Introduction to Auditing Networks

Harshul Joshi

hjoshi@cbiz.com

408-794-3597

TCP/IP fundamentals

- OSI Layer
  - 7 – Application
  - 6 – Presentation
  - 5 – Session
  - 4 – Transport
  - 3 – Network
  - 2 – Data Link
  - 1 - Physical

Protocols

- Protocol numbers:
  - IP 0
  - ICMP 1 (Internet Control Message Protocol)
  - IGMP 2 (Internet Group Multicast Protocol)
  - GGP 3 (Gateway-Gateway Protocol)
  - TCP 6 (Transmission Control Protocol)
  - UDP 17 (User Datagram Protocol)

Ports

- After IP passes incoming data to the transport protocol, the transport protocol passes the data to the correct application process. Application processes are identified by port numbers.
- The source port number, which identifies the process that sent the data, and the destination port number, which identifies the process that is to receive the data

Ports

- Port numbers below 256 are reserved for well know services such as FTP, Telnet etc.
- Port numbers from 256 to 1024 are used for UNIX specific services like rlogin. However, most of them are no longer Unix specific.
- TCP and UDP can both assign same port numbers

Sockets

- Destination port for a well know service is fixed
- Source port is a dynamically allocated port
- Socket is IP*port on source and destination side and this pair makes a unique combination.

Perimeter Architecture

- Perimeter Devices
  - Routers
  - Switches
  - Firewalls
  - IDS/IPS
  - URL filtering
  - Anti-spam, Anti-Virus

Perimeter Devices

- Routers
  - Routing
  - ACL at Network Layer

Firewalls

- Firewalls
  - A firewall separates an internal network from the internet
  - Used to separate internal sensitive data and departments
  - Used to create DMZ for appropriate services
  - Can also be placed on laptops and desktops

Firewalls

- What are you trying to protect?
- What are you trying to protect it against?
- What is the realistic degree of protection you will achieve?

Firewall

- Some of the purposes:
  - Restricts people to entering at a carefully controlled point
  - Prevents attackers from getting close to your other defenses
  - Restricts people to leaving at a carefully controlled point
  - Think of firewall as a single point of entry or exit

Firewall

- It can’t
  - Protect you against malicious employees
  - Connections that by-pass firewalls
  - New threats for which you don’t have it configured
  - High end application layer attacks

High-Level strategies

- Principle of Least Privilege
  - Any object should have only the privileges it needs to perform its assigned tasks – no more
  - Examples – Don’t give all the users admin/root privileges, don’t open all the services for a specific connection etc.

High-Level strategies

- Layered security – Defense in Depth
  - Don’t rely on just one security mechanism
  - Firewalls can not be the only solution
  - All the perimeter security techniques and for that matter even the security architecture internally should be layered
    - Example – If you want an internal machine not to accept any mail, add an filter to the firewall to block SMTP traffic to that machine, but also remove the mail program all together from that machine itself

High-Level strategies

- Choke point
  - Pros and Cons
  - If there is some other mode of connection, it is useless
  - E.g. Out of band modem access or wireless access point that by-pass the choke point

High-Level strategies

- Weakest Link
  - You are only strong as your weakest link

High-Level strategies

- Fail-Safe
  - If everything fails, the default should be access deny not allow
  - E.g.: If a packet filtering router goes down, it doesn’t let any packets in.

High-Level strategies

- Universal Participation
  - Any exception will be your weakest link
  - Policy and Procedures required for universal participation

High-Level strategies

- Diversity of Defense
  - Using security systems from different vendors may reduce the chances of a common bug or configuration error to compromise them all.
  - Pros and Cons to this approach

High-Level strategies

- Incident response
  - Perimeter devices depend a lot on how effective is internal incident response system
  - Outsourcing of this aspect is normal
  - Lot of organizations miss granting the authority to the key individual who was pull the plug.

Key functionality of a Firewall

- Traffic forwarding
- IP address translation (NAT)
- Network differentiation
- Protection against DoS, scanning attacks
- IP filtering
- Port filtering
- Content filtering
- Enhanced authentication and encryption
- Logging and Monitoring

Types of Firewalls

- Packet Filters
- Stateful Inspection
- Application Proxies

Types of Firewalls

- Packet Filters
  - Makes a decision whether to forward a packet or not based on the IP layer
  - Glorified router
  - Does not keep track of TCP sessions

Types of Firewalls

- Benefits of Packet filter
  - Speed
  - No overhead

- Cons
  - Cannot inspect any content
  - Does not keep any state so all the attacks that manipulates the state cannot be detected

Types of Firewalls

- Stateful Inspection
  - A packet filter with stateful inspection is able to keep track of network sessions, so when it receives an ACK packet, it can determine its legitimacy by matching the packet to the corresponding entry in the connections table.
  - Entries in the connections table are automatically timed out after configurable time out period

Types of Firewalls

- Stateful firewalls
  - E.g.: Checkpoint and Cisco PIX
  - Still can provide lot more functionality with maintaining speed

Types of Firewalls

- Application Proxies
  - Act as intermediaries in the network session
  - User's connection terminate at the proxy and a corresponding separate connection is initiated from the proxy to the destination host
  - Connections are analyzed all the way up to the application layer to determine it they are allowed.
  - Higher security, but a higher toll on performance

