Global Information Assurance Certification Paper

Securing Cisco HomeOffice / Small Business Broadband Routers (2-interfaces)

Albert Wolfkiel
September 17, 2002
SANS GSEC Practical, Version 1.4, Option 2

1.0 Abstract

This paper shows how the author secured a Cisco 806, broadband router, for use in a Home Office / Small Business (HO/SB) environment. (The configuration should work for any recent Cisco two interface router with the firewall feature set.) A “Before” section details how basic security is provided with the router out of the box. Additional requirements including DHCP server, Network Time Protocol (NTP), Syslog, and NAT to inside services complete the typical requirements of a HO/SB configuration. Security is layered on with Access Control Lists (ACLs), Internet Protocol Security Virtual Private Network (IPSec VPN) Server, Context Based Access Control (CBAC), and various configuration recommendations from well-known security organizations including the National Security Agency (NSA), SANS SCORE, and Cisco SAFE. The “during” section takes advantage of non-core features of the Cisco Internet Operating System (IOS) including the Firewall (FW), Triple DES (3DES), and Intrusion Detection (IDS) feature sets found in IOS 12.2.8YJ. Finally, the “After” section outlines what has been accomplished, reviews challenges encountered, and attempts to assess residual risk. The final section “Future Work” identifies where future efforts could extend or complement this paper.

While significant challenges were encountered to meet the special needs of a HO/SB environment where a single router with two interfaces acts as the gateway, security overall has been improved to meet most Internet threats.

2.0 Introduction

The author is a part time instructor for the Cisco Academy at Oxnard Community College in California. The Cisco Academy teaches the core Cisco certifications Cisco Certified Networking Associate (CCNA) and Cisco Certified Networking Professional (CCNP). The CCNA and CCNP, in their current generations, cover very little security-related information (just ACLs). The Cisco Academy recently made available to students, at reduced cost, 806 Broadband routers, suitable for Digital Subscriber Line (DSL) or Cable Modem access. The Cisco Academy does not prepare students to configure these routers with Internet class security. Through this effort, the author is attempting to provide the information necessary to support students and others who want Internet class security while maintaining HO/SB type services.

The scope of this paper will not address many abilities of the higher end features of IOS routers or higher end hardware firewalls. These features are typically demanded by medium sized or enterprise businesses. These features

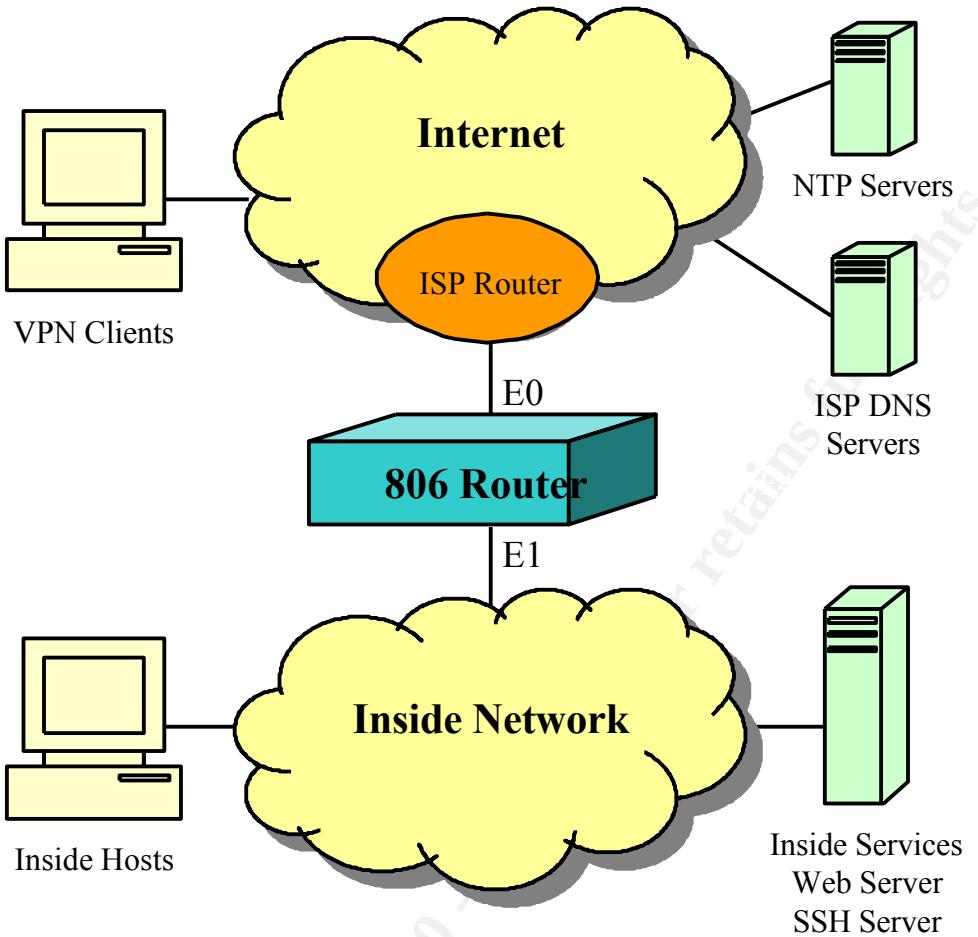
include: BGP, Multi-ISP access, DMZs, anything that requires more than two interfaces on the router, VLANs, inter-VLAN routing, extranets, router-to-router VPNs, routing of any kind, multicast (allowing), SNMP management (allowing), external authentication/authorization/accounting (RADIUS/TACACS), and sophisticated QOS.

