

Garante e Data Security

Nicola Fusco
South Europe Area Manager
Sales & Business Development

Raz-Lee Security Ltd.

IBM Italia Forum
Segrate 8 settembre 2009



Agenda

La Sicurezza dei dati e la piattaforma IBM System i

- Chi è Raz-Lee Security Ltd. ? e la sua esperienza!
- La “Sicurezza Operativa” per la protezione dei dati del sistema IBM AS400
- La Soluzione software di Raz-Lee: XXXXXXXXXX
 - Come Raz-Lee offre il supporto per le 2 tipologie di Sicurezza
 - Presentazione generale dei moduli della soluzione **iSecurity**
 - Prospetto Economico e Formule di Vendita

L'Azienda



Raz-Lee Security Ltd. Company Profile

- Multinazionale israeliana fondata nel 1983 dal Sig. Shmuel Zailer, attualmente in carica come CEO e R&D Technical Director;
 - Focalizzata 100% sulla piattaforma AS400 >> iSeries >> System i
 - Ha sviluppato più di 20 tool, con funzionalità esclusive per l' AS400
 - Dal 1998 si occupa della Sicurezza, per la piattaforma AS400
 - Uffici diretti a Tel Aviv (HQ + R&D) e USA (Sales)
 - Rete di Distribuzione e Reselling che si sta sviluppando in oltre 50 paesi, in tutto il globo
-
- FY 2007: 1mo Ufficio diretto in Europa a Cusano M.no (MI)
 - 1 x Sales & Business Development
 - 2 x Presales Technical Engineers for Security Support
 - 1 x Postsales Technical Engineer Support (Milano & Roma)
 - 1 x Postsales Technical Engineer Support 3° Livello (Israele, italiano)



Sicurezza Operativa



IBM Italia Forum
Segrate 23 luglio 2009



Sicurezza Operativa del PowerSystem i

1. Concetto base sulla sicurezza del System i, condiviso da Raz-Lee:

- Per le sue caratteristiche il System i è un sistema sicuro
 - OS400 è un Sistema Operativo proprietario
 - Tecnologia ad oggetti (applicazioni)
 - In ambito Networking (era) basato su Architettura SNA

2. Perché Raz-Lee produce una soluzione per proteggere il System i?

- perchè esiste Internet con il suo bagaglio di tecnologia
 - L'uso dei protocolli FTP, TCP/IP, ...
- Perché non è più "solo" il Sistema Aziendale, ma una risorsa integrata e condivisa all'interno del network aziendale alla quale tutti possono e devono accedere,aumentando le minacce alla sicurezza dei dati...
 - Servizi abilitati automaticamente nei software di emulazione
 - Uso spregiudicato dei Driver ODBC

Sicurezza Operativa del PowerSystem i

2. Perché Raz-Lee produce una soluzione per proteggere il System i?

-perchè in internet sono disponibili queste informazioni
- AS/400 FTP Server User Accounts Disclosure 5 Apr. 2005
- AS/400 servers support FTP in two modes, legacy mode and IFS mode, and supports switching between both modes by a special FTP command. When in IFS mode, it is possible to create a special symbolic link file and retrieve the full list of user accounts.

<http://www.securiteam.com/unixfocus/5XP031FFFQ.html>

- **Vulnerability in the 5250 terminal**
- Nowadays, when working with legacy AS/400 applications, most people use Telnet based terminal emulation programs, for example IBM Client Access. A vulnerability in the 5250 terminal support allows using it to cause the user to unwillingly execute arbitrary commands. For full details and sample code please read the following PDF file:

http://www.venera.com/downloads/Attack_5250_terminal_emulations_from_iSeries_server.pdf



Sicurezza Legislativa



IBM Italia Forum
Segrate 23 luglio 2009



Normative internazionali e nazionali

Ambito internazionale

- Sarbanes Oxley (SOX)
- Basel 2, PCI (Payment Card Industry Data Security)
- HIPAA (sanità)
- Allegati Tecnici relativi allo Standard ISO