Types of Firewalls

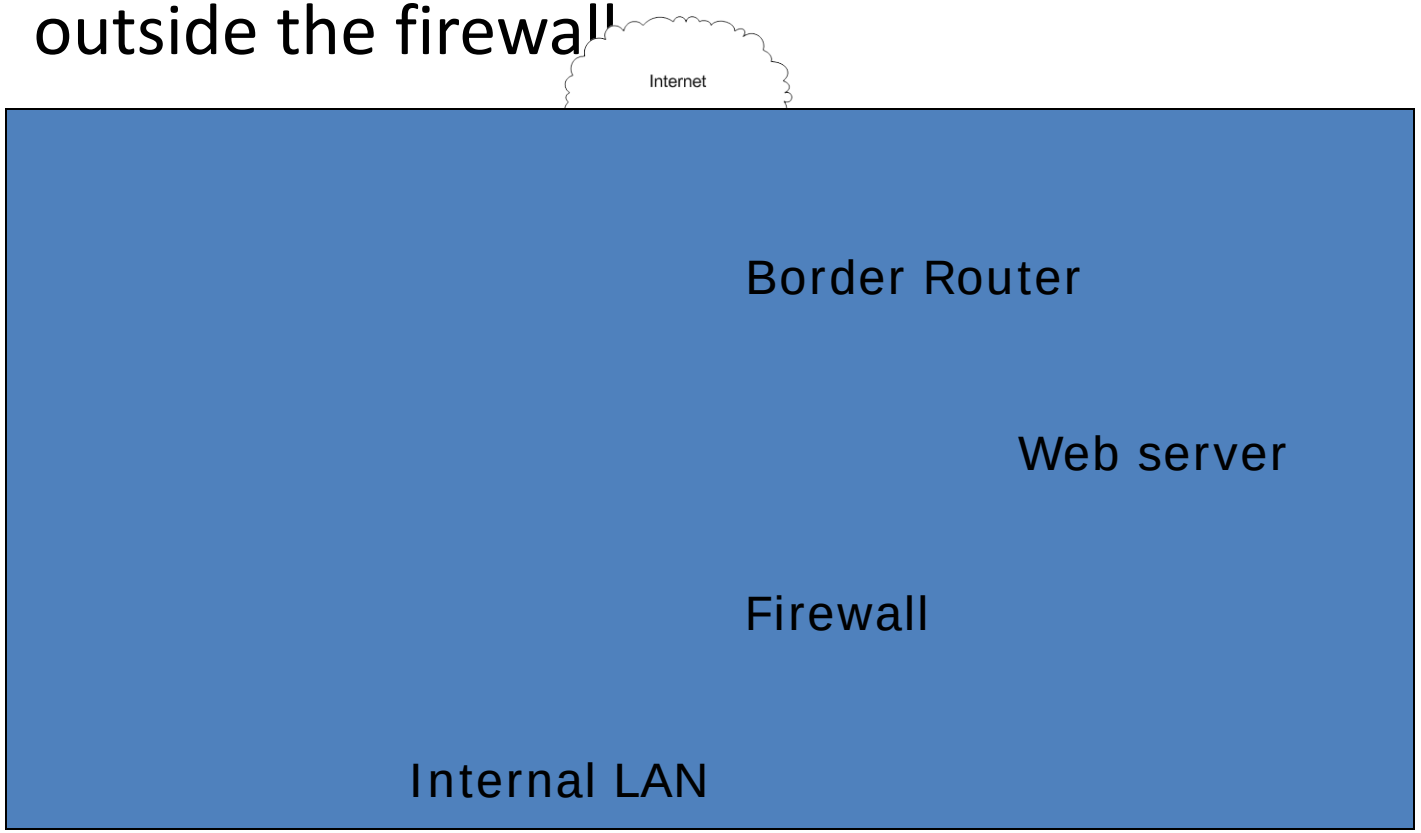
- Application proxies
  - Limitation – As new application protocols are implemented, corresponding proxies must be developed to handle them – Which means you can be at a mercy of the vendor

