

Sit'ová bezpečnosť a firewall



Oleksandr Petronyuk

Obsah

- Prvky ideálního firewallů
- Co firewall nevyřeší
- Základní služby a jejich slabiny
- Profily útoku
- Detekce průniku do sítě
- Typický postup pro vniknutí do sítě a protiopatření
- Jak ochránit středně malou firmu

Prvky ideálního firewallu

- Filtrování paketu
- Překlad síťových adres(NAT)
- Služby proxy

Co firewall nevyřeší

- Na světě existuje tolik různých způsobů napadení sítě, že úplně bezpečná není žádná metoda
- Dalším problémem je ochrana proti protokolům, které se se rozhodnete propouštět
- Skryté hraniční přechody
- Nepoučení zaměstnanci

Služby a jejich slabiny

- **Bežné internetové služby**
- -DNS(53 udp)
- -FTP(20 a 21 tcp)
- -HTTP(80 tcp)
- -IMAP(143 tcp)
- -NTP(123 udp)
- -POP(110 tcp)
- -SMTP(25 tcp)

Profily útoku

- Ping of Death
- Teardrop
- UDP floods
- SYN floods
- Smurf
- Fraggle
- Chybně formatované zprávy

Detekce vniknutí

- Skenování IP adres
- Skenování portů
- Průzkum služeb
- Výber cíle a průzkumy slabých míst
- Automatizované útoky na hesla
- Útoky na specifické služby

Detekce vniknutí

The screenshot displays the Advanced Port Scanner v1.3 interface. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu is a toolbar with icons for file operations and network connections. A banner for 'RADMIN® remote control software' is visible, with the tagline 'fast. secure. affordable.'.

The main interface features a configuration section with the following settings:

- Select IP: 10 . 0 . 0 . 0 Use range 10 . 0 . 0 . 255
- Use group of ranges
- Select ports range: default - default Use default ports list
- Use ports ranges list

The scan results are displayed in a tree view:

- 10.0.0.2 (revmira-d22f1ae) Ports (scanned 67 of 67, opened: 2 closed: 65)
 - Open ports (2)
 - 135 Open (loc-srv)
 - 139 Open (netbios-ssn)
 - Closed ports (65)
 - 0 - 134 Closed
 - 136 - 138 Closed
 - 140 - 65535 Closed
- 10.0.0.3 (PC01) Ports (scanned 67 of 67, opened: 4 closed: 63)
 - Open ports (4)
 - 21 Open (ftp)
 - 135 Open (loc-srv)
 - 139 Open (netbios-ssn)
 - 445 Open (microsoft-ds)
 - Closed ports (63)
 - 0 - 20 Closed
 - 22 - 134 Closed
 - 136 - 138 Closed
 - 140 - 444 Closed
 - 446 - 65535 Closed
- 10.0.0.7 (YOUR-RNKIHUXE3W) Ports (scanned 67 of 67, opened: 3 closed: 64)
 - Open ports (3)
 - 21 Open (ftp)
 - 80 Open (www-http)
 - 139 Open (netbios-ssn)
 - Closed ports (64)
- 10.0.0.138 Ports (scanned 67 of 67, opened: 3 closed: 64)
 - Open ports (3)
 - Closed ports (64)

At the bottom of the window, a status bar indicates 'Scan complete'.

Možné řešení

- V praxi existuje malo spolehlivých systému detekce vniknutí
- Většinou se zavádějí firewally s funkcemi protokolování a varování.
- Většina nedokáže reagovat na útok automaticky
- **Možné řešení**
- Kvalitní loggy
- Dohledové systémy(Nagios) atd...

