GIAC Level Two Practical Assignment

Firewalls and Perimeter Protection Curriculum

Monterey, CA
October 15 – 19, 2000

SANS Monterey 2000
Mark Evans
October 30, 2000

INTRODUCTION

This paper will outline the network architecture of GIAC Enterprises, an Internet eBusiness that sells online fortune cookie sayings. The emphasis on the architecture will be on security; i.e., the secure operations of daily business with customers, partners, and employees of GIAC Enterprises. To adequately illustrate the planned security architecture, a security policy and audit procedure must also be conceived and implemented to ensure any exposures to risks are mitigated and documented.

BACKGROUND

The booming Internet Business platform has extended its fibrous fingers to the most remote places on earth. In Paddywack, North Dakota, several venture capitalists have agreed to finance the startup of GIAC Enterprises, an online "fortune cookie saying" company. This corporation will rely on the heavy demand of Oriental cuisine and it's tradition of supplying a fortune cookie with every meal. GIAC has created strategic partnerships with several fortune cookie makers that have agreed to use GIAC-supplied fortune cookie sayings. The three cookie makers require access to ordering and inventory databases and shipping projections in order to accurately predict their cookie-baking schedule. Additionally, every fortune cookie saying will have the URL of GIAC Enterprises printed on the back so the restaurant customers can visit the company's website. At the website, visitors can receive virtual fortune cookies, register for a mailing list that will send them one fortune cookie saying everyday, and view corporate information such as investor relations, job opportunities for caption writers, and so forth.

The CIO at GIAC Enterprises allows employees to browse websites and send external email from corporate computers. She feels this keeps the writers abreast of current news and trends, which provides input for clever sayings.

Corporate employees must be able to login to the network from remote locations. Fortune cookie saying salesmen must have access to email and corporate data while traveling.

All of these requirements must be dealt with in a manner that will provide maximum security with adequate performance and the least exposure to undue risk of compromising corporate data and integrity.

SECTION 1

SECURITY ARCHITECTURE

To accurately detail the GIAC Enterprise's network it should be segmented into workable sections. Refer to figure 1 for details. These are outlined as follows:

- Internet or untrusted Zone – this area is considered hostile and requires extreme caution when allowing connections.
- Partner Zone – this area is where the business partners and remote users will gain access to their needed information.
- Screened Zone – this area is where customers will visit the website, the external DNS resides,
- Protected or Trusted Zone – this area is behind the perimeter and is generally considered a higher level of trust than the other zones

Internet Demarcation

Because of its ubiquitous nature and relative inexpensive cost, the Internet has become the de facto choice of interconnection between sites that only require intermittent connections. The GIAC Enterprises Internet connection is funneled through a Cisco PIX firewall with three interfaces, two internal and one external. This device acts as a first level packet filtering device and a router. It contains both ingress and egress access control lists (ACLs). Static routes are listed in the PIX to control data flow to appropriate networks and dropping packets that try to spoof valid addresses.

External Interface 1 (EX1) is connected to the ISP router and is considered a hostile connection. GIAC does have authority to request that the basic security ACLs be applied to it and an SLA establishes the ISP responsibility to ensure they are implemented at all times.

Internal Interface 1 (Screened IN1) is connected to the screened subnet portion of our perimeter. Because this subnet is accessed by Internet entities without full authentication or validation it must be considered untrusted from the viewpoint of the corporate network. Websurfers, customers and the like access the Webserver located on this screened subnet. On this public webserver is the corporate homepage, email listserver sign-up, e-commerce fortune cookie programs, and other such public information. Secure Socket Layer (SSL) encrypted sessions are established with external users that wish to pass personal information along to the company. This is accomplished via a Digital Certificate acquired from a trusted third party, such as Verisign. This subnet also houses the external DNS server that replies to UDP DNS queries from external DNS lookups. It does not support zone transfers since there is nothing to transfer with and it only supports type MX and type A DNS lookups for the two external devices. Removing all extraneous services from the systems hardens both of these devices. All critical system files are baselined using Tripwire (http://www.tripwire.com/). Any publicly accessed data is encrypted using Pretty Good Privacy Version 6.5 with a minimum of 1024bit encryption.

Internal Interface 2 (Partner IN2) is connected to the Partner subnet portion of outer perimeter. Suppliers, vendors, and partners access dedicated servers that contain data on inventory, shipment dates, etc. Because GIAC personnel cannot monitor, audit or control these external networks, they must be considered untrusted and limited access should be granted. To provide authorized personnel with access to the data, A VPN product is connected to this subnet. We are using the Shiva (formerly Isolation) Infocrypt hardware VPN. This device allows for fast hardware VPN authentication of clients utilizing a Shiva Client VPN service. This product is controlled and distributed by GIAC Security personnel and is hard coded with the appropriate interface's IP address. Once installed on the client machine, a password token is generated and communicated to the user via off-line methods. This ensures that the user is aware of his/her responsibilities that accompany the password, and it provides a medium level of trust in assuring that only the person given the password is using it. The VPN hardware/software combination provides an effective tunnel over the Internet that allows access to the partner data. This Ethernet then proceeds to the Gauntlet firewall.

Remote users that require access to the corporate data also access it via the VPN implementation. This software "shim" installed on remote computers just below layer three on the OSI stack examines the destination address and encrypts the entire packet. Only with a valid key will the Infocrypt device forward the information onto the appropriate destination. IPsec or proprietary algorithm can be utilized for the VPN encryption

On the other side of the Ethernet connecting the partners subnet is a Network Associates (formerly TIS) Gauntlet Firewall. This device acts as a proxy firewall for the GIAC Enterprises network.

At this point, the only packets the firewall should see are those destined for internal systems. By policy, these should only be email (SMPT), DNS lookups returns (UDP/53), web info (HTTP/HTTPS) and requests from the VPN remote users. It is important to note that allowed services should be proxied at this firewall. Merely filtering based on port/service numbering does not protect against trojans or other hidden data. More on that later.

Keeping up-to-date

With any security paradigm it is essential to stay current and up-to-date on what vulnerabilities are being uncovered. Many systems today have automatic update features to help assist administrators with this requirement. These are both a blessing and a curse. Unwittingly allowing a product to auto-update can have disastrous effects. Patches, especially security patches, must be treated cautiously when being applied. The last thing any administrator needs to have happen is a work stoppage because of a "simple" patch that was applied to the firewall or email server. When applying any security patch all factors must be looked at prior to implementation. Versions, hardware type, OS level, and actual exposure are a few of the areas that must be reviewed. A testbed implementation is always a good choice prior to fielding any patch. Automated update procedures should only be used in situations where the system impact is minimal such as a virus signature.

As a matter of policy, ALL GIAC administrators, not just security personnel are required to stay abreast of industry security issues. Among the places to check are vendor sites that support GIAC systems. These include:

- Microsoft Corp. (http://www.microsoft.com//security/)
- Compaq Corp. (http://www.compaq.com/)
- NAI (Gauntlet Firewall) (http://www.NAI.com/)
- TrendMirco Virus (http://www.trendmicro.com/)
- Hewlett-Packard (http://www.hp.com/security/support/)
- Cisco (http://www.cisco.com/warp/public/707/advisory.html)

Non-vendor sites that provide information regarding current exploits, virus trends, and the like are also invaluable. These include:

- CERT (http://www.cert.org)
- SANS Security (http://www.sans.org)
- Virus Security Alerts (http://www.antivirus.com/info)

Email lists are vital information as well. These include:

- BuqTraq lists (http://www.ntbugtraq.com)
- SANS Newsbites (http://www.sans.org)
- NT Security Updates: (subscribe-Security_UPDATE@list.win2000mag.net)

It is also worth while to mention that individual products require close attention as well. Email clients, browsers, PC operating systems, and the like are among the items that should be reviewed for security and operational updates.

Need-to-Know

At GIAC Enterprises confidential corporate information must be protected from external threats, but also internal threats, accidental disclosure, or unruly employees. As we all know, the greatest potential of risk comes from within the confines of the network because we trust the people working there. What happens when someone gets disgruntled or is too inquisitive? Financial data, Privacy Act data, Payroll, all become potential targets. To help ensure the protection of this data, a Client – Server encryption program will be utilized throughout the protected network. This product, Shiva VPN Client, is a software shim that sits in the OSI stack below layer three and inspects the destination address. When the address is a protected server, such as Payroll, HR information, etc., the entire packet is encrypted and a new header is placed on it. This accomplishes several tasks and prevents a few as well.