Firewall Interfaces

- Inside
- Outside
- DMZ

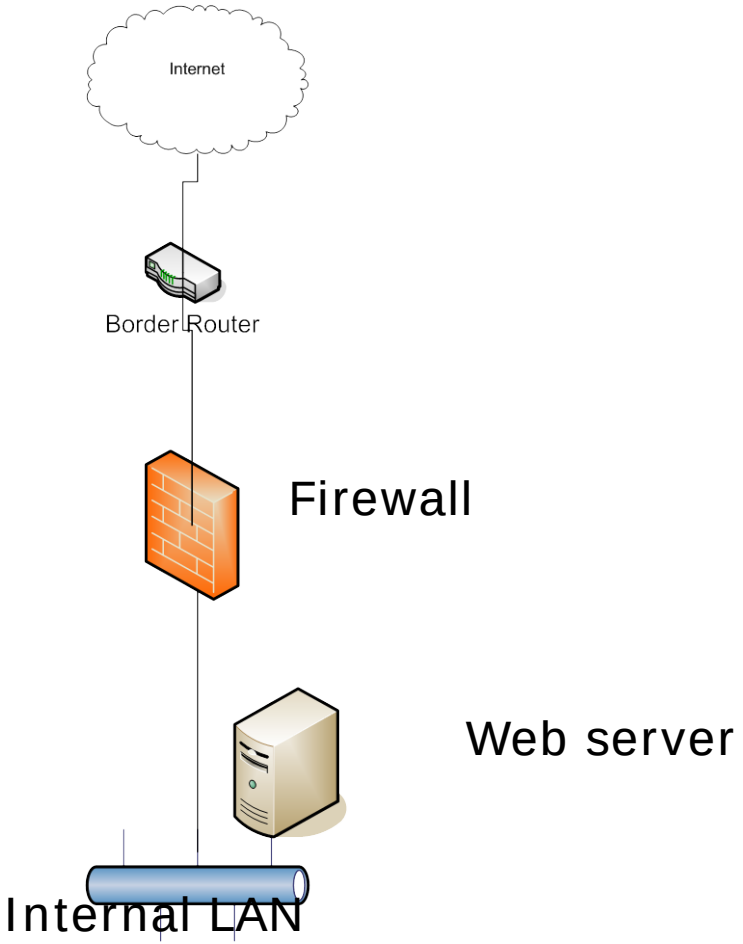
Architecture - 1

- Web Server located outside the firewall



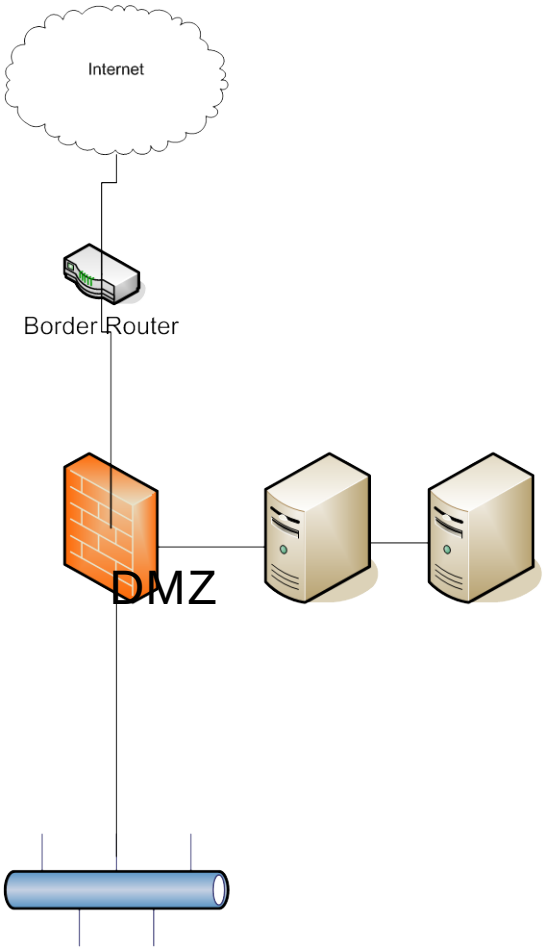
Architecture - 2

- Web Server Located Inside the Firewall



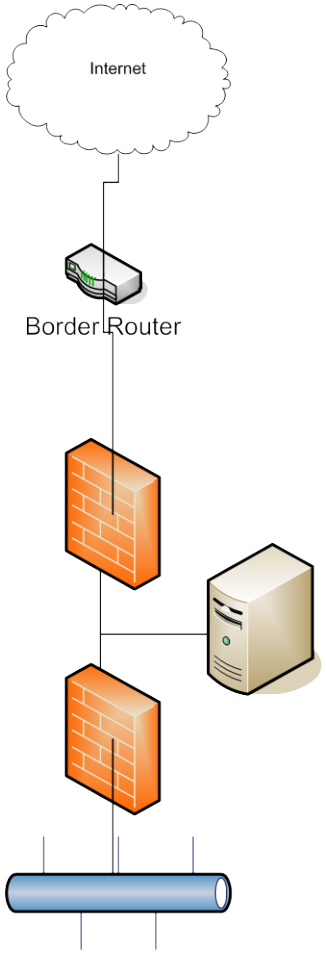
Architecture - 3

- A DMZ Network



Architecture - 4

- Two Firewall Architecture



DMZ Concepts

- One needs to visualize the traffic flow from – to – between Internet – DMZ – Firewall and Intranet.
- Placing servers at different levels have various effects
- Multi DMZ architecture can also be used to differentiate type of traffic.

E-Commerce example

- Multiple DMZ can be used for a three tier architecture

Traffic Flows

- Basic Single Firewall Flow
- Basic firewall with a server
- Basic firewall with server on the DMZ
- Dual Firewall with DMZ

DMZ architecture

- Application Servers in DMZ
  - Tight security in mind – all patches applied and all unnecessary services disabled
  - Functionality should be limited to specific tasks and as far as possible should not involve any sensitive data
  - Critical data should not be stored on any server on the DMZ

DMZ architecture

- Domain Controllers in DMZ
  - DC for Windows networks or other directory services authentication servers should never have those services located within the DMZ as far as possible

DMZ architecture

- RADIUS (Remote Authentication Dial-In User Service) servers
  - They are required to have full access to the authentication information provided by the Directory Services system
  - For the above mentioned reason, it must fully patched
  - Preferred option – RADIUS server located in the internal network with proxied requests coming from a Routing and Remote Access Services (RRAS) server and restricted communication that would be allowed through the firewall

DMZ architecture

- Business partner connections
- Extranets
- E-Commerce services
- E-Mail services
- Remote Administration

Translation

- Static Address Translation
- Dynamic Address Translation
- Port Translation

Checkpoint

- Firewall-1 and VPN-1
- Smart Dashboard
- Smart LSM
- Smart Update
- Smartview Monitor
- Smartview Tracker

Checkpoint

- Platforms
  - Windows
  - Solaris
  - Nokia

NetScreen

- Juniper's firewall + VPN + IDP product
- SSL VPN – clientless access into the network
- Core is based upon stateful inspection technology
- Based on a custom built architecture consisting of Application-Specific Integrated Circuit (ASIC) technology
- Supports Deep inspection – allows to inspect traffic at the application layer

NetScreen

- Content Filtering
  - URL filtering
  - WebSense redirect mode
  - SurfControl redirect mode
  - SurfControl Integrated mode
- Anti-Virus Scanning

NetScreen

- VPN
  - Site-to-Site VPNs
  - Policy-based VPN
  - Route-based VPN
  - Dialup VPN

NetScreen

- Advanced VPN configurations
  - VPN monitoring
  - Gateway redundancy
  - Back-to-Back VPN
  - Hub and Spoke VPN
  - Multi-tunnel Interfaces

IDS and IPS

- IDS – Intrusion Detection System
  - Host based
  - Network based
- IPS – Intrusion Prevention System

IDS and IPS

At first glance, intrusion detection and intrusion prevention systems look quite a bit alike. They both examine traffic going in and out of a network, looking for things that don't belong.

But there are significant differences that make some administrators reluctant to abandon IDS and just as reluctant to adopt IPS.

