Rodičovská kontrola

V sekcii Rodičovská kontrola môžete konfigurovať nastavenia rodičovskej kontroly, ktoré vám umožnia ochrániť vaše deti a nastaviť obmedzenia pri používaní zariadení a služieb. Cieľom je zabrániť deťom a dospievajúcim v prístupe na stránky s nevhodným alebo škodlivým obsahom.

Rodičovská kontrola vám umožňuje blokovať web stránky, ktoré môžu obsahovať potenciálne nevhodný obsah. Okrem toho môžu rodičia zakázať prístup na vyše **40 predvolených kategórii web stránok**. Aktiváciu rodičovskej kontroly pre konkrétny používateľsky účet je možné zabezpečiť podľa nasledovných inštrukcii:

1. Rodičovská kontrola je v predvolenom nastavení programu ESET Smart Security vypnutá. Sú dve možnosti, ako aktivovať funkciu rodičovskej kontroly:
    - Kliknutím v hlavnom okne programu na záložku **Nastavenia** a potom vedľa možnosti Rodičovská kontrola na **Vypnutá**. Týmto sa rodičovská kontrola prepne do stavu **Zapnutá**.
    - Stlačte F5 pre otvorenie stromu pokročilých nastavení, kliknite na **Rodičovská kontrola** a potom označte zaškrtávacie políčko **Integrácia do systému**.
2. V hlavnom okne programu kliknite na **Nastavenia** a potom na **Rodičovská kontrola**. Napriek tomu, že sa rodičovská kontrola objavuje v stave **Zapnutá**, musíte ešte inicializovať používateľský účet kliknutím na **Nedefinovaná**. V okne Nastavenie účtu zadajte požadovaný vek a vyberte jednu rolu z rolovacieho menu. Potom bude rodičovská kontrola aktívna pre daný používateľský účet. Kliknite na **Nastavenia...** pod konkrétnym používateľským účtom, ak si želáte meniť kategórie web stránok, ktoré chcete povoliť, alebo blokovať. Toto zabezpečuje záložka ***Filtrovanie obsahu webu***. Pre povolenie či blokovanie vlastných web stránok (ktoré nepatria do ani jednej predvolenej kategórie), kliknite na záložku ***Blokované a povolené stránky***.

Po kliknutí na možnosť **Rodičovská kontrola** v časti **Nastavenia** (z hlavného okna ESET Smart Security) sa prepnete do hlavného okna, rozdeleného na tri časti

1. **Rodičovská kontrola.** Po kliknutí na možnosť **Zapnutá** sa objaví okno Dočasné vypnutie ochrany kde môžete nastaviť časový interval počas ktorého je ochrana vypnutá. Táto možnosť sa potom zmení na **Vypnutá** a doleuvedené možnosti nebudú k dispozícii.

Zmeny nastavení je v ESET Smart Security možné chrániť heslom. Toto heslo je možné nastaviť v sekcii ***Prístup k nastaveniam.*** Ak nie je nastavené žiadne heslo na ochranu nastavení, pod možnosťou Vypnúť rodičovskú kontrolu sa zobrazí varovanie – *Rodičovská kontrola nie je chránená heslom!* – a možnosť **Nastaviť heslo**... bude dostupná. Obmedzenia nastavené v rodičovskej kontrole ovplyvnia iba štandardné používateľské účty. Pretože administrátor vie prekonať všetky obmedzenia, tieto nebudú mať želaný účinok.

Komunikácia pomocou protokolu HTTPS (SSL) nie je v predvolenom nastavení kontrolovaná. Z tohto dôvodu nemôže Rodičovská kontrola blokovať web stránky, ktorých adresa začína s *https://*. Pre povolenie tejto funkcionality kliknite na možnosť **Zapnúť** hneď vedľa varovného hlásenia s názvom **Skenovanie SSL-kryptovaných stránok (HTTPS) je vypnuté!**, alebo povoľte možnosť **Použiť kontrolu SSL protokolu vždy** v časti **Pokročilé nastavenia** (F5) **> Web a mail > Filtrovanie protokolov > SSL**.

