Windows Integrated Security what it is, why you should use it

Presented by

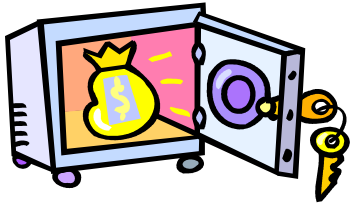
Martin Bryant

OSIsoft Field Service Engineer

Martin Bryant is a field service engineer and trainer based in OSIsoft's Houston office. Martin has twenty years of PI System experience and has been a Field Service Engineer for OSIsoft since 2003.

Welcome to

Security at a glance…

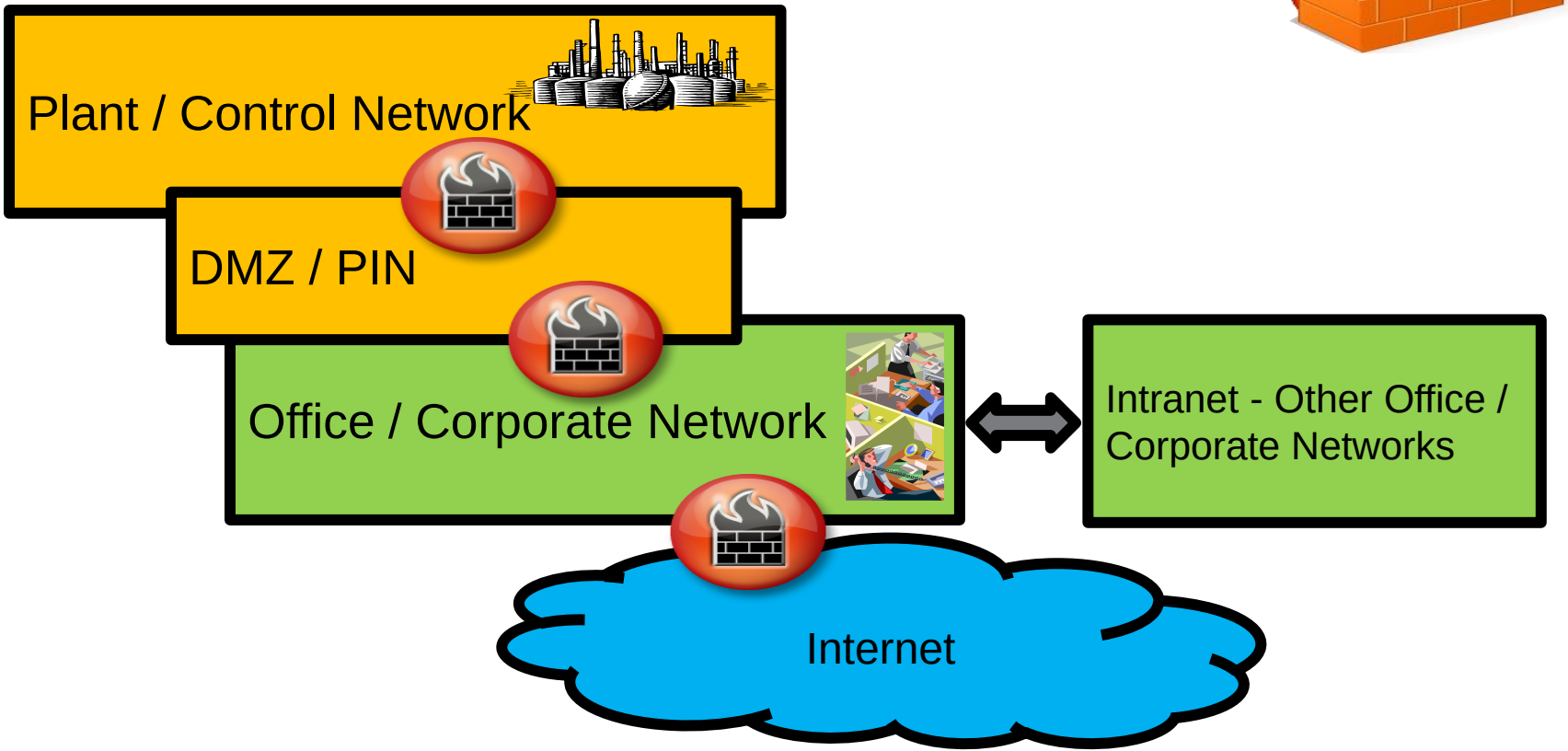


- **Connectivity – firewalls - what computers can connect to what computers (with what protocols, etc..)**
- **Identity – authentication - making sure you are who you say you are**
- **Access – ACL / security rules - who can do what, who can access what**

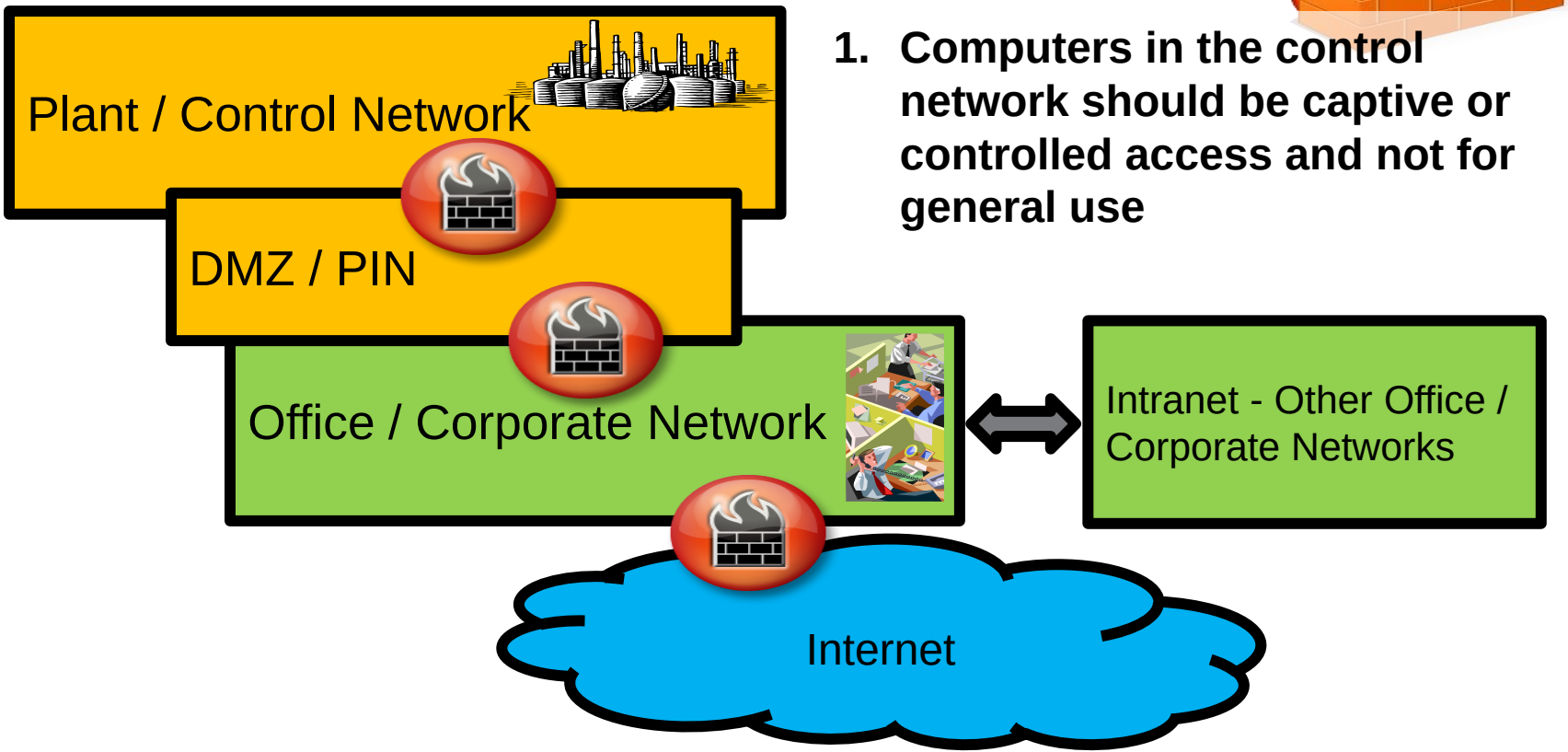
Firewalls..

- Today they are largely software - creating logical networks (VLANS)
- Permit/deny connectivity between nodes by IP subnet, port, protocol, MAC address & more
- Record connectivity events
- Changes are necessarily bureaucratic, require approvals, and record-keeping