- It helps prevents sniffing of clear text data on the wire.
- It aids in the prevention of destination port attacks and scanning since the software can redirect the port.
- It provides confidentiality
- It provides a higher level of authentication since the VPN software must authenticate the user.
- It restricts the user community to those that have the software and a valid business need.

Non-critical network access requires the standard loginID and password challenge at each server. Each user is required a unique userID. No sharing of accounts is allowed. Administrators are required to login to systems with a unique admin ID that is associated to them personally. No generic logins, such as “administrator” or “root” are allowed.

For device administration, a TACACS server is implemented to authenticate userID prior to connection to the devices. At the PIX, EXEC levels are established to limit the number of people that have full admin rights. The telnet session is performed via SSH to the TACACS server, which is then hardwired via serial port to the PIX. Administration of the Gauntlet is done through an encrypted session via a vendor-provided management tool. Alternatively and as a back up, the Cisco Security Manager can be used to configure the PIX. This has encrypted sessions and a GUI in which syntax is staged prior to uploading.

Keeping Viruses Out

Many IT professionals agree that the greatest single threat to a network is Virus Attacks. They expound great resources during recovery, shatter user and management confidence, and they can go undetected for a long time. Active virus scanning is performed on all GIAC systems on a daily basis. Users are not permitted to disable the program. I/O scanning is also performed on each PC to help prevent email viruses from email systems that circumvent the corporate email server, such as Hotmail, Yahoo Mail, etc. Updates are performed automatically by client software downloading signature files from a centralized secure server within the domain. This alleviates the need for each PC to access the Internet and ensures the source of the information is real and trusted. On the perimeter, active virus scanning is performed at the email server with TrendMicro’s Exchange Mail Virus scanning. It supports quarantining of any attachment that cannot be cleaned as well and blocking attachments by extension, size, or completely. The ScanMail engine and signatures can be updated on a scheduled basis automatically from an SSL server provided by TrendMirco. A daily update is performed at 7:00 a.m. at GIAC Enterprises.

Keeping Track

A centralized log server is deployed that receives notices of virus scan completion and detection. It is also used to review NT Event logs daily that track the logins by unique userID. Also tracked is object access and unsuccessful attempts to gain access. This server also is the logging server for the PIX and Gauntlet firewalls. All hits on ACLs and firewall rules are logged and reviewed daily. Depending on the severity level of the event logged, an alert can be sent out to notify the administrator.

One vital exercise concerning any security architecture is review and updating. Security plans are living documents. They must constantly be checked and revalidated against current trends and technology. At GIAC Enterprises, weekly staff meetings are held at which security topics are discussed. The policy is reviewed at a minimum semi-annually by the security manager to ensure it is up-to-date.

Testing of various systems should be performed on a weekly basis to ensure they are doing what they are supposed to do. This may be a simple at trying to telnet to a device or as complex as reviewing the complete baseline of a system.

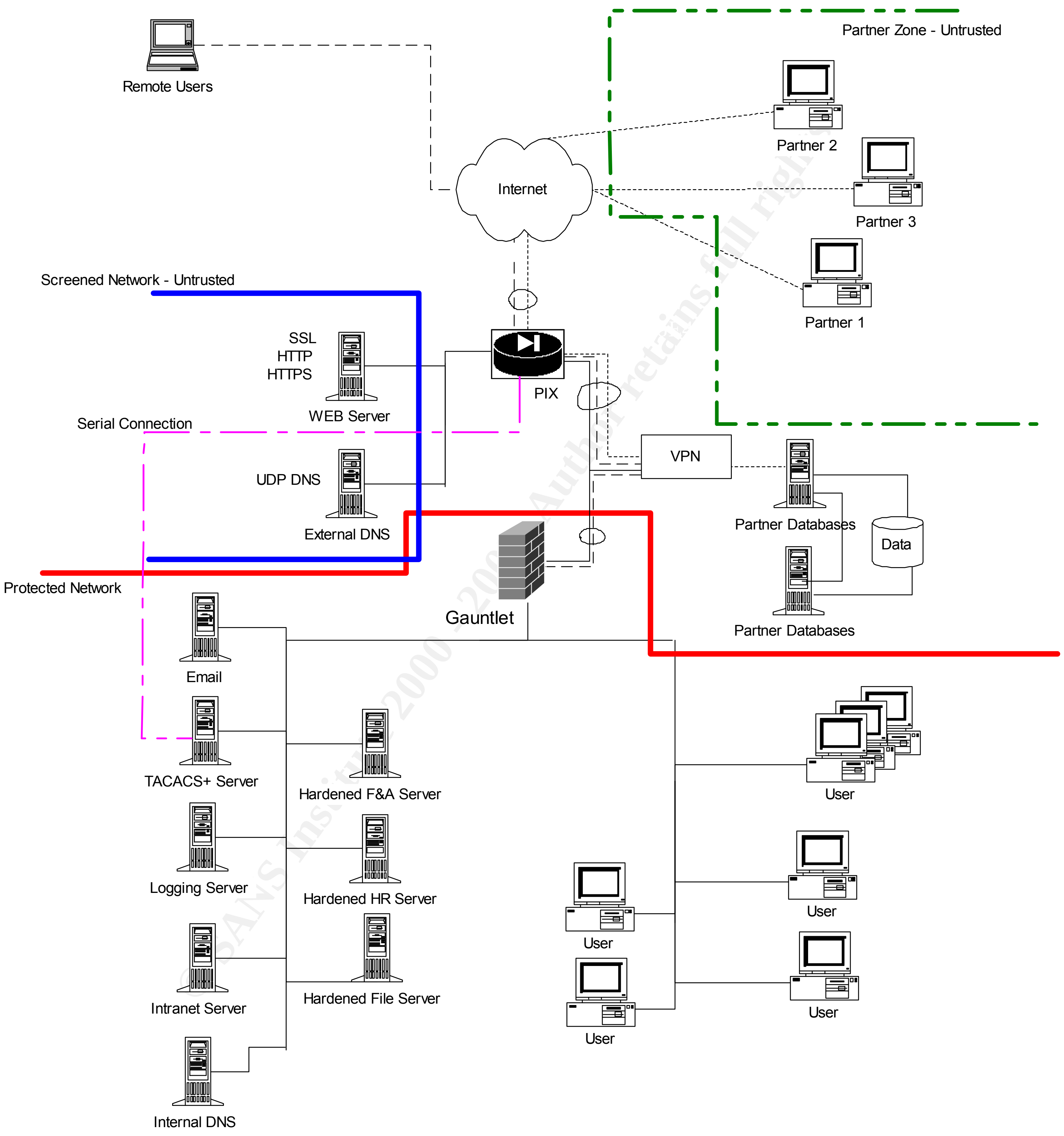


Figure 1 Network Architecture

SECTION TWO

SECURITY POLICY

The base line security policy implemented at the Internet gateway is that which is defined in Appendix B of the SANS Top Ten document located at http://www.sans.org/topten.htm. It is applied to the ISP router on which GIAC can only dictate policy settings; GIAC does not have change authority. Part of the Service Level Agreement (SLA) with the ISP is they will comply with the basic security policy set forth above.

One may ask why there is no premise router that we control to perform screening functions. The PIX in this scenario is acting as my premise router. It is connected to the router of the ISP handling my Internet connection. The PIX, by default, stops all incoming traffic from flowing across it so all the basic security policies are in place. There are static routes configured on the PIX to handle traffic flow between the ISP router and the GIAC network, and within the GIAC DMZ. This negates our need to have any dynamic routing functions. If a router were placed between the PIX and the ISP router it would not serve any routing purpose because it is a static route between the two devices. Secondly a premise router could serve as a potential Denial-of-Service attack point. The PIX is immune to DOS attacks because it has no TCP/IP services on the outside interface, it drops incoming SYNs to dynamic translation slots and PIX static conduits can have a maximum connection and embryonic connection number. For this reason, I chose not to put another device in the network to complicate matters.

The basic operation of the PIX is to deny everything inbound that is not explicitly allowed and to allow everything outbound unless explicitly denied. This may seem like the ideal scenario, but remember that anything outbound requires a return path. So all outbound connections also have an inbound connection. We will tighten both inbound and outbound traffic flows to provide the best protection possible while still accomplishing our goal – selling fortune cookie sayings.

