FortKnox Personal Firewall 2007

Uživatelský manuál

Dokument verze 1. 1 CZ (29. 10. 2007) - Preklad Sksoft.cz – Michal Adamek

Obsah

1. Úvod

Tento manuál umožňuje seznámit se s vlastnostmi a technologiemi, které program **FortKnox Personal Firewall 2007** nabízí.

1.1. Základní koncepce ochrany

V současnoti většina hrozeb využívá internet na rozšíření a stahování dalšího malware, který může poškodit počítače uživatelů. Spyware může monitorovat uživatelskou aktivitu a zasílat sesbírané údaje přes internet k jeho tvůrci. Firewall představuje jeden z nejdůležitějších bariér, která chrání systémy před potencionálními hrozbami.

1.2. Detekční technologie

FortKnox Personal Firewall 2007 používá následující technologie na ochranu Vašeho systémů:

- **Kontrola příchozích přenosů** – kontroluje přicházející přenosy ze sítě
- **Kontrola odchozích přenosů** – kontroluje odcházející přenosy do sítě
- **Statefull packet inspection** – analyzuje přenosy po stránce správnosti a povoluje jen spojení, které inicializoval uživatel
- **Intrusion prevention system –** analyzuje toky paketů na podezřelou aktivitu
- **Process defense system –** zabezpečuje integritu všech procesů, které přistupují na síť

1.3. Podporované operační systémy

FortKnox Personal Firewall 2007 je kompatibilní s Windows Vista (64-bit a 32-bit), Windows XP (32-bit) a Windows 2000 (32-bit) operačními systémy.

2. Instalace

FortKnox Personal Firewall 2007 může být nainstalován buď z instalačního souboru na Vašem CD nebo z webových stránek: www.fortknox-firewall.com v sekcii Download. Nejnovější verze je vždy přístupná na uvedené stránce.

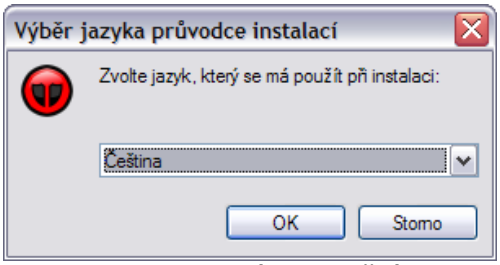
2.1. Instalace z webových stránek

Navštivte internetovou stránku **FortKnox Personal Firewall** na adrese www.fortknox-firewall.com, jděte do sekce **Download** a vyberte odkaz odpovídající Vámi preferované jazykové verzi. Uložte instalační soubor na Váš pevný disk. Spusťte instalaci.

2.2. Instalační proces

Nepřehlédněte, prosím: *Doporučuje se zavřít všechny běžící programy před spuštěním instalace; včetně ostatních bezpečnostních programů, které, mohou blokovat instalaci. Spouštějte instalační proces pod administrátorským účtem.*

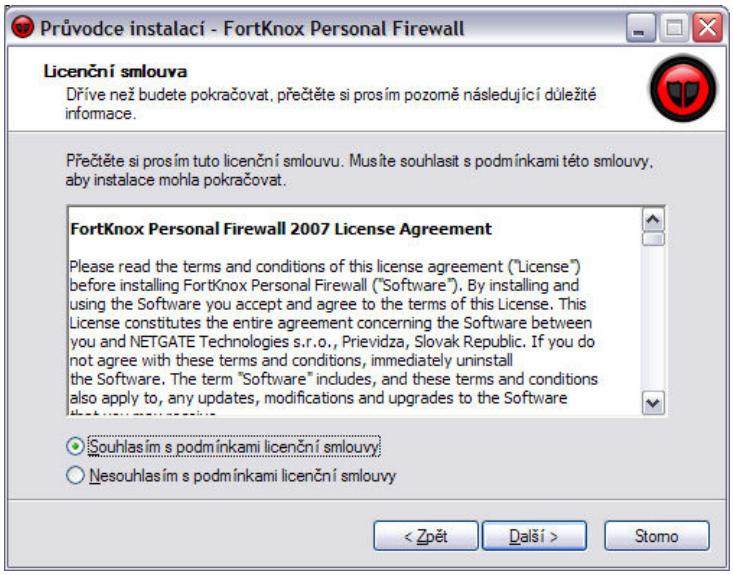
a) Dvojklikem na instalační soubor spustíte instalační proces.



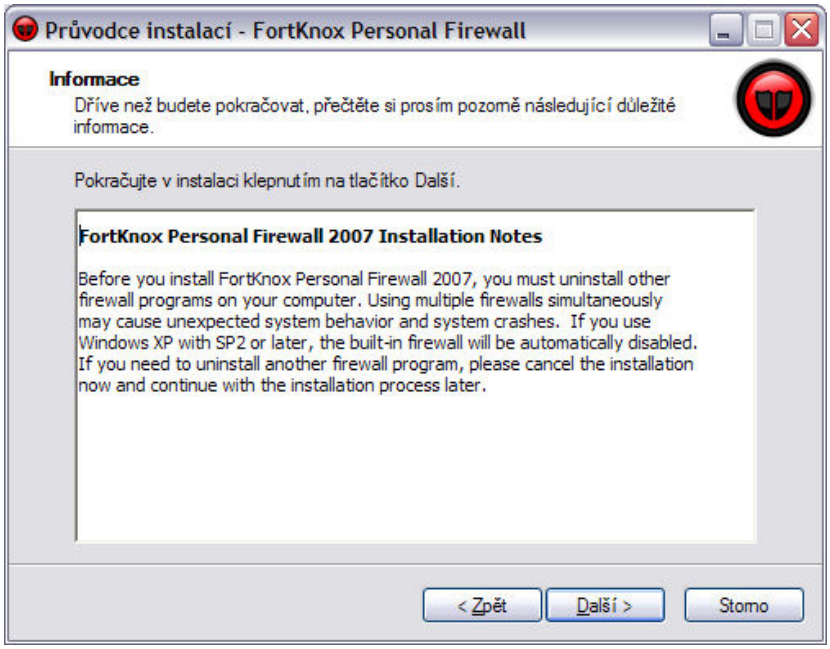
b) Vyberte preferovaný instalační jazyk a klikněte na tlačítko ***OK***.

