the next generation of

Crypt ‘ O ‘ Pack

in security

and communication

by innoidea

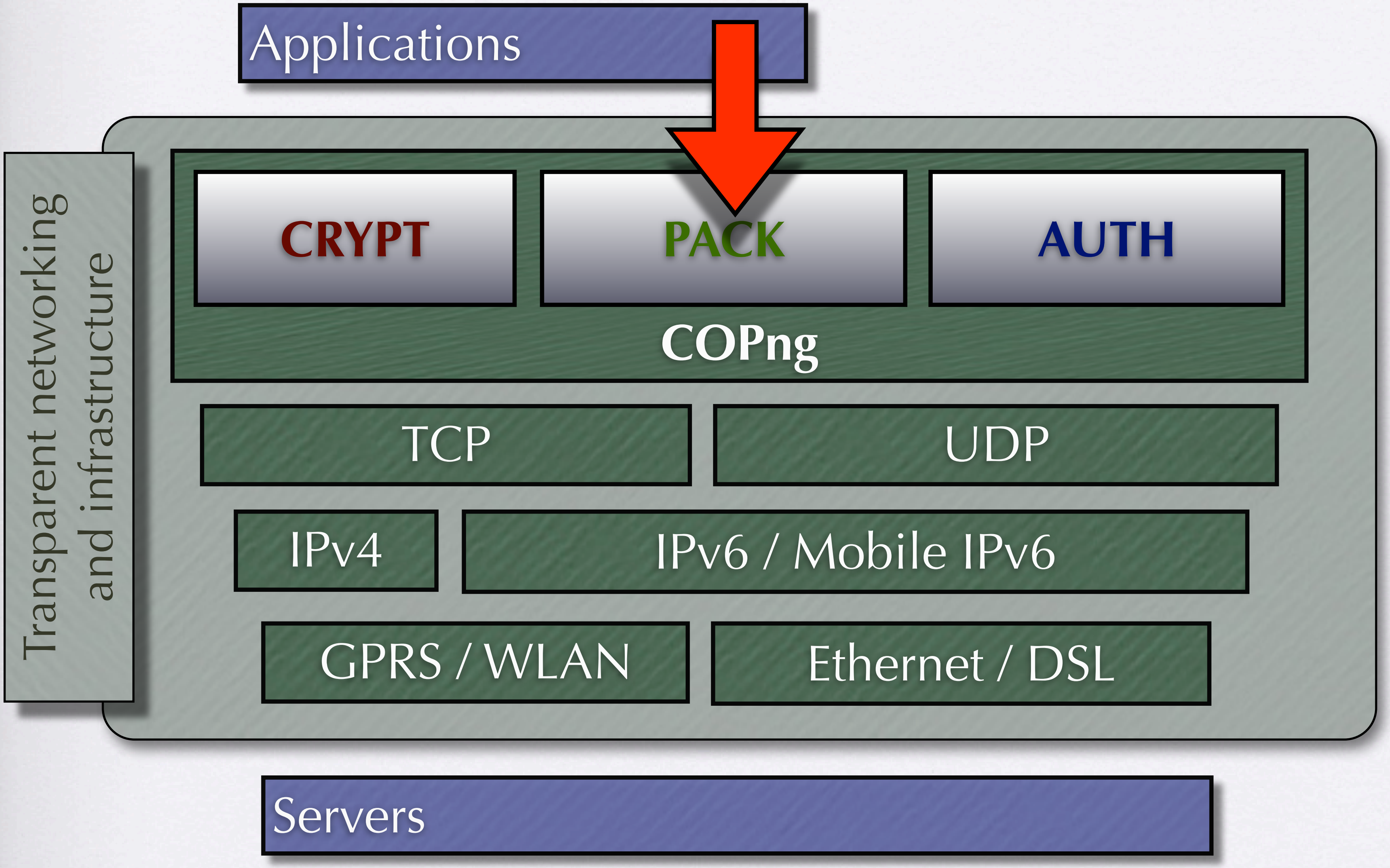
Lajos Nagy, 2005

SECURITY.INNOIDEA.HU

Crypt ’O’ Pack
next generation

- Realtime Encryption and Compression of data flow
- PKI Authentication
- Multiplatform solution
- Portable source
- Automatic, on-the-fly network/socket parameter modification - depend on network signal quality
- Works without robust Client side installation