Ambito nazionale

- **D Lgs 196/2003 (Privacy):**

Testo unico, di seguito denominato “Codice“

- **Comunicato Stampa del 22 marzo 2004:**

Introduzione e Presentazione del DPS Aziendale annualmente aggiornato

- **Provvedimento del 27 novembre 2008**

Funzione aziendali di Amministratore di Sistema

Elenco del Amministratori di sistema e valutazione caratteristiche

Verifica delle attività di garanzia della sicurezza informatica aziendale

Registrazione Accessi

Servizi in Outsourcing

Come approcciare le richieste delle Normative

- Le varie regolamentazioni attribuiscono delle responsabilità, per:
 - Il Top Management
 - Staff del Dipartimento EDP (in quella degli AdS)

Come devono essere qualificate le varie normative...?!?

- **Strumento di lavoro e parte del background aziendale, con le quali:**
 - Produrre un'analisi ed una valutazione del rischio di gestione (*Risk Assessment*)
 - Segnalare al Top Management la necessità e l'importanza dei controlli da realizzare
 - Definire una politica di sicurezza
 - Delimitare l'ambito di competenza degli Utenti
 - Redigere una relazione sul mantenimento delle normative (*Risk Management*)



iSecurity for System Administrators



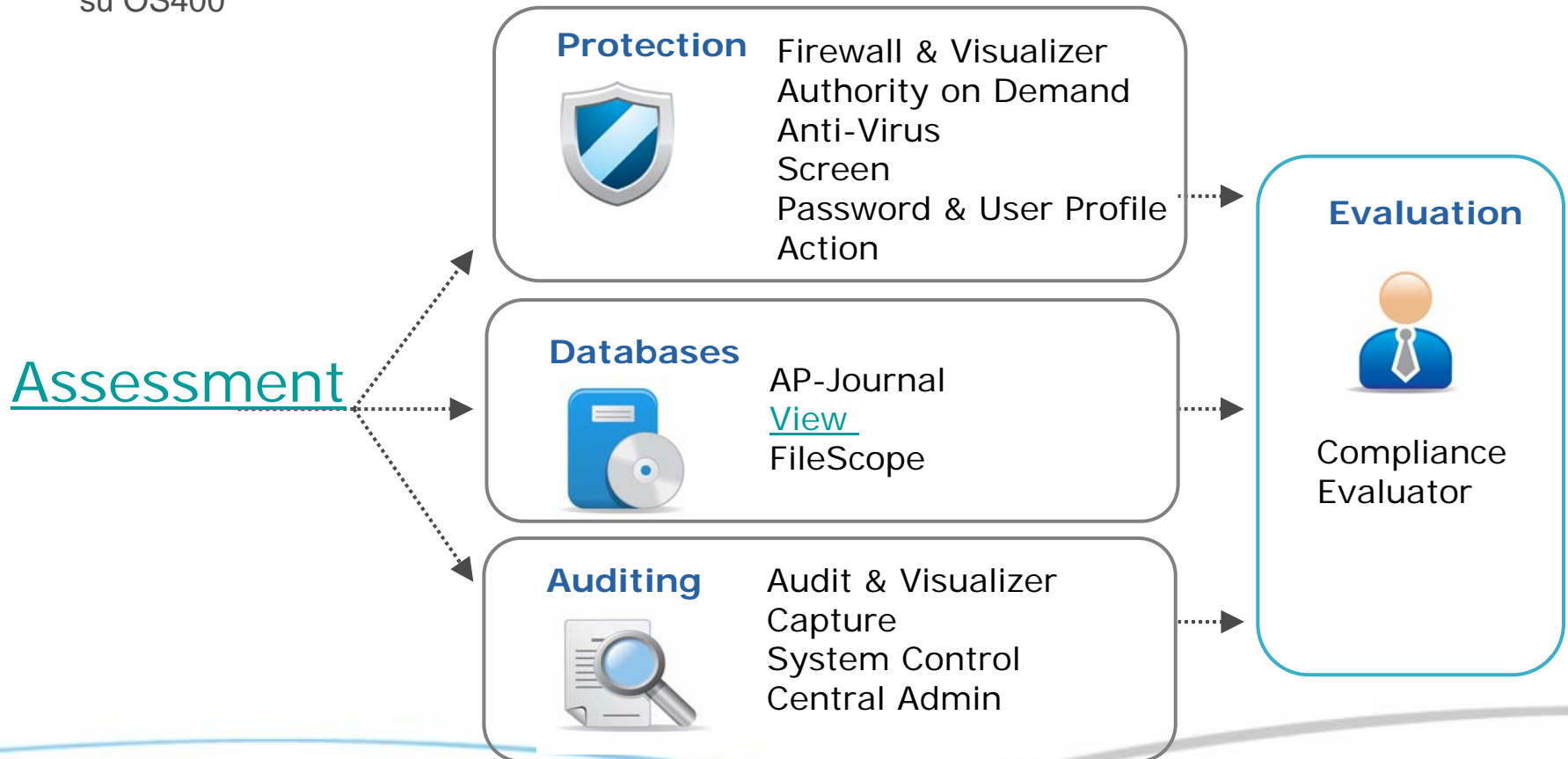
IBM Italia Forum
Segrate 23 luglio 2009



iSecurity – Missione della Soluzione

iSecurity è basata sul sistema operativo OS400; con iSecurity, l'Amministratore del Servizio è in grado di configurare il sistema in maniera centralizzata e secondo le regolamentazioni legate all'accesso, l'uso dei dati (singolo utente e per gruppi di utenti), eventi su applicazioni multiple.