> ***Nepřehlédněte:*** Zvolený jazyk se týká jen instalačního programu. Můžete si nastavit jazyk programu ***FortKnox Personal Firewall*** *později v* ***Skin/Languages*** *průvodci. Pokud chcete změnit jazyk po instalaci, klikněte pravým tlačítkem na ikonu v systémové liště a vyberte* ***Nastavení****. Vyberte z* ***Aktivní jazyk*** *preferovaný jazyk a stiskněte tlačítko* ***Použít.***

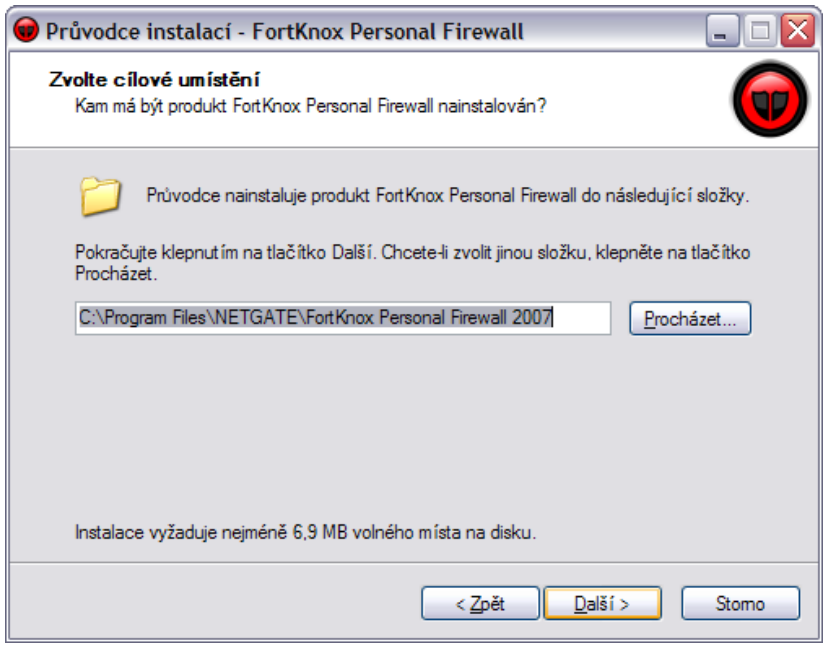
c) Jakmile byla instalace spuštěna, klikněte na tlačítko ***Další*** a přečtěte si licenční podmínky. Klikněte na ***Souhlasím s podmínkami licenční smlouvy*** pro odsouhlasení licenčních podmínek programu FortKnox Personal Firewall.



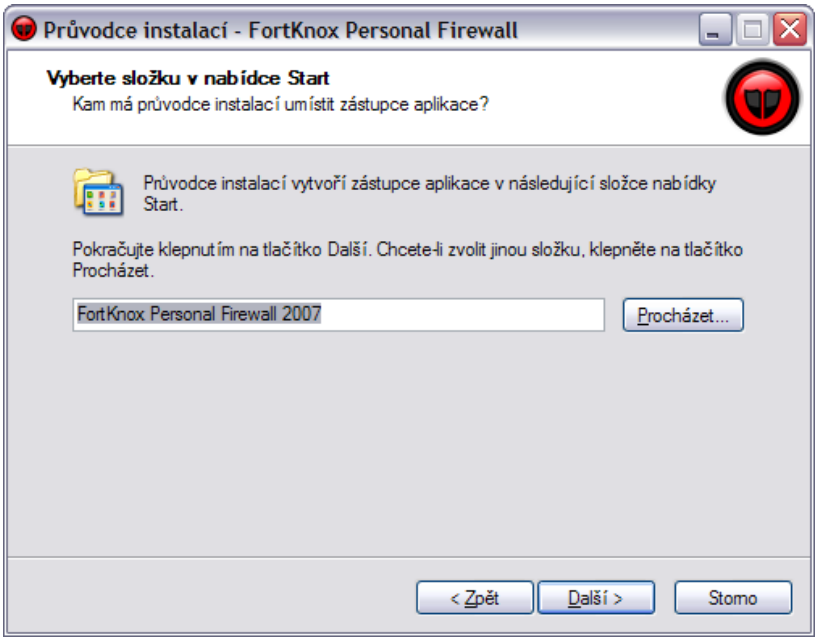
d) Prečtěte si instalační poznámky a následně klikněte na tlačítko ***Další***. Musíte **odinstalovat** vvšechny ostatní firewall programy před tím, než budete pokračovat v instalačním procesu.



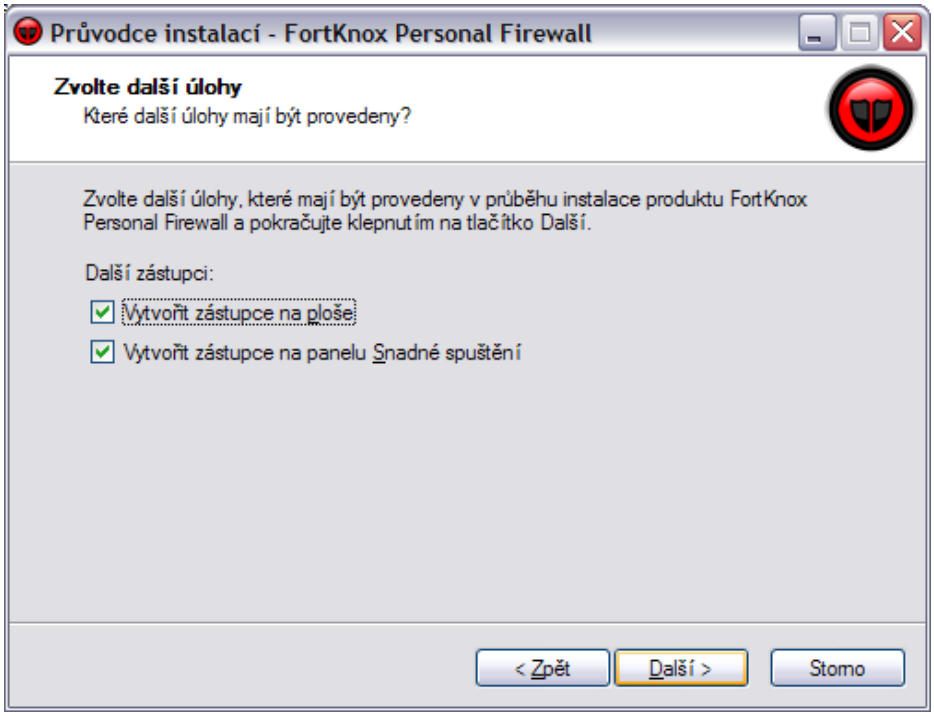
e) Vyberte cílovou složku instalace a klikněte na tlačítko ***Další***.