PIX Configuration

In addition to the base line security policy, the following items should be implemented as part of the PIX configuration:

**Note: Since this is not a configuration document, I am assuming the basic configuration of the PIX, such as interface names, static routes, etc. is already accomplished. I will concentrate on the security aspect of the configuration. The interface names are those defined in section one. All commands are entered while in the privileged mode and in CONFIG status. The first octet of the global IP address is marked with "XXX" to ensure it is not a real address. It is also assumed that the PIX version is 4.2(5) or higher.*

Configuring the Interfaces

The security level assigned to a PIX interface determines what level of protection it can have and what direction traffic will flow. The lowest security level is zero (0), and is almost always assigned to the interface connected to the Internet. Perimeter interfaces can be assigned any level between zero (0) and 100. When a command requires two interface names, such as *command (if_name, if_name)*, always specify the more secure interface first. (i.e., that one with a higher number). For the GIAC network, our interfaces are defined as follows:

Position	Name	Security Level
Outside	EX1	0 (zero)
Inside	Screened_IN1	50
Inside	Partner_IN2	100

Of particular note is that the partner zone has a higher security level than the Screened zone. Because the Screened zone is publicly accessed it has a higher risk potential. Having a lower security level prevents traffic from reaching the other interfaces unless specifically allowed. So, someone on the screened subnet of GIAC's network cannot get to the partner's subnet even if a server were to be compromised, it could not affect the other network.

Network Address Translation

One of the strong points of the PIX is its ability to use Network Address translation (NAT) to shield IP addresses from public view. This is particularly helpful in confusing those who wish to perform scans. It also give great flexibility to the network administrator in assigning network addresses according to RFC 1918 (http://rfc.fh-koeln.de/rfc/html/rfc1918.html).

To implement NAT, enter the following commands:

- `global (outside) EX1  XXX.193.220.8-XXX.193.220.254 netmask 255.255.255.0`
- `nat (inside) 1 0.0.0.0 0.0.0.0 0 0`

We start our pool at .8 because the addresses 1 through 7 are used in static mappings. The .3 address is reserved for future use incase we need to add another device somewhere on the network.

The reason for using NAT as a security technique is to shield real addresses from the world. Only publicly accessible devices, such as the web server and email server, need to be advertised. These two commands setup the available pool of addresses that can be used to translate an internal address to. The PIX keeps track of the translations in a table. In the table are the virtual IP addresses taken from the pool of the global list, their corresponding internal addresses, timeout limits, and connection statuses. This ensures no session can be hijacked or policy violations can be committed.

We will use the private class A network of 10.0.0.0 for out internal addresses with a 255.255.0.0 subnet mask. Our internal network scheme will use the following addresses:

- 10.1.0.0 – Partner_IN1 and Gauntlet
- 10.2.0.0 – Screened_IN1
- 10.3.0.0 – Protected network behind the Gauntlet

The public sees the following device available for GIAC Enterprises when it does a DNS query:

- XXX.193.220.4 MX record (email host)
- XXX.193.220.5 A record (web server)
- XXX.193.220.6 A record (DNS Server)

In reality, the actual IP addresses assigned to each device is a private network address from the 10.0.0.0 network. We assigned the following address to the devices:

- 10.3.0.5 Email Server (remember this is inside the protected network)
- 10.2.1.1 Web Server
- 10.2.1.2 DNS Server

WE will use the following static mappings for the GIAC network

External Address	Internal Address	Function	Advertised
XXX.193.220.4	10.3.0.4	Email	Yes
XXX.193.220.5	10.2.0.2	DNS	Yes
XXX.193.220.6	10.2.0.3	WEB	Yes
XXX.193.220.7	10.1.0.2	VPN	No

Screened Subnet

We must configure the PIX to allow web traffic and DNS requests to come in to the external screened network. First, we must assign static addresses to the devices, then establish conduits through which data is passed.

WEB server

- `static (IN1, EX1) XXX.193.220.5 10.2.1.1 netmask 255.255.255.255`
- *Note: Here we have no set limit on the number of connections.*

DNS server

- `static (IN1, EX1) XXX.193.220.6 10.2.1.2 netmask 255.255.255.255 10 10`

Once the static addresses are assigned, we can assign the conduit through which data will travel. We assign a specific port number to the conduit and only traffic of that type will go to the respective server.

Enter the following command to setup the conduits for the above static address assignments:

DNS server

- `conduit permit udp XXX.193.220.6 255.255.255.255 eq 53 0.0.0.0 0.0.0.0`
- *Note: The PIX supports a DNS guard the helps prevent session hijacking and DOS attacks by determining the last response packet, even on UDP packets, and closes the session which prevents open UDP ports from being hijacked.*

WEB server

- `conduit permit tcp XXX.193.220.5 255.255.255.255 eq 80 0.0.0.0 0.0.0.0`
- `conduit permit tcp XXX.193.220.5 255.255.255.255 eq 443`
- `0.0.0.0 0.0.0.0`
- `fixup protocol http 80`

Now the PIX will accept any traffic destined for these two advertised addresses.

Partners Zone Subnet

The partner zone contains the databases that business partners will access. The databases are shielded behind the VPN Gateway. This zone also has all the outbound and returning traffic of internal employees as well as remote users.
The PIX must be configured with a conduit and the static mapping of the outside interface of the VPN device, in our case that is 10.1.0.2. The PIX interface on that side is 10.1.0.1. Any traffic the comes to the PIX with the outside IP address of the VPN is translated and forwarded to the VPN device provided it is on the correct port. The port can be any arbitrary port assigned to the VPN tunnel. Once at the VPN device, authentication is carried out and if the user succeeds they are forwarded to the appropriate segment either the partner databases or the Gauntlet. If the user is a remote user trying to access the corporate LAN then he/she is authenticated by the VPN and allowed on to the Gauntlet. If the packet is a returning connection from an inside user it is allowed to continue to the Gauntlet as well where it is proxied for content. A conduit for the internal email must all be configured on the PIX. This will allow foreign email hosts to establish SMTP connections with our email server.
Enter the following commands:

EMAIL server

- `static (partner_IN1, EX1) XXX.193.220.4 10.3.1.5 netmask 255.255.255.255 5 5`

- *Note: The netmask of the PIX works in reverse. By using all 255's it assumes you mean that exact host. It is not the same as an IP subnet mask. The 5 5 at the end of the command determines the number of connections and embryonic connections to this host. Five is sufficient for an email server. This helps in preventing SYN attacks as well.*

VPN Gateway

-
  ```
  static (partner_IN1, EX1) XXX.193.220.7 10.1.0.3 netmask
  255.255.255.255 10 10
  ```

EMAIL server

-
  ```
  conduit permit tcp XXX.193.220.4 255.255.255.255 eq 25 0.0.0.0
  0.0.0.0
  ```
- *Note: This command allows any outside host to send any packets destined for port 25 on the email host to the email host.*

To enhance the protection of the EMAIL server, we will implement the fixup feature of the PIX. This command enables the PIX to look into the payload of a packet of the protocol type specified with the command and look for application layer data that might not be allowed by the rule set. For the email server the fixup command only allows the commands listed in RFC 821, section 4.5.1 (namely, HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT). These commands are sufficient to send any SMTP mail. Commands used to possibly probe your email server on port 25, such as VRFY are dropped and an OK is replied back. The command is:

-
  ```
  fixup protocol smtp 25
  ```

VPN Gateway

-
  ```
  conduit permit tcp XXX.193.220.7 255.255.25.255 eq XXXX 0.0.0.0
  0.0.0.0
  ```
- *Note: The XXXX represents the port number that assigned the VPN client software.*

This completes the inbound setup of the two interfaces. Nothing else will be allowed passed the PIX and onto the network unless it is a returning packet from an outbound connection. We will tackle that next.

Authorizing outbound traffic

Because the PIX allows all OUTGOING protocols and connections by default unless explicitly denied, we need to add a few lines to limit what can go out of the network. One may ask why we would care about what goes OUT of out network. Well, in the event that something does get compromised on our network if it can't send data out it may be less harmful. If an employee brings a program from home that contains malicious code, such as BackOrifice, and violates the security policy by running it their computer, the trojan will have a difficult time determining which port is available to escape the network. This will greatly limit the trojan's impact on the network and hopefully it will be detected during the next virus scan.

