Security of Control Networks

TROOPERS 10

IT-Security Conference & Workshops

An Insiders Perspective

Agenda

- Introduction
- Tuning the CIA model
- Control systems overview
- Live demo
- Mitigations
- Observations from the inside

The Systems

- Systems that provide Supervisory Control and Data Acquisition (SCADA) were intended to meet their goals
  - to provide data in a timely manner
  - to accept control signals to open and close devices

The Systems

- Deployed on whatever hardware/OS that was commonly available at the time of their creation
  - Window XP
  - Windows 2000
  - OS/2
  - VMS
  - Windows NT

SCADA Systems

- Typical time spent designing and deploying a SCADA/Plant control system is around 10,000 hours of engineering for larger systems.
  - In terms of gear this is a couple of PC's
  - And a handful to 100's of sensors on the machine
- An average plant has several hundred of these customized devices

SCADA Systems

- SCADA systems are designed with longer life cycles
- Designed to last 20 to 30 years or beyond
- This presents challenges that don’t show up in corporate IT systems where a 3 year replacement cycle is the norm

More Challenges Faced

- Cost
  - System upgrades in Generation
    - A large electric generation facility typically has over 400 racks of equipment
    - These racks cost about 60.000 (each) Euro to replace without respect to the labor involved to install the new equipment

But what keeps the lights on?

- It's a given that systems that have been deployed perhaps decades and have not been regularly patched or even patched at all
- Vendors may void support if patches are applied that are not approved for use with the SCADA system
- SCADA Software and the protocols used to operate these systems were built in a time where there was no specific attention paid to Secure Coding Practices

Discretion …

- These systems were originally designed on closed networks
- The business need for historical data was not considered
  - PC technologies of the day were not widely available when these systems were originally deployed
  - Who would have ever thought that the suits would want access to this data

The needs of the Business

- Corporate business concerns have been driving for greater access to historical and real time data that SCADA systems can provide

- Accessing this data impacts the bottom line
  - Energy is being traded in different time increments
    - Week Ahead
    - Day Ahead
    - Hour Ahead
    - Reactive Power

The needs of the Business

- PMU (Psynco-phaser Measurement Units)
  - Provide real time measures (60 times a second)
  - Consists of the Angle of the frequency or some such nonsense that involves physics
  - This angle of reference helps improve the reliability of the grid
- Smart Grid
  - Our customers want to better control their utility usage
  - The utility can benefit from better recovery of power costs during times of peak usage

More challenges

- Internet connectivity
  - Email
  - Web usage
  - FTP
- Business Lines
  - Real Time Data (Telemetry)
  - Historical Data
- Vendors

In the field

- There is no homogeneous approach to communications at substations. This is due to a host of factors
  - Size of footprint
    - Hundreds of substations above 138Kv spread out over large geographic areas
    - The transmission system is a patchwork of efforts of the individual companies that originally built their smaller systems
  - Lack of availability of communication facilities in remote (rural) location

