Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure Configuration of a Cisco 837 ADSL firewall router

Connecting a business office to the Internet is a task faced by many small business owners, most succeed. Connecting to the Internet in a secure manner is an entirely different task commonly overlooked. This paper describes, hopefully, a fairly typical small office/business scenario and one method to connect it securely to the Internet using a commercially available firewall/router, the Cisco 837 ADSL router. A summary of the relevant security features of the router is provided and a step-by-step explanation of the req...

Copyright SANS Institute
Author Retains Full Rights

AD

Secure Configuration of a Cisco 837 ADSL firewall router

GIAC Security Essentials Certification (GSEC)
Practical Assignment, Version 1.4b (August 29, 2002), Option 1
Author: Brett McIntosh

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Contents

Secure Configuration of a Cisco 837 ADSL firewall router 1
Contents 2
Abstract 3
Introduction 3
Scenario 4
  Cisco IOS access-lists 5
  Cisco IOS Firewall feature 6
  Cisco IOS IDS feature 8
IPSec (VPN) 9
Configuration line by line 9
  Basic router IP addressing 9
  ADSL interface 10
  Add Access-lists 11
  Add Firewall feature 15
  Add IDS 16
  Add VPN 17
  Router hardening 20
Nmap testing results 24
Comments 27
Conclusions 29
Glossary 30
References 31
Appendix 32

© SANS Institute 2003, Author retains full rights

Abstract

Connecting a business office to the Internet is a task faced by many small business owners, most succeed. Connecting to the Internet in a secure manner is an entirely different task commonly overlooked.

This paper describes, hopefully, a fairly typical small office/business scenario and one method to connect it securely to the Internet using a commercially available firewall/router, the Cisco 837 ADSL router. A summary of the relevant security features of the router is provided and a step-by-step explanation of the required configuration to use these features to their maximum-security effect. Finally some results are provided of a before and after scan performed on the network using the security scanning tool nmap. The paper is intended to provide a template and example for current recommended practices.

Introduction

It has become almost essential for business of all sizes to use the Internet to do business. Many businesses see the Internet as a way of increasing sales, working more efficiently or just keeping up with competitors. At the small business end of town this Internet connection tends to be done in hurry with the business just happy to have their Internet connection up and working. Typically not much thought or time is given to the security of the Internet connection.

The following paper explains, via example, how to configure a commercially available firewall/router to, as far as possible, securely connect a small business office to the Internet using the most current recommended practices.

A common cost effective method of connecting small business to the Internet is via ADSL. ADSL connections require a device at the business office to terminate the ADSL line from the local Telephone Company. This device can be a simple, cheap ADSL modem or more sophisticated ADSL router. Wise businesses will then use some type of Firewall software or equipment to protect the office internal network from potential attack from the Internet. The Firewall could be of the personal type, software installed on the end users workstations, e.g. Zone Alarm or Kerio firewall, dedicated, stand alone firewall installed between the Internet ADSL router/modem and the internal network, e.g. Checkpoint Firewall-1 or Cisco PIX, or a firewall function integrated into the ADSL router/modem. Personal firewalls have an issue that they need careful configuration not to restrict internal office PC-to-PC communications but at the same time stop access from the Internet. Stand-alone firewalls are an additional piece of equipment and cost that needs configuration and maintenance. Integrated firewalls can overcome some of these issues and, after all, if the business needs a device to connect to the Internet plus a firewall, why not buy something that does both.

Cisco systems released the Cisco 837 ADSL router in November 2002. Whilst there are numerous ADSL routers on the market, and not trying to sound like a Cisco Salesman,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

this ADSL router comes with a fairly full-featured operating system, called IOS by Cisco, for under $US500[1]. Cisco IOS is built with a number of feature sets, the more features you want, the more it will cost. The Cisco 837 ADSL[2] router standard IOS comes complete with the following three important security features, a stateful firewall, a simple Intrusion Detection System (IDS) with 104 built-in signatures and 3DES IPSec VPN feature. The 837 hardware has a built-in ADSL interface, a 4 port 10/100 Ethernet switch and hardware 3DES encryption engine. These features make the Cisco 837 an attractive device for use as a small office, home office or corporate branch office firewall/router.

An important issue with devices like firewall/routers, especially one with as many included features as the Cisco 837, is configuring it to correctly be the businesses first line of defence from the Internet.

The following pages will go through the steps required to securely configure a Cisco 837 ADSL firewall/router beginning with some detail about the example business, it's structure and how it uses the Internet. Following this a brief explanation of the Cisco firewall, IDS, VPN features and finally the step-by-step configuration of the router.

Scenario

A scenario small business will be used as an example to explain the configuration requirements of the router so, as far as practically possible, the business is protected from the Internet. While each business uses the Internet in different ways to suit their particular requirements, this example hopefully represents the most common set of uses.

Just a small note before we get started. Normal recommended design for Internet facing hosts is to place then on a screened segment, also know as a De-Militarised Zone (DMZ). The benefit being if an attacker does compromise an Internet facing server, the attacker is hopefully contained inside the DMZ and can't directly attack the internal network. Asmallbus management could not justify the cost of building a DMZ and accepted the risk of not using one in their network design.

A small business named, "Asmallbus", is in the business of selling widgets. It does this via a travelling Sales force and one small office. It has a Manager/owner who employs three office based staff plus four travelling Salesmen. Orders from customers are received either via normal mail, facsimile, E-mail or on-line via Asmallbus own web page www.asmallbus.com.

---

[1] CNET Networks, CNET review Cisco 837 ADSL router, URL: http://reviews.cnet.com/CISCO_837_ADSL_RTR/4505-3334_7-21042425.html?tag=dir

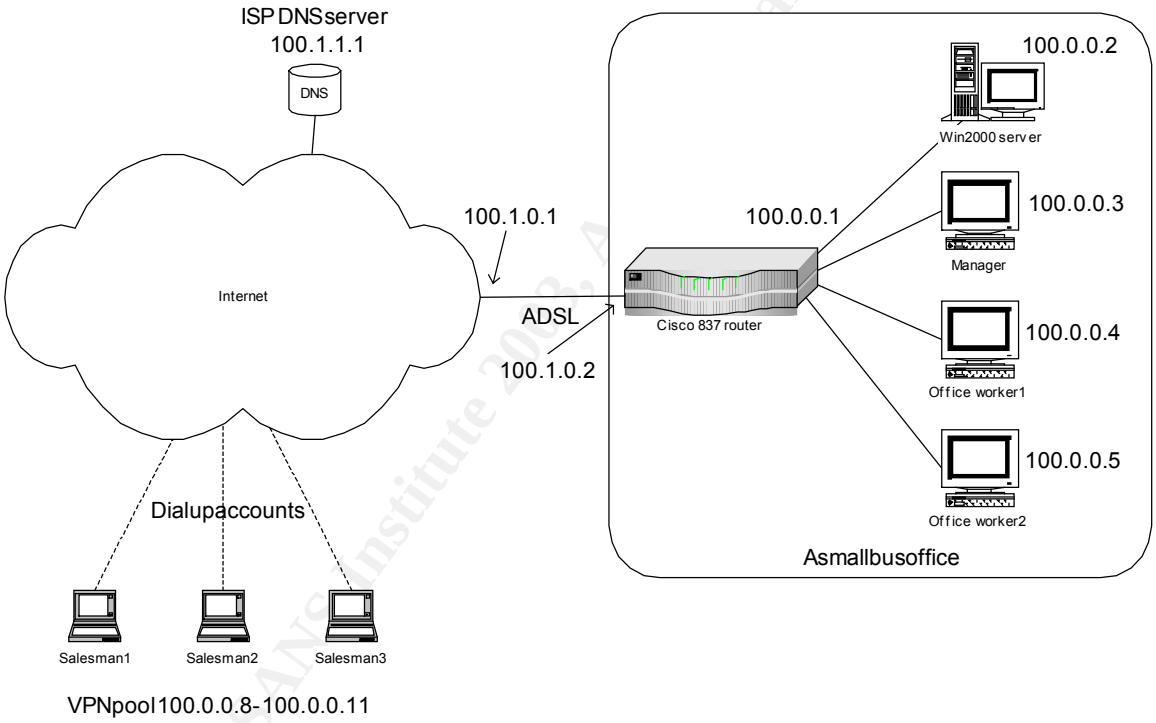
[2] Cisco Systems, Cisco 800 series routers data sheet, URL: http://www.cisco.com/en/US/products/hw/routers/ps380/products_data_sheet09186a008010e5c5.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The office is connected to Internet via 512k downstream, 128k upstream ADSL service. Office hardware is, a Cisco 837 router with four machines connected to it, a Windows 2000 server and three Windows 2000 professional machines for each of the office based staff. The travelling Sales force have laptops with built-in modems and accounts with a national ISP so they can connect to the Internet and using Cisco's VPN client software connect, via the Internet and the Cisco 837, to Asmallbus's internal network.

