



Securing Wireless Networks On a Budget

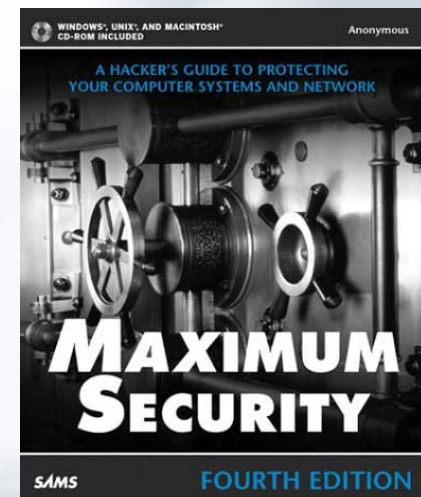
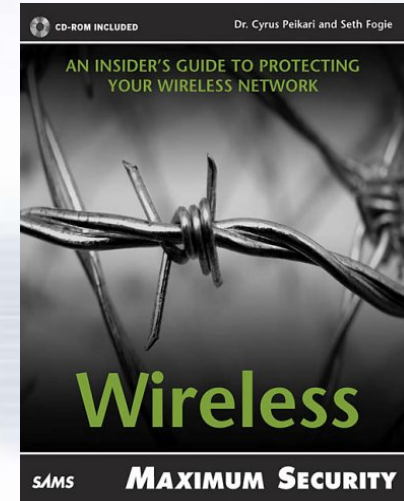


By Brett L. Neilson
hamcom@brettneilson.com



Who am I?

- **Brett L Neilson – KC7IIB**
- **Author**
 - Maximum Wireless Security
 - Maximum Security 4th Edition
- **By Day**
 - Networking Security Professional
 - Intrusion Prevention
 - RF Field Technician Systems Admin





Overview

- **Threats to Wireless Networks**
- **Access Point Security Options**
- **Security Topologies**
- **3rd Party Security Devices**
- **VPN Tunneling**
- **Recommendations for Security**



Threats to Wireless Networks



What is the threat?

- **WarDriving**
 - Searching and Logging
- **Data Snooping**
 - Capturing data
- **Jamming**
 - Disrupting legitimate signals
- **Insertion Attacks**
 - Unauthorized clients and APs
- **Malicious Code**
 - Virus / Worm / Trojan



Access Point Security Options



Access Point Security Options

- **Disabling the SSID Broadcast**
 - Prevents the Access Point from announcing itself
 - Helps to reduce reconnaissance attacks (NetStumbler) by not responding to broadcast 'Probe Request' frames
 - Hiding in plain sight

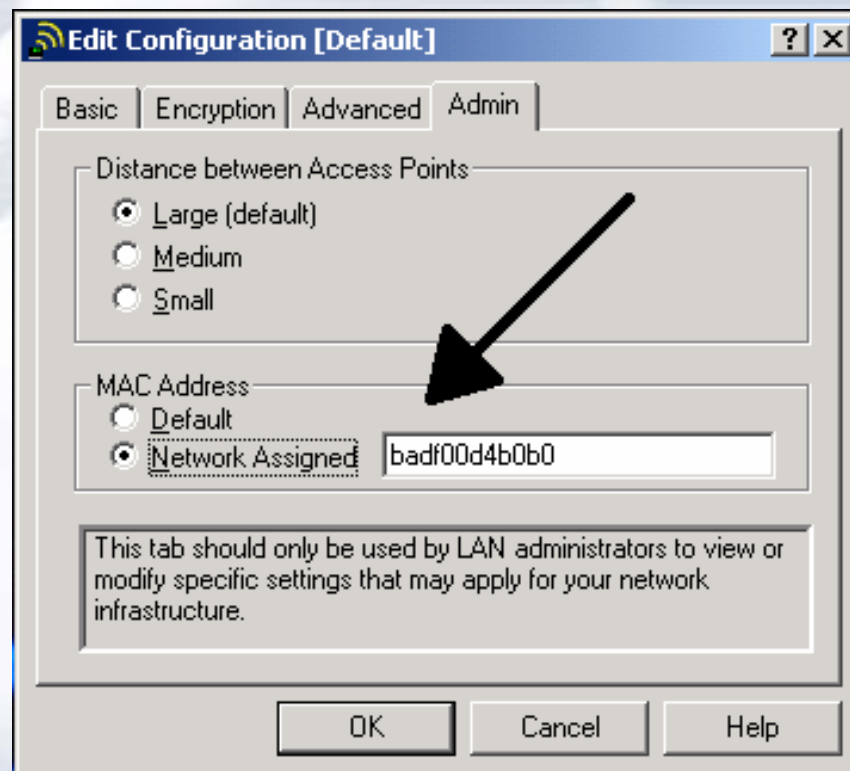
```
00000000: 80 00 00 00 ff ff ff ff ff ff 00 06 25 50 38 82 |...yyyyyy..%P8|
00000010: 00 06 25 50 38 82 10 c1 4e 12 7f 1e 06 01 00 00 |..%P8|.AN.|.....
00000020: 64 00 01 00 00 12 57 61 72 64 72 69 76 65 72 |d.....Wardrivers
00000030: 20 57 65 6c 63 6f 6d 65 01 04 82 84 8b 96 03 01 |Welcome..||||..
00000040: 0b 05 04 00 02 00 00 |.....
```



Access Point Security Options

- **MAC Address Filtering**
 - Restricts connections based on MAC Address
 - Good base level of security
 - Very little overhead
 - Provides no data security

