
the next generation of

# Crypt ‘ O ‘ Pack in security

by innoidea

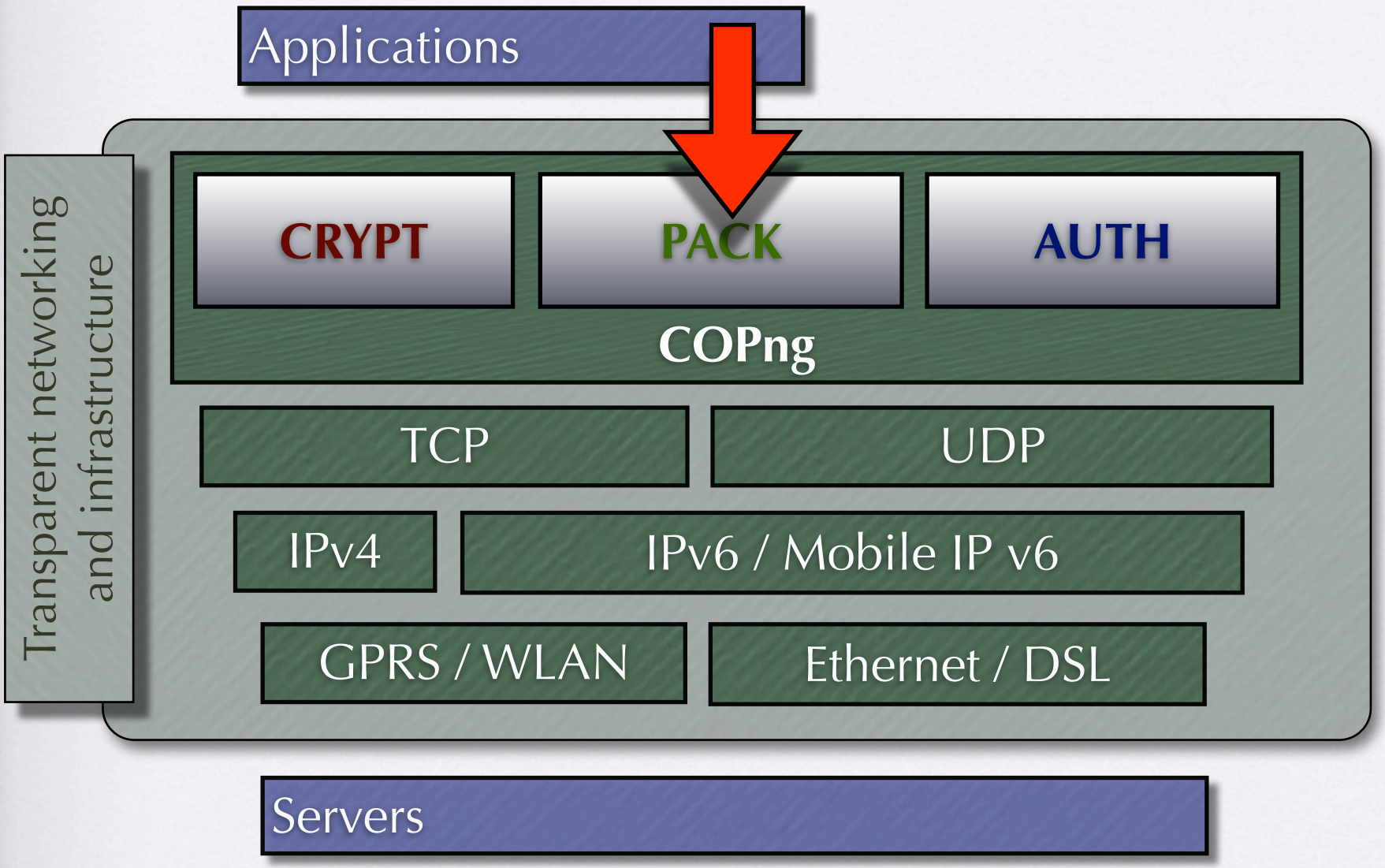

SECURITY.INNOIDEA.HU

Lajos Nagy, 2005

