je také možné kdykoliv dodatečně změnit v nastavení firewallu.

Obrázek 21 - Volba důvěryhodnosti sítě; zdroj vlastní

6.3.4 Popis nastavení a vzhledu

Činnost firewallu je signalizována ikonou v oznamovací oblasti (task bar). Grafické uživatelské rozhraní je tvořeno centrálním oknem s hlavní nabídkou na levé straně (Obrázek 22). Některé nabídky mají pak ještě dostupné podrobnější nastavení v záložkách centrálního okna. V horní liště jsou umístěné dva odkazy *Smart Update* pro aktualizaci programu a *Nápovědu*, která odkazuje na domovskou stránku PC Tools.



Obrázek 22 - Vzhled programu; zdroj vlastní

Nabídka *Stav* nás informuje o stavu firewallu, jeho aktualizaci a objemu přijatých a odeslaných dat. Tlačítka *Blokování aplikací* a *Profily* fungují jako stejnojmenné nabídky v levé části.

Nabídka *Aplikace* slouží pro správu aplikací, které mají povolen přístup k síti. U každé aplikace lze nastavit, jak se má firewall chovat v případě příchozí nebo odchozí komunikaci, popřípadě zda se mají události zapisovat do historie.

Nabídka *Profily* spravuje jednotlivé profily, kde můžeme nastavovat pokročilá pravidla síťového provozu. Záložka *Seznam důvěryhodných IP adres* obsahuje definice IP adres, které jsou (resp. mohou) být považovány za důvěryhodné a kterým je umožněný přístup s menšími restrikcemi k vašemu počítači podle definic v nabídkách *Profily* a *Aplikace*.

Nabídka *Historie* uchovává historii přenosů v síti a činnosti firewallu. A to těch, pro které je v nabídce *Profily* a *Aplikace* určené, aby byly v tomto seznamu zobrazeny a logovány.

Nabídka *Aktivita* zobrazí aktuální přenosy v síti a činnosti firewallu. Je možné zobrazit i detailnější údaje typu ID přenosu, umístění souboru, souhrn přijatých a odeslaných paketů a bajtů.

Nabídka *Nastavení* umožňuje nakonfigurovat různá nastavení brány firewall. Pomocí záložky *Obecné* se konfigurují možnosti ikony v oznamovací oblasti (výzvy k potvrzení, informace o přenosech a automatické povolení známých aplikací). Záložka *Sítě* umožňuje nastavit důvěryhodnou nebo nedůvěryhodnou síť, ke které je počítač aktuálně připojen. Záložka *Filtrování* umožňuje nakonfigurovat možnosti filtrování a pokročilé vlastnosti paketů. Záložka *Heslo* umožňuje chránit firewall před změnou nastavení nebo vypnutím samotného firewallu. Záložka Celá obrazovka umožňuje uživateli, pokud běží nějaká aplikace v režimu *Full screen*, aby nebyl rušený dotazy firewallu. Záložka *Předvolby* nastavuje možnost aktualizace a jazyk programu.

Nabídka *Upgradovat nyní* odkazuje na domovskou stránku PC Tools do nákupní sekce.

6.3.5 Průběh při testování

PC Tools Firewall sleduje a vyhodnocuje jednak síťový provoz počítače a jednak chování programů, které se pokoušejí o síťovou komunikaci. Při vyhodnocování se řídí přednastavenou sadou pravidel. Jestliže zjistí neznámou nebo podezřelou situaci, vyjede nad oznamovací oblastí upozornění s popisem situace a s dotazem, co má udělat. Upozornění obsahuje údaje o programu vykonávajícím akci, popis činnosti, o jakou se

program pokouší a dotaz, jak se má firewall zachovat. Pak je na rozhodnutí uživatele, jakou odpověď dá. Akci lze povolit, anebo zakázat. Pak je možné ještě firewallu určit, zda si má tuto odpověď pamatovat, čili vytvořit si pro ni aplikační pravidlo. Upozornění s modrým zbarvením se týkají síťové komunikace, upozornění se žlutým zbarvením (Obrázek 23) se týkají možného podezřelého chování aplikace uvnitř systému.

Obrázek 23 - Upozornění na chování aplikace; zdroj vlastní

6.3.6 Hodnocení

Program byl testován ve výchozím nastavení, kdy chrání před běžnými útoky a umožní normální provoz. Úspěšnost tohoto programu v testování je zobrazena v tabulce (Tabulka 5), kde jsou porovnány výsledky všech testovaných osobních firewallů. Odinstalování programu proběhlo v pořádku.

6.4 Sunbelt Personal Firewall

Pro testovací účely jsem použil Sunbelt Personal Firewall, verze 4.6.1861 vydaná roku 2008. Sunbelt Personal Firewall je na 30 dní poskytován v plné verzi, poté se přepne do freeware verze pro domácí použití.

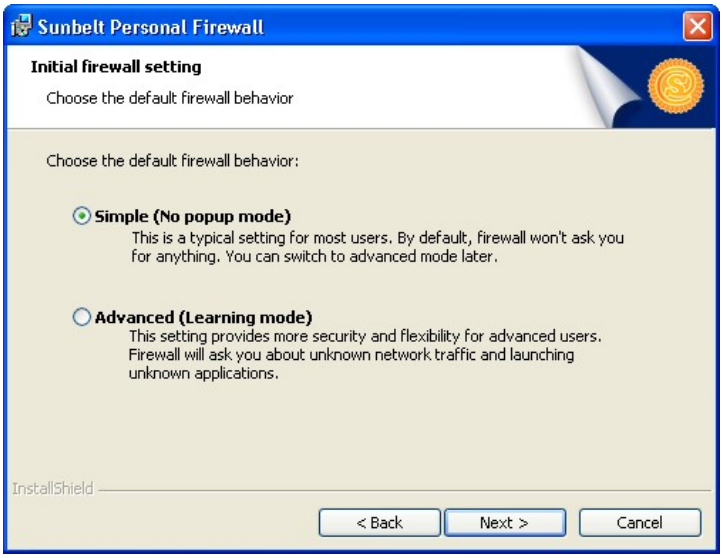
6.4.1 O produktu

Společnost Sunbelt Software (http://www.sunbeltsoftware.com/) byla předním poskytovatelem bezpečnostního software pro OS Windows, včetně antivirů, antispyware a nástrojů pro bezpečnost a analýzu malware . V polovině roku 2010 společnost Sunbelt Software koupila společnost GFI Software, která nabízí jednotný zdroj řešení webové

a emailové bezpečnosti, archivace, faxování a zabezpečení sítě pro malé a středně velké firmy prostřednictvím rozsáhlé globální partnerské komunity. Sunbelt Personal Firewall je pokračovatel jednoho z nejoblíbenějších firewallů pro operační systémy Windows Kerio Personal Firewall a můžeme si ho pořídit jako freeware s osekanými funkcemi, nebo si můžeme zaplatit full verzi. Předností plné verze je především vzdálená správa, systémový log, zaheslování nastavení či blokování skriptů. Freeware verze však umí vše potřebné pro ochranu počítače a filtrování dat.