Poznámka: *Pre správne fungovanie modulu Rodičovská kontrola je nevyhnutné, aby bola zapnutá aj Kontrola aplikačných protokolov, Kontrola protokolu HTTP a integrácia Personálneho firewallu do systému. Všetky spomínané funkcionality sú štandardne zapnuté.*

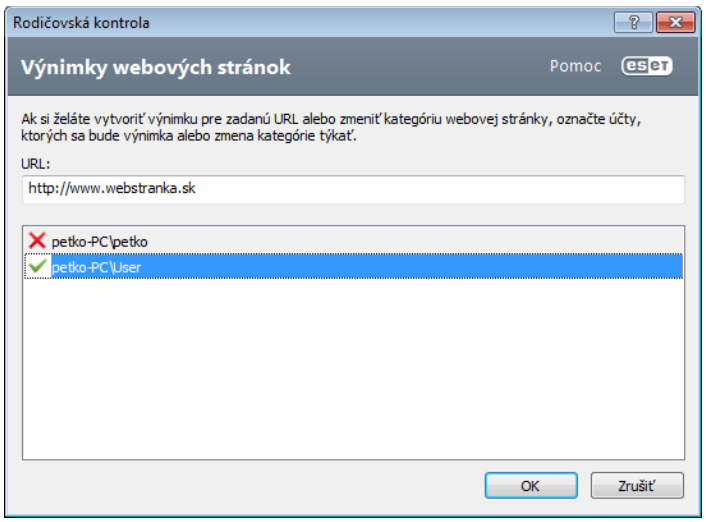
2. **Druhá časť patrí používateľským účtom** vo Windowse. Ak ste si vytvorili nový účet v **Pokročilé nastavenia > Rodičovská kontrola > Účty > Pridať**, zobrazí sa v tejto časti vo forme Doména\Účet s atribútom **Zapnutá**. Kliknutím na **Zapnutá** deaktivujete účet, a naopak. Pod aktívnym účtom je možnosť ***Nastavenia***.... Tu sa nachádza zoznam povolených kategórií pre tento účet, blokované a povolené stránky.

Dôležité: Pre vytvorenie používateľského účtu (napr. pre svoje dieťa) na platforme Windows 7 a Windows Vista môžete postupovať aj podľa nasledovných inštrukcií:

a. Otvorte okno **Používateľské kontá** tak, že kliknete na tlačidlo **Štart**, kliknete na položku **Ovládací panel**, kliknete na položku **Používateľské kontá**.
b. Kliknite na položku **Spravovať iné konto**. Vyžaduje sa oprávnenie správcu. Ak sa zobrazí výzva na zadanie hesla správcu alebo potvrdenie, zadajte heslo alebo potvrďte akciu.
c. Kliknite na položku **Vytvoriť nové konto**.
d. Zadajte názov, ktorý chcete priradiť používateľskému kontu, kliknite na typ konta a potom kliknite na položku **Vytvoriť konto**.
e. V programe ESET Smart Security zatvorte a znova otvorte sekciu Rodičovská kontrola kliknutím **na Setup > Parental control**.