Connectivity / Firewall Security Overview

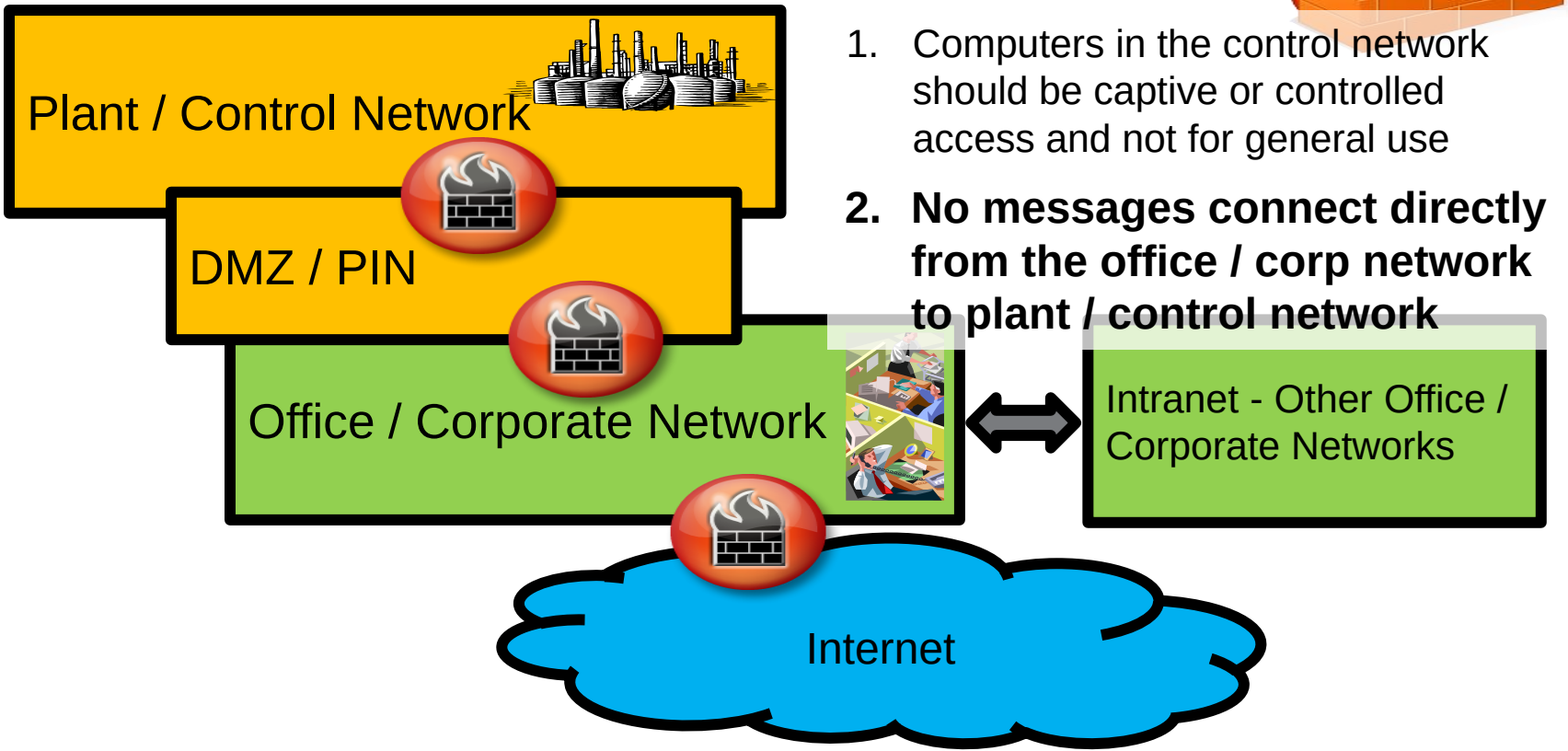


Connectivity / Firewall Security Overview



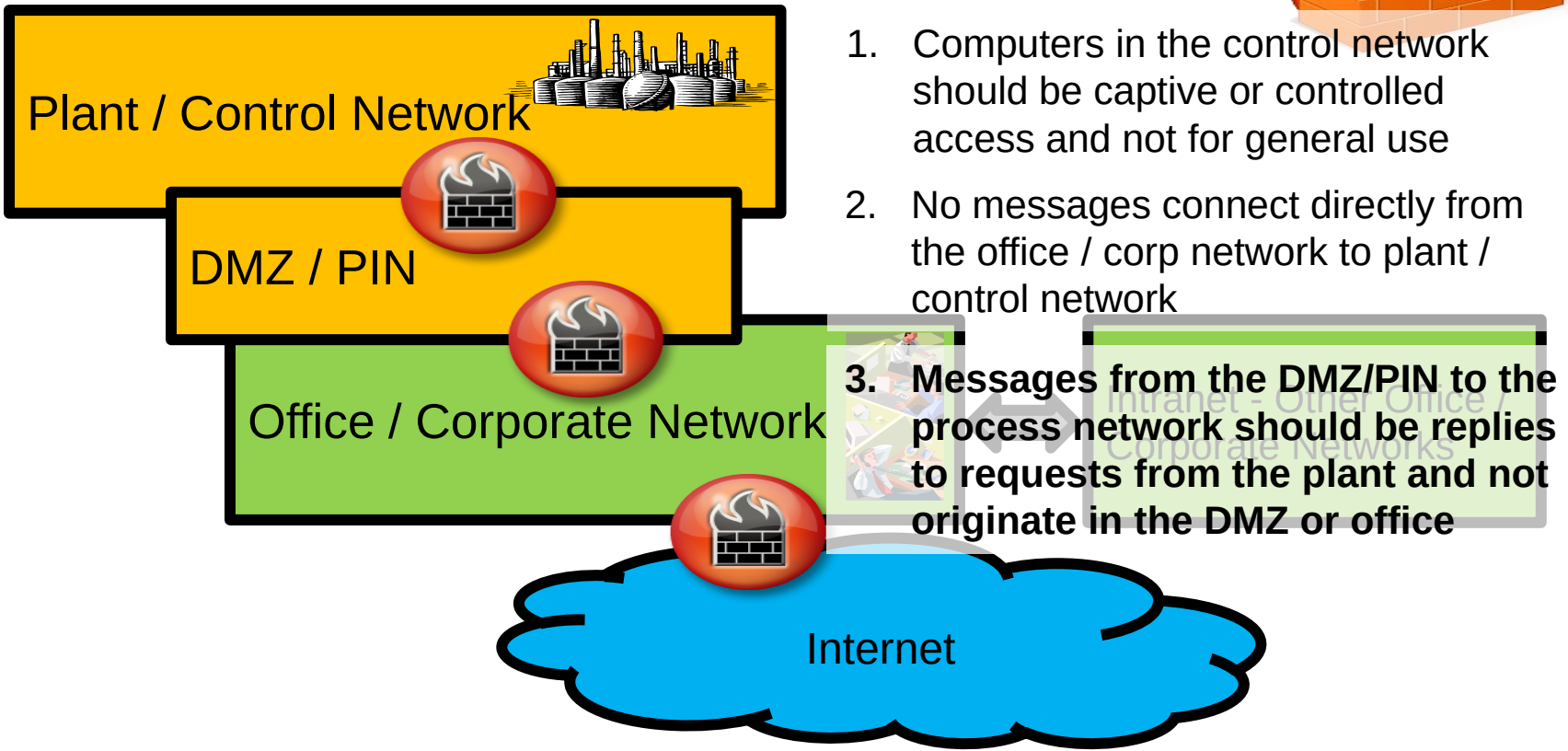
1. **Computers in the control network should be captive or controlled access and not for general use**

Connectivity / Firewall Security Overview



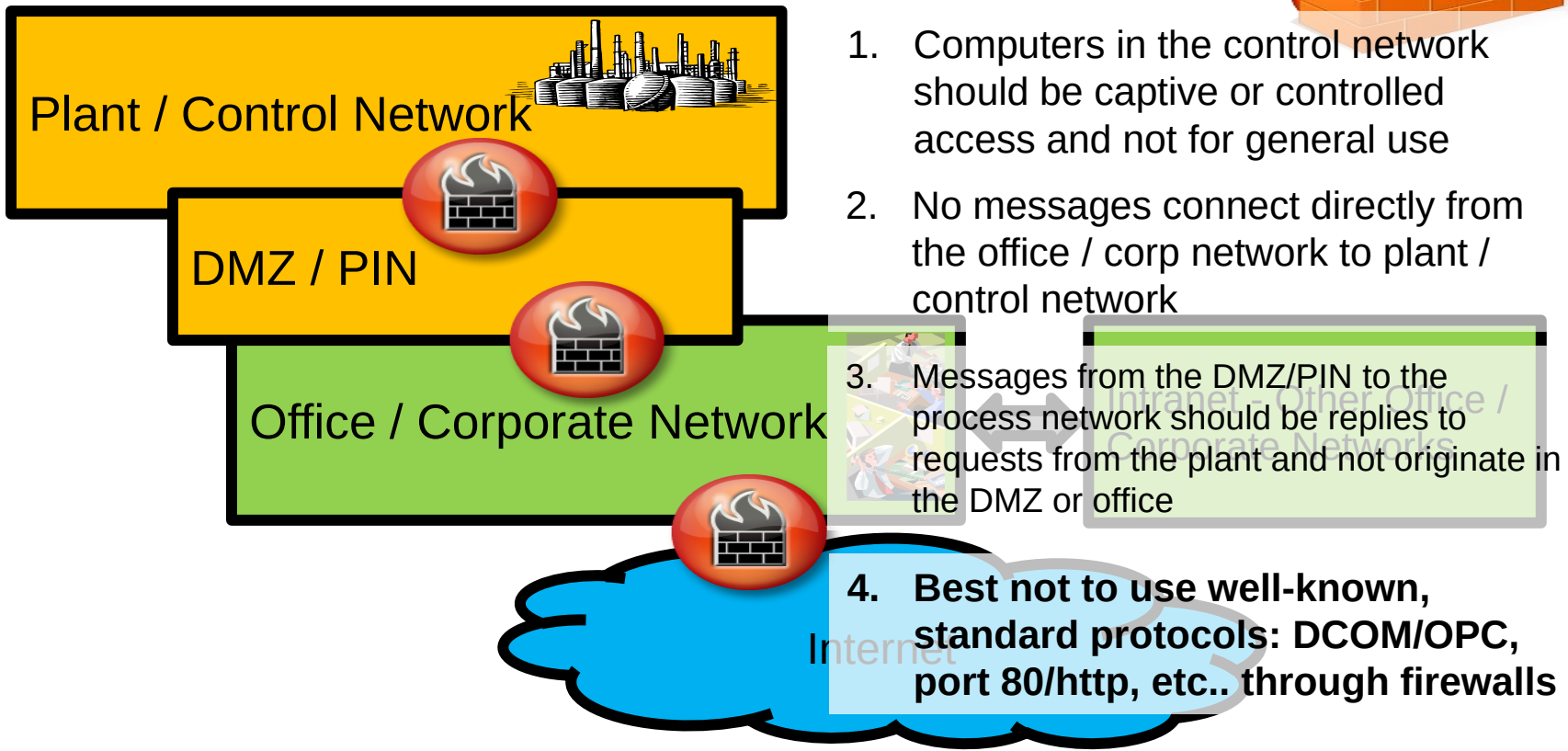
1. Computers in the control network should be captive or controlled access and not for general use
2. **No messages connect directly from the office / corp network to plant / control network**

Connectivity / Firewall Security Overview



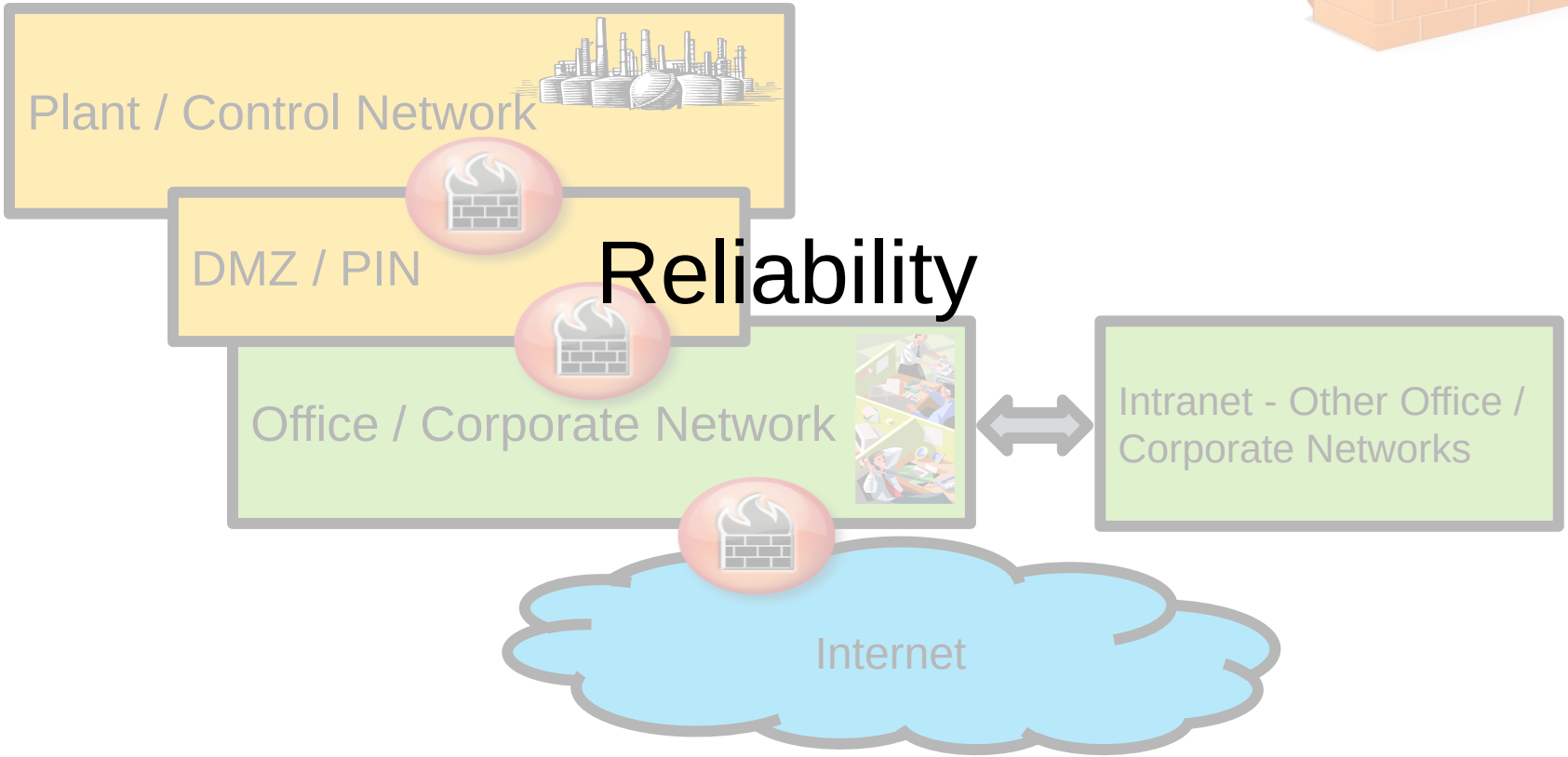
1. Computers in the control network should be captive or controlled access and not for general use
2. No messages connect directly from the office / corp network to plant / control network
3. **Messages from the DMZ/PIN to the process network should be replies to requests from the plant and not originate in the DMZ or office**