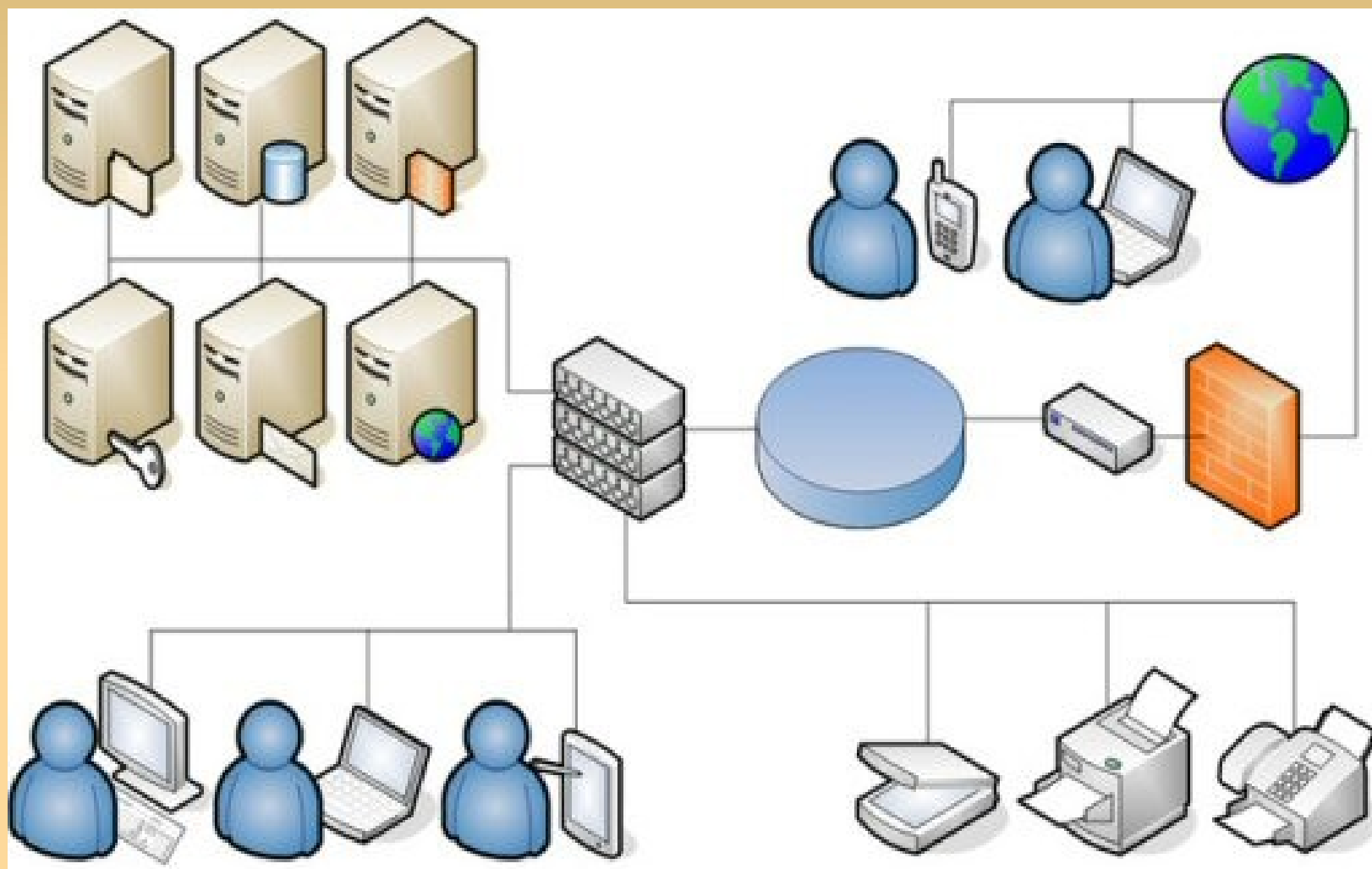
Analýza středně malých podniků

- Většinou 10-20 počítačů
- Vyhrazený jeden počítač pro služby souborů a tiskáren
- Menšina těchto podniků používá firewall
- Nejeví zájem o zabezpečení dokud nedojde ke ztratě důležitých dat