6.4.2 Instalace

Vlastní instalace je bezproblémová, řešená grafickým průvodcem v anglickém jazyce. Po první uvítací obrazovce musíme odsouhlasit licenční podmínky a poté zvolit cílový adresář instalace. Na další obrazovce musíme zvolit, v jakém módu se má program nainstalovat (Obrázek 24). Výběr z jedné možností lze později změnit i v samotném programu.



Obrázek 24 - Volba módu instalace; zdroj vlastní

Pokud zvolíme *Simple* (jednoduchý mód), tak se program na nic neptá, vše nastavuje automaticky (je tedy určený především pro začátečníky a méně zkušené uživatele).

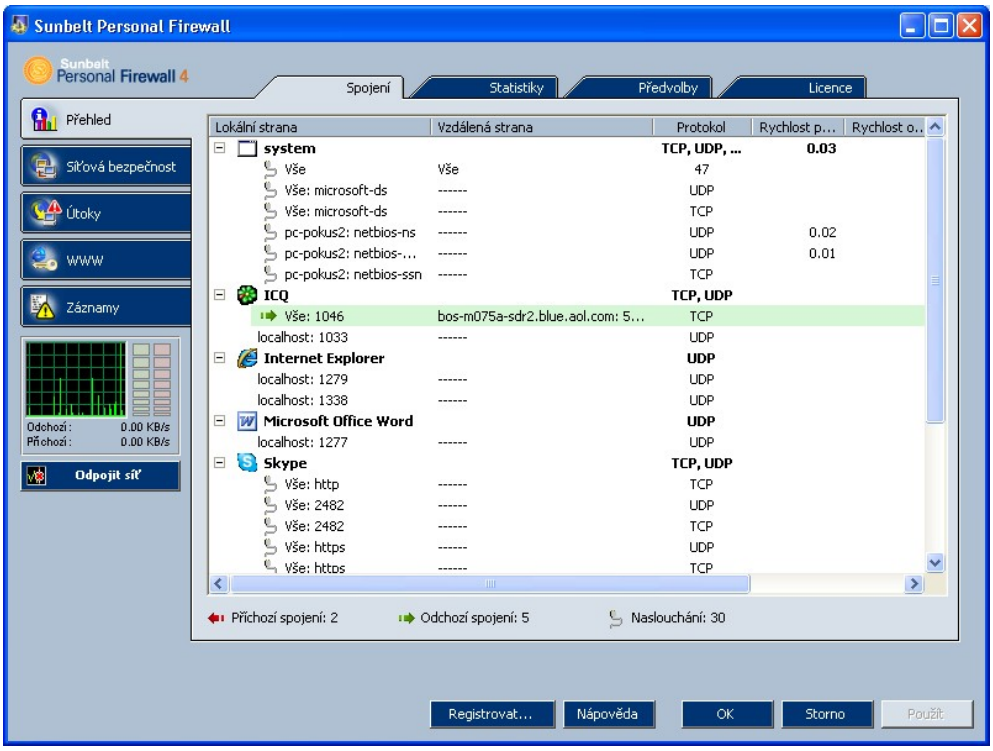
V druhém případě *Advanced* (pokročilý mód) musíme odpovídat na celou řadu dotazů ohledně nastavení počítače, povolení či zamítnutí aplikací (je tedy určen pro zkušené uživatele). V následujících krocích průvodce je pak už jen samotná instalace, oznámení o úspěšné instalaci a výzva k restartu počítače.

6.4.3 První spuštění

Pokud jsme zvolili jednoduchý mód instalace, tak se po restartu firewall vůbec na nic neptá. V druhém případě musíme odpovídat na celou řadu dotazů týkající se síťové komunikace.

6.4.4 Popis nastavení a vzhledu

Ačkoli instalace probíhala v anglickém jazyce, samotný program je už s podporou českého jazyka. Grafické uživatelské rozhraní je tvořeno s centrálním oknem s hlavní nabídkou na levé straně (Obrázek 25). Každá nabídka má dostupné podrobnější nastavení v záložkách nad centrálním oknem.



Obrázek 25 - Vzhled programu; zdroj vlastní

Nabídka *Přehled* v záložce *Spojení* zobrazuje seznam procesů se síťovou aktivitou naslouchající na některém z portů. Dále jsou v této tabulce informace o přenosovém protokolu a příchozí i odchozí rychlosti spojení. V záložce *Statistiky* jsou shrnuty souhrnné informace o blokování všech událostí, které firewall detekoval. V záložce *Předvolby* je samotné nastavení programu jako automatická aktualizace, import a export nastavení, ochrana heslem, vzdálená správa nebo výběr jazyka. Záložka *Licence* zobrazuje informaci o licenci.

Nabídka *Síťová bezpečnost* konfiguruje základní nastavení firewallu. Zde můžeme určit, jakým procesům bude firewall povolovat připojení. Záložka *Aplikace* zobrazuje seznam dříve rozpoznaných aplikací s přiřazenými pravidly pro příchozí a odchozí komunikaci v důvěryhodné síti a v internetu. U jednotlivých pravidel můžeme volit „povolit“, „ptát se“ a „zakázat“. Detailnější nastavení aplikací se provádí pomocí paketového filtru. V záložce *Předdefinované* jsou nastaveny obecná pravidla pro síťový provoz v internetové i důvěryhodné zóně. V záložce *Důvěryhodné* lze definovat důvěryhodné sítě a na záložce *Pokročilé* povolit, nebo zakázat ochranu během startu systému a režim internetové brány.