Can easily be spoofed





Access Point Security Options

- **Wired Equivalent Privacy (WEP)**
 - Encrypts data with an RC4 algorithm
 - Built into all access points
 - Easily configured and implemented

Can be compromised, however

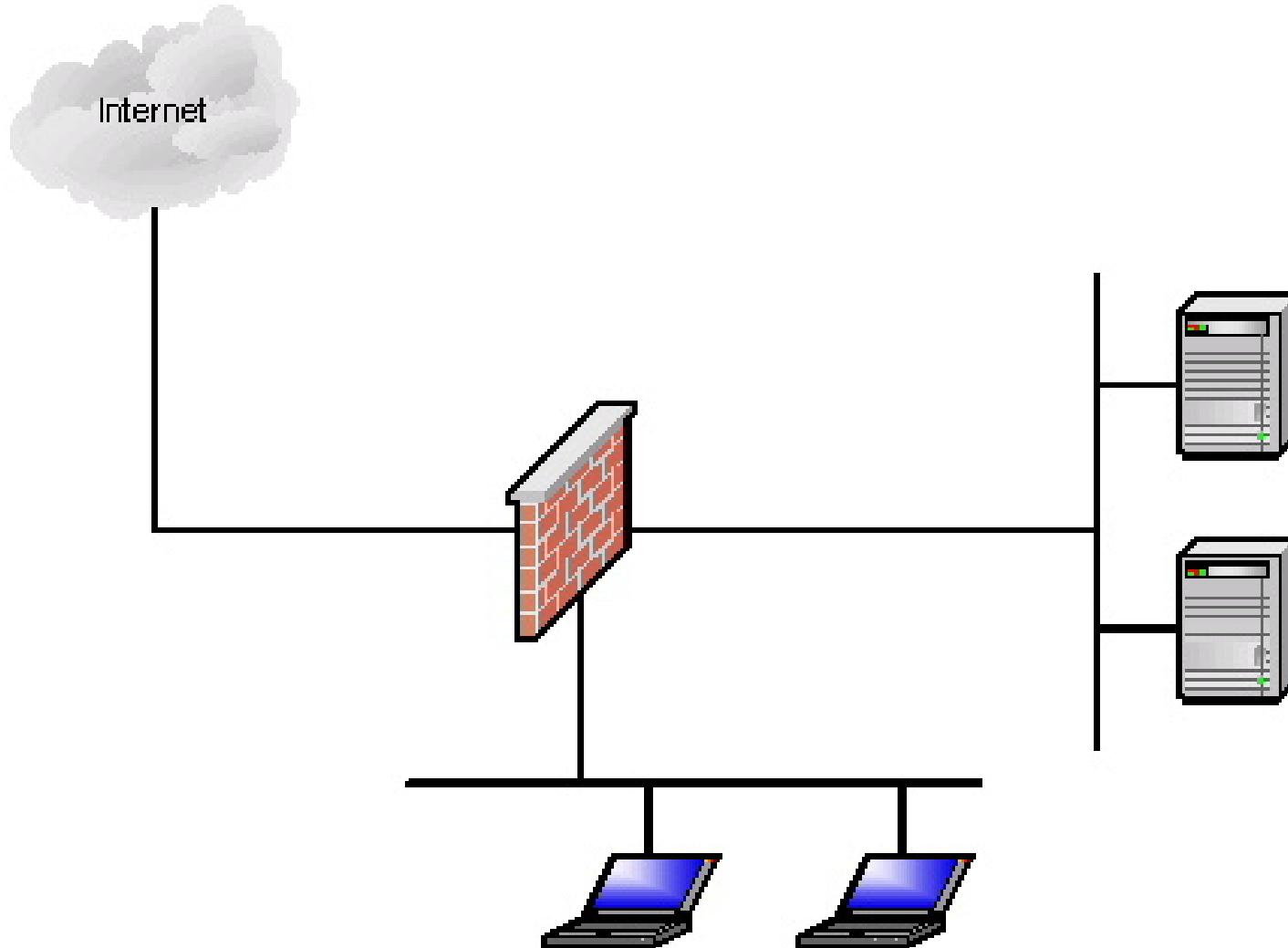
- Not as easy as it is portrayed by all the hype
- Two to four weeks of data on a low use network
- No Windows utilities



