Network Firewall Security

Auditing Firewalls

Module 1: Understanding Firewalls

Firewall Architecture Overview

What is a Firewall?

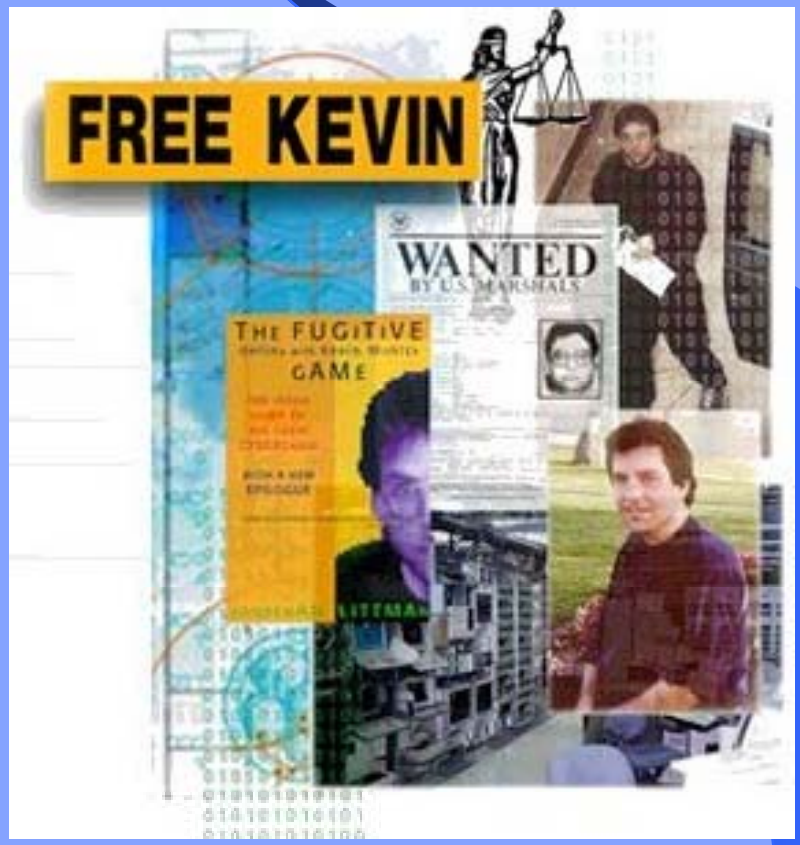
- A firewall is a security policy enforcement point that regulates access between computer networks
- Filters are inherently insecure services
- Controls TCP protocols
  - http, smtp, ftp, telnet etc
- Only one of many different security tool's to control and regulate network traffic

What do Firewalls Protect?

- Data
  - Proprietary corporate information
  - Financial information
  - Sensitive employee or customer data
- Resources
  - Computing resources
  - Time resources
- Reputation
  - Loss of confidence in an organization
  - Intruder uses an organization's network to attack other sites

Who do Firewalls Guard Against?

- Internal Users
- Hackers
- Corporate Espionage
- Terrorists
- Common Thieves



Basic Firewall Components

- Policy
- Advanced authentication
- Packet inspection
- Application gateways

Common Internet Threats

- Denial of service attacks
  - Specific attacks that can cause a server crash
  - Flooding the server with traffic to disrupt or deny service
- Intrusion threats
- Attacks on services/exploits
  - The backend server may not be hardened enough for adequate protection, but the firewall can block external attacks
- Information threats
- “Viral” threats
- Defacement

How Vulnerable are Internet Services?

- E-mail or smtp – Simple Mail Transfer Protocol
  - TCP/IP based port 25 (POP 110)
  - Risks Include
    - E-mail bombing (stalking)
      - Anonymous harassment
      - Large amounts of e-mail to a single user address
    - Spamming
      - Messages sent to numerous different users from a host
    - Virus download mechanism
      - Code Red
      - Nimda
    - Not always traceable
  - POP and IMAP can be very insecure

How Vulnerable are Internet Services?

- FTP - File Transfer Protocol
  - TCP/IP based port 20/21
  - Risks Include
    - Unencrypted authentication and data transfers
      - Usernames and passwords can be”sniffed”
    - Unencrypted data transfers
      - Data can be viewed
    - Often part of default installations
    - Anonymous ftp is possible
    - Privilege escalation

How Vulnerable are Internet Services?

- Telnet
  - TCP/IP based port 23
  - Risks include
    - Unencrypted authentication
    - Unencrypted interactive session
    - Session hijacking
    - Included in default installations
    - Can allow remote root login

How Vulnerable are internet services?

- HTTP – Hypertext Transfer Protocol
  - TCP/IP based port 80
  - Risks Include
    - Browsers can be used to run dangerous commands
    - Protocol can be used between user agents and other protocols i.e.. smtp, nntp, ftp
    - Difficult to secure
    - Remote execution of commands and execution (server side)
    - Non-secure add-on applications
      - Java
      - Cookies
      - soap

How Vulnerable are Internet Services?

- HTTPS – Secure Hypertext Transfer Protocol
  - TCP/IP based port 443
  - Risks Include
    - Browsers can be used to run dangerous commands
    - Remote execution of commands and execution (server side)
    - Becomes a tunnel for any data
    - Can be used to subvert firewall/security controls

How Vulnerable are Internet Services?

- DNS
  - TCP and UDP based ports 53 and 1024
  - Risks include
    - DNS cache poisoning
      - Bad data to redirect valid connections to the wrong server
    - DNS spoofing
      - Bad data to redirect valid connections to the wrong server
    - Absolutely needed for network services

How Vulnerable are Internet Services?

- SNMP – Simple Network Management Protocol
  - UDP based
  - Risk include
    - Unencrypted data transfers
    - Poor authentication through “community relationships”
    - Transfer of highly sensitive data
    - Does use access lists

How Vulnerable are Internet Services?

