Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Zabezpečení sítě pomocí technologie Microsoft ISA Server

Marek Zaremba

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zabezpečení sítě pomocí technologie Microsoft ISA Server" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.3.2011 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Martinu Papíkovi PhD. za jeho vydatnou pomoc, kterou mi poskytl svými odbornými radami a cennými podněty při vypracování mojí diplomové práce. Můj vděk patří též mému zaměstnavateli, který mi poskytl prostor na vypracování a dokončení této práce.

Zabezpečení sítě pomocí technologie Microsoft ISA Server

Network security with Microsoft ISA Server technology

Souhrn

V současné době se zabezpečení interních sítí nebere na lehkou váhu, protože se jedná o velmi citlivou záležitost každé společnosti. V této práci jsem řešil zabezpečení sítě pomocí technologie Microsoft ISA server. Microsoft ISA server jsem navrhl, protože se jedná o velmi kvalitní firewallový nástroj, který pomůže ochránit interní sítě za rozumnou cenu.

V první části popisuji obecné vlastnosti firewallu, které nám pomohou pochopit, proč je toto zařízení v soušasné době tolik potřebné pro ochranu ínterní sítě organizace.

Ve druhé části se zabývám porovnáním jednotlivých vlastností firewallů a jejich cenovou hladinou. Porovnáním jednotlivých produktů zjistíme, jaké vlastnosti mají jednotlivé firewally a podle nich si můžeme vybrat ten pravý, který nám bude vyhovovat.

V poslední třetí část se týká mojeho projektu, který řeší konkrétní nasazení firewallového produktu Microsoft ISA Server u klienta naší společnosti kde stále pracuji.

Summary

The security of internal network is very important subject of this time, becuase it is very sensitive matter of every copany. In this thesis I solved security of internal network by Microsoft ISA server. Microsoft ISA server I suggested, because it is high-quality firewall, which it will prevent internal network for reasonable price.

In the first part I describe common features of firewall, which it helps us to understand, wherefore is this device so needful for security of internal network in this time.

In the second part I am dealing with comparsion of every firewalls feature and their price level. With comparison of every firewall product we can determine, which features have individual firewalls and according to them we can choose the right, that will correspond with our needs.

The last part concerns my project, that solves particular deployment of firewall produkt named Microsoft ISA Server by client of our copany where I still work for.

Klíčová slova: Síťová bezpečnost, Firewall, MS ISA Server, VPN, Konfigurace, Proxy, NAT

Keywords: Network security, Firewall, MS ISA Server, VPN, Configuration, Proxy, NAT

OBSAH

1. ÚVOD

V době, kdy vznikaly první privátní sítě, začaly vznikat i nové, velmi závažné, otázky, jak je zabezpečit před jejich zneužitím. Nejdříve byly firewally součástí základních systémů zabezpečení, které v polovině osmdesátých let zavedli významní dodavatelé výpočetní techniky, jako byli Compaq a IBM. S narůstávajícími a inteligentnějšími průniky do systémů se také musely vyvíjet i tito strážci sítí. V této době se vylepšovaly jen ty schopnější firewally a ty horší, které byly drahé, špatně konfigurovatelné se většinou už nikde neobjevovaly. V minulosti se zabezpečení řešilo relativně jednoduchým paketový filtrem, který ovšem není dostatečný.

Protože Internet začal nabízet spoustu informací, tak se k němu narychlo a přímo připojovaly i privátní sítě. V případech přímých připojení k Internetu toho mohou hackeři zneužít a získat tak cenná data z privátních sítí. V době před Internetem se hackeři mohli připojit pouze pomocí vytáčeného připojení pomocí modemu a tedy zabezpečení se mohlo snáze nastavit. V okamžiku, kdy se síť spojí s Internetem, pak se také automaticky spojí i s jakoukoliv jinou sítí, která je rovněž připojená na Internet. V síti Internet vlastně vůbec neexistuje žádné zabezpečení.

V současnosti je třeba důsledně kontrolovat nejen původ a velikost paketů, ale také zejména to, co je jejich obsahem. Postupem času bude nezbytné pečlivě ověřovat každou www stránku, která bude mít platný certifikát nebo jiný bezpečnostní prvek, který nás ujistí, že stránka je důvěryhodná. Poté bude procházení Internetu, které úzce souvisí s firewally bezpečné.

Každá privátní síť, která by chtěla být napojená na síť Internet, by si měla vypracovat projekt, který by řešil dostatečné zabezpečení své sítě ještě dříve, než

bude privátní sít napojena na síť Internet. Tento projekt by měl vypracovat člověk nebo skupina lidí, kteří budou v budoucnu danou privátní síť spravovat. Centrálním prvkem zabezpečení by měl být firewall, který by měl být dostatečně a velmi pečlivě vybrán podle zatížení, velikosti privátní sítě, ceny a podpory pro daný firewall. Firewally by měly být umístěny v uzamčených místnostech, kde zásadně budou mít přístup pouze prověřené osoby podniku nebo konkrétní osoby outsoursingové společnosti, která bude spravovat danou privátní síť.

Je velmi prospěšné a užitečné, že otázka zabezpečení privátních sítí je nyní chápána jako zcela zásadní pro jejich budoucí a bezpečný provoz.

2. CÍL PRÁCE A METODIKA

Tato bakalářská práce řeší zabezpečení sítě pomocí technologie Microsoft ISA Server 2004 v rámci jedné firmy. Nasazení Aplikaci Microsoft ISA Server 2004 jsem prováděl u klienta společnosti Total Service s.r.o. U společnosti Total Service s.r.o. pracuji jako systémový administrátor. Cílem bylo zabezpečit vnitřní podnikovou síť proti napadení z vnější sítě. Protože celá interní počítačová síť byla postavena na platformě Active Directory od společnosti Microsoft, byl záměrně vybrán produkt Microsoft ISA Server 2004, který splňoval všechny požadavky klienta. Požadavky, které klient požadoval splnit, byly:

- Jednotný přístupový bod na Internet – Proxy server
- Vytvoření souboru pravidel přístupu k veřejné sítí Internet
- Publikování potřebných služeb, tak aby byly dostupné z Internetu
- Monitoring přístupů na Internet
- Měsíční reporty přístupů na Internet

Metodika projektu byla následující:

- Konzultace s klientem, který popsal své požadavky
- Návrh řešení
- Příprava na projekt (Studijní materiály, webové články)
- Simulace instalace v předpřipraveném prostředí
- Sepsání posloupnosti bodů projektu
- Návštěva s klientem a popsání postupu celého projektu
- Instalace Microsoft ISA Server 2004
- Nastavení Microsoft ISA Server 2004
- Závěrečné otestování funkčnosti

3. POPIS FIREWALLU

V současné době se firewally používají jak k zabezpečení sítí firem, tak i vládních institucí. Další doplňkové vlastnosti firewallů nám posílají varování a upozornění o případných hrozbách. I v budoucnu budou firewally jedním z pilířů celé podnikové sítě, protože zastávají funkci centralizované bezpečnostní politiky proti průnikům do systému. Pomocí firewallů se na rozhraních privátních sítí vytvářejí kontrolní uzly zabezpečení. V těchto uzlech firewally kontrolují všechny pakety, které mezi Internetem a privatní sítí procházejí. Pakety musí splňovat nastavená pravidla firewallu, jinak je firewall zablokuje. Když je firewall správně nakonfigurován a jsou povolené pouze protokoly, které chceme propouštět, pak je síť dobře zabezpečena. Dobré firewally nám poskytují ochranu na všech vrstvách OSI modelu.

„Mezinárodní normalizační organizace (ISO – International Standarts Organization) vyvinula užitečný model pro srovnání síťových protokolů, kterému se říka OSI (Open Systéme Interconnect). V zásobníku OSI je sedm vrstev, z nichž prvních pět popisuje pět spodních vrstev sady protokolů TCP/IP. Spodní tři vrstvy těchto prvních pěti vrstev popisují, jak dochází k přenosu dat z jednoho počítače na jiný.“[1]

Do firewallů bývá většinou zapojen router poskytovale přípojení, který nám dodává spojení s Internetem. Někdy se stává, že i poskytovatel připojení poskytuje službu firewallu již ve svých zařízení, ale za tu se musí platit. Podstatou firewallu je vytvořit úzká místa mezi interními a externími sítěmi, kde veškerý provoz musí projít právě schválně úzkým místem, ve kterém je vše zkontrolováno.

[1] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 56 s.

Toto je nutná daň za bezpečnost vaší sítě. Většina levných firewallů postačuje k běžnému podnikovému použití, protože většina externího připojení je pomalá. Existuji i velmi výkonné, ale drahé firewally, které se v rychlosti vyrovnají i té rychlejší podnikové síti.

Firewally fungují na základě tří funkcí. Filtrování paketů, překládání síťových adres (NAT) a služby Proxy. Filtrování paketů povoluje nebo zamítá pakety TCP/IP protokolu od neautorizovaných uživatelů a odmítá pokusy k neautorizovaným službám. Překladač síťových adres (NAT) překládá IP adresy interních hostitelských počítačů a skryje je před útokem zvenčí. Služba Proxy, na základě požadavků interní sítě, funguje pouze na aplikační vrstvě, a tedy nehrozí ohrožení ze síťové vrstvy. Je možné mít server, který bude plnit úlohu paketového filtru a Proxy server mít na jiném serveru mimo privátní síť nebo obráceně. Obě řešení ovšem nejsou tak bezpečná jako mít obě funkce na jednom firewallu. Firewall dále provádí další dvě důležité funkce. Šifruje autentizaci a propojuje privátní sítě pomocí virtuálního tunelu, virtuální privátní sítě (VPN). Šifrovaná autentizace umožňuje uživatelům ve veřejných sítí prokázat svou totožnost a tedy poskytnout jim přístup do privátní sítě.
Propojování virtuálních privátních sítí (VPN) znamená bezpečné propojení mezi dvěma privátními sítěmi přes nezabezpečenou síť Internet. Firewally také mohou mít funkce skenování virů nebo filtrování obsahu. Filtrování virů znamená, zda datový tok neobsahuje signatury virů. Filtrování obsahu umožňuje blokovat interním uživatelům přístup k obsahu na Internetu jako je pornografie, propaganda rasismu atd.

