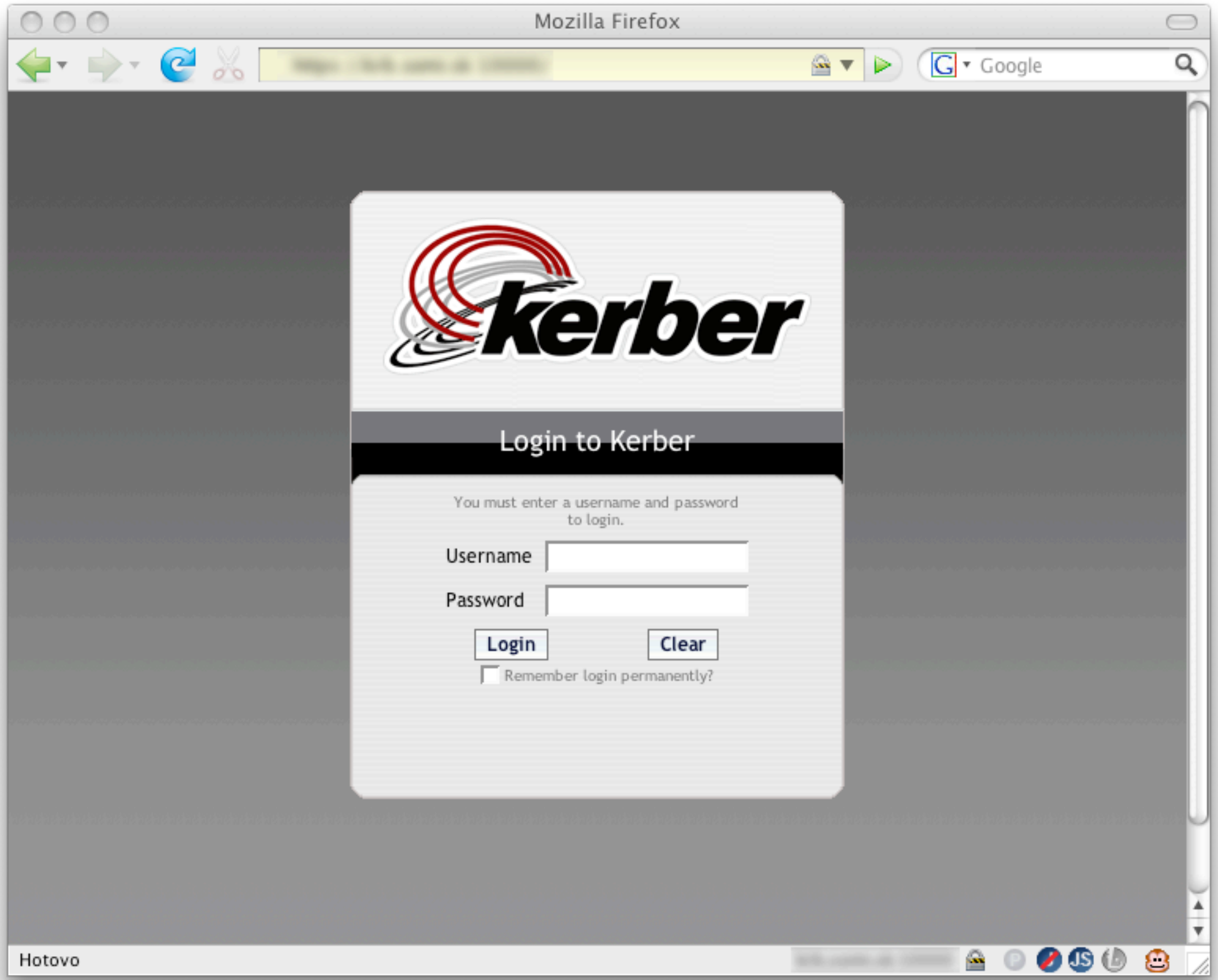
KERBER

komplexné riešenie bezpečnosti

Michal Žila
SOMI Systems a.s.


