PI and Security

Sharing the joy without exposing yourself

Ken Marsh
Service Manager, OSI Software Asia

Not Presented: Standard Policies/Practices

- password complexity / expiration
- physical security
- backup / restore
- intrusion detection
- auditing
- auto logout
- virus scanning

What is Presented?

Security considerations in deploying a PI-based Enterprise Architecture

Agenda

- Authentication
- Encryption
- Firewalls 101
- Attacks Prevented
- Common PI Scenarios
- Security Features of PI

Native PI Authentication

PI Username and Password

Pros:

- Domain not required

Cons:

- Login once for Windows, again for PI*
- No restriction on weak/blank passwords
- Not sufficiently encrypted

Encryption

Encryption uses a “key” and a math algorythm to change this:

> “**No Ferrari materials or data are or have ever been in the possession of any McLaren employee.**”

Into this:

> “**77ce615ca2ee098844f8566d9343db96d41d8cd98f00b204e9800998ecf8427e**”

Only with the “key” can it be changed back.

Windows Authentication

Trust Windows Domain (Kerberos)

Pros:

- Strong and Secure Cryptography
- Cross-Platform Industry Standard
- Single Sign-On
- Can secure with smart cards

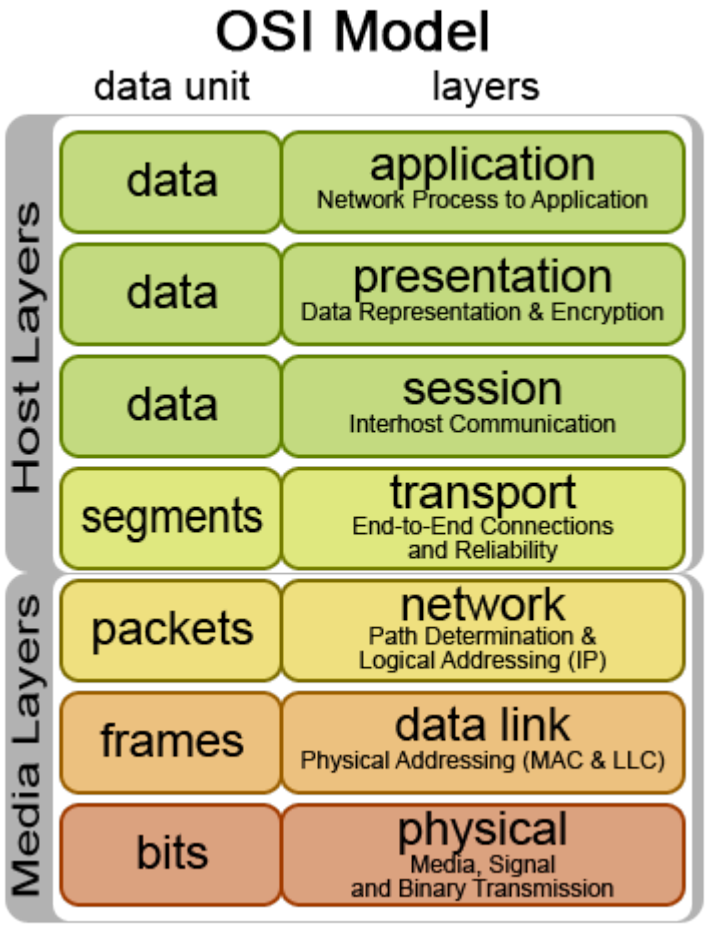
Kerberos

Cons?

- Machines and Users must be Domain members, including the PI Server
- Only as strong as the password