Connectivity / Firewall Security Overview

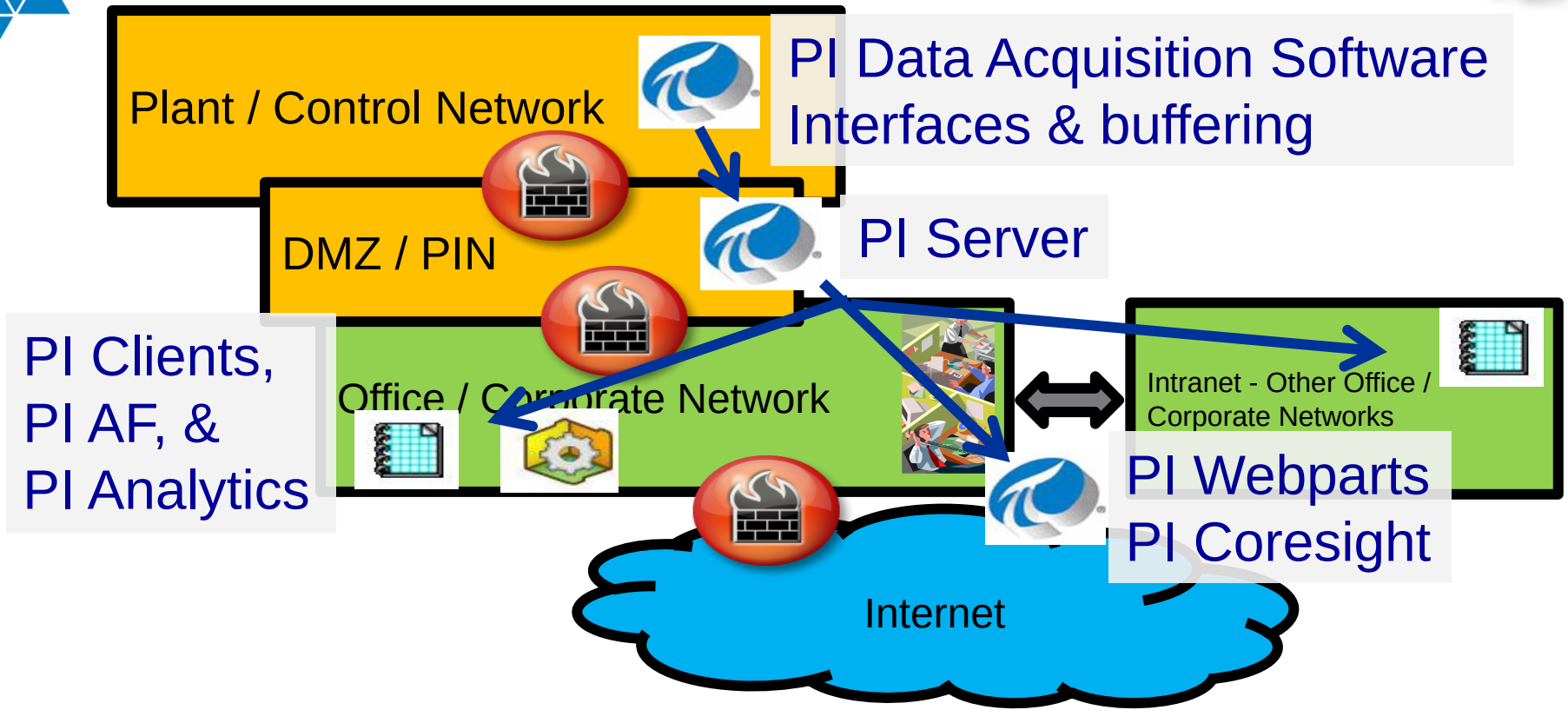


1. Computers in the control network should be captive or controlled access and not for general use
2. No messages connect directly from the office / corp network to plant / control network
3. Messages from the DMZ/PIN to the process network should be replies to requests from the plant and not originate in the DMZ or office
4. **Best not to use well-known, standard protocols: DCOM/OPC, port 80/http, etc.. through firewalls**

Connectivity / Firewall Security Overview



OSIsoft's PI System plays an important role…



OSIsoft's PI System plays an important role…

Move your people to the domain / corporate network and retain your commitment to continuous process improvement

Recommended PI System architectures have either a PI Server or PI-to-PI interface node (with a plant PI System) in the DMZ / PIN so there are no direct messages from the process to the corporate network or visa versa

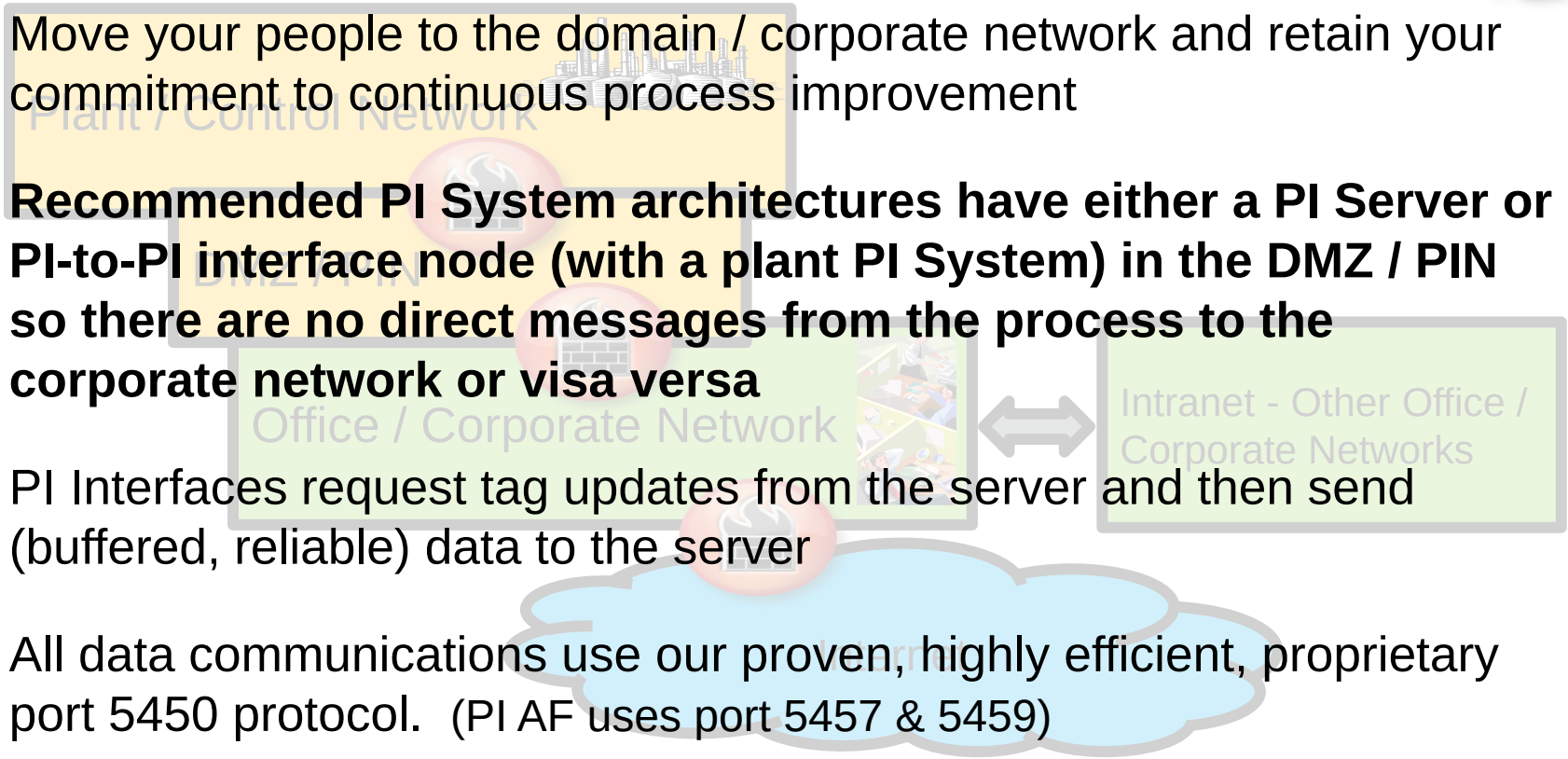
PI Interfaces request tag updates from the server and then send (buffered, reliable) data to the server

All data communications use our proven, highly efficient, proprietary port 5450 protocol. (PI AF uses port 5457 & 5459)

OSIsoft's PI System plays an important role…

Move your people to the domain / corporate network and retain your commitment to continuous process improvement

Recommended PI System architectures have either a PI Server or PI-to-PI interface node (with a plant PI System) in the DMZ / PIN so there are no direct messages from the process to the corporate network or visa versa