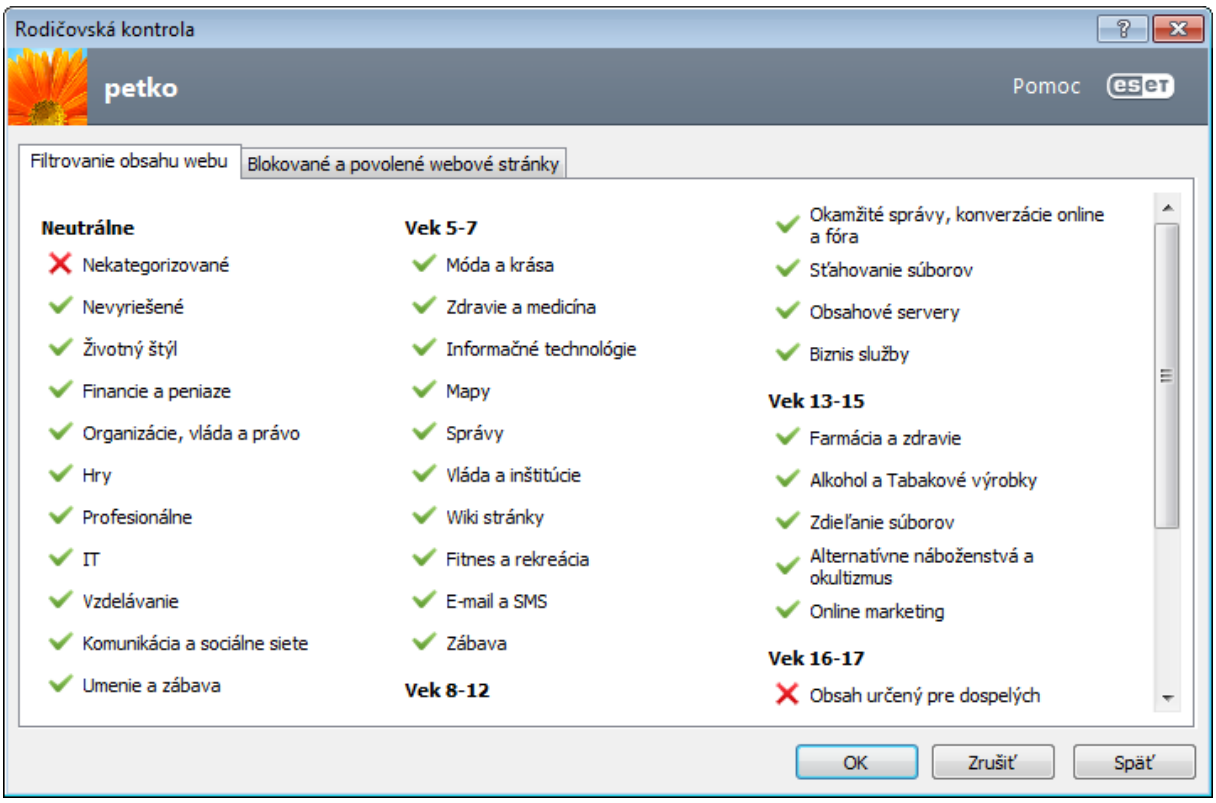
3. Posledná časť obsahuje dve možnosti

Nastaviť výnimku pre web stránku... – Toto je rýchly spôsob ako nastaviť výnimku pre web stránku pre konkrétny účet. Vpíšte adresu web stránky do textového pola **URL** a zvoľte účet zo zoznamu nižšie. Ak zaškrtnete políčko **Blokovať**, web stránka bude pre tento účet zablokovaná. Ak toto políčko necháte prázdne, stránka bude povolená. Výnimky definované v tejto záložke sú nadradené definovaným kategóriám pre jednotlivé roly. To znamená, že ak je napríklad pre určitý účet blokovaná kategória **Správy**, ale zároveň je pre ňu povolená výnimka pre stránku so správami – pre tento účet bude táto stránka prístupná. Zmeny vykonané v tejto záložke si môžete overiť v sekcii ***Blokované a povolené stránky***.



Zobraziť protokol – Zobrazí sa podrobný protokol o činnosti modulu Rodičovská kontrola (blokované stránky, účet pre ktorý bola stránka zablokovaná, dôvod zablokovania, atď.). Tiež môžete tento protokol filtrovať (pomocou tlačidla **Filtrovať**...) podľa vami zvolených kritérií.

Zoznam povolených kategórií web stránok
Ak je políčko pri kategórii zaškrtnuté, je povolená. Odškrtnite špecifickú kategóriu pre jej zablokovanie pre zvolený účet. Podržte kurzor myši nad kategóriou pre zobrazenie typu stránok ktoré spadajú do tejto kategórie.



Posúvaním myši po jednotlivých kategóriách sa zobrazí zoznam web stránok, ktoré spadajú do tejto kategórie. Nasleduje prehľad niektorých kategórii (skupín), s ktorými nemusí byť používateľ na prvý pohľad oboznámený:

- **Rôzne** – Spravidla privátne (lokálne) IP adresy ako intranet, 127.0.0.0/8, 192.168.0.0/16, a podobne. Ak obdržíte chybový kód 403 alebo 404, webová stránka spadá do tejto kategórie.

