APSYS

AUGMENTED TRUST

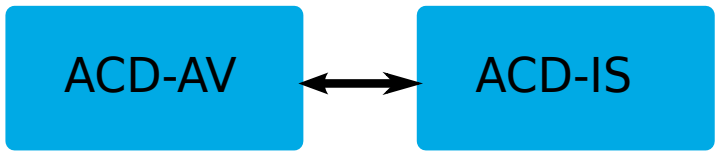
SECURITY ARCHITECTURE

A reference for embedded systems

Domains on real products

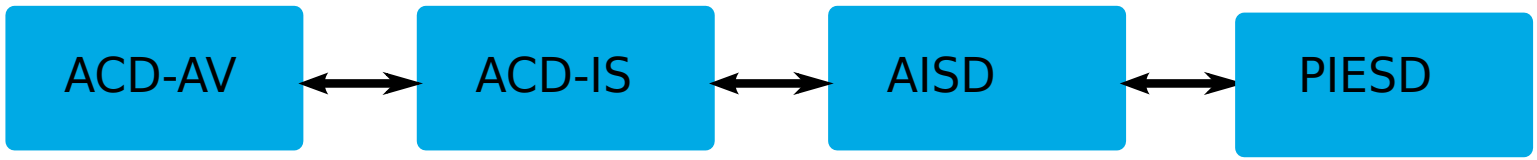
ACD-AV

Domains on real products



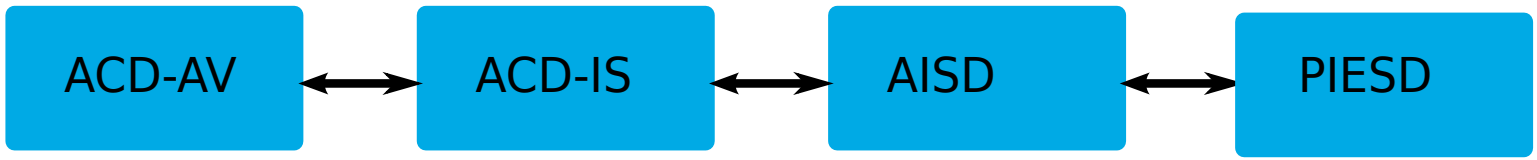
Domains on real products

Domains on real products



ARINC 811

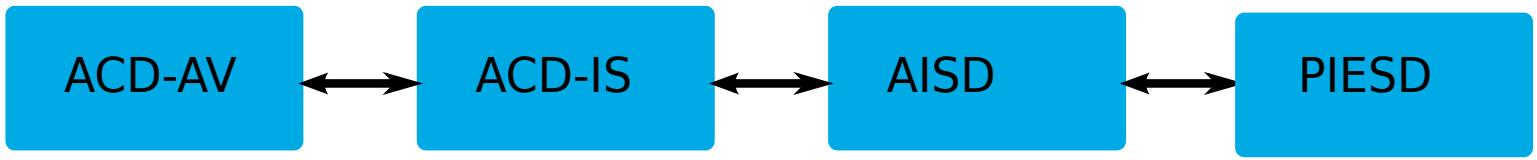
Domains on real products



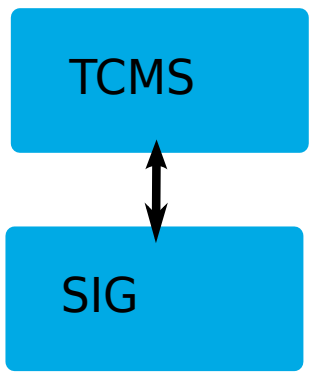
ARINC 811

SIG

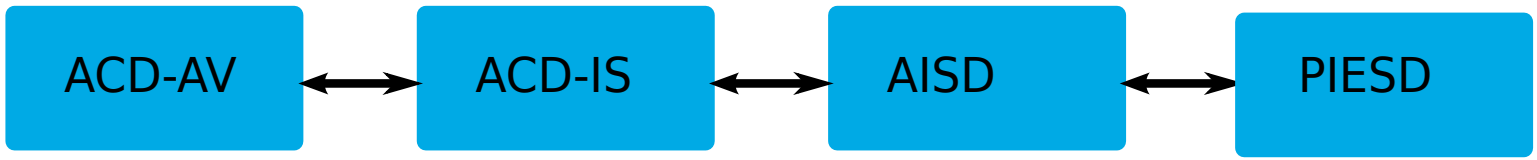
Domains on real products



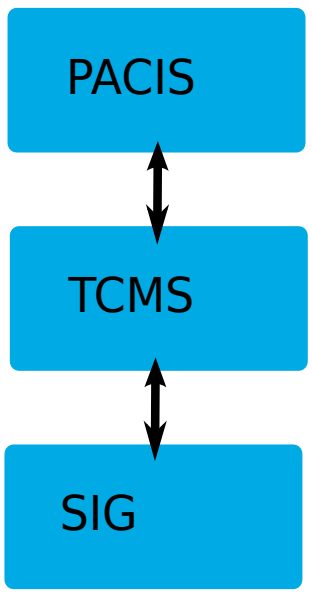
ARINC 811



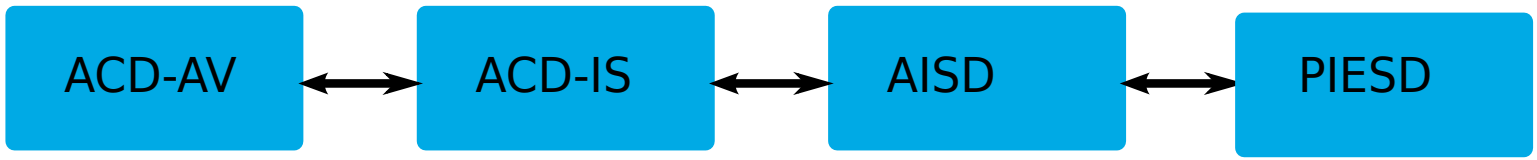
Domains on real products



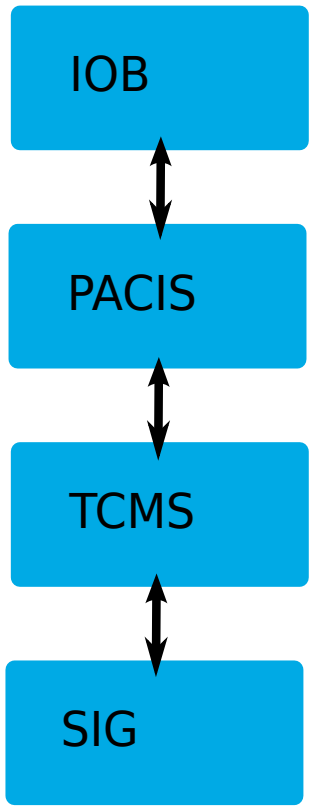
ARINC 811



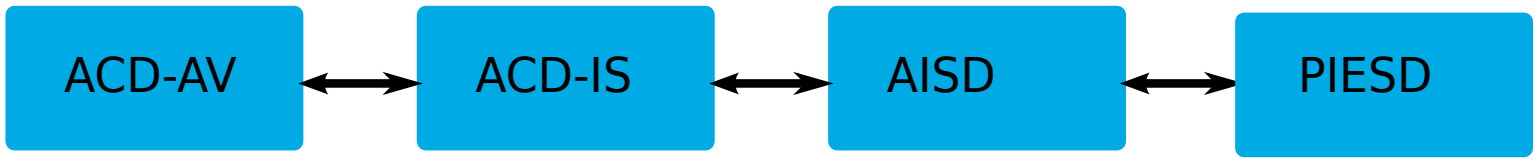
Domains on real products



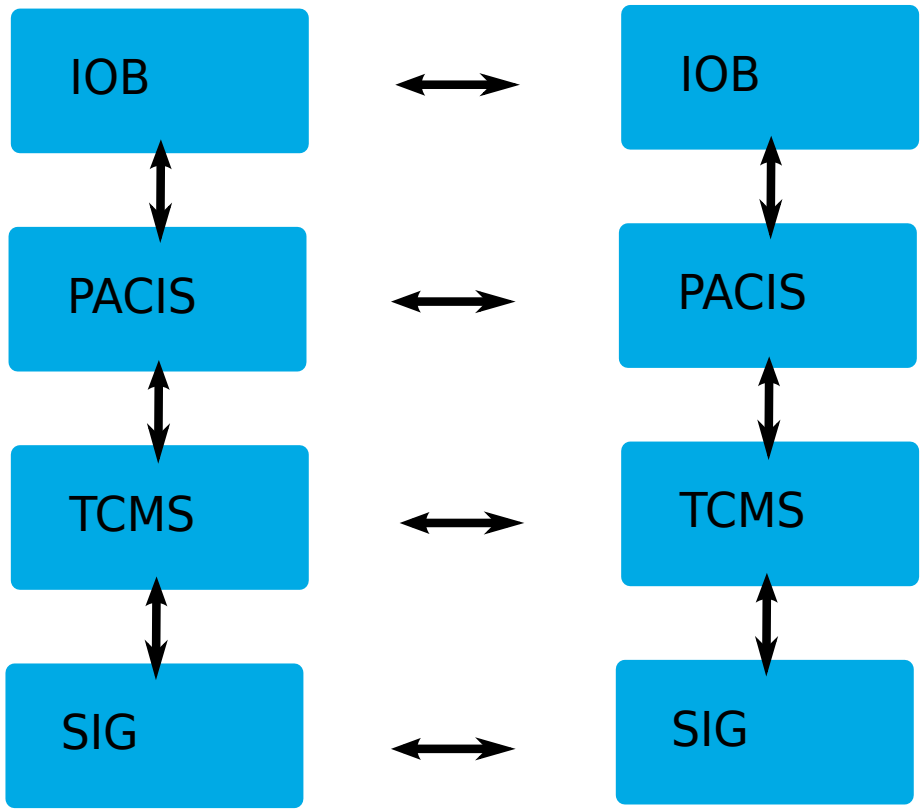
ARINC 811



Domains on real products



ARINC 811



Plan

1. Basic principles of security architecture
2. Typical requirements for embedded systems
3. Consequences on architectures
4. Main security functions
5. Reference architecture

Basic Principles

Security function shall be updatable

- Attacks get better
- Vulnerabilities are discovered

Separate Critical from Security

- Critical functions don't change often and are very costly to certify
- Security functions have to be updated over time
- Separating them makes the update easier and less expensive

Basic Principles

No single vulnerability shall compromise the system

- Do not trust any individual component

Defense in depth

Apply principle of least privilege

Control data entering higher-criticality domains

... using “proxies” or “application-level filters” (ALF)

Plan

1 Basic principles of security architecture

2 Typical requirements for embedded systems

3 Consequences on architectures

4 Main security functions

5 Reference architecture

Embedded systems requirements

Internet connection

- For updates, non-critical applicative communications
- Wi-Fi for passengers

No Internet connection

- Planes in warehouses
- Helicopters in the wilderness
- Trains in tunnels
- ...

