Securing home network with ZyAir B-2000 gateway.
Junghoon Sung
GSEC Practical Assignment Version 1.4b Option 1
March 31, 2003

1. Abstract

This document describes the process of securing home network using ZyXel's ZyAir B-2000 Wireless Gateway. To effectively implement variety of features the device offers, understanding what to protect and defining clear objectives is critical. Thus, the first step of the process is conducting an audit of the resources and building inventory of resources to be secured. Then, paper looks at the various NAT settings the device supports and why to select NAPT for the mapping method and how to prove it is actually working. The document also covers how to define packet filtering rules to block malicious packets based on SANS Top ten blocking recommendations and why monitoring and logging packet filtering event is important in terms of incident prevention and analysis. Finally, defense-in-depth approach to secure wireless LAN utilizing various wireless security features such as disabling SSID broadcasting, MAC address filtering and WEP against masquerading and eavesdropping threats is explained.

2. What to Protect?

The internal network that will be secured by ZyAir B-2000 consists of one FreeBSD server, two company issued Windows based (XP and 2000 Professional) workstations and one RedHat Linux based personal laptop. The network is connected to the Internet 24/7 via ADSL and two static IP addresses are available from ISP.

The FreeBSD server is the only computer that will be turned on 24/7 and for this reason the server needs to be cautiously monitored and protected. The server will host a publicly accessible small personal website on the Apache web server and run ssh daemon for allowing remote access to the server.

Below is the output of sockstat command on the FreeBSD server. sockstat command lists open sockets. Option -4 tells the command to list only IPv4 sockets.

```
zk# sockstat -4
USER    COMMAND   PID   FD PROTO  LOCAL ADDRESS        FOREIGN
ADDRESS
root    sshd    11654    4 tcp4   192.168.1.23:22      192.168.1.35:1200
nobody  httpd    4191   15 tcp4   192.168.1.23:80      *:*
nobody  httpd    2267   15 tcp4   192.168.1.23:80      *:*
nobody  httpd    2264   15 tcp4   192.168.1.23:80      *:*
```

```
root     httpd     2257   15 tcp4   192.168.1.23:80       *:*
root     sendmail    82    4 tcp4   127.0.0.1:25          *:*
root     sshd        79    3 tcp4   *:22                  *:*
root     syslogd     70    4 udp4   *:514                 *:*
```

To verify sockstat results, nmap tcp/udp scan has been as well. The result of TCP scan result is in line with the result of sockstat command but UDP scan revealed that udp port 67, 137 and 138 are also open.

In summary, following ports need to be protected and monitored through packet filtering.

22/tcp	ssh server
80/tcp	web site hosting
67/udp	dhcpserver
137/udp	netbios-ns
138/udp	netbios-dgm
514/udp	syslog

All the company issued computers run Nortel VPN client through IPSec. Because of this, support of VPN pass-through feature is the one of requirements of the device I was looking for and ZyAir B-2000 meets the requirement.

In addition to that, the device must have modest wireless security features to protect the company laptop which will use wireless connection most of time.

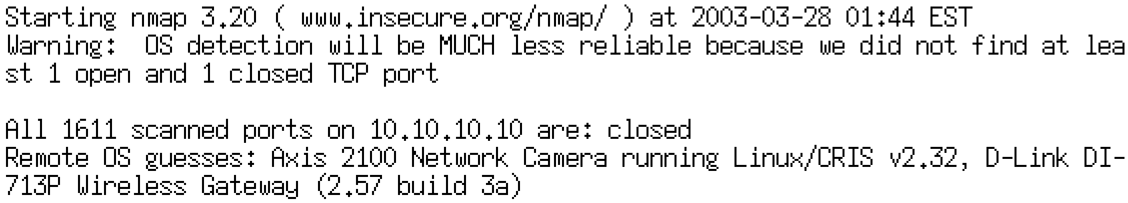
- Company desktop 1
  Windows NT Workstation.
  Remote access to company through VPN
- Company laptop
  Windows XP Professional
  Remote access to company through VPN
  Wireless LAN

The personal laptop is running Linux (RedHat 7.3) and is used for general computing needs: Internet surfing/shopping/banking, document creation and access to the FreeBSD server.