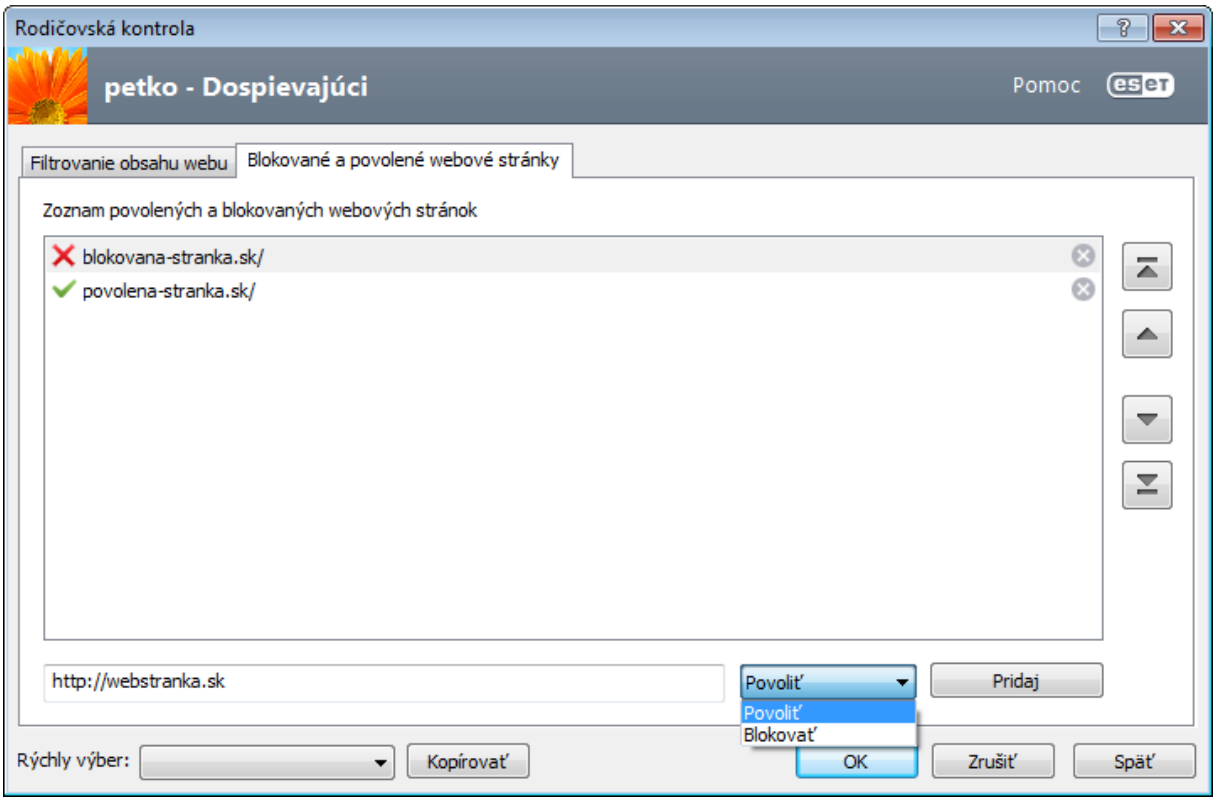
- **Nevyriešené** – Táto kategória zahŕňa web stránky, ktoré nebolo možné zaradiť kvôli chybe, ktorá nastala pri pokuse pripojiť sa na databázu rodičovskej kontroly.

- **Nekategorizované** – Neznáme web stránky, ktoré ešte neboli pridané do databázy rodičovskej kontroly.

- **Proxy servery** – Web stránky typu ako anonymizéry, redirektory a verejné proxy servery môžu byť použité na získanie (anonymného) prístupu na web stránku, ktoré sú väčšinou zakázané filtrom rodičovskej kontroly.

- **Zdieľanie súborov** – Tieto web stránky obsahujú veľké množstvo dát ako napr. fotky, videá a elektronické knihy. Existuje riziko, že tieto stránky môžu obsahovať aj potenciálne urážlivý materiál alebo obsah pre dospelých.