Mozilla Firefox
Google
kerber
Login to Kerber
You must enter a username and password to login.
Username
Password
Login
Clear
Remember login permanently?
Hotovo

KERBER

je modulárny

- VPN - Privátne siete
- HTTP filtrovanie
  - Clam Antivirus
- Sieťová ochrana (Firewall, IDS)
- Sieťové služby (DHCP, NTP)
- SAS - Secure Antispam Solution

Prečo práve KERBER?

- KERBER je zameraný na sieťovú bezpečnosť
- Grafické rozhranie
- Nie je potrebný príkazový riadok
- Správa užívateľov
- Jednoduchá konfigurácia
- Ucelený systém “všetko pod jednou strechou”

VPN - Privátne siete

- Šifrovanie pomocou SSL
- SSLv3/TLSv1 protokoly
- Portované na najrozšírenejšie platformy
- Jednoduchá konfigurácia
- Schopnosť prejsť cez NAT
- Možnosť kompresie (lzo)

HTTP Filtrovanie

- Filtrovanie prístupov k Internetovému obsahu na základe času, obsahu, zdroja a cieľa.

Situácia vo firemnom prostredí

- Zhruba 30% pracovného času venujú zamestnanci na súkromné použitie: surfovanie Internetom, chatovanie, zábava, atď.
- Iba 40% organizácií používa nejaký software na kontrolu internetovej prevádzky
- 90% organizácií by chcelo používať pokročilejší software na kontrolu internetovej prevádzky

Dan Malachowski (2005, July 11) Salary.com “Wasting Time at Work Costing Companies Billions”
Karl Donert, Sara Carro Martinez (2002, December 23) “End-user Requirements: Final Report”

Ciele HTTP Filtrovania v KERBERi

- Zabraňovať prístupom k nechcenému obsahu
- Detekovanie nebezpečného obsahu (vírusy, trójske kone, atď.)
- Redukovať počet únikov dôverných informácií v podnikovom sektore
- Zabraňovať nechcenému použitiu Internetu v pracovnom čase zamestnancov