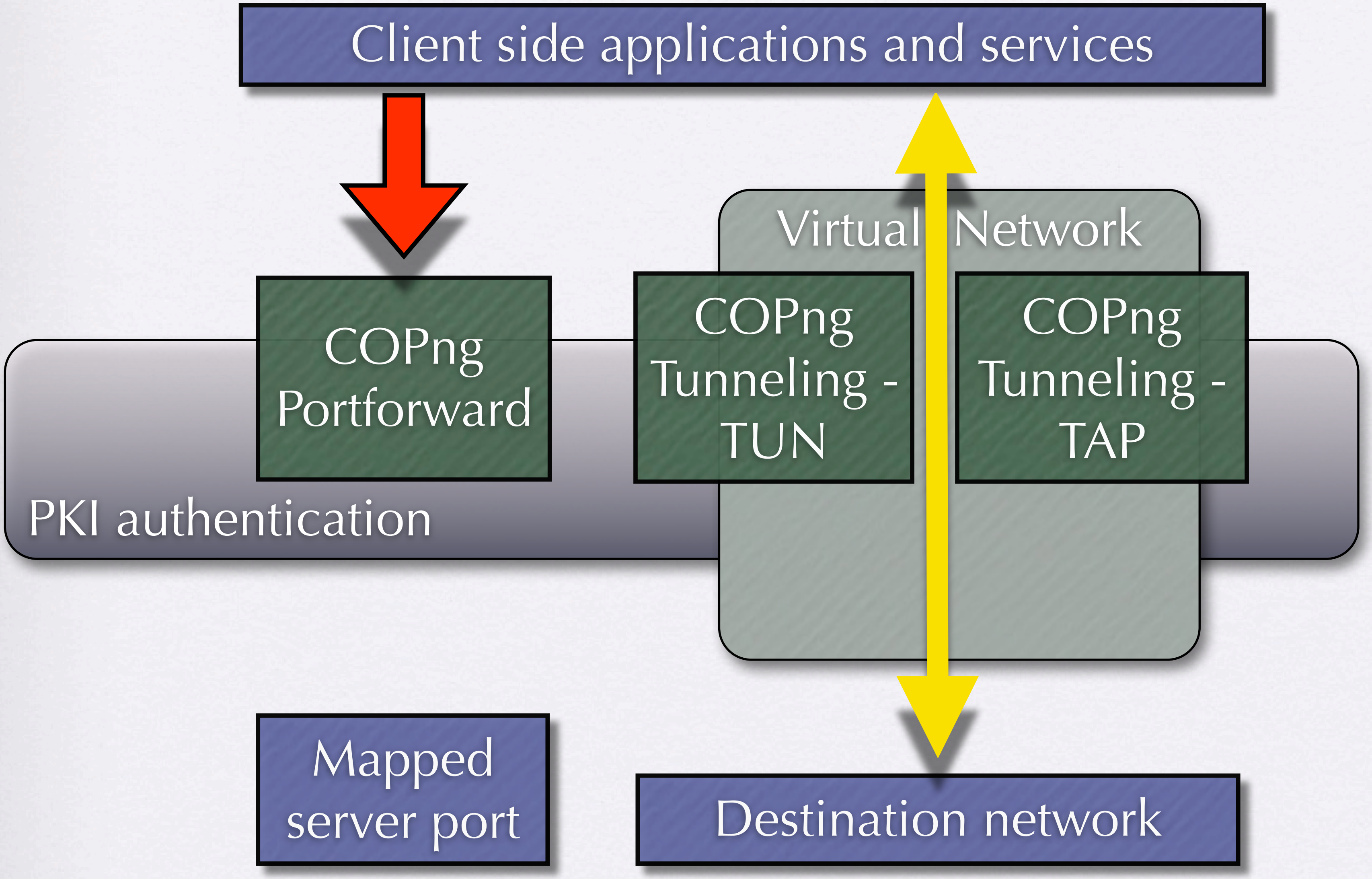
Crypt 'O' Pack
next generation



2009. augusztus 7.