3.1 Paketové filtry

Firewally nejdříve obsahovaly pouze jednoduché paketové filtry, které jsou a zůstávají jako hlavní funkce dnešních firewallů. Kvalitnější firewally zkoumají stav všech připojení, a kontrolují, zda jejich příznaky naznačují hackování, jako jsou falšování IP adres (IP spoofing) atd. Pokud nějaká připojení vykazují takovéto znaky, firewall je ukončí. Interní klientský počítač se může připojit k vnějším hostitelským počítačům, ale vnější hostitelské počítače nemají možnost zahajovat připojení. Pokud se interní počítač rozhodne navázat spojení TCP protokolem, pošle na IP adresu a na port veřejného serveru žádost připojení. Během toho sdělí svojí IP adresu a port na které očekává odpověď. Veřejný server tuto odpověď zašle zpět uživateli na příslušnou IP adresu a port. Tuto informaci má i firewall, který kontroluje všechen provoz a který si oba hostitelé vyměňují. Firewall poté očekává od veřejného serveru, že pošle data pouze na uvedený port. Když oba hostitelé ukončí mezi sebou komunikaci, pak i firewall si odstraní ze své stavové tabulky položku, která umožňovala posílat data zpět internímu počítači. Pokud interní počítač přestane reagovat na TCP spojení, odstraní firewall položku po skončení nastaveného časového limitu. Paketové filtry jsou pouze jednou z bezpečnostních vlastností firewallu, která nestačí k ochraně interní počítačové sítě. Je třeba nastavit další prvky, které znesnadní průnik a kombinují se servery proxy a překladači síťových adres. V současnosti existují dva druhy paketových filtrů:

- Bezstatové filtry, které používají operační systémy.
- Paketové filtry s kontrolou stavu se používají u moderních firewallů.

„Paketové filtry jsou hraniční, které posilují zabezpečení tím, že určují, zda paket na základě informací v hlavičce každého jednotlivého paketu přeposlat anebo nikoliv. Teoreticky mohou filtry tuto skutečnost určovat na základě jakékoliv části hlavičky protokolu, ale většinu filtrů lze nastavit, aby filtrovaly pouze nejužitečnější datová pole:

- *Typ protokolu*
- *Adresa IP*
- *Port TCP/IP*
- *Číslo fragmentu*
- *Informace o přímém směrování“*[2]

3.1.1 Filtrování paketů IP protokolu

Filtrování se provádí na základě informací v poli IP protokolu paketu. V poli IP protokolu se mohou vyskytovat tyto typy protokolů:

- UDP
- TCP
- ICMP
- IGMP

[2] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 129 – 130 s.

3.1.2 Filtrování IP adres

Filtrování IP adres lze provádět různými způsoby. Můžeme omezit připojení na konkrétní IP adresy hostitelských počítačů nebo do určitých sítí. Blokování konkrétních hostitelských počítačů je zbytečné, protože nemůžeme určit všechny počítače, které by mohly interní sít ohrozit. Druhá metoda se spoléhá na zablokování všech adres kromě vyjímek, které povolují konkrétním adresám přístup do určitých sítí. Toto je nejúčinnější forma zabezpečení, kterou mohou bezstavové filtry dovolit. Bezstavové filtry je třeba nastavit tak, že chrání před přímým směrováním, kdy by útočník mohl proniknout do vnitřní sítě.

3.1.3 Filtrování TCP portů

Po filtrování IP adres hostitelský počítačů ještě musíme specifikovat typ TCP portů, které budeme povolovat nebo zakazovat. Tak jako můžeme zakazovat u IP adres celé rozsahy sítí, nebo jen konkrétní počítače, můžeme takto konfigurovat i TCP porty. Pro ochranu vnitřní sítě musíme nejprve zakázat všechny TCP porty firewallu směřující do interní sítě a následně povolovat jen ty, které by měly být dostupné z externích sítí. Takto se to řeší i v praxi.

Nejpoužívanější TCP protokoly, které se povolují jsou tyto:

- HTTPS
- SMTP
- POP3
- RDP (Windows Terminal Services)

3.2 Network Address Translation - NAT

Jednou z dalších vlastností, jak efektivněji zabezpečit interní počítačovou síť je překlad síťových adres. Překlad síťových adres nám zajistí přeměnu lokálních IP adres na veřejnou IP adresu firewallu. Po této přeměně nebude schopen útočník zjistit kolik počítačů v interní počítačové síti existuje a jaké jsou jejich interní IP adresy. Překlad síťových adres funguje na síťové vrstvě. Další neméně důležitou funkcí je skutečnost, že překlad síťových adres nám umožňuje používat jakýkoliv rozsah IP adres v interní počítačové síti.

„Funkce NAT je vlastně jednoduchý server proxy. Požadavky provádí jediný hostitelský počítač jménem všech interních hostitelských počítačů, takže před veřejnou sítí skrývá jejich totožnost. NAT obsahují všechny moderní firewally. Funkce NAT se implementuje pouze na transportní vrstvě. To znamená, že informace skytá v datové části provozu TCP/IP lze zaslat na službu vyšší úrovně a tam jejich prostřednictvím napadnout její nedostatky, anebo ustavit komunikaci s trojským koněm.“[3]

3.2.1 Statické překládání

Statické překládání znamená přesměrování konkrétních portů z rozsahu veřejných IP adres do rozsahu IP adres interní počítačové sítě. Pro představu mohu tedy pomocí jedné veřejné IP adresy přesměrovat mnoho důležitých služeb http, POP, RDP, které je třeba míti dostupné mimo interní síť.

[3] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 141 s.

3.2.2 Dynamické překládání

Dalším důležitým překladem je dynamický překlad, který aktivně zaměňuje interní IP adresy za veřejné IP adresy a tím chrání interní počítače před napadením. Každý počítač v interní počítačové síti, který vytvoří připojení ven mimo interní síť, většinou do sítě Internet, musí zařízení NAT vytvořit tabulku spojení. V tabulce spojení pak je zaznamenána interní adresa počítače a port, kterým počítač chce komunikovat s vnější sítí a také cíl požadavku. Zařízení NAT vše toto zaznamená a zamění tuto interní hostitelovu IP adresu za svojí externí IP adresu a snaží se spojit s počítačem, se kterým se chtěl interní počítač spojit. Externí počítač odpoví a předá informaci zařízení NAT, které tuto informaci bezpečně předá počítači v interní síti.

„Je důležité podotknout, že zařízení NAT chrání klientské počítače pouze v tom smyslu, že neumožňuje aby se k nim připojovaly externí hostitelské počítače. V případě, že je klientský počítač sveden, aby se připojil ke škodlivému externímu hostitelskému počítači anebo v případě, že se nějakým způsobem nainstaluje na počítači, který se připojuje k určitému externímu hostitelskému počítači, trojský kůň, klient může být napaden stejně lehce, jako kdyby žádný firewall nebyl nainstalován. Proto samotný překladač síťových adres k zabezpečení nepostačuje.“[4]

[4] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 145 s.

3.2.3 Nevýhody NAT

Nevýhoda překladu síťových adres je ta, že nedokáží ochránit provoz na datové části TCP/IP spojení. Další nevýhodou překladu síťových adres je ta, že v okamžiku, kdy se administrátor počítačové sítě chce připojit na uživatelský počítač, tak jej nelze připojit ke konkrétnímu počítači. Z tohoto důvodu jsou na firewallu zabudována pravidla na přesměrování konkrétního TCP portu, které administrátor určí, na IP adresu vybraného počítače.

3.3 Virtuální privátní sítě - VPN

Virtuální privátní sítě slouží k propojení dvou fyzicky oddělených sítí pomocí Internetu. Tomuto typu připojení se někdy říká tunelové připojení, které je také součástí firewallu. Při konfiguraci virtuální privátní sítě se automaticky konfiguruje šifrovací metoda, která nám zajistí, že nikdo nemůže přenášená data zachytit v čitelné podobě. Pro propojení dvou fyzicky oddělených sítí je třeba dvou firewallů, které podporují stejný druh šifrované komunikace. Pokud by jeden ze dvou firewallů nepodporoval daný typ šifrování, tunelové připojení by se vůbec neuskutečnilo. Ve virtuální privátní síti můžeme pracovat, jako v interní počítačové síti. Můžeme tedy kopírovat soubory z jednoho počítače umístěného v jedné fyzické síti na server umístěný v druhé fyzické síti. Samozřejmě, že můžeme provádět i jiné běžné operace při práci s počítačovou sítí. VPN je velmi levný způsob, jak zvětšit interní počítačovou síť přes sít Internet.
Pokud je třeba, aby se klientský počítač vzdáleně napojil do VPN musí mít nastavené informace, které mu umožní přístup do VPN. Tyto připojovací informace většinou sděluje administrátor firewallu. Pro připojení do VPN může být použito buď speciálního software, který zajistí připojení nebo může být provedeno pomocí běžného nastavení operačního systému počítače.

Virtuální privátní sítě se také vytvářejí v případech, kdy máme pronajatou linku od ISP. ISP zde vystupuje v roli partnera, který nám pomáhá propojit a zabezpečit VPN.

3.2.3 Zapouzdření IP

Zapouzdřeni IP znamená, že paket IP obsahuje paket jiného IP. Zapouzdřením, si síťové počítače myslí, že vzdálená síť je vlastně sousedící, oddělená jedním směrovačem, přitom jsou oddělené více směrovači. Abychom se mohli spojit s vzdáleným počítačem provést zapouzdření IP.