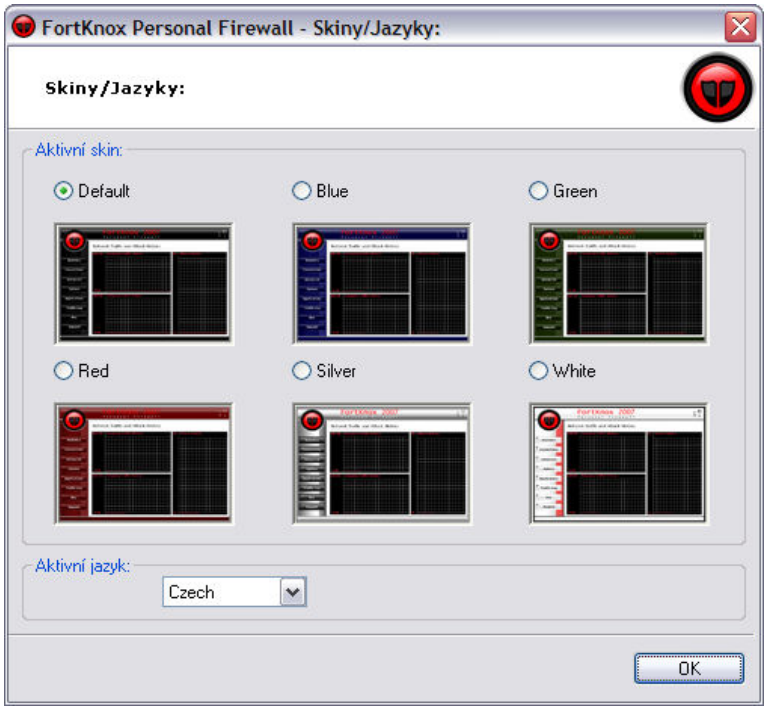
f) Vyberte složku v ***Start Menu***, kde se má nacházet zástupce. Klikněte na ***Další***, abyste mohli pokračovat.



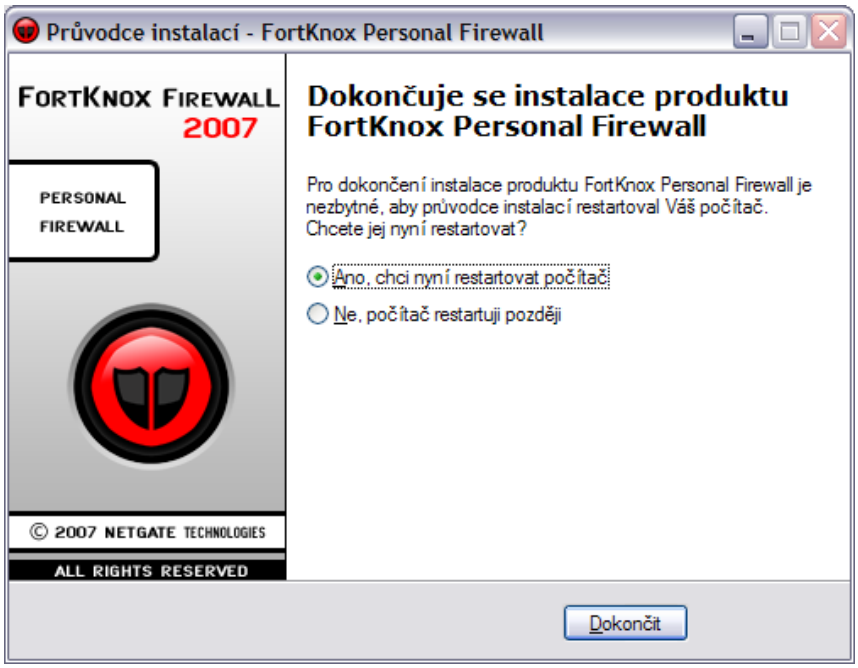
g) Zkontrolujte všechny doplňující úlohy, které se mají provést (vytvoření zástupce na ploše a v panelu rychlého spuštění). Doporučujeme vybrat všechny možnosti. Klikněte na ***Další***, pro pokračování.



h, V následujícím kroku se zobrazí volba vzhledu a jazyku. Umožní Vám vybrat si vzhled a jazyk, který Vám nejvíce vyhovuje.



i, Pro dokončení instalace je potřebné, aby byl počítač restartován. Zvolte tlačítko ***Dokončit*** pro restart počítače.



Pro úspěšný proces instalace **je potřebné, aby byl Váš systém restartován** a aby se **FortKnox Personal Firewall 2007** úspešně spustil. První spuštění po restartu může trvat déle na operačních systémech Windows Vista.

3. Aktivace programu

3.1. Zkušební verze

Z webové stránky FortKnox Personal Firewall si můžete stáhnout zkušební verzi programu **FortKnox Personal Firewall 2007**. Po instalaci zkušební verze funguje 15 dní. Tato verze je plně funkční s tím, že databáze z internetu se načítá pouze jednou a to hned po instalaci programu.

V průběhu 15 dní musíte program zaregistrovat pomocí registračních údajů k aktivaci plné verze programu **FortKnox Personal Firewall 2007**. Zakoupené registrační údaje můžete zadat kdykoliv během zkušební doby i po uplynutí této doby.

3.2. Nákup

V menu ***Buy*** (Koupit) vyberte **Buy Now** (Koupit nyní). Váš internetový prohlížeč se spustí s registrační webovou stránkou.