The Internet Service Provider (ISP) that provides Internet access to Asmallbus's routes a small subnet of 100.0.0.0 255.255.255.248 towards the Asmallbus router. The ADSL link IP address is 100.1.0.0 255.255.255.252 with 100.1.0.1 at the ISP and 100.1.0.2 at the office end. Asmallbus owns the domain name of "asmallbus.com", with primary DNS being the on-site Windows 2000 server and secondary DNS provided by the ISP. The Windows 2000 server is also the businesses web server, E-mail post-office, file server and database for customer orders.

The following drawing details Asmallbus network set-up.



The Manager of Asmallbus is critically concerned to have the firewall/router configured as securely as possible to protect his business operations.

Cisco IOS access-lists

Many documents and publications have been produced to explain access-lists in Cisco routers. The following is a very brief explanation.

Access-lists are Cisco IOS's method of controlling what data packets are allowed to enter and/or leave Cisco router interfaces. An access-list is a set of rules. It defines, line

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

by line, what data packets are allowed to pass (permitted) or be stopped (denied) entering and/or exiting a router interface. The list is processed in sequential order. As soon as a data packet matches a line of an access-list (whether permitted or denied) no further processing of subsequent lines in the list is carried out. Once defined an access-list is applied to interfaces in either incoming and/or outgoing direction.

Access-lists are identified by either a number (the old method) or name (the newer method). Cisco has two types of access-lists to control IP packets. Standard, where only the source IP address(es) of the packet are assessed and extended, where IP protocol number, source and destination IP address(es), TCP/UDP port number(s) and other optional IP packet parameters are assessed.

On their own, access-lists can give limited protection (well better than nothing) from the Internet by providing some filtering of incoming Internet sourced IP packets. The problem is the filtering, by necessity, needs to be very non-specific. An internal network user could browse to one of millions of possible IP addresses. The reply packets from these web server's needs to get back to the user so we can't filter on source IP address.

Example of access-list

```
ip access-list extended INTERNET-IN
 permit tcp any host 100.0.0.2 eq 25
 deny   ip  any any log

interface Dialer 1
 ip access-group INTERNET-IN in
```

This access-list will allow incoming packets to interface dialer 1 which are TCP, have any IP source address, any TCP source port, have the destination IP address of 100.0.0.2 and destination TCP port of 25 (SMTP). If an IP packet doesn't match this first line, the second line of the access-list will deny, that is drop, all other IP packets. The optional "log" command will cause the router to record a denied packet record in the log.

Cisco IOS Firewall feature

Cisco's IOS firewall feature[3] adds the concept of state to normal access-lists. The router is aware of the state and tracks TCP and UDP sessions through the router. Cisco calls this Context Based Access Control (CBAC). CBAC causes the router to inspect packets leaving a router interface. The source and destination IP addresses, source and destination ports of TCP or UDP packets are noted. The router will then dynamically add lines to the beginning of any incoming access-list on that interface to allow the incoming reply packet for the previous outgoing packet back through any incoming interface access-list. By doing this the incoming access-list, the one facing the Internet, is only

[3] Cisco Systems, Cisco IOS Firewall Data sheet, URL: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

opened up to allow specific reply packets back into the router. CBAC tracks the state of sessions and once the session is finished the dynamic entries in the access list are removed. As an option, the router will also keep an audit trail of each session through the router reporting on the number of bytes transferred and the session length.

CBAC actually does more than this. It inspects layer 5 to 7 information of some applications to take into account the particular protocols peculiarities. For example, CBAC is FTP aware, adding dynamic access-list rules for both command and data TCP sessions of the FTP protocol.

To further enhance security of some applications Firewall IOS adds checking of unusual behaviour. An example is SMTP command checking. Only “safe” SMTP commands are allowed to enter the router and travel towards the mail server. Unsafe SMTP commands cause the router to terminate the SMTP session.

To help control denial of service attacks, Firewall IOS, monitors the number of TCP sessions passing through an interface. Both half open and established TCP sessions are counted and checked against pre-set high-water trigger levels. If a high-water mark is reached the router will stop any more TCP sessions being established until the number of TCP sessions falls below a pre-defined low-water mark.

Configuration of the Firewall feature requires the defining of an inspection list detailing the protocols to be inspected, changing of any default settings like the half-open and established TCP session high and low water marks and applying the inspection list to an interface. The important thing to understand is the inspection of a packet travelling in one direction through the router will dynamically modify access-lists that the reply packet, of this inspected packet, would encounter travelling back through the router. That is, if you inspect a packet outgoing from the router, any access-list applied in the incoming direction on this same interface will be dynamically modified.

For example.

```
ip inspect name INTERNET-OUT tcp alert on audit-trail on
ip inspect name INTERNET-OUT udp alert on audit-trail on

interface Dialer 1
 ip inspect INTERNET-OUT out
 ip access-group INTERNET-IN in
```

Thus packets TCP and UDP leaving interface Dialer 1 will be inspected and dynamic entries added to the beginning of access-list INTERNET-IN to allow the reply packets to enter the router.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A more detailed explanation about how CBAC works can be found in Evan Davies GIAC Security Essentials Assignment, CBAC – Cisco IOS Firewall feature Set Foundations[4].

Cisco IOS IDS feature

Cisco has built into their Firewall IOS a basic Intrusion Detection System with a limited number of built-in Intrusion detection signatures. Dependent on the particular IDS signature the router can be configured to either alarm, via log message, drop the packet or disconnect the TCP session. In some ways the router has become a simple Intrusion Protection System. Cisco's initial IDS feature included 59 signatures which has been more recently increased to 104 in router IOS image 12.2(11)YU.[5]

Cisco classifies the signatures in two ways, severity and complexity. Severity is either an "info" signature, the signature of an information gathering activity or an "attack" signature, signature of a malicious activity. Complexity is either "atomic" or "compound". Atomic is a simple pattern on single host while "compound" signature is multiple packets to multiple hosts over a long period of time. The actions taken by the router when a signature is detected depends on how it's configured, either send alarm, drop the packet or if it's a TCP session reset the session.

Typically you would log informational signatures and drop and/or disconnect plus log attack signatures on being detected.

Using the IDS feature is fairly simple,

- Create and name an audit policy,
- Define what the router is to do when a signature is detected by this policy.
- Apply the audit policy to an interface of the router and define the direction to check packets either incoming or outgoing from the router.

For example

```
ip audit name INTERNET-IN info   action alarm
ip audit name INTERNET-IN attack action alarm drop reset

interface Ethernet 0
  ip audit INTERNET-IN in
```

This will start the router inspecting incoming packets to interface Ethernet 0 for the 104 IDS signatures. If an information signature is detected a message will be logged, if an attack signature is detected the packet will be dropped and if it's a TCP session, the session will be reset.

