



the next generation of

Crypt 'O' Pack in security

by innoidea

Lajos Nagy, 2005

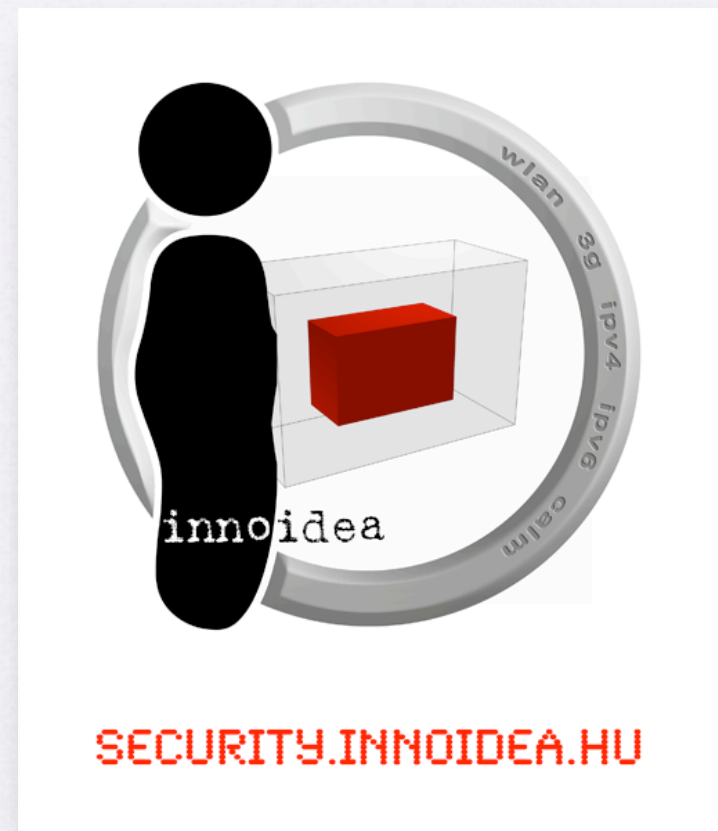


SECURITY.INNOIDEA.HU

Crypt 'O' Pack

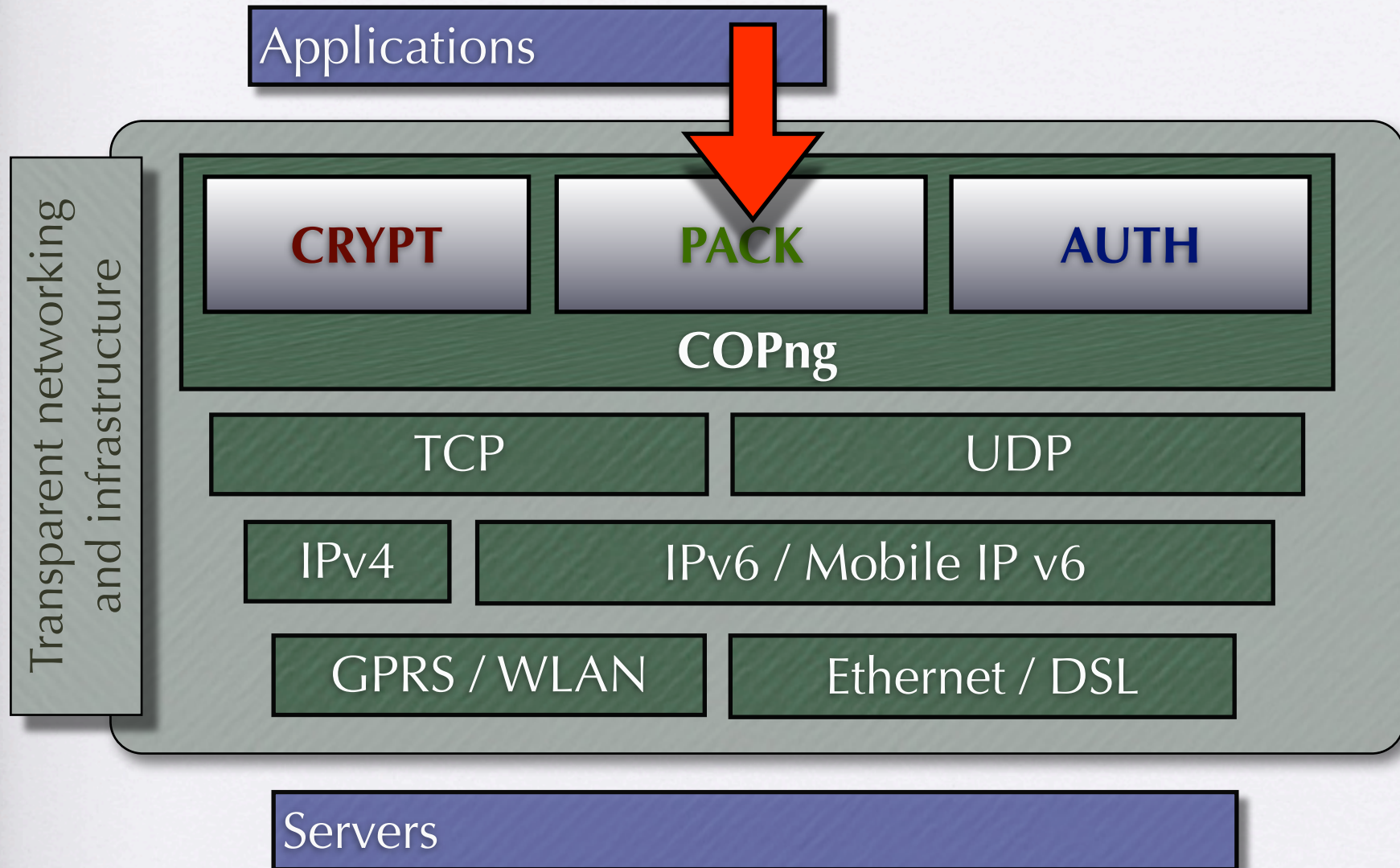
next generation

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

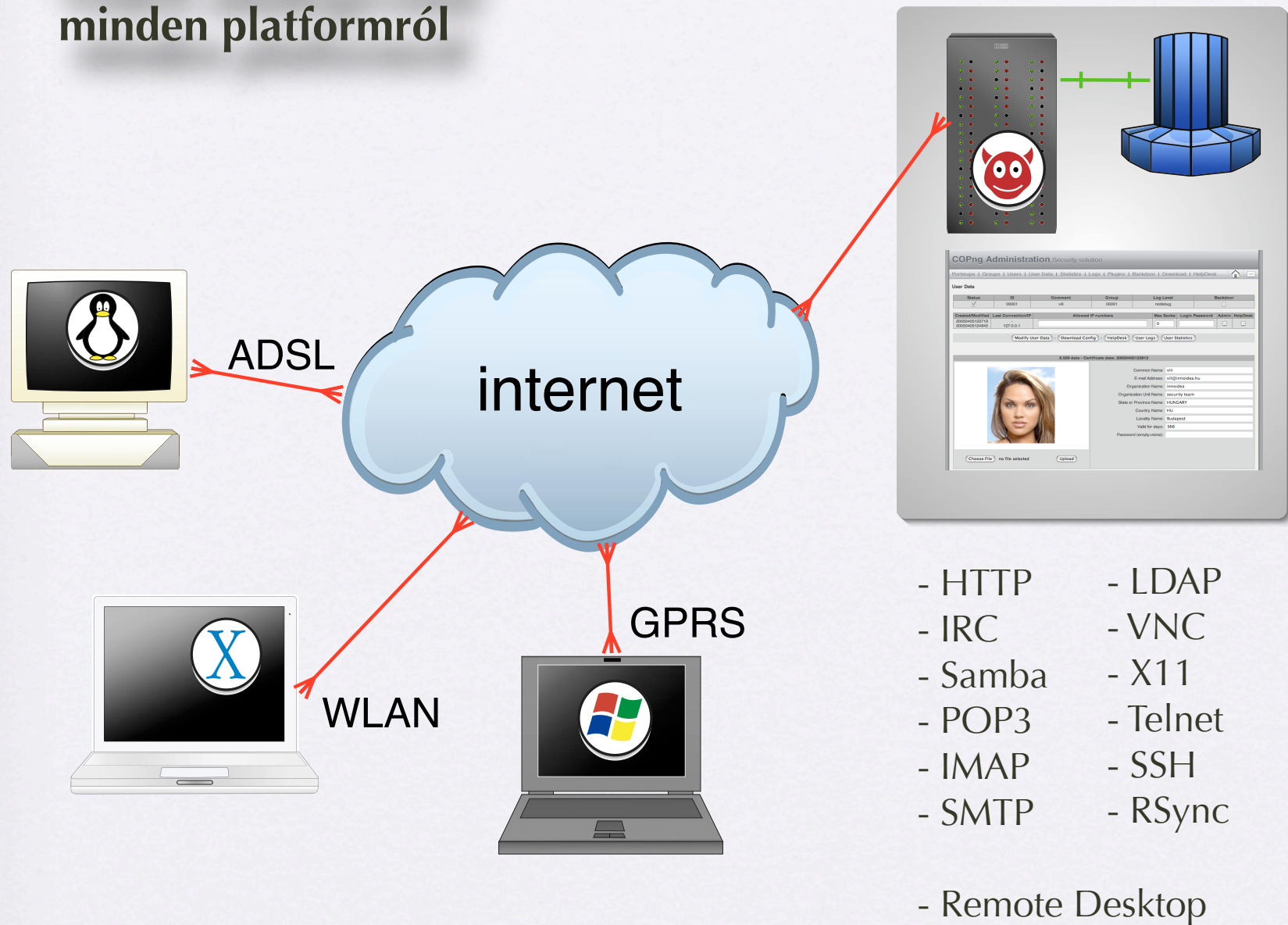


Crypt 'O' Pack

next generation

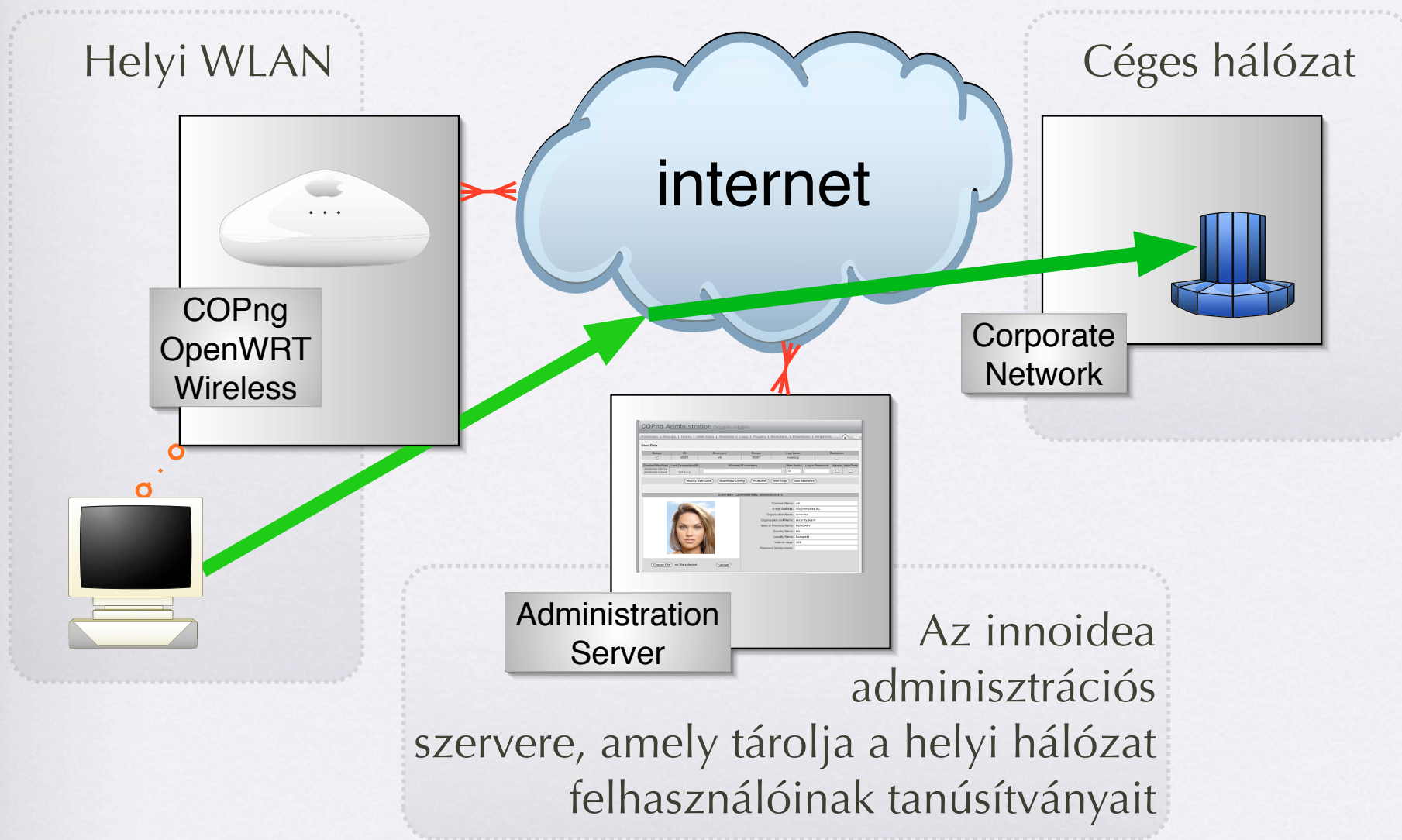


Védett adatkapcsolat minden platformról



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

Titkosított, autentikált 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

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

Crypt 'O' Pack

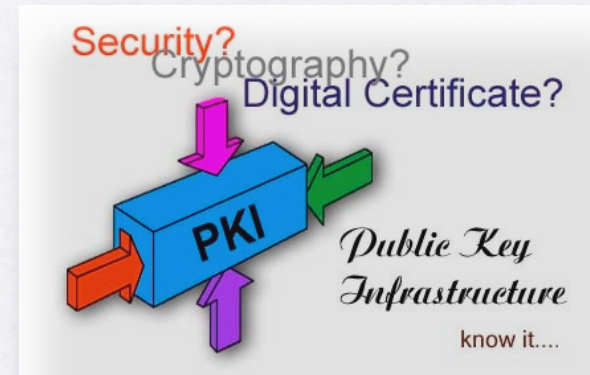
next generation

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

Crypt 'O' Pack

next generation

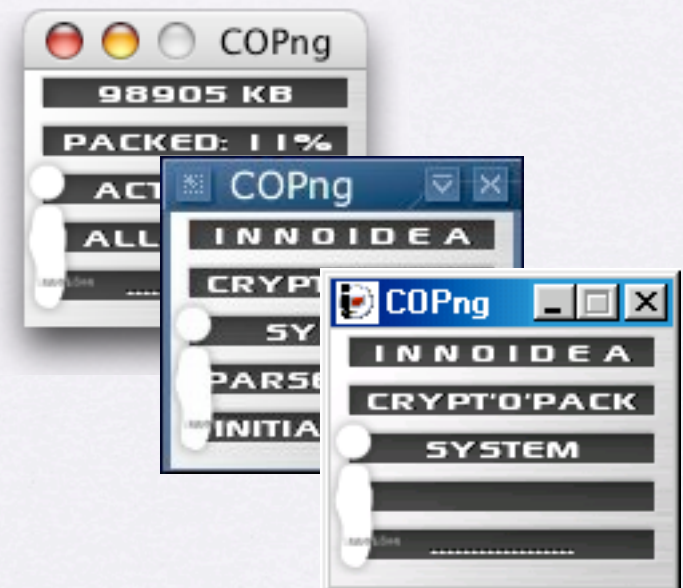
- Azonosítás
 - PKI rendszerű azonosítás
 - Saját PKI szerver
 - Integrálva az adminisztrációs rendszerbe