3.3. Registrace

V menu ***Buy*** klikněte na tlačítko **Enter serial** (vložit číslo). Zobrazí se registrační okno. Zakoupením programu **FortKnox Personal Firewall 2007** dostanete registračné údaje;

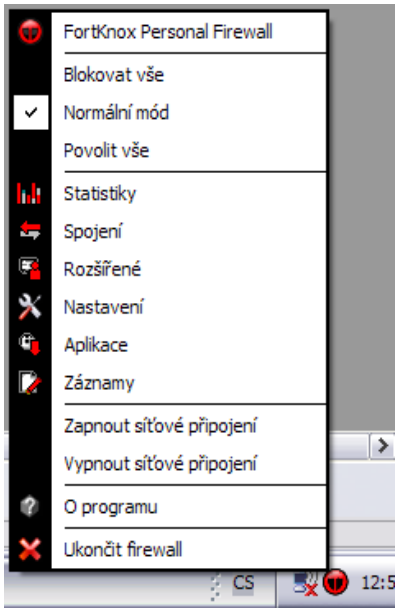
registrační jméno, registrační e-mail a sériové číslo. Tyto údaje musíte přesně vložit do registračního okna. Dávejte si pozor na to, že v sériovém čísle jsou pouze znaky **A-F** a **čísla**. Registrační jméno je bez diakritiky!

4. Práce s FortKnox Personal Firewall 2007

Po úspešné instalaci programu **FortKnox Personal Firewall 2007** na Vašem počítači se zobrazí ikona **FortKnox Personal Firewall 2007** na Vaší ploše. Dvoj-kliknutím na tuto ikonu se spustí program **FortKnox Personal Firewall 2007**

4.1. Ikona v systémové lište (vedle hodin)

Když je aplikace spuštěná, vidíte malou červeno-černou ikonku v systémové liště vedle hodin, která indikuje, že aplikace běží. Kliknutím pravým tlačítkem na tuto ikonu se zobrazí následující menu:



Jsou přístupné následující volby:

FortKnox Personal Firewall – zvolte tuto možnost pro zobrazení nebo skrytí hlavního okna aplikace.

Blokovat vše – pokud je tato volba aktivní, všechny přicházející a odcházející přenosy jsou blokovány.

Normální mód – pokud je tato volba aktivní, firewall bude filtrovat přenosy na základě nastavených pravidel.

Povolit vše – pokud je tato volba aktivní, všechny přicházející a odcházející přenosy jsou povoleny.

Statistiky – zobrazuje statistické informace o přicházejících a odcházejících přenosech a útocích.

Spojení – zobrazuje aktivní síťové spojení.

Rozšířené – umožňuje nastavit rozšířené uživatelské pravidla filtrování přenosů.

Nastavení – tato volba zobrazí dialog aplikace umožňující konfiguraci.

Aplikace – zobrazí pravidla pro jednotlivé aplikace.

Záznamy – zobrazí záznamy všech síťových přenosů kontrolovaných firewallem.

Zapnout síťové připojení – povolí všechny síťové rozhraní v systému.

Vypnout síťové připojení – vypne všechny síťové rozhraní v systému.

O programu – tato volba zobrazí dialogové okno s informacemi o programu.

Ukončit firewall – tato volba ukončí aplikaci.

4.2. Potvrzení síťového spojení

FortKnox Personal Firewall 2007 umožňuje potvrzení síťového spojení v reálném čase. Uživatelé mají možnost povolit nebo zakázat síťové spojení pro jednotlivé aplikace.

Před uskutečněním spojení se zobrazí následující dialog:

Tento dialog umožňuje následující akce:

Ano – spojení bude povoleno.

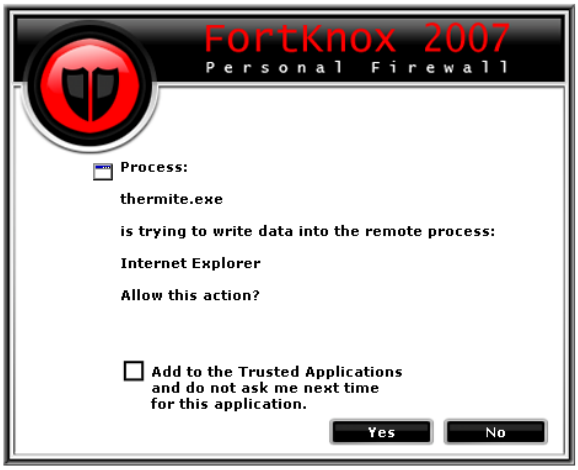
Ne – spojení bude zakázáno.

Zapamatovat si tuto odpověď a více se již na tuto aplikaci nedotazovat – firewall si uloží Vaše rozhodnutí a příště se již nebude opět ptát. Pravidla pro jednotlivé aplikace se dají změnit v menu **Aplikace**.

4.3. Potvrzení aktivity procesu

FortKnox Personal Firewall 2007 umožňuje potvrzení pro procesy, pro některé podezřelé aktivity. Uživatelé mají volbu povolit nebo zakázat takovou volbu.

Před touto akcí se zobrazí následující dialog:



Tento dialog umožňuje následující akce:

Ano – akce se vykoná.

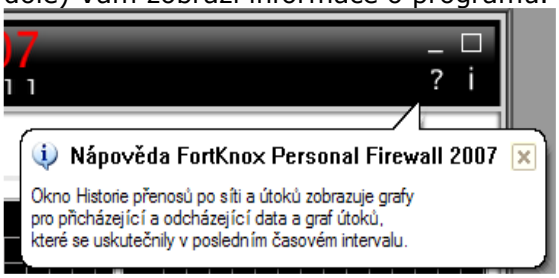
Ne – akce bude zamítnuta.

Přidat k důvěryhodným aplikacím a vícekrát se již na tuto aplikaci nedotazovat – firewall uloží Vaše rozhodnutí a příště se již nebude ptát. Pokud chcete resetovat tyto pravidla, zvolte tlačítko **Resetovat** v menu **Nastavení/Rozšírené** (vedle možnosti **Povolit systém ochrany procesů**). Poznámka: Systém ochrany procesů musí být zapnutý pto potvrzování aktivity procesů.