Since Internet access is only permissible for web and email traffic the PIX needs to forward those packets and block all else, except for DNS outbound packets. In the PIX world, you need to identify the host or network that the packet will be coming from and which interface will be listening. This is very similar to other Cisco products. On our PIX, we have two inside interfaces and one outside interface. We will define the hosts that require outbound traffic. Web browsing and email are the only services allowed so the following lines need to be added to the PIX:

- `outbound 1 permit 10.3.1.4 255.255.255.255 25 tcp`
- `outbound 1 deny 10.3.1.4 255.255.255.255 0 tcp`
- `outbound 1 deny 10.3.1.4 255.255.255.255 0 udp`
- `outbound 1 deny 10.3.1.4 255.255.255.255 0 icmp`
- `apply (inside) 1 outgoing_src`

- `outbound 2 permit 10.3.0.0 255.255.0.0 80 tcp`
- `outbound 2 permit 10.3.0.0 255.255.0.0 443 tcp`
- `outbound 2 deny 10.3.0.0 255.255.0.0 0 tcp`
- `outbound 2 deny 10.3.0.0 255.255.0.0 0 udp`
- `outbound 2 deny 10.3.0.0 255.255.0.0 0 icmp`
-
- `apply (inside) 2 outgoing_src`

- `outbound 3 deny 0.0.0.0 0.0.0.0 0 tcp`
- `outbound 3 deny 0.0.0.0 0.0.0.0 0 udp`
- `outbound 3 deny 0.0.0.0 0.0.0.0 0 icmp`
- `apply (inside) 3 outgoing_src`

The first outbound list (outbound 1) allows the email server (10.3.1.4) to send only SMTP on port 25 out to the Internet. This satisfies the requirement because internal connections will use this host to send outbound email. This prevents accessing "home" email accounts via SMTP that can circumvent the virus protection. The next three lines deny the server from sending out any other packets. UDP is not necessary because the server will point to the internal DNS for queries. The last line associates the ACL with the proper interface.

Outbound list 2 allows any device on the internal network (10.3.0.0) to initiate any web or SSL connection to the Internet. It denies any other attempts at initiating other protocol connections outbound. This will eliminate chat programs such as Powwow, instant messaging programs such as ICQ and AOL Instant Messenger. These programs have their own file transfer utility that can be extremely dangerous if not protected.

Finally, we have a catch all entry that denies any other address from initiating any connections with the Internet. This is applied to the inside as well, which covers both the screened subnet and the partners subnet.

Our first line perimeter is now in place and provides a high level of screening for the network.

Administering the PIX

We must add few lines that controls the administration of the PIX. Since no telnet sessions are allowed to connect to any external PIX interface there is no command to protect this. From the inside, however, the interface can be accessed and we must trap this. Enter the command:

- `no telnet 0.0.0.0 0.0.0.0`

Since we are connected to the PIX via a serial cable from the TACACS server we have no need to access it via a telnet session. Administrators telnet to the TACACS server and after being authenticated a terminal session is established with the PIX via the serial port.

We also want to make sure there is logging turned on at the PIX. Enter the commands:

- `logging facility 20`
- `logging host inside 10.3.0.6`

This sets the logging level to informational and directs the output to out log server.

We also need to make sure SNMP is not turned on and the default passwords are cleared. Enter the following commands:

- `no snmp-server location`
- `no snmp-server contact`
- `snmp-server community !@#$%^&`
- `no snmp-server enable traps`

These commands ensure the snmp password is not “public” and that the PIX does not accept traps which could be harmful.

Protecting against CERT advisory CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests (http://www.cert.org/advisories/CA-2000-02.html)

This vulnerability is exercised when a client inside the firewall browses to an external server and selects a link that the firewall interprets as two or more FTP commands. The client begins an FTP connection as expected and at the same time unexpectedly executes another command opening a separate connection through the firewall.

PIX can prevent malicious HTML code from reaching the screened web server and any other device by adding the following command:

- fixup protocol ftp strict 21

Protecting against CERT Advisory CA-96.21: TCP SYN Flooding and IP Spoofing Attacks

The TCP SYN attack is characterized by an influx of SYN packets from random source IP addresses. Any device behind a firewall that stops inbound SYN packets is already protected from this mode of attack and no further action is needed. Examples of firewalls include a Cisco Private Internet Exchange (PIX) Firewall or a Cisco router configured with access lists. By default we are protected.

Our PIX configuration should look like this. Not all the items in this configuration were covered in this document.

```
# Interface Section (3 interfaces)
#
# interface 'inside'
#
nameif partner_IN1  security100
interface ethernet1 10baset
ip address inside 10.2.0.1 255.255.0.0
no rip inside passive
no rip inside default
#
#
# interface 'inside'
#
nameif Screened_IN1  security50
interface ethernet2 10baset
ip address inside 10.1.0.1 255.255.0.0
no rip inside passive
no rip inside default
#
# interface 'outside'
#
nameif EX0 outside security0
interface ethernet0 10baset
ip address outside XXX.193.220.2 255.255.255.0
no rip outside passive
no rip outside default
#
# Routes Section
#
route outside 0.0.0.0 0.0.0.0 XXX.193.220.1 2
#
fixup protocol http 80
fixup protocol smtp 25
fixup protocol rsh 514
fixup protocol ftp strict 21
#
#     Static Mappings
#
# Email Server
static (Partner_IN1, EX1) XXX.193.220.4 10.3.1.4 netmask 255.255.255.255 5 5
# VPN Gateway
static (Partner_IN1, EX1) XXX.193.220.3 10.1.0.2 netmask 255.255.255.255 10
10
# WEB server
static (Screened_IN1, EX1) XXX.193.220.5 10.2.1.1 netmask 255.255.255.255
# External DNS
static (Screened_IN1, EX1) XXX.193.220.6 10.2.1.2 netmask 255.255.255.255 10
10
# VPN Gateway
static (partner_IN1, EX1) XXX.193.220.7 10.1.0.3 netmask 255.255.255.255 10
10
#
#     Conduits
#
# Email Server
conduit permit tcp XXX.193.220.4 255.255.255.255 eq 25 0.0.0.0 0.0.0.0
#  Web Sever
conduit permit tcp XXX.193.220.5 255.255.255.255 eq 80 0.0.0.0 0.0.0.0
conduit permit tcp XXX.193.220.5 255.255.255.255 eq 443 0.0.0.0 0.0.0.0
# DNS Server
conduit permit udp XXX.193.220.6 255.255.255.255 eq 53 0.0.0.0 0.0.0.0
# VPN Gateway
conduit permit tcp XXX.193.220.7 255.255.255.255 eq XXX 0.0.0.0 0.0.0.0
#     Note: the XXX is replaced with the port number assigned to the
#     VPN Client.
outbound 1 permit 10.3.1.4 255.255.255.255 25 tcp
outbound 1 deny 10.3.1.4 255.255.255.255 0 tcp
outbound 1 deny 10.3.1.4 255.255.255.255 0 udp
outbound 1 deny 10.3.1.4 255.255.255.255 0 icmp
apply (inside) 1 outgoing_src

#
outbound 2 permit 10.3.0.0 255.255.0.0 80 tcp
outbound 2 permit 10.3.0.0 255.255.0.0 443 tcp
outbound 2 deny 10.3.0.0 255.255.0.0 0 tcp
outbound 2 deny 10.3.0.0 255.255.0.0 0 udp
outbound 2 deny 10.3.0.0 255.255.0.0 0 icmp
apply (inside) 2 outgoing_src
#
outbound 3 deny 0.0.0.0 0.0.0.0 0 tcp
outbound 3 deny 0.0.0.0 0.0.0.0 0 udp
outbound 3 deny 0.0.0.0 0.0.0.0 0 icmp
```

```
apply (inside) 3 outgoing_src
#
no telnet 0.0.0.0 0.0.0.0
#
logging facility 20
logging host inside 10.3.0.6
#
no snmp-server location
no snmp-server contact
snmp-server community !@#$%^&
no snmp-server enable traps
#
mtu outside 1500
mtu inside 1500
floodguard 1
Cryptochecksum: 1233498459388993eabf0
: end
```