Nabídka *Útoky* povoluje, nebo zakazuje NIPS (systém prevence síťových útoků), HIPS (systém prevence útoků na hostitelský operační systém) a blokování aplikací.

Nabídka *WWW* zabezpečuje filtrování obsahu www stránek. Zde můžeme nastavit blokování reklam, soukromí a nadefinovat výjimky.

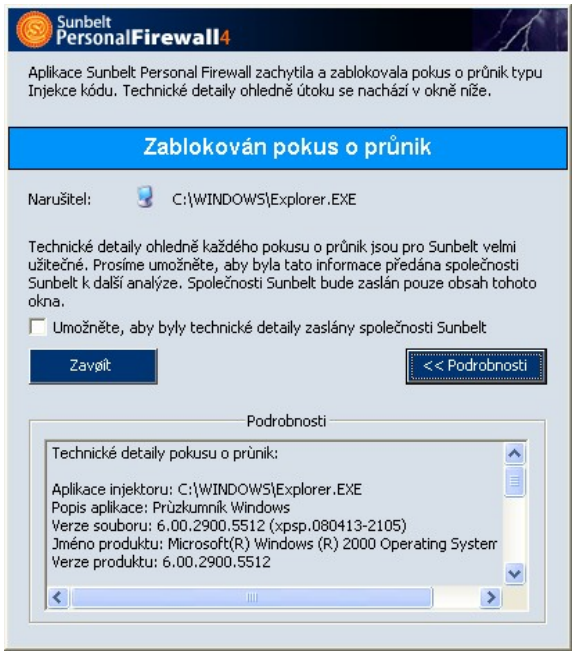
Nabídka *Záznamy* ukládá historii, díky které můžeme analyzovat možné útoky. Zaznamenávání můžeme vypnout, nebo povolit a nastavit velikost výstupního souboru. Je zde i možnost odeslat výpis na vzdálený server společnosti Sunbelt.

6.4.5 Průběh při testování

Během práce na počítači firewall upozorňuje uživatele na jednotlivé události pomocí vyskakujících oken (Obrázek 26). Pomocí voleb pak můžeme akci povolit, nebo zakázat.

Obrázek 26 - Upozornění firewallu; zdroj vlastní

Firewall nás také může jen informovat o nějaké činnosti, kterou provedl (Obrázek 27).



Obrázek 27 - Oznámení události; zdroj vlastní

6.4.6 Hodnocení

Osobní firewall blokuje příchozí a odchozí podezřelý provoz, z hlediska práce je pak ovládání příjemné, snadné a intuitivní. Program byl testován v nastavení *Simple* se zapnutou funkcí blokování chování aplikací (jedná se o spuštění aplikace aplikací či spuštění aplikace po její modifikaci). Úspěšnost tohoto programu v testování je zobrazena v tabulce (Tabulka 5), kde jsou porovnány výsledky všech testovaných osobních firewallů. Odinstalování programu proběhlo v pořádku.

6.5 ZoneAlarm Free

Pro testovací účely jsem použil ZoneAlarm Free, verze 9.2.102.000 vydaná 3. 9. 2010, je poskytována zcela zdarma.

6.5.1 O produktu

Společnost ZoneLabs (http://www.zonealarm.com/) vyvíjí řadu bezpečnostních řešení jak pro komerční použití, tak pro soukromé. Produkty jsou zaměřené na firewallovou, virovou, spywarovou ochranu a komunikační bezpečnost. ZoneAlarm Free je velmi jednoduchý softwarový firewall spíše pro méně zkušené uživatele. Hlavním posláním programu je ale zcela zjevně seznámit veřejnost s ostatními produkty a celkovou bezpečnostní nabídkou

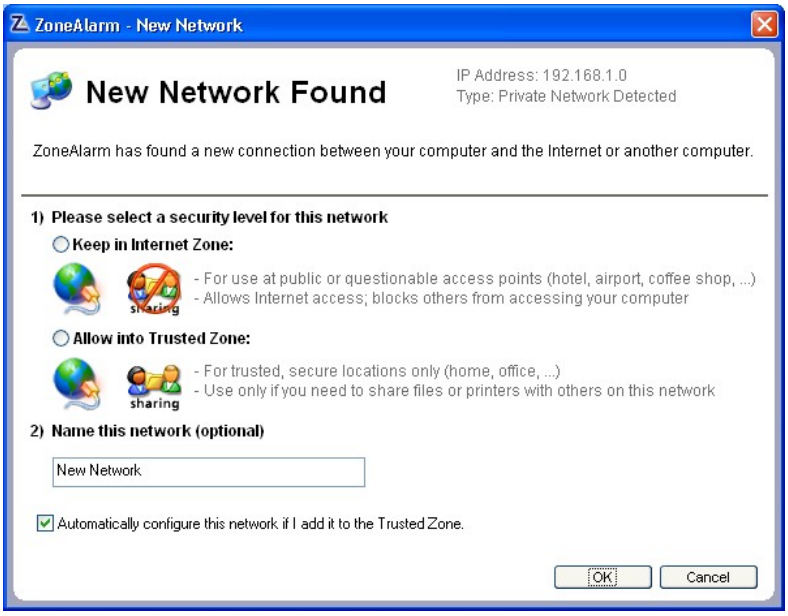
společnosti. Uživatel si sám může určit, který program má mít přístup k Internetu a který ne. V placené verzi Pro navíc dokáže sledovat přijímané emaily a vyhledat nebezpečné přílohy, pracovat s Cookies, vyhledat zdroj útoku, obsahuje Anti-Spyware atd.

6.5.2 Instalace

Vlastní instalace je bezproblémová, řešená grafickým průvodcem v anglickém jazyce. Na první uvítací obrazovce můžeme zvolit, zda instalace proběhne zcela automaticky nebo s dotazy s upřesněním, zda se má instalovat Security Toolbar, nastavit domovská stránka a umístit ikona na ploše. V dalších obrazovkách průvodce probíhá nepovinná registrace, odsouhlasení licence, volba automatického, nebo ručního nastavení samotného programu, skenování systému a nakonec požadavek na restart systému.

6.5.3 První spuštění

Při prvním spuštění firewall automaticky detekuje novou síť a dotazuje se ohledně úrovně bezpečnosti sítě, ke které jsme připojeni (Obrázek 28).