From the Inside

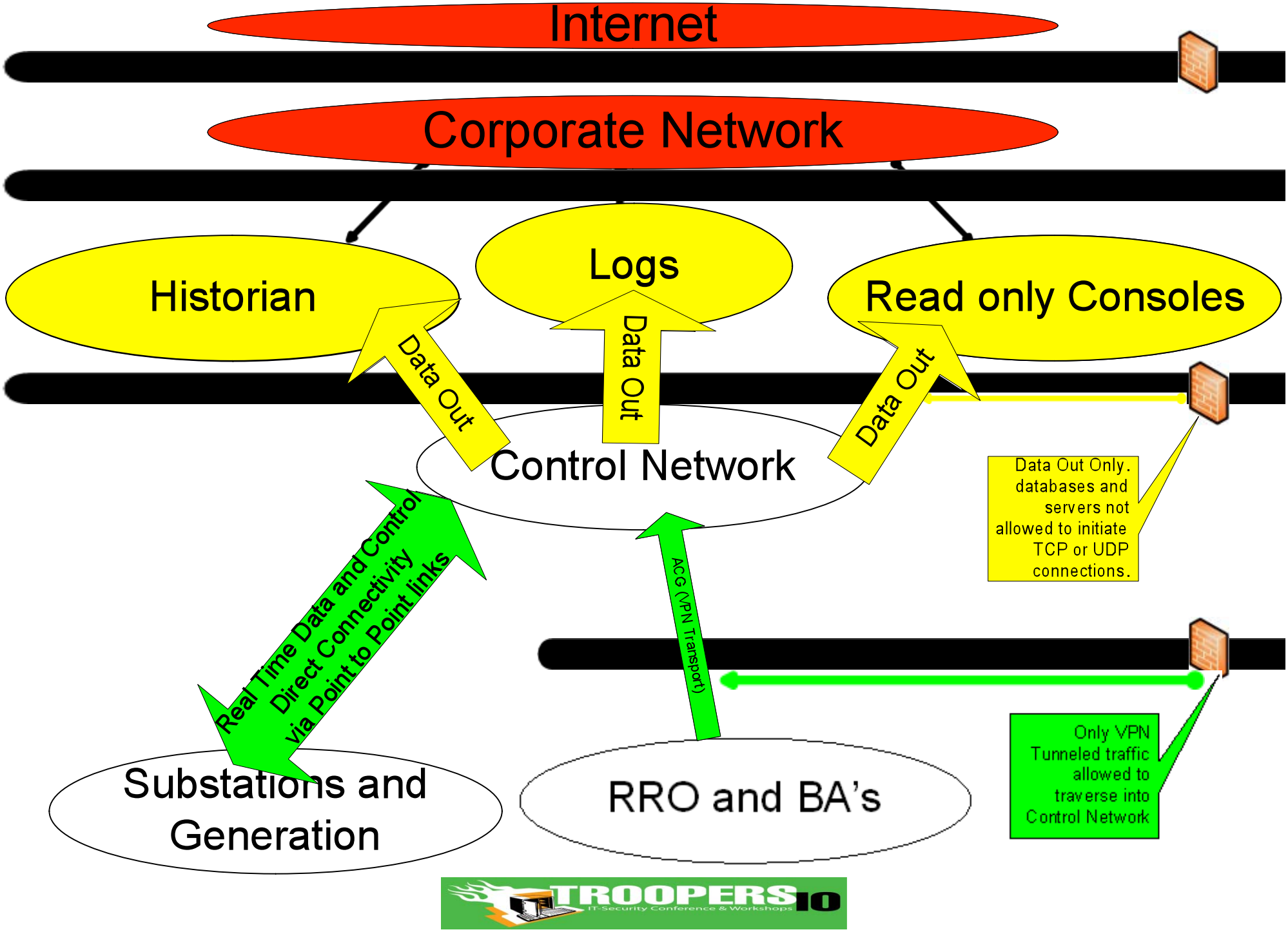
- Many aspects of the security models taught today are stressed by the needs of a control network
- The CIA just doesn't cut it on control networks
  - Confidentiality
  - Integrity
  - Availability