---

[4] Evan Davies, CBAC – Cisco IOS Firewall feature set foundations (2002), URL: http://www.sans.org/rr/papers/21/806.pdf

[5] Cisco Systems, Cisco IOS Intrusion Detection System Signature List, URL: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008014c532.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Specific signatures can be completely disabled if required, e.g. the signature indicating a ICMP echo has been detected, i.e. your been pinged.

Logging can be either directed to syslog feature or Cisco's Net ranger IDS system. Syslog messages can be directed into memory buffer on the router and/or to a remote syslog server on the network.

IPSec (VPN)

Cisco have built into their IOS, as an optional feature, an ISAKMP/IPSec based VPN system called Easy VPN[6]. It is comprised of two parts, a remote VPN client and a VPN server. These two parts create an encrypted IPSec VPN tunnel from the remote to the server. The remote appears as if it is connected to the local network.

The easy VPN server provides configuration information to the remote VPN client as part of the ISAKMP exchange at the beginning of a VPN session. This information includes the IP address assigned to the remote client VPN tunnel endpoint plus the DNS and WINS addresses the remote client should use while the VPN tunnel is up.

The remote client can be another Cisco router, PIX firewall or in this case remote PC's running Cisco's VPN client software.

Configuration line by line

Basic router IP addressing

Add IP address to Ethernet interface. This is the internal IP sub-network used by the office workstations and server. The router is assigned the first usable IP address.

```
interface Ethernet 0
  ip address 100.0.0.1 255.255.255.248
```

ISP has assigned the IP address 10.1.0.2 to this end of the ADSL link with a subnet mask of 255.255.255.252. Cisco routers use a dialer interface as its IP interface to ADSL services which use Point-to-Point (PPP) protocol.

```
interface Dialer 1
  ip address 100.1.0.2 255.255.255.252
```

Now we have the IP addresses of the two interfaces defined we need to inform the router in what direction to route IP packets. As this is an Internet connected router and there is only a single IP sub-net connected to the Ethernet interface, a default route, pointing all IP addresses back to the Internet is required.

---

[6] Cisco Systems, Cisco Easy VPN, URL: http://www.cisco.com/en/US/products/sw/secursw/ps5299/prod_brochure09186a00800a4b36.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
ip route 0.0.0.0 0.0.0.0 Dialer1
```

ADSL interface

The exact configuration of the ADSL interface depends on how the particular ISP provides their service. The following is just one method. You will need to consult your ISP to find out their preferred method for configuring Cisco routers on their ADSL service. In this case the ISP uses,

- PPP over Ethernet encapsulation
- ANSI-DMT DSL line coding
- ATM PVP/PVC 8/35 for ADSL connection.

```
interface ATM0
 dsl operating-mode ansi-dmt
!
interface ATM0.1 point-to-point
 pvc 8/35
  ip addr inarp
  pppoe-client dial-pool-number 1
```

The “dial-pool-number 1” indicates this particular connection is part of the dial pool number 1. Dial pools are used by dialer interfaces to make outgoing connections, see dialer interface details below.

ADSL use an ATM based line protocol, where each data of packet is divided up into 48 byte cells with a 5-byte header. The header contains addressing information, like the permanent virtual circuit identifier (PVC) and permanent virtual path identifier (PVP) numbers. ATM works on the concept of sharing a particular physical transmission link via defining virtual circuits. Each virtual circuit has it’s own PVP/PVC.

The dialer interface is the link between the ADSL interface and the IP protocol. In this case;

- The IP packets will be encapsulated into PPP protocol.
- The PPP protocol link will be authenticated using CHAP.
- The dialer interface will use physical interfaces in dialer pool 1, See ATM interface above.
- The Message Transfer Unit (MTU) of TCP connections is adjusted to 1492 bytes. This stops problems with packet fragmentation causing TCP connections to fail.

PPP is allows this ADSL router to authenticate its connection to the ADSL concentrator. Multiple ADSL services, from many different customers of the ISP will terminate on the ADSL concentrator. PPP allows for both the identification of this connection as belonging to Asmallbus, this is the hostname asmallbus-router@asmallbus.anisp.com and authentication via the Challenge Handshake Authentication Protocol (CHAP).

```
interface Dialer1
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
ip address 10.1.0.2 255.255.255.252
ip mtu 1492
encapsulation ppp
dialer pool 1
ppp authentication chap
ppp chap hostname asmallbus-router@asmallbus.anisp.com
ppp chap password 7 070754120300
```

Although the connection is using ADSL, the router treats it as a dial on demand type of interface. This requires “interesting traffic” to be defined in the router. Interesting means traffic that will cause the dialler interface to dial, or in this case attempt to connection the ADSL. Any IP packets are interesting in this case.

```
dialer-list 1 protocol ip permit
```

Add Access-lists

At this stage the router should have IP connectivity to the Internet via ADSL. Now comes the task of securing the internal network and the router itself from both the Internet and the internal network.

First stage is to define an access-list to protect the router from the Internet. This access-list will be applied to the interface that has the IP connectivity to the Internet, the dialer interface. The ATM interface is not configured for IP and is only used to accept IP packets to/from the dialer interface, segment or reassemble them to/from 53 byte ATM cells and transmit/receive these cells to the ADSL line.

This dialer access-list is the most important piece of security configuration in the router. It’s primary function is to control what IP packets are allowed to enter the router and get routed thru the router to the Ethernet interface and thus the internal network.

Asmallbus management have defined the following policy for incoming traffic from the Internet.

- SMTP to main Win 2000 server (Asmallbus mail post office).
- HTTP to main Win 2000 server (Asmallbus web server).
- DNS zone transfers from ISP hosted secondary DNS to Win 2000 server (Asmallbus.com domain primary DNS server).
- ICMP unreachable (See note 1 below).
- ICMP time-exceeded (For fault finding use, allows trace route to work).
- ICMP echo-reply (For fault-finding use, allows ping to work).
- ESP to router Internet interface (Allows IPSec packets from remote VPN clients).
- ISAKMP to router Internet interface (Allows VPN connections to be established from remote VPN clients).
- IP from remote VPN client pool addresses (See VPN section for explanation).
- All other packets are stopped.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Additional rules are required at the beginning of the access-list to drop packets from illegal, unused and reserved Internet sources addresses. These addresses can be found in RFC-3330[7]. Also protection against address spoofing is provided. The following access-list is in a format that can be cut and pasted directly into a Cisco router.

```
ip access-list extended Internet-in
  ! IP address spoof protection, deny internal addresses
 deny   ip   100.0.0.0 0.0.0.15       any log
  ! Protect against Land attack
 deny   ip   host 100.1.0.0 0.0.0.3   any log
  ! Illegal Internet source addresses
 deny   ip   0.0.0.0 0.255.255.255    any log
  ! Host local loop back address
 deny   ip   127.0.0.0 0.255.255.255  any log
  ! RFC-1918 private network addresses
 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
  ! Documentation/test network
 deny   ip   192.0.2.0 0.0.0.255      any log
  ! DHCP local link address
 deny   ip   169.254.0.0 0.0.255.255  any log
  ! Multicast source addresses
 deny   ip   224.0.0.0 31.255.255.255 any log
  ! Permit external SMTP traffic to internal SMTP server
 permit tcp  any gt 1023          host 100.0.0.2 eq smtp
 permit tcp  any gt 1023          host 100.0.0.2 eq www
  ! Allow secondary DNS server hosted by ISP to perform zone
  ! transfers from primary DNS
 permit tcp  host 100.1.1.1 gt 1023 host 100.0.0.2 eq domain
  ! Permit IPSec Encapsulating Security Protocol packet
  ! to reach router. See VPN section for explanation.
 permit esp  any                  host 100.1.0.2
  ! Permit ISAKMP packets the reach router.
  ! See VPN section for explanation
 permit udp  any eq 500           host 100.1.0.2 eq 500
  ! Permit decrypted VPN client packets enter internal network
  ! See VPN section for explanation
 permit ip   100.0.0.8 0.0.0.7    100.0.0.0 0.0.0.7
  ! Permit ICMP unreachable, time-exceeded and echo-reply
  ! reach internal network
 permit icmp any                  100.0.0.0 0.0.0.7 reachable
 permit icmp any                  100.0.0.0 0.0.0.7 time-exceeded
 permit icmp any                  100.0.0.0 0.0.0.7 echo-reply
```

[7] Internet Assigned Numbers Authority, Request For Comments: 3330, Special-Use IPv4 Addresses (September 2002), URL: http://www.ietf.org/rfc/rfc3330.txt?number=3330

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
  ! Deny all other TCP and UDP packets and log port numbers
 deny   tcp  any range 0 65535   any range 0 65535 log
 deny   udp  any range 0 65535   any range 0 65535 log
  ! Deny all other packets.
 deny   ip   any                 any log
exit
```