Smart Card Inventor, Helmut Gröttrup

Protecting Network Traffic



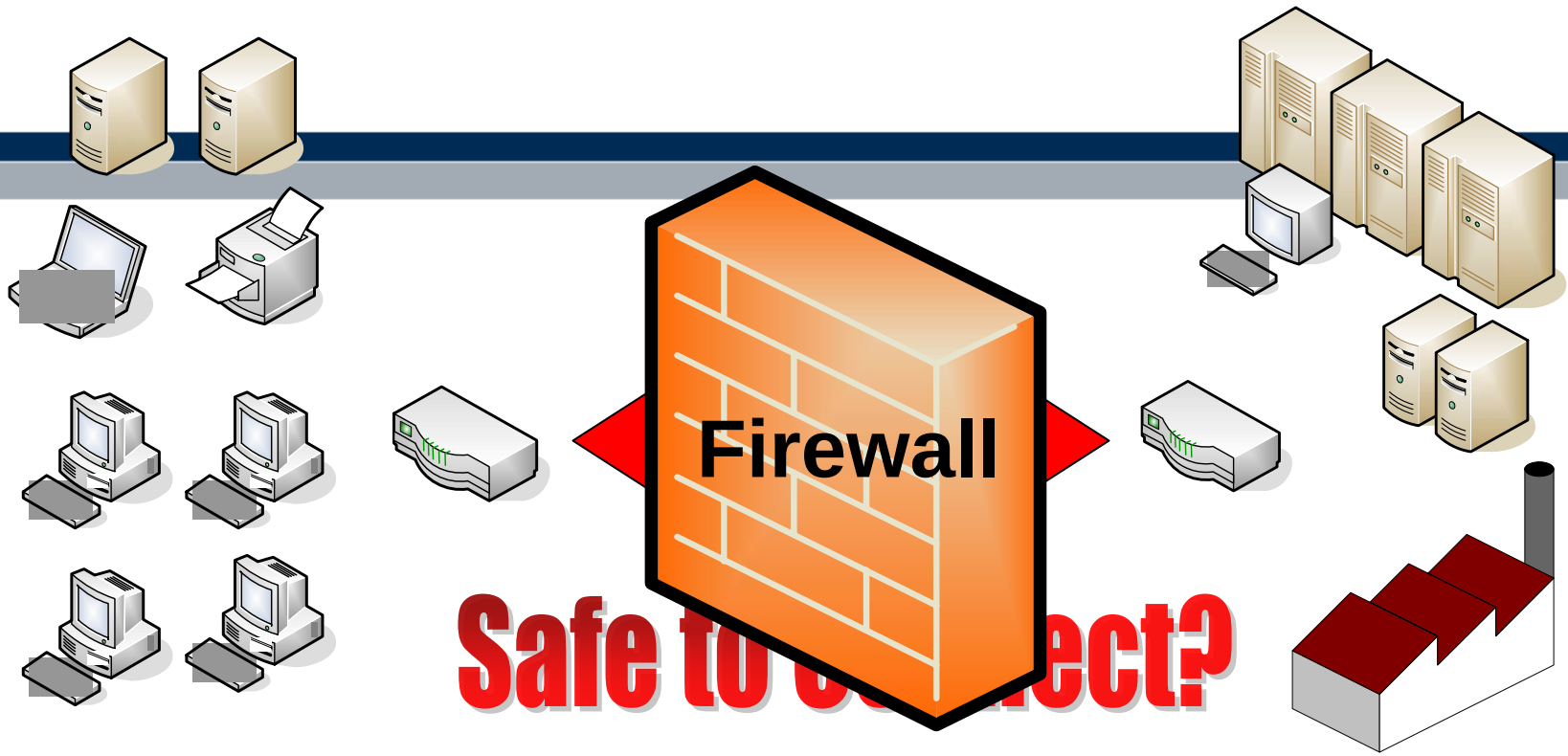
PINet Encryption?