This paper will also not address the multitude of other security aspects of a HO/SB network including: Personal Firewalls, syslog server setup, reviewing logs generated by syslog and Operating Systems, backups, and wireless networking--although the IPSec VPN server could be used as part of this solution.

The Pictures 1 and 2 below show how the 806 is hooked up at the authors home. Drawing 1 shows how the 806 is connected to the inside network and the Internet. The cabling to the author's roommates and the author's computers come in from the attic above to the patch panel. A pair of 10/100 switches, on top, aggregates the inside network into the Ethernet 1 (E1) interface (Inside) on the 806. The DSL modem on the bottom connects to the E0 interface (Outside) on the 806. Power is supplied by the small UPS on the left, and the telephone patch panel on the right provides the DSL input. The white cable is unconnected and previously connected to a cable modem.

Picture 1: Front view of Cisco 806 and Other Network Gear

Picture 2: Top view of Cisco 806 and Other Network Gear



D
n
N

rawi
g 1:
etwo

rk Diagram

The author modified the stock 806 router with an additional 16Mb of RAM necessary to run the 12.2.8YJ1 IP Plus/FW 3DES feature set. For simplicity, improved security, and clarity in this paper, the author is using three public static IP addresses. Most of this configuration could be done with a more typical single static IP, or even dynamic IP.

Interfaces E0 and E1 are swapped when compared to the default 806 configuration. E0 is the Internet interface and E1 is the inside network interface. The author has more than four devices on the inside and needs a larger hub/switch there, and the author has one additional outside device. Swapping the default uses of the Inside and Outside interfaces allows saving hubs by having the router perform outside hub duty.

Throughout the rest of this paper the following private internal IP addresses are used:
An inside DNS server at 192.168.1.1 (Internally Accessible).

An inside Web server at 192.168.1.1 (Internally Accessible).
An inside WINS server at 192.168.1.1 (Internally Accessible).
An inside DNS server at 192.168.10.1 (Externally Accessible).
An inside Web server at 192.168.10.1 (Externally Accessible).
An inside SSH server at 192.168.10.1 (Externally Accessible).
An inside Microsoft Windows 2000 (W2K) Remote Access Server at 192.168.10.1 (Externally Accessible).
Inside Router Addresses at 192.168.1.254 and 192.168.10.254.
Inside DHCP Range: 192.168.1.65 through 192.168.1.191.
IPSec VPN Client Address Range: 192.168.2.1 through 192.168.2.250.

In the author's network, there is a Windows 2000 Server running all services with a primary IP address of 192.168.1.1 and a secondary IP address at 192.168.10.1. An eventual migration will take place and external services will be run on either a separate machine or a virtual machine server.

The configurations in this paper use the following sanitized public IP addresses:
<ISP Router> This is the ISP's upstream router.
<ISP DNS Server1> This is the ISP's DNS server.
<ISP DNS Server2> This is the ISP's DNS server.
< Public IP Address used by Router Itself > This is the Internet address used to directly access the router.
<Public IP address used by inside hosts> This is the Internet address used by the router to NAT the inside hosts.
<Public IP address used for inside services> This is the Internet address used by the router to provide external services.
<Internet Remote Access IP> This is an IP address of a computer somewhere else on the Internet that is convenient for remote router maintenance during DOS attacks on the router VTY ports (Telnet/SSH).

This configuration should be tested in a lab environment (InsideTestPC<->Crossover<->Router<->Crossover<->OutsideTestPC) before it is connected to the Internet. Tests should include a port scan from the outside. Functional testing should include checking that all services can be reached from the outside and that inside hosts can reach outside hosts over protocols.

It is possible the author may update this paper as new features become available or new capabilities are added. Look for updates in the files section of the Southern California Cisco Users Group (SCCUG) message board: http://groups.yahoo.com/group/SCCUG.

Before any of these configurations are installed into a router, ensure that the router does not have old configuration commands present by executing the following commands:

Router**#erase startup-config**

Router#**reload**

Copy the configuration below into an editor--such as Notepad--put localized information into areas where <parameters> are needed and then use a cut and paste operation to put the configuration into the router. Always remember to save your configurations:

Router#**copy running-config startup-config**

3.0 A Configuration to Serve Home Office / Small Business (HO/SB) Needs (no added security) - "Before"

The following list defines the HO/SB features that the author thought would be valuable in his network and will likely be in demand by others.

Logging to an inside host (a Win2K box running Kiwi Syslog Server)
NTP Time Synchronization on the router for Logging
NAT to allow multiple inside hosts to share a single IP address.
Port Forwarding to inside hosts to support public services (Web, SSH, DNS, W2K Remote Access)
Access to inside services Web that should not be publicly available (unsecured for now - will be accessed by IPSec VPN later)
DHCP Server
DHCP MAC Mapping (samples for Windows & non-Windows hosts)
External router maintenance access (Telnet at this point)
Some basic QOS to keep the file sharing applications under control (Kaza, etc.)

Configuration 1 below implements the HO/SB features desired without any additional security. It is here for reference only and should not be used in an Internet connected router without modification. As features are implemented they are documented with comments in-line using an exclamation point (!) as the first character. Comments are also color coded blue.