Il tempo è inferiore di almeno 10 volte rispetto ad una parametrizzazione manuale, sviluppata direttamente su OS400



iSecurity “System Administrator Package”

Assessment

Prevenzione



Firewall + Visualizer
Authority on Demand
Password & User Managt

(Anti-Virus)

Controllo dei Dati



AP-Journal

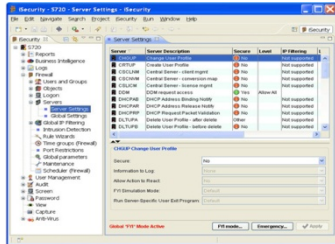
Auditing



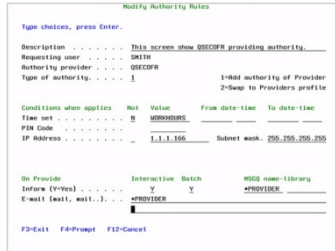
Assessment
Audit + Visualizer



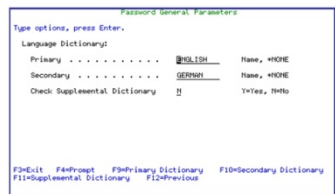
Prevenzione



Firewall - Sistema di Prevenzione di Intrusione globale che previene la possibilità di aggirare la sicurezza innata di OS/400, proteggendo tutti i 53 exit points. Supporta il sistema di allarme IDS (Intrusion Detection System).

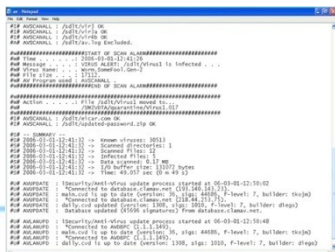


Authority on Demand - semplifica il processo per concedere in tempo reale profili speciali o fuori dal database degli utenti mediante meccanismi di divulgazione e supervisione facilmente utilizzabili.



Password - unisce tutte le capacità di gestione del password di OS/400 e contiene strumenti per bloccare l'uso di password facili da decifrare.

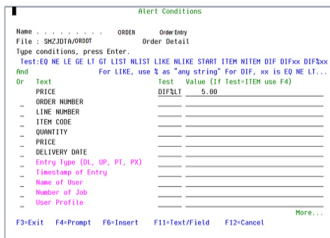
User Profile Manager - aiuta a gestire, monitorare e controllare tutte le definizioni collegate con il profilo dell'utente



Anti-Virus - scannerizza file e allegati a e-mail cercando virus per PC che possono essere dannosi e che possono influenzare PC collegati in rete di System i. Inoltre, nell'ambiente di green screen, segue l'uso non autorizzato e potenzialmente maligno di API standard di IBM.