HTTPS – Encrypted Web

VPN Tunnel / IPsec Transport

ATM Frame Relay

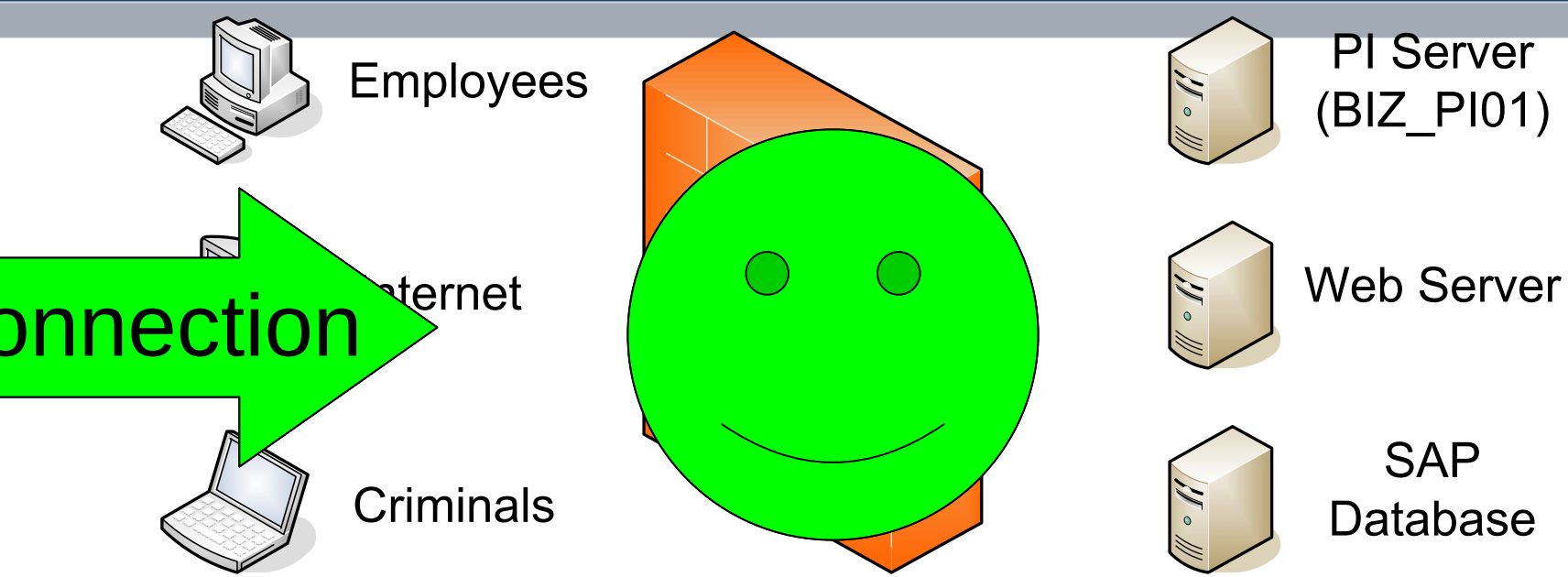
Dedicated Physical Cable



Business Network

Process Control Network

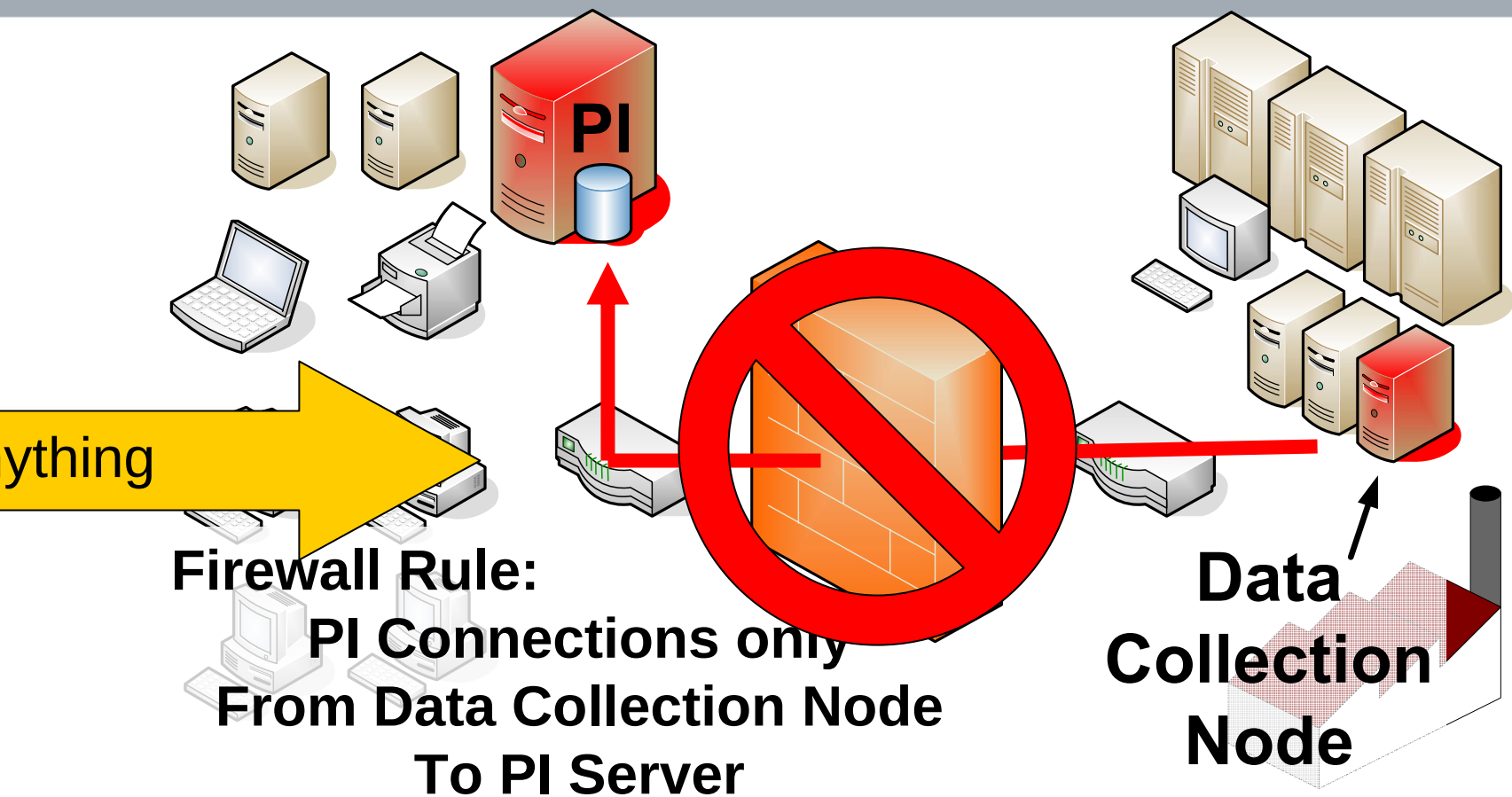
What is a Firewall?