Security Topologies

Security Topologies

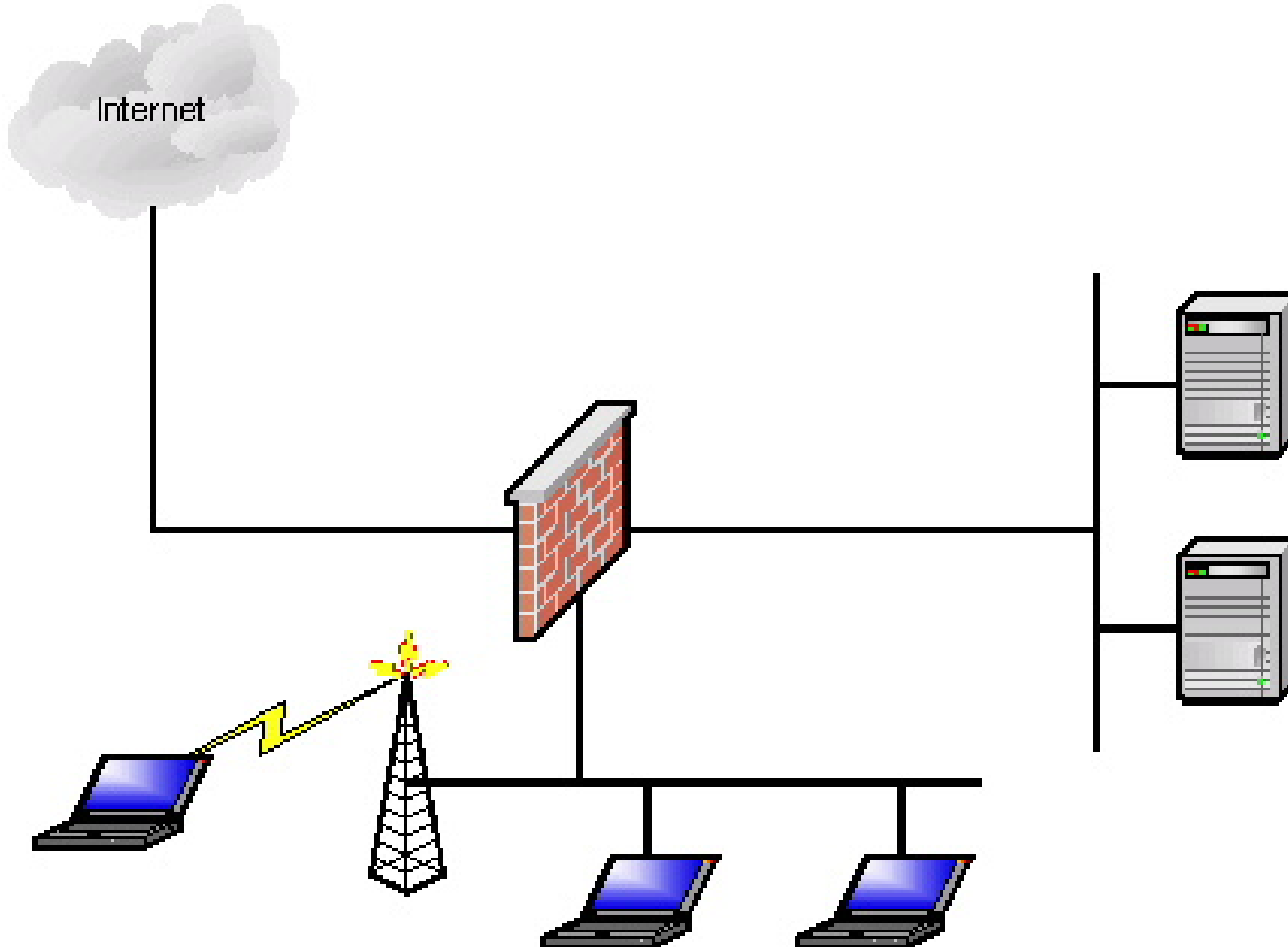
- **Traditional Generic Network**



Security Topologies