Configuration 1: Before Config

```
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname MyHome
! The following command keeps router messages to the console
!   down to only the important ones.
logging console notifications
!
```

```
enable secret 5 <password-md5-hash>
! The following command creates a user with a relatively insecure type 7
!   cipher.
username user password <password>
! The following commands set the local time zone, daylight savings time,
!    and GMT offset.
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip domain-name sanitized.net
!The following commands allow the router itself to resolve names to IPs.
ip name-server 192.168.1.1
ip name-server <ISP DNS Server1>
ip name-server <ISP DNS Server2>
! The following lines speed up DHCP address assignment to hosts
!   since we expect any computers with conflicting IPs to answer
!   quickly and with no packet loss in a small HO/SB network.
ip dhcp ping packets 1
ip dhcp ping timeout 100
! The following DHCP pool determines the default settings for all of the smaller
!   individual MAC address mapping pools below and for the non-MAC matched
!   clients.
ip dhcp pool AtHome
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.254
   dns-server 192.168.1.1 <ISP DNS Server1> <ISP DNS Server2>
   domain-name sanitized.net
   netbios-name-server 192.168.1.1
   netbios-node-type h-node
   lease 5
ip dhcp excluded-address 192.168.1.192 192.168.1.255
ip dhcp excluded-address 192.168.1.0 192.168.1.64
! Sample windows host MAC Map
ip dhcp pool Albert
   host 192.168.1.100 255.255.255.0
! notice the leading 0x01 for windows machines on Ethernet
   client-identifier 0100.9027.0000.00
   client-name Albert
! Sample non-windows MAC Map
ip dhcp pool Joe
   host 192.168.1.90 255.255.255.0
   hardware-address 0010.0000.0000
   client-name Joe
!
interface Ethernet0
 description "Internet - Outside"
 ip address <Public IP Address used by Router Itself> 255.255.255.0
 ip nat outside
!
interface Ethernet1
 description "AtHome - Inside"
 ip address 192.168.10.254 255.255.255.0 secondary
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
```

```
! The following command restricts the upload bandwidth for an inside File Sharing host
!   which for instance might be running Kaza. No restriction on download.
 rate-limit input access-group 188 8000 1500 2000 conform-action transmit exceed-action
drop
!
ip nat pool NAT-Pool <Public IP address used by inside hosts> <Public IP address used by
inside hosts> netmask 255.255.255.0
ip nat inside source list NAT-Authorized-Out pool NAT-Pool overload
! The following commands create paths from the public IP to the inside services.
!   Web, SSH, DNS, and W2K terminal server.
ip nat inside source static tcp 192.168.10.1 80 <Public IP address used for inside services>
80 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for inside services>
22 extendable
ip nat inside source static tcp 192.168.10.1 53 <Public IP address used for inside services>
53 extendable
ip nat inside source static udp 192.168.10.1 53 <Public IP address used for inside services>
53 extendable
ip nat inside source static tcp 192.168.10.1 3389 <Public IP address used for inside
services> 3389 extendable
! The following commands map non-standard ports to the SSH server on the inside.
!   This is done so that a connection can be made when the SSH outbound port is blocked
!   by a remote host network.
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for inside services>
110 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for inside services>
21 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for inside services>
443 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for inside services>
23 extendable
! The following maps all unmapped ports and ICMPs from the outside IP to the web
   server inside. This allows the inside hosts to get an ICMP redirect from the router.
   The redirect directs inside hosts to the inside web page IP address.
   Unused ports are blocked via ACL.
ip nat inside source static 192.168.10.1 <Public IP address used for inside services>
!
ip route 0.0.0.0 0.0.0.0 <ISP Router>
!
ip access-list extended NAT-Authorized-Out
 permit ip 192.168.1.0 0.0.0.255 any
!
! The logging commands send everything to the syslog server.
logging trap debugging
logging 192.168.1.1
logging buffered 16384
!
! This ACL is used to identify traffic to rate limit on Interface E1.
access-list 188 permit tcp any any eq 6699
!
line con 0
! This line causes the router to keep commands together on the command line
!   as they are typed in. Status messages don't split up your typing. Beware, this will
!   put router prompts into the syslog output which can cause problems with syslog
```

```
!   analysis tools.
 logging synchronous
 stopbits 1
line vty 0 4
 login
 password <password>
!   Set the timeout for remote access to 5 minutes of no activity.
 exec-timeout 5 0
 logging synchronous
!
scheduler max-task-time 5000
! Prevents the router from spending too much time handling interrupts from network
!   interfaces and not getting any work done.
scheduler interval 500
ntp server <Internet NTP Server1>
ntp server <Internet NTP Server2>
```

4.0 Cisco IOS Security Improvement Process - "During"

4.1 Context Based Access Control (CBAC)

Use CBAC for both inside to outside and outside to inside. CBAC is resource intensive. Cisco warns to ensure that your router has the resources to do CBAC. (An 806 has a 50MHz RISC processor and it is more than equal to the task.) CBAC default values should also be changed to match NSA recommendations.