Gauntlet Setup

On the GIAC network the main purpose behind the Gauntlet Firewall is to ensure packet content is safe. The PIX is providing a high level of security at the perimeter but it does not look at the content of the packets that are traversing it over authorized ports. The Gauntlet will perform content scanning looking for viruses and erroneous information on HTTP and SMTP. Web pages can contain malicious content and applications. When you enable content scanning, the firewall scans Web pages before it displays them. It scans files transferred via the HTTP proxy, whether they were retrieved via http or ftp URLs. **Note: it is assumed that the basic setup of the Gauntlet is already performed as whole books can be written describing how to setup the firewall. I will concentrate on the setting for this exercise.*

The type of content for which the firewall scans depends on user configurable options. The common types of files that these engines can scan are:

- e-mail messages
- attachments to e-mail messages (for example, Microsoft Word documents)
- program files (exe, com...)
- compressed or encoded files (for example, ZIP, MIME)
- Java applets, active X
- Javascript

To access content scanning configuration for mail:
1. From within the Gauntlet Firewall Manager, select the **Proxies** tab.
2. Double-click **smtp** from the list box, or select smtp and click **Modify Proxy Defaults**.
3. Click the **Virus Scan** button.
The Virus Scanning Settings screen displays.

4. Select the **Enabled** radio button to enable virus scanning, or select **Disabled** to disable the feature.
When **Enabled** is selected, provide information about the following.

Field	**Description**
Options	Select Repair
What to scan	Select ALL files.

To access content scanning configuration for the HTTP proxy service:
1. From within the Gauntlet Firewall Manager, select the **Proxies** tab.
2. Double-click **http** in the list box.
3. Click the **Virus Scan** button.
Select the **Enabled** or **Disabled** radio button to enable or disable virus scanning for the HTTP proxy.

To configure content scanning:
1. Select the **Proxies** tab.
2. Double-click **http** and **smtp** from the list box.
3. Click the **Virus Scan** button for **HTTP** and **SMTP**.
4. Click **Enabled** and provide information about the following.

Field	**Description**
Virus Scanning	Select Enabled to activate content scanning
Infected Files	Choose Repair Infected files
What to scan	Choose ALL files

5. Click **O**K.

You must configure the SMTP proxy and the HTTP proxy so the content scanning can work. Here are the setups to setup the proxies:

To configure the HTTP proxy:
1. In the Gauntlet Firewall Manager, click on the Proxies tab.
2. Double-click **http** in the list of proxies. The HTTP Proxy Default Configuration screen displays.
3. Keep or change the standard configuration.
Each proxy comes with standard or default configurations. You can change these configurations to match your security policy. Whichever you choose, the HTTP proxy provides the same services: passing requests through the firewall with access control, authentication, and logging.

Field	**Description**
Proxy Status	Select **Enabled**
Authentication Options	Click Never (http) to tell the proxy not to require authentication.
Timeout in Seconds	Enter 1200
Additional Ports to listen	Leave blank
Deny Message File	Create a text file that contains text with an

	appropriate message
HandOff Parameters	Leave Blank
Port	Leave Blank

In the “Feature(s) Blocked” section, select Java Script. Java Script has the ability to contain malicious code and should be blocked whenever possible.

Click OK

To configure the SMTP proxy:

1. Select the Proxies tab at the Gauntlet Firewall Manager.
2. Double-click **smtp** in the list box, or select **smtp** and click **Modify Proxy Detail**s.
The SMTP Proxy Configuration screen displays.
3. Enter the following information.

Proxy Status	Enabled
Enable Reverse DNS Lookup	Disable
Timeout in seconds	600
Mail Hub	10.3.0.4
Shorten Sender Address to Domain Name	Leave Blank

Click the VIRUS Button to access the Virus enable screen and turn that on.

This satisfies the requirements of our security architecture.

SECTION THREE

Security Audit of GIAC Enterprises

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises, a electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly.

Planning the Assessment

After reviewing the security documentation provided from the security manager at GIAC Enterprises, the following plan was developed to audit the network.

Since the network is segmented into three easily discernable segments auditing and penetration testing will be performed from the following areas:

- Externally from the Internet inward trying to penetrate the screened segment, the partner segment, and the protected network
- From the Screened subnet outward trying to penetrate the partner segment and the protected network
- From the partner segment trying to penetrate the screened network and the protected network
- Internally from the protected network outward trying to connect outbound with unauthorized protocols

Since this is a production environment and operational uptime is paramount the decision was made to run the test from midnight Saturday until Midnight Sunday. This provides a 24-hour window in which data can be gathered. Any traffic connecting to the site should be light and impact should be minimal on any production requirements.

After the data gathering is completed analysis should take approximately two days. A briefing will be provided to the CIO, Security Manager, and any other invited participants. Attendance should be minimized to key personnel only in case any unfavorable information is brought forth. This would help to prevent the “social gossip” that may ensue any report of security flaws or weaknesses.

The charge for the analysis is on a per job basis. This ensures the customer they are getting an adequate job based on need and observation and not on stretching out the time to make more money. Cost of the GIAC analysis is $6500.00. This includes any licensing requirements of software, the complete audit, hard copy analysis, interpretation of results, and recommendations.

The main tool that will be utilized in the audit is Internet Security Systems Internet Scanner.® (http://www.iss.net/securing_e-business/security_products/)
This product offers a robust suite of scanning tools that can be configured in various ranges, from light probing to heavy duty DOS attacks. The results are well laid out and even offer suggested resources to help fix the problem. It currently has a database of over 739 exploits.
Nmap, (http://www.insecure.org/nmap/) a freely available probing and scanning product, will also be used. This product will act as a sanity check to verify the results of the ISS scan. And since many would-be attackers will be using Nmap it will be prudent to test against it. Other tools that will be used to test the requirements are l0phtCrack, which will test password strength on Windows NT and Windows 95 machines and Crack which will test password strength on Unix machines.

Common Components

All four penetration scenarios share some common elements. These should be setup prior to any other setup required for the individual plan.

- Place a hub between the PIX and the ISP router.
- Place a hub on the screened segment
- Place a hub on the partner segment
- Place a hub behind the Gauntlet
- Connect one WindowsNT PC to each hub and run winDUMP to gather statistics

External Plan

Objective – Run a series of probes from the Internet side of the PIX to determine any infiltration of the network behind the PIX. The data received should not show any signs of connection on unauthorized ports and services.

- Connect a UNIX(Linux) and Windows NT-based computers to the hub.
- Configure the machines with the proper IP addresses and default gateway
- Disable the winDUMP on this segment
- Run Internet Security Systems Internet Scanner® against target network
- Run Nmap against the target network
- Record and save results.

Screened Segment Plan

Objective – Run a series of probes from the screened segment against the PIX with emphasis on penetrating the partners segment and the protected network. Packets should not be seen on any segment, including the Internet segment.

- Connect a UNIX(Linux) and Windows NT-based computers to the hub.
- Configure the machines with the proper IP addresses and default gateway

- Disable the winDUMP on this segment
- Run Internet Security Systems Internet Scanner® against target network
- Run Nmap against the target network
- Record and save results.

Partners Segment Plan

Objective – Run a series of probes from the partners segment against the PIX and the Gauntlet with emphasis on penetrating the protected network and the screened segment. Packets should not be seen on either segment, except for those authorized.

- Connect a UNIX(Linux) and Windows NT-based computers to the hub.
- Configure the machines with the proper IP addresses and default gateway
- Disable the winDUMP on this segment
- Run Internet Security Systems Internet Scanner® against target network
- Run Nmap against the target network
- Record and save results.

Internal Segment Plan

Objective – Run a series of probes from the internal network against the Gauntlet with emphasis on reaching the Internet from within the protected network.

- Connect a UNIX(Linux) and Windows NT-based computers to the hub.
- Configure the machines with the proper IP addresses and default gateway
- Disable the winDUMP on this segment
- Run Internet Security Systems Internet Scanner® against target network
- Run Nmap against the target network
- Run l0phtCrack and/or Crack against all the servers trying to crack passwords
- Try to capture passwords from login sessions to protected devices
- Capture sessions involving protected servers, such as HR and Payroll
- Record and save results.