Blokované a povolené stránky
URL adresu stránky vpíšte do prázdneho políčka pod zoznamom, kliknite na **Pridať** alebo **Blokovať** a stlačte **Pridaj** pre pridanie do zoznamu. Pre zmazanie zo zoznamu kliknite na URL adresu v zozname a potom na tlačidlo *„x"* nachádzajúce sa vpravo v každom jednom riadku.



V zoznamoch URL adries nie je možné používať špeciálne znaky * a ?. Adresy s viacerými TLD musia byť zadané manuálne *(webstranka.com*, *webstranka.sk*, atď.). Ak vložíte adresu domény do zoznamu, všetok obsah nachádzajúci sa na tejto doméne a všetky jej subdomény (napr. *sub.stranka.com*) budú blokované alebo povolené – podľa toho, akú akciu pre URL adresy ste si zvolili.

Poznámka: *Blokovanie alebo povolenie špecifickej internetovej stránky môže byť presnejšie ako blokovanie alebo povolenie celej kategórie internetových stránok. Buďte opatrný pri zmene týchto nastavení a pridávaní kategórií/ stránok do zoznamov.*

Filtrovanie protokolov
Antivírusový monitoring aplikačných protokolov je vykonávaný prostredníctvom skenovacieho jadra ThreatSense, v ktorom sú sústredené všetky pokročilé metódy detekcie škodlivého softvéru. Kontrola pracuje nezávisle od používaného internetového prehliadača, alebo poštového klienta. Pre kryptovanú komunikáciu (SSL) otvorte **Filtrovanie protokolov > SSL**.

Zapnúť kontrolu aplikačných protokolov – HTTP(S), POP3(S) a IMAP(S) komunikácia bude kontrolovaná antivírusovým skenerom.

Poznámka: Na systémoch Windows Vista so Service Pack 1; Windows server 2008 a novších je použitý odlišný spôsob kontroly komunikácie (využíva sa nová architektúra Windows Filtering Platform) ako na starších systémoch. Z tohto dôvodu nie sú tieto nastavenia dostupné:

- **Len na základe portov pre HTTP a POP3** – Pri výbere tejto možnosti je kontrolovaná len komunikácia, ktorá prebieha na portoch všeobecne známych pre tieto služby.
- **Len pre aplikácie označené ako internetové prehliadače alebo poštové klienty** – Filtrovaná bude komunikácia tých aplikácií, ktoré boli označené ako prehliadače alebo poštoví klienti (**Web a mail > Filtrovanie protokolov > Prehliadače**).
- **Na základe portov a aplikácií označených ako internetové prehliadače alebo poštoví klienti** – Zahŕňa obe predchádzajúce možnosti

HTTP, HTTPS
Štandardne je ESET Smart Security nakonfigurovaný na používanie noriem väčšiny internetových prehliadačov. Konfigurácia kontroly HTTP je možná v časti **Zobraziť pokročilé nastavenia > Web a mail > Ochrana prístupu na web**, položka **HTTP, HTTPS**. V hlavnom okne **Kontrola protokolu HTTP/HTTPS** môže používateľ túto kontrolu aktivovať alebo deaktivovať možnosťou **Aktivovať kontrolu protokolu HTTP**. Tiež je možné definovať čísla portov, na ktorých v systéme prebieha HTTP komunikácia. Štandardne sú prednastavené hodnoty 80 (HTTP), 8080 a 3128 (pre Proxy server).

ESET Smart Security podporuje kontrolu šifrovanej komunikácie HTTPS. Pri tejto komunikácií sú prenášané údaje medzi serverom a klientom zašifrované. Kontrolovaná je komunikácie šifrovaná pomocou SSL (Secure Socket Layer), alebo TLS (Transport Layer Security). HTTPS je možné filtrovať v dvoch režimoch:

Nepoužívať kontrolu protokolu HTTPS – Šifrovaná komunikácia nebude kontrolovaná.

Používať kontrolu protokolu HTTPS pre vybrané porty – Kontrolovaná bude len komunikácia cez porty definované v nastavení **Porty používané protokolom HTTPS**. Je to zoznam portov šifrovanej internetovej komunikácie, predvolený je štandardný port (443).
Kryptovaná komunikácia sa štandardne nekontroluje. Pre kontrolu kryptovanej komunikácie a pre povolenie možnosti nastavenia kontroly protokolu, otvorte okno ***Kontrola protokolu SSL*** v Pokročilých nastaveniach (**Web a mail > Filtrovanie protokolov > SSL**) a označte možnosť **Použiť kontrolu protokolu SSL vždy**.

