
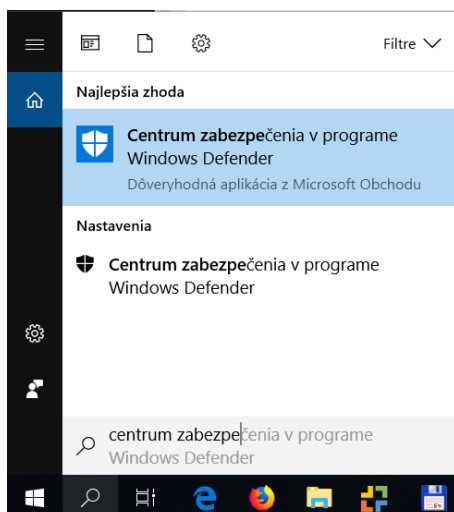


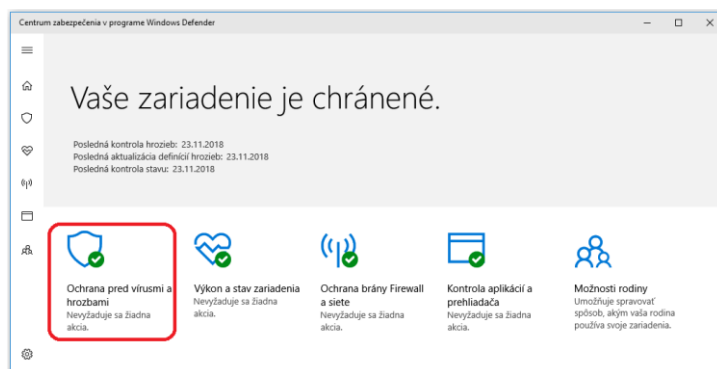
Postup nastavení Windows Defender pre zrýchlenie práce v Money S3

V prípade, že pracujete v programe Money S3 odporúčame správne nakonfigurovať aj antivírusový program pre urýchlenie práce a pre zabránenie blokovania komunikácie medzi serverom a klientom pri sieťovej prevádzke.

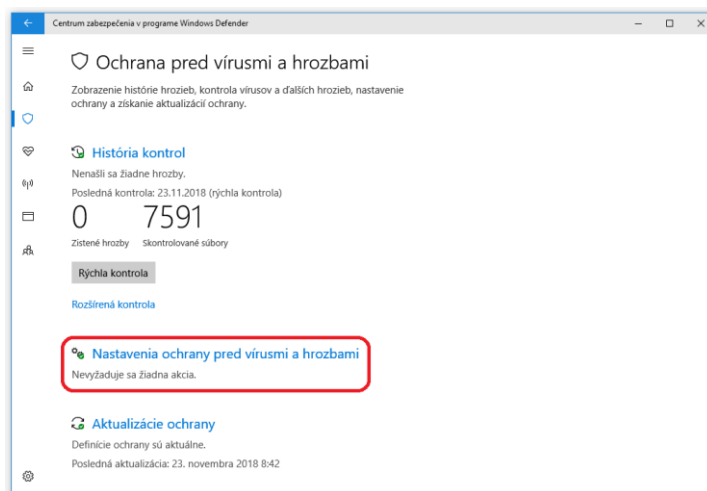
1. Postup je platný pre Windows 10 po aktualizácii Creators Update. Windows Defender je dostupný aj vo Windows 8.1, kde ale má rovnaké rozhranie ako Microsoft Security Essential.
2. Otvoríme konfiguračné okno Windows Defender cez kláves s logom Windows  + Q, kde začneme písať „Centrum zabezpečenia v programe Windows Defender“ a zvolíme zobrazenú voľbu.