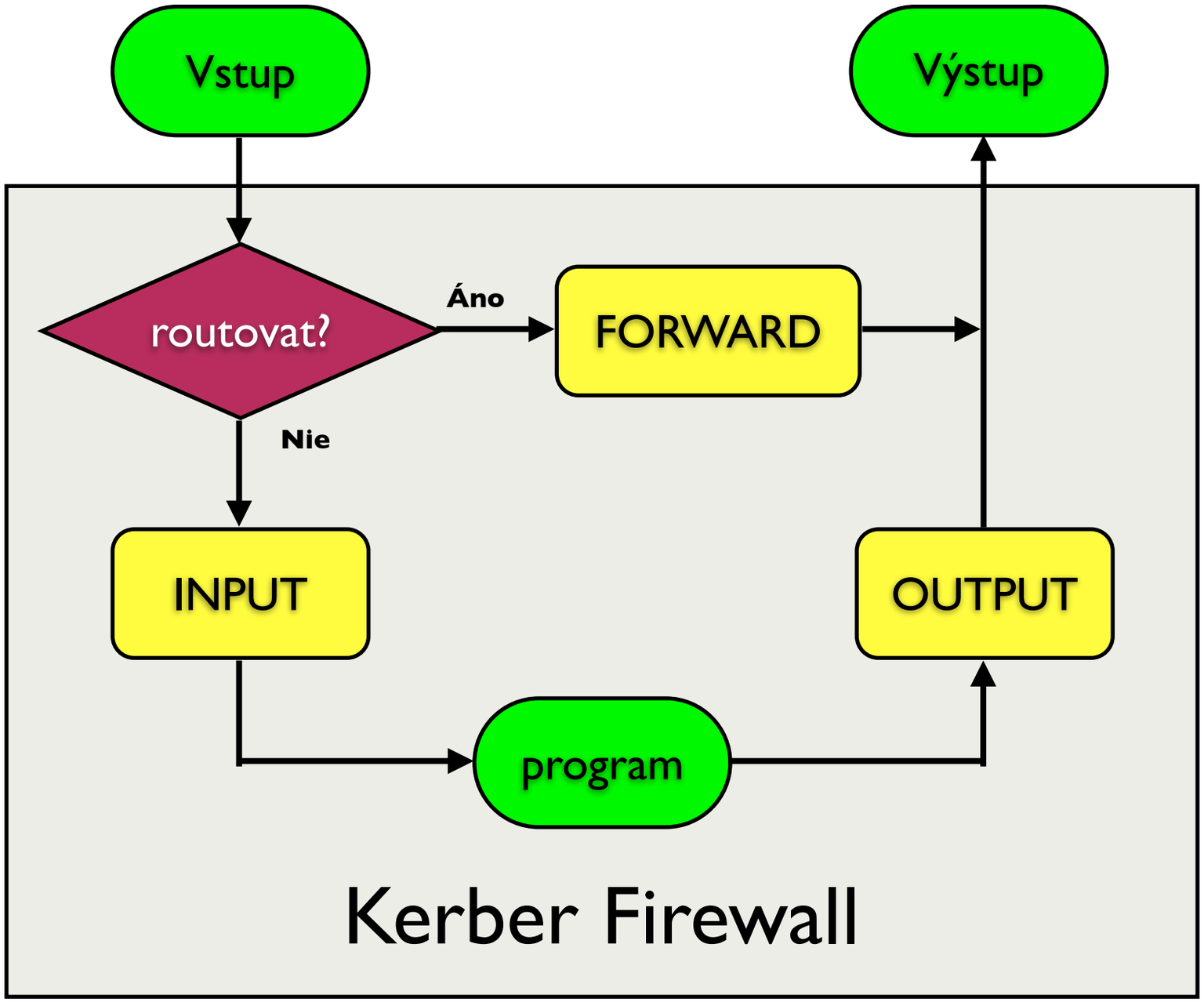
Možnosti HTTP filtrovania v KERBERi

- **ACR (Access Control Rules)**
  - Časové úseky
  - Zdrojové skupiny
  - Cieľové skupiny
  - Blacklisty
  - Content filter (malware)
- Grafická analýza prístupov

Stavový firewall

- Stavový firewall je firewall, ktorý sleduje a rozoznáva stav sieťových spojení (TCP, UDP)
- Väčšia precíznosť na rozdiel od obyčajných firewallov

Diagram cesty paketu



Peer-To-Peer (p2p)