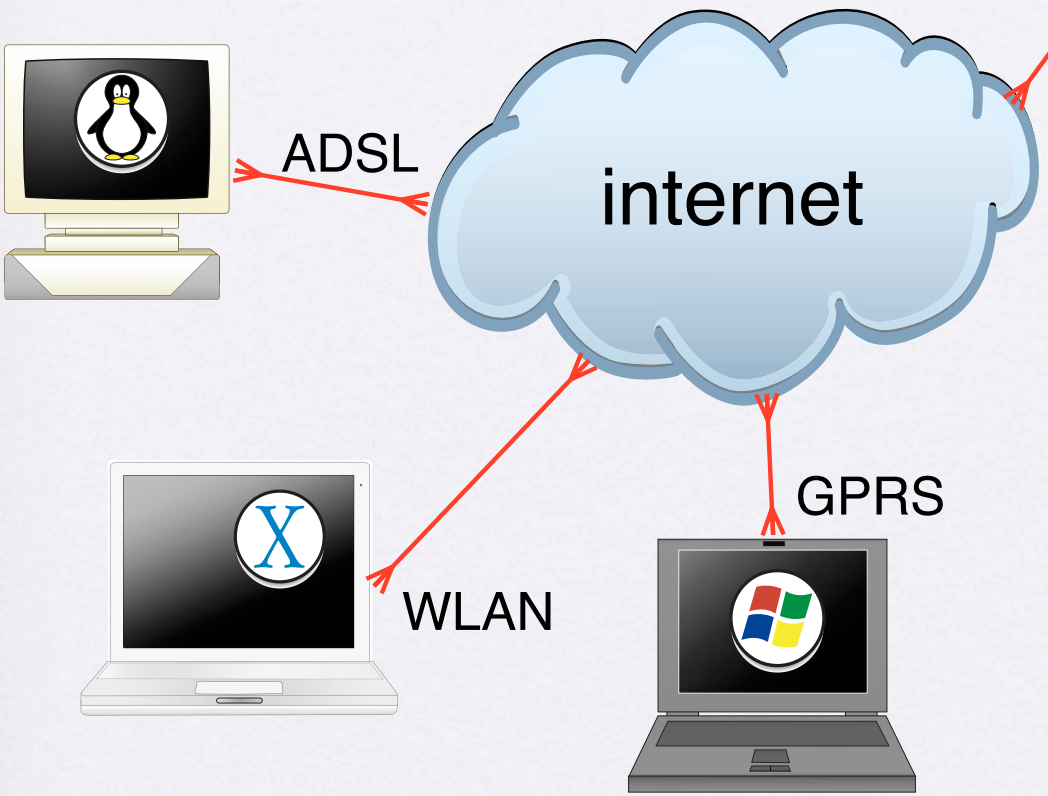
# Crypt 'O' Pack
## next generation

- Titkosítás
- Tömörítés
- Azonosítás
- Multiplatform megoldás
- Kliens oldali installáció nélkül használható!