3. Configuration.

The first step of configuring ZyAir B-2000 should be hardening the device as much as possible. In order to properly secure the device, weak points must be revealed and make sure those areas are protected.

nmap scanning is one of ways to audit the device and found those weakness. To get better understanding of the device I am going to configure, the first scan ran was remote host identification scan using –O option. Below is the result of the scan.



```
Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-03-28 01:44 EST
Warning:  OS detection will be MUCH less reliable because we did not find at lea
st 1 open and 1 closed TCP port

All 1611 scanned ports on 10.10.10.10 are: closed
Remote OS guesses: Axis 2100 Network Camera running Linux/CRIS v2.32, D-Link DI-
713P Wireless Gateway (2.57 build 3a)
```

From this result, I (or would-be-attacker) learned a good piece of information which can be used as ground for further information about the gateway. After couple of quick Google searches, I found that the device is built on ETRAX 100LX chip running embedded Linux/CRIS kernel. Then, I ran another Google search using “ETRAX” and “ZyXel” as keywords and one of returned links leads to this interesting page: “CyXla’s passwords database file” located at http://www.cyxla.com/passwords/passwords.html, The link contains all the default passwords of various devices from different vendors using the same chip. Apparently, ZyXel is on the list and I found out default password “1234” before reading the manual.

Thus, changing the default password and disabling remote administrative access from WAN to the device should be the first step of the configuration.

3.1. Changing password.

System password can be changed at

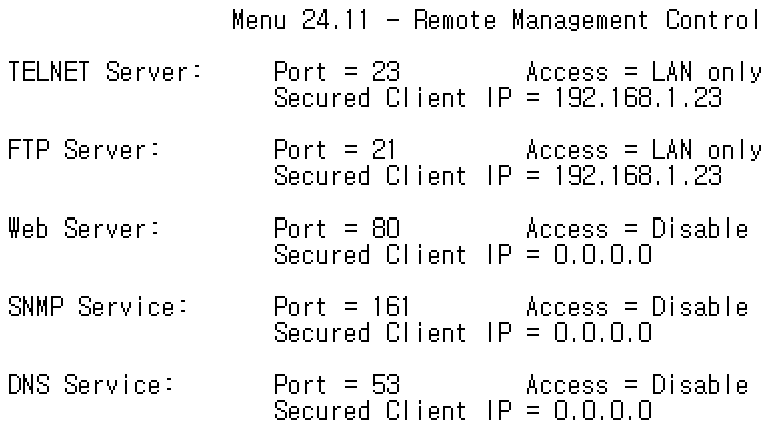
23. System Security -> 1. Change Password.

According to the manual, up to 30 characters including special characters can be entered. Apply strict rules to this password as it is root password. (It is root password indeed.)

3.2. Restrict configuration menu access

Administrative access to the B-2000 device can be configured at below location.

24.System Maintenance → 11. Remote Management.



```
                 Menu 24.11 - Remote Management Control

 TELNET Server:      Port = 23         Access = LAN only
                     Secured Client IP = 192.168.1.23

 FTP Server:         Port = 21         Access = LAN only
                     Secured Client IP = 192.168.1.23

 Web Server:         Port = 80         Access = Disable
                     Secured Client IP = 0.0.0.0

 SNMP Service:       Port = 161        Access = Disable
                     Secured Client IP = 0.0.0.0

 DNS Service:        Port = 53         Access = Disable
                     Secured Client IP = 0.0.0.0
```

Access to the Web interface, SNMP service and DNS server is disabled and only telnet and ftp* is allowed from the FreeBSD server (192.168.1.23).

This restriction on client IP provides additional layer of security of remote management access by providing additional authentication mechanism via the FreeBSD box; only users who have access to the FreeBSD box and know the ZyAir B-2000's password can access to the device and change the configuration settings. Otherwise, there would be no control over who can access to the gateway device. Also, ssh is used from end-to-end to access the FreeBSD server so there is no clear-text password passing around.

*Note: FTP is enabled for future firmware upgrade software upload to the device.