The CBAC commands are:

```
ip inspect audit-trail
ip inspect udp idle-time 15
ip inspect dns-timeout 7
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect name cbac-in-to-out cuseeme timeout 3600
ip inspect name cbac-in-to-out ftp timeout 3600
ip inspect name cbac-in-to-out h323 timeout 3600
ip inspect name cbac-in-to-out http timeout 3600
ip inspect name cbac-in-to-out netshow timeout 3600
ip inspect name cbac-in-to-out rcmd timeout 3600
ip inspect name cbac-in-to-out realaudio timeout 3600
ip inspect name cbac-in-to-out rtsp timeout 3600
ip inspect name cbac-in-to-out smtp timeout 3600
ip inspect name cbac-in-to-out sqlnet timeout 3600
ip inspect name cbac-in-to-out streamworks timeout 3600
ip inspect name cbac-in-to-out tcp timeout 3600
ip inspect name cbac-in-to-out tftp timeout 30
ip inspect name cbac-in-to-out udp timeout 15
ip inspect name cbac-in-to-out vdolive timeout 3600
ip inspect name cbac-in-to-out fragment maximum 256 timeout 1
! ip audit commands require IDS feature set.
ip audit attack action reset
ip audit notify log
```

ip audit po max-events 100

interface Ethernet0
ip access-group Allowed-In in
! As packets go out matching holes are created in inbound ACL.
ip inspect cbac-in-to-out out

ip access-list extended Allowed-In
deny ip any any log

However, now that we have in inbound access list, we need to open holes to all the services inbound that we are using:

! Whenever you are modifying an ACL make sure to delete the old one first.
! Remember if you are configuring remotely to take it off the interface too.
! Otherwise you will lock yourself out of your router. :)
no ip access-list extended Allowed-In
ip access-list extended Allowed-In
! Deny "Martian" IPs. "Not of this world."
! This deny covers broadcasts, 255.255.255.255 too.
deny ip 224.0.0.0 31.255.255.255 any log
deny ip 0.0.0.0 0.255.255.255 any log
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 169.254.0.0 0.0.255.255 any log
deny ip 192.0.2.0 0.0.0.255 any log
deny ip <Public IP Address used by Router Itself> **0.0.0.0 any log**
! Allow DNS lookups to come in to DNS server.
permit udp any host <Public IP address used for inside services> **eq domain**
! Allow access to the web server.
permit tcp any host <Public IP address used for inside services> **eq www**
! Allow access to the inside SSH server.
permit tcp any host <Public IP address used for inside services> **eq 22**
! Allow access to the W2K terminal server.
permit tcp any host <Public IP address used for inside services> **eq 3389**
! Allow access to the inside SSH server alternate ports.
! Allow NTP replies back in to the router. CBAC doesn't create holes for
! communication initiated from the router itself.
permit udp any host <Public IP Address used by Router Itself> **eq ntp**
! Allow DNS replies back in to the router. CBAC doesn't create holes for
! communication initiated from the router itself. (It turns out in my case
! that my ISPs two DNS servers are an odd and even pair so a wildcard
! mask of 0.0.0.1 covers both of them.)
permit udp <ISP DNS Server1> **0.0.0.1 eq domain host** <Public IP Address used by Router Itself>
! Allow Telnet in to the router for remote configuration.
permit tcp any host <Public IP Address used by Router Itself> **eq telnet**

! Before any ICMP is allowed in to router, hosts, or services redirects are blocked.
deny icmp any any redirect
! Allow all ICMP replies to come back to inside hosts.

```
 permit icmp any host <Public IP address used by inside hosts>
! Allow all ICMP in to router.
 permit icmp any host <Public IP Address used by Router Itself>
! Allow pings and packet-too-big ICMP messages in to inside services.
 permit icmp any host <Public IP address used for inside services> echo
 permit icmp any host <Public IP address used for inside services> packet-too-big
 deny   ip any any log
```

4.2 Cisco Express Forwarding (CEF)

CEF provides some built in security abilities (checking to make sure that packets source IP matches the interface it comes from) and speeds things up. CEF should only be turned off when debugging is required. CEF doesn't support debugging and packets will bypass debugging when CEF is enabled.

```
ip cef
interface Ethernet0
 description "Internet"
 ip verify unicast source reachable-via rx allow-default
!
interface Ethernet1
 ip verify unicast source reachable-via rx
```

4.3 Disable Cisco Discovery Protocol (CDP) generally and on external interfaces

This is the only router in the network, so having CDP available for other than troubleshooting between routers is not necessary.

```
no cdp run
interface Ethernet0
 description "Internet"
 no cdp enable
!
interface Ethernet1
 description "Inside AtHome"
no cdp enable
```

4.4 Disable the router's built in HTTP server

This closes an avenue for future attacks. HTTP server is unnecessary with Secure Shell (SSH) access to the router.

```
no ip http server
```

4.5 Disable Source Routing, Classless Routing, and the Bootp Server

In accordance with NSA best practice recommendations the bootp server is only used when a serial interface connection is required. It may be needed for routers that use other than Ethernet to the Internet.

```
no ip bootp server
no ip classless
no ip source-route
```

4.6 Block Unreachable and redirects messages, turn off Proxy ARP, turn on accounting access violations.

In accordance with NSA and Cisco best practice recommendations.

```
interface Ethernet0
 description "Internet"
! This command enables IP accounting on an interface with the ability
    to identify IP traffic that fails IP access lists.
 ip accounting access-violations
 no ip redirect
 no ip unreachables
 no ip proxy-arp
!
interface Ethernet1
 description "Inside AtHome"
 ip accounting access-violations
 no ip proxy-arp
 no ip redirect
 no ip unreachables
```