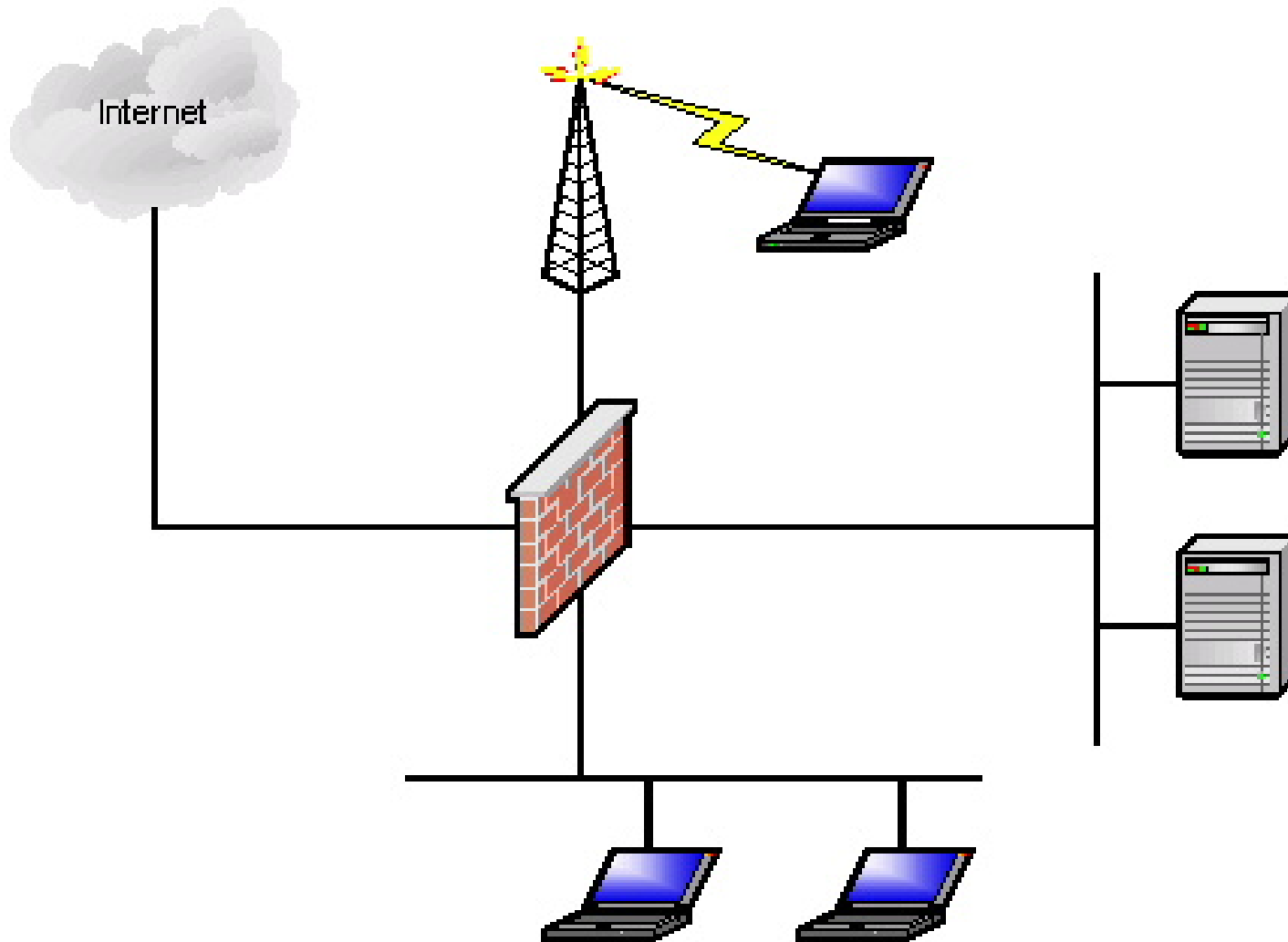
- **Traditional Network with Wireless**

Not Recommended



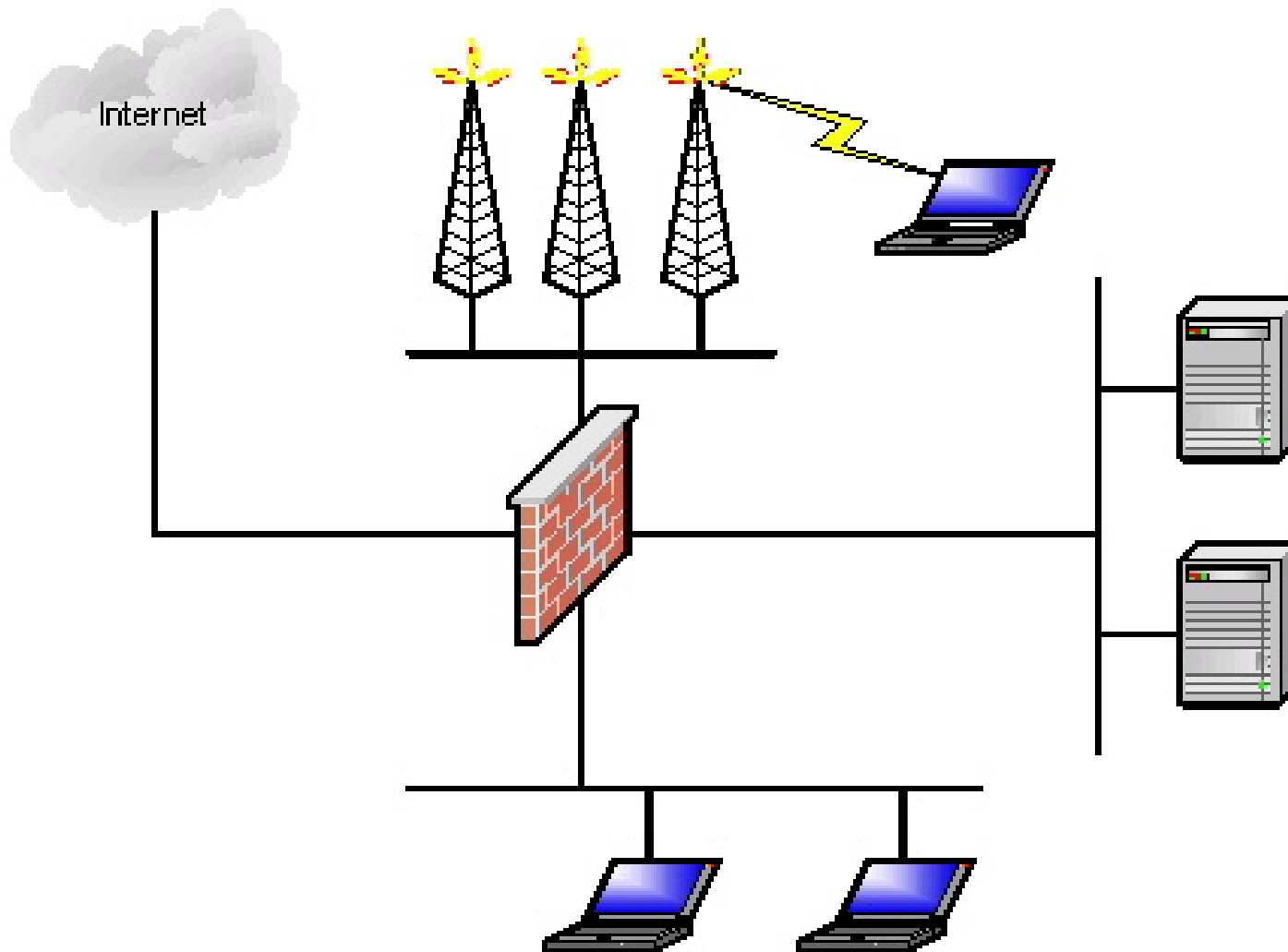