Now apply this access-list to the interface it is designed to protect.

```
Interface Dialer 1
 ip access-group Internet-in in
```

Notes;
1. It is important for the Win 2000 web server to receive ICMP unreachable messages so it can perform Maximum Transmission Unit (MTU) discovery[8]. The MTU of a link is the largest packet that a link can transport. Normally Ethernet's MTU is 1500 bytes but the addition of tunnelling technologies can decrease this. The Win 2000 server performs MTU discovery by sending IP packets with the Don't Fragment (DF) bit set. Normally if a packet, say 1500 bytes in size, is received by a router and the router wants to send it out an interface with a MTU setting of less than 1500 bytes, the packet is fragmented into two or more smaller packets. Setting the DF bit prevents the router doing this, the packet is dropped and the router sends an ICMP unreachable message back to the packet source indicating it wanted to fragment the packet but couldn't and the MTU size of the link on which it wanted to send the packet. The server now knows the MTU of this link and doesn't send any packets larger than this size. If the Win 2000 server didn't get this unreachable message then any large packets it's sends via this particular link are dropped and the server has no knowledge of this. The user of the Asmallbus web site gets symptoms like half loaded web pages.

The control of outgoing access to Internet by internal users and to protect the router from the Internal network users, an incoming access-list is applied to the Ethernet interface of the router. The Asmallbus Company Internet access policy only allows outgoing Internet access for business purposes. It further defines what types of outgoing traffic is allowed and this is enforced by the router's access-list.

Outgoing traffic from Asmallbus Policy
- HTTP to Internet for all internal machines
- HTTPS to Internet for all internal machines
- SMTP to Internet only from mail server
- TCP based DNS zone transfer only to ISP hosted secondary DNS from Win 2000 server.
- UDP based DNS lookups from all internal machines to Internet.
- ICMP echo from all internal machines (allows machines to perform test pings)

[8] Marc Slemko, Path MTU Discovery and Filtering ICMP (12 November 1998), URL: http://alive.znep.com/~marcs/mtu/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- SSH from manager desktop to routers Ethernet interface (allows only Manager's machine to access router)

As an additional precaution, and because Asmallbus is a good Internet citizen, packets to illegal, unused and reserved Internet addresses are stopped at the router.

```
ip access-list extended E0-in
 ! Stop illegal, unused and reserved destination IP addresses
 deny   ip   any 0.0.0.0 0.255.255.255    log
 deny   ip   any 10.0.0.0 0.255.255.255   log
 deny   ip   any 127.0.0.0 0.255.255.255  log
 deny   ip   any 172.16.0.0 0.15.255.255  log
 deny   ip   any 192.168.0.0 0.0.255.255  log
 deny   ip   any 224.0.0.0 31.255.255.255 log
 ! Documentation/test network
 deny   ip   any 192.0.2.0 0.0.0.255      log
 ! DHCP local link address
 deny   ip   any  169.254.0.0 0.0.255.255 log
 ! Allow managers local machines to SSH to router.
 permit tcp  host 100.0.0.3 gt 1023    host 100.0.0.1 eq 22
 ! Allow internal machines to ping router both interfaces
 permit icmp 100.0.0.0 0.0.0.7         host 100.0.0.1 echo
 permit icmp 100.0.0.0 0.0.0.7         host 100.1.0.2 echo
 ! Don't allow local machines any other access to router
 ! Both internal and external interfaces to protect router
 deny   ip   any                       host 100.0.0.1 log
 deny   ip   any                       host 100.1.0.2 log
 ! Finally allow local machines access to Internet
 permit tcp  100.0.0.0 0.0.0.7 gt 1023 any eq www
 permit tcp  100.0.0.0 0.0.0.7 gt 1023 any eq 443
 permit udp  100.0.0.0 0.0.0.7 gt 1023 any eq 53
 ! Allow reply packets back to remote VPN machines
 permit ip   100.0.0.0 0.0.0.7         100.0.0.8 0.0.3
 ! Allow mail to go out to Internet from mail server
 permit tcp  host 100.0.0.2 gt 1023    any eq smtp
 ! Allow DNS server to transfer information to secondary DNS
 permit tcp  host 100.0.0.2 gt 1023    host 100.1.1.1 eq domain
 ! Allow internal machine to ping Internet hosts.
 permit icmp 100.0.0.0 0.0.0.7         any echo
 ! Stop all other packets and log
 deny   tcp  any                       any range 0 65535 log
 deny   udp  any                       any range 0 65535 log
 deny   ip   any                       any log
```

Apply this access-list to the Ethernet interface.

```
Interface Ethernet0
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
ip access-group E0-in in
```

This completes the configuration of the access-lists in the router, other than access-list, 99 protecting SSH access to the router and is explained in the router hardening section later.

Add Firewall feature

Now the basic access-lists have been defined we need to add the Firewall feature. This is fairly simple procedure. Define and name an inspect list to detail what layer 4 to 7 protocols and applications to inspect. Apply this inspect list to an interface including setting the direction packets are to be inspected, either incoming and/or outgoing from the router. Typically, an incoming access-list requires an outgoing inspection list. Packets leaving the router are inspected and dynamic entries are added to be top of the incoming access-list on the same interface. This allows the reply packets, which would be normally stopped by the incoming access-list, to enter the router.

First name an inspect list for packets leaving the router heading towards the Internet. We'll inspect normal TCP, UDP and ICMP packets. Extra inspection will be performed on the TCP packets of SMTP and HTTP. Additionally fragment packets will be inspected and the numbers of fragments counted to ensure no more than 2 IP packet fragments are allowed to leave the router. Audit log messages will be produced for all inspected packet sessions listing the time the packet session commenced, finished and the number of bytes transferred in the session.

```
ip inspect name INTERNET-OUT tcp  alert on audit-trail on
ip inspect name INTERNET-OUT udp  alert on audit-trail on
ip inspect name INTERNET-OUT smtp alert on audit-trail on
ip inspect name INTERNET-OUT http alert on audit-trail on
ip inspect name INTERNET-OUT fragment maximum 2 timeout 1
```

Applying an incoming inspect list to the Internet connected interface will achieve a number of purposes. Incoming packets from the Internet will be inspected and checked. An audit trial log of each session will be produced. Reply packets for these incoming sessions will need to get past the incoming access-list applied to the Internal Ethernet interface. This inspection list will dynamically add these as required.

```
ip inspect name INTERNET-IN tcp  alert on audit-trail on
ip inspect name INTERNET-IN udp  alert on audit-trail on
ip inspect name INTERNET-IN smtp alert on audit-trail on
ip inspect name INTERNET-IN http alert on audit-trail on
ip inspect name INTERNET-IN fragment maximum 2 timeout 1
```

As suggested in the NSA router security configuration guide[9] some of the default setting for the Cisco CBAC should be changed. An idle UDP session is timed out after 15