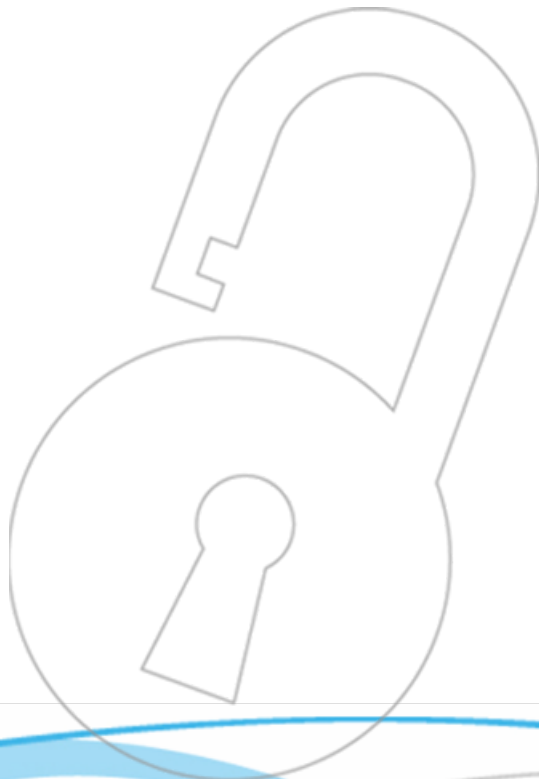
Controllo dei Dati



AP-Journal - fornisce risposte a query in batch e online come chi/cosa/quando/come/... relativamente a modifiche di data base applicativo, per soddisfare i requisiti regolatori e per ridurre le frodi.

iSecurity™ AP-Journal è un modulo che provvede a mantenere la sicurezza dei dati anche il supporto di "Business Analysis", visto che è in grado di documentare ed avvisare (anche in tempo reale) di tutti i cambiamenti, non pianificati, che i dati possono subire.

L'interfaccia dell'applicazione e le sue ulteriori funzionalità, rendono il modulo uno strumento fondamentale nella gestione ed il controllo degli eventi per ogni tipologia di applicazione utilizzata sul System i.



iSecurity L'Offerta Commerciale



IBM Italia Forum
Segrate 23 luglio 2009



Formule Commerciali

1. MTC Program:

E' il programma che consente l'acquisizione di un package studiata per offrire al Cliente la possibilità di un servizio interno di "Security Maintenance".

La formula commerciale MTC Program è attivabile sulla base di un corrispettivo economico così composto:

- 10% del valore del package;
- La quota relativa alla maintenance dei prodotti (20% sul prezzo di listino);

2. PFU Program:

E' il programma che consente al Cliente la valutazione di un package di moduli di iSecurity con la possibilità di poter confermarne l'acquisizione alla scadenza del 1mo anno e quindi di formalizzare l'acquisto nei 2 anni successivi.

Il PFU Program è attivabile sulla base di un corrispettivo economico così composto:

- 25% del valore dei prodotti che il cliente intende utilizzare;
- La quota relativa alla maintenance dei prodotti (20% sul prezzo di listino);

3. POC Program:

E' il programma che consente al Cliente la valutazione di tutti i moduli di iSecurity; alla fine del primo anno il cliente può di acquisire solo alcuni moduli (mediante le altre formule) o continuare con il POC Program, sempre su base triennale.

Il POC Program è attivabile sulla base di un corrispettivo economico così composto:

- Pagamento della sola quota relativa alla maintenance dei prodotti

4. PO Program:

E' il programma che consente al Cliente di poter acquistare qualunque modulo e/o package (proprietà della licenza d'uso), mediante un acquisto in un'unica soluzione alla quale Razlee, rilascia degli sconti finanziari sulla base della tempistica di acquisizione

..... Un "piccolo" presente!