Crypt 'O' Pack

next generation



Client side applications and services

Virtual Network

COPng Portforward

COPng Tunneling - TUN

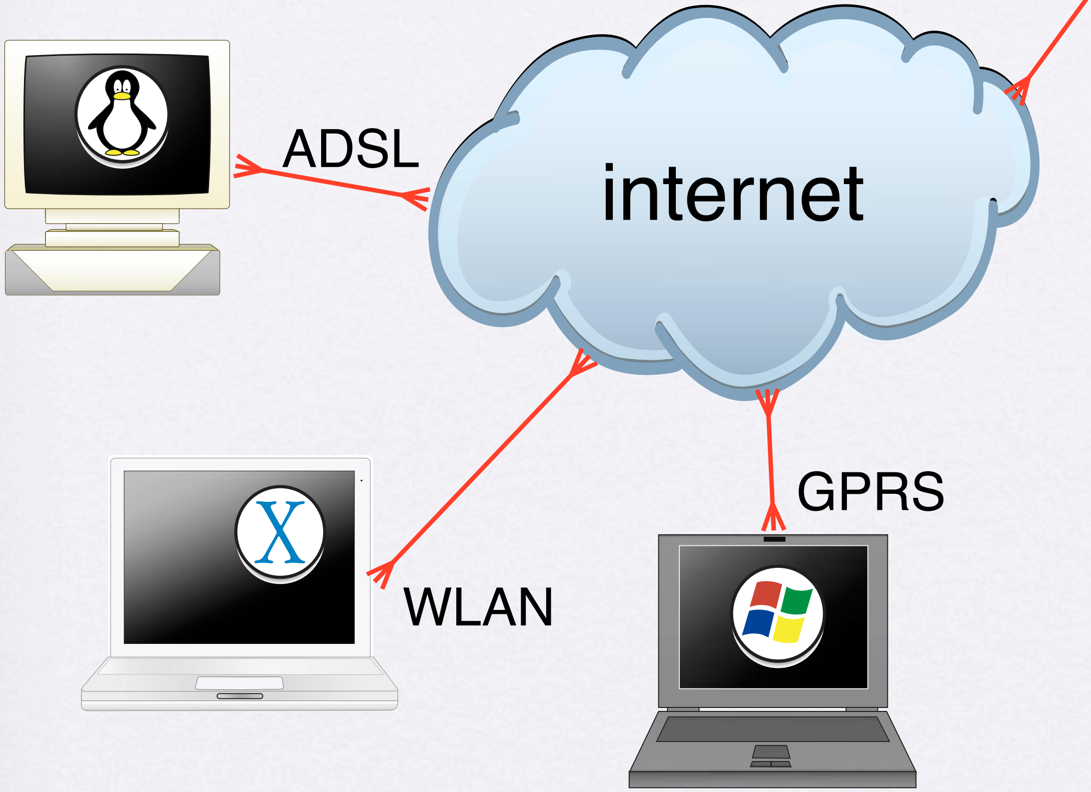
COPng Tunneling - TAP

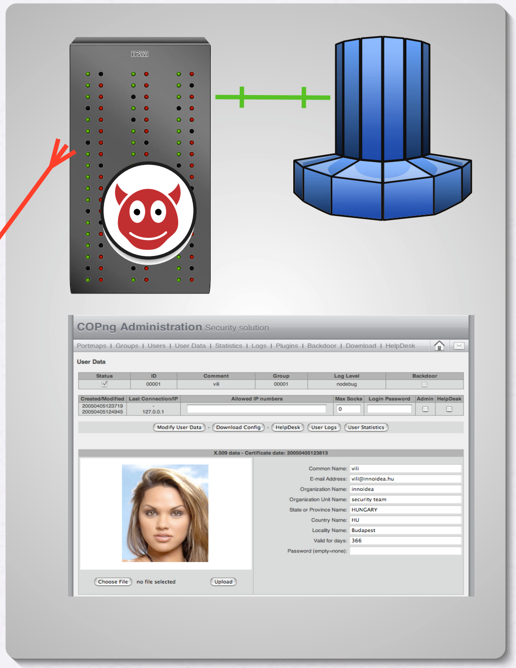
PKI authentication

Mapped server port

Destination network

Platform and network independent secure data connection





COPng Administration Security solution

Portmaps | Groups | Users | User Data | Statistics | Logs | Plugins | Backdoor | Download | HelpDesk

User Data

Status	ID	Comment	Group	Log Level	Backdoor
☑	00001	vili	00001	nodebug	□

Created/Modified	Last Connection/IP	Allowed IP numbers	Max Socks	Login Password	Admin	HelpDesk
20050405123719 20050405124945	- 127.0.0.1		0		□	□

Modify User Data - Download Config - HelpDesk User Logs User Statistics

X.509 data - Certificate date: 20050405123813

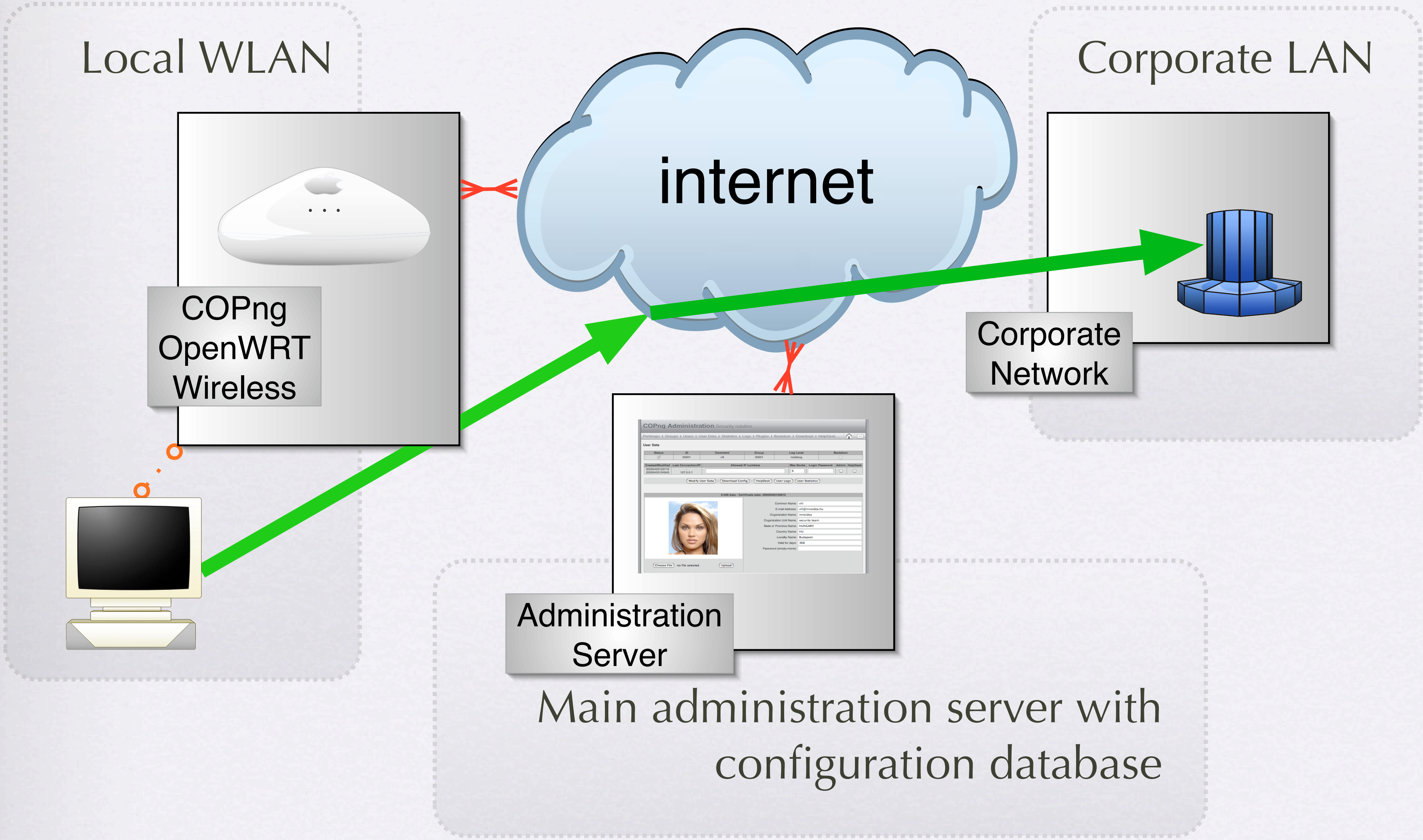
Common Name: vili
E-mail Address: vili@innoidea.hu
Organization Name: innoidea
Organization Unit Name: security team
State or Province Name: HUNGARY
Country Name: HU
Locality Name: Budapest
Valid for days: 366
Password (empty=none):