Security Topologies

- Network with Wireless DMZ



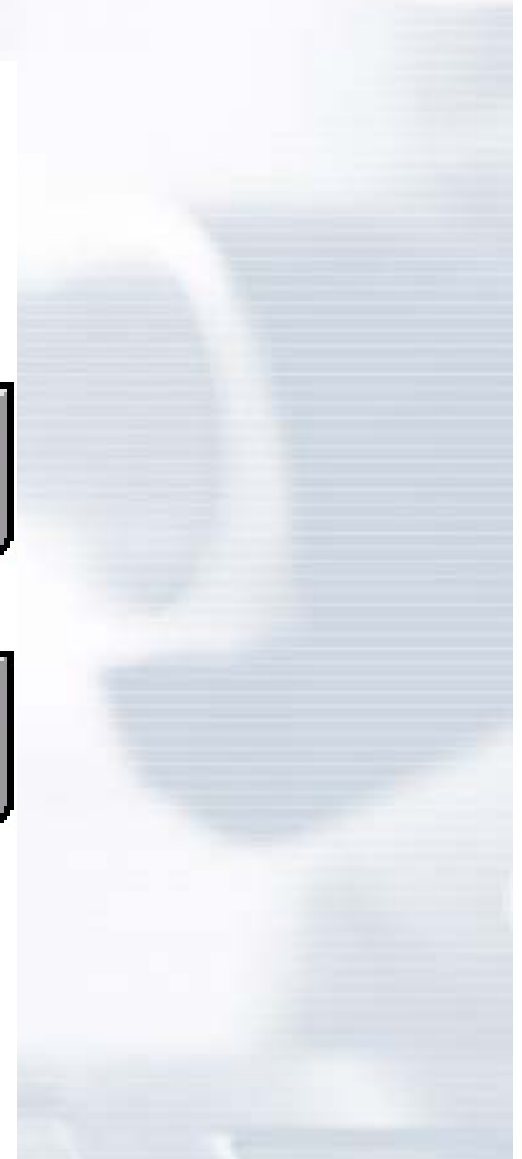
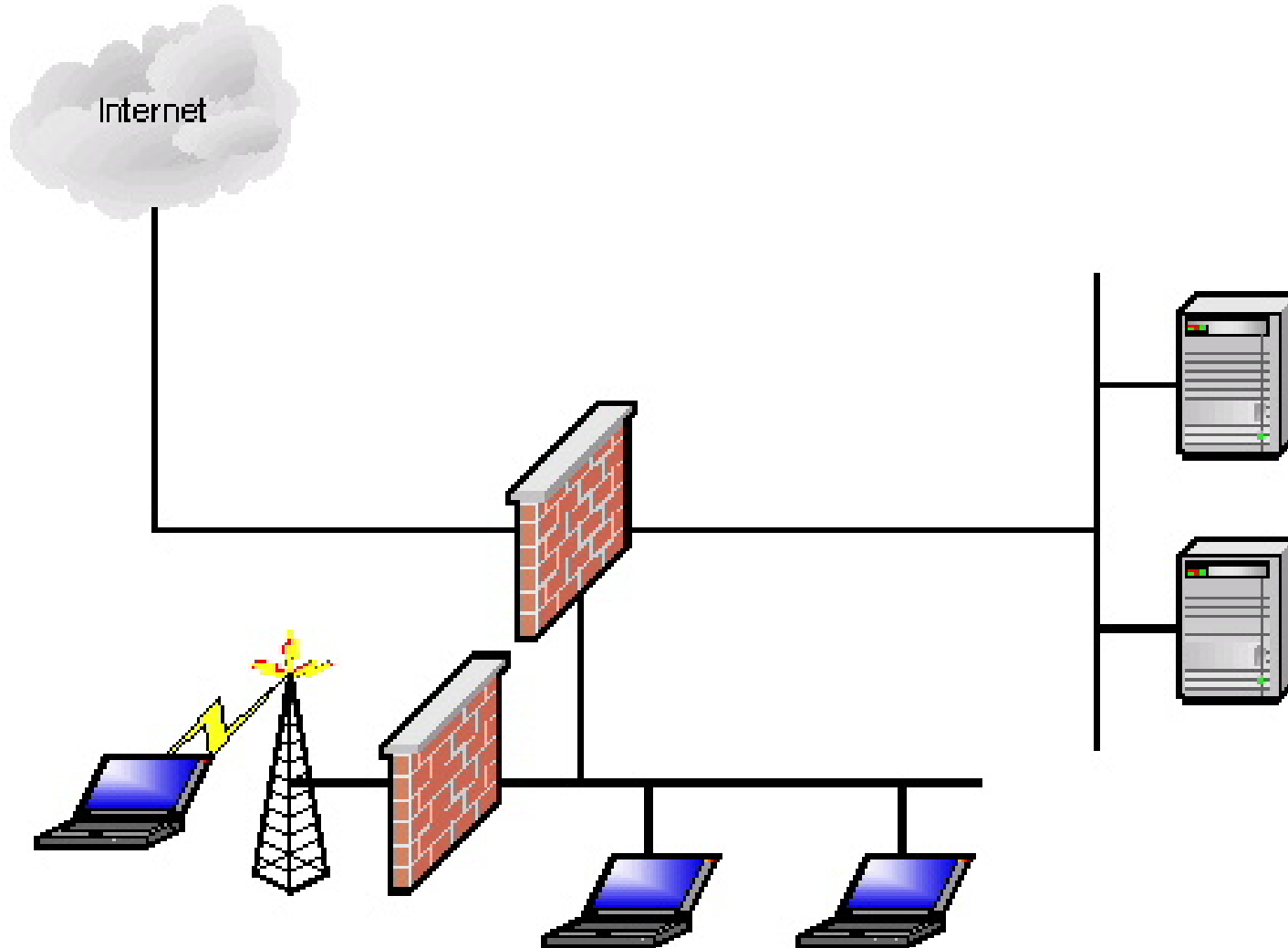
Security Topologies