3.2.4 Šifrování datové části

„Šifrování datové části se používá k zamlžení obsahu vložených dat, aniž by bylo nutné celý paket zapouzdřovat do jiného paketu. V tom je šifrování datové části stejné jako standardní propojování sítí IP, kromě toho, že datová část se šifruje. Šifrování datové části data zamlží, ale neutajuje informace z hlavičky, takže z nich lze zjistit podrobnosti interní síti. Šifrování datové části lze doplnit jednou z řady bezpečných šifrovacích technik, které se liší podle zvoleného řešení VPN.“[5]

[5] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 179 s.

3.4 Šifrování VPN

Šifrovaná autentizace je další nedílnou součástí firewallu. Konkrétně se pojí s vlastnosti virtuálních privátních sítí. Šifrovaní nám zajistí, že každý, kdo se chce připojit do virtuální privátní sítě, musí mít nastaven daný typ stejného šifrování, které vyžaduje firewall. Typy nejčastějších šifrovacích metod jsou PPTP(Point-tu-Point Tunneling Protocol), PPTP/SSL a L2TP (Layer-2 Tunneling Protokol) se zabezpečením IP vrstvy (IPsec). Druhá a třetí možnost je více bezpečná a tudíž se používá k zabezpečení společností a státní veřejné zprávy. Bohužel šifrovaná autentizace nám zmenšuje míru zabezpečení firewallu a je to dáno tím že, firewall musí na nějakém portu naslouchat danému typu šifrování. Další nevýhodou je to, že přístup do sítě lze získat při získání zcizeného, nalezeného počítače s potřebnými klíči. Nevýhoda je též, že zaměstnancův počítač připojený do privátní sítě se může stát cílem útoku. Šifrovaná autentizace též potřebuje řadu zkušeností a znalostí ke správné implementaci.

3.4.1 PPTP

PPTP je protokol, který vytváří šifrovanou relaci mezi dvěmi hostitelskými počítači s TCP/IP. Tento protokol byl vyvinut společností Microsoft a funguje pouze přes TCP/IP. Autentizace do VPN se provádí na základě jména a hesla mezi serverem a klientským počítačem. Šifrování autentizace se provádí na základě privátního klíče, který vychází z hodnoty „hash“ uživatelského hesla, kterou pak obohatí o náhodné číslo a tím se šifrování zesílí. Síla šifrování PPTP je 128 bitů. I když PPTP bylo vyvinuto společností Microsoft, tak vývojáři operačních systémů Unix, Linux je implementovali jako podporu pro vytvoření připojení se systém Windows.

3.4.2 PPTP/SSL

Tato verze zabezpečení VPN je bezpečnější než původní verze PPTP a implementovali ji vývojáři operačních systémů Unix, Linux. Výhoda o proti PPTP spočívá ve využití SSL protokolu, který je založen na asymetrickém šifrování dat.

3.4.3 IPSec

„IPSec je standardní sada organizace IETF pro bezpečné komunikace přes IP, která autenticitu a soukromí komunikací IP zajišťuje pomocí šifrování. IPSec má mechanizmy, kterými lze provádět:

- *Autentizaci jednotlivých paketů IP a zajištění, že nedojde k jejich úpravě.*
- *Šifrování datové části jednotlivých paketů IP a zajištění, že nedojde k jejich úpravě.*
- *Zapouzdření soketů TCP nebo UDP mezi dvěma koncovými systémy (hostitelskými počítači) v rámci zašifrovaného propojení IP (tunelu), který je ustaven mezi mezilehlými systémy (směrovači), a tím umožnění propojení virtuálních privátních sítí.“*[6]

Pro komunikaci mezi branami se doporučuje používat IPSec mezi branami, ale nepovažuje se za dobré jej používat pro komunikaci klient - server, protože sám neobsahuje autentizaci uživatele. IPSec se používá pro autentizaci mezi zařízeními.

[6] STREBE, M., PERKINS, CH. *Firewally a proxy-servery*, 190 s.

3.4.4 L2TP

L2TP je rozšířenější protokol PPTP, kdy do něj můžeme vložit jiný protokol na síťové vrstvě třeba IPX, NetBUI nebo AppleTalk. Protokol L2TP byl vyvinut speciálně pro autentizaci uživatele pro vzdálený přístup. L2TP využívá pro přenos dat protokol UDP s hodnotou 1701.

3.4.5 L2TP/IPSec

L2TP se zabezpečuje většinou šifrováním IPSec. Toto unikátní řešení spojující L2TP a IPSec vytvoří velmi dobrou autentizaci uživatele s velmi kvalitním šifrováním. Tuto volbu také doporučuje Microsoft pro vzdálený přistup uživatelů

3.5 Služba Proxy

Další neméně důležitou funkcí firewallu je služba Proxy, která může řešit další problém s připojováním na Internet a která odděluje interní počítačovou síť od Internetu. Služba Proxy funguje jako prostředník mezi uživatelem a cílovým počítačem, serverem. Překládá požadavky od uživatele na požadavky Proxy serveru, který zasílá požadavky na cílový počítač. Proxy server nemusí být nainstalován přímo na firewallu, ale může existovat samostatně. Přesto se doporučuje, aby právě služba Proxy byla implementována na firewallu. Chytřejší Proxy servery dokáží blokovat odchozí požadavky podle IP adresy nebo přihlašovacího jména uživatele. Proxy server, pokud je dobře nakonfigurován, tak propouští pouze komunikace HTTP a nikoliv TCP nebo IP.

Služba Proxy umožňuje, také zaznamenávání a upozorňování všech činností, které jí prochází. Z repotů Proxy můžeme zjistit kolik, kdo a jaké stánky navštívil a udělat si tak představu, jak často tráví uživatelé na Internetu.

3.5.1 Aplikační Proxy

Speciálním typem Proxy serveru je aplikační Proxy server. Ten je speciálně navržen pro definovaný protokol aplikace. Každý aplikační Proxy server funguje pro konkrétní aplikaci a tedy pokud chceme filtrovat HTTP, FTP provoz, musíme mít pro ně daný modul Proxy. Aplikační Proxy server analyzuje komunikaci protokolu, kde muže obsah komunikace pozměnit, nebo dokonce zakázat. Filtrování je velmi žádané z toho důvodu, že ochrání uživatele před stažením integrovaného trojského koně v podobě AktiveX doplňku. Aplikační Proxy nadále umožňuje ukládat veškeré požadavky do vyrovnávací paměti (Cache), kdy při příštím stejném požadavku dokáže aplikační Proxy vyřídit daný požadavek rychleji a tudíž dojde ke zvýšení rychlosti komunikace.

Příkladem filtrování obsahu HTTP je blokování URL. Blokování URL znamená, že administrátor zamezí prohlížení stránek, ke kterým nechceme povolit přístup. Princip blokování URL je takový, že se porovnají požadované stránky uživatele se seznamem zakázaných URL adres. Pokud se URL shoduje, daná URL se uživateli nezobrazí.

Ve shrnutí pro účinné zabezpečení Internetu, je nutné privátní síť zabezpečit pomocí firewallu. Firewall nám tedy provádí kontrolu filtrování paketů, překlad síťových adres, virtuální privátní síť a funkci Proxy.

4. POROVNÁNÍ MS ISA SERVERU A JINÝCH FIREWALLŮ

Porovnání firewalů není jednoduchá záležitost, protože se jedná o strategickou záležitost, při které musíme brát v úvahu mnoho aspektů. Hlavními aspekty jsou:

- Velikost interní sítě
- Struktura organizace
- Předpovědět, jak se bude měnit velikost interní sítě do budoucna
- Míru zabezpečení
- Cena řešení

Pokud všechny tyto aspekty budeme znát, můžeme přistoupit k porovnávání jednotlivých firewallů.

V této práci se zaměřuji na malé nebo středně velké organizace a podle toho jsem vybral podobné typy firewallů. V porovnávací tabulce funkcí firewallů dole, lze vidět jejich vzájemné porovnání.

Microsoft ISA Server 2004 Standart Edition obsahuje následující funkce:

- Firewall na aplikační vrstvě (HTTP, SMTP, FTP, PPTP atd.)
- Sítě VPN (s karanténou) protokolů IKE/IPSec, PPTP, L2TP,
- Proxy server vrstvy okruhu
- Zařízení NAT

Další funkce Microsoft ISA Serveru 2004:

- Detekce proti vniknutí
- Přemostění SSL
- Transparentnost proxy
- Reverzní proxy
- Centralizovaná podniková zpráva
- Monitoring v reálném čase
- Konfigurovatelné protokolování
- Ukládání obsahu do mezipaměti
- Vysoká dostupnost a load balancing
- Aplikační filtry výrobců třetích stran
- Silné šifrování DES, 3DES, AES
- Vysoká propustnost až 1,58 Gbps

ISA Server 2004 Standart Edition	ISA Server 2004 Enterprise Edition
Cena $ 1500	Cena $ 6000

Cisco PIX 515E obsahuje následující funkce:

- Firewall na aplikační vrstvě (pouze HTTP, FTP, SMTP)
- Sítě VPN (s karanténou) protokolů IKE/IPSec, PPTP, L2TP,
- Zařízení NAT

Další funkce Cisco PIX 515E:

- Detekce proti vniknutí
- Transparentnost proxy
- Reverzní proxy
- Centralizovaná podniková zpráva
- Monitoring v reálném čase
- Konfigurovatelné protokolování
- Vysoká dostupnost a load balancing
- Silné šifrování DES, 3DES, AES
- Propustnost až 188 Mbps

Cisco PIX 515E

Cena $ 2500

SonicWALL Pro 230 obsahuje následující funkce:

- Filtr paketů (s kontrolou stavu)
- Sítě VPN (s karanténou) protokolů IKE/IPSec, PPTP
- Zařízení NAT

Další funkce SonicWALL Pro 230:

- Detekce proti vniknutí
- Webové rozhraní
- Monitoring v reálném čase
- Konfigurovatelné protokolování
- Silné šifrování DES, 3DES, AES
- Propustnost až 190 Mbps

SonicWALL Pro 230
Cena $ 1700

Porovnávací tabulka funkcí firewallů

Název	Aplikační firewall	Paketový filtr	NAT	Proxy	VPN	Propustnost	Cena ($)
ISA Server 2004 St	*	*	*	*	*	1,58 Gbps	1500
Cisco PIX 515E	--	*	*	*	*	188 Mbps	2500
SonicWALL Pro 230	--	*	*	--	*	190 Mbps	1700

V této tabulce jsem vybral jen důležité funkce firewallu, které osobně považuji za důležité. Protože se jednalo o porovnání malých nebo středně velkých organizací doporučil bych ISA Server 2004 Standart Edition z důvodu ceny a množství podporovaných funkcí.