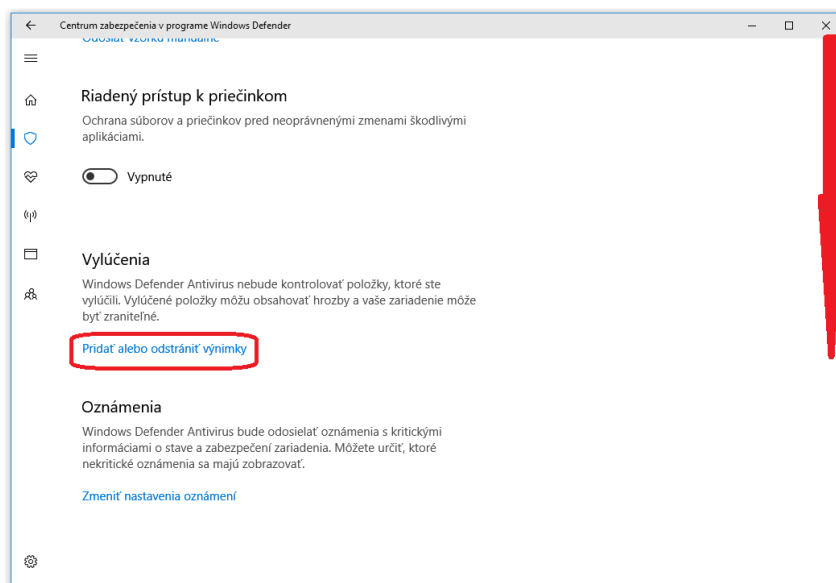
3. V novom okne vyberáme možnosť „Ochrana pred vírusmi a hrozbami“.