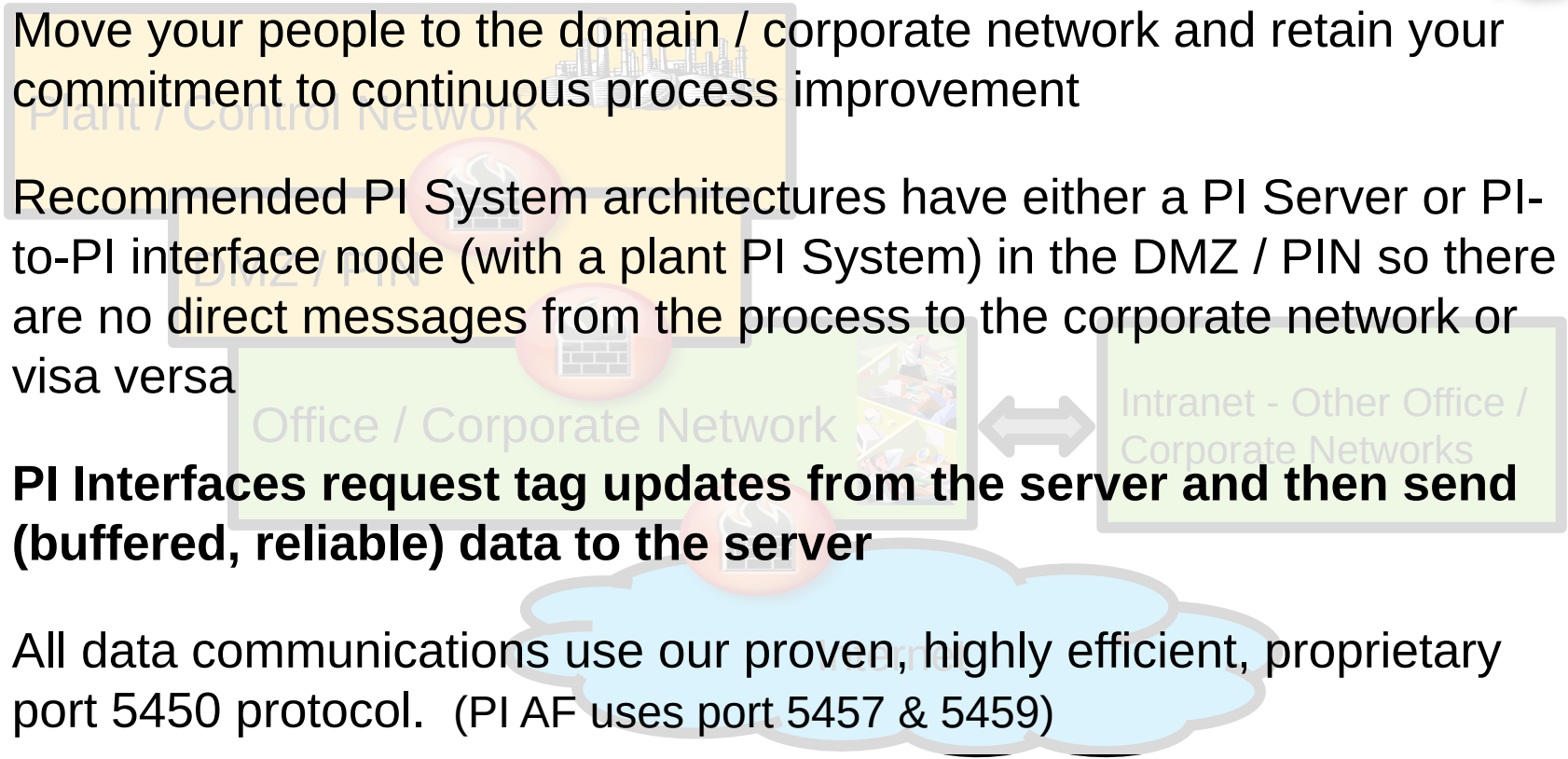
PI Interfaces request tag updates from the server and then send (buffered, reliable) data to the server

All data communications use our proven, highly efficient, proprietary port 5450 protocol. (PI AF uses port 5457 & 5459)

OSIsoft's PI System plays an important role…

Move your people to the domain / corporate network and retain your commitment to continuous process improvement

Recommended PI System architectures have either a PI Server or PI-to-PI interface node (with a plant PI System) in the DMZ / PIN so there are no direct messages from the process to the corporate network or visa versa



PI Interfaces request tag updates from the server and then send (buffered, reliable) data to the server

All data communications use our proven, highly efficient, proprietary port 5450 protocol. (PI AF uses port 5457 & 5459)

OSIsoft's PI System plays an important role…

Move your people to the domain / corporate network and retain your commitment to continuous process improvement

Recommended PI System architectures have either a PI Server or PI-to-PI interface node (with a plant PI System) in the DMZ / PIN so there are no direct messages from the process to the corporate network or visa versa

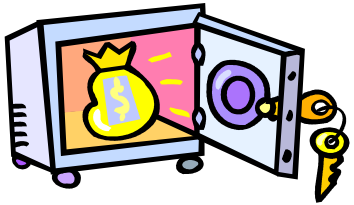
PI Interfaces request tag updates from the server and then send (buffered, reliable) data to the server

All data communications use our proven, highly efficient, proprietary port 5450 protocol. (PI AF uses port 5457 & 5459)

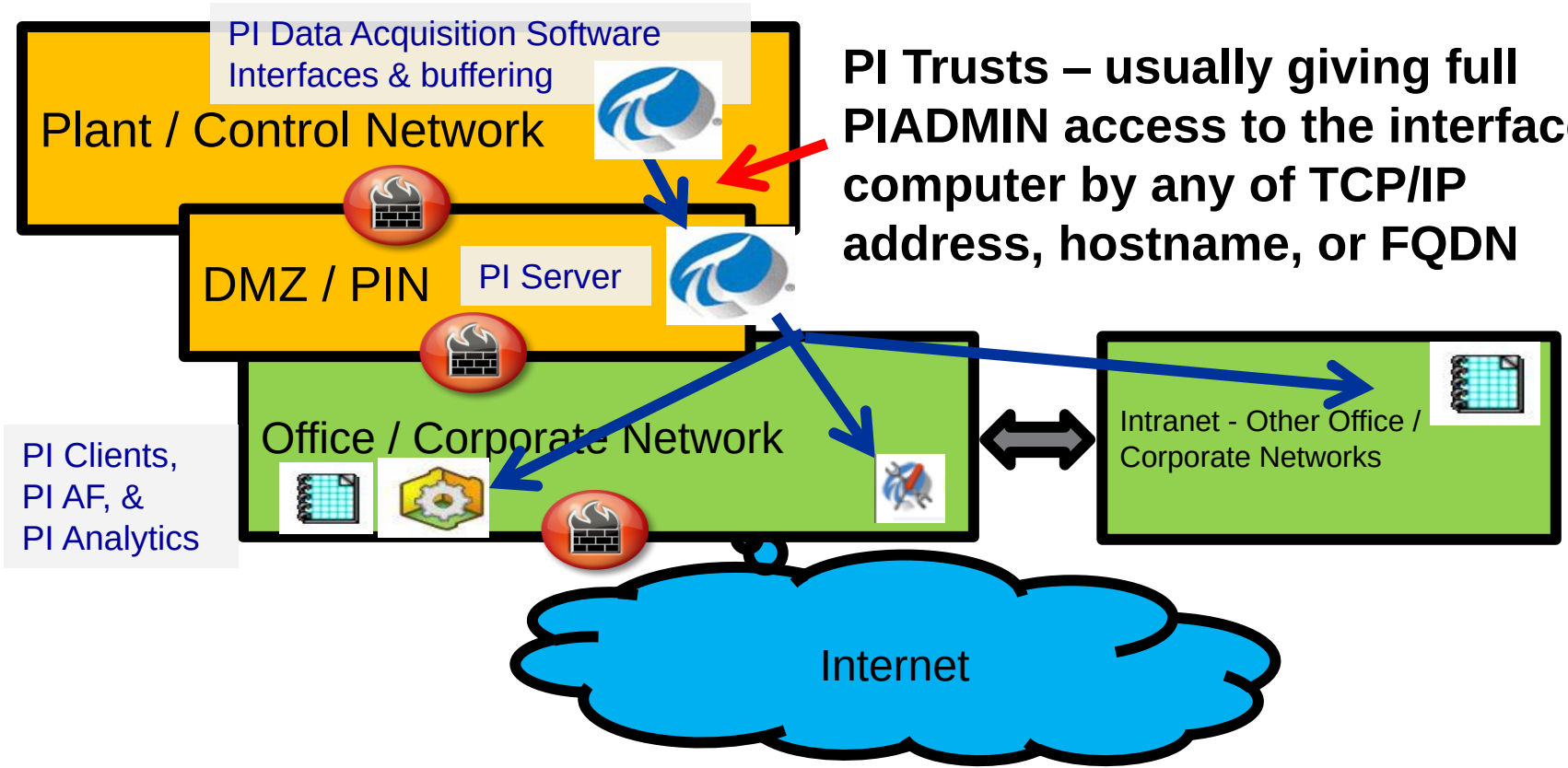
But even if you have done all of this…

The biggest problem with the security in most PI Systems today are that firewall / connectivity security is the only good part of the security, the rest of it is