5. ZABEZPEČENÍ LOKÁLNÍ SÍTĚ

Konfigurace ISA serveru byla provedena na organizaci středně velkého typu, která měla tři veřejné IP adresy, jednu interní síť a kolem šedesáti počítačů. Bylo nutné znát všechny požadavky jednotlivých vedoucích pracovníků a oddělení proto, aby implementace byla úspěšná. Na základě těchto požadavků jsem vytvářel pravidla, která se s nimi ztotožňovala. Na obrázku jsem znázornil schéma sítě.

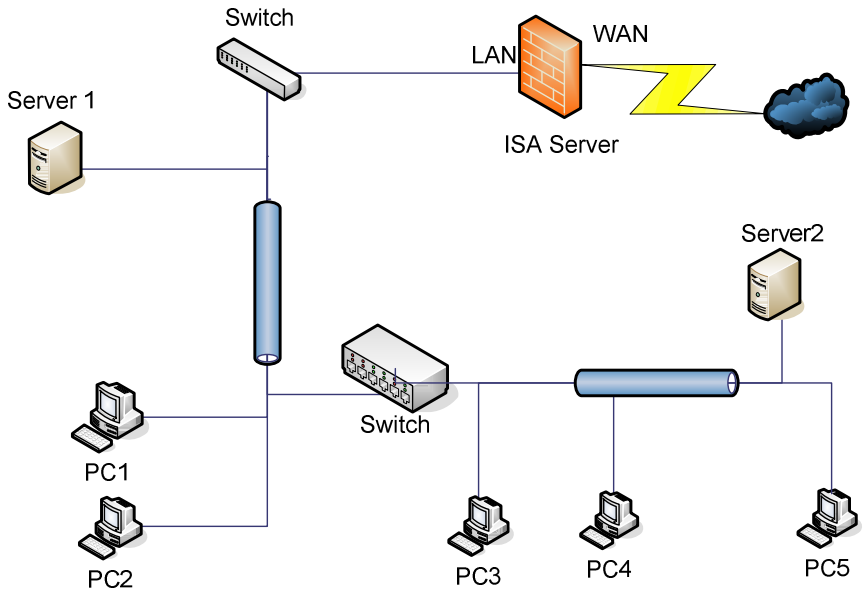


Schéma interní sítě

5.1 Popis ISA Serveru

Microsoft ISA Server je pokročilý firewall na zabezpečení interní počítačové sítě.

Microsoft ISA Server má dvě verze:

- Standart Edition
- Enterprise Edition

Standart Edition je vhodná pro menší nebo střední sítě. Enterprise Edition je vhodná pro rozlehlé, velmi zatížené sítě. Nabízí též škálovatelnost, odolnost proti chybám a centralizovanou správu.

ISA server poskytuje dvě různé vlastnosti, které organizace využívají. První vlastností je zabezpečení sítě a druhou je zrychlení přístupu k Internetu skrze akceleračních součástí ISA Serveru. Akcelerační schopností je myšleno ukládání webového obsahu do mezipaměti (Web caching).

Pro ISA server existuje mnoho filtrů obsahu od různých dodavatelů. Pomocí sady SDK si kdokoliv, kdo umí programovat, může vytvořit vlastní filtr obsahu.

„ISA server poskytuje vyšší výkon při přístupu k webu pro všechny uživatele v rámci celé organizace. Webové stránky jsou ukládány do mezipaměti obdobným způsobem, ne však na jednotlivých počítačích, ale přímo na ISA serveru. To znamená, že pokud někdo jiný již stánku, kterou chce otevřít, prohlížel před vámi, bude její kopie na ISA serveru uložena.“[7]

Filtrování na aplikační vrstvě znamená specifická pravidla pro určité aplikace. Základní filtry aplikací jsou:

- SMTP
- FTP
- HTTP

[7] SHINDER,T. W., SHINDER,T. W., GRASDAL, M. *ISA Server 2000*, 7 s.

Aplikační filtrování znamená nejenom propouštět dané protokoly třeba SMTP, HTTP, DNS, ale také nahlížet přímo do jejich obsahu protokolu. Nahlížení do obsahu protokolu je velmi důležité, protože uvnitř protokolu se může vyskytovat škodlivý kód, který by mohl interní síť zkompromitovat. Aplikační filtrování chrání před externími i interními útoky.

Díky silné Integraci svých služeb se službami VPN systémů Windows 2000 a Windows Server 2003 umožňuje ISA Server udělovat vzdálený přístup pro připojení sítí poboček a vzdálených uživatelů k firemním sítím. V zásadách VPN lze opět specifikovat druh šifrování, tak uživatelé, kteří se mohou připojit do VPN.

Při připojování do sítě VPN se nejdříve uživatel připojí do „karantény VPN“, kdy po úspěšném ověření dojde ke změně stavu na platného uživatele VPN. ISA server využívá silného ověřování uživatelů pomocí integrovaného ověřovacího mechanizmu systému Windows (Kerberos, Windows NT/LAN Manager) pro své firewall klienty, secure NAT klienty a web proxy klienty.
Secure NAT klient je počítač, který má nastavenou bránu sítě ISA server a při jeho ověřování nelze řídit přístup na základě účtu uživatelů ani skupin.
Firewall klient je klient, který se ověřuje na základě účtu uživatelů, skupin a je potřeba pro něj nainstalovat software (Firewall klient) ISA serveru.
Web proxy je posledním typem klienta ISA serveru, který se ověřuje na základě účtu uživatelů a skupin pouze pro odchozí web (TCP 80) požadavky. Klientem web proxy musí být webový prohlížeč vyhovující standardům CERN.

Další důležitou vlastností ISA serveru je zabezpečená publikace serverů. Zabezpečená publikace serverů znamená zpřístupnění interního serveru do sítě Internet. V pravidlech publikace specifikujeme, které služby se to týká (interního webového serveru, poštovního serveru, FTP serveru), jaké počítače k dané

službě by měly mít přístup a nakonec jaká skupina nebo jednotlivec se můžou na danou službu připojit.

„Pro webové servery, které požadují ověřovaný a šifrovaný přístup klientů, poskytuje ISA Server 2004 zabezpečení a filtrování na aplikační úrovni mezi koncovými body pomocí přemostění SSL-to-SSL. Na rozdíl od většiny bran firewall kontroluje ISA Server 2004 šifrovaná data, dříve než jsou přijata webovým serverem. Brána firewall dešifruje datový tok protokolu SSL, provede stavovou kontrolu a poté data znovu zašifruje a předá je publikovanému webovému serveru.“[8]

5.2 Příprava instalace

Před instalací je třeba mít rozmyšleno jaký typ firewallu budeme aplikovat při instalaci. Instalace ISA serveru není nijak složitá, přesto musíme rozumět dotazům, na které se nás bude instalační průvodce ptát. Nejtěžší práce nastane při konfiguraci ISA Serveru.

Je potřeba si připravit instalační CD s instalačním klíčem, který se nachází na obalu krabice. Jako minimální hardware k chodu ISA Serveru je třeba Intel nebo AMD procesor 550 MHz, 256 MB RAM, 150 MB HDD a příslušný počet síťových karet podle typu konfigurace. V mém případě jsem měl IBM server se dvěma procesory Intel na 3 GHz, 2 GB RAM, 200 GB HDD a 2 síťové karty. K instalaci ISA serveru bylo potřeba mít nainstalován minimálně Windows 2000 server SP4, v mém případě se však jednalo o Windows 2003 Standart server. Server, na který jsem ISA server instaloval byl členem Active Directory. Tato podmínka musí být dodržena v případě rozlehlé sítě. Instalaci jsem prováděl s účtem, který byl členem skupiny Domain Admins v Active Directory. Pokud by byla doména rozlehlá, musel bych být členem Enterprise Admins.

[8] MICROSOFT, Přehled vlastností [on-line]. [cit. 2006-9-5]. Dostupný z WWW: <http://www.microsoft.com/cze/windowsserversystem/isaserver/previousversions/2004/overview.mspx>.

5.3 Průběh instalace

Po vložení instalačního CD bylo potřeba vybrat možnost instalace ISA Serveru 2004. Dalším krokem byla nutná specifikace interní síťě, kdy jsem vybral síťovou kartu, pro kterou bude nastaven interní rozsah počítačové sítě. Na interní síťové kartě nesměly být vyplněny informace o IP adrese, bráně a serveru DNS. To ISA server vyžaduje. Ve třetím kroku jsem definoval sdílenou cestu k firewall klienta. Posledním krokem bylo dokončení instalace a zaškrtnutí volby Invoke ISA Management, který po prvním spuštění ISA Serveru spustí průvodce nastavení.

5.4 Konfigurace ISA serveru

5.4.1 Konfigurátor ISA Serveru

Po dokončení instalace se spustil prvotní konfigurátor ISA serveru. Nejprve jsem musel vybrat typ firewallu (Single network adapter, Front firewall, Back firewall nebo Edge firewall). Vybral jsem si Edge firewall. V dalším kroku jsem musel vybrat a specifikovat adapter interními sítě. Na další záložce mi průvodce nechal vybrat výchozí bezpečnostní pravidla, které po odklepnutí aplikoval. Jedno z výchozích pravidel bylo, že zakazovalo veškerý provoz umožňující komunikaci dovnitř nebo ven. Poté se nastavily výchozí bezpečnostní pravidla ISA serveru.