- HTTP
- IRC
- Samba
- POP3
- IMAP
- SMTP

- LDAP
- VNC
- X11
- Telnet
- SSH
- RSync

- Remote Desktop

Secure WLAN and internet sharing



Local WLAN

COPng OpenWRT Wireless

internet

Corporate LAN

Corporate Network

Administration Server

COPng Administration Security solution

Portmaps | Groups | Users | User Data | Statistics | Logs | Plugins | Backdoor | Download | HelpDesk

User Data

Status	ID	Comment	Group	Log Level	Backdoor
☑	00001	vili	00001	nodebug	□

Created/Modified	Last Connection/IP	Allowed IP numbers	Max Socks	Login Password	Admin	HelpDesk
20050405123719 20050405124945	- 127.0.0.1		0		□	□

Modify User Data - Download Config - HelpDesk User Logs User Statistics

X.509 data - Certificate date: 20050405123813

Common Name: vili
E-mail Address: vili@innoidea.hu
Organization Name: innoidea
Organization Unit Name: security team
State or Province Name: HUNGARY
Country Name: HU
Locality Name: Budapest
Valid for days: 366
Password (empty=none):

Main administration server with configuration database

Crypt 'O' Pack
next generation

- Crypt
  - SSL based library with automatic selection of the strongest available cryptographic algorithm by the beginning of connection
  - Modular algorithm handling
  - More SSL implementations are supported, but "session-caching" support is mandatory

Why buy an SSL toolkit as a black-box when you can get an open one for free?

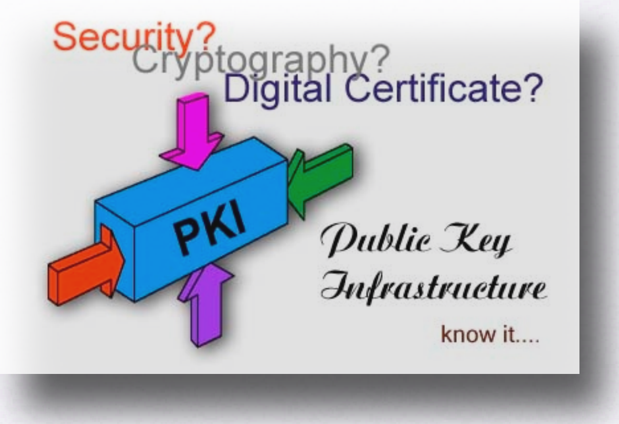
MatrixSSL SSL.com OpenSSL

Crypt ’O’ Pack
next generation

- Compression
  - Open-source standard compression libraries (BZIP2, GZIP, LZO).
  - Compression algorithm and method connectivity by application type.
  - Expandable algorithm store for special applications.

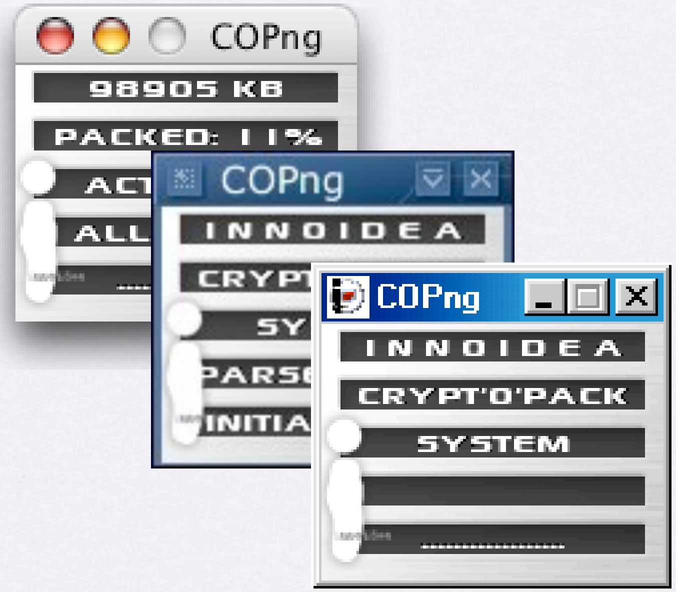
Crypt 'O' Pack
next generation

- Authentication
  - PKI based authentication
    - Own PKI server
      - Integrated into COPng administration system
    - External PKI server
      - X500
      - LDAP
      - Windows Active Directory