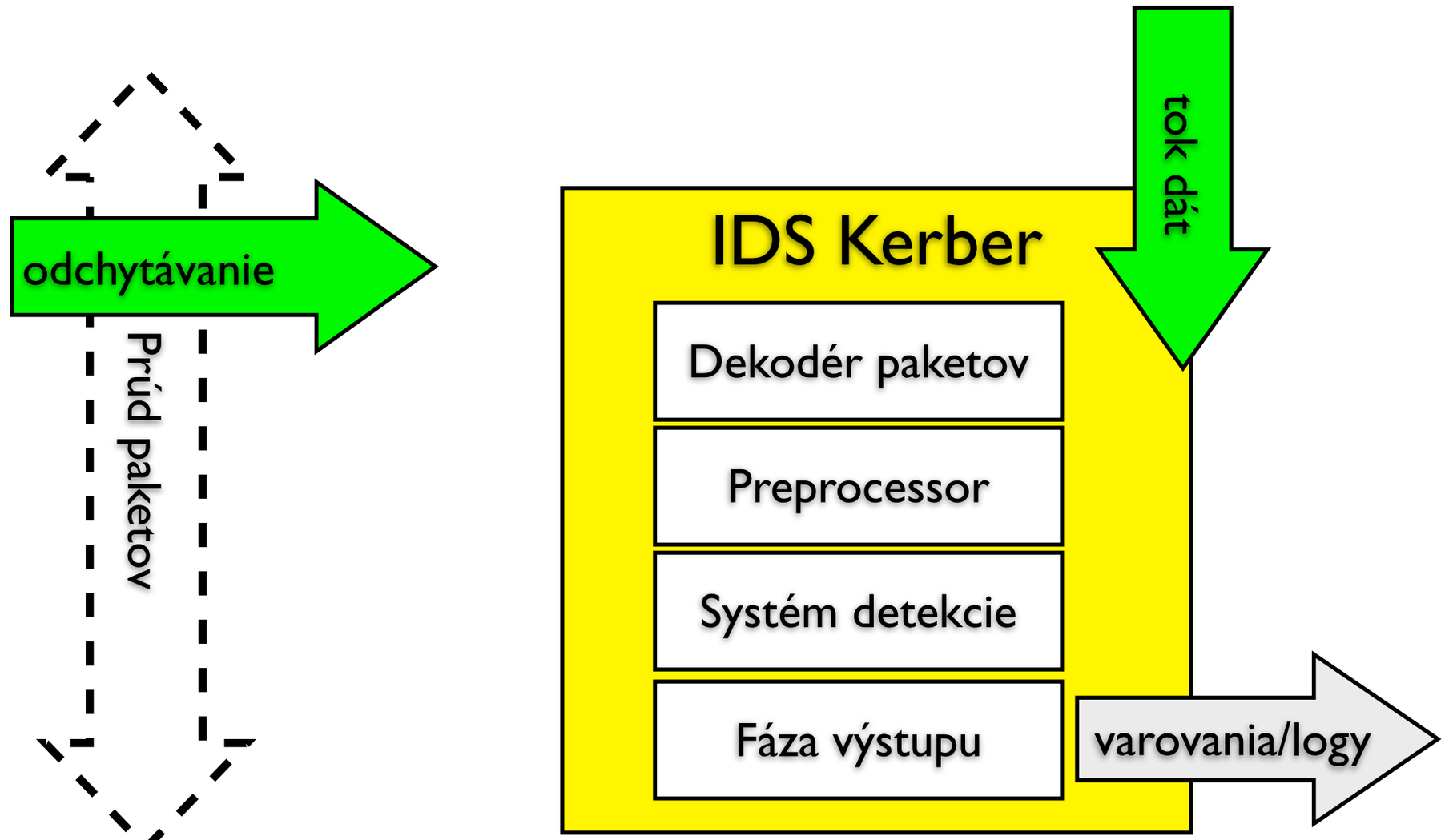
- BitTorrent, Direct Connect, eMule a pod.
- 50 až 65% všetkých stiahnutých dát tvorí peer-to-peer
- 75 až 90% percent všetkých poslaných dát tvorí peer-to-peer prevádzka

David Ferguson - CacheLogic (2006)

IDS - Intrusion Detection System

- Systém detekcie prieniku
- Slúži na odhalenie útoku na server a jeho prípadnému zabráneniu
- Sleduje neštandardnú aktivitu ako napr. pokusy o spojenie na príliš veľa portov
- Systém pravidiel je veľmi flexibilný a vytváranie nových pravidiel relatívne jednoduché

Tok dát v Kerber IDS



DHCP
Dynamic Host Configuration Protocol

- Automatické nastavenie sieťových parametrov klienta
- Prideľovanie adries na základe fyzickej adresy sieťového rozhrania klienta

NTP server

- Network Time Protocol
- Časový synchronizačný server, ktorý umožňuje klientským staniciam mať vždy správny čas

Bandwidth Monitor

- “Stopuje” všetky IP spojenia a na ich základe počíta prenesené dáta
- Výhodné v situáciách kedy, je nutné obísť proxy server
- Štatistiky využitia linky pre servery v DMZ
- Triedenie na základe viacerých možností

Show traffic by host for <everything>

For traffic after / Jan / ... :00

For traffic before / Jan / ... :00

Server ports only? Resolve hostnames?