5.4.2 Publikace serverů – „Publishing rules“

Publikace serverů znamená zpřístupnění interních serverů pro uživatele externích sítí. Toto se provádí pomocí vestavěných průvodců ISA serveru, které se mohou po vytvoření editovat. Editovat můžeme všechny vlastnosti daného pravidla. Publikace serverů znamená dynamické filtrová paketů, tedy TCP a UDP porty se otevírají dynamicky. Tento typ filtrování se nazývá „Stavové filtrování paketů“.
Publikovat v ISA serveru můžeme:

- Web server
- Zabezpečený web server
- Mail server

Protokoly, kterých se publikace týká, jsou:

- HTTP
- HTTPS
- FTP

„Průvodci publikováním webu zjednodušují celý proces zpřístupnění těchto služeb externím uživatelů a dovolují také přesměrovat požadavky na alternativní porty interního serveru. Tento druh přesměrování portů dovoluje zveřejnit více webů na jednom interním serveru, přičemž každý web očekává požadavky na svém přiděleném čísle portu.“[9]

[9] SHINDER,T. W., SHINDER,T. W., GRASDAL, M. *ISA Server 2000*, 520 s.

Jedním z dalších požadavků klienta byla publikace interních serverů počítačové sítě.

Před publikacemi jsem musel zkontrolovat specifické vlastnosti sítě, jako jsou záznamy DNS nebo správný veřejný DNS název ve vlastnostech certifikátu. Jako první jsem publikoval webové rozhraní poštovního serveru Exchange nazývaného OWA (Outlook Web Access), kdy uživatelé mohou přistupovat ke své poštovní schránce. Pro publikaci OWA bylo zapotřebí, abych vybral průvodce „Publish a Mail Server“ z nástrojové lišty. Poté bylo třeba zatrhnout možnosti „Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server Activesync“. Na další záložce jsem vybral typ Exchange serveru, typ služby která měla být publikována. Další záložka mi nakonfigurovala typ zabezpečení, kdy jsem vybral šifrování SSL jak mezi firewallem a klientem, tak mezi firewallem a poštovním serverem. Dále bylo třeba nastavit Web listener. Web listener je webový naslouchač, ve kterém muselo být nastaveno rozhraní, na kterém naslouchá.
Na Web listeneru jsem musel nastavit platný certifikát pro SSL a typ ověřování na „OWA Forms-based“. Jako poslední bylo třeba specifikovat seznam uživatelů, kteří tuto vlastnost mohli využívat.

V dalším kroku jsem musel publikovat „Outlook over RPC/HTTPS“. Tato vlastnost poštovního serveru Exchange nám umožňuje spojení Outlook s Exchange serverem pomocí šifrovaného protokolu HTTPS. Je to velmi efektivní způsob, jak připojovat externí nebo hodně cestující zaměstnance k poštovnímu serveru firmy.

Pro publikaci bylo zapotřebí vybrat průvodce „Publish a Secure Web server“ z nástrojové lišty. Pojmenoval jsem si nové pravidlo a v následujícím kroku jsem vybral možnost „SSL Bridging“, kdy ISA Server dešifruje komunikaci, provede její inspekci a následné filtrování pokud je to zapotřebí. Na další záložce jsem

vybral možnost „Allow“, která komunikaci povoluje. Další záložka mi nakonfigurovala typ zabezpečení, kdy jsem vybral šifrovací možnost „Secure connenction to clients and Web server“. Tato možnost je založena na komunikaci protokolu HTTPS. V dalším kroku bylo potřeba specifikovat interní jméno nebo IP adresu poštovního serveru s publikovanou cestou webového serveru IIS. Poté jsem musel nastavit veřejný DNS záznam naší externí IP adresy a cesta IIS už byla vyplněná.

Dále bylo třeba nastavit Web listener. Web listener je webový naslouchač, ve kterém muselo být nastaveno rozhraní, na kterém naslouchá.

Na Web listeneru jsem musel nastavit platný certifikát pro SSL a typ ověřování na Integrated. Posledním krokem bylo třeba specifikovat seznam uživatelů, kteří tuto vlastnost mohli využívat.

5.4.3 Access rules

Pravidla „Access rules“ poskytují konfiguraci statických paketových filtrů. Statické filtry paketů trvale otevírají nebo uzavírají cestu různým paketům. Statické filtry nejsou omezeny jen na filtrování portů TCP/UDP, ale mohou filtrovat i ostatní pakety různých protokolů IP (ICMP, GRE atd.). Je doporučeno, abychom převážně používali publikačních pravidel k přístupu interním zdrojů na podnikové síti.

Pro implementaci pravidel „Access rules“ je třeba znát tyto věci:

- Access rules povolují nebo zakazují provoz. Publishing rules nám povolují přístup udělit.
- Access rules mohou povolit provoz do vícenásobných cílů. Publishing rules povolují provoz do jednoho cíle.
- Access rules můžeme využít k různým protokolům. Publishing rules povolují použít jen jeden protokol.

- Access rules nepovolují přesměrování aktuálního portu na jiný port.
- Některé aplikační filtry se chovají různě, když provoz je povolen přes Access rule, ale ne přes Publishing rules. Například vestavěný filtr SMTP kontroluje SMTP provoz, který je pouze povolen Publishing rules.
- Publishing rules pracují jako příchozí TCP protokoly a Access rules je definován jako odchozí TCP protokol.

Vytvoření Access rules pro POP3 protokol se vytváří jako u Publishing rules a to výběrem průvodce z nástrojové lišty „ Create New Access rule“. Nové pravidlo jsem si pojmenoval podle svého uvážení. V dalším kroku jsem si musel vybrat možnost, jestli pravidlo bude zakazovat nebo povolovat přístup ke službě POP3. Vybral jsem možnost povolovat, protože jsem chtěl povolit přístup ke službě POP3, která slouží k vybírání emailů poštovní schránky ze serveru uživatelem. Poté bylo nutné specifikovat typ portu, který bude pravidlo používat, tedy POP3. Následně jsem si musel uvědomit, odkud bude směřovat komunikace, kterou vzdálení uživatelé budou inicializovat. Tedy vybral jsem možnost „External“ z externí sítě (vše mimo interní síť a ISA serveru samotného). Poté jsem musel nastavit kam bude komunikace směřovat, tedy do interní sítě volnou „Internal“. Poté bylo třeba specifikovat skupinu lidí, kteří měli mít možnost připojení protokolem POP3. Posledním krokem bylo třeba vytvořené pravidlo aplikovat tlačítkem „Apply“.

Další Access Rules, které jsem osobně vytvořil, byly:

- Vzdálený přístup RDP z externích sítí (TCP 3389)
- Vzdálený přístup RDP do externích sítí (TCP 3389)
- Přístup uživatelům do externí sítě (TCP 80)
- Přístup na externí síť programu Multi Cash (TCP 1500)

- Povolení programu Medikus do externí sítě (TCP 5910 – 5912)
- Pravidlo pro ISA Server samotný do externí sítě (TCP 80, TCP 443)
- Povolení monitorovacího programu Zabbix do interní sítě (TCP 10050)
- Pravidlo povolující FTP službu do externí sítě (TCP 21)

5.4.4 Konfigurace VPN

Jedením z dalších požadavků klienta bylo, umožnění vzdáleného připojování počítačů do interní počítačové sítě přes virtuální privátní síť VPN. Virtuální privátní síť nám zabezpečí, že data procházející tunelem mezi uživatelem VPN a interní sítí nelze nijak dešifrovat a zneužít je. Při konfiguraci typu VPN tunelu jsem zvolil PPTP tak L2TP/IPSec. PPTP jsem zachoval z důvodu zpětné kompatibility, kdy některé starší operační systémy nepodporují VPN tunel L2TP/IPSec. V sekci „Virtual Private Network (VPN) jsem z nástrojové lišty vybral možnost „Configure Client VPN access“ a zaškrtnul jsem možnost „Enable Client VPN access“ a specifikoval jsem množství současných VPN připojení. V dalším kroku jsem povolil přístup do VPN pouze omezenému množství uživatelů na základě jména a hesla z Active Directory. Vybral jsem protokoly PPTP tak L2TP/IPSec pro připojení do VPN. Následně jsem musel nakonfigurovat hlavní vlastnosti VPN připojení. V nástrojové liště jsem vybral možnost „Select Access Networks“ a na záložce „Access Networks“ jsem zaškrtnul volbu „External“. Na následující záložce jsem musel nakonfigurovat, zda bude VPN klientovi přidělená pevná IP adresa z pevně vytvořeného rozsahu adres a nebo mu bude dynamicky přidělena DHCP serverem naší sítě. Pro šifrované ověřování VPN klienta jsem vybral možnost „Microsoft encrypted authentication version 2 (MS-CHAPv2)“.

Pokud bych pro ověřování použil certifikát, kterým by se klient VPN přihlašoval do VPN, musel bych nakonfigurovat možnost „Extensible authentication protocol (EAP) with smartcard or other certificate“.

5.4.5 Konfigurace vlastností síťového nastavení

Konfigurace vlastností síťového nastavení je jednou z nejdůležitějších věcí celého ISA Serveru. Pokud nejsou správně nastaveny všechny tyto vlastnosti, nebude zabezpečení interní firemní sítě vůbec funkční. Proto je třeba zkontrolovat všechna nastavení, které byly vytvořeny při prvním spuštění konfigurátoru ISA Serveru.

V levé části konzole ISA Serveru se nachází sekce „Configuration“, ve které se konfigurují všechny vlastnosti síťového nastavení. Přešel jsem do části zvaná „Network“ a zde vše začalo. První záložka jménem „ Network“ obsahuje všechny druhy sítí jako jsou:

- External
- Internal
- Local Host
- Quarantined VPN Clients
- VPN clients

Zde jsem si mohl editovat nebo vytvářet nové druhy sítí, pokud by to bylo potřeba.