# Crypt 'O' Pack
## next generation



# Védett adatkapcsolat minden platformról

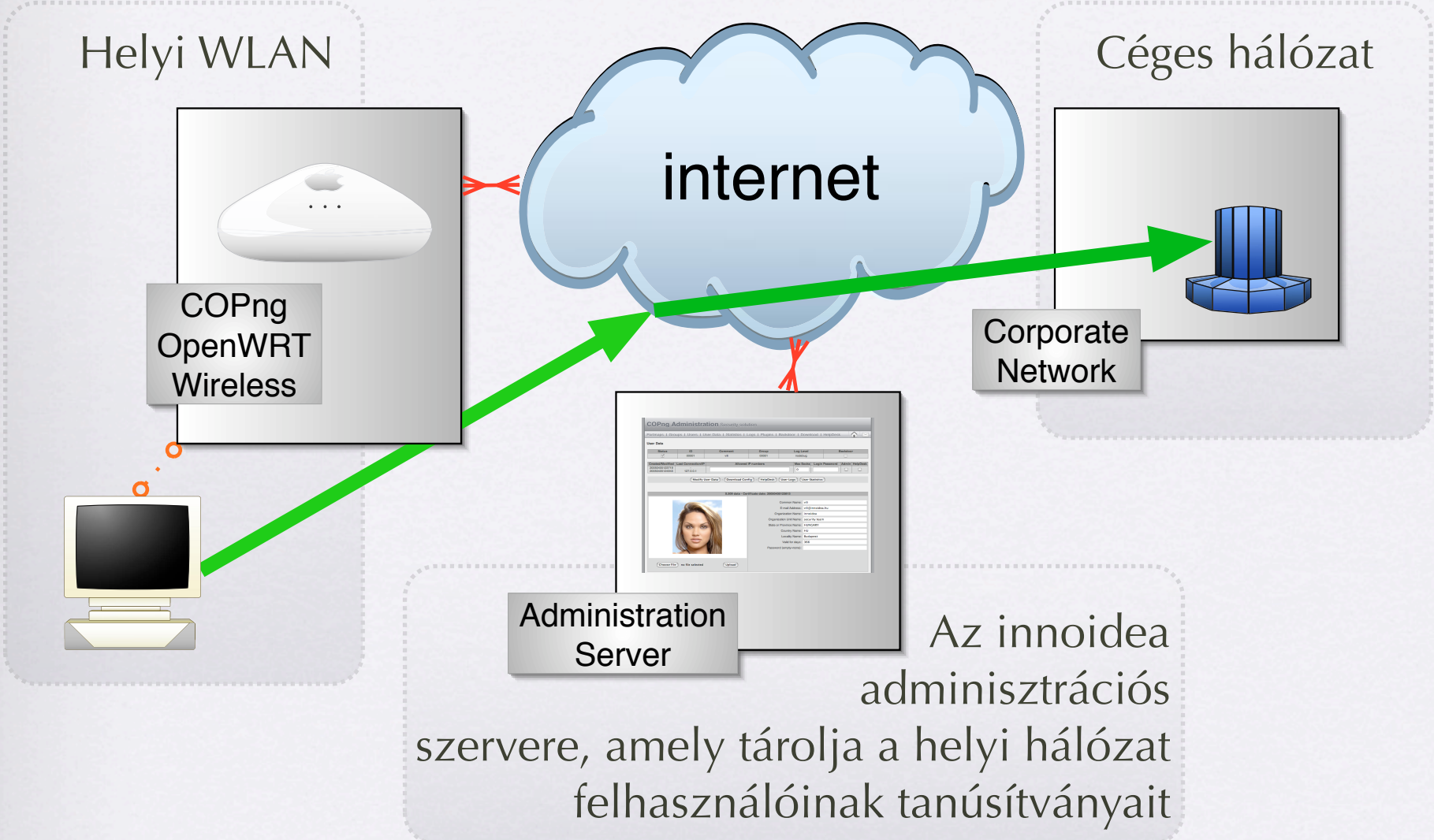




- HTTP
- IRC
- Samba
- POP3
- IMAP
- SMTP
- LDAP
- VNC
- X11
- Telnet
- SSH
- RSync

- Remote Desktop

# Titkosított, authentikált WLAN és internet kapcsolat



# Crypt 'O' Pack
## next generation

- Titkosítás
  - Az SSL által biztosított, a lehető legerősebb hatásfokú titkosító algoritmus kiválasztása automatikusan, a kapcsolat felvételekor
  - Moduláris algoritmus kezelés
  - Több SSL implementációt is támogatunk amely rendelkezik session-caching-el