Generate Report

Host	Network traffic downloaded and uploaded
192.168.236.210	936.30 MB/518.17 MB (1.42 GB)
192.168.139.66	1.09 GB/22.48 MB (1.11 GB)
195.80.182.211	626.46 MB/250.86 MB (877.32 MB)
192.168.139.142	400.66 MB/66.21 MB (466.86 MB)
192.168.139.105	361.44 MB/18.71 MB (380.16 MB)
192.168.139.54	265.78 MB/26.05 MB (291.83 MB)
192.168.139.28	267.34 MB/14.67 MB (282.01 MB)
192.168.139.135	253.11 MB/21.70 MB (274.82 MB)
192.168.139.33	225.65 MB/15.84 MB (241.49 MB)
192.168.139.55	204.29 MB/20.58 MB (224.87 MB)
192.168.139.204	171.42 MB/17.19 MB (188.61 MB)
192.168.139.30	166.84 MB/21.20 MB (188.05 MB)
192.168.139.23	160.40 MB/11.19 MB (171.59 MB)
192.168.139.140	153.47 MB/17.87 MB (171.34 MB)
192.168.139.167	162.76 MB/7.58 MB (170.34 MB)
192.168.139.155	148.45 MB/13.85 MB (162.30 MB)
192.168.139.160	125.90 MB/21.31 MB (147.20 MB)
192.168.139.15	115.99 MB/12.04 MB (128.03 MB)
192.168.139.177	108.98 MB/7.07 MB (116.05 MB)
192.168.139.22	98.64 MB/11.40 MB (110.03 MB)
192.168.139.108	82.72 MB/9.31 MB (92.04 MB)
192.168.139.43	80.97 MB/7.59 MB (88.57 MB)
192.168.139.41	80.13 MB/7.23 MB (87.36 MB)
192.168.139.103	72.85 MB/8.45 MB (81.31 MB)
192.168.139.47	54.75 MB/26.37 MB (81.13 MB)
192.168.139.13	73.85 MB/7.18 MB (81.03 MB)
192.168.139.1	30.29 MB/45.60 MB (75.90 MB)

SAS - Secure Antispam Solution

- SAS je komplexný nástroj na detekciu a ochranu pred nevyžiadanými správami
- SAS kombinuje všetky známe metódy ako sú:

  - Riadenie prístupu

    access listy, RBL, Greylisting, Rate Limit, Connection Limit

  - Kontrola obsahu

    REGEX filtering, Bayes Filtering, URL Filtering (URLBL database), RFC control

- SAS slúži ako SMTP gateway, cez ktorý prechádza celý vstupný alebo výstupný SMTP trafik. Každá správa je podrobená kontrole pričom výsledok je uvedený v hlavičke každej správy v podobe SPAM Score.
- SAS je optimalizovaný na výkon. Jedna SAS inštalácia dokáže skontrolovať viac ako 50 000 správ / hodinu.

Výhody SAS-u

- Otvorený modulárny systém
- Vysoký výkon
- Podrobné štatistiky a logy o behu a chovaní systému
- Chovanie SAS-u je možné modifikovať za behu bez nutnosti rebootu
- Funkčnosť SAS-u je možné prispôsobiť konkrétnym požiadavkám zákazníka na základe jeho vlastnej antispamovej politiky
- Možnosť definovania skupín odosielateľov a príjemcov ako aj výnimiek pre jednotlivé typy kontrol
- Možnosť vzdialenej správy a automatickej aktualizácie RBL a URLBL databáz

Ďakujem za pozornosť

Michal Žila
systémový administrátor