IDS and IPS

- IDS
  - An IDS examines packets, gathers information, logs it and can alert administrators when it thinks something bad is happening.
  - It is up to the administrator to decide what action to take.
  - Because the IDS does not make decisions about blocking traffic, it can take its time and can provide large amounts of data about network activity.

www.gcn.com

IDS and IPS

- Intrusion Detection
  - Administrators can be confident that legitimate traffic is not being blocked and that they have all the information they need to make decisions.
  - But on the other hand, they have to respond to those alerts and someone has to go through all of those logs if they are to be useful.

IDS and IPS

- Intrusion Prevention
  - An IPS not only examines network traffic, but can also automatically block traffic it thinks is inappropriate or malicious.
  - This takes a burden off the administrator, but many are uncomfortable with turning that responsibility over to a machine

IDS

- Signatures
  - Filters used to detect signatures
  - Updating signatures
  - Filter examples
    - Land attack
    - WinNuke
    - Christmas Tree

IDS

- Architecture
  - Sensor Placement
  - Outside firewall
  - Inside firewall
  - Both inside and outside firewall

IDS

- False Positive Management
- Correlation
- Weekly or Monthly reports
- Host or Network based IDS

IDS

- Network-Based IDS
  - ISS RealSecure
  - NFR
  - Cisco NetRanger

IDS

- Detection of Exploits
  - False Positives
  - All Response, No Stimulus
  - SYN Floods
- Denial of Service

IDS

- Intrusion Detection in a Security Model
- Security Policy
- Security Infrastructure
- Implementing priority countermeasures
- Periodic Reviews
- Implementing Incident Handling

IDS

- Defining Risk
- Accepting Risk
- Mitigating or Reducing the Risk
- Transferring the Risk

IDS

- Response
  - Automated
  - Manual

IDS

- Manual Response
  - Six steps
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery
    - Lessons Learned

IDS

- Making a Business Case

- Management Issues
  - Bang for the buck
  - The expenditure is finite
  - The Technology will not destabilize the organization
  - This is a part of the larger strategy

IDS

- Threats and Vulnerabilities
  - Threat assessment and analysis
  - Asset identification
  - Valuation
  - Vulnerability analysis
  - Risk evaluation

IDS

- Tradeoffs and Recommended Solutions
  - Defining an Information Assurance Risk Management Architecture
  - Identifying what is in place
  - Identifying your recommendation

Managing and Housekeeping a Firewall

- Rules and Policies
- Issues in implementing and managing enterprise level firewall
- How to reduce number of rules – Anomaly detection and rules editing
- Optimizing the rule base

Problems multiplies

- Large organizations – Many network segments and DMZ
- Firewall in critical path
- Numerous change request
- Little or No time to test changes and evaluate their impact

Problems

- Temporary rules not cleaned out an left in the rule base
- Lack of expertise
- Fear or breaking – so let it be
- Lack of intelligence and documentation
- Outsourcing and offshoring

Anomalies

- Stats show that traffic follows 80/20 rule
- Frequency analysis of traffic shows high hit counts for few rules and zero to low hit counts for a majority of the rules
- Log analysis sampled over a period of time can help determine rules which are no longer in use

FRAT

- Firewall Rulebase Analysis Tool
- Visual Basic – Perl Scripting
- Does Log analysis – Input from Log server
- Does Rule Base analysis – Input from Configuration files
- Output – Cleaned up configuration

Rulebase cleanup

- Create robust procedures for change control
- Create procedures for monitoring and administration
- Integrate FRAT
- Tool from www.cisecurity.org

Methodology

- Initiation
- Security and Architecture analysis
- Rulebase analysis
- Documentation
- Final cleanup

Project Objective

- Review existing rule base deployed on firewalls
- Enhance/Modify the rule base keeping in mind business requirements and objectives
- Document processes and procedures for implementing rules

Approach

- Freeze changes 2 days prior to implementation
- Obtain logs for 2 months
- Log analysis to determine hits on rules and rules with zero hit counts
- Redundant rules analysis and filtering
- Firewall rules analysis

Approach

- Grouped rules analysis
- Test changes in lab
- Open change request ticket
- Implement changes
- Monitor for any tickets based on the changes
- Implement changes permanently

Bottom Line – Clean up

- Firewalls are Critical elements to enforce enterprise security policy
- More often than not, enterprise firewalls have a voluminous rule base – that is cluttered and burdensome
- Inefficient change control process
- Critical to clean up firewall rule base to make them more efficient

Bottom line – clean up

- Automate firewall rules anomaly detection and log analysis
- Integrate Automation with an effective change management system
- Periodically audit

Network and Firewall penetration

- Firewall Identification
  - Direct Scanning – The Noisy Technique
  - The easiest way is to port scan the default ports. For E.g.: Checkpoint Firewall-1 listens on TCP ports 256, 257, 258 and 259; Checkpoint NG listens on TCP ports 18210, 18211, 18186, 18190, 18191 and 18192.

Network and Firewall penetration

- Banner Grabbing
  - Many firewalls will announce their presence when you connect to them.
- Deduction with nmap
  - Nmap will tell you which ports are open, and will also tell you which ones are being blocked.

Network and Firewall penetration

- Scanning through firewalls
- Firewalk
  - This tool will discover ports open behind a firewall.
- Source port Scanning

Network and Firewall penetration

- Denial of Service attacks
  - Infrastructure layer DoS
  - SYN Floods
  - UDP floods
  - DDoS
  - Application layer DoS

Network and Firewall penetration

- DoS counter
  - Block ICMP and UDP
  - Ingress filtering
  - Egress filtering
  - Disable directed IP broadcast
  - Implement Unicast Reverse path forwarding
  - Rate limit
  - Authenticate routing updates
  - Implement sink holes

Footprinting

- Footprinting is a process of creating a complete profile of target's IT posture.
- Internet footprinting ca be done using:
  - Whois
  - Sam Spade
- It provides the following information:
  - Internet Registrar data
  - Organizational information
  - Domain name system servers
  - Network address block assignment
  - Point of Contact information

Scanning

- After footprinting, identifying what systems are “alive” and what services they offer. Components to scanning are:
  - Ping sweeps
  - Port scans
  - Banner grabbing

Countermeasures

- Ping sweeps and port scans are blocked at the network layer using routers and/or firewalls
- Rewrite the banner
- ISAPI filter that interprets outbound HTTP responses and rewrites the banner

OS Fingerprinting

- If a TCP service is found to be available, the operating system of a target machine may also be detected simply by sending a series of TCP packets to the listening service and seeing what replies come back. Due to subtle differences in the TCP/IP implementations across various operating systems, one can fairly reliably identify the remote OS.