MatrixSSL

SSL.com

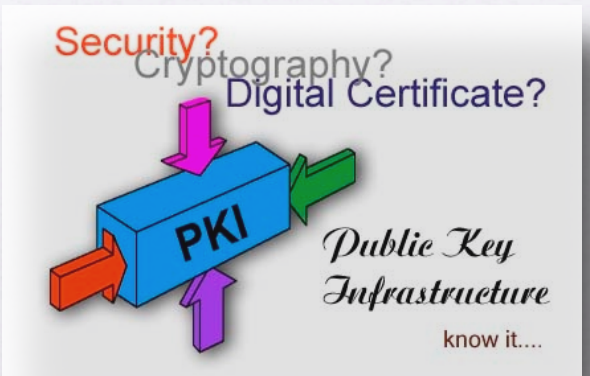
OpenSSL

# Crypt 'O' Pack
## next generation

- Tömörítés
  - Szabványos, nyílt forráskódú tömörítő eljárások használata (BZIP2, GZIP, LZO)
  - Applikációhoz, környezethez rendelhető tömörítési metódus, és hatásfok
  - Bővíthető algoritmus-tár, akár saját fejlesztésű tömörítő modulokhoz is

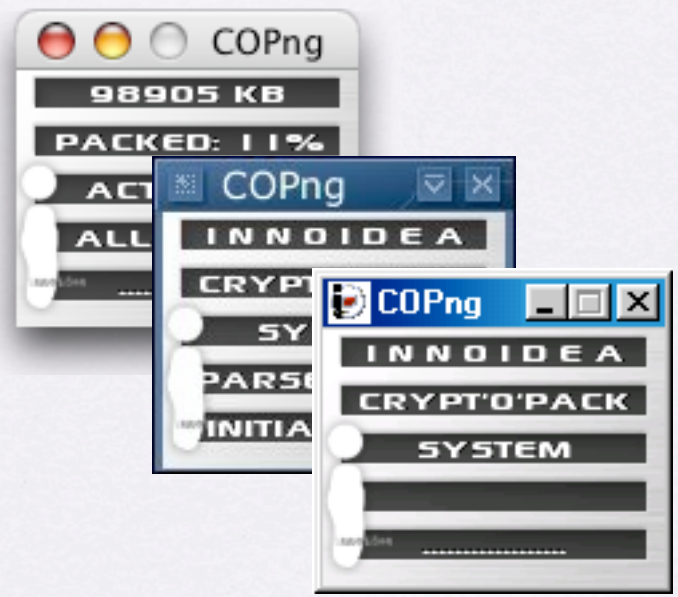
# Crypt 'O' Pack
## next generation

- Azonosítás
  - PKI rendszerű azonosítás
    - Saját PKI szerver
      - Integrálva az adminisztrációs rendszerbe
    - Külső PKI szerver
      - X500
      - LDAP
      - Windows Active Directory