*Voucher da allegare all'ordine del
System Administrator Package*

5284

8.9.2009

DATE

PAY TO THE
ORDER OF

Company

1 FREE iSecurity Anti Virus

DOLLARS



*Acquistando il System Administrator Package entro il 30 novembre,
il presente voucher dà il diritto alla Società di ricevere gratuitamente il modulo Anti Virus*

⑆ 22222222 ⑆ 123 111 555⑆ 5284

Per saperne di più.....

Per ulteriori informazioni visitate il sito
www.razlee.com

RAZ-LEE
The iSeries Security Experts

Products Compliance News Company Blog Customers Partners Downloads Search Contact Us

User-Friendly
Audit Trails
with
iSecurity
LEARN MORE >

Raz-Lee Security is the leading security solution provider for iSeries (Power i or AS/400) servers. iSecurity, Raz-Lee's unique iSeries security suite, helps companies protect valuable information assets against insider threat and unauthorized external access. It offers end-to-end security solutions, from network security to application security. Raz-Lee's solutions enable enterprises to comply with the requirements of PCI, Sarbanes-Oxley (SOX) and HIPAA. With iSecurity, professional security becomes easy.

Over 25 years of exclusive iSeries security focus and a strong IBM partnership have enabled Raz-Lee to achieve an outstanding level of expertise and development capacities. Raz-Lee's wide-ranging customer base includes large companies in all vertical markets, in over 30 countries worldwide.

Latest News
August 17, 2009
Raz-Lee Security and SEA to Jointly

Quick Links
Raz-Lee on Twitter
Our Blog
Compliance Evaluator
Subscribe to our Newsletter
Download a Product
Our IBM Partnership

System iNetwork
WEBCAST SPONSORED BY
iSecurity
How Can i PCI?

Copyright © 2009 Raz-Lee Security. All rights reserved. Terms & Conditions | Site Map

.....oppure richiedete il CD con i documenti dell'evento e altro, lasciando il feedback

- Presentazioni
- Documentazioni dei Prodotti
- Normative
- Listino
- Offerte

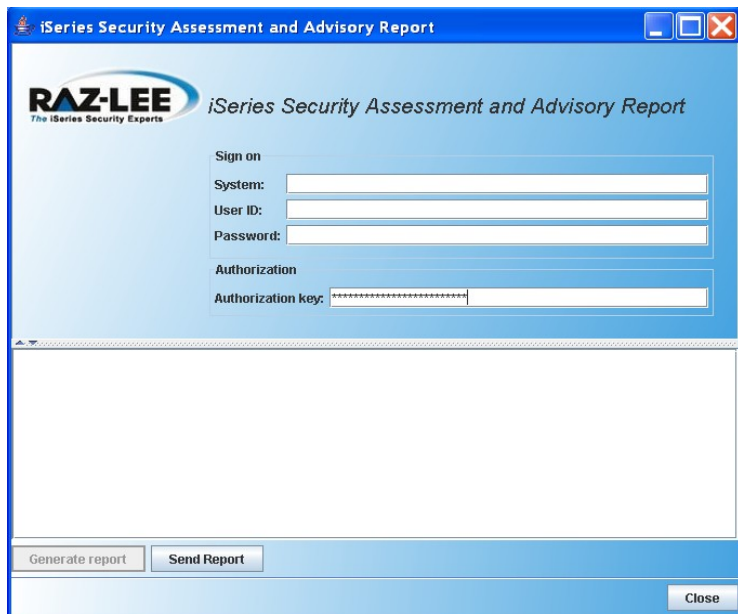
**Grazie per la
Vostra
Attenzione**

Nicola Fusco
nicola.fusco@razlee.com

m

Assessment Tool & Reporting


[back](#)



- Analisi completa del System i
- Individuazione delle aree di rischio
 - Classificazione di ogni valore di sistema di sicurezza
 - Generazione del Report con descrizione dei rischi

Il tool di Assessment è un potentissimo strumento di lavoro poichè presenta al cliente, in maniera comprensiva, l'attuale situazione della sicurezza del sistema informativo. L'approccio sarà pertanto assolutamente consulenziale.