Embedded systems requirements

Critical networks

- Impacts (catastrophic)
- Real-time requirements (i.e. availability)

BYOD : Bring Your Own Device

- E.g. Pilot EFB, Phones in cars, ...
- i.e. uncontrolled equipment connected to our system

Embedded systems requirements

Maintenance

- Software updates
- Testing

all requires access to the entire system

Standard IT solutions do not apply

- No admin
- No SOC
- No real-time reaction

But system entirely defined at design time

Plan

1 Basic principles of security architecture

2 Typical requirements for embedded systems

3 Consequences on architectures

4 Main security functions

5 Reference architecture

Domains

- Identify domains based on security impacts
- Segregate applications
- Identify dataflows between domains
- Protect Higher-impact domains from lower domains
  - Limit dataflows to specification
  - Limit data rates
  - Verify data format
- Avoid dataflows from domain n to $n + 2$

Each domain is a DMZ for the next domain up

Plan

1 Basic principles of security architecture

2 Typical requirements for embedded systems

3 Consequences on architectures

4 Main security functions

5 Reference architecture

Changing domains

Going down...

- Firewall (for confidentiality)

Changing domains

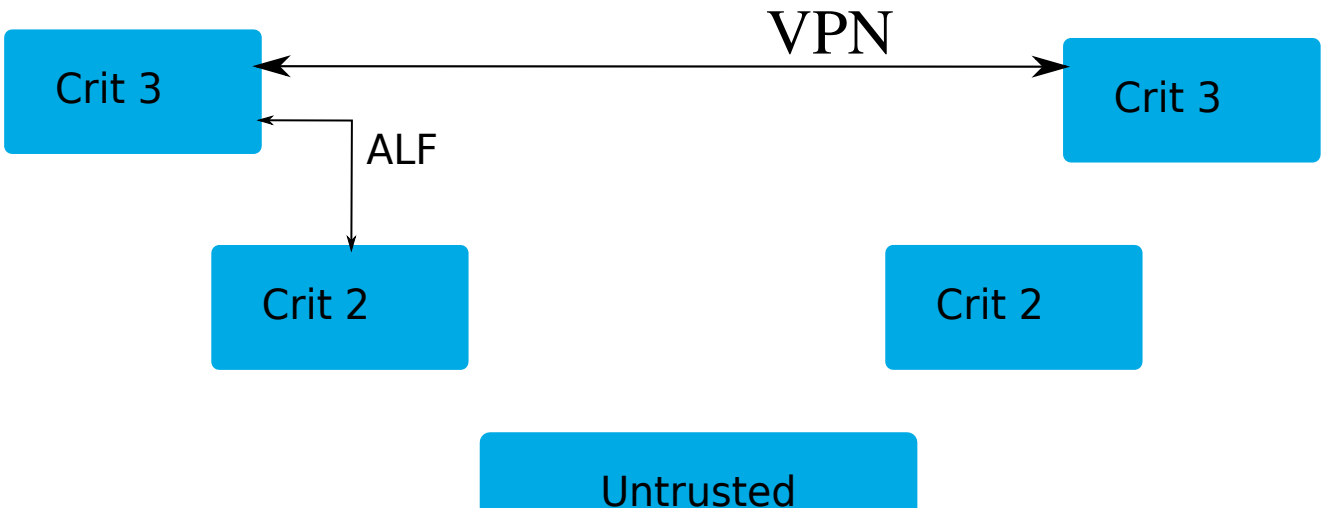
Going up...

Two threats :

- Incoherent corruption
- Coherent corruption

Two impacts : NSE, SE

	NSE	SE
Incoherent corruption	ALF	ALF
Coherent corruption	ALF	VPN to same-level or validation