4.7 ACL on VTY prevents Denial of Service (DOS)

To prevent a DOS to VTY ports use an access list on at least one of the VTY sessions.

```
line vty 4
 access-class 2 in
access-list 2 permit <IP of computer or computers to get in during DOS attack>
```

4.8 IPSec Tunnel

For VPN access IPSec is widely regarded as the best option. Cisco IOS 12.2.8YJ supports the Cisco Unity 3.x IPSec client (and the Microsoft IPSec client?). If the clients must be able to bypass the VPN tunnel best practices require that they run a host based firewall. (The unity client has one built in to the software but the VPN server cannot force it on.) Best practice is to force the

VPN client to send all traffic into the VPN. When all traffic from the client is routed into the VPN, clients can still access the Internet from behind the corporate firewall (NAT). The VPN access list can also be used to determine if VPN clients can talk to each other.

The configuration below uses route maps and loopback interfaces to route inbound IPSec packets bound for the Internet back out to the Internet. IPSec packets enter the router encrypted. They are then decrypted and routed again back in to the E0 (Internet) interface through the Allowed-In ACL. Internet bound IPSec packets are then route mapped to Loopback 0. When the packets reenter the router they are coming in on a NAT inside interface. The packets are then the address translated by the router and route mapped to Loopback 209, a NAT outside interface. When the packets reenter the router from Loopback 209 they create a return path firewall hole via reflexive access list IPSec-Reflexive. The packet then is routed normally and leaves the router through interface E0, to the Internet.

```
crypto isakmp policy 3
! Sets encryption to Triple DES.
 encr 3des
 authentication pre-share
 group 2
! Security Association is 12 Hours.
 lifetime 43200
!
! Give the group name and group key (password) to IPSec clients.
crypto isakmp client configuration group 806VPNClient
 key <group key>
 dns <DNS Server 1 IP> <DNS Server 2 IP>
 wins <WINS Server IP>
 domain <local domain>
 pool VPNIPPool
! If split tunneling will be allowed, it is enabled here with: “acl <extended acl number>”
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
! This loopback is used if split tunneling is not allowed, yet clients will
!   be allowed to access the Internet from inside the firewall.
interface Loopback0
 description Inside Interface to Originate Outbound IPSec Packets
 ip address 192.168.100.254 255.255.255.0
 ip nat inside
 ip policy route-map l0
```

```
!
! This loopback is used if split tunneling is not allowed, yet clients will
!   be allowed to access the Internet from inside the firewall.
interface Loopback209
 description To pick up IPSec Outbound Reflexive-List Entries
 ip address 192.168.209.254 255.255.255.0
 ip access-group IPSec-Reflexive in
 ip nat outside
!
interface Ethernet0
 description "Internet"
! This policy routing command is used if split tunneling is not allowed, yet clients will
!   be allowed to access the Internet from inside the firewall.
 ip policy route-map e0
!  The crypto map assigns the IPSec configuration to the Internet interface.
 crypto map clientmap

!  This pool sets the IP address range of the IPSec clients.
ip local pool VPNIPPool 192.168.2.1 192.168.2.250

! This policy routing command is used if split tunneling is not allowed, yet clients will
!   be allowed to access the Internet from inside the firewall. The reflexive list creates
!   holes in the firewall for returning IPSec client traffic. This is required because
!   CBAC doesn't work for IPSec returning traffic.
ip access-list extended IPSec-Reflexive
 permit ip any any reflect IPSec-Returning-Packets
ip access-list extended Allowed-In
! Add this lines to the Inbound ACL to open holes for the returning IPSec traffic.
 evaluate IPSec-Returning-Packets
! Add these lines to the Inbound ACL to allow IPSec clients in to the network.
 permit udp any host <Public IP Address used by Router Itself> eq isakmp
 permit esp any host <Public IP Address used by Router Itself>

! These route maps are used if split tunneling is not allowed, yet clients will
!   be allowed to access the Internet from inside the firewall.
route-map e0 permit 10
 match ip address IPSec-Outside
 set ip next-hop 192.168.100.100
route-map l0 permit 10
 match ip address Anything
 set ip next-hop 192.168.209.209
! This ACL is used by router-map l0.
ip access-list standard Anything
 permit any
! Create user accounts as shown below with the "username" command.
```

4.9 Router Warning Banner

Use a banner to warn of legal action for unauthorized use.

```
banner exec ^C * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

```
 * This system is the property of this corporation, and is intended for the  *
 * use of authorized users only. All activities of individuals using this    *
 * computing system without authority, or in excess of their authority, are  *
 * monitored and recorded by system personnel. If any such monitoring        *
 * reveals possible evidence of criminal activity, system personnel may      *
 * provide such evidence to law enforcement officials.                       *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