Esempio di Report

Importance	Description	Parameter name	Value	Recommended value	Risk	Current Score
	Inactive job time out Specifies when the system takes action on inactive interactive jobs. The system value QINACTMSGQ determines the action the system takes. Local jobs that are currently signed-on to a remote system are excluded.	QINACTIV	0000000060	15	Unattended terminals are very large risks; they enable anyone to easily use existing programs to access and modify data. iSecurity's Screen module controls screen activity time based on location/user.	★☆☆☆☆
Information Only	Inactive message queue Inactive message queue	QINACTMSGQ	QSYSOPR QSYS	*DSCJOB	It is recommended not to leave jobs in inactive status.	Information Only
Information Only	Disconnect job interval Specifies the length of time in minutes an interactive job can be disconnected before it is ended. An interactive job can be disconnected with the DSCJOB command or when an I/O error occurs at the interactive job's work station (the system value QDEVRCYACN).	QDSCJOBIV	0000000240	240	An interactive job must not be left idle for any length of time.	Information Only

Score with iSecurity: ★★★★★

Score: ★☆☆☆☆

Explanation: Your settings are faulty. Avoid a possible security threat to your network by implementing iSecurity Screen.

Network Security – The Challenge

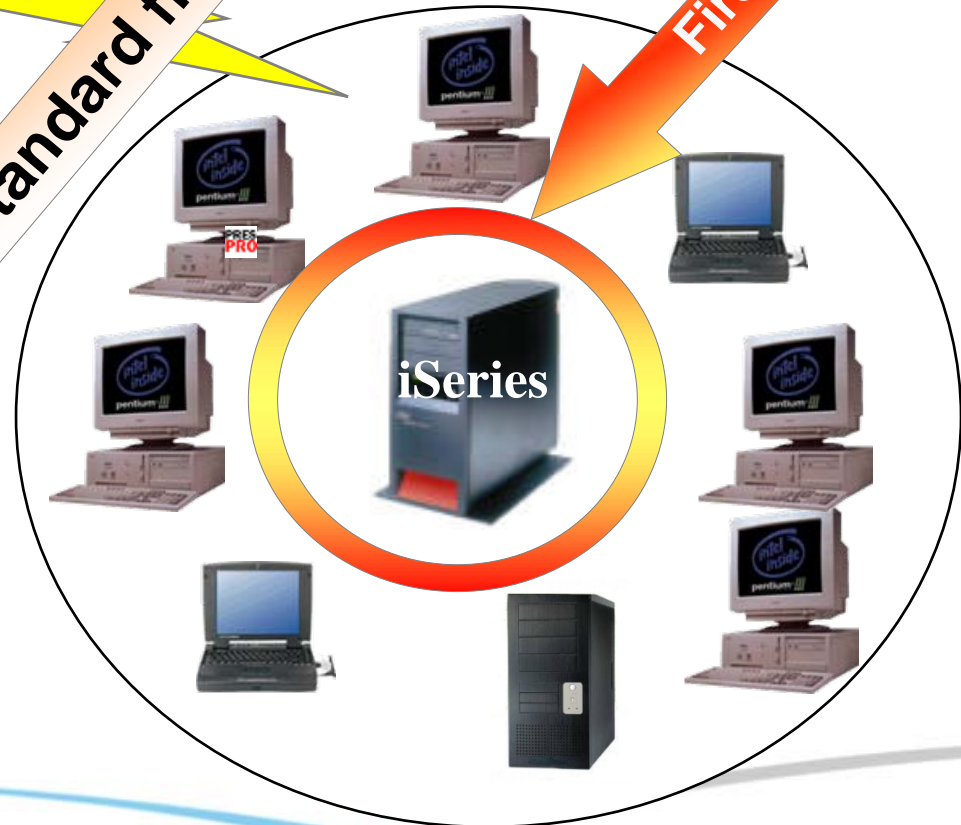
The Outside World

Standard firewall

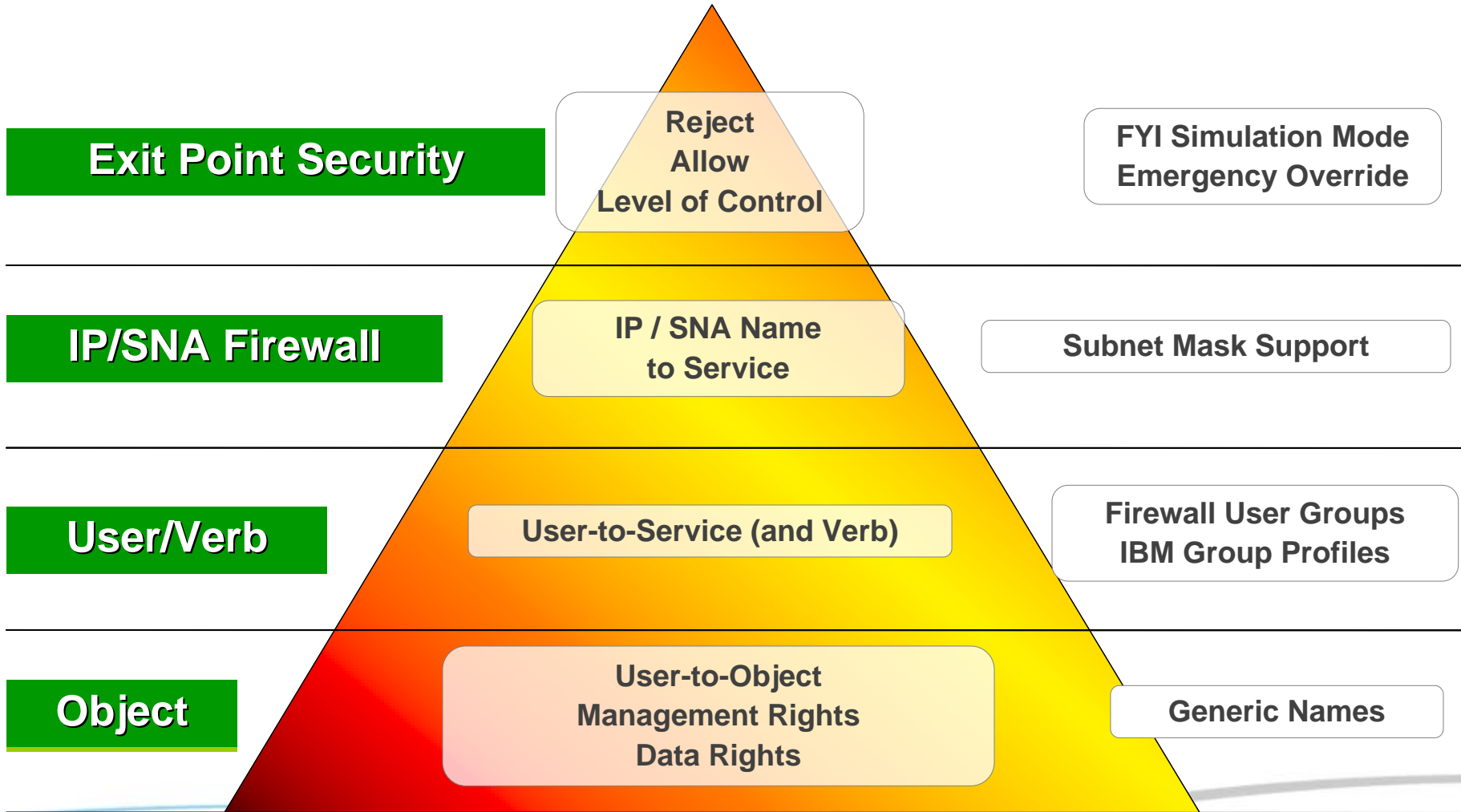
Firewall

iSecurity Firewall

- IP Address
- User
- Verb
- File
- Library
- Commands



Firewall - Top Down Security Design



Firewall - Top Down Security Design

Exit Point Control

Standard Firewall

User/Verb

Object

Remote Logon

- **FTP:** Authorities Based on IP & User
- **Telnet:** Terminal based on IP-Automatic Signon
- **Internet (WSG):** User to IP address
- **Passthrough:** User to System name (SNA)

Firewall - Java GUI

The screenshot shows the AS/400 Operations Navigator interface. The left pane displays a tree view with 'Firewall' selected. The main pane shows a list of objects for '1.1.1.100: Logon Control', including 'Telnet'. A context menu is open over the 'Telnet' object, showing options like 'Add TELNET Logon Security'.