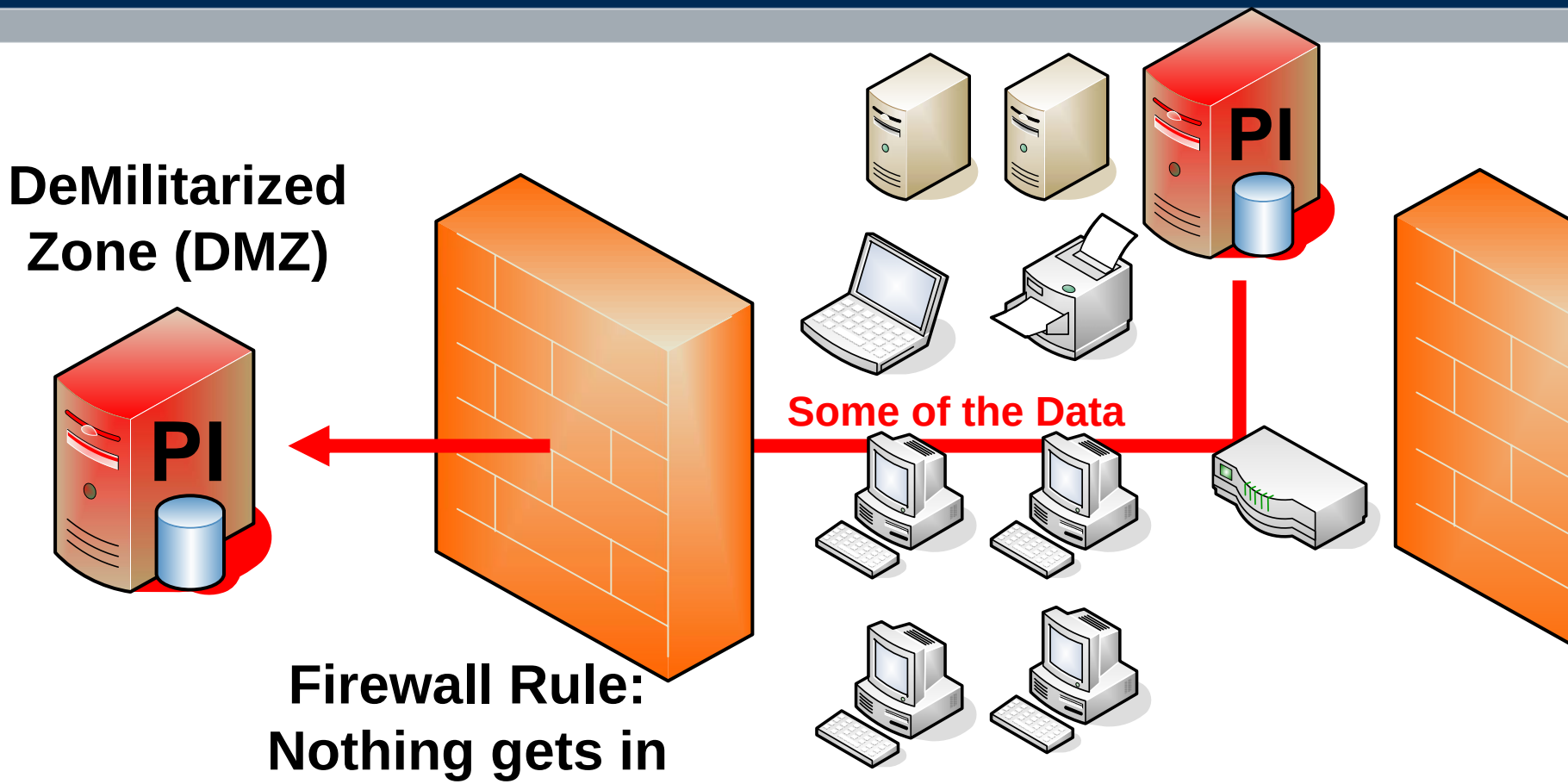
Rules:
Allow only PI Connections
Deny everything else