- NFS – Network File System
  - NFS is a shared file structure
  - Based on a trust model of network machines
    - Certain machines can access shared file systems
  - Risks include
    - No “user”authentication
    - IP Spoofing to gain access
    - Most secure NFS is still very insecure

The“2002 Computer Security Institute /FBI Computer Crime and Security Survey” Reported:

- 90% of survey respondents (primarily larger corporations) detected computer security breaches. Respondents reported a wide range of attacks:
- 44% detected system penetration from the outside
- 44% detected denial of service attacks
- 76% detected employee abuse of Internet access privileges
- 85% detected computer viruses, worms, etc.
- 80% acknowledged financial losses due to computer security breaches
- 44% were willing and/or able to quantify their financial losses (these losses were $455 million).
- Most serious losses occurred through theft of proprietary information and financial fraud.
- 74% cited their Internet connections as a frequent point of attack and 33% cited their internal systems ands frequent point of attack
- 34% reported intrusions to law enforcement (up from only 16% in 1996)

Firewall Architecture Overview

- Basic Firewall Components
  - Software
  - Hardware
  - Purpose Built/Appliance based

Module 1: Understanding Firewalls

Firewall Software Types

Firewall Software Types

- Problems to watch for
  - Administrative limitations
    - Access
    - Monitoring
    - logging
  - Management requirements
    - Additional control points
    - Additional non-secure applications required
  - Software limitations
    - Capacity
    - Availability
    - Hardware

Packet Filtering Firewalls

- Packet filtering is one of the oldest, and one of the most common types of firewall technologies. Packet filters inspect each packet of information individually, examining the source and destination IP addresses and ports. This information is compared to access control rules to decide whether the given packet should be allowed through the firewall.

- Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason they can decide packet flow very quickly.

- Because every packet of every connection is checked against the access control rules, larger, complex rule bases decrease performance. And because packet filters can only check low-level attributes, they are not secure against malicious code hiding in the other layers. Packet filters are often used as a first defense in combination with other firewall technologies, and their most common implementation today is seen in the access control lists of routers at the perimeters of networks.

- For simple protocols or one-sided connections, like ICMP or SNMP traps, it is still useful to use packet filtering technology.

Packet Filtering Firewalls

- Products
  - Cisco Pix
  - Typically routers
- First Generation Firewall Technology
  - Fast but not very flexible
- Can be used as a first line of defense

Application Level Firewalls

- Application level firewalls are the third firewall technology traditionally seen in the market. These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data. To achieve this security proxies, as their name suggests, actually mediate connections. The connection from a client to a server is intercepted by the proxy. If the proxy determines that the connection is allowed, it opens a second connection to the server from itself, on behalf of the original host. The data portion of each packet must be stripped off, examined, rebuilt, and sent again on the second connection.

- This thorough examination and handling of packets means that proxy firewalls are very secure and generally slow. Proxies are also limited as firewalls, because they must understand the application layer. As new protocols are developed, new proxies must be written and implemented to handle them.

Application Level Firewalls

- Web Proxy Severs
- Application Proxy Servers
- Products
  - None that are strictly Proxy based
  - “Gateway Servers”
- Second Generation Firewall Technology
  - Makes connections on behalf of the client
  - Not flexible

Hybrid Firewalls

- Performs Packet Filtering functions
- Performs Application Proxy functions
- Third Generation Firewall Technology
- Products
  - Raptor Firewall by Symantec
  - Firewall 1 by Checkpoint
  - Sidewinder Firewall by Secure Computing
  - Lucent Brick by Lucent

Stateful Inspection ©

- Stateful inspection architecture utilizes a unique, patented INSPECT Engine which enforces the security policy on the gateway on which it resides. The INSPECT Engine looks at all communication layers and extracts only the relevant data, enabling highly efficient operation, support for a large number of protocols and applications, and easy extensibility to new applications and services.

- The INSPECT Engine is programmable using Check Point's powerful INSPECT Language. This provides important system extensibility, allowing Check Point, as well as its technology partners and end-users, to incorporate new applications, services, and protocols, without requiring new software to be loaded. For most new applications, including most custom applications developed by end users, the communication-related behavior of the new application can be incorporated simply by modifying one of Firewall-1's built-in script templates via the graphical user interface. Even the most complex applications can be added quickly and easily via the INSPECT Language.

Stateful Inspection

- New technology incorporating
  - Patented technology
  - INSPECT engine
  - Application Level Proxy
- Products
  - Checkpoint NG (Exclusive)

Multi-Layer Inspection ©

- Multi-layer inspection is a packet and connection verification process developed by Stone soft to ensure maximum security without compromising system throughput. StoneGate's security policies determine when to use stateful connection tracking, packet filtering, or application-level security. The system expends the resources necessary for application-level security only when the situation demands it and without unnecessarily slowing or limiting network traffic.

Multi-Layer Inspection

- New technology incorporating
  - Application proxies
  - State Inspection
  - Packet filtering
- Products
  - StoneGate by Stone soft (exclusive)

Firewall Software Types

- Be sure to understand what your customer is using
  - Know your products
  - Speak to the firewall vendor for insight
  - Compare responses of customer and vendor
  - One firewall type or multiple types

Module 1: Understanding Firewalls

Firewall Hardware Types

Firewall Hardware Types

- Three basic hardware options
  - Appliance based systems
    - Purpose built
    - Simple
    - Highly integrated
  - 3rd Party servers
    - General use systems
    - Additional support channel
    - Greater flexibility
  - Hybrid servers
    - Purpose built for a limited product line
    - Often closely integrated with software offerings
    - May have separate support channel
    - Most have highly integrated components

Firewall Hardware Types

- Appliance based system problems
  - OS and Kernel hardening and security may be done by vendor only
  - Tightly coupled software and hardware may have insecure code unknown to user
    - Hard to inspect or verify
  - All security controls are determine through a single vendor
  - Appliances are used to simplify implementation and support efforts causing some loss of administrative control

Firewall Hardware Types

- 3rd Party server problems
  - OS and Kernel hardening and security must be done by implementation staff
    - Expertise
    - procedures
  - OS software may have many known vulnerabilities/security holes
    - Each must be plugged
  - All security controls are determine through corporate policy
    - Implementation difficulties
    - Consistency challenges
  - 3rd party systems require a larger degree of administration and procedure

Firewall Hardware Types

- Hybrid servers
  - OS and Kernel hardening is started by vendor and completed by end user security staff—can help to make it more robust
  - Packaged software and hardware are generally reviewed for security
    - May or may not adhere to policy
  - All security controls are determine through a more partnered structure
  - Hybrid servers are also used to simplify implementation and support efforts without giving away administrative control