not-so-good

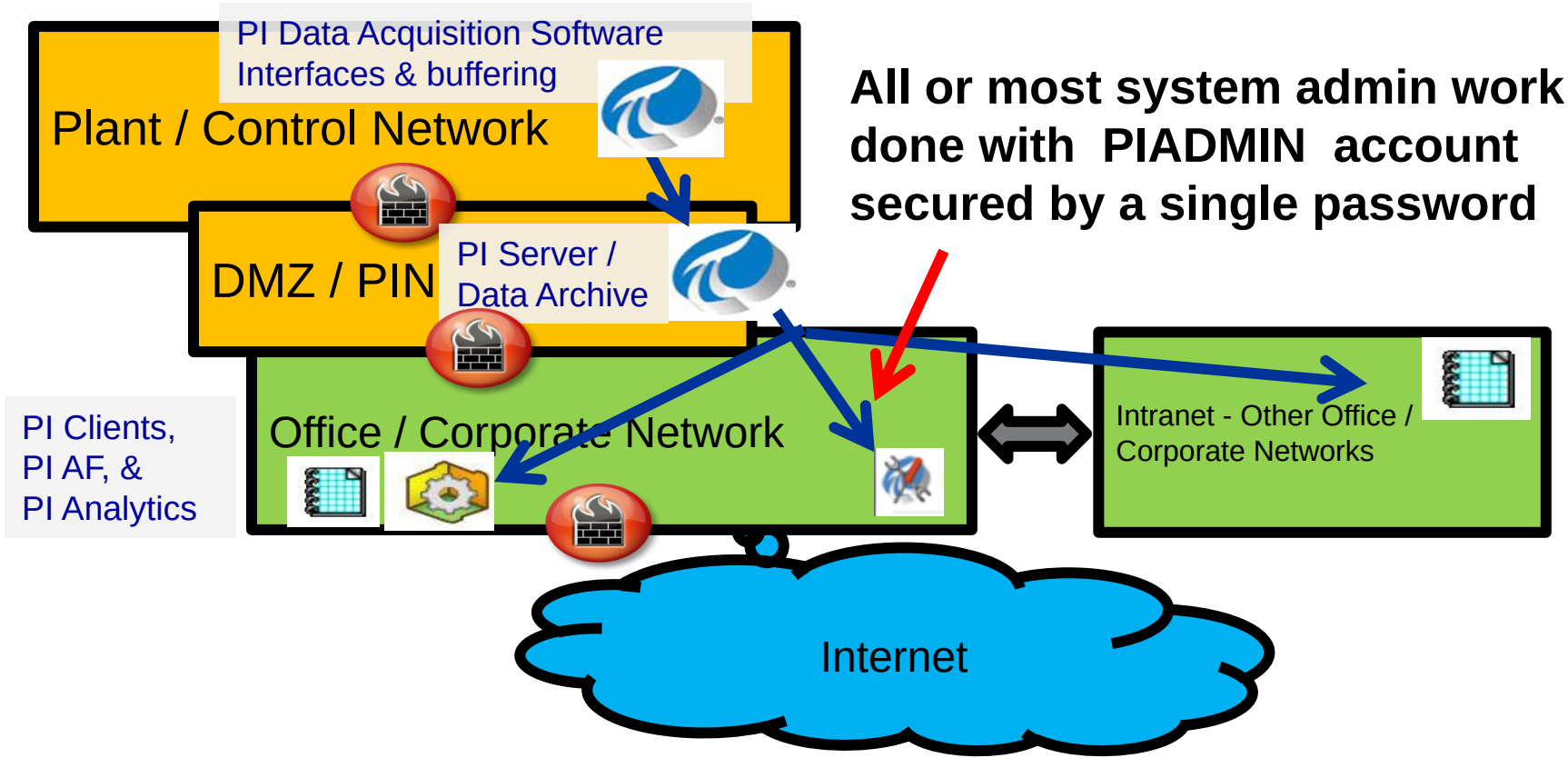


Typical “Old School” PI System Security



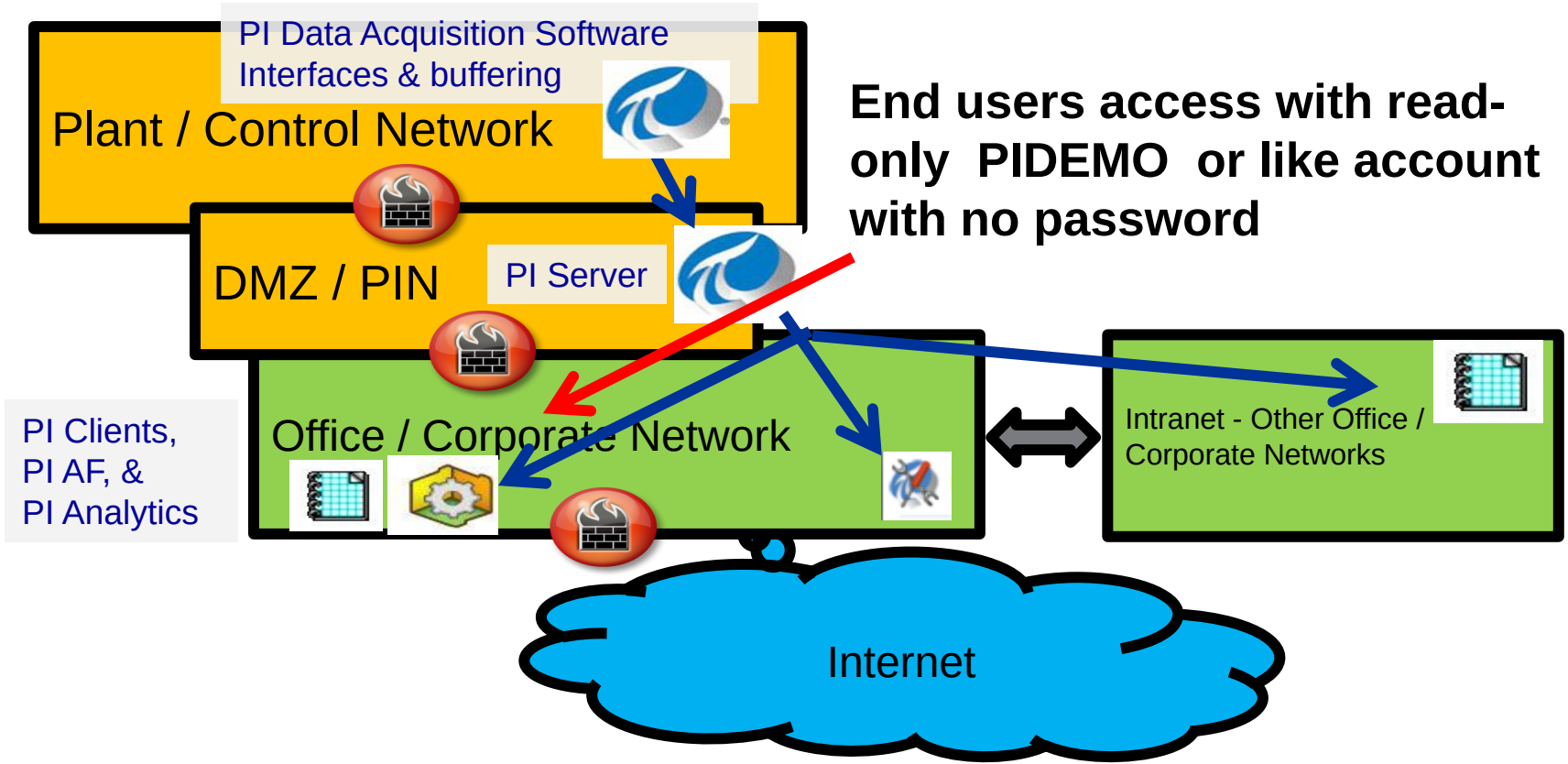
PI Trusts – usually giving full PIADMIN access to the interface computer by any of TCP/IP address, hostname, or FQDN

Typical “Old School” PI System Security



All or most system admin work done with PIADMIN account secured by a single password

Typical “Old School” PI System Security



End users access with read-only PIDEMO or like account with no password

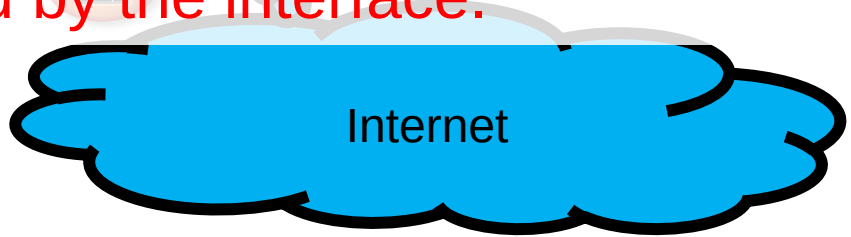
Typical “Old School” PI System Security

So, what’s so wrong with this?

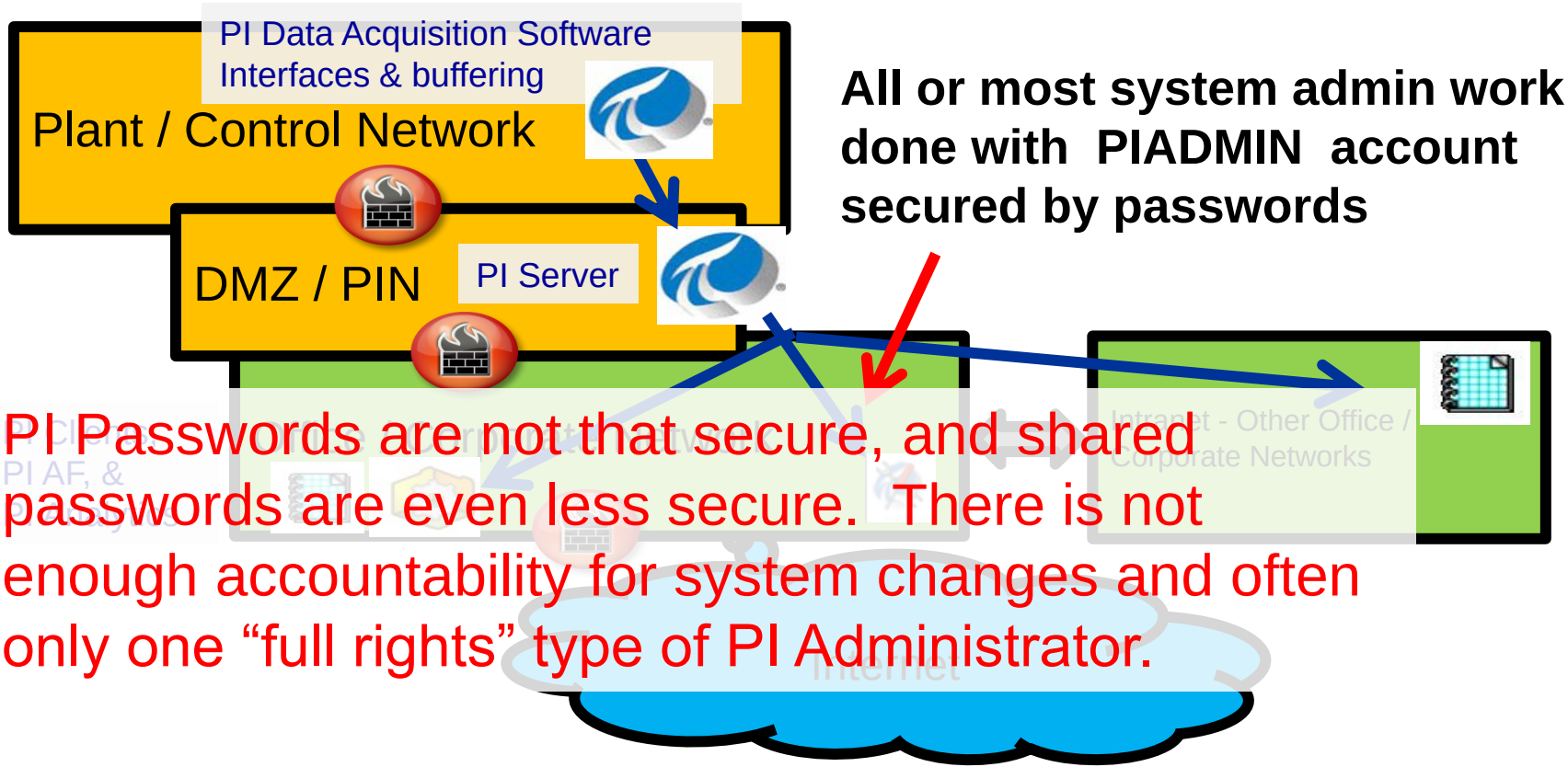
Typical “Old School” PI System Security

PI Trusts – often giving full PIAdmin Access to the interface computer by TCP/IP address, hostname, or FQDN

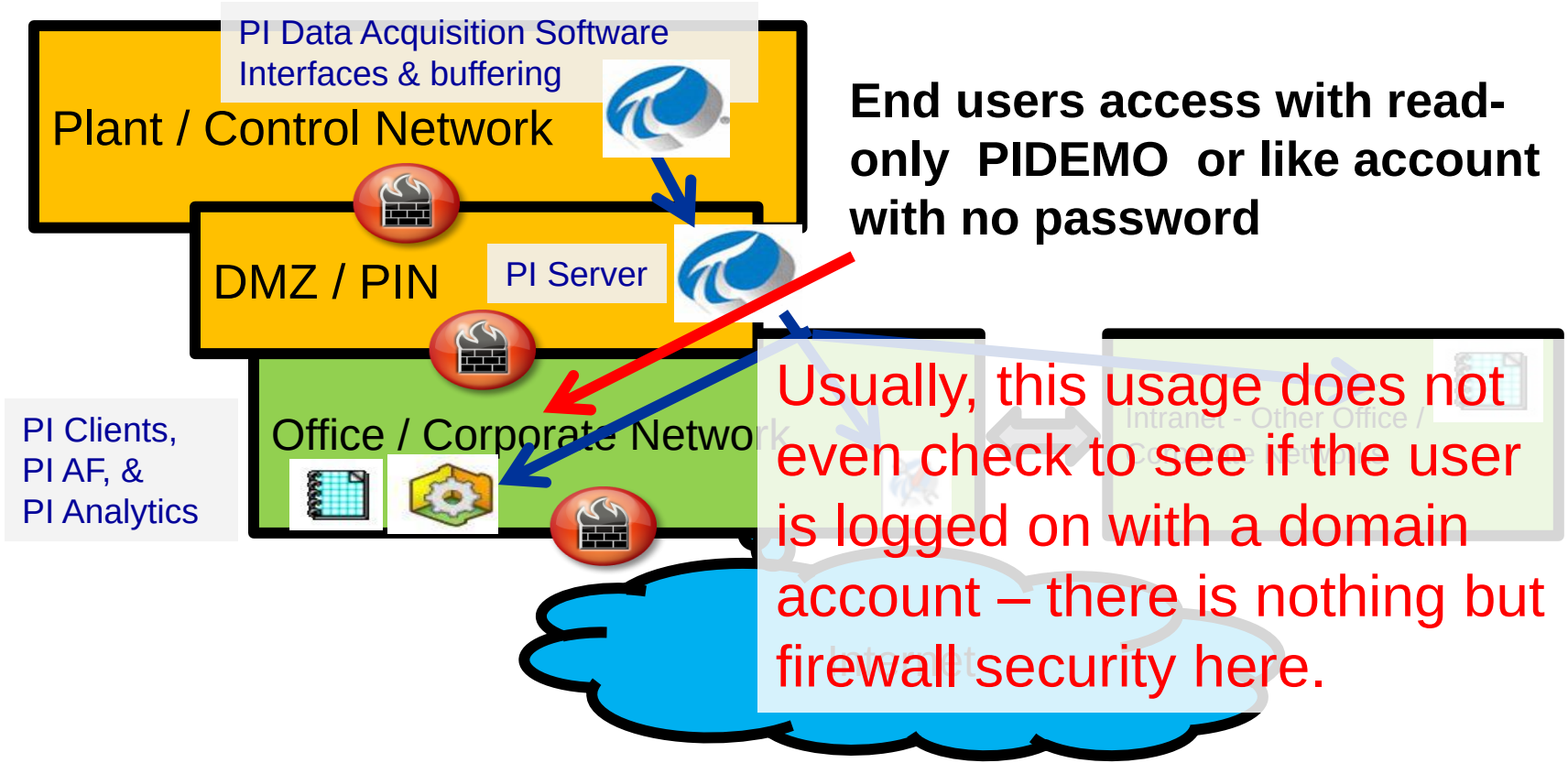
Anyone sitting at the interface computer has full PIADMIN access rights to reconfigure the PI Server even change the PI Server security for others. This is not required by the interface.