^C
!
```

4.10 Use SECRET Keyword for Enable and User Passwords

Use the “secret” keyword vice “password” keyword when defining the router enable password and user passwords.

enable secret <password>
!
username *user* **secret** <password>

4.11 SSH Remote Access

Use SSH if external management of the router is needed. Avoid external management of the router if possible (best practice). The PuTTy SSH client is free and easy to use. Use a 2048 bit key.

!*** SSH Key must still be generated once with command:
Router(config)# crypto key generate rsa
! Recommend: Select the 2048 bit key size.

line vty 0 4
transport input ssh

4.12 Internet Inbound ACL restrictions

Determine whether the router should be in “stealth mode” or if it is more important to have standard network services available to hosts and to computers on the Internet for troubleshooting. This will determine what types of ICMP is allowed. If “stealth mode” is desired, block all inbound access except ICMP packet-too-big messages (necessary for inside clients to communicate properly on the internet) and inbound services. If “stealth mode” is not selected, make sure that ICMP redirects, Private IP networks (192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8), Multicasts, Class E, and reserved networks (224.0.0.0/3), Test Net (192.168.2.0/24), Autoassigned IPs (169.254.0.0/16), broadcast (255.255.255.255/32), zero network (0.0.0.0/8), loopbacks (127.0.0.0/8), and the

source address of the inside network are disallowed. See the “Allowed-In” ACL in the CBAC section above.

4.13 Poor-Man’s Accounting (who’s logging on)

Use “debug aaa authorization” in combination with the syslog server to document who is logging into the router. This is useful because a small business may not have a TACACS or RADIUS server to record the accounting information. (It appears that IOS commands executed cannot be captured to the syslog server with debug commands.)

Some Best Practices recommendations are not listed in the configurations below because they are either because they are not necessary due to their default state in the 12.2 IOS, or the configuration of the router:

4.14 Disable SNMP

SNMP is disabled by default in 12.2T IOS for 806 but can be disabled with the following command.

no snmp-server

4.15 Small Services and Reverse Telnet

TCP and UDP small services are disabled by default in 12.2T IOS for 806.

With no aux port it is assumed that a modem will not be attached so reverse telnet blocking is not required. (It is possible to attach a modem to the console port but no flow control is provided so this is a bad idea.)

4.16 Router Scheduler interval

The router scheduler interval should be set to 500 milliseconds.

scheduler interval 500

4.17 TCP Keepalives

Provides protection against sessions accidentally left idle and can clears VTY ports potentially helping in a DOS attack against the router.

service tcp-keepalives-in
service tcp-keepalives-out

5.0 Cisco IOS Security Improvement Process – "After"

The configuration file in Appendix A shows the affect of making all the security changes above.

This configuration introduces numerous security holes related to having the services on the inside. In addition, all services are running on the same inside host. Any successful attack against any of the services (Windows Terminal Server, SSH Server, Web Server, and FTP server, if present) that allows control of the inside services machine, will allow the attacker freedom to launch attacks against any other inside machine. This is a calculated risk. Many recent vulnerabilities against Windows machines are significantly mitigated if the machine is behind an access list (firewall or router). Since in a home office, a successful attack on the services server would result in significant recovery, and the services machine is often used as a regular host (I can not afford to operate many machines) this was determined to be the best option. If the services were moved off of W2K to a bastion host (Linux?), the services could be safely moved to the outside.

The configuration allows inbound ICMP to the server running the services. However, these are limited to echo requests, traceroute request, and packet-too-big notifications. The configuration also allows inbound ICMP requests to the router itself.

This configuration does nothing to defend against the insider. Without a switch and some of the newer layer two attack mitigation techniques (may require 802.1q trunking ability on the router) an insider or a compromised inside host has unlimited access. Host based firewalls are a must in a Home Office network such as this.

6.0 Future Work

This paper does not address many areas of concern for small (10 – 50 network devices), medium (50 – 200 network devices), or enterprise (200+ network devices) / service provider security. It also does not address wireless security, integrating with a firewall, Cisco PIX, for example, or how to configure with a Demilitarized Zone (DMZ). It also does not address how to deal with datalink layer attacks (this paper assumes all insiders are good guys). It does not deal with redundancy of any kind. Finally, this paper does not deal with non-router areas of security. Computers providing services are assumed to be secured

sufficiently through other means. Small projects to extend this paper may be found in: (1) configuring a wireless access point either on the inside or outside; (2) configuring a AAA (Authentication, Authorization, Accounting) server; (3) adding a DMZ; and (4) Authenticating routing and NTP.

7.0 References

Naidu, Krishni. SANS Security Checklist, May 25, 2001. http://www.sans.org/SCORE/checklists/CiscoChecklist.doc

Winters, Scott. Securing the Perimeter with Cisco IOS 12 Routers, August 15, 2000. http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

Kyger, David. Implementing and Subverting Cisco's Port Security, July 17, 2000. http://rr.sans.org/firewall/port_security.php

Wilson, Curt. Protecting Network Infrastructure at the Protocol Level, December 15, 2000. http://rr.sans.org/threats/protocol_level.htm

Langley, Richard. Securing Your Internet Access Router, January 23, 2001. http://rr.sans.org/firewall/router.htm

Eldridge, Brett. Building Bastion Routers Using Cisco IOS, Phrack Magazine --- Vol. 9 | Issue 55 --- 09.09.99, September 9, 1999 http://www.mycert.mimos.my/resource/bastionrouter.htm

Unknown. Benefits and Limitations of Context-Based Access Control, Cisco Corporation, April 2, 2002. http://www.cisco.com/warp/public/110/36.html

Mordijck, Toon. Disabling Unneeded Features and Services on Cisco Internet Gateway Routers, August 13, 2001. http://rr.sans.org/netdevices/disabling.php

Unknown. Improving Security on Cisco Routers, Cisco Corporation, Unknown Date. http://www.cisco.com/warp/public/707/21.html

Graesser, Dana. Cisco Router Hardening Step-by-Step, July 25, 2001. http://rr.sans.org/firewall/router2.htm

Wenstrom, Michael J. Managing Cisco Network Security Cisco Press, 2001

Antione, Vanessa, et al., NSA/SNAC Router Security Recommendation Guide: Executive Summary, December 2001 http://nsa1.www.conxion.com/cisco/index.html

Unknown. Security Technical Tips, Cisco Corporation, April 12, 2002. http://www.cisco.com/warp/public/707/index.shtml

Unknown. Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks, Cisco Corporation, Unknown Date. http://www.cisco.com/warp/public/707/3.html

Unknown. Building a Perimeter Security Solution with the Cisco Secure Integrated Software, Cisco Corporation, December 13, 2001. http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

Unknown. Internet Security for Small Businesses, Cisco Corporation, December 13, 2001. http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/fire_wp.htm

Unknown. Access Control Lists and IP Fragments, Cisco Corporation, 2001. http://www.cisco.com/warp/public/105/acl_wp.html

Simon Tatham, PuTTY: A Free Win32 Telnet/SSH Client, February 27, 2002. http://www.chiark.greenend.org.uk/~sgtatham/putty

Appendix A – Complete Configuration File