# Crypt 'O' Pack
## next generation

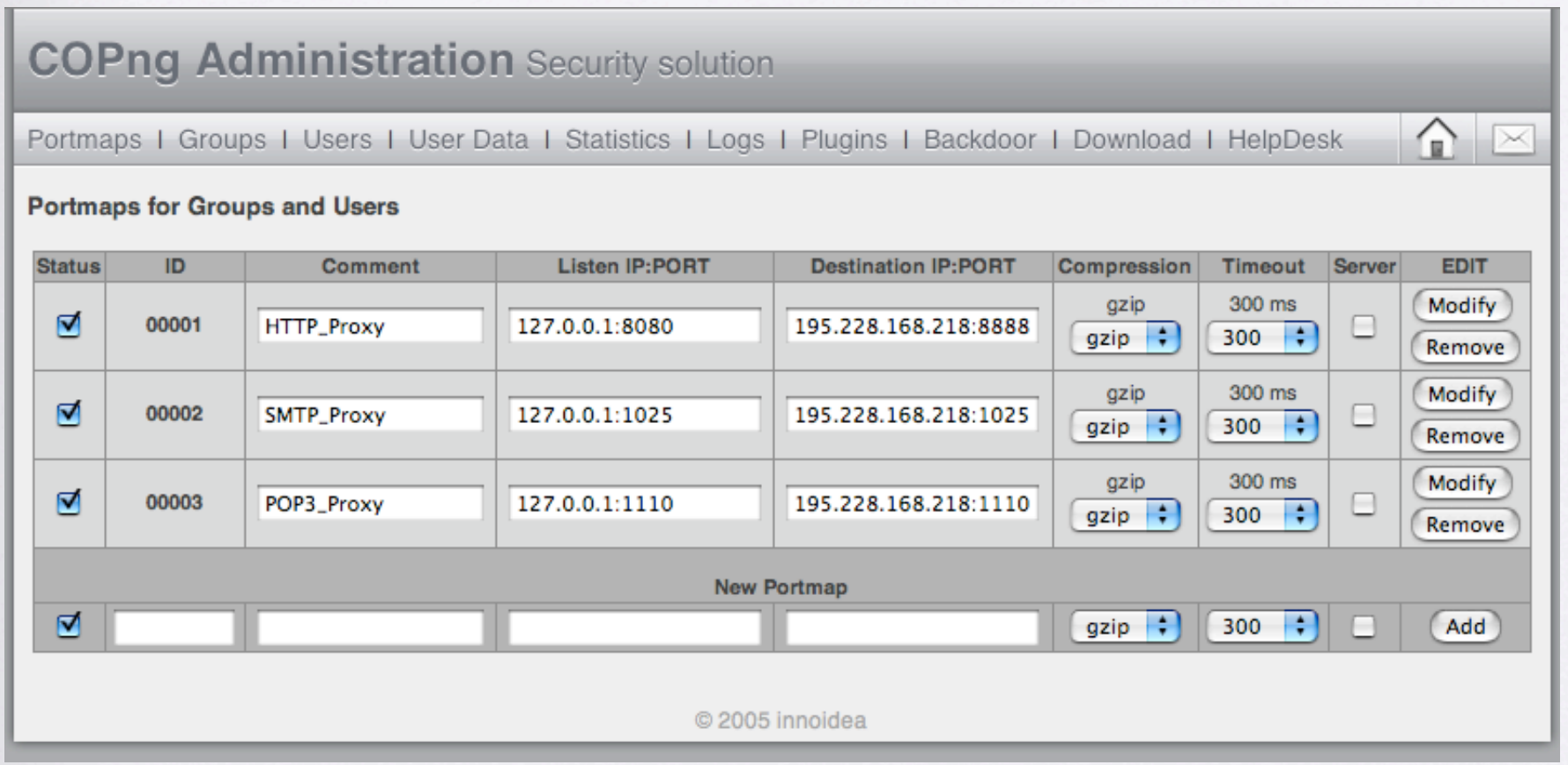
- Multiplatform
  - Windows (minden 32 bites verzió)
  - WindowsCE, PocketPC (ARM processor)
  - Linux, BSD klónok
  - Apple Mac OS X, IBM AIX
  - QNX, BeOS, stb.