Environment: My Connections

1.1.1.100: Logon Control

Name	Description
FTP/REXEC	FTP/REXEC
Telnet	Telnet
Internet (WSG)	
Passthrough	

Firewall 1.1.1.1

Work with TELNET Logon Security

IP Address	Subnet Mask
1.1.1.1	255.255.255.255
1.1.1.211	
1.2.3.4	
11.12.13.	
66.36.55.	255.
66.77.66.	

Add TELNET Logon Security

IP Address	
Subnet Mask	255.
Incoming Terminal Na...	
Minimum pwd Validation	No p
Logon	*AC
Assigned Terminal Na...	
Alt User	
Alt Current Library	

Security tasks
Configure the security of the server

1 - 4 of 4 objects

Firewall - Java GUI

[back](#)

The screenshot displays the '1.1.1.100 - Firewall Settings' application window. The 'Group Definitions' tab is active. A 'Work with Location Groups' dialog is open, showing a list of location groups: '%HEADQUART...', '%LA', and '%NY'. The '%LA' group is selected. A 'Modify Location Group Security' dialog is also open, showing the configuration for the '%LA' group. The 'Description' field contains 'Los-Angles branch'. The 'Activity Time' section has 'Time groups: LAREG' selected. The 'Authorities and Locations' section has 'IP Address' and 'Device Name' fields, each with an 'Open...' button. An 'IP Address' dialog is open in the foreground, showing a table of IP addresses and their authorization status.

IP Address	Subnet Mask	Authorization	Text
-ALL	0.0.0.0	Reject	
184.90.10.1	255.255.255.128	Allow	LA branch IPs

Sample View Application

Work with Customers

Type options, press Enter.

1=Modify 4=Remove

Opt	Cust	State	Name	Contact person	Zip	Credit
█	209	CA	kuki d Bar	kuki Cohen	95500	8000
—	447	CA	Damon Films	Lewis Saifer	91444	7000
—	594	CA	Krasti Adventures	Hershel Krastovski	89977	2000
—	791	CA	Pola Fish Products	Pola Yang	96670	5000
—	901	CA	Chi Exotic Spices	Chan Lee	90060	9000
—	999	CA	Skud Traveling	Abdul Ziad	99000	3000
—	129	NY	ARISTO TOYS	Mr DODO RICHIE	81406	7000
—	433	NY	Simpson & Son Tools	Marti Twain	45699	1000
—	563	NY	Ali Pharmaceuticals	Felix Araagon	99977	5000
—	589	NY	Infotelligence	Homer Flanders	80090	6000
—	644	NY	Mr. White Cinema	Ali Jackson	89900	7000
—	678	NY	Gore Industries	Bill Gore	90080	4000

More...

F3=Exit

F6=Add New

F12=Cancel

Sample View Application

Work with Customers

[Back](#)

Type options, press Enter.

1=Modify 4=Remove

Opt	Cust	State	Name	Contact person	Zip	Credit
█	209	CA	kuki d Bar	*****	95500	0
—	447	CA	Damon Films	*****	91444	0
—	594	CA	Krasti Adventures	*****	89977	0
—	791	CA	Pola Fish Products	*****	96670	0
—	901	CA	Chi Exotic Spices	*****	90060	0
—	999	CA	Skud Traveling	*****	99000	0
—	129	NY	ARISTO TOYS	*****	81406	0
—	433	NY	Simpson & Son Tools	*****	45699	0
—	563	NY	Ali Pharmaceuticals	*****	99977	0
—	589	NY	Infotelligence	*****	80090	0
—	644	NY	Mr. White Cinema	*****	89900	0
—	678	NY	Gore Industries	*****	90080	0

more...

F3=Exit

F6=Add New

F12=Cancel

Sensitive data in the “Contact person” and “Credit” fields are hidden...