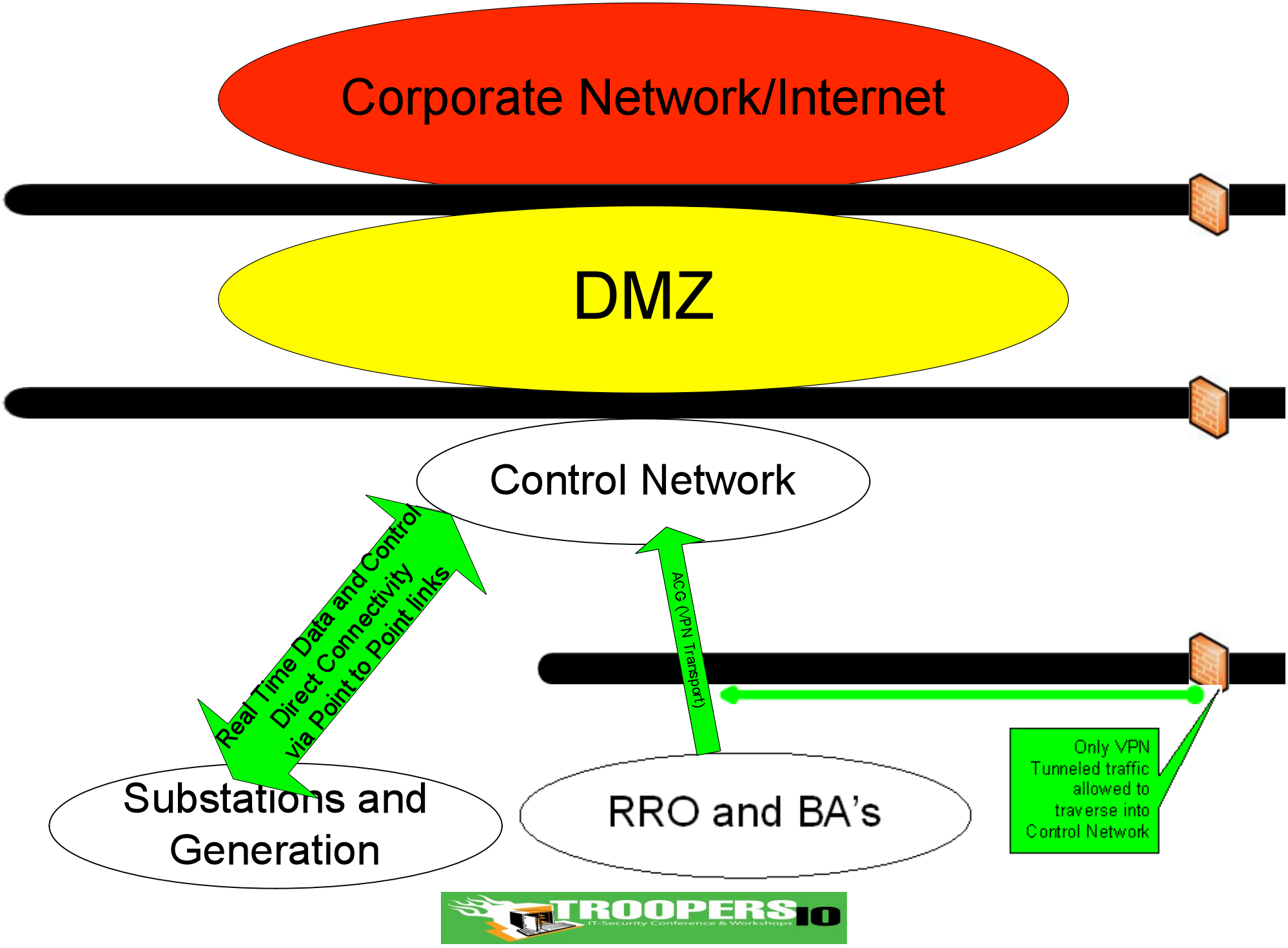
Some things are just more important

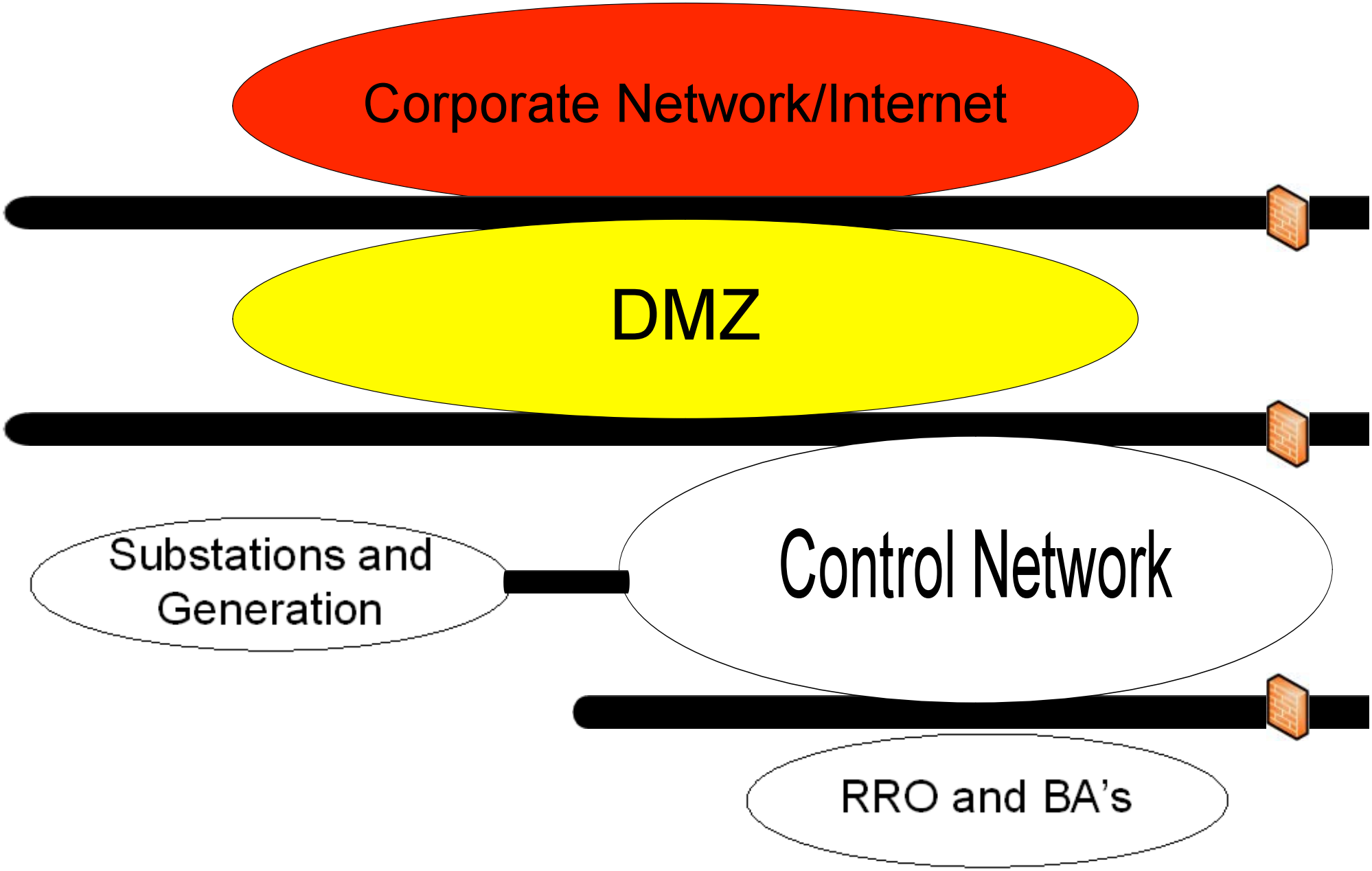
- **Utility control systems live in 6 second time slices**
- **In two seconds a control system has to digest and process telemetry from many data links spread over potentially thousands of kilometers**
- **After this information is delivered**
  - This leaves 4 seconds to solve the state of the system
- **What to do with data more than 6 seconds old?**