Enumeration

- Process to extract information such as valid usernames or shares. Windows 2000 enumeration can be grouped as follows:
  - NetBIOS network enumeration
  - DNS enumeration
  - Host enumeration
  - SNMP enumeration
  - Active Directory enumeration

NetBIOS Network Enumeration

- Enumerating Domains with Net View
  - List all domains available on network
- Nbtstat and nbtscan

Counter

- All attacks operate on TCP/UDP 135-139
- Also TCP/UDP 445

Enumeration Counter

- Filter access to TCP ports 389 and 3268 at network layer
- Disable the Alerter and Messenger services on NetBIOS aware hosts. This prevents user account information from appearing in remote NetBIOS Table dumps.
- Configure Windows 2000 DNS servers to restrict zone transfers to explicitly defined hosts, or disable zone transfers

Countermeasures

- Block untrusted access to or disable the SNMP service.
- Set complex, nondefault community names for SNMP services, if you use them.
- Remove the Everyone identity from the Pre-Windows 2000 compatible access on Windows 2000 domain controllers if possible.

PKI

- Goals to use PKI
  - Proper authentication
  - Trust
  - Confidentiality
  - Integrity
  - Non-repudiation
- By using the core PKI elements of public key cryptography, digital signatures and certificates, all of these goals can be met

PKI

- Components of PKI
  - Digital Certificates
  - Certification Authorities
  - Certificate Enrollment
  - Certificate Revocation
  - Encryption/Cryptography Services

PKI

- Digital Certificates
  - Small portable combination safe
  - Primary purpose – hold a public key
  - User Certificates
    - Enable the user to do something that wouldn't be allowed otherwise
  - Machine Certificates
    - Client side and server side authentication
  - Application Certificates
    - E.g.: IPSec and S/MIME encryption for e-mail

PKI

- Certificate Authorities
  - For a certificate to be of any use, it must be issued by a trusted entity – an entity that both the sender and receiver trust. Such a trusted entity is known as certification authority (CA)
  - With Win 2K, Microsoft has allowed the creation of a trusted internal CA, eliminating the need for the third party CA.
  - Windows 2003 CA verifies the identity of the user requesting the certificate by checking user's authentication credentials (using Kerberos or NTLM). If the credentials meet, the certificate is issued to the user. When the user needs to transmit his/her public key to another user or application, the certificate is used to prove to the receiver that the public key inside can be used safely.

PKI

- CA Hierarchy
  - Root CA
  - Subordinate CA
- Analyzing Certificate Needs
  - Need to understand different uses of certs
  - SSL – Web server, S/MIME for email encryption
  - Use of S/MIME might dictate that your CA hierarchy has a trust relationship with external CAs, and use of SSL might lead to stand alone CA instead of enterprise CA.