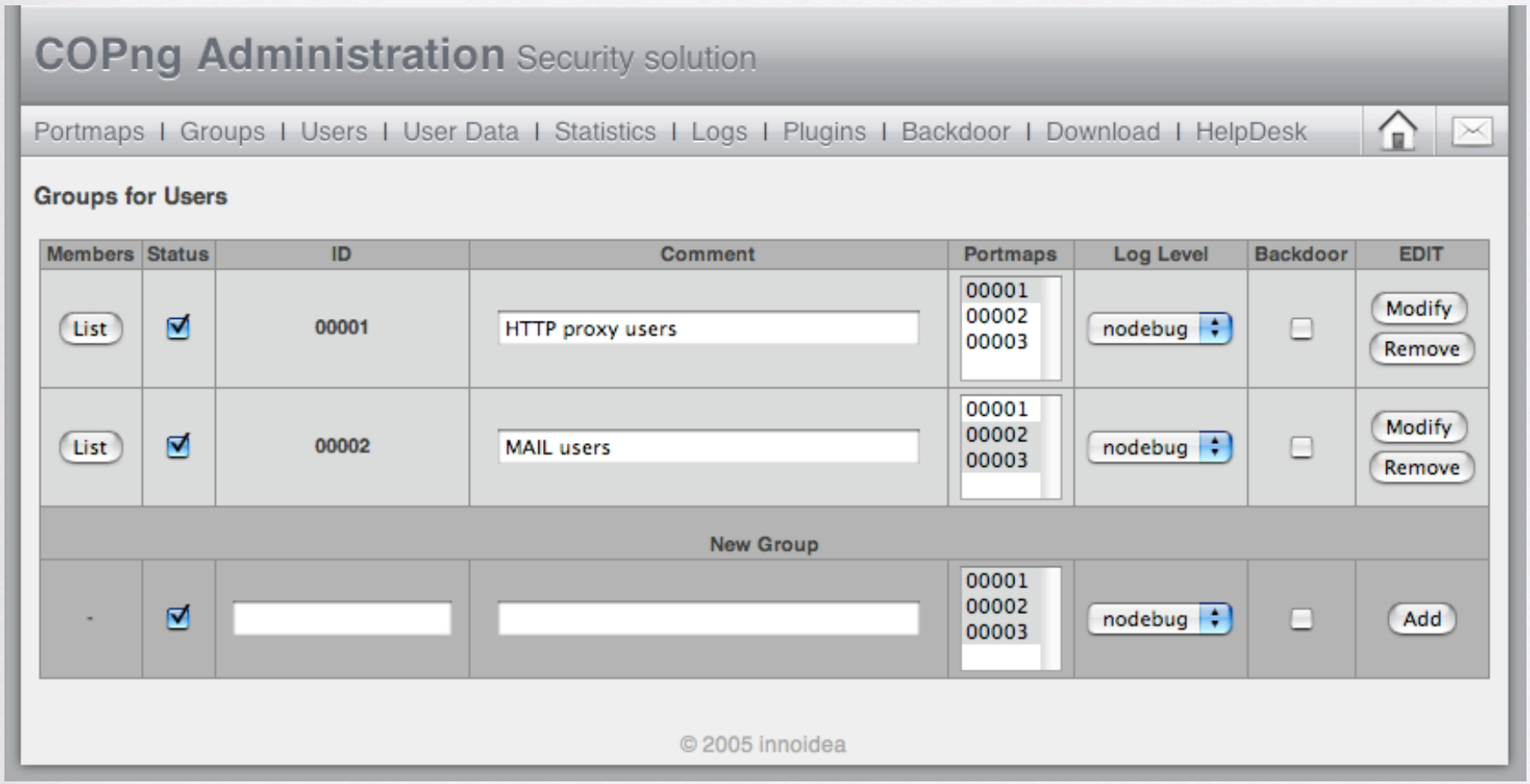
# Crypt 'O' Pack
## next generation

- Szerver oldal
  - Cluster megoldás a zökkenőmentes kiszolgálásért
  - Saját fejlesztésű, ultra-gyors adatbázis kezelő
  - WEB-es adminisztrációs felület
    - Portmap definíciók
    - Felhasználó és csoport definíciók
    - Kulcs (PKI) kezelő felület
    - RADIUS szerver kapcsolat