3.3. NAT (Network Address Translation) configuration.

ZyAir B-2000 supports two modes for NAT configuration: SUA (Single User Account) and Full Feature. SUA is ZyXel's implementation of NAPT (Network Access Port Translation, also called masquerading), which is one of the variation of the original NAT (RFC 1631). Full featured mode supports both static NAT and NAPT configuration for multiple IP addresses. Since two public IP addresses are available from the ISP, full featured NAT mode is selected.

Below lists various mapping options available for Full Featured mode.

Full Featured (NAPT + static NAT)

- Many-to-one (NAPT)
- Server (Port Forwarding)
- One-to-One (Static NAT)
- Many-to-many overload (multiple NAPT)
- Many one-to-one (multiple static NAT)

NAPT substitutes original private IP and port number with randomly generated port number and global IP on an outgoing packet to differentiate which hosts on the internal LAN the packet came from. Then, this mapping information is stored in the memory. When a resulting response arrives at the newly assigned port and IP pair, NAPT substitutes the public IP and assigned port number with the original private IP address and port number of the internal client where request was made.

Because of this translation, internal clients can share a single IP address and information about those clients can be hidden from outside. This port translation provides additional security layer by hiding port numbers of internal clients as well as by hiding IP address hiding through regular NAT functions.

Apparently, one-to-one mapping cannot hide original port numbers and proper port filtering rule must be designed and implemented to avoid security holes. Therefore, I decided to use two sets of Many-to-one mapping and assign public IP address to each mapping; one many-to-one mapping with port forwarding for the FreeBSD server and just many-to-one mapping for rest of workstations.

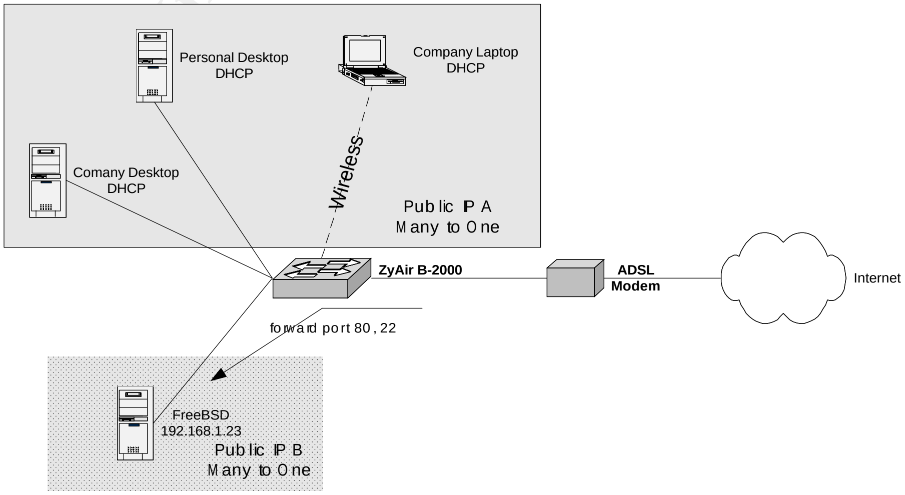
Three nmap scan has been run on different mapping settings and the scan has produced expected results.

1) Many to one(NAPT) setting actually blocks all the port
2) Server (port forwarding) actually opens specified port only.
3) One to One does not shield ports and exposes all the ports on the server.

These address mapping rules can be configured at:

15. NAT Setup → 1. Address Mapping Sets → 1. [setname]

Below diagram illustrated how the network is configured; one public IP is shared by workstations and the other IP is dedicated to the FreeBSD server where a small website is hosted.



3.4. Packet Filtering

ZyAir B-2000 provides two types of filter: Protocol (TCP/IP) filter and Generic (device) filter*. Protocol filter rules are applied to IP address and port numbers before NAT for outgoing packets and after NAT for incoming packets. In contrast, generic filter rules are applied at the interface to filter non-IP packets.

*Note: Call filter also can be configured if ISP requires login through (PPTP or PPPoE) to establish a connection. This requirement depends on what ISP and in this document call filters will not be covered, since my setup does not require login,.