Module 1: Understanding Firewalls

Network Firewall Architecture

Network Firewall Architectures

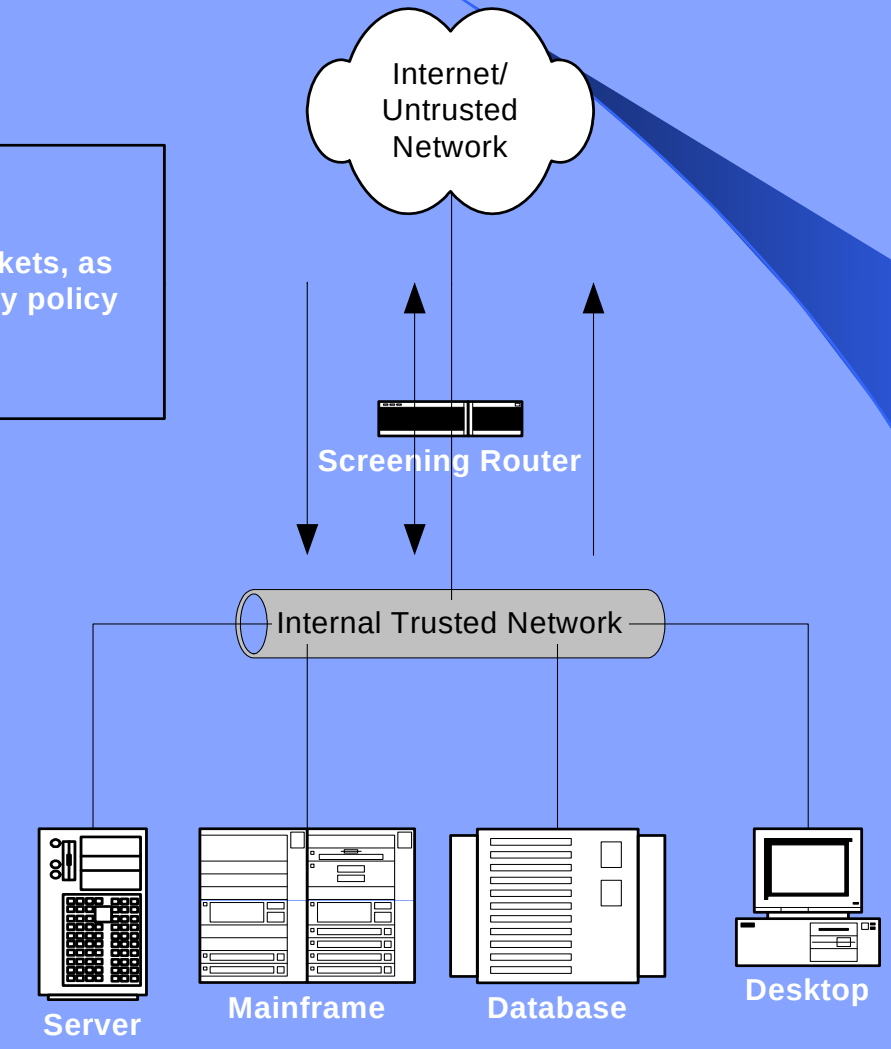
- Screening Router
- Simple Firewall
- Multi-Legged firewall
- Firewall Sandwich
- Layered Security Architecture

Screening Router

- Access Lists provide security
- Routers are not application aware
  - Only inspects network level information
  - Layer 3 of the OSI model
- Does not provide a great deal of security
- Very fast
- Not commonly used alone for security

Screening Router

Routes or blocks packets, as determined by security policy



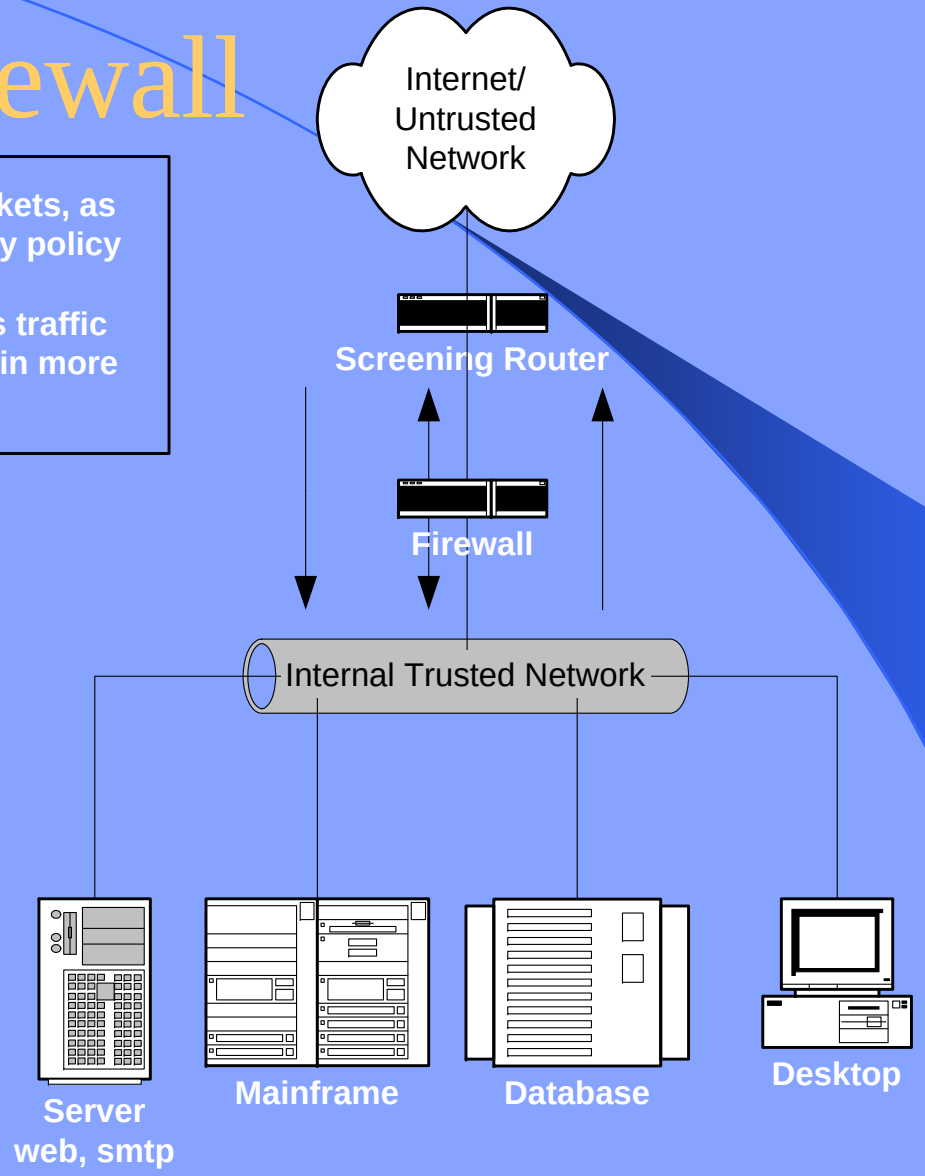
Simple Firewall

- Small Companies with limited security needs
- Only utilizes two interfaces
  - Trusted
  - Un-trusted
- Provides modest security
- Does not offer dmz sandbox
- Inherently allows some level of connections between trusted and un-trusted networks