Potvrzovací aktivity jsou:
- Zápis do cizího procesu
- Spuštění internetového prohlížeče
- Změny pozadí (Active desktop)
- Změny registračního klíče AppInit_DLLs

4.4. Ovládání hlavního okna

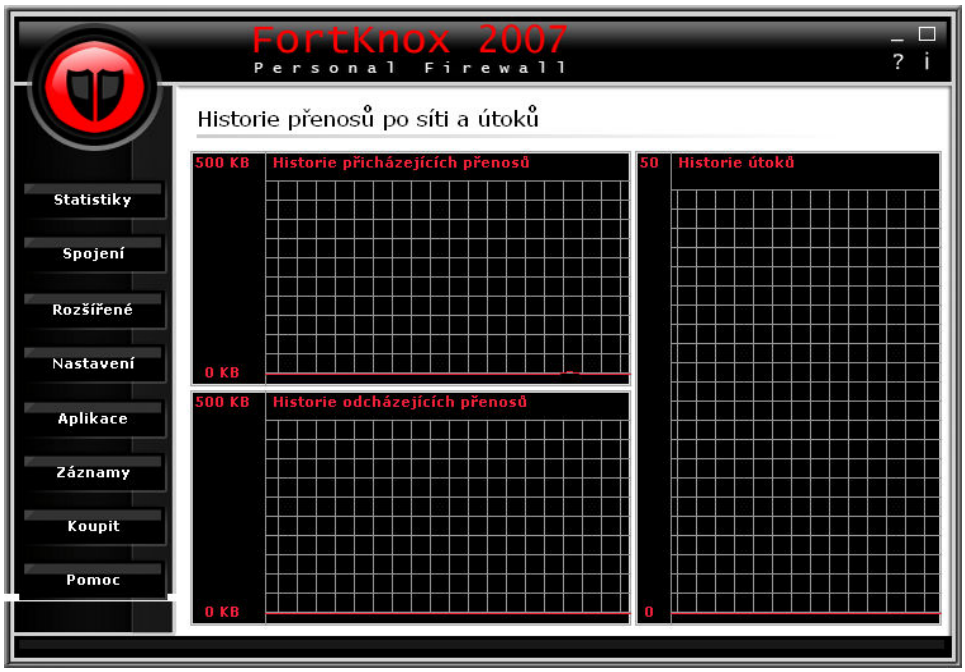
Hlavní okno obsahuje čtyři ikony v pravém horním rohu. Tlačítkem **Minimalizovat** (vlevo nahoře) schováte okno do systémové lišty. Tlačítkem **Maximalizovat/Obnovit** (vpravo nahoře) zvětšíte okno přes celou obrazovku nebo jej vrátíte do původní velikosti. Tlačítkem **Nápověda** (vlevo dole) zobrazíte informace o aktuálním okně. Tlačítko **Informace** (vpravo dole) Vám zobrazí informace o programu.



5. Hlavní okno

5.1. Statistiky

Dialog **Statistiky** zobrazuje informace o historii přicházejících a odcházejících přenosů a historii uskutečněných útoků.



5.2. Spojení

Dialog **Spojení** zobrazuje všechny aktivní síťové spojení v systému. Každá položka zobrazuje lokální a vzdálené IP adresy nebo jen lokální IP adresy pro čekající stavy, stav spojení a asociovaný proces.

Detaily – zobrazí detaily o zvolené položce.

Blokovat spojení – zablokuje zvolené síťové spojení.

Trace Route – zobrazí cestu sítí k zvolené cílové adrese. (Poznámka: tato metoda používá ICMP zprávy a některé systémy mohou tyto přenosy blokovat)

WhoIs Lookup – vyhledává cíl zvolené položky nebo zadané domény ve whois databázi.

Ukončit proces – ukončí proces zvolené položky.

5.3. Rozšířené

Dialog **Rozšířené** umožňuje editaci rozšířených aplikačních pravidel. Tyto pravidla mají **vyšší prioritu** než aplikační pravidla.

Přidat pravidlo – přidá nové rozšířené pravidlo.

Editovat pravidlo – edituje zvolené rozšírené pravidlo.

Odstranit – smaže označené rozšírené pravidlo.

Dialog **Přidat/Editovat rozšířené pravidla**:

Popis – pole může obsahovat libovolný text na identifikaci pravidla.

Protokol – typ protokolu, který je používán na komunikaci mezi dvěma počítači, zvolte **Kterýkoliv** protokol pro zvolení všech protokolů.

Akce – akce, která se uskuteční pro specifikované pravidlo; **Povolit** – povolí spojení, **Zakázat** – zakáže spojení.

Směr – může být přicházející nebo odcházející, zvolte 'Jakýkoliv' pro oba směry.

Proces – pole může být prázdné pro aplikaci na všechny aplikace nebo použijte tlačítko **...** na limitování pravidel pro specifickou aplikaci. Pro limitování pravidla ke specifické časové periodě nebo uživateli, zvolte seznamy **Uživatel** a **Časové omezení**.

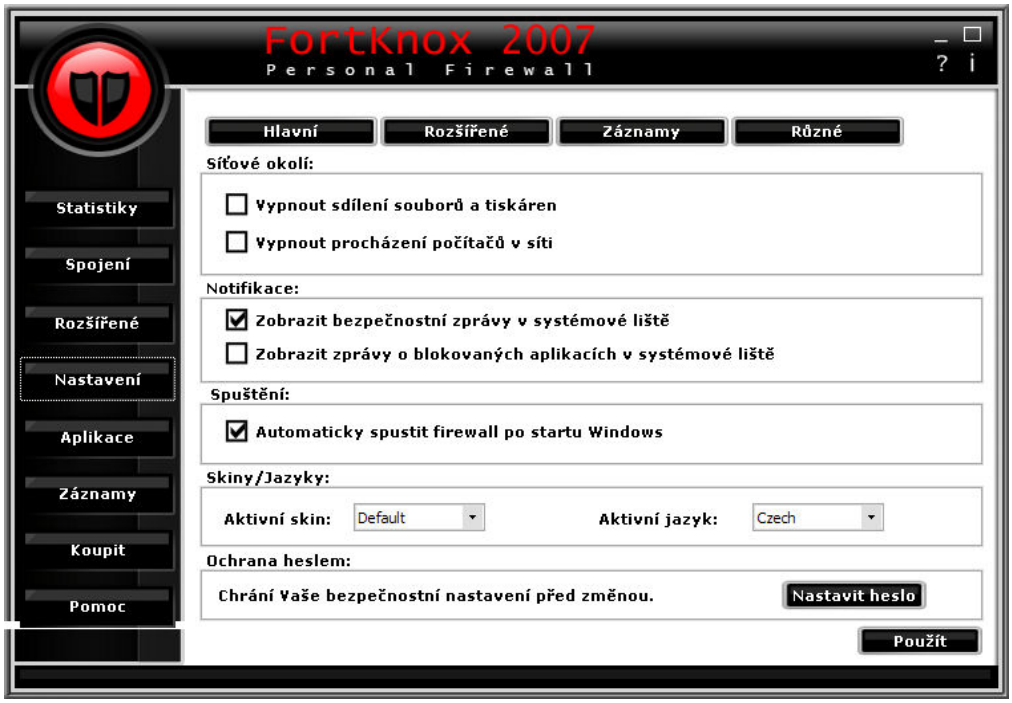
Lokální počítač - je IP adresa Vašeho počítače. Váš počítač může mít více než jednu síťovou kartu. Zvolte možnost **Všechny adresy** pro apliakci na všechny Vaše síťové připojení nebo můžete specifikovat individuální síťové karty/adresy zadáním MAC adresy nebo IP adresy. Při zadání IP adresy máte možnost specifikovat **Port** a **Masku podsítě**.