Some Common
PI System Security Scenarios

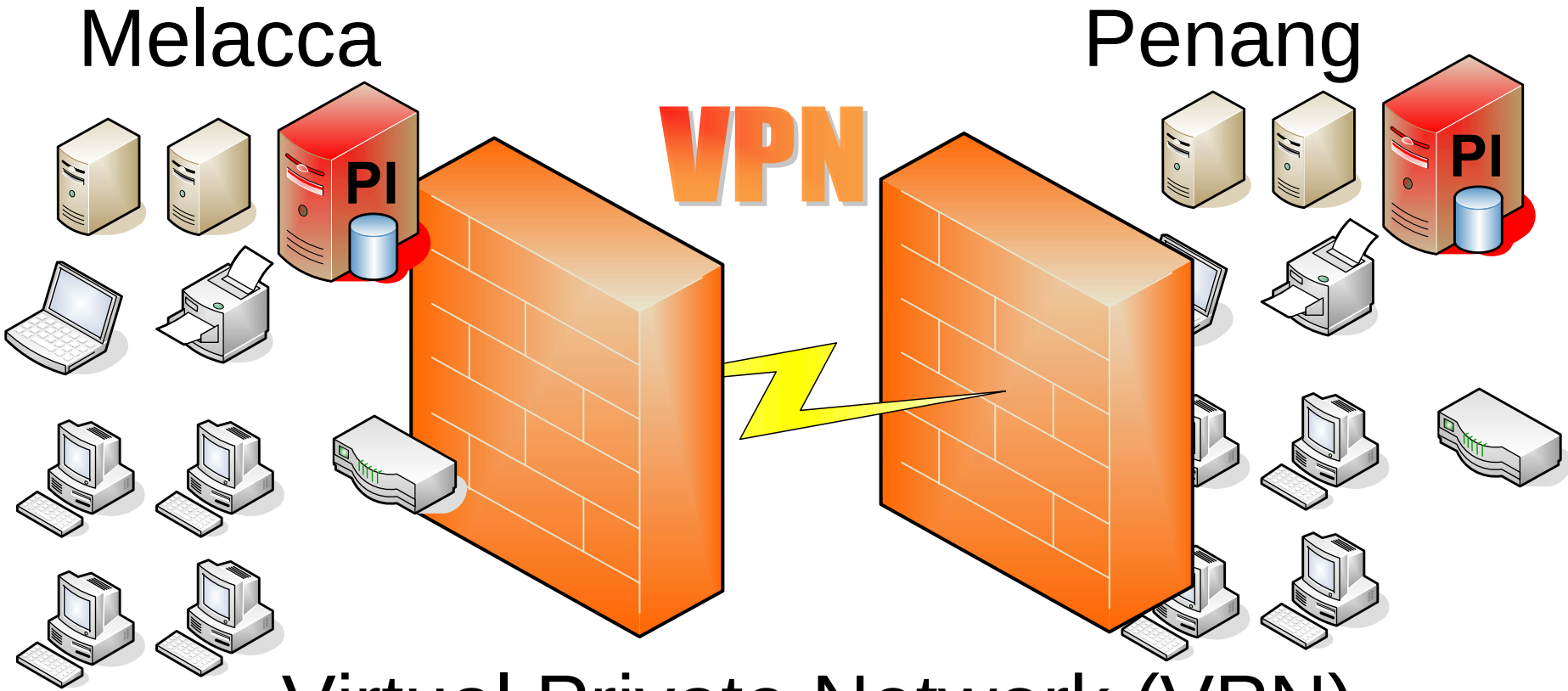
Data Collection on Control Network with PI on Business Network