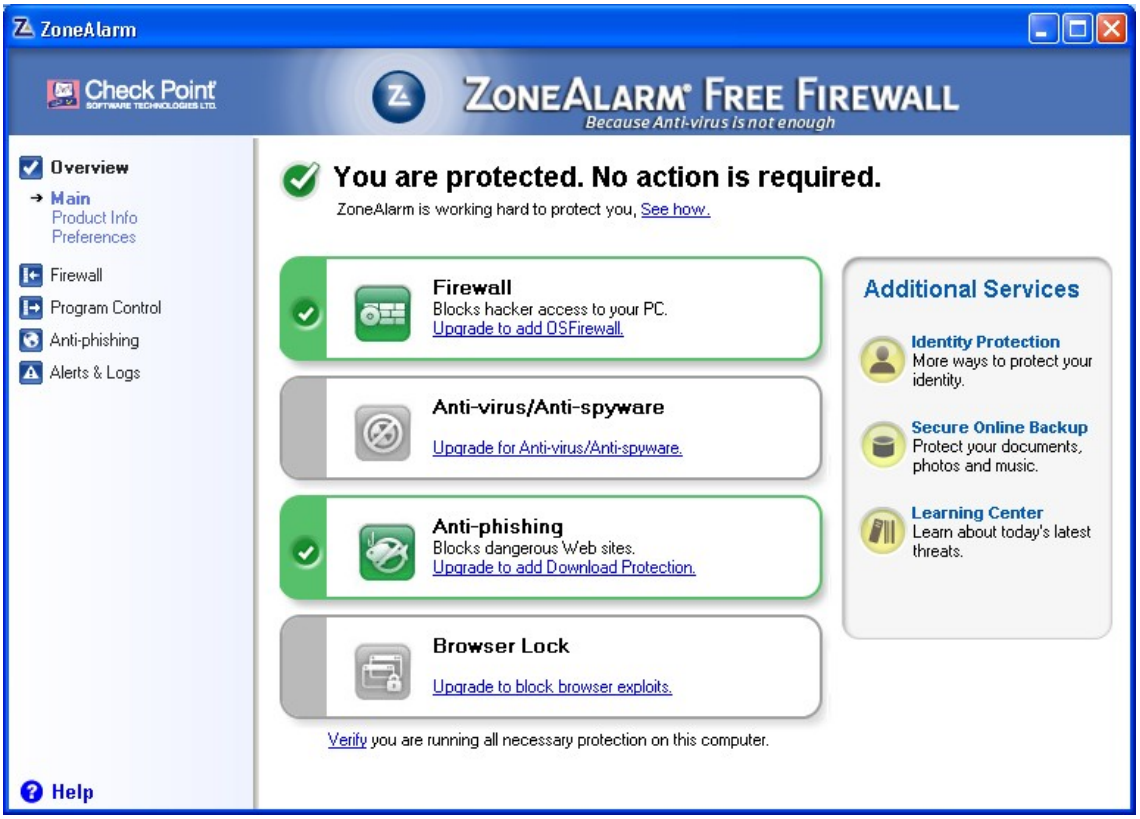


Obrázek 28 - Detekce nové sítě; zdroj vlastní

Při zvolení automatického nastavení ochrany program zasáhne do co největšího množství položek a připojení. Je tedy třeba začít postupně povolovat jednotlivé pokusy o spojení, kdy se u ikonky aplikace v systémové liště ukáže vyskakovací okno s informací o probíhajícím úsilí nějakého programu o připojení k internetu. Zde se pak rozhodujeme, zda přístup povolíme, nebo blokujeme.

6.5.4 Popis nastavení a vzhledu

V hlavním okně programu (Obrázek 29), kde dochází ke spuštění všech funkcí a nastavení, toho na výběr moc není. Vybledlé funkce v okně náleží funkcím, nástrojům a aplikacím, které si již musíme od autorů zakoupit (povýšit na verzi Pro). Nabízeny jsou antivirus a ochrana při surfování po webu. Zdarma je tedy pouze Firewall a Anti-phising (blokování nebezpečných stránek).



Obrázek 29 - Vzhled programu; zdroj vlastní

Grafické uživatelské rozhraní je tvořeno s centrálním oknem s hlavní nabídkou na levé straně.

Nabídka *Overview* informuje o spuštěných službách, informaci o instalovaných verzích a upřesňuje další nastavení jako aktualizace a spuštění programu hned po startu systému.

Nabídka *Firewall* umožňuje nastavit citlivost a chování firewallové ochrany. Zde můžeme pomocí jezdců nastavit úroveň zabezpečení zvlášť pro zónu internetu a důvěryhodnou zónu (např. vnitřní síť).

Nabídka *Program Control* umožňuje nastavit chování samotného programu a chování SmartDefense Advisor (rádce). V rozšířené volbě nastavení chování samotného programu můžeme pro každý program požadující připojení samostatně nastavit, jaké spojení má být

povoleno a které blokováno. SmartDefense Advisor je původně nastaven na automatický režim, sám tak tedy rozhoduje o povolení, či blokování programu. V manuálním režimu musí uživatel sám vyhodnocovat situace podle jeho doporučení.

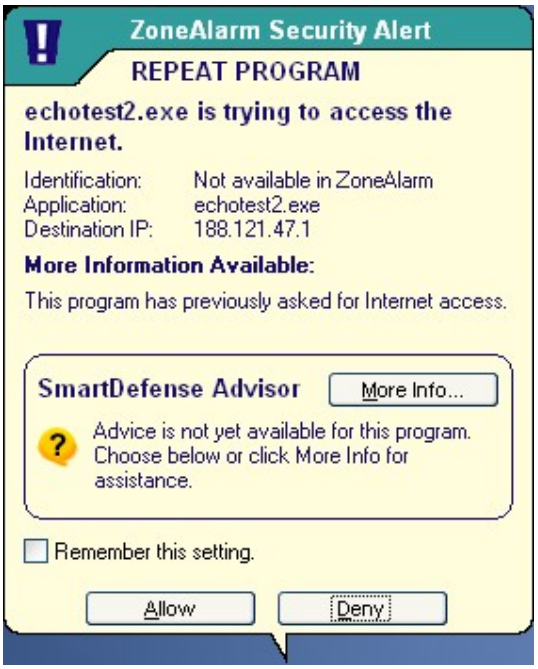
Nabídka *Anti-phising* umožňuje pouze zapnutí, či vypnutí této funkce a jeho drobné nastavení.