Vzdálený počítač - je IP nebo MAC adresa vzdáleného počítače. Adresa **0.0.0.0** s maskou **Jakákoliv** znamená všechny IP adresy.

5.4. Nastavení

Dialog **Nastavení** umožňuje konfiguraci jednotlivých funkcí **FortKnox Personal Firewall 2007**.

Záložka Hlavní:



Vypnout sdílení souborů a tiskáren – když je tato volba aktivní, všechen přístup k Vašim souborům a tiskárnám po síti je blokován.

Vypnout procházení počítačů v síti – aktivní volba blokuje procházení sdílených zdrojů síťových počítačů.

Nastavit heslo – tlačítko umožňuje chránit nastavení firewallu před jeho změnou nastavením hesla.

Zobrazit bezpečnostní zprávy v systémové liště – když je tato volba aktivní, zobrazí se informační bublina, pokud nastane bezpečnostní událost.

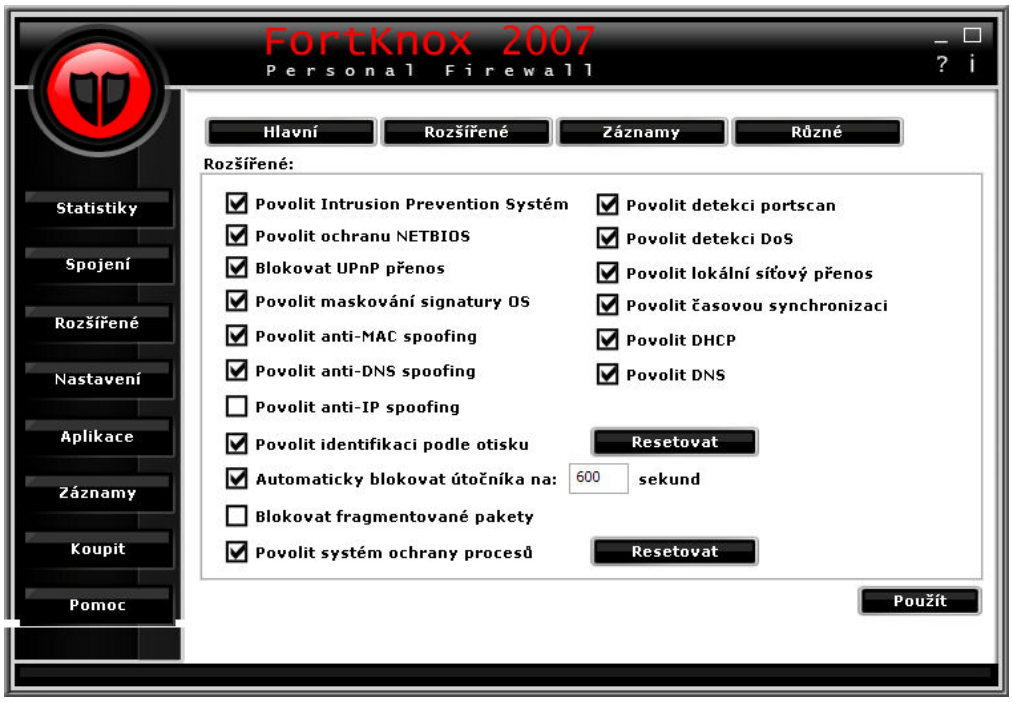
Zobrazit zprávy o blokovaných aplikácích v systémové liště – pokud je tato volba aktivní, zobrazí se informační bublina pokud dojde k blokaci některé aplikace.

Automaticky spustit firewall při startu Windows – když je tato volba aktivní, firewall bude spuštěn při startu systému Windows.

Pokud chcete změnit nastavení jazyku a skinu podle Vašich preferencí, zvolte seznamy **Aktivní jazyk** a **Aktivní skin**.

Pro aplikování změny v záložce **Hlavní**, zvolte tlačítko **Použít**.

Záložka Rozšířené:



Povolit Intrusion Prevention System (IPS) – IPS je integrovaný Intrusion Detection System (IDS) , ktoerý zjišťuje známé hrozby v paketovém toku a aktivně na ně reaguje. Pokud je hrozba zjištěna na základě signatury, uživatel je automaticky upozorněn a podle nastavené akce je zablokovaná.

Povolit ochranu NETBIOS – volba automaticky blokuje všechnu NETBIOS komunikaci z počítačů mimo lokální podsítě.

Blokovat UPnP přenos – volba blokuje UPnP přenosy, které se často používajú na DoS útoky. Upozornění: pokud některé Vaše aplikace používají UPnP protokol měli byste tuto volbu vypnout.

Povolit maskování signatury OS – volba blokuje běžné metody útočníků na zjištění Vašeho operačního systému.

Povolit anti-MAC spoofing – volba blokuje všechny neočekávané ARP přenosy, které nebyly vyžádané Vašim systémem. MAC spoofing je způsob jak se napojit na komunikaci mezi dvěmi počítači s cílem získat přístup na jeden z počítačů.

Povolit anti-DNS spoofing – volba blokuje všechny neočekávané DNS odezvy na Váš systém na prevenci DNS útoků.

Povoliť anti-IP spoofing – táto možnosť randomizuje sekvenčné číslo pre každý komunikačný paket ako prevencia nabúrania komunikácie pomocou IP spoofing útoku. Upozornenie: niektoré sieťové karty nie sú s týmto nastavením kompatibilné.

Povolit identifikaci podle otisku – volba ověřuje každou aplikaci na změny v souboru. Pokud chcete resetovat všechny otisky, zvolte tlačítko **Resetovat**.

Automaticky blokovat útočníka na: - když je tato volba zapnuta, všechny útoky na Váš systém jsou automaticky blokované na určený čas.

Blokovat fragmentované pakety – když je tato volba zapnutá, všechny fragmentované IP pakety jsou blokované.

