

# Securing the Internet Gateway and Business Applications

Patrick C Miller, CISSP SSCP IAM TCP

Andrew Garner, CCSI CCSE+ CCNA ACIA ACSE PCE

CBI Conference – Chicago, IL

May 17<sup>th</sup>, 2004



## **Information Security**

is a dynamic, constantly evolving, living system.

Breakwater keeps ahead of the curve and anticipates threats to provide clients with highly responsive protection.



# Presentation Overview

- **Breakwater Profile**

Why Breakwater?

- **Perimeter**

Secure your Network Edge

- **Secure Network (DMZ)**

Secure Your Public Presence

- **Internal Server Network**

Keep Intellectual Property Available, Yet Secure

- **Internal User Network**

The Most Volatile Network Area



# Presentation Format...

- **Two presenters – multithreaded**
- **Four parts – not necessarily divided equally**
- **Communicate personal experience**
- **Feel free to ask questions...**



# Breakwater Security Associates

*Information Security and Risk Management Services Firm since 1996.*

## **A few of the things we do...**

- **Security Program Development**
  - Risk, Security and Vulnerability Assessments
  - Regulatory Compliance Gap Analysis
  - Policy Development and Auditing
  - Security Strategy
- **Managed Security Services**
  - Device Management
  - Event Correlation (Security Risk Management)
  - Device and Software Health Monitoring
- **Training/Education**
- **Integration**



# Breakwater Product Mindset

## Breakwater's Product Philosophy

Breakwater prides itself on being product agnostic. We pride ourselves on independently evaluating new and existing technologies and forming our own opinions on the benefit of each in our clients' environments. This way we can effectively stay at the cutting edge of new security products in the industry.



# Section One (1/4)

## **The Perimeter: Secure Your Network Edge**



# The Current Situation...

- Corporate Accountability and Fraud
  - Enron, WorldCom, etc...
  - Id Fraud
- Weak Economy
  - Fewer jobs overall
  - Pink slips = increased workload, frustration and disgruntled employees
- Technology Shift
  - Automation (Process Control Systems); doing more with less
  - Ever-increasing complexity and power
- e-Business
  - Need for access to internal applications and data
  - Not all business units are ready for this; classification nightmare
- Terrorism
  - Can they use our people, processes, or technology against us?
- Lack of Expertise and Experience
  - Talent is scarce and “snake oil” is common



# Energy Security Basics

- Layered Security
  - Defense in depth
  - Data Classification and “Least Privileged” Model
  - The most sensitive data is behind several layers
  - Never allow crossing more than one security zone
- Access & Audit Controls
  - “Deny all policy” vs. “Allow all”
  - Authorization comes from system & data owners only
  - A formal authorization process must exist and be based on a “need to know” model
  - Audit controls must be automated and correlated
  - Audit controls should exist between all security zones
  - The longer an event goes unnoticed the more impact it will have



## Trends in the Security Product Marketplace

### Over the past 24 months we have seen some specific trends in Security products

1. Many devices/software packages are coming with well developed user interfaces for ease of management. Products of note (Netscreen, Pix, Checkpoint, PGP, and many others)
2. Many pre-existing mature software packages are being placed on pre-hardened Linux appliances with the above mentioned user interfaces
3. Products are continuing to become fully aware of application layer traffic. It is no longer good enough for a firewall to just filter on ports, all enterprise-level firewalls can now do at least initial application filtering.



# Securing your Perimeter

## Firewalls

What is a Firewall?

- A Firewall is a special host/device used to control access from zones with different security priorities
- Trivia: Where did the term Firewall originate?



# Securing your Perimeter Cont.

## Types of Firewalls

- Firewall “Appliances” = a dedicated firewall enforcement point
- Device Firewalls
  - Enterprise Firewalls
  - Personal home devices
- Software Firewalls
  - Enterprise Software Firewalls
  - Personal Firewall Agents
  - Application Firewalls



# Securing your Perimeter Cont.

## Enterprise Device Firewalls

Powerhouses in the industry: Netscreen, Cisco

### Netscreen

Recently acquired by Juniper networks

- Primary Firewall Products
  - Netscreen Firewall models: 25/50, 204/208, 500, 2000, 5200/5400

### Cisco

One of the most well known players in both the network and security market

- Primary Firewall Products
  - Cisco Pix models: 515, 525, 535
  - Cisco Firewall Blade - high-end blade that inserts into Catalyst hardware
  - Cisco Firewall Feature set for IOS Routers



# Securing your Perimeter Cont.

## Enterprise Device Firewalls Pros and Cons

### Juniper/Netscreen

- Pros: Application Layer Filtering; Great Performance (ASIC based); Runs on firmware written specifically for firewall filtering (no OS overhead)
- Cons: Poor logging system (syslog); minimal tools for troubleshooting; additional software license/product/hardware needed for multiple site management (NSM) java based and requires specific front-end that needs to be installed on client machines and the server portion comes on its own hardened Linux distro

### Cisco Pix

- Pros: Application layer filtering via IDS signatures ported to the system; Good Performance, Runs on pre-hardened proprietary (Linux) operating system
- Cons: Cisco Works VMS providing enterprise logging is available to solve the poor local logging (syslog) issues but requires a additional license/hardware/software and requires specific browser and java versions; minimal tools for troubleshooting; additional software license/product/hardware needed for multiple site management



# Securing your Perimeter Cont.

## Enterprise Software Firewalls

Powerhouse of the Industry: Check Point VPN-1/FW-1

Checkpoint Firewall-1 has long been the *de facto* standard and industry leader for enterprise firewall installation

Pros: Superior Log viewer, Superior management; Excellent Application Awareness; Out-of-the box Internet load balancing capability (only on Linux and SecurePlatform); Out-of-the box capability for managing multiple “Enforcement Points”

Cons: Expensive, Licensing is too complex, need of installation on an OS platforms (which is considered a strength to some), administration is complex due to large feature-set (also considered a strength to some)



# Securing your Perimeter Cont.

## Small Office/Home Devices Personal Firewall Agents

Some leading edge technology is coming from:

1. Juniper (Netscreen)
2. Checkpoint
3. Cisco
4. Personal Firewall Agents - Sybase, Cisco, Zone Labs (now owned by Check Point), ISS