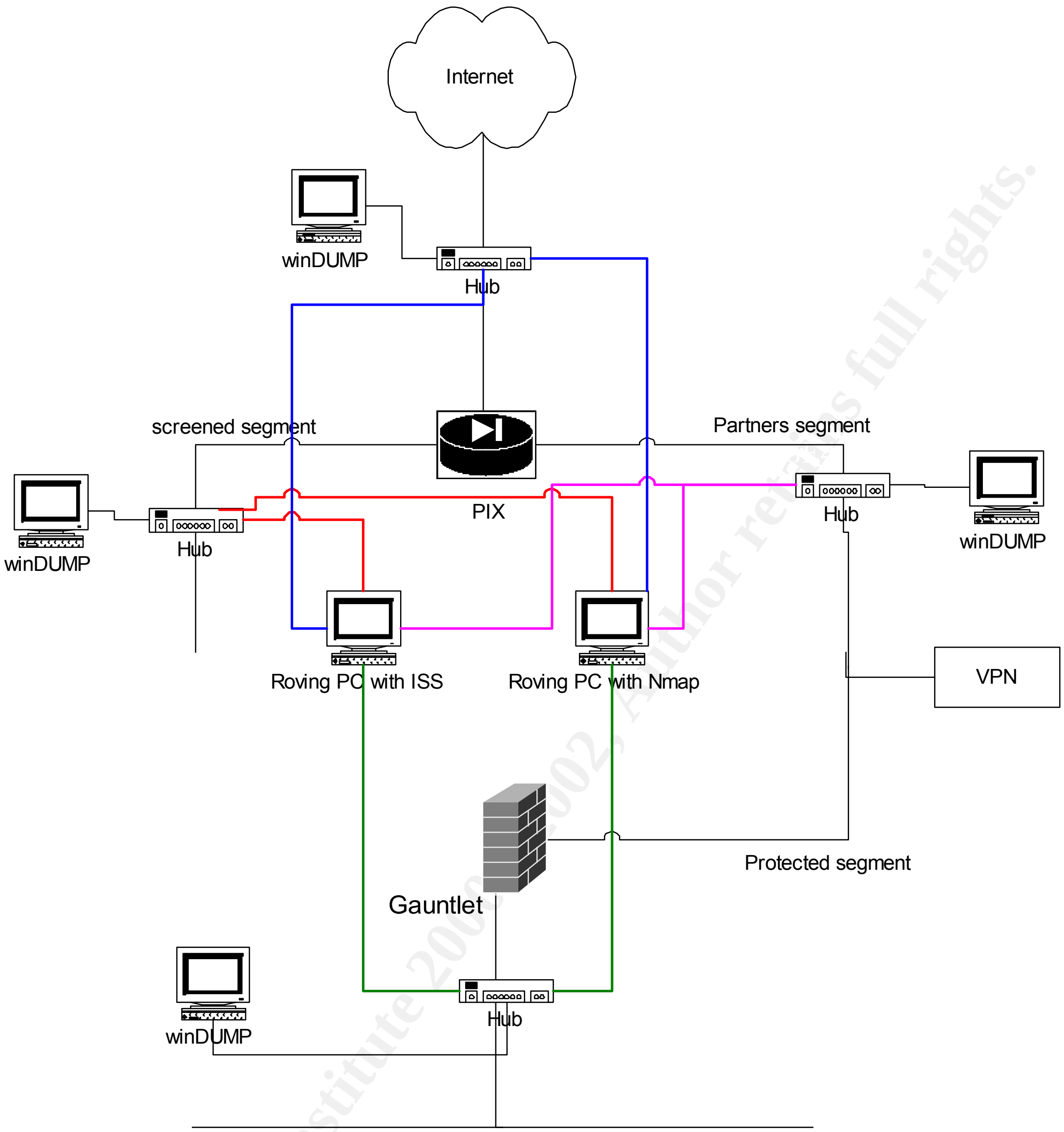


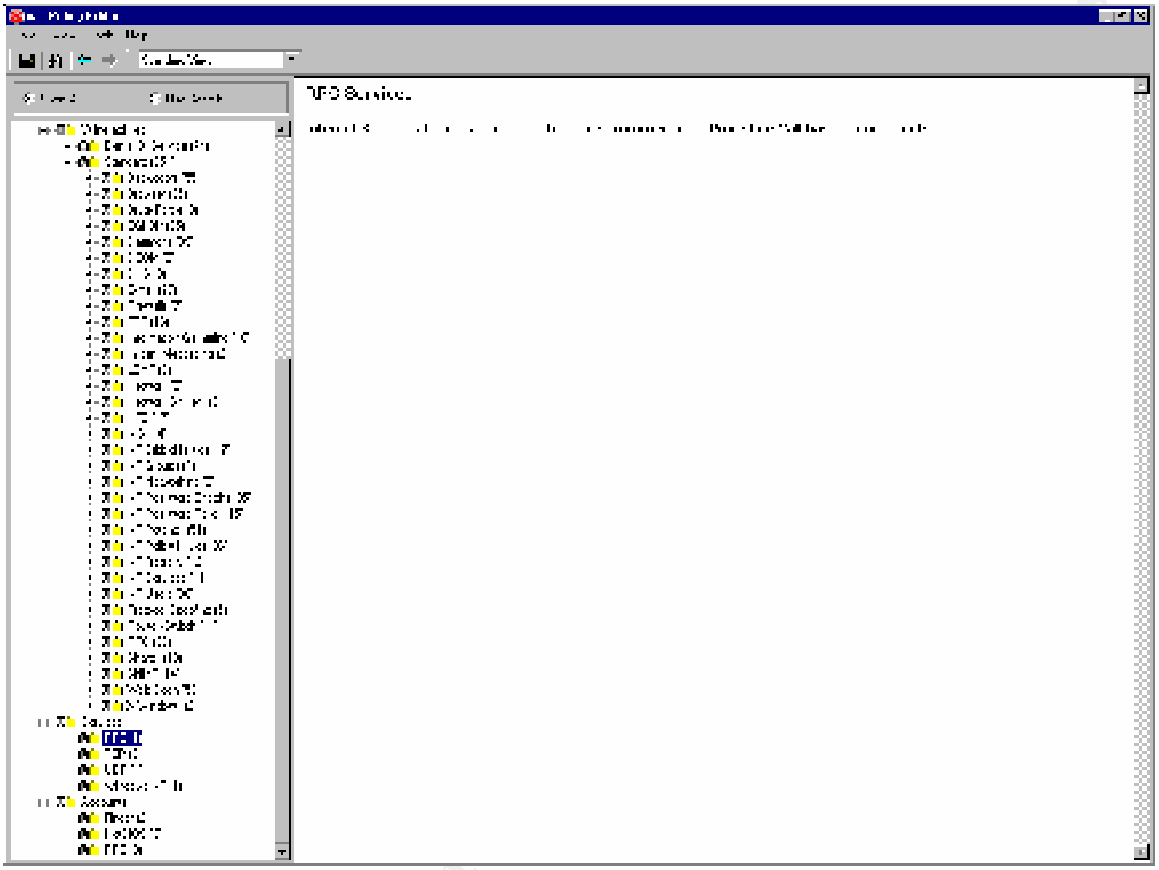
Figure 2 Audit setup

Implementation

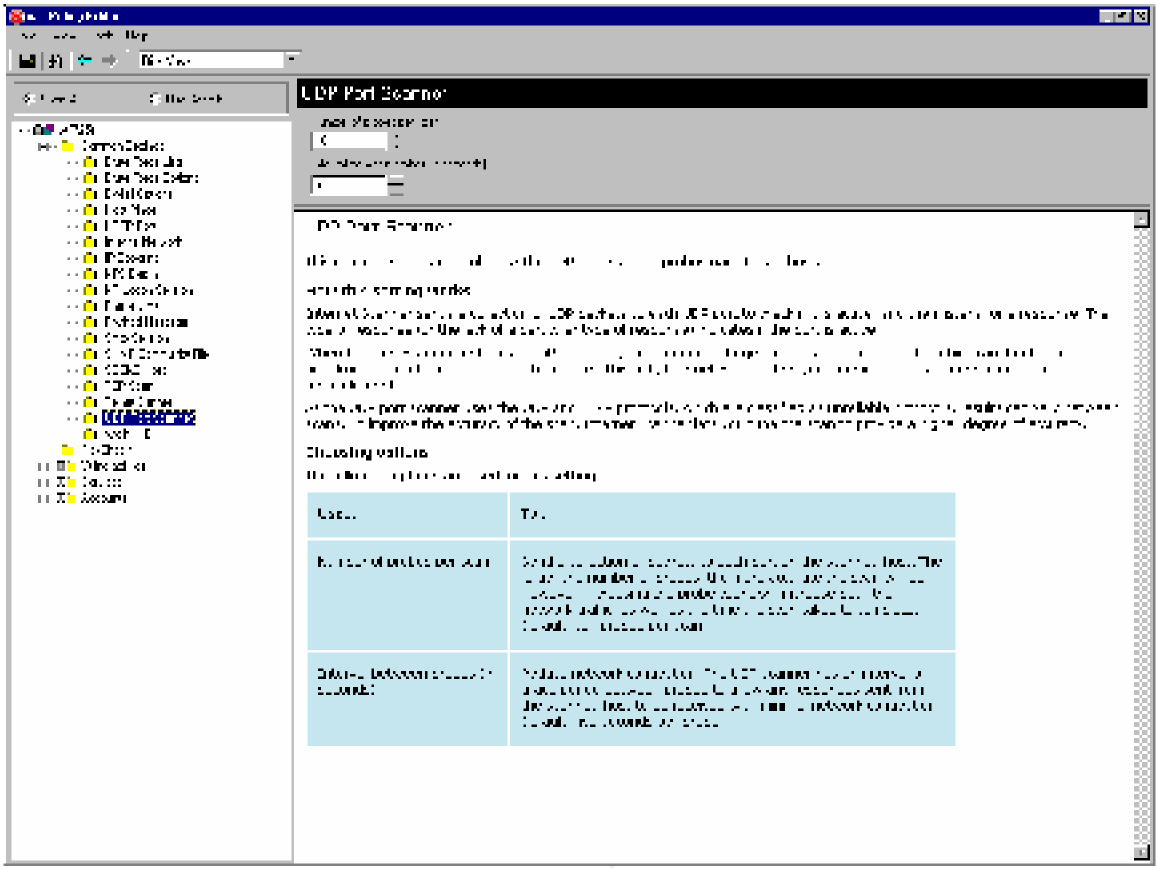
Prior to midnight on the chosen Saturday, all PCs should be loaded with the appropriate software, configured with the correct IP addresses, and staged in the area where they will be connected to the network. After meeting with network personnel on duty to ensure everything is still a go, testing can begin.

Because this is a scan of a production system, it is imperative that NO denial-of-service scans be accomplished. Although this is important to test it should be done in a lab with duplicate network setups or when the enterprise can be taken off line for maintenance. Since this is an unlikely event, DOS attempts will have to be conducted in a lab environment.

Using ISS to scan from the Internet zone requires settings to be configured to match what a would be attacker would perform. Port scans, network address scans, service and daemon registry, remote logins, etc. are but a few of the settings. Please refer to the following screen capture for reference.



Please note that all the scans are enabled except for the Denial of service scans that can cripple a network. In addition to the scans selected above, ISS will perform a list of common setting scans, as shown below.



This scan should be accomplished in three different stages. The first stage will concentrate on the port scanning and network mapping. The second stage will take information from the first stage and probe any hosts found. The final stage will perform light to medium brute force attacks against exposed hosts. This should not be confused with DOS attacks.

The scan from the screened subnet will include server attacks as this scan assumes someone has breached the first level security perimeter. Scans will attempt to crack passwords on the server using l0phtCrack and ISS. Windows NT registry vulnerabilities such as the WINREG key and write-enabled LSA-key vulnerabilities will be attacked. Scans against known HTTP and DNS vulnerabilities will be executed. These will include the following vulnerabilities:

- HTTPcgi buffer overflow attacks
- IIS HTR Overflow
- IIS Remote Data Services
- IIS Remote User Password Change
- IIS SampleCodebrws
- IIS adminpwd
- IIS DOT DOT Crash
- IIS bdir

And others as needed, this is not all encompassing. Since we know the web server is Microsoft IIS based, we can limit the scan to those vulnerabilities. Time permitting, we will run all the scans for all versions of http daemons.

The scan from the partners segment will concentrate mainly on breaking the VPN gateway. The potential here is mainly on DOS attacks which we can attempt since there will be no access to the VPN during the scan and the general public does not access this area. From behind the PIX looking at the VPN gateway we can perform the following:

- MIB Walking
- TCP scanning
- SNMP Community
- TearDrop
- TfnDos
- ICMP Redirect
- Oob_crash
- Pingbomb
- Syncstorm
- Udpbomb
- dataflood
- Any attack associated with the services behind the VPN Gateway

Of particular note here are the TearDrop and TfnDos attacks. If the winDump sees packets off this type we must rely solely on the OS for protection. We should not see any traffic traversing the gateway. The gateway itself should be immune to any of these attacks. The gateway should be observed from a console port to ensure it's integrity remains intact.

Against the Gauntlet we can run similar scans, also attacking the integrity of the host OS. All the Windows NT exploits should be run, including account brute force break-ins, registry attacks, and the Gauntlet CyberDaemon Buffer overflow attack, and the above attacks.

From behind the Gauntlet, on the protected network, scans should be run against all servers and PCs, against the internal interface of the firewall and attempts should be made to reach the Internet. In addition to the above, all servers should have the following scans run against them:

- l0phtCrack – for password integrity
- registry hacks, such as LSA, anonymous access, POSIX subsystem
- All up-to-date hotfixes and service packs

All the PCs should be checked for backdoor exploits such as:

- BackOrifice
- BackDoorCow
- BackDoorFrenzy

This will help ensure PCs are not vulnerable and have not become tainted with any trojans.

The sniffer outside the PIX should be monitored for unauthorized outbound traffic. The following attempts should be made:

- Send/retrieve email from foreign hosts (using SMTP and POP3)
- instant messaging agents should be executed
- ICMP protocol suite

PCs should also be checked for the ability to enter promiscuity mode. This would enable anyone to sniff-the-wire.

Nmap should be run from all the areas that ISS is run to use as a sanity check. T

ANALIZING THE DATA

Gather the information from all windump machines. Extrapolate the information into a extensible format suitable for searching, such as a spreadsheet or database. Gather the Nmap and ISS data. Compare the scans with the captured data.

The scans from the Internet inward toward the screen segment should show connections to ports 80 and 443 on the Web server and port 53/UDP on the DNS server. No service or user accounts should be visible or accessible. No connections should have been made to the VPN gateway. A connection should have been made to the internal email host on port 25/tcp. The PIX should not have returned any ICMP information, including error messages.

The data from the screened segment and out should have shown the services running on the DNS and WEB servers and nothing else. Accounts should not have had their passwords cracked. No traffic should have been seen on the partners segment or the protected segment that originated on this screened segment.

The partners segment scan should not have shown the devices sitting behind the gateway. It should have shown the interface for the VPN gateway and the Gauntlet. The sniffer on the screened segment should have shown attempts to access the WEB and DNS service since the partners PIX interface has a higher security level than that of the screened segment.

The internal scan should have shown only authorized protocols in the sniffer located on the Internet interface. The PCs would not have had any back doors or trojans.

Recommendations

Several recommendations come to light after analysis of the data. They are:

- Deploy intrusion detection appliances at key areas throughout the network. Such as:
  - In front of the PIX. This may seem frivolous; however, it is always a prudent security stance to see who is knocking at the door and what they are looking for when they knock. It also can be used to correlate data from both sides of the PIX and see what is actually happening to the packets.
  - Behind the Gauntlet on the protected network. This would help look at what the users are accessing. It will also aid in protocol isolation which can assist in troubleshooting.
  - A floating IDS that can be placed anywhere when needed.
- Move the screened subnet behind a proxy firewall. This will help ensure the content of the packets is that which was intended.
- Load balance/duplex the Gauntlet. This eliminates a single point of failure for the protected segment
- Load balance/duplex the PIX. This eliminates a single point of failure for the demarcation line into GIAC Enterprises.
- Run a system scanner on every server, both internal and external, to ensure they are hardened to the fullest extent possible.
- Move the VPN gateway to a segment off of the firewall instead of being a device between the PIX and Gauntlet.
- Create and install an external email host and relay email into the protected network. This ensures only known hosts are connecting to devices behind the firewall.