- Network with Wireless DMZ (Multiple AP)



Security Topologies

- **Wireless separated via a dedicated Firewall**





3rd Party Security Devices



3rd Party Security Devices

- **What is a 3rd party device?**
 - Any device that has been added to the typical configuration of a wireless network.
 - A device that provides enhanced or additional security to the clients or data on the wireless network.

Authentications servers

Protocol analyzers

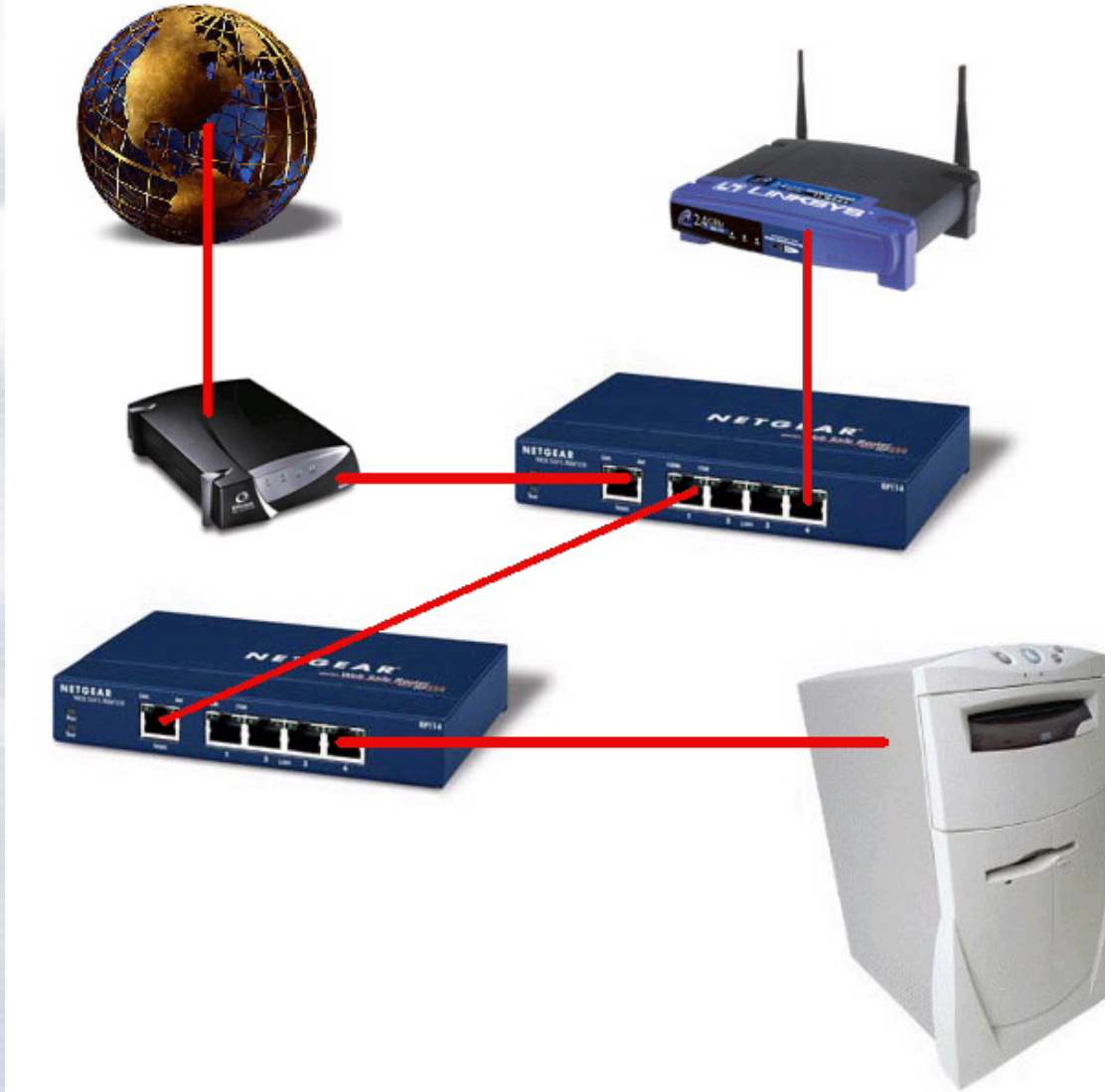
Enhanced data encryption

Proxy servers



3rd Party Security Devices

- Dual DSL Routers





3rd Party Security Devices

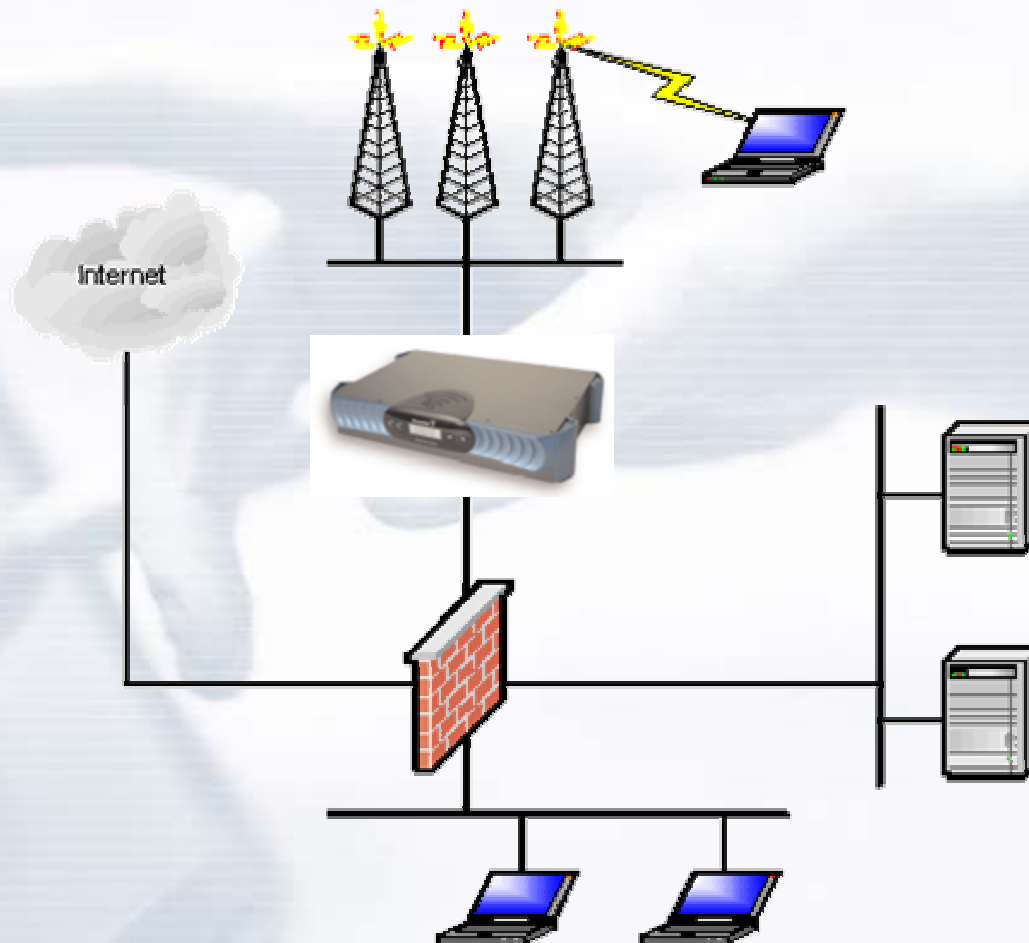