4. Volíme „Nastavenia ochrany pred vírusmi a hrozbami“.

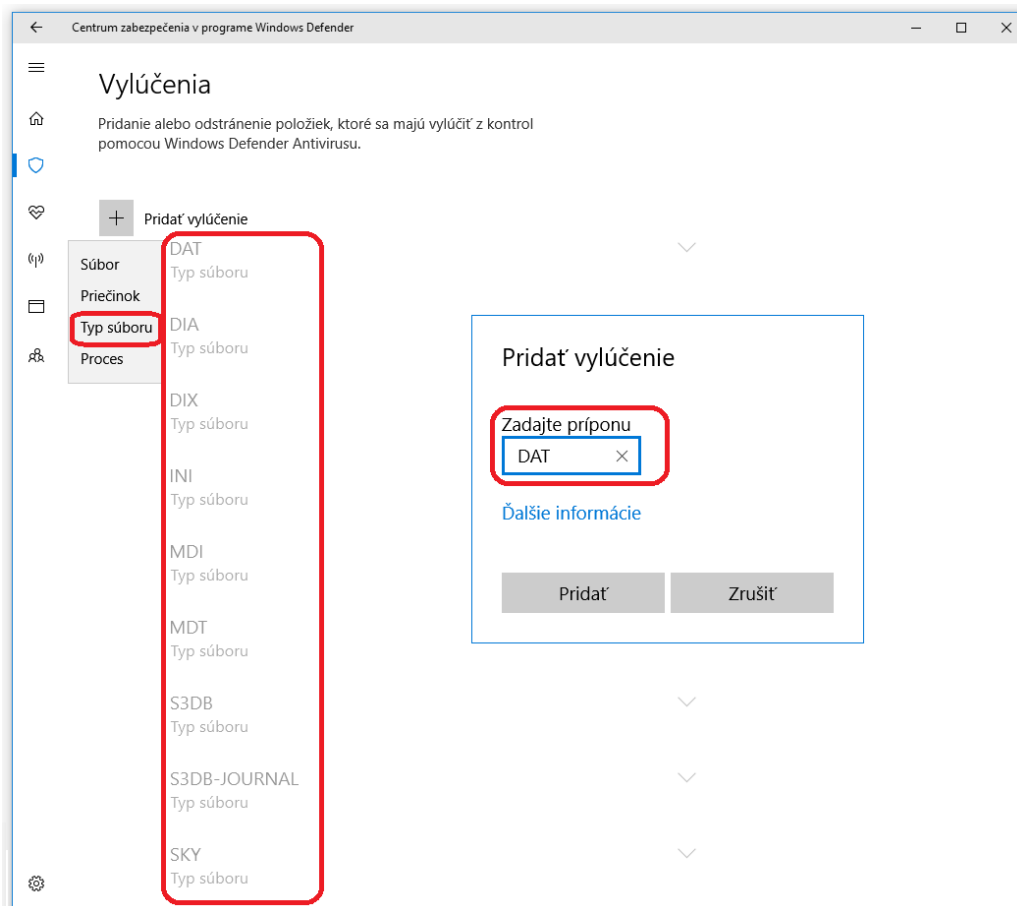


5. Posuvníkom sa posunieme dole až na sekciu „Vylúčenia“, kde klikneme na odkaz „Pridať alebo odstrániť výnimky“.

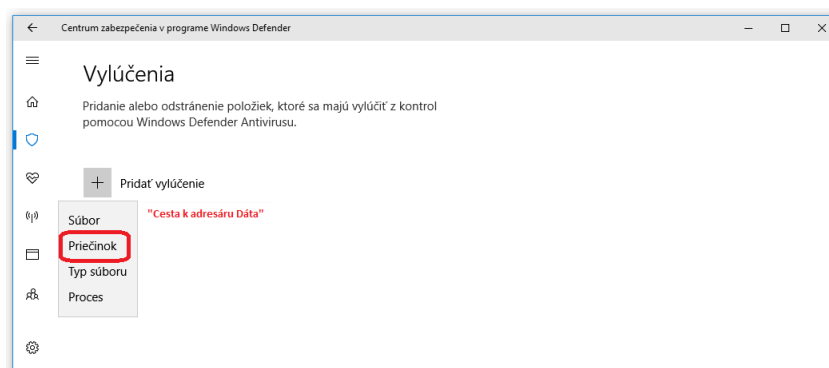


6. Tlačidlom „+“ a voľbou „Typ súboru“ nastavíme výnimky indexových súborov (DAT, DIX, DIA, SKY, INI, MD?, S3DB a S3DB-JOURNAL), ktoré Money S3 používa.

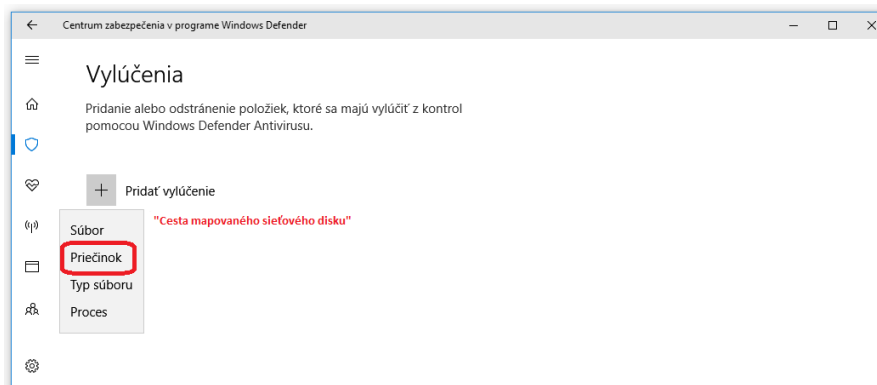
Pri pridávaní výnimiek sa môžete stretnúť s oknom „Kontrola používateľských kont“, ktoré je potrebné potvrdiť.



7. V prípade lokálnej alebo serverovej inštalácie pridáme tlačidlom „+“ a voľbou „Priečink“ výnimku na adresár Data, ktorý nájdete v ceste umiestenia dát (štandardne C:/Users/Public/Documents/Solitea/Money S3, v prípade starších inštalácií C:/Users/Public/Documents/CIGLER SOFTWARE/Money S3).



8. V prípade, že je Money S3 používané v režime sieťovej prevádzky, na klientskom počítači pridáme do výnimiek mapovaný sieťový disk s dátami zo servera.




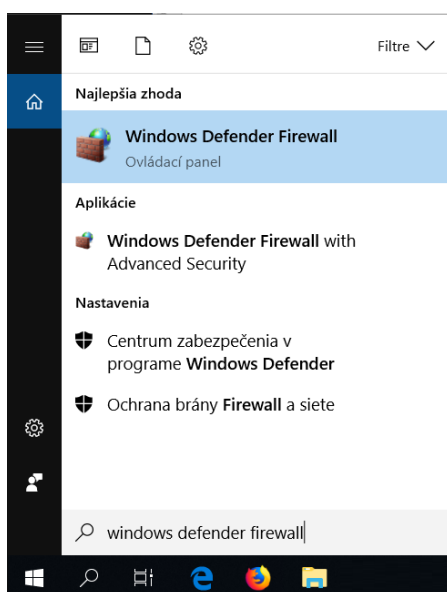
9. Pokiaľ je Money S3 inštalované na niekoľkých klientských staniciach je potrebné hore uvedené nastavenie vykonať na každej klientskej stanici.
10. Tieto nastavenia kompletne vylúčia kontrolu indexových súborov Money S3 z rezidentnej kontroly, preto odporúčame nastaviť pravidelnú kontrolu celého počítača antivírusovým systémom.