Okay We get it

- Data older than 6 seconds or so has no operational value
- This data is stored and archived
  - Historical
  - Planning
  - Regulatory
- Accessing the historical data presents challenges for the protectors of the network


Internet
Corporate Network
Historian
Logs
Read only Consoles
Data Out
Data Out
Data Out
Control Network
Data Out Only. databases and servers not allowed to initiate TCP or UDP connections.
Real Time Data and Control Direct Connectivity via Point to Point links
ACG (VPN Transport)
Substations and Generation
RRO and BA's
Only VPN Tunneled traffic allowed to traverse into Control Network

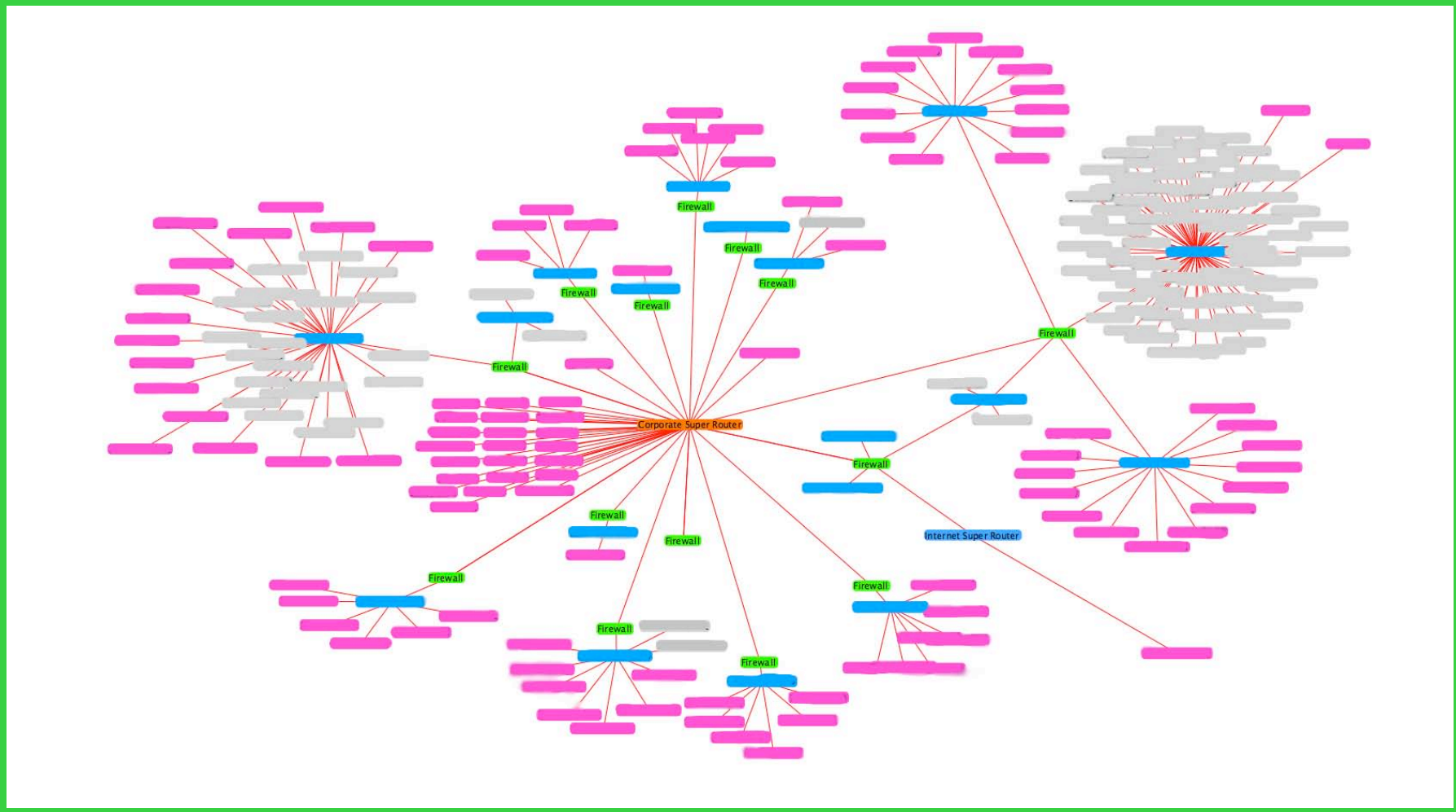

Corporate Network/Internet
DMZ
Control Network
Real Time Data and Control
Direct Connectivity
via Point to Point links
ACG (VPN Transport)
Substations and
Generation
RRO and BA's
Only VPN
Tunneled traffic
allowed to
traverse into
Control Network


Corporate Network/Internet
DMZ
Substations and Generation
Control Network
RRO and BA's

The Control Network

- The control network is complex organism
- It feeds on data in real time and provides situational awareness to system operators
- Protection of these systems requires balls

Soft Chewy Inside



Scary Shit you probably already know

- Given that we have access to the inside, other more useful tools can be used to gather much more interesting data about the insiders network

- Tools such as ettercap can interject themselves as a man in the middle and allow for traces of network traffic from a higher value target, such as the gateway IP address of the ethernet segment the insider is connected to

- http://ettercap.sourceforge.net/

  - From their own description:
  - Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks.
    It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis.

What can you do?

- IPSEC
- VPN tunnel protected traffic across the corporate network (firewall to firewall VPN)
- Encryption inside the application (Digital signing of data)
- Watch layer 2 for spoofing attempts at the switch
  - Duplicate packets on the network
  - Arp firewall technology in the switch
  - Duplicate IP addresses on different ports

Lock it down

- Default to only allowing **outbound** connections (i.e., only allow traffic to be initiated from the control network outbound to a DMZ)
- Outbound connectivity should only allow for sending data (i.e., PI, eDNA, SQL, etc)
- Outbound connectivity should only be configured to specific destination IPs
- Consider using data diodes