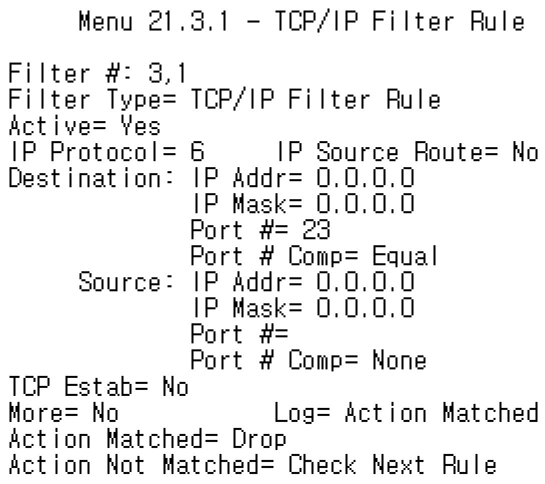
Each filter set can contain up to 6 filter rules and total 12 filter sets can be defined. Thus, 72 filtering rules can be configured on the device. One thing worth mentioning is both protocol and generic filter rule cannot be configured within the same set. Separate filter sets for each filter type must be created. Individual filter sets can be applied to both WAN interface and LAN interface as either input filter or an output filter.

ZyAir B-2000 comes with 3 preconfigured packet filters.

1) NetBIOS_WAN: TCP and UDP port 137 (NetBIOS name service), 138 (NetBIOS datagram service) and 139 (NetBIOS session service).
2) NetBIOS_LAN: A packet from source port 137 to destination port 53 for both TCP and UDP is blocked.
3) TEL_FTP_WEB_WAN: Blocks telnet(23), ftp(21) and http(80) ports. Due to the web site hosted on the FreeBSD server, port 80 blocking has been removed.

1) and 3) is applied to WAN interface as output filter and input filter respectively. Rule 2) is applied LAN interface as input filter to block any outbound packet matching the condition.

Below screen capture is an example of an active TCP/IP filter that drops and logs telnet connection attempt (TCP port 23) from outside WAN to the device. Any packet that does not match the rule will be forwarded to the next rule for further analysis. (as defined in Action Not Matched field.)



```
     Menu 21.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6     IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 23
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #=
             Port # Comp= None
TCP Estab= No
More= No           Log= Action Matched
Action Matched= Drop
Action Not Matched= Check Next Rule
```

TCP/IP filtering is based on the information in the IP header and TCP/UDP header. Each field in Menu 21.3.1 is rearranged under proper layer for better explanation.

IP layer:

- Source IP address
- Destination IP address
- IP Protocol is the IP Protocol identifies which identifies what protocol send data to IP. A value of 6 indicates TCP, 1 is for ICMP, 2 for IGMP and 17 for UDP.
- IP source route options checks whether a packet contains routing information about how it can reach its destination.

TCP/UDP layer:

- Source port
- Destination port
- TCP Estab field only applies when IP Protocol field type is TCP. By checking this, the rules will exam ACK bit and match if ACK bit equals 0, the first packet initiating a TCP connection.

If More filed is checked “yes”, next rule will be examined before action is taken. If it’s checked “no”, none of Action Matched or Action Not Matched will be available. Both Action Matched and Action Not Matched field has drop, forward and check next rule options.

SANS “How To Eliminate The Ten Most Critical Internet Security Threats” document lists commonly probed and attacked ports. Even NAPT supposed to block these ports inherently, active monitoring on the ports is critical to understand and detect malicious attempts against the network. With logging functionality, packet filtering can be used to detect outside the NAPT network activity. For this reason, logging is critical.

Logging feature can be configured to log activities based on whether that activity matches the rule or not. In this example, any incoming packet head to port 23 will be dropped and logged. Detail information on what's logged and how to configure syslog daemon on the FreeBSD box is presented in next section.

Up to 4 filter sets, separated by commas, can be applied to an interface. Due to the limitation of number of filter set that can be applied to an interface., it is not possible to block and monitor all the recommended ports.

Total 23 filter rules have been defined under 4 filter sets and all the sets have been applied to the WAN interface as ingress filter. It is important to apply those filter sets to the target interface after design the rules. Filter set can be applied to WAN interface from Menu 11.5 Remote Node Filter and LAN interface from Menu 3.1 LAN Port Filter Setup. Multiple filter sets can be applied by separate them by comma with correct order. Any packets matching the criteria will be dropped (except ssh connection) and logged on the syslog server.