# Securing your Perimeter Cont.

## Web Application Firewalls

**Web Application firewalls are software packages designed to specifically monitor the security of mission critical web applications and protect them specifically from cloaked threats across allowed ports**

Leading Technology Vendors:

1. Sanctum
2. Teros
3. eEye
4. Cisco CSA



# Enterprise Firewall Policy

## For hardware firewalls...

- Require minimal administrative access (3)
- Require an approval process for rule changes
- Require all rule changes to be documented
- Require all configurations to be documented
- Require secure logging mechanism
- Require extensive auditing/logging
- Require strong administrative password
- Require escrow of administrative password
- Require immediate password change for termination of administrative personnel
- Require password change every 90 days (max)
- Require a default “deny all” policy



# Enterprise Firewall Policy Cont.

## For hardware firewalls...

- Require minimal administrative access (3)
- Require an approval process for rule changes
- Require all rule changes to be documented

**These standards are not just for hardware firewalls, but for all external-facing network devices and systems such as load balancers, switches, VPNs, etc...**

- Require escrow of administrative password
- Require immediate password change for termination of administrative personnel
- Require password change every 90 days (max)
- Require a default “deny all” policy



# Enterprise Firewall Policy Cont.

## **For software/personal firewalls (if used)...**

- Require a default “deny all” ingress policy for all public and non-corporate IP addresses
- Require “allow” necessary corporate systems
- Require enablement when on non-corporate networks such as Internet, hotel, home, etc.
- Require minimal user interaction, zero is best
- Remove user interface, or any components that require the user to make security choices
- Enforce policy from a central solution, if possible



# Perimeter Security Management

**The real key is to be reactive - *and* proactive**

- Minimize the “Ostrich Factor”
  - IDS, log surfing/parsing, event correlation, etc
  - Alerting is key (incident response follows...)
- Minimize the “Not Me Factor”
  - Accountability, Least Privilege, Separation of Duties
- Subscription to **all** vendor notification lists
- Keep a steady pace on the “patch treadmill”
- Direct contact with vendor technical staff
- Provide appropriate training and education
- Conferences and seminars; talk to peers



## Section Two (2/4)

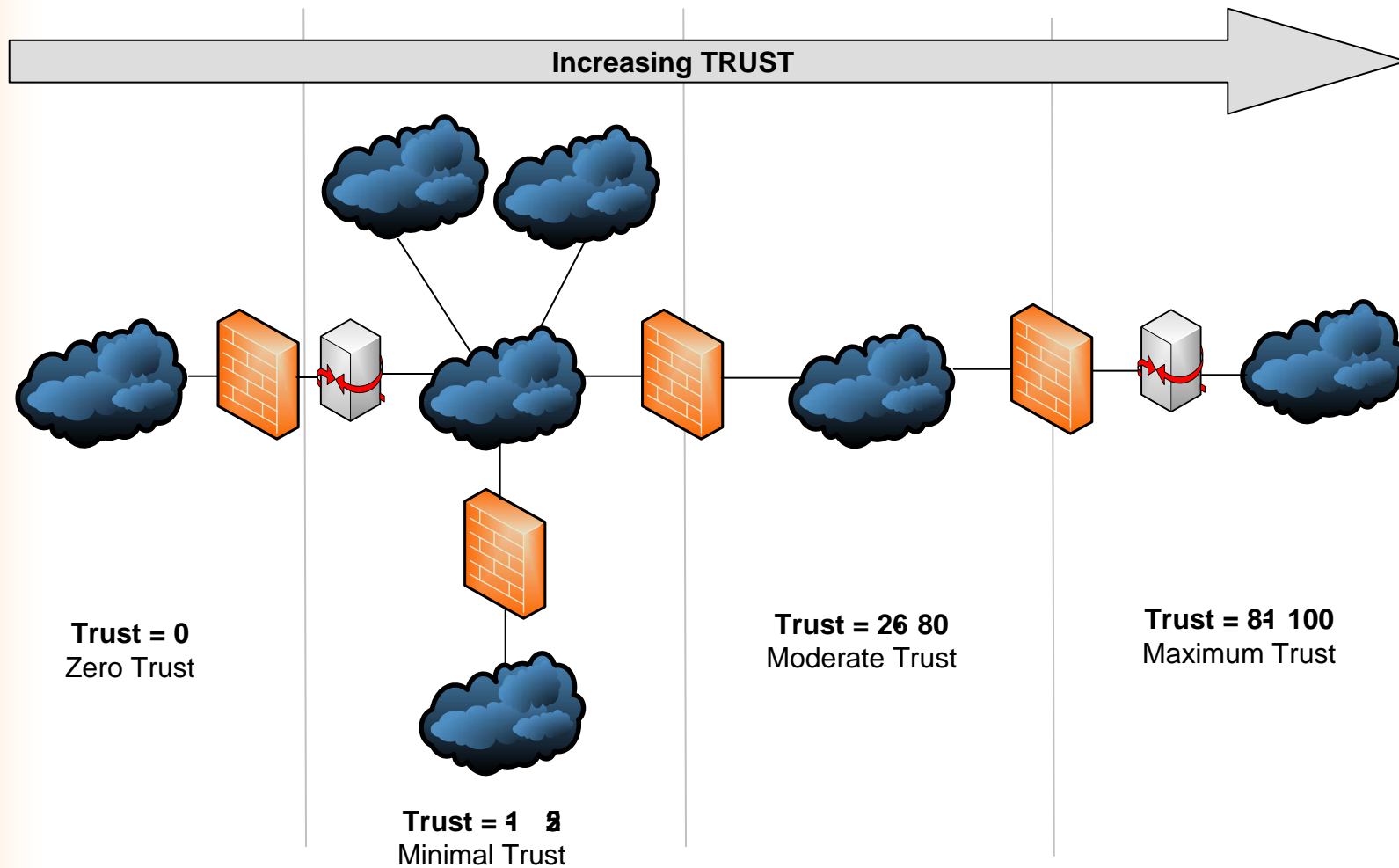
# The DMZ: Secure Your Public Presence



# Energy Security Solutions

- Customer Applications are driving many organizations to allow public access to internal applications and/or data
  - In most cases the business units and their data are not classified, segmented or internally controlled
  - If one business unit is compromised it is usually an easy transition to the entire infrastructure
- In order to reduce the external threat, create an n-tiered portal
  - Old idea... common to all big ecommerce environments
  - Migrate all "e-Apps" into public portal
  - Migrate user and vendor remote access to corporate portal
- Be sure to use appropriate controls between the portal and the internal network
  - Secure application development is essential
  - Two-Factor credentials
  - Rigorous patch and configuration management