Crypt 'O' Pack
next generation

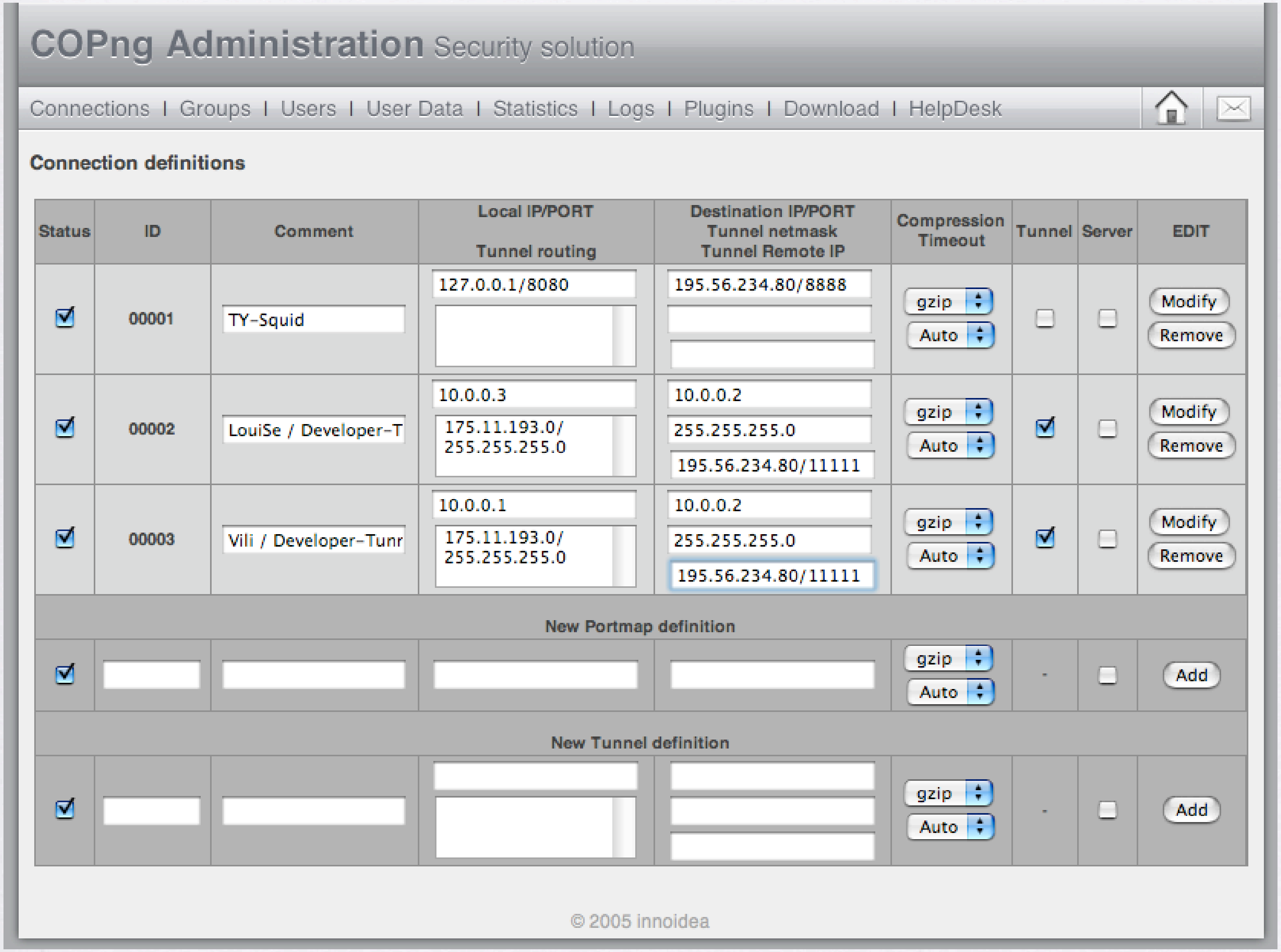
- Multiplatform solution
  - Windows (all 32 bit version)
  - WindowsCE, PocketPC (ARM processor)
  - Linux, BSD clones
  - Apple Mac OS X, IBM AIX
  - QNX, BeOS, stb.