- **BlueSocket**
 - Redirects traffic to specific page upon connection
 - Authenticates users via SSL web interface
 - Standalone or integrated with Radius
 - Logs statistics for data transfer and sessions
 - Allows for secure data transmission via VPN
 - L2TP and PPTP





3rd Party Security Devices

- Topology example using BlueSocket



3rd Party Security Devices

Firebox SOHO 6 Wireless – WatchGuard

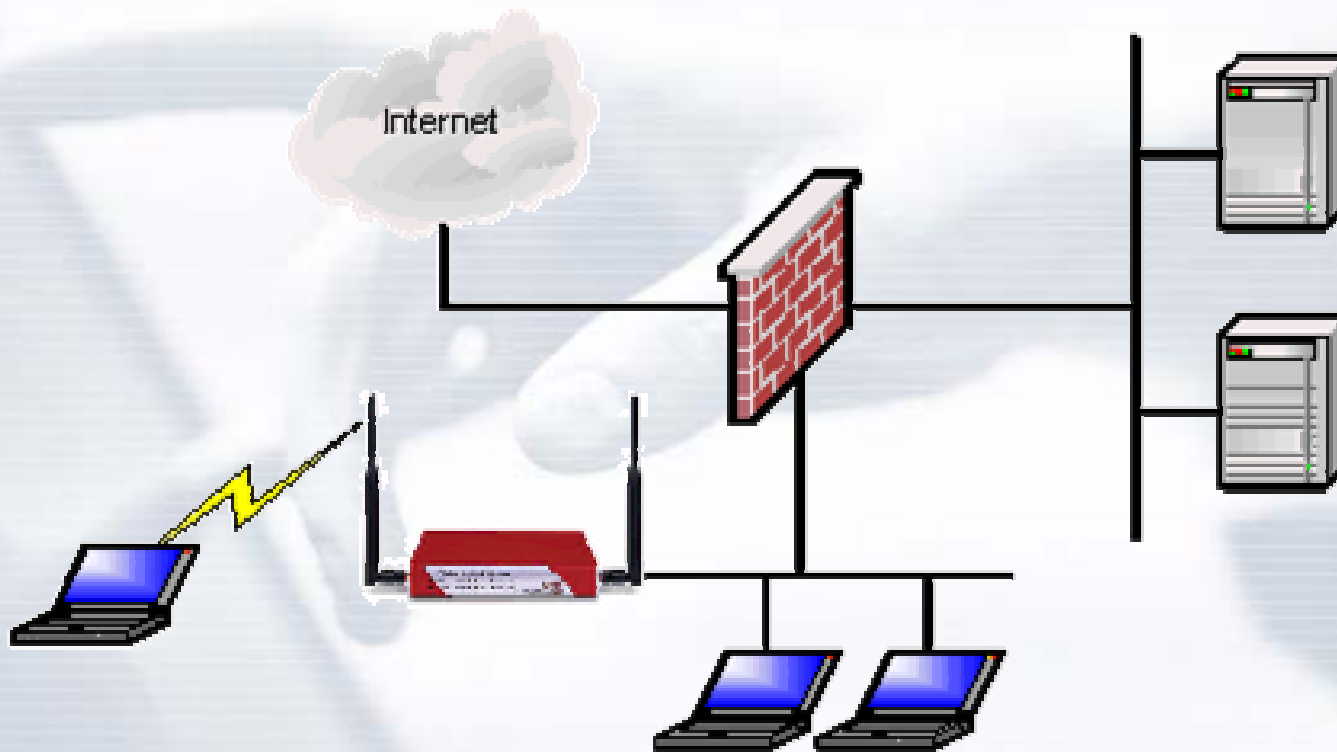
- **802.11b Access Point**
 - All the usual features and security options
 - ICSA Certified Firewall (3 Interface)
 - Stateful packet filtering
 - Full IPSec Encryption of wireless data