Justification for a screening Router

- Place a screening router between the PIX and the ISP to ensure that all basic blocking filters are in place and under the control of GIAC personnel. Although the PIX will block everything a screening router would block, this measure would help because of the lack of control at the ISP router and more importantly it would help in detecting and analyzing DoS attacks, such as 'smurf', 'fraggle', and SYN flood.

**Note: The following is excerpted from the Cisco document "*Characterizing and Tracing Packet Floods Using Cisco Routers" *located at http://www.cisco.com/warp/public/707/22.html*

The packets in many DoS attack streams can be isolated by matching them against Cisco IOS software access list entries. This is obviously valuable for filtering out attacks, but is also useful for characterizing unknown attacks, and for tracing "spoofed" packet streams back to their real sources.

Cisco router features such as debug logging and IP accounting can sometimes be used for similar purposes, especially with new or unusual attacks. However, with recent versions of Cisco IOS software, access lists and access list logging are the premiere features for characterizing and tracing common attacks. A wide variety of DoS attacks are possible. Even if we ignore attacks that use software bugs to shut down systems with relatively little traffic, the fact remains that any IP packet that can be sent across the network can be used to execute a flooding DoS attack. When you are under attack, you must always consider the possibility that what you're seeing is something that does not fall into the usual categories. We can use a screening router to help analyze the flow of this traffic. Now, suppose that we apply an access list as follows:

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

This list doesn't filter out any traffic at all; all the entries are permits. However, because it categorizes packets in useful ways, the list can be used to tentatively diagnose all three types of attacks: smurf, SYN floods, and fraggle.

If we issue the **show access-list** command, we'll see output similar to the following:

```
Extended IP access list 169
permit icmp any any echo (2 matches)
permit icmp any any echo-reply (21374 matches)
permit udp any any eq echo
permit udp any eq echo any
permit tcp any any established (150 matches)
permit tcp any any (15 matches)
permit ip any any (45 matches)
```

It's obvious that most of the traffic arriving on the serial interface consists of ICMP echo reply packets. This is probably the signature of a smurf attack, and our site is the ultimate target, rather than the reflector. We can easily gather more information about the attack by revising the access list, as shown below:

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

```
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

The change here is that we've added the **log-input** keyword to the access list entry that matches the suspect traffic. (Cisco IOS software earlier than version 11.2 lacks this keyword, and we would use the keyword "**log**" instead.) This will cause the router to log information about packets that match the list entry. Assuming that **logging buffered** is configured, we can see the resulting messages with the **show log** command (it may take a while for the messages to accumulate because of rate limiting). The messages might look something like this:

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33 (Serial0 *HDLC*) ->
10.2.3.7 (0/0), 1 packet
```

We see that the source addresses of the echo reply packets are clustered in a few address prefixes: 192.168.212.0/24, 192.168.45.0/24, and 172.16.132.0/24. This is very

characteristic of a smurf attack, and the source addresses are the addresses of the smurf reflectors. By looking up the owners of these address blocks in the appropriate Internet "whois" databases, we can find the administrators of these networks, and ask for their help in dealing with the attack.
It's important at this point in a smurf incident to remember that these reflectors are fellow victims, ***not*** attackers. It's extremely rare for attackers to use their own source addresses on IP packets in any DoS flood, and impossible for them to do so in a working smurf attack. Any address in a flood packet should be assumed to be either completely falsified, or the address of a victim of some sort. The most productive approach for the ultimate target of a smurf attack is to contact the reflectors, either to ask them to reconfigure their networks to shut down the attack, or to ask for their assistance in tracing the stimulus stream.

Because the damage to the ultimate target of a smurf attack is usually caused by overloading of the incoming link from the Internet, there's often no response other than to contact the reflectors; by the time the packets arrive at any machine under the target's control, most of the damage has already been done.
One stopgap measure is to ask the upstream network provider to filter out all ICMP echo replies, or all ICMP echo replies from specific reflectors. This sort of filter shouldn't usually be left in place permanently. Even for a temporary filter, only echo replies should be filtered, *not* all ICMP packets. Another possibility is to have the upstream provider use quality of service and rate limiting features to restrict the bandwidth available to echo replies; a reasonable bandwidth limitation can be left in place indefinitely. Both of these approaches depend on the upstream provider's equipment having the necessary capacity, and sometimes that capacity is not available. This is where having a good relationship and SLA with your ISP comes in handy.

As we can see, there is more value to a screening router than basic filtering.

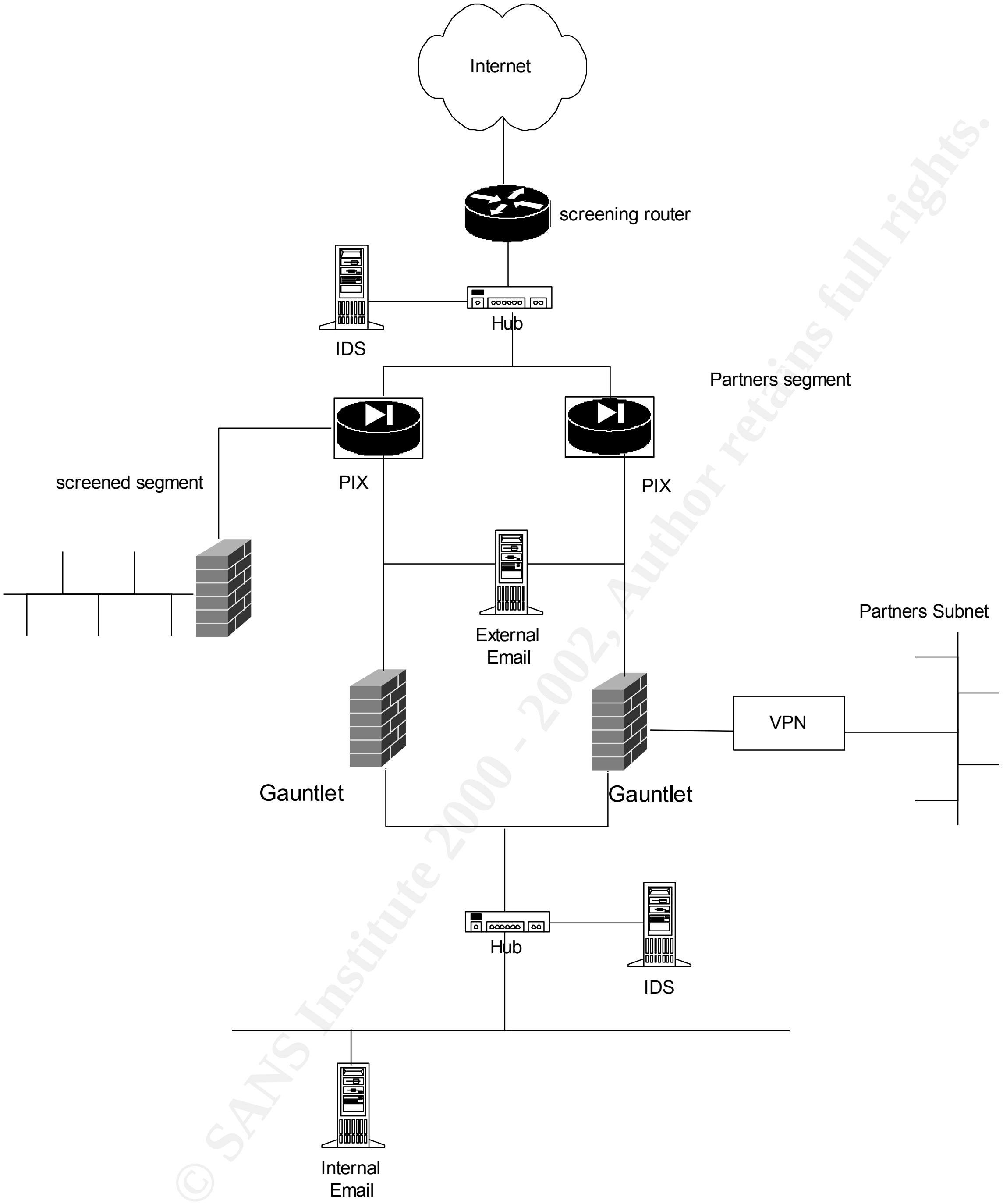


Figure 3 – Recommended network architecture