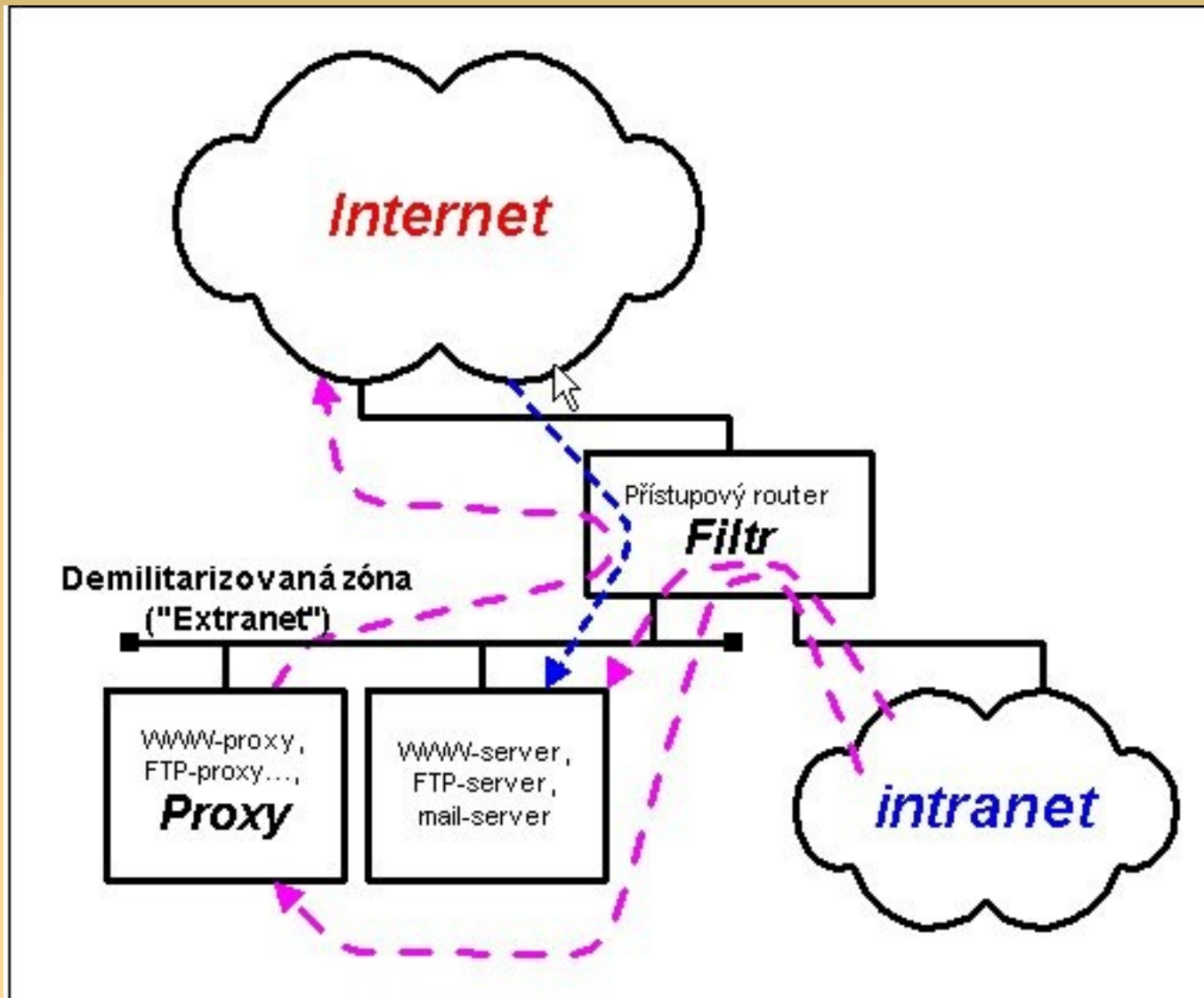
Jak ochránit středně velkou firmu

- U středně malých podniků není třeba při zabezpečování sítě jít do extrému
- Analýza nákladů a vynosů prozradí, že stačí méně přísné zabezpečení
- Tyto firmy nemají tolik důležitých informací, které by zajímali náhodného hackera nebo konkurenci
- Výstavba firewallu za switchem

Jak ochránit středně malou firmu



Jak ochránit středně malou firmu



Použitá literatura

Sit'ová bezpečnost a firewall Oleksandr Petronyuk

Děkuji za pozornost