# Trust Level Architecture Model

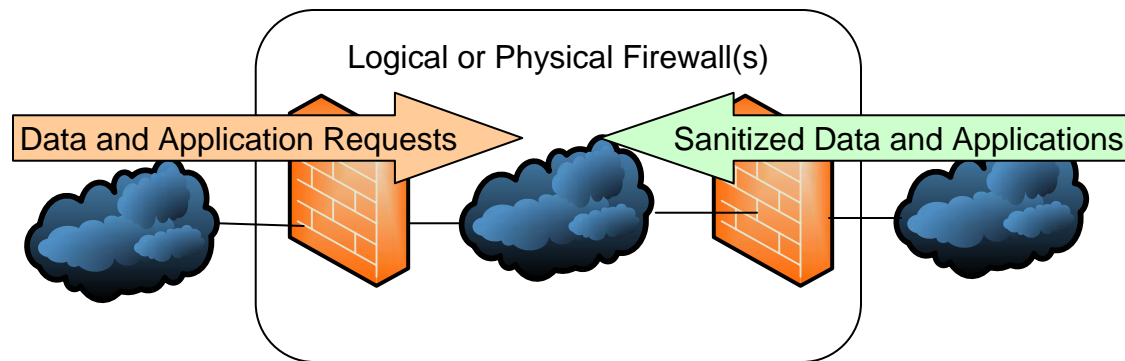




## Trust Level Model Cont.

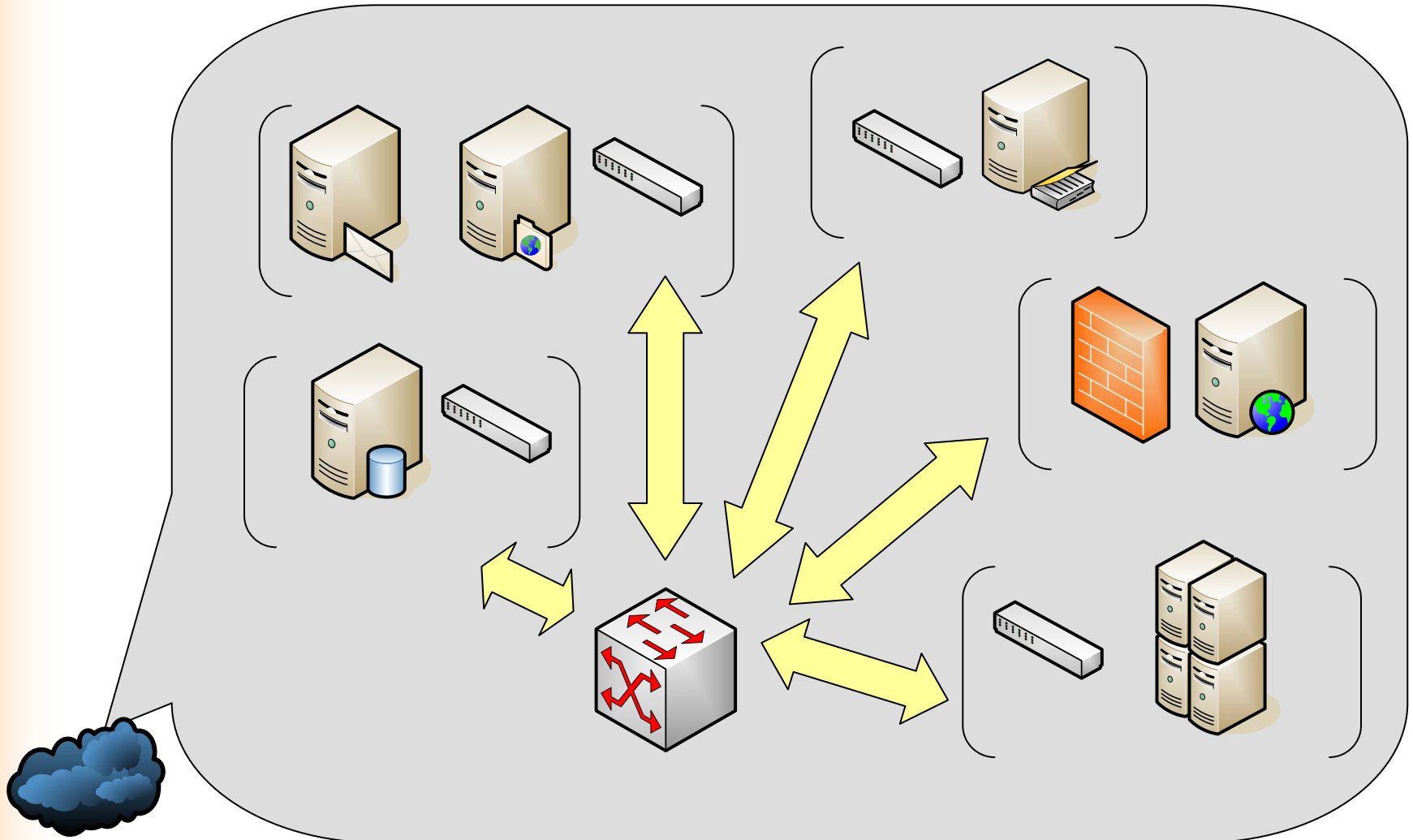
- Establish policy requiring adherence
- Classify all systems and data based on trust
- Document trust level for all systems and data
- “Certify” and allow applications, systems and data based on level of trust
- Restrict remote access based on trust level
- Design authentication and authorization requirements based on trust level
- Design patching requirements based on trust
- Periodically test systems for compliance

# De-Militarized Zone (DMZ)



- Essentially, an area between two firewalls (logical or physical) designed to serve data and applications from a network of a higher trust level to a network of a lower trust level
- There should be no ingress from the DMZ into the private network – only allow appropriate data to be “pushed” from the private network to the DMZ

# De-Militarized Zone (DMZ) Cont.





# De-Militarized Zone (DMZ) Cont.

Question: What technology do you deploy to effectively tighten down the Security in DMZ environment?