Postup nastavení Windows Defender pre povolenie portu 511 v Money S3 pri sieťovej prevádzke

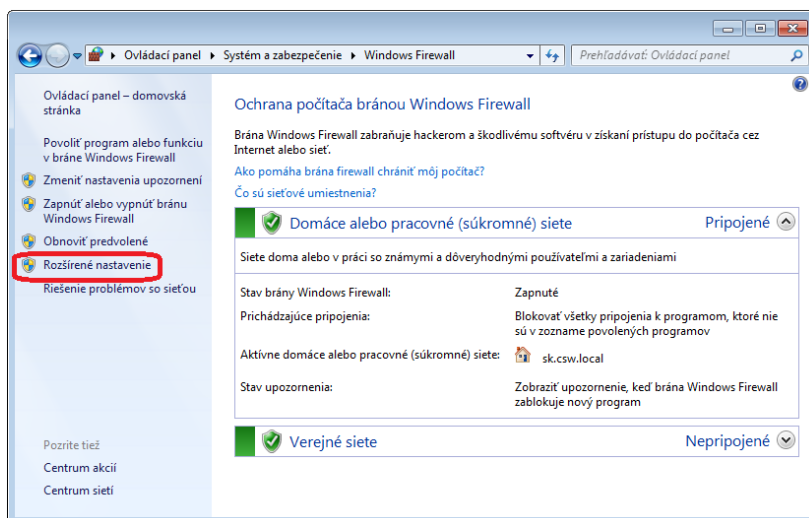
V prípade, že pracujete v programe Money S3 s typom inštalácie Server - Klient môže byť antivírusovým programom blokovaný port 511 potrebný pre komunikáciu klienta so serverom.

Windows Defender neobsahuje vlastný aparát firewallu, preto je potrebné výnimky na port 511 nastaviť manuálne vo Windows Defender Firewall

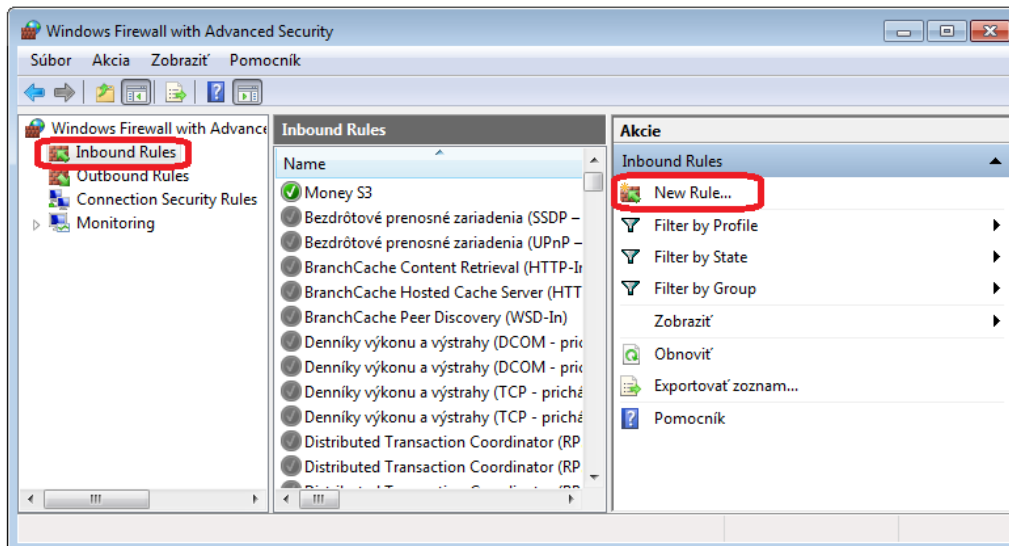
1. Otvoríme konfiguračné okno „Windows Defender Firewall“ cez kláves s logom Windows  + Q, kde začneme písať „Windows Defender Firewall“ a zvolíme zobrazenú voľbu.