Povolit systém ochrany procesů – volba zabezpečuje integritu aplikací a potvrzuje potencionálně nebezpečné aktivity procesů. Pokud je volba zapnutá, dialog **Potvrzení aktivity procesu** se zobrazí, v případě, že je taková aktivita zjištěna. Pokud chcete resetovat všechny důvěryhodné aplikace, zvolte tlačítko **Resetovat**.

Povolit ochranu AppInit DLL – volba upozorňuje na změny tohto registru aplikacemi.

Povolit detekci portscan – volba zjišťuje, upozorňuje a blokuje skenování Vašich portů, což představuje běžnou techniku útočníků na zjištění otevřených portů a či jsou vhodné na útoky.

Povolit detekci DoS – volba kontroluje všechen přenos na známé Denial of Service (DoS) útoky, které přetěžují systémové služny a blokují použití služeb pro běžné uživatele.

Povolit lokální síťový přenos – volba umožňuje přenosy po lokální síti.

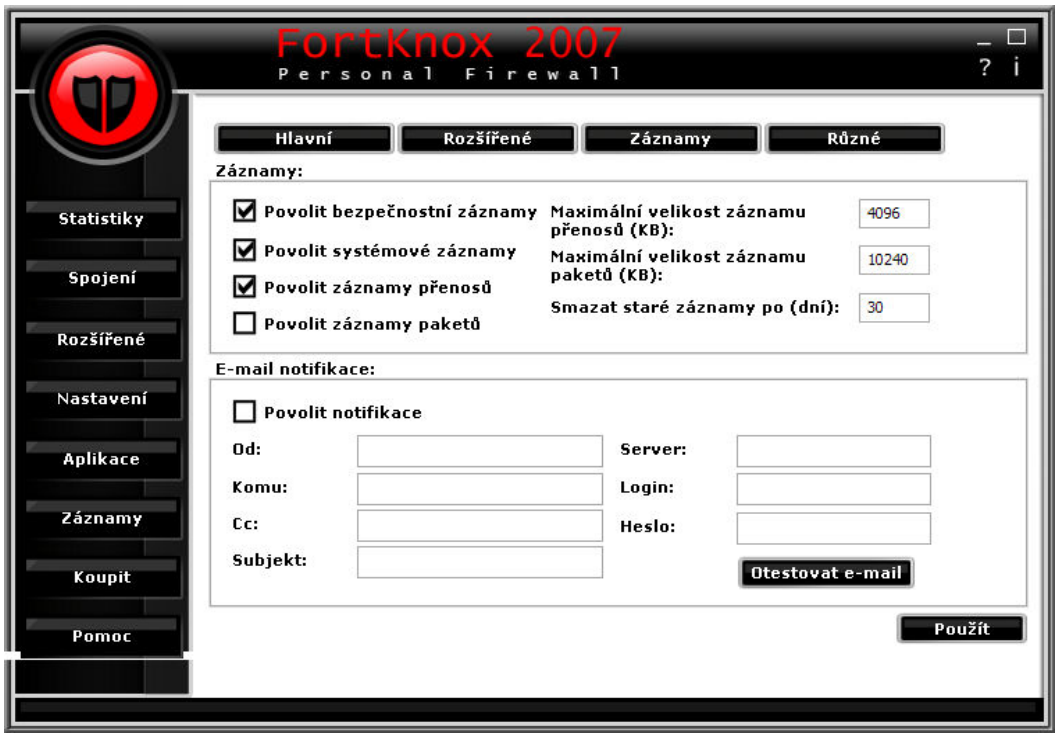
Povolit časovou synchronizaci – volba umožňuje přenosy pro časovou synchronizaci pomocí internetových serverů.

Povolit DHCP – volba umožňuje Dynamic Host Configuration Protocol přenosy, které bývají použity na automatické přidělováníIP adres a jiné TCP/IP konfigurační informace. Upozornění: Pokud vypnete toto nastavení a potřebujete DHCP pro korektní fungování systému, musíte vytvořit rozšířené pravidlo pro UDP pakety na vzdálených portech 67 a 68.

Povolit DNS – volba umožňuje překlad doménových jmen na IP adresy. Upozornění: pokud vypnete toto nastavení, musíte vytvořit rozšířené pravidlo pro UDP přenosy na vzdálený port 53.

Pro aplikování změn v záložce **Rozšířené**, zvolte tlačítko **Použít**.

Záložka Záznamy:



Povolit bezpečnostní záznamy – volba povoluje zaznamenávání důležitých a bezpečnostních událostí.

Povolit systémové záznamy – volba povoluje zaznamenávání událostí vztahující se k funkčnosti firewallu.

Povolit záznamy přenosů - volba povoluje zaznamenávání všech přicházejících a odcházejících síťových přenosů.

Povolit záznamy paketů – volba povoluje zaznamenávání komunikačních paketů včetně dat..

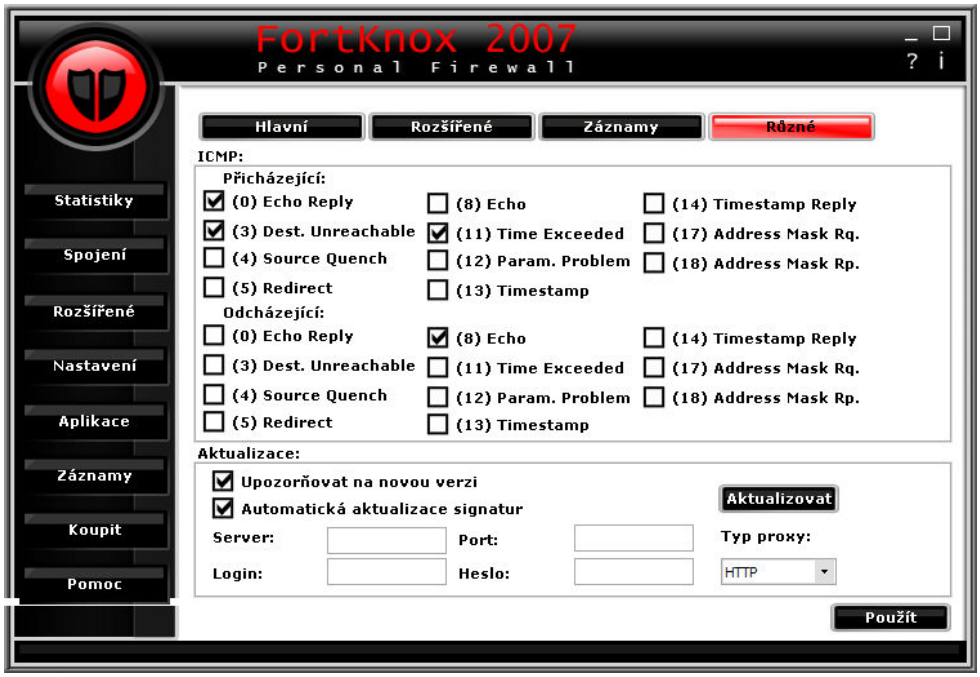
Pokud chcete omezit velikost záznamů přenosů a paketů, použijte volby **Maximální velikost záznamů přenosů** a **Maximální velikost záznamů paketů**.