Typical “Old School” PI System Security



Typical “Old School” PI System Security



But I have trusts!

Although trusts are rule-based and better than passwords in that respect, trusts are always permissive, never restrictive and so the security is provided by passwords and those are not-so-good.

Trusts are just too…

trusting.

Typical “Old School” PI System Security

and none of this is likely to stand up to any sort of I.T. audit…

So what do I do about it?

What if I told you that you could have easier to manage, much more secure PI System security and it would only take a few hours…?

well, it may also take something else

(we'll come back to that)

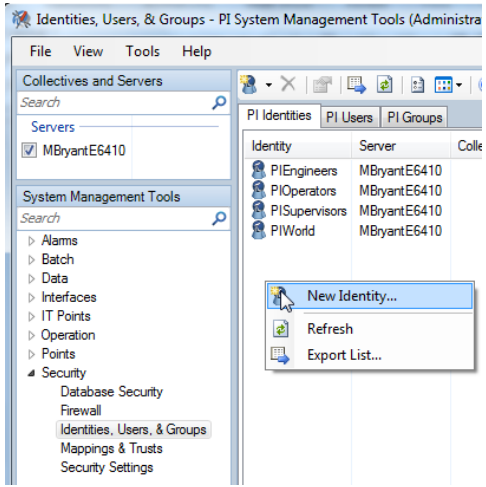
First, better secure your interfaces

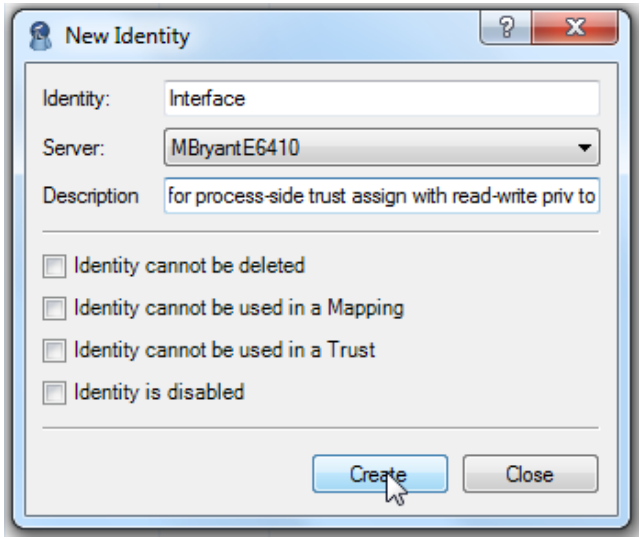
Our interface software currently does not yet support Windows Integrated Security, (it is unlikely you would have a domain which could authorize to the PI Server in the plant anyway) so we must continue to use trusts in the plant/process network.

But there are some things we can do, and you are already likely using trusts for your interface so you just have to improve them a little…

First, better secure your interfaces

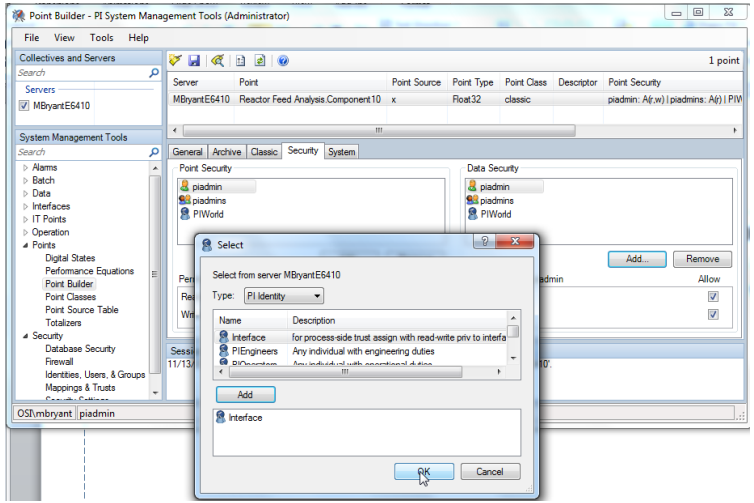
1. First, using the PI System Management Tools (PI SMT) create a new identity (or user), say “Interface” to assign the interface node privilege

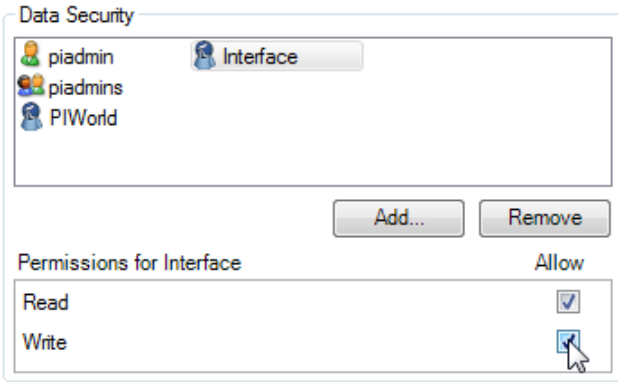




First, better secure your interfaces

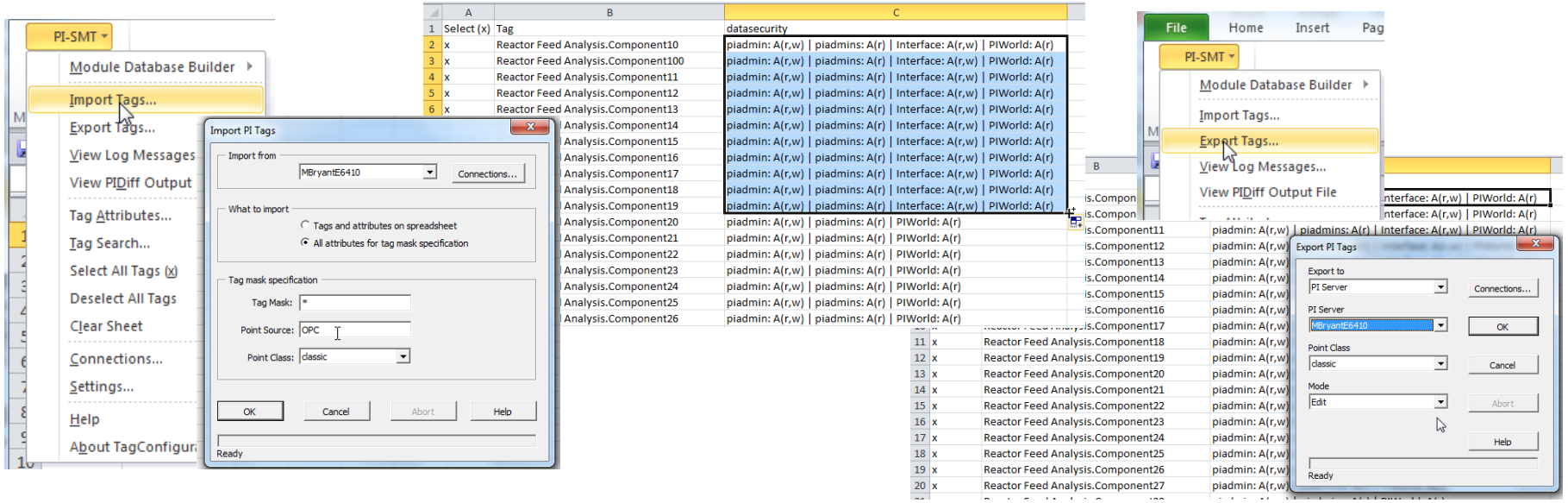
2. Using the PI SMT tag builder, set one interface tag so that your new identity has read/write privilege to it.
   (note: PIADMIN can always write to the tag, you can't change it's privilege so this tag will continue to update, even before you change the trust).





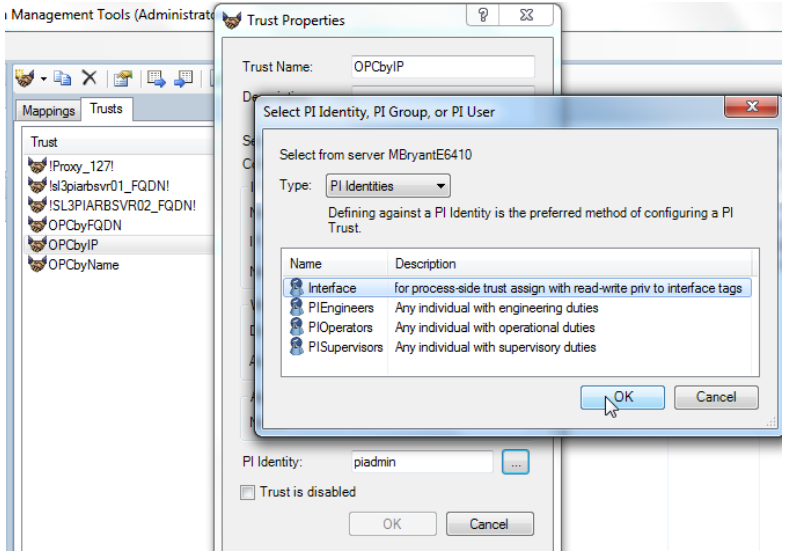
First, better secure your interfaces

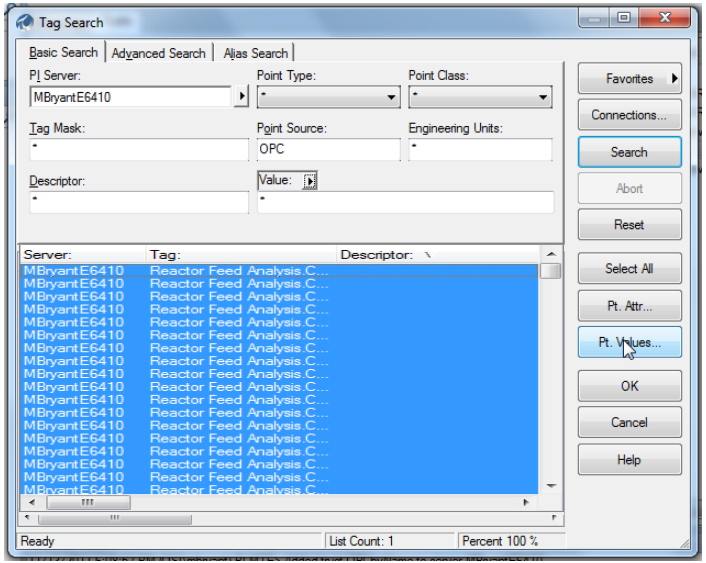
3. Use the PI SMT Tag builder for Microsoft Excel to copy the DataAcess tag attribute from this tag to all of the other tags in the interface – in minutes – even if there are tens of thousands of them.