Crypt ’O’ Pack
next generation

- Server side
  - FreeBSD-based COPng HA Cluster
  - Special, ultra-fast database engine
  - WEB based administration interface
    - Connection definitions
    - User and Group definitions
    - Certificate (PKI) administrator
    - RADIUS server connection

Connection definitions



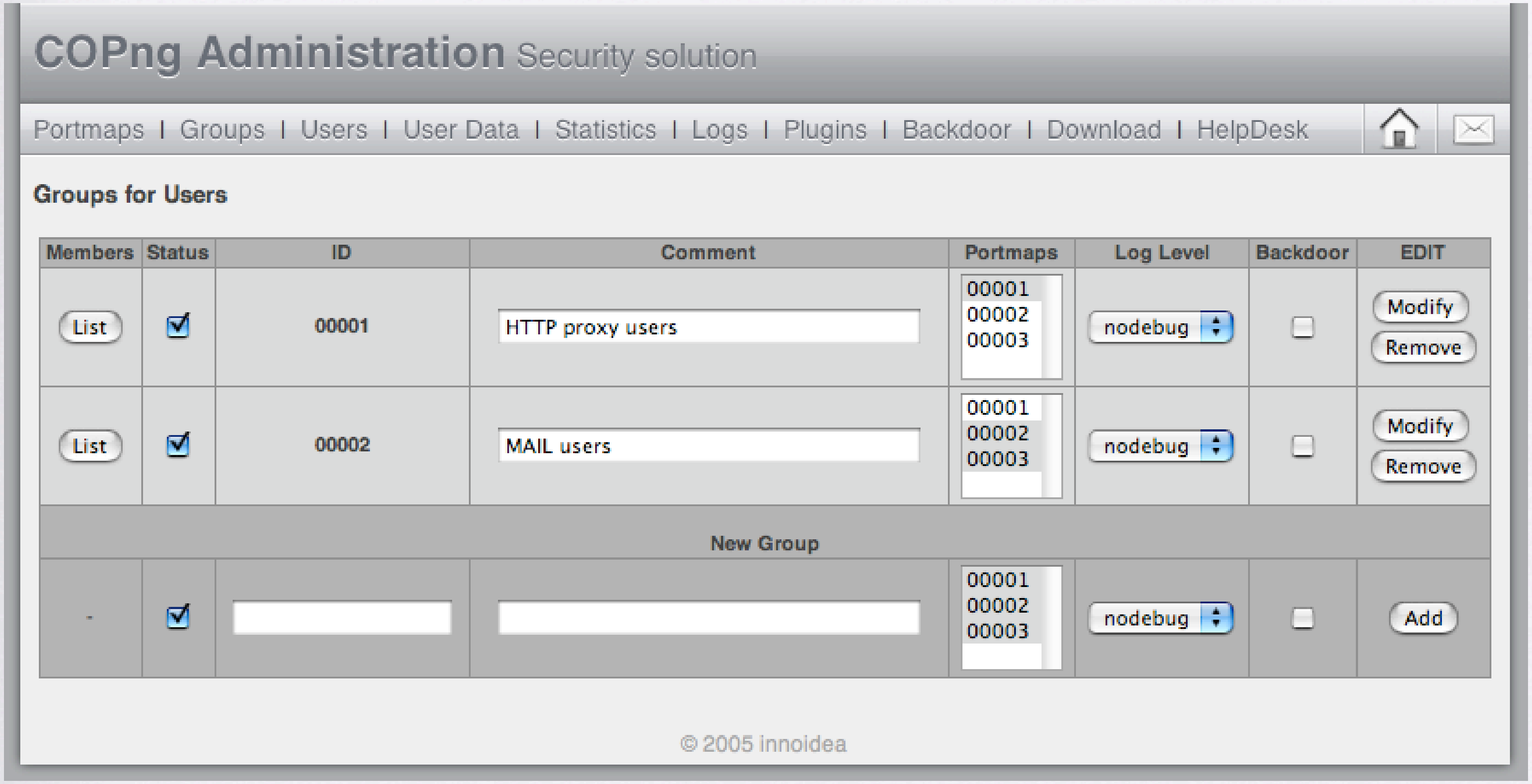
COPng Administration Security solution
Connections | Groups | Users | User Data | Statistics | Logs | Plugins | Download | HelpDesk

Connection definitions

Status	ID	Comment	Local IP/PORT Tunnel routing	Destination IP/PORT Tunnel netmask Tunnel Remote IP	Compression Timeout	Tunnel	Server	EDIT
☑	00001	TY-Squid	127.0.0.1/8080	195.56.234.80/8888	gzip Auto	□	□	Modify Remove
☑	00002	LouiSe / Developer-T	10.0.0.3 175.11.193.0/ 255.255.255.0	10.0.0.2 255.255.255.0 195.56.234.80/11111	gzip Auto	☑	□	Modify Remove
☑	00003	Vili / Developer-Tunr	10.0.0.1 175.11.193.0/ 255.255.255.0	10.0.0.2 255.255.255.0 195.56.234.80/11111	gzip Auto	☑	□	Modify Remove
New Portmap definition								
☑					gzip Auto	-	□	Add
New Tunnel definition								
☑					gzip Auto	-	□	Add