3rd Party Security Devices

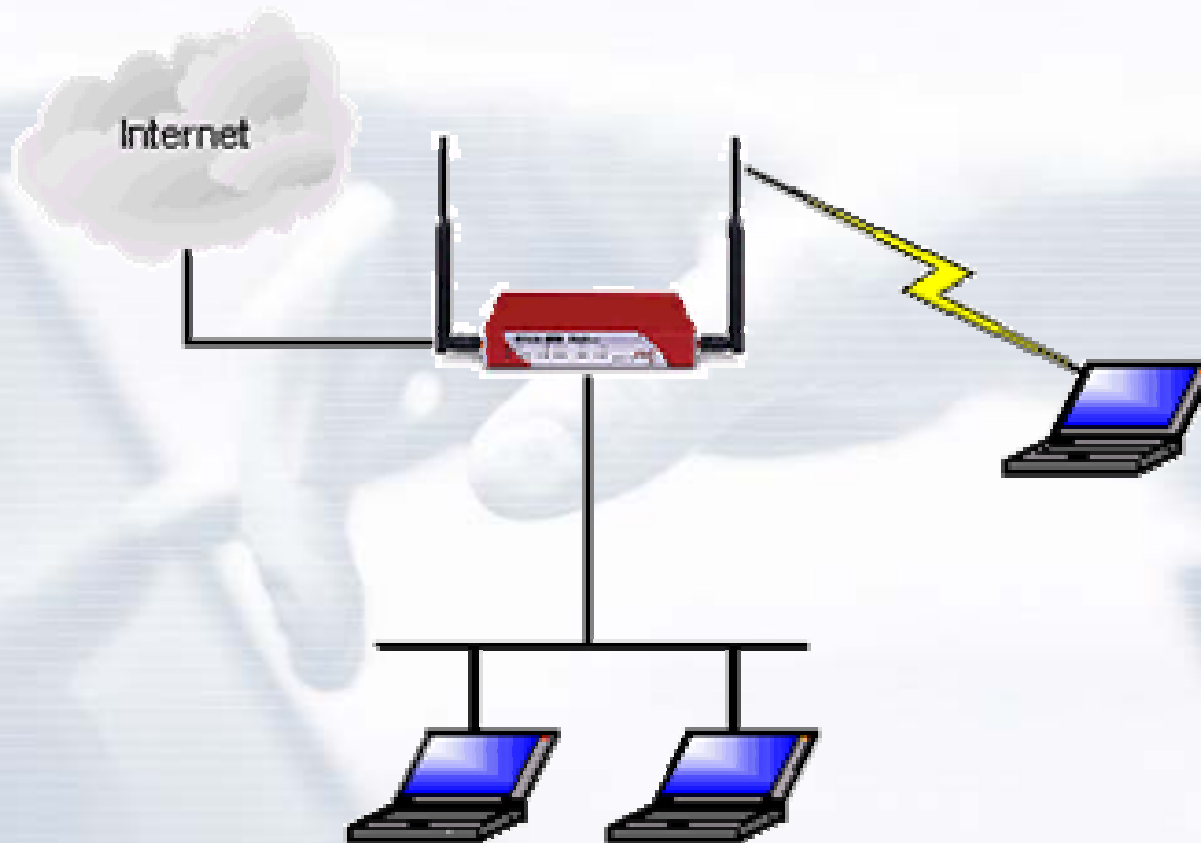
- Topology example using the SOHO 6 Wireless





3rd Party Security Devices

- **Topology example using the SOHO 6 Wireless**





Virtual Private Network



Virtual Private Network

- **Encrypts data stream**
- **Authenticates users**
- **Available in Windows 2000 Server**
 - From the MMC open Routing & Remote Access
 - XP and 2K have built in client support
- **Commonly supported on 3rd party devices**
 - Firewalls
 - SOHO 6 Wireless
 - BlueSocket



Virtual Private Network

- Topology example using Windows 2000 RRAS





Recommendations



Recommendations

- **Disable SSID Broadcast**
- **Restrict connections via MAC Address**
- **Encrypt data transmissions**
 - WEP / VPN
- **Look into low cost 3rd party security devices**
- **Don't be scared, just be smart...**



Brett L. Neilson
hamcom@brettneilson.com



Securing Wireless Networks On a Budget