```
version 12.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
!
hostname MyHome
!
logging console notifications
logging buffered 16384
aaa new-model
!
!
aaa authentication login default local
aaa authentication login userauthen local
aaa authorization network groupauthor local
aaa session-id common
enable secret *** Deleted ***
!
username MyUser secret *** Deleted ***
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip domain-name myhouse.net
ip name-server 192.168.1.1
ip name-server <ISP DNS Server 1>
ip name-server <ISP DNS Server 2>
ip dhcp excluded-address 192.168.1.192 192.168.1.255
ip dhcp excluded-address 192.168.1.0 192.168.1.64
ip dhcp ping packets 1
ip dhcp ping timeout 100
!
ip dhcp pool AtHome
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.254
   dns-server 192.168.1.1 <ISP DNS Server 1> <ISP DNS Server 2>
   domain-name myhouse.net
   netbios-name-server 192.168.1.1
   netbios-node-type h-node
   lease 5
```

```
!
ip dhcp pool Albert
   host 192.168.1.100 255.255.255.0
   client-identifier 0100.9027.0000.00
   client-name Albert
ip dhcp pool Joe
   host 192.168.1.90 255.255.255.0
   hardware-address 0010.0000.0000
   client-name Joe
!
no ip bootp server
ip cef
ip inspect audit-trail
ip inspect udp idle-time 15
ip inspect dns-timeout 7
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect name cbac-in-to-out cuseeme timeout 3600
ip inspect name cbac-in-to-out ftp timeout 3600
ip inspect name cbac-in-to-out h323 timeout 3600
ip inspect name cbac-in-to-out http timeout 3600
ip inspect name cbac-in-to-out netshow timeout 3600
ip inspect name cbac-in-to-out rcmd timeout 3600
ip inspect name cbac-in-to-out realaudio timeout 3600
ip inspect name cbac-in-to-out rtsp timeout 3600
ip inspect name cbac-in-to-out smtp timeout 3600
ip inspect name cbac-in-to-out sqlnet timeout 3600
ip inspect name cbac-in-to-out streamworks timeout 3600
ip inspect name cbac-in-to-out tcp timeout 3600
ip inspect name cbac-in-to-out tftp timeout 30
ip inspect name cbac-in-to-out udp timeout 15
ip inspect name cbac-in-to-out vdolive timeout 3600
ip inspect name cbac-in-to-out fragment maximum 256 timeout 1
ip audit attack action reset
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
 lifetime 43200
!
crypto isakmp client configuration group 806VPNClient
 key <group key>
 dns 192.168.1.1 <ISP DNS Server 1>
```

```
 wins 192.168.1.1
 domain myhouse.net
 pool VPNIPPool
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface Loopback0
 description Inside Interface to Originate Outbound IPSec Packets
 ip address 192.168.100.254 255.255.255.0
 ip nat inside
 ip policy route-map l0
!
interface Loopback209
 description To pick up IPSec Outbound Reflexive-List Entries
 ip address 192.168.209.254 255.255.255.0
 ip access-group IPSec-Reflexive in
 ip nat outside
!
interface Ethernet0
 description "Internet"
 ip address <Public IP Address used by Router Itself> 255.255.255.0
 ip access-group Allowed-In in
 ip verify unicast source reachable-via rx allow-default
 ip accounting access-violations
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip inspect cbac-in-to-out out
 ip policy route-map e0
 no cdp enable
 crypto map clientmap
 hold-queue 32 in
 hold-queue 100 out
!
```

