Tunelování SSH přes HTTP(S)

Ondřej Caletka
o.caletka@sh.cvut.cz
http://shell.sh.cvut.cz/~oskar

SUT SH

Tunelování pomocí SSH

- Opakování matka moudrosti:
  - `ssh -L <locport>:<remotehost>:<remoteport>`
  - `ssh -R <remoteport>:<localhost>:<localport>`
- SSH umí i primitivní VPN pomocí TUN/TAP
  - viz ssh -w
- => Funguje-li ssh, je problém vyřešen ☺
- Bohužel, většina korporátních prostředí port 22 blokuje ☹
- Naproti tomu port 443 (https) bývá zpřístupněn

Využití portu 443 pro SSH (1)

- Spustit/přesměrovat ssh na port 443

```
Port 443 >> /etc/ssh/sshd_config
```

```
iptables -t NAT -A PREROUTING -p tcp
--dport 443 -j REDIRECT --to-ports 22
```

- Výhody
  - Extrémně jednoduché
  - Bude fungovat skoro všude
- Nevýhody
  - Není možné provozovat HTTPS server na stejné adrese
  - Super chytré dokonalé firewally poznají, že nejde o HTTPS handshake

Využití portu 443 pro SSH (2)

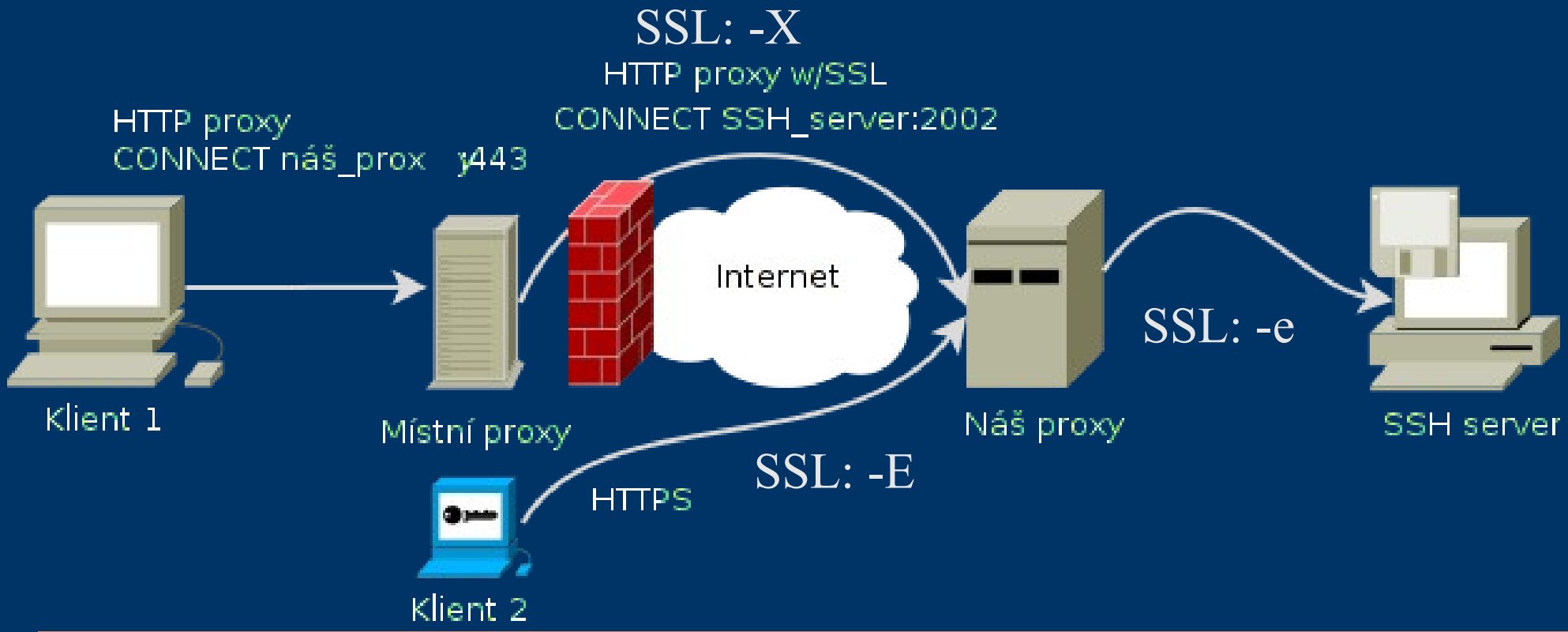
- Princip stejný jako (1), ale vtipně využít rozdílů v handshake SSH vs. HTTPS:
  - HTTPS používá SSL handshake, první mluví klient
  - V SSH handshake mluví první server
  - Existuje přepínač jménem sslh
- Výhody
  - HTTPs i SSH na jednom portu
  - Jednoduché
- Nevýhody
  - Špatně se loguje
  - Performance issues
  - SSH není SSL – firewall to pozná – viz (1)

Využití portu 443 pro SSH (3)

- Pomocí (patchnutého) mod_proxy_connect v Apache umožnit HTTPS serveru proxy režim, který příkazem CONNECT připojí klienta na SSH.
- Výhody
  - Opravdové SSL, nerozlišitelné od HTTPS
  - Může procházet proxy servery
  - Možnost provozovat zároveň HTTPS server
- Nevýhody
  - Složitější konfigurace
  - Performance issues
  - Problém s logy, možnost abuse

Proxytunnel

- Pomocný program pro stavění tunelů HTTP proxy serverem
- V aktuální verzi umí projít místní proxy (-p) na vzdálenou (-r) a z té na cíl (-d).



Patchování apache

- Standardní Apache HTTPd nepodporuje proxy režim CONNECT v SSL režimu
- Bez patchování je možné provozovat pouze čistě HTTP proxy režim
  - Přijdeme o možnost provozovat HTTPS
  - Některé firewally poznají, že se nejedná o SSL
- Existuje patch na Apache Bug 29744
  - Nahlášen 2004
  - Dosud neopraven ☺
- Proxytunnel neumí kontrolovat certifikáty
  - Riziko MitM útoku

Webové zdroje

- Řešení ad (2)
  - http://www.rutschle.net/tech/sslh.shtml
- Řešení ad (3)
  - http://dag.wieers.com/howto/ssh-http-tunneling/
- Proxytunnel
  - http://proxytunnel.sourceforge.net/
- Jiné řešení – GNU httptunnel
  - http://www.nocrew.org/software/httptunnel.html
  - Server/klient aplikace pro HTTP bez SSL
  - Zabaluje komunikaci do HTTP GET/PUT zpráv

Závěr

- Děkuji za pozornost
- RTFM
- UTFG
- Přístí týden LVM, RAID
- EOF ❑

VLAK PŘIJÍŽDÍ
DO STANICE

TRAIN
IS APROACHING
THE STATION

No Show