V mém případě jsem nepotřeboval měnit žádné vlastnosti sítí, protože všechny byly vytvořeny prvním konfigurátorem ISA Serveru. Proto, abych si byl jist, že PROXY je správně nastavena, vybral jsem síť „Internal“. Na záložce „Web Proxy“ jsem zkontroloval, že volba „Enable Web Proxy“ a „Enable HTTP“ byla zatrhnuta. Na záložce „Domains“ jsem se přesvědčil, že v seznamu domén je nastavena aktuální doména Active Directory.

Ostatní záložky „Network Sets, Network Rules, Web chaining“, jsem také nechal beze změny, protože již byly nastaveny prvotním konfigurátorem ISA Serveru, ale pro jistotu jsem si všechny zkontroloval.

5.4.6 Konfigurace Cache ISA Serveru

Jak jsem již uvedl v úvodu, druhou vlastností ISA Serveru je akcelerovat požadavky uživatelů. Proto aby ISA server mohl tyto požadavky akcelerovat musela být nastavena paměť „Cache“ pro ukládání webového obsahu uživatelů. Ve stejné části, kde se konfigurují vlastnosti sítí, existuje zde část zvaná „Cache“. V nástrojové liště byla vybrána možnost „Define Cache Drives (Enable Caching)“, kde byl zvolen určitý disk, na který se bude ukládat webový obsah uživatelů. Možností „Configure Cache settings“ se specifikují, jak velké a jak dlouho se URL adresy uchovávají. Změnu již nastavených vlastností jsem nedělal, protože mi dané nastavení připadalo správné. V prostřední části konzole již existovalo výchozí pravidlo pro ukládání webového obsahu uživatelů. Proto jsem pouze zkontroloval nastavené hodnoty a vlastnosti daného výchozího pravidla. Jako první, co jsem zkontroloval, bylo, pro jaké sítě se má webový obsah ukládat. Možnost byla nastavena pro všechny sítě. Na záložce HTTP jsem zkontroloval, jestli je volba „Enable HTTP caching“ zaškrtnuta. Poslední záložku FTP výchozího pravidla jsem zkontroloval a i volba „Enable FTP caching“ byla zatrhnuta. Pokud by někomu výchozí pravidlo nevyhovovalo, může ho smazat nebo editovat. Pokud bychom měli více sítí můžeme pro každou síť specifikovat svoje Cache pravidlo.

ZÁVĚR

Pokud se organizace připojuje k Internetu, měla by jako první vyřešit otázku zabezpečení interní sítě. Zabezpečení interních sítí je v dnešní době velmi důležitým a sledovaným tématem, protože útoky hackerů jsou stále agresivnější a propracovanější. Nemůžeme se tedy divit, že mnoho společností nabízí různé firewallové produkty a poptávka po nich prudce stoupá. Firewall je bariéra, která odděluje vnější sítě (většinou Internet) od vnitřní sítě. Firewall nám umožňuje používat bezpečnostní prvky, které pomáhají efektivně zabezpečit interní síť. Existují různé kategorie firewallových produktů pro různé klienty - od domácích uživatelů až po velké organizace. Správné zabezpečení interní sítě není jednoduché a proto se nesmí být zapomenouto na všechna slabá místa, která nám bude chránit.

ISA Server je jednou z možností, jak se efektivně chránit před útoky čekající mimo interní síť. Velmi významnými přednostmi ISA Serveru jsou jeho spolehlivost, škálovatelnost, podpora více procesorů, rozložení zátěže sítě (load balancing). ISA Server je aplikační firewall, který kontroluje nejen typ protokolu, ale i obsah daného protokolu. ISA Server plní celkem čtyři role. První rolí je funkce firewallu a druhou rolí je funkce akcelerace webového obsahu, kdy se ukládá do mezipaměti. Třetí rolí je funkce NAT a čtvrtou rolí je služba proxy.

Funkce firewallu nám umožňuje vytvářet bezpečnostní pravidla, kterými povolujeme nebo zakazujeme přístup do interní sítě. Vytváření pravidel se provádí pomocí průvodců, kteří nám ulehčují konfiguraci nového pravidla. V průvodci je většinou i popis, který má být stručný a věcný.

Funkce akcelerace webového obsahu se provádí nastavením mezipaměti (Cache), kdy je v pravidlu definována délka časového limitu a velikost obsahu URL adresy, která se uloží.

Funkce NAT ISA Serveru nám překládá a zaměňuje interní IP adresy sítě na veřejnou IP adresu organizace, kterou má u svého providera pronajatou. Funkce NAT je dalším bezpečnostním prvkem ISA Serveru, který jsem musel nastavit.

Poslední funkcí ISA Serveru je služba Proxy, která je postavena na základě webové komunikace (HTTP, HTTPS). Nastavení Proxy nám umožňuje specifikovat seznam uživatelů, kteří mohou mít přístup do Internetu.

Po výčtu požadavků na zabezpečení interní sítě našeho klienta mi bylo jasné, že se musím zaměřit na produkty firewallů, které budou splňovat jeho požadavky a navíc budou cenově dostupné. Věděl jsem, že celá klientova platforma je tvořena servery společnosti Microsoft, proto jsem vybral firewall Microsoft ISA Server. Výhody ISA serveru jsou, oproti jiným řešením, v integraci firewallu v prostředí Windows. Bylo by velmi smutné, kdyby tomu tak nebylo.

Nedílnou součástí firewallového řešení je návratnost investic. Návratnost investic u firewallu lze jen s těží odhadnout, protože firewall chrání data, která mohou mít i nevyčíslitelnou hodnotu. Proto lze vyčíslit pouze návratnost investice při nákupu ISA Server firewallu. Z porovnávací tabulky rychle zjistíme, že náklad na investici je u ISA Serveru nejnižší a proto se tato investice rychleji vrátí.

Při instalaci a následné konfiguraci ISA serveru mě překvapila jednoduchost a perfektní propracovanost všech průvodců, kteří mi nastavení ulehčili. ISA Server má všechna nastavení logicky srovnané a nic se nemusí dlouze hledat. Dále je možné rozšířit ISA Server o doplňky firem třetích stran, které zabezpečení ještě více posílí, tedy pokud budeme chtít akceptovat jejich cenu.

Jediné co bych ISA serveru vytkl je omezené množství předdefinovaných filtrů, které si volíme při vytváření reportů. Na tuto vlastnost reagovaly některé firmy třetích stran, které nabízejí za poplatek lepší filtrování a následné vytvoření svých ISA Server reportů.

Zabezpečení sítě ISA Serverem mohu jen vřele doporučit a troufám si tvrdit, že se jedná o jedno z nejlepších řešení na trhu s firewally.

Seznam použitých zdrojů:

KNIHY

SHINDER, D. L., SHINDER, T. W., GRASDAL, M. *Dr. Tom Shinder`s Configuring ISA Server 2004*. Brno: Computer Press, 2003. 1022 s. ISBN 1931836191.

RATLIFF, B., BALLARD, J., *Microsoft Internet Security and Acceleration (ISA) Server 2004 Administrator`s Pocket Consultant*. Microsoft Press, 2006. 432 s. ISBN 0735621888

NOEL, M., *ISA Server 2004 UNLEASHED*. Sams Publishing, 2005. 576 s. ISBN 0-672-32718-X.

STREBE, M., PERKINS, CH., *Firewally a proxy servery*. Brno: Computer Press, 2003. 450 s. ISBN 80-722-6983

SHINDER, D. L., SHINDER, T. W., GRASDAL, M., *ISA Server 2000*. Brno: Computer Press, 2003. 760 s. ISBN 80-7226-916-X.

KABELOVÁ, A., DOSTÁLEK, L., *Velký průvodce protokoly TCP/IP a systémem DNS*. Brno: Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.

DONAHUE, G. A., *Kompletní průvodce síťového experta.* Brno: Computer Press, 2009. 528 s. ISBN 978-80-251-2247-1.

LOCKHART, A., *Bezpečnost sítí na maximum*. Brno: Computer Press, 2005. 280 s. ISBN 80-251-0805-8.

THOMAS, M. T., *Zabezpečení počítačových sítí*. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

KOSTRHOUN, A., *Stavíme si malou síť*. Brno: Computer Press, 2001. 216 s. ISBN 8072265105.

SMITH R. W., *Linux ve světě Windows*. Praha: Grada, 2006. 460 s. ISBN 80-247-1470-1.

BOTT, E., SIECHERT, C., *Mistrovství v zabezpečení Microsoft Windows 2000 a Xp.* Brno: Computer Press, 2004. 696 s. ISBN 80-7226-878-3.

INTERNETOVÉ ADRESY

MICROSOFT, Přehled vlastností [on-line]. [cit. 2006-9-5]. Dostupný z WWW: <http://www.microsoft.com/cze/windowsserversystem/isaserver/previousversions/2004/overview.mspx>.

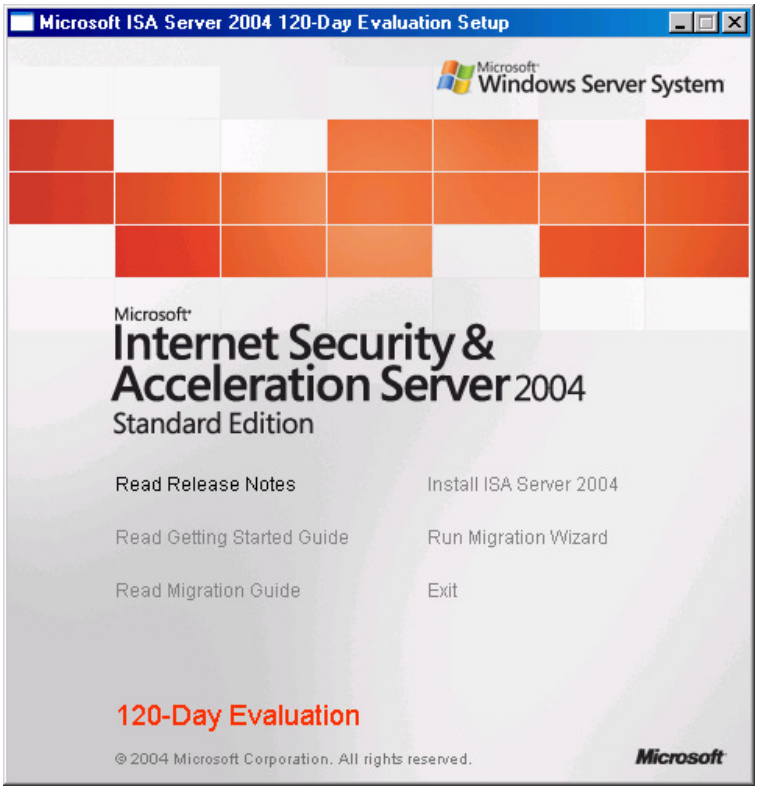
SHINDER, T. *Using ISA Server 2004 Network Templates to Automatically Create Access Policy: The Edge Firewall Template* [on-line]. [cit. 2004-7-19]. Dostupný z WWW: <http://www.isaserver.org/tutorials/2004edgefirewall.html>.