Simple Firewall

Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security



Multi-Legged Firewall

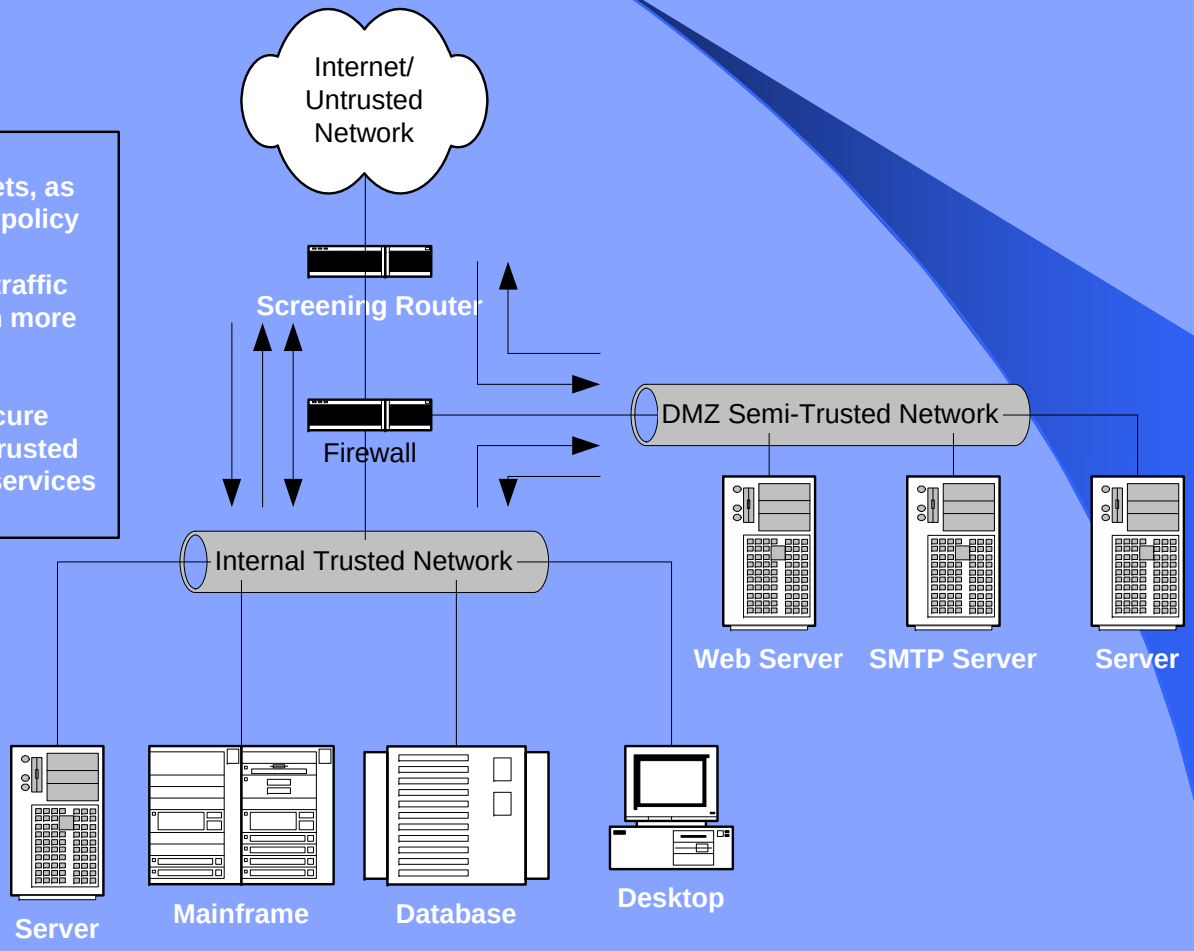
- Small to large sized business
- Security need is expanded
- Provides stronger security
- Creates a secure sandbox for semi-trusted services
- Flexible and secure

Multi-Legged Firewall

Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security

DMZ now offers a secure sandbox to handle un-trusted connections to internet services



Firewall Sandwich

- Medium to large businesses
  - Higher costs
- More serious need for security
  - Provides a physical separation of networks
- Provides policy segregation between inside and outside firewalls
  - Reduces administrative holes