 - Külső PKI szerver
 - X500
 - LDAP
 - Windows Active Directory



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

COPng Administration Security solution

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

Portmaps for Groups and Users

Status	ID	Comment	Listen IP:PORT	Destination IP:PORT	Compression	Timeout	Server	EDIT
<input checked="" type="checkbox"/>	00001	HTTP_Proxy	127.0.0.1:8080	195.228.168.218:8888	gzip gzip ▾	300 ms 300 ▾	<input type="checkbox"/>	Modify Remove
<input checked="" type="checkbox"/>	00002	SMTP_Proxy	127.0.0.1:1025	195.228.168.218:1025	gzip gzip ▾	300 ms 300 ▾	<input type="checkbox"/>	Modify Remove
<input checked="" type="checkbox"/>	00003	POP3_Proxy	127.0.0.1:1110	195.228.168.218:1110	gzip gzip ▾	300 ms 300 ▾	<input type="checkbox"/>	Modify Remove
New Portmap								
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	gzip ▾	300 ▾	<input type="checkbox"/>	Add

© 2005 innoidea

Csoport definíciók

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	<input checked="" type="checkbox"/>	00001	HTTP proxy users	00001 00002 00003	nodebug	<input type="checkbox"/>	Modify Remove
List	<input checked="" type="checkbox"/>	00002	MAIL users	00001 00002 00003	nodebug	<input type="checkbox"/>	Modify Remove
New Group							
-	<input checked="" type="checkbox"/>			00001 00002 00003	nodebug	<input type="checkbox"/>	Add

© 2005 innoidea

Felhasználói alap definíciók

COPng Administration Security solution

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

Users

Search 00001 List

UserData	Status	ID	Comment	Group	Log Level	Backdoor	MODIFY
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	00001	Vili test user	00001	nodebug	<input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	00009	LouiSe test user	00002	nodebug	<input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	000011	Example User	00001	nodebug	<input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
New User							
-	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	00001	nodebug	<input type="checkbox"/>	<input type="button" value="Add"/>

© 2005 innoidea

Egyedi felhasználói és PKI definíció

COPng Administration Security solution

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


User Data

Status	ID	Comment	Group	Log Level	Backdoor
<input checked="" type="checkbox"/>	00001	vili	00001	nodebug	<input type="checkbox"/>

Created/Modified	Last Connection/IP	Allowed IP numbers	Max Socks	Login Password	Admin	HelpDesk
20050405123719	-		0		<input type="checkbox"/>	<input type="checkbox"/>
20050405124945	127.0.0.1					

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):

Choose File no file selected Upload

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!

innoidea

info@innoidea.hu