[9] USA National Security Agency, Router Security Configuration Guide, Version 1.1 (27 September 2002), URL:http://www.nsa.gov/snac/cisco/download.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

seconds of no traffic, an idle TCP session time out is reduced from 3600 to 1800 seconds, decreasing the time CBAC will continue to manage a TCP session after being closed by a FIN exchange to 1 second and the time to wait for new TCP session to reach established state made 15 seconds.

```
ip inspect udp idle-time    15
ip inspect tcp idle-time    1800
ip inspect tcp finwait-time 1
ip inspect tcp synwait-time 15
```

Finally, the Firewall feature tracks both the total number of half-open TCP sessions and the rate at which new TCP connections are established. As Asmallbus has a small number of users these settings can be greatly reduced from there default settings of 500 for high-water mark and 400 for low-water mark.

```
ip inspect max-incomplete high 20
ip inspect one-minute     high 20
ip inspect max-incomplete low  10
ip inspect one-minute     low  10
```

Now apply the inspection lists to the Internet facing interface.

```
Interface Dialer1
 ip inspect INTERNET-IN IN
 ip inspect INTERNET-OUT out
```

Add IDS

Activating the built-in IDS feature is simple. Define a name for the audit policy. Include the actions to take when an attack or informational IDS signature is detected and then apply to an interface. For information signatures just generate a syslog message, for attack signatures, drop the packet and reset the connection.

```
ip audit name INTERNET-IN info   action alarm
ip audit name INTERNET-IN attack action alarm drop reset
```

Perform the same function for outgoing packets.

```
ip audit name INTERNET-OUT info   action alarm
ip audit name INTERNET-OUT attack action alarm drop reset
```

Change the maximum number of mail recipients before it is considered a spam attack from the by default of 250 down to a reasonable number for Asmallbus, say 30.

```
ip audit smtp spam 30
```

Apply the audit policy the Internet facing interface.

© SANS Institute 2003, Author retains full rights

```
Interface Dialer 1
 ip audit INTERNET-IN in
 ip audit INTERNET-OUT out
```

Add VPN

To allow the travelling Sales Force secure access to internal documentation, files and E-mail the router is configured to accept IPSec VPN connections, over the Internet, from the remote Salesman laptop. The following VPN policy is used for these remote connections.

- Encryption, 3DES
  (Two options, DES and 3DES. DES is now considered not very secure)
- Diffie-Hellman policy, group 2
  (Provides a more secure authentication than DH group 1)
- No split tunnelling allowed
  (When connected via VPN tunnel to the main office the remote laptop, in effect, has no connection to it's local Internet other than IPSec VPN connection)
- Use pre-shared keys authentication keys
  (Could use Digital Certificates but low number of users doesn't justify the expense)
- Once successfully authenticated, the remote PC is permitted full access to the internal office network.
  (That is, as if remote PC was connected to local office network)
- Each remote user must authentication themselves via their own individual username and password.
- VPN users, username and passwords are configured and stored in the router.
  (It is possible to configure router to use centralised authentication system like RADIUS but again small number of users doesn't justify the expense)

The following router configuration for is based on a similar Cisco remote VPN example.[10]

Configuration of IPSec VPN's on the router can be done in stages.

First stage is to configure the ISAKMP key management policy between the remote VPN client and the VPN server. In this case use 3DES encryption, Diffie-Hellman group 2 policy with a pre-shared key. Cisco routers can have a number of ISAKMP policies defined. Incoming VPN setup attempts try these policies one after the other, in order as determined by the sequence number. Here only one policy is used, policy sequence number 10.

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
```

[10] Cisco Systems, Configuring IPSec Between Two Routers and a Cisco VPN Client 3.x (12 November 2002), URL: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a0080094685.shtml

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
 group 2
```

The remote VPN client configuration will be sent to the remote client if they authenticate successfully. A number of these VPN client configuration groups can be defined in the router. As Asmallbus have only one small group of remote Salesman they will all share the same configuration details. One drawback of doing this is all remote Salesmen will use the same encryption key that could be viewed as a security risk.

If the remote client has the correct group name and key, then the DNS and WIN server IP addresses, the domain name and IP address to be used by the remote client end of the VPN tunnel will be sent to the remote PC. The IP address is provided from a pool configured in the router. Each new VPN connection will be assigned a unique IP address from this pool, named “ippool”. It’s important the key is kept secure; it’s the main item that protects this connection from attackers on the Internet. The key should also be made fairly long and obscure so it can’t be easily guessed or remembered if viewed.

```
crypto isakmp client configuration group remotesalesgroup
 key 0 th1sISl0gpReSHaREDkEy
 dns 100.0.0.2
 wins 100.0.0.2
 domain asmallbus.com
 pool ippool

ip local pool ippool 100.0.0.8 100.0.0.11
```

The router needs to be told to respond to a request for an IP address from the remote VPN client.

```
crypto map clientmap client configuration address respond
```

Although the remote client may have matching pre-shared keys, this only authorizes the establishment of the VPN tunnel. Additional authentication from the remote user is required to login to the VPN. The pre-shared key authorizes the remote machine while the remote users username and password authenticates the user of the remote machine. As part of the VPN establishment process the user is prompted for their own individual username and password. These username/password pairs are stored in the router because the number of remote users is small. Cisco calls this local authentication. It is possible to use a centralized authentication method like RADIUS for this.

```
username salesman1 password 7 01040316540F000720484801185E11
username salesman2 password 7 0942430C0B531D1A595B52383A213F
username salesman3 password 7 04510F1509294A17011356434B5309
```

To allow the router to use it’s locally stored username and passwords it needs to be placed into Authentication, Authorisation, Accounting (AAA) new-model mode. It is possible to have a number of authentication and authorisation sources tried by the router to find a match for an incoming AAA request. Lists can be created defining these AAA

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

sources. For Asmallbus only the local database is used. The AAA lists "userauthenticate" for incoming user login authentication requests and "groupauthorise" for incoming network connection authorisation requests are defined.

```
aaa new-model
aaa authentication login   userauthenicate local
aaa authorization  network groupauthorise  local
```

Next the authentication and authorization request from the remote client are configured to use the local password database.

```
crypto map clientmap client authentication list userauthenticate
crypto map clientmap isakmp authorization  list groupauthorise
```

This completes the ISAKMP definition of the VPN setup. Next is the IPSec configuration starting with the definition of an IPSec transform set. Transform sets specify the encryption and authentication to be used on a particular VPN tunnel, here pairing encapsulating Security Protocol (ESP) using 3DES encryption and SHA-HMAC authentication is given the transform set name of ts-asmallbus.

```
crypto ipsec transform-set ts-asmallbus esp-3des esp-sha-hmac
```

As the remote users will be attempting to connect to the router from unknown source IP addresses, a dynamic crypto map is required in the router. Dynamic maps allow IPSec sessions to be established with unknown remote peer IP addresses. A dynamic map "dynmap" is defined to use the IPSec transform defined above to select the required encryption and authentication protocol.

```
crypto dynamic-map dynmap 10
 set transform-set myset
```

This dynamic map is then assigned to a normal crypto map that is then applied to an interface. As an IPSec connection attempt is received by the router, a number of different IPSec session definitions can be tried as the router searches for one that matches the particular IPSec requirements of the remote client. We have only one definition here, sequence number 10.

```
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

All these VPN configuration lines are then assigned to an interface of the router. As the incoming VPN request will be coming from the Internet, the crypto map is assigned to the Dialer interface. The remote VPN client would be configured to establish its VPN tunnel to the endpoint IP address of the dialer interface.