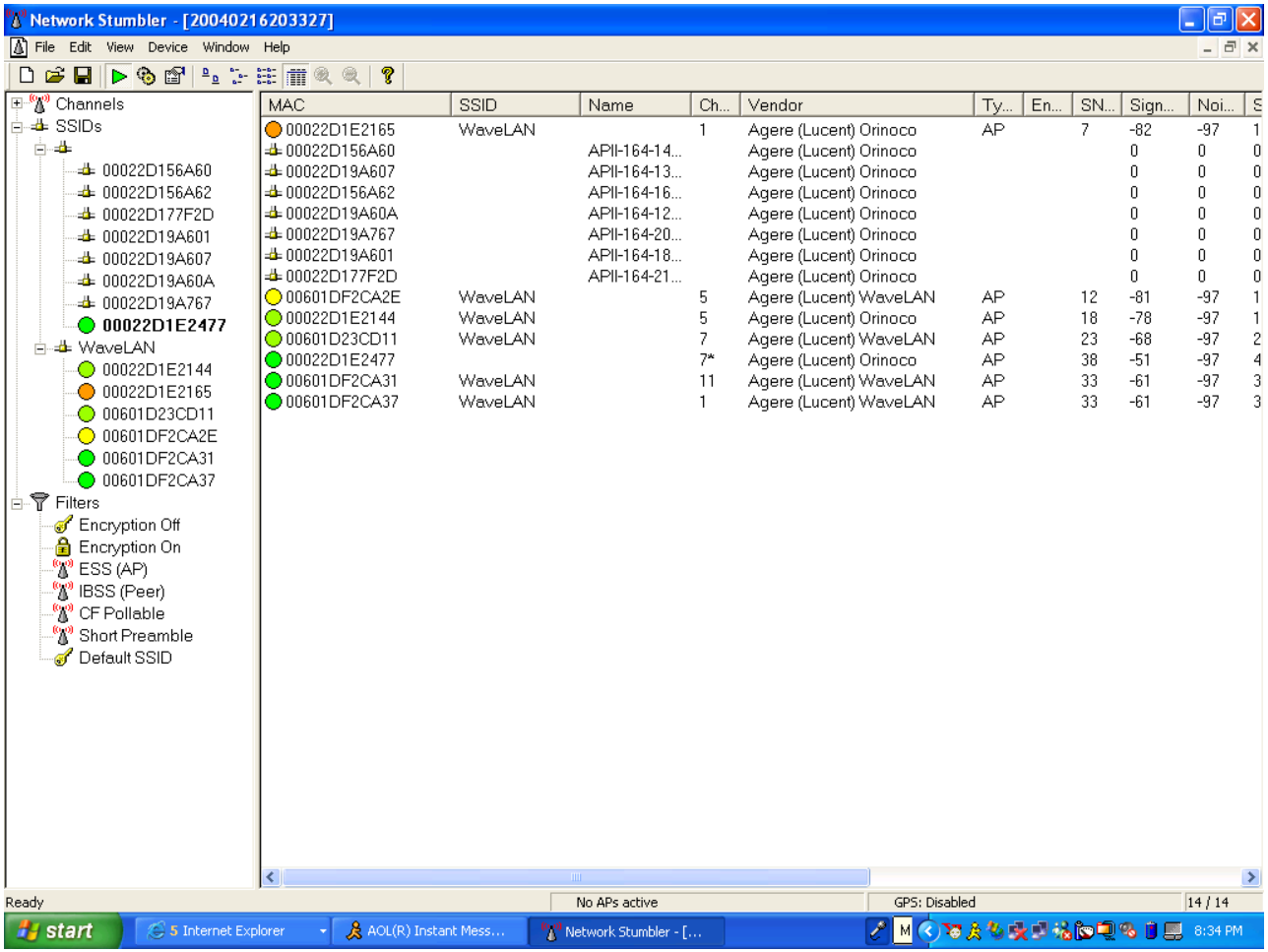
Perimeter architecture for Wireless

- Wireless networks are growing with leaps and bounds
- This presents an additional challenge with respect to Perimeter security

Attack/Auditing Tools

- NetStumbler
  - Sends out 802.11b probe requests
  - Listens for responses
  - Windows based
  - Cannot monitor beacon packets
  - Relies on only one form of wireless network detection – the Broadcast Probe Request. If this feature is disabled by vendors, NetStumbler is useless

Attack/Auditing Tools



Attack/Auditing Tools

- MiniStumbler
  - Smaller version of Netstumbler
  - Works on handhelds like Compaq IPAQ
- Hotspotter
  - Utilized to find wireless hotspots or wireless networks

Attack/Auditing Tools

- Kismet
  - Linux and BSD based wireless sniffer that has war-driving functionality
  - Passive network-detection tool that cycles through available wireless channels looking for 802.11 packets that indicates the presence of wireless LAN, such as Beacons and Association requests

Attack/Auditing Tools

- Kismet
  - Uses Monitor mode
  - Can detect “closed” networks
  - Logs traffic in tcpdump format
  - Works on both 802.11a and 802.11b
  - Can configure channel hopping
  - Hidden SSID decloaking
  - Runtime decoding of WEP packets

Attack/Auditing Tools

- Wellenreiter
  - Better GUI
  - Works with all 3 major wireless cards
    - Prism2
    - Cisco
    - Lucent

Attack/Auditing Tools

- Dstumbler
  - Wardiving/lanjacking utility for BSD
  - Part of bsd-airtools released by Dachb0den Labs

Attack/Auditing Tools

- Aerosol
  - Wardriving tool for Prism2 cards

Attack/Auditing Tools

- Wireless Monitoring Tools
  - Prisn2dump
  - Tcpdump
  - Ethereal
  - Airfart
  - AiroPeek NX
  - WifiScanner

Attack/Auditing Tools

- Ethereal
  - Works on both windows and Linux
  - Can read the input from the captured files from Airopeek
  - Can replay sessions

Attack/Auditing Tools

- Commercial Sniffers
- AiroPeek NX
  - Windows platform
  - Most comprehensive wireless analyzer
  - Works with 802.11a, 802.11b and 802.11g as well as multi-mode cards
  - On the fly WEP decryption
  - Post-capture WEP decryption

Attack/Auditing Tools

- AiroPeek NX
  - Multiple cards supported
  - Analyze VoIP

Attack/Auditing Tools

- Handheld Sniffers
  - CEMyNetwork Standard 3.2
  - AirMagnet (Version 2.5)

Attack/Auditing Tools

- Tools used for Cracking WEP
  - AirSnort
  - WLAN-Tools
  - DWEPCrack
  - WEPAttack

Attack/Auditing Tools

- AirSnort
  - Cracks 802.11b WEP Keys
  - Passive monitoring of wireless data
  - Approximately 1 GB required to crack
  - Solely *nix based
  - Supports both ORiNOCO and Prism II cards