Plan

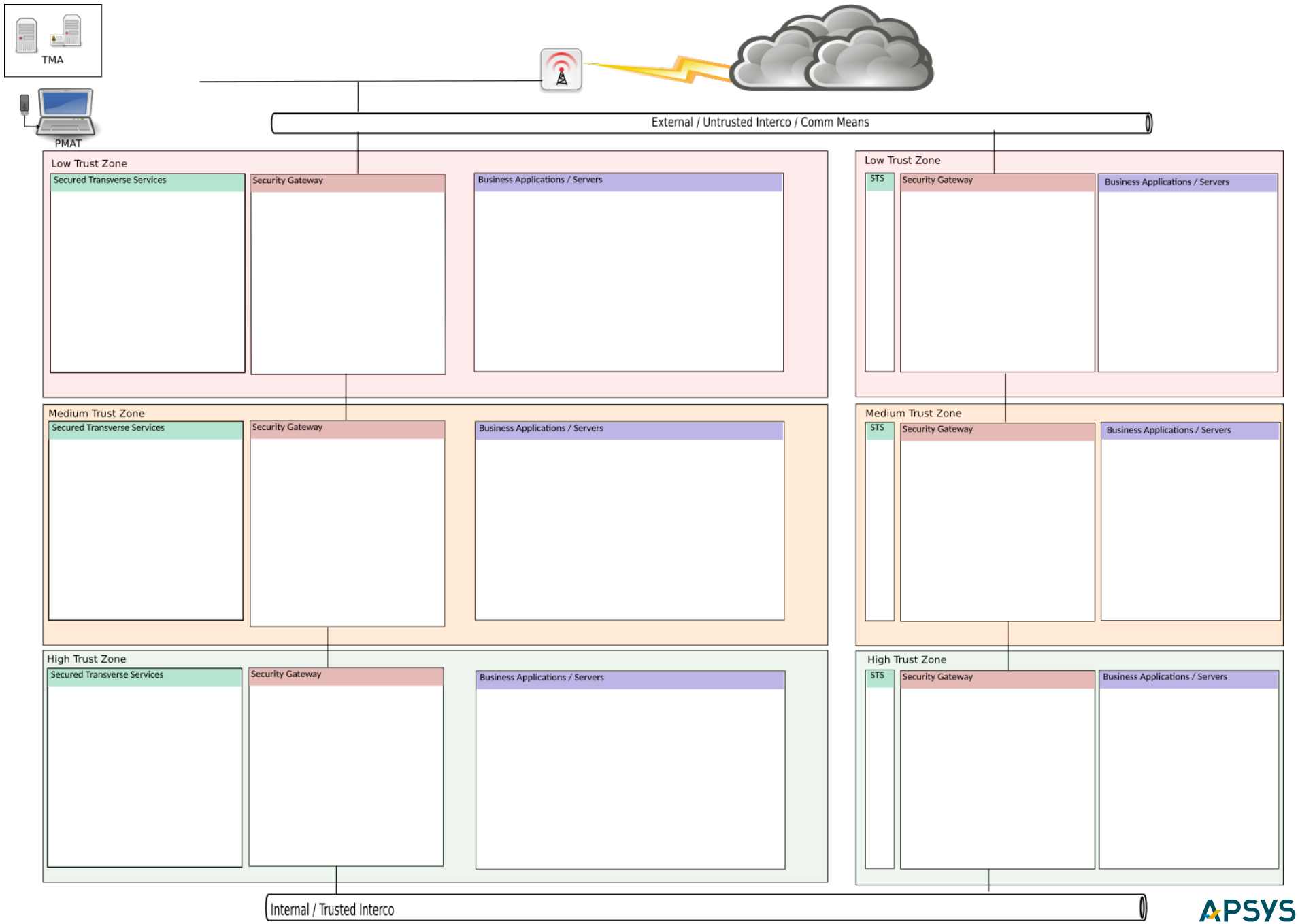
1 Basic principles of security architecture