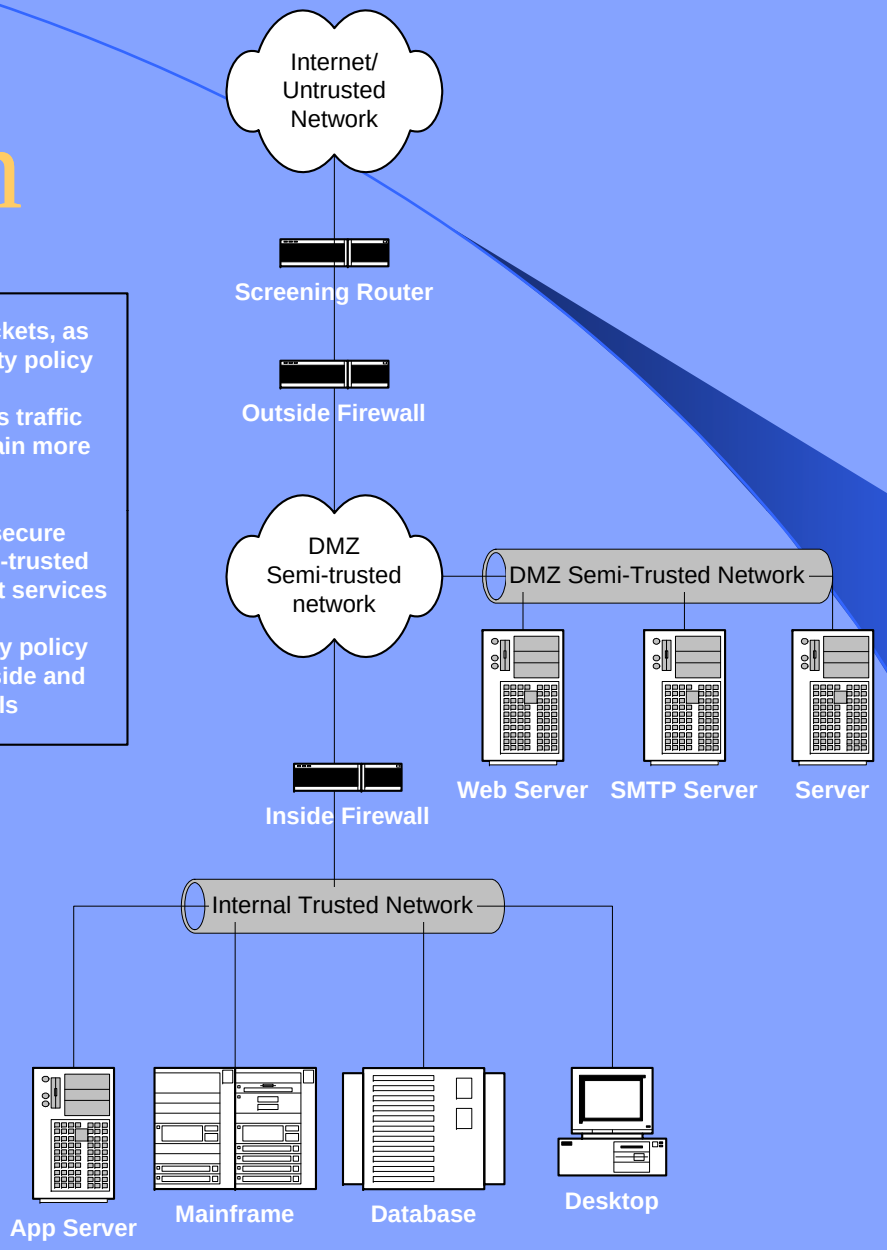
Firewall Sandwich

Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security

DMZ now offers a secure network to handle un-trusted connections to internet services

Separation of security policy controls between inside and outside firewalls



Layered Firewall Approach

- Large enterprises with low risk tolerance
  - Separates internal environments
  - Reduces computer crimes
    - Most attacks are internally based
    - Deters malicious activities
  - Controls overhead administrative traffic
  - Allows IDS to work more effectively

Layered Firewall

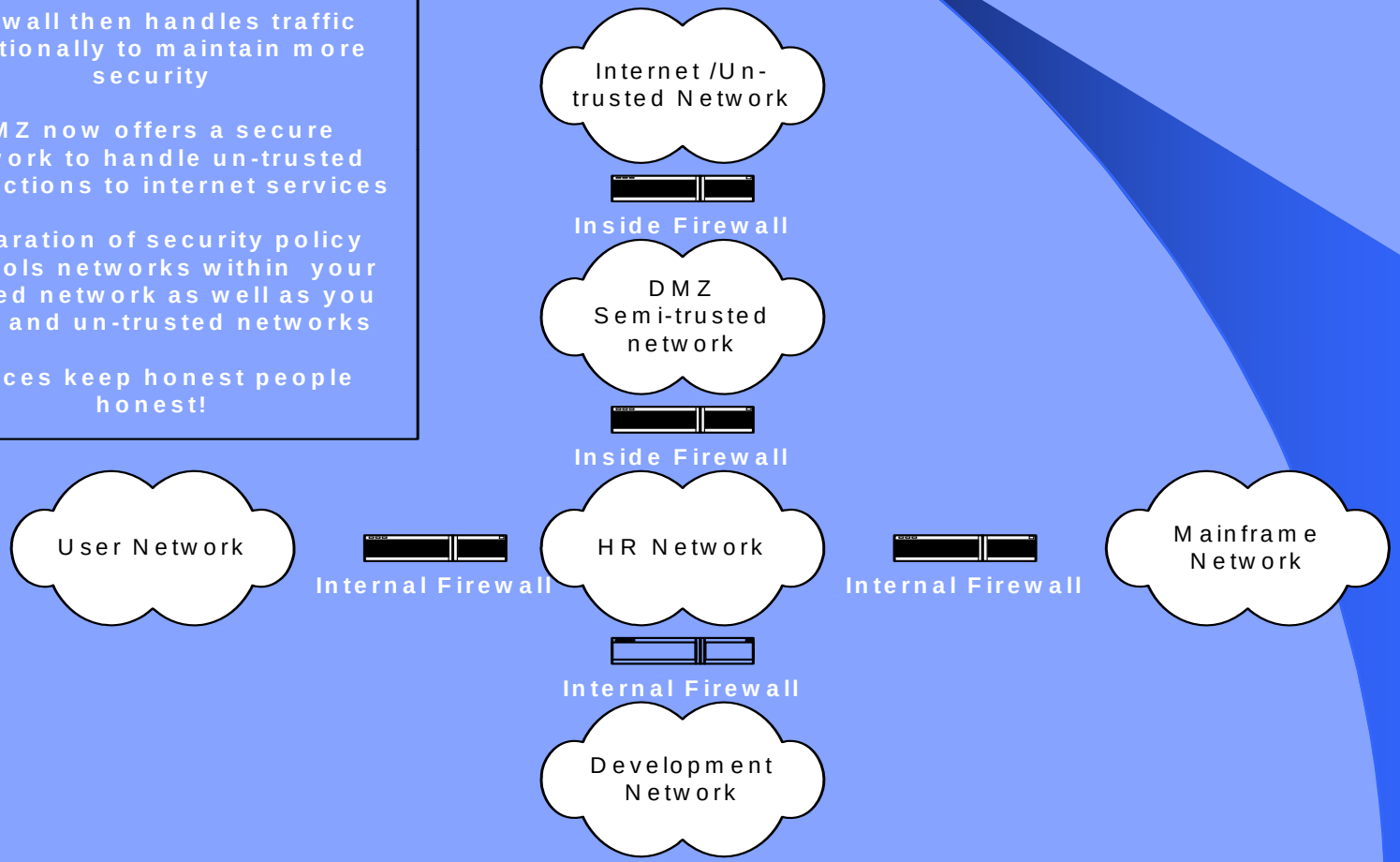
Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security

DMZ now offers a secure network to handle un-trusted connections to internet services

Separation of security policy controls networks within your trusted network as well as you semi and un-trusted networks

Fences keep honest people honest!