Attack/Auditing Tools

- WEPCrack
  - Program coded in Perl
  - Perl is required to run WEPCrack

Securing WLANS

- Firewalls
- VPN
- 802.1x/EAP

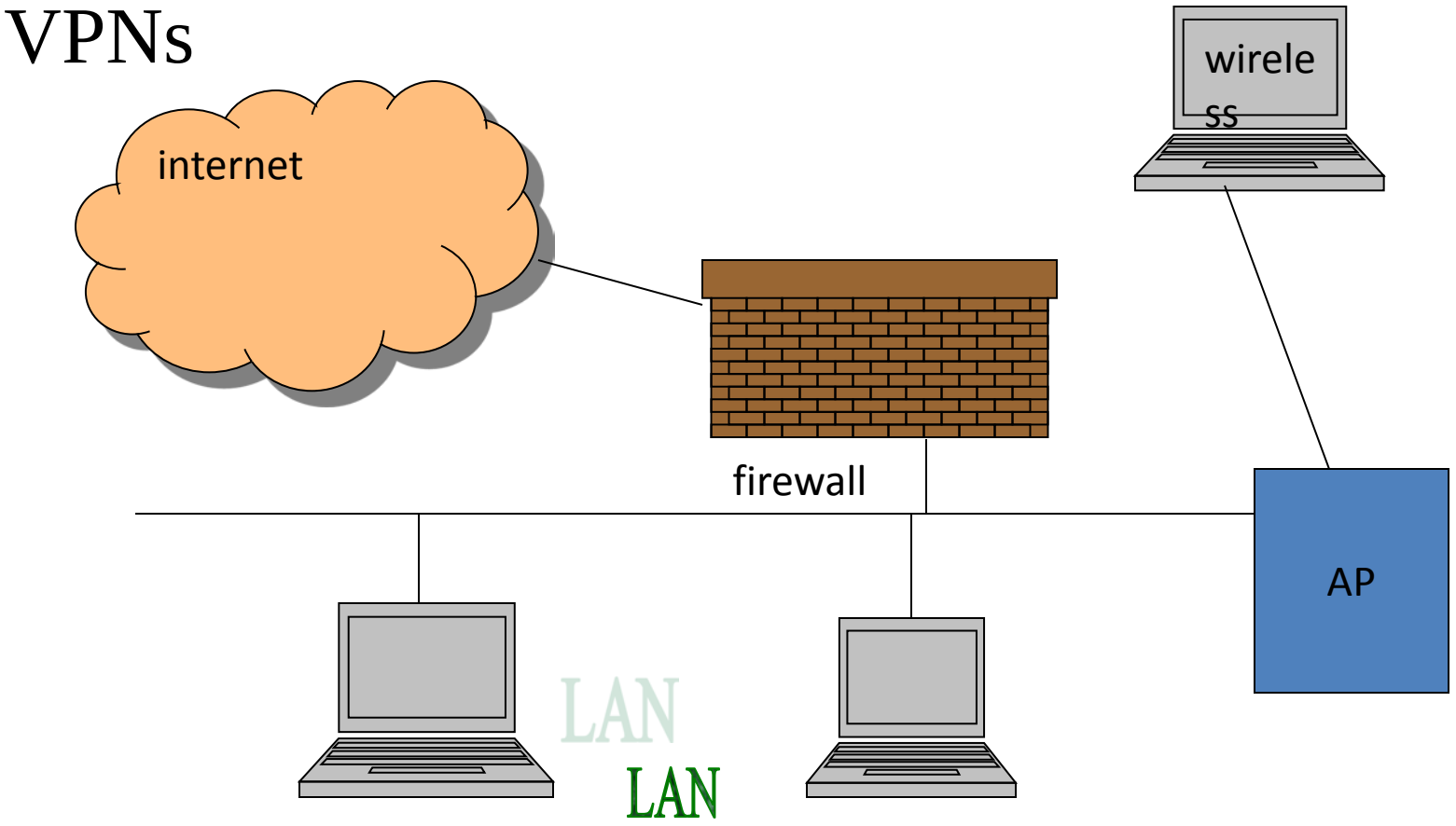
Securing WLANS

- Firewalls
  - Consider WLAN users as remote access users
  - Separate WLAN on a different segment of a Firewall
  - Limit the amount of traffic from WLAN to internal network