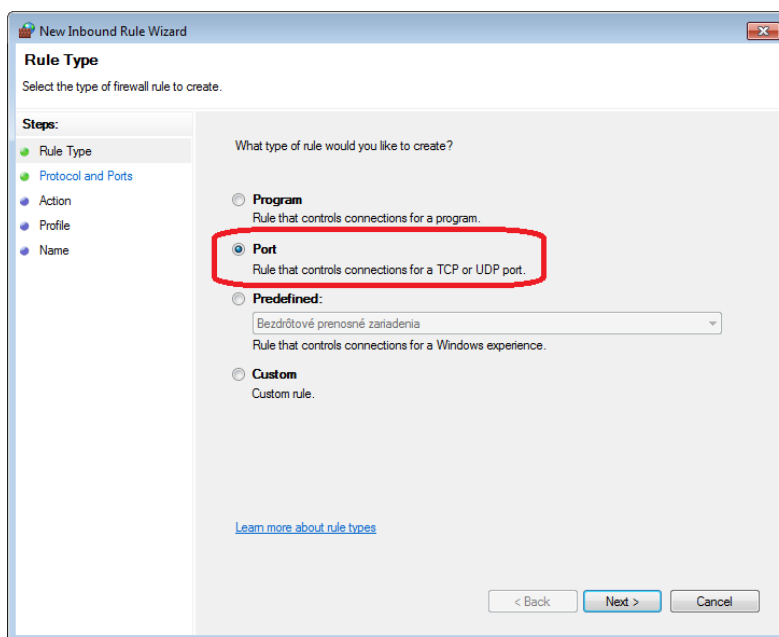
2. Otvoríme menu „Rozšírené nastavenie“.



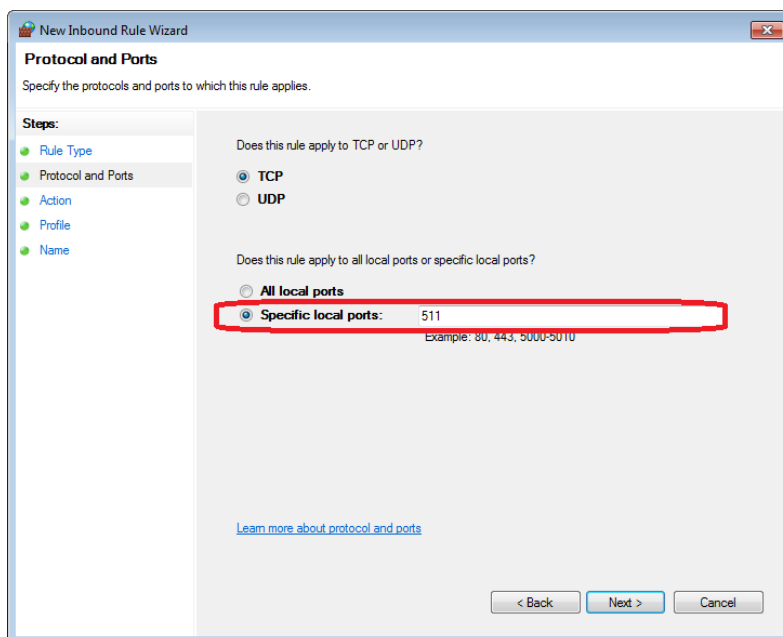
3. V novozobrazenom okne rozšírených nastavení zvolíme položku „Inbound rules“ a následne „New Rule“.