Smazat staré záznamy po (dní) – volba nastavuje počet dní po kterých jsou všechny staré záznamy smazány. Nastavení hodnoty na nulu toto nastavení vypne.

Povolit notifikace – volba zapne e-mailové upozornění v případech, když nastane bezpečnostní událost. Na otestování Vašich nastavení e-mailu použijte tlačítko **Otestovat E-Mail**.

Pro aplikování změny v záložce **Záznamy**, zvolte tlačítko **Použít**.

Záložka Různé:



ICMP – nastavení pro přicházející a odcházející pakety. Měnit toto nastavení se doporučuje jen zkušeným uživatelům.

Upozorňovat na novou verzi – volba Vás upozorní na nové verze programu FortKnox Personal Firewall.

Automatická aktualizace signatur – když je tato volba aktivní, nové signatury se automaticky stáhnou a nainstalují ze serveru. Pro ruční aktualizaci zvolte tlačítko Aktualizovat.

Pro aplikaci změny v záložce **Různé**, stiskněte tlačítko **Použít**.

5.5. Aplikace

Dialog **Aplikace** zobrazuje všechny specifické pravidla aplikací. Každé pravidlo může mít akci nastavenou na povolit, zakázat nebo Ptát se a každá aplikace, která byla potvrzené při ptaní se, je zde zobrazená.

Označit vše – označí všechny položky v seznamu.

Odznačit vše – odznačí všechny položky v seznamu.

Povolit – nastaví zvolené položky do módu povolit; přenos takového procesu bude automaticky povolen.

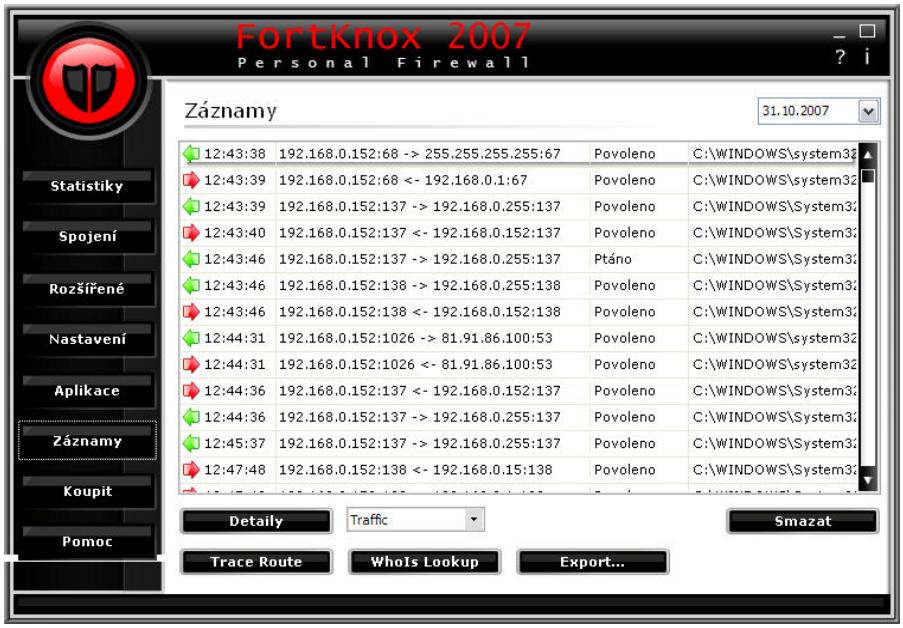
Zakázat – nastaví zvolené položky do módu zakázat; přenos takového procesu bude automaticky zakázán.

Ptát se – nastaví zvolené položky do módu ptát se; pro potvrzení takového procesu se zobrazí dialog.

Odstranit – tato volba smaže zvolenou položku/pravidlo ze seznamu.

5.6. Záznamy

Dialog **Záznamy** zobrazuje všechny síťové přenosy kontrolované programem FortKnox Personal Firewall 2007.



Detaily – zobrazí detaily o zvolené položce.

Trace Route – zobrazí cestu sítí ke zvolené cílové adrese. (Poznámka: tato metoda využívá ICMP zprávy a některé systémy můžou tyto přenosy blokovat)

WhoIs Lookup – vyhledává cíl zvolené položky nebo zadané domény ve whois databázi.

Export... – uloží aktivní záznam do souboru.

Smazat – smaže uložený záznam/záznamy.

Na **přepínání** mezi jednotlivými **typy** záznamů zvolte seznam vedle tlačítka **Detaily**.

5.7. Koupit/O programu

Ve zkušební verzi se zobrazuje dialog s vlastnostmi FortKnox Personal Firewall; v registrované verzi se zde zobrazují informace o registrovaném uživateli a informace o databázi. Po registraci se změní tlačítko **Koupit** na **O programu** po restartu programu.

Vložit číslo – stiskem tohto tlačítka má uživatel možnost vložit registrační informace; registrační okno vyskočí.

Koupit nyní – stiskem tohto tlačítka Váš standardní internetový prohlížeč otevře stránku s on-line obchodem, kde si můžete produkt zakoupit.

5.8. Technická podpora

Dialog **Technické podpory** umožňuje uživateli poslat e-mail přímo technickému týmu FortKnox Personal Firewall. K odeslání zprávy vyplňte e-mail, jméno a popis problému a stiskněte tlačítko **Odeslat.** Můžete též přidat přílohu stiskem tlačítka **...** .

6. Technická podpora

Technický tým podpory je Vám dostupný na support@netgate.sk.

Všechny ostatní otázky týkající se prodeje, prosím, posílejte na netgate@netgate.sk