Defense in depth

- Security has no single right answer
  - Use every tool available to bolster security
- Layered security is always the best approach
- Strong security controls coupled with audit, administrative reviews, and an effective security response plans will provide a strong holistic defense

End of Module 1

Network Firewall Security

Auditing Firewalls

Module 2:
Security Operations

Firewall Administration Overview

Firewall Administration Overview

- Administrative Access
- Break Fix Response
- Monitoring and Alarming
- Logging
- Policy/Rule set Administration

Module 2:
Security Operations

Administrative Access

Administrative Access

- What is Administrative access?
  - Administrative Access refers to a group's need to gain control over a system for the purpose of discharging their chartered duties. This access includes, but is not limited to: Monitoring, Log Analysis, Break fix support, User administration, Rule/Policy implementation, OS configuration , software/hardware implementation, and patch/upgrade implementation.

    The need of any group to have this control should be carefully considered. Control rights delegated to teams should be clearly stated in your Corporate Security Policy.

Administrative Access

- Who might need access?
  - Support Staff
  - Implementation staff
  - Design staff
  - Network staff
  - Audit or Review staff
  - Many groups depending on your organizational structure

Administrative Access

- Types of access
  - Read/View
    - Typical need for design or Network staff
  - Add
    - Typical needs for Support and/or Implementation
  - Change
    - Typical needs for Support and/or Implementation
  - Delete
    - Typical needs for Support and/or Implementation
  - Audit/Over-site
    - Typical for Audit or review teams

Administrative Access

- Software Access control
  - Most systems are restrictive
    - Role based access is often missing
    - Inherent user rights of root/admin cause challenges
      - Root/Admin privilege is required to run firewall app
      - Root privilege is same on OS and firewall
    - Access to view often equals access to change or delete
      - Elevation of privileges
    - Organizational roles add complexity
      - The have and have nots vs. need and function

Administrative Access

- Products to help provide control
  - Many and diverse: sudo
  - All have limitations
    - Control commands
    - Create separate user group from root
    - Privilege can be upgraded inappropriately by user
    - Most provide a patch and not the solution
- Firewall products need to incorporate the required control

Administrative Access

- Passwords
  - Strong passwords
  - Centralized administration
    - De-centralized management in a large environment is trouble
  - Two factor authentication
- Physical access
  - Access points for administration a must
  - Operation Center with strong physical controls

Module 2:
Security Operations

Break Fix Response

Break Fix Response

- Business units must have clear notification path
- Organizations must have clear response plan
  - What teams perform support?
    - What support level is each responsible for
      - 1ST LEVEL
      - 2ND LEVEL
      - 3RD LEVEL
    - What privileges do each of these team have

Break Fix Response

- Talent
  - Each group must be properly trained
    - For every product they support
    - Certifications
    - General security knowledge
      - Running firewalls and running them securely are different
    - Procedurally
      - How they discharge their responsibilities properly
        - i.e. Allowable change
        - Break fix clearly defined from change

Break Fix Response

- Vendor relationships and support
  - Notification path clear to all team members
    - Internal web site a good communication device
  - Support contracts
    - Up to date
    - Inclusive of all products
    - Repercussions of no support agreement
      - Patch update access
      - Security fix access

Break Fix Response

- Interaction with product owners
  - Business units own application and are experts in the business need which typically conflicts with security policy/process
    - Put in a change when fixing a problem
    - Make changes on the BU side that requires a firewall change that is insecure
    - Without regard implement changes that break service and require firewall changes to restore production
      - Re-IP a dB sever
      - Change the communication protocol

Break Fix Response

- Oversight
  - Does the fix change security
    - Policies are done slowly with forethought
    - Break fix is done fast and in a vacuum
  - Does the fix change the design
    - Updating designs/risk matrixes
    - Who is responsible
    - How do we ensure it is done?

Module 2:
Security Operations

Monitoring and Alarming

Monitoring and Alarming

- Firewall Monitoring Problems
  - OPSEC
    - Greatly limits a groups ability to perform good monitoring
    - Monitoring and communication fly in the face of “need to know” security concepts
  - Products
    - Geared toward functionality—not security
    - Host Agents often open serious security holes
      - Remote login access
      - Random ports
      - Root level access for tools
  - Customer disclosure
    - Customer want access to tools to track system performance
    - Good monitoring often discloses sensitive information

Monitoring and Alarming

- Who performs monitoring?
  - Requires access
  - Discloses information
- Is access being delegated to others for any reason?
  - Who has access?
  - What controls are in place?
  - What rights have they been delegated?
- What product is being used?
  - Check for encryption and transport protocol
  - Check loading and maintenance plans

Monitoring and Alarming

Module 2: Security Operations

Logging

Logging

- Logging is very important
  - Provides history of access
  - Provides attack information
  - Provides for Policy audit checking
  - Provides trending analysis for capacity planning
  - Provides evidence for events

Logging

- Firewall Logging Problems
  - Many firewalls do not log effectively
  - Extremely large files
  - Difficult to manage and review
  - Products have logs written to different files
  - Access to many logs requires root access to firewalls
  - Log analysis products are add-on and expensive
  - Few organizations log effectively

Logging

- Logging Methods
  - Local
    - Directed to files (poor from a security perspective)
  - Remote
    - Syslog
      - Udp protocol is not reliable or secure (new syslog is better)
      - Cannot be used as evidence: not credible
    - Separated management network
      - Some products are managed and logged in an isolated network
      - Logging can be reliable and separate from firewall system
  - Firewall products often account for good logging
    - Ask good questions

Policy/Rule set Administration

- General security Policy Guidelines
  - Least Privilege Concept
    - Allow least amount of access to allow someone to complete their duties
  - Government orange and red books
    - Detailed security controls
    - Great reference material

Policy/Rule set Administration

- General security Policy Guidelines
  - Modems
    - Very insecure
    - Look for them on routers as a backup
    - Remote vendor administration
    - Banned by policy, allowed only by documented exceptions
  - Protocols
    - Tcp is the most easily controlled
      - Session oriented
      - Firewall compatible

Policy/Rule set Administration

- General security Policy Guidelines
  - Protocols continued
    - UDP
      - Use as little as possible
        - Needed for some require and some desired functions
        - Monitoring, logging, snmp management
    - Netbios
      - Easily attacked
      - Bad trust model

Policy/Rule Set Administration

- General Security Policy Guidelines
  - Authentication
    - Passwords
    - Two factor
    - Controls
    - CA and digital certificates
  - Encryption
    - Data classification
    - Strength
    - Where/when