Replicating data to PI server in DMZ with PI-to-PI



Disaster Recovery Location

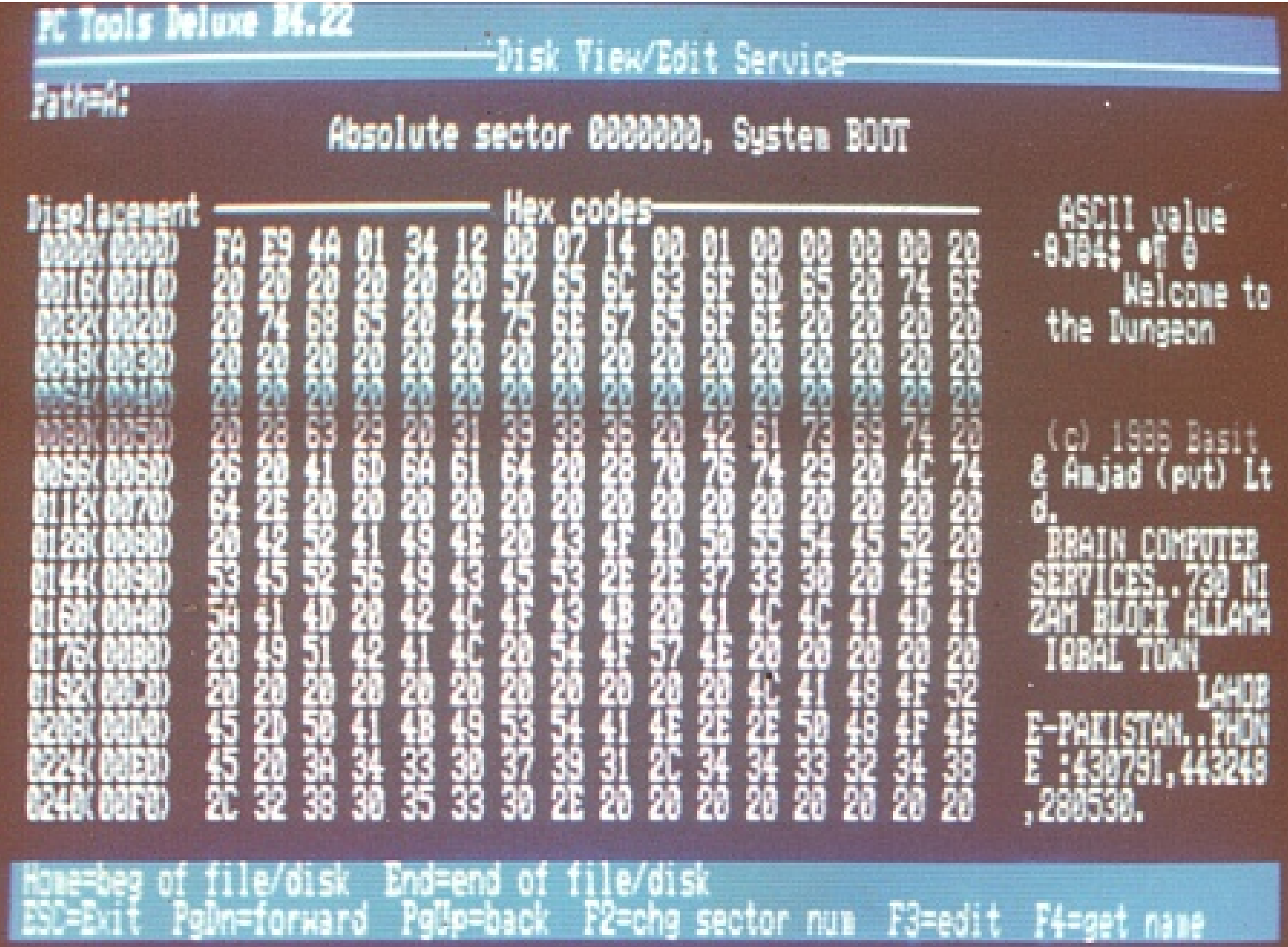


Virtual Private Network (VPN)

Attacks – Virus and Worm

Common sources:

- USB drive, floppy disk
- Downloaded from web (Trojan Horses)
- IRC, email, file sharing
- Network


PC Tools Deluxe 04.22
Disk View/Edit Service
Path=A:
Absolute sector 0000000, System BOOT
Displacement
Hex codes
ASCII value
0000(0000) FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20
0016(0010) 20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F
0032(0020) 20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20
0048(0030) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050) 20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20
0096(0060) 26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74
0112(0070) 64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0128(0080) 20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20
0144(0090) 53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49
0160(00A0) 5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41
0176(00B0) 20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20
0192(00C0) 20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52
0208(00D0) 45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E
0224(00E0) 45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38
0240(00F0) 2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES..730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN..PHONE :430791,443249,280530.
Home=beg of file/disk End=end of file/disk
ESC=Exit PgDn=forward PgUp=back F2=chg sector num F3=edit F4=get name

Network Virus Attacks

- **Nimda** 80/tcp (web servers), by email, shared drives
- **SQL Slammer** 1434/udp (resolution service of Microsoft SQL)
- **Sobig** 25/tcp (email)
- **Blaster** 135/tcp (DCOM buffer overrun, MS-RPC used by exchange and Active Directory)
- **MyDoom** 25/tcp (email)
- **PI-in-your-face Virus?** 5450/tcp (not yet!)