Nabídka *Alerts & Logs* zobrazuje historii akcí a upozornění firewallového provozu.

Firewall lze přes kontextové menu ze systémové lišty uvést i do tzv. herního módu a nastavit jej tak, aby povolil nebo blokoval veškerou komunikaci bez upozorňování.

6.5.5 Průběh při testování

Během práce na počítači firewall upozorňuje uživatele na jednotlivé události pomocí vyskakujících oken (Obrázek 30), kde buď vytváříme pravidla pro programovou, nebo firewallovou ochranu.



Obrázek 30 - Událost firewallu; zdroj vlastní

V pop-up oknech se zobrazuje název spuštěného souboru, jeho činnost, IP adresa cíle a informace o této události. Podle zobrazených informací se pak můžeme rozhodnout, zda akci povolíme, nebo zamítneme a zatržením volby *Remember* nastavíme, aby si odpověď pro tuto akci napříště pamatoval.

6.5.6 Hodnocení

Jeho ovládání je velice jednoduché, ale jako kompletní bezpečnostní nástroj je jednoduše značně osekaný. Instalace programu proběhla v automatickém režimu. Úspěšnost tohoto programu v testování je zobrazena v tabulce (Tabulka 5), kde jsou porovnány výsledky všech testovaných osobních firewallů. Pro bezproblémové odinstalování je potřeba program nejdříve deaktivovat. Ale i tak nechá na ploše a v nabídce start svoje již nefunkční zástupce.

6.6 Systémové nároky a kompatibilita jednotlivých produktů

Vzhledem k tomu, že dnešní hardwarové vybavení osobních počítačů je na vysoké úrovni, neboť disponují procesory s několika jádry či novějšími technologiemi, s velkou operační pamětí v jednotkách GHz a pevnými disky o velikosti několika stovek GB, jsou systémové nároky těchto produktů zanedbatelné, mnozí výrobci je na svých webových stránkách ani neuvádějí. V následující tabulce (Tabulka 4) alespoň uvádím jejich kompatibilitu s operačními systémy a pak skutečně naměřené hodnoty využití systémových prostředků během testování, jako je průměrná spotřeba operační paměti a skutečné zabrané místo na pevném disku. Maximální využití CPU všech produktů během testování nepřekročilo 5%.

Tabulka 4 - Kompatibilita a využití systémových prostředků; zdroj vlastní

software	Comodo Firewall	Online Armor free	PC Tools Firewall Plus	Sunbelt Personal Firewall	ZoneAlarm Free
Podporované 32-bit systémy	Win 7, Vista, XP SP2	Win 7, Vista SP2, XP SP3	Win 7, Vista, XP	Win 7, Vista, XP , Win 2000	Win 7, Vista, XP
Podporované 64-bit systémy	Win 7, Vista, XP SP2	Win 7	Win 7, Vista	nepodporuje	Win 7, Vista
Místo na HDD [MB]	95	55	26	16	19
Průměrná spotřeba paměti [MB]	12	16	23	20	13

6.7 Porovnání výsledků

Výsledky testování osobních firewallů jsou uvedeny v tabulce (Tabulka 5). Některé firewally si vedly v testech lépe, některé hůře. Všechny firewally byly testované v automatickém nastavení od výrobce. Některé produkty nabízely jen samotný firewall, některé měly integrované přídavné funkce týkající se vylepšené bezpečnosti. S určitostí lze tvrdit, že firewally disponující pokročilejšími funkcemi jako NIPS (systém prevence síťových útoků), HIPS (systém prevence útoků na hostitelský operační systém) a především blokování chování aplikací (jedná se o spuštění aplikace aplikací či spuštění aplikace po její modifikaci) si vedly v testech mnohem lépe. Pokud firewall během leak testů zareagoval s dotazem na povolení, či zakázání činnosti, odpovídal jsem zakázat.

Hodnocení výsledku testu, které je v tabulce použito, má následující význam:

PASSED Firewall úspěšně zablokoval daný leak-test.

FAILED Firewallu se nepodařilo daný leak-test zablokovat.

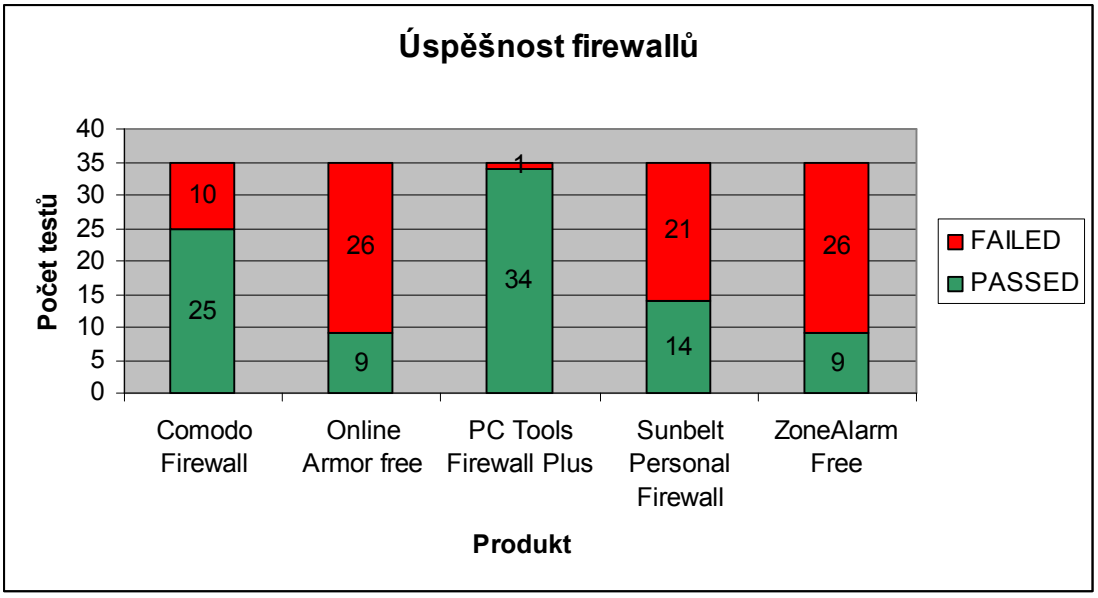
U každého firewallu je pak také vypočítána procentuální úspěšnost zablokování leak-testů. Na první pozici s úspěšností 97% zachycených útoků se umístil PC Tools Firewall Plus. Výsledky testovaných osobních firewallů byly určitě překvapující a myslím si, že při pokročilejším nastavení s důrazem na maximální bezpečnost by se výsledky testů u všech produktů změnily k lepšímu výsledku.