Kontrola protokolu SSL
ESET Smart Security umožňuje aj kontrolu protokolov zapuzdrených v protokole SSL. Kontrolu možno prispôsobiť podľa toho, či certifikát využívaný danou SSL komunikáciou je dôveryhodný, neznámy, alebo je v zozname certifikátov, pre ktoré sa nebude vykonávať kontrola obsahu v protokole SSL.

Použiť kontrolu protokolu SSL vždy (vylúčené a dôveryhodné certifikáty ostanú platné) – Pri tomto nastavení sa bude vykonávať kontrola každej komunikácie cez protokol SSL okrem komunikácie využívajúcej certifikáty vylúčené z kontroly. Pri komunikácii využívajúcej zatiaľ neznámy certifikát, ktorý je dôveryhodne podpísaný, nebude používateľ upozornený na použitie daného certifikátu a komunikácia sa bude automaticky filtrovať. Ak používateľ pristupuje na server používajúci nedôveryhodne podpísaný certifikát, pričom bol tento používateľom označený ako dôveryhodný (zaradený do zoznamu dôveryhodných certifikátov), prístup bude povolený a komunikácia bude filtrovaná.

Pýtať sa na nenavštívené stránky (neznáme certifikáty) – V prípade neznámeho certifikátu bude zobrazené okno s možnosťou výberu akcie. Tento režim umožňuje vytvoriť zoznam certifikátov, pre ktoré sa nebude vykonávať kontrola v protokole SSL.

Nepoužívať kontrolu protokolu SSL – Nebude sa používať filtrovanie komunikácie cez protokol SSL.

Používať vytvorené výnimky z filtrovania na základe certifikátov – Pri kontrole SSL budú použité výnimky definované vo vylúčených a dôveryhodných certifikátoch. Nastavenie je dostupné pod **Filtrovanie protokolov > SSL > Použiť kontrolu protokolu SSL vždy**.

Blokovať kryptovanú komunikáciu používajúcu zastaraný protokol SSL v2 – Komunikácia cez staršiu verziu SSL protokolu bude automaticky pri jej nadviazaní blokovaná.

Integrácia do systému
Personálny firewall môže byť integrovaný do systému v niekoľkých úrovniach.

- **Všetky časti aktívne** – Firewall je plne integrovaný do systému a všetky jeho súčasti sú aktívne (predvolená možnosť). Ak je počítač pripojený do väčšej siete alebo internetu, odporúča sa ponechať túto možnosť aktivovanú. Táto možnosť je najviac bezpečná a váš systém je vo vysokej miere chránený.
- **Personálny firewall neaktívny** – Firewall je integrovaný do systému, prebieha cez neho sieťová komunikácia, ale kontrola sa nevykonáva.
- **Iba kontrola aplikačných protokolov** – Aktívne sú iba tie časti personálneho firewallu, ktoré zabezpečujú kontrolu aplikačných protokolov (HTTP, POP3, IMAP a ich SSL varianty). Túto možnosť je dobré zvoliť, ak nechcete používať personálny firewall, ale chcete, aby boli kontrolované aplikačné protokoly. Ak sa aplikačné protokoly nekontrolujú, ochrana sa vykonáva štandardne na úrovni rezidentnej ochrany súborového systému a kontroly (skenovania) počítača.
- **Personálny firewall úplne vypnutý** – Po zvolení tejto možnosti je firewall úplne odhlásený zo systému a neprebieha žiadna kontrola. Táto možnosť je užitočná napríklad pre testovanie – ak je určitá aplikácia zablokovaná, je možné overiť si či nie je zablokovaná firewallom. Je to ale najmenej bezpečná možnosť, preto odporúčame byť opatrný pri úplnom vypnutí firewallu.

Ak je zaškrtnutá možnosť **Aktualizáciu modulu personálneho firewallu vykonávať až po reštarte počítača**, zmeny v module sa prejavia až po reštarte počítača.