IPSec - krok po kroku

1) Úvod

IPsec je rozšíření IP protokolu, které poskytuje bezpečnost pro IP protokol a protokoly vyšších vrstev. Nejdříve byl vyvinut pro nový standard IPv6 a následně byl zpětně implementován na IPv4. Výhoda tohoto způsobu zabezpečení je v tom, že se děje na úrovni operačního systému, takže aplikace o něm nemusí vědět, tj. nemusí být upravovány. Na druhou stranu nezabezpečuje data mezi uživateli, či aplikacemi běžícími na témže počítači. IPsec užívá dva rozdílné protokoly - AH a ESP - aby zajistil ověřování identity, neporušenost a důvěryhodnost komunikace. Může chránit buď celý IP datagram nebo pouze protokoly vyšší vrstvy. Módy IPSec:

- **Tunelovací**: IP datagram je plně zapouzdřený do nového IP datagramu, který používá IPsec protokol.
- **Transportní**: pouze užitečná část (payload) IP datagramu je zpracovaná IPsec protokolem a to tím způsobem, že se vkládá IPsec hlavička mezi IP hlavičku a hlavičku protokolu vyšší vrstvy.

2) IPSec ve Windows XP:

V následujících krocích je popsáno, jak IPSec nastavit a spravovat v prostředí operačního systému Windows XP, popřípadě Windows 2000.

- Konfigurace se provádí pomocí programu Microsoft Management Console, který spustíme z nabídky *Start* → *Spustit* → *mmc*.
- V nabídce programu mmc klikneme na volbu Soubor → Přidat nebo odebrat modul snap-in → Přidat... → Vybereme ze seznamu a přidáme modul Správa zásad zabezpečení protokolu IP (budeme vyzváni zvolit, jaký počítač nebo doménu bude tento modul spravovat - např. místní počítač). Dále zde přidáme modul Sledování zabezpečení protokolu IP (jde o dřívější komponentu zvanou IPSecMon)
- Po přidání modulu do konzoly a po kliknutí na něj jsou v pravém okně programu **mmc** tři předdefinované pravidla připojení, které loužít či nikoliv Vše je podrobně popsáno. Pro daný účel je lépe vytvořit pravidlo nové a to následovně: pravým tlačítkem myši kliknout v oblasti pravého okna a vybrat nabídku *Vytvořit zásadu zabezpečení protokolu IP* (viz. Obr. 2.1).

🚡 Konzola1			_02
Soubor Akce	Zobrazit Oblíbené položky Okno Nápověda		
← → 🖬	Přidat nebo odebrat modul snap-in	<u>? × </u>	
🖌 Kořenový	Samostatný Rozšíření		_ _ ×
🔄 Kořenový a	Pomocí této stránky můžete přidávat a odebírat z konzoly samostat moduly snap-in.	né Přidat samostatný modul snap-in	?[×]
	Moduly snap-in 🖾 Kořenový adresář konzoly 💌	Samostatné moduly snap-in k dispozici:	
		- Modul snap-in	Dodavatel
	Popis	Složka Služba Component Services Služba Indexing Service Služby Správa disků Správa počítače Správa vyměnitelného úložiště Správa zásad zabezpečení protoko Správce zařízení Ponis	Microsoft Corporation Microsoft Corporation Microsoft Corporation, Microsoft Corporation Microsoft and VERITAS Microsoft Corporation Microsoft Corporation Microsoft Corporation
	Přidat Odebrat O'modulu	Správa protokolu IPSec (Internet Protocol Security). Umožňuje správu zásad protokolu IPSec za účelem bezpečné komunikace s jinými počítači.	

Obr. 2.1: Nabídka vytvoření zásady zabezpečení

- Objeví se Průvodce zásadami zabezpečení → Další → zvolit nějaký smysluplný název zásady a její stručný popis. Požaduje se například vytvořit zásadu, která bude zajišťovat to, že konfigurovaný počítač komunikuje se všemi ostatními stanicemi pouze zabezpečeně, takže volba může být: "Zabezpečená komunikace" a do popisu: "Pro veškerý síťový přenos protokolu IP vyžadovat zabezpečení. Neumožní nezabezpečenou komunikaci s nedůvěryhodnými klienty.".
- Kliknout na Další → zde ponechat vybranou možnost Zapnout výchozí pravidlo odpovídání, pak opět Další
- Nyní se objeví okno s možností volby počáteční metody ověřování. Na výběr jsou tři možností:
 - Protokol Kerberos V5
 - o Certifikát od certifíkačního úřadu (tj. autority)
 - Předsdílený klíč
- Pro dané potřeby vyberat *Předsdílený klíč* a zapsat jej do boxu. Zvolit libovolné heslo, nejlépe dle všeobecně známých pravidel pro tvorbu hesel (např. KadeJos57PokUs).
- Kliknout na tlačítko Další a v novém okně opět ponechat vybranou možnost Upravit vlastnosti → Dokončit → vyvolá se okno Zabezpečená komunikace - vlastnosti (Obr. 2.2).