Tabulka 5 - Úspěšnost jednotlivých firewallů při leak testech; zdroj vlastní

software / test	Comodo Firewall	Online Armor Free	PC Tools Firewall Plus	Sunbelt Personal Firewall	ZoneAlarm Free
awft1	PASSED	FAILED	PASSED	PASSED	FAILED
awft3	PASSED	FAILED	PASSED	FAILED	FAILED
awft4	PASSED	FAILED	PASSED	PASSED	FAILED
bitstest	PASSED	PASSED	PASSED	PASSED	PASSED
breakout1	PASSED	FAILED	PASSED	FAILED	FAILED
coat	FAILED	FAILED	PASSED	FAILED	PASSED
copycat	PASSED	FAILED	PASSED	FAILED	PASSED
cpil	PASSED	FAILED	PASSED	FAILED	FAILED
cpilsuite1	PASSED	FAILED	PASSED	FAILED	FAILED
cpilsuite2	PASSED	PASSED	PASSED	FAILED	FAILED
cpilsuite3	PASSED	FAILED	PASSED	FAILED	PASSED
ddetest	FAILED	FAILED	PASSED	FAILED	FAILED
dnstest	FAILED	FAILED	PASSED	PASSED	FAILED
dnstester	FAILED	FAILED	PASSED	FAILED	FAILED
echotest	PASSED	FAILED	PASSED	FAILED	PASSED
echotest2	PASSED	FAILED	PASSED	FAILED	PASSED
firehole	PASSED	FAILED	PASSED	FAILED	FAILED
firehole2	PASSED	FAILED	PASSED	FAILED	FAILED
flank	PASSED	FAILED	PASSED	PASSED	FAILED
jumper	PASSED	PASSED	PASSED	FAILED	FAILED
leaktest	PASSED	FAILED	PASSED	FAILED	PASSED
newclass	PASSED	PASSED	PASSED	FAILED	FAILED
osfwbypass	FAILED	FAILED	FAILED	FAILED	FAILED
runner	PASSED	PASSED	PASSED	PASSED	FAILED
runner2	PASSED	PASSED	PASSED	PASSED	PASSED
schedtest	PASSED	FAILED	PASSED	FAILED	FAILED
schedtest2	PASSED	FAILED	PASSED	FAILED	FAILED
thermite	PASSED	FAILED	PASSED	FAILED	FAILED
tooleaky	FAILED	PASSED	PASSED	PASSED	FAILED
vbstest	FAILED	PASSED	PASSED	PASSED	FAILED
wallbreaker1	FAILED	FAILED	PASSED	PASSED	FAILED
wallbreaker2	FAILED	FAILED	PASSED	PASSED	FAILED
wallbreaker3	FAILED	FAILED	PASSED	PASSED	FAILED
wallbreaker4	PASSED	FAILED	PASSED	PASSED	FAILED
yalta	PASSED	PASSED	PASSED	PASSED	PASSED
úspěšnost	**71%**	**26%**	**97%**	**40%**	**26%**

7 Závěr

Ve své diplomové práci jsem se zabýval bezpečností počítačových sítí. V teoretické části jsme se seznámili se základy bezpečnosti a vysvětlili si, že skutečná bezpečnost se nedá koupit jen v jednom produktu, ale že je to celá řada funkcí a procesů. Základní princip zabezpečení spočívá tedy ve vrstvené bezpečnosti, která obsahuje nejen účinný firewall, antivirus, antispam, detekci narušení, ale také aktualizaci systémů, monitorování a především poučení uživatelů. V praktické části jsme si pak otestovali několik osobních firewallů. Při těchto testech jsme si ověřili, že při výběru softwaru pro zabezpečení počítače je potřeba doopravdy brát ohledy na kvalitu, jinak se vystavujeme velkému bezpečnostnímu riziku. Na následujícím grafu (Obrázek 31) je vidět úspěšnost jednotlivých osobních firewallů, jak se jim dařilo dané leak testy blokovat. U každého produktu je znázorněn počet úspěšně zablokovaných i neúspěšných testů.



Obrázek 31 - Úspěšnost osobních firewallů při testování; zdroj vlastní

Ačkoli jsme otestovali pět firewallů zdarma, jen PC Tools Firewall Plus a Comodo Firewall obstály v testování dobře. Na první pozici s úspěšností 97% zachycených útoků se umístil PC Tools Firewall Plus. Pokud bych měl osobně doporučit osobní firewall , byl by to určitě PC Tools Firewall Plus. Kromě vynikající úspěšnosti v leak testech je určitě pro mnohé domácí uživatele výhodou i podpora českého jazyka a možnost detailního nastavení funkce firewallu.

Z popisu dnešních funkcí firewallů je zřejmé, že se výrobci těchto zařízení snaží získat své zákazníky buď integrovaným, nebo specifickým řešením. Integrované řešení označované jako UTM (Unified Threat Management) zahrnuje základní i rozšířené funkce v jednom zařízení. Tato zařízení jsou rozšířena o dodatečné funkce poskytující autentizaci, VoIP brány, VPN, IDS/IPS, antivirovou a antispamovou kontrolu nad přenášenými daty, filtrování webových stránek od nežádoucího obsahu, monitorování síťových prvků a koncových stanic. Výhodou integrovaných řešení je eliminace duplicitních bezpečnostních funkcí a s nimi spojených nároků na administraci. Výrobci specifických řešení se naopak specializují na kontrolu jednotlivých aplikací na aplikačních serverech, jako je e-bankovnictví, sociální sítě, poskytování multimediálních dat a dalších webových služeb.

Do budoucna lze očekávat, že pokročilé bezpečnostní funkce, které byly doposud dostupné pouze velkým společnostem, se rozšíří také mezi jednotlivce a domácnosti. Aby výrobci těchto bezpečnostních zařízení získali náskok před konkurencí, budou se snažit implementovat další nové funkce, např. podporu mobilních zařízení a. kompletní podporu protokolu IPv6, ten je v současnosti podporován u některých výrobců pouze částečně.