```
Interface Dialer 1
  crypto map clientmap
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This, however, isn't the end of it. The dialer interface has an incoming access-list applied to it. Cisco routers process incoming packet through the incoming access-list before any crypto processing is performed. The requests from remote client must be allowed to enter the router. The previously defined access-list named "Internet-in" has been configured to allow this. ISAKMP uses the UDP protocol on well-known port 500 for both source and destination. IPSec uses IP protocol number 50. Note the IP protocol number is not a port number in the sense of TCP and UDP. It defines the particular protocol contained in the IP packet; other examples of IP protocol numbers are TCP, protocol number 6 and UDP, protocol number 17.

This explains why the following lines appear in the "Internet-in" access-list. Note the destination address is the router's Internet facing interface IP address, the packets terminate and are processed by the router.

```
 ! Permit IPSec Encapsulating Security Protocol packet
 ! to reach router
 ! See VPN section for explanation
 permit esp any        host 100.1.0.2
 ! Permit ISAKMP packets reach router
 ! See VPN section for explanation
 permit udp any eq 500 host 100.1.0.2 eq 500
```

But wait there's more. Once an IPSec packet is decrypted by the router, the decrypted packet is sent back through the same incoming interface access-list that the IPSec and ISAKMP passed through initially. Why, to allow the router a chance to apply access rules to the incoming decrypted VPN tunnel packets. Thus the following lines were added to the incoming access-list allowing successfully connected VPN remote client full access to the internal Asmallbus network. At first look it may appear this has opened up a hole in the incoming access-list allowing spoofed source address IP packets into the internal network. The router however expects these packets to be IPSec ESP packets, if they aren't it drops them.

```
 ! Permit decrypted VPN client packets enter internal network
 ! See VPN section for explanation
 permit ip 100.0.0.8 0.0.0.3 100.0.0.0 0.0.0.7
```

This completes the configuration of the router for VPN IPSec client termination.

Router hardening

There are a number of configuration options/features on the router that need to be checked, changed or configured to increase the security of the router itself. Some of default settings on the router are for historical reasons, when the Internet was a more caring, sharing and trusted place. Most of the following recommendations come from the excellent, but very large, "Router Security Configuration Guide" produced by the USA National Security Agency.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

On all interfaces of the router turn off the following features, they either give information away about the router or can be used by attackers to help gain access to the internal network.

```
Interface Ethernet 0
 no ip unreachables
 no ip redirect
 no ip directed-broadcast
 no ip mask-reply
 no ip proxy-arp
 no cdp enable

Interface Dialer 1
 no ip unreachables
 no ip redirect
 no ip directed-broadcast
 no ip mask-reply
 no ip proxy-arp
 no cdp enable
```

Enable the encryption of passwords in the router configuration. Although the encryption algorithm isn't strong, and is easily reversed it does provide a limited protection from "over the shoulder" viewing of the router configuration and learning of passwords.

```
service password-encryption
```

Encrypt the enable password for the router using the strong MD5 algorithm and remove any possible trace of the enable password configured using the reversible encryption algorithm.

```
no enable password
enable secret 5 $1$V1ZA$hJBcNbS4ZqgkmOejWTaGM.
```

Turn off all potentially dangerous services that are not required for the operation of the router. In this configuration, the router doesn't need the following features or services.

- Bootp server
  (allows other routers to boot from this router)
- HTTP server
  (allows some configuration of the router to be performed via web browser)
- HTTP secure server
  (same as HTTP but encrypts data using SSL)
- SNMP server
  (Simple Network Management Protocol, allows remote machines to collect and configure information about router)
- TCP and UDP small servers
  (A number of simple servers like, TCP echo and chargen not used anymore and potential security holes)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- IP finger
  (a protocol which allow hosts to gather information about who is logged into router)

```
no ip bootp server
no ip http server
no ip http secure-server
no snmp-server
no tcp-small-servers
no udp-small-servers
no ip finger
```

Cisco Discovery protocol is a layer 2 protocol which informs adjacent Cisco devices of the presence this router; it's leaks information about the router, so turn it off.

```
no cdp run
```

It's possible for the router to load its configuration at boot-up. We definitely want the router to load its stored configuration so these are turned off.

```
no service config
no boot network
```

Router doesn't need to perform any DNS lookups itself, so turn off this service.

```
no ip domain lookup
```

Packet assembler and disassembler (PAD) are used by X.25 services. This router isn't using any X.25, so turn it off.

```
no service pad
```

Source routing enables an IP packet to be directed to other than what is specified in the routers routing table. It usually isn't required and certainly isn't required in the Asmallbus network.

```
no ip source-route
```

Turn-on logging and send it to a syslog server. In this case, the Windows 2000 server is running a freeware syslog server to collect and store all the messages from the router. Also, create a 16,000-byte buffer in the router memory, which can be useful for router debugging purposes. At the same time have log messages time stamped with the date and time but ensure the router's time is correctly synchronized to an accurate time source, see NTP configuration later. Also ensure logging isn't sent to the console interface of the router as this can impact on router performance. Cisco uses logging levels similar to Unix systems, from critical, only the most important information is reported, to debugging, send all messages, no matter how trivial. For maximum information, set this to debugging level.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
no logging console
logging trap debugging
logging buffer 16000
logging host 100.0.0.2
service timestamps debug datetime msec show-timezone
service timestamps log   datetime msec show-timezone
```

Allow console access to router, you never know when you may require it but apply a strong and long password to the console port, timeout idle sessions after 10 minutes and don't allow this port to be used of outgoing connections. Of course, this assumes the router is placed in a secure location at Asmallbus offices.

```
line con 0
 exec-timeout 10 0
 login
 transport output none
 password 7 110A1016141D63A7593F3493E
```

Stop back door access via the auxiliary port, timeout idle sessions immediately, don't allow login via this port and don't start an exec (i.e. router prompt) session but as a backup still apply a password to it.

```
line aux 0
 exec-timeout 0 1
 no exec
 login local
 password 7 110A1016141D
 transport input none
```

Allow remote access to the router but only via SSH and only from the IP address defined in access-list 99 that happens to be the Manager's workstation. As we are using SSH a username/password needs to be entered for the manager to access to router via SSH. Timeout idle sessions after 10 minutes and use the username and password defined in the routers local database for access. Note there is a backdoor here. Each of the Salesman have also a username and password defined in the router, they could, if they can get access to the Manager's Workstation they could get first level access to the router. They would still need the enable password to be able to make any configuration changes. SSH requires a username and password pair, while telnet login only requires a password which can be defined under the "line vty 0 4" configuration, it's a trade-off.

```
username manager password 7 065982367F543D46A72389127316

line vty 0 4
 access-class 99 in
 exec-timeout 10 0
 login local
 transport input ssh
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
access-list 99 permit 100.0.0.3
access-list 99 deny any log
```

A banner also needs to be configured in the router to inform anyone accessing this router that there access will be logged and access must be authorized.

```
Banner login $
Access to this device is only permitted by authorised users
All access to this device is logged
$
```

Allow the router to send periodic keep alive packets on TCP sessions into and out of the router. The router will then be able to detect dead TCP sessions and end them.

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

To control the number of times a SSH session can be tried and the time period the router will wait for a password.

```
ip ssh time-out 60
ip ssh authentication-retries 2
```

Asmallbus ISP provides a Network Time Protocol (NTP) service to their customers by providing an NTP server on the router Asmallbus ADSL service is connected too. Typically, you would attempt to get network time protocol from an authenticated and verified source. In this case, Asmallbus have determined they can trust their ISP.

```
sntp server 100.1.0.1
```

This ends the configuration of the Asmallbus router. As stated at the beginning lots of the configuration settings are specific to the example network. This configuration can be used as a template, modified to suit your particular requirements.

Nmap testing results

Nmap was let loose to scan this network from the Internet side (outside). The following is what nmap could determine.

First test, nmap was targeted against the Windows 2000 server without any security rules in the router. This was a simple TCP connect scan on the most common low ports as a quick check to see what nmap could determine and produce a baseline for comparision.