Stopping Attacks

Reasons for Attack
- spying
- data manipulation
- sabotage

Attacks from outside
- firewall
- authentication

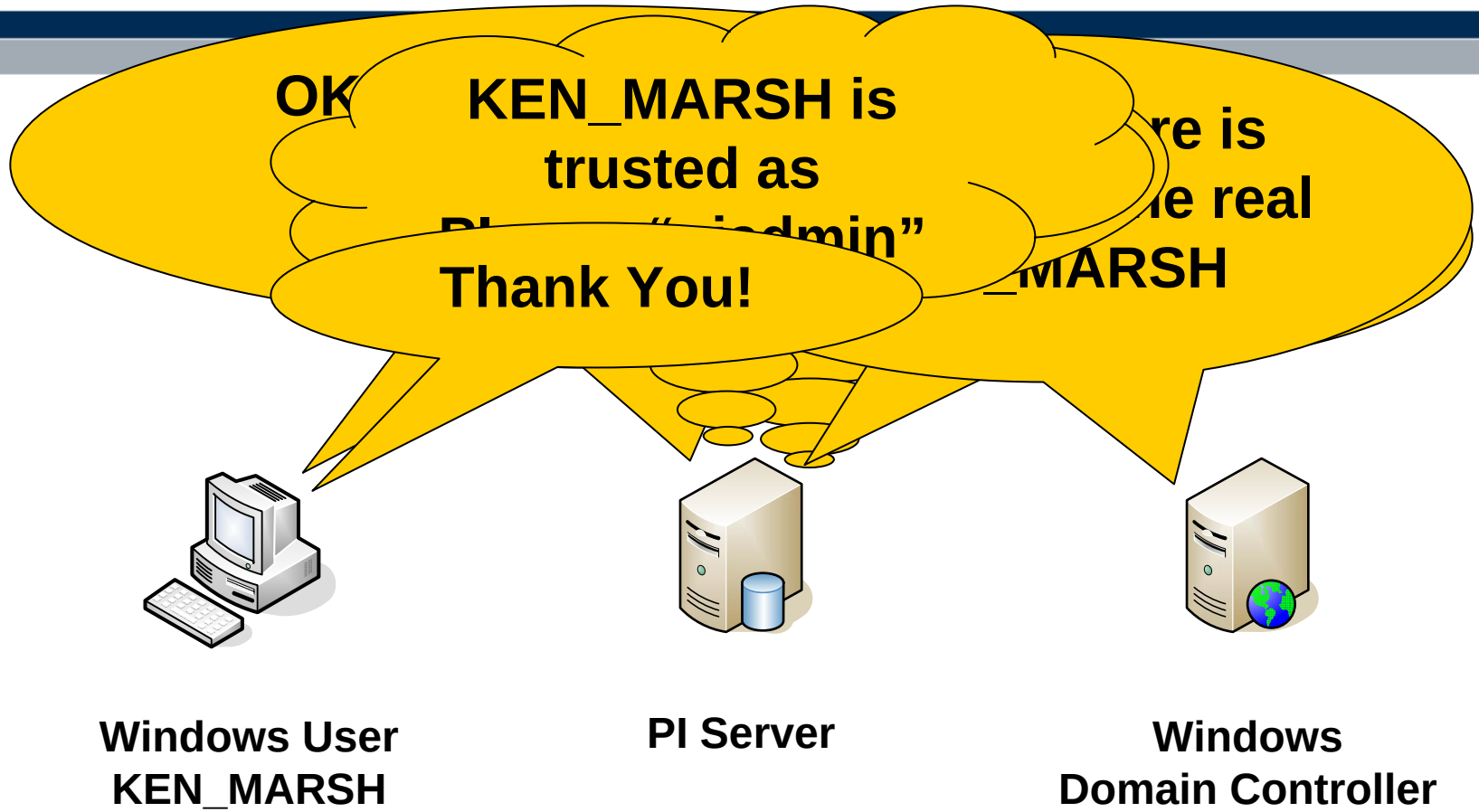
Attacks from inside
- encryption
- authorization
- physical protection