Jsem rád, že jsem mohl vypracovat diplomovou práci na téma *Síťová bezpečnost*, protože rozšířila mé znalosti, jak po stránce teoretické, tak pro stránce praktické, které mohu dále aplikovat v práci jako správce počítačové sítě.

8 Seznam použitých zdrojů

Použitá literatura:

[1] NORTHCUTT, Stephen a kol. *Bezpečnost počítačových sítí*. 1. vyd. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

[2] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[3] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce*. 1. vyd. Brno: Computer Press, 2003. 472 s. ISBN 80-7226-983-6.

[4] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. 1. vyd. Brno: Computer Press, 2004. 990 s. ISBN 80-251-0178-9

[5] ENDORF, Car, SCHULTZ, Ebene, MELLANDER, Jim. *Hacking detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada Publishing, 2005. 356 s. ISBN 80-247-1035-8.

[6] KUCHAŘ, Miloš. *Bezpečná síť: Jak zajistíte bezpečnost vaší sítě.* 1. vyd. Praha: Grada, 1999. 91 s. ISBN 80-7169-886-5

[7] SCAMBRAY, Joel, McCLURE, Stuart, KURTZ, George. *Hacking bez tajemství.* 2. vyd. Brno: Computer Press, 2002. 646 s. ISBN 80-7226-644-6

[8] BOTT, Ed, SIECHERT, Carl. *Mistrovství v zabezpečení Microsoft Windows 2000 a XP*. 1. vyd. Brno: Computer Press, 2004. 696 s. ISBN 80-722-6878-3

Elektronické zdroje:

[9] *SANS Internet Storm Center* [online]. 2011 [cit. 2011-03-18]. Survival Time. Dostupné z WWW: <http://isc.sans.edu/survivaltime.html>.

[10] PETERKA, Jiří. *E-archiv Jiřího Peterky* [online]. 2011 [cit. 2011-03-14]. Rodina protokolů TCP/IP Verze 2.7. Dostupné z WWW: <http://www.earchiv.cz/l223/index.php3>.

[11] HORNÍČEK, Jan. *Sociální inženýrství* [online]. 2009 [cit. 2011-03-04]. Sociální inženýrství a další metody počítačové kriminality. Dostupné z WWW: <http://www.sociotechnika.ic.cz/>.

[12] PECHO, Peter. *Lupa.cz* [online]. 2010 [cit. 2011-02-18]. Klasifikace dnešních firewallů. Dostupné z WWW: <http://www.lupa.cz/clanky/klasifikace-dnesnich-firewallu/>.
[13] PECHO, Peter. *Lupa.cz* [online]. 2010 [cit. 2011-03-14]. Použijte správný firewall pro ochranu své sítě. Dostupné z WWW: <http://www.lupa.cz/clanky/pouzijte-spravny-firewall-pro-ochranu-sve-site/>.
[14] MATOUŠEK, David. *Matousec.com* [online]. 2011 [cit. 2011-03-01]. Proactive Security Challenge. Dostupné z WWW: <http://www.matousec.com/projects/proactive-security-challenge/>.
[15] *Kerio.cz* [online]. 2011 [cit. 2011-03-18]. Koupit Kerio Control. Dostupné z WWW: <http://www.kerio.cz/cz/control/buy>.

9 Seznam Příloh

Příloha P1 - Přehled nejčastěji používaných portů

Příloha P2 – Cenová nabídka firewallů od firmy Autocont

Příloha P1 - Přehled nejčastěji používaných portů

U standardních serverů jsou služby nastavené tak, aby poslouchaly na následujících portech. Jednoduché služby TCP/IP obvykle poslouchají na těchto portech:

Port	Služba TCP/IP
7	Echo
9	Discard
13	Daytime
17	Quote of the Day
19	Character generator

Internetové servery většinou poslouchají na těchto portech:

Port	Server
21	File Transfer Protocel (FTP)
23	Telnet
70	Gopher
80	World Wide Web (HTTP)
119	Net News (NNTP)
22	Secure Shell
443	Secure HTTP (HTTPS)

Souborové servery obvykle poslouchají na těchto portech:

Port	Služba
53	DNS (Domain Name Service) (služba DNS v případě, že je instalovaná)
135	RPC Locator Service (pouzr u Windows NT)
137	NetBIOS Name Service (Pouze servery Wins)
139	NetBIOS Session Service (pouze síťové servery založené na Windows a SMB/CIFS
515	LPR používá služba tisku TCP/IP v případě, že je nainstalovaná
530	RPC (Remote Procedure Call) (připojení RPC používá služba WinLogon Windows NT i mnoho dalších jiných náročnějších síťových aplikací)
3389	Na tomto portu přijímá připojení Windows Terminal Services pomocí protokolu RDP

Poštovní servery jsou obvykle nastaveny, aby poslouchaly na těchto portech:

Port	Poštovní server
25	SMTP (Simple Mail Transfer Protocol) (poštovní server na ústředny serverů)
110	POP (Post Office Protocol) verze 3 (server na poštovní ústředny klienta)
143	IMAP (Internet Mail Access Protocol) (přístup klienta na poštovní server)

Příloha P2 – Cenová nabídka firewallů od firmy Autocont

AutoCont CZ a.s.
Závodu míru 2738, Pardubice 53002
petr.senkerik@autocont.cz
(platnost nabídky do 31.3.2011)