4. V sprievodcovi konfiguráciou pravidla zvolíme voľbu „Port“ a potvrdíme tlačidlom „Next“.

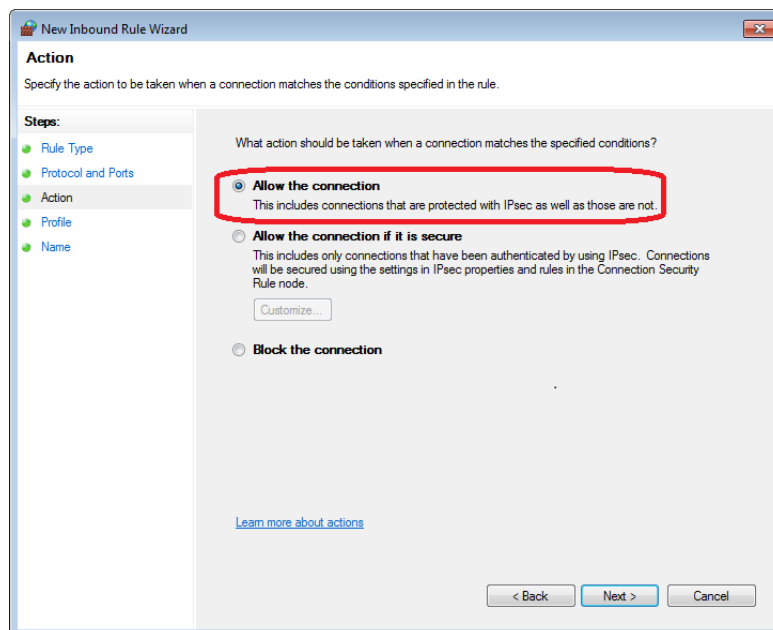


5. Zadáme číslo portu – „511“ a pokračujeme cez „Next“.



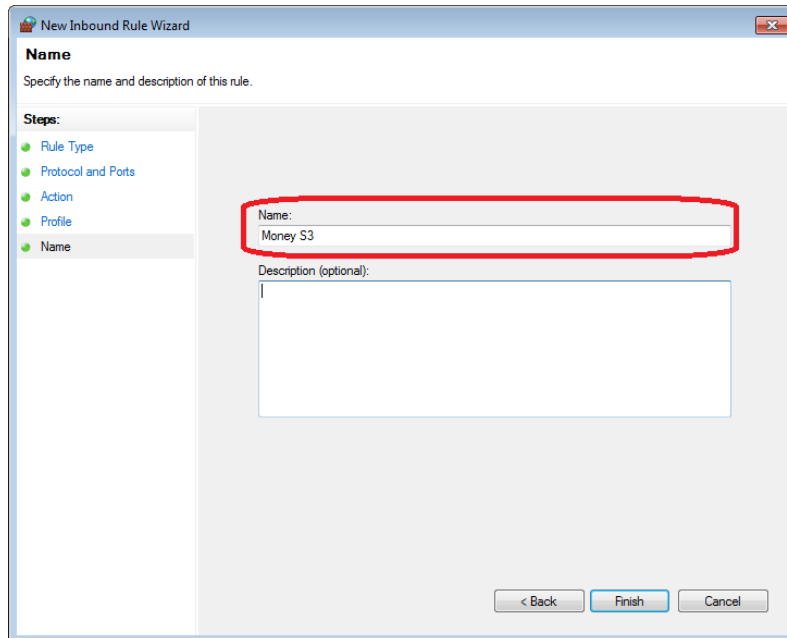
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports' (selected), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:'. The 'Specific local ports' option is selected, and the text '511' is entered in the adjacent input field. Below the input field is the example text 'Example: 80, 443, 5000-5010'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

6. V nasledujúcom okne sprievodcu zvolíme možnosť „Allow the connection“ a znovu pokračujeme cez „Next“.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action' (selected), 'Profile', and 'Name'. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option is highlighted with a red box. Below it is a 'Customize...' button. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

7. V nasledujúcom okne pokračujeme znovu cez „Next“ bez zmeny. V poslednom okne sprievodcu pomenujeme pravidlo, napr. Money S3. Sprievodcu ukončíme tlačidlom „Finish“.



The screenshot shows a window titled "New Inbound Rule Wizard" with a "Name" step selected. The window contains a list of steps on the left: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area has a "Name:" label with a text box containing "Money S3", which is highlighted with a red rectangle. Below it is a "Description (optional):" label with an empty text box. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

8. Následne v okne „Rozšírených nastavení,, postup zopakujeme aj pre vytvorenie pravidla v sekcii „Outbound Rules“.