MAGALHAES, R. M. *Optimizing ISA 2004 caching (Part 1)* [on-line]. [cit. 2006-6-15]. Dostupný z WWW: <http://www.isaserver.org/tutorials/Optimizing-ISA-2004-caching-Part1.html>.

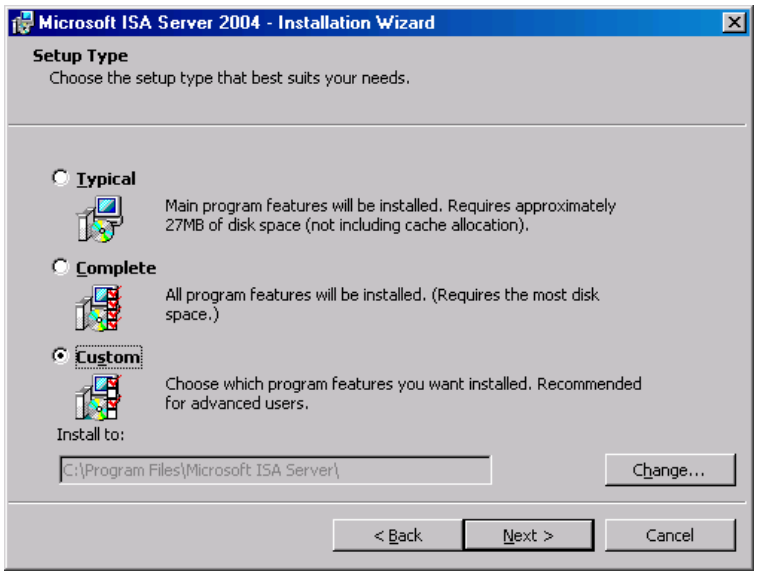
MAGALHAES, R. M. *Optimizing ISA 2004 caching (Part 2)* [on-line]. [cit. 2006-6-15]. Dostupný z WWW: <http://www.isaserver.org/tutorials/Optimizing-ISA-2004-caching-Part2.html>.

MULHOLLAND G. *Remote Administration of ISA Server 2004* [on-line]. [cit. 2006-6-16]. Dostupný z WWW: < http://www.isaserver.org/tutorials/2004remoteadmin.html>.

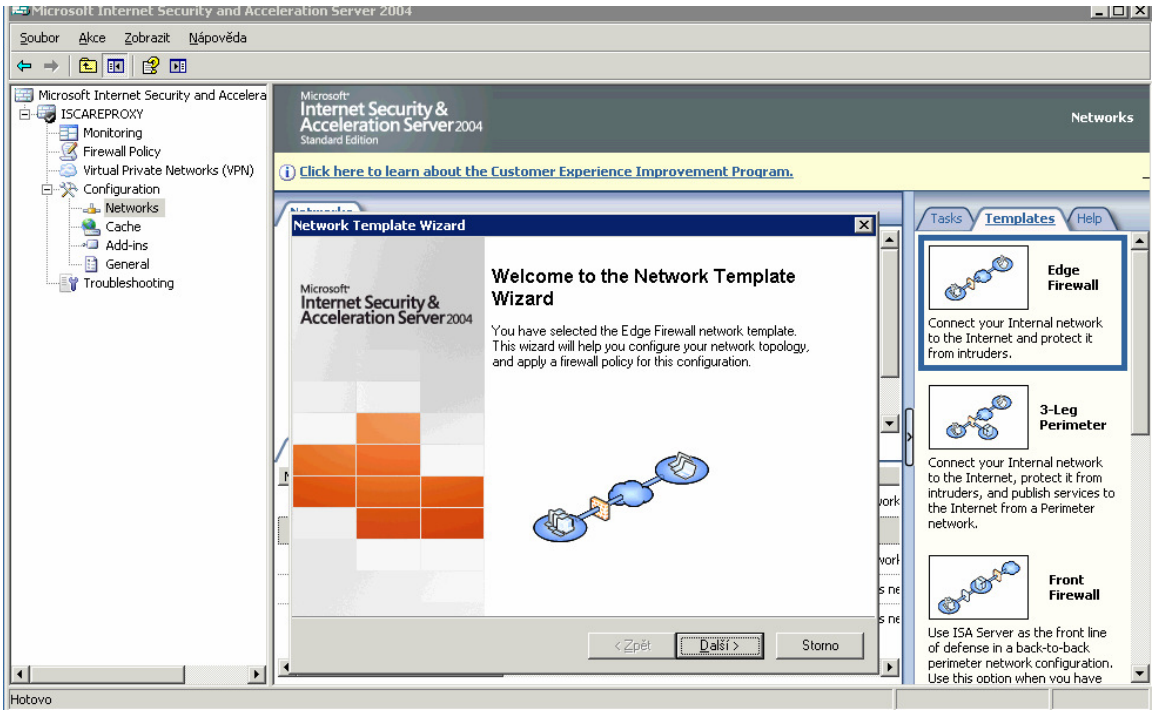
Seznam příloh



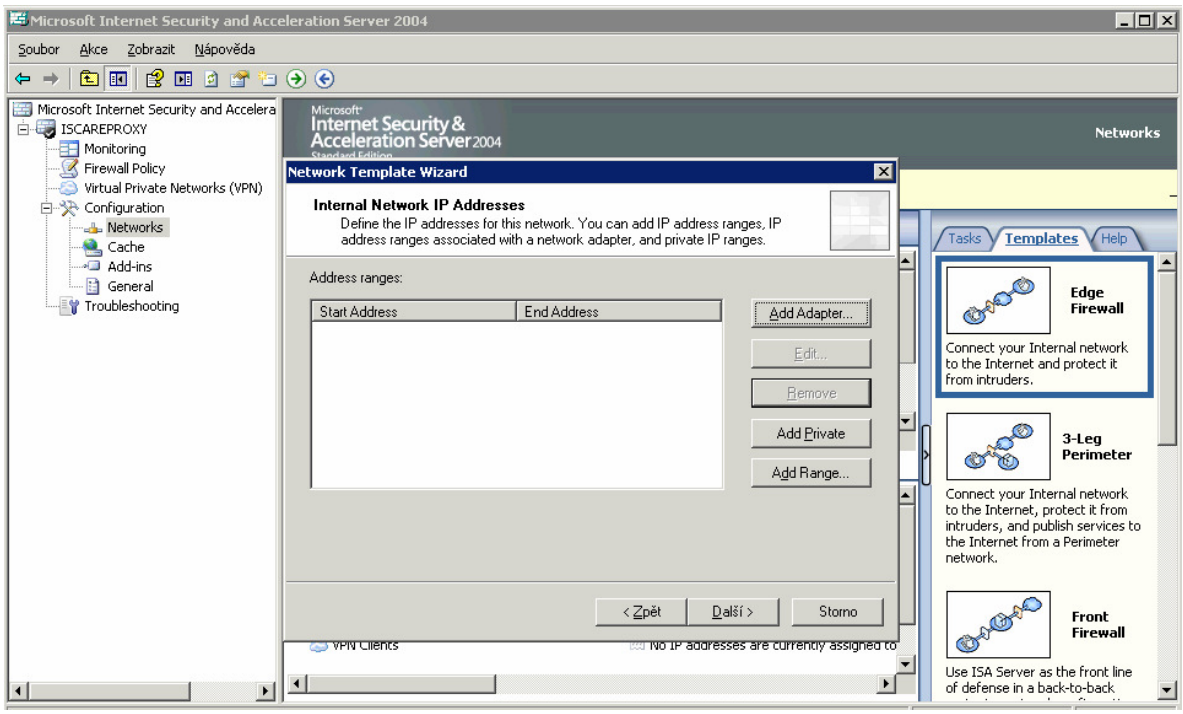
Příloha č.1 - Počátek instalace ISA Serveru