Answer:

1. Intrusion Detection Technology (IDS) or Intrusion Detection and Prevention (IDP)
2. Web Application Firewalls that we discussed earlier
3. Threat Correlation Technology to observe new threats as they appear on your DMZ network
4. Employing stringent Virus Checking with aggressive updates
5. Firewall Technology employing a additional layer of security above statefull packet filtering
6. Encryption Technology utilizing Virtual Private Networking (VPN) and Email encryption
7. Host Security Agents (Discussed in the next section)



# De-Militarized Zone (DMZ) Cont.

## IDS/IDP Technology

IDS/IDP Technology is a technology that is installed either on a network sensor in the case of network ids (NIDS) or installed directly on the host to be monitored in the case of host ids (HIDS) This software will “listen” for threat signatures in your environment and produce alerts if it finds any matches, or in the case of IDP technology either actually drop the malicious traffic or work inline with your firewalls or routers to drop the malicious traffic.

What should you be looking for IDS/IDP technology?

1. Integration into your current environment (if using HIDS do they support all of your platforms?)
2. Ease of management and signature updates
3. Mature Monitoring Interface
4. How often are signature updates released, what's the mean time after a new attack hits that you can expect a update?
5. Mature Reporting capabilities



# De-Militarized Zone (DMZ) Cont.

## IDS/IDP Technology Leaders

1. Cisco: IDS sensor, Router, Host, Catalysts Module, Coupled with Cisco Works VPN/Security Management Solution (VMS)
2. Juniper: Netscreen IDP
3. NFR Sentivist
4. Network Associates: Intrushield Appliances and Manager
5. Sourcefire: Network Sensor and Management Console
6. Symantec: ManHunt (NIDS) Intruder Alerts (HIDS)
7. Airdefense: Airdefense 4.0 (Wi-fi IDS system)



# De-Militarized Zone (DMZ) Cont.

## Threat Correlation Technology

Threat Correlation Technology is a system designed to receive log output from multiple sources and correlate threat based on impact to your environment. This type of technology can be used to tighten security in every area of your network, but is particularly useful in the partially trust scenario of the DMZ.

What Should you be looking for:

1. Mature Monitoring interface
2. Support for a large amount of devices and Operating Systems
3. Ease of Management and threat correlation signatures
4. Mature Logging/Reporting capabilities



# De-Militarized Zone (DMZ) Cont.

## Threat Correlation Providers:

1. ArcSight
2. NetIQ: Security Manager
3. OpenService: Security Threat Manager



# De-Militarized Zone (DMZ) Cont.

## Anti-Virus Technology

Anti-virus technology is defined as a system that prevents infection and spread of malicious code throughout your environment. It usually comes in two different flavors: gateway and local agents. The gateway in this sense is a server specifically scanning incoming or outgoing content for malware and the local agent is a piece of software running locally monitoring for infection by periodically scanning the files on the local hard drive.

What should you be looking for in AV technology?

1. Ease of Management
2. Ease of use for signature updating (specifically auto-updating)
3. Multiple Platform Support (if needed)
4. How often are signature updates released, what's the mean time after a new virus hits that you can expect a update?
5. Heuristics vs. patterns/definitions



# De-Militarized Zone (DMZ) Cont.

## Anti-Virus Technology Providers

1. Trend Micro: PC-Cillin (host), VirusWall (gateway), ScanMail (Exchange, Lotus Notes), InterScan Suite
2. Symantec: AntiVirus Gateway, AntiVirus Corporate
3. Sophos: Anti-virus (local agent and gateway product), PureMessage (Spam and Antivirus combo), MailMonitor(Exchange, Lotus)
4. Network Associates: Webshield, VirusScan



# De-Militarized Zone (DMZ) Cont.

## Encryption Technology

Encryption technology is at use securing site-to-site access and remote user access using Virtual Private Networking (VPN). This technology is factored into every market-leading firewall technology and is also used in many stand-alone device or software installs. Most of the new technology in this space has been devoted to SSL VPN devices/software. Encryption is also used in Email communication and Secure Data Storage.



# De-Militarized Zone (DMZ) Cont.

## Encryption Technology, Continued

Some example VPN Products:

- Cisco: VPN concentrator, Router based, Catalyst VPN module, Pix
- Checkpoint: VPN-1
- Juniper: Netscreen Firewalls, Neoteris

Some example Email/Data encryption Products:

- PGP: PGP Universal, PGP Corporate
- Entrust: Entrust Entelligence
- RSA Keon



# De-Militarized Zone (DMZ) Cont.

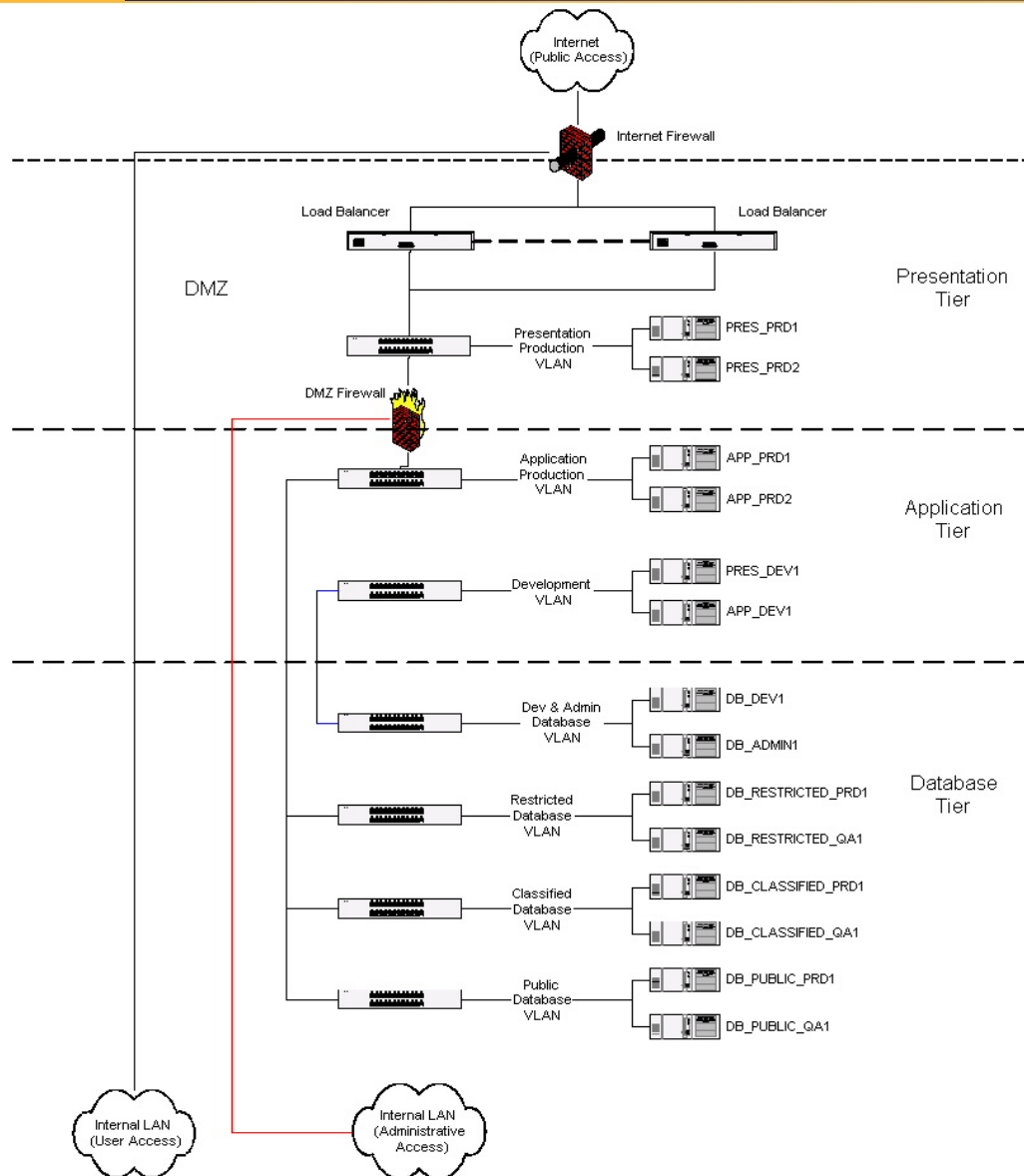
## Additional Firewall Protection

Many enterprise firewalls employ mechanisms to provide an additional layer of protection for DMZ servers. They achieve this by utilizing proxy server technology to add an additional layer of security to the sensitive services passing through the DMZ.

Examples of this technology at work:

1. Cisco Pix Fixup Protocols
2. Check Point Security Server
3. Specific Web Application Firewalls mentioned earlier

# General *n*-Tier Architecture DMZ



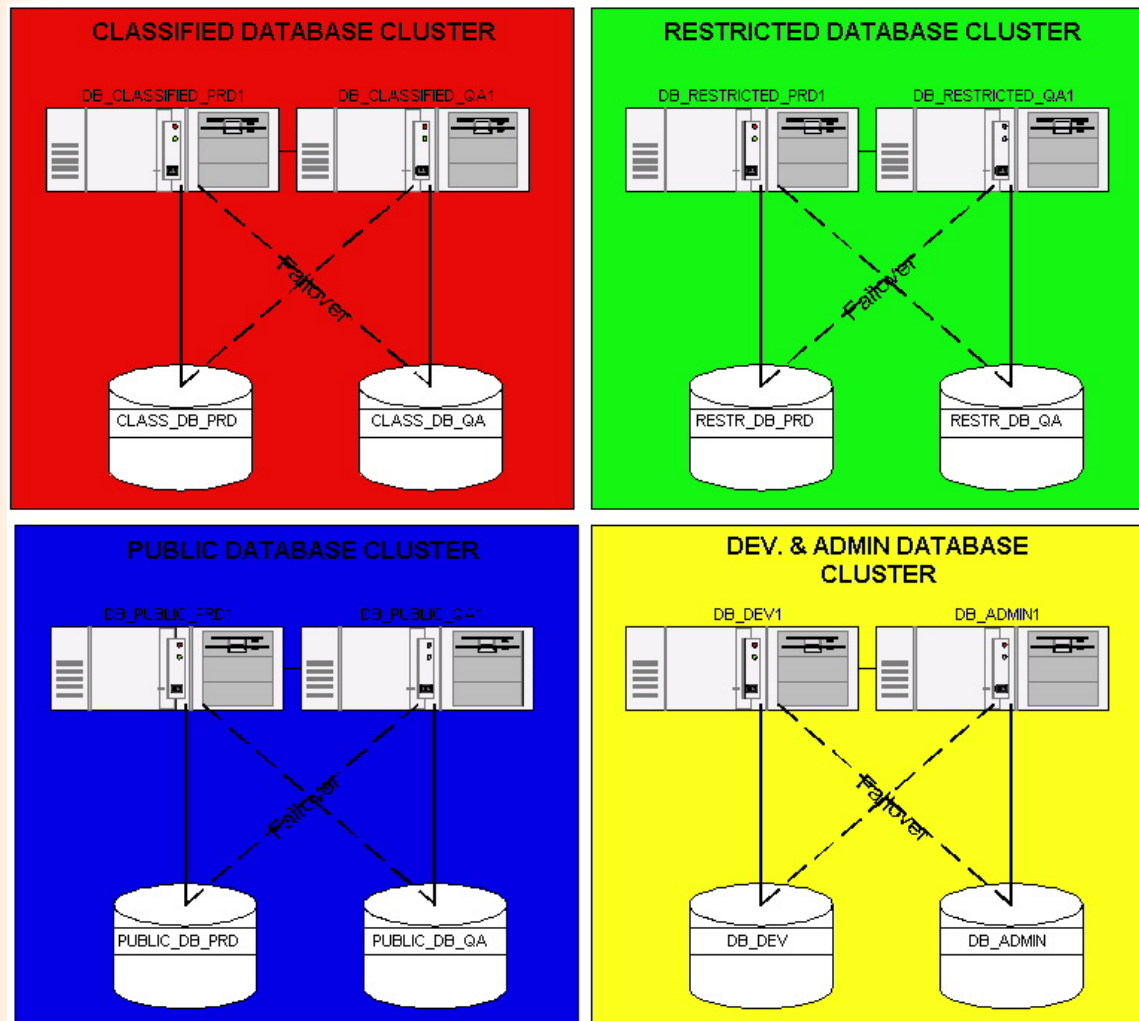
The *n* Tier Architecture is made up of the following layers:

- External Public Interface
  - Presentation Tier
  - Application Tier
  - Database Tier
- Support/Admin Tier

*Insert additional layers if appropriate/necessary...*

*Establish Trust Levels for each layer...*

# DMZ Database Model



- Classify
- Sanitize
- Audit
- Encrypt
- Hash



# Secure Builds

## **Secure builds assure system integrity and consistency**

- Establish and document Secure Build baseline procedures for all servers
- Provide appropriate training and education for necessary skills to perform secure build
- Obtain signature of server administrator(s) who build all systems to provide accountability
- Enforce principle of least privilege
- Research “known good” models (NSA, NIST)
- Establish checklist with evidence for decisions



# DMZ Email Servers

- Rigorous patching
- Rigorous change control
- No relaying
- Strong virus scanning
- Content filtering (spam control)
- Extra-hardened servers; secure builds
- Frequent vulnerability scans
- Regular and frequent backups
- Email has become a critical application (always-on requirement), so plan for appropriate protection and availability...



# DMZ FTP Servers

- Rigorous patching
- Rigorous change control
- Strict upload/download controls
  - Size, number, IP, etc.
- Strong virus scanning
- Extra-hardened servers; secure builds
- Verbose auditing
- Frequent vulnerability scans
- Many critical file transfers happen via ftp processes, so ensure you have the necessary availability to provide always-on coverage...



# DMZ Web Servers

- Rigorous patching
- Rigorous change control
- No Web Administration on external interface
- Strong logging and log surfing/parsing
- URL filtering (URL Scan for IIS)
- Extra-hardened servers; secure builds
- Frequent vulnerability scans
- Regular and frequent backups
- The web presence is vital to the public image of the organization, so plan for appropriate protection and availability...



# DMZ Application Servers

- Rigorous patching
- Rigorous change control
- No Web Administration on external interface
- Strong logging and log surfing/parsing
- Input filtering/validation
- Extra-hardened servers; secure builds
- Frequent vulnerability scans
- Regular and frequent backups
- The web applications are often the business and/or productivity portals, so plan for appropriate protection and availability...



# DMZ Database Servers

- Rigorous patching
- Rigorous change control
- No Web Administration on external interface
- Strong logging and log surfing/parsing
- Extra-hardened servers; secure builds
- Frequent vulnerability scans
- Regular and frequent backups
- Powerful hardware
- The database supports the application and is vital to the overall web presence...



# DMZ Domain/Directory Servers

- Rigorous patching
- Rigorous change control
- Extra-hardened servers; secure build
- Periodic vulnerability scans
- Regular and frequent backups
- Powerful hardware
- Distribute controllers to spread load and speed login response time
- The domain/directory supports all authentication and authorization to resources for the organization, with always-on status



# Secure Code Is Vital

- Secure code starts with a Software Development Life Cycle (SDLC) or similar
- Train and educate developers on secure coding practices
- Ensure appropriate **input validation**
- Ensure appropriate separation of duties
- Ensure principal of least privilege
- Encrypt credentials – ***always***
- Ensure user accountability and non-repudiation
- Choose vendors with the most secure code



# Repeatable Architecture

**Not just for Internet connections anymore...**

- The DMZ model can be used
  - Between the corporate network and the process control network(s)
  - Between the corporate network and business partner network(s)
  - Between the corporate network and financial or other critical systems
  - Anywhere you would place a firewall



## Section Three (3/4)

# The Internal Servers: Secure Your Intellectual Property



# Internal Server Network

- Moderate increase in trust level
- Data classification is essential
- Network segmentation is still required
- Enforce RFC 1918 addressing model
- Establish a specific range for server IPs
- Remove all unnecessary services
- Maintain strict controls on all network devices blocking all unnecessary ports



# Internal Server Network

## Internal Server Technology

There are many “seamless” types of technology at work on the internal server network, some of these are:

1. Host based IDS/Network based IDS (discussed earlier)
2. Threat Correlation Agents (discussed earlier)
3. Local Anti-Viral Agents (discussed earlier)
4. Encryption Technology (discussed earlier)
5. Host Security Agents
6. Internal “bridging” Firewalls or IDP



# Internal Server Network

## Host Security Agents “Endpoint”

A Host security agent is a software package installed on a host that acts as a combination Host Firewall and IDS depending on the product.

Some of the new technology in this space has the capability of effectively quarantining known infected portions of your network and also provides great central management functionality for monitoring and reporting.