© 2005 innoidea

Group definitions

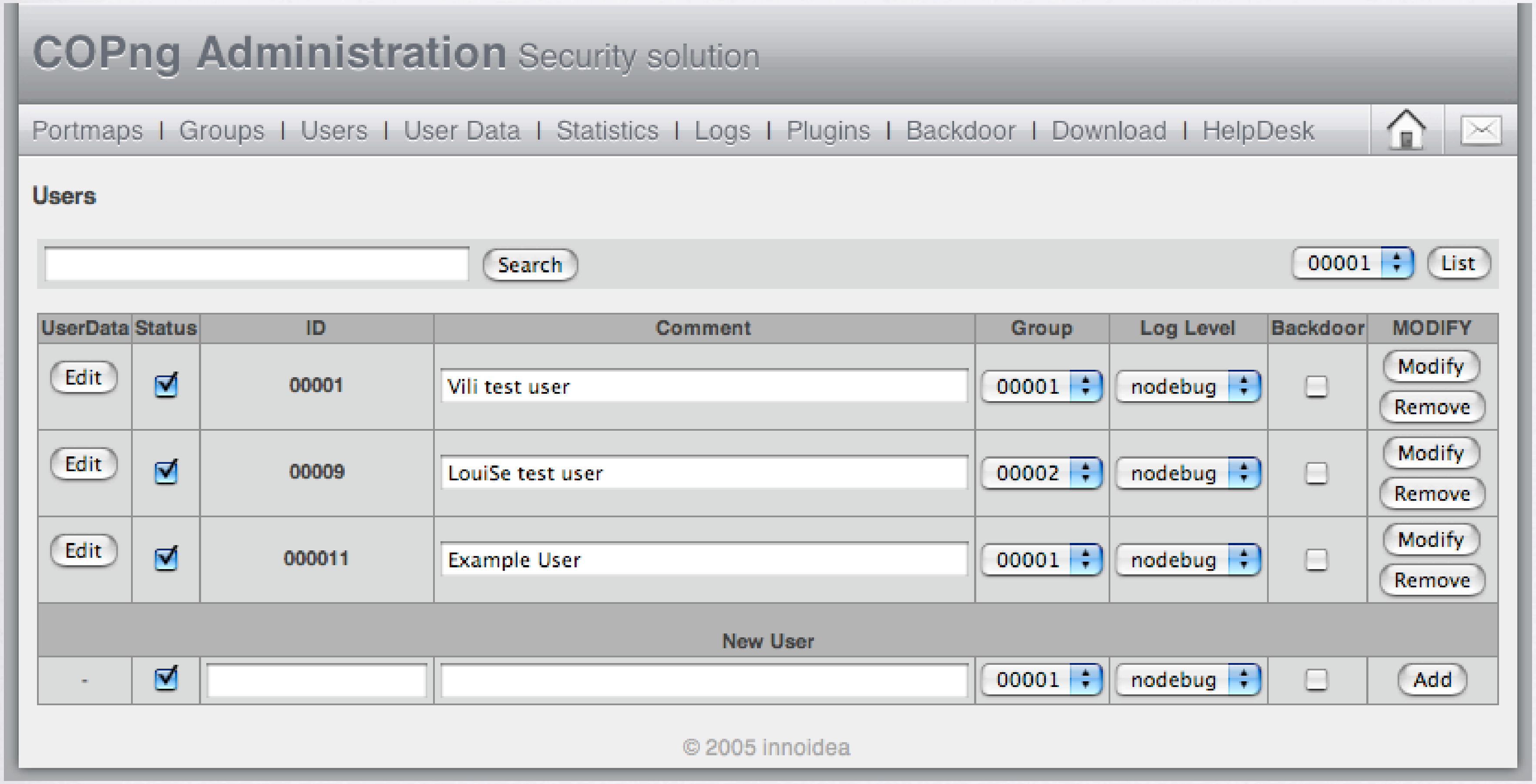

COPng Administration Security solution
Portmaps | Groups | Users | User Data | Statistics | Logs | Plugins | Backdoor | Download | HelpDesk

Groups for Users

Members	Status	ID	Comment	Portmaps	Log Level	Backdoor	EDIT
List	☑	00001	HTTP proxy users	00001 00002 00003	nodebug	□	Modify Remove
List	☑	00002	MAIL users	00001 00002 00003	nodebug	□	Modify Remove
New Group							
-	☑			00001 00002 00003	nodebug	□	Add