2 Typical requirements for embedded systems

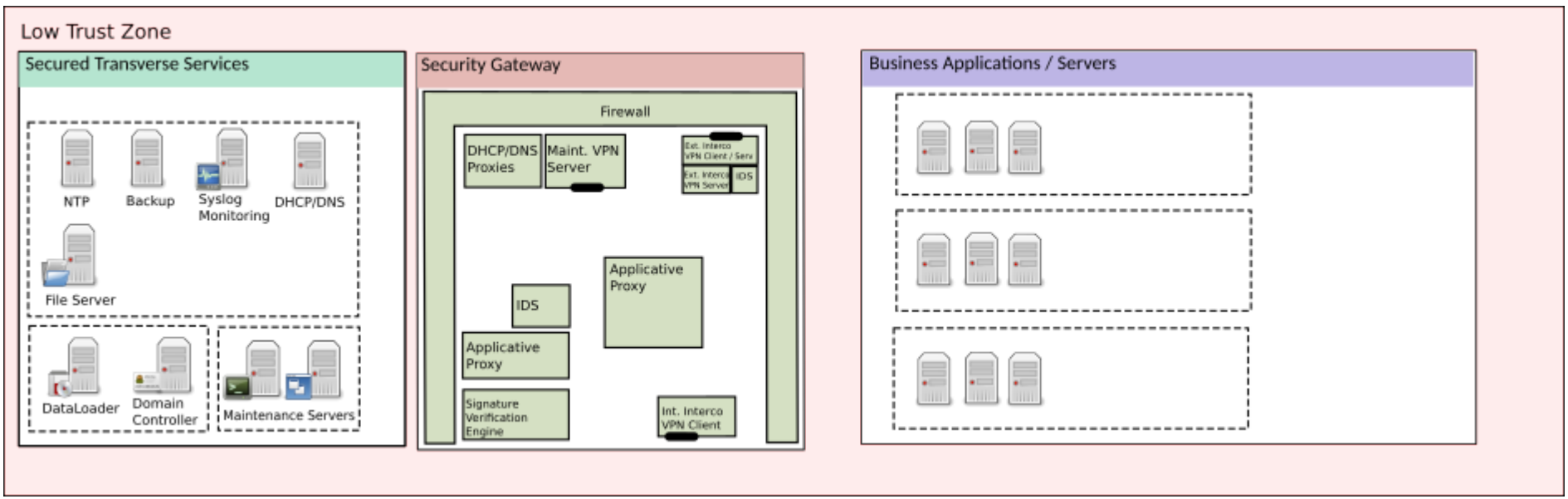
3 Consequences on architectures

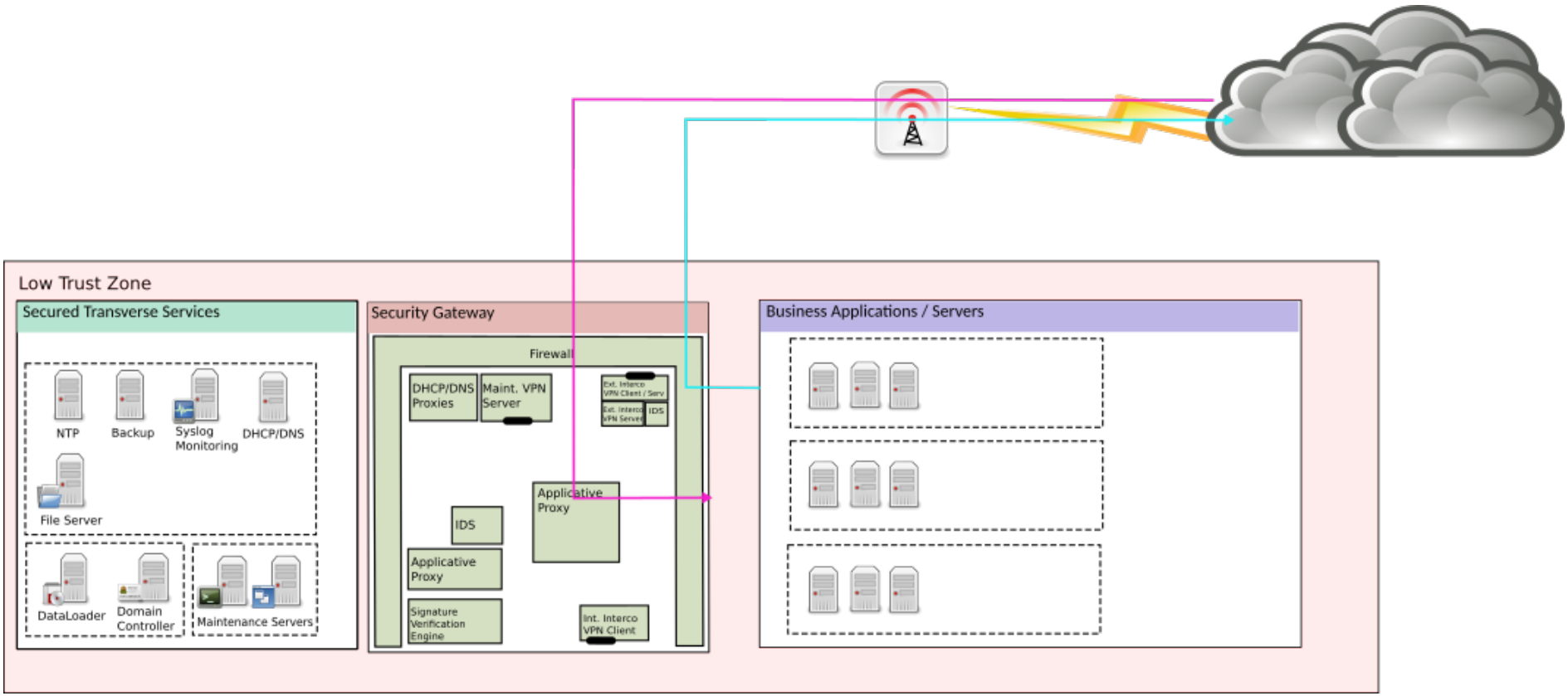
4 Main security functions

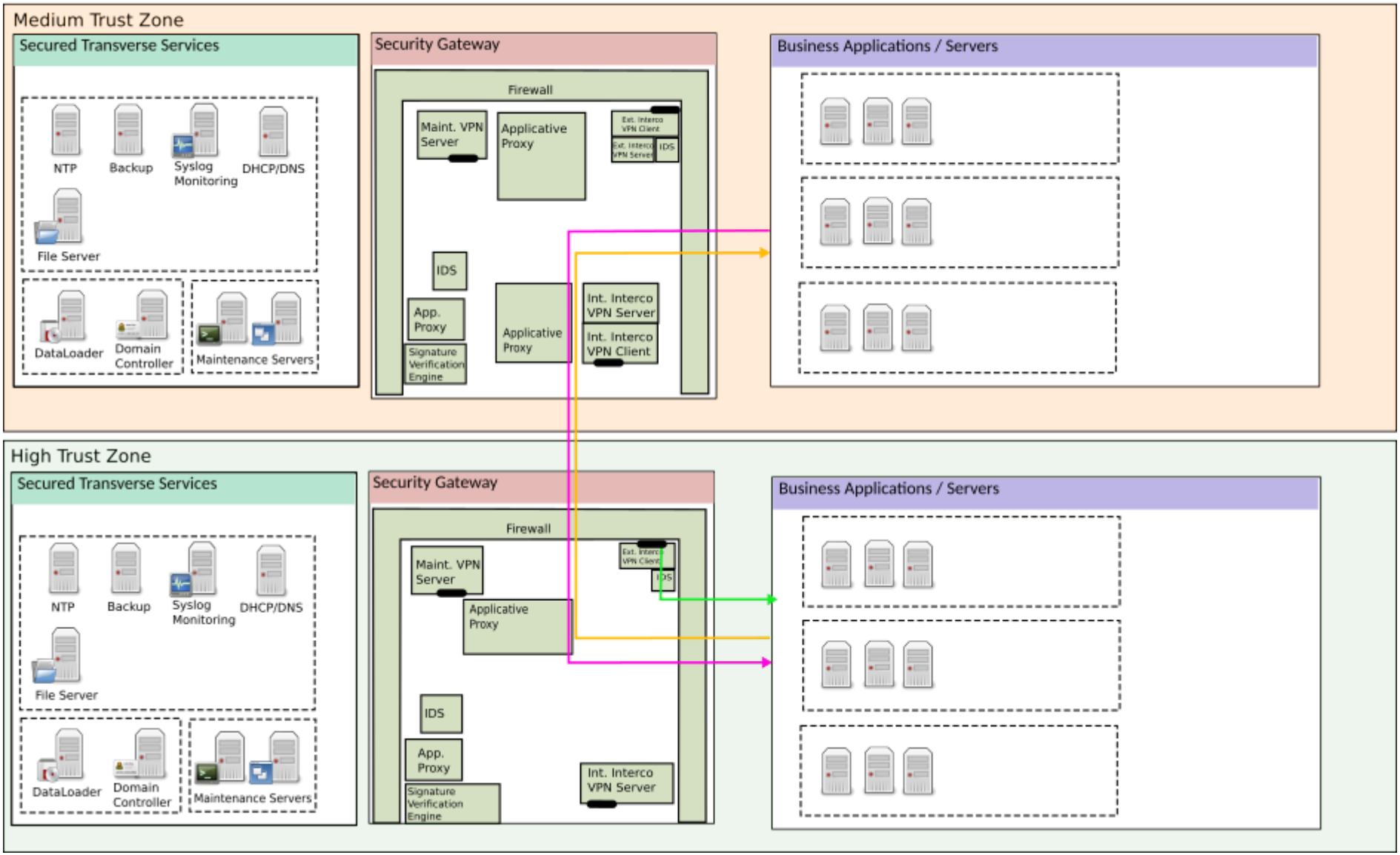
5 Reference architecture

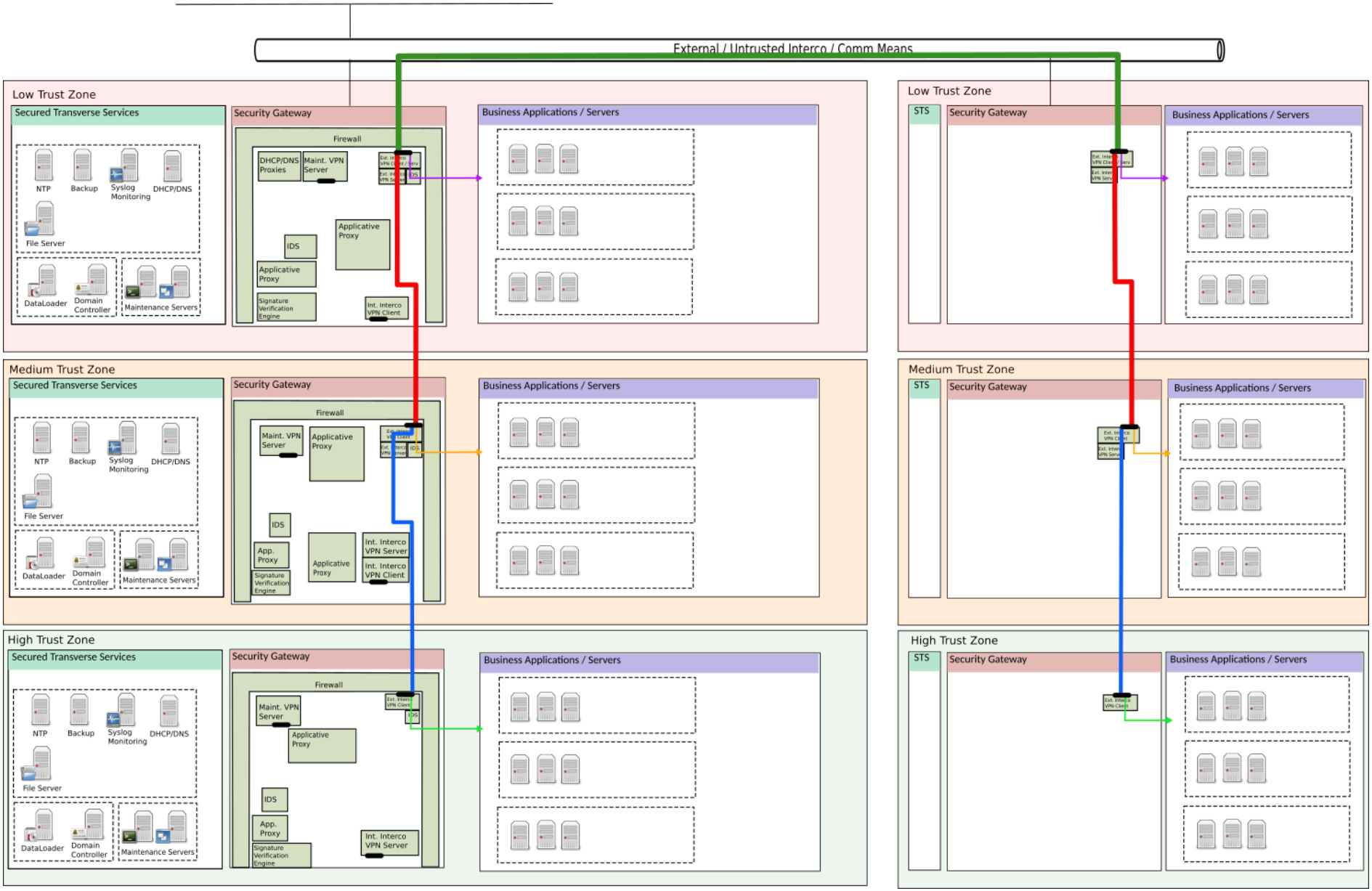

TMA
PMAT
External / Untrusted Interco / Comm Means
Low Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
Low Trust Zone
STS
Security Gateway
Business Applications / Servers
Medium Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
Medium Trust Zone
STS
Security Gateway
Business Applications / Servers
High Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
High Trust Zone
STS
Security Gateway
Business Applications / Servers
Internal / Trusted Interco