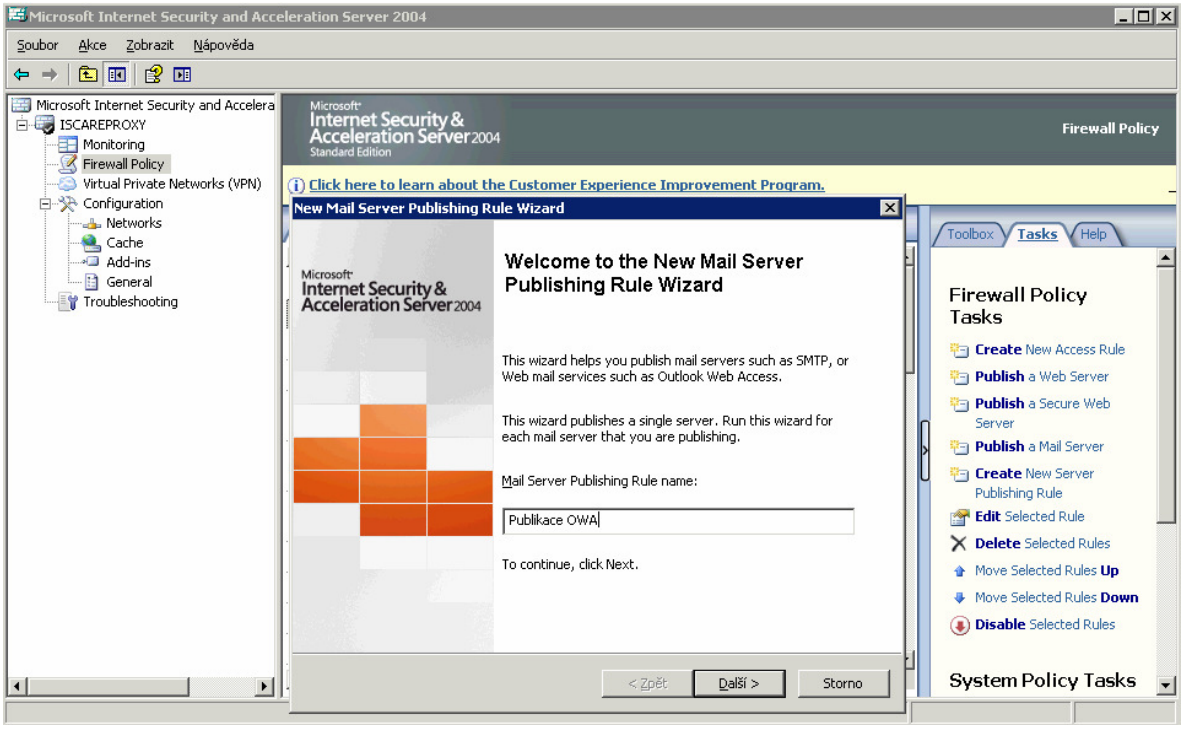
Příloha č.2 - Pokračování instalace



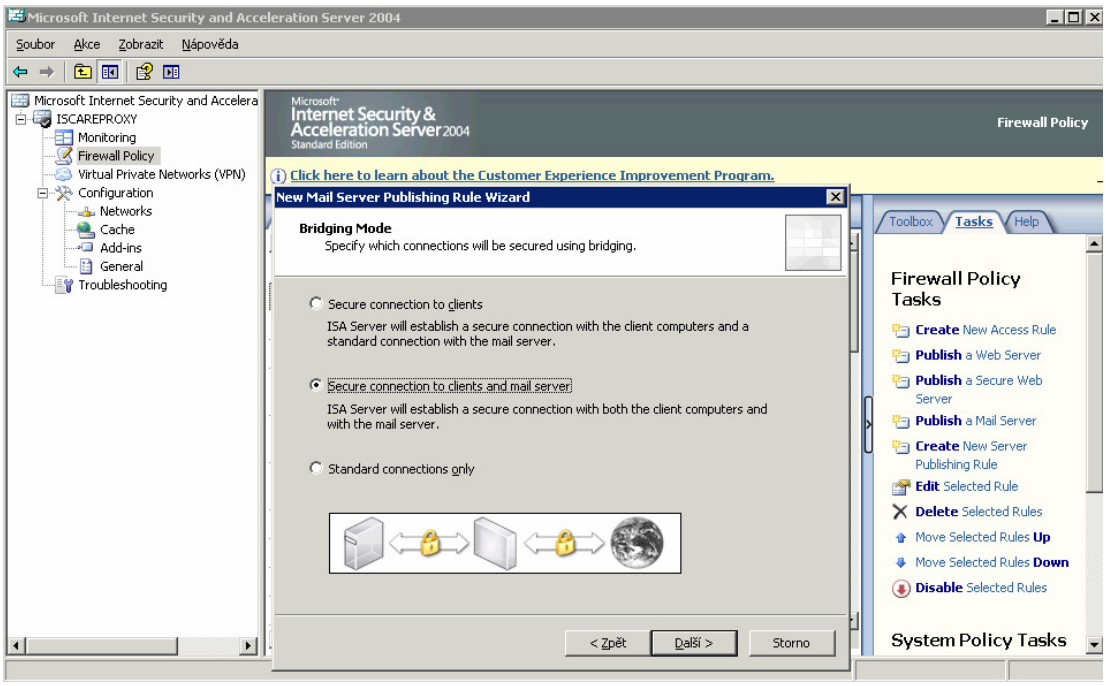
Příloha č.3 - Počáteční výběr typu firewallu



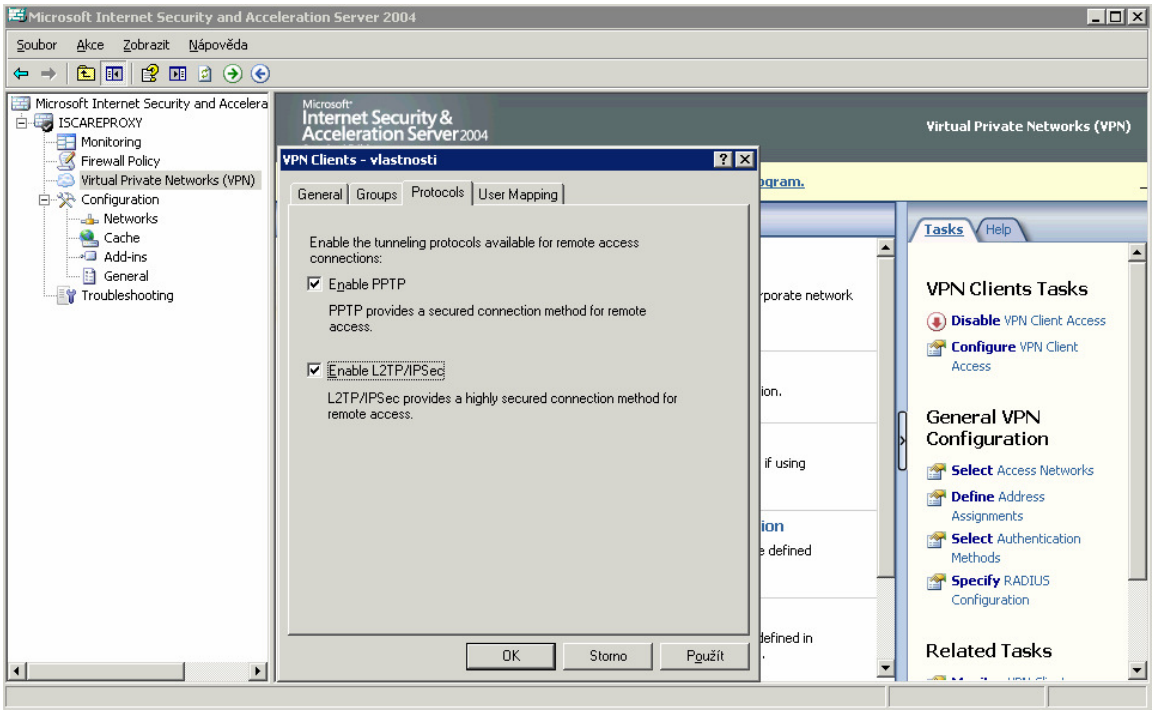
Příloha č.4 - Konfigurace síťových adaptérů



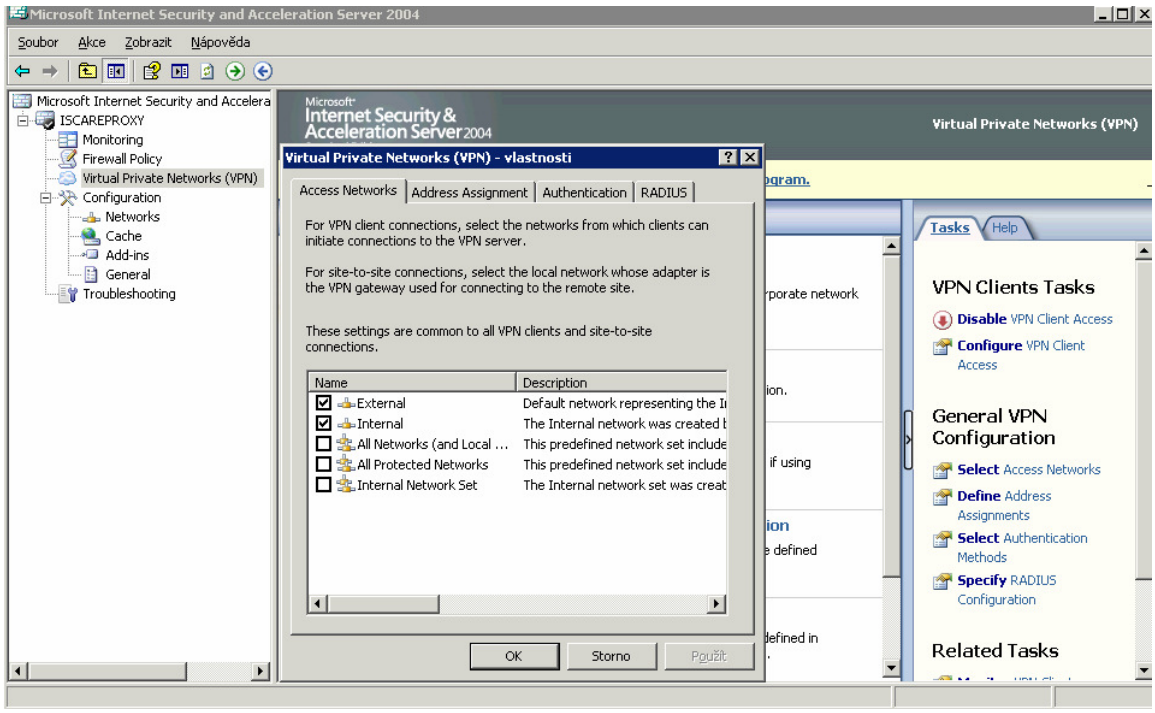
Příloha č.5 - Pravidlo publikující Outlook Web Access



Příloha č.6 - Výběr zabezpečení pravidla publikující Outlook Web Access



Příloha č.7 - Specifikace typu VPN připojení



Příloha č.8 - Výběr síťových adaptérů pro komunikaci s VPN klienty