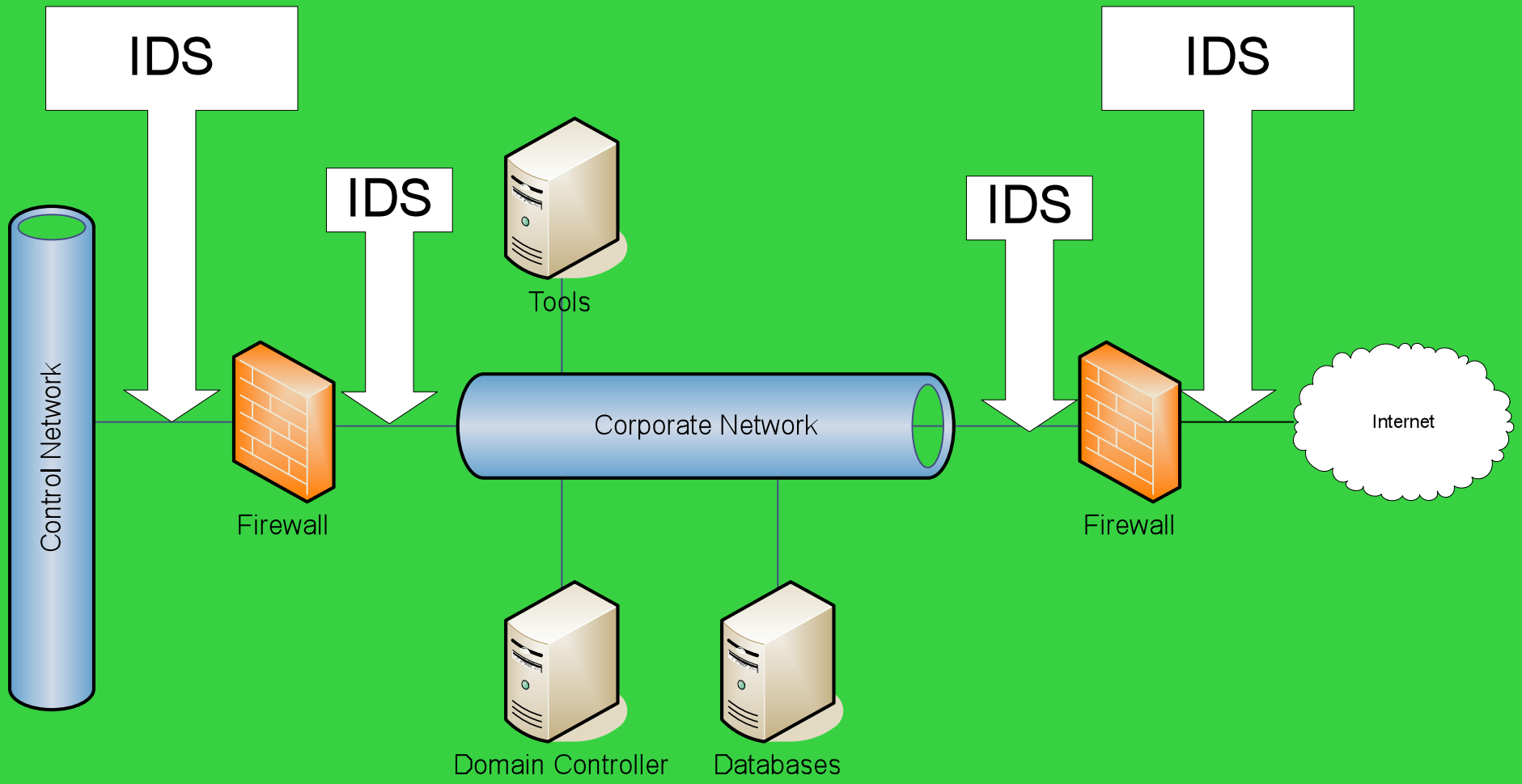
Limit Exposure

- Require two-factor authentication for any and all connectivity to or across the firewall.
- Limit inbound access to specific source IPs and specific destinations (on a DMZ if possible)
- Limit inbound access to very specific ports
  - For remote support, that should be limited to things like RDP, SSH, etc

Keep an eye out

- Ensure proper logging is established
  - **All critical systems within the control network**
  - **Border devices such as the firewalls**
- Best option is a centralized log management solution where automated reporting and alerting can be configured
- Deploy an IDS or IPS

Intrusion Detection Systems



We are not even halfway there

- Simply allowing access is only the beginning
- Processes for approving and documenting all access need to be established
- Continued diligence includes:
  - Regular Vulnerability Assessments
  - Monitoring of log files
  - Ongoing access account reviews
  - Work with vendors

What is coming?

- The next generation of communications will need to address many concerns.

- These concerns include:
  - Multiple business operations needing access to historical information
  - The need for real time information
  - Regulatory issues

The future

- Protocols and processes developed will need to consider the granular accounting practices called for in compliance regulations
- The need for real time information needs to be taken into account
- New technologies will have to work in remote areas and under severe industrial and environmental conditions

What can you do to protect your crown jewels

- Work to understand your control system and its normal operation
  - Take Baselines
  - Operator Testing
  - Perform advanced security research on your systems
  - Utilize all defense in depth you can put to bear to protect your network

- “Nedd’ lang schnagge, Kopp’ in Nagge”

- Thanks for giving me some of your valuable time . . .