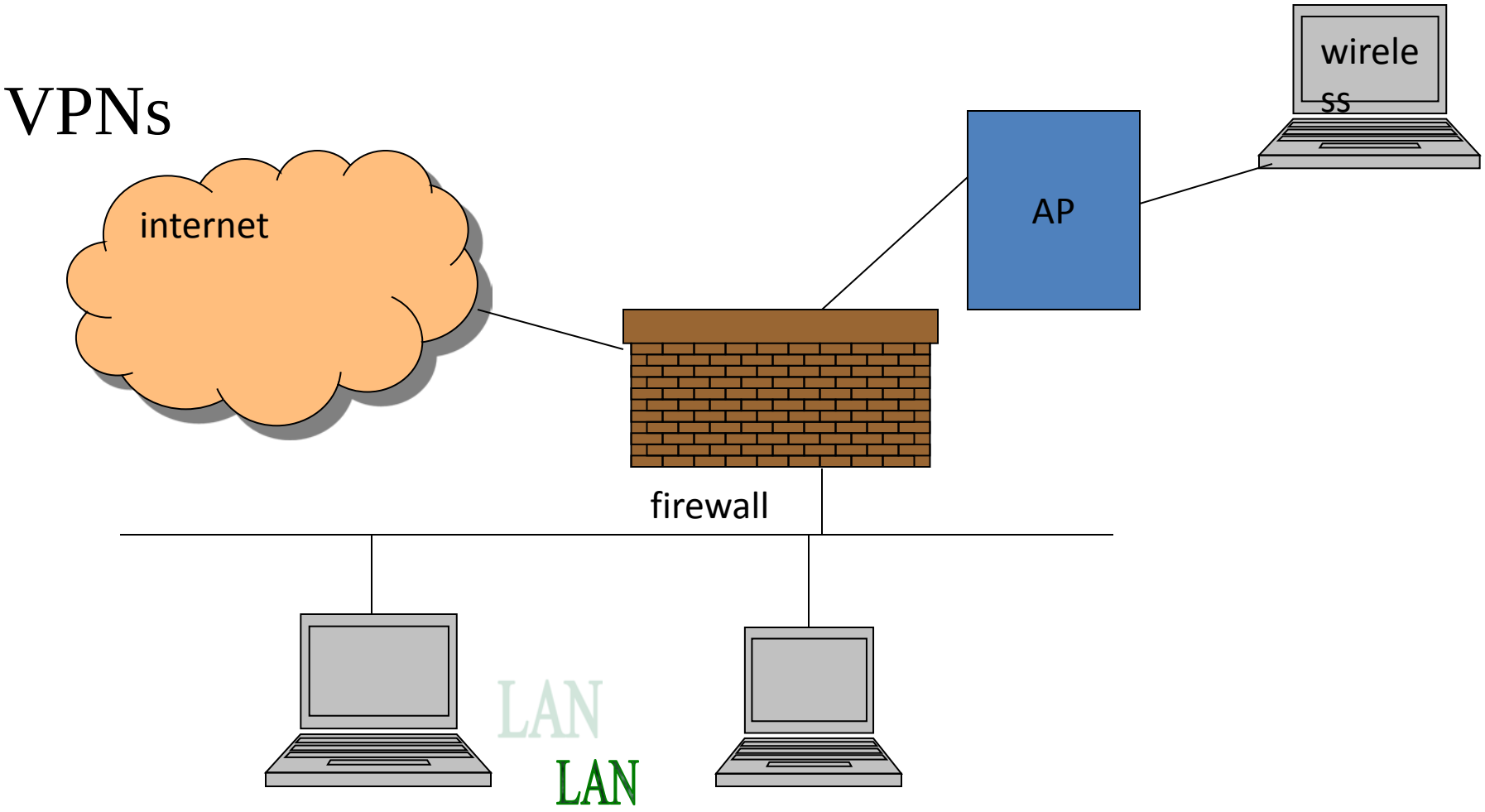
Securing WLANS

- Firewalls
  - Mirror the data if possible for WLAN users to segregate them from internal network (For e.g.: FTP server, Web server, Mail server)

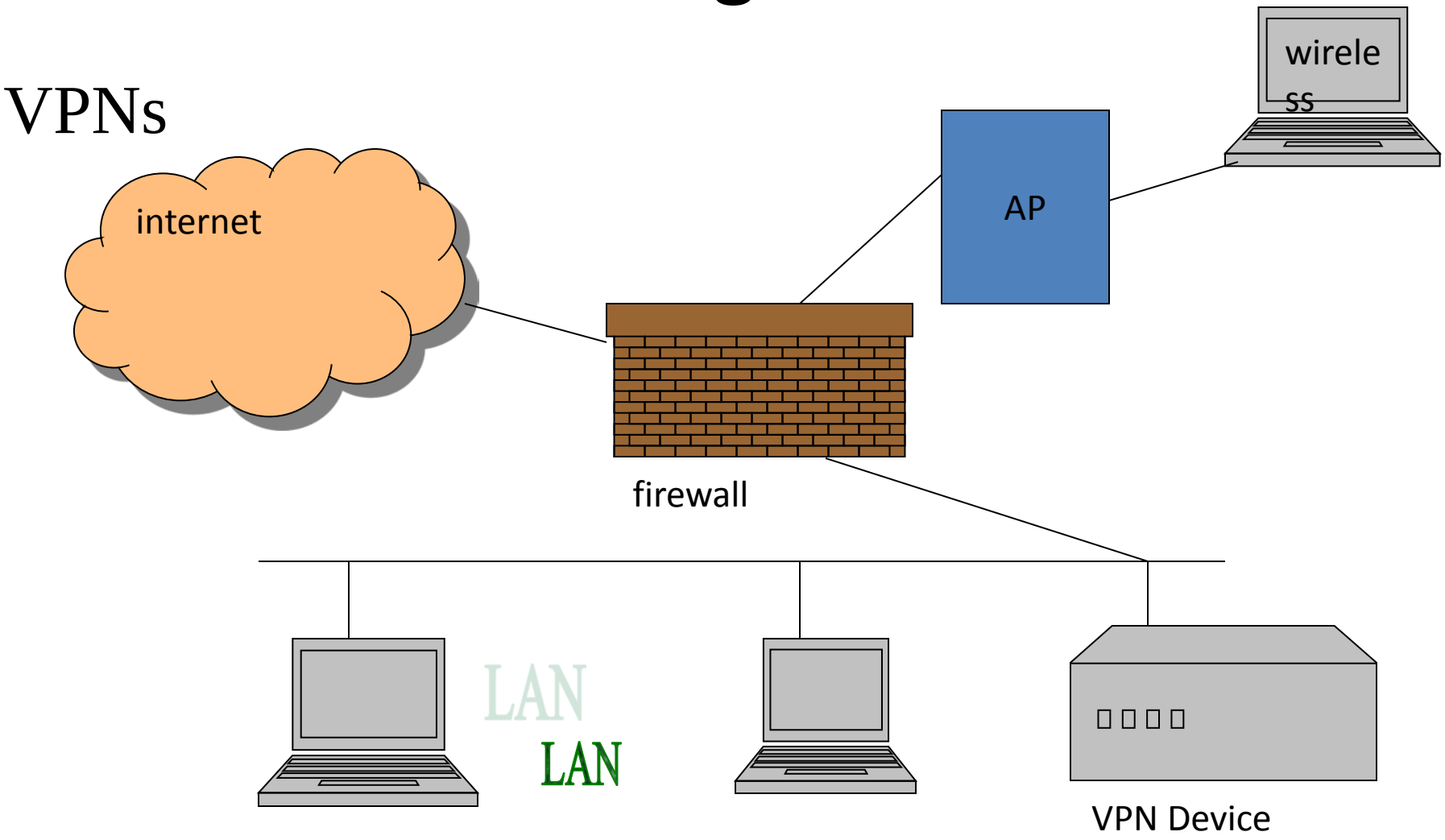
Securing WLANS



Securing WLANS



Securing WLAN



Hardening Wireless

- Plan Secure Wireless Networks
- Seek and Destroy Rogue WLANs
- Design your WLAN Topology
- Harden your Wireless WAN

Hardening WLAN

- Plan Secure Wireless Networks
  - Wireless security policy
    - Who has authority over wireless networks
    - Define wireless network segmentation requirements
    - Define hardware and software requirements
    - Define authentication method
    - Define encryption method
    - Define logging and accounting requirements
    - Define WAP security requirements

Hardening WLAN

- Seek and Destroy Rogue WLANs
  - Implement WLAN discovery procedures
  - Detecting unauthorized WLANs wirelessly
  - Detecting unauthorized WAPs from the wired network

Hardening servers and services

- Perimeter security is not just firewalls, routers, IDS and IPS
- The way we secure our servers sitting on the DMZ matter a lot.