Dovoluji si Vám nabídnout následující produkty:		
HW firewall:		
popis	**ks**	**cena 1ks bez DPH**
FortiGate-50B	1	12 100 Kč
FortiGate-50B nabízí kompletní zabezpečení a vysoký výkon pro pobočky, malé kanceláře / domácí kanceláře (SOHO). Jeho operační systém FortiOS obsahuje kompletní sadu bezpečnostních služeb v jedné odolné platformě: antivirus / antispyware / antimalware, detekci průniku do systému (IPS), filtrování webových stránek, stavový firewall a trafic shaping, nechybí ani IPSec / SSL VPN. Tato kombinace poskytuje vynikající ochranu proti hrozbám IM / P2P, phishingu a pharmingu. Rychlé nasazení do provozu a jednoduchá správa přináší nízké celkové náklady. Parametry FortiGate-50B: Firewall Throughput 50 Mbps IPSec VPN Throughput 48 Mbps Antivirus Throughput 19 Mbps IPS Throughput 30 Mbps Dedicated IPSec VPN Tunnels 20 Concurrent Sessions 25000 New Sessions/Second 2000 LAN Switching Interfaces 3 WAN Interfaces 2 Environmental Compliance RoHS Compliant DMF Free		
Cisco ASA5505-50-BUN-K9	1	8 500 Kč
Technické informace: Přenos dat. Aktuální rychlost datového přenosu 100 Mbit/s, VPN výkonnost-100 Mbit/s, Firewall výkonnost-150 Mbit/s Početr VPN spojení-10000 / 25000, Performance, Up to 100 Mbps 3DES & AES Performance Virtualization 10000 Concurrent Sessions, 10 IPSec VPN Peers, 3 VLANs Supported 2 SSL VPN Peers Included, 25 SSL VPN Peers Maximum, 3000 New Sessions/second 50 User, Firewall Protections Intrusion Prevention, Keylogger Protection Worm Scanning, Anti-spyware, Malware Protection, Hacker Defense Licence, 1 3DES/AES Encryption Licences, I/O Expansions Rozšiřující sloty-1 x Expansion Slot, Paměti-256MB RAM-64MB Flash Memory Software v balení-ASA 5500 Series Software v8.3 Cisco VPN Client Software (Windows, Solaris, Linux, Mac)		
FortiGate-110C	1	48 200 Kč
Maximum Firewall Throughput (512 byte UDP packets)FortiGate-110C zvedá laťku bezpečnostních zařízení, které jsou určené pro potřeby malých až středních podniků nebo větších vzdálených poboček. FortiGate-110C obsahuje FortiASIC čipy, které jsou vyvynuty pro jeden účel a tím tak dodávají zařízení vysoký výkon. Zařízení má větší hustotu portů, které umožňují vyšší flexibilitu při nasazení do provozu a lepší segmentaci celé sítě. Díky tomu je FortiGate-110C ideální jako doplněk do stávající sítě nebo jako all-in-one řešení poskytující bezpečnostní bránu s pokročilým firewallem, VPN, prevenci proti průniku do systému (IPS), webové filtrování, antivirus / antispyware / antimalware a antispam. Parametry FortiGate-110C: Maximum Firewall Throughput (1518 byte UDP packets)-1 Gbps Maximum Firewall Throughput (512 byte UDP packets)-500 Mbps Maximum IPSec VPN Throughput-100 Mbps Maximum Antivirus Throughput-65 Mbps Maximum IPS Throughput-200 Mbps Maximum Concurrent Sessions-400 000 Network Interfaces-2 Copper GigE 10/100/1000 Base-T,8 10/100 Base-T		

Cisco ASA5510-SEC-BUN-K9	1	45 400 Kč
ASA 5510 Security Plus Appliance with SW, HA, 5FE, 3DES/AES. Produktová řada:ASA Série:5500 Typ produktu:VPN/Firewall, Porty:5 x RJ-45 10/100Base-TX 2 x USB 2.0, 1 x Console Management, 1 x Auxiliary Management Přenosová rychlost::10Mbps Ethernet, 100Mbps Fast Ethernet Výkon dat:Up to 300 Mbps Firewall Throughput 170 Mbps 3DES/AES VPN Throughput, Virtualizace:32000 Concurrent Sessions 150 IPSec VPN Peers, 50 Web VPN Peers, 6000 New Sessions/second Firewall zabezpečení: Intrusion Protection Antivirus, Access Control, Worm Scanning, Virus Protection Malware Protection, VPN podpora:Scalable IPSec and SSL VPN services Remote user/site connectivity, Encryption: 3DES/AES Licence:Unlimited Users Licence, Rozšiřující sloty:1 x SSM External 1 x CompactFlash (CF) Card External, Protokoly:TCP/IP, IPSec Management:Cisco Adaptive Security Device Manager Processor:Intel Celeron 1.6GHz, Paměti:256MB DRAM 64MB Flash paměť, Software v balení:ASA 5500 Series Software Indikátor stavu:LED diody na předním panelu: Power,Status,Active,VPN,Flash LED diody na předním panelu: 2 x Power indicator,VPN,Flash, Status indicator,Active		
SW firewall:		
Kerio Control 7.1.1 - Kerio Control s integrovaným antivirem Sophos	1	6 000 Kč
(server včetně 5 uživatelů) Systém prevence útoků Firewall certifikovaný ICSA Labs Síťový firewall a aplikační brána Antivirová ochrana Filtrování obsahu WWW VPN server		
Microsoft Forefront Threat Management Gateway 2010 Std	1	31 400 Kč
ForeFront Threat Management Gateway 2010, zkráceně TMG 2010 přináší mnohé novinky. První z novinek je plná integrace do rodiny ForeFront, jakožto rodiny produktů pro zajištění bezpečnosti v organizacích. Další noviny jsou například: - URL Filtering - filtrování adres, na které uživatelé přistupují. Je možné definovat ručně, na které adresy uživatel může či nemůže přistupovat (což bylo možné i v předchozí verzi, nyní zjednodušeno), ale pomocí předplatného je TMG schopna stahovat automaticky definice nebezpečných webů, které šíří například viry nebo malware obecně a to včetně různých kategorizací stránek. - Zabezpečení emailu - ve spolupráci s Exchange serverem je TMG 2010 schopna zajistit kompletní kontrolu nad doručovanými a odesílanými emaily. - Kontrola HTTPS - TMG 2010 je schopna kontrolovat provoz, který uživatel vyžádal z internetu a probíhá po protokolu HTTPS. Zde je několik možností - ukončit HTTPS na TMG a uživateli se bude předávat HTTP nebo TMG znovu zašifruje komunikaci a uživateli se předává HTTPS nebo HTPPS kompletně zakázat. Před tím, nežli je HTTPS provoz kontrolován, je uživatel upozorněn hlášením v prohlížeči. Možná si říkáte proč kontrolovat HTTPS provoz, tvůrci škodlivého software jsou nevyzpytatelní. - Network Inspection System (NIS) - provoz, který prochází přes TMG může být skenován, zdali nejsou adresovány exploity Microsoft software - není-li veden útok na známou chybu. Pokud tomu tak je, TMG automaticky blokuje tento provoz. - Podpora 64-bit a Windows Server 2008 R2		