© 2005 innoidea

Main user definitions

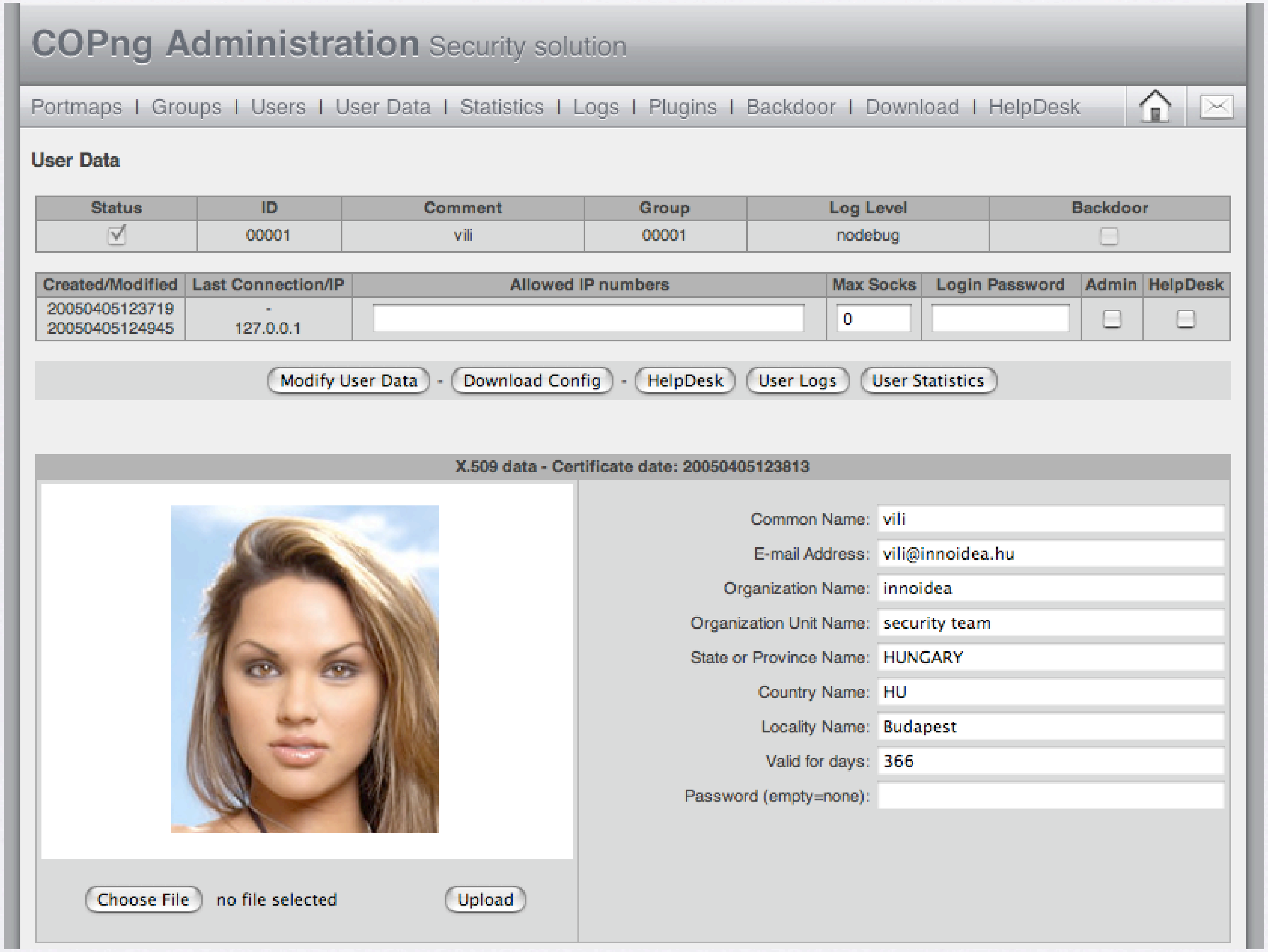

COPng Administration Security solution
Portmaps | Groups | Users | User Data | Statistics | Logs | Plugins | Backdoor | Download | HelpDesk
Search
00001
List

Users

UserData	Status	ID	Comment	Group	Log Level	Backdoor	MODIFY
Edit	☑	00001	Vili test user	00001	nodebug	□	Modify Remove
Edit	☑	00009	LouiSe test user	00002	nodebug	□	Modify Remove
Edit	☑	000011	Example User	00001	nodebug	□	Modify Remove
New User							
-	☑			00001	nodebug	□	Add

© 2005 innoidea

User with PKI defintions


COPng Administration Security solution
Portmaps | Groups | Users | User Data | Statistics | Logs | Plugins | Backdoor | Download | HelpDesk

User Data

Status	ID	Comment	Group	Log Level	Backdoor
☑	00001	vili	00001	nodebug	□

Created/Modified	Last Connection/IP	Allowed IP numbers	Max Socks	Login Password	Admin	HelpDesk
20050405123719 20050405124945	- 127.0.0.1		0		□	□

Modify User Data - Download Config - HelpDesk User Logs User Statistics

X.509 data - Certificate date: 20050405123813

Common Name:	vili
E-mail Address:	vili@innoidea.hu
Organization Name:	innoidea
Organization Unit Name:	security team
State or Province Name:	HUNGARY
Country Name:	HU
Locality Name:	Budapest
Valid for days:	366
Password (empty=none):	

Comparison of different solutions

	COPng	IPSec	OpenVPN
Tunneling support	TUN/TAP	modified IP stack	TUN/TAP
Security protocol	SSL	IPSec	SSL
Multi threaded application	YES	no	YES
Compression	gzip, bzip2, lzo, none	no	no
Automatic socket tuning	YES	no	no
Running in ...	users pace	kernel space	user space

Crypt 'O' Pack
next generation

- Development strategy
  - Optimization of IPv6 and Mobile IPv6 implementation
  - Support for other embedded systems
    - OpenWRT
    - uCLinux
  - Improvement of intelligent network parameter handling for wireless networks

Crypt ’O’ Pack
next generation

- Why COPng?
  - Simultaneous encryption and compression of data makes it a faster and more secure transfer layer than existing alternatives!
  - No bloated client-side installation required, works even with a pendrive copy...
  - Intelligent, automatic network parameter handling to optimize air-net (GPRS, WiFi, Bluetooth) usage
  - Integrated RADIUS server administration and connection

Crypt 'O' Pack
next generation

- Why not COPng?
  - Not free, not opensource
  - Not cheap
  - Unable to monitor the data in COPng channel

thanks for participating

info@innoidea.hu