```
#nmap -sT -O -p20-100 -v -P0 100.0.0.2

Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-07-14 22:22
CEST
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
Host 100.0.0.2 appears to be up ... good.
Initiating Connect() Scan against 100.0.0.2 at 22:22
Adding open port 25/tcp
Adding open port 53/tcp
Adding open port 80/tcp
Adding open port 21/tcp
Adding open port 42/tcp
Adding open port 23/tcp
The Connect() Scan took 0 seconds to scan 81 ports.
For OSScan assuming that port 21 is open and port 20 is closed
and neither are firewalled
Interesting ports on 100.0.0.2:
(The 75 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
42/tcp     open        nameserver
53/tcp     open        domain
80/tcp     open        http
Remote operating system guess: Windows Millennium Edition (Me),
Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=6197 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 1.293
seconds
```

Nmap seems to have guessed the operating system was from Microsoft and found lots of open ports on the server, which would be expected.

Second test, the same scan as performed above but with all the access-list, inspect and audit rules in place on the router. The incoming dialer interface access-list allows nmap to probe only the SMTP and HTTP ports of the server.

```
#nmap -sT -O -p20-100 -v -P0 100.0.0.2

Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-07-14 20:25
CEST
Host 100.0.0.2 appears to be up ... good.
Initiating Connect() Scan against 100.0.0.2 at 20:25
Adding open port 25/tcp
Adding open port 80/tcp
The Connect() Scan took 21 seconds to scan 81 ports.
Warning:  OS detection will be MUCH less reliable because we did
not find at least 1 open and 1 closed TCP port
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
For OSScan assuming that port 25 is open and port 39804 is closed
and neither are firewalled
Interesting ports on 100.0.0.2:
(The 79 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
80/tcp     open        http
Remote operating system guess: Windows XP Professional RC1+
through final release
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=15750 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 26.099
seconds
```

The router produced the following log messages while nmap was running.

```
Jul 14 12:24:36.003 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6(47760) -> 100.0.0.2 (46), 1 packet
Jul 14 12:24:38.999 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47760) -> 100.0.0.2 (46), 1 packet
Jul 14 12:24:41.979 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47790) -> 100.0.0.2 (46), 1 packet
Jul 14 12:24:45.023 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47760) -> 100.0.0.2 (46), 1 packet
Jul 14 12:24:45.599 UTC: %SEC-6-IPACCESSLOGRL: access-list
logging rate-limited or missed 145 packets
Jul 14 12:24:48.003 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47820) -> 100.0.0.2 (71), 1 packet
Jul 14 12:24:50.979 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47790) -> 100.0.0.2 (46), 1 packet
Jul 14 12:24:54.063 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47850) -> 100.0.0.2 (88), 1 packet
Jul 14 12:24:55.331 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (47960) -> 100.0.0.2 (20), 1 packet
Jul 14 12:24:56.343 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (48040) -> 100.0.0.2 (75), 1 packet
Jul 14 12:24:57.639 UTC: %IDS-4-TCP_NO_FLAGS_SIG: Sig:3040:TCP -
No bits set in flags - from 100.1.0.6 to 100.0.0.2
Jul 14 12:24:57.643 UTC: %IDS-4-TCP_SYN_FIN_SIG: Sig:3041:TCP -
SYN and FIN bits set - from 100.1.0.6 to 100.0.0.2
Jul 14 12:24:57.647 UTC: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP -
FIN bit with no ACK bit in flags - from 100.1.0.6 to 100.0.0.2
Jul 14 12:24:57.651 UTC: %SEC-6-IPACCESSLOGP: list INTERNET-IN
denied tcp 100.1.0.6 (46010) -> 100.0.0.2 (39804), 1 packet
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
Jul 14 12:24:59.091 UTC: %FW-6-SESS_AUDIT_TRAIL: smtp session
initiator (100.1.0.6:47875) sent 0 bytes -- responder
(100.0.0.2:25) sent 107 bytes
```

The router could see something strange was happening. The denied packet records were produced as nmap scanned thru the ports and was stopped by the router access-list rules. At the same time the IDS function picked up some unusual TCP packets. The three Cisco IDS signatures detected were all “attack” signatures so the router dropped these packets. The router seems to have confused nmap’s operating system determination feature, getting it slightly wrong.

Note, the router protects itself by rate limiting the production of access-list log messages. If too many log messages are being produced, the router drops the excess. Also notice the audit record produced by nmap’s connection to the SMTP port of the server.

Comments

The entire firewall router configuration detailed in this document forms only one small part of the security for a small business. As stated by SANS “A firewall is the primary opportunity for attack negation[11]”. Many other avenues of attack are still open even with the most comprehensively configured firewall protecting your internal network.

By necessity, the SMTP, HTTP and DNS ports of the Windows 2000 server must the left open to the Internet. Although the firewall router will check for some of the more “simple” types of attacks on these open application ports, nothing is more important than making sure all machines have the latest security patches installed.

Other security software that should be considered are;

- Virus scanning with up to date virus signatures on all machines.
- Incoming and outgoing virus scanning of mail on Win 2000 server.
- Personal firewalls installed on all machines or at least the travelling Salesman laptops.
- Host based Intrusion detection on the server.
- Syslog package for the server to collect the logs from the firewall/router.
- Log analysis package for the firewall/router logs.

Security is also not just about hardware and software. Every business needs a security policy that defines things like;

- What staff can and can’t do, that is, what is acceptable behaviour?
- Who loads the patches in the machines and when?
- Who is responsible for creating and deleting user accounts?
- Who authorises new user accounts?
- How often are the logs from the firewall/router and server inspected?

[11]The SANS Institute, SANS Security Essentials III: Internet Security Technologies (2003), Firewalls and Honeypots, slide 4.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Who inspects these logs?
- How acts on the findings in the logs?
- Are the servers backed up?
- Who backs up the servers?
- Who does what in the event of a security incident?
- And so on…

© SANS Institute 2003, Author retains full rights

Conclusions

Creating a secure environment to conduct business on the Internet is possible. What has been presented here is really just a template that would need to be modified to suit each particular businesses needs. It should, however, provide a good starting point to getting your firewall configured as securely as possible and thus putting in place a strong first line of defence against attacks from the Internet on your business.

© SANS Institute 2003, Author retains full rights

Glossary

ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
CBAC	Context Based Access Control
CHAP	Challenge Handshake Authentication Protocol
DES	Digital Encryption Standard
DF	Don't Fragment
DMZ	De-Militarised Zone
DNS	Domain Name Service
ESP	Encapsulating Security Protocol
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IOS	Input Output System
IPSec	IP Security
ISAKMP	Internet Security Association Key Management Protocol
MD5	Message Digest 5
MTU	Maximum Transfer Unit
NSA	National Security Agency
NTP	Network Time Protocol
PPP	Point-to-Point Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

© SANS Institute 2003, Author retains full rights

References

1. CNET Networks, CNET review Cisco 837 ADSL router URL: http://reviews.cnet.com/CISCO_837_ADSL_RTR/4505-3334_7-21042425.html?tag=dir

2. Cisco Systems, Cisco 800 series routers data sheet, URL: http://www.cisco.com/en/US/products/hw/routers/ps380/products_data_sheet09186a008010e5c5.html

3. Cisco Systems, Cisco IOS Firewall Data sheet URL: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

4. Evan Davies, CBAC – Cisco IOS Firewall feature set foundations (2002), URL: http://www.sans.org/rr/papers/21/806.pdf

5. Cisco Systems, Cisco IOS Intrusion Detection System Signature List URL: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008014c532.html

6. Cisco Systems, Cisco Easy VPN, URL: http://www.cisco.com/en/US/products/sw/secursw/ps5299/prod_brochure09186a00800a4b36.html

7. Internet Assigned Numbers Authority, Request For Comments: 3330, Special-Use IPv4 Addresses (September 2002), URL: http://www.ietf.org/rfc/rfc3330.txt?number=3330

8. Marc Slemko, Path MTU Discovery and Filtering ICMP (12 November 1998), URL: http://alive.znep.com/~marcs/mtu/

9. USA National Security Agency, Router Security Configuration Guide, Version 1.1 (27 September 2002) URL: http://www.nsa.gov/snac/cisco/download.htm

10. Cisco Systems, Configuring IPSec Between Two Routers and a Cisco VPN Client 3.x (12 November 2002), URL: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a0080094685.shtml

11. The SANS Institute, SANS Security Essentials III: Internet Security Technologies (2003), Firewalls and Honey pots, slide 4.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix

The following is the complete listing from the “Asmallbus” Cisco 837 router. Note some configuration entries are default settings.