First, better secure your interfaces

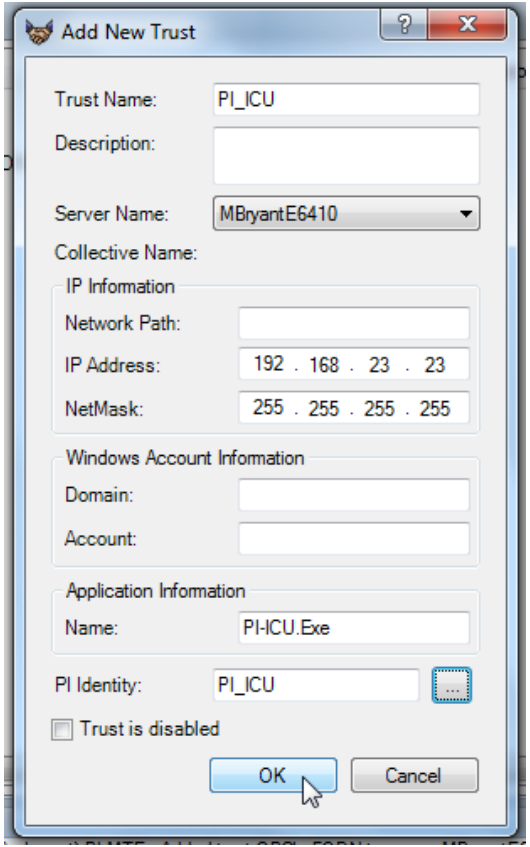
4. Change your trust(s) so they no longer give privilege to PIADMIN, but rather to your new identity. Verify you are still getting updates (Tag Search / Pt Values can do this from any tool)…





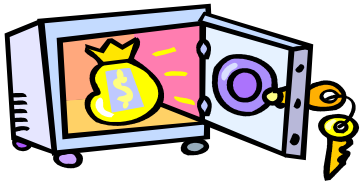
First, better secure your interfaces

Note: PI ICU (Interface Configuration Utility) still requires more privilege (build tags, edit PI MDB), so you may have to connect as a privileged user on those few occasions when you are running the PI ICU. You could make a trust for this, using the application name PI ICU.exe and limit it to that workstation.



Now for your admins & end users –
Windows Integrated Security

More secure – each new connection is required to present a Kerberos compliant expiring token from a Windows Active Directory domain controller to prove they are who they say they are.



Easier to Manage – not restricted to three access rules (Owner, Group World) per tag or object – you can have as many as you need. Identities don't just get one best fit ruleset as with a trust – they get all they are entitled to. No need to have individual PI Users, no need to have passwords.

What will I need? Won't I have to upgrade everything?

PI Server 3.4.380 (fall 2009) or PI System 2010

Interfaces are not affected

PI Clients - PI SDK 1.3.6

PI ProcessBook 3.1 (fall 2008) or higher

PI DataLink 4.0 (summer 2008) or higher

PI WebParts (RtWebParts) 2.2 (summer 2008) or higher

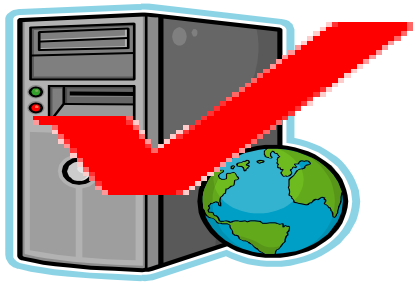
Two new things in PI Windows Integrated Security:

- **Identities** - are role-based “place holders” used to create access rules for tags & database rights in the PI System. Easy to build – easy to apply (only three possible privs: Read, Read/Write, and none) .
- **Mappings** - tie an Active Directory domain user or group to a PI Identity. Easier to build than and less complicated than a trust (five mouse clicks) .

Mappings require a domain controller

Mappings require Kerberos token validation to a domain controller.

You must be able to connect to a valid domain controller to gain access through a mapping and you must be logged into the domain that that controller supports.

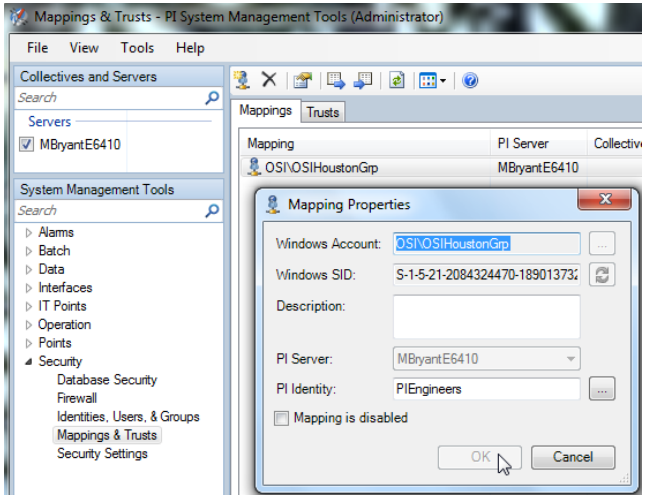


Sample Active Directory Groups for PI System Applications…

	Intended use:
PI_servername_ProcDataIntf	Primary process interfaces, usually assigned to service accounts allocated to interfaces and buffer system services- given read/write to process data tags
PI_servername_ProcDataCfg	System managers and others configuring the PI tag database - could be given read/write on almost all tags and PIPoint Database and PI digital states database. May also include read/write privilege to PI MDB and batch. May be used to configure interfaces and assigned to service accounts supporting PI APS.
PI_servername_LabEntry	Low volume/frequency interfaces (like lab or Html) or privilege to users who enter data into PI through PI ML or other application.
PI_servername_PISysMgr	System managers responsible for security, backup, archive management, tuning parameters, collective management and troubleshooting the PI system may not imply or require direct application to PIadmin.
PI_servername_ProcAnalyst	Engineers, integrators, and others developing PI MDB, PI AF, Sigmafine, PI Notifications, PI ACE and potentially PI Performance Equation and totalizer tags. May be used to permit specialized access for batch configuration datasets for RtWebParts or RtReports.
PI_servername_SiteReadOnly	Broadbase read-only user population for the site (analogous to current usage of PIDemo)
PI_servername_OrgReadOnly	To provide data viewing to those at other sites in the same organization - may be assigned to a PI-to-PI interface through a system service
PI_servername_Restricted	PI viewers in another organization (partners, suppliers, regulatory agencies) or others with a access to read data for only a subset of PI tags - may be assigned to a PI-to-PI interface through a service account.

But maybe it doesn't have to be that complicated…

- Do you already have some of these groups? If you already have Windows Active Directory groups for any of these needs – you could just use those geographic or functional groups that your I.T. dept. is already maintaining and create your mappings to those.
- Maybe you only need two groups: PI Administration & PI End Users.

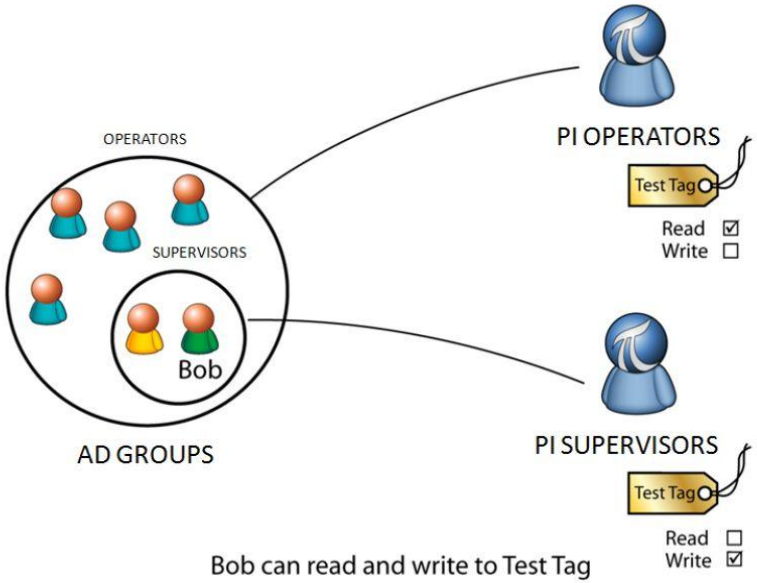


I’m not sure I want I.T. to manage this….

You don't want to have someone else manage your groups? Make local groups on the PI Server - put Active Directory / Windows domain users in the local group and Windows Integrated Security / Kerberos will still validate the users and you can manage the groups...

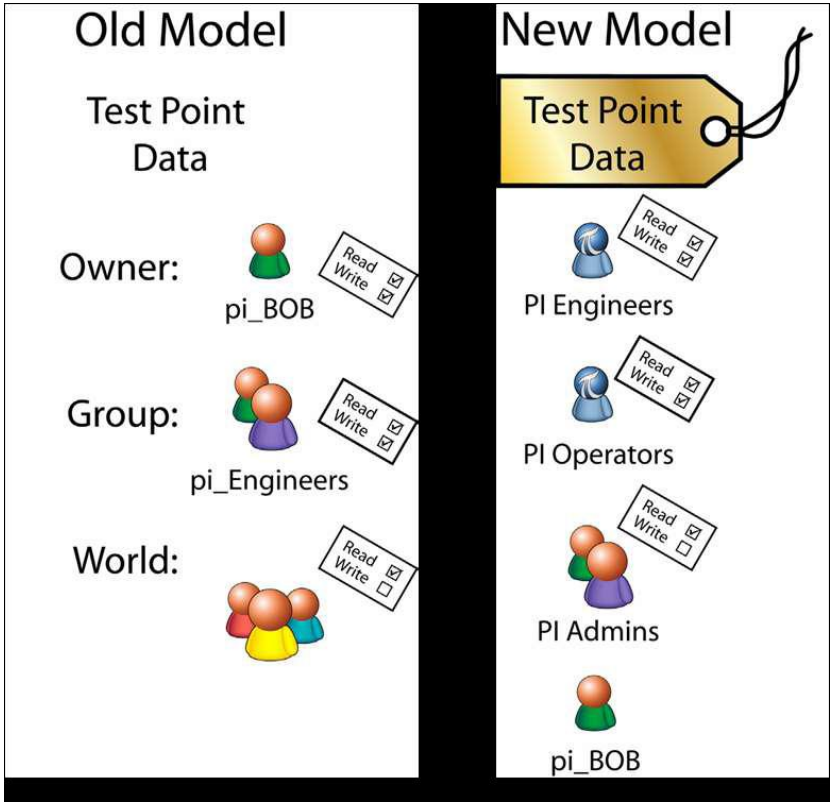
Remember…

Mappings are cumulative, not exclusive, so if Bob has a mapping made for his individual user (to say, _LABENTRY so he can write to a tag) and Bob is a member of a group (maybe for the Houston office) who can read a different tag. He gets both privileges. By comparison PI Trusts only allow one “best fit” association based on a scoring algorithm.