1) SPOOD (6 rules)
   Any packets with IP source route check will be dropped.
   Source IP numbered as below will be dropped.
   - 255.255.255.255
   - 127.0.0.1
   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/32
2) LOGIN (6 rules)
   Based on destination port: telnet (23/tcp), FTP (21/tcp), Netbios(139/tcp) rlogin (512/tcp, 513/tcp, 514/tcp)
3) DNS_MAIL_FINGER (6 rules)
   SMTP – (25/tcp)
   finger (79/tcp)
   DNS – (53/udp, 53/tcp)
   netbios-ns 137/udp
   netbios-dgm 138/udp

4) MISC (5 rules)
   Ports below 20 for tcp and udp.
   syslog (514/udp)
   dhcpserver (67/udp)
   ssh (22/tcp, forward)

3.5 Logging

Logging is associated with each individual packet filter rule. When there is an incoming or outgoing packet that matches or does not match a filter rule, information about that packet can be forwarded and logged to remote syslog daemon.

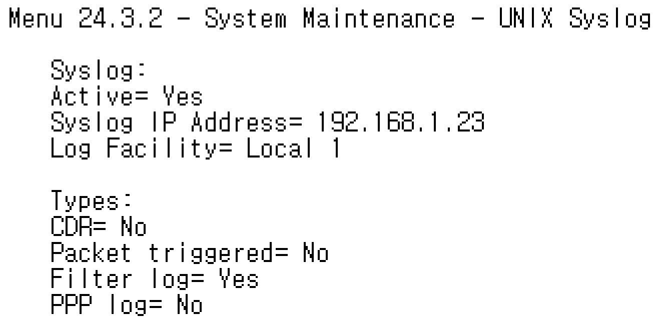
Logging feature is important because logs can be used to detect unusual activities or intrusion attempts and to determine how an intrusion happened.

ZyAir B-200 can forward 4 types of system activity to syslog daemon.

- Call Detail Record: Data phone line activity
- Packet Triggered: The first 48 bytes and protocol type of triggering packet.
- Filter Log: Filters set to log on filter configuration menu.
- PPP Log: PPP related events.

Neither PPP over Ethernet nor dialup connection via the device is used within the network, the logs generated from filter are the only interesting data we need to capture and monitor.

On ZyAir B-2000 – Below screen capture illustrates how to configure syslog client on the device. Just assign IP address of syslog server and select log facility from 1-7.



```
Menu 24.3.2 - System Maintenance - UNIX Syslog

   Syslog:
   Active= Yes
   Syslog IP Address= 192.168.1.23
   Log Facility= Local 1

   Types:
   CDR= No
   Packet triggered= No
   Filter log= Yes
   PPP log= No
```

On FreeBSD server (require root access)

1) Start option for syslogd has to be changed. By default, syslogd on FreeBSD start with –s option, operates in secure mode. In order to allow remote client to log into syslogd, this option needs to be disabled. Disabling –s option is less secure but the benefit overrides the risk. Removing –s option opens udp port 514 for syslogd.

   To change this, remove –s from below line in /etc/rc.conf file.

   ```
   syslogd_flags=" "
   ```

   After change, the server needs to be rebooted or syslogd has to be killed and restarted.

3) Since we are going to use Local 1 facility to log the data, following line needs to be added to /etc/syslog.con file.

```
local1.*                              /var/log/zyxel.log
```

4) Under /var/log directory, create zyxel.log file.

```
touch /var/log/zyxel.log
```

5) Change ACL of the file to only allow root to read the file.

```
chmod 600 /var/log/zyxel.log
```

6) On /etc/newsyslog.conf, add below line.

```
/var/log/zyxel.log                600  5    100  *     Z
```

Below is an actual log from the server:

```
Mar 31 15:27:48 zkun zkun: Jan 04 2000 14:29:15 IP[Src=61.x.x.x Dst=66.x.x
.x UDP spo=01026  dpo=00137]}S05>R05mD
```

For more information about syslog, please refer to man page of syslog.conf and syslogd.