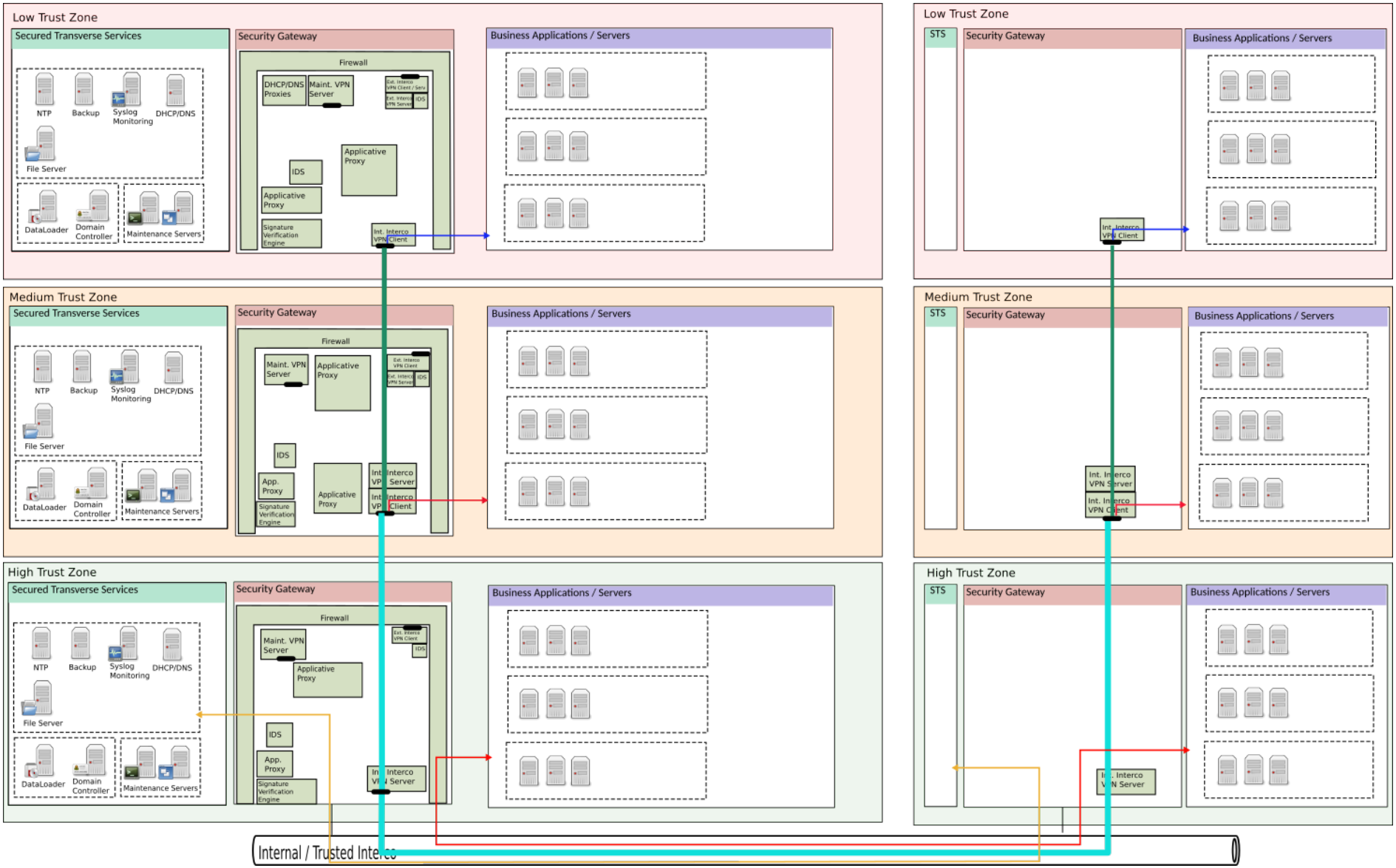
One domain

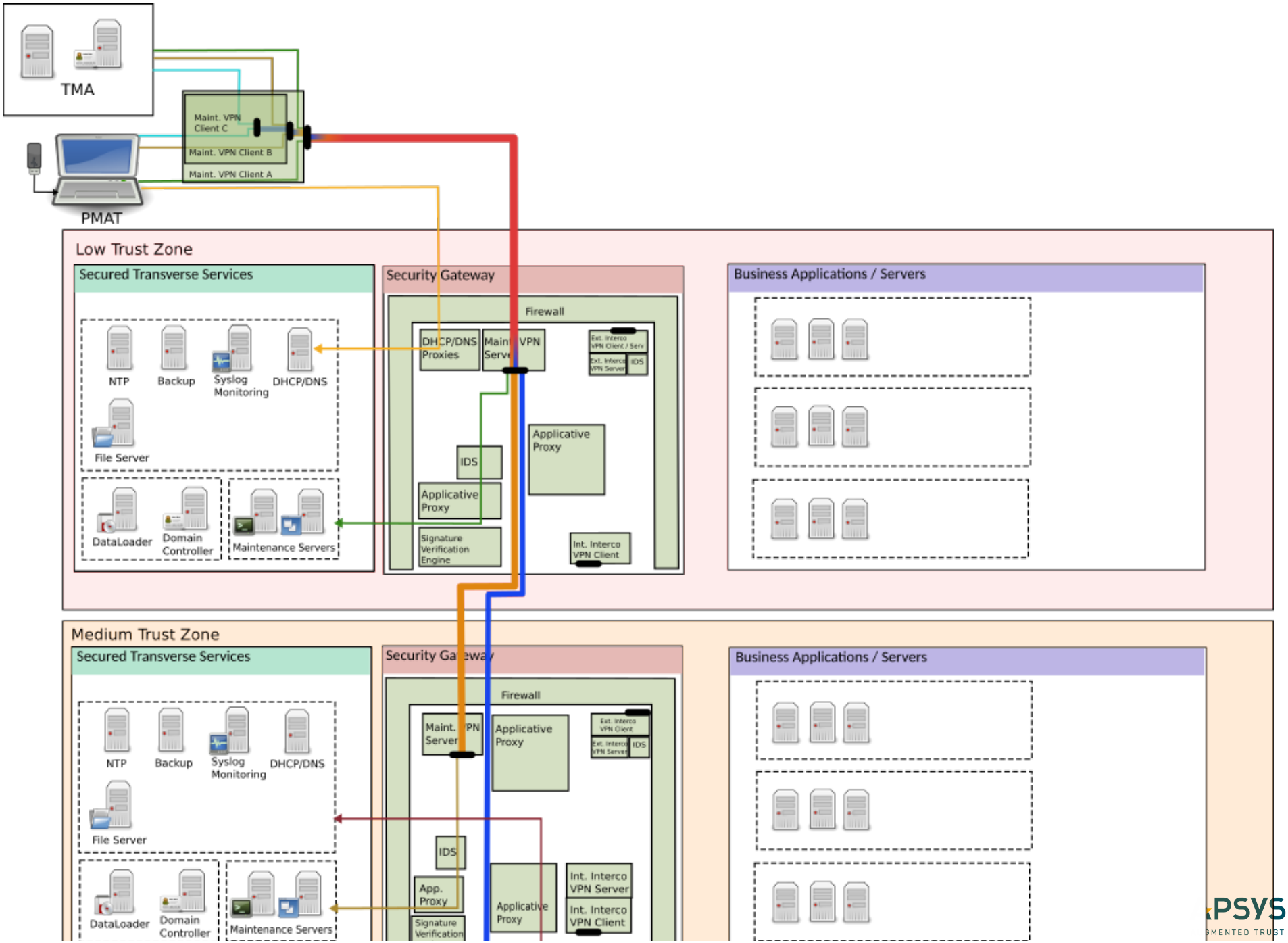

Low Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
DHCP/DNS Proxies
Maint. VPN Server
IDS
Applicative Proxy
Applicative Proxy
Signature Verification Engine
Int. Interco VPN Client
Business Applications / Servers


Low Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
DHCP/DNS Proxies
Maint. VPN Server
Ext. Interco VPN Client / Serv
Ext. Interco VPN Server
IDS
Applicative Proxy
IDS
Applicative Proxy
Signature Verification Engine
Int. Interco VPN Client
Business Applications / Servers


Medium Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
Maint. VPN Server
Applicative Proxy
Ext. Interco VPN Client
IDS
App. Proxy
Signature Verification Engine
Applicative Proxy
Int. Interco VPN Server
Int. Interco VPN Client
Business Applications / Servers
High Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
Maint. VPN Server
Applicative Proxy
IDS
App. Proxy
Signature Verification Engine
Int. Interco VPN Server
Business Applications / Servers


External / Untrusted Interco / Comm Means
Low Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
DHCP/DNS Proxies
Maint. VPN Server
IDS
Applicative Proxy
Applicative Proxy
Signature Verification Engine
Int. Interco VPN Client
Business Applications / Servers
Low Trust Zone
STS
Security Gateway
Business Applications / Servers
Medium Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
Medium Trust Zone
STS
Security Gateway
Business Applications / Servers
High Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