### Technology Providers:

1. Cisco: Cisco Secure Agent (CSA)
2. Zone Labs (Checkpoint): ZoneAlarm Pro
3. Sygate: Sygate Security Agent



# Internal Server Network

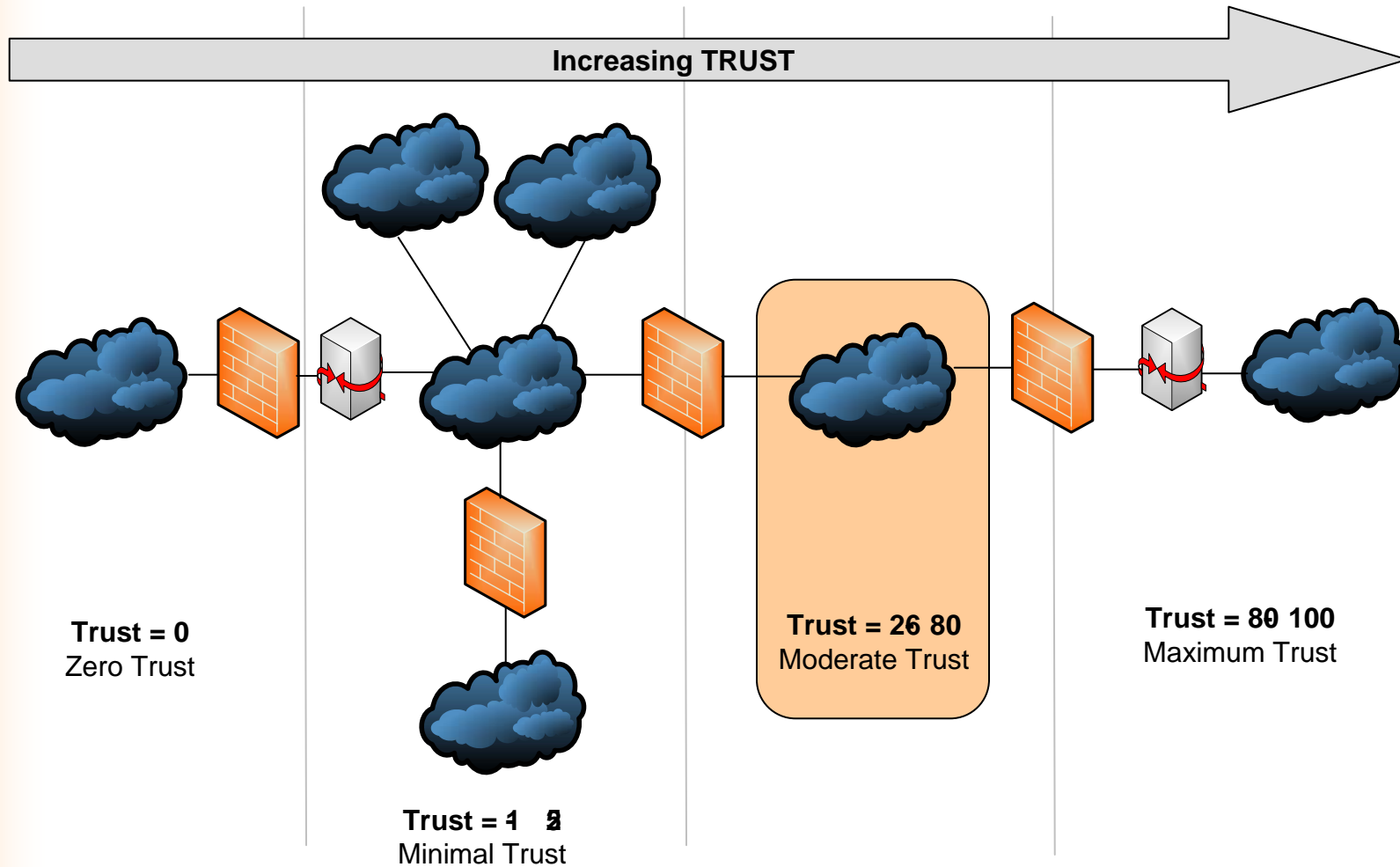
## Internal “Bridging” Firewalls or IDP

Internal firewalls/IDP are a relatively new concept, these systems are set up in bridging mode so as to not affect your current network architecture. They provide protection for multiple internal networks based on both protocol control and application awareness.

### Technology Providers:

1. Juniper IDP
2. Checkpoint Interspect

# Trust Level Architecture Model





# Data Classification...

- It is paramount that you **classify all data**
  - Restricted, Confidential, Public, etc...
  - Choose your own terms, but stay within the lexicon
- What are your criteria?
  - High risk, Medium risk, Low risk
  - Be very careful and selective
- Consider the business impact vs. the likelihood of the event when determining risk
- Do not assign High risk rankings often, they can be **very** expensive



# Sample CIA/Risk Matrix

	High Risk	Medium Risk	Low Risk
Confidentiality	<p>Catastrophic loss of reputation</p> <p>Catastrophic loss of public confidence</p>	<p>Moderate loss of reputation</p> <p>Lawsuit as a result of a breach in confidentiality</p> <p>Moderate erosion of public confidence</p>	<p>Minor loss of reputation</p> <p>Minor erosion of public opinion</p> <p>Loss of morale</p>
Integrity	<p>Loss of life or serious consequences</p> <p>Loss of critical data</p> <p>Errors in information potentially resulting in catastrophic damage to public health or safety</p> <p>Substantial economic loss &gt; 5% of Gross Revenue</p>	<p>Loss of sensitive information</p> <p>Material economic loss between 1% &amp; 5% of Gross Revenue</p>	<p>Errors in information resulting in service disruption</p> <p>Material economic loss less than 1% of Gross Revenue</p>
Availability	<p>Loss of life or serious consequences</p> <p>Catastrophic impact on productivity or ability to provide services</p> <p>Critical Information unavailable for more than 4 hours (up to one day)</p>	<p>Critical Information unavailable between 1 to 5 days</p> <p>Moderate loss to productivity</p>	<p>Critical Information unavailable for more than 5 days</p> <p>Some loss to productivity</p>



# Sample Classification Criteria

- **Public** – Information that if the confidentiality, integrity or availability of the data were altered would cause *low to no* business impact based on the criticality criteria established
- **Confidential** – Information that if the confidentiality, integrity or availability of the data were altered would cause *medium* business impact based on the criticality criteria established
- **Restricted** – Information that if the confidentiality, integrity or availability of the data were altered would cause *high* business impact based on the criticality criteria established



# Sample Asset Criticality Matrix

Information Asset	Confidentiality	Integrity	Availability	Classification
Hydro Flow	L	M	L	Public ( <i>Low</i> )
Permits/Contracts	M	H	M	Confidential ( <i>Medium</i> )
Billing	H	H	M	Restricted ( <i>High</i> )
Process Control Data	M	H	H	Restricted ( <i>High</i> )



# Network Segmentation

- Apply appropriate trust levels to different IP segments of the server environment
  - Log traffic crossing trust boundaries; parse traffic for correlation
  - Use realistic trust levels, it can get expensive
  - document everything
- Use different segments for different platforms
  - Financial, domain/directory, database, web/ftp, file, print, backup, etc.
  - For more granularity, break it up by Operating System
- Employ ACLs or VLANs on network devices to restrict access to only known approved service/application ports
  - Only allow appropriate traffic between segments
  - Audit access to banned ports
- Adhere to RFC 1918 model
  - Do not use public addresses in the private (corporate) space
  - Choose an appropriate range (class A or B, most likely)