Zabezpečená komunika	ce - vlastnosti		? ×
Pravidla Obecné			
Pravidla zabe	zpečení při komunikaci s	jinými počítač	ä
Pr <u>a</u> vidla zabezpečení IP	:		
Seznam filtrů IP	Akce filtru	Způsoby ov	ěř Na
✓ <dynamický></dynamický>	Výchozí odpověď	Předsd ilený	klíč Žá
I I I I I I I I I I I I I I I I I I I	avit	Použít	۲ pnjvodce
		ОК	Stomo

Obr. 2.2: Zabezpečená komunikace - vlastnosti

- Zde se automaticky vybere filtr *Dynamický*, což v praxi znamená, že se počítač při vyjednávání komunikace bude pokoušet nabídnou protistraně všechny možné metody zabezpečení. To znamená protokol AH, či ESP (nebo oba) a pro každý z protokolů určit protokoly pro kontrolní součet (MD-5, SHA-1). Pro protokol ESP je třeba určit šifrovací algoritmus (DES, 3DES).
- Pokud by tento filtr nevyhovoval, protože existují přesné požadavky na komunikaci mezi stanicemi (např. ESP, 3DES, SHA-1), není nic jednoduššího než si vytvořit filtr nový, což je popsáno v dalším textu
- Za předpokladu, že filtr *Dynamický* vyhovuje daným požadavkům a není důvod ho nijak měnit, postačí kliknout na tlačítko OK a navrátit se do okna konzole.
- Zbývá poslední krok a tím je aktivace samotného pravidla. Tu se provede velice lehce, kliknutím pravým tlačítkem na něj a výběrem položky *Přidělit* z kontextového menu.

3) Tvorba konkrétního filtru IPSec:

Specifikovat požadavky na filtr:

- Šifrovaná komunikace pouze se stanicí IP 192.168.0.10, ostatní komunikace nešifrovaná.
- Požaduje se protokol ESP (MD-5, 3DES).
- Metoda ověřování pomocí předsdíleného klíče (KadeJos57PokUs)

PO ujasnění si požadavků lze přistoupit k jeho vlastní tvorbě, přičemž bude využito dříve vytvořeného pravidla zabezpečení *Zabezpečená komunikace*.

• Kliknout pravým tlačítkem myši v pravém okně konzole na pravidlo *Zabezpečená komunikace* a vybrat možnost *Vlastnosti* (viz. Obr. 3.1).

🚡 Konzola1							
Soubor Akce Zobrazit Oblíbené položky Okno Nápověda							
← → 🖻 🖪 🗙 😭 🗟 😫							
🚡 Kořenový adresář konzoly\Zásad	🖌 Kořenový adresář konzoly \Zásady zabezpečení protokolu IP - Místní počítač						
Kořenový adresář konzoly	Název A	Popis Zi	ásady jsou přiřazeny				
 Zásady zabezpečení protokolu ! 	Zabezpečená komunikace Přidělit	N	e				
	Všechny úkoly	•					
	Odstranit Přejmenovat	_					
	Vlastnosti						
	Nápověda						
Utevre dialog vlastnosti pro aktuální výběr.	•			1			

Obr. 3.1: Změna vlastností pravidla

- Objeví se již známé okno s vlastnostmi pravidla, zde ze seznamu filtrů smazat filtr *Dynamický* (nebo zrušit jeho zaškrtnutí).
- Zrušit zaškrtnutí u *Použít průvodce* \rightarrow kliknout na tlačítko *Přidat*.
- Zobrazí se okno vlastností dle obrázku (Obr. 3.2).
- Zde nastavit nový filtr IP adres. Stisknout tlačítko *Přidat* → vložit název a popis IP filtru (např. IPSec pouze proti notebooku Dell).
- Zrušit zaškrtnutí u *Použít průvodce* \rightarrow kliknout na tlačítko *Přidat*.
- Otevře se okno *Filtr vlastnosti*, kde budou nadefinovány požadované IP adresy. Jako zdrojová adresa bude zvolena možnost *Adresa IP tohoto počítače*, jako cílovou *Určená adresa IP* a bude zapsána její hodnota (192.168.0.10)

Nové pravidlo - vlastnosti 🛛 🕺 🗙					
Nastavení tunelového propojer Seznam filtrů IP Akce		ní Typ připojení filtru Metody ověřová		vřipojení ověřování	
Zvolený sez bude vztaho	seznam filtrů IP určuje typy přenosu, na které se tahovat toto pravidlo.				
<u>S</u> eznamy filtrů IP:					
Název		Popis			
Proti Dellu	Proti Dellu Šifrovat vše proti notebooku			ooku	
Pēdat		Odebrat	1		
	Zav	řít	Storno	P <u>o</u> užít	

Obr. 3.2: Nové pravidlo vlastností

- Zaškrtnout možnost Zrcadlený a tlačítkem OK (2x) okno zavřít.
- Do okna dle Obr. 3.2 přibyl nový IP filtr, ten pak kliknutím aktivovat.
- Zvolit záložku Akce filtru → Upravit → Vyjednat metodu zabezpečení → Přidat → Vlastní → MD-5, 3DES → OK→. Dále zde zaškrtnout možnost Povolit nezabezpečenou komunikaci s počítači, které nepodporují IPSec → OK.
- Akci filtru v záložce pojmenovat (!).
- Kliknout na záložku *Metody ověřování* (Obr. 3.2) a výchozí hodnotu Kerberos změnit na předsdílený klíč. Zadat požadované heslo.
- Vše potvrdit a přidělit pravidlo.
- Provoz sítě využívající IPSec lze monitorovat pomocí modulu *Sledování zabezpečení protokolu IP* (resp. programu *IPSecMon*).