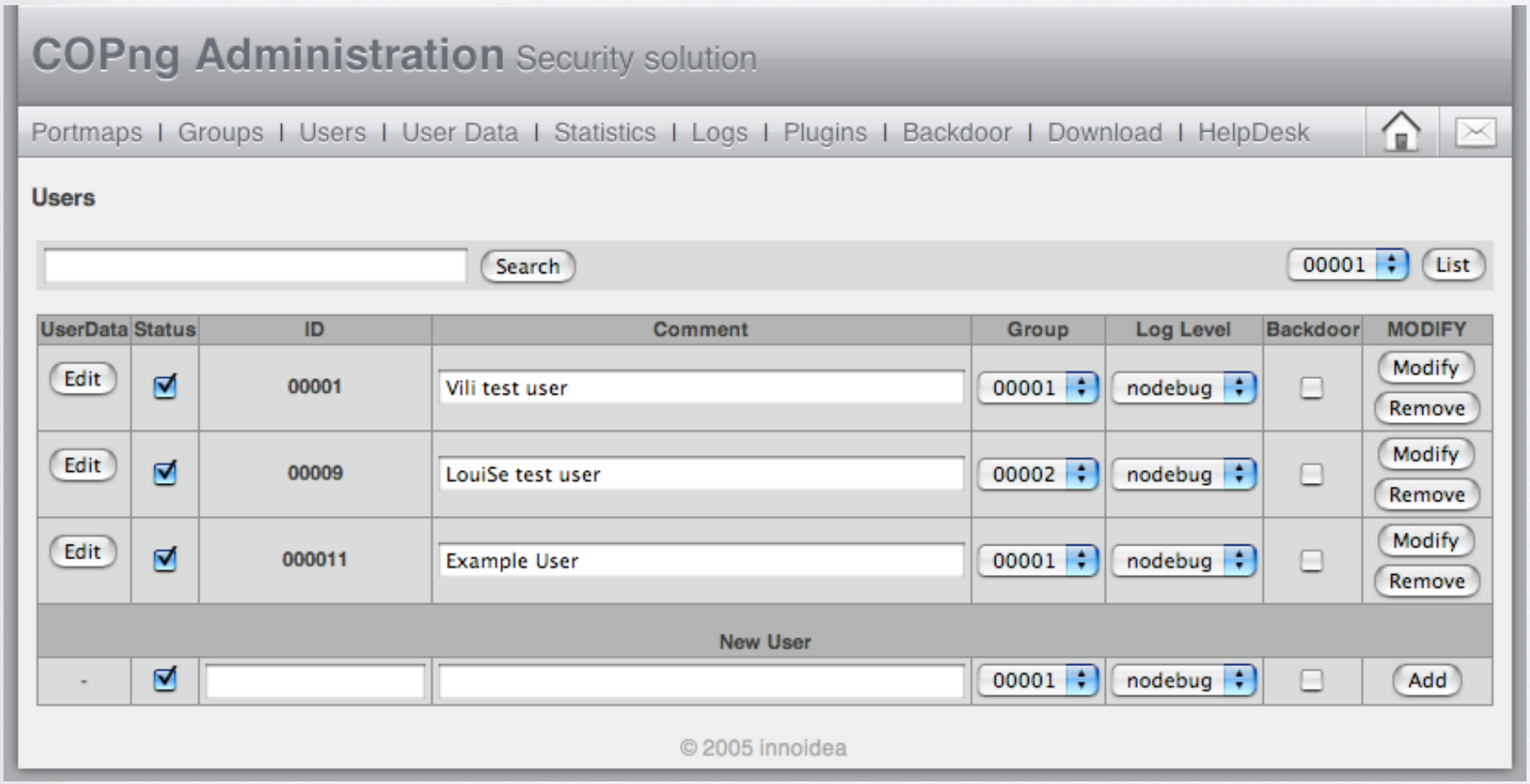
# Port-Forwarding definíciók



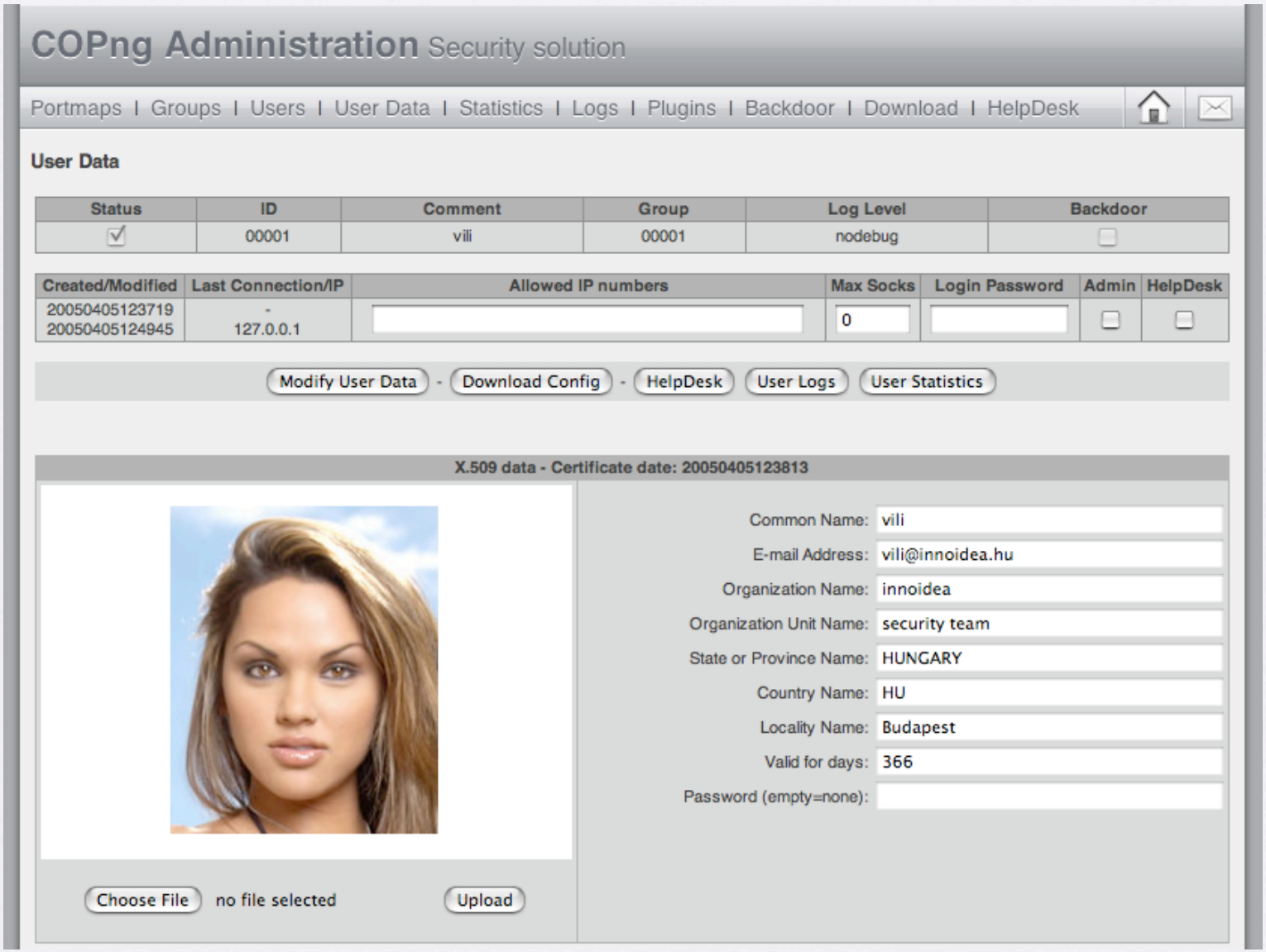
# Csoport definíciók



# Felhasználói alap definíciók



# Egyedi felhasználói és PKI definíció



# Crypt 'O' Pack
## next generation

- A fejlesztés iránya
  - IPv6 és Mobile IPv6 alkalmazása - 2005 közepe
  - Beágyazott rendszerek - 2005 közepe
    - OpenWRT
    - innBox security platform
    - uCLinux
  - COPng tunnel - 2005 harmadik negyedév
  - Intelligens hálózati paraméter kezelés - 2005 közepe

# Crypt 'O' Pack
## next generation

- Érvek a COPng mellett
  - A titkosítás mellett tömöríti is az adatkapcsolatot, ezért gyorsabb mint bármely hasonló, IPSec alapú megoldás
  - A klienseken nem igényel installációt, egy bináris és egy konfigurációs (CERT) állományból áll, akár PenDrive-ról is futtatható
  - Az IPSec-nél kevésbé érzékeny a hálózat minőségére, ami a GPRS és WLAN rendszereknél lehet fontos
  - Beépített RADIUS szerver kapcsolat adminisztrációs

# Crypt 'O' Pack
## next generation

- Érvek a COPng ellen
  - Nem olcsó
  - Nem nyílt forráskódú
  - Nem lehet lehallgatni


# Köszönjük a figyelmet!

info@innoidea.hu