# Remove Unnecessary Services

- Understand exactly which services are required for functionality and run only those
- At a minimum, remove...
  - Echo (7)
  - QOTD (17)
  - Chargen (19)
  - TFTP (69)
  - Finger (79)
  - RPC
  - Messenger
- Communicate with vendors for product details
- Use Xinetd on Unix systems to restrict open ports



# Replace Unsecure Services

- Replace SSL with TLS
- Replace Telnet and RLOGIN with SSH (v2)
- Replace FTP with SFTP or SCP
- Replace VNC or pcAnywhere with Microsoft Terminal Services over VPN (or SSH in the \*ix-based environment)
- Replace LDAP with SLDAP
- Replace LEAP (or lesser) wireless authentication with Fast-EAP
- Replace SNMPv2 with SNMPv3
- Ensure that OWA has two-factor authentication



# Internal Application Servers

- Moderate patch management requirement
- Rigorous change control
- Moderately hardened servers; secure build
- Verbose security auditing
- Regular and frequent backups
- Periodic vulnerability scans
- Powerful hardware
- The applications are often necessary for business and/or productivity, so plan for appropriate protection and availability



# Internal Database Servers

- Moderate patching, with the exception of financial systems which should be patched at a higher frequency
- Rigorous change control
- Moderately hardened servers; secure build
- Verbose security auditing
- Regular and frequent backups
- Periodic vulnerability scans
- Powerful hardware
- The databases support the applications and are vital to the overall corporate functionality



# Internal Domain/Directory Servers

- Rigorous patching
- Rigorous change control
- Extra-hardened servers; secure build
- Verbose security auditing
- Periodic vulnerability scans
- Regular and frequent backups
- Powerful hardware
- Distribute controllers to spread load and speed login response time
- The domain/directory supports all authentication and authorization to resources for the organization, with always-on status



## Section Four (4/4)

# **The Internal Users: Secure Your User-base**



# Internal Users (Workstations)

- Moderate *decrease* in trust level
- Network segmentation is still required
- Enforce RFC 1918 addressing model
- Establish a specific range for workstation IPs
- Remove all unnecessary software
- Adhere to strict secure build practices
- Maintain strict controls on all network devices blocking all unnecessary ports
- Don't rule out Citrix, WYSE, etc



# Workstation Hardening

- Strong authentication
- Screensaver password lock (where appropriate)
- Enable security auditing locally
- Use Internet Explorer Administrator Kit and other tools to lock down the browser
- Force users to go through a web-proxy
- Remove local administrator privilege
- Do not allow unsigned driver installation
- Disable any on-board wireless in BIOS
- Host Security agents (discussed earlier)



# Workstation Protection

- Anti-virus
  - Always enabled
  - Automatically updated (within 4 hours of pattern/definition file release from vendor)
- Personal Firewall
- Host-based Intrusion Detection
- Strong authentication
  - SecurID
  - Biometric
  - Digital Certificate
- Hard drive encryption (specific products mentioned earlier)
- Physical cable lock for laptops



# Network Segmentation

- Establish separate IP segments for the following workstation environments
  - Executives
  - General Users
  - Traders
  - Developers
  - IT support staff
  - PCS staff
  - PCS IT support staff
- Allow restricted egress accordingly
- Apply appropriate trust levels



# Approved Software Policy

- Establish an Approved Software policy prohibiting unapproved software from being loaded on any corporate system
- Publish the list of approved software on the corporate intranet for easy reference
- Provide appropriately licensed and approved software on a central server
  - Restrict and log access to this system
- Explicitly ban access to specific software
  - Instant Messenger, IRC, Filesharing, etc



# Security Awareness Training

Typically one of the last things addressed by management, but could, arguably, be one of the most important.

- Users are on frontline of corporate security
- Should be considered experts in their job so they should know what is normal and what is anomalous in their environment
- Need to be trained on “thinking security”
- Should be encouraged to report unusual behavior, without fear of penalty
- Should be rewarded when they succeed in demonstrating security awareness – make it noisy so everyone knows their success (this encourages compliance)
- Training should occur on regular basis via various methods – email, CBTs, posters, formal and informal training. Don’t just do once and forget
- Don’t forget non-technical training – Social Engineering is still most successful form of information gathering



# Where to go from here?

**There are many security products out there but without the proper policy and controls wrapped around any new rollout you are fighting a losing battle.**

**We have spoken about many products currently in the security space but remember that there is no magic bullet. Today's modern networks and user populations usually need a combination of the correct products and procedures to secure your environment properly.**

**The policy set forth by management is the most important step in providing direction on just what products you should be evaluating. Senior level management buy-in is absolutely paramount...**



# Useful Links...

## Secure Build Documents

- <http://csrc.nist.gov/publications/nistpubs/index.html>
- <http://www.nsa.gov/research/resea00003.cfm>
- <http://nsa1.www.conxion.com/>

## NERC 1200 Urgent Action Cyber Security Standard (NERC 1200 UAS)

- [http://www.esisac.com/library\\_guidelines.htm](http://www.esisac.com/library_guidelines.htm)
- <http://www.nerc.com>
- <http://www.breakwatersecurity.com/energyandutility/>

## The Department of Homeland Security

- <http://www.nipc.gov/dailyreports/dailyindex.htm>- DHS IAIP Daily Report
- <http://www.dhs.gov/dhspublic/display?theme=10> – Grants from the DHS
- <http://www.dhs.gov/dhspublic/display?theme=13&content=3345> – Organizations within the DHS

## Security News

- <http://news.ists.dartmouth.edu/todaysnews.html>- Security in the news from Dartmouth
- <http://www.securitynewsportal.com>- Security news Portal

## Multi purpose Security Sites

- [www.cert.org](http://www.cert.org)- Center of Internet Security Expertise (great FAQ's, incident response and much more)
- <http://isc.sans.org/>- Internet Storm Center (Live reports of which Ports are being attacked along with the handlers diary)



# Questions?

**Andrew Garner** CCSI CCSE+ CCNA ACIA ACSE PCE  
*Senior Engineer and Instructor*  
agarner@breakwatersecurity.com  
877.952.5500 x157 (desk)  
206-228-5590 (mobile)

**Patrick C Miller** CISSP SSCP IAM TCP  
*Senior Energy Security Advisor*  
energy@breakwatersecurity.com  
503.312.0703 (mobile)