Unstoppable Attacks
- disaster recovery plan

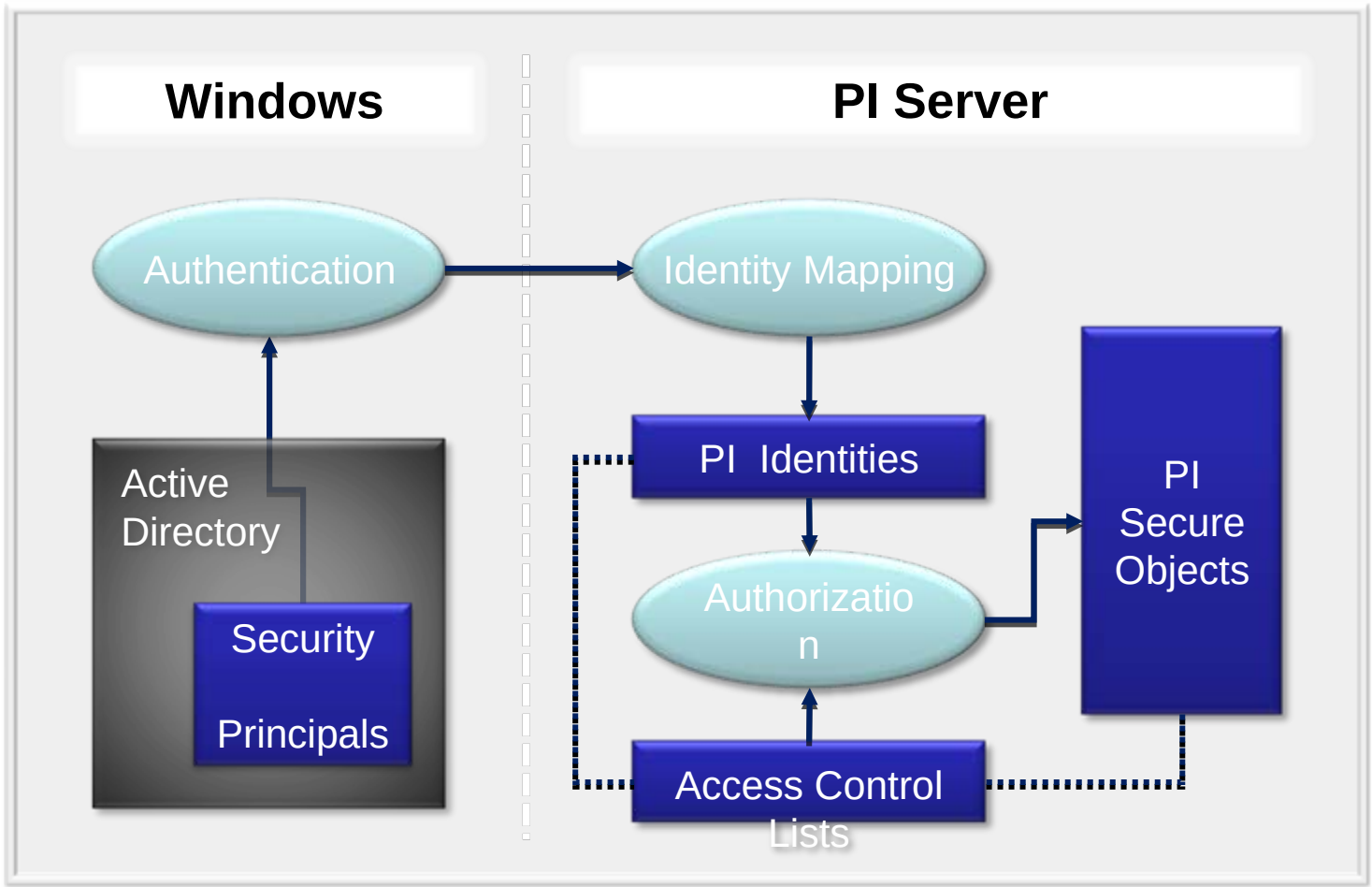
PI Security Features

- PI security features
- TCP Port 5450 - Compatible with firewalls, authentication encryption mentioned so far.
- PI Trust - give PI account based on Windows domain/username and soon Windows Groups
- Database Security
- Points Security
- AF Elements Security

PI Trusts


OK
KEN_MARSH is trusted as
Thank You!
re is
e real
_MARSH
Windows User KEN_MARSH
PI Server
Windows Domain Controller

WIS: Simplified Diagram



Conclusion

- PI Authentication based on Active Directory provides the best security
- PInet is an ordinary TCP/IP protocol that can be properly secured using industry standard methods – Firewalls, IPsec, etc.
- PI Security features let you secure PI objects individually if desired

Thank You!