And …

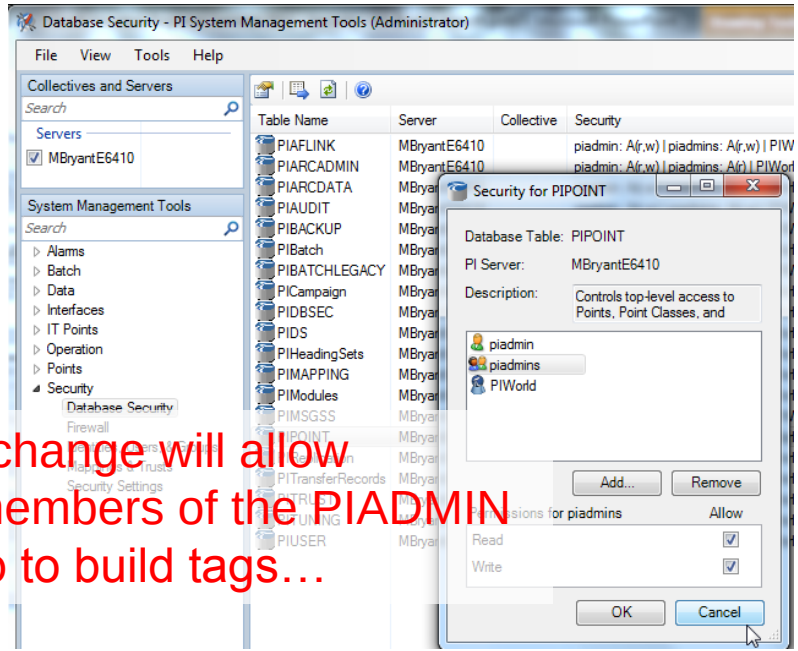
Tags and PI System databases (PIADMIN functions) aren't limited to three rulesets (Owner, Group, World) – you can make as many simple rules as you need.



Now about PI Server administration…
You really shouldn't be using PIADMIN for everything

So what do I do?

1. Create an identity or use the PIADMINS group
2. Assign "Write" privilege to Databases (which are really PI Admin functions) using the Database security tool in PI SMT…
3. Associate the individuals or groups who should have these PIADMIN privs with a mapping



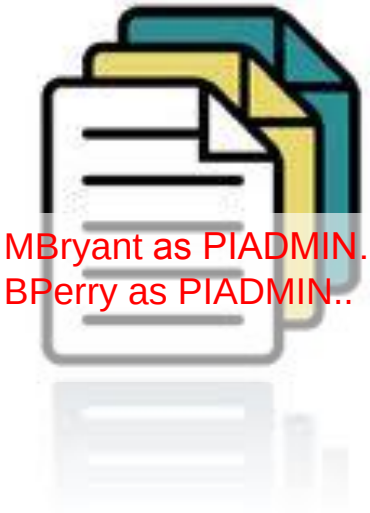
This change will allow the members of the PIADMIN group to build tags…

And even if you don't use Windows Integrated Security / Mappings…

With PI Server 3.4.380 (and higher)-

The PI Server captures the Active Directory account of PI Server changers /admins (if available) and records them in the PI Server log.

Even if they are all connecting as PIADMIN (which they really shouldn't).

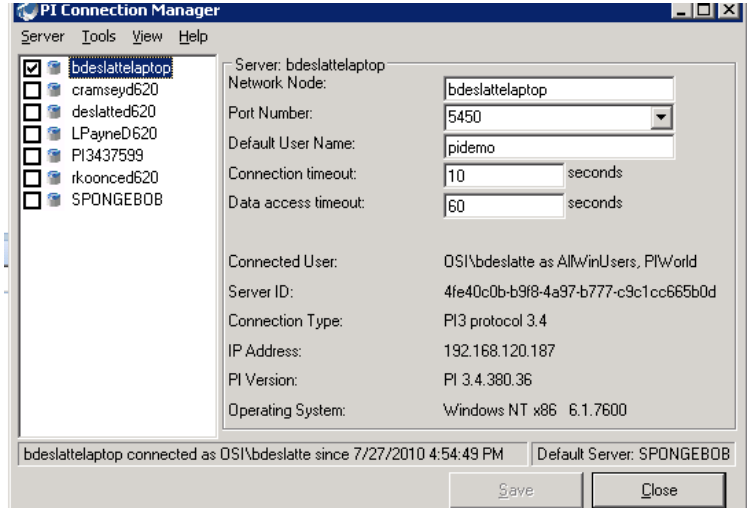


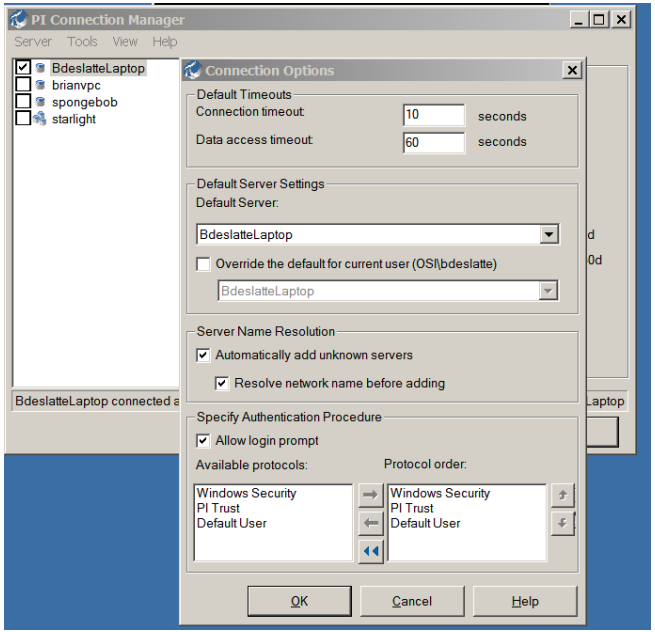
For end-users

<u>The same basic process</u>

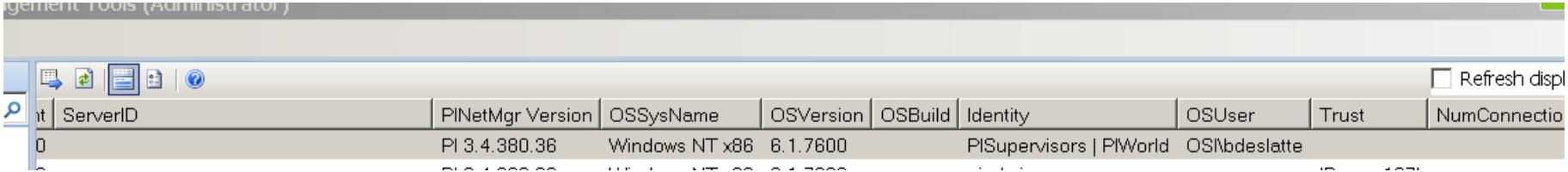
1. Create an identity or identities as needed
2. Grant Read access to databases (PIARCDATA, PI MODULE DB, PIBATCH, PIDS, etc..)
3. Map to groups in Active Directory – either those you had I.T. create, those that already exist and are maintained by I.T. or local groups of domain users…

PI Client 1.3.6 more information & more choices

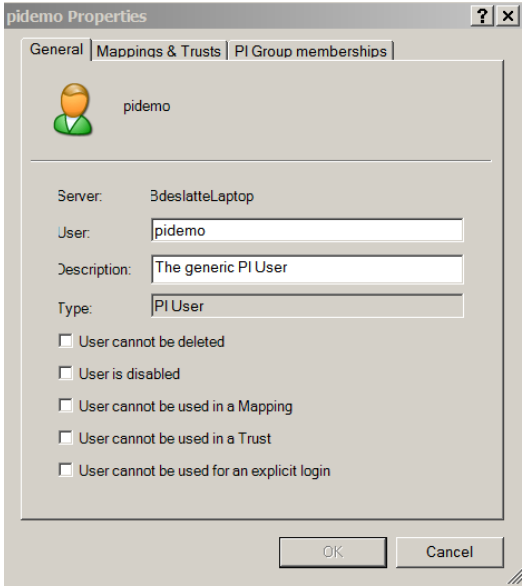




PI Server 3.4.380 & beyond gets more too…



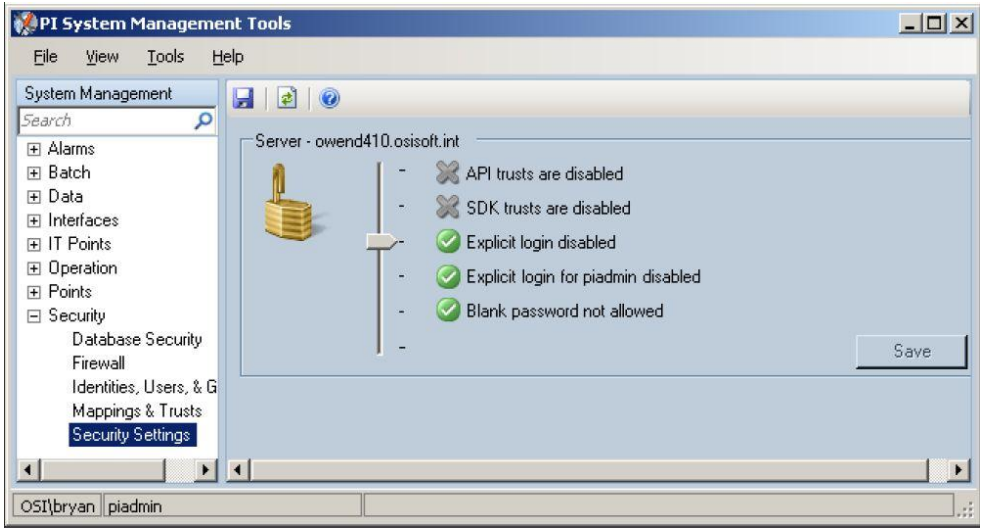
- **PI Network Management Statistics in PISMT shows you more information..**
- **Create a trust from a Network Mgt Connection**
- **Convert a Trust to a Mapping**
- **Identities, Users have more options**
- **Trusts, mappings can be disabled**
- **PIWorld (“everyone”) can also be managed and disabled…**



After your groups and mappings and rules are in place…

- Disable PI World (identity) and PI Demo (user)
- Raise the Security settings slider bar to disable explicit logins

  (requires a PI System restart)
- No need to change the PIADMIN password
- No need for passwords
- No need for users
- No need to manage either
- **Better, more convenient rules-based security**



Two more great reasons to use Windows Integrated Security:

PI AF (Asset Framework)

and

PI Coresight

Both require Active Directory

So if this is not that hard…

and I'm not likely to have to upgrade everything

and in the long run it's going to be less trouble

and I'll be so much more secure

and I'm going to wind up doing this anyway because I want the new products…

Why doesn't everyone just do this?

Well… remember that other thing I mentioned?

Firewalls present challenges for Kerberos

Most firewalls aren't set up to permit Windows / Kerberos validation – very often you can't use Windows Integrated Security through a firewall. So if your PI Server is the DMZ/PIN, you may not be able to get tokens to it if it can't "see" the Active Directory Domain Controller.

There are ways to deal with this –

a trusted domain in the DMZ is one

very specific firewalls rules are another

But that means even if you made your own local groups in the PI server

you may have to…

Get some help from I.T.

(they respond well to offers of food)

Two other tips

You can install PI AF in the corporate/domain network, it doesn’t have to be on the same computer as the PI System. In fact, one PI AF server/PI System can support the module databases of several PI System 2010 data servers (even through firewalls) and if it is in the domain you’ll be more easily able to use the Table lookup databases to get data from other relational database sources.

Two other tips

Be careful if you are using PI AF with PI WebParts and/or PI Coresight so that you get a big enough PI WebParts / PI Coresight server to handle the PI AF client software for multiple users.

Thank you