Policy/Rule set Administration

- General security Policy Guidelines
  - Allowed Services
    - Should be known and highly controlled
      - www
      - http
      - smtp
      - vpn service
      - dns
    - Avoid inherently insecure services where possible
      - Finger
      - Telnet
      - ftp
      - nfs
      - Remote admin tools (some have good controls others do not)

Network Firewall Security

Auditing Firewalls

Module 3: Security Policy

Understanding Firewall Policies, Standards and Procedures

Why Conduct a Policy Audit

- The policy audit is the most difficult portion of a firewall audit
- The security policy is the single most important part of the firewall setup
- Security policy must be tied to the overall risk –vs.– cost benefit
  - If your security policy does not account for backups, risk is not controlled.
- Today we will discuss a department audit (firewalls)

Policy Defined

- Policy
  - The rules and regulations set by the organization. Policy determines the type of internal and external information resources employees can access, the kinds of programs they may install on their own computers as well as their authority for reserving network resources.
  - Generally a security policy is a document that states in writing how a company plans to protect the company's physical and information technology assets. A security policy is often considered to be a “living document”
  - Policy is typically general and set at a high level within the organization. Polices that contain details generally become too much of a “living document”

Standards

- Ensure that a product is fit for it's intended purpose and to ensure compatibility between computers
  - Industry Standards
  - For a Department audit, standards should exist between different business units and internally so that all team members understand how the different products work together

Procedure

- Established or prescribed methods to be followed routinely for the performance of designated operations or in designated situations -- called also *standing operating procedure*

Example

- The policy may indicate what type of data or protocol must run through a firewall
- Standards will dictate the type of firewall
- Procedure will show how the day to day tasks ensure that the spirit of the policy is maintained
- Today we will use the term policy to include Policy, Standards, and Procedure

Overview of this Module

- Policy Minimums
- Access
- Break Fix Response
- Monitoring and Alarming
- Logging
- Policy/Rule Set Administration

Starting the Policy Audit

- Identify who are the player
  - implementation, support, and design
- Wait to define scope until you understand the policy and players
- Does the division support the company's goals
- Does the department support the division policy
- Interaction with other groups (network, IDS, Anti-virus, business units,)

Identify Right Away

- Does the policy permit anything that’s not explicitly prohibited, or does it prohibit everything that's not explicitly permitted
  - Pros and Cons to each approach
  - Depends on the corporate philosophy but either is acceptable; however, most will tend to be more restrictive

Identify Right Away

- Authority for Policy
  - Without authority no security policy can succeed
  - Business units will always attempt to meet their needs, security is in their way
  - Must have authority to make business follow the policy
  - If they violate there must be consequences

Initial Items to Review

- Contingencies
  - How many items must line up for the policy to be effective.
- Complexity
  - Length of policies
- Part of overall organization risk management strategy
  - You can not do a firewall audit without familiarity of general security policy

Initial Items to Review

- Out of date
- Version control of the policy
- Approval process/Change management
- Who will own findings

Initial Items to Review

- Does policy innumerate the apps in use
  - Does policy address the hardware/software, versions
- How is policy updated
  - Can it react with the speed of new technology
- Define responsibility of tasks
- Overall controlling authority
  - Internal audit controls
  - Tools
  - Oversight
- Process to update failed procedures
- Information sharing

Specifics Necessary in Policy

- Policy should address
  - Risk vs. cost trade off
    - Sign off for exceptions
    - Risk avoidance or informed acceptance
  - Who polices / enforces the policy
  - Role based admin
    - Root password control
    - How is access defined and controlled
    - Password strength/resets grant access
  - Reporting, alarming

Specifics Necessary in Policy

- The groups that should be accounted for:
  - Implementation
    - Changes, new systems, removing, tracking changes, proper approval,
    - Easiest to audit and everyone focuses on the most, spend the least amount of time here
  - Design
    - Approval, templates/format, traffic allowed, protocols, general defined guidelines, channel back to policy makers to get new changes
    - Hardest, so many spend little time, should spend the most time

Specifics Necessary in Policy

- Support
  - Inventory control, response to issues, engage vendors, track issues, trend problems, access to designs,
  - Almost equal to design, ok one day does not matter if someone makes a simple change to the system
  - Hands on audit
- Others optional

Specifics Necessary in Policy

- Sensitive data storage/transportation
  - Rule sets
  - System Backup
  - Logs
- Physical security of systems
  - Good network security will not help if the firewall has unrestricted physical access
  - On premises
  - Off premises
  - Transit

Module 3:
Security Policy

Policy as the Underpinnings of a Secure Infrastructure

Access Control Policy

- The box
- The software
- The connected storage devices
- Roles
  - Controls
  - Tools

Break Fix Response

- Controls to maintain system integrity
- Availability
- Response times
- Skills of available engineers
- Interaction with other groups
  - Vendors
  - Business units
  - Support partners

Administration

- Security is a function of system administration
- System administration must be based in policy
- Tools
  - System configuration checkers
- Build documents
  - Allows for consistency
- Lists of installed software
  - Location within file structure
  - Permissions

Code

- Software/Hardware Vendors
  - Patches/fixes
  - New applications/OS upgrades
  - Kernel changes
- Business Unit requests
  - Application updates
  - New applications
  - Authentication changes
- Security updates/patches
  - Sense of urgency/timelines
- Testing
  - Procedures
  - Not co-mingled with production environment

Policy to Ensure Security of the Code

- Why
  - Most secure environments can be breached through a firewall accessible services
    - Poor coding allows remote administrative access through common HTTP services
- Problems
  - Buffer overflows
  - Cross Site Scripting
- Mechanisms
  - Code review
  - Application firewall products
  - Applications proxies

Infrastructure in Support of Policy

- Infrastructure allow you to meet policy requirements
- Once you know version check available resources for known issues and compare to the firewalls
- Engineering resources available
  - Can they fulfill the policy requirements
  - Training

Module 3:
Security Policy

Rule Base, Logging, Reporting

Monitoring

- What is required to be monitored in order to comply with policy
- Reporting
  - Who has access to the data
  - What tools are used to parse data
- Transportation of data
  - Tools and protocols allowed
  - If policy requires certain levels of data to be encrypted how is monitoring data transported
    - SNMP (version 3 is encrypted) /Mail/UDP/TCP
- Alarming
  - How
  - To where

Logging

- Daily review at a minimum
  - Tools are important, more reliable than a person and can be done constantly
- Done by someone with knowledge of what they are looking for
- Forensic analysis
- What is logged
  - successful attempts, failed?
- Where is the data stored
  - Should be remote to server
  - How is it transported

Response to Alerts

- Does the policy differentiate alerts
  - Incident response (hacking)
  - System problems
  - Network problems
  - Application problems
- Interaction with outside agencies
  - Police
  - Press
- Discloser of information
  - Who/when

Rule Set Administration

Firewall rules are the heart of any firewall system. A mistake in the firewall rules can undermine all security controls.