```
interface Ethernet1
 description "Inside AtHome"
 ip address 192.168.10.254 255.255.255.0 secondary
 ip address 192.168.1.254 255.255.255.0
 ip verify unicast source reachable-via rx
 ip accounting access-violations
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat inside
 rate-limit input access-group 188 8000 1500 2000 conform-action transmit
exceed-action drop
 ip policy route-map e1
 no cdp enable
!
ip local pool VPNIPPool 192.168.2.1 192.168.2.250
ip nat pool NAT-Pool <Public IP address used by inside hosts> <Public IP
address used by inside hosts> netmask 255.255.255.0
ip nat inside source list NAT-Authorized-Out pool NAT-Pool overload
ip nat inside source static tcp 192.168.10.1 80 <Public IP address used for
inside services> 80 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for
inside services> 22 extendable
ip nat inside source static tcp 192.168.10.1 53 <Public IP address used for
inside services> 53 extendable
ip nat inside source static udp 192.168.10.1 53 <Public IP address used for
inside services> 53 extendable
ip nat inside source static tcp 192.168.10.1 3389 <Public IP address used for
inside services> 3389 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for
inside services> 110 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for
inside services> 21 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for
inside services> 443 extendable
ip nat inside source static tcp 192.168.10.1 22 <Public IP address used for
inside services> 23 extendable
ip nat inside source static 192.168.10.1 <Public IP address used for inside
services>
no ip classless
ip route 0.0.0.0 0.0.0.0 <ISP Router>
ip route 192.168.2.0 255.255.255.0 Ethernet0
no ip http server
ip pim bidir-enable
!
!
```

```
ip access-list standard Anything
 permit any
!
ip access-list extended Allowed-In
 deny ip 224.0.0.0 31.255.255.255 any log
 deny ip 0.0.0.0 0.255.255.255 any log
 deny ip 127.0.0.0 0.255.255.255 any log
 deny ip 10.0.0.0 0.255.255.255 any log
 deny ip 172.16.0.0 0.15.255.255 any log
 deny ip 192.168.0.0 0.0.255.255 any log
 deny ip 169.254.0.0 0.0.255.255 any log
 deny ip 192.0.2.0 0.0.0.255 any log
 deny ip <Public IP Address used by Router Itself> 0.0.0.0 any log
 permit udp any host <Public IP address used for inside services> eq domain
 permit tcp any host <Public IP address used for inside services> eq www
 permit tcp any host <Public IP address used for inside services> eq 22
 permit tcp any host <Public IP address used for inside services> eq 3389
 permit tcp any host <Public IP address used for inside services> eq ftp
 permit tcp any host <Public IP address used for inside services> eq telnet
 permit tcp any host <Public IP address used for inside services> eq pop3
 permit tcp any host <Public IP address used for inside services> eq 443
 deny   icmp any any redirect
 permit icmp any host <Public IP address used by inside hosts>
 permit icmp any host <Public IP address used for inside services> echo
 permit icmp any host <Public IP address used for inside services> packet-too-
big
 evaluate IPSec-Returning-Packets
 permit icmp any host <Public IP Address used by Router Itself>
 permit udp any host <Public IP Address used by Router Itself> eq ntp
 permit udp <IP Addresses of the ISPs DNS servers> eq domain host <Public IP
Address used by Router Itself>
 permit udp any host <Public IP Address used by Router Itself> eq isakmp
 permit esp any host <Public IP Address used by Router Itself>
 permit ip 192.168.2.0 0.0.0.255 any
 permit tcp any host <Public IP Address used by Router Itself> eq 22
 deny   ip any any log
ip access-list extended IPSec-Outside
 deny   ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.3.255
 deny   ip 192.168.2.0 0.0.0.255 host <Public IP address used for inside
services>
 deny   ip 192.168.2.0 0.0.0.255 192.168.10.0 0.0.0.255
 permit ip 192.168.2.0 0.0.0.255 any
ip access-list extended IPSec-Reflexive
 permit ip any any reflect IPSec-Returning-Packets
ip access-list extended NAT-Authorized-Out
 deny   ip 192.168.0.0 0.0.3.255 192.168.0.0 0.0.3.255
```

```
 permit ip 192.168.0.0 0.0.3.255 any
!
logging trap debugging
logging 192.168.1.1
access-list 2 permit <IP of computer or computers to get in during DOS attack>
access-list 188 permit tcp any any eq 6699
no cdp run
route-map e1 permit 10
 match ip address Inside-Host-to-Service
 set ip next-hop <ISP Router>
!
route-map e1 permit 20
 match ip address Anything
 set ip precedence critical
 set ip tos min-delay
!
route-map e0 permit 10
 match ip address IPSec-Outside
 set ip next-hop 192.168.100.100
!
route-map l0 permit 10
 match ip address Anything
 set ip next-hop 192.168.209.209
!
radius-server retransmit 3
banner exec ^C * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
 * This system is the property of this corporation, and is intended for the  *
 * use of authorized users only. All activities of individuals using this    *
 * computing system without authority, or in excess of their authority, are  *
 * monitored and recorded by system personnel. If any such monitoring        *
 * reveals possible evidence of criminal activity, system personnel may      *
 * provide such evidence to law enforcement officials.                       *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

^C
!
line con 0
 exec-timeout 120 0
 password *** Deleted ***
 logging synchronous
 stopbits 1
line vty 0 3
 exec-timeout 5 0
 logging synchronous
 transport input ssh
line vty 4
```

```
 access-class 2 in
 exec-timeout 5 0
 logging synchronous
 transport input ssh
!
scheduler max-task-time 5000
scheduler interval 500
ntp clock-period 17168714
ntp server <Internet NTP Server1>
ntp server <Internet NTP Server2>
end
```