High Trust Zone
STS
Security Gateway
Business Applications / Servers


Low Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
DHCP/DNS Proxies
Maint. VPN Server
IDS
Applicative Proxy
Signature Verification Engine
Int. Interco VPN Client
Business Applications / Servers
Low Trust Zone
STS
Security Gateway
Business Applications / Servers
Int. Interco VPN Client
Medium Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
Maint. VPN Server
Applicative Proxy
IDS
App. Proxy
Int. Interco VPN Server
Int. Interco VPN Client
Medium Trust Zone
STS
Security Gateway
Business Applications / Servers
Int. Interco VPN Server
Int. Interco VPN Client
High Trust Zone
Secured Transverse Services
Security Gateway
Business Applications / Servers
Maint. VPN Server
Applicative Proxy
IDS
App. Proxy
Int. Interco VPN Server
High Trust Zone
STS
Security Gateway
Business Applications / Servers
Int. Interco VPN Server
Internal / Trusted Interco


TMA
Maint. VPN Client C
Maint. VPN Client B
Maint. VPN Client A
PMAT
Low Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Security Gateway
Firewall
DHCP/DNS Proxies
VPN
IDS
Applicative Proxy
Applicative Proxy
Signature Verification Engine
Int. Interco VPN Client
Business Applications / Servers
Medium Trust Zone
Secured Transverse Services
NTP
Backup
Syslog Monitoring
DHCP/DNS
File Server
DataLoader
Domain Controller
Maintenance Servers
Firewall
Applicative Proxy
IDS
App. Proxy
Applicative Proxy
Int. Interco VPN Server
Int. Interco VPN Client
Business Applications / Servers

Questions ?