3.6. Wireless LAN security

ZyAir B-2000 provides following wireless security features:

1) Custom Service Set Identifier (SSID): Can define SSID up to21 characters using 0-9, a-z, A-Z, ‘-‘ or ‘_’.
2) Disable SSID broadcasting
3) Wired Equivalent Privacy (WEP): 64 or 128 bit key length. Can store up to 4 keys for easy key rotation.
4) MAC address filtering
5) IEEE 801.x authentication: Supports internal

None of above technologies is perfect. However, securing wireless is an application of defense-in-depth. Multiple layers of security feature modestly protect the network against masquerading and eavesdropping threats.

Customizing SSID settings are considered the first level security. Most of default SSID for any devices can be easily guessed and available from the Internet. Thus, default SSID should be changed to something a little bit harder to guess. The SSID should be treated like password.

Additionally, SSID broadcasting must be disabled to prevent strangers from detecting the SSID of my Access Point (AP). With Network Stumbler, I verified that disabling SSID broadcasting actually turns off the beacon transmitting.

However, hiding customized SSID by no means mitigate masquerading threats completely. Anyone who can guess correct SSID can connect to the AP. Thus, further security measures must be implemented.

WEP is one of solutions to the problem; anyone who wants to access the network must know the shared key; knowing SSID alone is not enough. On ZyAir B-2000, 4 shared keys can be stored. This is a convenient feature since frequent rotation of WEP key is critical to protect against key cracking attempt. AirSnort is one of tools that can decrypt WEP key.

If WEP key is decrypted, the protection against both eavesdropping and masquerading is compromised. MAC address filtering, disabling DHCP server and IEEE 802.x specification can provide more security layers against masquerade threats in addition to WEP.

To protect against eavesdropping threat, it is recommended to utilize higher level end-to-end encryption such as VPN. Fortunately, the company issued laptop has VPN client and I am using this VPN connection to connect to the company's network and proxy.

In regards to IEEE 802.x, there's one catch about IEEE 802.x authentication support on ZyAir B-2000. Since there is no available server to install "RADIUS" authentication server within my network, I tried to configure the internal authentication server that is already embedded on the device.

The internal authentication server requires a client to use MD5/CHAP encryption and the original built-in 802.x that Windows XP comes with use MD5/CHAP encryption support. However, after installing XP Service Pack 1, this support was removed and only PEAT authentication is supported. For this reason, IEEE 802.x is not utilized in the network.

Reference

ZyXel Communication Corporations, "ZyAir B-2000 Support Notes: ZyNOS Faq" V3.50 HB.0. 1 Oct. 2002. URL: http://www.zyxel.com/support/supportnote/ZyAIR_B2000/faq/ZyNOS_faq.htm (13 Mar. 2003).

Hasenstein, Michael. "IP Network Address Translation." 1997. URL: http://www.suse.de/~mha/linux-ip-nat/diplom/nat.html (15 Mar. 2003).

Smith, M. and Hunt, R., “Network Security using NAT and NAPT" 27-30 Aug. 2002.
URL: http://www.cosc.canterbury.ac.nz/research/RG/i-et_security/SmithHunt.pdf (12 Mar. 2003)

CERT Coordination Center. "Packet Filtering for Firewall Systems." 6 Feb. 2002. URL: http://www.cert.org/tech_tips/packet_filtering.html (19 Mar. 2003).

Tiedemann, Paul. "Top Ten Blocking Recommendations Using ipchains." 8 Aug. 2000. URL: http://www.sans.org/rr/firewall/blocking_ipchains.php (29 Mar. 2003).

CERT Coordination Center. “Configure firewall logging and alert mechanisms.” 1 May 2001. URL: http://www.cert.org/security-improvement/practices/p059.html (20 March 2003).

Constantine, Carl. “Tools of trade: part 3.” 13 Jul. 2001. URL: http://linux.oreillynet.com/pub/a/linux/2001/07/13/tools_trade_three.html (20 Mar. 2003)

Dismukes, Trey. “Ars Technica: Wireless Security Blackpaper.” 1.0. 18 Jul 2002. URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html (20 Mar 2003)

Chapman, D. Brent. Building Internet Firewalls. O'Reilly & Associates, Nov. 1995. Chapter 6.