- Who designs the changes
  - Who approves the designs
- Are there standards to creating a design
  - E-mail, FTP, Web
  - Blocking Sites/Ports
- Who is authorized to change the rules
  - Who reviews these changes
- Mechanics of making the change
  - On the machine directly
  - Staged
  - Access points

Backup/Restore

- Media
  - Tape
  - Mainframe
  - Another host
- Frequency of backups
  - Consider the type of data
  - Consider frequency of changes to the environment
- Restoration
  - Contingencies for types of problems
    - Hacking
    - Loss of hardware
    - Loss of network
    - Loss of data center

Module 3:
Security Policy

Mapping Policy to the Firewall

Goals

- Match policy to the physical systems
- Match policy to team member processes
- Random sample of systems
- Review of system inventory
- System review
  - Define Files to see
  - Results of previous internal/external scans
  - Penetration tests

Mechanics

- Interview
  - Establish a rapport
  - Down play your role
  - Sympathize
  - Discuss opportunities that audits can present
  - Ask for “off the record” feedback about processes
  - Look for opportunities to move in a new direction
  - Identify others to interview
- Job shadow
  - Is it difficult to do the work in compliance with policy
    - Do short cuts result

Mechanics

- System review
  - Define files to see
    - Rule sets
    - Password
    - Operating system
    - Software configuration
    - Logs
      - Must be archived elsewhere
  - Define the manner in which you will have access

Pitfalls of too Much Policy

- Can’t be followed
- Impedes implementation
- Costs too much to the organization
- Too restrictive for business
- Does not allow for risk (risk avoidance opposed to informed acceptance)

Module 3: Security Policy

Understanding Firewall Policies, Standards and Procedures

Network Firewall Security

Auditing Firewalls

Module 4: Understanding Firewalls

Building An Audit Plan

Overview of the Basic Steps

- Review the policy
- Get an organization chart
- Determine the abilities of the firewall
  - What “add on” applications (e.g. IDS, anti-virus)
  - Can it enforce the policy
  - Does the design enforce the policy
- Identify the supporting components
  - Log server
  - Backup server
  - Access points
- Review the configuration of the firewall
- Conduct spot tests

Firewall Review

- As you are auditing the implementation
  - Build a list of:
    - Software used (include versions)
      - Don’t forget the remote access software
      - Don’t forget any clients running on the users end
    - Hardware
      - Operating system
      - Custom kernels

Research

- Check available online resources looking for known security holes
- Follow up with the manufacture to find out their recommendations for configuration/administration
- What are the newest versions and why are they not being utilized
  - Watch for end of life products

Back to the Firewall

- Check to see if is susceptible to any of the known vulnerabilities
  - Patches
  - Mitigating controls
- Proceed to the “Detail Audit” and use of tools
  - Run netstat to identify open ports
  - Run LSOF = list of open files

Spot Checks

- Attempt to bypass various controls
  - If an outbound only rule try to run the service inbound
    - FTP
    - Telnet
  - If it is suppose to filter content, try to pass the content
- Ensure you have management approval, plan to do the work after business hours

Tools to Aid the Audit

- Be careful to trust in tools too much
  - A lack of findings does not mean the system is set up well
- Use them to verify what you have already found out
- We are not doing a penetration test
- Firewalls have changed so fast that good comprehensive auditing tools have not been developed

Tools to Aid the Audit

- Port Scanner (nmap)
  - Should re-enforce what you found from running netstat
- Security scanning tools should show little information
  - Satan, Internet Scanner, work good to audit a trusted network for obvious issues but do not work well on a bastion hosted locked down OS
- Go to a class and be proficient

Detail Audit

- Access to the firewall should be authorized
  - How are employees and non employees given access
  - Obtain a list of users on the firewall
  - Cross check with staff lists/organization chart
  - Remote Administration
    - Onetime passwords
    - Other secure methods
    - Encrypted link
  - How is access changed or revoked
  - How is access reviewed
    - Mechanics of authentication
    - Frequency of review
    - Password reset/changing passwords
    - Root password control

Detail Audit

- Firewall should enforce security policy (encryption, viruses, URL blocks, proxy/packet filter types of traffic)
  - Obtain the rule set
  - How are rule sets stored to maintained to ensure that they have not been tampered with
    - Checksums regularly verified?
  - Is effectiveness of firewall tested
  - Review processes running on firewall; are they appropriate
  - Does the firewall provide adequate notice when an exploit is attempted?

Detail Audit

- Control
  - Physical access to the firewall controlled
  - How are software updates done
  - Control of sensitive information
    - IP addresses
  - Access tied to an individual
    - Control of hidden/system accounts
  - Control of devices used to manage firewalls

Detail Audit

- Network configuration
  - Obtain a design
  - Does the firewall properly protect the DMZ
  - Identify the monitoring and control of traffic procedures used
  - NAT to protect internal address space
  - Does firewall use dynamic or static address translation

Detail Audit

- Connections should be logged and monitored
  - What events are logged
    - Inbound services
    - Outbound services
    - Access attempts that violate policy
  - How frequent are logs monitored
    - Differentiate from automated and manual procedures
  - Alarming
    - Security breach response
    - Are the responsible parties experienced?
  - Monitoring of privileged accounts

Detail Audit

- Custom written scripts
  - Prolific in Unix environments
  - Should be listed, and reviewed
- Use of mail services

Detail Audit

- Management Reports
  - Capacity
  - Incidents
  - Alerts
  - Trending

Detail Audit

- Changes to the firewall configuration
  - How are they authorized
  - How are they tested
    - Safe environment
    - Tracked
    - Back out plan
  - Staging of rules/review by a second party
  - Change control vs. break fix
    - Changes should be scheduled and approved
    - Break fix should be limited to restore to working state without adding anything new
    - Any new IP addresses, URL changes must be approved and can not be addressed as break fix

Detail Audit

- Recovery
  - Plan developed in compliance with business continuity requirements
  - Are the time limits acceptable and achievable
  - Frequency of testing
  - Review the results of the most recent test