```
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
service password-encryption
no service config
no boot network
!
hostname asmallbus-router
!
logging buffered 16000 debugging
no logging console
enable secret 5 $1$V1ZA$hJBcNbS4ZqgkmOejWTaGM.
!
username manager password 7 065982367F543D46A72389127316
username salesman1 password 7 01040316540F000720484801185E11
username salesman2 password 7 0942430C0B531D1A595B52383A213F
username salesman3 password 7 04510F1509294A17011356434B5309
!
aaa new-model
!
aaa authentication login   userauthenicate local
aaa authorization  network groupauthorise  local
!
ip subnet-zero
no ip source-route
no ip domain lookup
!
no ip bootp server
ip cef
ip inspect audit-trail
ip inspect max-incomplete low 20
ip inspect one-minute low 20
ip inspect udp idle-time 15
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect tcp synwait-time 15
ip inspect name INTERNET-IN tcp alert on audit-trail on
ip inspect name INTERNET-IN udp alert on audit-trail on
ip inspect name INTERNET-IN smtp alert on audit-trail on
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
ip inspect name INTERNET-IN http alert on audit-trail on
ip inspect name INTERNET-IN fragment maximum 2 timeout 1
ip inspect name INTERNET-OUT tcp alert on audit-trail on
ip inspect name INTERNET-OUT udp alert on audit-trail on
ip inspect name INTERNET-OUT smtp alert on audit-trail on
ip inspect name INTERNET-OUT http alert on audit-trail on
ip inspect name INTERNET-OUT fragment maximum 2 timeout 1
ip audit notify log
ip audit po max-events 100
ip audit smtp spam 20
ip audit name INTERNET-IN info action alarm
ip audit name INTERNET-IN attack action alarm drop reset
ip audit name INTERNET-OUT info action alarm
ip audit name INTERNET-OUT attack action alarm drop reset
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group remotesalesgroup
 key 0 th1sISl0gpReSHaREDkEy
 dns 100.0.0.2
 wins 100.0.0.2
 domain asmallbus.com
 pool ippool
!
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 userauthenticate
crypto map clientmap isakmp authorization list groupauthorise
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0
 ip address 100.0.0.1 255.255.255.248
 no ip proxy-arp
 no ip unreachables
 no ip ip mask-reply
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
 ip access-list E0-in in
 ip tcp adjust-mss 1400
 no ip mroute-cache
!
interface ATM0
 description ADSL service
 no ip address
 no ip mroute-cache
 no atm ilmi-keepalive
 dsl operating-mode ansi-dmt
!
interface ATM0.1 point-to-point
 no ip mroute-cache
 pvc 8/35
  vbr-nrt 64 64 32
  ip addr inarp
  pppoe-client dial-pool-number 1
 !
!
interface Dialer1
 description ADSL service
 ip address 100.1.0.2 255.255.255.252
 ip access-group Internet-in in
 no ip proxy-arp
 no ip unreachables
 no ip ip mask-reply
 ip mtu 1492
 ip inspect INTERNET-IN in
 ip inspect INTERNET-OUT out
 ip audit INTERNET-IN in
 ip audit INTERNET-OUT out
 encapsulation ppp
 no ip mroute-cache
 dialer pool 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname asmallbus@asmallbus.anisp.com
 ppp chap password 7 030752180500
 crypto map clientmap
!
ip local pool ippool 100.0.0.8 100.0.0.11
no ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip ssh time-out 60
ip ssh authentication-retries 2
no ip http server
no ip http secure-server
```

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
!
access-list 99 permit 100.0.0.3
access-list 99 deny any log
!
ip access-list extended Internet-in
 deny   ip   100.0.0.0 0.0.0.15       any log
 deny   ip   host 100.1.0.0 0.0.0.3   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   192.0.2.0 0.0.0.255      any log
 deny   ip   169.254.0.0 0.0.255.255  any log
 deny   ip   224.0.0.0 31.255.255.255 any log
 permit tcp  any gt 1023          host 100.0.0.2 eq smtp
 permit tcp  any gt 1023          host 100.0.0.2 eq www
 permit tcp  host 100.1.1.1 gt 1023 host 100.0.0.2 eq domain
 permit esp  any                  host 100.1.0.2
 permit udp  any eq 500           host 100.1.0.2 eq 500
 permit ip   100.0.0.8 0.0.0.7    100.0.0.0 0.0.0.7
 permit icmp any                  100.0.0.0 0.0.0.7 reachable
 permit icmp any                  100.0.0.0 0.0.0.7 time-exceeded
 permit icmp any                  100.0.0.0 0.0.0.7 echo-reply
 deny   tcp  any range 0 65535   any range 0 65535 log
 deny   udp  any range 0 65535   any range 0 65535 log
 deny   ip   any                 any log
exit
!
ip access-list extended E0-in
 deny   ip   any 0.0.0.0 0.255.255.255    log
 deny   ip   any 10.0.0.0 0.255.255.255   log
 deny   ip   any 127.0.0.0 0.255.255.255  log
 deny   ip   any 172.16.0.0 0.15.255.255  log
 deny   ip   any 192.168.0.0 0.0.255.255  log
 deny   ip   any 224.0.0.0 31.255.255.255 log
 deny   ip   any 192.0.2.0 0.0.0.255      log
 deny   ip   any  169.254.0.0 0.0.255.255 log
 permit tcp  host 100.0.0.3 gt 1023    host 100.0.0.1 eq 22
 permit icmp 100.0.0.0 0.0.0.7         host 100.0.0.1 echo
 permit icmp 100.0.0.0 0.0.0.7         host 100.1.0.2 echo
 deny   ip   any                       host 100.0.0.1 log
 deny   ip   any                       host 100.1.0.2 log
 permit tcp  100.0.0.0 0.0.0.7 gt 1023 any eq www
 permit tcp  100.0.0.0 0.0.0.7 gt 1023 any eq 443
 permit udp  100.0.0.0 0.0.0.7 gt 1023 any eq 53
 permit ip   100.0.0.0 0.0.0.7         100.0.0.8 0.0.3
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
 permit tcp  host 100.0.0.2 gt 1023    any eq smtp
 permit tcp  host 100.0.0.2 gt 1023    host 100.1.1.1 eq domain
 permit icmp 100.0.0.0 0.0.0.7         any echo
 deny   tcp  any                       any range 0 65535 log
 deny   udp  any                       any range 0 65535 log
 deny   ip   any                       any log
exit
!
logging trap debugging
logging host 100.0.0.2
logging buffer 16000
dialer-list 1 protocol ip permit
no cdp run
!
Banner login $
Access to this device is only permitted by authorised users
All access to this device is logged
$
!
line con 0
 exec-timeout 10 0
 login
 transport output none
 password 7 110A1016141D63A7593F3493E
line aux 0
 exec-timeout 0 1
 no exec
 login local
 password 7 110A1016141D
 transport input none
line vty 0 4
 access-class 99 in
 exec-timeout 10 0
 login local
 transport input ssh
!
sntp server 100.1.0.1
!
end
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**